

SOPHOS

 email **security and data protection**

Reviewer's Guide

Models: ES1000, ES5000 and ES8000



WELCOME

Welcome to the reviewer's guide for Sophos Email Appliances. The guide is structured to reflect a typical day in the life of an email system administrator. It provides a review of the core functionalities of our Email Appliances, highlighting their effectiveness and ease of use. After reading the guide, you will have a deeper understanding of how our Email Appliances deliver the most reliable and intelligent email gateway security available.

The ES1000, ES5000 and ES8000 are part of Sophos Email Security and Data Protection which includes managed email appliances and software protection for Exchange, UNIX and Domino servers at the gateway and groupware levels. Every Sophos email solution provides unique integration of anti-virus, anti-spam, anti-phishing and data leakage prevention capabilities to secure and control email content.

Like all our solutions, Sophos Email Appliances are the product of more than 20 years' experience protecting business, education, and government. They are powered by the combined in-house anti-virus, anti-spyware and anti-spam expertise of SophosLabs™ – our global network of threat analysis centers. Pre-emptive detection and protection from ever-more complex and fast-spreading security threats is one of the reasons that Sophos is acclaimed for delivering the highest level of customer satisfaction and protection in the industry.

All our licenses include comprehensive 24-hour support from our worldwide network of support engineers, available at no additional cost, every day of the year.

Email Security and Data Protection is available separately or can be incorporated in a single Sophos Security and Data Protection license along with Web Security and Control, Endpoint Security and Data Protection and Sophos NAC Advanced. For information on pricing and availability of all our products, please contact your local Sophos representative. To find out who serves your area, please visit:

www.sophos.com/products/howtobuy

If you would like to evaluate a Sophos Email Appliance, please fill out our online request form at:

www.sophos.com/free-trials

CONTENTS

1 INTRODUCTION	6
Management highlights	7
Core features and benefits	8
2 PRODUCT FUNCTIONALITY	9
Software architecture	9
Data leakage protection	15
3 SETUP	17
Configuration	17
Directory Services setup	17
End-user preferences	18
Policies	19
4 MANAGING THE APPLIANCES	25
Status checks	25
Updates	26
Backups	27
Quarantine	27
End-to-end message search	28
End-user options	30
5 REPORTING	32
Dashboard reports	32
Reports page	33
Detailed reporting	34
6 SUPPORT	36
The Managed Appliance	36
Warranty	38
24/7 Sophos support	38
APPENDIX	
I Default policy settings	39
II Hardware specifications	40

1: INTRODUCTION

Sophos Email Appliances are secure email gateway solutions providing integrated protection against spam, malware, phishing and data leakage via email. They are built on the concept of the Managed Appliance – combining the control and visibility of an appliance with the simplicity and ease of use of a managed service. The ES1000, ES5000 and ES8000 models are built on robust hardware platforms, delivering high-capacity, high-availability security for enterprise email networks.

Efficient email protection

Sophos Email Appliances provide maximum protection for your email with minimum administrative effort.

Capacities:

ES1000 – processes up to 50,000 messages an hour

ES5000 – processes up to 380,000 messages an hour

ES8000 – processes up to 550,000 messages an hour

Components include:

Advanced threat detection technology: Award-winning scanning technology is powered by SophosLabs – our global network of threat detection and analysis centers. Automated tuning constantly balances a range of detection techniques, adapting to evolving threats and preventing protection failures.

Sender Genotype watches for characteristic botnet behavior at the connection level, preventing spammers from sending email even before their reputation has been established. New threat definitions and anti-spam rules are automatically downloaded every few minutes, ensuring the most up-to-date protection available. SXL technology narrows the gap between detection and protection even further, by making the latest intelligence from SophosLabs available online in realtime, rather than waiting for the next update.

Data leakage prevention: Sophos Email Appliances include powerful tools to help guard against the loss of confidential information and maintain regulatory compliance. Using a simple step-by-step wizard, you can quickly and easily create customized rules to monitor message bodies and attachments for keywords, file types, size, and other attributes, for both inbound and outbound mail. TLS encryption provides additional protection by encrypting outbound messages so that only intended recipients can read them. If more granular encryption policies are required, Sophos Email Appliances integrate easily with any third-party system.

Monitoring and alerting: All Sophos appliances feature built-in monitoring and alerting for quicker issue resolution and greater peace of mind. More than 40 different settings and conditions are constantly monitored for peak performance. Alerts are sent to the system administrator and to Sophos, so that corrective action can take place as quickly as possible. If further assistance is required, administrators can also take advantage of on-demand remote assistance and let Sophos troubleshoot the appliance directly.

Management console: Managing these powerful technologies is easy, thanks to an intuitive web-based management console that simplifies administrative tasks and provides better insight and control over the email infrastructure. The easy-to-navigate ‘three clicks to anywhere’ console provides instant access to relevant, actionable information so that administrators can make informed decisions about system performance and future capacity requirements.

Management highlights

Sophos Email Appliances offer features that simplify email management:

- A fully web-based “three clicks to anywhere” management console
- Configurable policies for managing viruses, spam, message content and attachments
- TLS encryption and custom certificate support for secure access to the management console and to the end-user web interface
- End-to-end message forensics with access to quarantine, mail logs, and mail queue
- One-click clustering of up to 10 appliances
- Integration with Microsoft Active Directory® and other LDAP systems for easy setup, policy enforcement, and authentication
- Email digest or web interface for end-user quarantine self-management
- Global and per-user allow lists and block lists
- Built-in hardware and software maintenance and alerting
- Proactive “heartbeat” monitoring
- On-demand remote assistance
- Two-unit active/passive failover clustering.

Award-winning protection

The excellence of Sophos security is regularly recognized by a wide variety of independent test bodies, including the ICSA, West Coast Labs, Veritest, eVision IT Labs, av-test.org and leading industry publications such as IT PRO and SC Magazine.

Core features and benefits

Core feature	Core benefit
Platform-independent	Easily fits into any existing email infrastructure
Unrivaled spam and malware detection	Fully integrated and award-winning anti-spam and anti-malware powered by SophosLabs
Genotype proactive protection	Blocks up to 90% of new threats without specific signatures
Behavioral Genotype Protection	Pre-runtime intrusion prevention to detects and block malicious code before it can execute
Data leakage prevention	Provides powerful content scanning controls and TLS encryption to protect against confidential information leakage
Sender Genotype service	Blocks up to 90% of spam at the connection level through reputation filtering and proactive botnet detection.
SXL real-time anti-spam protection	SXL real-time access to the latest anti-spam intelligence from SophosLabs catches short duration spam campaigns
High accuracy	Detects more than 99% of spam and protects against email scams, including phishing attacks. Delivers consistent accuracy with negligible false positives
High availability	Ensures continuous uptime with redundant, hot-swappable hard drives and power supplies (not ES1000)
High capacity	Provides maximum processing and storage capacity in a compact 1U rack-mounted design
Regulatory compliance	Incorporates a configurable policy environment to support corporate or regulatory compliance requirements
Encryption-enabled	Includes TLS encryption for enhanced security
Multilingual protection	Protects organizations from spam and viruses in multiple language message streams
Automatic updating	Ensures up-to-date protection with automatic updates from SophosLabs – a global network of threat analysis centers
End-user controls	Offloads administrative burden by providing end-user quarantine management, allow lists, and block lists
Comprehensive support	Includes unlimited 24-hour telephone, email, and online support, 365 days a year

2: PRODUCT FUNCTIONALITY

Overview

Sophos ES1000, ES5000 and ES8000 Email Appliances are plug-and-protect email gateway security solutions. They fit easily into any network configuration, and since both have a self-contained operating system, you do not need any knowledge of UNIX, Linux, Solaris, or other server platform language.

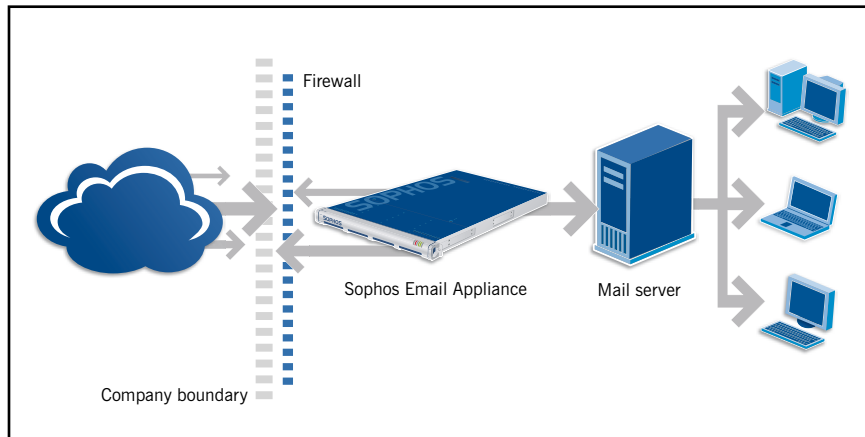


Figure 1: Typical installation of a Sophos Email Appliance

As gateway appliances, they are typically installed in the DMZ – the neutral zone inside the network firewall and upstream from the mail server(s).

This section outlines the software architecture of the appliances, and provides a review of their internal email security and regulatory compliance policy.

Software architecture

The onboard software comprises five major elements:

- 1 Hardened FreeBSD operating system
- 2 High-performance email filtering system
 - Postfix MTA (Mail Transfer Agent)
 - Anti-spam engine
 - Anti-virus engine
 - Sender Genotype advanced connection control
 - Policy engine
- 3 Management console and dashboard
- 4 Onboard quarantine
- 5 Monitoring, alerting, and notification system.

