Intranets and Virtual Private Networks (VPNs)

Definition

Private networking involves securely transmitting corporate data across multiple sites throughout an entire enterprise. Creating a truly private corporate network generally requires an intranet. A virtual private network (VPN) is one means of accomplishing such an implementation using the public Internet.

Overview

This tutorial explores the benefits of a private corporate network and reviews a traditional wide-area network (WAN) architecture implementation. It then compares the WAN model to present-day private-networking strategies, specifically examining two types of modern private-network implementations: encryption-based VPNs and private networks based on frame-relay permanent virtual circuits (PVCs). It also reviews important security issues associated with the different technologies used to implement a private network.

Topics

1. Introduction
2. Benefits of ISP–Based Private Networks
3. Traditional WAN Network Architecture
4. Encryption-Based VPNs
5. Private Networking Using Frame-Relay PVCs
Self-Test
Correct Answers
Glossary

1. Introduction

Today's corporations are challenged by the need to support a wide variety of communications across a highly distributed number of sites and offices. At the same time that the number of sites and offices increases, corporations are pressured to reduce the cost of their overall communications expenses. In addition to the increased number of office locations, employees expect to access corporate resources from a more diverse set of locations, including customer sites, home offices, and travel destinations. As more emphasis is placed on electronic communication, business partners also expect to access corporate-partner data as well. All of these trends drive the need to establish a corporate private-network infrastructure.

With regard to communications expenses, however, corporations are finding that traditional architecture does not provide the flexibility and solutions required. Using dedicated leased-line circuits to interconnect main offices and branch offices often requires significant planning time, and once in place the circuits cannot support remote or customer sites. The increase in telecommuting and remote computing is, in turn, increasing resources spent on remote-access modems, servers, and long-distance telephone charges.

Private networks that utilize the Internet backbone can significantly reduce the costs of establishing and maintaining a WAN for private-networking purposes. Internet service provider (ISP)–based private networks offer a global footprint with ubiquitous local network access. Using an ISP–based private network, corporations can connect their offices to the ISP's local points of presence (PoPs) rather than purchase costly leased-line circuits to interconnect their office locations. The corporation takes advantage of the ISP's established backbone, which is usually more geographically diverse than its WAN architecture. The ISP can also offer local dial-up access at a diverse number of locations, which helps reduce long-distance remote-access costs.

2. Benefits of ISP–Based Private Networks

ISP–based private networks can offer direct cost savings over traditional WAN architectures as well as other indirect cost savings. The increased flexibility and scalability of ISP–based private networks can often reduce equipment costs while minimizing network management and technical-training resources.

The most significant benefit of an ISP–based private network is its direct cost savings over traditional WANs. A traditional WAN is composed of distance-sensitive leased-line circuits, which can be subject to interstate and international tariffs and taxes. In comparison, an ISP–based private network only requires shorter leased-line circuits from each office to the ISP's closest PoP. ISPs can also offer flexibility in line speeds; corporations can usually purchase access in

fractional tier-1 (T1) increments rather than in an entire T1 circuit from a telco or local exchange carrier (LEC).

Outsourcing network management to an ISP can also indirectly reduce operating costs and resources. In-house technical resources are no longer needed to install, configure, and manage network equipment. A corporation will not need to support dial-up plain old telephone service (POTS) lines or integrated services digital network (ISDN) and leased-line circuits. The information technology (IT) department can concentrate resources on data and server equipment rather than on low-level network equipment.

