

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: 0017CS88E1C
 Registration Code: T2HT98NH
 Authentication Code: 6R0FA-DHLM
 Trusted: Yes
 Registered On: 10 Nov 2008

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

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

My TZ 210 [RENAME] [TRANSFER] [DELETE]

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 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: [001ZCS88E1C](#)
 Activation Status: Enabled
 Expiration Date: 10 Dec 2008

[BACK](#)

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:

[BUY](#)

[SUBMIT](#)

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		Security Services	
Model:	TZ 210	Service Name	Status
Product Code:	6800	Nodes/Users	Licensed - Unlimited Nodes
Serial Number:	0617CS28EE1C	VPN	Licensed
Authentication Code:	6RCH-DHAM	Global VPN Client	Licensed - 1 License (0 in Use)
Firmware Version:	SonicOS Enhanced 5.1.3.0-210	CPS (Content Filter)	Licensed
Safemode Version:	Safemode 5.0.1.13	Client AV Enforcement	Licensed
ROM Version:	SonicROM 5.0.2.11	Gateway Anti-Virus	Licensed
CPU:	0.50% - 500 MHz; Mips64 Octeon Processor	Anti-Spyware	Licensed
Total Memory:	256 MB RAM, 32 MB Flash	Intrusion Prevention	Licensed
System Time:	11/10/2008 16:04:20	NetPoint	Not Licensed
Up Time:	2 Days 20:59:36		
Connections:	33		
Last Modified By:	192.168.168.62:30 11/10/2008 15:03:47		
Registration Code:	TZHT18NH		

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:

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

For Free Trials, click here.

Enabling Gateway Anti-Virus

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

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

Security Services / Gateway Anti-Virus

Accept

Gateway Anti-Virus Status

Gateway Anti-Virus Status

Signature Database: Downloaded

Signature Database Timestamp: UTC 11/07/2008 14:37:07.000

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enable Outbound Inspection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Protocol 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** button to apply changes.

GAV contains many other useful features, including:

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



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

Enabling Intrusion Prevention Services

To enable Intrusion Prevention (IPS) in SonicOS:

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

Security Services /
Intrusion Prevention

Accept

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

Notes: 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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Medium Priority Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Low Priority Attacks	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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** 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

Anti-Spyware Status

Anti-Spyware Status

Signature Database: Downloaded

Signature Database Timestamp: UTC 11/10/2008 13:01:59.000 Update

Last Checked: 11/11/2008 18:13:53.320

Anti-Spyware Expiration Date: 12/10/2008

Notes: 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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Medium Danger Level Spyware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Low Danger Level Spyware	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

Configure Anti-Spyware Settings Reset Anti-Spyware Settings & Policies

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**  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.



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**  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.

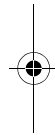
<input type="checkbox"/>	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
<input checked="" type="checkbox"/>	LAN	Trusted	X0, X2, X3, X4, X5, X6								
<input type="checkbox"/>	WAN	Untrusted	X1								
<input type="checkbox"/>	DMZ	Public	N/A								
<input type="checkbox"/>	VPN	Encrypted	N/A								
<input type="checkbox"/>	MULTICAST	Untrusted	N/A								
<input type="checkbox"/>	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.

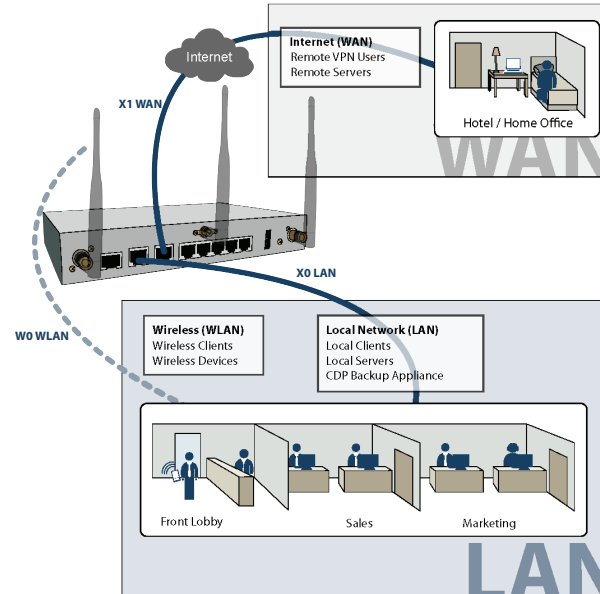
WLAN—Local wireless network resources originating from SonicWALL wireless enabled appliances.

