SonicWALL Network Security Appliances

NETWORK SECURITY

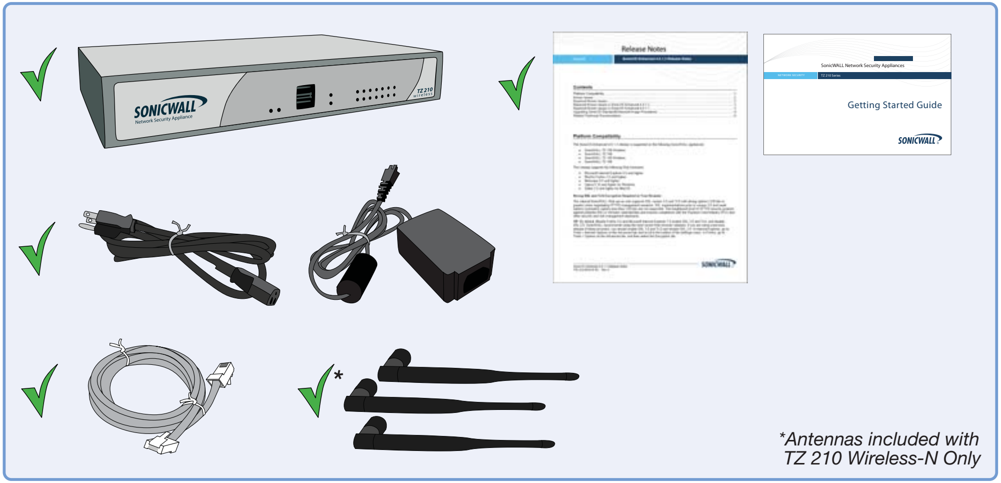
TZ 210 Series

# Getting Started Guide

SONICWALL®

# SonicWALL TZ 210 Series | **Quick Start**

Start here if you are new to SonicWALL appliances. The next few pages provide a Quick Start to connecting your appliance. For a complete listing of contents, including more advanced network deployments, see the *Table of Contents* on *page i* of this guide.



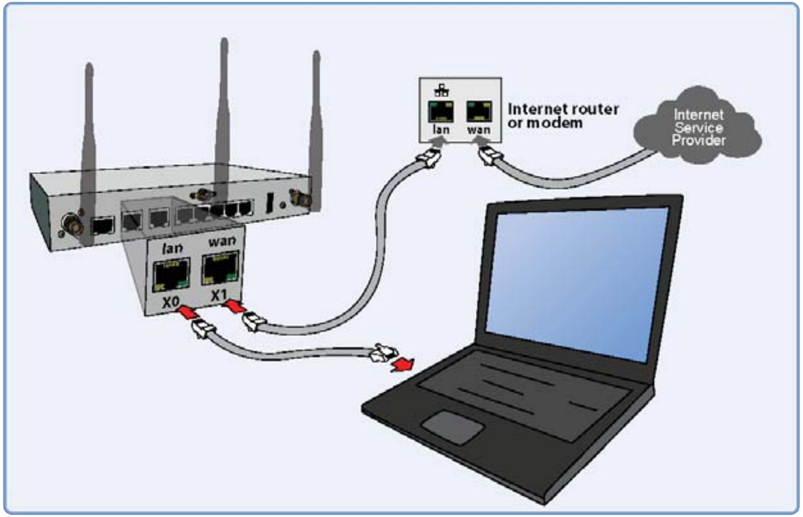
*Antennas included with TZ 210 Wireless-N Only

1. *Verify Contents*
2. *Connect Network*
3. *Connect Power*
4. *Boot Appliance*
5. *Setup Wizard*

**Missing Items?**
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>

# SonicWALL TZ 210 Series | **Quick Start**

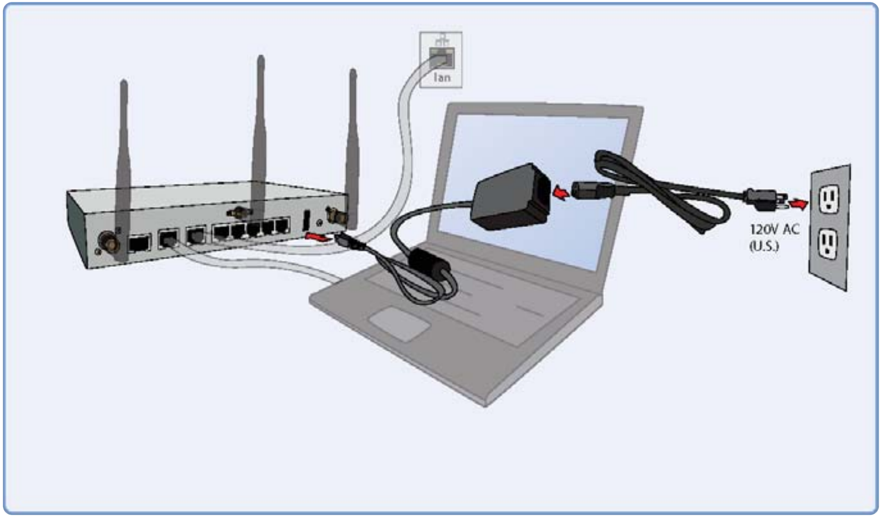
Connect the SonicWALL TZ 210 series appliance using standard CAT-5 Ethernet cables as shown in the illustration below.



1. *Verify Contents*
2. *Connect Network*
3. *Connect Power*
4. *Boot Appliance*
5. *Setup Wizard*

# SonicWALL TZ 210 Series | **Quick Start**

Connect the included power cable and adaptor and plug into a properly grounded 120V AC outlet.

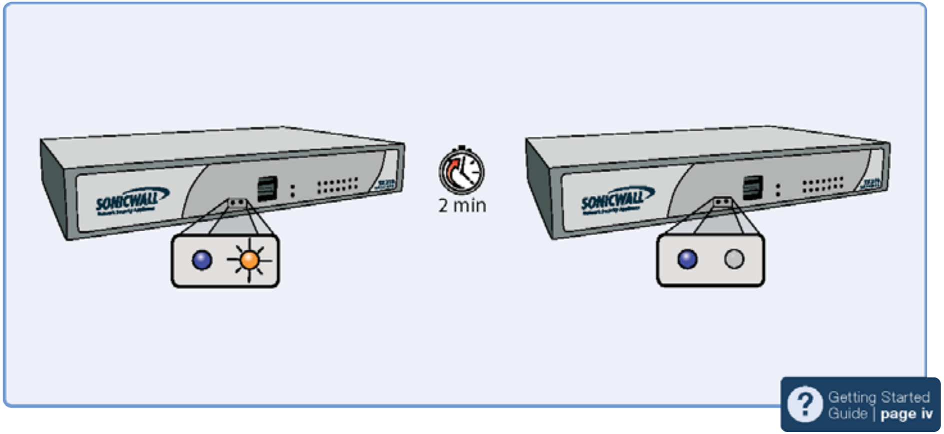


1. *Verify Contents*
2. *Connect Network*
3. *Connect Power*
4. *Boot Appliance*
5. *Setup Wizard*

# SonicWALL TZ 210 Series | **Quick Start**

The TZ 210 series appliance powers on and the orange “test” LED blinks during the boot sequence. Continue to the next step when the “test” LED is no longer lit. This process may take up to 2 minutes.

For troubleshooting this step, see *page iv* of this guide.



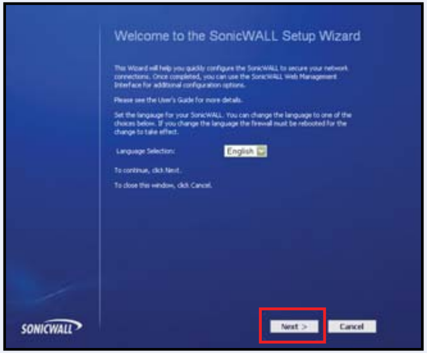
Getting Started Guide | **page iv**

1. *Verify Contents*
2. *Connect Network*
3. *Connect Power*
4. *Boot Appliance*
5. *Setup Wizard*

Using a computer connected to the LAN port of the SonicWALL TZ 210 series appliance, navigate to "http://192.168.168.168/" in a Web browser. The SonicWALL Setup Wizard displays.

Continue to *page 4* of this guide to complete the Setup Wizard.

http://192.168.168.168/
http://192.168.168.168/



Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections. Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

Set the language for your SonicWALL. You can change the language to one of the choices below. If you change the language the firewall must be rebooted for the change to take effect.

Language Selection: English

To continue, click Next.

To close this window, click Cancel.

Getting Started Guide | **page 4**

1 *Verify Contents*
2 *Connect Network*
3 *Connect Power*
4 *Boot Appliance*
5 *Setup Wizard*

# SonicWALL TZ 210 Series Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL TZ 210 series appliance running SonicOS Enhanced.

## Document Contents

This document contains the following sections:

1 Setting Up Your Network - page 1

2 Registering Your Appliance - page 9

3 Enabling Security Services - page 13

4 Advanced Network Configuration - page 21

5 Advanced Deployments - page 33

6 Support and Training Options - page 59

7 Product Safety and Regulatory Information - page 67

# SonicWALL TZ 210 Series Front Panel

## LAN/WAN Port Status

Provides dedicated LAN/WAN port status as follows:

**link/spd**: ○ Off=10M
● Green=100M
● Amber=1,000M

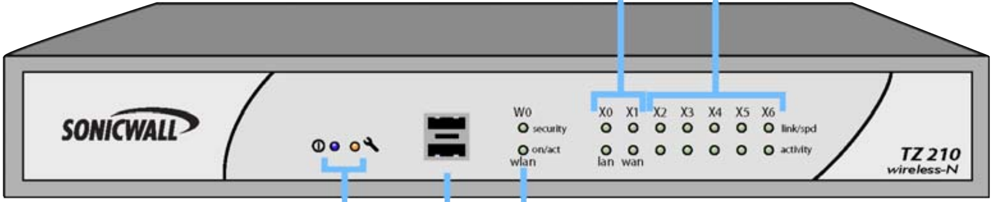
**activity**: ● Solid=link
☀ Blinking=activity

## 10/100 Ethernet Port Status

Provides Ethernet port status as follows:

**link/spd**: ○ Off=10M
● Green=100M

**activity**: ● Solid=link
☀ Blinking=activity



## Indicator LEDs

Provides power and test status
(refer to page iv)

## USB Ports

For future applications

## Wireless LAN Status

**On the TZ 210 Wireless only.** Provides Ethernet port status as follows:

**security**: ○ Off=no activity
☀ Blinking=activity

**on/act**: ○ Off=wireless radio off
● Solid=wireless radio on

# SonicWALL TZ 210 Series Rear Panel

### WAN Port (X1)

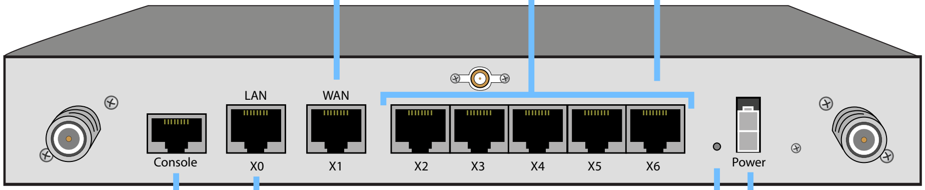
Provides dedicated WAN (Internet)

### Ethernet Ports (X2-X6)

Provides configurable 10/100 Ethernet ports for connection to network devices on WAN, LAN, DMZ, and other zone types

### HA Ethernet Port (X6)

Provides 10/100 Ethernet port for high availability (HA) connectivity



### Console Port

Provides access to the SonicOS Command Line Interface (CLI) via the DB9 -> RJ45 cable

### LAN Port (X0)

Provides dedicated LAN access to local area network resources

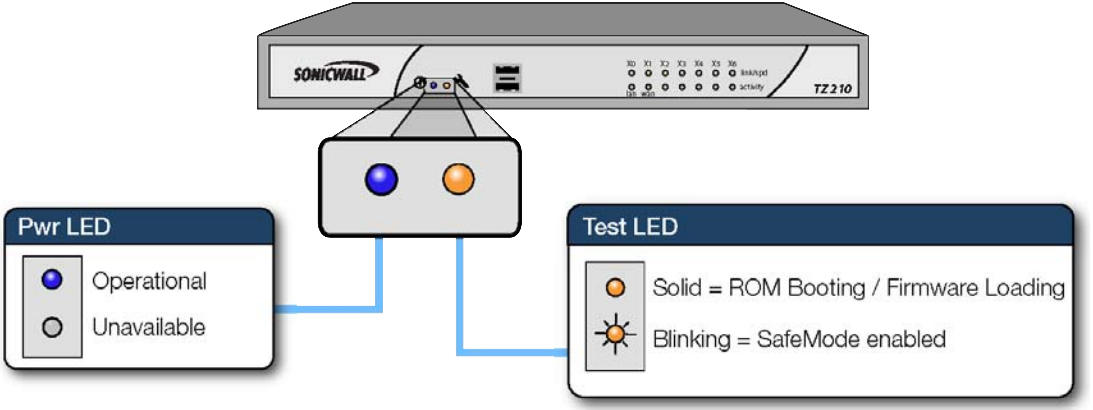
### Power Supply

Provides power connection using supplied power cable

### Reset Button

Press and hold to manually reset the appliance to SafeMode

# SonicWALL TZ 210 Series LED Reference



Pwr LED

● Operational

○ Unavailable

Test LED

● Solid = ROM Booting / Firmware Loading

✹ Blinking = SafeMode enabled

# Setting Up Your Network 1

## In this Section:

This section provides pre-configuration information. Review this section before setting up your SonicWALL TZ 210 series appliance.

- System Requirements - page 2
- Recording Configuration Information - page 2
- Completing the Setup Wizard - page 4
- Accessing the Management Interface - page 5
- Verifying WAN (Internet) Connectivity - page 6
- Connecting Your Network Devices - page 6
- Troubleshooting Initial Setup - page 7

# 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** |
|---|---|---|
| e | Internet Explorer | 6.0 or higher |
| | Firefox | 2.0 or higher |
| N | Netscape | 9.0 or higher |
| O | Opera | 9.10 or higher<br>for Windows |
| | Safari | 2.0 or higher<br>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**:<br>_______._______._______._______ | 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**:<br>_______._______._______._______ | Record the subnet mask for the local subnet where you are installing your SonicWALL appliance. |
| **Ethernet WAN IP Address**:<br>_______._______._______._______ | 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.<br>Host Name: ____________________ |
| **Home DSL** | PPPoE | User Name: ____________________<br>Password: ____________________<br>*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: _____._____._____._____<br>Subnet Mask: _____._____._____._____<br>Default Gateway (IP Address): _____._____._____._____<br>Primary DNS: _____._____._____._____<br>Secondary DNS (optional): _____._____._____._____ |
| **Dial-in to a server** | PPTP | Server Address: ____________________<br>User Name: ____________________<br>Password: ____________________ |

## Secondary ISP Information

Record the following information about your secondary ISP:

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

# Completing the Setup Wizard

The Setup Wizard takes you through several basic steps to get your SonicWALL TZ 210 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).

