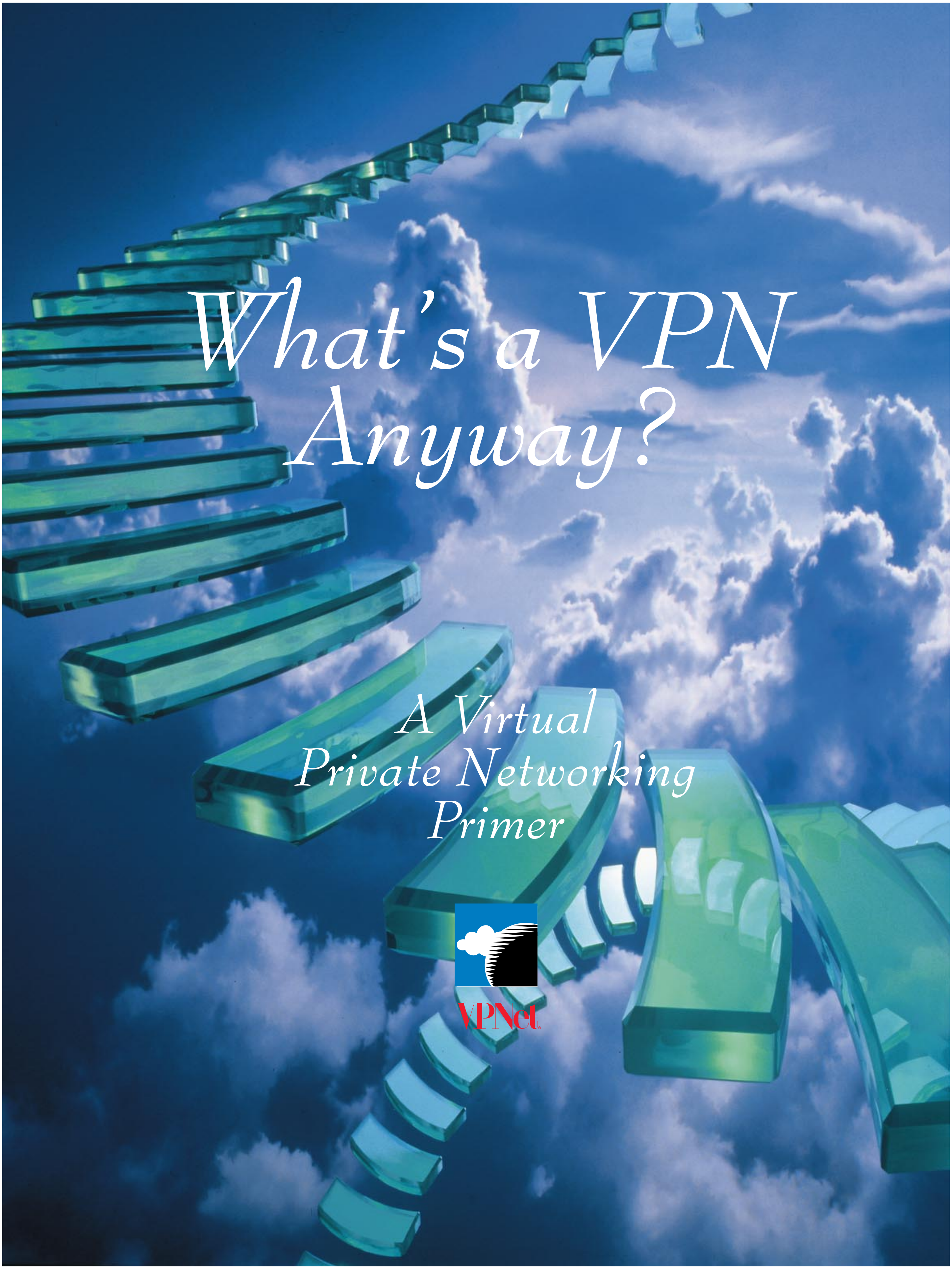

What's a VPN Anyway?

A Virtual Private Networking Primer

VPNet

What's a VPN Anyway?

or

The Cloud's Silver Lining Is Your Net

Table of Contents

Table of Contents
(continued)

By VPNet Technologies

What's a Virtual Private Network anyway?

