

TP Configuration NAT sur Cisco Packet tracer

Sommaire

- 1- Introduction
- 2- Configuration du réseau
- 3- Configuration du routeur
- 4- Configuration du NAT
- 5- Test

Introduction

Le NAT (*Network Address Translation*) permet de faire le lien entre un réseau privé (LAN) et un réseau public (WAN), lorsque l'on ne peut pas configurer librement le réseau public. Le NAT modifie les adresses IP des paquets sortants pour qu'ils semblent venir du routeur lui-même, facilitant ainsi le retour des réponses.

Objectifs :

- Permettre à un réseau privé d'accéder à un réseau public.
- Cacher les IP internes à des réseaux externes.
- Mettre en œuvre un NAT dynamique avec surcharge (*overload*).

Configuration du réseau

Le réseau de test sur Cisco Packet Tracer sera composé de deux routeurs (R0 et R1), d'un switch et d'un PC.

Switch : LAN : 192.168.0.0

R1 : 192.168.0.1 (Routeur NAT entre LAN et WAN)

R0 : 10.0.0.1 / 10.0.0.2 (Routeur distant, Simulateur de réseau externe)

Configuration des routeurs

Sur le routeur R0, on configure deux interfaces réseau, une pour le LAN et une pour le WAN.

```
R0>enable
R0#configure terminal

R0(config)#interface fa0/0
R0(config-if)#ip address 192.168.0.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit

R0(config)#interface fa0/1
R0(config-if)#ip address 10.0.0.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit
```

Sur le routeur R1, qui joue le rôle d'internet dans notre TP, on configure l'interface réseau de la sorte :

```
R1> enable
R1# configure terminal
R1(config)# interface fa0/0
R1(config-if)# ip address 10.0.0.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

Configuration du NAT

On configure ensuite notre routeur pour qu'il puisse faire le NAT, en définissant quelle interface est l'intérieur (NAT) et laquelle est l'extérieur (WAN).

```
R0(config)#interface GE0/0
R0(config-if)#ip nat inside
R0(config-if)#exit

R0(config)#interface GE0/1
R0(config-if)#ip nat outside
R0(config-if)#exit
```

On crée aussi une règle d'accès pour s'assurer que le NAT fonctionne :

```
R0(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

On active aussi la translation d'adresse avec surcharge (overload). Cela permet de gérer plusieurs demandes en même temps et différencier les IP entrantes dans le routeur.

```
R0(config)#ip nat inside source list 1 interface fa0/1 overload
```

Test du NAT

On active le débogage pour pouvoir ce qui se passe en direct et comprendre si ça fonctionne bien.

```
R0# debug ip nat
```

Et on lance un ping depuis le PC sur le réseau local, vers le routeur « WAN ».

```
Router#debug ip nat
IP NAT debugging is on
Router#
NAT: s=192.168.0.10->10.0.0.1, d=10.0.0.2 [33]
NAT*: s=10.0.0.2, d=10.0.0.1->192.168.0.10 [12]
NAT: expiring 10.0.0.1 (192.168.0.10) icmp 18 (18)
NAT: s=192.168.0.10->10.0.0.1, d=10.0.0.2 [34]
NAT*: s=10.0.0.2, d=10.0.0.1->192.168.0.10 [13]
NAT: s=192.168.0.10->10.0.0.1, d=10.0.0.2 [35]
NAT*: s=10.0.0.2, d=10.0.0.1->192.168.0.10 [14]
NAT: s=192.168.0.10->10.0.0.1, d=10.0.0.2 [36]
NAT*: s=10.0.0.2, d=10.0.0.1->192.168.0.10 [15]
NAT: expiring 10.0.0.1 (192.168.0.10) icmp 19 (19)
NAT: expiring 10.0.0.1 (192.168.0.10) icmp 20 (20)
```

Le NAT est bien fonctionnel !