Hardened FreeBSD operating system

Sophos Email Appliances are built on a hardened FreeBSD operating system, optimized for the hardware platform and for the embedded Sophos software. FreeBSD is extremely stable and reliable, and offers tremendous speed and performance for network security appliances. Refer to Appendix II for complete hardware specifications.

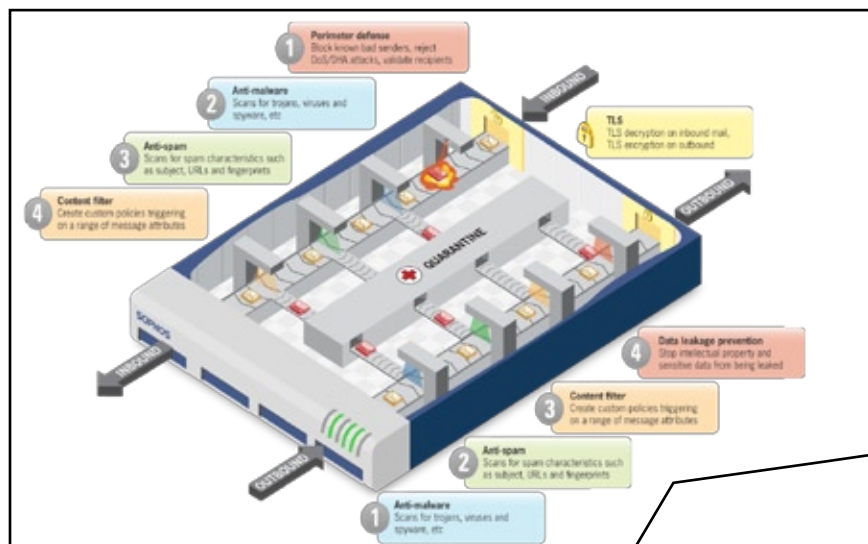


Figure 2: The Sophos Email Appliance scans inbound and outbound messages

High-performance email filtering system

The email filtering system performs the following tasks:

Inbound email traffic:

- The built-in MTA intercepts inbound messages at the email gateway
- Messages and attachments are scanned for spam, viruses, and other conditions as defined by the filtering policy
- Defined tests and actions are applied to the messages
- Messages are routed for delivery to the intended recipient or to the quarantine for review, or discarded.

Outbound email traffic:

- Messages are routed from internal mail servers to the appliance
- Messages and attachments are scanned for viruses and other conditions as defined by the filtering policy
- Defined tests and actions are applied to the messages
- Messages are relayed to the built-in MTA for external delivery, or to the quarantine for review.

During initial setup, administrators can choose to enable the recommended default message policies and actions, including TLS encryption for outbound messages. Using the web-based management console, defaults can be modified at any time, and customized tests and actions can be set up. (See *Policies* in section 3 for details).

Note

Sophos Email Appliances will never deliver an inbound or outbound message containing a known virus, or allow it to be released from the quarantine.

Message delivery options include:

Inbound and outbound (unless specified):

- Continue processing
- Deliver immediately
- Quarantine
- Quarantine and continue
- Quarantine, drop attachment(s) and continue
- Tag subject and continue
- Discard
- Reject (outbound only)
- Redirect
- Add banner
- Add/replace header
- Notify
- Re-route
- Copy.

Management console and dashboard

The management console is the secure, web-based graphical user interface between the system administrator and the appliance, enabling you to:

- Configure system and network settings
- Create a cluster of up to 10 appliances, or add a new appliance to an existing cluster
- Configure and manage the anti-spam, anti-virus, and content policies
- Monitor system status and diagnose interruptions
- Manage the quarantine
- Search the message logs, queue, and quarantine to trace “lost” messages
- Generate real-time reports
- Delegate some administrative tasks and control end-user interface capabilities
- Set up and administer two-unit failover configuration.

Three clicks to anywhere

Built on a strict discipline of minimal navigation, every feature of the management console is no more than three clicks away, and command-line access is *never* required.



Figure 3: Management console dashboard

The dashboard, the console’s home page shown in Figure 3, provides an at-a-glance summary of overall system performance. From the dashboard, the administrator can determine protection status, check mail flow and volume, and ensure system availability. More details on the appliances’ powerful yet easy-to-use management tools can be found in Section 4.

Clustering

Multiple appliances can be clustered together for scalability, availability, and simplicity of management.

Scalability: Clustering enables an administrator to quickly and easily add appliances to handle increasing amounts of email traffic at the gateway, without any additional administrative overhead.

Availability: Clustering provides redundancy in mail processing. The failure of a single appliance will not affect the flow of email through the other appliances in the cluster. In addition, FTP configuration back-up, directory services synchronization and end-user quarantines in a cluster will continue to function even if one appliance fails.

Simplicity of management: Centralized management of all appliances within a cluster allows administrators to view the dashboard, reports, quarantine, log, and queue information across the cluster as if they are one larger appliance. (Each appliance can also be viewed individually.) End-user functions, such as email quarantine summaries and end-user web quarantine access, function the same as they would in a single appliance environment.

Quarantine

The quarantine provides safe storage of unwanted or potentially dangerous inbound and outbound messages. Any message that violates a security policy (e.g. virus, spam, keyword, or content match) can be routed to the quarantine for review by the system administrator, and optionally to the message recipient (inbound) or to the originator (outbound). The reviewer can then choose to release or discard the quarantined message, with the exception of messages containing viruses.

Onboard storage

The onboard quarantine is a high-capacity message store capable of handling millions of messages. Unlike many competitive solutions, the quarantine is maintained on the appliance itself, and not on another server. This offers the dual benefit of eliminating both the need for additional off-box storage, and the need for an additional quarantine management system and interface. Administrators access the quarantine using the same management console that is used to manage all other system functions.

Delegated management

Administrators can also create dedicated Help Desk accounts to delegate quarantine management to other system administrators without exposing the full range of system configuration options. Help Desk administrators can then handle all the internal inquiries about lost or missing messages, freeing up the senior administrator to focus on other priorities.

The administrator can allow intended recipients of inbound email and originators of outbound email to view quarantined messages either through an email digest or through a web interface. In both cases, only their own personal messages can be viewed. When the web interface is enabled, administrators can also enable recipients to set up personal allow lists and block lists, and to opt out of spam checking.

Monitoring, alerting, and notification

Operating on the principle of exception-driven management, Sophos Email Appliances feature advanced technology designed to reduce or eliminate as much administrative burden as possible. Automated self-maintenance and a comprehensive monitoring system that keeps regular watch over 40 different functions ensure higher performance with less effort.

Pre-emptive actions

In the event of system interruption, the appliance sends email alerts to the system administrator for resolution, and changes the color of the master System Status indicator in the management console. For a mission-critical condition requiring external assistance, (e.g. a failed power supply), an alert is also sent to Sophos. Resolution of such a condition can often be initiated by Sophos before the administrator is aware of it (e.g. shipping a replacement power supply*).

As an added measure of security and confidence, Sophos uses innovative remote “heartbeat” monitoring to ensure that every installed appliance is downloading up-to-date threat definitions and software updates on schedule. If an appliance fails to download or apply an update, it will alert the administrator. If it fails more than three times in a 15-minute period, the appliance will also alert Sophos support. If an appliance has not drawn down updates for more than two hours, Sophos support will phone you.

Spam protection

Sophos’s unique method of spam identification features the most advanced detection technologies in the industry, provided by SophosLabs 24 hours a day, every day of the year. SophosLabs has spam traps all around the world that review millions of messages a day, providing in-depth visibility and insight into global email traffic. Based on this continuous monitoring, two categories of spam are identified: high and medium. Administrators can choose the default handling rules for these categories, or set up specific rules based on internal needs. This simplified approach means that Sophos focuses on the spam so you can focus on other priorities.

Reputation filtering

The first line of spam and malware defense is connection-level protection. Sender Genotype watches for characteristic botnet behavior at the connection level, preventing spammers from sending email even before their reputation has been established. When combined with the ability to drop connections from known spammer IP ranges at the MTA level prior to scanning, as much as 90% of inbound spam can be eliminated this way, substantially increasing message throughput without the need for additional infrastructure investments. The appliance can also allow the message to pass through the MTA and perform a reputation filter just before scanning (see below). Email identified at this stage as originating from known bad senders is treated the same as other messages identified as spam according to Sophos spam tests, and is handled according to the specified security policy.

* ES5000 and ES8000 only

Security made simple

If there are no alerts generated by the appliance, then email security is performing as expected and there is no need for intervention.

Proven spam protection

Sophos Email Appliances detect up to 99.4% of spam at the email gateway.
eVision IT Labs, October 2007

The scanning engine uses a wide range of filtering methodologies, combining hundreds of different tests to expose filter-evading tactics. For example, one test looks for the many different ways (more than 5.6 billion) that spammers spell the word Viagra. If a spam indicator is triggered, that result contributes to the message's overall spam score. The message headers, structure, content, and call-to-action URIs (uniform resource identifiers, i.e. web page, email address, file name, etc) are also scanned for thousands of different conditions.

Spam detection techniques include the following:

- Known security threat sensors to protect against scams, such as phishing, which trick users into submitting personal or financial information
- Sender Genotype analysis to eliminate botnet spam at the IP-connection level
- Genotype campaign analysis to identify complex spam campaigns by recognizing characteristics common to a series of messages
- Offensive content sensors to target pornographic and other sensitive content
- "Fingerprinting" techniques that detect and block image spam and attachment spam using PDF, Excel or other common types of attachments
- Spammer asset tracking to identify the advertised website operators and to block unsolicited messages
- Destination URI filtering to block messages to hijacked, freeweb, and other advertised websites
- Obfuscation sensors to identify techniques spammers use to hide their messages from spam filters.