Virtual Private Networks (VPNs) extend the corporate network out to distant offices, home workers, salespeople, and business partners. But, rather than using expensive dedicated leased lines, VPNs use worldwide IP network services, including the Internet "cloud" and service provider IP backbones. Rather than dialing in at long distance rates, remote users can make a local Internet call.

VPNs allow:

- Network managers to cost-efficiently increase the span of the corporate network
- Remote network users to securely and easily access their corporate enterprise
- Corporations to securely communicate with business partners
- Service providers to grow their businesses by providing substantial incremental bandwidth with value-added services

As with any network deployment, careful planning must precede any VPN implementation. Specifically, this plan must address questions related to connectivity and security. The first step in planning a VPN is to determine the connectivity requirements between corporate offices, telecommuters, and traveling employees (see Figure 1).

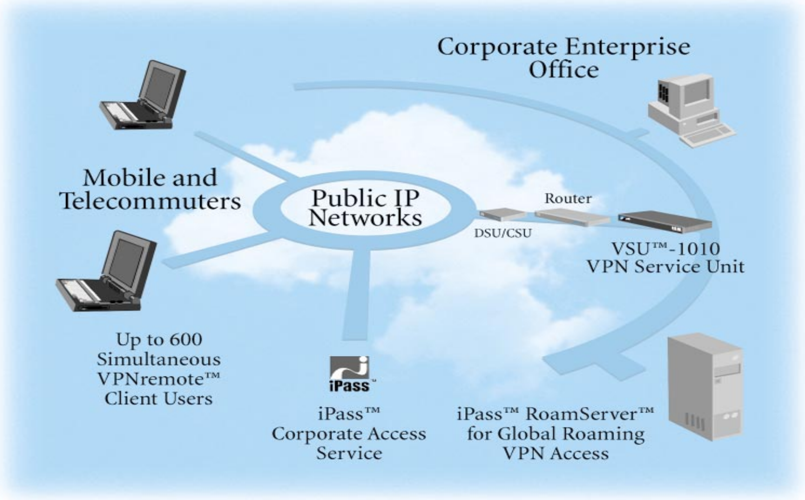
Corporate Enterprise Office
Mobile and Telecommuters
Public IP Networks
Router
DSU/CSU
VSU™-1010 VPN Service Unit
Up to 600 Simultaneous VPNremote™ Client Users
iPass
iPass™ Corporate Access Service
iPass™ RoamServer™ for Global Roaming VPN Access

Figure 1. Virtual Private Network

A VPN can be established that allows any network resource in the branch office to communicate with any network resource in the corporate headquarters. On the other hand, a VPN can be very explicit, allowing an individual network resource in the branch office to connect to only one or two network resources at the corporate headquarters.

Determining which network resources should be linked via a VPN depends on the applications used on the various systems. For example, it is likely that all of the branch office workstations as well as the traveling employees and telecommuters will need access to the corporate office email server. Thus, one VPN might consist of the corporate office email server and all other workstations in the corporate network.

Requirements often used to determine network connectivity include:

- Security policy
- Business models
- Intranet server access
- Application requirements
- Data sharing
- Application server access

VPNs are platform independent. Any computer system that is configured to run on an IP network can be incorporated into a VPN with no modifications required except the installation of remote software. Additionally, VPNs can be implemented between corporations. VPNs that connect two or more corporations' networks are known as extranets. The only difference between a traditional, intra-company VPN (intranet) and an inter-company VPN (extranet) is the way the VPN is managed. With an intranet VPN, all network and VPN resources are managed by a single organization. With an extranet VPN, no single organization has management control over all network and VPN resources; rather, each company manages its own VPN equipment. The extranet VPN configuration process involves first configuring a portion of the VPN and then exchanging with partner VPN management organizations the needed subset of configuration information.

Why should we implement VPNs?

Network managers can save on remote access equipment and connection costs, while providing reliable corporate dial-up access for traveling and telecommuting employees. Network managers can also replace expensive leased line connections to remote offices and connect all remote offices to the corporate network at substantial savings.

How much can we save?

Savings are typically 20 to 40% for site-to-site domestic networks, more internationally, and 60 to 80% for traveling and telecommuting employee access. In addition to saving on-line charges, WAN equipment and personnel costs are dramatically less expensive with a VPN solution.

