

Internet Security Issues and Solutions for Small and Medium Business

A White Paper

by SonicWALL, Inc.



Overview

Your Internet service is more than just a data communications link—it's a vital connection to customers, employees, and business services. A wide range of business practices are directly impacted by your company's effective use of the Internet. With the growing availability of affordable broadband services such as DSL (Digital Subscriber Line) and cable, your Internet access becomes even more essential to your business. And record numbers of small businesses recognize the advantages of broadband and are switching over to these high-speed Internet connections. According to International Data Corporation (IDC), there are currently 700,000 small businesses (defined as 100 employees or smaller) in the United States with a broadband Internet connection.

While high-speed, always on Internet connections offer businesses significant advantages, they also raise new network security concerns. As small businesses shift from dial-up to always-on broadband Internet connections, their networks become more vulnerable to Internet hackers. These Internet security attacks can wreak havoc on your business. A single attack can be devastating with all your valuable data wiped out, confidential information stolen or corrupted, your entire network made inoperable, or access to sites vital to your business operations shut down.

This paper addresses the opportunities and risks of broadband Internet access for small and medium size enterprises (SMEs), professional offices, branch offices, and telecommuters. It explains the types of Internet security threats and your strategy options for incorporating security into your broadband Internet service.

Working Smarter with Broadband

Once a business taps into the power of a broadband Internet connection, the business works smarter. Broadband is more than just faster Internet access; it changes the way your business works as many offline business tasks get converted into convenient online activities. With broadband, your business gets a front row seat to innovative business services available on the Internet. The business case for powering your business with broadband is compelling.

Do More in Less Time

Broadband is about doing more in less time. Faster, always-on Internet access via broadband means people are more productive. Sending a PowerPoint presentation that took an hour to send using a dial-up modem now takes only a few minutes. Researching information or doing e-commerce from a number of Web sites can be done simultaneously instead of waiting for each page to slowly appear one at a time. E-mail is instantly sent and received for quick turnarounds. Software is efficiently downloaded and updated. Multiply all these timesaving benefits across all

the people in your office and you see what speed means to your business.

Save Money on Your Internet Access Costs

A broadband connection can save you money over using dial-up Internet access. Even moderate use of a dial-up or ISDN Internet connection can cost a hundred dollars a month for the telephone line, business telephone usage costs, and Internet access. A small office with five PCs and dial-up Internet connections can easily incur costs of \$500 per month. Converting to a 784 Kbps DSL-powered Internet connection can typically save your business up to 50% per month and deliver almost 20 times faster than a dial-up modem. All your employees can share this single, high-speed connection. No more separate telephone lines, modems, and Internet access accounts for each computer. Instead, you link up all the computers in your business via a local area network (LAN).

Tap into Online Business Services

Online business transactions are about convenience, saving time, and saving money. Business-to-business services on the Internet continue to expand and your broadband powered business can take full advantage of them. Whether it's ordering office supplies, managing your business finances with online banking, conducting online meetings, doing data backup, hunting and gathering information, or downloading software, broadband makes using these services a normal course of everyday business.

Make the Right Connections with VPN

A Virtual Private Network (VPN) moves your private data securely over the public Internet. This allows your business network resources to be available to telecommuters, remote workers, branch offices, consultants, contractors, and partners. Virtual Private Networking uses data encryption and the Internet to provide high-performance, secure communications between sites without incurring the high expense of leased site-to-site data communication lines. VPN isn't new, large enterprises have been using it for years, but thanks to the affordability of broadband, the benefits of Virtual Private Networking are now available to small and medium size enterprises. A VPN delivers these benefits to your business:

- Allows people to telecommute enabling your business to share in their productivity gains. With fewer meetings, less interruptions, and no commute, employee productivity dramatically improves.
- Eliminates the need for maintaining expensive dedicated site-to-site data communication links or multiple telephone lines with modems and paying telephone company usage costs to support dial-up connections to your office network. With a VPN, broadband and

dial-up telecommuters, remote workers, and branch offices all use the Internet to connect to your main office network.

What are the Security Threats?

Security is the soft white underbelly of broadband Internet service and the threats are real. How pervasive are security threats on the Internet?

- The 2000 Computer Crime and Security Survey published by the FBI and Computer Security Institute found that 71% of all companies reported being attacked by independent external hackers in the last 12 months.
- A Gartner Group survey shows more than over 50% of small and midsize enterprises (SMEs) using the Internet will be hit by hackers.
- According to IDC, the average new DSL connection experiences three attempted “hacks” in the first 48 hours.

