



Enabling Enhanced Retail Applications with Secure IP and Wireless Communications

Constant VPN connectivity, enhanced wireless security, and central management enable new POS productivity applications

CONTENTS

IP Network and Wireless-Based Productivity Applications	1
Security Challenges for Broadband and Wireless	2
Additional Networking Considerations	4
SonicWALL Solutions for Secure POS Applications	5
Conclusion	8
Appendix	9



Abstract: In an increasingly competitive environment, retailers are seeking ways to improve productivity, reduce costs, and generate incremental revenue. IP network and wireless-based applications offer proven solutions. Popular examples include Internet and wireless-enabled POS systems, browser-based supply chain applications, wireless handheld devices, and self-service kiosks. By improving the timeliness and flow of information, these solutions lead to better overall customer satisfaction and increased profitability.

To successfully adopt IP network and wireless-based applications, retailers need solutions that overcome the inherent challenges posed by these technologies. They need a means of ensuring business continuity in the event of a network failure, protecting sensitive customer and business information, and facilitating the deployment and management of widely distributed POS devices.

This white paper describes how retailers are gaining a competitive advantage from these new applications. It explains the security considerations of these networks, and describes how SonicWALL POS solutions address these requirements, providing retailers with a competitive edge.

IP Network and Wireless-Based Productivity Applications

As retailers build systems based on IP networks and extend these systems wirelessly, they are enhancing both front and back office applications to improve customer service and drive revenue growth.

Front office applications such as IP-based credit card processing and temporary wireless POS terminals are leading to faster transaction times which increases customer satisfaction. Back office applications such as Internet-based ordering, employee portals, and wireless inventory management are creating efficiencies and dramatically reducing costs.

Front Office Applications

- ▷ **IP Credit Card Processing** - Internet-based credit card processing allows retailers to reduce costs and dramatically speed up transaction times.
- ▷ **Customer Loyalty Programs** - New generation POS systems accept loyalty and gift cards in addition to credit cards, offering customers greater payment choices and supporting retailers' customer loyalty programs.
- ▷ **Mobile Order Taking** - Wireless handheld devices enable waiters in restaurants to take orders and process payments at a customer's side, improving service and reducing the risk of fraudulent charges.
- ▷ **"Line-Busting"** - Wireless applications can bring the transaction to the customer rather than making the customer wait in the checkout line. Sales associates scan a waiting customer's merchandise using a handheld computer and provide the customer with a plastic card or bar code printout, which the cashier then scans to process the payment.
- ▷ **Temporary POS Terminals** - Wireless POS terminals set up in mall walkways or at trade shows can take advantage of temporary short-term sales opportunities.
- ▷ **Wireless Hot Spots** - Wireless hot spots deliver convenient public Internet access, allowing restaurants, coffee shops and bookstores to improve customer satisfaction and generate incremental revenue.
- ▷ **Kiosks** - Kiosks give customers the option of searching gift registries or looking up catalog items online while they are in the store.

Back Office Applications

- ▶ **Internet-Based Ordering** - Internet-based ordering applications facilitate closer cooperation with the supply chain, creating efficiencies, improving margins, and reducing costs.
- ▶ **Employee Portals** - Internet-enabled POS terminals can be used to extend HR functions directly to employees, offering access to Web-based training courses, online forms and benefits information.
- ▶ **Inventory Management** - Wireless handheld devices can be used to perform inventory management on a regular basis, gaining real-time visibility into POS transaction totals and stock levels.
- ▶ **Hard-to-Wire Locations** - Wireless POS terminals are ideal for hard-to-wire buildings or large, open spaces.
- ▶ **Access for Traveling Managers** - Wireless access to corporate resources can be provided for regional managers who move from store to store.

