



EMAIL SECURITY

SonicWALL E-Class Email Security for the Enterprise

- **Inbound and outbound e-mail threat management**
- **Highly available and scalable Split Mode architecture**
- **Regulatory compliance framework**
- **E-mail policy management**
- **Advanced Reputation Management**
- **Seamless multi-LDAP integration**
- **Robust reporting**
- **SonicWALL GRID Anti-Virus™**
- **DHA, Dos, and zombie attack protection**
- **Advanced end-user controls**
- **Rapid installation and ease-of-management**

High-Performance, Highly Scalable E-mail Security

Status quo vendors cannot keep up with today's increasing volumes of sophisticated e-mail attacks, stricter new compliance regulations and dynamic business environments. Enterprises demand powerful solutions that reduce costs and complexity.

Offering outstanding performance value, SonicWALL® E-Class Email Security delivers highly effective, responsive protection that streamlines administrative overhead. Available as appliances or software, the SonicWALL E-Class Email Security solutions, including the Email Security Appliance (ESA) ES6000 and ES8300 or E-Class Email Security Software, provide self-running, self-updating, future-proofed security. Scanning both inbound and outbound traffic, E-Class Email Security boosts productivity by stopping spam, viruses and phishing; and supports regulatory compliance by blocking leaks of confidential data.

SonicWALL E-Class is a line of premium, enterprise-class solutions offering outstanding protection and high-performance protection while delivering elegant simplicity and unparalleled value. The E-Class portfolio of products and services offers a comprehensive line of e-mail protection, network security and secure remote access solutions.

Features and Benefits

Inbound and outbound e-mail threat management monitors content passing bi-directionally through the SMTP gateway. Utilizing award-winning anti-spam, anti-phishing and advanced anti-virus technologies, SonicWALL stops inbound e-mail threats before they invade the network. Outbound e-mail and attachments are inspected and properly blocked or routed to prevent confidential information leaks.

Highly available and scalable Split Mode architecture let businesses flexibly mix and centrally manage SonicWALL E-Class software and appliances to effectively meet their needs, freeing e-mail administrators from the mandated limitations of competing vendors. SonicWALL offers a truly scalable, high availability, e-mail protection solution for archiving, outsourcing, managed services, mergers, acquisitions and expansion into globally distributed environments.

Regulatory compliance framework helps organizations become compliant by automating requirements set forth by laws such as HIPAA, SOX and GLBA. SonicWALL E-Class Email Security intelligently identifies e-mail that violates compliance policies; monitors and reports the problem; and uses policy-based routing to send mail to archiving and encryption technologies.*

E-mail policy management enables IT to enforce organizational policies such as preventing the dissemination of inappropriate content, protecting confidential information, adding e-mail disclaimers or blocking distribution of executables.

Advanced Reputation Management combines IP Reputation plus SonicWALL's GRIDprints to reject up to 80% of known junk e-mail at the connection stage with any remaining junk e-mail being removed in the Advanced Content Management stage. Advanced Reputation Management not only improves overall system scalability and performance but unlike other vendor's systems all connections are logged, offering greater peace of mind.

Seamless multi-LDAP integration ensures that SonicWALL E-Class Email Security solutions automatically synchronize with multiple LDAP servers to automatically manage e-mail addresses, accounts and user groups.

Robust reporting provides easily customizable, system-wide and granular reporting, including information on attack types, solution effectiveness and built-in performance monitoring. For system deployed in Split Mode, reporting and monitoring is completely centralized for all systems, saving valuable time and simplifying overall system management.

SonicWALL GRID Anti-Virus™ leverages SonicWALL's anti-virus and anti-spyware technology to deliver anti-virus and anti-spyware protection. SonicWALL also offers additional layers of protection with signature update subscriptions from McAfee™ and Kaspersky Lab™.*

DHA, Dos, and zombie attack* protection starts with powerful connection management capabilities to defer, throttle or block invalid connections before they reach your system. When combined with SonicWALL's anti-spam, anti-phishing and anti-virus capabilities these capabilities establish a complete solution for stopping all types of e-mail threats.