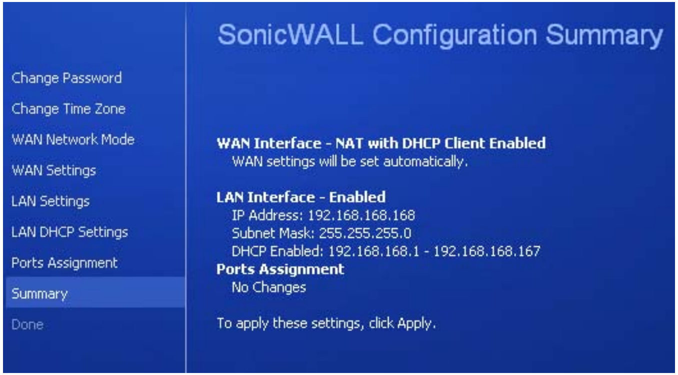
**WAN Settings**—Required for some WAN modes. This information is also provided by your ISP.

**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 210 series appliance to automatically connect other local computers by specifying a DHCP range, or use the default.

**Ports Assignment**—Configure the extra interfaces (X2-X6) 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 210 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 210 series appliance required a reboot after completing the Setup Wizard, wait until the 🔧 LED is no longer lit before continuing.

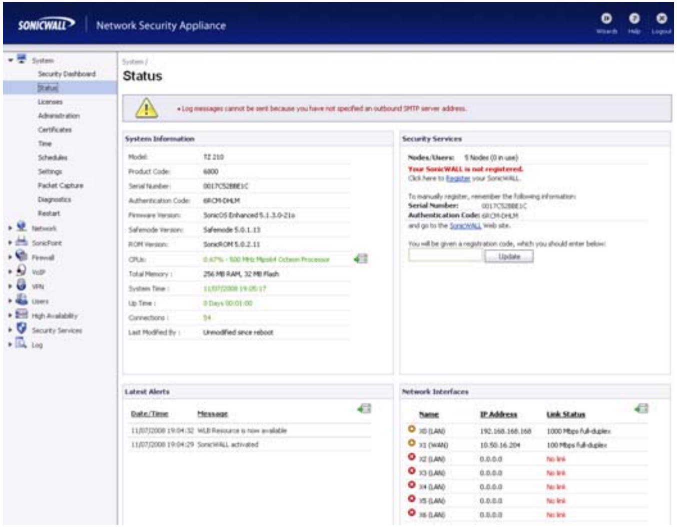
To access the SonicOS Web-based management interface:

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 210 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: 0017C52BBE1C
Authentication Code: 6RCM-DHLM
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 |

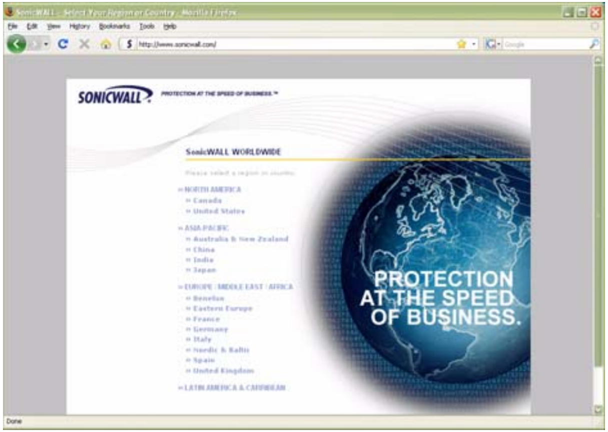
Network Interfaces

| 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
http://www.sonicwall.com/
Google
SONICWALL
PROTECTION AT THE SPEED OF BUSINESS.™
PROTECTION AT THE SPEED OF BUSINESS.
Done

SonicWALL WORLDWIDE

Please select a region or country

» NORTH AMERICA
- » Canada
- » United States

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

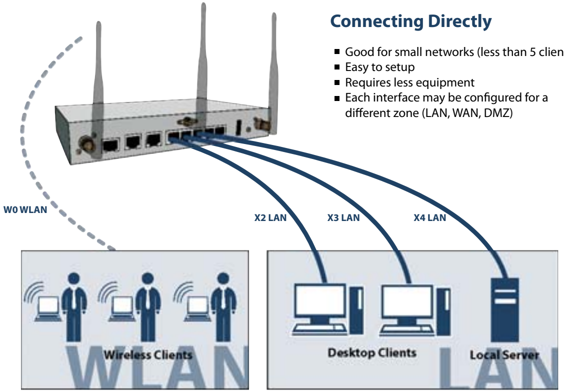
» EUROPE / MIDDLE EAST / AFRICA
- » Benelux
- » Eastern Europe
- » France
- » Germany
- » Italy
- » Nordic & Baltic
- » Spain
- » United Kingdom

» LATIN AMERICA & CARIBBEAN

# Connecting Your Network Devices

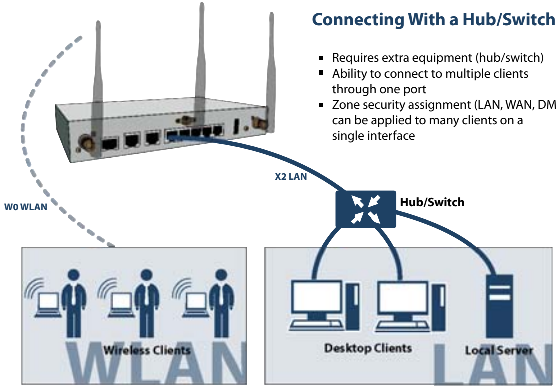
## Connecting Directly

- 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 210 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 210 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 210 series appliance.

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

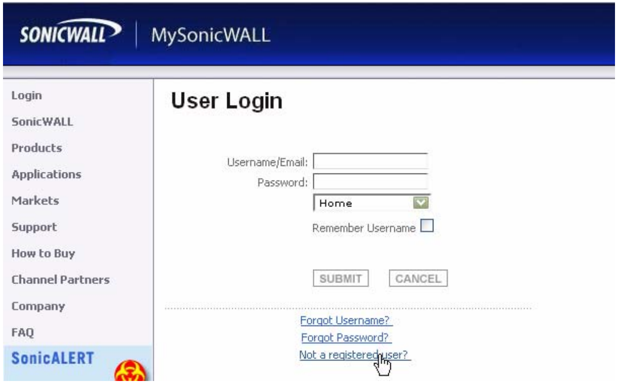
**Note:** *Registration is an important part of the setup process and is necessary to receive the benefits of SonicWALL security services, firmware updates, and technical support.*

# 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

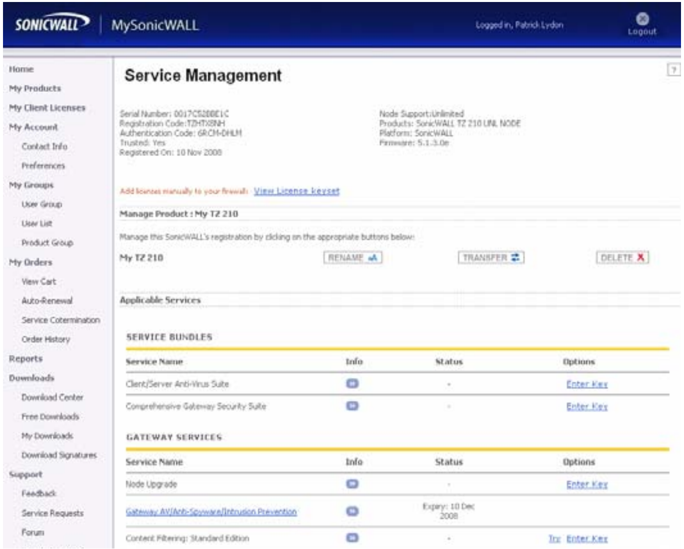
You must register your SonicWALL security appliance on MySonicWALL to enable full functionality.

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 210 series appliances:

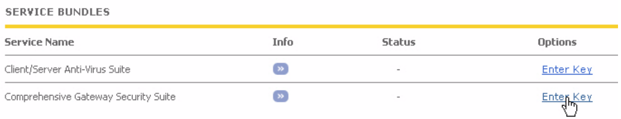
- **Gateway Service Bundles:**
  - Client/Server Anti-Virus Suite
  - Comprehensive Gateway Security Suite
- **Individual Gateway Services:**
  - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention
  - Global Management System
  - Content Filtering: Premium Edition
  - High Availability Upgrade
- **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.

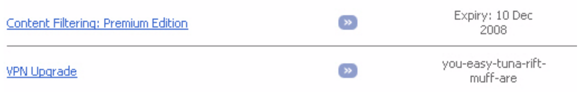


SERVICE BUNDLES

| 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**.

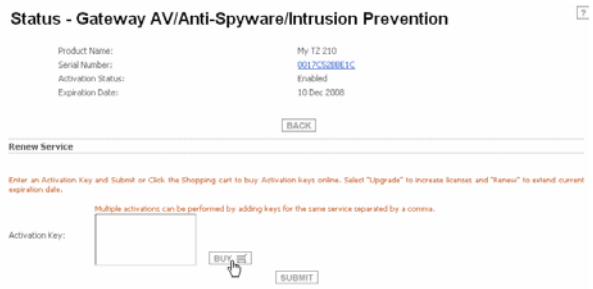
   Once the service is activated, you will see an expiration date or a license key string in the **Status** column on the Service Management page.



| | | |
|---|---|---|
| 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: | 0017C5200E1C |
| Activation Status: | Enabled |
| Expiration Date: | 10 Dec 2008 |

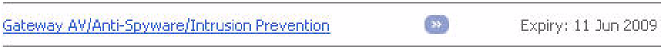
Renew Service

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 210 series appliance.

- Enabling Security Services in SonicOS - page 14
- Verifying Security Services on Zones - page 19

# 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.

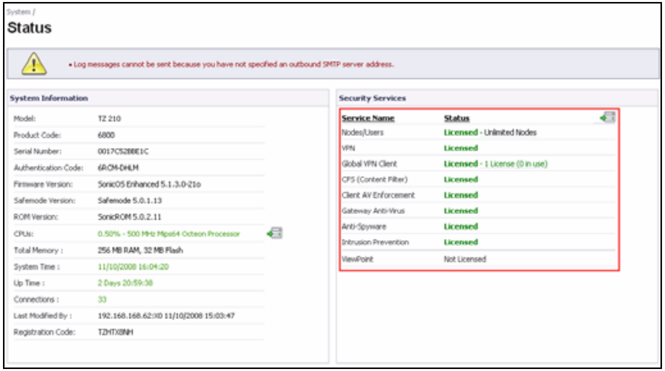
SonicWALL security services are key components of threat management in SonicOS. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

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**

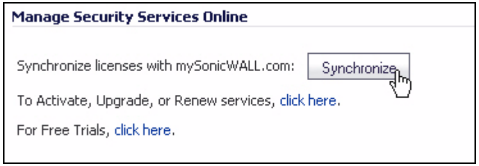
| | |
|---|---|
| Model: | TZ 210 |
| Product Code: | 6800 |
| Serial Number: | 0017C52BBE1C |
| Authentication Code: | 6RCM-DHLM |
| Firmware Version: | SonicOS Enhanced 5.1.3.0-21o |
| Safemode Version: | Safemode 5.0.1.13 |
| ROM Version: | SonicROM 5.0.2.11 |
| CPUs: | 0.50% - 500 MHz Mips64 Octeon 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

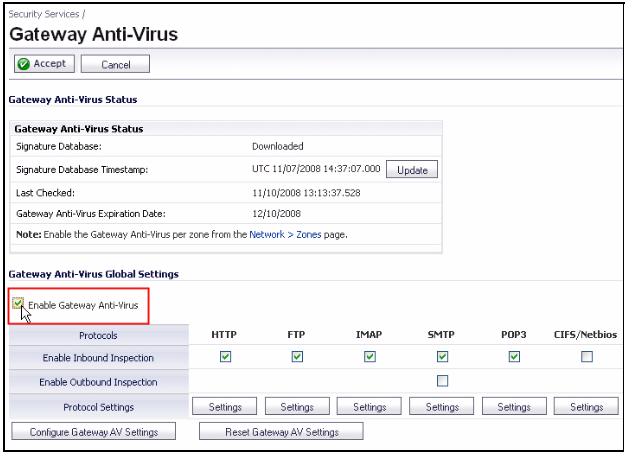
To Activate, Upgrade, or Renew services, click here.

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

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 |

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:

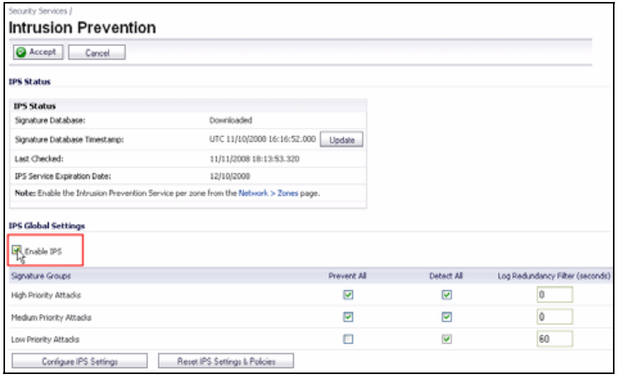
- **Outbound SMTP Inspection** scans outbound email
- **User Notification** notifies users when content is blocked
- **File-Type Restrictions** blocks various non-scannable files
- **Exclusion Lists** for network nodes where Gateway Anti-Virus enforcement is not necessary.

**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.



**IPS Status**

| IPS Status | |
|---|---|
| Signature Database: | Downloaded |
| Signature Database Timestamp: | UTC 11/10/2008 16:16:52.000 |
| 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.*

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

Intrusion Prevention contains other useful features, including:

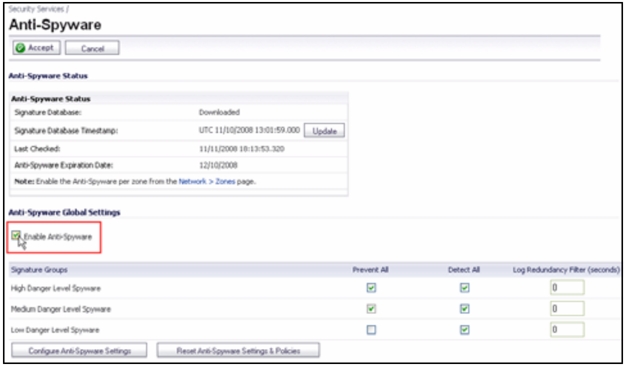
- **Exclusion Lists** for network nodes where IPS enforcement is not necessary.
- **Log Redundancy** to control log size during high-volume intrusion attack attempts by enforcing a delay between log entries.

