

Intro

Se connecter à Internet sans précaution, c'est rendre son ordinateur vulnérable en permettant aux pirates de profiter de votre matériel, de votre connexion, de vos données.

Les risques sont divers : en s'introduisant dans votre système, le pirate peut se « contenter » de violer vos données personnelles, mais il peut aussi les diffuser ou les détruire. Il peut également se servir de votre machine pour aller « attaquer » un autre ordinateur plus important à ses yeux ; dans ce cas, vous êtes légalement responsable s'il est prouvé que votre ordinateur a servi de « passerelle ».

Le dernier numéro de CRI Pratique, consacré aux **spywares** (logiciels espions), mentionnait à plusieurs reprises l'intérêt de se doter d'un firewall.

Cet outil, matériel ou logiciel, vous permettra de vous protéger contre bien des dangers. Cependant, comme pour tout ce qui concerne la sécurité informatique, une prévention complète est impossible. Un peu de bon sens et la connaissance des risques vous permettront cependant de surfer en toute sérénité !

Définition

Un firewall (ou pare-feu) est le gardien de la porte virtuelle de votre ordinateur : il vérifie et vous alerte (si vous l'avez configuré ainsi) de tout ce qui circule entre votre machine et l'extérieur.

LE FIREWALL VOUS PROTÈGE

◇ Dans le sens « entrée » :

- Contre les tentatives d'intrusion, et donc de violation, vol ou destruction de vos données personnelles
- Contre les détournements de votre connexion
- Contre la modification ou la suppression non autorisée de fichiers vitaux pour le système
- Contre les risques de servir de « passerelle » pour des attaques dirigées contre d'autres machines
- Contre les virus, vers et autres trojans : les machines infectées par ces virus vont chercher à les répandre de manière automatique en utilisant les ports non protégés d'autres machines (voir plus loin).

◇ Dans le sens « sortie » :

- Contre la divulgation non autorisée d'informations personnelles
- Contre l'exécution de logiciels espions

Certains firewall permettent également de centraliser les risques sur un point unique du réseau, ce qui facilite nettement le travail de sécurité. Enfin, les firewall permettent de contrôler les flux du trafic, c'est-à-dire tout ce qui est émis par ou en direction de votre machine.

IL EXISTE DEUX TYPES DE FIREWALL

◇ **Firewall logiciels ou personnels** : ils s'installent directement sur votre ordinateur.

Le CRI propose 3 firewall gratuits (pour les systèmes d'exploitation Windows) à télécharger sur son serveur FTP (voir plus loin).

◇ **Firewall matériels** : ces équipements dédiés sont placés entre le ou les ordinateur(s) et la connexion Internet. Ils filtrent les allers et venues en amont de l'ordinateur.

En matière de firewall, sachez qu'il n'existe qu'une seule stratégie pour un filtrage efficace : tout interdire, pour ensuite accorder des autorisations au cas par cas. Cette politique peut se révéler contraignante, mais elle est vivement recommandée.

À noter : le CRI dispose d'un firewall, qui protège ainsi tous ses utilisateurs connectés en mode RTC ou RNIS. Ceux-là n'ont pas besoin de se doter d'un firewall sur leur propre machine. Attention ! Cette protection ne les dispense pas de se doter d'un système anti-virus, anti-spam, etc.

Un peu de technique

Avant d'aller plus loin, il est nécessaire d'aborder certaines notions pour mieux comprendre le fonctionnement d'un firewall.

LE PROTOCOLE TCP/IP

Des millions de machines sont connectées à Internet. Ces machines peuvent être de toute nature et utiliser des systèmes d'exploitation très différents : ordinateurs, routeurs, serveurs, téléphones, systèmes de chauffage, horloges, etc.

Toutes fonctionnent de manière différentes, mais toutes ont la possibilité de communiquer entre elles et de se comprendre grâce au protocole TCP/IP.

En effet, lorsque vous souhaitez envoyer un e-mail à un correspondant, il faut que votre machine connaisse le nom et l'adresse de la machine destinataire. Chaque machine est donc identifiable grâce à une adresse IP, unique, et correspondant à une seule machine, quelle qu'elle soit.

L'adresse IP prend la forme XXX.XXX.XX.XXX.

LES PORTS

Connaître le nom de la rue ne suffit pas à trouver le bon destinataire sans le numéro de son appartement. Il faut donc connaître le « port » : selon la nature de l'action que vous souhaitez faire, l'application correspondante utilise un « port ». La messagerie utilise ainsi le port 25, quel que soit le logiciel que vous utilisez. La navigation sur le web utilise le port 80, quel que soit le logiciel que vous utilisez. Il s'agit de normes : votre e-mail ne doit pas passer par le port 80 (en théorie, car il est possible de le faire passer malgré tout).

