



## KERIO *WinRoute* Firewall Informations techniques

Chapter - 1	<a href="#"><u>Introduction à Kerio WinRoute Firewall</u></a>
Chapter - 2	<a href="#"><u>Fonctionnalités</u></a>
Chapter - 3	<a href="#"><u>Procédures d'installation</u></a>
Chapter - 4	<a href="#"><u>Support technique</u></a>
Chapter -5	<a href="#"><u>Questions fréquentes</u></a>

Lien vers [Manuel détaillé \(pdf\)](http://www.kerio.com/supp_kwf_manual.html)  
([http://www.kerio.com/supp\\_kwf\\_manual.html](http://www.kerio.com/supp_kwf_manual.html))

Lien vers [Centre de support en ligne](http://www.kerio.com/manual/kwf/en/index.html)  
(<http://www.kerio.com/manual/kwf/en/index.html>)

## INTRODUCTION A KERIO WINROUTE FIREWALL

Pare-feu conçu pour les sociétés PME PMI, Kerio WinRoute Firewall 6.4 est un gestionnaire d'accès Internet qui procure une sécurité de pointe pour les réseaux de toutes tailles, les protège contre toute attaque extérieures et virus et permet de contrôler les accès aux sites web selon leur contenu.

### NOUVEAUTE DE KERIO WINROUTE FIREWALL

- **2 Moteurs de scan antiviral:** Avec la version Kerio Winroute Firewall avec McAfee, vous pouvez utiliser le moteur interne de McAfee et un antivirus supplémentaire externe pour double contrôle des mails
- **Limiteur de bande passante:** Cette fonction à évaluer absolument permet de limiter les téléchargements et de maintenir une qualité de service constante.
- **Nouveau VPN 64 bits - Accès VPN avec sécurité SSL sans agent client:** Le VPN SSL intégré indépendant du poste client permet aux entreprises d'offrir un accès sécurisé à leurs ressources à partir d'un simple navigateur Internet. L'utilisateur peut naviguer sur l'arborescence de son poste, télécharger des fichiers, créer des répertoires. Avec l'antivirus intégré McAfee, Kerio WinRoute Firewall peut même vérifier ces fichiers transférés.
- **Routage avancé par Tunnel VPN:** Permet aux administrateurs de contrôler le transfert de l'information échangé entre deux points de tunnels VPN. Evite que les tables ne soient endommagées.
- **Nouveauté : La module 'STaR' :** module de statistiques et rapports qui analysent automatiquement le trafic du réseau et s'affiche sous forme de graphiques simple à parcourir à partir d'un navigateur web.



### NOUVEAUTES VERSION 6.4

- Le nouveau module Kerio StaR offre désormais:
  - Un profil Internet complet pour chaque utilisateur du réseau
  - Les rapports listent clairement les sites web visités dans la journée
  - Le temps passé sur chaque site,
  - Les requêtes de moteurs de recherches effectuées
  - Les téléchargements de fichiers importants.
  - Indiquent également l'activité de chat et multimédia (radio Internet, videos Youtube)
  - Les connexions à distance (VPN et SSL)
  - Tous ces rapports peuvent être également facilement imprimés
- Performance améliorée (600 Mbs sur NAT et 200 Mbs sur inspection de protocole)
- Support pour DNS dynamique

Et aussi ...

- Meilleure intégration des applications Voix sur IP
- Il est possible d'exclure certains URL connus pour un affichage plus clair des rapports
- Support de quotas hebdomadaires

## FONCTIONNALITES

*Kerio WinRoute Firewall* est un outil complet pour la connexion d'un réseau à Internet et la protection de celui-ci contre les intrusions. Il est conçu pour les systèmes Windows 2000, XP, et 2003.

