

SonicWALL White Paper

Internet Security Issues
for Small to Medium Size Enterprises



Introduction

In just a few short years, the Internet has been transformed from a mysterious “thing”, used exclusively by government and scientific organizations into a mass medium used daily by individuals and organizations for communications, research, entertainment and multi-million dollar business to business exchanges.

Many small to medium enterprises and branch offices have addressed the need for Internet access by installing a single computer with a dial-up connection that is shared throughout the office, or by installing a dedicated network data connection at a significantly greater expense, such as a T-1 line. Recently, new high-speed technologies have emerged that can better satisfy the bandwidth requirements of small to medium enterprises at a fraction of the cost of traditional solutions. These technologies include DSL and cable modems, which provide access speeds up to 100 times faster than traditional 28.8 kbps analog modems. Because broadband technologies, including DSL and cable, are always connected to the Internet, they present greater security issues than dial-up connections and increase the risk that proprietary data or other sensitive information might be compromised.

High-speed, always-on Internet connections, such as cable or DSL, offer businesses significant advantages but also threaten network security. Hackers or unauthorized users may steal or corrupt important information and disrupt access to sites vital to costly business transactions. Confidential data may be inadvertently disclosed during transmission. Viruses and Trojan Horses, transmitted across the Internet or in portable media, can infect and damage local networks and rapidly spread to other networks. Hate groups and pedophiles use the Internet to distribute propaganda and prey on young children.

This paper addresses the security issues raised by the “connected” society, framed in the context of the needs of the small to medium size enterprise (SME), branch office, telecommuter, consumer and education markets.

The Risks

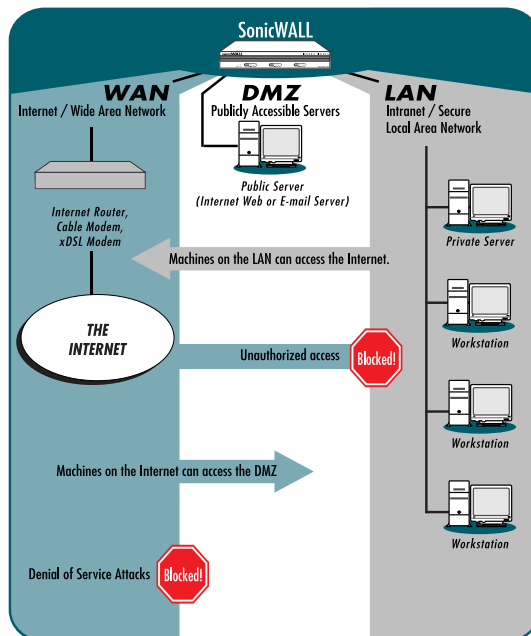
Anxious to leverage the power and speed of inexpensive broadband connections, many organizations do not adequately address the security issues these connections raise. Connecting a LAN (“Local Area Network”) to the Internet is not a task to be taken lightly. Like any other large community, the Internet consists of both good and bad elements. And, as broadband Internet access solutions proliferate, the opportunities for malicious individuals to exploit network security weaknesses multiply.

Increasing numbers of small businesses, telecommuters and home Internet users are taking advantage of low-cost, high-speed Internet connection technologies such as cable and DSL. Unlike their previous dial-up connections, however, these “always-on connections” make their networks vulnerable to attack.

Hackers attempt to break into networks to view, alter, or destroy private files. Upon accessing a network, a hacker could, for example, modify accounting, medical, or academic records, and then leave, with the break-in and changes going undetected until it is too late. Increasingly prevalent Denial of Service Attacks (“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. For example, “WinNuke”, a widely available DoS tool, is used to remotely crash any unprotected Windows PC on the Internet. The widespread availability of “hacker-helper” programs on the Internet can make anyone a virtual hacking professional.

Even if they are not being attacked, networks may be used as unwitting allies in Denial of Service attacks. Smurf, Tribe Flood Network and Trinoo Attacks use amplifier networks created by a hacker long before the attack actually begins. 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 their own LAN from attacks, network administrators need to prevent LAN PCs from being compromised and used in attacks on others.

Hacker attacks are not the only problem administrators of Internet-connected networks must resolve. Destructive computer “viruses” and inappropriate Internet content can cause significant headaches for network administrators. Users may quickly damage entire networks by unknowingly downloading and launching dangerous computer viruses. Network users risk viewing inappropriate content, decreasing productivity and even inviting lawsuits by abusing company resources with unregulated web browsing.



Protecting Network Resources and Users

Fortunately, network managers now have many resources for fortifying the LAN against Internet based theft, modification, or deletion of data and for protecting users from objectionable Internet content. These security measures fall into four general categories: firewall, Virtual Private Networking (VPN), anti-virus and content filter.

