

CORTAFUEGOS I

1. Permite poder hacer conexiones ssh al exterior.

Partiendo de que la **Política** por defecto es **DROP**.

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
root@Cortafuegos:/home/debian# iptables -P INPUT DROP
root@Cortafuegos:/home/debian# iptables -P OUTPUT DROP
```

Las reglas para permitir la **conexión ssh** son las siguientes:

```
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
```

Probamos que podemos conectarnos de nuevo con **ssh**.

```
miguel@MCA:~$ ssh debian@192.168.122.139
debian@192.168.122.139'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: Thu Jan 27 12:01:38 2022 from 192.168.122.1
```

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

Para este ejercicio he tenido que habilitar varias reglas. Son las siguientes:

En primer lugar he tenido que habilitar las reglas para el **DNS** para poder instalar **apache2** desde los repositorios.

```
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
```

En segundo lugar he tenido que habilitar las reglas de **HTTP, HTTPS y aceptar la conexión** al **servidor web**.

--HTTP--

```
iptables -A INPUT -i enp1s0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

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

--HTTPS--


```
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
```

--ACCESO AL SERVIDOR WEB--

```
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
```

 192.168.122.139


debian

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining

Y en tercer lugar **denegar la conexión** a una **ip concreta** para que no pueda conectarse a nuestro **servidor web**.

```
iptables -I INPUT 1 -s 192.168.122.1 -p tcp --destination-port 80 -j DROP
```

```
iptables -I OUTPUT 1 -d 192.168.122.1 -p tcp --destination-port 80 -j DROP
```



La conexión ha caducado

El servidor 192.168.122.139 está tardando demasiado en responder.

- El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.
- Si no puede cargar ninguna página, compruebe la conexión de red de su equipo.
- Si su equipo o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.

Reintentar

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

Para este ejercicio he añadido las siguiente reglas:

```
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 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

```

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

```
#PLEDIN 3.0 Feed
* Skip to primary navigation
* Skip to content
* Skip to footer

PLEDIN 3.0
* Inicio
* Blog
* Plataforma
* Módulos
* Presentación

(BUTTON) Toggle search (BUTTON) Toggle menu
Plataforma Educativa Informática

Servidores IESGN

Bienvenidos a la página personal de José Domingo Muñoz Rodríguez, aquí podrás encontrar...

Accede a las entradas de mi blog donde escribo de Informática y Educación.

Blog Pledin

Accede a los materiales de los cursos que he impartido.

Plataforma Pledin

Accede a los contenido de los módulos de FP que estoy impartiendo en la actualidad.

Módulos FP

Últimos posts...

Introducción a las redes y almacenamiento en LXC

lxc
```

--HTTP--

```
iptables -I INPUT 2 -s 37.187.119.60 -p tcp --sport 80 -m state --state ESTABLISHED -j DROP
```

```
iptables -I OUTPUT 2 -d 37.187.119.60 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j DROP
```

--HTTPS--

```
iptables -I INPUT 2 -s 37.187.119.60 -p tcp --sport 443 -m state --state ESTABLISHED -j DROP
```

```
iptables -I OUTPUT 2 -d 37.187.119.60 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j DROP
```

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

Tampoco me puedo conectar a **fp.josedomingo.org** porque la **web** está en el mismo servidor

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

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

--ICMP--

```
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
```

--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
```

--SMTP--

```
iptables -A INPUT -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j 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)
```

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

Para realizar este ejercicio he realizado los siguientes pasos:

1. He creado un usuario en **MySQL** de que permita la conexión remota.

```
#create user pruebafw@'%' identified by 'hola';
```

2. He configurado **MySQL** para permitir conexiones remotas comentando la línea **bind-address**.

```

SERVIDOR
Last login: Thu Feb  3 13:20:28 2022 from 192.168.122.1
debian@Cortafuegos:~$
debian@Cortafuegos:~$ ip a | egrep enpls0
2: enpls0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo fast state UP group default qlen 1000
    inet 192.168.122.139/24 brd 192.168.122.255 scope global dynamic enpls0
debian@Cortafuegos:~$

CLIENTE1
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 34
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)]>

CLIENTE2
miguel@MCA:~$ 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 38
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)]>

```

3. He añadido las siguientes reglas iptables:

--CONEXION REMOTA MYSQL--

```
iptables -A INPUT -s 192.168.122.115 -p tcp --dport 3306 -j ACCEPT
iptables -A OUTPUT -d 192.168.122.115 -p tcp --sport 3306 -j ACCEPT
```

En la captura vemos que **CLIENTE 1** con ip **192.168.122.115** ha podido conectarse al servidor MySQL mientras que **CLIENTE 2** le ha rechazado la conexión.

```

CLIENTE1
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)]>

CLIENTE2
miguel@MCA:~$ mysql -u pruebafw -h 192.168.122.139 -p
Enter password:

```