

Internet Security Issues and Solutions for Small Business and Education

A White Paper prepared by Sonic Systems, Inc.

Sonic Systems, Inc.
575 N. Pastoria Ave.
Sunnyvale, CA 94086
1-888-557-6642
<http://www.sonicsys.com>

Introduction

These are exciting times. A major shift is underway which changes the way the human race communicates, shares ideas and information, and educates its children and members of society. The barrier of time and place is being removed in favor of open communications and the free flow of ideas and beliefs.

Companies and organizations who do not have a Web site today are often viewed in the same light as those without a fax machine. The E-mail address has become a standard element of the traditional business card. This shift is remarkable, as only a few years ago, the Internet was a mysterious “thing” that was used only by the extremely technical and dedicated.

It is now common to turn on the television or pick up a newspaper and see a report on the Internet. Unfortunately, many of these reports now revolve around problems surrounding the Internet: hacker intrusions costing organizations hundreds of thousands of dollars and untold losses in productivity, hate groups using the Internet to distribute their propaganda, pedophiles using the Internet to prey on young children.

This paper addresses these security issues, framed in the context of the needs of small business and educational institutions.

The Internet's Explosive Growth

The Internet's dramatic and sudden shift from the domain of technical wizards and research institutions to that of the general public can be tied to several events, but none more so than the World Wide Web.

The Web removed the arcane, text-only interface from the Internet, making it graphical and user friendly. Now, extensions to this graphical, interactive communications media, such as push-technologies, streaming audio and video, online commerce, and the television set-top-box or “Network Computer”, are pushing the Internet further into the mass commercial audience.

While it is difficult to get an exact figure on the number of users connected to the Internet, there are several surveys that predict a similar trend: a huge market that is growing. Recently, Neilson Research performed a study to quantify the online community in the US:

Year	Population
1995	22,000,000
1996	37,840,000
1997	50,600,000
1998	72,600,000
1999	94,600,000
2000	116,600,000

International Data Corporation (IDC) estimates that, world-wide, there will be 233.3 million users connected to the Internet by 2001, generating \$100 billion in related sales. In another study, Matrix Information & Directory Service (<http://www.mids.org>) estimated that there were approximately 71 million users of the Internet as of January 1997. They predict that by the year 2000, this will grow to 827 million.

Businesses and organizations have taken to the Internet en-masse, a trend easily quantified by looking at the number of domain names registered. A domain name is the unique name, such as “sonicsys.com” or “microsoft.com”, that an organization uses as its Internet identity. According to Network Wizards (<http://www.nw.com>), there were over 1.3 million domains, or organizations with an Internet presence, registered by July, 1997, up 267% from the same period the previous year.

Year	Domains
1994	46,000
1995	120,000
1996	488,000
1997	1,301,000

While these numbers are staggering, all is not rosy for some members of the business community. According to The Internet Society (<http://www.isoc.org>), about half of all networks are not tied to the Internet because of the security risks. In another study, Deloitte & Touche found that 74% of CEOs consider a lack of security to be the major barrier to Internet use. These fears are not unfounded.

The Risks

Connecting a school or business to the Internet is not a task to be taken lightly. The simple fact is that the Internet is just like any other large community with both good and bad elements.

Sites offering pornographic images are rampant on the Internet. Search engines report that some of the most common Internet search keywords are “sex”, “nude”, “xxx”, and others of this ilk. While adults who desire access to these sites should be given such access when requested, there is no means to verify the age of a site’s visitor. As a famous cartoon states, “On the Internet, nobody knows you’re a dog.”

It’s not only deliberate attempts to locate offensive or inappropriate material that causes problems, innocent and well-intentioned surfing can also lead to less-than-desirable results. For example, even though commercial search engines are an indispensable aid in finding information on the Internet, all too often searches return results that are not only inappropriate, but often dangerous. Searches for “art” lead to the Louvre, as well as a place that calls itself “The House of Digital Art, Music, and Underground Culture”; searches for “religion” display sites on Christianity as well as Satanic Worship; searches for “cookbooks” can show users how to bake pastries, as well as teach them bomb-making skills.

