Pare-feux

Yannick Chevalier
Université de Toulouse
CSA M1, Security

CONTEXTE

SÉCURITÉ D'UN RÉSEAU LOCAL

- Contrôle de la frontière entre l'extérieur d'un réseau et le réseau
- Séparation d'un réseau interne en différentes zones

FONCTIONNEMENT

- Périphériques physiques chargés de transformer des signaux externes information représentatble
- Noyau (Système d'exploitation) : interprète ces informations en paquets décrits par des protocoles connus

PARE-FEU

- Altération des actions par défaut définies par les protocoles
- But : protection, mais aussi nouvelles fonctionnalités
- ce cours : iptables

PLAN

STRUCTURE DES PAQUETS

TRAITEMENT DES PAQUETS

Interfaces

Périphérique

- dénoté par le système d'exploitation
- VLAN : périphérique ethernet annoté par la marque (un entier entre 0 et 4094) des paquets (*e.g.*, `eth0.456`)

Iptables

- `-i eth0.20` : sélection des paquets arrivant avec la marque 20 sur le périphérique `eth0`
- `-o eth1.30` : sélection des paquets sortant avec la marque 30 sur le périphérique `eth1`

Adresses

Adresse d'origine

- adresse de la machine ayant initié l'envoi du paquet
- iptables : `-s 192.168.0.3`

Adresse de destination

- adresse de la machine destinataire du paquet
- iptables : `-d 192.168.0.3`

Sous-réseau

Dans les deux cas il est possible de spécifier un sous-réseau (*e.g.*, `192.168.0.3/24`

Protocole et Port

Protocole

- **tcp**, **udp**,icmp, ou autre (`/etc/protocols`). Par défaut, tous les protocoles sont sélectionnés.
- iptables : `-p tcp`

Port

- port d'arrivée ou de sortie
- le protocole doit être précisé
- soit un port numérique, soit un nom défini dans `/etc/services`
- iptables : `-sport 80`, `-dport smtp`

Position dans la conversation

Problème

- on peut vouloir refuser une connexion entrante et accepter une connexion sortante
- mais la connexion sortante reçoit en général une réponse
- but : accepter la réponse tout en bloquant de nouvelles connections

Module state/conntrack

- `-m state` ou `-m conntrack` pour pouvoir spécifier un état
- `-state` pour spécifier l'état
- marche pour tcp **et** udp

Principaux états

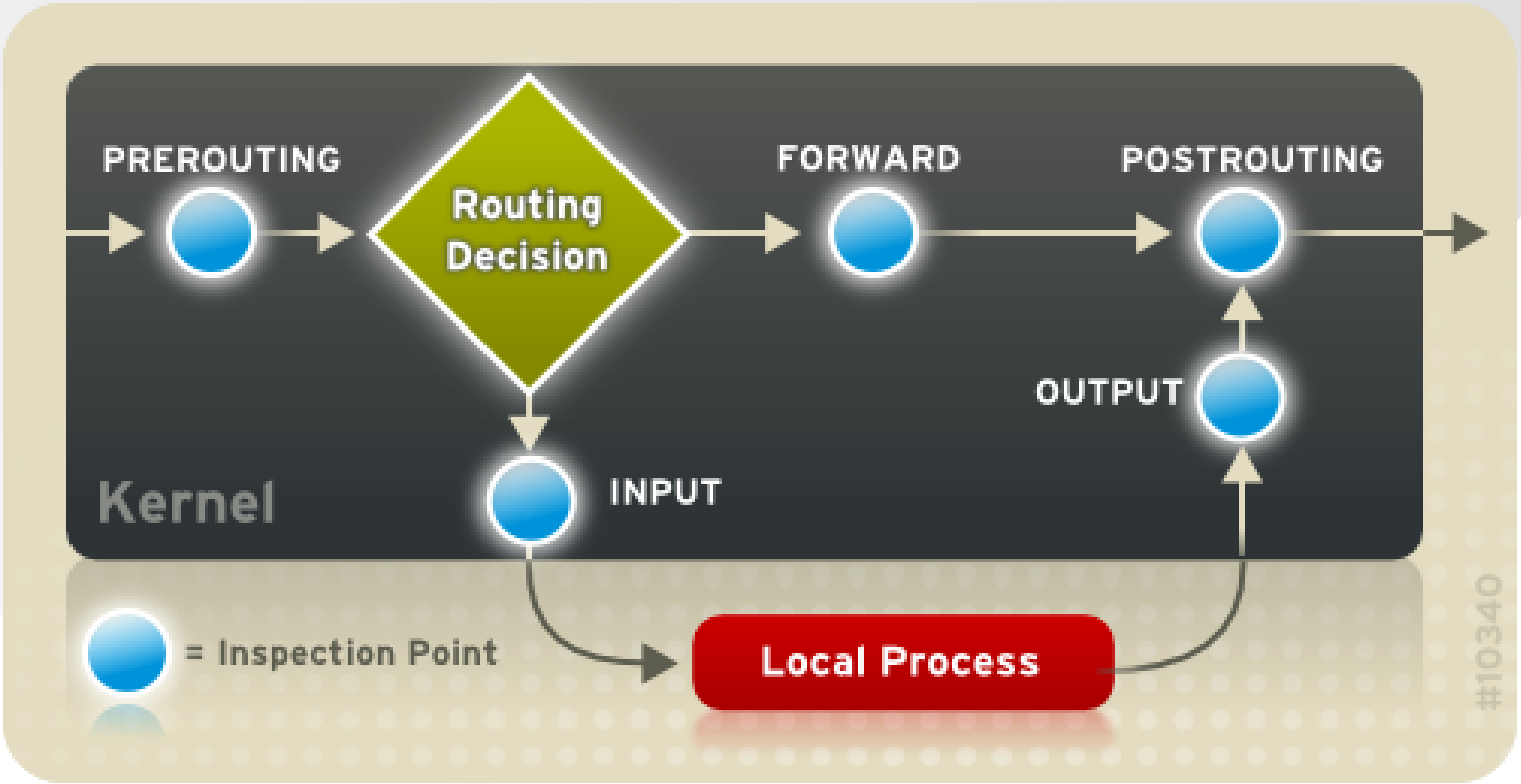
- `new` : nouvelle connection
- `established` : réponse à un paquet précédent
- `related` : reliée (données FTP par rapport à une connexion ftp) à une connexion existante

