
KERIO TECHNOLOGIES

KERIO WINROUTE FIREWALL 6.3 REVIEWER'S GUIDE

WHO IS KERIO?

Kerio Technologies provides Internet messaging and firewall software solutions for small to medium sized networks, emphasizing the secure delivery of network data. For more information go to www.kerio.com.

Details

- Headquartered in the heart of the Silicon Valley
- First product launched in 1997, WinRoute Pro
- Incorporated as Kerio Technologies, Inc. in 2001
- Kerio WinRoute Firewall was first certified by ICSA Lab in June 2000
- Messaging product line launched with Kerio MailServer April 2002
- Network of more than 500 resellers supports customers in 74 countries with thousands of users
- Offices worldwide with presence in the UK and Czech Republic
- Self-sustaining, revenue-generated funding

Target Markets

- Small to medium-sized corporate networks
- Windows (Kerio WinRoute Firewall and Kerio MailServer)
- Macintosh and Linux platforms (Kerio MailServer)

Kerio Technologies Customers

- Transport: Wey Group couriers
- Education: McKendree College
- Non-profit: HOPES, Inc.
- Hospitality: St. Johns Park Bowling Club

Did you know?

Kerio WinRoute Firewall's proprietary SSL based VPN allows companies to configure their VPN in three scenarios: server to server, client to server, and clientless.

INTRODUCING KERIO WINROUTE FIREWALL

Kerio WinRoute Firewall is a network-based firewall that provides industry-leading security for networks of all sizes. On top of the standard router features, Kerio WinRoute Firewall also provides a VPN server, anti-virus gateway protection, surf protection, content filtering, user-specific access management, extended logging, graphical statistics and more.

WHAT'S NEW WITH VERSION 6.3?

- **Web-based Statistics and Reporting:** Kerio WinRoute Firewall 6.3 introduces new on-demand reporting using web-based diagrams to display Internet usage for specific users or the entire network. Administrators log in over a secure connection to easily access the reports and identify bandwidth bottlenecks and Internet usage abuse. The reports show how much bandwidth is being used, the top websites visited, and when combined with the optional URL filtering service, it can display the percentage of time spent browsing by categories. StaR can be accessed remotely through a browser without having to log in to the Administration Console.
- **64-bit support:** For added flexibility, Kerio WinRoute Firewall has new drivers that allow installation on either 32-bit or 64-bit Windows operating systems. Administrators may choose to install on a 64-bit Windows operating system to take advantage of larger virtual memory-address space, support for larger physical RAM, improved performance and reliability, and enhanced security of the operating system.
- **Windows Vista Compatibility:** Kerio WinRoute Firewall and Kerio VPN Client can both be installed on Windows Vista. It is the first Client/Server VPN solution to run on Microsoft's new operating system. This ensures that new PCs added to Kerio protected networks will not be denied secure remote access.
- **Enhanced Peer-to-Peer Blocking:** Nowadays, more advanced peer-to-peer (P2P) applications tunnel through well-known ports such as port 80, or encrypt data to avoid being blocked or detected. In addition to its existing P2P blocking capabilities, Kerio WinRoute Firewall adds payload analysis and improved adaptive P2P blocking that can identify and block P2P traffic more effectively than port analysis.

Kerio WinRoute Firewall uses payload analysis on all ports to detect P2P traffic on well-known and unknown ports. Then it uses the improved behavior analysis to help block encrypted P2P traffic. The behavioral analysis initially monitors and determines normal traffic behavior. As a host exhibits suspicious P2P-like behavior the security policy for the host tightens. For example, a host that is using legitimate applications will have a certain number of ports being used. But when a host launches a P2P application, multiple connections are made on various ports to search for and connect to other P2P hosts. Both P2P blocking techniques have proven to be highly effective in blocking and adapting to evolving P2P applications.

