

Kerio Personal Firewall 2.1

Guide de l'utilisateur

Kerio Technologies Inc.

© 1997-2002 Kerio Technologies. Tout droits réservés.

Date de réalisation: le 22 avril 2002

Windows est une marque de Microsoft Corporation.

Traduction: J. Calicis (Jack@websecurite.net)

Table des matières

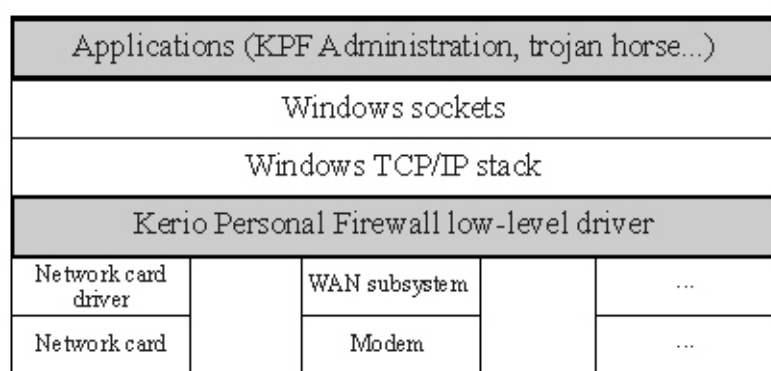
1	Introduction	5
1.1	Système requis	5
1.2	Installation	6
2	Administration	7
2.1	Composants du Personal Firewall	7
2.2	Sécuriser l'accès à l'Administration	8
2.3	Login d'Administration	9
2.4	Personal Firewall Status Window	9
3	Paramètres de sécurité	13
3.1	Introduction à TCP/IP	13
3.2	Comment fonctionne Kerio Personal Firewall?	14
3.3	IP Address Groups	15
3.4	Niveaux de Sécurité	15
3.5	Interaction avec l'utilisateur	16
3.6	Règles de filtrage des packets	18
3.7	Réseau Microsoft	23
3.8	Application MD5 Signatures	24
3.9	Internet Gateway Protection	26
4	Firewall Logging	27
4.1	Configuration du loggin	27
4.2	Filter.log file	28

Chapitre 1

Introduction

Kerio Personal Firewall est un utilitaire léger et facile destiné à protéger un PC contre les attaques de hackers et le vol de données. Il est basé sur la technologie certifiée ICSA utilisée pour le firewall WinRoute.

Le firewall lui-même tourne en fond de tâche, utilisant un driver à un niveau particulièrement bas chargé dans le system kernel. Ce Driver est placé au niveau le plus bas possible au-dessus des drivers hardware du réseau. De cette façon, il a un contrôle absolu sur tous les packets passant et est apte à garantir une protection complète du système sur lequel il est installé.



1.1 Système requis

La configuration suivante minimum est recommandée pour *Kerio Personal Firewall*:

- CPU Intel Pentium ou 100% compatible
- 32 MB RAM
- 3 MB d'espace disque (pour installation seulement); au moins 10 MB d'espace additionnel pour les loggings recommandé
- Windows 98 / Me / NT 4.0 / 2000 / XP

Kerio Personal Firewall est destiné à la protection des PC n'utilisant pas *WinRoute Pro* ou *WinRoute Lite*. Ces produits utilisent la même technologie de sécurité et pourraient entrer en conflit avec *Kerio Personal Firewall*.

1.2 Installation

Pour l'installation, il suffit simplement d'exécuter l'archive d'installation (typiquement `kerio-pf-211-en-win.exe`).

Pendant l'installation, vous pouvez choisir le répertoire d'installation de *Kerio Personal Firewall*, ou conserver les paramètres par défaut

(`C:\Program Files\Kerio\Personal Firewall`).

Il est nécessaire de redémarrer le système après l'installation pour permettre au pilote de bas niveau d'être chargé.

Chapitre 2

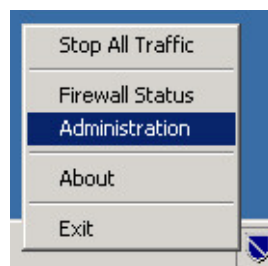
Administration

2.1 Composants du Personal Firewall

Kerio Personal Firewall consiste en trois programmes: *Personal Firewall Engine*, *Personal Firewall Administration* et *Personal Firewall Status Window*.



Personal Firewall Engine est le programme qui gère toutes les fonctions du *Personal Firewall*. Il tourne en fond de tâche (ou comme service pour WinNT/2K/XP) et sa présence est signalée par une icône dans le System Tray.



Un clic du droit sur l'icône fait apparaître un menu avec les options suivantes: stoppe tout trafic [*Stop All Traffic* — si sélectionné, il s'inverse en *Enable Traffic* (autoriser le trafic) et l'icône du System Tray change pour indiquer que le trafic est bloqué], exécuter l'application *Administration* ou voir la fenêtre de status (*Firewall Status*), information sur la version (*About*) ou stopper le moteur *Personal Firewall* (*Exit*). Stopper le moteur arrête bien sûr toute les fonctions de sécurité.

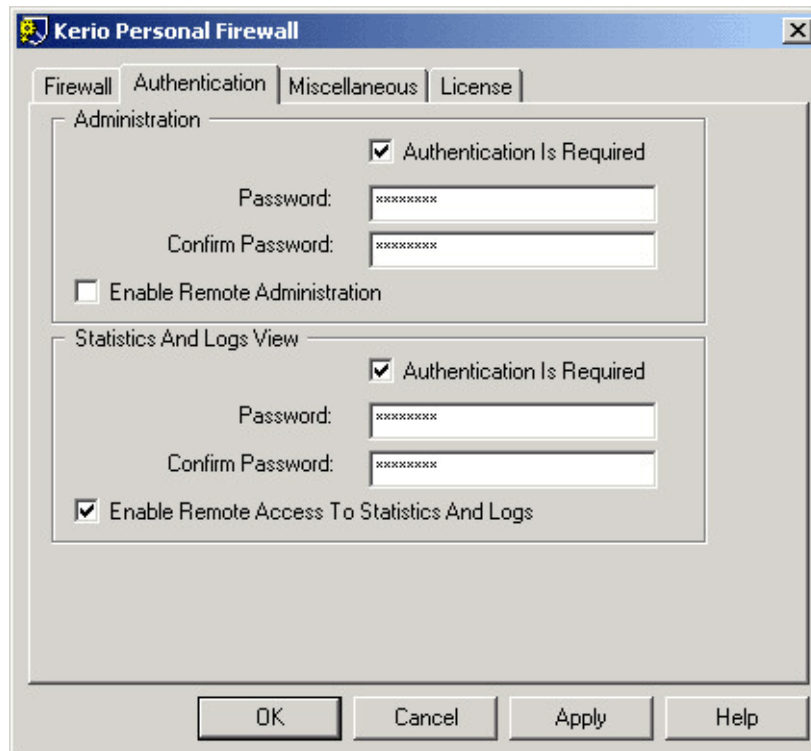
Le double clic du gauche sur l'icône ouvre le programme *Personal Firewall Status* dans une fenêtre.

Personal Firewall Administration est l'outil principal de configuration pour le moteur de *Personal Firewall*, nous reviendrons plus loin aux différentes options.

Personal Firewall Status Window présente les informations concernant toutes les applications en cours communiquant via le protocole TCP/IP, c'est également décrit dans un chapitre particulier.

2.2 Sécuriser l'accès à l'Administration

Pour assurer une sécurité maximum, il est vital que *Personal Firewall* tourne chaque fois que le PC est branché et que seules les personnes autorisées aient accès à sa configuration. Ceci peut être stipulé dans le programme d'administration de *Personal Firewall*, à l'onglet *Authentication*.

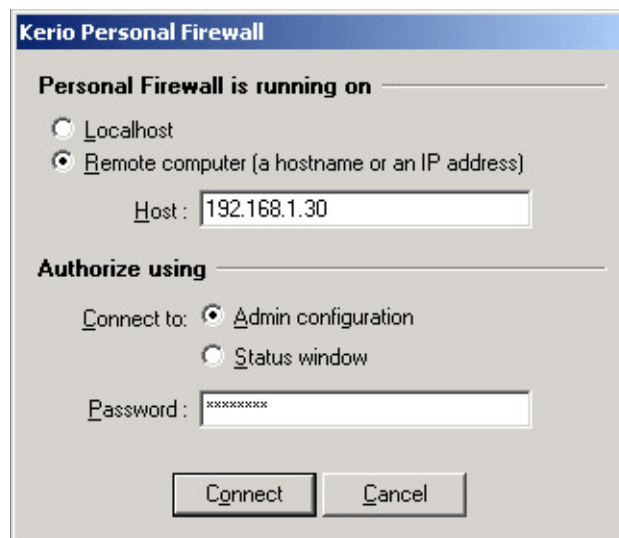


Section administration *Authentication Is Required* signifie qu'un mot-de-passe sera exigé pour exécuter le programme d'administration de *Personal Firewall*. Après avoir validé la fonction, les champs pour entrer le mot-de-passe et sa confirmation vous seront accessibles. Valider Remote Administration permet de gérer la configuration à distance.

Statistics and Logs View section Les paramètres pour l'accès et l'accès à distance aux logs et statistiques se règlent ici. Tous les champs sont les mêmes qu'à la section précédente. Configurer ces deux sections séparément permet deux niveaux de droits d'accès différents, soit voir les logs et statistiques uniquement, soit accès complet à l'administration.

2.3 Login d'Administration

Pour administrer *Kerio Personal Firewall* ou visualiser tous les logs, démarrez respectivement les applications *Personal Firewall Administration* ou *Personal Firewall Status Window*. Notez que le dialogue de connexion suivant apparaîtra uniquement si l'authentification est requise, autrement vous serez connecté directement au moteur local de *Kerio Personal Firewall*.



Vous pouvez choisir ici si vous voulez vous connecter au *Personal Firewall* tournant sur le PC local (*Localhost*) ou sur un ordinateur distant spécifié par son identité DNS ou son adresse IP. Vous pouvez choisir d'exécuter le programme d'administration du *Personal Firewall* (*Admin configuration*) ou celui de *Personal Firewall Status Window* (*Status Window*). Entrez votre mot-de-passe dans le champs correspondant.

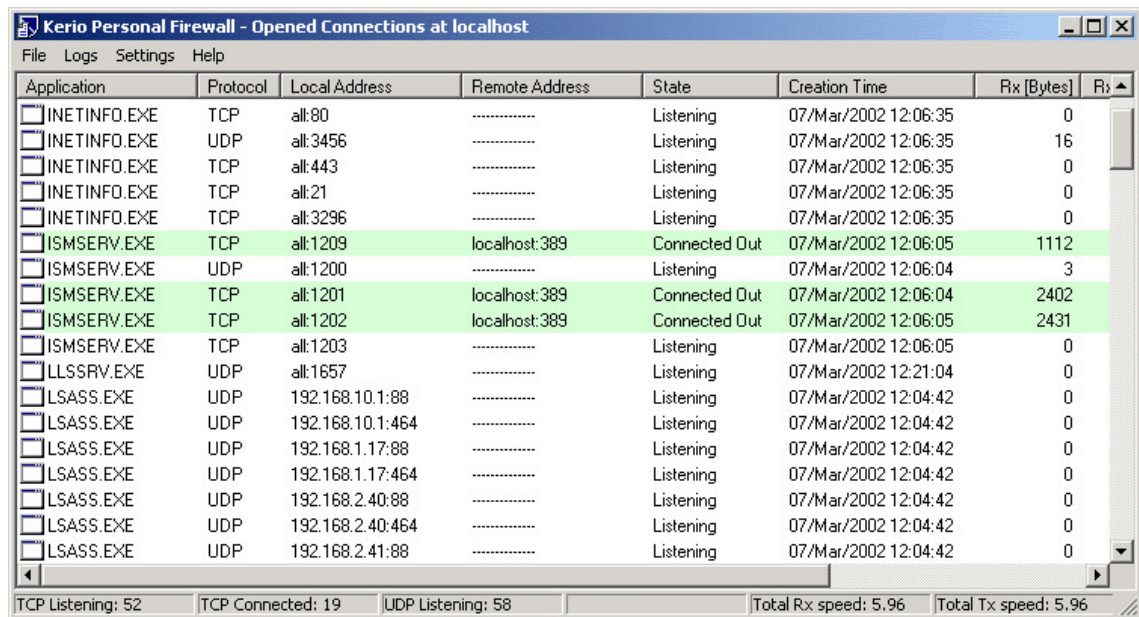
2.4 Personal Firewall Status Window

Personal Firewall Status Window permet de monitoriser toutes les activités TCP/IP du système et présente une information détaillée concernant les applications connectées.

Fenêtre principale

la fenêtre principale présente les informations concernant un point final local sur une ligne (le point final est défini par son adresse IP, le port et le protocole). Un point final local peut seulement correspondre à une seule application. Cependant, une application peut avoir plusieurs points finaux (par exemple, un serveur FTP écoute les connexions entrant sur les ports 20 et 21).

Chapitre 2 Administration



Application	Protocol	Local Address	Remote Address	State	Creation Time	Rx [Bytes]	Tx
<input type="checkbox"/> INETINFO.EXE	TCP	all:80	-----	Listening	07/Mar/2002 12:06:35	0	
<input type="checkbox"/> INETINFO.EXE	UDP	all:3456	-----	Listening	07/Mar/2002 12:06:35	16	
<input type="checkbox"/> INETINFO.EXE	TCP	all:443	-----	Listening	07/Mar/2002 12:06:35	0	
<input type="checkbox"/> INETINFO.EXE	TCP	all:21	-----	Listening	07/Mar/2002 12:06:35	0	
<input type="checkbox"/> INETINFO.EXE	TCP	all:3296	-----	Listening	07/Mar/2002 12:06:35	0	
<input type="checkbox"/> ISMSERV.EXE	TCP	all:1209	localhost:389	Connected Out	07/Mar/2002 12:06:05	1112	
<input type="checkbox"/> ISMSERV.EXE	UDP	all:1200	-----	Listening	07/Mar/2002 12:06:04	3	
<input type="checkbox"/> ISMSERV.EXE	TCP	all:1201	localhost:389	Connected Out	07/Mar/2002 12:06:04	2402	
<input type="checkbox"/> ISMSERV.EXE	TCP	all:1202	localhost:389	Connected Out	07/Mar/2002 12:06:05	2431	
<input type="checkbox"/> ISMSERV.EXE	TCP	all:1203	-----	Listening	07/Mar/2002 12:06:05	0	
<input type="checkbox"/> LLSSRV.EXE	UDP	all:1657	-----	Listening	07/Mar/2002 12:21:04	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.10.1:88	-----	Listening	07/Mar/2002 12:04:42	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.10.1:464	-----	Listening	07/Mar/2002 12:04:42	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.1.17:88	-----	Listening	07/Mar/2002 12:04:42	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.1.17:464	-----	Listening	07/Mar/2002 12:04:42	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.2.40:88	-----	Listening	07/Mar/2002 12:04:42	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.2.40:464	-----	Listening	07/Mar/2002 12:04:42	0	
<input type="checkbox"/> LSASS.EXE	UDP	192.168.2.41:88	-----	Listening	07/Mar/2002 12:04:42	0	

TCP Listening: 52 TCP Connected: 19 UDP Listening: 58 Total Rx speed: 5.96 Total Tx speed: 5.96

Les colonnes séparées présentent les informations sur les points finaux:

Application Le nom de l'exécutable de l'application auquel le point final appartient. Le nom peut être indiqué en précisant le chemin complet en sélectionnant *Settings / Don't Cut Pathnames*.

Protocol Le protocole de communication (soit TCP — protocole connecté ou UDP — protocole datagram non-connecté)

Local Address Une adresse IP locale et le port (présenté dans le format suivant — `address:port`). Dans le menu *Settings* vous pouvez choisir d'indiquer le nom DNS plutôt que l'adresse IP et service (standard).

Remote Address L'adresse IP et le port ne sont pas indiqués si la connexion n'est pas établie.

