SonicWALL Network Security Appliances

NETWORK SECURITY

TZ 100 / TZ 200 Series

Getting Started Guide

SONICWALL®

SonicWALL TZ 100/200 series Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL TZ 100/200 series appliance running SonicOS Enhanced.

Document Contents

This document contains the following sections:

Setting Up Your Network 1

In this Section:

This section provides pre-configuration information. Review this section before setting up your SonicWALL TZ 100/200 series appliance.

System Requirements

Before you begin the setup process, verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

	Supported Browsers	Browser Version Number
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

Recording Configuration Information

Record the following setup information to use during the setup process and for future reference:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your SonicWALL appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your SonicWALL appliance.

Networking Information

LAN IP Address: ______.______.______.______	Select a static IP address for your SonicWALL appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: ______.______.______.______	Record the subnet mask for the local subnet where you are installing your SonicWALL appliance.
Ethernet WAN IP Address: ______.______.______.______	Select a static IP address for your Ethernet WAN. *This setting only applies if you are already using an ISP that assigns a static IP address.*

Administrator Information

Admin Name:	Select an administrator account name. (default is *admin)*
Admin Password:	Select an administrator password. (default is *password*)

Primary Internet Service Provider (ISP) Information

Record the following information about your current ISP:

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	*No Internet connection information is usually required*, although some service providers require a host name. Host Name: ______________________
Home DSL	PPPoE	User Name: ______________________ Password: ______________________ *Note: Your ISP may require your user name in the format: name@ISP.com*
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway (IP Address): _____._____._____._____ Primary DNS: _____._____._____._____ Secondary DNS (optional): _____._____._____._____
Dial-in to a server	PPTP	Server Address: ______________________ User Name: ______________________ Password: ______________________

Secondary ISP Information

If applicable, record the following information about your secondary ISP or WWAN service provider:

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	Host Name: ______________________
Home DSL	PPPoE	User Name: ______________________ Password: ______________________
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway (IP Address): _____._____._____._____ Primary DNS: _____._____._____._____ Secondary DNS (optional): _____._____._____._____
Dial-in to a server	PPTP	Server Address: ______________________ User Name: ______________________ Password: ______________________

Completing the Setup Wizard

The Setup Wizard takes you through several basic steps to get your SonicWALL TZ 100/200 series appliance configured for your network. **Use the *Recording Configuration Information*** section, on page 2 **to record your configuration information as you complete the wizard.**

Note: *If you are having trouble accessing the Setup Wizard, see the Troubleshooting the Setup Wizard section, on page 7 of this document.*

The Setup Wizard guides you through the following steps:

Change Password—Create a new password so that only you have access to the management interface. The default password is “password.”

Change Time Zone—Select the correct time zone for proper updates and time-based functionality.

WAN Network Mode—Choose your method of connecting to the Internet. This information is provided by your Internet Service Provider (ISP).

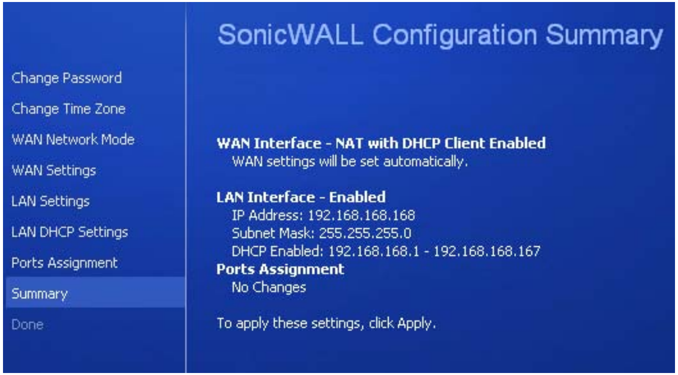
WAN Settings—Required for some WAN modes. This information is also provided by your ISP.

LAN Settings—Enter custom local network address settings, or use the default values, which work well for most networks.

LAN DHCP Settings—Allow your SonicWALL TZ 100/200 series appliance to automatically connect other local computers by specifying a DHCP range, or use the default.

Ports Assignment—Configure the extra interfaces (X2-X5) for different network requirements.

At the end of the wizard, a configuration summary displays. It is recommended that you record this information in the *Recording Configuration Information* section, on page 2 of this guide.



SonicWALL Configuration Summary

WAN Interface - NAT with DHCP Client Enabled
WAN settings will be set automatically.

LAN Interface - Enabled
IP Address: 192.168.168.168
Subnet Mask: 255.255.255.0
DHCP Enabled: 192.168.168.1 - 192.168.168.167
Ports Assignment
No Changes

To apply these settings, click Apply.

After the Setup Wizard completes, the appliance may reboot. Please wait a few minutes while the SonicWALL appliance reboots to save the updated firmware settings, and then continue with the next section of this guide.

Accessing the Management Interface

The computer you use to manage the SonicWALL TZ 100/200 series appliance must be set up to connect using DHCP, or with a static IP address in your chosen subnet. The default subnet for LAN zone ports is 192.168.168.x.

If your SonicWALL TZ 100/200 series appliance required a reboot after completing the Setup Wizard, wait until the 🔧 LED is no longer lit before continuing.

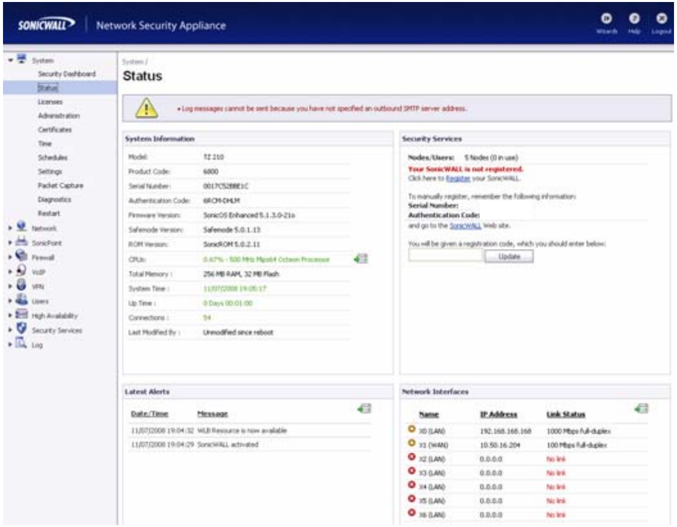
To access the SonicOS Web-based management interface:

1. Enter the default IP address of **http://192.168.168.168**, or the LAN IP address you chose during the Setup Wizard, in the **Location** or **Address** field of your Web browser.

Tip: *If you changed the LAN IP of your SonicWALL during the Setup Wizard, you may need to* ***restart your computer*** *for changes to take effect.*

2. When the SonicWALL Management Login page displays, enter your **username** and **password** (default values are “admin” for user name and “password” for password).

If the **System > Status** page (shown below) displays, then you have correctly configured the SonicWALL TZ 100/200 series appliance to work with the computer on your LAN.



Status

• Log messages cannot be sent because you have not specified an outbound SMTP server address.

System Information

Model:	TZ 210
Product Code:	6800
Serial Number:	0017C52BBE1C
Authentication Code:	6RCM-DHLM
Firmware Version:	SonicOS Enhanced 5.1.3.0-21o
Safemode Version:	Safemode 5.0.1.13
ROM Version:	SonicROM 5.0.2.11
CPUs:	0.67% - 500 MHz Mips64 Octeon Processor
Total Memory :	256 MB RAM, 32 MB Flash
System Time :	11/07/2008 19:05:17
Up Time :	0 Days 00:01:00
Connections :	54
Last Modified By :	Unmodified since reboot

Security Services

Nodes/Users: 5 Nodes (0 in use)

Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number:
Authentication Code:
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

Update

Latest Alerts

Date/Time	Message
11/07/2008 19:04:32	WLB Resource is now available
11/07/2008 19:04:29	SonicWALL activated

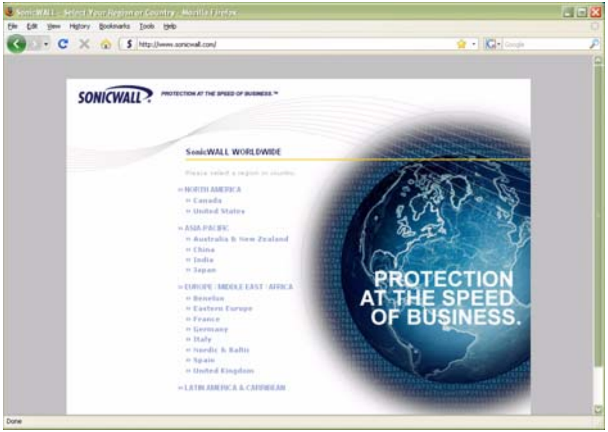
Network Interfaces

Name	IP Address	Link Status
X0 (LAN)	192.168.168.168	1000 Mbps full-duplex
X1 (WAN)	10.50.16.204	100 Mbps full-duplex
X2 (LAN)	0.0.0.0	No link
X3 (LAN)	0.0.0.0	No link
X4 (LAN)	0.0.0.0	No link
X5 (LAN)	0.0.0.0	No link
X6 (LAN)	0.0.0.0	No link

Verifying WAN (Internet) Connectivity

Complete the following steps to confirm your Internet connectivity:

1. In the Windows interface, launch your Web browser.
2. Enter “http://www.sonicwall.com” in the address bar and press **Enter** on the keyboard. The SonicWALL website displays. If you are unable to browse to a Website, see “Troubleshooting Internet Connection” on page 7.


