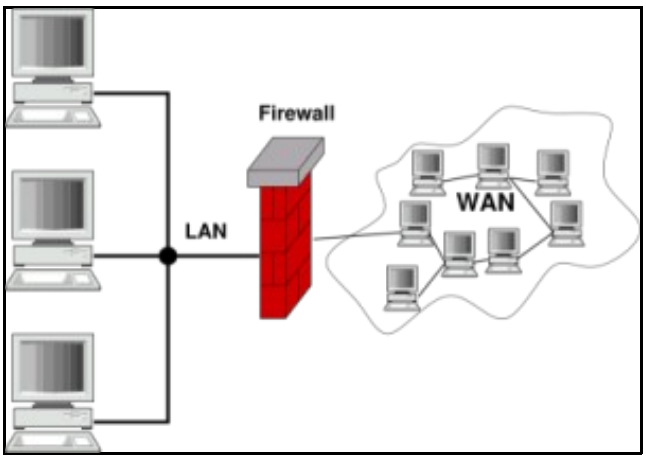
Devasa ou Cortalumes

Sumario

Definición

Un firewall, devasa ou cortalumes é un compoñente hardware ou software que permite **filtrar paquetes** TCP/IP en función dunhas políticas de seguridade (regras de filtrado). Polo tanto, un firewall é un elemento de seguridade que permite filtrar as comunicacións que se establecen a través de Internet determinando que servizos son accesibles e cales non, co obxecto de protexer a nosa rede (integridade e confidencialidade).



Un firewall permite tamén que dous equipos poidan establecer comunicación entre eles aínda que as súas direccións IP non sexan públicas. Isto consíguese mediante o que se coñece como **NAT** (*Network Address Translation*).

NAT

A tradución de direccións de rede ou NAT permite alterar a orixe e o destino dun paquete actuando sobre as cabeceiras, cando pasa por unha máquina que ten activado o módulo NAT de iptables. Ademais, mantense un rexistro de entrada/saída dos paquetes modificados. Polo tanto, NAT permite enmascarar unha rede enteira detrás dunha única IP pública.

Existen dous tipos de NAT:

- *Source NAT* (**SNAT**). Cambia a dirección orixe do paquete (petición de dentro a fóra):

1. Un equipo da Intranet con dirección IP privada xera un paquete destinado cara a Internet.
2. Como o destinatario é un equipo que está noutra rede o paquete envíase ao router/gateway para que decida por donde encamiñalo.
3. O router, en función das súas táboas, encamiña o paquete cara o destino pero antes de envialo altera o paquete enmascarando a dirección IP de orixe (SNAT) intercambiándoa pola súa dirección IP pública (SNAT POSTROUTING, posterior ao enrutamento altérase o paquete).
4. Por último, o equipo externo responde contestanto cun paquete dirixido á dirección IP pública, que é a do router. Este, ao recibilo, desenmascara o paquete e entrégallo ao equipo da Intranet.

- *Destination NAT* (**DNAT**). Cambia a dirección de destino do paquete (petición de fóra a dentro):

1. Un equipo externo á nosa rede realiza unha solicitude a un dos nosos servizos (dirección IP privada inaccesible), usando como dirección IP pública a do router que fai de intermediario.
2. O router recibe a solicitude e recoñece o servizo ao que se quere conectar polo porto de comunicación de destino.
3. Intercambia a dirección IP pública de destino (DNAT) pola dirección IP privada do equipo que ofrece o servizo solicitado. Unha vez alterado (PREROUTING) o paquete enrútase pola interface de rede que lle permite establecer a comunicación co servidor da Intranet (DNAT PREROUTING, previo ao enrutamento modifícase o paquete).
4. O servidor da Intranet emite unha resposta entregándolla novamente ao router para que a faga chegar ao equipo externo que iniciou a comunicación.

Filtrado de paquetes

Para poder desenvolver esta función o firewall inspecciona a cabeceira dos paquetes TCP/IP que pode recibir polas distintas interfaces de rede que teña (eth0, eth1, eth2, etc.) e decidir que facer con eles. En concreto, examina a dirección IP e os portos de orixe e destino de cada paquete.

O filtrado depende das regras que se utilicen, as cales permiten cerrar o tráfico de paquetes cara a determinados portos e só deixar abertos os que necesitan os servizos que se están executando. Por exemplo, se se quere que ninguén se baixe nada da intranet utilizando FTP debe pecharse o porto 20 (FTP Data). Unha regra pode desencadear varias **accións**:

- **Accept**. Permite pasar o paquete.
- **Drop**. Permite ignorar o paquete.
- **Reject**. Permite denegar o paquete. A diferenza con Drop é que devolve ao emisor do paquete unha mensaxe ICMP indicando o motivo de rexeite do mesmo.

