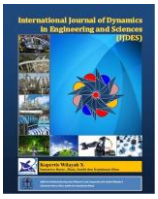
INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES)
LLDIKTI WILAYAH X
Vol. 7, No. 1, Month 2022
e-ISSN: 2502-0692



DESIGN AND IMPLEMENTATION OF VPN SERVER USING L2TP PROTOCOL

Teri Ade Putra [1,*], Aulia Fitrul Hadi [2], Rima Liana Gema[3]
[123] Universitas Putra Indonesia YPTK Padang
Jl. Lubuk Begalung, Padang, Indonesia

doi.10.22216/jod.v7i1.1063
*Correspondence should be addressed to teriadeputra@upiyptk.ac.id

Article Information

Submitted :
03 March 2022

Accepted :
28 May 2022

Published :
30 May 2022

Abstract

This study aims to design a VPN network system by utilizing a public network, where this system aims to provide security by using IPSec in providing confidential information through the L2TP tunnel method from the server to the branch/client computer and vice versa. VPN is implemented using layer 2 tunneling protocol (L2TP) using two Mikrotik routers. There are only a few changes in the computer network configuration to minimize costs 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 security quality on the network.

Keywords: Virtual private network, Mikrotik, VPN, L2TP, IPsec

1. Introduction

The development of Information Technology is currently very fast, especially the Internet, however, the development of technology has a bad impact on agencies that do not have strong enough security, especially in terms of network security, even though the security has many types of security protocols. One of them is like an agency or company where there is so much important information data that can be stolen due to irresponsible individuals, therefore a method is needed to reduce even prevent various acts of theft of information or attackers carried out via the Internet.

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 a local network and even joins the local network itself. By using a public network, users can access information on the local network, get the same rights and settings [1].

One of the VPN services found on Mikrotik is Layer 2 Tunneling Protocol (L2TP), especially using L2TP can help exchange information and improve network security between several networks through a tunnel that passes through the internet network safely. L2TP is an extension of PPTP plus L2F. Network Security and encryption used for authentication are the same as PPTP, usually for better security with this VPN, information data security and network security are better than previous VPN services [1].

The IPSec protocol provides an Internet Key Exchange (IKE) that can fulfill the need for authentication and make an agreement between 2 computers, called the Security Association (SA). Authentication and agreement between the 2 computers are stored in a digital certificate that must be owned by the server and client.

2. Method

The research methods carried out are as follows:

a. Field Research

This research was conducted by interviewing staff working in the IT department in particular, asking questions and analyzing problems and obtaining the required data.

b. Research Library (Library Research)

This library research was conducted by reading journals, books, internet, articles discussing computer networks, VPN Servers, L2TP, PPTP, IPSec and related to Network Security. So that the data obtained can be used as a basis for the next stage of research.

3. Result and Discussion

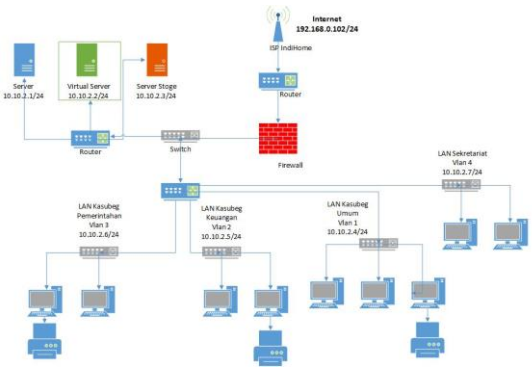


Figure 1. LAN Topology Schematic

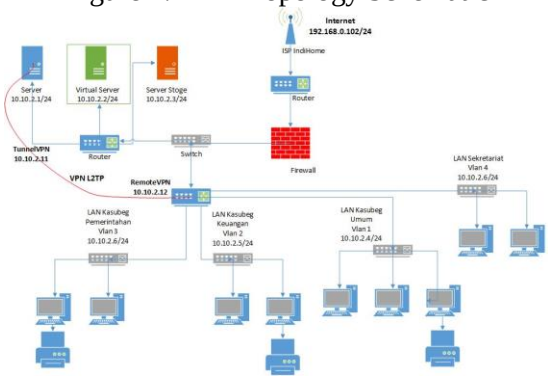


Figure 2. L2TP VPN Network Topology Schematic

In proposing a network topology to be implemented, it will not change the shape of the existing topology, because the shape of the topology used is already very good. The topology used is a star topology. And it is proposed to use a VPN to communicate or exchange private data to be more secure.

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

In the following network system design, the researcher will create a VPN network with the L2TP/IPsec method to connect the server computer with the client/branch computer at the Camat office. The following are the configuration stages on the router side (CHR) server.

