

Práctica

Cortafuegos con iptables

Franco Larrea

2º SMR-A
(Prof. Fernando Albert González)
Instituto IES SAN VICENTE

Indice

Teoría.....	Pag. 3
Tareas y cuestiones.....	Pag. 4-11
Problemas encontrados.....	Pag. 12
Fuentes.....	Pag. 12
Alumnos participantes.....	Pag. 12

Teoría

Para realizar esta practica es conveniente saber algunos conceptos:

Cortafuegos

Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Iptables

Es una utilidad de línea de órdenes para configurar el cortafuegos del kernel de Linux implementado como parte del proyecto Netfilter. El término iptables también se usa comúnmente para referirse a dicho cortafuegos del kernel. Puede configurarse directamente con iptables, o usando uno de los muchos frontend existentes de consola y gráficos.

Tareas y cuestiones

Configura un firewall usando iptables en un equipo que funcionará como:

Servidor Web (servicio Apache)
 Servidor FTP (servicio vsftpd)
 Servidor SSH (servicio ssh)

- Lo primero que tendrás que hacer es establecer la POLÍTICA por defecto de entrada como DENEGAR (iptables -P INPUT DROP)
- Permitiremos las conexiones al servidor WEB de todos los equipos de la red de clase 192.168.0.0 excepto la IP de un equipo específico de un compañero de clase.
 - Escribe el comando iptables. Toma una captura del equipo del compañero y de otro, comprobando que deniega y permite el acceso respectivamente.
- Añade una nueva regla para permitir el acceso unicamente a 2 equipos al servidor FTP.
 - Escribe los comandos iptables. Toma capturas de los equipos que pueden acceder al servidor.
- Añade otra regla que permita conectar a un equipo al servidor SSH. Este equipo se deberá especificar por su dirección MAC.
 - Escribe los comandos iptables. Toma capturas de los equipos que pueden acceder o no al servidor.
- Cierra todos los puertos mayores de 1024
 - Escribe los comandos iptables.

Realiza primero la tabla teórica de filtrado de paquetes y luego escribe las iptables.

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Acción
1	192.168.0.uno	*	servidor	20:21	PERMITIR
2	192.168.0.dos	*	servidor	20:21	PERMITIR
3	192.168.0.cmp	*	servidor	80	DENEGAR
4	192.168.0.0	*	servidor	80	PERMITIR
5	MAC	*	servidor	22	PERMITIR
P	*	*	Servidor	1024:65535	IGNORAR
P	*	*	Servidor	*	IGNORAR

1. iptables -A INPUT -s 192.168.0.102 -d 192.168.0.244 -p tcp --dport 20:21 -j ACCEPT
2. iptables -A INPUT -s 192.168.0.113 -d 192.168.0.244 -p tcp --dport 20:21 -j ACCEPT
3. iptables -A INPUT -s 192.168.0.135 -d 192.168.0.244 -p tcp --dport 80 -j DROP
4. iptables -A INPUT -s 192.168.0.0/24 -d 192.168.0.244 -p tcp --dport 80 -j ACCEPT
5. iptables -A INPUT -m mac --mac-source 50:65:f3:27:aa:09 -d 192.168.0.244 -p tcp --dport 22 -j ACCEPT
6. iptables -P INPUT DROP

192.168.0.244 = IP del servidor.

192.168.0.102 = IP 1 de una maquina virtual para probar FTP.

192.168.0.113 = IP 2 de una maquina virtual para probar FTP.

192.168.0.135 = IP de una maquina virtual para probar WEB.

50:65:f3:27:aa:09 =MAC real del equipo I103-02 para probar SSH.

Esta práctica se ha realizado en maquinas virtuales con Debian 6.3.0.

Una vez comprendido lo que se nos pide, hecha la tabla teórica y los comandos iptables podemos empezar con la práctica.

Primero instalaremos los servicios que se nos piden en el servidor, tales como Apache, vsftpd y ssh. Con el siguiente comando podemos instalar los tres servicios:

