▷ SONICWALL TECHNICAL FAQ:

SonicWALL TZ 170 Wireless FAQ

OVERVIEW

How is the TZ 170 W different from the TZ 170, or the SOHO TZW?
The TZ 170 W incorporates 802.11b/g wireless networking capabilities into SonicWALL's TZ product line of home office/remote office and small business security appliances. The TZ 170 W adds a new type of network – the 'WLAN' interface (Wireless LAN), which terminates 802.11b and 802.11g wireless client connections. The WLAN port has full support for DHCP, NAT, stateful packet inspection firewall access rules, CFS, AV Enforcement, and Wireless Guest Services (WGS), which will be discussed at length in this document. It's also possible to enforce the use of the SonicWALL Global VPN Client on all wireless clients in order to authorize, authenticate, and encrypt all wireless traffic via IPSec (also referred to as WiFiSec). This method of deployment ensures that only authorized users are attaching to the TZ 170 W, and that the wireless traffic of authorized users is truly secure against capture and decoding from undesired third parties.

HARDWARE/SOFTWARE FEATURES

Can I run SonicOS Enhanced on the TZ 170 W?
Not at present, although SonicWALL will release a version of SonicOS Enhanced for the TZ 170 W at some point in the future. There is no ETA for this release; please check the MySonicWALL customer portal for firmware updates as the year progresses.

Can I import a prefs file from a SOHO TZW into a TZ 170 W?
You can, although it will import and report errors, and some settings will not be transferred since the hardware and prefs storing mechanisms are different in the two models. If you are replacing a SOHO TZW with a TZ 170 W, it's recommended that you manually copy over the settings from the SOHO TZW to avoid any potential issues.

Can I manage my TZ 170 W remotely using SonicWALL Global Management System (GMS)?
Yes, the TZ 170 W can be centrally managed using SonicWALL's award-winning Global Management System version 2.8 or newer.

Can I use my TZ 170 W with ViewPoint?
Yes, with Viewpoint 2.8 and newer.

What is the minimum firmware for the TZ 170 W?
The minimum level of firmware the TZ 170 W can run is SonicOS 2.6 Standard. The TZ 170 W does not support older SonicOS releases, or any of the older "6.x"-series firmware releases.

How do I get firmware for the TZ 170 W?
SonicOS 2.6 Standard is available to customers for 90 days after they have registered their devices on the https://www.mysonicwall.com customer portal, and for customers who have valid support contracts. After 90 days, customers must purchase a support contract in order to continue to receive firmware updates and new versions. When SonicOS Enhanced for TZ 170 W is released, it will also be available for download at mysonicwall.com for those that have purchased the SonicOS Enhanced Upgrade.

What is the difference between signed and non-signed firmware?
The TZ 170 W requires signed firmware images, unlike other SonicWALL Firewall/VPN devices. This is a new security mechanism added to the firmware to prevent tampering, and ensures that the image is both valid and originates from SonicWALL. Because of this, the TZ 170 W will not accept non-signed firmware images. All signed images end with a '.sig' extension.

Is there still a 'diag.html' page?
Yes. This page is kept to store configuration settings that are rarely used, and for extremely specific environments. Do not modify values on this page unless SonicWALL requests you do so.

Is the TZ 170 W ICSA-Certified?
SonicWALL has submitted the TZ 170 W for ICSA 1.1 IPSec and ICSA 4.0 Firewall certification and is currently awaiting approval (ETA Fall 2004).

Does the TZ 170 W support protocols other than IP?
No. The TZ 170 W can only process IP traffic and cannot process IPX/SPX, NetBEUI, AppleTalk, DECNet, LAT, or SNA traffic natively. In addition, when running SonicOS Standard, the TZ 170 W cannot pass GRE or Multicast packets. In order for the TZ 170 W to process such traffic, it must first be encapsulated into IP packets by another device before it reaches the TZ 170 W's interfaces, or it must be running SonicOS Enhanced (which, as noted elsewhere in this FAQ, is not currently available). PPTP is supported as a pass-through protocol if a specific rule is written for it.

Which routing protocols does the TZ 170 W support?
Support for routing protocols is limited in SonicOS 2.6 – at present, the device is only capable of using RIPv1 and RIPv2 to advertise networks, for security reasons. RIP advertisements may be enabled and configured on any interface (previously it could only be enabled on the LAN and DMZ). Support for default route advertisement has been added. For each interface, the user may configure RIP to:

- always advertise the default route.
- never advertise the default route.
- conditionally advertise the default route depending on the viability of the WAN connection (non-WAN interfaces only). This taps into the wan-failover logic to determine the viability of our WAN connection(s).

The user now has the choice of enabling or disabling advertisement of remote VPN networks that are accessible via the interface for which RIP is being configured. Remote VPN networks will only be advertised when the remote address object is of the type "Network". "Range" and "Host" networks cannot be advertised. When advertisement of static routes is enabled, RIP will advertise all accessible routes, regardless of the route's egress interface. Previously, only routes that egressed out of the WAN interface were advertised. Intra-zone route advertisement (for devices running SonicOS Enhanced) will be consistent with the configuration of intra-zone communication on the 'Network >Zones' page. Dynamic routing support will be expanded in future releases of firmware.

Does the TZ 170 W have a console-port?
Yes, it has a single RJ-45 console port. The TZ 170 W Unrestricted-Node model ships with a RJ-45 to DB-9 serial cable to allow you to attach a workstation to the console port. In addition, the SonicOS Enhanced upgrade for TZ 170 W includes a RJ-45 to DB-9 serial cable. The settings for the console port are 9600 bits per second, 8 data bits, No parity, 1stop bit, and no flow control. These settings cannot be modified at present. With SonicOS 2.6 Enhanced, the CLI attached to the console port is much more functional than in previous versions of firmware. The CLI's capability will be greatly expanded over the next six months.

I lost the RJ-45 to DB-9 serial cable – where can I get a new one?
You will need to contact SonicWALL tech support in order to obtain a replacement serial cable. Alternately, you can make one, using the pinouts listed below:

DB-9 Side	RJ-45 Side
1	2
2	5
3	6
4	3
5	4
6	not used
7	8
8	7
9	1

Can I operate my TZ 170 W with the cover removed?
NO! Operating the TZ 170 W with the cover removed can cause permanent damage to the processor and motherboard, and void the warranty. Do not power up your TZ 170 W with the cover removed.