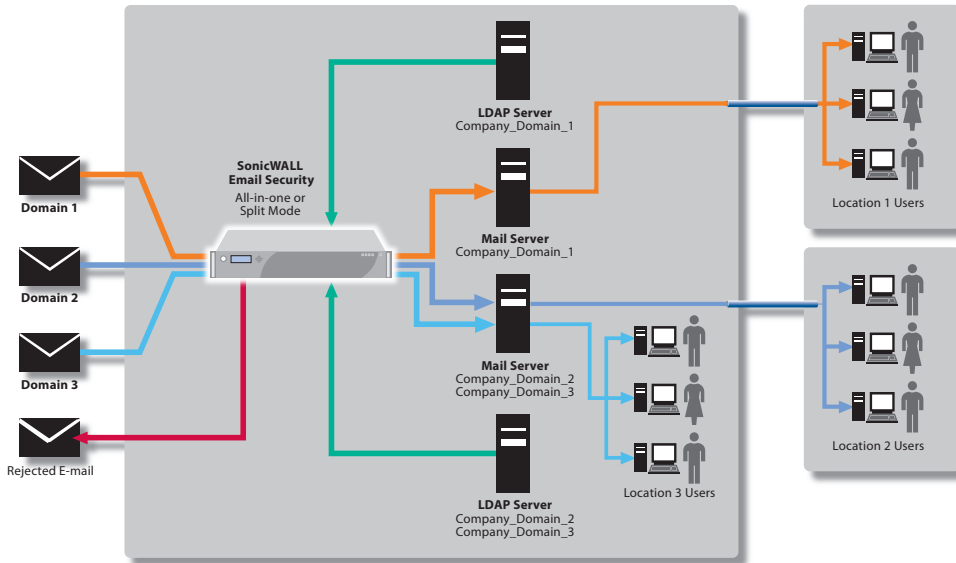
Advanced end-user controls enable administrators to give end-users greater control over their own spam management, allowed and blocked lists, spam aggressiveness, and account delegation. Using the downloadable Junk Button for Outlook® plug-in, end-users may actively respond to junk e-mail that inadvertently arrives in their inbox. The administrator defines all end-user controls, and may assign them by user, group or function.

Rapid Installation and ease-of-management drastically reduces the burden on IT departments to implement and manage a comprehensive e-mail security solution. Judgment Details provides insight into message judgment to ease troubleshooting and prevent legitimate e-mail from being junked.

*Additional subscription service required.

SonicWALL Email Security Deployments

The highly flexible architecture of SonicWALL Email Security (SES) enables deployments in organizations that require a highly scalable, redundant and distributed e-mail protection solution that can be centrally managed. SES can be deployed in either all-in-one or split mode. In split mode a system can be a remote analyzer or a control center. A typical split-mode setup is one or more **remote analyzers** connected to a **control center**: The **remote analyzer** receives e-mail from one or more domains and applies connection management, e-mail filtering (anti-spam, anti-phishing and anti-virus) and advanced policy techniques to deliver good e-mail to the downstream e-mail server. The **control center** centrally manages all remote analyzers and collects and stores junk e-mail from the remote analyzers. Centralized management includes reporting, and monitoring of all related systems. This paradigm allows SonicWALL Email Security to adapt its solution to protect both inbound and outbound e-mail for any organization in a cost-effective, comprehensive manner.



