Benjamin Huang

August 18, 2023

A Comparative Analysis of IPsec and TLS Network Protocols for Implementing VPNs: Performance and Security Considerations

Abstract

With the increasing number of people and the increasing number of devices accessing the global internet, network security has become a critical concern for individuals, companies, and governments. This research paper will go over two types of protocols that are used to enhance network security: IPsec and TLS. Both protocols are used to provide confidentiality and integrity when communicating through networks by encrypting the contents of the messages. TLS is used in the transport layer while IPsec operates at the network layer. This research paper examines the implementation of Virtual Private Networks (VPNs) using IPsec and TLS network protocols. This paper will go into a deep dive of the workings of both protocols, underlying mechanisms, security features, performance characteristics, the advantages, and the disadvantages. It aims to provide an in-depth analysis of the two protocols to help businesses and organizations make informed decisions when choosing the appropriate protocol for their VPN needs.

Introduction

In today's increasingly interconnected world, the need for secure communication and data exchange over public networks has become paramount for individuals, businesses, and organizations. Many organizations have implemented Virtual Private Networks (VPNs) as a solution to address this demand by creating an encrypted tunnel through which data can be transmitted securely. While there are numerous VPN protocols available, this research paper focuses on the two widely used and prominent protocols, IPsec and TLS, exploring their implementation in VPNs and evaluating their differences in performance.

The Internet Protocol Security (IPsec) and Transport Layer Security (TLS) protocols both play pivotal roles in securing data transmissions, but they differ in their approach and implementation. IPsec is implemented at the network layer, providing security for the entire IP packet, while TLS operates at the transport layer, ensuring secure communication at the application layer. Understanding the unique features, strengths, and limitations of each protocol is essential for making informed decisions when implementing VPNs to safeguard sensitive information.

By undergoing this in-depth analysis, we aim to contribute valuable insights that will enable organization’s stakeholders to make well-informed decisions in implementing VPNs securely and efficiently, safeguarding their critical data and communication channels in an ever-evolving digital landscape.

Overview of VPNs

2.1 Definition and Purpose of VPNs

VPN stands for Virtual Private Network and Geof Huston in his "What is VPN?"[1] article breaks the acronym down into well understood segments. "Network" is a collection of devices that can communicate with each other. "Private" means the communication is hidden from the public. "Virtual" is a simulation of the function which in this case is the "private network." VPNs utilize virtualization to build a private connection between two different systems/organizations. The strict definition of VPN from the article is "a communications environment in which access is controlled to permit peer connections only within a defined community of interest and is constructed though 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." [1] In simpler terms, VPN can be defined as a private network built within a public network.

Setting up the infrastructure for a public network is already a very costly expenditure. If an organization wanted to set up their own internet infrastructure, they would have to run the same physical connections as the public network. Therefore, aggregating both physical networks is more cost-effective which was one of the motives of creating VPNs. Another main reason is the privacy aspect of VPNs. Sending data communications over the public network allows any prying eyes to view that data easily.

In the 1960s the United States Department of Defense created the first network system called Advanced Research Projects Agency Network (ARPANET) which also led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP). TCP/IP is not an encrypted communication protocol and was quickly adopted commercially. The first generation of VPNs came when different organizations were researching IP-layer encryptions in the 1990s. The US Navy developed the Simple Internet Protocol Plus (SIPP).[2] In 1993, Columbia University and AT&T Bell labs created the Software IP Encryption Protocol (SwIPe) which was the first VPN. The first commercial IPSec VPN protocol was created by Xu Wei for the Trusted Information Systems (TIS) and is still used today. Organizations continued to create diverse types of VPNs for unique needs or to improve the VPN capabilities.

2.2 Types of VPNs

To understand the distinct types of VPNs, there needs to be an understanding of the TCP/IP model. The TCP/IP protocol consist of multiple layers as shown in Figure. 1. IP communications consist of four layers: application, transport, and network. There are security controls at each layer and as data is prepared for transport, it is passed from the highest to the lowest layer, with each layer adding more information. Security controls at higher layers cannot provide full protection for lower layers because the lower layers add information to the communications after the higher layer security controls have been applied. IPsec will be discussed more later in the paper; it is a network layer protocol. TLS will also be discussed later in the paper; it is a transport layer protocol.

---

[1] Ferguson, Paul, and Geoff Huston. "What is a VPN?" (1998): 01-22. https://libguides.murdoch.edu.au/footnote/text

[2] Alexiei Zahorski, "How VPNs Have Shaped the Internet over the Years," MUO, June 15, 2022, https://www.makeuseof.com/how-vpns-shaped-internet/.

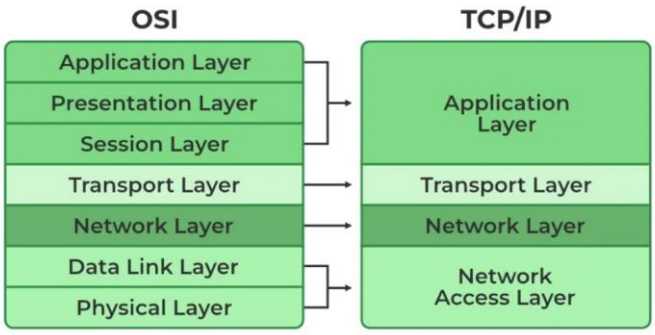

Figure. 1TCP/IP and OSI [3]

The application layer sends and receives data for applications including Domain Name System (DNS), Hypertext Transfer Protocol (HTTP)/ HTTP secure (HTTPS), Simple Mail Transfer Protocol (SMTP), and Internet Message Access Protocol (IMAP).

