

Protecting and Connecting the Distributed Organization A Comprehensive Security and VPN Strategy

A White Paper

by SonicWALL, Inc.



Introduction

Today's distributed organizations are increasingly made up of remote offices, telecommuters, mobile workers, and business partners. These geographically dispersed locations are dependent on access to the organization's network, but they also represent a new security challenge for organizations. The challenge is to provide this rapidly growing segment of network users, often without on-site IT support, with cost-effective, enterprise-class Internet security and VPN solutions.

As networks extend across the Internet connecting customers, partners, and remote employees, every network entry point must be protected. Without an enterprise-class security and remote access solution at every network entry point, the organization leaves an unguarded "back door" into the fortified headquarters network. Paradoxically, the high cost and complexity of enterprise security and VPN products and the challenges of implementing and managing them without on-site IT support leaves the distributed organization's network vulnerable.

This white paper explains the essential issues in evaluating a comprehensive Virtual Private Network (VPN) solution that meets the diverse needs of distributed organizations. It provides a framework for evaluating VPN solutions in the context of overall security for each remote site, and how to deploy a distributed security and VPN solution to protect every network entry point.

The Distributed Workplace

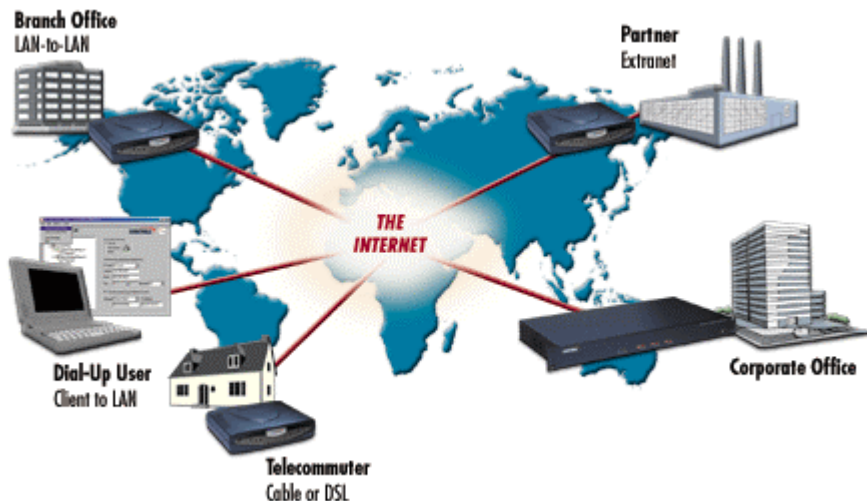
Demand for remote access to an organization's network resources is being driven by an undeniable combination of business trends. Employees are demanding flexible work arrangements. Companies are being driven to improve productivity and reduce costs. Business partners want real-time access to critical 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.

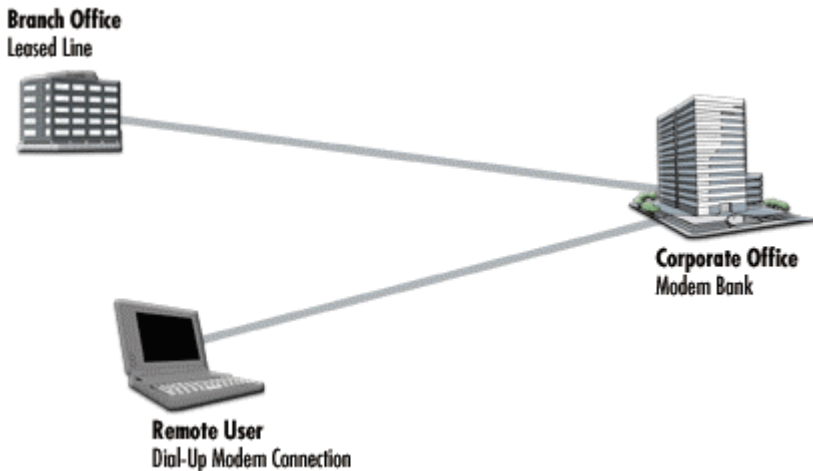
Implementing a VPN for remote access to your network creates new ways of getting things done, including:

- 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.