What are other less-apparent costs of WANs over leased lines?

The real cost of corporate dial-up connections includes a load on the network staff:

- Buying, installing, and configuring remote access servers and modem racks
- Working with telephone companies to install lines
- Installing new client software on laptops
- Monitoring traffic patterns on remote access ports
- Supplying sufficient ports for increasing numbers of telecommuters
- Monitoring and paying for dial-up telephone charges
- Keeping up with fast-changing technology

The costs of installing and managing VPNs should be viewed in relation to these “soft” costs, as well as the more obvious costs for lines and equipment.

What other benefits do VPNs offer?

Besides lowering costs, VPNs provide access from anywhere the Internet reaches. Internet points of presence are available worldwide, providing potential VPN connection points in nearly every country and in most of the major cities of the world. Most importantly, VPNs enable rich, flexible communications with customers, suppliers, and business partners over extranets. These allow users to establish interactive links with every business partner—not just a few. The expensive dedicated network is no longer a necessity. Instead, VPN technology creates a secure communications ring that members may join at a moment’s notice. So beyond the tactical cost savings, extranets are strategic: they change the way people communicate much the same way as fax, voice mail, and e-mail have in the past.

Why can't we use just the Internet for our business communications?

In spite of the positive worldwide revolution produced by the Internet, the following problems still exist on the Net:

- Reliability
- System maintenance
- Access problems
- Security

The Internet was not designed with high security in mind. For corporations to entrust it with their most sensitive data, some additional work must be done to assure that the right people are accessing the corporation's networks and that outsiders cannot read transient data.

What are the relative merits of a VPN over the Internet vs. over a private IP backbone?

Many service providers offer VPN services over private IP backbones. While these VPNs may be limited to subscribers of the service provider network, they offer more predictable and controllable performance than today's Internet. The public Internet offers ubiquitous access and low cost.

Private IP backbones can provide VPNs with levels of quality of service (QoS). With the appropriate mix of services, enterprise network managers can develop an outsourced WAN strategy that meets a range of cost and performance needs. The Internet was not designed to deliver performance guarantees. Applications designed to work with a guaranteed network latency may not perform adequately on the Internet.

What standards exist to ensure compatibility between vendors?

The most popular emerging VPN standards are PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security). The PPTP, L2TP, and IPSec specifications are sets of requests for comment (RFCs) to the IETF (Internet Engineering Task Force) that describe protocols to be used for tunneling. All are proposed for inclusion in IP protocol, IPv6. IPSec is already being implemented in IPv4. PPTP was driven by Microsoft and Ascend to support packet tunneling in Ascend's remote access server hardware and Microsoft's NT software. The backers of the PPTP protocol combined efforts with Cisco and its L2F protocol to produce a hybrid called L2TP. IPSec is a general initiative to add security services to the IP protocol. A growing number of VPN, security, and major network companies—over 30 as of October 1997—either support or plan to support IPSec. The International Computer Security Association (ICSA) and Automotive Network eXchange® (ANX®) are spearheading IPSec interoperability testing. Of the three standards, IPSec is the only protocol being driven by major network users.

IPSec is the preferred solution for IP environments because it has security built in. PPTP and L2TP are most appropriate for multiprotocol environ-ments, but both require additional support to deliver data privacy, integrity, and authentication. Unless augmented with IPSec, PPTP and L2TP cannot support extranets because extranets require keys and key management.

How can we be sure that equipment from different vendors will be compatible in an extranet?

The best way to ensure that equipment from different vendors will work together in an extranet is to choose VPN equipment that has been certified to be IPSec compliant. The ICSA IPSec Certification Program has the objective to enable multi-vendor VPNs on the Internet that can provide interoperability along with the security functions of data source authentication, data integrity, and confidentiality.

Who is the ISCA?

Established in 1989, the International Computer Security Association (ICSA) develops security products through its product certification program and establishes better security practices through management of security-focused consortia. ICSA is an independent organization that strives to improve security and confidence in global computing through awareness and the continuous certification of products, systems, and people. As a member-oriented organization, ICSA fosters the exchange of knowledge among three constituent groups: users of computer systems, developers of computer products, and experts in computer security. As a service organization, ICSA applies its unique Risk Framework and Continuous Certification Model to reduce risk and improve computer security products.

