

Virtual Private Networks for Small to Medium Organizations

A White Paper

by SonicWALL, Inc.



Introduction

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. This new 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 IT and financial resources. Why? Because until now, most small and medium organizations that wanted to link remote offices and users muddled through limited bandwidth options, high prices, and complex 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 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 size 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.

The Distributed Workplace

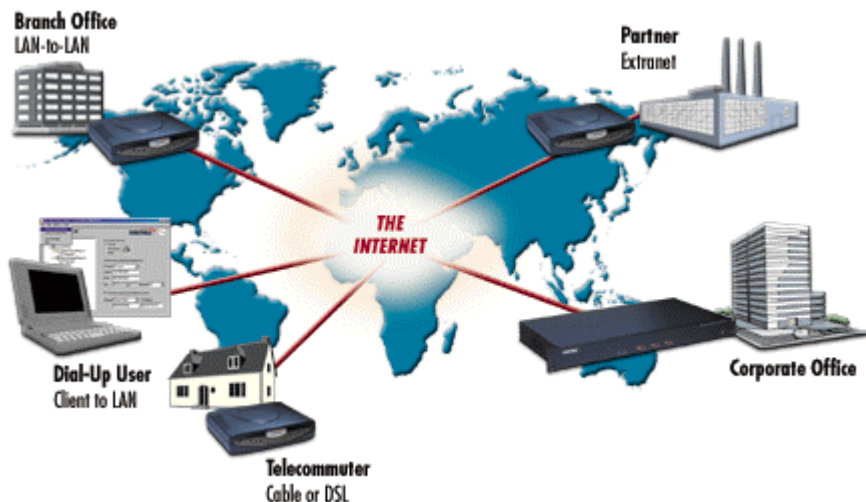
Demand for remote access to an organization's network resources is being driven by an undeniable combination of business trends. Employees are demanding flexible work arrangements. Companies are being driven to improve productivity and reduce costs. Business partners want real-time access to critical information. A Gartner Group study predicts more than 137 million workers worldwide will be involved in some sort of remote work by 2003.

Also accelerating the distributed organization is the rapid adoption of affordable, widely available broadband Internet access. Internet users with broadband access will triple from 7% to 21% to 25 million users by

2003 and VPN expenditures will increase 529% by 2004 (Infonetics Research).

Working Smarter with VPNs

VPNs enable organizations of any size to leverage the Internet's cost-savings and flexibility, while protecting sensitive information. A VPN provides the infrastructure to support the secure transmission of data across the Internet. A VPN is called virtual because the connections have no real physical presence, but consists 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, cheaply, and safely across the world.



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

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 enabling centralization of 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.

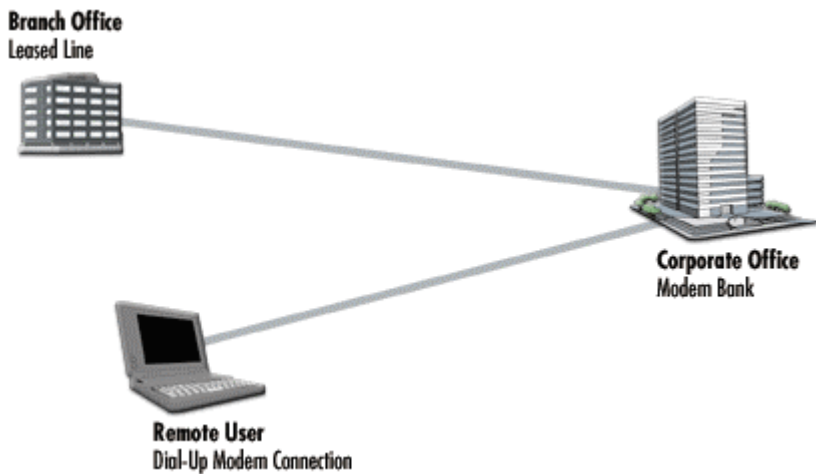
Broadband Powered VPN

With broadband Internet connections, VPN comes to life as a serious remote access solution for small to medium 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, no more dialing up to send or receive messages. Intranets and databases are quickly and seamlessly accessible, 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 their 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.

