Contenido

[IPTABLES 1](#_Toc497145238)

[Introducción: 1](#_Toc497145239)

# 4. IPTABLES

# 4.1 Introducción:

Disponemos de 5 opciones (chains) generales donde poder crear nuestras reglas

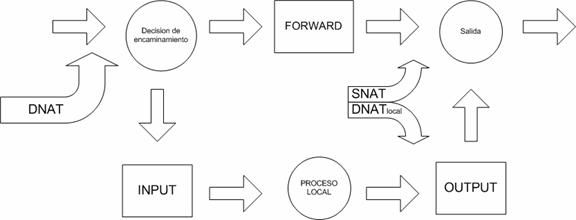
* Nat
* Filter
* Mangle
* Raw
* Security

Un firewall sirve para bloquear o permitir algunas comunicaciones en función de algunos parámetros.

Lo normal es que el firewall este centralizado y en un equipo (aunque podrían ser mas de uno).

Siempre se cortan las comunicaciones lo antes posible.

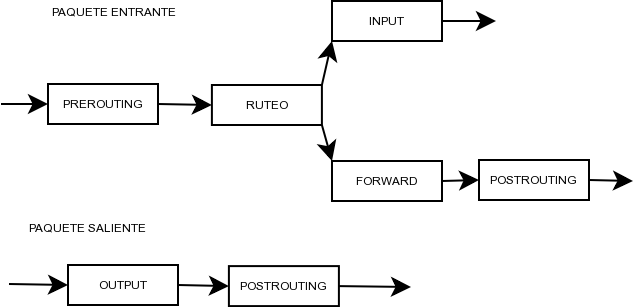
Cuando un pauqete entra o sale del equipo, va pasando por distintas zonas, y es en estas tablas donde vamos a poner nuestras condiciones.



# 4.2 Comando iptables. Nociones básicas:

* -t permite indicar que opción (filter,nat…) nos estamos refiriendo. Por defecto toma el valor de filter.
* -L muestra el contenido de las tablas de la opción elegida ( iptables –t nat –L ) -> muestra las tablas nat

### 4.2.1 Tablas NAT



Lo que hace un nat es un cambio de ip en el paquete.

Podemos hacer un nat que cambie la ip de origen o que cambie la ip de destino

* Si cambiamos el origen SNAT (source nat) (cambiaremos la ip a la salida, es decir, en postrouting)
* Si cambiamos el destino DNAT (destiny nat)(cambiamos la ip a la entrada, antes de enrutar, es decir, en prerouting)

Ejemplo: el router de casa hace snat en los pquetes que salen (cambia nuestra dirección local a nuestra dirección publica)

Ejemplo: el router de casa hace dnat en los pquetes que entran (por ejemplo si tenemos un servidor web)

Toda tabla tiene asociada una politia por defecto, que por defecto es aceptar

-A añade una regla a la tabla indicada

-I insertar una regla en una posición determinada en una tabla

El orden en la tabla importa ya que un paquete hara lo que le diga la primera regla que le afecte, y obviara el resto, si ninguna regla le afecta hara lo que defina la política por defecto.

-D borra una regla

-F borra todas las reglas de una tabla

Regla global para dar acceso al exterior a todas las redes internas

Iptables –t nat –A POSTROUTING –j MASQUERADE -> lo que hace es un snat con mi ip externa para todas las comunicaciones internas que tengan que salir al exterior.

Parametros

-j -> indica la operación a realizar podemos hacer un dnat, un snat o un masquerade

-j -> con snat y dnat tenemos “- - to” para darle una ip que asigna al cambiar

-i -> indicamos la interface de entrada (tarjeta) (hay tablas que admiten el –i y otras el –o)

-o -> indicamos interface de salida (tarjeta) (hay tablas que admiten el –i y otras el –o)

-s -> indica lo que viene de una red (ip)

-d -> indica la dirección (red) de destino (ip)

-p -> indicar el protocolo ip (tcp,udp,icmp)

-P -> cambia política por defecto (ej. Iptables –t filter –P INPUT DROP)

--sport -> indicar el puerto origen de la comunicacion

--dport -> indicar el puerto origen de la comunicación

Ejercicio. Proporcionar internet únicamente a la red del cliente1

~~Iptables –t nat –A POSTROUTING –i ens37 –j MASQUERADE~~

Esta no funciona porque como es postrouting, ya ha hecho el enrutamiento asi que ya no sabe por donde entro.