Sophos SXL technology

Only Sophos Email Security and Data Protection solutions – including Sophos Email Appliances – feature SXL technology. SXL provides up-to-the-second anti-spam protection by enabling real-time network checks for the latest anti-spam intelligence from SophosLabs. SXL servers not only contain the latest information from SophosLabs, they also retain older anti-spam intelligence that may be dormant – such as botnet IPs or destination URLs – but which takes up valuable local storage space. SXL technology enables each installation to benefit from the growing body of anti-spam intelligence without requiring ever-increasing local storage.

SophosLabs continually analyzes the flow of spam messages through its network of traps, pushing protection data to the SXL servers and automatically updating appliances every few minutes. This allows you to maintain up-to-date protection from the latest spammer activity without any administrative effort.

A final option available to administrators (on by default) is automatic protection against Denial of Service and Directory Harvest Attacks (DoS and DHA). When enabled, the appliance can throttle inbound traffic and block inbound connections that often indicate such an attack.

Additional custom spam settings

The appliances offer two anti-spam mechanisms – allow listing and block listing – for further customization of inbound email policy.

Allow-listing: An optional element of spam filtering is managing an organization's allow list – the list of sender addresses or domains that are considered safe and therefore are not filtered for spam. Adding addresses and domains of trusted senders to the allow list eliminates the risk that their mail will be inadvertently blocked by the spam filter, and enables the filter to be more aggressive, testing only suspicious messages. Allow lists can be applied globally and, if enabled, to individual email accounts.

Block-listing: The opposite of an allow list, a block list contains sender addresses or domains that are considered “dangerous” or unwanted and are therefore blocked. Adding addresses to the block list reduces the volume of messages that have to go through a complete scan, thereby improving throughput and increasing system capacity. Block lists can be applied globally and, if enabled, to individual email accounts.

Administrators can also allow users to opt out of spam checking but, most importantly, virus checking cannot be disabled.

Virus protection

A business is more likely to receive a virus through its email gateway than via any other route. Virus protection at the email gateway provides an important first level of security, safeguarding the entire organization at a single point and enabling continued protection with one simple update. Sophos Email Appliances incorporate Sophos's industry-leading virus detection engine to protect organizations from viruses entering the organization through email.

The appliances check all traffic passing through the server in real time, providing protection against mass-mailing worms and viruses, including the latest blended threats that combine virus, spam, and Denial of Service attacks.

Zero-day protection

Advanced, proactive protection from SophosLabs means you're safe from zero-day threats and outbreaks. Genotype technology detects new variants of families of viruses, providing pre-emptive protection for up to 90% of new threats even before specific detection is available. The appliances automatically check executable content and files in email for malicious code and apply the appropriate policy to handle the message actions, ensuring fast and reliable protection.

Perimeter protection

Denial of Service (DoS) and Directory Harvest Attacks (DHA) are security threats that result in overloaded internal and gateway systems. To protect against these threats, Sophos Email Appliances measure message velocity to detect anomalous traffic patterns that exceed the organization's typical legitimate mail volumes from all or from specific senders. This monitoring enables you to detect and respond appropriately to DoS and DHA attacks.

Zero-day protection

Threat-reduction technology protects against fast-moving threats such as internet worms that can cause havoc before specific detection is available.

Data leakage prevention

Confidentiality breaches, legal liability, lost productivity, and damage to reputation can cost companies millions of dollars each year. Complex and evolving regulatory environments require organizations to protect themselves by establishing, monitoring, and enforcing appropriate policies and procedures at both the end-user and infrastructure levels.

The appliances' policy framework enables you to enforce a clear policy governing the messages and content allowed into and out of the gateway. A range of policy actions can be configured from within the management console by the administrator. Standard policies that organizations enforce are:

- Reject messages from known bad senders
- Set up allow lists and block lists (globally and individually)
- Quarantine messages containing harassing or offensive language
- Quarantine and review messages with specific keywords or attachments to protect against leakage of intellectual property or sensitive content
- Add banners to the message header and/or footer
- Re-direct messages based on message content
- Monitor and log suspicious traffic for system abuse detection.

For a complete list of default policy settings, see Appendix I.

Summary

Sophos Email Appliances provide the ideal mix of automation and control to support enterprise email management needs. They combine automated threat definition updating with quick and easy administrative capabilities and exception-driven alerting. This combination of functions minimizes the day-to-day administrative load while providing real insight and control.

Sophos Email Appliances draw on the extensive resources of SophosLabs around the world. The continued exposure of SophosLabs to email-borne threats enables proactive protection through faster analysis of new threats, multiple detection/update techniques (such as virus, spam, or policy updates), and complete management of the entire threat lifecycle.

Using Sophos Email Appliances, organizations benefit from:

- Reliable protection against new threats, virus variants and evolving spam campaigns
- Reduced administrative workload
- Greater peace of mind knowing the email infrastructure is protected.

Round-the-clock protection

SophosLabs™ threat analysis centers around the world provide 24-hour research and identification of emerging threats.

3: SETUP

Overview

This section covers basic appliance setup, including configuration, directory services setup, end-user preferences and default policy settings. It is not a substitute for the setup guide, but is intended to demonstrate the appliances' simplicity and ease of administration.

Configuration

Configuring Sophos Email Appliances is easy and straightforward. The Setup Wizard guides the administrator through basic configuration and enables live email scanning within 15 minutes.

The configuration categories are shown in Figure 4.

Administrators can modify these settings at any time through the management console.

Fast, easy setup

A simple setup wizard helps you get the appliance up and running in less than 15 minutes.

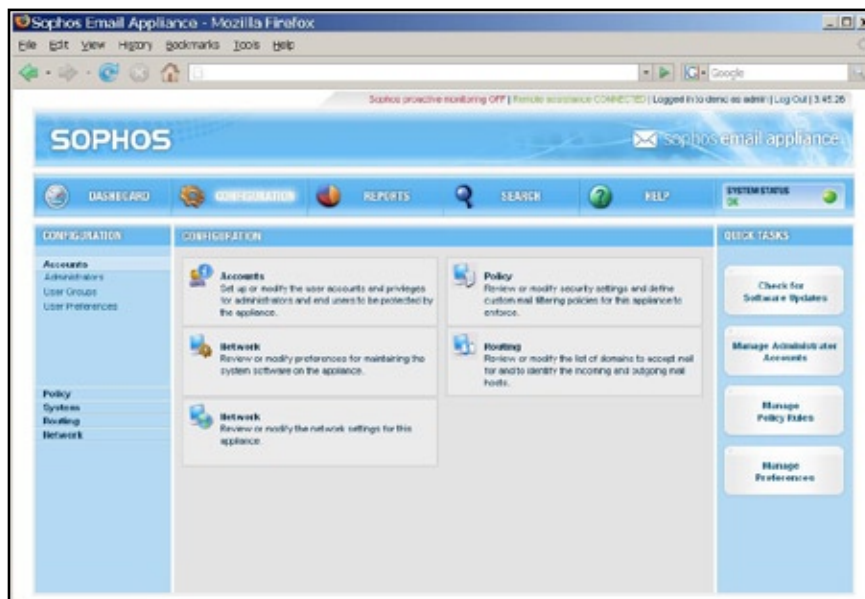


Figure 4: Configuration home page

Directory services setup

The appliances enable rapid setup of users and user groups through advanced LDAP integration, including Microsoft Active Directory®. This method provides simpler recipient validation as well as deployment of message policies to specific users and user groups.

On the Directory Services configuration page, the administrator can automatically detect and import LDAP settings, or enter settings manually. The appliance stores a local version of Active Directory to maintain

“ It took longer to get the appliance out of the box than to get it up and running. ”

Noe Arzate, Mount Pleasant Independent School District

functionality and to avoid downtime should the Active Directory server become unavailable. Administrators can set a synchronization schedule to ensure that the appliance uses the most up-to-date version.

User groups can be set up manually or using LDAP.



Figure 5: Configuring Directory Services

End-user preferences

The appliances feature smart capabilities for setting up and handling email users. Starting with complete LDAP integration, administrators can quickly and easily set up user privileges, such as:

- Authentication
- Allow lists and block lists
- Quarantine access via email digest or web interface
- User interface language preference
- Email delivery frequency
- Spam check opt-out.

For additional details on end-user quarantine access options, see *End-user options* in Section 4: Managing the appliances.

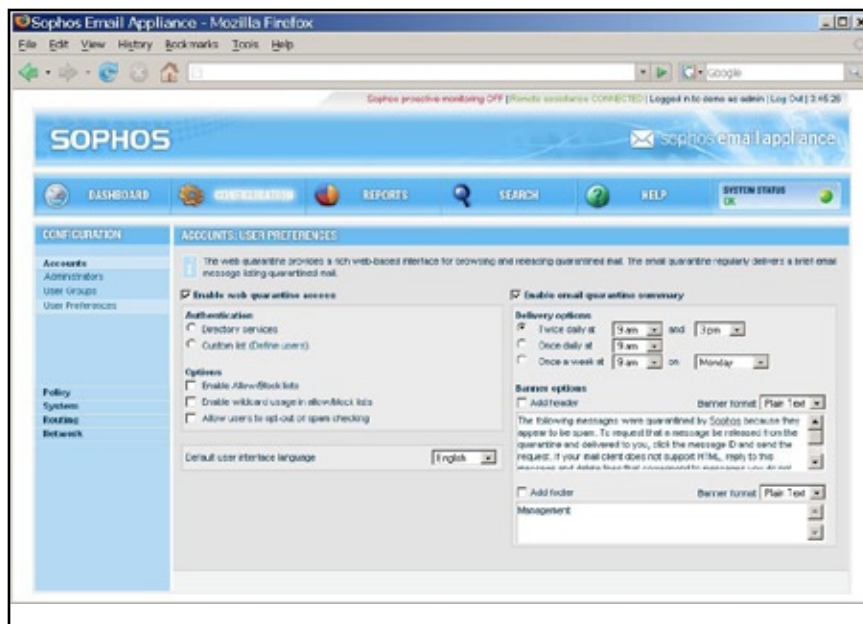


Figure 6: End-user preferences

Policies

Sophos Email Appliances are designed to deliver maximum security and flexibility with minimum administrative burden. Capitalizing on Sophos's extensive experience in detecting viruses, spam, and other types of malware, the appliances feature default policy settings that provide the highest degree of security to take the guesswork out of system configuration. However, if customization is required, the management console makes it quick and easy (see P.19 for a view of the policy wizard).

