Chapter 1

Why Do You Need a Firewall?

In This Chapter

- Understanding what a firewall does
- Connecting to the Internet
- Figuring out Internet protocols
- Understanding how a firewall works
- Identifying hackers
- Setting rules

If you want to find out about firewalls, you bought the right book. Before we start exploring the gory details of how firewalls work and how to configure them, we use this chapter to lay the groundwork. If you are already familiar with how the Internet works and how you connect to it, and if you have a basic understanding of firewalls, then you can skip this chapter. If these topics are new to you, if you want to refresh your knowledge of any of these topics, or if you want to get an overview of what a firewall is, then read on.

Defining a Firewall

A *firewall* is a piece of software or hardware that filters all network traffic between your computer, home network, or company network and the Internet. It is our position that everyone who uses the Internet needs some kind of firewall protection. This chapter tells you what a firewall does and sets down the basic questions that you should ask as you are evaluating specific firewalls.

Not too long ago, only construction workers and architects asked the question, "Why do we need a firewall?" Before the term *firewall* was used for a component of a computer network, it described a wall that was designed to

contain a fire. A brick and mortar firewall is designed to contain a fire in one part of a building and thus prevent it from spreading to another part of the building. Any fire that may erupt inside a building stops at the firewall and won't spread to other parts of the building.

A firewall in a computer network performs a role that is very similar to that of a firewall in a building. Just as a firewall made out of concrete protects one part of a building, a firewall in a network ensures that if something bad happens on one side of the firewall, computers on the other side won't be affected. Unlike a building firewall, which protects against a very specific threat (fire), a network firewall has to protect against many different kinds of threats. You read about these threats in the papers almost every day: viruses, worms, denial-of-service (DoS) attacks, hacking, and break-ins. Attacks with names like SQL Slammer, Code Red, and NIMDA have even appeared on the evening news. Unless you haven't read a newspaper or watched the news in the last year, you surely have heard at least one of these terms. It's no secret: *they* are out there, and *they* are out to get us. Often we don't know who *they* are, but we do know where possible intruders are and where we don't want them to penetrate. Hackers are roaming the wide expanses of the Internet, just like the outlaws of the Old West roamed the prairies, and we don't want them to enter our network and roam among the computers in it.

You know that you need to protect your network from these outlaws, and one of the most efficient methods of protecting your network is to install a firewall. By default, any good firewall prevents network traffic from passing between the Internet and your internal network. "Wait a second," you may be thinking. "I just spent a lot of time, effort, and money to get my network connected to the Internet so that I can send e-mail to business partners, look at my competitor's Web site, keep up-to-date on sports scores, and check the latest fashion trends. And now you're telling me that a firewall blocks network traffic. How does this make sense?"

The answer is easy. Keep in mind that separating the Internet from your internal network traffic is the default behavior of most firewalls. However, the first thing that you will probably do after installing the firewall is to change the defaults to allow selected traffic network through the firewall. This is no different from a building inspector who allows fire doors in a physical firewall. These doors are designed to provide an opening while still guaranteeing safety for all occupants. When you configure a firewall, you create some controlled openings that don't compromise your network's safety but that allow selected network traffic to pass through.

As you are designing your protection against attacks from the Internet, never rely on a single form of protection for your network. Doing so can give you a false sense of security. For example, even if you completely disconnect your network from the Internet to prevent a computer virus from entering your network, an employee can still bring to work a floppy disk that has been infected with a virus and inadvertently infect computers in your network.

Just because you're paranoid . . .

"Aren't you a little paranoid?" is a question that we're often asked. Thus far, we haven't consulted a medical professional because to us, the answer is clear: You bet we're paranoid. We know that *they* are out to get us. Sometimes we think that there are millions of people out on the Internet who want to break into the computers on our networks. If only the Trojans had been as paranoid, they would have looked more carefully at the horse that they were given. When dealing with computer networks, a moderate amount of paranoia is a very healthy trait — the more you are concerned about possible risks, the more likely you'll be in a position to provide adequate protection for your network. As the saying goes, "Just because you're paranoid doesn't mean that they're not really out to get you."

The Value of Your Network

Before you look in more detail at what threats you face and how you can protect yourself against these threats by using a firewall, take a minute to look at your network and establish how much it is worth to you. The best way to establish the value of something is to evaluate the cost of a loss. Take a look at some different types of damage and consider the cost of each:

- **Lost data:** How important is the data on your corporate network? To answer this question, try to estimate what would happen if the data disappeared. Imagine that someone managed to break into your network and deleted all your accounting data, your customer list, and so on. Hopefully you have methods in place to restore lost data from a backup — no matter how you lose it. But, for just a second, imagine that all your corporate data is gone and you have to reconstruct it. Would your company still be in business if this happened to you tomorrow?
- **Confidential data:** If anyone were to break into your network and get access to confidential data — for example, the secret plans for the perpetual motion machine that you are developing — imagine what could happen. What would an intruder do with the data? Because you don't know, you have to assume the worst. If the secret plans end up in the hands of a competitor, he or she may beat you to the market with a miracle machine, and the profits and the Nobel Prize in Physics go to that person instead of you. The damage may even be worse if the data that is stolen is your entire customer list, including complete contact and billing information.
- **Downtime:** Have you ever called a company to order an item or to complain about something, and you were told, "I can't help you, the network is down." If so, you probably remember your reaction. The excuse sounded cheap, and you felt like taking your business somewhere else.

However, network outages do happen, and often the best thing that employees can do is twiddle their thumbs and tell customers to call again later. Preventing intrusions from the Internet may cost a little bit of money, but the amount of money lost due to downtime caused by such an intrusion could cost a lot more.

- **Staff time:** Each time an attack on your network is successful, you must take time to fix the hole and to repair any damage. For example, if a virus infects the computers in your company, you may have to go to each computer to remove the virus and repair any damage. The time that you spend doing this adds up quickly, and — as the saying goes — time is money. Don't expect to fix a large-scale problem quickly; that is, unless you are in the information technology department of an organization that we know. After a recent virus outbreak, they solved the problem by erasing the hard drives of every single computer and reinstalling everything from scratch. When the employees came to work the next morning, they realized that all of their data was lost, and they had to start the arduous task of reconstructing it from scratch. The IT people were nowhere to be found; for them the problem had been solved — the virus was gone. For everyone else the problem had just started.
- **Hijacked computer:** Imagine that someone broke into your computer and used it for his own purposes. If your computer is not used much anyway, this may not seem like a big deal. However, now imagine that the intruder uses your computer for illegitimate purposes. For example, a hacker uses your computer to store stolen software. When law enforcement personnel, who have partially traced the hacker's tracks, come knocking on your door, you have some explaining to do.
- **Reputation:** Do you want to be the company that is mentioned in the local or national news as the latest victim of a computer attack? Imagine what this would do to your company's reputation. The potential damage from such publicity has even caused some companies to sweep network intrusions under the table.

Get Yourself Connected

Not too long ago, you only had a choice between two types of connections to the Internet: a slow modem dial-up connection for individuals and smaller organizations, or a fast and very expensive connection for larger companies and institutions. Things have changed. In many parts of the world, you now have a choice among several different types of Internet connections, each of them providing different access speeds and different security risks. Increasingly, these choices are becoming available in many parts of the world. In this section, we examine the different types and assess the benefits that they provide and the risks that they pose. As you will see, an important factor here is the bandwidth — the amount of data you can transfer across a network connection. Bandwidth is directly related to the connection speed.

Network and modem transfer speeds are normally measured in bits per second (bps). Computers keep track of data using a binary system in which all characters are translated to zeros and ones. A *bit* is a single one or zero. Most characters in the alphabet, including digits and special characters, can be expressed using eight bits; this is often referred to as a *byte.* So, if your network connection allows for data transfer at 8 kilobits per second (that's 8,000 bits per second), or 8 Kbps, your computer will transfer about 1,000 characters per second — minus a few because of the overhead to keep track of the connection. You may also have heard the term *baud,* which used to be a common measurement for modem speeds. A baud is a measurement for the number of electrical signals that are sent per second. At low transfer rates, the baud number is identical to the bps rate, but at higher rates the two differ. Because of this difference, you don't see the term *baud* used much anymore. When comparing modem speeds you only have to look at the bps numbers. These numbers are easy to interpret and compare: The higher the number, the faster the connection. Another good thing to remember is that a kilobit per second (Kbps) is about 1,000 bps, and a megabit per second (Mbps) is about 1 million bps.

Modem dial-up connections

Most dial-up connections use a modem to connect to the Internet. You connect a modem to your telephone line and all data between your computer and the Internet service provider (ISP) is transmitted using POTS (plain old telephone service), also referred to as PSTN (public switched telephone network).

Current modem technology allows you to connect at speeds of up to 56 Kbps — blazing fast compared to the speeds that were available just a few years ago, but agonizingly slow compared to most other technologies available. To make things worse, a 56 Kbps modem can connect at this speed only under ideal circumstances, which almost never happen. Poor line conditions, too many telephone switches, and regulatory limitations can all contribute to limiting the actual bandwidth that you can attain. After you are connected, you can transmit data only at the maximum speed in the downstream direction, from your ISP to your computer. Current technology limits upstream connections from your computer to your ISP to 33.6 Kbps. Still, because of their low cost, modems are still what most individuals use to connect to the Internet.

Some modems don't even operate at 56 Kbps. Modems and line conditions can have an effect on the actual data throughput. For example, one of the authors of this book went on a recent vacation to a small, remote island in Malaysia. There he discovered that the only Internet connection on the island was via a satellite phone connection, which limited connection speeds to 9,600 bps — furthermore, that limited bandwidth was shared by the two computers on the island.

Modem connections have one feature that can be both an advantage and a disadvantage. With a modem you have to establish a new connection each time you want to connect to the Internet. Connecting takes only a minute, but when you stare at your computer screen while the modem is dialing, this minute can seem like an eternity. From a security point of view, though, this characteristic of a dial-up connection is a good thing. Your computer is only connected to the Internet while you are dialed in. During all other times, nobody on the Internet can contact your computer and break into it.

ISDN connections

The ISDN line and dial-up connection have one major similarity: They're both used for both voice communications and data transmission. (By the way, ISDN stands for Integrated Services Digital Network, but almost everyone uses the acronym.) One main difference between the two technologies is that using an ISDN line enables you to have a voice call and a data transfer at the same time. The other main difference is that an ISDN enables you to transfer data at higher speeds than dial-up connections allow. Depending on the exact ISDN implementation, speeds of up to 128 Kbps are possible. Installing and configuring ISDN takes more skill and effort than plugging a modem into a telephone line, but many people find it worth the extra effort to get a faster connection.

Like a regular telephone dial-up connection, an ISDN connection is only active while you are dialed into the Internet.

DSL connections

The newest type of connection that telephone companies are offering is called a Digital Subscriber Line (DSL). DSL is a nifty enhancement to your telephone service that allows high-speed data transmissions over regular telephone lines, while enabling you to also use your telephone line for a voice call at the same time. This almost sounds like ISDN, but read on for some big differences.

You'll find much to like about DSL:

- **Speed:** DSL comes in many flavors, each with a different acronym, such as ADSL (Asymmetric Digital Subscriber Line), and each gives you much better bandwidth than a dial-up modem or ISDN connection. DSL bandwidth ranges from 256 Kbps all the way up to 7 Mbps or more. Some types of DSL feature different upload and download speeds, and sometimes the actual speed depends on how many other people are surfing

the Internet at the same time. However, independent of what type of DSL you use, the transmission speeds are very fast. Most people who move from a dial-up connection to a DSL connection are amazed by the speed difference and have a hard time imagining ever going back to a modem.

- **Cost:** DSL costs more than a dial-up connection, but most subscribers find it well worth the cost. Most types of DSL feature an "always on" connection, which means that you don't need to establish a dial-up connection each time you start using the Internet. Instead, you are always connected and your Web browser displays a Web page immediately each time you open it.

So, what's not to like about DSL?

- **Availability:** DSL is not available everywhere. Not all local telephone companies have installed the required hardware, and DSL is only available if you live within a certain distance from your telephone company's central office.
- **Telephone requirements:** The telephone line to your house has to be in good condition, and telephone companies often have other technical limitations. In addition, some telephone technicians are not familiar with DSL and have a hard time configuring it. The good news is that service is getting better as telephone companies are getting used to supporting DSL.
- **The always-on connection:** Although you never have to wait for an Internet connection to be established, anyone who can connect to your computer from the Internet can do so anytime that he or she wants to. Hackers like targets that are always there and predictable, such as computers that use DSL to connect to the Internet. Hackers are not so thrilled by targets that are disconnected from the Internet for most of the day, such as computers that use dial-up connections.

Although DSL has some disadvantages, it is an amazing technology. If it is available in your area, then you should definitely evaluate it as an option to connect to the Internet, but keep in mind that this type of connection increases the importance of using the protection that a firewall provides.

If you want to know more about DSL, we recommend the book *DSL For Dummies* by David Angell, published by Wiley Publishing, Inc.

Cable modems

Cable modems provide an Internet connection over cable television wiring. In addition to connecting your television to this cable, you also connect a cable modem to the wiring, and you suddenly have a high-speed Internet connection. Although the technology itself is distinct from DSL technology, the benefits

are similar: You get a very fast Internet connection that's always on. Just like DSL, cable modem availability is still spotty, but it's getting better all the time as cable TV providers are upgrading their equipment and adding this service.

How fast is a cable modem? The answer is: It depends on the technology, but also on how many other users are currently connected to the Internet and are sharing the cable that connects your cable modem to your cable TV provider's office. Many cable modem users find that initially their connection is blazing fast, as much as 1 Mbps or more. However, as more and more subscribers are added, everyone has to share the same bandwidth, and soon every subscriber's share of the bandwidth becomes less. However, when everyone except for you is asleep or at the beach, you will find that a cable modem lets you surf the Internet faster than a DSL connection would.

Cable modems have the same security issues as DSL, and then some. Like DSL, cable modems are always on. This means that whenever your computer is running, an intruder could break in; that is, unless you have taken proper precautions to secure your computer. Computers with always-on connections are a favorite target of hackers. Some computers — especially Windows-based computers with shared resources, such as shared folders or printers — announce themselves on the local network so that other users can easily find these shared resources and connect to them. This is great in a home network, but with a cable modem, these computers announce their shared resources to everyone on the same cable segment. This means that your neighbor's printer may show up as a resource as you look for the shared printer on your spouse's computer. Although a cable modem connection does not present a danger to a securely configured computer, many people don't take the proper security precautions and suddenly find that a stranger has connected to their computer or has sent a mystery message to their printer.

T1 and T3

T1 and T3 are telephone company terms for very fast connections. A T1 line can carry 1.544 Mbps; a T3 line carries 43 Mbps. These types of connections are usually too expensive for individuals and small companies. However, they provide reliable connections for medium-sized and large companies. Very large companies may even need multiple T3 lines.

T1 and T3 lines (and the similar E1 and E3 lines in Europe) are always on and present the same security challenges as a DSL line. In addition, although DSL connections are often utilized by a single home computer, T1 and T3 lines are almost always used by an entire corporate network to which multiple computers are connected.

Address types

Another important security consideration, which applies to each type of connection, is the type of network address that your computer is assigned. This is the IP address, which we cover in more detail in the next chapter. Some types of connections, such as dial-up modem connections, give your computer a new network address each time that you connect, which is referred to as a *dynamic* address. Dynamic addresses make it difficult for a hacker to initiate any extended effort to break into your computer. Because your computer doesn't use the same address for a long time, it's like a moving target for hackers.

Some Internet connections use *static* addresses. Using a static address means that your computer is assigned the same address each time it connects to the Internet. T1 and T3 connections almost always use static addresses; some DSL and cable modem connections do, too. Even if addresses do change with these connections, those changes may not happen frequently. When a hacker knows that he or she can connect to a single address and connect to the same computer every single time, the hacker is able to launch long, sustained attacks.

Although static addresses represent a risk, they provide you with a predictable method to access your computer from the Internet, including connections that are legitimate. For example, if you run a Web server, people need to be able to find your computer. At the same time, static addresses make life easier for hackers.

The need for speed and security

To enable you to easily compare and contrast the options covered in this chapter, Table 1-1 presents a comparison of the Internet connection methods that we cover in this section.

Table 1-1 Comparing Connection Options

Connection Type	*Speed*	*Security Considerations*
Dial-up modem	Up to 56 Kbps downstream; up to 33.6 Kbps upstream	No permanent connection, uses dynamic address
ISDN	Between 56 Kbps and 128 Kbps in both directions	No permanent connection, uses dynamic address

(continued)

Table 1-1 ***(continued)***

Connection Type	*Speed*	*Security Considerations*
DSL	Speeds vary; common speeds range from 256 Kbps to 1.4 Mbps	Often permanent connection, uses dynamic or static address
Cable modem	Speeds vary and depend on number of concurrent users; average speed up to 1 Mbps	Permanent connection, uses dynamic or static address
T1	1.544 Mbps	Permanent connection, uses static IP addresses
T3	43 Mbps	Permanent connection, uses static IP addresses

TCP/IP Basics

To understand how firewalls work, you have to know a little about how computers communicate and what language they speak. Just like people communicate on different levels, such as with spoken language, gestures, and intonation, computers also use different languages at the same time. As far as Internet connections and firewalls are concerned, the most important such language is TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP is a collection of *protocols,* each of which defines the rules for how computers communicate across the Internet. In Chapter 2 of this book you can find out a lot more about TCP/IP and how it works. For now, simply think of TCP/IP as a language that is used between computers on the Internet. One of the most important elements of TCP/IP is its addressing scheme. Computers that use TCP/IP use a unique number, called an IP address, to identify themselves. All data that is sent from one computer to another using TCP/IP includes information on what IP address the data comes from and what IP address it is being sent to.

TCP/IP defines the methods that computers connected to the Internet use to transmit information. This includes dividing this information in small manageable chunks called *packets.* Each packet contains header information and data. Most firewalls examine the packet header to determine whether the packet should be allowed to enter or leave a network behind a firewall. The header contains valuable information about where a packet comes from, what computer is the intended recipient of the packet, and even what program on the

destination computer should process the information in the packet. This program could be a Web server or a mail server application. Some firewalls can also examine the inside of a packet or the insides of multiple packets, such as all packets that comprise an e-mail message or a Web page, and then decide how to handle this traffic.

What Firewalls Do

So what exactly does a firewall do? As network traffic passes through the firewall, the firewall decides which traffic to forward and which traffic not to forward, based on rules that you have defined. All firewalls screen traffic that comes into your network, but a good firewall should also screen outgoing traffic.

Normally a firewall is installed where your internal network connects to the Internet. Although larger organizations may also place firewalls between different parts of their own network that require different levels of security, most firewalls screen traffic passing between an internal network and the Internet. This internal network may be a single computer or it may contain thousands of computers.

The following list includes the most common features of firewalls:

- **Block incoming network traffic based on source or destination:** Blocking unwanted incoming traffic is the most common feature of a firewall.
- **Block outgoing network traffic based on source or destination:** Many firewalls can also screen network traffic from your internal network to the Internet. For example, you may want to prevent employees from accessing inappropriate Web sites.
- **Block network traffic based on content:** More advanced firewalls can screen network traffic for unacceptable content. For example, a firewall that is integrated with a virus scanner can prevent files that contain viruses from entering your network. Other firewalls integrate with e-mail services to screen out unacceptable e-mail.
- **Make internal resources available:** Although the primary purpose of a firewall is to prevent unwanted network traffic from passing through it, you can also configure many firewalls to allow selective access to internal resources, such as a public Web server, while still preventing other access from the Internet to your internal network.
- **Allow connections to internal network:** A common method for employees to connect to a network is using virtual private networks (VPNs). VPNs allow secure connections from the Internet to a corporate network. For example, telecommuters and traveling salespeople can use a VPN to

connect to the corporate network. VPNs are also used to connect branch offices to each other. Some firewalls include VPN functionality and make it easy to establish such connections.

- **Report on network traffic and firewall activities:** When screening network traffic to and from the Internet, it's also important to know what your firewall is doing, who tried to break into your network, and who tried to access inappropriate material on the Internet. Most firewalls include a reporting mechanism of some kind or another.

What Firewalls Look Like

When you look at the graphics in this book, you see a firewall represented by a little brick wall. If you are a structural engineer, you know right away that this is not a real firewall, because a real firewall in a building must have structural reinforcements. Whether you are an engineer of any kind or not, though, you probably realize that a computer firewall doesn't look like a brick wall, anyway. Take a look at what computer firewalls look like.

A firewall that fits

Clothing salespeople want us to believe that there is a size that fits all. As a smart consumer and a fashionable dresser, you know that there is no such thing as one size that fits all. Similarly, there is also no size firewall that works well for every organization. Firewalls usually fall into one of the categories in the following list. The type of firewall that you install depends on your exact requirements for protection and management.

- **Personal firewall:** A personal firewall is most often installed as a piece of software on a single computer and protects just that computer. Personal firewalls also come as separate hardware components, or they may be built into other network devices, but they all protect a single computer or a very small number of computers. Personal firewalls also normally have very limited reporting and management features.
- **Departmental or small organization firewall:** These firewalls are designed to protect all the computers in an office of limited size that is in a single location. Firewalls in this category have the capacity to screen network traffic for a limited number of computers, and the reporting and management capabilities are adequate for this function.
- **Enterprise firewall:** Enterprise firewalls are appropriate for larger organizations, including organizations with thousands of users that are geographically dispersed. The reporting capabilities include consolidated reports for multiple firewalls; the management tools enable you to configure multiple firewalls in a single step.

As you are evaluating firewalls, keep in mind that some firewall products can work well in more than one setting. However, few firewalls — if any — work well in all three settings: personal, departmental, and enterprise.

Network router

One of the basic network connectivity devices is a *router.* A router transfers network packets between two different networks. In order for network traffic to get from one computer to another on the Internet, this traffic normally has to traverse a number of routers. Some router manufacturers have enhanced the functions of their products by including firewall features.

If you already have a router that connects your network to the Internet, you should explore whether it can perform packet filtering or other firewall functions. Most likely, you will find that your router provides some rudimentary firewall capabilities but that it doesn't give you any advanced features.

Appliance

Some firewalls consist of a piece of hardware with integrated software that provides a number of firewall functions. Such a device is often referred to as a *firewall appliance.* Just like a refrigerator that simply works when you plug it into an outlet, a firewall appliance starts working the moment you plug it in — there's no separate software to install. However, you still may have to do some configuration, which most often entails using a Web browser that's running on another computer. If you use such a firewall, the device is fairly simple to administer. You don't have to worry about configuring a separate operating system, and most often the device has no other functions that may interfere with the firewall's operations.

Software-only firewalls

Software-only firewalls run on a computer that can also perform other functions. Most personal firewalls that protect a single computer fall into this category. After all, the reason you get a personal firewall is to protect your computer while you are using the Internet — not to make your computer a dedicated firewall. Some enterprise firewalls are also software-based.

All-in-one tools

An increasingly popular type of network device is the all-in-one tool. One vendor, for example, offers a small box that promises to act as a cable modem,

router, network hub, wireless networking base station, and firewall. If it did the laundry and cooked dinner, it would be close to perfect — at least according to the specifications on the box. We have not tested this particular type of device, but often when we evaluate multifunction devices that include a firewall, we find that the manufacturer excludes some functions that we consider important. The device performs several functions reasonably well, but not necessarily well enough. There are a few exceptions to this rule, so don't dismiss a product just because it performs several functions; however, be skeptical as you evaluate such products.

When evaluating an all-in-one product, make sure that you pay special attention to the firewall features. The cost of the damage that can be done by hackers that are able to break through a firewall that doesn't work well is normally much more than what you can save by buying an all-in-one tool.

Rules, Rules, Everywhere Rules

Life has more than its share of rules. We just can't seem to get away from them. When it comes to firewalls, rules play an important part, too. A firewall enforces rules about what network traffic is allowed to enter or leave your personal computer or network. Most firewalls come with some preconfigured rules, but most likely you will have to add more rules. After the rules are in place, a firewall examines all network traffic and drops the traffic if the rules prohibit it. A large part of administering a firewall consists of configuring rules, such as the following:

- Allow everyone to access all Web sites.
- Allow outgoing e-mail from the internal mail server.
- Drop all outgoing network traffic unless it matches the first two rules.
- Allow incoming Web requests to the public Web server.
- Drop all incoming network traffic except for connections to the public Web server.
- Log all connection attempts that were rejected by the firewall.
- Log all access to external Web sites.

Configuring rules for a home network can be very easy. You may merely have to define a rule that allows all outgoing network traffic and another one that allows no connections to be established from the outside. Setting up the rules for a large corporation with many Web servers, thousands of users, and many departments (each with different needs for accessing the Internet) can be much more complicated.