### 2.1. PRINCIPALES FONCTIONNALITES

- **Firewall d'entreprise certifié par le laboratoire ICSA Labs:** Certifié depuis 2000, Kerio WinRoute Firewall, pare-feu dynamique de réseau propose une définition détaillée des règles pour assurer une inspection dynamique du protocole de tout le trafic Internet entrant et sortant.
- **Client/Serveur VPN intégré, avec protection SSL**  
Le serveur VPN intégré sécurisé SSL fonctionne aussi bien mode client serveur que serveur à serveur, permettant ainsi à deux sites d'une entreprise de communiquer ou à des correspondants itinérants de se connecter à leur siège. Le VPN SSL sans agent Client permet à des utilisateurs nomades de se connecter de façon sécurisée pour partager des fichiers à partir de n'importe quel navigateur et connexion Internet.
- **Protection antivirus de la passerelle**  
Kerio WinRoute Firewall propose en option le scanning antivirus de la messagerie électronique entrante et sortante, du trafic Internet et des transferts FTP. En plus d'une version à antivirus McAfee intégré, vous pouvez choisir parmi différentes autres options antivirus.
- **Protection de navigation**  
L'option de filtrage Internet incorporée ISS Orange Web Filter bloque l'accès aux usagers, jusqu'à 58 catégories de contenus de pages Internet, diminuant les responsabilités légales pour les environnements d'entreprises et scolaires
- **Supervision réseau en temps réel:**  
Les administrateurs ont un accès en temps réel à toute activité de navigation sur le web, afin de suivre de près ce à quoi est exposé leur réseau et prévenir les brèches de sécurité.
- **Filtrage de contenu**  
Kerio WinRoute Firewall offre une variété d'éléments de sécurité de contenu. Le P2P Eliminator détecte automatiquement et bloque le réseau particulier à particulier tels que Kazaa. Le pare-feu Kerio WinRoute Firewall peut filtrer les fichiers potentiellement dangereux ou indésirables tels que des fichiers exécutables ou la musique MP3. Avec la filtration http, le pare-feu bloque les fenêtres pop-up dérangeantes de publicité.
- **Gestion d'accès personnalisée**  
Chaque usager du réseau peut être invité à se connecter à Kerio WinRoute Firewall avant de se raccorder à Internet. Ceci permet l'application de règles de sécurité et d'accès restrictives, basées sur l'utilisateur spécifique, plutôt qu'en fonction de l'adresse IP du système se connectant au serveur.
- **Partage de l'Internet rapide**  
Le support pour Internet par DSL, modems à câble, ISDN, satellite, ligne commutée ou WiFi permet aux administrateurs de déployer Kerio WinRoute Firewall dans les réseaux de toutes dimensions et en tous les endroits. Les utilisateurs peuvent partager une connexion Internet à basculement vers une connexion de secours.

- Support VoIP et UPnP

Le pare-feu Kerio WinRoute Firewall permet aux protocoles H.323 et SIP de se connecter par son intermédiaire, éliminant la nécessité d'exposer publiquement l'infrastructure VoIP à Internet. Il intègre aussi la technologie UPnP, ce qui permet aux applications compatibles telles que MSN Messenger de fonctionner instantanément sans nécessité de configuration supplémentaire du pare-feu.

- Statistiques de web et rapportage : (module StaR) : La nouvelle version 6.3 introduit le module StaR, module de statistiques et rapports qui analysent automatiquement les données du réseau et le trafic réseau sous-jacent et les différentes utilisations sous forme de graphiques simple à parcourir. Il permet également de consulter les trafics par individus, avec les liens des sites Web visités, ou la possibilité de couper la navigation par catégorie lorsque le pare-feu Kerio est combiné avec le filtre Web ISS Proventia

## 2.2 FONCTIONS DE BASES

### 2.2.1 Accès Internet Transparent

Grâce à la technologie NAT (Network Address Translation), le réseau local peut accéder à Internet au travers d'une seule adresse IP (statique ou dynamique). Contrairement aux serveurs Proxy, avec cette technologie NAT, tous les services Internet seront accessibles à partir de n'importe quel poste et il est possible de lancer la plupart des applications réseaux comme si tous les systèmes du réseau avait chacun leur propre connexion Internet.

