



- **Verwaltung von ein- und ausgehenden E-Mail-Bedrohungen**
- **Hardware-, Software- oder Virtual Appliance-Optionen**
- **Hochverfügbare und skalierbare Split Mode-Architektur**
- **Einhaltung von gesetzlichen Vorschriften**
- **Verwaltung von E-Mail-Regeln**
- **Erweitertes Reputation Management**
- **Nahtlose Integration mehrerer LDAP-Server**
- **Umfassende Berichte**
- **SonicWALL GRID Anti-Virus™**
- **Schutz vor DHA-, DoS- und Zombie-Angriffen**
- **Erweiterte Kontrollmöglichkeiten für Endbenutzer**
- **Schnelle Installation und benutzerfreundliche Verwaltung**

Leistungsstarke, hochskalierbare E-Mail Security-Lösungen

Viele E-Mail Security-Anbieter sind mit der steigenden Flut komplexer E-Mail-Angriffe, den immer strengeren neuen Compliance-Vorgaben und den dynamisch strukturierten Unternehmensumgebungen überfordert. Doch Unternehmen benötigen heute mehr denn je leistungsstarke Lösungen, mit denen sie nicht nur die Kosten, sondern auch die Komplexität reduzieren können.

Als flexibelste E-Mail-Sicherheitslösung auf dem Markt bietet SonicWALL® E-Class Email Security neben einem herausragenden Preis-Performance-Verhältnis äußerst effektive, schnell reagierende Schutzfunktionen und reduziert den Verwaltungsaufwand. Verfügbar als SonicWALL Email Security Appliance (ESA) ES6000 und ES8300, als SonicWALL E-Class Email Security Software auf einem Drittanbieter-Windows® Server oder als SonicWALL Email Security Virtual Appliance in einer VMware®-Umgebung, sorgen die SonicWALL E-Class Email Security-Lösungen für einen automatisierten zukunftssicheren Schutz, der sich eigenständig aktualisiert. E-Class Email Security scannt den ein- und ausgehenden Datenverkehr und erhöht die Produktivität, da Spam, Viren und Phishing-Angriffe gestoppt werden. Außerdem verhindert die Lösung, dass sensible Daten nach außen dringen, und unterstützt so die Einhaltung gesetzlicher Vorschriften.

Die E-Class von SonicWALL besteht aus Premium-Enterprise-Class-Lösungen, die ein außergewöhnlich hohes Maß an Sicherheit und Performance bieten und gleichzeitig äußerst skalierbar, benutzerfreundlich und kosteneffizient sind. SonicWALLs Portfolio an E-Class-Produkten und -Services umfasst eine große Auswahl an E-Mail Protection-, Network Security- und Secure Remote Access-Lösungen.

Funktionen und Vorteile

Verwaltung von ein- und ausgehenden E-Mail-Bedrohungen. Eingehende E-Mails werden gescannt, um Spam-Mails, Phishing-Angriffe und Malware zu stoppen, bevor sie in das Netzwerk gelangen. Gleichzeitig werden ausgehende E-Mails und Anhänge geprüft, um zu verhindern, dass vertraulichen Informationen nach außen dringen und Malware weitergegeben wird.

Flexible Implementierung entweder als **Hardware Appliance** (Einsatz einer gehärteten High-Performance-Appliance), **Server-Software** (Nutzung bestehender Infrastruktur) oder als **Virtual Appliance** (gemeinsame Nutzung von IT-Ressourcen, um die Auslastung zu optimieren, Migrationen zu vereinfachen und Investitionskosten zu senken).

Hochverfügbare und skalierbare Split Mode-Architektur. Im Gegensatz zu den eingeschränkten Produkten anderer Anbieter können Unternehmen die E-Class Hardware Appliance-, Software- und Virtual Appliance-Lösungen von SonicWALL flexibel und effektiv entsprechend ihren individuellen Anforderungen kombinieren und zentral verwalten. SonicWALL bietet eine skalierbare, hochverfügbare E-Mail-Sicherheitslösung für Archivierung, Outsourcing und Managed Services, die auch bei Fusionen, Firmenübernahmen und dem Ausbau von Netzwerken in global verteilte Umgebungen mitwächst.