1. Login to Mikrotik using Winbox software software

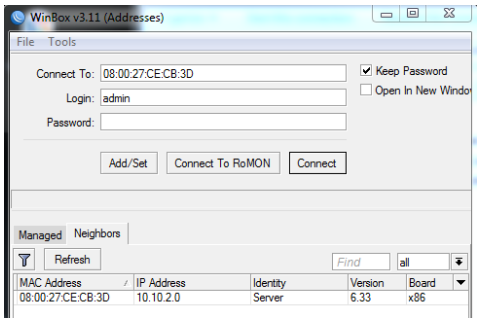


Figure 3. Winbox Display

2. IP Address Configuration

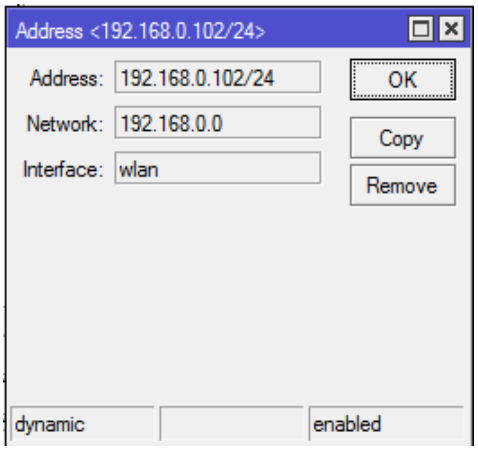


Figure 4. IP wlan configuration

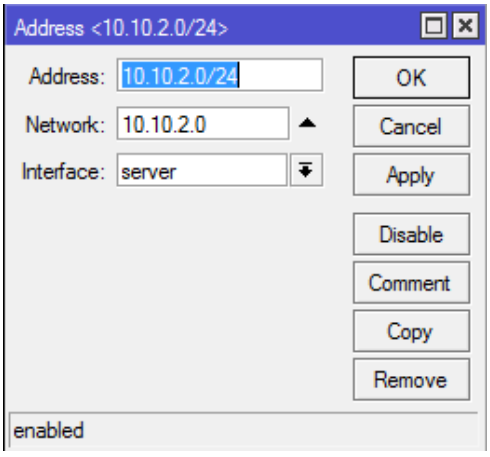


Figure 5. Configure local IP

3. Router Configuration

Configure NAT on the firewall. NAT is an IP address mapping so that many private IPs in a LAN can access public IPs. After installing the Mikrotik, the next step is to configure NAT via the terminal. After forming a server configuration to be able to connect to the internet, the next step is to create a proxy configuration to create VPN technology.

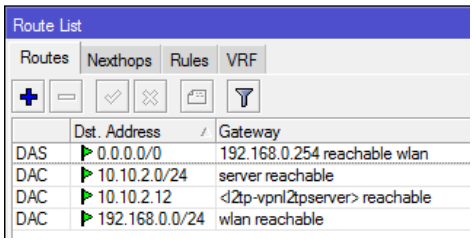


Figure 6. Router Configuration

4. L2TP Server Configuration

The first menu selection is selecting the PPP menu on the left side of the winbox until the PPP dialog box appears. In the PPP dialog box, select the L2TP server menu until the L2TP server dialog box appears.

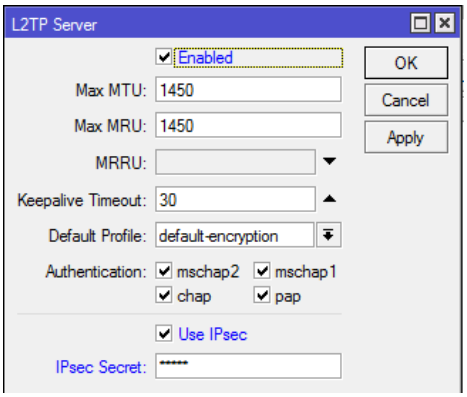


Figure 7. L2TP Server Configuration

5. L2TP Secret Creation

In this section, the purpose of making L2TP secrets is to create accounts for users who will access the VPN network.

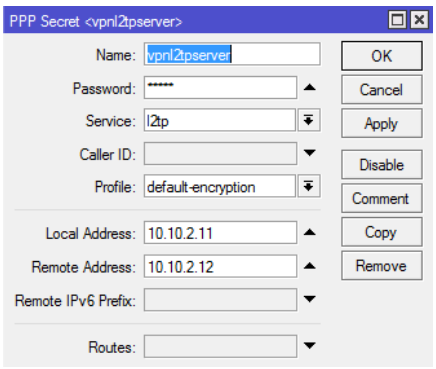


Figure 8. L2TP Secret Creation

6. VPN client/branch configuration

The first step in making a VPN client uses the facilities circulating in Windows 7, namely the Network and sharing center, then continues with the VPN connecting process, then a VPN is formed on the remote client.