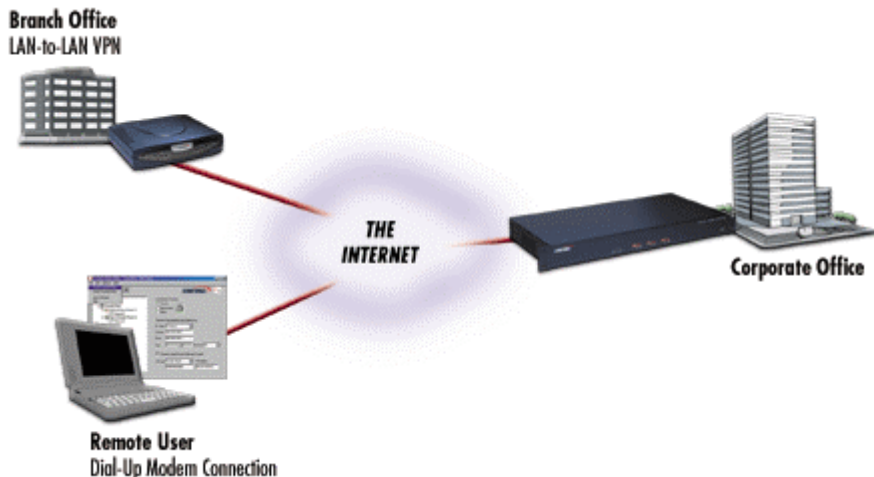
Secure Remote Access via VPN

Traditional remote access required companies to lease expensive, dedicated data lines or maintain modem banks, 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, direct links were made between remote sites and the corporate network 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.



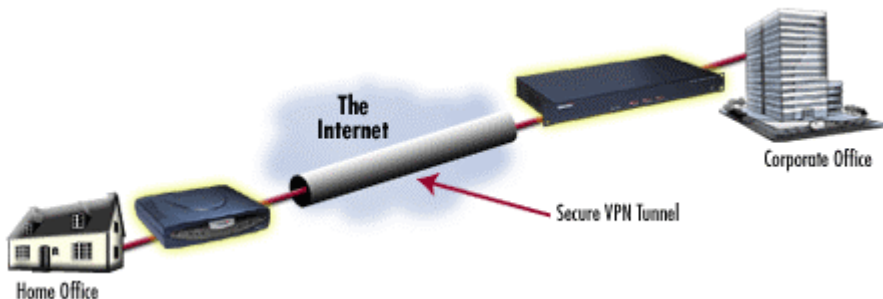
With the advent of ubiquitous Internet access and VPN technology, remote access is handled through the same connection used for Internet service.

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.

How 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 their 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 SAs (Security Associations), provides tunneling services, and generally makes sure things get done to make a VPN connection.

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 an important factor in deciding on a VPN solution.

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.

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 driver’s 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

Any security solution for remote sites using the Internet as their primary connection to the organization's network needs to address a variety of security threats. Remote offices and telecommuters often connected directly to the Internet via their own Internet Service Provider (ISP) link. This Internet connection is used for multiple purposes that make the remote computer or network vulnerable to a host of security threats.

In determining the best security and VPN solution for remote offices and workers, there are important considerations. The following guidelines will help you evaluate the right security and VPN solution for remote offices and workers.

Firewall Protection

VPN is not a complete remote access solution without symbiotic Internet access security. Using a VPN without a firewall to protect local computers and networks opens up a back door for hacker attacks on your organization’s network. Hackers can access information off a remote site computer to find their way back into the corporate network via the VPN.

