EXPLORING THE EFFECTIVENESS OF VPN ARCHITECTURE IN ENHANCING NETWORK SECURITY FOR MOBILE NETWORKS: AN INVESTIGATION STUDY

Khawla Azwee[1], Mokhtar Alkhattali[1] and Mostafa Dow[2]

[1]Department of Computer Science, High Institute of Science and Technology, Qaser Bin Ghashir, Libya
[2]Department of Computer Science, College of Science and Technology, Jadu, Libya

ABSTRACT

The rapid development of technology in communications has transformed the operations of companies and institutions, paving the way for increased productivity, revenue growth, and enhanced customer service. Multimedia calls and other modern communication technologies boost mobile network, thus their utilization is critical to moving the business forward. However, these widely used networks are also vulnerable to security threats, leading network vendors and technicians to implement various techniques to ensure network safety. As the need to safeguard technologies grow and there has been a significant increase in growth the idea of a virtual private network (VPN) emerged as a key strategy for tackling the threat to network security. the authors suggested looking into this issue and presenting the findings of a study that contained insightful observations from the literature reviews that served as the primary source of research besides questionnaire responses as opinions from those who have experience in the network industry and its security. Through this research, it became evident that several technologies and approaches exist to safeguard networks, but the Transport Layer Security (TLS) architecture stood out as a superior solution, particularly for mobile networks.

KEYWORDS

VPN, TLS, Mobile Networks, Network Security, Risk Mitigation.

1. INTRODUCTION

In today's digital age use of digital technology has become ubiquitous in almost every aspect of modern life. This has led to an increase in the use of digital transformation in the work of organizations and institutions, which has led to raising the level of service provision in terms of ease of use and security. Due to the presence of a wide range of applications and programs provided by companies to communicate with customers and provide their services electronically (27), as a result, focusing on the security aspect for networks has become one of the most important priorities for these institutions and companies(1). However, with the increasing use of networks, especially multi-use networks for encapsulating audio and video files(29), the ability to scale real-time data traffic, and dynamic memory usage, network security has become a major concern. As the use of the Internet as a basis for network design increases the security problem and facilitates network penetration. To overcome this problem, a virtual private network (VPN) is created for network security(20),this network connection provides a secure alternative to public networks by connecting multiple customer sites to a shared network with similar security measures as a private network. It allows these customer sites to access the network and exchange

data with each other while ensuring the safety and privacy of their information. This network serves as a reliable and protected connection that mimics the functionality of a VPN to ensure secure communication between the customer sites involved. (3-14).

There are two main categories of VPN protocols, namely Site-to-Site VPN and Remote VPN. Site-to-Site VPN is basically to connect more than one customer using the internet to transfer information securely(5-7-26). Mostly the protocols used in VPN are Sit-to-sit Internet Protocol Security (IPSec),Generic Routing Encapsulation (GRE) and Multiprotocol Label Switching (MPLS). To serve as a medium for securely transmitting information. A Remote Access protocol can be provided using MPLS, Transport Layer Security (TLS), and IPSec (15-19-25).In terms of scalability, MPLS VPN is among the best. IPSec ensures the transmission of data over an IP network while also providing the reliability, credibility, confidentiality, and safety of the information transmitted using this technology. As for what is known as TLS, it is widely used on the Web (10-18). However, the use of VPNs brings with it certain risks, particularly if they are used over public internet connections. Thus, it is essential to carefully analyze and select the appropriate VPN architecture for mobile networks(13). This paper aims to study the various types of VPN solutions available for the mobile network and provide recommendations on the best VPN architecture for the mobile network, based on the analysis and opinion of a group of specialists, and the data collected from literature studies and online questionnaires or interviews.
This research also has many significant implications, particularly for organizations seeking to secure their mobile network communications, and provides a valuable resource for network administrators, and security personnel and a good reference for researchers.

2. RELATED WORKS

For organizations seeking to maintain secure remote access to their online resources, VPNs ensure the confidentiality and integrity of transmitted data. Several VPN technologies can provide different levels of security and efficiency, including TLS, MPLS, and IPSec. This allows organizations to choose the VPN solution best suited to their specific needs(3-9).

