Paramétrer Kerio Personal

Contrairement au pare-feu de Windows XP, Kerio Personal Firewall doit être soigneusement configuré, mais la protection qu'il assure est alors bien supérieure.

Inutile d'installer Kerio Personal Firewall si vous en acceptez les paramètres par défaut. Vous obtiendriez alors le même niveau de sécurité qu'avec le pare-feu de Windows XP. Pour une protection optimale, vous devez indiquer à Kerio Personal Firewall quels logiciels installés sur votre PC sont autorisés à envoyer ou récupérer des informations sur Internet... mais aussi quels protocoles et quels ports ils sont censés utiliser ! Pour chaque logiciel accédant à Internet, il faut donc que vous définissiez une règle de filtrage adaptée (parfois même plusieurs). Une opération très simple, à condition de savoir comment procéder... Nous détaillons ici la marche à suivre pour les logiciels les plus couramment employés.

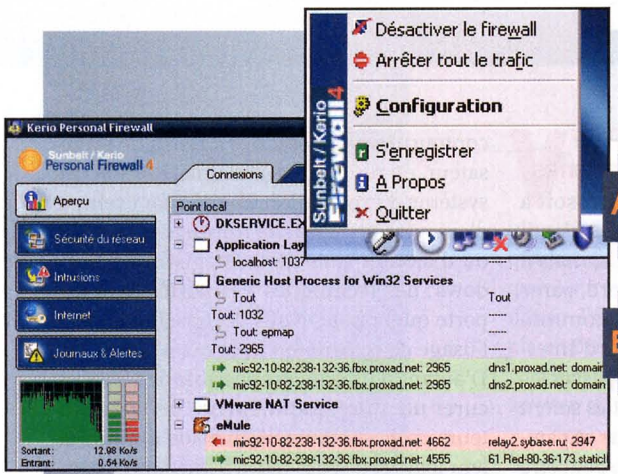
Installer le pare-feu

1 TELECHARGEZ LE LOGICIEL

Rendez-vous sur le site Web de Sunbelt ***(www.sunbelt-software.com /Kerio-Download.cfm).*** Après avoir saisi vos prénom, nom et adresse e-mail, cliquez sur le bouton **Download Sunbelt Kerio Personal Firewall !** Cliquez sur le lien **Download,** à gauche de **NON-English Only Version 4.2.3.912.** Le téléchargement effectué, double-cliquez sur le fichier récupéré (kerio-912.exe) pour lancer l'installation.

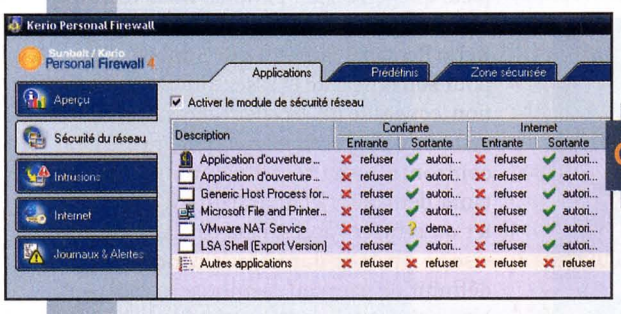
2 PROCEDEZ A L'INSTALLATION

Le logiciel a été francisé mais pas son assistant d'installation, qui est proposé en anglais ou en allemand. Sélectionnez **Anglais** et cliquez sur **OK.** Cliquez sur **Next,** deux fois. Cochez **I accept the terms...** et cliquez sur **Next,** deux fois. Laissez l'option **Simple** sélectionnée : le pare-feu fonctionnera comme celui de Windows XP, les demandes de communication sortantes étant toujours autorisées, et les entrantes toujours bloquées. Nous modifierons ces paramètres par la suite. Cliquez sur **Next,** sur **Install** puis, après la copie des fichiers, sur **Finish.** Enfin, cliquez sur **Yes** pour redémarrer l'ordinateur.



3 DECOUVREZ L'INTERFACE

La barre des tâches de Windows XP compte désormais une icône supplémentaire représentant un bouclier. Un clic droit dessus fait apparaître un menu déroulant qui comporte diverses options : **Désactiver le firewall, Arrêter tout le trafic** et **Configuration** (voir écran A). Cliquez sur cette dernière option pour accéder au panneau de configuration de Kerio Personal Firewall (KPF). C'est ici que vous pourrez paramétrer le pare-feu, mais aussi surveiller en temps réel l'activité réseau du PC (échanges avec Internet et aussi, s'il y a lieu, avec les autres ordinateurs du réseau local). Pour cela, cliquez sur l'onglet **Aperçu,** à gauche, et **Connexions,** en haut (voir écran B).