What is the ANX?

The Automotive Network eXchange (ANX) is a TCP/IP (Transmission Control Protocol/Internet Protocol) network service allowing for efficient and secure electronic communication among automotive trading partner subscribers and delivered by interconnected certified Internet Service Providers and certified network Exchange Points. When completed, the ANX will provide automotive trading partners a single, secure, standards-based network for electronic commerce and data transfer. It will replace complex, redundant, and costly multiple connections that exist throughout the automotive supply chain. The ANX will be the world's largest business extranet.

What are the security requirements of VPNs?

Security is the central issue for VPN applications. Some VPN technologies have security built in (as part of their IETF specification); others require one or more add-ons. To meet corporate standards, VPN communications must be:

- **Guarded from prying eyes** – Data privacy is provided using encryption. Encryption uses complex mathematical transformations in which the original data is combined with a logical key and later decrypted by the receiver using the same key. Managing the keys is the most critical and difficult aspect of encryption systems. Any viable VPN solution must have a key management mechanism to negotiate and exchange secret encryption keys in a secure manner.

- **Safe from tampering** – Data tampering is thwarted by using mathematical transformations called hashing functions that create fingerprints used to detect altered data.

- **Spoof-proof** – User authentication prevents one user from masquerading as another. The ability to positively authenticate network users is vital to ensuring VPN security. Password protection is easily circumvented and thus inherently insecure. However, X.509 digital certificates provide stronger authen-tication and more reliable performance.

To avoid severe performance degradation, all security measures—encryption, hashing, authentication, and key management—must be performed on VPN systems that are optimized for these functions.

What factors determine the performance of a VPN?

Performance of VPNs is determined by two factors:

- The speed of transmissions over either the Internet or a public IP backbone network
- The efficiency of VPN processing at each end of the connection

Encapsulation requires adding information to each packet, which increases the packet size. This in turn increases the likelihood that internetwork routers will find the packets oversized and fragment them, further degrading performance. Packet fragmentation and data encryption can reduce dial-in system performance to unacceptable levels. Data compression can help solve this problem. However, the combination of compression and encapsulation requires additional computational power beyond that needed for security.

Should we implement hardware- or software-based VPNs?

Because of the computational power required to implement VPNs, hardware-based VPN products deliver the best performance. They also offer tighter physical and logical security. Software-based solutions are best suited for lower-volume connections at small- and medium-sized companies that have lower security requirements. High volumes of traffic with maximum security solutions require dedicated hardware.

Router and server add-ons such as encryption cards may be limited in performance because they depend on the performance of the device to which they attach. Standalone devices are designed to be more scalable, which means they can accommodate increasing bandwidth demand, more VPNs, and higher-speed lines.

Encryption is processor intensive. Whereas a router needs to only process the packet header, an encrypting process operates on each byte in the packet. Triple DES encryption, for example, requires 50 to 100 times more processing power than straight IP routing. Thus, when performance is a concern, standalone hardware-based solutions provide a critical advantage.

What are trusted and untrusted networks?

Trusted networks are comprised of workstations in which the users are given open access to other systems with little concern about sabotage or abuse. Untrusted networks are comprised of workstations in which unknown or untrusted users could sabotage or abuse access to an organization's network resources. Therefore, the Internet is an untrusted network for most corporate traffic, and the potential for abuse prevents many corporations from using the Internet to connect corporate offices without using the cryptographic security inherent in VPNs. Public WANs that some consider trusted do exist, however. They include the Public Switched Telephone Network (PSTN) and networks such as Frame Relay and X.25 that are provided by the major telecommunications carriers. But in reality, these WANs are accessible by hundreds or even thousands of users and should be considered untrusted. While corporations depend on the free exchange of information and shared resources, portions of a corporate LAN must sometimes be secured from unauthorized internal access. After identifying the trusted and untrusted portions of a corporate network, the next step is to decide how to interconnect the various trusted networks. VPNs provide the capability of interconnecting trusted networks via an untrusted network.

What is member and non-member traffic?

