Chapter 29

PROTECTING SERVERS AND CLIENTS WITH FIREWALLS

INTRODUCTION

As previously explained in Chapter 20, a firewall puts up a barrier that controls the flow of traffic among domains, hosts and networks. The safest firewall would block all traffic, but that defeats the purpose of making the connection. According to a logical security policy, you need strict control over selected traffic. Enterprises typically put a firewall between the public Internet and a private and trusted network. A firewall can also conceal the topology of your inside networks and network addresses from public view, here, as well as elsewhere. But, that's only the beginning [4].

This chapter is intended to present a brief overview of firewall components, types available, and the relative advantages and disadvantages of each. It is intended to lay out a general road map for administrators who wish to publish information for public consumption with regards to protecting servers and clients, while preventing unauthorized access to their private or confidential network [4].

The information presented in this chapter is intended to simplify what can sometimes be intimidating or complex security and network setups. This chapter was not intended to be a complete manual on firewall types. Unfortunately the nature of firewall technology does not allow for a uniform "drop-in" installation setup, so every private network should research the topic of firewalls and network security to find a personalized solution or type that best fits their needs. This chapter should not be used as a replacement for knowledgeable network or security administrators [4].

Conceptually, there are three types of firewalls. Let's briefly discuss all three.

TYPES OF FIREWALLS

Now, let's start off with a brief review of basic firewall types: As previously mentioned, there are three types of firewalls:

- Simple Packet Filtering: IP or Filtering Firewalls – block all but selected network traffic.
- Application-layer Firewalls: Proxy Servers – act as intermediary to make requested network connections for the user.
- Stateful multilayer-inspection firewalls [1].

The preceding firewall types are not as different as you might think, and the latest technologies are blurring the distinction to the point where it's no longer clear if either one is "better" or "worse." As always, you need to be careful to pick the type that meets your needs (for further information, see Chapter 30, "Choosing The Right Firewall") [4].

Which is which depends on what mechanisms the firewall uses to pass traffic from one security zone to another. The International Standards Organization (ISO) Open Systems Interconnect (OSI) model for networking defines seven layers, where each layer provides services that "higher-level" layers depend on. In order from the bottom, these layers are physical, data link, network, transport, session, presentation, application [4].

The important thing to recognize is that the lower-level the forwarding mechanism, the less examination the firewall can perform. Generally speaking, lower-level firewalls are faster, but are easier to fool into doing the wrong thing [2].

Simple Packet Filtering: IP Or Filtering Firewalls

An IP filtering firewall works at the simple IP packet level. It is designed to control the flow of data packets based on their header information (source, destination, port and packet type) [3].

In other words, these types of firewalls generally make their decisions based on the source, destination addresses and ports in individual IP packets. A simple router is the "traditional" packet filtering firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or where it actually came from. Modern simple packet filtering firewalls have become increasingly sophisticated, and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. One thing that's an important distinction about many simple packet filtering firewalls is that they route traffic directly though them, so to use one, you either need to have a validly assigned IP address block or use a "private Internet" address block. Simple packet filtering firewalls tend to be very fast and tend to be very transparent to users [4].

In Fig. 29-1, a simple packet filtering firewall, called a "screened host firewall," is represented [4]. In a screened host firewall, access to and from a single host is controlled by means of a router operating at a network layer. The single host is a bastion host; a highly-defended and secured strong-point that (hopefully) can resist attack.