

Índice

Introducción

Funcionamiento

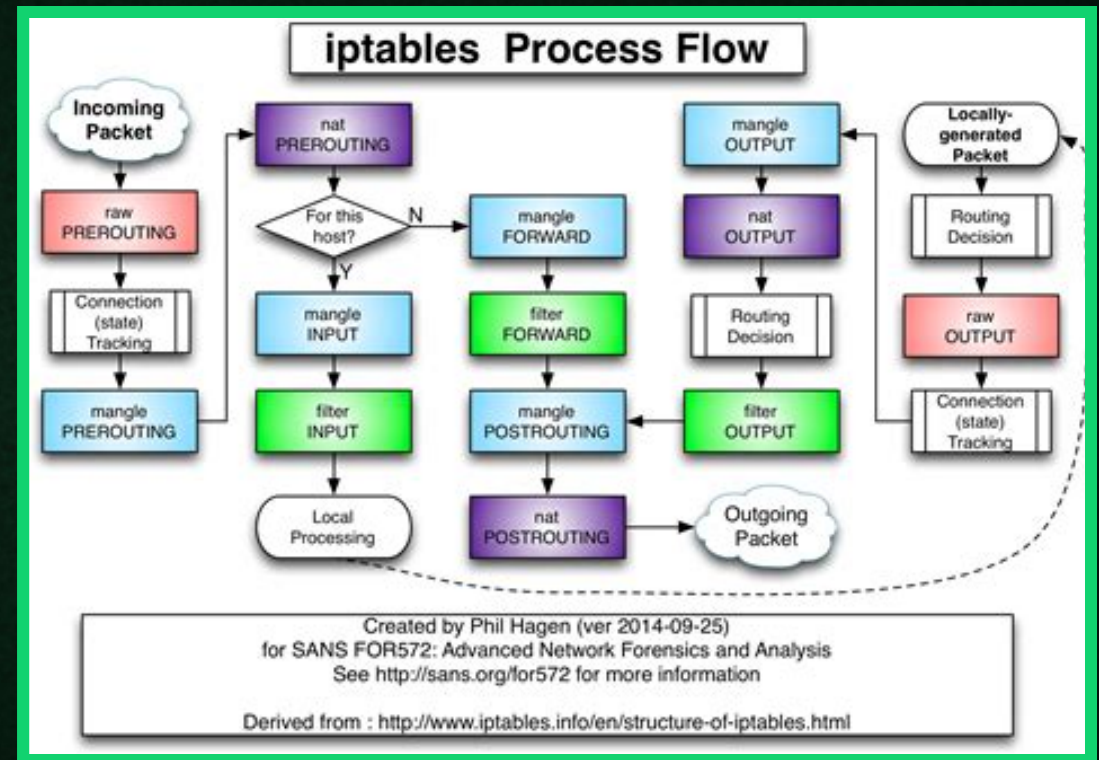
Reglas

Políticas por Defecto

Práctica

Preguntas

Gracias por atender

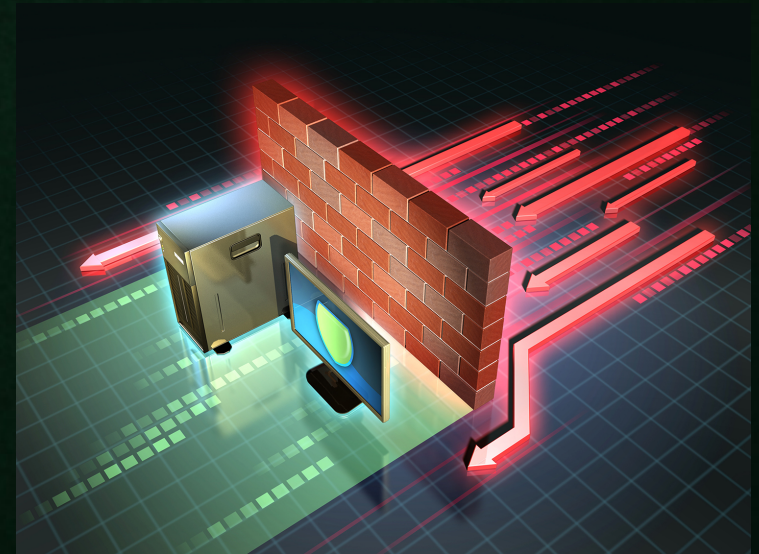


Introducción

¿Qué es?