The MPLS protocol has emerged as an important enhancement to networks as it supports many services to improve the efficiency and functionality of IP networks (6). MPLS simplifies encryption and traditional complex routing protocols to create secure communication channels by adding a label to each packet (23), which enables faster and more accurate routing within the network while maintaining data security and confidentiality. Moreover, MPLS supports traffic engineering to avoid network congestion and ensure the most efficient use of resources to minimize delays and packet loss, thus being very useful for applications with stringent Quality of Service (QoS) requirements and very useful in multimedia traffic (28-30).The MPLS backbone encapsulates VPN frames and transmits them using MPLS labels at Layer 2 by integrating various Layer 2 services, such as ATM Cell Relay and Ethernet, with MPLS to integrate with MPLS functionalities to provide a comprehensive networking solution (22).To establish connectivity, between locations, within a VPN, Layer 3 MPLS VPNs rely on the utilization of Multiprotocol Border Gateway Protocol (MP BGP). They offer flexibility, security, and segmentation advantages over traditional overlay VPN technologies (6).The adoption of MPLS technology brings benefits to both service providers and enterprises. Service providers find MPLS cost-effective, and enterprises utilize MPLS features such as Traffic Engineering and Fast ReRoute for improved connectivity and network management (29).

IPv6 mandates security features like confirmation and encryption. Internet Protocol Security (IPSec), which is interoperable across vendors, provides secure communication over networks and enables the creation of VPNs (21).IPSec enables secure access to organizational networks through a local call to an Internet Service Provider (ISP) while extending security to both wired

and wireless connections (3). Its implementation requires dynamic IP addresses, client protection, network shielding, and robust authentication (32).Implementing IPSec at the network level ensures strong security and requires no modifications to user applications or server systems (17). It can establish secure virtual subnets within a company, providing security for individual users or specific applications (16).

Cryptographic protocol TLS can be used at the application layer, the transport layer in the mobile network security stack, and commonly at the application layer to secure web traffic, email communications, and other applications that require a secure connection. In mobile networking environments networked devices rely on Protocol TLS in the transport layer to enable communication (3–8–17). This becomes crucial for mobile network operators as TLS encryption safeguards the data between devices ensuring a high level of information security (11).

3. METHODOLOGY OF THE RESEARCH

The researchers utilized two methods for gathering information as shown in figure 1.

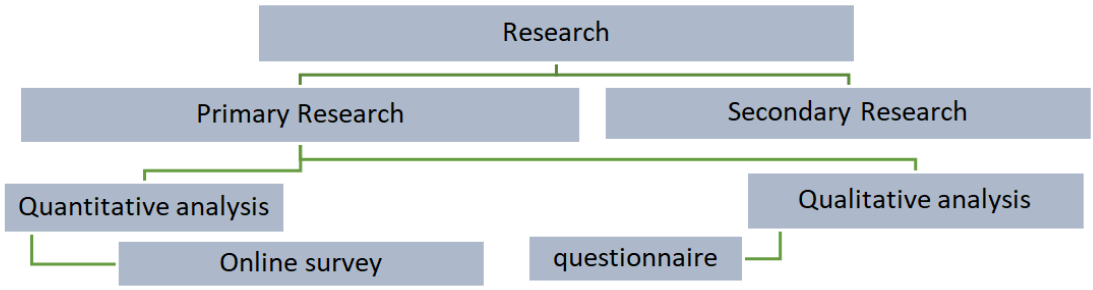

Fig1. Methods used to collect information in this study.

- ***The First Method***

served as the primary source of data and involved conducting a literature review. This involved searching for relevant academic materials from libraries, specialized journals, and online articles related to the subject of the study. In addition, researchers utilized specific keywords to narrow down the search and focused on obtaining reliable and credible references, both open-source and paid. The collected data was then condensed and summarized to facilitate faster access and comprehension of information, leading to clear and concise results. Reasonable conclusions were drawn based on the available evidence, and a comprehensive qualitative data analysis approach was employed. Following data reduction and presentation, a thorough analysis was conducted to ensure alignment with the study's objectives. The results derived from these sources are deemed highly reliable with dependable results to enhance understanding.

- ***The Second Method***

A questionnaire was distributed to reinforce the results obtained from the initial data collection method. The survey was administered to 130 engineers from the best four private companies(PCo) as internet service providers, state-owned telecommunications companies, and academic institutions in Libya. To ensure accuracy, the researchers conducted field visits to each company, dedicating one day for each organization to meet with the target participants. The respondents were required to possess a master's degree or possess a minimum of 10 years of

experience in the fields of networks, communications, and data and information security. Gender, age, and nationality were not emphasized, as the focus was on acquiring relevant information.
The study sample comprised respondents from diverse sectors, with 54.6% affiliated with academic faculty, 17.7% representing private communication and technology firms, 12.3% associated with AlmadarAljadid mobile network company, 8.5% affiliated with Libyana, a mobile network operator, and 6.9% from Libyan Post Telecommunication and Technology(LTT). And Figure 2 displays the number of participants in the questionnaire according to the companies they work for.

