TECHNOLOGY

Overview

IRONPORT

Virus Defense Technology

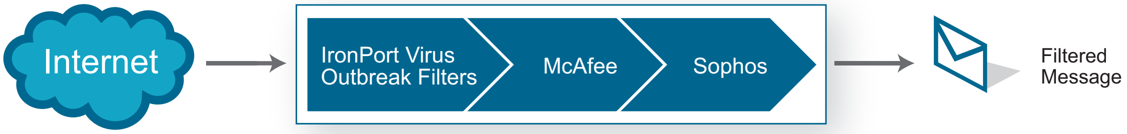
THE MOST COMPREHENSIVE MULTI-SCAN, MULTI-VENDOR ANTI-VIRUS SOLUTION.

OVERVIEW

The scale and complexity of recent virus attacks have highlighted the importance of a robust, secure messaging platform to protect your network perimeter. The traditional approach of being able to identify and block known viruses is no longer enough.

To combat this evolving threat, IronPort® offers the most comprehensive multi-scan, multi-vendor anti-virus solution:

- IronPort Virus Outbreak Filters™ – a critical first layer of preventive defense against new outbreaks, detecting and stopping viruses before any other technology.
- Integrated McAfee and Sophos anti-virus engines – enabling multiple traditional virus detection methods to ensure protection against even the most complex virus attacks.



Maximum Virus Protection: Proprietary IronPort technology and virus filtering from McAfee and Sophos.

FEATURES

With the highest performance virus detection and scanning technologies in the industry, anti-virus technologies from IronPort, McAfee and Sophos provide fully integrated layers of virus protection on the *IronPort C-Series*™ and *IronPort X-Series*™ email security appliances.

VIRUS OUTBREAK PREVENTION AND PROTECTION

During any virus outbreak, there is invariably a period of time between virus detection and when the actual anti-virus identity file is deployed. During this period, administrators can utilize *IronPort Virus Outbreak Filters* technology to identify and quarantine viruses based on known patterns and delete or archive the messages until new identity files can be updated. This innovative preventive anti-virus solution is fully integrated with anti-virus engines from both McAfee and Sophos and has the ability to rescan messages automatically when new signature updates are available during an outbreak.

MULTIPLE DETECTION METHODS: PROTECTION AGAINST THE WIDEST VARIETY OF VIRUSES

During the scanning process, the McAfee and Sophos anti-virus engines both analyze each incoming message and file, identify the type and then apply the relevant technique to ensure highest efficacy and throughput. The McAfee and Sophos anti-virus engines employ multiple detection methods, such as:

FEATURES
(CONTINUED)

Pattern Matching detects viruses and other potentially unwanted software by specific code sequences known to be present within a virus. The patterns are created to ensure that the engine catches not only the original virus but derivatives within the same virus family. In doing so, McAfee and Sophos approach viruses in a complementary fashion. McAfee's scanning engine starts from a known place in a file, then searching for a virus signature. Often, they must search only a small part of a file to determine that the file is free from viruses. Conversely, Sophos' scanning engine searches for multiple short code sequences in tandem to detect virus signatures.

Advanced emulation technology is used to detect encrypted and polymorphic viruses. If either engine suspects that a file contains a virus, it creates an artificial environment in which the virus can run harmlessly until it decodes itself and its true form becomes visible. The engine then identifies the virus by scanning for a virus signature. The robust engine supports multiple scanning modes to optimize performance.

Heuristic analysis is utilized by both engines to ensure that variants of viruses are caught with minimal information available about virus code patterns. Heuristic analysis is based on the fact that programs, documents or email messages that carry a virus often have distinctive features. They might attempt unprompted modification of files, invoke mail clients, or use other means to replicate themselves. The engines analyze the program code to detect these kinds of computer instructions. The engines also search for legitimate non-virus-like behavior before taking anti-virus action to avoid raising false alarms.

