

SonicWALL Email Security Appliances

EMAIL SECURITY

ES 4300

Getting Started Guide



SonicWALL ESA 4300 Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL Email Security 4300 appliance into an existing or new network.

SonicWALL ESA 4300 provides effective, high-performance, and easy-to-use inbound and outbound email threat protection. Ideal for any size business, this self-running, self-updating appliance delivers powerful protection. Combining anti-spam, anti-phishing, content filtering, policy management and content compliance capabilities in a single seamlessly integrated solution, SonicWALL Email Security provides powerful protection without complexity.

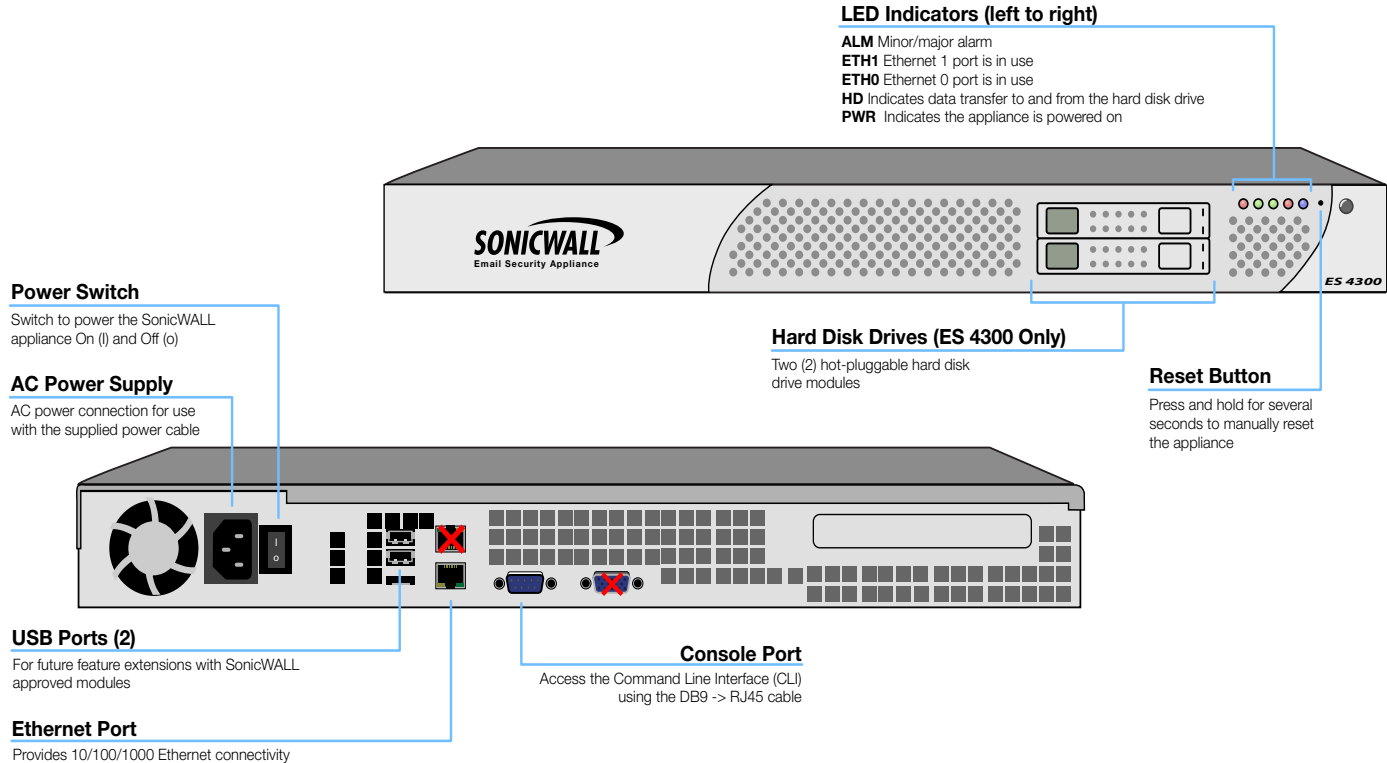
Please read this entire *Getting Started Guide* before setting up your *SonicWALL ESA 4300*. For more detailed technical documentation, refer to the *SonicWALL Email Security Appliance Administrator Guide* at:
<<http://www.sonicwall.com/us/support>>

Steps

Step	Procedure
1	<i>Pre-Configuration Tasks - page 1</i>
2	<i>Setting Up the SonicWALL - page 5</i>
3	<i>Preparing for First Use - page 11</i>
4	<i>Support and Training Options - page 19</i>
5	<i>Safety and Regulatory Information - page 25</i>

Overview of the SonicWALL ESA 4300

The graphic below is an overview of the Front and Rear panels of the SonicWALL ESA 4300 appliance.



In this Section:

This chapter provides pre-configuration information. Review this section before setting up your SonicWALL ESA 4300.

- *Checking ESA 4300 Package Contents* - page 2
- *What You Need to Begin* - page 3
- *Obtaining Configuration Information* - page 3

Checking ESA 4300 Package Contents

Before setting up your SonicWALL ESA, verify that your package contains the following parts:

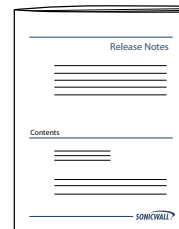
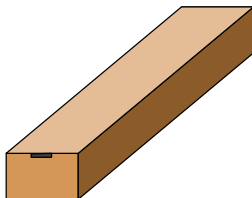
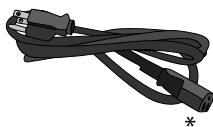
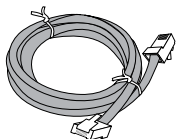
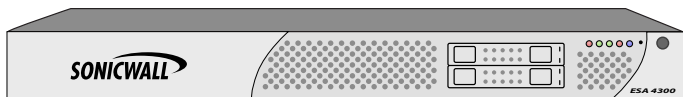
- SonicWALL Email Security 4300 Appliance
- Getting Started Guide
- Release Notes
- Ethernet Cable
- Standard Power Cord
- Rack Mounting Kit

Any Items Missing?

