

En savoir plus sur le firewall

Un ordinateur connecté à Internet est une maison avec 65536 portes ouvertes sur un incendie.

Préambule

Dans la tradition de la construction, un mur pare feu est un mur sans fenêtre et ignifugé, construit pour empêcher la progression d'un incendie d'une partie à l'autre d'un bâtiment. Par extension, le terme de mur pare feu est utilisé en informatique pour désigner un programme informatique placé sur un réseau pour empêcher certaines communications qui sont interdites par des règles préétablies.

La notion de ports

De nombreux programmes peuvent être exécutés simultanément sur Internet (par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages web tout en téléchargeant un fichier). Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données. Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits : un port. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. S'il s'agit d'une requête à destination de l'application, l'application est appelée application serveur. S'il s'agit d'une réponse, on parle alors d'application cliente.

Assignations des ports par défaut

Il existe des milliers de ports (ceux-ci sont codés sur 16 bits, il y a donc 65536 possibilités). Afin de faciliter la configuration des réseaux, une organisation a été mandatée pour standardiser les assignations ports/applications : l'IANA (Internet Assigned Numbers Authority, <http://www.iana.org>).

Les ports 0 à 1023 sont réservés aux processus système ou à certains utilisateurs privilégiés. Voici certaines de ces assignations par défaut:

Port/Application

21/FTP

22/ssh

23/Telnet

25/smtp

53/DNS

63/Whois

70/Gopher

79/Finger

80/http

Ainsi, un serveur (un ordinateur que l'on contacte et qui propose des services) possède des numéros de ports fixes auxquels des services sont associés.

Le mur pare feu (aussi appelé mur de feu ou en anglais firewall)

Un mur pare feu correctement configuré se doit de rejeter tout ce qui n'a pas été explicitement autorisé. C'est le rôle de la « politique par défaut ». Pour fixer celle-ci, nous utilisons les 3 règles suivantes : gérer les entrées, gérer les sorties, autoriser les flux locaux. Comme toutes les entrées/sorties de données passent par les ports, gérer les flux consiste à se donner des règles de visibilité, d'ouverture et de fermeture pour chacun d'eux.

Le premier niveau consiste à autoriser (ou interdire) un paquet de données à transiter en fonction des adresses de départ et de destination du dit paquet. C'est ce qu'on appelle un « stateless firewall », c'est à dire sans contrôle de l'état de la connexion. Si la connexion existe sur le port de destination, elle sera utilisée, et ce, quelle que soit la raison de l'existence de cette communication. Le deuxième niveau consiste à ajouter la condition d'état de la connexion, c'est à dire que le paquet de données, s'il arrive sur un port « ouvert » doit aussi être issu d'une communication préalablement validée comme apte à le recevoir. C'est ce qu'on appelle un « stateful Firewall ». C'est un mur pare feu qui garde la trace de l'état des connexions du réseau. Il est programmé pour savoir quels paquets sont légitimes pour les différents types de connexions. Seuls les paquets qui correspondent à un état de connexion connu seront autorisés à transiter. Les autres seront rejetés.

La mise en place d'un Mur Pare Feu

La mise en place d'un mur pare feu nécessite une intervention sur le PC qui sert de passerelle vers Internet. Une fois en place, le mur pare feu est paramétré pour rejeter tout ce qui n'a pas été explicitement autorisé. En pratique : Toutes les applications qui tournent sur le réseau client sont autorisées à ouvrir des ports pour échanger avec l'extérieur. Les paquets de données entrant ne sont autorisés que s'ils utilisent une connexion préalablement initiée par le client. Seuls quelques ports précis sont ouverts à des requêtes en provenance de l'extérieur comme le port 22 pour la maintenance, le port 53 pour la résolution de nom, le port 80 en cas d'hébergement d'un site web, etc. Les quelques cas particuliers comme le « peer-to-peer » ou les conférences téléphoniques en IP par exemple, qui nécessitent de pouvoir autoriser une connexion à la demande d'un serveur extérieur sont étudiés au cas par cas.

Mur pare feu, logiciels libres et PraKsys

Il existe plusieurs logiciels libres permettant de réaliser un mur pare feu. Quel que soit le choix du logiciel retenu, retenons toutefois leurs quelques avantages : les murs de feu libres sont disponibles pour tous les clients, quels que soit leur système d'exploitation. les murs de feu libres tournent avec des systèmes d'exploitation libres (dont Linux) qui permettent des niveaux de sécurités sans doute inégalés. les murs de feu libres sont gratuits. les murs de feu libres sont les plus utilisés, et donc les plus connus des administrateurs systèmes. PraKsys met en place des murs pare feu. Le mur pare feu utilisé est netfilter. C'est un « statefull Firewall ».

Voir le site de [Netfilter](#)