3com

WHITE PAPER

Network Security: A Simple Guide to Firewalls

Network Security

A Simple Guide to Firewalls

Loss of irreplaceable data is a very real threat for any business owner whose network connects to the outside world. Remote access for employees and connection to the Internet may improve communication in ways you've hardly imagined. Access to the Internet can open the world to communicating with customers and vendors, and is an immense source of information. But these same opportunities open a local area network (LAN) to the possibility of attack by thieves and vandals and abuse by your own employees.

Figuring out the right amount of security for your network takes some consideration. The first thing to consider is what your data is worth. A quick answer is, "Maybe more than you think." When you consider the value of your data, remember risks such as legal liability and loss of competitive edge, or the effect of lost production if your network is compromised. Many analysts say very bluntly, "If you are on the Internet, you need a firewall."

The benefits of connecting to the Internet are clear. This paper discusses the risks you face when you connect to the Internet, describes the types of attacks that can occur, and offers an overview of firewall technology, which can protect your network from hackers. Specifically, the paper discusses the implementation of a firewall and what you should consider in choosing the type of firewall you require.

CONTENTS

Why a Firewall—Am I Really at Risk?

Anyone can become a hacker. It doesn't require a technological whiz kid to wreak havoc on your network. A wide range of tools and utilities can be easily downloaded from the Internet; and with their help, almost anyone can become a competent hacker at the touch of a button.

There are experts who say, "If you are connected to the Internet, you need a firewall." The decision may not be more complicated than that. However, you'll probably consider a combination of factors. Start with the basic questions you'd ask about any other security system.

Do I Have Anything Worth Protecting?

Be sure to consider:

- Confidential client, supplier, or employee information that might expose you to a lawsuit if you allow someone else to capture it
- Intellectual property that gives you a competitive edge in the market
- Critical business records that would have to be recovered and/or recreated

It isn't always safe to assume that no one else wants your data. Some hackers operate on a nonprofit basis. They may capture data or vandalize your system just because they can.

Aren't My Valuables Already Adequately Protected?

The truth is that if you have valuable electronic property, it may not be as safe as you would like to think it is. You can do a lot to protect your system if you:

- Back up your information every night
- Set up unshared folders behind tough passwords and password rules
- Use your access router or browser to filter incoming traffic from all but trusted sites

Unfortunately, hackers have many sophisticated software tools at their disposal. Given enough time and determination, a skilled hacker may get through the standard safeguards.

3DES Data Encryption Standard (168-bit)

DMZ demilitarized zone

DoS denial of service

FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol

ICSA International Computer Security Association

LAN local area network

NAT Network Address Translation

POP3 Post Office Protocol, Version 3

SMTP Simple Mail Transfer Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

VPN virtual private network

WAN wide area network

If he does, he can run software programs to break your passwords. If you have valuable data on your network and the network is exposed to outside computers, chances are very good you need a firewall.

What Is a Firewall?

A firewall is a system that enforces an access control policy between two networks—such as your private LAN and the unsafe, public Internet. The firewall determines which inside services can be accessed from the outside, and vice versa. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one to block traffic, and one to permit traffic. A firewall is more than the locked front door to your network—it's your security guard as well.

Firewalls are also important because they provide a single "choke point" where security and audits can be imposed. A firewall can provide a network administrator with data about what kinds and amount of traffic passed through it, how many attempts were made to break into it, and so on. Like a closed circuit security TV system, your firewall not only prevents access, but also monitors who's been sniffing around, and assists in identifying those who attempt to breach your security.

Basic Purpose of a Firewall

Basically, a firewall does three things to protect your network:

- It blocks incoming data that might contain a hacker attack.
- It hides information about the network by making it seem that all outgoing traffic originates from the firewall rather than the network. This is called Network Address Translation (NAT).
- It screens outgoing traffic to limit Internet use and/or access to remote sites.

Screening Levels

A firewall can screen both incoming and outgoing traffic. Because incoming traffic poses a greater threat to the network, it's usually screened more closely than outgoing traffic.

When you are looking at firewall hardware or software products, you'll probably hear about three types of screening that firewalls perform:

- Screening that blocks any incoming data not specifically ordered by a user on the network
- Screening by the address of the sender
- Screening by the contents of the communication

Think of screening levels as a process of elimination. The firewall first determines whether the incoming transmission is something requested by a user on the network, rejecting anything else. Anything that is allowed in is then examined more closely. The firewall checks the sender's computer address to ensure that it is a trusted site. It also checks the contents of the transmission.

Types of Attack

Before determining exactly what type of firewall you need, you must first understand the nature of security threats that exist. The Internet is one large community, and as in any community it has both good and bad elements. The bad elements range from incompetent outsiders who do damage unintentionally, to the proficient, malicious hackers who mount deliberate assaults on companies using the Internet as their weapon of choice.