### 2.2.2 Sécurité

Ce pare-feu intégré protège tout le réseau local (y compris le poste sur lequel il est installé), que la fonction NAT soit installé (IP translation) ou que *WinRoute* soit utilisé comme un routeur neutre entre deux réseaux. *Kerio WinRoute Firewall* offre la même protection que les solutions hardware couteuse du marché.

### 2.2.3 Un contrôle complet

Tous les paramètres de sécurité dans *WinRoute* sont gérés par des règles de trafic. Celles-ci offre une protection complète contre les attaques extérieures ainsi qu'un accès sécurisé à tous les services du réseaux (par exemple serveur Web, serveur de messagerie, Serveur FTP, etc.). Ces règles peuvent également restreindre l'accès des utilisateurs à certains sites Web.

### 2.2.4 Limiteur de bande passante

Les problèmes de connections Internet surviennent de façon typique lorsque certains utilisateurs cherchent à télécharger de gros volumes de données (installation d'archives, d'images disque, de fichiers audio/vidéo, etc.) et ralentissent ainsi la vitesse d'accès pour les autres. Le module de limitation de bande passante de *WinRoute* permet d'en réserver une part pour le téléchargement de gros fichiers, le reste de bande restant constant pour les autres services.

### 2.2.5 Inspecteurs de protocoles

Il est possible de rencontrer des applications qui ne supportent pas le standard de communication et qui utilisent des protocoles incompatibles. Pour résoudre ce problème, *WinRoute* inclut aussi

l'inspecteur de protocoles qui identifient le protocole approprié des applications et modifie le comportement du Firewall dynamiquement : les accès temporaires à un port spécifique (le port peut être ouvert momentanément par le serveur), le FTP en mode actif, Real Audio ou PPTP en sont quelques exemples.

### 2.2.6 Configuration réseau

*WinRoute* contient un serveur DHCP intégré qui établit les paramètres TCP/IP pour chaque poste du réseau. Les paramètres des stations peuvent être gérés de façon centralisée à par d'un seul point. Ceci réduit le temps de mise en place sur les réseaux et en minimise le risque d'erreur.

Le module *DNS Forwarder* permet un paramétrage DNS simple et des réponses plus rapides des requêtes DNS. Il s'agit d'un serveur tampon relayant les requêtes vers un autre serveur DNS. Les réponses sont enregistrées dans sa mémoire. Ceci augmente de manière importante les réponses à des requêtes récurrentes. Combiné au serveur DHCP et au fichier systèmes HOSTS, le *DNS Forwarder* peut être aussi utilisé comme un serveur DNS dynamique pour un domaine local.

### 2.2.7 Administration, alertes et statistiques

La console d'administration peut être installée à distance pour permettre la configuration sécurisée depuis n'importe quel endroit du réseau. Chaque événement important est rapporté à l'administrateur par email. Des diagrammes et statistiques bien organisés aident à déterminer le problème et les habitudes d'utilisation.

### 2.2.8 Systèmes d'exploitation variés au sein du réseau local

*WinRoute* fonctionne avec les protocoles TCP/IP standard. Du point de vue des postes clients, il agit comme un simple routeur et aucune application cliente particulière n'est nécessaire. C'est pourquoi tout OS avec TCP/IP, tel que Windows, Unix/Linux, Mac OS etc., peuvent fonctionner au sein du réseau.

*Note: WinRoute* ne tourner qu'avec les paramètres de protocoles TCP/IP. Il n'affecte pas les fonctionnalités des autres protocoles (IPX/SPX, NetBEUI, AppleTalk, etc.).

## 2.3. AUTRES FONCTIONS

### 2.3.1 Filtrage HTTP et FTP

*WinRoute* contrôle toutes les communications HTTP et FTP et bloque les objets qui ne correspondent pas aux profils établis. Ceux-ci peuvent être fixé de manière générale ou spécifiquement par utilisateur.

