

IES Valle Inclán



Enrutamiento NAT

Carlos González Martín

Contenido

1.	Primeros pasos	3
2.	Cambiar el nombre al server	3
3.	Configurar interfaces.....	4
4.	Instalar iptables	6
5.	Habilitar enrutamiento	6
6.	IPTABLES	8
7.	Script.....	9
8.	Conclusión	12

1. Primeros pasos

Deberemos tener 2 máquinas en la cual tendremos un bastión y un cliente, el cliente podemos tener tanto Windows como Linux, en el bastión sí que necesitamos un equipo Linux ya que vamos a usar las “maravillosas” iptables, también debe tener 2 interfaces de red en la cual una de ellas estará en red interna conectada al cliente y otra conectada a nuestra red local.

2. Cambiar el nombre al server

Una vez arrancado el server procederemos a cambiar el nombre al servidor y poder diferenciarlo, en este caso como solo tenemos un cliente y un server no hace mucha falta, pero cuando tengamos varias máquinas sin interfaz gráfica como es mi caso nos podremos liar si tenemos el mismo hostname

Hostnamectl set-hostname bastion

```
root@debian-12:~# hostnamectl set-hostname bastion
root@debian-12:~#

Debian GNU/Linux 12 bastion tty1

bastion login: root
Password:
Linux bastion 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) 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: Sun Sep 22 13:35:38 CEST 2024 on tty1
root@bastion:~#
```

En mi caso siempre suelo iniciar sesión con superusuario o Root, no es una práctica muy común, pero para estos pequeños casos es mucho mejor ya que así no tenemos que poner todo el rato delante del comando “sudo”.

Ahora cambiamos en el /etc/hosts el nombre que tiene la máquina, ya que a veces nos puede dar fallos la máquina, ya que el DNS interno no encuentra el nombre de la maquina que le hemos indicado anteriormente.

Nano /etc/hosts

```
GNU nano 7.2 /etc/hosts
1 127.0.0.1    localhost
2 127.0.1.1    bastion debian-12
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1         localhost ip6-localhost ip6-loopback
6 ff02::1     ip6-allnodes
7 ff02::2     ip6-allrouters
8
```

3. Configurar interfaces

Como vemos haciendo un “ip -c a”, vemos que la primera interfaz esta levantada, pero sin IP, ya que es red interna y la segunda interfaz está en modo puente y no está configurada.

Ip -c a

```
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 noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:73:59:ce brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe73:59ce/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:9f:17:a8 brd ff:ff:ff:ff:ff:ff
root@bastion:~# _
```

Una vez que hemos visto que no tenemos IPs ni conexión modificaremos el archivo de configuración de la red que está en el directorio /etc/

Nano /etc/network/interfaces

```
GNU nano 7.2 /etc/network/interfaces
1 # This file describes the network interfaces available on your system
2 # and how to activate them. For more information, see interfaces(5).
3
4 source /etc/network/interfaces.d/*
5
6 # The loopback network interface
7 auto lo
8 iface lo inet loopback
9
10 # The primary network interface
11 allow-hotplug enp0s3 enp0s8
12 iface enp0s3 inet static
13     address 192.168.10.224
14     netmask 255.255.255.0
15
16 # The second network interface
17 iface enp0s8 inet dhcp
18
19
```

Ahora reiniciamos el servicio, podemos reiniciar la maquina o reiniciar el servicio y levantar los interfaces.

Service networking restart ; ifup enp0s3 ; ifup enp0s8

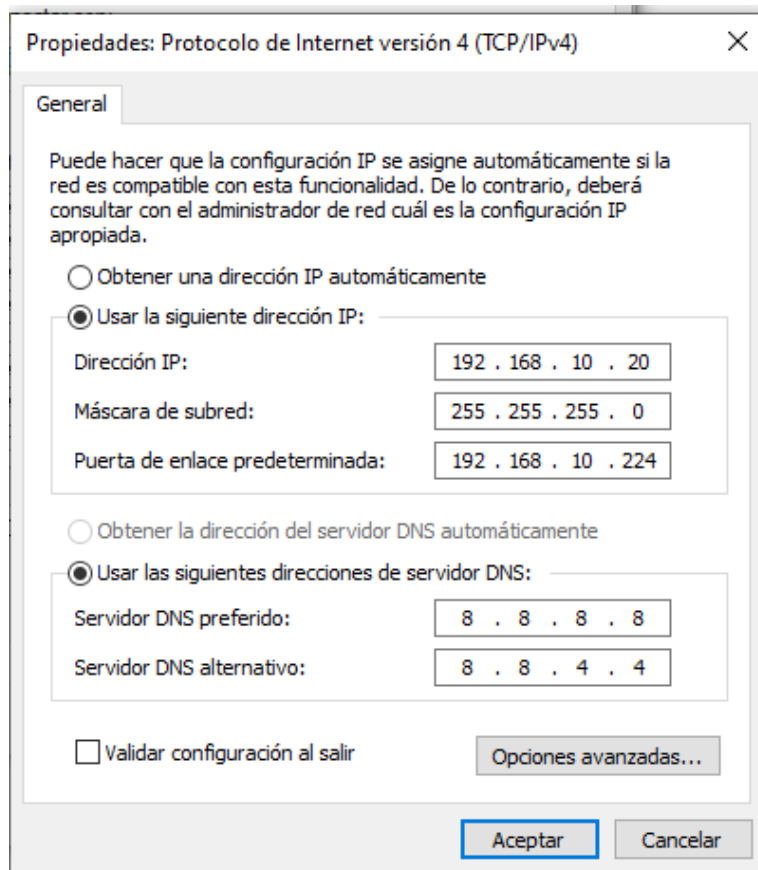
```
root@bastion:~# service networking restart ; ifup enp0s3 ; ifup enp0s8
ifup: interface enp0s3 already configured
ifup: interface enp0s8 already configured
```

Ahora con un “ip -c a” revisamos si se han levantado los servicios y tienen las direcciones IP correctas.

Ip -c a

```
root@bastion:~# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:73:59:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.224/24 brd 192.168.10.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe73:59ce/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9f:17:a0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.185/24 brd 192.168.1.255 scope global dynamic enp0s8
        valid_lft 86398sec preferred_lft 86398sec
    inet6 2a0c:5a80:5508:6200:a00:27ff:fe9f:17a0/64 scope global dynamic mngtmpaddr
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9f:17a0/64 scope link
        valid_lft forever preferred_lft forever
root@bastion:~#
```

Una vez que hemos cambiado las IP al server vamos a cambiárselo al cliente.



Importante cambiar los DNS preferido para poder comunicarnos con el exterior.

4. Instalar iptables

Ahora lo que haremos será comprobar si podemos descargar el paquete iptables, para ello usaremos el comando “APT update”.

Apt update

```
root@bastion:~# apt update
Obj:1 http://deb.debian.org/debian bookworm InRelease
Des:2 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Des:3 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Des:4 http://security.debian.org/debian-security bookworm-security/main Sources [111 kB]
Des:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [182 kB]
Des:6 http://security.debian.org/debian-security bookworm-security/main Translation-en [111 kB]
Descargados 507 kB en 0s (1.053 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se puede actualizar 1 paquete. Ejecute «apt list --upgradable» para verlo.
root@bastion:~# _
```

Una vez que vemos que tenemos conexión a internet procederemos a instalar iptables.

Apt install iptables

```
root@bastion:~# apt install iptables
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libip6tc2 libnetfilter-conntrack3 libnfnctlink0
Paquetes sugeridos:
  firewallld
Se instalarán los siguientes paquetes NUEVOS:
  iptables libip6tc2 libnetfilter-conntrack3 libnfnctlink0
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 435 kB de archivos.
Se utilizarán 2.728 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://deb.debian.org/debian bookworm/main amd64 libip6tc2 amd64 1.8.9-2 [19,4 kB]
Des:2 http://deb.debian.org/debian bookworm/main amd64 libnfnctlink0 amd64 1.0.2-2 [15,1 kB]
Des:3 http://deb.debian.org/debian bookworm/main amd64 libnetfilter-conntrack3 amd64 1.0.9-3 [40,7 kB]
Des:4 http://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
Descargados 435 kB en 0s (8.648 kB/s)
```

5. Habilitar enrutamiento

Una vez que hemos instalado el paquete iptables podremos ya configurar todas las reglas iptables.

Echo “1” > /proc/sys/net/ipv4/ip_forward

```
root@bastion:~# echo "1" > /proc/sys/net/ipv4/ip_forward
root@bastion:~# cat /proc/sys/net/ipv4/ip_forward
1
root@bastion:~#
```

Ahora modificamos la línea 28 del siguiente archivo de configuración.

Nano /etc/sysctl.conf

```

21
22 # Uncomment the next line to enable TCP/IP SYN cookies
23 # See http://lwn.net/Articles/277146/
24 # Note: This may impact IPv6 TCP sessions too
25 #net.ipv4.tcp_syncookies=1
26
27 # Uncomment the next line to enable packet forwarding for IPv4
28 net.ipv4.ip_forward=1
29
30 # Uncomment the next line to enable packet forwarding for IPv6
31 # Enabling this option disables Stateless Address Autoconfiguration
32 # based on Router Advertisements for this host
33 #net.ipv6.conf.all.forwarding=1
34

```

Y aplicamos el cambio.

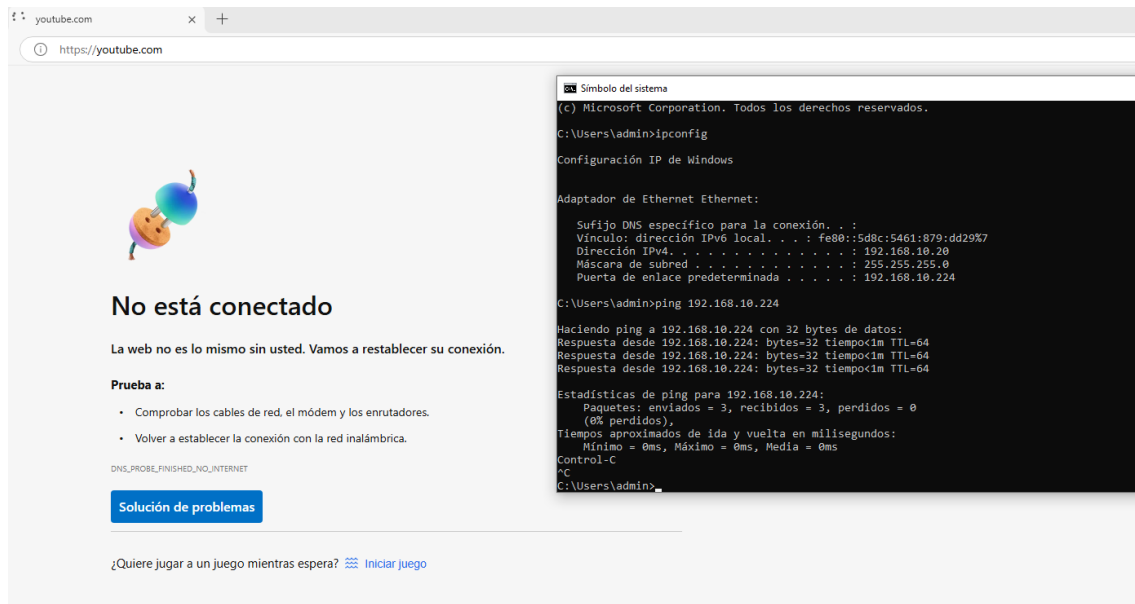
Sysctl -p

```

root@bastion:~# sysctl -p
net.ipv4.ip_forward = 1
root@bastion:~#

```

Si probamos por como lo tenemos ahora no podremos conectarnos, pero si podremos hacer ping entre las dos máquinas.



The screenshot shows a Windows desktop. On the left, a web browser window displays a 'No está conectado' (Not connected) error message from YouTube, indicating that the network connection is not working. On the right, a command prompt window is open, showing the IP configuration for the 'Ethernet' adapter. The configuration includes the IPv4 address 192.168.10.20, subnet mask 255.255.255.0, and default gateway 192.168.10.224. Below the configuration, the command prompt shows the results of a ping command to 192.168.10.224, which is successful, with 3 bytes of data received and 0% loss.

6. IPTABLES

Ahora configuraremos las iptables.

```
Iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
Iptables -A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT
Iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
root@bastion:~# iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
root@bastion:~# iptables -A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT
root@bastion:~# iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
root@bastion:~# _
```

Ahora veremos si se ha configurado las iptables correctamente.

Iptables -L

```
root@bastion:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@bastion:~# _
```

Una vez puesta las reglas podremos cargar la página web de YouTube sin problema alguno.

The screenshot shows a web browser window with the URL <https://www.youtube.com/watch?v=yukkp3m1YqQ>. The video player shows a scene with two turkeys in a grassy field. A terminal window is overlaid on the right side of the browser, displaying the following output:

```
C:\Users\admin>ping 192.168.10.224

Haciendo ping a 192.168.10.224 con 32 bytes de datos:
Respuesta desde 192.168.10.224: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.224: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.224: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.10.224:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\admin>ping 192.168.10.224

Haciendo ping a 192.168.10.224 con 32 bytes de datos:
Respuesta desde 192.168.10.224: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.224: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.10.224: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.10.224: bytes=32 tiempo=3ms TTL=64

Estadísticas de ping para 192.168.10.224:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 3ms, Media = 1ms
C:\Users\admin>
```


7. Script

Ahora lo que haremos será poner las reglas de iptables en un script para que cuando arranquemos la maquina solo tengamos que ejecutar una instrucción.

