MPLS vs. IPsec VPN: Choosing the Right Network Architecture for Enterprise WAN

Nikhil Bhagat
Principal Network Engineer
Independent Scholar, Network
Engineering
nikhil.bhagat90@gmail.com

***Abstract*— The rapid expansion of the global business has increased the demand for secure, resilient and optimized WANs. Enterprises had traditionally used Wide Area Network (WAN) technologies like Multi-Protocol Label Switching (MPLS) or Internet Protocol Security (IPsec) VPNs to link geographically separated data centers. Each of these technologies provides their own benefits, based on an organization's requirement and a combination of performance, price and security needs. This paper will dive deep to provide a comparative analysis between MPLS and IPsec VPNs technologies and the enterprise WAN scenarios in which these VPNs could be deployed. The paper describes internet circuits, their drawbacks, the benefit of MPLS circuits, and how IPsec VPN can protect public internet circuits. Last but not least, the paper aims to provide network administrators with the necessary tools to choose an appropriate circuit for their organization by providing network architecture scenarios in which MPLS or IPsec VPN over internet circuits is the best choice.**

Keywords*— Internet Circuits, MPLS, IPSec VPN, Tunnel, Budget, Reliability, Security.

I. INTRODUCTION

As the businesses grow globally, their IT systems must adapt to connect branch offices, sites, and data centers across large geographical areas. A solid and effective WAN is necessary for a smooth communications across these distributed sites. For a long time, WANs have been designed using leased lines, MPLS, and internet-based VPN solutions [1]. However, as organizations become more reliant on cloud computing, remote work, and other bandwidth-intensive applications, determining the appropriate WAN solution can become increasingly challenging [2].

MPLS and IPsec VPN over internet circuits are the two standard connectivity technologies used within enterprise WANs [3]. MPLS provides high performance, predictable and private WAN connections, whereas IPsec VPNs are inexpensive ways to secure information over public networks. The paper compares the respective methodologies across different networking environments and provides guidance on which architecture would best fit the organization's requirements.

II. INTERNET CIRCUITS

Internet circuits form the foundation of IP communications and are becoming an increasingly preferred WAN connectivity option due to their affordability and availability [4]. An internet circuit is a link between a private network and the rest of the work i.e. internet, provided by an Internet Service Provider. These circuits are mostly destined to transport data from enterprise sites to the internet, connecting to cloud applications, services and remote access [5]. Four of the major internet circuits are listed below.

A. Broadband

Broadband circuits include DSL, cable and fiber optic networks, which provide high-bandwidth at relatively low cost [6]. Broadband internet is universally accessible and it is also a common way to link smaller or medium-sized branch offices to the corporate network.

B. Dedicated Internet Access (DIA)

DIA circuits give a secure and more reliable internet connection. In contrast to the shared broadband, DIA offers dedicated bandwidth that doesn't get impacted by other customers on the network [7]. That makes DIA ideal for sensitive and business-critical applications.

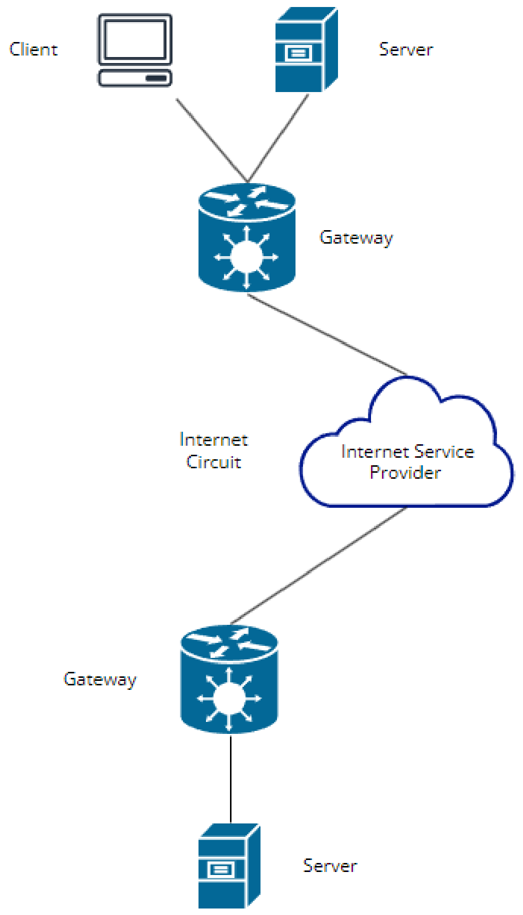

Fig. 1 Internet Circuit

C. *Cellular and Wireless*

With the evolution of 4G, 5G, and other wireless technologies, enterprises have shifted to wireless internet connections for back-up or primary WAN in outbound or mobility-centric environments [8].

