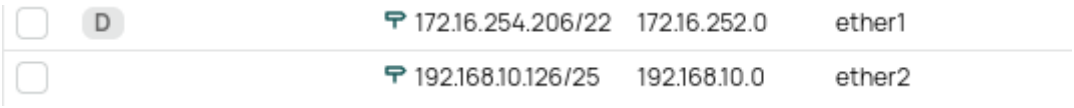
Compte rendu TP NAT sortant avec routeur virtuel

Interfaces:



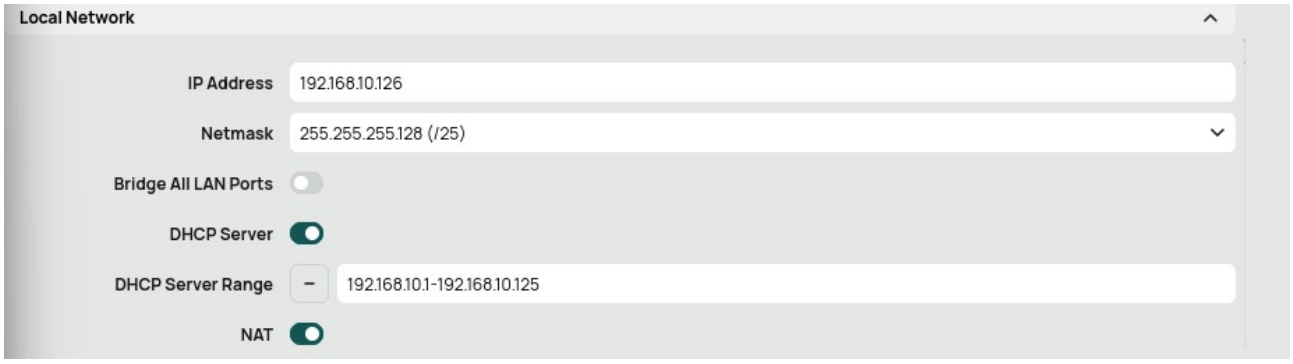
Client Debian :
→ IP dynamique 102.168.10.2 passerelle 192.168.10.126

Règle NAT :

Test d'accès à Internet :

```
user@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=20.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=20.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=20.2 ms
```

Serveur DHCP :
↘ Configuré sur ether2.



Test du serveur DHCP depuis un autre client

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mt
    link/ether 08:00:27:c4:76:18 brd ff:ff:ff:
    altname enx080027c47618
    inet 192.168.10.124/25 brd 192.168.10.127
```

→ Le serveur DHCP distribue bien une IP comprise entre .1 et .125 à mon client.

Vérification par capture :

Côté client :

```
11:11:41.855783 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 38, length 64
11:11:41.881759 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 38, length 64
11:11:42.860670 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 39, length 64
11:11:42.881185 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 39, length 64
11:11:43.866468 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 40, length 64
11:11:43.893539 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 40, length 64
11:11:44.871839 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 41, length 64
11:11:44.899742 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 41, length 64
11:11:45.876933 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 42, length 64
11:11:45.898637 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 42, length 64
11:11:46.882551 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 43, length 64
11:11:46.902716 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 43, length 64
11:11:47.896177 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 44, length 64
11:11:47.926385 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 44, length 64
11:11:48.897894 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 45, length 64
11:11:48.930466 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 45, length 64
11:11:49.900780 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 46, length 64
11:11:49.929181 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 46, length 64
11:11:50.906469 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 47, length 64
11:11:50.938027 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 47, length 64
11:11:51.913731 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 48, length 64
11:11:52.928787 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 49, length 64
11:11:52.952841 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 49, length 64
11:11:53.938297 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 50, length 64
11:11:53.956491 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 50, length 64
11:11:54.947354 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 51, length 64
11:11:54.966372 IP 8.8.8.8 > 192.168.10.2: ICMP echo reply, id 2, seq 51, length 64
11:11:55.948563 IP 192.168.10.2 > 8.8.8.8: ICMP echo request, id 2, seq 52, length 64
```

Côté hôte :

```
91 3.429816    172.16.254.206    8.8.8.8           ICMP    98 Echo (ping) request  id=0x0002, seq=35/8960, ttl=63 (reply in 92)
92 3.455072    8.8.8.8           172.16.254.206    ICMP    98 Echo (ping) reply    id=0x0002, seq=35/8960, ttl=112 (request in 91)
```

Côté LAN (tcpdump)	Côté WAN (Wireshark)	Interprétation
Source = 192.168.10.2	Source = 172.16.254.206	Le routeur a remplacé l'IP LAN par son IP WAN
Destination = 8.8.8.8	Destination = 8.8.8.8	La destination reste identique

On voit que le routeur a bien appliqué la règle NAT sortant et remplace l'IP 192.168.10.2 par 172.16.254.206.

BONUS :

Règles du firewall :

#	Comment	Action	Chain	Src. Addr...	Dst. Addr...	Src. A...	Dst. A...	Pro...	Src. Port	Dst. Port	Any. Port	In. Int...	Out. I...
0	Bloquer accès W...	drop	forward									ether1	ether2
1	Autoriser ssh dep...	accept	input					tcp		22		ether1	
2	Bloquer accès htt...	drop	input					tcp		80		ether1	
3	Bloquer accès htt...	drop	input					tcp		443		ether1	
4	Bloquer tout le re...	drop	input									ether1	

Test accès ssh depuis le wan :

Test accès au routeur depuis le wan :