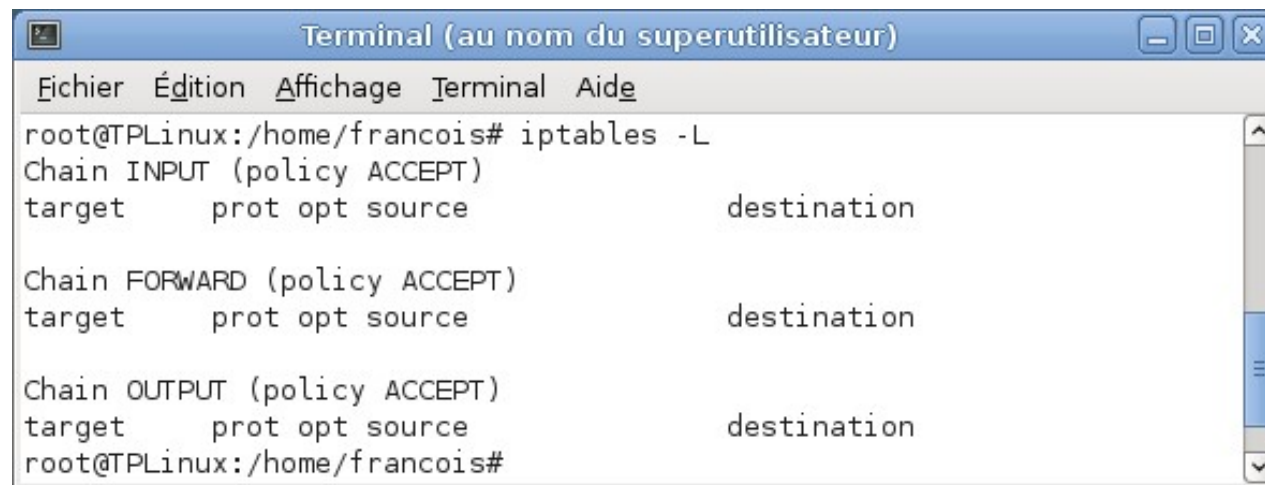


Pare-feu sous Linux : exemple d'IPTables

Installé par défaut (sinon `#apt-get install iptables`)

Pare-feu permissif (`#iptables -L` pour lister toutes les règles)

A screenshot of a terminal window titled "Terminal (au nom du superutilisateur)". The window has a menu bar with "Fichier", "Édition", "Affichage", "Terminal", and "Aide". The terminal shows the command `root@TPLinux:/home/francois# iptables -L` and its output. The output lists three chains: INPUT, FORWARD, and OUTPUT, all with a policy of ACCEPT. Each chain has a single rule with target "ACCEPT", protocol "all", source "0.0.0.0/0", and destination "0.0.0.0/0".

```
root@TPLinux:/home/francois# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@TPLinux:/home/francois#
```

Tout est autorisé depuis tout vers tout !

Pare-feu sous Linux : exemple d'IPTables

FILTER - - > fait appel à trois chaînes (fonction pare-feu la plus connue)

FORWARD : permet d'analyser et d'autoriser les trames à passer d'une interface à une autre, seulement dans le cadre d'une interface réseau servant de passerelle.

INPUT : filtrage des paquets entrant dans le pare-feu

OUTPUT : filtrage des paquets sortant du pare-feu

Remarque: une passerelle (*gateway*) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet

Pare-feu sous Linux : exemple d'IPTables

Quatre actions (cibles) possibles avec IPTables:

ACCEPT : les paquets sont acceptés et poursuivent leur « trajet »

DROP : les paquets sont ignorés systématiquement (aucune autre règle appliquée)

RETURN: stoppe un paquet traversant la chaîne dans laquelle la règle est placée

QUEUE : à oublier dans un premier temps ...

Pare-feu sous Linux : exemple d'IPTables

Construction des règles:

par exemple: **iptables -A <chaine> -s <source> -p <protocole> -d <destination> -j <cible>**

#iptables -L : liste toutes les règles

#iptables -D : suppression d'une règle

#iptables -A : ajout d'une règle

#iptables -P: configure temporairement le comportement de la chaîne avec la cible fournie

-s : source qui peut être une adresse IP ou un réseau (192.168.0.1, 192.168.0.0/24, 192.168.0.0/255.255.255.0, 0/0...)

