Virtual Private Networks (VPNs)

Definition

An Internet-based virtual private network (VPN) uses the open, distributed infrastructure of the Internet to transmit data between corporate sites.

Overview

This tutorial addresses the basic architecture and enabling technologies of a VPN. The benefits and applications of VPNs are also explored. Finally, this tutorial discusses strategies for the deployment and implementation of VPNs.

Topics

1. Introduction

Businesses today are faced with supporting a broader variety of communications among a wider range of sites even as they seek to reduce the cost of their communications infrastructure. Employees are looking to access the resources of their corporate intranets as they take to the road, telecommute, or dial in from customer sites. Plus business partners are joining together in extranets to share business information, either for a joint project of a few months' duration or for long-term strategic advantage.

At the same time, businesses are finding that past solutions to wide-area networking between the main corporate network and branch offices, such as dedicated leased lines or frame-relay circuits, do not provide the flexibility required for quickly creating new partner links or supporting project teams in the field. Meanwhile, the growth of the number of telecommuters and an increasingly mobile sales force is eating up resources as more money is spent on modem banks, remote-access servers, and phone charges. The trend toward mobile connectivity shows no sign of abating; Forrester Research estimated that more than 80 percent of the corporate workforce would have at least one mobile computing device by 1999.

VPNs using the Internet have the potential to solve many of these business networking problems. VPNs allow network managers to connect remote branch offices and project teams to the main corporate network economically and provide remote access to employees while reducing the in-house requirements for equipment and support.

Rather than depend on dedicated leased lines or frame relay's permanent virtual circuits (PVCs), an Internet-based VPN uses the open, distributed infrastructure of the Internet to transmit data between corporate sites. Companies using an Internet VPN set up connections to the local connection points (called points-of-presence [POPs]) of their Internet service provider (ISP) and let the ISP ensure that the data is transmitted to the appropriate destinations via the Internet, leaving the rest of the connectivity details to the ISP's network and the Internet infrastructure. Because the Internet is a public network with open transmission of most data, Internet-based VPNs include measures for encrypting data passed between VPN sites, which protects the data against eavesdropping and tampering by unauthorized parties.

In addition, VPNs are not limited to corporate sites and branch offices. As an added advantage, a VPN can provide secure connectivity for mobile workers. These workers can connect to their company's VPN by dialing into the POP of a local ISP, which reduces the need for long-distance charges and outlays for installing and maintaining large banks of modems at corporate sites.

2. Benefits of VPNs

While VPNs offer direct cost savings over other communications methods (such as leased lines and long-distance calls), they can also offer other advantages, including indirect cost savings as a result of reduced training requirements and equipment, increased flexibility, and scalability.

First and foremost are the cost savings of Internet VPNs when compared to traditional VPNs. A traditional corporate network built using leased T1 (1.5–Mbps) links and T3 (45–Mbps) links must deal with tariffs that are structured to include an installation fee, a monthly fixed cost, and a mileage charge, adding up to monthly fees that are greater than typical fees for leased Internet connections of the same speed.

Leased Internet lines offer another cost advantage because many providers offer prices that are tiered according to usage. For businesses that require the use of a full T1 or T3 only during busy times of the day but do not need the full bandwidth most of the time, ISP services, such as burstable T1, are an excellent option. Burstable T1 provides on-demand bandwidth with flexible pricing. For example, a customer who signs up for a full T1 but whose traffic averages 512 kbps of usage on the T1 circuit will pay less than a T1 customer whose average monthly traffic is 768 kbps.

Because point-to-point links are not a part of the Internet VPN, companies do not have to support one of each kind of connection, further reducing equipment and support costs. With traditional corporate networks, the media that serve smaller branch offices, telecommuters, and mobile works—digital subscriber line (xDSL), integrated services digital network (ISDN), and high-speed modems, for instance—must be supported by additional equipment at corporate headquarters. In a VPN, not only can T1 or T3 lines be used between the main office and the ISP, but many other media can be used to connect smaller offices and mobile workers to the ISP and, therefore, to the VPN without installing any added equipment at headquarters. A company's information technology (IT) department can reduce wide-area network (WAN) connection setup and maintenance by replacing modem banks and multiple frame-relay circuits with a single wide-area link that carries remote user, local-area network to local-area network (LAN–to–LAN), and Internet traffic at the same time.

VPNs can also reduce the demand for technical support resources. Much of this stems from standardization on one type of connection Internet protocol (IP) from mobile users to an ISP's POP and standardized security requirements. Outsourcing the VPN to a service provider can also reduce your internal technical-support requirements, because the service providers take over many of the support tasks for the network.

