

Puesta en marcha de un cortafuegos con IPTables



Orlando Alemán Ortiz
Samuel Díaz Cabrera

4º Ing. Informática
Curso 2005/06

Licencia



Esta obra ha sido publicada bajo licencia "Reconocimiento-NoComercial-CompartirIgual 2.5 Spain" de Creative Commons, la cual implica que:

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:



Reconocimiento. Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador.



No comercial. No puede utilizar esta obra para fines comerciales.



Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Y además:

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor
- Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.

Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-sa/2.5/es/> o envíe una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Índice de contenidos

| | |
|------------------------------------|---|
| 1. Previos..... | 2 |
| Introducción..... | 2 |
| Equipamiento empleado..... | 3 |
| 2. Desarrollo..... | 4 |
| Puesta en marcha del servicio..... | 4 |
| Configurando el cortafuegos..... | 4 |
| 3. Referencias bibliográficas..... | 8 |

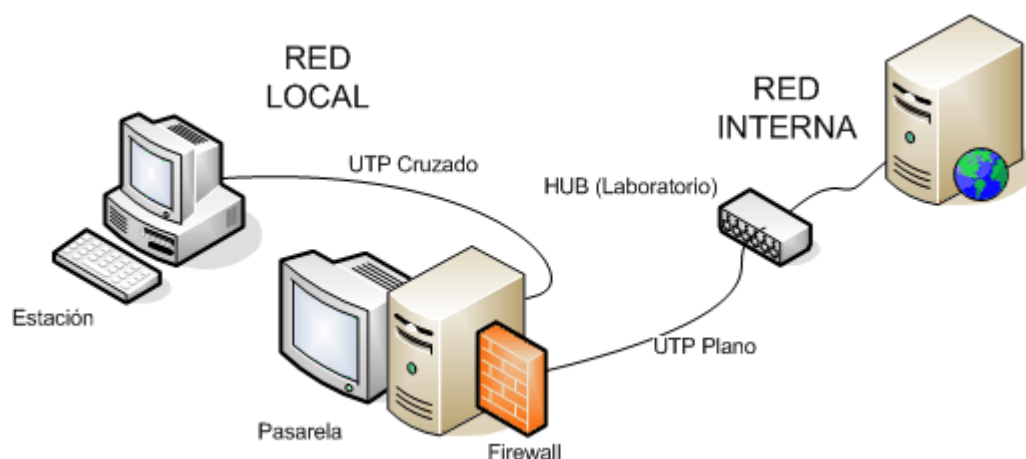
1. Previos

Introducción

El presente documento constituye la quinta memoria de prácticas de la asignatura. En esta ocasión el reto que se nos plantea es el de utilizar *IPTables* para establecer las reglas de filtrado de paquetes que *Netfilter* utiliza para gestionar el tráfico de datos de red entrante y saliente. Es, por tanto, una tarea de administración sobre la plataforma *GNU/Linux*.

Comúnmente se denomina *IPTables* al conjunto formado por las tablas de reglas y la herramienta de usuario que se le concede al administrador para modificarlas. A diferencia de otras soluciones firewall, se encuentra estrechamente vinculado con el kernel, lo que le permite cierta potencia y versatilidad que otras soluciones no disfrutaban. Por esta razón, se ha extendido enormemente a partir de la versión 2.4 del núcleo.

Siendo fieles a nuestro esquema habitual de red, introduciremos el firewall como un nuevo elemento en juego. En este caso será un componente software, aunque conceptualmente lo representaremos como una muralla que actúa entre Internet y la máquina que actúa como pasarela.



Tendremos por tanto un esquema muy típico donde se protege a la red local desde un servidor de seguridad, al cual se conectan el resto de equipos. No resultaría difícil tampoco que cada máquina dispusiese de un cortafuegos propio, si bien parece carecer de sentido en nuestro esquema.

Equipamiento empleado

Hardware:

- 1 x PC con 2 tarjetas de red, que actuará como pasarela.
- 1 x PC con 1 tarjeta de red, que actuará de estación.
- 1 x cable de red UTP Cat.5 plano con conectores RJ45
- 1 x cable de red UTP Cat.5 cruzado y con conectores RJ45

Software:

- Por cada PC, una instalación de *Fedora Linux*.
- En la pasarela, el software IPTables y la una compilación del núcleo que permita cargar los módulos adecuados [todo esto está disponible por defecto en esta distribución].

2. Desarrollo

Fedora Linux proporciona en su instalación por defecto (la que fue realizada en las máquinas del laboratorio) tanto las herramientas de gestión como la compilación adecuada del núcleo, para poder montar un servidor de seguridad en poco tiempo. Partiendo de esta premisa, vamos a explicar a continuación los pasos seguidos para llevar a cabo esta práctica.

