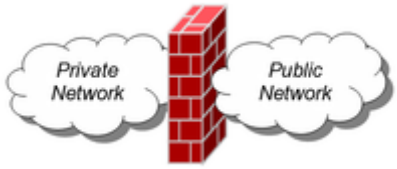
WIKIPÉDIA

Pare-feu (informatique)

Un **pare-feu**[1] (de l'anglais *firewall*) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).



Un pare-feu, représenté par un mur de briques, pour cloisonner le réseau privé.

Sommaire

Terminologie

Un pare-feu est parfois appelé *coupe-feu*, *garde-barrière*, *barrière de sécurité*, ou encore *firewall*. Traduction littérale : mur de feu [réf. souhaitée].

Dans un environnement Unix BSD (Berkeley Software Distribution), un pare-feu est aussi appelé *packet filter*.

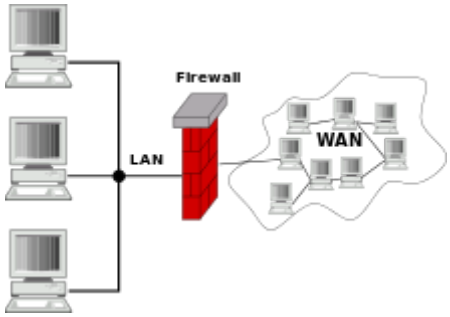
Origine du terme

Selon le contexte, le terme peut revêtir différentes significations :

- dans le domaine de la lutte contre les incendies de forêt, il se réfère aux allées pare-feu destinées à contenir l'extension des feux de forêts ;
- au théâtre, le déclenchement d'un mécanisme « *pare-feu* » (ou « *coupe-feu* ») permet d'éviter la propagation du feu de la salle vers la scène ;
- dans le domaine de l'architecture, il fait référence aux portes coupe-feu ou à tout autre dispositif constructif destiné à contenir l'extension d'un incendie ;
- en informatique, l'usage du terme « pare-feu » est donc métaphorique. Sa dénomination, reprend au sens figuré l'intention de "brûler par un mur de feu virtuel" tout ce qui tente d'entrer avec l'intention de nuire dans une machine ou un réseau. Il établit une barrière de protection contre les intrusions et les contaminations venant de l'extérieur

Fonctionnement général

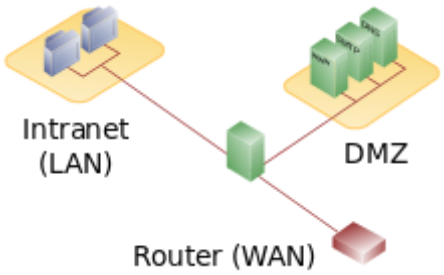
Le pare-feu est jusqu'à ces dernières années considéré comme une des pierres angulaires de la sécurité d'un réseau informatique (il perd en importance au fur et à mesure que les communications basculent vers le HTTP sur TLS, court-circuitant tout filtrage). Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs).



Pare-feu passerelle entre LAN et WAN.

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



Pare-feu routeur, avec une zone DMZ.

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

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, 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.

Enfin, le pare-feu est également souvent situé à l'extrémité de tunnel IPsec ou TLS. L'intégration du filtrage de flux et de la gestion du tunnel est en effet nécessaire pour pouvoir à la fois protéger le trafic en confidentialité et intégrité et filtrer ce qui passe dans le tunnel. C'est le cas notamment de plusieurs produits du commerce nommés dans la liste ci-dessous.

Catégories de pare-feu

Les pare-feux sont un des plus vieux équipements de sécurité informatique et, en tant que tel, ont subit à de nombreuses évolutions. Suivant la génération du pare-feu ou son rôle précis, on peut les classer en différentes catégories.

Pare-feu sans état (*stateless firewall*)

C'est le plus vieux dispositif de filtrage réseau, 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.

La configuration de ces dispositifs est souvent complexe et l'absence de prise en compte des machines à états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pare-feux ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation.

Pare-feu à états (*stateful firewall*)

Certains protocoles dits « à états » comme TCP introduisent une notion de connexion. Les pare-feux à états 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 fluxIP.

Enfin, si les ACL autorisent un paquet UDP caractérisé par un quadruplet (ip_src, port_src, ip_dst, port_dst) à passer, un tel pare-feu autorisera la réponse caractérisée par un quadruplet inversé, 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. Cependant dans le cas d'UDP, cette caractéristique peut être utilisée pour établir des connexions directes (P2P) entre deux machines (comme le faitSkype par exemple).

Pare-feu applicatif

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 parports.

Une autre raison de l'inspection applicative est l'ouverture de ports dynamique. Certains protocoles comme FTP, en mode passif, échangent entre le client et le serveur des adresses IP ou des ports TCP/UDP. Ces protocoles sont dits « **à contenu sale** » ou « passant difficilement les pare-feux » car ils échangent au niveau applicatif (FTP) des informations du niveau IP (échange d'adresses) ou du niveau TCP (échange de ports). Ce qui transgresse le principe de la séparation des couches réseaux. Pour cette raison, les protocoles « à contenu sale » passent difficilement voire pas du tout les règles de NAT ...dynamiques, à moins qu'une inspection applicative ne soit faite sur ce protocole.