Security threats come in a variety of forms, but the results are the same: a serious disruption to your business. Compounding the security weaknesses of the Internet is the widespread availability of “hacker-helper” programs on the Internet. Today, talented hackers are writing extremely powerful hacking tools and making them available for download on the Internet. No longer must the attacker be an expert or understand the nuances of the target’s vulnerabilities, all they need to do is point the tool at the target and hit the “Attack” button.

Here are the most common types of Internet security threats your business faces.

1. **Unauthorized Access to Your Network.** Hackers breaking into your network can view, alter, or destroy private files. A hacker can, for example, modify accounting, medical, or academic records, and then leave, with the break-in and changes going undetected until it is too late. Hackers may use a variety of readily available “hacker’s helper” tools to break into the network. Once in, the hacker has control of your computer and access to your confidential data.
2. **Denial of Service (DoS) Attacks.** Increasingly prevalent Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood and LAND Attack, aim not to steal information, but to disable a device or network so users no longer have access to network resources. Even if your network is not being attacked, it can be used as an unwitting ally in Denial of Service attacks on other networks. Using Trojan Horses or other malicious attachments, hackers plant tools on hundreds and sometimes thousands of computers to be used in future attacks. So, in addition to protecting your own

LAN from attacks, you need to prevent your LAN computers from being compromised and used in attacks on others.

3. **Viruses.** These are destructive programs that attach themselves to E-mail, applications and files. Once on your LAN computers, viruses can damage data or cause computer crashes. Users can quickly damage entire networks by unknowingly downloading and launching dangerous computer viruses. Viruses can also be used as delivery mechanisms for hacking tools, putting the security of the organization in doubt, even if a firewall is installed.
4. **Capture of Private Data Going Over the Internet.** As your private data moves over the Internet, hackers using programs called packet sniffers can capture your data as it passes from your network over the Internet and convert it into a readable format. The source and destination users of this information never even know that their confidential information has been tapped.
5. **Offensive Content.** Inappropriate Internet content can create an uncomfortable work environment and cause potential legal problems for your business. Network users risk viewing inappropriate content, decreasing productivity, and inviting lawsuits by abusing company resources with unregulated Web browsing.

Warning: *If your broadband Internet service uses a DSL or cable modem, your Internet connection is wide open to any kind of hacker attack. Broadband modems are simple internetworking devices that simply connect your network to the Internet without any security protection.*

Protecting Remote Offices and Workers

While security is the soft white underbelly of any broadband Internet connection, the good news is there are affordable security measures for fortifying remote offices and workers against Internet based attacks. Total security comes from integrating a variety of different security measures to counteract different types of security threats. Security measures for protecting these sites fall into the four general categories: firewall, anti-virus, content filtering, and Virtual Private Networking (VPN).

Firewalls

The International Computer Security Association (ICSA) classifies firewalls into three categories: Packet Filters, Application-Level Proxy Servers, and Stateful Packet Inspection Firewalls. Firewalls are just one part of a total integrated security solution.

- **Packet filter firewalls.** Typically implemented on DSL or Ethernet routers, 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.** This upper level examination of IP packets firewall approach, while superior to packet filtering, causes significant performance degradation to broadband Internet connections. Also, proxy servers can be difficult to set up and maintain for non-technical users.
- **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-handling 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.

Warning: *Many self-proclaimed "firewalls" are nothing more than "NAT boxes", which perform Network Address Translation (NAT). NAT allows networks to use a single public IP address to connect to the Internet and private IP addresses for LAN computers, thereby providing some privacy to LAN users. However, NAT does not constitute a secure firewall. Easily bypassed by "IP spoofing" and lacking the necessary logging and reporting features of firewalls for monitoring network security, NAT alone is not adequate for protecting your network resources. Make sure that a trusted third party, such as the International Computer Security Association (ICSA), certifies the security product claiming to be a firewall.*

Virus Protection

Computer viruses and other malicious programs, which attach themselves to applications and files in memory or on disks, are a leading security threat to Internet-connected networks. Destructive viral programs can infect networked PCs through E-mail attachments, web content or infected files. Viruses damage data, cause computer crashes, or lie dormant like a time bomb that explodes at some future event. Because users with infected machines may not discover viruses immediately, they can quickly and unwittingly spread damaging viruses throughout a network.

Virus protection can be accomplished in three ways: Desktop, Managed or Policy Enforced.

