COMPREHENSIVE INTERNET SECURITY

SonicWALL Internet Security Appliances

SonicWALL TZ 180 Wireless Recommends Guide

SONICWALL®

SonicWALL Recommends Guide

Recommended Solutions for the SonicWALL TZ 180 Wireless

SonicOS 3.8 Standard and Enhanced

Table of Contents

Recommends Guide Overview

Welcome to the 'SonicWALL Recommends' Guide for the SonicWALL TZ 180 Wireless security appliance. This guide is designed to help you configure the TZ 180 Wireless security appliance to provide reliable, secure, and trouble-free connectivity. This guide is not intended as a replacement for the Getting Started Guide or the Administrator's Guide, but rather as an addendum to both guides. The SonicWALL Recommends Guide for the SonicWALL TZ 180 Wireless security appliance can significantly simplify and enhance the installation and operation of the TZ 180 Wireless security appliance.

This SonicWALL Recommends Guide contains the following sections:

- "Registering and Enabling Support" section on page 4 – This section provides instructions for verifying that the TZ 180 Wireless security appliance is properly registered, keeping proper backups of critical files, and retrieving updated firmware files.
- "Security Best Practices for TZ 180 Wireless Running SonicOS Standard" section on page 9 – This section provides instructions for configuring security settings for the TZ 180 Wireless security appliance and its nterfaces.
- "Troubleshooting TZ 180 Wireless Configuration and Settings Issues " section on page 13 – This section provides troubleshooting for the most common configuration issues, as reported by SonicWALL's Technical Support department.
- "SonicWALL Solutions Integration" section on page 33 – This section provides information about SonicWALL's suite of products that are complementary to the TZ 180 Wireless security appliance and describes how they can be easily integrated into your network environment.
- "Obtaining Technical Support" section on page 41 – This section provides contact information for SonicWALL Technical Support.

The guide provides instructions and information to quickly configure and use a SonicWALL TZ 180 Wireless security appliance. For details about the features introduced in this guide, refer to the SonicOS Enhanced or SonicOS Standard Administrator's Guide and SonicWALL's ever-growing library of technical notes, all available on SonicWALL's Web site at http://www.sonicwall.com/us/support.

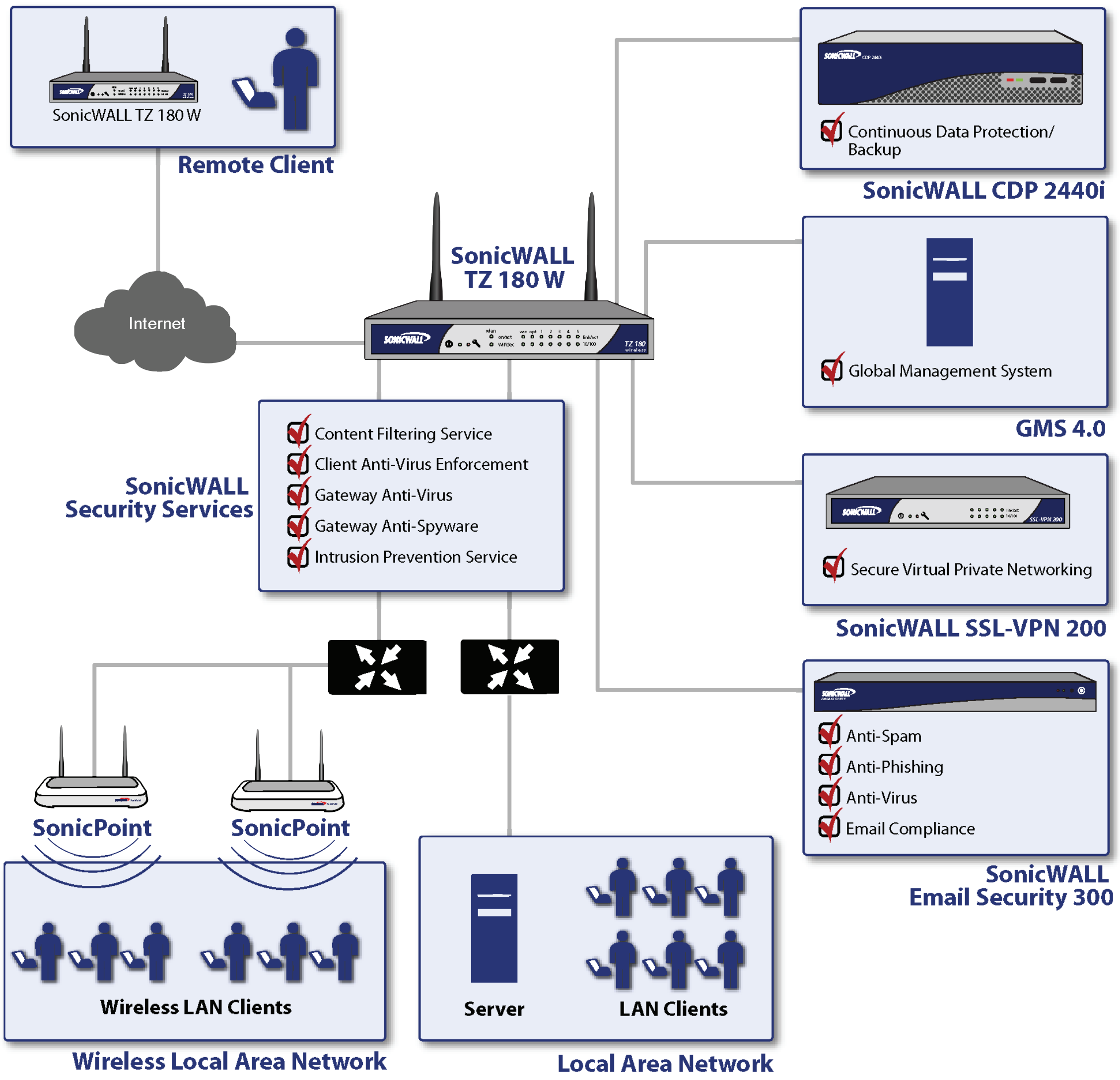
Document Scope

This ‘SonicWALL Recommends’ Guide describes how to how to plan, design, implement, and manage the TZ 180 Wireless security appliance on your network.

This document contains the following sections:

SonicWALL TZ 180 Wireless Network Topology

Figure 1 Sample Network Configuration



Registering and Enabling Support

Your TZ 180 Wireless security appliance provides 90 days of free software updates and technical support. To activate your free software updates and technical support, you must register your security appliance at mysonicwall.com before you install the appliance on your network. This process takes no more than a few minutes and significantly reduces future runtime and support issues with the appliance. Registering at mysonicwall.com also provides you access to new firmware patches and new firmware versions with added features.

It is critical to register the TZ 180 Wireless security appliance. If the TZ 180 Wireless security appliance is not registered, you cannot install new firmware or access new firmware updates on the MySonicWALL portal. As with other networking devices, the TZ 180 Wireless is shipped with the most current software possible; however, it is difficult to predict how much time may have elapsed since shipping. During this time it's possible that SonicWALL has updated the firmware. It is recommended that you visit mysonicwall.com to check for a more current version.

Once registered, SonicWALL products provide dynamic support by periodically checking with SonicWALL's security portal for firmware updates, and security services signature updates on appropriately licensed appliances. This ensures that your network, users, and data are protected from emerging threats. The communications channel between the SonicWALL security appliance and the security portal is SSL encrypted for confidentiality, and no sensitive or private data is exchanged.

Note Turn off pop-up blockers on your Web browser when accessing MySonicWALL Web site or the management interface of your TZ 180 Wireless security appliance.

Note Your SonicWALL TZ 180 Wireless security appliance should be operational and have Internet connectivity prior to enabling support. Refer to the *SonicWALL TZ 180 Wireless Getting Started Guide* to set up your SonicWALL TZ 180 Wireless security appliance for the first time. For additional setup information, refer to the "Basic SonicWALL Security Appliance Setup" section in the *SonicOS Standard 3.8 Administrator's Guide*.

To enable support on a SonicWALL TZ 180 Wireless security appliance, perform the following steps:

Step 1 Navigate to https://www.mysonicwall.com or navigate to **Wizards > License and Registration Wizard** in the SonicWALL TZ 180 Wireless management interface.

Step 2 Click the **Click here** link in **If you are not a registered user, Click Here**.

Step 3 Fill out the registration fields, including a working email address.

Note Your email address is used to send you important update information related to your TZ 180 Wireless and is not used for spam. Provide a working email address.

Step 4 To be a beta tester and be provided access to pre-release firmware updates for your TZ 180 Wireless security appliance, check the box next to **Yes, I would like to be a Beta Tester**.

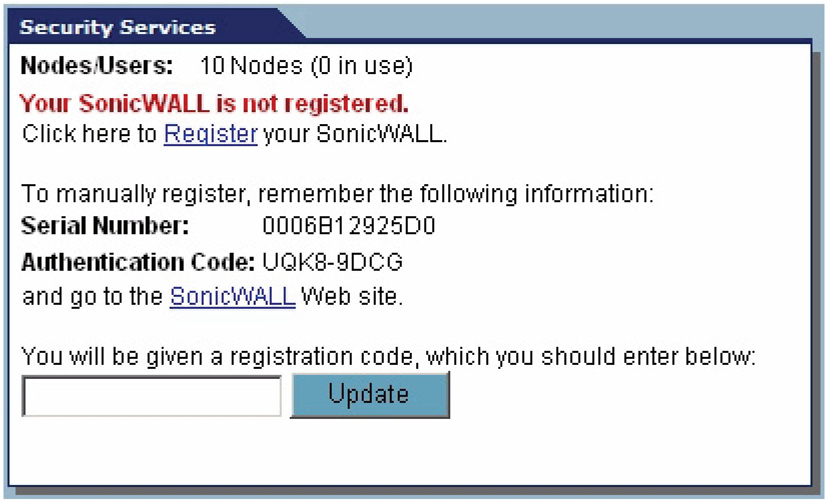
Step 5 Locate the serial number and authentication code of the appliance, located on the bottom of the appliance and on the **System > Status** page of the management interface of the security appliance.

Note The management interface can be accessed by default at http://192.168.168.168, using the LAN interface of the TZ 180 Wireless security appliance. Login using the default username **admin** and default password **password**.

Step 6 You can register appliance from the **System > Status** page, using the **Registration & License Wizard**, or directly from mysonicwall.com. To register your TZ 180 Wireless, log into MySonicWALL, enter your username and password, and enter the serial number of the TZ 180 Wireless in the **Quick Registration** field in the lower-left side of the page. Fill out the fields when prompted. A registration code is generated.

Step 7 Navigate to the **System > Status** page on the appliance management interface. Under **Security Services**, your registration code in the field below the message **You will be given a registration code, which you should enter below:**, illustrated in Figure 2, and click **Update**.

Figure 2 Unregistered TZ 180 Wireless Security Appliance



Nodes/Users: 10 Nodes (0 in use)

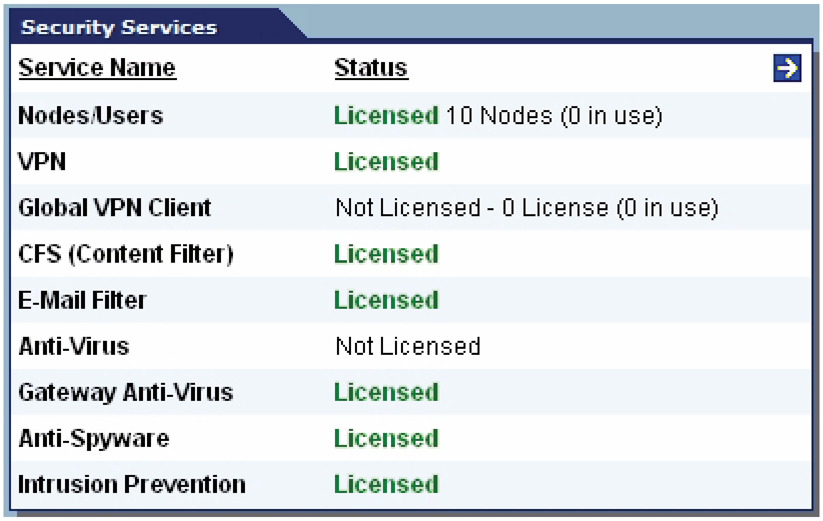
Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B12925D0
Authentication Code: UQK8-9DCG
and go to the SonicWALL Web site.

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

When the registration process is complete, the **Security Services** section displays the status of current licenses. Figure 3 provides a view of a registered TZ 180 Wireless appliance.

