LACROSSE UNIVERSITY

Virtual Private Networks

A PAPER SUBMITTED TO
THE FACULTY OF THE DIVISON OF SCIENCES
IN CANDIDACY FOR THE DEGREE OF
MASTER OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

By
Ayesha Asghar

August 1, 2006

To Zainab

Ideally, a VPN should behave similarly to a private network; it should be secure, highly available and have predictable performance

Christopher McDonald

Contents

ILLUSTRATIONS

Figures Page

Tables

PREFACE

The aim of this Applied Knowledge Paper is to give a deep insight on the basics, components and benefits of Virtual Private Networks. A detailed understanding has been given for the business benefits of a VPN.

The document starts by giving an introduction to a VPN, followed by its components and implementation.

Further the types of VPN have been discussed. Basic VPN requirements have been talked about next. Followed by data security issues in a VPN and the ways of settings up a VPN have been elucidated.

Finally, the document wraps up the paper by evaluating the pros and cons and alternatives of a VPN. The author of the paper hopes that this discussion will serve as a comprehensive guideline for the readers.

ACKNOWLEDGEMENTS

I would like to thank the auspicious instructors of Lacrosse University under whose guidance I've been able to come up with this report. I thank them for their cooperation through out and also for resolving all problems and every issue that I faced.

Next, I would like to thank my family who provided me with all the sources and material required for making this possible. Lastly; I would like to thank God Almighty who gave me the strength and will power to complete this piece of work.

ABBREVIATIONS

3DES	Triple Data Encryption Standard
ACL	Access Control Protocol
ADSL	Asymmetric Digital Subscriber Line
DES	Data Encryption Standard
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX	Internet work Package Exchange
Kbps	Kilobits Per Second
L2TP	Layer Two Tunneling Protocol
PKEY	Public Key Encryption
PPTP	Point to Point Tunneling Protocol
SLA	Service Level Agreement
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
VPDN	Virtual Private Dialup Network
VPN	Virtual Private Network

1. Introduction

1.1. Purpose

The purpose of this paper is to describe a well-formed and a thorough understanding of the Virtual Private Networks. This paper also gives an insight into composition and basic requirements of creating it. Further it throws light on components and implementation of VPN.

It focuses on the types of VPN discusses them. Further the basic requirements, data security and way of creating VPN have been talked about.

This paper provides an understanding of the trends and applications of VPN. And it concludes by critically evaluating the benefits of VPNs.

This paper will assist the novice programmers/non-programmers to have a better understanding of Virtual Private Networks.

1.2. Scope

The paper provides answers to what, when, how and who questions related to VPN; such as:

- What is a VPN?
- What are basic components of a VPN?
- Types of VPN.
- Data Security in VPN.
- Business benefits of a VPN.
- VPN Alternatives.

2. Virtual Private Networks

2.1. Introduction

Virtual private networks (VPNs) offer low-cost, secure, dynamic access to private networks. Such access would otherwise only be possible by using an expensive leased line solution or by dialling directly into the local area network (LAN).

VPNs allow remote users to access private networks securely over the internet. A remote user in one part of the UK can establish a secure network connection using a VPN to a school LAN in another part of the UK and only incur the call cost for the local internet connection.

2.2. What is a VPN?

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

A virtual private network gives secure access to LAN resources over a shared network infrastructure such as the Internet. It can be conceptualised as creating a tunnel from one location to another, with encrypted data travelling through the tunnel before being decrypted at its destination.

Remote users can connect to their organisation's LAN or any other LAN. They can access resources such as email and documents as if they were connected to the LAN as normal. By using VPN technology it is possible to connect to a school LAN from anywhere in the world via the internet, and to access it securely and privately without incurring the large communication costs associated with other solutions.

Example:

One user uses 56 kilobits per second (Kbps) modem to dial their internet service provider (ISP) and connects to the central LAN with VPN software.

A remote site uses ADSL (asymmetric digital subscriber line) to connect to its ISP and a VPN router (a hardware solution) to carry out the VPN connection. Few changes are made to the PCs at the remote site and the VPN router carries out the encryption and decryption of data.

As both connect to their usual ISP, they only incur their normal ISP call tariffs.

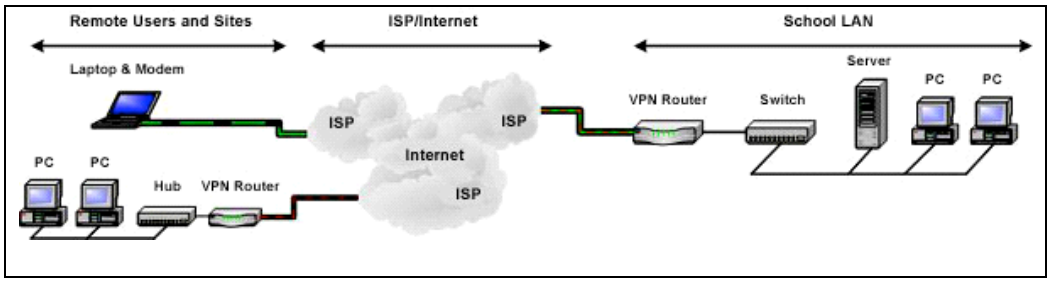

Fig. 1. Two methods of connecting to a school's LAN using a VPN

A Virtual Private Network allows the creation of a secure private network over a shared public network infrastructure such as the Internet. It does that by using a combination of VPN gateways, routers and VPN clients to set up:

- Packet tunnelling
- Encryption/Decryption
- Authentication and secure access to IP services

The term ----virtual private network

Virtual – means that the connection is dynamic. It can change and adapt to different circumstances using the Internet's fault tolerant capabilities. When a connection is required it is established and maintained regardless of the network infrastructure between endpoints. When it is no longer required the connection is terminated, reducing costs and the amount of redundant infrastructure.

