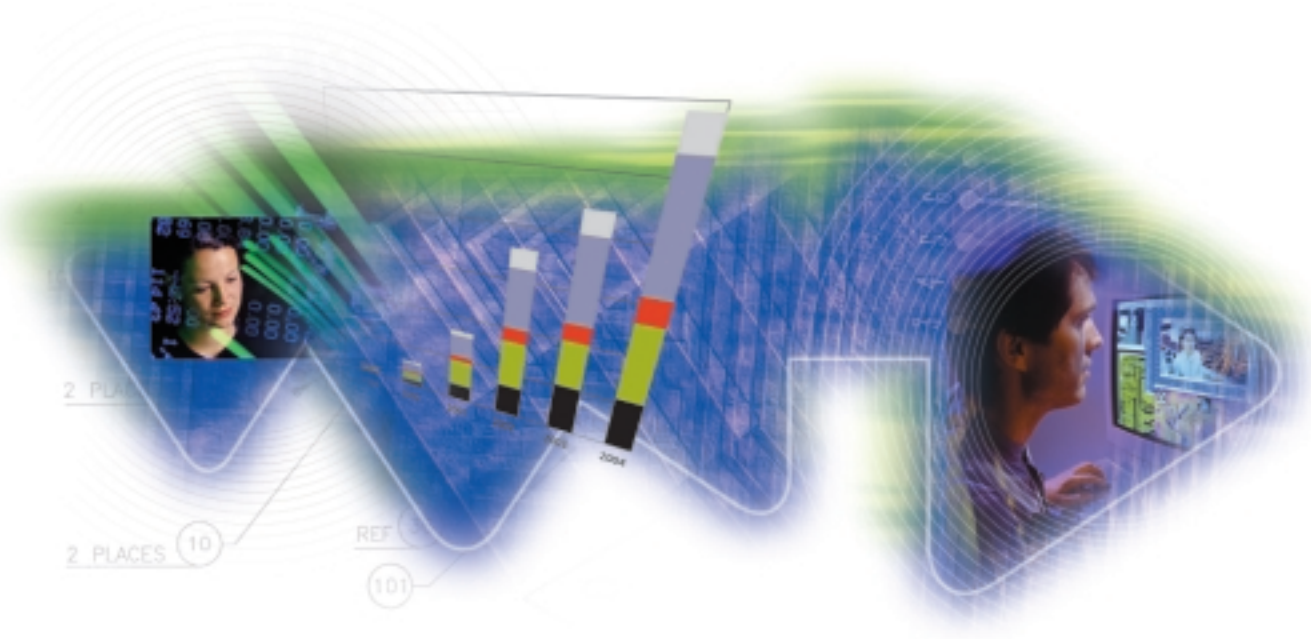
Security in DSL Networks

Issues and Solutions for Small-to-Medium Sized Enterprises

TECHNICAL PAPER



ALCATEL

ARCHITECTS OF AN INTERNET WORLD

Security in DSL Networks

The High Cost of Internet Security Breaches

According to the Computer Security Institute's 2001 Computer Crime and Security Survey, 85 percent of respondents detected computer security breaches within the last 12 months. Sixty-four percent of respondents acknowledged financial losses due to computer breaches. The 35 percent of respondents who were willing and/or able to quantify their financial losses reported losses exceeding U.S. $375 M. And this number represents an increase of more than 300 percent over the average annual losses reported from 1997 to 1999.

Even more alarming than the preceding figures is the fact that 70 percent of respondents cited their Internet connection as a frequent point of attack — up 11 percent from just one year earlier.

Cyberattacks are on the rise, and the cost is staggering:

- Code Red: 1 million computers affected; cleanup costs of U.S. $1.1 B; lost productivity costs of U.S. $1.5 B.
- Love Bug: 50 variants; 40 million computers affected; cleanup and lost productivity costs of U.S. $8.7 B.
- Nimda: Cost still to be determined.