- **Desktop.** Protection at the desktop level is the most effective way to combat viruses, because doing so ensures protection from viruses received from E-mail, Internet downloads, and portable media such as floppy disks. Because most desktop anti-virus programs can be deactivated by PC users, require manual installation, and need regular updates on each PC, they are rarely used without centralized management to immunize networks from viruses.
- **Managed.** These anti-virus programs function at the gateway level. Downloads and emails are scanned at the entrance to the network, the gateway. More easily managed than basic desktop scanning programs, gateway anti-virus programs do not scan the source of a large number of all viruses: portable media and LAN-based infections. Also, the extra scanning required at the gateway level can slow the processing of network traffic.
- **Policy Enforced.** This form of virus protection has all the advantages of desktop and managed scanning without the disadvantages. Automatically updated anti-virus software is maintained on each desktop by the firewall. When users attempt to access the Internet, the firewall checks to verify the user's PC has the latest version of the virus scanning engine installed and active. In the event of out-of-date or deactivated anti-virus software, the firewall automatically updates and activates the virus protection. Users' computers are then secure against viruses in E-mail, downloads and portable media.

Content Filtering

Content filtering allows schools, businesses, and other organizations to set and enforce Acceptable Use Policies (AUPs) governing what materials can and cannot be accessed on the organization's computers. Without content filtering, your LAN users have unlimited access to all Internet resources, appropriate and inappropriate, benign and dangerous.

Creating and enforcing Internet access policies enables you to block incoming content and filter out Internet sites with offensive material. Content filtering can be accomplished using these methods:

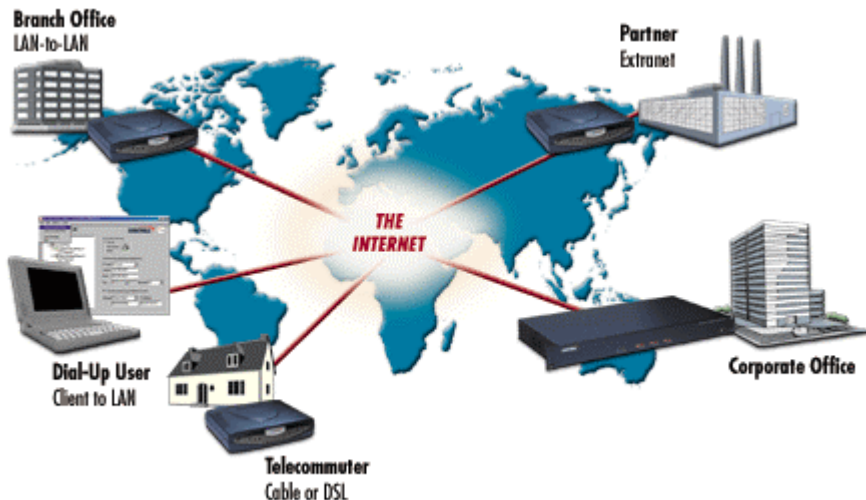
- **Text Screening.** Stops Internet pages from loading when the filter words on a predefined list are encountered in either the URL or body of a page. Text Screening is most effective when used in conjunction with other filtering measures and must be used with caution. For example, screening for the word "breast" will block out breast cancer sites, "sex" will block out "Anne Sexton" and sites without any text from the block list will not be screened.

- **Proxy or Allow Only Lists.** Implemented via client software that only allows access to approved sites or via centralized proxy servers that pre-load all approved content. All clients access the proxy server instead of accessing the Internet directly. The proxy server then connects to the Internet to download the latest content. For example, a teacher might use a proxy list to allow students to search for material only from a pre-selected list of approved sites. With careful screening, this method can be almost 100% effective at blocking pornography and other objectionable material. The key disadvantage is that many useful sites will also be blocked until they are “discovered” by the administrator.
- **URL Blocking.** Blocks content via content filter lists provided by a trusted third-party content filtering organization that continuously searches the Internet looking for offensive sites. Sites are selected and placed in one or more categories, such as “Full Nudity”, “Profanity”, or “Racial Intolerance.” Editors review selections before adding them to the filter list. URL Blocking, based upon a frequently updated filter list from a reputable organization, is the preferred method of Content Filtering because it blocks objectionable or inappropriate content while preserving access to valuable Internet resources. Because of the adoption of the CyberNOT filter list by organizations such as Microsoft, Netscape, AT&T, America Online, IBM, and The Scholastic Network, it’s becoming the standard for implementing URL Blocking.

