International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

Review on protocols of Virtual Private Network

Shaikh Shahebaz[1], Sujay Madan[2], Sujata Magare[3]

[1] Student, Dept. Of MCA [JNEC College] Cidoco N-6, Aurangabad, Maharashtra, India
[2] Student Dept. of MCA [JNEC College] Cidoco N-6, Aurangabad, Maharashtra, India
[3]AssistantProfessor, Dept. of MCA, [JNEC College]Cidoco N-6, Aurangabad, Maharashtra, India

---

Abstract – *Virtual: Virtual means not real or in a different state of being. In a VPN, private communication between two or more devices is achieved through a public network the Internet. Therefore, the communication is virtually but not physically there.*

Private: Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.

Key Words: VPN Tunneling, VPN protocols, Point 2 Point Tunneling protocol, Layer 2 Tunneling Protocol.

1. INTRODUCTION

The VPN connection allows users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by public internetworks (such as the Internet). From the user's perspective, the VPN connection is a point-to-point connection between the user's computer & a corporate server. The nature of the intermediate internetworks is irrelevant to the user because it appears as if the data is being sent over a dedicated private link. VPN connection also allows a corporation to connect to branch offices or to other companies over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites. In both these cases, the secure connection across the internetwork appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork. Hence, the name - *virtual private network*.

1.1 Protocols used in VPN:

[A]. Point to Point Tunnel Protocol (PPTP)

Point to Point Tunneling Protocol is an OSI layer two protocol built on top of the Point to Point Protocol (PPP). PPTP connects to the target network by creating a virtual network for each remote client. The PPTP control connection carries the PPTP call control and management message that is used to maintain the PPTP tunnel [3].PPTP allows a PPP session, with non-TCP/IP protocols, to be tunneled through an IP network. The authentication protocols used by PPTP are: Extensible Authentication Protocol (EAP), Microsoft Challenge-Handshake uthentication Protocol (MCHAP), Shiva Password Authentication Protocol (SPAP), and Password Authentication Protocol (PAP).

[B]. Layer 2 Tunneling Protocol (L2TP)

Asynchronous Transfer Mode, Frame Relay and X.25 networks use L2TP as tunneling protocol for data transmission between the communicating nodes. L2TP is also operated at the layer 2 of OSI architecture. One tunnel can allow multiple connections. Layer two tunneling protocol encapsulates data in PPP frames and is capable of transmitting non-IP protocols over an IP network. L2TP connections use the same authentication mechanisms as PPP connections, such as EAP, CHAP, and MSCHAP. L2TP tunneling is accomplished through multiple levels of encapsulation. The PPP data is encapsulated within a PPP header and an L2TP header. The encapsulated L2TP packet is further encapsulated in a UDP header. The final packet is encapsulated with an IP header containing the source and destination IP addresses of the VPN client and VPN server.

[C].Secured Socket Layer

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It's used to give remote users with access to Web applications, client/server applications and internal network connections.

[D].OpenVPN

VPN Unlimited currently supports only OpenVPN via the UDP port. It is a simple OSI transport layer protocol for network applications based on internet Protocol (IP). UDP is the main alternative to TCP and one of the oldest network protocols, introduced in 1980. UDP is an ideal protocol for network applications in which perceived latency is critical such as gaming, voice and video communications. The

protocol permits individual packets to be dropped and UDP packets to be received in a different order than that in which they were sent, allowing for better performance.

2. PPTP

A consortium, consisting of Ascend Communications, 3Com, ECI Telematics, U.S. Robotics, and Microsoft, developed the PPTP specification for the tunneling of data across the Internet.The PPTP protocol [4] is built on the well-established Internet Communications Protocol PPP (point-to-point protocol), and TCP/IP (Transmission Control Protocol/Internet Protocol).Multiprotocol PPP offers authentication as well as methods of privacy and compression of data. IP is routable, and has an Internet infrastructure. PPTP allows a PPP session to be tunneled through an existing IP connection, no matter how it was set up. An existing connection can be treated as if it were a telephone line, so a private network can run over a public one. Tunneling is achieved because PPTP provides ncapsulation 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. PPTP encapsulates Point-To-Point Protocol (PPP) frames into IP data grams for transmission over an IP-based Internet work, such as Internet. To encapsulate PPP frames as tunneled data, PPTP uses a TCP connection known as PPTP control connection to create, maintain and terminate the tunnel & a modified version of Generic Routing Encapsulation (GRE). PPTP inherits encryption or compression or both, of PPP payloads from PPP. Authentication that occurs during the creation of PPTP-based VPN connection uses the same authentication mechanisms as PPP connections, such as:

· Extensible Authentication Protocol (EAP).
· Challenge Handshake Protocol (CHAP).
· Shiva Password Authentication Protocol (SPAP) and
· Password Authentication Protocol (PAP).

2.1 PAP

Password Authentication Protocol (PAP) provides a method for the peer to establish its identity using a 2-way handshake. This is one of the ways of user authentication. A stronger authentication such, as CHAP must negotiate prior to PAP.