What are the interfaces on the TZ 170 W?
- LAN - 5 port 10/100 Mbps switch; port 1 is a dedicated 802.3af PoE port
- Opt. Zone – 1 port 10/100 Mbps port (NOTE: disabled in SonicOS 2.6 Standard)
- WAN – 1 port 10/100 Mbps
- WLAN – up to 11Mbps 802.11b, up to 54Mbps 802.11g

Are all of the fixed Ethernet interfaces on the TZ 170 W AutoMDIX-capable?
Yes, all Ethernet interfaces are capable of automatically sensing polarity and adjusting to the cable type attached to the interfaces (i.e. straight-through or crossover). Users are now free to attach either type of cable to the interfaces when connecting the TZ 170 W. Please note that if auto-negotiation of speed and duplex is disabled on a port, it will also disable AutoMDIX.

Can I individually set the speed and duplex of the LAN switch's 5 ports?
No, this is not possible. The speed and duplex configuration settings for the LAN interface apply to all five ports.

Can I hook a hub or switch up to the TZ 170 W's switch ports?
Yes, you can cascade hubs/switches off any interfaces on the TZ 170 W.

What are the physical specs for the TZ 170 W?
- Dimensions: 9.07 x 6.80 x 1.63 inches (23.03 x 17.27 x 4.14 cm)
- Weight: 1.40 LBS
- Power Supply: 5V, 2.4A; 12W
- Input Power: 100-240VAC, 50-60Hz, 600mA
- Max Power: 10.5W
- Environment: Temperature: 40-105 °F, 5-40 °C, Humidity: 10-90% non-condensing
- Regulatory: EMC: FCC Class B, ICES Class B, CE, C-Tick, VCCI, BSMI, MIC
- Safety: UL, cUL, TUV/GS, CB, NOM
- MTBF: *TBD*
- Total Heat Dissipation: 35.8BTU
- Antenna: 5dBi
- RF output power: 19dBm/79mW (6–24Mbps), 17dBm/50mW (24-54Mbps)
- Radio Receive Sensitivity: (-86,-78,-70,-68) dBm at multiple (6, 24, 48, 54) Mbps
- Fan: 5.2CFM, 18dB(A) Ultra Quiet Fan

How much memory is on the TZ 170 W?
The TZ 170 W contains 8MB of onboard, non-upgradeable flash, and 64 MB of onboard, non-upgradeable RAM.

What kind of processor does the TZ 170 W use?
The TZ 170 W uses a multifunction MIPS RISC-based security processor that handles all processor-based I/O functions, as well as all crypto functions (3DES, AES, MD5/SHA-1, DH, and ESP) directly in hardware. This significantly speeds all crypto functions for VPN traffic.

What does the 'Opt. zone' interface do?
If the TZ 170 W is running SonicOS 2.6 Standard, the 'Opt. Zone' interface is disabled and cannot be used. A future release of SonicOS Enhanced for the TZ 170 W will enable this interface and allow it to be used as an additional internal interface, as a DMZ interface, or as a secondary WAN interface.

Can I run the TZ 170 W in transparent mode?
No, If the TZ 170 W is running SonicOS Standard, this is not possible.

Can I change the default IP address of the LAN interface?
Yes. The devices ship with 192.168.168.168/24 as the default IP address, for the LAN interface but can be changed to any value. Please note that the new value will take effect as soon as the 'OK' button is clicked, so you will need to change the IP address of your management station to match the new IP subnet of the LAN interface, and then log back into the device to continue device setup.

Can I assign multiple IP addresses to the LAN interface?
Yes, as long as they are from unique subnets.

How long does it take for the TZ 170 W to start up?
The average startup time from power-on to operation is approximately one minute. The device performs a number of hardware and software diagnostic check routines upon warm and cold boots to ensure the device, wireless radio, and firmware are fully operational.

Where should I install the TZ 170 W?
You can install it anywhere you wish, as long as the TZ 170 W is placed in an area where the largest number of wireless users have the best "point a to point b" path to it. In most buildings, the ideal location for a TZ 170 W would be to centrally mount the device on the ceiling. If this is not possible, it is advisable to mount the TZ 170 W on a high surface such that the two antennas are not blocked by environmental factors (walls, cubicle dividers, steel I-beams, etc). Please refer to the SonicWALL whitepaper "Wireless Site Survey and Placement Guide" (http://www.sonicwall.com/services/pdfs/SonicWALL_SOHO_TZW_Wireless_Site_Survey_Placement_Guide.pdf) for a more detailed discussion of this topic. When installing the TZ 170 W, please take care not to block or obstruct the internal fan port on the top of the unit, as doing so may cause the device to overheat and/or fail.

Can I set up VPN tunnels to older SonicWALL devices?
Yes – all versions of SonicOS are backwards compatible with all previous VPN-capable versions of SonicWALL firmware.

Can I set up site-to-site VPN tunnels from the TZ 170 W to third-party VPN devices?
Yes, as long as the other device supports manual IPSec or IKE IPSec. This would include all other IPSec-capable SonicWALL models, and devices from other manufacturers.

Is User-Level Authentication (ULA) supported in SonicOS 2.6 Standard?
Yes – there's a check box on the 'Users > Settings' page that, when checked, will force all systems on the LAN and OPT interface to log into the TZ 170 W and authenticate with a username and password before any traffic is allowed to pass across the device. ULA is also supported in SonicOS 2.6 Enhanced, but is configured in a different manner (instead of an all-or-nothing mechanism, ULA is enforced on a fully granular, per-rule basis between security zones).

I have AV enabled on an interface, but I can't seem to install the client on my system – why?
The AV installation is done via browser and relies on a pop-up window to install properly. If you are not able to install the SonicWALL AV Client on a system, check to see if the system's web browser is actively blocking pop-ups, or that it does not have a third-party program (such as 'Pop-Up Stopper') that is blocking the AV installation screen. In order to install the SonicWALL AV Client, you must allow pop-ups during this process.

How many remote access VPN sessions are supported by the TZ 170 W?
The 25-node and Unrestricted-node versions ship with a license for one concurrent remote access VPN session, and must be upgraded with SonicWALL Global VPN Client licenses to accept incoming connections. Both versions can support up to 50 concurrent remote access VPN sessions, when properly licensed. The term "remote access VPN session" refers to an IPSec connection to a unique remote SonicWALL Global VPN client.

