e-JURNAL PENYELIDIKAN DAN INOVASI
ISLAMIC INNOVATION CENTER FOR TECHNOLOGY, UIS
https://ejpi.uis.edu.my
e-ISSN 2289-7909

VOL. 12 NO. 2, SPECIAL EDITION, (SEPTEMBER, 2025): page 1-14
DOI: 10.53840/ejpi.v12i2.276

Received: May 14, 2025 | Accepted: July 7, 2025 | Published: September 19, 2025

Simulation L2TP/IPSEC VPN Site-to-Site on Mikrotik Using GNS Emulator

Simulasi L2TP/IPSEC VPN Tapak-ke-Tapak Pada Mikrotik Menggunakan GNS Emulator

Hafizatun Muawiyah[1], Ade Hendri Hendrawan[2], Yuggo Afrianto[3]
[1,2,3] Informatics Engineering, Faculty of Technology & Science, Universitas Ibn Khaldun Bogor
Jl. Sholeh Iskandar, RT.01/RW.10, Kedungbadak, Kec.
Email: [1]fizamuawiyah14@gmail.com, [2]adehendri@uika-bogor.ac.id, [3]yuggo@uika-bogor.ac.id

ABSTRACT

The use and analysis of IPSec Site to Site VPN simulation with MikroTik devices in a GNS3 emulation environment is discussed in this study. The main objective of this study is to use GNS3 emulators to simulate and execute IPSec site-to-site connections. The L2TP VPN technique is recommended as a way to run an IPSec site-to-site connection. The research methodology consists of four stages, starting with preparation, which involves the installation of Winbox, GNS3, and virtual machines. Network topology and process diagrams are then included in the design, and network configurations, L2TP VPN, and IPSec are included in the implementation. The test is completed by presenting the results of the IPSec L2TP VPN test.

Keywords: VPN; IPSec; L2TP; Mikrotik; GNS3

INTRODUCTION

One of the biggest concerns for companies and organizations in the modern digital environment is data and communication security (Munawar & Putri, 2020). Security for the network has become a necessity. Virtual Private Networks (VPNs) allow secure data exchange over public networks, including the Internet. Virtual network services known as virtual private networks (VPNs) are one option to protect sensitive or confidential data. VPN users can provide access to local networks, provide remote access to devices connected to the network, and have the ability to view and retrieve data from within the network itself (Nurdi Afrianto et al., 2024). In a business or organizational environment with multiple separate locations, issues arise such as how to provide site-to-site access, how to configure each router, and how to access the VPN through each client. In addition, a site-to-site connection requires a method to support the implementation of IPSec VPN (Sari, Sulistiyono, & Kemala, 2020). MikroTik is a Linux-based router operating system that provides advanced networking features, including the ability to configure IPSec VPN with L2TP (Ardianto & Akbar, 2017).

By using network emulators such as GNS3 (Graphical Network Simulator 3), network administrators can simulate and test IPSec VPN configurations in MikroTik without disrupting the actual production environment (Amarudin & Ulum, 2018). Because PPTP uses weaker encryption that makes it open to

attack, L2TP offers the advantage of protecting data using IPSec encryption. More than PPTP, L2TP can bypass firewalls and NAT (Network Address Translation). This study aims to simulate and analyze the configuration of IPSec VPN site-to-site with L2TP on MikroTik using a GNS3 emulator (Prasetyo, Budiman, & Putra, 2019). The main advantage of GNS3 is its ability to accurately describe and simulate complex network topologies, including IPsec VPN configuration with L2TP on MikroTik devices. With GNS3, users can try out various network scenarios and test security configurations such as IPsec and L2TP virtually without the need for physical hardware, saving costs and facilitating the learning or troubleshooting process. This is especially beneficial for networking professionals and students who want to deepen their knowledge of VPNs and network security. However, the downside of GNS3 is the relatively large size of the application, which can overwhelm the user's device and require high computer specifications to run it optimally (Aprillianto & Pamungkas, 2023). A deeper understanding of this procedure will be possible thanks to this simulation. Configure IPSec VPN with L2TP in the MikroTik environment, as well as help identify challenges and solutions that may be encountered in the actual implementation (Jayanto, 2019). This research was conducted using information from previous publications to develop previous approaches and draw interest in this issue to provide more effective and secure network security solutions.

PROBLEM STATEMENT

Based on the introduction, the formulation of the problems in this study is:

1. How to implement Mikrotik IPSec site-to-site access and configuration?
2. What methods are used to run IPSec site to site?

LITERATURE REVIEW

Broadly speaking, this research will later create a security system on a virtual private network using microtik routers.

