Miguel Córdoba Aranda 2º ASIR Seguridad

CORTAFUEGOS III

1. Permite poder hacer conexiones ssh al exterior desde la máquina cortafuegos.

```
iptables -A INPUT -s 192.168.122.0/24 -p tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -d 192.168.122.0/24 -p tcp --sport 22 -m state --
state ESTABLISHED -j ACCEPT
```

1.1 Politica por Defecto

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

```
root@Cortafuegos:/home/debian# iptables -A INPUT -s 192.168.122.0/24 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -d 192.168.122.0/24 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
root@Cortafuegos:/home/debian# iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

2. Permite hacer consultas DNS desde la máquina cortafuegos sólo al servidor 192.168.202.2. Comprueba que no puedes hacer un dig @1.1.1.1.

```
iptables -I INPUT -s 192.168.202.2 -j ACCEPT
iptables -I OUTPUT -d 192.168.202.2 -j ACCEPT
```

```
root@Cortafuegos:/home/debian# dig @192.168.202.2 www.google.es

; <<>> DiG 9.16.22-Debian <<>> @192.168.202.2 www.google.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50820
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 54c5cf7b4f5478043bb06fae6220a4d4323e145d3f2bcab1 (good)
;; QUESTION SECTION:
;www.google.es.                 IN      A

;; ANSWER SECTION:
www.google.es.          156     IN      A       142.250.185.3

;; AUTHORITY SECTION:
google.es.              71770   IN      NS      ns3.google.com.
google.es.              71770   IN      NS      ns1.google.com.
google.es.              71770   IN      NS      ns2.google.com.
google.es.              71770   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         158441  IN      A       216.239.32.10
ns2.google.com.         158441  IN      A       216.239.34.10
ns3.google.com.         158441  IN      A       216.239.36.10
ns4.google.com.         158441  IN      A       216.239.38.10
ns1.google.com.         158441  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         158441  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         158441  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         158441  IN      AAAA    2001:4860:4802:38::a

;; Query time: 0 msec
;; SERVER: 192.168.202.2#53(192.168.202.2)
;; WHEN: Thu Mar 03 12:21:56 CET 2022
;; MSG SIZE  rcvd: 344

root@Cortafuegos:/home/debian# dig @1.1.1.1 www.google.es

; <<>> DiG 9.16.22-Debian <<>> @1.1.1.1 www.google.es
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

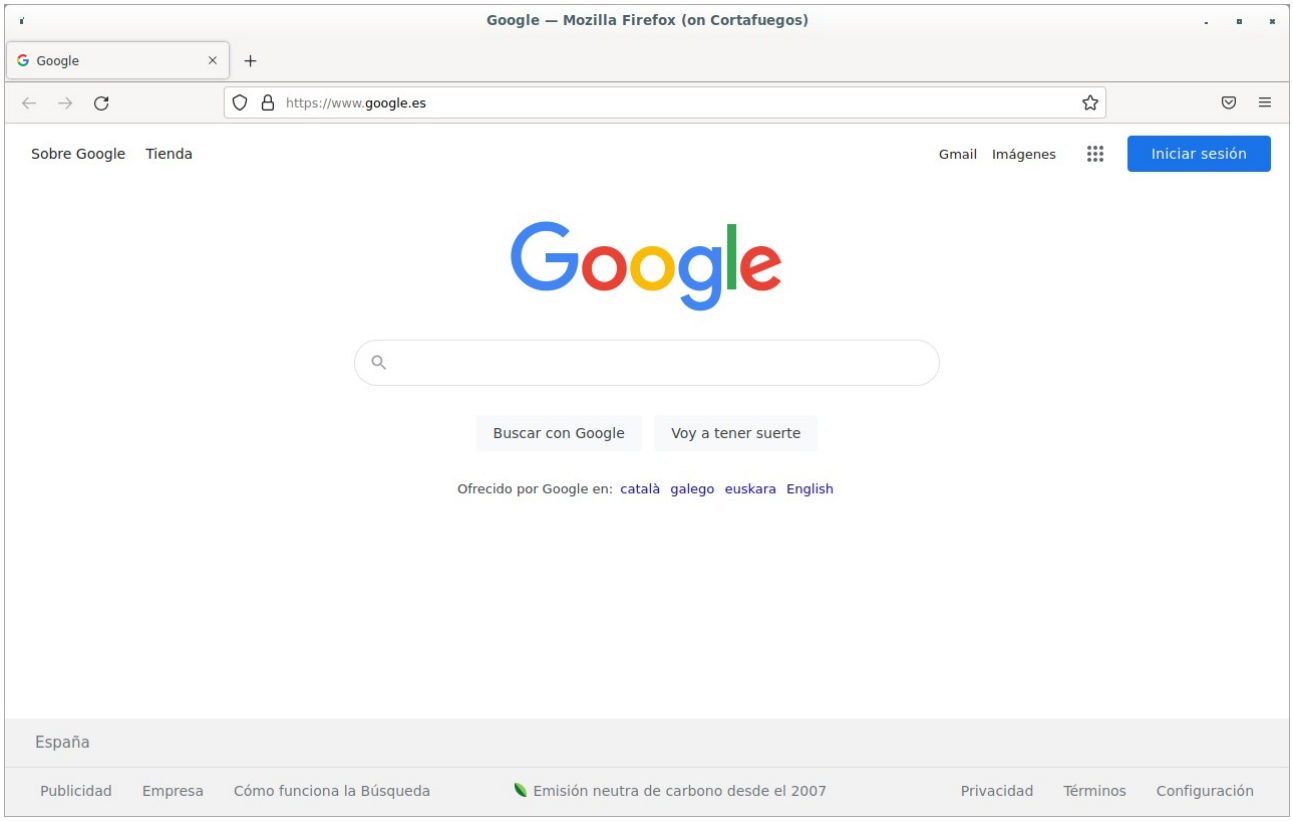
3. Permite que la máquina cortafuegos pueda navegar por internet.

```
iptables -A INPUT -i enp1s0 -p tcp --dport 80 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp1s0 -p tcp --sport 80 -m state --state
ESTABLISHED -j ACCEPT

iptables -A INPUT -i enp1s0 -p tcp --sport 443 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp1s0 -p tcp --dport 443 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

3.1 DNS

