

Actividad 11

CORTAFUEGOS EN LINUX

ORQUÍDEA SEIJAS

CONTENIDO

1.	Introducción: Configuración previa	2
2.	Ejercicio 1	2
a.	Configuración por defecto y restricciones a implementar	2
b.	Primer script implementado: iptables-drop-1	3
i.	Conexión telnet desde interno a externo	3
ii.	Conexión web desde externo al firewall.....	4
iii.	Conexión web desde interno a externo.....	4
iv.	Escaneo de puertos nmap desde el firewall hacia interno y externo.....	4
3.	Ejercicio 2	4
a.	iptables-drop-2.....	5
i.	Filtro para limitar ICMP	5
ii.	Filtro de entrada a la red interna	5
iii.	Filtro de salida para la red interna	5
iv.	Filtro de conexiones hacia el firewall.....	5
b.	Verificación del script.....	5
i.	Configuración actual	5
ii.	Escaneo de puertos desde interno y externo hacia el firewall	6
iii.	Conexión TELNET desde interno a externo.....	7
iv.	Conexión web desde interno a externo y desde externo al firewall	7
v.	Verificación del registro de accesos en el firewall.....	7
4.	Conclusiones finales.....	7

1. INTRODUCCIÓN: CONFIGURACIÓN PREVIA

En esta sesión se realizaron una serie de ejercicios para verificar la configuración y operación del cortafuegos incorporado en el kernel de Linux: NETFILTER. Concretamente, la que más se utilizó fue *iptables*.

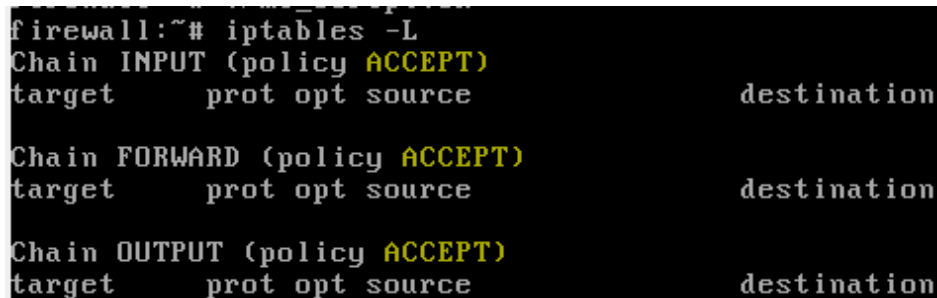
Para la realización del ejercicio 1 tanto como del ejercicio 2, fue necesario crear y configurar las máquinas virtuales asociadas a los mismos, de forma que se pudo simular dos pequeñas redes: una interna segura y una externa no segura. El cortafuegos se encargará de separarlas. Estas máquinas virtuales son: interno, con una dirección MAC correspondiente a 080027111111, externo, con una dirección MAC correspondiente a 080027222222, y firewall, con dos adaptadores de red y, por lo tanto, dos direcciones MAC: 080027333333 y 080027444444.

2. EJERCICIO 1

Este primer ejercicio consiste en la configuración de reglas de filtrado y NAT en NETFILTER utilizando la herramienta *iptables*. La configuración se realiza utilizando *scripts* en *Bash* que contienen los comandos *iptables* deseados.

a. CONFIGURACIÓN POR DEFECTO Y RESTRICCIONES A IMPLEMENTAR

La configuración inicial viene dada en el archivo *iptables-inicial.sh*. Para verificar la configuración de partida, se utilizó el siguiente comando:



```
firewall:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source      destination

Chain FORWARD (policy ACCEPT)
target     prot opt source      destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source      destination
```

Tal y como se puede ver, la política por defecto es aceptar siempre.

