

Un coupe-feu (firewall en anglais) contribue à bloquer les accès non autorisés à votre ordinateur. C'est en fait une excellente mesure pour contrer les pirates informatiques et les tentatives d'intrusion. Toutes les données entre votre ordinateur et Internet passe par une zone contrôlée. À ne pas confondre avec un anti-virus, il arrive par contre souvent qu'un logiciel anti-virus comprenne aussi un coupe-feu - l'anti-virus sera alors beaucoup plus dispendieux à l'achat.

Le coupe-feu peut-être configuré de façon à n'autoriser que quelques applications à envoyer ou recevoir des données de sources extérieures. Si une application n'est pas cochée "autorisée" dans votre configuration, chaque fois que vous voudrez ouvrir celle-ci, une fenêtre s'ouvrira pour vous demander si vous accepter de laisser cette application passer le mur coupe-feu. D'autres programmes, comme votre anti-virus par-exemple, devront obligatoirement être autorisés à passer le mur.

Un coupe-feu peut aussi générer des rapports indiquant les tentatives d'intrusion dans votre ordinateur, notamment en vous indiquant l'adresse IP du mal intentionné.

.....
Le fonctionnement du pare-feu se résume à examiner les informations en provenance et en direction d'Internet. Il détecte et ignore les informations provenant d'un emplacement douteux ou qui semblent suspectes. Si vous configurez convenablement votre pare-feu, les pirates à la recherche d'ordinateurs vulnérables ne peuvent pas détecter le vôtre.

.....
Réf.: <http://www.microsoft.com/france/securite/gpublic/protect/firewall.aspx>

Qu'est-ce qu'un pare-feu ?

Un pare-feu Internet est une solution matérielle ou logicielle qui écarte certains trafics Internet malveillants en provenance de pirates, et certains types de virus et de vers qui peuvent infecter votre ordinateur. Si vous travaillez à domicile ou dans une petite entreprise, l'installation d'un pare-feu est la procédure la plus importante et la plus efficace pour protéger votre ordinateur. Il est important que votre pare-feu et votre logiciel antivirus soient activés *avant* la connexion à Internet.

Pourquoi ai-je besoin d'un pare-feu ?

Si votre ordinateur n'est pas protégé lorsque vous vous connectez à Internet, des pirates peuvent accéder aux informations personnelles figurant sur votre ordinateur. Ils peuvent installer du code qui détruit les fichiers ou entraîne des dysfonctionnements de votre ordinateur. Ils peuvent également utiliser votre ordinateur pour générer des problèmes sur d'autres ordinateurs personnels et professionnels connectés à Internet. Un pare-feu permet d'écarter de nombreux types de trafics Internet malveillants avant qu'ils n'atteignent votre ordinateur.

Certains pare-feu permettent également d'éviter que d'autres personnes utilisent votre ordinateur pour attaquer d'autres ordinateurs, à votre insu. Il est important d'utiliser un pare-feu quelle que soit la méthode de connexion à Internet que vous utilisez (modem d'accès à distance, modem câble ou ligne ADSL).

Comment fonctionne le pare-feu de connexion Internet de Windows XP ?

Le pare-feu de connexion Internet analyse tout le trafic réseau des connexions pour lesquelles il est activé. Par exemple, un pare-feu peut analyser l'ensemble du trafic sur votre connexion d'accès à distance à Internet. Le pare-feu effectue un suivi de toutes les communications émanant de votre ordinateur et il empêche tout trafic indésirable d'atteindre votre ordinateur. Si besoin est, le pare-feu ouvre des ports de manière dynamique et permet à votre ordinateur de recevoir le trafic que vous avez demandé ; par exemple, une page Web dont vous avez cliqué sur l'adresse.

Un port est un terme de réseau qui identifie le point auquel un type de trafic réseau atteint votre ordinateur. Les ports que vous ouvrez dépendent du type de trafic que vous voulez envoyer et recevoir.

Si vous n'avez pas demandé le trafic entrant, le pare-feu le bloque avant qu'il ne puisse atteindre votre ordinateur. Dans le cas d'une utilisation particulière, telle que la mise en réseau, l'hébergement de jeux en ligne ou l'hébergement sur votre propre serveur Web, vous pouvez sélectionner les ports que vous voulez laisser ouverts. Ainsi, d'autres utilisateurs peuvent établir des connexions à votre ordinateur, mais la sécurité peut également être moindre.