A firewall protects your network against Internet based theft, destruction, or modification of data by examining all data traffic passing from the Internet or Wide Area Network (WAN) to the local area network (LAN). The International Computer Security Association (ICSA) classifies firewalls into three categories:

- **Packets filter firewalls.** Typically implemented on DSL routers, they examine data passing to and from a network using rules to block access according to information located in each packet's addressing information. While many router vendors promote their router's packet filtering capabilities as a firewall, in reality packet filter firewalls are vulnerable to a number of hacker attacks, not to mention difficult to set up and maintain.

- **Proxy servers or session-level firewalls.** These firewalls go beyond basic packet filtering by also examining the data within IP packets to verify their authenticity. A proxy server accepts or rejects data traffic based on the entire set of IP packets associated with an entire application session to the same IP address. This upper level examination, however, causes significant performance degradation on your Internet connection. Also, proxy servers are more difficult to set up and maintain. Each client on your network must also have client software installed and one computer on your network with two network adapters must act as the proxy server. Proxy servers come in the form of either stand-alone boxes or as software products.
- **Stateful Packet Inspection.** Because of their shortcomings, both packet filters and proxy servers have fallen from favor with many network security experts, being replaced by stateful packet inspection as the most trusted firewall technology. Stateful packet inspection is a sophisticated firewall technology found in large enterprise firewalls. It's based on advanced packet-filtering technology that is transparent to users on the LAN, requires no client configuration, and secures the widest array of IP protocols. Instead of just checking addresses in incoming packets headers, the stateful packet inspection firewall intercepts packets until it has enough to make a determination as to the secure state of the attempted connection. Stateful packet inspection is also well suited to protect networks against the growing threat of Denial of Service attacks.

Ala Carte or Integrated Security Solutions

The distributed organization can deploy security measures for remote offices and workers via an ala Carte or integrated approach. The ala Carte method requires evaluating products from multiple vendors, installing and managing separate products for each security measure, and often costs considerably more than an integrated security solution. Additionally, integrating security products from different vendors can be difficult and lead to interoperability problems, which, in turn can lead to security vulnerabilities.

Hardware or Software Based Security

There are two main types of security and remote access options available today: software and hardware. Software based security and VPN gateways running a computer or server have inherent problems.

- A general-purpose computer is not the most reliable device for the processing demands of security. Security and VPN applications are data intensive, and placing these processing demands on a computer or processor can slow down the network.

- A general-purpose computer's operating system isn't designed with bulletproof security in mind. Configuring computer-based security and VPN gateways require that you harden the operating system. This means ensuring the operating system always has the latest security patches to fix new security flaws.
- The complexity of current software configurations has been problematic, particularly ease of use and management.

The hardware based security and VPN solutions, typically embodied in security appliances, protect the entire network and offload all the security and VPN processing off computers. Because security appliances protect the network at the Internet gateway, they provide a platform for seamless local or remote management of all security and remote access services. A security appliance is a solid-state platform with a powerful onboard processor to handle the demands of security and VPN processing. This architecture allows the integration of multiple security features – firewall, VPN, anti-virus, and other services without sacrificing performance. Security appliances are also designed for easy management and security upgrades.

Build or Outsource?

Your organization can choose from two VPN implementation choices: in-house VPN or managed VPN service. Building a VPN requires your organization to deploy VPN gateways at every site you want to access your network. A high-end 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.

With a managed VPN service approach, your organization enters into an agreement with a service provider 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 to the service provider, but typically at a higher cost.

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 almost never 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.

Security Management

Any secure connectivity solution that relies on user intervention to install and manage is fraught with security holes. Security's weakest link at many remote sites is the computer user. Remote offices and users must operate within the context of the organization's network security requirements. A security solution deployed in a distributed network environment needs to include support for global management of security policies and services.

Centralized configuration, monitoring and distribution of security and VPN policies ensure a uniform security environment throughout the organization. Centralized security management also dramatically reduces security and VPN deployment and management costs. 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.



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

Scalability

To protect your security and VPN investment, consideration must be made for future growth of the organization. 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 where a single device would have been sufficient.