4 EXAMINEZ LES AUTORISATIONS PAR DEFAUT...

Un clic sur l'onglet **Sécurité du réseau,** à gauche, affiche les paramètres que KPF a définis automatiquement pour certains composants de Windows XP (voir écran C), comme par exemple le gestionnaire d'impression. Pour chaque logiciel, le pare-feu indique le comportement qu'on lui a demandé d'adopter en fonction de deux critères : la zone d'où provient la demande de communication, **Confiante** (c'est-à-dire en local) ou **Internet ;** et la direction de la communication, **Entrante** (à destination du logiciel) ou **Sortante** (émanant du logiciel). Un **X** rouge indique que KPF bloque le trafic, un **V** vert qu'il l'autorise, et un **?** jaune qu'il doit demander à l'utilisateur.

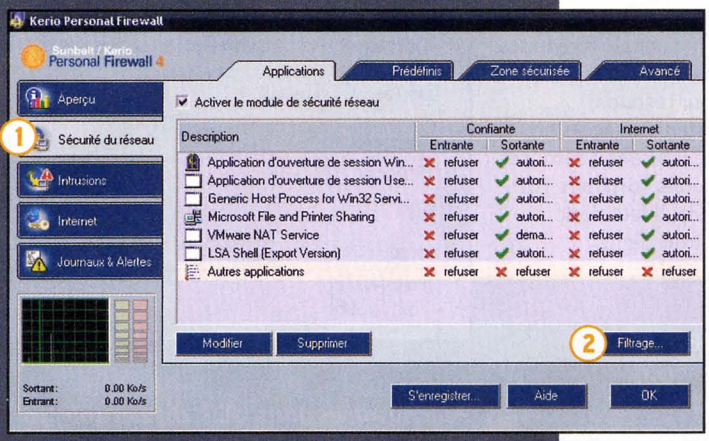
5 ... ET ANNULEZ-EN CERTAINES

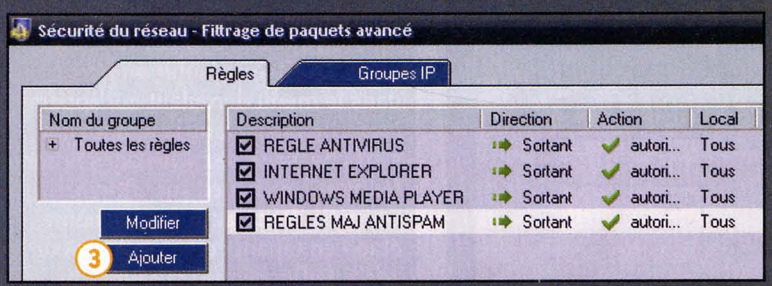
La catégorie **Autres applications** concerne tous les logiciels pour lesquels KPF n'a pas encore d'instructions précises. Dans ce cas, le pare-feu est paramétré par défaut pour bloquer toutes les requêtes entrantes et autoriser toutes les sortantes. Un comportement trop permissif. Cliquez plusieurs fois sur les **V** verts de la ligne pour tous les transformer en **X** rouges, et cliquez sur **Appliquer.** Désormais, les logiciels pour lesquels aucune règle de filtrage n'a été définie ne peuvent plus communiquer avec l'extérieur.