The transport layer is for connecting the application layer through the network. TCP is for ensuring reliable communication because it ensures a successful delivery of data using a three-way handshake. UDP does not require a three-way handshake and just sends data without ensuring delivery. This makes UDP communication less dependable. IP information is handled at the network layer and the transport layer is above that, meaning the transport layer control cannot protect IP information. Transport Layer Security (TLS) is used to protect TCP and UDP data.

The network layer is what routes packets through the network. The Internet Control Message Protocol (ICMP), using the IP protocol, can perform packet routing. Internet Group Management Protocol (IGMP) can also be used. The network layer is more standardized than the application layer, this means there is also less flexibility for protecting specific applications. IPsec is used at this layer to protect IP information.

The network access layer or data link layer handles the physical connection throughout a network. Ethernet and Wi-Fi (802.11) protocols are the most common.

2.2.1 Types of VPN Models

There are two main models of VPNs, the peer and overlay VPN. A peer VPN model allows users to send and receive data across the network through several nodes using “hopping” rather than a single place because every node acts as a potential point of connection. The ISP participates in the customer routing meaning the customer routes are carried within the core network of the ISP. The ISP edge routers exchange routing information with the customer edge routers, and layer three routing is established between the edge routers. The advantages of peer VPN model are that it allows optimal routing, adding new sites is easier, and there is no circuit capacity sizing issue. Figure 2 shows the implementation of this VPN model. Customer routing information is exchanged between Paris ISP edge router and the customer edge router, and the routes are then broadcasted through the core network to London ISP edge router and Zurich ISP edge router.[4]

[3] “TCP/IP Model,” GeeksforGeeks, July 21, 2023, https://www.geeksforgeeks.org/tcp-ip-model/.
[4] “The VPN Overview.” July 22, 2023, https://media.techtarget.com/searchNetworking/downloads/Buildvpn1.pdf

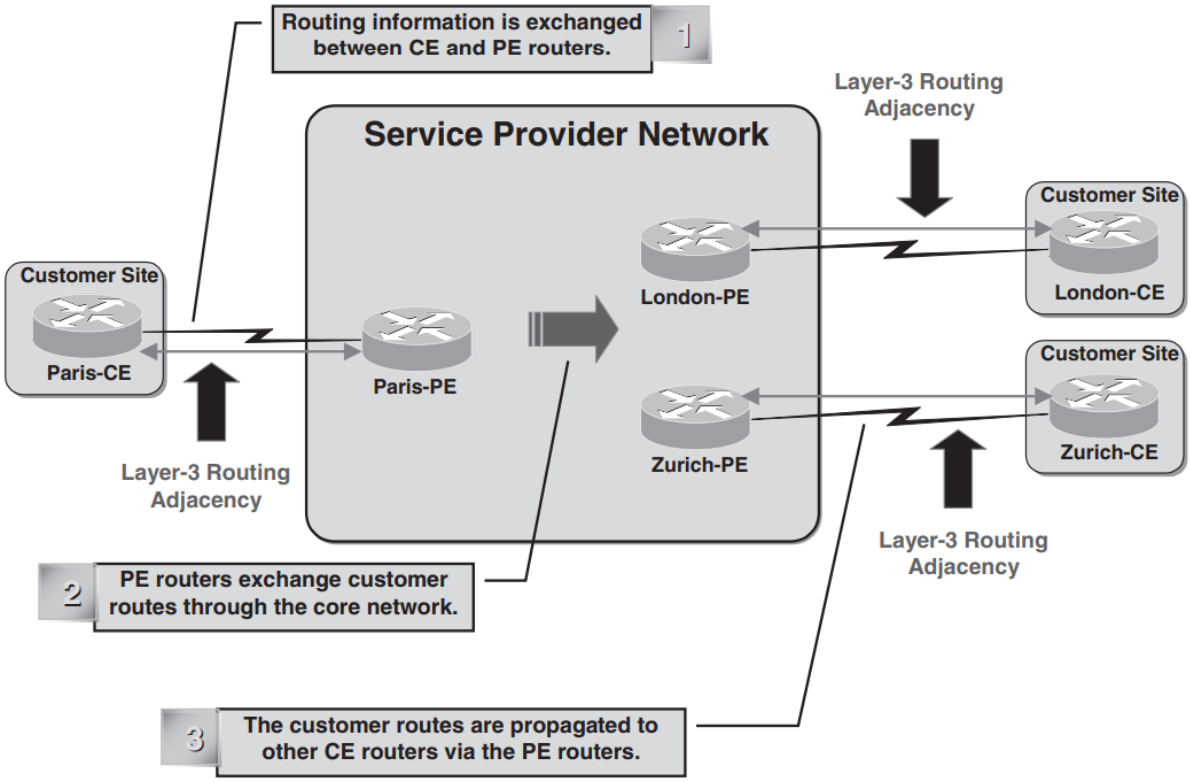

Figure 2 Peer-to-peer VPN model [4]