Quelques ports parmi les plus utilisés :

◇ Le Web

- Port 80 : utilisé par votre navigateur
- Ports 8080 ou 3128 : si vous passez par le relais d'un serveur proxy

◇ Les e-mails

- Port 110 : utilisé par votre outil de messagerie pour télécharger les courriers
- Port 25 : utilisé par votre outil de messagerie pour envoyer votre courrier

◇ Les news : port 119 (recevoir et poster les news)

◇ Télécharger des fichiers par FTP : ports 20 et 21 (ce sont les ports que vous utiliserez en téléchargeant un des firewall proposés par le CRI74 sur son serveur FTP, par exemple)

Il existe 65 536 numéros de ports !

Action du Firewall

Le firewall peut agir à ces deux niveaux

LE FILTRAGE IP

Lorsque votre machine cherche à communiquer avec une autre (parce qu'elle veut lui envoyer un e-mail, parce qu'elle veut accéder à un site web...), elle envoie sa requête à l'adresse IP concernée (qu'elle connaît grâce au nom de domaine contenu dans l'URL du site web, par exemple).

Si la requête est acceptée, la réponse est envoyée en retour à votre machine. La machine qui vous a répondu sait où vous joindre, puisque votre propre adresse IP figurait dans votre requête. La réponse utilise votre adresse IP pour accéder à votre machine.

Le filtrage IP consiste donc à bloquer toute adresse IP inconnue, hormis la vôtre.

À noter : certains pirates peuvent s'emparer d'une adresse IP contenue dans une réponse à une requête. Ils s'en servent pour pénétrer votre système et exploiter une faille. Ce genre d'attaque, le spoofing, est cependant relativement rare.

LE FILTRAGE APPLICATIF

Le firewall peut également filtrer les applications (ou logiciels) en fermant tous les ports.

Exemple : Firefox (logiciel de navigation) veut aller chercher une page web située sur un serveur distant ; il lance sa requête vers l'extérieur via le port 80 (relatif à la navigation). Ce port est bloqué.

Le firewall peut alors :

- ◇ **répondre que ce port est interdit.** Vous pourrez peut-être recevoir un message d'erreur stipulant, par exemple, « connection refused » ; ce message n'est pas propre au firewall, il peut également signifier d'autres problèmes (le serveur sur lequel se trouve la page web est indisponible, etc.).
- ◇ **ne pas répondre à l'application** qui, ignorant l'interdit, continuera à tenter de sortir par ce port. Dans ce cas, vous pourrez recevoir un message d'erreur stipulant « connection timeout ».

Qu'elle ignore ou non l'interdiction, l'application cherchera quand même à sortir !

À noter : c'est bien l'application, via le port, qui est bloquée. **Le firewall ne peut pas surveiller le contenu de la requête.** Si un e-mail infecté que vous avez reçu reçoit l'autorisation de passer (parce que l'adresse IP n'est pas bloquée et que le port 110 est utilisable), c'est tout son contenu, et donc son virus, qui sera autorisé à passer ! **Il est donc indispensable de multiplier les protections en installant un anti-virus efficace en plus du firewall.**

De la même manière, si le firewall logiciel (c'est-à-dire placé sur votre ordinateur) est recommandé pour se protéger des spywares, notamment, c'est parce qu'il empêche tout programme inconnu et non autorisé à fonctionner. Le firewall n'empêchera pas le spyware de s'installer sur votre machine, mais le rendra inoffensif en l'enfermant à l'intérieur de votre machine. Or, la raison d'être d'un spyware est de communiquer des informations confidentielles vers l'extérieur.

À noter : le firewall matériel ne peut voir la différence entre une application innocente et un logiciel espion dès lors que celui-ci utilise le même port pour sortir vers l'extérieur.

Ce qu'il faut retenir

- ◇ **Vous utilisez une connexion RTC ou RNIS via le CRI :** un firewall placé sur les serveurs du CRI vous protège efficacement. Vous n'avez pas besoin de vous en procurer un.

◇ **Vous utilisez une connexion ADSL** : vous devez être particulièrement prudent. En effet, la possibilité de piratage est bien plus grande puisque la connexion est quasiment permanente. Cela revient à accrocher un panneau sur votre porte d'entrée indiquant qu'elle est ouverte 24 h / 24h ! Cependant, si vous utilisez une Freebox, LiveBox et autres 9Box, vous pouvez être tranquille : ces outils font office de routeur filtrant, et la plupart n'ont besoin d'aucune configuration.

À noter : vous pouvez opter pour la mise en place d'un routeur. Cet outil est l'équivalent de l'agent de circulation : il s'assure que vos requêtes sont acheminées à bon port. Il peut donc filtrer les adresses IP, et est généralement moins lourd à configurer qu'un firewall logiciel.

