Différents types de firewalls

Pare-feu niveau réseau. (iptables, paquet filter, . . .)

- ⋆ Firewall fonctionnant à un niveau bas de la pile TCP/IP
- ⋆ Basé sur le filtrage des paquets
- ⋆ Possibilité (si mécanisme disponible) de filtrer les paquets suivant l'état de la connexion

Intérêt : Transparence pour les utilisateurs du réseau

Pare-feu au niveau applicatif. (inetd, xinetd, . . .)

- ⋆ Firewall fonctionnant au niveau le plus haut de la pile TCP/IP
- ⋆ Généralement basé sur des mécanisme de proxy

Intérêt : Possibilité d'interpréter le contenu du trafic

Pare-feu des applications. (/etc/ftpaccess pour ftp, . . .)

- ⋆ Restrictions au niveau des différentes applications

Iptables (1/2)

- ⋆ Module du noyau Linux réalisant le filtrage de paquets (noyaux $\geq$ 2.4).
- ⋆ Améliorations en matière de filtrage et de translation d'adresses par rapport à Ipchains.

Fonctionnement :

À l'arrivée d'un paquet (après décision de routage) :

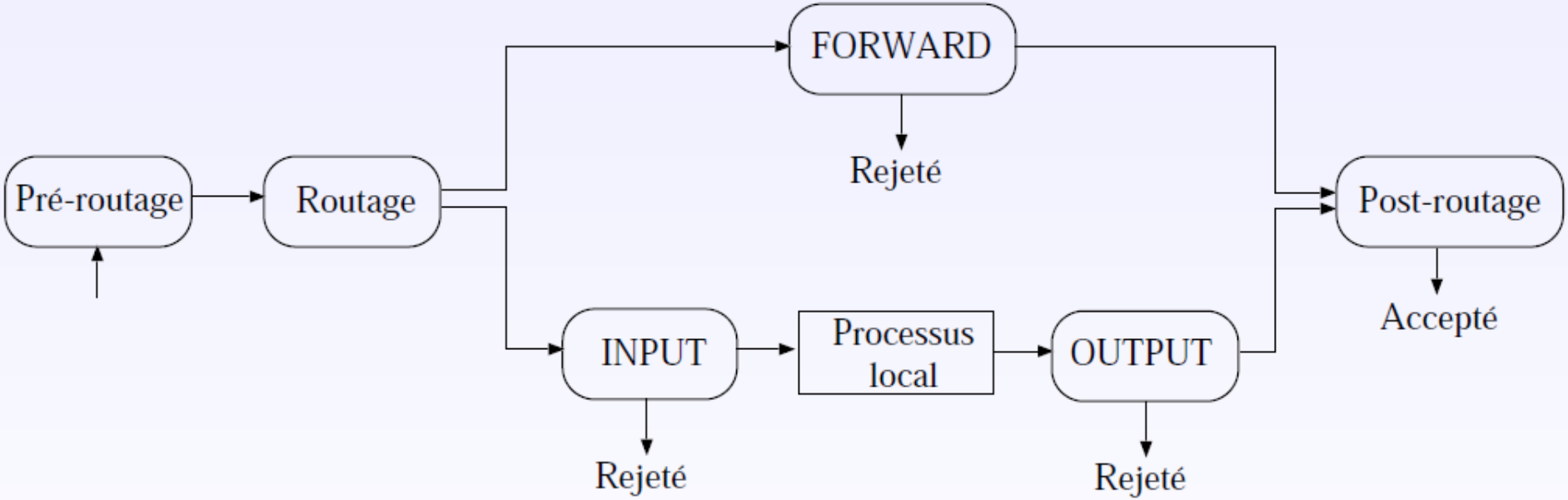
1: **Si** le paquet est destiné à l'hôte local **Alors**
2: il traverse la chaîne INPUT.
3: **Si** il n'est pas rejeté **Alors**
4: il est transmis au processus impliqué.
5: **Sinon**
6: **Si** le paquet est destiné à un hôte d'un autre réseau **Alors**
7: il traverse la chaîne FORWARD
8: **Si** il n'est pas rejeté **Alors**
9: il poursuit alors sa route

Tous les paquets émis par des processus locaux au routeur traversent la chaîne OUTPUT.

Iptables (1/2)

- Module du noyau Linux réalisant le filtrage de paquets (noyaux $\geq$ 2.4).
- Améliorations en matière de filtrage et de translation d'adresses par rapport à Ipchains.

Fonctionnement :



Iptables (2/2)

Fonctionnalités :

- ★ Filtrage de paquets
- ★ NAT
- ★ Marquage de paquets

Architectures :Trois tables de chaînes (FILTER, NAT et MANGLE).