```
iptables -A INPUT -i enp1s0 -p udp --sport 53 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp1s0 -p udp --dport 53 -m state --state
NEW,ESTABLISHED -j ACCEPT
```



4. Los equipos de la red local deben poder tener conexión al exterior.

4.1 Primero he puesto la regla **POSTROUTING** y luego he activado el **BIT FORWARD** en la máquina **Cortafuegos**.

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o enp1s0 -j MASQUERADE

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

4.2 Luego he activado el protocolo ICMP en las interfaces enp1s0 (red publica) y enp7s0 (red lan)

```
iptables -A INPUT -i enp1s0 -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A OUTPUT -o enp1s0 -p icmp --icmp-type echo-request -j ACCEPT

iptables -A OUTPUT -o enp7s0 -p icmp -m icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -i enp7s0 -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
```

```
debian@Cortafuegos-Cliente:~$ ip a | egrep enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 10.0.0.2/24 brd 10.0.0.255 scope global enp1s0
debian@Cortafuegos-Cliente:~$ ping 1.1.1.1 -c 4
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=53 time=46.3 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=53 time=47.2 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=53 time=47.2 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=53 time=620 ms

--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 46.306/190.169/620.001/248.163 ms
```

5. Permitimos el ssh desde el cortafuego a la LAN

```
iptables -A OUTPUT -p tcp -o enp7s0 -d 10.0.0.0/24 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -i enp7s0 -s 10.0.0.0/24 --sport 22 -j ACCEPT
```

```
debian@Cortafuegos:~$ ssh debian@10.0.0.2
debian@10.0.0.2's password:
Linux Cortafuegos-Cliente 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar  7 08:41:19 2022 from 10.0.0.1
debian@Cortafuegos-Cliente:~$
```

6. Permitimos hacer ping desde la LAN a la máquina cortafuegos.

```
iptables -A OUTPUT -o enp7s0 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -i enp7s0 -p icmp --icmp-type echo-reply -j ACCEPT
```

```
debian@Cortafuegos-Cliente:~$ ip a | egrep enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 10.0.0.2/24 brd 10.0.0.255 scope global enp1s0
debian@Cortafuegos-Cliente:~$ ping 10.0.0.1 -c 4
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.174 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.451 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3024ms
rtt min/avg/max/mdev = 0.174/0.728/1.185/0.427 ms
```

7. Permite realizar conexiones ssh desde los equipos de la LAN

```
iptables -A INPUT -s 10.0.0.0/24 -p tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -d 10.0.0.0/24 -p tcp --sport 22 -m state --state
ESTABLISHED -j ACCEPT
```

```
debian@Cortafuegos-Cliente:~$ ssh debian@10.0.0.1
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:oRZPMyMzm2O0oCo2MSFXUVnoJqgI7U9YZghuNO6n54A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.1' (ECDSA) to the list of known hosts.
debian@10.0.0.1's password:
Linux Cortafuegos 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar  7 10:14:35 2022 from 192.168.122.1
```

Conexión ssh desde la LAN hasta mi maquina anfitrión.

