

Introduction

This document answers a number of frequently asked questions about SonicWALL Email Security 6.0 and 5.0.x.

Frequently Asked Questions

What do the SonicWALL Email Security Products do for me?

SonicWALL Email Security can protect your email server from junk mail of all types: spam, phishing, Directory Harvest Attacks (DHA), and viruses. The product is most often configured as a first-touch server for inbound SMTP. It forwards good mail to your in-house mail server and stores or deletes junk mail. When the junk mail is stored, a friendly Web user interface allows viewing and un-junking by users. Email Security can also be used in your outbound SMTP email path.

Are the Email Security Products hardware or software?

The SonicWALL Email Security product line includes both hardware and software versions. We offer both Linux-based Email Security appliances and Email Security server software that can be run on your own Windows 2000 or Windows 2003 Server. One of the minimum requirements for running on Windows servers is a minimum of one Gigabyte (GB) of RAM.

How does Email Security fit into my existing network, and interact with my mail server?

The Email Security server uses a static IP address and is usually placed on the same private network as the mail server and LDAP server, since both communicate with it. It uses the same subnet mask, default gateway, and DNS settings as other devices on your network. On Windows servers, SonicWALL Email Security is aware of the TCP/IP properties already assigned to the server's Ethernet card, including the hostname. You will have to specify the desired IP address, subnet mask, default gateway, DNS settings, and hostname on the Email Security appliances in your network.

Your organization's inbound mail flow is based on a DNS record type called MX that usually points to a mail server name such as '**mail.sonicwall.com**', which then resolves to a public IP address like **67.115.118.12**. The firewall or router is usually configured to forward SMTP inbound from the public IP address to a private IP address on an internal network. Usually this configuration is pointing to a mail server. For example, the mail server might have an IP address of **192.168.219.8**. In this situation, the SonicWALL Email Security could use an IP address of **192.168.219.9**. SonicWALL Email Security will filter out junk mail, and will then send good mail on TCP port 25 to the mail server at **192.168.219.8**.

Tech Note

What is the easiest way to install and configure Email Security for protecting my inbound mail?

There are quite a few settings needed to get started, but you can usually finish within an hour. Besides email addresses for administrators, and the above types of TCP/IP settings, you will configure LDAP in most cases, and set preferences for handling spam and phishing. By default, the **Anti-Spam + Anti-Phishing** screen has **Action for messages marked as Definite Spam** (and Likely Spam) set to **'filtering off (deliver messages to users)'**, but SonicWALL recommends changing both to **'Store in Junk Box'**.

One important part of the configuration is on the **Server Configuration – Network Architecture** screen. This is where the **Inbound Path** is configured. After the inbound path is set, the firewall's inbound SMTP forwarding can be directed to the SonicWALL Email Security on IP address **192.168.219.9** as a first-touch email server. This configuration has three main sections, and usually you can use the following settings:

- 1) Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains: (such as **sonicwall.com**)
- 2) Listen on all IP addresses on port 25
- 3) Select one of the following:
 - This is a proxy. Pass all email to destination server: **192.168.219.8** on port 25 (No queuing or routing).
 - This is a Mail Transfer Agent (MTA). Route email using SmartHost to destination server: **192.168.219.8** on port 25.

Notes on this sample Inbound Path:

- Listing your domain(s) is crucial in part 1, so don't use the other option which has the open relay warning
- Part 2 is set this way by default and is safe that way
- Part 3 allows either MTA or proxy, but both ultimately forward good mail to the mail server IP address on the LAN. Proxy is a bit faster, but doesn't offer any queuing of mail when your mail server is down.

Can I use SonicWALL Email Security to protect multiple mail servers and multiple internet domains?

Yes, the inbound path configuration allows you to list multiple domains in step 1 above. That same inbound path has advanced destination options that allow the SonicWALL Email Security MTA to route inbound email for different domains to different downstream mail server IP addresses.

What kinds of traffic must be allowed by my firewall or router, inbound to the Email Security server?

The only inbound traffic type required for all configurations is SMTP (Simple Mail Transfer Protocol), on TCP port 25. Some customers will also allow external access to the browser-based Email Security user interface so that external users can login to view their junk box contents (which is usually needed only when the user needs to unjunk false positives).

Do I have to use SonicWALL Email Security for outbound traffic if I use it for inbound?

No.

Can SonicWALL Email Security block outbound junk mail when used for the outbound path?

Yes, but only when used with a SonicWALL Email Security Anti-Virus subscription. Email Security can be used to block outbound email traffic from infected computers (aka zombies), and/or to block outbound emails from users who are not in the LDAP directory listings.



Tech Note

What kinds of traffic must be allowed to the Internet outbound from the Email Security server?

SonicWALL Email Security servers and appliances need to regularly communicate with the SonicWALL Data Center for anti-spam updates, and to communicate with SonicWALL registration servers. Outbound HTTP (TCP port 80) traffic is required for these products to work properly. Many of the updates occur every five minutes and are very small, so you don't have to worry about large downloads happening all of the time. In some cases, where the local network doesn't have its own DNS servers, SonicWALL Email Security servers and appliances need to be able to send DNS queries out to the name servers configured in their settings. This requires the firewall or router to allow outbound UDP traffic on port 53.

For both Email Security 6.0 Software and Email Security 6.0 Appliance, a new licensing system is used. This new system has an additional requirement for outbound HTTPS traffic to the SonicWALL back end servers. This was not needed in Email Security 5.0.x .

Can I install SonicWALL Email Security Software on the same server as the one running Microsoft Exchange?

Yes you can, but the minimum memory requirements double from the normal 1 GB of RAM to 2 GB of RAM when both are combined on the same server. This also requires a few extra steps in the configuration of Exchange's SMTP properties, since it will need to run its SMTP services on a TCP port other than 25.

What if I don't host my own mail server?

If your ISP handles your mail for you, you cannot use the Linux-based SonicWALL Email Security Appliances or Email Security Software. You can run the SonicWALL Anti-Spam Desktop 5.0 Software to protect your email account from junk mail, which works only with Outlook and Outlook Express on Windows computers. This user-level product delivers many of the same features delivered by our server products.

How will I know if SonicWALL Email Security incorrectly judges a legitimate message as spam or some other kind of junk (false positive)?

You will receive a Junk Box Summary in your email from the SonicWALL Email Security server on a regular basis, assuming that Email Security is configured to store these messages in your Junk Box. The summary contains links which allow you to view or unjunk any message which is stored in the Junk Box. You can also log into your Junk Box using a Web browser, in most cases.

Document created: March, 2007

Last updated: 9/24/07

