TD – NAT/PAT

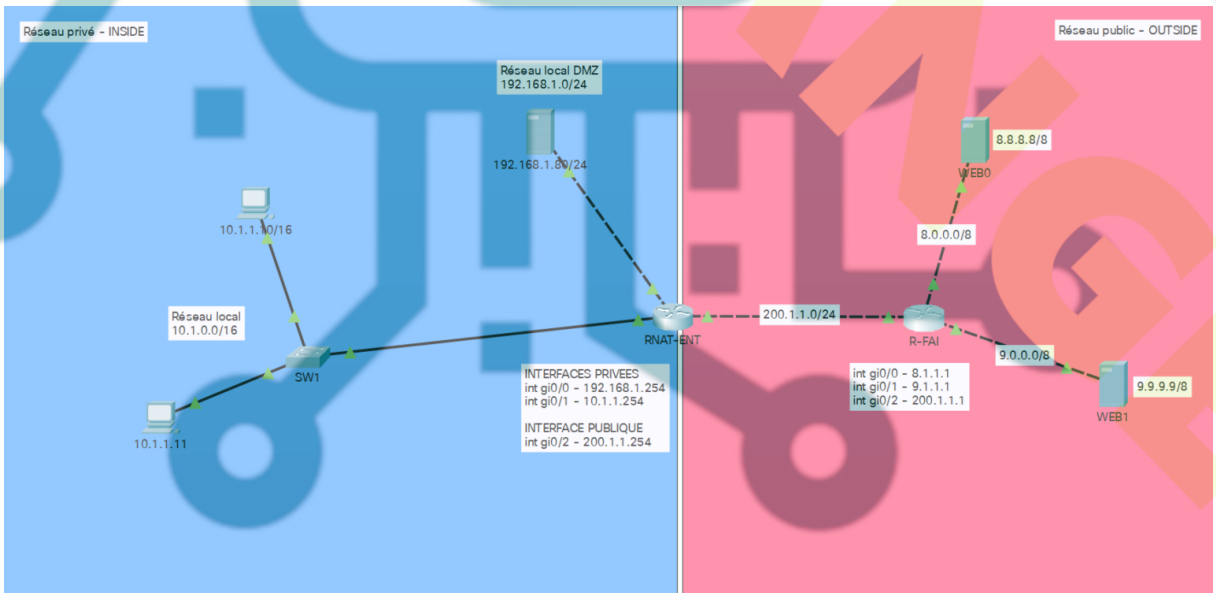
Quand il s'agit d'interconnecter un réseau privé IPv4 (que ce soit d'entreprise ou particulier) avec un réseau public, on doit la plupart du temps passer par du NAT.

Le NAT dynamique avec surcharge (NAT overload, aussi connu sous le nom de PAT)

Le TD est divisé en deux parties, le côté privé (réseau de l'entreprise) et le côté publique (le FAI et Internet). le routeur ISP (qui représente le FAI), n'a aucune connaissance des réseaux privés de l'entreprise et ne peut donc rien router à destination des réseaux 192.168.1.0. et 10.1.0.0/16

Dés lors, nous allons configurer le NAT afin de permettre un accès à Internet (simulé par 8.8.8.8 et 9.9.9.9)

- Le réseau 10.1.0.0/16 utilisera du NAT dynamique avec surcharge.
- La machine 192.168.1.80 sera accessible depuis le réseau public grâce à une configuration de NAT statique.



Les routeurs utilisés sont les 2911

Configuration de base routeur FAI

en
conf t
hostname R-FAI
interface GigabitEthernet0/0
ip address 8.1.1.1 255.0.0.0
no shut
interface GigabitEthernet0/1
ip address 9.1.1.1 255.0.0.0
no shut
interface GigabitEthernet0/2
ip address 200.1.1.1 255.255.255.0
no shut
exit

Configuration de base du routeur entreprise

en
conf t
hostname RNAT-ENT
interface GigabitEthernet0/0
ip address 192.168.1.254 255.255.255.0
no shut
interface GigabitEthernet0/1
ip address 10.1.1.254 255.255.0.0
no shut
interface GigabitEthernet0/2
ip address 200.1.1.254 255.255.255.0
no shut
exit
!configuration de la route par défaut vers internet
ip route 0.0.0.0 0.0.0.0 200.1.1.1

Tests à effectuer

Test depuis le PC 10.1.1.10 vers le serveur de la DMZ 192.168.1.80
Reply from 192.168.1.80: bytes=32 time<1ms TTL=127

Test depuis le PC 10.1.1.10 vers le routeur coté WAN
Reply from 200.1.1.254: bytes=32 time<1ms TTL=255

Test de RNAT-ENT vers internet
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Test depuis le PC 10.1.1.10 vers internet
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.

