R401 – Architectures sécurisées

NAT et Filtrage sous linux

TP 4

Consignes

L'objectif de ce TP est de vous familiariser avec le filtrage de paquets sur un routeur Linux. On abordera les différents types de NAT mais également le filtrage de paquets avec état (prise en compte de l'historique des paquets filtrés). Ce TP sera effectué en binôme et un compte rendu sera rendu en fin de séance. Vous réaliserez le montage présenté sur la figure 1 en respectant le plan d'adressage indiqué. Vous pourrez réaliser la partie réseau interne avec des machines virtuelles ainsi que le routeur. Le PC dans la salle pourra être celui de votre binôme. Le serveur web interne sera un simple serveur apache2 avec une page statique indiquant le nom de votre binôme en remplacement de la page d'accueil.
Un document de synthèse des règles est présent à l'URL suivante : https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes.

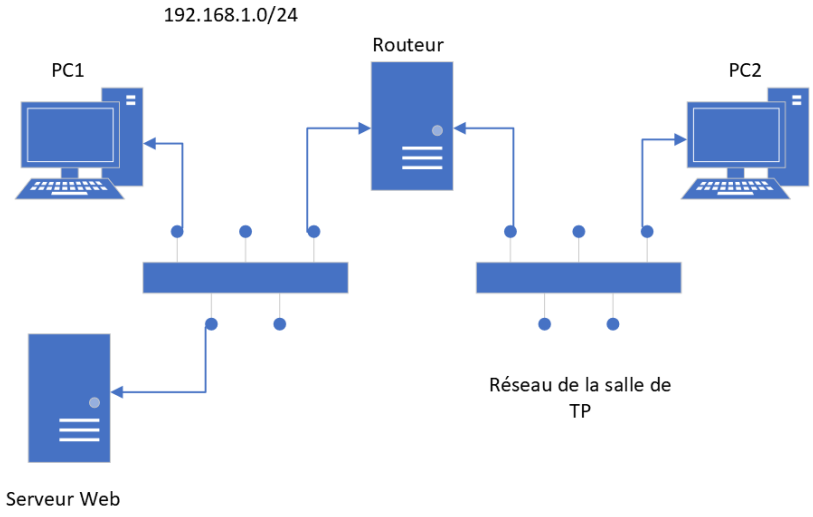

FIGURE 1 – Architecture réseau pour mise en place de filtrage et NAT.

1 Le NAT

Dans cette section, nous allons mettre en place les différents types de NAT possibles.

1.1 SNAT

Le premier et le plus courant des types de NAT est le SNAT. Celui-ci consiste à changer l'adresse IP source d'un paquet. C'est ce qui est utilisé dans les BOX internet de vos domiciles pour transformer l'adresse IP privée de vos machines en une adresse IP publique

pouvant circuler sur internet. Généralement, cette adresse est l'adresse publique affectée à votre Box par votre fournisseur d'accès à Internet.

Une commande vous permettant de visualiser toutes les règles sur votre machine est

```
nft list ruleset
```

Exercice 1 Sur quel hook doit se placer la règle de SNAT ?

Exercice 2 Configurer les tables, chaînes et règles pour faire du SNAT afin de changer l'adresse IP du PC1 lorsqu'il essaie de s'adresser au PC2 et ainsi rendre la communication possible. Vous indiquerez dans votre compte-rendu les commandes saisies.

Exercice 3 Proposer une méthode pour tester votre configuration et effectuer les relevés nécessaires pour illustrer le bon fonctionnement de votre configuration.

1.2 MASQUERADE

Lorsque l'adresse IP de sortie du réseau n'est pas fixe, il n'est pas possible de réaliser du SNAT avec une règle précisant en dur l'adresse de sortie. On met en place alors une règle de type SNAT qui s'appelle MASQUERADE.

Exercice 4 Supprimer la règle précédente et la remplacer par une règle de type MASQUERADE. Proposer une méthode pour tester votre configuration et faire les relevés pour illustrer son bon fonctionnement.

1.3 DNAT

Le DNAT est utilisé quand une machine de l'Internet essaie de joindre un serveur se trouvant dans une zone avec un adressage privé. Il faut donc que le client sur internet passe par le routeur et que celui-ci relaie le message vers le serveur interne.

Exercice 5 Sur quel hook doit se placer la règle de DNAT ?