Member traffic is defined as IP traffic where the source and destination workstations are within a VPN. Non-member traffic is defined as all other IP traffic (i.e., traffic to network resources that are not in a VPN). To determine how non-member traffic should be handled, each trusted network should be analyzed to ascertain the types of traffic flowing in and out of the network.

What is non-IP traffic?

Non-IP traffic includes protocols such as IPX, DecNet, SNA, and AppleTalk. By definition, non-IP traffic cannot be part of a VPN because it is not IP-based. Thus, non-IP traffic should always be treated as non-member traffic and must be handled by access control components such as router filters or firewalls. Note: Some WANs such as the Internet are "natural" non-IP traffic filters. Since the Internet can only route IP traffic, non-IP traffic cannot be transported across the Internet unless it is encapsulated in IP. Therefore, if the Internet is used to connect trusted networks via VPNs, it is not necessary to implement non-IP traffic filters. The Internet itself will filter non-IP traffic.

How are remote users authenticated?

Remote access allows traveling or telecommuting employees to access corporate network resources from outside the company campus. Authorized remote users are allowed access, while unauthorized users are denied access.

When using VPNs for remote access, each remote access user account must be configured with the cryptographic algorithms and keys used for encryption and authentication. Without the proper keys, a user cannot remotely access a corporate network using VPNs. Thus, user authentication can be achieved simply by careful distribution and control of VPN cryptographic keys. For many networks, this level of user authentication is sufficient.

If the inherent user authentication mechanism of VPNs is not sufficient, additional methods can also be employed. The simplest method is to require a user ID and password each time a user connects to the corporate network via a VPN. The weakness in this approach lies in the choice of passwords. Many users choose easy-to-remember passwords (such as their names, birth dates, spouse's name, etc.) which are easy to guess. If such easily guessed passwords are prohibited, users may write down their password, thus compromising the user authentication mechanism.

One solution to this problem is "two-factor" user authentication. The two factors usually refer to "something you have, and something you know." The "something you know" factor is typically a login ID or Personal Identification Number (PIN), similar to the information used in the login/password mechanism. The "something you have" factor corresponds to a device that generates a value, based on factors such as time, or an input phrase called a "challenge." An example of "something you have" is a SecurID card, which generates random token values every 60 seconds. The token value is generated in a cryptographically secure manner and changes from one use to the next, thus preventing the use of a previous value for future authentication. In order to compromise the two-factor mechanism, an attacker must know the login and must have the token device. Two-factor authentication mechanisms also can be used with the Remote Authentication Dial-In User Service (RADIUS) protocol. Typically, a secondary server for the given two-factor mechanism works in conjunction with the RADIUS server. In these scenarios, a VPN device accesses the RADIUS server, and the RADIUS server accesses the two-factor authentication server.

How do we choose VPN services?

Choosing VPN services can be a simple process for most networks. Most applications will use Triple DES encryption and compression. Variations to these services may be required for the following applications:

- **International VPNs** – With few exceptions, the United States government currently restricts export of cryptographic algorithms with the security strength of Triple DES. Therefore, Triple DES cannot be used as a VPN service for any VPNs that cross U.S. borders. The alternative in this case is 56-bit DES.

- **Network compression** – Some networks may implement compression prior to the application of VPN services. For these networks, use of VPN compression services is redundant. By disabling compression, a slight performance improvement may be achieved.

- **Observable traffic** – While one of the major benefits of a VPN is data privacy, there may be occasions when the ability to monitor packet payloads is needed. Examples include news reports, stock quotes, or other public information where secrecy may not be vital, but data alteration is disastrous. For these applications, compressing or encrypting packets is not desirable; however, data authenticity is still desired. Note: Authentication does not modify the packet payload.

What tools are needed to manage a VPN?

Implementing and using VPNs should be as transparent as possible for users, network managers, and service providers. VPNs must include tools for the network manager and service providers to manage security, performance, and costs. Both enterprise network managers and service providers must be able to:

- Install and provision equipment in a secure fashion.
- Scale the VPN when the requirements grow beyond its current capabilities.
- Track problems beyond their own borders. For the network manager, this means across the outsourced WAN. For the service provider, this means across multiple subscriber networks.
- Establish extranet relationships with a variety of business partners.

