Filtrage avec Netfilter

Principe de fonctionnement

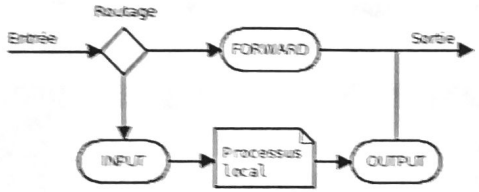
Netfilter permet d'effectuer du filtrage réseau sous Linux. Le filtrage s'effectue en fonction des informations contenues dans les en-têtes des trames, des paquets (adresses source et destination) et des segments (ports source et destination). Pour pouvoir indiquer les différentes règles au noyau, on dispose de l'utilitaire appelé **iptables**.

L'outil **iptables** utilise le concept de tables de règles, chaque table correspondant à une fonctionnalité d'examen du paquet.

- La table *filter* correspond au filtrage des paquets,
- la table *nat* concerne la traduction d'adresse,
- et la table *mangle* permet la modification des paquets.

Nous nous intéressons ici uniquement à la table *filter*.

Avec iptables, les différentes règles de filtrage sont organisées et regroupées dans des chaînes. Par défaut, il y a trois chaînes appelées : *INPUT*, *OUTPUT* et *FORWARD*. L'arrangement de ces chaînes est proposé sur le schéma suivant :



Les différentes chaînes sont consultées suivant la procédure suivante :

1. Quand un paquet arrive, le noyau décide de la destination de ce paquet : c'est la phase de routage.
2. Si le paquet est **destiné à la machine**, le paquet descend dans le diagramme et la chaîne **INPUT** est appliquée. Si le paquet passe cette chaîne, celui-ci sera transmis à l'un des processus locaux.
3. Si le routage décide que le **paquet est destiné à un autre réseau**, alors c'est la chaîne **FORWARD** qui est appliquée.
4. Enfin, les paquets **envoyés par un processus local** seront examinés par la chaîne **OUTPUT**. Si le paquet est accepté, celui-ci sera envoyé quelle que soit son interface de sortie.

Une chaîne est composée d'une liste de règles. Une règle décide de l'avenir d'un paquet en fonction de son en-tête. **Les règles d'une chaîne sont examinées les unes après les autres jusqu'à ce qu'une correspondance soit trouvée**. Finalement, si aucune correspondance n'est trouvée, la règle par défaut, ***policy***, est appliquée. On associe à chaque règle une action (appelée cible) à réaliser qui décide de l'avenir du paquet. Les fonctions principales sont les suivantes :

- **ACCEPT** : cette cible permet d'accepter les paquets.
- **DROP** : cette cible permet de refuser les paquets sans avertir le demandeur que sa demande de connexion a été refusée.

- **REJECT** : cette cible permet de refuser les paquets, mais en avertissant le demandeur que sa demande de connexion a été refusée en lui envoyant un paquet RESET (RST).

Consultation des règles de filtrage

Lister toutes les règles :

```
#iptables -L -n
```

L'option -n produit un affichage numérique des adresses IP et des numéros de ports. Par défaut, le programme essaie de les afficher sous forme de noms d'hôtes, de noms réseaux ou de services.

Lister les règles d'une chaîne :

```
#iptables -L INPUT -n
```

Modification de la *Policy*

Modification de la règle par défaut (seules les cibles ACCEPT et DROP peuvent utilisées) :

```
#iptables -P FORWARD DROP
```

Ajout d'une règle de filtrage

L'ajout d'une règle s'effectue avec l'option -A de l'outil **iptables**. La règle est ajoutée à la fin de la liste de règles de la chaîne concernée. L'option -j permet de spécifier la cible.

```
#iptables -A INPUT -s 192.168.1.0/24 -i eth0 -j ACCEPT
```

L'option -I permet d'insérer une règle en première position :

```
#iptables -I FORWARD -s 10.0.0.0/8 -d 192.168.2.5 -p tcp --dport 80 -j ACCEPT
```

ou à une position donnée (en 4ème position dans cet exemple) :

```
#iptables -I OUTPUT 4 -d 192.168.10.23/32 -j ACCEPT
```

Les principales spécifications sur lesquelles les règles peuvent s'appuyer sont les suivantes :

- -s : spécifie l'adresse IP source
- -d : spécifie l'adresse IP de destination
- -p : spécifie le protocole. Le protocole peut être tcp, udp ou icmp
- --dport : spécifie le port de destination (uniquement si -p est utilisée)
- --sport : spécifie le port source (uniquement si -p est utilisée)
- -i : spécifie le nom de l'interface physique à travers laquelle les paquets entrent
- -o : spécifie le nom de l'interface physique à travers laquelle les paquets sortent

Suppression d'une règle

L'option -D permet de supprimer une règle en indiquant le numéro de la règle à supprimer :

```
#iptables -D OUTPUT 4
```

Suppression de toutes les règles d'une chaîne :

```
#iptables -F INPUT
```

Suppression de toutes les règles de filtrage :

```
#iptables -F
```

Le suivi de connexion : *stateful firewalling*

Le suivi des «communications» se base sur trois états :

- **NEW** : correspond à la demande de communication TCP initiale, au premier datagramme UDP ou au premier message ICMP.

- **ESTABLISHED** : si une entrée de la table de suivi des communications correspond, alors le paquet appartient à une communication de type ESTABLISHED. Dans le cas du protocole TCP, on se réfère au bit ACK après qu'une communication ait été initiée. Dans le cas de datagrammes UDP, c'est l'échange entre deux hôtes et les correspondances de numéros de ports qui sont prises en compte. Enfin, les messages ICMP echo-reply doivent correspondre aux requêtes echo-request.

- **RELATED** : se réfère aux messages d'erreurs ICMP correspondant à une «communication» TCP ou UDP déjà présente dans la table de suivi.

D'un point de vue pratique, le module de suivi des communications sera activé grâce à l'option **-m state** de la commande iptables. L'option **–state** permet de spécifier l'état de la communication à considérer.

```
#iptables -A INPUT -i eth1 -m state -state ESTABLISHED,RELATED -j ACCEPT
```

Sauvegarde des règles de filtrage

La commande **iptables-save** permet d'enregistrer les règles de filtrage dans un fichier :

```
#iptables-save > /etc/regles_de_filtrage
```

Pour restaurer des règles enregistrées avec la commande iptables-save, il faut utiliser **iptables-restore** :

```
#iptables-restore < /etc/regles_de_filtrage
```