DESIGN ALTERNATIVES FOR Virtual Private Networks

G.I. Papadimitriou[1], M. S. Obaidat[2], C. Papazoglou[3] and A.S. Pomportsis[4]
[1]Department of Informatics, Aristotle University, Box 888, 54124 Thessaloniki, Greece

[2]Department of Computer Science, Monmouth University, W. Long Branch, NJ 07764, USA

[3]Department of Informatics, Aristotle University, Box 888, 54124 Thessaloniki, Greece

[4]Department of Informatics, Aristotle University, Box 888, 54124 Thessaloniki, Greece

Keywords. Virtual private networks (VPNs), PPTP, L2TP, IPSec, tunneling, encryption, SSL, QoS

Abstract. Virtual private networks (VPNs) are becoming more and more important for all kinds of businesses with a wide spectrum of applications and configurations. This paper presents the basic concepts related to VPNs. These include the different types of VPN services, namely Intranet, Extranet and Remote Access VPNs. The concept of tunneling, which is fundamental in VPNs, is discussed in great detail. The tunneling protocols that are employed by VPNs, such as PPTP, L2TP and IPSec are also presented. Furthermore, the issue of Quality of Service, QoS, support in VPN configurations is briefly addressed.

1 Introduction

The best way to come up with a definition of the term Virtual Private Network (VPN) is to analyze each word separately. Having done that, Ferguson and Huston (1998) came up with the following definition:

A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis. Ferguson and Huston also provided a simpler and less formal description. A VPN is a private network constructed within a public network infrastructure, such as the global Internet. Others define a virtual private network (VPN) as a network that allows two or more private networks to be connected over a publicly accessed network. It is similar to wide area networks (WAN) or a securely

I. Papadimitriou G., S. Obaidat M., Papazoglou C. and S. Pomportsis C. (2004).
DESIGN ALTERNATIVES FOR Virtual Private Networks.
In *Proceedings of the 1st International Workshop on Electronic Government and Commerce: Design, Modeling, Analysis and Security*, pages 35-45
DOI: 10.5220/0001404400350045

encrypted tunnel. The chief feature of VPNs is that they use public networks like the Internet rather than using expensive, private leased lines while having similar security and encryption features as a private network.

Virtual Private Networks (VPNs) have evolved as a compromise for enterprises desiring the convenience and cost-effectiveness offered by shared networks, but requiring the strong security offered by private networks. Whereas closed WANs use isolation to ensure data is secure, VPNs use a combination of encryption, authentication, access management and tunneling to provide access only to authorized parties, and to protect data while in transit [2]. To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides the routing information allowing it to traverse the shared or public internetworks to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys [3].

Traditional private networks facilitate connectivity among various network entities through a set of links comprised of dedicated circuits. These are leased from public telecommunication carriers as well as privately installed wiring. The capacity of these links is available at all times, albeit fixed and inflexible. The traffic on these private networks belongs only to the enterprise or company deploying the network. Therefore, there is an assured level of performance associated with the network. Such assurances come with a price. The drawbacks of this approach [3] are related with the money and the time that have to be spent for the installation and maintenance of dedicated links. Additionally, in the case of a private network, the management burden lies entirely on the company, so the overall investment is difficult to justify for many small or medium sized companies.

In this direction, a VPN can reduce costs by replacing multiple communication links and legacy equipment with a single connection and one piece of equipment for each location [6]. In order to extend the reach of a company's Intranet(s), a VPN over the Internet promises two benefits: cost efficiency and global reachability. However there are three major concerns about VPN technology: security, manageability and performance [7].

Security: In order for Virtual Private Networks to be private the transmitted data must be encrypted before entering the Internet, since the Internet is considered an untrusted network [7].

Manageability: VPN management must be able to cope with the high rate of changes in the companies' telecommunication requirements and equipment, while avoiding high expenses [7].

Performance: Since Internet Service Providers (ISPs) deliver IP packets still on a "best effort" basis, the transport performance of a VPN over the Internet cannot be predicted and is variable. Furthermore, security measures (encryption and authentication) can decrease transport performance significantly.

