

# Virtual Private Networks for Small to Medium Organizations

## CONTENTS

Overview	1
Enabling of the Distributed Workplace	1
Evaluating Your VPN Options	6
SonicWALL's Integrated Security and VPN Solution	10
Assembling Your SonicWALL Security/VPN System	13
Conclusion	15

*Abstract: Demand for remote access is being driven by an undeniable combination of business, social and technology trends. Employee demands for flexible work arrangements, company drives for improved productivity and reduced costs, and new enabling technologies are fueling the emergence of the distributed workplace. The distributed workplace is made up of headquarters, branch offices, telecommuters, mobile workers, contractors, suppliers, and partners, all needing secure access to an organization's network resources.*

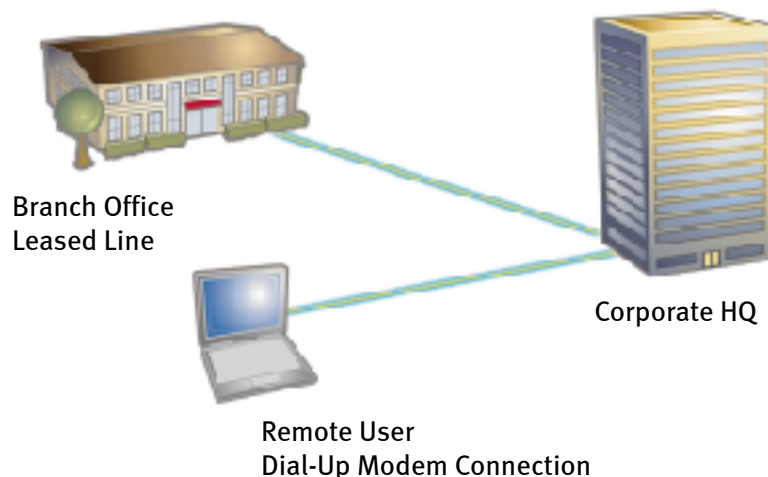
*Until recently, connecting remote offices and users remained the province of only the largest companies with enough technical skill and financial resources. Why? Because until now, most small and medium organizations that wanted to link remote offices and users were faced with limited bandwidth options, high prices, and difficult technical requirements.*

*Today, two key technologies are converging to open up cost-effective, robust, Internet-based remote access solutions for small and medium organizations. First is the rapid proliferation of affordable broadband Internet access technologies, including DSL (Digital Subscriber Line), cable, and wireless. Second is the emergence of standards-based Virtual Private Network (VPN) solutions that allow small and medium organizations to transfer private data securely over the public Internet. Together, these technologies promise to usher in the new distributed workplace to enable small and medium organizations to tap into the compelling benefits of remote access to work smarter, reduce costs, and gain competitive advantage.*

*This white paper shows how small to medium-sized organizations can use a Virtual Private Network and broadband Internet access to connect geographically dispersed offices and users to create a distributed workplace. It explains how a VPN works, how to evaluate VPN technology options, and how to deploy a VPN solution for your organization.*

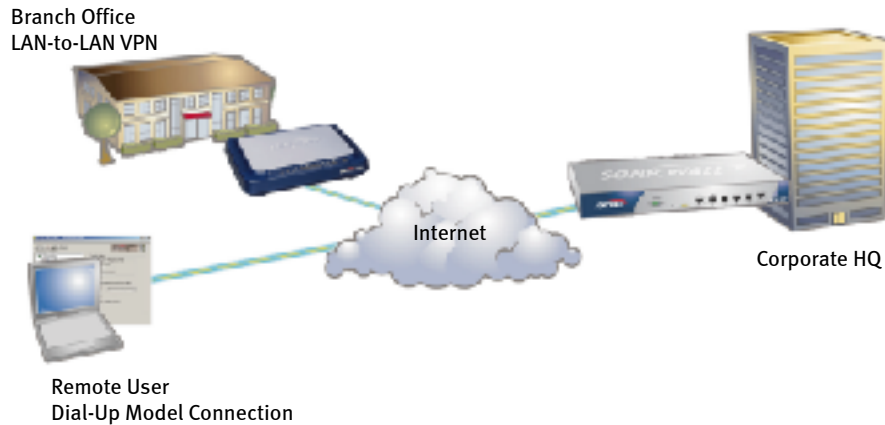
## **ENABLING THE DISTRIBUTED WORKPLACE**

Traditional remote access required companies to lease expensive, dedicated data lines or maintain modem banks and telephone lines, and pay telecommunication usage charges to support dial-up users. The prohibitive costs of dedicated data lines forced most small and medium organizations to use slow, dial-up connections for remote access. Even this option was expensive and complex to deploy.



*In the old model of remote access, remote sites and the corporate network are directly linked using expensive leased lines or usage-based dial-up connections.*

With the advent of affordable broadband and standards-based VPN, small and medium organizations can bypass these expensive and complex remote access solutions. A VPN delivers remote access via ubiquitous Internet connections. With today's VPN technology and broadband connections, companies of any size use the Internet to securely extend the reach of their network resources.



*With the advent of ubiquitous Internet access and VPN technology, remote access is handled through the same connection used for Internet service.*

### Working Smarter with VPNs

Implementing a VPN for remote access to your network creates new ways of getting things done, including:

- ▶ Arming employees with up-to-date information, enabling them to make the most informed decisions possible.
- ▶ Streamlining access to information and centralizing mission-critical data and content.
- ▶ Reducing networking costs by using the Internet.
- ▶ Extending the workplace beyond the office walls to increase employee productivity through workplace flexibility.
- ▶ Providing an edge in recruiting employees looking for flexible work schedules.
- ▶ Fostering competitive advantage by creating closer links with customers, suppliers, and employees.
- ▶ Allowing for centrally enforced security and remote access policies.

