

Contents

Chapter 1: Introduction

- <u>Introduction</u>	<u>2</u>
- <u>Definition</u>	<u>2</u>
- <u>What makes a VPN</u>	<u>2</u>

Chapter 2: Virtual Private Network Technologies

- <u>VPN Solution Components</u>	<u>4</u>
- <u>VPN Technologies</u>	<u>4</u>
- <u>Protocols</u>	<u>5</u>
- <u>Pros and Cons</u>	<u>7</u>
- <u>References</u>	<u>8</u>

CHAPTER 1

Introduction

The world has changed a lot in the last couple of decades. Instead of simply dealing with local or regional concerns, many businesses now have to think about global markets and logistics. Many companies have facilities spread out across the country or around the world, and there is one thing that all of them need: A way to maintain fast, secure and reliable communications wherever their offices are. Until fairly recently, this has meant the use of leased lines to maintain a wide area network (WAN). Leased lines, ranging from ISDN (integrated services digital network, 128 Kbps) to OC3 (Optical Carrier-3, 155 Mbps) fiber, provided a company with a way to expand its private network beyond its immediate geographic area. A WAN had obvious advantages over a public network like the Internet when it came to reliability, performance and security. But maintaining a WAN, particularly when using leased lines, can become quite expensive and often rises in cost as the distance between the offices increases.

As the popularity of the Internet grew, businesses turned to it as a means of extending their own networks. First came intranets, which are password-protected sites designed for use only by company employees. Now, many companies are creating their own VPN (virtual private network) to accommodate the needs of remote employees and distant offices.

Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. In this article, you will gain a fundamental understanding of VPNs, and learn about basic VPN components, technologies, tunneling and security

Definition:

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

What makes a VPN

A well-designed VPN can greatly benefit a company. For example, it can:

- Extend geographic connectivity
- Improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support

- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN

What features are needed in a well-designed VPN? It should incorporate:

- Security
- Reliability
- Scalability
- Network management
- Policy management

CHAPTER 2

Virtual Private Network Technologies

VPN Solution Components

Depending on whether the PPVPN is layer 2 or layer 3, the building blocks described below may be L2 only, L3 only, or combinations of the two. MPLS functionality blurs the L2-L3 identity.

While these terms were generalized to cover L2 and L3 VPNs in RFC 4026, they were introduced in ^[4].

Customer Edge Device (CE)

In general, a **CE** is a device, physically at the customer premises, that provides access to the PPVPN service. Some implementations treat it purely as a demarcation point between provider and customer responsibility, while others allow it to be a customer-configurable device.

Provider Edge Device (PE)

A **PE** is a device or set of devices, at the edge of the provider network, which provides the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and do maintain VPN state.

Provider Device (P)

A **P** device is inside the provider's core network, and does not directly interface to any customer endpoint. It might, for example, be used to provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, as, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of provider.

VPN Technologies

Remote Access VPN

Remote Access VPNs provide communications between a corporate network and remote and/or mobile employees.

Remote Access VPNs require:

- Strong authentication is critical to verify remote and mobile users' identities as accurately and efficiently as possible.
- Centralized management.
- A high degree of scalability to handle the vast number of remote users accessing the VPN.

Extranet VPN

Extranet VPNs are between a company and its strategic partners, customers and suppliers.

Extranet VPNs require:

- Open standards-based solution to ensure interoperability. The accepted standard for Internet-based VPNs is the Internet Protocol Security [IPSec] standard.
- Traffic control to eliminate bottlenecks at network access points and guarantee swift delivery of and rapid response times for critical data.

Intranet VPN

VPNs are between internal corporate departments and branch offices, it facilitate secure communications between a company's internal departments and its branch offices.

Intranet VPNs require:

- Strong data encryption to protect sensitive information.
- Reliability to ensure the prioritization of mission-critical applications.
- Scalable management to accommodate rapidly growing numbers of new users, new offices and new applications.

Protocols:

PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. Layer 2 Tunneling Protocol (L2TP) or IPsec are the standards-based replacements for. The protocol was developed by a vendor consortium formed by Microsoft, Ascend Communications (today part of Lucent/Alcatel), 3COM, and others, as described by the RFC document.

