Technical Overview of Virtual Private Networks(VPNs)

Article *in* International Journal of Scientific Research · June 2012

DOI: 10.15373/22778179/JULY2013/32

2 authors, including:

Manjaiah D H
Mangalore university
130 PUBLICATIONS **478** CITATIONS

SEE PROFILE

Volume : 2 | Issue : 7 | July 2013 • ISSN No 2277 - 8179

Technical Overview of Virtual Private Networks(VPNs)

International Journal of Scientific Research

Computer Science

KEYWORDS :

Sridevi	Assistant Professor,Department of computer Science,Karnatak University Dharwad
Dr.Manjaiah D.H	Professor, Department of Computer Science,Mangalore University Managalore.

ABSTRACT

In this paper we will discuss some of the dominant VPN technologies have been reviewed and compared. Finally, a comparison is made among different VPN technologies and a decision is made to choose a particular VPN technology to add mobility support.

1. Introduction

A Virtual Private Network (VPN) is a connection which provides secure private communication over an insecure network such as the public network [19]. Typically, a VPN provides connections between fix network devices. The term "Private" means that all the traffic inside the VPN is encrypted and the resources are only shared among an authorized group of users, and are controlled by different levels of access control. The term "Virtual" indicates that VPN looks like a private network from the user's perspective and consists of an independently administered virtual topology, although the underlying network is shared by anyone using the network. Furthermore, VPN is cheap, as it normally uses the public network instead of costly leased line services.

Originally, the VPN was associated with Frame Relay networks [10]. Companies used dedicated lines and layer 2 services such as Frame Relay to interconnect their nodes with links that they owned. Frame relay networks are considered secure, as customer traffic will be sent through a predetermined path (Permanent Virtual Circuit). However, with the rapid development of IP network, VPN began to migrate from a conventional Layer 2 Frame Relay to a Layer 3 IP-based network.

The primary advantages of IP VPNs over Frame Relay VPNs are:

- Reduced network cost (Internet Service Providers charge more for a Frame Relay Permanent Virtual Circuit).
- Easy to provide network connectivity to geographically dispersed offices and remote users.
- Convergence of other services such as voice and video, which reduces cost.

Currently, VPNs provide connections at different OSI layers. VPN has become more and more popular for a variety of reasons; a VPN can be encrypted for security or to defeat firewalls and proxy servers. VPNs make it easier to manage geographically separated physical networks as if they were one network. Businessmen and other persons from remote offices often use VPNs to connect to company networks.

2. VPN Classification

VPN can be classified in a variety of ways.

2.1 By topology:

2.1.1 Peer to Peer VPN

Peer to Peer VPN sets up a secure tunnel between two computers via public networks. An IP address will be assigned to each end of the tunnel so that the two computers can communicate with each other as if they are connected by a physical Ethernet cable. The limitation of Peer to Peer VPN is that the VPN tunnel can be shared by only two computers. This solution is not widely used due to the limitation. The topology of Peer to Peer VPN is shown as follows

Figure 1: Peer to Peer VPN

2.1.2 Client to Server VPN

Client to Server VPN sets up a secure tunnel between a VPN client and a specific network via public networks. The VPN client can connect to all the computers inside the specific network. However, unlike peer to peer VPN, Client to Server VPN only encrypts the traffic between VPN Client and VPN server, and the traffic between VPN server and other computers in the specific network is not protected. Although it does not protect the full path between end users(no protection within the company network), client to server VPN is widely used in today's networks because businessmen outside usually want to connect to company network, not a single computer.

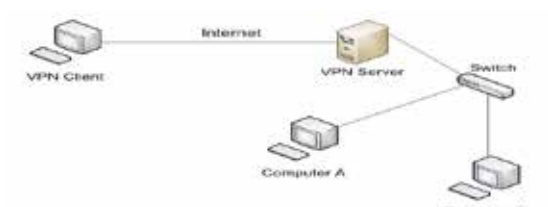

Figure 2: Client to server VPN

2.1.3 Site to Site VPN

Site to Site VPN sets up a secure tunnel between 2 networks via the public Internet where the tunnel endpoints are a VPN concentrator and a VPN server. These VPNs only encrypt the traffic between VPN concentrators and VPN servers, and any traffic outside the tunnel endpoints is not protected. Site to Site VPN is widely used between company's main office and remote office.

