Virtual Private Networking

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

Virtual private networking via the Internet has been promoted as a viable, secure and cost-effective way to connect businesses with their partners, suppliers and customers.

How did this come about?

The world has changed a lot since PCs burst onto the scene in the early 1980s. Nowadays, instead of simply dealing with local or regional concerns, many businesses have to think about international markets and logistics. Many businesses have facilities spread out across the branch offices or at homeworking locations or even around the world. The one thing that all of them need is a way to maintain fast, secure and reliable communications wherever their offices and workers are located

Virtual private networks (or VPNs for short) create extranets and offer secure access to remote data and enterprise-wide communications (such as Microsoft Exchange and Outlook). VPNs allow access to protected network resources to authorized users via the public Internet to securely connect remote offices and remote employees at a fraction of the cost of dedicated, private telephone lines. There are two major uses for VPNs:

- To connect two or more geographically separated networks, such as those at a main office and a remote branch office.
- To allow employees and or authorised users to access a network from a remote PC, such as travelling laptop or home computer.

Although widely hyped as a quick and easy communication and connectivity solution, security concerns have stopped many businesses from moving forward with VPNs. The associated administration and management issues, such as activating or installing VPN client software on PCs and troubleshooting an external user's connectivity problems, have also contributed to the slowdown in deploying VPNs into every network.

Background[1]

Until recently, to achieve the connectivity that VPNs now offer, it has meant the use of leased lines to maintain a Wide Area Network (WAN). Leased lines provided a business with a way to expand their private network beyond their immediate geographic area. A WAN had obvious advantages over a public network such as the Internet when it came to reliability, performance and security. But maintaining a WAN, particularly when using leased lines can become very expensive and often there is a delay in physically getting the leased line installed.

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 businesses are creating their own VPNs to accommodate the needs of remote employees and distant offices.

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.

Despite the problems with VPNs, many businesses are moving ahead with plans to use them and they are set to become part of business strategy for both corporate organisations and leading-edge SMEs with on-the-move and remote networking requirements.

What Is a VPN?

A virtual private network (VPN) is a private data network that transmits data over the public telecommunication infrastructure and which maintains privacy through the use of "tunnelling" protocols and security procedures. Another, more expansive, definition is given in the margin.

VPNs do not inherently change WAN requirements, such as support for multiple protocols, high reliability, and extensive scalability. Instead, a VPN meets these requirements more cost-effectively and with greater flexibility. The functionality of a VPN is mainly determined by the equipment deployed at the edge of the enterprise network and feature integration across the WAN, not by the WAN transport protocol itself.

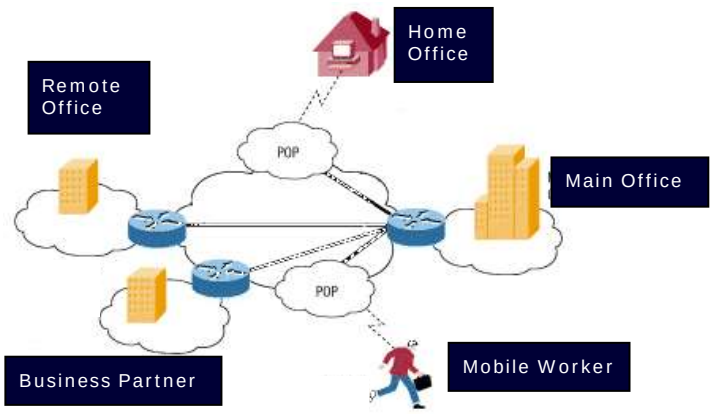
Definition of VPN:

"A private communications network using a private network, other than the PSTN, as its WAN backbone. A VPN is usually a software-defined network running over a shared private network (for example, one used by a common carrier) and offering the appearance, functionality, and usefulness of a dedicated private network, at a lower cost."

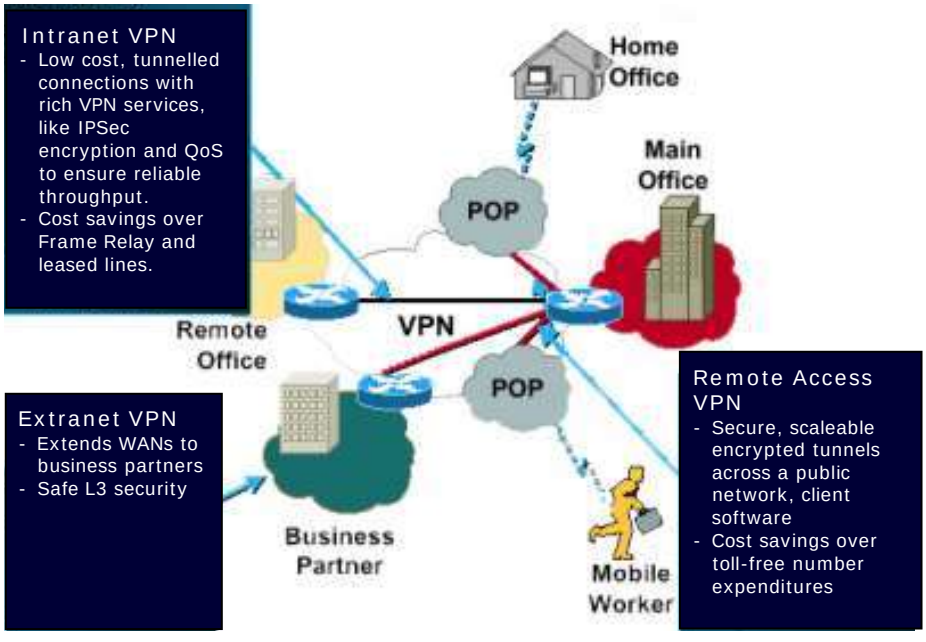
Source: Harry Newton's Telecom Dictionary