Electronic commerce and electronic government are two areas in which VPNs are recognized as enabling technologies. The amount of business that takes place over the Internet is constantly increasing. Companies are using the Internet not only for retailing merchandise (business-to-consumer e-commerce - B2C), but also as a mean for trading goods and services among themselves (business-to-business e-commerce - B2B). The security of information flowing through a network is an essential element in e-commerce applications. It is a necessary part of building trust in the integrity of transactions made over the information and communication infrastructure. Consumers should have confidence that both the content and the infrastructure are secure [11].

Private networks can not be used to guarantee the security of e-commerce transactions, since it is not practical for a company to maintain a separate infrastructure for each partner, let alone for each customer. The use of a public infrastructure (namely the Internet) combined with VPN technology can ensure both flexible interconnectivity and security [4].

The term e-government refers to the conversion of government information and applications to a digital, accessible format [11]. An example of a widely used service is electronic tax filing. In this context, central and local public sector bodies can share information about citizens appropriately and securely, to deliver more personalized services and improve value for money. Exchanging citizen data in such a dynamic manner is of course only viable if that information is kept secure and this can be achieved in a cost-effective and flexible manner with the use of VPN technology. For example, a local authority can, seamlessly create virtual private networks that link up staff in different sites, allowing them to work securely online together and share information in real-time [10].

This paper is organized as follows: Section 2 presents the different types of VPN services. The concept of tunneling is analyzed in Section 3. The tunneling protocols that are used with VPNs are presented in Section 4. Section 5 discusses the issue of Quality of Service support in VPNs. Finally, Section 6 concludes the paper.

2 Types of VPN Services

A variety of VPN implementations and configurations exists to cater for a variety of needs. Organizations may require their VPN to offer dial-up access, or to allow third parties such as customers or suppliers to access specific components of their VPN [2]. VPNs can be classified into three broad categories: Intranet, Extranet and Remote Access VPNs. The different types of VPNs are illustrated in Figure 1.

2.1 Intranet VPNs

An Intranet VPN connects a number of local area networks (intranets) located in multiple geographic areas over the shared network infrastructure. Typically, this service is used to connect multiple geographic locations of a single company [3]. An Intranet VPN enables the sharing of information and resources amongst dispersed employees. For example, branch offices can access the network at the head office, typically including key resources such as product or customer databases. Intranet access is strictly limited to these networks, and connections are authenticated. Differing levels of access may be allocated to different sites on the Intranet, depending on their purpose [2]. Since an Intranet VPN is formed by connecting two or more trusted sites (corporate LANs), which will certainly be protected by firewalls, most security concerns are alleviated.

2.2 Extranet VPNs

An extranet VPN extends limited access to corporate computing resources to business partners, such as customers or suppliers, enabling access to shared information [8].

