

Virtual Private Network (VPN)

Samuvel A

sbsam0624.a@gmail.com

Anna University, Chennai

Research Article

Keywords: WireGuard, ephemeral VPN, Zero Trust, X25519, ECDH, AES-256-GCM, dual-condition expiry, tunnel lifecycle management

Posted Date: October 6th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11084421/v2>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

1. Abstract

The world has become a small village because of the advancement in IT technologies and communications. Specially the rapid growth of the internet, which is becoming a medium for business transactions for many globally competitive organizations. E-commerce is the latest trend which require secure and cost effective connection to companies various resources like their ERP systems and applications. Virtual Private Networks (VPN) became very trendy and handy because they provide cost effective, and secure connection over a public medium, such as the internet. Which facilities remote access. Any organization or even normal user can benefit from it because it doesn't require leased dedicated circuits from a SP, which can be limited and expensive. VPN has many uses and types, but the scope of this paper focus manly on business uses not end user as they are most valuable to our specialization.

2. Keywords

Virtual Private Networks (VPN), Tunnel, Internet, Public Medium, Encryption, Decryption, (PPTP), (L2TP), (SSTP), Remote Access, Site-to-Site, Server, Privacy.

3. Introduction

Nowadays, the market place is very competitive and doing business without the help of IT is impossible. Companies are always in the hunt for latest technologies to help them obtain smooth processes and to create a competitive edge. One of the most useful technologies in that sense is virtual privates networks (VPNs). It enables various secure connections through public networks, mostly WANs, and creates "private" channels. IT departments including network administrators, and IS professionals can adapt this technology in their organizations and have knowledge of its implementations, protocols, and troubleshot.

(Gupta & Meeta, 2003) believe that there is an increasing demand for more cost efficient ways of transmitting data securely over the "insecure" public networks, such as the internet. Which made the VPN very popular today, because of the number of benefits they offer.

The main idea of VPN and why it become popular is that it uses the internet as a global medium which grants global accessibility. However, the internet is a shared medium and everyone is using it, so the data is highly vulnerable to various breaches. Those breaches includes unauthorized access,

eavesdropping, and damage, which could turn into a disadvantages to the organization instead of benefiting them. Nevertheless, the goal of VPN is to provide reliable, secure, and stated networks within the stated budget of implementation. The user can come over the disadvantages by implementing various security measures, in the end, he or she can balance if this technology is appropriate to their organization/use scope and if benefits exceed the drawbacks.

4. Definitions

Virtual: logical connection, not physical through cable, provided by software application.

Private: only the involved end users in the tunnel know or see what is travelling through it, they have the authority to use the tunnel.

Network: group of clients and servers and various peripherals connected and able to communicate together.

Remote User: a user who wants to access organization entrant from outside location.

Tunnel: dedicated path established between to ends through a many-users medium.

Eavesdropping: when unauthorized user, e.g. hacker, or third party use special techniques to listen to communication between two parties on a private channel.

5. Description of the technology:

a. Components

There is no common standard for building VPNs and many companies implement solutions that fit them best. Keeping in mind that the design depends on several factors such as the number of users, internet connection, and VPN type. However, based on the type of VPN (remote-access or site-to-site), you need to put in place certain components to build your VPN. According to cisco support community these are some of the basic components you will need to build a VPN:

1. Dedicated hardware such as a VPN Concentrator or a Secure PIX Firewall.
2. VPN-Enabled Router.
3. Each remote user requires desktop software client.
4. Dedicated VPN server for dial-up services.
5. Network Access Server (NAS) used by service provider for remote user VPN access.

6. Private network and policy management center.

b. How it works

VPN technology is based on the concept of what is called tunnels, tunnel means a path or channel. Those tunnels are created between two communication ends on the public network and enable them to exchange data in like the point to point connection. Those private tunnels are logical not physical, that's one of the reasons they are cost effective. After the tunnels are created, the data travelling through uses what is called encryption which is one of many other security measures VPN uses to make sure data is reached safely to its destination, as they are travelling through unsecure medium (the internet). (Gupta & Meeta, 2003)

To explain VPN methodology, let's say we want to link to branches with VPN, note that this is for site to site type of VPN. First, both need to have internet connection from ISP. Second, both LANs (each branch LAN) needs a VPN server. Third, the internet gateway or router should be VPN enable, meaning it supports VPN software. Forth, a firewall is needed to block any unwanted traffic. Then, the VPN software is installed on both VPN servers. Fifth, the software is configured and to establish connection between the two branches, both servers have to agree to communicate. Last, after the connection is established and working, several security measures are implemented, like encryption. Receiving end decrypt the data using special key. Then the process is repeated. (Feilner, 2006)

c. Technologies and protocols used

The main concept of VPN is tunneling, which is the private virtual path that is created between to ends on the public network. VPN can be based on three different protocols for encapsulating IP packets over a public network, such as the internet. They are Point to Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), and Secure Socket Tunneling Protocol (SSTP). They all mainly use features that was originally meant for Point to Point Protocol (PPP). PPP was created to communicate through dedicated circuits. It is responsible for encapsulating IP packets within PPP frames then transmitting them across the path. Those protocols are mainly used by windows server as they were defined by Microsoft Library.

