Kerio WinRoute Firewall Features Summary and Simple Setup Guide (for version 6.x)

Network setup and KWF installation/administration

General features and concepts

VPN - Virtual Private Networking

Licensing

Network setup and Kerio WinRoute Firewall Deployment - This section describes basic TCP/IP configuration and KWF installation instructions for administration.

Before installing

Kerio WinRoute Firewall (KWF) integrates with the underlying Windows Operating System, which allows all the features of

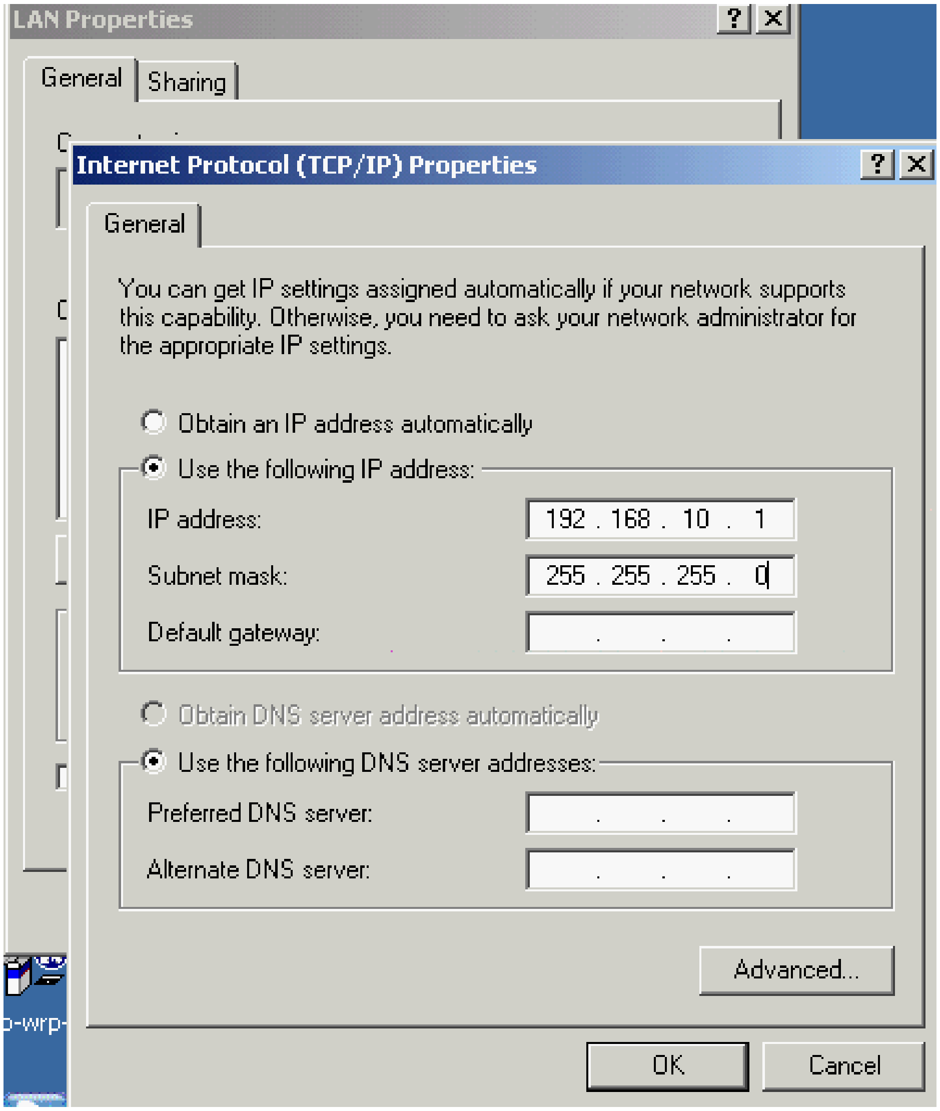
KWF to operate in conjunction with the many services offered by the OS. This flexibility however requires that certain conditions are met before KWF can be installed. The gateway where KWF will be installed must have at least 2 network interfaces to accommodate proper IP routing between the local network interface and the Internet interface. This can include Ethernet, modem, USB, wireless... or any medium which communicates over TCP/IP. The interface which will connect to the public network must be configured according to the specifications of the Internet Service Provider. There cannot be any 3rd party firewall or VPN software installed on the the gateway. Internet Connection Sharing and Internet Connection Firewall for Windows XP must not be enabled! If ICS for Windows 2000 has ever been installed, it is absolutely necessary to uninstall/reinstall TCP/IP.

Manual TCP/IP configuration on the firewall host

KWF routes all packets using IP forwarding in Windows. Therefore, it is absolutely imperative that TCP/IP is properly configured in the OS.

Wan Interface - The Interface connected to the Internet/WAN will be configured based on the specifications of the ISP.

Lan Interface - Other interfaces must be configured manually. In most cases, a reserved private IP address such as 192.168.10.1 should be assigned. A subnet mask of 255.255.255.0 would allow up to 253 client PCs, which should be sufficient for most networks. The IP address and subnet mask are the only parameters which should be defined. There should be no default gateway or DNS servers assigned to any local network interface. These values are assigned only to the Internet/WAN interface by the Internet Service Provider.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

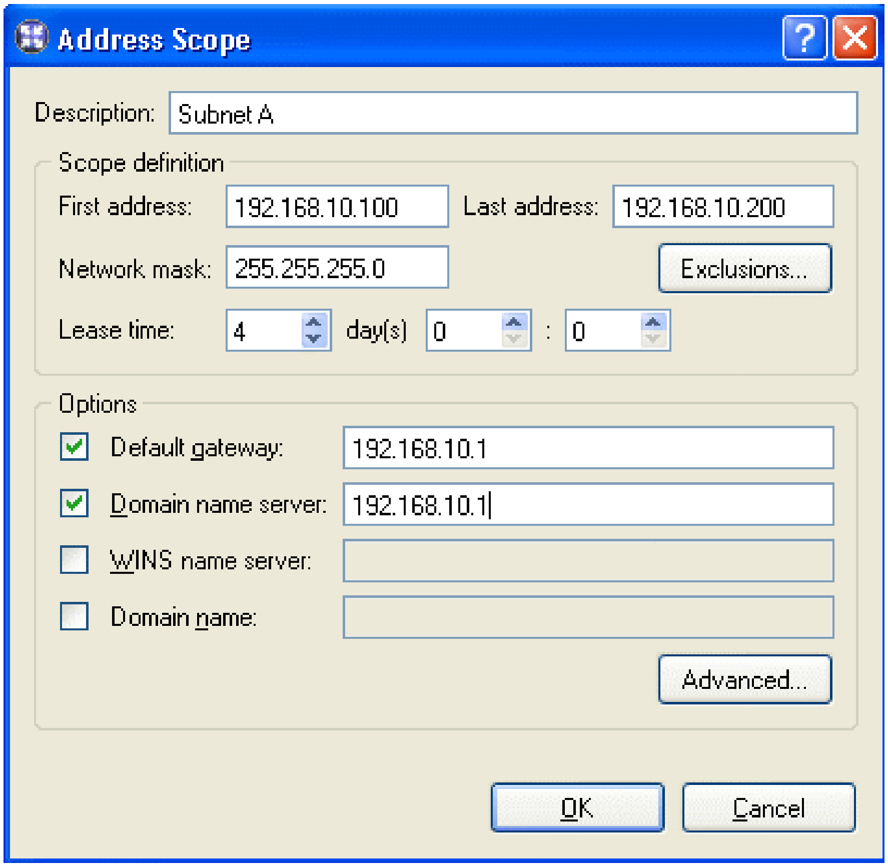
IP address: 192 . 168 . 10 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

DHCP TCP/IP configuration on the clients

Each workstation must be configured with (at a minimum) an IP address, Default gateway and DNS server. The IP addresses must be in the same IP subnet range as the WinRoute Firewall's local network interface(s). The default gateway must be the IP address of the local network interface of the WinRoute firewall (e.g. 192.168.10.1). The DNS server can be any valid Internet name server, or it can be the IP address of the WinRoute firewall, in which case the built-in DNS forwarder will handle the DNS requests. The default action of KWF's DNS forwarder is to send all queries to the DNS servers assigned to the IP stack of the firewall host computer (usually the ISP's DNS servers). For simple management and quick deployment of workstations in the network, it is recommended to use KWF's DHCP server. For further explanation of DHCP configuration, refer to the KWF documentation, Section *DHCP Server*, Chapter *Settings for Interfaces and Network Services*.



