FIREWALL (PARE-FEU)

On désigne sous le nom de Pare-feu (Firewall) un dispositif, placé au point de connexion d'un système d'information avec l'extérieur et qui permet de contrôler les flux entrants ou sortants.

Ce dispositif était initialement conçu pour empêcher le piratage et de cette finalité vient l'origine du terme employé.

Un firewall, ou pare-feu, est une barrière qui empêche la propagation d'un incendie. Il s'agit en général d'un système de portes complètement étanches, placées aux endroits stratégiques d'un bâtiment. Leur fermeture en cas d'incendie permet de contenir le feu dans des zones réduites, d'où il ne se propagera pas.

De la même façon, un firewall était à l'origine placé en un point stratégique d'un réseau, afin d'éviter que l'incendie que représentait la compromission d'une ou plusieurs machines du système ne se répande en direction des serveurs stratégiques.

Aujourd'hui, les fonctions d'un firewall se sont étendues, puisqu'il est aussi bien question d'empêcher la compromission de machines du réseau que d'empêcher la sortie de certaines informations du réseau local, voire l'utilisation de certains logiciels.

Un pare-feu permet de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes :

- **Une interface pour le réseau à protéger (réseau interne) ;**
- **Une interface pour le réseau externe.**

Par exemple prenons une entreprise qui souhaite protéger son réseau interne contre les menaces externes provenant d'Internet et limiter les accès aux ressources internes uniquement aux utilisateurs autorisés.

Elle pourra via son pare-feu mettre en place des règles :

- **Bloquer tout le trafic non autorisé : le pare-feu sera configuré pour bloquer tous les accès non voulus venant de l'extérieur du réseau, sauf ceux explicitement autorisés. Cela empêche les pirates informatiques d'essayer de se connecter au réseau de l'entreprise.**
- **Autoriser certains services : par exemple, seules les connexions vers le serveur web (port 443 pour HTTPS) sont autorisées. Les employés et les clients peuvent ainsi accéder au site web de l'entreprise, mais tous les autres services, comme le partage de fichiers, sont bloqués depuis l'extérieur.**
- **Filtrage de contenu sortant : l'entreprise ne souhaite pas que ses employés accèdent à certains sites. Le pare-feu peut être configuré pour bloquer l'accès à des sites spécifiques ou des catégories de sites (réseaux sociaux, jeux, etc.).**
- **Détection d'intrusion : si une attaque est détectée (par exemple, une tentative de déni de service), le pare-feu peut automatiquement bloquer les adresses IP suspectes et envoyer une alerte aux administrateurs réseau.**

Quel que soit le pare-feu utilisé, les règles de filtrage sont similaires. Il s'agit de préciser qui est la source, qui est la destination, de préciser le service et le protocole, et enfin d'autoriser ou bloquer le trafic.

Numéro	Protocole	IP Source	Port Source	IP Destination	Port Destination	Etat
1	TCP	ANY	ANY	@IP du server web	443	Autoriser
2	TCP / UDP	ANY	ANY	ANY	ANY	Bloquer
3	TCP	Adresse IP LAN	ANY	Adresse serveur Messagerie	SMTP	Autoriser

1. **Autoriser uniquement les connexions entrantes sur le 443 (HTTPS) pour le serveur web quel que soit l'IP source et le port source.**
2. **Bloquer toutes les connexions entrantes sur d'autres ports (ex : port 22 pour SSH, port 21 pour FTP) quel que soit l'IP source et le port source et quel que soit l'IP et le port de destination.**
3. **Permettre à n'importe quelle IP du LAN d'accéder aux services de messagerie (SMTP).**

- **L'IP source correspond à l'IP de la machine qui émet la trame.**
- **Le port source est le port ouvert par la machine qui émet la trame.**
- **L'IP de destination correspond à l'IP de la machine destinataire du message.**
- **Le port de destination est le port correspondant au service que l'on souhaite solliciter.**
- **Any signifie n'importe quelle adresse IP ou n'importe quel port suivant la colonne.**