Security: Research Article

Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)

Aliyyah Rosyidah[1], Jumadi Mabe Parenreng[2*]

[1,2]Department of Computer Engineering, Universitas Negeri Makassar, Makassar 90222, South of Sulawesi, Indonesia
*Corresponding author: jparenreng@unm.ac.id

Abstract:
The network security system is continuously advancing alongside technological developments. VPNs, which utilize open networks, aim to provide security by leveraging IPSec to transmit private data through L2TP tunneling strategy from the server to the branch computer/client and vice versa. Conversely, it can also lead to poor security practices. VPNs are implemented using the layer 2 IPSec tunneling protocol with two MikroTik devices. Testing is conducted to assess the security and speed of the network using the command line and MikroTik Winbox, where the server monitors packet delays to determine the improvement in network security quality. This research has identified several weaknesses in implementing this VPN protocol, namely the need for caution regarding the security of transmitted data to prevent misuse by the VPN provider.

Keywords: VPN, Network Security, L2TP or IPSec, Mikrotik Winbox, Security System

Citation: A.Rosyidah & J.M.Parenreng" Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)". *Iota,* **2023**, ISSN 2774-4353, Vol.03, 03. https://doi.org/10.31763/iota.v3i3.613

Academic Editor : Adi, P.D.P

Received : June, 04 2023

Accepted : July, 03 2023

Published : July, 06 2023

1. INTRODUCTION

It is crucial to establish an alternative pathway by utilizing and implementing the Virtual Private Network (VPN) protocol while ensuring the security level of the transmitted data[1]. The increasing demand for network security in the complex digital era is evident. In network environments connected to the Internet, security threats such as hacking, viruses, malware, and other cyber attacks are on the rise, posing a risk to the integrity and confidentiality of data transmitted through the network[2]. Many organizations and companies employ network security technologies such as IPSec and VPN to address this issue. IPSec technology is a security protocol used to secure network connections between two points, while VPN technology allows users to access private networks through public internet connections[3]. However, despite the enhanced network security provided by these technologies, it is still necessary to conduct a security analysis on the network being used to determine the level of network security achieved[4]. Therefore, this journal aims to perform a network security analysis using IPSec and VPN technologies, conduct experiments on network configurations to establish connections between the server and client and determine the level of network security achieved.

A VPN network is a technology that enables the creation of a private information network within a public network by implementing authentication and encryption, thus limiting access to specific parties. On the other hand, IPSec is a set of protocols that provide security for communication at the IP layer[5].

This alternative pathway security also includes a network security system that encrypts all data transmitted. Based on the conducted experiments and analysis, it has been found that the Virtual Private Network (VPN) protocol is highly suitable for implementation[1]. Utilizing the Internet for communication offers advantages such as convenience, speed, and cost reduction for companies. However, the Internet also poses security risks due to its openness and accessibility to everyone, making it insecure for transmitting confidential information[2]. VPN data serves as a network security solution by creating a tunnel that allows a trusted network to connect with external networks over the Internet [4]. The use of L2TP (Layer 2 Tunneling Protocol) / IPSec (IP Security) protocol provides dual-layer protection for data transmission.

The protection is achieved through L2TP authentication and IPSec encryption, and it also acquires a virtual IP address within the same subnet as the internal network[5]. In a VPN, each device has the same IPSec configuration, enabling secure traffic flow between sources and destinations. This research utilizes Quality of Service (QoS) parameters on a network connected through L2TP VPN with IPSec protocol. The study will evaluate the quality of service provided by the network based on the measured parameters to assess if the service quality is adequately met[6]. MikroTik offers Layer 2 Tunneling Protocol (L2TP) as One of the VPN services. Specifically, utilizing L2TP can facilitate secure data exchange and enhance security settings between multiple systems through tunnels traversing the Internet [7].

Designing a VPN network with IPsec technology can be implemented on MikroTik Routerboard. MikroTik Routerboard is an operating system for routers that enables comprehensive management and control of network activities, including bandwidth management, routing, firewall configurations, and more. Using MikroTik Routerboard, you can configure and deploy a VPN network with IPsec for secure communication and data transmission across the network[8]. By establishing a VPN network, access rights can be granted exclusively to individuals responsible for maintaining campus data. This ensures that only authorized personnel with valid can securely access and manage network resources, thereby maintaining confidentiality and integrity and limiting access to qualified individuals only[10].

