Chapitre 2 : Les Pare-Feux

2.1 Définitions

Programme ou matériel chargé de protéger le réseau local du monde extérieur
Ensemble de composants appliquant une politique de contrôle d'accès entre deux réseaux.

- Empêche un intrus d'effectuer des accès non autorisé via internet sur un réseau privé
- Filtre les paquets entrant et sortant du réseau surveillé et les bloques le cas échéant.
- Il peut être incorporé à un routeur, une passerelle ou un ordinateur.
- Trois types principaux de pare-feu : pare-feu a filtrage des paquets, pare-feu applicatifs et pare-feu des applications

2.2 Plusieurs types de FireWire

pare-feu niveau réseau

pare-feu applicatif (proxy) :

pare-faux des applications

2.3 Le filtrage des paquets (filtrage réseaux)

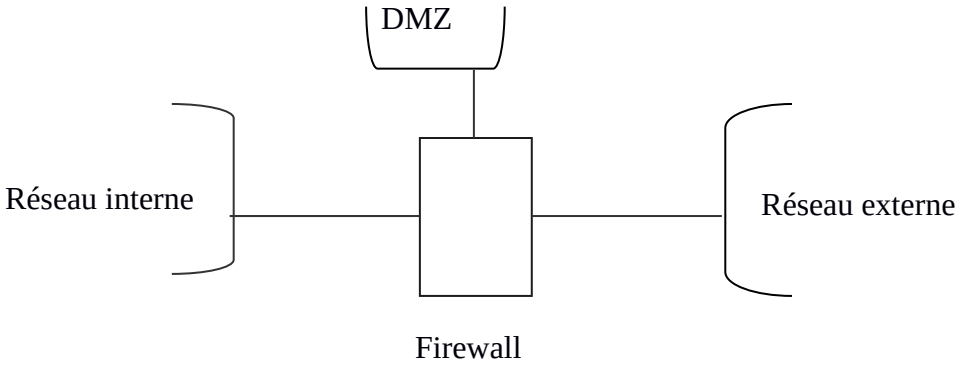
- Il existe deux types deux pare-feu à filtrage des paquets,
  - Pare-feu sans états (Stateless) : Analyse les paquets indépendamment les uns des autres.
  - Pare-feu avec états (Stateful) : vérifie que les paquets appartiennent a une session régulière, ce type de pare-feu possède une table d'états ou est stocké un suivi de chaque connexion établie ce qui permet au pare-feu de prendre des décisions adaptées au filtrage.
- Le filtrage des paquets autoriser/interdire le passage d'un paquet selon différents critères :

  Adresse IP Source
  Adresse IP Destination
  Port source
  Port destination
  Protocole (TCP, UDP, ICMP)
  Les interfaces d'entrée et de sortie

2.4 DMZ (zone démilitarisée)

Définition :

Une zone démilitarisée est un sous réseau se trouvant entre le réseau local et le réseau externe qui contient des serveurs interne (voir schéma ci-dessous).
La DMZ est une partie d'un pare-feu qui est un sous-réseau placé en passerelle entre un réseau à protéger (réseau interne) et un réseau externe non protégé.
Propriétés visées d'une DMZ : La zone démilitarisée est plus ouverte sur le réseau externe que le réseau interne, elle dessert les serveurs exposés à l'extérieur.



2.5 Mise en place d'un Firewall sous linux avec IPTABLES

Iptables :

Iptables est une solution complète de firewall linux (noyau 2.4) remplaçant ipchain (noyau 2.2) tournant sous le système GNU/Linux. Iptables permet de faire du fairewalling stateful, de la translation de port et d'adresse et du filtrage niveau 2.
IPtables utilise 3 tables :

- La tables de filtrage appelée **Filter**
- La tables de NAT appelée **NAT**
- La table de modification des entêtes appelé **Mangle** (peu utilisée)

2.5.1 La table Filter

C'est la table par défaut lorsque l'on en spécifie pas cette table contient toutes les règles de filtrage, il existe 3 types de chaines associées a cette table :

- **INPUT :** un paquet a destination du système entrant dans une interface (toujours en entrée d'interface)
- **OUTPUT :** un paquet généré par le système sortant par une interface (toujours en sortie d'interface).
- **FORWARD :** un paquet traversant le système (en entrée ou en sortie d'interface)

Les cibles disponibles dans cette table sont :