Total Cost of Ownership

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 total cost of ownership. Use the Total Cost of Ownership chart below as a starting point for comparing different security and VPN solutions.

Total Cost of Ownership	
One Time Costs	
Equipment Cost	\$ _____
Installation Cost	\$ _____
Total One Time	\$ _____
Annual Costs	
Software Maintenance	\$ _____
Technical Support Fees	\$ _____
IT Labor Estimate	\$ _____
Annual Estimate	\$ _____
Years of Product Life	_____
Total Annual Costs	\$ _____
Total Cost of Ownership	\$ _____

Total Cost of Ownership Worksheet

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.

SonicWALL's Integrated Security and VPN Solution

SonicWALL delivers integrated security and VPN solutions tailored to the needs of small and medium organizations. SonicWALL's family of plug-and-play Internet security appliances with an ICSA-certified, stateful packet inspection firewall and IPSec VPN deliver a cost-effective and integrated security and VPN solution. SonicWALL's renowned ease-of-use enables small and medium organizations to deploy an enterprise class security and VPN solution within the constraints of limited IT resources.

SonicWALL delivers more than just the parts—we offer a complete enterprise-class VPN and security solution. Small and medium size organization can assemble a comprehensive security and remote access infrastructure with the following SonicWALL components.

- **SonicWALL Internet security appliances.** These solid-state, integrated, network security platforms include a state-of-the-art, ICSA-certified firewall, IP address management, and support for an expanding array of SonicWALL security applications, such as network anti-virus and content filtering. SonicWALL Internet security appliances eliminate the complexity of separately managing computer hardware, operating systems, and security software.
- **SonicWALL IPSec VPN.** A robust, IPSec VPN solution that is seamlessly integrated into the family of SonicWALL Internet security appliances. SonicWALL VPN is interoperable with VPN gateways from any manufacturer's IPSec-compliant VPN gateway.
- **SonicWALL Authentication Service.** Provides strong authentication of VPN users and devices using Public Key Infrastructure (PKI) and digital certificates in an easy-to-deploy service that avoids the complexity of existing PKI solutions.
- **SonicWALL Global Management System.** Enables the distributed organizations to manage thousands of SonicWALL Internet security appliances and applications from a central location to dramatically lower security and VPN management costs and uniformly enforce policies.

Assembling a SonicWALL VPN

Putting together a SonicWALL VPN and Internet security solution is a simple, modular process using SonicWALL's Internet security appliances as the basic building blocks. Your organization deploys the appropriate SonicWALL Internet security appliance for each location, adds VPN

authentication with SonicWALL Authentication Service, and ties it all together with SonicWALL's GMS (Global Management System).

VPN Building Blocks: SonicWALL Internet Security Appliances

The family of SonicWALL Internet security appliances provides the first line of defense for networks with an ICSA-certified, stateful packet inspection firewall combined with IPSec VPN for remote access. SonicWALL Internet security appliances are built on SonicWALL's ASIC-based acceleration that delivers industry-leading firewall and VPN throughput. All SonicWALL Internet security appliances support the seamless integration of SonicWALL security applications, including network anti-virus and content filtering, and a streamlined Web management interface that makes setup and management a snap.



The SonicWALL Internet security appliance family.

To choose the right SonicWALL Internet security appliance, match the number of network users for Internet security and the number of VPN tunnels required at each site with the right SonicWALL Internet security appliance. Broadband connected telecommuters, day-extenders, and small offices with up to 5 computers can use TELE3s. For small to medium size remote offices the SOHO3, PRO 100, and PRO 200 can be deployed. At the larger central sites supporting 1,000 to 10,000 VPN tunnels, administrators can deploy the PRO 300, SonicWALL GX 250 or SonicWALL GX 650 with support for Gigabit Ethernet. Dial-up mobile workers use SonicWALL VPN Client software.