State L'état d'un point local final: end-node: **Listening** (à l'écoute) — waiting for incoming connection (en attente de connexion entrante), **Connected In** — connection established from a remote client to a local service (connexion établie depuis un client distant à un service local), **Connected Out** — connection established by a local application to a remote server (connexion établie par une application locale à un serveur distant).

Creation Time L'heure de l'établissement de la connexion ou quand l'application concernée a commencé à recevoir sur un port déterminé.

Rx [bytes] La quantité de data reçues par un point final (en bytes)

Rx speed [bytes/sec] La vitesse moyenne de transfert de données (en kilobytes par seconde)

Tx, Tx speed Idem pour les données sortantes.

Menu principal

File *Connect...* connecte au moteur de *Personal Firewall* (sur un système local ou distant). Utiliser *Close* pour fermer l'application *Personal Firewall Status Window*.

Logs Affiche la fenêtre log du *Firewall* ou les statistiques de transferts et les données filtrées.

Settings Contient les paramètres des informations à afficher et comment:

- *Hide Listening Sockets* (cacher les sockets à l'écoute) — hides end-nodes that have no established connection [cacher les points finaux sans connexion établie (leur statut est à l'écoute)]
- *Hide Local Connections* (cacher les connexions locales) — hides connections established within a local system (loopback) [cacher les connexions établies à l'intérieur du système local (loopback)]
- *Hide Admin-Firewall Connection* — cacher les connexions établies entre les différents composants du *Personal Firewall*
- *Don't Resolve Domain Names* — les adresses IP ne seront pas traduites par leur noms DNS
- *Don't Show Port Names* — les N° de ports ne seront pas remplacés par les noms des services (pe telnet, SMTP, HTTP)
- *Displayed Application Name* — change le mode d'affichage du nom de l'application: *Whole Pathname* (nom entier), *Cut Pathname* (seul le nom du fichier sera indiqué) or *File Information* (indique le nom de l'application si possible, autrement un nom de fichier abrégé sera affiché)
- *Update frequency* — change le taux de rafraîchissement de la fréquence d'information (*Slowest* — 5 secondes, *Slower* — 2 secondes, *Normal* — 1 seconde, *Fast* — 0.5 seconde)

Help Aide et informations à propos du fabricant du programme et la version.

Paramètres de sécurité

3.1 Introduction à TCP/IP

Pour pouvoir configurer et profiter au mieux des fonctions de *Kerio Personal Firewall*, il est nécessaire de comprendre le principe des communications TCP/IP. Les utilisateurs avancés peuvent sauter ce chapitre qui est cependant fortement recommandé aux débutants.

TCP/IP TCP/IP est l'appellation commune pour les protocoles de communication utilisés sur Internet. Les données sont divisées en petites parties appelées *packets* à l'intérieur de chaque protocole. Chaque *packet* contient un en-tête et une partie de données. Le header (en-tête) contient l'information (pe. source et adresse de destination), tandis que la partie data (données) transporte l'information transmise entre les applications.

Le protocole est ensuite subdivisé en plusieurs niveaux. Les *packets* de *lower-level protocols* (protocoles de bas-niveaux) contiennent des *packets* de niveaux supérieurs dans leur partie data (pe. les TCP protocol packets sont transférés à l'intérieur des IP packets).

IP IP (Internet Protocol) transporte dans sa partie tous les autres protocol packets. La partie la plus importante d'information contenue dans le header est la source et l'adresse IP de destination, c'est l'adresse du computer qui a envoyé le packet et à quel computer il est adressé.

ICMP ICMP (Internet Control Message Protocol) transfère les messages de contrôle. Il y en a plusieurs types, pe information concernant la disponibilité d'un ordinateur distant, routing request (requête de routage) ou reply request [réponse à une requête (utilisé dans une commande PING)].

TCP TCP (Transmission Control Protocol) est utilisé pour des transferts de données fiables via «un canal virtuel» (connexion). Il est utilisé comme protocole porteur pour la plupart des protocoles d'applications, pe SMTP, POP3, HTTP, FTP, Telnet, etc.

UDP UDP (User Datagram Protocol) est un non-connected protocol (protocole non connecté), cela signifie qu'il ne crée pas un channel — toutes les data sont transférées via messages individuels (appelés datagrams). UDP n'assure pas la livraison

sure et fiable de données car les datagrams peuvent être perdus pendant le transfert. Comparé au TCP protocol, UDP demande beaucoup moins de ressources (il n'y a pas d'établissement ni de fin de connexions, acceptation de data, etc.). UDP protocol est utilisé pour les requêtes de DNS, transferts de données son ou video, etc.

Ports La partie la plus importante d'information dans l'en-tête du TCP et UDP packet est le port source et destination. Alors qu'une adresse IP localise un PC sur Internet, un port définit une application tournant sur ce computer. Les ports 1—1023 sont réservés aux services standards, les ports 1024-65535 peuvent être utilisés par n'importe quelle application. Lors d'une communication typique client-serveur le port de destination est connu (une connexion est établie avec ce port ou un UDP packet lui est envoyé) le port source port est habituellement assigné automatiquement par le système.

Protocoles d'application les protocoles transportés dans les TCP/UDP packets sont utilisés pour les transferts de données utilisateur (application). Il y a de nombreux protocoles standards d'application (pe SMTP, POP3, HTTP, FTP, etc.). Cependant, un programmeur peut utiliser ses propres (non-standard) moyens de communications.

3.2 Comment fonctionne Kerio Personal Firewall?

Toutes les communications Internet sont transportées à l'aide des protocoles TCP/IP. Ces protocoles sont habituellement aussi utilisés pour la communication à l'intérieur des réseaux locaux. Le protocole (porteur) principal est l'IP (Internet Protocol), ses packets transportent toutes les autres informations (ils renferment les autres protocoles). Un véritable firewall doit avoir un contrôle complet sur tous les IP packets — il doit être capable de les capturer, de trouver toutes les informations nécessaires à l'intérieur pour les laisser passer ou les filter. Et, bien sûr, il doit pouvoir garder un enregistrement des actions accomplies, attaques détectées, etc.

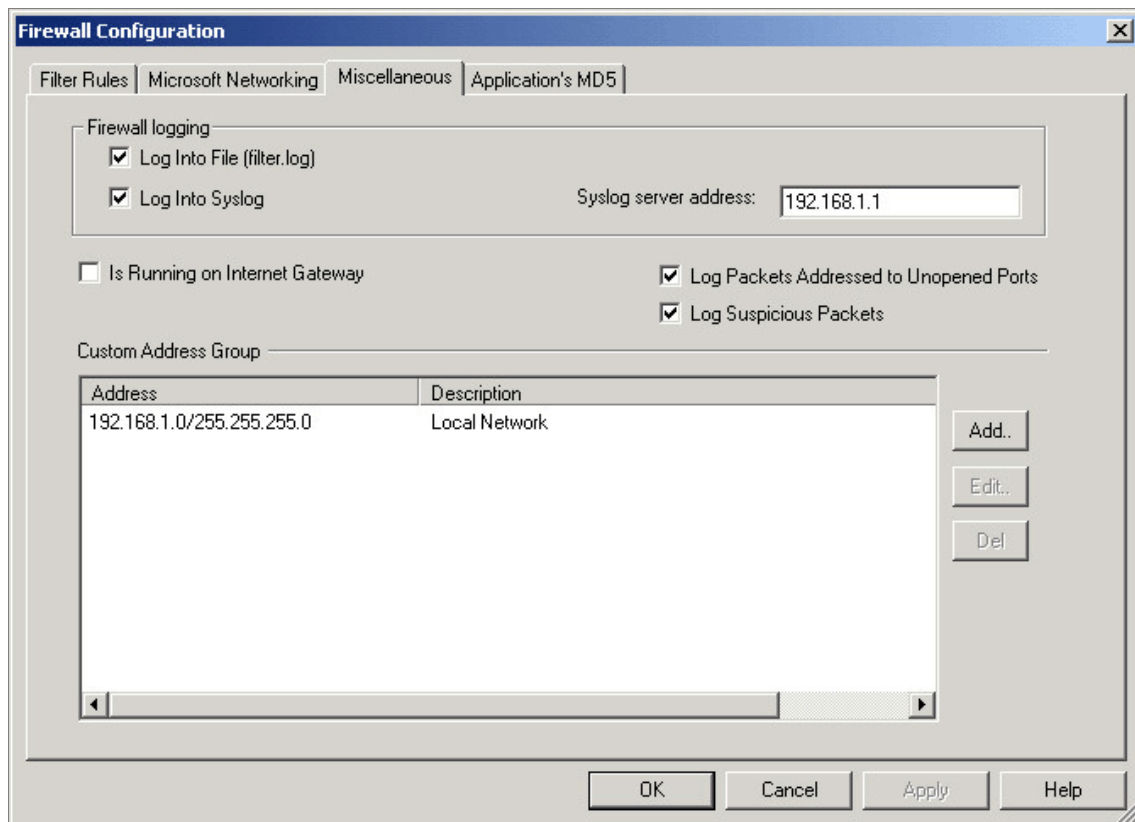
La méthode principale d'un firewall tel que KPF est la «stateful inspection». Cela signifie qu'une analyse est effectuée sur chaque packet passant par votre computer et que seul un packet correspondant à cette analyse est autorisé à le traverser. Tous les autres packets sont ignorés. Cela assure que *Personal Firewall* autorise seulement les communications initiées depuis le réseau local.