D. *Satellite*

Satellite internet is utilized when an organization needs connectivity in remote areas with less to no connectivity options [9]. It supports general coverage but is very latency prone and not really ideal for real-time applications.

Even though Internet circuits are cost-effective and provide scalable bandwidth, they have a few downsides to consider, which may prevent them from being deployed in certain use cases.

III. DRAWBACKS OF INTERNET CIRCUITS

Though they're commonly used, internet circuits are hampered by some issues that make them not the best choice for WAN deployments in enterprises, especially those that need high performance, security, and reliability. Below are the major disadvantages of internet circuits for WAN connectivity:

A. *Unpredictable Performance*

The internet is always a best-effort network and there are no guarantees of latency, jitter, packet loss or bandwidth [10]. As internet traffic relies on public infrastructure, speed will vary due to congestion, routing inefficiencies, and bandwidth share with other customers. This uncertainty has a negative effect on real-time services such as VoIP, video calling and online collaboration systems.

B. *Security Risks*

Internet circuits pass data over a public network, and are thus far less secure than private connections [10]. Without proper encryption and authentication, business critical and sensitive data traveling across the internet can be intercepted, manipulated, and is prone to various cyber-attacks. For data sent over the internet, enterprises need to add further security features like IPSec [11].

C. *Reliability Issues*

Internet circuits, in contrast to dedicated leased lines or MPLS circuits, do not typically come with SLAs for uptime or availability [6]. Without a guarantee of availability, it's not suitable for mission-critical applications that demand high availability and high performance.

D. *Limited Traffic Control*

The distributed internet makes it impractical for companies to regulate traffic routing, prioritization, or QoS [12]. Therefore, enterprises have limited visibility into traffic dynamics between sites, resulting in poor routing and poor bandwidth usage.

However, internet circuits are still a viable option for WAN connectivity especially when they're used in conjunction with security solutions like IPsec VPN to resolve security concerns.

IV. INTRODUCTION TO MPLS CIRCUITS

Multi-Protocol Label Switching (MPLS) is a data-carrying mechanism that forwards the traffic over a private network using short path labels rather than full IP addresses. Enterprises deploy MPLS to build WANs that span sites at scale. It enables better traffic routing control and empowers service providers to construct high quality, resilient networks for their customers.

MPLS circuits are supplied by telecommunications providers and usually include performance guarantees like SLAs for latency, jitter, packet loss, and uptime. Instead of traditional internet circuits, MPLS is delivered through a private network, separating traffic from the public internet and adding security.

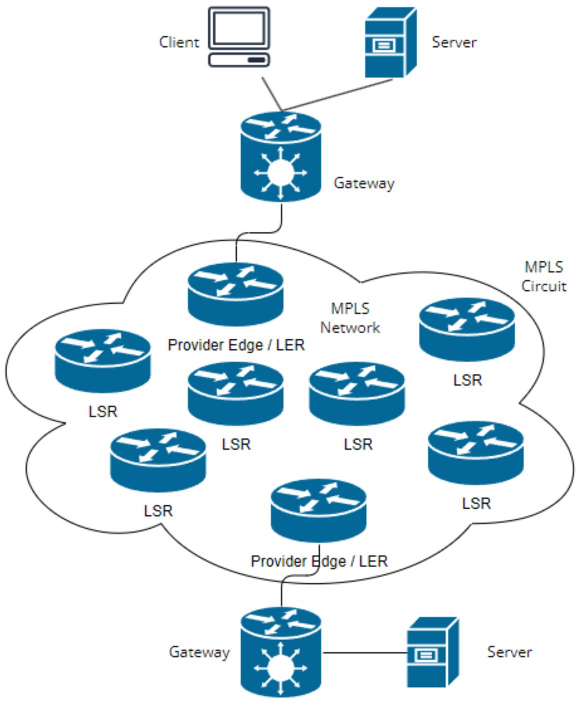

Fig. 2 MPLS Provider Network and MPLS Circuit

A. Label Assignment

In an MPLS network, rather than forwarding packets based on their IP address, each packet is tagged with a fixed-length label [15]. This label is put on the packet at the point of entering the MPLS network and can be used to find its route through the network.