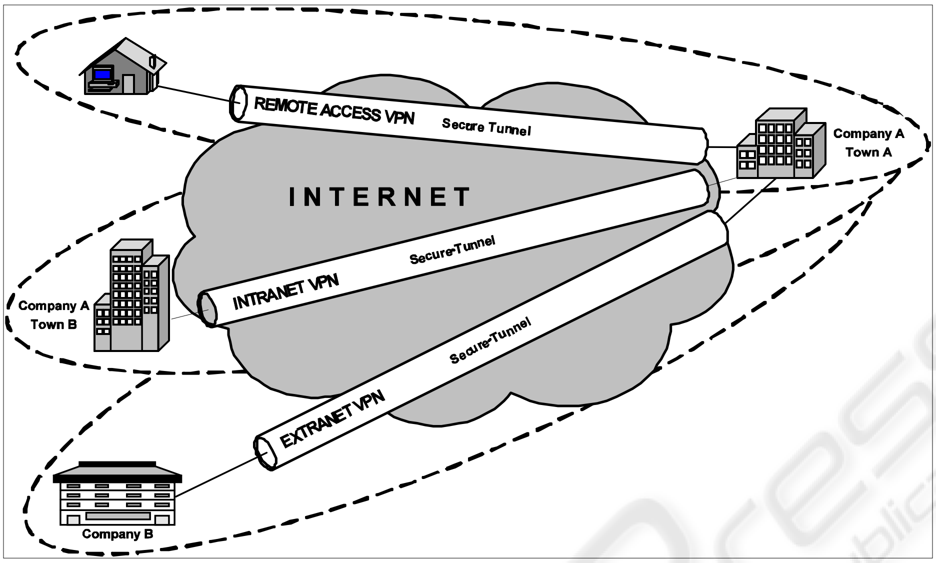

Fig. 1. Types of VPN services

Such users are restricted to specific areas of the Intranet, usually denoted as the De-Militarized Zone (DMZ). It is the responsibility of the firewall and authentication and access management facilities to identify between company employees and other users, and differentiate their access privileges accordingly; employee connections should be directed to the company Intranet, whereas recognized third party connections should be directed to the DMZ [2]. An Extranet VPN helps provide connectivity to new external suppliers and customers within a short period of time. Additionally, an Extranet VPN supports a number of important e-commerce initiatives, providing opportunities for significant cost savings and efficiency gains.

2.3 Remote Access VPNs

A remote access VPN connects telecommuters and mobile users to corporate networks. An ideal VPN enables the remote user to work as if he was at a workstation in the office. Deployment of a remote access VPN can result in considerable cost savings, eliminating the need for the company to manage large modem pools, and replacing the need for toll-calls to these modems with calls to local ISP accounts. By taking advantage of a high-speed access infrastructure such as DSL, cable modem, or ISDN, some of the performance limitations typically associated with remote access can be diminished [2]. In addition, wireless networks enable computers to achieve network connectivity with a reasonable amount of bandwidth without a physical connection [15].

The deployment of remote access VPNs also gives rise to several security concerns. Precautions must be taken to ensure that the corporate network is not compromised by an insecure remote user. The enforcement of company security policies on remote users is a necessary step in this direction, especially regarding virus protection. The security concerns relating to VPNs are discussed in more detail in the following sections.

3 Tunneling

Tunneling is defined as the encapsulation of a certain data packet (the original or inner packet) into another data packet (the encapsulating, or outer packet) so that the inner packet is opaque to the network over which the outer packet is routed [4].

The need for tunneling arises when it is not appropriate for the inner packet to travel directly across the network for various reasons. For example, tunneling can be used to transport multiple protocols over a network based on some other protocol, or it can be used to hide source and destination addresses of the original packet. When tunneling is used for security services, an unsecured packet is put into a secure, usually encrypted packet [4].

Tunneling allows network traffic from many sources to travel via separate channels across the same infrastructure, and it enables network protocols to traverse incompatible infrastructures. Tunneling also allows traffic from many sources to be differentiated, so that it can be directed to specific destinations and receive specific levels of service [8]. Two components can uniquely determine a network tunnel: the endpoints of the tunnel and the encapsulation protocol used to transport the original data packet within the tunnel [4].

Tunneling is the most important mechanism used by VPNs. The idea behind this concept is that a part of the route between the originator and the target of the packet is determined independent of the destination IP address. The importance of tunneling in the context of access VPNs in broadband access networks is twofold [12]. First, the destination address field of a packet sent in an access VPN may indicate a non-globally-unique IP address of a corporate internal server. Such an address must not be exposed to the Internet routers because these routers do not know how to route such packets. Second, very often a packet sent by a user of an access VPN should be forwarded first to the ISP of this user, and only then from the ISP toward the corporate network. In such a case, the first leg of the routing between the host and the ISP cannot be performed based on the destination IP address of the packet, even if this address is globally unique [12].

The devices at one or both ends of a tunnel could be Network Address Translation (NAT) devices. NAT is another important mechanism employed by VPNs. The need for IP address translation arises when a network's internal IP addresses cannot be used outside the network either because they are invalid for use outside, or because