Table 1: Literature review

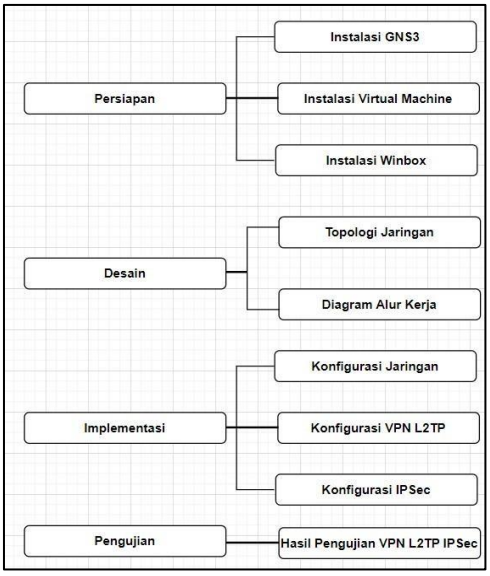
No	Author Name, Journal Title, Journal Name and Year	Intention	Conclusion
1	Bayu Gagat Rahino & Atang Susila. Implementation of Mikrotik VPN network (L2TP / IPSec) for remote access as security during Work From Home. Journal of Computer Science and Science. 2022.	The research was to collect data through surveys and interviews, then analyze existing networks and the need for design support network.	L2TP/IPSec VPNs are successfully used to connect employees with company systems through encryption and decryption that work well.
2	Ayu Purnama Sari, Sulistiyono, Naga Kemala. "Network Design Virtual Private Network IP Security-Based Using A Mikrotik Router". Prosisko Journal. 2020	Design secure communication lines using IPSec VPN.	IPSec provides a line of communication of personal data via WiFi or public hotspots by tunneling to the local network.

No	Author Name, Journal Title, Journal Name and Year	Intention	Conclusion
3	Fitri Sjafrina, Pipit Dewi Arnesia, and Arif Aqim. "Design and Build a VPN-Based Network IPSEC Using Mikrotik Routerboard". International" National Seminar on Information and Communication Technology STIK (SeNTIK). 2019.	Hands-on implementation and configuration using MikroTik RouterBoard.	IPSec VPN was successfully tested with a remote connection, supports high bandwidth up to 100 Mbps, and authentication works well.
4	São Paulo Wicaksana, Febri Hadi, Aulia Fitrul Hadi. "Designing VPN Server Implementation Using L2TP Protocol". Komtek Info Journal. 2021.	Design and implementation of VPN servers with L2TP and IPSec protocols.	IPSec improves network security with firewall and proxy support; ensure the confidentiality of information flow.
5	Maryanto, Maisyaro, Budi Sentoso. "The internet method Protocol security (IPSec) with a virtual private network (VPN) for data communication". Journal Computer Science Research. 2018.	Build an internal VPN network between SOEs (PT PPA and PT Penas).	IPSec VPN as a secure, cheap, and efficient solution for communication and integration of corporate systems over public networks.

METHODOLOGY

There are four steps in the research techniques used in this study: planning, design, implementation, and testing. The research approach is illustrated in Figure 1.

Figure 1: Stages of research method



This diagram illustrates the systematic flow from start to finish in a VPN network simulation research using GNS3 and MikroTik, which is suitable for illustrating virtual real-world implementations.

1. Preparation

This stage focuses on setting up the initial setup so that the simulation environment is ready to use.

- **GNS3 Installation**
  Install GNS3 software as the main network emulator used to build and simulate virtual networks.
- **Virtual Machine (VM) Installation**
  Set up VMs as add-ons to run network operating systems, such as MikroTik RouterOS or other systems in GNS3.
- **Winbox Installation**
  Install Winbox as a graphical interface to manage and configure MikroTik devices.

2. Design

This stage involves planning and designing the network scenario to be simulated.

- **Network Topology**
  Designing the structure and relationships between devices in a network, including routers, PCs, and internet connections.
- **Workflow Diagram**
  Create a process diagram or sequence of work steps that illustrates how IPSec and L2TP VPNs will be configured and tested.

3. Implementation

At this stage, the real configuration is done as planned.

- Network Configuration: Sets IP addresses, routing, and basic settings of communication between devices in GNS3.
- L2TP VPN configuration: Configure a VPN connection using the L2TP protocol as a site-to-site alternative.
- IPSec configuration: Configuring a VPN connection using the IPSec security protocol to protect traffic between networks.

4. Testing

The final stage to verify the success of the configuration.

- **L2TP and IPSec VPN Test Results**

Testing the VPN connection with methods such as *ping* to ensure that two networks can communicate with each other securely over the VPN. These results are used to assess whether the configuration is successful and stable.