Description: Subnet A

First address: 192.168.10.100 Last address: 192.168.10.200

Network mask: 255.255.255.0

Lease time: 4 day(s) 0 : 0

☑ Default gateway: 192.168.10.1

☑ Domain name server: 192.168.10.1

☐ WINS name server:

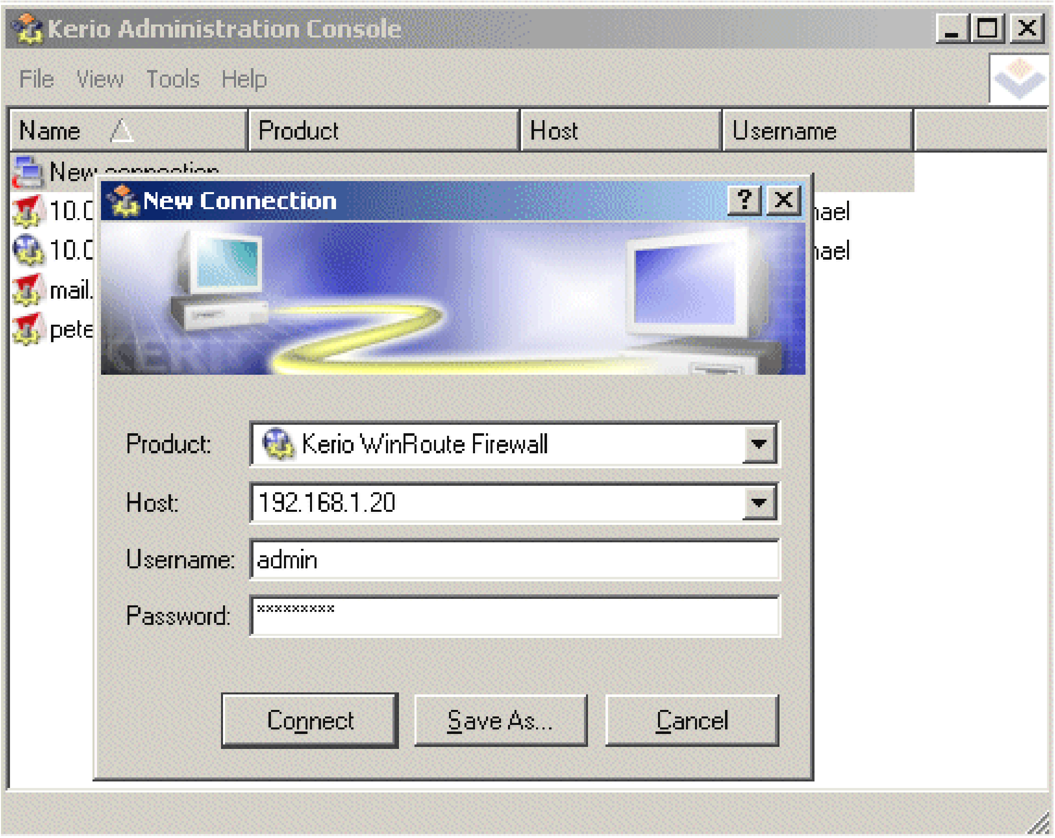
☐ Domain name:

Installation

There are two installation packages available: KWF standard and KWF with McAfee Anti-Virus. Both versions come with all components necessary to run KWF, which includes: WinRoute engine, WinRoute engine monitor, H.323 protocol inspector, administration console, administration console plug-in and the ISS OrangeWeb Filter. During installation it will be necessary to specify the installation directory, which should contain sufficient storage space (minimum of 10 MB, recommended 3 GB for logs and cache file). Other parameters include the administrator account (which will be used to log into the firewall) and the option to import settings from WinRoute Pro (if applicable).

Administration (local/remote)

KWF administration is all managed through a separate application (admin.exe), which can be installed individually using the custom option of the product installation package. All administrative functions use a proprietary communication link which is securely encrypted. The communication port is TCP/UDP port 44333. All changes to the security policy are logged in the config log. If you need to configure KWF from the Internet, it is necessary to configure a traffic rule which allows access to a predefined service called KWF admin. Explanation of traffic policy is defined later in this document. Note that the administrative application takes advantage of the right mouse button to extend options in most dialogs.



Product: Kerio WinRoute Firewall

Host: 192.168.1.20

Username: admin

Password: *********

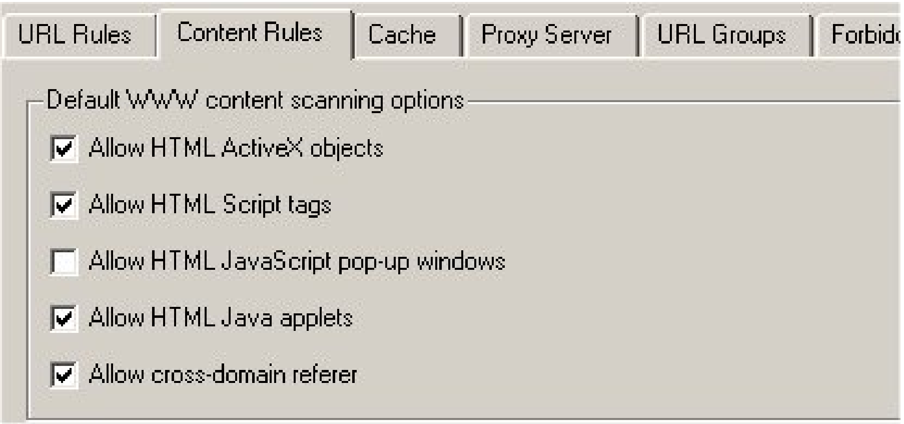
General features and concepts - This section briefly describes the primary components in KWF and how to effectively use them.

Transparent architecture

To improve monitoring, filtering, scanning, and support for the latest multimedia and messaging applications, KWF incorporates a sophisticated mechanism for interpreting the entire TCP stream of routed traffic. As with most NAT devices, only the IP header of each routed data packet is modified. KWF however, uses a special process to capture and manipulate the data stream of routed packets. In order to properly handle the intercepted communication, KWF must be able to interpret the application protocol. A handful of supported transparent parsers are available - they are called Protocol Inspectors. These components will be discussed in more detail later in this document.

Content Filtering

To improve user productivity in corporate environments it is sometimes necessary to restrict access to certain websites. It is impossible to block every offensive web site, however KWF offers several tools to manage this task. A predefined list of URL groups can be enabled to block advertisements, banners, pop-ups and similar marketing type material. Other custom URL groups can be added to the list. A predefined list of forbidden words can be enabled to block websites containing pornography or illegal software distribution. Each forbidden word group contains individual words which are weighted. If a page contains enough words, its total weight may exceed the threshold and the page will be restricted. Additional word group categories can be added by the administrator. URL rules are a separate component which allow the administrator to enforce policies by requiring authentication for specific events. URL rules can include custom definitions (e.g. *whitehouse.com*) or they can reference a category of URL groups (e.g. ads/banners) or they can reference the ISS OrangeWeb Filter. The order of rules is very important as KWF processes rules from top down. Forbidden word groups are filtered separately based on the weight system, and are applied globally to all users. Content rules are divided into 5 options: Allow HTML ActiveX objects, Allow HTML script tags, Allow HTML javascript pop-up windows, Allow java applets, Allow inter-domain referrer. These options can be disabled globally by an administrator, or by individual users through the firewall web interface described later in this document. Due to the transparent architecture, KWF is able to automatically redirect users to the KWF authentication page if they are not currently authenticated to the firewall. Without any customization or installation to the workstations, they will be automatically and transparently monitored/filtered by Kerio WinRoute Firewall.



