GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Understanding Virtual Private Networks (VPN) Moye Fraser

Introduction

"What's a VPN?"

"I don't know…but why don't you check it out in cyberspace, then we'll both know!!"

"Yeah…why not…..!!"

This paper explores the realms of cyberspace in an attempt to glean the appropriate information and hopefully an understanding for the author and readers alike that know little about Virtual Private Networks.
This document is divided into two sections. The first section deals with the Basic concepts "So tell me, what's VPN all about…" and the second section focuses on the Protocols and Security Associations "OK, you've got my attention, so tell me more…."

Section 1 – Basics (I know nuf fing!!)

What's a VPN?

A VPN (Virtual Private Network) is an enterprise network which traverses a *shared* or public infrastructure, like the Internet and establishes private and secure connections over an untrusted network, with geographically dispersed users, customers, and business partners. A VPN employs the same security and management policies as applied in a private network. Transport technologies which VPN solutions utilize are the public Internet, service provider IP backbones as well as service provider Frame Relay and ATM networks.

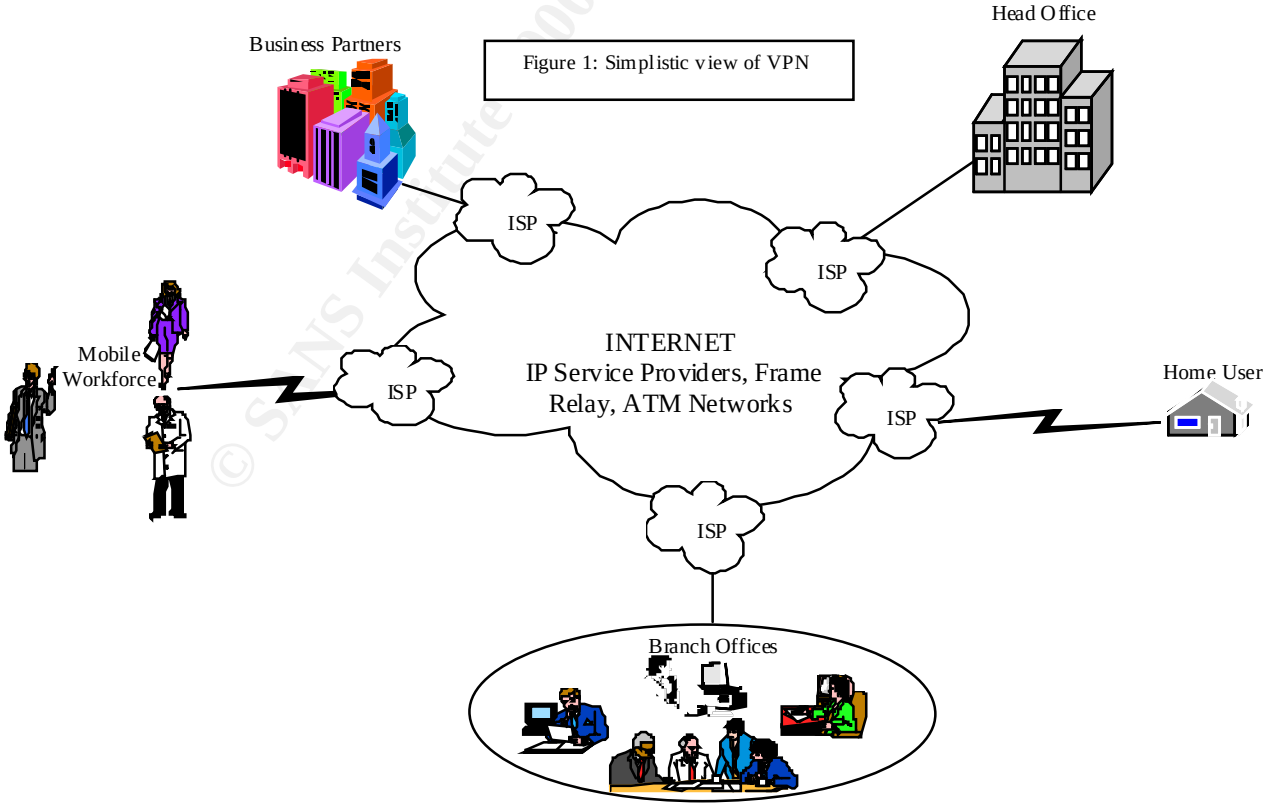
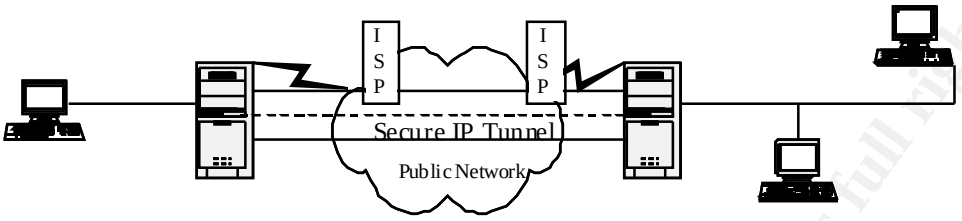