1. PPTP

Through the public network, VPN server enables PPTP with two interfaces, one is on the internet and the other is on the intranet. It allows multiprotocol data to be encapsulated and encrypted in the IP header and sent through the internet. Encapsulation of PPP frames is transmitted in IP datagrams over the network. PPTP uses a TCP connection for tunnel management and Generic Routing Encapsulation (GRE) for encapsulating tunneled data. Encapsulated PPP frames can be encrypted, compressed, or both. PPTP uses includes remote access and site to site.

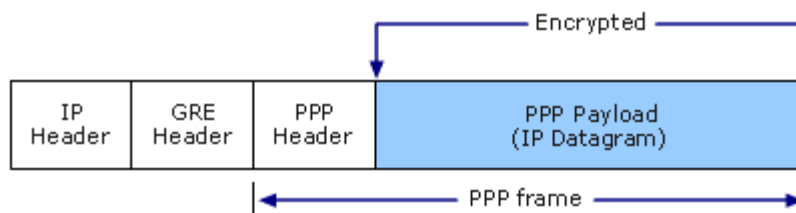


Figure 1: Structure of a PPTP Packet, Adapted from Microsoft Library.

2. L2TP

L2TP is installed with the TCP/IP protocol. L2TP must be supported by both the VPN client and the VPN server. L2TP relies on Internet Protocol security (IPsec) in Transport Mode for encryption services. The combination of L2TP and IPsec is known as L2TP/IPsec. Multiprotocol encrypted data can be sent over any medium which supports point to point datagram delivery, such as IP or asynchronous transfer mode (ATM). Encapsulation for L2TP/IPsec packets consists of two layers: L2TP and IPsec encapsulation. In the first layer L2TP header and a UDP header is added to the PPP frame. While in the second layer IPsec Encapsulating Security Payload (ESP) header and trailer is added to the pervious L2TP message, which provides message authentication and IP header. The IP header contains the source and destination IP address that corresponds to the VPN client and VPN server.

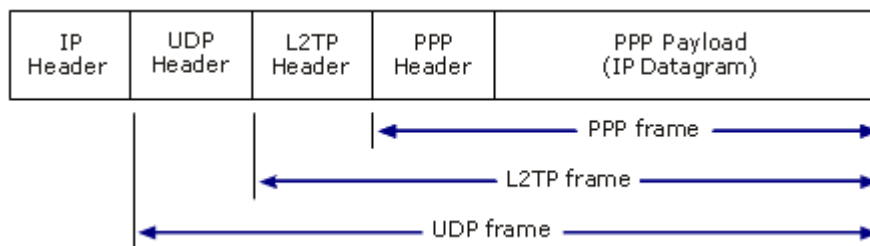


Figure 2 structure of an L2TP packet, Adapted from Microsoft Library.

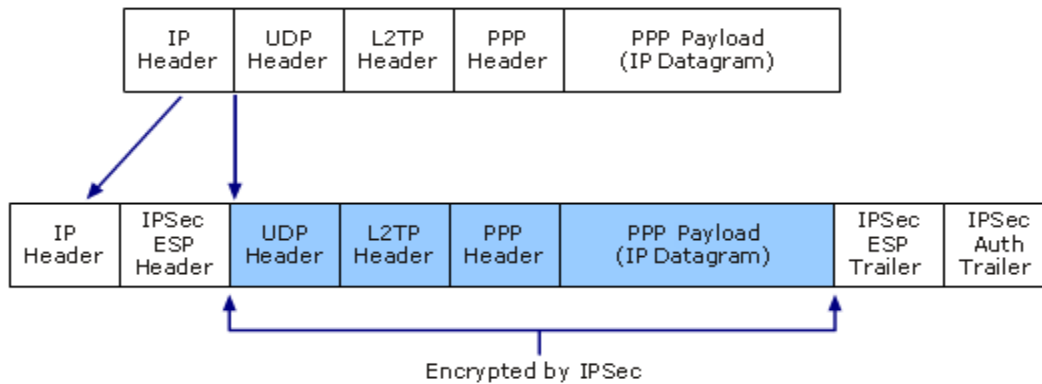


Figure 3: Encryption of L2TP Traffic with IPsec ESP, Adapted from Microsoft Library.

