

SOPHOS

 email **security and data protection**

Reviewer's Guide

E-mail Appliances

Modelle: ES1000, ES5000 und ES8000



WILLKOMMEN

Willkommen zum Reviewer's Guide für Sophos E-Mail Appliances. Diese Anleitung ist um den Alltag eines E-Mail-Systemadministrators herum aufgebaut. Wir erklären Ihnen die wichtigsten Funktionen unserer E-Mail Appliances und veranschaulichen deren Effektivität und Benutzerfreundlichkeit. Wenn Sie die Anleitung gelesen haben, werden Sie besser verstehen, was unsere E-Mail Appliances zum zuverlässigsten und intelligentesten E-Mail Gateway-Schutz macht, der zurzeit auf dem Markt erhältlich ist.

Die Appliances ES1000, ES5000 und ES8000 sind Komponenten der Lösung „Sophos E-mail Security and Data Protection“, zu der Managed E-Mail Appliances und Software-Schutz für Exchange-, UNIX- und Domino-Server auf Gateway- und Groupware-Ebene gehören. Jede Sophos E-Mail-Lösung bietet Schutz vor Viren, Spam und Phishing sowie Funktionen zur Verhinderung von Datenverlusten. So sind Ihre E-Mail-Inhalte gesichert und Sie behalten stets die Kontrolle.

Wie all unsere Lösungen sind Sophos E-Mail Appliances das Ergebnis von mehr als 20 Jahren Erfahrung im Schützen von Unternehmen, Bildungseinrichtungen und Behörden. Die Appliances profitieren vom kollektiven Fachwissen der SophosLabs™ – unserem globalen Netzwerk von Bedrohungsanalysecentern – über Viren, Spyware und Spam. Rechtzeitiges Erkennen und Schützen vor immer komplexer werdenden und sich rasant ausbreitenden Sicherheitsbedrohungen ist einer der Gründe, weshalb Sophos immer wieder die größte Kundenzufriedenheit und den besten Schutz in der Branche erzielt.

In allen Sophos Lizenzen ist umfassender Support durch unser weltweites Netzwerk von Support-Technikern rund um die Uhr und an 365 Tagen im Jahr inbegriffen.

„E-mail Security and Data Protection“ ist separat erhältlich oder kann mit einer einzigen „Sophos Security and Data Protection“-Lizenz erworben werden, die auch „Web Security and Control“ und „Endpoint Security and Data Protection“ enthält. Informationen zu Preis und Verfügbarkeit dieser Appliances an Ihrem Standort erhalten Sie von Ihrem Sophos Account Manager. Auf unserer Homepage erfahren Sie, wer für Ihren Standort zuständig ist:

www.sophos.de/products/howtobuy

Sie möchten die Sophos E-Mail Appliances testen? Dann füllen Sie bitte folgenden Online-Antrag aus:

www.sophos.de/free-trials

INHALT

1 EINFÜHRUNG	5
Management-Highlights	6
Hauptfunktionen und -vorteile	7
2 PRODUKTFUNKTIONEN	8
Software-Aufbau	8
Data Leakage Prevention	15
3 SETUP	17
Konfiguration	17
Verzeichnisdienste	18
Endnutzer-Präferenzen	18
Richtlinien	19
4 VERWALTUNG DER APPLIANCES	25
Statusprüfungen	25
Updates	26
Backups	27
Quarantäne	28
E-Mail-Suche	28
Endnutzer-Optionen	30
5 REPORTING	32
Dashboard-Reports	32
Reports-Seite	33
Detailliertes Reporting	34
6 SUPPORT	36
Managed Appliance	36
Garantie	38
Sophos Rund-um-die-Uhr-Support	38
ANHANG	
I Richtlinienvoreinstellungen	39
II Technische Daten	40

1: EINFÜHRUNG

Sophos E-Mail Appliances sind sichere E-Mail-Gateway-Lösungen, die integrierten Schutz vor Spam, Malware, Phishing und Datenverlust per E-Mail bieten. Sie basieren auf dem Konzept von Managed Appliances, d.h. sie vereinen Kontrolle und Überblick einer Appliance mit der Unkompliziertheit von Managed Services. Die ES1000, ES5000 und ES8000 laufen auf einer robusten Hardware-Plattform. Sie liefern leistungsstarke, lückenlose Sicherheit für E-Mails in Unternehmensnetzwerken.

Kapazitäten:

ES1000 bis zu 50.000 E-Mails pro Stunde

ES5000 bis zu 380.000 E-Mails pro Stunde

ES8000 bis zu 550.000 E-Mails pro Stunde

Die E-Mail Appliances bestehen aus folgenden Komponenten:

Zukunftsweisende Threat Detection Technology: Vielfach ausgezeichnete Überprüfungs-Technologie aus den SophosLabs, unserem globalen Netzwerk von Bedrohungserkennungs- und Bedrohungsanalysecentern. Die automatische Feinabstimmung sorgt für ein ständiges Gleichgewicht verschiedener Erkennungstechniken, passt sich an entstehende Bedrohungen an und gewährleistet so lückenlosen Schutz.

Das Sender Genotype-Verfahren führt bereits bei Verbindungsherstellung eine Überprüfung auf Botnet-Indizien durch und deckt so auch E-Mails von bisher unbekanntem Spammern auf. Neue Bedrohungskennungen und Anti-Spamregeln werden alle fünf Minuten automatisch heruntergeladen und stellen so den neuesten Schutz bereit. Durch die in Echtzeit erfolgende Online-Bereitstellung neuester Bedrohungsinformationen aus den SophosLabs sorgt Sophos SXL für noch schnelleren Schutz und macht das Warten auf neue Updates überflüssig.

Data Leakage Prevention: Sophos E-Mail Appliances enthalten wirksame Mittel, die vor dem Verlust vertraulicher Daten schützen und bei der Einhaltung gesetzlicher Vorschriften helfen. Mit einem Assistenten können Sie schnell und einfach eigene Regeln zur Überwachung von ein- und ausgehenden E-Mail-Textkörpern und Anhängen auf Stichwörter, Dateitypen, Größe und andere Attribute erstellen. Zusätzlicher Schutz ist durch TLS-Verschlüsselung ausgehender E-Mails gewährleistet, sodass sie nur vom gewünschten Empfänger gelesen werden können. Sollten noch individuell abgestimmtere Verschlüsselungsrichtlinien benötigt werden können die Sophos E-Mail Appliances auch mit Fremdsystemen kombiniert werden.

Überwachung und Alarmer: Die Appliances von Sophos verfügen

Effizienter E-Mail-Schutz

Sophos E-Mail Appliances bieten maximalen E-Mail-Schutz bei minimalem Administrationsaufwand.

über eine integrierte Überwachungs- und Alarmfunktion für eine schnellere Problembhebung. Für höchste Leistung werden mehr als 40 verschiedene Einstellungen ständig überwacht. Damit im Ernstfall schnellstmöglich Gegenmaßnahmen ergriffen werden können, werden Alarme sowohl an den Systemadministrator als auch an Sophos gesendet. Sollte weitere Unterstützung erforderlich sein, können Administratoren von der Remote- Unterstützung bei Bedarf Gebrauch machen und Sophos die Fehlersuche direkt überlassen.

Management-Konsole: Diese leistungsfähigen Technologien werden durch eine intuitive webbasierte Management-Konsole ergänzt, welche die administrativen Aufgaben vereinfacht und bessere Einsicht und Steuerung über die E-Mailinfrastruktur gewährt. Die benutzerfreundliche Management-Konsole ermöglicht den sofortigen Zugriff auf relevante Daten und solche, auf deren Basis gehandelt werden kann, so dass Administratoren sachkundige Entscheidungen über Systemleistung und künftige Kapazitätsanforderungen treffen können.

Management-Highlights

Die Eigenschaften der Sophos E-Mail Appliances vereinfachen den Umgang mit E-Mails:

- Vollständig webbasierte, benutzerfreundliche Management-Konsole
- Konfigurierbare Richtlinien zur Verwaltung von Viren, Spam, E-Mail-Inhalten und Datei-Anhängen
- TLS-Verschlüsselung und Unterstützung kundenspezifischer Zertifikate für sicheren Zugriff auf die Management-Konsole und die webbasierte Endnutzeroberfläche
- E-Mail-Analysen mit Zugriff auf Quarantäne, E-Mail-Protokolle und E-Mail-Warteschlangen
- Mit nur einem Klick Zusammenfassen von bis zu 10 Appliances zu einem Cluster
- Einbindung von Microsoft Active Directory® und anderen LDAP-Systemen für einfache Einrichtung, Richtliniendurchsetzung und Authentifizierung
- E-Mail-Digest oder webbasierte Benutzeroberfläche zur Quarantäne-Selbstverwaltung für Endnutzer
- Allow-/Block-Lists – global und pro Benutzer
- Integrierte Wartung von Hard- und Software sowie Alarmfunktionen
- Proaktive Funktionsüberwachung
- Remote-Unterstützung bei Bedarf

Vielfach ausgezeichnete Schutz

Die hervorragenden Eigenschaften der Sophos Sicherheitsprodukte werden regelmäßig von diversen unabhängigen Prüfungskommissionen einschließlich ICSA, West Coast Labs, Veritest, eVision IT Labs, av-test.org und führenden IT-Magazinen wie IT PRO und SC Magazine ausgezeichnet.

Hauptfunktionen und -vorteile

- Failover-Cluster mit zwei Einheiten aktiv/passiv

Hauptfunktion	Hauptvorteil
Plattformunabhängig	Lässt sich problemlos in jede vorhandene E-Mail-Infrastruktur integrieren
Unübertroffene Spam- und Malware-Erkennung	Voll integrierter und vielfach ausgezeichneter Spam- und Malware-Schutz aus den SophosLabs
Proaktiver Genotype-Schutz	Aussonderung von bis zu 90% neuer Bedrohungen ohne spezifische Kennungen
Behavioral Genotype Protection	Proaktive Intrusion Prevention erkennt und blockiert Schadprogramme noch vor deren Ausführung
Data Leakage Prevention	Bietet leistungsstarke Funktionen zur Inhaltsüberprüfung sowie zur TLS-Verschlüsselung und schützt so vor dem Verlust vertraulicher Daten
Sender Genotype-Verfahren	Blockiert mittels Reputation Filtering und proaktiver Botnet-Erkennung 90% des Gesamtspams bereits bei Verbindungsherstellung.
SXL-Echtzeit-Spamschutz	Mit SXL sofortiger Zugriff auf Spamschutz-Informationen der SophosLabs zum Schutz vor neuesten Spamkampagnen
Hohe Genauigkeit	Erkennt mehr als 99% aller Spam-Mails und schützt vor E-Mail-Scams, einschließlich Phishing-Attacken. Hohe Genauigkeit mit einer unbedeutend geringen Anzahl an False Positives
Hohe Verfügbarkeit	Gewährt durchgehende Verfügbarkeit mit redundanten Hot-Swap-fähigen Festplatten und Netzgeräten
Hohe Kapazität	Liefert maximale Prozessor- und Speicherkapazität in einem kompakten Format
Einhaltung von Richtlinien	Schließt eine konfigurierbare Richtlinienumgebung ein, um interne oder gesetzliche Einhaltungsanforderungen zu unterstützen
Verschlüsselung	Erhöhter Schutz durch TLS-Verschlüsselung
Mehrsprachiger Schutz	Schützt Unternehmen vor Spam und Viren in mehrsprachigen E-Mails
Automatische Updates	Gewährt aktuellen Schutz durch automatische Updates aus den SophosLabs – einem globalen Netzwerk von Bedrohungsanalysecentern
Endnutzer-Funktionen	Verringerter Verwaltungsaufwand durch Endnutzer-Quarantäneverwaltung sowie Allow-/Block-Lists
Umfassender Support	Uneingeschränkter Support per Telefon, E-Mail und Online – rund um die Uhr, an 365 Tagen im Jahr

2: PRODUKTFUNKTIONEN

Übersicht

Die Sophos E-Mail Appliances ES1000, ES5000 und ES8000 sind Sicherheitslösungen, die einfach an den E-Mail-Gateway angeschlossen werden und sofort ihre Schutzfunktion erfüllen. Sie lassen sich problemlos in jede Netzwerkkonfiguration integrieren; und da beide über ein separates Betriebssystem verfügen, benötigen Sie keine Kenntnisse über UNIX, Linux, Solaris oder andere Serverplattform-Sprachen.

Wie die Gateway Appliances werden sie gewöhnlich in der DMZ, der neutralen Zone innerhalb der Netzwerk-Firewall und außerhalb der Mailserver, installiert.

In diesem Abschnitt finden Sie Informationen zum Software-Aufbau der Appliances und einen Überblick über die Einhaltung der internen E-Mail-Sicherheits- und gesetzlichen Richtlinien.