How many site-to-site VPN policies are supported by the TZ 170 W?
The 25-node and Unrestricted-node models each support 10 site-to-site VPN sessions. Please note that while the license will limit connections to the number of unique remote peers, it does not limit the number of destination networks (phase two SA's) that can be negotiated for each remote peer (that number is only limited by the amount of free memory on the device). The term "VPN policy" refers to an IPSec connection to a unique remote site-to-site VPN peer, such as another SonicWALL device, or an IPSec-capable 3rd party device.

Can I assign multiple public IP subnets to a WAN interface?
It is not currently possible to assign more than a single IP address to a primary or secondary WAN interface, but the device is capable of answering on behalf of a 1-2-1 NAT policy set up for a network resource. This would be useful in environments where and ISP has assigned a customer multiple dissimilar public IP subnet blocks, and the customer wishes to use IP's from these dissimilar blocks to provide access to internal network resources. What is required is for the ISP's upstream routing be capable of routing these subnets to the fixed IP address of the primary or secondary WAN interfaces of the SonicWALL.

Is there an easy way to erase the config file on the TZ 170 W?
This is done from the 'System > Settings' menu by booting the box with the 'Current Firmware with Factory Default' settings button. All stored settings (including username, password, and LAN IP address) will be discarded and the device will reboot with factory settings (username: admin, password: password, LAN IP Address: 192.168.168.168).

Is there an easy way to erase the firmware on the TZ 170 W?
Simply load a new version and boot that one instead – the previous one will be erased and replaced with the new version. If the process fails, the device will boot into the SafeMode menu.

What is SafeMode?
SafeMode is a feature of the SonicOS Standard & Enhanced firmware that allows firewall administrators to switch between firmware builds and revert to known-good versions in case a new firmware image turns out to cause issues. In cases of firmware corruption, the device will boot into a special GUI mode that allows the administrator to choose which version to boot, and also allows the administrator to run hardware diagnostics, view the bootlog, or export the bootlog to a file.

How do I access the SafeMode menu?
In emergency situations, you can access the SafeMode menu by holding in the Reset button on the back of the TZ 170 W (it's the small pinhole button located to the left of the Console port) for 12-14 seconds until the 'Test' light begins flashing yellow. When the SonicWALL is booted into the SafeMode menu, assign a workstation a temporary IP address of '192.168.168.200' and attach it to a LAN interface on the TZ 170 W. Then, using a modern web browser (Microsoft IE6.x, Mozilla 1.4+), access the special SafeMode GUI using the device's default IP address of '192.168.168.168'. You will be able to boot the device using a previously saved image, or you can upload a new version of firmware with the 'Upload New Firmware' button.

WIRELESS

How many wireless clients can the TZ 170 W simultaneously support?
There are multiple factors that can affect how many simultaneous wireless clients are connected to the TZ 170 W, thus the number changes for each environment. The TZ 170 W's WLAN connection is hardcoded to 11Mbps half-duplex for 802.11b and 54Mbps half-duplex for 802.11g, so it would be important to factor in the connection speed of each client, transmission overhead, distance, sustained rate of transmission from each client, etc. Although both the TZ 170 W and the wireless clients may report that the connection is "11 Mbps" for 802.11b and "54 Mbps" for 802.11g, packet and signaling overhead limit any 802.11b connection to about 4-5Mbps, and any 802.11g connection to 802.11g to 22-24Mbps, so this also must be taken into consideration. If most of the wireless clients are within good range and are connecting at 11Mbps/54Mbps, it's advisable to lock the TZ 170 W to allow no more than 20-25 simultaneous users. The maximum number of unique client associations the WLAN port accepts is 255.

What radio chipset does the TZ 170 W use?

The TZ 170 W uses a Mini PCI onboard wireless radio based upon the Conexant 'PRISM GT/Frisbee' chipset. The power output for the wireless radio is adjustable. Maximum power output for the radio is 21dBm at 11Mbps, depending upon the regulatory domain the device is operating in. The radio's receive sensitivity at 11Mbps is –86dBm.

What type of antenna does the TZ 170 W use?

The TZ 170 W ships with two detachable 5dBi omnidirectional antennas, which can both be oriented in any direction. The antenna attachments on the back of the TZ 170 W are RP-TNC male connectors, rated for 50-Ohm impedance. Any third-party external antenna added to the device needs a RP-TNC female connector in order to connect to the TZ 170 W. Loss in the cable connector between the radio and the antenna connectors is approximately 1dB.

Why does the TZ 170 W have two antennas?

The TZ 170 W uses a method of tuning known as "antenna diversity" – this allows the TZ 170 W to lock on to the wireless client with the antenna receiving the clearest and strongest signal. While it is likely that both antennas can detect the same signal, it is probable that one of the two antennas is in a better position to lock onto the signal, due in part to placement issues, signal reflection issues, the positioning of the antennas, and the signal pattern characteristics of omnidirectional antennas. It's possible to deactivate antenna diversity if the TZ 170 W is running SonicOS 2.6 Standard or newer.

Can I attach external antennas?

Yes, you can. At present, SonicWALL does not manufacture or resell any type of third-party external antenna. SonicWALL has successfully tested HyperLink Technologies "HyperGain 2.4GHz" external antennas (http://www.hyperlinktech.com) with the TZ 170 W, although most third-party external 2.4GHz antennas should work if they have the correct antenna connector to attach to the TZ 170 W. For additional info, please refer to the SonicWALL whitepaper "Adding External Antennas to the SOHO TZW".

Will anything interfere with the TZ 170 W's signal?

Yes -- the 802.11b/g ISM band is subject to interference from multiple external sources -- 2.4GHz cordless phones, microwaves, and Bluetooth devices (especially these since they hop frequencies 1600 times faster than 802.11b/g devices). It may be necessary to move these devices away from the TZ 170 W and from any wireless clients that connect to the TZ 170 W to minimize the potential for signal interference.

How far does the TZ 170 W's 802.11b/g wireless signal reach?