If any items are missing from your package, please **contact SonicWALL support**.

A listing of the most current support documents are available online at: <<http://www.sonicwall.com/us/support.html>>

*The pictured power cord is intended for use in North America only.



What You Need to Begin

To configure a SonicWALL ESA 4300, you must have a computer that meets or exceeds the following requirements:

- An Internet connection
- A computer to use as a management station for initial configuration of SonicWALL Email Security software
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

Accepted Browser	Browser Number Version
Internet Explorer	7.0 or higher
Firefox	3.0 or higher
Opera	9.10 or higher for Windows
Chrome	4.0 or higher
Safari	3.0 or higher for MacOS

For the latest list of supported Windows operating systems and service packs, refer to the *SonicWALL Email Security Release Notes* and the following web page:

<http://www.sonicwall.com/us/products/email_security_anti-spam_67.html>

Obtaining Configuration Information

Record the following configuration information to configure your SonicWALL ESA 4300:

Networking Information

Email Security IP Address: _____	Select a free static IP address in the range of your local subnet.
Email Security Subnet Mask _____	Enter the subnet mask for the local subnet.
Gateway IP Address _____	Record the IP address of your network's gateway device (such as your perimeter firewall/router).
DNS Server 1 _____ DNS Server 2 (optional) _____	Record your DNS server information.
Host Name _____	Record the fully qualified domain name within your network for your SonicWALL ESA 4300 (maximum 32 characters).

LDAP Server IP _____	Record the IP address or hostname of your directory services server, such as LDAP or Microsoft Active Directory.
-------------------------	--

General Information

Server Name: _____	Select a friendly name for your SonicWALL ESA 4300 (maximum 32 characters).
Password: _____	Select a password for your SonicWALL ESA 4300 (default is <i>password</i>).
Serial Number: _____	Record the serial number found on the label of your SonicWALL appliance.
Registration Code: _____	Record the registration code that is generated in mysonicwall.com . See Registering Your SonicWALL ESA 4300 Appliance section, on page 6.

In this Section:

This chapter contains instructions for connecting and registering your SonicWALL ESA 4300 appliance.

- *Registering Your SonicWALL ESA 4300 Appliance* - page 6
- *Connecting the SonicWALL ESA 4300 Appliance to Your Network* - page 9
- *Activating Your SonicWALL ESA 4300 Appliance* - page 10



Note: *Registration is an important part of the setup process and is necessary to receive the benefits of SonicWALL security services, firmware updates, and technical support.*

Registering Your SonicWALL ESA 4300 Appliance

The SonicWALL SonicWALL ESA 4300 appliance must be registered with the firmware license key before first use. Perform the following steps to register your SonicWALL appliance:

1. Supply power to your appliance by connecting the power cord into the back of the SonicWALL ESA 4300 and the other end into an appropriate power outlet.
2. Turn on the power switch of the appliance. The Power LED on the front panel is green when you power on the appliance. The HDD LED may blink while the appliance performs a series of diagnostic tests. When the HDD LED is no longer lit, the SonicWALL Email Security appliance is ready for configuration.
If the alert light stays lit, ensure that the power supply is properly plugged in.
3. Open a Web browser on the computer you are using to manage the SonicWALL ESA 4300. Navigate to: <http://www.mysonicwall.com>.
4. Enter your MySonicWALL account **username** and **password** in the appropriate fields and click **Submit**.



Note: *You must have a MySonicWALL account to register the SonicWALL ESA 4300.*

5. Under the **Quick Register** section of your MySonicWALL account, enter the **Activation Key** or **Serial Number** of the appliance.
6. Confirm your Serial Number, enter a Friendly Name for your appliance, and enter your Authentication Code in the **Quick Register > Add New Product** section.
7. Click **Register**. Follow the online prompts to fill out the survey and complete the registration process. A confirmation window displays when you have successfully completed the registration process.

Configuring Appliance Settings

Specific appliance settings must be configured for your appliance to communicate with your network. The following procedures configure local time zone settings and network settings on your appliance.

This section contains the following subsections:

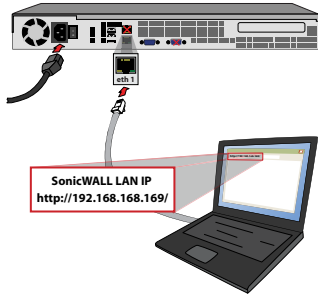
- [Logging Into the Web Management Interface - page 7](#)
- [Configuring Local Time Zone Settings - page 7](#)
- [Configuring Static IP Address - page 8](#)
- [Configuring Default Gateway Address - page 9](#)
- [Configuring Domain Name Server Address - page 9](#)


Logging Into the Web Management Interface

The SonicWALL Email Security appliance comes pre-configured with an IP address of **192.168.168.169**. Set the administration computer to have a static IP address on the 192.168.168.0/24 subnet.

To configure a static IP address on your computer, refer to [Configuring a Static IP Address](#) section, on page 18.

