Comparing residential gateways to firewall routers

If you peruse the shelves of your local big-box electronics store, you'll see a variety of devices called *Wi-Fi routers.* Technically, these devices are actually called *residential gateways*, because they provide more than just Wi-Fi capability. A residential gateway typically combines four distinct components in one handy package:

- A router that can connect a small network to the Internet.
- A firewall to protect the internal network from hackers who would love nothing more than to compromise your network.
- A small switch (typically four ports) to connect a few computers to the network. If you have more than four users, you can connect a larger switch to one of the gateway's switch ports. (For more information about switches, refer to Chapter 7.)
- A Wireless Access Point, which allows wireless devices to connect. (For more information about wireless access, refer to Chapter 8.)

Residential gateways are fine for home networks or for very small businesses. However, if your network has more than a dozen computers, you should consider stepping up to a dedicated firewall router, which separates the firewall and router features from the switching and Wi-Fi features.

A true firewall router has just two types of ports:

- A wide area network (WAN) port, which connects the firewall router to the Internet
- A local area network (LAN) port, which connects the firewall router to your internal network

Some firewall routers contain more than one WAN port, allowing you to connect to two separate Internet connections. For more information about this capability, see the section "Providing a Backup Internet Connection" later in this chapter.

Looking at the built-in Windows firewall

Windows includes a built-in firewall that provides basic packet-filtering firewall protection. In most cases, you're better off using a dedicated firewall router because these devices provide better security features than the built-in Windows