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.

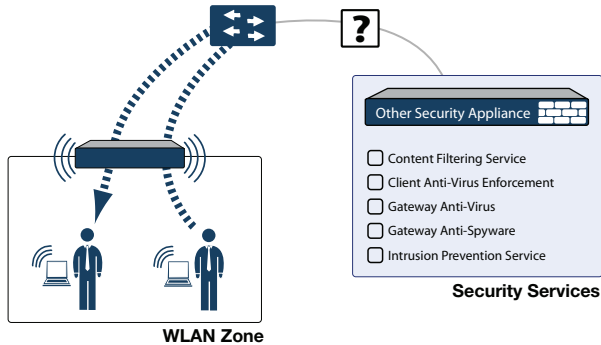
The X1 and X0 interfaces are preconfigured as WAN and LAN respectively. The remaining ports (X2-X6) are also LAN ports by default, however, these ports can be configured to meet the needs of your network, either by using basic zone types (WAN, LAN, WLAN, DMZ, VPN) or configuring a custom zone type to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



SonicWALL Wireless Firewalling

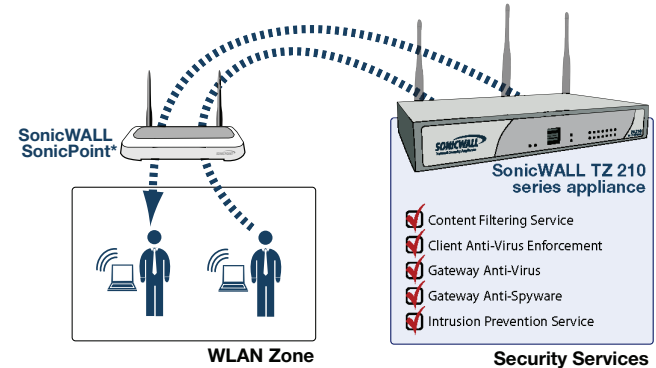
When a wireless device uses an access point to communicate with a device on another subnet or on a completely different network, traffic between the devices is forced to traverse the network gateway. This traversal enables Unified Threat Management (UTM) services to be enforced at the gateway.

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.



*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:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Ping <input type="checkbox"/> SNMP <input type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input type="checkbox"/> 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 X1: WAN	Connect any local network device to X0, or X2-X6 for local and Internet connectivity.
WAN/LAN/DMZ	X0, X3-X6: LAN X1: WAN X2: DMZ	Connect any local network device to X0, or X3-X6 for local and Internet connectivity. 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:

Port Enable:

PortShield Interface:

Link Speed:

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
<input type="checkbox"/> 1	1	Any	All X1 Management IP	192.168.169.1 Server Services	Allow	All		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	2	Any	X1 IP	ubuntu Services	Allow	All		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 3	3	Any	Any	Any	Deny	All		<input checked="" type="checkbox"/>	

Add... Delete Restore Defaults...

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.