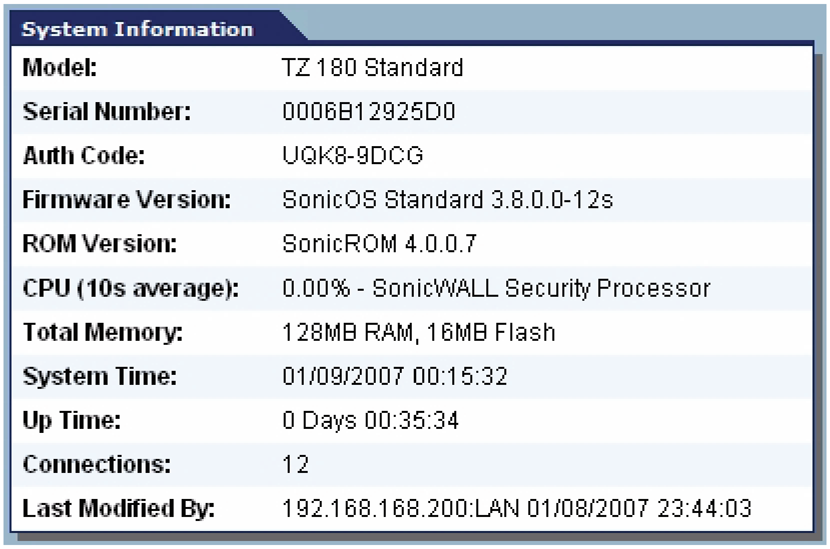
Figure 3 Registered TZ 180 Wireless Security Appliance



Service Name	Status
Nodes/Users	Licensed 10 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Not Licensed - 0 License (0 in use)
CFS (Content Filter)	Licensed
E-Mail Filter	Licensed
Anti-Virus	Not Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed

Step 8 Determine what firmware version is on the TZ 180 Wireless security appliance by navigating to the **System > Status** page of the management interface. Figure 4 provides a view of the System Information tab.

Figure 4 Determining the TZ 180 Wireless Current Firmware



System Information

Model:	TZ 180 Standard
Serial Number:	0006B12925D0
Auth Code:	UQK8-9DCG
Firmware Version:	SonicOS Standard 3.8.0.0-12s
ROM Version:	SonicROM 4.0.0.7
CPU (10s average):	0.00% - SonicWALL Security Processor
Total Memory:	128MB RAM, 16MB Flash
System Time:	01/09/2007 00:15:32
Up Time:	0 Days 00:35:34
Connections:	12
Last Modified By:	192.168.168.200:LAN 01/08/2007 23:44:03

Step 9 Log into mysonicwall.com and select the TZ 180 Wireless security appliance you just registered. Download the most recent version of firmware, if applicable.

Note When your support contract expires, you will only be able to download the last current version available upon expiration and will not have access to subsequent versions until a software support contract has been renewed. To renew, contact the reseller you purchased the TZ 180 Wireless from, or contact SonicWALL.

Note Before updating the firmware on the TZ 180 Wireless security appliance, always perform these steps: Create a backup, store the current settings, store a copy of the current firmware, and record the details of the appliance along with the details of the MySonicWALL account the appliance has been registered under. This ensures that you can return the security appliance to a known-good state if any errors occur during the installation of new firmware.

Step 10 Navigate to **System > Settings** in the management interface and click the **Create Backup Settings...** button to create a restorable backup of the current appliance settings.

Note The TZ 180 Wireless security appliance can store one backup.

Step 11 Manually download the preferences file of the TZ 180 Wireless to a safe location by clicking **Export Settings**. Provide the preferences file a name that you can recognize, for example, tz180settings18jan2006-440pm.exp.

Step 12 Click the **Download** icon next to **Current Firmware** to manually download a copy of the current firmware.

Step 13 Navigate to **System > Diagnostics**. Check all four boxes and generate the Tech Support Report. Save the file, which contains the serial number, auth code, registration code, and all other administrator settings, to your computer.

Step 14 Make a note of the serial number of the appliance, the authorization code, the registration code, the name and password of the MySonicWALL account the appliance is registered under, and the date when the software support contract expires for the appliance.

Save all files on a secure network resource that is backed up on a regular basis. Refer to "SonicWALL Backup and Recovery Solutions" section on page 34 for information about how a SonicWALL CDP appliance to perform this task.

If any problems occur, restore using the backup snapshot. If this fails, reload the firmware and preferences manually using SafeMode.

Step 15 If you found and downloaded a more recent firmware version, navigate to the **System > Settings** page on the management interface and click on the **Upload New Firmware…** button. Click **Browse** and find the firmware file you downloaded.

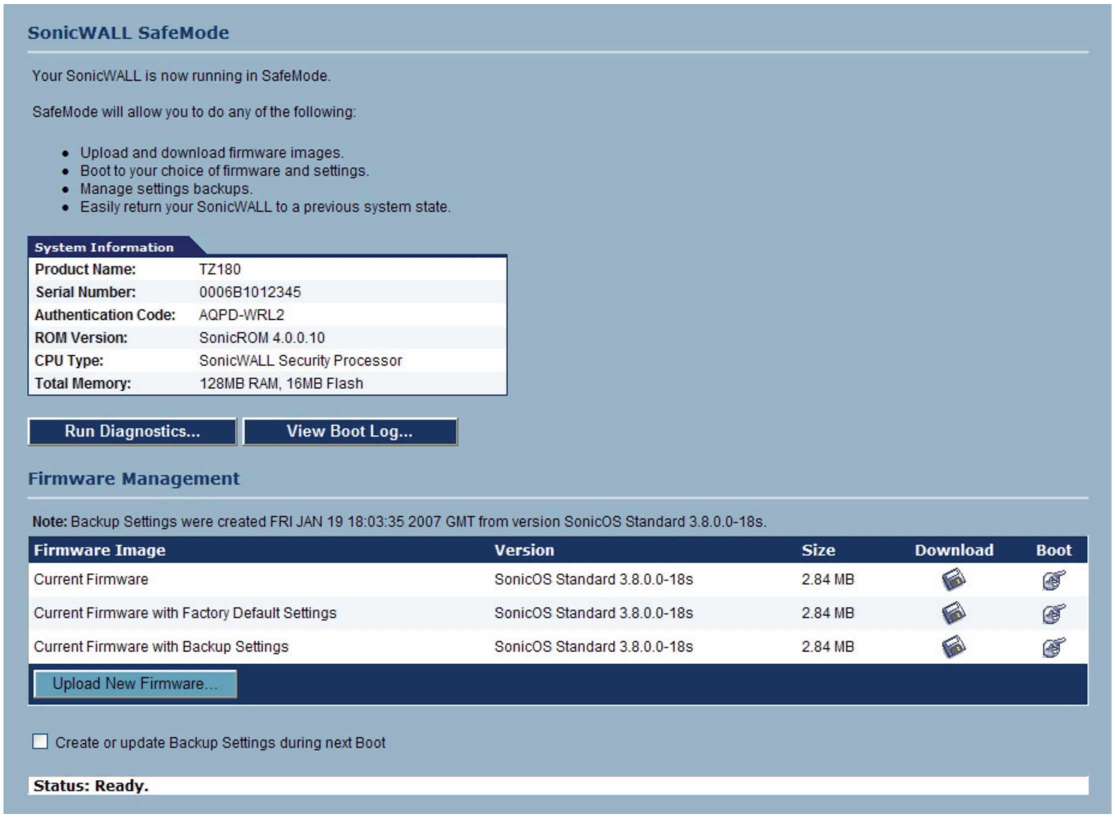
Step 16 After approximately two days, if the new firmware has had no issues, copy the new files. Refer to the backup section above and save a copy of the new firmware and the new settings, making sure to differentiate them from the older versions. It is recommended that you keep multiple sets of 'known-good' firmware.

Your security appliance has a protected boot loader that allows you to reset the security appliance, even if the firmware has become inoperable or corrupted. To access SafeMode, connect a computer to one of the LAN interfaces on the TZ 180 Wireless security appliance using a standard crossover Ethernet cable and assign this computer a static IP address of 192.168.168.200 with a netmask of 255.255.255.0. If the SafeMode interface does not display, wait 10-15 seconds and try again. When the link is active, unplug the power cable to the TZ 180 Wireless and insert a straightened-out paperclip into the small opening next to the power port until you feel a small switch depress. Keep this small switch depressed and plug the power cable back in. Hold the small switch in for about 20 seconds until the "wrench light" on the front of the TZ 180 Wireless flashes, then release it. The security appliance is now in SafeMode.

For more information on SafeMode, refer to the "Resetting the SonicWALL Security Appliance Using SafeMode" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.

Open a Web browser and navigate to the default SafeMode address at http://192.168.168.168. Figure 5 provides an example of SafeMode view.

Figure 5 SafeMode



SonicWALL SafeMode

Your SonicWALL is now running in SafeMode.

SafeMode will allow you to do any of the following:

- Upload and download firmware images.
- Boot to your choice of firmware and settings.
- Manage settings backups.
- Easily return your SonicWALL to a previous system state.

System Information

Product Name:	TZ180
Serial Number:	0006B1012345
Authentication Code:	AQPD-WRL2
ROM Version:	SonicROM 4.0.0.10
CPU Type:	SonicWALL Security Processor
Total Memory:	128MB RAM, 16MB Flash

Firmware Management

Note: Backup Settings were created FRI JAN 19 18:03:35 2007 GMT from version SonicOS Standard 3.8.0.0-18s.

Firmware Image	Version	Size	Download	Boot
Current Firmware	SonicOS Standard 3.8.0.0-18s	2.84 MB		
Current Firmware with Factory Default Settings	SonicOS Standard 3.8.0.0-18s	2.84 MB		
Current Firmware with Backup Settings	SonicOS Standard 3.8.0.0-18s	2.84 MB		

☐ Create or update Backup Settings during next Boot

Status: Ready.

In SafeMode, you can boot the security appliance with the current firmware with default settings, or you can click on the **Upload New Firmware** button and load a newer or previously known-good version. Once the security appliance has successfully booted, you can then restore the settings file from the management interface.

No matter what happens to the TZ 180 Wireless firmware or settings, you can return to this SafeMode menu and get the appliance running again. It is recommended that you save your known-good settings and firmware for this purpose.

Security Best Practices for TZ 180 Wireless Running SonicOS Standard

By default the TZ 180 Wireless security appliance is available with a number of security settings enabled and disabled to provide a moderate level of initial security to protect your network environment and the appliance, while simultaneously allowing basic and commonly used outbound network communications. Some of the security settings can have a potentially disruptive effect if configured incorrectly. Always activate, deactivate, and change settings with consideration and care. Table 1 provides an overview of the settings available on the TZ 180 Wireless security appliance.

Table 1 Security Settings Best Practices

Solution	Description	Related Information
Secure management access to the appliance from any interface, including across the public Internet	Navigate to the **Firewall > Access Rules** page and modify the default rule for HTTPS management. Click the **Configure** icon, change the **Source** drop-down from **LAN** to *****, and click **OK** to save and activate the change.	For more information on secure management access, refer to the "Configuring Network Access Rules" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Create a secure default administrator name	Navigate to the **System > Administration** page and change the **Administrator Name**. Make a note of your new administrator name. Change the password to something complex (for example, a combination of letters, numbers and/or symbols at least six characters in length).	For more information on changing default Administrator names, refer to the "Using System Administrator" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Verify time settings	Navigate to the **System > Time** page and verify that the time zone settings are correct based on the location of the appliance. The use of NTP for accuracy is recommended. Accurate time settings are crucial for the logging and reporting functions of the appliance.	For more information on verifying time settings, refer to the "Setting System Time" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Configure DNS settings	Navigate to the **Network > Settings** page and verify that the appliance has valid DNS server(s) configured (if running Enhanced, the DNS server(s) can be found on the configuration page of the WAN interface). This is crucial for the logging, lookup, DHCP, and reporting functions of the appliance. If you do not know your ISP DNS servers, you can temporarily use 4.2.2.1 and 4.2.2.2, but discontinue use once your ISP has provided you with the correct DNS server address.	For more information on configuring DNS settings, refer to the "Configuring Network Settings" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.

Solution	Description	Related Information
Use Dynamic DNS (DDNS) to make your WAN IP address easily resolvable	Navigate to the **Network > Dynamic DNS** page and configure the security appliance for DDNS. You can find a technote on how to do this on the SonicWALL support site. This feature makes remote management and VPN connectivity significantly easier, especially if your TZ 180 has a dynamically-obtained (DHCP, PPPoE, L2TP) WAN IP address.	For more information on using Dynamic DNS, refer to the “Configuring Dynamic DNS” chapter in the *SonicOS Standard 3.8 Administrator’s Guide*.
Audit your firewall access rules monthly	Navigate to the **Firewall > Access** rules page, and perform an audit of rules on a monthly basis. It is strongly recommended to re-evaluate your settings and policies at regular intervals for optimum functionality.	For more information on auditing your firewall access rules, refer to the “Configuring Network Access Rules” chapter in the *SonicOS Standard 3.8 Administrator’s Guide*.
Enable better support for Microsoft networks	Navigate to the **Firewall > Advanced** page. If you have a Microsoft networking environment that spans across the LAN and OPT/DMZ interfaces of the TZ 180, and security has been set to allow this, check the boxes to allow NetBIOS broadcast for **LAN to DMZ** and **DMZ to LAN**. Microsoft networking relies on NetBIOS broadcasts to identify and register network resources such as servers and printers, so enabling these checkboxes can resolve network connectivity issues.	For more information on enabling support for Microsoft Networks, refer to the “Configuring Advanced Rule” chapter in the *SonicOS Standard 3.8 Administrator’s Guide*.
Properly configure advanced firewall features	Navigate to the **Firewall > Advanced** page. Some security features can cause issues if arbitrarily enabled. For example, enabling Stealth Mode causes the appliance to silently drop any unauthorized connection to the WAN interface, instead of sending a deny back to the source (that tells the source that there is a security appliance at that address). Enabling the Randomize IP ID scrambles the packet identification sequence and prevents “fingerprint” detection toolkits from determining the appliance’s make and model. Enabling both is recommended. Checksum enforcement options should only be enabled if the network security policy of your organization requires it, because it can lead to significant connectivity issues with certain applications that do not conform to TCP/IP standards.	For more information on configuring advanced firewalls, refer to the “Configuring Advanced Rule Options” chapter in the *SonicOS Standard 3.8 Administrator’s Guide*.

