Release Notes for the SOHO TZW Internet Security Appliance

Prepared by SonicWALL, Inc.
04/25/03

SonicOS 1.0 is now available only on the SOHO TZW Internet Security appliance. This release note provides technical information on the initial release of this product.

- Some firmware updates include updates for the wireless radio card. This information is provided when the firmware update is released. Firmware updates that include updates for the Wireless radio card can cause the Test, WLAN, WiFiSec, and Wireless LEDs to remain lit while the firmware is uploading to the appliance**. Do not** power the unit off during the update as this permanently damages your wireless radio card. After the firmware upload is complete, the SOHO TZW automatically restarts and completes the firmware update.

- If you begin a management session using the WLAN interface and interrupt the session by opening another management session on the LAN, you can interrupt active WLAN to LAN sessions at the TCP layer.

- If you experience multiple failures while attempting to establish a PPPoE connection, it may be necessary to reboot the SOHO TZW to restore PPPoE functionality.

- Wireless Guests and Users are not unique accounts. If the same user name and password is created for a wireless guest and a user, the Wireless Guest account is referenced.

- Changing the HTTP management port on a SOHO TZW providing Wireless Guest Services requires a reboot to ensure that wireless guest Web browsers are redirected to the correct URL (specifying the new port) for authentication.

- To create simultaneous Global VPN Client connections through the SOHO TZW to a remote point and the WLAN, with or without WiFiSec enforcement, you must first create the connection through the SOHO TZW to the remote termination point on the Internet, and then to the WLAN port.

- Attempting to create a VPN policy that enables Perfect Forward Secrecy and Forward Packets to Remote VPNs can cause unfounded proposal-based Phase 2 failures.

- If WiFiSec is enforced on the WLAN, the only broadcast traffic allowed on the WLAN is NetBIOS, DHCP, and ARP. All other broadcast traffic is dropped by design.

- If the WLAN radio fails, the SOHO TZW watchdog automatically reboots in an attempt to recover from the failure. If the WLAN LED blinks following the automatic recovery process, this indicates that the WLAN radio requires a full reset. Please power off the SOHO TZW; wait a few seconds, then power on to completely reset the WLAN radio.

- XAUTH support for SecureID's New PIN Mode, Next PIN Mode, and Next Token Mode is excluded from this release.
- Changing the VPN keying method, for example, IKE to Manual Mode or Manual Mode to IKE, can inadvertently change the subnet mask of the defined remote destination network.
- Some wireless cards, notably Netgear and Linksys 54G cards, have demonstrated compatibility issues when connecting to other manufacturer's devices. Compatibility issues are further complicated by the use of WEP, or by increasing the beaconing interval beyond its default value. It is strongly recommended that you upgrade to the latest firmware and device drivers available from your wireless client card's manufacturer, particularly if you are using Netgear or Linksys 54G equipment.
- By default, the TZW does not handle WLAN based WiFiSec tunneled packets larger than 1,518 bytes (packets requiring fragmentation). If you are running a large packet protocol (such as Kerberos or certain UDP applications), you must create a specific access rule for that protocol, and enable fragmentation on that rule.
- Extremely heavy WiFiSec WLAN traffic loads could result in spurious **IPSec Replay Attack** log messages.
- Changing the WAN interface mode, for example, from **NAT Enabled** to **NAT with DHCP Client** while using DHCP services on the TZW can cause the current DHCP lease table to be flushed.
- Attempting a configuration requiring wireless clients to connect to the TZW with a WiFiSec connection, and the TZW then attempts to route all traffic through a VPN connection to a hub termination point can result in failed phase 2 negotiations between the hub and the TZW.
- Although validation and error-checking is implemented on all management entry fields, it is strongly recommended that user names, service names, comments, etc. not contain any non-alphanumeric characters such as apostrophes or backslashes.
- Internet Explorer 5.2.2 running on a Mac exhibits numerous page rendering problems. When using a Mac for management, an alternative browser (e.g. Safari, iCab, Opera, Mozilla) is recommended.

Microsoft Windows XP and the SOHO TZW

If you are running Microsoft Windows XP as your computer's operating system, Windows XP, by default, manages your wireless PC card settings. If you want to use the Microsoft wireless management tools rather than your card vendor's management tools, please note the following information:

- Your wireless PC card drivers must be compatible with Microsoft's Wireless Zero Configuration service.
- You can access the wireless card 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 appears it lists all of the wireless networks available. Click **Advanced** on the lower left side of this screen.

- Be sure **Use Windows to configure my wireless network settings** is selected.
- If your TZW SSID name appears in the **Available Networks** box, select it and then click Configure. If you do not see it, try clicking Refresh. Please note that if **Hide SSID in Beacon** and **Block Response to Unspecified SSID** are selected on the SOHO TZW, then you must use the Add button to manually enter the SSID.

WEP Considerations for Windows XP and the SOHO TZW

- If you are using WEP, select **Data encryption (WEP enabled)** and **Network Authentication (shared mode)**.
- Clear the **The key is provided to me automatically** checkbox.
- If using WEP, enter the TZW WEP key in the **Network Key** and **Confirm Network Key** fields.
- If using WEP, Windows XP prior to Service Pack 1 requires you to select the type of key (alphanumeric, hexadecimal) and the key size (40, 104). Please note that although the TZW lists different key sizes (64,128) they are actually the same. For this purpose, 40=64 and 104=128. After Service Pack 1, these drop-down boxes are not displayed, and XP automatically determines the type and size.
- If using WEP, Windows XP prior to Service Pack 1 has a different key index and uses 0-3 instead of 1-4. The TZW key index uses 1-4. For this purpose, 0=1, 1=2, 2=3, 3=4. This was resolved in Service Pack 1.
- Click the **Association** tab and make sure **Enable IEEE 802.1x authentication for this network** is not selected.

Additional Regulatory Statement Model APL11-027 and Model APL11-031

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.