

IES Fernando Aguilar Quignon

2º ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

SEGUIMIENTO DEL CURSO IPTABLES.

José María Riol Sánchez

14 de febrero de 2023

Índice

Introducción a la tarea.	2
1. Prueba de vida.	3
1.1. Implementar un cortafuegos personal.	3

Introducción a la tarea

Vamos a seguir un curso de [Alberto Molina](#) de OpenWebinars acerca de iptables en el que llevaremos a cabo una serie de ejercicios.

El esquema que usaremos es el que tiene pensado Alberto de forma simplificada para no tener muchas máquinas con las que hacer la demostración, tendremos una DMZ con un equipo servidor que se encontrará en la red **192.168.200.0/24** y luego nuestra red local con nuestro equipo que se encontrará en la red **192.168.100.0/24**. En ambas redes tendremos un Switch para hacer más fiel la simulación, para el caso en el que hubiera más de un equipo en cada subred.

Luego nuestro Router/firewall es el que hace de firewall con 3 interfaces, una para la DMZ, otra para la red interna local y otra con el router isp actuando como firewall perimetral. Por último nuestro isp llamado router es el que estará conectado con el exterior y con nuestro firewall

El laboratorio que usaremos para hacer las prácticas se pueden encontrar en mi [GitHub](#), por si se quiere descargar y hacer uso de él y realizar los ejercicios reflejados en este documento.

Esquema.

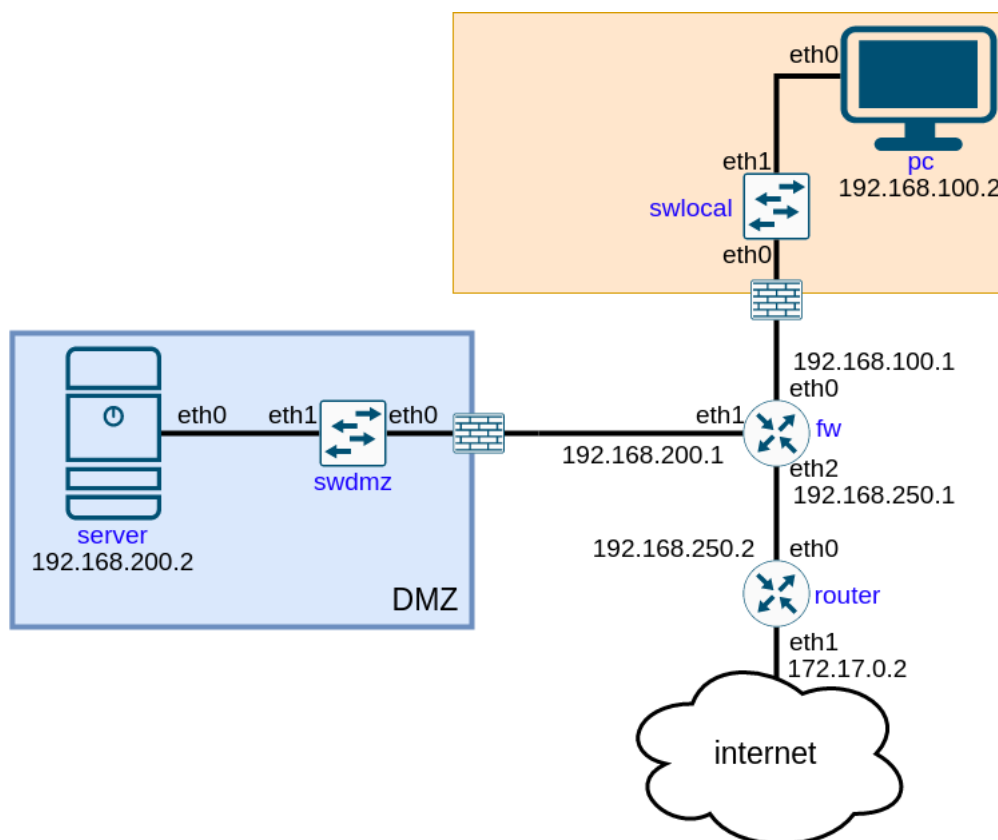


Figura 1: Esquema de la red a usar.

1. Prueba de vida.

Sintaxis de iptables MIN 11:51

1.1. Implementar un cortafuegos personal.

Probamos primero a hacer ping a un DNS (1.1.1.1) y lo hace sin problema, incluso puede navegar por la red sin problemas.

```
root@pc: /

inet 192.168.100.2 netmask 255.255.255.0 broadcast 0.0.0.0
ether 9e:50:18:0b:05:83 txqueuelen 1000 (Ethernet)
RX packets 489 bytes 415664 (405.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 604 (604.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@pc:/# ping 1.1.1.1
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=54 time=20.5 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=20.8 ms
^C
--- 1.1.1.1 ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 6ms
rtt min/avg/max/mdev = 20.463/20.617/20.771/0.154 ms
root@pc:/#
```

Figura 2: Ping al DNS.