MULTIPLE OPTIONS FOR VIRUS HANDLING

Administrators have multiple options to handle virus infected messages. As viruses evolve, new strains of attacks try to bypass anti-virus protection by concealing viruses within password protected, encrypted files or malformed messages. The IronPort solution detects potentially dangerous messages, giving the administrator full control over how these messages should be handled by the system.

The fully integrated Virus Quarantine provides additional options to customers to determine what actions to take on viral messages along with end-user notification options.

SCALABLE GATEWAY WITH BEST-OF-BREED INTEGRATED ANTI-VIRUS DEFENSE

The unparalleled performance of IronPort's email security appliances enables the scalability required for fully integrated anti-virus protection for continued message growth. The anti-virus solution likewise protects your infrastructure from being overwhelmed by complex virus outbreaks and ensures that your mission critical email will continue to be accepted.

BENEFITS

Highest Efficacy By combining *IronPort Virus Outbreak Filters* with anti-virus technology from McAfee and Sophos, IronPort appliances provide industry-leading virus prevention and protection, while maintaining near zero false-positive rates. By integrating multiple independent solutions, IronPort appliances leverage the efficacy of each to provide maximum security.

Scalable Virus Protection The unparalleled performance of the IronPort appliances ensures the scalability required for fully integrated anti-virus protection for continued message growth. Performing virus filtering at the gateway significantly reduces the resources needed at the groupware servers and the bandwidth requirements within the network.

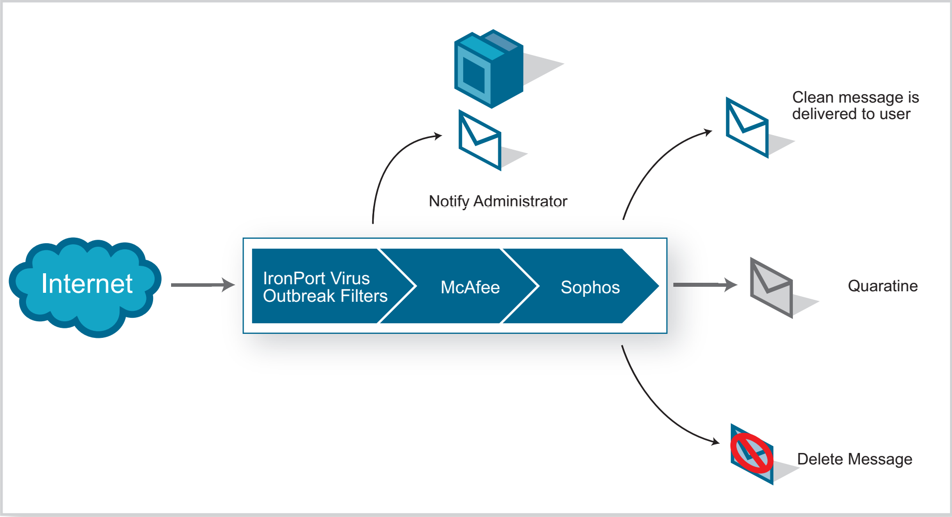
BENEFITS (CONTINUED)