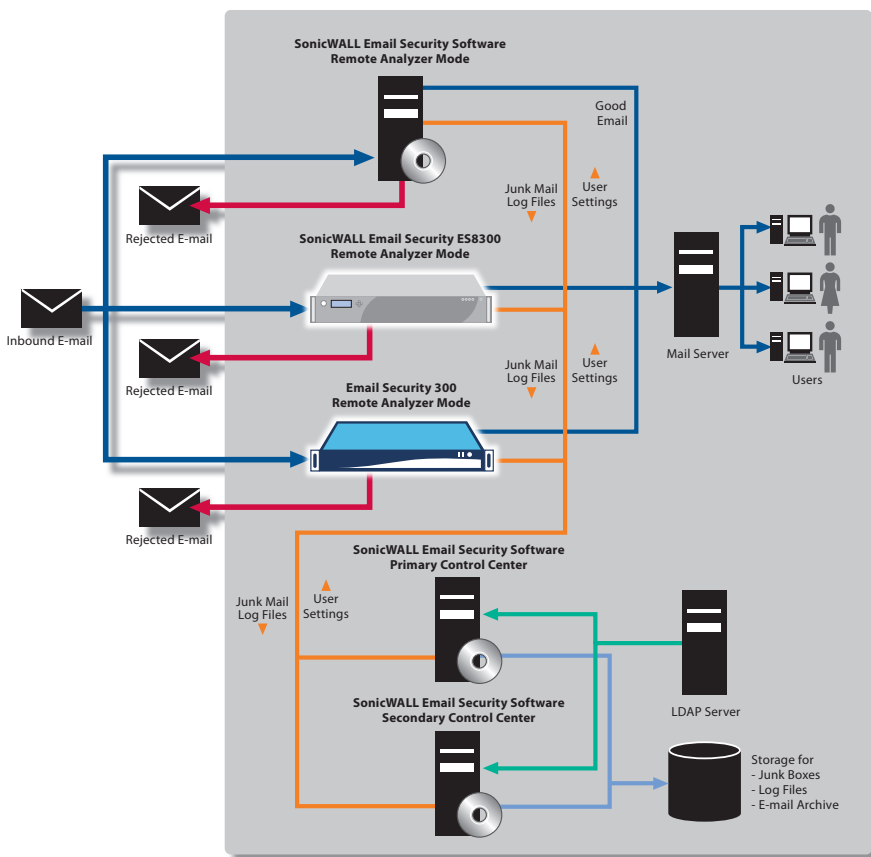
Multi-Domain, Central Control

SonicWALL Email Security centralizes management of multiple e-mail domains.

Typically used in medical consortiums, insurance companies, franchises, multi-brand/multi-division companies

Benefits

- Easy-to-use centralized management of multiple domains
- Apply corporate (centralized) e-mail policies to everyone and/or apply policies per domain/group/user
- Centralized per-domain reporting
- Centralized control over outbound e-mail to apply policy/routing rules per domain or on a corporate-wide basis



Scalable and Redundant

A centrally managed e-mail security system that is highly scalable, can utilize multiple types of platforms (appliances and software) and has failover built into the architecture as well as the hardware.

Typically used in medium and large enterprises, organizations with high uptime requirements for e-mail security, mixed platform environments or organizations with a requirement to store e-mail on SAN (Storage Area Network)

Benefits

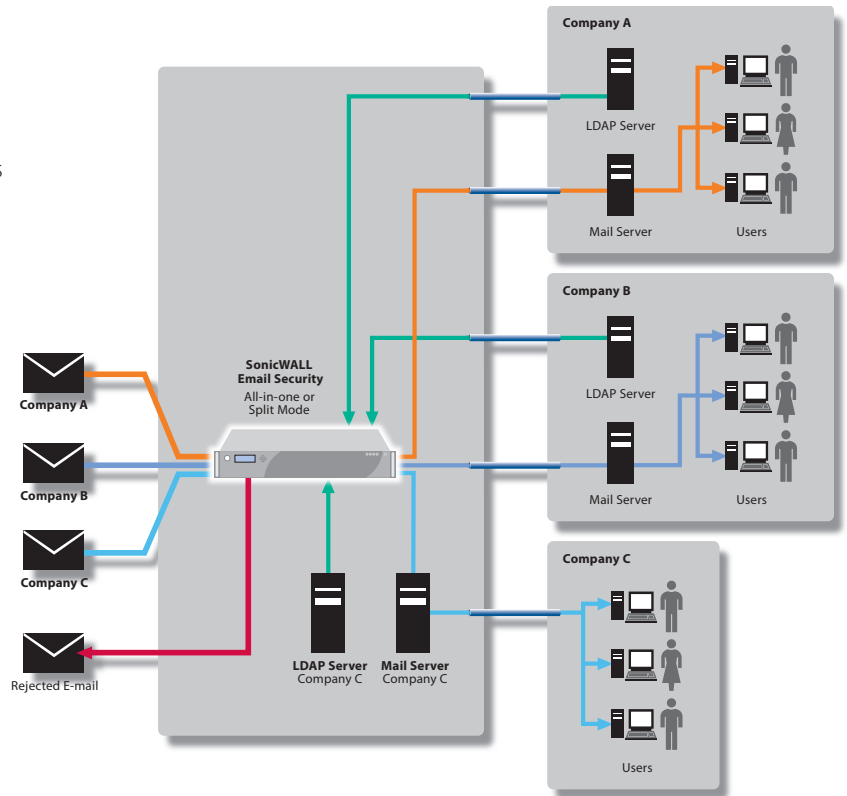
- Any remote analyzer can failover to any other remote analyzer—ensuring mail-flow continues
- Having primary and secondary control centers provides complete redundancy
- Storing e-mail, etc., on corporate SAN centralizes data storage and simplifies backup procedures
- Allowing mixed platforms to be centrally controlled reduces management overhead
- Adding a remote analyzer easily scales the system or extends deployment to other locations as desired

Managed Service Provider

A Managed Service Provider (MSP) can provide e-mail filtering services for their clients and possibly e-mail server services as well. The SonicWALL Email Security solution is flexible enough to allow for multiple domains that can be centrally managed by the MSP, but still allows a given client to have their own users, policy rules, Junk Boxes and more, all under the control of the MSP.

