Chapitre 3

La sécurité du Pare-feu (Firewall)

3.0.1 Introduction

Chaque système ou ordinateur connecté à l'Internet est susceptible d'être victime d'une attaque d'un pirate (attaquant) informatique. Ainsi, il est nécessaire de le protéger en installant un dispositif de protection (pare-feu, antivirus, réseaux privés virtuels, systèmes de détection d'intrusions, proxy, ...). Dans ce chapitre, on va s'intérésser aux techniques basées sur le pare-feu.

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall), est un système logique (sofware : IPCop, IP-Tables, Norton,. . .) ou physique (hardware : CISCO, Junipr,. . .) permettant de protéger un système, un ordinateur, ou un réseau d'ordinateurs, des intrusions indésirables 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.

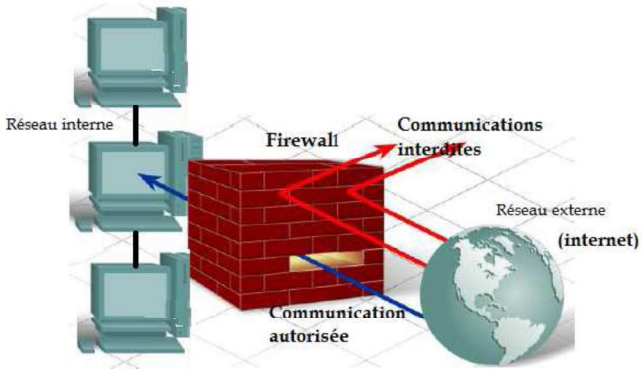

FIGURE 3.1 – Principe de firewall.

Le pare-feu représente ainsi généralement dans les entreprises un dispositif à l'entrée du réseau qui permet de protéger le réseau interne d'éventuelles intrusions en provenance des réseaux externes (souvent internet).

Le système pare-feu est un système reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- la machine soit suffisamment puissante pour traiter le trafic ;
- le système soit sécurisé ;
- aucun autre service que le service de filtrage de paquets ne

fonctionne sur le serveur.

Dans le cas où le système pare-feu est fourni dans une boîte noire «clé en main», on utilise le terme d'appliance.

3.1 Principe de fonctionnement

Un système pare-feu contient un ensemble de règles prédéfinies permettant :
- d'autoriser la connexion (allow) ;
- de bloquer la connexion (deny) ;
- de rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en oeuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :
- soit d'autoriser uniquement les communications ayant été explicitement autorisées : ≪Tout ce qui n'est pas explicitement autorisé est interdit≫ ;
- soit d'empêcher les échanges qui ont été explicitement interdits.

Un pare-feu peut faire :
1) Etre un guichet de sécurité : un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs.
2) Appliquer une politique de contrôle d'accès.
3) Enregistrer le trafic : construire des journaux de sécurité.

Ce que ne peut pas faire un pare-feu :
1) Protéger contre les utilisateurs internes (selon leurs droits).
2) Protéger un réseau d'un trafic qui ne passe pas par le pare-feu (exemple de modems additionnels)
3) Protéger contre les virus.
4) Protéger contre des menaces imprévues (hors politique).

3.2 Type de firewalls

Selon la nature de l'analyse et de traitements effectués par un Firewall, différents types de Firewalls existent. Ils se distinguent le plus souvent en fonction du niveau de filtrage des données auquel ils opèrent : niveau 3 (IP), niveau 4 (TCP, UDP) ou niveau 7 (FTP, HTTP, etc.) du modèle OSI.

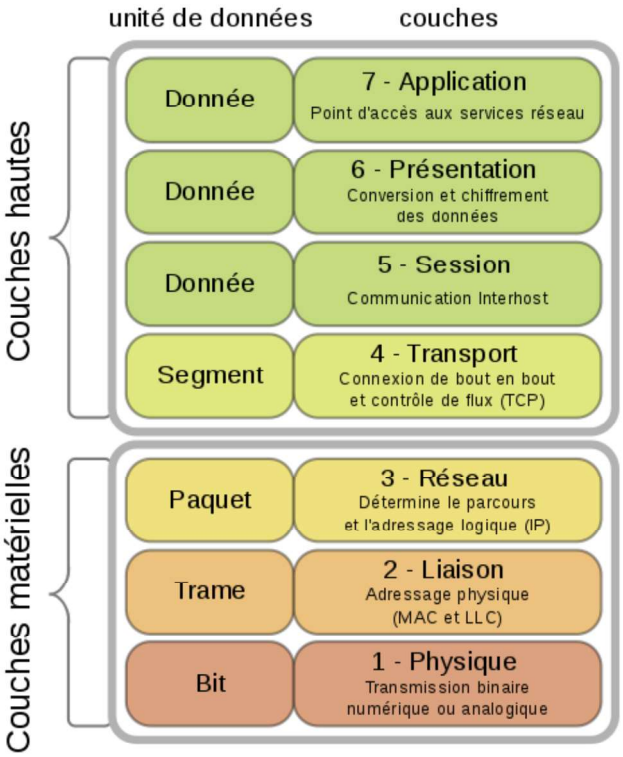

FIGURE 3.2 – Diagramme du modèle OSI (Open Systems Interconnection).

3.2.1 Filtrage simple de paquets

Ce sont les firewalls les plus anciens mais surtout les plus basiques qui existent. Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (stateless packet filtering). Ces firewalls interviennent sur les couches réseau et transport (3 et 4). Il analyse les en-têtes de chaque paquet IP de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure. En effet les machines d'un réseau relié à Internet sont repérées par une adresse appelée adresse IP.

Ainsi, lorsqu'une machine de l'extérieur se connecte à une machine du réseau local, et vice-versa, les paquets de données passant par le firewall contiennent les en-têtes suivants, qui sont analysés par le firewall :

- L'adresse IP de la machine émettrice
- L'adresse IP de la machine réceptrice
- Le type de paquet (TCP, UDP, ...)
- Le numéro de port (rappel : un port est un numéro associé à un service ou une application réseau)
- le port IP du service demandé
- le port IP du poste demandeur
- le flag (drapeau) qui précise si le paquet est une réponse à une demande de service, ou un demande d'établissement de connexion. Un flag ayant la valeur "ACK" (acknowledge) indique que le paquet fait partie d'une connexion en cours, un flag "SYN" définit une ouverture de connexion.

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Les ports reconnus (dont le numéro est compris entre 0 et 1 023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). Le tableau ci-dessous donne des exemples de règles (généralement appelées ACL, Access Control Lists) de pare-feu :

N°	Action	IP destination	Port dest.	IP source	Port src	Commentaires
1	Autorise (Accept)	172.16.0.0/16	>1023	Toutes	80	WEB vers réseau interne
2	Autorise	Toutes (any)	80	172.16.0.0/16	>1023	Réseau interne vers WEB
3	Bloque (Deny)	Toutes	Tous	Toutes	Tous	Défaut

FIGURE 3.3 – Exemple de filtrage simple par paquets.

Nous remarquons dans ce tableau de règles (ACL) que pour autoriser les postes du réseau local à accéder au Web, on est obliger de laisser ouverts le port 80.

3.2.2 Filtrage dynamique

Le filtrage dynamique fonctionne comme le filtrage statique au niveau de la couche 3 et 4 du modèle OSI, mais la différence du filtrage statique (fixe ou non-aléatoire) est qu'il implémente des tables d'état pour chaque connexion établie (state table). Ce genre de filtre bloque ou autorise les paquets en fonction :

- De leur contenu actuel
- Du contenu des paquets précédents

Ces fire-walls sont capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session :

– NEW : Un client envoie sa première requête.
– ESTABLISHED : Connexion déjà initiée. Elle suit une connexion NEW.
– RELATED : Peut être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
– INVALID : Correspond à un paquet qui n'est pas valide.

Les attributs gardés en mémoires sont les adresses IP, numéros de port et numéros de séquence des paquets qui ont traversé le firewall.

3.2.3 Filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4 ou 3). Le filtrage applicatif suppose donc une connaissance des applications présentes sur le réseau, et notamment de la

manière dont les données sont échangées (ports, etc.). Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application.

Un firewall effectuant un filtrage applicatif est appelé généralement passerelle applicative ou serveur mandataire(ou proxy), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

L'exemple le plus connu est le Proxy HTTP. Mais il existe d'autres types de serveurs proxy pour d'autres protocoles (SMTP, POP3, IMAP, FTP)

3.2.4 Pare-feu personnel

Dans le cas où la zone protégée se limite à l'ordinateur sur lequel le firewall est installé on parle de firewall personnel (pare-feu personnel). Ainsi, un firewall personnel permet de contrôler l'accès au réseau des applications installées sur la machine, et notamment empêcher les attaques du type cheval de Troie, c'est-à-dire des programmes nuisibles ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un pirate informatique. Le firewall personnel permet en effet de repérer et d'empêcher l'ouverture non sollicitée de la part d'applications non autorisées à se connecter.

3.2.5 Zone démilitarisée (DMZ)

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de cloisonnement des réseaux (le terme isolation est parfois également utilisé). Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, serveur de messagerie, serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de zone démilitarisée (notée DMZ, DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

Les serveurs situés dans la DMZ sont appelés **bastions** en raison de leur position d'avant-poste dans le réseau de l'entreprise. La politique de sécurité mise en oeuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

3.2.6 Limites des systèmes pare-feu

Un système Pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du Pare-feu.De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.

Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le Pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies. Par ailleurs, il est recommandé d'effectuer une veille de sécurité (en s'abonnant aux alertes de sécurité) afin de modifier le paramétrage deson dispositif en fonction de la publication des alertes.

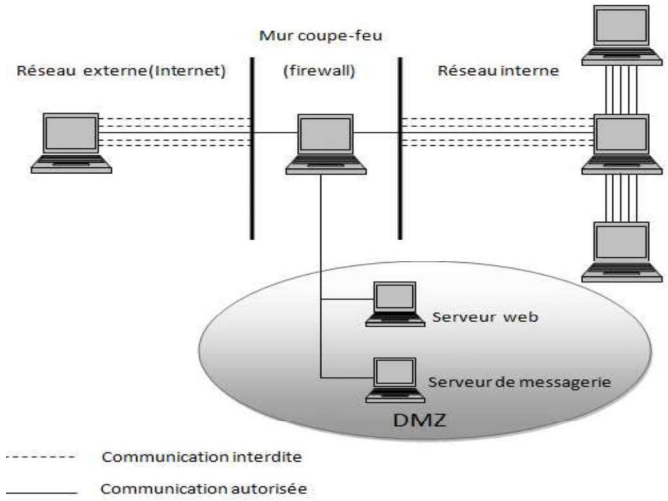

FIGURE 3.4 – Exemple d'une zone démilitarisée (DMZ).

La mise en place d'un Firewall doit donc se faire en accord avec une véritable politique de sécurité

3.2.7 Honeypots

Dans un réseau d'entreprise, le honeypot est un ordinateur créé pour détourner les attaques potentielles des pirates. Sa principale caractéristique est qu'il ressemble à un ordinateur mal sécurisé et doit attirer l'attention des hackers. En réalité, il s'agit d'une voie sans issu car ce PC n'est pas relié au reste des services réseaux de l'entreprise. Cette machine peut aussi servir de système d'alerte pour les administrateurs. Elle sera placée volontairement derrière les défenses (parefeu, routeur ; ...) du réseau.

3.3 Le choix d'un Firewall

La façon de configurer un Firewall et de le gérer est tout aussi importante que les capacités intrinsèques qu'il possède. Toutefois, lorsque le choix s'impose, on prendra en considération les critères suivants :

- La nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, vidéoconférence, etc.),
- Type de filtres, niveau de filtrage (niveau applicatif, niveau TCP, niveau IP, possibilité de combiner ces niveaux),
- Facilités d'enregistrement des actions et des événements pour audits future,
- Les outils et facilités d'administration (interface graphique ou lignes de commandes, administration distante après authentification de gestionnaire, etc.),
- Simplicité de configuration et de mise en oeuvre,
- Sa capacité à supporter un tunnel chiffré permettant éventuellement de réaliser un réseau privé virtuel (VPN pour Virtuel Private Network),
- La disponibilité d'outils de surveillance, d'alarmes, d'audit actif,
- Possibilité d'équilibrage de charges et de gestion de la bande passante de réseau,
- L'existence dans l'entreprise de compétences en matière d'administration du système d'exploitation du firewall,
- Son prix.

Chapitre 4

Réseaux privés virtuels (VPN)

4.1 Introduction

Les réseaux virtuels (VLAN - Virtual Local Area Network) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints (limités), cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN. Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN.

Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN.

Afin de sécuriser les échanges de données entre deux LAN, on peut recourir à deux alternatives :

- Relier les deux sites par une ligne spécialisée.
- Créer un réseau privé virtuel sécurisé autrement dit un VPN. On encapsule (en anglais tunneling) les données dans un tunnel crypté.

4.2 Définition d'un VPN

VPN (Virtual Private Network) correspond à une interconnexion sécurisée de réseaux locaux en utilisant un réseau public (ex : Internet) via une technique de "tunnel" c'est-à-dire que seuls les ordinateurs des réseaux interconnectés peuvent voir les données échangées.

4.3 Fonctionnement d'un VPN

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

Les Objectifs et caractéristiques des VPN sont : la confidentialité des données, l'intégrité des données, l'authentification et la gestion des clés.

4.4 Catégories de VPN

Il existe trois types de VPN :

- Le VPN d'accès

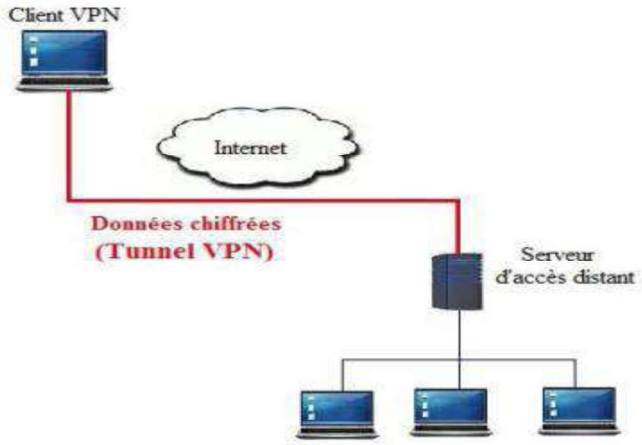

FIGURE 4.1 – Connexion VPN entre un client et un serveur.

Il est utilisé pour permettre _a des utilisateurs itinérants d'accéder au réseau de leurs entreprises. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.

- L'intranet VPN

Il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseaux est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

- L'extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et partenaires. Elle ouvre alors son réseau local à ces derniers, dans ce cas il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

4.5 Les protocoles de tunnelisation

Les principaux protocoles de tunneling sont les suivants :

- PPTP (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Tele-com et Shiva.
- L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.