Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

A Survey on Categories and Efficient Protocols for Virtual Private Networks

Sapna Devi B
Assistant Professer, Department of Computer Science, Gonzaga College of Arts and Science for Women, kathampallam,krishnagiri,Tamilnadu, India

Abstract - Businesses have come to depend and act upon real time information. While the openness and availability of the internet has facilitated explosive growth, the need for privacy has been a constant problem. Businesses that have computers in more than one physical location are faced with the problem of how to communicate privately with their various offices across long distances. To overcome on this aspects a VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses. In this article we have analyzed the needs of VPN, protocol usages in different aspects, and how to connect the network through WAN.

Keywords: Virutal Private Network, protocol, Tunnel, IPsec WAN, Private Network.

INTRODUCTION

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost. A virtual private network (VPN)is a private network that uses a public network (the Internet) to connect users. Secure VPNs use cryptographic tunneling protocols to provide confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing, and provide message integrity by preventing message alteration. The traditional Layer 2 WAN (Wide Area Network) has developed more than 20 years, based on private connections between two or more locations. However, with the development of technology, companies evolve faster and the traditional ways seem less suitable for modern companies, due to the costs of leasing lines from Telecom Service Provider. In the mean time, people have an easier access to the Internet even in rural area, and the costs of access becomes cheaper and cheaper. The development of wide band technology makes the speed faster and faster. For this reason companies more likely to choose a new technology called VPN (Virtual Private Network) to implement WAN access. As we see from the name “Virtual Private”, this technology uses public Internet service and acts as a private way such as frame relay and ATM by using end-to-end tunnel technology. Organizations use VPNs to provide a virtual WAN infrastructure that connects branch offices, home offices, business partner sites, and remote telecommuters to all or portions of their corporate network.

WAN LINK CONNECTION

WAN connections can be either over a private infrastructure or a public infrastructure. Private WAN connections include both dedicated and switched communication link options. A public WAN connection option, such as the internet is now a sophisticated technology widely used in our daily communication. The differences between them are technology speed and cost.

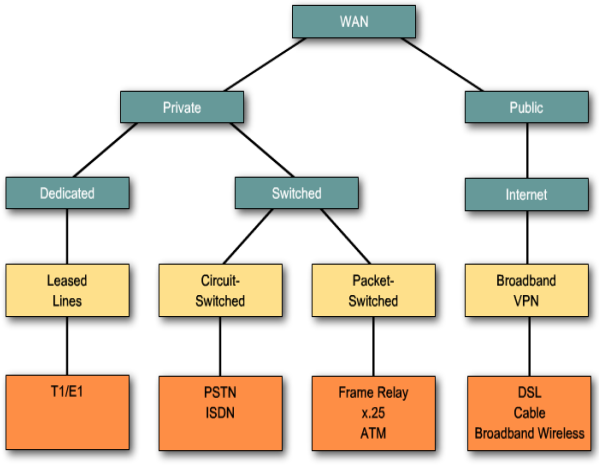

Fig 1. different ways of WAN link connection.

In ***Leased lines*** services (or private line services) became digital with the conversion of the Bell backbone network from analog to digital circuit. Leased line needs a permanent dedicated connection, which for sure costs plenty of money. Therefore it is not very suitable for a long distance connection due to the cost and time of pre-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

established line before successful transportation. Besides, the bandwidth of the leased line is fixed whereas the traffic is variable, sometimes even empty.The dedicated capacity removes latency or jitter between the endpoints. Constant availability is essential for some applications such as VoIP or Video over IP.

In ***Circuit switching*** is a telecommunications technology by which two network nodes establish a dedicated communications channel (circuit) connecting them for the duration of the communication session before the nodes may communicate. There are two main technologies using circuit switched technology, Analog Dialup and ISDN (Integrated Services Digital Network). Analog Dialup works just like a normal telephone using PSTN (Public Switched Telephone Network). The line is engaged when transmitting data. Compared to leased line, it has a lower price. On the contrary, user should be subject to the lower speed. In order to address the problem, ISDN is invented to enables the line from home to local telecom operator to carry digital signals. But in today's network, circuit switched connection has been substituted by new faster and cheaper technology.