Firewall

A firewall protects the private network against Internet based theft, destruction, or modification of data by examining all traffic passing from the Internet or Wide Area Network (WAN) to the private, local area network (LAN). The International Computer Security Association (ICSA) classifies firewalls into three categories: Packet Filters, Application-Level Proxy Servers, and Stateful Packet Inspection Firewalls.

Packet Filters

Packet filters, the first generation of firewalls, are typically implemented on routers and examine the individual packets of data passing across the firewall. Examining data passing to and from a network, packet filters use rules to block access according to information located in each packet: the TCP/IP port number for which data is intended, source or destination address, or data type. Unfortunately, configuring a packet filter firewall can be arduous and confusing. Packet filters are also prone to IP spoofing, in which an IP packet is altered to appear to have an internal, rather than external, source address. The fooled packet filter passes this counterfeit IP packet to the protected network. Some protocols, such as FTP and DNS, can't be safely passed through packet filters because they require opening "holes" in the firewall which compromise security. Packet filters also lack a DMZ port, which separates public servers, such as Web or FTP servers, from the rest of the network while protecting both from Internet based attacks.

Application-Level Proxy Server

Communications between networked end users are divided into layers. Each layer adds its own set of special, related functions. IP packets typically consist of seven "layers", including the "physical", "network" and "application" layers. In a given message there will be a flow of data down through each layer at one end, and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user.

Application-Level Proxy Servers examine the application layers of IP packets to verify their authenticity. This upper level examination, however, causes significant performance degradation. Also, each application type, such as HTTP, FTP, SMTP or POP3, typically requires installation and configuration of a different application proxy. Finally, these proxy servers require the administrator to reconfigure their network settings to support the proxy.

Stateful Packet Inspection

The third generation in firewall technology, Stateful Packet Inspection, is considered by Internet experts to be the most advanced firewall technology because it examines all network layers to either accept or reject the requested communication. Stateful Packet Inspection, transparent to users on the LAN, requires no client configuration. Stateful Packet Inspection supports numerous Internet protocols, including TCP, used by applications such as HTTP, FTP, SMTP, POP3, Telnet and others; and UDP, used by applications such as DNS, DHCP and RealAudio. Packet filters and proxy servers typically do not support UDP. Stateful packet inspection is similar to the algorithms used by enterprise level firewall vendors, such as Check Point and Cisco, and is widely considered to be the most effective method of protecting the private LAN.

Network Address Translation

A cautionary note: Many self-proclaimed "firewalls" are nothing more than "NAT boxes", appliances that perform Network Address Translation (NAT). NAT allows networks to use a single public IP address to connect to the Internet, thereby providing some privacy to LAN users. However, NAT alone 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 to protect network resources. Network administrators should make sure that firewalls are certified by a trusted third party, such as the International Computer Security Association (ICSA).

Virtual Private Networking (VPN)

Today's business environment requires close, real-time collaboration with trading partners, legal and financial advisors, and remote and branch offices. This "real-time" requirement often leads to the creation of an "extranet", in which branch offices and partners are connected to the primary business network. Organizations may create these extranets by leasing dedicated data lines to connect the sites. Since this method is cost prohibitive, companies are turning to technology that allows creation of Virtual Private Networks (VPN).

VPN uses data encryption and the public Internet to provide high performance, secure communications between sites without incurring the expense of leased site-to-site lines. The standard for VPN is IPSec. IPSec VPN offers standards-based, flexible solutions for secure data communications across a public network such as the Internet.

Small to medium size organizations, just like large enterprises, need secure, cost effective communications with business partners, clients and telecommuters. VPNs enable SMES to establish these secure communications in a manner that is seamless and transparent to end-users. With VPN, SMEs can migrate from expensive, private leased lines to using the Internet for secure communications.

SonicWALL VPN provides an easy, affordable, and secure means for businesses to connect all offices and partners together. Using SonicWALL's intuitive Web browser management interface, a secure connection may be easily created between two or more sites. Whenever data is intended for the remote site, SonicWALL VPN automatically encrypts the data and sends it to the remote site over the Internet, where it is automatically decrypted and forwarded to the intended destination

Anti-Virus Protection

Computer viruses are a leading security threat to Internet-connected networks. Viruses are malicious software programs that attach themselves to applications and files in memory or on disks. Destructive viral code may infect networked PCs through E-mail attachments, seemingly harmless ads on web pages or infected files on floppy disks. Viruses may damage data, cause computer crashes or lie dormant for later use. Because users with infected machines may not discover viruses immediately, they can unwittingly spread damaging viruses throughout a network. Anti-Virus protection can be accomplished in three ways: Desktop, Managed or Policy Enforced.

