

Résumé

Un firewall ou pare-feu est un dispositif physique (matériel) ou logique (logiciel) servant de système de protection pour les ordinateurs domestiques. Il peut également servir d'interface entre un ou plusieurs réseaux d'entreprise afin de contrôler et éventuellement bloquer la circulation des données en analysant les informations contenues dans les flux de données (cloisonnement réseau).

Il permet donc d'une part de bloquer des attaques ou connexions suspectes pouvant provenir de virus, vers ou trojans ainsi que de les tracer. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur.

Table des matières

- 1 C'est quoi ? →
- 2 Comment cela fonctionne-t-il ? →
- 3 Menaces contrées →
- 4 Exemples →
- 5 Recommandations →



1 C'est quoi ?

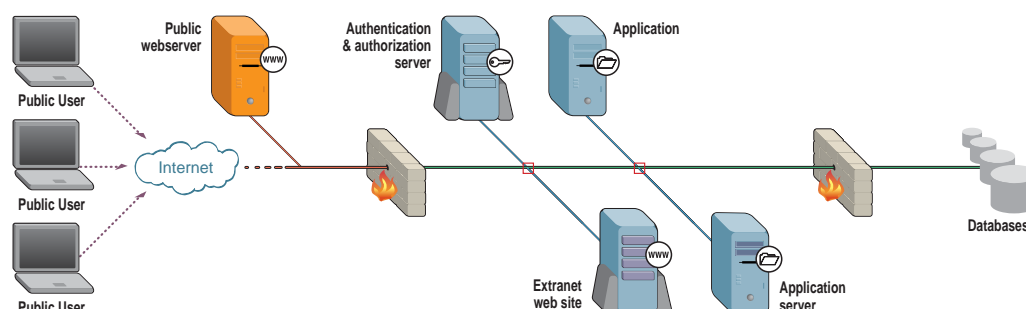
Un firewall ou pare-feu est un dispositif physique (matériel) ou logique (logiciel) servant de système de protection pour les ordinateurs domestiques. Il peut également servir d'interface entre un ou plusieurs réseaux d'entreprise afin de contrôler et éventuellement bloquer la circulation des données en analysant les informations contenues dans les flux de données (cloisonnement réseau).

Il permet donc d'une part de bloquer des attaques ou connexions suspectes pouvant provenir de virus, vers ou trojans ainsi que de les tracer. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur.

Il existe principalement 2 catégories de firewalls :

- ➔ Les firewalls personnels protégeant uniquement les stations de travail ou ordinateurs personnels. Ils sont installés directement sur l'ordinateur de l'utilisateur.
- ➔ Les firewalls d'entreprise installés sur des machines dédiées. Ce type de firewall est souvent placé entre Internet et un réseau d'entreprise afin de protéger ce dernier des différentes menaces d'Internet.

Il est également utilisé pour la création de zones démilitarisées (DMZ) pour l'hébergement de serveurs publics. Dans certains cas, il sert même à séparer différentes parties du réseau d'entreprise en périmètres de sécurité différents (cloisonnement réseau).



[→ suite](#)

2

Comment cela fonctionne-t-il ?

Principe de fonctionnement

Un firewall agit sur un ensemble de règles définies correctement par un utilisateur se basant généralement sur le principe suivant :

⚠ Tout ce qui n'est pas explicitement autorisé est interdit

Cela signifie que les règles constituant une partie de la configuration du firewall doivent explicitement autoriser une action ou un flux de données pour que la connexion puisse s'établir.

Le tableau ci-dessous montre un exemple de configuration des règles d'un firewall :

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

Filtrage de contenu

Certains firewalls permettent en plus du filtrage de paquets d'analyser et de filtrer les données contenues dans les paquets. Cela permet dans certains cas de :

- empêcher la consultation de sites web Internet interdits
- empêcher le téléchargement de fichiers ou logiciels malicieux
- empêcher l'envoi et la réception par e-mail de fichiers potentiellement dangereux

En plus des fonctionnalités énoncées ci-dessus, certains firewalls vérifient même que le contenu applicatif du trafic traversant le firewall (protocole applicatif utilisé, instructions, codification, ...) correspond effectivement au protocole applicatif attendu.

Filtrage de paquets

Internet et les réseaux fonctionnent par envoi/réception de blocs de données appelées « paquets ». Un firewall analyse chacun de ces paquets sur base d'un certain nombre de caractéristiques définies dans les règles.

Un firewall fonctionnant sur le principe du filtrage de paquets analyse les en-têtes des paquets échangés entre deux ordinateurs en considérant les éléments suivants :

- L'adresse IP de la machine émettrice
- L'adresse IP de la machine réceptrice
- Le type de paquet TCP, UDP, ICMP ou IP
- Le service ou port demandé

Ceci permet d'éviter par exemple qu'un cracker accède à un cheval de troie en utilisant un autre protocole applicatif à travers le port 80 (http).

3

Menaces contrées

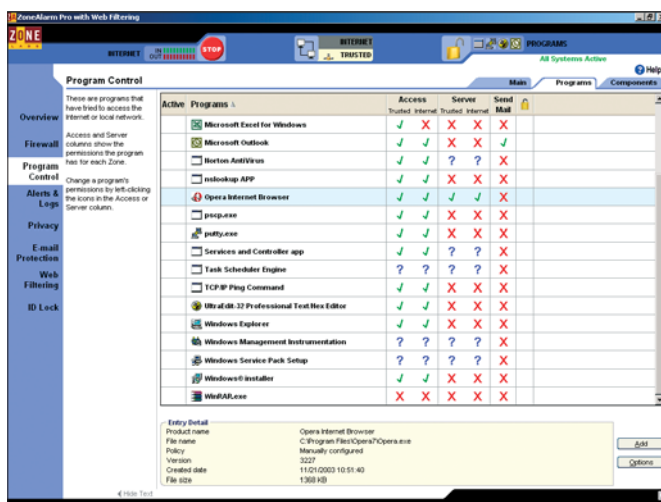
L'utilisation d'un firewall configuré correctement permet de contrer les menaces suivantes :

- Attaques de type intrusion réseau (cf. fiche thématique « Attaques »)
- Chevaux de Troie (cf. fiche thématique « Chevaux de Troie »)
- Vers (cf. fiche thématique « Virus et ver »)

→ suite

4 Exemples

L'illustration ci-dessous présente les règles de configuration d'un firewall personnel :



5 Recommandations

Un firewall peut dans certains cas limiter les possibilités accordées à un utilisateur voulant accéder à un réseau tel que Internet. Dans d'autres cas, l'installation d'un firewall peut donner également une mauvaise impression de sécurité « j'ai un firewall, je suis totalement protégé ».

Il convient donc d'appliquer les recommandations suivantes pour s'assurer de la pleine efficacité du firewall :

- 1 Configuration correcte des règles et des différents paramètres du firewall
- 2 Trouver un équilibre entre sécurité et fonctionnalité. Le firewall doit assurer une protection adéquate (sécurité) tout en évitant de limiter trop les fonctionnalités de l'utilisateur (fonctionnalité)
- 3 Il est recommandé de limiter le nombre d'utilisateurs pouvant configurer et modifier les règles et paramètres du firewall.