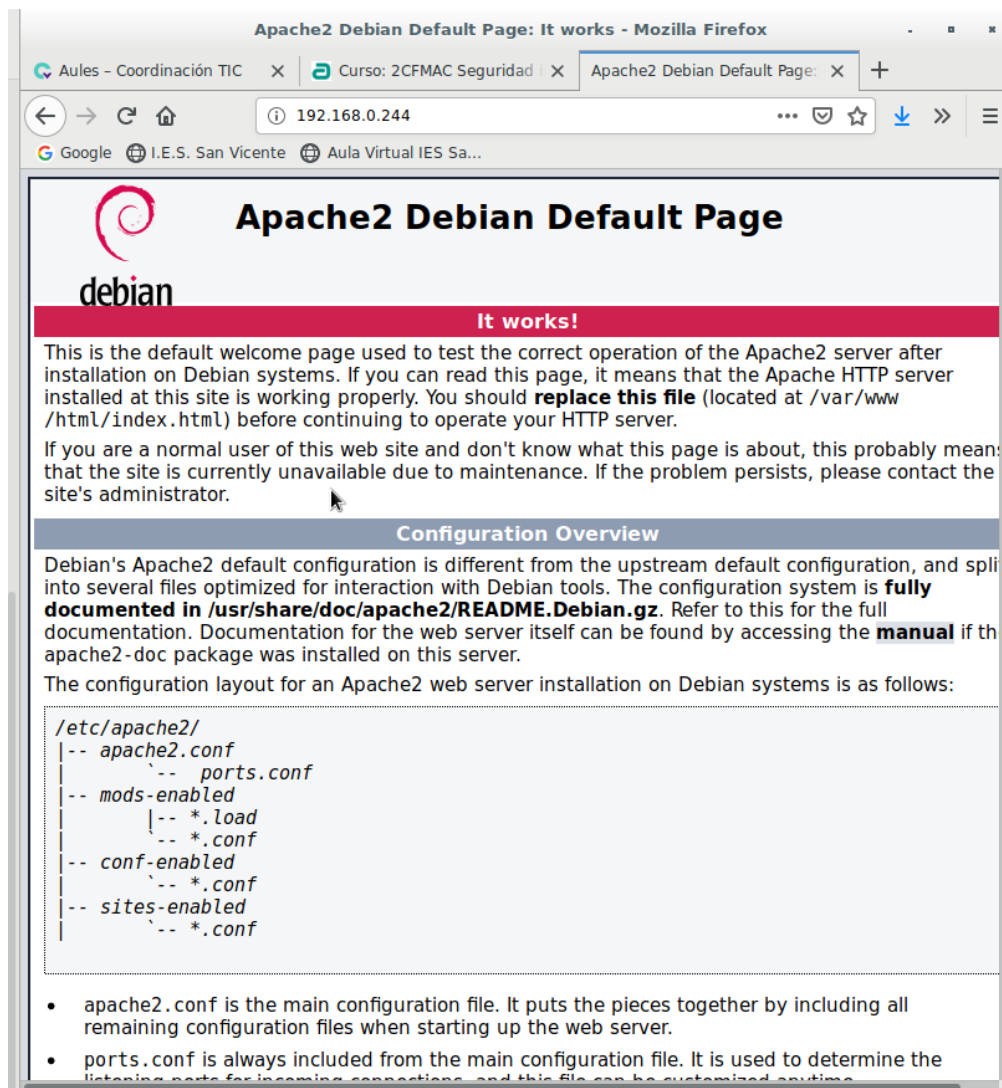
- **sudo apt-get install apache2 ssh vsftpd -y**

```
student@study:~$ sudo apt-get install apache2 ssh vsftpd -y_
```

Antes de continuar vamos a comprobar que los tres servicios funcionan.

Si pongo la IP de mi servidor(192.168.0.244) en el navegador web de mi maquina real podemos comprobar que nos sale la pagina por defecto de Apache2.

El servicio apache2 funciona correctamente.



Ahora vamos a comprobar el servicio ssh, para ello abrimos un terminal en la maquina real y ejecutamos el siguiente comando:

- **ssh student@192.168.0.244**

student es mi usuario como administrador, la IP es la del servidor.

Al ejecutar este comando y poner la contraseña del usuario *student* iniciamos sesión mediante ssh al servidor.

El servicio ssh funciona correctamente.

```
alumno@I103-02:~$ ssh student@192.168.0.244
student@192.168.0.244's password:
Linux study 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64
Last login: Mon Feb  3 12:11:09 2020 from 192.168.0.109
student@study:~$
```

Por ultimo vamos a comprobar el servicio vsftpd, en el mismo terminal ejecutamos el siguiente comando:

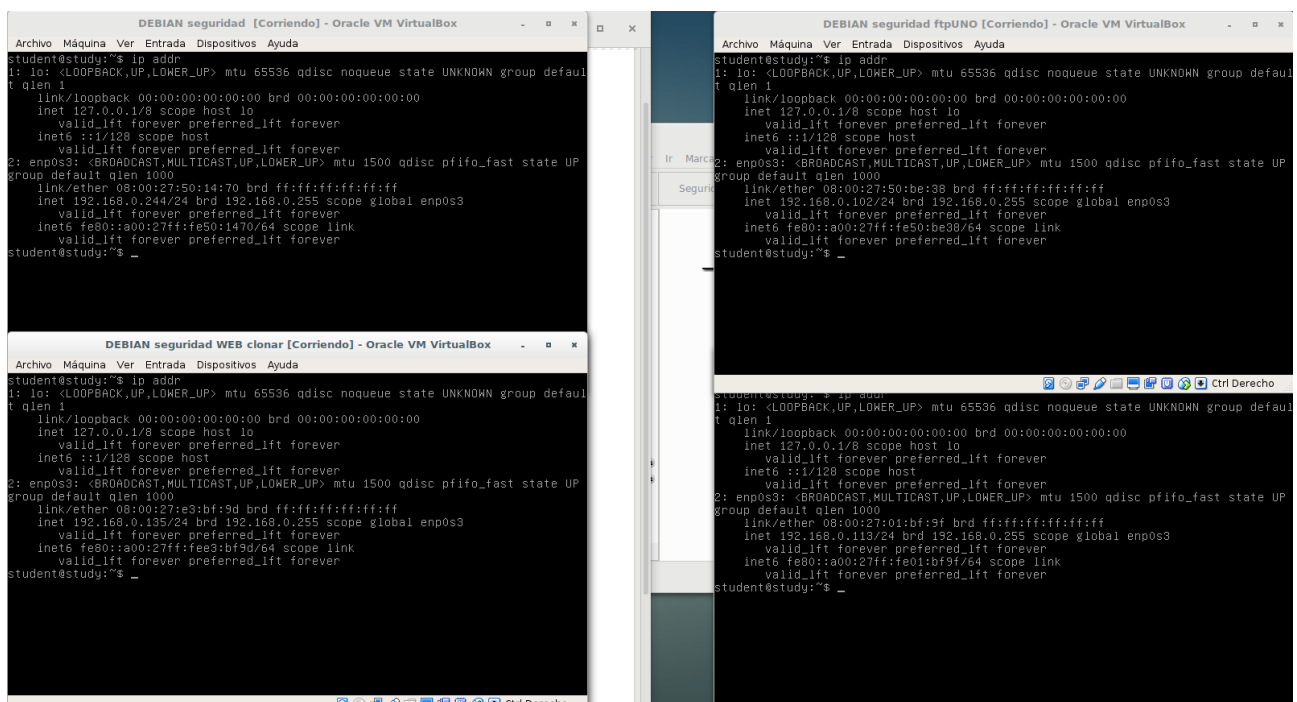
- **ftp 192.168.0.244**

Ingresando el usuario y la contraseña del servidor iniciaremos sesión satisfactoriamente.

El servicio vsftpd funciona correctamente.

```
alumno@I103-02:~$ ftp 192.168.0.244
Connected to 192.168.0.244.
220 (vsFTPd 3.0.3)
Name (192.168.0.244:alumno): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Para efectuar las comprobaciones he creado 3 maquinas virtuales Debian, estas maquinas harán de distintos clientes, cada uno con su propia IP. Además también cuento con la maquina real.



Debian seguridad	Servidor	IP=192.168.0.244
Debian seguridad WEB	Comprobar servicio web	IP=192.168.0.135
Debian seguridad ftpUNO	Comprobar servicio ftp	IP=192.168.0.102
Debian seguridad ftpDOS	Comprobar servicio ftp	IP=192.168.0.113
Maquina real	Comprobar servicio ssh	MAC=50:65:f3:27:aa:09

Vamos a empezar añadiendo las políticas de iptables en el servidor.

```
student@study:~$ sudo iptables -P INPUT DROP
```

Esta política deniega todo lo que entra.

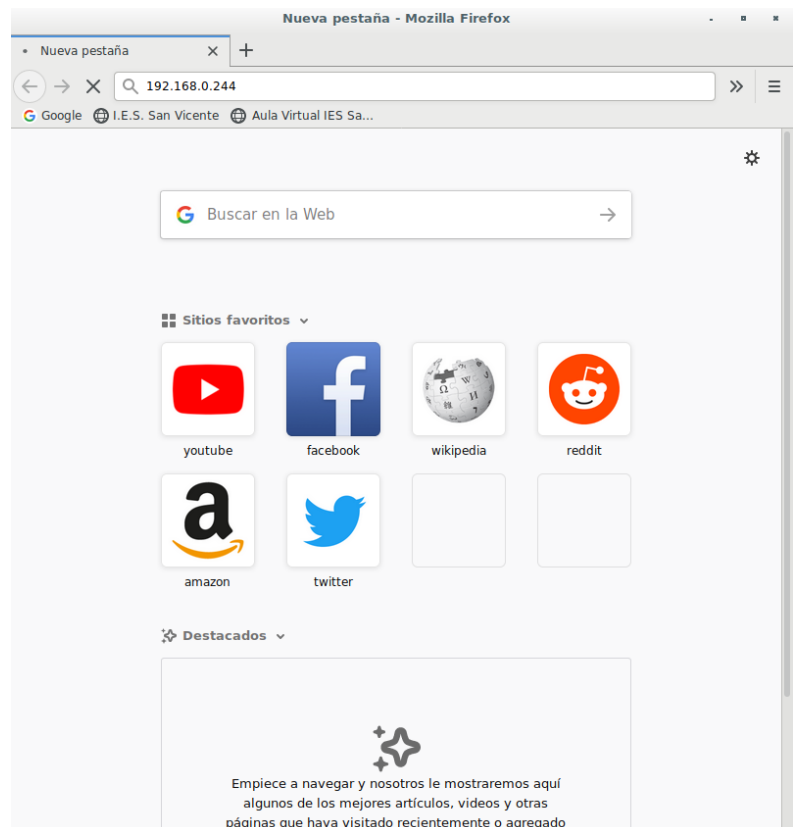
Estaba conectado mediante ssh al servidor pero, obviamente, al establecer esta política dejo de funcionar la conexión.