Figure 1: Simplistic view of VPN

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

What's the difference between a private network and a virtual private network?
A private network uses leased lines, whereas a ***virtual*** private network creates a secure tunnel between two endpoints to send data via the public Internet.

Figure 2: Virtual Private Network



What types of VPNs are there?
VPN products can be segmented into 3 categories:

- Firewall-based VPNs make use of firewall's security mechanisms and restrict access to the internal network. They perform address translation; satisfy strong authentication requirements; real-time alarms and extensive logging.
- Hardware-based VPNs provide the highest network throughput of all VPN systems. As there is no operating system or other applications there is no processor overhead. Most hardware-based VPN systems are encrypting routers. Hardware-based products generally tunnel all traffic regardless of protocol. Best hardware VPN packages offer software-only clients for remote installation and include access control features managed by firewalls or other perimeter security devices.
- Standalone VPN application packages offer the most flexibility in how network traffic is managed. Software-based products allow traffic to be tunneled based on address or protocol. Ideal in situations where both endpoints of the VPN are not controlled by the same organisation e.g. client support, business partners. Also suitable when different firewalls and routers are implemented within the same organisation.

What are the basic VPN requirements?
Microsoft VPN Overview White Paper (1999)
A VPN solution should provide:

- User Authentication - The solution must verify the user'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 client's address on the private network 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.
- Multiprotocol Support – The solution must handle common protocols used in the public network. These include IP, IPX, etc.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Where is VPN technology used?
VPN technology allows an enterprise network to securely share information with branch offices, telecommuters, mobile users, home users and business partners. Thus, VPNs can be classified into three categories:

- ***Intranet VPN*** connects fixed locations such as branch offices and home offices
- ***Extranet VPN*** connects business partners such as suppliers and customers
- ***Remote Access VPN*** connects the telecommuters, mobile users, and in some instances smaller remote offices with minimal traffic to the enterprise WAN and corporate computing resources

What are the components of a VPN?
(Reference Guide A Primer for Implementing a Cisco Virtual Private Network)
The essential elements of a VPN are categorized as follows:

- Platform Scalability – each element must be scalable across VPN platforms ranging from small office configuration to larger enterprise implementations; the ability to adapt the VPN to meet changing bandwidth and connectivity needs is crucial in a VPN solution.
- Security – Tunneling, encryption, and packet authentication are necessary for transport security on public networks; in addition, user authentication and access control are essential for assigning network privileges and access.
- VPN services – Bandwidth management and quality of service functions such as queuing, network congestion avoidance, traffic shaping, and packet classification, as well as VPN routing services utilizing Enhanced Interior Gateway Router Protocol (EIGRP), Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) are essential elements of a VPN.
- Appliances – Firewalls, intrusion detection, and active security auditing are essential for comprehensive VPN perimeter security.
- Management – Enforcing security and bandwidth management policies across the VPN and monitoring the network are necessary for a VPN solution.

How does a VPN work?
The concept of VPN technology focuses on the inter-medium between private networks and the public network. The intermediate device, be it software oriented, hardware oriented or a combination of the two, acts on behalf of the private network that it protects. When a local hosts sends data to a host in a remote network, the data must first pass from the private network through the protecting gateway device, travel through the public network, and then pass through the gateway device that is protecting the destination host in the remote network. A VPN protects the data by automatically encrypting it before it is sent from one private network to another, encapsulating it into an IP packet, and then automatically decrypting the data at the receiving end.