Anti-virus policy

Inbound messages containing viruses can be managed according to the nature of the threat:

- Virus
- Unscannable attachment
- Encrypted attachment
- Suspect attachment.

You can manage up to 20 separate rules and actions for both inbound and outbound mail. A range of actions are available, including notification (e.g. notify HR when offensive content is detected, or notify Legal when patent information is detected), banners and header modification. These actions enable comprehensive enforcement of your organization's acceptable email use policy.

See Appendix I for a complete list of the default policy settings.

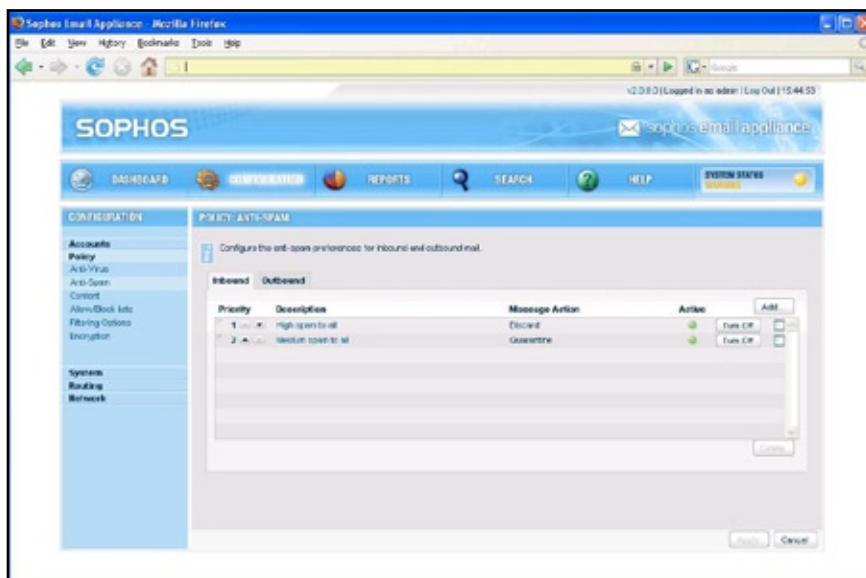


Figure 7: Anti-virus policy main page

Anti-spam policy

By default, the appliances discard messages from known bad senders and messages with high spam scores, and quarantines spam with medium spam scores. You can modify these settings according to Active Directory groups or custom lists.

Figure 8 shows the main anti-spam policy page in the management console. From here you can create and manage up to 20 different anti-spam rules, ensuring that your Sophos Email Appliance fits your organization's requirements.

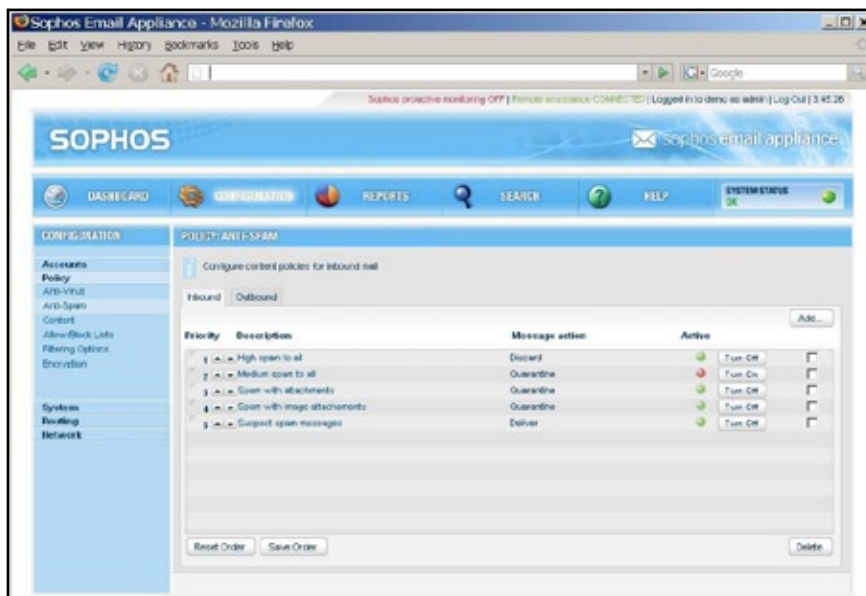


Figure 8: Anti-spam policy main page

Content policy

Emails can often contain content that can expose organizations to internal and regulatory liability issues. It is essential that your security solution enforce your policy for acceptable use. To prevent misuse, the filtering system scans email bodies and attachments for offensive language, specific keywords and file types, enabling you to maintain tight control over all message content.

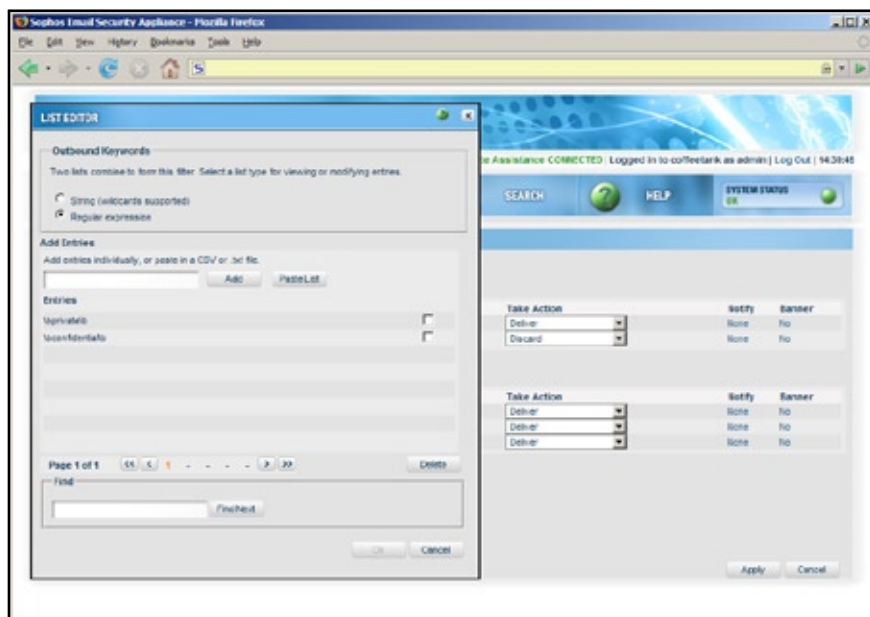


Figure 9: Customizing outbound content policy

Using the built-in policy wizard (see figure 9), you can customize up to 40 rules to watch for attributes such as attachment type and content (in regular expressions and strings with wildcards) specific to your organization or industry.



Step 1: Rule description

Select the type of content rule. Options include banner, keyword, attachment, language, watch list, hostname/IP address list, or message attributes such as size.





Step 2: Rule configuration

Specify the details for the rule, against the type chosen. For example, if the rule governs keywords, this page is where the keyword list is managed.



Step 3: Message attributes

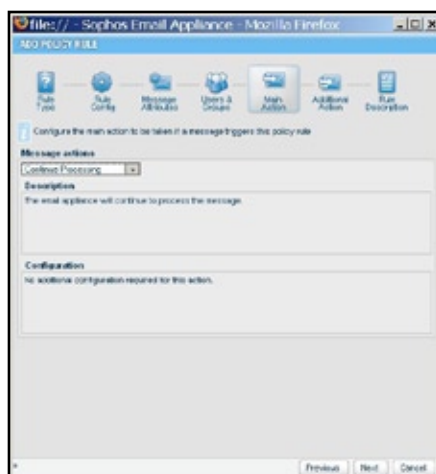
This is where other message attributes such as size are specified.



Step 4: Users and groups

Specify which users and/or groups are subject to the rule. You can maintain separate lists for senders and recipients.





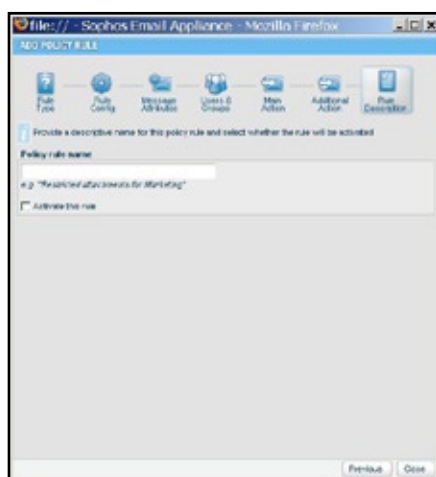
Step 5: Main action

This is where the administrator specifies what action should take place when the rule is triggered. A list of available actions can be found on page 9.



Step 6: Additional actions

This is where additional actions such as adding banners, modifying headers or setting notifications are managed.



Step 7: Rule description

Assign a name to the rule and choose whether or not to activate it. Activation and prioritization of rules is also managed from the main policy pages for viruses, spam and content.



For each type of content filter, and for both inbound and outbound mail, the administrator can set the following actions:

- Continue processing
- Deliver immediately
- Discard
- Quarantine
- Quarantine and continue
- Redirect
- Tag subject and continue
- Re-route
- Copy.

