Fiche Technique

e pare-feu de Windows Le pare-feu de Windows 7

Présentation du problème

On peut parfaitement protéger son ordinateur gratuitement : Rappel : Votre sécurité sur Internet nécessite plusieurs logiciels installés et lancés en permanence.

- 1. Un antivirus (les gratuits sont Avast, AVG, Microsoft Security Essentials)
- 2. Un pare-feu (ne pas désactiver celui du Windows 7, qui est efficace)
- 3. Un logiciel pour surveiller les sites visités (McAfee site Advisor)
- 4. Des logiciels comme spybot et malware byte's anti malware que l'on lance régulièrement.

Vous devez faire un scan régulièrement avec votre antivirus, et les deux derniers logiciels cités. Spybot possède d'ailleurs un résident sensé vous protéger sur Internet mais ... Si malgré toutes ces précautions, vous réussissez à attraper un virus ou trojan, ce qui peut vous arriver par un script (Java, VBS, Java Script) depuis un message de type spam en html ou depuis une page vérolée sur Internet, il vous reste encore trois solutions efficaces.

- 1. Téléchargez la dernière version de Stinger (logiciel gratuit de chez McAfee, mis à jour régulièrement). Installez-le et exécutez-le. Supprimez les malwares éventuellement trouvés)
- 2. Téléchargez Kapersky Virus Removal Tools, lui aussi gratuit. Il s'installe, s'exécute et se désinstalle dans la foulée après avoir supprimé les malwares.
- 3. Si les ennuis persistent (c'est rare), rendez-vous sur Secuser.com et cherchez un traitement approprié au malware (généralement un trojan qui vous est signalé par les autres logiciels mais qui n'a pas réussi à être éradiqué)

Le pare-feu va lui servir à empêcher certains logiciels malwares d'entrer et de s'installer sur votre ordinateur. De même en sortie. Le but est d'empêcher ces logiciels de communiquer, moucharder lorsque vous vous connectez. Ces logiciels peuvent essayer de transformer votre ordinateur en zombie. Un pirate prend la main sur votre ordinateur pour lui faire exécuter des actions illicites, pour pister vos mots de passe ou votre numéro de carte bleue avec un key logger, essayer de voler ou polluer votre carnet d'adresse etc...l'imagination des pirates n'a pas de limite. Concernant votre vie privée, une inscription sur Facebook est déjà dangereuse, si vous y laissez des informations personnelles ou confidentielles.

En résumé le pare-feu est un bouclier chargé de protéger votre PC :

- 1. Contre les intrusions (en entrée)
- 2. Contre les logiciels de piratage (en sortie).

En toute logique un logiciel qui envoie des renseignements en **sortie** a commencé par **entrer pour s'installer sur votre PC.**

sociation loi 1901

er Informatique

Siège Sallan-Miré

Vidéo Multimédi

Les vecteurs de pollution

Il existe un peu plus de 65000 adresses pour qu'un ordinateur communique avec l'extérieur. Certains malwares utilisent ces adresses pour communiquer. Ces trous de non sécurité sont utilisés dans les logiciels du type Adobe Reader, Flash player, Internet Explorer, Firefox et autres. Les langages Java, JavaScript et VB Script sont les supports de transmission. Ces logiciels de communications sont évidemment très exposés et des MAJ de sécurités sont très fréquentes. Il est indispensable de faire ces MAJ. Windows Update doit être actif. Les newletters de Secuser.com, Clubic ou PcAstuces vous permettent de vous tenir informer sur ces MAJ.

Pare-feu de Windows 7

Accéder au pare-feu

Deux solutions.

