Université Sorbonne Paris Nord : IUT Villetaneuse
Dr. Mohamed Amine Ouamri
Matière : SAE Supervision de la Sécurité

Objectif

Cette seconde partie de la SAE portera sur pratique avec les équipements Cisco à savoir Switch routeur et Firewall. Trois exercices sont à réaliser. Le premier exercice traite la problématique de translation d'adresse (Network Adress Translation) que vous avez réalisé avec Marionnette. Dans le second exercice vous allez aborder la notion d'ACL (Access Control List), c'est-à-dire les listes de contrôle d'accès au niveau routeur. Enfin, le dernier exercice sera une pratique simple de votre choix en utilisant le Farewell Stormshield. Il est important de rappeler que cette partie d'SAE sera réalisé et exposé suivant les groupes formés.

Exercice 1

Le **NAT** ou **"Network Address Translation"** est une bonne réponse aux problématiques de routage que l'on peut rencontrer lorsque l'on souhaite lier un réseau dit **"privé"** (c'est à dire sur lequel nous avons la main) à un réseau dit **"publique"** (sur lequel nous ne pouvons modifier la configuration). Le but du **NAT** quand il est mis sur un routeur séparant deux réseaux comme ceux-ci est de faire passer toutes les requêtes provenant du réseau privé (que nous identifierons comme le **LAN)** comme des requêtes provenant de ce routeur est nous d'un élément derrière lui possédant un autre adressage. Le schéma ci-dessous illustre le cas de figure que vous allez étudier.

Pour mettre en place votre infrastructure, vous devez configurer l'architecture présentée. Je propose la configuration dans la figure, mais vous pouvez utiliser votre propre configuration.

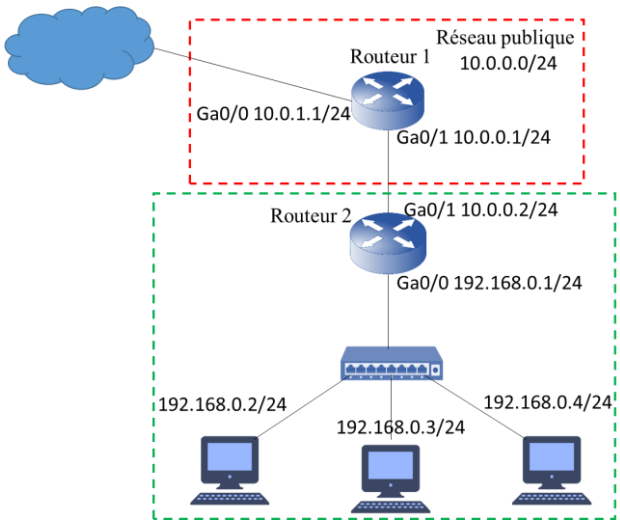

Figure 1. Architecture réseau pour création de NAT.

On va à présent configurer le routeur 2 :

R2>enable
R2#configure terminal
R2(config)#interface Gi0/0
R2(config-if)#ip address 192.168.0.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Gi0/1
R2(config-if)#ip address 10.0.0.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

Vous devez ensuite indiquer quelle interface sera à l'intérieur du NAT ("inside") et quelle interface sera à l'extérieur ("outside"). Cela permettra de dire au routeur dans quel sens il doit affecter les translations d'adresses. Ici, l'interface Ga0/0 (192.168.0.1) sera l'interface Inside et l'interface Ga0/1 (10.0.0.1) sera l'interface Outside.

R2(config)#interface Gi0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface Gi0/1
R2(config-if)#ip nat outside
R2(config-if)#exit

Ensuite créer les règles d'accès qui permettra au LAN de sortir du NAT comme suit :

R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R2(config)#ip nat inside source list 1 interface Gi0/1 overload

Le processus de translation d'adresse est maintenant opérationnel. Pour vérifier que votre routeur est bien en mode NAT, vous devriez pouvoir communiquer à présent avec le routeur R1 depuis le poste LAN. Avant cette communication, vous pouvez saisir la commande suivante dans votre routeur R2.