In ***Packet switched*** there is no need to establish a circuit before communication. Instead, packet switching splits data into packets and allows many pairs of nodes to communicate over the same channel. In order to determine which direction the packet must be sent on next, there are two approaches, connectionless and connection-oriented. Connection-oriented connection relies on DLCIs (Data Link Control Identifiers) working like a VC (Virtual Circuit) used in Frame Relay networks, a widely used packet switched connection nowadays developed from. X.25.Internet Connection Now, there are mainly three different ways accessing to the internet, DSL (Digital Subscriber Loop), using telephone networks, cable modem, using cable television networks and wireless such as municipal Wi-Fi, WiMAX and Satellite.

Broad Band Nowadays, internet has become to part of our life. On work time, office workers use it to send e-mail and even use online office software to deal with their daily work.If the access speed is high enough, an operating system only with web browser is enough to solve the most of our daily application. This is actually the reason why Google developed an operating system called Chrome OS. The main advantage of Chrome OS compared to other operating systems is that Chrome has a very short user interface launching time. Below, I present the main broadband access methods, DSL, cable and broadband wireless

Types of vpn

Remote access VPN

Remote access VPNs enables mobile users to establish a connection to an organization server by using the infrastructure provided by an ISP (Internet Services Provider). Remote access VPN allows users to connect to their corporate intranets or extranets wherever or whenever is needed. Users have access to all the resources on the organization's network as if they are physically located in organization. The user connects to a local ISP that supports VPN using plain old telephone services (POTS), integrated services digital network (ISDN), digital subscriber line (DSL), etc. The VPN device at the ISP accepts the user's login, then establishes the tunnel to the VPN device at the organization's office and finally begins forwarding packets over the Internet. Creating remote access VPN between companies and SOHOs (small office home office) can save commuting time especially in metropolis. The VPN tunnel configuration is always configured on an enterprise level Firewall while in personal level the computer itself can act as a VPN tunnel end using software called VPN client to access to the main building. Usually the VPN can be classifying as a remote access and site-to- site.

Site-to-site VPN

The organizations always create a site-to-site VPN between headquarter and branch companies (Called Intranet) as well as their business partners (Called Extranet). A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

There are two types of site-to-site VPNs:

- **Intranet-based** -- If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.
- **Extranet-based** -- When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate internet.

Even though the purpose of a site-to-site VPN is different from that of a remote-access VPN, it could use some of the same software and equipment. Ideally, though, a site-to-site VPN should eliminate the need for each computer to run VPN client software as if it were on a remote-access VPN.

Vpn categories and vpn protocol

According to the tunnels termination point, VPN can be classified into End-to-End, End-to-LAN, End-to-POP, LAN-to-LAN, LAN-to-POP and POP-to-POP. In the End-to-End tunnel model, the tunnel is from one terminal side to the other side, so it has the highest security. The information

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

transformed from one side to the other side is encrypted and cannot be detected and ruined by others. In the End-to-LAN model, the tunnel starts from one computer to the gateway of the other LAN. This technology also called remote access. In the LAN-to-LAN model, well known as site-to-site VPN, the tunnel is created between two remote gateways, providing encrypted information transmitting. This technology is always used to create the private connection between headquarter and branch offices. While in the End-to-POP model, starting from one end computer to the other side of telecom operator, does not have great implementation. Also the same situation exists in the POP-to-POP and the LAN-to-POP.

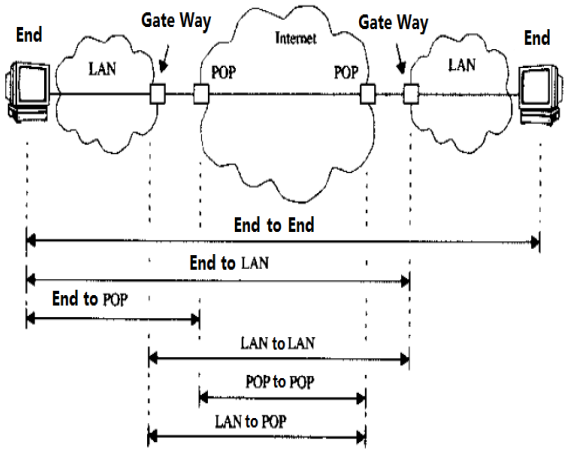

Fig 2. Category according to tunnel's termination point

Vpn protocols

Protocols can be classified with the tunnel by tunnel protocol. There are some Data Link Layer protocols to provide a tunnel connection, such as Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). Besides, there are some Layer 3 tunneling protocol Generic Routing Encapsulation (GRE) and IPsec protocol suite. There is a tunnel working between Layer2 and Layer3, called Multiprotocol Label Switching (MPLS).

