

CORTAFUEGOS II

1. Permite poder hacer conexiones ssh al exterior.

```
nft add rule inet filter input ip saddr 192.168.122.0/24 tcp dport 22 ct state new,established counter accept
nft add rule inet filter output ip daddr 192.168.122.0/24 tcp sport 22 ct state established counter accept
```

Luego pondremos la política **DROP**.

```
nft chain inet filter input { policy drop \; }
nft chain inet filter output { policy drop \; }
```

```
root@Cortafuegos:/home/debian# nft list ruleset
table inet filter {
  chain input {
    type filter hook input priority filter; policy drop;
    ip saddr 192.168.122.0/24 tcp dport 22 ct state established,new counter packets 310 bytes 20932 accept
  }
  chain output {
    type filter hook output priority filter; policy drop;
    ip daddr 192.168.122.0/24 tcp sport 22 ct state established counter packets 174 bytes 40660 accept
  }
}
```

2. Deniega el acceso a tu servidor web desde una ip concreta.

Para este ejercicio he habilitado varias reglas.

En primer lugar he tenido que habilitar **DNS** para instalar **Apache2** de los repositorios.

```
nft add rule inet filter output oifname enp1s0 udp dport 53 ct state new,established counter accept
nft add rule inet filter input iifname enp1s0 udp sport 53 ct state established counter accept
```

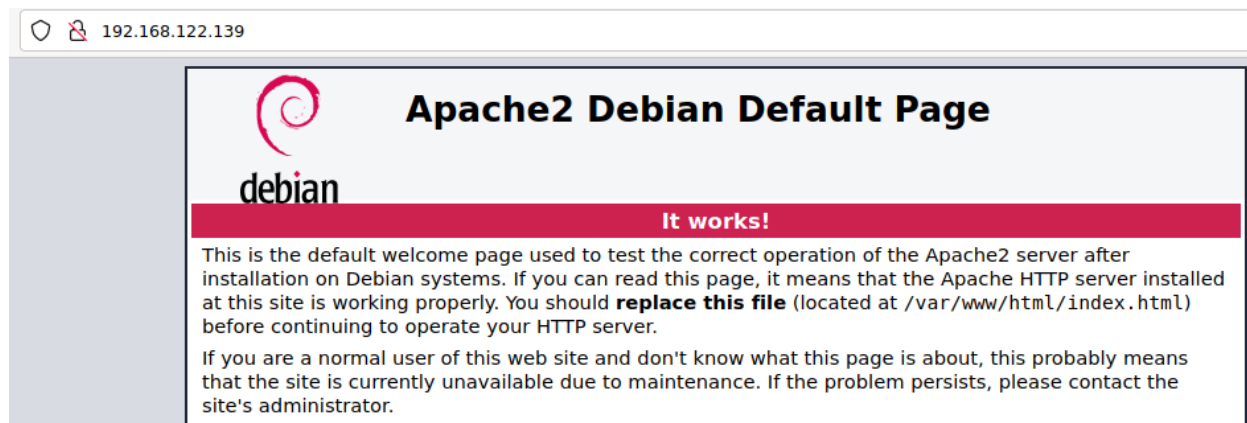
En segundo lugar he habilitado el trafico **HTTP/HTTPS** para poder descargarme la herramienta.

```
nft add rule inet filter output oifname enp1s0 ip protocol tcp tcp dport { 80,443 } ct state new,established counter accept
nft add rule inet filter input iifname enp1s0 ip protocol tcp tcp sport { 80,443 } ct state established counter accept
```

Luego he añadido las reglas necesarias para **acceder** a nuestro **Servidor Web**.

```
nft add rule inet filter output oifname enp1s0 tcp sport 80 ct state established counter accept
```

```
nft add rule inet filter input iifname enp1s0 tcp dport 80 ct state new,established counter accept
```



En este paso rechazo la ip **192.168.1.51** lo que denegará a mi máquina anfitrión el acceso a al **Servidor Web**.

```
nft add rule inet filter input ip saddr 192.168.122.1 tcp dport 80  
counter drop
```

```
nft add rule inet filter output ip daddr 192.168.122.1 tcp sport 80  
counter drop
```