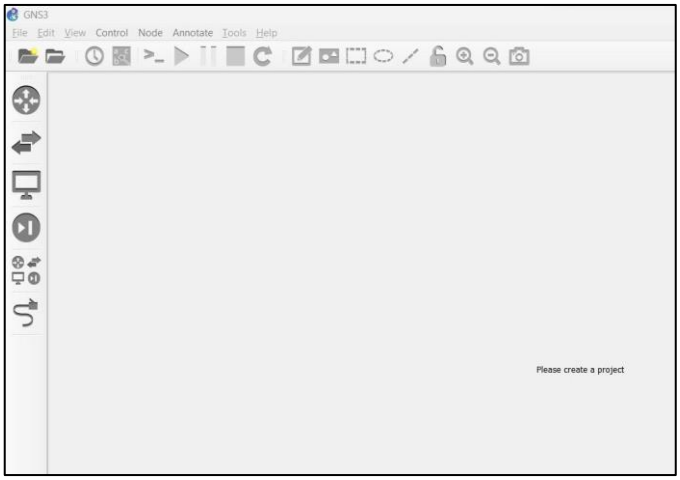
The selection of GNS3 as the main tool in this study is based on its advantages over other network simulation tools such as Cisco Packet Tracer or Boson NetSim. GNS3 offers greater flexibility as it supports the use of real operating systems and devices through integration with Virtual Machines (VMs) and third-party software such as MikroTik RouterOS. This allows for more realistic network simulations and closer to real-world conditions, especially in testing complex protocols such as IPSec and L2TP. Unlike Packet Tracer which is more limited to Cisco devices and is static, GNS3 provides full control over configuration, traffic monitoring, and supports a wide range of hardware vendors. Meanwhile, NetSim tends to be better suited for certification exercises with scenario-based simulations rather than free experiments. As such, GNS3 is a great choice because it supports research needs that require a high level of precision, flexibility, and multi-platform compatibility in thoroughly testing a site-to-site VPN connection.

FINDINGS AND DISCUSSION

Planning

The first step in this simulation is to install GNS3. GNS3 is available for Windows, Linux, and macOS operating systems. After successfully installing GNS3, the next step is to download and install a virtualization application such as VMware or VirtualBox. This virtualization application is used to run the network operating system that will be used in the simulation, in this case the MikroTik OS Router.

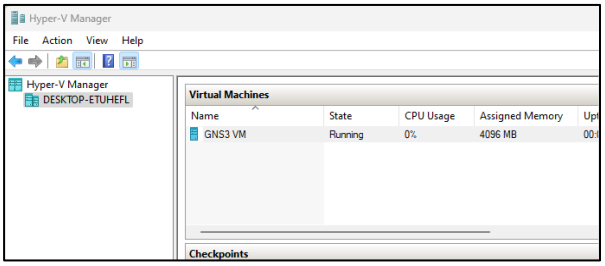
Figure 2: GNS3 interface



Hyper-V Installation

To install Hyper-V on Windows 11, follow these steps: go to the Start menu, click the Settings icon, select the "Apps" category, click on the "Optional features" option, click the "Other Windows features" button, check the box next to "Hyper-V" and all its sub-options, click "OK" to start the installation process, wait for Windows to finish downloading and installing the necessary drivers, restart the computer when prompted, and then launch Hyper-V Manager from the Start menu.

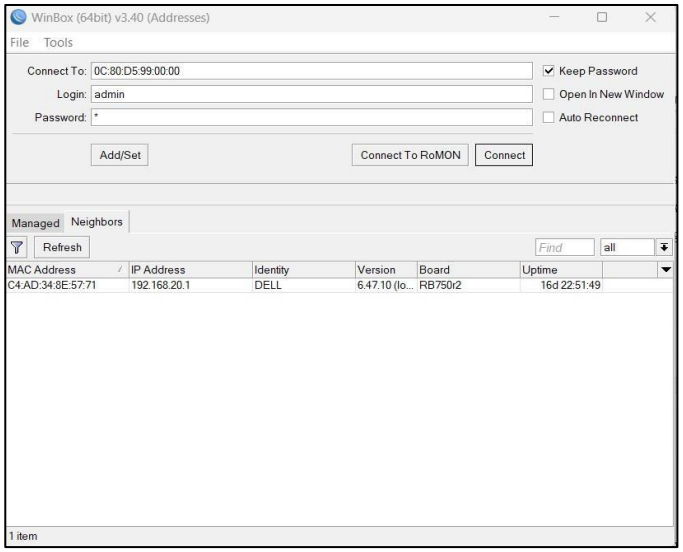
Figure 3: Hyper-V manager display



Installation Victory Box

The Winbox installation process is very simple and can be done quickly. First, you need to download the Winbox installation file from the official Mikrotik website. Make sure to download the latest version that is compatible with your computer's operating system. Once the file has been successfully downloaded, run the installer file and follow the instructions provided. The Winbox installation process is very efficient and fast. Within a few minutes, Winbox will be installed on your computer. In a site-to-site IPSec VPN simulation, Winbox is very useful for configuring a VPN on any Router OS virtual machine. You can easily create IPSec policies, set up encryption proposals, create IPSec profiles, and configure firewall rules through Winbox. By using Winbox, the process of configuring and simulating IPSec VPN site-to-site in Mikrotik becomes easier and more efficient. The intuitive graphical interface allows for quick understanding and mastery of complex network configuration concepts.