L2F, or Layer 2 Forwarding, is a tunneling protocol developed by Cisco Systems, Inc. to establish virtual private network connections over the Internet. L2F does not provide encryption or confidentiality by itself; It relies on the protocol being tunneled to provide privacy. L2F was specifically designed to tunnel Point-to-Point Protocol (PPP) traffic.

L2TP (Layer 2 Tunneling Protocol is an extension of the PPTP (Point to point tunneling protocol), used by internet service providers to provide VPN services over the internet. L2TP combines the functionality of PPTP and L2F (Layer 2 forwarding protocol) with some additional functions using some of the IPsec functionality. Also L2TP can be used in conjunction with IPsec to provide encryption, authentication and integrity. IPsec is the way forward and is considered better than the layer 2 VPN's such as PPTP and L2TP.

The Point-to-Point Tunneling Protocol (PPTP)is a protocol or technology that supports the use of VPN's. Using PPTP, remote users can access their corporate networks securely using the Microsoft Windows Platforms and other PPP (Point to Point tunneling Protocols) enabled systems. This is achieved with remote users dialing into their local internet security providers to connect securely to their networks via the internet

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. It cannot provide security, and always working together with IPsec to perform secure transmission.

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. In the following chapter, I will briefly explain the working mechanism of IPsec.

MPLS (Multiprotocol Label Switching) operates at an OSI Model layer that is generally considered to lie between traditional definitions of Layer 2 (Data Link Layer) and Layer 3 (Network Layer), and thus is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model.

SSL VPN (Secure Socket Layer Vpn) provides excellent security for remote access users as well as ease of use. SSL is already heavily used such as when you shop online, accessing your bank account online, you will notice an SSL protected page when you see the "https" in your browser URL bar as opposed to "http". The difference in using SSL VPN to IPSec is with IPSec a remote user would require client software which would need installing, configuring and sometimes troubleshooting. However with SSL there is no client software if a user was using the SSL portal.

Ipsec protocol

IPsec framework

The IPsec protocol that makes it possible to transport information safely through public internet. It provides data confidentiality, data integrity, and origin authentication. IPsec suite works at the Network Layer, protecting and authenticating IP packets between participating IPsec devices (peers). As a result, IPsec can protect virtually all application traffic because the protection can be implemented from Layer 4 through Layer 7 or even the original Layer 3 information. There are some tricky when protecting Layer 3 because all packets should have a plaintext Layer 3 header, so there are no issues with routing. IPsec provides the framework, and the network administrator just need to choose the algorithms to implement the security services and be sure the same

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

algorithms are used between two sides. By not binding IPsec to specific algorithms, it allows newer and better algorithms to be implemented in the IPsec frame. IPsec can secure a path between a pair of gateways (site-to-site), a pair of hosts, or a gateway and host (remote access).

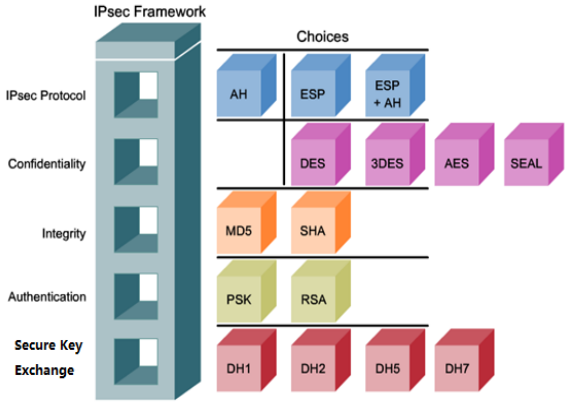

Fig.3 IPSEC Framework

Encryption Algorithms for IPsec

DES (Data Encryption Standard) - DES is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key.

3DES (Triple DES) - A variant of the 56-bit DES, because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks. Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm.

AES (Advanced Encryption Standard) - The AES is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor DES.

SEAL (Software Encryption Algorithm) - The Software optimized Encryption Algorithm (SEAL) is an alternative algorithm to software-based DES, 3DES, and AES. It is a stream cipher that uses a 160-bit encryption key.

INTEGRITY

Routers use hash method to provide integrity and get a series of hexadecimal number attached to the packet before sending out. The length of hash value depends on which algorithm has been chosen and this digest is used to authenticate when receiver gets packet. The hash function hashes arbitrary data into a fixed-length digest known as the hash value, message digest, digest, or fingerprint. There are two common HMAC (Hashed Message Authentication Codes) algorithms:

HMAC-Message Digest 5 (HMAC-MD5) - Uses a 128-bit shared-secret key. The variable- length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash.

HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) - Uses a 160-bit secret key. Working the same way as MD5 and the output is a 160-bit hash. The algorithm is slightly slower than MD5. Put the arbitrary length text into hash function and get a series of hexadecimal hash value.

AUTHENTICATION

Authentication always works together with a hash method. Put the secret key and variable text into the hash function and get a fixed hash value. This part is to specify what kinds of keys are used. Pre-shared Keys (PSKs): This is a one-way authentication method. Two peers should specify the key manually. RSA signatures: The exchange of digital certificates authenticates the peers. Each peer must authenticate its opposite peer before the tunnel is considered secure. Unlike PSK, it is a two- way authentication procedure. Local device hash its private key and message and get the hash value. The remote peer should authenticate the received message by recalculating the hash value using the received public key from the original peer. RSA-encrypted nonces: A nonce is a random number that is generated by the peer. RSA- encrypted nonces use RSA to encrypt the nonce value and other values. This method is the least used of the authentication methods. The DH algorithm is the basis of most modern automatic key exchange methods and is one of the most common protocols used in networking today. Diffie-Hellman is not an encryption mechanism and is not typically used to encrypt data. Instead, it is a method to securely exchange the keys that encrypt data. Encryption algorithms such as DES, 3DES, and AES as well as the MD5 and SHA-1 hashing algorithms require a symmetric, shared public secret key. DH provides a secure key exchange method. There are four DH groups: 1, 2, 5, and 7. Cisco devices supports group 1 (768-bit key), 2 (1024-bit key) and 5 (1536-bit key). DES and 3DES support groups 1 and 2. AES supports groups 2 and 5.

CONCLUSION

Virtual Private Network provides a means of accessing a secure, private, internal network over insecure public networks such as the Internet. A number of VPN technologies have been outlined, among which IPsec and SSL VPN, L2TP, PPTP are the most common. Although a secure communication channel can be opened and tunneled through an insecure network via VPN. In this survey we have analyzed the concepts of VPN protocols and the major support on IPsec encryption algorithm to secure the data to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

get transfer from source to destination with VPN support. In further study the comparison of secure in public and private network will be done.

ACKNOWLEDGEMENTS

The present work is benefited from the input of my research guide Mrs. M.Savitha Devi, Assistant Professor in PG and Research Department of Computer Science, Don Bosco College, Dharmapuri. I would like to thank her, for her valuable assistance to the undertaking of the study report summarized here. And also I would like to thank my management Don Bosco College, Dharmapuri, for giving me this opportunity to present the article.

REFERENCES

[1] Wikipedia 2011,Virtual Private Network. Updated 28.3.2011. Referred 2.4.2011.
[2] C.M. King, “Remote Access VPNs : Selection and Deployment Issues”, 2000.
[3] J.S.Tiller, “Security of Virtual Private Networks. Information Systems Security”, 2001
[4] Shah Deval and Helen Holzbaur, “Virtual Private Networks: Security With an Uncommon Touch,” Data Communications
[5] R.Malhotra , R.Narula, "Techno-Evaluation and Empirical Study of Virtual Private Networks Using Simulations," Journal of Computing, Volume 3, Issue 7, July 2011.
[6] VPN Technologies: Definitions and Requirements, Paper, VPN Consortium.
[7] V. Manral, “Cryptographic Algorithm Implementation Requirements for (ESP) and (AH)” RFC 4835.
[8] S. Kent, “IP Authentication Header”, RFC4302.
[9] Black, Ulysses. “PPP and L2TP: Remote Access Communications”, Pren-tice Hall: New York, 1999.
[10] T. Rowan, “VPN Technology: IPSEC vs SSL,” Network Security”, Vol. 2007, No. 12, December 2007, pp. 13-17. doi: 10.1016/S1353-4858(07)70104-6 .
[11] Wikipedia 2011, “Point-to-Point Tunneling Protocol. URL http://en.wikipedia.org/wiki/Point-to-Point_Tunneling”.
[12] Wikipedia 2011. IPsec. Updated 10.4.2011. Referred 12.4.2011. URL http://en.wikipedia.org/wiki/IPsec.

AUTHOR BIBLOGRAPHY

1. .**B.SapnaDevi** has completed M.Sc(IT).,B.Ed M.Phil,.,She is working as Assistant Professor in Gonzaga College krishnagiri,.