B. Label Switching

Each router in an MPLS network is a Label Switch Router (LSR). LSRs do not look at the entire IP packet to determine the destination of the packet [15]. Rather, they just examine the packet label. Based on this label, LSR sends the packet to the next hop in the network.

C. Label Edge Routers (LERs)

Label Edge Routers are the edge routers that associate the initial label to packets arriving (Ingress LER) in the MPLS network and discard the label as the packet leaves the MPLS network (Egress LER) [16].

D. Core LSRs

In the MPLS network, core LSRs do label switching and pass packets according to their labels without checking the IP header of the packet [13].

E. Label Distribution Protocol (LDP)

In order to enable every LSR of the MPLS network to be able to decode the labels, the LSRs communicate label data via a protocol known as the Label Distribution Protocol (LDP) [13]. This allows LSRs to build a Label Forwarding Information Base (LFIB) that associates labels to next-hop LSRs.

F. Traffic Engineering (TE)

Traffic engineering is one of the major strengths of MPLS. MPLS allows service providers to manage traffic and maximize network bandwidth and latency by choosing paths based on defined parameters, rather than just forwarding the packets using shortest-path IP routing [17].

G. Forwarding Equivalence Class (FEC)

MPLS employs Forwarding Equivalence Class (FECs) to organize packets that must take the same route over the network [18]. Every packet inside the same FEC is labeled with the same path and routes, making it easier for the core network to take routing decisions.

H. Quality of Service (QoS)

MPLS supports Quality of Service (QoS) by giving the network administrator the ability to prioritize certain types of traffic over others [19]. Since MPLS labels allow different types of information to be carried, packets can be assigned different labels based on priority. As a result, critical traffic (such as voice or video) can receive higher priority labels compared to non-essential data.

I. MPLS Packet Flow

- Ingress: When a packet flows into the MPLS network, the Ingress LER checks the IP header and assigns a label with respect to the FEC. The packet is then forwarded to the next LSR.

- Label Switching: During the routing of the packet, all LSRs examine the label and replace it with another label given by the LFIB [18]. This new label indicates to the next router where to send the packet.
- Egress: When a packet reaches the Egress LER (the last router before it leaves the MPLS network), the label is removed, and the packet is forwarded using its IP address.

J. Application

- VPNs (Virtual Private Networks MPLS is used to create most Layer 3 VPNs, which provide isolated and secure networks for a large number of customers on a unified infrastructure.
- Traffic Engineering: MPLS allows network administrators to steer traffic using the optimal routes for the best possible bandwidth and performance.
- Quality of Service: Packet labels enable MPLS to offer differentiated services and provide QoS for critical traffic by decoding the packets by service class [20].

V. ADVANTAGES OF USING MPLS CIRCUITS

MPLS has many advantages over other internet circuits, making it a popular choice for enterprise WAN connectivity:

A. Predictable Performance

MPLS circuits have SLAs that guarantee the metrics like latency, jitter, and packet loss [21]. Such predictability is vital for companies operating latency-critical applications like VoIP, videoconferencing, and real-time data analytics.

B. Enhanced Security

MPLS networks work in a private network context, where business traffic remains disconnected from the public internet infrastructure [22]. MPLS doesn't encrypt traffic by default, but a private network mitigates interception and attacks. MPLS can be combined with encryption methods for greater data security for businesses that need a very secure network.

C. Quality of Service (QoS)

MPLS offers advanced QoS functionality where enterprises can deprioritize certain types of traffic (e.g., voice and video) over more critical traffic (e.g., file transfer) [23]. This makes sure high-value apps get the bandwidth they need and don't get throttled.

D. Traffic Engineering

MPLS provides traffic engineering, where network administrators can manage how data travels through the network. By designing traffic flows enterprises will be able to optimize bandwidth usage and eliminate network bottlenecks.