Underlying all of the applications listed above is a trusted network infrastructure, providing secure, fast and reliable connectivity between store locations as well as secure wireless connectivity within each store:

- ▶ **Connecting Stores** - For most retailers, the traditional WAN connectivity choices of dial-up and frame relay are giving way to virtual private networks (VPNs) over broadband Internet connections (see appendix #1). Broadband provides the necessary high-speed connectivity at a cost retailers can afford, from small, independent merchants to large retail chains. Coupled with VPN technology for secure communications over the public Internet, broadband connectivity is a compelling option for retailers.
- ▶ **Wireless Connectivity** - To take advantage of the exciting wireless-based applications listed above, retailers need a secure wireless network capable of protecting confidential data being transmitted over public airwaves.

Security Challenges for Broadband and Wireless

Broadband and wireless networks are inherently insecure because they transmit information over the public Internet and public airwaves, respectively. Security risks of broadband and wireless connectivity include stolen customer information, viruses, worms and inappropriate use of network resources. These threats erode productivity, can prevent sales if the network is taken down, and open the door to possible legal action should a customer's confidential information fall into the wrong hands.

To protect their customers and their business, retailers need connectivity solutions that mitigate the following potential security risks.

Hacker Attacks

Many retailers are moving from dial-up and frame relay to broadband connections in order to take advantage of fast, affordable connections. However, if the broadband connection is not properly secured, the POS systems using these connections can be compromised. This can lead to stolen corporate or customer information, destruction of vital business databases, and theft of Internet services all of which can interfere with day-to-day business transactions.

Retailers must secure their Internet connections using a firewall and protect sensitive data being transmitted over the Internet with a virtual private network (VPN) (see figure 1.). Encryption provided by VPNs is required for retailers that want to participate in certain payment programs, such as the Visa USA Cardholder Information Security Program (CISP) (see appendix #2).

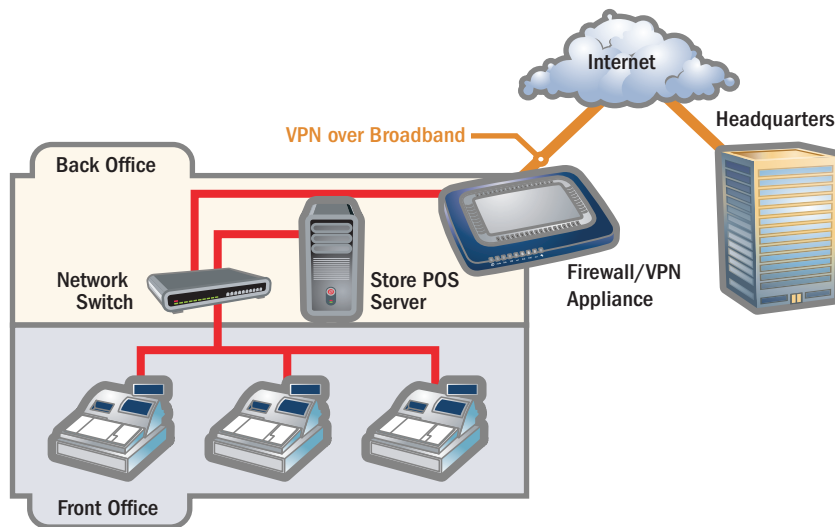


Figure 1 - Virtual Private Network.

Viruses and Worms

Increasingly, retailers are deploying open operating systems such as Microsoft and Linux. Virus creators target Microsoft products because of their popularity, while hackers target both Microsoft and Linux systems due to their popularity and known vulnerabilities. As outlined by Microsoft on its security website (<http://www.microsoft.com/security/protect/>), anti-virus solutions are crucial in these systems as are firewalls, which can limit the damage done by worms.

Certain retail deployments are particularly vulnerable to viruses and worms:

- ▷ **POS Terminals** - New generation POS terminals based on open systems have the same vulnerabilities commonly seen on corporate networks. Yet, since the POS system is the lifeblood of a retail organization, there is no room for downtime due to virus outbreaks.
- ▷ **Managers' Laptops** - Manager's laptops can become breeding grounds for viruses, since they are mobile and often get connected to multiple, untrusted networks. In addition, managers remotely connecting to the local restaurant, store or corporate office via their home computer can unwittingly introduce viruses that enter via unsecured home networks

Wireless Network Breaches

Wireless networks are even more vulnerable to hacker attacks because data travels over public radio waves and can be intercepted with fairly simple technology. In fact, if a store's or restaurant's wireless network is not protected, a hacker could even intercept communications while sitting in the parking lot.