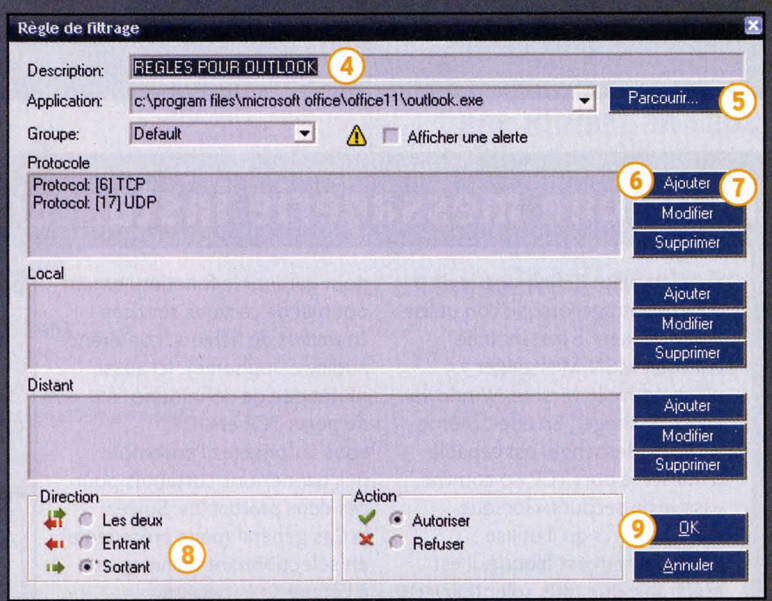
Firewall

Cas général pour la plupart des logiciels

Le plus souvent, les logiciels qui accèdent à Internet utilisent plusieurs protocoles réseau standard pour envoyer ou récupérer des données. Un navigateur Web exploite ainsi trois protocoles : le HTTP (port TCP 80) ; le HTTPS (TCP 443), la version sécurisée du HTTP, utilisée par exemple pour les achats en ligne ; et le FTP (TCP 20 et TCP 21), pour télécharger des fichiers. Un logiciel de messagerie emploie les protocoles SMTP (port TCP 25) et POP3 (TCP 110) pour, respectivement, émettre et recevoir des courriers électroniques. Pourtant, vous ne définirez pas, pour chaque logiciel, une règle de filtrage par port utilisé, ce qui serait extrêmement fastidieux (d'autant plus que certains logiciels ont également besoin de ports réseau non standard pour fonctionner), mais vous fixerez, pour chacun, une règle autorisant l'ensemble des communications TCP et UDP en sortie. Cette autorisation globale ne réduit pas l'efficacité du pare-feu puisqu'elle s'applique à un logiciel spécifique et authentifié. Les spywares, par exemple, resteront bloqués.





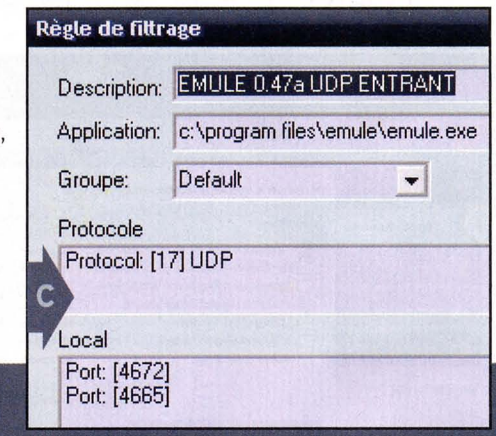


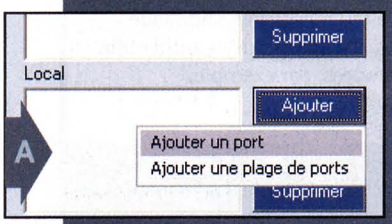
1. Dans le panneau de configuration de KPF, sélectionnez l'onglet **Sécurité du réseau.**
2. Cliquez sur le bouton **Filtrage.**
3. La liste des règles de filtrage apparaît dans une fenêtre. Cliquez sur le bouton **Ajouter.**
4. Une autre fenêtre apparaît. Dans la zone **Description,** tapez le nom du logiciel pour lequel vous définissez la règle de filtrage.
5. Cliquez sur le bouton **Parcourir** et sélectionnez le fichier exécutable du programme (**outlook.exe,** par exemple).
6. Cliquez sur le bouton **Ajouter** situé à droite de la zone **Protocole.** Une fenêtre apparaît. Sélectionnez **TCP** dans la liste déroulante et validez.
7. Réitérez l'étape 6 en sélectionnant cette fois **UDP.**
8. Cochez **Sortant** dans la zone **Direction.**
9. Cliquez sur **OK** pour fermer la fenêtre **Règle de filtrage.**
10. La liste des règles de filtrage réapparaît. Cliquez sur **Appliquer** pour rendre la nouvelle règle effective.