E. Scalability

MPLS can scale up incredibly well, suited for larger organizations with multiple offices. MPLS operators are able to simply add new locations to their existing network and scale their bandwidth according to need, thereby allowing for exponential growth [24].

F. Reliability

MPLS providers offer SLAs to ensure uptime and availability making MPLS circuits desirable over the internet circuits. This is important for critical applications that cannot tolerate downtime.

MPLS can be a great performance, security, and reliability enhancement, but it comes at a high price tag compared to the internet circuits. Therefore, some companies use IPsec VPNs over the existing internet circuits as an economical alternative.

VI. HOW IPSEC VPN ADDS SECURITY OVER INTERNET CIRCUITS

IPsec is a protocol suite that encrypts the IP traffic by authenticating and encrypting each IP packet. IPsec VPN is used primarily for protecting information sent over network circuits to ensure the security of traffic between multiple locations traversing through the internet [25]. IPsec secures your data from eavesdropping and manipulation, even when it is communicated through public networks. Below are IPsec VPN's most important security features.

A. Encryption

IPsec encrypts and ciphers data at the IP layer, so that even if it is intercepted in the public internet, the data will not be readable by others. The most popular encryption protocols are AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard).

B. *Authentication*

IPsec employs some type of authentication system, such as pre-shared keys or digital certificates to ensure only approved participants are allowed to connect to a VPN connection. This keeps rogue users on the network.

C. *Data Integrity*

Integrity checks make sure that information is not corrupted during transfer using IPSec [12]. If the data is compromised, the IPsec protocol discards the packet.

D. *Tunnel Security*

IPsec builds a tunnel between two endpoints (e.g., a branch office and the headquarters), where all traffic is encrypted and secure from outside bad actors [12].

VII. ADVANTAGES OF IPSEC VPN OVER INTERNET CIRCUITS

A. *Cost-Effective*

IPsec VPNs over the internet circuits are less costly than MPLS and ideal for smaller branches or offices located in the remote areas [26].

B. *Global Reach*

The circuits are available virtually everywhere and companies can connect to facilities in remote or underserved locations.

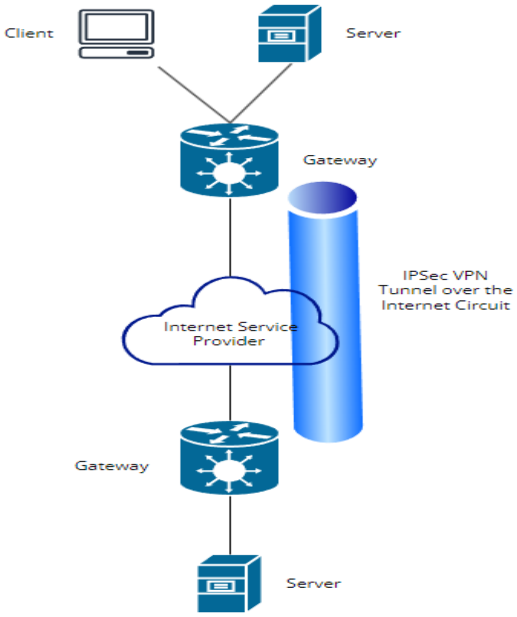
Client
Server
Gateway
IPSec VPN Tunnel over the Internet Circuit
Internet Service Provider
Gateway
Server

Fig. 3 IPSec VPN tunnel over the Internet Circuit

C. *Scalability*

IPsec VPNs can easily scale up to new sites or users, making them suitable for organizations that are growing rapidly [25].

VIII. RECOMMENDED NETWORK ARCHITECTURE SCENARIOS TO USE MPLS

MPLS circuits should be used when performance, reliability, and security are the top pillars for the organization. Below are just a few of the scenarios where MPLS should be the go-to enterprise WAN solution:

A. *Latency Sensitive Applications*

MPLS is a great choice for businesses with high-latency applications like VoIP, video conferencing, and real-time analytics. The guaranteed uptime of MPLS SLAs makes sure that these applications function without compromising on quality.

B. *Business-Critical Networks*

Businesses that require a highly reliable connection and cannot tolerate network downtime should use MPLS circuits for its guaranteed uptime [19]. MPLS circuits typically provide a high level of redundancy. High redundancy provides the organization an assurance of a guaranteed uptime even during a link failure.