Figure 4: Winbox display



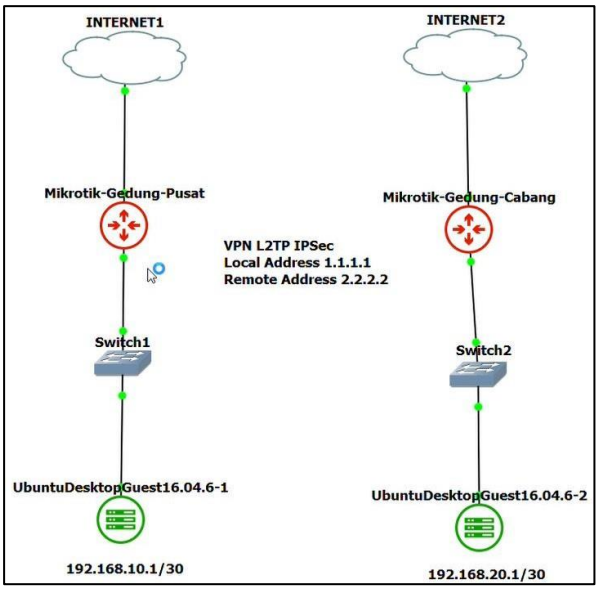
Design

At this point, we'll discuss the site-to-site network architecture to use and how utilizing a VPN for data transmission or communication will make it more secure.

Topology Design

In Mikrotik's site-to-site IPSec VPN simulation using a GNS3 emulator, network topology design is an important factor to consider. The network topology will determine how network devices such as routers, switches, and hosts will connect to each other.

Figure 5: Network topology

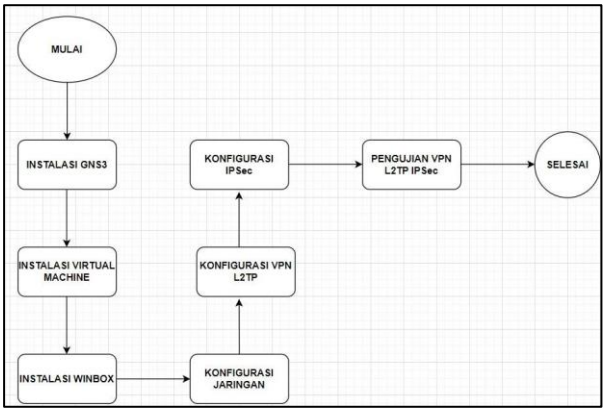


Based on Figure 5, there are two buildings, each with a different internet source. In order for each client to be able to remotely access each other between routers, the first step is to determine the placement of the IP address first. IP 192.168.10.2/30 is intended for clients connected to the MikroTik central building, where this IP will be configured on the MikroTik central building. while IP 192.168.20.2/30 is intended for clients connected to Mikrotik branch buildings. Once the IP is defined, the next step is to configure the VPN on each Mikrotik. Local IP address 1.1.1.1 is used to identify and receive connections from VPN clients, while remote IP address 2.2.2.2 is used to connect to a VPN server when establishing a VPN connection. Once the VPN is configured, the final step is to set up static routing so that clients can exchange data with each other.

Workflow Diagram

Workflow Diagram In performing a site-to-site IPSec VPN simulation on Mikrotik using a GNS3 emulator, it is very important to understand the workflow diagram or the sequence of steps to follow. This workflow diagram will help ensure that the simulation process runs smoothly and systematically.

Figure 6: Workflow diagram



In Figure 6, the workflow process diagram begins with the network configuration, followed by the L2TP IPSec configuration on the central building router, then the L2TP client configuration on the branch

building, and finally the static routing configuration to map the communication paths between the networks. Once all the configurations are complete, the next step is to perform a connection test to ensure that data communication can run smoothly from one building to another through the configured L2TP IPSec VPN. If the connection test is successful, the simulation is considered successful and can proceed with configuration optimization or further evaluation as needed.