Desktop Anti-Virus Protection

Protecting 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. But, because most desktop anti-virus programs can be deactivated by PC users and require manual installation and regular updates on each network PC, they are rarely used by network administrators to immunize their networks from viruses.

Managed Anti-Virus Protection

Managed anti-virus programs function either at the desktop or gateway level. Downloads and E-mails are scanned either at each desktop or at the entrance to the network, the gateway. More easily managed than basic desktop scanning programs, managed or gateway anti-virus programs do not, however, scan the source of a large number of all viruses: portable media. Users can also deactivate managed scanning solutions that work at the desktop level, and the extra E-mail scanning required at the gateway level can slow the processing of network traffic.

Policy Enforced Anti-Virus Protection

Policy enforced anti-virus protection, such as SonicWALL's, has all the advantages of desktop and managed scanning without the disadvantages. Automatically updated anti-virus policies are enforced on each desktop, and managed from 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, before allowing the request. Users' PCs are then secure against viruses in E-mail, downloads and portable media. Users cannot

deactivate policy enforced anti-virus programs and all scanning takes place at the PC level, without slowing network traffic for E-mail scanning. Policy enforced anti-virus scanning is a technology unique to the SonicWALL family of Internet security appliances.

Content Filter

A content filter 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 a content filter, users have unlimited access to all Internet resources, appropriate and inappropriate, benign and dangerous. Content filtering can be accomplished by varying methods: Text Screening, Proxy or "Allow Only" Lists, and URL Blocking.

Text Screening

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 rarely used because it blocks non-objectionable speech and is ineffective against sites with no text. 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

Proxy or "Allow Only" Lists are 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 may be nearly 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 via Content Filter Lists

In URL or Web Blocking, members of a committee continuously search the Internet looking for offensive sites. Sites are selected and placed in one or more categories, such as "Full Nudity", "Profanity", "Racial Intolerance" and others. 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. Due to its adoption by organizations such as Microsoft, Netscape, AT&T, America Online, IBM, and The Scholastic Network, the CyberNOT filter list from The Learning Company is becoming the standard for implementing URL Blocking.

Network Security Requirements

Because of the wide array of opportunities offered by the Internet, organizations have different requirements when applying the Internet to their daily operations. However, one theme rings through all: the need for robust security.

Small to Medium Size Enterprises

SMEs connected to the Internet with always-on, broadband connections, such as cable and DSL, need reliable protection for their private LANs. A single security breach, such as an attack on the company's Web or E-mail server, can have a catastrophic effect on the organization's viability. Destructive computer viruses can quickly spread throughout a network and cripple applications. Administrators may also need content filters to protect employees from harmful Internet material and to minimize vulnerability to harassment lawsuits that might result from employees using company resources to access objectionable material on the Internet.

Since many SMEs do not have dedicated IT staffs or large IT budgets, ease of installation and maintenance, as well as affordability are key factors in the network security solutions they choose.

The Distributed Enterprise

Since the rise of the Internet, IT managers and corporate executives of large enterprises have been diligent in educating themselves and taking steps necessary to protect their networks from attacks. High-end solutions, such as Check Point Software's Firewall-1, guard the main entrances to the network from hackers— the publicly known servers and services providing Web, telnet, and ftp access for customers.

The recent proliferation of inexpensive high-speed broadband access has allowed enterprises to effectively connect branch offices, telecommuters and key business partners to corporate headquarters.

Though the main entrance to an organization's LAN may be fortified and monitored, other entrances may not be as well protected against external or internally launched attacks. Remote offices may not be protected at all, placing their own data and application availability at risk, and perhaps also providing an unguarded "back door" into the fortified headquarters network. Alternative portals into an enterprise network need the same kind of protection used at the main network entrance. This perimeter defense consists of firewalls at remote locations, and virtual private networks between sites.

Internet Service Provider (ISP)

In addition to selling broadband connections to the Internet (e.g., DSL, Cable, T1, ISDN), many ISPs now provide complete "turnkey" installations, providing routers and other necessary hardware and software. ISPs help sometimes wary SMEs establish their Internet

presence and, by offering these partners additional networking products and expertise, increase their own sales and service revenues. Service offerings such as global management of customers' access and security policies are possible through global management tools that allow ISP administrators to centrally manage and monitor the security of their customers.

Schools and Libraries

Schools and libraries have a rapidly growing need for network security. For many years, educators have seen the Internet as a tremendous resource for helping students expand their skills in research, science, technology, and critical thinking, as well as helping them understand different cultures and social organizations through direct interaction.

While protecting the LAN from Internet based break-ins and attacks is of great importance, many educators are becoming more concerned about restricting access to dangerous content on the Internet. Libraries often wish to restrict certain users access to objectionable sites, such as children's access to sexually explicit or racially intolerant sites, without restricting other patrons' access to Internet resources. Much to their credit, educators and librarians are taking a proactive approach by installing content filtering and other security products.

Many schools and libraries do not have a dedicated network administrator. Instead, a teacher or other member of the staff assumes the position of "Technology Coordinator" and the additional duties associated with maintaining a computer lab and network. Because a Technology Coordinator's time is better spent with students and patrons, and not maintaining computer equipment, ease of installation and minimal maintenance are often a prerequisite for these users. A severe lack of funds for such purchases is often the norm, making affordability especially important for librarians, educators and school administrators.

Network Security Products

The Internet Security market is serviced by many companies that offer products with a wide variety of features and implementations. These products fall into three general categories: software, hardware, and appliance.

Software Internet Security Products

Software Internet security products are typically sophisticated, complex applications that run on a dedicated UNIX or Windows NT server. Some of the market leaders in this product category are Check Point's Firewall-1 and Axent Technologies' Raptor Firewall.

Check Point's Firewall-1 (\$7,995 retail with 100 user license) is a Stateful Inspection firewall that runs on either an NT or UNIX server, and supports IPSec VPN. Axent Technologies' Raptor Firewall (\$6,500 retail) is an Application Gateway Proxy Server that runs on either an NT or UNIX server.

The prices listed do not include the server hardware and operating system for the software to run on. The necessary hardware may add \$3,500 for a low-end NT server, to well over \$15,000 for a Sun Solaris server, to the total cost of the network security system. These products are also susceptible to the security holes in the server's operating system (OS). Gartner Group projects that at least one major NT networking security vulnerability will be discovered and exploited by Internet hackers each year through the year 2002. Without the dedicated MIS staff installing the patches to cover newly discovered security holes as they are discovered, the resulting security holes can render the software firewall useless. These products do not provide anti-virus protection or content filtering.

Software Internet security products are well suited for organizations with the extensive technical and financial resources required for their setup, configuration, and maintenance. However, because of the required expertise and the lack of automatic software updates or anti-virus protection, software security products are not well suited for the SME market.

Hardware Internet Security Products

Hardware Internet security products, such as the Cisco PIX, are dedicated firewalls, or firewall software installed on a router, such as Lucent's Secure Access. Since they usually run on a dedicated, embedded operating system, hardware firewalls may not be susceptible to many of the security weaknesses inherent in the NT and UNIX operating systems. Most of these high performance firewalls satisfy the extremely high throughput requirements of large enterprises with T3 connections to the Internet, or carrier class ISPs, such as Sprint or MCI.

Cisco's PIX (retail: \$9,000 to \$22,000) is a Stateful Inspection firewall that is well suited for large networks with dedicated MIS professionals. Pricing varies based on hardware

options such as CPU, RAM and disk storage, network interface, etc. Lucent's Secure Access is a software upgrade to the Pipeline family of ISDN and T1 routers. These products do not provide anti-virus protection, content filtering or auto-update features.

Because there is no need to harden the OS, these products are usually easier to install and configure than the software firewall products, but still lack the "plug and play" installation, minimal maintenance and complete security solution offered by products in the next category, Internet Security Appliances.

Internet Security Appliance

Internet Security Appliances are pre-configured to best meet specific needs. These turn-key plug-and-play appliances provide ease of installation and maintenance, and high performance for specific markets, such as the SME, branch office, telecommuter and branch office markets.

SonicWALL Internet security appliances (U.S. retail \$495 to \$4,995) offer an ICSA certified stateful packet inspection firewall, integrated with optional virus protection, content filtering, IPSec VPN compatibility, and IP address management, all in one powerful, easy-to-use security solution. Without the complexity of traditional high-end firewalls or the shortcomings of combined router/firewall devices, SonicWALL products provide a complete network security solution meeting the unique needs of networks ranging in size from a single telecommuter to a distributed enterprise with thousands of nodes. Firmware updates are free for the life of the product.

SonicWALL Internet Security Appliance

High-speed, always-on Internet connections offer businesses significant advantages but also threaten network security. Hackers or unauthorized users may steal or corrupt important information. SonicWALL state-of-the-art technology provides robust, reliable, and affordable Internet security for businesses with a few users to several thousand users.