1. Connect the Ethernet cable from the **LAN (eth 1) port** on the SonicWALL to the **Ethernet port** of the computer.

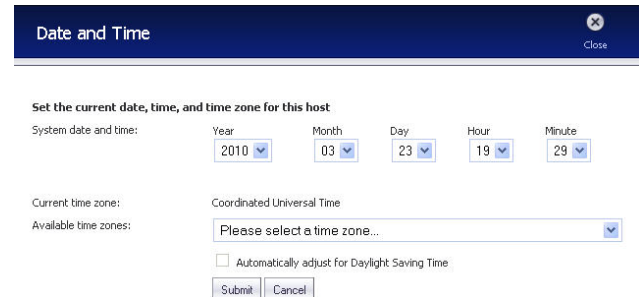


 **Note:** *One or more security warnings may display while connecting to the Email Security Web management interface. Accept the certificates in order to log in to the SonicWALL Email Security appliance.*

2. Open a Web browser and enter **http://192.168.168.169** (the default IP address of the appliance) in the **Location** or **Address** bar.
3. On the SonicWALL ESA 4300 Web management login screen, enter “admin” in the **Name** field and “password” in the **Password** field, select your language from the **Language** drop-down menu, and click **Login**.

Configuring Local Time Zone Settings

1. Navigate to **System > Host Configuration** in the left navigation menu.
2. Scroll down to the More Settings section, and click **Set Date and Time**.



Configure the following fields:

Field	Description
System date and time	Select the date (year, month, day) and time (hours:minutes) in 24-hour format.
Available Time Zones	Select your local time zone.
Automatically adjust for Daylight Savings Time	Select the checkbox if you would like to enable this feature.

3. Click **Submit** to save changes.

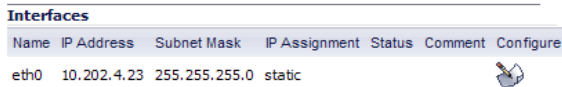
Your SonicWALL ESA 4300 appliance is now set to your local time. The Web management interface may log you out after the time is set. This is normal—Just log in again.


Configuring Static IP Address

Once the IP address of your SonicWALL ESA 4300 appliance is changed, you cannot access the appliance without this address. Before continuing, enter the chosen IP address for your SonicWALL ESA 4300 appliance.

Email Security IP address:	_____
-----------------------------------	-------

1. On the **Network > Settings** page of the Web Management interface, click the **Configure** icon in the **Interfaces** table.



Interfaces						
Name	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
eth0	10.202.4.23	255.255.255.0	static			

2. In the **IP Address** field, enter an unused static IP address that is within the range of your local subnet.



Note: *Using an IP address within the range of a local subnet is usually accomplished by keeping the first three groups of numbers (**xxx.xxx.xxx.xxx**) of the LAN IP address the same.*

3. Enter your subnet mask, for example, 255.255.255.0.
4. In the **Comment** field, optionally enter a descriptive comment such as “WAN” or “DMZ” to identify your appliance if you have more than one.
5. Click **OK**.
6. Click **Accept** at the top of the screen to save your settings.

Your SonicWALL ESA 4300 appliance is now set to communicate with your network using a static IP address. Disconnect your management computer from the appliance and continue to the next section to connect the appliance to your local area network. Note that you may lose connectivity with the SonicWALL ESA 4300 appliance during an IP address change. This occurs because the appliance is now on a different subnet than the management computer.

Configuring Default Gateway Address

Configure the static IP address before configuring the default gateway address settings to register and use your SonicWALL ESA 4300 appliance.

Default Gateway:	_____
------------------	-------

1. Navigate to **Network > Settings** in the left navigation menu.
2. Click the **Configure** icon in the **Network Routes** table.
3. Enter the IP address of your gateway device and click **OK**.
4. Click **Accept** at the top of the screen to save your settings.

Configuring Domain Name Server Address

Configure the DNS address settings to register and use your SonicWALL ESA 4300 appliance. The DNS server must be able to resolve external Internet names.

My SonicWALL DNS address:	_____
------------------------------	-------

1. Navigate to **Network > Settings** in the left navigation menu.
2. Scroll down to **Name Servers** and click **Add...**

3. In the **Add/Entry** field, enter a single Domain Name Server and click **OK**. Repeat steps 2 and 3 to add additional DNS entries.
4. Click **Accept** at the top of the screen to save your settings.

Connecting the SonicWALL ESA 4300 Appliance to Your Network

Your SonicWALL Email Security appliance is designed to operate in most network setups with minimal configuration. The diagrams below provide before and after views of a network using SonicWALL Email Security.

To physically connect your SonicWALL ESA 4300 appliance to your network:

1. Plug one end of the provided Ethernet cable into the LAN port on the back of your appliance.
2. Plug the other end of the Ethernet cable into an open port on your network hub or switch.
3. Plug the supplied power cable into the back of the appliance.
4. Plug the other end of the supplied power cable into an AC socket. The appliance automatically powers on and begins the initial boot process.

Your SonicWALL Email Security Appliance will perform better if you follow proper shutdown procedures. To shut down your appliance, use the web interface, or press the power button on the front of the appliance once. Holding down the power button or unplugging your appliance does not give it time to write all the data from volatile memory in to stable memory, and you may lose settings or data.

Activating Your SonicWALL ESA 4300 Appliance

SonicWALL Email Security provides dynamic licensing, which allows you to activate your licenses by logging into your mysonicwall.com account. Mysonicwall.com server uses the serial number and authentication code that came with your Email Security appliance.

1. Log in to mysonicwall.com.
2. Choose **My Products** from the left navigation bar.
3. Enter your serial number, the friendly name if you wish, and choose the product group. The serial number is found on the tri-fold postcard or email that confirmed your SonicWALL Email Security order.
4. Click **Register**. The product is added to the list of your registered products, and you can click on it to add or activate services.

5. You can check that the registration is correct by logging in to your SonicWALL Email Security administration site and clicking **System/License Management**. All your license information should be available. If it is not, click **Test Connectivity to SonicWALL** to check that you are connected.



Note: *If you purchased Total Secure Email, licensing is automatic and you do not need to take any action activate your licenses.*

In this Section:

This section provides instructions to configure your SonicWALL ESA 4300 appliance for first time use.