The overlay VPN model does not allow hopping, it uses an intermediary network to connect users, which means there is no routing peering between end nodes. The ISP provides virtual point-to-point links between customer sites. The overlay VPN is deployed via private trunks across a service provider's shared infrastructure at layer 1(dial up), layer 2(using X.25/frame relay/ATM, or layer 3(using IP and GRE). Routing within the customer network is transparent to the service provider network, and routing protocols run directly between customer routers, but the ISP does not know the customer routes. One of the disadvantages of overlay is the difficulty in sizing the inter-site circuit capacities. And the second disadvantage is the need for fully meshed deployment of point-to-point links or virtual circuits at the layer two level over the ISP's backbone. Figure 3 Overlay VPN Model [4]Figure 3 shows the routing of an overlay VPN set up. The ISP only see the connections between London to Paris and Paris to Zurich.[4]

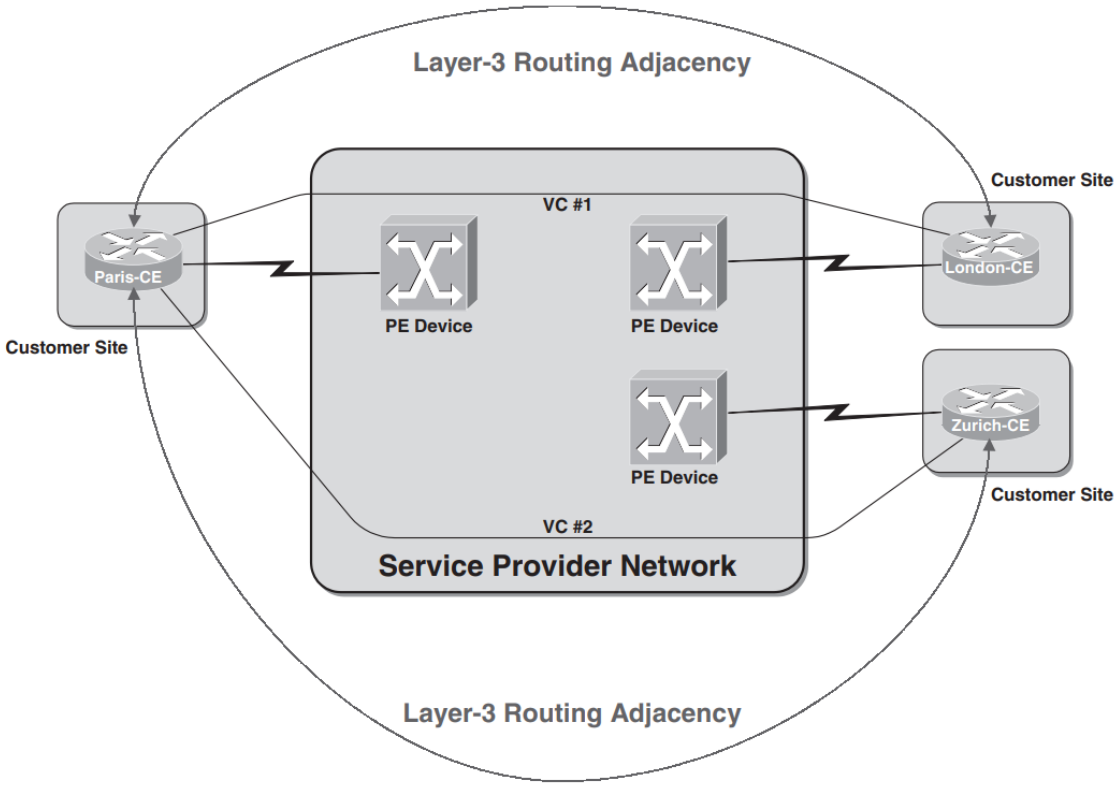

Figure 3 Overlay VPN Model [4]

2.2.2 Types of Tunneling

Tunneling is used to construct a VPN by having each point of connection to the public network configured as a physical link which uses addressing and routing from the host network. Each tunnel endpoint logically links to the point of connection to the public network to other remote points with the same VPN. Tunnel egress address is used to define the address space within the host network, while the packets carried within the tunnel use the address space of the VPN. Tunneling is what isolates the VPN routing from the routing of the public network. VPNs can reuse the same private address space within multiple VPNs without any impact to each other. Tunneling can encapsulate different protocol families, allowing it to be more flexible and allow it to mimic a private network. 1

Examples of tunneling VPN protocols are Generic Routing Encapsulation (GRE), Layer 2 Tunneling protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Distance Vector multicast Routing Protocol (DVMRP). Tunneling can be point-to-point or point-to-multipoint. Point-to-point tunnels scale better than point-to-multipoint tunnels. Except where a single node builds multiple point-to-point tunnels with multiple endpoints.[1] Tunneling encapsulates packets by wrapping packets within packets, where packets are small units of data. Packets are made up of a header, storing the destination and protocol information, and the payload, the contents of the data. An encapsulates packet is a packet that is contained in the payload of another packet. Encapsulation allows the actual data packet to be encrypted and then stored inside the outer packet. If the data was all encrypted that means the header will also be encrypted and the data will not be able to enumerate its destination.

