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.

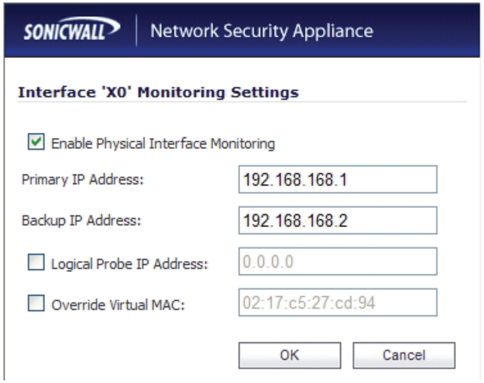
Logical monitoring involves configuring the SonicWALL to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Idle unit. If neither unit in the HA Pair can connect to the 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:

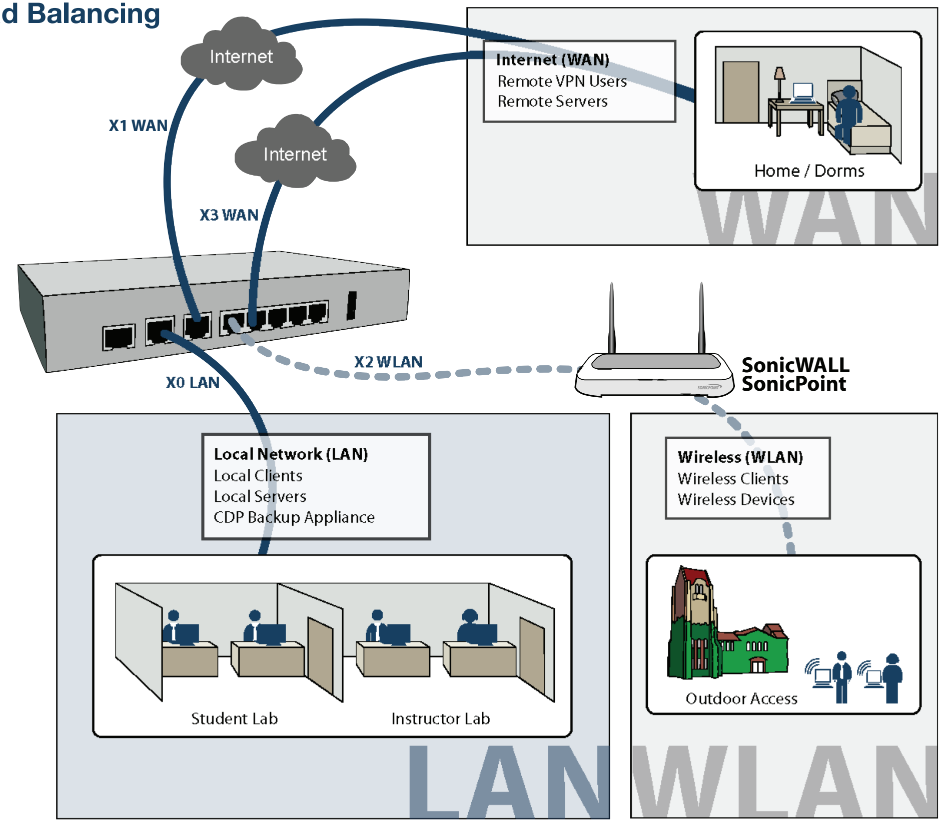
Local Network (LAN) - wired local client computers and servers

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:

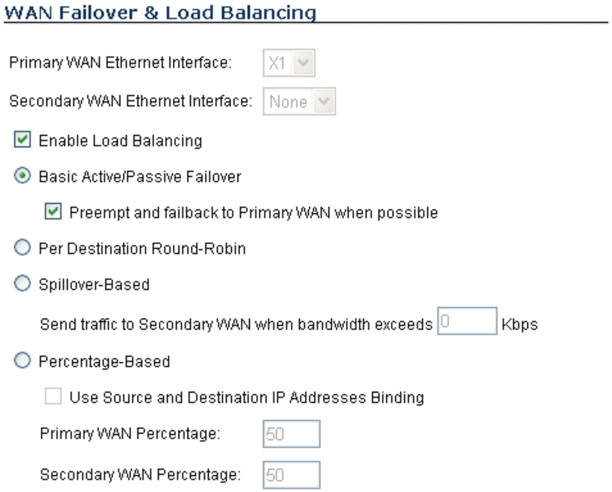
1. On **Network > Interfaces** page, configure the chosen port to be in WAN zone, and enter the correct address settings provided by the Secondary ISP.

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. 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.