- *Initial Configuration Settings* - page 12
- *The SonicWALL Email Security Interface* - page 14
- *Verification* - page 17
- *Configuring a Static IP Address* - page 18

Initial Configuration Settings

The first time you log in to the SonicWALL Email Security appliance, you are directed to the system configuration page. Configure your settings as follows:

Monitoring

Email address of the administrator who receives emergency alerts	The email address of the mail server administrator. Enter the complete email address. For example, <i>user@example.com</i>
Postmaster for the MTA	The email address of the Mail Transfer Agent administrator who will receive non-deliverable receipts. For example, <i>mail@example.com</i>
Name or IP address of backup SMTP servers	Enter fully qualified domain names or IP addresses. For example, <i>mail2.example.com</i> or <i>10.100.0.1</i>

Hostname and Networking

Hostname	Enter a hostname you can use within your network to address the SonicWALL Email Security appliance. Enter a fully qualified domain name. For example, <i>emailsecurity.example.com</i>
Get all network settings from DHCP	Select this if you want your SonicWALL Email Security appliance to get dynamic IP settings from the DHCP server on your network.
Use the static settings below	Select this to assign your SonicWALL Email Security appliance a static IP address. Enter: <ul style="list-style-type: none">• This machine's IP address• Primary DNS server IP address (the local DNS server that has the MX record for your mail server)• Fallback DNS server IP address• Default gateway IP address• Subnet mask

Date and Time

System Date and Time	Select the current year, month, day, hour, and minute.
Current Time Zone	Displays the currently configured time zone.
Available Time Zones	Select the time zone for your area.
Automatically Adjust for Daylight Savings Time	Select this if your area observes Daylight Saving Time.

Select the proper time zone to ensure optimal network performance of your SonicWALL Email Security appliance.

1. Click **Apply Changes** to save this configuration.
2. A popup will display. Click **Continue** to reboot the SonicWALL Email Security appliance with your new settings.
3. Disconnect the crossover cable from the SonicWALL Email Security appliance.
4. Reset your administration computer's IP settings to work with your network. For example, if your network uses DHCP, reset your Local Area Connection to obtain an IP address and DNS settings dynamically from the server.
5. Reconnect your administration computer to your network. You will use the network to access the SonicWALL Email Security appliance in the next steps.



Alert: *Your ESA 4300 is equipped with a battery backup unit on the RAID Controller Card, which allows the appliance to write volatile memory to disk in the event of a loss of power. This battery backup unit must be charged for 24 hours. When deploying your ESA 4300 appliance, follow the startup and registration instructions detailed in this document, and then allow the battery backup in the unit to charge for 24 hours. If the battery is not fully charged, some RAID features are turned off, and the appliance performance is temporarily impaired until the battery is fully charged.*

The SonicWALL Email Security Interface

This section describes the SonicWALL ESA 4300 administrator's interface. For a detailed SonicWALL Email Security user interface overview, refer to the *SonicWALL Email Security Administrator's Guide*.

The screenshot displays the SonicWALL Email Security Administrator's Interface. The top navigation bar includes the SonicWALL logo, the text "Email Security", and "Help" and "Log out" buttons. A left sidebar contains a menu with categories like "System", "Anti-Spam, Anti-Phishing", "Anti-Virus Techniques", "Auditing", "Policy & Compliance", "Users & Groups", "Junk Box", and "Reports & Monitoring". The main content area is titled "License Management" and includes a sub-header "System / License Management". Below this, there is a note: "Check system status under Reports & Monitoring". A table displays license information for various services, with a "Serial Number: 004010221DD4" displayed above it. The table has columns for "Security Service", "Status", "Count", and "Expiration". Below the table are three buttons: "Manage Licenses", "Refresh Licenses", and "Upload Licenses". At the bottom of the interface, there are links for "Contact us", "About", and "Sign in as any user", along with "Language" and "System hostname: myrtle".

System /

License Management

Check system status under Reports & Monitoring

Serial Number: 004010221DD4

Security Service	Status	Count	Expiration
Users	Licensed	2000	
Email Security	Licensed		Never
Email Protection Subscription (Anti-Spam and Anti-Phishing)	Free Trial		29 Feb 2008
Email Anti-Virus (McAfee and SonicWALL Time Zero)	Licensed		29 Feb 2008
Email Anti-Virus (Kaspersky and SonicWALL Time Zero)	Licensed		29 Feb 2008
Email Compliance	Licensed		29 Feb 2008
Email Security Transition	Perpetual		Never

Manage Licenses Refresh Licenses Upload Licenses

Contact us | About | Sign in as any user Language | System hostname: myrtle

Changing the Default Administrator Password

To protect your appliance, change the password from its default.

1. Log in to the SonicWALL Email Security appliance using the IP address you entered in *Hostname and Networking* - page 12.
2. Enter a new management password.
3. Navigate to the **System > Administration** page.
4. Enter it again in the **Confirm Password** field.
5. Click **Apply Changes**.

Using Quick Configuration to Set Up Email Management

The Quick Configuration page walks you step-by-step through the configuration of your SonicWALL Email Security appliance. Use this window the first time you configure SonicWALL Email Security if you are installing SonicWALL Email Security as an All-In-One server and have only one downstream server.

The information you enter for LDAP configuration is used to authenticate users as they log in to their personal Junk Boxes.

For detailed configuration instructions, refer to the SonicWALL Email Security Administrator's Guide.

1. Navigate to the **System > Administration** page.
2. Click **Click Here for Quick Configuration**.
3. In the Quick Configuration dialog box under **Network Architecture**, enter the host name or IP address and the port into the **Inbound destination server** fields.

The inbound destination server is the email server that will accept good email after SonicWALL Email Security removes and quarantines junk email. For example, this could be the IP address of a Microsoft Exchange server. The default port is 25.