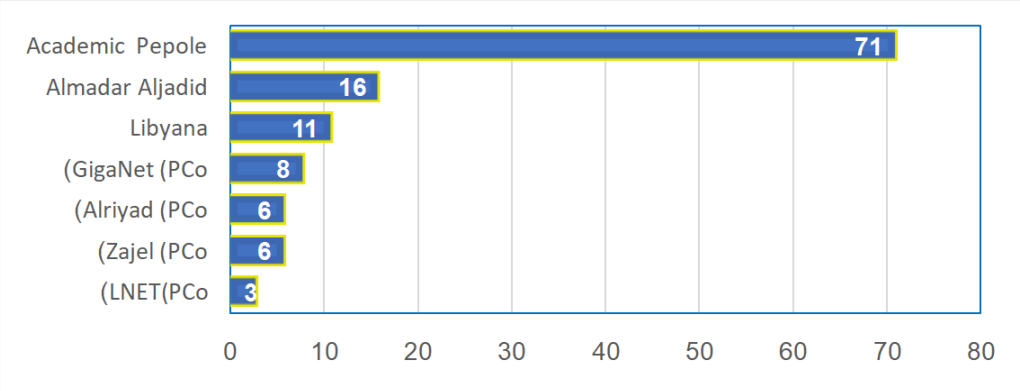

Fig 2. Shows the number of survey participants from each institution.

This heterogeneity within the participant composition allowed for a broad spectrum of perspectives on mobile networks, consequently offering invaluable insights into network security pertaining to VPN technologies.

3.1. Types of Survey Questions

A collection of inquiries was presented in the following format across 10 samples containing 25 questions, each these inquiries explore various aspects of MPLS, IPSec, and TLS protocols, encompassing their respective strengths and weaknesses in addition to their primary characteristics and ratings categorized accordingly. A final question was included at the conclusion of the questionnaire, inquiring as to the respondent's personal recommendation for a VPN protocol deemed most suitable for deployment within the mobile network industry.

3.1.1. Sample of Questions Used for the Interview and Investigation

[1] What are the advantages of MPLS?
[2] What are the disadvantages of TLS?
[3] What are the main features of TLS Encryption?
[4] What are the main features of MPLS?
[5] What are the disadvantages of using IPSec?
[6] Estimate MPLS, IPSec,TLS with respect to remote A (from 1 to 5 Ratings).
[7] Estimate IPSec, MPLS, TLS with respect to Security (from 1 to 5 Ratings).
[8] Estimate MPLS, TLS, IPSec with respect to QoS (from 1 to 5 Ratings).
[9] Estimate MPLS, IPSec, and TLS with respect to trouble protection (from 1 to 5 Ratings)
[10] Choose one of the three VPN protocols to suggest for use in a mobile network.

4. ANALYSIS PERFORMANCE OF VPN PROTOCOLS

The infrastructure of mobile networks must be carefully considered and studied, particularly in terms of security and quality, to evaluate VPN technologies and the protocols that are used in the networks. The main considerations include the ability to deliver data efficiently, support dynamic tunneling, and adapt to changing network conditions. Thus, when analyzing VPN protocols that are optimized for mobile networks, it is crucial to take into account specific security features of the network topology, scalability, site-to-site capabilities, management options, VPN client compatibility, and network placement. All these factors have been extracted and summarized in a convenient Table 1 to provide a comprehensive overview for further examination and analysis.

Table 1. Comparison table between TLS, IPSec and MPLS

	MPLS-Based VPN	**IPSec-Based VPN**	**TLS-Based VPN**
Topology Support	Full mesh	Hub and spoke, Full mesh	Point to point
Security	Limited, using labels (VPN) Protection	Strong protection, using encryption algorithms	Strong protection, using encryption algorithms
Quality of Service (QoS)	High, using Differentiated Services	Medium, using Differentiated Services	Low to medium, not specifically used for QoS
Scalability	High, supports large networks with many nodes	Medium, supports small to medium networks	Low, supports only point-to-point connections
Site-to-Site	YES	YES	YES
Management	Complex, requires specialized skills Remote access management not available	Moderate, requires some technical skills Remote access management available	Easy, widely supported by software vendors Remote access management available
Remote	NO	YES	YES
VPN Client	Limited, requires specialized hardware	Widely supported, but may require software installation	Not applicable
Place in network	Primarily used in service provider networks (core and edge routers)	Used in various types of networks (firewalls, routers, gateways)	Primarily used in web applications and e-commerce
Transparency	Partial, not all routers support the same features	Partial, VPN tunnelling can sometimes interfere with network transparency	Full, operates at the application layer and does not interfere with network transparency
Data integrity	Network layer	Packet level	Transport layer
Threat protection	Limited	Secure data transmission	Secure data transmission

