

SonicWALL Makes Wireless Networking Secure

*Defines the Challenges Facing Organizations
Interested in Deploying Wireless Network
Security*

CONTENTS

Abstract	1
The Demand for Wireless	1
IT Concerns—No Small Issue	1
SonicWALL's SOHO TZW Makes Wireless Networking Secure	2
Business Benefits	4
Deployment Scenarios	5
Conclusion	6



Abstract: Organizations of all sizes are adding wireless technology to their networks at an increasing rate. This explosion of growth has companies adding access points to networks frequently without the necessary wireless security infrastructure in place. Wired Equivalent Privacy (or WEP) is the common entry-level technology used to provide baseline security. At the other end of the spectrum, organizations are integrating firewall and VPN concentrators to each wireless access point to ensure business grade security.

This white paper discusses the challenges facing organizations interested in deploying wireless network security.

The Demand for Wireless

Why do employees want their companies to implement wireless networks? The reasons are simple. According to a 2002 study released by InfoTech, the number one desire for end users is increased productivity. Workers want the ability to use their laptop computers anywhere and remain connected. The convenience of wireless networking immediately appeals to users. With the ability to roam, workers can easily obtain key files and information during meetings, they can work in a team environment without sharing offices permanently and they can carry their laptops to other rooms or buildings without interrupting workflow. Now that laptop computers are readily available with built-in wireless access cards, users are further motivated to demand wireless LAN access at work.

And companies are taking action on these requests. A recent study by Gartner Dataquest released in September 2002 predicted that wireless LAN equipment shipments would grow to 26.5 million units in 2003, up from 15.5 million units in 2002.

IT Concerns—No Small Issue

But, with this increasing demand from wireless users comes a daunting task for IT administrators—the requirement for wireless security. The primary challenge of securing a wireless network is the requirement to purchase additional products, such as a firewall and VPN appliance, to provide adequate security. Wireless Equivalent Privacy (WEP), the current WLAN security standard, is not robust enough to provide true business-class security; additional steps are required. However, IT teams want to avoid the inefficient and expensive practice of “cobbling together” equipment and software from multiple vendors. These solutions involve multiple devices—i.e. firewall, VPN, wireless access point—which leads to the hassle of managing multiple products adding to IT overhead.

To gain the convenience of wireless, despite rules prohibiting the practice, some employees may even install their own “rogue” wireless access points on the company’s network. This practice leaves gaping backdoor vulnerabilities in the corporate network, by bypassing corporate security policies.

Wireless Networking Challenges:

Drive-By Hacking. Perhaps the most descriptive form of security breach of a wireless network is “drive-by” hacking. If the network is unprotected, access to the organization’s intranet is virtually instant. If WEP has been deployed, hackers need to do little other than exercise the known holes in WEP to gain access.

Access Control. Another security issue with wireless LAN involves access control, including both authentication and authorization. In some cases, the wireless LAN does not incorporate authorization, so IT departments do not have the ability to control access to different areas of a network by those provided with basic access. The challenge of unauthorized access results in serious issues: the possibility of denial of service attacks, the inability to maintain the confidentiality of data on the network and the inherent problem of ensuring the network and/or the data on the network is unchanged.

Wireless Standard Weaknesses. The 802.11 wireless standard commonly used today specifies WEP as its security protocol. WEP uses RC4 encryption, which is reasonably strong, but the keying is flawed. What this means is that, by using commonly available tools such as AirSnort or WEPCrack, a hacker can determine the keys within hours. In addition, the user authentication specified in the 802.11 standard is weak. The standard includes use of a password along with an SSID for each access point. But because the password is sent in the clear, it is worthless. Another weakness with the 802.11 standard involves the use of Media Access Control (MAC) address filtering, which can be spoofed. Many access points allow for access control lists based on MAC address. Hackers can sniff the MAC address and easily spoof it to gain access to the network.