SonicWALL - Select Your Region or Country - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Google
SONICWALL
PROTECTION AT THE SPEED OF BUSINESS.™
PROTECTION AT THE SPEED OF BUSINESS.
Done

http://www.sonicwall.com/

SonicWALL WORLDWIDE

Please select a region or country.

» NORTH AMERICA
» Canada
» United States

» ASIA PACIFIC
» Australia & New Zealand
» China
» India
» Japan

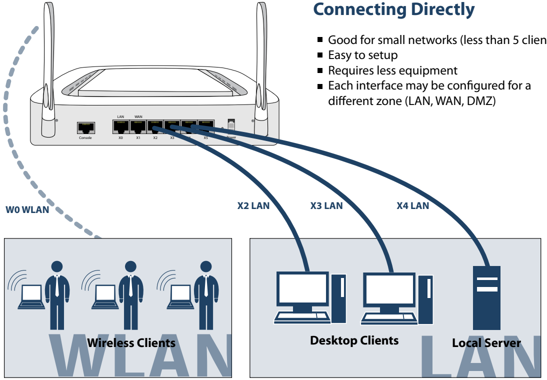
» EUROPE / MIDDLE EAST / AFRICA
» Benelux
» Eastern Europe
» France
» Germany
» Italy
» Nordic & Baltic
» Spain
» United Kingdom

» LATIN AMERICA & CARIBBEAN

Connecting Your Network Devices

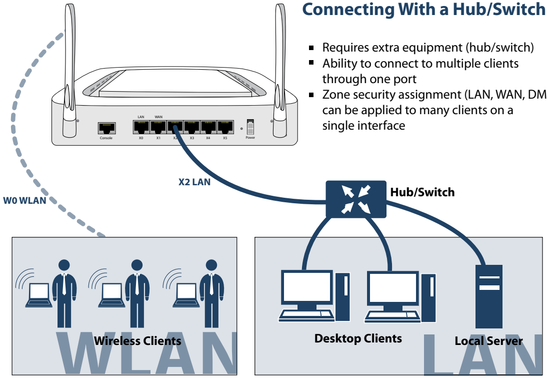
Connecting Directly

- Good for small networks (less than 5 clients)
- Easy to setup
- Requires less equipment
- Each interface may be configured for a different zone (LAN, WAN, DMZ)



Connecting With a Hub/Switch

- Requires extra equipment (hub/switch)
- Ability to connect to multiple clients through one port
- Zone security assignment (LAN, WAN, DMZ) can be applied to many clients on a single interface



Troubleshooting Initial Setup

This section provides troubleshooting tips for the following initial setup topics:

- Troubleshooting the Setup Wizard - page 7
- Troubleshooting Internet Connection - page 7
- Configuring DHCP IP Addressing - page 8

Troubleshooting the Setup Wizard

- **If you see the login screen, but not the Setup Wizard:**
  - Configure your Web browser to allow pop-ups.
  - Log into the security appliance using “**admin**” as the user name and “**password**” as the password. After you log in, click the **Wizards** button at the top right.

- **If you do not see the login screen or the Setup Wizard, verify the following:**
  - Did you correctly enter the SonicWALL TZ 210 series appliance management IP address, *192.168.168.168*, in your Web browser?
  - Is your computer set to accept DHCP addressing or set to a static IP address within the 192.168.168.x subnet range? If not, see the *Configuring DHCP IP Addressing* section, on page 8 for instructions.
  - Is the Ethernet cable connected between your computer and the LAN (X0) port on your SonicWALL?
  - Do you need to add the SonicWALL appliance to your list of trusted sites in your Web browser? Use the default IP address (192.168.168.168) for this.
  - Is the Test LED on the front panel of your SonicWALL appliance lit? If the Test LED stays lit for more than a few minutes after the initial power on sequence, power cycle the SonicWALL appliance.

Troubleshooting Internet Connection

If you can view the SonicWALL home page, you have configured your SonicWALL TZ 100/200 series appliance correctly. If you cannot view the SonicWALL home page, try the following:

- **Renew your management station DHCP address** if you changed the IP address/subnet of your network during setup.
- **Restart your management station** to accept new network settings from the DHCP server in the SonicWALL appliance.
- **Restart your Internet router or modem** to communicate with the DHCP client in the SonicWALL appliance.
- **Log into the SonicOS management interface** and launch the Setup Wizard again by clicking the Wizards button in the top right corner of the interface. Ensure that all of your settings are correct.

Configuring DHCP IP Addressing

If you are having trouble connecting to the SonicWALL TZ 100/200 series appliance, complete the following section based on your Windows operating system flavor. Configure your management computer to obtain an IP address using DHCP.

Windows Vista

1. From the **Start** menu, right-click **Network** and select **Properties**.
2. In the **Tasks** menu, click **Manage network connections**. The Network Connections windows 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 **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
6. Click **OK**, and then click **OK** again for the settings to take effect.

Windows XP

1. From the **Start** menu, highlight **Connect To** and then select **Show All Connections.**
2. Right-click on your **Local Area Connection** and select **Properties**.
3. In the list, double-click **Internet Protocol (TCP/IP)**.
4. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
5. Click **OK**, and then click **OK** again for the settings to take effect.

Windows 2000

1. From the Windows **Start** menu, select **Settings**.
2. Open **Network and Dial-up Connections**.
3. Click **Properties**.
4. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
6. Click **OK** for the settings to take effect.

Registering Your Appliance 2

In this Section:

This section provides instructions for registering your SonicWALL TZ 100/200 series appliance.

- Creating a MySonicWALL Account - page 10
- Registering and Licensing Your Appliance on MySonicWALL - page 10

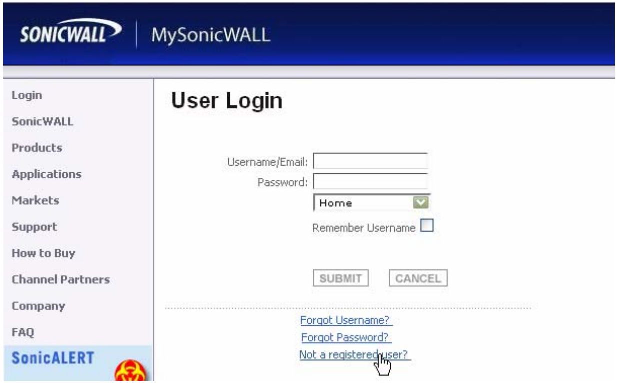
Note: *Registration is an important part of the setup process and is necessary to receive the benefits of SonicWALL security services, firmware updates, and technical support.*

Creating a MySonicWALL Account

A MySonicWALL account is required for product registration. If you already have an account, continue to the *Registering and Licensing Your Appliance on MySonicWALL* section.

Perform the following steps to create a MySonicWALL account:

1. In your browser, navigate to www.mysonicwall.com.
2. In the login screen, click the **Not a registered user?** link.



3. Complete the Registration form and click **Register**.
4. Verify that the information is correct and click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

Registering and Licensing Your Appliance on MySonicWALL

This section contains the following subsections:

- Product Registration - page 10
- Security Services and Software - page 11
- Activating Security Services and Software - page 12
- Trying or Purchasing Security Services - page 12

Product Registration

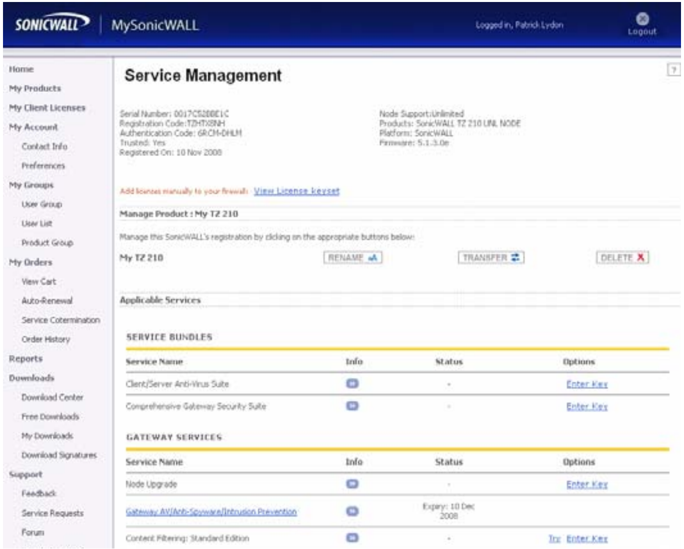
You must register your SonicWALL security appliance on MySonicWALL to enable full functionality.

1. Login to your MySonicWALL account. If you do not have an account, you can create one at www.mysonicwall.com.
2. On the main page, type the appliance serial number in the **Register A Product** field. Then click **Next**.
3. On the My Products page, under **Add New Product**, type the friendly name for the appliance, select the **Product Group** if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.

Security Services and Software

The Service Management - Associated Products page in MySonicWALL lists security services, support options, and software, such as ViewPoint, that you can purchase or try with a free trial. For details, click the **Info** button.

If you purchased an appliance that is pre-licensed, you may be required to enter your activation key here unless current licenses are already indicated in the **Status** column with either a license key or an expiration date.