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

**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 10:13:53.320 |
| 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:

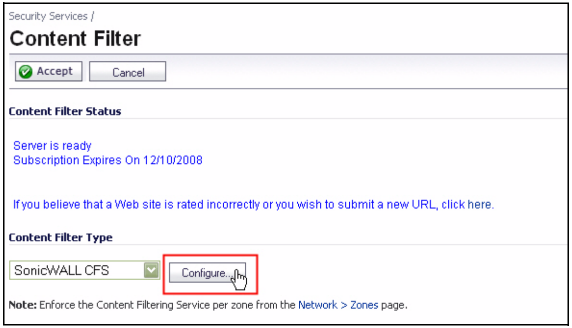
- **Exclusion Lists** excludes network nodes when Anti-Spyware enforcement is not necessary.
- **Log Redundancy** controls log size during high-volume intrusion attack attempts by enforcing a delay between log entries.
- **Clientless Notification** displays messages to users when content is blocked by 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.



**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.

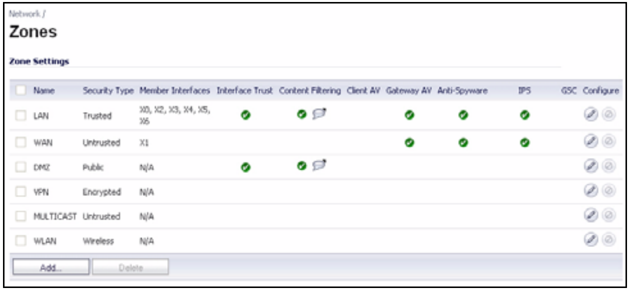
**Tip:** *For a complete overview of CFS features, refer to the SonicOS Enhanced Administrator’s Guide.*

## 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 210 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 210 series appliance to various network devices.

- An Introduction to Zones and Interfaces - page 22
- SonicWALL Wireless Firewalling - page 23
- Configuring Interfaces - page 24
- Creating Network Access Rules - page 27
- Address Objects - page 29
- Network Address Translation - page 31

**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

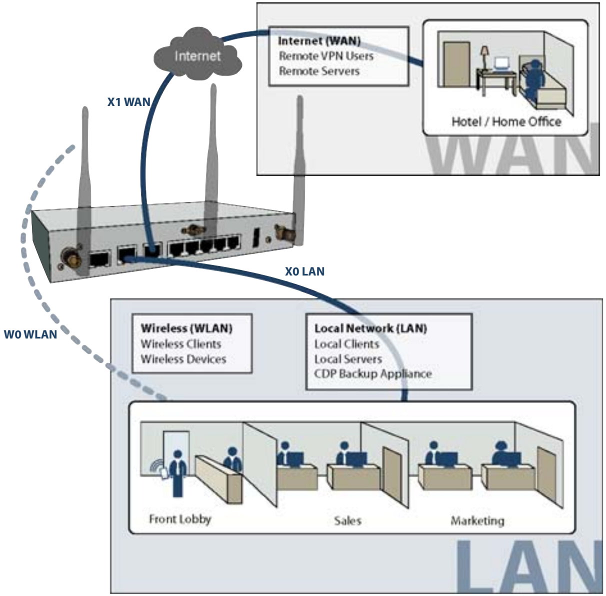
**WLAN**—Local wireless network resources originating from SonicWALL wireless enabled appliances.

**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 210 series appliance.

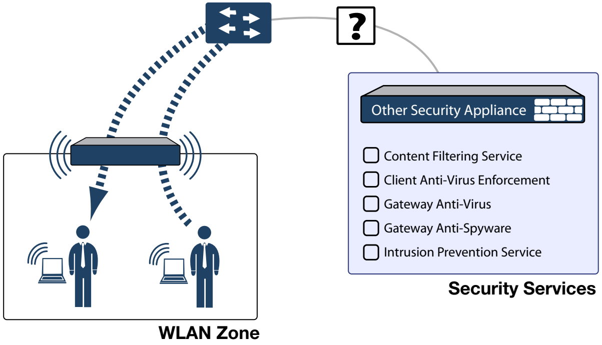
The X1 and X0 interfaces are preconfigured as WAN and LAN respectively. The remaining ports (X2-X6) are also LAN ports by default, however, these ports can be configured to meet the needs of your network, either by using basic zone types (WAN, LAN, WLAN, DMZ, VPN) or configuring a custom zone type to fit your network requirements (Gaming Console Zone, Wireless Printer Zone, Wireless Ticket Scanner Zone, and more).



## SonicWALL Wireless Firewalling

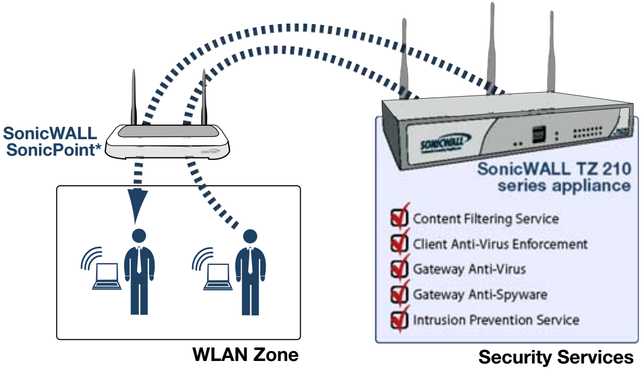
When a wireless device uses an access point to communicate with a device on another subnet or on a completely different network, traffic between the devices is forced to traverse the network gateway. This traversal enables Unified Threat Management (UTM) services to be enforced at the gateway.

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 210 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 TZ 210 wired 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

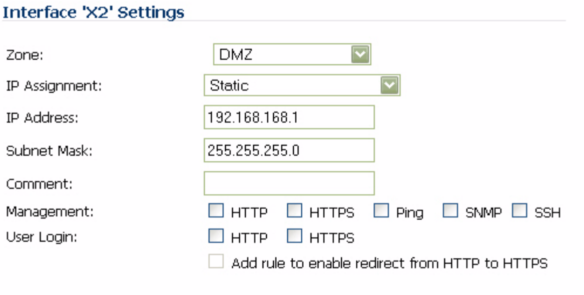
## Configuring an Interface

The SonicOS Enhanced Web-based management interface allows you to configure each individual Ethernet port (from X2-X6) 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

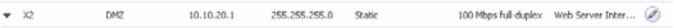
Comment:

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 210 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** | X0, X2-X6: LAN<br>X1: WAN | Connect any local network device to X0, or X2-X6 for local and Internet connectivity. |
| **WAN/LAN/ DMZ** | X0, X3-X6: LAN<br>X1: WAN<br>X2: DMZ | Connect any local network device to X0, or X3-X6 for local and Internet connectivity.<br>Connect public-facing servers or other semi-public resources to X2. |

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.

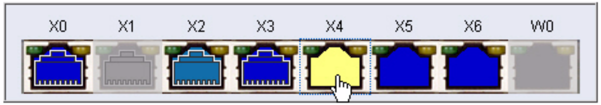
**Note:** *For more information about PortShield interfaces, see the SonicOS Enhanced Administrator’s Guide.*

## Manual PortShield Configuration

You can also manually group ports together using the graphical PortShield Groups interface. Grouping ports allows them to share a common network subnet as well as common zone settings.

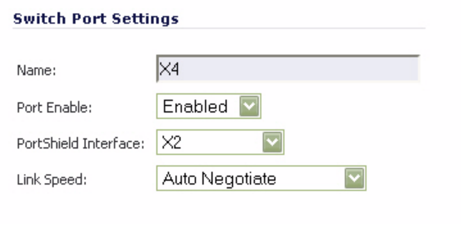
To manually configure a PortShield interface:

1. Navigate to the **Network > PortShield Groups** page.
2. Click one or more interfaces in the PortShield interface and then click the **Configure** button.



3. Select Enabled from the **Port Enable** drop-down menu.
4. Select the port with which you wish to group this interface from the **PortShield Interfaces** drop-down menu

**Note:** *Interfaces must be configured before being grouped with PortShield. For instructions, see the Configuring an Interface section, on page 24.*



**Switch Port Settings**

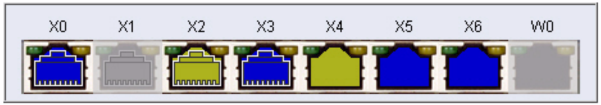
Name: X4

Port Enable: Enabled

PortShield Interface: X2

Link Speed: Auto Negotiate

5. Click the **OK** button. Your new port groupings display as color-coded ports.



# Creating Network Access Rules

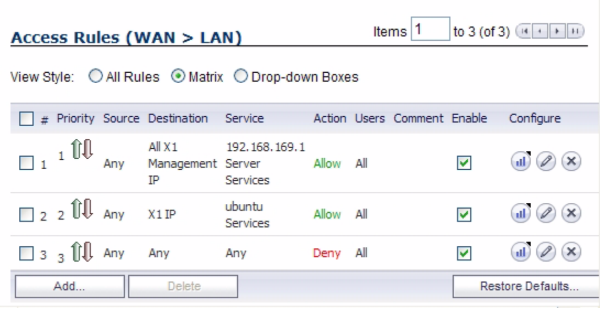
A Zone is a logical grouping of one or more interfaces designed to make management a simpler and more intuitive process than following a strict physical interface scheme.

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)

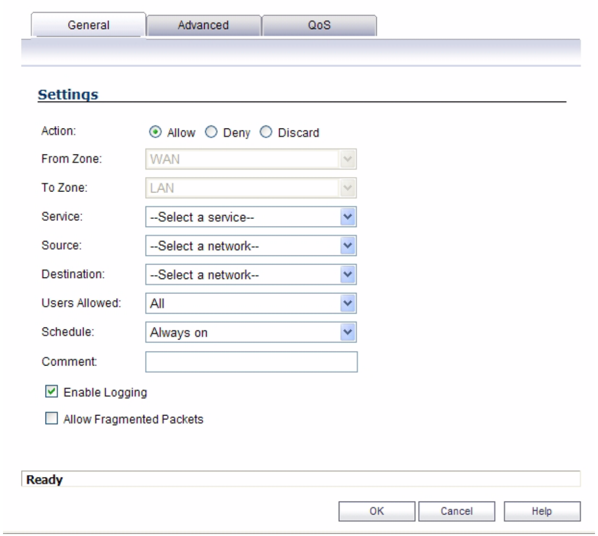
View Style: ○ All Rules ● Matrix ○ Drop-down Boxes

| □ | # | 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:

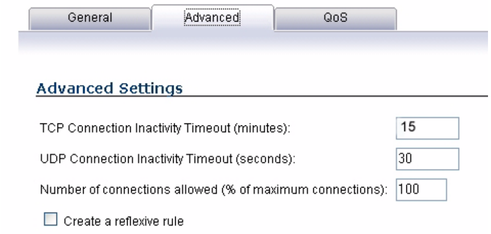
☑ Enable Logging

□ 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.*

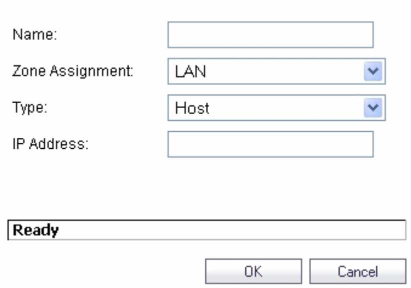
## Creating an Address Object

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.

To add an Address Object:

1. Navigate to the **Network** > **Address Objects** page.
2. Below the **Address Objects** table, click **Add**.
3. In the **Add Address Object** dialog box, enter a name for the Address Object in the **Name** field.



Name:

Zone Assignment: LAN

Type: Host

IP Address:

Ready

4. Select the zone to assign to the Address Object from the **Zone Assignment** drop-down list.
5. Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.
   - For **Host**, enter the IP address in the **IP Address** field.
   - For **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
   - For **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.
   - For **MAC**, enter the MAC address in the **MAC Address** field.
   - For **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.
6. Click **OK**.

# 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** > **NAT Policies** page. Click **Add**. The **Add NAT Policy** dialog box displays.
2. For **Original Source**, select **Any**.
3. For **Translated Source**, select **Original**.
4. For **Original Destination**, select **X0 IP**.
5. For **Translated Destination**, select **Create new address object** and create a new address object using **WAN** for Zone Assignment and **Host** for Type.
6. For **Original Service**, select **HTTP**.
7. For **Translated Service,** select **Original**.
8. For **Inbound Interface**, select **X0**.
9. For **Outbound Interface**, select **Any**.
10. For **Comment**, enter a short description.
11. Select the **Enable NAT Policy** checkbox.
12. 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 policies.
13. Click **Add**.

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

# Advanced Deployments 5

## In this Section:

The advanced deployments contained in this chapter are based on the most common customer deployments and contain best-practice guidelines for deploying your SonicWALL TZ 210 series appliances. These deployments are designed as modular concepts to help in deploying your SonicWALL as a comprehensive security solution.

- SonicPoints for Wireless Access - page 34
- Public Server on DMZ - page 40
- Configuring High Availability - page 44
- Multiple ISP / WAN Failover and Load Balancing - page 53

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

# SonicPoints for Wireless Access

This section describes how to configure SonicPoints with the SonicWALL TZ 210 series appliance. SonicPoints can be used to add wireless features to a SonicWALL TZ 210 wired appliance, or to create a more robust distributed wireless network with a SonicWALL TZ 210 Wireless-N appliance.

This section contains the following subsections:

- Configuring Provisioning Profiles - page 36
- Configuring a Wireless Zone - page 37
- Assigning an Interface to the Wireless Zone - page 39
- Connecting the SonicPoint - page 40

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances. Before you can manage SonicPoints in the Management Interface, you must first:

- Configure your SonicPoint provisioning profiles.
- Configure a Wireless zone.
- Assign profiles to Wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.
- Attach the SonicPoints to the interface in the Wireless zone and test.