O iptables

GNU/Linux pode funcionar como firewall a través do software iptables.

A sintaxe de iptables é a seguinte:

```
iptables [-t <nome_táboa>] <opcións> <cadea> <parámetro 1>/<opción 1> <parámetro n>/<opción n>
```

Táboas

Para o seu funcionamento utiliza as seguintes **táboas**:

- **Táboa filter**. Permite efectuar o filtrado de paquetes. **É a táboa por defecto**.
- **Táboa nat**. Permite que máquinas con direccións IP privadas poidan formar parte da rede como se fosen IP públicas.
- **Táboa mangle** (manipulación). Permite alterar os paquetes (non se verá nesta unidade).

Por exemplo, o seguinte comando amosa todas as regras da táboa filter:

```
iptables -t filter -L
```

Regras de filtrado ou cadeas

O iptables dispón de tres tipos de **regras de filtrado**, ás que tamén se lles chama **listas** ou **cadeas** (*chains*) e son as seguintes:

- **INPUT** (entrada). As súas regras aplícanse cando un paquete que entra por unha interface do firewall ten como **dirección IP de destino** o propio firewall.
- **OUTPUT** (saída). As súas regras aplícanse cando un paquete que sae por unha interface do firewall ten como **dirección IP de orixe** o propio firewall.
- **FORWARD** (reenvío). As súas regras aplícanse cando un paquete que chega ao firewall por unha interface non ten como **dirección IP de destino** o propio firewall, é dicir, é un paquete que non vai dirixido a el.

É moi importante destacar que as regras de filtrado se len de xeito secuencial ata que se atopa unha regra que afecta ao paquete que se analiza nese intre. Polo tanto, **a orde na que se escriban estas regras é determinante para o correcto funcionamento do firewall**.

Opcións ou comandos

As **opcións** dispoñibles son moitas e poden consultarse tecleando:

```
iptables -h
```

Algunhas das máis importantes son as seguintes:

- **-P**. Política, determina cal é a política por defecto para unha lista/cadea concreta. O seguinte exemplo establece como política por defecto rexeitar calquera paquete de entrada (observa que non se usa o parámetro -j para especificar a acción):

```
iptables -P INPUT DROP
```

- **-F**. *Flush* ou valeirar, elimina as regras dunha lista/cadea. Por exemplo:

```
iptables -F OUTPUT
```

- **-A**. *Add* ou engadir, dada unha lista/cadea engade unha nova regra ao final de dita cadea. O seguinte exemplo, permite as conexións locais (lo:interace loopback):

```
#Esta regra é útil para facer probas con servidores Web locais, BBDD locais, etc.
iptables -A INPUT -i lo -j ACCEPT
```

- **-D**. *Delete* ou borrar, elimina unha regra dunha lista. No seguinte exemplo, da lista INPUT elimínase a regra que denega o acceso ao porto 80.

```
iptables -D INPUT --dport 80 -j DROP
```

- **-L**. Lista para unha táboa as regras introducidas no firewall. Ten dúas subopcións interesantes que son **-v**, que permite amosar información detallada e **-n**, que evita resolver os nomes de dominio (polo que a saída é máis rápida). O seguinte exemplo amosaría as regras da lista INPUT para a táboa filter, de xeito detallado:

```
iptables -t filter -vnL INPUT
```

- **-Z**. *Zero*, pon a cero o contador do número de regras que posúe unha lista. É útil usalo tras ter borrado todas as regras dunha táboa ou lista:

```
iptables -t filter -Z OUTPUT
```

Parámetros

O iptables ten moitos parámetros. Algúns dos máis usados son os seguintes:

- **-j**. Indica que acción se debe executar: ACCEPT, DROP, REJECT.
- **-s**. *Source* ou orixe, indica a IP da máquina orixe dun paquete. Para unha rede debe indicarse a máscara en formato CIDR. O seguinte exemplo admite paquetes que veñan da rede 192.168.100.0/24 (por defecto, úsase sempre a táboa filter, así que non hai que especificala):

```
iptables -A INPUT -s 192.168.100.0/24 -j ACCEPT
```

