

définition :

un Firewall (en français "pare-feu") est un système de défense d'un réseau connecté à l'Internet contre les agressions.

caractéristiques :

ce qui est protégé : applications, données, machines

comparaison :

par rapport à un proxy, un firewall n'est ni une machine ni un logiciel, c'est un système

domaine d'application :

interconnexion d'un LAN d'entreprise à l'Internet

Que protège-t-on ? ses ressources (calculateur, disques, fichiers) et sa réputation.

Que cherche l'agresseur éventuel ?

- se vanter d'avoir pénétré le système (plaisantin)
- utiliser l'ordinateur pour des calculs
- voler des informations (espionnage)
- empêcher l'agressé d'utiliser son système informatique
- détruire les données de l'agressé

Un Firewall est une architecture de système qui doit assurer la sécurité, empêcher l'agresseur d'accéder au réseau interne, faciliter l'enregistrement des activités Internet. Il ne protège pas contre un utilisateur malveillant interne, ni contre des menaces complètement nouvelles, ni contre les virus.

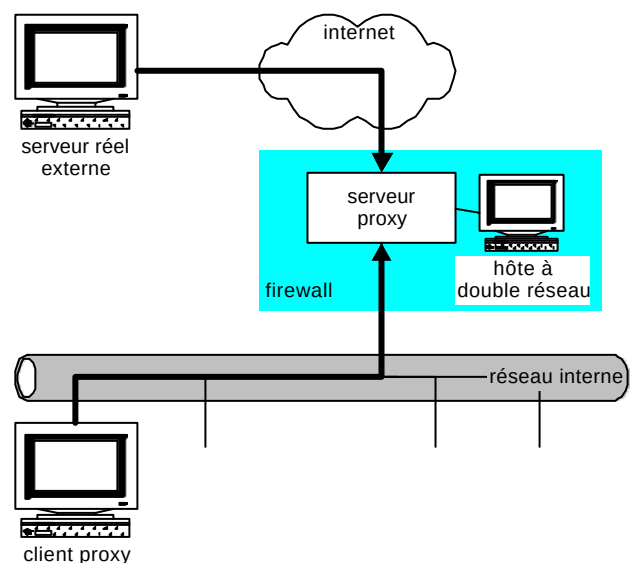
Services Internet : courrier électronique (SMTP), transfert de fichier (FTP), news (NNTP), accès distant (TELNET), accès web (HTTP), recherche de noms (DNS)

Stratégies de sécurité :

- moindre privilège : n'autoriser que les accès nécessaires au travail demandé
- défense en profondeur : installer plusieurs mécanismes de sécurité qui se soutiennent les uns les autres
- goulet d'étranglement : forcer les attaquants à utiliser un canal étroit facile à surveiller
- le maillon le plus faible : à connaître, surveiller ceux qu'on ne peut pas éliminer
- panne sans danger : un routeur filtrant doit tout bloquer quand il est en panne
- participation universelle des employés de l'entreprise

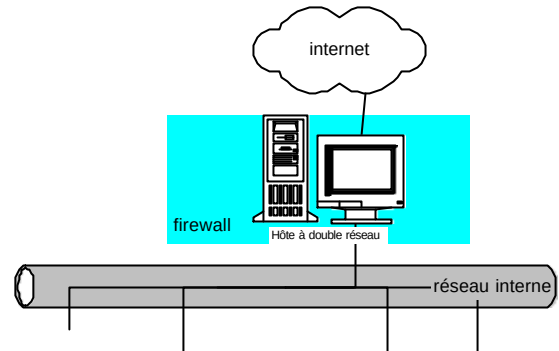
Eléments de la défense :

- filtrage des paquets (sur adr.IP source ou dest., sur protocole (TCP, UDP, ICMP), sur port TCP ou UDP source ou dest., sur type de message ICMP)
- blocage des connexions entrantes hors SMTP (courrier)
- blocage des connexions sortantes vers certains sites
- proxy : programme serveur spécialisé qui tourne sur l'hôte d'un firewall
 - il reçoit les requêtes des utilisateurs et les dirige vers les vrais services selon la sécurité désirée,
 - ils fournissent des connexions de remplacement (passerelle au niveau applicatif)
 - ils sont transparents (l'utilisateur ne s'en rend pas compte)

