All network traffic into and out of the LAN must pass through the firewall, which prevents unauthorized access to the network.

WARNING

Some type of firewall is a must-have if your network has a connection to the Internet, whether that connection is residential or business-class broadband (cable modem or DSL) or enterprise-grade fiber. Without a firewall, hackers will quickly discover your unprotected network. Within a few hours your network will be toast.

The most common way to set up a firewall is to purchase a *firewall appliance,* which is basically a self-contained router with built-in firewall features. Most firewall appliances include a web-based interface that enables you to connect to the firewall from any computer on your network using a browser. You can then customize the firewall settings to suit your needs.

Alternatively, you can set up a server computer to function as a firewall computer. The server can run just about any network operating system, but most dedicated firewall systems run Linux. However, this alternative is less commonly used.

Whether you use a firewall appliance or a firewall computer, the firewall must be located between your network and the Internet, as shown in Figure 20-1. Here, one end of the firewall is connected to a network hub, which is, in turn, connected to the other computers on the network. The other end of the firewall is connected to the Internet. As a result, all traffic from the LAN to the Internet and vice versa must travel through the firewall.

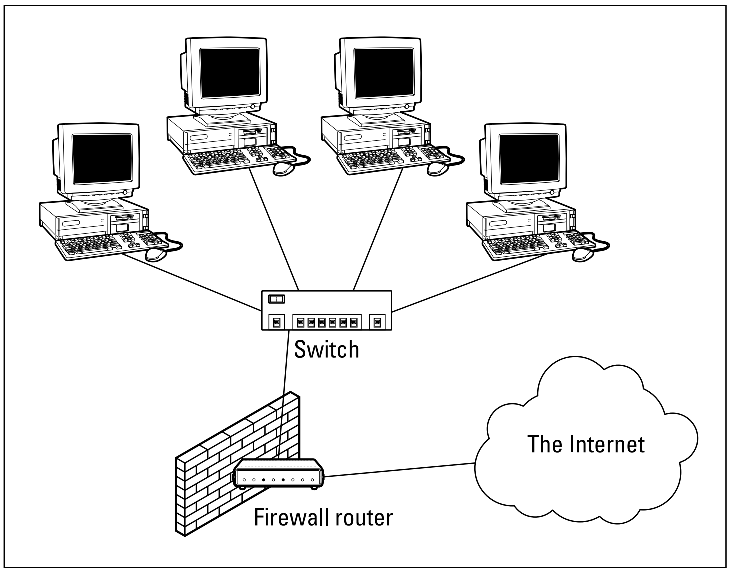

FIGURE 20-1: A firewall router creates a secure link between a network and the Internet.