- Bouton Démarrer → Tapez Parefeu dans la zone de recherche → Sélectionnez Pare-feu Windows dans la rubrique panneau de configuration.
- Ouvrez le panneau de configuration → Section Système et sécurité → Pare-feu Windows

| Programmes (1) | - |
|--|---|
| Pare-feu Windows avec fonctions avancées de sécurité | |
| Panneau de configuration (4) | - |
| 🔗 Pare-feu Windows | |
| 😭 Autoriser un programme via le Pare-feu Windows | |
| 🔐 Vérifier l'état du pare-feu | |
| 🚩 Vérifier l'état de sécurité | |
| Documents (18) | - |
| av\$095_Pare-feuWindows7.docx | |
| IT095_Pare-feuWindows7.docx | |
| 🔁 JT094_OutilsSystem.pdf | |
| Évaluation de la sécurité avec Baseline.docx | |

Le pare-feu



Voici l'écran qui se présente. Les actions à mener se trouvent sur la gauche de votre écran. Les règles sont plus strictes sur un réseau public que sur un réseau privé ce qui est normal.

| Assurez-vous que votre | e pare-feu est actif en | liquant sur « Activer ou | désactiver le Pare-feu | Windows ». |
|------------------------|-------------------------|--------------------------|------------------------|------------|
| | • | | | |

| 20 | | Taura las Danasas | unde service a Dese for Windows & Deserve lies he serve these | Deaharrhan | |
|-----------------|-----------------|-------------------------------|---|------------|--|
| |) • 🔤 « | Tous les Panneau | ix de configuration + Pare-feu Windows + Personnaliser les parametres | Rechercher | |
| <u>F</u> ichier | <u>E</u> dition | <u>A</u> ffichage <u>O</u> ut | ils <u>?</u> | | |
| | | Person | naliser les paramètres pour chaque type de réseau | | |
| | | Vous pou | uvez modifier les paramètres de pare-feu pour chaque type d'emplacement réseau que yous utilisez. | | |
| | | Que sont | t les emplacements réseau ? | | |
| | | Paramèt | res des emplacements réseau domestique ou d'entreprise (privés) | | |
| | | | O Activer le Pare-feu Windows O | | |
| | | • | Bloquer toutes les connexions entrantes, y compris celles de la liste des programmes autorisés | | |
| | | | 📝 Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme | | |
| | | 8 | Désactiver le Pare-feu Windows (non recommandé) | | |
| | | Paramèt | res des emplacements réseau public | | |
| | | | Activer le Pare-feu Windows | | |
| | | | Bloquer toutes les connexions entrantes, y compris celles de la liste des programmes autorisés | | |
| | | | 📝 Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme | | |
| | | 8 | Désactiver le Pare-feu Windows (non recommandé) | | |
| | | | | | |
| | | | OK Annuler | | |

Vous pouvez modifier les paramètres, mais jamais vous ne devez <u>« Désactiver ».</u> Ceci dit tout bloquer ne peut être qu'une solution temporaire, sur un site douteux. Mais que faites-vous sur un site douteux ? Attention tout de même, les sites douteux ne sont pas toujours ceux auxquels on pense. Un beau site avec des images du Pérou, anodin peut s'avérer dangereux. Voir ce que signale McAfee site Advisor.

Le lien « Autoriser un programme »

| | | | | | | x |
|------------------------------|--|-------------------------------|-------------------|--------------|------------|---|
| 🔾 🗢 🗑 « Tous | les Panneaux de configuration 🔸 Pare-feu Windows 🕨 Pro | ogrammes autorisés | _ | ▼ 4 9 | Rechercher | ٩ |
| <u>Fichier</u> Edition Affic | hage <u>O</u> utils <u>?</u> | | | | | |
| | | | • | | | * |
| | Programmes et fonctionnalités <u>a</u> utorisés : | | | | | |
| | Nom | Domestique/entreprise (privé) | Public 🔺 | | | |
| | Assistance à distance | \checkmark | | | | |
| | Connexion à un projecteur réseau | | | | | |
| | Coordinateur de transactions distribuées | | | | | |
| | CyberLink Media Service | V | | | | |
| | CyberLink Media Service | V | | | | |
| | CyberLink PowerDirector | | | | | |
| | ✓ FileZilla FTP Client | | | | | |
| | ✓ Firefox | V | | | | = |
| | Gestion à distance de Windows | | | | | |
| | Gestion à distance des journaux des événements | | | | | |
| | Gestion à distance des tâches planifiées | | | | | |
| | Gestion à distance du Pare-feu Windows | | | | | |
| | | Détai <u>l</u> s | <u>S</u> upprimer | | | |
| | | Autoriser un autre p | rogramme | | | |
| | | OK | Annuler | | | |

Vous voyez ici les programmes autorisés (en privé ou en public) ceux qui ne sont pas cochés, donc interdits. Pour ajouter vous-même un programme, cliquez le bouton « Autoriser un autre programme » et inscrivez le programme. Soyez cependant conscient de ce que vous faites. Vous pouvez aussi désactiver un programme douteux

Fonctions avancées de sécurité

| Pare-feu Windows avec fonctions avancées de sécurité | | | | | | | | | | | |
|--|--|------------------------------|----------|---------|-----------|-----------|-------------|----------------|-------------|--------------------------|----------|
| Eichier Action Affichage ? | | | | | | | | | | | |
| (= =) (2 🗔 🔒 🛛 🗔 | | | | | | | | | | | |
| Pare fau Windows was fan stie | Rooles de trafic entrant Actions | | | | | | | | | | |
| Règles de trafic entrant | Regles de trafic entrant | | | | | | | | Actions | | |
| Règles de trafic sortant | Nom | Groupe | Profil | Activée | Action | Remplacer | Programme | Adresse locale | Adresse (^ | Règles de trafic entrant | ^ |
| Règles de sécurité de conne | Service de partage réseau du Lecteur Win | Service de partage réseau d | Public | Non | Autoriser | Non | %SystemRo | Tout | Sous-rés | 🚉 Nouvelle règle | |
| Analyse | 🔇 Service de partage réseau du Lecteur Win | Service de partage réseau d | Domaine | Oui | Autoriser | Non | %SystemRo | Tout | Tout | Filtrer par profil | • |
| | Service de partage réseau du Lecteur Win | Service de partage réseau d | Privé | Oui | Autoriser | Non | %SystemRo | Tout | Sous-rés | 🐨 Eiltror par átat | |
| | Service de partage réseau du Lecteur Win | Service de partage réseau d | Public | Non | Autoriser | Non | %SystemRo | Tout | Sous-rés | | |
| 4 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Domain | Oui | Autoriser | Non | %SystemRo | Tout | Sous-rés | Filtrer par groupe | • |
| 4 1 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Public | Non | Autoriser | Non | %SystemRo | Tout | Sous-rés | Affichage | • |
| 4 1 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Privé | Oui | Autoriser | Non | %PROGRAM | Tout | Sous-rés | Actualiser | |
| 4 1 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Domaine | Oui | Autoriser | Non | %PROGRAM | Tout | Tout | Evporter la liste | |
| 4 1 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Public | Non | Autoriser | Non | %PROGRAM | Tout | Sous-rés | Exporter la liste | |
| 4 1 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Privé | Oui | Autoriser | Non | %PROGRAM | Tout | Sous-rés | Aide | |
| 4 1 | Service de partage réseau du Lecteur Win | Service de partage réseau d | Public | Non | Autoriser | Non | %PROGRAM | Tout | Sous-rés | | |
| | Service de partage réseau du Lecteur Win | Service de partage réseau d | Domaine | Oui | Autoriser | Non | %PROGRAM | Tout | Tout | | |
| | Service de partage reseau du Lecteur Win | Service de partage reseau d | Public | Non | Autoriser | Non | System | Tout | Sous-res | | |
| | Service de partage reseau du Lecteur Win | Service de partage reseau d | Domain | Oui | Autoriser | Non | System | Tout | Sous-res | | |
| | Service de partage reseau du Lecteur Win | Service de partage reseau d | Domain | Non | Autoriser | Non | System | Tout | Tout | | |
| | Service ISCSI (TCP-Entree) | Service ISCSI | Domaine | Non | Autoriser | Non | %Systemko | Tout | Tout | | |
| | Service ISCSI (TCP-Entree) | Service ISCSI | Prive, P | Non | Autoriser | Non | %Systemico | Tout | Sous-resi | | |
| | Unites Media Center Extender - Diffusion | Unites Media Center Extender | Tout | Non | Autoriser | Non | System | Tout | Sous-resi | | |
| | Unites Media Center Extender - Dirusion | Unites Media Center Extender | Tout | Non | Autoriser | Non | System Ro | Tour | Sous-resi | | |
| | Unites Media Center Extender - gwave (1 | Unites Media Center Extender | Tout | Non | Autoriser | Non | %SystemRo | Tout | Sous-resi | | |
| | Munités Media Center Extender - Qwave (0 | Unités Media Center Extender | Tout | Non | Autoriser | Non | %SystemRo | Tout | Sourceée | | |
| | Unités Media Center Extender - KSTP (TC | Unités Media Center Extender | Tout | Non | Autoriser | Non | %SystemRo | Tout | Sous rés | | |
| | Munités Media Center Extender - 330P (00 | Unités Media Center Extender | Tout | Non | Autoriser | Non | %SystemRo | Tout | Sourceée | | |
| | Munités Media Center Extender - VSD (TCD | Unités Media Center Extender | Tout | Non | Autoriser | Non | System | Tout | Sous-rés | | |
| | Windows Live Messenger | Windows Live Messenger | Tout | Oui | Autoriser | Non | C:\Program | Tout | Tout | | |
| | Windows Live Messenger (SSDP-In) | Windows Live Messenger | Tout | Oui | Autoriser | Non | sychost eve | Tout | Sous-rési | | |
| | Windows Live Messenger (UPnP-In) | Windows Live Messenger | Tout | Oui | Autoriser | Non | System | Tout | Sous-rés | | |
| | Windows Peer to Peer Collaboration Fou | Windows Peer to Peer Colla | Tout | Oui | Autoriser | Non | %SystemRo | Tout | Tout | | |
| | Windows Peer to Peer Collaboration Fou | Windows Peer to Peer Colla | Tout | Oui | Autoriser | Non | %SystemRo | Tout | Sous-rési ≡ | | |
| | Windows Peer to Peer Collaboration Fou | Windows Peer to Peer Colla | Tout | Oui | Autoriser | Non | %SystemRo | Tout | Tout | | |
| | Windows Peer to Peer Collaboration Fou | Windows Peer to Peer Colla | Tout | Oui | Autoriser | Non | %SystemRo | Tout | Sous-rés + | | |
| ۰ III ا | • | III | | | | | - | | F | | |
| | | | | | | | | | | , | |