It’s not just the content that can cause problems. Hackers attempt to break into networks to view, alter, or destroy private files. More disturbing is the fact that hackers no longer need to be skilled in attacking a network as there are “hacker’s helper” programs with point-and-click interfaces readily available to any user with an Internet connection.

These “advances” in hacking technology make it relatively easy for a dishonest or malicious individual to break into an organization’s computers. Once in, a hacker could, for example, modify accounting, medical, school records, or other critical data and then leave, with the break-in and changes going undetected until it is too late.

The risks are significant. WarRoom Research estimates that 58% of all reported computer security breaches originated from the Internet (outside the LAN), and 41% of these attacks had losses totaling over \$500,000 per attack. Another staggering figure: the US Department of Defense estimates that there have been 250,000 attacks on its systems, 64% of which resulted in unauthorized access. Only 4% of these attacks were detected.

Protecting Network Users and Resources

Fortunately, there are measures that a network manager can take to protect users from objectionable or inappropriate Internet content, and secure the LAN from Internet based theft, modification, or deletion of data.

These security measures fall into two general categories: content filter and firewall.

Content Filter

A content filter allows schools, businesses, and other organizations to set and enforce the standard of what is and what is not appropriate material. Without a content filter, an Internet connection is an all-or-nothing proposition; users have unlimited access to all resources, both appropriate and inappropriate, benign and dangerous.

Content filtering's ability to enforce community standards was one of the key reasons the courts struck down the Communications Decency Act (CDA), which would have led to federal censorship of the Internet.

Content filtering can be accomplished by varying methods: Text Screening, Proxy or "Allow Only" Lists, Web Rating Systems, and URL Blocking.

Text Screening

Text Screening, the method that most of the early filters relied on, stops Internet pages from loading when the filter encounters a word on its list. Text Screening of sites cannot be implemented without blocking non-objectionable speech. Words like "breast" will block out breast cancer sites, and "sex" will block out "Anne Sexton". Text screening is also ineffective if content does not contain any words on the block list. For example, a site which has pornographic images that do not contain any accompanying text will likely be allowed.

It is for this reason that Text Screening is typically not used in most networks.

Proxy or "Allow Only" Lists

With a Proxy or "Allow Only" list, only sites that have been screened and approved are allowed. Typically, this is done in an educational environment where a teacher will create a lesson plan that allows students to search for material only from a pre-selected list of approved sites. Aside from being labor intensive, many useful sites could be left out merely because the teachers or administrators haven't discovered them yet.

There are two methods of implementing this. First is by use of client software that only allows access to approved sites. The second is by use of a centralized proxy server that pre-loads all approved content; all client access is to the proxy server and never directly to the Internet.

With careful screening, this method has the advantage of being very close to 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.

Web Rating Systems

In the Web Rating System, the person running the Web site assigns a rating to each page on the site. For example, the Motion Picture Association rates movies in the USA as G, PG-13, R, and NC-17.

Currently, there are several rating Systems: The Ages Rating Service, Recreational Software Advisory Council (RSAC) Rating Service, and The SafeSurf Rating Service

Outside the problems associated with establishing a single rating system which is accepted by the global community of Internet content providers and users, and supported by all Web browsers, this system has two serious flaws. First, if the site's Webmaster has not rated the site or page, the Web browser is unable to enforce any restrictions, which can lead to restricting access to sites that would otherwise be acceptable, or granting access to sites that should be restricted. Second, in the event that a rating system becomes widely accepted and implemented, it is still dependent on the Webmaster's honesty when assigning a valid rating to the content.

URL Blocking

The preferred method of Internet filtering is to use “URL Blocking” or “Web Blocking” of pre-selected sites. In URL 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”, “Drug Use”, “Illegal Acts”, “Racial Intolerance” and others. An editor reviews the selections before the site is added to the filter list.

When based upon a frequently updated filter list from a reputable organization, URL Blocking is the preferred method of Content Filtering because of its ability to block 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 Microsystems Software is becoming the de facto standard for implementing URL Blocking.