GRE tunneling encapsulates data packets that use one routing protocol inside the packets of another protocol. GRE is a point-to-point tunnel across a network and is defined in RFC 2784, meaning any vendor can support it. GRE works by adding two headers to each packet. One of the headers is the GRE header that indicates the protocol type used by the encapsulated packet. The IP header encapsulates the original packet's IP header and payload. The routers at the ends of the tunnel will use the IP header. GRE does not have built-in encryption, making it lightweight and configurable. One way to add encryption is to add a layer of IPsec. In a GRE VPN, the end routers are configured with a Virtual Tunnel Interface (VTI). The VTI configures each router with the destination IP of the router at the other end. There may be multiple connected routers in between the end routers which make up the underlay network. All the underlay routers do is pass data so that data reaches its correct destination. When data from the end router sends data to the other end router, the data is encapsulated with the GRE and IP header. Encapsulation uses encryption to hide the data from the underlay router and stops unauthorized users from reading the data being communicated between the GRE tunnel. [5]

Original Packet:

IP Header	Payload

GRE Encapsulated Packet:

Outer IP Header	GRE Header	Inner IP Header	Payload

L2TP tunneling like GRE is a Layer 2 point-to-point VPN and does not provide encryption by itself but can be encrypted by passing over a Layer 3 encryption protocol such as IPsec. L2TP is defined using RFC 2661 and is built using Microsoft's PPTP and Cisco's LTF and is implemented with the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). The LAC and LNS serve as endpoints for the tunnel. The LAC receives data from remote devices and routes it securely to the LNS and then the LAC negotiates a PPP connection to transmit encapsulated data to the LNS. The LAC can be a server hosted by the organization itself or by an Internet Service Provider (ISP). [6]

L2TP Encapsulated Packet:

L2TP Header	PPP header	PPP Payload

PPTP is one of the older VPN protocols and originally designed to tunnel dial-up connections. PPTP is now obsolete and recommended not to be used. PPTP uses Microsoft Remote Access Service (RAS) for Windows NT operating system. RAS allows a Windows NT server with a modem to be set up as a dial-in point for remote users. The server authenticates users and then sets up a session with the PPP protocol. Users can connect to the VPN in two ways, the first way is the user to dial into an ISP with a PPTP-enabled remote access switch that can connect to the RAS server; the second way is the user connects to an ISP with no PPTP offering and must initiate the PPTP connection on their client machine.[7]

PPTP Encapsulated packet:

PPTP Header	IP header	GREv2 Header	Payload

2.2.3 Types of VPN Architectures

There are four primary VPN architectures: Gateway-to-gateway, remote access, host-to-host, and mesh.

Gateway-to-gateway protects communication between two specific networks, such as an organization's primary office network and a branch office network. Either of the VPN gateways can initiate a request to the other to establish VPN connection. Only one single connection can be used to tunnel devices from

[5] "GRE Tunnel," Network Direction, accessed August 1, 2023, https://networkdirection.net/articles/routingandswitching/gretunnels/.
[6] "Layer Two Tunneling Protocol (L2TP)", NordLayer, accessed August 1, 2023, https://nordlayer.com/learn/vpn/l2tp/
[7] "How PPTP Works", O'Reilly, accessed August 1, 2023, https://www.oreilly.com/library/view/virtual-private-networks/1565925297/ch04s02.html

one side to devices on the other side. It is important to note the VPN tunnel is only between the two gateways. There is no tunneling between the individual devices and the gateway. This can be seen in Figure 4, the solid lines represent the VPN connection, and the dotted lines are the connection unprotected by the VPN. The devices do not need any VPN software to connect to the VPN, it is all done by the gateways. [8]

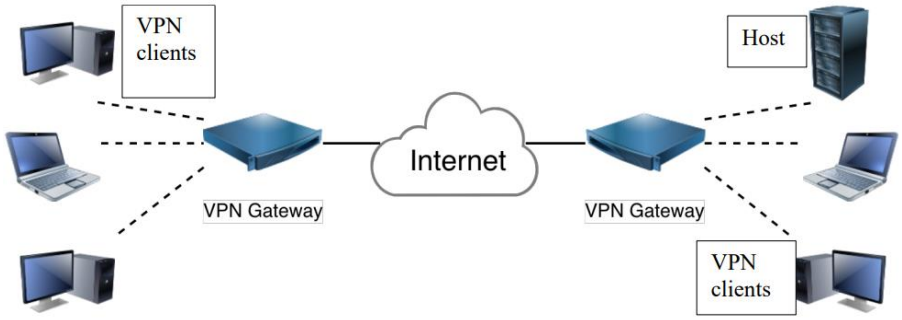

Figure 4 Gateway-to-gateway VPN [8]

Remote access or host-to-gateway is for one or more individual hosts and a network belonging to an organization. Remote access is usually used to allow users on unsecured networks like public Wi-Fi, to gain access to internal organization's network. The organization sets up a VPN gateway in their internal network and the user connects to the VPN gateway through the internet to access the internal network. The VPN tunnel connection is only between the user and the VPN gateway. This can be seen in Figure 5, the solid lines represent the VPN connection, and the dotted lines are the connection unprotected by the VPN. Remote access VPNs can be split-tunneled which means if the user is browsing the internet, that traffic is separate from when the user is accessing internal company data. Remote access VPN is not transparent to the user, the user needs a client to connect to it. [8]