L'utilisateur/administrateur peut spécifier des conditions de filtrage de packets avec des règles de filtrage. Seuls les packets correspondant aux critères établis sont acceptés.

3.3 IP Address Groups

Quand on définit certaines règles de filtrage autorisant ou refusant certaines communications, il se peut que la même règle soit applicable à un groupe d'adresses IP (peu plusieurs postes dans un réseau local).

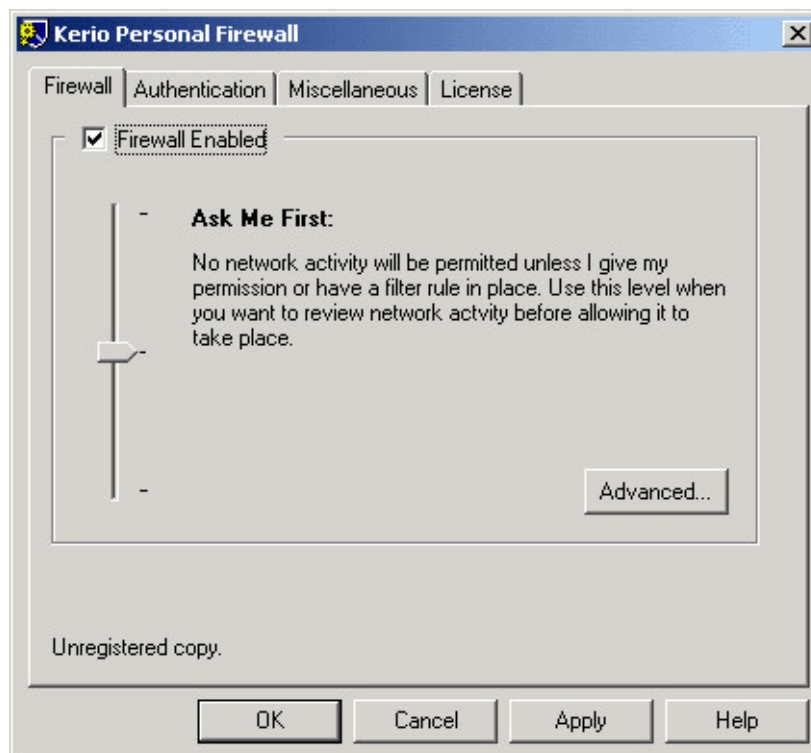
Kerio Personal Firewall permet à l'utilisateur de définir un groupe d'adresses IP qui peut facilement être utilisé par la définition de règles de filtrage. Un groupe peut contenir n'importe quel nombre d'adresses IP ou de plages d'adresse IP ou de sous-réseaux.



Le custom address group (groupe d'adresses défini) peut être entré dans la fenêtre *Firewall Configuration*, onglet *Miscellaneous*. En pressant, vous pouvez ajouter une seule adresse IP, une plage d'adresses (*Network / Range*) ou un sous-réseau (*Network / Mask*). Les boutons *Edit...* et *Del* permettent respectivement d'éditer ou de supprimer des entrées individuellement.

3.4 Niveaux de Sécurité

Kerio Personal Firewall permet 3 niveaux de sécurité de base:



Permit Unknown (Don't Bother Me) Sécurité minimum [Autoriser l'inconnu (ne pas me déranger)]: *Personal Firewall* autorise toute communication, sauf explicitement refusée par les règles de filtrages. *Personal Firewall* est totalement transparent s'il n'y a pas de règles de filtrage établies (il se comporte comme s'il n'était pas en fonction du tout).

Ask Me First (Me demander d'abord) Toute communication est refusée implicitement à ce niveau. Si une application tente de communiquer ou si quelqu'un essaie d'établir une connexion de l'extérieur, *Personal Firewall* intercepte la requête et affiche une fenêtre de dialogue demandant si vous acceptez ou refusez la communication. Ceci peut être autorisé une fois seulement ou de façon permanente (recommandé).

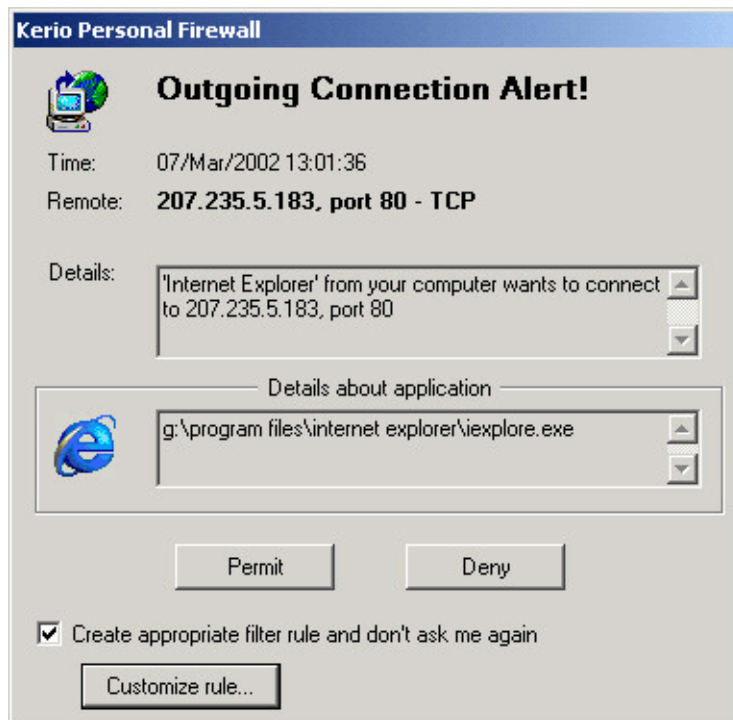
Deny Unknown (Cut Me Off) [Refuser l'inconnu (Isolez moi)] Toute communication qui n'est pas explicitement autorisée par les règles de filtrage établies est rejetée. *Personal Firewall* ne demande rien à l'utilisateur.

3.5 Interaction avec l'utilisateur

Si le niveau de sécurité *Ask Me First* est sélectionné, *Personal Firewall* permet seulement automatiquement les communications autorisées par les règles de filtrage. Si un packet capturé ne correspond à aucune règle, il est présumé que l'utilisateur utilise une nouvelle

application et une fenêtre de dialogue est présentée où l'utilisateur peut accepter ou refuser une telle communication. La permission ou l'interdiction peut être temporaire ou permanente (en créant une règle appropriée).

