Kerio Control Technical Specifications

Kerio Control 7

Firewall and Router

Connection tracking (SPI)
Connection Limit
Anti-Spoofing
Protocol Inspection
Traffic Rules Configuration Wizard
DHCP server
DNS Forwarder
IDS/IPS (Snort based)

- Kerio Certified IDS Signatures
- IP Blacklists
- Three severity levels

Reporting

Historical analysis
Individual, Group, Entire Network Internet Usage Reports
User based reports
Bandwidth utilization
Security
Kerio Web Filter Reports
External Logging to Syslog
Email Alerts
Web site usage
Protocol usage
Browser based activity

User Authentication

Kerberos/Active Directory
NT Domain
Web login
Proxy Server authentication (for Terminal services)
NTLM authentication

Virtual Private Networking

Split tunnel support
Windows/MacOS/Linux clients
VPN Client can run as service

User based authentication
Multiple tunnels (site to site)
Web SSL-VPN (Windows only)

NAT and traffic rules

Pre-configured services
User based traffic rules
Time based rules
NAT Mapping
Group Based rules
Dynamic DNS
MAC filtering
Blacklist in IDS/IPS
Rule Exemption Capability

Content Filtering

Time interval restriction
P2P Eliminator
URL Categories
Custom denial page
Administrative alerts
Custom URLs
Forbidden Words
FTP Policy
Proxy server
URL White-listing
Anti-Virus Filtering

- Sophos integration
- Dual scanning with plug-in

Load Balancing and QoS

Supports multiple Internet links
Policy based routing
Implicit failover
Bandwidth Limiter

Administration

Administration
Web-based administration
Multiple IP addresses on a single network interface
Customizable routing table
Variable Level Administrative Rights
Update Checker Option
Configuration Export/Import
Active Directory Integration
Local User Database
Domain Template for default user configuration
Auto Logout after Timeout
Configurable Time Ranges for groups
Multi-Language Support

- English
- Chinese (Simplified)

- Croatian
- Czech
- Dutch
- French
- German
- Hungarian
- Italian
- Japanese
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Certifications

ICSA Labs Certified – Corporate Firewall
Windows 7

System Requirements

Windows

CPU: 1 GHz
Memory: 1 GB RAM
Hard drive: 8 GB HDD space for product, logs, and StaR data
Network interface: 1 Ethernet (10/100/1000 Mb) network interface supported by the OS

Operating systems*:
Windows 7 (all editions)
Windows XP (all editions)
Windows Vista (all editions)
Windows 2000 Professional
Windows Server 2008 (all editions except Core)
Windows Server 2008 R2 (all editions except Core)
Windows Server 2003 (all editions)
Windows Server 2003 R2 (all editions)
Windows Server 2000 (all editions)
**Latest service pack and up to date security patches are required unless otherwise stated.*

Software Appliance

CPU: 500 MHz
Memory: 1 GB RAM
Hard drive: 8 GB HDD space for OS, product, logs, and StaR data
Network interface: 1 Ethernet (10/100/1000 Mb) network interface supported by the Linux kernel 2.6.30
(Majority of current NICs supported.)

VMware Virtual Appliance

CPU: 2 GHz
Memory: 1 GB RAM assigned to the virtual machine
Hard drive: 8 GB assigned HDD space for OS, product, logs, and StaR data
Network interface: 1 assigned virtual network adapter

VMware hypervisor:
VMware Workstation 6.5 or 7.0
VMware Server 1.0 or 2.0
VMware Fusion 2.0 or 3.0
VMware Player 2.5 or 3.0
VMware ESX 3.5 or 4.0
VMware ESXi 3.5 or 4.0

Kerio VPN Client

Windows
Operating systems*:
Windows 7 (all editions)
Windows XP (all editions)
Windows Vista (all editions)
Windows 2000 Professional
Windows Server 2008 (all editions except Core)
Windows Server 2008 R2 (all editions except Core)
Windows Server 2003 (all editions)
Windows Server 2003 R2 (all editions)
Windows Server 2000 (all editions)

Mac OS X
(Only Intel based Macs supported)
Operating systems:
Mac OS X 10.4 Tiger
Mac OS X 10.5 Leopard
Mac OS X 10.6 Snow Leopard

Linux
Operating Systems:
Debian 5.0
Ubuntu 8.04 to 10.04

Web Browsers

Basic User Login/Logout:
All HTTP(S)-compliant web browsers including mobile browsers are supported.