It's all too common for wireless networks to employ no security measures at all, or to use an easily defeated method, such as MAC address filtering or Wired Equivalent Privacy (WEP). WEP is based on a shared key common to all users, making it an easier target for security attacks. Using readily available tools like AirSnort or WEPCrack a hacker could root out these keys in as little as five hours.

Additional Networking Considerations

Ensuring Business Continuity

Once an IP application becomes an integral part of a retailer's network, loss of Internet connectivity can prevent sales transactions, disrupting productivity. Broadband connections do occasionally become unavailable. Therefore, it's critical for the retailer to have both a reliable connection and a back up. Options for the redundant connection can include a second broadband line or a dial-up phone line (see figure 2). For optimum business continuity, the POS connectivity solution should be able to sense when the primary connection becomes unavailable, and automatically activate the back-up connection. Similarly, for optimum performance, the solution should automatically reinstate the primary connection when it returns to service.

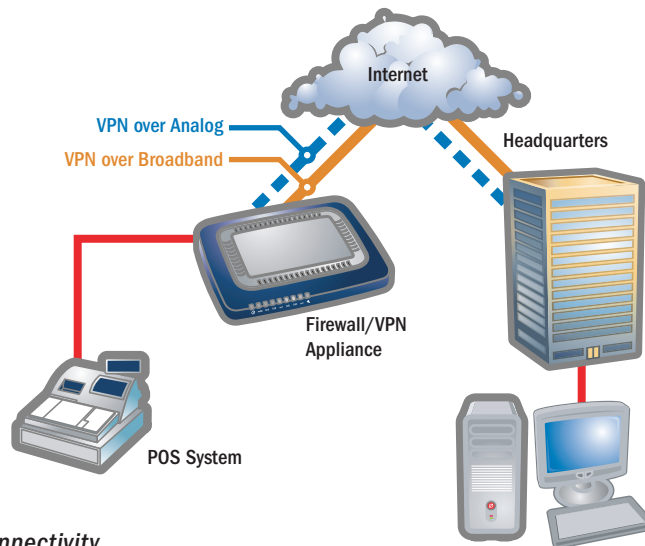


Figure 2-Constant VPN Connectivity.

Central Control and Management

Easy central management is an essential ingredient for security. Retailer networks often comprise of hundreds or thousands of widely distributed broadband and wireless Internet security devices. Manually upgrading anti-virus software and content filtering software, reconfiguring hardware, or deploying a new application can be extremely time-consuming and costly. It can also lead to inaccuracies and oversights. Therefore, retailers need automated tools for network management. Ideally, each firewall should forward its logs to a single collection point within the corporate LAN, creating a single repository for monitoring virus and hacking attacks against outward-facing connections.

Inappropriate Web Surfing

While providing employees with access to sites that are not business-related is not precisely a security risk, it does degrade productivity and can potentially introduce legal problems. Businesses that do not prevent access to objectionable content expose themselves to potential legal liability that can arise if a co-worker or customer can see offensive material on an employee's computer. By implementing a content filtering solution, retailers can restrict access to certain websites. For example, they could allow access to sites with merchandise information and employee portals, but disallow access to all others.

The security stakes are high for retailers. While the business benefits of broadband and wireless are too great to ignore, these technologies do expose retail networks to many vulnerabilities. Security breaches can result in lost productivity, missed revenue opportunities and potential legal action. Security can no longer be considered an add on. Instead, it must be integrated into every network node, deployed at the perimeter of a network and be easily managed and updated.

SonicWALL Solutions for Secure POS Applications

SonicWALL offers an integrated, flexible, easy-to-manage security platform for retail POS networks. SonicWALL's security platform enables retailers to capitalize on the productivity benefits of real-time POS applications for IP and wireless networks while protecting confidential data and ensuring continuous connectivity.