1. Network Architecture

(Use this pane to configure the inbound and outbound message processing paths.)

Inbound destination server: [What is this?](#)
Host name or IP address Port

Inbound SMTP setup:

Allow SMTP recipient addresses to all domains on inbound path or...
(Warning: may make an open relay.)

Only allow SMTP recipient addresses to these domains on inbound path

Separate domains with a <CR>. Example:
example.com
example.net

Outbound path setup:

If the above server contacts SonicWALL Email Security, assume all messages it routes through SonicWALL Email Security are outbound email and route them across the internet using MX records.

4. For Inbound SMTP setup, select one of the following:
 - **Allow SMTP recipient addresses to all domains on inbound path or...**
This option does not restrict incoming email to any domain.
 - **Only allow SMTP recipient addresses to these domains on inbound path**
This option allows you to specify the domains to which incoming email will be delivered. In the text box, type the allowed domains one per line.
5. Click **Test Mail Servers** to verify connectivity to the downstream Email Security server specified in preceding steps.
6. Select the **Outbound path setup** check box to route outbound email across the Internet using MX records.

7. Under LDAP Configuration, enter a hostname or IP address into the **LDAP server name** field. This is often your Exchange server or email server.

2. LDAP Configuration

Use this pane if you use default LDAP queries, no SSL, and the default LDAP port. Otherwise, your setup is too complicated to use quick configuration.

LDAP server name: [What is this?](#)

LDAP server type:

Login name: [What is this?](#)

Password:

NetBIOS domain names:
(For Active Directory and Exchange 5.5 servers.) [What is this?](#)

8. Select your LDAP server type.
9. Enter a valid LDAP login name and password.
10. Click **Test LDAP Login** and **Test LDAP Query** to verify your settings.
11. Enter one or more NetBIOS domain name in the **NetBIOS domain names** field. Click **What is this?** for more information.
12. Under Message Management, specify how junk mail will be handled by selecting one of the following:
 - **Quarantine junk** - sends junk mail to the user's junk box
 - **Deliver all messages to users** - does not separate junk mail from good email

13. Under Junk Box Summary, select **Send daily summaries** to receive daily summary messages about junk mail caught by SonicWALL Email Security.
14. To allow users to preview their junk mail messages without unjunking them, select **Users can preview their own quarantined junk mail**.
Summaries will contain a preview link for each junk email.
15. Type the URL where users can view their email junk boxes in the **URL for user view** field. Click **Test this Link** to verify connectivity.
16. Under Updates, click **Test Connectivity to SonicWALL** to test your connection to mysonicwall.com for automated software updates.
17. Click **Apply Changes**.

Verification

Routing Mail to Your SonicWALL ESA 4300

For your SonicWALL Email Security appliance to start filtering and monitoring mail, you must re-route mail traffic through your SonicWALL Email Security appliance. Mail traffic must pass from the Internet to the appliance, and then the appliance sends the good mail on to your mail server.

You have two choices for routing mail traffic to your SonicWALL Email Security appliance instead of to your mail server:

- Change the MX record in your DNS server to resolve to the IP address of your SonicWALL Email Security appliance.
You may have to work with your ISP to change this record.

- Create a rule in your firewall or router to route all port 25 (SMTP mail) traffic to your SonicWALL Email Security appliance. Refer to your firewall or router documentation for instructions on creating rules to route traffic.

Verifying Mail from the Internet Through Your SonicWALL ESA 4300

1. Go to an external mail account, for example Yahoo mail or GMail.
2. Create a new email message:

To	An email address where you receive email that is on the mail server for which you have configured the SonicWALL Email Security appliance.
Subject	SonicWALL Email Security Verification Message
Body	SonicWALL Email Security Verification Message

3. Send the message.
4. In the SonicWALL Email Security appliance administrative interface, click **Auditing**.
5. Check the **Inbound** auditing reports to make sure the email appears as Delivered.
6. Check the mail account you sent the message to. If you received the message, you have correctly configured your SonicWALL Email Security appliance.

Configuring a Static IP Address

Complete the following section based on your operating system in order to configure your management computer with a static IP address:

Windows XP

1. From the **Start** menu, highlight **Connect To** and then select **Show All Connections**.
2. Open the **Local Area Connection Properties** window.
3. Double-click **Internet Protocol (TCP/IP)** to open the **Internet Protocol (TCP/IP) Properties** window.
4. Select **Use the following IP address** and type **192.168.168.50** in the **IP address** field.
5. Type **255.255.255.0** in the **Subnet Mask** field.
6. Click **OK** for the settings to take effect.

Windows Vista

1. On the Windows **Start** menu, right-click **Network** and select **Properties**.
2. In the **Tasks** menu, click **Manage network connections**. The Network Connections window displays.
3. Right-click on your **Local Area Connection** and select **Properties**.
4. In the list, double-click **Internet Protocol Version 4 (TCP/ IP)**
5. Select **Use the following IP address** and type **192.168.168.50** in the **IP address** field.
6. Type **255.255.255.0** in the **Subnet Mask** field.
7. Click **OK**, and then click **OK** again for the settings to take effect.

If you are not using Windows XP or Windows Vista, please consult your operating system instructions to configure a static IP address for your system.

In this Section:

This chapter provides an overview of customer support and training options for the SonicWALL ESA 4300.

- *Customer Support* - page 20
- *Knowledge Base* - page 20
- *SonicWALL Live Product Demos* - page 21
- *Related Documentation* - page 21
- *User Forums* - page 22
- *Training* - page 23
- *SonicWALL Secure Wireless Network Integrated Solutions Guide* - page 24

Customer Support

SonicWALL offers Web-based and telephone support to customers who have a valid Warranty or who purchased a Support Contract. Please review our Warranty Support Policy for product coverage. SonicWALL also offers a full range of consulting services to meet your needs, from our innovative implementation services to traditional statement of work-based services.

