FIREWALL

DÉFINITION

- Un *firewall* (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

  Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

I/ Qu’est-ce qu’un Firewall ?

Ici, un Fortigate 60E, modèle de Firewall de Fortinet

I/ Qu’est-ce qu’un Firewall ?

Le pare-feu est une passerelle filtrante qui protège un ordinateur ou un réseau des intrusions venues d'Internet.

Il filtre les paquets de données qui sont échangés.

Il est parfois traduit comme pare-feu, barrière de sécurité ou garde-barrière. Il est doté d’au moins deux interfaces, l'une destinée au réseau interne et l'autre au réseau externe.

I/ Qu’est-ce qu’un Firewall ?

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.
Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).

Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.

Le filtrage se fait selon divers critères. Les plus courants sont :

- L'origine ou la destination des paquets (adresse IP, ports TCP, etc...) ;
- Les options contenues dans les données (fragmentation, validité, etc...) ;
- Les données elles-mêmes (taille, correspondance à un motif, etc...) ;
- Les utilisateurs pour les plus récents ;
- Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte.

I/ Qu’est-ce qu’un Firewall ?

Le firewall fonctionne en fonction de la politique mise en place.

Il existe deux grandes politiques de sécurité :

- La plus sûre consiste à n'autoriser que les communications explicitement admises au nom du principe du moindre privilège.
- Interdire que les échanges explicitement prohibés.

La méthode la plus efficace est la première option, même si celle-ci est plus contraignante. Dans le cadre du pare-feu il s'agit d'appliquer les trois principales règles prédéfinies : accepter la connexion, la bloquer, refuser la demande de connexion sans prévenir l'émetteur.

I/ Qu’est-ce qu’un Firewall ?

Il existe plusieurs catégories de Firewall, le plus ancien étant le **pare-feu sans état** (ou stateless firewall), il fut introduit sur les routeurs.

Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.

Ces règles peuvent avoir des noms très différents en fonction du pare-feu :

- « ACL » pour Access Control List (certains pare-feux Cisco) ;
- politique ou policy (pare-feu Juniper/Netscreen) ;
- filtres ;
- règles ou rules… etc

I/ Qu’est-ce qu’un Firewall ?

Viens ensuite les **pare-feu à états** (appelé stateful firewall), ils vérifient la conformité des paquets à une connexion en cours.
C’est-à-dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens. Ils savent aussi filtrer intelligemment les paquets ICMP qui servent à la signalisation des flux IP.

Si les ACL autorisent un paquet UDP à passer, un tel pare-feu autorise la réponse sans avoir à écrire une ACL inverse.
Ceci est fondamental pour le bon fonctionnement de tous les protocoles fondés sur l'UDP, comme DNS par exemple. Ce mécanisme apporte en fiabilité puisqu'il est plus sélectif quant à la nature du trafic autorisé.

I/ Qu’est-ce qu’un Firewall ?

Le **pare-feux applicatif** est la dernière génération de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu.
Par exemple, ce type de pare-feu permet de vérifier que seul le protocole HTTP passe par le port TCP 80.
Ce traitement est très gourmand en temps de calcul dès que le débit devient très important. Il est justifié par le fait que de plus en plus de protocoles réseaux utilisent un tunnel TCP afin de contourner le filtrage par ports.

Le **pare-feux identifiant** réalise l’identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC, et ainsi suivre l'activité réseau par utilisateur.

II/ Son utilisation

Le pare-feu ou firewall sert naturellement à protéger un ou plusieurs ordinateurs contre des logiciels malveillants. Son utilité et son efficacité s'accroissent à mesure qu'il intègre des fonctionnalités nouvelles.

Il peut être utilisé en entré de réseau d’une entreprise, puis installer sur chaque poste des utilisateurs afin de maximiser la protection.

Il est d’ailleurs conseillé d’installer 2 pare-feux de constructeur différent à l’entrée du réseau d’une entreprise, et ainsi d'entourer la zone démilitarisée.

Une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

II/ Son utilisation

Les firewall, comme les technologies, évoluent au fil du temps.
Les nouveaux pare-feu sont dotés de multiples fonctionnalités qui décuplent leur utilité :

- Traducteurs d'adresse ;
- Protocole et filtrage des adresses IP ;
- Identifications connexion ;
- Détection des trafics anormaux grâce à l'intelligence artificielle ;
- Trivial File Transfer Protocol (TFTP) ou protocole simplifié de transferts de fichiers ;
- Contrôle des URL accessibles ;
- Serveur Internet de protocoles.

II/ Son utilisation

Il est nécessaire de le configurer avec soin pour lui donner un maximum d'efficacité.

Installer un pare-feu logiciel, et limiter l’ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.