VIRTUAL PRIVATE NETWORK(VPNS)

Virtual Private Networks are implementations of cryptographic technology (which you learn about in Chapter 8 of this book). A Virtual Private Network (VPN) is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network. The Virtual Private Network Consortium (VPN (*www.vpnc.org)* defines a VPN as "a private data network that makes use of the Public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPNs are commonly used to extend securely an organinization's internal network connections to remote locations beyond the trusted network.

The VPNC defines three VPN technologies: trusted VPNs, secure VPNs, and hybrid VPNs A trusted VPN, also known as legacy VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits . The organization must trust the service provider, who provides contractual assurance that no one else is allowed to use these circuits and that the circuits are properly maintained and protected-hence the name *trusted* VPN. Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the internet . A hybrid VPN combines the two providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used:

- . Encapsulating of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network as well as be usable by the server network environment.

- Encryption of incoming and outgoing data to keep the data contents private while in transit over the public network but usable by the client and server computers and/or the local networks on both ends of the VPN connection.

- Authentication of the remote computer and, perhaps, the remote user as well.
- Authentication and the subsequent authorization of the user to perform specific options are predicated on accurate and reliable identification of the remote system and/or user.

In the most common implementation, a VPN allows a user to turn the Internet in private network. As you know, the Internet is anything but private. However, using the tunneling approach an individual or organization can set up tunneling points across the Internet and send encrypted data back and forth, using the IP-packet-within-an-IP-packet method to transmit data safely and securely. VPNs are simple to set up and maintain usually require only that the tunneling points be dual-horned-that is, connecting a private network to the Internet or to another outside connection point. There is VPN support built into most Microsoft server software, including NT and 2000, as well as client support for VPN services built into XP. While true private network services connections can cost hundreds of thousands of dollars to lease,configure, and maintain, a VPN can cost next nothing. There are a number of ways to implement a VPN. IPSec, the dominant protocol used in VPNs, uses either transport mode or tunnel mode. IPSec can be used as a stand alone protocol, or coupled with the Layer 2 Tunneling Protocol (L2TP).

Transport Mode

In transport mode, the data within an IP packet is encrypted) but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contains of the packet. The downside to this

implementation is that packet eavesdroppers can still determine the destination system. Once an attacker knows the destination, he or she may be able to compromise one of the end nodes and acquire the packet information from it. On the other hand, transport mode eliminates the need for special servers and tunneling software, and allows the end users to transmit traffic from anywhere. This is especially useful for traveling or telecommuting employees.

There are two popular uses for transport mode VPNs . The first is the end-to-end transport of encrypted data. In this model, two end users can communicate_directly, encrypting and decrypting their communications as needed. Each machine acts as the end node VPN server and client In the second, a remote access worker or teleworker connects to an office network over the Internet by connecting to a VPN server on the perimeter. This allows the teleworker's system to work as if it were part of the local area network. The VPN server in this example acts as on intermediate node, encrypting traffic from the secure intranet and transmitting it to the remote client, and decrypting traffic from the remote client and transmitting it to its final destination.

This model frequently allows the remote system to act as its own VPN server, which is a weakness, since most work-at-home employees are not provided with the same level of physical and logical security they would be if they worked in the office.

OFFLINE

VPN vs. Dial-Up

Modern organizations can no longer afford to have their knowledge workers "chained" to hardwired local networks and resources. The increase in broadband home services and public Wi-Fi networks has increased use of VPN technologies, enabling remote connections to the organization's network to be established from remote locations, as when, for example, employees work from home or are traveling on business trips. Road warriors can now access their corporate e-mail and local network resources from wherever they happen to be.

Remote access falls into three broad categories: 1) connections with full network access, where the remote computer acts as if it were a node on the organization's n work; 2) feature-based connections, where users need access to specific, discrete network features like e-mail or file transfers; and 3) connections that allow remote control of a personal computer, usually in the worker's permanent office. It is the first category of connections that now use VPN instead of the traditional dial-up access based on dedicated inbound phone lines.

In the past, mobile workers used Remote Access Servers (RAS) over dial-up or ISDN leased lines to connect to company networks from remote locations (that is, when they were working from home or traveling). All things considered, RAS was probably more secure than the current practice of using a VPN, as the connection was made on a t private network. However, RAS is expensive because it depends on dedicated phone circuits specialized equipment, and aging infrastructure.

The alternative is VPN, which makes use of the public Internet. It is a solution that offers industrial-grade security. VPN today uses two different approaches to the technolgy-IPSec and Secure Sockets Layer (SSL). IPSec is more secure but is more expensive and requires more effort to administer. SSL is already available on most common Internet browsers and offers broader compatibility without requiring special software on the client computer. While SSL-based VPN has a certain attractiveness on account of its wide application cability and lower cost, it is not a perfect solution. The fact that it can be used nearly any where makes losses from user lapses and purposeful abuse more likely.

Tunnel Mode

In tunnel mode, the organization establishes two perimeter tunnel servers. These servers serve as the encryption points, encrypting all traffic that will traverse an unsecured network. In tunnel mode, the entire client packet is encrypted and added as the data of a packet addressed from one tunneling server and to another. The receiving ser decrypts the packet and sends it to the final address. The primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.

One example of a tunnel mode VPN is provided with Microsoft's Internet Security and Acceleration (ISA) Server. With ISA Server, an organization can establish a gateway-to-gateway tunnel, encapsulating data within the tunnel. ISA can use the Point to Point nneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), or Internet Securi1 Protocol (IPSec) technologies. Additional detail on these protocols is provided in Chapter 8. Figure 6-19 shows an example of tunnel mode VPN implementation. On the client end, a user with Windows 2000 or XP can establish a VPN by configuring his or her system connect to a VPN server. The process is straightforward. First, connect to the Internet through an ISP or direct network connection. Second, establish the link with the remote VPN server. Figure 6-20 shows the connection screens used to configure the VPN link. .

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf