

DESIGN OF A VIRTUAL PRIVATE NETWORK (VPN) NETWORK BASED ON IP SECURITY USING A MIKROTIK ROUTER WITH LP2P METHOD

Billy Hendrik^{*1}, Mardhiah Masril², Hasri Awal³, Firdaus⁴

¹²³⁴Universitas Indonesia - Indonesia

Email : billyhendrik@upiypk.ac.id

Vol. 17 No.4 2023

Submit :

12/10/2023

Accept :

14/12/2023

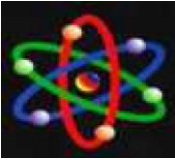
Publish :

31/12/2023

Abstract

One way to maintain and improve the quality of service and security on the network of an institution of the West Pasaman Regency Archives and Library Office is to add a VPN feature. Administrators who are always monitoring traffic by accessing routers and access points to determine network conditions. There are times when the Administrator is on a public network, so he cannot access routers and access point devices because the public IP obtained is Dynamic (random). To overcome these problems, the Network Development Life Cycle (NDLC) method is carried out by combining the L2TP and IPSec VPN protocol systems that exist on Mikrotik. VPN is a private and secure network using a public network such as the internet. One of the security bases for VPN technology is Internet Protocol Security (IPSec). IPSec is a protocol used to secure datagram transmission on TCP/IP-based networks. This study aims to design and implement a Virtual Private Network (VPN) network system by utilizing a public network, where this system provides advanced security enhancements to internet networks using IPSec.

Keywords: VPN, Mikrotik, L2TP, IPSec, Networking



INTRODUCTION

The need for the availability of communication networks and the internet is currently very high with the increasing dependence of humans on the role of information technology. This has the impact that it is necessary to have an internet service provision system that is efficient, reliable but still economical and safe. Advances in technology, especially network technology, make it easier for companies or offices to develop more and be able to face future business challenges [1]. Virtual Private Network (VPN) is an alternative for data security because it is private. VPN allows users to enter the local network, allows users to retrieve data from within the local network and perform remote on devices on the network [2]. In its implementation, VPN is divided into remote access VPN and site-to-site VPN. Site-to-site VPN is used to connect between two places that are located far apart, such as a head office and a branch office. This type of VPN remote access is used by company employees who want to connect to their company's local network from various remote locations [3].

Virtual Private Network (VPN) is a network security technique that works by creating a tunnel so that trusted networks can connect to outside networks via the internet [4]. Internet Protocol Security (IPSec) is a framework of a set of protocols for security on networks or packets processed at the layer of network communications. The big advantage of IPSec is that security stacks can be handled without requiring changes to individual users. Cisco has been a leader in proposing IPSec as a standard or a combination of standards and technologies,

and has included support for it in its routers. IPSec provides cryptographic services for secure data transmission. These services include authentication, integrity, access control, confidentiality, and antireplay [5].

RESEARCH METHODS

In conducting research in order to get the results as expected, then if we need a research method that is usually done, namely.

Library Research

This library research was carried out by reading, discussing, summarizing and making conclusions from books on the IPSec VPN method using a proxy router to obtain scientific materials that can be used as a basis for compiling this thesis report.

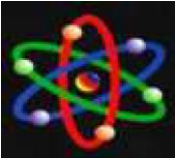
Field Research

Where the author goes directly into the field to retrieve the data needed to collect data on the Archives and Libraries Service Office network of West Pasaman Regency. In this activity the author asked questions to Ms. Evita Murni as the Head of the West Pasaman Regency Archives and Library Service Office to find out whether data leaks or unstable connections often occur at the West Pasaman Regency Archives and Library Service Office.

Analysis

This analysis phase aims to identify the problems that exist in the system and determine the requirements of the system being built. The analysis includes data analysis, process analysis and system analysis.





Implementation

Implementation is the stage to map the system so that it is ready to operate. The purpose of implementation is to confirm design modules, so that users can provide input to system development. At this stage the researcher will discuss the devices used, this research uses a router proxy which will pass IP packets from one network to another network. Using certain addressing methods and protocols to pass data packets in which the RouterOS (Operating System) is used on the routerboard.

RESULT

The topology design used is a tree type topology, has 4 network devices, namely wireless, router, switch, modem. The West Pasaman Regency Archives and Library Office uses a bandwidth of 20MBps for internet bandwidth. In the topology design, a modem that is connected to the internet will be connected and allocated in advance to a router where the router is used as a VPN proxy as a gateway on the network, all access information traffic entering and leaving the network will pass through the network. proxy identified by the VPN so that traffic cannot be detected by other people using the same internet network.