Solution	Description	Related Information
Optimize your firewall access rules	On any firewall rule, enable fragmented packet handling, and verify that the connection timeout for the rule is appropriate to the referenced service. For example, telnet connections tend to be long-lasting, so TCP timeout should be set accordingly. Similarly, timeout can be set lower for short-lived services, thus keeping the connection cache clean.	For more information on firewall access, refer to the "Configuring Network Access Rules" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Optimize your VPN settings	Navigate to the **VPN > Advanced** page and verify that fragmented packet handling/NAT traversal/IKE DPD is enabled, and if you use Microsoft networking across VPN tunnels, uncheck the box next to **Disable all VPN Windows Networking (NetBIOS) Broadcasts**. When creating VPN policies, be sure to check the box next to **Enable Windows Networking (NetBIOS) Broadcasts** on the **Advanced** tab of the VPN policy.	For more information on VPN settings, refer to the "Configuring Advanced VPN Settings" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Audit your User accounts	Navigate to the **Users > Local Users** page and audit user entries at least once a month to verify there are not inappropriate accounts. Also enforce the use of complex passwords, and require users to change passwords on a regular basis. Three months is the recommended interval. Do not allow the use of common accounts, in which the username and password are known to a wide audience.	For more information on user accounts, refer to the "Configuring Local Users" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Establish, a logging baseline	On the **Log > View** page, it is recommended to enable all categories and alerts for at least the first few days of a new installation, allowing a better understand the various functions. This generates a lot of log messages, so after a few days, configure logs a level appropriate for your environment.	For more information on logging baselines, refer to the "Viewing Log Events" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.
Deliver logs and alerts by email	On the **Log > Automation** page, enter in the fully-qualified domain name (FQDN) or IP address of a mail server that you relay SMTP mail through, and a working email address that the appliance uses to notify in case of alerts, and to email the logs to on a periodic basis. This is strongly recommended.	For more information on logs and alerts, refer to the "Configuring Log Automation" chapter in the *SonicOS Standard 3.8 Administrator's Guide*.

Solution	Description	Related Information
Map logged IP address to machine name for identification	On the **Log > Name** Resolution page, set it to **DNS then NetBIOS** and click the **Apply** button in the upper-right-hand part of the screen to save and activate the change. This lets the appliance apply more a “friendly” name to the IP address in the log, including the NetBIOS names of systems on the LAN, which is easier than using a non-fixed IP address. Do not use this setting if you are using DNS servers supplied by your ISP.	For more information on mapping a logged IP address, refer to the “Configuring Name Resolution” chapter in the *SonicOS Standard 3.8 Administrator’s Guide.*
Keep backups	Store known-good preferences and firmware in a safe place that is accessible in the event of problems with the appliance, and verify the appliance is always under a valid service and software support contract. Disaster recovery can be fairly painless if you follow these policies.	For more information on keeping backups, refer to the “Configuring System Settings” chapter in the *SonicOS Standard 3.8 Administrator’s Guide.*
Control physical access	Other measures are irrelevant if you do not limit physical access to the security appliance itself, as it can be easily reset and illegally accessed if an intruder can get to the security appliance.	For more information on controlling physical access, refer to the “Mounting Instructions” chapter in the *SonicWALL TZ 180 Series Getting Started Guide.*

Troubleshooting TZ 180 Wireless Configuration and Settings Issues

This section provides troubleshooting information for the six most common issues reported by SonicWALL technical support for the TZ 180 Wireless security appliance running SonicOS Standard firmware. If you need to troubleshoot an issue that is not listed below, or if the suggestions below do not resolve your issue, visit SonicWALL's support Web site at www.sonicwall.com to review the SonicOS Administrator's Guides and technotes. Another resource is SonicWALL's interactive online Knowledge Portal.

Note The six issues listed below have detailed technotes available on www.sonicwall.com.

This section provides troubleshooting for the SonicWALL TZ 180 Wireless security appliance. This section contains the following subsections:

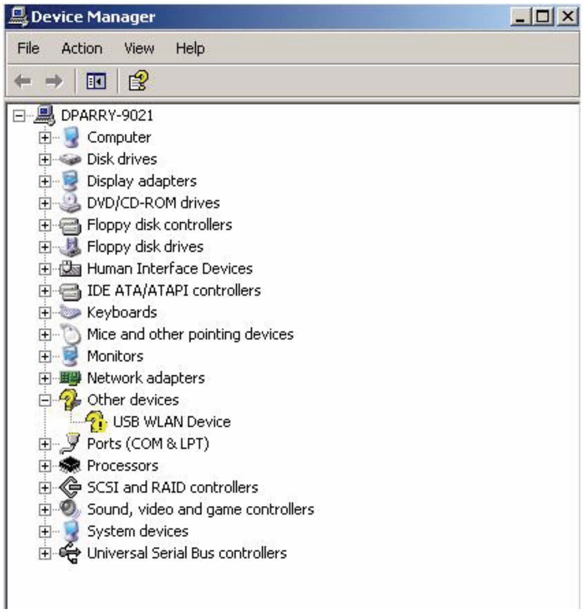
Wireless Connectivity Troubleshooting

Symptom: I Cannot Connect to the TZ 180 Wireless Security Appliance's Wireless Port

Is your wireless card installed correctly?

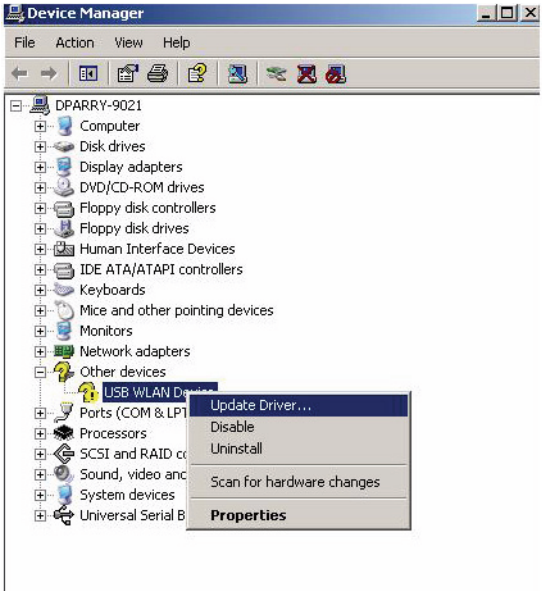
To verify that the wireless LAN card is installed correctly, right-click on the **My Computer** icon on the desktop and select **Properties**. Select the **Hardware** tab and click on the **Device Manager** button. Under the **Network adapters** section, verify that the wireless LAN card is listed and is functioning correctly. Figure 6 provides an example of a Device Manager view displaying a wireless LAN under the **Other devices section** because it is not functioning correctly.

Figure 6 Device Manager Displaying Non-Functioning Wireless LAN Card



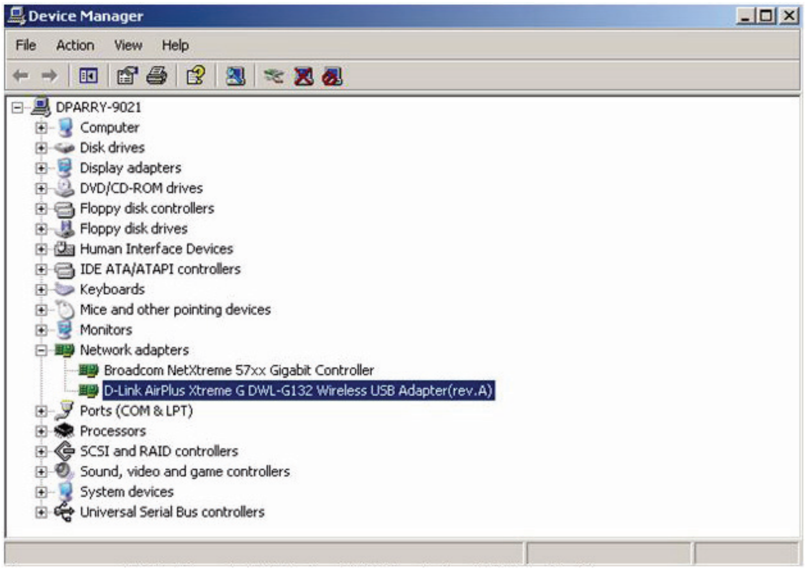
If the wireless LAN card is not functioning correctly, you will need to install updated drivers. Contact the manufacturer of the wireless LAN card or search their support Web site for the driver. This is a good practice for any networking device, as updated drivers may have been released since the product was originally released. If the manufacturer included an executable installer program for the driver, run it. If not, right-click on the non-functioning wireless LAN card, as illustrated in Figure 7, and select **Update Driver**.

Figure 7 Updating Wireless LAN Card Driver



Once the drivers have been installed successfully, the wireless LAN card will display as in Figure 8, under **Network adapters.**

Figure 8 Correctly Installed Wireless LAN Card


Device Manager
File
Action
View
Help
DPARRY-9021
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Floppy disk controllers
Floppy disk drives
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Broadcom NetXtreme 57xx Gigabit Controller
D-Link AirPlus Xtreme G DWL-G132 Wireless USB Adapter(rev.A)
Ports (COM & LPT)
Processors
SCSI and RAID controllers
Sound, video and game controllers
System devices
Universal Serial Bus controllers

Are You Connecting with an Intel Wireless adapter?

The following Intel chipsets are publicly known and acknowledged by Intel to have disconnect issues with third-party wireless access points such as the SonicWALL SonicPoint, SonicPoint-G and TZ series Wireless security appliances:

- Intel PRO/Wireless 2100 Network Connection
- Intel PRO/Wireless 2100A Network Connection
- Intel PRO/Wireless 2200BG Network Connection
- Intel PRO/Wireless 2915ABG Network Connection
- Intel PRO/Wireless 3945ABG Network Connection

These wireless cards are provided to OEM laptop manufacturers and are often rebranded under the manufacturers name – for example, both Dell and IBM use the above wireless cards but the drivers are branded under their own name.

Step 1 To identify the adapter, navigate to Intel's support site and do a search for Intel Network Connection ID Tool. Install and run this tool on any laptop experiencing frequent wireless disconnect issues. The tool will identify which Intel adapter is installed inside the laptop.

Step 2 Once you have identified the Intel wireless adapter, navigate to Intel's support site and download the newest software package for that adapter – it's recommended you download and install the full Intel PRO/Set package and allow it to manage the wireless card, instead of Windows or any OEM-provided wireless network card management program previously used. As of January 2007 the most recent version of the full Intel PRO/Set Wireless software driver/manager is 10.5.2.0. SonicWALL recommends you use this version or newer.

Step 3 In the Advanced section, disable the power management by unchecking the box next to Use default value, then move the slidebar under it to Highest. This instructs the wireless card to operate at full strength and not go into sleep mode.

Step 4 Click on the **OK** button to save and activate the change.

Step 5 Reboot the laptop.

Step 6 In the Advanced section, adjust the roaming aggressiveness by unchecking the box next to Use default value, then move the slidebar under it to Lowest. This instructs the wireless card to stay stuck to the AP it's associated as long as possible, and only roam if the signal is significantly degraded. This is extremely helpful in environments with large numbers of access points broadcasting the same SSID.

Step 7 Click on the **OK** button to save and activate the change.

Step 8 Reboot the laptop.

If you continue to have issues, you may also try adjusting the Preamble Mode on the wireless card. By default the Intel wireless cards above are set to auto. All SonicWALL wireless products by default are set to use a Long preamble, although this can be adjusted in the Management GUI.

Step 9 To adjust the Intel wireless card's preamble setting, go to the Advanced section and uncheck the box next to Use default value, then select Long Tx Preamble from the drop-down below it.

Step 10 Click on the **OK** button to save and activate the change.

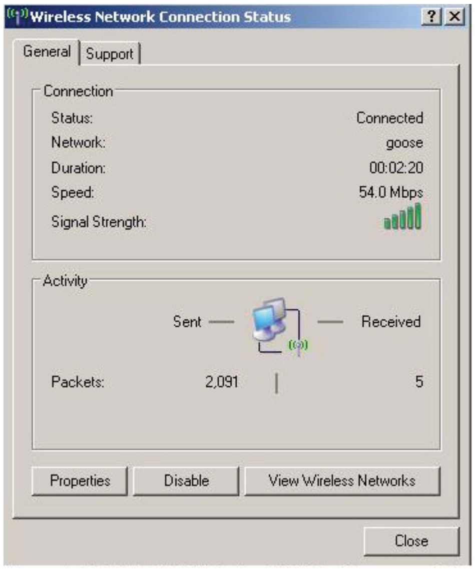
Step 11 Reboot the laptop.

If the above steps fail to resolve the disconnect issues, it may be necessary to replace the wireless card with an external model.