Einhaltung von gesetzlichen Vorschriften. Organisationen können E-Mails, die gegen gesetzliche Vorgaben und Richtlinien verstoßen (z. B. HIPAA, SOX, GLBA oder PCI), auf intelligente Weise identifizieren und überwachen. Außerdem können sie entsprechende Berichte generieren. Regelbasiertes Routing wird eingesetzt, um E-Mails an Archivierungs- oder Verschlüsselungssysteme* zu senden.

Verwaltung von E-Mail-Regeln. IT-Abteilungen können unternehmensweite Regeln anwenden, beispielsweise um zu verhindern, dass ungeeignete Inhalte verbreitet werden, um vertrauliche Informationen zu schützen, um E-Mail-Disclaimer einzufügen oder um die Verbreitung von ausführbaren Dateien zu blockieren.

Erweitertes Reputation Management. Blockt bis zu 90 % der bekannten Junk-Mails bereits in der Verbindungsphase ab. Die übrigen Junk-Mails werden mittels SonicWALL Advanced Content Management eliminiert. Dies verbessert die Performance und Skalierbarkeit und bietet umfassende Transparenz (im Gegensatz zu den Produkten anderer Anbieter).

Nahtlose Integration mehrerer LDAP-Server.

Gewährleistet, dass die SonicWALL E-Class Email Security-Lösungen automatisch mit mehreren LDAP-Servern synchronisiert werden, um E-Mail-Adressen, -Konten und Benutzergruppen automatisch zu verwalten.

Umfassende Berichte. Systemweites Reporting mit detaillierten und flexibel anpassbaren Berichten, z. B. zu Angriffstypen, Effizienz der durchgeführten Maßnahmen und System-Performance. Bei Systemen mit Split Mode-Konfiguration werden Reporting und Überwachung für alle Systeme zentralisiert, was Zeit spart und die Verwaltung des gesamten Systems vereinfacht.

SonicWALL GRID Anti-Virus™. Greift auf Anti-Virus- und Anti-Spyware-Technologien von SonicWALL zurück und gewährleistet wirksamen Schutz vor Viren und Spyware. Mit Signaturenupdate-Abos von McAfee™ und Kaspersky Lab™ bietet SonicWALL darüber hinaus eine zusätzliche Sicherheitsschicht.*

Schutz vor DHA-, DoS- und Zombie-Angriffen.* Mit effizienten Funktionen zur Verbindungsverwaltung können ungültige Verbindungen umgeleitet, gedrosselt oder blockiert werden, bevor sie das System erreichen. In Kombination mit der Anti-Spam-, Anti-Phishing- und Anti-Virus-Technologie von SonicWALL bilden diese Funktionen eine Komplettlösung, die alle Arten von E-Mail-Bedrohungen stoppt.

Erweiterte Kontrollmöglichkeiten für Endbenutzer.

Geben dem Endbenutzer mehr Kontrolle über die eigene Spam-Verwaltung, Freigabe- und Sperrlisten, Spam-Aggressivitätsstufen und das Delegieren von Konten. Über ein herunterladbares Plug-In, mit dem in Outlook® eine Junk-Schaltfläche installiert wird, können Benutzer selbstständig auf ungewollte Junk-Mails reagieren. Der Administrator definiert alle Endbenutzer-Kontrollmöglichkeiten und kann diese nach Benutzer, Gruppe oder Funktion zuweisen.

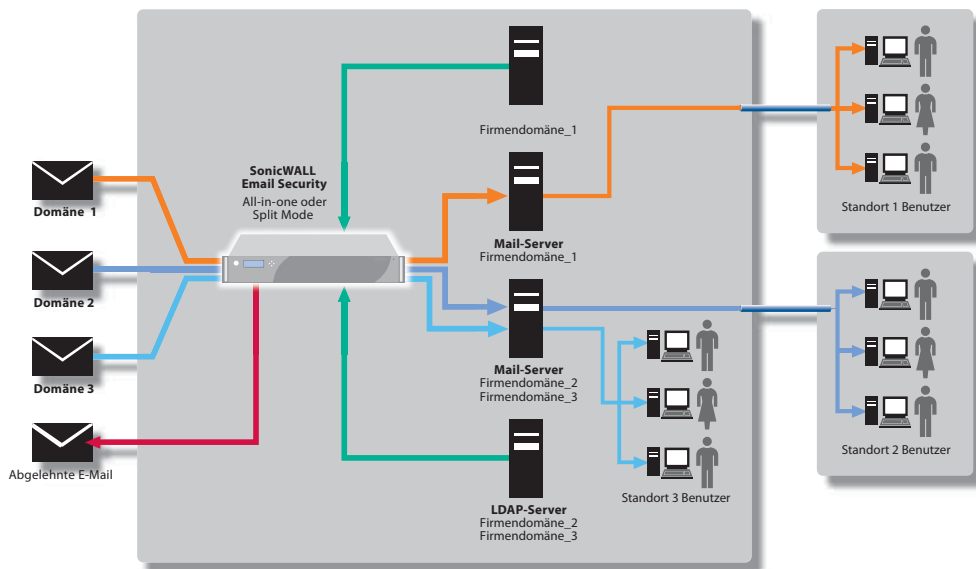
Schnelle Installation und benutzerfreundliche Verwaltung.

Entlastet die IT-Abteilungen spürbar bei der Implementierung und Verwaltung einer umfassenden E-Mail-Sicherheitslösung. Die Funktion Judgment Details vereinfacht die Fehlersuche und verhindert, dass legitime E-Mails verworfen werden.

*Zusätzlicher Subskriptions-Service erforderlich.

SonicWALL Email Security-Konfigurationen

Dank seiner flexiblen Architektur lässt sich SonicWALL Email Security (SES) in Unternehmen implementieren, die eine hochskalierbare, redundante und verteilte E-Mail-Sicherheitslösung mit zentraler Verwaltung benötigen. SES kann entweder im All-in-One- oder im Split Mode konfiguriert werden. Im Split Mode kann das System als Remote Analyzer oder als Kontrollzentrum fungieren. Bei einer typischen Split Mode-Konfiguration wird mindestens ein **Remote Analyzer** an ein **Kontrollzentrum** angeschlossen: Der **Remote Analyzer** empfängt E-Mails von einer oder von mehreren Domänen und verwendet Funktionen zur Verbindungsverwaltung, E-Mail-Filterung (Anti-Spam, Anti-Phishing und Anti-Virus) sowie erweiterte Regeln, um unbedenkliche E-Mails an den nachgeschalteten E-Mail-Server zu leiten. Das **Kontrollzentrum** verwaltet alle Remote Analyzer zentral. Außerdem werden alle Junk-Mails von den Remote Analyzern gesammelt und gespeichert. Das zentrale Management umfasst die Erstellung von Berichten und die Überwachung aller angeschlossenen Systeme. Auf diese Weise kann SonicWALL Email Security sowohl den eingehenden als auch den ausgehenden E-Mail-Verkehr für Organisationen jeder Größenordnung kosteneffizient schützen. Die SonicWALL Email Security Virtual Appliances erlauben eine vollständige Implementierung im Split Mode auf einem oder auf mehreren Servern und sorgen so für optimale Skaleneffekte.