These statistics raise a number of questions. Who is most at risk? What can you do to keep from becoming a statistic? And how can your service provider help?

Who is Most at Risk

Small-to-medium sized enterprises (SMEs) with broadband networks are intrinsically more vulnerable to outside attacks than are narrowband dial networks. Due to the always-on nature and larger bandwidth of a broadband network, hackers have more time and bandwidth available to hack into your system. The intruder may block your Internet connection, corrupt your sensitive data or even use your digital subscriber line (DSL) connection to attack public and well known sites such as large Internet service providers (ISPs), security agencies or government departments.

Typical Security Risks

Typical risks in a business environment fall into three categories:

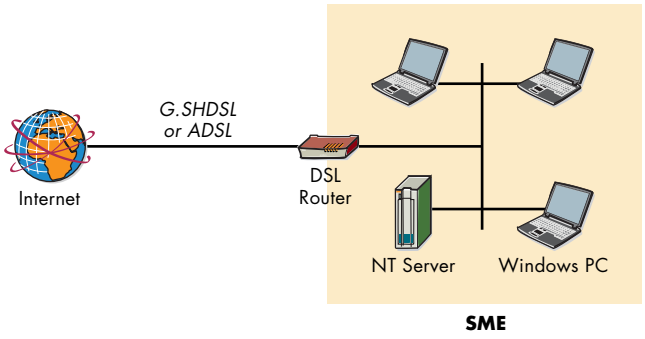
- Confidentiality: Information should be available only to those with appropriate access.
- Integrity: Information should be modified only by people who are authorized to do so.
- Availability: Information should be accessible only to those who need it.

As shown above, these risks translate into huge financial risks, especially when e-business is being conducted at the enterprise.

The Good News for SMEs

Despite the pervasive security threats, and the financial risks they bring, there is good news. SMEs usually have only one access to the Internet, via asymmetric DSL (ADSL) or symmetric DSL (SDSL), connected to a DSL router (see Figure 1). SMEs generally have a limited set of applications that need to be supported. Unlike large corporations, SMEs don't have to control multiple sites, support complex applications or have various interfaces to the Internet. All of these factors make it simpler to implement network security than it would be for a large enterprise.

Figure 1: Common SME Internet Connection



Helping SMEs to implement security is the purpose of this paper. It explains common Internet security threats and recommends ways that SMEs can effectively block the most common attacks and how the service provider can help. The paper also discusses the impact of network address translation (NAT), firewalls and virtual private networks (VPNs) on security.

Common Internet Security Threats

Common Internet security threats fall into six main areas:

- Back door programs and Trojan horses
- E-mail attacks
- Internet site-related threats
- Denial-of-service attacks
- Packet sniffing
- Microsoft Windows-related attacks

Back Door Programs and Trojan Horses

Back door programs

On Windows computers, intruders often use three tools to gain remote access to your computer: BackOrifice, Netbus and SubSeven. Once installed, these back door programs (also called remote administration programs) allow other people to access and control your computer without your knowledge. Intruders can change your system configurations or can infect your computer with a computer virus.

Trojan horses

A Trojan horse is a software program that creates and installs a version of a system utility that copies information or hides it. Intruders often use Trojan horses to trick users into installing back door programs.

E-Mail Attacks

E-mail-borne viruses

Viruses and other types of malicious code are often spread as attachments to e-mail messages. Often, the viruses or malicious code are distributed in amusing or enticing programs.

Hidden file extensions

Windows operating systems contain an option to "Hide file extensions for known file types". By default, the option is enabled. Multiple e-mail-borne viruses are known to exploit hidden file extensions.

The first major e-mail attack that took advantage of a hidden file extension was the VBS/LoveLetter worm. (A worm is a self-copying virus that spreads very fast, for example, to all correspondents in your address book). The VBS/LoveLetter worm contained an e-mail attachment named LOVE-LETTER-FOR-YOU.TXT.vbs. Other malicious programs have since incorporated similar naming schemes.