La fenêtre de dialogue offre les informations suivantes:



Incoming / Outgoing Connection Alert! Indique si la requête de connexion est sortante (depuis le réseau local) ou entrante (pe depuis Internet)

Time L'heure et la date précises de la requête

Remote Information sur le point final distant (adresse IP, port et protocole de communication)

Details informations détaillées à propos de la connexion

Details about application Informations au sujet de l'application locale concernée (comme client ou comme serveur)

Permit Autorise la communication

Deny Stoppe (filtre) la communication

Create appropriate filter rule... Si cette option est sélectionnée, presser *Permit* ou *Deny* crée automatiquement une règle de filtrage, les prochains packets de même type

se verront ensuite autoriser ou refuser l'accès. Ceci peut être utilisé lors de la configuration initiale de *Personal Firewall* — l'utilisateur n'a pas besoin de définir de règles, mais lorsqu'il utilisera ses applications favorites, des règles pourront être créées pour elles de cette façon.

Customize rules Ici, un utilisateur avancé peut éditer et peaufiner la règle créée automatiquement.

Une règle créée ainsi est toujours validée pour une application déterminée qui envoie ou reçoit un packet (voir les *Details* au sujet d'application field). Une signature MD5 est aussi créée automatiquement de sorte que lors des exécutions suivantes de l'application du même nom soit comparée avec la signature initiale, ceci pour prévenir un trojan de remplacer son nom par celui de l'application de confiance, telle que outlook.exe. Des détails sur les signatures MD5 peuvent être trouvés au chapitre 3.8.

Par défaut une règle de filtrage pour une application est créée de façon à ce qu'elle puisse communiquer à n'importe quel port local avec n'importe quel computer sur Internet (n'importe quelle adresse distante) et aussi avec n'importe quel port distant. Il est supposé que si l'utilisateur autorise la communication pour cette application une fois, celle-ci est sûre et ne sera plus limitée dans le futur. Cependant, ce n'est pas toujours vrai, c'est pourquoi l'utilisateur peut ajuster la règle à ses besoins. Les règles créées automatiquement peuvent toujours être ajustées ou supprimées plus tard des règles de filtrage dans l'option advanced.

Ajuster une règle créée automatiquement

Le paramétrage concret d'une règle dépend d'une situation précise, particulièrement quant à l'application concernée par l'autorisation ou le refus. Voici quelques principes généraux:

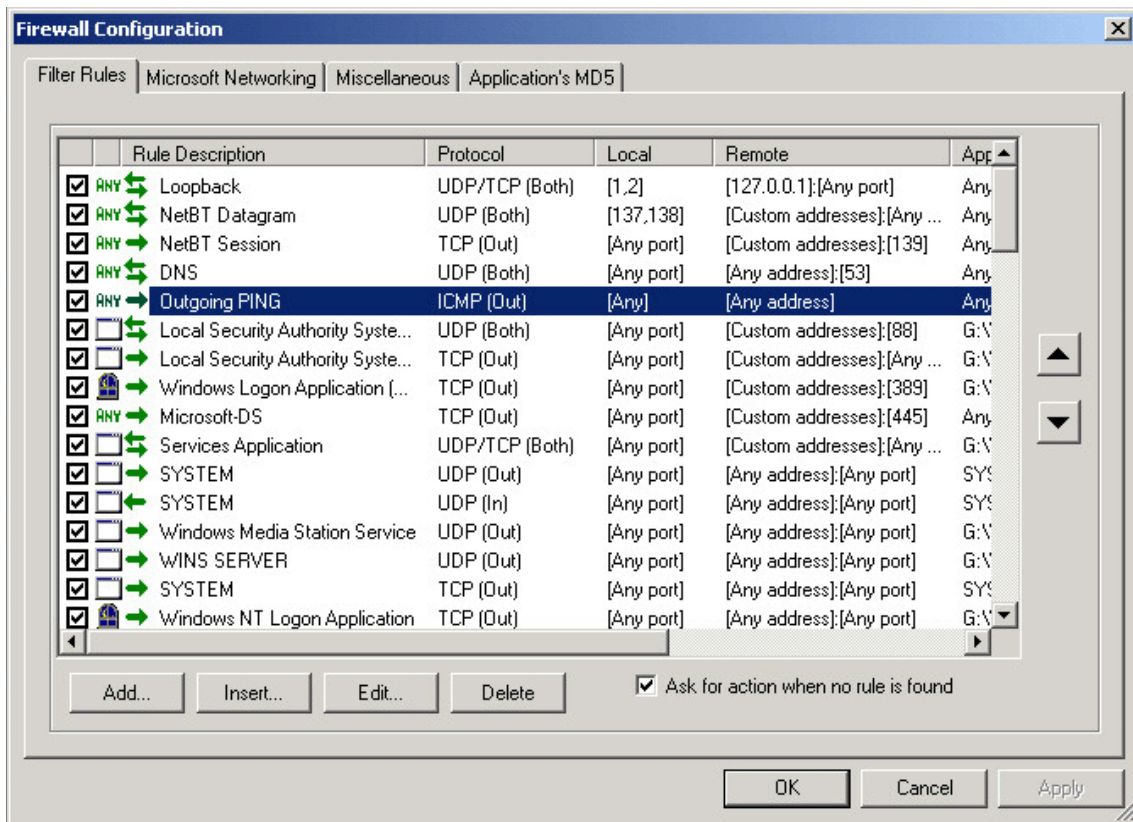
- Seuls des utilisateurs expérimentés, familiarisés avec les communications TCP/IP devraient modifier les paramètres des règles.
- Déterminer le port local pour une application n'est pas recommandé, en effet le port local est assigné par le système et n'est pas connu à l'avance dans la plupart des cas.
- Applicable également aux ports distants, si nous avons affaire à une application de type serveur (pe un serveur WWW).

3.6 Règles de filtrage des packets

Les règles de filtrage définissent quels packets seront autorisés ou refusés à communiquer. Sans ces règles, *Kerio Personal Firewall* fonctionnerait seulement en 2 modes: toute communication autorisée ou toute communication refusée.

Il y a deux façons de créer les règles: soit automatiquement lors de la détection d'un packet inconnu (l'utilisateur doit soit accepter soit refuser un tel packett — voir le chapitre 3.5) ou manuellement dans le programme *Personal Firewall Administration*. Ici l'utilisateur peut non seulement créer des règles mais aussi les éditer, les supprimer ou les ordonner dans l'ordre de leur priorité.

Les règles de filtrage définies sont affichées dans l'onglet *Filter Rules* (après avoir pressé le bouton *Advanced* dans la fenêtre principale *Personal Firewall Administration*, onglet *Firewall*).



Liste des règles de filtrage

Les règles sont présentées dans un tableau, chaque ligne représentant une règle. Les colonnes ont la signification suivante:

- Checkbox — indique si la règle est active ou non. L'utilisateur peut l'activer ou la désactiver d'un simple clic, inutile de la supprimer ou de l'ajouter.
- Application icon — montre l'icône de l'application locale à laquelle la règle est applicable. Si la règle est validée pour toutes les applications, une icône spéciale verte

"Any" est affichée à la place. Seulement dans de rares cas une telle règle devrait exister.