Nano script.sh

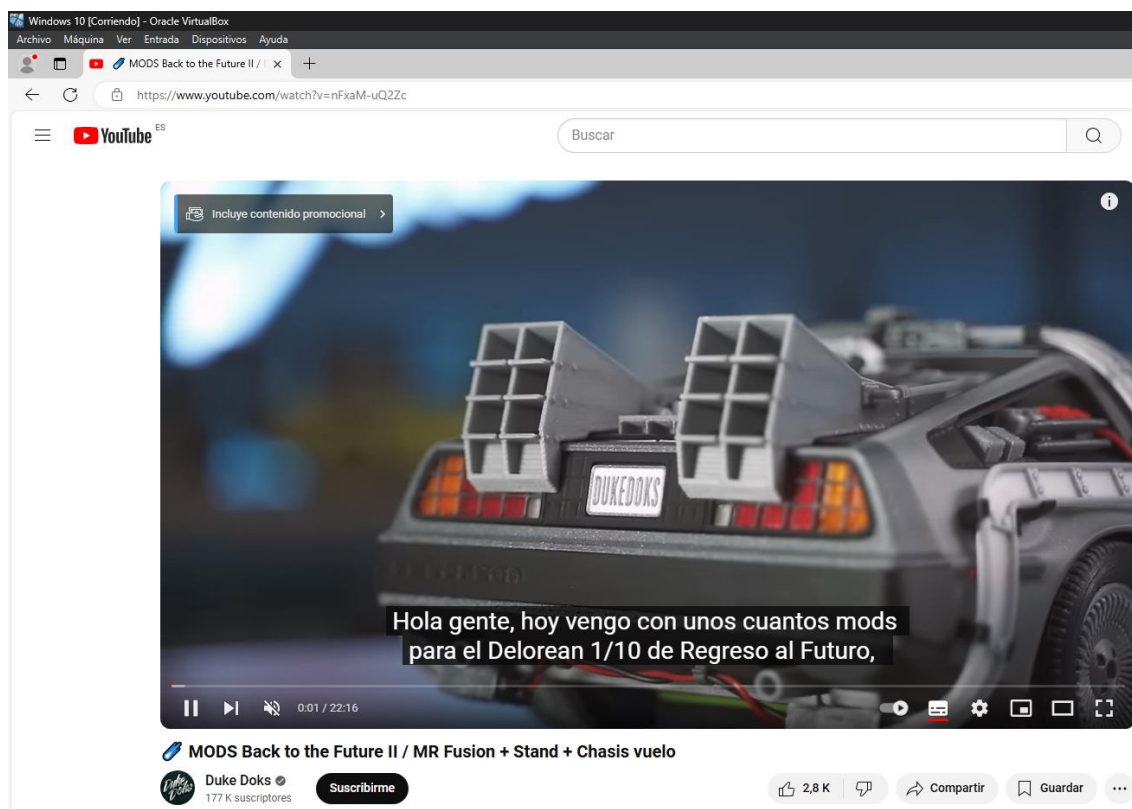
```
GNU nano 7.2 script.sh
1 #!/bin/bash
2
3 echo "1" > /proc/sys/net/ipv4/ip_forward
4
5 iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
6 iptables -A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT
7 iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
8
```

Ahora lo que haremos será dar permisos de ejecución al grupo otros, ya que ese grupo pertenece en una parte al sistema, ya que vamos a tocar parámetros del sistema.

Chmod o+x script.sh

```
root@bastion:/home/usuario# chmod o+x script.sh
root@bastion:/home/usuario# ls -la
total 32
drwx----- 3 usuario usuario 4096 sep 29 15:29 .
drwxr-xr-x 3 root    root    4096 sep 11 12:04 ..
-rw----- 1 usuario usuario  12 sep 17 10:02 .bash_history
-rwxrwx--- 1 usuario usuario  220 sep 25  2021 .bash_logout
-rwxrwx--- 1 usuario usuario 3525 sep 25  2021 .bashrc
drwxr-xr-x 3 usuario usuario 4096 sep 16 10:10 .local
-rwxrwx--- 1 usuario usuario  807 sep 25  2021 .profile
-rw-r--r-x 1 root    root    247 sep 29 15:29 script.sh
root@bastion:/home/usuario# _
```

Y ahora ejecutaremos el script y probaremos si las reglas de iptables se configuran correctamente.