3. VPN Technologies: Part I

Two primary concerns when deploying VPNs over the Internet are security and performance. The transmission control protocol (TCP)/IP and the Internet were not originally designed with either of these concerns in mind, because the number of users and the types of applications originally did not require either strong security measures or guaranteed performance.

But if Internet VPNs are to serve as reliable substitutes for dedicated leased lines or other WAN links, technologies for guaranteeing security and network performance must be added to the Internet. Fortunately, standards for network data security on IP networks have evolved to where IP networks can be used to create VPNs. Work on providing guaranteed performance is at an earlier stage of development, with service providers not yet deploying these technologies to any great degree as of yet.

VPNs need to provide the following four critical functions to ensure security for data:

- **authentication**—ensuring that the data originates at the source that it claims

- **access control**—restricting unauthorized users from gaining admission to the network

- **confidentiality**—preventing anyone from reading or copying data as it travels across the Internet

- **data integrity**—ensuring that no one tampers with data as it travels across the Internet

Various password-based systems, and challenge-response systems—such as challenge handshake authentication protocol (CHAP) and remote authentication dial-in user service (RADIUS)—as well as hardware-based tokens and digital certificates can be used to authenticate users on a VPN and control access to network resources. The privacy of corporate information as it travels through the VPN is guarded by encrypting the data.

In the past, private networks were created by leasing hard-wired connections between sites; these connections were devoted to the traffic from a single corporate customer. In order to extend that concept to the Internet, where the traffic from many users usually passes over the same connection, a number of protocols have been proposed to create tunnels. Tunneling allows senders to encapsulate their data in IP packets that hide the underlying routing and switching infrastructure of the Internet from both senders and receivers. At the same time, these encapsulated packets can be protected against snooping by outsiders using encryption techniques.

In VPNs, *virtual* implies that the network is dynamic, with connections set up according to the organizational needs. It also means that the network is formed logically, regardless of the physical structure of the underlying network (the Internet, in this case). Unlike the leased lines used in traditional corporate networks, VPNs do not maintain permanent links between the end points that make up the corporate network. Instead, when a connection between two sites is needed, it is created; when the connection is no longer needed, it is torn down, making the bandwidth and other network resources available for other uses. Thus the connections making up a VPN do not have the same physical characteristics as the hard-wired connections used on the LAN, for instance.

Tunnels can consist of two types of end points, either an individual computer or a LAN with a security gateway, which might be a router or firewall. Only two combinations of these end points, however, are usually considered in designing VPNs. In the first case, LAN–to–LAN tunneling, a security gateway at each end point serves as the interface between the tunnel and the private LAN. In such cases, users on either LAN can use the tunnel transparently to communicate with each other.

The second case, that of client–to–LAN tunnels, is the type usually set up for a mobile user who wants to connect to the corporate LAN. The client, i.e., the mobile user, initiates the creation of the tunnel on his end in order to exchange traffic with the corporate network. To do so, he runs special client software on his computer to communicate with the gateway protecting the destination LAN.

4. VPN Technologies: Part II

Four different protocols have been suggested for creating VPNs over the Internet: point-to-point tunneling protocol (PPTP), layer-2 forwarding (L2F), layer-2 tunneling protocol (L2TP), and IP security protocol (IPSec).

One reason for the number of protocols is that, for some companies, a VPN is a substitute for remote-access servers, allowing mobile users and branch offices to dial into the protected corporate network via their local ISP. For others, a VPN may consist of traffic traveling in secure tunnels over the Internet between protected LANs. The protocols that have been developed for VPNs reflect this dichotomy. PPTP, L2F, and L2TP are largely aimed at dial-up VPNs, while IPSec's main focus has been LAN–to–LAN solutions.

One of the first protocols deployed for VPNs was PPTP. It has been a widely deployed solution for dial-in VPNs since Microsoft included support for it in RRAS for Windows NT Server 4.0 and offered a PPTP client in a service pack for Windows 95. Microsoft's inclusion of a PPTP client in Windows 98 practically ensures its continued use for the next few years, although it is not likely that PPTP will become a formal standard endorsed by any of the standards bodies (like the Internet Engineering Task Force [IETF]).

The most commonly used protocol for remote access to the Internet is point-to-point protocol (PPP). PPTP builds on the functionality of PPP to provide remote access that can be tunneled through the Internet to a destination site. As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP the flexibility of handling protocols other than IP, such as Internet packet exchange (IPX) and network basic input/output system extended user interface (NetBEUI).