The screenshot shows the 'Add Rule' configuration page with the 'General' tab selected. The 'Settings' section includes the following fields:

- Action:** Radio buttons for Allow (selected), Deny, and Discard.
- From Zone:** Dropdown menu with 'WAN' selected.
- To Zone:** Dropdown menu with 'LAN' selected.
- Service:** Dropdown menu with '--Select a service--' selected.
- Source:** Dropdown menu with '--Select a network--' selected.
- Destination:** Dropdown menu with '--Select a network--' selected.
- Users Allowed:** Dropdown menu with 'All' selected.
- Schedule:** Dropdown menu with 'Always on' selected.
- Comment:** Text input field containing 'Ready'.
- Enable Logging**
- Allow Fragmented Packets**

At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

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.

The screenshot shows a configuration window with three tabs: 'General', 'Advanced', and 'QoS'. The 'Advanced' tab is selected. Below the tabs, the 'Advanced Settings' section is displayed. It contains three input fields: 'TCP Connection Inactivity Timeout (minutes)' with the value '15', 'UDP Connection Inactivity Timeout (seconds)' with the value '30', and 'Number of connections allowed (% of maximum connections)' with the value '100'. At the bottom of this section, there is a checkbox labeled 'Create a reflexive rule' which is currently unchecked.

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:

Type:

IP Address:

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

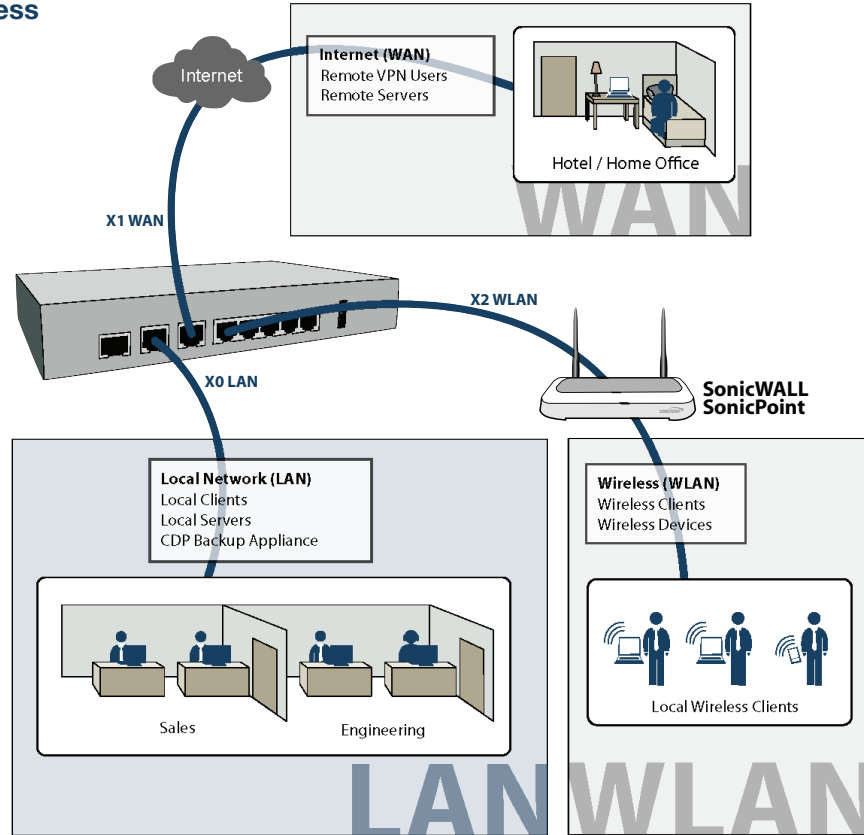
In this deployment, the SonicWALL TZ 210 is configured to operate as a network gateway with the following zones:

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.