Quelle type de protection le pare-feu de connexion Internet assure-t-il ?

Le pare-feu constitue votre principale défense contre différents virus informatiques transmis sur le réseau. Un virus informatique est similaire à un virus mais il n'est pas contenu dans un autre programme et peut se répandre sans l'intervention d'autres programmes. Le pare-feu de connexion Internet assure la protection de votre ordinateur dans la mesure où les utilisateurs externes n'y ont pas accès et où toute connexion non autorisée à votre PC est interdite.

Quels sont les éléments que le pare-feu de connexion Internet ne permet pas de protéger ?

Le pare-feu de connexion Internet de Windows XP ne peut pas vous protéger contre les virus répandus via des courriers électroniques (par exemple les chevaux de Troie), qui se font passer pour des logiciels utiles et vous incitent à les télécharger. Le pare-feu ne peut pas interdire les messages publicitaires non sollicités. Il n'interdit pas l'accès à un réseau sans fil non sécurisé. Toutefois, le pare-feu permet de protéger les ordinateurs de votre réseau. Aussi, si un intrus réussit à accéder à votre réseau, il ne peut pas accéder à votre ordinateur personnel.

Pourquoi quelqu'un voudrait-il pirater votre ordinateur ?

Non seulement les pirates cherchent à accéder à des informations privées, telles que des enregistrements financiers ou des fichiers de mots de passe, mais ils se servent aussi des ordinateurs aux fins suivantes :

- Lancer des attaques de déni de service (DoS - *Denial of Service*) contre un site Web en vue. Après en avoir pris le contrôle, le pirate peut contraindre votre ordinateur ainsi que des centaines, voire des milliers d'autres "zombies" à agir simultanément, ce qui surcharge un site populaire et provoque son indisponibilité.
- Distribuer des logiciels de façon illicite. Après s'être approprié l'espace sur votre disque dur, ils permettent à d'autres d'accéder à votre ordinateur en tant que site "warez" et de télécharger des divertissements ou des applications piratées.



Quel est le risque d'une connexion ADSL ou d'un modem câble ?

Si vous disposez d'une connexion haut débit ADSL ou via le câble active en permanence, les risques sont plus grands car votre ordinateur n'est pas une cible mouvante. Ainsi, lorsque vous utilisez une connexion d'accès à distance, l'adresse réseau de votre ordinateur est différente à chaque fois ; avec une connexion ADSL ou câble, en revanche, l'adresse réseau est inchangée pendant de longues périodes de temps (24 h. maximum). Si cette connexion permanente est un avantage, l'adresse de votre ordinateur est encore plus exposée aux pirates.

Pourquoi un firewall sur son ordinateur personnel ?

Un firewall (pare-feu) filtre les communications entrantes et sortantes sur Internet, parfois malveillantes. Le mode discret (stealth) améliore la protection.

Réf.: <http://eservice.free.fr/firewall.html>

Filtrer les communications entrantes

En filtrant les communications entrantes, un firewall vous protège des menaces suivantes :

- tout logiciel Internet ouvre un port sur votre ordinateur, pouvant servir aussi à une intrusion (directement ou en exploitant une faille de sécurité à distance)
- une tentative de déconnexion à distance
- une connexion avec un troyen installé sur votre ordinateur (pour une intrusion ou une prise de contrôle à distance de votre ordinateur)

Filtrer les communications sortantes

Vos applications Internet cherchent à communiquer vers l'extérieur, sans vous demander votre autorisation, pour :

- envoyer vos informations privées à leur serveur (spyware)
- récupérer un bandeau publicitaire (adware) : seul moyen de financer un logiciel gratuit
- envoyer vos mots de passe (troyen)
- améliorer la qualité du service (par exemple savoir si une nouvelle version du logiciel est disponible).

Un firewall détecte ces communications et vous décidez une fois pour toutes, lesquelles vous autorisez et celles que vous interdisez.

Le mode discret (mode stealth)

Des pirates cherchent des ordinateurs connectés à Internet en envoyant des requêtes sur des plages d'adresse IP (scan d'adresse IP). Votre ordinateur répondra et le pirate saura que vous êtes connecté. Un bon firewall bien paramétré ne répond pas comme si vous n'étiez pas connecté. Ainsi un firewall réduit la possibilité d'intrusion, en plus de la tentative elle-même.