Iptables –t nat –A POSTROUTING –s 192.168.1.0 –j MASQUERADE

Iptables –t nat –A POSTROUTING –s 192.168.1.0 –o ens33 –j SNAT –to 192.168.40.125

Ejercicio:

Cuando me conecte por ssh desde la real al servidor debe mandarme automaicamente al cliente2

Iptables –t nat –A PREROUTING –s 192.168.40.1 –p TCP –dport 22 –j DNAT –to 192.168.2.1

iptables-save muestra las iptables por pantalla

### 4.2.2 tabla filter

Tenemos 3 tablas de filtrado

* Input
* Forward
* Output

#### Input

Por la tabla input pasa todo lo que entra al firewall con destino él mismo.

#### Forward

Todo lo que es enrutado por el firewall

Opción –j -> tres opciones

* ACCEPT -> acepta el paquete
* DROP -> deniega el paquete -> no informa a nadie (corta el paquete y se acabó)
* REJECT -> deniega el paquete -> avisa al origen de que el paquete ha sido denegado. (con el protocolo icmp)

#### Output

Todo lo que es generado en el firewall (servidor) y sale hacia otro destino

Ejemplo:

Permitir el acceso al servidor únicamente via ftp o ssh

Iptables –t filter –A INPUT –p TCP –dport 20:22 –j ACCEPT

Iptables –t filter –P INPUT DROP

Permitir conectarse desde el servidor únicamente a las webs internas

Iptables –t filter –A OUTPUT –o ens37 –p TCP –m multiport –dport 80,443 –j ACCEPT

Iptables –t filter –A OUTPUT –o ens38 –p TCP –m multiport –dport 80,443 –j ACCEPT

Iptables –t filter –A OUTPUT –p TCP –m multiport –dport 80,442 -j DROP

Manteniendo los ejercicios anteriores:

Desde la red del equipo real acceda a la web del cliente 1 poniendo la ip del servidor

Iptables –t NAT –A PREROUTING –p tcp –dport 80 –j SNAT –TO 192.168.1.1

Permitir al servidor navegar únicamente a la red de iescomercio y a las webs internas

Iptables –t filter –A INPUT –d 192.168.1.0/24 –p tcp –m multiport –dport 80,443 –j ACCEPT

Iptables –t filter –A INPUT –d 192.168.2.0/24 –p tcp –m multiport –dport 80,443 –j ACCEPT

Iptables –t filter –A INPUT –d www.iescomercio.com –p tcp –m multiport –dport 80,443 –j ACCEPT

Iptables –A ouput –p tcp –m multiport –dport 80,443 –j drop

Evitar que el servidor responda a los pings pero no que el pueda hacer ping

Iptables –t filter –A input –p icmp –j DROP

Con esta solución el servidor al hacer ping a un host, cuando le vuelven las respuestas no puede recibirlas porque las hemos cortado.

¿Cómo cortar un tipo especifico de paquetes icmp?

Iptables –p icmp –help

El ejercicio anterior la respuesta es:

iptables -A INPUT -p icmp --icmp-type ping -j DROP

Crear archivos de inicio en debían

Los archivos de inicio están en /etc/init.d/

1. Creamos un fichero con el nombre que queramos
2. Tienen una cabecera que es obligatorio

#!/bin/sh

### BEGIN INIT INFO

# Provides: dbus

# Required-Start: $remote\_fs $syslog

# Required-Stop: $remote\_fs $syslog

# Default-Start: 2 3 4 5

# Default-Stop:

# Short-Description: D-Bus systemwide message bus

### END INIT INFO

Required-Start define los servicios que tienen que arrancar antes de este

Required-Stop define los servicios que tienen que ser parados antes de este

Default-Start: define los modos en los que va a cargar este script

1. Metemos los comandos de ese fichero
2. Guardamos y asignamos permisos de ejecución
3. Ejecutar comando inserv fichero para que cree los enlaces simbólicos necesarios en los modos de arranque indicados o update-rc

