



ANTI SPAM SOLUTIONS TECHNOLOGY REPORT

Sophos ES4000 Email Security Appliance



JANUARY 2007



www.westcoastlabs.org

CONTENTS

Sophos ES4000 Email Security Appliance **SOPHOS**

Sophos Plc, The Pentagon, Abingdon Science Park, Abingdon OX14 3YP, United Kingdom
Tel: +44 (0)1235 559933 • Fax: +44 (0)1235 559935 • www.sophos.com

Introduction3

Test Network4

Test Methodology5

Product Testing Reporting6

Checkmark Certification7

The Product8

Test Report9

Test Results15

West Coast Labs Conclusion16

Security Features Buyers Guide17



INTRODUCTION



As the war for corporate inboxes intensifies, and unmonitored emails disrupt effective and secure working practices, Anti-Spam solutions continue to evolve to deal with this menace.

In this, the second Anti-Spam Technology Report, we examine the functionality and performance of the leading products in this market, which are aimed specifically at the SME network environments.

A key objective of the testing is to replicate the installation, configuration and use of the solutions in a real-world business environment to enable readers of the White Paper – prospective buyers – to make a meaningful assessment of the product that is right for protecting their corporate email environment.

Test Engineers have evaluated how the solutions install to ensure timely and effective spam protection. Consideration has also been given to the level of security administrator expertise and technical support required to facilitate both out-of-the-box operation and thereafter product training to ensure maximum effective spam protection.

This reports provides an independent assessment of effectiveness with regard to:

- The features and functionality of the solution.
- Integration into a network infrastructure.
- The level of user administration required to operate the product effectively.
- Spam detection capability and rates of detection.

TEST NETWORK

WCL has a number of domains that collect genuine spam. These domains receive varying levels of spam and are consistent with different email environments.

To reflect the email usage within a corporate environment, within each domain are a number of designated user accounts with a variety of email practices and needs including some that are subscribed to a variety of newsgroups and mailing lists. Some user accounts actively contribute to mailing lists.

The multiple domains designated for testing purposes were those that, between them, receive spam at a level consistent with the defined requirements of testing.

Software solutions included in the test program were installed on servers that meet the minimum specifications required by the vendor. Appliance-based solutions were installed on the network according to the vendor's recommended placing.

For hosted services, WCL testes through identified email domains and changed the MX records to divert the mail stream through the hosted service.

TEST METHODOLOGY



WCL initially performed the testing with an “out-of-the-box” configuration, changing only those settings on the solution needed to ensure correct operation in line with the vendor’s recommended installation and configuration procedures.

Further testing was then performed following the vendor’s advice for the tuning or training of the solution under test. WCL fine-tuned the solution each day of the test, spending no more than half an hour per day undertaking such work.

Throughout the course of testing, a mixture of email was sent to the test domains from other email addresses and domains controlled by WCL to mirror genuine email activity common in business, for example, requesting meetings, sending notifications to groups and non-business related social emails.

Emails were also sent from web-based accounts such as Hotmail and Google’s Gmail in order to simulate external users sending non-business related social emails, and home workers.

Thus, during the testing period the domains received some spam, some list/newsgroup mailings and “genuine” individual emails.

PRODUCT TEST REPORTING

Product evaluation addresses three specific areas* - Management/Administration, Functionality, Performance plus Additional Feature Testing.

1. MANAGEMENT/ADMINISTRATION

- Ease of Setup/Installation
- Ease of Use
- Logging and reporting function
- Rule creation
- Customization
- Content Categories

2. FUNCTIONALITY

- Email Processing Steps
- Allow/Blocking of Email
- Quarantine Area
- Additional functionality reporting
- Steps to Process Email
- Block Email Addresses
- Blacklist/Whitelist
- Allow Email Addresses

3. PERFORMANCE

- Volume or Percentage of spam detected
- False positive rate
- Spam incorrectly passed through
- Legitimate mail blocked
- Legitimate subscription mail blocked

CHECKMARK CERTIFICATION

Upon completion of the testing, individual product results are analyzed, resulting in accreditation to one of the two Checkmark Certifications for Anti-Spam subject to achieving the following catch rates:-

- Checkmark Anti-Spam Certification - Premium - 97% and over Catch Rate.
- Checkmark Anti-Spam Certification - Standard - 90% and over Catch Rate.



