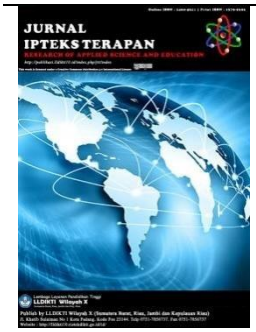

Vol. 17 No.4 2023

DESIGN AND IMPLEMENTATION OF VPN SERVER USING L2TP PROTOCOL (LAYER 2 TUNNELING PROTOCOL) AND IPSEC METHOD AS SECURITY

Silky Safira*[1], Deval Gusrion[2], Rima Liana Gema[3], Dinda Djesmedi[4], Ipriadi[5]
[12345]Universitas Prima Indonesia - Indonesia
Email : silkysafira@upiyptk.ac.id

Submit :
18/09/2023

Accept :
15/12/2023

Publish :
31/12/2023

Abstract

One way to maintain and improve the quality of service and security on the network of the Padang City Transportation Agency is to add a VPN feature. Administrators who always monitor traffic flow by accessing routers and access points to determine network conditions. There are times when the Administrator is on a public network, he cannot access routers and access point devices because the Public IP obtained is Dynamic (random). To overcome this problem, the Network Development Life Cycle (NDLC) method is carried out by combining the L2TP and IPsec VPN protocol systems on Mikrotik. A Virtual Private Network (VPN) is a private and secure network using a public network such as the internet. One of the foundations for securing 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 VPN network system by utilizing a public network, where this system provides further security enhancements to internet networks using IPSec. The information/data sent will be kept confidential by means of an automatic encryption method via the L2TP tunnel method from the main field room to the UPT room computer and vice versa. VPN is implemented using the layer 2 tunneling protocol (L2TP) using two Mikrotik routers. There are slight changes to the computer network configuration to minimize cost and implementation time. Tests are carried out to implement security on the network using the command prompt, where the admin observes packet loss and delay parameters to find out the increase in the quality of security on the network.

Keywords: VPN, Mikrotik, L2TP, IPSec, NDLC

http://publikasi.lldikti10.id/index.php/jit DOI : https://doi.org/10.22216/jit.v17i4 PAGES : 1069-1074

ISSN :1979-9292 / 2460-5611
JIT is Sinta 3 Journal (https://sinta3.kemdikbud.go.id/journals/profile/2143) accredited by Ministry of Research & Technology, Republic Indonesia

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i4 (1069-1074)

ISSN : 1979-9292

E-ISSN : 2460-5611

INTRODUCTION

The development of information technology is currently very rapid, especially the internet, so many human activities are resolved more quickly with the existence of this internet technology. However, the development of technology has a negative impact on agencies that do not have strong enough security, especially in terms of network security, even though this security has a good type of security protocol, there are still certain people or groups who can penetrate security which results in loss of important information data. Stolen. One of them is similar to a business or agency where a lot of sensitive data is stored and is susceptible to theft by careless parties, costing the agency money. As a result, a strategy to lessen or even stop different types of information theft or cyberattacks by attackers using an Internet network is needed. Virtual Private Network (VPN) is one way to prevent and protect the exchange of information data through the internet network. VPN itself is a communication technology that allows connections from public networks and uses them like local networks and even joins the local network itself. By using a public network , users can access existing information on the local network, get the same rights and settings. (Rahman, F., Sahari, S., & Robianto, R. (2020)). One of the VPN services found on Mikrotik is Layer 2 Tunneling Protocol (L2TP). In particular, using L2TPcan help exchange information and increase network security between several networks through a tunnel that passes through the internet network safely. L2TP is a development of PPTP plus L2F. Network security and encryption used for authentication are the same as PPTP, usually for better security with this VPN security data information and network security are better than previous VPN services. (Rahman, F., Sahari, S., & Robianto, R .(2020)).

To be able to meet the security needs of L2TP, security implementation must be implemented using the transport-type IPSec protocol, or better known as the L2TP over IPSec (L2TP/IPSec) protocol, the IPSec protocol. The IPSec protocol provides an Internet Key Ecchonge (IKE) that can meet these needs. authenticate and make an agreement between 2 computers, which is called the Security Association (SA). Authentication and agreement between the 2 computers is stored in a digital certificate that must be owned by the server or clien. The research was carried out on the awareness of the limited understanding obtained in previous journals, inorder to develop the methods used previously and to encourage curiosity about all problems so that they can design a solution that is better, more effective, efficient and affordable in terms of network security. The research provides a formulation of the problem where later the researcher will design a VPN server network with the L2TP and IPSec methods to increase the resilience of the network system so that it is hoped that it can provide alternative solutions to network security.

