Virtual private networks (VPN) and IPsec are discussed in this chapter. A VPN emulates a private wide area network (WAN) facility using IP networks, such as the public Internet or private IP backbones.

When VPNs are used, the Internet offers the appearance, functionality, and usefulness of a dedicated private network. One of the problems in using the Internet as a WAN is that the Internet is a public network and has relatively little security.

IPsec provides the following security services to VPNs: data origin authentication, access control, confidentiality (encryption), connectionless integrity, rejection of replayed packets (a form of partial sequence integrity), and limited traffic flow confidentiality.

Objectives

• Understand VPN concepts and advantages
• Learn how IPsec provides security services to IP Networks
• Become familiar with IPsec concepts of security associations, security protocols, and key management
Introduction

In RFC 2764 (Gleeson, Lin Heinanen, Armitage, & Malis, 2000), an IP based virtual private network is defined as an “emulation of a private wide area network (WAN) facility using IP facilities, including the public Internet, or private IP backbones.” VPNs are used as the basic transport for connecting corporate data centers, remote offices, mobile employees, telecommuters, customers, suppliers, and business partners. The public network is used as a wide area communications network, and it offers the appearance, functionality, and usefulness of a dedicated private network.

Service providers sold T1 services to corporate clients as a way for the clients to create their own private networks for data traffic. Other technologies such as Frame Relay (FR) and asynchronous transfer mode (ATM) also allow the connection of different sites. The service provider maintains a “cloud” of frame relay connections, and the links are assigned only when needed. As a result, communication prices have gone down considerably.

A T1 leased line normally has a fixed price, with an additional mileage charge per month per mile. Even though frame relay fees do not include a charge for distance and are considerably less expensive than leased lines, monthly fees are still required for the permanent virtual circuits. T1 Internet connections have a monthly fixed price, so one of the main reasons to use the Internet as a corporate WAN is cost savings. There are other compelling arguments for replacing a private network, for example, scalability, responsiveness, and flexibility. Today, most corporations are using the Internet as their corporate WAN because of cost savings and reduced time to set up a connection.

There is a growing need to integrate more closely with partners, suppliers, and customers; there is also a corresponding need to “virtually” extend a company’s geographic reach to include telecommuters and mobile personnel, remote offices and sites, and major vendors and contractors. Therefore, another reason to use the Internet as the corporate WAN network is the savings in long distance charges resulting from, for example, mobile employees not having to call an 800-number to access corporate modem banks. Instead, telecommuters and the mobile force place local calls to the ISP’s POP to connect to the corporate network.

The following are some of the VPN benefits:

Figure 11-1. A corporate virtual private network over the Internet

With Secure VPNs,
• I am sure to whom I am talking.
• I know my message has not been modified.
• I know that only authorized persons have seen my message.
• I know that the message recipient can’t deny receiving my message.