#limpiamos el firewall

iptables -t nat -F

iptables -F

#ponemos las politicas por defecto a DROP

iptables -P INPUT DROP

iptables -P FORWARD DROP

#hablitamos internet a la red 2.0/24

iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -j SNAT --to 192.168.40.145

# habilitamos que el servidor pueda recibir las respuestas de los pings que hace

iptables -A INPUT -p icmp --icmp-type pong -j ACCEPT

iptables -A INPUT -s 192.168.1.0/24 -p icmp --icmp-type ping -j ACCEPT

iptables -A INPUT -p icmp --icmp-type ping -j DROP

iptables -A INPUT -s 192.168.2.0/24 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -j DROP

iptables -A INPUT -p tcp --dport 1:1024 -j ACCEPT

iptables -A INPUT -p udp --dport 1:1024 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -s 192.168.2.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -s 192.168.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -s 192.168.40.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.40.0/24 -s 192.168.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -s 192.168.40.0/24 -p tcp --dport 20:21 -j ACCEPT

iptables -A FORWARD -d 192.168.40.0/24 -s 192.168.1.0/24 -p tcp --sport 20:21 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -s 192.168.2.0/24 -p tcp --dport 20:21 -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -s 192.168.1.0/24 -p tcp --sport 20:21 -j ACCEPT

iptables -A FORWARD -d 0.0.0.0/0 -s 192.168.2.0/24 -p all -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -s 0.0.0.0/0 -p all -j ACCEPT

iptables -A FORWARD -d 192.168.1.1/32 -s 192.168.2.0/24 -p tcp --dport 22 -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -s 192.168.1.1/32 -p tcp --sport 22 -j ACCEPT

# EJERCICIO SISTEMA EMULADO SPAINSKILLS

echo "Iniciando firewall"

echo 1 >/proc/sys/net/ipv4/ip\_forward

iptables -F

iptables -t nat -F

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to 192.168.40.158

iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to 192.168.40.158

iptables -t nat -A PREROUTING -s 192.168.40.0/24 -p tcp -m multiport --dport 80,443 -j DNAT --to 172.16.1.2

iptables -t nat -A PREROUTING -s 192.168.40.0/24 -p tcp --dport 2222 -j DNAT --to 192.168.1.100:22

iptables -P FORWARD DROP

iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT

iptables -A OUTPUT -s 172.16.1.0/24 -j ACCEPT

iptables -A INPUT -s 192.16.40.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A INPUT -s 172.16.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT

iptables -A INPUT -s 192.168.40.44/32 -d 192.168.1.0/24 -p icmp -j DROP

iptables -A INPUT -s 192.168.40.0/24 -d 192.168.1.0/24 -p icmp -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 53 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -p tcp --sport 53 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p udp --dport 53 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -p udp --sport 53 -j ACCEPT

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -A INPUT -d 192.168.1.0/24 -p icmp -j DROP

iptables -A INPUT -d 172.16.1.0/24 -p icmp -j DROP

iptables -A INPUT -d 192.168.1.1/32 -s 192.168.1.0/24 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -d 192.168.1.1/32 -p tcp --dport 22 -j DROP

iptables -A INPUT -s 192.168.1.0/24 -d 192.168.1.1/32 -p tcp -m multiport --sport 20,21,80,443 -j DROP

iptables -A FORWARD -j LOG --log-prefix "firewall forward"

corrección

echo "Iniciando firewall"

echo 1 >/proc/sys/net/ipv4/ip\_forward

iptables -F

iptables -t nat -F

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to 192.168.40.158

iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to 192.168.40.158

iptables -t nat -A PREROUTING -s 192.168.40.0/24 -p tcp -m multiport --dport 80,443 -j DNAT --to 172.16.1.2

iptables -t nat -A PREROUTING -s 192.168.40.0/24 -p tcp --dport 2222 -j DNAT --to 192.168.1.100:22

iptables -P FORWARD DROP

iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT

iptables -A OUTPUT -s 172.16.1.0/24 -j ACCEPT

iptables -A INPUT -s 192.16.40.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A INPUT -s 172.16.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT

iptables -A INPUT -s 192.168.40.44/32 -d 192.168.1.0/24 -p icmp -j DROP

iptables -A INPUT -s 192.168.40.0/24 -d 192.168.1.0/24 -p icmp -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 53 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -p tcp --sport 53 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p udp --dport 53 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -p udp --sport 53 -j ACCEPT