When setting up these rules and actions, you can choose to have them apply to specific users and/or user groups within your organization, as determined by the Active Directory server or by a custom list. Individual and group exceptions can also be specified. You can also opt to copy, blind copy, or redirect messages containing a content violation to a specified email address (e.g. a compliance officer), copy the sender/recipient, and add a notification message. A customized banner can also be added to either the top or bottom of the message.

You can also set an upper limit on message size (2 MB to 50 MB) in order to preserve space on the appliance and on downstream servers.

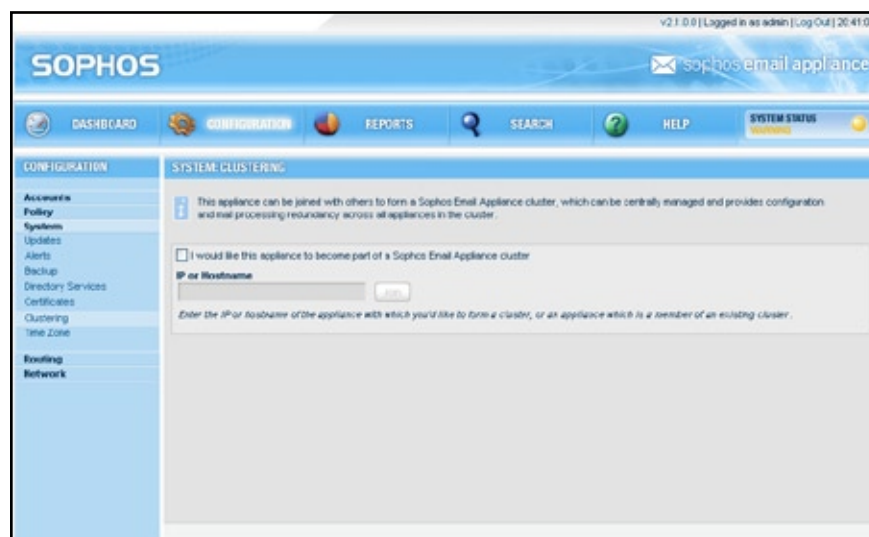


Figure 10: Adding an appliance to a cluster

Clustering

If you're installing more than one appliance, simply enter the hostname or IP address of the first appliance you configured and click 'join' in the clustering section of the install wizard. All configuration is automatically synchronized.

Summary

Sophos Email Appliances feature strong default policy settings for anti-virus, anti-spam, and message content. They also let you easily customize these policies to fit the specific needs of your organization. Whether you seek basic protection from spam and malware, or advanced prevention of data leakage via email, the result is complete, enterprise-grade email security with minimal effort.

4: MANAGING THE APPLIANCES

Overview

With Sophos Email Appliances, administration and control of the email gateway has never been easier. They feature a wide range of tools and settings designed to eliminate or automate the vast majority of administrative tasks, driven by a strict philosophy of exception-driven management.

It all begins with what we call the 'Managed Appliance' experience. Put simply, if you receive no alerts or notifications from the appliance (or from Sophos), then everything can be assumed to be working as intended and no interaction or intervention is required. Your appliance will notify you only if something requires attention. Otherwise, you can go about your daily tasks in complete confidence that the email gateway is operating safely and efficiently.

The appliances reduce the administrative burden by means of an intricate network of more than 40 built-in system sensors. When a sensor is triggered, a dashboard alert and/or an email alert is sent to the administrator. Logging in and clicking on the System Status button provides quick, at-a-glance feedback on the situation, along with recommended steps for resolution.

This section briefly outlines the daily administrative task of managing your appliance.

Reduced administration

More than 40 system sensors keep track of the appliance so you don't have to.

Status checks

You can instantly determine the overall status of the appliance by logging on to the management console and checking the System Status indicator, shown at the top right of every page (see Figure 11). Green indicates that all systems are normal; yellow, a temporary or low-level disruption; and red, a critical disruption. (In the event of a critical disruption, the appliance will send an email alert to the named technical contact, as well as to Sophos).

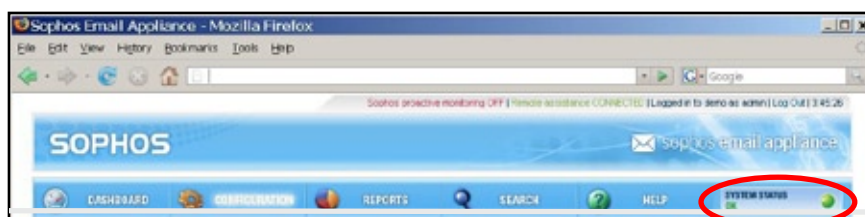


Figure 11: Checking system status on the management console

Clicking on the System Status indicator links to the System Status page, which provides details on the following environmental characteristics:

- **Mail flow:** spikes in mail volume, blocked messages, spam, and viruses
- **Quarantine:** size of the onboard message store
- **Software:** process health, protection status, connection to Sophos, system reboot, and system updates
- **Hardware:** component performance, temperature, memory usage, etc.
- **Certificates:** status of certificates used for TLS encryption or end-user authentication.
- **Licensing:** the time remaining on the software license.

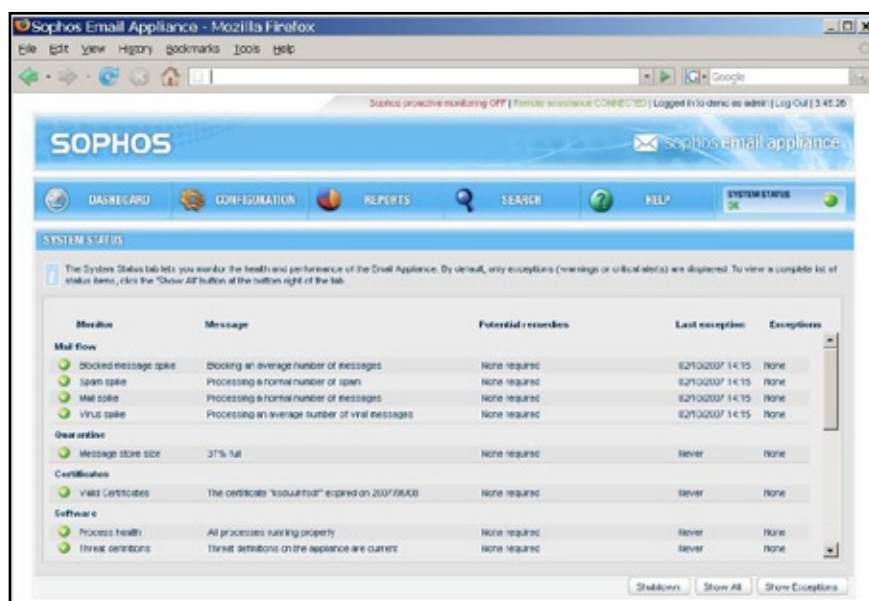


Figure 12: System Status page

As shown in Figure 12, the System Status page displays an indicator for each monitor, as well as a message that explains the current status, instructions for remediation, and details on the date and time of the last exception. If an exception occurred, you would be able to click on it to see more details of the incident and whether any automatic actions took place.

From this single page in the management console, you can check into every critical operation of the appliance. The System Status page makes it easy to conduct spontaneous comprehensive reviews of overall performance and protection status, and to obtain guidance on how to rectify system interruptions.

If you are administering multiple appliances, the cluster status page also provides valuable information about the appliances within a cluster, as well as scheduled jobs, such as email quarantine summaries, FTP configuration backup and directory services synchronization.

Updates

Sophos Email Appliances connect to Sophos every few minutes to download threat definition and software updates – by default, both are downloaded and applied automatically. The administrator has the option of downloading and applying non-critical software updates on a fixed schedule, or conducting on-demand, one-click updates. Non-critical updates can be deferred for up to seven days. Critical software updates such as vulnerability patches are applied instantly. As mentioned on page 12, access to the latest spam intelligence is available online and in real-time between downloads via SophosLabs' SXL network.

Backups

Administrators can set up the appliance to initiate automatic FTP backups of configuration data and system logs. Backups can take place on the following schedule:

- Daily, at midnight
- Weekly, on Friday at midnight
- Monthly, on the first day at midnight

Data backups can take place on the following schedule:

- On expiry
- Every half hour
- Every hour
- Daily, at midnight
- Weekly, on Friday at midnight
- Monthly, on the first day after midnight

Configuration data can also be backed up manually with one click on the System Backup page in the management console, as shown in Figure 13.

