UFR
de **mathématique** et d'**informatique**
Université de Strasbourg

TP n°3

Objectifs

- Mettre en œuvre une solution de filtrage sous Linux avec Netfilter/Iptables

1. Présentation

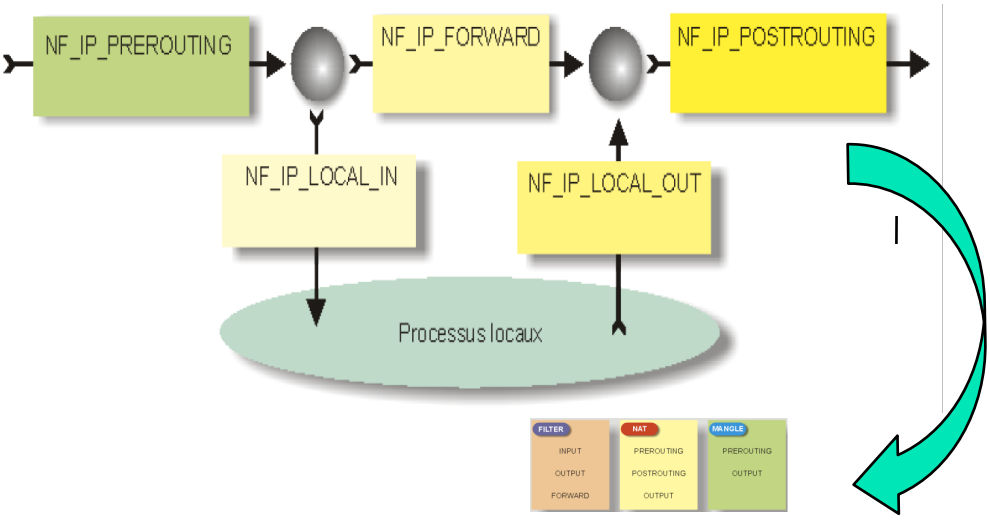
Iptables est un outil de gestion de pare-feu, intégré au noyau Linux (depuis la version 2.4). Le pare-feu en lui-même s'appelle Netfilter.

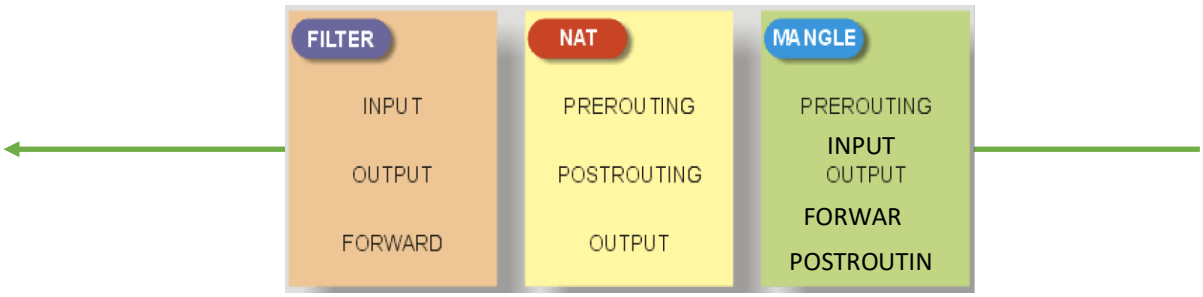
Netfilter offre plusieurs fonctionnalités : translation d'adresse, flitrage et modification de paquets.

Son fonctionnement est le suivant :

- Lorsqu'un paquet est reçu, il est transmis à Netfilter ;
- Netfilter va étudier ce paquet en se basant sur des règles définies par l'administrateur (grâce à la commande iptables) ;
- Un paquet arrivant sur l'interface réseau va traverser le noyau et subir plusieurs traitements au gré de tests effectués tout au long de son cheminement ;
- Si le paquet est par exemple destiné à être modifié par la fonctionnalité de translation d'adresse il va être traité dans une « chaîne de traitement » destinée à la translation d'adresse (ex : chaîne PREROUTING) et suite à cela poursuivre son chemin pour subir si nécessaire d'autres traitements ;
- Les traitements sont mis en œuvre au sein de tables ;
- Il existe trois tables :
    - filter : filtrage réseaux (ex : accepter/refuser un paquet)
    - nat : translation d'adresse (ex : sur une passerelle pour remplacer une adresse privée par une adresse public pour communiquer sur Internet)
    - mangle : modifier les paquets (ex : pour faire de la QoS)

Les tables sont traversées par les « chaînes » qui véhiculent les paquets de la pile réseau à travers le noyau du système d'exploitation.