Hay una serie de restricciones que se quieren implementar en la red:

- Enmascaramiento del enrutado interno (10.0.3.0)
- Peticiones web: redirigidas a la máquina 10.0.3.40
- Permitir únicamente tráfico de salida vía web o ssh.
- Registro de los intentos de acceso desde la red externa al firewall, y a las máquinas internas.
- El firewall solo admitirá conexiones ssh de la red interna.
- Limitación: control de tráfico ICMP para evitar ataques DoS.

b. PRIMER SCRIPT IMPLEMENTADO: IPTABLES-DROP-1

Para probar las herramientas proporcionadas por NETFILTER se implementó el script *iptables-drop-1.sh*. En este script se vacían y reinician las tablas, se establecen las políticas por defecto (que serán denegar por defecto con DROP), se dan permisos al cortafuego (que serán permitirle todo). Además, se añaden reglas para realizar enmascaramiento de paquetes de la red interna a la externa, para redireccionar el servicio HTTP a la red interna y para permitir el redireccionamiento de paquetes.

Para la verificación del este script, es necesario realizar `iptables -L` e `iptables -t nat -L`, así se podrá conocer la configuración actual del firewall. Tal y como se escribió en el script, las políticas por defecto son DROP, lo que se puede ver en la imagen añadida a continuación:

```
firewall:/mnt/compartida# ./iptables-drop-1.sh
firewall:/mnt/compartida# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
```

En el script también se definieron las políticas para PREROUTING y POSTROUTING, que son ACCEPT. Tal y como se puede ver en la imagen adjuntada a continuación:

```
firewall:/mnt/compartida# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
DNAT       tcp  --  anywhere              anywhere          tcp dpt:www to:10.0.3.40:80

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  10.0.3.0/24           anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
firewall:/mnt/compartida#
```

Además, en el POSTROUTING se puede ver que se configuró correctamente el enmascaramiento y en el PREROUTING que se configuró correctamente el redireccionamiento.

A continuación, se realizarán una serie de pruebas entre interno y externo para ver el funcionamiento del firewall.

i. Conexión telnet desde interno a externo

En primer lugar, se estableció una conexión telnet desde interno a externo. En externo se verificaron las conexiones establecidas y se pudo comprobar que fue posible realizar la conexión. Esto es así, puesto que de momento no se han limitado las conexiones a HTTP y a DNS. Se puede ver en la imagen adjuntada a continuación:

```

externo:~# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
getnameinfo failed
getnameinfo failed
tcp6      0      0 [UNKNOWN]:telnet        [UNKNOWN]:35759        ESTABLISHED
externo:~# _

```

ii. Conexión web desde externo al firewall

A continuación, se estableció una conexión web desde externo al firewall y, tal y como se puede ver a continuación, esta fue exitosa:

```

Pagina web de prueba en texto.dvi
* Texto1 texto1 texto1 texto1
* Texto2 texto2 texto2 texto2

```

iii. Conexión web desde interno a externo

También se estableció una conexión web desde interno a externo y, tal y como se puede ver, esta fue exitosa:

```

Pagina web de prueba en texto.dvi
* Externo
* Texto2 texto2 texto2 texto2

```

iv. Escaneo de puertos nmap desde el firewall hacia interno y externo

Ambos escaneos fueron exitosos, tal y como se puede ver en las siguientes dos imágenes.

```

interno:~# nmap 10.0.3.1 -p 22

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-25 14:18 CET
Interesting ports on 10.0.3.1:
PORT      STATE      SERVICE
22/tcp    filtered  ssh
MAC Address: 08:00:27:33:33:33 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.336 seconds

```

```

externo:~# nmap 192.168.100.77 -p 22

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-25 14:19 CET
Interesting ports on 192.168.100.77:
PORT      STATE      SERVICE
22/tcp    filtered  ssh
MAC Address: 08:00:27:44:44:44 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.296 seconds

```

3. EJERCICIO 2

En este apartado se realizarán las restricciones que aún no han sido implementadas:

- Permitir únicamente tráfico de salida vía web o ssh.
- Registro de los intentos de acceso desde la red externa al firewall, y a las máquinas internas.
- El firewall solo admitirá conexiones ssh de la red interna.
- Limitación: control de tráfico ICMP para evitar ataques DoS.

a. IPTABLES-DROP-2

En este script se añadieron reglas para el filtrado de tráfico.