While P2P applications continue to evolve in bypassing network security measures, the potential threats and liabilities P2P networks pose are also increasing. Although P2P applications have many legitimate uses, they can overload Internet bandwidth, expose confidential data, allow malware to infiltrate the network, compromise security compliance, and impose legal liability for illegally sharing copyright material. With new and enhanced P2P blocking technologies, Kerio WinRoute Firewall adds another layer to its unified network security to provide enterprise-level protection for small to medium-sized organisations.

CORE FEATURES

1. **ICSA Labs-certified corporate firewall:** Certified since 2000, Kerio WinRoute Firewall provides targeted, thorough stateful firewall protection for small to medium-sized corporations.

2. Integrated SSL-based VPN Server and Client: Simple yet powerful one-click VPN Client for Windows is the easiest way to deploy VPN. Kerio's SSL-based VPN Client for Windows allows remote employees to have full access to company resources for all and every application - at no extra cost!

3. Surf protection: When employees spend more time browsing useless Internet sites than working, Kerio WinRoute Firewall sets them straight. With about 60 categories of web content, Kerio WinRoute Firewall can restrict which sites employees can and cannot view.

4. Anti-virus protection: With built-in McAfee Anti-Virus, Kerio WinRoute Firewall will act as an anti-virus gateway. It will scan all email (SMTP, POP3) and web (HTTP, FTP) traffic for viruses.

5. Real-time network monitoring: Administrators have real-time access to all web surfing and other activities, in order to keep a close eye on what the network is exposed to and to prevent security breaches.

HOW TO INSTALL KERIO WINROUTE FIREWALL 6.3

Kerio WinRoute Firewall 6.3 is a complex tool for connection of the local network to the Internet and protection of this network from intrusions, but it is specially designed to be easy to setup for networks with little or no IT staff.

MINIMUM SYSTEM REQUIREMENTS

- Pentium III
- 256 MB RAM
- 20 MB HDD free for installation
- Additional space for logging and cache
- Minimum of two network interfaces
- Windows 2000/XP/2003/Vista

Did you know?

Kerio WinRoute Firewall offers advanced features for experienced administrators such as content-filtering and real time network monitoring so they can accurately review (including dial-up) a user's network activities.

Quick Start

1. Run the Kerio WinRoute installer and select the "Complete" installation.

* Disable the Internet Connection Sharing (Windows 2000, XP) or Internet Connection Firewall (Windows XP sp2) services if detected by the installer, otherwise Kerio WinRoute Firewall might not function correctly.

2. Define a username and password that will be used for the administrative account.

3. You will be asked several times to confirm the installation of unsigned driver software. This is only necessary for the initial installation.

4. You might receive a warning that the Kerio VPN adapter has not passed Windows Logo testing. It is safe to ignore these warnings and click "Continue Anyways."

5. Restart your machine when the installation is completed.

6. After reboot, run the Kerio Administration Console (Start / Programs / Kerio). Connect to the localhost (the local computer) with the user name and password defined during installation. The Network Rules Wizard will be started automatically after the first login.

You are able to set the following parameters using the Wizard:

- Internet connection type — type of interface via which the firewall is connected to the Internet.

- Internet interface — select an Internet interface or appropriate dial-up. Supply the username and password for the appropriate account if the selected type is a dial-up connection.

* In case of dial-up connection, WinRoute requires a corresponding username and password. Specification of this login data is not required if the information is already saved in the operating system. If not, specify a Username and Password for a corresponding dial-up connection.

- Rules used for outgoing traffic — these rules enable access to Internet services.

- VPN Server policy — check Yes, I want to use Kerio VPN to create rules that will enable interconnection of the headquarters with branch offices as well as connections of remote clients.

- Rules for incoming traffic — for example, a mapping to an SMTP (email) server.

- Sharing of the Internet connection — network address translation (NAT) must be enabled if private IP addresses will be used within the LAN.