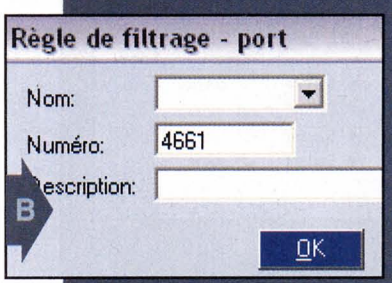
Paramétrer Kerio Personal Firewall

Pour un logiciel de partage de fichiers

Tous les logiciels d'échange de fichiers, notamment Emule, ont besoin de se connecter à un serveur central pour obtenir la liste des autres utilisateurs connectés. Emule peut accéder à deux réseaux simultanément (eD2K et Kad) mais il a besoin pour cela que les ports TCP 4661, TCP 4662, UDP 4672 et UDP 4665 soient ouverts en entrée au niveau du pare-feu (ces ports, définis par défaut, peuvent avoir été changés ; vérifiez les paramètres d'Emule). Pourtant, l'ouverture de ces ports ne suffit pas. Elle permet bien la communication avec les serveurs, mais les capacités de téléchargement sont alors réduites, la connexion étant qualifiée de « Low ID ». Pour résoudre le problème et obtenir un accès en « High ID », un seul moyen : autoriser toutes les connexions sortantes TCP et UDP pour Emule. Il faut donc finalement créer trois règles.







1 Pour ouvrir les ports TCP 4661 et 4662 en entrée, commencez par suivre la procédure décrite dans le Cas général (page précédente), de l'étape 1 à l'étape 6 incluse.

2 Cliquez ensuite sur le bouton Ajouter, à droite de la zone Local, et sélectionnez Ajouter un port dans le menu déroulant qui apparaît (voir écran A). Dans la fenêtre qui s'affiche, saisissez *4661* dans la zone Numéro, et cliquez sur OK (voir écran B). Réitérez cette deuxième étape en tapant cette fois la valeur *4662*. Enfin, cliquez sur Entrant dans la zone Direction, puis cliquez sur OK pour valider la règle.

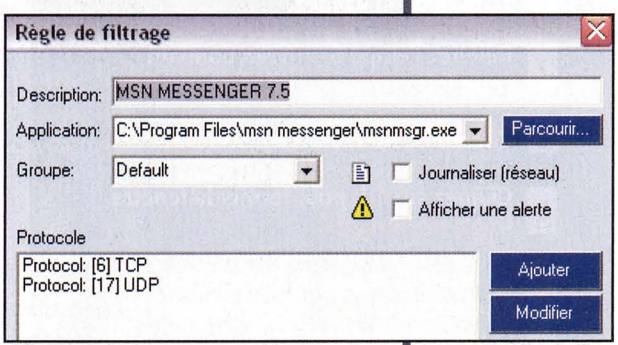
3 Pour ouvrir les ports UDP 4672 et 4665 en entrée, commencez par suivre la procédure décrite dans le Cas général, de l'étape 1 à l'étape 6 incluse, mais en sélectionnant UDP. Réitérez ensuite l'étape 2, ci-dessus, en saisissant cette fois les valeurs de ports *4672* et *4665* (voir écran C).

4 Pour ouvrir l'ensemble des ports TCP et UDP en sortie, reproduisez toutes les étapes du Cas général, en sélectionnant le fichier exécutable emule.exe à l'étape 5.

5 Cliquez sur Appliquer pour mettre en service les trois règles qui viennent d'être créées, puis sur OK pour fermer la fenêtre.

Pour une messagerie instantanée

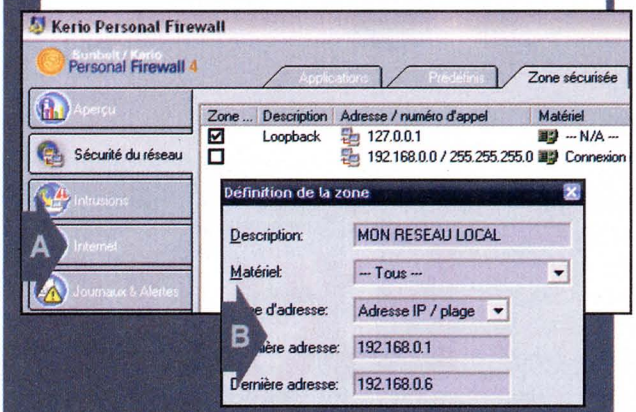
Mieux vaut définir une règle de filtrage lorsque l'on utilise une messagerie instantanée telle que MSN Messenger 7.5 ou sa nouvelle version, Windows Live Messenger. En effet, même si MSN Messenger est capable d'utiliser le port TCP 80 comme « issue de secours » lorsque l'un des ports qu'il utilise normalement est bloqué, il est préférable que tous soient ouverts pour garantir le fonctionnement optimal de certains services (transfert de fichiers, conférence audio, visiophonie). Ici aussi, plutôt que de définir une liste de ports TCP et UDP, vous autoriserez l'ensemble des connexions sortantes pour ces deux protocoles. Suivez le Cas général (page précédente), en sélectionnant **msnmsgr.exe** à l'étape 5 (voir écran).



