Configuration du service iptables

1 Présentation

Un **pare-feu** (ou **Firewall**) est un dispositif logiciel permettant de filtrer les paquets réseau afin de mettre en place une politique de sécurité. Un pare-feu peut être avec états (*stateful firewall*) (il mémorise l'état des connexions, en vérifie la conformité et applique des règles adaptées) ou sans état (*stateless firewall*) (il applique des règles sur chaque paquet de manière indépendante). Plus d'information ici [1].

Le pare-feu linux (appelé `iptables`) est sans état. Les règles de filtrage sont regroupées dans des chaînes elles mêmes placées dans des tables (`filter`, `nat`, `mangle`). La table `filter` contient trois chaînes (ou plus) :

- `INPUT` : pour les paquets entrants dans la machine,
- `OUTPUT` : pour les paquets générés localement,
- `FORWARD` : pour les paquets routés à travers la machine.

Lorsqu'un paquet traverse une chaîne, les règles sont testées dans l'ordre les unes après les autres. Une règle sélectionne un paquet en fonction de critères (protocole, adresses, type, etc.) et lui applique une **cible** (`ACCEPT`, `DROP`, `QUEUE` ou `RETURN`). Si une règle est appliquée, le traitement de la chaîne est terminé. Si les règles ne sont pas applicables, la cible par défaut de la chaîne est utilisée (faites `man iptables` pour plus de précision).

Structure classique :

- la chaîne `INPUT` regroupe les règles de filtrage des paquets entrants. Chaque règle code un droit, c'est-à-dire un paquet accepté dans un certain contexte (cible `ACCEPT`).
- La cible par défaut de la chaîne `INPUT` est fixée à `DROP`. Donc, tout ce qui n'est pas **accepté** (par une règle) est **refusé** (par la cible de la chaîne).

2 Quelques exercices sur `client0`

Placez vous dans le `client0` et commencez par supprimer les règles de la table `filter` :

```
iptables -t filter -F
```

Mettez en place ces politiques de filtrage (attention, entre chaque exercice, repartez d'une base vierge) :

- Ajoutez des règles à la chaîne `INPUT` (commande `iptables`) pour interdire certains protocoles (par exemple `ssh` à certains clients (par exemple `client1`). Testez le FW en analysant les ports ouverts de votre machine à partir de la source avec la commande `nmap`.

```
dnf -y install nmap
nmap client0    # exécuté sur client 1
```

- Ajoutez des règles à la chaîne `INPUT` (commande `iptables`) afin d'interdire complètement l'accès à votre machine à partir d'un client particulier.
- Essayez de sauvegarder un jeu de règles en utilisant la clause `save` du service `iptables` :

```
/usr/libexec/iptables/iptables.init save
```

1. http://fr.wikipedia.org/wiki/Pare-feu_(informatique)

Elles seront automatiquement restaurées au démarrage du service `iptables` (voir le fichier `/etc/sysconfig/iptables`).

3 Quelques exercices sur `VM`

- Placez vous dans `VM`.
- Commencez par supprimer les règles de la table `filter` :

```
iptables -t filter -F
```

- Ajoutez une règle à la chaîne `FORWARD` de votre machine principale (`VM`) afin de limiter l'accès au WEB des postes clients (par exemple seuls les serveurs google seraient accessibles : `dig www.google.fr`).