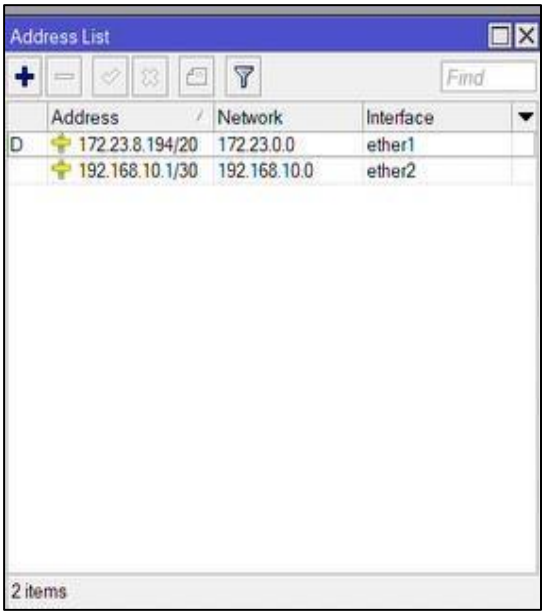
Implementation

At this stage, implementation continues from the preparation and design stages. The researchers now divide the implementation procedure into several phases.

Network Configuration

In the IPSec VPN site-to-site simulation in Mikrotik using the GNS3 emulator, the first step to do is network configuration. The purpose of this network configuration is to ensure that each network device in the simulated topology has the correct settings so that it can communicate with each other.

Figure 7: Basic network configuration

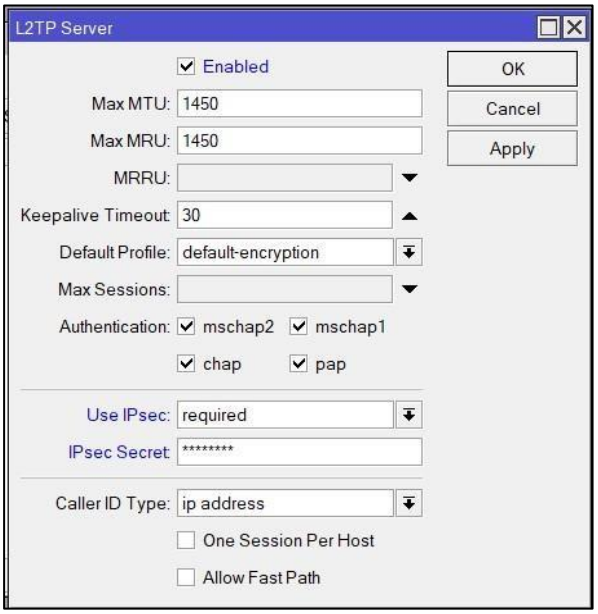


In Figure 7, inside the main building router, the first step to take is to configure the DHCP IP to automatically assign an IP address to a host connected to the local network. The DHCP IP configuration includes the determination of the IP address range to be distributed, the default gateway, and the DNS server address. Similarly, branch office routers also require DHCP IP configuration so that hosts on the local network can automatically obtain IP addresses. Once the DHCP configuration is complete, admins can continue testing to ensure that hosts on each local network can correctly obtain IP addresses and can communicate with each other within the same network.

L2TP Configuration

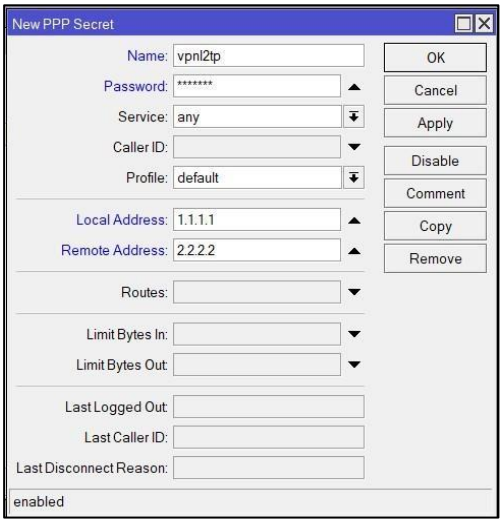
Once the network configuration is complete, the next step in the IPSec VPN site-to-site simulation on Mikrotik using the GNS3 emulator is to configure L2TP (Layer 2 Tunneling Protocol). L2TP is a protocol used to establish a VPN connection by routing data packets from one network to another over a secure communication path.

Figure 8: L2TP server configuration



In Figure 8, there is a view of the L2TP server configuration, which is located in the main building. To enable this L2TP Server VPN, click on the box labeled "activate".

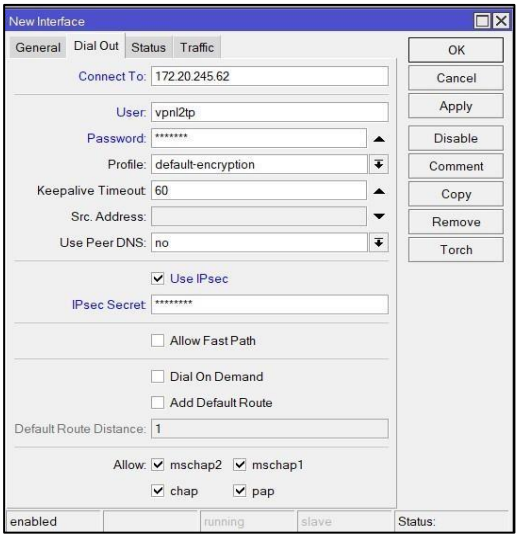
Figure 9: Secret configuration



The explanation for Figure 9 is as follows:

a) Name
In the name field, fill in as needed.
b) Password
In the password field, fill in as needed.
c) Local Address
In the local address field, fill in it with IP 1.1.1.1.
d) Remote Address
In the remote address field, fill in it with IP 2.2.2.2.