Default WWW content scanning options

☑ Allow HTML ActiveX objects

☑ Allow HTML Script tags

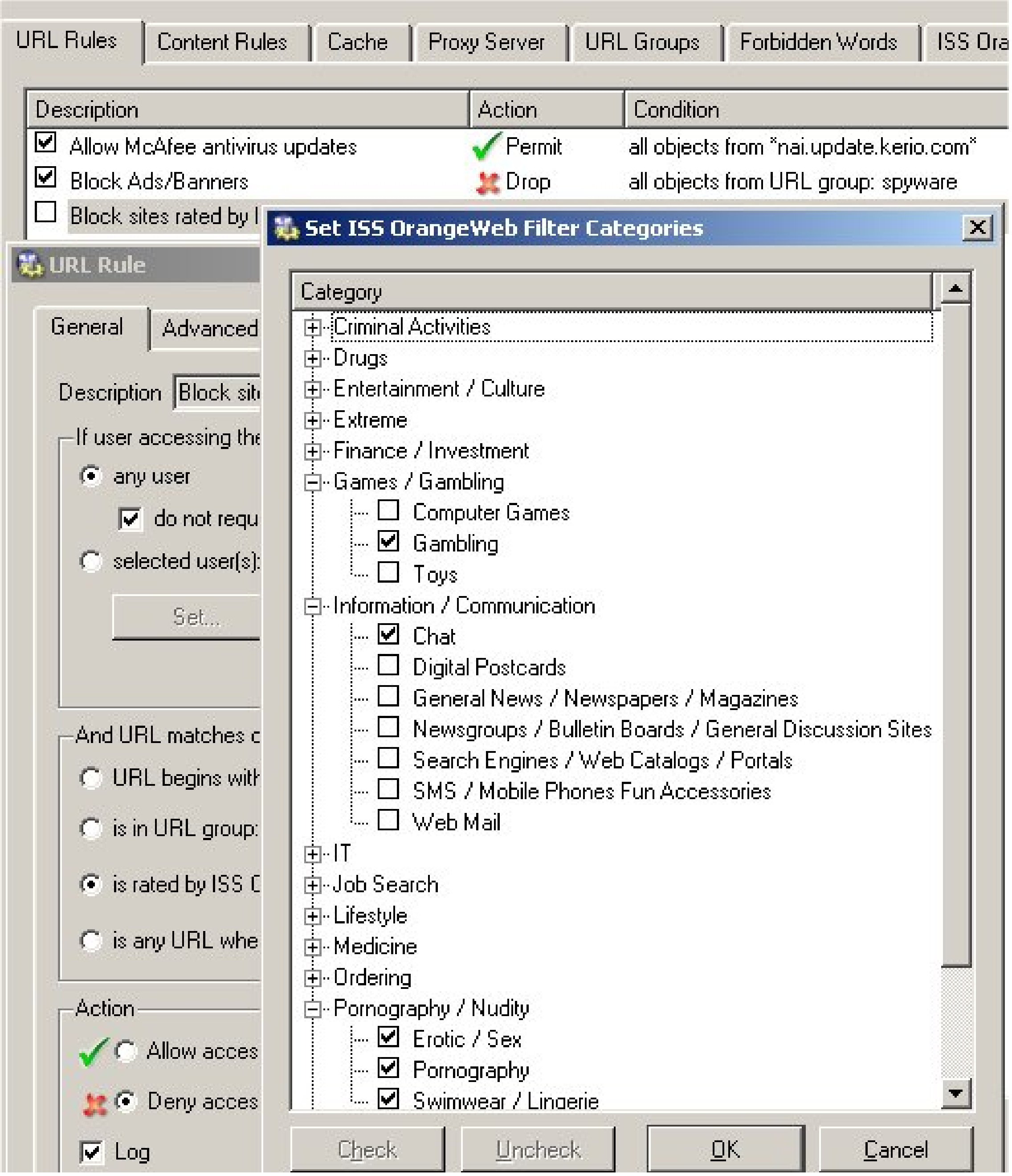
☐ Allow HTML JavaScript pop-up windows

☑ Allow HTML Java applets

☑ Allow cross-domain referer

ISS OrangeWeb Filter

The ISS OrangeWeb Filter is an intelligent software component of KWF that (if used) will forward queries to a central server which houses the database of categorized websites. Each URL rule can have different categories of access. URL categories include: Criminal Activities, Drugs, Entertainment, Extreme, Finance, Games... A separate dialog is available in the HTTP policy -> ISS OrangeWeb Filter dialog to specify whitelisted URLS.



Description	Action	Condition
☑ Allow McAfee antivirus updates	✓ Permit	all objects from "nai.update.kerio.com"
☑ Block Ads/Banners	Drop	all objects from URL group: spyware
☐ Block sites rated by I		

Description: Block sit

If user accessing the

● any user

☑ do not requ

○ selected user(s):

And URL matches c

○ URL begins with

○ is in URL group:

● is rated by ISS C

○ is any URL whe

Action

○ Allow acces

● Deny acces

☑ Log

Set ISS OrangeWeb Filter Categories

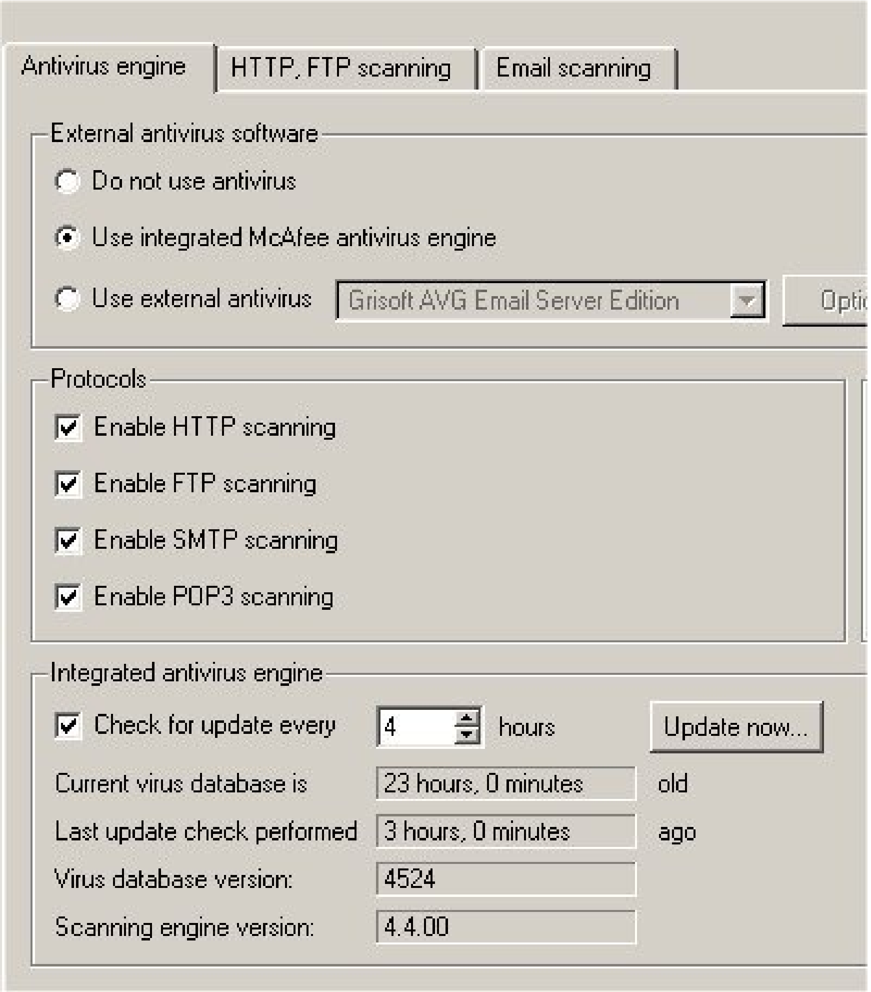
Category

- ⊞ Criminal Activities
- ⊞ Drugs
- ⊞ Entertainment / Culture
- ⊞ Extreme
- ⊞ Finance / Investment
- ⊟ Games / Gambling
  - ☐ Computer Games
  - ☑ Gambling
  - ☐ Toys
- ⊟ Information / Communication
  - ☑ Chat
  - ☐ Digital Postcards
  - ☐ General News / Newspapers / Magazines
  - ☐ Newsgroups / Bulletin Boards / General Discussion Sites
  - ☐ Search Engines / Web Catalogs / Portals
  - ☐ SMS / Mobile Phones Fun Accessories
  - ☐ Web Mail
- ⊞ IT
- ⊞ Job Search
- ⊞ Lifestyle
- ⊞ Medicine
- ⊞ Ordering
- ⊟ Pornography / Nudity
  - ☑ Erotic / Sex
  - ☑ Pornography
  - ☑ Swimwear / Lingerie

OK
Cancel
Kerio WinRoute Firewall / Configuration / Content Filtering / HTTP Policy
10.0.

McAfee and 3rd party Anti-Virus

Due to the transparent architecture, KWF is capable of capturing the entire TCP stream of network traffic routed through the firewall. This allows KWF to reassemble each packet to create the object being requested by a client behind the firewall. KWF can pass this object to a local Anti-Virus component. The McAfee version of KWF is available as a complete package, with no additional software required (i.e. the McAfee AV engine is built-in and automatically enabled). Updates are automatically processed by KWF and managed through the KWF administration console. Email and Web HTTP protocols are filtered for viruses. This includes HTTP, FTP, SMTP and POP3.



