Feature Article: Walls of Fire

This Week's A+ Newsletter...

With security at the forefront of IT these days, you hear a lot about firewalls. A firewall acts as a barrier between an internal local area network (LAN) and the "outside world" – the LAN's connection to the Internet or another internetwork. Another type of intermediary is a proxy server. It's important for IT professionals to understand the difference between the two.

In this week's feature article, we will discuss how firewalls and proxies differ, what a firewall does and how it accomplishes its purpose(s), why firewalls are important in our Internet-connected world, and some of the ways firewalls can be implemented.

What's a Proxy?

First, let's distinguish between proxy servers and full-fledged firewalls. A proxy is a stand-in; it sits between the internal and external networks and acts as a go-between for communications that are exchanged between the two. The word "proxy" means "one who is authorized to act on behalf of another." You've probably heard of proxy weddings, whereby someone stands in for one of the parties (bride or groom) so a wedding ceremony can legally be performed without both being physically present. Proxy servers are so named because, like the hapless stand-in who says "I do" when it's really someone else who does, they act as go-betweens to allow something to take place (in this case, network communications) between systems that must remain separate.

Proxy servers provide a measure of security to the internal network. The proxy usually uses Network Address Translation (NAT) to allow all the internal computers to connect to the Internet using only a single public IP address (that of the proxy server itself). The other computers' internal IP addresses are not visible over the Internet; to outsiders it looks as if the proxy server is the only machine that is there. Proxies can also provide performance enhancement, by caching objects that are retrieved frequently from the 'Net and making them available locally to the internal network. Just as a web browser's cache speeds up access to web pages you visit often by storing copies of them on your local disk, a proxy performs the same function for the entire LAN.

What's a Firewall?

Like the proxy server, a firewall is a "middle man" that sets between the internal and external networks. However, it goes further than the proxy in terms of controlling what goes into and out of the LAN. A product can be both a proxy and a firewall; Microsoft's ISA Server is a good example of this. While its predecessor, Microsoft Proxy Server, was not considered to be a full-fledged firewall, ISA is.

The job of a firewall is to use filtering to prevent unauthorized data from entering the network and restricting the data that can be sent out. Just as a physical firewall in a building or vehicle is designed to stop a fire from spreading from one area to another, a network firewall is designed to keep data in or out of a network.

Firewalls can be hardware devices, which are dedicated single-purpose computers that run proprietary software, or they can be software-only packages that are installed on a regular PC running on top of on operating system like Windows or UNIX. Hardware firewalls tend to be more expensive (since you're buying both hardware and software) but also usually offer better performance. Firewalls use NAT or router software to get data to the appropriate internal computer after checking it to ensure that the filtering rules allow it to go through.

Firewall Filtering

Firewalls can filter data at different levels (different layers of the OSI networking model). The most common filtering methods are:

- Packet filtering, which works primarily at the network layer
- Circuit filtering, which works at the transport layer
- Application filtering, which works at the application layer

Packet filters examine the information in the IP packet headers of messages and make the decision as to whether the data is allowed in (or out) based on that information. Thus packet filtering allows you to designate specific IP addresses (or host or domain names) that will be specifically blocked or specifically allowed. Filters can also process information at the transport layer (TCP and UDP port numbers). Specific ports can be blocked or left open. Because particular services use specific ports (for example, POP 3 incoming email uses port 110), this allows you to prevent specific types of data from entering the network (in this case, incoming POP3 email). There are two types of filtering, static and dynamic. With dynamic filtering, the necessary ports are opened up only when a communication is actually taking place, rather than staying open all the time. As soon as the communication ends, the port is closed. Circuit filtering lets you examine sessions instead of packets. Circuit filters don't restrict access based on user information, but control access based on TCP data streams or UDP datagrams.

Packet and circuit filtering don't make access decisions based on the content of the data itself. If you want to do that, you need to use application filtering. Application filtering can also let you accept or reject data based on user information. You could restrict a particular user from using a particular network service (such as FTP) or even more specifically, you could allow a particular user to upload via FTP, but block him/her from using FTP to download.

There are a couple of ways filtering can be configured. In the first model, by default all filters are open and you specifically block those addresses, ports or content that you don't want to come through. In the second model, all filters are closed by default (nothing can come through) and you must specifically allow the addresses, ports or content types that you want to come through. The second model is more secure, but may be impractical at the application level. Different models can be used at different levels.

Why You Need a Firewall

Firewalls can prevent many common hack attacks, such as popular Denial of Service attacks, and can keep viruses/worms and even spam out of your network. Most computer operating systems are not inherently secure, and with many systems now connected to the Internet 24/7 via broadband technologies such as cable and DSL, they are more vulnerable than ever.

Every computer or LAN that connects to the Internet should use a firewall of some type to protect it against intrusions. Business networks may also benefit from being able to control what data employees can send out.

Popular Firewall Solutions

There are a number of popular commercial firewall solutions. Companies such as Cisco Systems (www.cisco.com) make sophisticated hardware firewalls. Microsoft's ISA Server (www.microsoft.com or www.isaserver.org) and CheckPoint's Firewall-1 (www.checkpoint.com) are popular business oriented software firewalls. All of these are relatively expensive – too expensive for most home users and many small business users. However, home computers and small business networks need firewalls, too, especially when connected to the Internet continuously. Luckily, there are also a number of consumer oriented firewall programs that are relatively inexpensive. These include ZoneAlarm (www.zonelabs.com) and Tiny Personal Firewall (www.tinysoftware.com) for Windows and

Operating system vendors are also incorporating rudimentary firewall services into the operating systems. Windows XP has the built-in Internet Connection Firewall (ICF) that can be configured through the properties for each network connection. The Linux kernel provides firewall services, administered via the ipfwadm utility.

There are also freeware software firewalls that can be downloaded from various websites. Check out http://www.webattack.com/Freeware/security/fwfirewall.shtml for several freeware firewall downloads.

Summary

Firewalls have become a necessary and important part of every network or standalone computer that is connected to the Internet. There are firewalls available for all budgets, and you should have one if you want to protect your computer or LAN from unauthorized intrusions and control what goes in and out.

Deb Shinder A+ Weekly News Author