NAT et Filtrage sous linux

Adressage: PC2: 10.203.0.116 Routeur, réseau de la salle: 10.203.0.194 Routeur, réseau privé: 192.168.1.254 Serveur Web: PC1:

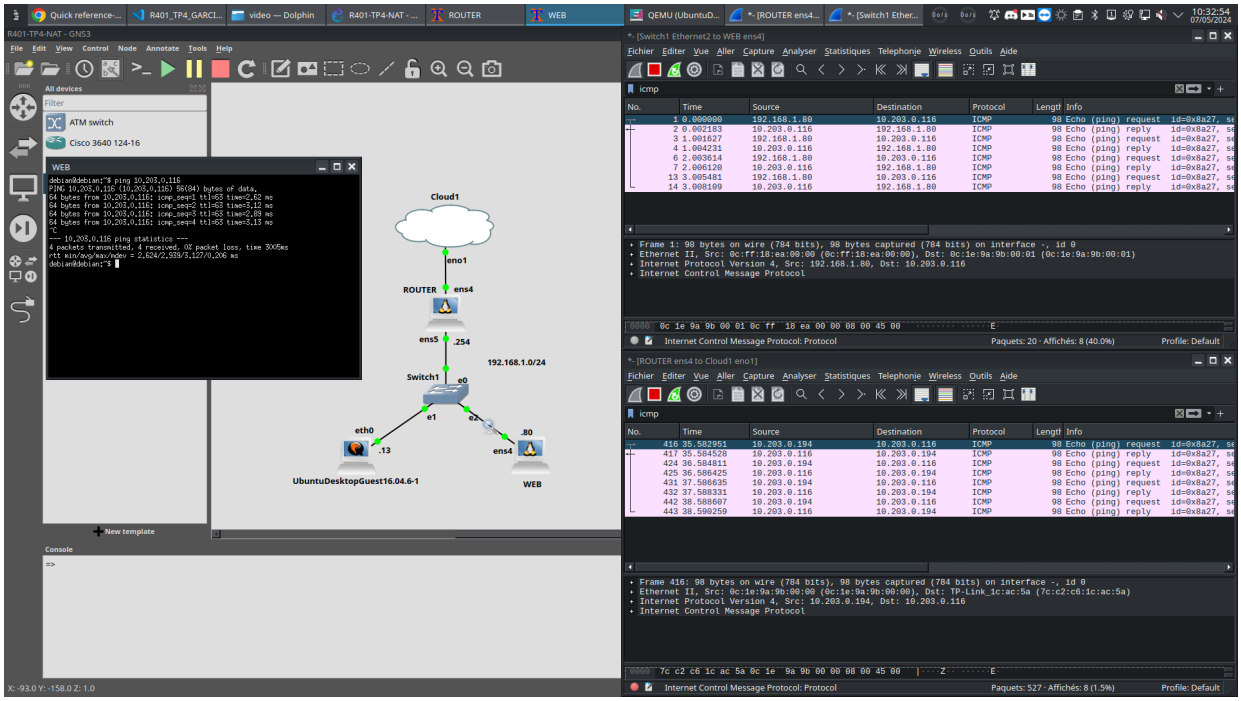
1. Le NAT

1.1 SNAT

1. Le SNAT doit être sur le hook PostRouting, ceci est une action sur la sorti d'interface.
2. Voici les commandes

```
nft add table nat
nft add chain nat natexterne {type nat hook postrouting priority 0 \;}
nft add rule nat natexterne ip saddr 192.168.1.0/24 oif ens4 snat 10.203.0.194
```