### VPN Coupled with Broadband Brings Remote Access to Life

With broadband Internet connections, VPN comes to life as a serious remote access solution for small to medium sized organizations. The new dynamics of broadband technology coupled with VPN is morphing the typical slow dial-up telecommuter who occasionally checks e-mail into an indispensable team member with the ability to contribute to the mission regardless of physical location. Downloading a large PowerPoint presentation that took an hour using a dial-up modem takes only a few minutes. E-mail is instant, with no more dialing up to send or receive messages. Intranets and databases are quickly and seamlessly accessed, and new Web-based collaborative tools keep remote users in the loop at the office.

VPN can be easily integrated into wireless networking technology for mobility at home or offices. An employee with a notebook can use VPN connected to the broadband Internet connection accessible from a wireless LAN in the home or

small office. And because many broadband Internet modems use the Ethernet interface to connect to computers, multiple users can share a broadband connection.

### VPN's Bottom-Line Benefits

VPN delivers powerful "win-win" solutions for both employers and employees. By synching work with peak performance times, creating uninterrupted time for focused work, and eliminating time-consuming commutes, telecommuters can boost their productivity 22 percent to 45 percent (The Gallup Organization and Opinion Research). Studies also show telecommuting delivers other compelling benefits for organizations to capture big savings that can be poured back into the business with positive effect, including:

- ▶ Employers can save up to 63% of absenteeism costs per telecommuter (ITAC).
- ▶ Telecommuting can reduce manager to staff ratios from 1-4 to 1-40 (Fort Lauderdale Sentinel).
- ▶ Companies can save up to \$8,000 annually in office space for each telecommuter. Companies save money on office space and its required components, such as rent, furniture, lighting, and facilities.
- ▶ Deploying telecommuter solutions are easier and cheaper than ever. Powerful and affordable PCs, broadband Internet access, and VPN solutions enable companies to cost-effectively set up telecommuters.
- ▶ US employers could save \$441 billion in reduced absenteeism and recruiting costs, and increased productivity from telecommuting.

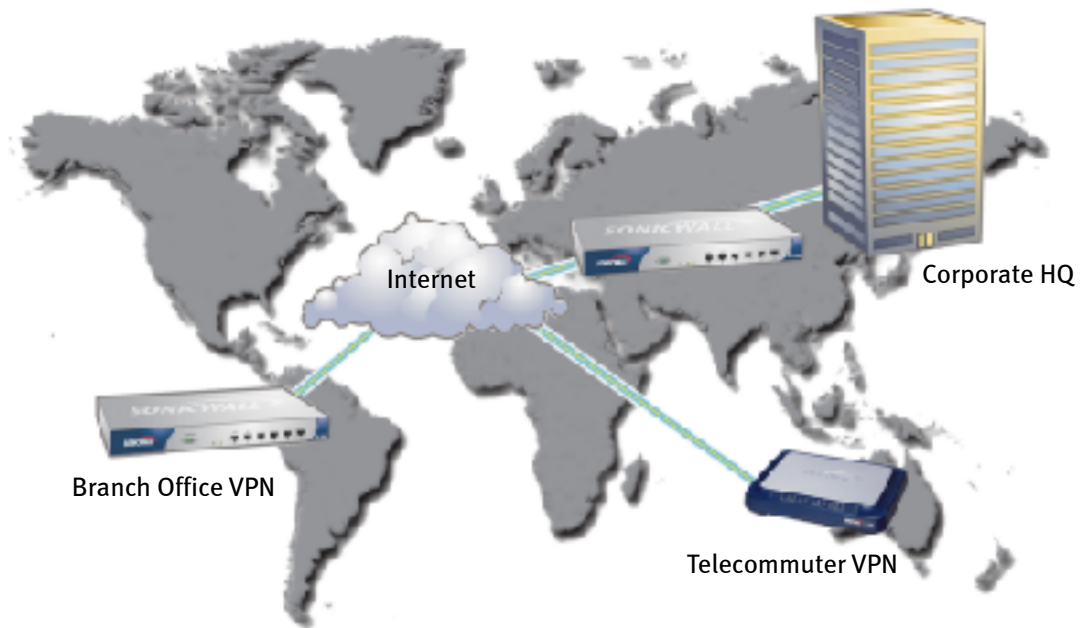
### Beyond the Technology

VPN is about enabling remote access for your organization. To help your organization manage the effects of a VPN, you need to create a remote access policy and procedures for supporting remote users. You'll need to choreograph the new technology, supporting tools, and employee work activities to get the most out of your VPN. Coordinating the implementation of a telework program across different people and groups within your organization takes careful planning. A remote access policy and procedures guide lays the foundation for effectively implementing a remote access solution by specifying the rules for employees working remotely.

## VPN 101

Internet-based remote access presents challenges in protecting the confidentiality and integrity of essential business information as it travels over the public Internet. Hackers can capture the data as it passes over the Internet and convert it into a readable format or gain entry into your network. Exposure to these security risks means unauthorized users can initiate fraudulent transactions, as well as steal, alter, or destroy confidential information, exposing your organization, customers, vendors, and business partners to financial losses.

A Virtual Private Network provides the infrastructure to support the secure transmission of data across the Internet. A virtual private network is called virtual because the connections have no real physical presence but consist of packets routed over the Internet. The appeal of a VPN is its global presence and the use of the Internet. Communications links can be done quickly, inexpensively, and safely across the world.

