

Les pare-feux

Plan du chapitre :

- Introduction
- Les pare-feux
- Fonctionnement d'un système pare-feu
- Les catégories des pare-feux
- Le pare-feu et le problème de trafic crypté
- Conclusion

1.1 INTRODUCTION

La technologie des pare-feux est apparue dans les années 80 pour palier à un nouveau problème de sécurité lié à l'émergence de l'Internet. En 1988, un employé de NASA Armes Research Center en Californie a envoyé un mémo par courrier électronique à son collègue qui a pu lire « Nous sommes actuellement attaqué par un virus Internet appelé *Morris Worm* ». Ce virus était la première attaque à grande échelle sur Internet. La communauté d'Internet a collaboré à la recherche de nouveaux moyens de protection contre ces nouvelles menaces. A la suite de cela des nouveaux produits de protection contre ces attaques sont apparus comme les anti-virus et les pare-feux. [1]

Et actuellement chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

Cette menace est d'autant plus grande que la machine est connectée en permanence à internet pour plusieurs raisons :

- La machine cible est susceptible d'être connectée sans pour autant être surveillée ;
- La machine cible est généralement connectée avec une plus large bande passante ;
- La machine peut être cible ne change pas ;

Donc et pour ces raisons là les pare-feux sont mis en œuvre.

1.2 Qu'est-ce qu'un pare-feu?

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant 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 [1] :

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

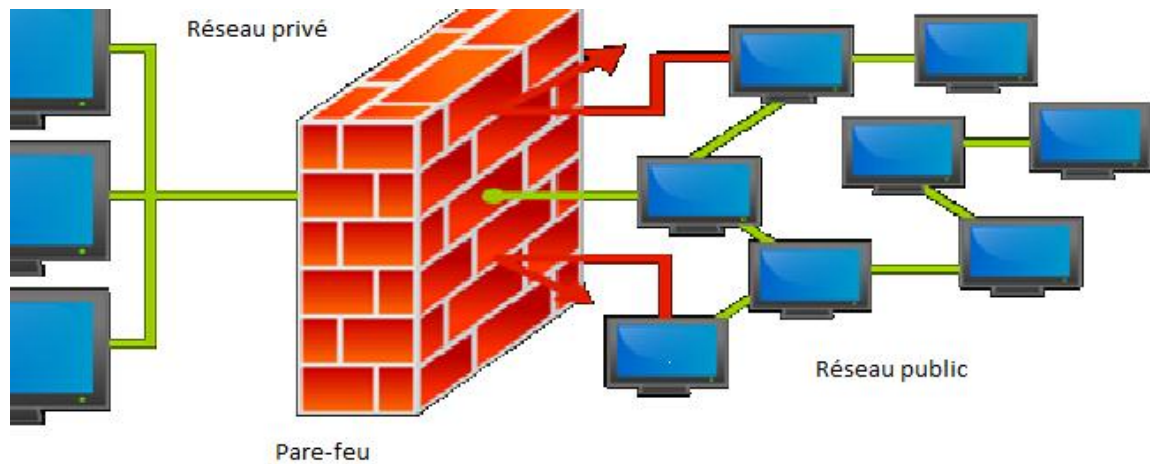


Figure 1.1 architecture de pare-feu.

Le système pare-feu est un système logiciel, 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 ».

1.3 Fonctionnement d'un système pare-feu

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 permettent de mettre en œuvre 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.
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

1.4 Les catégories des pare-feux [2]

La révolution des pare-feux est passé par plusieurs étapes ce qui résulte des plusieurs catégories des pare-feux selon leur besoins.

1.4.1 Le filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « *stateless packet filtering* ») ; Il analyse les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau externe et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port.

Table 1.1 : exemple des règles de pare-feu.

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	Tcp	any	25
2	Accept	Any	192.168.10.3	Tcp	any	80
3	Accept	192.168.10.0/24	Any	Tcp	any	80
4	Deny	any	Any	Any	any	any

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 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

1.4.2 Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire).

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de **filtrage dynamique de paquets** qui est basé sur l'inspection aux niveaux des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « **state ful inspection** » ou « *stateful packet filtering* », traduisez « *filtrage de paquets avec état* ».

Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

1.4.3 Le 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). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées.

Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (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.

1.5 Le pare-feu et le problème de trafic crypté

Le grand problème de pare-feu est l'utilisation des paquets cryptés de types **HTTPS** (**https** est une combinaison de **HTTP** avec une couche de chiffrement de type **SSL/TLS** (le plus utilisé.)) où tout le trafic sera crypté et le pare-feu devenu incapable d'inspecter ce trafic.

SSL/TLS (Secure Socket Layer /Transport Layer Protocole) est un protocole de sécurité qui permet d'établir des communications cryptées via l'internet. Les connexions à l'aide des protocoles **SSL/TLS** protègent le canal d'échange des données sur Internet. Les protocoles **SSL/TLS** permettent d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus malintentionnés afin de diffuser leurs logiciels malveillants car la majorité des pare-feux n'analyse pas le trafic **SSL/TLS**.

1.6 Conclusion

Nous avons vu, dans ce chapitre, les différents types de pare-feu, leur fonctionnement et leurs limites sur tout avec la cryptographie. Et nous avons pris comme un champ d'étude la cryptographie selon le protocole **SSL** car il est énormément utilisé dans les communications internet. Donc pour une vraie sécurité le pare-feu doit inspecter tout le trafic et aussi le trafic crypté en entré ou en sorti de chaque entreprise ; Ce problème est connu sous le nom **l'inspection HTTPS** ou **l'inspection SSL/TLS** et nous aurons utilisé le terme **l'inspection SSL/TLS** car il est le plus utilisé. Alors en a besoin d'une étude bien détailler de l'architecture de protocole **SSL** pour peut protéger notre entreprise et ce qu'on le verra dans le chapitre suivant.