For further information, visit:

<http://www.sonicwall.com/us/support/contact.html>



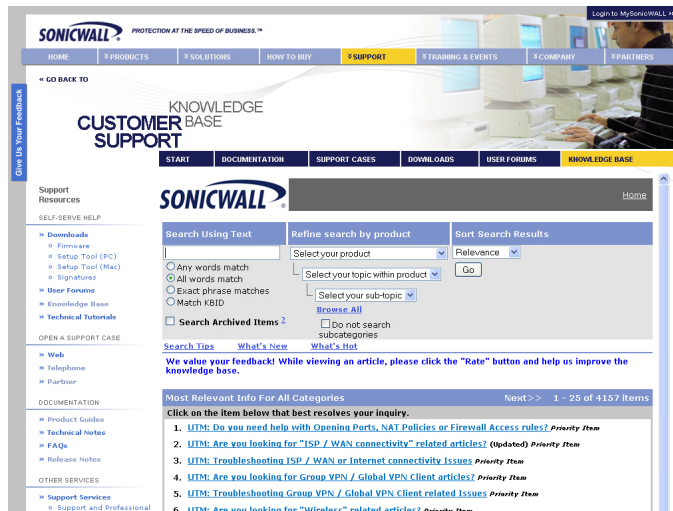
Knowledge Base

The Knowledge Base allows users to search for SonicWALL documents based on the following types of search tools:

- Browse
- Search for keywords
- Full-text search

For further information, navigate to the **Support > Knowledge Base** page at:

<http://www.mysonicwall.com/>



SonicWALL Live Product Demos

Get the most out of your Global Management System with the complete line of SonicWALL products. The SonicWALL Live Demo Site provides free test drives of SonicWALL security products and services through interactive live product installations:

- Unified Threat Management Platform
- Secure Cellular Wireless
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Secure Wireless Solutions
- Email Security
- SonicWALL GMS and ViewPoint

For further information, visit:

<http://livedemo.sonicwall.com/>

SONICWALL Live Demo

Click an Appliance to Launch Demo

UTM / Firewall / VPN / CSM

Management & Reporting

SSL VPN Secure Remote Access

Backup & Recovery

NSA E7500

NSA 2400

NSA 240

TZ 210 Wireless

TZ 190 Wireless

SONICWALL E-Class NSA

Blistering UTM performance robust enough for the most demanding environments.

Introducing an industry first re-assembly free deep packet inspection engine in combination with multi-core specialized security microprocessors to deliver gateway anti-virus, anti-spyware and intrusion prevention at high-speed so you don't have to sacrifice network performance.

Installed at This Site:
NSA E7500 with SonicOS Enhanced 5.4.1.0

Related Documentation

See the following related documents for more information:

- *SonicWALL Email Security Administrator's Guide*
- *SonicWALL Email Security User's Guide*

For further information, visit:

<http://www.sonicwall.com/us/support/289.html>

SEARCH | SITE MAP | NORTH AMERICA | WORLDWIDE

SONICWALL

HOME | PRODUCTS & SOLUTIONS | HOW TO BUY | SUPPORT | COMPANY | CHANNEL PARTNERS | MY SONICWALL

GO BACK TO

PRODUCT GUIDES REFERENCE LIBRARY

SUPPORT RESOURCES

- Recently Published
- Guides for UTM / Firewall / VPN Products
- Guides for Secure Remote Access Products
- Guides for Email Security Products
- Guides for Content Security Mgmt Products
- Guides for Backup & Recovery Products
- Guides for Management & Reporting Products
- Guides for Security Services
- Guides for SonicOS
- Guides for Support Services

SELF-SERVE HELP

- » Downloads
 - Firmware
 - Setup Tool
 - Signatures
- » User Forums
- » Knowledge Portal

OPEN A SUPPORT CASE

- » Web
- » Telephone
- » Partner

REFERENCE LIBRARY

- » Product Guides
- » Tech Notes
- » FAQs
- » Release Notes

RECENTLY PUBLISHED

#	Date	Description
1	07.17.2007	SonicWALL CDP 3.0 Administrator's Guide
2	07.13.2007	SonicWALL CDP 3.0 Site-to-Site Feature Module
3	06.30.2007	SonicOS Enhanced 4.0 Virtual Access Points Feature Module
4	06.30.2007	SonicOS Enhanced 4.0 Application Firewall Feature Module
5	06.30.2007	SonicOS Enhanced 4.0 Packet Capture Feature Module

Guides for UTM / FIREWALL / VPN Products

#	Date	Description
---	------	-------------

User Forums

The SonicWALL User Forums is a resource that provides users the ability to communicate and discuss a variety of security and appliance subject matters. In this forum, the following categories are available for users:

- Content Security Manager topics
- Continuous Data Protection topics
- Email Security topics
- Firewall topics
- Network Anti-Virus topics
- Security Services and Content Filtering topics
- SonicWALL GMS and Viewpoint topics
- SonicPoint and Wireless topics
- SSL VPN topics
- NSA 2400MX / Wireless WAN - 3G Capability topics
- VPN Client topics
- VPN site-to-site and interoperability topics

For further information, visit:

<<https://forum.sonicwall.com/>>



SonicWALL Forums

Welcome, amendoza@sonicwall.com.
You last visited: 01-01-1970 at 12:00 AM
Private Messages: Unread 0, Total 0.