Indoors, you can expect an 11Mbps signal to reach from 150 to 208 feet (40 to 63 meters), but this is entirely dependent upon building construction, environmental factors, and placement issues of both the TZ 170 W itself and the antennas of the wireless clients. The 802.11b/g signal can be significantly impeded by concrete or masonry walls, steel plating, water, people, and silvered surfaces. The signal can also be impeded by environments with an unusual amount of deflecting surfaces, such as an office with many cubicle partitions and filing cabinets. Also note that the speed of 802.11b/g signals degrades significantly over distance, so wireless clients located far from the TZ 170 W may only be able to connect at 1-2Mbps, if at all. Most wireless PC Cards, unfortunately, orient their antennas in an up/down fashion, effectively radiating half their signal straight into the desk surface. It may be necessary to install an external antenna on wireless clients experiencing connectivity difficulty, although sometimes re-orienting the antennas on the TZ 170 W helps resolve the issue. For an extended discussion on this topic, please refer to the whitepaper 'Wireless Site Survey and Placement Guide for TZ 170 W'.

Which wireless card should I use?

SonicWALL recommends its Long Range (802.11b) and Long Range Dual Band (802.11a/b/g) PCMCIA cards for use with the TZ 170 W.

Which third-party wireless cards work with the TZ 170 W?

Any WECA-certified card should work. Hybrid cards (a/b, b+, g, a/b/g) should be able to connect when operating in 802.11b/g mode.

Can wireless users seamlessly roam between TZ 170 W's?

The TZ 170 W does not currently support seamlessly roaming between separate TZ 170 Ws– it's possible to roam between TZ 170 Ws when using WiFiSec without having to manually log in again, but the disassociation and reassociation will interrupt application-level connectivity. If seamless wireless roaming is required, it is recommended that you instead use SonicWALL SonicPoints.

Is the TZ 170 W WECA-Certified?

No, it is not, although SonicWALL is investigating doing so.

Does the TZ 170 W support 802.11a?

No, the TZ 170 W only supports 802.11b/g. For environments that need to deploy 802.11a, we recommend the use of the SonicWALL SonicPoint wireless device, as it includes separate 802.11a and 802.11b/g radios in a single enclosure.

Does the TZ 170 W support 802.11 "b+"?

No, the TZ 170 W only supports 802.11b/g, but wireless cards that support 802.11 "b+" should be able negotiate a connection with the TZ 170 W at 802.11b/g speeds. The "b+" method is based upon a proprietary chipset from Texas Instruments and a different modulation scheme (PBCC). Most manufacturers do not support it.

Can I lock the TZ 170 W to do 802.11b only, or 802.11g only?

Yes, this can be set from the "Wireless > Settings' page on the TZ 170 W's management GUI.

Does the TZ 170 W support "Turbo G"?

No, it does not. However, the SonicWALL SonicPoint can be configured in Turbo mode for 802.11a and 802.11g, so if this feature is required, it is recommended you use the SonicPoint instead.

Can I attach SonicPoint devices to the TZ 170 W?

Not at present, but when SonicOS Enhanced for TZ 170 W is released it will be possible to attach up to two SonicPoint devices to the TZ 170 W's Optional port.

Does the TZ 170 W support WEP?

Yes, it supports WEP using key strengths of 64-bit, 128-bit, or 152-bit using ASCII or Hexidecimal keys, although use of WEP is strongly discouraged by SonicWALL due to weaknesses in the implementation of WEP. We instead recommend that you use WiFiSec when connecting to a SonicWALL SOHO TZW, TZ 170 W, or SonicPoint device.

What are the key sizes for WEP?

The TZ 170 W supports 64-bit and 128-bit keys, either in ASC-II character or hexidecimal format. Please note the TZ 170 W does not support WEP passphrases. You can enter in up to four unique WEP keys. When using these key sizes, you will need to note the following:

- If using a 64-bit alphanumeric key, use 5 characters
- If using a 64-bit hexidecimal key, use 10 hexadecimal digits
- If using a 128-bit alphanumeric key, use 13 characters
- If using a 128-bit hexidecimal key, use 26 hexidecimal digits

My wireless card configuration program asks for a WEP "passphrase" – what is this?

Some wireless card manufacturers support the use of a passphrase that the WEP keys are derived from, instead of requiring the administrator and enduser to enter in long, complex alphanumeric or hexidecimal keys. The TZ 170 W does not currently support this feature.

Is it true that WEP is unsafe?

Yes – due to a flaw in the construction of WEP, keys of any size (64,128,256,etc) can be compromised, and traffic data can be decoded by anyone who recovers the keys. There are several open-source tools posted around the Internet (most notably AirSnort and WEPCrack) that make the process a fairly trivial task.

Does the TZ 170 W support WPA?
Yes, it supports WPA-PSK, WPA-EAP-TLS, WPA-EAP-TTLS, and WPA-EAP-PEAP.

Can the wireless radio in the TZ 170 W use AES as well as TKIP for WPA?
No, just TKIP.

Does the TZ 170 W support 802.11i security mechanisms?

Not at this time. The 802.11i standard was only recently ratified, and it will be several months between ratification and delivery of a firmware upgrade that will allow wireless cards to connect using 802.11i. SonicWALL is currently investigating implementing 802.11i security mechanisms in a future firmware release. It's recommended that you periodically check SonicWALL's support site for updated firmware as the year progresses.

Does the TZ 170 W support 802.1x security mechanisms?

802.1x refers to the mechanisms for securely authorizing wireless users against a common database. At present, there are several competing methods – EAP-MD5, EAP-TTLS, EAP-TLS, LEAP, and PEAP. Most of these methods are fairly complex as well as proprietary, and many of them require the use of digital certificates. Since these are not standards, SonicWALL relies on proven IPSec technology built into the new Global VPN client to securely authorize wireless users against an internal user database, or against external RADIUS servers.

Does the TZ 170 W support 802.11d?
Yes, it does, although at present the user cannot select which regulatory domain to operate in (it's automatically set in firmware).

What exactly is 802.11d?
802.11d compliance is a regulatory domain update wherein physical and MAC layer signaling automatically behaves in accordance with geographic requirements for such settings as channels of operation and power. Access Points and wireless clients implement 802.11d differently; the Access Point can be thought of as the 802.11d provider, wherein it either provides the 802.11d capability or not – the Access Point remains agnostic to the 802.11d capabilities of associated clients. The wireless client is in turn the 802.11d consumer – if the client is not 802.11d capable, it can associate with an Access Point regardless of its 802.11d capabilities. If the client is 802.11d capable, it can generally operate in one of three 802.11d modes:

- **None** – The wireless device will communicate with any other available wireless device, regardless of 802.11d compliance. This is useful for peer-to-peer (IBSS) networking which currently is not supported by the 802.11d standard.
- **Flexible** – The wireless device will communicate with any other available wireless device, and will abide by 802.11d information if it is presented.
- **Strict** – The wireless device will only communicate with devices that support the 802.11d standard.

