EXHIBIT 12

SONICWALL™

SonicWall™ Email Security 9.0

Release Notes

February 2017

These release notes provide information about the SonicWall™ Email Security 9.0 release.

Topics:

About Email Security 9.0

Email Security 9.0 provides a flexible solution to protect email from spam, phishing, and viruses. This release extends Email Security to a new family of appliances that takes advantage of 64-bit architecture. The new appliances are the ESA 5000, ESA 7000 and ESA 9000. New features were added and enhancements were made as well. Refer to New Features and Enhancements for more details.

IMPORTANT: Because Email Security 9.0 is a 64-bit implementation and prior versions are 32-bit, SonicWall recommends a fresh deployment for Email Security 9.0.

Email Security 9.0 is supported as firmware on SonicWall Email Security appliances, as a software installation on Windows Server systems, and as a Virtual Appliance on VMware ESXi platforms. See the following sections for detailed requirements:

- Supported Platforms
- Software Requirements
- Virtual Appliance Requirements

Supported Platforms

Email Security 9.0 firmware is supported on the following SonicWall appliances:

32-Bit Versions

- Email Security 3300
- Email Security 4300
- Email Security 8300

64-Bit Versions

- Email Security Appliance 5000
- Email Security Appliance 7000
- Email Security Appliance 9000

Software Requirements

When installed as software, SonicWall Email Security is supported on systems that meet the following requirements:

Requirements	Definitions
Processor	Intel Pentium: P4 or compatible CPU
Memory	8 GB of RAM
Hard Disk Space	Additional 160 GB minimum Recommend installation on a separate drive. Your storage needs are based on your mail volume, quarantine size, archived data, and audit settings.
Operating System	Microsoft Hyper-V Server 2012 R2 (64-bit) Microsoft Hyper-V Server 2012 (64-bit) Microsoft Hyper-V Server 2008(64-bit) Windows Server 2012 R2 (64 bit) Windows Server 2012 (64 bit) Windows Server 2008 R2 (64 bit) Windows Small Business Server (SBS) 2008 (64-bit)

Virtual Appliance Requirements

When installed as a Virtual Appliance, SonicWall Email Security is supported on systems that meet the following requirements:

Requirements	Definition
Processor	1 CPU, can be expanded to 8 CPU
Memory	8 GB of RAM, can be expanded to 64 GB
Hard Disk Space	160 GB thick provisioned hard disk space
VMware Platforms	ESXi 5.5 and newer

New Features and Enhancements

Email Security firmware has been updated to run on three new appliances that are being released concurrently. In addition, new features were added and enhancements made to improve protection from spam, phishing and viruses.

New features and enhancements include:

- Updated Email Security Appliances
- Capture ATP Integration
- Office 365 Support
- Improved Anti-Virus Offerings
- Performance Enhancements

Updated Email Security Appliances

The Email Security Appliances (ESA) have been refreshed. They are built using 64-bit architecture, offering increased memory and the option for faster, detachable disk drives. Appliance functionality focuses on:

- Effectively scanning inbound and outbound email
- Providing multi-layer protection
- Managing compliance and encryption

Refer to the *Email Security Appliance 5000 and Email Security Appliance 7000 Getting Started Guide* and the *Email Security Appliance 9000 Getting Started Guide* for more information about the appliances.

Capture ATP Integration

Capture Advanced Threat Protection (Capture ATP) is a cloud-based service that analyzes various types of content for malicious behavior, and this function is being extended to Email Security. It work similar to the anti-virus engines already integrated into Email Security and does the following:

- Scan suspected messages.
- Render a verdict about the message.
- Take action based on what the administrator configures for that verdict.

NOTE: All three anti-virus options (McAfee, Kaspersky, and Cyren) and Capture ATP need to be licensed separately to use Capture functionality.

Unlike the anti-virus engines that check against malware signatures stored locally, messages for Capture ATP are uploaded to the back end cloud servers for analysis. These messages are typically advanced threats that evade identification by traditional static filters. They need to be identified by their behavior, and thus need to be run in a highly instrumented environment. Capture ATP accepts a broad range of file types to analyze.

To engage Capture ATP:

1. Inbound email is first scanned by the other anti-virus plug-ins.
   - If a threat is detected, then the appropriate action is taken (discard, junk, tag, etc.).
   - If the service is enabled, all the anti-virus plug-ins return a *no threat* result ,and the message contains an eligible attachment, the email is sent to Capture ATP for analysis.
2. The attachment is uploaded to the Capture server and quarantined in the Capture Box.
3. Capture ATP performs the analysis and returns a verdict.
4. Further analysis is performed and Email Security applies the policy based on the final disposition of the message.

Capture ATP status and settings can be manage through the **Capture** command on the user interface. For details, refer to the *Email Security 9.0 Administration Guide*.

Office 365 Support

Organizations that use Office 365 for email can now route their email through their Hosted Email Security (HES) to get added protection for their messages. A path can be created based on both the sender domain and the source IP address so outbound mail from ISPs can be scanned while still maintaining the privacy of the IPS customer.

NOTE: Office 365 is supported only for Hosted Email Security; it is not supported for the on-premise products.

Customers are strictly limited to one ISP as the source for one outbound path. If a customer wants a second ISP that customer must configure a second path. Similarly, no IP addresses outside of the ISP-owned range are allowed on a shared-IP path. Only one path can handle email for a particular sender domain.

Because upstream TLS must be negotiated before the path is selected, weak ciphers are not allowed.

Improved Anti-Virus Offerings

Email Security 9.0 improved its core virus filtering capability with improved Kaspersky and Cyren filtering engines. Email Security integrated the Kaspersky 8.5 Anti-Virus DAT and scan engine and the Cyren 5.4.25 AV scan engine into the Email Security gateway and backend servers. Both utilizes 64-bit specific data for both Windows and Linux platforms. Both engines provide improved scanning and filtering to detect malicious content.

Performance Enhancements

Improvements have been made to the Email Security application that can lead to an improved user experience. Some message attributes can be sent to SonicWall for analysis. These features, when combined with other data, can be used to identify and track new trends in spam and other junk mail. Those trends can be used to refine configurations and filtering.

Be aware, when opting to share this information, some of the message attributes may contain human-readable information. Information about the sender, recipient, subject or content is accessible by SonicWall. It is, however, very difficult to recover the entire message that corresponds to a specific set of attributes.

Resolved Issues

This section provides a list of resolved issues in this release.

Administration

Resolved issue	Issue ID
Internet Explorer 11 cannot see Junk Box contents or auditing. Occurs after firmware upgrade to 8.3.1/8.3.2 and when customer enables **Display intranet sites in compatibility view** option.	179297
A scheduled backup isn't saved to the specified FTP destination. Occurs after updating to 8.3.2 while making use of special characters in the FTP password.	178780
Outbound paths do not support more than a class C subnet. Occurs when customers tried to use Office 365.	170510
On HES system, the global user view setup seems to override the per OU user view setup. Occurs when defining the user download settings. After navigating away from the page and then coming back to view it, it doesn't retain the settings you initially defined.	166525
Auditing fails to reveal attachment information. Occurs when trying to get details about an attachment and archiving is disabled.	162534

Anti-Spoofing

Resolved issue	Issue ID
DKIM check fails. Occurs for emails sent from AOL.com when DKIM is enabled.	148258

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.