



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	2
Security Challenges for Broadband and Wireless	3
Additional Networking Considerations	5
SonicWALL Solutions for Secure POS Applications	6
Conclusion	10

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 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 increase 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 HotSpots** – Wireless HotSpots 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 these applications 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 **Broadband Use in Retail**). 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 exciting new wireless-based applications, 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.

Broadband Use in Retail

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
- Provides bandwidth to support future applications

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 below). 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 (see **Credit Card Information Security**).

Credit Card Information Security

VPNs are required for retailers 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.

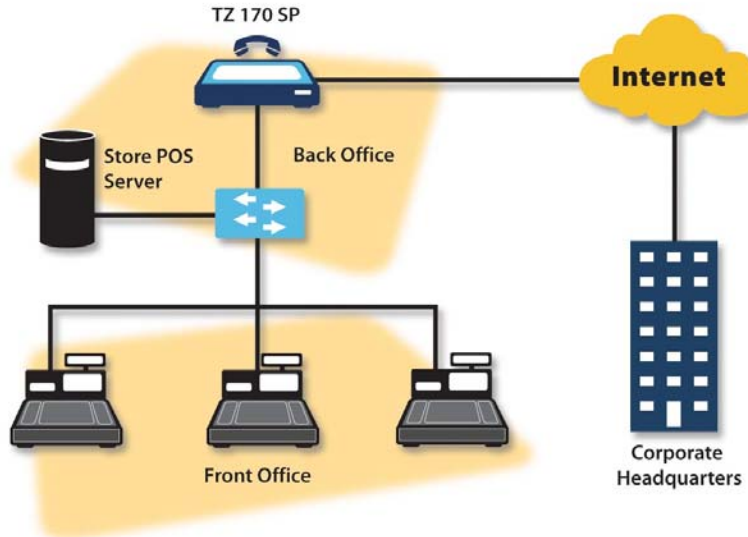


Figure 1
Virtual Private Network

Viruses and worms

Increasingly, retailers are deploying open operating systems such as Windows 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 Web site (<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** – Managers' 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 just a few 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 primary connection and a seamless back-up option. 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.

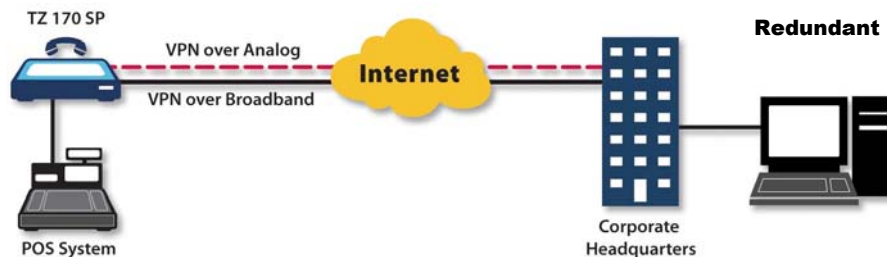


Figure 2
Redundant Connection Options

Central control and management

Easy central management is an essential ingredient for security. Retailer networks are often comprised of hundreds or thousands of widely distributed retail locations. Manually upgrading anti-virus 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 device should forward its logs to a single collection point within the corporate LAN, creating a single repository for monitoring viruses 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 Web sites. 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 designed into the network, deployed at the perimeter and be easily managed and updated.

SonicWALL Solutions for Secure POS Applications

SonicWALL offers integrated, flexible and easy-to-manage security platforms for POS networks. SonicWALL's security platforms enable 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 TZ 170 Series

Powerful, proven network protection for small networks

The TZ 170 is the base model of the SonicWALL TZ 170 Series and provides solid, proven security for small networks, including POS networks in retail and restaurant locations. Offering a wide array of integrated security and reliability capabilities in a cost-effective solution, the SonicWALL TZ 170 scales as your organization grows and your needs change.

The SonicWALL TZ 170 offers:

- A powerful deep packet inspection firewall to protect against the latest threats
- IPSec virtual private networking (VPN) for secure communications over the Internet
- Support for a second, back-up broadband connection, providing WAN redundancy and load balancing
- Intuitive configuration wizards to simplify even the most complicated tasks
- Support for advanced security services to provide multi-layer security
- Support for award-winning Global Management System (GMS) for comprehensive monitoring, management and reporting

Three additional SonicWALL TZ 170 Series models provide added hardware capabilities.