Does TZ 170 W support 802.11e?
The current version of firmware/software does not support 802.11e QoS mechanisms, although a future version may support this. Please check SonicWALL's support sites for updated versions of the card's firmware/software as the year progresses.

What happens if I enable 'WiFiSec Enforcement' on the TZ 170 W?

Activating this causes the TZ 170 W to pass only IPSec packets to and from its WLAN interface. All Wireless clients must connect to the TZ 170 W via the Global VPN Client if they wish to access anything (policy-allowed LAN resources, policy-allowed WAN access, other wireless clients). Enforcing WiFiSec ensures that wireless users are authenticated and that their wireless traffic is fully encrypted. Please note that if guest services are enabled along with WiFiSec enforcement, the traffic of authenticated guests will not be encrypted unless they too use the Global VPN client.

What does the 'Enforce WiFiSec for tunnel traversal' option do?

If this option is enabled, wireless clients cannot access resources across any WAN site-to-site VPN tunnel the TZ 170 W may have – unless the wireless clients first connect to the TZ 170 W with the Global VPN client. Enforcing this option ensures that the wireless clients have first been properly authenticated (via XAUTH), and that the wireless traffic is fully encrypted.

Do I need to enable any special settings to allow WiFiSec users to access resources across a WAN site-to-site VPN tunnel on the TZ 170 W?

Yes – you need to enable the advanced setting 'Forward Packets to Remote VPNs' on the 'GroupVPN' connector and on the policy for that site-to-site VPN.

What's an Association ID?

The TZ 170 W tracks all active wireless clients by issuing them an association ID and a timeout value. You can control the number of allowed active wireless clients by adjusting the 'Maximum Client Associations' in the Wireless/Advanced tab. When a wireless client disconnects or powers down, it will send a signal to the TZ 170 W to remove its association ID from the active 'Station Status' table. The TZ 170 W also has an adjustable 'Association Timeout' field, which can be manually adjusted in the Wireless/Advanced tab, in case a wireless client does not gracefully disconnect from the TZ 170 W. This feature prevents the active 'Station Status' table from filling up with wireless clients that may not, in fact, be active.

Why do I see high Association ID numbers on my TZ 170 W?

The TZ 170 W will increment Association ID numbers for each subsequent connection until it hits number 2006, at which point it will start reusing unused numbers starting from 1. This means that a TZ 170 W that has been powered on for some time may display what seem to be unusually large Association ID's, even though there may be only a handful of currently associated and active wireless users. This behavior is normal and is nothing to worry about.

What is Power Management?

Many wireless cards have a special software setting that reduces the transmit/receive levels in the radio, in order to conserve power usage (and in the case of battery-based systems such as laptops and PDA's, extend remaining battery lifetime). When power management is enabled on the wireless client, it goes into 'sleep' mode whenever wireless activity is low, but wakes up at regular intervals to verify whether there is network traffic addressed to it. When the TZ 170 W is associated with a wireless client with power management enabled, it buffers frames destined for that wireless client when it is in this 'sleep' mode, and transmits the destined frames when the wireless client signals to the TZ 170 W that it is active.

Does the TZ 170 W support Power Over Ethernet (PoE)?

Yes, this is supported on port 1 of the LAN interfaces. You can use the SonicWALL PoE Injector (North America Part #01-SSC-5531, International Part#01-SSC-5532) to provide power and network connectivity over a single CAT5/CAT6 cable over distances of up to 330 feet (100 meters). Both the SonicWALL TZ 170 W and the SonicWALL PoE Injector are 802.2af compliant. You may also use a third-party PoE device/injector, as long as it complies with 802.3af standards for Power over Ethernet.

What channel should I set my TZ 170 W to?

If you only have one wireless base station (i.e. a TZ 170 W, or another manufacturer's access point), you may set it to any selectable channel you wish. However, if you have more than one access point within several hundred feet of each other, signal overlap interference is likely to occur unless the access point channels are spaced appropriately. Due to the signaling mechanism in 802.11b/g, there is significant overlap across the eleven available channels - for instance, the signal for channel one overlaps the next four channels (two through five), and the signal for channel six overlaps the next four channels (seven through ten). This means that access points within range of one another must be set to channels that do not overlap. If you were to have two access points, you could set them to 1/6, 2/7, 3/8, 4/9, 5/10, or 6/11. If you were to have three access points, you could only set them to 1/6/11. However, SonicWALL recommends using the 'AutoChannel' feature in SonicOS 2.6 Standard that allows the TZ 170 W to automatically scan the channels, determine the best channel to use, and set itself.

What SSID should I use?

The SSID is used by the TZ 170 W to distinguish itself from other access points, and can be set to any 32-character setting you wish. By default the TZ 170 W uses a SSID of "sonicwall". We strongly recommend that you change the TZ 170 W's SSID to something non-descriptive and non-obvious.

I'm not ready to implement WiFiSec - what other TZ 170 W security features can I enforce?

The TZ 170 W has a number of 'deflective' security features that can be enabled to deter most attempts to gain unauthorized access to the TZ 170 W. The term 'deflective' is used because these methods do not truly ensure security – they just make it extremely difficult for anyone trying to compromise the TZ 170 W. The only true way to provide wireless security is enforcing WiFiSec usage across all wireless clients, but the methods below are better than nothing:

- You can remove the SSID from management beacon frames that the TZ 170 W sends out. This forces all wireless clients to manually enter the TZ 170 W's SSID into the settings before it can successfully connect.
- You can stop the TZ 170 W from responding to management probe request frames using a null SSID from wireless clients. Many wireless sniffing & cracking toolkits available on the Internet allow the wireless card to send out management probe request frames, which seek to force the access point (i.e. the TZ 170 W) to respond with its connection details. Enabling this feature causes the TZ 170 W to ignore and not respond to these attempts.
- You can use MAC filter lists on the TZ 170 W. By enabling this feature, the TZ 170 W does not allow wireless clients to associate unless the MAC address of that wireless client has been added to its internal 'allow' list.
- You can enforce the use of WPA on the TZ 170 W. By enabling this feature, all wireless clients must manually enter the WPA passphrase configured on the TZ 170 W.
- You can enforce the use of Wireless Guest Services (WGS). By enabling this feature, all wireless clients must authenticate themselves to the TZ 170 W via HTTP before they are allowed access to resources on the WAN. The user and password database can either be stored onboard the TZ 170 W, or the TZ 170 W can authenticate users from external RADIUS servers. Please see the section below on Wireless Guest Services (WGS).
- You can disable DHCP services on the WLAN interface. This requires all of your wireless clients to manually input the correct IP information, but it prevents unwanted wireless clients from obtaining DHCP lease information from the TZ 170 W. Alternately, you can configure DHCP services to only hand out leases to specific MAC addresses.

