Chapter 20

THE IMPORTANCE OF FIREWALLS

INTRODUCTION

If you have been using the Internet for any length of time, and especially if you work at a larger enterprise and browse the Web while you are at work, you have probably heard the term firewall used. If you have a fast Internet connection into your home (either a DSL connection or a cable modem), you may have found yourself hearing about firewalls for your home network as well. It turns out that a small home network has many of the same security issues that a large enterprise network does. You can use a firewall to protect your home network and family from offensive Web sites and potential hackers as shown in Fig. 20-1 [1].

Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why its called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next. As you read through this chapter, you will learn more about the importance of firewalls, how they work and what kinds of threats they can protect you from, how to use a packet filter to shield against bombardment, and how to use application proxies to manage Internet communications [1].

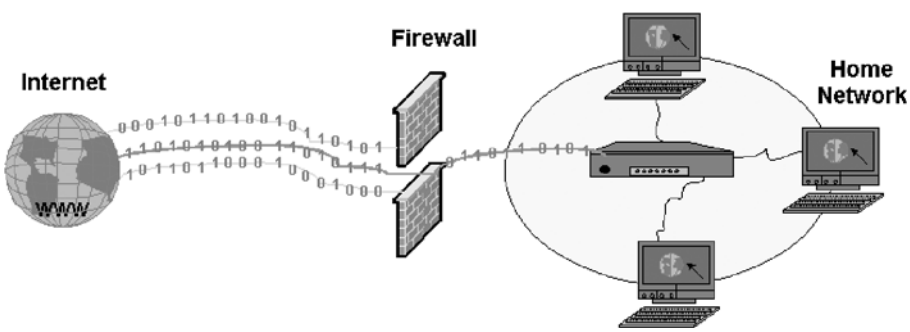

Figure 20-1. Protecting your home network.

WHAT IT DOES

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed to get through [1].

By now, you probably know a good bit about how data moves on the Internet, and you can easily see how a firewall helps protect computers inside a large enterprise. Let's say that you work at an enterprise with 500 employees. The enterprise will therefore have hundreds of computers that all have network cards connecting them together. In addition, the enterprise will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make FTP connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole [1].

With a firewall in place, the landscape is much different. An enterprise will place a firewall at every connection to the Internet (for example, at every T1 line coming into the enterprise). The firewall can implement security rules. For example, one of the security rules inside the enterprise might be: Out of the 500 computers inside this enterprise, only one of them is permitted to receive public FTP traffic. Allow FTP connections only to that one computer and prevent them on all others [1].

An enterprise can set up rules like this for FTP servers, Web servers, Telnet servers and so on. In addition, the enterprise can control how employees connect to Web sites, whether files are allowed to leave the enterprise over the network and so on. A firewall gives an enterprise tremendous control over how people use the network [1]. Firewalls use one or more of three methods to control traffic flowing in and out of the network:

- Packet filtering: Packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- Proxy service: Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- Stateful inspection: A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded [1].

MAKING THE FIREWALL FIT

Firewalls are customizable. This means that you can add or remove filters based on several conditions. Some of these are: