Tutoriel : configurer le pare-feu (firewall) de Windows XP

Date de dernière mise à jour : 27/06/2007 à 19:36

Source : http://www.vulgarisation-informatique.com/pare-feu-xp.php. Distribution interdite sans accord écrit d'Anthony ROSSETTO (http://www.vulgarisation-informatique.com/contact.php)

Pour qui ne dispose pas d'un pare-feu plus évolué, le pare-feu inclus avec Windows service pack 2 (SP2) suffira pour assurer une sécurité suffisante pour qui ne télécharge pas n'importe quoi. Il dispose désormais de règles de filtrage basiques qui vous permettront de contrôler plus efficacement les **connexions entrantes**. Et oui, la nouvelle mouture du pare-feu XP ne contrôle toujours pas les connexions sortantes. Autrement dit, si vous avez un programme traître sur votre PC qui envoie des informations via votre connexion internet par exemple, ce programme a de grandes chances de ne pas être inquiété.

Après vous avoir légèrement refroidi (le but étant simplement de faire prendre conscience qu'en ne téléchargeant pas n'importe quoi, on a de grandes chances d'avoir un PC sain pour de très longues années), passons à la présentation puis à la configuration de ce firewall :

Désormais accessible via le panneau de configuration, le pare-feu ICS (pour **Internet connection firewall**) dispose de sa propre icône intitulée comme son nom ne l'indique pas " **pare-feu Windows**". Double-cliquez dessus, vous arrivez face à une fenêtre de ce style :



Tout d'abord, commencez par activer le firewall en sélectionnant Activé (recommandé). Laissez la case Ne pas autoriser d'exceptions décochée (les exceptions sont des actions qui ne rentrent pas dans les règles préétablies, comme par exemple le lancement pour la première fois d'un client FTP qui reçoit des données). Cliquez ensuite sur l'onglet Exceptions. Nous allons pouvoir via cet onglet configurer le pare-feu un peu plus finement. Un écran ressemblant à celui-ci s'ouvre alors :

Pare -	feu Window		
Général	Exceptions	wancé	
Le Pare et servi progran	e-feu Windows ces sélectionné nmes de mieux nmes et service	loque les connexions réseau entrantes ci-dessous. Le fait d'ajouter des exce sinctionner, mais peut également augm	a, à l'exception des programmes ptions peut permettre à certains enter vos risques
Nom			1
As	sistance à dist	nce	
B	ireau à distanc		
	a second second		

Par défaut, une liste de programmes et services sera affichée. Cette liste n'est pas exhaustive. Les exceptions sont stockées dans la base de registres à la clé suivante : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\ StandardProfile (ou DomainProfile)\AuthorizedApplications\List. Vous allez pouvoir ici contrôler quels programmes peuvent recevoir des données de l'extérieur sans provoquer d'alerte du système. Les alertes du firewall se présentent généralement comme ça :

🎽 Aleri	te de sécurité Windows 🛛 🔁
V	Pour vous aider à protéger votre ordinateur, le Pare-feu Windows a bloqué certaines fonctionnalités de ce programme.
Voulez	-vous continuer à bloquer ce programme ?
FC	<u>N</u> om : FTP Expert Édit <u>e</u> ur : Visicom Media Inc. Maintenir le blo <u>c</u> age <u>D</u> ébloquer
	Maintenir le blocage et me redemander ultérieurement
Pour plu connexi program program	us de sécurité, le Pare-feu Windows bloque actuellement l'acceptation des ions Internet ou réseau pour ce programme. Si vous faites confiance à ce ime ou à son éditeur, vous pouvez le débloquer. <u>Quand puis-je débloquer un</u> i <u>me ?</u> Vulgarisation-informatique.com

Vous avez alors plusieurs options, si vous ne doutez pas du programme mentionné, débloquez le programme. Une exception sera ajoutée pour ce programme dans la liste des exceptions. Tout ça c'est bien beau, mais vous aimeriez peut-être en faire plus ? Le firewall vous permet d'ouvrir un port quel que soit le programme l'utilisant. Attention, ouvrir un port peut être dangereux si une application écoute sur ce port. Pour en savoir plus, je vous renvoie à la notion de port. Pour autoriser un port, cliquez sur **Ajouter un port**. Une petite fenêtre apparaît :

Ajouter un port		
Utilisez ces paramètres pour our le numéro et le protocole du por du service que voulez-vous utili	vrir un port du Pare-leu Window t, consultez la documentation d ser.	s. Pour identifier u programme ou
Nom:		
Numéro <u>d</u> u port :		
⊙ <u>I</u> CP	OUDP	
Quels sont les risques associés	à fouveiture d'un port ? Vulgarisation-inf	ormatique.com
Modifier l'étendue	QK	Annuler

Vous allez maintenant pouvoir entrer une description légère dans la zone **Nom**, ainsi que le numéro du port (vous pouvez par exemple mettre **80** si vous souhaitez ouvrir le port 80). Sélectionnez ensuite le mode de transmission (**TCP** ou **UDP**, si vous ne savez pas, faites d'abord l'opération en TCP, puis refaites la manipulation d'ajout de port en sélectionnant UDP). Tout cela est bien beau, mais vous avez peut-être envie de n'ouvrir ce port 80 uniquement pour une machine connectée à votre réseau local par exemple, et non pour tout le monde. Dans ce cas, il va falloir restreindre l'exception à une ou plusieurs adresses IP. Pour ce faire, cliquez sur **Modifier l'étendue**. Une fenêtre ressemblant à celle-ci s'ouvre alors :