Using a VPN makes it possible to establish a virtual connection between devices outside the local network and the local network itself, simulating a physical connection. Network infrastructure refers to the hardware and software components that connect computers and devices within a network, including the TCP/IP protocol. Network security plays a crucial role in safeguarding data from unauthorized access, employing firewalls and data encryption measures. Furthermore, troubleshooting is essential for resolving various network issues. VPN technology enables users to access private networks through public networks like the Internet [20].

Network security is crucial for any computer network. If Vulnerabilities in a computer network are not adequately protected and guarded, they can lead to significant losses. Breaches in network security can result in unauthorized access, data breaches, loss of sensitive information, disruption of services, financial losses, damage to reputation, and legal implications. Therefore, it is essential to implement robust security measures such as firewalls, intrusion detection systems, encryption, access controls, and regular security audits to mitigate risks and safeguard the network from potential threats. Proactive network security practices are vital for maintaining network resources' integrity, confidentiality, and availability [20].

Indeed, network security has become a primary focus in computer networking in recent years due to the increasing threats and attacks from the Internet. To maintain and enhance the protection provided to employees, network technicians continuously monitor network traffic and the condition of network devices. By monitoring data traffic, technicians can identify suspicious or malicious activities, detect potential security breaches, and take appropriate measures to mitigate risks. Additionally, monitoring the condition of network devices helps ensure their proper functioning, timely detection of vulnerabilities or malfunctions, and prompt remediation. Regular monitoring is crucial in maintaining a secure network environment and minimizing the impact of security incidents[21].

The research methodology involves conducting a network security analysis using Internet Protocol Security (IPsec) and Virtual Private Network (VPN). The research process follows a specific flow, starting with the planning phase, where the researcher develops a research design to analyze network security using IPsec and VPN. Next is the system architecture design phase, where the researcher creates the architecture for the VPN and IPsec systems to understand the workflow. Then, in the observation phase, the researcher observes the research by measuring Quality of Service (QoS) parameters to evaluate the network's ability to provide good service, including bandwidth provisioning, jitter, and delay management. The researcher also observes the network's condition after connecting to the VPN. In the data analysis phase, the researcher analyzes the collected data after conducting tests using IPsec and VPN methods to assess network security. Finally, the conclusion phase involves evaluating the entire research process and documenting the findings in a report based on the observed data.

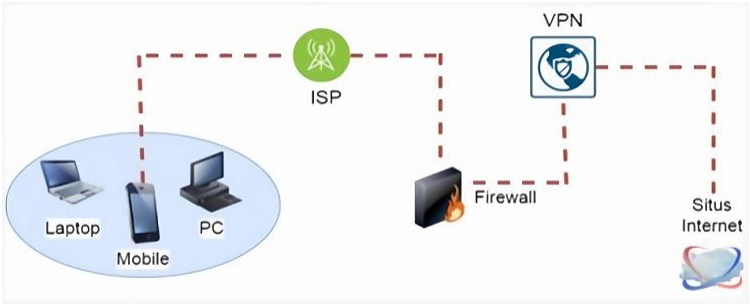

Figure 1. VPN System Architecture

In Figure 2, when users access websites through communication devices such as laptops, mobile devices, and PCs. The user's request is then sent to the Internet Service Provider (ISP). The user's internet traffic passes through a firewall, a security system that monitors and controls network traffic to enhance privacy and security; internet traffic is directed through a virtual private network (VPN). The VPN encrypts the user's data, protecting personal information and securing the connection from third-party attacks or surveillance. After passing through the VPN stage, the internet traffic is sent to the accessed website. Therefore, by using a virtual private network, users can access websites more securely and maintain their privacy by encrypting the data transmitted through the network.