Private – means that the transmitted data is always kept confidential and can only be accessed by authorised users. This is important because the internet's original protocols –TCP/IP (transmission control protocol/internet protocol) – were not designed to provide such levels of privacy. Therefore, privacy must be provided by other means such as additional VPN hardware or software.

Network – is the entire infrastructure between the endpoints of users, sites or nodes that carries the data. It is created using the private, public, wired, wireless, Internet or any other appropriate network resource available.

2.3. Components of a VPN

As VPN topologies can vary greatly there is no standard for a definitive VPN. However, it is possible to specify what each main component of a VPN does:

- VPN gateways – create the virtual tunnels that the data passes through, carrying out the encryption before transmission and decryption at the other end. Gateways can be software, or built into a firewall, or a server or router or a dedicated appliance.
- Security servers – maintain the access control list (ACL) and other user-related information that the security gateway uses to determine which traffic has authorised access.

- Keys – used for the encryption and decryption of data. Sites can choose to maintain their own database of digital certificates (keys) for users by setting up a certificate server, or they can use an external certificate authority.

- Network – there must be an Internet infrastructure at both ends to provide the actual transmission medium.

Some of these components may be built into a single device or spread over many devices over several sites.

2.4. Basic VPN Requirements

Typically, when deploying a remote networking solution, an enterprise needs to facilitate controlled access to corporate resources and information. The solution must allow roaming or remote clients to connect to LAN resources, and the solution must allow remote offices to connect to each other to share resources and information (router-to-router connections). In addition, the solution must ensure the privacy and integrity of data as it traverses the Internet. The same concerns apply in the case of sensitive data traversing a corporate Internet work.

Therefore, a VPN solution should provide at least all of the following:

- **User Authentication**. The solution must verify the VPN client's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.

- **Address Management**. The solution must assign a VPN client's address on the intranet and ensure that private addresses are kept private.

- **Data Encryption**. Data carried on the public network must be rendered unreadable to

unauthorized clients on the network.

- **Key Management**. The solution must generate and refresh encryption keys for the client and the server.

- **Multi-protocol Support**. The solution must handle common protocols used in the public network. These include IP, Internet work Packet Exchange (IPX), and so on.

An Internet VPN solution based on the Point-to-Point Tunnelling Protocol (PPTP) or Layer Two Tunnelling Protocol (L2TP) meets all of these basic requirements and takes advantage of the broad availability of the Internet. Other solutions, including Internet Protocol Security (IPSec), meet only some of these requirements, but remain useful for specific situations.

2.5. Ways to Create VPN

There are two ways to create a VPN connection: By dialling an ISP, or by connecting directly to the Internet, as shown in the following examples.

By Dialling an ISP

In this way, the VPN connection first makes a call to an ISP. After the connection is established, the connection then makes another call to the remote access server that establishes the PPTP or L2TP tunnel. After authentication, one can access the corporate network, as shown in the following illustration.

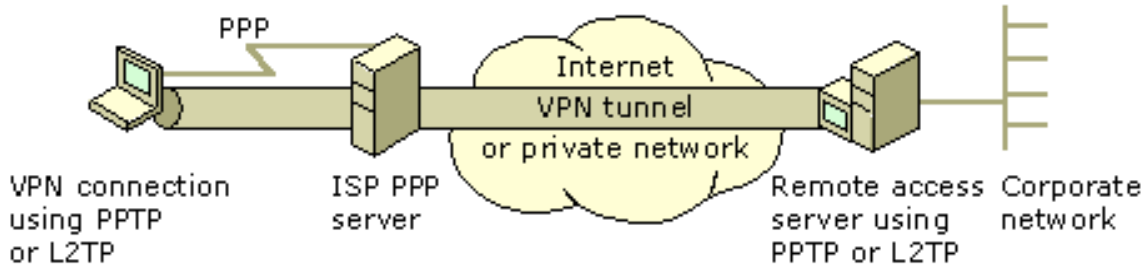

Fig. 2. Creating a VPN by dialling an ISP

By Connecting To Internet

In this case, a user who is already connected to the Internet uses a VPN connection to dial the number for the remote access server. Examples of this type of user include a person whose computer is connected to a local area network, a cable modem user, or a subscriber of a service such as ADSL, where IP connectivity is established immediately after the user's computer is turned on. The PPTP or L2TP driver makes a tunnel through the Internet and connects to the PPTP-enabled or L2TP-enabled remote access server. After authentication, the user can access the corporate network, achieving the same functionality as the preceding example.

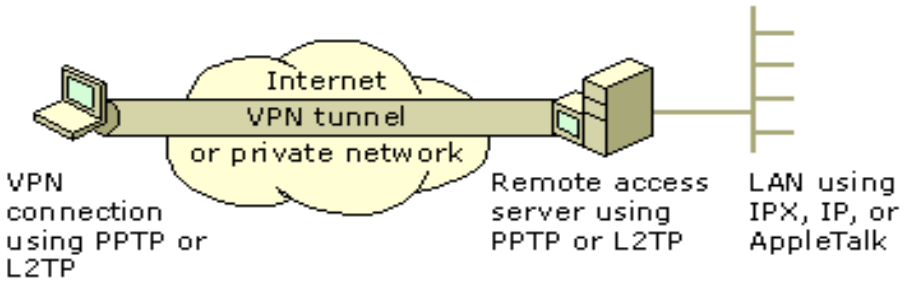

Fig. 3. Creating a VPN by connection to Internet

Note

- Connecting directly to the Internet means direct IP access without going through an ISP. (For example, some hotels allow one to use an Ethernet cable to connect to the Internet.)

- If one has an active Winsock Proxy client, one cannot create a VPN. A Winsock Proxy client immediately redirects data to a configured proxy server before the data can be processed in the fashion required by a VPN. To establish a VPN, one should disable the Winsock Proxy client.

2.6. Types of VPN

There are many variations of virtual private networks, with the majority based on two main models.