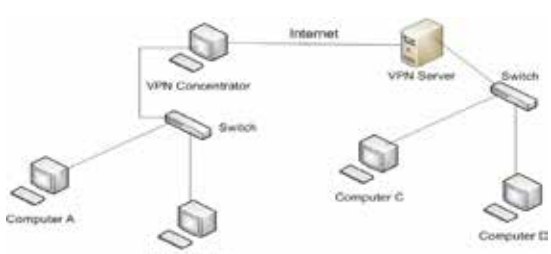

Figure 3: site to site VPN

2.2 By protocols:
The choice of a VPN protocol depends on the type of traffic to be sent via the tunnel. VPN protocols can be classified according to OSI layers of received packets used for encryption. There are currently 3 kinds of VPN:

2.2.1 Layer 2 VPN
A Layer 2 VPN encapsulates packets on the OSI Layer 2: Data Link Layer. Main Layer 2 VPN protocols are: Layer 2 MPLS VPN, OpenVPN, PPTP and L2TP. Chapter 2.3 discusses the details of Layer 2 VPN protocols.

2.2.2 Layer 3 VPN
Layer 3 VPN encapsulates packets on the OSI Layer 3: Network Layer. Main Layer 3 VPN protocols are: Layer 3 MPLS VPN, IPsec and OpenVPN. Chapter 2.4 discusses the details of Layer 3 VPN protocols.

2.2.3 Layer 4 VPN
Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are Layer 4 VPN protocols that encrypt segments of network connections at the OSI Layer 4 (transport layer). A prominent use of TLS is for securing web traffic carried by HTTP to form HTTPS. Although TLS is widely used, it can only encrypt Layer 4 packets, not lower layers. This greatly limits its applications.

2.3 Layer 2 MPLS VPN

Multiprotocol Label Switching (MPLS) [17] is a mechanism used in high-performance networks and it carries data from one network node to the other. In an MPLS network, labels are added to each data packet and packets are switched according to these labels. MPLS is a scalable protocol as MPLS labels can be added to various network protocols. Layer 2 MPLS VPN is a type of Virtual Private Network (VPN) that uses MPLS labels to transport OSI Layer 2 packets. It is commonly used when customers want to communicate between remote offices through the Internet Service Provider (ISP) network [12], but they have no access to the public Internet. The edge routers on the Service provider side are called Provider Edge (PE) routers and the edge routers on the customer side are called Customer Edge (CE) routers. The topology of a Layer 2 MPLS VPN network is shown in Figure 4.