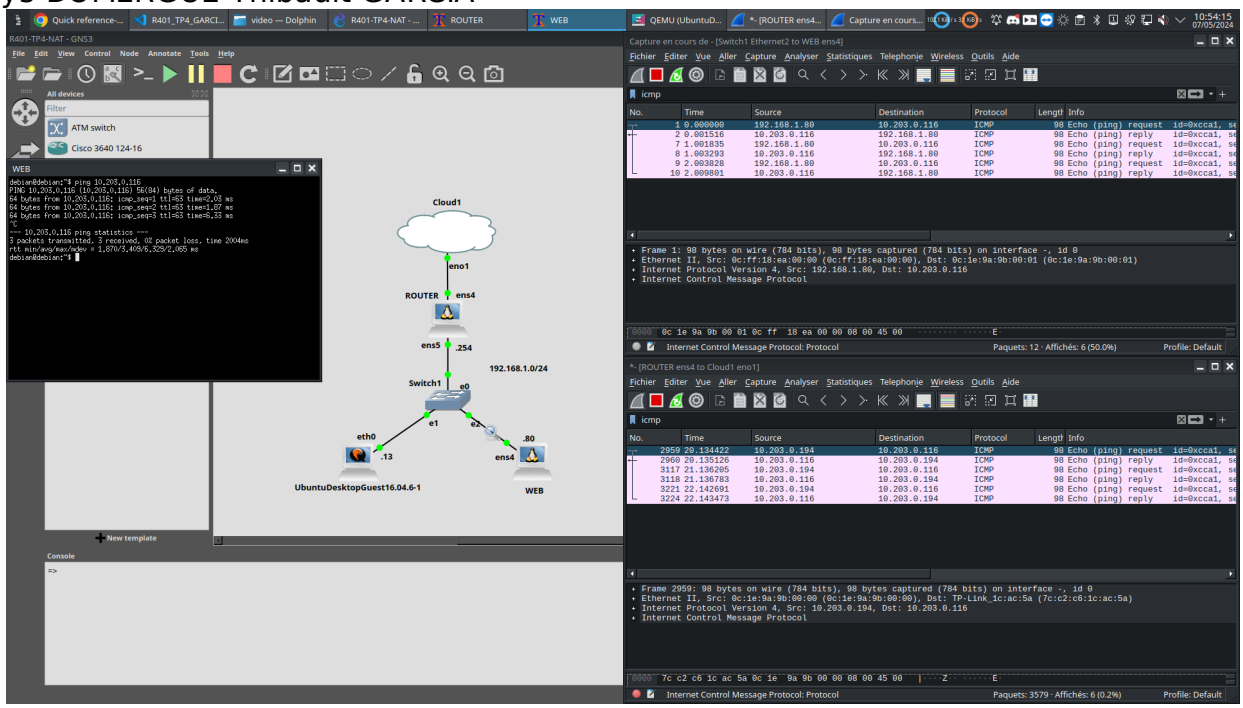
3. On peut effectuer un ping, voici le résultat:



1.2 MASQUERADE

4. Voici les commandes à mettre, et la preuve avec le ping:

```
nft -n -a list table nat #permet de lister la table de nat avec le numéro de handle, c'est mieux que nft list ruleset.
nft delete rule nat natexterne handle 11 #handle est la position de la règle.
nft add rule nat natexterne masquerade
```