Generally there are three types of attack that could potentially affect your business:

- *Information theft*: Stealing company confidential information, such as employee records, customer records, or company intellectual property

- *Information sabotage:* Changing information in an attempt to damage an individual or company's reputation, such as changing employee medical or educational records or uploading derogatory content onto your Web site

- *Denial of service (DoS):* Bringing down your company's network or servers so that legitimate users cannot access services, or so that normal company operations such as production are impeded

Attempts to Gain Access

A hacker may attempt to gain access for sport or greed. An attempt to gain access usually starts with gathering information about the network. Later attacks use that information to achieve the real purpose—to steal or destroy data.

A hacker may use a port scanner—a piece of software that can map a network. It is then possible to find out how the network is structured and what software is running on it.

Once the hacker has a picture of the network, he can exploit known software weaknesses and use hacking tools to wreak havoc. It is even possible to get into the administrator's files and wipe the drives, although a good password will usually foil that effort.

Fortunately, a good firewall is immune to port scanning. As new port scanners are developed to get around this immunity, firewall vendors produce patches to maintain the immunity.

Denial-of-Service Attacks

DoS attacks are purely malicious. They don't result in any gain for the hacker other than the "joy" of rendering the network, or parts of it, unavailable for legitimate use. DoS attacks overload a system so that it isn't available—they deny your ability to use your network service. To overload the system, the hacker sends very large packets of data or programs that require the system to respond continuously to a bogus command.

To launch a DoS attack, a hacker must know the IP address of the target machine. A good firewall doesn't reveal its own IP address or the IP addresses on the LAN. The hacker may think he has contacted the network when he has only contacted the firewall—and he can't lock up the network from there. Furthermore, when a hacker launches an attack, some firewalls can identify the incoming data as an attack, reject the data, alert the system administrator, and track the data back to the sender, who can then be apprehended.

Firewall Technologies

Firewalls come in all shapes, sizes, and prices. Choosing the correct one depends mainly on your business requirements and the size of your network. This section discusses the different types of firewall technologies and formats available.

Above all, no matter what type of firewall you choose or its functionality, you must ensure that it is secure and that a trusted third party, such as the International Computer Security Association (ICSA), has certified it. The ICSA classifies firewalls into three categories: packet filter firewalls, application-level proxy servers, and stateful packet inspection firewalls.

Packet Filter Firewall

Every computer on a network has an address commonly referred to as an IP

address. A packet filter firewall checks the address of incoming traffic and turns away anything that doesn't match the list of trusted addresses. The packet filter firewall uses rules to deny access according to information located in each packet such as: the TCP/IP port number, source/destination IP address, or data type. Restrictions can be as tight or as loose as you want.

An ordinary router on a network may be able to screen traffic by address, but hackers have a little trick called *source IP spoofing* that makes data appear to come from a trusted source, even from your own network. Unfortunately, packet filter firewalls are prone to IP spoofing and are also arduous and confusing to configure. And any mistake in configuration could potentially leave you wide open to attack.

Application-Level Proxy Server

An application-level proxy server examines the application used for each individual IP packet to verify its authenticity. Traffic from each application—such as HTTP for Web, FTP for file transfers, and SMTP/POP3 for e-mail—typically requires the installation and configuration of a different application proxy. Proxy servers often require administrators to reconfigure their network settings and applications (i.e., Web browsers) to support the proxy, and this can be a labor-intensive process.

Stateful Packet Inspection Firewall

This is the latest generation in firewall technology. Stateful packet inspection is considered by Internet experts to be the most advanced and secure firewall technology because it examines all parts of the IP packet to determine whether to accept or reject the requested communication.

The firewall keeps track of all requests for information that originate from your network. Then it scans each incoming communication to see if it was requested, and rejects anything that wasn't. Requested data proceeds to the next level of screening. The screening software determines the state of each packet of data, hence the term *stateful packet inspection*.

Additional Firewall Features and Functionality

In addition to the security capability of a firewall, a wide range of additional features and functionalities are being integrated into standard firewall products. These include support for public Web and e-mail servers, normally referred to as a demilitarized zone (DMZ), content filtering, virtual private networking (VPN) encryption support, and antivirus support.

Demilitarized Zone Firewalls

A firewall that provides DMZ protection is effective for companies that invite customers to contact their network from any external source, through the Internet or any other route—for example, a company that hosts a Web site or sells its products or services over the Internet.

The deciding factors for a DMZ firewall would be the number of outsiders or external users who access information on the network and how often they access it.

A DMZ firewall creates a protected ("demilitarized") information area on the network. Outsiders can get to the protected area but can't get to the rest of the network. This allows outside users to get to the information you want them to have and prevents them from getting to the information you don't want them to have.

Content Filtering

A Web site filter or content filter extends the firewall's capability to block access to certain Web sites. You can use this add-on to ensure that employees do not access particular content, such as pornography or

racially intolerant material. With this functionality you can define categories of unwelcome material and obtain a service that lists thousands of Web sites that include such material. You can then choose whether to totally block those sites, or to allow access but log it. Such a service should automatically update its list of banned Web sites on a regular basis.