Iptables es un sistema de filtrado de paquetes.

Esto permite llevar un control de los paquetes que entran o salen de nuestro dispositivo.



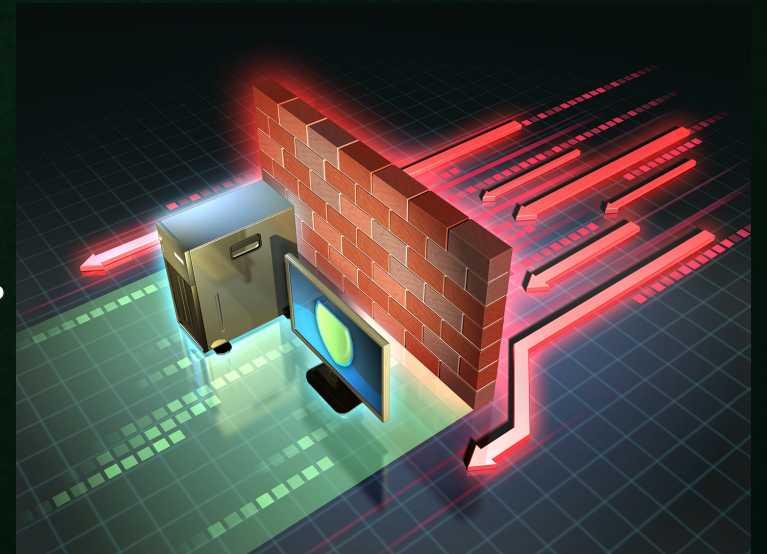
Funcionamiento

¿Cómo funciona?

El administrador define unas tablas, las cuales contienen cadenas de reglas.

Los paquetes pasarán por al menos una cadena de filtrado antes de aceptarse o rechazarse.

Si no hay una regla específica, Tomará la política por defecto.



Reglas

(En este caso para activar HTTP)

```
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT  
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Políticas por defecto

(En este caso para rechazar todo lo que no sea aceptado)

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```


Práctica

Para activarlo:

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

Práctica

Script

```
#!/bin/bash

# Eliminamos las reglas preexistentes.
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD

# Ponemos las políticas por defecto.
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```




"Cut here to activate firewall"

Práctica

Script que permite sólo SSH.

```
# Eliminamos las reglas preexistentes.
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD

# Ponemos las políticas por defecto.
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# SSH
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Práctica

Comprobación.

```
root@iptables:~# iptables -L -v
Chain INPUT (policy DROP 269 packets, 20875 bytes)
  pkts bytes target     prot opt in     out     source            destination
    826 61733 ACCEPT     tcp  --  any    any     anywhere          anywhere          tcp dpt:ssh
      0      0 ACCEPT     all  --  any    any     anywhere          anywhere          state RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy DROP 84 packets, 27552 bytes)
  pkts bytes target     prot opt in     out     source            destination
      0      0 ACCEPT     tcp  --  any    any     anywhere          anywhere          tcp dpt:ssh
    636 97784 ACCEPT     all  --  any    any     anywhere          anywhere          state RELATED,ESTABLISHED
root@iptables:~# iptables -L -v
```


Práctica

Prueba de Ping

```
[Alex@Aspire ~]$ ping 10.116.65.156
PING 10.116.65.156 (10.116.65.156) 56(84) bytes of data.
^C
--- 10.116.65.156 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14176ms
```

Práctica

Prueba de DNS con Dig