Are You Connected to the TZ 180 Wireless LAN Interface?

If you see this icon in the lower-right-side of your Windows Taskbar, you are not connected to the TZ 180 Wireless LAN interface. This icon means you are connected to a wireless network. To see if you are associated to the correct Wireless Access Point (or SSID), right-click on the icon and select **Status** from the menu that displays. On the pop-up that displays, verify that you are associated to the SSID of the TZ 180W WLAN interface, as illustrated in Figure 9.

Figure 9 Wireless Connection Status



Status: Connected
Network: goose
Duration: 00:02:20
Speed: 54.0 Mbps
Signal Strength:

Sent — — Received
Packets: 2,091 | 5

Is the Wireless Card's Management Software Able to See the TZ 180 Wireless SSID?

Most wireless cards have proprietary management software for configuring wireless settings, but Windows XP by default attempts to configure the wireless cards itself. If the wireless card cannot see the SSID, it may be out of range of the TZ 180 Wireless and should be moved or reoriented so that the wireless card antennas can pick up the SSID broadcasts coming from the TZ 180 Wireless. If the TZ 180 Wireless has been set to suppress SSID broadcasts and not answer to null SSID requests, it may be necessary to manually input the SSID into the wireless card setup tool. Some setup tools do not allow the user to do this, and it may be necessary to reconfigure the TZ 180 Wireless to broadcast SSID.

Is the Wireless Card Management Software Configured Correctly?

In order to properly associate with and authenticate to the TZ 180 Wireless, the wireless cards must be configured to match the TZ 180 Wireless security appliance wireless settings. If any settings do not match, it may result in the wireless card being unable to connect to the TZ 180 Wireless. The terms used by each manufacturer may differ, but configuration with the management software generally includes the following options:

- Selecting the TZ 180 Wireless SSID, either by broadcast or manual configuration
- Entering the Network Authentication type, typically WPA-PSK
- Choosing **Infrastructure** mode (instead of Ad Hoc)
- Choosing the wireless data rate, usually **auto**, but this is dependent upon the environment
- Setting the power saving mode, turning this feature off is recommended
- Setting to use auto, short, or long preamble, auto is recommended, and any other setting must exactly match the setting on the TZ 180 Wireless

Is Windows XP Managing the Wireless LAN Card?

Windows XP has a built-in wireless configuration program that is on by default, and may cause problems if configured incorrectly. It is strongly recommended that you disable this feature and use the management driver and software that ships with the wireless card. If the Windows XP configuration program must be used, follow these guidelines:

- The wireless card software drivers must be compatible with Microsoft's Wireless Zero Configuration service.
- You can access the settings by clicking on the wireless card icon in the system tray, or by right-clicking on the **My Network Places** icon on the desktop and double-clicking on the wireless card icon. When the initial configuration screen displays, it lists all of the wireless networks that it sees. Click on the **Advanced…** button on the lower left side of this screen.
- Check the **Use Windows to configure my wireless network settings** box.
- If your TZ 180 Wireless SSID name appears in the **Available Networks** box, select it and then click on the **Configure** button to the right. If you do not see it, click the **Refresh** button. If the TZ 180 Wireless has been set to suppress SSID and not respond to probe request frames (advanced settings), then it is necessary to instead use the **Add** button below to manually enter in the SSID.
- If you are using WEP, check the boxes next to **Data encryption (WEP enabled)** and **Network Authentication (shared mode)**. Both must be checked or it will not work.
- Uncheck the box next to **The key is provided to me automatically**.
- If using WEP, enter the TZ 180 Wireless WEP key into the **Network Key** and **Confirm Network Key** fields.
- When using WEP with Windows XP prior to Service Pack 1, it is required to select what type the key is (alphanumeric, hexidecimal) and the key size (40, 104). Although the TZ 180 Wireless lists different key sizes (64,128), they are actually the same. For this purpose, 40=64 and 104=128. After Service Pack 1, these options are not displayed, and XP automatically determines the type and size.
- When using WEP with XP prior to Service Pack 1, a different key index is used: 0-3 instead of 1-4. The TZ 180 Wireless key index uses 1-4. For this purpose, 0=1, 1=2, 2=3, 3=4. This was resolved in Service Pack 1.
- Click on the **Association** tab and uncheck the box next to **Enable IEEE 802.1x authentication for this network**.
- Click **OK** to save all changes. You may need to reboot the XP system and the TZ 180 Wireless if you are switching WEP keys.

Is the Signal Strength Sufficient?

If all the settings are correct on each side, and the wireless card still cannot connect to the TZ 180 Wireless, there may be environmental factors involved. It may be that the wireless card is located too far from the TZ 180 Wireless, or that there is substantial signal interference. This may be the result of passive interference in the form of concrete or steel walls, or active interference in the form of another wireless access point broadcasting on the same or adjacent channel. It may also be the result of active interference from a microwave oven, 2.4Ghz cordless phone, x10 security systems, baby monitoring systems, or Bluetooth devices. Correcting this problem may require moving the wireless card closer to the TZ 180 Wireless, reorienting the antennas on the wireless card and TZ 180 Wireless, adjusting the power output on the TZ 180 Wireless, or purchasing a higher power wireless card. In the case of active interference, it may require moving the TZ 180 Wireless to a different channel where no interference occurs from external sources. This may require the use of a wireless sniffer or spectrum analyzer.

Are the Wireless Card and TZ 180 Wireless set for DHCP or Static IP?

If all the settings are correct on each side, and the wireless card cannot access any resources through the TZ 180 Wireless, check the wireless card's TCP/IP settings. If the TZ 180 Wireless is set to issue DHCP addresses using the WLAN interface, check to make sure there are available addresses and that the scope has been set up correctly. If the TZ 180 Wireless is not issuing DHCP addresses using the WLAN interface, you will need to set the wireless card to use a unique static IP address from the same subnet attached to the TZ 180 Wireless WLAN interface, the correct mask, the TZ 180 Wireless WLAN IP address as the default gateway, and the correct DNS/WINS information for the user's environment. If DHCP is in use and the card is unable to retrieve a lease from the TZ 180 Wireless, it may be necessary to issue the Windows commands **ipconfig/release** and **ipconfig/renew** to obtain a new lease, or to reboot.

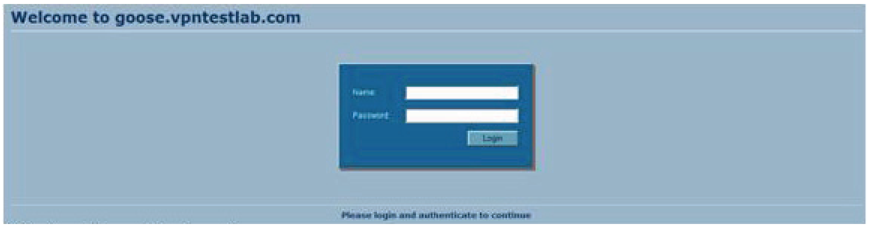
Is the TZ 180W using MAC Filtering?

If the TZ 180 Wireless is using MAC filtering, then the TZ 180 Wireless administrator must add the wireless card's MAC address to the **Wireless/MAC Filter List** as an **Allow** entry. Most wireless card manufacturers list the MAC address on the bottom of the card. You can also find the MAC address by installing the card and issuing the Windows command **ipconfig/all**. This is not necessary for Wireless Guest Services users, as their MAC addresses are automatically added upon successful authentication.

Is the TZ 180W Using Wireless Guest Services?

If the TZ 180 Wireless has Wireless Guest Services activated, the TZ 180 Wireless blocks all communications to the WAN until the wireless user authenticates to the TZ 180 Wireless using the login screen illustrated in Figure 10, or connects to the TZ 180 Wireless with the Global VPN Client (GVC). Users are authenticated using HTTP on a Web browser by intercepting the wireless user's attempt to connect to a webserver on the WAN side of the TZ 180 Wireless. For example, if a wireless user opens Microsoft Internet Explorer and attempts to access http://www.sonicwall.com, the TZ 180 Wireless presents a login screen to the user, which requires a username and password. These user names and accounts must be configured on the TZ 180 Wireless first; there are both permanent accounts and time-based accounts that can be used for Wireless Guest Services. Successful authentication then opens up WAN access for the wireless user for all policy-allowed protocols and destinations. Unsuccessful authentication causes the TZ 180 Wireless to log the failed attempt, and block the wireless user access.

Figure 10 Wireless Guest Services Login Window



Welcome to goose.vpntestlab.com

Please login and authenticate to continue

Wireless Guest Services controls access to the WAN. Activating Wireless Guest Services blocks all guest users from accessing anything on the LAN, even if there are policy entries created to permit it (Wireless Guest Services overrides these entries). Wireless Guest Services requires the use of MAC address filtering, but that successful authentication of a guest user automatically allows the guest's MAC address to connect. As a result, it is not necessary to manually input the MAC address of the guest user's wireless card on the TZ 180 Wireless. If a MAC address is manually entered, those users will not get prompted with the Wireless Guest Services login.

Is the TZ 180 Wireless Using WiFiSec?

If the TZ 180 Wireless has WiFiSec Enforcement enabled, it will only accept IPSec packets through the WLAN interface, unless Wireless Guest Services is also enabled (and if so, it will force unencrypted attempts to access the WAN to first authenticate themselves). This means that all wireless users must use the Global VPN Client to authenticate and connect to the TZ 180 Wireless before being able to access any WAN or LAN resources, policy permitting. If the wireless user is unable to successfully connect to the TZ 180 Wireless with the Global VPN Client, verify the following:

- The wireless user's Global VPN Client must be configured with the TZ 180 Wireless WLAN IP address and not its LAN or WAN IP address (or, for more recent versions of the client, use the default **Office Gateway** entry). This is a common mistake and should be the first thing checked.
- Activate the GroupVPN on the TZ 180 Wireless by checking the **Enable** checkbox in the **VPN/Settings** screen. The GroupVPN is the built-in connector for all incoming VPN clients.
- Set the keying mode is set appropriately to preshared secret or certificates.
- Set policy appropriate to the environment.
- The VPN should terminate on the **LAN/WLAN** port and not just the **LAN** port.
- If requiring user authentication, check the **Require Authentication of VPN Clients via XAUTH** box in the GroupVPN connector's **Advanced** tab, and verify that the accounts have been correctly set up on the TZ 180 Wireless (internal list or external RADIUS).
- If not using simple key provisioning, the preshared key must be configured and users must know it. They will be prompted for the preshared key before the username and password prompt.

Is the Policy Set Up Correctly?

By default, the TZ 180 Wireless is set to allow all WLAN traffic access any destination and protocol using the WAN interface, but not access any destination or protocol on the LAN. If the wireless users need to access resources on the LAN side of the TZ 180 Wireless, it is necessary to create policy entries allowing this. However, this may compromise the security of the TZ 180 Wireless. To fully protect the LAN resources, verify that **WiFiSec Enforcement** is enabled and use the **Virtual IP** option on the **GroupVPN** connector. This will require wireless users to first connect to the TZ 180 Wireless with the Global VPN Client, which then assumes an IP address on the LAN side of the TZ 180 Wireless. This ensures that any wireless user has been authenticated before they can access the LAN resources, and bypasses the WLAN to LAN restriction the Wireless Guest Services users are subject to.

Is the Wireless Radio in the TZ 180 Wireless Operating?

In rare instances, the radio inside the TZ 180 Wireless may not initialize correctly, resulting in all wireless users being unable to associate, even though LAN users are not experiencing any issues connecting through the TZ 180 Wireless. There are several ways to check the radio status. First, verify the TZ 180 Wireless front panel to see if the amber test light (the one with the wrench icon above it) is lit, or if the green on light is steadily flashing. If either of happening, unplug the power cable from the TZ 180 Wireless, wait a minute, then plug the power cable back in and wait for the test light to shut off. The second method is to check, using the management interface from a system on the LAN. If you can log into the TZ 180 Wireless and the management interface either hangs when clicking on the **Wireless** section, or the **WLAN Statistics** all report zero counts, this means that the wireless radio is not operating. If this happens, unplug the power cable from the TZ 180 Wireless, wait a minute, then plug the power cable back in and wait for the test light to shut off.

Is the Wireless System Attempting to Log Into an Active Directory Network?

Verify that the WLAN-to-LAN rule allowing access to the LAN resources has the advanced **Allow Fragmented Packets** checkbox enabled. Active Directory uses Kerberos as part of the login mechanism, and it is therefore necessary to allow the fragmented authentication packets to pass between the WLAN and LAN. It may help to activate NetBIOS pass-through from the WLAN to LAN and from WLAN to LAN; this option can be accessed by clicking on the **Advanced** button at the bottom right side of the firewall policy on the **Firewall/Access Rules** section. Verify that the wireless systems are using internal WINS/DNS for resolution or manual HOSTS/LMHOSTS entries for the LAN-based systems that need to be accessed.

Is the Preamble Length Set Correctly?

Most of the newer 802.11b wireless cards and drivers are capable of using **Auto** or **Short** preambles, which are faster and more efficient than the older **Long** type of preamble. Some older cards and drivers may not understand short preambles, so it may be necessary to set this option to **Long** in order for them to associate. Preamble length is a global setting, so all wireless cards associating with the TZ 180 Wireless will need to use the same setting.

Global VPN Client

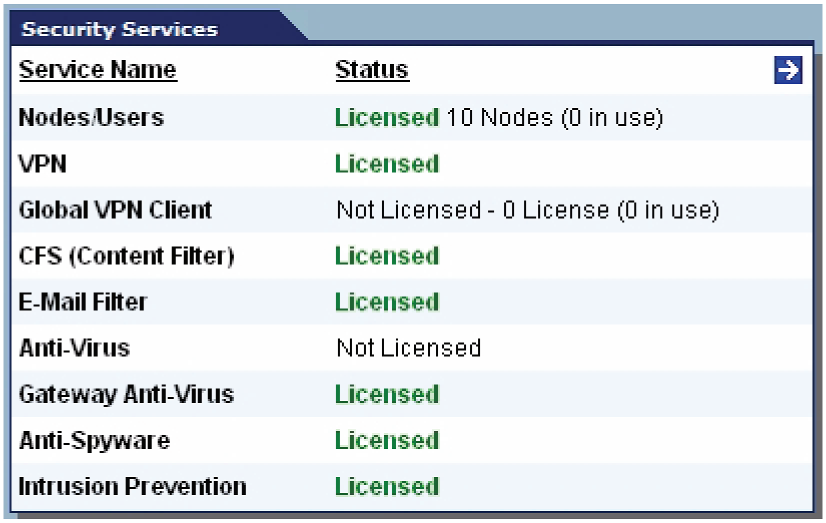
Symptom: GlobalVPN Clients Are Unable to Access the Server on the OPT Interface

Select the radio button on the GroupVPN policy's **Advanced** tab to allow the tunnel to terminate at the LAN/OPT interface; by default, it only attaches to the LAN interface. Verify that the GroupVPN policy is enabled.

Symptom: I Cannot Get the Global VPN Client Working

Verify that the TZ 180 Wireless has licenses for the GlobalVPN client. The appliance does not have default licenses for SonicWALL's Global VPN client (GVC), so the appropriate licenses must be purchased and installed. Navigate to the **System > Status** page and review the **Security Services** section. As an example, the TZ 180 Wireless shown in Figure 11 does not have GVC licensed.

Figure 11 TZ 180 Wireless with No Global VPN Licenses



Security Services

Service Name	Status
Nodes/Users	Licensed 10 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Not Licensed - 0 License (0 in use)
CFS (Content Filter)	Licensed
E-Mail Filter	Licensed
Anti-Virus	Not Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed

Verify that You Have Not Exceeded the Active License Count

Licenses for the Global VPN client are used on a concurrent basis and not on a per-user basis, which means while you may have 40 unique users installed, if you only had a 10 user GVC license, only 10 of those users could connect at once. Determine the maximum "peak" number of users and plan appropriately. You do not need to get a license for every unique user, but you do need enough licenses to support your peak of concurrent users.

Verify that GVC Is Enabled

Navigate to the **VPN > Settings** page and verify that the box next to **Enable** is checked, then click the **Apply** button in the upper-right-hand corner. Verify that global VPN capability is enabled.

Verify that the GVC Policy is Configured Correctly

There are a number of important settings on this policy. It is recommended that you download the GVC technote from the SonicWALL support site at http://www.sonicwall.com, for full details on this topic.

Symptom: The GlobalVPN Client Asks for a Key on First Connection

Provide users with the shared secret key when using this feature. To simplify this, you can navigate to the **Advanced** tab and enable the **Use Default Key for Simple Client Provisioning** option, which allows users to only enter a username and password to connect.

Symptom: The GlobalVPN Client Displays a Tmeout with a DHCP Error

If you are using the Virtual Adapter, verify that the appliance is set for DHCP over VPN, and then verify that the appliance has a DHCP scope set up, or is pointed to an internal DHCP server that can issue an address to the GlobalVPN's Virtual Adapter. This is found on the **VPN > DHCP over VPN** page. Click the **Configure** button next to **Central Gateway** and specify if the appliance should assign from an internal pool or using an external DHCP server.

Symptom: The GlobalVPN Client Has Connectivity Issues or Reports Unusual Messages upon Failure

Visit the MySonicWALL portal to see if you are using the most current version.

Symptom: GlobalVPN Users Have Problems Accessing Microsoft Networking Resources over the Connection

Use a resolving mechanism such as WINS, Active Directory/DNS, or static HOSTS/LMHOSTS files for the GVC. The easiest solution is to provide the appropriate WINS and DNS entries in the DHCP scope, and to use the Virtual Adapter capability of the GroupVPN policy. The GlobalVPN clients receive the correct IP address in the DHCP lease.

Registration Troubleshooting

Symptom: I Am Having Registration Problems with the TZ 180 Wireless

Review the "Registering and Enabling Support" section on page 4, which provides instructions for registering the TZ 180 Wireless security appliance.

If you are attempting to use the Registration & Licensing Wizard, or the registration link on the **System > Status** page, there may be a connectivity issue. The most common issue is that the DNS address is not set properly. Navigate to the **Network > Settings** page and verify that the DNS is set to a valid, known-good DNS server that the appliance can reach. If you do not know your ISP DNS servers, you can use 4.2.2.1 and 4.2.2.2 temporarily. Also verify that the appliance is set to the proper time zone. The security appliance cannot contact the registration servers unless these settings are correct.

Verify that the Security Appliance Is Able to Connect to the Internet

Navigate to the **System > Diagnostics** page and use the **TraceRoute** utility to see if the appliance has a working connection, using a known-good public IP address or name on the Internet (for example, www.sonicwall.com).

Symptom: The Appliance Is Reporting that the Security Appliance Is Already Registered

If you get this message, the appliance is registered to another MySonicWALL account. If you have multiple accounts, login to each of your accounts to determine the appliance registration account. If you no longer know which account the appliance is registered to, contact SonicWALL technical support and ask for the appliance serial number to be unregistered.

Symptom: The Appliance Reports that the Connection Timed Out

During peak periods, the appliance may be unable to connect to the MySonicWALL portal. Wait 15 minutes before attempting to connect again.

VPN Troubleshooting

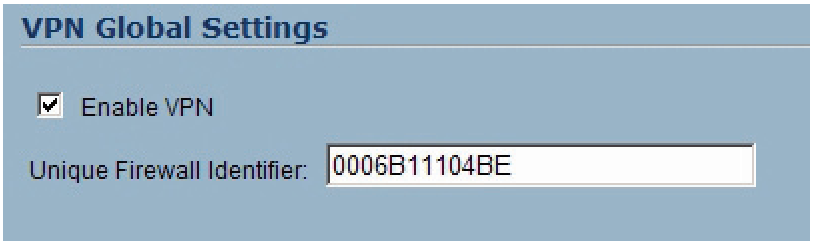
Symptom: I Cannot Get Site-to-Site VPN to Work

For a VPN tunnel to successfully negotiate, a number of settings must exactly match on both sides, otherwise the tunnel fails to negotiate. The following is a list of settings to verify on both sides.

Verify that the VPN is Enabled on the SonicWALL Security Appliance

VPN is enabled by default but can be shut off inadvertently. Navigate to the **VPN > Settings** page and verify that the checkbox next to **Enable VPN** is checked. Figure 12 provides a view of the VPN Global Settings section. Verify that the **Enable** checkbox to the right of your VPN Policy is also checked.

Figure 12 SonicWALL VPN Global Settings with UFI



VPN Global Settings

☑ Enable VPN

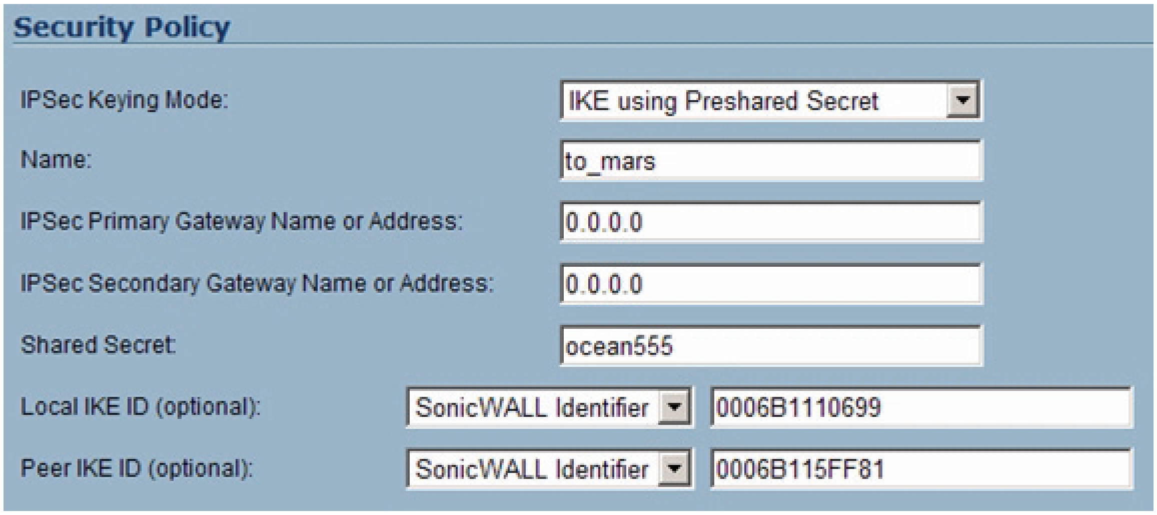
Unique Firewall Identifier: 0006B11104BE

Fix Incorrect UFI Settings

If one side of the VPN tunnel is a SonicWALL security appliance with a WAN IP address that is obtained dynamically, then Aggressive Mode must be used. For detailed information about configuring site-to-site SonicWALL security appliances for VPN tunnels, refer to *Configuring VPNs Between SonicOS Standard and SonicOS Enhanced* technote document.

When a SonicWALL security appliance negotiates Aggressive Mode VPN tunnels, it uses the Unique Firewall Identifier (UFI), illustrated in Figure 12, as its identity. Both sides must be set to know the other side's UFI. In SonicOS Standard, this is done by naming the VPN Policy with the remote peer's UFI. In SonicOS Enhanced, it is controlled by setting the Local and Peer IKE IDs, as illustrated in Figure 13, in the VPN policy's **General** tab.

Figure 13 SonicOS Enhanced: VPN Policy Aggressive Mode Using UFIs



Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: to_mars

IPSec Primary Gateway Name or Address: 0.0.0.0

IPSec Secondary Gateway Name or Address: 0.0.0.0

Shared Secret: ocean555

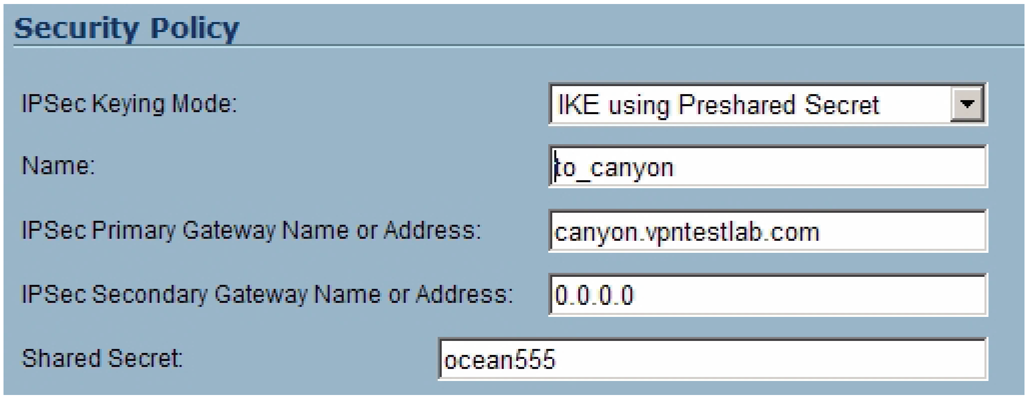
Local IKE ID (optional): SonicWALL Identifier 0006B1110699

Peer IKE ID (optional): SonicWALL Identifier 0006B115FF81

Navigate to the VPN policy **General** tab, verify that the **IPSec Keying Mode** is set the same on both sides, and verify that you are using the correct IP address or FQDN for the remote peer. Figure 14 provides a view of the Security Policy section. Verify that you have the same shared secret set on both sides.

Note The following log messages are additional indicators that you have used mismatched shared secrets: **Failed payload verification after decryption. Possible preshared key mismatch**, and **Received Notify: PAYLOAD_MALFORMED**.