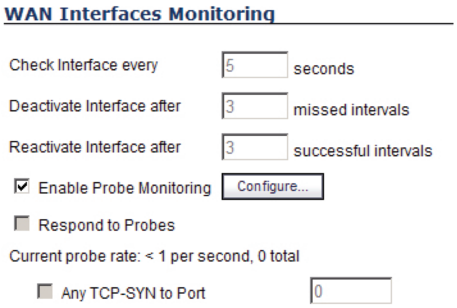
Under the default probe monitoring configuration, the SonicWALL performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther upstream. If your ISP is experiencing problems in 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

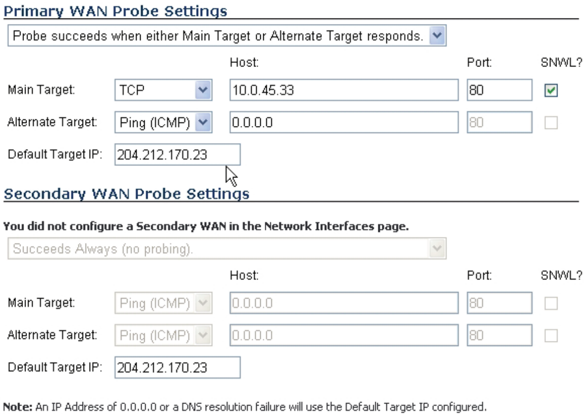
☐ Respond to Probes

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:

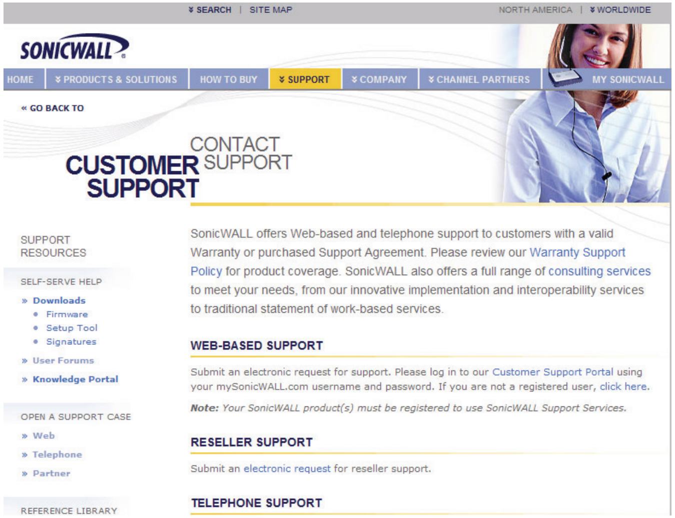
This section provides overviews of customer support and training options for the SonicWALL TZ 210 series appliances.

- 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.

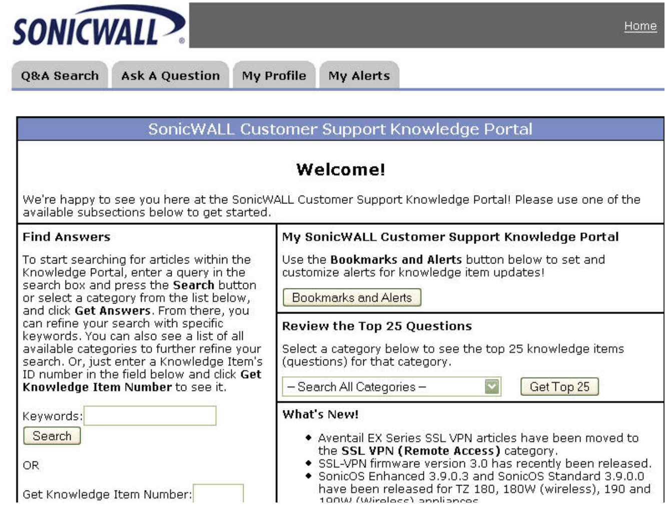
TELEPHONE SUPPORT

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:

OR

Get Knowledge Item Number:

My SonicWALL Customer Support Knowledge Portal

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

Review the Top 25 Questions

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

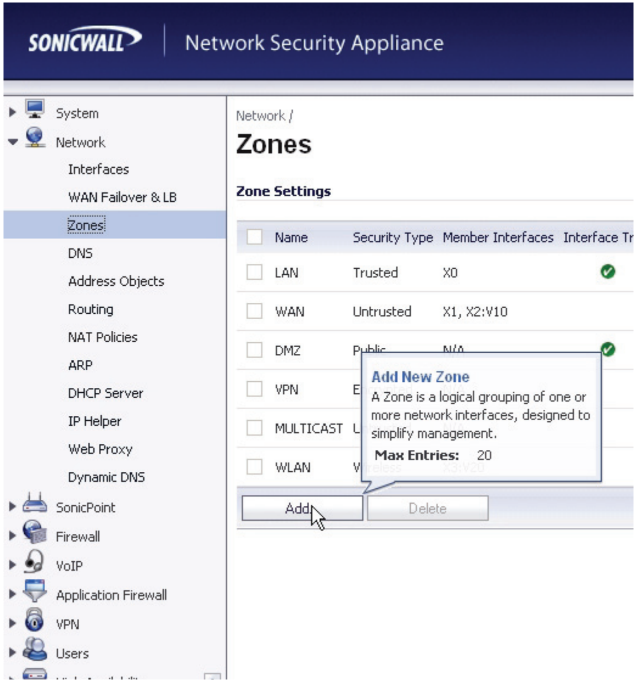
– Search All Categories –

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.