## Internet Gateway with SonicPoint Wireless

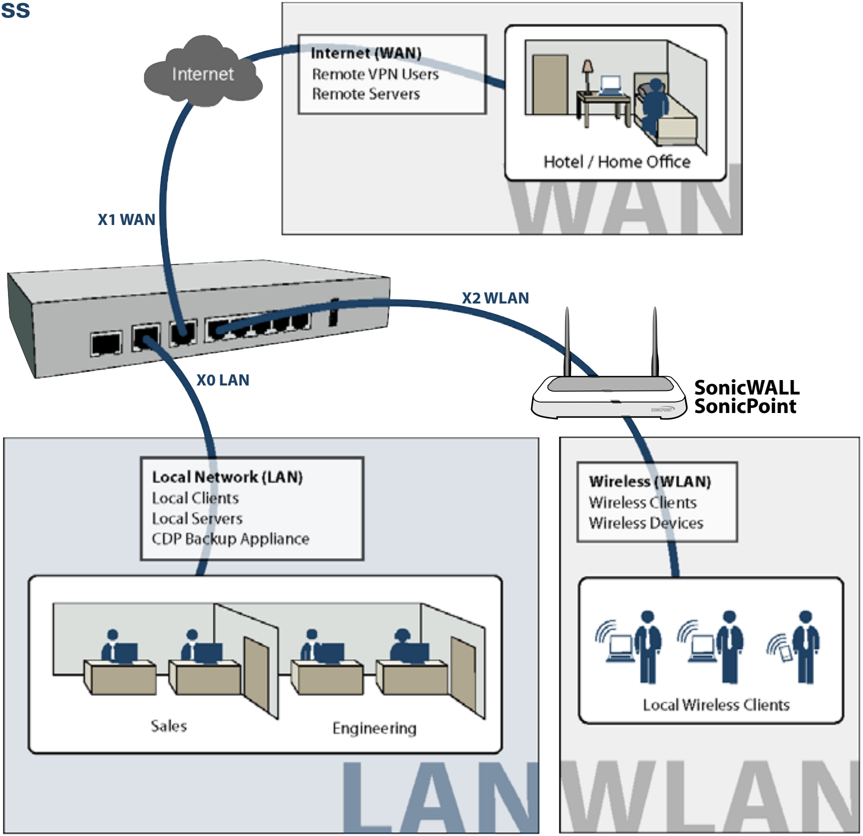
In this deployment, the SonicWALL TZ 210 is configured to operate as a network gateway with the following zones:

**Local Network (LAN)** - wired local client computers and servers

**Wireless (WLAN)*** - using a SonicPoint to deliver wireless to local client computers and devices

**Internet (WAN)** - worldwide public and private networks

*For the TZ 210 wired appliance, wireless is achieved by adding a SonicWALL SonicPoint appliance to any free interface (X2-X5) and zoning that interface as WLAN.



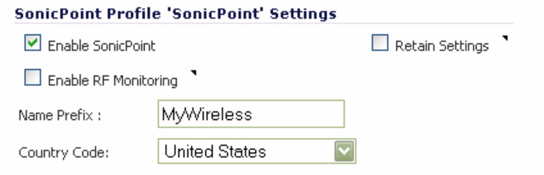
## Configuring Provisioning Profiles

SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSIDs, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. When a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone. SonicOS includes a default SonicPoint profile, named SonicPoint.

To add a new profile, click **Add** below the list of SonicPoint provisioning profiles. To edit an existing profile, select the profile and click the **Configure** icon in the same line as the profile you are editing.

1. In the Add/Edit SonicPoint Profile window on the **General** tab:
   - Select **Enable SonicPoint**.
   - Enter a **Name Prefix** to be used as the first part of the name for each SonicPoint provisioned.
   - Select the **Country Code** for where the SonicPoints are operating.



SonicPoint Profile 'SonicPoint' Settings

☑ Enable SonicPoint ☐ Retain Settings

☐ Enable RF Monitoring

Name Prefix : MyWireless

Country Code: United States

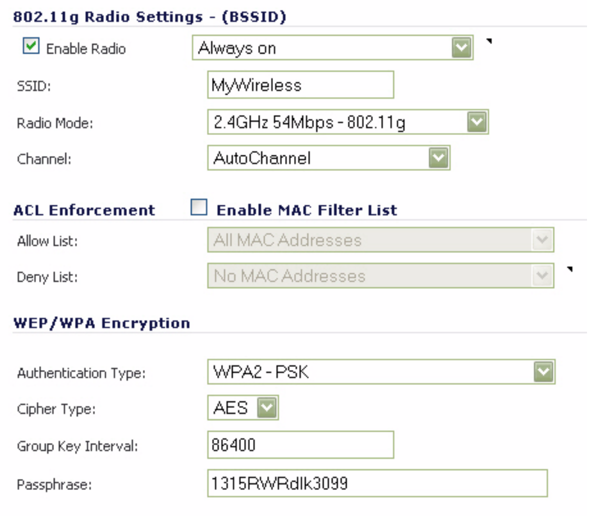
2. In the **802.11g Radio** tab:
   - Select **Enable Radio**.
   - Optionally, select a schedule for the radio to be enabled from the drop-down list.
   - For **Radio Mode**, select the speed that the SonicPoint will operate on. You can choose from the following:
     - 11Mbps - 802.11b
     - 54 Mbps - 802.11g
     - 108 Mbps - Turbo G

**Note:** *If you choose Turbo mode, all users in your company must use wireless access cards that support Turbo mode.*

   - For **Channel**, use AutoChannel unless you have a reason to use or avoid specific channels.
   - Enter a recognizable string for the **SSID** of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.
   - Under **ACL Enforcement**, select **Enable MAC Filter List** to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address object group from the **Allow List** to automatically allow traffic from all devices with MAC addresses in the group. Select a MAC address group from the **Deny List** to automatically deny traffic from all devices with

MAC addresses in the group. The Deny List is enforced before the Allow List.

- Under **WEP/WPA Encryption**, select the **Authentication Type** for your wireless network. SonicWALL recommends using **WPA2** as the authentication type.
- Fill in the fields specific to the authentication type that you selected. The remaining fields change depending on the selected authentication type.



**802.11g Radio Settings - (BSSID)**

☑ Enable Radio: Always on

SSID: MyWireless

Radio Mode: 2.4GHz 54Mbps - 802.11g

Channel: AutoChannel

**ACL Enforcement** ☐ **Enable MAC Filter List**

Allow List: All MAC Addresses

Deny List: No MAC Addresses

**WEP/WPA Encryption**

Authentication Type: WPA2 - PSK

Cipher Type: AES

Group Key Interval: 86400

Passphrase: 1315RWRdlk3099

3. In the **802.11g Adv** tab, configure the advanced radio settings for the 802.11g radio. For most 802.11g advanced options, the default settings give optimum performance. For a full description of the fields on this tab, see the *SonicOS Enhanced Administrator’s Guide*.
4. In the **802.11a Radio** and **802.11a Adv** tabs, configure the settings for the operation of the 802.11a radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.

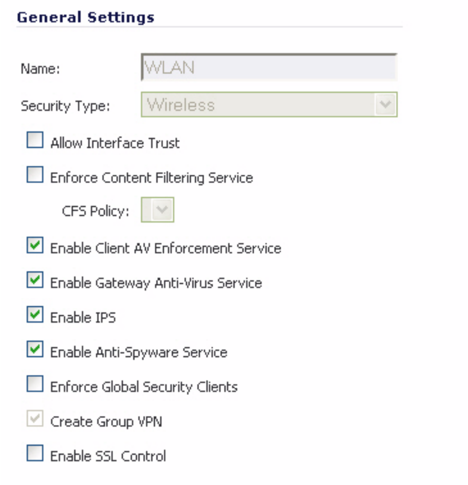
   The settings in the **802.11a Radio** and **802.11a Advanced** tabs are similar to the settings in the **802.11g Radio** and **802.11g Advanced** tabs.
5. When finished, click **OK**.

## Configuring a Wireless Zone

You can configure a wireless zone on the **Network** > **Zones** page. Typically, you will configure the WLAN zone for use with SonicPoints.

1. On the **Network** > **Zones** page in the **WLAN** row, click the icon in the **Configure** column.
2. In the Edit Zone dialog box on the **General** tab, the **Allow Interface Trust** setting automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the WLAN Zone has both the **X2** and **X3** interfaces assigned to it, selecting the **Allow Interface Trust** checkbox on the WLAN Zone creates the

necessary Access Rules to allow hosts on these interfaces to communicate with each other.



**General Settings**

Name: WLAN

Security Type: Wireless

☐ Allow Interface Trust

☐ Enforce Content Filtering Service

CFS Policy:

☑ Enable Client AV Enforcement Service

☑ Enable Gateway Anti-Virus Service

☑ Enable IPS

☑ Enable Anti-Spyware Service

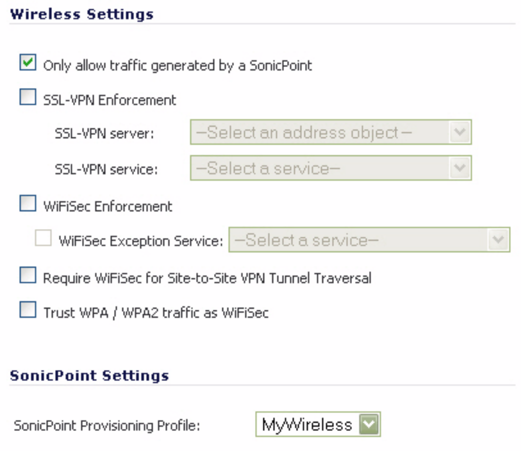
☐ Enforce Global Security Clients

☑ Create Group VPN

☐ Enable SSL Control

3. Select the checkboxes for the security services to enable on this zone. Typically, you would enable **Gateway Anti-Virus**, **IPS**, and **Anti-Spyware**. If your wireless clients are all running SonicWALL Client Anti-Virus, select **Enable Client AV Enforcement Service**.

4. Click on the **Wireless** tab.
   - In the **Wireless Settings** section, select **Only allow traffic generated by a SonicPoint** to allow only traffic from SonicWALL SonicPoints to enter the WLAN Zone interface. This provides maximum security on your WLAN. Uncheck this option if you want to allow any traffic on your WLAN Zone regardless of whether or not it is from a SonicPoint.



**Wireless Settings**

☑ Only allow traffic generated by a SonicPoint

☐ SSL-VPN Enforcement

SSL-VPN server: –Select an address object –

SSL-VPN service: –Select a service–

☐ WiFiSec Enforcement

☐ WiFiSec Exception Service: –Select a service–

☐ Require WiFiSec for Site-to-Site VPN Tunnel Traversal

☐ Trust WPA / WPA2 traffic as WiFiSec

**SonicPoint Settings**

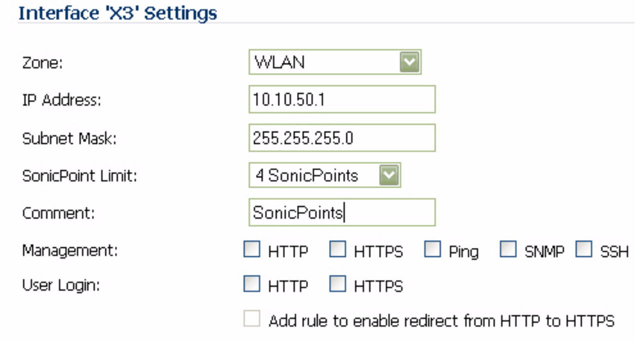
SonicPoint Provisioning Profile: MyWireless

5. Optionally configure the settings on the **Guest Services** tab. For information about configuring Guest Services, see the *SonicOS Enhanced Administrator’s Guide*.
6. When finished, click **OK**.

## Assigning an Interface to the Wireless Zone

Once the wireless zone is configured, you can assign an interface to it. This is the interface where you will connect the SonicPoint.

1. On the **Network** > **Interfaces** page, click the **Configure** icon on the row of the interface that you want to use, for example, X3. The interface must be unassigned.



Interface 'X3' Settings

|  |  |
|---|---|
| Zone: | WLAN |
| IP Address: | 10.10.50.1 |
| Subnet Mask: | 255.255.255.0 |
| SonicPoint Limit: | 4 SonicPoints |
| Comment: | SonicPoints |
| Management: | □ HTTP □ HTTPS □ Ping □ SNMP □ SSH |
| User Login: | □ HTTP □ HTTPS |
|  | □ Add rule to enable redirect from HTTP to HTTPS |

2. In the Edit Interface dialog box on the **General** tab, select **WLAN** or the zone that you created from the **Zone** drop-down list. Additional fields are displayed.
3. Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.
4. In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface. If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
5. If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
6. Click **OK**.

## Connecting the SonicPoint

When a SonicPoint unit is first connected and powered up, it attempts to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint locates a peer SonicOS device, such as your SonicWALL TZ 210 series appliance, the two units perform an encrypted exchange and the profile assigned to the relevant wireless zone is used to automatically configure (provision) the newly added SonicPoint unit.

To connect the SonicPoint:

1. Using a CAT 5 Ethernet cable, connect the SonicPoint to the interface that you configured. Then connect the SonicPoint to a power source.
2. In the SonicOS user interface on the **SonicPoint** > **SonicPoints** page, click the **Synchronize SonicPoints** button. The SonicWALL appliance downloads a SonicPoint image from the SonicWALL back-end server.
3. Follow the instructions in the SonicPoint wizard. Be sure to select the same authentication type and enter the same keys or password that you configured in SonicOS.

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

# Public Server on DMZ

This section provides instructions for configuring your SonicWALL TZ 210 series appliance to support a public Web server on a DMZ zone.

A Web server can be placed on the LAN by completing the server wizard, which creates the proper address objects and rules for safe access.

Many network administrators, however, choose to place the Web server on a DMZ, as it provides a dedicated Ethernet interface for added security and bandwidth management.

This section contains the following subsections:

- Completing the Public Server Wizard - page 42
- Configuring a DMZ Zone - page 43
- Editing the Address Object - page 43
- Editing the Firewall Access Rule - page 44

## Internet Gateway with Public Server on DMZ

In this deployment, the SonicWALL TZ 210 is configured to operate as a network gateway with the following zones:

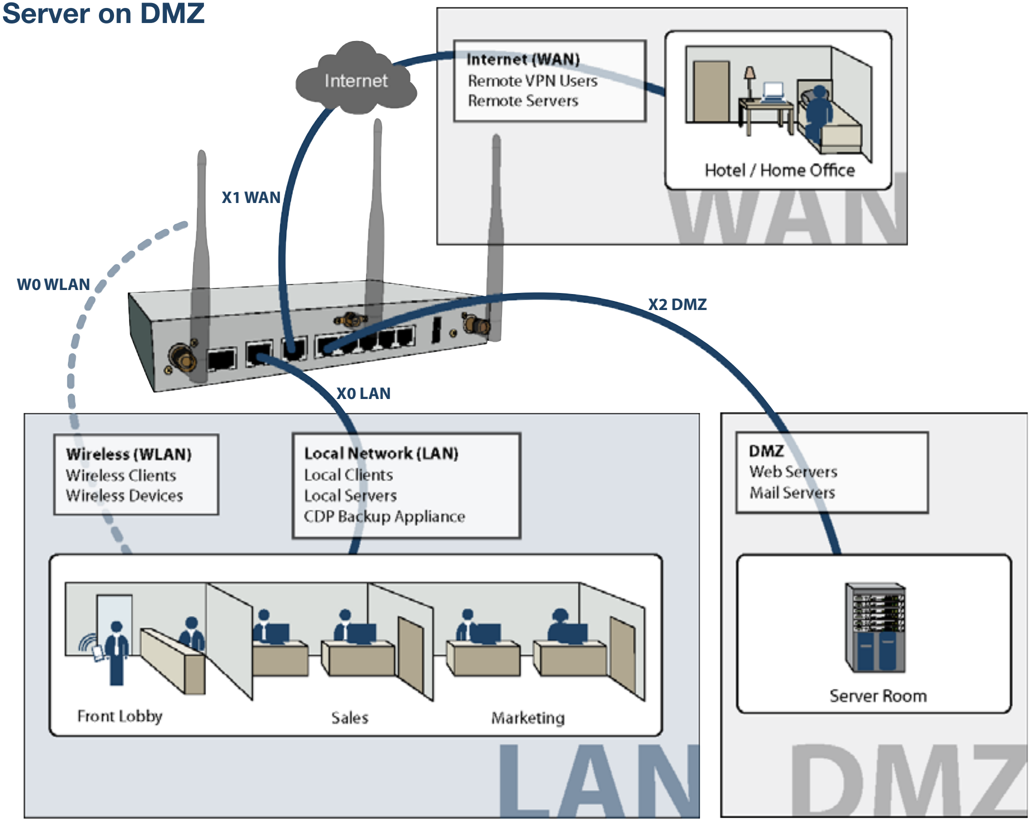
**Local Network (LAN)** - wired local client computers and servers

**Wireless (WLAN)*** - wireless local client computers and devices

**DMZ** - wired resources available to public Internet such as Web servers and Mail servers.

**Internet (WAN)** - worldwide public and private networks

*For the TZ 210 wired appliance, wireless is achieved by adding a SonicWALL SonicPoint appliance to any free interface (X3-X5) and zoning that interface as WLAN.