Over time, the quality, completeness, and security of VPN management tools will play a dominant role in the effectiveness of any VPN implementation.

How should tasks be split between network managers and service providers?

Service providers can take many different approaches to their VPN offerings. For example, they may simply supply the Internet or IP network bandwidth needed to handle VPN traffic. Alternatively, service providers can offer more products and services, including design, management, service, and training for the corporate VPN. Flexible service providers will offer a range of VPN service options so that the corporate network manager can outsource all functions determined to be cost effective for business and security requirements. Some selected VPN service offerings for service providers may include:

- Selling basic Internet access and bandwidth; the enterprise customer handles all VPN products and operations.
- Selling business-quality Internet or IP network services; the enterprise customer handles all VPN products and operations.
- Selling compulsory VPNs embedded in POP equipment.
- Offering VPN hardware and software bundled with VPN bandwidth and services.
- Designing the customer's VPN solution.
- Operating the total VPN solution for the customer, including design, equipment installation and service, and help desk support (100% outsource).

Network managers need to determine how much of the implementation tasks they want to off load to the service provider. Security may have to be kept in-house, while costly help desk services may be off-loaded to the service provider. In-house security may require that the network management staff include a security expert.

Some VPN implementations cannot be achieved without involving the service provider. IPSec and voluntary mode of PPTP handle all VPN operations at the end points and are thus transparent to the service provider. PPTP requires service provider participation to establish a VPN connection when compulsory mode is used.

Network managers who want to do it all should find a service provider that can provide low-cost, high bandwidth at service levels that meet corporate needs. If VPN services are to be outsourced, the network manager should find a reliable full-service provider. VPNs are about partnerships, and the most important VPN partnership for many organizations will be the one they establish with their VPN service provider.

What is the VPNware™ System?

The VPNware System is an integrated family of VPN hardware and software that takes the guesswork out of purchasing and deploying VPNs. VPNware Systems offer enterprises the benefits of VPNs at the lowest price per user of any system currently on the market. The VPNware System includes all of the necessary components for deploying VPNs:

- One or more VPNware Service Units (VSUs), for IPSec-based VPN support for 25 to 2400 concurrent users.
- A VPNmanager™ tool, for Web-based, VPN-centric configuration and management of single-site VPNs with up to 100 remote users or of multi-site VPNs with unlimited remote users.
- A multi-user license for VPNremote™ Client Software for Windows 95 or Windows NT, enabling VPN access for traveling employees or telecommuters.
- RoamServer™ from iPass™ Inc., the leading provider of global Internet roaming services, for local access to VPNware VPNs from more than 150 countries worldwide.

How do we integrate VPNware solutions into our corporate network?

To implement a VPNware solution, a network manager must understand Internet Protocol (IP) networking concepts, as well as the functionality of VPNet's VPNware Service Units (VSUs), VPNremote Client Software, and VPNmanager Tool Suite. VSUs must be configured to work with existing equipment. Most networking equipment requires little or no modification to work with VSUs. However, some products, such as filters within routers, firewalls, and Network Address Translation (NAT) devices, will require careful configuration in order to coordinate their operation with VSUs. In general, any network device that uses or modifies IP layer information within a packet will require careful configuration.

Where do we install VPNware Service Units in a network?

VPNware Service Units (VSUs) are physical devices that provide transparent VPN services by processing IP packets on a trusted network before the packets reach an untrusted network.

Inline VSU Placement

The typical placement of a VSU is inline, on the link between the trusted and untrusted network; specifically, in the direct path of packets transferred to or from the untrusted network. An example network showing VSUs installed in a simple inline configuration is shown in Figure 2.

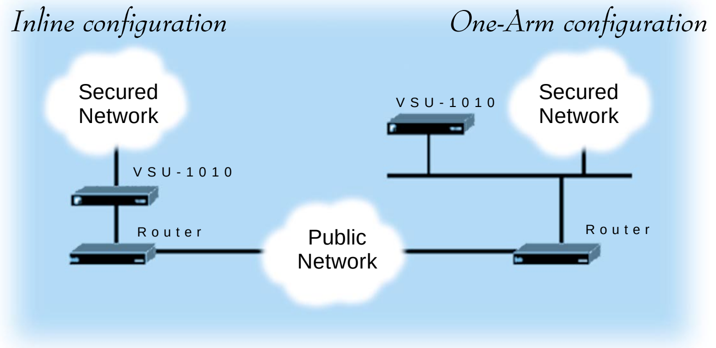

Figure 2. VSU Placement

While the example network is simple, it is typical of many corporate networks. For more complicated networks with multiple links to the public network, it is important to maintain VPN traffic symmetry. That is, outbound VPN packets and inbound replies should be routed through the same VSU.