Kerio Control Administration, StaR and SSL-VPN:

Microsoft Internet Explorer 7 and 8
Firefox 3 and higher
Safari 4

Unified Security

Put a Stop to Evolving Threats.
Get Comprehensive Network Protection.

Intrusion Prevention System

- Signature based packet analysis
- IP blacklisting
- Rule management

ICSA Labs Certified Firewall

- Industry accepted standard test criteria
- Corporate level criteria - enforces default security policy immediately after installation
- Secure access remote administration - all changes to security policy are logged

Application Layer and Network Firewall

- Create inbound and outbound traffic policies.
- Protect servers without the need for a DMZ through application-friendly NAT traversal.
- Perform stateful packet and protocol inspection and logging.

Anti-virus Protection

- Filter viruses and worms from incoming and outgoing traffic.
- Simplify deployment with integrated Sophos engine.
- Dual anti-virus ready for extra protection.

Web Filter

- Block access to websites with harmful or inappropriate content
- 53 different categories of web content
- Apply categorization to traffic statistics

VPN Server

- Unlimited site to site connections

- Mac, Windows, and Linux VPN clients
- Clientless SSL-VPN for Windows networks

Anti-virus Protection

Remove Viruses, Worms, Trojans and Spyware from Incoming and Outgoing Web and E-mail Traffic.

Integrated Sophos engine

SOPHOS

Turn on the integrated Sophos anti-virus protection for

- Instant protection
- Advanced scanning technology
- Easy maintenance
- Updates as often as every hour

Third-party anti-virus plug-ins
Use other anti-virus engines with Kerio Control easily through Kerio's built-in anti-virus plug-ins.

Dual anti-virus ready
Combine Sophos with a second anti-virus engine for double the anti-virus protection.

Email Protection (SMTP & POP3)
Scan incoming and outgoing emails and attachments. Viruses found in attachments are removed and a notification is added into the email message.

Web (HTTP)
Scan web pages, downloads and all other HTTP traffic for embedded viruses and malware. Scan traffic from Kerio VPN connections as well.

File transfers (FTP)
Scan downloads and uploads through the FTP protocol.

Network Firewall and Router

Multi-Level Security and Management

Application layer firewall

- Create inbound and outbound traffic policies
- Protect servers without the need for a DMZ through application-friendly NAT traversal
- Perform stateful packet and protocol inspection on specified ports
- Log all incoming and outgoing traffic for security audits and troubleshooting
- Restrict FTP commands and file types

Integrated proxy server

- Monitor and log all web activities
- Restrict URLs, forbidden words, web objects, andweb content categories
- Increase web browsing with web caching
- Simplify network management with transparent proxy

Routing

- Manage and share Internet connections to internal systems with DHCP
- Connect VoIP and other multimedia services over the Internet
- Make smooth and easy IPsec, PPTP or RRAS connections through NAT traversal
- Integrate easily into existing infrastructures with DNS forwarding

ICSA Labs Certified
Rigorously Tested and Proven for
Trusted Security

ICSA Labs firewall certification provides security and functional testing of firewall features and continuous testing for new vulnerabilities.

Certification through ICSA reinforces credibility and resonates with all domestic and foreign requirements through the testing process.

The criteria against which vendor-submitted products are tested is an industry-accepted standard to which a consortium of firewall vendors, end-users, and the ICSA labs staff contributed.

Intrusion Detection and Prevention

Monitor inbound and outbound network communication for suspicious activity.

Protect Servers from unauthorized connections

Signature based packet analysis

At the core of its scanning technology, Kerio Control integrates a packet analyzer based on Snort. Snort is an open source IDS/IPS system that transparently scans all network communication, and provides a framework for incorporating custom rules.