Hacemos un curl porque no tiene GUI nuestra máquina.

```
root@pc: /

root@pc:/# curl https://openwebinars.net | head -n 40
  % Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left     Speed
  0   0   0    0    0    0     0      0      0  0  0  0  0  0  0  0  0  0  0
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="google-site-verification" content="3x1l8wvbZFWv20s_ecSG1PPw0uE11U5J9Ks2bbas"/>
<meta property="fb:pages" content="411445362304338"/>
<title>Cursos online de Programación y Sistemas en video | OpenWebinars</title>
<link rel="shortcut icon" href="/static/public/images/favicons/Favicon.ico" sizes="64x64"/>
<link rel="apple-touch-icon" sizes="57x57" href="/static/public/images/favicons/apple-icon-57x57.png, pagespeed, ic.70yMpP566m.png">
<link rel="apple-touch-icon" sizes="60x60" href="/static/public/images/favicons/apple-icon-60x60.png, pagespeed, ic.2Mu0sdKt-v.png">
<link rel="apple-touch-icon" sizes="72x72" href="/static/public/images/favicons/apple-icon-72x72.png, pagespeed, ic.0cX12U6yaF.png">
<link rel="apple-touch-icon" sizes="76x76" href="/static/public/images/favicons/apple-icon-76x76.png, pagespeed, ic.0H96G2UxLF.png">
<link rel="apple-touch-icon" sizes="114x114" href="/static/public/images/favicons/apple-icon-114x114.png, pagespeed, ic.r6hp2WpL.png">
<link rel="apple-touch-icon" sizes="120x120" href="/static/public/images/favicons/apple-icon-120x120.png, pagespeed, ic.0VXVsTsPtv.png">
<link rel="apple-touch-icon" sizes="144x144" href="/static/public/images/favicons/apple-icon-144x144.png, pagespeed, ic.Mzcew6Mskz.png">
<link rel="apple-touch-icon" sizes="152x152" href="/static/public/images/favicons/apple-icon-152x152.png, pagespeed, ic.a775KwHnKE.png">
<link rel="apple-touch-icon" sizes="180x180" href="/static/public/images/favicons/apple-icon-180x180.png, pagespeed, ic.oxc109U2mj.png">
<link rel="icon" type="image/png" sizes="192x192" href="/static/public/images/favicons/android-icon-192x192.png, pagespeed, ic.Yq1lxL07Kc.png">
<link rel="icon" type="image/png" sizes="32x32" href="/static/public/images/favicons/favicon-32x32.png, pagespeed, ic.1RfJ6u4vw4.png">
<link rel="icon" type="image/png" sizes="96x96" href="/static/public/images/favicons/favicon-96x96.png, pagespeed, ic.tH1t13X4K.png">
<link rel="icon" type="image/png" sizes="16x16" href="/static/public/images/favicons/favicon-16x16.png, pagespeed, ic.eLdn8rJyTZ.png">
<link rel="manifest" href="/static/public/images/favicons/manifest.json">
<meta name="msapplication-TileColor" content="#ffffff">
<meta name="msapplication-TileImage" content="/static/public/images/favicons/ms-icon-144x144.png">
<meta name="theme-color" content="#ffffff">
<meta name="robots" content="index, follow">
<link rel="canonical" href="https://openwebinars.net/">
<meta name="description" content="Aprende tecnología desde cero. Cursos de Ethical Hacking, Cloud Computing, Devops, Big Data, Sistemas, Programación, Frameworks y Metodologías."/>
<!-- Google Authorship and Publisher Markup -->
<link type="text/plain" rel="author" href="http://openwebinars.net/humans.txt"/>
<link rel="alternate" type="application/rss+xml" title="OpenWebinars.net &quot;Feed" href="/feed"/>
<!-- Twitter Card data -->
```

Figura 3: Puede navegar por la red.

Vemos si hay alguna regla para hacer flush o no.

```

root@pc: /
root@pc:~# iptables -L -nv
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination
root@pc:~#

```

Figura 4: Listado de reglas.

Cambiamos las iptables haciendo que no tenga conexión ninguna.

```

root@pc: /
root@pc:~# iptables -P OUTPUT DROP
root@pc:~# iptables -P INPUT DROP
root@pc:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 104ms
root@pc:~# curl https://openwebinars.net | head -n 40
% Total    % Received % Xferd  Average Speed   Time    Time     Current
   0      0    0     0    0      0     0      0  0 --:--:-- --:--:-- --:--:--    0curl: (6) Could not resolve host: openwebinars.net
root@pc:~#

```

Figura 5: Cambio en la iptables a drop dejándolo sin conexión.