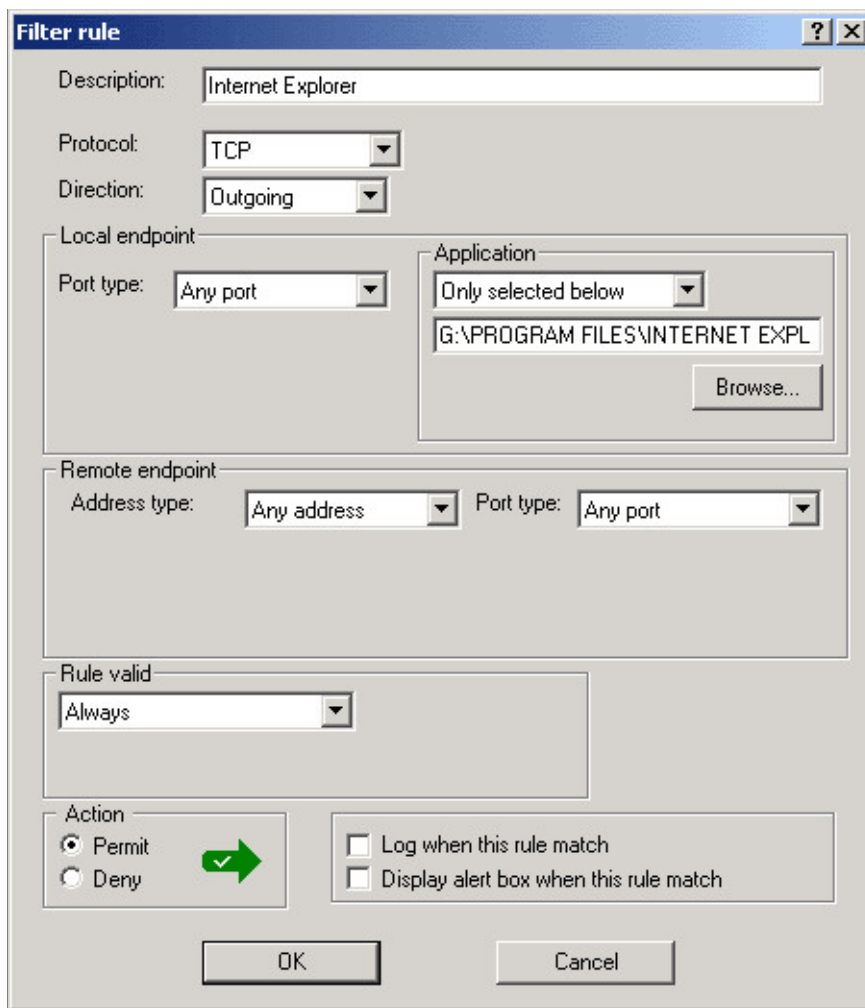
- *Rule Description* — la direction et la description d'une règle. Les symboles suivants sont utilisés pour la direction: flèche droite (packet sortant), flèche gauche (packet entrant), flèche double (bi-direction — la règle s'applique aux packets In et Out). La description de la règle peut contenir ce que l'utilisateur désire. Pour les règles créées automatiquement, le nom de l'application est utilisé pour sa description.
- *Protocol* — protocoles de communication utilisés (TCP, UDP, ICMP...). La direction de la communication [In, Out ou Both (les deux)] est aussi indiquée entre parenthèses après le nom du protocole.
- *Local* — port local
- *Remote* — adresse IP distante et port (séparé par un double-point)
- *Application* — l'exécutable de l'application locale incluant le chemin complet. Si l'application est un service du système, le nom indiqué sera SYSTEM.

Controls

- *Add* — ajoute une nouvelle règle à la fin de la liste
- *Insert* — insère une nouvelle règle au-dessus de la règle sélectionnée. Cette fonction évite à l'utilisateur le déplacement de la règle dans la liste comme elle permet l'insertion d'une nouvelle règle à l'endroit désiré
- *Edit* — edite la règle sélectionnée
- *Delete* — supprime la règle sélectionnée
- Les boutons flèches (à droite de la liste des règles) — autorise le déplacement de la règle sélectionnée dans la liste. Notez que les filtres sont validés de haut en bas, la position d'une règle est donc très importante.

Ajouter ou éditer une règle

Après avoir pressé le bouton *Add*, *Insert* ou *Edit*, une boîte de dialogue est affichée pour définir une règle.



Options générales

- *Description* — une règle peut être définie par n'importe quel texte. Nous recommandons de décrire les règles sur base de leur fonction (pe. DNS resolution, requête de ping entrant...). Cette option est seulement nécessaire pour les utilisateurs avancés.
- *Protocol* — Le protocole de communication auquel la règle est applicable. TCP, UDP, TCP et UDP, ICMP ou autre (choisir *Other* ensuite définir le protocole par le nombre dans le header du packet IP). Une option spéciale Any signifie tous les protocoles, pe tous les IP packets.
- Si *ICMP* protocol est choisi, un nouveau bouton *Set ICMP...* apparaît. Après l'avoir pressé, l'utilisateur peut choisir le type de messages ICMP auquel la règle

s'appliquera. Les types d'ICMP choisis sont indiqués dans un champs de texte spécial.

- *Direction* — une direction dans laquelle les packets seront filtrés (*Outgoing*, *Incoming* ou *Both*)

Local endpoint section

- *Port type* — le port (seulement si TCP et/ou UDP sont sélectionnés). Les options possibles sont: *Any* (n'importe quel port), *Single Port* (un seul port), *Port Range* or *List of ports* (une liste de N de ports, séparés par des virgules)
- *Application* — indique si la règle s'applique à tous les packets (any application) ou au incoming/outgoing packets d'une application particulière (Only selected below). L'exécutable de l'application doit être entré incluant son chemin complet. Ceci peut être fait manuellement ou à l'aide du bouton Browse.

Remote endpoint section

- *Address type* — Adresse IP de l'ordinateur distant. Ceci peut être spécifié comme *Any address*, *Single address* (l'adresse d'un PC précis), *Network/Mask*, *Network/Range* ou un groupe d'adresses IP défini par l'utilisateur (*Custom Address Group*).
- *Port type* — port distant. Les options sont les mêmes que définies dans local port.

Other parameters

- *Rule valid* — indique si la règles es toujours valide ou seulement à certains moments (In this time interval only). Dans le second cas, l'utilisateur peut déterminer la période en pressant le bouton *Set...*

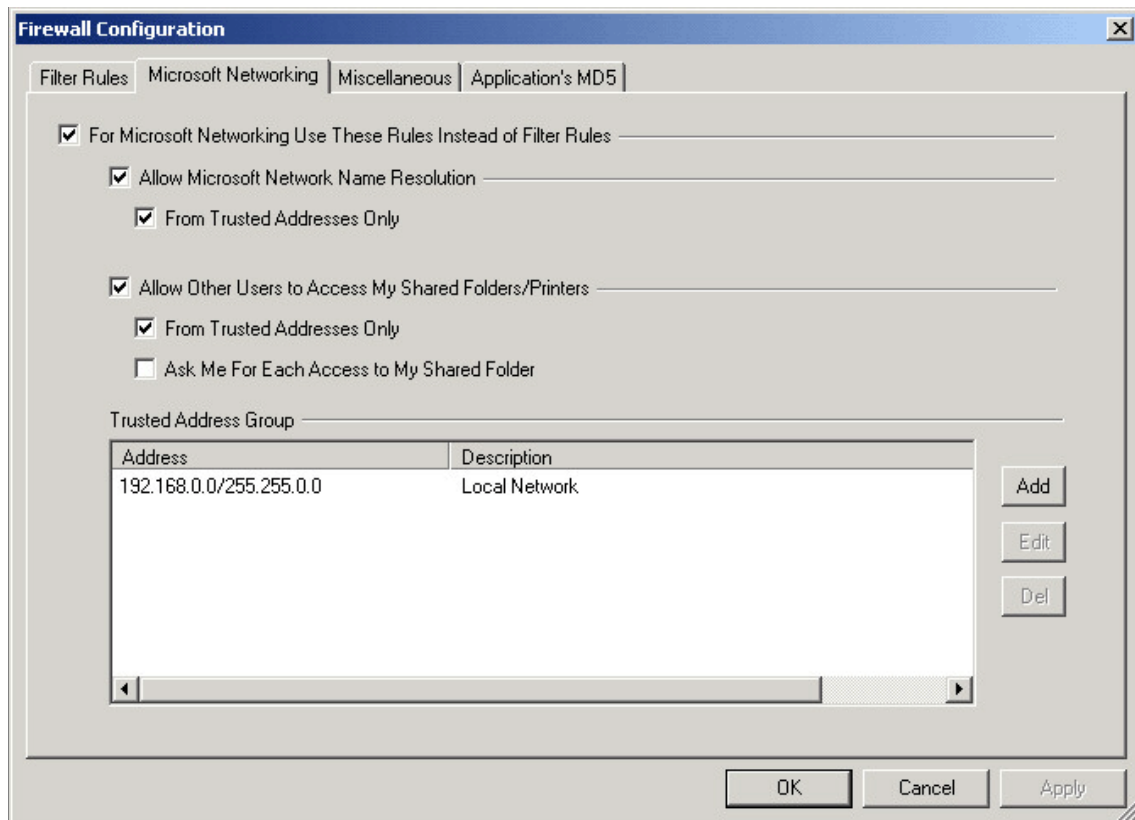
L'usage de time intervals requiert un paramétrage correct du systeme temps!