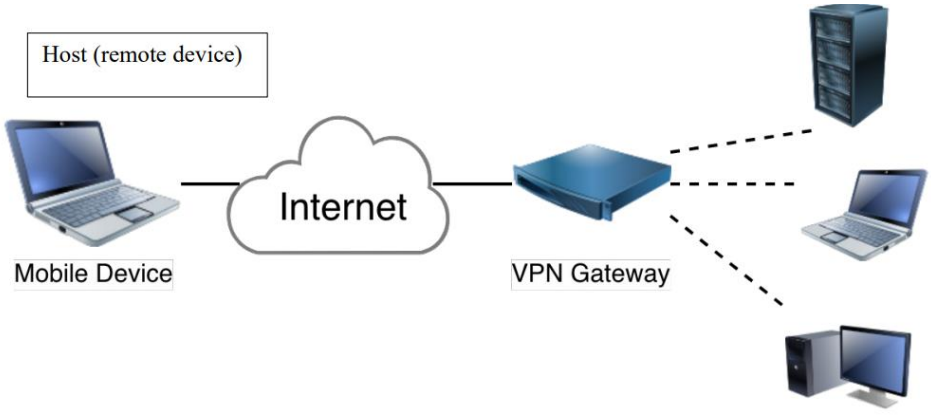

Figure 5 Remote Access VPN [8]

Host-to-host is for two specific computers, usually for a small number of users to connect. In the two previous VPN architecture, there were some gaps in the connection that were not protected by the VPN. This implementation solves that and protects the entire connection. This is seen in Figure 6, represented

by the solid line from the host on the left to the host on the bottom right. When the user on the left wants to connect to the host on the bottom right, the user on the left initiates a VPN connection. The host on the bottom right then authenticates the user and then establishes the connection. Now the entire connection is protected by the VPN. [8]

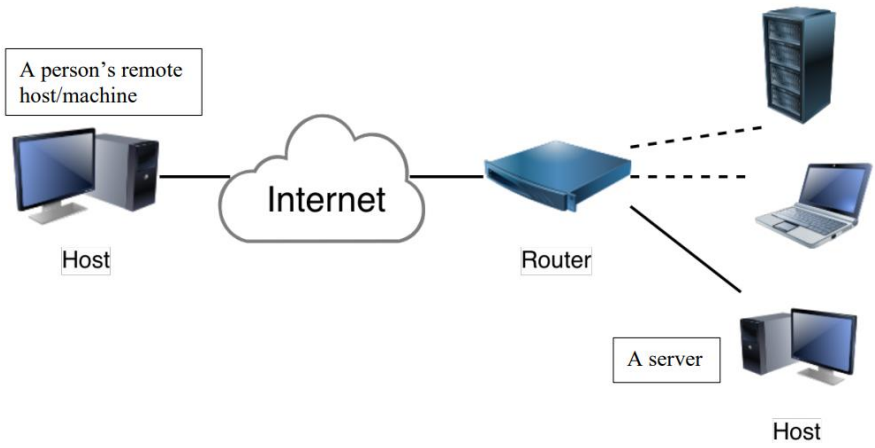

Figure 6 Host-to-host VPN [8]

Mesh is for many users within one or a few networks to connect individuals together securely. Every node in the network can connect directly to each other without a central gateway. [8]

2.3 Importance of Security in VPNs

The most vital role of VPNs is the privacy and security it provides users. By encrypting, tunneling, and rerouting internet traffic through secure servers, VPNs protect users from prying eyes, including ISPs and malicious hackers. VPNs offer end-to-end encryption, ensuring that data transmitted between devices remains unreadable to unauthorized entities. This is extremely important when utilizing public/unsecure Wi-Fi networks, which are vulnerable to man-in-the-middle attacks. VPNs can help bypass geographic restrictions that limit access to online content and services based on a user's physical location. This is done by connecting to servers in various locations worldwide. Because of the ability to divert geographic restrictions and prevent prying eyes, VPNs help promote digital freedom and circumvent censorship. Businesses and organizations are the main users of VPNs because they protect proprietary data. VPNs facilitate secure remote access for employees, enabling them to work from anywhere without compromising data integrity. VPNs have evolved into essential tools for safeguarding privacy, data integrity, and unrestricted access to the internet. Its versality makes them indispensable for individuals, businesses, and society.

IPsec Protocol

3.1 Introduction to IPsec

IPsec is the most used network layer security control. It is a collection of communication rules or protocols called that are used to establish secure network connections. IPsec ensures confidentiality by encrypting data and decrypting data which allows only parties with the secret key to read and exchange data. IPsec VPN uses symmetric keys to encrypt and decrypt data because it is more efficient. A NIST approved symmetric encryption algorithm includes the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Symmetric keys require both parties to have the secret key. Secret

keys are shared by using asymmetric cryptography. IPsec VPN usually uses the Diffie-Hellman key exchange algorithm. Integrity is ensured by generating a message authentication code (MAC) which is a checksum of the data. If the checksum does not match, then the receiver knows the data has been changed. A secret integrity key is used to calculate the MAC and it is received with the message. Algorithms that are used to generate the MAC include SHA-3 or HMAC. [8]

IPsec can authenticate IPsec endpoints by confirming their identity using a digital signature algorithm that is used for peer authentication, using a public and private key pair. Digital Signature Algorithm (DSA), RSA, or Elliptic Curve Digital Signature Algorithm (ECDSA) can be used. IPsec has replay protection which is a queue that stores out-of-order messages and will reorder the messages before decrypting and sending it to the endpoint device. IPsec tunneling prevents ISP or other third parties from analyzing frequency of communication or how much data is being sent. IPsec has perfect forward secrecy; session keys expire and are erased. This stops old traffic from being stored and decrypted later with a compromised session key. [8]