```
alumno@I103-02:~$ ssh student@192.168.0.244
```

```
□
```

El servicio web y ftp también dejo de funcionar.

```
alumno@I103-02:~$ ftp 192.168.0.244
ftp: connect: Connection timed out
ftp> □
```

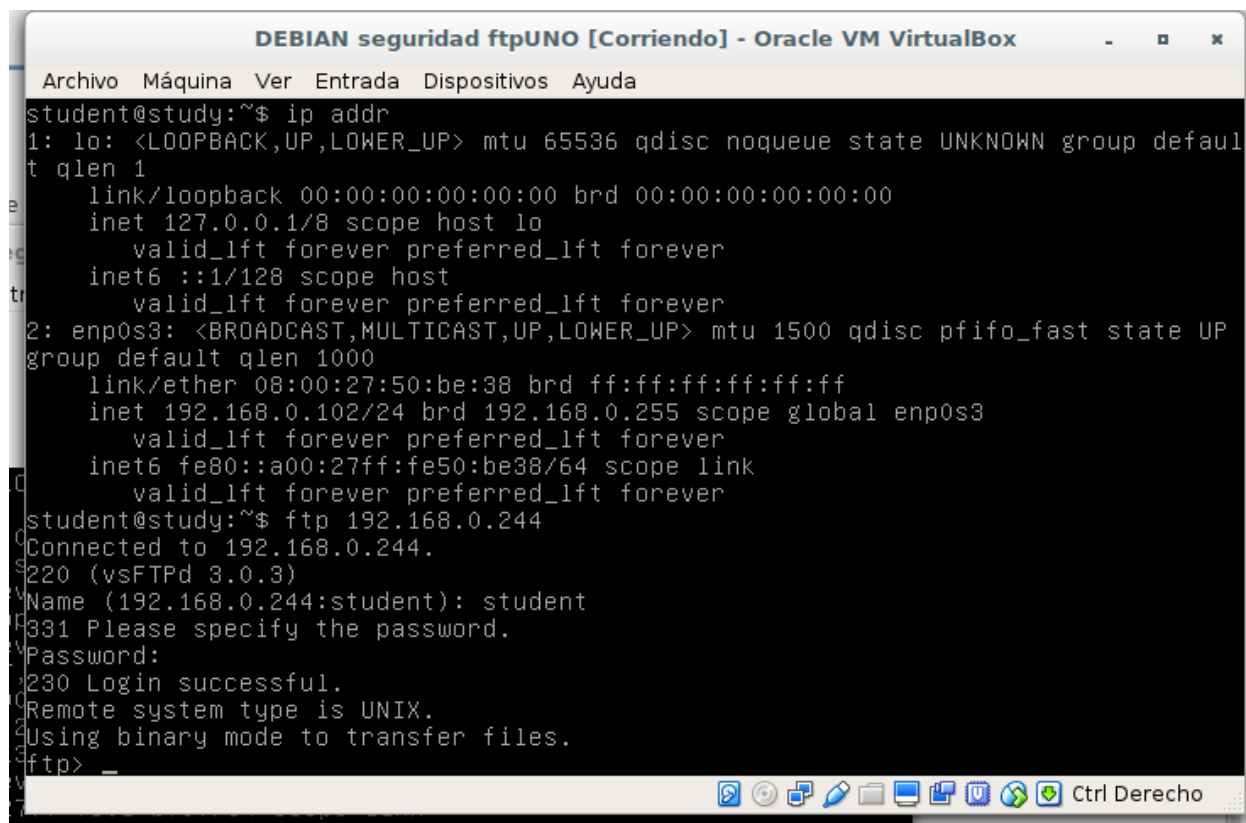


Vamos a añadir una regla para permitir el acceso FTP unicamente a dos equipos, estos será las maquinas virtuales llamadas *Debian seguridad ftpUNO* y *Debian seguridad ftpDOS*.