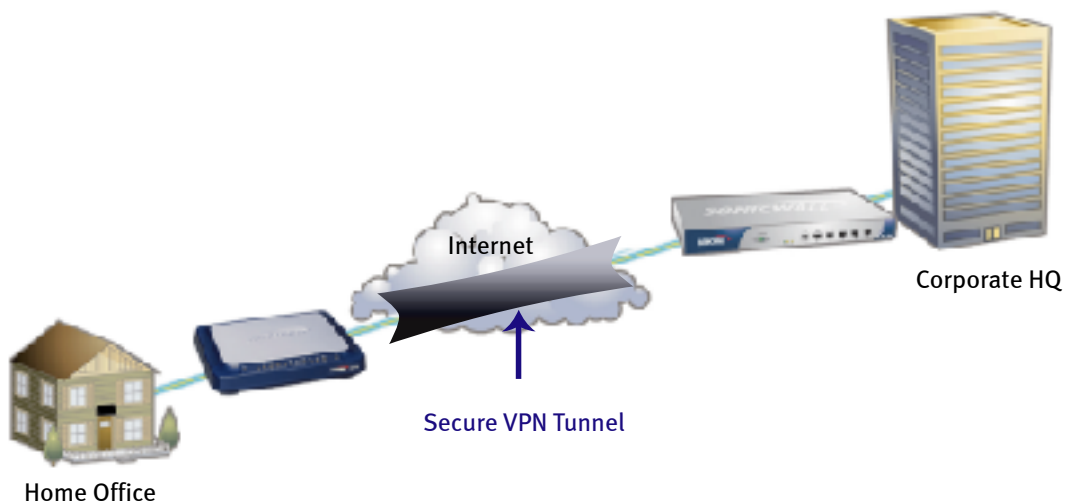


*VPN creates a private means for communication between geographically distributed locations.*

#### How a VPN Works

VPN is an umbrella term that refers to all the technologies enabling secure communications over the public Internet. VPN-related technologies include tunneling, authentication, and encryption.

VPN uses "tunnels" between two gateways to protect private data as it travels over the Internet. Tunneling is the process of encapsulating and encrypting data packets to make them unreadable as they pass over the Internet. A VPN tunnel through the Internet protects all data traffic passing through, regardless of the application.

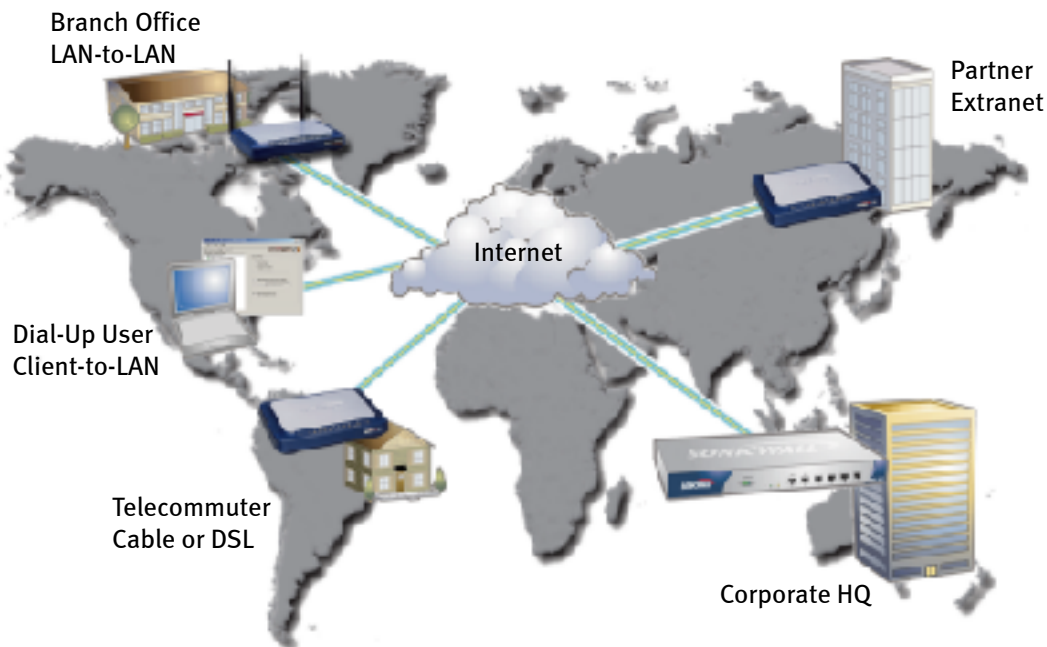


*A VPN tunnel establishes a secure connection between two sites over the Internet.*

Authentication schemes are essential to VPNs, since authentication assures the communicating parties that they are exchanging data with the correct users or host. VPNs use cryptographic technologies to ensure secure passage of data over the Internet. Cryptographic algorithms are mathematical functions used to perform the encryption and decryption, which is the process of scrambling information so it's unintelligible to anyone but the intended recipient.

VPNs can be used to support a variety of different types of connections, including:

- ▶ **Client-to-LAN.** A VPN can connect mobile users using dial-up Internet connections. A single VPN tunnel is used for each VPN client.
- ▶ **LAN-to-LAN.** VPNs link two LANs together using a single tunnel that handles all the secure data traffic between two locations. Most broadband connections use this method.
- ▶ **Intranets.** VPNs allow remote offices and users to securely access internal TCP/IP applications running on the corporate Intranet.
- ▶ **Extranets.** VPNs enable secure access to the corporate Extranet for vendors, partners, and customers.



From the VPN user's perspective, a VPN operates transparently melding the computer desktop at home with the resources of the office network. VPN users use their network applications and data as if they're sitting in front of their computer in the office. A VPN extends the Microsoft Windows network to give remote sites the same look and feel as working at the office. E-mail, databases, Intranets, or any application can pass through a VPN tunnel.