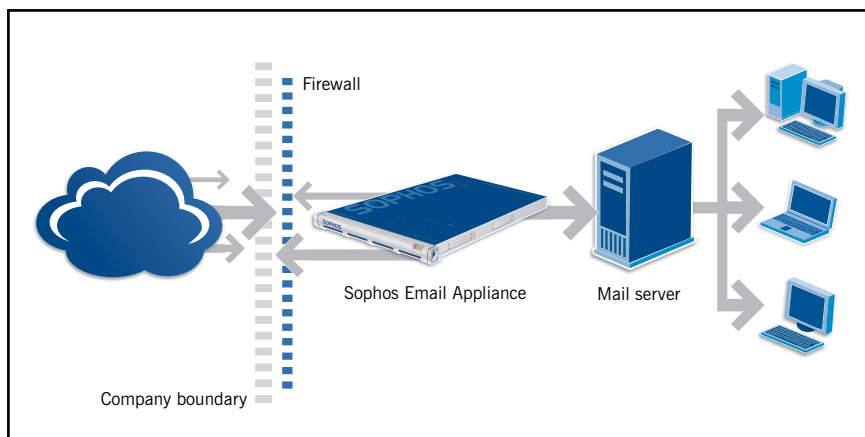


Abbildung 1: Typische Installation einer Sophos E-Mail Appliance

Software-Aufbau

Die enthaltene Software besteht aus fünf Hauptelementen:

- 1 Optimiertes FreeBSD Betriebssystem
- 2 Leistungsstarkes E-Mail-Filterungssystem
 - Postfix MTA (Mail Transfer Agent)
 - Antispam-Engine
 - Antivirus-Engine
 - Erweiterte Sender Genotype Connection Control
 - Richtlinien-Engine
- 3 Management-Konsole und Dashboard
- 4 Integrierte Quarantäne
- 5 Überwachungs-, Alarm- und Benachrichtigungssystem

Optimiertes FreeBSD-Betriebssystem

Die Sophos E-Mail Appliances laufen auf einem gehärteten FreeBSD-Betriebssystem, optimiert für die Hardwareplattform und die integrierte Sophos Software. FreeBSD ist extrem stabil und zuverlässig und liefert enorme Geschwindigkeit und Leistung für Network Security Appliances. In Anhang II finden Sie die vollständigen technischen Daten.

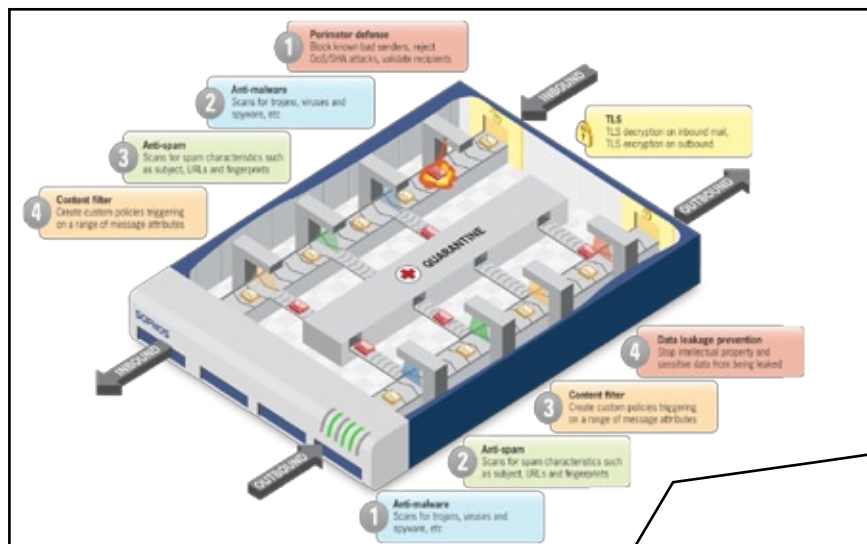


Abbildung 2: Die Sophos E-Mail Appliance überprüft ein- und ausgehende E-Mails

Leistungsstarkes E-Mail-Filterungssystem

Das E-Mail-Filterungssystem führt folgende Aufgaben aus:

Eingehende E-Mails:

- Der integrierte MTA fängt eingehende E-Mails am E-Mail-Gateway ab.
- E-Mails und Anhänge werden auf Spam, Viren sowie andere Bedrohungen überprüft, die in der Filterrichtlinie definiert sind.
- Definierte Tests und Maßnahmen werden auf die E-Mails angewandt.
- E-Mails werden entweder zur Zustellung an den vorgesehenen Empfänger oder zur Prüfung in Quarantäne geleitet oder gelöscht.

Ausgehende E-Mails:

- E-Mails werden von internen Mailservern zu den Appliances geleitet.
- E-Mails und Anhänge werden auf Viren sowie andere Bedrohungen überprüft, die in der Filterrichtlinie definiert sind.
- Definierte Tests und Maßnahmen werden auf die E-Mails angewandt.
- E-Mails werden zum integrierten MTA zur externen Zustellung weitergeleitet oder zur Prüfung in Quarantäne.

Beim erstmaligen Einrichten können Administratoren festlegen, ob die empfohlenen standardmäßigen E-Mail-Richtlinien und -Maßnahmen, inkl. TLS-Verschlüsselung für ausgehende E-Mails, aktiviert werden sollen. Mithilfe der webbasierten Management-Konsole können Standards zu

Hinweis

Sophos E-Mail Appliances versenden weder ein- oder ausgehende E-Mails, die mit einem bekannten Virus infiziert sind, noch geben sie infizierte E-Mails aus der Quarantäne frei.

jeder Zeit modifiziert und anwenderspezifische Tests und Maßnahmen eingerichtet werden. (Weitere Informationen dazu entnehmen Sie bitte dem Abschnitt *Richtlinien* in Kapitel 3).

Es gibt folgende Optionen zum Zustellen von E-Mails:

Eingehend und ausgehend (falls nicht anders festgelegt):

- Weiterverarbeiten
- Sofort zustellen
- Isolieren (in die Quarantäne verschieben)
- Isolieren und fortfahren
- Isolieren, Anhänge entfernen und fortfahren
- Betreff markieren und fortfahren
- Löschen
- Abweisen (nur ausgehend)
- Umleiten
- Banner hinzufügen
- Header hinzufügen/ersetzen
- Benachrichtigen
- Umleiten
- Kopieren

Management-Konsole und Dashboard

Die Management-Konsole ist die sichere, webbasierte grafische Benutzeroberfläche der Appliance für den Systemadministrator. Mit ihr können Sie:

- System- und Netzwerkeinstellungen konfigurieren
- Cluster mit bis zu 10 Appliances zusammenstellen oder eine neue Appliance zu bestehendem Cluster hinzufügen
- Spamschutz-, Virenschutz- sowie Inhaltsrichtlinien konfigurieren
- Systemstatus und Diagnoseunterbrechungen überwachen
- Quarantäne verwalten
- E-Mail-Protokolle, Warteschlangen und Quarantäne nach „verlorenen“ E-Mails durchsuchen
- Echtzeit-Reports generieren
- Bestimmte administrative Aufgaben delegieren und Endnutzer-Oberflächenfunktionen steuern
- Konfiguration für eine Ausfallsicherheit mit zwei Einheiten einrichten und verwalten

Mit drei Mausklicks zum Ziel

Die Bedienung ist auf ein absolutes Minimum reduziert: Keine Funktion der Management-Konsole erfordert mehr als drei Mausklicks oder gar den Aufruf einer Eingabeaufforderung.



Abbildung 3: Dashboard der Management-Konsole

Das Dashboard, die Startseite der Konsole (siehe Abb. 3), liefert eine Zusammenfassung der gesamten Systemperformance auf einen Blick. Über das Dashboard kann der Administrator den Schutzstatus ermitteln, E-Mail-Durchsatz und -Volumen prüfen und die Systemverfügbarkeit sicherstellen. Weitere Details über die leistungsstarken, benutzerfreundlichen Management-Tools finden Sie in Abschnitt 4.

Clustering

Mehrere Appliances können für erhöhte Skalierbarkeit, bessere Verfügbarkeit und einfachere Verwaltung zu einem Cluster verbunden werden.

Skalierbarkeit: Über die Cluster-Funktion können Administratoren Appliances schnell und einfach zu einem Cluster hinzufügen und so steigenden E-Mail-Traffic am Gateway ohne zusätzliche Verwaltungskosten abwickeln.

Verfügbarkeit: Clustering sorgt für mehr freie Kapazitäten bei der E-Mail-Verarbeitung. Fällt eine Appliance aus, hat dies keinen Einfluss auf die E-Mail-Verarbeitung der anderen Appliances im Cluster. Auch FTP-Konfigurations-Backup, Verzeichnis-Synchronisation und Endnutzer-Quarantänen innerhalb eines Clusters sind nach Ausfall einer Appliance weiterhin verfügbar.

Vereinfachte Verwaltung: Durch die zentrale Verwaltung aller Appliances in einem Cluster können Administratoren Daten zu Dashboard, Reports, Quarantäne, Protokoll und Warteschlange für das gesamte Cluster und ganz wie bei einer größeren Appliance einsehen. (Alle Informationen können auch für jede Appliance separat eingesehen werden.) Endnutzer-Funktionen wie E-Mail-Quarantäneberichte und Quarantäne-Internetzugriff für Endnutzer besitzen die gleiche Funktionalität wie in Umgebungen mit nur einer Appliance.

Quarantäne

Die Quarantäne gewährleistet sicheres Speichern von unerwünschten oder potenziell gefährlichen ein- oder ausgehenden E-Mails. Jede E-Mail, die gegen eine Sicherheitsrichtlinie verstößt, (z.B. aufgrund von Viren, Spam, bestimmten Stichwörtern oder Inhalten) kann in Quarantäne verschoben werden, wo der Systemadministrator sie prüft oder optional zum Empfänger (eingehend) bzw. zum Absender (ausgehend) geleitet werden. Der Prüfer kann dann entscheiden, die in Quarantäne verschobenen E-Mails freizugeben oder zu löschen, mit Ausnahme der E-Mails, die einen Virus enthalten.

Integrierter Speicher

Die eingebaute Quarantäne ist ein leistungsstarker E-Mail-Speicher, der Millionen von E-Mails speichern kann. Anders als bei vielen konkurrierenden Lösungen, befindet sich die Quarantäne direkt auf der Appliance und nicht auf einem anderen Server. Daraus ergibt sich ein doppelter Vorteil: Es ist kein zusätzliches externes Speichern und kein zusätzliches Quarantäneverwaltungs-System oder -Benutzeroberfläche erforderlich. Administratoren greifen auf die Quarantäne mit derselben Management-Konsole zu, mit der auch alle anderen Systemfunktionen verwaltet werden.

Sicherheit leicht gemacht

Wenn keine Alarme von der Appliance generiert werden, dann arbeitet die E-Mail-Sicherheit erwartungsgemäß und es besteht keine Veranlassung, einzugreifen.

Delegierte Verwaltung

Administratoren können auch spezielle Helpdesk-Konten erstellen, um die Quarantäneverwaltung an andere Systemadministratoren zu delegieren, ohne dabei alle Systemkonfigurations-Optionen anzuzeigen. So können Helpdesk-Administratoren alle internen Anfragen nach verlorenen oder fehlenden E-Mails bearbeiten und dem leitenden Administrator bleibt Zeit, sich auf andere Prioritäten zu konzentrieren.

Der Administrator kann es den vorgesehenen Empfängern von eingehenden E-Mails und den Verfassern von ausgehenden Mails ermöglichen, die in Quarantäne verschobenen E-Mails einzusehen. Dies geschieht entweder über einen E-Mail-Digest oder eine webbasierte Benutzeroberfläche. In beiden Fällen können nur ihre eigenen persönlichen E-Mails angesehen werden. Ist die webbasierte Benutzeroberfläche aktiviert, können Administratoren auch Empfänger dazu berechtigen, persönliche Allow- und Block-Lists zu erstellen und sich von der Spamprüfung abzumelden.

Überwachung, Alarmer und Benachrichtigungen

Die Sophos E-Mail Appliances verfügen über eine hochentwickelte Technik, die dafür konzipiert wurde, den Verwaltungsaufwand zu verringern. Automatische Wartung und ein umfassendes Überwachungssystem, das mehr als 40 verschiedene Funktionen regelmäßig kontrolliert, garantieren eine höhere Leistung mit geringerem Aufwand.

Vorbeugende Maßnahmen

Im Falle eines Systemausfalls sendet die Appliance E-Mail-Alarmer zur Fehlerbehebung an den Systemadministrator und ändert die Farbe des Hauptanzeigers für den Systemstatus in der Management-Konsole. Handelt es sich um eine unternehmenskritische Störung, für deren Behebung externe Unterstützung erforderlich ist, z.B. beim Ausfall eines Netzgeräts, wird auch ein Alarm an Sophos gesendet. Die Behebung einer solchen Störung kann von Sophos häufig schon initiiert werden, bevor der Administrator überhaupt etwas bemerkt (z.B. Lieferung eines Ersatznetzgerätes*).

Für ein noch größeres Maß an Sicherheit und Vertrauen verwendet Sophos eine innovative, Remote-Funktionsüberwachung. Sie garantiert, dass jede installierte Appliance aktuelle Bedrohungskenntnisse und Software-Updates nach Zeitplan herunterlädt. Schlägt das Herunterladen oder Anwenden eines Updates bei einer Appliance fehl, wird der Administrator informiert. Sollte diese Funktion mehr als dreimal innerhalb von 15 Minuten fehlschlagen, so alarmiert die Appliance auch den Sophos Support. Sollte eine Appliance länger als zwei Stunden keine Updates heruntergeladen haben, erhalten Sie einen Anruf vom Sophos Support.

Spamschutz

Die einzigartige Methode, mit der Sophos Spam identifiziert, repräsentiert die fortschrittlichsten Erkennungsverfahren – entwickelt von den SophosLabs – in der IT-Branche rund um die Uhr das ganze Jahr über. In der ganzen Welt verfügen SophosLabs über Spamfallen, die täglich

Bewährter Spamschutz

Sophos E-Mail Appliances erkennen bis zu 99,4% aller Spam-Mails bereits am E-Mail-Gateway.