User CP | FAQ | Calendar | New Posts | Search | Quick Links | KnowledgePortal | Log Out

Forum	Last Post	Threads	Posts
Firewalls Firewall related topics			
Network Networking related topics.	Multiple T-1's and Sonicwall... by theynon Today 10:56 PM	4,538	19,051
VPN VPN site to site and interoperability topics	VPN client for MAC OSX adn... by mdominquez@marlinengineering.com Today 08:52 PM	1,973	6,800
VPN Client VPN Client related topics	VPN Global Client behind a... by mdominquez@marlinengineering.com Today 02:44 PM	1,795	8,366
SonicPoint / Wireless SonicPoint and wireless related topics	IP Helper and DHCP on 2040... by idement@shetm.com Today 08:26 PM	536	2,492
SGMS / Viewpoint SGMS and Viewpoint related topics	Pls help--No syslog files... by indcenter Today 08:36 PM	756	2,650
Security Services All IPS, Gateway Anti-Virus, Anti Spyware, Client AV, Application Firewall, and Content Filtering topics	AV and Spyware updates? by Huegel_admin Today 09:41 AM	1,062	4,316
Network Anti-Virus Network Anti-Virus related topics	Network Antivirus Blocking... by templeiv@yahoo.com 07-20-2008 01:56 AM	225	1,028
TZ 190 / Wireless WAN 3G Capability on the new TZ 190	SonicOS Enhanced 3.9.0.1e... by jamesright22 Today 07:38 PM	113	461
Misc Miscellaneous topics relating to SonicWALL firewalls	SDH03 Upgrade to TZ180 by PAWFELD Today 02:21 PM	1,112	4,047
SonicWALL SSL-VPN SSL-VPN Topics			
SSL-VPN 4000 SSL-VPN 4000 related topics	unsupported authentication... by johnt@alaskabilingservices.com Today 08:02 PM	58	253

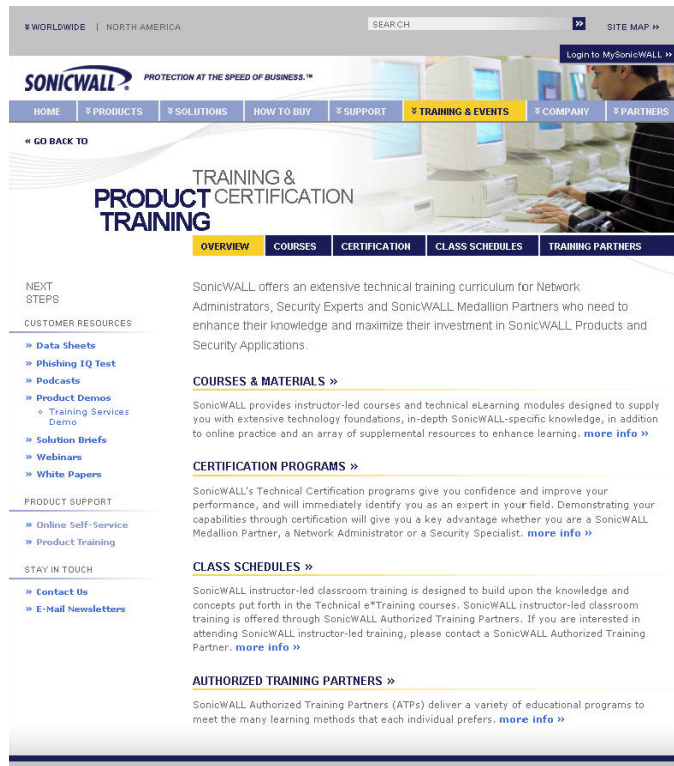
Training

SonicWALL offers an extensive sales and technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications. SonicWALL Training provides the following resources for its customers:

- E-Training
- Instructor-Led Training
- Custom Training
- Technical Certification
- Authorized Training Partners

For further information, visit:

<<http://www.sonicwall.com/us/support/training.html>>



WORLDWIDE | NORTH AMERICA

SEARCH

Log in to MySonicWALL

SONICWALL PROTECTION AT THE SPEED OF BUSINESS.™

HOME | PRODUCTS | SOLUTIONS | HOW TO BUY | SUPPORT | **TRAINING & EVENTS** | COMPANY | PARTNERS

GO BACK TO

TRAINING & CERTIFICATION

PRODUCT TRAINING

OVERVIEW | COURSES | CERTIFICATION | CLASS SCHEDULES | TRAINING PARTNERS

NEXT STEPS

CUSTOMER RESOURCES

- » Data Sheets
- » Phishing IQ Test
- » Podcasts
- » Product Demos
 - » Training Services Demo
- » Solution Briefs
- » Webinars
- » White Papers

PRODUCT SUPPORT

- » Online Self-Service
- » Product Training

STAY IN TOUCH

- » Contact Us
- » E-Mail Newsletters

SonicWALL offers an extensive technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications.

COURSES & MATERIALS »

SonicWALL provides instructor-led courses and technical eLearning modules designed to supply you with extensive technology foundations, in-depth SonicWALL-specific knowledge, in addition to online practice and an array of supplemental resources to enhance learning. [more info »](#)

CERTIFICATION PROGRAMS »

SonicWALL's Technical Certification programs give you confidence and improve your performance, and will immediately identify you as an expert in your field. Demonstrating your capabilities through certification will give you a key advantage whether you are a SonicWALL Medallion Partner, a Network Administrator or a Security Specialist. [more info »](#)

CLASS SCHEDULES »