Service Management

Serial Number: 0017C52DDE1C
Registration Code:TZHTX8NH
Authentication Code: 6RCM-DHLM
Trusted: Yes
Registered On: 10 Nov 2008

Node Support:Unlimited
Products: SonicWALL TZ 210 UNL NODE
Platform: SonicWALL
Firmware: 5.1.3.0e

Add licenses manually to your firewall: View License keyset

Manage Product : My TZ 210

Manage this SonicWALL's registration by clicking on the appropriate buttons below:

My TZ 210

Applicable Services

SERVICE BUNDLES

Service Name	Info	Status	Options
Client/Server Anti-Virus Suite	●	-	Enter Key
Comprehensive Gateway Security Suite	●	-	Enter Key

GATEWAY SERVICES

Service Name	Info	Status	Options
Node Upgrade	●	-	Enter Key
Gateway AV/Anti-Spyware/Intrusion Prevention	●	Expiry: 10 Dec 2008	
Content Filtering: Standard Edition	●	-	Try Enter Key

The following products and services are available for the SonicWALL TZ 100/200 series appliances:

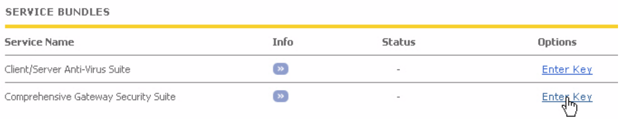
- **Gateway Service Bundles:**
  - Client/Server Anti-Virus Suite
  - Comprehensive Gateway Security Suite
- **Individual Gateway Services:**
  - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention
  - Global Management System
  - Content Filtering: Premium Edition
  - High Availability Upgrade
- **Desktop and Server Software:**
  - Enforced Client Anti-Virus and Anti-Spyware
  - Global VPN Client
  - Global VPN Client Enterprise
  - ViewPoint
- **Support Services:**
  - Dynamic Support 8x5
  - Dynamic Support 24x7
  - Software and Firmware Updates

Activating Security Services and Software

If you purchase a service subscription or upgrade from a sales representative, you will receive an activation key. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase.

To activate existing licenses, perform the following tasks:

1. Navigate to the **My Products** page and select the registered product you want to manage.
2. Locate the product on the Service Management page and click **Enter Key** in that row.

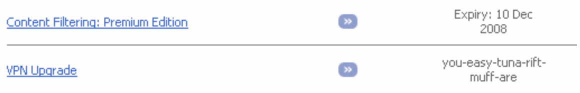


SERVICE BUNDLES

Service Name	Info	Status	Options
Client/Server Anti-Virus Suite	»	-	Enter Key
Comprehensive Gateway Security Suite	»	-	Enter Key

3. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**.

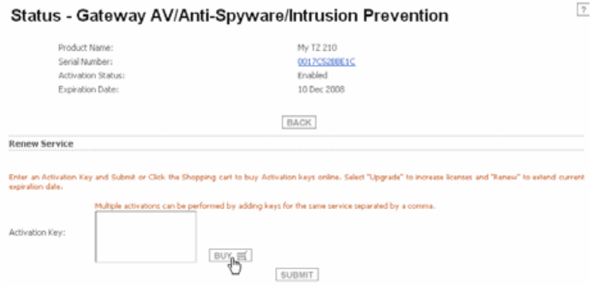
   Once the service is activated, you will see an expiration date or a license key string in the **Status** column on the Service Management page.



Content Filtering: Premium Edition	»	Expiry: 10 Dec 2008
VPN Upgrade	»	you-easy-tuna-rift-muff-are

Trying or Purchasing Security Services

To try a Free Trial of a service, click **Try** in the Service Management page. **To purchase a product or service**, click **Buy Now** in the Service Management page.



Status - Gateway AV/Anti-Spyware/Intrusion Prevention

Product Name:	My TZ 210
Serial Number:	0017C5280E1C
Activation Status:	Enabled
Expiration Date:	10 Dec 2008

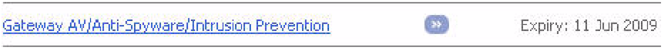
Renew Service

Enter an Activation Key and Submit or Click the Shopping cart to buy Activation keys online. Select "Upgrade" to increase licenses and "Renew" to extend current expiration date.

Multiple activations can be performed by adding keys for the same service separated by a comma.

Activation Key:

When activation is complete, MySonicWALL displays an activation screen with service status and expiration information. The service management screen also displays the product you licensed.



Gateway AV/Anti-Spyware/Intrusion Prevention	»	Expiry: 11 Jun 2009

You have successfully registered your SonicWALL appliance. And now you need to enable Unified Threat Management (UTM) security services. SonicWALL UTM security services are not enabled by default.

Enabling Security Services 3

In this Section:

Security services are an essential component of a secure network deployment. This section provides instructions for registering and enabling security services on your SonicWALL TZ 100/200 series appliance.

Enabling Security Services in SonicOS

After completing the registration process in SonicOS, perform the tasks listed below to activate your licenses and enable your licensed services from within the SonicOS user interface.

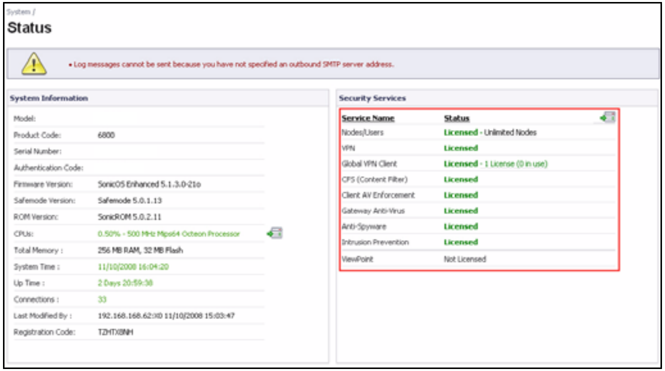
SonicWALL security services are key components of threat management in SonicOS. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

You must enable each security service individually in the SonicOS user interface. See the following procedures to enable and configure your security services:

- Verifying Licenses - page 14
- Enabling Gateway Anti-Virus - page 15
- Enabling Intrusion Prevention Services - page 16
- Enabling Anti-Spyware - page 17
- Enabling Content Filtering Service - page 18

Verifying Licenses

Verify that your security services are licensed on the **System** > **Status** page.



System /

Status

• Log messages cannot be sent because you have not specified an outbound SMTP server address.

System Information

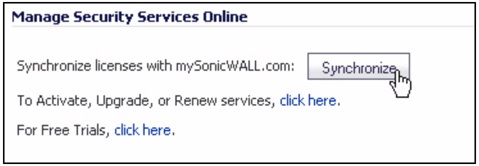
Model:	
Product Code:	6800
Serial Number:	
Authentication Code:	
Firmware Version:	SonicOS Enhanced 5.1.3.0-21o
Safemode Version:	Safemode 5.0.1.13
ROM Version:	SonicROM 5.0.2.11
CPUs:	0.50% - 500 MHz Mips64 Octeon Processor
Total Memory :	256 MB RAM, 32 MB Flash
System Time :	11/10/2008 16:04:20
Up Time :	2 Days 20:59:38
Connections :	33
Last Modified By :	192.168.168.62:X0 11/10/2008 15:03:47
Registration Code:	TZHTX8NH

Security Services

Service Name	Status
Nodes/Users	Licensed - Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 1 License (0 in use)
CFS (Content Filter)	Licensed
Client AV Enforcement	Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
ViewPoint	Not Licensed

If services that are already activated on MySonicWALL do not display as licensed, you need to synchronize your SonicWALL with the licensing server.

If initial setup is already complete, click the **Synchronize** button to synchronize licenses from the **System** > **Licenses** page.



Manage Security Services Online

Synchronize licenses with mySonicWALL.com: Synchronize

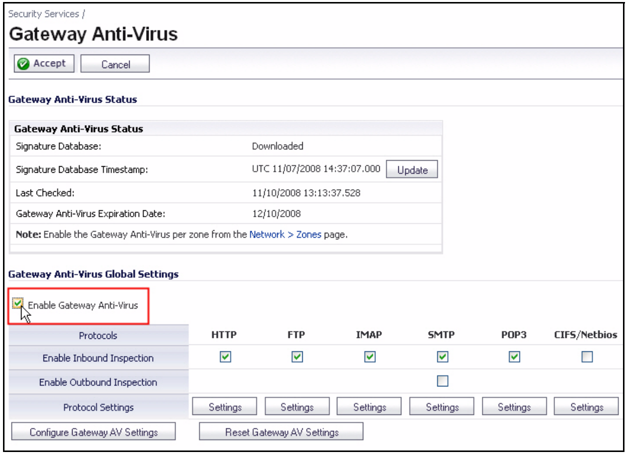
To Activate, Upgrade, or Renew services, click here.

For Free Trials, click here.

Enabling Gateway Anti-Virus

To enable Gateway Anti-Virus (GAV) in SonicOS:

1. Navigate to the **Security Services** > **Gateway Anti-Virus** page.
2. Select the **Enable Gateway Anti-Virus** checkbox and click **Accept** to apply changes.



Security Services /

Gateway Anti-Virus

Accept | Cancel

Gateway Anti-Virus Status

Gateway Anti-Virus Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 11/07/2008 14:37:07.000 Update
Last Checked:	11/10/2008 13:13:37.528
Gateway Anti-Virus Expiration Date:	12/10/2008

Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page.