```
root@iptables:~# dig www.google.com
;; communications error to 10.239.3.7#53: timed out
;; communications error to 10.239.3.7#53: timed out
;; communications error to 10.239.3.7#53: timed out
;; communications error to 10.239.3.8#53: timed out

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.google.com
;; global options: +cmd
;; no servers could be reached
```

Práctica

Script: Aceptamos conexiones DNS

```
# Variables
```

```
SERVDNS1="10.239.3.7"
```

```
SERVDNS2="10.239.3.8"
```

```
IF1="enp0s3"
```

```
# DNS 1
```

```
iptables -A OUTPUT -p udp -o $IF1 -d $SERVDNS1 --sport 1024:65535 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p udp -i $IF1 -s $SERVDNS1 --dport 1024:65535 --sport 53 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -o $IF1 -d $SERVDNS1 --sport 1024:65535 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p tcp -i $IF1 -s $SERVDNS1 --dport 1024:65535 --sport 53 -m state --state ESTABLISHED -j ACCEPT
```

```
# DNS 2
```

```
iptables -A OUTPUT -p udp -o $IF1 -d $SERVDNS2 --sport 1024:65535 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p udp -i $IF1 -s $SERVDNS2 --dport 1024:65535 --sport 53 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -o $IF1 -d $SERVDNS2 --sport 1024:65535 --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p tcp -i $IF1 -s $SERVDNS2 --dport 1024:65535 --sport 53 -m state --state ESTABLISHED -j ACCEPT
```

```
~
```

```
..
```


Práctica

Prueba de DNS con Dig

```
root@iptables:~# dig www.google.com
```

```
; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.google.com
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57356
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 1232
```

```
; COOKIE: 51e0134abd8178e80100000067aaafc16ca49f34d6ce1c661 (good)
```

```
;; QUESTION SECTION:
```

```
www.google.com.                IN      A
```

```
;; ANSWER SECTION:
```

```
www.google.com.                5       IN      CNAME   forcesafesearch.google.com.
```

```
forcesafesearch.google.com. 2073    IN      A        216.239.38.120
```

```
;; ADDITIONAL SECTION:
```

```
rpz.local.                    1       IN      SOA      localhost. root.localhost. 1739255403 86400 7200 3600000 86400
```

```
;; Query time: 8 msec
```

```
;; SERVER: 10.239.3.7#53(10.239.3.7) (UDP)
```

```
;; WHEN: Tue Feb 11 03:30:20 EST 2025
```

```
;; MSG SIZE rcvd: 176
```

Práctica

Prueba de conexión Web (puertos 80 y 443)

```
root@iptables:~# lynx 10.116.65.136
```

```
Making HTTP connection to 10.116.65.136
```

(No puede conectar, ya que por defecto lo rechaza)

Práctica

Script: Añadimos regla de aceptación de Web

```
# Web (TCP 80 y 443)
iptables -R INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
```


Práctica

Tenemos acceso a servicios web

```
root@iptables:~# lynx 10.116.65.136
```

Bienvenido

Commands: Use arrow keys to move, '?' for help, 'q'
, '<-' to go back, and Down to move. Right to follow
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=sea

Práctica

Script: Añadimos Log para peticiones web

```
#LOG para Web
iptables -A INPUT -p tcp --dport 80 -j LOG --log-prefix "Apertura de Conexión Web: "

