

Master 1 Informatique Université de Strasbourg

Rappels **NETFILTER/IPTABLES**

Sébastien Schmitt

Jean-Marc Muller



Exemple de filtrage sous Linux

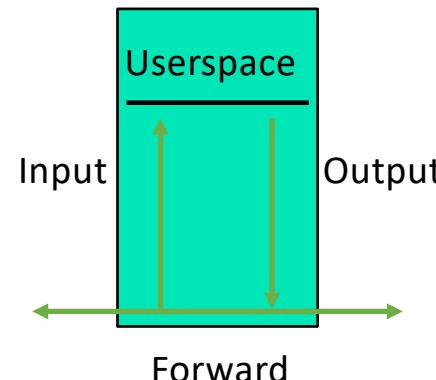
- Iptables & Netfilter

- Filtre de paquet statefull
- Niveau accès réseau, réseau et transport
- Partie utilisateur (Iptables)
- Partie noyau (Netfilter)
- Filtrage grâce aux règles
 - Renseignées par Iptables
 - Interprétées par Netfilter
- Ex : `iptables -A INPUT -p tcp -s 192.168.10.2 --sport 1024: --dport 21 -j ACCEPT`

Exemple de filtrage sous Linux

- Iptables & Netfilter

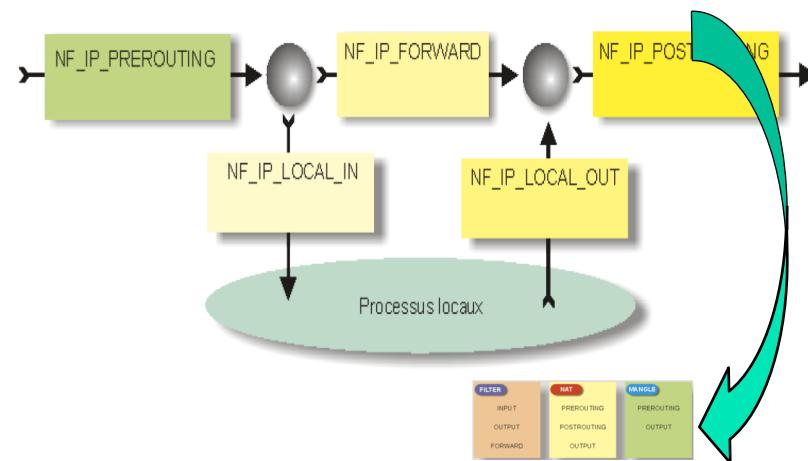
- Notion de chaîne
 - INPUT : vers le pare-feu
 - OUTPUT : à partir du pare-feu
 - FORWARD : à travers le pare-feu
- Les règles sont regroupées dans des chaines
- Elles sont appliquées par Netfilter quand un paquet les traversent
- Un paquet qui entre dans une chaîne
 - Teste les règles de la chaîne dans l'ordre où elles ont été saisies par l'administrateur
 - S'il en trouve une qui lui correspond
 - Obéit à la cible spécifiée et quitte la chaîne sans tester d'autres règles
 - Si aucune règle ne s'applique
 - Obéit à la politique par défaut



Exemple de filtrage sous Linux

- Iptables & Netfilter

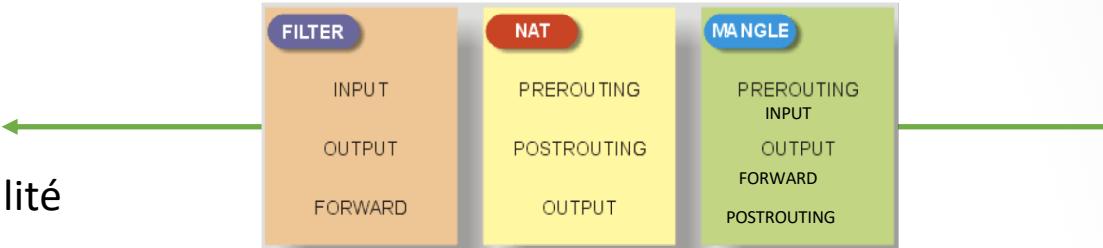
- Netfilter ajoute aux couches réseaux une série de points d'entrées (hook)
- Lorsqu'un paquet arrive sur un hook
 - Il sort de la pile réseau
 - Il est transmis à la chaîne correspondante
 - Il traverse le système d'évaluation
- Les tables



Exemple de filtrage sous Linux

- Iptables & Netfilter

- Les tables
 - Regroupement des règles par fonctionnalité
 - Mangle = modification de paquets
 - Nat = translation d'adresse
 - Filter = filtrage
 - Les tables sont traversées par plusieurs chaînes
 - La priorité d'évaluation des tables est la suivante : Mangle, Nat, Filter
 - Une table est peuplée d'une suite de règles
 - Quand un paquet est envoyé par un hook; il suit sa chaîne pour traverser les différentes tables
 - Il teste les règles de ces tables jusqu'à en trouver une et réintègre la couche réseau
 - Sinon il passe à la table suivante
 - Etc



Exemple de filtrage sous Linux

- Construction d'une règle
 - Quatre parties
 - ➔ Une table d'application (-t)
 - ➔ Une chaîne d'application (-A)
 - ➔ Un motif de reconnaissance (concordance ou « matches »)
 - ➔ Une cible représentant la décision à appliquer (-j)
 - Ex : iptables –t filter –A FORWARD –p tcp –dport 80 –j ACCEPT