SonicWALL TELE3 SP Firewall/VPN Appliance

Continuous Internet connectivity via an integrated, automated analog modem

The TELE3 SP is a compact, all-in-one security solution that includes VPN connectivity based on hardware-accelerated 3DES encryption and a hardened, ICSA-certified stateful packet inspection firewall. The TELE3 SP overcomes the inherent reliability limitations of broadband connections with an integrated analog v.90 modem and automated fail-over and fail-back technologies.

The TELE3 SP continuously monitors availability by checking link status and a heartbeat to a remote device. Should either fail, the device automatically fails over to the integrated analog modem. When the broadband connection has been re-established, the TELE3 SP detects the restored connection and fails back. Thus, retailers have constant access to critical data with the highest available performance. This ensures an uninterrupted revenue stream and continued employee productivity.

Several configurable Toll Saver features incorporated into the TELE3 SP appliance minimize the costs of back-up analog connectivity. For example, the connection is automatically terminated if there is no activity for a specified interval and then re-connected once activity is detected. For retail locations without broadband connectivity, or where a broadband connection is impractical, the integrated analog modem can be the primary means of connectivity.

At about the size of a paperback book, the TELE3 SP is designed to be wall or surface mounted out of harm's way-for example, under the counter, on the wall, or inside a kiosk.

SonicWALL SOHO TZW Firewall/VPN Appliance

Solid wireless LAN security through enforced WiFiSec encryption

The award-winning SOHO TZW firewall/VPN appliance provides secure wireless and wired connectivity to POS registers and kiosks as well as wireless-enabled laptops and handheld devices. This eliminates the need for expensive and restrictive wiring solutions. A Web-based interface and installation wizards simplify installation, saving time and money.

Offering unsurpassed security for wireless networks, the SOHO TZW features a high-powered (200mw) 802.11b wireless access point integrated with a stateful packet-inspection firewall and VPN appliance. By creating IPSec-based VPNs and enforcing them on the wireless LAN (WLAN), the SOHO TZW establishes secure tunnels that encrypt communications containing sensitive customer and business information.

Retailers that want to provide wireless access for guests-while protecting their internal networks - can take advantage of the SOHO TZW Wireless Guest Services feature. It enables the company to create a separate, trusted access zone for guest wireless users, while maintaining the security of VPN access to the corporate LAN, all on a single device. The SOHO TZW accomplishes this by creating a separate service for guest users, who are only allowed to send and receive data through the WAN port connected to the Internet, and can never connect to the LAN port, regardless of the firewall configuration (see figure 3).

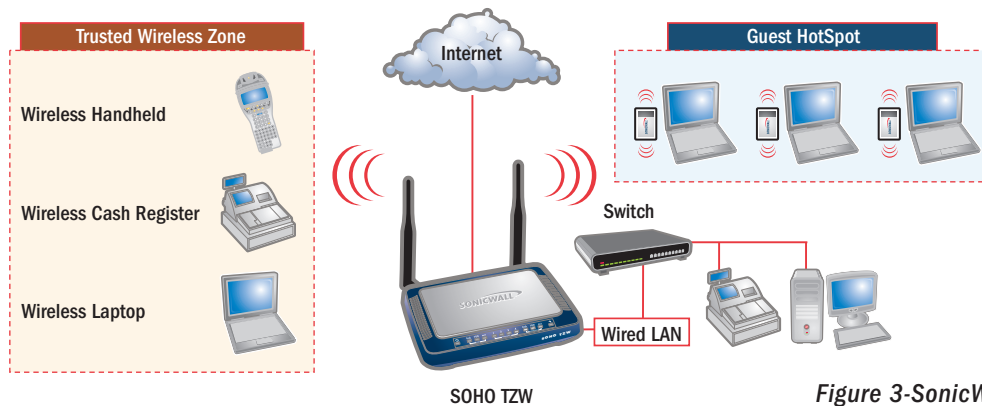


Figure 3-SonicWALL SOHO TZW.

SonicWALL SOHO TZ 170 Firewall/VPN Appliance **Flexible WAN/LAN connectivity with Optional Port**

Like all SonicWALL appliances, the TZ 170 is a stateful packet inspection firewall with support for IPSec VPN. The TZ 170 also provides significant interface flexibility with its built in five-port switch, dedicated WAN, and Optional Port. This flexibility allows for multiple connectivity scenarios in the POS network environment utilizing a single network device.

