Procédure de configuration d'éléments d'interconnexion : Le NAT

Contexte Cyres.

Dans une architecture réseau classique, il est nécessaire de faire correspondre les multiples adresses du LAN à une adresse publique unique. Pour pallier à ce problème d'adressage, le NAT, pour Network Translation, va nous permettre de faire communiquer des machines internes de notre LAN avec des machines externes sur internet. Pour que les multiples postes clients de l'entreprise Cyres soient capables d'accéder à des ressources externes, nous allons mettre un place un NAT sur le routeur de périphérie.

Il existe trois différents types de NAT :
- Le NAT statique permet de créer une table de correspondances d'adresses et de ports. Ainsi, une table va être configurés, spécifiant vers quel port les connexions initiés vers une adresses spécifique vont être redirigés.

- Le NAT Dynamique PAT, ou NAT PAT, permet de faire correspondre un pool d'adresse interne vers une adresse publique unique. Les postes du LAN sont identifiées au travers d'un port spécifique. De cette façon, le routeur de sortie va attribuer un port à une IP du LAN, et retourner la réponse du serveur sollicité à l'IP de destination locale en fonction du port attribué à la requête.

- Le NAT Dynamique, ou avec pool d'adresses. Pour ce type de translation d'adresses, un pool d'adresse LAN et un pool d'adresses WAN sont utilisés. Les adresses WAN sont attribués méthodiquements : la première adresse LAN est attribuée à la première adresse publique disponible dans le pool d'adresse WAN disponibles. Le nombre d'adresses disponibles dans le pool va définir le nombre de postes locaux pouvant se connecter à internet simultanéments.

Au sein du contexte actuel, nous allons implémenter un NAT PAT, ou dit NAT Overload (avec surcharge).

Nous allons commencer par identifier les interfaces LAN et WAN aux yeux du NAT. L'interface LAN sera considéré comme l'interface "inside" du NAT, et l'interface WAN comme "outside".

```
en
conf t
interface fastethernet 0/1
ip nat inside
```

```
interface fastethernet 0/0
ip nat outside
exit
```

Il est ensuite nécessaire de créer une ACL autorisant nos hôtes locaux à sortir du réseau. Cette ACL sera posée sur l'interface "inside" du routeur de sortie.

```
access-list 100 permit ip any any any
ip nat inside source list 100 interface fastethernet 0/1 overload
```

Il ne reste qu'à tester le bon fonctionnement du notre NAT en produisant du trafic sortant depuis les postes clients. Il sera ainsi possible d'observer la translation d'adresse au niveau du routeur avec la commande *show ip nat translation* :

Pro Inside global	**Inside local**	**Outside local**	**Outside**
udp 200.2.2.1:53427	192.168.0.6:53427	74.200.84.4:53	74.200.84.4:53
udp 200.2.2.1:53427	192.168.0.6:53427	195.170.0.1:53	195.170.0.1:53

La maquette téléchargeable à l'adresse suivante résume les configurations effectuées :
http://www.mediafire.com/file/o3q15a84gic2l48/NAT.pkt