5. FINDINGS

The performance analysis of these protocols helps readers choose the most appropriate option for their networking requirements. Readers can make knowledgeable decisions based on their unique needs for VPN technologies such as MPLS, IPSec, and TLS. All widely used protocols in the networks, each with its own strengths and weaknesses. When it comes to security measures, IPSec and TLS are distinguished because they ensure data protection, privacy ability, provide user authentication and authorization, as well as advanced encryption algorithms. making them preferred choices in network industries that require stringent data privacy policies. On the other hand, MPLS is found to be less secure as it transmits user information without encryption over the public internet, making it at risk of attacks and breaches.

In terms of scalability in networks, MPLS and IPSec both exhibit traits that make them suitable for accommodating increasing numbers of subscribers and expanding network capacity. In addition to elasticity and flexibility to allow the network to grow and adapt to changing demands. However, despite all the features of TLS, it is not as flexible and limits user access to the network duo to not permitting connections from external sources.

6. CONCLUSIONS

The objective of this research was to explore the different types of VPN technologies and determine the most suitable one for mobile networks. This aim was accomplished through two research methodologies (literature survey and questionnaire) on VPN protocols MPLS, TLS, and IPSec. Based on our findings, TLS and IPSec are suitable options for mobile networks. Depending on the organization's needs, either TLS or IPSec can be implemented individually. However, for security, scalability and portability in networks, it is recommended to combine both TLS and IPSec. This combination provides a comprehensive solution to ensure data privacy and protection in the mobile network industry. By leveraging the strengths of both TLS and IPSec organizations can achieve and improve security measures while maintaining the flexibility and adaptability required for networks. Therefore, utilizing a combination of TLS and IPSec is highly recommended for organizations aiming to establish an efficient VPN infrastructure in their networks.

REFERENCES

[1] Akter, H., Jahan, S., Saha, S., Faisal, R. H., & Islam, S. (2022, February). Evaluating performances of VPN tunneling protocols based on application service requirements. In Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering: TCCE 2021 (pp. 433-444). Singapore: Springer Nature Singapore.

[2] Almomani, A. (2022). Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms. Egyptian Informatics Journal, 23(4), 57-68.

[3] Alshalan, A., Pisharody, S., & Huang, D. (2015). A survey of mobile VPN technologies. IEEE Communications Surveys & Tutorials, 18(2), 1177-1196.

[4] Amaldeep, S., & Sankaran, S. (2023, May). Cross Protocol Attack on IPSec-based VPN. In 2023 11th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[5] Aung, S. T., & Thein, T. (2020, February). Comparative analysis of site-to-site layer 2 virtual private networks. In 2020 IEEE Conference on Computer Applications (ICCA) (pp. 1-5). IEEE.

[6] Bensalah, F., El Kamoun, N., &Bahnasse, A. (2017). Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec). International Journal of Computer Science and Network Security (IJCSNS), 17(3), 87

[7] Deshmukh, D., & Iyer, B. (2017, May). Design of IPSec virtual private network for remote access. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 716-719). IEEE.

[8] Dowling, B., Fischlin, M., Günther, F., &Stebila, D. (2021). A cryptographic analysis of the TLS 1.3 handshake protocol. Journal of Cryptology, 34(4), 37.

[9] Firdaouss, L., Ayoub, B., Manal, B., & Ikrame, Y. (2022). Automated VPN configuration using DevOps. Procedia Computer Science, 198, 632-637.

[10] Frahim, J., Santos, O., &Ossipov, A. (2014). Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services. Cisco Press.

[11] Gentile, A. F., Fazio, P., & Miceli, G. (2021, November). A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. In Telecom (Vol. 2, No. 4, pp. 430-445). MDPI.

[12] Guo, L., Wu, Q., Liu, S., Duan, M., Li, H., & Sun, J. (2020). Deep learning-based real-time VPN encrypted traffic identification methods. Journal of Real-Time Image Processing, 17, 103-114.

[13] Harmening, J. T. (2017). Virtual private networks. In Computer and Information Security Handbook (pp. 843-856). Morgan Kaufmann.