Virtual Private Networking (VPN)

Today’s business environment requires real-time collaboration among geographically dispersed people and offices. A VPN (Virtual Private Network) is part of your business security package if you plan to allow partners, clients, telecommuters, and remote workers access to your company network resources. A VPN uses data encryption and the Internet to provide high performance, secure communications between sites without incurring the expense of leased site-to-site lines, or modem banks and telephone lines.

A VPN enables your organization to establish secure communications in a manner that is transparent to end-users. A VPN can connect individual telecommuters to the office network, creating a separate, secure tunnel for each connection or connect remote office networks together as a LAN-to-LAN connection over the Internet using a single data tunnel.



A VPN enables geographically dispersed people and offices to securely link up over the Internet to access business-critical information on the company network.

Internet Protocol Security (IPSec) is a robust standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity, and authentication.

Digital certificates add even more security to VPN connections by allowing businesses to authenticate individuals wanting access to confidential company resources. For example, digital certificates can be used to authenticate a remote user before granting access to highly confidential information, such as medical records distributed over a VPN, which connects doctors, insurers and patients.

Evaluating Security Options

In determining the best security product for your needs, there are several important considerations to keep in mind. Here are guidelines to help you evaluate security solutions for your business.

Ala Carte or Integrated Security

You can deploy the multiple security measures for your business by going with 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 costs considerably more than an integrated security solution.

A firewall from one vendor only protects against certain types of security threats. Viruses pass right through a firewall, so you'll need to purchase an anti-virus solution to protect the computers on your LAN. Neither a firewall nor an anti-virus program will protect your business from employees causing potential legal problems for your business by viewing inappropriate content. You'll need a content filtering product from another vendor. If you want VPN, you'll need to purchase a VPN solution from yet another vendor. In addition, integrating security products from different vendors can be difficult and lead to security vulnerabilities if not done correctly.

An integrated security approach involves evaluating a security suite of products from a single vendor that puts it all together for you. Starting with the base platform, you can enable additional security features such as virus protection, content filtering, and VPN. This integrated approach may be embodied in a product called an Internet security appliance that supports all the security measures as an integrated solution in a single device that sits between your LAN and the Internet to defend your business at the point where the Internet meets your local network.

Gateway Security

The positioning of your network security solution at your LAN gateway to the Internet is the best place. Security at the gateway means the security for your network is positioned at the Internet entry point to the network to monitor all inbound and outbound traffic, allowing only permitted traffic to pass. A gateway security product allows you to centralize the management of your LAN security at one point of interface instead of on each client computer on your network.

Up-to-Date Protection

Just as the Internet is a dynamic, changing environment, Internet-borne threats are also constantly changing. Look for security products that can easily adapt to the changing threats by providing the ability to update the software that provides protection against the latest hacker 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 easy to perform, if not automatic, so that the security product can keep pace with the latest threats.

Ease of Use

Purchasing the appropriate security product is not enough to guarantee security. It needs to be easy enough for small organizations without in-house IT professionals to set up and manage. Many security products on the market today are complex and unconfigured for protecting your business out of the box. They use cryptic commands or menus that require the additional cost of a security consultant to setup and maintain.

Look for products with a reputation for ease-of-use, and with an intuitive, graphical interface that can be taken out of the box and installed with minimal configuration. Internet security appliances provide this type of plug-and-play installation.

Total Cost of Ownership

Larger organizations have traditionally been able to justify the high cost of security professionals to implement and maintain their complex security solutions. This is almost never the case in smaller businesses because they lack the resources to support expensive in-house technical expertise to manage their security solutions. Your budget for a security 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 largest 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. The Total Cost of Ownership chart provides a worksheet to use as a starting point for comparing different security 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	\$ _____

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 enterprise. 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.

The SonicWALL Solution

SonicWALL Internet security products and services provide a comprehensive, integrated security solution that can be tailored to fit the needs of small and medium size businesses. Core SonicWALL security technologies include firewall, VPN, PKI and digital certificate authentication, network anti-virus, content filtering, and security management. An organization of any size can affordability and quickly deploy enterprise-class security and remote access with SonicWALL's ease-to-use Internet security solutions.

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.

SonicWALL VPN, based on the IPSec (Internet Protocol Security) industry standard, offers an easy, affordable, and secure means to connect small and medium size businesses. SonicWALL VPN is compatible with other IPSec-compliant VPN gateways.