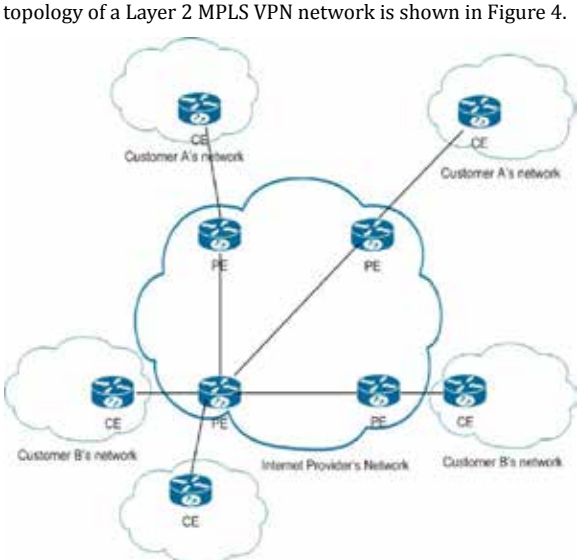

Figure 4 : Layer 2 MPLS Network Topology

Layer 2 MPLS VPN networks are quite fast. All kinds of traffic, i.e. Frame Relay (FR), Asynchronous Transfer Mode (ATM) and Ethernet traffic, can be sent through the network. The Provider Edge (PE) routers are not responsible for routing and they only forward packets according to Layer 2 information and MPLS labels. All traffic going through Internet Provider's network is protected by Layer 2 MPLS VPN because other customers cannot access these packets. Security is a big issue for Layer 2 MPLS VPN. If several customers share a Layer 2 medium on ISP network, there is often no control over the packets transferred to that device so that the packets from other customers can be easily captured. The chance for using exclusive network devices on ISP network is very limited because of the high cost. One solution is to use a port-based Ethernet connection between two physical data ports provided across an MPLS network. This means that the Layer 2 packets are encapsulated in 802.1Q Ethernet frames and sent to the destination. Another big security issue is that Layer 2 MPLS VPN packets are not encrypted in ISP network[11]. Layer 2 MPLS VPN has not been chosen to add mobility support because of its security issues.

3. OpenVPN
OpenVPN is an open source Layer 2 or Layer 3 tunneling protocol. It works by encapsulating Layer 2 and Layer 3 packets inside UDP or TCP packets and sending them to the destination. It uses OpenSSL for encryption and implements SSL and TLS (the advanced and standardized version of SSL) [2]. It uses pre-shared, certificate-based, and username/password-based key for authentication. It is capable of establishing direct links between computers across network address translators (NATs) and firewalls. It is easy to configure but it has not been widely used [5]. The packet structure of Open VPN is shown in Figure 5.

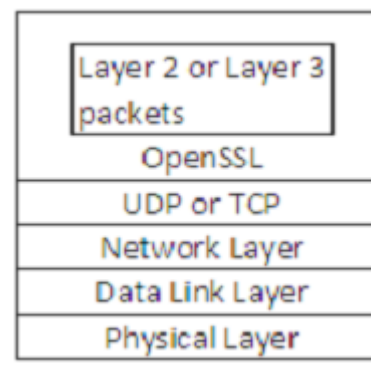

Figure 5 : Packet Structure of OpenVPN

The main problem in OpenVPN is security. The key exchange in TLS is weak, for example completely anonymous sessions are vulnerable to man-in-the-middle attacks and public key and private keys are exposed in RSA key exchange. OpenVPN is not recommended when security is a concern [3]. OpenVPN by itself is not useful for mobile business scenarios as it has no native ability to cope with mobile clients.

3.1 Point-to-Point Tunneling Protocol (PPTP)
PPTP [1] is a layer 2 tunneling protocol which works by sending a regular PPP session [16] to a peer with the Generic Routing Encapsulation (GRE) protocol. A second session is used to initiate and manage the GRE session. This session is a simple TCP connection from the PPTP client to port 1723 on the PPTP server. PPTP also works in sending IPX packets [7].The main disadvantage in PPTP is the security. PPTP itself does not specify any authentication or encryption algorithms, and the only algorithms used are inside the PPP sessions [16]. Microsoft Challenge-handshake authentication protocol (MS-CHAP) [14] and Microsoft Point-to-Point Encryption (MPPE) [15] are used for PPP authentication and encryption. MS-CHAP is known to be a weak algorithm, easily cracked by software such as L0phtcrack. MPPE is also weak in security because an attacker can spoof resynchronize keys packets easily [13]. Also, there are many unauthenticated control packets that are readily spoofed [1]. PPTP is widely used in Microsoft Windows and some parts of it are patent encumbered. It has no native ability to cope with mobile clients.

3.2 Layer 2 Tunneling Protocol (L2TP)
L2TP [8] is an open source layer 2 tunneling protocol. It is originally used to encapsulate PPP frames into UDP packets and send UDP packets over existing networks. The two endpoints of an

L2TP tunnel are the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC receives PPP packets from users, encapsulates the PPP packets into UDP packets and then sends these to the LNS. The LNS decapsulates the UDP packets and sends the PPP packets to the destination computers. IP packets can also be tunnelled through L2TP and the process of tunneling IP packets is similar to that of tunneling PPP packets. L2TP does not provide strong authentication by itself and often uses IPsec to secure the tunnel [8]. The topology of an L2TP tunnel is shown in Figure 6.