- **ACCEPT :** Permet d'accepter un paquet grâce à la règle vérifiée
- **DROP :** rejet d'un paquet sans message d'erreur
- **REJECT :** rejet avec retour de paquet d'erreur a l'expéditeur

2.5.2 La table NAT

La table NAT est utilisée pour la translation d'adresse ou la translation de port

Il ya deux type de chaines pour cette table :

- **PREROUTING :** qui permet de spécifier « à l'arrivée du firewall »
- **POSTROUTING :** qui permet de spécifier « à la sortie du firewall »

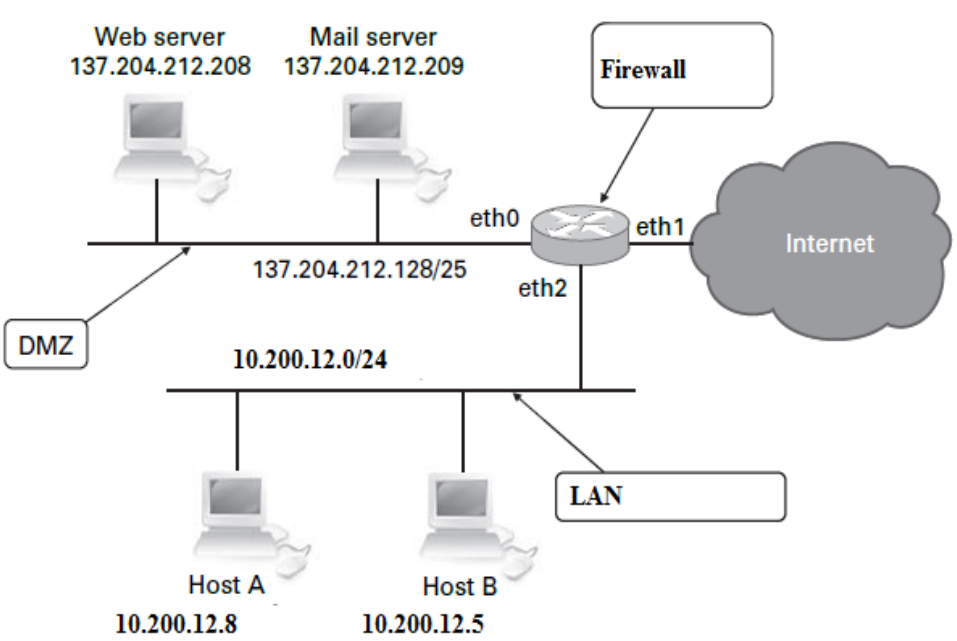
Il existe trois targets (cible) pour la table NAT :

- **SNAT :** permet de modifier l'adresse source du paquet
- **DNAT :** permet de modifier l'adresse destination du paquet
- **MASQUERADE** : une passerelle (gateway) transforme les paquets sortant passant par elle pour donner l'illusion qu'ils sortent de la passerelle elle même par un port alloué dynamiquement.

Iptables n'est pas livré avec une interface graphique les commandes et les règles sont passées en ligne de commande

iptables –A	Ajoute la règle a la fin de la chaine spécifiée
iptables –D	Permet de supprimer une chaine
iptables –R	Permet de remplacer la chaine spécifiée
iptables –I	Permet d'ajouter une chaine dans un endroit spécifié de la chaine
iptables –L	Permet d'afficher les règles
iptables –J	Défini l'action a prendre si un paquet répond aux critères de cette règle
iptables –A chain –p protocol	Ou –p peut être remplacé par –protocol . Le protocole est TCP, UDP ou ICMP ou l'un de ceux spécifies dans /etc/protocols On peut utiliser une valeur entière, par exemple 1 pour ICMP.
iptables –A chain –d interface	Spécifier l'adresse IP destination
iptables –A chain –s interface	Spécifier l'adresse IP source
iptables -F	vider la chaine complète
--dport	Spécifier le port destination
--sport	Spécifier le port source

2.5.3 Exemples avec IPTABLES



1) Bloquer tout le trafique sortant du réseau local (LAN) sauf pour une requête http
   # iptables –A OUTPUT –p TCP –o eth2 –i eth1 –dport !80 –j DROP

2) Bloquer tout le trafique sortant vers internet
   # iptables –A OUTPUT–j DROP

3) Bloquer tout le trafique entrant au réseau LAN vers les services SSH
   # iptables –A INPUT –p TCP –i eth2 –o eth1 –dport 22 –j DROP