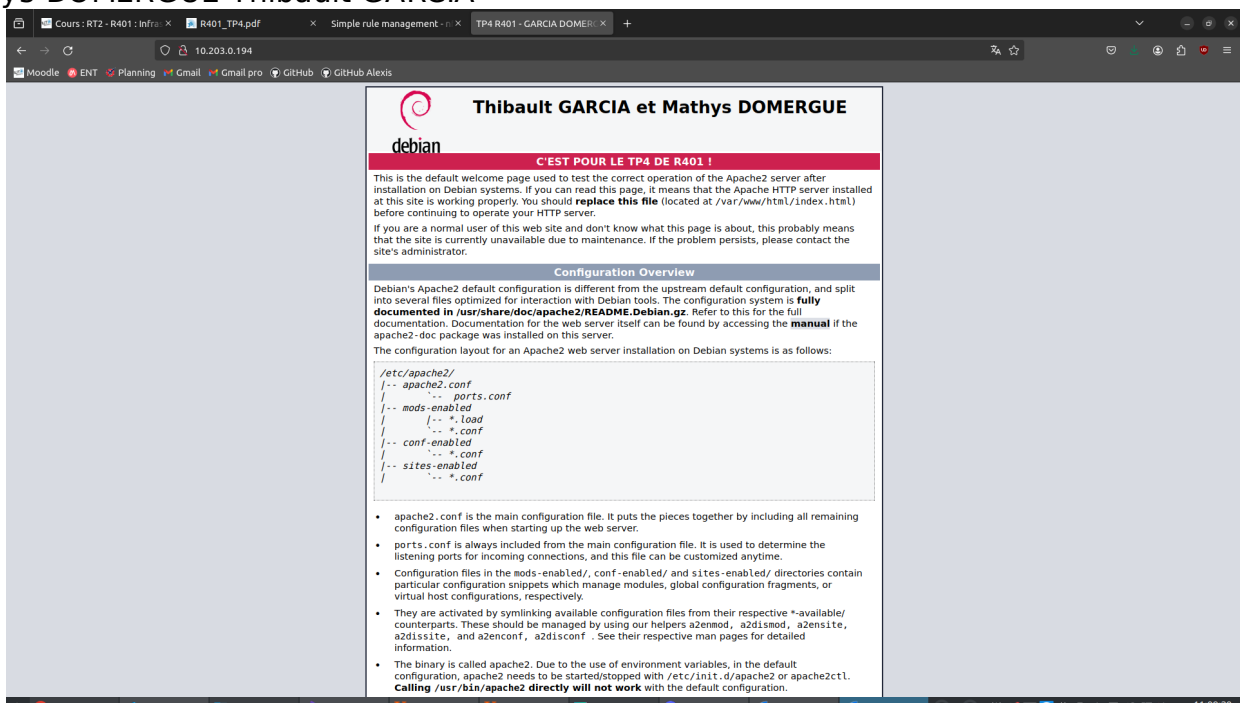
1.3 DNAT

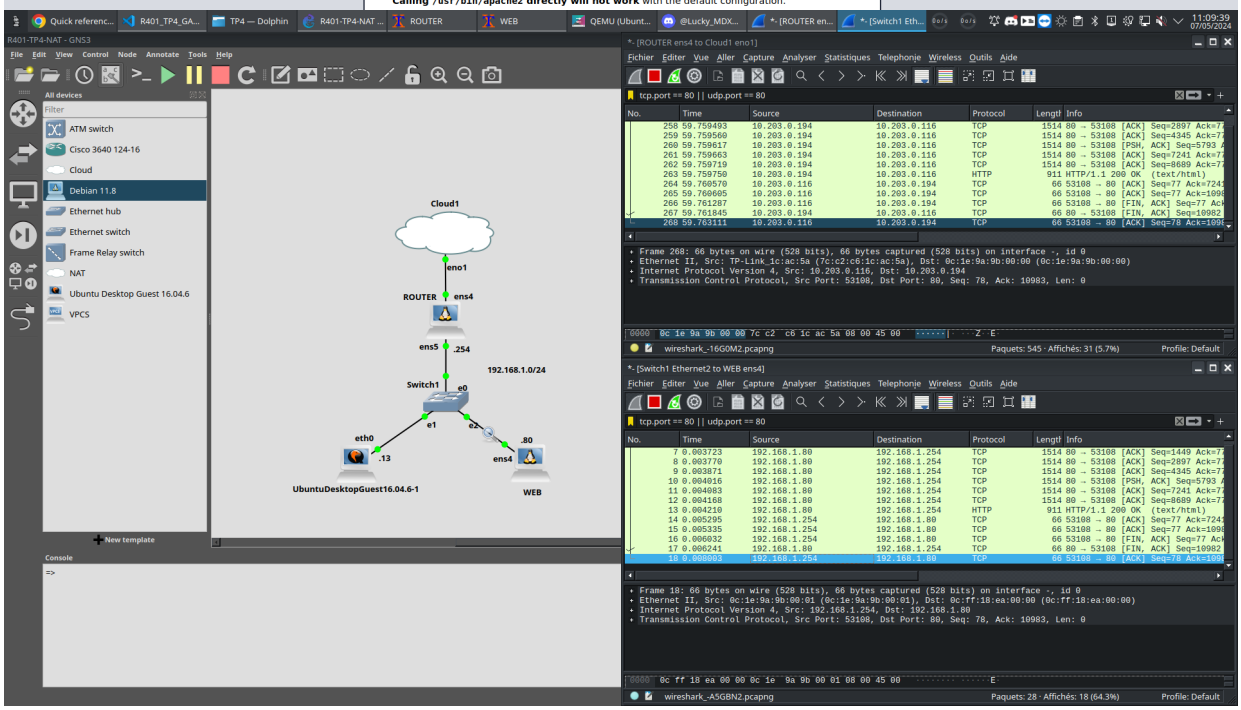
5. La règle de DNAT se place sur le hook du prerooting.

