Journal of Information Systems and Informatics
Vol. 6, No. 2, June 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i2.746 Published By DRPM-UBD

Analysis of the effectiveness of VPN and PPTP Protocol in E-Link Health Report Application Using NDLC Method

Dwi Nor Amadi[1], Arief Budiman[2], Pradityo Utomo[3]*

[1,2,3]Informatics Management Departement, Merdeka Madiun University, Madiun, Indonesia
Email: [1]dwinor@unmer-madiun.ac.id, [2]arief@unmer-madiun.ac.id, [3]pradityo@unmer-madiun.ac.id

Abstract

The rapid development of computer networks and data communications has significantly impacted all government sectors in Indonesia. The Madiun Regency Health Service relies on a web-based health reporting application, E-link Health Report, to manage health information data from community health centers. However, this application is vulnerable to cyber-attacks, necessitating enhanced security measures. To address this issue, the health service implemented a Virtual Private Network (VPN) using the Point-to-Point Tunneling Protocol (PPTP) to bolster system security. The aim of this research is to analyze the effectiveness of the implemented VPN with PPTP protocol in enhancing network reliability and data transmission security. The Network Development Lifecycle (NDLC) method was employed to conduct this analysis, focusing on parameters such as network reliability and the ability to secure data transmission against cyber threats. The results demonstrate a significant improvement in both network reliability and data transmission security following the implementation of the VPN with PPTP protocol. This study provides a comprehensive comparison of network performance before and after the implementation, highlighting the effectiveness of VPNs in securing web-based health reporting applications.

Keywords: VPN, PPTP Protocol, Network Developmen lifecycle

1. INTRODUCTION

In the digital era, information and communication technology (ICT) has become indispensable, simplifying numerous activities through client-server and web-based applications. This trend is evident in Madiun Regency, particularly within the Madiun Regency Health Service, which utilizes web-based applications to manage health information reports from all Community Health Centers across the region. However, these web-based platforms have become prime targets for cyber attacks, highlighting the need for enhanced data security measures.

Previous research has demonstrated success in developing a data security method using a virtual private network (VPN) on a public network to protect data and information [1]. Despite these advancements, there is a significant gap in

understanding the effectiveness of VPNs, particularly those using the Point-to-Point Tunneling Protocol (PPTP), in providing robust data security and improving internet use efficiency within the Madiun District Health Service.

A VPN enables different private entities to share information as if they were part of the same private network, offering an isolated and secure environment that does not interfere with other data traffic. PPTP, one of several VPN protocols, is advantageous due to its inclusion in the PPP package and automatic installation on most client operating systems [2]. The Network Development Life Cycle (NDLC) method, used in this research, allows for comprehensive monitoring of network statistics and performance through its six stages: analysis, design, simulation or prototyping, implementation, monitoring, and management [3]. Wireshark, a widely used network analyzer application, provides detailed information about data captured on the network, facilitating analysis of data packet transmission and connectivity processes. This tool's capabilities are crucial in assessing the performance and security of VPN implementations [4].

While several studies have investigated VPNs and the PPTP protocol, there remains a lack of comprehensive analysis regarding their specific application within public health service networks. Research by S. Ikhwan and A. Amalina demonstrated that VPN networks using the PPTP protocol offer better Quality of Service (QoS) and higher data transfer speeds in FTP services, while the Layer 2 Tunneling Protocol (L2TP) provides better data security due to its layered encryption [5]. However, comparative studies of PPTP and L2TP protocols indicate no significant difference in overall internet performance, highlighting the need for further evaluation in specific contexts such as public health services [6], [7], [8], [9].

The aim of this research is to fill this gap by analyzing the effectiveness of the PPTP protocol in providing data security and improving internet use efficiency within the Madiun District Health Service. This study will use the NDLC method to evaluate the performance and security of the VPN implementation, employing tools such as Wireshark for detailed network analysis. By addressing this gap, the research seeks to enhance the understanding of VPN applications in public health services, contributing to more secure and efficient network infrastructures.