### VPN Gateways

A VPN gateway can be embodied in software on a server, an enhancement to a router or firewall, or a security appliance. A VPN gateway handles the high-speed encryption/decryption, negotiates the VPN policies, and provides tunneling services, ensuring the VPN connection occurs.

The data processing requirements for running a VPN are high because of the heavy demands of encrypting and decrypting data as it passes through the VPN gateway. Because of these demands, choosing a VPN gateway that can handle the load is a critical factor in deciding on a VPN solution.

The better VPN solutions use a dedicated security device or appliance that offloads the VPN and Internet security processing off a computer or router and puts it on a platform with a high-performance processor designed for high-demand data processing. An Internet security appliance is a standalone hardware platform that sits between the public and private networks to prevent unauthorized intrusions into the private network and acts as the VPN gateway.

### IPSec-Based VPNs

An international group organized under the Internet Engineering Task Force (IETF) developed the Internet Protocol Security (IPSec) protocol suite to provide security services at the network level. IPSec technology is based on modern cryptographic technologies, making possible very strong data authentication and privacy guarantees. It supports a variety of cryptographic technologies and authentication schemes.

Because the IPSec protocol suite is an open Internet standard, it enables interoperability between VPN products and delivers economies of scale for VPN vendors. For customers, the benefits of standards-based VPN mean more product choices, faster product innovations, and lower prices.

### VPN User Authentication

Establishing the identity of a VPN user prior to granting access to valuable, confidential resources protects the integrity of a VPN and ensures network security. An essential element of the cryptography used to scramble the data in a VPN connection is the use of secret codes, called keys, which are shared only by the communicating parties. Acting like a drivers license or a passport, a certificate provides a generally recognized proof of a person's identity.

Public-key cryptography based on Public-Key Infrastructure (PKI) uses certificates to address the problem of impersonation. Digital certificates and public key infrastructure (PKI) are widely accepted in the industry as the best solution for establishing user identities over the Internet with absolute confidence. Beyond protecting your network from unauthorized VPN access, authentication using PKI and digital certificates allows you to enhance the management of your VPN, such as revoking VPN access to remote users.

## EVALUATING YOUR VPN OPTIONS

Putting together VPN for your organization requires evaluating a number of important, interrelated technical and business issues. Here are guidelines to help you make an education decision on the best VPN solution for your organization.

### VPN in the Security Context

VPN is not a complete remote access solution without symbiotic Internet access security. Using a VPN without security measures to protect local computers and networks opens up a back door for hacker attacks on your organization's network. Hackers can access information off the home computer or use that computer to find their way back into the corporate network. A VPN connection can also allow e-mail messages with dangerous payloads into the corporate network.

Any security solution for remote sites using the Internet as their primary connection to your network needs to address these key security threats to provide a safe platform for your VPN:

1. **Unauthorized Network Access.** Unauthorized access to the remote site's LAN not only jeopardizes the local network but also opens up potential access to the enterprise network. Hackers breaking into a remote site can gain access to the organization's network through the back door.

2. **Denial of Service (DoS) Attacks.** Increasingly prevalent DoS attacks can disable remote networks so users no longer have access to network resources. Even if a remote network is not being attacked, it can be used as an unwitting ally in a distributed DoS attack on the enterprise network. While successful DoS attacks on remote offices may not have as severe an impact as an attack on the headquarters, it still causes lost productivity and revenue to the organization.
3. **Viruses.** Virus attacks are one of the greatest security threats today, and statistics show that outbreaks will continue to increase. Remote users can quickly damage the entire network by unknowingly downloading and launching dangerous computer viruses. Viruses are also used as delivery mechanisms for hacking tools, putting the security of the entire organization in doubt, even if a firewall is installed.
4. **Internet Access Control.** Inappropriate Internet content can create an uncomfortable work environment and cause potential legal problems. Network users at remote sites risk viewing inappropriate content, decreasing productivity, and inviting lawsuits by abusing company resources with unregulated Web browsing.
5. **Users.** Security's weakest link at many remote sites is the computer user. Security is both a technical and behavioral problem and users at remote sites without on-site IT can easily open security holes. For example, a desktop anti-virus installed on a telecommuter's computer that is turned off or not kept current with the latest virus cures is a security hole. Not keeping the firewall updated also creates vulnerabilities from new hacker threats.

An effective VPN solution is built on an integrated security platform that delivers a comprehensive security solution without the integration and management problems that result from sourcing, installing and maintaining security products from different vendors. A comprehensive security solution should support the following security countermeasures:

- ▶ **Firewall.** A firewall is the foundation of any remote site security solution. It protects against unauthorized access to the local network and closes the back door to the corporate network. A firewall should also protect the distributed network from DoS attacks.
- ▶ **Virus Protection.** Anti-virus scanners are the front line of preventing virus attacks. Policy-enforced virus protection offers the best defense by combining desktop anti-virus with network management at the Internet gateway to ensure anti-virus software is always running at the remote site. Single-user desktop anti-virus software installed and maintained on each computer lacks centralized management to ensure uniform and consistent anti-virus protection across the network.
- ▶ **Content Filtering.** Content filtering allows organizations to set and enforce Acceptable Use Policies (AUPs) governing what materials can and cannot be accessed on the organization's computers. URL, domain and IP blocking, based upon a continually updated filter database, is the preferred method of content filtering because it blocks objectionable content while preserving access to valuable Internet resources.
- ▶ **Global Management.** Remote offices and users must operate within the context of the organization's network security requirements. Any security solution deployed in a distributed environment needs to include support for global management of security policies and services. Centralized configuration, monitoring and distribution of security and VPN policies ensures a uniform security environment throughout the organization.

