

Firewall, Virus, Spam

Administration Système et Réseaux, Sécurité

Firewall, Spam, Virus

Philippe Harrand

¹Departement Informatique
Pôle Sciences et Technologie

²Direction Territoriale Sud Ouest
France Télécom

13 octobre 2007

Firewall

Généralités

Définitions

Mise en oeuvre iptables

Virus

Spam

Définition

Firewall

- ▶ Un firewall est un logiciel qui
 - ▶ Analyse les trames qu'il reçoit et prend une décision en fonction des adresses de couche 2, 3 et 4 => filtrage sans état
 - ▶ La décision peut être prise en fonction de l'état d'une connexion et/ou des drapeaux TCP => filtrage dynamique
 - ▶ La décision peut être prise en fonction du contenu de couche 7 => filtrage applicatif
- ▶ Un firewall protège tout un réseau

Pare-feux libres

- ▶ Linux Netfilter/Iptables, pare-feu libre des noyaux Linux 2.4 et 2.6
- ▶ Linux Ipchains, pare-feu libre du noyau Linux 2.2
- ▶ Packet Filter ou PF, pare-feu libre de OpenBSD
- ▶ IPFilter ou IPF, pare-feu libre de BSD et Solaris 10
- ▶ Ipfirewall ou IPFW, pare-feu libre de FreeBSD

Distributions Linux dédiées

- ▶ Smoothwall
Passerelle, pare-feu, proxy WEB, DNS dynamique, VPN, IDS, etc
Existe en libre et en commercial
- ▶ IPCop
Passerelle, pare-feu, proxy WEB et DNS, VPN, etc
- ▶ ...

Logiciels commerciaux

- ▶ Check Point FireWall-1
logiciel pare-feu commercial commercialisé par Check Point
- ▶ Seclutions AirLock
pare-feu applicatif commercial
- ▶ NuFW
logiciel pare-feu authentifiant en GPL pour environnement GNU/Linux, client sous licence commerciale pour postes clients Windows
- ▶ Pare-feu personnel de Windows XP
- ▶ Zone Alarm
- ▶ ...

Pare-feux dédiés

Il existe un certain nombre de boîtiers combinant souvent pare-feu et routeur

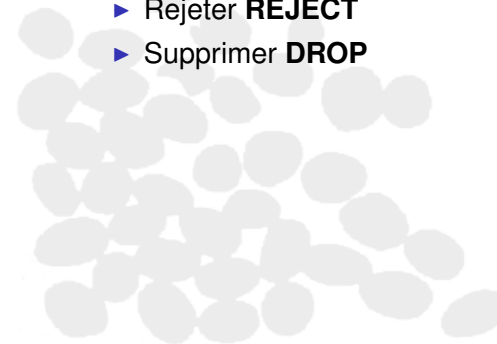
- ▶ Cisco Systems
- ▶ NetASQ
- ▶ Juniper Networks
- ▶ ...

Iptables



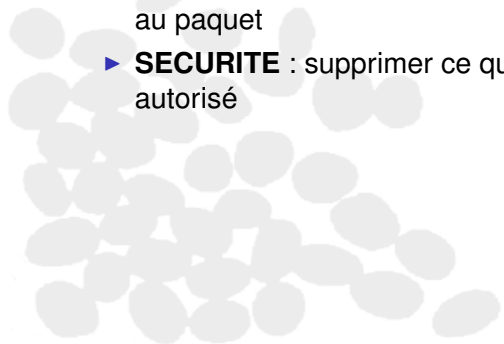
Décisions

- ▶ Accepter **ACCEPT**
- ▶ Rejeter **REJECT**
- ▶ Supprimer **DROP**

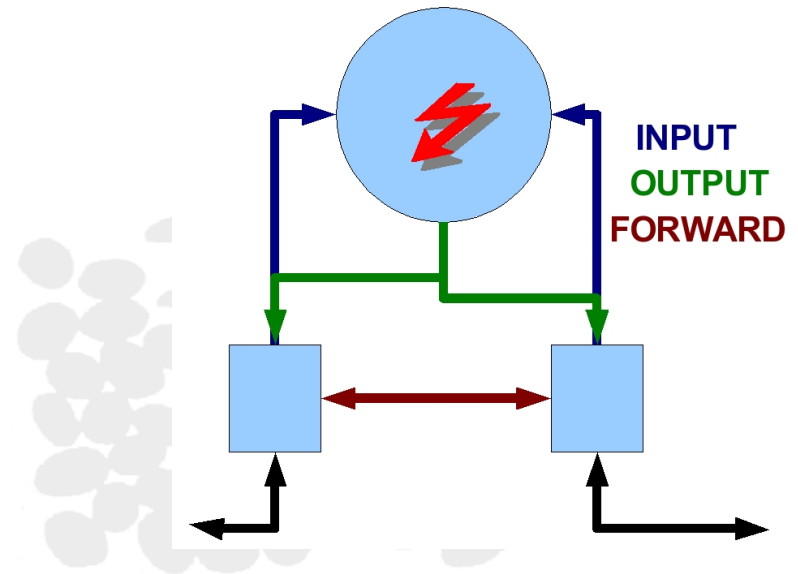


Stratégie

- ▶ **POLICY**
- ▶ Décision qui s'applique quand aucune règle ne correspond au paquet
- ▶ **SECURITE** : supprimer ce qui n'est pas explicitement autorisé