Gateway Anti-Virus Global Settings

☑ Enable Gateway Anti-Virus

Protocols	HTTP	FTP	IMAP	SMTP	POP3	CIFS/Netbios
Enable Inbound Inspection	☑	☑	☑	☑	☑	□
Enable Outbound Inspection				□		
Protocol Settings	Settings	Settings	Settings	Settings	Settings	Settings

Configure Gateway AV Settings | Reset Gateway AV Settings

3. Verify that the **Enable Inbound Inspection** checkboxes are selected for the protocols you wish to inspect. See the following table for an explanation of these protocols.

The following table gives descriptions and default values for GAV-enforced protocols:

Protocol	**Default**	**Description**
HTTP	Enabled	Hyper-Text Transfer Protocol, common Web-browsing traffic
FTP	Enabled	File Transfer Protocol, dedicated file download servers
IMAP	Enabled	Internet Message Access Protocol, standard method for accessing email
SMTP	Enabled	Simple Mail Transfer Protocol, standard method for accessing email
POP3	Enabled	Post Office Protocol 3, standard method for accessing email
CIFS/ Netbios	Disabled	Intra-network traffic on Windows operating system (network file-sharing)
TCP Stream	Disabled	Any other non-standard type of network data transfer

4. Click the **Accept** ✓ Accept button to apply changes.

GAV contains many other useful features, including:

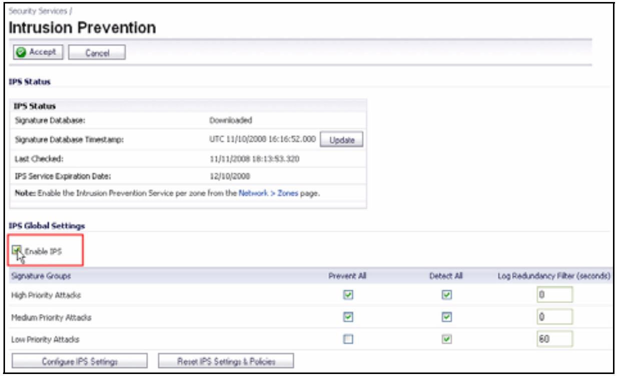
- **Outbound SMTP Inspection** scans outbound email
- **User Notification** notifies users when content is blocked
- **File-Type Restrictions** blocks various non-scannable files
- **Exclusion Lists** for network nodes where Gateway Anti-Virus enforcement is not necessary.

Tip: *For a complete overview of GAV features, refer to the SonicOS Enhanced Administrator's Guide.*

Enabling Intrusion Prevention Services

To enable Intrusion Prevention (IPS) in SonicOS:

1. Navigate to the **Security Services** > **Intrusion Prevention** page.
2. Select the **Enable Intrusion Prevention** checkbox.



Security Services /

Intrusion Prevention

IPS Status

IPS Status		
Signature Database:	Downloaded	
Signature Database Timestamp:	UTC 11/10/2008 16:16:52.000	Update
Last Checked:	11/11/2008 18:13:53.320	
IPS Service Expiration Date:	12/10/2008	

Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page.

IPS Global Settings

☑ Enable IPS

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Priority Attacks	☑	☑	0
Medium Priority Attacks	☑	☑	0
Low Priority Attacks	☐	☑	60

3. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes based on attack priority.

Note: ***Prevent All*** *blocks attacks of the chosen priority, and* ***Detect All*** *saves a log of these attacks that can be viewed on the* ***Log*** *>* ***View*** *page. A common setting is to enable* ***Prevent*** *for High and Medium Priority threats, and* ***Detect*** *for all threats.*

4. Click the **Accept** Accept button to apply changes.

Intrusion Prevention contains other useful features, including:

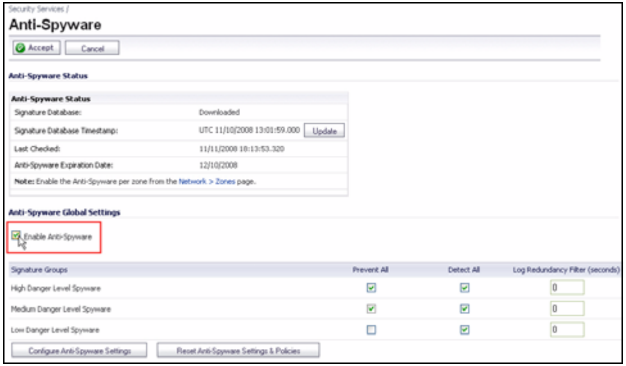
- **Exclusion Lists** for network nodes where IPS enforcement is not necessary.
- **Log Redundancy** to control log size during high-volume intrusion attack attempts by enforcing a delay between log entries.

Tip: *For a complete overview of IPS features, refer to the SonicOS Enhanced Administrator’s Guide.*

Enabling Anti-Spyware

To enable Anti-Spyware in SonicOS:

1. Navigate to the **Security Services** > **Anti-Spyware** page.
2. Select the **Enable Anti-Spyware** checkbox.


Security Services /
Accept
Cancel
Update
Configure Anti-Spyware Settings
Reset Anti-Spyware Settings & Policies

Anti-Spyware

Anti-Spyware Status

Anti-Spyware Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 11/10/2008 13:01:59.000
Last Checked:	11/11/2008 18:13:53.320
Anti-Spyware Expiration Date:	12/10/2008

Note: Enable the Anti-Spyware per zone from the Network > Zones page.

Anti-Spyware Global Settings

☑ Enable Anti-Spyware

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Danger Level Spyware	☑	☑	0
Medium Danger Level Spyware	☑	☑	0
Low Danger Level Spyware	☐	☑	0

3. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each spyware danger level that you want to prevent.

Note: *Prevent all blocks attacks of the chosen priority, Detect All saves a log of these attacks which can be viewed in the **Log** > **View** screen.*

4. Click the **Accept** Accept button to apply changes.

Anti-Spyware contains other useful features, including:

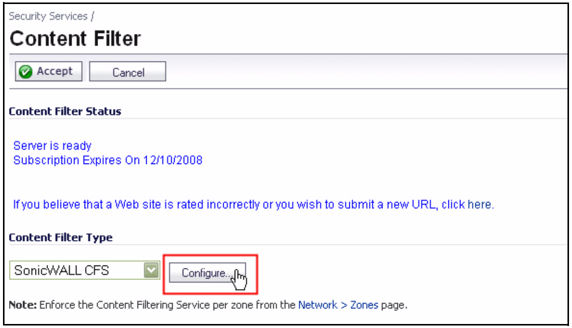
- **Exclusion Lists** excludes network nodes when Anti-Spyware enforcement is not necessary.
- **Log Redundancy** controls log size during high-volume intrusion attack attempts by enforcing a delay between log entries.
- **Clientless Notification** displays messages to users when content is blocked by SonicWALL Anti-Spyware.
- **Outbound Inspection** enables scanning and logging of outbound spyware communication attempts.
- **Disable SMTP Responses** suppresses the sending of email messages to clients when spyware is detected.

Tip: *For a complete overview of Anti-Spyware features, refer to the SonicOS Enhanced Administrator’s Guide.*

Enabling Content Filtering Service

To enable Content Filtering Service (CFS) in SonicOS:

1. Navigate to the **Security Services** > **Content Filter** page.
2. Select **SonicWALL CFS** in the Content Filter Type drop-down list and then click the **Configure** button.



Security Services /

Content Filter

Content Filter Status

Server is ready
Subscription Expires On 12/10/2008

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

Content Filter Type

SonicWALL CFS

Note: Enforce the Content Filtering Service per zone from the Network > Zones page.

3. In the **Policy** tab, click the **Configure** button for the default policy. The Edit CFS Policy windows displays.
4. In the **URL List** tab, review and select additional exclusion categories as needed.
5. Click **OK** to both pop-up windows.
6. Click the **Accept** ✓ Accept button to apply changes.

Content FIltering Service contains other useful features, including:

- **URL Rating Review** allows the administrator and users to review blocked URL ratings if they think a URL is rated incorrectly.
- **Restrict Web Features** restricts features such as cookies, Java, ActiveX, and HTTP Proxy access.
- **Trusted Domains** allows access to restricted features on trusted domains.
- **CFS Exclusion List** excludes administrators and/or IP ranges from content filtering enforcement.
- **Blocked Content Web Page** displays a custom HTML page to users when content is blocked.

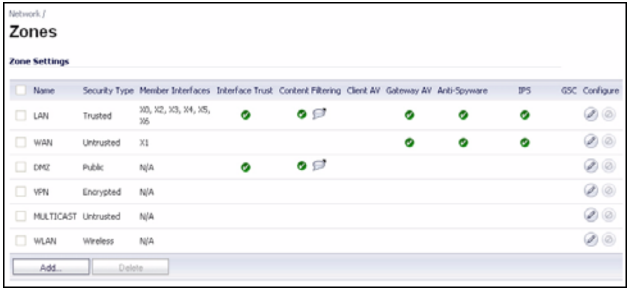
Tip: *For a complete overview of CFS features, refer to the SonicOS Enhanced Administrator's Guide.*

Verifying Security Services on Zones

Security services such as Gateway Anti-Virus are automatically applied to the LAN and WAN network zones. To protect other zones such as the DMZ or Wireless LAN (WLAN), you must apply the security services to the network zones. For example, you can configure SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic.