GRE

The Protocol GRE (Generic Routing Encapsulation) is for performing encapsulation of an arbitrary network layer protocol over another arbitrary network layer protocol. The payload is first encapsulated in a GRE packet, which possibly includes the route. The resulting GRE packet can then be encapsulated in some other protocol and then forwarded. The outer protocol is the delivery protocol.

3. Tunneling in PPTP

A tunnel is defined by PNS (PPTP network server) - PAC (PPTP access concentrator) pair. The tunnel protocol is defined by a modified version of GRE .The tunnel carries PPP datagrams between the PAC and the PNS. A control connection operating over TCP controls the establishment, release and maintenance of sessions and of the tunnel itself.

Comparison of VPN Protocols: IPSec, PPTP, and L2TP

Before PPP tunneling can occur between a PAC and PNS, a control connection must be established between them. The control connection is a standard TCP session over which PPTP call control and management information is passed. This tunnel is used to carry all user session PPP packets for sessions involving a given PNS-PAC pair.

3.1 Types of Tunneling:

Tunnels can be created in various ways:

3.1.1 Compulsory Tunneling:

Compulsory tunneling (also referred to as NAS-initiated tunneling) enables users to dial to NAS(Network Access Servers), which then establishes tunnel to the server. The connection between the client of the user and the NAS is not encrypted.

3.1.2 Voluntary Tunneling

Voluntary tunneling (also referred to as client-initiated tunneling) enables clients to configure and establish encrypted tunnels to tunnel servers without an intermediate NAS participating in the tunnel negotiation and the establishment. For PPTP, only voluntary tunneling is supported. PPTP works by encapsulating the virtual private network packets inside of PPP packets which are in turn encapsulated in Generic Routing Encapsulation (GRE), packets sent over IP from the client to the gateway PPTP server and back again. In conjunction with this encapsulated data channel, there is a TCP-based control session. The control session packets are used to query status and convey signaling information between client and the server. The control channel is initiated by the client to the server on TCP port. In most cases this is a bi-directional communication channel where the client can send requests to the server and vice-versa.

3.2 Encryption in PPTP

Microsoft Point-to-Point Encryption (MPPE) may be used with PPTP to provide an encrypted connection but PPTP itself doesn't use encryption. MPPE uses the RC4 algorithm with either 40 or 128-bit keys. All keys are derived from the cleartext authentication password of the user. RC4 is stream cipher; therefore, the sizes of the encrypted and decrypted frames are the same size as the original frame.

RC4 is stream cipher designed by Ron Rivest for RSA data security. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is the use of random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100 years. Eight to sixteen machine operations are required per o/p byte; and the cipher can be expected to run very quickly in software. Independent analysts have scrutinized the algorithm and it is considered secure. For VPNs, IP data grams sent across the Internet can arrive in a different order from the one in which they were sent, and a higher proportion of packets can be lost. Therefore, MPPE for VPN connections changes the encryption key for each packet. The decryption of each packet is independent of the previous packet. MPPE includes a sequence number in the MPPE header. If packets are lost or arrive out of order, the encryption keys are changed relative to the sequence 28 number. Although this level of encryption is satisfactory for many applications, it is generally regarded as less secure than some of the encryption algorithms.

There are two modes of encryption in MPPE:

· Stateful
· Stateless

Stateful encryption will provide the best performance but may be adversely affected by networks experiencing substantial packet loss. If you choose stateful encryption you should also configure flow control to minimize the detrimental effects of this lossiness. Because of the way that the RC4 tables are reinitialized during stateful synchronization, it is possible that two packets may be encrypted using the same key. For this reason, Stateful encryption may not be appropriate for lossy network environments (such as Layer 2 tunnels on the Internet) Stateless MPPE Encryption provides a lower level of performance, but will be more reliable in a lossy network environment.

4. Layer 2 Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) [2] is a combination of Microsoft's PPTP & Layer 2 Forwarding (L2F), a technology proposed by Cisco System's, Inc. L2TP supports any routed protocol such as, IP, IPX, and AppleTalk. It also supports any WAN technology including frame relay, ATM, X.25, and SONET. L2TP can be used as a

Tunneling protocol over the Internet or private Intranets. 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 (dial-up, ISDN 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) L2TP extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices Interconnected by a packet-switched network. With L2TP, a user has an L2 connection to an access-concentrator and the access-concentrator then tunnels individual PPP frames to the NAS. This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit. L2TP uses UDP messages over IP internetworks for both tunnel maintenance and tunneled data. L2TP therefore uses message sequencing to ensure the delivery of messages. L2TP supports multiple calls for each tunnel. To identify the tunnel and a call, there is a Tunnel ID and Call ID in the L2TP control message and the L2TP header for tunneled data.

Authentication that occurs during the creation of L2TP tunnels must use the same authentication mechanisms as PPP connections such as, EAP, CHAP, SPAP, and PAP.

4.1 How does it work?

L2TP tunnels are initiated inside the service provider network & terminated on the customer premise. The central components of an L2TP networks are the LAC (Link Access Concentrator) & the LNS (L2TP Network Server). The LAC performs the following functions:

· Termination of modem & ISDN calls.

· First-level authentication and tunneling via RADIUS.

· Some level of initial PPP setup, much of which is overridden at a later stage by the LNS.