PLAN

STRUCTURE DES PAQUETS

TRAITEMENT DES PAQUETS

TRAITEMENT SIMPLIFIÉ



TABLES (IPTABLES)

BUT

- organisation du traitement suivant le but recherché
- pour la sécurité, on s'intéresse surtout à la table `filter`
- c'est la table par défaut

SPÉCIFICATION

- `-t nom`
- `mangle` : changement des paquets
- `nat` : Network Address Translation, voir plus loin
- `security` : MAC avec SELinux
- Il est possible de créer d'autres tables

CHAÎNES

CHAÎNES DE LA TABLE `FILTER`

- INPUT : traitement des paquets destinés à la machine courante
- OUTPUT : traitement des paquets issus de la machine courante
- FORWARD : traitement des paquets passant seulement à travers la machine courante (passerelle)

FONCTIONNEMENT DES CHAÎNES

- chaque chaîne est une liste de règles
- on peut ajouter une règle au début d'une chaîne avec `-I chaine` ou à la fin avec `-A chaine`
- la première règle applicable est choisie en partant du début

Règles

Principe

- chaque règle est associée à une chaîne dans une table
- elle décrit les caractéristiques des paquets auxquels elle va s'appliquer (*cf.* planches précédentes)
- elle contient l'action à effectuer lorsque les conditions sont remplies par le paquet
- spécification d'une action : `-j action`

Actions spécifiques pour le filtrage

- `accept` : laisse passer le paquet
- `reject` : bloque le paquet et signale le blocage par un paquet ICMP destination unreachable
- `drop` : bloque silencieusement le paquet

Exemple

But

interdire l'accès au réseau servi par eth0 à partir de l'extérieur (connecté à eth1)

Première version

```
iptables -I FORWARD -i eth1 -o eth0 -j REJECT
```

Seconde version (n'empêche pas les réponses)

```
iptables -I FORWARD -m state --state NEW -i eth1 -o eth0
-j REJECT
```

Autorise l'accès à une machine (règle à évaluer avant)

```
iptables -I FORWARD -i eth1 -d 10.0.0.2
```

Exemple

But

interdire l'accès au réseau servi par eth0 à partir de l'extérieur (connecté à eth1)

Première version

```
iptables -I FORWARD -i eth1 -o eth0 -j REJECT
```

Seconde version (n'empêche pas les réponses)

```
iptables -I FORWARD -m state --state NEW -i eth1 -o eth0
-j REJECT
```

Autorise l'accès à une machine (règle à évaluer avant)

```
iptables -I FORWARD -i eth1 -d 10.0.0.2 -j ACCEPT
```

Exemple

But

interdire l'accès au réseau servi par eth0 à partir de l'extérieur (connecté à eth1)

Première version

```
iptables -I FORWARD -i eth1 -o eth0 -j REJECT
```

Seconde version (n'empêche pas les réponses)

```
iptables -I FORWARD -m state --state NEW -i eth1 -o eth0
-j REJECT
```

Autorise l'accès à une machine (règle à évaluer avant)

```
iptables -I FORWARD -i eth1 -d 10.0.0.2 -j ACCEPT
```

Exemple

But

interdire l'accès au réseau servi par eth0 à partir de l'extérieur (connecté à eth1)

Première version

```
iptables -I FORWARD -i eth1 -o eth0 -j REJECT
```

Seconde version (n'empêche pas les réponses)

```
iptables -I FORWARD -m state --state NEW -i eth1 -o eth0
-j REJECT
```

Autorise l'accès à une machine (règle à évaluer avant)

```
iptables -I FORWARD -i eth1 -d 10.0.0.2 -j ACCEPT
```

La table NAT

Utilisation

- Partager une adresse IP entre plusieurs machines d'un réseau interne
- Exemple d'utilisation : box internet
- Sécurité :
  - permettre aux machines du réseau local de se connecter à Internet
  - mais par manque d'adresse publique, il est impossible à une machine externe d'initier une connexion vers une machine du réseau interne

Commande

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```