1. **Remote access, virtual private dial-up network (VPDN) or client - to - site**

   A remote access VPN is for home or travelling users who need to access their central LAN from a remote location. They dial their ISP and connect over the Internet to the LAN. This is made possible by installing a client software program on the remote user's laptop or PC that deals with the encryption and decryption of the VPN traffic between itself and the VPN gateway on the central LAN.

2. **Fixed Intranet, Extranet or site – to – site**

   A fixed VPN is normally used between two or more sites allowing a central LAN to be accessed by remote LANs over the Internet or private communication lines using VPN gateways. VPN gateways (normally a VPN-enabled router) are placed at each remote

site and at the central site to allow all encryption and decryption and tunnelling to be carried out transparently.

2.7. Implementation of VPN

- National and global expansion
- Access to remote sites possible only via Internet
- Secure access to sensitive services
- Secure access for travelling and telecommuting users
- Secure access for wireless LAN users

2.8. Data Security in VPN

TCP/IP is not designed for security, so VPNs use a mix of IP protocols and systems to provide the best security solution for each type of connection. Some protocols encrypt the packets of data while other protocols protect the packet whilst it is being transmitted. Some of the more popular protocols and systems that a VPN uses to keep the data secure are:

- **PPTP (point-to-point tunnelling protocol)**

Creates a virtual tunnel for connections that, along with L2TP (layer two tunnelling protocol) and L2F (layer two forwarding), are used mainly for remote access VPNs.

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavours of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

Point-to-Point Tunnelling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking. PPTP operates at Layer 2 of the OSI model.

Using PPTP

PPTP packages data within PPP packets, then encapsulates the PPP packets within IP packets (datagrams) for transmission through an Internet-based VPN tunnel. PPTP supports data encryption and compression of these packets. PPTP also uses a form of **General Routing Encapsulation (GRE)** to get data to and from its final destination.

PPTP-based Internet remote access VPNs are by far the most common form of PPTP VPN. In this environment, VPN tunnels are created via the following two-step process:

1. The PPTP client connects to their ISP using PPP dial-up networking (traditional modem or ISDN).

2. Via the broker device (described earlier), PPTP creates a TCP **control connection** between the VPN client and VPN server to establish a tunnel. PPTP uses TCP port 1723 for these connections.

PPTP also supports VPN connectivity via a LAN. ISP connections are not required in this case, so tunnels can be created directly as in Step 2 above.

Once the VPN tunnel is established, PPTP supports two types of information flow:

- **control** messages for managing and eventually tearing down the VPN connection. Control messages pass directly between VPN client and server.

- **data** packets that pass through the tunnel, to or from the VPN client

PPTP Control Connection

Once the TCP connection is established in Step 2 above, PPTP utliizes a series of **control messages** to maintain VPN connections. These messages are listed below.

Table 1

PPTP Control Messages

Number	Name	Description
1	StartControlConnectionRequest	Initiates setup of the VPN session; can be sent by either client or server.
2	StartControlConnectionReply	Sent in reply to the start connection request (1); contains result code indicating success or failure of the setup operation, and also the protocol version number.
3	StopControlConnectionRequest	Request to close the control connection.
4	StopControlConnectionReply	Sent in reply to the stop connection request (3); contains result code indicating success or failure of the close operation.
5	EchoRequest	Sent periodically by either client or server to "ping" the connection (keep alive).
6	EchoReply	Sent in response to the echo request (5) to keep the connection active.
7	OutgoingCallRequest	Request to create a VPN tunnel sent by the client.
8	OutgoingCallReply	Response to the call request (7); contains a unique identifier for that tunnel.
9	IncomingCallRequest	Request from a VPN client to receive an incoming call from the server.
10	IncomingCallReply	Response to the incoming call request (9), indicating whether the incoming call should be answered.
11	IncomingCallConnected	Response to the incoming call reply (10); provides additional call parameters to the VPN server.
12	CallClearRequest	Request to disconnect either an incoming or outgoing call, sent from the server to a client.
13	CallDisconnectNotify	Response to the disconnect request (12); sent back to the server.
14	WANErrorNotify	Notification periodically sent to the server of CRC, framing, hardware and buffer overruns, timeout and byte alignment errors.
15	SetLinkInfo	Notification of changes in the underlying PPP options.

With control messages, PPTP utilizes a so-called **magic cookie**. The PPTP magic cookie is hardwired to the hexadecimal number 0x1A2B3C4D. The purpose of this cookie is to ensure the receiver interprets the incoming data on the correct byte boundaries.

PPTP Security

PPTP supports **authentication**, **encryption**, and **packet filtering**. PPTP authentication uses PPP-based protocols like EAP, CHAP, and PAP. PPTP supports packet filtering on VPN servers. Intermediate routers and other firewalls can also be configured to selectively filter PPTP traffic.

PPTP and PPP

In general, PPTP relies on the functionality of PPP for these aspects of virtual private networking.

- authenticating users and maintaining the remote dial-up connection
- encapsulating and encrypting IP, IPX, or NetBEUI packets

PPTP directly handles maintaining the VPN tunnel and transmitting data through the tunnel. PPTP also supports some additional security features for VPN data beyond what PPP provides.

PPTP Pros and Cons

PPTP remains a popular choice for VPNs thanks to Microsoft. PPTP clients are freely available in all popular versions of Microsoft Windows. Windows servers also can function as PPTP-based VPN servers.

One drawback of PPTP is its failure to choose a single standard for authentication and encryption. Two products that both fully comply with the PPTP specification may be totally incompatible with each other if they encrypt data differently, for example. Concerns also persist over the questionable level of security PPTP provides compared to alternatives.

- **IPSec (Internet Protocol Security)**

It's becoming the most commonly used security option for fixed VPN solutions. Each packet of data is encrypted and has an authenticating stamp verifying its origin. This makes IPSec a very secure option. IPSec works in one of two ways:

  - In 'transport mode' only the payload portion of the packet is encrypted. (The payload consists of the actual data that is being transmitted.).
  - In 'tunnel mode' the entire packet, including the header is encrypted. (The header contains the source and destination IP addresses.)