Figure 10: L2TP client configuration



There are several configurations shown in Figure 10, including:

a. Connect To to start configuring the L2TP client on a branch office router, in the Connect To field, enter the public IP found on the headquarters internet. The IP can be found on the MikroTik router in the central building in the IP Address (Ether 1) section.
b. User Enter a user that has been created on the central building router.
c. Password Enter the password that has been created on the central building router.

IPSEC Configuration

In Figure 11, in the IPsec Secret field, enter the password according to your needs so that the data exchange will be more secure. This IPsec Secret serves as a secret key used for authentication and encryption in IPsec VPN connections, so it is important to use a strong and unique password. In Figure 10, fill in the IPsec Secret on the branch office router by entering the code generated on the head office router. Be sure to enter the exact same IPsec Secret on both sides, both on the central building router and the branch building router, so that the data authentication and encryption process can work correctly. Additionally, it is recommended to use a combination of characters such as uppercase, lowercase, number, and special symbols to create a stronger and more secure IPsec Secret password.

Figure 11: Static routing configuration for main building routers

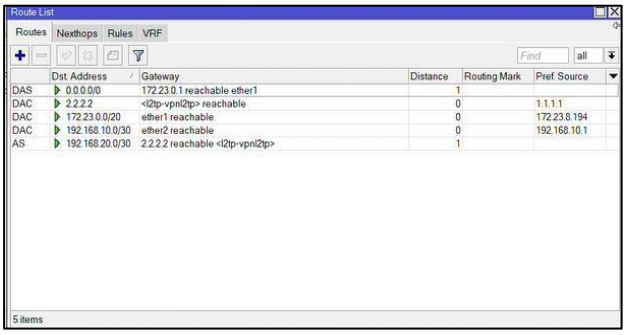
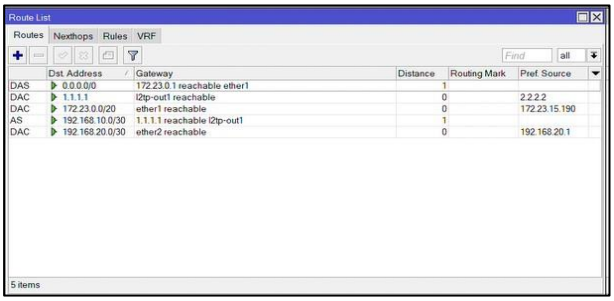


Figure 12: Static routing configuration for branch office routers



Based on Figure 11 and 12, a static routing configuration that allows the main building client and the branch building client to communicate or exchange data over a pre-established VPN connection. This static routing is necessary to map the communication path between two geographically separated local networks, using an IP tunnel as a gateway. An IP tunnel is a virtual IP address used to create data packets over a VPN connection established between a central building router and a branch building router. By configuring static routing on each router, data packets destined for the network on the other hand will be forwarded through an IP tunnel, ensuring they reach their destination securely and encrypted. In addition, static routing also ensures that only data packets destined for the network on the other side will be forwarded through the VPN, while other data packets will be routed according to the existing routing table.

Testing

IPSec L2TP VPN Test Results

Once all network configuration, L2TP, IPSec VPN, and static routing are complete, the next step is to perform a network connection test to ensure that the site-to-site IPSec VPN simulation on Mikrotik using the GNS3 emulator is working properly. This connection test is essential to verify whether the configuration that has been performed is successful or not.

