COMPREHENSIVE ANTI-SPAM SERVICE

Sofortiger Spamschutz am Gateway

Rund 80 Prozent aller E-Mails fallen heutzutage in die Kategorie Junkmails (Spam, Phishing und virenbefallene Nachrichten). Gelangen diese störenden und gefährlichen Daten ins Netzwerk, können sie die Kommunikation und Produktivität in einem Unternehmen stark beeinträchtigen. Durch Ausfiltern der Junkmails am Gateway wird nicht nur die Netzwerkeffizienz optimiert, sondern auch die E-Mail-Kommunikation und Mitarbeiterproduktivität verbessert.

Der SonicWall® Comprehensive Anti-Spam Service (CASS) bietet kleinen bis mittelgroßen Unternehmen umfassenden Spam- und Virenschutz und lässt sich in kürzester Zeit auf bestehenden SonicWall-Firewalls implementieren. Neben einer rascheren Bereitstellung vereinfacht CASS auch die Administration und reduziert durch die Konsolidierung mehrerer Lösungen den Gesamtaufwand.

Der Anti-Spam-Service lässt sich innerhalb von nur zehn Minuten konfigurieren und mit einem Mausklick aktivieren. Dabei bietet CASS umfassende Anti-Spam-, Anti-Phishing- und Anti-Malware-Funktionen für eingehende E-Mails sowie SonicWall Capture Threat-Netzwerk (früher als GRID-Netzwerk bekannt), IP-Reputation, Advanced Content Management, Schutz vor Denial-of-Service-Angriffen, umfangreiche Quarantänefunktionen und individuell konfigurierbare Junkmail-Übersichten für jeden Benutzer. CASS ist RBL-Filtern leistungsmäßig deutlich überlegen und schützt mit über 99-prozentiger Zuverlässigkeit vor Spam. Über 80 Prozent aller Spammails werden bereits am Gateway abgefangen; dabei kommen erweiterte Anti-Spam-Techniken wie Adversarial-Bayesian™- und Machine-Learning-Filter zum Einsatz.

Vorteile:

- Abwehr von Spamangriffen
- Echtzeit-Informationsupdates zu Bedrohungen dank dem SonicWall Capture Threat-Netzwerk
- Capture Threat Network Anti-Virus
- Optionaler Junkordner für Benutzer
- Integrierte Freigabe- und Sperrlisten
- Integriertes Reporting und Logging
- LDAP-Integration
- Unterstützt nachgeschaltete E-Mail-Sicherheitssysteme

Funktionen und Vorteile

Abwehr von Spam-, Phishing-, und Virenangriffen dank bewährter und patentierter* Technologien wie den Reputationsprüfungen. Hierbei werden nicht nur die IP-Reputation des Absenders, sondern auch Inhalt, Struktur, Verknüpfungen, Bilder und Anhänge überprüft. Erweiterte Techniken, die ebenfalls zum Analysieren von E-Mail-Inhalten eingesetzt werden, sind Adversarial-Bayesian-Filtering, Bildanalyse und „Kauderwelsch"-Erkennung, um verborgene bekannte und auch neue Bedrohungen aufzufinden. Das Cloud-basierte Design wendet diese Spamschutzmaßnahmen an, ohne die Firewall-Performance oder den Netzwerkdurchsatz zu beeinträchtigen.

Echtzeitinformationen zu Bedrohungen aus dem SonicWall Capture Threat-Netzwerk. Das Capture Threat-Netzwerk sammelt und analysiert Informationen aus Bedrohungslisten von Unternehmen und führt eingehende Tests und Auswertungen bei Millionen von E-Mails am Tag durch. Darauf basierend werden Reputation-Scores für Absender und Inhalt erstellt und neuartige Bedrohungen in Echtzeit erkannt, um ultrapräzisen und topaktuellen Schutz vor neuartigen Spamangriffen zu bieten und dafür zu sorgen, dass unbedenkliche E-Mails zugestellt werden.

SonicWall Capture Threat Network Anti-Virus™ greift auf Informationen aus dem SonicWall Capture Threat-Netzwerk zurück und gewährleistet wirksamen Schutz vor Viren und Spyware.

Flexibles Junkmail-Routing kategorisiert Junkmails als Spammails, potenzielle Spammails, Phishing-Mails, potenzielle Phishing-Mails, Viren und potenzielle Viren. Pro Kategorie können Nachrichten anschließend zurückgewiesen, gekennzeichnet und übermittelt, in den Junkordner des Benutzers übertragen oder gelöscht werden. Auf diese Weise ist eine umfassende Kontrolle und Einhaltung von unternehmenseigenen oder gesetzlichen Compliance-Vorgaben gewährleistet.