How does VPN keep data secure?
The focus of VPN components is encryption. The aim is to restrict access to appropriate users and hosts and to ensure that the data transmitted over the Internet is encrypted so that only authorized system hosts and remote users see the data. A VPN needs complete end-to-

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

end packet encryption. The technique used to wrap encrypted payloads with openly read headers is called tunneling. Once connected, a VPN opens a secure tunnel, in which content is encapsulated and encrypted and the users are authenticated.

How does the use of encryption affect the performance of a network connection?
(Pete Davis – VPN FAQ – http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html)
The use of encryption adds some additional overhead to a session. Most VPN devices, whether hardware or software based, will be able to process encryption for connections up to 10base T speeds. On a lower speed connection like a modem, VPN processing is much faster than delays introduced by the limited bandwidth availability. Packet loss and latency on bad Internet connections potentially affect performance more often, than the encryption overhead.

What is the Internet VPN Process?
(From October 21, 1997 issue of PC Magazine)
1. A client computer calls the local ISP and connects to the Internet
2. Special client software recognizes a specified destination and negotiates an encrypted VPN session.
3. The encrypted packets are wrapped in IP packets to tunnel their way through the Internet
4. The VPN server negotiates the VPN session and decrypts the packets.
5. The unencrypted traffic flows normally to other servers and resources

Why are VPN solutions preferred?
The trump for VPN solutions is the significant cost saving over private leased lines and long distance telephone bills. The lure of the Internet with its global presence and the ability to transmit securely confidential data over an untrusted network, is probably also an appealing factor. VPNs offer an alternative to wide area networks and remote access solutions and often require less money and administration than traditional private networks. Communications links can be done quickly, cheaply and safely across the world. However, having said that, though leased lines are more expensive, they provide safe and reliable data transport as opposed to transportation over the Internet which may result in unaccounted for delays or a sudden loss of connectivity when glitches occur.

When should an enterprise network implement VPN technology?
It is more justifiable to implement VPN solutions when the enterprise network has more locations, longer distances less bandwidth and the quality of service is less critical. The reverse applies when there are fewer locations, shorter distances, more bandwidth and the quality of service is critical. In this case the option for enterprise network to opt for leased lines is probably more viable, especially if there is a premium on the quality of service.

Section 2 – The FUN stuff……

"OK, I get the general idea, but I'm interested in the nuts and bolts of the technology……please explain…..!!"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

What is tunneling?
Tunneling is a technique of using an internetwork infrastructure to transfer data for one network over another network. The data or payload to be transferred can be the frames of another protocol. The tunneling protocol encapsulates the frame in an additional header, instead of sending the original frame as produced by the originating node. The additional header provides routing information to enable the encapsulated payload to traverse the intermediate internetwork. The encapsulated frames are routed between tunnel endpoints over the internetwork. A tunnel is the logical path through which the encapsulated packets travel through the internetwork. When an encapsulated frame arrives at its destination on the internetwork it is unencapsulated and sent on to its final destination. Tunneling includes the entire process of encapsulation, transmission and unencapsulation of frames.
Tunneling technologies include:

- DLSW- Data Link Switching (SNA over IP)
- IPX for Novell Netware over IP
- GRE – Generic Routing Encapsulation (rfc 1701/2)
- ATMP – Ascend Tunnel Management Protocol
- Mobile IP – For mobile users
- IPSec – Internet Protocol Security Tunnel Mode
- PPTP - Point-to-Point Tunneling Protocol
- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protocol

How does it work?

IPSec - Internet Protocol Security (RFCs 2401-2411,2451 Standards Track)
(White Paper for IPSec by Cisco and White Paper VPN Overview Microsoft)

IPSec is an Internet Draft Standard and was developed by the Internet Engineering Task Force (IETF) to ensure secure transfer of information across s a public IP network.

IPSec is a layer 3 protocol standard that combines several different security technologies to provide confidentiality, integrity, and authenticity. IPSec implements network layer encryption and authentication, providing an end-to-end solution in the network architecture.