To apply services to network zones:

1. Navigate to the **Network** > **Zones** page.



Network /

Zones

Zone Settings

□	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
□	LAN	Trusted	X0, X2, X3, X4, X5, X6	✓	✓		✓	✓	✓		
□	WAN	Untrusted	X1				✓	✓	✓		
□	DMZ	Public	N/A	✓	✓						
□	VPN	Encrypted	N/A								
□	MULTICAST	Untrusted	N/A								
□	WLAN	Wireless	N/A								

2. In the Zone Settings table, click the **Configure** icon for the zone where you want to apply security services.
3. In the **Edit Zone** dialog box on the **General** tab, select the checkboxes for the security services to enable on this zone.
4. Click **OK**.

Congratulations! Your SonicWALL TZ 100/200 series appliance is registered and fully functional with active UTM security services enabled.

For advanced network setup information, continue to:

- Advanced Network Configuration - page 21
- Advanced Deployments - page 33

Advanced Network Configuration 4

In this Section:

This section provides detailed overviews of advanced deployment scenarios, as well as configuration instructions for connecting your SonicWALL TZ 100/200 series appliance to various network devices.

Tip: *Before completing this section, fill out the information in* Recording Configuration Information *- page 2.*

An Introduction to Zones and Interfaces

Zones split a network infrastructure into logical areas, each with its own set of usage rules, security services, and policies. Most networks include multiple definitions for zones, including those for trusted, untrusted, public, encrypted, and wireless traffic.

Some basic (default) zone types include:

WAN—Untrusted resources outside your local network.

LAN—Trusted local network resources.f

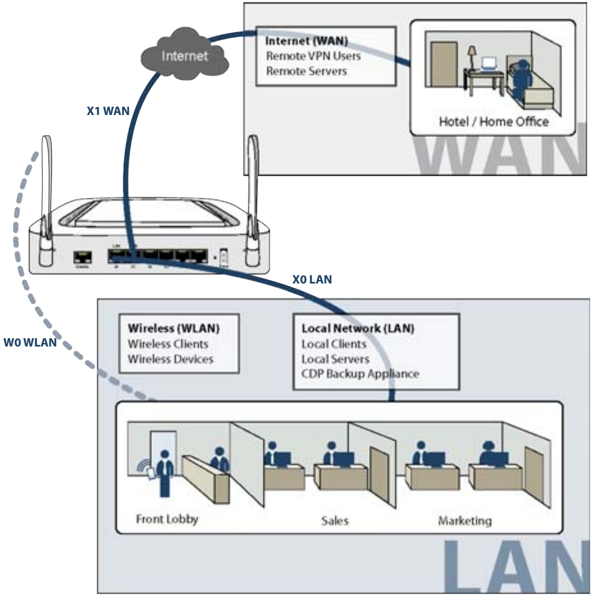
WLAN—Local wireless network resources originating from SonicWALL wireless enabled appliances.

DMZ—Local network assets that must be accessible from the WAN zone (such as Web and FTP servers).

VPN—Trusted endpoints in an otherwise untrusted zone, such as the WAN.

The security features and settings that zones carry are enforced by binding a zone to one or more physical interfaces (such as, X0, X1, or X2) on the SonicWALL TZ 100/200 series appliance.

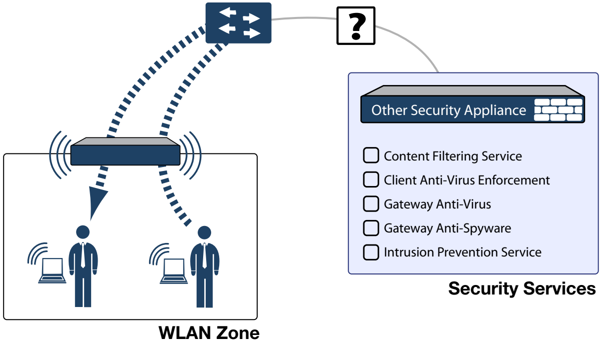
The X1 and X0 interfaces are preconfigured as WAN and LAN respectively. The remaining ports are also LAN ports by default, however, these ports can be configured to meet the needs of your network, either by using basic zone types (WAN, LAN, WLAN, DMZ, VPN) or configuring a custom zone type to fit your network requirements (Gaming Console Zone, Wireless Printer Zone, Wireless Ticket Scanner Zone, and more).



SonicWALL Wireless Firewalling

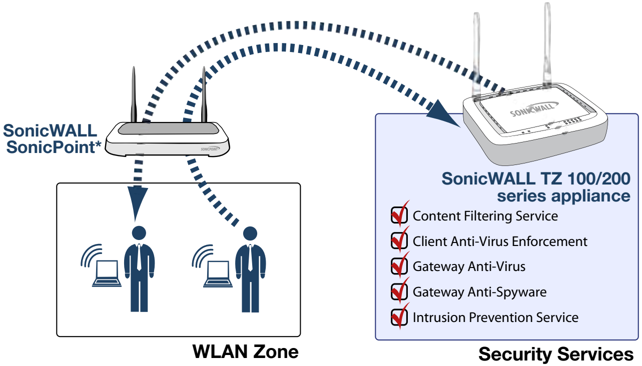
When a wireless device uses an access point to communicate with a device on another subnet or on a completely different network, traffic between the devices is forced to traverse the network gateway. This traversal enables Unified Threat Management (UTM) services to be enforced at the gateway.

Standard practice for wireless firewalling (where one wireless client is communicating with another) bypasses many of the critical UTM security services. The illustration below shows the standard practice for wireless firewalling.



Many security products on the market share this potential vulnerability when two users connected by a common hub or wireless access point wish to exchange data.

SonicWALL addresses this security shortcoming by managing the SonicPoint access points from the UTM appliance. This allows complete control of the wireless space, including zone enforcement of security services and complete firewalling capabilities, as shown in the illustration below.


SonicWALL SonicPoint*
SonicWALL TZ 100/200 series appliance
☑ Content Filtering Service
☑ Client Anti-Virus Enforcement
☑ Gateway Anti-Virus
☑ Gateway Anti-Spyware
☑ Intrusion Prevention Service
WLAN Zone
Security Services

*SonicPoint needed for wireless access on wired-only models

Configuring Interfaces

Interfaces, also known as ports, are physical network connections that can be configured to provide different networking and security features based on your network needs.

Note: *For more information on Zone types, see "An Introduction to Zones and Interfaces" on page 22.*

This section contains the following sub-sections:

- Configuring an Interface - page 24
- PortShield Wizard - page 25
- Manual PortShield Configuration - page 26

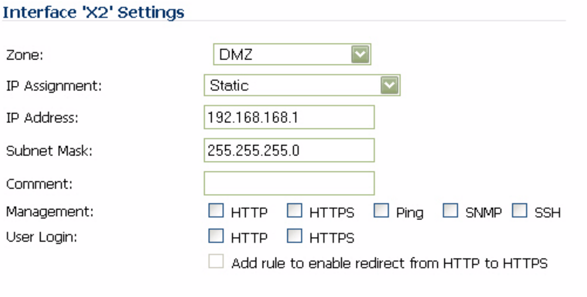
Configuring an Interface

The SonicOS Enhanced Web-based management interface allows you to configure each individual Ethernet port (from X2-X5) with its own security settings through the use of zones.

To configure a network interface:

1. In the **Network > Interfaces** panel, click the **Configure** button for the interface you wish to configure. The Edit Interface window displays.

Note: *If only X0 and X1 interfaces are displayed in the Interfaces list, click the **Show PortShield Interfaces** button to show all interfaces.*



Interface 'X2' Settings

Zone: DMZ

IP Assignment: Static

IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

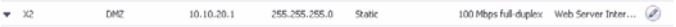
Comment:

Management: □ HTTP □ HTTPS □ Ping □ SNMP □ SSH

User Login: □ HTTP □ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

2. Select a **Zone Type** for this interface.
3. Select an **IP assignment** for this interface. If you intend to create a new network segment on this interface such as a DMZ or secondary LAN, this value should be set to **Static**.
4. Enter a static **IP Address** for the interface. For private and semi-private network segments, any private static IP address such as 10.10.20.1 is appropriate. Ensure that the static IP address you choose does not conflict with any currently existing interfaces. The newly created interface appears in the Interfaces list. You may now connect the appropriate network resources to this interface.



▾ X2	DMZ	10.10.20.1	255.255.255.0	Static	100 Mbps full-duplex	Web Server Inter...

PortShield Wizard

With PortShield, multiple ports can share the network settings of a single interface. The SonicWALL PortShield feature enables you to easily configure the ports on the SonicWALL TZ 100/200 series appliance into common deployments.

Tip: *Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.*

To configure ports using the SonicWALL PortShield Wizard:

1. Click the **Wizards** button on the top-right of the SonicOS management interface.
2. Choose **PortShield Interface Wizard** and click Next.
3. Select from the following:

Selection	Port Assignment	Usage
WAN/LAN	X1: WAN All Other Ports: LAN	Connect Internet connection to X1 Connect network devices to any remaining portfor local and Internet connectivity.
WAN/LAN/ DMZ	X1: WAN X2: DMZ All Other Ports: LAN	Connect Internet connection to X1. Connect public-facing servers or other semi-public resources to X2. Connect network devices to any remaining port for local and Internet connectivity.

4. WAN/LAN or WAN/LAN/DMZ and click **Next** to continue.This will prompt a configuration summary to appear. Verify that the ports assigned are correct.
5. Click **Apply** to change port assignments.