Chaque type de pare-feu sait inspecter un nombre limité d'applications. Chaque application est gérée par un module différent pour pouvoir les activer ou les désactiver. La terminologie pour le concept de module est différente pour chaque type de pare-feu : par exemple : Le protocole HTTP permet d'accéder en lecture sur un serveur par une commande GET, et en écriture par une commande PUT. Un pare-feu applicatif va être en mesure d'analyser une connexion HTTP et de n'autoriser les commandes PUT qu'à un nombre restreint de machines.

- **Pare-feu applicatif** sur Bee Ware; DenyAll
- **Firewall as a Service** (filtrage en fonction de l'origine et de la destination de chaque paquet) surUPPERSAFE
- **Conntrack** (suivi de connexion) et **l7 Filter** (filtrage applicatif) surLinux Netfilter
- **CBAC** sur Cisco IOS
- **Fixup** puis **inspect** sur Cisco PIX
- **ApplicationLayerGateway** sur **Proventia M**,
- **Predefined Services** sur Juniper ScreenOS
- **Stateful Inspection** sur Check Point FireWall-1
- **Deep Packet Inspection** sur Qosmos
- **Web Application Firewall** sur BinarySEC

Pare-feu identifiant

Un pare-feu 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 paradresse IP ou adresse MAC, et ainsi suivre l'activité réseau par utilisateur.

Plusieurs méthodes différentes existent qui reposent sur des associations entre IP et utilisateurs réalisées par des moyens variés. On peut par exemple citer authpf (sous OpenBSD) qui utilise ssh pour faire l'association. Une autre méthode est l'identification connexion par connexion (sans avoir cette association IP = utilisateur et donc sans compromis sur la sécurité), réalisée par exemple par la suite NuFW, qui permet d'identifier également sur des machines multi-utilisateurs.

On pourra également citer Cyberoam qui fournit un pare-feu entièrement basé sur l'identité (en réalité en réalisant des associations adresse MAC = utilisateur) ou Check Point avec l'option NAC Blade qui permet de créer des règles dynamiques basée sur l'authentification Kerberos d'un utilisateur, l'identité de son poste ainsi que son niveau de sécurité (présence d'antivirus, de patchs particuliers).

Pare-feu personnel

Les pare-feux personnels, généralement installés sur une machine de travail, agissent comme un pare-feu à états. Bien souvent, ils vérifient aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

Portail captif

Les portails captifs sont des pare-feux dont le but est d'intercepter les usagers d'un réseau de consultation afin de leur présenter une page web spéciale (par exemple : avertissement, charte d'utilisation, demande d'authentification, etc.) avant de les laisser accéder à Internet. Ils sont utilisés pour assurer la traçabilité des connexions et/ou limiter l'utilisation abusive des moyens d'accès. On les déploie essentiellement dans le cadre de réseaux de consultation Internet mutualisés filaires ou Wi-Fi.

Technologies utilisées

Les pare-feux récents embarquent de plus en plus de fonctionnalités, parmi lesquelles on peut citer :

- Filtrage sur adresses IP / protocole,
- Inspection *stateful*[2] et applicative,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif :
  - HTTP (restriction des URL accessibles),
  - Courriel (Anti-pourriel),
  - Logiciel antivirus, anti-logiciel malveillant
- Traduction d'adresse réseau,
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveurs de protocoles de connexion (telnet, SSH), de protocoles de transfert de fichier (SCP),
- Clients de protocoles de transfert de fichier (FTP),
- Serveur Web pour offrir une interface de configuration agréable,
- Serveur mandataire (« *proxy* » en anglais),
- Système de détection d'intrusion (« IDS » en anglais)
- Système de prévention d'intrusion (« IPS » en anglais)

Notes et références

1. Terme recommandé par la Commission générale de terminologie et de néologie et couramment employé, chercher *firewall* dans FranceTerme (http://franceterme.culture.fr/FranceTerme/).
2. Stateful Inspection est une technologie inventée et déposée par Check Point Software. Technologie Stateful Inspection (http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf) **[PDF]**.

Voir aussi

Articles connexes

- Liste de pare-feu
- Bastion (informatique)

Sur les autres projets Wikimedia :

Firewall et proxy, sur Wikiversity

- Sécurité informatique
- Zone démilitarisée (informatique)
- Pare-feu virtuel

Liens externes

- {10 ans de sécurité applicative - un article de DenyAll (Web Application Firewall)
- NAXSI - Web Application Firewall (WAF) Opensource basé sur Nginx
- Comment ça marche, un pare-feu ?
- Les Firewalls sur www.frameip.com
- **(en)** Technologie Stateful Inspection
