Les Firewalls

Gérald Masquelier
Antoine Mottier
Cédric Pronzato

03-01-2006

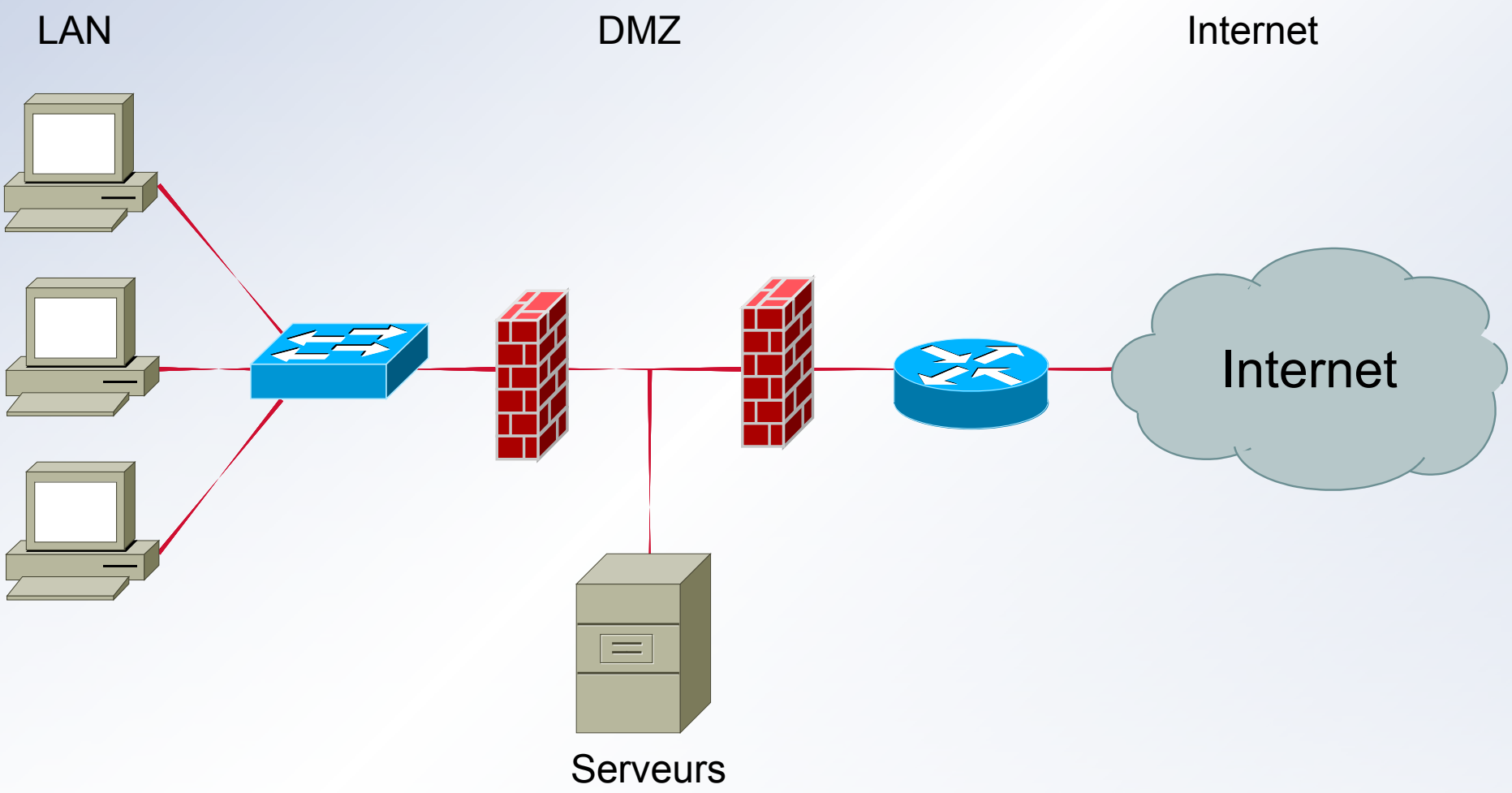
Plan

- Pourquoi un firewall ?
- Les différentes catégories de firewall
- Qualité de service
- NetFilter
- Les différents types de firewall (matériel / logiciel)

Pourquoi un firewall ?

- Réseau local
  - Partage de données
- Ouverture sur internet
  - Besoin d'échange avec l'extérieur
- Porte ouverte aux attaques
  - Vols de données, dénis de services (DoS),...
- Nécessité de protection => firewall
  - Se protéger des attaques externes et internes
- Firewall :
  - Concept
  - Protection : contrôle des flux
  - Gestion : priorisation des flux

Exemple d'application : DMZ



Les différentes catégories de firewall

- Firewall stateless
  - Contrôle paquet par paquet
  - Filtrage par adresses IP et par ports
  - Se base sur des ACL (Access Control List)
  - Limites :
    - Obligation d'ouvrir les ports > 1024 pour les connexions vers l'extérieur
    - Ne protège pas des attaques IP Spoofing et SYN flood

Les différentes catégories de firewall

- Firewall stateful
  - Prends en charge l'état de la connexion TCP
  - Vérifie la validité des paquets
  - Acceptation de connexions
  - Protège des attaques de types IP Spoofing et SYN Flood
  - Limites :
    - Nécessite des ressources supplémentaire

