Firewall Overview

etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+2.+Introduction+to+Firewalls/Firewall+Overview/

Firewall technologies have undergone substantial changes since their entry into the marketplace in the early 1990s. These first firewalls were simple packet-filtering devices. Since those days, firewalls have become much more sophisticated in their filtering features, adding such capabilities as stateful filtering, Virtual Private Networks (VPNs), intrusion-detection systems (IDS), multicast routing, connection authentication, Dynamic Host Configuration Protocol (DHCP) services, and many others. One of the driving forces of these enhancements, besides vendor competition, was the explosion of Internet usage in the mid- to late 1990s. This huge growth brought many beneficial services to individuals and companies, but it also brought its own set of problems, including hacking, break-ins, and other types of undesirable actions. Given these problems and the need to protect a company's assets, firewalls have become a common technology for not only enterprise companies, but also small businesses and personal computers that have Internet access.

As you will see in this chapter, many components make up a firewall solution; naturally, a firewall, or filtering device, is an important part of that solution. Normally, firewalls are seen as your first layer of defense when protecting company or personal assets. However, a complete firewall solution involves many components that are used to protect not only the perimeter of your network, but also your internal network infrastructure.

Definition of a Firewall

People use many descriptions when defining a firewall. Its first use had to do not with network security, but with controlling actual fires. A firewall is a method of constructing walls so that when a real fire breaks out, it can be contained easily within one part of a building instead of spreading to other parts.

Of course, when we talk about network security, the term firewall means something different, but the original essence is carried over: It is used to protect your network from malicious people and to stop their illicit actions at defined boundary points.

Basically, a firewall is a device or systems that control the flow of traffic between different areas of your network. Notice something important about this definition: The definition can include one or more devices. In simple, small network designs, such as a small office/home office (SOHO) environment, this typically is done with one device. For example, I use a wireless Linksys router at home to protect my home network. In an enterprise network, the firewall system includes many components, such as perimeter firewalls, stateful firewalls, VPNs, IDS solutions, and others.

Many people assume that firewalls are used to protect assets from external threats, such as those from the Internet, where the protocol used is TCP/IP. However, most malicious network threats and attacks occur, interestingly enough, within the interior of your network; in many instances, they come from a company's own employees. Many studies have found that between 60 and 70 percent of network attacks are internal, not external. On top of this, you might have more than one protocol running on your internal network, such as TCP/IP, IPX, AppleTalk, SNA, NetBIOS, and others. A comprehensive firewall solution must be capable of dealing not only with both internal and external threats, but also with multiple protocols.

NOTE

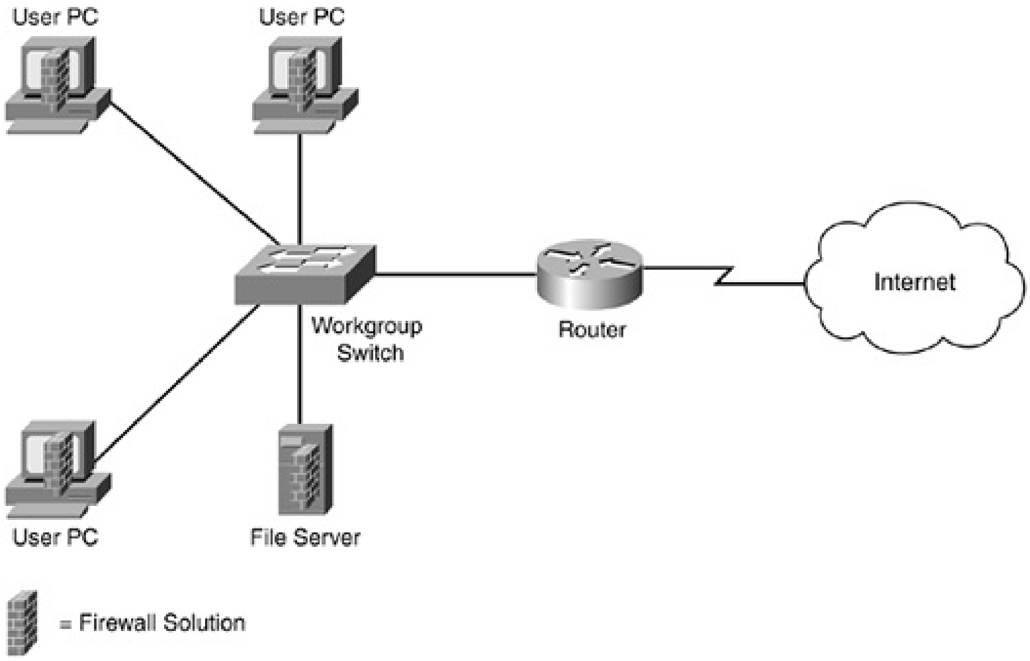
I like to refer to a firewall solution as a firewall system because you typically use more than one technology and one or more devices to implement your firewall solution. Firewall systems are used to control access to resources. A firewall system can be contained in one chassis, or your solution can involve many different devices. Choosing the right firewall system is critical in developing a secure network.