Because of its dependence on PPP, PPTP relies on the authentication mechanisms within PPP, namely password authentication protocol (PAP) and CHAP. Because there is a strong tie between PPTP and Windows NT, an enhanced version of CHAP, MS–CHAP, is also used, which utilizes information within NT domains for security. Similarly, PPTP can use PPP to encrypt data, but Microsoft has also incorporated a stronger encryption method called Microsoft point-to-point encryption (MPPE) for use with PPTP.

Aside from the relative simplicity of client support for PPTP, one of the protocol's main advantages is that PPTP is designed to run at open systems interconnection (OSI) layer 2, or the link layer, as opposed to IPSec, which runs at Layer 3. By supporting data communications at Layer 2, PPTP can transmit protocols other than IP over its tunnels. PPTP does have some limitations. For example, it does not provide strong encryption for protecting data nor does it support any token-based methods for authenticating users.

5. VPN Technologies: Part III

L2F also arose in the early stages of VPN development. Like PPTP, L2F was designed as a protocol for tunneling traffic from users to their corporate sites. One major difference between PPTP and L2F is that, because L2F tunneling is not dependent on IP, it is able to work directly with other media, such as frame relay or asynchronous transfer mode (ATM). Like PPTP, L2F uses PPP for authentication of the remote user, but it also includes support for terminal access controller access control system (TACACS)+ and RADIUS for authentication. L2F also differs from PPTP in that it allows tunnels to support more than one connection.

Paralleling PPTP's design, L2F utilized PPP for authentication of the dial-up user, but it also included support for TACACS+ and RADIUS for authentication from the beginning. L2F differs from PPTP because it defines connections within a tunnel, allowing a tunnel to support more than one connection. There are also two levels of authentication of the user, first by the ISP prior to setting up the tunnel and then when the connection is set up at the corporate gateway. Because L2TP is a layer-2 protocol, it offers users the same flexibility as PPTP for handling protocols other than IP, such as IPX and NetBEUI.

L2TP is being designed by an IETF working group as the heir apparent to PPTP and L2F, designed to address the shortcomings of these past protocols and become an IETF–approved standard. L2TP uses PPP to provide dial-up access that can be tunneled through the Internet to a site. However, L2TP defines its own tunneling protocol, based on the work done on L2F. L2TP transport is being defined for a variety of packet media, including X.25, frame-relay and ATM. To strengthen the encryption of the data it handles, L2TP uses IPSec's encryption methods.

Because it uses PPP for dial-up links, L2TP includes the authentication mechanisms within PPP, namely PAP and CHAP. Similar to PPTP, L2TP supports PPP's use of the extensible authentication protocol for other authentication systems, such as RADIUS. PPTP, L2F, and L2TP all do not include encryption or processes for managing the cryptographic keys required for encryption in their specifications. The current L2TP draft standard recommends that IPSec be used for encryption and key management in IP environments; future drafts of the PPTP standard may do the same.

The last, but perhaps most important protocol, IPSec, grew out of efforts to secure IP packets as the next generation of IP (IPv6) was being developed; it can now be used with IPv4 protocols as well. Although the requests for comment (RFCs) defining the IPSec protocols have already been part of the IETF's standards track since mid-1995, the protocols are still being refined as engineers learn more as more products appear in the marketplace. The question of which methods to employ for exchanging and managing the cryptographic keys used to encrypt session data has taken more than a year to answer. This challenge has been largely resolved and the ISAKMP/Oakley scheme (now also called Internet key exchange [IKE]) is being readied for acceptance as an IETF standard.

IPSec allows the sender (or a security gateway acting on his behalf) to authenticate or encrypt each IP packet or apply both operations to the packet. Separating the application of packet authentication and encryption has led to two different methods of using IPSec, called modes. In transport mode, only the transport-layer segment of an IP packet is authenticated or encrypted. The other approach, authenticating or encrypting the entire IP packet, is called tunnel mode. While transport-mode IPSec can prove useful in many situations, tunnel-mode IPSec provides even more protection against certain attacks and traffic monitoring that might occur on the Internet.