2. METHODS

2.1. Research Methods

The method used in this research is the Network Development Lifecycle method [10], [11], [12]. This method relies on previous development processes such as business strategy planning, application development life cycle, and data

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

distribution analysis. With this method, the aim is to have stages, steps, or process mechanisms for redesigning computer networks properly and correctly.

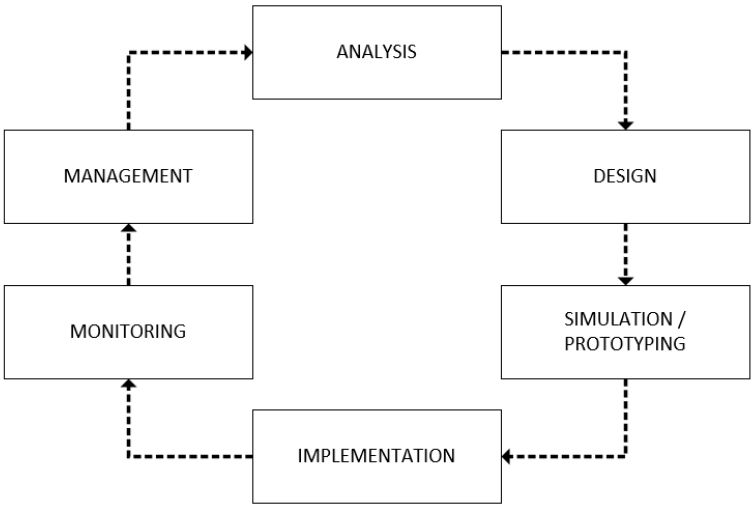

Figure 1. NDLC Method [13]

As in Figure 1, the NDLC method has six stages that are applied to analyze the effectiveness of VPN use with the PPTP protocol at the Madiun District Health Service.

1. Analysis is the initial stage for researchers to assess needs, problems, and user requirements. It involves analyzing the network topology currently existing at the Madiun District Health Service as a basis for conducting test scenarios.
2. Design from previously obtained data: At this stage, we will create a design drawing of the interconnection network topology built and studied again to find weaknesses in the existing network topology. It is hoped that this will provide a complete picture of the existing needs of the Madiun district health service
3. Simulation is the stage where the author builds a system prototype for the Madiun district health service using data from previous stages and tools to design the topology.
4. The implementation uses design specifications as input to the process to produce output that has been produced at the simulation and prototyping stages. The results are in the form of implementation instructions, which are divided into two parts: configuration and analysis at the Madiun district health service.
5. At this stage, monitoring and supervision are conducted to ensure the system's effectiveness, allowing the computer and communications network to operate according to the user's initial desires and objectives.

6. Management or regulation is a special concern, especially policy issues that need to be addressed to ensure that the system built can run well, last a long time, and maintain reliability.

3. RESULTS AND DISCUSSION

3. 1 Network Design

At this design stage, the author compares existing networks. Where the network design still needs to use VPN, there are still many weaknesses that can be mapped. The following is the network design topology that connects the e-link server at the Madiun District Health Service and the Community Health Center