Can I turn on every single wireless security feature at once?

Yes, if you chose to, you could activate WiFiSec Enforcement, Wireless Guest Services, WEP, MAC Address Filtering, SSID Beacon hiding, and Unspecified SSID response blocking. However, this would probably create an administrative nightmare and is not recommended.

How many unique MAC addresses can I add to the 'MAC Filter List'?

You may enter up to 128 unique MAC addresses.

How does the Global VPN Client Licensing work on the TZ 170 W?

The Global VPN Client licensing is only enforced on the WAN port – not the WLAN port. All of your wireless users can use the Global VPN Client to securely connect to the TZ 170 W without having to purchase any extra license. However, if you wish to terminate Global VPN Clients on the WAN port (for example, users working from home via broadband connection, or dialed into an ISP POP), you must purchase separate Global VPN Client licenses.

Can I use Apple-based or Linux-based wireless clients with the TZ 170 W?

Yes – you may use any System/OS combination, as long as the wireless card in that system is compatible with the TZ 170 W.

Can I use wireless PDA's with the TZ 170 W?

Yes – you may to use any PDA/OS combination, as long as the wireless card in the PDA is compatible with the TZ 170 W.

Can I use other third-party VPN clients to connect to the TZ 170 W?

SonicWALL officially supports IPSec VPN connections to the TZ 170 W with the older SonicWALL VPN Client (versions 5.1.3 & 8.0) for Windows-based systems, the SonicWALL Global VPN Client (version 1.x and 2.x) for Windows-based systems, the Equinux VPN Tracker (version 1.0.2) for Apple OSX 10.2-based systems, and the Funk AdmitOne VPN Client (version 2.0) for PocketPC 2002-based systems. It may be possible to make a Manual IPSec or IKE IPSec connection with other third-party clients, but SonicWALL does not endorse or support their use. If the PDA is running Pocket PC 2003, you can use the built-in L2TP client to connect to the TZ 170 W's L2TP server; however, this feature is only supported if the TZ 170 W is running SonicOS 2.6 Standard or newer.

Can I set up site-to-site VPN tunnels from the TZ 170 W to other devices?

Yes, as long as the other device supports manual IPSec or IKE IPSec. This would include all other IPSec-capable SonicWALL models, and devices from other manufacturers.

How do I use Wireless Guest Services (aka WGS)?

This feature allows you to provide controlled, authenticated access to the resources the TZ 170 W controls. When activated, the TZ 170 W forces wireless users to authenticate themselves via HTTP web browser against an internal user database, or against an external RADIUS user database. All the user has to do is open a web browser and attempt to access any external site – the TZ 170 W intercepts the attempt and present a login screen for the user to input his/her username and password. If the username and password are correct, the user is granted access to the resource. This can be further controlled by the security policy in the TZ 170 W. Please note that activating WGS on the TZ 170 W requires activating MAC address filtering. WGS creates a temporary, unlisted 'permit' entry for the authenticated user for the duration of their connection, so it's not necessary for the administrator to have to manually input the guest's MAC address. In fact, if the administrator manually adds that guest's MAC address, then the guest would not then get prompted with the WGS login screen – they'd actually have unrestricted access – so make sure **not** to do this for your guest users.

There are two types of guest services accounts in the TZ 170 W -- you may choose between creating temporary, time-limited accounts that expire and disconnect based upon the duration you enter, or creating more permanent user accounts and granting them 'Wireless Guest Service' and 'WGS Easy ACL' permissions.

How many permanent user accounts can I create?

You can add up to 100 unique user accounts on the TZ 170 W.

How many WGS accounts can I create?

You can add up to 100 unique WGS accounts on the TZ 170 W. If you need to create more than 100 unique WGS accounts, you can assign the permanent user accounts WGS permissions, allowing for a total of 200 user accounts that have WGS permissions.

Is the TZ 170 W's wireless radio power adjustable?

Yes, there are four settings that control the signal strength of the TZ 170 W's internal wireless radio: High (23dBm), Medium (17dBm), Low (11dBm), and Lowest (1dBm). Please note that merely increasing the power in the TZ 170 W may not necessarily solve connectivity problems with wireless clients. Boosting the signal in the TZ 170 W only increases the TZ 170 W's signal strength – it does not make the TZ 170 W any more sensitive to weak signals emanating from the wireless clients themselves. Wireless clients experiencing difficulty connecting to the TZ 170 W as a result of distance issues, or environmental/blocking issues may need to replace their wireless cards with more powerful models.

Can I use a wireless print server with the TZ 170 W?
Yes. SonicWALL has successfully tested the TZ 170 W with the LinkSys "WPS 11" wireless print server, the HP "JetDirect 380x" external wireless print server, and the HP "JetDirect 680n" internal wireless print server. Please note that if you use the 'Enforce WiFiSec' feature in the TZ 170 W, you must use the new 'WEP-on-Demand' security feature for the wireless print server(s), since they are incapable of running any sort of IPSec client.

How do I adjust the TZ 170 W's Wireless 'Advanced Options'?

- Hide SSID in Beacon. Activating this feature removes the TZ 170 W's SSID from the management frame beacons it sends out. By default, the TZ 170 W broadcasts a beacon 10 times a second, although this is adjustable (see below). The beacon is used by unassociated wireless clients to obtain the necessary information to properly associate with the TZ 170 W. Removing the SSID from the beacon forces the wireless clients to manually input the SSID in order to properly associate. In environments where security is critical, it may be preferable to activate this option, but also note that some wireless card drivers may not work if this is activated.