Additional Features:

- Proprietary SSL-based VPN server and client: Kerio WinRoute Firewall provides a proprietary VPN solution that can be applied to the server-to-server and client-to-server modes. This VPN solution can perform NAT (even multiple) at both ends.

- Email notifications: Kerio WinRoute Firewall can send email notifications informing users about various events. All sent notifications are saved in a special log file.

- Blocking of P2P networks: Kerio WinRoute Firewall can detect and block so called peer-to-peer networks (networks used for sharing of files, such as Kazaa, Direct Connect etc.).

- Statistics: Detailed statistics of the firewall interface (current speed of transmitted data, amount of data transmitted in certain time periods) as well as of individual users (amount of transmitted data, used services, categories of connected Websites, etc.) can be viewed in Kerio WinRoute Firewall.

- VoIP support: Kerio WinRoute Firewall does not interfere with a network's VoIP technology and also protects your infrastructure from unwanted VoIP activity.

SPECIALIZED TECHNICAL SUPPORT FOR REVIEWERS

Kerio Technologies offers users of its products comprehensive, easy-to-understand materials for general support as well as top-of-the-line, free of charge access to our technical support staff. These tools include:

- Manuals are included on http://www.kerio.com/supp_kwf_manual.html

- A thorough Knowledge Base on <http://support.kerio.com> which is furthered by our staff and our community of active Kerio WinRoute Firewall administrators.

- Complimentary telephone and email support for reviewers.

- Help pages are available throughout the setup process, and within the working software.

- Kerio's website is constantly updated, to reflect the latest product update information and supporting materials

FREQUENTLY ASKED QUESTIONS

1. What is the difference between Kerio WinRoute Firewall and a firewall appliance?

Kerio WinRoute Firewall is an Internet security software solution designed for small to medium-sized businesses. Because it is software, it can be updated regularly and is able to grow with an organization. Firewall appliances typically have a ceiling of users, and to upgrade, additional appliances – or “boxes” – need to be purchased. Kerio WinRoute Firewall is flexible and easier to administrate.

2. How do I know if my organization is large enough to require a corporate gateway firewall like Kerio WinRoute Firewall?

Network level protection is a necessity for networks of all sizes. With financially driven attacks on the rise, Kerio WinRoute Firewall allows administrators to control and protect all the machines inside the network.

3. Where can I download my unrestricted 30-day trial copy of Kerio WinRoute Firewall 6.3?

Kerio WinRoute Firewall 6.3 is available for download on a 30-day trial basis at http://www.kerio.com/kwf_download.html. The trial version is unrestricted due to our belief that it is vital for an administrator to have access to all features and functions of a corporate firewall product before making an informed purchasing decision.

4. What is the core market for Kerio WinRoute Firewall 6.3?

Kerio WinRoute Firewall is designed primarily for small to medium-sized networks, for corporations up to 1,000 users. Kerio WinRoute Firewall is used in a variety of different industries including education, government, technology, marketing and design.

5. What is the maximum number of users that can be managed through Kerio WinRoute Firewall 6.3?

The number of users that can be supported through Kerio WinRoute Firewall is dependent on the hardware used. The number of concurrent connections to the internet generally limits up to 1,000 nodes.

6. How long will installation take?

Installation and setup of Kerio WinRoute Firewall 6.3 by an experienced administrator should take anywhere from 30-45 minutes.

7. With the addition of clientless SSL-based VPN, will I still need to configure desktops to access our corporate VPN connections?

No – that is the benefit of clientless SSL-based VPN. In Kerio’s implementation of the technology, administrators can control, configure and manage VPN “clients” through an easy to use and access remote Web application. This Web-based application removes the need for client to client configuration, which often leaves room for error.

With an online knowledge base of process information and extended logging administrators will be more prepared for attacks and can customize the security so they can set it and forget it.

Contact:

John Wu
pr@kerio.com
+1 408 496 4500

Technical Support
<http://support.kerio.com>
+1 408 496 4500