```
student@study:~$ sudo iptables -A INPUT -s 192.168.0.102 -d 192.168.0.244 -p tcp --dport 20:21 -j ACCEPT
```

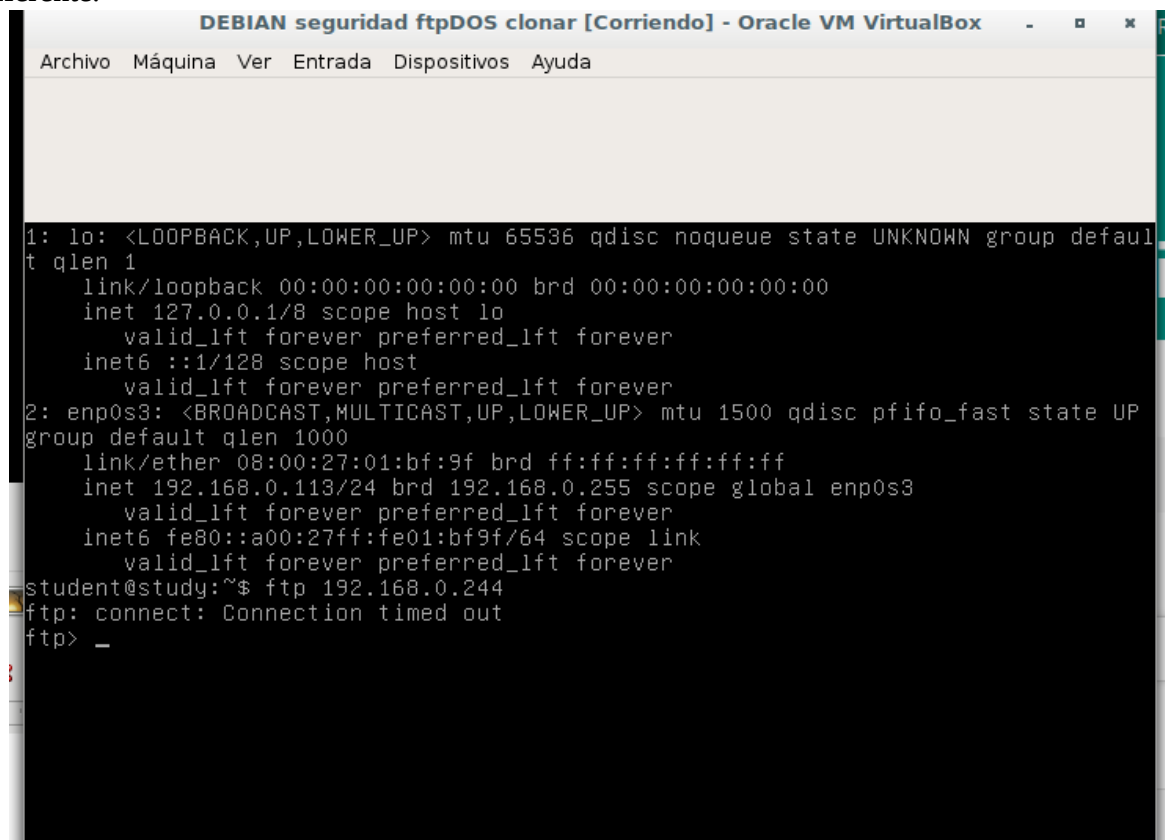
Esta regla debería dar acceso solamente a la maquina con la IP 192.168.0.102.

Efectivamente podemos conectarnos con la maquina *Debian seguridad ftpUNO* al servicio FTP.



```
DEBIAN seguridad ftpUNO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
student@study:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:50:be:38 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe50:be38/64 scope link
        valid_lft forever preferred_lft forever
student@study:~$ ftp 192.168.0.244
Connected to 192.168.0.244.
220 (vsFTPd 3.0.3)
Name (192.168.0.244:student): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

Ahora vamos a intentar conectarnos con la máquina *Debian seguridad ftpDOS*, este cliente tiene una IP diferente.



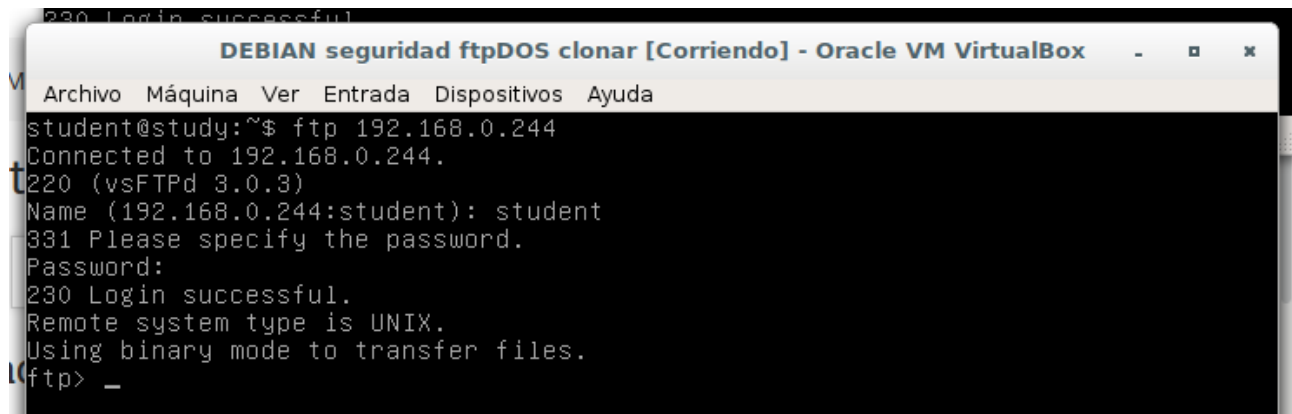
```
DEBIAN seguridad ftpDOS clonar [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:01:bf:9f brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.113/24 brd 192.168.0.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe01:bf9f/64 scope link
        valid_lft forever preferred_lft forever
student@study:~$ ftp 192.168.0.244
ftp: connect: Connection timed out
ftp> _
```

Podemos ver que con esta máquina no podemos conectarnos. De momento solo le permitimos el acceso a la máquina con IP 192.168.0.102.