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i4 (1069-1074)

ISSN : 1979-9292

E-ISSN : 2460-5611

RESEARCH METHODS

This test session was conducted to find out whether the network simulation can run successfully without errors with the initial planning. Testing is attempted only on one server computer and several client computers with the aim of identifying whether the design is in accordance with the initial plan. Testing the VPN server was attempted by testing the connectivity of the request reply information packet to the internet network via the command prompt.

RESULT

Comparison between the topology schemes before and after the VPN feature was added to the LAN network of the Barangin Sub-district Office, Sawahlunto City. The topology used can be seen in Figure 1.

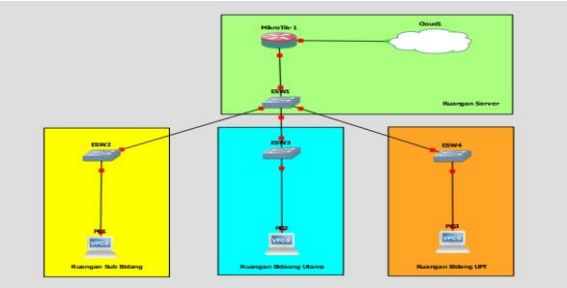

Figure 1. LAN Topology Scheme

The star network topology used in the Barangin District Office instances that have not yet used the establishment of a VPN is shown in Figure 2.

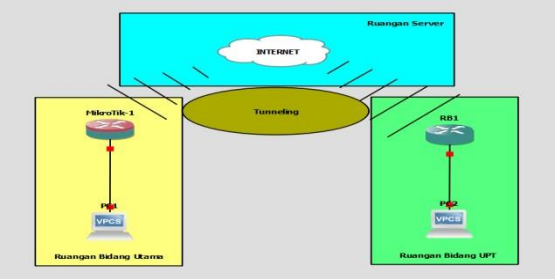

Figure 2. L2TP VPN Network Topology Scheme

In designing a L2TP VPN network there are several steps that must be taken, a system that is in accordance with the design will make it easier to manage network configuration and not make an administrator confused in managing it.

In designing this network system, researchers will create a VPN network using the L2TP/IPsec method to connect server computers to client computers at the Transportation Agency office. The following are the configuration steps on the router side server (CHR).

Winbox a portable application that can be used without having to install it first. Confuguration to mikrotik using the Winbox software is presented in figure 3.

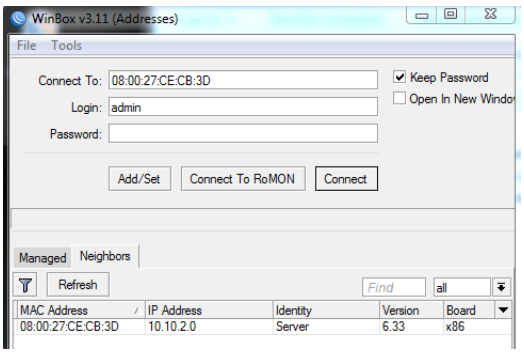

Figure 3. Appearance Winbox

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i4 (1069-1074)

ISSN : 1979-9292

E-ISSN : 2460-5611

Activate winbox to connect to the internet by clicking Connect To wait until the MAC address appears after appearing, click login with the default configuration listed on the application and Connect.

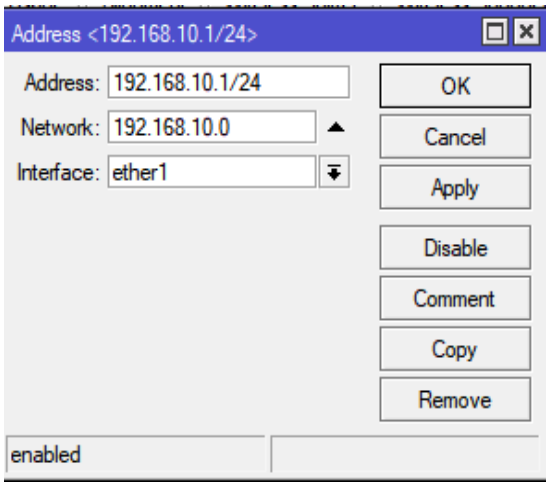

Figure 4. L2TP Server Configurtion

Either 1 which is the first port used to configure the IP wlan which functions as a gateway to the internet.

first menu selection is selecting the PPP menu on the left side of Winbox until the PPP dialog box appears. In the PPP dialog box, select the L2TP server menu until the L2TP server dialog box appears as shown in Figure 4.

Fill in the L2TP Server form box by ticking enable, for the default profile select default-encryption and IPSec Secret enter the desired password. In this section, the purpose of creating an L2TP secret is to create an account for users who will access the VPN network presented in Figure 5.