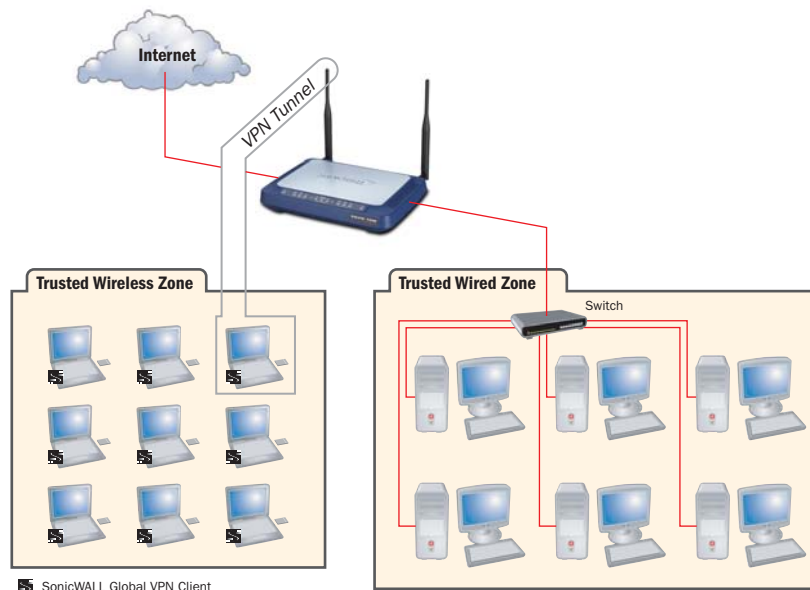
Cost. In addition to the continually increasing expense of the equipment and software, the cost of maintaining a multi-vendor supported wireless LAN can be incredibly steep. Currently available solutions, when taking into account the cost for the equipment and software for wireless access point, VPN and VPN client, plus firewall, can cost a business thousands of dollars. This does not include the cost of managing the wireless network and security devices and software—this increases the cost significantly.

SonicWALL’s SOHO TZW Makes Wireless Networking Secure

What the business world needs to resolve the conflict between employee desires and IT concerns is a *secure* wireless LAN solution at an affordable price—a solution integrating the bulletproof security of a firewall, VPN concentrator and VPN client. SonicWALL’s new SOHO TZW wireless LAN gateway provides the features and benefits required to create a trusted zone for both wired and wireless users at an affordable price for small businesses.

Figure 1 - Trusted Zones

The SonicWALL SOHO TZW secure wireless gateway establishes secure zones for wireless or wired users. Unlike solutions using WEP (Wired Equivalent Privacy), the SOHO TZW utilizes robust VPN technologies to create a trusted wireless connection.



The SOHO TZW incorporates features designed to provide the convenience and benefits of secure wireless networking while meeting the stringent security requirements of IT professionals.

Three Components, One Bulletproof Device. The SOHO TZW includes a wireless access point, a firewall, and VPN tightly integrated in a single appliance. SonicWALL is the first security company to integrate these security functions into one easy to manage product. The SOHO TZW secure wireless access point utilizes 802.11b technology for the wireless LAN, the most mature and prolific of the wireless standards for wireless access cards today. 802.11b provides data rates up to 11 Mbps with a range up to 500 meters.

Complete Security for both the Wired and Wireless LAN. The firewall incorporated into the SOHO TZW provides protection for the wireless and wired LAN. Off the shelf, the SOHO TZW supports up to 25 users and it is upgradeable to support either 50 or an unlimited number of wired or wireless users. This provides total flexibility to the network administrator for supporting a variety of business architectures.

Tightly Integrated Global VPN Client. The SOHO TZW includes tight integration with SonicWALL's Global VPN Client. The client has a number of important features:

- ▷ Use of the industry-accepted IPSec 3DES encryption to secure data on the network
- ▷ Step-by-step wizards for quick and easy installation of the product and configuration of the VPN client connection
- ▷ A simple user interface with point-and-click VPN activation plus streamlined management tools
- ▷ Automatic downloading of the VPN configuration data and establishment of a connection from VPN gateway

Enforced Use of Industry Standard IPSec VPN. The SonicWALL Global VPN Client makes it possible for IT departments to enforce the use of the VPN for wireless users, creating a trusted zone which is Wi-Fi compatible.

Wireless Guest Services. The SOHO TZW allows the IT manager to set levels of access—for guests in the business network as well as restricted levels of access for different job functions in the company. For consultants, contractors, and guests, the Wireless Guest Services (WGS) feature in the SOHO TZW makes it possible for IT to create a guest zone on the wireless LAN, setting up temporary accounts with usernames and passwords. Guests then have full Internet access, but no access to the LAN or to other guest users. WGS is ideal for corporate day guests, temporary employees and free short-term public Internet access to customers (such as for coffee shops and bookstores).