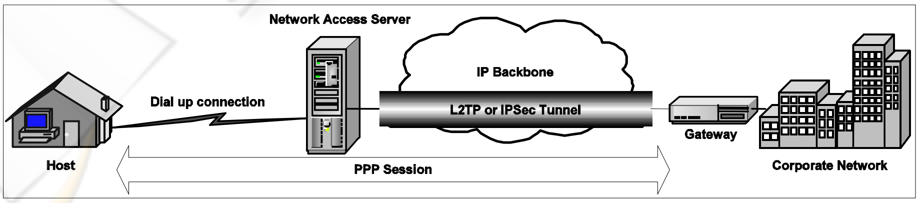

Fig. 2. Compulsory tunneling scenario

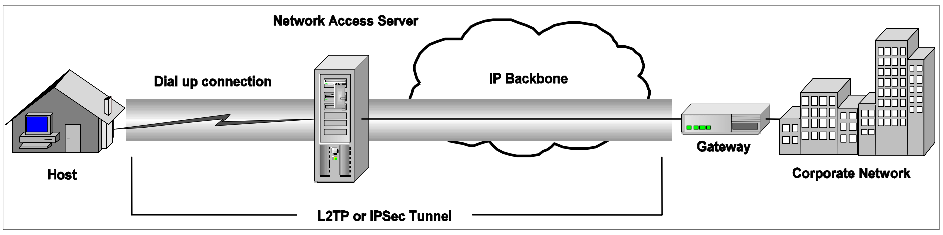

Fig. 3. Voluntary tunneling scenario

the internal addressing must be kept private from the external network. Address translation allows hosts in a private network to transparently communicate with destinations on an external network and vice versa. Network Address Translation is a method by which IP addresses are mapped from one address realm (i.e. network domain) to another, providing transparent routing to end hosts (Srisuresh and M. Holdrege, 1999).

Two main types of tunneling techniques are employed by VPNs [2]:

End-to-End Tunneling, also known as "transport model" tunneling. The VPN devices at each end of the connection are responsible for tunnel creation and encryption of the data transferred between the two sites, so the tunnel may extend through edge devices such as firewalls to the computers sending and receiving the traffic. This solution is extremely secure, because the data never appears on the network in clear-text form. However, performing encryption at the end-hosts increases the complexity of the process of enforcing security policies. The network gateways, which would normally be responsible for enforcing security policy, are used only for forwarding the packets to their destination in this scenario, and as such they possess no knowledge of the content or purpose of the traffic. This is particularly problematic for filtering programs installed at the gateway.

Node-to-Node Tunneling. Node-to-node tunnel creation and termination occurs at the gateway devices comprising the edge of the networks, which are typically firewalls. Under this model, the traffic that reaches the gateway, is encrypted and sent via a dynamically established tunnel to the equivalent device on the receiving LAN, where the data is decrypted to recover its original format, and transmitted over the LAN to the intended recipient. This has an additional security advantage, in that an attacker operating a network analyzer at some point on the network between the two tunnel servers would see IP packets with the source and destination addresses corresponding to those two servers - the true source and destinations are hidden in the encrypted payload of these packets.

There are two main drawbacks associated with node-to-node tunneling [2]:

1. **Poor scalability.** The number of tunnels required for a VPN increases geometrically as the number of VPN nodes increases, and that has serious performance ramifications for large VPNs.
2. **Sub-optimal routing.** Since tunnels represent only the end-points and not the path taken to reach the other end of the tunnel, the paths taken across the shared network may not be optimal, which may cause performance problems.

One can also distinguish between two different tunneling modes; "voluntary" and "compulsory" tunneling. Voluntary tunneling is where the tunnel is created at the request of the user for a specific purpose while compulsory tunneling is where the tunnel is created without any action from the user, and without allowing the user any choice in the matter [1]. The concepts of compulsory and voluntary tunneling are illustrated in Figures 2 and 3, respectively. In both figures, a host is attempting to connect to a corporate network using a dial-up connection to a network access server.

Three major tunneling protocol suites have been developed for building VPNs: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec). These protocols are discussed later.

4 Protocols Employed by VPNs

4.1 Point-to-Point Tunneling Protocol (PPTP)

The Point-to-Point Tunneling Protocol [19] allows the Point-to-Point Protocol (PPP) [9], to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol, but rather describes a new vehicle for carrying PPP. The PPTP Network Server (PNS) is envisioned to run on a general purpose operating system while the client, referred to as a PPTP Access Concentrator (PAC), operates on a dial access platform. PPTP specifies a call-control and management protocol which allows the server to control access for dial-in circuit switched calls originating from a PSTN or ISDN or to initiate outbound circuit- switched connections. A Network Access Server (NAS) provides temporary, on-demand network access to users. This access is point-to-point using PSTN or ISDN lines.