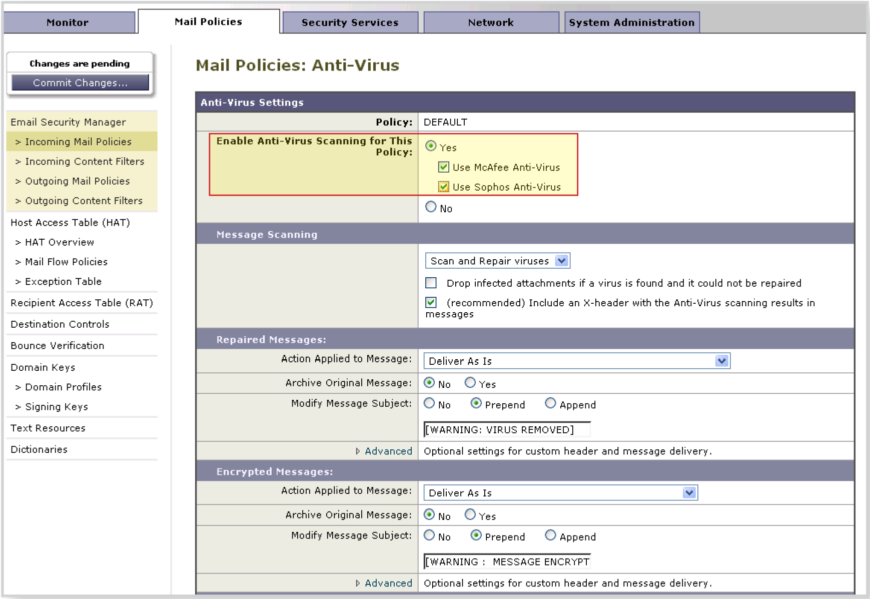
Lower TCO with an Integrated Gateway Solution With integrated management and deployment within the appliances, the solution offers ease of management with automatic updates and "set and forget" policies to address any customer specific requirements.

Additionally, performing virus filtering at the gateway significantly reduces the resources needed at the groupware servers and the bandwidth requirements within the network.

FIGURE 1. FLEXIBLE AND INTUITIVE INTERFACE FOR EASE OF MANAGEMENT

IronPort email security appliances provide multiple layers of defense against potential viruses.


Notify Administrator
Clean message is delivered to user
Internet
IronPort Virus Outbreak Filters
McAfee
Sophos
Quaratine
Delete Message



Mail Policies: Anti-Virus

Anti-Virus Settings

Policy: DEFAULT

Enable Anti-Virus Scanning for This Policy: ● Yes
☑ Use McAfee Anti-Virus
☑ Use Sophos Anti-Virus
○ No

Message Scanning

Scan and Repair viruses
☐ Drop infected attachments if a virus is found and it could not be repaired
☑ (recommended) Include an X-header with the Anti-Virus scanning results in messages

Repaired Messages:

Action Applied to Message: Deliver As Is
Archive Original Message: ● No ○ Yes
Modify Message Subject: ○ No ● Prepend ○ Append
[WARNING: VIRUS REMOVED]
Advanced Optional settings for custom header and message delivery.

Encrypted Messages:

Action Applied to Message: Deliver As Is
Archive Original Message: ● No ○ Yes
Modify Message Subject: ○ No ● Prepend ○ Append
[WARNING : MESSAGE ENCRYPT
Advanced Optional settings for custom header and message delivery.

SUMMARY

MULTI-SCAN, MULTI-VENDOR SECURITY WITH IRONPORT

With the growth in number and complexity of viruses, it is critical that customers protect their networks with solutions that provide coverage against the widest variety of virus threats.

IronPort's anti-virus offerings (IronPort Virus Outbreak Filters, McAfee Anti-Virus and Sophos Anti-Virus) provide a multi-layered, multi-vendor approach to virus filtering – by offering a high performance virus scanning solution, integrated at the gateway.

With IronPort's proprietary AsyncOS™ operating system, the IronPort C-Series and IronPort X-Series email security appliances can process hundreds of messages per second. Whereas, traditional MTAs can only handle 10 to 20 messages per second. The unparalleled performance of IronPort's email security appliances protects your email infrastructure from being overwhelmed by large-scale virus outbreaks and ensures that your mission critical email will continue to be accepted.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

IronPort sales representatives, channel partners, and support engineers are ready to help you evaluate how IronPort products can make your email infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from IronPort's industry leading products, please call 650-989-6530 or visit us on the Web at www.ironport.com/leader

VIRUS DEFENSE
04/08
DOC RELEASE

IRONPORT®

IronPort Systems
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

P/N 435-0226-2 4/08

IronPort is now part of Cisco.

CISCO.