Sécurité Linux – NetFilter – IpTables

I► IPTABLES est un mécanisme FireWall reposant sur un système de tables :

La table **FILTER** permet de filtrer les paquets réseaux. Tout paquet entrant est surveillé et rediriger en entrée ou en sortie. Cette table **FILTER** est composée de chaînes

- LA **CHAINE INPUT** :Analyse tous les paquets entrants dans la machine
- LA **CHAINE FORWARD** :Analyse les paquets entrants à passer d'une interface à l'autre dans le cas d'une passerelle réseau.autre, seulement dans le cadre d'une interface réseau servant de passerelle.
- LA **CHAINE OUTPUT** : Analyse les paquets sortants quand ceux-ci sortent de la machine.

Les règles que l'on peut appliquer à cette Tabe FILTER (policy) sont : **DROP**, **LOG**, **ACCEPT** et **REJECT**.

Voici un exemple de configuration :

```
#!/bin/bash
#FLUSH des tables
iptables -F
#Le trafic entrant est Dropé
iptables -P INPUT DROP
#Tout le traffic sortant est dropé également
iptables -P OUTPUT DROP
#On drop le forward aussi
iptables -P FORWARD DROP
#S'il y a une connexion ouverte en entrée, elle peut recevoir du trafic
```

```
iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
#S'il y a une connexion ouverte en sortie, elle peut recevoir du trafic
iptables -A OUTPUT -m state ! –state INVALID -j ACCEPT
#On accepte la boucle locale en entrée.
iptables -I INPUT -i lo -j ACCEPT
#Log des paquets entrants
iptables -A INPUT -j LOG
#Log des paquets forward
iptables -A FORWARD -j LOG
```

Autre exemple avec la table NAT qui permet de faire du NAT :

```
#!/bin/sh
# FLUSH de toutes les regles
iptables -t filter -F
iptables -t nat -F
#POLICY par defaut
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
# REJECT en sortie en sortie
#autorise l adresse 2 a faire du nat
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -d /0/0 -j SNAT –to-source 10.4.3.11
# les regles se placent sur l interface pour le reseau local
#iptables -A FORWARD -d 192.168.1.0/24 -j ACCEPT
#iptables -A FORWARD -s 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -d 192.168.1.3 -j ACCEPT
iptables -A FORWARD -s 192.168.1.3 -j ACCEPT
#autorise une remote connexion ssh
iptables -I INPUT -p tcp –sport 22 -j ACCEPT
iptables -I OUTPUT -p tcp –dport 22 -j ACCEPT
```