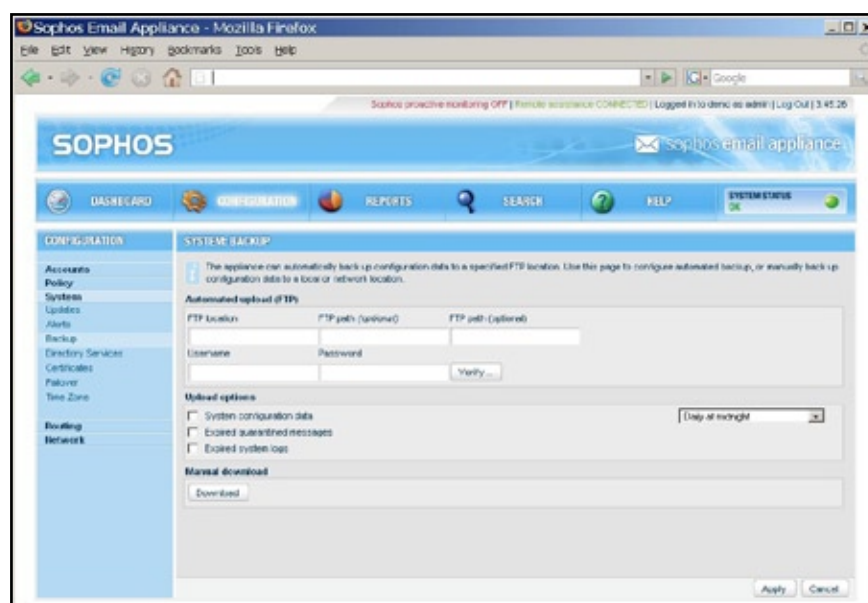


Figure 13: System Backup page

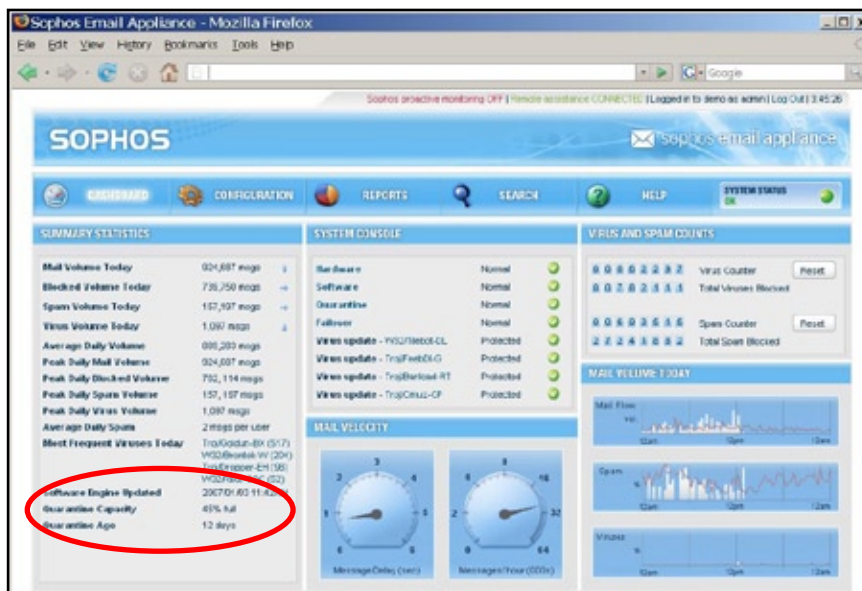


Figure 14: Viewing quarantine capacity on the dashboard

Quarantine

The appliances feature an onboard quarantine that can store millions of email messages. Depending on your organization's unique mail traffic patterns and policy settings, this storage capacity can translate into several weeks' worth of stored messages.

You can quickly check on quarantine status straight from the dashboard. At the bottom of the Summary Statistics section at the far left of the screen, there are two dynamic measurements of performance: Quarantine Age and Quarantine Capacity, as shown in Figure 14. Quarantine Age shows how many days' worth of storage is currently retained, e.g. 1 day, which means that the oldest message in the quarantine is 1 day old. Quarantine Capacity represents the percentage of storage space currently used, e.g. 1.5% full.

The appliances use automatic quarantine archiving in order to maintain optimum performance and ensure adequate onboard storage capacity. If the data on the hard disk reaches 70% of capacity, data will be automatically archived so that a minimum of 40% of disk capacity is available. The administrator must configure the FTP backup location within the appliance management console.

End-to-end message search

Extending well beyond storage capacity, Sophos Email Appliances also provide end-to-end message search capabilities. They are designed to alleviate the most time-consuming aspect of email gateway management – finding “lost” messages. With this feature you can search easily across different parameters and reduce the time spent finding out what happened to a given message.

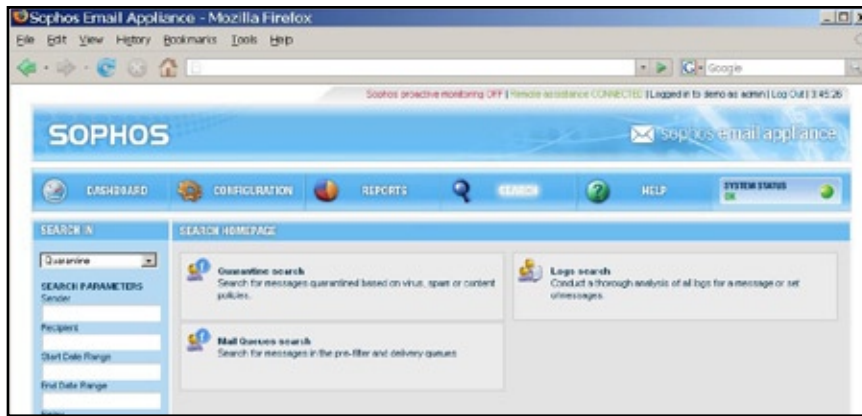


Figure 15: Sample mail log search

The search function is accessed from the navigation bar of the management console, as shown in Figure 15. Searches can be conducted separately in the mail logs, mail queue, or quarantine.

Mail logs can be searched using the following parameters:

- Sender
- Recipient
- Start date range
- End date range
- Relay
- Message ID

The log data is presented in an easily readable format, hiding the unnecessary details and highlighting the information that reveals what actually happened with the message in question. A search will sort the details under the following headings:

- Date and time
- Sender
- Recipient
- Relay
- Subject

Clicking on an entry in the search results will reveal more complete details about the log.

The mail queue can be searched using the following parameters:

- Sender
- Recipient
- Start date range
- End date range
- Queue (All, Pre-filter, Delivery)

The queue data provides details on where a message is within the mail flow – queued for filtering, or queued for delivery to the downstream mail server. Information is presented in an easily readable format. A search will sort the details under the following headings:

- Date and time
- Size
- Recipient
- Sender
- Queue status

The quarantine can be searched using the following parameters:

- Sender
- Recipient
- Start date range
- End date range
- Reason
- Relay
- Message ID

A quarantine search will sort the details under the following headings:

- Date and time
- Sender
- Recipient
- Subject
- Reason

Note

You can search by the following reasons: All, Virus, Spam, Keyword, Suspect attachment, Encrypted attachment, Unscannable attachment, Offensive language.

Clicking on an entry in the search results will reveal more complete details about the quarantine entry, including the option to view the message details. An administrator can then select messages for release, forwarding, or deletion.

To further reduce day-to-day management workload, the administrator can set up special accounts for help desk staff charged with handling internal email-related inquiries. These accounts have access to all the quarantine management functions, but not to system settings or configuration options. For administrators with wide-ranging responsibilities and access to additional staff, this feature enhances group productivity and frees up time to focus on other business matters.

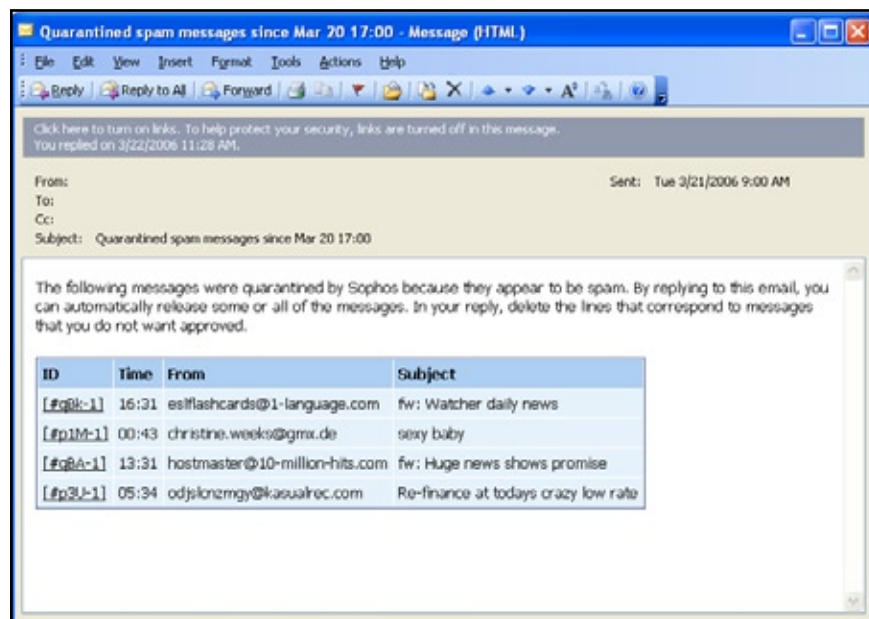


Figure 16: Email digest (note: may be rendered differently depending on your email client).

End-user options

In order to alleviate some of the pressure on the IT department, many organizations delegate some responsibility for managing inbound spam to its intended recipients. Sophos Email Appliances provide two options for this:

- Email digest
- End-user web interface.

Email digests are system-generated emails that contain a list of quarantined messages. Recipients can manage their personal quarantine simply by responding to the email with instructions to hold, release, or delete the messages on the list.

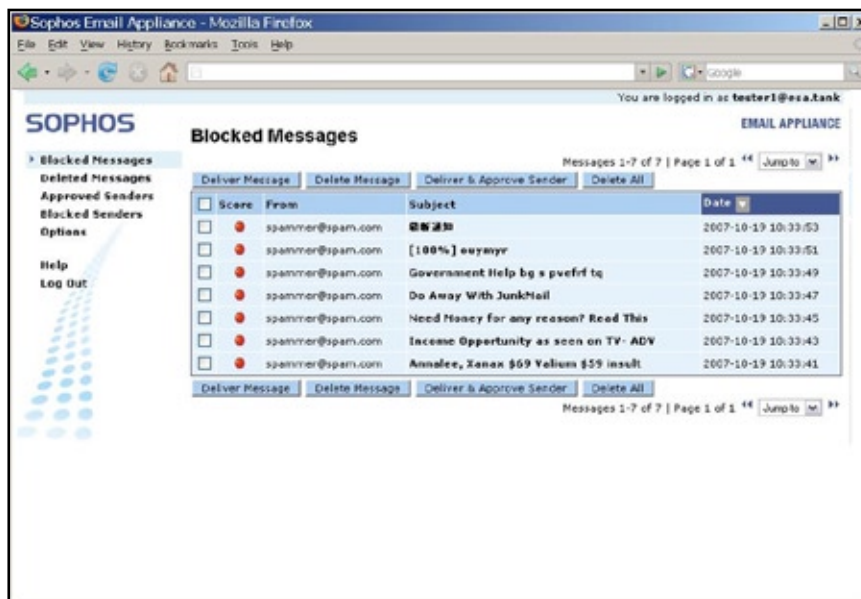


Figure 17: End-user web interface

The email digest shown above can be scheduled for delivery at specific times once per day, twice per day, or once per week.