External antivirus software

○ Do not use antivirus

● Use integrated McAfee antivirus engine

○ Use external antivirus: Grisoft AVG Email Server Edition

Protocols

☑ Enable HTTP scanning

☑ Enable FTP scanning

☑ Enable SMTP scanning

☑ Enable POP3 scanning

Integrated antivirus engine

☑ Check for update every 4 hours

Current virus database is 23 hours, 0 minutes old

Last update check performed 3 hours, 0 minutes ago

Virus database version: 4524

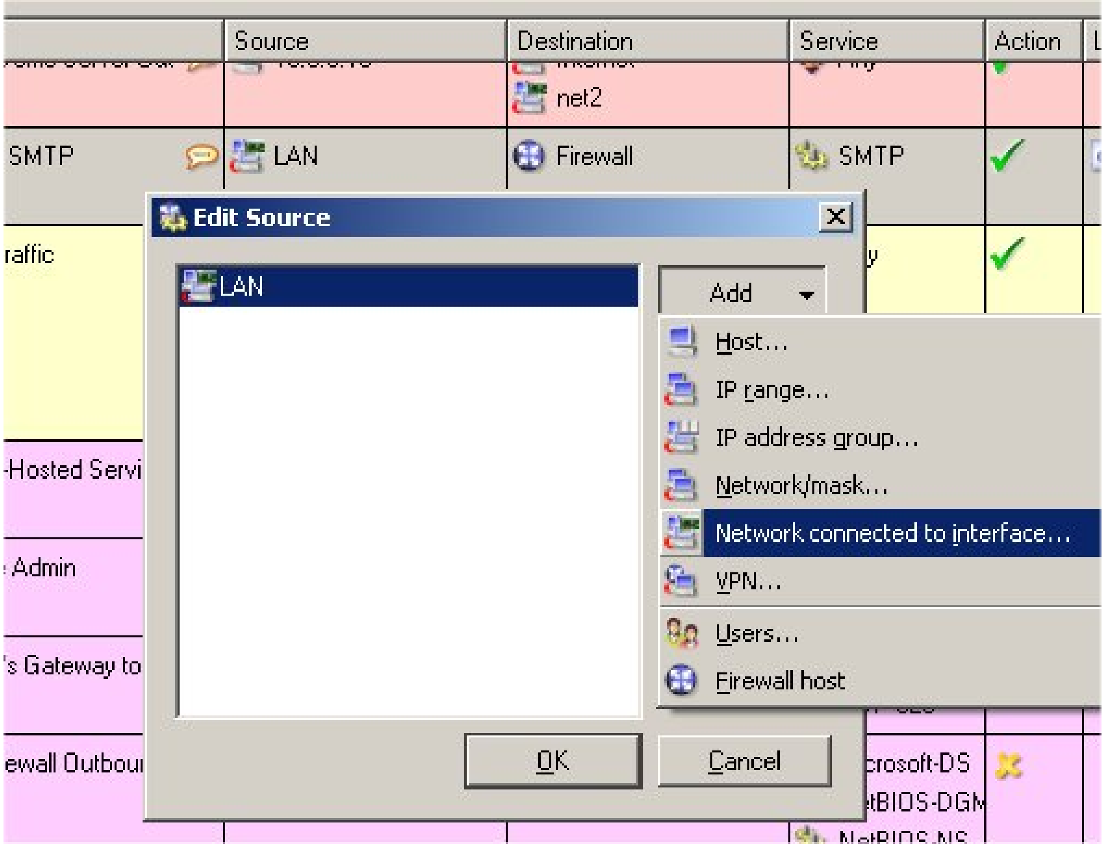
Scanning engine version: 4.4.00

UPnP

UPnP allows devices running UPnP enabled software to obtain Internet access through a UPnP enabled gateway. KWF offers limited UPnP support for applications such as Microsoft's MSN messenger. This feature is enabled by default, and can be disabled through the advanced options.

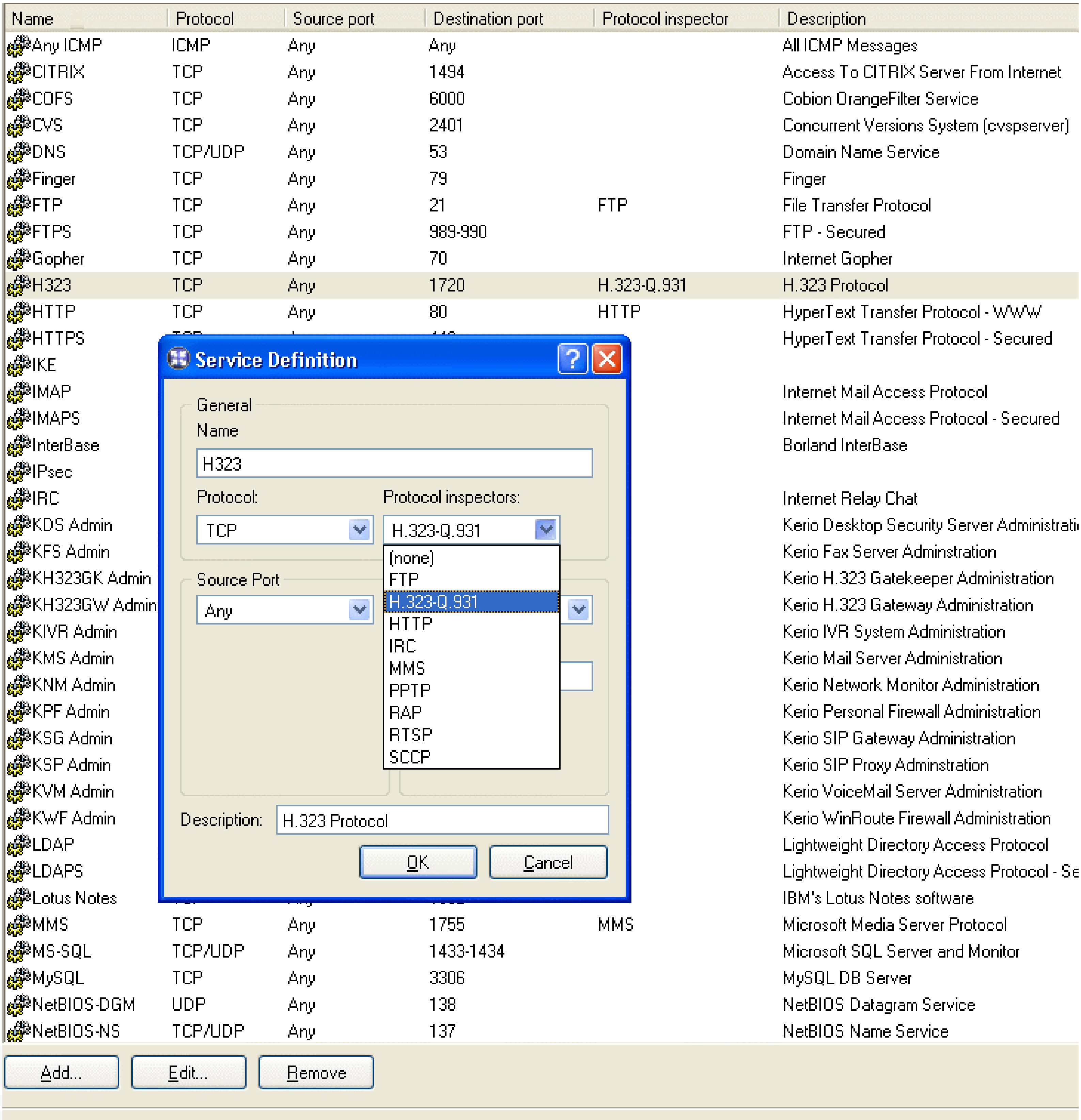
Interfaces and traffic policy source/destination entities

When configuring traffic policy rules KWF requires specification of source and destination objects. These objects can include: a predefined address group, a host IP address, a network range, an IP subnet, the firewall, authenticated users, specific users, specific groups, a network behind an interface or any. Most rules will consist of either 'network behind interface' or 'firewall'. The option 'network behind interface' refers to any IP address which exists on a network behind the specified interface. For this reason it is recommended to label all interfaces (e.g. LAN, or Inet) through the *Configuration/Interfaces* dialog before configuring the traffic policy. 'Firewall' refers to any IP address which is assigned to the Kerio WinRoute Firewall computer. The authenticated users, or selected users/groups option means that the specified IP traffic will only be allowed if the user has logged into the firewall through the web interface. The default setting will associate the IP to the authenticated user for 120 minutes. This timeout can be modified from the advanced options. As an example, a user may be denied the right to ping unless he/she authenticates to the firewall, after which time ping will be allowed from the user's IP address for the following 120 minutes. Users should use the web interface to logout if other users may be working with the same computer for other purposes.



Services and Protocol Inspectors

KWF ships with many predefined services, which include the IP protocols and port allocations used by well known services. For example, SMTP service is defined as TCP over port 25. These services are objects which can be referenced by traffic policy rules. For example, the SMTP service can be a selected object in the traffic policy for communication from the network behind a local interface to the firewall, in the case that a mail server resides on the Firewall PC and should be accessible from the local network. Some services include a Protocol Inspector. Protocol Inspectors allow KWF to properly handle complex protocols which are not allowed by most network firewalls. KWF supports the following Protocol Inspectors: FTP, SMTP, POP3, H.323-Q.931, HTTP, IRC, MMS, PPTP, RAP, RTSP, SCCP. If a service containing a Protocol Inspector is permitted by a traffic policy rule, the appropriate Protocol Inspector will automatically parse the routed traffic. Protocol Inspectors are activated on demand due to the transparent architecture of KWF described earlier in this document. In the traffic policy dialog it is possible to configure Protocol Inspectors by enabling the 'Protocol Inspectors' column through the right click option -> 'modify columns'. It is recommended to use 'default', however in some cases it may be desired to disable the Protocol Inspector, or to enable a specific Protocol Inspector for a custom service.