Vamos a añadir la regla que permitirá el acceso ftp a la maquina *Debian seguridad ftpDOS*.

```
student@study:~$ sudo iptables -A INPUT -s 192.168.0.113 -d 192.168.0.244 -p tcp --dport 20:21 -j ACCEPT
```

Una vez añadida la regla ya podemos acceder:

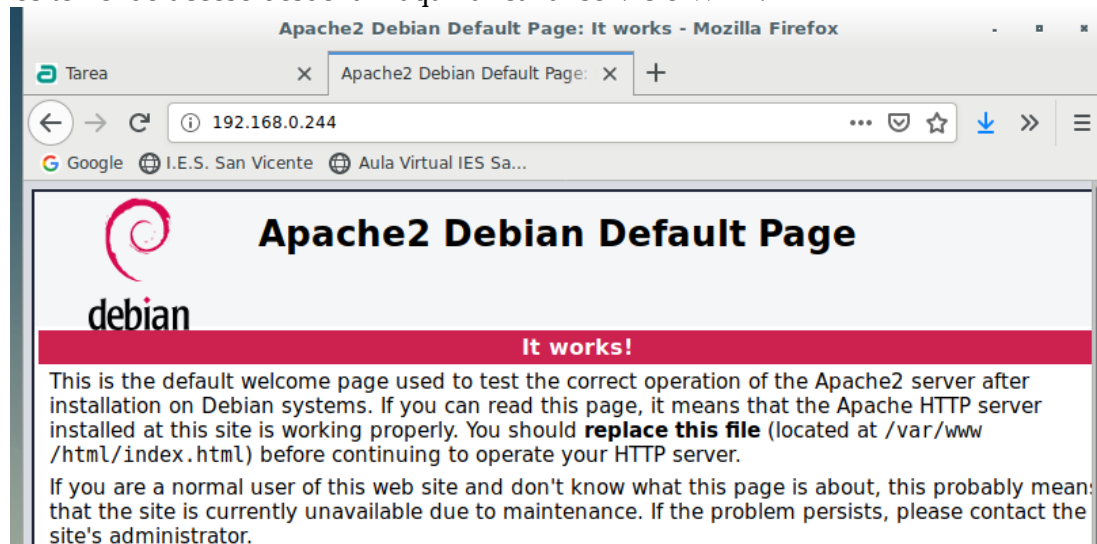


Ahora vamos a añadir una regla iptables para permitir el servicio web para toda la clase menos para un equipo específico, este será la maquina virtual llamada *Debian seguridad WEB*.

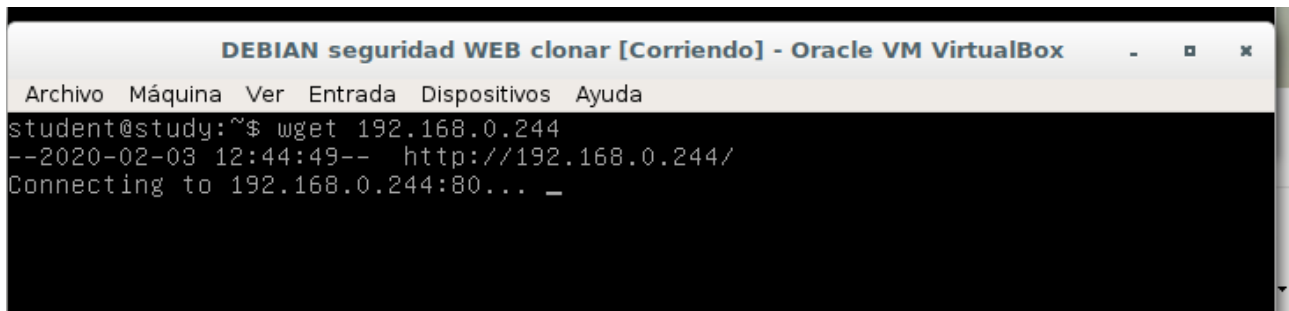
```
student@study:~$ sudo iptables -A INPUT -s 192.168.0.135 -d 192.168.0.244 -p tcp --dport 80 -j DROP
student@study:~$ sudo iptables -A INPUT -s 192.168.0.0/24 -d 192.168.0.244 -p tcp --dport 80 -j ACCEPT
```

Con estas reglas estamos denegando el acceso al servidor a el equipo con IP 192.168.0.135. A su vez estamos permitiendo el acceso al resto de la red.

Seguimos teniendo acceso desde la maquina real al servicio WEB.



Pero al intentar descargar la misma pagina desde la maquina *Debian seguridad WEB* se queda bloqueado.



```
DEBIAN seguridad WEB clonar [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
student@study:~$ wget 192.168.0.244
--2020-02-03 12:44:49-- http://192.168.0.244/
Connecting to 192.168.0.244:80... _
```

Por ultimo vamos a añadir una regla iptables para que solo un equipo con una determinada dirección MAC pueda conectarse al servidor SSH.