PPTP uses an extended version of the Generic Routing Encapsulation mechanism [20] to carry user PPP packets. These enhancements allow for low-level congestion and flow control to be provided on the tunnels used to carry user data between PAC and PNS. This mechanism allows for efficient use of the bandwidth available for the tunnels and avoids unnecessary retransmissions and buffer overruns. PPTP does not dictate the particular algorithms to be used for this low level control, but it does define the parameters that must be communicated in order to allow such algorithms to work [19]. PPTP allows existing Network Access Server (NAS) functions to be separated using a client-server architecture.

The security of user data passed over the tunneled PPP connection is addressed by PPP, as is authentication of the PPP peers. Because the PPTP control channel messages are neither authenticated nor integrity protected, it might be possible for an attacker to hijack the underlying TCP connection. It is also possible to manufacture false control channel messages and alter genuine messages in transit without detection [19].

PPTP is limited in usage. It offers remote connections to a single point. It does not support multiple connections nor does it easily support network-to-network connections. PPTP’s security is also limited. It does not offer protection from substitution- or playback attacks, nor does it provide perfect forward secrecy. PPTP has no clear mechanism for renegotiation if connectivity to the server is lost [7].

4.2 Layer-2 tunneling protocol (L2TP)

L2TP [21] facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end-users and applications. PPP defines an encapsulation mechanism for transporting multiprotocol packets across layer 2 (L2) point-to-point links. Typically, a user obtains a L2 connection to a Network Access Server (NAS) using one of a number of techniques (e.g., dialup through the telephone system, ISDN, ADSL, etc.) and then runs PPP over that connection. In such a configuration, the L2 termination point and PPP session endpoint reside on the same physical device (i.e., the NAS) [21].

The L2TP tunnel endpoints may optionally perform an authentication procedure of one another during tunnel establishment. This authentication provides reasonable protection against replay and snooping during the tunnel establishment process. This mechanism is not designed to provide any authentication beyond tunnel establishment; it is fairly simple for a malicious user to inject packets once an authenticated tunnel establishment has been completed successfully [21].

Securing L2TP [24] 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 its tunnel endpoints. L2TP is similar to PPTP and they both target the remote access scenario. L2TP delegates security features toward IP Security (IPsec) which is presented later. Besides that it suffers from the same drawbacks as PPTP [7].

4.3 IP Security (IPSec)

IP Security (IPSec) is an open architecture for IP-packet encryption and authentication, thus it is located in the network layer. IPSec adds additional headers/trailers to an IP packet and can encapsulate (tunnel) IP packets in new ones [12]. A number of security services are provided by IPSec, including access control, connectionless integrity, non-repudiation, protection against replay attacks, confidentiality and limited traffic flow confidentiality. These services are provided at the transport layer, offering protection for IP and upper layer protocols [2]. There are three main functionalities of IPSec separated in three protocols. One is the authentication through an Authentication Header (AH); the other is the encryption through an Encapsulating Security Payload (ESP) and finally automated key management through the Internet Key Exchange (IKE) protocol. IPSec provides an architecture for key management, encryption, authentication and tunneling [12]. IPSec was designed to be algorithm independent. It supports several encryption and authentication algorithms, which allow the companies using VPN to select the desired security level for each VPN [6].

IPSec is an optimum solution for trusted LAN-to-LAN VPNs [7]. IPsec can ensure authentication, privacy and data integrity. It is open to a wide variety of encryption mechanisms. It is an application transparent and a natural IP extension, thus ensuring interoperability among VPNs over the Internet. Router vendors and VPN hardware vendors support IPsec. Nevertheless, there are some disadvantages for IPsec. It is bound to the TCP/IP stack. IP addressing is part of IPsec's authentication algorithm. This is less secure than higher layered approaches and it is a problem in dynamic address environments, which are common to ISPs. Moreover, it requires a public key infrastructure, which is still subject to current research, and it does not specify a methodology for access control beyond simple packet filtering [7].