La table filter (dans ce TP c'est la seule que nous allons manipuler)

La table filter est traversée par trois chaînes : INPUT, OUTPUT et FORWARD.

Quand un paquet arrive au niveau du pare-feu via une carte réseau, le noyau regarde la destination du paquet et prend une décision de routage.

Deux possibilités :

1. Le paquet est destiné à cette machine : il passe dans la chaîne INPUT, en direction des processus qui l'attendent.
2. Le paquet est destiné à une autre machine (située dans un autre réseau) et passe par la chaine FORWARD :

   Dans ce cas deux possibilités :

   a. Le forwarding est autorisé par le système : le paquet passe dans la chaîne FORWARD.
   b. Le forwarding n'est pas autorisé par le système : le paquet est effacé.

La chaîne OUTPUT enfin, concerne les paquets créés par la machine locale. Ces paquets passent par la chaîne OUTPUT afin de sortir vers le réseau.

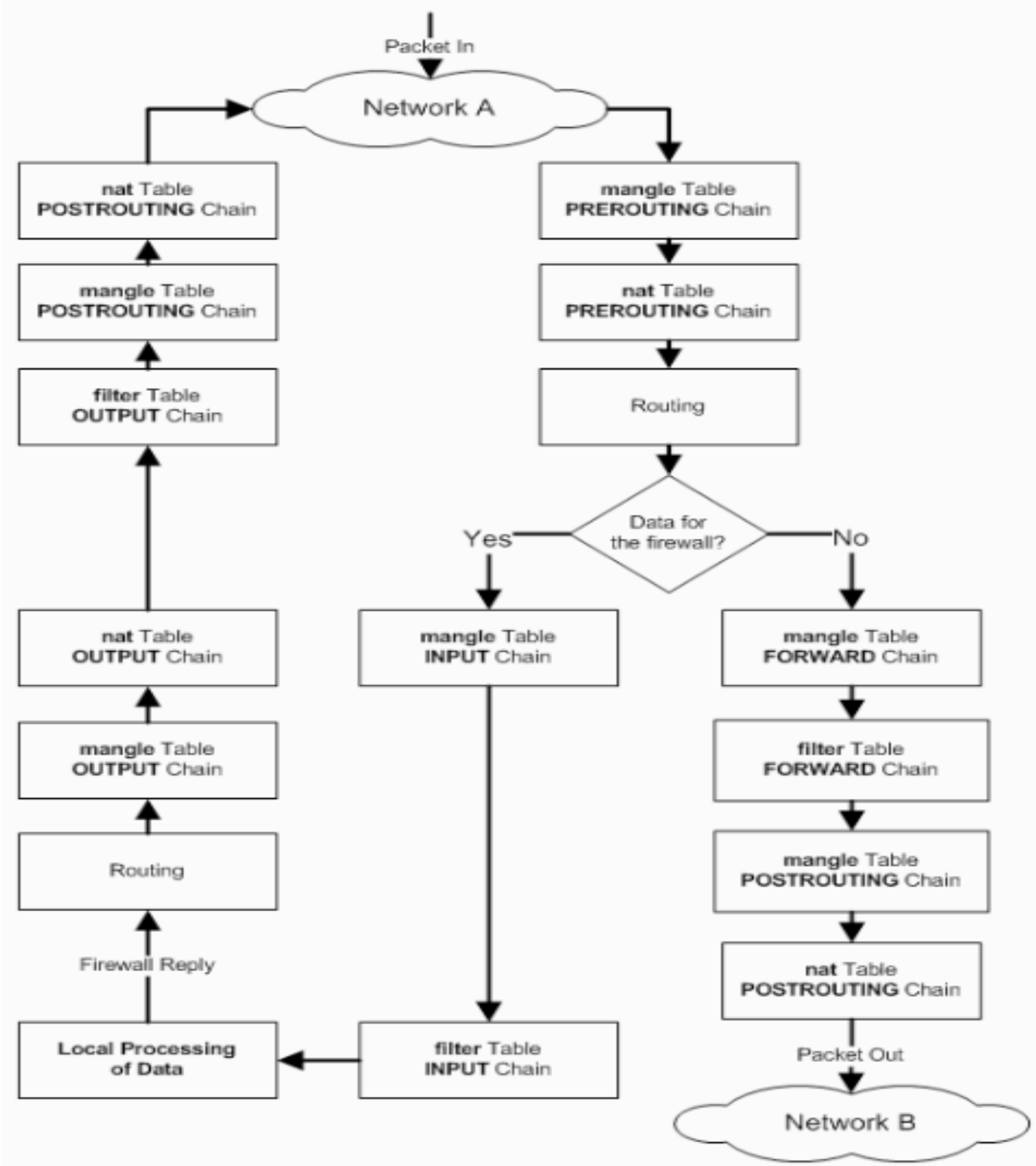
Chacune de ces chaînes va traverser la table filter afin de tester les règles contenues par la table. Les règles contenues dans la table vont être testées dans l'ordre les unes après les autres. Si une des règles testées correspond à notre paquet (motif de reconnaissance correspond à notre paquet) alors la « décision » de la règle s'applique à notre paquet et il ne teste alors plus les autres règles qui suivent dans la chaîne.