3. SSTP

Some firewalls and web proxies might block PPTP and L2TP/IPsec, so the Secure Socket Tunneling Protocol (SSTP) is a new tunneling protocol that uses the HTTPS protocol over TCP port 443 to pass traffic through those proxies and firewalls. PPP frames are encapsulated in IP datagrams by using TCP connection (over port 443) for tunnel management. The SSTP message is encrypted with the SSL channel of the HTTPS protocol.

PPTP, L2TP and SSTP all three tunnel types carry PPP frames and the common features of PPP, such as authentication schemes, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPV6) negotiation, and Network Access Protection (NAP), remain the same for the three tunnel types.

d. Applications of the technology

The most two common types of VPN are Site-to-Site and remote-access VPN. Each VPN is used for different applications based on user's needs and requirements. First, the remote access, it is usually called Dial-up Network. From the name remote access, this VPN is used when employees, for example, want to connect to the company network (LAN) from various external locations.

Second, site to site VPN, which is used in a case where a company wishes to connect distanced branches together. In this type larger scale devices and encryption are required. Site to site has two categories, intranet VPN and extranet VPN. Intranet VPN is in the scope of the same branch or building while extranet is linking to external agents like customer or supplier for example.

e. Security Measures

Many security measures are used with VPN technology to ensure the safety of the tunnel and reliability to send sensitive data across unsafe medium (public). Some of those safety mechanisms include the following:

1. Encryption

Encryption is used when the sender wants the data to be read only by the anticipated receiver. So the sender will encrypt it with special key to open it, and the receiver cannot decrypt it unless he or she has the correct key of decryption. According to Gupta & Meeta (2003) there are two main methods of encryption: traditional scheme and the public key scheme. The traditional scheme suggest that both sender and receiver use mutual key to encrypt and decrypt the data. While the public key scheme uses two keys, one called public key, the other is called private key. Any one on the network can use the public key, which could belong to any user, to encrypt data. However, each public key has a corresponding private key indicated to specific owner which is necessary to decrypt the send message, that is send to its destination. Example of public key encryption schemes are Data Encryption Standard (DES) and Pretty Good Privacy (PGP).

2. Authentication

Authentication is a procedure in which data is confirmed to be delivered to the intended receiver. Moreover, it checks the integrity of the message and its source. How it works is that it asks for username and password to gain access to the specified data. It can be also based on a secret-key encryption or on public-key encryption.

3. Authorization.

Which happens after user get access, after authentication, and it is responsible for giving or denying access to network's located resources.

7. Future developments

In any technology, there is endless aspects for improvements as no technology is perfect. One main point of VPN withdraws is that there is no agreed on standard for VPN, which can be set in the future. If VPN is not compatible with many devices, e.g. VPN enabled router, which maybe the organization is using, it can prevents them from using VPN. Thus, it won't be accessible for everyone. On the other hand, the main advantage of VPN is cost effectiveness because internet is a relatively cheap medium,

however, the performance of VPN is dependent on the performance of the internet which cannot be monitored. This issue arises as well as the security debates of internet as a medium. Other issue some users were complaining about is the big size of the message overhead that VPN requires which is resulting from the encryption, which slows the VPN. Last, some countries blocks IP address which given from certain VPN providers which limit the use of it, this problem arises because of the different regulations for using the internet. Many organizations stood up for similar issues and calling for transparency regarding internet services. All those gaps allow for improvement and developments in the future. Maybe VPN will evolve into new technology based on similar concept but with standard and improved performance in the future.

7. Conclusion

After understanding how VPNs work, their technology, and the different component associated with them, we realize that each technology has limitations because of some factors. Those factors could be time to implement the technology in the organization, the budget and cost and the number of employees/users. So with these considerations the user make his decision of which technology he will use, VPN could be on optimal solution for some but hinder the business process for others. It is not only used for entertainment purposes as the common conception, it can be a powerful tool to use to enhance our privacy when transmitting data on the internet.

8. References

Gupta, M., & NIIT, (. (Corporation). (2003). *Building a Virtual Private Network*. Cincinnati, Ohio: Premier Press.

Feilner, M. (2006). *Open VPN: Building and Operating Virtual Private Networks*. Birmingham, [U.K.]: Packt.

How Virtual Private Networks Work. (2008, October 13). Retrieved May 11, 2015, from <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>

Virtual Private Networking. (n.d.). Retrieved May 11, 2015, from [https://technet.microsoft.com/en-us/library/cc772120\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772120(v=ws.10).aspx)

Bridgwater, A. (2013, August 1). VPNs: The past, present and future. Retrieved May 12, 2015, from <http://www.computerweekly.com/feature/VPNs-The-past-present-and-future>