Figure 14 VPN Policy General Settings



Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: to_canyon

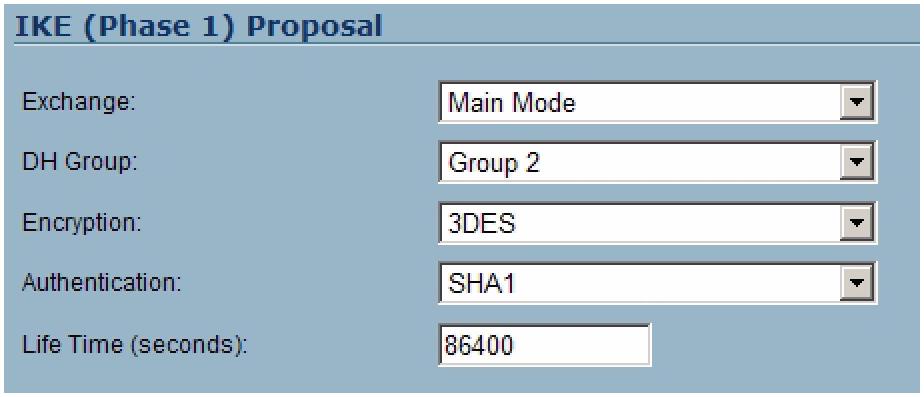
IPSec Primary Gateway Name or Address: canyon.vpntestlab.com

IPSec Secondary Gateway Name or Address: 0.0.0.0

Shared Secret: ocean555

If the SonicWALL security appliance logs display **NO_PROPOSAL_CHOSEN**, **IKE proposal does not match**, or **IKE negotiation aborted due to timeout**, the Phase 1 settings are probably incorrectly set on one or both sides. Most settings in the **Proposals** tab of the VPN policy must exactly match on each side, and if they do not match exactly, the tunnel fails in Phase 1 and Phase 2. The exception to this rule the **Life Time** setting; if these do not match, the VPN policy negotiates using the lower of the two settings. Figure 15 provides an example of Phase 1 setting.

Figure 15 VPN Policy Phase 1 Settings



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 86400

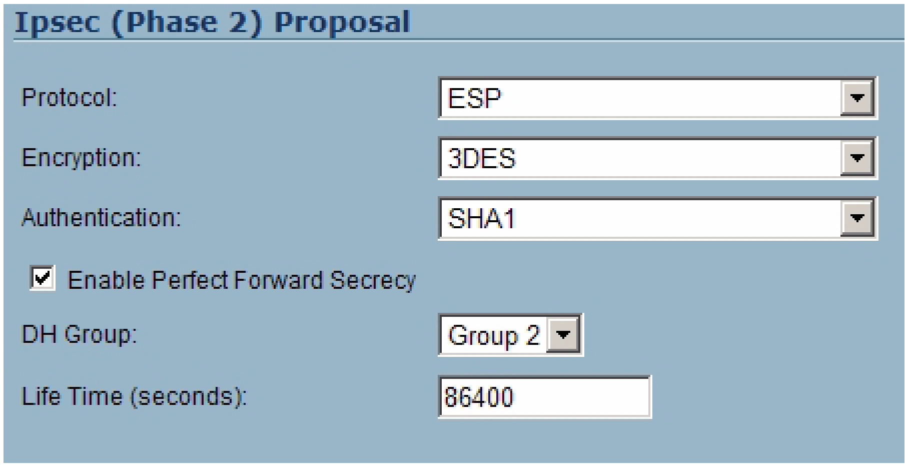
If you have implemented the troubleshooting solutions to this point with no success, there may be something between the two VPN devices that is blocking communication. If this is the case, verify that NAT Traversal is enabled on both SonicWALL security appliances, and that any firewall in between is set to pass UDP port 500 and UDP port 4500. If one of the sides is not a SonicWALL security appliance, it is necessary to open UDP port 500 and IP type 50, since NAT Traversal may not negotiate with the third-party security appliance.

Symptom: Phase 1 Settings Are Identical on Both Sides, but the Log Displays a Failure in Phase 2

For a VPN tunnel to successfully negotiate, most of the settings must exactly match on both sides. Below is a list of settings that must match.

Verify that both sides have their **Protocol**, **Encryption**, and **Authentication** settings set to match, or the tunnel fails. These settings are found by clicking the **Configure** icon next to the VPN policy and clicking on the **Proposals** tab. Figure 16 provides an example of Phase 2 settings.

Figure 16 Phase 2 Settings



Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☑ Enable Perfect Forward Secrecy

DH Group: Group 2

Life Time (seconds): 86400

Perfect Forward Secrecy (PFS) Mismatch - By default, PFS is disabled on SonicWALL security appliances. PFS is a security mechanism in IPsec that adds a layer of security to the VPN tunnel. To use PFS, check the box next to **Enable Perfect Forward Secrecy** on the VPN policy's **Proposals** tab, verify that the **DH Group** matches, and verify that the **Life Time (seconds)** field entry matches on both sides. If the **Life Time** settings do not match, the VPN policy negotiates using the lower of the two settings. Figure 16 provides a view of the **Life Time** field.

Incorrect destination network(s) -If an incorrect destination exists, for example, if one side of the connection has **Keep Alive** enabled and does not match one-to-one the destination networks configured on the peer, it displays the message **NO PROPOSAL CHOSEN**.

Missing 'Default LAN Gateway' Option - When running SonicOS Standard or Firmware 6.x on a SonicWALL security appliance at a main site, using the **Use this VPN Tunnel as default route for all Internet traffic** option (also referred to as tunnel-all mode), a LAN default gateway must be specified on the other side's VPN. This LAN default gateway cannot be the LAN IP address of the SonicWALL security appliance, and must be a separate internal router residing on the other side's LAN segment. To configure this feature, log into the main site's SonicWALL security appliance, navigate to the **VPN > Settings** page, click the **Configure** icon next to the VPN policy to the remote site that is set to tunnel-all to the main site, and click the **Advanced** tab. In the **Default LAN Gateway** field, enter the IP address of the third-party router on the main SonicWALL security appliance LAN segment. Click **OK**.

Note You do not need to update the Default LAN Gateway option when using SonicOS Enhanced.

Symptom: General, Phase 1, and Phase 2 Settings All Seem Correct on Both Sides but It Still Does Not Negotiate

There may be something in between the two VPN devices that is blocking communication. This can be hard to determine, since portions of the network path between the two VPN devices may lie underneath the control of external parties.

If this is the case, verify that NAT Traversal is enabled on both SonicWALL security appliances, and that any firewall, router or NAT security appliance in between is configured to pass UDP port 500 and UDP port 4500. If one of the sides is not a SonicWALL security appliance, it is also necessary to open UDP port 500 and IP type 50, since NAT Traversal may not negotiate with the third-party security appliance.

Symptom: The VPN tunnel Negotiated and Both Sides Show the Tunnel as Up, but I Cannot Reach Anything on Either Side of the Tunnel from the Other Side, Respectively

This problem can be the result of several factors, described below.

DHCP MTU Issues

If the SonicWALL security appliance WAN interface is receiving an IP address dynamically using DHCP, it may be necessary to lower the WAN interface MTU. DHCP is common among cable ISPs, and many of them require unconventionally low MTU settings.

Log into the SonicWALL security appliance management interface, navigate to the **Network > Settings** page, click on the **Configure** icon next to the WAN interface. On the page that displays, click the **Ethernet** tab, change the **WAN MTU** from 1500 to 1404, then click **OK**.

User-Level Authentication

Check the **Advanced** settings for the VPN policy to ensure that this feature is off (there are two checkboxes for **Require Authentication of Local Users** and **Require Authentication of Remote Users**.

TCP Settings

Some applications do not work with the default TCP enforcement settings on the SonicWALL. It may be necessary to deactivate one or more of these settings on both sides of the VPN tunnel.

Log into the SonicWALL security appliance management interface. Modify the management interface URL from **/main.html** to **/diag.html**, which opens the Diagnostics Settings Menu. When this menu displays, click on the **Internal Settings** button to the left and uncheck the box next to **Enable TCP Handshake Enforcement**. Click the **Apply** button in the upper-right-hand corner then click on the **Close** button in the lower-left-hand corner to return to the management interface.

Note In newer versions of SonicOS Standard, the checkbox for **Enable TCP Handshake Enforcement** is located on the **Firewall > Advanced** page.

Hardware Accelerated Cryptographic Miscalculations

If the VPN tunnel negotiates successfully but still does not pass traffic across the VPN tunnel, and the log is filled with **IPSec Authentication Failed** messages, the onboard hardware cryptographic acceleration chip may have not be processing traffic correctly.

To remedy this, log into the SonicWALL security appliance management interface.Modify the management interface URL from **/main.html** to **/diag.html**, which opens the Diagnostics Settings Menu. When the menu displays, click on the **Internal Settings** button to the left. On this menu, uncheck the boxes next **Enable inbound VPN hardware acceleration (if available)** and **Enable outbound VPN hardware acceleration (if available)**.

Click on the **Apply** button in the upper-right-hand corner, then click on the **Close** button in the lower-left-hand corner to return to the management interface. Restart the SonicWALL for the changes to take effect. With these settings disabled, the SonicWALL performs cryptography in software, which reduces VPN throughput but is still functional.

Note If disabling hardware cryptographic fixes the problem, contact SonicWALL technical support to arrange for further diagnostics.

Symptom: The VPN Tunnel Works but Needs to be Faster

A VPN tunnel is limited by the slowest point between the two links. This is often referred to as the chokepoint. For example, if you have a VPN tunnel between a central office that has a 1.5Mbps T1 connection to the Internet and a remote office that has a 256Kbps ADSL connection to the Internet, the VPN tunnel is going to be constrained by the ADSL connection speed and also by any traffic flowing in and out of that connection at any time (for example, if there is someone at the remote office downloading data in high volumes from the Internet, the VPN tunnel is likely to be even slower). Distance may also affect perceived throughput. The farther apart the two links, the slower it may seem, due to a number of factors, including latency, potential for packet loss and retransmission, or transient traffic in between the two points.

There are settings on the SonicWALL security appliance that may improve throughput.

Log into the SonicWALL security appliance management interface. Navigate to the **VPN > Advanced** page and check the boxes next to **Enable Fragmented Packet Handling** and **Ignore DF (Don't Fragment) Bit**. Click on the **Apply** button in the upper-right-hand corner then reboot the appliance for the changes to take effect.

For further assistance, refer to the *Site-to-site VPN Troubleshooting on SonicWALL Security Appliances* technote, available at:

http://www.sonicwall.com/downloads/site_to_site_vpn_troubleshooting_on_sonicwall_security_appliances.pdf

Internet Connectivity Troubleshooting

Symptom: I Do Not Have Internet Access from Behind the TZ 180 Wireless

Verify the WAN Interface on the Appliance Is Connected Properly to the Security Appliance Providing Internet Access

Verify the **Status** section of the **System > Settings** page to see if the link is down or has a duplex. It is recommended that the speed and duplex be locked on both sides of the connection to prevent auto-negotiation problems.

Verify that the WAN Interface is Set to the Correct Mode

Contact your ISP to determine if your public Internet connection is set for Static IP, DHCP, PPPoE, L2TP, or PPTP. If the connection is Static IP, the ISP needs to provide you with one or more public IP addresses, a netmask, a gateway IP, and one or more DNS server address for the TZ 180 Wireless to successfully connect to the Internet.

Determine if the Security Appliance Is Upstream of the TZ 180 Wireless Already Performing NAT

Contact your ISP to determine how their equipment functions. It may be that the ISP security appliance is already acting as a Firewall/NAT security appliance, and should be re-configured to allow the SonicWALL security appliance to connect to the Internet. This is an increasingly common issue as ISPs provide xDSL and cable modem equipment with 'all in one' functionality. You may need to purchase a generic xDSL or cable modem and swap out the ISP equipment if it cannot be configured to allow the SonicWALL security appliance to work properly.

Verify if the WAN MTU is Set Correctly for Your Type of Connection

You may need to change the WAN MTU setting, found on the **WAN interface Ethernet** tab, to a value appropriate to your type of connection. For example, set it to 1492 for DHCP connections, and 1404 for PPPoE connections.

Verify that the TZ 180 Wireless Can Contact the Upstream Gateway

Use the tools found on the **System > Diagnostics** page to determine if the connectivity problem is between the TZ 180 Wireless and the upstream gateway, or farther upstream. It may not be an issue with the TZ 180 Wireless, but with the ISP itself.

Verify that the Firewall and NAT Rules Are Configured Properly

Firewall rules can get changed or deleted inadvertently. Verify that the resources on the LAN and OPT interfaces have a rule allowing them to access the WAN. If there are resources on the OPT interface that have a unique public IP address, check the NAT rules.

Symptom: Users on the WAN Cannot Get to Servers on the OPT or LAN Interfaces, but the NAT/Firewall Rules Look Fine

Your ISP may be blocking specific inbound ports, which is an increasingly common problem. Contact your ISP. You may need to upgrade or replace your service to allow full connectivity.

Firmware Update Troubleshooting

Symptom: I Want to Update the Firmware on the TZ 180 Wireless

For users of SonicOS Standard, refer to the "Registering and Enabling Support" section on page 4 section of this document, as it covers the process of downloading and installing firmware for the SonicWALL TZ 180 Wireless security appliance.

If you are upgrading to SonicOS Enhanced, refer the *SonicOS Standard to SonicOS Enhanced* technote on SonicWALL's support site.

Note Before upgrading, record the settings related to the security appliance. These settings will be manually re-entered when the appliance reboots with SonicOS Enhanced. Settings are not saved when upgrading to SonicOS Enhanced, and the preferences files between SonicOS Standard and SonicOS Enhanced are incompatible, and problems can arise if the proper upgrade procedure is not followed.

It is necessary to purchase a SonicOS Enhanced license. If you do not install the SonicOS Enhanced license prior to upgrading the security appliance, it boots in evaluation mode and connectivity is severely limited until a license is installed. You can purchase a license for SonicOS Enhanced from your reseller, channel distributor, or SonicWALL. The license must be installed and the appliance must be synchronized with the MySonicWALL portal before upgrading.