i. Filtro para limitar ICMP

Estas reglas permiten limitar el tráfico ICMP, con la opción --limit, con el fin de permitir como mucho cinco peticiones por segundo de INPUT, OUTPUT o FORWARD para evitar ataques DoS.

ii. Filtro de entrada a la red interna

Estas reglas permiten redirigir los servicios. Cuando se trata de la interfaz asociada a la red externa y el destino es interno, siempre se acepta la redirección: con -i se indica la interfaz a través de la que se reciben paquetes y con -j la acción. Además, se indica que siempre se trata con el puerto 80, asociado a HTTP. Cuando se trata de la interfaz asociada a la red interna y el emisor es interno, también se acepta y además se añade el campo estado con la información ESTABLISH, RELATED. Para el resto de casos, en los que se parte de la interfaz externa y el destino es interno, se registran los accesos a la red interna.

iii. Filtro de salida para la red interna

En primer lugar, se establece que se permiten paquetes que hayan sido recibidos desde la red interna, con la opción -i, y cuyo emisor sea interno. También se aceptan paquetes que hayan sido enviados desde la red interna, con la opción -o, y cuyo destinatario sea interno. Todo esto permite conexiones HTTP salientes y sus respuestas.

Para permitir peticiones DNS salientes y sus respuestas, el procedimiento es el mismo. Únicamente cambia el puerto, en lugar de 80 es 53, y además se añaden reglas asociadas a UDP, ya que de momento todas las reglas estaban asociadas a TCP.

Finalmente, se rechaza cualquier otro intento de salida con la opción -j REJECT --reject-with-icmp-port-unreachable.

iv. Filtro de conexiones hacia el firewall

El filtrado de conexiones hacia el firewall permite el tráfico SSH de entrada y de salida desde la red interna, mientras que bloquea el resto, siguiendo la política por defecto. Para ello, simplemente se añaden dos reglas con las opciones -i, -o para la interfaz, en las que el emisor y el destinatario, respectivamente, es interno. En este caso no se utiliza forward, sino INPUT para la regla -i y OUTPUT para la regla -O.

Además, se registran los intentos de acceso al firewall desde la red externa.

b. VERIFICACIÓN DEL SCRIPT

i. Configuración actual

En primer lugar, se verificó la configuración del firewall y se introdujo en un archivo el resultado de la verificación con el siguiente comando:

```
iptables -L > file.txt
```

Esto permitiría una mayor legibilidad, tal y como se puede ver a continuación:

```
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere          limit: avg 5/sec burst 5
ACCEPT     tcp  --  10.0.3.0/24           anywhere          tcp dpt:ssh
LOG         all  --  anywhere              anywhere          LOG level warning prefix `Acceso al firewall:'

Chain FORWARD (policy DROP)
target     prot opt source                destination
ACCEPT     icmp --  anywhere              anywhere          limit: avg 5/sec burst 5
ACCEPT     tcp  --  anywhere              10.0.3.40         tcp dpt:www
ACCEPT     tcp  --  10.0.3.40            anywhere          tcp spt:www state RELATED,ESTABLISHED
LOG         all  --  anywhere              10.0.3.0/24       LOG level warning prefix `Acceso a la red interna:'
ACCEPT     tcp  --  10.0.3.0/24          anywhere          tcp dpt:www
ACCEPT     tcp  --  anywhere              10.0.3.0/24       tcp spt:www state RELATED,ESTABLISHED
ACCEPT     tcp  --  10.0.3.0/24          anywhere          tcp dpt:domain
ACCEPT     tcp  --  anywhere              10.0.3.0/24       tcp spt:domain state RELATED,ESTABLISHED
ACCEPT     udp  --  10.0.3.0/24          anywhere          udp dpt:domain
ACCEPT     udp  --  anywhere              10.0.3.0/24       udp spt:domain state RELATED,ESTABLISHED
REJECT     all  --  10.0.3.0/24          anywhere          reject-with icmp-port-unreachable

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere          limit: avg 5/sec burst 5
ACCEPT     tcp  --  anywhere              10.0.3.0/24       tcp spt:ssh
```