- 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 :

Country Code:

- 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

SSID:

Radio Mode:

Channel:

ACL Enforcement Enable MAC Filter List

Allow List:

Deny List:

WEP/WPA Encryption

Authentication Type:

Cipher Type:

Group Key Interval:

Passphrase:

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:

Security Type:

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:

SSL-VPN service:

WiFiSec Enforcement

WiFiSec Exception Service:

Require WiFiSec for Site-to-Site VPN Tunnel Traversal

Trust WPA / WPA2 traffic as WiFiSec

SonicPoint Settings

SonicPoint Provisioning Profile:

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:	<input type="text" value="WLAN"/>
IP Address:	<input type="text" value="10.10.50.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
SonicPoint Limit:	<input type="text" value="4 SonicPoints"/>
Comment:	<input type="text" value="SonicPoints"/>
Management:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Ping <input type="checkbox"/> SNMP <input type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input type="checkbox"/> 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:

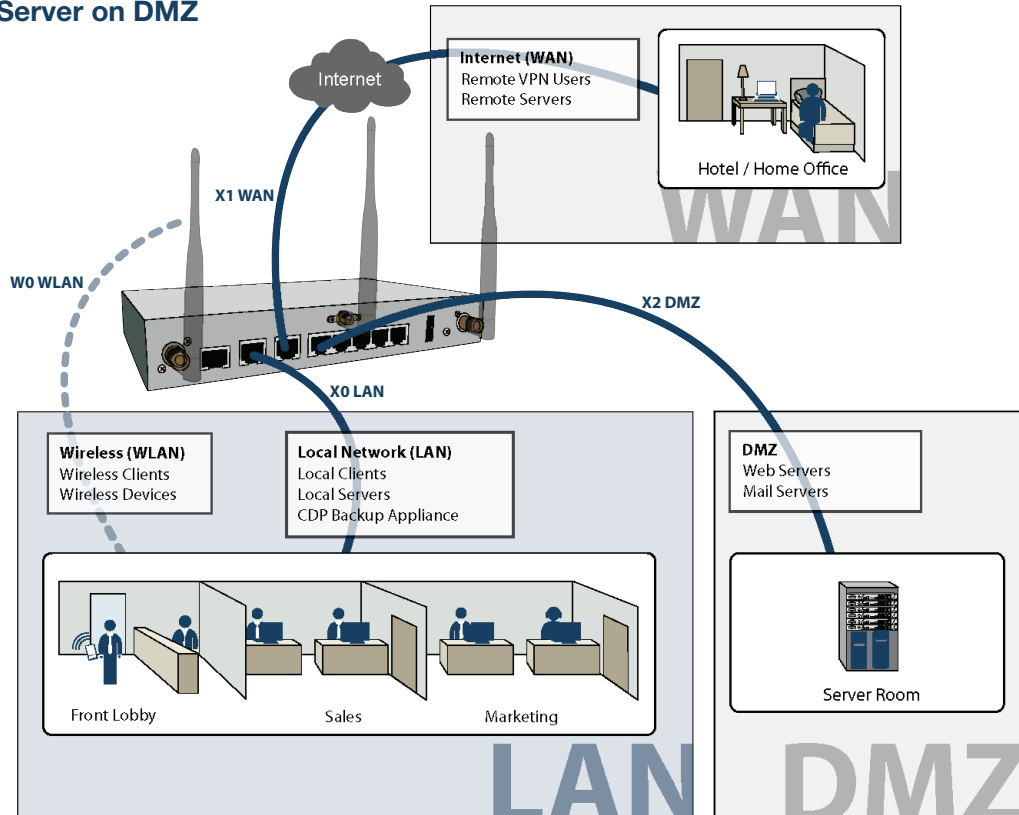
Local Network (LAN) - wired local client computers and servers

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**.

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:	<input type="text" value="DMZ"/>
IP Assignment:	<input type="text" value="Static"/>
IP Address:	<input type="text" value="192.168.168.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Comment:	<input type="text"/>
Management:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Ping <input type="checkbox"/> SNMP <input type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input type="checkbox"/> 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:	<input type="text" value="My Web Server Private"/>
Zone Assignment:	<input type="text" value="DMZ"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text" value="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.