### 2.3.2 Contrôle Antivirus

*WinRoute* peut effectuer un contrôle antivirus de fichiers transmis. Il offre pour ceci une version avec l'antivirus intégré *McAfee*. L'accès à un antivirus externe (*NOD32*, *AVG*, *Sophos*, etc.) est également possible. L'antivirus contrôle alors les flux *HTTP*, *FTP*, *SMTP* et *POP3*.

### 2.3.3 Un support Active Directory transparent

Une base d'utilisateurs locale n'est pas nécessaire, car ils sont tous authentifiés par un Active Directory centralisé. La gestion et l'administration des utilisateurs s'en trouvent largement simplifiée.

#### 2.3.4 Alertes Email

*WinRoute* peut envoyer d'email d'alertes informant les utilisateurs de divers évènements. Cette fonction simplifie l'administration du pare-feu, évitant à l'administrateur réseau de se connecter au *WinRoute* pour contrôler ce qui se passe. Toutes les alertes sont sauvegardées dans un fichier log spécifique.

#### 2.3.5 Quotas utilisateurs

On peut également fixer une limite aux données transférées par chaque utilisateur. Cette limite peut être fixée selon la taille des données téléchargées, par jour/mois. Ces limitations sont appelées quotas. Si le quota est dépassé, la connexion Internet est bloquée pour l'utilisateur concerné. Un email d'alerte peut également être activé.

#### 2.3.6 Blocage des flux Peer to Peer

*WinRoute* peut détecter et bloquer les accès aux réseaux Peer-to-Peer (réseaux de partage de fichiers tels que *Kazaa*, *DirectConnect* etc.).

#### 2.3.8 Serveur et client VPN propriétaire VPN

*WinRoute* offre aussi une solution VPN propriétaire qui peut être appliquée en mode *serveur à serveur* et *client à serveur*. Cette solution VPN peut offrir un service NAT (même multiple) au deux bouts. Le *Kerio VPN Client* est inclus dans le package *WinRoute* et peut être utilisé pour la création de connexions VPN client serveur (connexions à distance au réseau local).

#### Le saviez vous?

Le VPN sécurisé SSL de Kerio *WinRoute* Firewall permet aux entreprises de configurer leur VPN en deux scénarios: serveur à serveur et client à serveur,

#### 2.3.9 VPN sécurisé SSL sans agent client

Les solutions VPN pour accéder à un réseau à partir d'un poste distant sont nombreuses à nécessiter l'installation d'une application cliente spécifique. La solution VPN de Kerio ne nécessite pas d'agent client. Sécurisée SSL, elle permet la navigation sur le réseau pour un accès aux postes et fichiers partagés ainsi que le téléchargement et l'enregistrement de données. Le transfert est sécurisé *SSL (HTTPS)*.

## Chapitre -3 PROCEDURES D'INSTALLATION

### 3.1 CONFIGURATION REQUISE

#### Configuration requise pour installer *WinRoute*:

- CPU Intel Pentium II ou compatible; 300 MHz
- 256 Mo RAM
- 2 cartes réseaux
- 20 MB d'espace disque pour l'installation
- mémoire libre pour logs (dépend du trafic et du niveau de log sélectionné)
- Pour une protection maximale, il est recommandé d'utiliser un système de fichier *NTFS*.

**Le saviez vous?**  
*Kerio WinRoute Firewall offre des fonctions avancées telles que le filtrage de contenu et contrôle en temps réel afin de superviser au plus près l'activité d'un utilisateur.*

Le produit peut être installé sur les systèmes suivants :

- Windows 2000
- Windows XP (Edition 32-bit seulement)
- Windows Vista
- Windows Server 2003 (Edition 32-bit seulement)

*Note:* Le composant *Client for Microsoft Networks* doit être installé pour tous les OS supporté, sinon *WinRoute* ne sera pas accessible comme un service et l'authentification NTLM ne fonctionnera pas. Le composant est inclus dans les packs d'installation de tous les OS.