THE PRODUCT



SOPHOS ES4000 EMAIL SECURITY APPLIANCE

The ES4000 Email Security Appliance is designed for organizations with up to 2 million messages per day, seeking a high-availability, high-capacity, low-administration managed appliance for protection against all inbound and outbound email-borne threats.

www.sophos.com/es4000

SOPHOS SAYS ABOUT THE PRODUCT'S BUSINESS BENEFITS...

The ES4000 is built to deliver superior protection at the email gateway, offering the administrator better insight and control over email traffic while greatly reducing the amount of day-to-day maintenance and interaction. Built on Sophos' innovative Managed Appliance platform, the ES4000 uses extensive task automation and remote monitoring and support by Sophos to provide more dependable, easier to use email gateway security. The ES4000 offers comprehensive protection, simple web-based management and proactive, accessible customer support.

www.sophos.com/es4000

SOPHOS SAYS ABOUT THE PRODUCT'S TECHNICAL BENEFITS...

The ES4000 is capable of handling more than 2 million messages a day, using advanced filtering techniques such as reputation filtering, and Genotype™ technology to provide proactive protection against known and unknown threats. An extensive array of onboard sensors monitors system health and performance, and triggers alerts to the administrator and to Sophos only when intervention is required. The ES4000 appliance fits seamlessly into any network infrastructure, and includes dual disk drives and power supplies for built-in redundancy. It also features an onboard quarantine for high-capacity storage of suspicious messages that doesn't require an additional server or management console.

www.sophos.com/es4000

TEST REPORT



INTRODUCTION

The ES4000 Email Security Appliance offers email protection to Enterprise level organizations. While the primary goal of this report is to evaluate the performance of spam protection, it should be noted that the ES4000 also provides protection from other email-borne threats such as viruses, phishing, and spyware.

The device itself is fully rack mountable, requiring 1U of rack space. For added protection and performance the ES4000 appliance hosts a specialist hardened operating system running on two Intel Xeon processors. Thanks to the high system specification, SOPHOS describes ES4000 as being capable of handling up to 80,000 messages per hour.

TEST REPORT

INSTALLATION AND CONFIGURATION

The ES4000 appliance is received with the operating system and management software preinstalled, reducing setup time. The only action required of the administrator before starting configuration is the entry of a license key which is sent to the registered user at time of purchase.

The license key is entered via the login page of a secured web interface on a non-standard port, which is used to control every aspect of the appliance. Upon activation, the administrator may then log in and begin configuring the appliance, using a simple and time-saving configuration wizard. The wizard prompts the administrator to enter all vital networking information, such as network addresses and domain names.

Further configuration is available in the setup of user groups. The administrator may create groups and manually populate them with user accounts, or lists of users may be imported straight from Active Directory. The latter option will save a vast amount of time for larger companies with thousands of employees.

Once configuration is complete, the ES4000 appliance provides the administrator with a Post-Configuration Checklist. This list contains a set of four tasks that may improve the functionality of ES4000 but could be overlooked during setup. Alongside each of the tasks is a description of the benefits associated with performing them. These are: Active Directory Setup, End User Preferences, Outbound Mail Host/Proxy, and Trusted Relays.



TEST REPORT

INTERFACE

When logging into the ES4000 appliance, the administrator is presented with a neat and tidy interface utilizing both graphics and text. The menu system is easily navigated and each available option is carefully explained to the user. Online help is also provided via the web interface; all the information contained here is descriptive and does a good job of aiding the administrator in both configuration and day-to-day use.

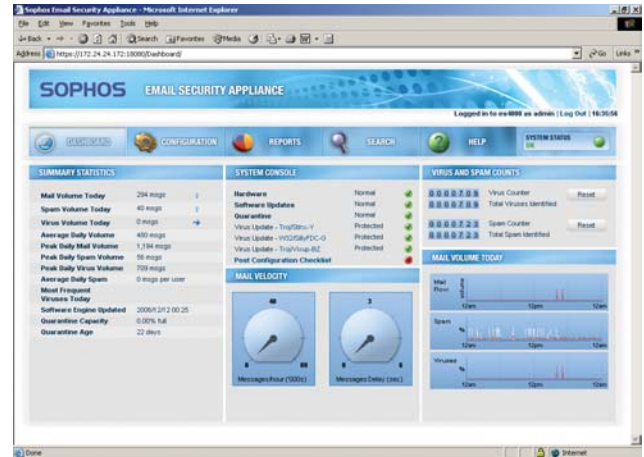
Each time the administrator logs in, he or she is presented with the Dashboard. This provides a summary of the system performance and includes information on the number of emails, with a breakdown of spam and viruses received. Data is also displayed in a series of three bar charts split into the categories of Spam, Viruses, and Mail Flow.