- *Action* — l'action à effectuer — si un packet doit être accepté ou refusé
- *Log when this rule matches* — un packet sera logé s'il correspond à la règle (voir logging options dans la fenêtre *Firewall Configuration*, onglet *Miscellaneous*)
- *Display alert box when this rule matches* — si un packet correspond à cette règle, une fenêtre d'information (*Firewall Rule Alert*) sera affichée contenant une description détaillée du packet et s'il a été accepté ou refusé.

3.7 Réseau Microsoft

Il est courant qu'un PC sous Microsoft Windows soit connecté à un réseau local utilisant le partage de dossiers et d'imprimante pour les réseaux Microsofts. Plusieurs services sont utilisés pour la communication sous cet environnement et la mise en place d'un personal firewall pour des performances optimum et sécurisées dans de telles conditions n'est pas toujours aisée.

Kerio Personal Firewall permet des règles séparées pour un environnement Microsoft Network. Ces paramètres sont disponibles dans *Advanced* section à l'onglet Microsoft Networking.



For Microsoft Networking Use These Rules... Cette option signifie que les règles spéciales définies dans cette boîte de dialogue seront utilisées.

Allow Microsoft Network Name Resolution Valider cette option permettra l'échange des noms de computers du réseau Windows.

From Trusted Addresses Only Le protocole utilisé pour Windows name resolution sera uniquement applicable au groupe d'adresses définies. Ce groupe est généré auto-

matiquement par la collecte d'information TCP/IP depuis le système local et peut être modifié si nécessaire.

Allow Other Users to Access My Shared... Permet l'accès aux répertoires et imprimantes partagés.

From Trusted Addresses Only L'accès est uniquement autorisé aux adresses de confiance définies.

Ask Me For Each Access... A chaque tentative de connexion à un répertoire partagé, *Personal Firewall* demandera si la connexion est accordée ou refusée.

Trusted Address Group Un groupe d'adresses défini comme de confiance. En utilisant les boutons Add, Edit et Del l'utilisateur peut ajouter, changer ou supprimer une adresse IP, une range d'adresse IP, ou un sous-réseau complet. La validité pour ce groupe d'adresses IP est limitée à l'onglet Microsoft Networking. Le groupe ne peut être utilisé pour définir d'autres règles.

Exemples de paramétrage optimum

- Si vous avez un seul PC, non connecté à un réseau local (pe un notebook connecté à Internet via modem), simplement valider cette option *For Microsoft Networking Use These Rules Instead Of Filter Rules*. Laisser toutes les autres options sur *Off*. Cela invalidera toutes les communications pour les réseaux Microsoft qui ne s'appliquent pas à ce cas de figure.
- Si votre PC est connecté à un LAN où vous faites confiance à vos collègues et désirez leur laisser l'accès à vos répertoires et imprimantes partagés, validez toutes les options sauf *Ask Me For Each Access to My Shared Folders*. Dans le champs *Trusted Address Group* définissez votre reseau local (pe comme un sub-network avec un mask correspondant ou avec une range d'adresses IP).
- Si vous désirez accorder l'accès à votre matériel partagé tout en ayant un contrôle complet sur qui peut y accéder, procédez comme dans l'exemple précédent mais validez aussi l'option *Ask Me For Each Access to My Shared Folders*.

3.8 Application MD5 Signatures

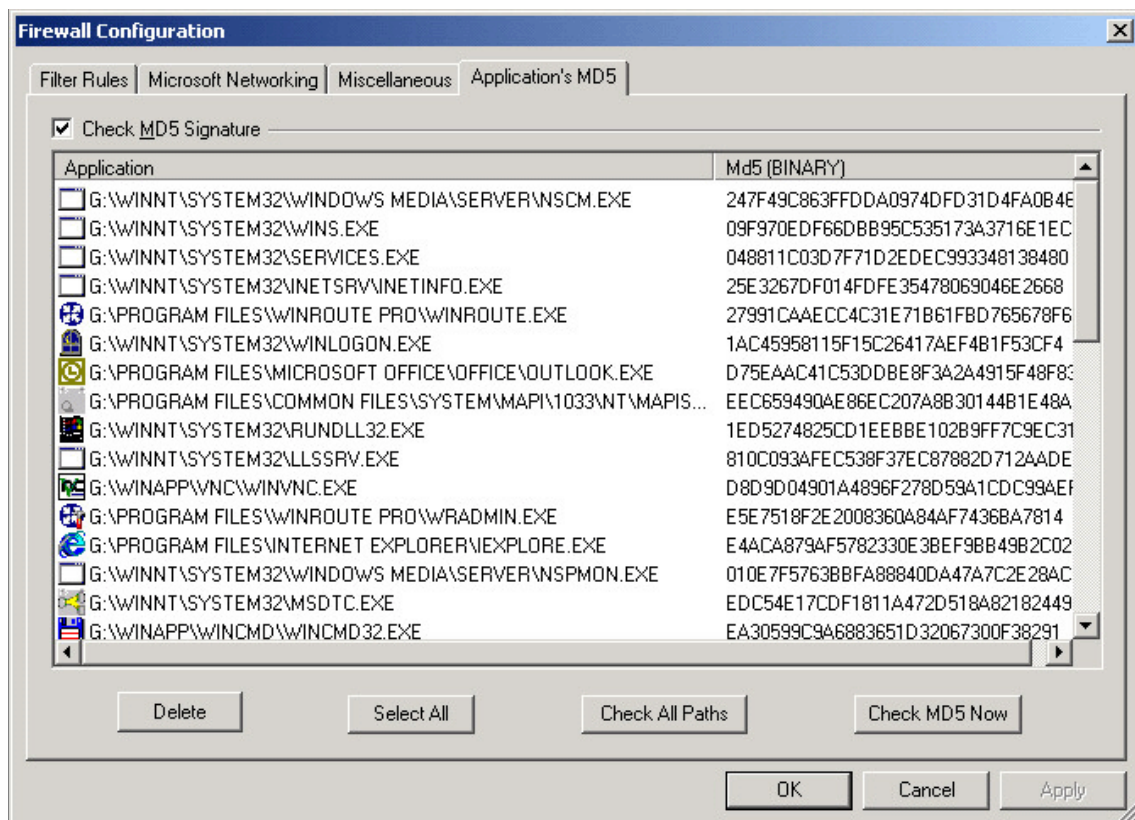
En plus du contrôle des packets entrants ou sortants *Kerio Personal Firewall* peut aussi détecter si les packets autorisés sont envoyés par les applications autorisées. Une application pourrait s'infiltrer dans votre computer (pe par email, depuis une disquette, etc.),

3.8 Application MD5 Signatures

agissant comme un programme connu et correct (il remplace généralement l'exécutable original) et tente d'envoyer des données depuis votre computer. Une telle application est généralement référencée comme «cheval de Troie». Habituellement, elle peut être découverte lors d'un checking anti-virus/anti-trojans mais il pourrait être déjà trop tard.

Kerio Personal Firewall utilise un procédé de création et de surveillance de signatures MD5 des applications. En termes simples, une signature MD est un checksum de l'exécutable d'une application. La première fois qu'une application est lancée (ou lorsque l'application essaie pour la première fois de communiquer via le réseau) *Personal Firewall* crée une signature MD5 pour cette application. Cette signature est contrôlée à chaque tentative de communication suivante de la-dite application avec le réseau. Si l'exécutable de l'application a été modifié (pe s'il est infecté par un virus ou a été remplacé par un autre programme) *Personal Firewall* refuse la communication à cette application, présente un avertissement et demande si le changement doit être accepté ou non (pe en cas d'upgrade de l'application).

Les signatures MD5 peuvent être vues et supprimées dans le tableau *Application's MD5*. Elles peuvent seulement être créées automatiquement.



Les options suivantes sont disponibles dans le tableau *Application's MD5*:

Check MD5 signature Cette option valide/invalidé la création et le checking des signatures MD5 des applications.