6. Voici les règles utilisées:

```
nft nft add chain nat dstnat {type nat hook prerouting priority 0 \;}
nft add rule ip nat dstnat iif ens4 tcp dport 80 dnat 192.168.1.80:80
```

7. Voici la page du serveur web depuis le PC2:





2. Filtrage

2.1 Sans état: Stateless

8. Voici la règle utilisée:

```
nft add rule filter refus ip daddr 141.94.78.218 drop
```

La limite des cette méthode est les grosses structures comme Youtube ou Facebook, avec beaucoup de serveurs.

9. Voici le filtre

```
nft add rule filter refus iif ens5 tcp dport 22 reject
```


10. Par default, il vaut mieux de mettre une table en drop puis d'ajouter les règles une par une.

11. Voici les commandes passés:

```
nft add rule filter OUTPUT icmp type echo-request reject
nft add rule filter OUTPUT icmp type echo-request drop
```

12. Voici les commandes:

```
nft add rule filter FORWARD icmp type echo-request accept  // Pour ping
l'Internet
nft add rule filter FORWARD icmp type echo-reply accept    // Pour ping
l'Internet
nft add rule filter INPUT icmp type echo-request accept    // Pour ping le
Router
nft add rule filter INPUT icmp type echo-reply accept      // Pour ping le
Router
nft add rule filter INPUT tcp dport 22 ip saddr 192.168.1.0/24 accept // accept
le SSH du LAN
nft add rule filter FORWARD tcp dport 80 accept // accept les acces WEB http
nft add rule filter FORWARD tcp dport 443 accept // accept les acces WEB https
(On va plus loin que la question)
drop
```

2.2 Avec état: Satefull

13. Voici l'option à utiliser :

```
ct state
```

14. Voici les commandes :

```
nft add rule filter FORWARD tcp dport 22 daddr 192.168.1.0/24 ct state
established accept // Autorise les réponses ssh
( tcp port 22 )

nft add rule filter FORWARD tcp dport 22 saddr 192.168.1.0/24 ct state new
accept // Pour qu'il y est established, il faut
un new (donc que le LAN puisse initier une connexion)
```

15.

```
nft add rule filter FORWARD tcp dport 22 daddr 192.168.1.0/24 ct state
established accept // Autorise les réponses ssh
( tcp port 22 )

nft add rule filter FORWARD tcp dport 22 saddr 192.168.1.0/24 ct state new
accept // Pour qu'il y est established, il faut
un new (donc que le LAN puisse initier une connexion)
```

16.


```
nft add rule filter FORWARD counter tcp dport 80 ct state new accept
```

17.

```
nft list counters
```