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 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.*

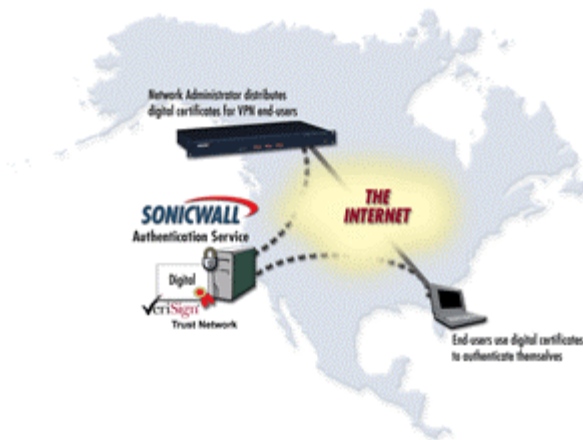
SonicWALL Authentication Service

Establishing the identity of users on the Internet to allow VPN access to resources is a significant challenge for network administrators. Digital certificates are widely accepted as the best solution for establishing user

identities with absolute confidence, and VeriSign is the worldwide leader in the market for digital certificates and trusted services.

SonicWALL Authentication Service is an affordable, easy to administer, end-to-end digital certificate solution for secure remote access. Utilizing VeriSign technology to deliver strong authentication of VPN users across the Internet, SonicWALL Authentication Service protects your organization's valuable and confidential resources.

SonicWALL Authentication Service allows network administrators to add strong VPN user authentication using Public Key Infrastructure (PKI) and digital certificates without the cost and complexity of a do-it-yourself solution. Certificate distribution is streamlined via a secure, Web-based (HTTPS) server. Network administrators can quickly issue and revoke digital certificates for VPN users to facilitate the timely management of access services.



SonicWALL's Authentication Service allows your organization to protect your network from unauthorized VPN users using PKI and digital certificates without the high cost and complexity of a do-it-yourself solution.

Network Anti-Virus

SonicWALL Network Anti-Virus delivers industry-leading, proactive virus protection with zero administration. Developed in partnership with McAfee, the market leader in business anti-virus solutions, SonicWALL Network Anti-Virus dramatically reduces time-to-protection with advanced heuristics and automatic alerts to provide the most reliable anti-virus solution on the market today.

SonicWALL Network Anti-Virus is also the only zero administration solution that automatically manages all aspects of virus protection

including client auto-installation, virus definition updates, and network-wide policy enforcement to significantly reduce support costs.

SonicWALL's Network Anti-Virus is a subscription-based service for SonicWALL's family of Internet Security Appliances that transparently monitors virus definition files, and automatically triggers new virus definition file downloads and installations for each PC on the network. Acting as an auto enforcer of virus policy, the SonicWALL Internet Security Appliance with SonicWALL Network Anti-Virus ensures every PC accessing the Internet has the most up-to-date anti-virus software installed and active, preventing the spread of new viruses or a rogue user from exposing the entire organization to an outbreak.



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.

Content Filtering

SonicWALL Content Filtering allows your enterprise to maintain Internet access policies tailored to their specific needs, with built-in support for URL filtering, keyword blocking and cookie, Java and ActiveX blocking. The optional SonicWALL Content List Subscription, based on the widely accepted CyberNOT List, ensures proper enforcement of access restrictions. Automatic updates keep administrators current on the sites containing inappropriate online material. Administrators can customize categories of Internet sites, such as pornography or racial intolerance, to block or monitor access.

SonicWALL Global Management System

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 enterprise. SonicWALL GMS enables network administrators to uniformly define, deploy, and enforce security and VPN policies from a central location to protect your entire business.

An administrator can configure SonicWALL firewall settings as well as SonicWALL upgrade and subscription services, such as VPN, network anti-virus and content filtering. Security policies can be centrally pushed to SonicWALL Internet security appliances on an individual, group, or global basis. SonicWALL GMS pushes security policies over encrypted VPN tunnels to ensure maximum security for deploying security policies and firmware updates.



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

Internet Security Bottom Line

The bottom line is your business needs to incorporate security into any broadband Internet service implementation. Attacks by Internet hackers can destroy your valuable business data, expose confidential information, or shut down critical business operations. There are many factors to consider when purchasing a network security solution for your organization. Every organization is different, and in no way have we covered every possibility, but this paper has presented the key issues that need to be addressed when choosing the right security solution. The good news is that affordable Internet security appliances from SonicWALL offer integrated security solutions for small and midsize enterprises to make your security 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.