Cours : Introduction aux Firewalls

1. Qu'est-ce qu'un Firewall ?

Un **firewall** est un dispositif de sécurité réseau conçu pour surveiller et contrôler le trafic réseau entrant et sortant selon des règles de sécurité prédéfinies. Il agit comme une barrière entre un réseau de confiance (interne) et un réseau non fiable (externe, comme Internet).

2. Direction et Types de Firewalls

Direction :

Ingress (entrant) : Filtrage des paquets entrant dans le réseau.

Egress (sortant) : Filtrage des paquets sortant du réseau.

Types de Firewalls :

1. Packet Filter (Filtrage de paquets) : Examine les paquets individuellement, sans état ni contexte.

2. Stateful Firewall : Suit l'état des connexions (TCP/UDP) et applique des règles en fonction de cet état.

3. Application/Proxy Firewall : Fonctionne au niveau des applications pour analyser et contrôler des protocoles comme HTTP ou FTP.

3. Fonctionnement d'un Firewall

Un firewall inspecte les paquets à l'aide de règles, puis décide de l'action :

NF_ACCEPT : Permettre au paquet de continuer.

NF_DROP : Bloquer et supprimer le paquet.

NF_QUEUE : Envoyer le paquet à l'espace utilisateur pour traitement.

NF_STOLEN : Le firewall gère entièrement le paquet.

4. Netfilter et Iptables

Netfilter:

- Un module du noyau Linux pour le traitement des paquets.

- Permet de manipuler les paquets à différents points (étapes d'accès).

- Utilisé pour des fonctions comme le filtrage de paquets, la traduction d'adresses (NAT), et le suivi des connexions.

Iptables :

- Une interface utilisateur pour configurer **Netfilter**.

- Les règles sont organisées dans des **tables** (filter, nat, mangle) et des **chaînes** (INPUT, FORWARD, OUTPUT).