

Scalable and Flexible Deployments

Enable email security cost-effectively for 10 or 100,000 mailboxes



Introduction

Easy to set up and administer, SonicWall™ Email Security is designed to cost-effectively scale from 10 to 100,000 mailboxes. It can be deployed as a hardware appliance, as a virtual appliance leveraging shared computing resources, or as software—including software optimized for Microsoft® Windows® Server or Small Business Server (SBS). Additionally, Email Security can be deployed as a cloud-based service or as an add-on service for SonicWall firewalls.

Optional high availability and scalable split mode let you centrally and reliably manage multiple enterprise-class deployments. In large distributed environments, multi-tenancy support lets you delegate sub-administrators to manage settings at multiple organizational units (such as enterprise divisions or MSP customers) within a single Email Security deployment.

The basics of SonicWall Email Security deployment

SonicWall Email Security 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 email from one or more domains and applies connection management, email filtering (anti-spam, anti-phishing and anti-virus) and advanced policy techniques to deliver good email to the downstream email server.
- The control center centrally manages all remote analyzers, and collects and stores junk email from the remote analyzers. Centralized management includes reporting, and monitoring of all related systems.

Below are sample deployments for SonicWall Email Security. Of course, every organization is different, but the deployments below demonstrate the flexibility and scalability of the SonicWall Email Security solution.

Optional high availability and scalable split mode let you centrally and reliably manage multiple enterprise-class deployments.

Multi-location, central control deployments for distributed organizations

This deployment is typical of distributed organizations where the optimal—location for processing email—centralized versus local—is critical. The flexible SonicWall Email Security architecture enables a solution that fits the unique needs of any distributed organization. This type of deployment is often found in organizations with multiple locations or organizations that have added locations through an acquisition. The local processing of email to remove the “junk” reduces overall network traffics while the centralized management ensures corporate control. An added benefit is that the remote analyzers can be “clustered” for failover from location to location if desired.

Flexible deployments for the Managed Service Provider

A Managed Service Provider (MSP) can provide email-filtering services for their clients and possibly email server services as well. The Email Security solution is flexible enough to allow for multi-tenancy and multiple domains that can be centrally managed by the MSP, but still allows a given client to have their own administrators, users, policy rules, junk boxes and more, all under the control of the MSP. Reporting is centralized, but can be done on a per-domain basis as required. Outbound email can be routed through the Email Security system for some or all clients as desired. In addition, the flexible architecture allows the MSP to start with

single system and easily move to the fail-over enabled, split-mode architecture as their business grows. MSPs can easily deploy additional virtual appliances for new or existing customers with minimal incremental investment.

Scalable and redundant deployments provide peace-of-mind

SonicWall Email Security is available as a hardware appliance, Windows server-software, and virtual appliance in a VMWare® environment; as a cloud-based solution through SonicWall partners; or as a hosted hybrid-cloud solution with the Comprehensive Anti-Spam Service on our SonicWall TZ, Network Security Appliance (NSA) and E-Class NSA Series appliances. Uniquely scalable, flexible and redundant, SonicWall Email Security works in stand-alone, distributed or clustered deployments. The highly flexible architecture of Email Security delivers scalable, redundant and centrally managed multi-location email protection that can be managed easily and centrally. The deployment and operational flexibility of SonicWall Email Security allows organizations to protect both inbound and outbound email in the most comprehensive and cost-effective manner available.

No on-premises installation required for hosted email security

With SonicWall Hosted Email Security, there is no hardware or software equipment to install on premises, minimizing upfront deployment expenses, capital and ongoing administrative costs.

© 2017 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING,

BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com