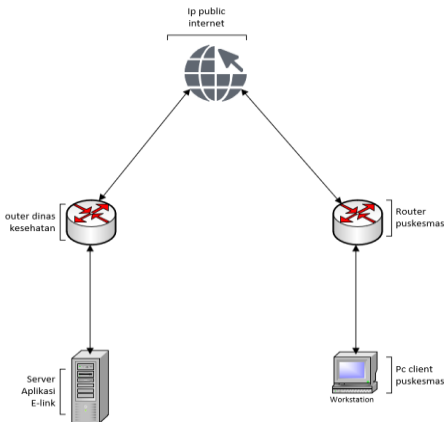

Figure 2. Network Topology Without Vpn Connection

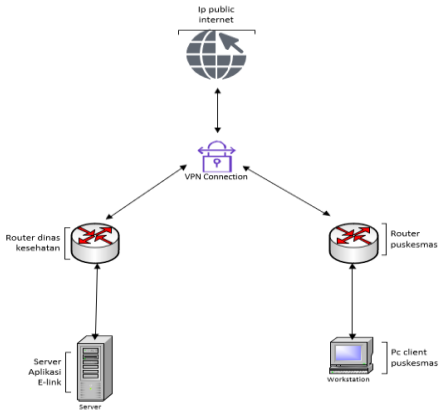

Figure 3. Network Topology with Vpn Connection

The topology on Figure 2, shows that the e-link server and health center are connected directly to the public internet IP address without adequate data security, making them vulnerable to cyber-attacks. For this reason, it is necessary to redesign the topology by utilizing VPN and the PPTP protocol. Figure 3 shows a topology that has been designed using VPN lines with the PPTP protocol. We will test this topology's speed, effectiveness, and security by comparing the two topologies.

3. 2 Testing Scenario

The research includes various test scenarios, such as connectivity testing, which involves ping time testing to measure response time and connection success. Additionally, hop testing was conducted using traceroute to analyze the path of data packets through tunnels in the VPN network. Security was a key focus, particularly in examining encryption to ensure proper packet delivery.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Connectivity testing involves comparing network performance using a VPN and a network without a VPN. Likewise, network security testing is conducted in two stages: first without VPN, and then with Tunnel VPN using Wireshark tools.

1) Connectivity testing, with VPN.

We conducted VPN tunnel connectivity testing on the Mikrotik network at the local health center to the local network of the health service's Mikrotik. Specifically, we tested the IP address of the e-link server, which is 10.10.10.10 (local IP). The testing involved using the ping command (Figure 4) to measure response time and TTL (Time to Live) parameters for sending ICMP packets. We also obtained traceroute results, as shown in Table 1.

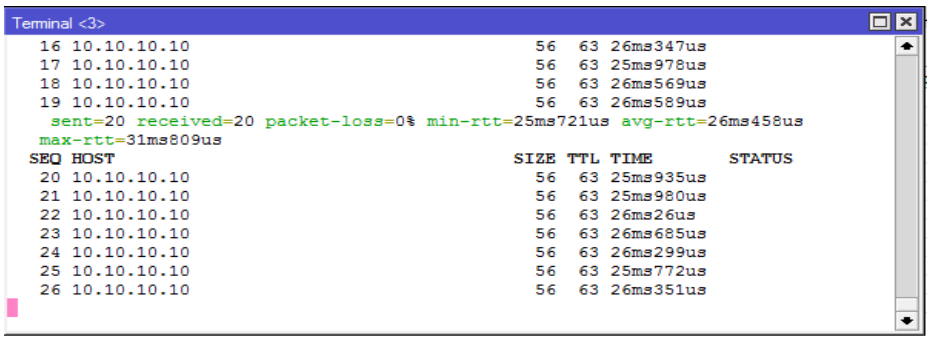

Figure 4. Tunnel VPN Network Ping Results

In Figure 4, it is evident that the response time on the VPN tunnel network ranges from 25ms to 26ms, with a TTL (time to live) of 63. The observed response time suggests that the connection performance is quite responsive. Additionally, a TTL value of 63 indicates that the packet has traversed 63 hops in the network.

Table 1. VPN tunnel Traceroute

Src Address	Dst Address	Hops Count
10.8.8.100	10.10.10.10	10.8.8.1 10.20.30.1 10.10.10.10

In Table 1, you can see the results of the VPN Tunnel traceroute test. After implementing the Tunnel VPN, the number of hops between the health center's router and the health service's router has been reduced, leading to an increase in data transfer speed. The source address originating from the local IP of the health center's router can bypass hops to the health service's router using only hops

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

10.20.30.1. This means that it only takes three hops to reach the health service router.

2) Connectivity testing without VPN

In the second connectivity test, the author attempted to perform a ping and traceroute between the local health center's Mikrotik network and the elink server's public IP 103.228.246.18. This test was conducted to measure response time, TTL (as shown in figure 5), and the number of hops taken when transferring data packets without using a VPN tunnel (as shown in Table 2).