EVisionIT Labs, Oktober 2007

Millionen von E-Mails prüfen. Diese Spamfallen ermöglichen eine eingehende Sichtung der E-Mails und geben Einblick in den globalen E-Mail-Verkehr. Auf Basis dieser ständigen Überwachung lassen sich zwei Spam-Kategorien identifizieren: hoch und mittel. Administratoren können die standardmäßigen Bearbeitungsregeln für diese Kategorien auswählen oder spezielle Regeln erstellen, die auf den internen Anforderungen basieren. Sophos kümmert sich also um die Spam-Bewältigung, damit Sie sich auf andere Aufgaben konzentrieren können.

Reputation Filtering

Der erste Abwehrmechanismus vor Spam und Malware ist Schutz auf Verbindungsebene. Das Sender Genotype-Verfahren führt bereits bei Verbindungsherstellung eine Überprüfung auf Botnet-Indizien durch und deckt so auch E-Mails von bisher unbekanntem Spammern auf. In Kombination mit unserer Reputation Filtering-Technologie, die bekannte Spammer-IP-Bereiche auf MTA-Ebene noch vor der Überprüfung blockiert, werden 90% aller eingehenden Spam-Mails, insbesondere der zunehmende E-Mail-Durchsatz, ohne zusätzliche Investitionen in die Infrastruktur eliminiert. Ebenso kann die Appliance die E-Mail bis zur MTA-Ebene passieren lassen, damit sie erst unmittelbar vor der Überprüfung den Reputation Filter durchläuft (siehe unten). E-Mails, die auf dieser Stufe als von bekannten unerwünschten Sendern erkannt werden, werden ebenso behandelt wie andere E-Mails, die mithilfe der Sophos-Spamtests als Spam identifiziert sind und entsprechend der spezifizierten Sicherheitsrichtlinie behandelt werden.

Bei der Überprüfung wird eine Vielzahl von Filterungsmethoden angewandt, die Hunderte von verschiedenen Tests miteinander kombinieren, um so Taktiken zu entlarven, die die Filterfunktion zu umgehen suchen. Ein Test sucht nach vielen unterschiedlichen Arten (mehr als 5,6 Milliarden) der Buchstabierung von „Viagra“. Wird ein Spamindikator ausgelöst, so trägt das Ergebnis zur gesamten Spam-Wahrscheinlichkeit dieser E-Mail bei. Headers, Struktur und Inhalt von E-Mails sowie Call-to-Call-Action URIs (Uniform Resource Identifiers, d.h. Website, E-Mailadresse, Dateiname etc.) werden ebenfalls auf Tausende von unterschiedlichen Aspekten überprüft.

Einige Spamerkenntnis-Verfahren:

- Sensoren zur Erkennung bekannter Sicherheitsbedrohungen, die vor Scams schützen, wie zum Beispiel Phishing-Attacken, die Benutzer zur Eingabe persönlicher bzw. finanzieller Daten verleiten
- Sender Genotype-Analyse zur Eliminierung von Botnet-Spam auf IP-Verbindungsebene
- Genotype-Kampagnen-Analyse, mit der komplexe Spam-Kampagnen identifiziert werden. Dies geschieht durch das Erkennen von Merkmalen, die eine Reihe von E-Mails gemeinsam haben
- Sensoren, die anstößige, pornografische oder andere Inhalte delikater Natur erkennen
- Fingerprinting-Verfahren zur Erkennung und Abwehr von Spam, der in Bildern und Dateianhängen (PDF, Excel u.a.) enthalten ist
- Nachverfolgung der Spammer-Vermögenswerte, um die Website-Betreiber zu identifizieren und unerwünschte E-Mails zu blockieren
- Ziel-URI-Filterung, um E-Mails an zweckentfremdete, freeweb und

sonstige Werbe-Websites zu blockieren

Verschleierungssensoren, um die von Spammern verwendeten Methoden zu identifizieren, mit denen sie ihre E-Mails vor Spamfiltern verbergen wollen.

Sophos SXL

Nur Sophos E-mail Security and Data Protection-Lösungen – zu der auch die Sophos E-Mail Appliances zählen – bieten SXL. Diese Technologie bietet sekundengenauen Spamschutz durch Echtzeit-Netzwerkprüfungen auf die neuesten Spamdaten der SophosLabs. SXL-Server enthalten nicht nur die neuesten Daten aus den SophosLabs, sondern auch ältere, zurzeit nicht genutzte Spamdaten (z.B. IP-Adressen von Botnets oder Ziel-URLs), die wertvollen lokalen Speicherplatz in Anspruch nehmen würden. Mit SXL profitieren Sie vom ständig wachsenden Volumen an Spamdaten, ohne dass Sie diese lokal in Ihrem Netzwerk unterbringen müssten.

Die SophosLabs analysieren eingehende Spam-E-Mails über ein Netzwerk aus so genannten „Traps“, senden die Schutzdaten an SXL-Server und lassen die Appliances alle fünf Minuten automatisch aktualisieren. Dies gewährleistet einen immer aktuellen Schutz vor der neuesten Spammer-Aktivität, ohne den geringsten Verwaltungsaufwand.

Eine weitere, dem Administrator zur Verfügung stehende Option (standardmäßig aktiviert), ist der automatische Schutz vor Denial-of-Service- und Directory Harvest-Attacks (DoS und DHA). Ist diese Option aktiviert, kann die Appliance eingehenden Verkehr unterdrücken und eingehende Verbindungen blockieren, die häufig auf solch einen Angriff hinweisen.

Zusätzliche angepasste Spam-Einstellungen

Die Appliances verfügen über zwei Antispam-Mechanismen – Allow-Listen und Block-Listen – zur weiteren Anpassung der Richtlinie für eingehende E-Mails.

Allow-Listen: Ein optionales Element des Spamfilters ist das Verwalten der Allow-Listen in einem Unternehmen. Sie enthalten Senderadressen oder -Domänen, die als sicher gelten und nicht als Spam herausgefiltert werden. Das Hinzufügen von Adressen und Domänen vertrauenswürdiger Sender in Allow-Listen eliminiert das Risiko, dass ihre E-Mails ungewollt vom Spamfilter aussortiert werden und führt außerdem dazu, dass der Filter verdächtige E-Mails eingehender prüft. Wenn Allow-Listen aktiviert sind, können sie global und auf einzelne E-Mail-Konten angewandt werden.

Block-Listen: Das Gegenstück zur Allow-Liste ist die Block-Liste. Sie enthält Senderadressen oder -Domänen die als „gefährlich“ oder unerwünscht gelten und aus diesem Grund ausgesondert werden. Das Hinzufügen von Adressen in die Block-Liste verringert das Aufkommen von E-Mails, die eine vollständige Überprüfung durchlaufen müssen. Dabei wird der Durchsatz verbessert und die Systemleistung gesteigert. Wenn Block-Listen aktiviert sind, können sie sowohl im gesamten Netzwerk als auch auf einzelne E-Mail-Konten angewandt werden.

Administratoren können Benutzern erlauben, sich von der Spamprüfung abzumelden, doch was am allerwichtigsten ist, die Virenprüfung kann nicht deaktiviert werden.

Zero-Day-Schutz

Sophos E-Mail Appliances schützen vor sich rasch verbreitenden Bedrohungen wie Internetwürmern, die Schaden anrichten können, noch bevor eine spezifische Erkennung verfügbar ist.

Virenschutz

Die Wahrscheinlichkeit, dass sich ein Virus über den E-Mail-Gateway in ein Unternehmensnetzwerk einschleicht, ist höher als über einen anderen Weg. Virenschutz am E-Mail-Gateway ist die erste Schutzinstanz, schützt das gesamte Unternehmen an einem einzelnen Punkt und ermöglicht dank einfacher Updates nahtlosen Schutz. Sophos E-Mail Appliances integrieren die marktführende Sophos Virus Detection Engine, damit Unternehmen vor Viren geschützt sind, die über E-Mails ins Unternehmen gelangen.

Die Appliances prüfen den gesamten E-Mail-Verkehr in Echtzeit, der den E-Mail-Server passiert und garantieren so Schutz vor Massmailing-Würmern und Viren, einschließlich der neuesten Mischbedrohungen, in welchen Viren, Spam und Denial-of-Service-Attacken miteinander kombiniert werden.

Zero-Day-Schutz

Durch den fortschrittlichen, proaktiven Schutz der SophosLabs bleiben Sie von Zero-Day-Bedrohungen und -Infektionen verschont. Genotype-Technologie erkennt neue Varianten von Virenfamilien und liefert in bis zu 90% der Fälle präventiven Schutz, noch bevor eine spezifische Erkennung verfügbar ist. Die Appliances prüfen automatisch ausführbare Inhalte und Dateien in E-Mails auf schädliche Codes und wenden die entsprechende Richtlinie zur Bearbeitung der E-Mail-Maßnahmen an, um schnellen und zuverlässigen Schutz zu gewährleisten.

Perimeterschutz

Denial Of Service- und Directory Harvest-Attacken (DoS- und DHA-Attacken) sind Sicherheitsbedrohungen, die zur Überlastung von internen Systemen und Gateway-Systemen führen. Um Sie vor diesen Bedrohungen zu schützen, messen die Sophos E-Mail Appliances die E-Mail-Frequenz und können so abweichende Muster erkennen, die das typische legitime E-Mail-Aufkommen des Unternehmens von allen oder einem bestimmten Absender übersteigt. Diese Überwachung ermöglicht es, DoS und DHA-Attacken zu erkennen und entsprechend darauf zu reagieren.

Data Leakage Prevention

Verstöße gegen den Datenschutz, Haftbarkeit und Produktivitätsverlust sowie Rufschädigung können Unternehmen jährlich mehrere Millionen Euro kosten. Komplexe und sich weiterentwickelnde regulative Umgebungen machen es erforderlich, dass Unternehmen sich selbst durch folgende Maßnahmen schützen: Überwachung und Durchsetzung geeigneter Richtlinien und Verfahren sowohl auf Endnutzer- als auch auf Infrastrukturebene.

Mit dem Richtliniengerüst der Appliance können Sie eine klare Richtlinie zur Abwicklung aller am Gateway ein- und ausgehenden E-Mails und Inhalte durchsetzen. Der Administrator kann eine Auswahl an Richtlinienmaßnahmen über die Management-Konsole konfigurieren. Häufig von Unternehmen durchgesetzte Richtlinien erfüllen folgende Funktionen:

- Zurückweisen von E-Mails bekannter unerwünschter Absender
- Festlegung von Allow- und Block-Listen (global und einzeln)
- Isolieren von E-Mails mit anstößigen Inhalten

Schutz rund um die Uhr

Die SophosLabs™, unser Netzwerk aus Bedrohungsanalysecentern in der ganzen Welt, identifizieren und untersuchen auftretende Bedrohungen rund um die Uhr.

- Isolieren und Untersuchen von E-Mails mit bestimmten Anhängen, um die Preisgabe geistigen Eigentums oder vertraulicher Daten zu verhindern
- Einfügen eines Banners in Kopf- und/oder Fußzeile von E-Mails
- Inhaltsabhängiges Umleiten von E-Mails
- Überwachen und Protokollieren verdächtigen E-Mail-Verkehrs, um Systemmissbrauch zu erkennen

Eine vollständige Liste der Richtlinienvoreinstellungen finden Sie in Anhang I.

Zusammenfassung

Sophos E-Mail Appliances verfügen über die ideale Mischung von Automatisierung und Steuerung, um die Anforderungen der E-Mail-Verwaltung in Unternehmen zu unterstützen. Sie vereinen automatische Bedrohungs-Updates mit einfacher Verwaltung und Versendung von Alarmen. Die Kombination dieser Funktionen minimiert den täglichen Administrationsaufwand und sorgt für Übersicht und Kontrolle.

Sophos E-Mail Appliances basieren auf den umfangreichen Ressourcen der SophosLabs in der ganzen Welt. Die SophosLabs sind Bedrohungen durch E-Mail-Viren ständig ausgesetzt und dadurch in der Lage, proaktiven Schutz durch schnellere Analyse neuer Bedrohungen, mehrere Erkennungs-/Aktualisierungsmethoden (wie Viren-, Spam- oder Richtlinien-Updates) sowie die vollständige Verwaltung des gesamten Bedrohungskreislaufs zu ermöglichen.

Sophos E-Mail Appliances bietet Unternehmen folgende Vorteile:

- Zuverlässiger Schutz vor neuen Bedrohungen, Virenvarianten und entstehenden Spam-Kampagnen
- Reduzierter Administrationsaufwand
- Gewissheit darüber, dass die Infrastruktur geschützt ist

3: SETUP

Übersicht

In diesem Abschnitt werden grundlegende Appliance-Einstellungen wie Konfiguration, Verzeichnis-Einrichtung, Endnutzer-Präferenzen sowie Standardrichtlinien behandelt. Dieser Abschnitt soll das Handbuch nicht ersetzen, sondern vielmehr aufzeigen, wie einfach und benutzerfreundlich die Administration der Appliance aufgebaut ist.

Konfiguration

Die Konfiguration der Sophos E-Mail Appliances ist leicht und unkompliziert. Der Setup-Assistent führt den Administrator durch die grundlegende Konfiguration, so dass Ihnen bereits in 15 Minuten die Live E-Mail-Überprüfung zur Verfügung steht.

Die Konfigurationskategorien sind in Abbildung 4 dargestellt.

Administratoren können die Einstellungen jederzeit über die Management-Konsole ändern.

Schnelles und einfaches Setup

Ein Setup-Assistent hilft Ihnen dabei, die Appliance in weniger als 15 Minuten zu installieren und in Betrieb zu nehmen.