· Execution of the L2TP protocol in terms of command & control messages & encapsulation of the remote user's PPP traffic in L2TP packets. The LNS can be thought of as that which resides "virtually" as a software function inside of another piece of networking equipment on the customer premises. It's responsible for executing key aspects of PPP, such as:

· Link Control Protocol (LCP).

· Network Control Protocol (NCP).

4.2 L2TP Protocol Characteristics

The characteristics of L2TP protocol are:

1.Multiplexing

L2TP has inherent support for the multiplexing of multiple calls from different users over a single link. Between the same two IP endpoints, there can be multiple L2TP tunnels, as identified by a tunnel-id, and multiple sessions within a tunnel, as identified by a session-id.

2. Signaling

This is supported via the in-built control connection protocol, allowing both tunnels and sessions to be established dynamically.

3. Data Security

By allowing for the transparent extension of PPP from the user, through the LAC to the LNS, L2TP allows for the use of whatever security mechanisms, with respect to both connection setup, and data transfer, may be used with normal PPP connections.

4. Multiprotocol Transport

L2TP transports PPP packets (and only PPP packets) and thus can be used to carry multiprotocol traffic since PPP itself is multiprotocol.

4.3 L2TP Security Considerations

L2TP suffers from the lack of solid tunnel protection mechanisms. Because L2TP encapsulates PPP, it inherits PPP's security mechanisms, including authentication and encryption services. PPP authenticates the client to the LNS but does not provide per-packet authentication. L2TP itself includes support for mutually authenticating the LAC and LNS tunnel endpoints at tunnel origination, but it too lacks stronger tunnel security mechanisms such as control and data packet protection. It doesn't provide key management facility, even though tunnel endpoint authentication relies on the distribution of tunnel passwords.

4.3.1 Tunnel Endpoint Security

The tunnel endpoints may optionally perform an authentication procedure of one another during tunnel establishment. This authentication has same security attributes as CHAP, and has reasonable protection against replay & snooping during the tunnel establishment process. This mechanism is not designed to provide authentication but just tunnel establishment only. So, it's quite easier for any intruder to snoop the tunnel stream to inject packets once an authenticated tunnel establishment has been completed successfully. For authentication to occur, the LAC and LNS must share a single secret. Since a single secret is used and to guard against replay attacks, the tunnel authentication AVPs must include differentiating values in the CHAP ID fields for each message digest calculation.

4.3.2 Packet Level Security

The underlying transport makes available encryption, integrity and authentication services for all L2TP traffic for security. This secure transport operates on the entire L2TP packet and is functionally independent of PPP and the protocol being carried by PPP. L2TP is concerned with confidentiality, authenticity, and integrity of the L2TP packets between its tunnel endpoints (the LAC and LNS).

4.3.3 End-to-End Security

Protecting the L2TP packet stream via a secure transport does, in turn, also protect the data within the tunneled PPP packets while transported from the LAC to the LNS.

So, summarizing the above said facts of L2TP as:

· Lacks tunnel protection mechanisms.
· Lacks tunnel security mechanisms.
· No key management facility but, authentication of tunnel endpoints relies on distribution of tunnel passwords

So, usually IPSec is used in conjunction with L2TP to protect L2TP traffic over IP and non-IP networks.

Comparative Study:

Table -1: Comparative study of Protocols

Characteristics	PPTP	L2TP
VPN Encryption	128 bit	256 bit
Vyper VPN Apps Supported	-Windows -Mac -Android	-Windows -Mac -Android -IOS
Manual setup Supported	-Windows -MacOs -Linux -IOS -Android -DD-WRT	-Windows -MacOs -Linux -IOS -Android
VPN Security	Basic Encryption	Highest Encryption. Checks data integrity and encapsulates the data twice.

VPN Speed	Fast due to low Encryption	Requires more CPU processing To encapsulate twice.
Stability	Works well on most wi-fi hot-spots, very stable. PPTP is fast & Easy to use.	Stable on NAT supported Devices.

5. CONCLUSION :

PPTP:

-PPTP protocol is east to use.

-It is good choice if OpenVPN isn't supported by your choice.

L2TP:

-Provides Higher Security as it provides DataEncryption and Decryption.

-If OpenVPN is not supported by your choice & security in top priority.

-L2TP is More Secure than PPTP protocol.

REFERENCES:

[1] Gleeson, B. et al, "A Framework for IP Based Virtua private Networks", RFC 2764, February 2000.

[2] Kent, S. and Atkinson, R., Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[3] Hamzeh, K. et al, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

[4] Townsley, W. et al, "Layer Two Tunneling Protocol - L2TP", RFC 2661, August 1999.

[5] Hussein S N and Hadi A (2013), The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network, International Journal of Scientific & Technology Research, Volume 2, Issue 11, ISSN 2277-8616, pp. 170-175.

[6]https://www.giganews.com/vyprvpn/compare-vpn-protocols.html

BIOGRAPHIES

Student of MCA Department at Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra, India.

Student of MCA Department at Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra, India.

Assistant Professor-MCA at Jawaharlal Nehru Engineering College Aurangabad, Maharashtra, India.