También se realizó el mismo procedimiento con:

iptables -t nat -L > file2.txt

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
DNAT       tcp  --  anywhere              anywhere          tcp dpt:www to:10.0.3.40:80

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  10.0.3.0/24           anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Tal y como se puede ver en ambas imágenes, las configuraciones son las detalladas previamente.

ii. Escaneo de puertos desde interno y externo hacia el firewall

Desde interno, el puerto ssh está abierto sin restricciones, tal y como se puede ver a continuación:

```
Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-25 14:38 CET
Interesting ports on 10.0.3.1:
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:33:33:33 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.085 seconds
```

Desde externo, el puerto ssh está limitado, tal y como se puede ver a continuación:

```
externo:~# nmap 192.168.100.77 -p 22

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-25 14:41 CET
Interesting ports on 192.168.100.77:
PORT      STATE SERVICE
22/tcp    filtered ssh
MAC Address: 08:00:27:44:44:44 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.295 seconds
externo:~#
```

iii. Conexión TELNET desde interno a externo

Tal y como se puede ver, es imposible realizar la conexión, ya que todo lo que no sea HTTP no está permitido.

```
interno:~# telnet 192.168.100.212
Trying 192.168.100.212...
telnet: Unable to connect to remote host: Connection refused
```

iv. Conexión web desde interno a externo y desde externo al firewall

Tal y como se puede ver, desde intento a externo todo funciona correctamente. Y desde externo al firewall este redirige y se obtiene la web de interno.

```
Pagina web de prueba
Pagina web de prueba en texto.dvi
* Externo
* Texto2 texto2 texto2 texto2
```

```
Pagina web de prueba
Pagina web de prueba en texto.dvi
* Texto1 texto1 texto1 texto1
* Texto2 texto2 texto2 texto2
```

