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

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

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 :

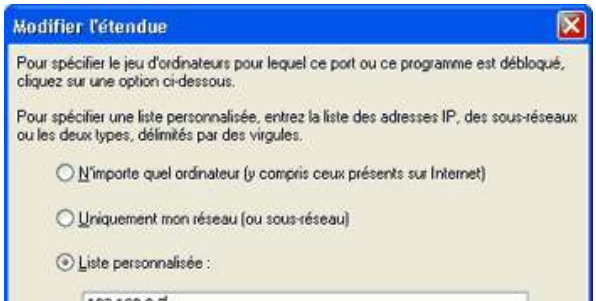
Désormais accessible via le panneau de configuration, le pare-feu ICS (pour **Internet connection firewall**) dispose de sa propre icône intitulée comme son nom ne l'indique pas "**pare-feu Windows**". Double-cliquez dessus, vous arrivez face à une fenêtre de ce style :

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 :

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 :

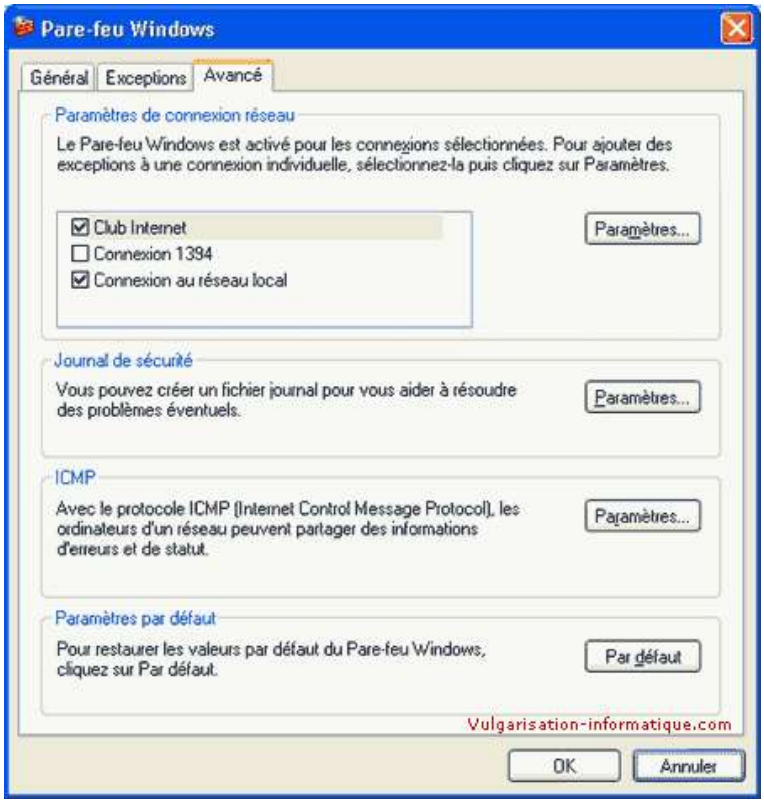
Vous avez alors plusieurs options, si vous ne doutez pas du programme mentionné, débloquez le programme. Une exception sera ajoutée pour ce programme dans la liste des exceptions. Tout ça c'est bien beau, mais vous aimeriez peut-être en faire plus ? Le firewall vous permet d'ouvrir un port quel que soit 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 :

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 :



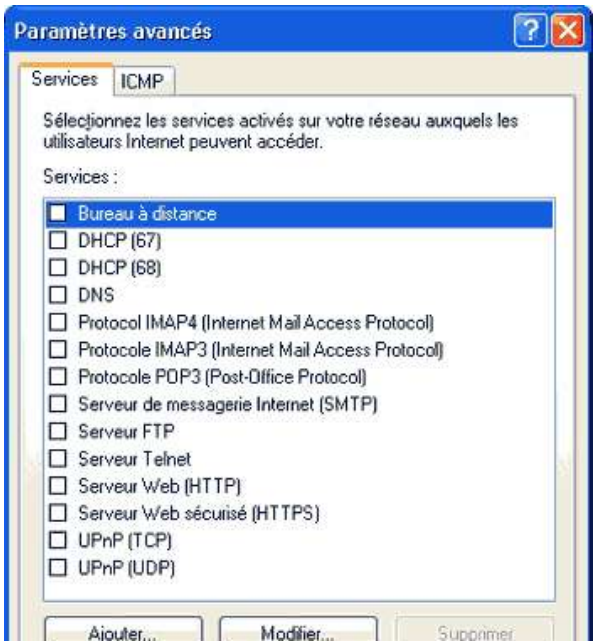
Vous avez alors trois choix. Le premier est le choix par défaut, il permet à tout le monde de profiter de l'exception. Ce n'est pas intéressant dans notre cas puisque nous souhaitons restreindre l'exception. Le second choix vous permet de restreindre l'exception à tout ordinateur de votre réseau. Cela 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** :



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 :



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 :

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.