Firewall

A firewall is used to protect the private network against Internet based theft, destruction, or modification of data. The National Computer Security Association (NCSA) classifies firewalls into three categories: Packet Filters, Application-Level Proxy Servers, and Stateful Inspection Firewalls.

Packet Filters

Packet filters were the first generation of firewalls and are typically implemented on routers. They examine data passing to and from a network, and can block access according to rules restricting TCP/IP port number, source or destination address, or data type. The configuration of the router’s firewall software can be difficult, confusing, and time-consuming.

Packet filters are prone to being compromised using IP spoofing, which involves altering an IP packet so the firewall thinks the packet has an internal, rather than external, source address and therefore grants it network access. Some protocols, such as FTP and DNS, can't be safely passed through packet filters because they require opening "holes" in the firewall which compromises security. Packet filters also do not have a DMZ port which is used to protect public servers, such as Web or FTP servers from certain types of attacks, such as SYN Flood, Ping-of-Death, and IP Spoofing.

Application-Level Proxy Server

Application-Level Proxy Servers are considered the second generation in network security and protect the network by examining the application layers. Unfortunately, this upper level examination leads to an unacceptable performance penalty. In addition, each application type, such as HTTP, FTP, SMTP or POP3, requires the installation and configuration of a different application proxy, making support for new applications a problem. Finally, this approach requires the user to reconfigure their network settings to support the proxy.

Stateful Inspection

The third generation in firewall technology is called Stateful Inspection, and is considered by Internet experts to be the most advanced and secure firewall technology because it examines all OSI layers to either accept or reject the requested communication. Because of this, Stateful Inspection is invisible to users on the LAN and requires no client configuration. Stateful 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 don't support UDP.

Network Security Requirements

Most Internet security solutions are designed with the requirements of the large enterprise in mind and miss the mark when addressing the needs of small-to-medium size networks: ease of use, minimum maintenance, and affordable cost. Examples of these networks include: Small Business, Education, and the ISPs who service these networks. This White Paper is written with these smaller networks in mind.

Small Business

Protecting the LAN from Internet based break-ins and attacks is a key issue for many small businesses. 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. Business owners are also installing content filters to mini-

mize vulnerability to harassment lawsuits. These lawsuits can result from employees who were subjected to a hostile work environment because co-workers were using company resources to access sites that cater to racial intolerance or pornographic material.

Most small businesses do not have the resources for a dedicated network administrator or computer expert. Instead, the small business owner or manager assumes this responsibility, making ease of installation and minimal maintenance key factors.

Education

The education market has 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. Much to their credit, educators are taking a proactive approach by installing content filtering and other security products.

Many schools 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 not maintaining computer equipment, ease of installation and minimal maintenance are often a prerequisite for the education market. A severe lack of funds for such purchases is often the norm, making affordability especially important for educators and school administrators.

Internet Service Provider (ISP)

The role of the ISP is changing from offering flat-rate connections to dial-up Web surfers to being a key business partner and system integrator. In addition to selling a connection to the Internet, be it ISDN, T1, or Frame Relay, many ISPs are providing complete "turnkey" installations where they also provide the router and other necessary hardware and software.

An ISP can be the closest thing to an MIS department that smaller businesses have. Lacking the necessary expertise in Internet security, many of these businesses have voiced concerns about implementing an Internet strategy. ISPs have found that offering security services not only overcomes one of the primary objections that small businesses have to an Internet presence, but it also increases sales and service revenues.

Network Security Products

The Internet Security market is serviced by many companies which 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 and complex applications which are run on a dedicated UNIX or Windows NT server. Some of the market leaders in this product category are CheckPoint's Firewall-1, Raptor's EagleNT, and Microsoft's Proxy Server 2.0.

CheckPoint's Firewall-1 is a Stateful Inspection firewall that runs on either an NT or UNIX server and uses Text Screening and Application Gateway Proxy Server for content filtering. The SurfWatch filter list is supported for URL Blocking, but must be purchased from SurfWatch and installed separately. The cost for Firewall-1 with a 100 user license is \$7,995.