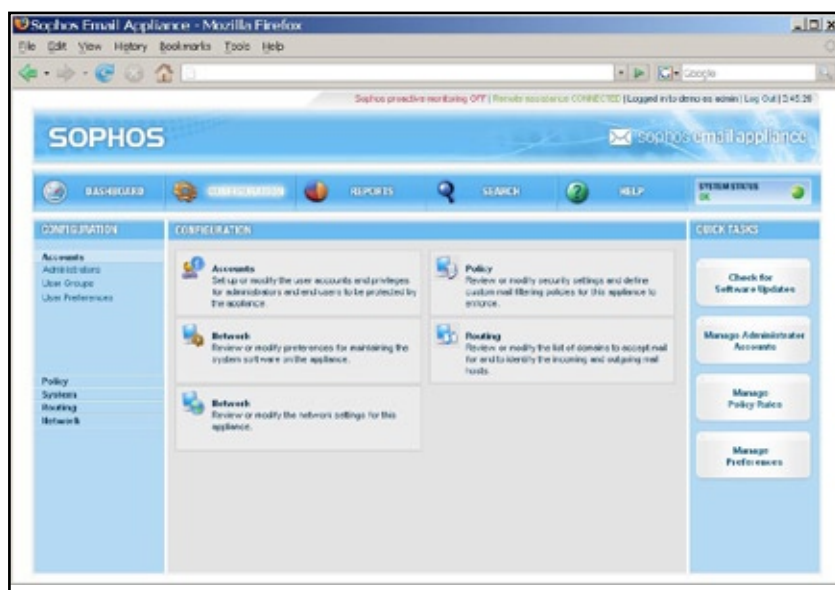


Abbildung 4: Konfigurationsseite

Verzeichnisdienste

Die Appliances ermöglichen ein rasches Einrichten von Benutzern und Benutzergruppen durch LDAP-Integration mit Active Directory® von Microsoft. Mit diesem Verfahren können Empfänger leichter geprüft und E-Mail-Richtlinien für spezifische Benutzer und Benutzergruppen erstellt werden.

Auf der Konfigurationsseite „Directory Services“ kann der Administrator LDAP-Einstellungen automatisch suchen und importieren lassen oder die Einstellungen manuell vornehmen. Die Appliance verfügt über eine lokale Version von Active Directory, um die Funktionalität zu gewährleisten und Ausfallzeiten zu vermeiden, wenn der Active Directory-Server nicht zur Verfügung steht. Administratoren können einen Zeitplan für die Synchronisation erstellen und so sicherstellen, dass die Appliance die aktuellste Version verwendet.

Benutzergruppen können manuell oder über LDAP eingerichtet werden.

“ Es dauerte länger, die Appliance aus dem Karton zu holen und aufzubauen, als sie zum Laufen zu bringen. ”

Noe Arzate, Mount Pleasant Independent School District



Abbildung 5: Konfigurieren der Verzeichnisdienste

Endnutzer-Präferenzen

Die Appliances verfügen über Smart-Funktionen, mit denen sich E-Mail-Benutzer einrichten und verwalten lassen. Mit der vollständigen Integration von LDAP können Administratoren schnell und einfach Benutzerrechte einrichten, wie beispielsweise:

- Authentifizierung
- Allow-Listen und Block-Listen
- Quarantänezugriff über E-Mail-Digest oder webbasierte Benutzeroberfläche
- Bevorzugte Sprache für Benutzeroberfläche
- E-Mail-Zustellungsfrequenz
- Abmeldung von der Spamprüfung

Lesen Sie mehr über die Quarantäne-Zugriffsoptionen unter *Endnutzer-Optionen* in Kapitel 4: „Verwaltung der Appliances“.

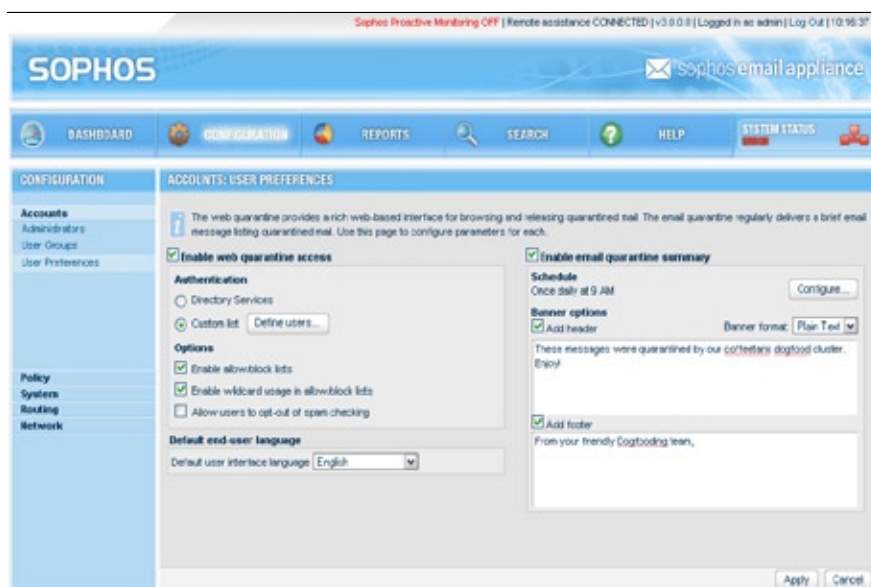


Abbildung 6: Endnutzer-Präferenzen

Richtlinien

Sophos E-Mail Appliances wurden dafür entwickelt, maximale Sicherheit bei minimalem Administrationsaufwand zu garantieren. Die große Erfahrung in Bezug auf das Erkennen von Viren, Spam und anderen Malware-Typen macht es Sophos möglich, Appliances mit Richtlinienvoreinstellungen auszustatten, die ein Höchstmaß an Sicherheit sowie eine geradlinige Systemkonfiguration bieten. Sollte jedoch eine Anpassung erforderlich sein, geht dies mit der Management-Konsole ganz einfach (siehe Abbildung 8).

Virenschutzrichtlinie

Eingehende E-Mails, die Viren enthalten, können entsprechend ihrer Bedrohungsart verwaltet werden:

- Virus
- Nicht überprüfbarer Anhang
- Verschlüsselter Anhang
- Verdächtiger Anhang

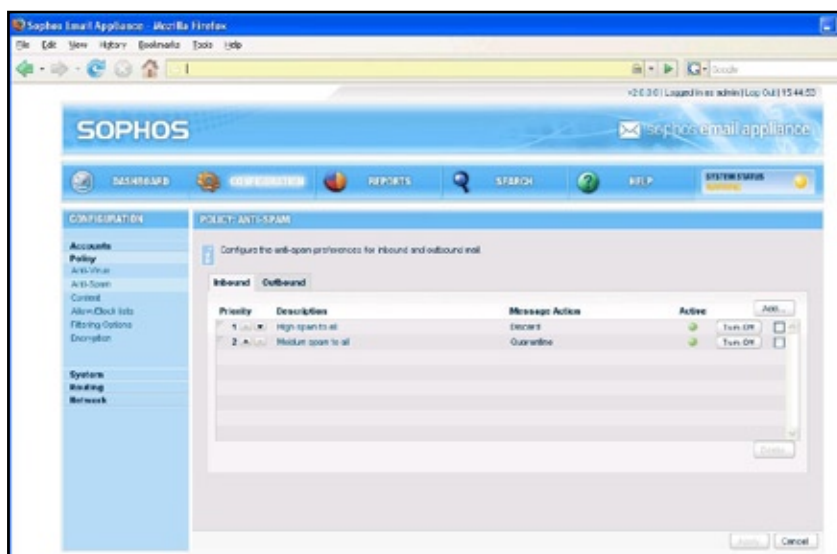


Abbildung 7: Hauptseite der Virenschutzrichtlinie

Für eingehende und ausgehende E-Mails lassen sich bis zu 20 separate Regeln und Maßnahmen einrichten. Es steht eine Reihe von Maßnahmen zur Auswahl, z.B. Benachrichtigung (Meldung an Personalabteilung bei Erkennung anstößigen Inhalts oder an Rechtsabteilung bei Erkennung von Patentinformationen) und die Änderung von Bannern und Headern. Diese Maßnahmen ermöglichen eine umfassende Durchsetzung der in Ihrem Unternehmen geltenden Nutzungsbedingungen.

In Anhang I finden Sie eine vollständige Liste der Richtlinienvoreinstellungen.

Spamschutzrichtlinie

Standardmäßig werden E-Mails von bekannten schädlichen Sendern bzw. mit hoher Spam-Wahrscheinlichkeit durch die Appliance gelöscht, E-Mails mit mittlerer Spam-Wahrscheinlichkeit werden in Quarantäne verschoben. Diese Einstellungen können entsprechend den ActiveDirectory-Gruppen- oder Anwenderlisten geändert werden.

In Abbildung 8 sehen Sie die Hauptseite der Spamschutzrichtlinie in der Management-Konsole. Über diese Seite können Sie bis zu 20 verschiedene Spamschutzregeln erstellen und verwalten. So stellen Sie sicher, dass Ihre Sophos E-Mail Appliance die Anforderungen Ihres Unternehmens erfüllt.

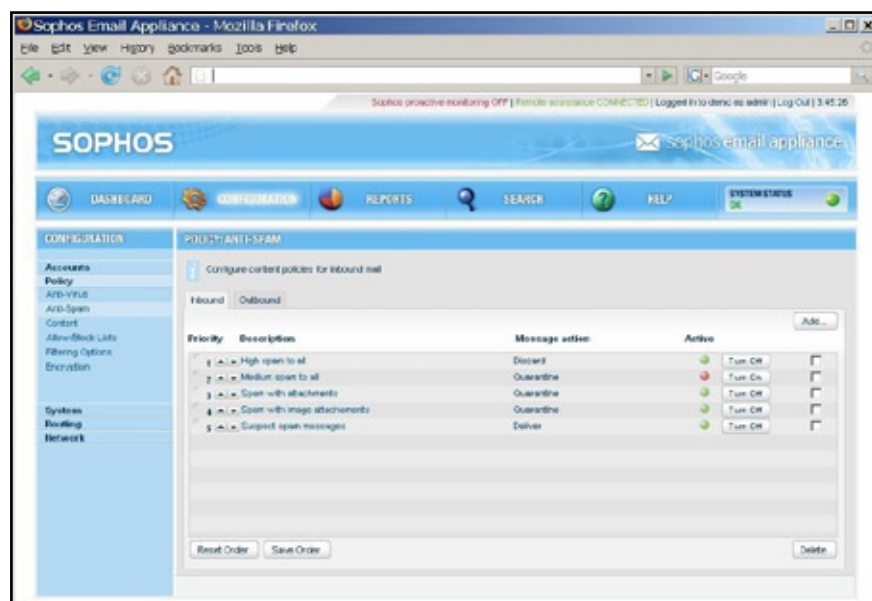


Abbildung 8: Hauptseite der Spamschutzrichtlinie

Inhaltsrichtlinie

E-Mails enthalten häufig Inhalte, die für das Unternehmen interne und gesetzliche Haftungsansprüche bedeuten können. Daher ist es wichtig, dass Ihre Sicherheitslösung allgemeine Nutzungsbedingungen durchsetzen kann. Um Missbrauch zu vermeiden, prüft das Filterungssystem E-Mails und Anhänge auf anstößigen Text, bestimmte Stichwörter und Dateitypen. So behalten Sie stets die Kontrolle über Ihren gesamten E-Mail-Verkehr.

Mit dem integrierten Richtlinienassistenten (siehe Abbildung 9) können Sie bis zu 40 Regeln zur Überwachung von Attributen wie Anhangstyp und Inhalt speziell (in regulären Ausdrücken und Zeichenfolgen mit Platzhaltern) speziell für Ihr Unternehmen oder Ihre Branche festlegen.

Der Administrator kann für jeden Inhalts-Filtertyp sowie für ein- und ausgehende E-Mails folgende Maßnahmen einrichten:

Weiterverarbeiten

- Sofort zustellen
- Löschen
- Isolieren (in Quarantäne verschieben)
- Isolieren und fortfahren
- Umleiten
- Betreff markieren und fortfahren
- Umleiten
- Kopieren

Beim Einrichten dieser Regeln und Maßnahmen können Sie wählen, ob diese, entsprechend der Festlegung durch den Active Directory-Server oder einer Anwenderliste, auf bestimmte Benutzer und/oder Benutzergruppen im Unternehmen angewandt werden sollen. Einzel- oder Gruppenausnahmen lassen sich ebenfalls spezifizieren. Mit weiteren Optionen können E-Mails, die gegen Richtlinien verstoßen, als Kopie, Blindkopie oder als umgeleitete E-Mail an eine spezifizierte E-Mail-Adresse geleitet werden (z.B. an einen für die Einhaltung von Richtlinien verantwortlichen Bearbeiter), Sender/Empfänger können kopiert und eine Zustellungsbenachrichtigung kann hinzugefügt werden. Ein individuelles Banner kann in der Kopf- oder Fußzeile der E-Mail hinzugefügt werden.

Sie können eine Obergrenze für die Größe von E-Mails festlegen (2 MB bis 50 MB), um so Speicherplatz auf der Appliance und auf Downstream-Servern zu sparen.