- Transmit Power. This drop-down box can be used to change the power output of the TZ 170 W's wireless radio. The four settings (High – 23dBm, Medium – 17dBm, Low – 11 dBm, Lowest – 1dBm) control the signal strength and distance the signal travels; lower settings will result in a smaller coverage area. The standard rule of thumb for ideal wireless signaling conditions is that for every increase of 6dBm, coverage doubles, and for every decrease of 6dBm, coverage is halved. Thus, the High, Medium and Low settings for the TZ 170 W are defined such that a High setting gives the normal coverage as outlines in the Table below; the Medium setting will half the coverage and the Low setting will reduce the coverage by one fourth.

- Preamble Length. Most of the newer 802.11b/g wireless cards (and their drivers) are capable of using 'short' preambles, which are more efficient (and faster) than the older 'long' type of preamble. Some older cards (and older drivers) may not understand short preambles, so it may be necessary to set this option to 'long' in order for them to associate. Please note that this is a global setting, so all wireless cards associating with the TZ 170 W must use the same setting.

- Fragmentation Threshold. This setting can be used to increase wireless performance if a large number of collisions are occurring on the TZ 170 W WLAN interface. By default the threshold is set to 2346 bytes, effectively disabling fragmentation capability. Lowering the threshold causes the TZ 170 W to fragment all frames larger than the new setting. As smaller frames are generally less susceptible to interference (and also less likely to produce collisions) the number of retransmissions are reduced, and more bandwidth becomes available.

- RTS Threshold (bytes). This feature allows the TZ 170 W to reduce wireless traffic contention issues. Wireless networks are extremely susceptible to the "hidden node" problem – where two wireless stations are attempting to transmit at the same time without knowledge of one another. Activating RTS/CTS may improve performance on networks where this is occurring, by requiring the wireless client to first send a Request to Send (RTS), and then waiting for the TZ 170 W to issue a Clear to Send (CTS) before it transmits the frame. By default the threshold is set to 2432, effectively disabling RTS/CTS capability. Lowering the threshold causes the TZ 170 W to require a RTS/CTS exchange for all frames larger than the new setting.

- DTIM Interval. The DTIM (Delivery Traffic Information Map) is the interval for how often a wireless client in 'sleep' mode wakes up to poll the TZ 170 W to see if there are any buffered frames for it. The default setting is 3, but it can be adjusted from 1 to 65, 535. Increasing the DTIM interval allows wireless clients to conserve more power.

- Station Timeout (seconds). This feature allows the administrator to control the time before the TZ 170 W kicks out an inactive wireless client. Most of the time, wireless clients signal to the TZ 170 W that they wish to gracefully disassociate, but there may be situations where this does not occur, and the TZ 170 W is not aware that the wireless client is disconnected. The default is 300 seconds, and generally does not need to be adjusted – when associated, any traffic to and from the wireless client constantly resets this value in the TZ 170 W. In environments where a large number of wireless clients contend for a small number of allowed wireless connections on the TZ 170 W, it may be desirable to decrease the timeout period.

How do I interpret the 'WLAN Statistics'?

- Unicast Frames. This counter displays the number of frames received (Rx) and transmitted (Tx) by the TZ 170 W.

- Multicast Frames. This counter displays the total number of frames received and transmitted by the TZ 170 W as broadcast or multicast (destined at multiple other devices). This counter will typically be higher than the Unicast Frames Counter.

- Fragments. This counter displays the total number of frame or frame fragments sent and received by the TZ 170 W. The running rate of this counter is a general indication of activity at this wireless device. The value within the Rx column of this counter should be greater than the sum of the Unicast and Multicast Rx columns, and the value within the Tx column should be greater than the sum of the Unicast and Multicast Tx columns.

- Unicast Octets. This counter displays the total number of bytes received and transmitted by the TZ 170 W as part of unicast messages.

- Multicast Octets. This counter displays the total number of bytes received and transmitted by the TZ 170 W as part of multicast messages.

- Deferred Transmissions. This counter displays the number of times the TZ 170 W deferred a transmission to avoid collisions with messages transmitted by other devices. Deferral is normal behavior for 802.11 devices, and a high value is to be expected.

- Signal Retry Frames. This counter displays the number of messages that were retransmitted a single time before being acknowledged by the receiving device. Retransmission is a normal behavior for the IEEE 802.11 protocol in order to recover quickly from lost messages. A relatively high value for this counter in comparison with the Fragments counter suggests wireless interference, or a heavy wireless data load.

- Multiple Retry Frames. This counter displays the number of messages that were retransmitted multiple times before being acknowledged by the receiving device. Retransmission is a normal behavior for the IEEE 802.11 protocol in order to recover quickly from lost messages. A relatively high value for this counter in comparison with the Fragments counter suggests wireless interference, or a heavy wireless data load. Excessive Multiple Retry Frames result in lower throughput for the TZ 170 W as the system falls back to the next lower transmit rate when more than one retransmission retry is needed to transfer a message.

- Retry Limit Exceeded. This counter displays the number of messages that cannot be delivered after the maximum number of retransmissions. This counter together with Discards can be used to identify a wireless network that is overloaded due to severe interference or excessive load of wireless data traffic. The system drops such frames and relies on the upper layer communication protocols to recover from the losses.

- Discards. This counter displays the number messages that could not be transmitted due to congestion. In normal situations, the TZ 170 W temporarily stores messages that are to be transmitted in an internal buffer. When this buffer is full, frames will be discarded until buffer space becomes available again. When this counter is relatively high, this may identify a wireless network with a heavy load of wireless data traffic.

- FCS Errors. This counter displays the number of received frames or frame parts that contained an erroneous checksum requiring deletion. In the IEEE 802.11 protocol, such messages are recovered by the ACK (Acknowledgment) protocol and then retransmitted by the sending device.

- Discards: No Buffer. This counter displays the number of times an incoming message could not be received due to a shortage of receive buffers. A non-zero value identifies heavy data traffic for your wireless network.

- Discards: Wrong SA (Station Address). This counter displays the number of times a message transmission was not done because a wrong MAC address was used by the protocol stack. A non-zero value indicates an error situation in the communication between your driver and the protocol stack.

- Discards: Bad WEP Key. This counter displays the number of times a received message was discarded because it cannot be decrypted. This could mean that both devices have enabled encryption, but have mismatched keys, or that one of the devices does not support encryption or does not have encryption enabled.

- Messages In. This counter displays the number of times messages were received while another transmission was in progress. It is a measure of the amount of overlapped communication on your wireless network. Zero values indicate low to moderate load of your network. Non-zero values identify a wireless medium that is being used simultaneously by multiple users.