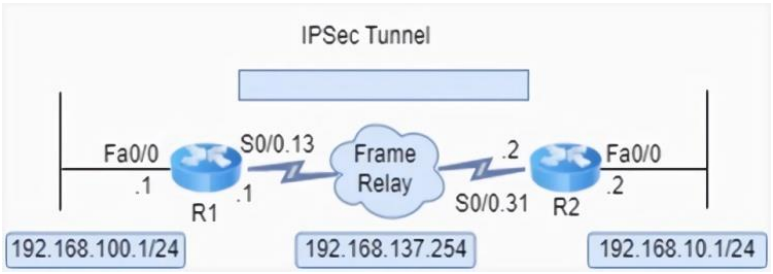

Figure 2. System Architecture of IPSec

In Figure 3, IPSec Tunnel is used for securing packets transmitted over the network. Suppose two IP addresses, the server IP 192.168.100.1/24 and the client IP 192.168.10.1/24, want to connect through a frame relay network. An IPSec Tunnel is established between the two IP addresses to ensure communication security, as shown in Figure 3. When a packet is sent from IP 192.168.10.1/24, it will pass through the router and connect to the frame relay network, but the client IP is encrypted to protect the packet's contents from unauthorized access. On the receiving side, the destination IP 192.168.100.1/24, the encrypted packet transmitted through the router, is decrypted to read using the IPSec Tunnel; the packets transmitted between these two IP addresses remain secure and cannot be accessed by unauthorized third parties.

2. RESULT AND DISCUSSION

Furthermore, this Network system will be designed and planned to build a network using L2TP/IPSec features to establish an excellent secure private connection between the server and the client. The security system implemented on both the server and client involved using VPN with the L2TP/IPSec method for network security. This implementation helps prevent data leakage to unauthorized parties since VPN operates on a private network, ensuring the confidentiality of server and client data. We conducted tests on the implementation of L2TP/IPSec VPN on MikroTik routers using the PPP menu to establish a connection between the networks on the server and client, provided that each location has an internet connection. Once these two local networks are connected, users of the server and client can access the Internet at speed using VPN without any filtering or firewall restrictions. This implementation using VPN helps assess the security of our data, ensuring its confidentiality and preventing unauthorized access from external sources.

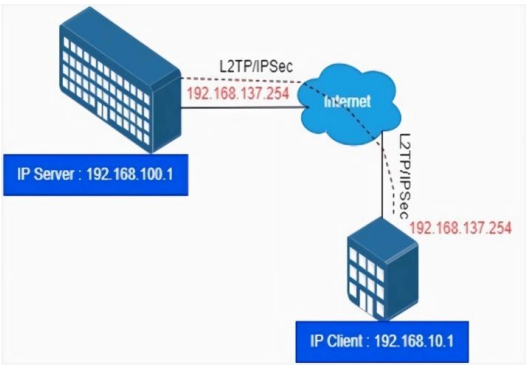

Figure 3. Network Topology

Table 1. Devices, IP Address, and Subnet

No	Devices	IP Address	Subnet
1	ISP (Server)	192.168.100.1	255.255.255.0
2	ISP (Client)	192.168.10.1	255.255.255.0
3	File Server	192.168.137.254	255.255.255.0

Table 1 explicitly states the IP Address on the type of device, namely ISP Server, ISP Client, and File Server, each expressed by IP Address and Subnet. Moreover, the analysis of this network testing will first compare the client's computer network before and after implementing VPN. This testing will utilize Virtualbox, MikroTik, and Winbox application simulators.

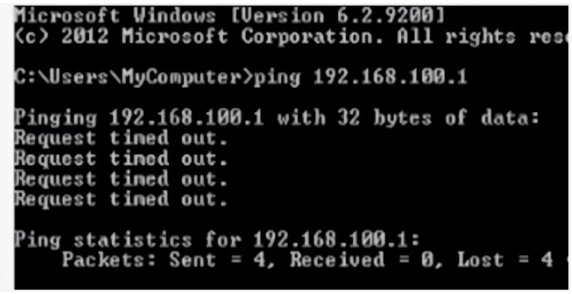

Figure 4. Ping Command to the gateway on the server and client before connecting to the VPN

Moreover, the Initial network testing in Figure 4 involved ping commands to the gateway on the Server and Client before establishing a connection with the VPN. The IP address of the server is 192.168.100.1, and the IP address of the client is 192.168.10.2, which was tested before the connection of the Server and Client IPs. However, Figure 5 shows that the requests resulted in a timeout because the IP configuration for the Server (192.168.100.1) and the Client (192.168.10.2) has not been configured to establish the VPN connection. Therefore, the initial network testing aimed at achieving the intended outcome of timeout requests.