Name	Protocol	Source port	Destination port	Protocol inspector	Description
Any ICMP	ICMP	Any	Any		All ICMP Messages
CITRIX	TCP	Any	1494		Access To CITRIX Server From Internet
COFS	TCP	Any	6000		Cobion OrangeFilter Service
CVS	TCP	Any	2401		Concurrent Versions System (cvspserver)
DNS	TCP/UDP	Any	53		Domain Name Service
Finger	TCP	Any	79		Finger
FTP	TCP	Any	21	FTP	File Transfer Protocol
FTPS	TCP	Any	989-990		FTP - Secured
Gopher	TCP	Any	70		Internet Gopher
H323	TCP	Any	1720	H.323-Q.931	H.323 Protocol
HTTP	TCP	Any	80	HTTP	HyperText Transfer Protocol - WWW
HTTPS					HyperText Transfer Protocol - Secured
IKE					
IMAP					Internet Mail Access Protocol
IMAPS					Internet Mail Access Protocol - Secured
InterBase					Borland InterBase
IPsec					
IRC					Internet Relay Chat
KDS Admin					Kerio Desktop Security Server Administrati
KFS Admin					Kerio Fax Server Adminstration
KH323GK Admin					Kerio H.323 Gatekeeper Administration
KH323GW Admin					Kerio H.323 Gateway Administration
KIVR Admin					Kerio IVR System Administration
KMS Admin					Kerio Mail Server Administration
KNM Admin					Kerio Network Monitor Administration
KPF Admin					Kerio Personal Firewall Administration
KSG Admin					Kerio SIP Gateway Administration
KSP Admin					Kerio SIP Proxy Adminstration
KVM Admin					Kerio VoiceMail Server Administration
KWF Admin					Kerio WinRoute Firewall Administration
LDAP					Lightweight Directory Access Protocol
LDAPS					Lightweight Directory Access Protocol - Se
Lotus Notes					IBM's Lotus Notes software
MMS	TCP	Any	1755	MMS	Microsoft Media Server Protocol
MS-SQL	TCP/UDP	Any	1433-1434		Microsoft SQL Server and Monitor
MySQL	TCP	Any	3306		MySQL DB Server
NetBIOS-DGM	UDP	Any	138		NetBIOS Datagram Service
NetBIOS-NS	TCP/UDP	Any	137		NetBIOS Name Service

Service Definition

General

Name: H323

Protocol: TCP

Protocol inspectors: H.323-Q.931

Source Port: Any

Description: H.323 Protocol

Routing tables and IP forwarding

The Windows NT/2000/XP operating systems are all capable of IP forwarding. Because other Windows components may depend on this information, KWF does not use any internal routing functionality, rather it simply enables IP forwarding in Windows during the boot process and allows Windows to make routing decisions based on the local routing table. KWF is however capable of modifying the routing table which is used by the Operating System. The routing table is located under *Configuration/Routing Table* in the administration console. Static (Persistent) routes can be added/removed through a separate tab of this dialog.

NTLM authentication

As mentioned in the Content Filtering section, it is possible to automatically redirect users' browsers to the firewall authentication page if they are not already authenticated to the firewall. Users may become bothered by the necessity to log into the firewall several times a day. Although the default timeout of 120 minutes can be increased, a more viable option to users of NT domains or Active Directory Domains is available. In the *Configuration/Advanced Options/User Authentication* dialog there is an option Use "NTLM Authentication". This will allow users who participate in the local domain to automatically (no keystroke) log into the firewall using their NT logon account. Only MSIE browsers support this authentication method. Otherwise the user must login through the standard HTML based login page. Once the user has authenticated, KWF can now associate the authenticated user to his/her IP address. Traffic policy rules can enforce any IP based policy by the authenticated user. Additionally, all log data from each authenticated user's workstation will include both IP address and the name of the authenticated user.

Anti-Spoofing

Anti-Spoofing is located in *Configuration/Advanced Options/Anti-Spoofing*. If enabled, KWF will deny inbound traffic which is received on a particular interface if the source IP address is known to exist on a network of any other interface. This option is enabled by default.

Stateful packet inspection/connection tracking

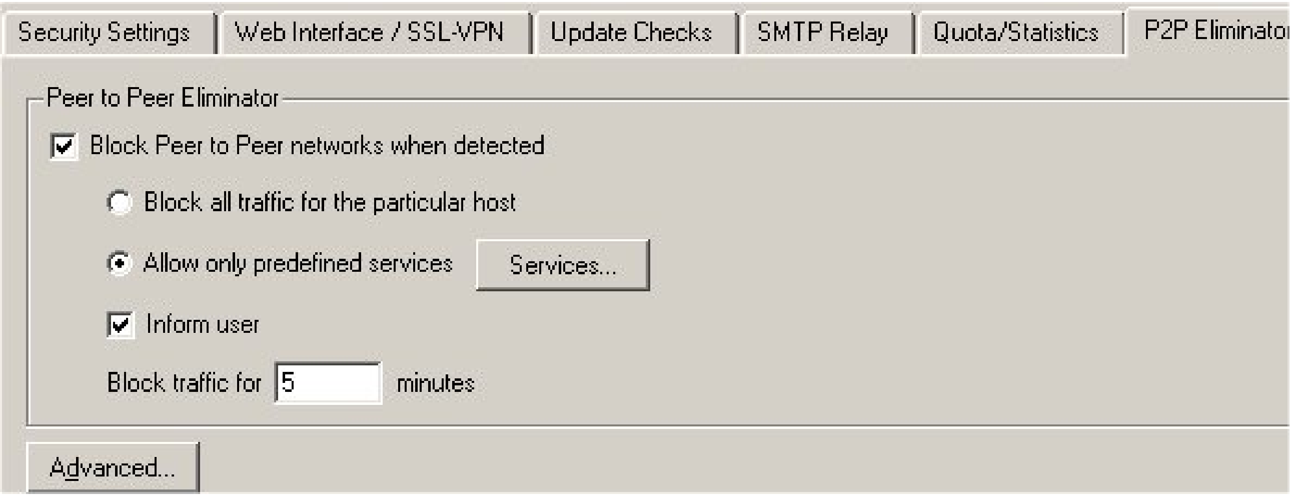
All permitted traffic through the firewall is recorded into a table in memory. This allows KWF to recognize returning traffic based on a previous outbound packet. In the *Configuration/Status/Connections* you can view all current connections from each workstation in the network. Stateful inspection is an implied feature and cannot be changed within the product.

Web interface

In order to enforce user based access policies KWF incorporates a small web engine to allow users to authenticate to the firewall using a web browser. The web component listens for connections on port 4080 for HTTP and 4081 for HTTPS. The web interface can be accessed through any web browser using HTTP://winroute:4080, or through SSL using HTTPS://winroute:4081. Users can also refer to this interface to view information such as their http access policy, restrictions for browser based scripting components, RX/TX statistics and cache content. Specific settings for the web interface are located in *Configuration/Advanced/User Authentication* .

P2P Eliminator

Peer to Peer applications are generally unwelcome in the work place. These applications are typically used to illegally transfer media and software. Examples of these types of applications include: Kazaa, BearShare, BitTorrent and eDonkey. Kerio WinRoute Firewall has a built-in feature that looks for network traffic that is typical of P2P software. This feature is automatic, and should not involve any modification. WinRoute has built-in intelligence to identify ports and connection oriented behavior that is known to originate from P2P applications. Specific settings for the P2P Eliminator are located in *Configuration/Advanced/P2P Eliminator*.



Peer to Peer Eliminator

☑ Block Peer to Peer networks when detected

○ Block all traffic for the particular host

● Allow only predefined services

☑ Inform user

Block traffic for 5 minutes

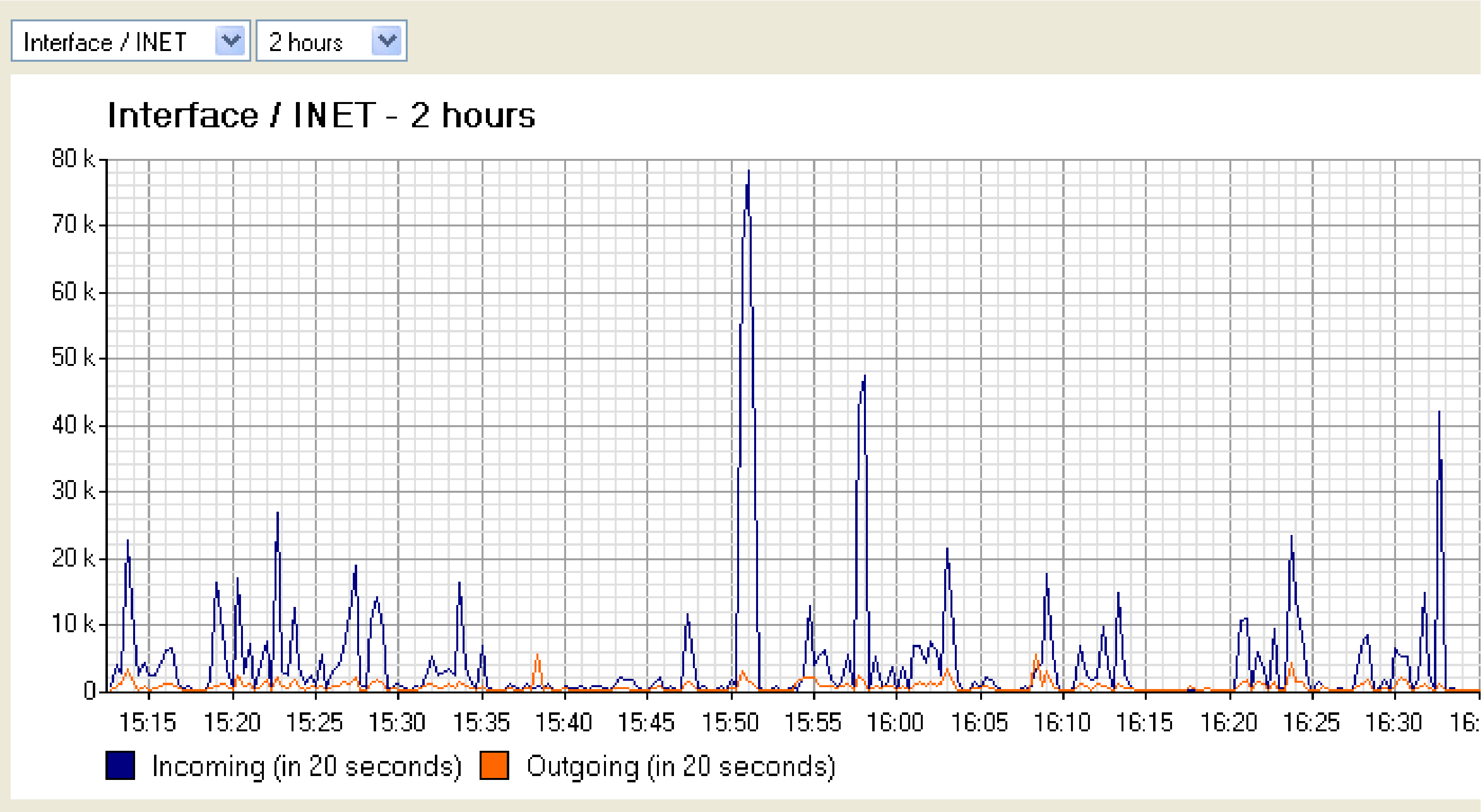
Logging

In KWF 6.1 there are twelve different logs which can be divided roughly into three categories: security events, user monitoring, and debugging.

- *alert*: reports security and administrative related events, including: Virus detection, port scans, new version availability, user quota status, connection limit exceeded, P2P detection, license status and failover activation.
- *config*: records the time and a simple description of all changes to the firewall configuration and the responsible admin.
- *connection*: if a traffic policy rule is configured to 'log connections' then each connection allowed or denied by the rule (based on the action) with be logged.
- *debug*: by right clicking in this window and selecting 'messages' there are many options which provide detailed activity of the selected KWF component. This log is useful in determining the root of a problem.
- *dial*: logs the time a RAS connection was established or disconnected.
- *error*: logs information which is useful in determining the reason for some failure in a component of the firewall.
- *filter*: logs specific details for packets meeting a traffic policy rule configured to 'log matching packets'. This log is intended for thorough analysis, whereas the connection log is recommended for monitoring user activity because it logs only the initial connection attempt, as opposed to the entire communication.
- *http*: logs all http get requests processed by the http protocol inspector.
- *security*: logs security related events generated by the content filter (e.g. detected virus).
- *sslvpn:* Reports SSL-VPN related events, such as file copy, deletion, rename...
- *warning*: logs events that could potentially cause problems in the future.
- *web*: logs in a readable and concise form each web site accessed by users through the http protocol inspector. This log is intended for monitoring purposes, whereas the http log is intended for more in depth analysis of each users' web browsing activity.

Status

For 'real time' viewing of network activity KWF includes 3 Status windows: charts, hosts, and connections. The charts display total network activity during specified time intervals. The right mouse click enables the option of saving the chart as a .png image, which can be viewed by most Internet browsers. The connections window displays all current connections both in and out of the Firewall. The right mouse button enables the option to forcibly close a selected connection or to show additional info for each connection by unlocking specific details which are not enabled by default. The hosts window displays a concise version of the connections window and only shows connections for local PCs behind the Firewall. All inbound connections can be viewed by double clicking on the IP host of a local server which has current inbound connections through the firewall. The hosts window can be used to determine the number of licenses consumed at a given time. Each unique IP address (represented by a row) counts as one license.



VPN - Virtual Private Networking

Site-to-Site tunneling

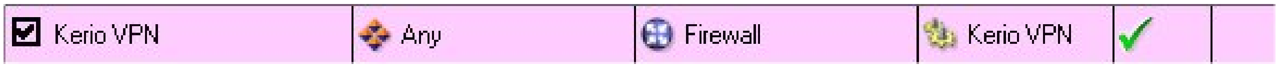
Kerio WinRoute Firewall includes a VPN server that can be used to establish secure data connections, or tunnels, to other networks behind a WinRoute Firewall. This 'tunneling' allows geographically separate computers to securely share information by encrypting the data using SSL, then encapsulating this data in lightweight UDP packets.

There is no limit to the number of WinRoute managed networks that can be connected at the same time. Site-to-Site tunneling can be implemented as a 'hub and spoke' or a 'mesh' scenario. WinRoute implements a proprietary routing protocol for the exchange of routing information. Connected WinRoute VPN servers regularly exchange their routing tables so that each WinRoute server participating in the VPN tunnel will automatically learn how to route to each network. From an administrative standpoint, there is very little setup, and no maintenance required. The drawback to this proprietary implementation is that KWF is not interoperable with other 3rd party VPN servers.

When installing WinRoute, you will by asked by Windows if you would like to allow the installation of our virtual VPN interface. This must be allowed in order to use Kerio VPN. Once installed, there will be a new Interface called 'Kerio VPN' added to the Windows 'Network Connections'. The interface will be configured to obtain its IP address automatically. This is the correct configuration, and should not be modified. It will not obtain an IP, and will use the Windows automatically assigned private IP address (APIPA).