Figure 13: Remote testing from main building client to branch building

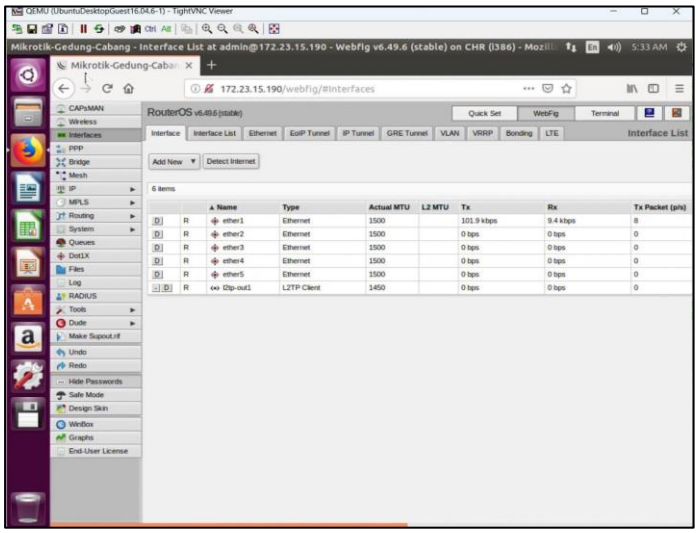
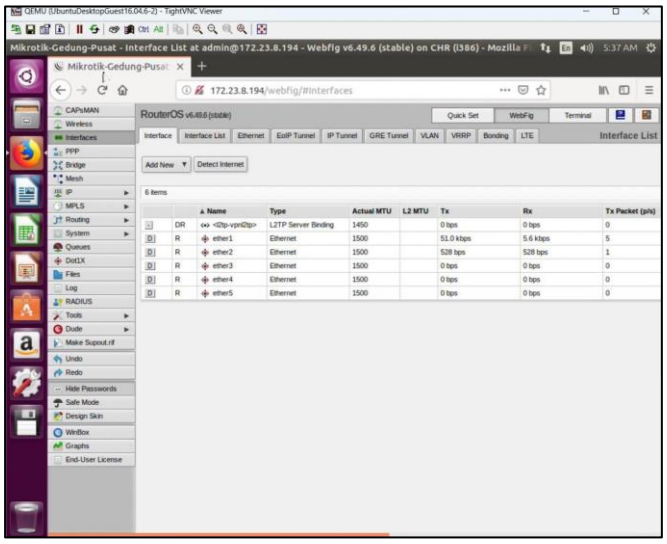


Figure 14: Remote testing from branch office client to head office



One way to perform a connection test is to try to ping from the host on the main building's local network to the host on the branch building's local network, and vice versa. If the ping is successful, it indicates that the VPN connection has been established correctly and that the data communication between the two networks can run smoothly. Network connection testing is a very important stage in network simulations like this. By conducting a thorough connection test, we can ensure that the configuration that has been created is running well and meeting expectations.

In the testing phase, evaluations are conducted using several key metrics to assess the success and quality of the implementation of a site-to-site VPN connection. Connection stability is tested by continuously ping between devices over a period of time to ensure that the connection remains active without interruption. The test results show that the VPN connection is able to hold up for a long period of time without interruptions. Packet loss is also measured using pings of various packet sizes to observe packets lost during data transmission. The percentage of packet loss is very small, indicating a fairly reliable connection.

Furthermore, the encryption strength is analyzed based on the algorithms used in IPSec and L2TP/IPSec configurations. Security protocols such as AES-256 and SHA-1 or SHA-256 are used to guarantee the confidentiality and integrity of data, which demonstrates a strong level of encryption and complies with industry standards. Finally, in terms of configuration efficiency, L2TP/IPSec connections require additional configuration compared to pure IPSec, but it is easier to manage connections because it uses an additional tunneling layer. Both methods show high efficiency in their implementation, but L2TP/IPSec tends to be more flexible for new users. Overall, this test provides a comprehensive overview of the performance and security of VPN connections built in the simulation environment.

CONCLUSION

This study successfully implemented and simulated a site-to-site IPSec connection using a GNS3 emulator effectively. The simulation results show that a site-to-site IPSec configuration can be well established in a simulated environment, facilitating secure communication between two geographically separated networks over a public network such as the Internet. In addition, integration with L2TP VPN is also done to improve the security and performance of the VPN connection. However, this study has some limitations that need to be considered. The simulation is only tested using ping as a measurement metric, and no real data loading is tested in this scenario. This needs to be considered for further research to evaluate the true performance of VPN connections in the face of larger data loads and more complex traffic variations. For future research directions, it is recommended to explore the implementation of raw IPSec without L2TP to understand the differences in performance and security between these two methods. In addition, evaluation of alternatives such as OpenVPN can also provide additional insight into more flexible and efficient VPN connection options in a simulated environment such as the one used in this study.

APPRECIATION

The author would like to thank Mr. Yuggo Afrianto, S.T., M.Kom. and Mr. Ade Hendri Hendrawan, M.Kom. for their understanding and willingness to take the time to provide advice, guidance, and guidance, making this writing successfully completed. Gratitude was also conveyed to Mr. Fitrah Satrya Fajar Kusumah, M.Kom. as the Head of the Computer Science and Information Engineering Study Program at Ibnu Khaldun University Bogor. Dear Father and Mother who always provide support in the form of prayers, encouragement, attention, and affection that has been bestowed on the author until now. Mr. Dr. Mamat Rahmat, S.Si., M.Si, as the Head of the Computer Systems and Network Lab, who always provides encouragement, guidance, and assistance in completing this thesis. Mr. Ritzkal, S.Kom., M.Kom, as a Lecturer in the Computer Systems and Network Lab, who always provides encouragement, guidance, and guidance for writing this thesis. The extended family of Computer Science majors from the 2018, 2019, and 2020 batches, as well as seniors who always help and provide motivation in the preparation of this final project. Colleagues in the Computer Systems and Network Laboratory who always help and provide motivation in the preparation of this final project. Fellow fighters, especially Halimatusyadiah and Wildania Fasha, who always provide motivation in the preparation of this final project. All parties who have helped and cannot be mentioned one by one. The author realizes that the knowledge and abilities he has are very limited, so it is far from perfect and not free from mistakes in the making of this writing.