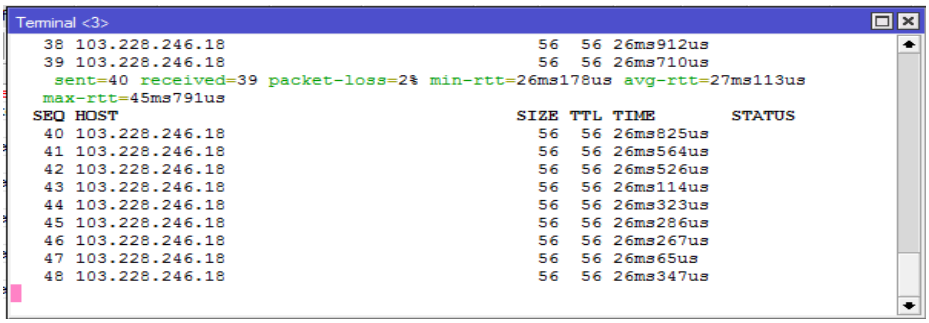

Figure 5. Tunnel VPN Network Ping Results without VPN

In Figure 5, it is explained that the response time on a network without a VPN does not show a significant difference from a network that uses a VPN. The network response time without a VPN is 26 ms. On the other hand, the TTL (Time to Live) on networks that use VPN is considered better, with a TTL value on a VPN Tunnel network reaching 63, while the TTL on a network without using a Tunnel is only 56. TTL is a value that is decremented every time a packet passes through a hop or relay point in a network. The packet will be ignored or dropped if the TTL value reaches zero. Therefore, the more hops traversed, the smaller the TTL value.

Table 2. Traceroute without VPN

Src Address	Dst Address	Hops Count
10.8.8.100	103.228.246.18	10.8.8.100
		10.106.208.1
		10.99.100.125
		10.99.100.109
		103.127.65.18
		103.144.133.113
		123.108.9.146
		103.228.247.10
		103.228.246.18

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 2 shows that when transferring data on a network without VPN from network 10.8.8.0/24 to 103.228.246.18, the number of hops is nine. This results in low reliability of data transfer on the network, as data packets are more likely to be lost when passing through multiple hops. In contrast, networks that have implemented VPN allow the same router to pass through only three hops, significantly improving reliability. The Time to Live (TTL) is explained in Figure 2, and it significantly impacts the reliability of data transfer.

3) Sniffing result without VPN

Wireshark will be a man-in-the-middle attack between the health center's Mikrotik router and the Elink server. The tool will capture every data packet that goes to the Elink server's public IP and analyze its contents to identify security gaps when sending and receiving data.

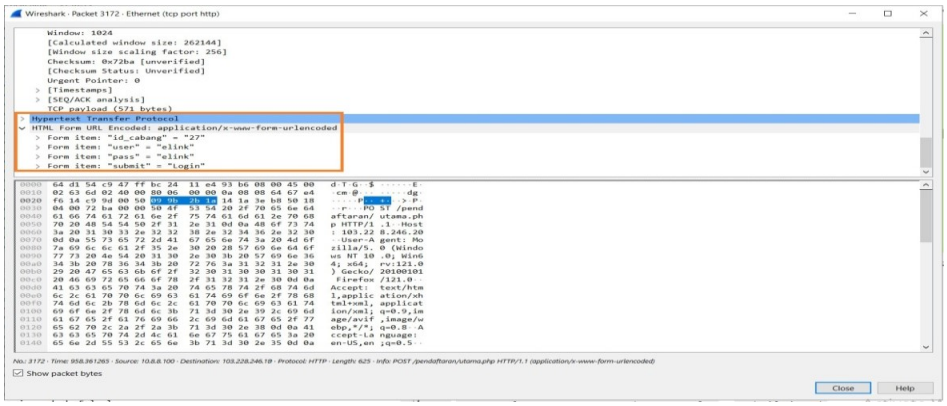

Figure 6. Sniffing Result Without VPN

Figure 6 concludes that Wireshark can identify and record HTTP POST activity between the health center proxy and the link server. It can also capture posted data, including sensitive information such as usernames and passwords. This shows that E-link servers accessed without the use of a VPN are very vulnerable to security attacks because unauthorized parties can read information that should be confidential.