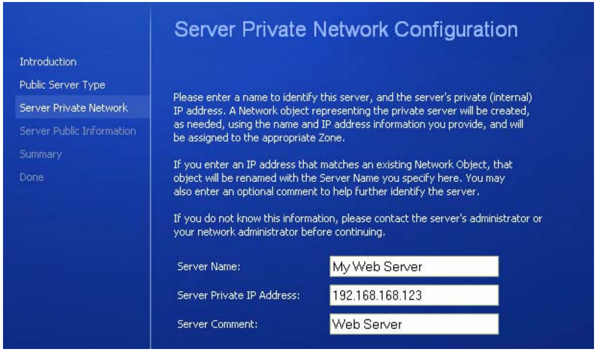
## Completing the Public Server Wizard

The Public Server Wizard guides you through a few simple steps, automatically creating address objects and rules to allow server access. To complete the public server wizard, perform the following steps:

1. Click the **Wizards** button in the upper right corner of the SonicOS management interface to launch the wizard.
2. Select **Public Server Wizard** and click **Next** to continue.
3. Select **Web Server** as the server type and ensure that the **HTTP** and **HTTPS** services are selected.

**Tip:** *HTTPS is required for servers authenticating SSL or other HTTPS-supported encryption methods. If your server does not require encryption, you can de-select the HTTPS service.*

4. Enter a **Server Name** in the field that is easy to remember such as “My Web Server”. This name is for your reference and does not necessarily need to be a domain or address.
5. Enter the **Private IP Address** of your server. This is the IP address where the server will reside within the DMZ zone. If you do not have a DMZ configured yet, select a private IP address (such as 192.168.168.123) and write it down, you will need to refer to this later.
6. Enter a **Server Comment** (optional) and click **Next**.



Server Private Network Configuration

Please enter a name to identify this server, and the server's private (internal) IP address. A Network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be renamed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

Server Name: My Web Server

Server Private IP Address: 192.168.168.123

Server Comment: Web Server

7. Enter the **Server Public IP Address** in the field (normally your primary WAN IP address). This IP Address is used to access your Web server from the Internet.
8. Click **Next** and then click **Apply** to finish the wizard.

**Note:** *If your server is on the LAN zone, you have completed the required steps for basic server access.*

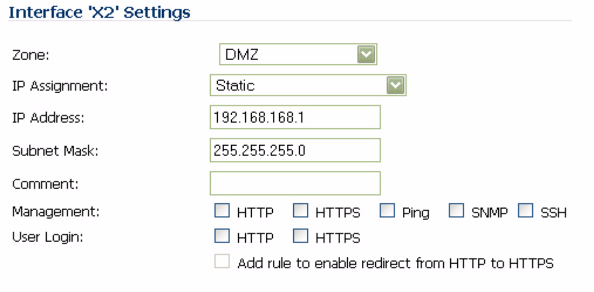
*If you wish to continue with an advanced DMZ zone configuration, turn to the Configuring a DMZ Zone section, on page 43.*

## Configuring a DMZ Zone

Since the public server is added to the LAN zone by default, configure a DMZ zone by performing the following steps:

1. In the **Network > Interfaces** panel, click the **Configure** button for the X2 interface. The Edit Interface window displays.

**Note:** *If the X2 interface is not displayed in the Interfaces list, click the **Show PortShield Interfaces** button to show all interfaces.*



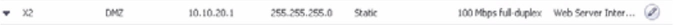
Interface 'X2' Settings

|  |  |
|---|---|
| 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 DMZ as the **Zone Type**.
3. Select Static as the **IP assignment**.
4. Enter an **IP Address** for the interface. This IP address must be in the same subnet as your Web server's local IP address.

**Tip:** *Since we used 192.168.168.123 in the example on page 42, use **192.168.168.1** as the DMZ interface IP.*

The newly created DMZ interface appears in the Interfaces list.

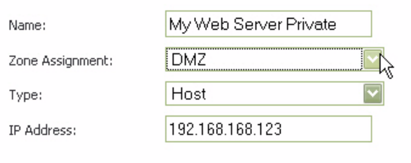


|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| X2 | DMZ | 10.10.20.1 | 255.255.255.0 | Static | 100 Mbps full-duplex | Web Server Inter... |

## Editing the Address Object

The address object that was automatically created must be changed from the LAN zone to DMZ zone.

1. On the **Network > Address Objects** page, click the configure button corresponds to your Web server object. In our case, the object is called "My Web Server Private".



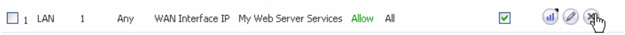
|  |  |
|---|---|
| Name: | My Web Server Private |
| Zone Assignment: | DMZ |
| Type: | Host |
| IP Address: | 192.168.168.123 |

2. Change the **Zone Assignment** to DMZ and click **OK**.

## Editing the Firewall Access Rule

An access rule that allows traffic from the WAN zone to the server on the DMZ must be created, and the original WAN > LAN rule that was created by the Public Server Wizard should be deleted.

1. On the **Firewall > Access Rules** page, chose Drop-down Boxes as the **View Style**.
2. Select WAN as the **From Zone** and ALL as the **To Zone**, then click **OK**. All of the WAN-based access rules display.
3. Click the **Delete** button corresponding to the WAN My Web Server Services rule. Click **OK** when prompted.

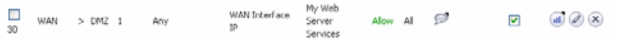


□ 1 LAN 1 Any WAN Interface IP My Web Server Services Allow All ☑

4. On the **Firewall > Access Rules** page, click the **Add** button. The **Add Rule** window displays.
5. Configure the new rule as follows:

| **Selection** | **Port Assignment** |
|---|---|
| **Action** | Allow |
| **From Zone** | WAN |
| **To Zone** | DMZ |
| **Service** | My Web Server Services. This service was automatically created during the Public Server Wizard and is named based on the Server Name you provided during setup. |
| **Source** | Any |
| **Destination** | WAN Interface IP. All traffic attempting to access your WAN IP address will be bound by this rule. |
| **Users Allowed** | All |
| **Schedule** | Always on, unless you choose to specify an uptime schedule such as “business hours only”. |
| **Comment** | Leave a comment such as “Web server on DMZ” |

6. Click **OK** to create this rule.
The new rule displays in the Access Rules table:



□ 30 WAN > DMZ 1 Any WAN Interface IP My Web Server Services Allow All ☑

# Configuring High Availability

This section provides instructions for configuring a pair of SonicWALL TZ 210 series appliances for redundant High Availability (HA) networking.

This section contains the following subsections:

- About High Availability - page 46
- Initial HA Setup - page 46
- HA License Synchronization Overview - page 47
- Associating Pre-Registered Appliances - page 48
- Disabling PortShield Before Configuring HA - page 48
- Configuring HA Settings - page 49
- Configuring Advanced HA Settings - page 49
- Configuring HA Monitoring - page 51
- Synchronizing Settings - page 52
- Verifying HA Functionality - page 53

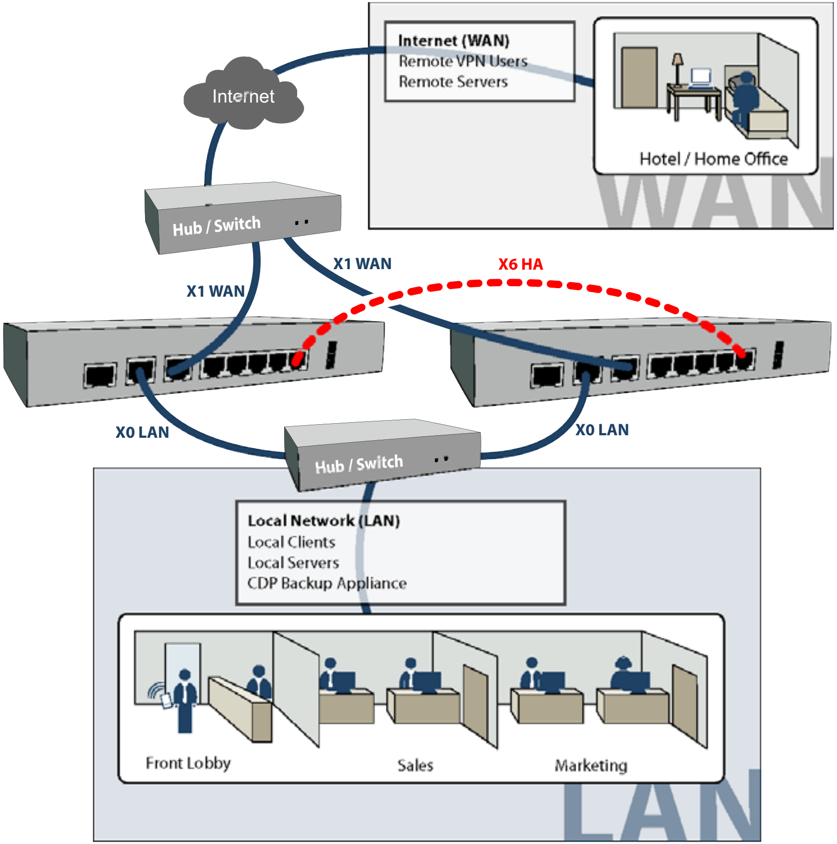
## High-Availability Mode

In this scenario, two SonicWALL TZ 210 series appliances are each configured with a single LAN zone and High Availability (HA) zone and linked to the LAN and WAN segments with a hub or switch. Typical zone assignments in this deployment are as follows:

**Local Network (LAN)** - linked to wired local client computers and servers through a hub or switch.

**Internet (WAN)** - linked to your internet service provider using a hub or switch connected to your modem.

**HA** - linked between two TZ 210 series appliances using the X6 port



## About High Availability

In this scenario, one SonicWALL TZ 210 series appliance operates as the Primary gateway device and the other acts as the Backup. Once configured for High Availability, the Backup SonicWALL contains a real-time mirrored configuration of the Primary SonicWALL via an Ethernet link between the designated HA interfaces on each appliance.

During normal operation, the Primary SonicWALL is in Active mode and the Backup SonicWALL is in Idle mode. If the Primary device loses connectivity, the Backup SonicWALL transitions to Active mode and assumes the configuration and role of the Primary gateway device. This automatic failover ensures a reliable connection between the protected network and the Internet.

After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

## Initial HA Setup

Before you begin the configuration of HA on the Primary SonicWALL security appliance, perform the following setup:

1. On the back panel of the Backup SonicWALL security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability** > **Settings** page.
2. Verify that the Primary SonicWALL appliance is registered and licensed for SonicOS Enhanced and the desired SonicWALL security services.
3. Associate the two SonicWALL appliances as HA Primary and HA Secondary on MySonicWALL, for license synchronization.
4. Make sure the Primary SonicWALL and Backup SonicWALL security appliances' LAN, WAN and other interfaces are properly configured for failover.
5. Connect the **X6** ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT 5 Ethernet cable. The Primary and Backup SonicWALL security appliances must have a dedicated connection.
6. Power up the Primary SonicWALL security appliance, and then power up the Backup SonicWALL security appliance.
7. Do not make any configuration changes to the Primary's X6 interface; the High Availability configuration in an upcoming step takes care of this issue.

## HA License Synchronization Overview

You can configure HA license synchronization by associating two SonicWALL security appliances as HA Primary and HA Secondary on MySonicWALL. Note that the Backup appliance of your HA pair is referred to as the HA Secondary unit on MySonicWALL.

You need only purchase a single license for SonicOS Enhanced, a single Support subscription, and a single set of security services licenses for the HA Primary appliance. These licenses are shared with the HA Secondary appliance. Only consulting services such as the SonicWALL GMS Preventive Maintenance Service license are not shared. See Registering and Licensing Your Appliance on MySonicWALL - page 10.

License synchronization is used during HA so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable HA, you can use the SonicOS UI to configure your two appliances as a HA pair in Active/Idle mode.

MySonicWALL provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. You can associate two units that are both already registered. Or you can select a registered unit and then add a new appliance with which to associate it.

**Note:** *After registering new SonicWALL appliances on MySonicWALL, you must also register each appliance from the SonicOS management interface by clicking the registration link on the **System** > **Status** page. This allows each unit to synchronize with the SonicWALL license server and share licenses with the associated appliance.*

## Associating Pre-Registered Appliances

To associate two already-registered SonicWALL security appliances so that they can use HA license synchronization, perform the following steps:

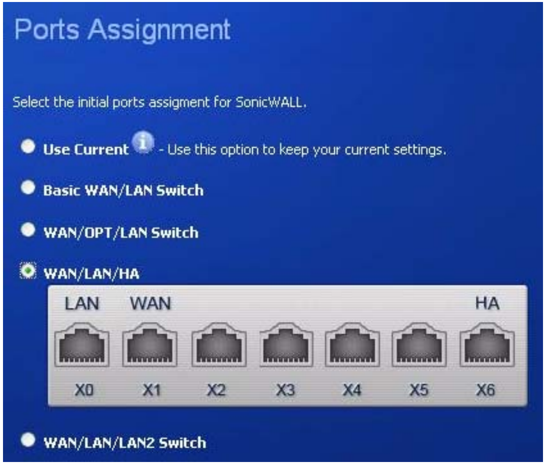
1. Login to MySonicWALL and click **My Products**.
2. On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or primary, unit. Click the product **name** or **serial number**.
3. On the Service Management page, scroll down to the Associated Products section.
4. Under Associated Products, click **HA Secondary**.
5. On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the secondary/backup unit.
6. Select the group from the **Product Group** drop-down list. The product group setting specifies the MySonicWALL users who can upgrade or modify the appliance.
7. Click **Register**.