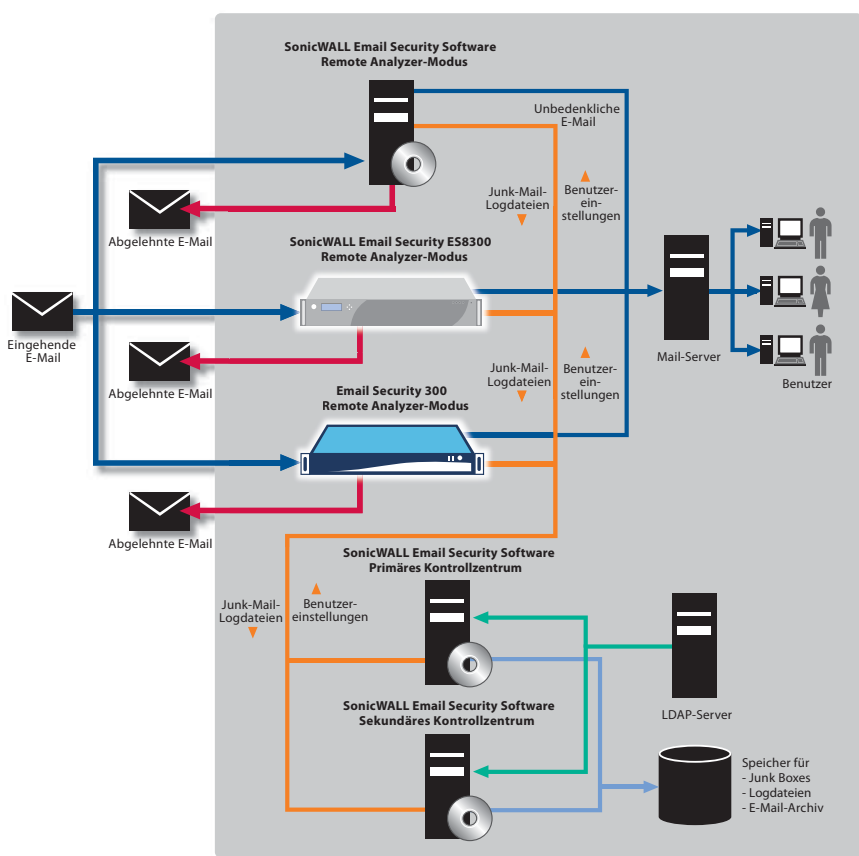
Mehrere Domänen, zentrale Kontrolle

SonicWALL Email Security zentralisiert die Verwaltung mehrerer E-Mail-Domänen.

Typische Einsatzfelder: Große medizinische Einrichtungen, Versicherungs- und Franchise-Unternehmen sowie Unternehmen mit mehreren Marken und Geschäftsbereichen

Vorteile

- Benutzerfreundliche zentrale Verwaltung mehrerer Domänen
- Anwendung von unternehmensinternen (zentralisierten) E-Mail-Regeln auf alle Anwender und/oder Durchsetzung von Regeln pro Domäne/Gruppe/Benutzer
- Zentrale Berichte pro Domäne
- Zentrale Kontrolle über ausgehende E-Mails; Policy/Routing-Regeln können dabei pro Domäne oder unternehmensweit angewendet werden.



Skalierbar und redundant

Das zentral verwaltete und hochskalierbare E-Mail-Sicherheitssystem kann mit unterschiedlichen Plattformen (Software, Hardware Appliance oder Virtual Appliance) arbeiten und verfügt über Failover-Funktionen, die nicht nur in die Architektur, sondern auch in die Hardware integriert sind.

Typische Einsatzfelder: Mittlere und große Unternehmen, Organisationen, die ein hochverfügbares E-Mail-Sicherheitssystem benötigen, Umgebungen mit unterschiedlichen Plattformen oder Organisationen, die E-Mails in einem SAN (Storage Area Network) speichern möchten

Vorteile

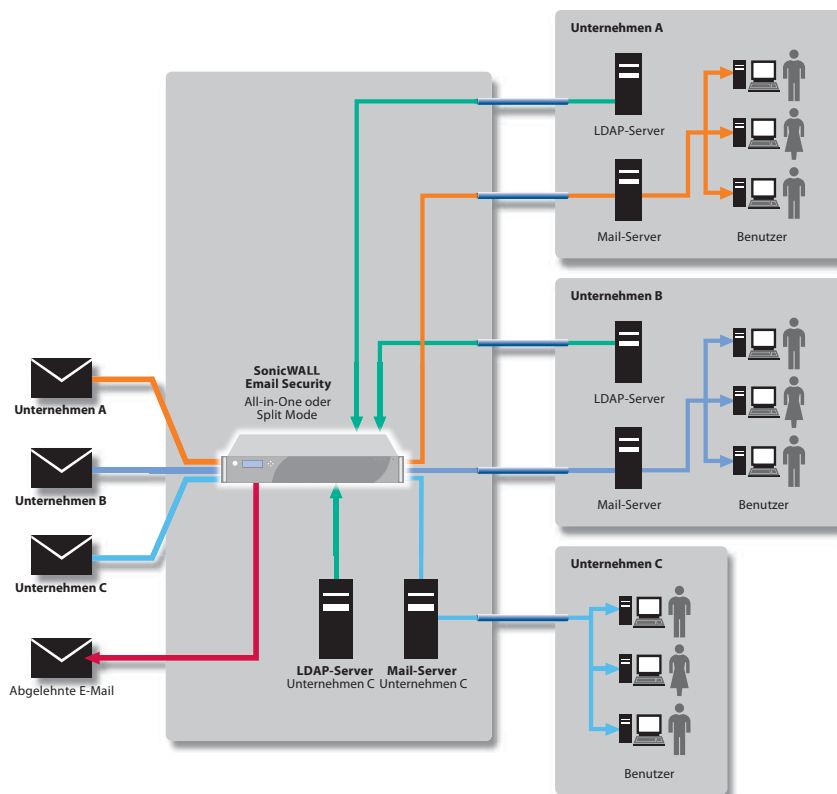
- Jeder der Remote Analyzer kann ein Failover auf einen anderen Remote Analyzer durchführen, so dass die E-Mail-Verfügbarkeit gewährleistet ist.
- Primäre und sekundäre Kontrollzentren sorgen für vollständige Redundanz.
- Durch das Speichern von E-Mails und anderen Dateien im Firmen-SAN lässt sich die Datenspeicherung zentralisieren und Backup-Prozesse werden vereinfacht.
- Die zentrale Kontrolle unterschiedlicher Plattformen reduziert den Verwaltungsaufwand.
- Durch Hinzunahme weiterer Remote Analyzer lässt sich das System einfach skalieren oder je nach Bedarf um zusätzliche Standorte erweitern.