To protect the private network against Internet-based theft, destruction, or modification of data, SonicWALL implements firewall security with stateful packet inspection. SonicWALL allows data from the Internet only if it's part of a session that was initiated by a user on the secure private network; hackers and other unauthorized Internet users will be blocked.

SonicWALL protects the network from Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, IP Spoofing, and LAND Attack. When new hacker attacks are discovered, SonicWALL adds protection from them to the SonicWALL software and automatically notifies the administrator of the new firmware releases. All registered SonicWALL customers get free software updates.

SonicWALL VPN Upgrade provides an easy, affordable, and secure means for businesses to connect offices and partners together. Using data encryption and the Internet, SonicWALL VPN provides secure communications between two or more sites without the expense of leased site-to-site lines. Encryption methods include 168 bit Data Encryption Standard (Triple-DES), 56 bit Data Encryption Standard (DES) and 56 bit ARC4 (ARC4). SonicWALL VPN can be used with other VPN products with the same IPSec implementation, such as Check Point Firewall-1, Cisco PIX and Axent Raptor. SonicWALL VPN Upgrade also includes a single-user license VPN client for Windows to allow secure remote management. SonicWALL VPN is included in the SonicWALL PRO.

SonicWALL Network Anti-Virus eliminates the challenges of managing network-wide anti-virus solutions. SonicWALL Network Anti-Virus transparently deploys an agent configured by the administrator to each of the systems to be protected - no desktop-by-desktop installation or configuration required. Because the agent is automatically updated each time end-users access the Internet, SonicWALL Network Anti-Virus ensures that all nodes on the network are protected with the most current anti-virus engines.

Content filtering allows businesses to create and enforce Internet access policies tailored to the needs of the organization. An optional Content Filter List subscription is available which allows the administrator to select categories of Internet sites, such as pornography or racial intolerance, to block or monitor access. Automatic weekly updates of the customizable Content Filter List make sure that access restrictions to new and relocated sites are properly enforced. Users may be given a password to bypass the filter, giving them unrestricted access to the Internet.

SonicWALL Global Management System is a scalable, cost-effective solution that extends the SonicWALL Internet security appliance's renowned ease of installation and administration, giving network administrators the tools to easily manage the security policies of remote, geographically distributed networks. The recent proliferation of inexpensive high-speed broadband access has accelerated the connection of branch offices, telecommuters and key business partners to corporate headquarters. SonicWALL GMS reduces staffing requirements, speeds up deployment and lowers the cost of delivering services to these remote locations by centralizing the management and monitoring of security policies.

SonicWALL's Key Features

- **Firewall Security.** SonicWALL Internet security appliances use stateful packet inspection to protect the private LAN from hackers and vandals on the Internet.
- **IPSec VPN.** SonicWALL VPN provides an easy, affordable, and secure means for businesses to connect offices and partners together. Encryption methods include 168 bit Data Encryption Standard (Triple-DES), 56 bit Data Encryption Standard (DES) and 56 bit ARC4 (ARC4). SonicWALL VPN can be used with IPSec VPN products such as Check Point Firewall-1, Cisco PIX and Axent Raptor.
- **Network Anti-Virus.** SonicWALL Network Anti-Virus, based on Network Associates' market-leading anti-virus product, ensures corporations are protected against the latest virus outbreaks as soon as cures are available.
- **Internet Content Filtering.** SonicWALL's content filtering functions allow businesses to create and enforce Internet access policies tailored to the needs of the organization. An optional subscription to the CyberNOT Content Filter List is available.
- **AutoUpdate.** SonicWALL Internet security appliances maintain the highest level of security by automatically checking if firmware updates with protection against newly discovered hacker attacks are available. All firmware updates are free for the life of the product.
- **ICSA Certified.** SonicWALL Internet security appliances have been awarded the internationally accepted ICSA Firewall Certification.

SonicWALL Feature Chart

The following chart shows the number of LAN IP addresses (nodes) supported and other features in each SonicWALL model.

SonicWALL Model	Nodes	VPN	Anti-Virus	DMZ Port	10/100 Ethernet
SonicWALL Telecommuter	5	Included	Optional		
SonicWALL SOHO/10	10	Optional	Optional		
SonicWALL SOHO/50	50	Optional	Optional		
SonicWALL DMZ	Unlimited	Optional	Optional	Included	
SonicWALL XPRS	Unlimited	Optional	Optional	Included	Included
SonicWALL PRO	Unlimited	Included	Optional	Included	Included
SonicWALL PRO-VX	Unlimited	Included	Optional	Included	Included



SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Tel: 408-745-9600
Fax: 408-745-9300
E-mail: sales@sonicwall.com
Web: <http://www.sonicwall.com>