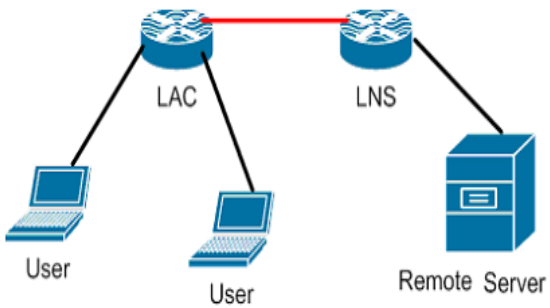

Figure 6 : L2TP Topology

A problem with L2TP/IPsec tunneling is that it does not support NAT. However, IPv6 (next generation network) has an almost infinite number of addresses that makes NAT unnecessary [6]. L2TP by itself is not useful for mobile business scenarios as there is no native ability to cope with mobile clients.

3.3 Layer 3 MPLS VPN

Similar to Layer 2 MPLS VPN, Layer 3 MPLS VPN, also known as L3VPN, is a type of VPN that uses MPLS labels to transport OSI Layer 3 packets. It is commonly used when customers want to communicate between remote offices through the Internet Service Provider (ISP) network [12]. Customers can still access the public Internet through L3VPN via an Internet Customer Edge router though strict security policies should be applied to the Internet Customer Edge router. The topology of a Layer 3 MPLS VPN network is shown in Figure 7.

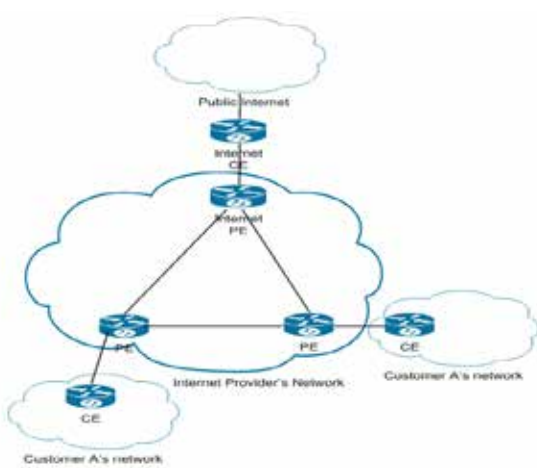

Figure 7 : Layer 3 MPLS Network

Layer 3 packets are protected by Layer 3 MPLS because other customers cannot access these packets. Unlike Layer 2 MPLS VPN, the Provider Edge (PE) routers in Layer 3 MPLS VPN are responsible for routing and forwarding packets according to IP addresses and MPLS labels. Security is also a big drawback of Layer 3 MPLS VPN. The VPN does not provide any confidentiality or integrity services. This means that a service provider can easily sniff VPN data and there is no guarantee that the packets are not corrupted or changed during transfer. Customers can only trust the service provider, or give up this VPN solution [11]. Layer 3 MPLS VPN has not been chosen to add mobility support because of its security issues.

3.4 Internet Protocol Security (IPSec)

(IPsec) [4,9] is a suite of protocols for securing IP communications at the OSI Network Layer. It encrypts IP frames into IPsec packets and sends the packets to the other end of the networks. It supports peer authentication, data integrity and data confidentiality (encryption). IPsec can be used to protect IP packets (OSI Layer 3 packets) between a pair of hosts (Peer to Peer VPN), between a security gateway and a host (Client to Server VPN), or between a pair of security gateways (Site to Site VPN). Compared to other VPN protocols, IPsec is a suite of VPN protocols with very strong security. It is very popular and has already integrated into the next generation network (IPv6). IPsec is a complex system which includes encapsulation, encryption, authentication, and key exchange and management. IPsec by itself is not useful for mobile business scenarios as there is no native ability to cope with mobile clients. An IPsec extension adds mobility support to IPsec, which is discussed in RFC 4555 [18]. However, that solution has some limitations.