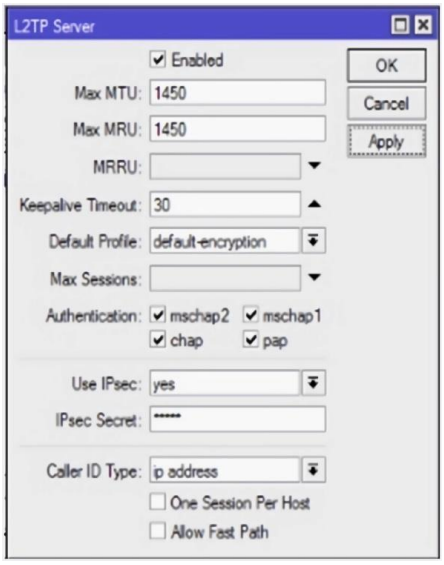

Figure 5. To enable the L2TP server on the Mikrotik router board

The initial step taken for configuration in supporting software using Winbox, then select IP > Address > Add Address List > Next, create two IP addresses. The first is the server IP, which is 192.168.100.1, and the second is the client IP, which is 192.168.10.1. Afterward, go to the L2TP server menu, check the enable option, then click OK, as shown in Figure 5.

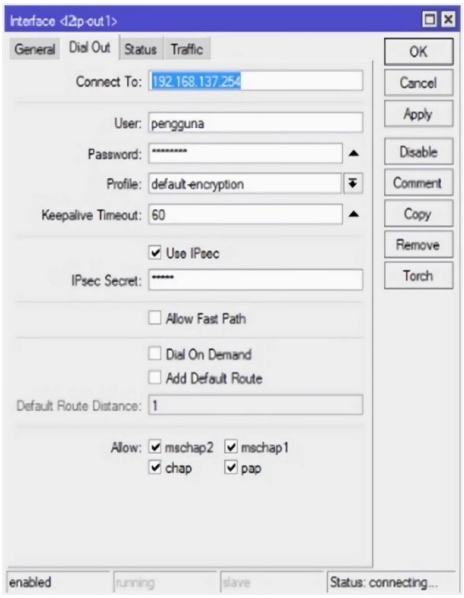

Figure 6. To connect the configuration to the server IP and client IP

The next step is to go to the PPP secret menu for the user and create a username and password for the login. Then, go to the <l2tp out1> interface and connect the IP accessed using the Internet, as shown in Figure 6.

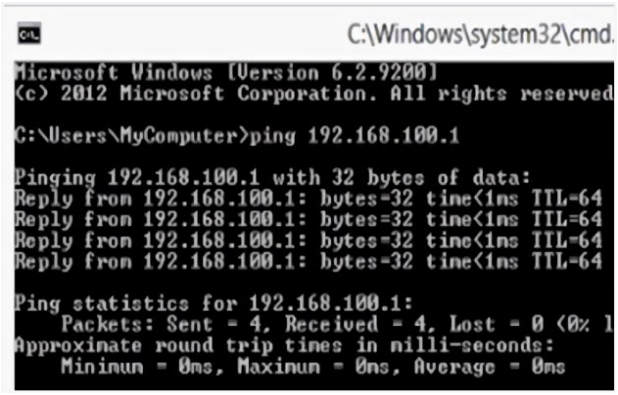

Figure 7. Ping Command to a gateway on the server after establishing a VPN connection

Furthermore, in Figure 7, The final network testing involved the ping command to the gateway on the server and client after establishing the VPN connection. The server's IP is 192.168.100.1, and the client's IP is 192.168.10.1. In the testing, we performed ping commands from both the server and client to the gateway of the local server network. The results showed success or a TTL (Time to Live) value, indicating that the IP server 192.168.100.1 and IP client 192.168.10.1 were successfully connected to the local server network.

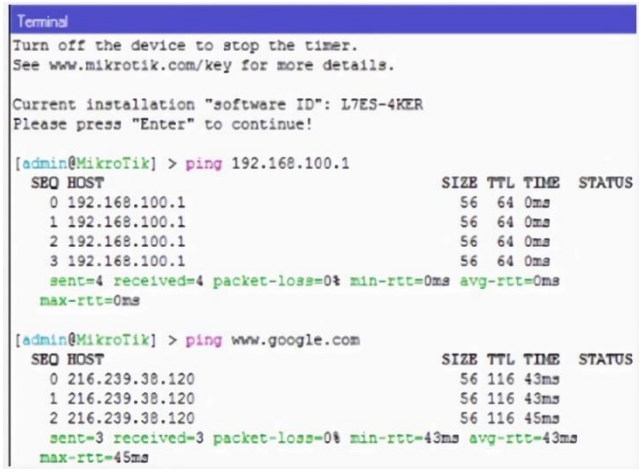

Figure 8. The checking result in the winbox terminal shows that the IP server is successfully connected

The result of the network testing in the Winbox terminal after the local network of the server and client are connected, as shown in Figure 8 when testing the IP Server 192.168.100.1. IP Client 192.168.10.1, the result is a successful TTL, indicating that the configuration has been successfully implemented and can connect to the Internet using the IP on the server. However, the author cannot guarantee the network's security using Internet Protocol Security (IPSec), as if the password is leaked, third parties can access the network.