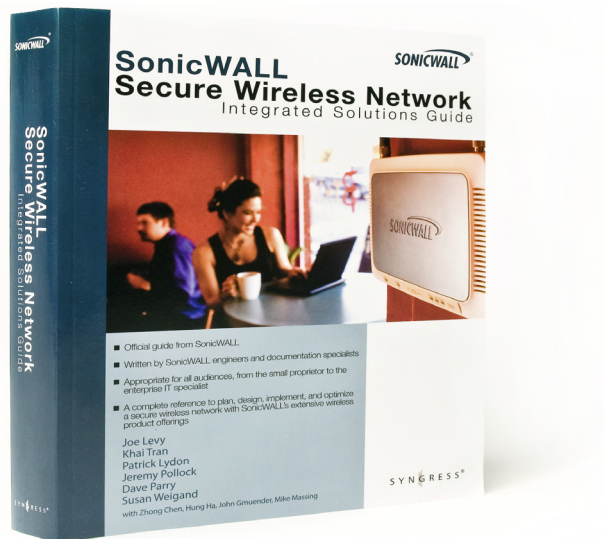
SonicWALL instructor-led classroom training is designed to build upon the knowledge and concepts put forth in the Technical eTraining courses. SonicWALL instructor-led classroom training is offered through SonicWALL Authorized Training Partners. If you are interested in attending SonicWALL instructor-led training, please contact a SonicWALL Authorized Training Partner. [more info »](#)

AUTHORIZED TRAINING PARTNERS »

SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. [more info »](#)

SonicWALL Secure Wireless Network Integrated Solutions Guide

The Official Guide to SonicWALL's market-leading wireless networking and security devices. This book is available in hardcopy by ordering directly from Elsevier Publishing at: <http://www.elsevier.com>



In this Section:

This chapter provides regulatory, trademark, and copyright information.

- *Mounting the SonicWALL ESA 4300* - page 26
 - *Weitere Hinweise zur Montage* - page 26
- *Safety and Regulatory Information* - page 27
 - *Cable Connections* - page 30
- *Copyright Notice* - page 30
- *Trademarks* - page 30

Mounting the SonicWALL ESA 4300

When mounting your SonicWALL ESA 4300:

- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application.
- Four mounting screws, compatible with the rack design, must be used and hand tightened to ensure secure installation. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch, rack mount cabinet.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers.
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.4mm) clearance is recommended.
- If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum recommended ambient temperature shown above.
- Mount the SonicWALL appliances evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- Reliable grounding of rack-mounted equipment must be maintained. Particular attention must be given to power supply connections other than direct connections to the branch circuits, such as power strips.

Weitere Hinweise zur Montage

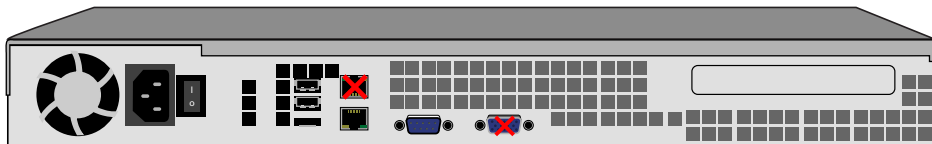
- Vergewissern Sie sich, dass das Rack für dieses Gerät geeignet ist und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an. Wählen Sie einen Ort im 19-Zoll-Rack, wo alle vier Befestigungen der Montageschienen verwendet werden.
- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Achten Sie darauf, dass sich die Netzkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- Das beigefügte Netzkabel ist nur für den Gebrauch in Nordamerika vorgesehen. Für Kunden in der Europäischen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Wenn das Gerät in einem geschlossenen 19"-Gehäuse oder mit mehreren anderen Geräten eingesetzt ist, wird die Temperatur in der Gehäuse höher sein als die Umgebungstemperatur. Achten Sie darauf, daß die Umgebungstemperatur nicht mehr als 40° C beträgt.
- Bringen Sie die SonicWALL waagrecht im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.
- Eine sichere Erdung der Geräte im Rack muss gewährleistet sein. Insbesondere muss auf nicht direkte Anschlüsse an Stromquellen geachtet werden wie z. B. bei Verwendung von Mehrfachsteckdosen.

Safety and Regulatory Information

Regulatory Model/Type	Product Name
1RK24-07D	SonicWALL ESA 4300

Unauthorized Ports

Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative; doing so may void your warranty.



FCC Part 15 Class A Notice

This equipment was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. And if not installed and used in accordance with the instruction manual, the device may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.



Note: *Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment.*

BMSI Statement

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI- A

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A conforme à la norme NMB-003 du Canada.


CISPR 22 (EN 55022) Class A

Complies with EN 55022 Class A and CISPR22 Class A. This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Declaration of Conformity

Application of council Directive	2004/108/EC (EMC) and 2006/95/EC (LVD)
Standards to which conformity is declared	EN 55022 (2006) Class A EN 55024 (1998) +A1 (2001), +A2 (2003) EN 61000-3-2 (2006) EN 61000-3-3 (1995) + A1 (2001), +A2 (2005) EN 60950-1 2006+
	National Deviations: AR, AT, AU, BE, CA, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IL, IN, IT, JP, KE, KR, MY, NL, NO, PL, SE, SG, SI, SK, US

Regulatory Information for Korea

 방송통신위원회	Ministry of Information and Telecommunication Certification Number SWL-1RK24-07E (A)
--	---

All products with country code "" (blank) and "A" are made in the USA. All products with country code "B" are made in China. All products with country code "C" or "D" are made in Taiwan R.O.C.

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Lithium Battery Warning

The lithium battery used in the SonicWALL appliance may not be replaced by the user. The appliance must be returned to a SonicWALL authorized service center for battery replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the SonicWALL is located.

Regulatory and Safety Instructions in German

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance von SonicWALL verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die SonicWALL in ein von SonicWALL autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der SonicWALL Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWALL keine Kabel an, die aus dem Gebäude in dem sich das Gerät befindet, herausgeführt werden.

Copyright Notice

© 2010 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format. Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc. Microsoft Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2000, Windows Server 2003, Windows Server 2008, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

SonicWALL, Inc.

2001 Logic Drive
San Jose CA 95124-3452

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

P/N 232-001700-50
Rev A 06/10



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.

Download from www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>