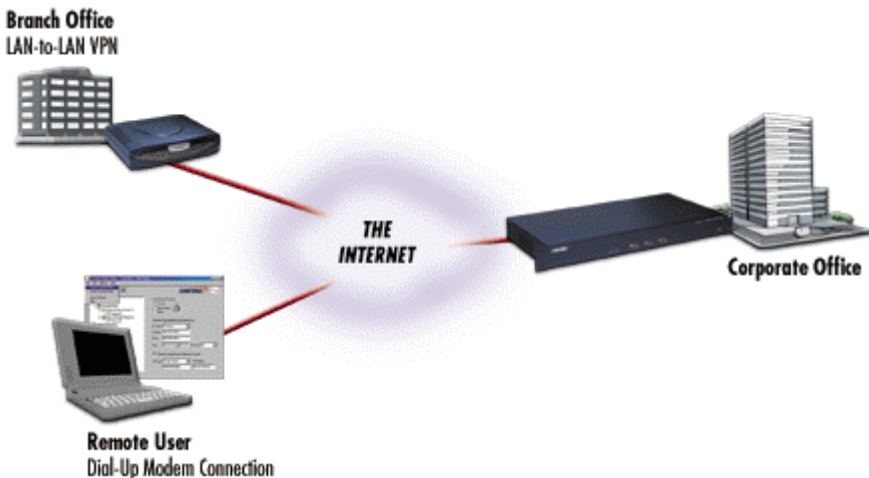
Secure Remote Access via VPN

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. With the advent of affordable broadband Internet connections and standards-based VPN, organizations can bypass these expensive and complex remote access solutions.



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

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

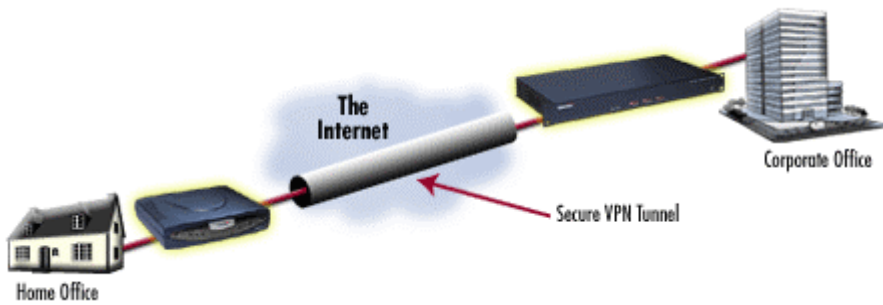
- **Client to LAN.** A VPN can connect mobile users using dial-up Internet connections.
- **LAN-to-LAN.** A VPN links two LANs together via the Internet to secure data traffic between two locations. Most broadband connections use this method.
- **Intranets.** A VPN allows remote offices and users to securely access internal TCP/IP applications running on the corporate Intranet.
- **Extranets.** A VPN enable secure access to the corporate Extranet for vendors, partners, and customers.

While Internet-based remote access delivers big cost savings, it also presents security challenges in protecting the confidentiality and integrity of essential information and network resources. 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 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.

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.



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

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.

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.

IPSec VPN

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 VPN customers, the benefits of standards-based

VPN also mean more product choices, faster innovations, and lower prices.

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.

The Distributed Security Challenge

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 ISPs 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.

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.

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

Meeting the Distributed Security Challenge

Protecting the distributed organization is at the heart of SonicWALL's Distributed Security Architecture (DSA). Based on this model, SonicWALL's family of plug-and-play Internet security appliances with IPSec VPN deliver a secure, affordable, comprehensive, flexible, and easy-to-deploy VPN solution.

SonicWALL delivers more than just the parts—we offer a complete enterprise-class VPN and security solution. SonicWALL's Distributed Security Architecture integrates the following core components into a seamless and scalable VPN solution that meets the needs of the single telecommuter up to the large central site supporting tens of thousands of VPN tunnels.