Si llevamos a cabo un iptables para permitir el ping, esta vez permitirá la operación pero no tendremos respuesta, porque los paquetes que le llegan tienen la política drop entonces no los recibe.

```

root@pc: /
root@pc:~# iptables -A OUTPUT -o eth0 -p icmp -j ACCEPT
root@pc:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
^C
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 97ms

root@pc:~# iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination
    5   420 ACCEPT      icmp -- *          eth0      0.0.0.0/0    0.0.0.0/0
root@pc:~#

```

Figura 6: Hace ping pero no le llega las respuestas.

Recordemos que las reglas van por pares así que tengo que hacer otra regla INPUT que me permita tener los paquetes de vuelta sin problemas.

```
root@pc: /
root@pc:/# iptables -A INPUT -i eth0 -p icmp -j ACCEPT
root@pc:/# ping 1.1.1.1
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=54 time=18.8 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=32.1 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=20.5 ms
^C
--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 18.806/23.799/32.086/5.900 ms
root@pc:/# iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
    3   252 ACCEPT     icmp -- eth0    *            0.0.0.0/0         0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
    8   672 ACCEPT     icmp -- *      eth0    0.0.0.0/0         0.0.0.0/0
root@pc:/#
```

Figura 7: Hace ping pero no le llega las respuestas.

Es bueno observar los paquetes enviados y recibidos en la figura 6 y 7, en la figura 6 tenemos enviados 5 y recibidos ninguno y luego en la figura 7 enviados 8 y recibidos 3.

Las reglas toman la interfaz 0 como entrada/salida, si hacemos ping al 127.0.0.1 que es nuestra propia máquina volverá a ser una operación no permitida.

```
root@pc: /
root@pc:/# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 41ms
root@pc:/#
```

Figura 8: Ping interno.

Para permitirlo pondremos las reglas **iptables -A INPUT -i lo -j ACCEPT** y **iptables -A OUTPUT -o lo -j ACCEPT** siendo lo loopback.

No podríamos hacer consultas DNS como por ejemplo con dig, para ello, debemos poner también reglas que permitan ese tipo de tráfico, para ello...

```
root@pc: /

root@pc:/# iptables -A OUTPUT -o eth0 -d 8.8.8.8 -p udp --dport 53 -j ACCEPT
root@pc:/# iptables -A INPUT -i eth0 -s 8.8.8.8 -p udp --sport 53 -j ACCEPT
root@pc:/# dig @8.8.8.8 www.google.es

; <<>> DiG 9.11.5-P4-5.1+deb10u8-Debian <<>> @8.8.8.8 www.google.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47127
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.es.                IN      A

;; ANSWER SECTION:
www.google.es.                190     IN      A      172.217.17.3

;; Query time: 19 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Feb 14 11:39:37 UTC 2023
;; MSG SIZE rcvd: 58

root@pc:/#
```

Figura 9: Consulta DNS.

Seguimos sin tener tráfico web, como podremos observar.

```
root@pc: /

root@pc:/# curl https://openwebinars.net | head -n 40
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %         0         0             0             0 --:--:--  0:00:02 --:--:--  0^C
root@pc:/#
```

Figura 10: Sin tráfico web.

Por ello tenemos que añadir las reglas de ACCEPT para los puertos 80 y 443 tanto de entrada como salida.

```

root@pc: /
root@pc:/# curl https://openwebinars.net | head -n 40
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
  0     0     0     0     0     0     0 --:--:--  0:00:02 --:--:--    0^C
root@pc:/# iptables -A OUTPUT -o eth0 -p tcp --dport 80 -j ACCEPT
root@pc:/# iptables -A INPUT -i eth0 -p tcp --sport 80 -j ACCEPT
root@pc:/# curl https://openwebinars.net | head -n 40
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
  0     0     0     0     0     0     0 --:--:--  0:00:06 --:--:--    0^C
root@pc:/# iptables -A OUTPUT -o eth0 -p tcp --dport 443 -j ACCEPT
root@pc:/# iptables -A INPUT -i eth0 -p tcp --sport 443 -j ACCEPT
root@pc:/# curl https://openwebinars.net | head -n 40
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
  0     0     0     0     0     0     0 --:--:--  --:--:--  --:--:--    0
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="google-site-verification" content="3xI16rwbZFMPw20s_ecSG1PPwrQuE11U5J9Ko2bbas"/>
<meta property="fb:pages" content="411445362304338"/>
<title>Cursos online de Programación y Sistemas en vídeo | OpenWebinars</title>
<link rel="shortcut icon" href="/static/public/images/favicons/favicon.ico" sizes="64x64"/>

```

Figura 11: Con tráfico web.