Administrators also have the option of deploying web-based access to the quarantine, complete with user authentication through either Active Directory or a custom list. The end-user web interface, as shown in Figure 17, is a real-time view of quarantined messages for each user, providing the same options for holding, releasing, or deleting quarantined messages.

Both the email digest and the web interface can be deployed in one of the following languages: English, French, German, Italian, Japanese, and Spanish. This is a global setting determined by the administrator, and cannot be changed by the end user.

End-user preferences are global – if the email digest is enabled, every user will get the email digest. If the web interface is enabled, every user will get access to the web interface. The only exception is if the end user web interface is enabled, then individual users can choose to opt out of the email digest.

Administrators can grant users options to maintaining personal allow lists and block lists, and to opt out of spam checking completely. (For details, see *Additional custom spam settings* in Section 2: Product functionality). The administrator must enable these features globally on the End-User Preferences page (see Figure 6 in Section 3: Setup). Access to the end-user web interface must also be enabled by the administrator.

Faster filtering

Administrators can increase the efficiency of email filtering by applying allow lists and block lists globally or to individual email accounts.

5: REPORTING

Overview

In order to maintain control and visibility over the email gateway, administrators need a detailed understanding of what is happening with the mail flow. Simply knowing that the network has up-to-date protection from spam and viruses is not enough – administrators are often asked by senior management to provide a more holistic analysis of the email gateway. This type of request requires delving more deeply into factors such as what comprises the mail flow and how the hardware and software are performing. The appliances' real-time reporting capabilities make it easy to acquire this level of insight, leading to better management and smarter system administration.

While it is important to understand what is happening currently, it is equally, if not more, important to understand what is changing over time. The appliances provide a wealth of relevant, actionable reports to help administrators understand what goes on at the email gateway, and to help plan for future capacity requirements as the email system grows.

Aggregate reports are accessed in two locations within the management console. Key statistics such as mail volume and threat behavior are summarized on the dashboard (see Figure 3 in Section 2: Product functionality). More complete statistics covering a wider spectrum of information are accessible from the Reports page. Both areas are discussed below.

Dashboard reports

The dashboard provides a quick summary of live system performance, automatically refreshing the data every five minutes. The dashboard groups this data into three sections – **Summary Statistics**, **Mail Velocity** and **Mail Volume** – providing easy access to the most frequently referenced statistics.

Summary statistics

The summary statistics shown at the far left of the dashboard reveal daily and peak mail volumes and highlight the most common virus threats encountered. They also reveal when the last update took place and how much capacity remains in the onboard quarantine.

The arrows to the right of the top three lines indicate the variation against the previous day's traffic. For example, an arrow pointing down would indicate that today's volume is lower than yesterday's.

Average Daily Volume is a running total based on total mail processed since the appliance was first brought online. Peak volumes reflect the maximum values per category for the same period.

SUMMARY STATISTICS		
Mail Volume Today	924,887 msg/s	↓
Blocked Volume Today	739,750 msg/s	→
Spam Volume Today	157,197 msg/s	→
Virus Volume Today	1,097 msg/s	↓
Average Daily Volume	889,283 msg/s	
Peak Daily Mail Volume	924,887 msg/s	
Peak Daily Blocked Volume	762,114 msg/s	
Peak Daily Spam Volume	157,197 msg/s	
Peak Daily Virus Volume	1,097 msg/s	
Average Daily Spam	2 msg/s per user	
Most Frequent Viruses Today	Troj/Golden-BX (517) W32/Bronok-WX (204) Troj/Cropper-EM (98) W32/Revk-CDC (52)	
Software Engine Updated	2007-01-03 11:42AM	
Quarantine Capacity	45% full	
Quarantine Age	12 days	

Mail velocity

In the lower middle section are two dials, shown opposite, measuring messages processed per hour, and message delay, i.e. the time it takes the mail filter to scan a single message.

These dials provide an instant picture of the mail volume flowing through the appliance, and how long it is taking to process each message. If the dial on the left (messages/hour) is topping out, it could indicate a spike in email traffic, which would normally be accompanied by the dial on the right (latency) also topping out. Conversely, if the messages/hour dial is at zero, it could indicate a connection problem.



Mail volume today

On the bottom right of the dashboard, shown opposite, are three line graphs that measure daily mail, spam, and virus traffic.

The white fill area represents up-to-the-moment daily traffic flow, while the red line represents a running 7-day average. If there is a noticeable difference in the two patterns, there could be a mail spike or virus outbreak (white higher than red), or a connection/relay problem (red higher than white). Note that since these graphs measure the true nature of the mail flow, a spike in spam or viruses would indicate that the appliance is intercepting these threats, keeping them out of the mail stream.



Reports page

Clicking on the Reports tab on the management console navigation bar provides access to a greater scope and depth of reports (see Figure 18).



Figure 18: Reports page

Under Volume Info, mail characteristics for the most recent seven-day period are compared to the previous seven-day period, together with the variance between the two periods – providing a quick indication of how traffic is changing from week to week. Just below this section is the numerical presentation of system throughput and latency, also for the two most recent seven-day periods.

The pie chart on the bottom left breaks down total mail volume over the most recent seven days into six categories: **Legitimate**, **Blocked connections**, **Other** (messages with keyword or offensive content violations), **Spam medium**, **Spam high**, and **Virus**. This chart provides an instant perspective on the composition of the mail stream.

The bar graph on the bottom right covers the same period, displaying data for all but legitimate mail. This chart includes blocked connections (at the MTA), and counts each blocked connection as one message.

Finally, the two sections on the top right of the Reports home page show the five most recent alerts generated by the appliance, and the most frequent viruses detected.

Detailed reporting

The navigation pane at the left of the Reports page (and sub-pages) links to a wide range of customizable, dynamically generated reports. These reports are grouped into four categories, as shown in the table below:

Category	Report name	Description
Mail trends	Volume	Breaks down the daily mail stream into six components*
	Message actions	Delivered, dropped and quarantined messages
Performance	Latency	Time (in seconds) to scan a message
	Throughput	The quantity of messages scanned per second
Senders	Virus relays	IP origin of inbound viruses
	Spam relays	IP origin of spam messages
	Blocked connections	Number of connections blocked per IP address
Recipients	Spam recipients	Top ten spam recipients on your network
Policy analysis	Anti-Virus	Categorizes messages labeled “Virus” as Suspect, Encrypted attachment, Restricted attachment, Unscannable attachment, or Virus
	Anti-Spam	Categorizes messages labeled “Spam” as Blocked, Spam high, and Spam medium
	Content	The breakdown of messages blocked due to content keyword or offensive content violations

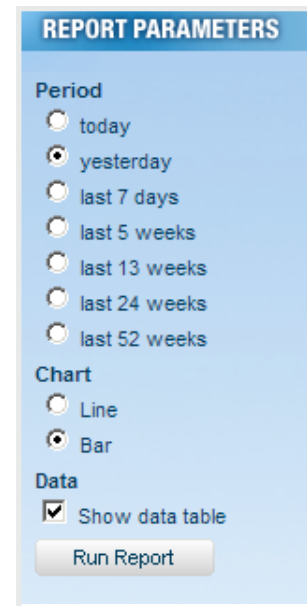
Note

The Anti-Virus and Content reports can be run against inbound or outbound email traffic.

* Blocked Connections, Legitimate, Other, Spam High, Spam Medium, Viruses

The report parameters can be applied to every report named in the table on the previous page. There is also the option to display the Data Table with each report.

Reports can be printed or exported as CSV files for use in other applications. For example, an exported report can be included in a presentation to senior management or to the compliance officer to demonstrate the effectiveness of the appliance on maintaining email security.



REPORT PARAMETERS

Period

- ☐ today
- ☒ yesterday
- ☐ last 7 days
- ☐ last 5 weeks
- ☐ last 13 weeks
- ☐ last 24 weeks
- ☐ last 52 weeks

Chart

- ☐ Line
- ☒ Bar

Data

- ☒ Show data table

6: SUPPORT

The Managed Appliance

Sophos Email Appliances introduce a new concept in network security: the Managed Appliance. A Managed Appliance combines the advantages of an appliance solution – visibility, platform independence, robust security – with the advantages of a managed service – ease of use, high availability, high capacity. The Managed Appliance, however, resides within your own network, preserving the control and visibility that is sacrificed through a managed service. Merging these two form-factors into one product provides peace of mind and confidence that cannot be obtained with any other solution.

The sections below provide an outline of the features that distinguish the Managed Appliance.

Automatic updates

In order to maintain up-to-date threat protection, most vendors' appliances initiate a data lookup every 30 or 60 minutes. With the increasing pace and rapidly evolving scope of email-borne threats, this scale of time delay can introduce considerable vulnerabilities in gateway security. Sophos Email Appliances eliminate long delays and improve security by automatically downloading new threat definitions from SophosLabs every few minutes. They also enable real-time network checks for late-breaking anti-spam intelligence in SophosLabs' unique SXL online database.