5. Permite hacer consultas DNS sólo al servidor 192.168.202.2. Comprueba que no puedes hacer un dig @1.1.1.1.

```
nft insert rule inet filter input ip saddr 192.168.202.2 counter accept  
nft insert rule inet filter output ip daddr 192.168.202.2 counter accept
```

```

root@Cortafuegos:/home/debian# dig @192.168.202.2 google.com

; <<>> DiG 9.16.22-Debian <<>> @192.168.202.2 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38391
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 43974c826c450bc1fa29bc1761f79e28b5d491b5e6ca80a9 (good)
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                268     IN      A      142.250.200.142

;; AUTHORITY SECTION:
google.com.                5460    IN      NS      ns2.google.com.
google.com.                5460    IN      NS      ns1.google.com.
google.com.                5460    IN      NS      ns4.google.com.
google.com.                5460    IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.            5460    IN      A      216.239.32.10
ns2.google.com.            5460    IN      A      216.239.34.10
ns3.google.com.            5460    IN      A      216.239.36.10
ns4.google.com.            5460    IN      A      216.239.38.10
ns1.google.com.            5460    IN      AAAA   2001:4860:4802:32::a
ns2.google.com.            5460    IN      AAAA   2001:4860:4802:34::a
ns3.google.com.            5460    IN      AAAA   2001:4860:4802:36::a
ns4.google.com.            5460    IN      AAAA   2001:4860:4802:38::a

;; Query time: 4 msec
;; SERVER: 192.168.202.2#53(192.168.202.2)
;; WHEN: Mon Jan 31 09:30:33 CET 2022
;; MSG SIZE rcvd: 331

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

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

```

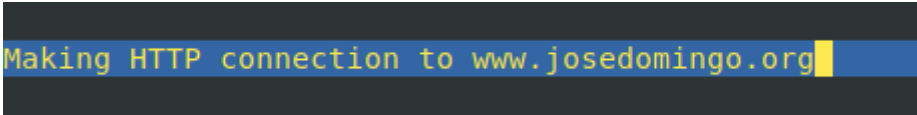
6. No permitir el acceso al servidor web de www.josedomingo.org (Tienes que utilizar la ip).
¿Puedes acceder a fp.josedomingo.org?

```
nft insert rule inet filter input ip saddr 37.187.119.60 tcp sport 80 ct state established counter drop
```

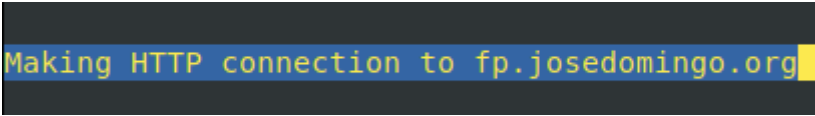
```
nft insert rule inet filter output ip daddr 37.187.119.60 tcp dport 80 ct state new,established counter drop
```

```
nft insert rule inet filter input ip saddr 37.187.119.60 tcp sport 443 ct state established counter drop
```

```
nft insert rule inet filter output ip daddr 37.187.119.60 tcp dport 443 ct state new,established counter drop
```



```
Making HTTP connection to www.josedomingo.org
```

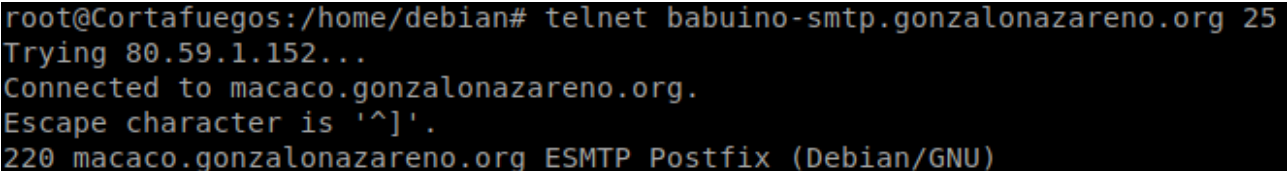


```
Making HTTP connection to fp.josedomingo.org
```

7. Permite mandar un correo usando nuestro servidor de correo: babuino-smtp. Para probarlo ejecuta un telnet bubuino-smtp.gonzalonazareno.org 25.

```
nft add rule inet filter input tcp sport 25 ct state established counter accept
```

```
nft add rule inet filter output tcp dport 25 ct state new,established counter accept
```



```
root@Cortafuegos:/home/debian# telnet babuino-smtp.gonzalonazareno.org 25
Trying 80.59.1.152...
Connected to macaco.gonzalonazareno.org.
Escape character is '^]'.
220 macaco.gonzalonazareno.org ESMTP Postfix (Debian/GNU)
```

8. Instala un servidor mariadb, y permite los accesos desde la ip de tu cliente. Comprueba que desde otro cliente no se puede acceder.

```
nft add rule inet filter input ip saddr 192.168.122.115 tcp dport 3306 counter accept
```

```
nft add rule inet filter output ip daddr 192.168.122.115 tcp sport 3306 counter accept
```

debian@Cortafuegos: ~ 176x9
root@Cortafuegos:/home/debian#

CLIENTE 1
debian@MariayPostgres:~\$ mysql -u pruebafw -h 192.168.122.139 -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.5.12-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

CLIENTE 2
miguel@MCA:~\$ mysql -u pruebafw -h 192.168.122.139 -p
Enter password:
█