Si aucune règle ne correspond au paquet qui traverse une chaîne, il est traité par la politique par défaut de la chaine avant de quitter cette dernière (chaque chaîne possède une politique de filtrage par défaut).

Chacune des règles peut prendre plusieurs décisions pour un paquet qui correspond à son motif (pattern) de reconnaissance :

- ACCEPT : le paquet est accepté ;
- DROP : le paquet est refusé, on l'efface et on ne répond rien ;
- REJECT : le paquet est refusé et on signale le rejet à l'expéditeur ;
- Log : une trace du paquet est consignée dans les logs.

Si aucune règle ne correspond au paquet qui traverse une chaîne, il est traité par la politique par défaut de la chaine avant de quitter cette dernière (chaque chaîne possède une politique de filtrage par défaut).



2. Plateforme de TP

Le matériel nécessaire consiste en deux PC sous Linux connectés au réseau de la salle.
Ces deux PC permettront ainsi de tenter de se connecter l'un à l'autre et expérimenter les règles de filtrage entre ces deux machines.

3. Travail à réaliser

Exercice 0 : scan de ports

Installer l'outil nmap sur votre poste

Nmap est un logiciel générant des paquets de différents formats et permettant par ce biais de tester les ports ouverts sur une machine cible. Il permet par exemple de :

- *Voir tous les ports TCP ouverts sur une machine, utilisation de messages SYN, donc pas de log sur la machine cible :*
  - *nmap -sS 127.0.0.1*
- *Voir tous les ports UDP ouverts sur une machine :*
  - *nmap -sU 127.0.0.1*
- *Voir si une machine est sur le réseau (scan Ping) :*
  - *nmap -sP 127.0.0.1*
- *Scanner une plage d'adresses. Ici toutes les adresses de 192.168.0.0 à 192.168.0.255 :*
  - *nmap 192.168.0.0-255*
- *Connaitre le système d'exploitation de la machine (TCP/IP fingerprint) :*
  - *nmap -O 127.0.0.1*
- *Si nmap n'arrive pas à determiner la version, on pourra lui demander de nous donner une liste des systèmes qui pourraient potentiellement correspondre :*
  - *nmap -O --osscan-guess 127.0.0.1*
- *Scanner un port précis ou une plage de ports. Ici on scanne du port 0 au 80 et tous ceux supérieurs à 60000) :*
  - *nmap -p 0-80,60000 127.0.0.1*
- *Usurper l'adresse ip source. Ici on scanne 127.0.0.1, par l'interface réseau eth0, en se faisant passer pour 10.0.0.0 depuis le port 80 :*
  - *nmap -S 10.0.0.0 -g 80 -e eth0 -P0 127.0.0.1*
- *Modifier son adresse MAC :*
  - *nmap --spoof-mac 01:02:03:04:05:06 127.0.0.1*
- *Choisir un fichier de sortie pour y ecrire les résultats du scan :*
  - *nmap -oN resultat 127.0.0.1*
  - *nmap -oX resultat.xml 127.0.0.1*
- *Tracer les paquets et les données envoyés et reçus.*
  - *nmap --packet-trace -S 10.0.0.0 -eth0 127.0.0.1*

Question 1. Quels sont les ports qui sont ouverts sur votre propre machine ?

Question 2. Quels sont les ports qui ouverts sur la machine de votre voisin ?

Question 3. Quel est le système qui tourne sur la machine de votre voisin ?

Exercice 1 : la base pour comprendre

Question 4. Installez le logiciel wireshark sur votre poste

Question 5. Trouvez la commande permettant de visualiser les règles de filtrage (la table filter) définies sur votre machine.