Table 2. Analysis Result

No	Analysis Aspect	Description
1	Advantages of Implementing an IPSec VPN	The advantages of implementing an IPSec-based VPN, particularly in ensuring data security over a public network.
2	Client-Side Security	Security issues, such as credential leaks or malware attacks, may arise on the client side when using a VPN. The importance of training and education for clients to enhance awareness of good network security practices.
3	Server-Side Security	The importance of security on the server side, including security issues related to the VPN server itself, such as inadequate maintenance and updates, as well as the security of other networks connected to the VPN. Therefore, testing is crucial to ensure the security of the VPN network and protect against attacks.
4	No Perfect Security Solution	A VPN is not a perfect security solution and needs to be complemented with good network security practices, continuous testing, and monitoring.
5	Evaluation and Configuration Updates	The importance of evaluating and updating the configuration and policies of the VPN to address emerging security issues.
6	Implementation of IPSec VPN and Comprehensive Security Practices	Organizations can enhance the overall security of their network infrastructure and protect sensitive data from unauthorized access.
7	Network Security as a Continuous Process	The security process requires constant attention and adaptation to address emerging threats. Emphasizing the importance of regular audits and security assessments to maintain network security.
8	Differences Before and After VPN Testing	VPN testing using Winbox. Before the testing, there was no connection between the server and the client, as indicated by Figure 5 showing Request Time Out (RTO). After successfully configuring and establishing the VPN connection, Figure 9 shows that the TTL indicates the IP server and IP client are connected, and communication is established.

5. CONCLUSION

Implementing a Virtual Private Network (VPN) and IPSec/L2TP network has successfully connected two networks, namely the server and client. The presence of VPN and IPSec establishes a secure communication pathway for data transmission, thanks to the tunneling capabilities of the VPN. This tunneling feature provides a dedicated path to access the local network, ensuring data communication security. Data security is guaranteed through the IPSec protocol, which encrypts inbound and outbound data to conceal information transmitted by unauthorized parties. This encryption mechanism ensures the confidentiality and integrity of the data, providing a robust layer of security to protect sensitive information.

However, specific vulnerabilities and risks are still associated with implementing a Virtual Private Network (VPN). It is essential to exercise caution and remain vigilant to protect data from potential misuse or unauthorized access by the VPN provider.

ACKNOWLEDGMENTS

Thanks to the Department of Computer Engineering, Universitas Negeri Makassar, for the guidance of the lecturers and the cooperation of fellow students, who have supported this research so that it can be completed well. Hopefully, this paper can be developed in more detail.

AUTHOR CONTRIBUTIONS

Conceptualization; Aliyyah Rosyidah [A.R], Jumadi Mabe Parenreng [J.M.P], Methodology; [A.R],[J.M.P], validation; [A.R],[J.M.P], formal analysis; [A.R],[J.M.P], investigation; [A.R],[J.M.P], data curation; [A.R],[J.M.P], writing—original draft preparation; [A.R],[J.M.P], writing—review and editing; [A.R],[J.M.P], visualization; [A.R],[J.M.P], supervision project administration; [A.R],[J.M.P], funding acquisition; [A.R],[J.M.P], have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. Amarudin, A., & Riskiono, S. D. (2019). Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn). *Jurnal Teknoinfo*, *13*(2), 100. https://doi.org/10.33365/jti.v13i2.309
2. Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI : Jurnal Sains Dan Manajemen*, *8*(1), 128 139. https://doi.org/10.31294/evolusi.v8i1.7658
3. Hauser, F., Häberle, M., Pascasarjana, A. M., Mahasiswa, A., & Schmidt, M. (2020). *P4-IPsec : VPN Situs-ke-Situs dan Host-ke-Situs Dengan IPsec di SDN Berbasis P4*. *8*, 139567–139586.
4. Sumarna, S., & Maulana, A. (2021). Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta. *EXPERT: Jurnal Manajemen Sistem Informasi Dan Teknologi*, *11*(2), 90.https://doi.org/10.36448/expert.v11i2.1829