Unmatched Flexibility in End User Devices. The SOHO TZW works with multiple devices, including desktop PCs, tablet PCs, PDAs and laptop computers. A SOHO TZW-based wireless LAN also allows for use of any third party PC cards that are compatible with the 802.11b Wi-Fi standard.

Bulletproof Security Features. The SOHO TZW includes a complete suite of security features. As previously stated, the device utilizes IPSec 3DES encryption on the wireless LAN, including VPN client with VPN tunneling for the highest level of security available today. At the same time, the solution is Wi-Fi compatible for those environments already running wireless LAN using Wi-Fi technology.

Business Benefits

The SonicWALL SOHO TZW takes SonicWALL's industry-leading technology and adapts it for the wireless LAN environment. This means the network has bulletproof wireless security—there is no way for a drive-by hacker to obtain access, and there is no way for workers using the network to access or change information without permission.

Because of the tight integration with the SonicWALL Global VPN Client, users of the SOHO TZW-based wireless LAN have secure access to the corporate network to maintain the confidentiality of private data. In addition, the Global VPN Client is easy to implement by IT and easy to use by the worker.

The SOHO TZW provides the IT manager with complete control. If a customer visits for a meeting and needs to utilize the network to access the Internet, there is absolutely no chance that he or she will inadvertently (or purposefully) obtain access to confidential information. And a hacker sitting in the parking lot will quickly determine that the network is impenetrable and move on to another target. The security in the SonicWALL-safe network is rock solid.

The SOHO TZW is extremely cost effective. Not only is it incredibly easy to implement, but it is also affordable to support and maintain. Because the IT department manages only one product (rather than three), administrative costs are minimal. The company choosing to implement the SOHO TZW will find savings in equipment and network deployment as well as in ongoing maintenance. The following chart itemizes the savings:

	Leading Security Device	Leading Wireless Device	SonicWALL SOHO TZW
Device cost	\$995	\$1,049	\$895
Firewall	~ \$1,000	~ \$1,000	Included
VPN w/VPN client	Included	Included	Included
WAP	~ \$1,000	Included	Included
IT personnel cost —setup only	12 hours @ \$50 per hour—\$600	12 hours @ \$50 per hour—\$600	4 hours @ \$50 per hour—\$200
Total cost per device or access point (25 users)	\$3,595	\$2,649	\$1,095

In this comparison based on current market figures, savings are substantial—between 58% and 69%, depending on the solution. These figures do not take into consideration ongoing maintenance costs for IT personnel, but it can easily be assumed that the cost to maintain multiple devices (and multiple interfaces) will increase overall costs significantly.

Deployment Scenarios

The SOHO TZW is so versatile that it can fulfill the secure wireless LAN requirements in many different scenarios.

Office Gateway. The most obvious of the scenarios is the business with a mixed wired and wireless network. According to a 2002 study by Infonetics, Inc., 21% of small businesses already have wireless LANs and 42% plan to implement wireless LANs by 2004. In this scenario, while using the SOHO TZW solution, a business can set up any combination of wired and wireless users as well as make space for guest users—people who are temporarily located at the business and would like to utilize the business’ network to access the Internet, email and their own networks. Not only is the network safe from outside intrusion, it is safe from unauthorized access of information by the guest users. Because of the affordability of the solution and the limited cost of long-term maintenance and administration, it is ideal for small businesses.

This product is also ideal for branch offices requiring VPN to corporate headquarters. SonicWALL has taken its industry-leading security platform and integrated it with a flexible, easy to use wireless LAN so that branch offices are able to mirror the network configurations of the head office—making it feasible to have secure access to the corporate network. Along with this comes the ability to provide secure VPN access to telecommuters. Basically the SOHO TZW works just like a secure wired LAN in this scenario.