REFERENCES

Aprillianto, B., & Pamungkas, D. (2023). Analysis of the development of a virtual network laboratory model using GNS3.

Ardianto, F., & Akbar, T. (2017). The design of the remote network security monitoring system uses the Mikrotik Operational System through the Virtual Private Network.

Candra, A. M., & Samsugi, S. (2021). Design and implementation of Access Point System Manager (CAPSMAN) Mikrotik Controller using the Winbox application. TELEFORTECH, 2(2), 26–32. https://doi.org/10.33365/tft.v2i2.1990

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). Network security uses VPN (Virtual Private Network) with the PPTP (Point To Point Tunneling Protocol) method at the Kertaraharja Ciamis Village Office. Journal of Science and Management, 8(1).

Fitri, S., Pipit, D. A., & Aqim, A. (2019). Designing and building an IPSEC-based VPN network using Mikrotik Routerboard at PT. Seminar Nasional Teknologi Informasi dan Komunikasi (SeNTIK), 3(1), 211–217.

Jayanto, R. D. (2019). Design and build a network monitoring system using the Mikrotik Router OS.

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Improved security of Mikrotik routers against Denial of Service (DoS) attacks. Journal of Information Systems and Technology, 2(4), 115–123. https://doi.org/10.37034/jsisfotek.v2i4.32

Korniyenko, B., Galata, L., & Ladieva, L. (2019). Research on GNS3-based enterprise network information protection systems. In Proceedings of ATIT IEEE.

Mentang, R., Sinsuw, A. A. E., & Najoan, X. B. N. (2015). Design and analysis of wireless network security using a Wireless Intrusion Detection System. Electrical and Computer Engineering, 5(7).

Munawar, Z., Kom, M., & Putri, N. I. (2020). Computer network security in the era of big data. Journal of Information Systems (J-SIKA), 2(1), 14–20.

Prasetyo, B., Budiman, E., & Mahendra Putra, G. (2019). The implementation of the Network Monitoring System (NMS) as an early warning system on Mikrotik routers with SMS Gateway services (Case Study: Mulawarman University). Proceedings of Seminar Nasional Komputer dan Teknologi Informasi, 4(1).

Pratama, H., & Puspitasari, N. F. (2020). Implementation of L2TP/IPSec protocol and port forwarding for remote Mikrotik on dynamic IP networks. Citec Journal, 7(1).

Purnama Sari, A., & Kemala, N. (2020). IP Security-based Virtual Private Network design using Mikrotik Router. Prosisko Journal, 7(2).

Rahino, B. G., & Susila, A. (2022). Implementation of Mikrotik VPN network (L2TP/IPSec) for remote access as security during Work From Home. OKTAL: Journal of Computer Science and Science, 1(11), 1911–1918. https://doi.org/10.53801/oktal.v1i11.192

Riskiono, S. D. (2019). Analysis and design of alternative network transmission lines using Virtual Private Networks (VPNs).

Santoso, B. (2018). Internet Protocol Security (IPSec) method with Virtual Private Network (VPN) for data communication. Journal of Computer Science Research, Embedded Systems & Logic, 6(2), 179–188.

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). Site-to-site VPN implementations use L2TP and IPSec protocols. TEKNOKOM, 4(1), 30–36. https://doi.org/10.31943/teknokom.v4i1.59

Ulum, F. (2018). The network security design on the Mikrotik Router OS uses the Port Knocking method.

Wicaksana, P., Hadi, F., & Hadi, A. F. (2021). The design of the VPN server implementation uses the L2TP and IPSec protocols as network security. KomtekInfo, 8(3), 169–175. https://doi.org/10.35134/komtekinfo.v8i3.128

Yaqin, A. (2020). Development of a network security system with Mikrotik at SMK Muhammadiyah 2 Kuningan. Journal of Artificial Intelligence, 4(36), 117–122.

Zhang, Z., Chandel, S., Jingyao, S., Shilin, Y., Yunnan, Y., & Jingji, Z. (2018). VPN: A scam or a trap? In Proceedings of the 2nd International Conference on Computational Methodology and Communication.