Note: *For more information about PortShield interfaces, see the SonicOS Enhanced Administrator's Guide.*

Creating Network Access Rules

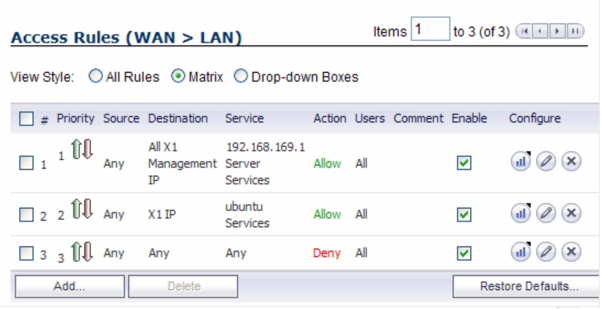
A Zone is a logical grouping of one or more interfaces designed to make management a simpler and more intuitive process than following a strict physical interface scheme.

By default, the SonicWALL security appliance’s stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN. The following behaviors are defined by the “Default” stateful inspection packet access rule enabled in the SonicWALL security appliance:

Originating Zone	**Destination Zone**	**Action**
LAN, WLAN	WAN, DMZ	Allow
DMZ	WAN	Allow
WAN	DMZ	Deny
WAN and DMZ	LAN or WLAN	Deny

To create an access rule:

1. On the **Firewall** > **Access Rules** page in the matrix view, select two zones that will be bridged by this new rule.
2. On the Access Rules page, click **Add**.



Access Rules (WAN > LAN)

Items 1 to 3 (of 3)

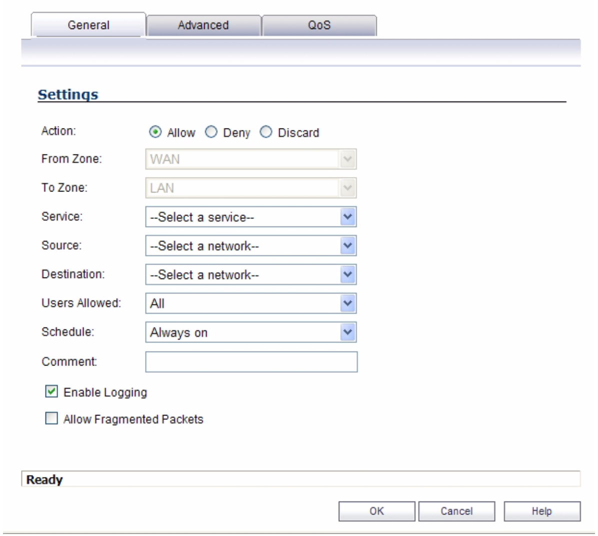
View Style: ○ All Rules ● Matrix ○ Drop-down Boxes

□	#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
□	1	1	Any	All X1 Management IP	192.168.169.1 Server Services	Allow	All		☑	
□	2	2	Any	X1 IP	ubuntu Services	Allow	All		☑	
□	3	3	Any	Any	Any	Deny	All		☑	

The access rules are sorted from the most specific to the least specific at the bottom of the table. At the bottom of the table is the **Any** rule.

Note: *SonicWALL’s default firewall rules are set in this way for ease of initial configuration, but do not reflect best practice installations. Firewall rules should only allow the required traffic and deny all other traffic.*

3. In the Add Rule page on the **General** tab, select **Allow** or **Deny** or **Discard** from the **Action** list to permit or block IP traffic.



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: WAN

To Zone: LAN

Service: --Select a service--

Source: --Select a network--

Destination: --Select a network--

Users Allowed: All

Schedule: Always on

Comment:

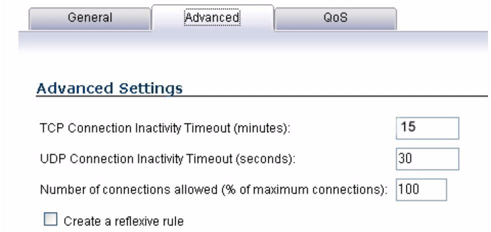
☑ Enable Logging

□ Allow Fragmented Packets

Ready

4. Configure the other settings on the **General** tab as explained below:
   - Select the service or group of services affected by the access rule from the **Service** drop-down list. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
   - Select the source of the traffic affected by the access rule from the **Source** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
   - Select the destination of the traffic affected by the access rule from the **Destination** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
   - Select a user or user group from the **Users Allowed** drop-down list.
   - Select a schedule from the **Schedule** drop-down list. The default schedule is **Always on**.
   - Enter any comments to help identify the access rule in the **Comments** field.

5. Click on the **Advanced** tab.



Advanced Settings

TCP Connection Inactivity Timeout (minutes): 15

UDP Connection Inactivity Timeout (seconds): 30

Number of connections allowed (% of maximum connections): 100

☐ Create a reflexive rule

6. Configure the other settings on the **Advanced** tab as explained below:
   - In the **TCP Connection Inactivity Timeout (minutes)** field, set the length of TCP inactivity after which the access rule will time out. The default value is **15** minutes.
   - In the **UDP Connection Inactivity Timeout (minutes)** field, set the length of UDP inactivity after which the access rule will time out. The default value is **30** minutes.
   - In the **Number of connections allowed (% of maximum connections)** field, specify the percentage of maximum connections that is allowed by this access rule. The default is 100%.
   - Select **Create a reflexive rule** to create a matching access rule for the opposite direction, that is, from your destination back to your source.
7. Click on the **QoS** tab to apply DSCP marking to traffic governed by this rule.
8. Click **OK** to add the rule.

Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. Once you define an Address Object, it becomes available for use wherever applicable throughout the SonicOS management interface. For example, consider an internal Web server with an IP address of 67.115.118.80.

Rather than repeatedly typing in the IP address when constructing Access Rules or NAT policies, you can create an Address Object to store the Web server’s IP address. This Address Object, “My Web Server,” can then be used in any configuration screen that employs Address Objects as a defining criterion.

Available Address Object types include the following:

- **Host –** Define a single host by its IP address.
- **Range –** Define a range of contiguous IP addresses.
- **Network –** Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask.
- **MAC Address –** Allows for the identification of a host by its hardware address.
- **FQDN Address –** Fully Qualified Domain Names (FQDN) Address Objects allow for the identification of a host by its domain name, such as www.sonicwall.com.

Tip: *SonicOS Enhanced provides a number of default Address Objects that cannot be modified or deleted. You can use the default Address Objects when creating a NAT policy, or you can create custom Address Objects to use. All Address Objects are available in the drop-down lists when creating a NAT policy.*

Creating and Managing Address Objects

The **Network** > **Address Objects** page allows you to create and manage your Address Objects. You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** – displays all configured Address Objects.
- **Custom Address Objects** – displays Address Objects with custom properties.
- **Default Address Objects** – displays Address Objects configured by default on the SonicWALL security appliance.

Network Address Translation

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to perform Many-to-One NAT between the systems on the LAN and the IP address of the WAN interface. The appliance does not perform NAT by default when traffic crosses between the other interfaces.

You can create multiple NAT policies on a SonicWALL running SonicOS Enhanced for the same object – for instance, you can specify that an internal server uses one IP address when accessing Telnet servers, and uses a different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to access multiple internal servers from the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

Before configuring NAT Policies, you must create all Address Objects that will be referenced by the policy. For instance, if you are creating a One-to-One NAT policy, first create Address Objects for your public and private IP addresses.

Configuring NAT Policies

NAT policies allow you to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. The following NAT configurations are available in SonicOS Enhanced:

- Many-to-One NAT Policy
- Many-to-Many NAT Policy
- One-to-One NAT Policy for Outbound Traffic
- One-to-One NAT Policy for Inbound Traffic (Reflexive)
- One-to-Many NAT Load Balancing
- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

This section describes how to configure a One-to-One NAT policy. One-to-One is the most common NAT policy used to route traffic to an internal server, such as a Web server. Most of the time, this means that incoming requests from external IP addresses are *translated* from the IP address of the SonicWALL security appliance WAN port to the IP address of the internal Web server. The following example configuration illustrates the use of the fields in the Add NAT Policy procedure. To add a One-to-One NAT policy that allows all Internet traffic to be routed through a public IP address, two policies are needed: one policy for the outbound traffic, and one policy for the inbound traffic.

To add the components of a One-to-One NAT policy, perform the following steps:

1. Navigate to the **Network > Address Objects** Page and choose the Custom radio button.
2. Click the **Add** button; define a network address object (example named '**webserver 10.33.4.101**' ; a LAN host object w/ IP address 10.33.4.101)
3. Navigate to the **Network > NAT Policies** page. Click Add. The Add NAT Policy dialog box displays.
4. For **Original Source**, select **Any**.
5. For **Translated Source**, select **Original**.
6. For **Original Destination**, select **WAN Primary IP**.
7. For **Translated Destination**, select '**webserver 10.33.4.101**'
8. For **Original Service**, select **HTTP**.
9. For **Translated Service**, select **Original**.
10. For **Inbound Interface**, select **X1**.
11. For **Outbound Interface**, select **Any**.
12. For **Comment**, enter a short description.
13. Select the **Enable NAT Policy** checkbox.
14. Select the **Create a reflexive policy** checkbox if you want a matching NAT policy to be automatically created in the opposite direction. This will create the outbound as well as the inbound NAT Policy.