FILTER (filtrage des paquets)		NAT (translation d'adresses)	
INPUT	paquet entrant sur le routeur	PREROUTING	NAT de destination
OUTPUT	paquet émis par le routeur	POSTROUTING	NAT de source
FORWARD	paquet traversant le routeur	OUTPUT	NAT sur les paquets émis localement

La table MANGLE sert au marquage des paquets

Iptables et filtrage(1/2)

- Filtrage des paquets IP, TCP, UDP ou ICMP
- Spécification de règle pour le rejet ou l'acceptation de paquet
- Utilisation de la table FILTER et des chaînes INPUT, OUTPUT et FORWARD
- Règles traitées de manière séquentielle : Le paquet sort dès qu'il rencontre une règle qui peut lui être appliquée

Exemples :

- Accepter tous les paquets en provenance de n'importe où et destinés à l'adresse du routeur 192.168.1.1.

```
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP
-j ACCEPT
```

- Accepter de router les paquets entrant sur eth0 tels que :

@source	@dest	P-source	P-dest
0/0	192.168.1.58	1024-65535	80

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o
eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT
```

Iptables et filtrage(2/2)

- Accepter un paquet ICMP “echo-request” (ping) par seconde

```
iptables -A INPUT -p icmp --icmp-type echo-request -m
limit --limit 1/s -i eth0 -j ACCEPT
```

- Accepter 5 segments TCP ayant le bit SYN positionné par seconde (permet d’éviter de se faire inonder)

```
iptables -A INPUT -p tcp --syn -m limit --limit 5/s -i
eth0 -j ACCEPT
```

- Accepter de router les paquets entrants sur eth0 tels que :

@source	@dest	P-source	P-dest
0/0	192.168.1.58	1024-65535	80 ou 443

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o
eth1 -p TCP --sport 1024:65535 -m multiport --dport
80,443 -j ACCEPT
```

Iptables et suivi des connexions

- Suivi des connexions disponible (*conntrack*)
- Quatre états possibles pour une connexion :

NEW .	Nouvelle connexion établie
ESTABLISHED .	La connexion analysée est déjà établie
RELATED .	La connexion est en relation avec une connexion déjà établie (ftp-data par exemple)
INVALID .	Le paquet reçu n'appartient à aucune des trois catégories précédentes.

Exemples :

- Autoriser tous les paquets émis par le routeur concernant des connexions déjà établies.

```
iptables -A OUTPUT -o eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Iptables et suivi des connexions

- Suivi des connexions disponible (*conntrack*)
- Quatre états possibles pour une connexion :

NEW .	Nouvelle connexion établie
ESTABLISHED .	La connexion analysée est déjà établie
RELATED .	La connexion est en relation avec une connexion déjà établie (ftp-data par exemple)
INVALID .	Le paquet reçu n'appartient à aucune des trois catégories précédentes.

Exemples :

- Autoriser le routeur à relayer tous les paquets reçus concernant de nouvelles connexions sur le port 22.

```
iptables -A FORWARD -p tcp -i eth0 --dport 22 --sport
1024:65535 -m state --state NEW -j ACCEPT
```

Exemples Iptables

Autorisation de connexions entrantes : ICMP, SSH, SNMP :

```
:RH-Firewall-1-INPUT - [0:0]
:RH-Firewall-2-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 162 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
```

Le reste est rejeté

Commandes Iptables

Les règles sont évaluées dans l'ordre, par défaut la table *FILTER* est vide et donc accepte tout.

policy ACCEPT

Permet d'accepter un paquet grâce à la règle vérifiée.

policy DROP

Rejet d'un paquet sans message d'erreur si la règle est vérifiée ("non ! j'en veux pas mais je dis rien à l'expediteur")

policy REJECT

Rejet avec un retour de paquet d'erreur à l'expediteur si la règle est verifiée ("un paquet recommandé de La Poste refusé par son destinataire").

policy LOG

Affiche le résultat vers la sortie standard.

Commandes Iptables

-A --append : Ajoute la règle à la fin de la chaîne spécifiée

Exemple :

 # iptables -A INPUT

-I --insert : Permet d'ajouter une chaîne dans un endroit spécifié de la chaîne ou en début de chaine

Exemple :

 # iptables -I INPUT --dport 80 -j ACCEPT

-R --replace : Permet de remplacer la chaîne spécifiée

Exemple :

 # iptables -R INPUT -s 192.168.0.1 -j DROP

-L --list : Permet d'afficher les règles

Exemples :

 # iptables -L

...

Commandes Iptables

-D --delete : Permet de supprimer une chaîne. On peut l'utiliser de 2 manières, soit en spécifiant le numéro de la chaîne à supprimer, soit en spécifiant la règle à retirer

Exemples :

 # iptables -D INPUT --dport 80 -j DROP

-F --flush : Permet de vider toutes les règles d'une chaîne

Exemple :

 # iptables -F INPUT

-P --policy : Permet de spécifier au noyau la politique par défaut d'une chaîne DENY, ACCEPT, REJECT, DROP ...

Exemple :

 # iptables -P INPUT DROP