Ahora haremos que se inicie el script nada más arranque la máquina.

Nano /etc/systemd/system/autorun.service

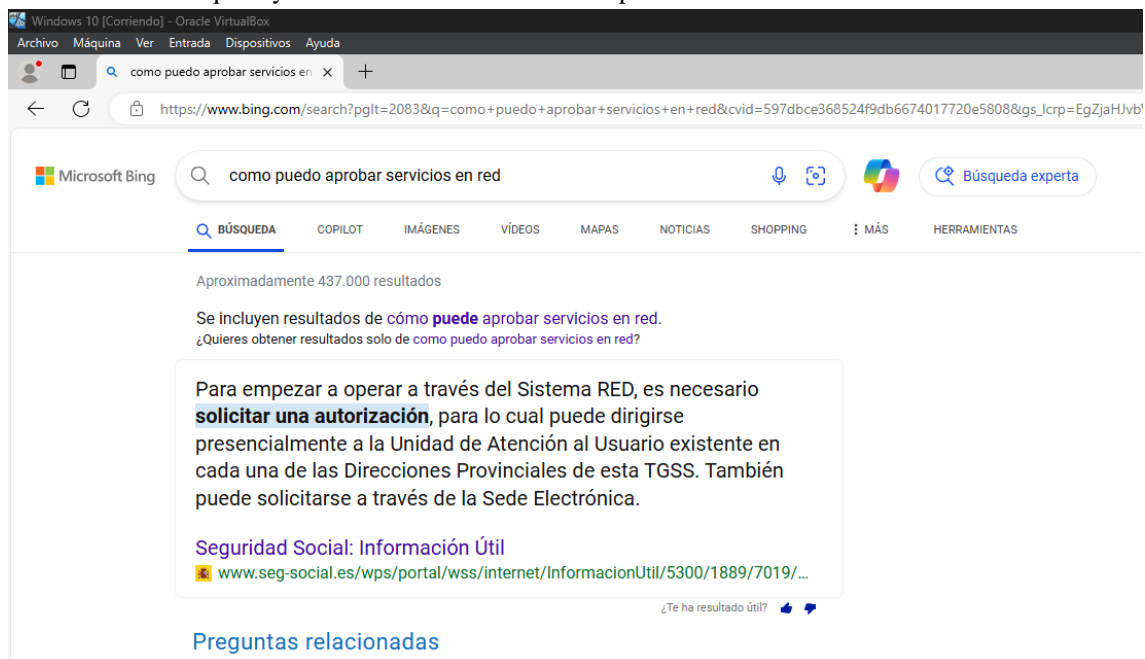
```
GNU nano 7.2 /etc/systemd/system/autorun.service
1 [Unit]
2 Description=IPTABLES
3 After=Network.target
4 [Service]
5 ExecStart=/home/usuario/script.sh
6 [Install]
7 WantedBy=default.target
8
```

Escribiremos lo siguientes comandos para indicar que tiene que arrancar el archivo.

Systemctl Daemon-reload
Systemctl enable autorun.service
Systemctl start autorun.service

```
root@bastion:~# systemctl daemon-reload
root@bastion:~# systemctl enable autorun.service
root@bastion:~# systemctl start autorun.service
root@bastion:~# _
```

Reiniciamos la maquina y sin iniciar sesión vamos a comprobar si funciona.



Como cosa extra hemos puesto los siguientes comandos, para que cuando inicie la maquina modifique el archivo /etc/issue, que es el encargado de que podamos ver el nombre de la máquina, el tty..., modificar y también poner el “iptables activadas”, si hacíamos solo el ultimo comando al final de varios días de apagar y encender la maquina nos saldrían muchos más y al final no sabríamos si esta activado o no.

Nano /home/usuario/script.sh

```
GNU nano 7.2 /home/usuario/script.sh
1 #!/bin/bash
2
3
4 echo "1" > /proc/sys/net/ipv4/ip_forward
5
6 iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
7 iptables -A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT
8 iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
9
10
11 echo "Debian \n \1 \4" > /etc/issue
12 echo "iptables activadas" >> /etc/issue
13
```

Reiniciamos la maquina para ver si se ha configurado correctamente el archivo /etc/issue.

```
Debian bastion tty1 192.168.10.224
iptables activadas
bastion login: _
```

8. Conclusión

Para esta práctica hemos aprendido como hacer un enrutamiento entre 2 interfaces, esto viene bien para cuando tenemos otras reglas de iptables y hacer una “DMZ” salvando las distancias y poder separar los equipos más vulnerables y no tener hackeos