The Managed Appliance

Sophos Email Appliances combine the visibility and robustness of an appliance with the availability and simplicity of a managed service.

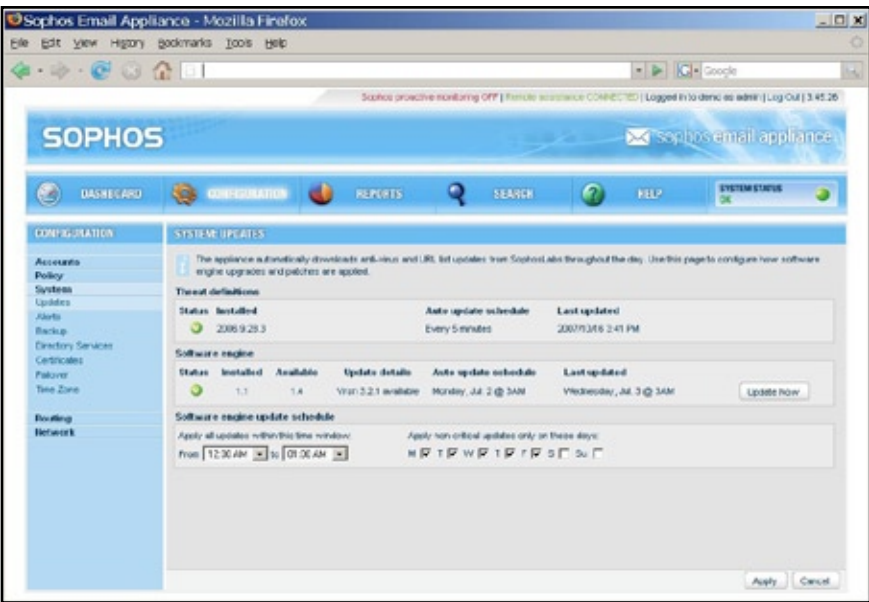


Figure 19: System Updates page

Updating at this frequency enables Sophos to narrow the gap between discovering a new threat and offering protection against it. It also reduces bandwidth consumption by requiring significantly smaller update file sizes – an important factor in the timing and effectiveness of protection. The result is the most reliable and dependable email security available.

New threat definitions and critical software upgrades are applied automatically upon download. Non-critical software upgrades can be applied instantly, or according to a schedule determined by the administrator, as shown in Figure 19 on the previous page.

“Heartbeat” monitoring

Frequent downloads go a long way to ensuring the best security possible. Sophos takes this concept one step further by remotely verifying that each appliance is equipped with the most up-to-date threat definitions. Rather than simply push out scheduled updates, Sophos appliances pull updates from a central repository. The repository actively checks to make sure every installed appliance “phones home” and downloads the updates on schedule. If an appliance fails to make contact for more than two hours, the repository alerts the Sophos support team to contact the administrator and investigate the situation.

This unique “heartbeat” monitoring provides a valuable layer of insurance and confidence to administrators, who no longer have to worry about whether or not their email gateway security is up to date.

Alerting

The appliances use more than 40 different sensors to monitor everything from Active Directory synchronization to virus spikes. Most of these sensors appear on the System Status page in the management console. If a sensor detects behavior outside the normal operating parameters of the appliance, it generates an alert that appears on the System Status page, along with a recommended course of action for remediation. The System Status button on the navigation bar also changes color as a visual indicator – green for normal, yellow for a warning and red for a critical alert. Clicking on the button leads to the System Status page, where further details can be found and corrective action initiated, if required.

The nature and severity of the condition can also trigger an email alert to the administrator, or another assigned individual. This has the advantage of not requiring the administrator to be logged in to the appliance in order to check on its status.

Mission-critical conditions also trigger an alert directly to Sophos support, as a step toward more rapid remediation. When this occurs, Sophos can initiate corrective action without contacting the administrator. For example, if one of the two power supplies fails, Sophos can initiate delivery of a replacement before the administrator even knows of the failure.

Proactive alerts

Alerts can be sent to an assigned individual when the administrator is not available, and mission-critical conditions automatically alert Sophos to take pre-emptive action.

On-demand remote assistance

Sophos Email Appliances feature a robust, searchable Help index to assist with troubleshooting. In the event that an administrator cannot resolve a system problem, live remote assistance can be requested from a Sophos engineer. The secure remote assistance session, which can only be initiated by an administrator with proper security clearance, allows the Sophos engineer to access the appliance to assist with troubleshooting. The session uses Secure Shell (SSH) technology that does not require any change to firewall settings, and expires automatically after four hours for additional security. Furthermore, every modification made to your appliance by the Sophos engineer is fully logged and recorded, right down to the keystrokes, as an exhaustive compliance measure. This means that remote assistance sessions do not materially compromise the integrity and security of your email network.

Warranty

Sophos offers an Advance Replacement Warranty on every Email Appliance, for up to three years. Should a major component (hard drive, power supply, entire unit) fail during normal use, Sophos will automatically send you a replacement part before you are required to send the defective part back. This warranty, which is standard on every appliance, demonstrates the confidence that we have in Sophos Email Appliances and provides the peace of mind administrators deserve.

There are two field-replaceable units in the ES5000 and ES8000 – the hard disks and the power supplies. Both these units can be swapped out without requiring a system shutdown or reboot. Any other component failure will require a completely new appliance. The ES1000 does not have any field-replaceable units.

You will never need to open the lid of a Sophos Email Appliance for servicing or maintenance. Note that, for security purposes, opening the lid will void your product warranty and trigger an alert to Sophos.

For complete details on Sophos Email Appliance warranties, please consult the End-User License Agreement.

Note

For local terms and conditions of your product warranty, contact your Sophos representative.

24/7 Sophos support

The excellence of Sophos support services sets us apart from our competitors. We provide 24-hour support, every day of the year and you can contact our globally managed support team for one-to-one assistance at any time.

We have support centers in Australia, Canada, France, Germany, Japan, Italy, Singapore, the UK and USA. Our experts can replicate, analyze and resolve your problems, backed by the resources of SophosLabs and product development.

This service is standard with every Sophos product. Sophos support is **not** outsourced and never closes – if you need to talk to an engineer, we're always just a phone call or email away.

APPENDIX I: DEFAULT POLICY SETTINGS

General						
For messages with	To	Except to	Take action	Notify/redirect	Users	Add banner
Known bad senders	All	None	Reject (at MTA)	No		No
Inbound and outbound messages greater than 10 MB (with or without attachment)	All	None	Reject (at MTA)	No		No
Inbound anti-spam						
For messages with	To	Except to	Take action	Notify users	Users	Add banner
High spam ratings	All	Spam opt-outs	Discard	No		No
Medium spam ratings	All	Spam opt-outs	Quarantine	No		No
Inbound anti-virus						
For messages with	To	Except to	Take action	Notify users	Users	Add banner
Viruses	All	None	Discard	No		No
Unscannable attachments	All	None	Deliver with warning banner	No		Can't clean
Encrypted attachments	All	None	Deliver with warning banner	No		Encr_file
Suspect attachments	All	None	Quarantine, drop file, deliver	No		Suspicious
Outbound anti-spam						
For messages with	To	Except to	Take action	Notify users	Users	Add banner
High score	All	None	Quarantine	No		N/A
Medium score	All	None	Quarantine			
Outbound anti-virus						
For messages with	To	Except to	Take action	Notify users	Users	Add banner
Viruses	All	None	Quarantine	No		N/A
Unscannable attachments	All	None	Deliver	No		N/A
Encrypted attachments	All	None	Deliver	No		N/A
Suspect attachments	All	None	Discard	No		N/A

APPENDIX II: HARDWARE SPECIFICATIONS

ES1000, ES5000 and ES8000 Email Appliance specifications*		
On-board software		
<p>Sophos anti-virus engine</p> <p>Sophos anti-spam engine</p> <p>Both engines feature Genotype™ and Behavioral Genotype proactive protection</p> <p>Sender Genotype provides connection-level protection</p> <p>TLS encryption</p> <p>Active/passive failover with shared configuration</p> <p>Web-based dashboard and management console</p> <p>System health alerting and notification</p> <p>LDAP integration including Active Directory</p> <p>Postfix MTA (mail transfer agent)</p> <p>Hardened FreeBSD operating system</p>		
Hardware – ES1000	Hardware – E5000	Hardware – E8000
Single core processor	Quad core processor	Quad core processor
160 GB SATA hard drive	Dual hot-swap 160 GB SAS (RAID 1) hard drives	Dual hot-swap 300 GB SAS (RAID 1) hard drives
260 W 100/240 V AC power supply	Dual hot-swap 920 W 100-240 V AC power supplies	Dual hot-swap 920 W 100-240 V AC power supplies
50,000 messages per hour	380,000 messages per hour	550,000 messages per hour
1U rack-mountable	1U rack-mountable	1U rack-mountable
Dimensions (W x H x D): 16.8" x 1.7" x 14.0" (427mm x 43mm x 356mm)	Dimensions (W x H x D): 17.0" x 1.7" x 25.6" (432mm x 43mm x 650mm)	Dimensions (W x H x D): 17.0" x 1.7" x 25.6" (432mm x 43mm x 650mm)
Weight 26 lbs/11.8 kg	Weight 45 lbs/20.5 kg	Weight 45 lbs/20.5 kg
Regulatory/safety certifications		
UL 60950, CE, FCC PART 15, VCCI, C-TICK, TUV-GS, SABS, RoHS, WEEE Certifications		
Support		
Up to 3-year advance-replacement hardware warranty (subject to valid software licensing)		
24/7 support		
*Sophos specifications may be updated without notice. Please check www.sophos.com regularly.		