IPSec is built around a number of standardized cryptographic technologies to provide confidentiality, data integrity, and authentication. For example, IPSec uses

- Diffie-Hellman key exchanges to deliver secret keys between peers on a public net
- public-key cryptography for signing Diffie-Hellman exchanges, to guarantee the identities of the two parties and avoid man-in-the-middle attacks

- data encryption standard (DES) and other bulk encryption algorithms for encrypting data
- keyed hash algorithms (HMAC, MD5, SHA) for authenticating packets
- digital certificates for validating public keys

There are currently two ways to handle key exchange and management within IPSec's architecture: manual keying and IKE for automated key management. Both of these methods—manual keying and IKE—are mandatory requirements of IPSec. While manual key exchange might be suitable for a VPN with a small number of sites, VPNs covering a large number of sites or supporting many remote users benefit from automated key management.

IPSec is often considered the best VPN solution for IP environments, as it includes strong security measures—notably encryption, authentication, and key management—in its standards set. Because IPSec is designed to handle only IP packets, PPTP and L2TP are more suitable for use in multiprotocol non–IP environments, such as those using NetBEUI, IPX, and AppleTalk.

6. VPN Solutions

There are four main components of an Internet-based VPN: the Internet, security gateways, security policy servers, and certificate authorities. The Internet provides the fundamental plumbing for a VPN. Security gateways sit between public and private networks, preventing unauthorized intrusions into the private network. They may also provide tunneling capabilities and encrypt private data before it is transmitted on the public network. In general, a security gateway for a VPN fits into one of the following categories: routers, firewalls, integrated VPN hardware, and VPN software.

Because routers have to examine and process every packet that leaves the LAN, it seems only natural to include packet encryption on routers. Vendors of router-based VPN services usually offer two types of products, either add-on software or an additional circuit board with a coprocessor-based encryption engine. The latter product is best for situations that require greater throughput. If you are already using a particular vendor's routers, then adding encryption support to these routers can keep the upgrade costs of your VPN low. But adding the encryption tasks to the same box as the router increases risks—if the router goes down, so does the VPN.

Many firewall vendors include a tunnel capability in their products. Like routers, firewalls must process all IP traffic—in this case, to pass traffic based on the filters defined for the firewall. Because of all the processing performed by firewalls, they are ill-suited for tunneling on large networks with a great deal of traffic. Combining tunneling and encryption with firewalls is probably best used only on small networks with low volumes of traffic. Also, like routers, they can be a single point of failure for a VPN.

Using firewalls to create VPNs is a workable solution—for some networks. Firewall-based VPNs are probably best suited to small networks that transfer small amounts of data (on the order of 1–2–Mbps over a WAN link) and remain relatively static, i.e., do not require frequent reconfiguration.

Another VPN solution is to use special hardware that is designed for the task of tunneling, encryption, and user authentication. These devices usually operate as encrypting bridges that are typically placed between the network's routers and WAN links. Although most of these hardware tunnels are designed for LAN–to–LAN configurations, some products also support client–to–LAN tunneling.

Integrating various functions into a single product can be particularly appealing to businesses that do not have the resources to install and manage a number of different network devices (and also do not want to outsource their VPN operations). A turnkey installation can certainly make the setup of a VPN much easier than installing software on a firewall and reconfiguring a router as well as installing a RADIUS server, for example.

While many of these hardware devices are likely to offer you the best performance possible for your VPN, you will still need to decide how many functions you want to integrate into a single device. Small businesses or small offices without large support staffs (especially those experienced in network security) will benefit from products that integrate all the VPN functions as well as a firewall and perhaps one or two other network services. Some products—usually the more expensive ones—include dual power supplies and failover features to ensure reliability.

It is hard to beat many of these products for throughput and handling large numbers of simultaneous tunnels, which should be crucial to larger enterprises. Also, do not overlook the importance of integrating the control of other network-related functions, such as resource reservation and bandwidth control. Some companies already include these features in their products, and it is a step that will most likely gain more support in the future. Integrating traffic control with authentication and access control also makes sense over the long run, as policy-based network management becomes more prevalent (and useful).

VPN software is also available for creating and managing tunnels, either between a pair of security gateways or between a remote client and a security gateway. These software VPN systems are often good low-cost choices for systems that are relatively small and do not have to process a lot of traffic. These solutions can run on existing servers and share resources with them and they serve as a good starting point for getting familiar with VPNs. Many of these systems are well suited for client-to-LAN connections.

In addition to the security gateway, another important component of a VPN is the security-policy server. This server maintains the access-control lists and other user-related information that the security gateway uses to determine which traffic is authorized. For example, in some systems, access can be controlled via a RADIUS server.