When installing SonicOS Enhanced the first time, select the **Reboot with factory defaults** option to ensure that the SonicOS Standard settings do not corrupt the security appliance preferences file. If the appliance reboots and the wrench light flashes amber for several minutes, you need to boot the box in SafeMode and then boot it with factory defaults. For more information, refer to the "Registering and Enabling Support" section on page 4.

SonicWALL Solutions Integration

Now that your TZ 180 Wireless has been successfully installed on your network, consider these other SonicWALL solutions that are designed for easy integration and quick deployment.

The following SonicWALL solutions are described in this section:

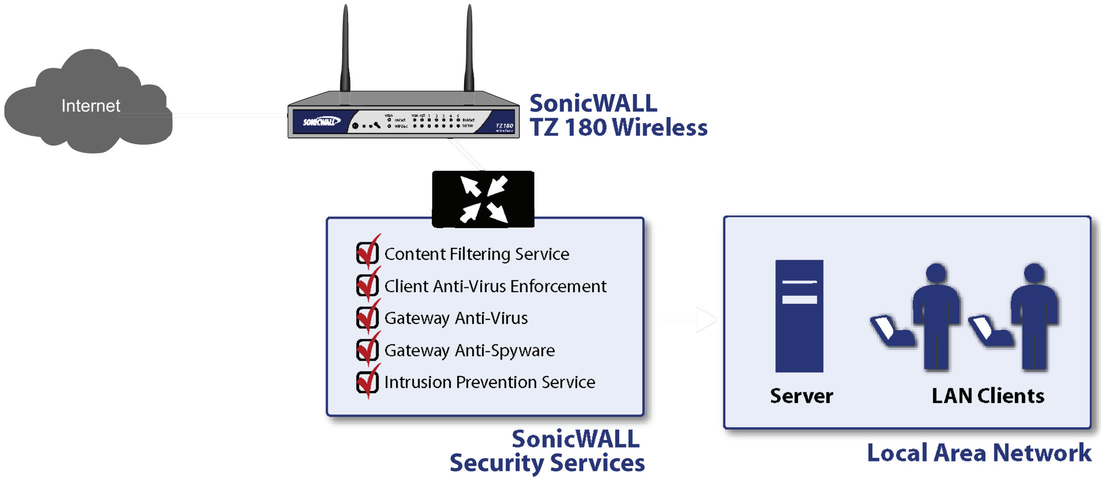
- SonicWALL Security Services, page 33
- SonicWALL Backup and Recovery Solutions, page 34
- SonicWALL Secure Remote Access Solutions, page 36
- SonicWALL Email Security Solution, page 37
- SonicWALL SonicPoint Wireless Access Points, page 38
- SonicWALL Global Management System (GMS), page 39

SonicWALL Security Services

There is an increasing number of gateway-based security services built right into SonicOS Standard and Enhanced, and you can maximize your TZ180 investment and security protection by subscribing to SonicWALL Unified Thread Management (UTM) services. These services require no extra software, just a software key for activating the features. With SonicWALL's security services, your network can be protected in a manner of minutes. Figure 17 provides the recommended deployment of SonicWALL security services with the TZ 180 Wireless security appliance.

To purchase and activate SonicWALL security services, log into the TZ 180 Wireless management interface and navigate to **Wizards > Registration & License Wizard**. The wizard walks you through the purchase and installation procedures. You can also purchase the security services from your reseller or channel distributor.

Figure 17 SonicWALL Security Services



SonicWALL Content Filter Service (CFS)

SonicWALL Content Filtering Service (CFS) provides businesses and schools with greater control to transparently enforce productivity and protection policies and block inappropriate, illegal and dangerous Web content. Featuring a dynamic rating and caching architecture, SonicWALL CFS blocks multiple categories of objectionable Web content, providing the ideal combination of control and flexibility to ensure the highest levels of productivity and protection.

For more information about CFS, refer to the *SonicWALL CFS Administrator's Guide*.

Enforced Client Anti-Virus and Anti-Spyware

Developed in partnership with McAfee, SonicWALL Enforced Client Anti-Virus and Anti-Spyware delivers enforced and auto-updated desktop protection through automatic system-wide updates of virus definitions, eliminating the need for time-consuming, machine-by-machine anti-virus deployments. Combining the enforced desktop security in SonicWALL Enforced Client Anti-Virus and Anti-Spyware with advanced server protection, the SonicWALL Client and Server Anti-Virus Suite leverages the award-winning McAfee NetShield and GroupShield applications for networks with Windows-based file, print and Exchange servers. By delivering very fast response during rapid virus outbreaks, SonicWALL anti-virus solutions reduce the time and costs associated with administering an anti-virus policy throughout your entire network.

For more information about SonicWALL Enforced Client Anti-Virus and Anti-Spyware, refer to the *SonicWALL Client-Server AV Product Guide*.

Gateway Anti-Virus Anti-spyware and Intrusion Prevention Service

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent, real-time network security protection against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows, as well as back door exploits and other malicious code.

As an added layer of security, this powerful solution provides application layer attack protection not only against external threats, but also against those originating inside the network. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service closes potential back doors by inspecting ba multitude of email, Web, file transfer and stream-based protocols as well as instant messaging (IM) and peer-to-peer (P2P) applications.

For more information about Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, refer to the *SonicWALL GAV 2.0 Administrator's Guide* and *SonicWALL IPS 2.0 Administrator's Guide.*

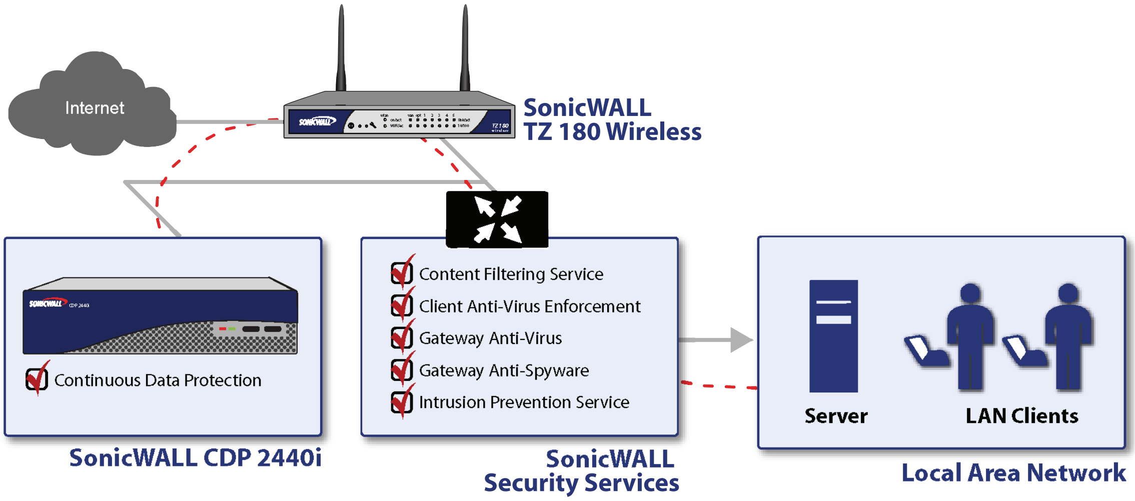
SonicWALL Backup and Recovery Solutions

SonicWALL Continuous Data Protection (CDP) is a tapeless, enterprise-level backup and recovery appliance that provides deep protection for businesses and remote offices. This hands-free, disk-based data protection solution provides automatic continuous data backup for servers, laptops and PCs, both locally and off site. By combining the advantages of local disk-based backup (instant recovery) with off site backup (insurance against local disasters), SonicWALL CDP is the first solution that eliminates, not just mitigates, exposure to threats of data loss. SonicWALL CDP also includes central management and remote administration features that enable IT administrators to more effectively and efficiently protect an organization's data.

SonicWALL's CDP1440i and 2440i appliances are ideal for TZ 180 Wireless-based networks. Install the CDP appliance directly into one of the LAN interfaces on the TZ 180 Wireless, install the software-based agents onto your servers and workstations, and immediately benefit from the protection that CDP provides. Figure 18 provides an example of the recommended deployment of a CDP 1440i or 2440i appliance with a TZ 180 Wireless security appliance.

For more information, refer to the *SonicWALL CDP Enterprise Manager Administrator's Guide.*

Figure 18 SonicWALL CDP Solution



Backup settings, firmware, and username and password files

As noted in the "Registering and Enabling Support" section on page 4, it is critical that you store known-good versions of TZ 180 Wireless firmware, settings files, and documents that detail the username and login information of the TZ 180 Wireless as well as the MySonicWALL account the security appliance is registered under. You can place these into a folder that the CDP Agent monitors, and then mark this file for the SonicWALL Offsite Backup service, ensuring backup of the files necessary for disaster recovery of your TZ 180 Wireless.

Backup remote users using GVC

As long as remote users can connect using SonicWALL GVC to the TZ 180 Wireless security appliance, they can synchronize their monitored folders and applications to the CDP 1440i or 2440i appliance.

Backup remote users across site-to-site VPN tunnels

You can maximize the purchase of your CDP 1440i or 2440i appliance by extending the backup and restore capabilities to systems on the other side of VPN tunnels. While it is faster to have a local CDP appliance for these systems, it is not feasible in many network environments.

Backup and restore SonicWALL's Global Management System (GMS)

You can use the SonicWALL CDP to create real-time snapshots and restore points for both the files and Microsoft SQL databases of SonicWALL's GMS. This can dramatically speed the restore and recovery time in the event that the GMS system become inoperable due to hardware or software failure.

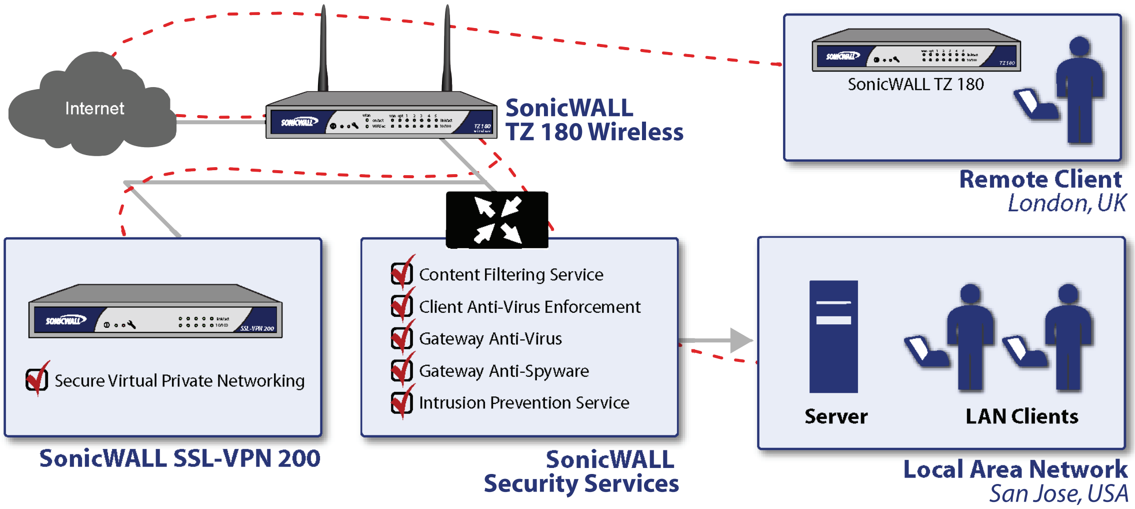
SonicWALL Secure Remote Access Solutions

The SonicWALL SSL-VPN series provides organizations of any size with an affordable, simple and secure clientless remote network and application access solution that requires no pre-installed client software. Utilizing only a standard Web browser, users can easily and securely access email, files, intranets, applications, remote desktops, servers and other resources on the corporate LAN from any location. SonicWALL SSL-VPN solutions integrate seamlessly into virtually any wired or wireless network topology to deliver powerful, scalable and affordable remote access to corporate resources.

For more information about SonicWALL SSL-VPN, refer to the *SonicWALL SonicOS SSL-VPN Administrator's Guide.*

The SonicWALL SSL-VPN 200 appliance is a perfect complement to your TZ 180 Wireless security appliance to add Web browser-based remote access and management for your users. Figure 19 provides an example of the recommended deployment using SonicWALL SSL-VPN and TZ 180 Wireless security appliance. The SSL-VPN 200 allows users to access their desktops, your internal servers, and many other network devices, from anywhere they need to – home, on the road, from a public Internet kiosk, and other remote locations – all without the need to install or constantly update a VPN client. You don't need a separate public IP address, because you can utilize the TZ 180 Wireless WAN IP address for access, or you can configure the IP to be dynamically obtained.

Figure 19 SonicWALL SSL-VPN Solution



The SSL-VPN 200 can be installed and configured in minutes. For example, configure the TZ 180 Wireless OPT port for NAT Mode and assign it an address of 192.168.200.2 with a netmask of 255.255.255.0. Then, deactivate any HTTP and HTTPS access firewall policies for the WAN interface, which is used to allow remote users to access to the SSL-VPN 200. Run the Public Server Wizard and specify the IP address of the SSL-VPN 200, 192.168.200.1 by default, and HTTP/HTTPS as the services to which access is provided. If the TZ 180 Wireless WAN IP address is dynamically obtained, use the DDNS feature to map a fully-qualified domain name (FQDN) to the IP address so your users can enter the FQDN (for example, sslvpn.ddnsservice.com) to access the SSL-VPN portal.