Network /

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	Wireless	X3:V20	

Add New Zone

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

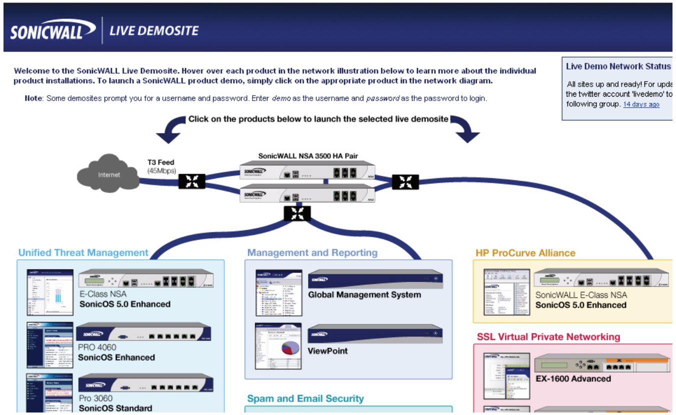
Max Entries: 20

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.

Click on the products below to launch the selected live demosite

Live Demo Network Status

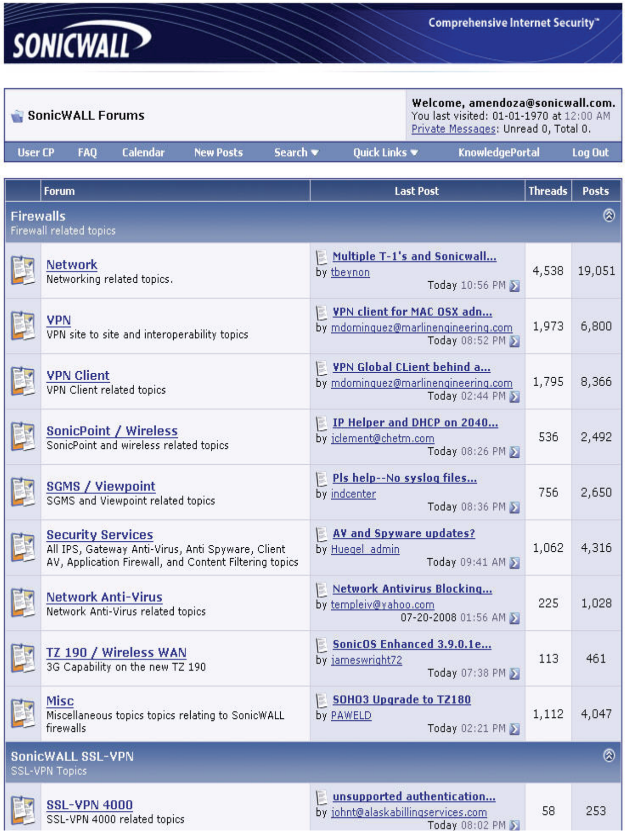
All sites up and ready! For upda
the twitter account 'livedemo' to
following group. 14 days ago

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.

