Controlling Traffic and the OSI Reference Model

Before I can begin discussing the various firewall categories and their functions, I need to cover some basics of firewall operations: how firewalls deal with traffic. A good place to start is to review the Open System Interconnection (OSI) reference model, developed by the International Organization for Standardization (ISO). The ISO is a standards body that defines standards for interoperability, including networking standards. Using the OSI reference model will help you understand how firewalls process traffic. Many different categories of firewall solutions exist; each functions differently. This is particularly true of firewalls that filter traffic.

OSI Reference Model Overview

The ISO developed the OSI reference model to describe how devices communicate with each other. This model was developed to help instruct people on the communication process, simplify troubleshooting tasks, break related components into a modular structure, and ease development and implementation tasks for vendors.

The OSI reference model breaks up the communication process into seven layers, shown in Figure 2-3. It defines the general process that takes place when a user sitting at a keyboard types in information, and how it is transported across the network and processed at a destination device.

Figure 2-3. OSI Reference Model

Table 2-1 shows the seven layers and their descriptions. When talking about protocols and the OSI reference model, not all protocols used today have seven layers. The OSI reference model is just that: a model used generically to describe interactions between layers. For example, in TCP/IP, the application, presentation, and session layer functions are grouped into one generic layer, called the application layer. The transport, network, data link, and physical layers are used to handle the mechanics of the transmission of data between devices.

Table 2-1. OSI Reference Model Description

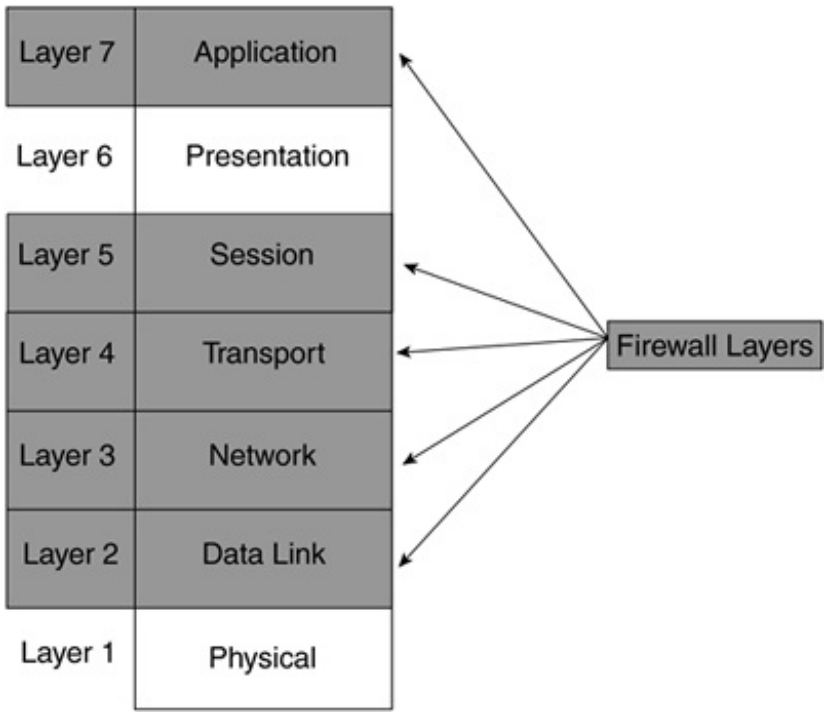
Layer	Name	Description
7	Application	Handles the command-line or graphical user interface (CLI or GUI) that an individual uses to interact with the device
6	Presentation	Identifies how data types, such as text, pictures, sound, and movies, are presented on an individual's monitor
5	Session	Sets up, monitors, and tears down network connections between devices
4	Transport	Provides a reliable or unreliable delivery mechanism for connections, as well as optional flow control
3	Network	Defines a logical topology for the network through the use of logical addressing schemes, such as IP and IPX

Layer	Name	Description
2	Data link	Defines how devices on a specific media type, such as Ethernet, communicate with each other, and hardware addresses, such as MAC addresses
1	Physical	Defines the physical characteristics and properties used to transmit data across a physical medium, such as copper, fiber, or air

Firewalls and the OSI Reference Model

As shown in Figure 2-4, a firewall system can operate at five of the seven layers of the OSI reference model. However, most firewall systems operate at only four layers: the data link, network, transport, and, possibly, application layers. Based on the simplicity or complexity of a firewall product or solution, the number of layers covered varies. For example, a standard IP access control list (ACL) on a Cisco router functions at OSI Layer 3, and an extended IP ACL functions at Layers 3 and 4.

Figure 2-4. Firewalls and the OSI Reference Model



The more layers that a firewall product or solution can cover, the more thorough and effective it can be in restricting access to and from devices. For example, a firewall that operates at only Layers 3 or 4 can filter only on IP protocol information, IP addresses, and TCP or UDP port numbers; it cannot filter on application information such as user authentication or commands that a user enters. Therefore, the more layers a firewall can process information from, the more granular it can be in its filtering process.