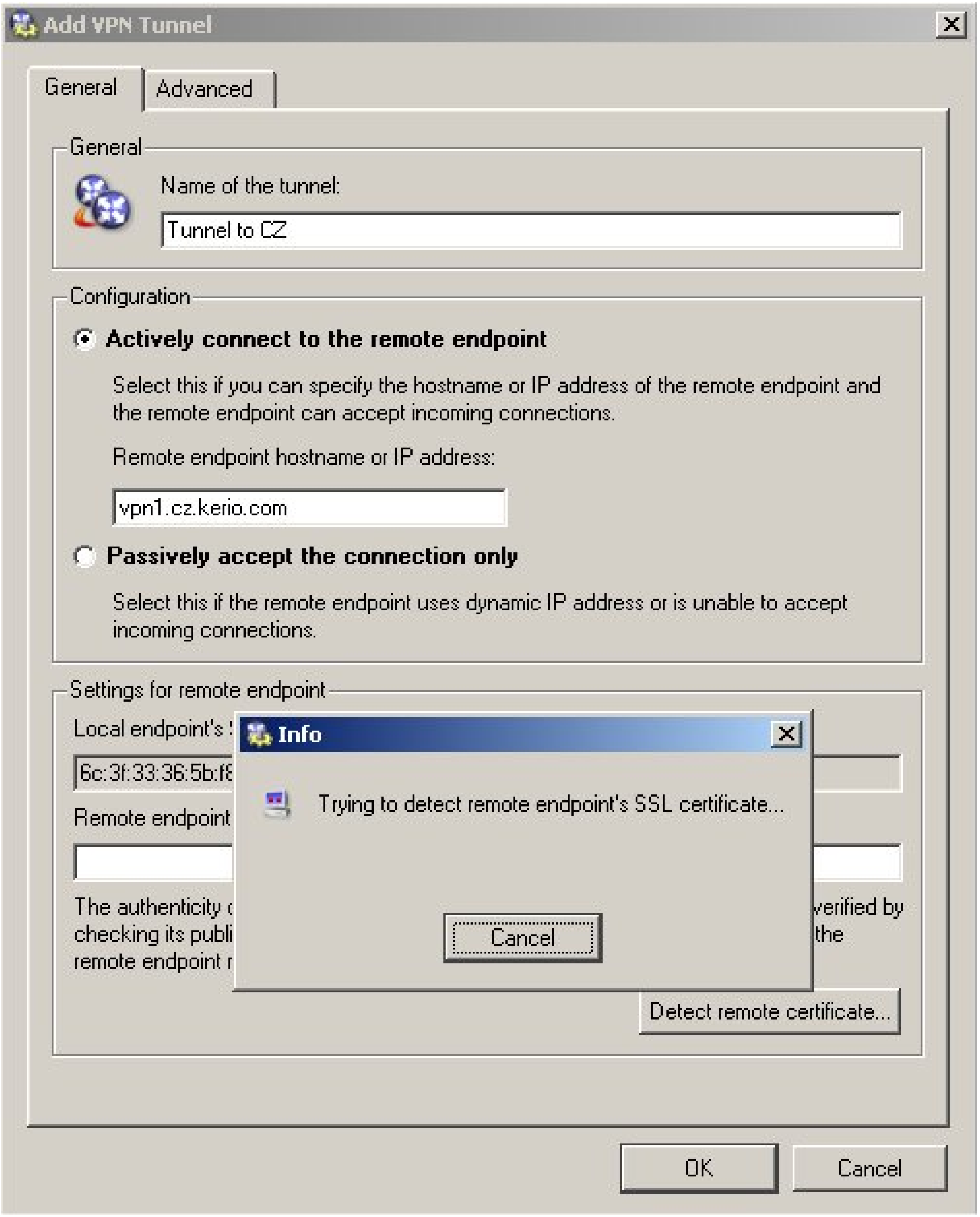
Configuration of Kerio WinRoute Firewall Site-to-Site tunneling requires 3 basic steps. The following configuration must be performed on each Kerio WinRoute Firewall that will participate in the VPN tunnel.

- Allow the Kerio VPN service: Kerio VPN protocol uses a combination of TCP and UDP port 4090. By default, there is already a service defined for the Kerio VPN protocol. It is necessary to make sure the Traffic Policy is configured to allow this service.

☑ Kerio VPN	Any	Firewall	Kerio VPN	✓	

- *Add a new tunnel:* A new tunnel is added from Configuration/Interfaces, choose 'Add -> VPN tunnel...'. All that is needed is to provide the IP or hostname of the remote endpoint, then choose the 'detect remote certificate' option.



Add VPN Tunnel

General

Name of the tunnel: Tunnel to CZ

Configuration

● Actively connect to the remote endpoint

Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.

Remote endpoint hostname or IP address: vpn1.cz.kerio.com

○ Passively accept the connection only

Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.

Settings for remote endpoint

Local endpoint's !

6c:3f:33:36:5b:f{

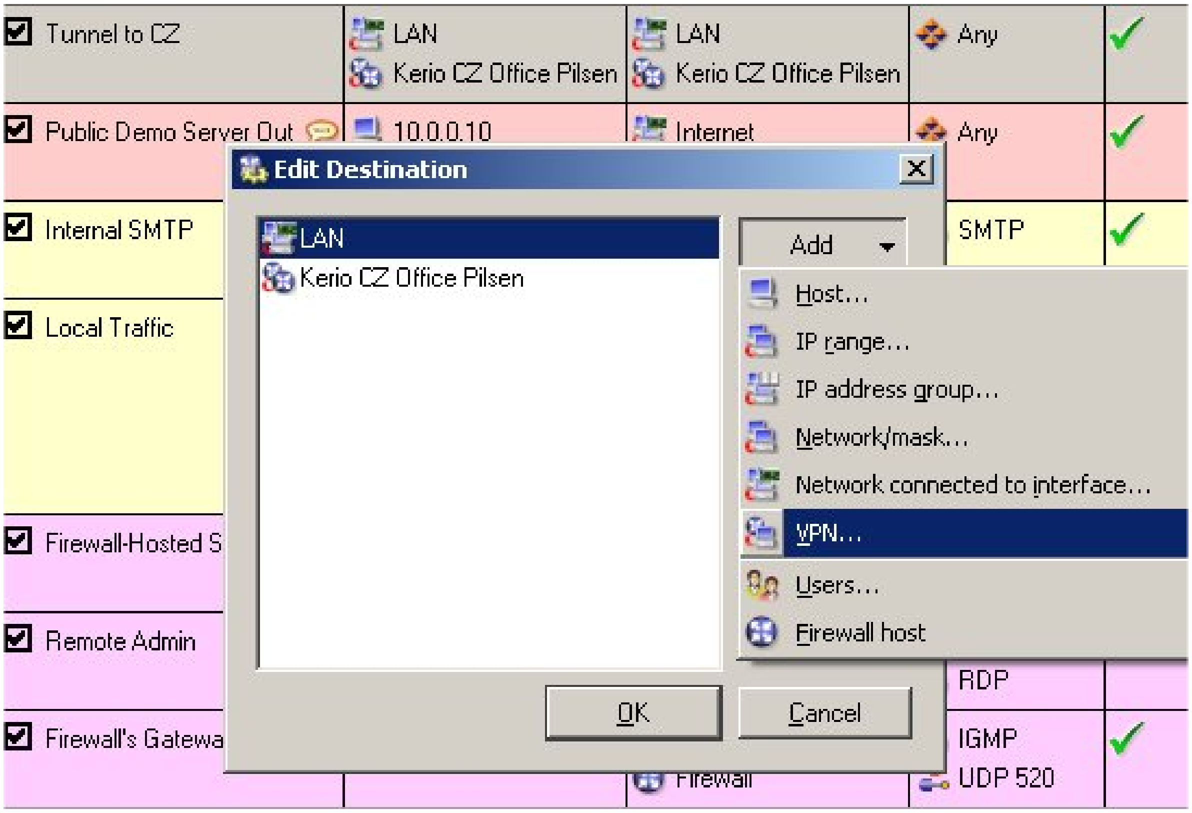
Remote endpoint

The authenticity c … verified by checking its publi … the remote endpoint r

Info

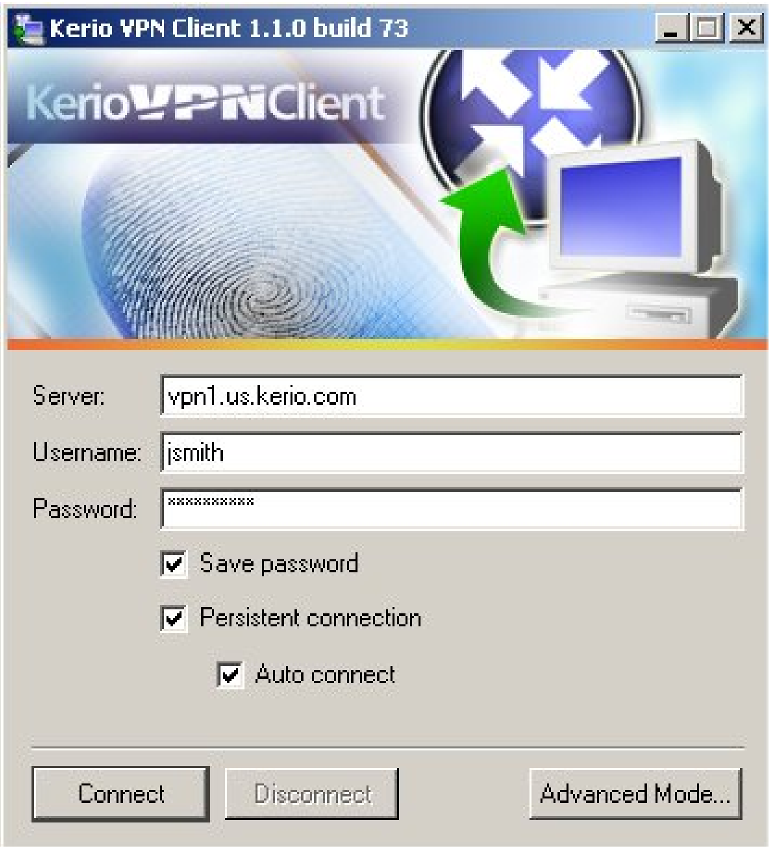
Trying to detect remote endpoint's SSL certificate...

- *Allow the VPN tunnel to access the local network:* Although the tunnel may be established, it is necessary to configure the traffic policy to allow 'tunneled' hosts to access resources on the local network. VPN Tunnels are defined as objects in the traffic policy. There should be a rule allowing any, or selected services to and from the local network and the VPN Tunnel.



VPN Client

A freely downloadable VPN client is available from the WinRoute download page. The client will install a virtual network interface in the Windows 'Network Connections'. The properties of this interface should not be modified. The Client is launched from the *Start menu* -> *Programs* -> *Kerio* -> *VPN Client*. The simple mode asks for the host name or IP address of the WinRoute firewall, and the user name and password. Once connected, the client can access resources on computers behind the WinRoute firewall, as though it is located on the same local area network.



Server: vpn1.us.kerio.com

Username: jsmith

Password: **********

☑ Save password

☑ Persistent connection

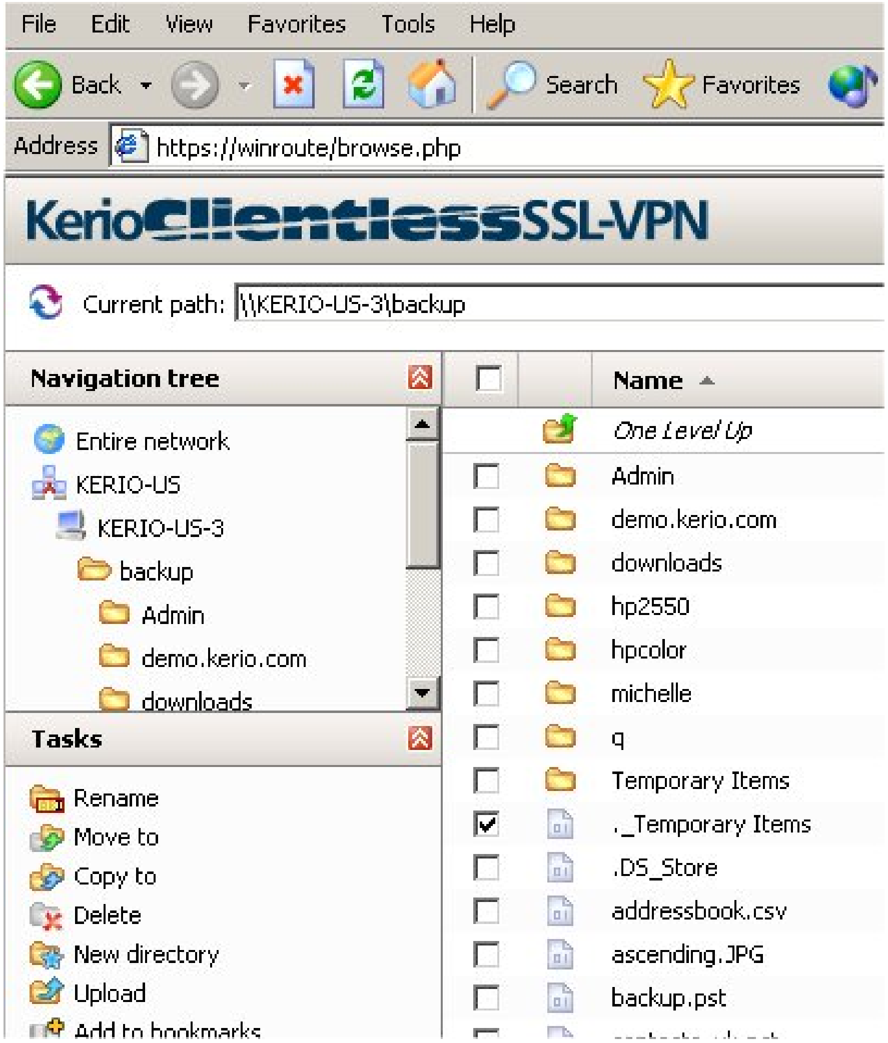
☑ Auto connect

Configuration of Kerio WinRoute Firewall Client to Server tunneling requires 3 basic steps.

- Allow the Kerio VPN service: Kerio VPN protocol uses a combination of TCP and UDP port 4090. By default, there is already a service defined for the Kerio VPN protocol. It is necessary to make sure the Traffic Policy is configured to allow this service.
- *Assign VPN dial-in rights for users:* Users must be given the right to connect using VPN. This right is defined in the properties of a user under the 'rights' tab. In this dialog, there is an option 'this user can connect using VPN', which must be enabled.
- *Allow VPN Clients to access the local network:* Although the tunnel may be established, it is necessary to configure the traffic policy to allow VPN clients to access resources on the local network. VPN Clients are defined as objects in the traffic policy. There should be a rule allowing any, or selected services to and from the local network and VPN Clients.

SSL-VPN

Although the VPN client routes all IP protocols, it does not fully accommodate Windows NetBIOS protocol. The Kerio SSL-VPN can be used with, or independently of the Kerio VPN client to work with files of remote computers using Windows NetBIOS protocol. By opening any current web browser, a user can type https://winroute.server, where 'winroute.server' represents the host name or IP address of the WinRoute computer. They will be presented with a login screen, where they must provide a valid domain account (this feature requires Active Directory). Once connected, the user will be able to browse the network behind WinRoute, and can manage files and folders which are accessible to that user based on the Active Directory policies.



Address https://winroute/browse.php

Current path: \\KERIO-US-3\backup

Entire network
KERIO-US
KERIO-US-3
backup
Admin
demo.kerio.com
downloads

	Name
	One Level Up
□	Admin
□	demo.kerio.com
□	downloads
□	hp2550
□	hpcolor
□	michelle
□	q
□	Temporary Items
☑	._Temporary Items
□	.DS_Store
□	addressbook.csv
□	ascending.JPG
□	backup.pst

Licensing

How licenses are counted

Any IP host on any LAN segment which routes traffic through KWF to the Internet will be counted towards the license. If users, independent of their location, authenticate to the firewall's web admin login page then the user's IP address will be counted. Any

VPN client will be counted towards the license. A table of all hosts occupying licenses is located under *configuration/status/hosts*. Additionally, the total licenses consumed vs. total available is located in the information dialog just above the configuration option in the left pane of the administration console.

General licensing model

The minimum licensing is for 10 users. All KWF licenses require the base license. If additional users are required then add-on packages are available in 5, 20, 100, 250, 1000. These packages can be purchased in any combination, for example a 60 user license could be purchased as: one 10 user base + two 20 user add-ons + two 5 user add-ons. In such cases it may be more cost effective however to purchase one 10 user base and one 100 user add-on.

Subscription licensing model

Subscriptions entitle the customer to current product releases, technical support, and anti-virus definitions (if applicable). When the KWF base license is purchased, the customer is entitled to one year of subscription. Subsequent annual subscriptions are purchased under the same licensing model as the original purchase, and can be purchased at any time during the current subscription period. Note that after the subscription period, KWF will continue to function.

ISS OrangeWeb Filter licensing

ISS OrangeWeb licenses are purchased separately and must be purchased in the same licensing quantities as the KWF licenses.

McAfee licensing

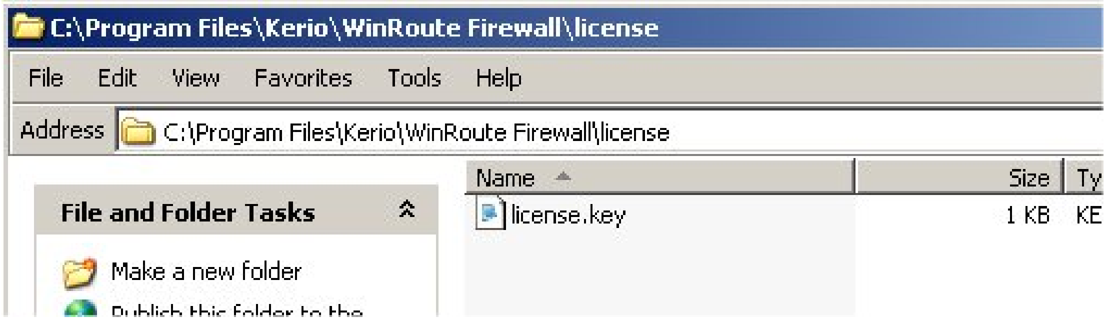
KWF + McAfee licenses are purchased together and can be purchased in the same licensing quantities as KWF without AV support.

3rd Party AV licensing

Contact sales@kerio.com for the latest pricing and user licensing options.

License Registration and Installation

After purchasing a KWF license you will receive the base key and keys for any additional components (add-ons, ISS OrangeWeb, subscriptions...). The base key is registered on the kerio website. The next page will allow you to include all additional keys. After submitting personalized information (e.g. company, name, phone, email...) you will download the certificate key file. This file should be placed in the *Kerio/Winroute firewall/license* folder, then installed through the license dialog of the administration console.



C:\Program Files\Kerio\WinRoute Firewall\license

Address C:\Program Files\Kerio\WinRoute Firewall\license

Name	Size	Ty
license.key	1 KB	KE