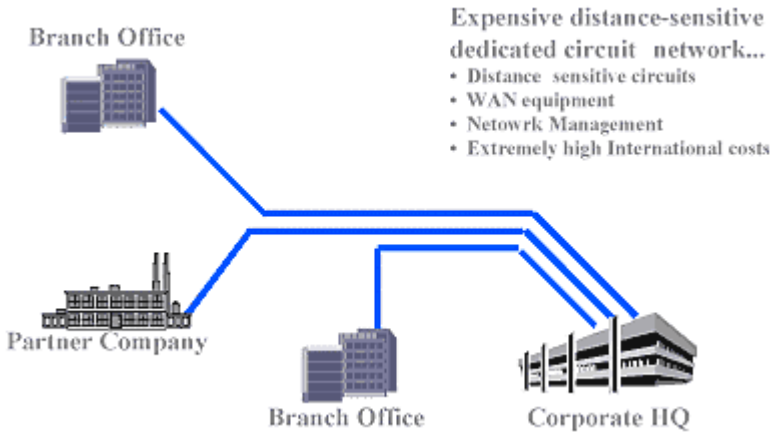
Several different ways to implement an ISP–based private network can be used. One common implementation transmits corporate traffic over the public Internet but uses encryption to protect the data from unauthorized access. Frame-relay technology also enables the creation of logically isolated circuits or PVCs that provide a private network in which data does not need to be encrypted because it travels only along these logically private circuits.

3. Traditional WAN Network Architecture

Traditional WAN–based private networks used leased-line circuits from each site back to a corporate headquarters. These leased-line circuits were priced according to distance, making them expensive for geographically dispersed locations. These traditional WANs often used a hub-and-spoke model, requiring traffic going between branch offices to travel through the corporate headquarters. Despite these disadvantages, traditional WANs did offer the highest level of security and network performance. Corporations were paying for the full-dedicated bandwidth of the network.

Traditional WANs required highly specialized technical in-house resources and required corporations to manage their own networks. Older corporations often have extensive WAN infrastructure investments and are hesitant to adopt newer infrastructure implementations despite large potential cost savings. *Figure 1* illustrates a typical WAN implementation where all traffic is cross-connected at the corporate headquarters. Each branch office or partner company is connected directly to the headquarters location.

Figure 1. Traditional WANs



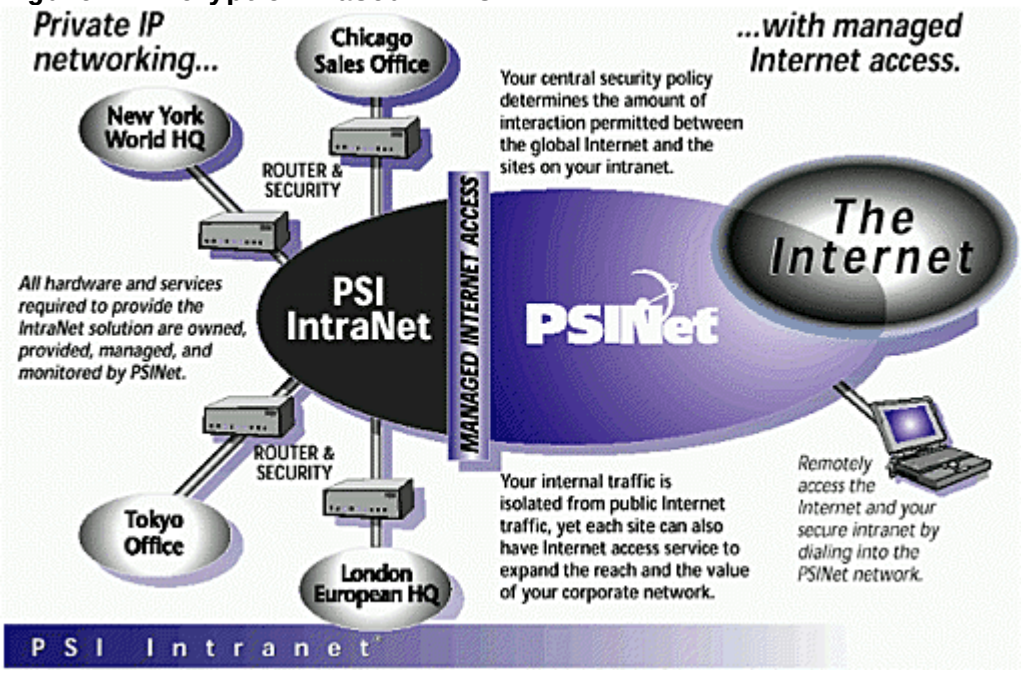
4. Encryption-Based VPNs

Encryption-based VPNs create a VPN using the public Internet infrastructure. A corporation establishes public Internet connections from each of its office locations to an ISP's PoP. The corporation can establish the connections with a single ISP or multiple ISPs.