- **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 organization 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. The distributed 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 provide 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 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 SonicWALLs 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 distributed organization.



SonicWALL GMS (Global Management System) enables network administrators to manage a distributed security network made up of tens of thousands of SonicWALL Internet security appliances—all from one central location.

A VPN Solution Scenario

The following solution scenario shows the process for a fictitious organization deploying a SonicWALL security and VPN solution to support telecommuters. It's based on the aggregation of concerns and/or issues faced by existing and potential SonicWALL customers.

HDA Corporation faced several challenges in upgrading its existing software-based security and remote access telecommuter infrastructure to handle a rapidly growing telecommuter base. These challenges included enforcing and extending security policies, reducing support costs,

The first challenge HDA encountered was to enforce its security policies with the current 500 telecommuters. HDA was using a software firewall and VPN solution because at the time they first explored a firewall and VPN solution for its first few hundred remote workers, the company did

not find a hardware solution that would support DHCP and PPPOE. The majority of telecommuters connected via DSL were using DHCP and PPPOE.

The software VPN solution created numerous problems, including the significant issue of security policy enforcement. The VPN software upgrades and/or configuration updates were e-mailed as attachments to remote workers with the hope that the employees would install it themselves. Many employees simply didn't see the upgrade as a priority, therefore left the upgrade e-mail in their inbox, and soon forgot about them.

Employee compliance was a major concern for IT management because each telecommuter was a point of entry for the following vulnerabilities to the corporate network.

- Telecommuters using always-on DSL Internet connections for remote access to the corporate network also used the connections for personal use, exposing the employee's computer to the Internet security threats.
- HDA Corporation had no method to enforce and update anti-virus software on telecommuter computers. Without these updates, an employee could unknowingly expose the entire corporate network to viruses from their home computer simply by browsing the Internet and later checking company e-mail by activating their VPN client software.
- Unprotected telecommuter's computers from outdated firewalls could be compromised and used by hackers to gain unauthorized access to the corporate network or launch Distributed Denial of Service (DDoS) attacks.

On the flip side of non-compliance, those accommodating employees who tried to upload the upgrades flooded the help desk with questions, which led to havoc and as a consequence, a degradation of help desk service for other employees.

The second challenge for HDA was extending security policies to a growing base of telecommuters. With the current software solution, additional network security managers were required to make all VPN configurations changes for each user and make changes on the corporate VPN concentrator for each individual VPN client.

The Solution

After identifying the challenges they faced in implementing a large telecommuting program, HDA Corporation decided to implement SonicWALL's telecommuting solution that included the following components:

- SonicWALL TELE3 Internet Security Appliances for telecommuters
- SonicWALL Global Management System (GMS) for centralized security policy enforcement
- SonicWALL GX 250 Internet Security Appliances for the HDA corporate site

SonicWALL TELE3 for Telecommuters

HDA Corporation used the SonicWALL TELE3 for telecommuters. The SonicWALL TELE3 Internet Security Appliance includes an enterprise-class, ICSA-certified firewall and VPN solution that supports DHCP and PPOE for broadband DSL users, and provides central management support for updates and configurations.

Each SonicWALL TELE3 included SonicWALL's policy-enforced anti-virus solution to ensure every telecommuter was protected from viruses. Enforced anti-virus ensured all clients behind the TELE3 have the latest anti-virus software updates before being allowed access to the Internet. Anti-virus management is automatic with no user intervention.

The TELE3s combined with SonicWALL's Global Management System eliminated the back-door vulnerabilities to the corporate network, the problems of employee compliance for updates, and the corresponding side effects of overloading the company's help desk.

SonicWALL Global Management System for Centralized Management

HDA Corporation decided on SonicWALL GMS (Global Management System) for software version control, license management, security policy standardization, and general security device management. With SonicWALL GMS, HDA Corporation's security administrators can control all aspects of its remote employees' firewalls through encrypted security tunnels to each appliance in the field. SonicWALL GMS also provided the ability to roll out policy changes and firmware updates automatically at scheduled times.

