



Best Practices in Deploying a Secure Wireless Network

CONTENTS

Abstract	2
Today's concerns	2
Purpose	2
Technology background	3
Today's challenges	4
Key security requirements of an integrated network	4
SonicWALL leadership	6
Summary	8

Abstract

Wireless technology is dramatically changing the way companies operate. Employees have immediate access to business-critical applications and information from anywhere in the office, enabling them to respond to customers and colleagues in real time. The result is increased productivity and enhanced customer service. Consequently, work has become less of a place to go and more of an activity that can be conducted from anywhere.

However, wireless networks pose inherent security risks as they eliminate physical boundaries for the network. No organization can afford this convenience at the expense of network security. This paper documents potential risks and associated best practices to help you fully realize the benefits of a secure wireless network.

Today's Concerns

The old network paradigm of the wired user going to where the data resides is obsolete. The growing popularity of wireless LANs brings the data to the user, yielding a more productive and efficient workforce. Mobile users access the network from anywhere in range of the wireless network, at any time. However, despite the overriding benefits, business owners and network administrators have legitimate concerns about implementing and managing wireless access to the network. Wireless networks introduce a number of critical security risks and challenges, making it important to implement strong security measures to mitigate these risks.

Purpose

This document will help business owners and network administrators understand the required elements for a secure wireless network, allowing them to avoid the expense and risks associated with an inadequate deployment. It also provides background information and guidelines for assessing the various types of wireless solutions available today and an overview of centralized management for both wired and wireless networks.

Owners and managers want to select the core technology most suitable for their industry and business requirements. Companies need a solution that is cost effective today, yet can scale to support future growth. This paper also provides an overview of total cost of ownership (TCO) and scalability issues to help readers identify the correct solution for their businesses.

Discussed are security solutions that tie together both wired and wireless networks and are available in various configurations designed to address the needs of different organizations' sizes and types. All solutions discussed meet the key assessment criteria for secure, cost-effective, manageable and scalable network operations.

Technology Background

The wired LAN resides inside a company's building, and the data stays on the wire, available only to authorized users with physical connections to that wire. However, any network—wired or wireless—is subject to security risks and issues. These include threats to the physical security of a network, unauthorized access or eavesdropping and attacks from within the network's (authorized) user community.

Separate from the physical wire, a wireless LAN (WLAN) has all of the properties and security risks present for a wired LAN. Therefore, security measures taken to ensure the integrity and security of data in the wired LAN environment are also applicable to wireless LANs. Wireless LANs include an additional set of unique security elements though. By their nature, wireless networks have the potential to provide access to any party in range of the coverage area, including parties outside the network's physical security perimeter. Although the range of the wireless LAN is limited, wireless signals can often be received at distances of several hundred feet beyond the physical perimeter of a facility. In larger facilities that use multiple wireless LAN access points to interconnect wireless users with wired networks, each access point is a potential point of entry to the internal network.

Different vendors have developed varying types of wireless security solutions to address these security risks and issues, each with a unique set of characteristics. Most wireless solutions fall into one of the three categories described below.

Stand-alone Access Points

The initial wave of wireless technology consisted of standalone access points (APs). These products simply aggregated 802.11 wireless traffic. There was no centralized management and it was challenging to create a larger, more distributed wireless network that maintained consistent performance as users roamed. Scalability was also an issue, since each AP required local management. More importantly, stand-alone APs offered no centralized security policies. The basic level of built-in security, usually WEP (Wired Equivalent Privacy) or increasingly WPA (Wi-Fi Protected Access) with a pre-shared password, gave unsuspecting users a false sense of security. Network administrators understandably worried, because they recognized that such products left their networks vulnerable to “backdoor” attacks such as dictionary and man-in-the-middle attacks.

Secure Wireless Gateways

In response to growing security concerns, some vendors have developed secure wireless gateways, a separate device that can be added to the existing network. Operating in conjunction with other vendors' APs, gateway security appliances apply security and management policies to all WLAN traffic. However, they don't manage the AP devices themselves, which means firmware upgrades or radio tuning must be individually applied to each AP, consuming a greater amount of resources than a centralized solution.

Combined Switch and Access Points

Most recently, the industry has seen the introduction of a single vendor wireless switch combined with manageable APs. These solutions provide centralized management of the APs as well as WLAN traffic, application of wireless security policies and granular control of the radios.

The drawbacks to this type of solution are cost and management. It requires an additional wireless-specific switch with a specific WLAN management system that runs alongside a company's existing LAN management platform, so business owners are still left with two parallel networks. This type of solution would still be prone to more evasive and dynamic threats presented by application level malware such as viruses, spyware, worms and phishing attacks.

Today's Challenge

Network and security administrators are seeking ways to protect their wireless networks from the very same threats against which they must diligently guard their wired networks. Data security is reported as the primary reason for organizations not implementing wireless LANs. Not coincidentally, unauthorized access to sensitive information and eavesdropping on the network are the same security concerns related to implementing a wired network. Similar to data transmitted from the Internet, one cannot be sure of where wireless data entering the network originates since it is transmitted through walls and buildings. Therefore, as with data from the Internet, the wireless network must be treated as “untrusted” and segmented from the internal network.

Although all three of the product categories detailed earlier address valid wireless needs and concerns, they ignore network administrators' requirement for a secure and convenient method of applying the same robust level of security on the wireless network that currently exists on their wired network—without implementing a parallel wireless network and a separate management system. Guarding against a more sophisticated class of threats tends to consume a far greater amount of resources, so duplication of these sorts of threat management systems for a wireless network is not practical. There needs to be a converged method of threat management.

Key Security Requirements of an Integrated Network

Start with the Basics

The basis of a sound wireless security strategy requires the following guidelines:

- Apply the same security policies to the wireless network as with any untrusted network.
- Implement a layered security approach, starting with a robust firewall (one that integrates a configurable, high performance deep packet inspection engine as the foundation) and then adding a dynamically updated database containing thousands of attack and vulnerability signatures.
- A layered approach results in a complete security solution that protects your network against a comprehensive array of dynamic threats, including: viruses, worms, Trojans, software vulnerabilities (such as buffer overflows), peer-to-peer and instant messenger applications, backdoor exploits and other malicious code.
- Apply the same security policies for wireless clients connecting through the wireless network as you would to remote users connecting through the Internet to the internal trusted network.

Such a deployment method must be thoughtfully planned and proactive measures must be put into place to ensure security, reliability, scalable performance and the ease of centralized management.

Demand Proven Security

Any user crossing an untrusted network to get to an internal network must use IPSec VPN client software on their computers (laptops, home office desktops or branch office workstations). IPSec has been the standard for many years and has proven to be rock solid in providing everything from VPN access over the Internet to secure communication for financial transactions. The VPN client addresses authentication and traffic encryption with the internal network gateway.

Although the main standard for WLAN specific encryption lies in the IEEE 802.11i standard, the convenience of utilizing IPSec VPN lies in its dual purpose flexibility. User credentials and privileges remain the same whether the employee is away from the office or using a wireless connection in a meeting room. Therefore, the same VPN client used to access the internal LAN network is the same VPN client used to access network resources remotely while traveling, from home or from branch offices. IT administrators only need

to establish one account for users to access the WLAN sites making it more efficient and less costly to securely provide access. A secure wireless access solution should have the flexibility to provide both IPSec VPN access over the WLAN and support WLAN encryption standards such as IEEE 802.11i.

Centralized security products implementing wireless security must also be able to differentiate between trusted and untrusted networks and enforce security policies to all traffic traversing the network. A company should employ a user database to identify users for the purpose of granting access and tracking usage for accountability. One user database should be shared between the wired and wireless networks so the network administrator does not have to maintain two discrete databases.

Address Evolving Threats and Productivity Issues

Network attacks are evolving rapidly and becoming more sophisticated. A stateful packet inspection firewall and VPN solution are necessary, but no longer sufficient to ensure network integrity and comprehensive security. Even traditional desktop anti-virus clients were not adequate in blocking the latest variants of viruses, worms and Trojans that have taken the spotlight in recent security news headlines. Regardless of the type of network (wired or wireless), it is imperative for business owners and network administrators to take the necessary security precautions to avoid being vulnerable to blended attacks. These types of attacks are introduced through e-mail, attachments, embedded in Web pages or transmitted through peer-to-peer applications. Security solutions such as gateway anti-virus, anti-spyware and intrusion detection and prevention are required to mitigate these types of blended attacks. The centralized security solution should apply security services to all network traffic and between network segments in combination with traditional firewall and VPN policies.