Puesta en marcha del servicio

Antes de ejecutar cualquier otro paso, comprobamos que *IPTables* está instalado en el sistema

```
$ rpm -q iptables
iptables-1.2.11-3.1
```

Como la respuesta ha sido afirmativa (es decir, devolvió el nombre canónico del paquete), podemos pasar a la fase de configuración. Si no estuviese instalado, por cualquier razón, podríamos obtenerlo desde un repositorio oficial, con la herramienta YUM:

```
$ yum install iptables
```

Configurando el cortafuegos

Como ya sabemos, *IPTables* es una herramienta que permite añadir, modificar o borrar reglas. Existen dos formas de utilizarla: estableciendo manualmente las reglas en el fichero “/etc/sysconfig/iptables” o directamente pasándolas como argumento al binario ejecutable. La primera implica la utilización del script “/etc/init.d/iptables” que nos facilita la distribución para arrancar el firewall; la segunda, permite comprobar la aplicación de reglas “al vuelo”.

Para activar el servicio en los niveles para los cuales la red está activa, tecleamos:

```
$ chkconfig --level 345 iptables on
```

Nótese que siempre es posible combinar ambas estrategias, guardando las nuevas reglas con

```
$ service iptables save
```

de forma que sean aplicadas tras reiniciar el servicio “iptables”:

```
$ service iptables restart
Parando iptables: [ OK ]
Iniciando iptables: [ OK ]
Aplicando las reglas del cortafuegos iptables: [ OK ]
```

Práctica 5: Puesta en marcha de un cortafuegos con IPTables

Después de estos preludios, vamos a pasar a la parte que nos interesa: la implementación del cortafuegos.

La política que estableceremos por defecto es la de DENEGAR todos los paquetes, salvo aquéllos que hayan sido permitidos explícitamente. Para ello, borramos todas las reglas que pudieran haber sido introducidas previamente y aplicamos la regla “DROP” a las cadenas INPUT, OUTPUT y FORWARD, responsables del tráfico entrante, saliente y de paso, respectivamente:

```
# Desechamos las reglas previas
## Borra todas las cadenas (de la tabla filter, la tabla por defecto)
iptables -F
## Borra las cadenas opcionales definidas por el usuario
iptables -X
## Pone a 0 el contador de byte y de paquete en todas las cadenas
iptables -Z

# Bloqueamos todo el tráfico
## (la política por defecto será desechar)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Resulta interesante permitir el tráfico con la interfaz “loopback”, sin el cual muchos de los servicios que corren en nuestra máquina no pueden funcionar correctamente. Lo haremos con:

```
# Permitimos el tráfico de red dentro de nuestra máquina (por medio de la
interfaz loopback)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Para evitar el “spoofing” de nuestras tramas TCP/IP denegaremos todos los paquetes que, procedentes de la interfaz de acceso al exterior, tengan dirección IP local:

```
#!/bin/sh

REDLOCAL=172.16.14.0/24
DEVLOCAL=eth1
DEVINET=eth0

...

# Desechamos los paquetes entrantes que lleguen por la interfaz de acceso a
internet y utilicen IP local
iptables -A INPUT -i $DEVINET -s $REDLOCAL -j DROP
```

Los mensajes ICMP pueden resultar interesantes para la supervisión de los ordenadores de nuestra red. Permitiremos que desde la pasarela se puedan enviar de cualquier tipo, excepto de “icmp-reply”. Y denegaremos “icmp” request desde la estación.

Práctica 5: Puesta en marcha de un cortafuegos con IPTables

```
# Se permite cualquier ICMP en la Red local, exceptuando "echo-request"
entrantes
iptables -A INPUT -s $REDLOCAL -p icmp -m icmp --icmp-type ! echo-request -j
ACCEPT
iptables -A OUTPUT -d $REDLOCAL -p icmp -m icmp --icmp-type ! echo-reply -j
ACCEPT
```

El resto de reglas necesarias son las siguientes:

FTP como cliente

```
# GENERALIDADES (CONEXIÓN A FTP)
iptables -A INPUT -p tcp -m tcp --sport 21 -m state --state ESTABLISHED \
-j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 21 -m state --state NEW,ESTABLISHED \
-j ACCEPT
iptables -A FORWARD -i $DEVINET -o $DEVLOCAL -p tcp -m tcp --sport 21 \
-m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $DEVLOCAL -o $DEVINET -p tcp -m tcp --dport 21 \
-m state --state NEW,ESTABLISHED -j ACCEPT

# FTP ACTIVO
iptables -A INPUT -p tcp -m tcp --sport 20 -m state -state \
RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 20 -m state --state ESTABLISHED \
-j ACCEPT
iptables -A FORWARD -i $DEVINET -o $DEVLOCAL -p tcp -m tcp --sport 20 \
-m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $DEVLOCAL -o $DEVINET -p tcp -m tcp --dport 20 \
-m state --state ESTABLISHED -j ACCEPT

# FTP PASIVO
iptables -A INPUT -p tcp -m tcp --sport 1024:65535 --dport 1024:65535 \
-m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 1024:65535 --dport 1024:65535 \
-m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i $DEVINET -o $DEVLOCAL -p tcp -m tcp \
--sport 1024:65535 --dport 1024:65535 \
-m state --state ESTABLISHED -j ACCEPT

iptables -A FORWARD -i $DEVLOCAL -o $DEVINET -p tcp -m tcp \
--sport 1024:65535 --dport 1024:65535 \
-m state --state ESTABLISHED,RELATED -j ACCEPT
```

POP3 como cliente a través de las interfaces Ethernet y en ambos sentidos sobre enlaces PPP

```
iptables -A INPUT -p tcp -i eth+ -m tcp --sport 110 -m \
state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -o eth+ -m tcp --dport 110 -m \
state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -i ppp+ -m tcp --sport 110 -m \
state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -o ppp+ -m tcp --dport 110 -m \
state --state NEW,ESTABLISHED -j ACCEPT
```

Práctica 5: Puesta en marcha de un cortafuegos con IPTables

SMTP como cliente a través de 172.16.1.1

```
iptables -A INPUT -s 172.16.1.1 -p tcp -m tcp --sport 25 \
-m state --state ESTABLISHED -j ACCEPT \
iptables -A OUTPUT -d 172.16.1.1 -p tcp -m tcp --dport 25 \
-m state --state NEW,ESTABLISHED -j ACCEPT \
iptables -A FORWARD -i $DEVINET -o $DEVLOCAL -s 172.16.1.1 \
-p tcp -m tcp --sport 25 \
-m state --state ESTABLISHED -j ACCEPT \
iptables -A FORWARD -i $DEVLOCAL -o $DEVINET -d 172.16.1.1 \
-p tcp -m tcp --dport 25 \
-m state --state NEW,ESTABLISHED -j ACCEPT
```

HTTP como cliente a través del Proxy 193.145.133.12

```
iptables -A INPUT -s 193.145.133.12 -p tcp -m tcp --sport 3128 \
-m state --state RELATED,ESTABLISHED -j ACCEPT \
iptables -A OUTPUT -d 193.145.133.12 -p tcp -m tcp --dport 3128 -j ACCEPT \
iptables -A FORWARD -s 193.145.133.12 -i $DEVINET -o $DEVLOCAL \
-p tcp -m tcp --sport 3128 \
-m state --state RELATED,ESTABLISHED -j ACCEPT \
iptables -A FORWARD -d 193.145.133.12 -i $DEVLOCAL -o $DEVINET \
-p tcp -m tcp --dport 3128 -j ACCEPT
```

Consultas a DNS en ambos sentidos, pero sólo con 172.16.1.1

```
iptables -A INPUT -s 172.16.1.1 -p udp -m udp --sport 53 -j ACCEPT \
iptables -A OUTPUT -d 172.16.1.1 -p udp -m udp --dport 53 -j ACCEPT \
iptables -A FORWARD -i $DEVINET -o $DEVLOCAL -p udp \
-m udp --sport 53 -j ACCEPT \
iptables -A FORWARD -i $DEVLOCAL -o $DEVINET -p udp \
-m udp --dport 53 -j ACCEPT
```

Telnet como cliente

```
iptables -A INPUT -p tcp -m tcp --sport 23 -m state \
--state ESTABLISHED -j ACCEPT \
iptables -A OUTPUT -p tcp -m tcp --dport 23 -j ACCEPT \
iptables -A FORWARD -i $DEVINET -o $DEVLOCAL -p tcp -m tcp \
--sport 23 -m state --state ESTABLISHED -j ACCEPT \
iptables -A FORWARD -i $DEVLOCAL -o $DEVINET -p tcp -m tcp \
--dport 23 -j ACCEPT
```

3. Referencias bibliográficas

- Manual de IPTables. Comando “man 8 iptables”
- IPTables. Manual práctico
URL=”<http://www.pello.info/filez/firewall/iptables.html>”
- Guía rápida iptables: cortafuegos Linux
URL=”<http://www.mononeurona.org/index.php?idp=276>”