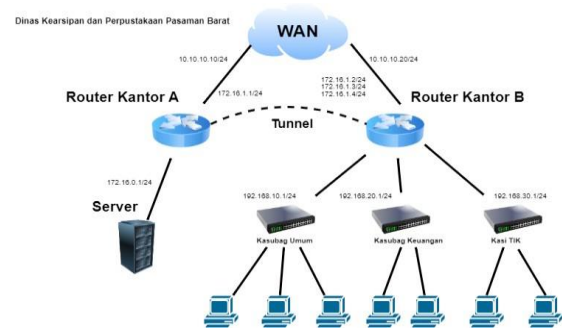


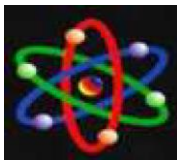
Figure 1. VPN + L2TP Network Topology

In designing this network system, the researcher will create a VPN network using the IPsec method to connect server computers to client/branch computers at the West Pasaman Regency Archives and Libraries Office. The following are the configuration steps on the router side server. Winbox is a free and portable-based application where users don't need to install it and can use it right away, the use of the Winbox application itself is to configure routers quickly because it has a friendly Graphic User Interface (GUI) appearance. Winbox can be applied to Linux, MacOS and Windows operating systems. Winbox is an application that is suitable for creating a VPN server network in order to provide encryption on the public network used.

Address	Network	Interface
172.16.0.1/24	172.16.0.0	Server
10.10.10.1/24	10.10.10.0	Kantor Pusat

Figure 2. IP Address Configuration





So that later each interface that is connected to router A and router B can be connected to each other, it is necessary to do routing first. So, we need to register each network from the interface on router.

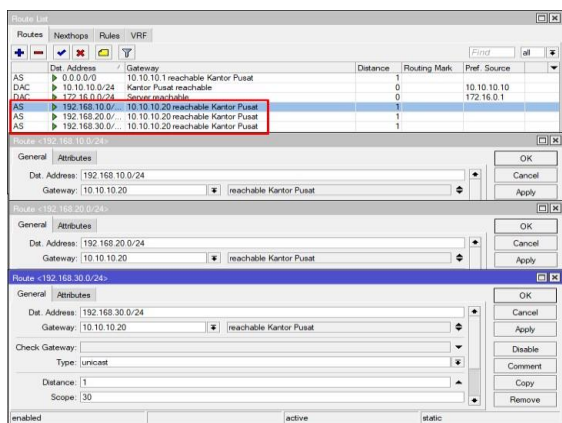


Figure 3. Routing Router A

uses MPPE. To add a level of network security by combining L2TP with IPsec, select the IP menu > IPsec > select the Proposal menu > Click New (+). In the available parameters (default) fill in as shown below :

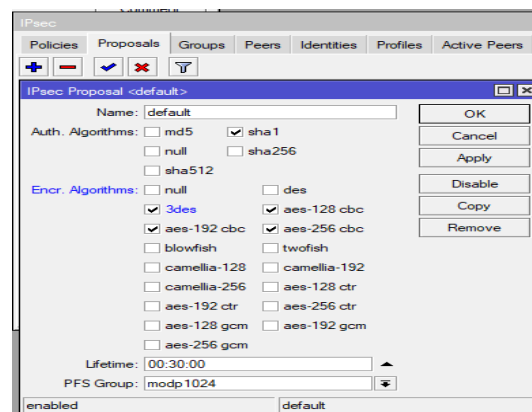


Figure 5. IP Sec Configuration

L2TP server is a development of PPTP plus L2F. L2TP is more firewall friendly than other VPN types such as PPTP.

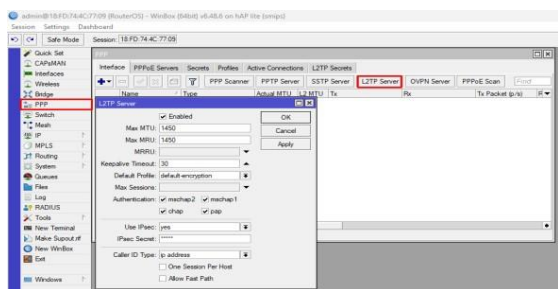


Figure 4. Set Secret L2TP Server

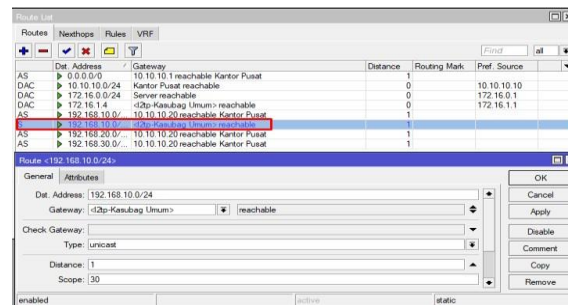
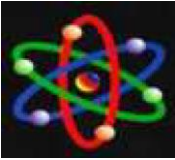