Raptor's EagleNT is an Application Gateway Proxy Server that runs on either an NT or UNIX server. EagleNT uses WebNot for URL Blocking. The cost for EagleNT is \$6,500.

Microsoft has recently entered the Internet security market with the release of Proxy Server 2.0. Proxy Server 2.0, which lists for \$995, is an Application Gateway Proxy Server which runs on Microsoft's Windows NT. As Proxy Server 2.0 doesn't support URL Blocking, Microsoft recommends the use of an external content filter.

The prices listed for these software Internet security products are for the software only, and do not include the actual cost of the server hardware and operating system. These costs can add an additional \$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.

Software Internet security products are well suited for organizations with existing NT or UNIX

servers and the technical resources required for their extensive setup, configuration, and maintenance. Because of these requirements, they are not well suited for the smaller business and education markets.

Software Internet security 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. As new security holes on the host OS are discovered, it is incumbent upon the network administrator to install the patch that corrects the security breach. While larger organizations often have an MIS staff dedicated to maintaining the organization's network and security, smaller organizations and schools often lack this resource and the resulting security holes can render the software firewall useless.

Hardware Internet Security Products

Hardware Internet security products are dedicated firewalls, such as the Cisco PIX, or firewall software which is installed on a router, such as Ascend's Secure Access. Since they usually run on a dedicated, embedded operating system, they may not be susceptible to many of the security weaknesses inherent in the NT and UNIX operating systems.

Most of these products, such as the PIX, are high performance firewalls that are ideally suited for the extremely high throughput requirements of a large enterprise with a T3 connection to the Internet, or carrier class ISPs, such as Sprint or MCI.

Cisco's PIX is a Stateful Inspection firewall with an Application Gateway Proxy Server to allow the network manager to control the content and applications which users on the LAN are permitted to access; URL Blocking is not supported. PIX costs between \$9,000 and \$22,000, depending on the capabilities of the hardware, including CPU, RAM and disk storage, network interface and other related options.

Ascend's Secure Access is a software upgrade to the Pipeline family of ISDN and T1 routers. Like PIX, Secure Access is a Stateful Inspection firewall with an Application Gateway Proxy Server for control of Internet access. Secure Access is supported only by Ascend's low-end router line, which are not able to handle the high bandwidth requirements of the enterprise. It also does not support URL Blocking. Secure Access is available only as an option for the Ascend router line and costs between \$1,500 and \$5,500.

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 and minimal maintenance offered by the next category, Internet Security Appliances.

Internet Security Appliance

The Internet Security Appliance is a new category that offers a complete, turnkey plug-and-play solution. The appliance emphasis is on ease of use, minimal maintenance, and high performance. Much of this is accomplished by making certain assumptions about the needs of the user, and pre-configuring the firewall to best meet those needs. As a result, Internet Security Appliances are developed for a few specific markets, such as small business or education, making them inappropriate for others, such as large enterprises or carrier class ISPs. Currently, only Sonic's SonicWALL and WatchGuard's Firebox qualify as Internet Security Appliances.

WatchGuard's FireBox is essentially a Pentium class PC that is pre-installed with a hardened version of Linux (a public domain version of UNIX) and WatchGuard's firewall software pre-installed. FireBox is a Stateful Inspection firewall with an Application Gateway Proxy Server to allow the network manager to control the content and applications that users on the LAN are permitted to access. FireBox costs between \$3,495 and \$6,500, depending on the management software and related options. Support for URL Blocking using the CyberNOT filter list is a \$1000 option. Since FireBox uses a freeware version of UNIX, it could be susceptible to breaches should any new security holes be found in the Linux operating system.

The SonicWALL Internet security appliance includes four point products within a box about the size of a video cassette. SonicWALL is platform independent, easy-to-install and requires no security or networking expertise. Once installed, it runs quietly and is easily managed via Web browser with activity logs sent via E-mail. Prices for SonicWALL start at \$495 for 10 IP addresses.