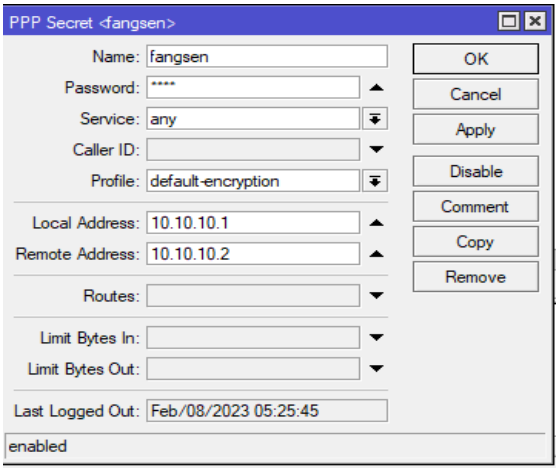

Figure 5. L2TP Secret Configuration

DDoS is a type of attack that is carried out by flooding the internet network traffic on a server, system or network. Generally this attack is carried out using several attacker host computers until the target computer cannot be accessed. The following is the result of a network attack using DdoS. Figure bellow shows the results of the Request Time Out (RTO). Testing was carried out with the UDP Unicorn attack to the ip address of the server showing that the attack was successful by making the server not respond/answer, which means the attack succeeded in flooding the server's network traffic.

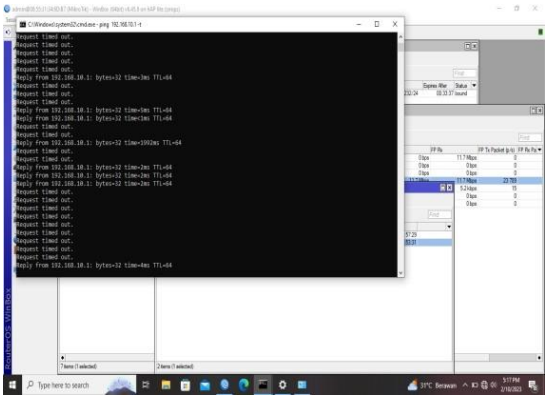

Figure 6. DDoS Attack not connecting L2TP/IPSec

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i4 (1069-1074)

ISSN : 1979-9292

E-ISSN : 2460-5611

Figure above shows the results of the Request Time Out (RTO). Testing was carried out with the UDP Unicorn attack to the ip address of the server showing that the attack was successful by making the server not respond/answer, which means the attack succeeded in flooding the server's network traffic.

After designing a VPN network device in the Camat's office using a Mikrotik router to send confidential information/data, the following results are obtained: Room 1 network server with room 3 can be connected by a tunneling line that uses the internet network.

a. Room 1 network server with room 3 can be connected by a tunneling line that uses the internet network.
b. The process of exchanging confidential data is no longer withdrawn manually or using e-mail, but instead uses a VPN network that is integrated into the local network between the head office and branch offices.
c. The VPN network system is much more secure and the funds needed to build a VPN network with a proxy router are much more affordable.

Implementation of using a VPN with the L2TP method and IPSec security system can be done if both routers access the same internet provider. The design of a VPN tunneling network uses the L2TP method with an IPSec security system equipped with a secret, which means an identity that will be given to the user when doing the L2TP line. Implementation of a wireless L2TP Client can be done with the help of VPN Settings on the operating system with the aim of connecting to the L2TP Server line and connecting to the internet network on wifi. Improved network security system by activating the IPSec feature.

CONCLUSION

IPSec can also be developed with other security systems such as proxies and firewalls, in order to implement layered security on the network or also called multiple layer security. IPSec support that performs automatic encryption of information sent on the network. Connected users can access the Padang City Transportation Office databases. 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. VPN Server network with the L2TP/IPSec method, the security of the network system will increase because IPSec supports automatically encrypt information sent on the network. The implementation of a VPN server network using the L2TP/IPSec method is fairly easy and can be done easily so that it does not require special skills that must be possessed by network administrators.

BIBLIOGRAPHY

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.

Wicaksana, P., Hadi, F., & Hadi, A. F. (2021). Perancangan Implementasi

ISSN : 1979-9292
E-ISSN : 2460-5611

VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. Jurnal KomtekInfo, 8(3), 169-175.

Jahan, S., Rahman, M. S., & Saha, S. (2017, January). Application specific tunneling protocol selection for Virtual Private Networks. In 2017 international conference on networking, systems and security (nsyss) (pp. 39-44). IEEE.

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

Kadry, S., & Hassan, W. (2008). DESIGN AND IMPLEMENTATION OF SYSTEM AND NETWORK SECURITY FOR AN ENTERPRISE WITH WORLDWIDE BRANCHES. Journal of Theoretical & Applied Information Technology, 4(2).

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.

Kadry, S., & Hassan, W. (2008). DESIGN AND IMPLEMENTATION OF SYSTEM AND NETWORK SECURITY FOR AN ENTERPRISE WITH WORLDWIDE BRANCHES. Journal of Theoretical & Applied Information Technology, 4(2).

Lewis, M. (2006). Comparing, designing, and deploying VPNs. Adobe Press.

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.

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.