Managed Service Provider

Managed Service Provider (MSP) können E-Mail-Filter-Services für ihre Kunden und meistens auch E-Mail-Server-Services anbieten. Die Email Security-Lösung von SonicWALL ist flexibel genug, um mehrere Domänen zuzulassen, die vom MSP zentral verwaltet und kontrolliert werden. Dabei ermöglicht sie es dem Kunden, eigene Benutzer, Regeln, Junk Boxes etc. einzusetzen.

Vorteile

- Zentrale Verwaltung mehrerer Domänen, so dass Junk-Mails gleichzeitig für alle Benutzer gelöscht werden können
- Zentrale E-Mail-Regeln für alle Benutzer und/oder Kunden-Regeln pro Domäne/Gruppe/Benutzer
- Zentrales Reporting mit Berichten pro Domäne
- Zentrale Kontrolle über ausgehende E-Mails kann für einige oder für alle Kunden genutzt werden und Policy/Routing kann pro Domäne angewendet werden.
- E-Mail-Server und LDAP-Server können beim Kunden, beim MSP oder bei beiden installiert sein.
- Flexible Expansionsmöglichkeiten erlauben es dem MSP, mit einem einzigen System anzufangen und dieses je nach Bedarf zu einer hochskalierbaren Split-Mode-Architektur mit Failover auszubauen.
- Mit einer Virtual Appliance lässt sich die Lösung schneller bei neuen oder bestehenden Kunden implementieren. Es fallen nur minimale Mehrkosten an. Außerdem ist der Implementierungsaufwand äußerst gering.