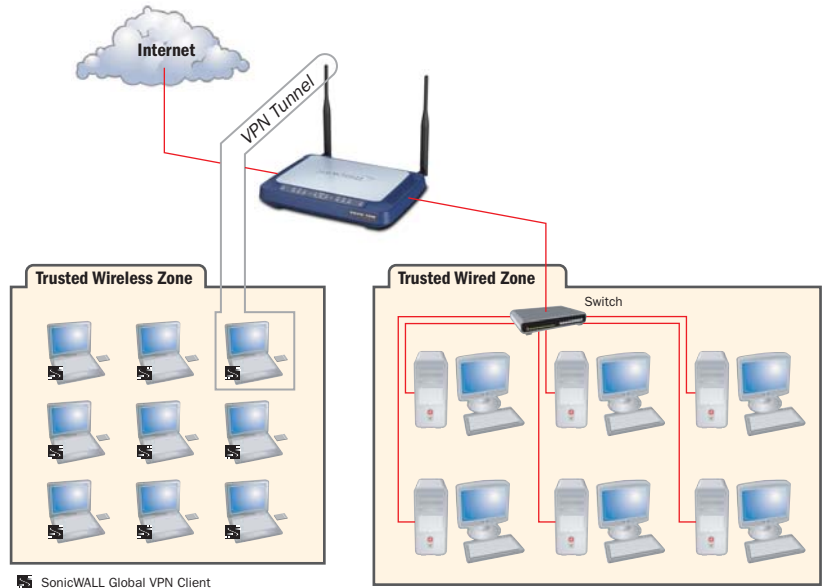
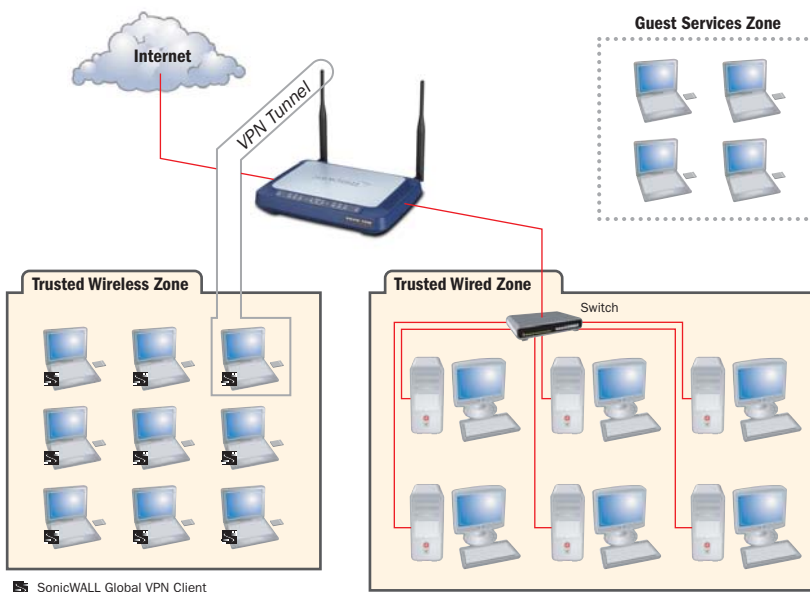


Figure 2 - SonicWALL TZW as an Office Gateway

The SonicWALL SOHO TZW provides organizations with the ability to offer secure wireless access to users.

The product can also be used for training and educational scenarios as well. Having a wireless network in a training center makes it feasible to use wireless computers for distance learning. With the shrinking training budgets typical in today’s business environment, it is beneficial that the SOHO TZW can save companies from having to set up hard-wire workstations. And from a training perspective, the integration of a wireless LAN makes it easy for classmates to collaborate. With the security inherent in the product, companies can conduct training on highly sensitive information without being concerned about the confidentiality and integrity of the data or the network.



Office Gateway Plus Guest Services. The SOHO TZW has another very practical use—businesses and retail stores can use a secure wireless network for business functions such as inventory management, process control and shipping while also providing guest services to customers, clients and partners. The company’s IT department maintains complete access control while providing guests with temporary usernames and passwords. MAC address filtering is an option so that guests cannot access restricted areas of the company’s network or other guest’s systems. Guests have full Internet access, but not LAN access. This scenario is particularly useful for conference rooms for meetings with customers and vendors.