## Disabling PortShield Before Configuring HA

The HA feature can only be enabled if PortShield is disabled on *all* interfaces of *both* the Primary and Backup appliances. You can disable PortShield either by using the **PortShield Wizard**, or manually from the **Network** > **PortShield Groups** page.

To use the PortShield Wizard to disable PortShield on each SonicWALL, perform the following steps:

1. On one appliance of the HA Pair, click the **Wizards** button at the top right of the management interface.
2. In the **Welcome** screen, select **PortShield Interface Wizard**, and then click **Next**.
3. In the **Ports Assignment** screen, select **WAN/LAN/HA**, and then click **Next**.



Ports Assignment

Select the initial ports assignment for SonicWALL.

○ Use Current - Use this option to keep your current settings.

○ Basic WAN/LAN Switch

○ WAN/OPT/LAN Switch

● WAN/LAN/HA

○ WAN/LAN/LAN2 Switch

4. In the **SonicWALL Configuration Summary** screen, click **Apply**.

5. In the **PortShield Wizard Complete** screen, click **Close**.
6. Log into the management interface of the other appliance in the HA Pair, and repeat this procedure.

## Configuring HA Settings

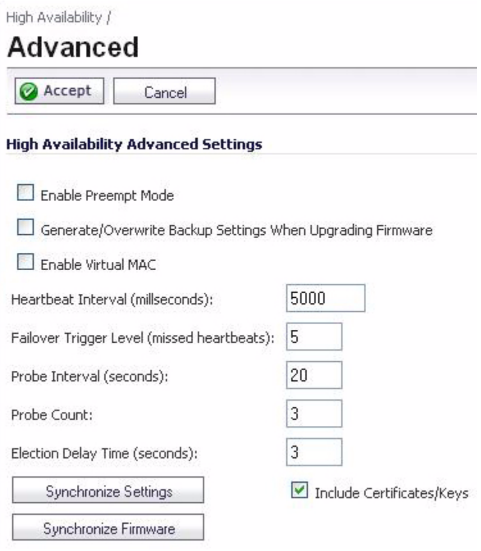
After disabling PortShield on all interfaces of both appliances, the next task in setting up HA is configuring the **High Availability** > **Settings** page on the Primary SonicWALL security appliance. Once you configure HA on the Primary, it communicates the settings to the Backup SonicWALL security appliance.

To configure HA on the Primary SonicWALL, perform the following steps:

1. Navigate to the **High Availability** > **Settings** page.
2. Select the **Enable High Availability** checkbox.
3. Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance.
   You can find the serial number on the back of the SonicWALL security appliance, or in the **System** > **Status** screen of the backup unit. The serial number for the Primary SonicWALL is automatically populated.
4. Click **Apply** to retain these settings.

## Configuring Advanced HA Settings

1. Navigate to the **High Availability** > **Advanced** page.



High Availability Advanced Settings

□ Enable Preempt Mode

□ Generate/Overwrite Backup Settings When Upgrading Firmware

□ Enable Virtual MAC

Heartbeat Interval (millseconds): 5000

Failover Trigger Level (missed heartbeats): 5

Probe Interval (seconds): 20

Probe Count: 3

Election Delay Time (seconds): 3

☑ Include Certificates/Keys

2. To configure the HA Pair so that the Primary SonicWALL resumes the Active role when coming back online after a failover, select **Enable Preempt Mode**.
3. To backup the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.

4. Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address.
5. The **Heartbeat Interval** controls how often the two units communicate. The default is 5000 milliseconds; the minimum supported value is 1000 milliseconds.
6. Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. By default, this is set to 5 missed heartbeats.
7. Set the **Probe Interval** to the interval in seconds between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This is used in logical monitoring. SonicWALL recommends that you set the interval for at least 5 seconds. The default is 20 seconds, and the allowed range is 5 to 255 seconds. You can set the Probe IP Address(es) on the **High Availability** > **Monitoring** screen.
8. Set the **Probe Count** to the number of consecutive probes before SonicOS Enhanced concludes that the network critical path is unavailable or the probe target is unreachable. This is used in logical monitoring. The default is 3, and the allowed range is 3 to 10.
9. The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role. The default is 3 seconds.
10. Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
11. You do not need to click **Synchronize Settings** at this time, because all settings will be automatically synchronized to the Idle unit when you click **Accept** after completing HA configuration. To synchronize all settings on the Active unit to the Idle unit immediately, click **Synchronize Settings**. The Idle unit will reboot.
12. Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Backup unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Backup appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
13. When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

## Configuring HA Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability.

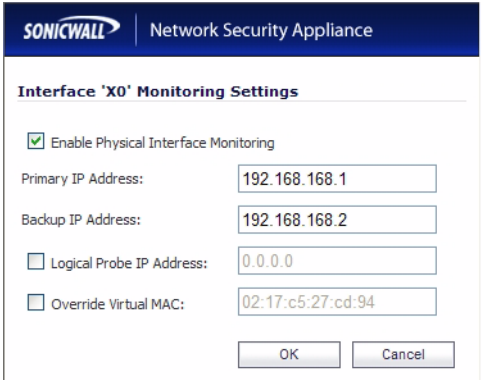
Logical monitoring involves configuring the SonicWALL to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Idle unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Backup IP addresses configured on this page are used for multiple purposes:

- As independent management addresses for each unit (only on X0 and X1 interfaces)
- To allow synchronization of licenses between the Idle unit and the SonicWALL licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring, perform the following steps on the Primary unit:

1. Navigate to the **High Availability** > **Monitoring** page.
2. Click the **Configure** icon for the **X0** interface.



Interface 'X0' Monitoring Settings

☑ Enable Physical Interface Monitoring

Primary IP Address: 192.168.168.1

Backup IP Address: 192.168.168.2

□ Logical Probe IP Address: 0.0.0.0

□ Override Virtual MAC: 02:17:c5:27:cd:94

3. To enable link detection between the designated HA interfaces on the Primary and Backup units, leave the **Enable Physical Interface Monitoring** checkbox selected.
4. In the **Primary IP Address** field, enter the unique LAN management IP address of the Primary unit.
5. In the **Backup IP Address** field, enter the unique LAN management IP address of the Backup unit.

6. In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.) The Primary and Backup appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the SonicWALL appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.

   The **Primary IP Address** and **Backup IP Address** fields must be configured with independent IP addresses on the **X0** interface (**X1** for probing on the WAN) to allow logical probing to function correctly.
7. SonicWALL recommends that you do not select **Override Virtual MAC**. When Virtual MAC is enabled, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.
8. Click **OK**.
9. To configure monitoring on any of the other interfaces, repeat the above steps.
10. When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

## Synchronizing Settings

Once you have configured the HA settings on the Primary SonicWALL security appliance, it will automatically synchronize the settings to the Backup unit, causing the Backup to reboot. You do not need to click the **Synchronize Settings** button. However, if you later choose to do a manual synchronization of settings, click the **Synchronize Settings** button. You will see a **HA Peer Firewall has been updated** notification at the bottom of the management interface page. Also note that the management interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that certificates, certificate revocation lists (CRL), and associated settings are synchronized between the Primary and Backup units. When local certificates are copied to the Backup unit, the associated private keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.

**Tip:** *A compromise between the convenience of synchronizing certificates and the added security of not synchronizing certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.*

### Verifying HA Functionality

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then trigger a test failover by logging into the Primary unit and powering it off. The Backup SonicWALL security appliance should quickly take over. After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

From your management workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet. Note that unless virtual MAC is enabled, the Backup SonicWALL will not assume the Ethernet MAC address.

Log into the Backup SonicWALL's unique LAN IP address. The management interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the management interface. If the Backup SonicWALL is active, you can use the shared IP address to log into it.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure correct configuration.

## Multiple ISP / WAN Failover and Load Balancing

WAN Failover and Load Balancing allows you to designate an interface as a Secondary or backup WAN port.

The secondary WAN port can be used as a backup if the primary WAN port is down and/or unavailable, or it can maintain a persistent connection for WAN port traffic to divide outbound traffic flows between the Primary fixed WAN port and the user-assigned Secondary WAN port.

This section contains the following subsections:

- Configuring Secondary WAN Interface - page 55
- Activating and Configuring WAN Failover - page 55
- Configuring WAN Interface Monitoring - page 56
- WAN Probe Monitoring Overview - page 56
- Configuring WAN Probe Monitoring - page 57

# Multiple ISP / WAN Failover and Load Balancing

In this scenario, the SonicWALL TZ 210 is configured in NAT/Route mode to operate as a network gateway with multiple Internet Service Providers (ISPs) to allow load balancing and/or failover. Typical zone assignments for this scenario are as follows:

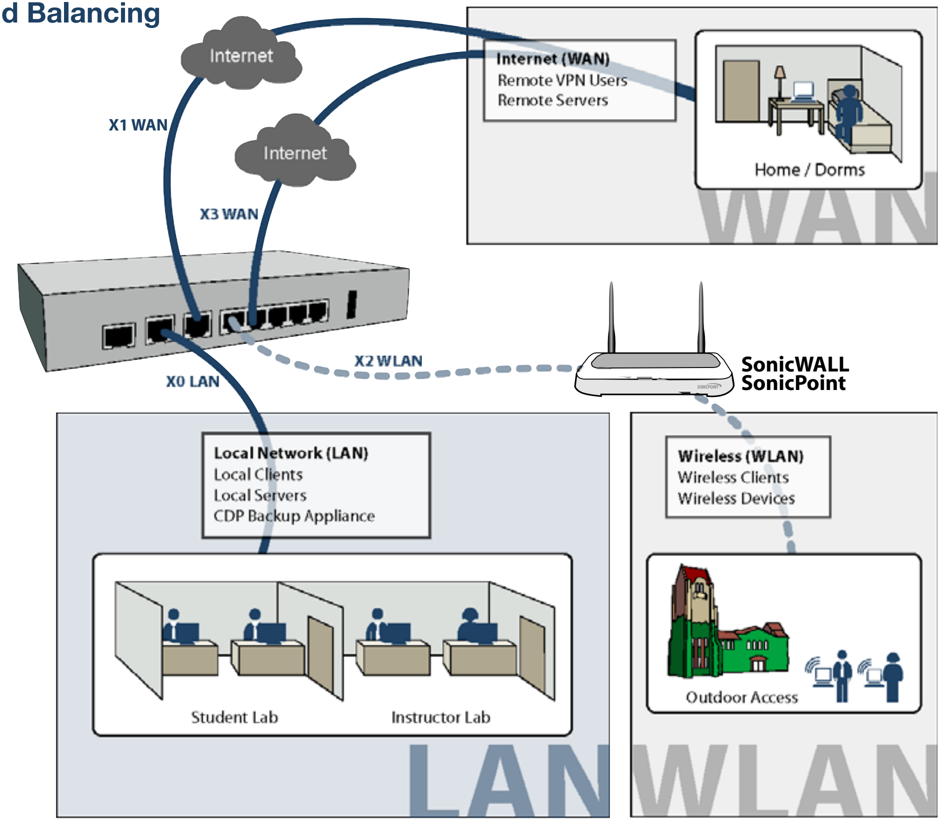
**Local Network (LAN)** - wired local client computers and servers

**Multiple Internet (WAN)** - two Internet service providers connected through X1 and a second open port (X3 in this case)

**DMZ** - (optional) wired resources available to public Internet such as Web servers and Mail servers

**Wireless (WLAN)*** - wireless local client computers and devices

*For the TZ 210 wired appliance, wireless is achieved by adding a SonicWALL SonicPoint appliance to any free interface (X4-X5) and zoning that interface as WLAN.



## Configuring Secondary WAN Interface

Perform the following steps to configure WAN Failover and Load Balancing on the SonicWALL security appliance:

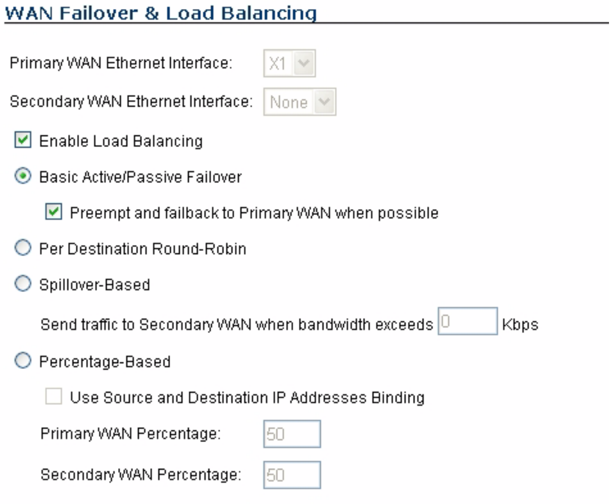
1. On **Network > Interfaces** page, configure the chosen port to be in WAN zone, and enter the correct address settings provided by the Secondary ISP.

**Note:** *In the example Multiple ISP / WAN Failover and Load Balancing section, on page 53, the SonicWALL security appliance is acquiring its secondary WAN address dynamically from ISP #2, using DHCP. Any interface added to the WAN zone by default creates a NAT policy allowing internal LAN subnets to enforce NAT on this Secondary WAN interface.*

## Activating and Configuring WAN Failover

To configure the SonicWALL for WAN failover and load balancing, follow the steps below:

1. On **Network > WAN Failover & LB** page, select **Enable Load Balancing**.
2. If there are multiple possible secondary WAN interfaces, select an interface from the **Secondary WAN Ethernet Interface**.



WAN Failover & Load Balancing

Primary WAN Ethernet Interface: X1

Secondary WAN Ethernet Interface: None

☑ Enable Load Balancing

● Basic Active/Passive Failover

☑ Preempt and failback to Primary WAN when possible

○ Per Destination Round-Robin

○ Spillover-Based

Send traffic to Secondary WAN when bandwidth exceeds 0 Kbps

○ Percentage-Based

□ Use Source and Destination IP Addresses Binding

Primary WAN Percentage: 50

Secondary WAN Percentage: 50

3. Select a load balancing method. By default, the SonicWALL will select **Basic Active/Passive Failover** as the method, but there are four load balancing methods available:

| | |
|---|---|
| **Basic Active/ Passive Failover** | Only sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. If the Primary WAN fails, then the SonicWALL security appliance reverts to this method. This mode will automatically return back to using the Primary WAN interface once it has been restored (preempt mode). |
| **Per Destination Round-Robin** | Load balances outgoing traffic on a per-destination basis. This is a simple load balancing method which allows you to utilize both links in a basic fashion (instead of the method above, which does not utilize the capability of the Secondary WAN until the Primary WAN has failed). |
| **Spillover-Based** | Allows you to control when and if the Secondary interface is used. You can specify when the SonicWALL security appliance starts sending traffic through the Secondary WAN interface. |
| **Percentage-Based** | Specifies the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces.<br>Optionally, enable **Source and Destination IP Address Binding**: Enables you to maintain a consistent mapping of traffic flows with a single outbound WAN interface, regardless of the percentage of traffic through that interface. |

## Configuring WAN Interface Monitoring

Under the **WAN Interface Monitoring** heading, you can customize how the SonicWALL security appliance monitors the WAN interface:

1. Enter a number between 5 and 300, in the **Check Interface Every _ Seconds** field. The default value is **5** seconds.
2. In the **Deactivate Interface after _ missed intervals**, enter a number between 1 and 10. The default value is **3**, which means the interface is considered inactive after 3 consecutive unsuccessful attempts.
3. Enter a number between 1 and 100 in the **Reactivate Interface after _ successful intervals**. The default value is 3, which means the interface is considered active after 3 consecutive successful attempts.

## WAN Probe Monitoring Overview

If Probe Monitoring is not activated, the SonicWALL security appliance performs physical monitoring only on the Primary and Secondary WAN interfaces, meaning it only marks a WAN interface as failed if the interface is disconnected or stops receiving an Ethernet-layer signal. This is not an assured means of link monitoring, because it does not address most failure scenarios (for example, routing issues with your ISP or an upstream router that is no longer passing traffic). If the WAN interface is connected to a hub or switch, and the router providing the connection to the ISP (also connected to this hub or switch) were to fail, the SonicWALL will continue to believe the WAN link is usable, because the connection to the hub or switch is good.

Enabling probe monitoring on the **Network > WAN Failover & Load Balancing** page instructs the SonicWALL security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable.

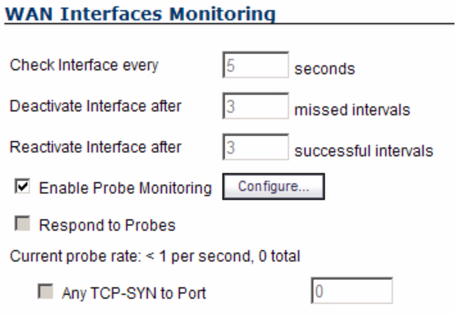
Under the default probe monitoring configuration, the SonicWALL performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther upstream. If your ISP is experiencing problems in its routing infrastructure, a successful ICMP ping of their router causes the SonicWALL security appliance to believe the line is usable, when in fact it may not be able to pass traffic to and from the public Internet at all.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port.

## Configuring WAN Probe Monitoring

To configure WAN probe monitoring, follow these steps:

1. On the **Network > WAN Failover & Load Balancing** page, under the **WAN Interface Monitoring** heading, select the **Enable Probe Monitoring** checkbox.



WAN Interfaces Monitoring

Check Interface every 5 seconds

Deactivate Interface after 3 missed intervals

Reactivate Interface after 3 successful intervals

☑ Enable Probe Monitoring

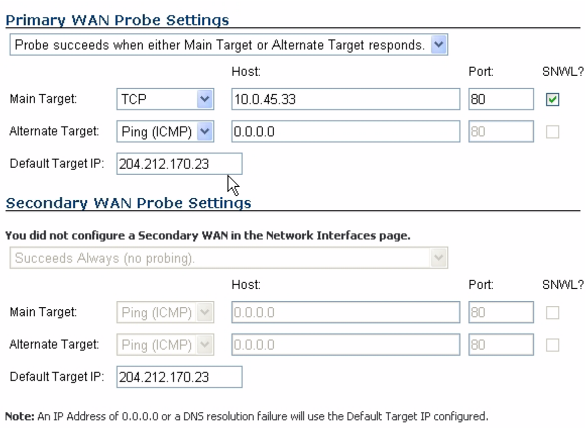
□ Respond to Probes

Current probe rate: < 1 per second, 0 total

□ Any TCP-SYN to Port 0

2. Select the **Respond to Probes** checkbox to have the SonicWALL security appliance respond to SonicwALL TCP probes received on any of its WAN ports. Do not select this checkbox if the SonicWALL security appliance should not respond to TCP probes.
3. Select the **Any TCP-SYN to Port** checkbox to instruct the SonicWALL security appliance to respond to TCP probes to the specified port number without validating them first. The **Any TCP-SYN to Port** box should only be selected when receiving TCP probes from SonicWALL security appliances running SonicOS Standard or older, legacy SonicWALL security appliances.

4. If there is a NAT device between the two appliances sending and receiving TCP probes, the **Any TCP-SYN to Port** checkbox must be selected, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.
5. Click on the **Configure** button. The **Configure WAN Probe Monitoring** window is displayed.
6. In the **Primary WAN Probe Settings** menu, select one of the following options:
    - Probe succeeds when either Main Target or Alternate Target responds
    - Probe succeeds when both Main Target and Alternative Target respond
    - Probe succeeds when Main Target responds
    - Succeeds Always (no probing)
7. Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.
8. Enter the host name or IP address of the target device in the **Host** field.
9. Enter a port number in the **Port** field.
10. If there is a NAT device between the two devices sending and receiving TCP probes, the **Any TCP-SYN to Port** checkbox must be selected, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.
11. Select the **SNWL?** checkbox if the target device is a SonicWALL security appliance. Do not select the **SNWL?** box for third-party devices, as the TCP probes may not work consistently.



Primary WAN Probe Settings

Probe succeeds when either Main Target or Alternate Target responds.

| | | Host: | Port: | SNWL? |
|---|---|---|---|---|
| Main Target: | TCP | 10.0.45.33 | 80 | ☑ |
| Alternate Target: | Ping (ICMP) | 0.0.0.0 | 80 | ☐ |
| Default Target IP: | 204.212.170.23 | | | |

Secondary WAN Probe Settings

You did not configure a Secondary WAN in the Network Interfaces page.

Succeeds Always (no probing).

| | | Host: | Port: | SNWL? |
|---|---|---|---|---|
| Main Target: | Ping (ICMP) | 0.0.0.0 | 80 | ☐ |
| Alternate Target: | Ping (ICMP) | 0.0.0.0 | 80 | ☐ |
| Default Target IP: | 204.212.170.23 | | | |

**Note:** An IP Address of 0.0.0.0 or a DNS resolution failure will use the Default Target IP configured.

12. Optionally, you can enter a default target IP address in the **Default Target IP** field. In case of a DNS failure when a host name is specified, the default target IP address is used.
13. An IP address of 0.0.0.0 or a DNS resolution failure will use the Default Target IP configured. If 0.0.0.0 is entered and no default target IP address is configured, the default gateway on that interface will be used.
14. Configure the **Secondary WAN Probe Settings**, which provide the same options as the **Primary WAN Probe Settings**.
15. Click **OK**.

# Support and Training Options 6

## In this Section:

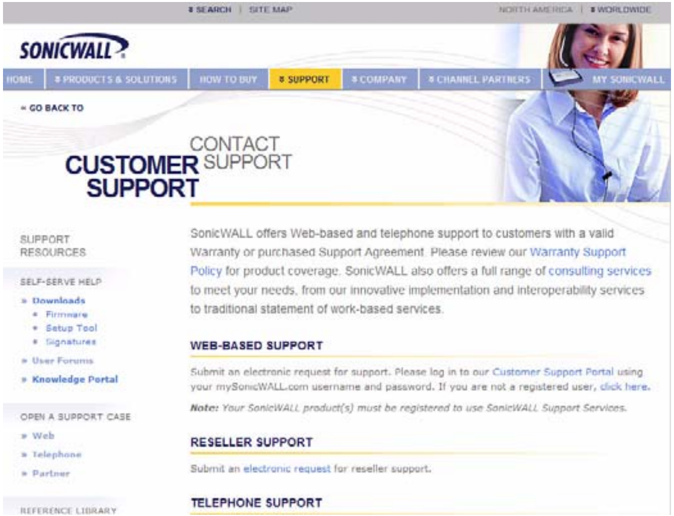
This section provides overviews of customer support and training options for the SonicWALL TZ 210 series appliances.

- Customer Support - page 60
- Knowledge Portal - page 60
- Onboard Help - page 61
- SonicWALL Live Product Demos - page 61
- User Forums - page 62
- Training - page 63
- Related Documentation - page 64
- SonicWALL Secure Wireless Network Integrated Solutions Guide - page 65

# 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>



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.

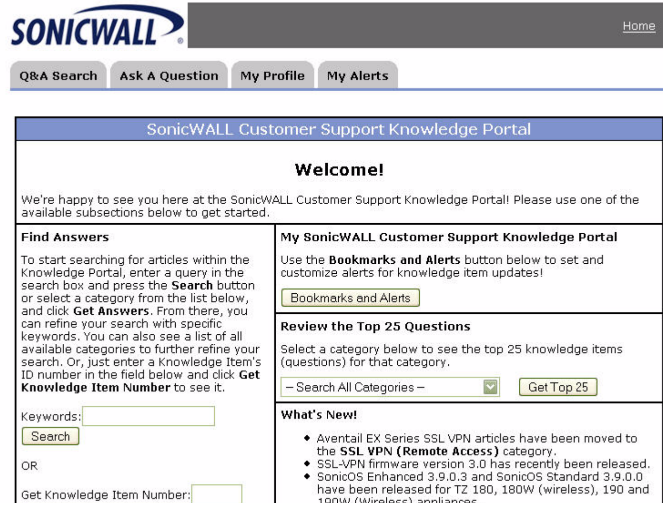
**TELEPHONE SUPPORT**

# 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:

Search

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!

Bookmarks and Alerts

**Review the Top 25 Questions**

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

– Search All Categories –

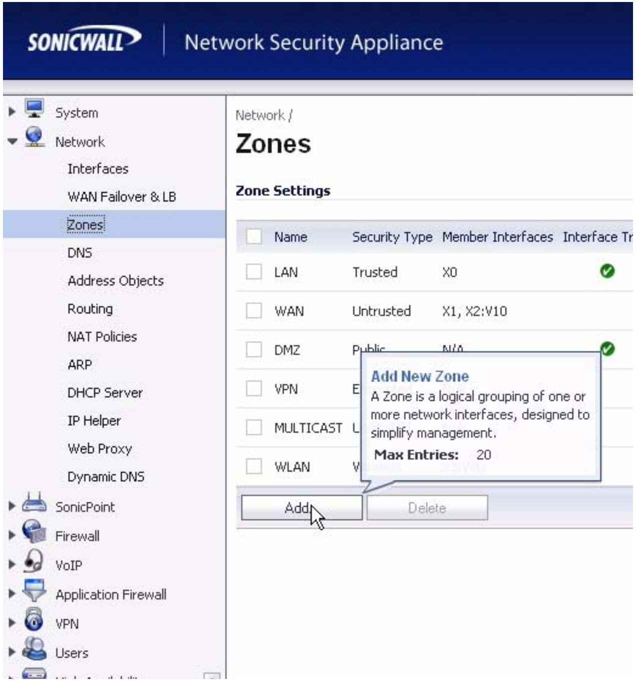
Get Top 25

**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 | W | | |

Add New Zone

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

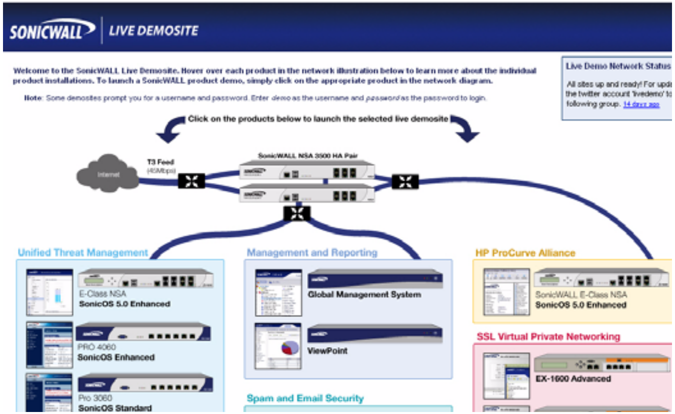
**Max Entries:** 20

## 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/>



Welcome to the SonicWALL Live Demosite. Hover over each product in the network illustration below to learn more about the individual product installations. To launch a SonicWALL product demo, simply click on the appropriate product in the network diagram.

Note: Some demosites prompt you for a username and password. Enter *demo* as the username and *password* as the password to login.

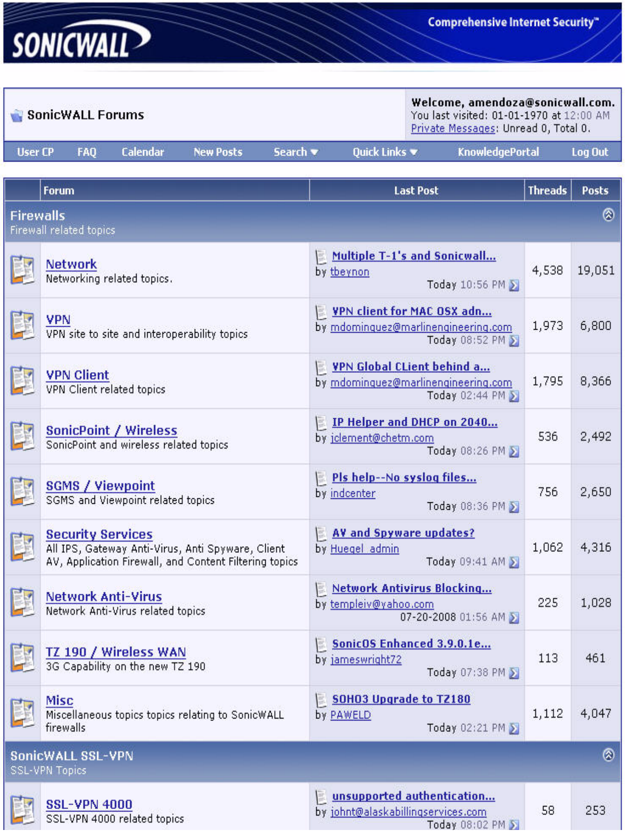
All sites up and ready! For upd
the twitter account 'livedemo' to
following group. 14 days ago