C. *Need for Private Connectivity*

If an organization running business-critical application requires a high-level security, like banks or hospitals, MPLS could help ensure that the sensitive data is transferred through a private network instead of the public internet [27].

D. *Multi-Site Enterprises*

Larger enterprises with multiple branches, data centers and regional offices can also take advantage of MPLS's scalability and central control. It enables you to interconnect several locations efficiently while ensuring the network performance and safety.

IX. RECOMMENDED NETWORK ARCHITECTURE SCENARIOS TO USE IPSEC VPN OVER INTERNET CIRCUITS

IPsec VPNs over internet circuits can be an affordable solution for companies that are seeking to establish secure connection on a budget. Below are some use cases where IPsec VPN would be a better option than MPLS:

A. Budget-Constraint Deployments

IPsec VPNs over internet circuits allow for secure access without the additional expense of MPLS, making them ideal for Small and medium-sized businesses (SMBs) or remote branches with limited budgets [28].

B. Connectivity in underserved areas

IPsec VPNs can secure connections to the internet via widely accessible internet circuits in remote or underserved areas where MPLS circuits are not feasible or cost prohibitive.

C. Failover Mechanisms

For enterprises, IPsec VPNs over internet circuits can serve as an off-site backup or failover layer for their main MPLS infrastructure. If an MPLS service is down, IPsec VPN can offer a secondary path for business continuity.

D. Connectivity between On-premises and Cloud

As cloud computing is being widely adopted by organizations, enterprises can leverage IPsec VPNs to securely connect on-premises networks to cloud infrastructure over the public internet [30].

X. CONCLUSION

MPLS and IPsec VPNs both have different advantages and trade-offs, making them ideal for specific type of enterprise WAN deployments. MPLS offers predictable performance, security, and high availability, which is the key for highly scalable and mission-critical applications. However, MPLS circuits are more expensive and are less accessible than internet circuits. Conversely, IPsec VPNs over the internet circuits are affordable ways to secure data communication across public networks and are well suited for Small and medium-sized businesses (SMBs), remote locations and backup environments.

Ultimately, the choice of deploying MPLS or IPsec VPN over internet circuits should be based on the specific needs of the organization, including performance requirements, security considerations, budget constraints, and geographical locations. In many cases, a hybrid approach that combines both MPLS and IPsec VPN can offer the best balance between performance, security, and cost, ensuring a robust and flexible enterprise WAN.

REFERENCES

[1] T. Birmingham, "Private WAN Infrastructures," Cisco Press, Feb. 14, 2014. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2202411&seqNum=7.

[2] "The 2017 Guide to WAN Architecture and Design - Part 1: State of the WAN," Cisco Press, 2017. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2202411&seqNum=7.

[3] "Distribution and Access Layer," Cisco Press, 2014. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2202411&seqNum=7.

[4] M. Zukerman, "Increasing scope for circuit switching in the optical internet," IEEE Communications Magazine, vol. 40, no. 5, pp. 66-72, May 2002.

[5] P. A. Rahman and E. Y. Bobkova, "The reliability model of the fault-tolerant border routing with two Internet services providers in the enterprise computer network," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, pp. 108-112.

[6] M. Fitzmaurice, "The use of packet-switched vs. circuit-switched networks for data transport in a public transit environment," in 2010 IEEE Intelligent Transportation Systems (ITSC), 2010, pp. 1618-1623.

[7] "The Pros and Cons of Dedicated Internet Access," Cisco Press, 2020. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5.

[8] E. J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bubley and J. Kusuma, "Revisiting wireless internet connectivity: 5G vs Wi-Fi 6," IEEE Communications Standards Magazine, vol. 4, no. 3, pp. 19-27, Sept. 2020.

[9] D. Bhattacherjee, W. Aqeel, I. N. Bozkurt, A. Aguirre, B. Chandrasekaran, P. B. Godfrey, G. Laughlin, B. Maggs, and A. Singla, "Gearing up for the 21st century space race," in Proceedings of the

17th ACM Workshop on Hot Topics in Networks (HotNets '18), New York, NY, USA, 2018, pp. 113–119. [Online]. Available: https://doi.org/10.1145/3286062.3286079.