Require Rogue Access Point Detection

Rogue AP detection is necessary to ensure there are no backdoor vulnerabilities introduced into the network through the addition of an unauthorized AP to the network. This requires the ability to conduct on-demand and scheduled scans of the radio frequency (RF) spectrum to locate, log and alert network administrators of neighboring APs.

Ensure Ease of Management/Total Cost of Ownership

The integration of wireless and wired security into one platform should include the capability to configure and manage both wired and wireless networks, and enforce corporate security policies for the networks from a single central management interface. This eliminates the need to train administrators on multiple security management platforms, as well as the need to perform redundant management activities. Central control of logging and reporting of auditable network activities should also be included.

An effective wireless security solution must allow the network administrator to communicate with hundreds of access points without having to deal with each one individually. Single security management requires the ability to manage and configure all access points from one central management interface, and security policy updates should be automatically provisioned to each access point from the central console.

Easily Deploy Wireless Guest Internet Access

A wireless security solution must be able to provide easy-to-deploy guest access, allowing easy, extemporaneous guest access to public resources such as the Internet, while ensuring that they do not have access to trusted network resources such as the wired LAN.

The challenge is in the ability to simultaneously support a wireless environment where trusted users can access network resources while still providing the continuity of guest access to visitors, without the need to deploy a separate, parallel network. To accomplish this goal, the security solution must provide guest access services with authentication mechanisms that differentiate guest users from trusted wireless users, and provide different levels of access based on the user and the company's acceptable use policies.

Easy deployment of guest access is also an important factor. The solution must provide a simple way to give wireless guest access through the automatic generation of guest accounts without compromising the integrity of the network.

Plan for Growth

A wireless security solution must be easy to deploy and scale, while providing an efficient transition from legacy wireless networks.

Scalability is essential. Organizations with large campuses may need hundreds of access points and a wireless security solution can simplify deployment by automating the initial provisioning of the access points, as well as automating large scale changes such as distribution of new firmware and configurations. A wireless security solution should make it easy to connect and automate the operability of as many sanctioned access points as needed.

Wireless security solutions should also be transparent to the user without the mandatory need for difficult to deploy and manage supplicant software or other changes to their devices.

Anticipate the User Experience

From the user perspective, a wireless solution must provide sustained network access with no discontinuity regardless of the user's location within a facility. This capability is fundamental if users are to fully leverage the convenience of wireless.

The user demands a transparent and uninterrupted network experience. At the same time, the network administrator must guarantee secure wireless coverage throughout the facility while still protecting the network. Improvements are constantly being made to this level of continuous service, and to enhancements for supporting streaming voice and video applications. It is therefore important to select a wireless security vendor committed to keeping pace with and to adopting emerging standards and innovations in these areas by means of timely and easily deployed updates to their access point's firmware.

Adhere to Standards-based Architecture

For a successful deployment, wireless solutions must be standards-based to ensure interoperability with existing wireless and security infrastructure. Such standards include IEEE 802.11a/b/g wireless access, IEEE 802.3af power over Ethernet (PoE), IEEE 802.11d, IPSec encryption for secure wireless LAN access, WPA and IEEE 802.11i. Solutions must also be hardware-ready to support near term enhanced security standards with a simple firmware upgrade.

SonicWALL Leadership

SonicWALL, Inc., a leading provider of Internet security solutions, offers multi-layered security solutions for networks of all sizes. SonicWALL has taken network security expertise and extended it to address wireless-specific security concerns.