Internet Site-Related Threats

Mobile code

There have been reports of problems with mobile code; code that is executed by your web browser. Examples of programming languages that produce mobile code include Java, JavaScript and ActiveX. Although the code is generally useful, it can be used by intruders to gather information, such as which web sites you visit, or to run malicious code on your computer.

Many e-mail programs use the same code as web browsers to display HTML text. Therefore, vulnerabilities that affect Java, JavaScript and ActiveX are often applicable to e-mail as well as to web pages.

Cross-site scripting

In cross-site scripting, a script is attached to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

Chat clients

Internet chat applications, such as instant messaging applications and Internet relay chat (IRC) networks, provide a mechanism for information to be transmitted bidirectionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs and, in many cases, files of any type. Because many chat clients allow for the exchange of executable code, they present risks similar to those of e-mail clients.

Denial-of-Service Attacks

Denial of your service

A denial-of-service (DoS) attack causes your computer to crash or to become so busy processing data that you are unable to use the computer. In addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a DoS attack on another system.

Being an intermediary for another attack

Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DDoS) tools are used. The intruders install an agent (frequently through a Trojan horse program) that runs on the compromised computer, awaiting further instructions. Once a number of agents are running on different computers, a single

handler instructs all the agents to launch a DoS attack on another system. The end target of the attack is not your computer, but someone else's. Your computer is simply a convenient tool.

Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords and proprietary information that travel over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. And installing a packet sniffer does not necessarily require administrator-level access.

Cable modem users have a higher risk of exposure to packet sniffers than do DSL users because entire neighbourhoods of cable modem users are effectively part of the same local area network (LAN). A packet sniffer installed on any cable modem user's computer in a neighbourhood may be able to capture data transmitted by any other cable modem in the same neighbourhood.

Packet sniffing in DSL networks requires access to service provider facilities, so the danger is not as great as for cable modem users.

Microsoft Windows-related attacks

Microsoft Windows has a standard mechanism to share a folder with everybody having access to the computer, which is the case when being connected to the Internet. The sharing can be restricted by username. The sharing can also be exploited by intruders, via search programs looking for shared folders, to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, it is also a threat to other sites on the Internet.

The greater immediate risk to the Internet community is the large number of computers with unprotected Windows networking shares attached to the Internet, combined with distributed attack tools such as DDoS tools as described above. Another threat is malicious and destructive code, such as viruses or worms, which takes advantage of unprotected Windows networking shares to propagate.

Security Recommendations in a SME Network Environment

Service Provider-Related Recommendations

Use anti-virus software

Be sure to keep your antivirus software up to date. Many antivirus packages support automatic updates of virus definitions. We recommend that you use these automatic updates when they are available.

Use a firewall

We strongly recommend that you use a firewall product. Many DSL modems now include firewall capabilities. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (both software- and hardware-based) can provide some degree of protection against these attacks. (The firewall functions are explained in more detail later in this paper.)

Remember, however, that no firewall can detect or stop all attacks, so it's not sufficient to install a firewall and then ignore all other security measures.

Common Sense Recommendations for Users

Don't open unknown e-mail attachments

Before opening any e-mail attachment, be sure you know the source of the attachment. But this is not the only step, it's just the first step. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address.

Unless an e-mail includes a message regarding an attachment that you specifically requested, check with the sender before opening any attachments.

Hint: Malicious code is often distributed in amusing or enticing programs, such as the recent My Party virus.

Don't run programs of unknown origin

Never run a program unless you know it to be authored by a person or company you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing — they might contain a Trojan horse program.

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Make regular backups of critical data

Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks away from the computer.

Make a boot disk in case your computer is damaged or compromised

To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk, to help when recovering a computer after such an event has occurred. Remember, however, that you must create this disk before you have a security breach. The standard installation of anti-virus programs will create a boot disk as part of the setup.

Software-Related Recommendations

Disable hidden filename extensions

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but you can disable it in order to have file extensions displayed.