The five-port switch enables organizations to support the POS LAN on a single device for up to five POS terminals or back-office servers. The WAN port offers support for any type of broadband connectivity such as DHCP or PPPoE provisioned DSL or cable modem service.

The Optional Port allows the TZ 170 running SonicOS Enhanced (SonicWALL's next generation operating system) to be configured with dual WAN interfaces for redundant, load balanced ISP connectivity. It can also serve as an additional DMZ interface, segmented from the LAN with its own firewall rules. Alternatively, it can also be used to add wireless to the POS network by connecting a SOHO TZW.

SonicWALL PRO Series of Firewalls **Range of scalable appliances for VPN tunnel termination at headquarters**

Located at headquarters, the SonicWALL PRO series of firewall/VPN appliances act as VPN concentrators, terminating up to thousands of VPN tunnels from SonicWALL TELE3 SP, SOHO TZW and TZ 170 appliances located at stores and restaurants. By analyzing every packet that enters the corporate network, SonicWALL PRO products ensure security without slowing network performance.

The PRO series of products offers multiple, configurable interfaces for network segmentation, dual WAN capabilities, and dedicated fail-over ports. For constant connectivity, retailers can deploy SonicWALL PRO Series appliances in a redundant, high-availability configuration, with one appliance in active mode and another on stand-by for fail-over.

Running the latest SonicOS firmware, the PRO series offers flexible and powerful configuration options to overcome the most challenging IP networking scenarios. Hardware cryptographic acceleration for all components of IPSec, including AES, faster processors and more memory enable the PRO series to serve any organization's VPN needs now, while allowing for future enhancements and growth.

SonicWALL Global Management System **Central control of all SonicWALL devices through a simple Web-based management interface**

SonicWALL Global Management System (GMS) enables retailers to centrally and globally manage all SonicWALL Internet security appliances whether they have just a few or several thousand (see figure 4).

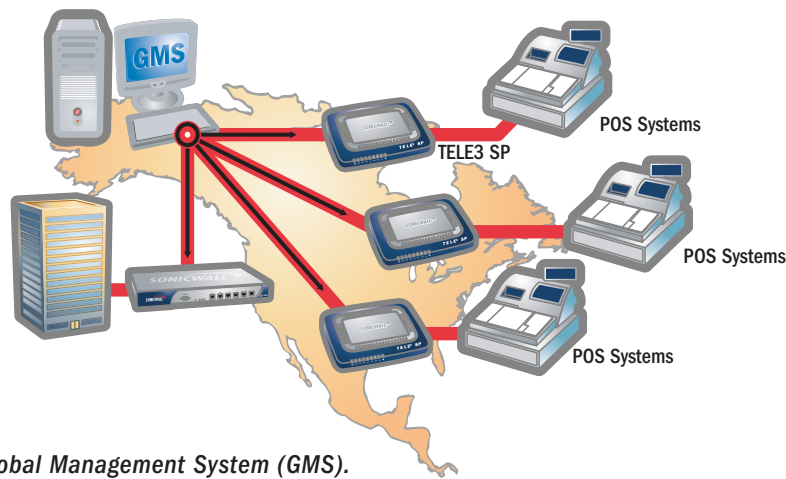


Figure 4-SonicWALL Global Management System (GMS).

Network administrators use SonicWALL GMS to quickly provision VPN tunnels, firewall rules, and other configurations for each store. They can then easily distribute new global or store-specific security policies and firmware upgrades adding new firewall and security features to remote SonicWALL appliances. SonicWALL GMS also allows network administrators to distribute security applications, such as SonicWALL Complete Anti-Virus or SonicWALL Content Filtering Service (CFS) software. To minimize network load, distribution of security policies and firmware updates can be scheduled for periods of low network traffic.

SonicWALL's Global Management System allows retailers to establish multiple sets of user privileges so that they can divide management responsibilities among several network administrators or operators. With clear-cut management responsibilities and appropriate user privileges, administrators become more productive and effective. SonicWALL GMS also facilitates network monitoring by providing reports and daily logs of usage trends, firewall activities, and other security events. Support for external syslog servers and SNMP traps is included, as is the ability to integrate SonicWALL GMS into other systems with its ability to accept XML commands.

Complete Anti-Virus and Content Filtering Service
Enterprise-class, centrally managed anti-virus and content filtering solutions

SonicWALL security appliances also support a portfolio of security applications:

Complete Anti-Virus - Developed in partnership with McAfee, SonicWALL Complete Anti-Virus protects IP-based POS systems and manager's workstations from viruses and worms. Retailers are particularly vulnerable to virus attacks because they use open systems based POS products and shared manager workstations. SonicWALL's desktop anti-virus solution provides automatic anti-virus policy enforcement, requiring users to utilize the anti-virus software and automatically providing the updates before passing traffic through the SonicWALL device. It also features "rapid E-mail attachment blocking," which blocks harmful virus/worm-specific attachments even before the virus signatures are available.

Content Filtering Service - SonicWALL Content Filtering Service (CFS) lets retailers provide employees and customers with Internet access to business-related sites while blocking sites that are inappropriate or non work-related. SonicWALL CFS features a powerful rating and caching architecture that leverages a comprehensive database of over four million continuously updated websites, domains, and IP addresses. Managed through any SonicWALL firewall, SonicWALL CFS delivers enterprise-class content filtering at an affordable price by eliminating the need for a dedicated filtering server.

Additionally, retailers can enter a wildcard-based list of URLs into any SonicWALL appliance limiting the available websites on any system to those that are work-related. This will prevent employees and customers from using POS systems or kiosks for anything other than intended business functions. SonicWALL Content Filtering Service adds an important layer of protection from legal liabilities for businesses offering Internet access to customers in public areas.

Conclusion

IP-based productivity applications for POS systems enable retailers to improve service, enhance productivity, and differentiate themselves for a competitive edge. To deploy these applications, stores and restaurants need broadband or wireless Internet access. They must also secure these networks to protect confidential customer information and defend against the devastating effects of security breaches, viruses, and worms.

SonicWALL offers a complete retail/POS solution, unavailable from any other vendor. Broadband connectivity with integrated fail-over ensures constant VPN connectivity. Advanced wireless LAN security through enforced 3DES encryption protects confidential information as it travels over the public airwaves. Central control of all remote SonicWALL devices through a simple Web-based management interface facilitates scalability. A range of firewalls for VPN termination at headquarters enables retailers and restaurants to purchase the right size solution today and scale as the business grows.

All SonicWALL devices support SonicWALL anti-virus solutions, which safeguard the network from viruses and worms, and content filtering solutions, which improve productivity and protect against legal liability. Finally, all solutions offer the cost-effectiveness and ease of management required for retailers and restaurants.

For more information about SonicWALL solutions, call FORTRESS Network Security at 1-866-948-7377 or visit www.fortressnetworksecurity.com.

Appendix

Appendix 1

Until a few years ago, most retailers relied on either dial-up or frame relay for connectivity into their POS systems. Now many are switching to broadband VPN over DSL or cable modem. Broadband improves POS application performance and dramatically reduces connectivity costs.

Compared to frame relay, broadband connectivity:

- ▷ Is a fraction of the cost
- ▷ Provides higher throughput

Compared to dial-up, broadband connectivity:

- ▷ Cuts credit card transaction time to a few seconds
- ▷ Improves reliability of POS polling and credit card processing
- ▷ Eliminates charges for long distance and extra phone lines
- ▷ Drastically increases throughput for current and future applications

Appendix 2

VPNs are requirements for retailers that want to participate in certain payment programs. The Visa USA Cardholder Information Security Program (CISP), for example, stipulates a standard of due care and enforcement for protecting sensitive customer information : all organizations that store, process, or transmit confidential account information and personal data are expected to comply with basic security requirements. These requirements include installing a firewall, encrypting data traveling across a VPN tunnel, and installing and continually updating anti-virus software.