One-Arm Configuration

When inline placement of VSUs is not preferred, VSUs can be configured as a network node, similar to a workstation or host. Configuring a VSU as a network node is called "one-arm configuration." An example of one-arm network configuration for a VSU is also shown in Figure 2.

The main advantages of using a one-arm configuration are load balancing and scaling to thousands of simultaneous VPNs with VPNremote clients. The one-arm configuration is only possible using the VSU-1010 or VSU-10. Also, note that the one-arm configuration for site-to-site operation requires modifying the router configuration. Contact VPNet technical support for assistance in configuring your router for one-arm site-to-site operation.

When Used with a Network Address Translator (NAT)

Two of the most popular applications of NAT are to hide corporate network addresses and to use private network addressing schemes. Both of these applications require that IP layer information (specifically the source address) within a packet be changed before delivery to a public network such as the Internet. If a NAT device performs address translation on a VPN packet, the address change will be detected as an unauthorized change and the packet will be dropped, thus making communications impossible. Therefore, to use NAT with VPNs, the following two rules must be observed:

- For outbound clear text packets that are part of a VPN, the NAT device must modify the packet before VPN services are applied to the packet.
- For inbound VPN traffic, the NAT device must modify the packet after VPN services have been removed from the packet.

The VSU-1010 and VSU-10 include NAT functionality, thus eliminating the need for an external NAT device. If an external NAT device is required, it should be placed on the private network side of the VSU.

In Relationship to a Remote Access Server (RAS)

One of the primary applications of VPNs is to provide traveling or telecommuting employees with secure remote access into a corporate network. VPNs meet many of the remote access requirements of a corporate network previously handled by traditional remote access devices (e.g., RAS). However, some corporations may have requirements that can only be met using a RAS. For these situations, VPNs can be used in conjunction with a RAS to provide an additional layer of security for employees accessing the corporate network over the PSTN. A traveling employee would still use VPNremote Client Software, and a VSU would be placed within the corporate network. The VSU would need to be placed after the RAS so that traffic from remote users would pass from the RAS, through the VSU, and on to the corporate LAN.

When Used with Frame Relay

Many corporations use Frame Relay to connect their various offices. Like the PSTN, Frame Relay networks are considered private by nature; however, many Frame Relay networks are not guaranteed to be private and do not have data security. Consequently, the potential exists for attackers to monitor and modify traffic traveling across such networks. VPNs can be used in conjunction with Frame Relay to provide an additional layer of security. All of the same actions and techniques used to deploy a VPN across the Internet are applicable to deploying a VPN over Frame Relay.

Who is VPNet?

VPNet Technologies, Inc. was the first company formed with a singular focus on VPNs and is the only company providing end users and service providers a complete and flexible spectrum of VPN solutions. Founded in October 1995 and based in San Jose, California, the company develops and markets cost-effective products and technologies for implementing high-performance virtual private networks. VPNet's scalable VPLink™ architecture delivers the highest levels of security, performance, and manageability across a wide range of VPN applications. Customers wanting more information about VPNet products and technologies can contact the company at 1-888-VPNET-88 or visit its World Wide Web site at www.vpnet.com.

Glossary

Authentication

Authentication is a cryptographic function that verifies user authorization and ensures data integrity. User authentication is a method of verifying a user's identity by challenging the user to provide secret information known only to the user and the authenticating system. Data authentication ensures that individual packets are not modified in transit.

Compression

When IP data is being encrypted or authenticated, additional header information must be added to the original IP packet. This increases the size of the packet a modest amount and can reduce performance; compression mitigates or eliminates this problem. Data compression is not a cryptographic function like encryption and authentication. However, compression is highly desirable for VPNs that use IPSec encryption and/or authentication.

Encryption

Encryption is a cryptographic function that ensures data privacy. Encrypted data cannot be read by intermediary observers in an untrusted network, but can be decrypted and read by the intended recipients who have the appropriate key for decrypting the data.

Filtering routers

Many routers have the capability to enforce access control on the traffic they route. Access control or filtering is a function whereby the IP layer information in a packet is examined to determine if the packet should be routed. The IP layer information can be used to determine the source and destination address or protocol type (i.e., Telnet or HTTP traffic) as well as other information about the packet. As an example, many corporations use filters within their Internet gateway router to allow only HTTP and SMPT traffic from the Internet to access the corporation's public web site and email, while at the same time allowing any type of traffic out to provide employees with the ability to use Telnet, FTP, and web browsing services. With such a filter in place, Internet users can access the corporate public web site, but cannot Telnet into any corporate resources. This provides a degree of security required by many companies.

Firewall

A firewall is a device (or software in a router) that links an organization's internal TCP/IP network to the Internet and restricts the types of traffic that it will pass, to provide security. Restrictions can be based on the type of access (email, Telnet, FTP, etc.), contents of the data accessed, direction, source or destination IP address, and time of day.

Integrated Services Digital Network (ISDN)

ISDN is a standard for simultaneous transmission of voice, video, and data represented in digital form. The most common configuration includes two voice and one signaling channel over existing copper wire line pairs.

Internet service provider (ISP)

An ISP is a company that provides access to the Internet through various telecommunications options, including modems, leased lines, ISDN, and Frame Relay. Large ISPs have their own high-speed backbones with a regional or national scope.

Internet

The Internet is a worldwide network of networks that connects universities, governments, businesses, and individuals around the world.

IPSec

IPSec is an IETF standard created to add security to TCP/IP networking. It is a collection of security measures that address data privacy, integrity, authentication, key management, and tunneling.

L2TP

The backers of PPTP combined efforts with Cisco and its L2F protocol to produce a hybrid layer 2 tunneling protocol called L2TP (Layer 2 Tunneling Protocol). PPTP and L2TP operate at layer 2 of the OSI network model. Layer 2 tunneling has the advantage of simplicity.

Latency

The time that passes between a command being sent to the time that a response is received. On a wide area network, latency is due to delays in routers or switches, congestion on a crowded backbone, and the time for electrons to travel between nodes on a WAN.

Leased line

A leased line is a point-to-point dedicated circuit that is not switched. Unlike Frame Relay or Internet-based technologies, the bandwidth on a leased line is not shared by multiple customers but rather is made available to and reserved for a client on a contractual basis with associated monthly fees.

Multipoint tunneling

Multipoint tunneling allows an Internet session at the same time as several VPN sessions.

Packet-based network

A packet-based network divides traffic into small blocks with destination addresses. Various paths can be taken to avoid overloading any one path on the network.

Permanent virtual connection (PVC)

A PVC is a logical connection between two sites on a digital switched network. The PVC defines parameters about the logical link, such as direction and speed, but not the physical path that the data will travel to get from one site to the other.

Point of presence (POP)

A site that has a collection of telecommunications equipment; usually refers to ISP or telephone company sites.

PPTP

PPTP is a point-to-point tunneling protocol created to support packet tunneling in Ascend's remote access server hardware and Microsoft's NT software.

RADIUS

Remote Authentication Dial-In User Service, or RADIUS, is the standard for centralizing the authentication, authorization, and accounting of remote access users. With RADIUS, a network manager or ISP need only maintain a single, central database used to authenticate remote users. This greatly eases the management burden associated with administering large numbers of dial-in users.

Tunneling (IP)

Tunneling is the encapsulation of point-to-point transmissions inside IP packets. PPTP and L2TP are tunneling protocols; IPSec is a collection of IP security measures that define standards for creating and managing encrypted tunnels for privacy, data integrity, and authentication. These tunneling methods differ in what they do to the data (encryption and authentication), their headers that describe the data transmission and packet handling, and the OSI layer at which they operate.

VPNet Technologies
1530 Meridian
San Jose, CA 95125

1-888-VPNET-88

or visit

www.vpnet.com

VPNet