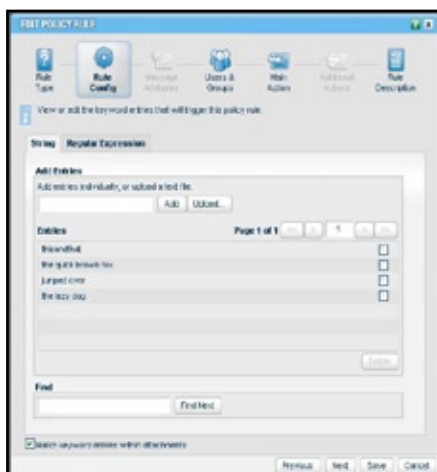


Abbildung 9: Anpassen der Richtlinie für ausgehende E-Mails



1. Schritt: Regeltyp

Wählen Sie einen Typ für die Inhaltsregel. Zu den Optionen gehören Banner, Stichwort, Anhang, Sprache, Überwachungsliste, Hostnamen-/IP-Adressenliste und diverse E-Mail-Attribute (z.B. Größe).



2. Schritt: Regelkonfiguration

Geben Sie für den ausgewählten Regeltyp weitere Details ein. Wenn es sich zum Beispiel um eine Stichwörter-Regel handelt, lassen sich auf dieser Seite die Stichwörter festlegen.



3. Schritt: E-Mail-Attribute

Hier legen Sie E-Mail-Attribute, wie die Größe, fest.



4. Schritt: Benutzer und Gruppen

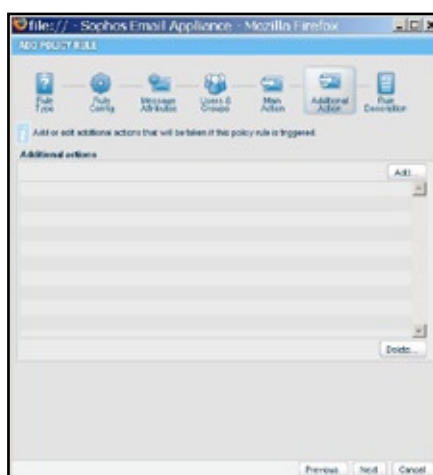
Legen Sie fest, für welche Benutzer und/oder Gruppen die Regel greifen soll. Es lassen sich separate Listen für Sender und Empfänger einrichten.





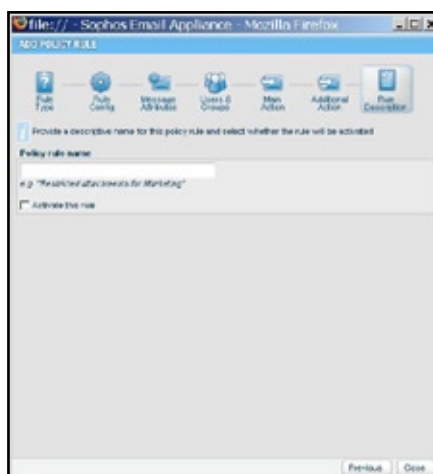
5. Schritt: Maßnahme

Hier legt der Administrator fest, welche Maßnahme stattfinden soll, wenn die Regel greift. Eine Liste der Maßnahmen finden Sie auf Seite 9.



6. Schritt: Weitere Maßnahmen

Hier lassen sich weitere Maßnahmen festlegen, z.B. das Einrichten von Bannern, Headern und Benachrichtigungen.



7. Schritt: Regelbeschreibung

Benennen Sie die Regel und bestimmen Sie, ob sie aktiviert werden soll. Die Aktivierung und Priorisierung von Regeln ist auch auf den Hauptseiten für Viren, Spam und Inhalt möglich.



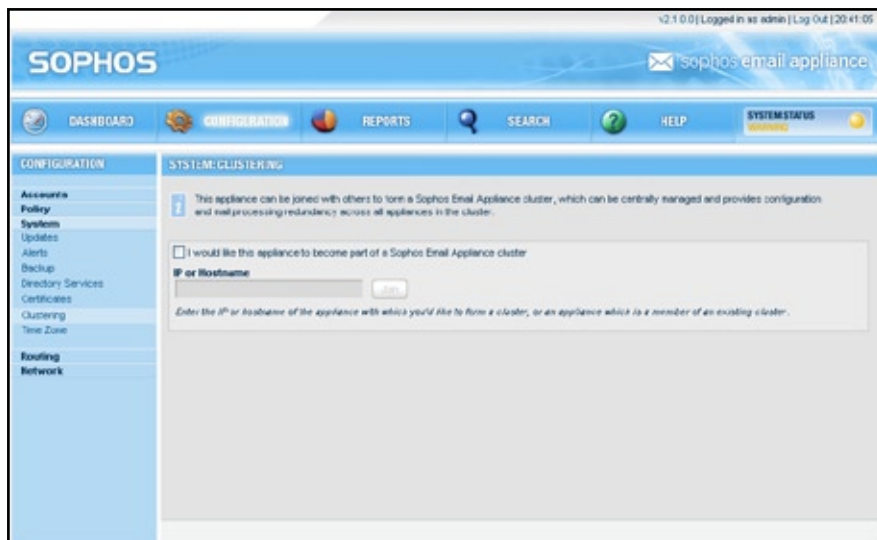


Abbildung 10: Appliance zu Cluster hinzufügen

Clustering

Wenn Sie mehr als eine Appliance installieren, brauchen Sie nur den Hostnamen und die IP- Adresse der zuerst konfigurierten Appliance einzugeben und im Abschnitt "Clustering" des Installations-Wizards auf "Join" zu klicken. Die Synchronisation sämtlicher Konfigurationen erfolgt automatisch.

Zusammenfassung

Sophos E-Mail Appliances verfügen über solide standardmäßige Richtlinieneinstellungen für Viren- und Spamschutz sowie für E-Mail-Inhalte. Darüber hinaus können diese Richtlinien problemlos an die spezifischen Anforderungen Ihres Unternehmens angepasst werden. Ob Sie nur einfachen Schutz vor Spam und Malware benötigen oder komplexere Verfahren zur Vermeidung von Datenverlust per E-Mail, Sie erhalten in jedem Fall eine umfassende Unternehmenslösung zum Schutz des internen E-Mail-Verkehrs bei minimalem Aufwand.

4: VERWALTUNG DER APPLIANCES

Übersicht

Mit Sophos E-Mail Appliances werden Administration und Kontrolle Ihres E-Mail-Gateways fast zum Kinderspiel. Sie verfügen über eine große Auswahl an Tools und Einstellungen, mit denen viele Administrationsaufgaben beseitigt oder automatisiert werden.

Am besten gehen Sie vom Konzept der „Managed Appliance“ aus. Dies heißt ganz einfach, dass Sie, wenn Sie keine Alarme oder Benachrichtigungen von der Appliance (oder von Sophos) erhalten, davon ausgehen können, dass alles soweit in Ordnung ist und keine Maßnahmen oder Eingriffe erforderlich sind. Ihre Appliance benachrichtigt Sie nur bei Auffälligkeiten. Sie können getrost Ihren täglichen Aufgaben nachgehen und darauf vertrauen, dass der E-Mail-Gateway sicher und effizient arbeitet.

Die Appliances reduzieren den administrativen Aufwand mithilfe eines komplizierten Netzwerks von mehr als 40 eingebauten Systemsensoren. Sobald ein Sensor ausgelöst wird, geht ein Dashboard-Alarm und/oder ein E-Mail-Alarm an den Administrator. Mit der Anmeldung und einem Klick auf die Schaltfläche „Systemstatus“ erhalten Sie rasch eine übersichtliche Darstellung der Situation und empfohlene Lösungsschritte.

Dieser Abschnitt umreißt kurz die täglichen administrativen Aufgaben zum Verwalten Ihrer Appliance.

*Weniger
Verwaltungsaufwand*

Mehr als 40 Systemsensoren
überwachen die Appliance für Sie.

Statusprüfungen

Sie können den Gesamtstatus der Appliance sofort bestimmen, indem Sie sich auf der Management-Konsole anmelden und den Systemstatus-Anzeiger prüfen, der auf jeder Seite rechts oben angezeigt wird (siehe Abbildung 11). Grün bedeutet, dass alle Systeme normal laufen. Gelb weist auf eine vorübergehende, schwache Störung hin. Rot zeigt eine kritische Störung an. (Im Falle einer kritischen Störung sendet die Appliance einen E-Mail-Alarm an den benannten technischen Kontakt und an Sophos).

Mit einem Klick auf die Systemstatus-Anzeige rufen Sie die Systemstatus-Seite auf, der Sie Details über folgende Umgebungsmerkmale entnehmen können:



Abbildung 11: Systemstatus-Anzeige auf der Management-Konsole

- **Mail flow:** Spitzen im E-Mail-Volumen, in blockierten E-Mails, Spam und Viren
- **Quarantine:** Größe des integrierten E-Mail-Speichers
- **Software:** Prozessüberprüfung, Schutzstatus, Verbindung zu Sophos, Neustart des Systems und System-Updates
- **Hardware:** Leistung der Hardware-Komponenten, Temperatur, Speicherverbrauch u.a.
- **Certificates:** Status der Zertifikate für TLS-Verschlüsselung oder Endnutzer-Authentifizierung.
- **Licensing:** Restlaufzeit der Software-Lizenz.

Wie Sie Abbildung 12 entnehmen können, zeigt die Systemstatus-Seite den Indikator für jeden Monitor, eine Benachrichtigung, die den aktuellen Status erklärt, sowie Korrekturanweisungen und Details zu Datum und Zeit der letzten Ausnahme an. Beim Auftreten einer Ausnahme können

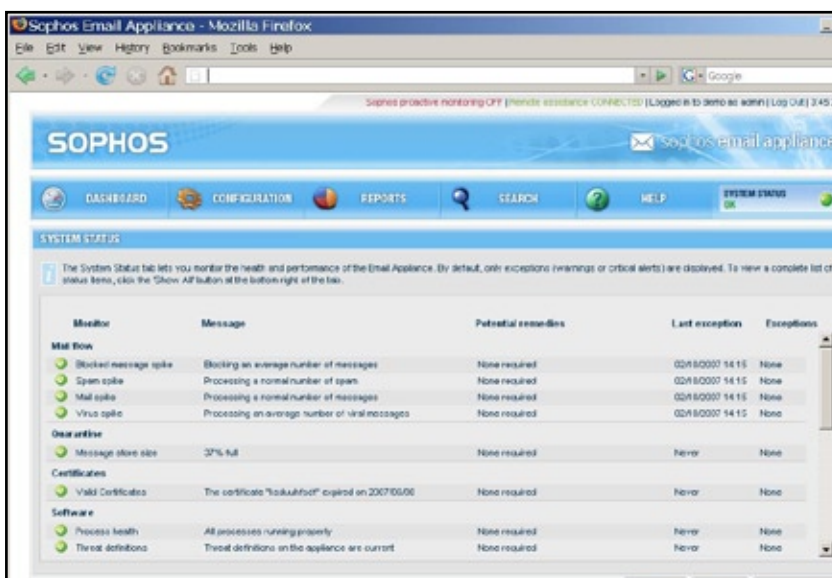


Abbildung 12: Seite „Systemstatus“

Sie diese anklicken und die aufgeführten Details über das Ereignis und eventuell durchgeführte Maßnahmen ansehen.

Von dieser einzelnen Seite in der Management-Konsole können Sie sich jeden wichtigen Vorgang der Appliance anzeigen lassen. Die Systemstatus-Seite ermöglicht die einfache Durchführung umfangreicher Prüfungen in Bezug auf Gesamtleistung und Schutzstatus sowie Unterstützung beim Wiederherstellen nach Systemausfällen.

Updates

Sophos E-Mail Appliances stellen in Abständen von wenigen Minuten eine Verbindung zu Sophos her, um neue Virenkennungen und Software-Updates herunterzuladen – standardmäßig werden beide automatisch heruntergeladen und angewandt. Der Administrator kann unkritische Software entweder nach einem festen Zeitplan herunterladen oder bei Bedarf mit nur einem Mausklick. Unkritische Updates können bis zu sieben Tage hinausgeschoben werden. Updates für kritische Software, wie beispielsweise Schwachstellen-Patches, werden umgehend angewendet.

Wie bereits erwähnt, stehen zwischen den Downloads die neuesten Spaminformationen online und in Echtzeit über SophosLabs' SXL Netzwerk zur Verfügung.

Backups

Administratoren können automatische FTP-Backups von Konfigurationsdaten und Systemprotokollen einrichten. Konfigurations-Backups können nach folgendem Zeitplan durchgeführt werden:

- Täglich um Mitternacht
- Freitags um Mitternacht
- Am ersten Tag des Monats um Mitternacht

Daten-Backups können nach folgendem Zeitplan durchgeführt werden:

- Nach Ablauf
- Halbstündlich
- Stündlich
- Täglich um Mitternacht
- Freitags um Mitternacht
- Am ersten Tag des Monats nach Mitternacht

Das Backup von Konfigurationsdaten kann auch manuell durchgeführt werden. Klicken Sie auf die System-Backup-Seite in der Management-Konsole (siehe Abbildung 13).

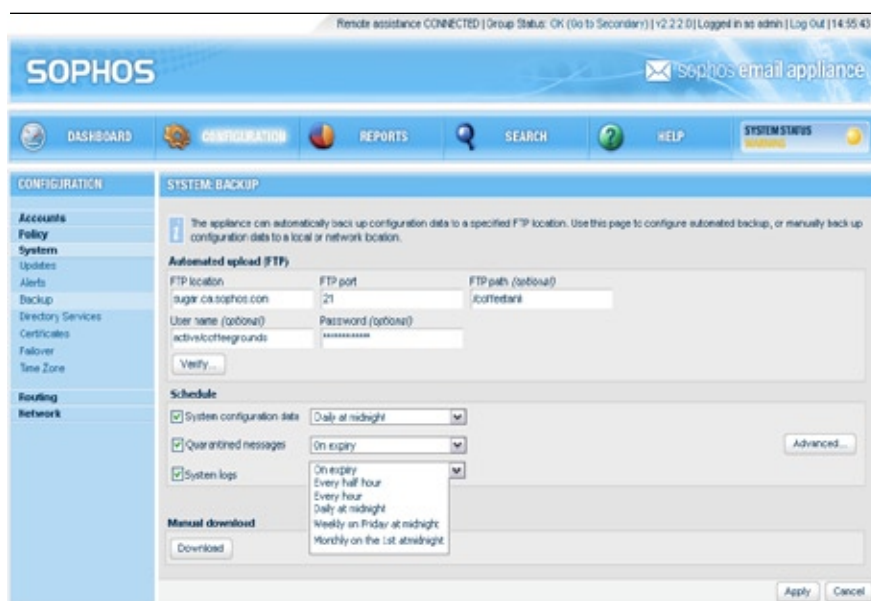


Abbildung 13: Seite „System Backup“

Quarantäne

Die Appliances verfügen über eine eingebaute Quarantäne, in der Millionen von E-Mails gespeichert werden können. Basierend auf den einzelnen Mustern des E-Mail-Verkehrs und der Richtlinien-Einstellungen in Ihrem Unternehmen können E-Mails über mehrere Wochen gespeichert werden.

Vom Dashboard aus kann der Quarantäne-Status direkt und schnell überprüft werden. Im unteren Bereich des Fensters „Summary Statistics“ (siehe Abbildung 14) werden zwei dynamische Leistungsmesser angezeigt: **Quarantine Age** (Quarantäne-Alter) und **Quarantine Capacity** (Quarantäne-Größe). Das Quarantäne-Alter gibt an, seit wie vielen Tagen E-Mails in der Quarantäne gespeichert sind. **12 days** (vgl. Abbildung) bedeutet, dass die älteste E-Mail in der Quarantäne 12 Tage alt ist. Die Quarantäne-Größe gibt an, wie voll der verfügbare Quarantänespeicher ist. Im hier gezeigten Beispiel sind 45% des Speichers belegt.

Die Appliances verwenden die automatische Quarantäne-Archivierung, um optimale Leistung und Ausnutzung der Onboard-Speicherkapazität zu gewährleisten. Wenn 70% der Speicherkapazität auf der Festplatte mit Daten belegt sind, werden Daten automatisch archiviert, damit wieder mindestens 40% der Festplattenkapazität verfügbar sind. Der Administrator muss den Speicherort für das FTP-Backup in der Management-Konsole der Anwendung konfigurieren.

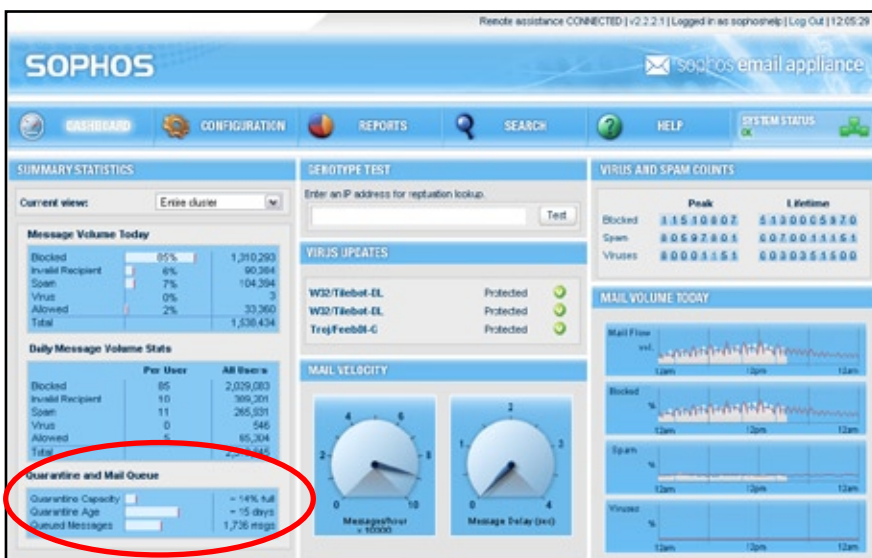


Figure 14: Quarantäne-Kapazität auf dem Dashboard

E-Mail-Suche

Sophos E-Mail Appliances bietet über die konventionellen Grenzen hinaus auch extensive E-Mail-Suchfunktionen. Sie sollen Ihnen das zeitaufwändige Suchen nach verloren geglaubten E-Mails erleichtern. Sie können unter Einsatz verschiedener Parameter problemlos effiziente Suchläufe durchführen, anstatt viel Zeit mit der Klärung über den Verbleib einer bestimmten E-Mail zu verbringen.

Die Suchfunktionen werden über die Navigationsleiste der Management-Konsole (siehe Abbildung 15) aufgerufen. Suchläufe können unabhängig voneinander in E-Mail-Protokollen, E-Mail-Warteschlangen oder in der Quarantäne durchgeführt werden.

Marktführender Support

Die herausragende Qualität der Sophos Support Services ist auf dem Sicherheitssektor unerreichbar – und das unterscheidet uns von anderen Anbietern.

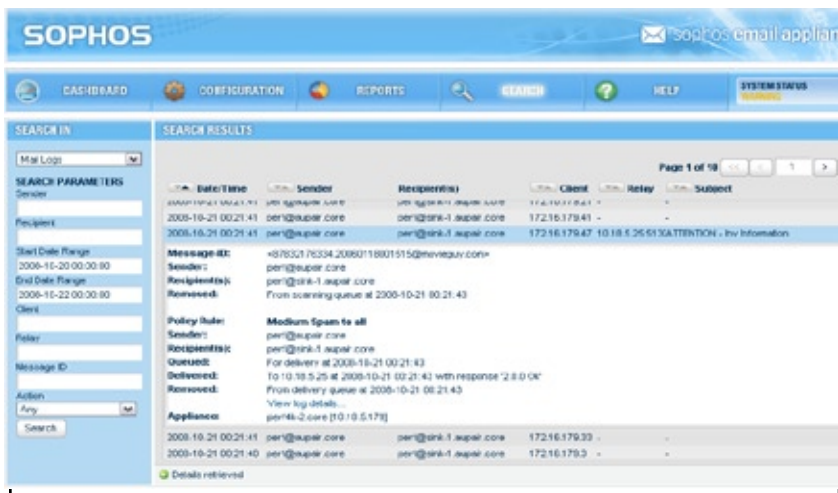


Abbildung 15: Suchseite E-Mail Protokoll

E-Mail-Protokolle können mit folgenden Parametern durchsucht werden:

- Sender
- Empfänger
- Anfangsdatumsbereich
- Enddatumsbereich
- Relay
- E-Mail-Kennung

Die Protokolldaten werden in einem leicht lesbaren Format dargestellt, dabei bleiben unwichtige Details verborgen, während solche Informationen hervorgehoben werden, die zur Klärung über den Verbleib der fraglichen E-Mail beitragen. Ein Suchlauf ordnet die Details unter folgenden Rubriken:

- Datum und Uhrzeit
- Sender
- Empfänger
- Relay
- Betreff

Wenn Sie auf einen Eintrag in den Suchergebnissen klicken, werden weitere Informationen zum Protokoll angezeigt.

Die **E-Mail-Warteschlange** kann unter Zuhilfenahme folgender Parameter durchsucht werden:

- Sender
- Empfänger
- Anfangsdatumsbereich
- Enddatumsbereich
- Warteschlange (Alle, Ungefiltert, Zustellung)

Die Warteschlangen-Daten geben Auskunft darüber, an welcher Stelle innerhalb des E-Mail-Flusses sich eine E-Mail befindet: in der Warteschlange zur Filterung oder in der Warteschlange zur Zustellung an den nachgeschalteten Mailserver. Details werden in einem gut lesbaren Format dargestellt. Ein Suchlauf ordnet die Details unter folgenden Rubriken:

- Datum und Uhrzeit
- Größe
- Empfänger
- Sender
- Warteschlangenstatus

Die **Quarantäne** kann über folgende Parameter durchsucht werden:

- Sender
- Empfänger
- Enddatumsbereich
- Relay
- E-Mail-Kennung
- Argument

Ein Quarantäne-Suchlauf ordnet die Details unter folgenden Rubriken:

- Datum und Uhrzeit
- Sender
- Empfänger
- Betreff
- Argument

Hinweis

Sie können nach folgenden Argumenten suchen: Alle, Virus, Spam, Stichwort, verdächtiger Anhang, verschlüsselter Anhang, unlesbarer Anhang, anstößiger Text.

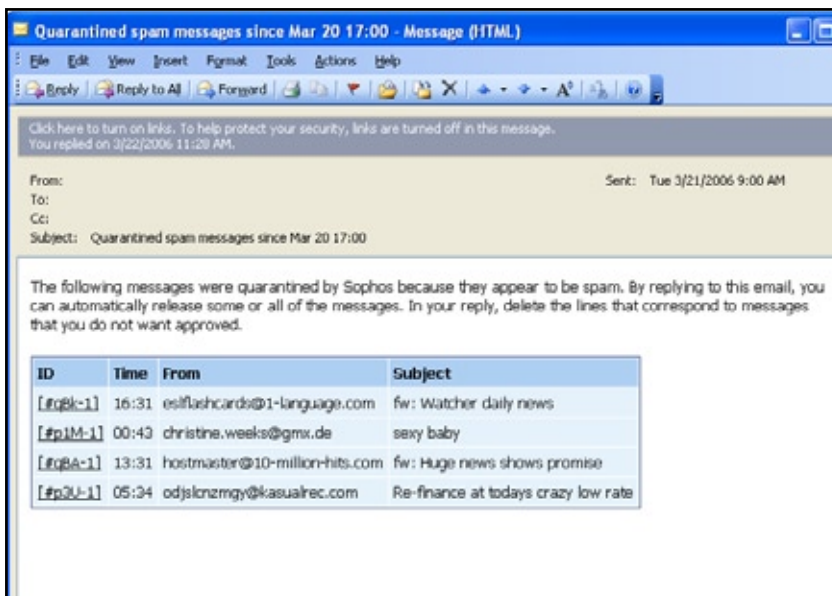


Abbildung 16: E-Mail-Digest (Hinweis: Kann je nach E-Mail-Client unterschiedlich aussehen).

Wenn Sie auf einen Eintrag in den Suchergebnissen klicken, werden weitere Informationen zum Quarantäne-Eintrag angezeigt. Hier können Sie außerdem nähere Informationen zur E-Mail abrufen. Der Administrator kann E-Mails zum Freigeben, Weiterleiten oder Löschen auswählen.

Damit der tägliche Verwaltungsaufwand weiter reduziert wird, können Administratoren spezielle Konten für Helpdesk-Mitarbeiter einrichten, die nur zur Bearbeitung interner Anfragen in Bezug auf E-Mails zuständig sind. Diese Mitarbeiter haben Zugriff auf alle Quarantäne-Managementfunktionen, aber nicht auf Systemeinstellungen oder Konfigurationsoptionen. Für Administratoren mit weitreichenden Verantwortlichkeiten und zusätzlichen Mitarbeitern erhöht diese Funktion die Produktivität der Gruppe und schafft Zeit, sich auf andere wichtige Aufgaben zu konzentrieren.

Endnutzer-Optionen

Um die Belastung der IT-Abteilung zu verringern, delegieren viele Unternehmen einen Teil der Verwaltung eingehender Spam-Mails an die beabsichtigten Empfänger. Die Sophos E-Mail Appliances bieten hierzu zwei Optionen:

- E-Mail-Digest
- Webbasierte Endnutzeroberfläche

Unter E-Mail-Digest versteht man systemgenerierte E-Mails, die eine Liste über in Quarantäne verschobene E-Mails enthalten. Empfänger können so ihre eigene Quarantäne verwalten, indem sie auf die E-Mail mit einer der folgenden Anweisungen reagieren: halten, freigeben oder die E-Mail aus der Liste löschen.

Die Zustellung des oben gezeigten E-Mail-Digests kann planmäßig zu bestimmten Zeiten einmal am Tag, zweimal am Tag oder einmal pro Woche erfolgen.

Administratoren haben auch die Möglichkeit, einen webbasierten Zugriff auf die Quarantäne einzusetzen. Dies erfolgt mit Benutzer-Authentifizierung entweder über Active Directory oder eine Anwenderliste.

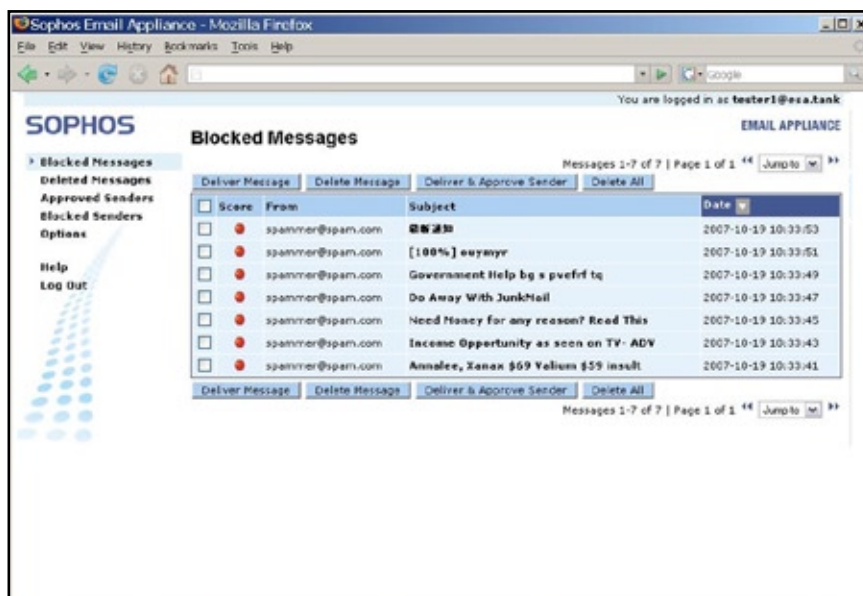


Abbildung 17: Webbasierte Endbenutzer-Oberfläche

Die webbasierte Oberfläche (siehe Abbildung 17) bietet jedem Benutzer eine ständig aktualisierte Anzeige der in Quarantäne verschobenen E-Mails und verfügt über dieselben Optionen zum Verwalten, Freigeben oder Löschen dieser E-Mails.