Internet Key Exchange (IKE) negotiates the security association between two entities and exchanges key material. A security association is a relationship between two or more entities that describe how the entities will use security services to communicate securely. IPSec does not have a mechanism for creating a security association. The IETF has chosen IKE as the standard method of configuring security associations for IPSec. The Internet Key Management Protocol (IKMP) negotiates security associations. IKE creates an authenticated, secure tunnel between two entities and then negotiates the security association for IPSec. This process requires that the two entities authenticate themselves to each other and establish shared keys.
IPSec uses:

- Diffie-Hellman key exchange for deriving key material between peers on a public network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks.
- Data Encryption Standard (DES), for encrypting the data.
- HMAC-Keyed Hashing for Message Authentication in conjunction with MD5-Message Digest Algorithm or SHA-Secure Hash Algorithm.
- Digital certificates signed by a certificate authority to act as digital ID cards.

The IPSec protocol suite defines the information to add to an IP packet to enable confidentiality, integrity, and authenticity controls as well as defining how to encrypt the packet data. The protocols Encapsulated Security Payload (ESP- rfc 2406) and Authentication Header (AH- rfc 2402) are included in the IPSec architecture. IPSec uses AH to provide source authentication and integrity without encryption, while ESP provides authentication and integrity along with encryption. With IPSec, only the sender and recipient know the security key. If the authentication data is valid, the recipient knows that the communication came from the sender and it was not modified en route.

IPSec provides two modes of operation, transport and tunnel mode. In transport mode, only the IP payload is encrypted, and the original IP headers are left intact. However, the layer 4 header will be encrypted and would limit examination of the packet. The advantage to using this mode is that it only adds a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet and would therefore allow an attacker to perform some traffic analysis. In additional to its definition of encryption mechanisms for IP traffic, IPSec defines the packet format for an IP over IP tunnel mode, known as IPSec Tunnel Mode. An IPSec tunnel consists of a tunnel client and a tunnel server, which are both configured to use IPSec tunneling and a negotiated encryption mechanism. IPSec Tunnel Mode uses the negotiated security method to encapsulate and encrypt entire IP packets for secure transfer across a private or public internetwork. The encrypted payload is then encapsulated again with a plain-text IP header, and then decrypts its contents to retrieve the original payload IP packet. The payload IP packet is then processed normally and routed to its destination on the target network.

IPSec sits below the TCP/IP stack, therefore, applications and higher level protocols inherit its behaviour. The layer is controlled by a security policy on each computer and a negotiated security association between the sender and recipient. The policy has a set of filters and associated security behaviours. If a packet's IP address, protocol, and port number match a filter the packet is subject to the associated security behaviour.

PPTP Point-to-Point Tunneling Protocol (RFC 2637 Informational)
The vendor consortium responsible for developing the PPTP protocol includes US Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics and Microsoft. There are several vendors who have created PPTP systems, but the majority of PPTP users implement the Microsoft version.

PPTP is a Layer 2 protocol and is built upon the well-established Internet communications protocol PPP (Point-to-Point Protocol), and TCP/IP (Transmission Control Protocol/Internet Protocol). PPP is multiprotocol, offers authentication, methods of privacy and compression

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

of data. PPTP allows a PPP session to be tunneled through an existing IP connection, no matter how it was set up. PPTP was originally designed as an encapsulation mechanism to allow the transport of non-TCP/IP protocols, such as AppleTalk and IPX, over the Internet using Generic Routing Encapsulation (GRE). It is a technology for securing TCP/IP traffic between Windows 95/98/NT clients, connected to the Internet via PPP and Windows NT servers on local area networks behind corporate firewalls. PPTP uses a TCP connection for tunnel maintenance and GRE encapsulated PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed. Tunneling is achieved because PPTP provides encapsulation by wrapping packets of information (IP, IPX, or NetBEUI) within IP packets for transmission through the Internet. Upon receipt, the external IP packets are stripped away, exposing the original packets for delivery. Encapsulation allows the transport of packets that will not otherwise conform to Internet addressing standards.

The following extract from http://kubarb.phsx.ukans.edu/~tbird/vpn.html about Security concerns are specific to the Microsoft implementations.