Rules Database

Kerio Control implements a set of rules maintained by a community sponsored project called Emerging Threats. Each rule is digitally signed to ensure the authenticity of updates, preventing any type of tampering. The rules are based on many years of contributors from industry professionals, and are continually updated. More information is available at emergingthreats.net

Server Security

As a network based intrusion prevention service, Kerio Control protects servers behind the gateway.
IPS protects servers against vulnurability in their software that can be exploited by attacks.

IP Blacklisting

Kerio Control maintains a database of IP addresses which are explicitly denied any type of access through the firewall. The IP addresses included in this database are known to be the origin of some form of attack. The IP addresses stored locally and updated automatically.

Rule Management

- **Automatic update** IPS engine checks for updates as frequently as every hour to ensure the signature database is current.
- **Exceptions** to eliminate false positives, rules that are confirmed as non threatening can be added to a white list using an ignored signatures setting.

Security Log

The IPS engine reports blocked communication to the security log that includes the details to each event, including the rule ID for the review of signature accuracy.

Virtual Private Network Server

Connect Remote Users and Offices Securely and Easily

Comprehensive VPN server

Get comprehensive VPN options that are easy-to-use, easy-to-setup, and NAT friendly.

Site-to-site / Server-to-server

- Connect headquarters and branch office networks securely.
- No limit to number of connections for creating a virtual WAN.
- Share and access vital resources securely over the Internet.

Kerio VPN Client (Client to server)

- Connect to network printers, servers, and shared files from home, the hotel or coffee shop.
- Use your network login for VPN authentication. (Active Directory integration required).
- Use on Mac, Windows or Linux.
- Run Kerio VPN Client as a service.

Kerio Clientless SSL-VPN

- Manage folders, upload and download files from network file shares with just a web browser.
- Create bookmarks for most frequently used folders.
- Available only for Kerio Control on Windows

Simple administration

Hassle-free setup

- Wizard based configuration
- Setup the Kerio VPN Client with just the IP or domain name, username and password.

NAT-friendly

- Connect site-to-site and client-to-server VPN tunnels flawlessly behind NAT routers.
- Kerio's VPN uses standard encryption algorithms to meet versatile VPN needs: SSL for the control channel (TCP) and Blowfish for the data transport (UDP).

Flexible security

- Limit network access to individuals with Kerio Control's traffic policies.
- Scan all VPN traffic with integrated anti-virus component.

Kerio Web Filter
Strong protection against malware

Kerio Web Filter

Kerio Web Filter prevents users from visiting websites that are known to contain malicious content, including viruses, spyware, Trojans, or web pages that engage in phishing attacks or online identity theft.

An optional module for Kerio Control, Kerio Web Filter organizes sites into 53 different categories of web content. Administrators block or log access to sites based on specific content categories.

Why do you need web filtering?

Kerio Web Filter

Gateway antivirus primarily blocks known viruses. Kerio Web Filter blocks sites known to contain malware, or harmful exploits, preventing unidentified viruses from being downloaded.

It complements gateway anti-virus scanning which blocks known viruses and malware when they are transmitted through the firewall.

Liability protection

Kerio Web Filter prevents the viewing of web content that may be deemed objectionable or illicet.

Productivity tool

Log or restrict access based on:
- Group policy
- Time of day
- User status
- User location

Kerio Web Filter categorizations and statistics are viewable through Kerio StaR.

Web content categories

The following web content categories can be blocked by Kerio Web Filter:

- Adware
- Alcohol
- Anonymizer
- Art
- Business / Services
- Cars / Transportation
- Chat / IM
- Community Sites
- Compromised
- Computers & Technology
- Criminal Skills / Hacking
- Dating
- Download Sites
- Education and Reference
- Entertainment / Videos
- Finance
- Gambling
- Games
- Government
- Hate Speech
- Health
- Home / Leisure
- Humor
- Illegal Drugs
- Job Search
- Mature
- Military
- Miscellaneous
- Music
- News
- Non-profits
- Nudity
- Personal Web Pages
- Pharmacy
- Phishing / Fraud
- Politics & Law
- Pornography / Sex
- Portal Sites
- Real Estate
- Religion
- Restaurants
- Search Engines
- Shopping
- Social Networking
- Spammed
- Sports and Recreation
- Spyware & Malicious Sites
- Tobacco
- Translator
- Travel
- Violence
- Weapons
- Web-based Email

User Management

Manage Users. Monitor Behavior.
Restrict Access.