One of the most interesting readouts supplied by the Dashboard is Mail Velocity. This is split into two graphs, both resembling car speedometers. The first meter displays the number of messages per hour being processed by ES4000, while the second displays the delay of each message. Using these an administrator can easily assess the current performance of the system.

The Dashboard can be viewed at anytime using its tab at the top of the interface. Alongside the Dashboard are tabs for Configuration, Reports, Search, and Help. Spam rules, and other settings such as network, domain, and antivirus, may be altered through the Configuration menu. Search allows the administrator to look for specific messages within the logs, quarantine, and message queue, while Help provides access to a fully searchable internal help file.

One of the time-saving features within the Configuration tab is a Quick Tasks menu. This provides access to four option categories that are often used in a variety of security solutions: check for software updates, manage administrator accounts, manage policy rules, and manage user preferences. Having these options readily available cuts back on the time spent performing day-to-day operations on the appliance.

Once fully configured, the ES4000 immediately begins providing antispam protection to the corporate network. When dealing with messages defined by the appliance as spam, the administrator is presented with the choice of several actions. By default the appliance tags all spam messages with a spam warning in the subject line. However the administrator may also choose to quarantine or block the message. The settings are easily altered and are applied with immediate effect.

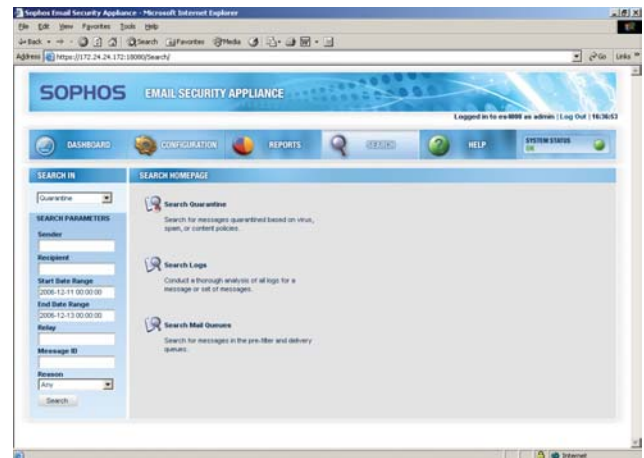


TEST REPORT

One technology offering protection to the client organization is Genotype. This forms part of the Host Intrusion Prevention System (HIPS), which provides early detection against spam and viruses, allowing the ES4000 appliance to offer further protection against families of viruses and spam campaigns.

An important feature of the ES4000 appliance is the Quarantine service, which may be configured to automatically backup quarantined messages once disk space passes a given level. The appliance also provides services such as message forensics and message tracking.

To ensure that this protection is constantly up to date all upgrades are downloaded automatically; however the administrator is free to perform them manually. Prompt notifications inform the administrator of any available patches or updates.



TEST REPORT

REPORTING

Reports may be viewed from within the web interface and can be generated to meet the demands of various intended recipients. For example, executive level reports may be generated to convey the general status of mail traffic to non-technical managers, and others to include the more technical information for system administrators. This level of customization will allow an administrator to present the appropriate data to all interested parties.

These reports may be generated using various categories from within the Reports tab on the web interface. There is also a highly informative Homepage that is initially displayed to the administrator after clicking on the Reports tab. This includes data on mail volumes, virus alerts, and performance information. This page, like the rest of the Reports section, makes good use of both tables and charts to portray collected information.

Also available from within Reports are four further report categories: mail trends, performance, senders, and policy analysis. Each of these contains a subset of options, allowing in-depth analysis to be performed.

Options available under the Mail Trends section allows an administrator to view data on traffic volumes and message actions, while Performance includes information regarding areas of network and processing efficiency. The Senders category allows the administrator to view the IP addresses of servers responsible for sending spam and virus-infected messages, along with those whose connection attempts have been blocked. The final category is Policy Analysis. From here the Administrator is presented with a breakdown of detected messages, including spam, viruses, and those messages where content was deemed offensive.



TEST REPORT

These reports may be generated to show data covering anywhere between the current day and the previous year. Also available are options to select to view the data for inbound or outbound traffic and to view any graphical data as either line or bar charts. The administrator may then choose to save the data in .CSV format for further analysis, or print a hardcopy using the available print function. The latter option opens a popup window containing just the relevant data without any options or menu bar, allowing for a clutter-free hardcopy.