Virtual Private Networks

A VPN is a private data network that makes use of the public network infrastructure, that is, the Internet. The idea of the VPN is to give the company the same capabilities as a private leased line but at much lower cost. A VPN provides secure sharing of public resources for data by using encryption techniques to ensure that only authorized users can view or "tunnel" into a company's private network.

Companies today are looking at VPNs as a cost-effective means of securely connecting branch offices, remote workers, and privileged partners/customers to their private LANs. A growing range of firewalls now have VPN encryption capability built in or offer it as an optional extra. This offers companies a simple, cost-effective alternative to traditional private leased lines or modem remote access.

When implementing a VPN, you need to ensure that all devices support the same level of encryption and that it is sufficiently secure. To date, 168-bit Data Encryption Standard (3DES) is the strongest level of encryption publicly available and is deemed unbreakable by security experts. One thing to bear in mind is that the stronger the encryption level, the more processing power is required by the firewall. A small number of firewall vendors are now offering VPN hardware acceleration to improve VPN traffic performance.

Antivirus Protection

Everyone should be concerned about the threat of viruses, which are among the most pernicious forms of computer hacking. Users can quickly damage entire networks by unknowingly downloading and launching dangerous computer viruses. Companies have lost enormous amounts of money due to resulting lost productivity and network repair costs.

Firewalls are not designed to remove or clean viruses, but they can assist with virus detection, which is an important part of an overall virus protection plan.

It is important to note that a firewall can only protect the network from the wide area device to which it is attached. A remote access server or a PC with a modem could provide a back door into your network that circumvents the firewall. The same is true if an employee inserts a virus-infected floppy disk into a PC. The ultimate place for antivirus software is on every user's PC; however, a firewall can assist in virus detection by requiring that every user's PC have the latest antivirus software running and enabled before the firewall permits that user to access the Internet or download e-mail.

Choosing a Firewall

Firewall functions can be implemented as software or as an addition to your router/gateway. Alternatively, dedicated firewall appliances are increasing in popularity, mainly due to their ease of use, performance improvements, and lower cost.

Router/Firmware-Based Firewalls

Certain routers provide limited firewall capabilities. These can be augmented further with additional software/firmware options. However, great care must be taken not to overburden your router by running additional services like a firewall. Enhanced firewall-related functionality such as VPN, DMZ, content filtering, or antivirus protection may not be available or may be expensive to implement.

Software-Based Firewalls

Software-based firewalls are typically sophisticated, complex applications that run on a dedicated UNIX or Windows NT server. These products become expensive when you account for the costs associated with the software, server operating system, server hardware, and continual maintenance required to support their implementation.

It is essential that system administrators constantly monitor and install the latest operating system and security patches as soon as they become available. Without these patches to cover newly discovered security holes, the software firewall can be rendered useless.

Dedicated Firewall Appliances

Most firewall appliances are dedicated, hardware-based systems. Because these appliances run on an embedded operating system specifically tailored for firewall use, they are less susceptible to many of the security weaknesses inherent in Windows NT and UNIX operating systems. These high-performance firewalls are designed to satisfy the extremely high throughput requirements or the processor-intensive requirements of stateful packet inspection firewalls.

Because there is no need to harden the operating system, firewall appliances are usually easier to install and configure than software firewall products, and can potentially offer plug-and-play installation, minimal maintenance, and a very complete solution. They also prove to be extremely cost-effective when compared to other firewall implementations.

Designing a Firewall into Your Network

Once you have familiarized yourself with all of the different firewalls on the market, the next step is to define your firewall policy. For example, will the firewall explicitly deny all services except those critical to the mission of connecting to the Internet? Or is it intended to provide a metered and audited method of "queuing" access in a nonthreatening manner? Decisions like these are less about engineering than politics.

The next decision is what level of monitoring, redundancy, and control you want. This involves juggling needs analysis with risk assessment, and then sorting through the often conflicting requirements in order to determine what to implement.

Where firewalls are concerned, the emphasis should be on security rather than connectivity. You should consider blocking everything by default, and only allowing the services you need on a case-by-case basis. If you block all but a specific set of services, you make your job much easier.

Conclusion

Security breaches are very real and very dangerous. Every company now recognizes how easily it can become the victim of deliberate or random attacks, and how much damage these attacks can cause. The good news is that 3Com Corporation is just as aware of the threats, and is developing better and stronger security solutions. Small and midsize companies and remote offices in particular can take advantage of new 3Com firewall solutions that are less costly and complicated to administer than traditional firewalls.

While firewalls are only one component of an overall security system, they are a vital component, and companies must invest the time required to evaluate the best system for their needs—and then deploy it as quickly as possible. Security breaches are an ever-present danger, and there's no time like the present to protect your company's valuable data.

3Com Corporation, Corporate Headquarters, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

503090-001 9/00