Les différentes catégories de firewall

- Firewall applicatif
  - Différencie les protocoles en fonction du contenu des paquets (couche 7)
  - Vérifie la validité des paquets
  - Limites :
    - Un module nécessaire par protocole
    - Très gourmand en ressources

Les différentes catégories de firewall

- Firewall authentifiant
  - Gestion de comptes utilisateurs
  - Haut niveau de sécurité
  - Limite :
    - Très gourmand en ressources

Qualité de service

- Optimisation de l'utilisation du réseau
  - réduction des coûts
- Classificateur de paquets
  - Aiguille les paquets dans les différentes files d'attentes
- Files d'attentes
  - Classless : non configurable
  - Classful : configurable

Exemple

```
tc class add dev eth0 parent 1: classid 1:1 htb rate 100kbps ceil 100kbps
tc class add dev eth0 parent 1:1 classid 1:2 htb rate 40kbps ceil 100kbps
tc class add dev eth0 parent 1:2 classid 1:10 htb rate 30kbps ceil 100kbps
tc class add dev eth0 parent 1:2 classid 1:11 htb rate 10kbps ceil 100kbps
tc class add dev eth0 parent 1:1 classid 1:12 htb rate 60kbps ceil 100kbps

tc filter add dev eth0 parent 1: protocol ip prio 1 handle 1 fw classid 1:1
tc filter add dev eth0 parent 1: protocol ip prio 1 handle 2 fw classid 1:2
tc filter add dev eth0 parent 1: protocol ip prio 1 handle 10 fw classid 1:10
tc filter add dev eth0 parent 1: protocol ip prio 2 handle 11 fw classid 1:11
```

iptables -A PREROUTING -i eth0 -t mangle ...

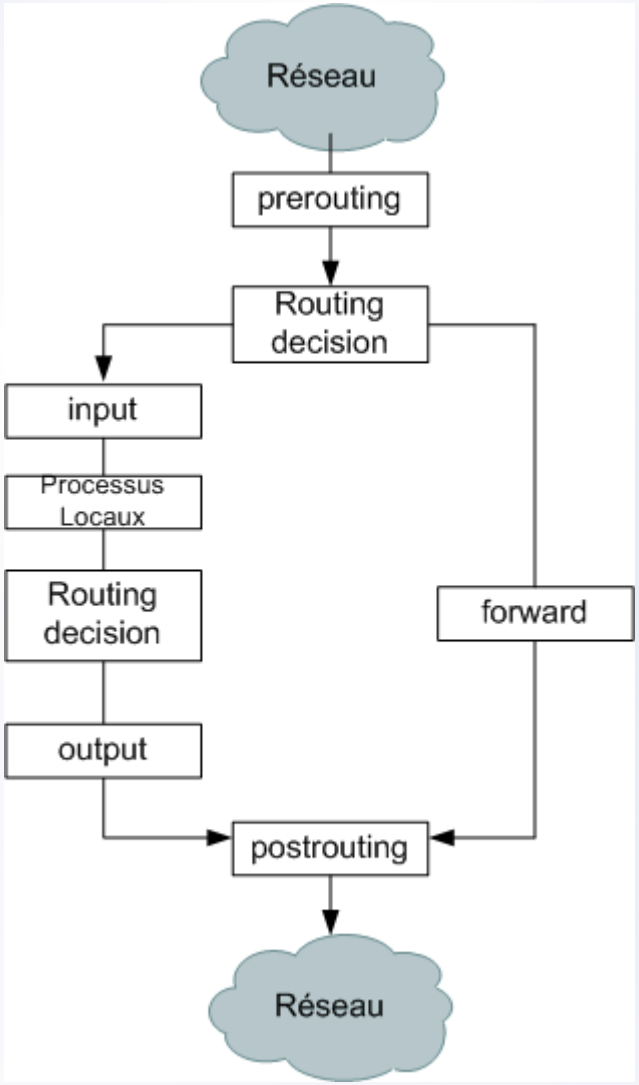
- -s 192.168.0.1 -j MARK --set-mark 1
- -s 192.168.0.1 -p tcp --dport 25 -j MARK --set-mark 11
- -s 192.168.0.1 -p tcp --dport 80 -j MARK --set-mark 10
- -s 192.168.0.2 -j MARK –ser-mark 2

NetFilter

- Intégré au noyau Linux depuis la version 2.4
- Iptables : commande de configuration
- Stateless de base
- Stateful avec un module externe
- Plus avec d'autres modules

NetFilter

- Fonctionnement
  - Tables
    - filter, nat, mangle
  - Chaînes
    - input, output, forward, prerouting, postrouting
  - Cîbles
    - accept, drop, reject, log, ulog, dnat, snat
- Modules
  - state
  - ipp2p



Exemple règles Iptables

```
#Suppression des régles prédéfinies
iptables -F
iptables -t nat -F
iptables -t mangle -F
#Suppression de toutes les régles de l'utilisateur
iptables -X
#Politique par defaut (tout rejeter)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# la loopback du firewall peut émetre dans tous les sens :
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# les connections invalides sont refusées :
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP
# les connections etablies ou assimilables sont acceptées en entrees :
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Le firewall peut emettre comme il veut sur ppp0 :
iptables -A OUTPUT -o ppp0 -j ACCEPT
```

Les différents type de firewall

- Matériel
  - Cisco PIX
- Logiciel
  - NetFilter
    - IPCop
  - Zone Alarm

Fin

Conclusion / Questions