VPNs are segmented into three categories (each with different security and bandwidth management issues to consider): remote access, intranets, and extranets:

1. Remote access VPNs connect telecommuters, mobile users, or even smaller remote offices with minimal traffic to the enterprise WAN and corporate computing resources. Remote-Access VPN is also called a Virtual Private Dial-up Network (VPDN). Remote-Access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.
2. An intranet VPN connects fixed locations, branch, and home offices, within an enterprise WAN. If a business has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.
3. An extranet VPN extends limited access of enterprise computing resources to business partners. When a business has a close relationship with another organisation (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various parties to work within a shared environment.



A Typical VPN: Image courtesy of Cisco Systems, Inc.
A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.



Examples of the three types of VPNs: Image courtesy of Cisco Systems, Inc.

VPN Advantages

VPNs offer many advantages over traditional, leased-line networks. The primary benefits include:

- Extend geographic connectivity.
- Lower cost than private networks - total cost of ownership is reduced through lower-cost transport bandwidth, backbone equipment, and operations.
- Improve security.
- More flexible and scalable network architectures than WANs - enabling enterprises to quickly and cost-effectively extend connectivity, facilitating connection or disconnection of remote offices, international locations, telecommuters, roaming mobile users, and external business partners as business requirements demand.
- Improved worker productivity.
- Telecommuter support.
- Reduced management burdens compared to owning and operating a private network infrastructure – organisations can outsource some or all of their WAN functions to a service provider, leaving the organisation to focus on core business objectives, instead of managing a WAN or dial-access network.
- Simplified network topologies, thus reducing management burdens - eliminating the complications associated with connection-oriented protocols.

VPN Security

Leased lines have traditionally been used to establish secure, private connections between sites. Connecting sites with a leased line was inherently secure, because the line was only available to the two sites. But connecting sites across the Internet sends data over the public network and makes it vulnerable to hacking. The biggest security threats occur from within the WAN where an intruder can intercept the data without detection.

A VPN encryption device is what keeps things safe in a VPN. It sits at the edge of the private network (LAN) and uses a combination of encryption and authentication techniques to secure the line.

The challenge of providing e-security services to a VPN application can be reduced to solving a few basic problems:

- Verifying the identity of one or more parties in a transaction (Authentication)
- Protecting the privacy and integrity of information on the network (Data Privacy, Data Integrity)
- Preventing authenticated parties in a transaction or exchange from denying the actions they have taken (Non-Repudiation)

A well-designed VPN uses several methods for keeping your connection and data secure:

- Firewalls - A firewall provides a strong barrier between your private network and the Internet. Encryption - This is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.
- IPSec - Internet Protocol Security Protocol (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication.
- AAA Server - (Authentication, Authorization and Accounting) are used for more secure access in a Remote-Access VPN environment. When a request to establish a session comes in from a dial-up client, the request is sent to the AAA server which then checks who you are (authentication), what you are allowed to do (authorisation) and what you actually do (for accounting and billing)

Microsoft provides an excellent paper on VPNs at: http://technet.microsoft.com/en-us/network/bb545442

How safe is your VPN? Well, maybe not quite as safe as you think. Whether virtual private networks are deployed in secure extranets or to link remote users, simple missteps (or intentional misdeeds) could lead to big trouble.

VPN Technologies

Depending on the type of VPN (Remote-Access or Site-to-Site), you will need to put in place certain components to build your VPN. These might include:

- Desktop software client for each remote user;
- Dedicated hardware such as a VPN Concentrator or Secure PIX Firewall;
- Dedicated VPN server for dial-up services;
- NAS (Network Access Server) used by service provider for remote user VPN access;
- VPN network and policy management centre.

Because there is no widely accepted standard for implementing a VPN, many companies (such as Cisco) have developed turn-key solutions on their own.

Links

HowStuffWorks (www.howstuffworks.com) is an amazing, award-winning online destination for anyone who wants to know how anything works. Originally started by author and entrepreneur Marshall Brain as an entertaining and fascinating place for people to learn about the world in which we live, the site has grown to be one of the top 500 Web sites in the United States.
Other useful links to VPN information are:

- Cisco and VPNs - www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm
- Understanding Virtual Private Dialup Networks - www.cisco.com/en/US/tech/tk801/tk703/technologies_tech_note09186a008009458 6.shtml
- Overview of VPNs - http://idm.internet.com/foundation/vpn-1.shtml
- Tom Dunigan's VPN Page - http://www.epm.ornl.gov/~dunigan/vpn.html
- Virtual Private Network Consortium - http://www.vpnc.org

Further Information

Picking a virtual private networking solution requires careful examination of your networking and security needs, because the chosen solution must be tightly integrated into your existing network. Ideally, your VPN solution should have as little impact as possible on how your users access network resources, because if networking becomes more complex for the average user, the less likely it is that they will be willing to adopt the VPN strategy.

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

If you would like to receive further information about this subject or other publications, please call us – see our contact details on the next page. If you wish, we can refer you to networking specialists who can establish a VPN in your organisation.

Reference:

[1] Sourced from How Stuff Works at www.howstuffworks.com.

Important Notice

Publication issued or updated on:
25 January 2012

Ref: 526