

# **Le parefeu (Firewall)**

Pourquoi un parefeu ?

Des outils simples à paramétrer

Dévier les attaques par saturation

Les ports IP à surveiller

Quelques parefeu gratuits...

## **Pourquoi un parefeu ?**

Aujourd'hui, la majorité des entreprises et une partie des particuliers dotés d'un accès à Internet ont installé un pare-feu (firewall) logiciel ou matériel pour faire face aux tentatives d'intrusion répétées sur leur réseau local. En effet, le sport favori d'un grand nombre de petits malins consiste à scanner les ports IP (un canal par lequel transitent les données sur Internet), des postes de travail ou des serveurs afin de trouver un port resté ouvert par mégarde. Exploitant les failles des systèmes d'exploitation ou des applications (backdoors), certains pirates réussissent à prendre le contrôle d'un serveur Web ou bien dérober des informations confidentielles. Voire à détruire des données en installant un virus ou un cheval de Troie sur un poste de travail ou un serveur.

Si les grandes entreprises ont pris depuis peu réellement conscience du danger, il n'en va pas de même des petites entreprises, des travailleurs indépendants ou des particuliers qui exploitent une liaison Internet, surtout si celle-ci offre un accès permanent comme l'ADSL, la boucle radio (BLR), le câble, et bientôt le GPRS. La majorité des postes de travail, que ce soient des PC de bureau ou des portables, sont aujourd'hui livrés en standard avec un logiciel antivirus qui est loin d'être la parade ultime aux problèmes de sécurité. Un pare-feu est le complément indispensable pour les postes de travail connectés à Internet. Le pare-feu personnel que les entreprises associent généralement à un réseau virtuel privé (VPN) avec leurs salariés nomades, répond au besoin de sécurité et de confidentialité des données.

## **Des outils simples à paramétrer**

Deux grandes catégories de produits se disputent aujourd'hui le marché de la sécurité.

Tout d'abord, les pare-feu surveillant l'activité des ports, des adresses IP et des logiciels. Dans ce cas de figure, l'utilisateur autorise ou bloque le fonctionnement de certains logiciels et s'assure qu'ils seront les seuls à accéder aux ports ouverts.

Tiny Personal Firewall , eSafe Desktop , Etrust EZ Firewall ou Norton Personal Firewall font ainsi partie de cette catégorie. Ces logiciels restent très simples à paramétrer puisqu'ils avertissent l'utilisateur à chaque fois qu'une application tente de communiquer avec l'extérieur. Libre à ce dernier de définir ensuite la règle à appliquer. Oui, l'application peut communiquer à chaque requête ou exceptionnellement avec l'extérieur, ou au contraire non, les échanges sont strictement interdits. Grâce à ce système de configuration par apprentissage, la liste des règles est très simple à établir.

Norton Personal Firewall de Symantec propose la création de règles automatiques lors de l'installation du logiciel. Ce dernier analyse en effet le disque dur du PC pour rechercher les applications susceptibles de poser un problème.

## **Dévier les attaques par saturation**

Certains logiciels comme ZoneAlarm ou Tiny Personal Firewall, possèdent plusieurs niveaux de sécurité : du plus laxiste au plus paranoïaque. Mais attention, le mode de protection le plus élevé interdit quasiment toute communication avec l'extérieur. Logiciel de partage, ftp, forums... plus rien ne passe.

Si ces pare-feu surveillent et filtrent l'activité des logiciels, ils repoussent également les tentatives de scan et bloquent les ports les plus vulnérables. A l'opposé, certains pare-feu comme Black Ice, se contentent simplement de scruter et de filtrer les paquets de données entrants. A l'instar d'un antivirus, ils évaluent les pratiques dangereuses. Cette particularité rend ce type de produit vulnérable aux attaques menées à travers les ports utilisés par certains logiciels. Comme pour les antivirus, il est donc nécessaire de mettre à jour la base de données de Black Ice pour garantir son efficacité. Précisons que Black Ice est l'un des rares pare-feu à résister aux attaques par saturation ou DDos (Distributed Denial of Service). Redoutable, ces derniers exploitent la vulnérabilité du protocole IP pour mettre hors service n'importe quel pc. Ce genre d'attaque est heureusement très rare sur un poste de travail et touche essentiellement les gros serveurs Web.

Signalons pour finir que quelques-uns de ces produits intègrent également un antivirus, Alladin eSafe Desktop par exemple. Gratuits pour les particuliers, certains de ces logiciels sont toutefois payants pour les entreprises. Dans tous les cas, ils sont faciles à tester. Pour ce faire, il suffit de les télécharger, de les installer et de demander à un site Web spécialisé comme Shields UP ou Gibson Research de scanner les défenses du PC. Le diagnostic est ensuite délivré en moins de trois minutes !

## **Les ports IP à surveiller**

L'une des techniques de hacking les plus courantes consiste à tester tous les ports d'une machine afin d'en dénicher un laissé ouvert par mégarde. Les logiciels de scan de port comme Superscan testent généralement dans un ordre croissant tous les ports IP. Mais pour que le pare-feu soit réellement imperméable à ce genre de tentative, il doit être correctement paramétré. De nombreux postes de travail "protégés" sont dans les faits de véritables passoires pour cause de firewall mal configuré et donc inefficace. Si certains ports doivent rester ouverts pour une utilisation normale d'Internet, il est inutile de laisser les autres ports actifs.