Benefits

- Centralized management of multiple domains to remove junk e-mail for everyone
- Centralized e-mail policies for everyone and/or client policies per domain/group/user
- Centralized reporting, with per-domain reporting
- Centralized control over outbound e-mail can be used for some or all of the clients, and policy/routing can be applied on per-domain basis
- Allows e-mail servers and LDAP servers to reside with the customer or with the MSP or any in combination
- Flexible expansion allows the MSP to start with a single system and scale as needed to the highly scalable, failover-enabled, split-mode architecture



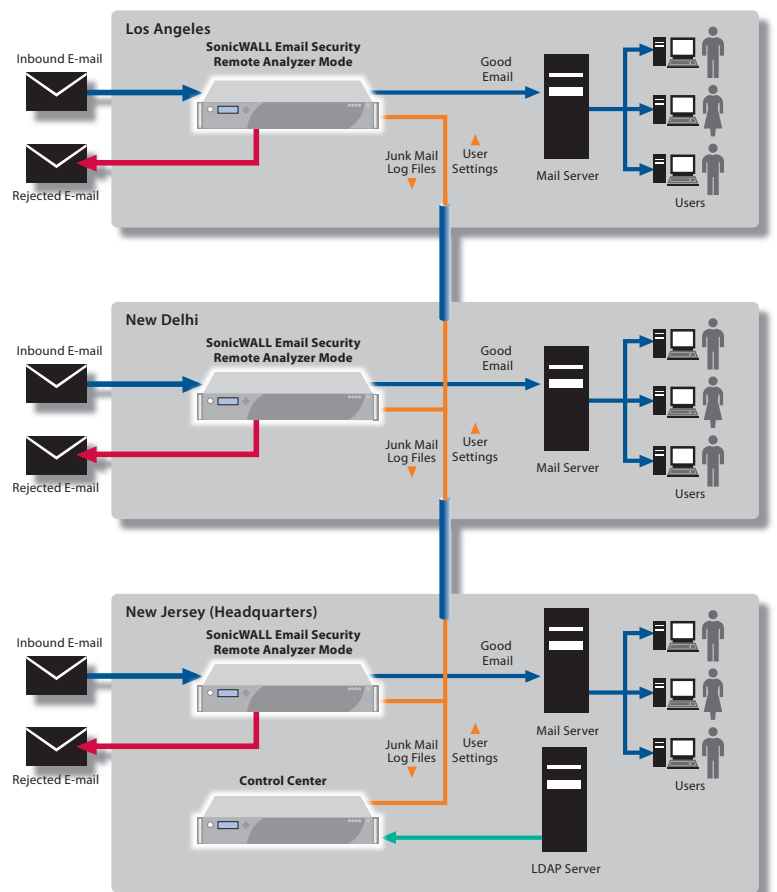
Multi-Location, Central Control

For distributed organizations, the optimal location for processing e-mail—centralized versus local—is critical: too centralized, and valuable IT time is wasted; too local, and corporate security can be compromised. The flexible SonicWALL Email Security architecture enables a solution that fits the unique needs of any distributed organization.

Typically used in companies with multiple locations, companies with recently added locations, such as through an acquisition or franchises that centralize the e-mail management of their corporate-owned or franchised operations

Benefits

- Localized processing of e-mail to remove junk and deliver good e-mail, reducing network traffic
- Centralized management of multiple locations, including policy enforcement, reporting and monitoring
- Centralized control over outbound e-mail to apply policy/routing rules per domain, per location or on a corporate-wide basis
- Clustering of remote analyzers allows for failover from location to location



Specifications

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



Software – E-Class

- SonicWALL Email Security Software
01-SSC-6636

Subscriptions – E-Class

- 5000 User Pack Subscriptions
- SonicWALL Email Protection with 24 x 7 support (1-year)
01-SSC-6674
- SonicWALL Email Compliance (1-year)
01-SSC-6644
- McAfee Anti-Virus with SonicWALL Time-Zero (1-year)
01-SSC-6764
- Kaspersky Anti-Virus with SonicWALL Time-Zero (1-year)
01-SSC-6774

(Visit www.sonicwall.com for additional user packs.)