Firewall Protection

Firewall systems can perform many functions and offer many solutions. However, one of its primary purposes is to control access to resources. You can use many methods to perform this task.

For instance, you could physically secure all of your servers and PCs by making sure that they all have the most up-to-date patches, have unnecessary services disabled, use a robust form of authentication and authorization for accessing and using resources, and have security software installed on them, as shown in Figure 2-1. In this example, firewall software is installed on each PC and file server, and is configured to allow only certain types of traffic to enter or leave the machine. This works well in a small office with only a handful of devices that need to be secured. In this example, the devices might need only file and print sharing, as well as Internet access, so setting up this security policy on each device is straightforward.

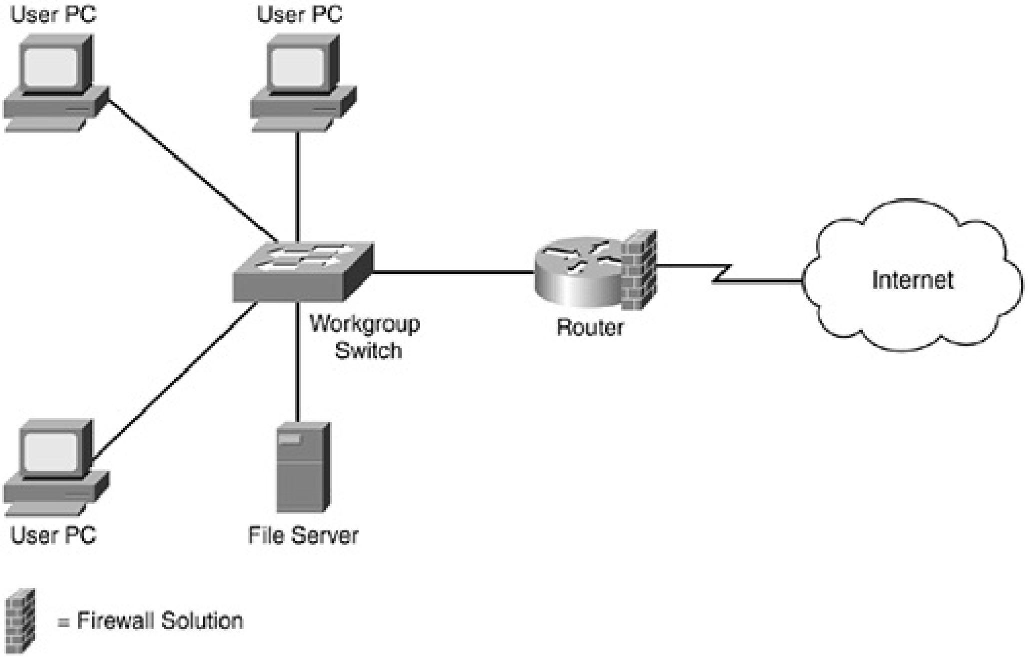
Figure 2-1. Securing All Network Devices



In a network with tens of thousands of devices, this becomes problematic: It would be very difficult to manage all of these devices to ensure that they were secured properly. Besides offering file and print sharing services, you might want to implement different levels of Internet access for different groups of users, you might need to protect certain internal resources based on a user's group membership, and you might allow only certain types of Internet traffic into your network.

A more scalable approach would be to centralize your security solution, as shown in Figure 2-2. I used the same example in Figure 2-1, but instead of using a firewall solution on each internal device, I placed it on the perimeter router. In this example, because the firewall solution is implemented in one device, it becomes much easier to manage security policies and their implementation. With a single device, it becomes easier to restrict traffic entering and leaving the network: You set up the policies only once instead of on all the internal devices. This also reduces the total cost of the solution.

Figure 2-2. Securing All Network Devices



This is not to say that you must use just one of these two solutions. However, it does begin to make you think about design issues as well as the types of access that you need to address. You must balance security, functionality, and cost in your design. For example, you still need to be concerned about internal threats to internal resources, so some of your critical internal resources might implement a firewall solution. I discuss design issues in much more depth in the "Component Placement" section.