5. Pratama, H., & Puspitasari, N. F. (2021). Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. *Creative Information Technology Journal*, *7*(1), 51.https://doi.org/10.24076/citec.2020v7i1.253
6. Olvia, D., & Zulhendra, Z. (2021). Analisis Quality of Service (QoS) Jaringan Virtual Private Network (VPN) dengan menggunakan protokol IPSec (Studi Kasus : SMK Negeri 3 Pariaman). *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, *9*(1), 92. https://doi.org/10.24036/voteteknika.v9i1.111056
7. Putra, U., Yptk, I., & Email, C. (2022). *PROTOCOL AND IPSEC METHODS AS NETWORK*. 754–760.
8. Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan Virtual Private Network IP Security Router Mikrotik. *Jurnal PROSISKO*, *7*(2), 150–164.
9. Maryanto, M., Maisyaroh, M., & Santoso, B. (2018). Metode Internet Protocol Security (IPSec) Dengan VirtualPrivate
   Network (VPN) Untuk Komunikasi Data. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *6*(2), 179 188.https://doi.org/10.33558/piksel.v6i2.1508
10. Olvia, D., & Zulhendra, Z. (2021). Analisis Quality of Service (QoS) Jaringan Virtual Private Network (VPN) dengan
    menggunakan protokol IPSec (Studi Kasus : SMK Negeri 3 Pariaman). *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, *9*(1), 92. https://doi.org/10.24036/voteteknika.v9i1.111056
11. Ekawati, I., & Irwan, D. (2021). Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik. *JREC(Journal of Electrical and Electronics)*, *9*(1), 41–48. https://doi.org/10.33558/jrec.v9i1.3110
12. Dahnial, D. (2019). Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik. *Jurnal Ilmiah Informatika Global*, *10*(2), 107–113. https://doi.org/10.36982/jig.v10i2.858
13. Hariyadi, D., Jinan, M. R., Bayuaji, N. S., & Hasan, A. S. (2019). Analisis Jaringan Pada Aplikasi Pengamanan Akses Internet. *Cyber Security Dan Forensik Digital*, *2*(1), 16–23. https://doi.org/10.14421/csecurity.2019.2.1.1416
14. Ningrat, A. P. S. N., & Yasa, N. N. K. (2022). *The 2nd Conference on Management , Business , Innovation , Education , and Social Science (CoMBInES) Taichung , Taiwan 3-6 March , 2022 AWARENESS , AND BRAND IMAGE ON PURCHASE INTENTION OF LOCAL The 2nd Conference on Management , Business , Innovation ,*. 289–303.
15. Subekti, R. (2020). *Implementasi Virtual Private Network (Vpn) Sebagai Solusi Security Selama Work From Home*. *1*(1), 57–65.
16. Permana, A. H. M., Widiyasono, N., & Rahmatulloh, A. (2020). Perbandingan Algoritma Pada Teknologi Virtual Private Network (VPN) IPSec Terhadap Kecepatan Transfer Data. *SISTEMASI: Jurnal Sistem Informasi*, *9*(2), 259273.
17. Andriani, R., Sa'di, A., & Putra, A. D. (2022). Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol. *Building of Informatics, Technology and Science (BITS)*, *4*(1), 184–190. https://doi.org/10.47065/bits.v4i1.1611
18. Ariyadi, T., & Prabowo, M. A. (2021). Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security. *INOVTEK Polbeng - Seri Informatika*, *6*(1), 80. https://doi.org/10.35314/isi.v6i1.1698
19. Suryantoro, H., Sopian, A., & Dartono, D. (2021). Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan Vpn-Ip Berbasis Ipsec. *Jeis: Jurnal Elektro Dan Informatika Swadharma*, *1*(1), 1–7. https://doi.org/10.56486/jeis.vol1no1.64

20. Phang, V., & Setyaningsih, E. (2021). Perancangan Virtual Private Network Dengan Protokol PPTP Menggunakan MikroTik Untuk Kebutuhan Remote Access. *Jurnal POLEKTRO: Jurnal Power Elektronik*, *10*(2), 2021.
21. Gustiawan, M., & Rismayadi, A. A. (2022). Remote Access Virtual Private Network Menggunakan Layer 2 Tunneling Protocol Berbasis Mikrotik. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *5*(4), 674–684. https://doi.org/10.32672/jnkti.v5i4.4612