Chapter IX
Firewalls as Continuing Solutions for Network Security

Andy Luse
Iowa State University, USA

Anthony Townsend
Iowa State University, USA

Kevin Scheibe
Iowa State University, USA

ABSTRACT

This chapter describes various firewall conventions, and how these technologies operate when deployed on a corporate network. Terms associated with firewalls, as well as related concepts, are also discussed. Highly neglected internal security mechanisms utilizing firewall technologies are presented, including host-based firewalls and the more novel distributed firewall implementation. Finally, a section on how to perform a cost-benefit analysis when deciding which firewall technologies to implement is included. The chapter is designed as an introductory tutorial to the underlying concepts of firewall technologies. This understanding should provide a starting point for both systems support specialists implementing network security and researchers who are interested in firewall technologies.

INTRODUCTION

The organizational firewall continues to be the most highly deployed information system security device by organizations. The traditional perimeter firewall provides an invaluable first line of defense against would-be attackers, malicious programs, and many other electronic nuisances which threaten the integrity of the corporate network. The key to maintaining the security protection of the firewall lies in the effective deployment and maintenance, to continually configure the firewall to balance security and usability for internal users as well as external customers, business partners, and so on.

In addition to the traditional challenges of network security, an emerging issue garnering increasing attention is that of internal network security. Scandals such as Enron, increasing governmental policies and regulations with regard to security and privacy, as well as increased anxiety regarding corporate intellectual property, have lead many corporations to implement heightened security measures on their internal network. Many falsely believe that firewalls have limited effectiveness when deployed within the internal network, and so only recently have internal firewall deployments been considered by many security professionals. Unfortunately, in spite of the increased
security that secondary firewall installations can provide, many network administrators continue to fear an unmanageable security infrastructure when firewalls are brought inside the corporate network perimeter.

WHAT IS A FIREWALL

The term firewall historically gets its name from the physical concrete barriers running from the basement to the roof in buildings designed to limit the spread of fire and heat from one portion of the building to another (Whitman & Mattord, 2005). This model is mirrored with the concept of a firewall as it pertains to computer networks. Firewalls are typically thought of as devices placed between the internal corporate network and the external Internet designed to keep the “bad guys” and mischievous programs out of the internal network.

Firewalls, in their simplest construct, can be defined as a collection of components placed between two networks of differing security levels (Cheswick & Bellovin, 1994). Firewalls are designed to allow certain information into and out of a group of computers, or possibly a standalone computer, by way of a controlled point of entry (Zalenski, 2002). This controlled point must use some mechanism to keep track of which types of traffic are both allowed to enter as well as leave the network or computer.

Firewall functions. Firewall technologies come in several types which implement varying functionality for protecting internal computer(s) from external threats. These different methods all have their associated advantages and disadvantages relating both to security as well as usability, speed, and manageability. Understanding these concepts can help in the evaluation of the correct firewall technology for a specific application. While the most common application of firewall technology involves leveraging the device to protect the corporate network from the outside Internet, all the underlying functional types described in this section can be used in a large external firewall down to a host-based firewall protecting a single machine.

While the primary objective of all firewalls is the same, the methods used to accomplish these goals may vary. The following is a description of three main categories of firewalls: Packet Filters, Circuit Gateways, and Application Gateways.

Packet Filtering

The first generation of firewall technology involved analyzing packets entering and leaving a network for malicious traffic. This can involve inspecting just certain header values within the packet all the way up to analyzing the actual content of the message being transmitted in the packet payload (Strassberg, Gondek, & Rollie, 2002). One of the original firewall mechanisms, packet filtering is still widely used in many firewall appliances and applications today.

Packet filtering is a broad term which subsumes two separate methodologies: static packet filtering and stateful packet inspection. Although they can operate independently, these methods are traditionally not seen in isolation from each other, so a de facto third category also exists, the hybrid packet filter.

Static Packet Filtering

Static packet filtering involves specifying a predefined set of rules by which each packet entering and/or leaving a network is evaluated for admittance. The rules are typically defined in a list or access control list (ACL). The rules must be identified and installed before they can be used by the firewall device (Whitman & Mattord, 2005). Typically, the traditional static packet-filtering firewalls rely on existing protocols for verifying the legitimacy of a packet. This involves analyzing the header of the packet to validate source and destination IP addresses, the network protocol involved (TCP, UDP, and so on), and the port number being used (Strassberg et al., 2002).

The static packet filter offers some advantages when compared to other packet filtering technologies. First, due to its simple implementation and overhead, it usually performs quite efficiently. Second, it is relatively inexpensive to implement due to its simple approach. Third, again due to its simplistic approach, static packet filtering systems are typically easy to understand and manage (Strassberg et al., 2002).

Despite its benefits, the static packet filter does not provide the functionality needed for most corporate firewall implementations. First, the system does not allow easy updateability. For new rules to be added to the system, and administrator must first input these rules. Second, by necessity, it leaves open a number of holes in the firewall due to its lack of knowledge about existing connections from internal clients. This is especially apparent when connectionless protocols such as UDP are utilized. For example, say