After disabling this option, there are still some file extensions that, by default, will continue to remain hidden. There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The NeverShowExt registry value is used to hide the extensions of basic Windows file types. For example, the .LNK extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

If possible, disable Java, Javascript, and ActiveX

Be aware of the risks involved in using mobile code programming languages such as Java, JavaScript and ActiveX. The easiest way to avoid the risk is to disable all scripting languages. However, be aware that doing so will limit the interaction you can have with some web sites. Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

Disable scripting features in e-mail programs

Because many e-mail programs use the same code as web browsers to display HTML text, vulnerabilities that affect Java, JavaScript and ActiveX are often applicable to e-mail as well as to web pages. Therefore, in addition to disabling scripting features in web browsers, we recommend that you also disable these features in your e-mail programs.

The Impact of NAT on Security

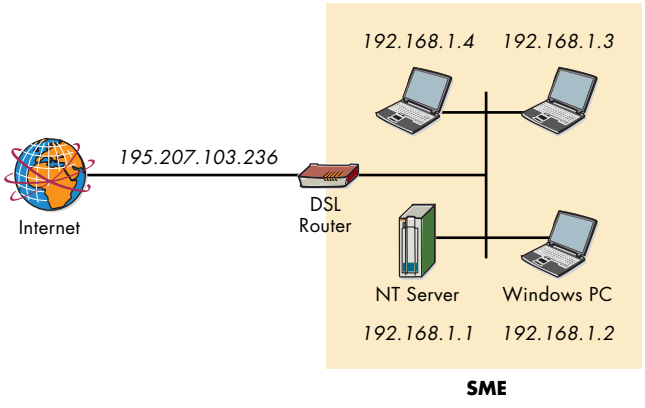
Network address translation (NAT) is a process that translates the internal address from the SME LAN to an outside public address. It is a common misconception that NAT is a security feature. Although NAT is common on DSL routers, it is not intended for security purposes.

While not a security feature, NAT does shield the SME network from the Internet. Because NAT translates the internal network address to a public address, hackers will have more difficulty accessing your network because they don't have your internal address.

As shown in Figure 2, the private addresses of the SME (for example, 192.168.x.y) are translated to one public IP address (195.207.103.236). This preserves the number of public addresses needed in the Internet and shields private addressing from the Internet.

All hosts in the SME network share the one public IP address for their public services such as e-mail and web browsing.

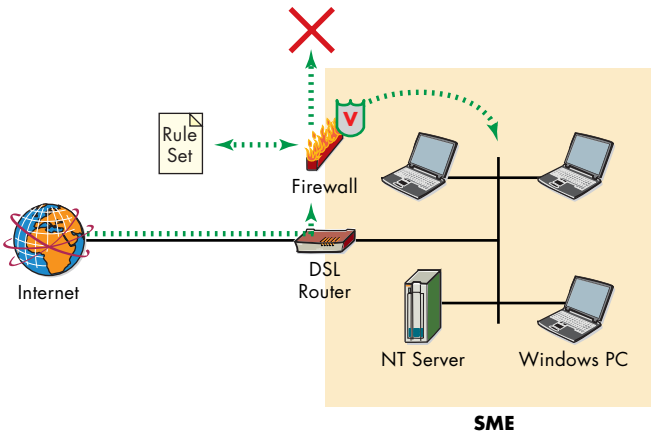
▼ **Figure 2: Network Address Translation and SME Internet Security**



The Impact of Firewalls on Security

A firewall provides a gateway function that screens all incoming traffic according to a predefined set of rules. As shown in Figure 3, traffic can be dropped or sent to the internal network. In many cases, the firewall function is part of the DSL router.

▼ **Figure 3: A Firewall for a SME**



Although firewalls are common and recommended security measures, they can instill a false sense of security. The effectiveness of a firewall relies heavily on the rules it has been programmed with.