NB. le test échoue car le NAT n'est pas activé et rien dans les tables de routage des routeurs internet ne permet de connaitre le réseau 10.

Configuration commune à tout type de NAT

La première chose à faire lorsque l'on configure du NAT, quel qu'en soit le type, c'est d'indiquer au routeur où se situe le réseau privé (INSIDE) et où se situe le réseau public (OUTSIDE).

Dans notre cas, les interfaces Gi0/0 et Gi0/1 sont du côté *privé* et seront déclarées comme **inside** , l'interface Gi0/2 par contre, étant du côté *public*, sera configurée comme **outside**.

```
conf t
int gi0/0
ip nat inside
int gi0/1
ip nat inside
int gi0/2
ip nat outside
exit
```

Configuration du NAT dynamique avec surcharge

Il faut maintenant configurer le routeur entreprise pour que le réseau 10.1.0.0/16 puisse accéder à l'extérieur. Pour cela nous allons configurer le le NAT dynamique avec surcharge (overload) en utilisant l'adresse publique configurée sur l'interface Gi0/2 du routeur entreprise (RNAT-ENT)

Nous devons cette fois aussi identifier les adresses sources à faire passer par le NAT, donc nous créons une ACL (liste de contrôle d'accès)

conf t
access-list 2 permit 10.1.0.0 0.0.255.255

Puis on paramètre le NAT

ip nat inside source list 2 interface gi0/2 overload

Nous disons ici au routeur de translater les paquets provenant des adresses décrites dans l'ACL 2 (10.1.0.0/16) et de remplacer l'adresse IP source par celle configurée sur l'interface Gi0/2 en la surchargeant pour permettre à plus d'une machine de communiquer avec l'extérieur (PAT).

Tests à effectuer

Test depuis le PC 10.1.1.10 vers internet
Reply from 8.8.8.8: bytes=32 time<1ms TTL=127

Test depuis le PC 10.1.1.11 vers internet
Reply from 8.8.8.8: bytes=32 time<1ms TTL=127

Du point de vue du routeur cela revient à modifier l'adresse IP destination dans l'en-tête IPv4 avant de router le paquet. Cela signifie que si les PC envoient un paquet vers internet, à la sortie de Gi0/2 de RNAT-ENT l'adresse source (10.1.1.x) sera remplacée par l'adresse indiquée dans la translation, soit 200.1.1.254

On peut le voir grâce a la commande **sh ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	200.1.1.254:1	10.1.1.11:1	9.9.9.9:1	9.9.9.9:1
icmp	200.1.1.254:28	10.1.0.10:28	8.8.8.8:28	8.8.8.8:28

Test depuis le serveur de la DMZ vers internet

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.

NB. Le test du serveur échoue car il n'y a pas de règle pour ce réseau

Configuration du NAT statique

Ce que nous allons configurer ici c'est une translation statique dans la table de translation NAT du routeur RNAT-ENT, ce qu'on appelle également la redirection de ports. Nous allons explicitement indiquer au routeur que ce qui arrive sur son interface publique (Gi0/2) et dont l'adresse destination est 200.1.1.254 (son adresse publique) doit être redirigé vers 192.168.1.80 (le serveur de la DMZ).

ip nat inside source static 192.168.1.80 200.1.1.254

Tests à effectuer

Test depuis le serveur 192.168.1.80 de la DMZ vers internet

Reply from 8.8.8.8: bytes=32 time<1ms TTL=127

Test depuis un serveur internet vers le serveur de la DMZ

Lancer le navigateur (Desktop/web browser), puis saisir 200.1.1.254

NB. vous pouvez constater que le navigateur affiche la page située sur le serveur de la DMZ

Vérification de la translation

sh ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	200.1.1.254:80	192.168.1.80:80	8.8.8.8:1025	8.8.8.8:1025