Chapter XI

Perimeter Defense: The Firewall

Introduction

As companies increasingly build private networks and connect them onto the Internet, securing such private networks has become a great concern. These networks are facing threats from two fronts: the external Internet and the users from within the company network. This requires security protocols that will effectively deal with these two fronts by first restricting access to the network from outside and controlling access between subnets from within. Ideal protocols to do such tasks are found in firewalls. A firewall is hardware, software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network. It is a tool that separates a protected network or part of a network, and now increasingly a user’s personal computer (PC), from an unprotected network—the “bad
network,” like the Internet. In many cases, the “bad network” may even be part of the company’s network. By definition, a firewall is a tool that provides a filter for both incoming and outgoing packets (see Figure 1). Most firewalls perform two basic security functions or a mixture of these two:

1. **Packet filtering**, which is based on an accept or deny policy that is itself based on rules of the security policy

2. **Application proxy gateways**, which provide services to the inside users and at the same time protect each individual host from the “bad” outside users

By denying a packet, the firewall actually drops the packet. In modern firewalls, the firewall logs are stored on log files and the most urgent or dangerous ones are reported to the system administrator. This reporting is slowly becoming real time. We will discuss this shortly.

The simplest form of a firewall can be implemented by using any device or tool that connects a network or an individual PC to the Internet. For example, a small router that connects your home to the Internet also can be used as a firewall. Currently the majority of firewalls are more complicated than that. They offer much more as they actively filter packets from and into the

*Figure 1. Basic firewall between private networks and the Internet*
Efficient Routing Protocol for Location Privacy Preserving in Internet of Things
International Journal of Information Security and Privacy (pp. 70-85).
www.igi-global.com/article/efficient-routing-protocol-for-location-privacy-preserving-in-internet-of-things/218847?camid=4v1a