Schnelle Erstellung von Junkordnern für Benutzer (optional), sodass alle Anwender ihre Junkmails darin ablegen können. Benutzer können per E-Mail Junkordner-Berichte erhalten, über die sie Nachrichten (als Text) einsehen und bei Bedarf wieder aus dem Junkordner herausnehmen können. Die IT-Abteilung behält dabei die Kontrolle über die angezeigten Kategorien, Zeitpläne und über die Aufbewahrung der Junkordner-Berichte.

Integrierte Freigabe- und Sperrlisten auf den Netzwerksicherheitsappliances von SonicWall. IP-Adressen können am Gateway freigegeben oder gesperrt werden. Freigabe- und Sperrlisten auf Mitarbeiter-, Unternehmens- und Listenebene erlauben zusätzlich eine gezielte Kontrolle. Diese Funktion wird vollständig vom CASS unterstützt und erfordert keine zusätzliche Implementierung oder Benutzerschulung.

Die SonicWall-Firewalls verfügen über **integrierte Reporting- und Loggingfunktionen**. Servicestatus und -statistiken lassen sich mit einem einzigen Mausklick einfach anzeigen und Logdateieinträge nach Servicename einsehen. Der Servicestatus zeigt die Verfügbarkeit des CASS sowie der Junkordner und der nachgeschalteten E-Mail-Server.

LDAP-Integration ermöglicht eine robuste, einfache und sichere Benutzerverwaltung und bietet zusätzliche Flexibilität, da die Integration von LDAP-Servern unterstützt wird.

Unterstützung nachgeschalteter E-Mail-Sicherheitssysteme wie beispielsweise Unternehmensrichtlinien oder Compliance-Regeln, Benutzerpräferenzen und -regeln, erweitertes Reporting sowie bei Bedarf zusätzliche Funktionen.

**U.S.-Patente: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

Wann ist der SonicWall Comprehensive Anti-Spam Service sinnvoll?

Kleinere Organisationen, die ihre bestehende SonicWall-Firewall ohne großen Mehraufwand weiter nutzen möchten, können mit CASS einfach sicherstellen, dass nur erwünschte E-Mails an den E-Mail-Server übermittelt werden. Der Administrator kann die Lösung über eine einzige integrierte Schnittstelle auf der Firewall verwalten. Größere Unternehmen können ihren Spamschutz stufenweise aufbauen und dafür CASS vor ihre SonicWall Email Security-Lösung schalten. Auf diese Weise werden mehr als 80 Prozent der Junkmails bereits auf der Verbindungsebene abgefangen, während sich gleichzeitig der Verarbeitungsaufwand für die nachgeschalteten Systeme verringert. Verteilte Unternehmen, die E-Mails an mehreren Standorten erhalten, können CASS auf Remote-SonicWall-Firewalls implementieren, um Spam zu reduzieren, und mithilfe von SonicWall Email Security die E-Mail-Sicherheitsservices zentralisieren.

Unterstützte Plattformen und E-Mail-Server

SonicWall Comprehensive Anti-Spam Service ist als Aboservice für die folgenden SonicWall-Produkte verfügbar:

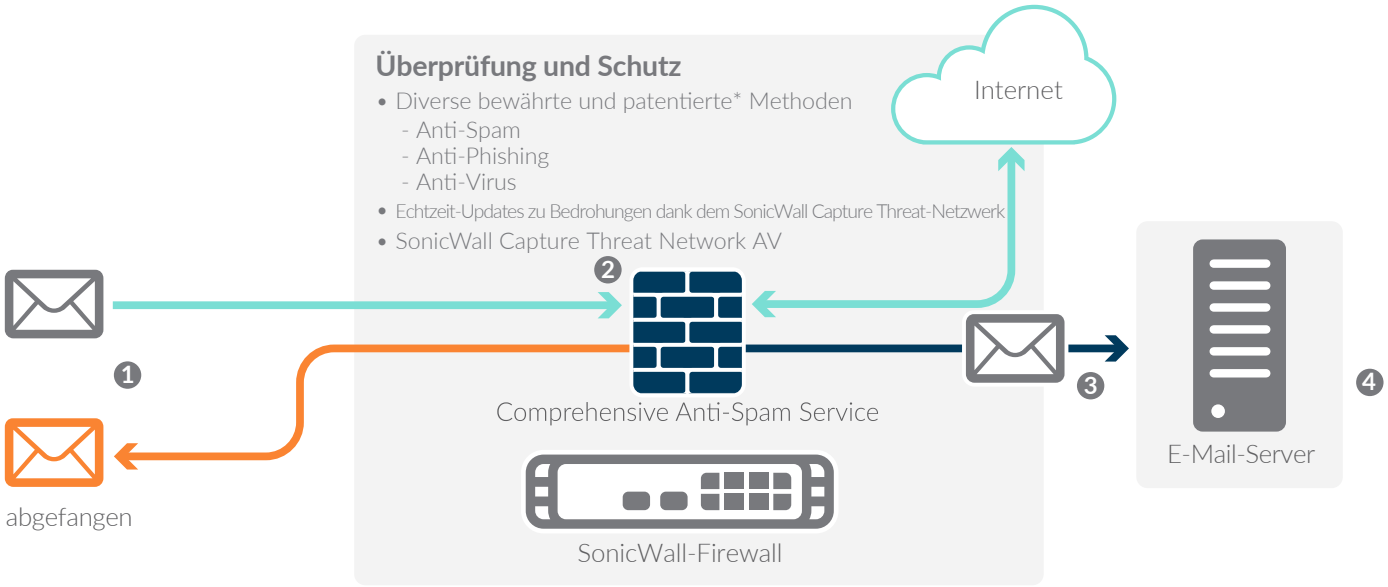
- Alle Appliances der SonicWall TZ, Network Security Appliance (NSA) und SonicWall E-Class NSA Series mit SonicOS 5.6.3 oder höher
- Nicht aufgeführte Plattformen und/oder SonicOS-Versionen werden nicht unterstützt.

Der SonicWall Comprehensive Anti-Spam Service ist mit sämtlichen E-Mail-Servern kompatibel, die eingehende SMTP-Nachrichten akzeptieren.

Im Comprehensive Anti-Spam Service enthaltene Optionen

Für die Option Junkordner für Benutzer muss die (im Service enthaltene) Junk-Speicher-Anwendung auf einem Server (normalerweise Ihr E-Mail-Server) mit Windows Server 2008 oder Windows Server 2012 installiert sein.

Wie funktioniert SonicWall Comprehensive Anti-Spam Service?



1. SMTP-Verkehr erreicht die SonicWall-Firewall.
2. Der Comprehensive Anti-Spam Service überprüft die Vertrauenswürdigkeit des Absender-IP-Servers mithilfe des SonicWall Capture Threat-Netzwerks in Echtzeit. Das Capture Threat-Netzwerk erhält weltweit von über 4 Millionen Endpunkten Echtzeitdaten, um die Vertrauenswürdigkeit von Servern zu ermitteln, die E-Mails senden. Bis zu 80 Prozent der Junkmails können auf der Verbindungsebene abgefangen werden, wodurch der Datenverarbeitungsaufwand der Firewall insgesamt reduziert wird. Die restlichen E-Mails werden mithilfe des Cloud-basierten SonicWall Capture Threat-Netzwerks verarbeitet. Das Capture Threat-Netzwerk wendet die bewährten Spamerkennungsmethoden von SonicWall an.
3. Erwünschte E-Mails werden an den E-Mail-Server übermittelt.
4. Optional lassen sich Junkmails an die SonicWall-Junkordner auf dem E-Mail-Server übermitteln und Junkordner-Berichte als E-Mail an die einzelnen Benutzer schicken.

Comprehensive Anti-Spam Service

01-SSC-9274 NSA E8510 (1 Jahr)

01-SSC-8950 NSA E8500 (1 Jahr)

01-SSC-9221 NSA E6500 (1 Jahr)

01-SSC-9222 NSA E5500 (1 Jahr)

01-SSC-9223 NSA 4500 (1 Jahr)

01-SSC-9000 NSA 3500 (1 Jahr)

01-SSC-8997 NSA 2400 Series (1 Jahr)

01-SSC-4600 NSA 250M Series (1 Jahr)

01-SSC-4642 NSA 220-Serie (1 Jahr)

01-SSC-4787 TZ 215 Series (1 Jahr)

01-SSC-4832 TZ 205 Series (1 Jahr)

01-SSC-4871 TZ 105 Series (1 Jahr)

Lizenzen auch für mehrere Jahre erhältlich. Weitere Informationen erhalten Sie unter: www.sonicwall.com/de

Der Comprehensive Anti-Spam Service unterstützt theoretisch beliebig viele Benutzer, wobei die empfohlene Anzahl 250 Benutzer oder weniger beträgt.

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, Kalifornien 95054, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-EmailAntiVirus-EU-IMAG-25864