- Flawed encryption mechanism – non-random keys, session keys weak hash of user password, key lengths too short (non-configurable)
- Bad password management in mixed Win95/NT environment; static passwords easily compromised
- Vulnerable to server spoofing attacks because packet authentication not implemented, easy denial-of-service attacks even inside firewalls
- MS claims cryptographic weaknesses not yet exploited

Microsoft Remote Access Service (RAS) was originally designed as an access server for dial-up users. RAS is also a tunnel server for PPTP, therefore setting up a PPTP system on an NT server requires configuring the RAS capability on the server, applying all the latest patches, configuring the PPTP specific registry keys, enabling IP forwarding as well as hardening the server itself. RAS supports Password Authentication Protection (PAP), Challenge Handshake Authentication Protocol (CHAP), a Microsoft adaptation of CHAP called MS-CHAP, as well as RSA RC4 and DES encryption technologies.

The initial release of PPTP used MS-CHAP mechanism for end-user authentication. It was found that MS-CHAP was easily compromised and so to minimize the risk of password compromise, Microsoft released MS-CHAP V2. Therefore the dependence of PPTP authentication on MS-CHAP makes it vulnerable to attacks using L0phtcrack. PPTP uses 40-bit, 56-bit and 128-bit encryption. However, the encryption process is weakened by the use of the user's password to create a session key, rather than a randomly generated key and can be compromised via a brute-force attack. Protection against a brute force is a long key length with *purely random* keys.

Note: This protocol has been combined with L2F and superceded by L2TP.

L2F Layer 2 Forwarding (RFC2341 Historic)
This technology was proposed by Cisco. L2F is a media independent layer 2 tunneling protocol offered in Cisco IOS software. It is a transmission protocol that allows dial-up

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

access servers to frame dial-up traffic in PPP. The L2F protocol focuses on providing a standard based tunneling mechanism for transporting link-layer frames (e.g. High-Level Data Link Control (HDLC), async PPP, SLIP, or PPP ISDN) of higher-layer protocols. Packets are transmitted over WAN links to an L2F server (a router) where they are unwrapped and injected into the network. L2F has no defined client and functions in compulsory tunnels only.

Note: This protocol has been combined with PPTP and superceded by L2TP.

L2TP Layer 2 Tunneling Protocol (RFC 2661 Standards Track)
Microsoft and Cisco have combined the best features of PPTP and L2F to produce a standard tunneling protocol called L2TP. L2TP is a network protocol that facilitates the tunneling of PPP frames across an internetwork. It encapsulates the PPP frames to be sent over IP, X25, Frame Relay or ATM networks. The payloads of encapsulated PPP frames can be encrypted and/or compressed. L2TP can also be used directly over various WAN media e.g. Frame Relay without an IP transport layer. L2TP uses UDP and a series of L2TPmessages for tunnel maintenance over IP internetworks. L2TP allows multiple tunnels between the same end-points.

L2TP consists of two pieces, the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). The LAC sits between a LNS and a remote system and forwards packets to and from each. The LNS is the peer to the LAC and is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC.

L2TP supports Compulsory and Voluntary tunnel modes.
The following processes are extracts from Martin W. Murhammer presentation on L2TP, (http://www.as400.ibm.com/tcpip/vpn/itsodocs/l2tp/ITSOl2tp.pdf)

L2TP Compulsory Tunnel
1. The remote user initiates a PPP connection to an ISP
2. The ISP accepts the connection and the PPP link is established
3. The ISP requests partial authentication to learn username
4. ISP maintained database maps users to services and LNS tunnel endpoint
5. LAC then initiates L2TP tunnel to LNS
6. If LNS accepts connection, LAC then encapsulates PPP with L2TP, and forwards over the appropriate tunnel
7. LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames
8. LNS then uses PPP authentication to validate user and then assigns IP address

L2TP Voluntary Tunnel
1. The remote user has pre-established connection to an ISP
2. L2TP Client (LAC) initiates L2TP tunnel to LNS
3. If LNS accepts connection, LAC then encapsulates PPP and L2TP, and forwards over tunnel
4. LNS accepts these frames, strips L2TP, and processes them as normal incoming frames

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. LNS then uses PPP authentication to validate user and then assign IP address