E-Mail-Digest und webbasierte Oberfläche können in einer der folgenden Sprachen eingesetzt werden: Deutsch, Englisch, Französisch, Italienisch, Japanisch und Spanisch. Dies ist eine globale Einstellung, die vom Administrator festgelegt wird und vom Endnutzer nicht geändert werden kann.

Endnutzer-Präferenzen sind global, deshalb erhält jeder Benutzer den E-Mail-Digest, sofern dieser aktiviert ist. Ist die webbasierte Oberfläche aktiviert, erhält jeder Benutzer Zugriff darauf. Die einzige Ausnahme: Wenn die webbasierte Endnutzeroberfläche aktiviert ist, können sich einzelne Benutzer aus dem E-Mail-Digest abmelden.

Administratoren können Benutzern Optionen gewähren, damit diese ihre persönlichen Allow-/Block-Lists verwalten und sich vollständig von der Spamprüfung abmelden können. (Weitere Informationen finden Sie unter *Zusätzliche anwenderdefinierte Spameinstellungen* in Kapitel 2: „Produktfunktionen“.) Der Administrator muss diese Funktionen global auf der Seite Endnutzer-Präferenzen aktivieren (siehe Abbildung 6 in Kapitel 3: „Einrichtung“). Der Zugriff auf die webbasierte Endnutzer-Oberfläche muss ebenfalls durch den Administrator aktiviert werden.

Schnellere Filterung

Administratoren können die Effizienz des E-Mail-Filters steigern, indem sie Allow- und Block-Listen einrichten, die entweder global oder für einzelne E-Mail-Konten gelten.

5: REPORTING

Übersicht

Damit Übersicht und Kontrolle des E-Mail-Gateways erhalten bleiben, benötigt der Administrator detaillierte Kenntnisse über den Verlauf des E-Mail-Flusses. Dabei reicht es nicht aus, einfach nur zu wissen, dass das Netzwerk über aktuellen Schutz gegen Spam und Viren verfügt. Oft werden Administratoren von der Unternehmensleitung gebeten, eine Analyse des E-Mail-Gateways zur Verfügung zu stellen. Dazu muss der gesamte E-Mail-Verkehr untersucht und ein Leistungsbericht über Hardware und Software vorgelegt werden. Mit den Echtzeit-Funktionen der Appliance ist es leicht möglich, diesen Einblick zu erreichen, der eine bessere Verwaltung und intelligente Systemadministration ermöglicht.

Es ist zwar wichtig, Kenntnis über das aktuelle Geschehen zu haben, doch mindestens genauso wichtig ist es, die über einen bestimmten Zeitraum auftretenden Veränderungen zu verstehen. Die Appliances verfügen über eine Fülle von zielgerichteten Reports, mit deren Hilfe der Administrator die Vorgänge am E-Mail-Gateway verstehen und für zukünftige Kapazitätsanforderungen in Bezug auf ein wachsendes E-Mail-System planen kann.

Auf die Gesamtreports kann in der Management-Konsole an zwei Stellen zugegriffen werden. Schlüsselstatistiken wie E-Mail-Volumen und Bedrohungsverhalten sind auf dem Dashboard zusammengefasst (siehe Abbildung 3, Kapitel 2: „Produktfunktionen“). Umfangreichere Statistiken über ein größeres Informationsspektrum finden Sie auf der Seite „Reports“. Beide Bereiche werden im Folgenden beschrieben.

Dashboard-Reports

Das Dashboard liefert eine kurze Zusammenfassung über die Live-Systemleistung und aktualisiert dabei die Daten alle fünf Minuten. Das Dashboard teilt diese Daten in drei Bereiche auf – **Statistikübersicht**, **E-Mail-Geschwindigkeit** und **E-Mail-Volumen** – und ermöglicht den Zugriff auf die am häufigsten verwendeten Statistiken.

Statistikübersicht

Die Statistikübersicht wird auf der linken Seite des Dashboards angezeigt und liefert Details über das tägliche E-Mail-Aufkommen (auch Spitzen) und hebt die gängigsten Virenbedrohungen hervor. Darüber hinaus wird angezeigt, wann das letzte Update durchgeführt wurde und wie viel verfügbarer Speicherplatz noch in der eingebauten Quarantäne vorhanden ist.

Die Pfeile in den oberen drei Zeilen zeigen die Abweichungen des Verkehrs im Vergleich zum Vortag an. Zeigt beispielsweise ein Pfeil nach unten, bedeutet dies, dass das heutige Volumen unter dem von gestern liegt.

SUMMARY STATISTICS	
Mail Volume Today	524,887 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	524,887 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	TrspCoburn-80 (517) W32/Bronck-49 (204) TrspCopper-EM (98) W32/Avail-CDC (52)
Software Engine Updated	2007.01.03 11:42AM
Quarantine Capacity	45% full
Quarantine Age	12 days

Das durchschnittliche Tagesvolumen ist eine fortlaufende Summe, die auf der Gesamtmenge der E-Mails basiert, die verarbeitet wurden seitdem die Appliance erstmals online ging. Spitzenvolumen geben die Maximalwerte pro Kategorie für denselben Zeitraum an.

E-Mail-Geschwindigkeit

Im unteren Teil des mittleren Abschnitts befinden sich zwei Skalen, zur Bemessung der verarbeiteten E-Mails pro Stunde und der Verzögerung von E-Mails, z.B. wie viel Zeit der Mailfilter benötigt, um eine einzige E-Mail zu überprüfen.



Diese Skalen liefern ein sofortiges Bild des Mailvolumens, das sich in der Appliance befindet und zeigen an, wie lange die Bearbeitung jeder E-Mail dauert. Wenn die Skala auf der linken Seite (E-Mails/Stunde) den Höhepunkt überschreitet, könnte dies ein Hinweis auf eine E-Mail-Spitze sein, die normalerweise eine Höhepunktüberschreitung der Skala auf der rechten Seite (Latenzzeit) nach sich zieht. Wenn im umgekehrten Fall die Skala E-Mails/Stunde auf Null steht, könnte dies auf ein Verbindungsproblem hinweisen.

Heutiges E-Mail-Volumen

Rechts unten auf dem Dashboard befinden sich drei Liniendiagramme, die den täglichen E-Mail-, Spam- und Virenverkehr messen.



Der weiße Füllbereich zeigt den E-Mail-Fluss an, der heute bis zum jetzigen Zeitpunkt stattgefunden hat, während die rote Linie den Durchschnitt der letzten sieben Tage anzeigt. Sollte eine deutliche Differenz zwischen diesen beiden Werten festgestellt werden, könnte dies auf eine E-Mail-Spitze oder einen Virus (weiß höher als rot), oder ein Verbindungs-/Relaisproblem (rot höher als weiß) hinweisen. Bitte beachten Sie, dass diese Diagramme die wahre Beschaffenheit des E-Mail-Flusses messen, daher bedeutet das Vorkommen einer Spitze in Spam oder Viren nichts weiter, als dass die Appliance diese Bedrohungen abfängt und sie aus dem E-Mail-Verkehr heraushält.

Reports-Seite

Wenn Sie auf der Navigationsleiste der Management-Konsole auf die Registerkarte Reports klicken, können Sie auf weitere Reports zugreifen



Abbildung 18: Seite „Reports“

(siehe Abbildung 18).

Unter „Volume Info“ werden E-Mail-Merkmale der letzten sieben Tage mit den Merkmalen der vorangegangenen sieben Tage und den Abweichungen beider Zeiträume verglichen. Dies liefert schnell Hinweise darüber, wie der E-Mail-Verkehr sich von Woche zu Woche ändert. Direkt unter diesem Abschnitt werden Systemdurchsatz und Latenzzeit numerisch auch für die letzten beiden Sieben-Tage-Zeiträume dargestellt.

Das Tortendiagramm links unten teilt das gesamte E-Mail-Volumen der letzten sieben Tage in sechs Kategorien ein: **Legitim**, **Blockierte Verbindungen**, **Andere** (E-Mails mit Stichwort oder anstößigem Inhalt), **Spam mittel**, **Spam hoch** und **Virus**. Dieses Diagramm zeigt sofort die Zusammensetzung des E-Mail-Flusses an.

Das Balkendiagramm rechts unten beschreibt denselben Zeitraum und zeigt Daten zu allen nicht legitimen E-Mails an. Dieses Diagramm schließt blockierte Verbindungen (auf MTA-Ebene) ein und zählt jede blockierte Verbindung als eine E-Mail.

Die zwei Abschnitte rechts oben auf der Report-Startseite zeigen die fünf letzten Alarme an, die von der Appliance generiert wurden und die am häufigsten erkannten Viren.

Detalliertes Reporting

Das Navigationsfenster auf der linken Seite der Reports-Seite (und Unterseiten) führt zu einer großen Auswahl an flexiblen, dynamisch generierten Reports. Diese Reports sind in vier Kategorien eingeteilt, siehe Tabelle:

Hinweis

Antivirus- und Inhalts-Reports können für ein- oder ausgehenden E-Mailverkehr aktiviert werden.

Kategorie	Report-Name	Beschreibung
Mail trends	Volumen	Teilt täglichen E-Mail-Fluss in sechs Komponenten ein*
	Message actions	Zugestellte, abgelegte und in Quarantäne verschobene E-Mails
Performance	Latenz	Zeit (in Sekunden) zum Überprüfen einer E-Mail
	Durchsatz	Anzahl der E-Mails, die pro Sekunde überprüft werden
Senders	Virus relays	IP-Quelle eingegangener Viren
	Spam relays	IP-Quelle von Spam-Mails
	Blocked connections	Anzahl per IP-Adresse blockierter Verbindungen
Recipients	Spam recipients	Top-Ten der Spam-Empfänger im Netzwerk
Policy analysis	Anti-Virus	Kategorisiert E-Mails mit der Bezeichnung „Virus“ als Verdächtig, Verschlüsseltes Attachment, Eingeschränktes Attachment, Unlesbares Attachment oder Virus
	Anti-Spam	Kategorisiert E-Mails mit der Bezeichnung „Spam“ als Blockiert, Spam hoch und Spam mittel
	Content	Aufteilung der blockierten E-Mails nach Stichwort oder anstößigen Inhalten

Die Reportparameter können auf alle Reports angewandt werden, die in der Tabelle auf der vorherigen Seite aufgeführt sind. Außerdem kann die Datentabelle mit jedem Report angezeigt werden.

Reports können gedruckt oder als CSV-Dateien exportiert werden, zur Verwendung in anderen Anwendungen. Ein exportierter Report kann beispielsweise in einer Präsentation an die Unternehmensleitung oder den Mitarbeiter, der für die Einhaltung von Richtlinien zuständig ist, enthalten sein, um die Effektivität der Appliance in Bezug auf die Verwaltung der E-Mail-Sicherheit zu demonstrieren.

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

Die Managed Appliance

Sophos E-Mail Security Appliances führen ein neues Netzwerksicherheitskonzept ein: die Managed Appliance. Eine Managed Appliance vereint die Vorteile einer Appliance-Lösung, d.h. Benutzerfreundlichkeit, Plattformunabhängigkeit, stabile Sicherheit, mit den Vorteilen eines Managed Service: ausgegliederte Sicherheit, hohe Verfügbarkeit, hohe Kapazität. Die Managed Appliance befindet sich jedoch in Ihrem eigenen Netzwerk, so dass Sie stets den Überblick behalten. Sie bietet somit umfassende Sicherheit, die weit über die anderer Lösungen hinausgeht.

In den folgenden Abschnitten erfahren Sie mehr über die Merkmale, die Managed Appliances von anderen Lösungen unterscheiden.

Automatische Updates

Um aktuellen Bedrohungsschutz gewähren zu können, initiieren die Appliances der meisten Anbieter alle 30 oder 60 Minuten einen Datensuchlauf. Doch aufgrund einer E-Mail-Bedrohung, die immer größere Ausmaße annimmt und sich immer rasanter ausbreitet, kann diese zeitliche Staffelung beträchtliche Sicherheitslücken für die Gateway-Sicherheit bedeuten. In den Sophos E-Mail Appliances wurden diese langen Verzögerungen eliminiert und die Sicherheit dadurch noch weiter verbessert, da in Abständen von wenigen Minuten automatisch die neuesten Virenkennungen aus den SophosLabs heruntergeladen werden.

Die Managed Appliance

Sophos E-Mail Appliances vereinen Übersicht und Robustheit einer Appliance mit der Verfügbarkeit und Einfachheit eines Managed Service.