Figure 6. Result Of VPN L2PT Configuration

Here we will fill in some of the main standard parameters for connection. Such as specifying the username and password for the client authentication process that will connect to the L2TP Server. At this point, the L2TP Server configuration is complete. Encryption on L2TP/IPsec has a higher level of security than PPTP which

Encryption on L2TP/IPsec has a higher level of security than PPTP which uses MPPE. To add a level of network security by combining L2TP with IPsec, select the IP menu > IPsec > select the Proposal menu > Click New (+). WLAN1, ether 2, ether 3, and ether 4 are interfaces used for routers that function as gateways for connecting to the internet. So that later each interface connected to router B and





router A can be connected to each other, it is necessary to do routing first. So, we need to register the network from the interface on router A. L2TP client is a development of PPTP plus L2F. L2TP is more firewall freindly than other VPN types such as PPTP.

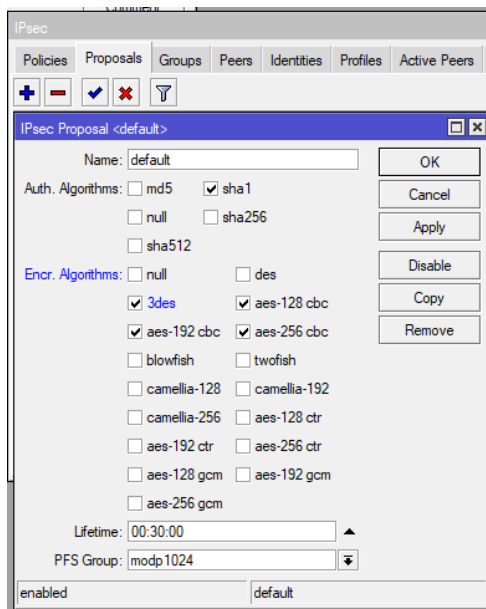


Figure 7. L2PT Routing

Encryption on L2TP/IPSec has a higher level of security than PPTP which uses MPPE. To add a level of network security by combining L2TP with IPSec, select the IP menu > IPSec > select the Proposal menu > Click New (+). In the available parameters (default) fill in as shown below. Adjust to Ipsec from the previous L2TP Server. In the initial network test, a test will be carried out on a server network that is running without a VPN. Packet Loss Test The packet loss test is carried out several times with the "ping" command to the destination IP using the command prompt to see the stability of the

connection on a network without a VPN. And the following results are obtained.

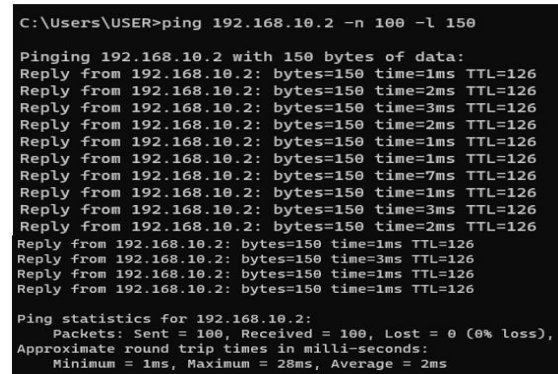


Figure 8. DOS Attack Initial Test

In this final network test, several tests will be carried out as was done in the initial test. That way you will be able to see changes from the network using a VPN. The packet loss test is carried out several times with the "ping" command to the destination IP using the command prompt to see the stability of the connection on the public network using L2TP/IPSec VPN. And the following results are obtained :

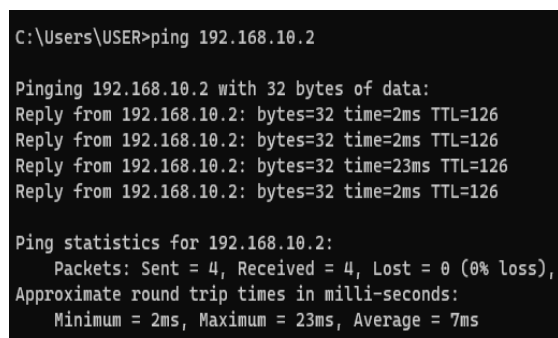
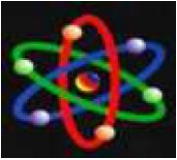


Figure 9. Packet Loss Network VPN Server to Client

From the data above it can be seen that the max and average round trip data for a package are still within reasonable limits.





