Chassat

Thomas

**NAT & PAT – Translation d’adresses avec access-list**

**Introduction :**

Cette procédure va vous expliquer comment fonctionnent les technologies NAT (Network Address Translation) et PAT (Port Address Translation) mais aussi comment les configurer sur un routeur de marque Cisco. Toutes les machines connectées (PC, serveurs, imprimantes réseau, smartphones, télévisions multimédias...) disposent d'une adresse IP permettant de l'identifier sur le réseau. Il existe deux sortes d'adresses: les adresses privées et les adresses publiques. Une adresse privée est seulement valable sur un réseau privé et ne peut donc pas être utilisé pour  communiquer sur un réseau public comme Internet. En effet, Internet n'accepte de véhiculer que des adresses publiques. Le principal intérêt de l'utilisation d'adresses IP privées est de disposer d'un grand nombre d'adresses pour bâtir ses réseaux privées (entreprises, domicile...) et ainsi de palier au cruel manque d'adresses IP publiques du réseau IP version 4.

Les plages d'adresses IPv4 privées sont les suivantes :

 - 10.0.0.0 -> 10.255.255.255 = 16 777 216 adresses réseaux possibles

 - 172.16.0.0 -> 172.31.255.255 = 1 048 576 adresses réseaux possibles

 - 192.168.0.0 -> 192.168.255.255 = 65 536 adresses réseaux possibles

On active le mécanisme de NAT sur les routeurs faisant le lien entre les réseaux privées et publics. Le principe général est de remplacer l'adresse IP source privée de la machine par l'adresse IP publique du routeur.

**Pré requis :**

Dans la situation que je vais vous présenter, nous allons prendre une plage d'adresse IP privée de classe A : la plage 10.0.0.0 -> 10.255.255.255 ainsi qu'un serveur qui se situe dans l'internet et qui a pour adresse IP 60.0.0.254. Il n’y a pas réellement de pré requis pour cette procédure étant donné que je me base sur le travail de l’installation VLAN Cisco. Le matériel est donc le même.

**Mise en place des règles NAT et access-list :**

Nous allons commencer par la configuration des deux interfaces concernées pour le réseau local de classe A (10.0.0.0) et le serveur situé sur internet (60.0.0.254).



La commande ***enable***  permet d’accéder au routeur en mode super-utilisateur.



La commande ***config terminal*** permet de rentrer en configuration du routeur.



La commande ***interface fastEthernet 0/0*** permet de rentrer en configuration de l’interface ethernet numéro 0.



La commande ***ip nat inside*** permet d’indiquer le réseau privé qui rentre dans le routeur.



La commande ***no shutdown*** permet de sauvegarder la configuration du routeur.



La commande ***exit*** permet de quitter le mode de configuration (vlan, interface fastEthernet).



La commande ***interface fastEthernet 0/1*** permet de rentrer en configuration de l’interface ethernet numéro 1.



La commande ***ip nat outside*** permet d’indiquer le réseau privé qui rentre dans le routeur.



La commande ***no shutdown*** permet de sauvegarder la configuration du routeur.



La commande ***exit*** permet de quitter le mode de configuration (vlan, interface fastEthernet).



La commande ***write*** permet d’inscrire la configuration dans la mémoire du routeur.

Maintenant que les interfaces sont configurées en NAT, nous allons affecter les adresses IP aux interfaces ethernet.









La commande ***ip address 10.0.0.254 255.0.0.0*** permet d’attribuer une configuration IP à l’interface fastEthernet 0 qui est reliée au réseau local.







La configuration du routeur est bientôt terminée. Il ne nous reste qu’à ajouter les access-list (les listes d’accès qui permettent ou interdisent les accès aux réseaux, aux hôtes). Par défaut, un routeur possède des access-list ne permettant que très peu de d'accès (seulement les plus basiques). C'est pourquoi, nous allons ajouter une access-list qui permettra aux adresses de notre réseau privé d'accéder au serveur situé sur internet.







Cette commande explique qu’une liste d’accès vient d’être créée, elle a le numéro 20, elle permet absolument tout aux éléments du réseau 10.0.0.0 avec comme masque 0.255.255.255 (qui est le masque générique).



Cette commande crée une étendue de translation d’adresses allant de 60.0.0.1 jusqu’à 60.0.0.254



Cette commande applique la règle de filtrage numérotée 20 à la plage NAT.