Figure 9. L2TP Secret Creation

7. Network Testing

In terms of network testing there are 2 ways to get maximum results. Especially in designing VPN technology, namely:

a. Initial network testing

1. *Packet loss test*

Packet loss testing was carried out several times with the "ping" command to the destination IP using a command prompt to see the stability of the connection on a public network without a VPN. And the result is thatfor

data max and average round trip a packet is still within a reasonable. From the experiment of 4 packets, max round trip = 2ms and average round trip = 1ms.

2. *Daniel of services test*

This test is useful to see connection resistance when in ddos attack. Testing is done with the pingflood.exe application. After testing by sending 4 data packets of 25 kb, the results showed that the network was not disconnected and the maximum round trip was 2ms.

b. Final network test

1. Packet loss test

Packet loss testing was carried out several times with the "ping" command to the destination IP using a command prompt to see the stability of the connection on a public network using L2TP/IPSec VPN. And the result is thatfor data max and average round trip a packet is still within a reasonable. From the experiment of 9 packets, max round trip = 3ms and average round trip = 1ms.

2. Daniel of services test

This test is useful to see connection resistance when in ddos attack. Testing is done with the pingflood.exe application. After donetesting by flooding the VPN server with 28 data packets of 25kb. The data obtained for max and average round trips of a packet are still within reasonable limits.

After designing a VPN network device at the Camat office using a Mikrotik router to send confidential information/data, the following results are obtained:

a. The sub-district office network server with the branch sub-district office network 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 email, but instead using a VPN network that is integrated into a local network between the head office and branch offices.

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.

4. Conclusion

After completing the stages of carrying out activities from needs analysis from design to testing and discussing the results, the following conclusions can be drawn:

1 Simulation design using Microsoft Visio 2013 application can be done virtually as a form of blue print before the application of the network system is improved.

2 Improved network security system by activating the IPSec feature found on the router so that the information backflow process is guaranteed confidentiality and security. 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, the security of the network system will increase due to IPSec supporters who perform automatic encryption of information sent on the network. The implementation of a VPN server network with the L2TP/IPSec method is fairly easy and can be done easily so that it does not require special skills that network administrators must have.

References

[1] Rahman, F., Sahari, S., & Robianto, R. (2020). *Building Lptp Vpn Network and User Management Using Fuzzy Logic Based on Age and Utilization of The Dude*

for Network Monitoring . KomtekInfo Journal, 7(1), 23-31.*https://doi.org/https://doi.org/10.35134/komtekinfo.v7i1.1201*

[2] Jogiyanto, Hartono. (2010). Information System Analysis and Design, Edition III.Yogyakarta: ANDI.

[3] Supendar, Hendra., & Handrianto, Y. (2017). *Frame Relay Techniques in Building a Wide Area Network With the Network Development Life Cycle Method.* Bina Insani ICT Journal, 4(2), 121-130.

[4] Eka, PIPA (2014) Computer Network Handbook, Bandung, Informatics Publisher.

[5] Technology, Citraweb, (2020). "Network Basics" *https://citraweb.com/article_see.php?id=67*.Accessed on November 29, 2020 at 08.30 WIB

[6] Patih, DFJ (2012). *Voip Server Design Analysis (Voice Internet Protocol) With Asterisk Opensource And VPN (Virtual Private Network) As i Network Security Between Clients*. Journal of Informatics and Applied Electrical Engineering, 1(1).

[7] Mufida, E., Irawan, D., & Chrisnawati, G. (2017). *Remote Site Mikrotik VPNWith Point To Point Tunneling Protocol (PPTP) Case Study at the Jakarta Global Lotus Foundation. MATRIX: Journal of Management, Informatics and Computer Engineering* , 16(2), 9-19.

[8] Meyatmaja, E., & Syafrizal, M. (2012).*Virtual Private Network Design at PT Pika Media Komunika .Data Management and Information Technology (DASI)* , 13(4), 11.

[9] Farly, KA, Najoan, XB, & Lumenta, AS (2017). Design and Implementation of VPN Server using SSTP Protocol (Secure Socket Tunneling Protocol) Case Study of Sam Ratulangi University Campus. Journal of Informatics Engineering, 11(1).

[10] Rudol. 2017. Implementation of Computer Network Security on Virtual Private Network (VPN) Using IPSec. Medan. Infotech Journal. 2: 65-68.

[11] Technology, Citraweb, (2020). "Network Interconnection with L2TP+IPSec".*http://www.mikrotik.co.id/article_lihat.php?id=152***.** Accessed on 23 November 2020 at 08.30 WIB.