SonicWALL TZ 170 SP

Integrated failover to back-up broadband connection or integrated analog modem for critical POS deployments

The SonicWALL TZ 170 SP is a complete security solution that includes high-performance VPN connectivity and an ICSA-certified stateful deep packet inspection firewall. The TZ 170 SP overcomes broadband failures with the ability to fail over to a backup broadband connections as well as an integrated v.92 modem analog.

The TZ 170 SP continuously monitors connection availability by checking link status and a heartbeat to a remote device. Should either fail, the device automatically fails over to the backup broadband connection or the integrated analog modem. When the primary broadband connection has been re-established, the TZ 170 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.

Configurable Toll Saver features minimize the costs of backup analog connectivity. For example, the connection is automatically terminated if there is no activity for a specified interval and then reconnected once activity is detected. For retail locations without broadband connectivity, or where a broadband connection is impractical, the integrated analog modem can serve as the primary connection.

SonicWALL TZ 170 Wireless

Secure 802.11b/g wireless platform to unwire your retail locations

The SonicWALL TZ 170 Wireless 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.

Offering unsurpassed security for wireless networks, the TZ 170 Wireless features a dual 802.11b/g wireless access point integrated with a stateful deep packet inspection firewall and VPN appliance. By creating IPSec-based VPNs and enforcing them on the wireless LAN (WLAN), the TZ 170 Wireless establishes secure tunnels that encrypt communications containing sensitive customer and business information.

Retailers who want to provide wireless access for guests – while protecting their internal networks – can take advantage of the Wireless Guest Services feature. It enables the creation of a separate access zone for guest wireless users, while separating that zone from the sensitive POS network. The TZ 170 Wireless and TZ 170 SP Wireless accomplished 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).

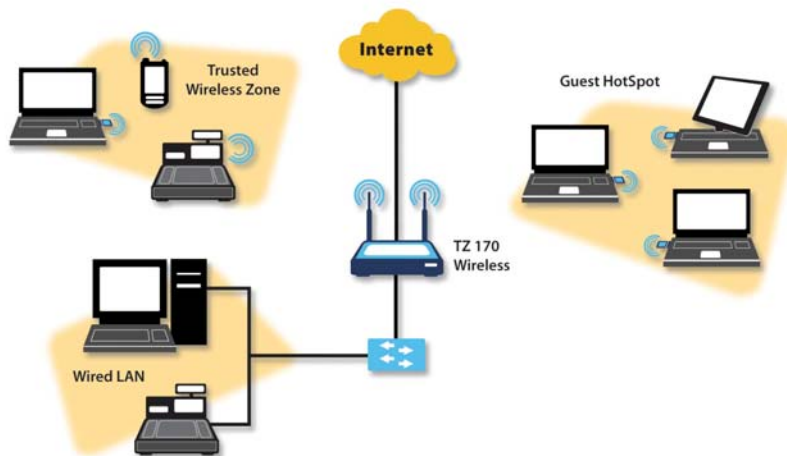


Figure 3
Wireless Guest Services

SonicWALL TZ 170 SP Wireless

Ultimate platform combines secure wireless with integrated and automated failover

The ultimate wired and wireless security platform for retail POS locations, the SonicWALL TZ 170 SP Wireless combines the secure wireless capabilities of the TZ 170 Wireless with the multiple failover options provided by the TZ 170 SP.

SonicWALL PRO Series

Range of powerful, scalable solutions for a retailer's headquarters and larger retail locations

Typically used at a retailer's headquarters, SonicWALL PRO Series appliances act as the central data communications hub for distributed retail organizations. PRO Series appliances can scale to handle up to 4,000 remote retail locations. These flexible, high performance products also offer high availability features to assure the constant availability of critical central resources.

The PRO Series further offers multiple, configurable interfaces for network segmentation, dual WAN capabilities, and dedicated failover ports. Running the latest SonicOS firmware, the PRO Series offers flexible and powerful configuration options to overcome the most challenging IP networking scenarios.

Advanced security services

SonicWALL security platforms offer an array of advanced security capabilities for multi-layer security, which allows you to add features and functionality as your security needs grow over time. These services are tightly integrated into SonicWALL security platforms. The complete SonicWALL security solution is managed with a common user interface, reducing the overall cost of ownership.