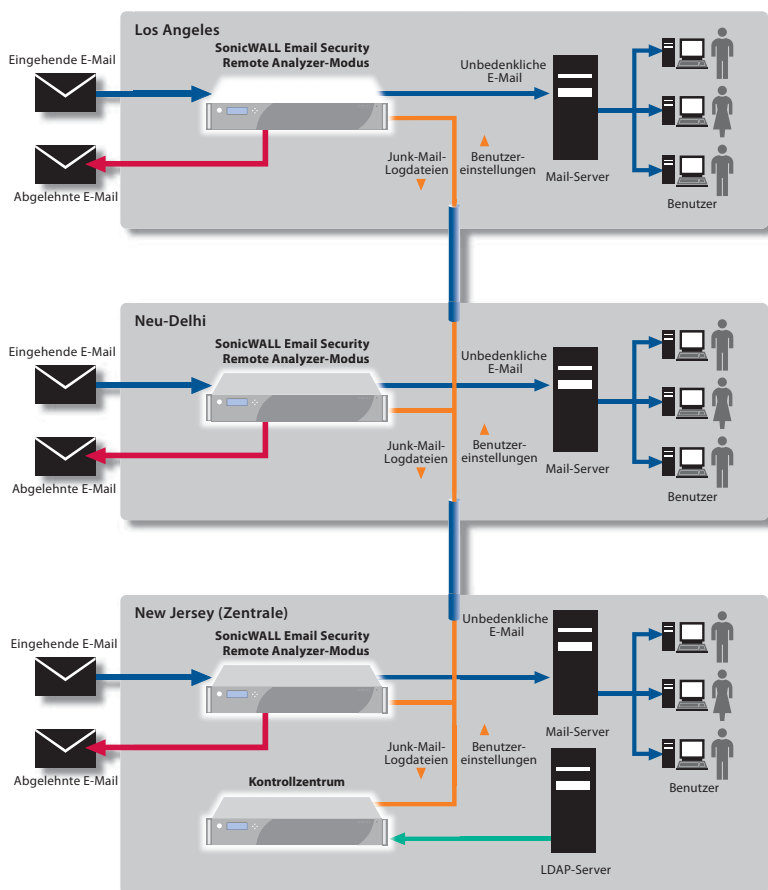
Mehrere Standorte, zentrale Kontrolle

In verteilten Organisationen ist der Standort des E-Mail-Systems (zentral oder lokal) von besonderer Bedeutung. Werden E-Mails zentral verarbeitet, verlieren IT-Abteilungen wertvolle Zeit. Erfolgt die Verarbeitung ausschließlich lokal, ist die E-Mail-Sicherheit im Unternehmen möglicherweise nicht umfassend gewährleistet. Mit der flexiblen Email Security-Architektur bietet SonicWALL verteilten Organisationen eine Sicherheitslösung, die sich gezielt auf ihre individuellen Bedürfnisse abstimmen lässt.

Typische Einsatzfelder: Unternehmen mit mehreren Standorten, Firmen, die beispielsweise durch Übernahmen neue Standorte dazugewonnen haben, oder Franchise-Unternehmen, die das E-Mail-System ihrer eigenen und ihrer Franchise-Filialen zentral verwalten möchten.

Vorteile

- Lokale Verarbeitung von E-Mails, wobei Junk-Mails gelöscht und unbedenkliche Mails zugestellt werden, was den Netzwerkverkehr deutlich reduziert
- Zentrale Verwaltung mehrerer Standorte mit automatisierten Regeln, Berichten und Überwachung
- Zentrale Kontrolle über ausgehende E-Mails; Policy/Routing-Regeln können dabei pro Domäne oder unternehmensweit angewendet werden.
- Remote Analyzer-Cluster erlauben ein Failover von Standort zu Standort.



Technische Daten

SonicWALL E-Class Email Security



SonicWALL E-Class Email Security Appliances

SonicWALL Email Security ES6000
01-SSC-6604
SonicWALL Email Security ES8300
01-SSC-6609



SonicWALL E-Class Email Security Software

SonicWALL Email Security Software
01-SSC-6636

SonicWALL E-Class Email Security Virtual Appliance

SonicWALL Email Security Virtual Appliance
01-SSC-7636

Abos – E-Class

User Pack-Abos für 5.000 Benutzer
SonicWALL Email Protection mit 24/7-Support (1 Jahr)
01-SSC-6674
SonicWALL Email Compliance (1 Jahr)
01-SSC-6644
McAfee Anti-Virus mit SonicWALL Time-Zero (1 Jahr)
01-SSC-6764
Kaspersky Anti-Virus mit SonicWALL Time-Zero (1 Jahr)
01-SSC-6774

(Weitere User Packs erhalten Sie unter www.sonicwall.com.)

Lizenzierungsmodelle

SonicWALL E-Class Email Security (Appliance, Software oder Virtual Appliance)

- Message Transfer Agent (MTA)
- Schutz vor DHA-/DoS-Angriffen
- Webbasierte Verwaltung
- Regelverwaltung/E-Mail Content Filtering
- Berichte und Überwachung
- LDAP-Synchronisierung

Email Protection-Abo mit Dynamic Support (8/5 oder 24/7) – Erforderlich

- Anti-Spam (1 Jahr)
- 8/5- oder 24/7-Support (1 Jahr)
- Anti-Phishing (1 Jahr)
- RMA (Appliance-Austausch)
- Software-/Firmware-Updates (1 Jahr)

Compliance-Abo

- Wörterbuch-Funktion
- Approval-Ordner
- Scannen der E-Mail-Anhänge
- Suche nach spezifischen Daten
- Verschlüsselungs-Reporting
- E-Mail-Archivierung
- Vordefinierte Regeln
- Konformitäts-Reporting

Anti-Virus-Abo (Kaspersky Lab und / oder McAfee mit SonicWALL Time Zero-Virenschutz)

- Kaspersky-Virenschutz
- SonicWALL Time Zero-Virenschutz
- McAfee-Virenschutz
- Zombie-Erkennung