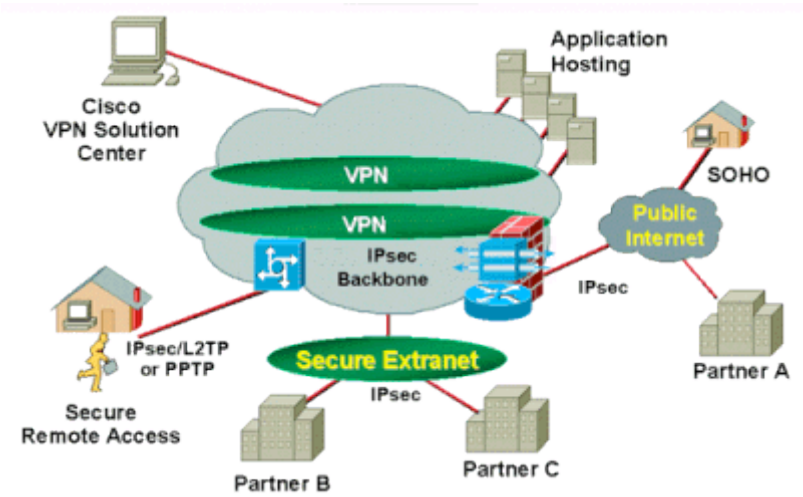

Fig. 4. A remote-access VPN utilizing IPsec

- **Encryption standards**

DES (data encryption standard) and 3DES (triple DES) secure the data to different levels ranging from 56- to 168-bit encryption.

Encryption 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. Most computer encryption systems belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption

In **symmetric-key encryption**, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that one knows which computers will be talking to each other so one can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message. Think of it like this: One creates a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C," and "B" becomes "D". One has already told a trusted friend that the code is "Shift by 2". One's friend gets the message and decodes it. Anyone else who sees the message will see only nonsense.

Public-key encryption uses a combination of a private key and a public key. The private key is known only to one's computer, while the public key is given by one's computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and

its own private key. A very popular public-key encryption utility is called **Pretty Good Privacy** (PGP), which allows ones to encrypt almost anything.

- **Authentication systems**

Prove that the sender of the packets is genuine and not a hacker attempting to deceive the receiver by intercepting and altering the packets before they arrive at their destination.

AAA (authentication, authorization and accounting) servers 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 proxied to the AAA server. AAA then checks the following:

- Who you are (authentication)
- What you are allowed to do (authorization)
- What you actually do (accounting)

The accounting information is especially useful for tracking client use for security auditing, billing or reporting purposes.

- **PKE (public key encryption)**

PKE can be used with VPNs. Instead of manually entering encryption codes, Internet key exchange (IKE) allows keys to be automatically exchanged – which are useful on larger networks.

There are many ways to protect the data during transmission. Most VPN solutions use either encryption or authentication for data security. As the security level increases so

does the time required to process and assembles each packet. The typical overhead for VPN encryption during web browsing is 20 per cent; other user applications that run over VPNs may increase the overhead significantly more. To alleviate this problem some VPN systems compress data before sending to improve network performance.

2.9. How does a VPN work?

Working Of a remote access VPN solution

A remote access solution works by the remote user first establishing an internet connection to an ISP in the normal way. The user activates the VPN client software to create a tunnel over the internet and to connect to the central LAN's VPN gateway. The VPN client software then passes its authorisation to the VPN gateway. The VPN gateway checks that the user is authorised to connect and then ensures the encryption key from the remote client is valid. All VPN data is encrypted using the key before being transmitted over the internet using a tunnelling protocol. It is decrypted at the other end by the VPN gateway, which has an identical set of keys to decrypt the data. Data sent from the central LAN to the remote user is encrypted by the VPN gateway before transmission and decrypted by the remote user's VPN client software.

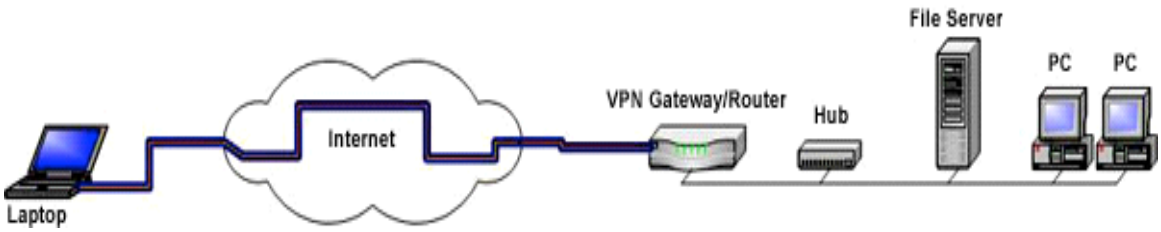

Fig. 5. Working of a remote access VPN solution

Working Of a fixed VPN solution

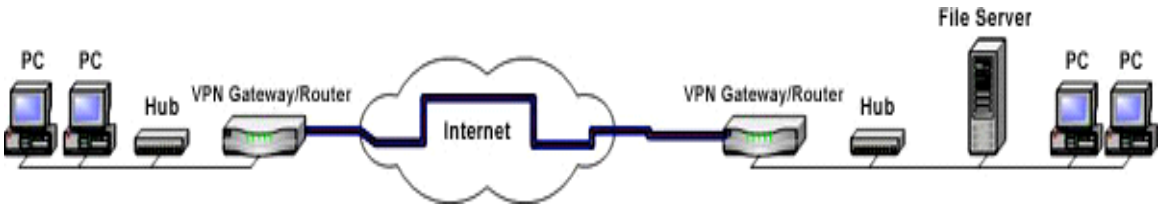

Fig. 6. Working of a fixed VPN solution

The choice of ISP is very important when implementing a VPN solution as it can have a major impact on VPN performance. It may be advisable for all VPN users and sites, including the central LAN, to use the same ISP for their Internet connections. This will lessen the amount of data that needs to cross into the networks of other ISPs, which could degrade performance. Most ISPs will offer a service level agreement (SLA) that agrees network uptime, latency, security and other functions. It is important to read the SLAs carefully before deciding which ISP will give the fastest and most reliable service.