The following paragraph is an extract from RFC2661 re Protocol Overview:
"L2TP utilizes two types of messages, Control messages and Data messages. Control messages are used in the establishment, maintenance and clearing of tunnels and calls. Data messages are used to encapsulate PPP frames being carried over the tunnel. Control messages utilize a reliable Control channel within L2TP to guarantee delivery. Data messages are retransmitted when packet loss occurs. PPP frames are passed over an unreliable Data Channel encapsulated first by an L2TP header and then a Packet Transport such as UDP, Frame Relay, ATM, etc. Control messages are sent over a reliable L2TP Control channel, which transmits packets in-band over the same Packet Transport. Sequence numbers are required to be present in all control messages and are used to provide reliable delivery on the Control channel. Data messages may use sequence numbers to reorder packets and detect lost packets."

L2TP uses Network Control Protocol (NCP) for IP address assignment and the authentication schemes of PPP, namely PAP and CHAP to authenticate users and control access to the network. Securing L2TP requires that the underlying transport make available encryption, integrity and authentication services for all L2TP traffic. This secure transport operates on the entire L2TP packet and is functionally independent of PPP and the protocol being carried by PPP. As such, L2TP is only concerned with confidentiality, authenticity, and integrity of the L2TP packets between tunnel endpoints LAC and LNS. When running over IP, IPSec provides packet-level security via ESP and/or AH.

Thoughts in closing……

At the completion of this practical exercise I now have a better understanding of the technology and its security associations. Having read relevant material on VPNs, I am of the same opinion as Robert Moskowitz http://www.networkcomputing.com/905/905colmoskowitz.html that virtual private networking means different things to different people, especially with vendors and consumers of the communications industry. However, the one area all agree upon and have continued to develop and improve since the technology's inception is SECURITY. As stated in Tina Bird's Virtual Private Networks Frequently Asked Questions, "Security features differ from product to product, but most security experts agree that VPNs include encryption, strong authentication of remote users or hosts, and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network." VPNs are truly emerging as a commendable technology in this very digital era, along with IPSec as the IETF standard for secure TCP/IP.

Many thanks to cyberspace for the infinite source of information and to the references listed below for sharing the information.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Bibliography:

Cisco, "Reference Guide A Primer for Implementing a Cisco Virtual Private Network" (Posted 28/8/2000)
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg,htm

Microsoft Corporation, White Paper – "Virtual Private Networking (VPN) Security" (Posted 5/01/1999)
http://www.microsoft.com/NTServer/commserv/deployment/planguides/VPNSecurity.asp

Microsoft Corporation, White Paper – "An Overview Virtual Private Networking" (Posted 25/6/1998)
http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp

Check Point, "Refining the Virtual Private Network" (May 1999)
http://www.checkpoint.com/products/vpn1/vpndef.html

Professor Raj Jain, "Class lecture on Virtual Private Network"(23/2/01)
http://www.cis.ohio-state.edu/~jain/cis788-99/h_7vpn.htm

T.Bird, P.Clark, D.Farmer, S.Goldhaber, B.Hotte, E.Johnson, I.Khalil, M.Petrovic, L.Phifer, T.Weil, "VPN Information on the World Wide Web"(25/2/01)
http://kubarb.phsx.ukans.edu/~tbird/vpn.html

Stallion Technologies, "What is Internet-based Virtual Private Networking?" (25/2/01)
http://www.stallion.com/html/solutions/vpn-overview.html

Assured Digital, Inc., "Dynamic VPN Switching" (24/2/01)
http://www.assured-digital.com/papers/whyvpn.htm

Robert Moskowitz, Article – "What is a Virtual Private Network?" 23/02/01
http://www.networkcomputing.com/905/905colmoskowitz.html

Ellen Messmer, Article – "Windows 2000 VPN technology causes stir" 12/01/00
http://www.cnn.com/2000/TECH/computing/01/12/vpn.stir.idg/

Tim Greene, Network World VPN Newsletter – "Lightning-fast VPNs" 14/02/01
http://www.nwfusion.com/newsletters/vpn/2001/00408513.html