4) Sniffing Result With VPN

Sniffing was also conducted to test the VPN network using the PPTP protocol. This involved capturing data packets passing between the health center's Microtik and the link server in the VPN network. The results of the security testing for the VPN with PPTP protocol are shown in Figure 7.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

In Figure 7, it can be explained that the public IP of the e-link Server used to communicate between the e-link Server and the health center's Mikrotik, cannot be directly seen in Wireshark because the Server's public IP, namely 103.228.246.18 has been encrypted using the PPTP protocol. During the communication process between the health center Client and the Server, only the source address (src address) 10.8.8.100, which is the local IP of the Mikrotik health center, is visible, and the destination address (dst address) 103.228.246.20, which is the IP of the Mikrotik PPTP server used by public health Office. Apart from that, in the information status of data packets sent and received, there is a "compressed data" status indicating that the data packets sent and received have been encrypted using PPTP. This means that the data sent and received between the health center client and the Server has gone through an encryption process, increasing the level of security and protecting the information in the data packet from unauthorized access during the communication process.

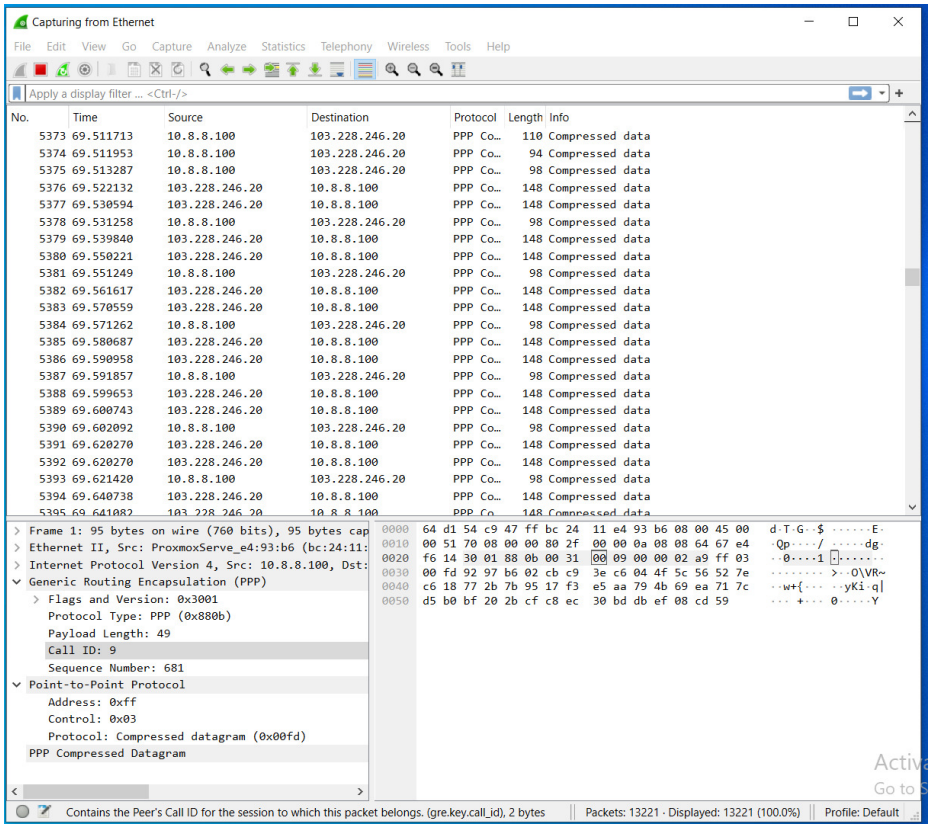

Figure 7. Sniffing Result With VPN

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

4. CONCLUSION

This research demonstrates that the implementation of a VPN in the Madiun District Health Service significantly reduces the number of hops, thereby decreasing network traffic and optimizing internet usage. The use of the PPTP protocol proves advantageous due to its ease of configuration, low cost, and broad compatibility with both desktop and mobile operating systems, while also providing reliable data security. To further enhance data security, it is recommended to incorporate a firewall to minimize potential cyber attacks. Additionally, continuous improvements in internet connectivity at the Madiun District Health Service are essential for maintaining optimal network performance and security.

REFERENCES