3.2 IKE session

To establish an IPsec connection, the parameters of the IPsec connection need to be negotiated between the two devices and this includes authentication, source, destination, encryption algorithm, and cryptographic keys. The Internet Key Exchange (IKE) protocol is most used to establish IPsec-based VPNs. The IKE protocol consists of UDP messages on port 500 and 4500. In Figure 7, the IKE packet format is shown. It includes the IKE header and the IKE data. The IKE header consists of the IKE Security Association (SA) Security Parameters Index (SPI) headers, the IKE version, exchange type, and flags.[8]

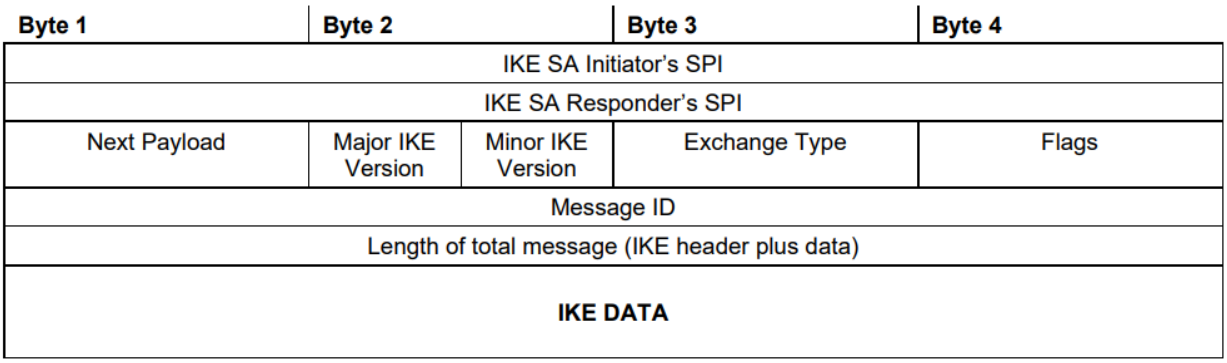

Figure 7 IKEv2 Packet Format [8]

The SPI numbers are used to uniquely identify an established IKE SA. The SPI numbers are used to select the corresponding IKE encryption/decryption key for the encrypted IKE message. To form an IKE session, Ike packet exchanges are made by sending a request packet and getting a reply packet. The sender/initiator will ensure that the send packet is delivered. Each exchange packet has a message ID, which is used to re-order the packets when received. For IKEv2 two exchanges are used, an IKE SA and an IPsec SA. [8]

[8] Barker, E. , Dang, Q. , Frankel, S. , Scarfone, K. and Wouters, P. (2020), Guide to IPsec VPNs, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-77r1 (Accessed June 15, 2023)

The following will be an example of establishing an IPsec connection using IKE. Device A wants to create a secure connection to device B using gateway-to-gateway.

1. Device A sends a message to device B without IPsec.
2. The message gets routed to Gateway A.
3. Gateway A checks the packet's Security Policy Database which dictates that ESP should be used to encrypt and ensure integrity. There is no Security Policy Database (SPD) entry.
4. Gateway A initiates an IKE SA negotiation with Gateway B. They determine that IKE SA has been established with IPsec SA.
5. The IKE SA dictates that ESP tunnel mode will be used. IPsec SAs are created for the Esp tunnel and added to the Security Association Database (SAD) which contain all active Sas for inbound and outbound traffic. The IPsec SAs are attached to the SPD entries which determine how packets are processed.
6. Gateway A adds IP headers to the packet following the SA that uses gateway A's IP address as the source IP address and gateway B's IP address as the destination IP address. The protocol is set to ESP and fills in the SPI number. It encrypts the original IP packet and adds it to the payload for the new packet. An integrity check is added.
7. Gateway A sends the packet to Gateway B.
8. Gateway B installs the IPsec SAs and SPD rules.
9. Gateway B receives the packet and uses the unencrypted SPI field in the ESP header to determine what SA to use. Gateway B can then decrypt the payload and check the integrity. Gateway B checks the SPD entry associated with the SAD entry to see if it is allowed to reach its destination and then sends it to Device B.
10. For Device B to reply, it will repeat steps 6 – 9 to send a pack to Device A but with the corresponding gateway and device.

If the IPsec connection reaches its expiration, then the gateway will initiate a rekeying process. This means both sides will need to install new inbound and outbound IPsec SAs and removing the old inbound and outbound IPsec SAs.

3.2 Authentication in IPsec

Certificate-based authentication is used for setting up IPsec for a large number of devices. The organization sets up an X.509 certificate and can reuse it for new devices as they are added. Certificate revocation list (CRLs) and the Online Certificate Status Protocol (OCSP) are used to revoke certificates that have been compromised or expired.