The International Computer Security Association (ICSA) classifies firewalls into three categories:

- Packet filter firewalls
- Application-level proxy servers
- Stateful inspection firewalls

Packet Filter Firewalls

A packet filter firewall is a processing function that inspects each incoming packet and checks its validity according to a number of predefined rules. For each packet, the firewall can decide, one packet at a time, whether to drop or to pass the packet. If the packet is dropped, the firewall will verify whether an alarm message needs to be sent.

Of course, a firewall is only efficient if the rule set (called policies) is defined in the correct way. Therefore, we recommend that business customers implement a predefined rule set. This predefined rule set may already be programmed in the firewall. If not, you can obtain the rule set from your service provider.

Application-Level Proxy Servers

Application-level proxy servers intervene when an application, such as a web browser or an e-mail program, requests information outside the private network. The applications in the Internet communicate only with the application proxy and not directly with the host. The proxy server forwards all communication to its final destination within the private network.

Application proxy servers are difficult to configure and are usually deployed by large corporations.

Stateful Inspection Firewalls

Stateful inspection firewalls are comparable to packet filter firewalls but have the unique feature of remembering the different connections. This memory enables you to set a policy that allows incoming packets only for applications that have been sending outgoing requests. This way, incoming traffic is only possible if someone from within the network has requested it.

A stateful inspection firewall is also useful if long packets will be entering the network in fragments. A packet filter will examine only the first packet, which contains the inspection information, and will allow the remaining packets to pass through. A stateful inspection firewall will examine all the fragmented packets.

The Impact of VPNs on Security

A virtual private network (VPN) offers the appearance, functionality and usefulness of a dedicated private network, over a shared network (often one owned by a common carrier). A VPN offers the features of a private network at a price savings. A VPN could be used by a car dealer, to order parts from a car parts supplier, or by bank branches, to connect to a main database.

Because the VPN is an intrinsic part of the telecom infrastructure of SMEs, it is vital that the VPN connection be secure. There are two main components in the security of the VPN connection:

- Authentication: The car parts supplier can verify that the dealer is genuine by password protection or stronger security services.
- Encryption: All data sent over the Internet can only be interpreted if the receiver has the decryption key.

Authentication

The first step in accessing a corporate VPN is authentication of the partner.

In its most basic form, authentication consists of a username and password for an individual to gain access to services or resources.

This authentication process can be enhanced by the use of token cards, which have numeric passwords that change automatically at short, set intervals. For example, the password may change once every minute. During the interval that a password is valid, it can be used to access remote networks. Because the passwords change so often, it is very difficult for unauthorized persons to guess or obtain a valid password.

Encryption

A second issue with VPNs is the readability of the traffic sent over the Internet. To avoid information being read, it can be encrypted. IPsec is a collection of security measures that enable setup of encrypted tunnels over the public Internet. These tunnels enable all distributed applications, including remote logon, to be secured.

For example, a partner wants to access a supplier's automated ordering system. The partner uses IPSec protocols to protect the access. These protocols can operate in networking devices, such as a DSL router or firewall that connects each LAN to the outside world, or they can operate directly on the workstation or server.

Conclusions

There is no such thing as bullet-proof security, and the main security threat comes from within the enterprise. However, DSL connections can be better secured by following the guidelines described in this paper. Service providers need to make sure the right tools are in place to provide customers with the correct level of security, and customers should follow common-sense security measures.

Firewalls and virus scanning are the security foundation but security requirements extend well beyond that. Security-conscious enterprises may decide to encrypt data traffic and to impose stringent security policies.

Service providers can play an important role in the security environment of the SME. They can provide regular updates to the virus-scanning software, update the policies of the firewall, and provide the necessary tools for VPN infrastructures. And, by working together, SMEs and their service providers can help to better protect the enterprise from cyberspace attacks.

www.alcatel.com

3CL 00469 0235 TQZCA Ed.01 11899

ALCATEL

ARCHITECTS OF AN INTERNET WORLD