[14] Hauser, F., Häberle, M., Schmidt, M., & Menth, M. (2020). P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. IEEE Access, 8, 139567-139586.

[15] Ivanov, O., Ruzhentsev, V., &Oliynykov, R. (2018, October). Comparison of modern network attacks on TLS protocol. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 565-570). IEEE.

[16] Jain, A. K., Sahoo, S. R., &Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177.

[17] Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), 3587-3608..

[18] Kotuliak, I., Rybár, P., &Trúchly, P. (2011, October). Performance comparison of IPsec and TLS based VPN technologies. In 2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 217-221). IEEE.

[19] López, G., &Grampín, E. (2017, October). Scalability testing of legacy MPLS-based Virtual Private Networks. In 2017 IEEE URUCON (pp. 1-4). IEEE.

[20] Mavoungou, S., Kaddoum, G., Taha, M., & Matar, G. (2016). Survey on threats and attacks on mobile networks. IEEE Access, 4, 4543-4572.

[21] Nixon, J. S., & Amenu, M. (2022). Investigating security issues and preventive mechanisms in IPv6 deployment. International Journal, 2, 1-20.

[22] Nugroho, E. (2022). ANALISIS PENCEGAHAN SINGLE POINT OF FAILURE PADA JARINGAN SERVICE LAYER 2 VPN DENGAN METODE FAST REROUTE MPLS TRAFFIC ENGINEERING (Doctoral dissertation, InstitutTeknologi Telkom Jakarta).

[23] Pepelnjak, I., & Guichard, J. (2002). MPLS and VPN architectures (Vol. 1). Cisco press.

[24] Ridwan, M. A., Radzi, N. A. M., Wan Ahmad, W. S. H. M., Abdullah, F., Jamaludin, M. Z., & Zakaria, M. N. (2020). Recent trends in MPLS networks: technologies, applications and challenges. IET Communications, 14(2), 177-185.

[25] Santhanamahalingam, S., Alagarsamy, S., & Subramanian, K. (2022, October). A study of cloud-based VPN establishment using network function virtualization technique. In 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 627-631). IEEE.

[26] Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. TEKNOKOM, 4(1), 30-36.

[27] Sistani, A. K. R., & Patel, A. M. (2016). Design and evaluation of a virtual private network architecture for collaborating specialist users. Asia-Pacific Journal of Information Technology and Multimedia, 5(1), 15-30.

[28] Streun, F., Wanner, J., &Perrig, A. (2022). Evaluating Susceptibility of VPN Implementations to DoS Attacks Using Adversarial Testing. In Proceedings 2022 Network and Distributed System Security Symposium (p. 43). Internet Society.

[29] Sulaiman, A. B. R., &Alhafidh, O. K. S. (2014). Performance analysis of multimedia traffic over MPLS communication networks with traffic engineering. International Journal of Computer Networks and Communications Security, 2(3), 93-101.

[30] Wibowo, B., &Alaydrus, M. (2019, October). Smart Home Security Analysis Using Arduino Based Virtual Private Network. In 2019 Fourth International Conference on Informatics and Computing (ICIC) (pp. 1-4). IEEE.

[31] Yuan, X., Yao, H., Wang, J., Mai, T., &Guizani, M. (2021). Artificial intelligence empowered QoS-oriented network association for next-generation mobile networks. IEEE Transactions on Cognitive Communications and Networking, 7(3), 856-870.

[32] Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 8(4), 422-435.

AUTHORS

Mokhtar S. Alkhattali is a dedicated lecturer and the head of the Department of Computer Science at the High Institute of Science and Technology (HIST), Qaser Bin Ghashir, Libya. He earned his bachelor's degree in Electrical and Electronic Engineering from HIST. He graduated at the top of his class. In pursuit of further knowledge, he completed an MSc degree from Near East University in North Cyprus in the computer information systems field with distinction in 2016. His research work on voice recognition. Interest in networks, and developing computer applications. For more information, contact alkhtale@gmail.com.

Khawla Azwee is presently working as an lecturer assistant of Network Computing in the Department of Computer & Information Technology, at the Higher Institute of Science and Technology, Qaser Bin Ghashir, Libya. She obtained her Master of Science in Network Computing in, 2016 from Coventry University in Uk. She has more than 14 years of teaching experience. Her research interests include computer networks and information Security..For more information, contact kazwee190@gmail.com.

Mostafa Dow is a dedicated lecturer and the head of the Department of Computer Science at the High Institute of Science and Technology (HIST), Jadu, Libya. He completed an MSc degree from Near East University in North Cyprus. For more information, contact mustafa.dwo@gmail.com.