Extensible Authentication Protocol (EAP) is for adding undecided authentication methods in a standardized way using an authentication, authorization, and accounting (AAA) server. When a user initiates an EAP authentication to a server, the server forwards the message to the AAA server and the AAA server responds to both with whether the user is authenticated to access the server. The most common EAP protocol is EAP-TLS and EAP-MSCHAPv2. [8]

Raw public key authentication is used for IoT devices because authentication is done by publication in DNSSEC. IoT devices do not have the capacity to validate an X.509 certificate and use a public key to authenticate peer devices. The DNS acts as the CA and stores the published public keys. [8]

Pre-shared Secret Key (PSK) authentication is easy to configure and does not require the generation of public keys, certificates, servers, or third party to authenticate. It is used for gateway-to-gateway VPN implementations. PSK are susceptible to man-in-the-middle attacks because if an attacker gets a hold of the PSK, then they can connect to the VPN. [8]

IKEv2 is the successor of IKEv1 which is now obsolete. IKEv2 got rid of the general-purpose key exchange protocol. IKEv2 has all the IKEv1 additions as part of its core functionality. IKEv2 does not need the exchange methods to be configured. In IKEv2, only the sender is responsible for delivery of packets. IKEv2 can use TCP and TLC encapsulation. IKEv2 overall; is faster, more reliable, and more compatible with modern networking protocols. [8]

3.3 Encryption: Encapsulating Security Payload ESP

ESP is used for encrypting data and providing integrity; however, it is important to keep in mind that the outer header is not fully protected. ESP uses symmetric cryptography to encrypt IP packets and generate MAC to ensure integrity. ESP has two modes: transport and tunnel. Tunnel mode is when the IP header and its payload is encapsulated like mentioned in section 2.2.2 and is used for gateway-to-gateway and remote access VPN. ESP transport mode is used for host-to-host VPNs within networks. ESP uses the original IP header and does not create its own header, meaning only the payload is encrypted. This decreases overhead. ESP in tunnel mode is most used with IPsec because it can encrypt the entire IP packet, concealing the original source and destination. ESP can also be encapsulated in UDP and TCP, making it compatible with Network Address Translation (NAT). ESP can add padding to packets or send dummy packets which prevent network traffic analysis. [9]

TLS Protocol

4.1 Introduction to TLS

SSL or TLS VPN, like IPsec VPN provides a secure way to remote access another endpoint and is implemented at transport level. There are two types: TLS Portal VPNs and TLS Tunnel VPNs. Portal VPN is when a user uses a single TLS connection to a website to access the VPN network. The Tunnel VPN is when the user uses a web browser to access the VPN network and applications non-accessible by the portal VPN. And just like IPsec, TLS provides confidentiality, integrity, peer authentication, replay protection, traffic analysis protection, and access controls.[10] Similar to IPsec, the tunnels fully protect IP traffic, but TLS tunnels are created by loading software onto the user's device.

Unlike IPsec, TLS uses cipher suites to define the cryptographic algorithms that a user and client use to communicate securely. The initiator of the TLS connection offers a list of cryptographic algorithms it can use, and the other side chooses from that list, usually the most secure method they can both use. For authentication, "SSL uses certificates that are signed by trusted entities to authenticate the server to the Web user."[10] After the cipher suite is chosen, the TLS handshake is performed to create the encryption keys. Then the TLS record applies encryption and sends data via the TLS tunnel. The record divides the payload into packets and uses digital certificates to authenticate each packet at either end of the tunnel. Encryption is built into SSL/TLS, so it does not need to be added like IPsec.

---

[9] Kent, S, "IP Encapsulating Security Payload (ESP)", Network Group, https://datatracker.ietf.org/doc/html/rfc4303 (Accessed Aug 3, 2023)
[10] Frankel, Sheila, et al. Special Publication 800-113 Guide to SSL VPNs Recommendations of the National Institute of Standards and Technology. July 2008.

SSL VPN has three main functions: proxying, application, translation, and network extension. Proxying is an intermediary device that proves communication between a client and a server and usually acts as the server, so the client thinks it talking directly to the server. The proxy server encrypts, decrypts, packet inspects, and redirect communication. Application translation is used to convert one protocol to another protocol such as when an outdated protocol is being used. Network extension is when a host-to-gateway tunnel allows a user to connect to an internal connection. [10]

There are still many disadvantages of TLS VPN such as application/client support is limited and network extension requires a client to be installed on the user's device,

"These include limitations on their ability to support a large number of applications and clients, the methods of implementing network extension and endpoint security, the ability to provide clientless access, the use of the SSL VPN from public locations, and product and technology education."

5 Performance Comparison between IPsec and TLS VPNs

In the Performance Comparison of IPsec and TLS Based VPN Technologies article[11]. They evaluated the throughput of IPsec and TLS VPN using a program called IxChariot and identical endpoints would generate traffic. Throughput is how much data can be transferred from one endpoint to the other, measured in units of time. The Figure 8, shows the measured throughput results of OpenVPN (TLS) and IPsec. The article concluded that "IPsec wins over OpenVPN (while using the same type of cipher) by a small margin. It is faster while using AES and Blowfish ciphers and has smaller delay. It loses only when 3DES cipher is used, but this is not that significant, since this obsolete cipher will not be used anymore."

Test	Response average (s)	Response maximum (s)	Average throughput (Mbps)	CPU utilization sending node	CPU utilization receiving node
A->B Ethernet	0,014	0,035	553	71	81
B->A Ethernet	0,018	0,038	440	90	59
A->B OpenVPN Blowfish	0,083	0,2	96	66	90
B->A OpenVPN Blowfish	0,081	0,3	99	95	77
A->B OpenVPN AES	0,092	0,19	98	62	94
B->A OpenVPN AES	0,093	0,3	99	93	78
A->B OpenVPN 3DES	0,131	0,263	60,98	78	94
B->A OpenVPN 3DES	0,129	0,352	61,77	92	86
A->B IPsec 3DES	0,184	0,28	45	99	40
B->A IPsec 3DES	0,212	0,37	37,7	99	32
A->B IPsec AES	0.056	0.077	142	90	84
B->A IPsec AES	0.059	0.1	135	97	63
A->B IPsec Blowfish	0,066	0,087	121,76	98	73
B->A IPsec Blowfish	0,08	0,197	99,87	99	52