TEST RESULTS

<u>Type of mail</u>	<u>Detected as genuine</u>	<u>Detected as SPAM</u>
GENUINE	100%	0%
SPAM	3%	97%

The ES4000 Email Security Appliance from Sophos performed well, delivering 100% of the genuine mail correctly and correctly classifying 97% of the spam mail.

It is also worth noting that the ES4000 delivers a good proportion of grey and list mail as genuine. This gives an organization the flexibility and opportunity to define policies during a training period without missing mail that could potentially be business-critical.

West Coast Labs is pleased to award the ES4000 Email Security Appliance the Premium Anti-Spam Checkmark.



WEST COAST LABS CONCLUSION

As an Enterprise level solution, the ES4000 Email Security Appliance performs very well and offers comprehensive email protection. The high hardware specification of the appliance, coupled with the well integrated operating system, ensures that ES4000 provides an organization with efficient antispam protection.

The interface is clearly laid out and provides plenty of information to the administrator when making configuration changes. The wide array of option categories available allows the ES4000 appliance to be configured to meet a variety of security protection demands.

This attention to detail continues when using the Reports function. Through the use of graphical and text-based reporting tools, ES4000 provides a clear picture of processed mail.

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose.

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. When West Coast Labs provide test results for any particular product tested, said results are most relevant at the time of testing and within the context of the specific scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools utilized during that specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

SECURITY FEATURES BUYERS GUIDE

DEVELOPMENTS IN THE PRODUCT OVER THE LAST 12 MONTHS AS STATED BY SOPHOS...

Reputation filtering - the ability to drop connections from known spammer IP ranges at the MTA (Mail Transfer Agent) level prior to scanning - has become a powerful weapon in the fight against spam. Sophos reputation filtering technology can identify as much as 80% of inbound spam this way, dramatically increasing catch rates and improving message throughput without the need for added infrastructure investments.

Sophos has introduced highly-effective weapons to combat the recent rise in image-based spam. These include 'fingerprinting' technology using image metadata (size, color map, compression ratio, etc.), and DNS hostname validation techniques that detect transient, dynamic hostnames, trademarks of spam botnets. Both of these techniques have significantly bolstered our ability to protect our customers from this emerging spam trend.

Another recent innovation by Sophos is Behavioral Genotype™ technology, a unique HIPS defense mechanism that identifies malicious executable code before it has a chance to install and run. In less than 2 months, Sophos has detected more than 17,000 variations of malicious code using this technology. This complements our traditional Genotype technology that provides proactive protection from variants of known spam campaigns. Genotype protection plays a vital role in advance protection, eliminating zero-day threats and blocking spam campaigns before they emerge.

Sophos continues to invest in our lab capabilities in order to extend the power of these and other tools, and to develop new weapons in the fight against spam, viruses and other network security threats.

ADDITIONAL NOTEWORTHY SECURITY FEATURES

- Integrated anti-virus protection includes Virus outbreak protection to block viruses sent from botnets & other hijacked systems
- Message content scanning for keywords, strings and common expressions
- True File Type attachment identification and control
- Threat definition updates every 5 minutes
- Hardened FreeBSD operating system resists hacking attempts

SECURITY FEATURES BUYERS GUIDE

NOTEWORTHY RELIABILITY AND SUPPORT IMPROVEMENT FEATURES:

- Built on the Sophos Managed Appliance platform for proactive support, remote “heartbeat” monitoring and reduced administration
- On-demand remote assistance using reverse SSH connection (no need to open firewalls)
- Hot-swappable power supplies and disk drives ensure availability and easy maintenance.
- Active/Passive failover for greater availability (effective Jan. 2007)
- Advance replacement warranty for up to three years (depends on valid subscription)
- 24/7/365 technical support included with every subscription at no extra cost

NOTEWORTHY ADMINISTRATION AND SELF-MANAGEMENT FEATURES:

- “3-clicks-to-anywhere” management console for quick navigation and easy management
- Message forensics quickly and accurately traces messages in logs & quarantine
- Powerful Dashboard provides instant access to all core performance indicators, including mail volumes and trends, threat counters, software and hardware status, and more
- Actionable, predictive reporting, provides deep insight into mail activity, throughput, performance and capacity trends to help diagnoses mail network issues
- End-user quarantine access via email digest or web-based real-time interface
- Automatic software updates ensure continuity of security
- Self-managing quarantine, logs and configuration backups maintain onboard storage capacity

DEPLOYMENT SIMPLIFICATION FEATURES:

- Configuration wizard for simple installation and setup
- Automatic Microsoft Active Directory discovery & synchronization