Exemple de filtrage sous Linux

- Construction d'une règle

- Les motifs basiques

- -p protocole

- Ex : iptables –A INPUT –p **tcp**

- -s adresse source

- Ex : iptables –A INPUT –s **192.168.1.1**

- -d adresse destination

- Ex : iptables –A INPUT –d **192.168.1.2**

- -i interface d'entrée

- Ex iptables –A INPUT –i **eth0**

- -o interface de sortie

- Ex iptables –A INPUT –o **eth0**

Exemple de filtrage sous Linux

- Construction d'une règle

- Les motifs TCP

- --s port source

- Ex : iptables -A INPUT -p tcp --sport 22

- --d port destination

- Ex : iptables -A INPUT -p tcp --dport 22

- --tcp-flags adresse destination

- Ex : iptables -A INPUT --tcp-flags SYN,FIN,ACK SYN

- Les motifs UDP

- --s port source

- Ex : iptables -A INPUT -p tcp --sport 53

- --d port destination

- Ex : iptables -A INPUT -p tcp --dport 53

Exemple de filtrage sous Linux

- Construction d'une règle
 - Les motifs de gestion de suivi de connexion
 - ➡ -m state --state
 - Ex : iptables -A INPUT -p tcp -m state --state NEW -j ACCEPT
 - ➡ NEW
 - Un paquet qui engendre une nouvelle connexion
 - ➡ ESTABLISHED
 - Un paquet qui appartient à une connexion existante
 - ➡ RELATED
 - Un paquet qui est relié à mais ne fait pas partie d'une connexion existante
 - Ex : un paquet FTP qui établit une connexion de données

Exemple de filtrage sous Linux

- Construction d'une règle
 - Les motifs de gestion de plage IP
 - ➡ --src-range
 - ⇒ Ex : iptables -A INPUT -p tcp -m iprange --src-range 192.168.1.13-192.168.2.19
 - ➡ --dst-range
 - ⇒ Ex : iptables -A INPUT -p tcp -m iprange --dst-range 192.168.1.13-192.168.2.19
 - Les motifs de longueur de trame
 - ➡ --length
 - ⇒ Ex : iptables -A INPUT -p tcp -m length --length 1400:1500
 - Les modules de gestion de l'adresse MAC
 - ➡ --mac-source
 - ⇒ Ex : iptables -A INPUT -m mac --mac-source 00:00:00:00:00:01

Exemple de filtrage sous Linux

- Les cibles
 - ACCEPT
 - ➡ Le paquet est accepté et retourne directement dans la pile réseau pour poursuivre son chemin
 - REJECT
 - ➡ Le paquet est détruit et un message d'erreur ICMP est envoyé à l'expéditeur
 - DROP
 - ➡ Le paquet est détruit silencieusement
 - LOG
 - ➡ Une trace du paquet est consignée dans les logs et le paquet continue à être évalué dans la chaîne dans laquelle il est

Exemple de filtrage sous Linux

- Manipulation des règles, des tables et des chaînes
 - Les règles sont placées grâce à la commande « iptables » dans les chaînes et les tables
 - ➡ Ex : iptables -t filter -A FORWARD -p tcp -dport 80 -j ACCEPT
 - ➡ La règle est placée dans la chaîne FORWARD et dans la table filter
 - ➡ Elle sera évaluée par un paquet quand celui-ci traversera la table filter dans la chaîne FORWARD
 - Manipulation d'une chaîne
 - ➡ Créer une chaîne USERS que l'on peut utiliser en plus des autres et la relier aux chaînes existantes
 - ➡ iptables -N nouvelle-chaine
 - ➡ iptables -A FORWARD -i eth0 -o eth1 -j nouvelle-chaine
 - ➡ iptables -A nouvelle-chaine -p tcp -dport ssh -j ACCEPT
 - ➡ Effacer une chaîne vide (-X)
 - ➡ Changer la politique par défaut d'une chaîne (-P)
 - ➡ Lister les règles d'une chaîne (-L)
 - ➡ Retirer les règles d'une chaîne (-F)

Exemple de filtrage sous Linux

- Manipulation des règles, des tables et des chaînes
 - Les règles sont stockées en RAM l'une après l'autre dans l'ordre de saisie grâce à l'option -A qui signifie Add
 - ➡ Il faut pouvoir réorganiser les règles dans les chaînes
 - Ajouter une règle à la chaîne (-A)
 - Insérer une règle à une position donnée (-I)
 - Remplacer une règle par une autre à une position donnée (-R)
 - Supprimer une règle à une position donnée (-D)

Exemple de filtrage sous Linux

- Méthodologie de configuration d'un pare-feu
 - Pour ne pas avoir à réorganiser les règles manuellement
 - ➡ Taper les règles dans l'ordre attendu dans un fichier texte (script)
 - ➡ Exécuter le script à chaque reconfiguration
 - Lister les règles pour voir si tout semble correct
 - Sauvegarder l'ensemble des règles chargées en mémoire grâce à la commande
 - ➡ `iptables-save > sauvegardeiptables`
 - Les règles sont alors rechargées automatiquement au redémarrage du pare-feu
 - On peut aussi recharger l'ensemble de ces règles manuellement grâce à la commande
 - ➡ `iptables-restore < sauvegardeiptables`