#### Configuration requise pour Kerio VPN Client

Pentium III  
 128 MB RAM  
 5 MB HDD

Windows 2000/XP/2003/Vista  
 32-bit or 64-bit Windows

#### Configuration requise pour Kerio StaR - web browsers

Internet Explorer 6 and 7  
 Firefox 1.5 and 2  
 Safari 1.3 and 2

### 3.2 Comment installer *Kerio WinRoute Firewall*

#### 3.2.1 Démarrage rapide

1. Lancez le programme d'installation de Kerio *WinRoute* et sélectionner l'installation standard. Désactivez le partage de connexion Internet (Windows 2000, XP) ou le service Internet Connexion Firewall (Windows XP sp2) si ils sont détecté par le programme d'installation (sinon *WinRoute* ne fonctionnera pas correctement).

2. Définissez un nom d'utilisateur et un mot de passe qui seront utilisés pour le compte administrateur.
3. Vous recevrez peut être un message alertant que l'adaptateur Kerio VPN n'a pas passé le test Windows. Il est conseillé d'ignorer ceci et de cliquer sur "Continue Anyway."
4. Redémarrer votre machine lorsque l'installation sera terminée.
5. Après redémarrage, lancez la console d'administration Kerio (Démarrez/ Programmes / Kerio). Connectez-vous au réseau local (sur le poste local) avec le nom et mot de passe défini durant l'installation. L'assistant de configuration se lancera automatiquement après le premier login.

Vous pouvez établir les différents paramètres suivants:

- Type de connexion Internet — interface par laquelle le firewall est connecté à Internet.
- Interface Internet — sélectionnez une interface Internet ou connexion Dial-up. Insérez le nom d'utilisateur et mot de passe pour le compte s'il s'agit d'une connexion Dial-up.
- Dans le cas d'une dial-up connexion, *WinRoute* nécessite nom d'utilisateur et mot de passe. Ceci n'est pas nécessaire si ces informations sont déjà enregistrées dans le système. Si non il faut ici les spécifier.
- Règles pour trafic sortant— ces règles permettent l'accès aux services Internet.
- Politique VPN — cocher Yes, I want to use Kerio VPN... permettra la connexion de filiale avec le siège de l'entreprise ainsi que des utilisateurs distants de se connecter.
- Règles pour trafic entrant — par exemple le mapping d'un serveur SMTP (email).
- Partage de la connexion Internet — La Network Address Translation (NAT) doit être activé si des adresses IP privées sont utilisées à l'intérieur du réseau

[Liste complète](http://www.kerio.com/manual/kwf/en/ch01.html)

(<http://www.kerio.com/manual/kwf/en/ch01.html>)

## SUPPORT TECHNIQUE

Kerio Technologies fournit un support email et téléphone gratuit pour les utilisateurs enregistrés de *Kerio MailServer*. Pour les coordonnées de contacts, reportez vous à la fin de ce chapitre. Notre équipe technique est à votre disposition pour résoudre vos moindres problèmes.

Vous pouvez également résoudre de nombreux problèmes vous même (et parfois plus rapidement): nous vous conseillons de procéder de la façon suivante avant de vous décider à contacter le support technique de *Kerio Technologies*:

- Essayez de trouver la réponse à vos questions dans ce manuel. Chaque chapitre décrit en détails les fonctions de *Kerio MailServer* et comment les utiliser pour optimiser les paramètres de votre futur serveur de messagerie.
- Si vous ne trouvez pas la solution dans ce manuel, reportez vous au:
  1. la page web de *Kerio WinRoute Firewall* ([http://www.kerio.com/kwf\\_home.html](http://www.kerio.com/kwf_home.html))
  2. notre site web de support technique (<http://www.kerio.com/support>)
- Deux autres sources d'informations très utiles sont d'une part le forum de discussion très actif des utilisateurs de *Kerio WinRoute Firewall* — allez sur la page <http://forum.kerio.com/> et d'autre part la base de données de connaissances Kerio accessible à la page suivante <http://support.kerio.com/>.
- Vous pouvez soumettre vos problèmes spécifiques via le formulaire de support technique spécial aussi accessible sur cette page <http://support.kerio.com/>.