For more information on creating NAT policies, refer to the *SonicOS Enhanced Administrator's Guide*.

Support and Training Options 5

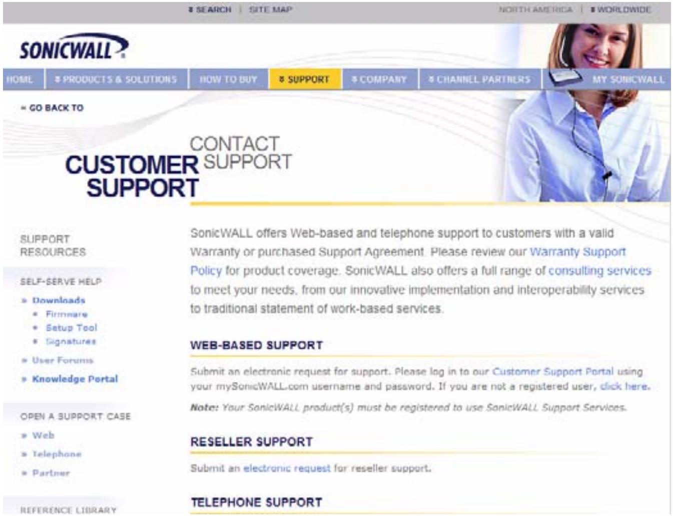
In this Section:

This section provides overviews of customer support and training options for the SonicWALL TZ 100/200 series appliances.

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>



CUSTOMER SUPPORT

SonicWALL offers Web-based and telephone support to customers with a valid Warranty or purchased Support Agreement. 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 and interoperability services to traditional statement of work-based services.

WEB-BASED SUPPORT

Submit an electronic request for support. Please log in to our Customer Support Portal using your mySonicWALL.com username and password. If you are not a registered user, click here.

Note: Your SonicWALL product(s) must be registered to use SonicWALL Support Services.

RESELLER SUPPORT

Submit an electronic request for reseller support.

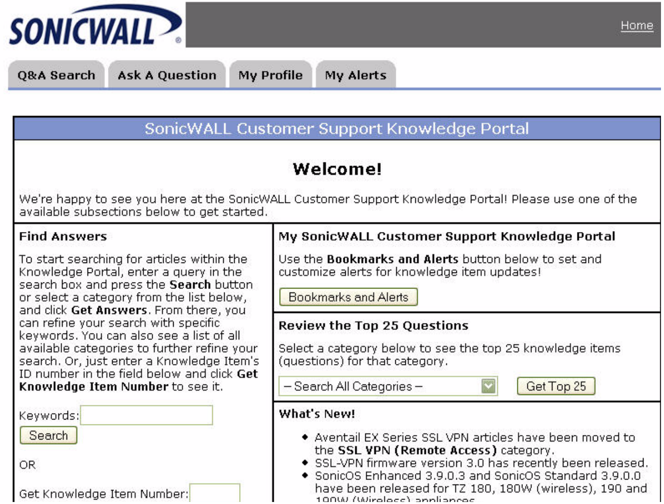
TELEPHONE SUPPORT

Knowledge Portal

The Knowledge Portal 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 Portal** page at:
<http://www.mysonicwall.com/>



SonicWALL Customer Support Knowledge Portal

Welcome!

We're happy to see you here at the SonicWALL Customer Support Knowledge Portal! Please use one of the available subsections below to get started.

Find Answers

To start searching for articles within the Knowledge Portal, enter a query in the search box and press the **Search** button or select a category from the list below, and click **Get Answers**. From there, you can refine your search with specific keywords. You can also see a list of all available categories to further refine your search. Or, just enter a Knowledge Item's ID number in the field below and click **Get Knowledge Item Number** to see it.

Keywords:

OR

Get Knowledge Item Number:

My SonicWALL Customer Support Knowledge Portal

Use the **Bookmarks and Alerts** button below to set and customize alerts for knowledge item updates!

Review the Top 25 Questions

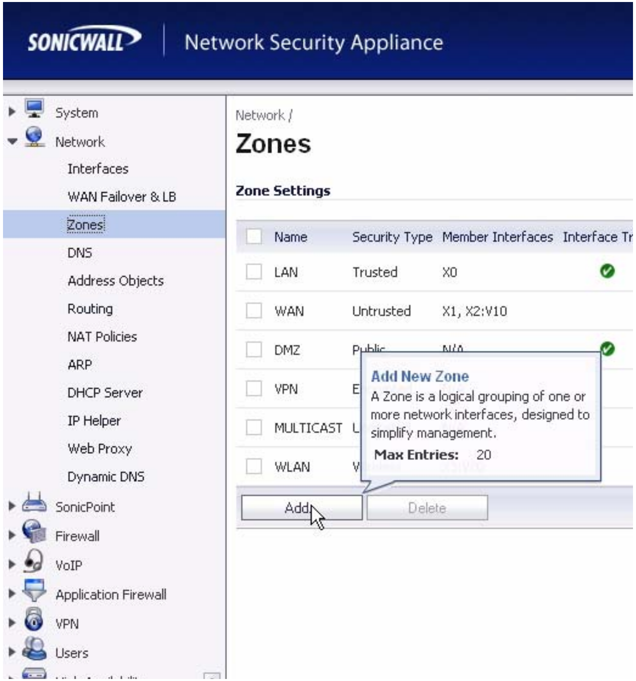
Select a category below to see the top 25 knowledge items (questions) for that category.

What's New!

- Aventail EX Series SSL VPN articles have been moved to the **SSL VPN (Remote Access)** category.
- SSL-VPN firmware version 3.0 has recently been released.
- SonicOS Enhanced 3.9.0.3 and SonicOS Standard 3.9.0.0 have been released for TZ 180, 180W (wireless), 190 and 190W (Wireless) appliances.

Onboard Help

SonicOS features a dynamic Onboard Help in the form of helpful tooltips that appear over various elements of the GUI when the mouse hovers over them. Elements that display these tooltips include text fields, radio buttons, and checkboxes.



Zones

Zone Settings

□	Name	Security Type	Member Interfaces	Interface Tr
□	LAN	Trusted	X0	✓
□	WAN	Untrusted	X1, X2:V10	
□	DMZ	Public	N/A	✓
□	VPN	E		
□	MULTICAST	U		
□	WLAN	V		

Add New Zone

A Zone is a logical grouping of one or more network interfaces, designed to simplify management.

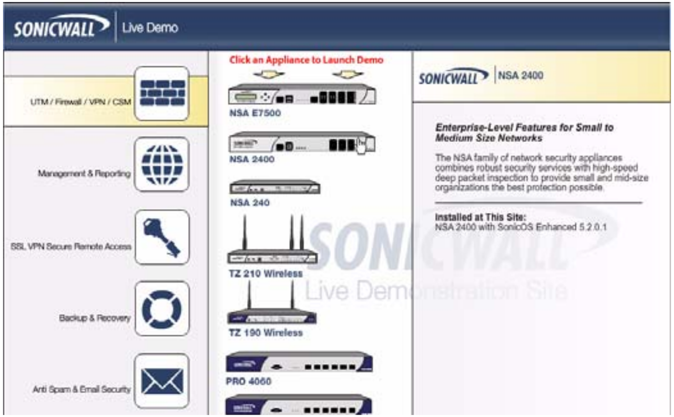
Max Entries: 20

SonicWALL Live Product Demos

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/>



Enterprise-Level Features for Small to Medium Size Networks

The NSA family of network security appliances combines robust security services with high-speed deep packet inspection to provide small and mid-size organizations the best protection possible.

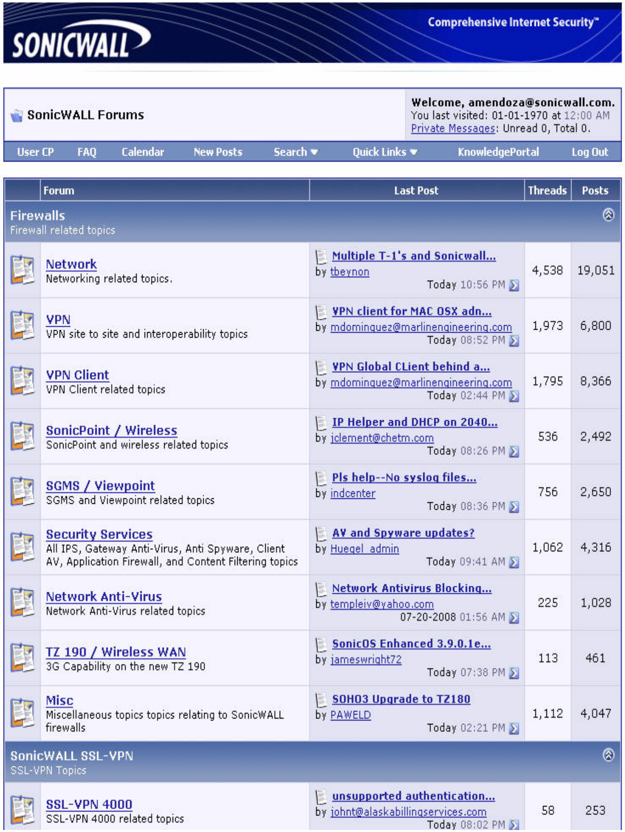
Installed at This Site:
NSA 2400 with SonicOS Enhanced 5.2.0.1

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
- TZ 200 / 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.