Manage

Policy based user access

- Integrate with Active Directory for simplified password management.
- Monitor and restrict Internet access based on user login.

Monitor

Kerio StaR: On-demand employee monitoring

- View and print individual Internet activity, down to the search engine keywords.
- Identify bandwidth bottlenecks and Internet abuse.

Restrict

P2P Eliminator

- Minimize liabilities and prevent data leakage and harmful downloads from peer-to-peer (P2P) networks.
- Utilize multiple technologies including port blocking, payload analysis and behavior analysis to adapt to evolving P2P applications.

P2P Eliminator

Block Peer-to-Peer Networks

What is P2P?

Peer-to-peer (P2P) networks are hosted file sharing services such as eDonkey, Gnutella and BitTorrent. The P2P networks and client applications are harmless, but play host to a large number of cyber criminals that target unsuspecting users. P2P networks are growing exponentially and are considered one of the world's top network security risks.

Eliminate P2P Vulnerabilities

- Stop identity theft from P2P-hosted spyware.
- Prevent confidential data from being shared through P2P networks.
- Minimize liabilities from objectionable or copyrighted downloads.

Apply Comprehensive P2P Protection

Just like viruses, P2P networks continue to evolve to circumvent security measures.

- Block various types of P2P networks with port blocking, payload analysis and behavior analysis.
- Arm yourself against evolving techniques such as encrypted P2P traffic tunneling through port 80.

Policy-based User Access

Manage Users More Effectively

Define access rights for individual users or groups

- Define access rights for individual users or groups
- Monitor and control Internet access with Kerio StaR and Kerio Web Filter
- Set custom bandwidth quotas and speed limits

Control access for

- Users
- Groups
- Remote VPN users
- Internal subnets

Manage access rights to

- Web content
- VPN connections
- P2P networks
- Statistics

Statistics and Reporting:
Kerio STaR

Comprehensive reports

Identify Internet abuse. Learn how users spend their time on the Internet. View:

- By total traffic volume
- By top visited website
- By Kerio WebFilter categories
- By individual user activity

Convenient and secure access

View graphical reports on-demand with a web browser and login. Supported browsers include:

- Internet Explorer
- Firefox
- Safari

Flexible reporting options

- Customize reports to a specific time range
- View data for specific network protocols
- Archive reports history
- Printer friendly pages

Quality of Service

Stop Bandwidth Abuse and
Eliminate Network Bottlenecks

Link-load balancing

- Expand network bandwidth by combining multiple Internet connections.
- Increase upload and download speeds.
- Improve the performance of high bandwidth services, such as VoIP or video conferencing.

Bandwidth limiter

- Set daily or monthly bandwidth usage quotas for individuals.
- Limit bandwidth on non-critical applications.

Connection failover

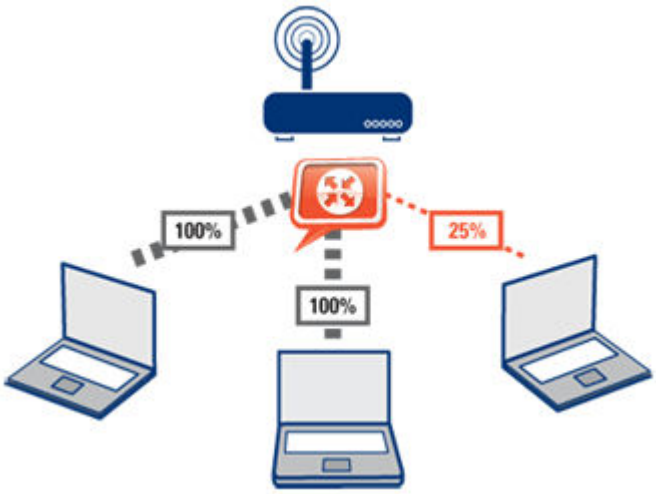
- Maintain connectivity for critical applications (email, SQL, web)
- Automatically switch to a second Internet connection in event of an Internet connection outage.