Encryption-based VPNs are susceptible to any weaknesses that the public Internet may experience. Typically, these weaknesses are related to data security and network performance. The original design and implementation of the Internet did not address the security and performance requirements of private networks.

Encryption-based VPNs are often the easiest type of ISP–based private network to create. Several different encryption vendors supply a large range of solutions. *Figure 2* shows a typical encryption-based VPN implementation. Each branch office or partner company connects to any ISP; users simply must have access to the public Internet. An encryption device (typically a router or firewall) is placed at each location. The encryption devices receive encrypted data from the other locations and perform the appropriate decryption.

Figure 2. Encryption-Based VPNs

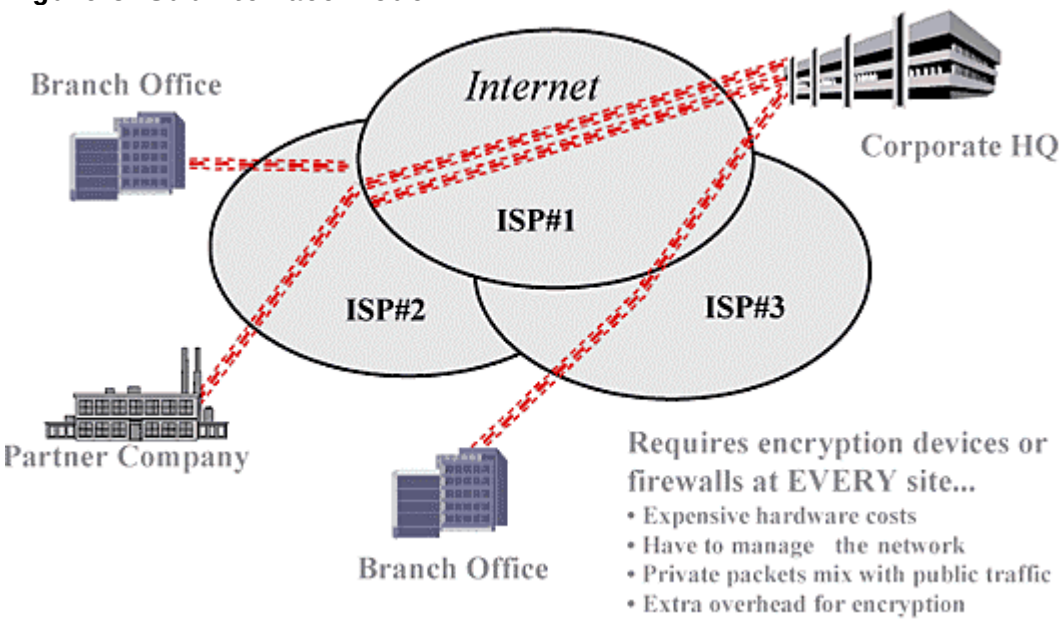


5. Private Networking Using Frame-Relay PVCs

Another way to implement a private-networking solution while capitalizing on an ISP's backbone is to create a private-network using frame-relay PVCs. Frame-relay PVC is a technology available to homogeneous frame-relay networks; the ISP must be able to implement the frame relay–networking protocol across its entire network.

A PVC is a way to logically create a separate independent circuit within the same physical circuit. *Figure 3* illustrates three separate PVCs within the same physical interface. Each PVC acts logically as a private circuit, similar to a traditional WAN–dedicated circuit.