Modifier l'étendue	×
Pour spécifier le jeu d'ordinateurs pour lequel ce port ou ce pr cliquez sur une option ci-dessous.	rogramme est débloqué,
Pour spécifier une liste personnalisée, entrez la liste des adre ou les deux types, délimités par des virgules.	sses IP, des sous-réseaux
○ N'importe quel ordinateur (y compris ceux présents :	sur Internet)
O Uniquement mon réseau (ou sous-réseau)	
● Liste personnalisée :	

Vous avez alors trois choix. Le premier est le choix par défaut, il permet à tout le monde de profiter de l'exception. Ce n'est pas intéressant dans notre cas puisque nous souhaitons restreindre l'exception. Le second choix vous permet de restreindre l'exception à tout ordinateur de votre réseau. Cela peut être intéressant dans le cas d'un réseau local. Le troisième choix est le plus restrictif de tous, vous pouvez n'autoriser qu'une adresse IP par exemple. Dans mon cas, j'ai choisi de n'autoriser que les connexions provenant de l'ip 192.168.0.2. Si vous souhaitez rajouter d'autres adresses IP, il suffit de les séparer par des virgules.

Vous allez maintenant pour chaque interface réseau (carte réseau, connexion internet) activer ou non le pare-feu. Cela se fait via le troisième onglet intitulé **Avancé** :

Pare-	feu Windows	
Général	Exceptions Avancé	
Paran Le Pa excej	mètres de connexion réseau are-feu Windows est activé pour les conne <u>x</u> ions sélectionnées. Pour ajouter des ptions à une connexion individuelle, sélectionnez-la puis cliquez sur Paramètres.	
	Club Internet Para <u>m</u> ètres Connexion 1394 Connexion au réseau local	
Journ Vous des p	al de sécurité pouvez créer un fichier journal pour vous aider à résoudre problèmes éventuels.	
Avec ordin. d'erre	: le protocole ICMP (Internet Control Message Protocol), les ateurs d'un réseau peuvent partager des informations uns et de statut.	
Paran Pour clique	nètres par défaut restaurer les valeurs par défaut du Pare-feu Windows, Par <u>d</u> éfaut ez sur Par défaut.	
	Vulgarisation-informatique.co	sm e

Pour chaque interface, cochez ou décochez la case présente pour activer ou désactiver le pare-feu pour l'interface sélectionnée. Si vous souhaitez en plus personnaliser les exceptions pour chaque interface réseau, sélectionnez l'interface pour laquelle vous souhaitez modifier les exceptions puis cliquez sur **Paramètres**.

Une petite fenêtre semblable à celle-ci apparaît :

rvic	es ICMP
éleo tilisa	clionnez les services activés sur votre réseau auxquels les ateurs Internet peuvent accéder.
ervi	ices :
	Bureau à distance
	DHCP (67)
	DHCP (68)
וכ	DNS
	Protocol IMAP4 (Internet Mail Access Protocol)
	Protocole IMAP3 (Internet Mail Access Protocol)
וכ	Protocole POP3 (Post-Office Protocol)
] :	Ser∨eur de messagerie Internet (SMTP)
] :	Serveur FTP
] :	Serveur Telnet
] :	Serveur Web (HTTP)
] :	Serveur Web sécurisé (HTTPS)
	UPnP (TCP)
	UPnP (UDP)

Vous allez pouvoir ici par exemple autoriser les internautes à accéder à divers services de votre ordinateur. Si vous cochez par exemple la case **serveur web** le port 80 sera accessible de l'extérieur. Si vous souhaitez personnaliser les règles permettant d'accéder ou non à votre ordinateur, cliquez sur **Ajouter**. Une fenêtre apparaît :

Paramètres de service		? 🔀
Description du service :		-
Nom ou adresse IP (par exemple 192 l'ordinateur hôte de ce service sur vo	2.168.0.12) de otre réseau :	
Numéro du <u>p</u> ort externe de ce servic	e:	
Ki wa da mana ta kao a sa s		P
Numero au port interne de ce service	91	
Vulg	arisation-informatio	que.com
	OK Anni	ler

Vous pouvez maintenant entrer une description de votre choix dans la première case. La seconde case désigne l'ordinateur qui pourra "recevoir la demande provenant d'internet". Si il s'agit de votre ordinateur actuel (sur lequel vous êtes en train de configurer le pare-feu), indiquez "127.0.0.1". Indiquez ensuite le numéro du port externe, puis celui du port interne (en TCP ou UDP). Le numéro du port externe sera le numéro du port par lequel les utilisateurs d'internet accèderont au service. Le numéro du port interne est quant à lui le numéro de port à utiliser pour que l'application située sur votre ordinateur puisse répondre. Prenons un exemple simple : Vous disposez d'un serveur web qui écoute par défaut sur le port 80. Or, le port 80 est très connu. N'importe qui connaissant votre adresse IP peut accéder à votre serveur web. Vous souhaiteriez que les utilisateurs utilisent le port 82 pour accéder à votreserveur web (qui je le rappelle écoute sur le port 80, port que vous avez bloqué). Dans ce cas, vous indiquerez "82" pour le port externe, et 80 pour le port interne du service. On appelle cette opération de la **redirection de port**, ou encore **port forwarding**. Cliquez sur Ok le nombre de fois nécessaires pour fermer le pare-feu Windows. Vous aurez peut-être besoin de vous déconnecter puis vous reconnecter à internet pour que les changements prennent effet.

Source : http://www.vulgarisation-informatique.com/pare-feu-xp.php. Distribution interdite sans accord écrit d'Anthony ROSSETTO (http://www.vulgarisation-informatique.com/contact.php)