Bandwidth Limiter

Control Throughput Usage.
Optimize Internet Performance.

Control and Optimize

Fight bandwidth abuse. Preserve valuable throughput to improve the performance of business critical applications such as VoIP and video conferencing.



Limit recreational web browsing and downloads to sustain stable performance of business-critical applications.

Set limits by

- Time intervals
- Protocols
- IP addresses
- Threshold amount

Set limits on

- Downloads (kb/s)
- Uploads (kb/s)

Limit upload and download speeds for users who exceed their configured daily or monthly quotas.

Other bandwidth management tools

- Combine multiple Internet connections with link load balancing.
- Maintain Internet uptime with Internet connection failover.

Internet
Connection
Failover
No More Internet Outages.

Automatic connection failover

Keep mission critical applications and connection available.

- Use any network interface or dial-up connection as a secondary connection
- Continue to run traffic policies on failover connection

Maintain Internet uptime with active/passive or active/active failover.

Other bandwidth management tools

- Combine multiple Internet connections with link load balancing.
- Control bandwidth usage with bandwidth limiter.

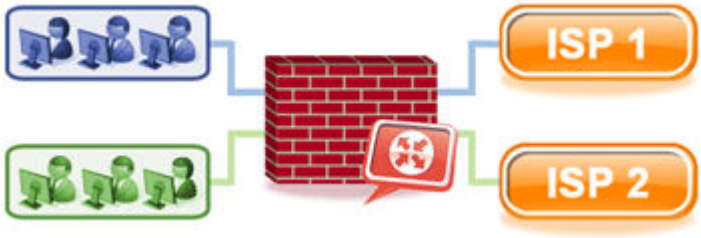
Link Load Balancing

Increase Internet Application Performance and Maintain Internet Uptime

Maximize bandwidth usage

Use multiple connections simultaneously. Maintain business-critical application performance and availability.

High Internet traffic can create bottlenecks that interrupt vital business applications.



Kerio Control's link-load balancing distributes excess load to other Internet connections to maintain high application performance.

Increase download and upload speeds

Combine several Internet connections to maximize bandwidth

Improve the quality of VoIP and video conferencing

Distribute Internet traffic across multiple connections

Prevent business interruption from Internet outage

Maintain connection uptime with automatic failover

Other bandwidth management tools

- Control bandwidth usage with bandwidth limiter.
- Maintain Internet uptime with Internet connection failover.

Virtual UTM
Build Your Own Software Appliance

Piece together your ideal solution any way you like.

Put together a firewall solution that can fit. As you grow, we grow.

Deploy on customized hardware for better efficiency and future scalability

- Choose between virtual environment or a dedicated server
- Expand/upgrade components as needed
- Available to run on a wide range of systems – desktop to server
- Flexible hardware form factor based on minimal system requirements
- Easy migration to secondary unit in event of hardware failure

Integrated hardened OS

- No exploitable/vulnerable system services
- No conflicting applications
- Easy to install and deploy
- Optimized for performance

Kerio Control Software Appliance

- Kerio Control combined with a hardened a 32-bit Operating System based on Linux Kernel 2.6
- Burnable ISO image
- CD/DVD to standard hardware devices

Kerio Control VMware Virtual Appliance

- Run multiple appliances on the same hardware
- 32-bit Operating System based on Linux Kernel 2.6
- Easy management through VMware tools
- Add multiple virtual network adapters

- Move the firewall to another server in minutes
- Add network adapters without touching the hardware
- Available as OVF or VMX format
- Add security to the existing network without adding hardware
- Download the Kerio Control VMware Virtual Appliance