```
root@Cortafuegos-Cliente:/home/debian# ssh miguel@192.1.100.1
The authenticity of host '192.1.100.1 (192.1.100.1)' can't be established.
ECDSA key fingerprint is SHA256:hiVx/7gNGEOeObnhw2zpmxcKNpqWDzE5zK4EjeL07A4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.1.100.1' (ECDSA) to the list of known hosts.
miguel@192.1.100.1's password:
Linux MCA 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
miguel@MCA:~$
```

8. Instala un servidor de correos en la máquina de la LAN. Permite el acceso desde el exterior y desde el cortafuego al servidor de correos. Para probarlo puedes ejecutar un telnet al puerto 25 tcp.

Para instalar el servidor de correos primero he tenido que insertar las siguientes reglas:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o enp1s0 -j MASQUERADE
```

8.1 DNS

```
iptables -A INPUT -i enp7s0 -p udp --sport 53 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp7s0 -p udp --dport 53 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

8.2 HTTP

```
iptables -A INPUT -i enp7s0 -p tcp --sport 80 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp7s0 -p tcp --dport 80 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

8.3 HTTPS

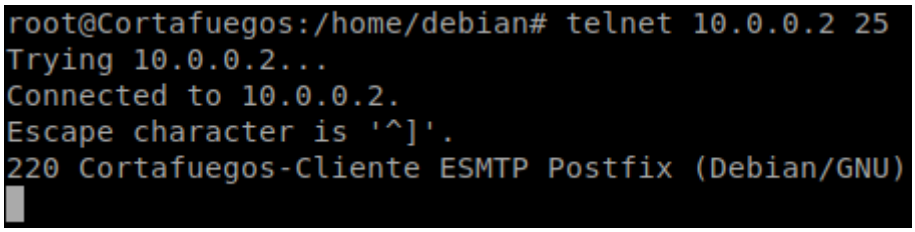
```
iptables -A INPUT -i enp7s0 -p tcp --sport 443 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp7s0 -p tcp --dport 443 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

Luego he instalado el servidor de correos **postfix** con `apt-get install postfix`.

Ahora añado las siguientes reglas para poder acceder al servidor de correo y hacer la prueba correspondiente.

Para poder acceder desde la máquina cortafuegos hacia la maquina del correo (LAN).

```
iptables -A INPUT -i enp7s0 -p tcp --sport 25 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp7s0 -p tcp --dport 25 -m state --state
NEW,ESTABLISHED -j ACCEPT
```



Acceso al servidor de correo desde el exterior.

```
iptables -t nat -A PREROUTING -p tcp --dport 25 -i enp1s0 -j DNAT --to
10.0.0.2
iptables -A FORWARD -i enp1s0 -o enp7s0 -p tcp --dport 25 -m state --
state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp1s0 -o enp7s0 -p tcp --sport 25 -m state --
state ESTABLISHED -j ACCEPT
```

9. Permite poder hacer conexiones ssh desde exterior a la LAN

```
iptables -t nat -A PREROUTING -p tcp --dport 22 -i enp1s0 -j DNAT --to 10.0.0.2
iptables -A FORWARD -i enp1s0 -o enp7s0 -p tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp7s0 -o enp1s0 -p tcp --sport 22 -m state --state ESTABLISHED -j
ACCEPT
```

10. Modifica la regla anterior, para que al acceder desde el exterior por ssh tengamos que conectar al puerto 2222, aunque el servidor ssh este configurado para acceder por el puerto 22.

```
iptables -t nat -A PREROUTING -p tcp --dport 2222 -i enp1s0 -j DNAT --to 10.0.0.2:22
```

11. Permite hacer consultas DNS desde la LAN sólo al servidor 192.168.202.2. Comprueba que no puedes hacer un dig @1.1.1.1.

```
iptables -A FORWARD -i enp7s0 -o enp1s0 -d 192.168.202.2 -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp1s0 -o enp7s0 -s 192.168.202.2 -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
```

12. Permite que los equipos de la LAN puedan navegar por internet

```
iptables -A FORWARD -i enp7s0 -o enp1s0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp1s0 -o enp7s0  -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp7s0  -o enp1s0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp1s0 -o enp7s0  -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```