

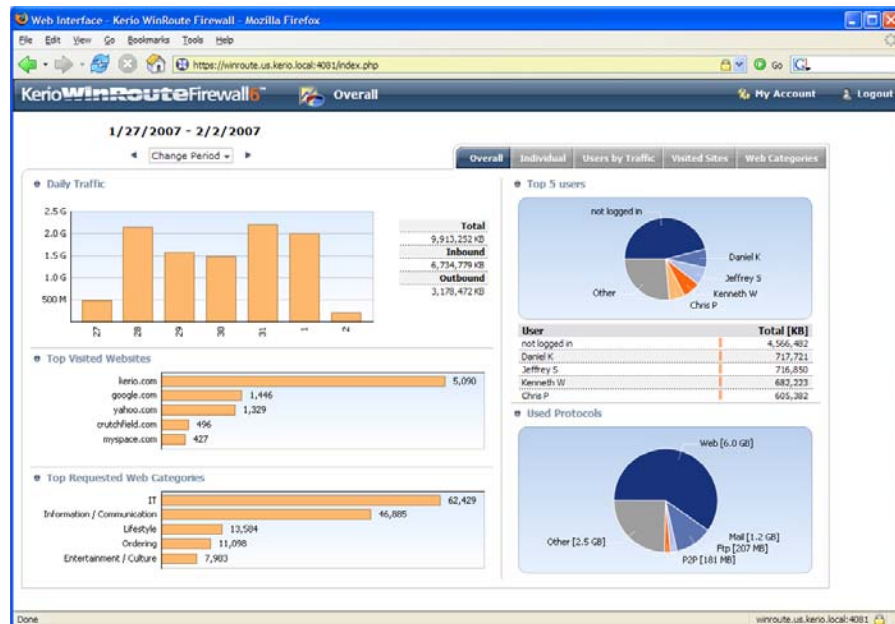


## Kerio WinRoute Firewall 6.3 – New Features

### Web-based Statistics and Reporting (StaR)

On-demand reporting of network and user activity

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.



### Now available for both 32-bit and 64-bit

Kerio WinRoute Firewall supports 64-bit Windows operating systems

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.

## **First network firewall with Windows Vista compatibility**

Windows Vista support for clients and server

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 won't be denied secure remote access.

## **Enhanced Peer-to-Peer Blocking**

Improved protection against evolving P2P networks

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 organizations.