

Configuración de enrutamiento para la red corporativa

Vamos a habilitar el enrutamiento y el enmascaramiento NAT de trafico proveniente de la red corporativa hacia internet; para ello debemos establecer reglas de reenviado de trafico entre interfaces y reglas de enmascaramiento nat en el cortafuegos iptables de “servidor-planetas”.

Instalación de iptables

En primer lugar instalamos iptables en “servidor-planetas” mediante el comando:

```
apt install iptables
```

Habilitar reenviado de paquetes

Ahora habilitamos el reenviado de paquetes modificando el archivo “/etc/sysctl.conf” y descomentamos la linea “net.ipv4.ip_forward=1”

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Añadir reglas de enmascaramiento y reenviado de paquetes

Posteriormente añadimos las reglas de enmascaramiento y de reenviado teniendo en cuenta que la interfaz que tiene acceso a internet es la “eno1” y la interfaz a la que queremos proporcionar servicio de enrutamiento es la “enp3s0” mediante los siguientes comandos:

```
iptables -A FORWARD -i enp3s0 -o eno1 -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -o eno1 -j MASQUERADE
```

```
[root@servidor-planetas:/home/admin-servidor# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A FORWARD -i enp3s0 -o eno1 -j ACCEPT
[root@servidor-planetas:/home/admin-servidor# iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-A POSTROUTING -o eno1 -j MASQUERADE
```

Reglas establecidas.

Instalación de “iptables-persistent” para la persistencia de las reglas

Para hacerlas persistentes debemos instalar el paquete “iptables-persistent”; procedemos a instalarlo mediante el comando:

```
apt install iptables-persistent
```

Ahora procederemos a comprobar la persistencia de las reglas tras un reinicio

```
no vm guests are running outdated hypervisor (qemu) binaries  
root@servidor-planetas:/home/admin-servidor# reboot -h now
```

```
[root@servidor-planetas:/home/admin-servidor# iptables -S  
-P INPUT ACCEPT  
-P FORWARD ACCEPT  
-P OUTPUT ACCEPT  
-A FORWARD -i enp3s0 -o eno1 -j ACCEPT  
[root@servidor-planetas:/home/admin-servidor# iptables -S -t nat  
-P PREROUTING ACCEPT  
-P INPUT ACCEPT  
-P OUTPUT ACCEPT  
-P POSTROUTING ACCEPT  
-A POSTROUTING -o eno1 -j MASQUERADE
```

Las reglas persisten tras el reinicio

Pruebas de conectividad en “equipo-cliente”

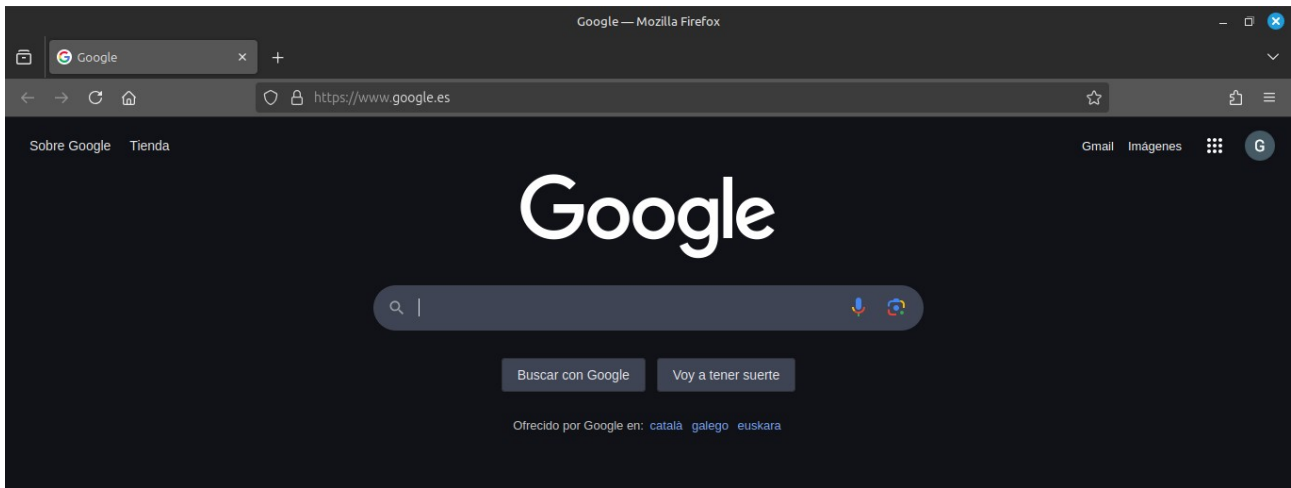
Comprobamos que “equipo-cliente” se encuentra dentro de la red corporativa y que todas sus demas interfaces de red no estan activas

```
guillermo@equipo-cliente:~$ ip 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: enp2s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000  
    link/ether b8:88:e3:c3:a1:11 brd ff:ff:ff:ff:ff:ff  
    inet 172.20.0.20/26 brd 172.20.0.63 scope global dynamic noprefixroute enp2s0f0  
        valid lft 538sec preferred lft 538sec  
    inet6 fe80::7c1c:af0:3bc4:ae83/64 scope link noprefixroute  
        valid lft forever preferred lft forever  
3: wlp3s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000  
    link/ether 1c:4d:70:01:f3:7e brd ff:ff:ff:ff:ff:ff
```

Tras esta comprobación hacemos ping a un sitio web alojado en internet como google.com

```
guillermo@equipo-cliente:~$ ping google.es  
PING google.es (142.250.184.163) 56(84) bytes of data.  
64 bytes from mad07s23-in-f3.1e100.net (142.250.184.163): icmp_seq=1 ttl=116 time=3.23 ms  
64 bytes from mad07s23-in-f3.1e100.net (142.250.184.163): icmp_seq=2 ttl=116 time=3.23 ms  
64 bytes from mad07s23-in-f3.1e100.net (142.250.184.163): icmp_seq=3 ttl=116 time=3.11 ms  
^C  
--- google.es ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 3.105/3.185/3.226/0.057 ms
```

Obtenemos respuesta, procedemos a corroborar el acceso a internet mediante el uso de navegador



La red corporativa ya tiene acceso a internet