2.10. A functional VPN network

2.10.1. Does a company need a VPN?

If one's company maintains a private data network today, a VPN can replace much of it while providing great cost savings. Many companies that don't currently use private data networks can increase business efficiency by implementing a cost effective VPN. If one's enterprise has any of the following characteristics, one should look at a VPN as a solution:

- Remote locations that need access to centralized corporate data
- Geographically diverse branches, departments or subsidiaries

- Secure information transfers between fixed locations
- Support for mobile employees or telecommuters with secure data access
- Polling secure data such as electronic commerce at kiosks
- Secure inter-company links for private data transfer between companies
- Virtual teams that need to access and update large, secure files such as engineering drawings and project management

In short, if one has more than one LAN, communicate secure data with employees, partners, vendors, consultants, telecommuters, branch offices or a sales staff, a VPN is likely to improve one's business efficiency while reducing cost.

2.11. Analogy: Each LAN is an Island

Imagine that one lives on an island in a huge ocean. There are thousands of other islands all around, some very close and others farther away. The normal way to travel is to take a ferry from one's island to whichever island one wishes to visit. Of course, traveling on a ferry means that almost no privacy. Anything one does can be seen by someone else.

Let's say that each island represents a private LAN and the ocean is the Internet. Traveling by ferry is like connecting to a Web server or other device through the Internet. One has no control over the wires and routers that make up the Internet, just like one has no control over the other people on the ferry. This leaves one susceptible to security issues if one is trying to connect between two private networks using a public resource.

Continuing with the analogy, one's island decides to build a bridge to another island so that there is easier, more secure and direct way for people to travel between the two. It is expensive to build and maintain the bridge, even though the island one is connecting with is very close. But the need for a reliable, secure path is so great that one do it anyway. One's island would like to connect to a second island that is much farther away but decides that the cost are simply too much to bear.

This is very much like having a leased line. The bridges (leased lines) are separate from the ocean (Internet), yet are able to connect the islands (LANs). Many companies have chosen this route because of the need for security and reliability in connecting their remote offices. However, if the offices are very far apart, the cost can be prohibitively high -- just like trying to build a bridge that spans a great distance.

So how does VPN fit in? Using this analogy, one could give each inhabitant of one's islands a small submarine. Let's assume that one's submarine has some amazing properties:

- It's fast.
- It's easy to take with, wherever one goes.
- It's able to completely hide one from any other boats or submarines.
- It's dependable.
- It costs little to add additional submarines to one's fleet once the first is purchased.

Although they are traveling in the ocean along with other traffic, the inhabitants of the two islands could travel back and forth whenever they wanted to with privacy and security. That's essentially how a VPN works. Each remote member of the network can communicate in a

secure and reliable manner using the Internet as the medium to connect to the private LAN. A VPN can grow to accommodate more users and different locations much easier than a leased line. In fact, **scalability** is a major advantage that VPNs have over typical leased lines. Unlike with leased lines, where the cost increases in proportion to the distances involved, the geographic locations of each office matter little in the creation of a VPN.

3. Business Benefits of VPN

Virtual Private Networks can replace expensive dedicated leased lines that connect Local Area Networks. Traditional Wide Area Networks consist of point-to point dedicated circuits that connect individual LANs. Charges for these circuits include mileage charges, fixed charges, and local loop charges and associated equipment. The cost is high because charges cover full bandwidth access, twenty-four hours per day. So, whether one uses 24 hours or 15 minutes, and whether the traffic takes up 10% of capacity or 100%, one pays the same price. Using frame relay circuits can add flexibility and reduce costs somewhat, but the use of a VPN can reduce these costs dramatically.

For example, let's look at a circuit between Lahore and Karachi City. At T1 capacity (1.544Mbps) the direct circuit would cost about $8,000 per month. Access provided by an ISP on a VPN would be approximately $2,400 per month for the same bandwidth -- a savings of 70%! T3 (45 Mbps) access on the same route would be $80,000 per month for the direct circuit. VPN access would be around $55,000 -- a savings of 40%. Since most private networks consist of multiple circuits, the cost savings add up quickly.

A VPN can also make use of the Internet to replace modem pools and eliminate long distance dial-up fees. They reduce network management expense by outsourcing many tasks to an Internet Service Provider.

Direct cost savings are only one side of the equation. A Virtual Private Network can increase business efficiency as well. Take a look at the following concrete examples to get an idea of how a VPN could benefit one's business:

1. Automobile manufacturer centralizes database to track inventory, increase sales

An automobile manufacturer uses a VPN to connect dealer locations to a centralized inventory-tracking database. As dealers receive requests from customers for automobiles or parts, the centralized database allows them to locate the desired item at the closest location and arrange for immediate shipping.

2. VPN ensures smooth and successful corporate merger

When a major corporation acquires a new subsidiary with multiple locations, a VPN is used to connect all of the locations and subsidiary headquarters to the parent corporation's systems. This provides the subsidiary with immediate access to the data it needs for the transition, while allowing management to monitor the ongoing progress of each location in real-time. The VPN is implemented using existing Internet access facilities at each location, so the time required establishing the entire network is only a few days, rather than the months typically required to implement a dedicated network.

3. County health department uses VPN to track diseases securely

A County health department establishes a centralized disease database and connects hospitals and other health facilities to the database via a VPN so that the incidence of communicable diseases can be tracked. Since the data contains specific patient information, the need for security is paramount.