SonicWALL GMS enabled administrators to dramatically reduce the resources required to manage the telecommuter solution, thereby reducing the overhead associated with telecommuting policy rollout.

With centralized management, HDA was able to save on additional overhead by eliminating the need to make one-by-one VPN configuration changes. The result was a direct overhead cost savings of an originally anticipated \$425,000 per year costs for Phase 1 of the telecommuter program, with additional savings as the telecommuter base grows into the thousands. This calculation is based on the cost of adding five additional

administrators at an average salary of \$85,000 per annum. On average, each administrator supports 100 users for this type of network support.

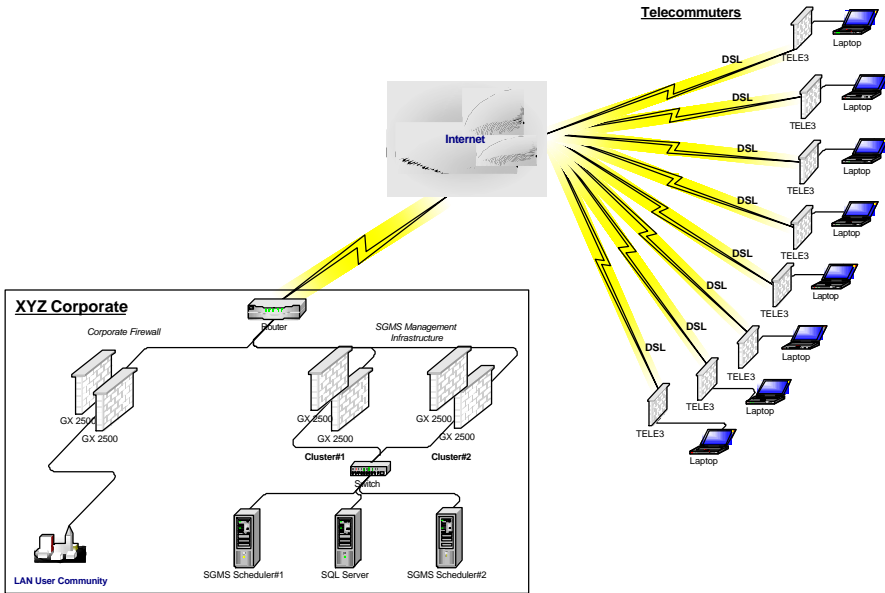
SonicWALL GX 250's for Corporate Site

To ensure that corporate resources are always accessible and eliminate network downtime to the telecommuting employees, a robust and redundant infrastructure was required. HDA Corporation chose the SonicWALL GX 250 Internet Security Appliance, a high-performance firewall and VPN solution that supports up to 5,000 VPN tunnels and include built-in high-availability.

Two pairs of high availability GX 250's were used as a part of the GMS management infrastructure and were selected due to HDA's aggressive growth plans. These two HA clusters serve as the company's VPN tunnel termination point for all of its telecommuters.

The installed base of telecommuters consisted of 500 employees around the country. Phase 1 of the telecommuting policy extension included an additional 500 remote workers by the end of the fiscal year with plans for thousands more over the next 2-3 years.

The tunnels between the SonicWALL GMS infrastructure and the TELE3's in the field were divided between the two GX 250 High Availability clusters. The first cluster manages 250 tunnels, and the second manages the other 250. Each GX 250 cluster handles 5,000 VPN tunnels. This insures complete redundancy in a fail-over situation. If both GX units in one cluster failed, the second cluster of GX's would assume management of all the tunnels. (See the network map for a visual description of this SonicWALL GMS architecture.) This new VPN infrastructure was placed in parallel to the company's existing corporate firewall solution.



Summary

SonicWALL is the only VPN and security solution designed from the ground up to support the diverse needs of the distributed organization's network from the telecommuter up to the large central site. SonicWALL's modular family of integrated VPN and security appliances allow the distributed organization to deploy cost-effective, scalable, enterprise-class security to remote offices, telecommuters, mobile workers, and business partners without the high cost and complexity of other VPN vendor solutions.

For more information, please visit SonicWALL 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.