R2#debug ip nat

Vous allez ensuite communiquer avec votre routeur R1 et vous devriez avoir les étapes de translation d'adresse s'afficher.

```
NAT: s=192.168.0.10->10.0.0.1, d=10.0.0.2 [10]

NAT*: s=10.0.0.2, d=10.0.0.1->192.168.0.10 [6]

NAT: s=192.168.0.10->10.0.0.1, d=10.0.0.2 [11]

NAT*: s=10.0.0.2, d=10.0.0.1->192.168.0.10 [7]
```

Exercice 2

Les ACL, pour Access Control List, sont des règles appliquées aux trafics transitant via les interfaces du routeur que ce soit en entrée (in) ou en sortie (out). Les ACL filtrent le trafic en demandant aux interfaces d'acheminer ou non les paquets qui y transitent. Pour ce faire, le routeur lit l'en-tête de chaque paquet afin de déterminer s'il doit être acheminé ou non en fonction des conditions définies dans la liste de contrôle d'accès ACLs. Une question très importante que l'on peut se poser lorsque l'on veut mettre en place l'ACLs, c'est savoir sur quelle interface faut-il

appliquer les ACLs ? L'interface entrante ou sortante du routeur ? Répondons à cette question dans cette première partie de l'article.
Les ACLs peuvent être associés à une interface particulière et pour une direction du flux (en entrée ou en sortie). En outre, ces règles de filtrages peuvent être appliquées avant que le routeur ne prenne sa décision de routage (interface en entrée), ce qui est un bon moyen d'économiser les ressources matérielles du routeur, ou après que le routeur ait pris sa décision de transfert et déterminé l'interface de sortie à utiliser pour acheminer le paquet.

1. Réalisation d'un ACL standard

Dans ce type, l'ACL ne peut être liée qu'à l'adresse IP source du paquet. Ces ACLs sont identifiables par identifiant correspondant à un nombre allant de 1 à 99 et de 1300 à 1999. Nous pourrons utiliser ce type d'ACL pour autoriser ou interdire un segment du réseau ou l'adresse IP d'une machine à communiquer avec un autre segment de réseau ou une autre machine. Afin de concrétiser la notion d'ACL standard, vous allez les mettre en place sur un routeur Cisco.

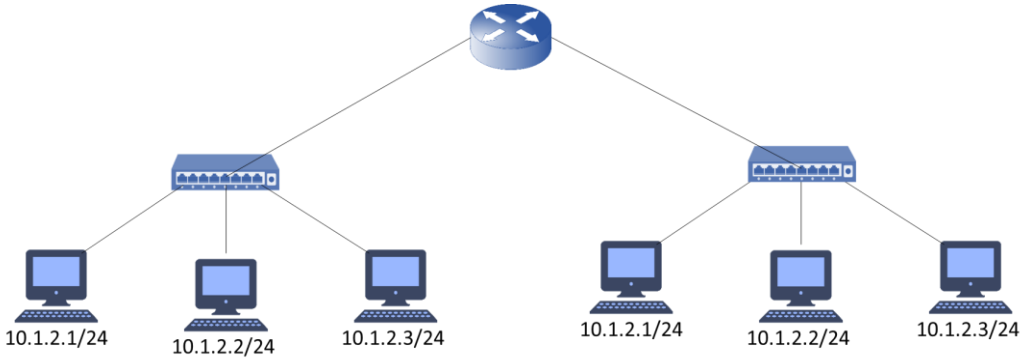

Figure 2. Network for ACL standard

Dans l'exemple ci-dessus, les trois ordinateurs, situés sur des segments réseau différents, communiquent entre eux. Le but est d'interdire au réseau « 10.1.1.0/24 » de communiquer avec le réseau « 10.1.2.0/24 » tout en ayant la possibilité de communiquer avec le réseau « 10.1.3.0/24 » pour ce faire, nous allons, sur l'interface Gi0/2, interdire les paquets provenant du réseau « 10.1.1.0/24 ». Pour parvenir aux résultats souhaités, nous appliquons trois étapes :