- Messages In Bad. This counter displays the number of times messages are received while a transmission elsewhere in the wireless network was in progress. This counter is expected to be zero. Non-zero-values indicate a heavily loaded system.

Can the default route be set off any interface on the TZ 170 W?
Yes – this is a new feature found in the SonicOS 2.0 Standard for TZ 170 W firmware release. It's now possible to set the default route to a router located on the LAN, WLAN, or WAN interface. In previous releases of firmware, the device would only allow default routes to be set to a router located on the WAN interface.

Is it possible to set up a wireless bridge between two TZ 170 Ws?
Yes – it's possible to bridge multiple TZ 170 Ws off a central TZ 170 W device, and can be set to do so securely by configuring VPN tunnels between the wireless links between the TZ 170 W devices to encrypt and protect all wireless traffic between the TZ 170 Ws. For instructions on how to set up this new feature, please refer to the whitepaper "Secure Wireless Bridging using SonicWALL TZ 170 Ws".

Is it possible to set up a wireless bridge between a TZ 170 W and a SonicPoint?
Yes, it is. Please refer to the whitepaper "Secure Wireless Bridging: TZ 170 Wireless Standard to a SonicPoint".

Can a TZ 170 W in 'bridge mode' also accept client wireless connections?
No, it cannot. When setting up a wireless bridge between two TZ 170 W's, one of the devices must be set to 'access point' mode, and one must be set to 'bridge mode'. Once a device is set to 'bridge mode', it can no longer accept client wireless connections. However, the device set to 'access point' mode can still accept client wireless connections.

Does the TZ 170 W support Dynamic Address Translation (DAT)?
Yes – this is a new feature found in the SonicOS Standard 2.0 for TZ 170 W firmware release. Dynamic Address Translation is a form of network address translation (NAT) that allows the TZ 170 W to support any IP addressing scheme for wireless guest services users (WGS), eliminating potential issues where the guest systems are not set for DHCP and have previously configured static IP address settings that do not match the IP address scheme of the TZ 170 W WLAN interface. For example, the TZ 170 W WLAN interface could be configured with its default address of 172.16.31.1, and one WGS client could have a static IP Address of 192.168.0.10 and a default gateway of 192.168.0.1, while another could have a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables IP communications for both of these clients. DAT is designed to provide support for unidirectional, non-dynamic TCP and UDP protocols, such as HTTP, HTTPS, SSH, RDP, NNTP, etc. Dynamic or bi-directional protocols, such as H.323 and FTP are not supported for DAT users.

Can the TZ 170 W perform any wireless intrusion detection and/or intrusion prevention?
Yes – this is a new set of features for the SonicOS Standard 2.6 for TZ 170 W firmware release:

Null Probing Detection: The TZ 170 W can detect attempts from wireless clients attempting to associate with the SSID unset (null).

Association Flood Detection. This is a wireless Denial of Service attack intended to interrupt wireless services by depleting the resources of a wireless Access Point. An attacker can employ a variety of tools to establish associations, and consequently association ID's, with an access point until that access point reaches its association limit (generally set to 255). Once association saturation has occurred, the access point will discard further association attempts until existing associations are terminated.

Rogue Access Point Detection. The TZ 170 W can detect rogue access points that may have sneaked into your network, or whose signal is bleeding into the broadcast footprint of the TZ 170 W. When activated, this is accomplished this in two ways: active scanning for access points on all 802.11b/g channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Can I create wireless guest services accounts that get auto-deleted after a specified amount of time?
Yes – this is a new feature found in the 'SonicOS 2.6 Standard for TZ 170 W' firmware release. When creating a wireless guest services account, simply check the auto-prune account checkbox. When the 'account lifetime' expires, the TZ 170 W will automatically delete the account, so you do not have to manually log into the device and clean out dead accounts. This feature is especially useful in environments where it is not always possible to perform system maintenance and cleanup on the TZ 170 W's guest account database.

What is the difference between account lifetime and session lifetime?
The 'account lifetime' for a wireless guest services account refers to the amount of calendar time that the account is valid for. For example, if it's November 1st, and I create a wireless guest services account with an account lifetime of 7 days, that account will become disabled on November 8th. This feature relies on the system time of the TZ 170 W, so you will need to ensure that the TZ 170 W's clock is always set correctly for the timezone it's in. The 'session lifetime' for a wireless guest services account refers to the amount of time within that 'account lifetime' period – think of this as an allotment of minutes that can be used within the 'account lifetime' window. This counter will not begin to decrement until the wireless guest account logs in for the first time, and will deactivate the account when the 'session lifetime' set for that account is reached. This way, you can create accounts that are good only for a fixed amount of time, and can only be used within a fixed window of time. For example, a coffee shop could offer its customers free wireless access through a TZ 170 W by generating unique wireless guest services accounts that are good for five days, and can be used for up to 60 minutes of free access. Because the window for the account is five days, a patron could return within that time window and use up the remaining minutes not used on the first visit.

Quick Speeds/Feeds Chart for TZ 170 W w/SonicOS 2.6 Standard

Feature	*Number*
Firewall Performance	90 Mbps
VPN Performance	30 Mbps
Concurrent firewall connections	6,144
Max Concurrent Site-to-site VPN connections	10
Max Concurrent Client VPN connections	WAN: 50, WLAN: Unlimited
Number of Site-to-site VPN licenses device ships with	10
Number of Client VPN licenses device ships with	1
Can upgrade concurrent Site-to-site VPN connections?	NO
Can upgrade concurrent Client VPN licenses?	YES
Can upgrade node count licenses?	YES
Max NAT Policies/1-2-1 NAT Entries	512
Max Static IP Routes	128
Max Firewall polices	100
Max DHCP Leases (global)	1,024
Max DHCP Scopes	2
Max Internal User Accts	100
Max Internal User Groups	N/A
Max Guest User Accts	100
Max Address Objects	N/A
Max Address Object Groups	N/A
Max Service Objects	N/A
Max Service Object Groups	N/A
Max Schedule Objects	N/A
Max SonicPoints per interface	2 on OPT port (requires SonicOS Enhanced)
Max SonicPoints supported on device	2 on OPT port (requires SonicOS Enhanced)

Document Created: 06/14/2004
Document Updated: 07/26/2004
Document Version: 1.1
Document Maintained By: Dave Parry