Licensing Overview

SonicWALL E-Class Email Security (appliance or software)

- Message Transfer Agent (MTA)
- Directory Harvest Attack/Denial of Service Protection
- Web-based management
- Policy Management/E-mail Content Filtering
- Reporting and Monitoring
- LDAP Synchronization

Email Protection Subscription with Dynamic Support (8x5 or 24x7) – Required

- Anti-spam (1-year)
- 8x5 or 24x7 support (1-year)
- Anti-phishing (1-year)
- RMA (Appliance replacement)
- Software/Firmware Updates (1-year)

Compliance Subscription

- Dictionaries (Functionality)
- Approval Boxes
- Attachment Scanning
- Record ID Matching
- Encryption Reporting
- E-mail Archiving
- Predefined Policies
- Compliance Reports

Anti-Virus Subscription (Kaspersky Lab and/or McAfee with SonicWALL Time Zero Anti-Virus)

- Kaspersky Anti-virus
- SonicWALL Time Zero Anti-Virus
- McAfee Anti-virus
- Zombie Detection

Email Security Appliances	SMB (Available for smaller deployments)		E-Class (Enterprise)	
	300	500	ES6000	ES8300
Domains	Unlimited			
Operating System	Hardened SonicWALL Linux OS Appliance			
Rackmount Chassis	1U Mini	1U Mini	1U Mini	2RU
CPU(s)	2.66GHz	2.66GHz	3.2GHz	Quad Core Xeon 2.0GHz
RAM	1 GB	1 GB	2 GB	4 GB
Hard Drive	80 GB	2 x 80 GB	2 x 160 GB	4 x 750 GB
Redundant Disk Array (RAID)	–	X	X	RAID 5
Hot Swappable Drives	–	–	–	X
Redundant Power Supply	–	–	–	X
Dimensions	16.8 x 14.0 x 1.7 in 42.67 x 35.56 x 4.32 cm	16.8 x 14.0 x 1.7 in 42.67 x 35.56 x 4.32 cm	16.8 x 14.0 x 1.7 in 42.67 x 35.56 x 4.32 cm	27.5 x 19.0 x 3.5 in 69.9 x 48.3 x 8.9 cm
Weight	18 lbs 8.16 kg	19 lbs 8.62 kg	19 lbs 8.62 kg	50.0 lbs 22.7 kg
WEEE Weight	13 lbs 5.90 kg	14 lbs 6.35 kg	14 lbs 6.35 kg	48.9 lbs 22.2 kg
Power Consumption (Watts)	189	201	201	280
BTUs	644.49	685.41	685.41	1098.0
MTBF @25C in Hours	125,004 (est.)			
MTBF @25C in Years	14.27 (est.)			

Email Security Software	
Domains	Unlimited
Operating System	Runs on Microsoft Windows 2000 Server or Microsoft Windows 2003 Server
CPU	2.66 GHz minimum configuration
RAM	2 GB recommended, 1 GB minimum configuration
Hard Drive	40 GB additional minimum configuration

Appliance and Software Features – Subscriptions available for Enterprise Deployments in 1,000, 2,000, 5,000, and 10,000 user packs

Threat Protection	
Inbound and outbound e-mail protection	Yes
Anti-spam effectiveness	98%+
Anti-phishing identified separately	Yes
SonicWALL GRID Anti-Virus	Yes
Anti-Virus: Dual-layer Commercial	Yes
Time Zero Virus Protection	Yes
DHA, DoS, Other Attack Protection	Yes
LDAP/Exchange Accelerator	Yes
Multi-LDAP support	Yes
Connection Management with IP Reputation	Yes
Compliance Subscription	
Robust Policy Management	Yes
Attachment Scanning	Yes
Dictionaries	Yes
Approval Boxes/Workflow	Yes
Installation and Management	
Installation	< 1 hour
Management per week	< 10 min
Compatible with all e-mail servers	Yes
Single sign-on	Yes
Group and user management	Yes
End user quarantine and settings	Yes
Junk Box Summary actionable e-mail	Yes
Monitoring, Reporting and Log Management	Yes
Judgment Details	Yes
Rapid Message Search Engine	Yes
Clustering and Remote Clustering	Yes

SonicWALL, Inc.

2001 Logic Drive T +1 408.745.9600 www.sonicwall.com
San Jose, CA 95124 F +1 408.745.9300



PROTECTION AT THE SPEED OF BUSINESS™