Exercice 6 Configurer les tables, chaînes et règles pour faire du DNAT afin de permettre au PC2 d'accéder au serveur web interne. Vous indiquerez dans votre compte-rendu les commandes saisies.

Exercice 7 Proposer une méthode pour tester votre configuration et effectuer les relevés nécessaires pour illustrer le bon fonctionnement de votre configuration.

2 Filtrage

Le module NETFILTER et son interface avec nftable peut également être utilisé pour filtrer les paquets entrants, sortants ou traversants le routeur. Dans cette deuxième partie, nous testerons différents filtres permettant de restreindre le trafic réseau.

2.1 Sans état : Stateless

La première partie consiste en du filtrage simple de paquets en fonction de critères sur les adresses ou sur les ports.

Exercice 8 Récupérer l'adresse IP d'un site web et proposer une règle permettant d'empêcher les consultations de ce site. Vous indiquerez dans votre compte-rendu les commandes saisies.

Quel peut être la limite de cette approche (on pourra penser aux adresses IP utilisées par des serveurs comme Facebook ou d'autres grosses entreprises qui gèrent beaucoup de trafic) ?

Exercice 9 On activera un serveur SSH sur le routeur pour que des personnes du réseau local puissent l'administrer. Le premier filtre que nous allons mettre en place est de bloquer le trafic sur le port 22 pour des messages provenant du réseau du PC2. Vous indiquerez dans votre compte-rendu les commandes saisies.

Exercice 10 Si on suppose que la passerelle ou le réseau interne dispose de plusieurs services, est-il raisonnable de spécifier un par un les ports accessibles depuis l'intérieur, mais pas l'extérieur ? Quel est le risque d'une telle approche ? Que faudrait-il préciser dans la déclaration de la chaîne pour se simplifier la vie et assurer une meilleure sécurité ?

Exercice 11 Proposer une règle permettant de rejeter les paquets entrants sur l'interface de sortie du routeur (celle reliée au réseau de la salle) correspondant à des ECHO_REQUEST ICMP. Tester la différence entre les 2 actions "REJECT" et "DROP". Vous illustrerez ceci avec des captures des résultats obtenus sur vos consoles.

Consignes

On peut également saisir ses règles dans un fichier texte et les exécuter avec la commande suivante *nft -f FILENAME*. Pour voir le format du fichier, il suffit de faire un export de vos règles actuelles grâce à la commande suivante : nft list ruleset > MonFichier.rule. Voici un exemple de format de fichier de règles (issu du site https://www.it-connect.fr/chapitres/gestion-des-regles-dans-nftables/.

```
table ip mon_filtreIPv4 {
    chain input {
        type filter hook input priority filter; policy accept;
        tcp dport 80 accept
        tcp dport 443 accept
        drop
    }
    chain output {
        type filter hook output priority filter; policy accept;
        tcp sport 80 accept
        tcp sport 443 accept
        drop
    }
}
```

Exercice 12 Donner le fichier de règles permettant de

- ▷ bloquer par défaut tout le trafic sur le routeur ;
- ▷ autoriser les ping sur le routeur
- ▷ n'autoriser que les connexions entrantes en SSH provenant du réseau interne (gauche sur la figure 1)
- ▷ autoriser les connexions traversant le routeur à destination de serveurs web (port destination 80)

2.2 Avec état : Statefull

Le filtrage peut se faire de façon plus fine si l'on tient compte de l'état des drapeaux TCP par exemple. On pourra alors autoriser du trafic correspondant à des connexions déjà établies passant par des ports non encore vus.

Exercice 13 Dans la documentation du site https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes, quel est le mot clef utilisé pour faire référence à du suivi de connexion ? Où s'applique-t-il ?

Exercice 14 Proposer une règle qui autorise le trafic depuis l'extérieur (partie de droite) vers l'intérieur (partie de gauche) que si elles ont été initiées par le réseau interne. Vous indiquerez la commande dans votre compte-rendu ainsi que le test et son résultat pour prouver son bon fonctionnement.

Exercice 15 Quelle instruction permet de bloquer les paquets entrants invalides et de les compter ?

> **Note**
>
> Pour les compteurs, vous pouvez vous référer à l'URL suivante : https://wiki.nftables.org/wiki-nftables/index.php/Counters

Exercice 16 Quelle instruction permet de compter les demandes de connexion provenant de l'extérieur à destination du serveur web interne ?

Exercice 17 Comment afficher la valeur du compteur précédemment défini ?