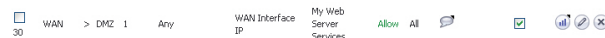


4. On the **Firewall > Access Rules** page, click the **Add** button. The **Add Rule** window displays.
5. Configure the new rule as follows:

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:



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

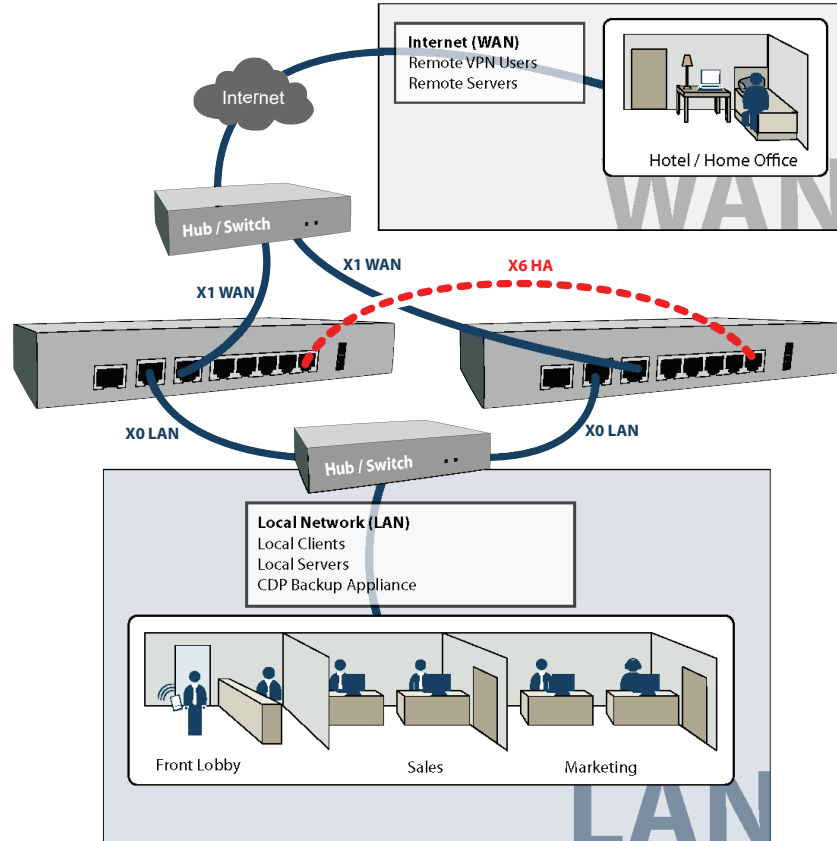
High-Availability Mode

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:

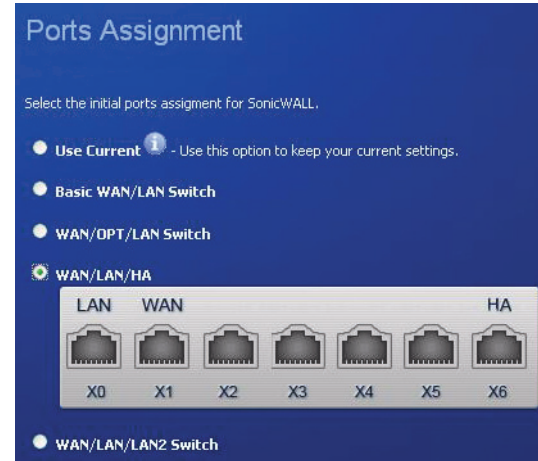
1. Login to MySonicWALL and click **My Products**.
2. On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or primary, unit. Click the product **name** or **serial number**.
3. On the Service Management page, scroll down to the Associated 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**.



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

Accept Cancel

High Availability Advanced Settings

Enable Preempt Mode

Generate/Overwrite Backup Settings When Upgrading Firmware

Enable Virtual MAC

Heartbeat Interval (milliseconds):

Failover Trigger Level (missed heartbeats):

Probe Interval (seconds):

Probe Count:

Election Delay Time (seconds):

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**.