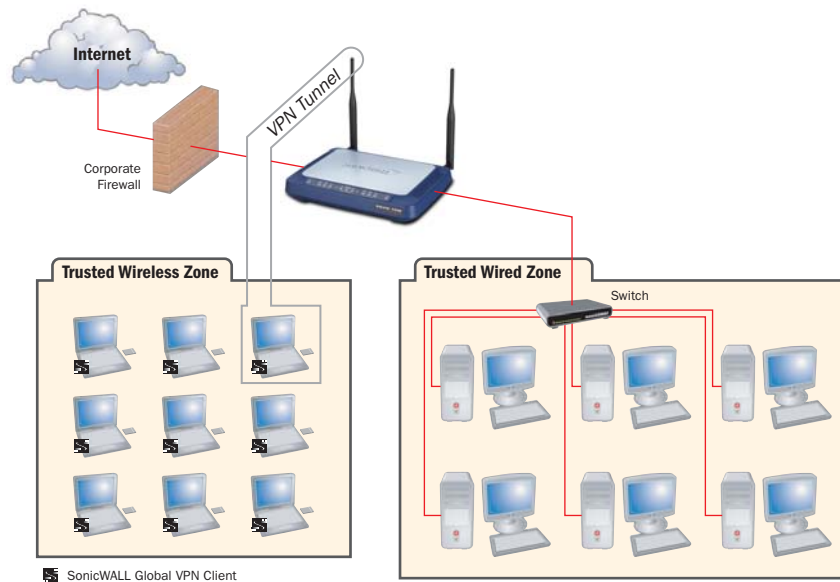
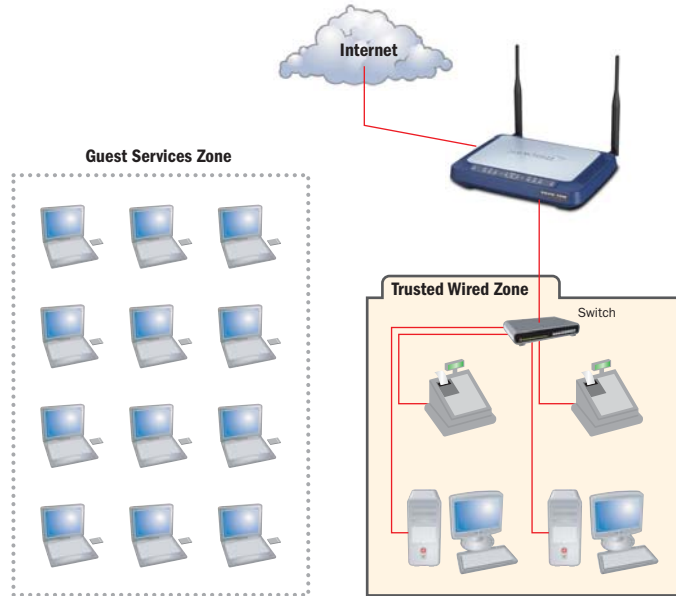
Figure 3 - Office Gateway plus Guest Services

The SonicWALL SOHO TZW provides guest users with Internet access while blocking all other network services.

HotSpot. In the hotspot scenario, the SOHO TZW can be used to provide secure Internet access to patrons and guests. The most common hotspot locations today are coffee shops, book stores, hotels, convention centers, restaurants and airports. The SOHO TZW includes features to control inter-client system access and time allotments. At the same time, the wired LAN portion of the SOHO TZW can be utilized for cash registers, employee email and other functions.

Figure 4 - HotSpots

The SonicWALL SOHO TZW allows organization to differentiate themselves by offering wireless Internet connectivity.



Departmental Secure Access Point. The SOHO TZW can also be utilized so that a department within a business environment may have a wireless zone for use by only that department. One example of this might be for the inventory management in a manufacturing company. Another example might be in a computer-testing lab, where the employees in that department have more of a need to be mobile than in other departments.

Figure 5 - Departmental Secure Access Point

The SonicWALL SOHO TZW provides organizations with existing networks the ability to add secure wireless to services to their networks.

Conclusion

Along with the demand for wireless networking in business environments comes significant challenges for corporate IT departments in securing wireless networks. SonicWALL has built the only truly secure wireless LAN solution that integrates a gateway and an access point with its industry-leading VPN/VPN client and firewall, making it not only safe, but also affordable to add wireless to a business network. The SOHO TZW provides businesses with an unmatched combination of bulletproof security features, tightly integrated VPN and VPN client, flexibility in end user devices and ability to provide guest services. Along with this comes a price point that is easily affordable for small and medium businesses and retail stores. The SOHO TZW is the most secure option for wireless networking in a business setting.

For more information

For more information about SonicWALL Wireless, call 1-888-557-6642 or visit www.sonicwall.com/products/sohotzw.html.