Email Security Appliances	KMU (Verfügbar für kleinere Netzwerke)		E-Class (Große Unternehmen)	
	300	500	ES6000	ES8300
Domänen	Unlimitiert			
Betriebssystem	Gehärtete SonicWALL Linux OS Appliance			
Rackoptimiertes Gehäuse	1 HE, Mini	1 HE, Mini	1 HE, Mini	2 HE
CPU(s)	2,66 GHz	2,66 GHz	3,2 GHz	Quad Core Xeon 2,0 GHz
RAM	1 GB	1 GB	2 GB	4 GB
Festplatte	80 GB	2 x 80 GB	2 x 160 GB	4 x 750 GB
RAID (Redundant Disk Array)	-	X	X	RAID 5
Hot-swappable Laufwerke	-	-	-	X
Redundante Stromversorgung	-	-	-	X
Abmessungen	42,7 x 35,6 x 4,3 cm	42,7 x 35,6 x 4,3 cm	42,7 x 35,6 x 4,3 cm	69,9 x 48,3 x 8,9 cm
Gewicht	8,16 kg	8,62 kg	8,62 kg	22,7 kg
WEEE-Gewicht	5,90 kg	6,35 kg	6,35 kg	22,2 kg
Leistungsaufnahme (Watt)	189	201	201	280
BTU	644,49	685,41	685,41	1098,0
MTBF bei 25 °C in Stunden	125.004 (geschätzt)			
MTBF bei 25 °C in Jahren	14,27 (geschätzt)			

Email Security Software	
Domänen	Unlimitiert
Betriebssystem	Kompatibel mit Microsoft Windows 2003 Server oder Microsoft Windows 2008 Server
CPU	2,66 GHz Minimal Konfiguration
RAM	2 GB empfohlen, 1 GB Minimal Konfiguration
Festplatte	40 GB zusätzliche Minimal Konfiguration
Email Security Virtual Appliance	
Hypervisor	ESXi™ und ESX™ (ab Version 4.0)
Installiertes Betriebssystem	Gehärtetes SonicLinux
Zugewiesener Speicher	2 GB
Festplattenkapazität der Appliance	80 GB
VMware-Kompatibilitätsrichtlinien für Hardware:	http://www.vmware.com/resources/compatibility/search.php

Appliance- und Software-Features – Abos für Enterprise-Netzwerke mit User Packs für 1.000, 2.000, 5.000 und 10.000 Benutzer verfügbar

Schutzfunktionen	
E-Mail-Schutz für ein- und ausgehenden Verkehr	Ja
Anti-Spam-Effizienz	Über 98 %
Separat identifizierte Phishing-Angriffe	Ja
SonicWALL GRID Anti-Virus	Ja
Anti-Virus: Dual-Layer Commercial	Ja
Time Zero-Virenschutz	Ja
Schutz vor DHA, DoS und weiteren Angriffen	Ja
LDAP/Exchange Accelerator	Ja
Unterstützung mehrerer LDAP-Server	Ja
Verbindungsverwaltung mit IP Reputation	Ja
Compliance-Abo	
Zuverlässige Regelverwaltung	Ja
Scannen der E-Mail-Anhänge	Ja
Wörterbücher	Ja
Approval-Ordner/Workflow	Ja
Installation und Verwaltung	
Installationsaufwand	Weniger als 1 Stunde
Verwaltungsaufwand pro Woche	Weniger als 10 Min.
Kompatibel mit allen E-Mail-Servern	Ja
Single Sign-On	Ja
Verwaltung von Gruppen und Benutzern	Ja
Endbenutzer-Quarantäne und Einstellungen	Ja
Junk Mail-Bericht mit Freigabemöglichkeit	Ja
Überwachung, Reporting und Protokollverwaltung	Ja
Judgment Details	Ja
Schnelle Nachrichten-Suchmaschine	Ja
Clustering und Remote-Clustering	Ja

SonicWALL-Lösungen für umfassende Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT

SonicWALL Deutschland

Tel: +49 89 4545 946 www.sonicwall.de

SonicWALL Schweiz

Tel: +41 44 810 31 35 www.sonicwall.ch

SonicWALL Österreich

Tel: +41 44 810 31 35 www.sonicwall.at



PROTECTION AT THE SPEED OF BUSINESS™