M2106 RT1
TP 02 — NAT et filtrage IP

Au cours de ce TP, vous ajouterez de la traduction d'adresse (Network Address Translation) au niveau d'un routeur sur un réseau configuré manuellement ou par DHCP. Vous ajouterez par la suite du filtrage IP pour ajouter de la sécurité à votre réseau. Tout au long du TP, vous observerez les messages circulant sur le réseau à l'aide du logiciel wireshark. Objectifs :

— Utiliser wireshark.

— Configurer la traduction d'adresse.

— Configurer le filtrage IP.

1 Traduction d'adresse

La traduction d'adresse consiste à remplacer les adresses IP de certains paquets par d'autres adresses prédéterminées. Le but est généralement de cacher des adresses ; par exemple, des adresses de réseau local non routables sur Internet. Sur Linux, la traduction d'adresse est réalisée par le biais d'une table intégrée dans le mécanisme de filtrage (cf. Figure 1).

Lorsqu'un paquet arrive sur la machine, il passe par la chaîne PREROUTING avant de subir le verdict de la décision de l'algorithme de routage puis soit il passe par la chaîne POSTROUTING avant d'être émis, soit il est délivré localement. Lorsqu'un paquet est généré localement sur la machine, il passe par la chaîne OUTPUT puis il passe par la chaîne POSTROUTING avant d'être émis.

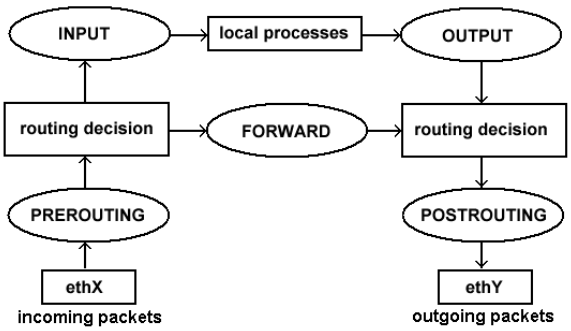

FIGURE 1 – La chaîne du filtrage [1]

```
(1) iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.17.11
(2) iptables -t nat -A POSTROUTING -p tcp --dport 80 -o eth0 -j SNAT --to 192.168.17.11
(3) iptables -t nat -A PREROUTING -p tcp -d 14.17.0.0/16 -dport 80 -j DNAT \
--to 14.17.16.100:8080
```

La commande (1) permet de changer l'adresse source de paquets sortants par l'interface eth0.

La commande (2) permet de réaliser la même opération mais uniquement pour le port 80 de TCP.

La commande (3) traduire l'adresse destination de tout paquet à destination du port 80 d'une machine du réseau 14.17.0.0 vers l'adresse 14.17.16.100, port 8080.

1) La figure 1 présente le parcours d'un paquet dans la chaîne de filtrage.

2) Vous configurerez une architecture avec un réseau local et un routeur. Vous ajouterez le NAT au niveau de votre routeur sur son port extérieur. Chaque routeur aura une adresse dans le réseau d'interconnexion pour pouvoir communiquer avec l'adresse publique des autres routeurs.
Vous observerez les modifications réalisées par le NAT sur les paquets.

2 Firewall

Nous allons appréhender la notion de pare-feu afin de savoir comment la mettre en œuvre.

On différencie généralement deux zones, la DMZ (zone démilitarisée) et le réseau interne. La première contient les serveurs susceptibles d'être accédés depuis des machines situées à l'extérieur, sur Internet ; alors que la seconde contient la majorité des machines qui devront être le plus isolées possible d'Internet.

Nous allons réutiliser la chaîne du filtrage présentée à la Figure 1 avec d'autres éléments pour limiter l'accès au réseau. La chaîne :

— d'entrée (INPUT) concerne tous les paquets entrants dont le firewall est le destinataire final ;

— de sortie (OUTPUT) concerne chaque paquet généré par le firewall ;

— de réexpédition (FORWARD) concerne les paquets que le firewall doit faire suivre à une autre station.

```
(1) iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
(2) iptables -L -v -n
(3) iptables -D INPUT 1
```

La commande (1) refuse (DROP) tous les paquets entrants (INPUT) en provenance -s de l'adresse 127.0.0.1 pour le protocole (-p) ICMP et à destination de la machine locale.

On peut observer l'état des chaînes à l'aide de la commande (2). Par la suite, on détruit la première règle de la chaîne INPUT avec la commande (3).

3) Vous allez désormais fusionner deux groupes de deux. Vous aurez un premier routeur qui fera office de routeur d'accès à Internet puis un deuxième routeur qui servira de firewall entre le réseau des machines accessibles de l'extérieur (serveurs) et celui des machines de travail.

Définissez une politique de sécurité à appliquer sur les deux routeurs puis testez-la. (Vous pouvez par exemple demander à d'autres groupes d'essayer de contrôler à distance une machine à laquelle ils ne devraient plus pouvoir accéder).

Références

[1] Image disponible à `http://www.sysresccd.org/images/dport-routing-02.png`.