Rappelons donc les ports TCP/IP (voir Liste des ports TCP et UDP) numéros 25 pour le SMTP (courrier sortant), 110 pour le POP (courrier entrant), 80 pour le HTTP (Web), 21 pour le FTP (voir Le FTP), 53 pour le DNS (voir Le DNS), 119 pour le NNTP (forums) et 6667 pour l'IRC (messagerie instantanée) restent généralement ouverts pour un usage normal d'Internet. Les autres, dont le fameux Telnet (23) qui permet de prendre le contrôle d'une machine à distance, devront être fermés afin de limiter les tentatives d'intrusion.

## Quelques parefeu gratuits...

Les firewalls sont un élément important de la protection des accès surtout avec le développement des connexions à haut débit. Il est donc important d'en choisir un qui puisse bloquer les applications (pour éviter que des ports soient inutilement ouverts) et qui puisse bloquer les entrées (hacking).

Voici une liste non exhaustive de firewalls ; certains sont gratuits. Utilisez les donc sans tarder.

### Agnitum Outpost Firewall

Un firewall performant et peu connu : il bloque les pages web dont le contenu et/ou l'URL contiennent des chaînes de caractères à définir soi-même. Il bloque aussi ( avec options O / ? / N ) au niveau des Mails/Web/News des ActiveX, Cookies, Popups, Referers, Applet Java, Java et VB scripts. Il filtre les attachments des E-mails par ajout d'une extension supplémentaire (ex: \*.EXE devient \*.EXE.VIR pour éviter un lancement intempestif). Il détecte les attaques Dos et mémorise les DNS. Seuls inconvénients : il n'y a pas de mot-de-passe pour interdire les modifs, ni de mémorisation des logs des différents blocages.

Lien : <http://www.agnitum.com/>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : oui

OS : Win 98 et supérieur

Prix : Gratuit

Efficacité : 3/5

### Kerio Personal Firewall

Kerio est le petit frère de ZoneAlarm : d'une part parce qu'il lui ressemble, d'autre part parce qu'il a les mêmes performances. Il bloque toute attaque de l'extérieur et vous prévient pour que vous choisissiez la meilleure réponse. Il n'y quasiment aucun réglage à faire : le logiciel est déjà configuré à l'installation. C'est l'un de mes préférés.

Lien : <http://www.kerio.com/kerio.html>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : oui

OS : Win 9x ; Nt ; Xp

Prix : Gratuit

Efficacité : 5/5

## Look'n'Stop

Look'n'Stop est un étonnant petit firewall français dont la version "Lite" est gratuite. Il utilise un système de règles paramétrable par l'utilisateur. La configuration d'origine est toutefois suffisamment bien conçue pour que les débutants puissent se contenter de l'installer... sans se poser d'autres questions. Un remarquable logiciel, très efficace, qui mérite vraiment que l'on s'y intéresse. Il ne consomme pas (trop) de ressources et constitue un excellent système de défense de base.

Lien : <http://www.looknstop.com/Fr/>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : partiel

OS : Win 95 ; Nt ; Xp

Prix : Version d'évaluation de 30 jours

Efficacité : 4/5

## Norton Personal Firewall

Simple à installer, sans configuration spéciale ni installation complexe, Norton Personal Firewall protège les utilisateurs de PC contre les connexions non autorisées en provenance et à destination d'Internet. L'utilisateur peut bloquer les connexions à son PC et empêcher les pirates d'accéder à ses fichiers personnels, mots de passe, numéros de comptes ou autres données confidentielles stockées sur le PC. Il détermine quelles applications sont autorisées à accéder à Internet. Il est averti lorsqu'un programme non autorisé, comme un cheval de Troie par exemple, tente d'envoyer des informations en provenance du PC.

Lien : <http://www.symantec.com/sabu/nis/npf/>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : oui

OS : Win 9x ; Nt ; Xp

Prix : payant

Efficacité : 3/5

## Tiny Personal Firewall

Tiny Personal Firewall représente une technologie de sécurité personnelle facile à utiliser et intelligente qui protège entièrement votre ordinateur des pirates. Fondé sur la technologie de sécurité certifiée ICISA, c'est également une part entière du système 'Tiny Software Centrally Managed Desktop Security' (CMDS) choisi par la force aérienne des Etats-Unis, cette dernière comprenant approximativement 500 000 ordinateurs. Disponible gratuitement pour un usage personnel.

Lien : <http://www.tinysoftware.com/home/tiny2?la=EN>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : oui

OS : Win 9x ; Nt ; Xp

Prix : payant

Efficacité : 4/5

## Sygate Personal Firewall

Connu anciennement sous le nom de Sybergen Secure Desktop, ce firewall gratuit (pour les particuliers) a suscité des opinions très contradictoires parmi ses usagers. Certains l'ont déclaré supérieur à ZoneAlarm, alors que d'autres l'ont accusé de planter régulièrement leur ordinateur et de ne pas repérer certaines connexions dangereuses. A vous de juger. Sygate paraît néanmoins être un firewall raisonnablement simple et efficace.

Lien : <http://soho.sygate.com/default.htm>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : oui

OS : Win 9x ; Nt ; Xp

Prix : gratuit

Efficacité : 4/5

## ZoneAlarm

Outil essentiel pour les utilisateurs de lignes ADSL et de modem câble car il fournit une protection solide contre les voleurs, les vandales et les pirates du Net.

Lien : <http://www.zonelabs.com/store/content/home.jsp>

Blocage d'applications : oui

Blocage entrant : oui

Blocage sortant : oui

OS : Win 9x ; Nt ; Xp

Prix : gratuit

Efficacité : 5/5