Internet Security Appliance	Maximum Internet Security Users	Maximum VPN Tunnels*
SonicWALL TELE3	5	5
SonicWALL SOHO3	10/50	10
SonicWALL PRO 100	Unlimited	50

SonicWALL PRO 200	Unlimited	500
SonicWALL PRO 300	Unlimited	1,000
SonicWALL GX 250	Unlimited	5,000
SonicWALL GX 650	Unlimited	10,000

**A single SonicWALL VPN tunnel can support a LAN-to-LAN connection between two SonicWALL Internet security appliances with multiple users on each LAN or multiple dial-up VPN clients using SonicWALL's Group VPN Client feature.*

Adding Authentication

SonicWALL Authentication Service provides strong authentication of VPN users and devices using PKI and digital certificates that seamlessly integrate into the SonicWALL VPN solution. Implemented in collaboration with VeriSign, the leading provider of trust services, SonicWALL Authentication Service offers an affordable, easy to administer, end-to-end solution for protecting highly confidential information from unauthorized access. SonicWALL Authentication Service also delivers powerful VPN management features, such as instantly revoking VPN access or turning on new telecommuters.

Tying It All Together with Global Management

SonicWALL Global Management System (GMS) ties together tens of thousands of SonicWALL Internet security appliances by enabling network administrators to uniformly define, deploy, and enforce security and VPN policies from a central location. SonicWALL GMS delivers a powerful, yet easy-to-use system for provisioning and managing SonicWALL Internet security appliances, which dramatically reduces IT staffing requirements, accelerates deployment, and lowers the cost of delivering security services throughout the organization.



SonicWALL Global Management System enables network administrators to manage a distributed security network of SonicWALL Internet security appliances—all from one central location.

Deployment Recipes

To get practical about what you need to assemble for a security and VPN system, let's look two deployment recipes for a small office with remote users and a larger multiple office organization with remote users.

A Security/VPN Solution for a Single Office with Remote Users

A small office has 8 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 SOHO3 10-User Internet security appliance with IPsec VPN is ideal for the office. It provides firewall protection for the entire office as well as support of up to 10 VPN tunnels for remote VPN connections.
- **Remote Broadband Users.** For the 3 broadband connected users, the SonicWALL TELE3 Internet security appliance delivers firewall security plus VPN support for up to 5 users.
- **Remote Dial-Up Users.** For the 4 dial-up users, you need four SonicWALL VPN Clients. These VPN clients can all share a single VPN tunnel 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 2 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 100 provides access security support for an unlimited number of users and up to 50 VPN tunnels. The 2 remote offices will each use a single VPN tunnel for a LAN-to-LAN connection and each of the 30 broadband users will use one VPN tunnel for a SonicWALL to SonicWALL VPN connection for a total of 32 VPN tunnels. As the organization grows, there is built-in scalability to support more VPN users.
- **Remote Office 1.** This small office has 9 users in the office. It needs one VPN connection to the main office and the other remote office, as well as VPN support for 5 remote users (2 broadband and 3 dial-up). The SonicWALL SOHO3 10 user model will support this office for Internet access security and the 5 tunnels required for remote user VPN support.
- **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 PRO 100 supports an unlimited number of users for Internet access security and up to 50 VPN tunnels. The number of VPN tunnels required for this office is 13.
- **Remote Broadband Users.** For the 42 broadband users, the SonicWALL TELE3 Internet security appliance delivers access security plus VPN support for up to 5 users at each location.
- **Remote Dial-Up Users.** Each of the 33 dial-up users wanting secure access to the office network will need the SonicWALL VPN Client.

Conclusion

The dynamics of broadband technology coupled with VPN creates a robust and secure remote access system that enables small and medium 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.

To learn more information on how SonicWALL can help you protect your business, call 1-888-557-6642 or visit us at www.sonicwall.com.



SonicWALL, Inc

E-mail: info@sonicwall.com

Web: www.sonicwall.com

©2001 SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.