## Reliability

High reliability is essential to maintaining always-on security and remote access. Server-based or desktop software security products are dependent on the reliability of the computer operating system, multiple moving computer parts, and user errors. Configuring computer-based security and VPN gateways requires hardening the operating system with the latest security patches to fix new security flaws. Computers are also subject to hardware failures and can be overwhelmed with the heavy processing demands of security and VPN applications. For desktop security software, such as personal firewalls and anti-virus software, the biggest security risk is the user who can easily turn off these services.

A hardware-based security appliance with its own robust, built-in processor, embedded operating system, and solid-state design offloads security processing. It delivers more reliability because it operates independently from a computer or LAN. Security appliances are purpose-built security hardware devices that can handle the security and VPN needs of the entire network. These devices use an integrated architecture that allows the combination of all security features (firewall, VPN, anti-virus, etc.) in one solution without sacrificing performance.

### Do It Yourself or Outsource?

Your organization can choose from two VPN implementation options: do it yourself or a managed VPN service. Do-it-yourself VPN means your organization sets up the VPN gateways at every site you want to access your network. A VPN gateway is installed at the office, and VPN gateways are installed at remote sites with broadband access. Mobile VPN clients connect via dial-up Internet access accounts. The VPN connections require no special processing from the Internet service providers. Your organization is responsible for setting up and managing the VPN gateways. Do-it-yourself VPN offers the most flexible and cost-effective approach for most small to medium organizations, but it requires security products that are easy to install and manage.

With a managed VPN service approach, your organization enters into an agreement with a service provider, such as an ISP, to provide the VPN gateways and service. The user connects through the ISP's network with a VPN client and the tunnel session is initiated at the POP (Point of Presence). Deployment is limited by the existence of VPN-enabled POPs and VPN encryption doesn't occur until the POP, thus leaving the communication unprotected between the remote user and the POP. Managed VPN service offloads the management of the VPN network to the service provider, but typically at a higher cost than the do-it-yourself approach.

### Ease of Use

Larger organizations have traditionally been able to justify the high cost of security professionals to implement and maintain their complex security and VPN requirements. This is rarely the case in small and medium organizations. They need security and VPN solutions that are powerful enough to protect the network and provide secure remote access, but easy enough to set up and run for organizations with limited IT resources. Look for products with a reputation for ease of use, and with an intuitive graphical interface that allows you to take the product out of the box and install it with minimal configuration.

### Total Cost of Ownership (TCO)

Your budget for any security and VPN solution must take into account not only the initial cost of the product but also the total cost of ownership over the life of the product. These costs include installation, service and support, IT resources for ongoing management, and the often hidden costs of software upgrades required to keep the product up to date. One of the biggest budgetary items associated with any security solution is the cost of IT resources. Savings in the amount of time needed for installation and maintenance can significantly reduce the TCO. Use the Total Cost of Ownership chart below as a starting point for comparing different security and VPN solutions.

Total Cost of Ownership			
<b>One Time Costs</b>			
Equipment Cost	<input type="checkbox"/>	<input type="checkbox"/>	\$ _____
Installation Cost	<input type="checkbox"/>	<input type="checkbox"/>	\$ _____
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>Total One Time</b> <input type="checkbox"/>
			\$ _____
<b>Annual Costs</b>			
Software Maintenance	<input type="checkbox"/>		\$ _____
Technical Support Fees	<input type="checkbox"/>		\$ _____
IT Labor Estimate	<input type="checkbox"/>	<input type="checkbox"/>	\$ _____
<b>Annual Estimate</b>	<input type="checkbox"/>		\$ _____
<b>Years of Product Life</b>			_____
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>Total Annual Costs</b> <input type="checkbox"/>
			\$ _____
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>Total Cost of Ownership</b> <input type="checkbox"/>
			\$ _____

Total Cost of Ownership Worksheet

## Scalability

To protect your security and VPN investment, future growth of the organization must be considered. For the security solution to be able to grow with the organization, it must be able to scale in terms of the number of users or size of the network it supports. Any security platform you choose should provide an upgrade path for supporting more users as well as integrating new security services, such as VPN, virus protection, and content filtering. Choosing a security platform that is unable to scale means expensive upgrades or deploying multiple devices.

## Up-to-Date Protection

Just as the Internet is a dynamic, changing environment, security threats are also constantly changing. Any security product should easily adapt to the changing threats by providing the ability to update the software that provides protection against the latest attacks. The cost, if any, of these software updates over the life of the product should be factored into the total cost of the solution. In addition, these updates should be automatic so that the security product can keep pace with the latest threats.

## Global Management

Any distributed security and VPN solution needs to include support for global management of security policies and services. Organizations can't afford to use a time-consuming, expensive device-by-device approach for configuring security policies and services for remote offices and users. The device-by-device approach also leads to a higher incidence of improperly configured security devices and inconsistent policy enforcement. Centralized configuration, monitoring and distribution of security policies and services allows your organization to maintain uniform security policies throughout all the remote sites.



*Global management support enables organizations to cost-effectively manage a distributed security and VPN network from one central location.*

# SONICWALL'S INTEGRATED SECURITY AND VPN SOLUTION

SonicWALL delivers complete integrated security and VPN solutions tailored to the needs of small and medium-sized organizations. SonicWALL's renowned ease of use enables small and medium-sized organizations to deploy an enterprise-class security and VPN solution within the constraints of limited IT resources.