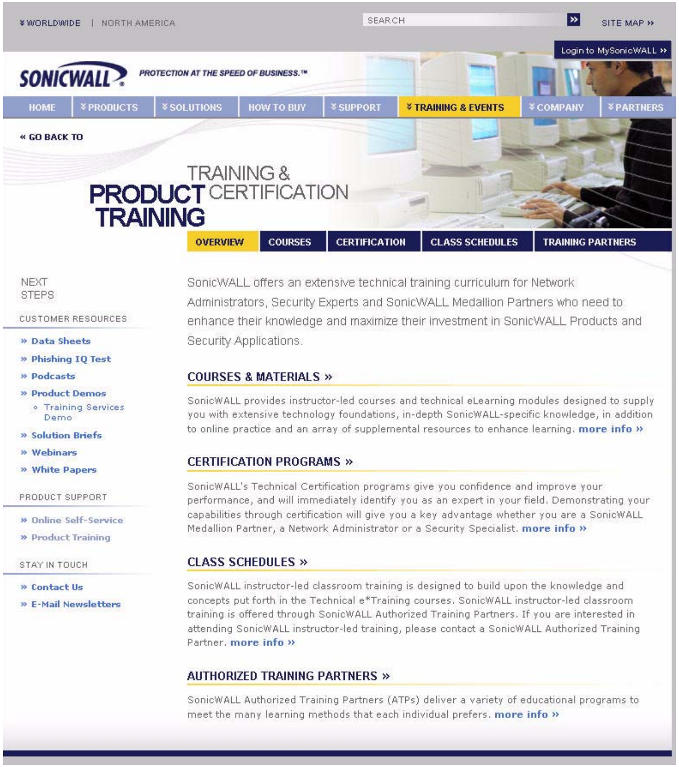
Forum	Last Post	Threads	Posts
Firewalls Firewall related topics			
Network Networking related topics.	Multiple T-1's and Sonicwall... by tbeynon Today 10:56 PM	4,538	19,051
VPN VPN site to site and interoperability topics	VPN client for MAC OSX adn... by mdominguez@marlinengineering.com Today 08:52 PM	1,973	6,800
VPN Client VPN Client related topics	VPN Global CLient behind a... by mdominguez@marlinengineering.com Today 02:44 PM	1,795	8,366
SonicPoint / Wireless SonicPoint and wireless related topics	IP Helper and DHCP on 2040... by jclement@chetm.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 jameswright72 Today 07:38 PM	113	461
Misc Miscellaneous topics topics relating to SonicWALL firewalls	SOHO3 Upgrade to TZ180 by PAWELD 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@alaskabillingservices.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/training.html>



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 e*Training 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 »

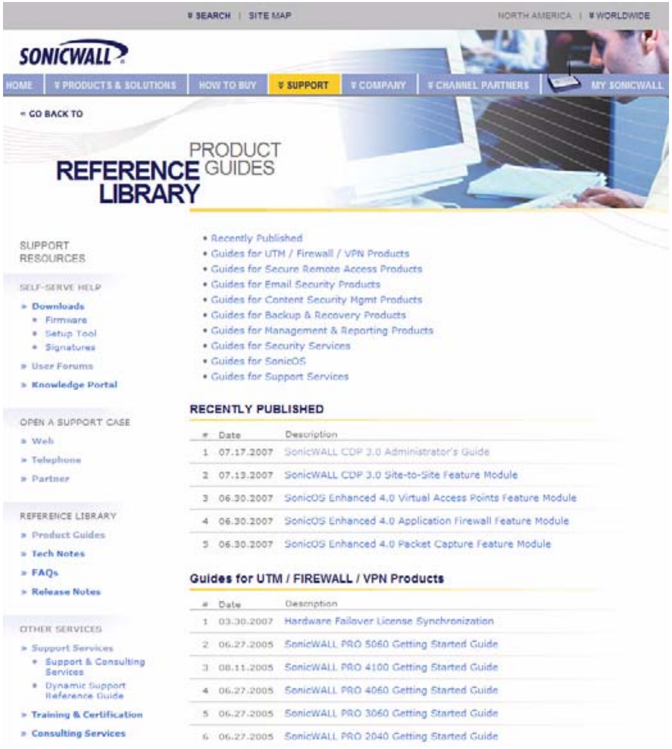
SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. **more info »**

Related Documentation

See the following related documents for more information:

- *SonicOS Enhanced Administrator’s Guide*
- *SonicOS Enhanced Release Notes*
- *SonicOS Enhanced Feature Modules*
  - Dashboard
  - High Availability
  - Multiple Admin
  - NAT Load Balancing
  - Packet Capture
  - Radio Frequency Monitoring
  - Single Sign-On
  - SSL Control
  - Virtual Access Points
- *SonicWALL GMS 5.0 Administrator’s Guide*
- *SonicWALL GVC 4.0 Administrator’s Guide*
- *SonicWALL ViewPoint 5.0 Administrator’s Guide*
- *SonicWALL GAV 4.0 Administrator’s Guide*
- *SonicWALL IPS 2.0 Administrator’s Guide*
- *SonicWALL Anti-Spyware Administrator’s Guide*
- *SonicWALL CFS Administrator’s Guide*

For further information, visit:
<http://www.sonicwall.com/us/support.html>



- 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

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

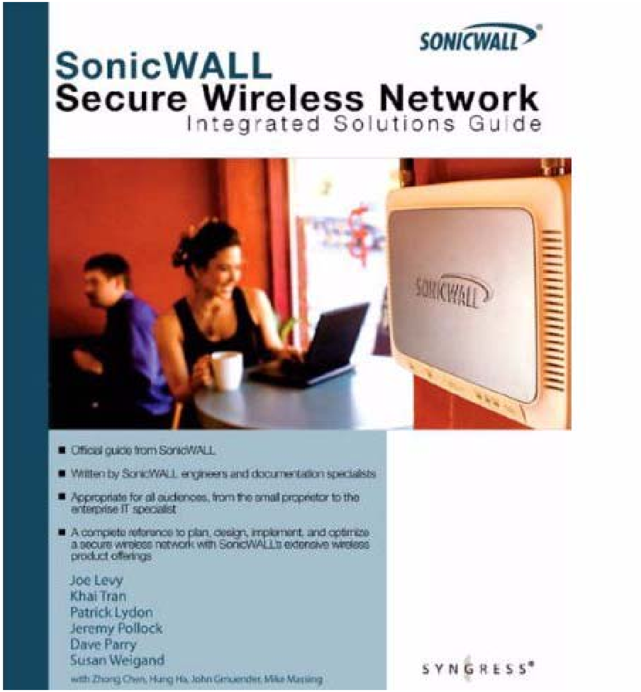
Guides for UTM / FIREWALL / VPN Products

#	Date	Description
1	03.30.2007	Hardware Failover License Synchronization
2	06.27.2005	SonicWALL PRO 5060 Getting Started Guide
3	08.11.2005	SonicWALL PRO 4100 Getting Started Guide
4	06.27.2005	SonicWALL PRO 4060 Getting Started Guide
5	06.27.2005	SonicWALL PRO 3060 Getting Started Guide
6	06.27.2005	SonicWALL PRO 2040 Getting Started Guide

SonicWALL Secure Wireless Network Integrated Solutions Guide

The Official Guide to SonicWALL's market-leading wireless networking and security devices.

This 512 page book is available in hardcopy. Order the book directly from Elsevier Publishing at: <http://www.elsevier.com>



SONICWALL

SonicWALL
Secure Wireless Network
Integrated Solutions Guide

- Official guide from SonicWALL
- Written by SonicWALL engineers and documentation specialists
- Appropriate for all audiences, from the small proprietor to the enterprise IT specialist
- A complete reference to plan, design, implement, and optimize a secure wireless network with SonicWALL's extensive wireless product offerings

Joe Levy
Khai Tran
Patrick Lydon
Jeremy Pollock
Dave Parry
Susan Weigand

with Zhong Chen, Hung Ha, John Gmuender, Mike Massing

SYNGRESS®

Use SonicWALL wireless solutions to deploy secure wireless networks of any shape or size!

Do Wireless. Securely.

Nearly forty percent of the world's 1 billion+ Internet users are wireless. It's a truly staggering fact to think that the majority of these wireless implementations are fundamentally insecure, leaving users and private data at risk.

Many wireless network proprietors think that the convenience of wireless outweighs the possible risk of an insecure implementation, or that secure wireless is far too complicated to worry about deploying.

Throughout this book, the engineers and documentation authors at SonicWALL prove the opposite is true. Wireless networks can be made as secure as wired networks, and deploying this type of security can be far less complicated than you think. In this book, and through their massive product offerings, SonicWALL gives you (the secure wireless network hopeful) all of the planning, design, implementation, and optimizing tools you need to do wireless. Securely.

Syngress Solutions Memberships!

Your Solutions Membership gives you access to the downloadable e-book version at no additional charge.

- Full color PDF format version of the print book
- Print, copy, and comment features all enabled
- Updates to the print book if needed

www.syngress.com/solutions

SonicWALL's Three Phases for a Secure Wireless Network

Using a comprehensive approach to security, SonicWALL guides you through a complete integrated solution for a secure wireless network using a three phase approach.

Phase 1
UTM Gateway

Phase 2
Secure Remote Access

Phase 3
Centralized Management

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

P/N 232-001720-00
Rev A 05/09