# 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 210 / 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.

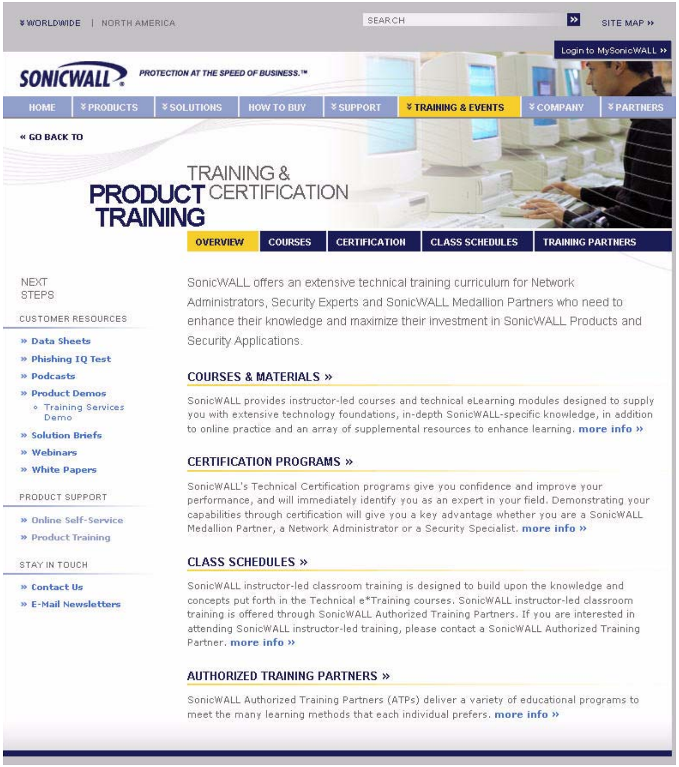
| Forum | Last Post | Threads | Posts |
|---|---|---|---|
| **Firewalls**<br>Firewall related topics | | | |
| Network<br>Networking related topics. | Multiple T-1's and Sonicwall...<br>by tbeynon<br>Today 10:56 PM | 4,538 | 19,051 |
| VPN<br>VPN site to site and interoperability topics | VPN client for MAC OSX adn...<br>by mdominguez@marlinengineering.com<br>Today 08:52 PM | 1,973 | 6,800 |
| VPN Client<br>VPN Client related topics | VPN Global CLient behind a...<br>by mdominguez@marlinengineering.com<br>Today 02:44 PM | 1,795 | 8,366 |
| SonicPoint / Wireless<br>SonicPoint and wireless related topics | IP Helper and DHCP on 2040...<br>by jclement@chetm.com<br>Today 08:26 PM | 536 | 2,492 |
| SGMS / Viewpoint<br>SGMS and Viewpoint related topics | Pls help--No syslog files...<br>by indcenter<br>Today 08:36 PM | 756 | 2,650 |
| Security Services<br>All IPS, Gateway Anti-Virus, Anti Spyware, Client AV, Application Firewall, and Content Filtering topics | AV and Spyware updates?<br>by Huegel_admin<br>Today 09:41 AM | 1,062 | 4,316 |
| Network Anti-Virus<br>Network Anti-Virus related topics | Network Antivirus Blocking...<br>by templeiv@yahoo.com<br>07-20-2008 01:56 AM | 225 | 1,028 |
| TZ 190 / Wireless WAN<br>3G Capability on the new TZ 190 | SonicOS Enhanced 3.9.0.1e...<br>by jameswright72<br>Today 07:38 PM | 113 | 461 |
| Misc<br>Miscellaneous topics topics relating to SonicWALL firewalls | SOHO3 Upgrade to TZ180<br>by PAWELD<br>Today 02:21 PM | 1,112 | 4,047 |
| **SonicWALL SSL-VPN**<br>SSL-VPN Topics | | | |
| SSL-VPN 4000<br>SSL-VPN 4000 related topics | unsupported authentication...<br>by johnt@alaskabillingservices.com<br>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>



PRODUCT TRAINING

TRAINING & CERTIFICATION

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 »

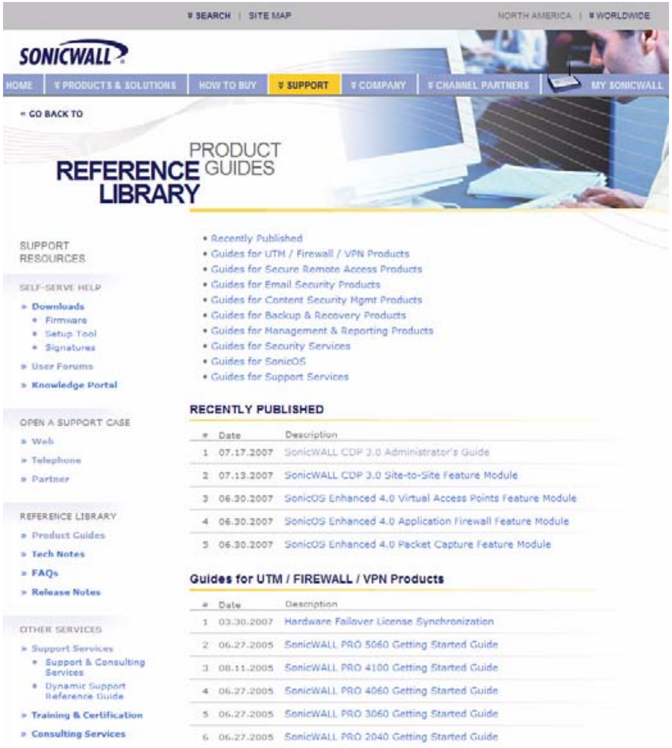
SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. more info »

# 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 |

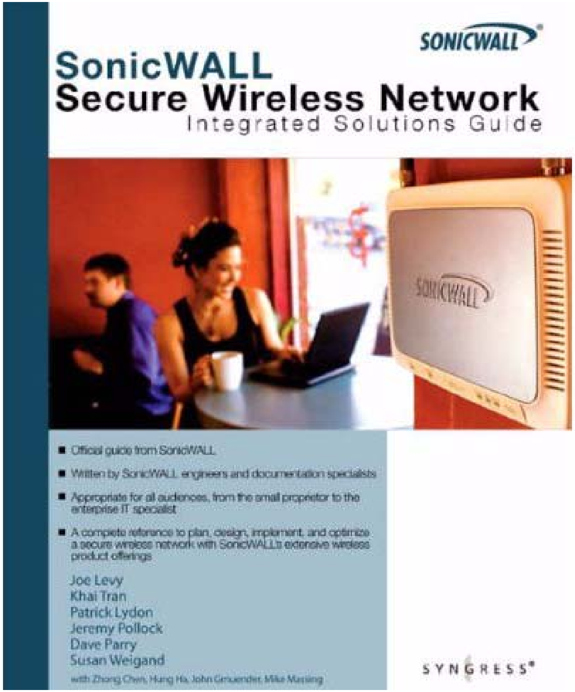
Guides for UTM / FIREWALL / VPN Products

| # | 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

# Product Safety and Regulatory Information 7

## In this Section:

This section provides regulatory, trademark, and copyright information.

- Safety and Regulatory Information for the SonicWALL TZ 210 Appliance - page 68
- Safety and Regulatory Information in German for the SonicWALL TZ 210 Appliance - page 69
- FCC Part 15 Class B Notice for the SonicWALL TZ 210 Appliance - page 70
- Safety and Regulatory Information for the SonicWALL TZ 210 Wireless Appliance - page 71
- Safety and Regulatory Information in German for the SonicWALL TZ 210 Wireless Appliance - page 72
- FCC Part 15 Class B Notice for the SonicWALL TZ 210 Wireless Appliance - page 73
- FCC RF Radiation Exposure Statement - page 73
- Copyright Notice - page 75
- Trademarks - page 75

# Safety and Regulatory Information for the SonicWALL TZ 210 Appliance

| Regulatory Model/Type | Product Name |
|---|---|
| APL20-063 | TZ 210 |

## Mounting the SonicWALL

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º 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 (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.

## Lithium Battery Warning

The Lithium Battery used in the SonicWALL security appliance may not be replaced by the user. Return the SonicWALL security appliance to a SonicWALL-authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL security 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.

## Power Supply Information

If the power supply is missing from your SonicWALL product package, please contact SonicWALL Technical Support at 408-752-7819 for a replacement. This product should only be used with a UL listed power supply marked “Class 2” or “LPS”, with an output rated 12 VDC, minimum 1.66 A.

# Safety and Regulatory Information in German for the SonicWALL TZ 210 Appliance

## Weitere Hinweise zur Montage

- 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.
- Führen Sie die Kabel nicht entlang von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern.
- Das beigefügte Netzkabel ist nur für den Betrieb in Nordamerika vergesehen. Für Kunden in der Europäischen Union ist kein Kabel beigefügt.
- 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.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist.

## 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 herausgeführt werden, in dem sich das Gerät befindet.

## Informationen zur Stromversorgung

Sollte das Netzteil nicht im Lieferumfang der SonicWALL enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von SonicWALL (Tel.: +1-408-752-7819). Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet" zugelassenen Netzteil der Kategorie „Class 2" oder „LPS" verwendet werden. Ausgang: 12 VDC Gleichsspannung, mind. 1,66 A.

# FCC Part 15 Class B Notice for the SonicWALL TZ 210 Appliance

NOTE: This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. And, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from the receiver connection.
- Consult SonicWALL for assistance.

Complies with EN55022 Class B and CISPR22 Class B.
*Refer to the label on the bottom of the unit for device information including Class A or Class B FCC information.

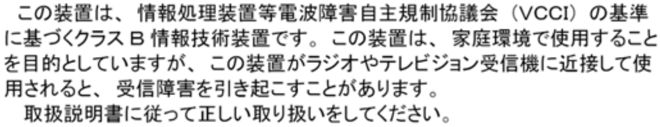
## Canadian Radio Frequency Emissions Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## 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 B<br>EN 55024 (1998) +A2<br>EN 61000-3-2 (2006)<br>EN 61000-3-3 (1995) +A2<br>EN 60950-1 (2001) +A11<br>National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI |

## VCCI Statement



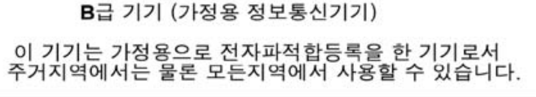
この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをしてください。

## Regulatory Information for Korea

| | |
|---|---|
| 방송통신위원회 | Ministry of Information and Telecommunication Certification Number |

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.



B급 기기 (가정용 정보통신기기)

이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든지역에서 사용할 수 있습니다.

# Safety and Regulatory Information for the SonicWALL TZ 210 Wireless Appliance

| Regulatory Model/Type | Product Name |
|---|---|
| APL20-065 | TZ 210 Wireless, TZ 210 W |
| APL20-064 | TZ 210 Wireless, TZ 210 W |

## Mounting the SonicWALL

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º 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 (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of over-loading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.

## Lithium Battery Warning

The Lithium Battery used in the SonicWALL security appliance may not be replaced by the user. Return the SonicWALL security appliance to a SonicWALL-authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL security 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.

## Power Supply Information

If the power supply is missing from your SonicWALL product package, please contact SonicWALL Technical Support at 408-752-7819 for a replacement. This product should only be used with a UL listed power supply marked “Class 2” or “LPS”, with an output rated 12 VDC, minimum 1.66 A.

# Safety and Regulatory Information in German for the SonicWALL TZ 210 Wireless Appliance

## Weitere Hinweise zur Montage

- 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.
- Führen Sie die Kabel nicht entlang von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern.
- Das beigefügte Netzkabel ist nur für den Betrieb in Nordamerika vergesehen. Für Kunden in der Europäischen Union ist kein Kabel beigefügt.
- 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.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist.

## 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 herausgeführt werden, in dem sich das Gerät befindet.

## Informationen zur Stromversorgung

Sollte das Netzteil nicht im Lieferumfang der SonicWALL enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von SonicWALL (Tel.: +1-408-752-7819). Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet“ zugelassenen Netzteil der Kategorie „Class 2“ oder „LPS“ verwendet werden. Ausgang: 12 VDC Gleichsspannung, mind. 1,66 A.

# FCC Part 15 Class B Notice for the SonicWALL TZ 210 Wireless Appliance

NOTE: This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. And, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from the receiver connection.
- Consult SonicWALL for assistance.

Complies with EN55022 Class B and CISPR22 Class B.
*Refer to the label on the bottom of the unit for device information including Class A or Class B FCC information.

**FCC Caution**: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

## FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (7.9 inches) between the radiator (antenna) and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. For more information regarding the above statement, please contact SonicWALL, Inc. at:

1143 Borregas Avenue
Sunnyvale, CA, 94089-1306
1-408-745-9600

## North American Authorized Channels

SonicWALL declares that the APL20-065 (FCC ID: QWU-06C) (IC: 4408A-06C) and APL20-064 (FCC ID: QWU-06D) (IC: 4408A-06D) when sold in US or Canada is limited to CH1~CH11 by specified firmware controlled in the USA.

## Canadian Radio Frequency Emissions Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

# Declaration of Conformity

## Certificate #: EU00165-A

| | |
|---|---|
| Application of council Directive | 2004/108/EC (EMC)<br>2006/95/EC (LVD)<br>1999/5/EC (R&TTE) |
| Standard(s) to which conformity is declared | EN 55022 (1998) +A1 +A2 Class B<br>EN 55024 (1998) +A2 +A2<br>EN 61000-3-2 (2000) +A2<br>EN 61000-3-3 (1995) A2<br>EN 60950-1 (2001) +A11<br>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<br>EN 300 328-1/-2 (2003)<br>EN 301 489-1/-17 (2002)<br>EN50385 : (2002) |
| Manufacturer/ Responsible Party | SonicWALL, Inc.<br>1143 Borregas Avenue<br>Sunnyvale, CA 94089 USA |
| Type of Equipment | Information Technology Equipment<br>Internet Security (Firewall/VPN) Appliance, with 802.11b/g/n  Wireless Router Tabletop with external power supply. |
| Type Numbers | APL20-065, APL20-064 |
| May be Marketed as | TZ 210 Wireless, TZ 210 W |

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards. Quality control procedures will ensure series production of equipment will be compliant.

| | |
|---|---|
| **Signature** /s/  John Gmuender<br>V.P. Engineering | **Date** 10/22/08 |

SonicWALL tímto prohlašuje, že tento APL20-065/APL20-064 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

Undertegnede SonicWALL erklærer herved, at følgende udstyr APL20-065/APL20-064 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

Hiermit erklärt SonicWALL, dass sich das Gerät APL20-065/APL20-064 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Käesolevaga kinnitab SonicWALL seadme APL20-065/APL20-064 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Hereby, SonicWALL, declares that this APL20-065/APL20-064 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Por medio de la presente SonicWALL declara que el APL20-065/APL20-064 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ SonicWALL ΔΗΛΩΝΕΙ ΟΤΙ APL20-065/APL20-064 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Par la présente SonicWALL déclare que l'appareil APL20-065/APL20-064 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Con la presente SonicWALL dichiara che questo APL20-065/APL20-064 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Ar šo  SonicWALL deklarē, ka APL20-065/APL20-064 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Šiuo SonicWALL deklaruoja, kad šis APL20-065/APL20-064 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Hierbij verklaart SonicWALL dat het toestel APL20-065/APL20-064 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Hawnhekk, SonicWALL, jiddikjara li dan APL20-065/APL20-064 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Alulírott, SonicWALL nyilatkozom, hogy a APL20-065/APL20-064 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

Niniejszym SonicWALL oświadcza, że APL20-065/APL20-064 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

SonicWALL declara que este APL20-065/APL20-064 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

SonicWALL izjavlja, da je ta APL20-065/APL20-064 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

SonicWALL týmto vyhlasuje, že APL20-065/APL20-064 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

SonicWALL vakuuttaa täten että APL20-065/APL20-064 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Härmed intygar SonicWALL att denna APL20-065/APL20-064 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

# Copyright Notice

© 2008 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 98, Windows Vista, Windows 2000, Windows XP, Windows Server 2003, 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.

# Notes

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

P/N 232-001620-50
Rev A 11/08