4. Physicians use VPN to reduce on-call time, expenses

On-call specialists must frequently travel to a hospital to view radiological scans or other visual data. A group of physicians is reducing the number of trips and associated expense by

implementing a high speed VPN that transmits diagnostic material to a desktop computer in their home. They reduce the number of hospital trips required by over 50%.

5. Hi-tech company makes sales automation and training easy

A high technology company with a staff of 200 salespeople provides mobile dial-up VPN access to headquarters data. The sales people have resources such as catalogs, presentations, proposals, order status and current inventory available from their laptops via a secure connection, whether in a hotel room or in a customer meeting. Video and interactive product training is available over the VPN. Each day, new contact data and sales order activity from each salesperson is updated to the main corporate database, reports are generated for sales and marketing management and secure e-mail is exchanged.

6. Insurers use VPN for secure e-commerce

Six major insurance firms have formed an alliance to build a VPN that will let them exchange electronic mail, access a common directory service and deploy electronic-commerce applications.

7. Leading importer improves customer satisfaction with VPN

One of the world's largest retail importers uses its VPN intranet to link stores, sales people and inventory to save money, increase efficiency, and improve customer satisfaction.

8. Service vendor increases security, minimizes staff expense

A vendor provides services at airport kiosks. Customers pay with a credit card. A VPN network is used to monitor video cameras in each kiosk to deter vandalism. Each hour, credit

card information is securely transferred from the kiosk to the corporate database over the VPN, eliminating the need for manual pick-up of the data.

9. Manufacturer saves big money with VPN

Looking for a way to let distributors access it's ordering process, an electronics manufacturer chose a VPN rather than building and managing its own wide-area network and expects to save more than $100,000 annually.

10. Aerospace manufacturer reduces cost of working with remote subcontractor

Not all subcontractors are created equal. In this case, the best subcontractor for a major aerospace manufacturer was located on the other coast. The companies use a VPN to tie purchasing, inventory, production and shipping computer systems together to create a "just-in-time" inventory replenishment system. The VPN is used to videoconference their staffs for engineering meetings, avoiding the high cost and productivity loss of cross-country travel.

11. Security experts collaborate on VPN extranet

The nation's top national security experts will increase efficiency by relying on a VPN extranet to collaborate on projects and documents, linking geographically diverse locations securely, as well as at low cost.

12. Virtual teams increase efficiency, share data securely

Today's business teams make use of the best talent available and increasingly include partners from all over the globe. These virtual collaborations are perfect for Virtual Private Networks. Engineering, product design, large consulting projects and major system implementations all

require geographically diverse entities to collaborate and share data. Many of these applications require access to large files such as engineering drawings, databases or project management software. In most cases, the projects are competitive and require a high degree of security. VPNs can be managed effectively, giving a business partner access to some information, while excluding other data and allowing access only as long as the collaborative project continues.

The list of applications is nearly endless. It includes video and teleconferencing, secure access to databases, secure remote access and enhanced efficiency in working with business partners. These few examples will give one an idea of the things that can be accomplished with the implementation of VPN in an organization.

4. Managing and Measuring a VPN

There are several management issues to consider before implementing a Virtual Private Network: Service Level Agreements, access to real-time status of one's VPN, accounting or usage tracking, VPN provisioning, trouble management, security management and real-time remote access authorization should all be primary concerns.

Quality of service is extremely important for a VPN. *Any VPN provider should be willing to enter into an agreement to guarantee a level of service on one's VPN. This Service Level Agreement (SLA) should guarantee availability of not less than 99.8%, including scheduled maintenance and local loop problems.* Be sure to ask if the ISP's availability statistics include these factors.

Service Level Agreements containing guarantees for latency are difficult for an ISP to provide. Latency can be affected by traffic that goes outside of an ISP's backbone, the type of encryption used, and network overhead beyond the ISP's control. Frankly, the best latency assurance achievable today is to select a facilities-based ISP that has points-of-presence where one's VPN nodes will be located and that employs hardware based encryption. When one finds such an ISP, it would be worthwhile to discuss latency SLA performance criteria for traffic under the control of the ISP. If one's system is designed properly, an ISP may be willing to issue a latency SLA.

Access to real-time information on the performance of one's VPN is essential. A VPN provider should be able to furnish tools that allow one's company to monitor network performance. The interface to these tools should be secure and easy to use. Most network managers prefer a Web-based interface for ease of accessibility and use. Be sure to ask for a

demonstration of one’s VPN provider's tools to make sure that they will meet one’s requirements.

Frequently, a network manager is required to provide information to internal users that allows for an accounting and allocation of network costs. If this requirement exists within one’s organization, be sure to discuss the needs with one’s ISP to make sure they'll meet one’s requirements.

Once one’s VPN is designed, how will it be implemented? Purchasing, integrating and deploying equipment and software, coordination of vendors, testing and troubleshooting a VPN can be expensive, time consuming and challenging for the most experienced network manager. Some ISPs offer turnkey solutions that include all of these functions. One’s VPN implementation will go much smoother if one chooses an ISP that has extensive experience in such implementations.

Trouble management is another key consideration: One VPN provider's trouble management system must integrate seamlessly with one company's system. This integration should be discussed with one’s ISP before an agreement is signed. How will trouble calls enter the system? Who will be notified? How will trouble escalation take place? What criteria must be met before a trouble report is closed? Most network managers agree that the ISP should take responsibility for end-to-end trouble management and that the network manager should be notified and participate in escalated trouble calls.

Security management can be a time consuming task, so it's a good idea to make one’s ISP responsible for issuing of digital authenticating certificates and encryption keys. This is

especially important as the VPN grows and the security infrastructure requires more frequent maintenance.

However, one will want to retain control over access privileges for one's dial-in clients so that one can make real-time adjustments if there are personnel changes, computers are misplaced or security is compromised. Remote user communities tend to be dynamically changing environments. One can retain control by implementing Remote Authentication Dial-in User Service (RADIUS). In a RADIUS system, a remote user dials into an ISP's modem/ISDN bank. A challenge is issued to the remote user, who must respond with correct identification. This information is routed to an authentication computer on one's company's premises, which issues an authorization back to the ISP to allow entrance of the user onto the VPN. Although this entire procedure is transparent to the user, it permits one's company to control dial access in real-time without having to update authorization tables throughout the ISP's network.

The main reason for implementing a VPN is to reduce costs. Be aware that many ISPs may charge extra to furnish the tools and support needed to manage and measure the performance of a VPN, while a few include them at no additional cost. Be sure to find out how much one will be charged to get the support one requires.

The Importance of end-to-end Responsibility

End-to-end responsibility has been discussed repeatedly throughout this guide. Nevertheless, it is worthwhile to summarize its importance here for the simple reason that it can't be overstated or overemphasized. By now, it should be clear that the success of one's VPN depends on the success of the partnership with the VPN provider. That success will, in turn, depend on the provider's ability to provide full end-to end responsibility for one's VPN.

The only ISPs that can provide this level of responsibility are first tier, facilities-based providers. *That's why it's so important to choose a provider that completely owns and controls its network facilities in every major node of one's VPN: If one's corporate data access is impaired, the last thing one needs is two or even three vendors insisting that other vendors are responsible.*

When one selects a facilities-based partner that takes end-to-end responsibility:

- One's service agreements will have more meaning
- Latency will be better controlled
- Security will be better maintained
- Hardware and software compatibility issues will be greatly reduced
- Hardware, software and network upgrades will be provided by the vendor, further reducing costs.
- Network management and maintenance tasks will be shifted from in-house to the ISP, reducing overhead costs.
- One retains control of remote user access, full network performance monitoring and trouble correction processes.
- Labour-intensive security management will be handled by the ISP, saving one more.

Creative use of bandwidth to one's company locations can allow secure VPN data, Internet, voice telephone, fax, video and other services to arrive via a single digital pipeline. This reduces cost while simplifying the task of network management. There are obvious advantages of managing a single network access facility, calling a single vendor and paying a

single, reduced bill. This approach can also simplify the lives of one's team members: Everyone from one's MIS staff to the Accounting department to the President of one's company will appreciate the wisdom of partnering with a VPN provider who takes end-to-end responsibility.

Remember, not every ISP can provide this level of service. Ask one's prospective VPN partner if they can support one to this degree.

Integrating a VPN into an existing network environment

Most companies that deploy a Virtual Private Network will integrate it into an existing network infrastructure that may contain Local Area Networks, Wide Area Networks, some form of dial-up access, Internet access, management tools, security systems and legacy hardware and software.

One's VPN provider should be made completely aware of all aspects of one's existing networks. The time to work out compatibility, protocol and management issues is before the final VPN design. The current design might demand layer 2 routing, rather than the preferred layer 3. The trouble management system may have specific requirements that the VPN provider's system must comply with. Bandwidth may be an issue at certain locations. Legacy systems may require gateways or routers to access the VPN. Firewalls and security must be discussed. Current user interfaces, operating systems and data exchange formats must be supported. Corporate network administration policies must be enforceable on the VPN.

One's VPN partner must be able to talk intelligently about these issues and accommodate one's requirements.

5. Pros and Cons

Virtual private networks have a number of advantages and disadvantages over direct dial or leased line solutions.

5.1. Advantages

- VPNs authenticate all packets of data received, ensuring that they are from a trusted source. Encryption ensures that the data remains confidential. The connection over the Internet is encrypted and secure. The remote access server enforces new authentication and encryption protocols. Sensitive data is hidden from Internet users, but made securely accessible to appropriate users through a VPN.

- Most VPNs connect over the Internet so call costs are minimal, even if the remote user is a great distance from the central LAN.

- Banks of modems at the central site are not required. Because an ISP maintains communications hardware such as modems and ISDN adapters, one's network requires less hardware to purchase and manage.

- Multiple telephone lines are not required as the Internet is used as a connection instead of a long distance telephone number or 1-800 service.

- A reduction in the overall telecommunication infrastructure – as the ISP provides the bulk of the network.

- Reduced cost of management, maintenance of equipment and technical support.

- Simplifies network topology by eliminating modem pools and a private network infrastructure.

- VPN functionality is already present in some IT equipment.
- VPNs are easily extended by increasing the available bandwidth and by licensing extra client software.
- If a LAN uses NetBeui or IPX/SPX (both incompatible with the internet) instead of TCP/IP to transmit data to its clients, the VPN gateway can encapsulate these languages into an IP packet and transmit it over the web to another VPN gateway.
- Provides IP address security: Because the VPN is encrypted, the addresses one specifies are protected, and the Internet only sees the external IP address. For organizations with nonconforming internal IP addresses, the repercussions of this are substantial, as no administrative costs are associated with having to change IP addresses for remote access via the Internet.

5.2. Disadvantages

- If the ISP or Internet connection is down, so is the VPN.
- The central site must have a permanent Internet connection so that remote clients and other sites can connect at anytime.
- VPNs may provide each user with less bandwidth than a dedicated line solution.
- Existing firewalls, proxies, routers and hubs may not support VPN transmissions.
- The internet connection of the central site must have sufficient bandwidth to cope with VPN traffic, the internet connections originating from the central site and any other traffic such as email and FTP (file transfer protocol).
- VPN equipment from different manufacturers may comply with different standards.

Any institution that has users who connect to a LAN from a remote location, or which requires its users to connect to a central LAN, should consider implementing a VPN solution. It is considered to be a superior alternative to long-distance dial-in and leased lines; VPNs can be used securely to carry information at a fraction of the cost of other solutions. An institution can reduce its connection and maintenance costs by replacing banks of modems and multiple leased lines with a single link that carries remote access and fixed VPN traffic along with existing Internet traffic.

