

ePrism™ Datasheet

Product Overview

Total Email Perimeter Defense

ePrism™ Enterprise is an Email Security Firewall that provides organizations with a total email perimeter defense solution. ePrism delivers a unique combination of email security, spam protection, anti-virus and content control in an easy-to-use, high-performance appliance. Designed to be deployed between internal email servers and the Internet, ePrism supports standard email protocols and features a complete set of email filtering and security capabilities specifically designed to protect against the full spectrum of email threats.



Highlights

- Stops Viruses and Worms at the Perimeter**
 ePrism offers Kaspersky Labs Antivirus®, which adds an additional level of security. This means fewer security risks, no business disruptions and lower overall cost.
- Provides Multiple Spam Protection**
 Multiple filtering technologies are employed to ensure accuracy and improve coverage. Administrators spend less time building filters and more time on important new projects. Employees don't waste time sifting through unwanted email.
- Maintains Message Integrity**
 ePrism protects you from 350 email threats including malformed messages so that only properly formatted messages get through. This protects your email server, email clients and improves virus-scanning effectiveness.

Features

Provides Content Filtering

ePrism filters content based on rules that are set by your organization. You filter content attempting to come into your organization and also content going out. This allows management to protect businesses by filtering confidential emails as well as increasing security and worker productivity.

ePrism Protects Against the Five Threats to Email

Email Threat	Consequences	ePrism Solution
Spam	Clogs inboxes, compromises network resources, nuisance factor	ePrism uses a variety of methods: White/Blacklists, RBL, DCC, Bayesian statistical analysis
Viruses	Most are sent via email. Malicious viruses can bring down your network	Viruses are stopped at the perimeter by Kaspersky Labs award-winning Antivirus.
Malformed Messages	Spammers and hackers use malformed messages to flood servers with Denial of Service attacks that can interrupt important business communication	Detects and blocks attacks at the perimeter.
Unauthorized Access	Illegal access to your email is a major threat to your firm. Encrypted email needs to be processed easily.	ePrism accepts and initiates your SSL/TLS Sessions.
Acceptable Use Content	Employees, partners and others violate your organization's Acceptable Use Policy introducing legal liability due to offensive, confidential and other unwanted content	ePrism lets you apply attachment controls. You can specify content controls and enforce your organization's email Acceptable Usage Policy.

Features
(CONTINUED)



Spam Protection

ePrism is designed to minimize administrative overhead and false positives, while maximizing spam detection. ePrism attacks spam with a multi-pronged defense that includes, White/Blacklists, Realtime Blackhole Lists (RBL), Distributed Checksum Clearinghouse (DCC) and Bayesian statistical analysis.

Virus Protection

Since the most common way to infect a network is through email, virus scanning is an important component of reliable email protection. ePrism includes Kaspersky Labs Antivirus®, recent winner of the coveted Best Anti Virus Solution award at the annual SC Magazine Global Awards. Automatic hourly updates to this virus-scanning engine ensure that the latest viruses are being identified and eradicated before they reach your host.

Malformed Message Protection

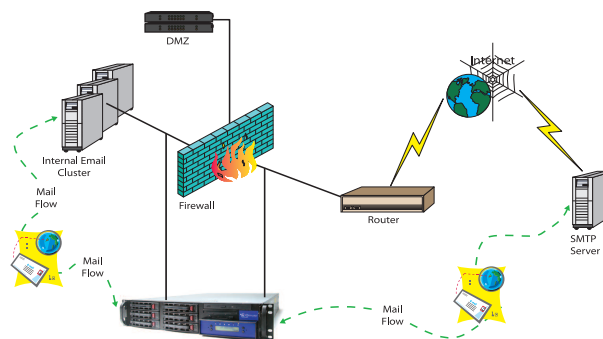
Malformed messages can allow viruses to avoid detection, crash your systems and lock up your mail servers. There are hundreds of ways to create malformed messages, but ePrism ensures that only correctly formatted messages are allowed into your systems.

High Performance Appliance

The ePrism appliance is manufactured to the highest standards of workmanship. Its hardened and optimized O/S makes it invulnerable to attacks. ePrism is designed to support the highest data throughputs thus minimizing the latency usually associated with intense security processing. In addition, ePrism is certified under Common Criteria EAL4+, a designation which increases the level of independent assurance that the product is well designed and engineered to offer the highest level of security.

Comprehensive Management

ePrism is managed through a simple Web-based interface and may be accessed remotely and locally. Sessions may be encrypted for added security. ePrism is easy to manage and offers a full range of tools to monitor and troubleshoot your mail delivery. Comprehensive logs record all mail activity.



ePrism Enterprise Hardware Specifications

M1000

- Stateful Failover Available
- Mini-1U Format
- P4 2GHz
- 256MB RAM
- 40 GB HD
- 2-10/100 fpx Ethernet NICs
- 511 BTU/hr @ 150 watt

M2000

- Stateful Failover Available
- 1U Format
- Xeon 2.4GHz
- 512MB RAM
- 2-40GB HD/RAID 1
- 3-10/100/1000 em0 Ethernet NICs
- LCD Display
- 2,185 BTU/hr @ 400 watt

M3000

- Stateful Failover Available
- 2U Format
- Xeon 2.4GHz
- 1GB RAM
- 4-36GB HD/SCSI/RAID 10
- 4-10/100/1000 em0 Ethernet NICs
- Redundant Power Supplies
- LCD Display
- 2,185 BTU/hr @ 400 watt

Note: Specifications subject to change without notice.

CORPORATE ADDRESS

15015 Avenue of Science
San Diego, CA 92128

MAIN PHONE: 858-676-2277
TOLL FREE: 800-782-3762
FAX: 858-676-2299
EMAIL: info@stbernard.com
WEB: www.stbernard.com

EUROPEAN ADDRESS

Unit 4, Riverside Way
Watchmoor Park, Camberley,
Surrey GU15 3YQ, United Kingdom

PHONE: +44 (0) 1276-401640
FAX: +44 (0) 1276-684479
EMAIL: info@uk.stbernard.com

© 2005 St. Bernard Software, Inc. All rights reserved. The St. Bernard Software logo, Open File Manager, SecurityEXPERT and ePrism are trademarks of St. Bernard Software Inc. UpdateEXPERT and iPrism are registered trademark of St. Bernard Software Inc. All other trademarks and registered trademarks are hereby acknowledged.