# Chapter 8
# Firewall

**Biwu Yang**
*East Carolina University, USA*

## ABSTRACT

*Firewall is a critical technology in protecting enterprise network systems and individual hosts. Firewalls can be implemented through a specific software application or as a dedicated appliance. Depending on the security policies in an organization, several firewall implementation architectures are available, each with its advantages and disadvantages. Therefore, a thorough understanding of firewall technology, its features and limitations, and implementation considerations is very important in the design and implementation of effective firewall architecture in an organization. This chapter covers the life cycle of firewall design, selection, and implementation.*

## INTRODUCTION

The function of a firewall is to provide network access regulations, that is, to determine what traffic is allowed and what traffic is not allowed based on network security policies adopted by an organization. Similar to a router, a firewall device is situated inline of the network traffic path, with one interface to receive incoming data packets and another interface to forward the data packets. However, different from a router, a firewall does not need to make a decision for a best path to forward the data packets. It either allows the packets to go through or drop them.

The decision to allow data packets to go through or not is made by examining various characters of the incoming packets. Depending on the feature and capacity of a firewall, the characters that can be used to make the decision include the source and destination IP addresses, the destination TCP and/or UDP ports specified in a packet, the application layer protocol used, the time of a day, etc.

Firewall filtering criteria is implemented by "firewall rules". Firewall rules are defined based on security policies developed and adopted by an organization. An organization defines its informa-

DOI: 10.4018/978-1-61350-507-6.ch008

tion technology policies to meet their business goals and need. Security policies are part of the general information technology policies. Some security policies are simple to implement and some are difficult. Yet, not all security policies can be implemented through firewall technology. For example, a user access policy may require that network administrators must change their administration password every 30 days; this policy will not be implemented effectively through a firewall device. On the other hand, a security policy to specify that data packets initiated from outside network is not allowed into the internal network unless it is a response to a request initiated by a host in the internal network can be effectively implemented on the firewall at the perimeter network of the organization.

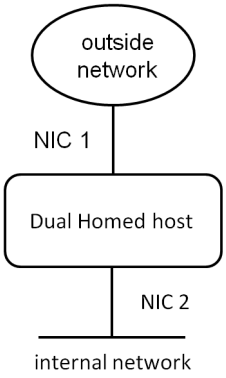
Depending on the security needs and policies, firewall can be implemented as a dedicated device, sometime called firewall appliance, or software solution, which is implemented on a regular computer. Also there are several designs in firewall architectures. For example, a perimeter firewall is typically situated between the outside network (untrusted side) of an organization and the internal network (trusted side). In addition, firewall devices are also used to protect critical network services, such as a server farm, where the key servers are located. In the design of a firewall architecture, several factors must be considered, including the location and selection of firewall devices, the impact of network traffic and throughput, the firewall device management, etc.

## TYPE OF FIREWALLS

Firewalls can be classified as software solution and dedicated hardware solution. In the early days, firewalls were software solutions.

As a software solution, a firewall is designed as an application to be installed on a regular computer. The computer would have at least two network interface cards (NIC) installed, one connects to the "outside" network and the other connects to the "internal" network, as illustrated in Figure 1. The computer is termed "dual homed host". More NICs can be used if the firewall is designed to connect to multiple internal networks.

*Figure 1. Dual Homed Host in a Network*




A hardware solution, also termed as "dedicated firewall" or "firewall appliance", is a device specifically designed to perform the function of monitoring and filtering network traffic. In most cases, this is a "single purpose" computer with a stripped down operating system that is specially designed to perform firewall related functions.

## Packet Filtering Firewall

The first generation of firewall uses packet filtering technology (Whitman & Mattord, 2004). Such a firewall would inspect incoming packets based solely on the network layer and transport layer information contained in an IP packet to determine whether the packet should be allowed or dropped.

Some protocol comparison between the OSI model and TCP/IP suite is shown in Table 1. In the TCP/IP suite, the IP header in the network layer indicates the type of protocol, such as ICMP, TCP, UDP, etc., in addition to the source and destination IP addresses. The transport datagram header in the transport layer indicates the TCP and UDP ports. Since most applications use "well known" TCP and/or UDP ports, the firewall administrator can