6. SSL VPN

SSL VPNs use existing web browser technology to create a secure VPN tunnel between a client and a server. Most, if not all, web browsers now have the capability to use SSL encryption to access secure websites and to transmit and receive secure or private information. SSL VPNs are limited to applications that can run in a browser window and therefore are not as popular as IPSec VPNs. While some might find the limitations of SSL-based VPNs a problem, these shortcoming may diminish as web-enabled or browser-based applications become more popular.

IPSec is application independent and is suitable for users who need to access all applications and resources as if they were physically connected to the LAN. SSL is suited to infrequent users who require web mail or browser-based application access.

Example:

A VPN gateway has been installed at site A and site B. These two devices are connected to the internet via an ISP's ADSL package, with each VPN gateway having a unique IP address. Each VPN gateway is configured with the same shared key or code.

The original IP packets on the LAN only contain the receiver's address (H1) called a header, the actual data being sent (payload) and sender's address (T1) called a trailer.

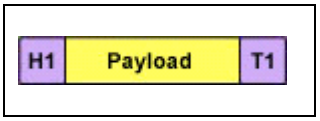

Fig. 7. IP Packet

Each individual packet of data that passes through the VPN gateway to be sent to site B is wrapped inside another packet that is encoded using the shared key. The original packet is encrypted and remains inside a wrapped layer of authentication, proving that it originated from site A.

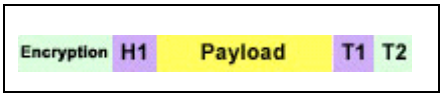

Fig. 8. Example of an IPSec fixed VPN solution

When the packet of data reaches the VPN gateway on site B, the gateway checks to see if the packet originated from site A and that the packet has not been tampered with. Then, if the packet meets these criteria, it decodes the packet using the shared code before passing it on to its destination on the LAN.

If the packet becomes subject to a so-called ‘middleman attack’ and a hacker collects the packet before it reaches site B then it will be useless without the shared code. The hacker cannot break into the packet’s payload without first decrypting the code.

7. Alternatives of VPN

When VPNs are used it is normally in place of other methods of communication. A VPN is designed to remove the need for fixed links, dedicated circuits and expensive long distance telephone calls. Remote access service (RAS) and leased lines are possible alternatives.

- ***Remote access service*** – via standard PSTN (public switched telephone network) or ISDN (integrated services digital network) lines requires the user and receiving site to have access to exclusive modems or similar devices, and different communication lines for each connection that is made. The caller may incur large telephone bills if they are a long distance from the network that they are accessing.

- ***Leased line*** circuits – can be very expensive (such circuits are normally charged by the mile) when compared to the cost of a VPN connection over the Internet, although there is a high quality of service. With the current poor quality of service within a VPN run over a public network, leased lines provide a good solution for when a 'guaranteed' level of service is required.

8. Conclusion

VPNs allow institutions to take advantage of the internet's infrastructure for secure, private communications between schools, remote sites, and home-based workers. Access to a school's LAN is entirely possible from home before, during or after school hours. A user can access all of resources on the LAN as if they were actually on site.

A VPN solution can reduce the need for dedicated equipment by using existing internet equipment. VPNs are scalable solutions which allow new users to be added without major restructuring.

Users are able to access an SSL VPN server from almost any internet-connected PC, even those in public locations. An SSL-based VPN does away with the need for VPN software to be installed on the users' PCs, although the applications that can used are limited to those available in a web-enabled format.

Implementing a VPN solution for home/school links would be extremely beneficial, allowing a large number of users to access a school's network from home while requiring very few changes to be made to the existing LAN infrastructure.

In conclusion VPN is a great option for business either small or large that has remote employees, need site-to-site access with remote offices or secure dial-up-connections.

The success of VPNs in the future depends mainly on industry dynamics. Most of the value in VPNs lies in the potential for businesses to save money. Should the cost of long-distance telephone calls and leased lines continue to drop, fewer companies may feel the need to

switch to VPNs for remote access. Conversely, if VPN standards solidify and vendor products interoperate fully with other, the appeal of VPNs should increase.

The success of VPNs also depends on the ability of intranets and extranets to deliver on their promises. Companies have had difficulty measuring the cost savings of their private networks, but if it can be demonstrated that these provide significant value, the use of VPN technology internally may also increase.

Bibliography

[Cisco, 2006]
Cisco. *Virtual Private Networks.* Retrieved: July 3, 2006 from
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm#wp1020548

[CSM, 2006]
CSM. *Virtual Private Networks*. Retrieved: July 3, 2006 from
http://www.csm.ornl.gov/~dunigan/vpn.html

[HomeNetHelp, 2006]
HomeNetHelp. *Virtual Private Networks, An Overview*. Retrieved: July 15, 2006 from
http://www.homenethelp.com/vpn/

[IEC, 2006]
IEC. *Virtual Private Networks*. International Engineering Consortium. Retrieved: July 8, 2006 from
http://www.iec.org/online/tutorials/vpn/

[McDonald, 2006]
McDonald, Christopher. *An overview of Virtual Private Networks*. AMS Centre for Advanced Technologies. Retrieved: July 10, 2006 from
http://www.intranetjournal.com/foundation/vpn-1.shtml

[Moskowitz, 2006]
Moskowitz, Robert. *What is a Virtual Private Network?* Network Computing. Retrieved: July 7, 2006 from
http://www.networkcomputing.com/905/905colmoskowitz.html

[Tyson, 2006]
Tyson, Jeff. *How virtual Private Networks Work*. How Stuff Works. Retrieved: July 5, 2006 from
http://computer.howstuffworks.com/vpn.htm

[Webopedia, 2006]
Webopedia. *What is VPN?* Retrieved: July 5, 2006 from
http://www.webopedia.com/TERM/V/VPN.html