Figure 8 Throughput Comparison between OpenVPN and IPsec

[11] I. Kotuliak, P. Rybár and P. Trúchly, "Performance comparison of IPsec and TLS based VPN technologies," 2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stara Lesna, Slovakia, 2011, pp. 217-221, doi: 10.1109/ICETA.2011.6112567. https://ieeexplore.ieee.org/abstract/document/6112567

Another article [12] comparing OpenVPN and IPsec performance said, “IPsec clearly outperforms OpenVPN... The main reason … [is] the CPU partly running in user, kernel and irq. irq mode handles interrupt routines required when switching from user to kernel mode and vice-versa, but in Linux systems also performs IPsec packet processing. …IPsec processing does not trigger expensive context switches and confirms … previous implications.” Comparing the key exchange showed that there is “idle CPU time frames, which can only … be caused by OpenVPN implementing an internal key exchange rate limiter.” [12] This shows that there are multiple steps in the establishment of OpenVPN connection is decreasing the throughput.

Although IPsec performed better than OpenVPN, there are advantages of using it over IPsec. The implementation of OpenVPN is extremely beginner friendly and quick. All it takes is the generation of certificates (often from a router or device with OpenVPN capability) and downloading a client on the endpoint. If an organization of individuals does not have the technical expertise or if they want to remote into a network/device only a few times or short amount of time, then OpenVPN is a clear winner. For larger implementation of a VPN where the extra performance builds up over millions of packets of communication then IPsec is recommended.

Conclusion

VPNs are great tools to address segregating and securing network issues, but they will not be useful if they cannot provide the same level of service if not close to the level of service as alternatives. Security should be the top priority when choosing a VPN, therefore a VPN protocol will need a strong encryption algorithm and support PFS. If a VPN provider is utilized, then the policy of the VPN provider needs to be carefully examined to ensure that they will not store or monitor activity. Speed and performance are important to consider because the quality of the service should not be impacted. This could mean looking at how many servers there are, the location of the servers, and what the throughput of the connection is. Compatibility is another consideration, especially in industries with extremely specific operating systems and devices. The VPN needs to be user-friendly, if the user must jump through many hoops to get connect to the VPN, then users may stop using it, rendering the VPN useless. Organizations need to research and compare different VPN options to find the one that best aligns their needs for security, performance, and usability.

There are many distinct types of VPNs that can solve the common problems of privacy, security, and segmentation without building an entirely separate physical infrastructure. There will not every be a single implementation of VPN that will fulfill everyone is needs. Every organization has its own specific use case and needs to meet specific requirements. Network engineers and architects will continue to see new VPN technologies emerge, increasing the options to choose from, and they will have to analyze each option meticulously.

[12] Pohl, F., & Schotten, H. D. (2017). Secure and scalable remote access tunnels for the IIOT: An assessment of openvpn and IPsec Performance. Service-Oriented and Cloud Computing, 83–90. https://doi.org/10.1007/978-3-319-67262-5_7

Bibliography

[1] Ferguson, Paul, and Geoff Huston. "What is a VPN?" (1998): 01-22.

https://libguides.murdoch.edu.au/footnote/text

[2] Alexiei Zahorski, “How VPNs Have Shaped the Internet over the Years,” MUO, June 15, 2022, https://www.makeuseof.com/how-vpns-shaped-internet/.

[3] “TCP/IP Model,” GeeksforGeeks, July 21, 2023, https://www.geeksforgeeks.org/tcp-ip-model/.

[4] “The VPN Overview.” July 22, 2023, https://media.techtarget.com/searchNetworking/downloads/Buildvpn1.pdf

[5] “GRE Tunnel,” Network Direction, accessed August 1, 2023, https://networkdirection.net/articles/routingandswitching/gretunnels/.

[6] “Layer Two Tunneling Protocol (L2TP)”, NordLayer, accessed August 1, 2023,

https://nordlayer.com/learn/vpn/l2tp/

[7] “How PPTP Works”, O’Reilly, accessed August 1, 2023, https://www.oreilly.com/library/view/virtual-private-networks/1565925297/ch04s02.html

[8] Barker, E. , Dang, Q. , Frankel, S. , Scarfone, K. and Wouters, P. (2020), Guide to IPsec VPNs, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-77r1 (Accessed June 15, 2023)

[9] Kent, S, “IP Encapsulating Security Payload (ESP)”, Network Group, https://datatracker.ietf.org/doc/html/rfc4303 (Accessed Aug 3, 2023)

[10] Kent, S, “IP Encapsulating Security Payload (ESP)”, Network Group, https://datatracker.ietf.org/doc/html/rfc4303 (Accessed Aug 3, 2023)

[11] I. Kotuliak, P. Rybár and P. Trúchly, "Performance comparison of IPsec and TLS based VPN technologies," 2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stara Lesna, Slovakia, 2011, pp. 217-221, doi: 10.1109/ICETA.2011.6112567. https://ieeexplore.ieee.org/abstract/document/6112567

[12] Pohl, F., & Schotten, H. D. (2017). Secure and scalable remote access tunnels for the IIOT: An assessment of openvpn and IPsec Performance. Service-Oriented and Cloud Computing, 83–90. https://doi.org/10.1007/978-3-319-67262-5_7