[1] B. A. Gumelar, G. D. S. Putra, and D. N. Amadi, "Mikrotik VPN Shielding E-Link Health Reports: Strengthening Data Security at Madiun Health Office," *J. Inf. Syst. Informatics*, vol. 5, no. 3, pp. 1194–1203, 2023, doi: 10.51519/journalisi.v5i3.524.

[2] P. Arora, P. R. Vemuganti, and P. Allani, "Comparison of VPN Protocols – IPSec , PPTP , and L2TP," vol. ECE 646, no. Fall (2021), pp. 1–45, 2021.

[3] A. Amarudin and S. D. Riskiono, "Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn)," *J. Teknoinfo*, vol. 13, no. 2, p. 100, 2019, doi: 10.33365/jti.v13i2.309.

[4] A. Averian, A. Budiono, and U. Y. K. S. Hediyanto, "Analisis dan Pengoptimalisasi Jaringan Wireless Local Area Network (WLAN) Pada PT.XYZ Dengan Menggunakan Metode Network Development Life Cycle (NDLC)," *eProceedings Eng.*, vol. 10, no. 2, pp. 1325–1330, 2023.

[5] I. Ubaedila, O. Nurdiawan, Y. A. Wijaya, and J. Sidik, "Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark," *INFORMATICS Educ. Prof. J. Informatics*, vol. 6, no. 1, p. 95, 2022, doi: 10.51211/itbi.v6i1.1697.

[6] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP," *J. Infotel*, vol. 9, no. 3, 2017, doi: 10.20895/infotel.v9i3.274.

[7] A. Kurniawan, "Analisis Performansi Remote Acces VPN Menggunakan PPTP dan L2TP Untuk Kebutuhan Work From Home (WFH) bagi Karyawan PT Dunia Makmur Jaya," *J. Pendidik. Tambusai*, vol. 7, no. 2, pp. 7378–7389, 2023.

[8] R. F. Syarif and I. A. Sobari, "Implementasi Virtual Private Network (VPN) menggunakan Metode PPTP pada PT. Sinar Quality Internusa," *J. Pendidik. Tambusai*, vol. 6, no. 2, pp. 15165–15184, 2022.

[9] Z. zul and J. Jackie, "Analisa dan Penerapan Pencadangan Pusat Data Antar Site dengan Teknologi VPN," *J. Inf. Syst. Technol.*, vol. 3, no. 2, pp. 257–269, 2022, doi: 10.37253/joint.v3i2.6764.

[10] R. A. Putra, H. Supendar, and R. Fahlapi, "Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik," *J. Komput. Antart.*, vol. 1, p. 2023, 2023.

[11] D. Lusi, Y. Suban Belutowe, U. I. Kupang Jl Perintis Kemerdekaan, K. Putih, and K. Kupang, "Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Ndlc (Network Development Life Cycle) Pada Kantor Balai Pelaksanaan Jalan Nasional Ntt," *J. Teknol. Inf.*, vol. 7, no. 1, 2023.

[12] Y. Mulyanto and S. B. Prakoso, "Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (Ndlc)," *J. Inform. Teknol. dan Sains*, vol. 2, no. 4, pp. 223–233, 2020, doi: 10.51401/jinteks.v2i4.825.

[13] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *Mhs. Bina Insa.*, vol. 4, no. 1, pp. 1–10, 2019.