Sylvain PASSEMAR sylvain.passemar@mirage4.net

Qu'est-ce qu'un firewall ?

Introduction :

Un firewall - littéralement "mur de feu" - est un ordinateur et un programme qui filtre ce qui passe d'un réseau à un autre.
On s'en sert pour sécuriser les réseaux et les ordinateurs, c'est-à-dire contrôler les accès et bloquer ce qui est interdit.
Généralement, on utilise un firewall pour protéger un réseau local du réseau internet :
Typiquement, il va:

- Autoriser les ordinateurs du réseau local à se connecter à internet.
- Bloquer les tentatives de connexion d'internet vers les ordinateurs du réseau local.

Explication :

Les données qui circulent sur le réseau sont découpées en morceaux qu'on appelle paquet, un paquet est constitué d'une entête qui contient des informations sur le paquet (émetteur, destinataire, taille des données, ...) et des données elle-mêmes (corps du paquet).
Sur le réseau on trouve des filtres de paquets, c'est à dire qu'à partir de certains critères, quand le paquet leur arrive, ils peuvent décider de son sort, soit en le laissant passer (accept), en le supprimant (deny) ou encore en le supprimant et en avertissant l'émetteur que le paquet a été rejeté (reject).

Placement dans le modèle OSI :

La majorité des firewalls travaillent à l’échelon des couches 4 (TCP, UDP...), 3 (IP...) et 2 (Ethernet...).
Ils ne comprennent rien aux protocoles au dessus (ils sont incapables de filtrer HTTP, SMTP, POP3...).
Certains firewalls sont capables de travailler au niveau de la couche 7 (applicative), rentrant en concurrence dans le filtrage avec certain proxy.
Ils sont généralement plus lents, plus lourds et plus complexes à configurer mais permettent de filtrer certains protocoles comme HTTP, SMTP, POP3, FTP ...
Par exemple, c'est utile pour bloquer le téléchargement de virus, interdire certains sites …

Protection des services vulnérables :

Dans le cas des ressources partagées via le protocole NetBios, telles que les répertoires ou les imprimantes dans un réseau local, n'importe quel attaquant ayant un accès direct au réseau local pourrait accéder à ces ressources et voler ou supprimer des données confidentielles. Grâce au pare-feu, les services et les protocoles du réseau local peuvent être isolés des connexions externes, puis filtrés, et toute tentative d'y accéder et de les exploiter peut ainsi être rejetée.

Contrôle de l'accès aux ressources du réseau :

Étant donné qu'ils filtrent toutes les communications au premier niveau, avant que les paquets atteignent les autres ordinateurs de l'entreprise, les pare-feu sont les points idéaux d'où

contrôler les accès. En effet, une connexion qui n'est pas authentifiée dans le pare-feu ne pourra pas interagir avec des informations sensibles dans le reste du réseau.

Concentration de la sécurité :

Comme le pare-feu est le seul point d'entrée au réseau local - depuis Internet - le reste du réseau est isolé de toute attaque, la sécurité étant concentrée à cet endroit.
Ce système soulage le travail des personnes responsables de la sécurité, car leur plus grand souci en ce qui concerne les attaques externes, est maintenant maîtrisé par le pare-feu ; ce dernier leur facilite la tâche, le contrôle et le maintien d'une seule machine étant plus simple que le contrôle et le maintien d'un réseau tout entier, ainsi que des nombreux systèmes et applications qu'il peut inclure.

Contrôle et statistiques :

Comme toutes les connexions vers et de Internet passent par le filtre du pare-feu, ce dernier est un outil très important pour recueillir les statistiques quant à l'utilisation du réseau.
Il permet de contrôler en interne l'utilisation d'Internet , fournit de précieuses informations sur les tentatives de connexions externes et aide à détecter toute activité douteuse.

Vous savez maintenant la théorie du principe de fonctionnement d’un FireWall.