[10] C. Johnson, Y. Kogan, Y. Levy, F. Saheban, and P. Tarapore, "VoIP reliability: A service provider's perspective," in 2004 IEEE International Conference on Communications (ICC), 2004, pp. 1563-1567.

[11] D. Street, "IPSec solution," EDPACS, vol. 38, no. 5, pp. 6–17, 2008. [Online]. Available: https://doi.org/10.1080/07366980802379871.

[12] F. Cangialosi, A. Narayan, P. Goyal, R. Mittal, M. Alizadeh, and H. Balakrishnan, "Site-to-site internet traffic control," in Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM), 2021, pp. 257-270.

[13] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol label switching architecture," RFC 3031, Jan. 2001.

[14] M. A. Ridwan, N. A. M. Radzi, W. S. H. M. W. Ahmad, F. Abdullah, M. Z. Jamaludin, and M. N. Zakaria, "Recent trends in MPLS networks: Technologies, applications, and challenges," Journal of Communications, vol. 13, no. 6, pp. 318-326, Jun. 2018.

[15] B. Daugherty and C. Metz, "Multiprotocol label switching and IP. Part I. MPLS VPNs over IP tunnels," IEEE Internet Computing, vol. 7, no. 3, pp. 68-74, May 2003.

[16] K. Owens and J. Kroculick, "Multiprotocol label-switching network functional description," in 2004 International Symposium on Applications and the Internet (SAINT), 2004, pp. 132-135.

[17] "Traffic Engineering with MPLS (MPLS-TE)."

[18] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. F. A. McManus, "Requirements for traffic engineering over MPLS," RFC 2702, Sept. 1999.

[19] F. Huang, X. Yi, H. Zhang, and P. Gong, "Key requirements of packet transport network based on MPLS-TP," in 2011 International Conference on Computer Science and Service System (CSSS), 2011, pp. 1620-1624.

[20] D. Awduche and B. Jabbari, "Internet traffic engineering using multi-protocol label switching (MPLS)," Computer Networks, vol. 40, no. 1, pp. 111-129, Sept. 2002.

[21] H. E. Wahanani, "Performance analysis of video on demand and video streaming on the network MPLS traffic engineering," in 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2020, pp. 463-468.

[22] M. Behringer, "Analysis of the security of BGP/MPLS IP virtual private networks (VPNs)," RFC 4381, Feb. 2006.

[23] S. H. Sridhar and J. Arunnehru, "Traffic engineering: An application of MPLS L3 VPN technology," in 2019 International Conference on Recent Advances in Computer Science and Engineering (ICRACSE), 2019, pp. 133-137.

[24] B. Decraene, N. Leymann, M. Konstantynowicz, C. Filsfils, and D. Steinberg, "Seamless MPLS architecture," RFC 7851, May 2016.

[25] D. Deshmukh and B. Iyer, "Design of IPSec virtual private network for remote access," in 2020 International Conference on Industry 4.0 Technology (I4Tech), 2020, pp. 275-279.

[26] N. Raghavan, R. Gopal, S. Annaluru, and S. Kura, "Virtual private networks and their role in e-business," in Proceedings of the 2001 International Conference on Information Technology: Coding and Computing (ITCC), 2001, pp. 101-105.

[27] P. Xu, Y. Wang, and W. Ding, "Promising network evolution technology: MPLS," China Communications, vol. 12, no. 6, pp. 76-87, Jun. 2015.

[28] D. Grayson, D. Guernsey, J. Butts, M. Spainhower, and S. Shenoi, "Analysis of security threats to MPLS virtual private networks," in Proceedings of the 2007 IFIP International Conference on Critical Infrastructure Protection, 2007, pp. 187-201.

[29] S. Patton, B. Smith, D. Doss, and W. Yurcik, "A layered framework strategy for deploying high assurance VPNs," in Proceedings of the 2002 Annual Computer Security Applications Conference (ACSAC), 2002, pp. 84-92.

[30] F. A. Arshad, G. Modelo-Howard, and S. Bagchi, "To cloud or not to cloud: A study of trade-offs between in-house and outsourced virtual private network," in 2018 IEEE International Conference on Cloud Engineering (IC2E), 2018, pp. 187-197.