4.4 SOCKS v5 and SSL

SOCKS v5 was originally approved by the IETF as a standard protocol for authenticated firewall traversal [7]. When combined with the Secure Socket Layer (SSL) it provides the foundation for building highly secure VPNs that are compatible with any firewall. SOCKS v5 strength is access control. It controls the flow of data at the session layer (OSI-layer 5) and establishes a circuit between a client and a host on a session-by-session basis. Thus it can provide more detailed access control than protocols in the lower layers without the need to reconfigure each application. SOCKS v5 and SSL can interoperate on top of IPv4, IPsec, PPTP, L2TP or any other lower level VPN protocol. A session layer solution does not have to interfere with the networking transport components, thus the clients are non-intrusive. SOCKS v5 provides plug-and-play capabilities including access control, protocol filtering, content filtering, traffic monitoring, reporting and administration applications. On the minus side, SOCKS v5 decreases performance. Also, client software is required to build a connection through the firewall to transmit all TCP/IP data through the proxy server [7].

4.5 Multiprotocol Label Switching (MPLS)

MPLS VPNs [25] provide a highly scalable technology for Internet Service Providers who want to offer Layer 3 VPN services to their customers. The basic idea is to do (intelligent) layer 3 routing at the edges of the backbone network and to do fast layer 2 forwarding inside the backbone network. Incoming IP packets get an attached MPLS header, they are labeled according to IP header information (mainly the target address, but also type of service and other fields). A label switched path is set up for each route or path through the network. Once this is done, all subsequent nodes may simply forward the packet along the label-switched path identified by the label at the front of the packet. Negotiations of labels between nodes are done by the label distribution protocol of MPLS and a connection is set up for each label-switched path. Thus, MPLS can support quality of service.

MPLS makes the underlying backbone infrastructure invisible to the layer 3 mechanisms. This light-weighted tunneling provides an extendible foundation that provides VPN and other service capabilities. Furthermore, the MPLS architecture enables network operators to define explicit routes [7]. MPLS technologies are useful for ISPs that want to offer their customers a wide band of IP services.

5 Quality of Service Support

Apart from creating a segregated address environment to allow private communications, there is also the expectation that the VPN environment will be in a position to support a set of service levels [26]. Such per-VPN service levels may be specified either in terms of a defined service level that the VPN can rely upon at all times, or in terms of a level of differentiation that the VPN can draw upon the common platform resource with some level of priority of resource allocation [1]. Efforts within the Integrated Services Working Group of the IETF have resulted in a set of specifications for the support of guaranteed and controlled load end-to-end traffic profiles using a mechanism, which loads per-flow state into the switching elements of the network. There are a number of caveats regarding the use of these mechanisms, in particular as related to the ability to support the number of flows that will be encountered on the public Internet. Such caveats tend to suggest that these mechanisms will not be the ones that will ultimately be adopted to support service levels for VPNs in very large networking environments [1].

The Differentiated Services (DiffServ) approach tries to provide a solution for Quality of Service (QoS) support with better scalability than Integrated Services (IntServ). Differentiated services can provide two or more QoS level without maintaining per-flow state at every router. The idea of DiffServ approach is to use the DiffServ field in the IP header to designate the appropriate DiffServ level that the packet should receive. DiffServ can provide scalability by aggregating the flows into a small number of DiffServ classes and by implementing traffic conditioning at the boundary routers of a network or an administrative domain [12].

It must be noted that QoS and VPN techniques introduce new challenges. They need extensive configurations in the routers. The local configurations have to be consistent across the network. Many companies may not have the knowledge and resources to deploy and manage enhanced Internet services by themselves. Rather, they will outsource the service management to their Internet service provider [13].

6 Conclusions

People increasingly depend on remote access to do their jobs, and demand is growing for access to large volumes of corporate information. Moreover, the upsurge of e-commerce means that companies are implementing business applications which share information among sites, extending the reach of their business to partners, contractors, and supply chain. In all these areas, VPNs promise to reduce recurring telecommunications charges, minimize the amount of access equipment required, and give managers better control over their networks [6]. VPNs offer a more affordable, scalable way to meet the demands of a growing community of remote users and to manage branch office connectivity.