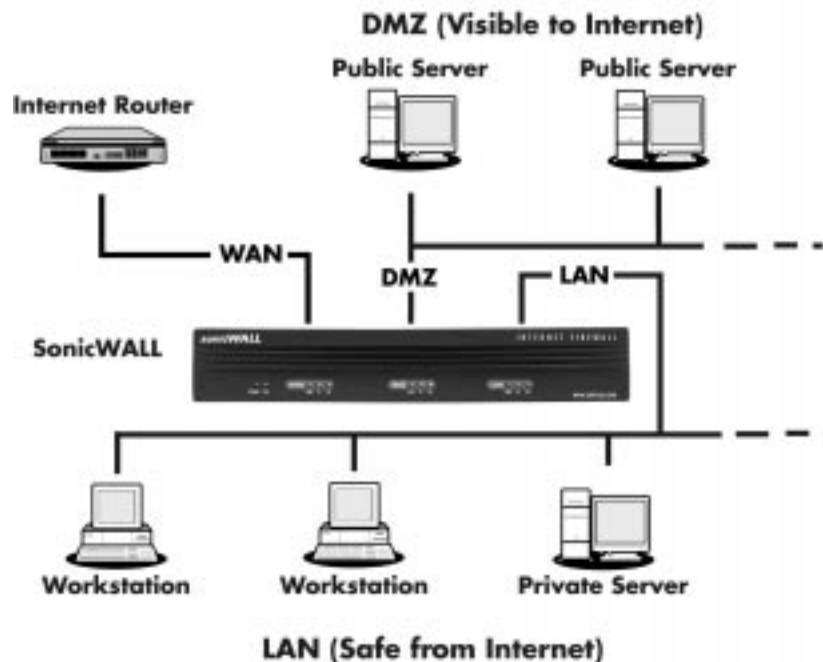
- 1 Firewall Security - stateful packet inspection firewalling; blocks denial of service (DoS) attacks, ActiveX, Java, cookies; lifetime subscription for updates of new hacking attacks via E-mail; sends alerts via E-mail when network is being attacked.
- 2 Content Filtering - allows businesses and schools to block access to adult and violent Web sites and receive weekly updates of the Content Filter List; reduces risk of lawsuits and loss of employee productivity.
- 3 Reports & Logs - performs a rolling analysis of the event log to show most accessed Web sites, top users of bandwidth, and top users of bandwidth by service; logs can be viewed or E-mailed on a regular interval.

- 4 Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) Server and Client - allows companies to use private addresses for security and easier address management; DHCP Server and Client provide centralized management of TCP/IP client configurations and ability to acquire TCP/IP settings from the ISP

SonicWALL by Sonic Systems

Schools and businesses can greatly benefit from the wealth of information that is available on the Internet. But with that benefit comes the security risk that unauthorized users may access the network to steal information. Some hackers get their thrill by crashing or corrupting PCs and servers. To help companies reduce these security risks, Sonic Systems developed SonicWALL. SonicWALL offers state-of-the-art software and hardware technology to provide a secure, easy-to-install, reliable, and affordable firewall for businesses with a few users to several hundreds of users.

To protect the private network against Internet-based theft, destruction or modification of data, SonicWALL implements stateful packet inspection, a technology similar to that used in enterprise level firewall products offered by Check Point and Cisco. SonicWALL will allow data coming from the Internet only if it's part of a session that was initiated by one of the users on the secure Local Area Network (LAN). Hackers and other unauthorized users will be stopped at SonicWALL and not allowed on the private network.



When SonicWALL is installed, the network is protected from Denial of Service Attacks, such as Ping of Death, SYN Flood, IP Spoofing, and LAND. When new hacker attacks are discovered, Sonic adds protection from them to the SonicWALL software. SonicWALL goes an extra step by automatically notifying the administrator when there is a new software release available. SonicWALL customers get free software updates.

In addition to stopping unauthorized users from accessing the secure LAN, SonicWALL allows a school or company management to determine which Internet sites or Newsgroups should be accessible. The network administrator simply selects the categories of content to block, such as pornography, intolerance or violence, and SonicWALL will automatically block the sites that fall under those categories. SonicWALL uses the highly regarded CyberNOT filter list from Microsystems Software, also used in products offered by distinguished organizations such as America Online, AT&T, IBM, Microsoft, Netscape and The Scholastic Network.

SonicWALL was designed for ease of installation and administration. Installation involves simply connecting SonicWALL between the private network and Internet router, spending a few minutes selecting the filtering options from the intuitive, Web browser based configuration screen, and the users and network are secure. No reconfiguration of any PC applications is needed.



SonicWALL's Key Features

- **Firewall Security.** SonicWALL uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. Stateful packet inspection is similar to the algorithms used by enterprise level firewall vendors such as CheckPoint and Cisco and is widely considered to be the most effective method of protecting the private LAN.
- **Hacker Attack Prevention.** SonicWALL is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack, IP Spoofing, etc. The goal of a DoS Attack is 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; SonicWALL protects the private LAN from WinNuke and many other DoS attacks.
- **Internet Content Filtering.** 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.
- **Network Address Translation (NAT).** NAT translates the IP addresses used on the private LAN to a single, valid IP address that is used on the Internet. This adds a level of security since the address of a PC on the LAN is never transmitted on the Internet. NAT also allows SonicWALL to support LANs using low cost Internet accounts, such as xDSL or cable modems, where only one IP address is provided by the ISP.
- **DHCP Server and Client.** DHCP Server provides centralized management of IP clients on the LAN by automatically configuring their IP address, gateway address, DNS address, and more. DHCP Client allows SonicWALL to acquire IP settings (such as IP address, gateway address, DNS address, etc.) from the ISP. This is ideal when the IP settings, which may change from time to time, are automatically provided by the ISP, as is the case with some xDSL and cable modem Internet accounts.

- **Network Access Rules.** Network Access Rules allow the administrator to extend SonicWALL's firewall functions. For example, a rule may be created which blocks all traffic of a certain type, such as Internet Chat (IRC), from the LAN to the Internet; another rule may be created which gives Internet users access to a server on the LAN, such as the organization's public Web server.
- **Remote Access Authentication.** Users can access Intranet resources on the private LAN by successfully logging into SonicWALL from the Internet. Authentication is established using an MD5-based encrypted security mechanism.
- **Web Browser Management.** SonicWALL is easily and securely configured and monitored through a Web-based interface. Authentication is established using an MD5-based encrypted security mechanism.
- **ICSA Certified.** After being subjected to a rigorous suite of tests intended to expose vulnerabilities to attacks and intrusions, SonicWALL has been awarded the internationally accepted ICSA Firewall Certification. Administrators can rest assured that SonicWALL has been tested and approved by the worldwide authority in independent security services.
- **Optional Enterprise Features.** In addition to the unlimited number of LAN clients supported, SonicWALL Plus and SonicWALL Plus DMZ have features that make them ideally suited for use in larger, enterprise networks. SonicWALL/10 and SonicWALL/50 may be upgraded to support the following Optional Enterprise Features.
 - **Custom Network Access Rules.** The administrator has fine-grain control over network traffic. For example, Custom Network Access Rules may be created which allow access to a Web server to everyone but competitors, or restrict use of certain protocols, such as Telnet, to authorized users on the LAN.
 - **Web Proxy Relay.** If use of a caching proxy server is required, SonicWALL and SonicWALL Plus DMZ may be used to transparently redirect all Web requests to the proxy without client configuration.
 - **Intranet Support.** SonicWALL and SonicWALL Plus DMZ allows Intranet firewalling by allowing the administrator to restrict access to certain resources on the LAN. For example, protection may be required for a company's accounting department against unauthorized access by other users on the same network.
 - **Static Routes.** SonicWALL and SonicWALL Plus DMZ may be configured to support large networks with internal routers.

SonicWALL Feature Chart

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

SonicWALL Version	# of Nodes	Enterprise Features	DMZ Port
SonicWALL/10	10		
SonicWALL/50	50		
SonicWALL Plus	Unlimited	✓	
SonicWALL Plus DMZ	Unlimited	✓	✓

© 1998 Sonic Systems, Inc. All Rights Reserved. All trademarks are the property of their respective holders.