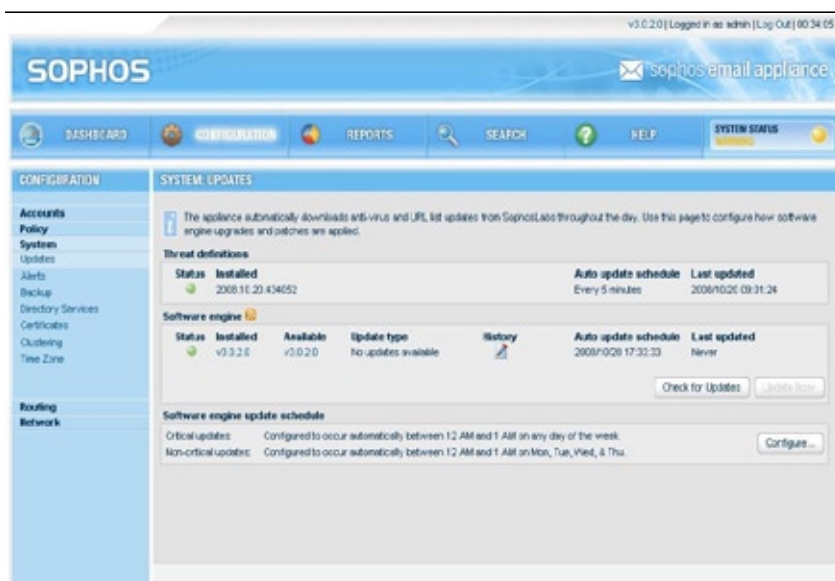


Abbildung 19: Seite "System Updates"

Sie ermöglichen auch Netzwerküberprüfungen in Echtzeit auf die neuesten Spamschutzdaten in SophosLabs' einzigartiger SXL-Online-Datenbank.

Die in so kurzen Zeitabständen durchgeführten Updates sorgen dafür, dass rasch Schutz vor neuen Bedrohungen verfügbar ist. Darüber hinaus wird deutlich weniger Bandbreite verbraucht, da die Updates wesentlich kleiner sind. Aktueller Schutz steht deshalb schnell und effektiv zur Verfügung. Das Ergebnis kann sich sehen lassen: Sophos liefert die zuverlässigste und umfassendste E-Mail-Sicherheit, die der Markt zu bieten hat.

Neue Bedrohungsdefinitionen und Upgrades für kritische Software werden automatisch beim Herunterladen angewandt. Upgrades für nicht-kritische Software können entweder sofort angewendet werden oder entsprechend dem Zeitplan, den der Administrator festgelegt hat. (siehe Abbildung 19 auf der vorherigen Seite)

Funktionsüberwachung

Häufige Downloads sind das A und O für bestmögliche Sicherheit. Sophos geht sogar noch einen Schritt weiter: Jede Appliance wird daraufhin überprüft, ob sie mit den aktuellsten Bedrohungskennungen ausgestattet ist. Anstatt einfach nur geplante Updates herunterzuladen, holen sich die Sophos Appliances die Updates aus einem zentralen Speicher. Der Speicher prüft, ob jede installierte Appliance Updates gemäß dem Zeitplan abrufen sollte. Sollte eine Appliance für mehr als zwei Stunden keine Verbindung herstellen können, alarmiert der Speicher das Support-Team von Sophos, damit dieses Team den Administrator darüber informiert und die Situation untersucht.

Diese einzigartige Funktionsüberwachung ist ein wichtiger Baustein für Administratoren in Bezug auf Sicherheit und Vertrauen – sie müssen sich keine Gedanken mehr darüber machen, ob die Sicherheit ihres E-Mail-Gateways auf dem neuesten Stand ist.

Alarme

Die Appliance verwendet mehr als 40 verschiedene Sensoren, um alles, von der Synchronisierung mit Active Directory bis hin zu Virenspezies, zu überwachen. Die meisten dieser Sensoren werden auf der Systemstatus-Seite in der Management-Konsole angezeigt. Erkennt ein Sensor Verhalten außerhalb der normal operierenden Parameter der Appliance, generiert er einen Alarm, welcher auf der Systemstatus-Seite zusammen mit einer empfohlenen Maßnahme zu Fehlerbehebung angezeigt wird. Zur visuellen Wahrnehmung ändert die Systemstatus-Schaltfläche auf der Navigationsleiste ihre Farbe: Grün für normal, Gelb für eine Warnung und Rot für einen kritischen Alarm. Durch Klicken auf die Schaltfläche wird die Systemstatus-Seite angezeigt, wo Sie weitere Details finden und gegebenenfalls korrigierende Maßnahmen einleiten können.

Je nach Art und Gewichtung des Ereignisses wird ein E-Mail-Alarm an den Administrator oder einen anderen Verantwortlichen ausgelöst. Das hat den Vorteil, dass der Administrator in der Appliance nicht angemeldet sein muss, damit er den Status überprüfen kann.

Unternehmenskritische Ereignisse lösen ebenfalls einen Alarm aus, der zur schnelleren Fehlerbehebung direkt an den Sophos Support gesendet wird. In einem solchen Fall kann Sophos korrigierende Maßnahmen einleiten, ohne den Administrator zu benachrichtigen. Fällt beispielsweise eines der beiden Netzgeräte aus, kann Sophos die Lieferung eines Ersatzgerätes veranlassen, bevor der Administrator Kenntnis über den Ausfall hat.

Proaktive Alarme

Alarme können an einen Verantwortlichen gesendet werden, falls der Administrator nicht verfügbar ist. Bei unternehmenskritischen Ereignissen wird Sophos zum Einleiten präventiver Maßnahmen automatisch benachrichtigt.

Remote-Unterstützung bei Bedarf

Sophos E-Mail Appliances verfügen über einen umfangreichen Hilfe-Index, der Sie bei der Fehlersuche unterstützt. Sollte ein Administrator ein Systemproblem nicht beheben können, können Sie einen Sophos-Techniker um Remote-Live-Unterstützung bitten. Bei einer sicheren Remote-Unterstützung, die nur von einem Administrator mit einer gültigen Sicherheitsermächtigung initiiert werden kann, greift der Sophos Techniker auf die Appliance zu und unterstützt die Fehlersuche. Dabei wird Secure Shell (SSH)-Technologie eingesetzt, die keine Änderungen der Firewall-Einstellungen erforderlich macht und aus Sicherheitsgründen nach vier Stunden automatisch abläuft. Darüber hinaus wird jede Änderung, die der Sophos Techniker an Ihrer Appliance vornimmt, protokolliert (alle verwendeten Tastenfolgen werden aufgezeichnet). Dies bedeutet, dass die Integrität und Sicherheit Ihres E-Mail-Netzwerks durch die Remote-Unterstützung nicht gefährdet wird.

Garantie

Sophos bietet für eine Dauer von bis zu drei Jahren eine Garantie für den Vorabtausch jeder E-Mail Appliance. Sollte eine Hauptkomponente (Festplatte, Netzgerät, Gesamtgerät) während des regulären Gebrauchs ausfallen, sendet Sophos Ihnen automatisch ein Ersatzteil zu, noch bevor Sie das defekte Teil zurückschicken müssen. Diese Garantie besteht auf jede Appliance. Sie beweist unser Vertrauen in Sophos E-Mail Appliances und entlastet Administratoren.

Zwei Komponenten der ES5000 und ES8000 können vor Ort ersetzt werden – Festplatten und Netzgeräte. Beide Komponenten können ersetzt werden, ohne dass das System heruntergefahren oder neu gestartet werden muss. Jeder andere Ausfall einer Komponente erfordert eine vollständig neue Appliance. Die ES1000 verfügt über keine vor Ort austauschbaren Komponenten.

Es besteht keine Veranlassung, das Gehäuse von einer Sophos E-Mail Appliance für Wartungszwecke zu öffnen. Hinweis: Aus Sicherheitsgründen wird durch das Öffnen des Gehäuses Ihre Produktgarantie ungültig und ein Alarm an Sophos ausgelöst.

Für weitere Informationen über die Garantie auf Sophos E-Mail Appliances lesen Sie bitte den Endnutzer-Lizenzvertrag.

Hinweis

Weitere Bedingungen und Bestimmungen Ihrer Produktgarantie an Ihrem Standort erhalten Sie von Ihrem Sophos Vertreter.

Sophos Rund-um-die-Uhr-Support

Unser hervorragender Support hebt uns von der Konkurrenz ab. Wir bieten unseren Kunden das ganze Jahr hindurch Rund-um-die-Uhr-Support. Jederzeit können Sie sich an unser weltweites Supportnetz wenden und individuelle Unterstützung erhalten.

Wir verfügen über Support-Zentren in Deutschland, Frankreich, Großbritannien, Italien, Singapur, Australien, Japan, Kanada und den USA. Unsere Experten arbeiten mit den SophosLabs und der Produktentwicklung zusammen und können so Ihre Probleme nachvollziehen, analysieren und lösen.

Dieser Service gehört zum Standard für jedes Sophos Produkt. Sophos Support wird **nicht** fremd vergeben und hat niemals Feierabend – wenn Sie die Unterstützung eines Technikers brauchen, reicht ein Anruf oder eine E-Mail an uns.

ANHANG I: RICHTLINIENVOREINSTELLUNGEN

Allgemein						
Für E-Mails mit	An	Außer an	Maßnahme durchführen	Benachrichtigen/ Umleiten	User	Banner hinzufügen
Bekannte unerwünschte Absender		Keine	Ablehnen (bei MTA)	Nein		Nein
Eingehende und ausgehende E-Mails, die größer als 10 MB (mit oder ohne Anhang) sind		Keine	Ablehnen (bei MTA)	Nein		Nein
Eingang Anti-Spam						
Für E-Mails mit	An	Außer an	Maßnahme durchführen	Benutzer benachrichtigen	User	Banner hinzufügen
Hohes Spamaufkommen		Spam-Abmeldungen	Löschen	Nein		Nein
Moderates Spamaufkommen		Spam-Abmeldungen	Quarantäne	Nein		Nein
Eingang Antivirus						
Für E-Mails mit	An	Außer an	Maßnahme durchführen	Benutzer benachrichtigen	User	Banner hinzufügen
Viren		Keine	Löschen	Nein		Nein
Unlesbare Anhänge		Keine	Zustellen mit Warnungs-Banner	Nein		Bereinigen unmöglich
Verschlüsselte Anhänge		Keine	Zustellen mit Warnungs-Banner	Nein		Verschl. Datei
Verdächtige Anhänge		Keine	Quarantäne, Datei ablegen, zustellen	Nein		Verdächtig
Spamschutz für ausgehende E-Mails						
Für E-Mails mit	An	Außer an	Maßnahme durchführen	Benutzer benachrichtigen	User	Banner hinzufügen
Hoher Punktzahl		Keine	Quarantäne	Nein		–
Moderater Punktzahl		Keine	Quarantäne			
Virenschutz für ausgehende E-Mails						
Für E-Mails mit	An	Außer an	Maßnahme durchführen	Benutzer benachrichtigen	User	Banner hinzufügen
Viren		Keine	Quarantäne	Nein		–
Unlesbare Anhänge		Keine	Zustellen	Nein		–
Verschlüsselte Anhänge		Keine	Zustellen	Nein		–
Verdächtige Anhänge		Keine	Löschen	Nein		–

ANHANG II: TECHNISCHE DATEN

Technische Daten* zu den E-Mail-Appliances ES1000, ES5000 und ES8000		
On-Board-Software		
<p>Sophos Anti-Virus-Engine</p> <p>Sophos Anti-Spam-Engine</p> <p>Beide Engines bieten Genotype™ und Behavioral Genotype Protection</p> <p>Das Sender Genotype-Verfahren sorgt bereits bei Verbindungsherstellung für lückenlosen Schutz</p> <p>TLS-Verschlüsselung</p> <p>Aktiv-/Passiv-Failover mit gemeinsamer Konfiguration</p> <p>Dashboard und Management-Konsole sind webbasiert</p> <p>Alarmer und Benachrichtigungen zu Systemstatus</p> <p>LDAP-Integration mit Active Directory</p> <p>Postfix MTA (Mail Transfer Agent)</p> <p>Optimiertes FreeBSD-Betriebssystem</p>		
Hardware – ES1000	Hardware – ES5000	Hardware – ES8000
Prozessor: Single Core	Prozessor: Quad Core	Prozessor: Quad Core
Festplatte: SATA, 160 GB	Festplatten: Dual Hot-Swap 160 GB SAS (RAID)	Festplatten: Dual Hot-Swap 300 GB SAS (RAID)
Netzteil: 260 W, 100/240 V AC	Netzteile: Dual Hot-Swap 920 W 100-240 V AC	Netzteile: Dual Hot-Swap 920 W 100-240 V AC
50.000 E-Mails pro Stunde	380.000 E-Mails pro Stunde	550.000 E-Mails pro Stunde
Format: 1U rackmontierbar	Format: 1U rackmontierbar	Format: 1U rackmontierbar
Abmessungen (b x h x t): 427 x 43 x 356 mm	Abmessungen (b x h x t): (432mm x 43mm x 650mm)	Abmessungen (b x h x t): 432 x 43 x 650 mm
Gewicht: 11,8 kg	Gewicht: 20,5 kg	Gewicht: 20,5 kg
Sicherheitszertifikate		
UL 60950, CE, FCC PART 15, VCCI, C-TICK, TUV-GS, SABS, RoHS, WEEE		
Support		
<p>Bis zu 3 Jahre Vorabaustausch-Garantie auf Hardware (in Abhängigkeit einer gültigen Softwarelizenz)</p> <p>Rund-um-die-Uhr-Support (24/7)</p>		
* Die technischen Daten können ohne Vorankündigung von Sophos aktualisiert werden. Die aktuellsten Daten sind jederzeit auf www.sophos.com einsehbar.		

SOPHOS

Boston, USA • Oxford, UK

rg/090224