A vous de modifier. Ce n'est pas facile. Faites des recherches sur Internet pour vous aider à prendre une décision. Cherchez des tutoriaux. Eviter les forums, au langage de Chimpanzés, ou l'on peut vous raconter tout et n'importe quoi.

Pour ceux qui ne veulent pas que le pare-feu pose des questions

Cliquez sur « Modifier les paramètres de notification » à la page d'accueil du pare-feu



Fiche Technique



Décocher alors « Me prévenir lorsque le pare-feu Windows bloque un nouveau programme. Je pense que la politique de l'autruche, n'est pas la bonne solution. Il est préférable d'être informé qu'un logiciel tente de forcer le pare-feu.

Vous trouverez un dossier qui complète celui-ci chez PcAstuces à l'adresse suivante : <u>http://www.pcastuces.com/pratique/windows/parefeu_windows7/page1.htm</u>

Sur Windows News, un article du journaliste **Jean-Paul Mesters** auteur du site <u>http://www.docmemo.com</u> propose une solution pour réinitialiser le pare-feu. J'ai regroupé les instructions dans un fichier batch que vous trouverez compressé en ZIP à l'adresse suivante <u>http://aivm.free.fr/BI/Erreur0X8007042C.zip</u>

Autre fiche Voir aussi la fiche 109. http://aivm.free.fr/BI/JT/JT109_Pare-feuWindows7.pdf