# TP – Administration des Access Lists et NAT

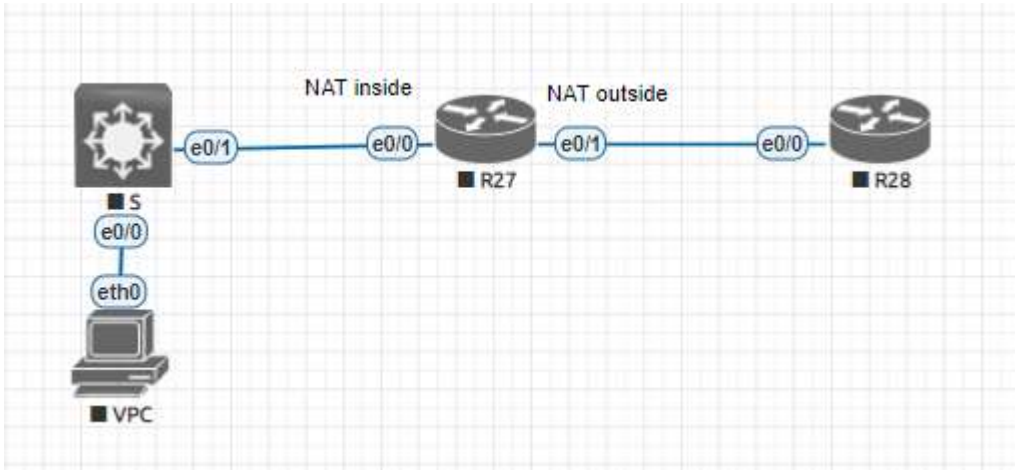
**Objectif :**

Le but de ce TP est de vous familiariser avec le contrôle des listes d'accès (ACL). Vous aurez les moyens pour gérer l'accès aux ressources pour mieux les sécuriser.

**Topologie :**

Vous êtes administrateur de votre réseau d'entreprise, l'adresse réseau globale est 10.0.x.0/24. Le réseau internet possède une adresse IP globale de 200.0.x.0/24. Il a été décidé de créer 4 Vlans : Accounting - Sales, usagers, Local servers et Admin. Les deux premiers sont destinés aux utilisateurs, le troisième Vlan est aux ressources de votre réseau (DNS et web) et le quatrième aux administrateurs réseaux. Un serveur DHCP dans le vlan administration pour assigner des adresses IP aux utilisateurs, les deux switchs supportent les deux Vlans.

Les passerelles des utilisateurs se terminent par « .1 ».




gPour accéder, aux différents réseaux, activez le routage OSPF avec le numéro de processus « 2 ».

**Configuration de NAT**

Jusqu'à présent toutes les communications de votre réseau local vers l'internet se fait avec des adresses privées. Dans la réalité, vous devez masquer ces adresses qui sont non-routables par des adresses routables.

Dans cette partie vous mettez en place les différentes configurations de NAT pour permettre aux utilisateurs et serveurs de communiquer avec le monde extérieur.

Toutes les configurations se font sur le routeur de bordure de votre réseau local c'est le routeur2

**Configuration type PAT – Port Address Translation**

Cette configuration sera utilisée par les adresses privées des utilisateurs.

Sur le routeur2, précisez le comportement de ses interfaces vis-à-vis du NAT. Ajoutez aux interfaces internes « ip nat inside » et à l'interface externe du réseau « ip nat outside ».

**Trafic issus des Vlans :**

Filtrez le trafic des vlans, revient à créer une access list :

**Exemple :**

***Ip access-list 1 permit 10.0.10.0 0.0.0.255***

Comme c'est une translation de type PAT, cela veut dire que tout le trafic interne sera mappé par l'interface de sortie.

**Exemple :**

***Ip nat inside source list 1 interface FastEthernet x/x overload*** (#Fx/x est l'interface externe)

Testez la communication depuis votre réseau vers le routeur externe

Affichez le résultat de votre table NAT avec la commande «show  ip nat translation » et la commande « show ip nat statistics ». Analysez le résultat ?

Cette partie à tester dans votre projet pour accéder aux serveur web, DNS etc.

**Translation statique (Port forwarding)**

Le but est de donner, accès à certaines ressources, aux utilisateurs qui sont à l'extérieur de votre réseau local. La translation statique est permanente et indique au routeur l'adresse publique, qui sera utilisée par ces utilisateurs pour accéder à la ressource demandée. Dans votre cas, vous configurez un accès web depuis l'extérieur.

- **Autorisez que le trafic web :**
  **Exemple :**
  ***Access-list 180 permit tcp any host 200.0.0.200 eq 80*** (#200.0.0.200 est l'adresse publique utilisée par tous les utilisateurs à l'extérieur de votre réseau)
  ***Access-list 180 permit tcp any host 200.0.0.200 eq 443***
  ***Access-list 180 deny ip any host 200.0.0.200*** (#interdire tout autre trafic)
- **Configuration du NAT statique :**
  **Exemple :**
  ***Ip nat inside static tcp 10.0.Z.Y 80 @IP_externe_Route_Edge 80***
  ***Ip nat inside static tcp 10.0.Z.Y 443 @IP_externe_Route_Edge 443***

Depuis un navigateur web externe, accédez à la page web interne avec l'adresse « @IP externe du routeur Edge »