Timestep, Technical Paper, "Understanding the IPSec Protocol Suite" (March, 2000)
http://www.timestep.com/doctypes/technewbridgenote/pdf/ipsec_nn.pdf

Cisco, White Paper, "IPSec" (Posted July, 2000)
http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/tech/ipsec_wp.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Microsoft Corporation, White Paper– "Using Point-to-Point Tunneling Protocol" (1996)
http://www.microsoft.com/ntserver/commserv/techdetails/prodarch/pptpwp.asp

"FAQ– Microsoft's PPTP Implementation"(1998)
http://www.counterpane.com/pptp-faq.html

Microsoft Corporation, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)"
http://www.counterpane.com/pptpv2-paper.html

Cisco Tech Notes L2F, "Virtual Private Dial-up Network (VPDN)"
http://www.cisco.com/warp/public/131/5.html

Martin W.Murhammer, "Layer 2 Tunneling Protocol", 1999
http://www.as400.ibm.com/tcpip/vpn/itsodocs/l2tp/ITSOl2tp.pdf

Cisco, "Layer 2 Tunnel Protocol Scalability Enhancements" (March 2000)
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc7/l2tpenhc.htm#xtocid206151

SANS GIAC Level 1 Reference:
Gregory J.Ciolek, "Virtual Private Network (VPN) Security" (January 2001)

Relevant RFCs
S.Kent, R.Atkinson, "Security Architecture for the Internet Protocol", Network Working Group, Standards Track, RFC2401, November 1998
http://www.ietf.org/rfc/rfc2401.txt
S.Kent, R.Atkinson, "IP Authentication Header", Network Working Group, Standards Track, RFC2402, November 1998
http://www.ietf.org/rfc/rfc2402.txt
C.Madson, R.Glenn, "The use of HMAC-MD5-96 within ESP and AH", Network Working Group, Standards Track, RFC2403, November 1998
http://www.ietf.org/rfc/rfc2403.txt
C.Madson, R.Glenn. "The Use of HMAC-SHA-1-96 within ESP and AH", Network Working Group, Standards Track, RFC2404, November 1998
http://www.ietf.org/rfc/rfc2404.txt
C.Madson, N.Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", Network Working Group, Standards Track, RFC2405, November 1998
http://www.ietf.org/rfc/rfc2405.txt
S.Kent, R.Atkinson, "IP Encapsulating Security Payload (ESP)", Network Working Group, Standards Track, RFC2406, November 1998
http://www.ietf.org/rfc/rfc2406.txt
D.Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", Network Working Group, Standards Track, RFC2407, November 1998
http://www.ietf.org/rfc/rfc2407.txt

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

D.Maughan, M.Schertler, M.Schneider, J.Turner, “Internet Security Association and Key Management Protocol (ISAKMP)”, Network Working Group, Standards Track, RFC2408, November 1998
http://www.ietf.org/rfc/rfc2408.txt
D.Harkins, D.Carrel, “The Internet Key Exchange (IKE)”, Network Working Group, Standards Track, RFC2409, November 1998
http://www.ietf.org/rfc/rfc2409.txt
R.Glenn, S.Kent, “The NULL Encryption Algorithm and its use with IPSec”, Network Working Group, Standards Track, RFC2410, November 1998
http://www.ietf.org/rfc/rfc2410.txt
R.Thayer, N.Doraswamy, R.Glenn, “IP Security Document Roadmap”, Network Working Group, Informational, RFC 2411, November 1998
http://www.ietf.org/rfc/rfc2411.txt
R.Pereira, R.Adams, “The ESP CBC-Mode Cipher Algorithms”, Network Working Group, Standards Track, RFC2451, November 1998
http://www.ietf.org/rfc/rfc2451.txt
K.Hamzeh, G.Pall, W.Verthein, J.Taarud, W.Little, G.Zorn, “Point-to-Point Tunneling Protocol (PPTP)”, Network Working Group, Informational, RFC2637, July 1999
http://www.ietf.org/rfc/rfc2637.txt
W.Townsley, A.Valencia, A.Rubens, G.Pall, G.Zorn, B.Palter, “Layer Two Tunneling Protocol (L2TP)”, Network Working Group, Standard, RFC2661, August 1999
http://www.ietf.org/rfc/rfc2661.txt

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.