From the server to client experiments, 4 packets were sent, max round trip = 23ms and average round trip = 7ms. Meanwhile, from the client to server experiment, 4 packets were sent, max round trip = 18ms and average round trip = 6ms.

This test is useful to see the robustness of the connection when ddos attack. Testing is done with Echo Request and Buffer Size. After testing, the following results were obtained. The data above is a test by flooding the VPN server with 100 data packets of 150kb. It can be seen that the max and average round trip data for a packet are still within reasonable limits.

CONCLUSION

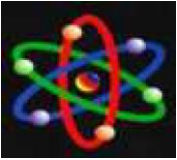
After completing the stages of implementation of activities from needs analysis from design to testing and discussion of the results, the following conclusions can be drawn. Design simulations using the Microsoft Visio 2013 application can be carried out virtually as a result of a blueprint before the application of the network system is increased. Improving the network security system by activating the IPsec feature found on the OSI 5 (Network) router layer so that the information flow back process is guaranteed confidentiality and security, especially in the ADM, secretariat section. IPsec can also be combined with other security systems such as proxies and firewalls, in order to implement layered security on the network or also called multiple layer security. By using a VPN Server network with the L2TP/IPsec method, security on the network system

will increase due to IPsec support which automatically encrypts information sent on the network. And accounts that have been activated can access the sub-district office database. Implementation of a VPN server network using the L2TP/IPsec method is fairly easy and can be done easily so it doesn't require special skills that network administrators must have.

BIBLIOGRAPHY

- [1] Parenreng, J. M. (2023). Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN). *Internet of Things and Artificial Intelligence Journal*, 3(3), 239-249.
- [2] Afira, R., Prawiro, R., & Jamhur, A. I. (2023). VIRTUAL PRIVATE NETWORK (VPN) BASED ON IP SECURITY DESIGN ON TOPOLOGY. *JOURNAL OF DYNAMICS (International Journal of Dynamics in Engineering and Sciences)*, 8(2), 56-59.
- [3] Putra, T. A., Hadi, A. F., & Gema, R. L. (2022). DESIGN AND IMPLEMENTATION OF VPN SERVER USING L2TP PROTOCOL. *JOURNAL OF DYNAMICS (International Journal of Dynamics in Engineering and Sciences)*, 7(1), 86-90.
- [4] Zain, R. H., Devita, R., & Putra, O. E. (2022). IMPLEMENTATION OF VPN SERVER USING L2TP PROTOCOL AND IPSEC METHODS AS NETWORK SECURITY. *Jurnal Ipteks Terapan*, 16(4), 754-760.
- [5] Ryansyah, M., & Musyaffa, N.





- (2020). Implementation of VPN Using Router MikroTik at Al-Basyariah Education Foundation Bogor. *Jurnal Teknik Informatika CIT Medicom*, 12(2), 49-55.
- [6] Wicaksana, P. (2023). Implementasi VPN Server Menggunakan Protokol L2TP dan Metode IPSEC. *Jurnal Sains Informatika Terapan*, 2(3), 119-123.
- [7] Wicaksana, P., Hadi, F., & Hadi, A. F. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, 8(3), 169-175.
- [8] Rahman, F. F., & Robianto, R. (2020). Building Lptp Vpn Network and User Management Using Fuzzy Logic Based on Age and Utilization of The Dude for Network Monitoring. *Jurnal KomtekInfo*, 7(1), 22-31.
- [9] Masril, M., Hendrik, B., Awal, H., & Fikri, H. T. (2023). optimization of wifi network placement using the simulation annealing method: Joirnal Network. *JOURNAL OF DYNAMICS (International Journal of Dynamics in Engineering and Sciences)*, 8(1), 41-44.
- [10] Tindall, J., Fishman, M., Stoudenmire, E. M., & Sels, D. (2024). Efficient tensor network simulation of ibm's eagle kicked ising experiment. *PRX Quantum*, 5(1), 010308.