References

1. Ferguson, P. and Huston, G., 1998. What is a VPN?. White paper, available online at http://www.employees.org/~ferguson.
2. Hunt, R. and Rodgers, C., 2003. Virtual Private Networks: Strong Security at What Cost?. Available at http://citeseer.nj.nec.com/555428.html.
3. Arora, P, Vemuganti, P.R. and Allani, P., 2001. Comparison of VPN Protocols – IPSec, PPTP, and L2TP. Project Report ECE 646, Fall 2001, available at http://ece.gmu.edu/courses/ECE543/reportsF01/arveal.pdf.
4. Strayer, W.T. and Yuan, R., 2001, Introduction to virtual private networks. Available online at http://www.awprofessional.com/articles/.
5. Brahim, H.O., Wright, G., Gleeson, B., Bach, R., Sloane, T., Young, A., Bubenik, R., Fang.L., Sargor, C., Weber, C., Negusse, I., Yu, J. J., 2003. Network based IP VPN Architecture using Virtual Routers, Internet draft <draft-ietf-l3vpn-vpn-vr-00.txt>.

6. Younglove, R., 2000. Virtual Private Networks: Secure Access for E-Business. *IEEE Internet Computing*, pp. 96, Volume 4, Number 4.

7. Günter, M., 2001. Virtual Private Networks over the Internet. Available at http://citeseer.nj.nec.com/480338.html.

8. Wright, M. A., 2000. Virtual Private Network Security. *Network-Security*, pp. 11-14, July 2000.

9. Network Working Group (Simpson, W., Editor), 1994. The Point-to-Point Protocol (PPP). RFC 1661.

10. Boon, S., 2003. Delivering the Foundations for Joined up E-Government. Available at http://www.publicnet.co.uk/publicnet/fe031021.htm

11. Boudriga N. and Obaidat, M. S., 2002. Driving Citizens to Information and Communications Technology. Mediterranean Development Forum 4, October 2002.

12. Cohen, R., 2003. On the Establishment of an Access VPN in Broadband Access Networks. *IEEE Communications Magazine*, pp. 156-163, February 2003.

13. Braun, T., Günter, M., Kasumi, M. and Khalil, I., 1999. Virtual Private Network Architecture. CATI Project Deliverable, January 1999, available at http://www.tik.ee.ethz.ch/~cati/deliverables.html.

14. Harding, A., 2003. SSL Virtual Private Networks. *Computers & Security*, Volume 22, Issue 5, pp. 416-420, July 2003.

15. Ribeiro S., Silva F. and Zuquete A., 2004. A Roaming Authentication Solution for Wifi using IPSec VPNs with client certificates, *TERENA Networking Conference*, June 2004.

16. Srisuresh P. and Holdrege M., 1999. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663.

17. Rosenbaum, G., Lau, W. and Jha, S., 2003. Recent directions in virtual private network solutions. *IEEE International Conference on Networks* (ICON 2003), September 2003.

18. Gleeson, B., Lin, A, Heinanen, J., Armitage, G. and Malis, A., 2000. A Framework for IP Based Virtual Private Networks. RFC 2764.

19. Pall, G., Verthein, W., Taarud, J., Little, W. and Zorn, G., 1999. Point-to-Point Tunneling Protocol (PPTP). RFC 2637.

20. Hanks, S., Li, T., Farinacci, D. and Traina, P., 1994. Generic Routing Encapsulation (GRE), RFC 1701.

21. Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and Palter, B., 1999. Layer Two Tunneling Protocol. RFC 2661.

22. Yuan, R., 2002. The VPN Client and the Windows Operating System. January 2002. Available online at: http://www.awprofessional.com/articles/

23. Rekhter Y., Watson T.J. and Li T., 1995. A Border Gateway Protocol 4 (BGP-4). RFC 1771.

24. Patel B., Aboba B., Dixon W., Zorn G. and Booth S., 2001. Securing L2TP using IPsec. RFC 3193.

25. Tomsu P. and Wieser G., 2002. *MPLS-Based VPNs – Designing Advanced Virtual Networks*, Prentice-Hall.

26. Zeng J. and Ansari N., 2003. Toward IP Virtual Private Network Quality of Service: A Service Provider Perspective. *IEEE Communications Magazine*, pp. 113-119, April 2003.

27. Braun T., Guenter M. and Khalil I., 2001. Management of Quality of Service Enabled VPNs. *IEEE Communications Magazine*, pp. 90-98, May 2001.