Paramétrer Kerio Personal Firewall

Pour un accès réseau

Si vous souhaitez que les PC de votre réseau local puissent com muniquer avec celui sur lequel vous avez installé Kerio Personal Firewall, il convient de l'indiquer au pare-feu. Pour cela, plutôt que d'accorder des autorisations à chaque PC, un par un, il est préférable de spécifier une plage d'adresses IP, incluant toutes les adresses IP attribuées aux PC du réseau.



1 Dans le panneau de configuration de KPF, cliquez sur l'onglet Sécurité du réseau, à gauche, et sur l'onglet Zone sécurisée, en haut (voir écran A).

2 Pour ajouter une zone sécurisée, cliquez sur le bouton Ajouter. La fenêtre qui s'ouvre contient plusieurs lignes à remplir. Tapez le nom de votre réseau dans le champ Description (*Mon réseau local*, par exemple). Choisissez Tous dans le menu déroulant de la ligne Matériel. Sélectionnez Adresse IP/plage dans le menu déroulant de la ligne Type d'adresse. Saisissez, dans le champ Première adresse, la valeur de la première adresse IP attribuée sur le réseau local. Puis tapez, à la ligne suivante, la valeur de la dernière adresse (voir écran B). Cliquez ensuite sur OK.

Pour le multiposte TV de la Freebox

Attention à l'écran noir! Les abonnés aux services télé de la Freebox qui utilisent le logiciel adsl TV pour transformer leur PC en magnétoscope numérique doivent paramétrer KPF en conséquence. Pour fonctionner, adsl TV exige l'ouverture de six ports au niveau du pare-feu : les ports TCP 554, UDP 32769, UDP 32771 et UDP 15947 en sortie; et les ports UDP 32771 et UDP 32779 en entrée. Ce qui suppose trois règles de filtrage.

1 Pour ouvrir le port TCP 554 en sortie, suivez les étapes 1 à 6 du Cas général, en sélectionnant le fichier exécutable adsltv.exe à l'étape 5.

2 Cliquez sur le bouton Ajouter à droite de la zone Local. Cliquez sur Ajouter un port dans le menu déroulant qui apparaît. Saisissez la valeur *554* dans la zone Numéro, et cliquez sur OK. Cochez Sortant dans la zone Direction. Enfin, cliquez sur OK pour valider la première règle.

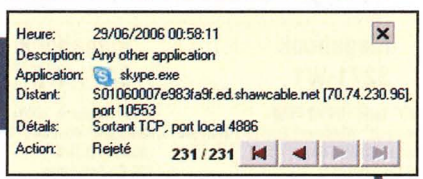
3 Pour ouvrir les ports UDP en sortie, reproduisez les étapes 3 à 6 du Cas général en sélectionnant UDP à la place de TCP. Réitérez alors l'étape 2, ci-dessus, pour chacun des ports *32769*, *32771* et *15947*. Cliquez sur OK pour valider la deuxième règle.

4 Pour ouvrir les ports UDP en entrée, reproduisez les étapes 3 à 6 du Cas général en sélectionnant UDP à la place de TCP. Réitérez alors l'étape 2, ci-dessus, pour les ports *32771* et *32779*. Cochez Entrant dans la zone Direction, et cliquez sur OK pour valider la troisième règle.

5 adsl TV exploitant lui-même l'outil VideoLAN (VLC), il faut maintenant renouveler les quatre étapes précédentes en choisissant le programme vlc.exe qui se trouve dans le même dossier qu'adsl TV.

6 Enfin, cliquez sur Appliquer, dans la liste des règles de filtrage, pour rendre vos nouvelles règles effectives.

Pour un logiciel de téléphonie



Impossible de téléphoner en voix sur IP (VoIP) sans d'abord paramétrer KPF. Pour Skype 2.5, le problème tient au fait que le logiciel fonctionne à la manière des logiciels de peer-to-peer. Il établit ainsi, lors de sa connexion au réseau, un ensemble de liaison TCP et UDP avec les autres utilisateurs de Skype connectés. Pas moins de 231 connexions sortantes vers des ports distincts sont ainsi immédiatement tentées (voir écran)! Dans ce contexte, mieux vaut ouvrir l'ensemble des ports TCP et UDP en sortie, comme indiqué dans le Cas général, en sélectionnant le bon fichier exécutable à l'étape 5 (**skype.exe** pour Skype, par exemple).