

IRONPORT SECURITY MODULES

RONPORT (FRONPORT (FRONPOR

Sophos Anti-Virus

OVERVIEW

The speed and variety of recent virus attacks has highlighted the importance of a robust, secure messaging platform to protect your network perimeter. Being able to simply identify and block known viruses is no longer enough, as today's attacks can easily overwhelm most email gateways with a sudden spike in message volume, creating a denial of service (DoS) situation. IronPort[®] offers integrated virus filtering at the gateway through Sophos. The Sophos engine scans messages for viruses based on a variety of characteristics, performing scanning operations on generic data sources, irrespective of type. The engine has specialized technology for loading and searching data which enables it to achieve the highest scanning speeds in the industry.

FEATURES

With the highest performance virus scanning technology in the industry and unique denial of service prevention, Sophos anti-virus technology is a fully integrated layer of virus protection on the *IronPort C-Series*TM email security appliances.

MULTIPLE DETECTION METHODS: PROTECTION AGAINST THE WIDEST VARIETY OF VIRUSES

During the scanning process, the Sophos AV engine analyzes each incoming message and file, identifies the type and then applies the relevant technique to ensure highest throughput and efficacy. The Sophos AV engine employs multiple detection methods, such as:

Pattern Matching can identify a virus by a specific code sequence or for code sequences known to be present within a virus. In doing so, the patterns are created to ensure that the engine catches not only the original virus but derivatives within the same virus family.

Advanced emulation technology is also included to detect polymorphic viruses and an online decompressor for scanning multi-layer attachments. The robust engine supports multiple scanning modes to optimize performance.

Heuristic techniques are utilized by the engine to ensure that variants of viruses are caught with minimal information available about virus code patterns.

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 files or mal-formed messages. The IronPort solution detects potentially dangerous messages, giving the administrator full control over how these messages are handled by the system.

FEATURES (CONTINUED)

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

Unparalleled performance of the *IronPort C-Series* appliance protects your email infrastructure from being overwhelmed by large-scale virus outbreaks and ensures that your mission critical email will continue to be accepted.

ONLY SIGNATURE-BASED GATEWAY AV SOLUTION INTEGRATED WITH A PREVENTIVE AV SOLUTION

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 AV solution is fully integrated with the Sophos AV engine and has the ability to rescan messages automatically when there are new signature updates during an outbreak.

BENEFITS

IronPort and Sophos - Better Together

IronPort combines Sophos' anti-virus technology with *IronPort Virus Outbreak Filters* – resulting in even better virus prevention and protection, while maintaining the extremely low false-positive rate.



Highest Efficacy Sophos is widely regarded within the industry as having the fastest performing and most accurate virus scanner available. Recently Sophos was awarded the VB 100% award in the June 2005 edition of Virus Bulletin. This is the 28th time Sophos Anti-Virus has won a VB 100% award, confirming its position as one of the most powerful and accurate virus protection products available.

Virus Bulletin tested 28 different anti-virus products for their detection rates, lack of false alarms, and speed of scanning. Sophos successfully detected all of the in the wild, macro and polymorphic viruses (100 percent detection rate) with no false alarms.

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.

Sophos Anti-Virus

FIGURE 1. The IronPort C-Series with Sophos anti-virus provides two layers of Clean message is delivered to user Notify Administrator defense against potential viruses. Internet Modify subject line of infected messages IronPort C-Series Messaging Gateway Appliance with Anti-Virus Scanning Drop infected attachment Delete Message

