Chapter 32

SELECTING FIREWALL SECURITY TOPOLOGY POLICY

INTRODUCTION

Network administrators have increasing concerns about the security of their networks when they expose their organization's private data and networking infrastructure to Internet crackers. To provide the required level of protection, an organization needs a security policy to prevent unauthorized users from accessing resources on the private network and to protect against the unauthorized export of private information. Even if an organization is not connected to the Internet, it may still want to establish an internal security policy to manage user access to portions of the network and protect sensitive or secret information [3].

With regards to the Internet, many organizations have connected or want to connect their private LANs to the Internet so that their users can have convenient access to Internet services. Since the Internet as a whole is not trustworthy, their private systems are vulnerable to misuse and attack. A *firewall* is a safeguard one can use to control access between a trusted network and a less trusted one. A firewall is not a single component, it is a strategy for protecting an organization's Internet-reachable resources. Firewalls can also be used to secure segments of an organization's *intranet*, but this chapter will concentrate on the Internet aspects of firewall policy [3].

A firewall enforces a security policy, so without a policy, a firewall is useless. This chapter will help the responsible manager and firewall administrator create useful policy for the firewall. Throughout this chapter, the term *firewall* refers to the sum of the hardware, software, policy and procedures used to implement the firewall policy. A firewall is not necessarily a single piece of software sitting on a single computer system [3].

FIREWALL PROTECTION

The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted. For example, if a traveling manager has a modem connected to his or her office PC that he or she can dial into while traveling (war-driving), and that PC is also on the protected internal network, an attacker who can dial into that PC has circumvented the firewall. Similarly, if a user has a dial-up Internet account with a commercial Internet Service Provider (ISP), and sometimes connects to the Internet from their office PC via modem, he or she is opening an unsecured connection to the Internet that circumvents the firewall. Firewalls provide several types of protection:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems.
- They hide vulnerable systems which can't easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.
- They can provide more robust authentication than standard applications might be able to do [1].

Each of the preceding functions are described in greater detail next.

As with any safeguard, there are trade-offs between convenience and security. Transparency is the visibility of the firewall to both inside users and outsiders going through a firewall. A firewall is transparent to users if they do not notice or stop at the firewall in order to access a network. Firewalls are typically configured to be transparent to internal network users (while going outside the firewall); on the other hand, firewalls are configured to be non-transparent for outside network coming through the firewall. This generally provides the highest level of security without placing an undue burden on internal users [3].

FIREWALL ARCHITECTURES

Firewalls can be configured in a number of different architectures, providing various levels of security at different costs of installation and operation. Organizations should match their risk profile to the type of firewall architecture selected. This part of the chapter describes typical firewall architectures and sample policy statements:

- Multi-Homed Host.
- Screened Host.
- Screened Subnet [2].