PPTP is popular because it is easy to configure and it was the first VPN protocol that was supported by Microsoft Dial-up Networking. All releases of Microsoft Windows since Windows 95 OSR2 are bundled with a PPTP client, although they are limited to only 2 concurrent outbound connections. The Routing and Remote Access Service for Microsoft Windows contains a PPTP server.

Until recently, Linux distributions lacked full PPTP support because MPPE was believed to be patent encumbered. Full MPPE support was added to the Linux 2.6.13 branch that is maintained by Andrew Morton. SuSE Linux 10 was the first Linux distribution to provide a complete working PPTP client. Official support for PPTP was added to the official kernel release in version 2.6.14 on October 28, 2005.

L2TP

L2TP acts like a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over an existing network (usually the Internet). L2TP is in fact a layer 5 protocol session layer, and uses the registered UDP port 1701. The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this an L2TP session (or call) is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP.

The packets exchanged within an L2TP tunnel are categorised as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for

data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel.

IPsec

Internet Protocol Security Protocol (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication. IPSec has two encryption modes: tunnel and transport. Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload. Only systems that are IPSec compliant can take advantage of this protocol. Also, all devices must use a common key and the firewalls of each network must have very similar security policies set up. IPSec can encrypt data between various devices, such as:

- Router to router
- Firewall to router
- PC to router
- PC to server

SOCKS

SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS is an abbreviation for "SOCKetS".

Clients behind a firewall, needing to access exterior servers, may connect to a SOCKS proxy server instead. Such proxy server controls the eligibility of the client to access the external server and passes the request on to the server. SOCKS can also be used in the opposite way, allowing the clients outside the firewall ("exterior clients") to connect to servers inside the firewall (internal servers).

The protocol was originally developed by David Koblas, a system administrator of MIPS Computer Systems. After MIPS was taken over by Silicon Graphics in 1992, Koblas presented a paper on SOCKS at that year's Usenix Security Symposium and SOCKS became publicly available. The protocol was extended to version 4 by Ying-Da Lee of NEC. The SOCKS reference architecture and client are owned by Permeo Technologies, (note that Permeo Technologies has been bought out by Blue Coat Systems) a spin-off from NEC. SOCKS performs at Layer 5 of the OSI model - the Session Layer (an intermediate layer between the presentation layer and the transport layer).

Pros and Cons

With the evident technical limitations of implementing VPN, why does VPN technology still deserve consideration? The answer lies in the many advantages offered by the new VPN products and services. Nevertheless VPN also has disadvantages, which are the main cause for which VPN is not yet the common way to use as a networking solution. In this section we will try to explore these advantages and disadvantages.

The main advantages:

- Cost saving:
 - Eliminating the need for expensive long-distance leased lines.
 - Reducing the long-distance telephone charges for remote access.
 - Transferring the support burden to the service providers.
 - Saves Operational costs.
- Scalability and interoperability - Due to the fact that IP networks are scalable in their essence and wide spread, VPN based solutions can be quite easily scaled whenever necessary. Connecting VPN networks together can be done easily, with minimum effort put into the process. Maintenance (Upgrades to existing services or introducing new services) can be easily done, as most applications are actually software based and do not require any hardware replacements and configuration.
- Flexibility of growth.
- Efficiency with broadband technologies.

The main disadvantages:

- VPNs require an in-depth understanding of public network security issues and proper deployment of precautions.
- Availability and performance depends on factors largely outside of their control.
- Immature standards.
- VPNs need to accommodate protocols other than IP and existing internal network technology
- Cost - As always, the main disadvantage of a new technology is its initial cost, wire line communication is very cost effective because almost all the R&D have been completed in the area, the infrastructures are already built, and the public is used to using this type of media. In order to use the VPN more often, costly changes will have to be taken: Stronger and more reliable networks will have to be built (Better bandwidth, better QoS compliance), new products and services will have to be developed and the main issue - people will have to become aware of this new technology.

References

- www.juniper.net
- M. Carugi, " Virtual Private Network services: service requirements and standardization activity", IETF PPVPN, November 30th
- www.itu.int
- www.wikipedia.com
- "Virtual Private Networks (VPNs)", IEC, 2002.