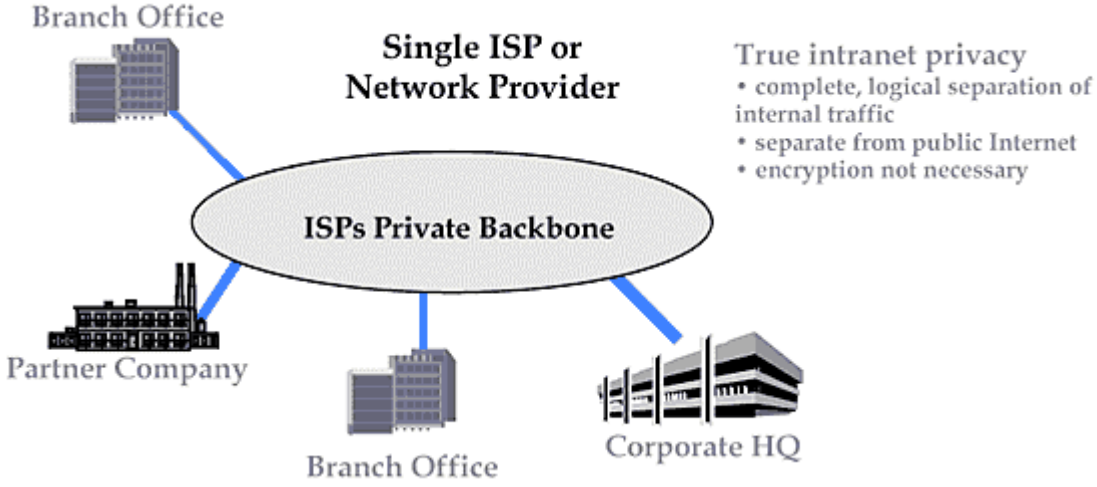
Figure 3. Subinterface Model



Frame-relay PVCs offer the advantages of high security because sensitive corporate data is not transmitted to the public Internet. Instead it is only transmitted down a customer's own PVC, which remains logically separate from the public Internet. A frame-relay PVC private-network implementation is also not as susceptible to network congestion, as each PVC only carries data for one customer.

Figure 4 illustrates a private network utilizing frame-relay PVCs. No additional encryption devices are necessary. Each branch office or partner company is connected to the homogeneous network of a selected ISP.

Figure 4. Frame-Relay PVC Networking Technology



Self-Test

1. *Private networking* refers to which of the following?

    a. different types of network firewalls

    b. networking where network protocols are not used

    c. securely transmitting corporate data

    d. accessing Web servers using the HTTP protocol

2. A VPN is which of the following?

    a. an implementation of a private network

    b. a network built using frame-relay technology

    c. a high-speed network protocol

    d. a standard way to encrypt files for secure transmission

3. Corporate networks are now challenged because of which of the following?

    a. computer equipment requires a greater amount of storage space

    b. centrally located computers are consuming greater amounts of electrical power

    c. multiple protocols are taxing existing network resources

    d. the need to support a wide variety of communications across a large geographic area

4. Traditional WAN architecture _____.

    a. is growing because it ideally meets corporate network needs

    b. is a low-cost solution to a wide variety of needs

    c. is less flexible and more costly to implement

    d. improves data transmission over long distances

5. Remote access modems require which of the following?

    a. increased equipment and management resources

b. minimal equipment and network resources

c. no additional long-distance charges

d. that telecommuters use specific remote-access hardware to access the internal network

6. ISP–based private networks _____.

a. require entirely new server and internal-network equipment

b. are a cost-effective alternative to traditional WANs

c. increase management costs as a result of additional network equipment

d. are more secure than traditional WANs

7. Compared to a single corporation, ISPs tend to have which of the following?

a. fewer remote-access dial-up ports

b. greater diversity in local remote-access points

c. minimal international remote-access capabilities

d. a smaller, more concentrated network backbone

8. Compared to a WAN, an ISP–based private network _____.

a. costs more due to the additional cost of a diverse network backbone

b. offers significant cost savings

c. offers a greater level of security and network performance

d. requires a greater number of dedicated leased-line circuits

9. Internal network management resources _____.

a. must be increased when using an ISP–based private network, as a result of Internet security issues

b. are still required when using an ISP–based private network to support network technologies including POTS, ISDN, and leased-line circuits

c. can be decreased when using an ISP–based private network due to the outsourcing of network management

d. never change regardless of private-network type

10. Traditional WANs are built using which of the following?

a. multiple dial-up links interconnecting each office location

b. short leased-line circuits connecting each office to its closest neighbor

c. inexpensive wireless network–transmission technologies

d. expensive, distance-sensitive leased-line circuits

11. International WANs are which of the following?

a. extremely expensive as a result of distance-sensitive leased-line circuits

b. impossible to build using traditional WAN technologies

c. inexpensive because corporations can share network costs with other corporations