Question 6. Visualisez les règles des autres tables.

Question 7. Cherchez les options à utiliser avec iptables permettant de produire des règles de filtrage s'appliquant aux paquets filtrés selon :

- l'adresse IP source
- l'adresse IP destination
- le protocole de couche transport (cf le fichier /etc/services pour la liste complète)
- le port destinataire
- le port source
- l'interface réseau d'entrée et celle de sortie

ainsi que l'option permettant de préciser l'action à faire (DROP, REJECT, ACCEPT).

Question 8. Affichez la politique par défaut de vos chaînes.

Question 9. Tentez de consulter le site web http://icube.unistra.fr. Est-ce possible ? Analysez le trafic avec Wireshark afin de voir ce qui est échangé entre votre machine et le serveur (au niveau Tcp).

Question 10. Modifiez la politique par défaut des chaînes INPUT et OUTPUT afin d'empêcher tout trafic de les traverser. Tentez de consulter le site web http://icube.unistra.fr.Est-ce possible ?

Question 11. Ajoutez une règle à la chaîne OUTPUT afin de permettre la sortie des requêtes http. Tentez de consulter l'url http://130.79.201.70. Est-ce possible ? Analysez le trafic avec Wireshark afin de déterminer ce qui est échangé entre votre machine et le serveur (au niveau Tcp).

Question 12. Ajoutez une règle à la chaîne INPUT afin de permettre le passage des réponses à vos requêtes HTTP. Tentez de consulter le site web http://icube.unistra.fr. Est-ce possible ? Pourquoi ?

Question 13. Ajoutez les règles nécessaires afin de permettre la résolution d'adresse grâce au DNS (UDP port 53). Vérifiez que vous êtes maintenant en mesure de consulter le site http://icube.unistra.fr.

Question 14. Ajoutez une règle à la chaîne OUTPUT afin d'interdire la sortie des requêtes http. Tentez de consulter le site web http://icube.unistra.fr. Est-ce possible ? Pourquoi ? (Listez l'ensemble des règles de filtrage de votre machine afin de vous aider).

Question 15. Supprimez la règle n°1 de la chaîne OUTPUT. Tentez de consulter le site web http://icube.unistra.fr. Est-ce possible ? Pourquoi ?

Exercice 2 : filtrage statique

Question 16. Empêchez toute connexion ssh (utilisant le protocole de transport TCP) sur votre machine en supprimant tout paquet dirigé vers le port correspondant.

Question 17. Essayez de vous connecter en ssh à la machine de votre voisin. Qu'observez-vous?

Question 18. Au lieu de les supprimer, essayez de rejeter ces paquets.

Normalement, toutes les connexions ssh à destination de votre machine sont maintenant rejetées.

Question 19. Faites en sorte de laisser votre voisin (et uniquement lui) accéder en ssh à votre machine.

N.B. La nouvelle règle (autorisant votre voisin) doit être insérée avant la première (rejetant toute connexion ssh) car les règles sont exécutées par défaut dans l'ordre de saisie

Question 20. Il peut être pratique de voir les numéros de chaque règle lorsqu'on les liste. Quelle option le permet ?

Question 21. Comment effacer une règle (la première règle par exemple) ? Et toutes les règles ?

iptables peut également accepter des fonctions supplémentaires via un système de modules.

Question 22. Pour spécifier que l'on veut utiliser un module particulier, quelle option utiliser ?

Question 23. Cherchez à l'aide de la commande man les différents modules existants.

Question 24. Utilisez par exemple le module multiport qui permet de spécifier plusieurs ports sources et/ou destinations dans une seule règle, afin de désactiver l'accès à vos ports 1 à 10 et 80 à 1023.

Question 25. Effacez à présent toutes les anciennes règles de la chaîne INPUT et de la chaîne OUTPUT

L'accumulation des règles se faisant assez rapidement, nous allons chercher un moyen d'organiser nos règles. Pour cela, nous pouvons créer nos propres chaînes utilisateurs.

Question 26. Créez une nouvelle chaîne utilisateur dans la table filter, et nommez la sshchain par exemple.

Question 27. Transférer l'étude de tous les paquets destinés à ssh (au port 22) depuis la chaîne INPUT vers sshchain. Ensuite, ajoutez les règles dans cette nouvelle chaîne autorisant uniquement votre voisin à se connecter en ssh sur votre machine.

Question 28. Changez la politique par défaut de la chaîne INPUT pour refuser tout paquet.

Question 29. A partir de toutes ces informations, essayez d'écrire une liste de règles pour autoriser votre voisin à se connecter sur les ports 22 (ssh) et loguez les tentatives de connexion ssh n'aboutissant pas.

Question 30. Supprimez toutes les règles de filtrage en remettant la politique par défaut de la chaine INPUT à ACCEPT. Filtrez maintenant les paquets sortants de votre machine : interdisez tout trafic web sortant (port 80 et port 443). Vérifiez que cela fonctionne.

Les attaques en « brute force ssh ou par dictionnaire » sont parmi les plus communes

Question 31. Trouvez un moyen de parer à ce type d'attaque grâce à une règle iptables

Question 32. L'applicatif « fail2ban » se base sur iptables et l'analyse des log pour contrer les attaques « brute force » ou « par dictionnaire ». Il permet notamment de gérer le service ssh. Installez cet applicatif et testez-le tout en observant les règles iptables de votre machine. Comment fonctionne-t-il ?

Exercice 3 : filtrage dynamique

Nous avons vu Netfilter travaillant paquet par paquet, sans se soucier des paquets précédents ni des suivants (filtrage statique sans états). Il n'a donc pas de notion de session ou de suivi d'un flux dans le temps. Il est mieux de procéder à un filtrage dynamique (avec suivi d'états) lié à ce qui s'est passé précédemment. Le principe d'un filtrage dynamique est de contrôler le trafic dans un sens pour en déduire ce qu'il faut laisser passer en retour.

Un module existe permettant de réaliser un filtrage dynamique en s'appuyant justement sur le type de flux (nouveaux flux, flux établis, flux liés à un autre flux, etc.).

Question 33. Quel est ce module ? Observez ses options en détail.

Question 34. Vérifiez que ce module de suivi de connexion est chargé, sinon chargez-le.

Question 35. Supprimez toutes les règles de vos chaînes. Modifiez la politique par défaut des chaînes INPUT et OUTPUT afin d'empêcher tout trafic de les traverser. Tentez de vous connecter à un site web connu

Question 36. Ajoutez une règle à la chaîne OUTPUT afin de permettre l'envoi de requêtes HTTP en utilisant le suivi de connexion.

Question 37. Ajoutez une règle à la chaîne INPUT afin de permettre le retour des réponses à vos requêtes HTTP en utilisant le suivi de connexion. Tentez de vous connecter au site web précédent.

Question 38. Visualisez le résultat du suivi de connexion grâce à /proc/net/...

Gestion du protocole FTP : on va appliquer le filtrage précédant sur un flux du protocole FTP. Le protocole FTP en mode actif est difficile à gérer car il utilise deux connexions. L'une sert à envoyer les commandes du client vers le serveur et l'autre connexion sert à envoyer les données du serveur vers le client. Dans son fonctionnement standard, un client FTP se connecte sur le port 21 du serveur FTP. Le client indique ensuite au serveur sur quel port il (le client) recevra les données. Le serveur FTP va alors établir une connexion depuis son port 20 vers le port (>1023) indiqué par le client.

Question 39. Installez un serveur FTP (par exemple proftpd) si ce n'est pas encore fait et chargez le module netfilter de gestion du protocole FTP

Question 40. Après avoir effacé toutes les règles précédentes, commencez par interdire tout paquet reçu.

Question 41. Testez les connexions FTP vers la machine de votre voisin. Qu'observez-vous ?

Question 42. Autorisez sur votre machine les paquets provenant du serveur et qui correspondent aux connexions (que le client connaît car c'est lui qui les a établis).

Question 43. Essayez ensuite (une fois connecté) un ls. Qu'observez-vous ? Pourquoi ?

Question 44. Autorisez les transferts de données en FTP depuis le serveur vers votre machine. Pour cela, il faut autoriser les connexions provenant du port 20 du serveur FTP et qui sont liées à la connexion initiée juste avant par notre machine (statut RELATED). N'oubliez pas de rajouter le statut ESTABLISHED;

En effet, la connexion n'aura le statut RELATED qu'un court instant, une fois identifiée par netfilter et par le client FTP, elle deviendra ESTABLISHED.

Essayez un nouvelle fois la commande ls après avoir ajouté le statut ESTABLISHED à la règle concernée.

Le suivi de l'état des connexions par netfilter peut se faire avec la commande iptstate ou en affichant le contenu du ficher /proc/net/ip_conntrack