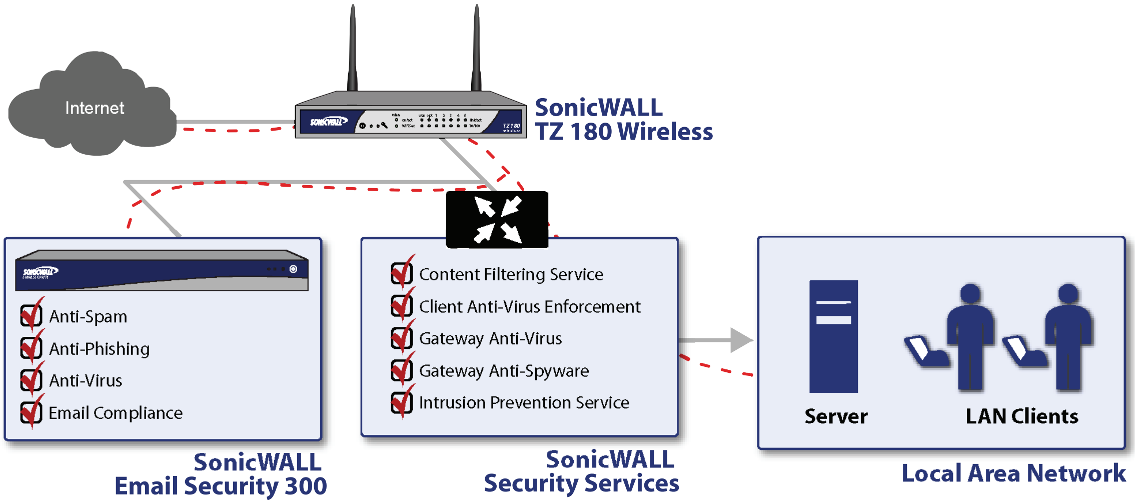
For information about detailed SSL-VPN configuration, including creating objects for users, refer to the *SonicWALL SonicOS SSL-VPN Administrator's Guide.*

SonicWALL Email Security Solution

SonicWALL Email Security provides effective, high-performance and easy-to-use inbound and outbound email threat protection. Ideal for organizations of any size, this self-running, self-updating solution delivers powerful protection against spam, virus and phishing attacks while preventing leaks of confidential information and violations of regulatory compliance laws.

If your internal SMTP-based email server is continually bombarded with spam, install a SonicWALL Email Security 200 or 300 server directly into one of the TZ 180 Wireless LAN interfaces. Figure 20 provides an example of the recommended deployment. Configure your internal SMTP server to forward outgoing mail to the ES server, and modify existing NAT rules so that incoming SMTP mail is forwarded to the ES server. The ES server has a wide array of licensable features that allow the server to scan incoming and outgoing mail for viruses using McAfee and Kaspersky anti-virus technology, scan for known spam and likely spam and phishing attempts, a full-featured compliance module for environments under HIPAA and SOX compliance rules, and extensive reporting features for both administrators and users.

Figure 20 SonicWALL Email Security Solution



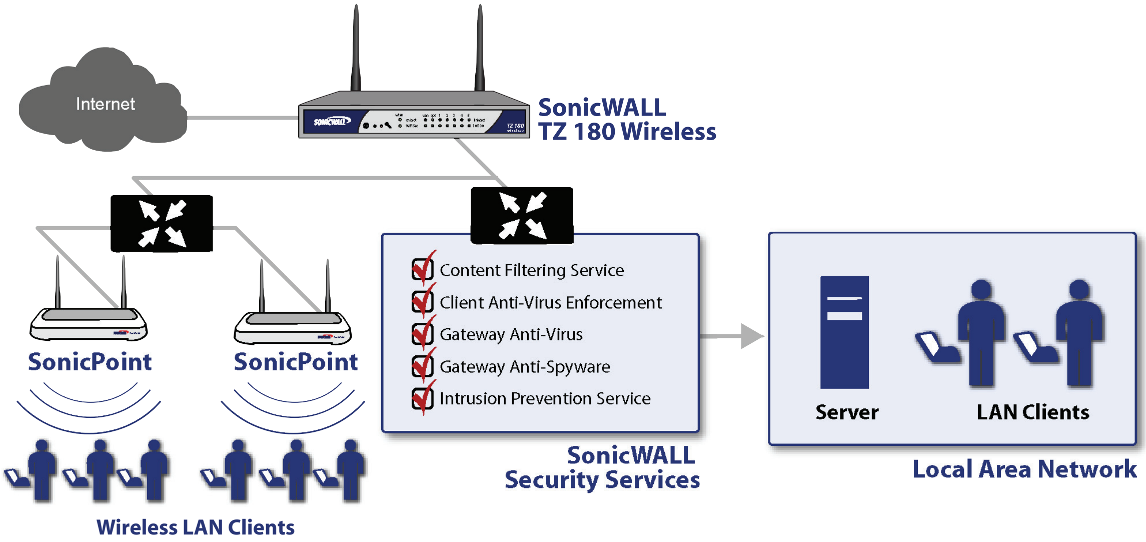
For more information about SonicWALL Email Security, refer to the *SonicWALL Email Security Administrator's Guide*.

SonicWALL SonicPoint Wireless Access Points

The SonicWALL Secure Distributed Wireless Solution is the first wireless networking security solution that integrates 802.11a/b/g wireless management and security enforcement into an enterprise-class firewall and VPN appliance. The innovative SonicWALL Secure Distributed Wireless Solution scales to fit virtually any network deployment by distributing SonicPoints at optimal locations throughout the building. Available in IEEE 802.11a/b/g and 802.11b/g options, SonicPoints are dependent access points that are utilized to provide seamless, secure wireless LAN (WLAN) connectivity as well as advanced features and services. SonicPoints can receive 802.3af power over Ethernet (PoE) to aid in their convenient deployment in any network.

You can add extensive wireless capability to your TZ 180 Wireless security appliance by upgrading to SonicOS Enhanced, which allows you to install up to eight SonicPoint or SonicPoint-G appliances on the OPT and DMZ interface. When combined with a Power over Ethernet (PoE) switch, you can provide power and connect the SonicPoints to the TZ 180 Wireless security appliance. SonicWALL's innovative central management system allows you to create shared wireless profiles on the TZ 180 Wireless security appliance, eliminating the need to individually configure each SonicPoint. Just plug them into the PoE switch and they automatically provision themselves with the newest firmware and settings files.Figure 21 provides an example of the recommended deployment of SonicPoints with a TZ 180 Wireless security appliance.

Figure 21 SonicWALL Wireless Solution

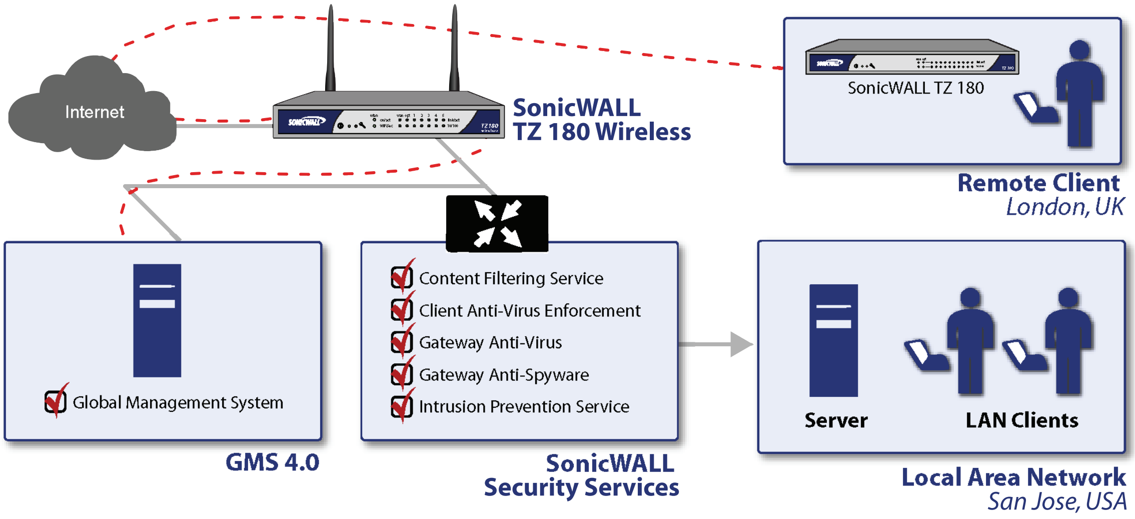


For more information about SonicWALL SonicPoints, refer to the *SonicWALL SonicPoint Administrator's Guide*.

SonicWALL Global Management System (GMS)

SonicWALL Global Management System (GMS) provides organizations, distributed enterprises and service providers with a flexible, powerful and intuitive tool to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations. Organizations can globally manage and collect detailed information from security applications such as gateway anti-virus, anti-spyware, intrusion prevention and content filtering, all from a single console. SonicWALL GMS enables organizations to reduce staffing requirements, speed deployment and lower costs. GMS comes with five security appliance license and can be expanded to handle hundreds, or even thousands, of SonicWALL appliances, including SSL-VPN, CDP, and Email Security. Figure 22 provides an example of the recommended deployment of SonicWALL GMS with a TZ 180 Wireless security appliance.

Figure 22 SonicWALL Global Management Solution



For more information about SonicWALL GMS, refer to the *SonicWALL GMS Administrator's Guide*.

Related Documentation

To access the SonicWALL technical reference library, visit the SonicWALL Web site at: http://www.sonicwall.com/us/support

For detailed information on configuring SonicOS Standard, refer to the SonicOS Standard Administrator's Guide, available at:

http://www.sonicwall.com/us/support/SonicOS_Standard_3.8_Administrator's_Guide.pdf

For detailed information on configuring SonicOS Enhanced, refer to the SonicOS Enhanced Administrator's Guide, available at:

http://www.sonicwall.com/us/support/SonicOS_Enhanced_3.8_Administrator's_Guide.pdf

For detailed information on configuring specific features, refer to SonicWALL's technical note library, available at:

http://www.sonicwall.com/us/support/

Obtaining Technical Support

If you require technical assistance for your TZ 180 Wireless for issues that this guide does not cover, refer to the resources available online at SonicWALL's North America support Web site at:

http://www.sonicwall.com/us/Support.html.

For international support Web sites, visit http://www.sonicwall.com and select the appropriate region or country, then click **Support** on the top navigation bar.

Also available is SonicWALL's interactive online Knowledge Portal:

http://www.nohold.net/noHoldCust22/Prod_3/Articles53234/sw_launch_frames.html.

If you cannot find an appropriate solution in the *SonicWALL TZ 180 Wireless Administrator's Guide*, or using a topic-based technote, you may contact SonicWALL Global Technical Assistance Center in your region at the telephone numbers listed in Table 2.

Table 2 SonicWALL Worldwide Support Phone Numbers

Country	Toll-free number	Local (toll) number
Calling from North America		
United States	+1 888.777.1476	
Canada	+1 888.777.1476	
Calling from Europe, the Middle East, and Africa (support available in English, French, German, Italian and Spanish)		
Austria		+43 (0) 820.400.105
Belgium		+31 (0) 411.617.810
Czech Republic		+31 (0) 411.617.810
Denmark	807.02.652	
Egypt		+31 (0) 411.617.810
Finland	800.77.0265	
France	0800.970.019	+31 (0) 411.617.812
Germany	0800.0003.668	+31 (0) 411.617.813
Ireland		+31 (0) 411.617.811
Italy	800.909.106	+31 (0) 411.617.814
Jordan		+31 (0) 411.617.810
Luxembourg		+31 (0) 411.617.810
Netherlands		0.411.617.810
Nigeria		+31 (0) 411.617.810
Norway	800.57.477	
Poland		+31 (0) 411.617.810
Russia		+31 (0) 411.617.810
Saudi Arabia		+31 (0) 411.617.810
South Africa		+31 (0) 411.617.810
Spain	900.811.056	+31 (0) 411.617.815
Switzerland	0800.562.221	+31 (0) 411.617.810
Sweden	+020.140.14.25	

Country	Toll-free number	Local (toll) number
Turkey		+31 (0) 411.617.810
United Arab Emirates	8000.4411.869	
United Kingdom	0800.0280.488	+31 (0) 411.617.811
All other countries		+31 (0) 411.617.810
Calling from Asia Pacific		
Australia		+1 800.35.1642
Hong Kong		+1 800.93.0997
India		+1 800.425.9255
Japan		+81 (0) 3.5460.5356
New Zealand		800.446489
Singapore		+ 800.110.1441
Calling from Latin America		
Brazil	0800.891.4306	
Mexico		+1 888.777.1476

Note Visit http://www.sonicwall.com/us/support/contact.html for the latest technical support telephone numbers.

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com

email: sales@sonicwall.com

Phone: (408) 745-9600

Fax: (408) 745-9300

Copyright and Trademarks

Copyright Notice

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

PN: 232-001110-00
Rev A 2/07