d. built using satellite technology, which limits network performance

12. Encryption-based VPNs _____.

a. use the public Internet infrastructure to create a VPN

b. use inexpensive hardware to encrypt data traveling across the Internet

c. are more secure than traditional WANs due to data encryption

d. are not susceptible to Internet weaknesses and outages

13. Encryption-based VPNs _____.

a. require encryption hardware only at the primary headquarters location

b. cannot accommodate dial-up remote-access users

c. require an encryption equipment at each location of the network

d. aggregate network traffic through a central location

Correct Answers

1. *Private networking* refers to which of the following?

    a. different types of network firewalls

    b. networking where network protocols are not used

    c. securely transmitting corporate data

    d. accessing Web servers using the HTTP protocol

    See Definition.

2. A VPN is which of the following?

    a. an implementation of a private network

    b. a network built using frame-relay technology

    c. a high-speed network protocol

    d. a standard way to encrypt files for secure transmission

    See Definition.

3. Corporate networks are now challenged because of which of the following?

    a. computer equipment requires a greater amount of storage space

    b. centrally located computers are consuming greater amounts of electrical power

    c. multiple protocols are taxing existing network resources

    d. the need to support a wide variety of communications across a large geographic area

    See Topic 1.

4. Traditional WAN architecture _____.

    a. is growing because it ideally meets corporate network needs

    b. is a low-cost solution to a wide variety of needs

    c. is less flexible and more costly to implement

d. improves data transmission over long distances

See Topic 2.

5. Remote access modems require which of the following?

a. increased equipment and management resources

b. minimal equipment and network resources

c. no additional long-distance charges

d. that telecommuters use specific remote-access hardware to access the internal network

See Topic 1.

6. ISP–based private networks _____.

a. require entirely new server and internal-network equipment

b. are a cost-effective alternative to traditional WANs

c. increase management costs as a result of additional network equipment

d. are more secure than traditional WANs

See Topic 2.

7. Compared to a single corporation, ISPs tend to have which of the following?

a. fewer remote-access dial-up ports

b. greater diversity in local remote-access points

c. minimal international remote-access capabilities

d. a smaller, more concentrated network backbone

See Topic 1.

8. Compared to a WAN, an ISP–based private network _____.

a. costs more due to the additional cost of a diverse network backbone

b. offers significant cost savings

c. offers a greater level of security and network performance

d. requires a greater number of dedicated leased-line circuits

See Topic 2.

9. Internal network management resources _____.

a. must be increased when using an ISP–based private network, as a result of Internet security issues

b. are still required when using an ISP–based private network to support network technologies including POTS, ISDN, and leased-line circuits

c. can be decreased when using an ISP–based private network due to the outsourcing of network management

d. never change regardless of private-network type

See Topic 2.

10. Traditional WANs are built using which of the following?

a. multiple dial-up links interconnecting each office location

b. short leased-line circuits connecting each office to its closest neighbor

c. inexpensive wireless network–transmission technologies

d. expensive, distance-sensitive leased-line circuits

See Topic 3.

11. International WANs are which of the following?

a. extremely expensive as a result of distance-sensitive leased-line circuits

b. impossible to build using traditional WAN technologies

c. inexpensive because corporations can share network costs with other corporations

d. built using satellite technology, which limits network performance

See Topic 2.

12. Encryption-based VPNs _____.

a. use the public Internet infrastructure to create a VPN

b. use inexpensive hardware to encrypt data traveling across the Internet

c. are more secure than traditional WANs due to data encryption

d. are not susceptible to Internet weaknesses and outages

See Topic 4.

13. Encryption-based VPNs _____.

a. require encryption hardware only at the primary headquarters location

b. cannot accommodate dial-up remote-access users

c. require an encryption equipment at each location of the network

d. aggregate network traffic through a central location

See Topic 4.

Glossary

ISP
Internet service provider

ISDN
integrated services digital network

IT
information technology

LEC
local exchange carrier

POP
point of presence

POTS
plain old telephone service

PVC
permanent virtual circuit

VPN
virtual private network

WAN
wide-area network