1Dv7 12x10			Lines Har	t charlie.nin Log Dut
I) IRONPORT C600			Login nos	HHD
Menitor	Mail Policies Security Services	Network	System Administration	
No changes are pending	Mail Policies: Anti-Virus			
	Anti-Virus Settings			20
Crisil Securits Nanager	Policy	DEFAULT		
- Incoming Hail Paluaes	Enable Anti-Virus Scanning for This Policy:	Tres C No.		
 Outgoing Nail Policies Outgoing Content Filters 	Consume Rooming			
Host Access Table (HAT)	Scan and Repair viruses			
> HAT Overview				
		Crop infected attachments	if a virus is found and it could	id not be repaired
> Mail Flow Policies > Exception Table		Drop infected attachments (recommended) Include en in messages		
 Mail Flow Policies Exception Table 	Personal Pressage -	F (recommended) Include en		
> Mail flow Policies > Exception Table Reopient Access Table (RAT)	Action Applied to Message	(recommended) Include an in messages	X-header with the Ario-Viro	
> Mail flow Policies > Exception Table Reopient Access Table (RAT)	Contraction of the Party of the Owner of the Party of the	(recommended) Include an in messages	X-header with the Ario-Viro	as scenting results
> Mail Flow Policies > Ecception Table Recipient Access Table (RAT) Domain Keys	Action Applied to Message:	(recommended) Include en in messages [Deliver As Is	X-header with the Ario-Viro	as scenting results
> Mail How Policies > Exception Table Recipient Access Table (RAT) Domain Kess > Domain Profiles > Signing Keys	Action Applied to Message: Anthive Original Message:	R (recommended) Include an in massages Defiver As IS Ro. C Yes C No. ← Prepared C Age	X-header with the Ario-Viro	as scenting results
> Mail How Palcies > Exception Table Recipient Access Table (KAT) Domain Keys > Domain Profiles > Sgning Keys Text Resources	Action Applied to Message: Anthive Original Message:	(recommended) Include an in massages [Deriver As Is	X-header with the Ario-Viro	as scenting results
 Mail Now Palcora Exception Table Receiver Access Table (KAT) Domain Kress Domain Fredies Signing Keys Test Resources 	Action Applied to MeriAgo: Archive Original Message Modify Message Subject	(recommended) Include an in massages (Deriver As II (Ao. C Yes (Ao. C Yes (Ao. C Yes (Ao. C Yes (MARING: YIRUS ARMOVED) (MARING: YIRUS ARMOVED) (scheader with the Arit-Vie and	as searching results
 Mail Now Palcora Exception Table Receiver Access Table (KAT) Domain Kress Domain Fredies Signing Keys Test Resources 	Action Applied to MeriAgo: Archive Original Message Modify Message Subject	(recommended) Include an in massages (Deriver As Is (Ao. C Yes (Ao. C Yes (Ao. C Yes (Ao. C Yes (MARKINS; VIRUS REMOVED) (MARKINS; VIRUS REMOVED) (scheader with the Arit-Vie and	as searching results
 Mail How Policies Exception Table Receptent Access Table (RAT) Domain Kess Domain Profiles 	Action Applied to Mersage: Anthree Organial Message: Modely Message Subject: Send Nonfristron Message: 4 Advanced	P (reconnected) to table an in message (Deriver As to P No. Crvs C No. Crvs C No. Crvs C No. Crvs C No. Crvs C no isoter C -to isoter C -to isoter C -to isoter C -to isoter C -to isoter C -to isoter	scheader with the Arit-Vie and	as searching results

FLEXIBLE AND INTUITIVE INTERFACE FOR EASE OF MANAGEMENT

SUMMARY MULTI-LAYERED SECURITY WITH IRONPORT AND SOPHOS

With over 90,000 known viruses in the wild and with several hundred in circulation at any one time, it is critical that customers protect their networks with solutions that provide coverage against the widest variety of virus threats.

IronPort's anti-virus offering (Sophos AV) provides a multi-layered, multi-vendor approach to virus filtering – by offering a high performance virus scanning solution integrated within the gateway.

The *IronPort C-Series* email security appliance, with its proprietary *AsyncOS*[™] operating system, can process up to 140 messages per second and sustain up to 10,000 concurrent SMTP sessions. Traditional MTAs can only handle 10 to 20 messages per second and hundreds of concurrent sessions. The unparalleled performance of the *IronPort C-Series* appliance 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



IronPort Systems, Inc.

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

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use, and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.



Copyright © 2006 IronPort Systems, Inc. All rights reserved. IronPort and SenderBase are registered trademarks of IronPort Systems, Inc. All other trademarks are the property of IronPort Systems, Inc. or their respective owners. Specifications are subject to change without notice. P/N 435-0205-1 4/06