### 4.1 Contacts

#### Etats-Unis

*Kerio Technologies Inc.*

2350 Mission College Blvd., Suite 400

Santa Clara, CA 95054

Phone: +1 408 496 4500

Support technique par email <http://support.kerio.com/>. <http://www.kerio.com/>

**Le saviez vous ?**  
Kerio offre ses produits en  
évaluation complète 30 jours pour  
encourager les administrateurs à les  
tester avant d'acheter.

#### Grande Bretagne

##### **Kerio Technologies UK Ltd.**

Enterprise House  
Vision Park, Histon,  
Cambridge CB4 9ZR

Tel: 01223 202 130, Fax: 01223 233 055

Email technical support is available at <http://support.kerio.com/>.  
<http://www.kerio.co.uk/>

#### République Tchèque

##### **Kerio Technologies s. r. o.**

Anglicke nabrezi 1/2434  
301 49 PLZEN

Phone: +420 377 338 902

Email technical support is available at  
<http://support.kerio.cz/>. <http://www.kerio.com/>

#### France (support premier niveau)

Siener Informatique  
51 rue Hoche  
95200 Ivry sur seine  
Email du support technique

Tél. : 01 56 20 24 21  
Fax : 01 56 20 24 30  
[support@sienerinformatique.com](mailto:support@sienerinformatique.com)

## Chapitre -5

### QUESTIONS FREQUENTES

#### **Quelle est la différence entre *Kerio WinRoute Firewall* et un appliance firewall?**

*Kerio WinRoute Firewall* est une solution logicielle de protection Internet conçu pour les PME. Parce qu'elle est logicielle, elle peut être mise à jour régulièrement et peut s'adapter à la taille grandissante d'un réseau. Les pare-feu matériels ont un plafond d'utilisateurs et il faut acquérir des appliance supplémentaires coûteux. *Kerio WinRoute Firewall* est plus flexible et simple à administrer.

#### **Comment puis-je savoir si ma société est assez grande pour héberger une solution passerelle d'entreprise comme *Kerio WinRoute Firewall*?**

Bien que nous ne sommes pas en position de spéculer autour des coûts croissants de gestion contre les virus et vers indésirables, notre expérience nous indique que toute entreprise quelque soit sa taille peut s'équiper de *Kerio WinRoute Firewall* si elle accède régulièrement à Internet

#### **Où puis-je télécharger ma version complète limitée 30 jours pour tester *Kerio WinRoute Firewall*?**

La version d'essai de *Kerio WinRoute Firewall* est disponible à l'adresse suivante [http://www.kerio.fr/kwf\\_download.html](http://www.kerio.fr/kwf_download.html) . Cette version n'est pas limitée dans ses fonctions de manière à les rendre toutes accessibles à l'administrateur pour son évaluation complète avant sa décision d'achat.

#### **Quel est le marché cible de *Kerio WinRoute Firewall*?**

*Kerio WinRoute Firewall* est conçu d'abord pour les réseaux PME, pour les structures de 10 à 1000 utilisateurs. *Kerio WinRoute Firewall* est utilisé dans tous les corps de métiers et tous les secteurs y compris l'éducation, les administrations, les technologies de pointes, le marketing ou le design.

#### **Quel est le nombre maximum d'utilisateurs que *Kerio WinRoute Firewall* peut gérer?**

Cela dépend du poste matériel sur lequel est installé. Nous estimons qu'environ 1 MB de capacité est nécessaire pour 5 utilisateurs.

#### **Combien de temps prendra l'installation?**

L'installation et la configuration de *Kerio WinRoute Firewall* par un administrateur expérimenté doivent prendre environ 30 à 45 minutes.

#### **Avec le VPN sécurisé SSL sans agent, dois-je configurer les postes clients pour qu'ils accèdent aux connexions VPN de l'entreprise?**

Non – c'est l'avantage d'un VPN sans agent client. Dans l'intégration de la solution, les administrateurs peuvent contrôler les « clients » VPN par une application Web simple qui évite à l'utilisateur de devoir lui-même configurer son poste, configuration souvent source d'erreur.