◇ **La mise en place d'un firewall logiciel est contraignante**. Rien n'est jamais simple en informatique. Un firewall est gourmand en ressources : bloquer et vérifier tout ce qui passe demande un gros effort qui peut ralentir notablement votre machine. C'est encore plus vrai si vous l'avez associé à un anti-virus et un anti-spam.

Astuce : un vieil ordinateur sous Linux peut faire un excellent firewall matériel : la distribution IPCOP, par exemple, est orientée vers le firewalling. Elle est gratuite et simple à installer.

À noter : les systèmes d'exploitation Windows XP, dont l'amélioration en terme de sécurité est notable, tendent à intégrer par défaut ce type de fonctionnalités.

Installer un Firewall logiciel

Il convient simplement de configurer au préalable votre firewall, afin de lui dire ce qu'il doit laisser passer et ce qu'il doit bloquer : ce sont **les règles de filtrage**.

Le serveur FTP du CRI vous propose 3 firewall pour Windows à télécharger (attention, seuls leurs éditeurs sont garants de leurs produits) :

Vous devez le configurer de manière à ne rien laisser entrer sans autorisation :

- ◇ Qui autorisez-vous à se connecter chez vous et par quelle voie de communication ?
- ◇ Quels logiciels autorisez-vous à se connecter sur Internet, vers qui et comment ?

Votre firewall est fourni avec des règles de filtrage qui répondent en partie à ces questions. La configuration à l'installation est très simple : le firewall se contente de demander s'il faut tout interdire ou tout autoriser. Ensuite, à chaque fois que vous lancerez une application, vous aurez à l'autoriser ou non à s'exécuter. Vous pourrez également décider de l'autoriser « définitivement » ou l'autoriser à chaque fois qu'elle se lance.

Exemple :

Votre logiciel de messagerie cherche à communiquer avec le serveur `www.domaine.net` sur le port 20. Ce port est réservé au FTP et non à la messagerie. Vous devez donc refuser la connexion. Mais s'il cherche à dialoguer avec `pop.edres74.net` sur le port 110 (courrier), vous pouvez l'autoriser (le CRI74 étant votre fournisseur d'accès, il est normal que votre outil de messagerie s'adresse à lui pour relever vos e-mails).

À noter :

- ◇ Il convient d'autoriser les programmes les plus utilisés à fonctionner. Sinon, vous devrez autoriser le programme à fonctionner à chaque utilisation. La messagerie et la navigation sont particulièrement concernés.
- ◇ Vous devrez autoriser le firewall à accepter ou refuser à nouveau toutes les applications à chaque fois que vous les mettez à jour, car il ne les reconnaîtra plus.

Les Firewall téléchargeables sur le serveur FTP du CRI74

ftp.cri74.org dossier **pub** puis **Win9x**

À noter : les firewall proposés par le CRI74 ne concernent que les systèmes d'exploitation Windows. En effet, les machines sous Linux, moins sensibles par définition, possèdent par ailleurs toutes les fonctionnalités nécessaires au firewalling. Directement intégrées au système, ces fonctionnalités ne sont pas gourmandes en ressources. Libres et gratuites, les distributions Linux présentent décidément bien des avantages !

◇ **Kerio Personal :**

- Si ce logiciel est gratuit pour un usage « personnel », l'utilisation de sa version complète est cependant limitée à 30 jours. Ce délai passé, il passe en version « free » qui a quelques fonctionnalités en moins.
- multilingue (dont le français) mais installation en anglais/allemand
- Prise en main assez simple : 1 mode "basique" et 1 mode "avancé" vous permettront de configurer « finement » le logiciel.

L'avis du CRI : Kerio Personal est un bon firewall qui propose même en version « free » tout le nécessaire.

◇ **ZoneAlarm Personal :**

- Gratuit pour un usage « personnel »
- Multilingue (dont français)
- La version « personal » est limitée dans certaines fonctionnalités, mais le principal fonctionne bien.

L'avis du CRI : une configuration fine peut s'avérer assez compliquée, mais les réglages par défaut suffisent en général. Ce firewall est tout à fait recommandable.

◇ **Sygate Personal :**

- Gratuit pour un usage « personnel »
- La dernière version 5.6 n'a pas été traduite en français.

L'avis du CRI : une configuration fine peut s'avérer assez compliquée, mais les réglages par défaut suffisent en général. Si vous ne souhaitez pas la version en anglais, vous pouvez prendre la 5.1 qui a été traduite.

Conclusion

◇ Un firewall personnel n'offre pas une protection parfaite. Du fait même de sa présence sur le poste de l'utilisateur, il reste particulièrement vulnérable : certains virus, certains troyens ou d'autres programmes hostiles peuvent ainsi désactiver ou contourner un firewall personnel (qui, encore une fois, ne filtre pas les données et n'empêche donc pas ces programmes de pénétrer).

Un minimum de vigilance reste nécessaire, et il est notamment indispensable de ne pas exécuter sans réfléchir les fichiers joints aux courriers électroniques que vous recevez. Un anti-virus est le complément naturel d'un firewall personnel (voir CRI Pratique n° 2 sur les virus)

◇ Méfiez-vous également de ce qu'on appelle le social Engineering (que l'on peut traduire par ingénierie sociale), qui consiste à exploiter la naïveté et la gentillesse des utilisateurs du réseau pour obtenir des informations sur ce dernier. Ce procédé consiste à entrer en contact avec un utilisateur du réseau (par e-mail, ou par téléphone ;..) afin d'obtenir des renseignements sur le système d'information ou pour obtenir directement un mot de passe. S'il vous semble normal de ne pas révéler votre code de carte bleue à un inconnu, adoptez le même réflexe en ce qui concerne vos codes informatiques !

◇ Il est toujours préférable d'avoir un équipement en amont de votre machine pour tout ce qui touche à la sécurité : un modem/routeur ADSL, un routeur RNIS, et sans oublier PingOO qui fait office de firewall !

À noter : si vous utilisez un modem/routeur ADSL (de type freebox ou autre), il faut absolument choisir l'option NAT. En effet, c'est cette technologie qui rendra votre machine invisible depuis Internet, en « déguisant » votre adresse IP de manière à ce qu'elle ne soit pas identifiable depuis Internet. C'est cette adresse IP masquée qui sera visée par des attaques éventuelles. Or, comme elle ne correspond plus à votre machine, celle-ci est donc protégée. Cette option NAT est donc très importante. Si vous ne la cochez pas, votre machine est plus vulnérable.

POUR RÉSUMER

- ◇ Il faut adopter une politique très stricte de sécurité en fermant tout pour n'autoriser qu'au cas par cas.
- ◇ Les firewall personnels et gratuits ne peuvent pas tout faire...
- ◇ Et sont obligatoirement à associer avec un antivirus et... une attitude responsable et consciente ! Ne sous-estimez pas les risques : les pirates, en effet, ne s'intéressent pas particulièrement à vos photos de famille ou à vos courriers personnels. Mais leur but est d'atteindre un maximum de machines et de faire un maximum de dégâts. Ils attaquent donc au hasard, mais massivement. Sachez ainsi qu'une machine sous Windows exposée sans protection sur Internet a une durée de vie de 4 minutes seulement !
- ◇ Le CRI74 assure la sécurité des utilisateurs qui ont une connexion RTC ou RNIS sur ces aspects.
- ◇ Pour les structures qui ont une connexion ADSL, il est essentiel de protéger leur réseau local : PingOO IGWan est spécialement conçu pour protéger les échanges sous ADSL (même si le CRI74 ne vous fournit pas l'accès ADSL, il peut vous fournir tous les services liés. N'hésitez pas à le contacter !).

POUR PLUS D'INFORMATIONS SUR LES LOGICIELS FIREWALL

- ◇ <http://www.firewall-net.com/>
- ◇ http://www.secuser.com/dossiers/firewall_personnel.htm
- ◇ <http://www.commentcamarche.net/pratique/zonealarm.php3>

Événements

◇ SÉMINAIRE : FIREFOX 1.0 & SES EXTENSIONS

Réappropriiez-vous le Web grâce à Firefox 1.0, le navigateur libre de Mozilla : rapide, efficace, sécurisé, puissant et multi-plates-formes. **Inscription et renseignement sur <http://www.cri74.org/>**

- Date : Mercredi 13 Avril.
- Lieu : Salle Menoge, Rez-de-chaussée Bâtiment Salève I, Site d'Archamps (74).
- De 14h00 à 15h45 : les fonctionnalités de Firefox 1.0.
- Public : grand public, utilisateur final.
- De 15h45 à 17h00 : les extensions de Firefox 1.0.
- Public : public averti, webmasters, informaticiens, administrateurs système.

◇ LINUXEDU 2005, SOLUTIONS LIBRES & TICE

La 3ème édition de LinuxEdu aura lieu du 19 au 21 mai. Réservez la date dès maintenant !

Destiné aux collectivités et aux acteurs de l'éducation, LinuxEdu est également ouverte à tous ceux qui souhaitent découvrir ces outils informatiques.

LinuxEdu propose 3 journées de conférences, d'ateliers, de présentations de logiciels métier et d'échanges riches et conviviaux.

Inscription et programme sur <http://www.linuxedu.org/>