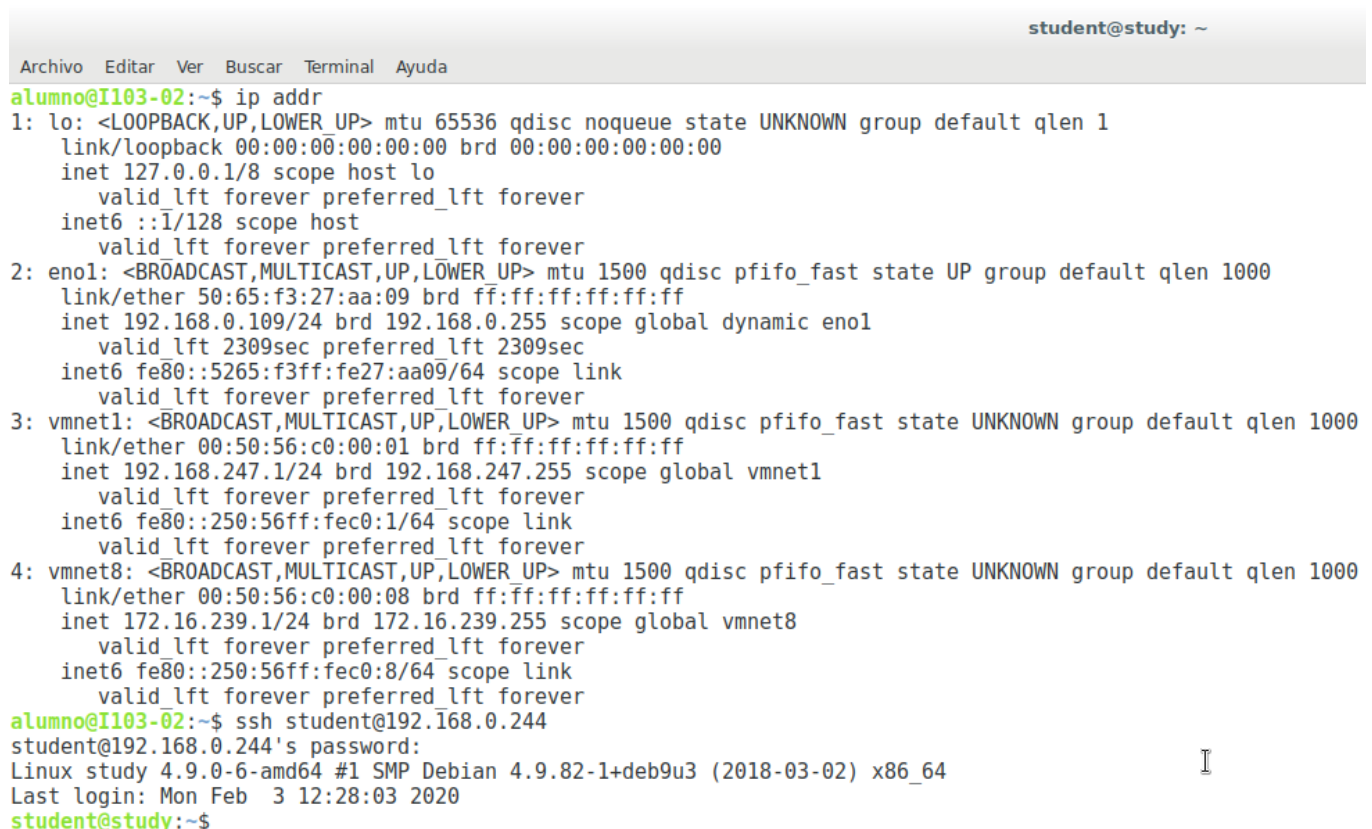
Este equipo será la maquina real I103-02.



```
student@study:~$ sudo iptables -A INPUT -m mac --mac-source 50:65:f3:27:aa:09 -d 192.168.0.244 -p tcp --dport 22 -j ACCEPT
```

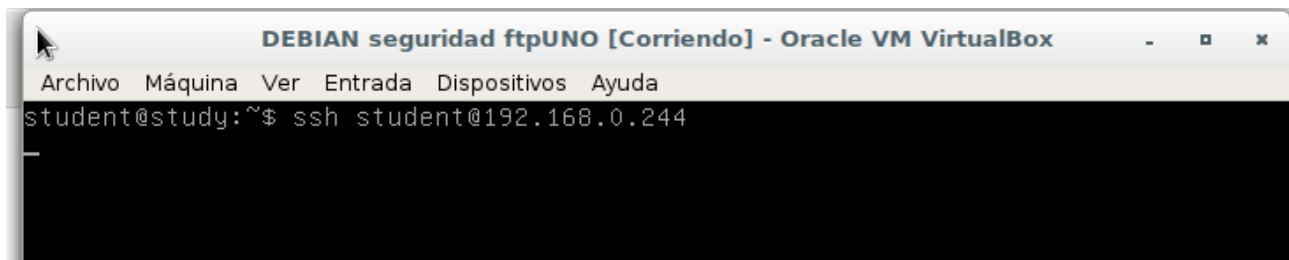
Con esta regla solo podrá acceder mediante SSH el equipo real con la MAC 50:65:f3:27:aa:09 .