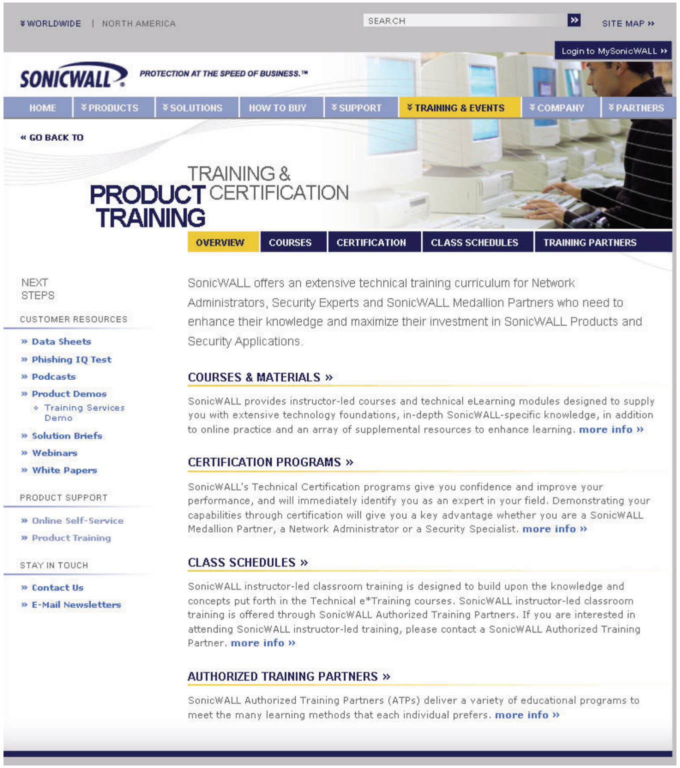
Forum	Last Post	Threads	Posts
Firewalls Firewall related topics			
Network Networking related topics.	Multiple T-1's and Sonicwall... by tbeynon Today 10:56 PM	4,538	19,051
VPN VPN site to site and interoperability topics	VPN client for MAC OSX adn... by mdominguez@marlinengineering.com Today 08:52 PM	1,973	6,800
VPN Client VPN Client related topics	VPN Global CLient behind a... by mdominguez@marlinengineering.com Today 02:44 PM	1,795	8,366
SonicPoint / Wireless SonicPoint and wireless related topics	IP Helper and DHCP on 2040... by jclement@chetm.com Today 08:26 PM	536	2,492
SGMS / Viewpoint SGMS and Viewpoint related topics	Pls help--No syslog files... by indcenter Today 08:36 PM	756	2,650
Security Services All IPS, Gateway Anti-Virus, Anti Spyware, Client AV, Application Firewall, and Content Filtering topics	AV and Spyware updates? by Huegel_admin Today 09:41 AM	1,062	4,316
Network Anti-Virus Network Anti-Virus related topics	Network Antivirus Blocking... by templeiv@yahoo.com 07-20-2008 01:56 AM	225	1,028
TZ 190 / Wireless WAN 3G Capability on the new TZ 190	SonicOS Enhanced 3.9.0.1e... by jameswright72 Today 07:38 PM	113	461
Misc Miscellaneous topics topics relating to SonicWALL firewalls	SOHO3 Upgrade to TZ180 by PAWELD Today 02:21 PM	1,112	4,047
SonicWALL SSL-VPN SSL-VPN Topics			
SSL-VPN 4000 SSL-VPN 4000 related topics	unsupported authentication... by johnt@alaskabillingservices.com Today 08:02 PM	58	253

Training

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

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

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



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

COURSES & MATERIALS »

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

CERTIFICATION PROGRAMS »

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

CLASS SCHEDULES »

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

AUTHORIZED TRAINING PARTNERS »

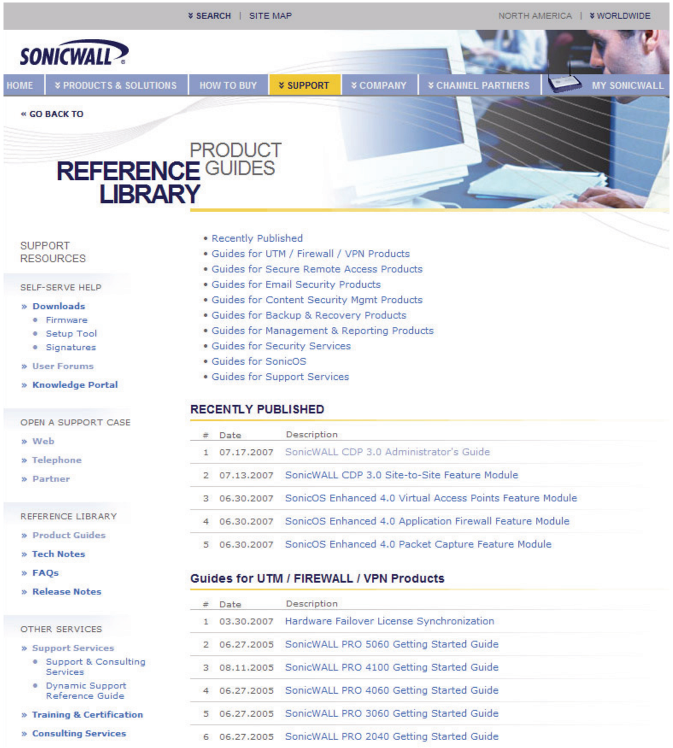
SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. **more info »**

Related Documentation

See the following related documents for more information:

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

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



SUPPORT RESOURCES

SELF-SERVE HELP

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

OPEN A SUPPORT CASE

- » Web
- » Telephone
- » Partner

REFERENCE LIBRARY

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

OTHER SERVICES

- » Support Services
    - Support & Consulting Services
    - Dynamic Support Reference Guide
- » Training & Certification
- » Consulting Services

- 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