v. Verificación del registro de accesos en el firewall

Tal y como se puede ver, todos los mensajes incluidos en el script propuesto están en el log.

```
Dec 25 14:29:38 observador kernel: [ 9884.474458] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:29:41 observador kernel: [ 9887.474077] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:29:46 observador kernel: [ 9912.475803] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:29:53 observador kernel: [ 9919.474550] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:30:00 observador kernel: [ 9932.474557] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:30:15 observador kernel: [ 9841.474080] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:30:22 observador kernel: [ 9846.474385] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:37:00 observador kernel: [10246.473522] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:37:04 observador kernel: [10250.474084] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:37:14 observador kernel: [10260.472582] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:37:20 observador kernel: [10274.473632] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:37:44 observador kernel: [10282.474603] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:37:59 observador kernel: [10305.474582] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:39:21 observador kernel: [10387.946634] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=44 TOS=0x00 PREC=0x00 TTL=59 ID=32618 PROTO=TCP SPT=41741 DPT=22
Dec 25 14:39:21 observador kernel: [10387.946634] VTI00=4996 RES=0x00 SYN URGP=0
Dec 25 14:39:21 observador kernel: [10388.045531] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=44 TOS=0x00 PREC=0x00 TTL=46 ID=43391 PROTO=TCP SPT=41742 DPT=22
Dec 25 14:39:44 observador kernel: [10413.074811] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=23888 DF PROTO=TCP SPT=46144 DPT=22
Dec 25 14:39:49 observador kernel: [10416.073757] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=23809 DF PROTO=TCP SPT=46144 DPT=22
Dec 25 14:39:55 observador kernel: [10422.073731] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=23810 DF PROTO=TCP SPT=46144 DPT=22
Dec 25 14:40:07 observador kernel: [10434.074154] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=23811 DF PROTO=TCP SPT=46144 DPT=22
Dec 25 14:40:33 observador kernel: [10458.075912] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=23812 DF PROTO=TCP SPT=46144 DPT=22
Dec 25 14:41:21 observador kernel: [10507.514736] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=42592 DF PROTO=TCP SPT=58866 DPT=22
Dec 25 14:41:24 observador kernel: [10516.514644] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=42593 DF PROTO=TCP SPT=58866 DPT=22
Dec 25 14:41:30 observador kernel: [10516.513900] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=68 TOS=0x00 PREC=0x00 TTL=64 ID=42594 DF PROTO=TCP SPT=58866 DPT=22
Dec 25 14:41:59 observador kernel: [10543.266800] Acceso a firewall:In:eth1 OUT: MAC=08:00:27:44:44:44:08:00:27:22:22:22:08:00 SRC=192.168.100.212 DST=192.168.100.77 LEN=44 TOS=0x00 PREC=0x00 TTL=56 ID=346 PROTO=TCP SPT=52577 DPT=22
Dec 25 14:41:59 observador kernel: [10543.266800] VTI00=1024 RES=0x00 SYN URGP=0
Dec 25 14:41:59 observador kernel: [10543.266800] VTI00=3072 RES=0x00 SYN URGP=0
Dec 25 14:42:39 observador kernel: [10585.474126] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:42:47 observador kernel: [10593.473950] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:43:00 observador kernel: [10606.473949] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:43:18 observador kernel: [10624.474355] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:43:38 observador kernel: [10644.473937] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:44:00 observador kernel: [10666.668882] Acceso a la red interna:In:eth1 OUT:eth0 SRC=192.168.100.212 DST=10.0.0.340 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=TCP SPT=80 DPT=56198 VTI00=5792 RES=0x00 ACK SYN URGP=0
Dec 25 14:44:00 observador kernel: [10666.669937] Acceso a la red interna:In:eth1 OUT:eth0 SRC=192.168.100.212 DST=10.0.0.340 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=55132 DF PROTO=TCP SPT=80 DPT=56198 VTI00=108 RES=0x00 ACK PSN URGP=0
Dec 25 14:44:00 observador kernel: [10666.670649] Acceso a la red interna:In:eth1 OUT:eth0 SRC=192.168.100.212 DST=10.0.0.340 LEN=489 TOS=0x00 PREC=0x00 TTL=63 ID=55129 DF PROTO=TCP SPT=80 DPT=56198 VTI00=108 RES=0x00 ACK PSN URGP=0
Dec 25 14:44:00 observador kernel: [10666.670748] Acceso a la red interna:In:eth1 OUT:eth0 SRC=192.168.100.212 DST=10.0.0.340 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=55130 DF PROTO=TCP SPT=80 DPT=56198 VTI00=108 RES=0x00 ACK PSN URGP=0
Dec 25 14:44:00 observador kernel: [10666.672545] Acceso a la red interna:In:eth1 OUT:eth0 SRC=192.168.100.212 DST=10.0.0.340 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=55131 DF PROTO=TCP SPT=80 DPT=56198 VTI00=108 RES=0x00 ACK PSN URGP=0
Dec 25 14:46:17 observador kernel: [10803.474556] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:46:20 observador kernel: [10806.473817] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:46:28 observador kernel: [10816.473702] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:46:47 observador kernel: [10833.474114] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Dec 25 14:47:00 observador kernel: [10854.400253] Acceso a firewall:In:eth1 OUT: MAC=ffff:ffff:ffff:ffff:08:00:27:22:22:22:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
```

4. CONCLUSIONES FINALES

Tras realizar la práctica, la mejor conclusión que se puede extraer es que es necesario limitar las comunicaciones de una red interna, que puede tener información sensible, con una red externa desconocida lo máximo posible.

En primer lugar, con las configuraciones por defecto, esta limitación era inexistente, ya que se aceptaban todos los paquetes sin ningún criterio. Con el primer script, se añadieron políticas de

redireccionamiento y se establecieron políticas por defecto asociadas al firewall, lo que permitía, al menos, descartar paquetes que pasaran a través de él.

Finalmente, con el segundo script, se añadieron políticas para limitar el acceso a la red por parte de elementos externos y, además, se añadieron protecciones contra posibles ataques, tales como un ataque DoS.

Es necesario conocer las necesidades de una red a la hora de implementar un cortafuegos con el fin de poder obtener una seguridad apropiada.