Podemos establecer una conexión sin problemas mediante SSH con el servidor.



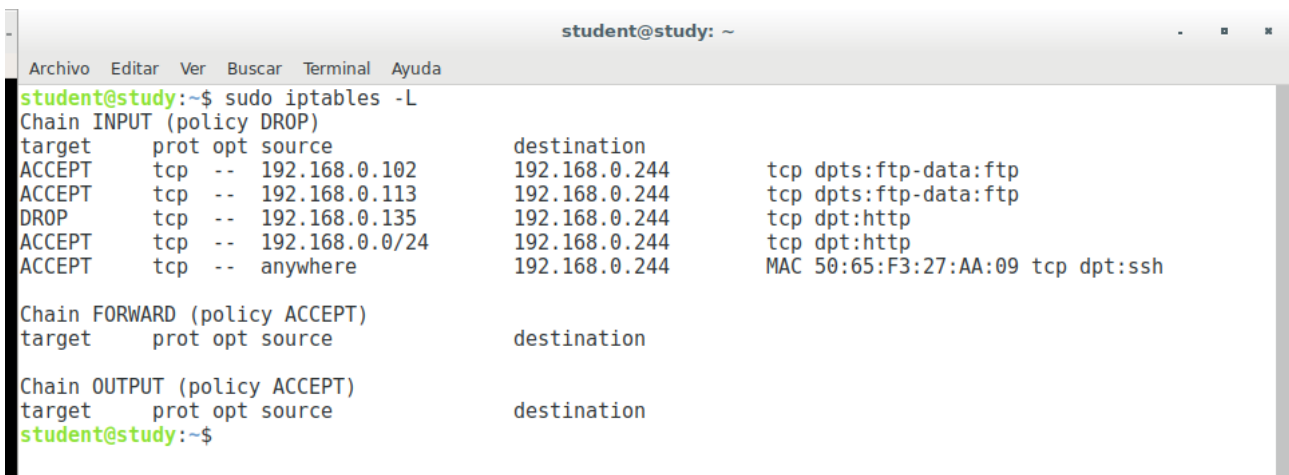
```
student@study: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
alumno@I103-02:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 50:65:f3:27:aa:09 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.109/24 brd 192.168.0.255 scope global dynamic eno1
        valid_lft 2309sec preferred_lft 2309sec
    inet6 fe80::5265:f3ff:fe27:aa09/64 scope link
        valid_lft forever preferred_lft forever
3: vmnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.247.1/24 brd 192.168.247.255 scope global vmnet1
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fec0:1/64 scope link
        valid_lft forever preferred_lft forever
4: vmnet8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:08 brd ff:ff:ff:ff:ff:ff
    inet 172.16.239.1/24 brd 172.16.239.255 scope global vmnet8
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fec0:8/64 scope link
        valid_lft forever preferred_lft forever
alumno@I103-02:~$ ssh student@192.168.0.244
student@192.168.0.244's password:
Linux study 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64
Last login: Mon Feb  3 12:28:03 2020
student@study:~$
```

En cambio si intentamos conectarnos desde las maquinas virtuales donde hemos realizado el resto de comprobaciones, simplemente, no se conectará.



```
DEBIAN seguridad ftpUNO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
student@study:~$ ssh student@192.168.0.244
```

Para finalizar esta práctica vamos a ejecutar el comando **iptables -L** para listar las reglas de iptables.



```
student@study:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination           tcp dpts:ftp-data:ftp
ACCEPT     tcp  --  192.168.0.102          192.168.0.244         tcp dpts:ftp-data:ftp
ACCEPT     tcp  --  192.168.0.113          192.168.0.244         tcp dpt:http
DROP       tcp  --  192.168.0.135          192.168.0.244         tcp dpt:http
ACCEPT     tcp  --  192.168.0.0/24         192.168.0.244         tcp dpt:http
ACCEPT     tcp  --  anywhere              192.168.0.244         MAC 50:65:F3:27:AA:09 tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
student@study:~$
```

Problemas encontrados:

Esta práctica se ha realizado sin dificultades.

Fuentes:

- <https://aules.edu.gva.es/moodle/mod/resource/view.php?id=230893>
- <https://aules.edu.gva.es/moodle/mod/resource/view.php?id=230887>
- [https://wiki.archlinux.org/index.php/Iptables_\(Espa%C3%B1ol\)](https://wiki.archlinux.org/index.php/Iptables_(Espa%C3%B1ol))
- <https://es.wikipedia.org/wiki/Netfilter>
- [https://es.wikipedia.org/wiki/Cortafuegos_\(inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica))

Alumnos participantes:

- Franco Matias Oscar Larrea