TP NAT - SERPOLLET - VALETTE

Created	@13 avril 2022 15:15
Class	NE372
Type	TP
Materials	

1 - Routage

- Le routage est actif sur le firewall, en effet on arrive à ping les clients depuis le firewall.
- Il n'y avait pas de route par défaut. On ajoute donc le firewall en route par defaut sur les clients et le routeur FAI pour le firewall.

Le firewall et les clients peuvent communiquer entre eux (ils sont sur le même réseau). Le serveur cache ne peut pas communiquer car il est en DMZ.

Les clients peuvent accéder au router FAI et donc à internet mais ils ne peuvent pas recevoir de réponses. Avec un ping on obtient donc que tous les paquets sont perdus mais au moins on a pas "host unreachable".

2 - Translation d'adresse

On utilise nft pour créer une table nat et dedans on crée une chaine de postrouting :

```
nft add table nat
nft 'add chain nat postrouting { type nat hook postrouting priority 100 ; }'
```

Puis on ajoute les règles de masquerade pour les client 1 et 3, ainsi qu'une règle de translation pour le client 2 :

```
nft add rule nat postrouting ip saddr 192.168.100.1 oif eth0 masquerade
nft add rule nat postrouting ip saddr 192.168.100.3 oif eth0 masquerade
nft add rule nat postrouting ip saddr 192.168.100.2 oif eth0 snat to 193.23.23.2
```

Il reste un problème, le client 2 envois des requêtes avec une adresse IP qui ne correspond à rien. Il faut donc configurer le firewall pour répondre. On utilise donc un proxy arp.

```
echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy_arp_pvlan
```

Nous ping-ons depuis le client 1 et 3 www.monsite.fr et au debut rien ne marche (😑), il faut penser à modifier le /etc/resolv.conf et aussi rajouter le serveur FAI dans la gateway du serveur HTTP et le firewall en gateway du serveur cache.

Après ces modifications tout fonctionne de manière nominale.

Les paquets icmp arrivent sur le serveur HTTP avec l'adresse du firewall pour les clients 1 et 3 et avec l'adresse 193.23.23.2 pour le client 2.

3 - Filtrage

On fait toutes les commandes données dans le sujet puis on ajoute les règles :

```
nft 'add rule ip filter forward ip saddr 192.168.100.0/24 oif eth0 tcp dport { 80. 443 } accept' #accepter HTTP et HTTPs
nft 'add rule ip filter forward ip protocol icmp accept' #accepter ICMP
nft 'add rule ip filter forward ip saddr 192.168.110.254 oif eth0 udp dport { 53 } accept' #accepter DNS
nft 'add rule ip filter forward ip saddr 192.168.100.0/24 oif eth2 udp dport { 53 } accept' #accepter DNS
```