- **-d**. *Destination* ou destino, indica a IP da máquina destino. Para unha rede debe indicarse a máscara en formato CIDR.
- **-i**. Indica a interface de entrada sobre a que se avalía a regra.
- **-o**. Indica a interface de saída sobre a que se avalía a regra.
- **-p**. Protocolo, indica o protocolo (icmp, tcp ou udp) que se quere usar para o filtrado. Pódense usar as opcións --sport (source port, ou porto de orixe) e --dport (destination port, ou porto de destino). Os seguintes son exemplos do seu uso:

```
# Abre o porto tcp 80 para todo o mundo.
iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT

# Se temos un servidor Web instalado na nosa rede abre o porto 80 para que estea accesible
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

# Queremos pechar todos os portos por debaixo do 1024
iptables -t filter -A INPUT -p tcp --dport 1:1024 -j DROP
```

- **-m state**. Permite ter en conta o estado das conexións para, así, determinar se o tráfico de entrada ou saída pertence a unha conexión establecida (`ESTABLISHED`) ou está relacionado cunha conexión establecida (`RELATED`). O seguinte exemplo permite o tráfico polos portos de orixe e destino dunha conexión establecida:

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Configuracións típicas cun firewall

SNAT

Nesta configuración úsase SNAT para permitir todo o tráfico TCP e UDP desde a rede interna cada Internet. O resto do tráfico está pechado. As regras básicas a aplicar son as seguintes:

```
#Activamos o reenvío
echo 1 > /proc/sys/net/ipv4/ip_forward

#Reiniciamos contadores e táboas
iptables -F
iptables -t nat -F
iptables -Z
iptables -t nat -Z

#Activamos NAT
iptables -t nat -A POSTROUTING -j MASQUERADE

#Permitimos todo  o tráfico TCP e UDP desde a rede interna cada Internet
iptables -A FORWARD -s 10.0.0.0/8 -i eth1 -j ACCEPT

#Permitimos o tráfico entrante para as conexións previamente establecidas
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#Rexeitamos todo o resto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Graficamente pódese ver na seguinte figura: Archivo:IMSI UD8 2.jpg

DNAT

Nesta situación hai que facer DNAT, xa que se accede dende Internet a servizos da intranet (servizo Web neste exemplo e o servidor con IP privada 10.0.0.50):

```
#Activamos o reenvío
echo 1 > /proc/sys/net/ipv4/ip_forward

#Reiniciamos contadores e táboas
iptables -F
iptables -t nat -F
iptables -Z
iptables -t nat -Z

#Activamos NAT
iptables -t nat -A POSTROUTING -j MASQUERADE

#Activamos DNAT para o porto 80 e dirección IP a do servidor
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.0.0.50:80

#Permitimos o tráfico de todos os paquetes dirixidos ao porto 80
iptables -A FORWARD -i eth0 -p tcp --dport 80 -j ACCEPT

#Permitimos o tráfico TCP e UDP desde a rede internat cara Internet
iptables -A FORWARD -s 10.0.0.0/8 -i eth1 -j ACCEPT

#Permitimos o tráfico para as conexións establecidas
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#Rexeitamos todo o resto
```

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Graficamente pódese ver na seguinte figura: Archivo:IMSI UD8 3.jpg

Zona desprotexida ou DMZ

Esta configuración é típica en moitas organizacións coa finalidade de enmascarar os servizos ofrecidos por diferentes equipos servidores internos (DMZ ou zona DesMilitariZada), a través dunha única dirección IP pública, a do router/firewall, protexendo ao mesmo tempo a intranet contra calquera acceso externo non desexado.

As regras para esta configuración cun sevidor Web na DMZ son iguais que no caso anterior, só que o router/firewall ten tres interfaces de rede:

```
#Activamos o reenvío
echo 1 > /proc/sys/net/ipv4/ip_forward

#Reiniciamos contadores e táboas
iptables -F
iptables -t nat -F
iptables -Z
iptables -t nat -Z

#Activamos NAT
iptables -t nat -A POSTROUTING -j MASQUERADE

#Activamos DNAT para o porto 80 e dirección IP a do servidor
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.100.10:80

#Permitimos o tráfico de todos os paquetes dirixidos ao porto 80
iptables -A FORWARD -i eth0 -p tcp --dport 80 -j ACCEPT

#Permitimos o tráfico TCP e UDP desde a rede internet cara afora (incluída a DMZ)
iptables -A FORWARD -s 192.168.200.0/24 -i eth1 -j ACCEPT

#Permitimos o tráfico para as conexións establecidas
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#Rexeitamos todo o resto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Graficamente pódese ver na seguinte figura: Archivo:IMSI UD8 4.jpg

Contornos gráficos

Existen distintos contornos gráficos para configurar o iptables como o shorewall ou o firestarter. En xeral, este tipo de programas non proporcionan toda a potencialidade da liña de comandos pero, pola contra, son máis doados de usar.

--Arribi 11:49 3 feb 2009 (GMT)