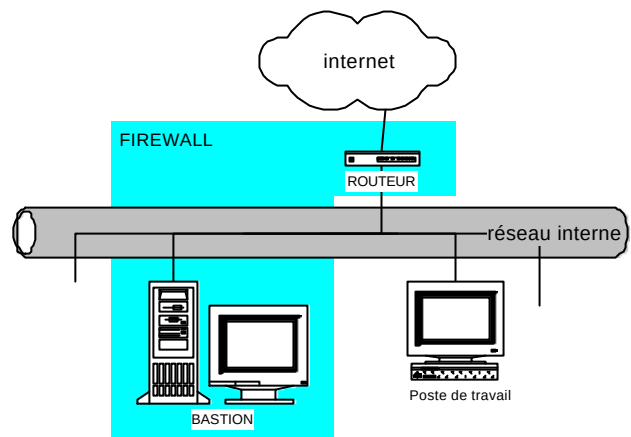


Architecture des firewalls :**Hôte à double réseau :**

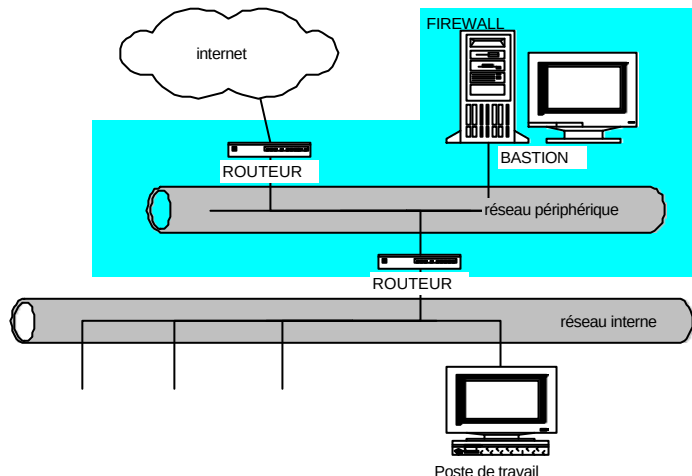
- ordinateur ayant au moins 2 interfaces réseau
- agit comme un routeur, capable d'acheminer les paquets IP d'un réseau à l'autre, mais il faut désactiver cette fonction de routage et implémenter une architecture d'hôte à double réseau
- le trafic IP est bloqué entre l'Internet et le réseau interne
- si on voit un paquet sur le réseau interne provenant de l'Internet, c'est sûr qu'il y a un problème de sécurité
- seul le proxy permet la communication entre Internet et réseau interne

**Hôte à écran :**

- les services sont sur un hôte rattaché au réseau interne
- un routeur assure le filtrage des paquets entre Internet et réseau interne
- le seul système interne auquel peuvent accéder les hôtes de l'Internet est le bastion (grâce au filtrage)
- le trafic entre les postes de travail et l'Internet est bloqué par le routeur

**Sous-réseau à écran :**

- couche de sécurité supplémentaire par rapport à l'hôte à écran
- le réseau périphérique isole encore plus le réseau interne de l'Internet
- pour accéder aux postes, l'agresseur devrait passer 2 routeurs



- le bastion est le principal point de contact entre intérieur et extérieur
- le routeur intérieur protège le réseau interne de l'Internet et du réseau périphérique, il effectue l'essentiel du filtrage de paquets
- le routeur extérieur bloquera essentiellement tout paquet provenant de l'Internet dont les adresses sources sont falsifiées

Diverses variantes de firewall sont possibles à partir de ces quelques principes de base.

On peut aussi mettre en place une victime sacrificielle (ordinateur sur lequel rien n'a d'importance) pour tester de nouveaux services mal connus ou mal sécurisés