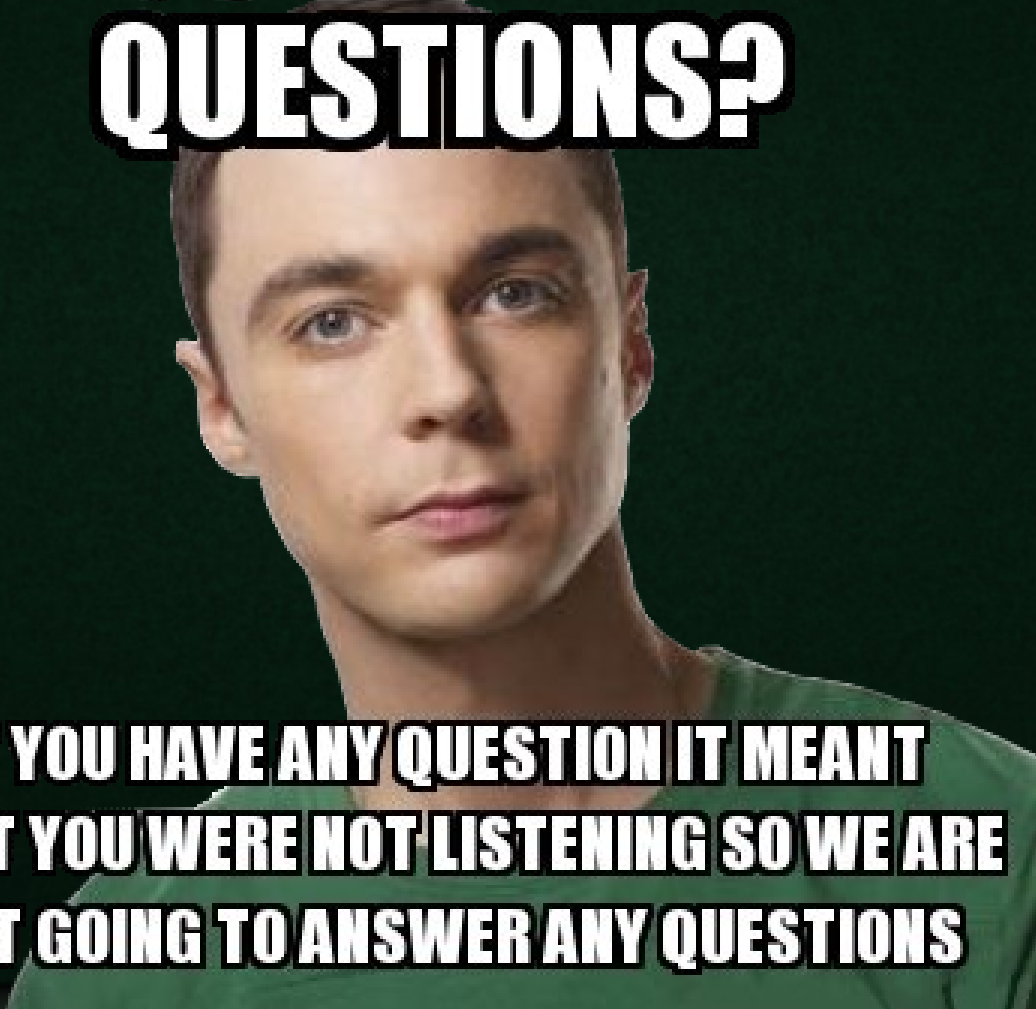
# Aceptar Conexiones Web
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Nos crea el log

```
root@iptables:~# journalctl lgrep "Web"
Feb 14 05:21:29 iptables kernel: Apertura de Conexión Web: IN=enp0s8 OU
T= MAC=08:00:27:1e:3b:97:40:c2:ba:f9:d1:52:08:00 SRC=10.116.65.158 DST=
10.116.65.156 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=54485 DF PROTO=TCP SP
T=44866 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
```

¿Alguna pregunta?

**YOU HAVE ANY
QUESTIONS?**

A portrait of Sheldon Cooper from the TV show 'The Big Bang Theory'. He is looking directly at the camera with a serious expression. He has short brown hair and is wearing a green t-shirt.

**IF YOU HAVE ANY QUESTION IT MEANT
THAT YOU WERE NOT LISTENING SO WE ARE
NOT GOING TO ANSWER ANY QUESTIONS**

Gracias por Atender



Espero que os
haya gustado

Creado por: Alejandro Hurtado Fernández