SonicWALL Complete Anti-Virus

Rapid enforced virus protection for Windows-based POS systems

Retailers are becoming more vulnerable to virus attacks because their POS systems are moving to open operating systems like Microsoft Windows. Developed in partnership with McAfee®, SonicWALL Complete Anti-Virus rapidly protects against fast-moving viruses that can cripple Windows-based POS systems. SonicWALL's anti-virus solution utilizes patent-pending enforcement architecture to provide automatic anti-virus policy enforcement. POS systems are automatically updated with the latest anti-virus software and signature files before any traffic can be passed through the SonicWALL appliance. This service also features a rapid e-mail attachment blocking feature which blocks known harmful attachments in the critical first hours before the new virus signatures are available.

SonicWALL Intrusion Prevention Service (IPS)

Protection against sophisticated application layer attacks

SonicWALL Intrusion Prevention Service (IPS) integrates a configurable, ultra-high performance deep packet inspection engine and dynamically updated database of over 1,800 attack and vulnerability signatures to protect networks against sophisticated application layer attacks, including buffer overflow vulnerabilities in software, worms, Trojans, backdoor exploits and the use of peer-to-peer and instant messaging applications. With its powerful performance, leading-edge features and extensive management capabilities, SonicWALL IPS delivers the advanced network protection with low total cost of ownership.

SonicWALL Content Filtering Service (CFS)

Manage access to Web content to enhance productivity and limit liability

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 hamper productivity. SonicWALL CFS features a powerful rating and caching architecture that leverages a comprehensive and continuously updated database of over four million Web-sites, domains, and IP addresses. Additionally, retailers can customize the content filtering solution to allow or deny specific Web sites based on their particular business needs. SonicWALL Content Filtering Service adds an important layer of protection from legal liabilities for businesses offering Internet access to customers in public areas.

SonicWALL Global Management System (GMS)

Scalable Central Management and Reporting

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

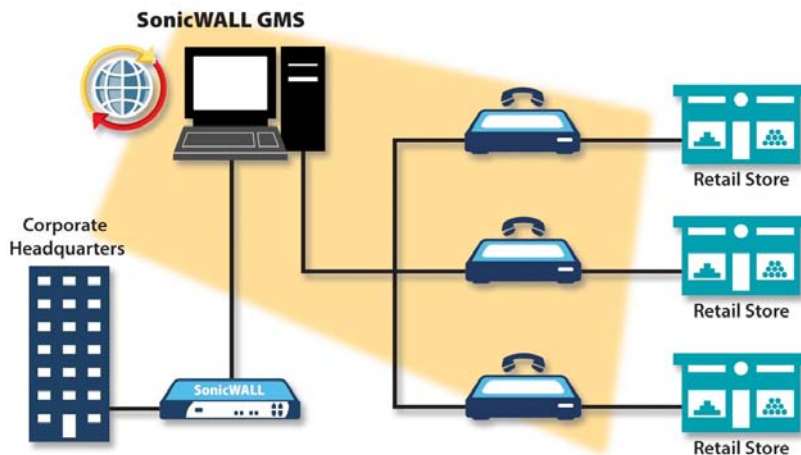


Figure 4
Global Management
System

Network administrators use SonicWALL GMS to quickly provision VPN tunnels, security policies, and other configurations for each store. They can easily distribute new chain-wide or store-specific security policies and firmware upgrades adding new security features to remote SonicWALL appliances. SonicWALL GMS also allows network administrators to fully manage SonicWALL's advanced security services, such as SonicWALL Complete Anti-Virus and SonicWALL Intrusion Prevention Service. To optimize network performance, 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 administration privileges so that they can divide management responsibilities among several network administrators and operators. SonicWALL GMS also facilitates network monitoring by providing logs and reports of usage trends, security events, and other activities.

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 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 failover ensures constant VPN connectivity. Advanced wireless LAN security through enforced 3DES/AES encryption protects confidential information as it travels over the public airwaves. Central control of all remote SonicWALL appliances 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 appliances support SonicWALL enforced-anti-virus solutions, which safeguard the network from viruses and worms, content filtering solutions, which improve productivity and protect against legal liability, and intrusion prevention solutions, which protect networks against today's sophisticated application threats. Finally, all solutions offer the cost-effectiveness and ease of management required for retailers and restaurants.

For more information about SonicWALL solutions, call SonicWALL Sales at 888-557-6642, e-mail sales@sonicwall.com, or contact your authorized SonicWALL Solutions Provider.