

La translation d'adresses (NAT/PAT)

Et la redirection de port

Objectifs :

- Comprendre le fonctionnement de la redirection de port ;
- Configurer la redirection de port sur des routeurs Cisco ;
- Diagnostiquer le service.

1. Rappel :

Nous avons réalisé la translation d'adresses NAT qui permet la communication des postes d'un réseau local (LAN) avec des serveurs sur Internet.

2. Problématique :

Comment rendre accessible un serveur situé dans un LAN privé via le réseau public Internet ?

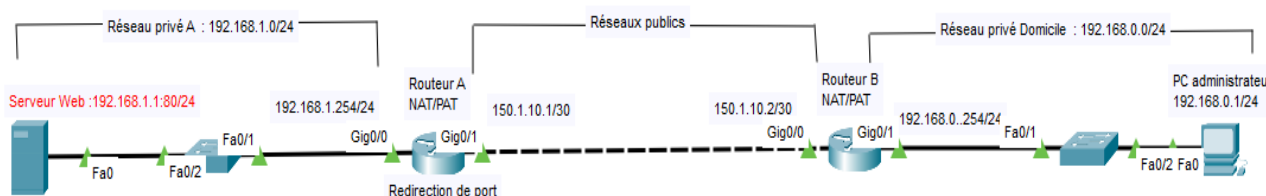
3. Solution :

Il existe une technique appelée « **redirection de port** » ou « **NAT statique** » qui consiste à configurer la passerelle pour transmettre à une machine **spécifique du réseau interne**, tous les paquets reçus sur **un port particulier**.

4. Illustration :

Sur cette maquette, les 2 réseaux privés (LAN) communiquent via le réseau public (Internet). Ces 2 réseaux privés sont connectés à Internet à l'aide de 2 routeurs NAT/PAT.

- Le routeur A effectue le NAT/PAT et la **redirection de port** ;
- Le routeur B effectue le NAT/PAT.



IP source		IP destination	
...	150.1.10.2	192.168.1.1 :80	...

←

IP source		IP destination :port des	
..	150.1.10.2	150.1.10.1:8080	..

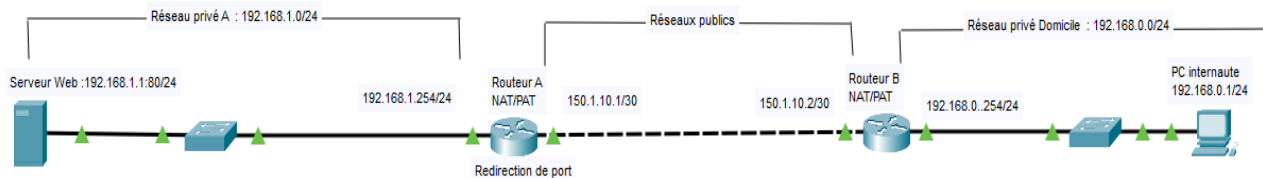
Explications :

- Le PC administrateur envoie une requête vers l'adresse publique du routeur A ;
- Le routeur B reçoit la requête et effectue la translation NAT/PAT en modifiant l'adresse IP source du paquet;
- Le routeur A reçoit la requête sur le port 8080 et la redirige vers l'adresse du serveur web 192.168.1.1 sur le port 80.

5. Mise en place de la redirection de port :

Objectif : permettre au PC internaute et d'autres PC l'accès au serveur Web 192.168.1.1/24.

a. Réaliser la maquette suivante :



b. Configurer les postes et les interfaces des routeurs.

c. Configurer le routage statique sur les routeurs.

d. Définir les interfaces pour le NAT entrant et sortant.

```
Router(config)#interface nom_interface      #interface interne (côté LAN)
Router(config-if)#ip nat inside
Router(config)#interface nom_interface      #interface externe (côté Internet)
Router(config-if)#ip nat outside
```

e. Configuration de la liste d'accès (ACL)

Une liste d'accès ou Access Control List (ACL) permet de filtrer les paquets IP au niveau 3 du modèle OSI.

Ainsi, une ACL va indiquer au routeur les paquets qu'il doit accepter et ceux qu'il doit refuser, notamment en fonction de leur adresse IP de provenance, leur IP destination et les ports source et destination.

Syntaxe :

```
Router(config)#access-list n° permit @réseau masque_générique
```

f. Configuration du NAT dynamique avec surcharge

Syntaxe :

```
Router(config)#ip nat inside source list n° interface nom-interface-externe overload
```

g. Vérifier le bon fonctionnement du NAT

Réaliser plusieurs ping entre le PC-internaute et le serveur Web puis, taper la commande suivante :

```
#show ip nat translation
```

Réaliser une copie d'écran et commenter le résultat :

Activer le mode « debug » et réaliser un ping entre le PC-internaute et le serveur Web :

```
#debug ip nat
```

Réaliser une copie d'écran et commenter le résultat :

h. Analyser le contenu des trames en réalisant des copies d'écrans et les commentant

i. Réaliser la redirection de port (NAT statique) sur le routeur A

Syntaxe :

```
R-A(config)# ip nat inside source static tcp ip-serveur-privé port-serveur ip-  
publique port-public
```

Adapter la commande à votre cas :

```
R-A(config)# ip nat ...
```

**j. Tester la redirection de port en tapant dans le navigateur du PC-internaute
l'adresse IP publique du routeur A avec le n° de port 8080.**

k. Analyser le contenu des trames avant et après redirection de port

6. Synthèse :