SonicWALL SOHO TZW, TZ 170 Wireless and TZ 150 Series

In 2003, SonicWALL pioneered the industry's first single point solution that provided security enforcement and management for both wired and wireless networks. Following the phenomenal success of this initial release, SonicWALL introduced the TZ 150 Wireless and TZ 170 Wireless products. These products were secure wireless gateways that integrated secure 802.11b/g wireless, deep packet inspection firewall and virtual private network (VPN) technologies in a single, easy-to-use solution. By enforcing the use of VPN encryption on the wireless LAN, the TZ 150 Wireless and TZ 170 Wireless provide impenetrable wireless security, bridging IT administrator security concerns with user demands for wireless in small offices. The TZ 150 Wireless and TZ 170 Wireless integrate tightly with SonicWALL's Global VPN Client and Global Security Client to provide secure wireless and remote access to the corporate network. Additional security layers are provided for the wireless network through rogue AP detection and advanced wireless intrusion detection services, all standard features on SonicWALL wireless solutions. Network administrators create multiple zones of access—for wired and wireless workers as well as guest wireless users—providing an unprecedented level of control and flexibility without compromising network security.

SonicWALL Secure Distributed Wireless Solution

Building on the innovative single point wireless solutions, SonicWALL's Secure Distributed Wireless Solution addresses larger network requirements. The SonicWALL Secure Distributed Wireless Solution consists of a SonicWALL TZ 170 or PRO Series security appliance (PRO 1260, 2040, 3060, 4060 or 5060) running SonicOS Enhanced 2.5 or greater combined with SonicPoints. Available in IEEE 802.11a/b/g and 802.11b/g options, SonicPoints are dependent access points that provide secure wireless LAN connectivity to users on the network



Figure 1: Secure Distributed Wireless Solution – PRO Series security appliances and SonicPoints (APs)

The SonicWALL TZ 170 or PRO Series appliance provides centralized management of both wired and wireless LANs. Through the SonicWALL Discovery Protocol (SDP), the security appliance automatically detects when SonicPoints are added to the (Layer 2) network. After detecting SonicPoints, the security appliance utilizes auto-provisioning capabilities through the SonicWALL Simple Provisioning Protocol (SSPP) to auto-configure all APs with a pre-defined configuration. Utilizing SonicWALL's SonicOS Enhanced operating system, any SonicWALL TZ 170 or PRO Series appliance can take advantage of SonicWALL's Secure Distributed Wireless Solution.

Above and beyond other wireless security solutions, SonicWALL's Secure Distributed Wireless Solution not only addresses wireless-specific security issues, it also provides security policy enforcement and central management for both the wired and wireless LAN. While other wireless solutions leave your network vulnerable to viruses, application exploits, worms and malicious traffic, SonicWALL offers an integrated security solution which enforces firewall policies to all network traffic and is capable of enforcing security services—such as Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service—on both wired and wireless traffic.

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent, file-based virus and malicious-code prevention through a powerful scanning engine that inspects for viruses, worms and other Internet threats in real-time over the corporate network. This unique solution delivers threat protection directly on the security gateway by matching downloaded or e-mailed files against an extensive and dynamically updated database of high-threat virus signatures. Because new threats emerge daily and are often unpredictable, the deep packet inspection architecture is constantly updated to deliver the highest protection possible against an ever-changing threat landscape.

SonicWALL Gateway Anti-Virus inspects e-mail, Web, file transfer and a multitude of stream-based protocols (including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS) and scans instant messaging and peer-to-peer applications, providing comprehensive network virus prevention and control. As an added layer of security, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection not only against external threats, but also against those originating inside the network.

Unlike other threat management solutions, Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service analyze files of any size in real-time—without adding expensive hardware drives or extra memory. Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service is a fundamental requirement for ultimate security protection and a key component of SonicWALL's strategy of providing scalable, multi-layered security to networks of all sizes.

SonicWALL's Secure Distributed Wireless Solution provides advanced features such as: wireless guest services (providing guest Internet access without compromising the trusted network), IPSec VPN enforcement for secure access to the wireless LAN, rogue AP detection and both wired and wireless security and configuration policies that are centrally configured through the security appliance user interface.