☞ Après s'être connecté sur le routeur en mode de configuration globale en tapant les commandes "enable" puis "configuration terminal", on commence par la création de la règle :

Router(config)#access-list 1 deny 10.1.2.0 0.0.0.255

☞ En précisant "access-list 1" on attribue un ID à notre ACL, puis ensuite on précise que l'on veut refuser avec "deny", et enfin on précise l'adresse IP de destination (10.1.2.0) et le masque au format inversé appelé wildcards mask (0.0.0.225).

☞ Deuxièmement, comme évoqué précédemment, il faut autoriser explicitement les réseaux que l'on veut laisser passer, dans notre exemple c'est « 10.1.3.0/24 ». À défaut, il n'y aura pas de correspondance entre l'IP source contenue dans l'en-tête du paquet et les règles ACL, ce qui veut dire que le routeur va les refuser implicitement et notre réseau en 10.1.3.0/24 ne pourra pas non plus communiquer avec le 10.1.2.0/24.

Router(config)#access-list 1 permit 10.1.3.0 0.0.0.255

☞ Troisièmement, on sélection l'interface concernée et enfin on applique la règle en sortie
Router(config-if)# ip access-group 1 out
Router(config)#interface gigabitEthernet 0/1 (l'interface liée au réseau 10.1.2.0/24)

2. Les ACL étendues

Les ACL étendues présentent plusieurs similitudes par rapport aux ACL Standards décrites dans la section précédente. Tout comme une ACL standard, on active les ACL étendues sur les interfaces pour les paquets entrants ou sortants, puis le routeur cherche dans la liste de manière séquentielle. Les ACL étendues utilisent également la logique de première correspondance, car dès que la première instruction est mise en correspondance, le routeur arrête la recherche dans la liste d'ACL, en effectuant l'action définie. En comparaison des ACL standards, les ACLs étendues vont permettre d'analyser une plus grande variété de champs au sein de l'en-tête d'un paquet. Cela rend les ACL étendues plus puissantes, plus précises, mais aussi un peu plus complexes. Les ACL étendues suivent la même logique que les ACL standards, elles sont identifiables par un numéro, allant de 100 à 199 et de 200 à 2699.

Un exemple sera plus parlant, nous allons créer une règle qui aura pour but d'interdire le Ping de réseaux 10.1.2.0/24 vers le réseau 10.1.3.0/24, en posant les règles sur les sous-réseaux (tous en /24). Mettons ça en place en reprenant la même topologie.
Sur votre routeur appliqué la commande suivante

Router(config)# access-list 100 deny icmp 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
Router(config)#interface gig 0/1
Router(config-if)#ip access-group 100 in

Il est à noter que les ACLs étendues peuvent aussi examiner des parties d'en-têtes TCP ou UDP, en particulier les champs qui contiennent le numéro de port source et port de destination. Les numéros de port identifient le service qui envoie ou reçoit les données. Quand le mot "tcp" ou "udp" est inclus dans la règle de l'ACL, cela permet de préciser le port source et le port de destination afin d'avoir une règle plus précise. Voici un exemple :

Router (config)# access-list 100 permit tcp 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255 eq 21

Trouver une règle pour permettre le ping entre les deux réseaux.

Exercice 3

En vous servant de vos connaissances sur le firewall Stormshield, proposer un cas d'étude simple pour filtrer un trafic dans un réseau en utilisant le firewall. Vous pouvez revoir les TPs déjà réalisé dans d'autres modules. Pour cet exercice un compte rendu est nécessaire avec toutes les étapes de pratique.