## SonicWALL Internet Security Appliances

SonicWALL Internet security appliances are high performance, hardware-based security platforms that provide support for an expanding array of security services. All SonicWALL appliances include these features:

- ▶ **Stateful Packet Inspection Firewall.** All SonicWALL Internet security appliances use Stateful Packet Inspection, the sophisticated firewall technology found in enterprise firewalls. Based on advanced packet-handling technology, this firewall technology protects your network from Denial of Service attacks, IP spoofing, and other TCP/IP borne attacks. It's transparent to users on the LAN and requires no client configuration. SonicWALL appliances are ICSA (International Computer Security Association) certified, demonstrating their effectiveness at protecting networks of any size.
- ▶ **IP Address Management.** SonicWALL Internet security appliances include built-in NAT (Network Address Translation) and DHCP (Dynamic Host Configuration Protocol) features that enable remote offices to be integrated into the organization's network and allow offices with multiple PCs to share broadband connections.
- ▶ **Ease of Management and Administration.** SonicWALL Internet security appliances are designed for easy setup and administration using a streamlined Web-based interface. They can also be managed remotely from a central location using SonicWALL's global management console.
- ▶ **Free AutoUpdates.** Internet protocols and security technologies frequently change. SonicWALL Internet security appliances can be updated with new firmware updates to protect against the latest threats or add new security features. These updates can be implemented automatically with a click of the mouse.
- ▶ **High Performance, Scalable Hardware Architecture.** SonicWALL's robust architecture supports throughput rates of over 100 Mbps, allowing maximum performance of your network. In addition, our appliances utilize a solid-state design with no moving parts, which increases reliability and reduces downtime.
- ▶ **Additional Upgrade Services.** SonicWALL products enable customers to add features and functionality when required without upgrading the hardware platform. These features, including anti-virus, content filtering and more, are fully integrated with the firewall security software thus ensuring ease of use and reliability.

## Internet Security Appliances for Every Site

The SonicWALL line of Internet security appliances scales to meet the diverse needs of different locations, from the single telecommuter, to the branch or remote office, up to the large office.

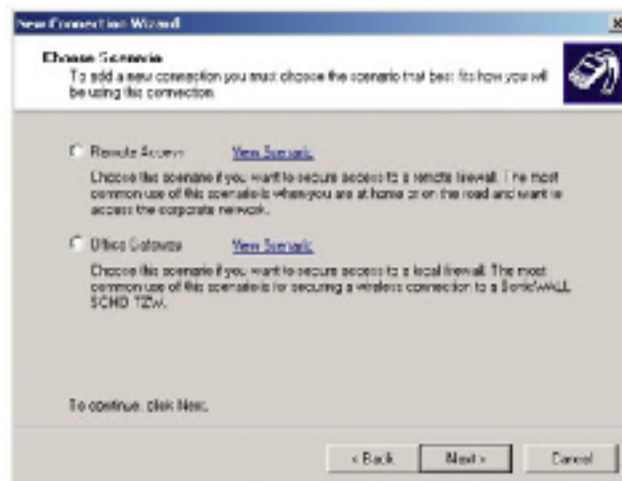


*The award-winning family of SonicWALL Internet Security Appliances delivers a complete security and VPN solution.*

- ▶ **SonicWALL TELE3 SP.** Ideal for retail and Point-of-Sale (POS) businesses that require continuous access to customer transactions and inventory data, the TELE3 SP features an integrated analog modem for automated fail-over and fail-back technology supporting both broadband and dial-up connectivity.
- ▶ **SonicWALL SOHO TZW.** Ideal for small to medium-sized networks, the SOHO TZW integrates secure wireless, firewall, and VPN technologies in one easy-to-use solution, bridging IT administrator security concerns with user demands for wireless connectivity. Includes SonicWALL's Global VPN Client software and unrestricted wireless LAN (WLAN) VPN connections.
- ▶ **SonicWALL TZ 170.** Ideal for home, small, remote, and branch offices, the TZ 170 is a total security platform. Featuring an integrated 5-port auto-sensing MDIX switch, the TZ 170 also offers an Optional Port that can be configured as a WorkPort for secure telecommuting, a second WAN for ISP Fail-Over and Load Balancing, or a second LAN for added internal security. The TZ 170 is available in multiple node configurations and includes SonicWALL Global VPN Client connections.
- ▶ **SonicWALL PRO 230.** Ideal for complex distributed networks of all sizes, the PRO 230 provides robust, integrated business security and complete, powerful, and reliable VPN concentration. The PRO 230 also supports an unlimited number of nodes and includes SonicWALL Global VPN Client connections.
- ▶ **SonicWALL PRO 3060.** Ideal for complex networks, the PRO 3060 is a total security platform delivering cost-effective, enterprise-class firewall and VPN concentration. The PRO 3060 supports an unlimited number of nodes and includes SonicWALL Global VPN Client connections for remote access.
- ▶ **SonicWALL PRO 4060.** Ideal for even the most complex networks, the PRO 4060 is a total security platform utilizing six configurable Ethernet interfaces to provide powerful, enterprise-class firewall and VPN concentration. The PRO 4060 supports an unlimited number of nodes and includes SonicWALL Global VPN Client connections for remote access.

## SonicWALL VPN

SonicWALL VPN enables simple and cost-effective remote access for telecommuters, branch offices, partners, and others you want to have access to your network resources. SonicWALL's IPSec-based VPN seamlessly operates with SonicWALL Internet security appliances to create an integrated security and remote access solution. Because SonicWALL VPN is based on the IPSec standard, it's compatible with other VPN gateways. SonicWALL VPN is easy to set up using the streamlined Web-based interface incorporated in every SonicWALL Internet security appliance.

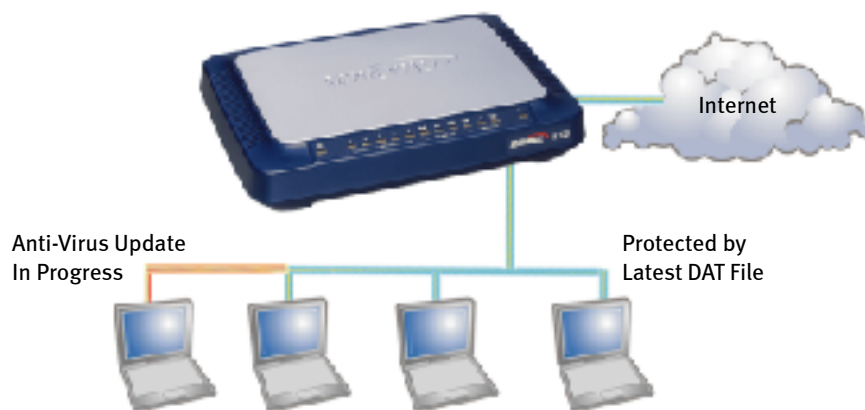


SonicWALL's Global VPN Client software allows mobile users to create a secure VPN tunnel to either a remote or local SonicWALL firewall over the Internet using broadband and dial-up modem connections. SonicWALL's GroupVPN feature eases deployment of Global VPN Clients by automatically generating a VPN Client configuration file for multiple clients.

Microsoft Windows network support is integrated into the SonicWALL VPN gateway and does not require any extra servers or applications. Simply click a checkbox during configuration and your remote PC integrates into the office Windows network. Viewing local and remote resources is transparent via the Windows Networking Neighborhood.

### SonicWALL Complete Anti-Virus

SonicWALL Complete Anti-Virus delivers enforced anti-virus protection for an entire network. SonicWALL has partnered with McAfee, the market leader in business anti-virus solutions, to provide a robust, centrally managed anti-virus solution. Enforced virus protection ensures network-wide virus protection by verifying that every PC accessing the Internet has the most up-to-date version of anti-virus software installed and active. SonicWALL Complete Anti-Virus transparently deploys an agent to each of the computers on the network, with no desktop-by-desktop installation, configuration, or maintenance required. This innovative approach prevents users from disabling virus protection or not running the most up-to-date virus protection. SonicWALL Complete Anti-Virus updates are automatically updated via the Internet.



*Enforced virus protection is a hybrid anti-virus solution that adds centralized enforcement and management to the complete protection of desktop anti-virus software along with automatic virus updates.*

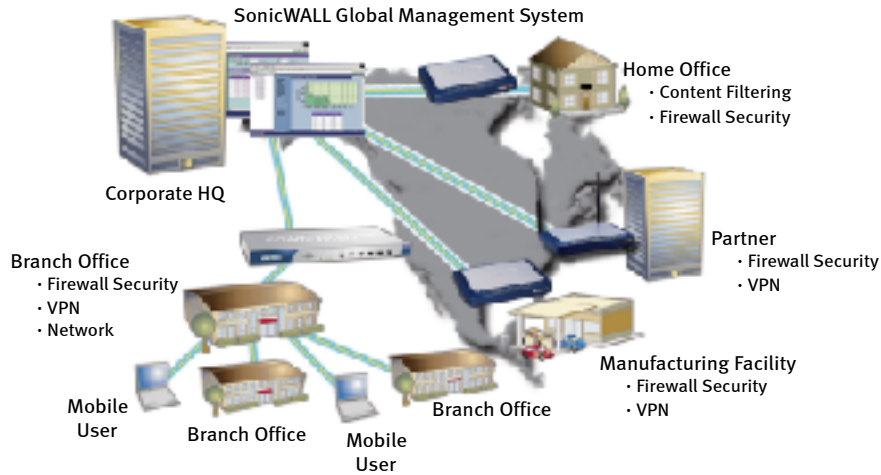
### SonicWALL Content Filtering Service (CFS)

SonicWALL Content Filtering Service enhances protection and productivity for your business or school by employing an innovative rating architecture utilizing a dynamic database of URLs, IP addresses and domains to block multiple categories of objectionable Web content. An easy-to-use management interface provides network administrators with greater control to transparently enforce acceptable use policies. At the core of SonicWALL CFS is a powerful website caching engine that stores URL ratings locally on the SonicWALL appliance, reducing response time to frequently-visited sites to a fraction of a second. SonicWALL Content Filtering Service combines appliance-based policy enforcement with comprehensive content filtering in a cost-effective, manageable solution.

### SonicWALL Global Management System

SonicWALL's Global Management System (GMS) enables your organization to define, deploy, and enforce security policies

across the distributed network from a central location. Via a secure VPN tunnel, a single administrator can manage remote SonicWALL Internet security appliances to ensure uniform security and VPN policies are pushed to all remote sites. This centralized management of your security and VPN system eliminates the user from the security management matrix to ensure uniform policies across all your remote sites. SonicWALL GMS reduces IT requirements, accelerates deployment, and lowers the cost of delivering services by centralizing the management and monitoring of SonicWALL Internet Security Appliances, VPN, and security services.



*SonicWALL GMS enables your organization to manage all the SonicWALL Internet security appliances from a central location to ensure uniform security and VPN policies across all remote sites.*

## ASSEMBLING YOUR SONICWALL SECURITY/VPN SYSTEM

Assembling a comprehensive SonicWALL security and remote access solution for your organization is easy. To determine your SonicWALL Internet security appliance requirements for your organization, you need to determine the number of network users at each site that you want to protect against Internet security attacks and the maximum number of simultaneous VPN connections you plan to support at each site.

### Determining Your Access Security Needs

SonicWALL Internet security appliances provide Internet access security from a single telecommuter up to a network supporting an unlimited number of users. The table below lists each SonicWALL Internet security appliance model and the number of network users it supports. Use this table to calculate the SonicWALL Internet security appliance required to protect every user on the network at each remote site and your headquarters.

SonicWALL MODEL	NODES SUPPORTED FOR ACCESS SECURITY
SonicWALL TELE3 SP	10 nodes Can be upgraded to support up to an unlimited number of nodes.
SonicWALL SOHO TZW	10 or 25 wired LAN node models Both models can be upgraded to support up to an unlimited number of wired LAN users. The number of wireless LAN users is unrestricted.
SonicWALL TZ 170	10, 25 or Unrestricted node models The 10 and 25 node configurations can be upgraded to support higher node counts.
SonicWALL PRO 230	Unlimited
SonicWALL PRO 3060	Unlimited
SonicWALL PRO 4060	Unlimited

## Determining Your VPN Needs

Determining the right SonicWALL Internet security appliance for your VPN needs is based on the number of site-to-site VPN policies each model supports. A VPN policy refers to all the necessary settings needed to create a single VPN tunnel. The number of VPN Policies does not correlate specifically to the number of VPN users. A single VPN policy can support a LAN-to-LAN VPN connection between two SonicWALLs with multiple users on each LAN. On the other hand, a single dial-up Global VPN Client can count as a single VPN Policy or, using SonicWALL's Group VPN Client feature, you can support multiple dial-up VPN clients using a single VPN policy.

To help you choose the right SonicWALL Internet security appliance to meet your security VPN needs, the table below lists the SonicWALL Internet security appliance models, whether VPN is included standard or available as an optional upgrade, and the maximum number of VPN policies supported.

SonicWALL MODEL	SonicWALL VPN	MAXIMUM SITE-TO-SITE VPN POLICIES
SonicWALL TELE3 SP	Included	10
SonicWALL SOHO TZW	Included	10
SonicWALL TZ 170	Included	1 with 10 node model, 10 with 25 and Unrestricted node models
SonicWALL PRO 230	Included	500
SonicWALL PRO 3060	Included	1,000
SonicWALL PRO 4060	Included	3,000

## A Security/VPN System for a Single Office with Remote Users

To get practical about what you need to assemble a security and VPN system, let's look at a hypothetical small office scenario. The office has 10 computers networked together with a high-speed, always-on DSL connection. Three people at the firm have broadband connections (DSL or cable) at home and four people have dial-up Internet access at home or use it on the road.

- ▶ **Office.** The SonicWALL TZ 170 10 node Internet security appliance is ideal for the office. It provides firewall protection for the entire office as well as support for one policy for site-to-site VPN connection. An optional SonicWALL Global VPN Client upgrade will provide network access for the remote and mobile users.
- ▶ **Remote Broadband Users.** For the three broadband connected users, the SonicWALL TZ 170 10 node Internet security appliance delivers firewall security plus VPN support for up to 10 users. Configuring the Optional Port as a WorkPort creates a "trusted zone" of network security between the corporate office and the telecommuter, protecting the corporate network against malicious intrusions that occur when work computers share broadband Internet access with networked family computers.
- ▶ **Remote Dial-Up Users.** For the four dial-up users there are two options: the SonicWALL TELE3 SP, which provides the option to connect via broadband or dial-up via an integrated analog modem OR the SonicWALL Global VPN Client. These VPN clients users can all share a single policy using SonicWALL's Group VPN Client feature.

## A Security and VPN System for Multiple Offices with Remote Users

For an organization with a main office, two small remote offices, and multiple remote broadband and dial-up users, you need to assemble the following SonicWALL security and VPN solution:

- ▶ **Main Office.** The main office includes 100 people working on the network and requires VPN support for two remote offices and 50 remote users (30 broadband, 20 dial-up). The company expects the number of broadband VPN users to grow to 50 in the near future. The SonicWALL PRO 3060 provides access security support for an unlimited number of users and up to 1,000 site-to-site VPN policies with SonicOS Enhanced. The two remote offices will each use a single site-to-site VPN policy for LAN-to-LAN connectivity and each of the 30 broadband users will use one policy for a SonicWALL to SonicWALL VPN connection for a total of 32 VPN policies. As the organization grows, there is built-in scalability to support more VPN users.
- ▶ **Remote Office 1.** This small office has 15 users in the office. It needs one VPN connection to the main office and the other remote office, as well as VPN support for five remote users (two broadband and three dial-up). The SonicWALL TZ 170 25 node model will support this office for Internet access security. An optional SonicWALL Global VPN Client upgrade will provide broadband and dial-up network access for the remote users.
- ▶ **Remote Office 2.** This mid-size office has 35 users in the office and expects to add more broadband remote users to the network. It needs one VPN connection to the main office and the other remote office, as well as VPN support for 20 remote users (10 broadband and 10 dial-up). The SonicWALL TZ 170 Unrestricted node model supports an unlimited number of users for Internet access security and up to 10 site-to-site VPN policies. An optional SonicWALL Global VPN Client upgrade will provide broadband and dial-up network access for the remote users.
- ▶ **Remote Broadband Users.** For the 42 broadband users, the SonicWALL TZ 170 10 Node Internet security appliance delivers access security plus VPN support for up to 10 users at each location. An optional SonicWALL Global VPN Client upgrade will also provide broadband network access for the remote users.
- ▶ **Remote Dial-Up Users.** Each of the 33 dial-up users wanting secure access to the office network will need either SonicWALL TELE3 SP for hardware-accelerated VPN connectivity or the Global VPN Client.

## CONCLUSION

The dynamics of broadband technology coupled with VPN create a robust and secure remote access system that enables small and medium-sized organizations to harness the compelling benefits of the distributed workplace. There are many factors to consider when purchasing an Internet access security and remote access system for your organization. This paper has presented the key issues that need to be addressed when choosing the best solution. The good news is that SonicWALL's affordable, integrated, and easy-to-use Internet access security and VPN solutions make your decision-making easier.