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -A INPUT -d 192.168.1.0/24 -p icmp -j DROP

iptables -A INPUT -d 172.16.1.0/24 -p icmp -j DROP

iptables -A INPUT -d 192.168.1.1/32 -s 192.168.1.0/24 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -d 192.168.1.1/32 -p tcp --dport 22 -j DROP

iptables -A INPUT -s 192.168.1.0/24 -d 192.168.1.1/32 -p tcp -m multiport --sport 20,21,80,443 -j DROP

iptables -A FORWARD -j LOG --log-prefix "firewall forward"

# 4.3 Crear archivos de inicio en debían

# 4.4 logs y estados de conexión

ESTO NO ENTRA PARA EL EXAMEN

## 4.4.1 Estados de conexión

Hay cuatro tipos de estados de conexión:

* New -> cuando es una conexión nueva (pauqetes que van a crear una nueva conexión)
* Established -> paquetes que recibimos tras una conexión nueva por dichos puertos
* Related -> paquetes que van por otro puerto del que se uso para una conexión new (ejemplo ftp)
* Invalid: 🡪 cualquier paquete que no hemos establecido

Ejemplo

Iptables –A FORWARD –s 10.1.4.0/24 –p tcp –m state - -state NEW -m multiport –dport 80,443 –j ACCEPT

Iptables –A FORWARD –d 10.1.4.0/24 –p tcp –m state –state ESTABLISHED,RELATED [-m multiport –sport 80,443] –j ACCEPT

## 4.4.2 logs

-j LOG

Ejemplo. Evitar entrada de ping en el servidor 10.1.2.20 pero logueando los paquetes rechazados

Iptables –A FORWARD –s 10.1.2.20/32 –j LOG –log-prefix “textoquequeramos”

Iptables –A FORWARD –s 10.1.2.20/32 –p ICMP –ICMP-TYPE PING –j DROP

Limitar el numero de paquetes que loguea por tiempo

-m limit --limit paquetes/tiempo

Numero de paqutes máximo que admite en el log

-m limit –limit-burst

APACHE

Rsa: openssl req –nodes –x509 –newkey rsa:1024 –days 365 –keyout clave.pem –out cert.pem

El –nodes hace que no nos pida contraseña al usar el certificado

Ejercicio iptables y apache

ables -t nat -A POSTROUTING -s 192.168.2.0/24 -j MASQUERADE

iptables -A FORWARD -s 192.168.2.0/24 -j LOG --log-prefix “CLIENTE2salida”

iptables -A FORWARD -d 192.168.2.0/24 -j LOG --log-prefix “CLIENTE2entrada”

iptables -A FORWARD -s 192.168.2.0/24 -d 80.58.0.33/32 -m state --state NEW -p udp --dport 53 -j ACCEPT

iptables -A FORWARD -s 80.58.0.33/32 -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT

iptables -A FORWARD -s 192.168.2.0/24 -d 192.232.216.164/32 -m state --state NEW,ESTABLISHED -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -s 192.232.216.164/32 -p tcp -m multiport --sport 80,443 -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -s 192.168.2.0/24 -d www.educarioja.org -m state --state NEW,ESTABLISHED -p tcp -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -m state --state ESTABLISHED -j ACCEPT

iptables -A FORWARD -s 192.168.2.0/24 -d 193.146.250.35 -m state --state NEW,ESTABLISHED -p tcp --dport 20:21 -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -m state --state RELATED -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -s 192.168.1.0/24 -m state --state NEW,ESTABLISHED -p tcp --dport 137:139 -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -s 192.168.1.0/24 -m state --state NEW,ESTABLISHED -p tcp --dport 445 -j ACCEPT

iptables -A FORWARD -d 192.168.1.0/24 -m state --state ESTABLISHED -j ACCEPT

iptables -A FORWARD -d 192.168.2.0/24 -j DROP