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

iptables y NAT para vagos

Por **Ricardo Galli Granada**, ***gallir*** (http://mnm.uib.es/~gallir/)
Creado el 30/09/2002 13:57 y modificado por última vez el 14/01/2003 18:47

A pesar que en Bulma hay varios artículos[2] explicando estos temas, es una pregunta recurrente[3] en la lista Bulmailing. Además no se suelen usar las características, muy buenas, de control de conexiones del netfilter. Aquí doy un par de ejemplos concretos, especialmente preparados para los vagos que no se leen ningún tutorial :−)

En nuestros ejemplos vamos aprovechar las capacidades de control de conexiones que tienen las iptables. Primero, hay que tener en cuenta que el forwarding debe estar habilitado:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Y también recordar que para cambiar las reglas, primero hay que borrar las anteriores, por ejemplo:

```
iptables −F
iptables −t nat −F
```

Ahora veremos ejemplos particulares, en todos los ejemplos suponemos que las direcciones de nuestra red privada son 192.168.0.0/24 (es decir la máscara es de 24 bits: 255.255.255.0)

Sólo quiero hacer masquerading de una IP asignada dinámicamente

Caso común para un Linux que obtiene direcciones dinámicas de su proveedor de Internet, en el ejemplo lo doy con la interfaz ippp0, que es la que se usa para RDSI, pero podéis sustituirla por caulquier interfaz que uséis (eth0, ppp0...).

Además de hacer el NAT, vamos a permitir el tráfico ICMP (de los pings...) ya que está recomendado que así funcione. Veremos que las última 3 reglas, que no son obligatorias, peri os las recomiendo, lo que haces es descartar cualquier paquete que no sea de uina conexión previamente establecida.

```
# Habilito el NAT
iptables −t nat −A POSTROUTING −s 192.168.0.0/24 −d 0.0.0.0/0  \
     −j MASQUERADE
# Dejo pasar los paquetes ICMP
iptables −A INPUT −i ippp0 −p ICMP −j ACCEPT
# Acepto paquetes de conexiones ya establecidas
iptables −A INPUT −p TCP −m state −−state RELATED \
    −j ACCEPT
# Rechazamos paquetes de conexiones nuevas
iptables −A INPUT −i ippp0 −m state −−state NEW,INVALID −j DROP
# Rechazamos paquetes de forwarding de conexiones no establecidas
iptables −A FORWARD −i ippp0 −m state −−state NEW,INVALID −j DROP
```

Pero también quiero permitir conexiones entrantes SSH y HTTP

Eso es fácil, antes de las últimas reglas DROP hay que poner unas que permitan las conexiones nuevas a esos puertos. Las reglas nos quedan de la siguiente forma:

```
# Habilito el NAT
iptables −t nat −A POSTROUTING −s 192.168.0.0/24 −d 0.0.0.0/0  \
    −j MASQUERADE
# Dejo pasar los paquetes ICMP
iptables −A INPUT −i ippp0 −p ICMP −j ACCEPT
```

```
# Permito conexiones al puerto 80 (HTTP)
iptables -A INPUT -i ippp0 -p TCP --dport 80 -m state --state NEW  \
    -j ACCEPT
# Permito conexiones al puerto 22 (SSH)
iptables -A INPUT -i ippp0 -p TCP --dport 22 -m state --state NEW  \
    -j ACCEPT
# Acepto paquetes de conexiones ya establecidas
iptables -A INPUT -p TCP -m state --state RELATED  \
    -j ACCEPT
# Rechazamos paquetes de conexiones nuevas
iptables -A INPUT -i ippp0 -m state --state NEW,INVALID -j DROP
# Rechazamos paquetes de forwarding de conexiones no establecidas
iptables -A FORWARD -i ippp0 -m state --state NEW,INVALID -j DROP
```

Si queréis abrir otros puestos, sólo tenéis que agregar esas nuevas reglas.

Tengo dirección IP fija, ¿como lo hago?

Es muy fácil, en vez de usar *masquerading*, vamos a usar una solución mejor: *source NAT*. Sólo hay que cambiar la regla del nat (la primera en los ejemplos anteriores). Si la interfaz que tiene la IP fija es la eth0, y la IP fija es la 111.111.111.111, nos quedaría:

```
# Habilito el SNAT
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 111.111.111.111
# Dejo pasar los paquetes ICMP
iptables -A INPUT -i eth0 -p ICMP -j ACCEPT
# Permito conexiones al puerto 80 (HTTP)
iptables -A INPUT -i eth0 -p TCP --dport 80 -m state --state NEW  \
    -j ACCEPT
# Permito conexiones al puerto 22 (SSH)
iptables -A INPUT -i eth0 -p TCP --dport 22 -m state --state NEW  \
    -j ACCEPT
# Acepto paquetes de conexiones ya establecidas
iptables -A INPUT -p TCP -m state --state RELATED  \
    -j ACCEPT
# Rechazamos paquetes de conexiones nuevas
iptables -A INPUT -i eth0 -m state --state NEW,INVALID -j DROP
# Rechazamos paquetes de forwarding de conexiones no establecidas
iptables -A FORWARD -i eth0 -m state --state NEW,INVALID -j DROP
```

Vale, pero ahora quiero redireccionar las conexiones a un puerto hacia un ordenador interno de mi LAN

Esto se llama destination NAT es bastante sencillo, sólo hay que poner una regla adicional. Por ejemplo, si queremos redireccionar las conexiones al puerto 80 hacia el puerto 80 de un ordenador en la red interna (192.168.0.111).

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \
          --to 192.168.0.111:80
```

Otro ejemplo sencillo y muy útil, redireccionar el puerto 2022 del ordenador haciendo de NAT o firewall hacia el puerto 22 (ssh) de un ordenador de la red interna.

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2022 -j DNAT \
          --to 192.168.0.111:22
```

Voilà, funciona. También podéis leer los *Howtos* y tutoriales[1], que están hasta en castellano.

Lista de enlaces de este artículo:

1. http://www.netfilter.org/documentation/
2. http://bulmalug.net/htdig-bin/htsearch?config=htdigand>
3. http://bulmalug.net/htdig-bin/htsearch?config=htdigand>

E−mail del autor: gallir@uib.es
Podrás encontrar este artículo e información adicional en: http://bulmalug.net/body.phtml?nIdNoticia=1522