Delete Supprime la signature MD5 de la/des application(s) sélectionnée(s).

Select All Sélectionne toutes les applications de la liste.

Check All Paths Contrôle toutes les applications quant à l'existence d'exécutables. Si l'exécutable n'existe pas (pe après une désinstallation) il vous est demandé si la signature MD5 pour l'application doit être supprimée.

Check MD5 Now Contrôle la validité des signatures MD5. En cas de non-validité, *Personal Firewall* demande si un changement doit être accepté ou non.

Note: Plusieurs applications peuvent être sélectionnées en utilisant les touches *Ctrl* or *Shift* key.

3.9 Internet Gateway Protection

Kerio Personal Firewall peut aussi être utilisé pour protéger un Internet gateway, pe. un computer fournissant l'accès Internet à des computers dans un réseau local (un router ou un NAT router). Typiquement, cela peut être fait en combinaison avec l'application Microsoft's *Internet Connection Sharing* (ICS), un composant des systèmes Windows 98 SE, Me, 2000 et XP. ICS valide l'accès à Internet pour tous les computers via une seule adresse IP. Cependant, il ne fournit aucune protection contre les attaques extérieures. Associé à *Kerio Personal Firewall* vous pouvez bénéficier d'une connexion internet partagée sécurisée.

Personal Firewall est conçu pour la protection d'un seul computer. Cependant, un grand nombre de packets traverse l' internet gateway (router) qui ne sont pas destinés à ce computer. De façon à ne pas être contraint à établir des filtres complexes de packets, *Personal Firewall* peut être basculé en mode particulier destiné aux Internet gateways. Ceci peut se faire dans la fenêtre *Firewall Configuration* (après avoir pressé le bouton

Advanced sur le tableau *Miscellaneous* en validant l'option *Is running on Internet gateway*.

Note: Ne validez pas cette option si *Personal Firewall* ne tourne pas réellement sur un véritable Internet gateway car le niveau de sécurité sur votre computer en sera diminué.

Firewall Logging

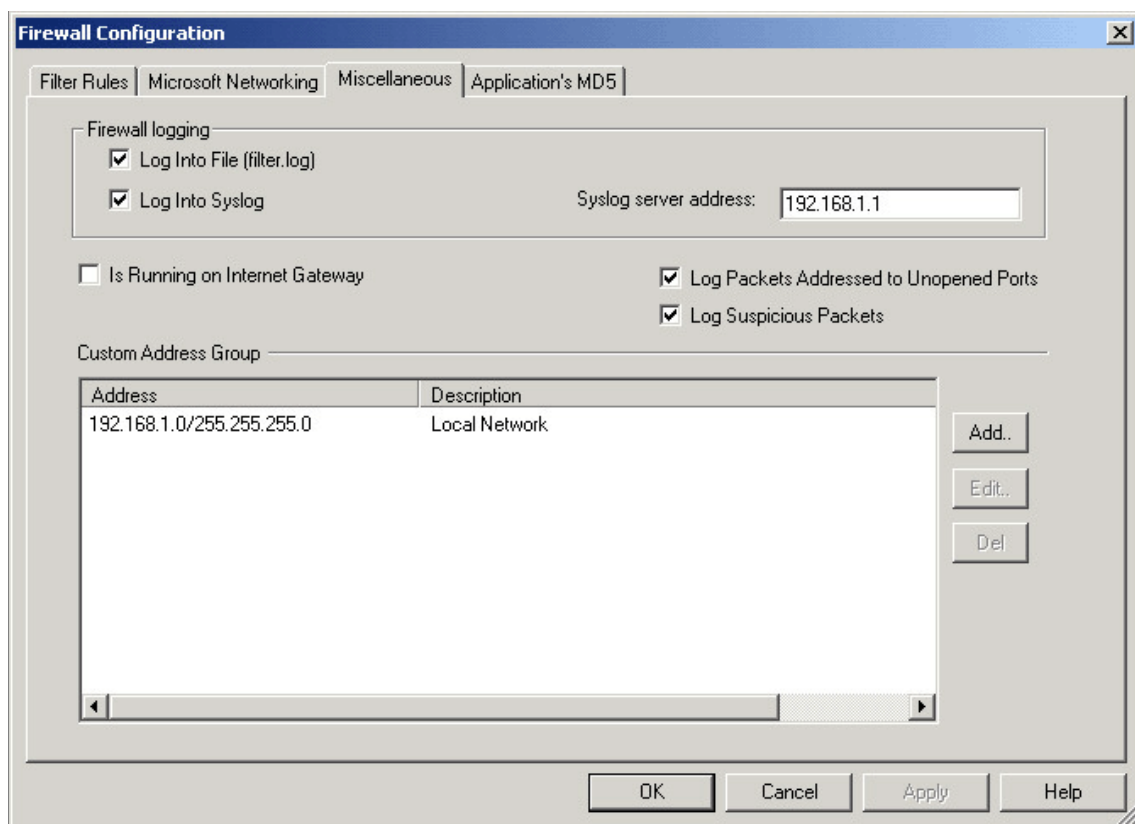
4.1 Configuration du loggin

Kerio Personal Firewall permet la création de fichiers log détaillés concernant l'acceptation et le filtrage des packets. L'utilisateur (ou l'administrateur) a une palette d'options pour déterminer quelle information et où la logger. Les logs peuvent être sau- vés soit vers un fichier (avec le nom filter.log sauvegardé sous le répertoire d'installation de *Personal Firewall* — typiquement

C:\Program Files\Kerio\Personal Firewall)

ou envoyé à un *Syslog* server.

La configuration de base du log se fait dans la fenêtre *Firewall Configuration*, onglet *Miscellaneous* dans la section *Firewall*.



Log Into File (filter.log) Les logs seront sauvegardés dans le fichier `filter.log` (dans le répertoire d'installation de *Personal Firewall*). La limite de ce fichier est seulement celle de l'espace disponible sur le disque.

Log Into Syslog Les logs seront envoyés à un *Syslog* server tournant à une adresse IP spécifiée.

Log Packets Addressed to Unopened Ports Loge les packets adressés à des ports depuis lesquels aucune application ne tourne (typique d'un portscanning).

Log Suspicious Packets Loges les packets que *Kerio Personal Firewall* considère suspects. Ce sont ea les packets TCP qui n'appartiennent pas à une connexion ouverte et n'initient pas une nouvelle connexion (les «TCP PINGS»).

4.2 Filter.log file

Le fichier `filter.log` est utilisé pour logger les actions de *Kerio Personal Firewall* sur un PC local. Il est créé dans le répertoire d'installation de *Personal Firewall* (typiquement

`C:\Program Files\Kerio\Personal Firewall`).

Il est créé lors du premier enregistrement.

`Filter.log` est un fichier texte où chaque enregistrement est placé sur une nouvelle ligne. Il a le format suivant:

```
1,[08/Jun/2001 16:52:09] Rule 'Internet Information Services':  
Blocked: In TCP, richard.kerio.cz [192.168.2.38:3772]->localhost:25,  
Owner: G:\WINNT\SYSTEM32\INETSrv\INETINFO.EXE
```

Comment lire cette ligne:

- 1 — type de règle (1 = refuser, 2 = accepter)
- [08/Jun/2001 16:52:09] — date et heure de détection du packet (vérifier le setting correct du systeme temps de votre PC)
- Rule 'Internet Information Services' — nom de la règle appliquée (d'après le champs *Description*)
- Blocked: / Permitted: — indique si le packet a été accepté ou refusé (correspond au nombre indiqué au début de la ligne)
- In / Out — indique un incoming ou outgoing packet

- IP / TCP / UDP / ICMP etc. — protocole de communication (pour lequel la règle a été définie)
- richard.kerio.com [192.168.2.38:3772] — nom DNS du computer, depuis lequel le packet a été envoyé, entre crochets l'adresse IP avec le port source après les double-points
- localhost:25 — adresse IP de destination (ou nom DNS) et port (localhost = ce computer)
- Owner: — nom de l'application locale à laquelle le packet est adressé (incluant le chemin complet). Si l'application est un system service le nom affiché est SYSTEM.