-d : destination qui peut être une adresse IP ou un réseau (192.168.0.1, 192.168.0.0/24, 192.168.0.0/255.255.255.0, 0/0...)

Pare-feu sous Linux : exemple d'IPTables

-p : protocole utilisé. La plupart du temps ce sera TCP, UDP, ICMP ou ALL. Un numéro de protocole peut également être spécifié (TCP=6, UDP=17,... Cf fichier /etc/protocols) ou une liste de protocoles séparés par des virgules

-i : interface réseau d'entrée, ne fonctionne qu'avec les chaines INPUT et FORWARD (et aussi PREROUTING). Le caractère "+" peut être utilisé pour spécifier plusieurs interfaces du même type (eth+ signifie toutes les interfaces ethernet)

-o : interface réseau de sortie, ne fonctionne qu'avec les chaines OUTPUT et FORWARD (et aussi POSTROUTING). Le caractère "+" peut être utilisé pour spécifier plusieurs interfaces du même type (eth+ signifie toutes les interfaces ethernet)

Pare-feu sous Linux : exemple d'IPTables

Exemple de règles:

Règle temporaire par défaut pour la chaîne INPUT (chaîne action)

#iptables -P INPUT DROP

#iptables -P OUTPUT DROP



iptables bloque les paquets entrants et sortants

#iptables -P FORWARD DROP



pas de routage

NB: Par défaut, la commande iptables crée des règles dans FILTER (sauf si une autre table est spécifiée)

Pare-feu sous Linux : exemple d'IPTables

Exemple de règles:

(#iptables-restore < /etc/mesregles)

```
*filter

# accepte tous les paquets reçus dans le cadre de connexions déjà établies
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# autorise tout le trafic sortant
-A OUTPUT -j ACCEPT

# Autorise les demandes HTTP et HTTPS (sur les ports classiques) émises de n'importe où
-A INPUT -p tcp --dport 80 -j ACCEPT
-A INPUT -p tcp --dport 443 -j ACCEPT

# autorise les trames deping (ICMP, type 8)
-A INPUT -p icmp --icmp-type 8 -j ACCEPT

# log les refus d'IPTables (avec limitation à 5 entrées par mn max)
-A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7

# règles par défaut interdisant tout ce qui n'est pas autorisé explicitement
-A INPUT -j REJECT
-A FORWARD -j REJECT

COMMIT
```

Pare-feu sous Linux : exemple d'IPTables

Le cas de la cible RETURN:

`iptables -P INPUT DROP` 1°: indique une cible par défaut (DROP ici) pour la chaîne INPUT:
1 paquet non traité par une règle explicite suivra cette stratégie

(Remarque : « `iptables -A INPUT ...` » place une règle à la fin de toutes les règles de la chaîne INPUT)

`iptables -A INPUT -p tcp --dport 80 -j AUTRECHAINE` 2°: Tout paquet à destination du port 80 est
envoyé dans la chaîne AUTRECHAINE

`iptables -A INPUT -p tcp --dport 80 -j AUTRECHAINE2` 5°: Tout paquet à destination du port 80 est
envoyé dans la chaîne AUTRECHAINE2

`iptables -A AUTRECHAINE -p tcp --dport 80 --s 192.168.0.0/16 -j ACCEPT` 3°: Si la source de ce paquet à destination du
port 80 est 192.168.0.0/16 ou 10.10.0.0/16,
`iptables -A AUTRECHAINE -p tcp --dport 80 --s 10.10.0.0/16 -j ACCEPT` alors le paquet est autorisé à passer le PF

`iptables -A AUTRECHAINE -p tcp --dport 80 -j RETURN` 4°: Dans le cas contraire, le paquet est renvoyé dans la
chaîne INPUT et on passe à la règle suivante

`iptables -A AUTRECHAINE2 -p tcp --dport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT`
6°: Si le paquet intervient dans une connexion déjà établie sur le port 80, il est accepté

`iptables -A AUTRECHAINE2 -p tcp --dport 80 -j RETURN` 7°: Si le paquet intervient dans une connexion sur le port 80 mais
non établie au préalable il est rejeté

Pare-feu sous Linux : exemple d'IPTables

Remarque: les règles ne s'appliquent plus après un redémarrage



Pratique en phase de test (évite de perdre définitivement le contrôle de sa machine ...)

Comment charger une série de règles au démarrage?

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