Lastly, certificate authorities are needed to verify keys shared between sites and can also be used to verify individuals using digital certificates. Companies can choose to maintain their own database of digital certificates for users by setting up a corporate certificate server. For small groups of users, verification of shared keys might require checking with a third party that maintains the digital certificates associated with shared cryptographic keys. If a corporate VPN grows into an extranet, then an outside certificate authority may also have to be used to verify users from your business partners.

Self-Test

1. A VPN uses the open, distributed infrastructure of the Internet to transmit data between corporate sites.

    a. true

    b. false

2. One drawback to VPNs is that although they allow network managers to connect to remote-branch offices, they do not enable remote access for individual employees.

    a. true

    b. false

3. VPNs are a bit more expensive than other communications methods (such as leased lines and long-distance calls) but offer more benefits to the user in the long run.

    a. true

    b. false

4. Two primary concerns when deploying VPNs over the Internet are security and performance.

    a. true

    b. false

5. In VPN, virtual implies that the network is static.

    a. true

    b. false

6. VPNs must provide which critical function to ensure security for data?

    a. authentication

    b. access control

    c. confidentiality

    d. data integrity

    e. none of the above

    f. all of the above

7. Among the protocols suggested for creating VPNs over the Internet are the following:

    a. PPTP

    b. L2F

    c. L2TP

    d. IPSec

    e. b and c only

    f. all of the above

8. _____ differs from PPTP in that it allows tunnels to support more than one connection.

    a. L2F

    b. IPSec

c. L2TP

d. none of the above

e. all of the above

9. How can key exchange and management be handled within IPSec's architecture?

   a. manual keying

   b. remote keying

   c. Internet key exchange

   d. all of the above

   e. a and c only

10. What are the main components of an Internet-based VPN?

   a. the Internet

   b. security gateways

   c. security-policy servers

   d. certificate authorities

   e. all of the above

   f. a and b only

Correct Answers

1. A VPN uses the open, distributed infrastructure of the Internet to transmit data between corporate sites.

   a. true

   b. false

   See Topic Definition.

2. One drawback to VPNs is that although they allow network managers to connect to remote-branch offices, they do not enable remote access for individual employees.

   a. true

   b. false

   See Topic 1.

3. VPNs are a bit more expensive than other communications methods (such as leased lines and long-distance calls) but offer more benefits to the user in the long run.

   a. true

   b. false

   See Topic 2.

4. Two primary concerns when deploying VPNs over the Internet are security and performance.

   a. true

   b. false

   See Topic 3.

5. In VPN, virtual implies that the network is static.

   a. true

   b. false

   See Topic 3.

6. VPNs must provide which critical function to ensure security for data?

   a. authentication

   b. access control

   c. confidentiality

   d. data integrity

   e. none of the above

f. all of the above

See Topic 3.

7. Among the protocols suggested for creating VPNs over the Internet are the following:

   a. PPTP

   b. L2F

   c. L2TP

   d. IPSec

   e. b and c only

   f. all of the above

   See Topic 4.

8. _____ differs from PPTP in that it allows tunnels to support more than one connection.

   a. L2F

   b. IPSec

   c. L2TP

   d. none of the above

   e. all of the above

   See Topic 5.

9. How can key exchange and management be handled within IPSec's architecture?

   a. manual keying

   b. remote keying

   c. Internet key exchange

   d. all of the above

   e. a and c only

See Topic 5.

10. What are the main components of an Internet-based VPN?

a. the Internet

b. security gateways

c. security-policy servers

d. certificate authorities

e. all of the above

f. a and b only

See Topic 6.

Glossary

ATM
asynchronous transfer mode

CHAP
challenge handshake authentication protocol

GRE
generic routing encapsulation

IETF
Internet Engineering Task Force

IKE
Internet key exchange

IPSec
Internet protocol security protocol

IPX
Internet packet exchange

ISDN
integrated services digital network

ISP
Internet service provider

IT
information technology

L2F
Layer 2 forwarding

L2TP
Layer 2 tunneling protocol

LAN
local area network

MPPE
Microsoft point-to-point encryption

NetBEUI
network basic input/output system extended user interface

OSI
open systems interconnection

PAP
password authentication protocol

POP
point of presence

PPP
point-to-point protocol

PPTP
point-to-point tunneling protocol

PVC
permanent virtual circuit

RADIUS
remote authentication dial-in user service

TACACS
terminal access controller access control system

TCP/IP
transmission control protocol/Internet protocol

VPN
virtual private network

WAN
wide area network

xDSL
digital subscriber line