Understanding Windows Firewall settings

Windows Server 2012 R2 includes a firewall program called Windows Firewall, which is activated by default on all systems. In its default configuration, Windows Firewall blocks most network traffic from entering the computer. Firewalls work by examining the contents of each packet entering and leaving the computer and comparing the information they find to a series of rules, which specify which packets are allowed to pass through the firewall and which are blocked.

The Transmission Control Protocol/Internet Protocol (TCP/IP) is used by Windows systems to communicate functions by packaging application data using a series of layered protocols that define where the data comes from and where it is going. The three most important criteria that firewalls can use in their rules are as follows

- **IP addresses** *IP addresses* identify specific hosts on the network. You can use IP addresses to configure a firewall to only allow traffic from specific computers or networks in and out.
- **Potocol numbers** *Protocol numbers* specify whether the packet contains TCP or User Datagram Protocol (UDP) traffic. You can filter protocol numbers to block packets containing certain types of traffic. Windows computers typically use UDP for brief message exchanges, such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) transactions. TCP packets usually carry larger amounts of data, such as the files exchanged by web, file, and print servers.

- **Port numbers** *Port numbers* identify specific applications running on the computer.

The most common firewall rules use port numbers to specify the types of application traffic the computer is allowed to send and receive. For example, a web server usually receives its incoming packets to port number 80. Unless the firewall has a rule opening port 80 to incoming traffic, the web server cannot function in its default configuration.

Firewall rules can function in two ways, as follows:

■■ Admit all traffic, except that which conforms to the applied rules

■■ Block all traffic, except that which conforms to the applied rules

Generally, blocking all traffic by default is the more secure arrangement. From the server administrator’s standpoint, you start with a completely blocked system, and then begin testing your applications. When an application fails to function properly because network access is blocked, you create a rule that opens up the ports the application needs to communicate.

This is the method that Windows Firewall uses by default for incoming network traffic.

There are default rules preconfigured into the firewall that are designed to admit the traffic used by standard Windows networking functions, such as file and printer sharing. For outgoing network traffic, Windows Firewall uses the other method, allowing all traffic to pass the firewall except that which conforms to a rule.