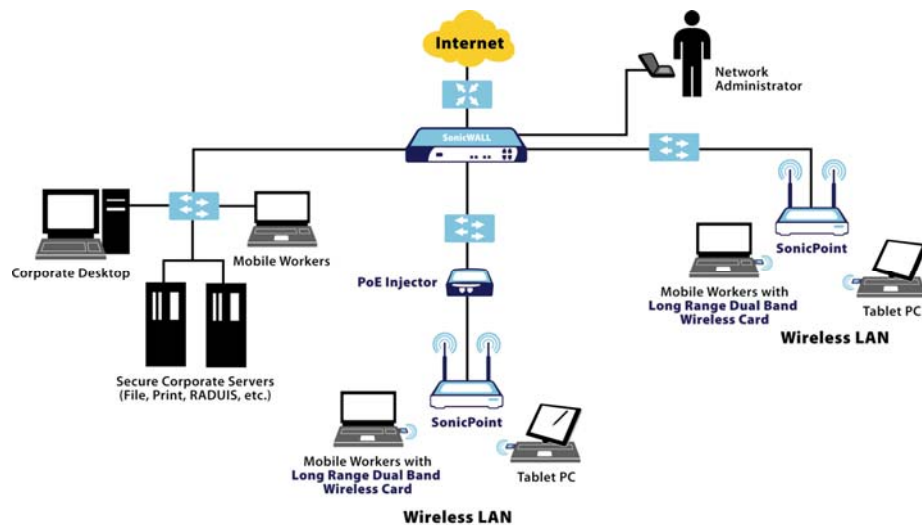


Figure 2: Secure Wireless Deployment

SonicPoints

Available in IEEE 802.11a/b/g and 802.11b/g options, SonicPoints are dependent access points that provide secure wireless LAN connectivity to users on the network. The SonicPoint model is a tri-mode, dual band, dual radio, IEEE 802.11a/b/g compliant, dependent access point. For customers requiring deployment flexibility, SonicPoint G is a dual-mode, single band, IEEE 802.11b/g dependent access point with detachable high gain antennas. SonicPoints high-powered radios support 802.11a and 802.11b/g users. SonicPoints support both 802.11a and 802.11g 108Mbps turbo-mode when used with SonicWALL's Long Range Dual Band Wireless Card.

In addition to IPSec VPN over WLAN, WPA and 802.11i can be configured globally on SonicPoints for security. SonicPoints are compliant with the IEEE 802.3af standards. Therefore, they can accept power over Ethernet (POE)—simplifying wall or ceiling mounting since no electrical wiring needs to be installed. No individual management is required as SonicPoints are completely configurable and manageable from the security appliance's management interface. Finally, 802.11d multi-country roaming directs supported clients to automatically adjust settings (such as power and channel of operation) for compliance with regional regulatory requirements.

Management

SonicWALL's Secure Distributed Wireless Solution allows network administrators to centrally manage and configure all SonicPoints. For geographically distributed offices, SonicWALL's Global Management System (GMS) enables network administrators to globally manage and enforce wired and wireless network security policies for central, branch and telecommuter offices. The solution scales from managing as few as 10 offices to up to thousands of distributed networks.

Summary

Regardless of whether the network is wired or wireless, steps should always be taken to preserve network security and integrity. Because the strongest security approach is to treat your wireless network with the same distrust as the Internet, a gateway security appliance should be deployed which can centrally manage and enforce security on both the wired and wireless networks as well as segment the untrusted network from the internal network.

Although there is much discussion surrounding the latest wireless security standards, it is currently recommended to deploy proven security technologies and techniques such as IPSec VPN. The maturity and proven security of IPSec VPNs assures that your investment in wireless security, as part of a complete security policy, is not wasted. There is no guarantee with these new wireless security standards. They must be proven over time.

A comprehensive firewall appliance that has multiple integrated security functions and integrated wireless functionality offers the most effective and efficient way of providing rock solid protection for your network—both wired and wireless. This solution provides maximum protection by integrating firewall, VPN, gateway anti-virus, intrusion detection, intrusion prevention and content filtering capabilities in a single platform.

Disparately viewed and managed wired and wireless networks are destined for obsolescence. Wireless security must move in a new direction with solutions that converge both wired and wireless networks in a cost-effective, efficient and highly secure platform. Only this type of comprehensive solution can address the needs of all classes of network user and network administrator.

©2005 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. wp_wireless_0805