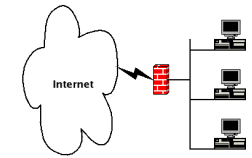
Types de flux



Types de flux

- ▶ **Entrant**
Les paquets à destination des processus internes à la machine
- ▶ **Sortant**
Les paquets issus des processus internes à la machine
- ▶ **TRANSIT**
Les paquets qui traversent la machine
Les paquets entrent par une interface et ressortent par une autre

Exemples



Vu du Pare-feu, Le trafic

- ▶ Internet => local est **FORWARD**
- ▶ local => Internet est **FORWARD**

Une requête

- ▶ "ping request" local => pare-feu est **INPUT**
- ▶ "ping request" Internet => pare-feu est **INPUT**
- ▶ "ping reply" pare-feu => Internet est **OUTPUT**
- ▶ "ping reply" pare-feu => local est **OUTPUT**

Principes

- ▶ Effacer toutes les règles existantes
- ▶ Définir la stratégie par défaut
- ▶ Définir les règles
 - ▶ Les règles sont parcourues dans l'ordre. Dès qu'une règle correspond (« match ») on « saute » (-j) vers la chaîne indiquée
 - ▶ Si aucune règle ne correspond on applique la stratégie par défaut

Table "filter"

- ▶ Chaque paquet passe à travers cette table
- ▶ A ajout, D supprime, I insère, F efface toutes les règles mais pas la stratégie par défaut, L liste
- ▶ Chaîne INPUT, OUTPUT ou FORWARD
- ▶ Critères de sélection du paquet
- ▶ Décision

```
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 10.2.0.0/16
-d !192.168.12.0/24 -sport 1024 :65535 -dport 80 -j REJECT
-reject-with icmp-host-unreachable
```

Filtrage à états

- ▶ différents états
 - ▶ NEW
 - ▶ ESTABLISHED
 - ▶ RELATED

- ▶ nécessite `-p tcp`

```
iptables -A FORWARD -i eth0 -o eth1 -s 10.2.10.134 -d 192.168.12.65 -p tcp --state ESTABLISHED, RELATED -j ACCEPT
```

Table NAT

- ▶ Permet la translation d'adresses
- ▶ Le premier paquet de chaque connexion passe à travers cette table
- ▶ 3 chaînes prédéfinies :
 - ▶ PREROUTING
l'adresse de destination est modifiée pour les paquets entrants AVANT la décision de routage
 - ▶ POSTROUTING
l'adresse source est modifiée pour les paquets sortants APRES la décision de routage
 - ▶ OUTPUT translation d'adresses de destination uniquement pour les paquets créés par cet ordinateur

Table Mangle

- ▶ transformation des options des paquets, comme la régulation de la bande passante, très utile pour lutter contre les attaques en « DOS »

Virus

Définitions

Sous le vocable virus on trouve des

- ▶ Virus
 - ▶ morceaux de codes binaires
 - ▶ qui s'insinuent dans un exécutable
 - ▶ et s'auto-répliquent
 - ▶ déclenchent une action à un instant T
- ▶ Vers
 - ▶ Exécutables autonomes
 - ▶ qui se diffusent par le Net
- ▶ Chevaux de troie
 - ▶ exécutables autonomes
 - ▶ exécutés comme démons
 - ▶ fournissent un accès distant au système

Antivirus

Méthodes de fonctionnement

- ▶ Méthode par signature
 - ▶ Recherche dans les fichiers d'une "signature"
 - ▶ contenue dans une liste de virus connus
 - ▶ sans effet sur les virus inconnus
- ▶ Méthode heuristique
 - ▶ Analyse du comportement des processus en cours
 - ▶ Gourmand en ressources
 - ▶ Faux positifs
- ▶ Les deux

SPAM

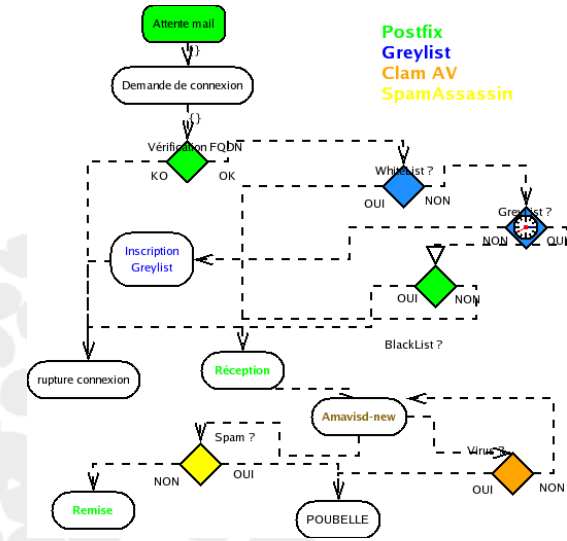
- ▶ Courrier non sollicité
- ▶ Généralement commercial
- ▶ Encombre le réseau et les boites aux lettres
- ▶ La loi française réprime cette pratique

Définitions

Anti spam

- ▶ La reconnaissance du nom de l'émetteur ne fonctionne plus
- ▶ Apprentissage
 - ▶ Reconnaissance de mots dans le texte
 - ▶ Sans effet sur les images
- ▶ Vérification FQDN
- ▶ GeyListing

Serveur Mail Antivirus/Antispam



Postfix
 Greylist
 Clam AV
 SpamAssassin