4. Choosing VPN to add mobility support

The VPN protocols examined do not have a native ability to cope with mobile clients. Adding mobility support to existing VPN protocols is one way to solve the problem. The final solution should have a wide range of applications, good security, small handoff time and simplicity of usage. A VPN that transfers Layer 2 packets will be chosen as it has a better range of applications and can transfer almost all kinds of Internet packets: IP packets, non-IP packets (such as IPX packets) and Layer 2 packets (such as PPP packets [16]). A brief comparison among different Layer 2 VPN is shown below.

- Layer 2 MPLS VPN has big security issues. It assumes that ISP network can be trusted and all the packets within ISP network are not encrypted.
- OpenVPN is not widely used and is relatively weak in security
- PPTP is weak in security and is patent encumbered. It is difficult to modify PPTP.
- L2TP provides Layer 2 tunneling functions and together with IPsec provides good security. Although L2TP/IPsec tunnels do not support NAT, IPv6 (next generation network) has an almost infinite number of addresses that makes NAT unnecessary.

The L2TP/IPsec tunnel has been chosen to add mobility support because it has a good range of applications (transferring Layer 2 packets) and is strong in security (using IPsec).

5. Conclusion

A Virtual Private Network (VPN) is a connection which provides secure private communication over an insecure network. VPNs can be classified by topology or by protocol and the examined VPNs do not have native mobility support. L2TP is an open source layer 2 tunneling protocol which does not provide strong authentication by itself and often uses IPsec to secure the tunnel. L2TP/IPsec is most suitable for adding mobility support as other VPN protocols have problems with security or other issues.

REFERENCE

[1] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", IETF RFC 2637, July 1999. | [2] "OpenSSL", OpenSSL project website, http://www.openssl.org, accessed October 8, 2008. | [3] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", IETF RFC 5246, August 2008. | [4] J. H. Carmouche, "IPsec virtual private network fundamentals", Indianapolis: Cisco Press, 2007. | [5] M. Feilner, "OpenVPN: building and integrating virtual private networks", Birmingham: Packt, 2006. | [6] P. Loshin, "IPv6: Theory, Protocol, and Practice, 2nd ed.", United States of America: Elsevier, 2003. | [7] K. Hamzel, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", IETF RFC 2637, 1999. | [8] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn and B. Palter, "Layer Two Tunneling Protocol (L2TP)", IETF RFC 2661, August 1999. | [9] R. Thayer, N. Doraswamy and R. Glenn, "IP Security Document Roadmap", IETF RFC 2411, November 1998. | [10] From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task", Cisco Website, ttp://www.cisco.com/warp/ public/cc/so/neso/vpn/vpnsp/vpnmi_wp.pdf | [11] M. H. Behringer and M. J. Morrow, "MPLS VPN Security", Cisco Press, June 2005. | [12] C. Lewis and S. Pickawance, "Selecting MPLS VPN Services", Cisco Press, 2006. | [13] O. Kolesnikov and B. Hatch, "Building Linux Virtual Private Networks (VPNs)", New Riders, 2002. | [14] G. Zorn, "Microsoft PPP CHAP Extension, Version 2", IETF RFC2759, January 2000. | [15] G. Pall and G. Zorn, "Microsoft Point-To-PointEncryption (MPPE) Protocol", IETF RFC3078, March 2001. | [16] W. Simpson, "The Point-to-Point Protocol (PPP)", IETF RFC1661, July 1994. | [17] E. Rosen, A. Viswanathan and R. Callon, "Multiprotocol Label Switching Architecture", IETF RFC 3031, January 2001. | [18] P. Eronen, Ed, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", IETF RFC 4555, June 2006. | [19] R. Deal, "The Complete Cisco VPN ConfigurationGuide", Cisco Press, 2006. |