INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES)
LLDIKTI WILAYAH X
Vol. 8, No. 2, Oct 2023
e-ISSN: 2502-0692

VIRTUAL PRIVATE NETWORK (VPN) BASED ON IP SECURITY DESIGN ON TOPOLOGY

Riandana Afira[*1], Radius Prawiro[2], Annisak Izzaty Jamhur[3]
[123] University Putra Indonesia YPTK Padang

*Correspondence should be addressed to riandanaafira@upiyptk.ac.id

Article Information

Submitted :
15 Jun 2023

Accepted :
20 Sept 2023
Published :
01 Oct 2023

Abstract

One way to maintain and improve the quality of service and security on the organization's network at the West Pasaman Regent Library and Archives Office is to add VPN functionality. Administrators always monitor traffic by accessing routers and access points to determine network status. Sometimes the administrator is on a public network and cannot access the router and access point because the obtained public IP address is dynamic (random). To overcome these problems, the Network Development Life Cycle (NDLC) approach is implemented by combining the L2TP and IPSec VPN protocol system that exists on Mikrotik. A VPN is a private, secure network that uses a public network like the Internet. One of the security foundations of VPN technology is Internet Protocol Security (IPSec). IPSec is a protocol used to secure datagram transmission over TCP/IP networks. This research aims to design and implement a Virtual Private Network (VPN) network system using public networks, which provides advanced security enhancements to the Internet using IPSec.

Keywords: VPN, Mikrotik, L2TP, IPSec

1. 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 Networt (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].

2. Research Method

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.

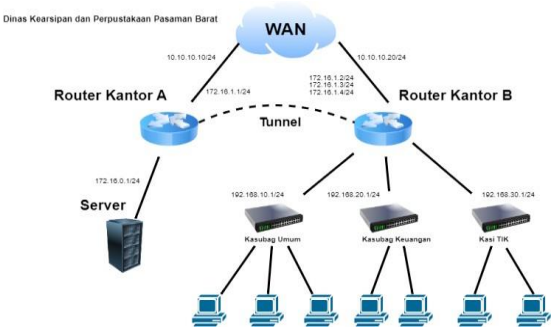

Figure 1. VPN + L2TP Network Topology

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.

3. Results of the Discussion

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 networkused.

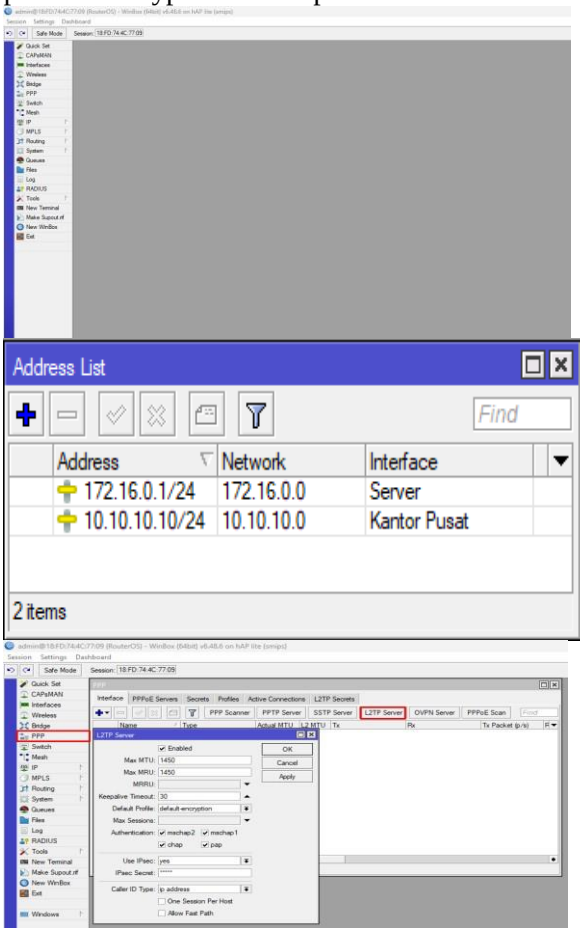

Figure 2. Win Box Configuration

WLAN1 and ether 2 are interfaces used for routers that function as gateways for connecting to the internet. 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 B. 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 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.

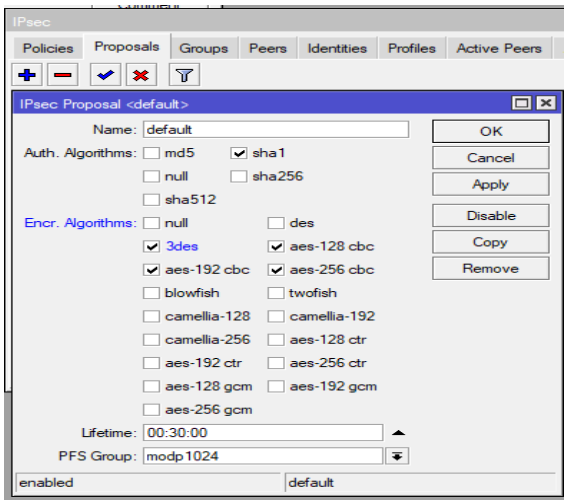

Figure 3. IPSec Protocol Configuration

From the results of the configuration made above, the VPN L2TP server and IPSec will automatically create their own rules indicating that the configuration results were successful.

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.

```
C:\Users\USER>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 4. Packet Lost Trafic Test

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. 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. 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.

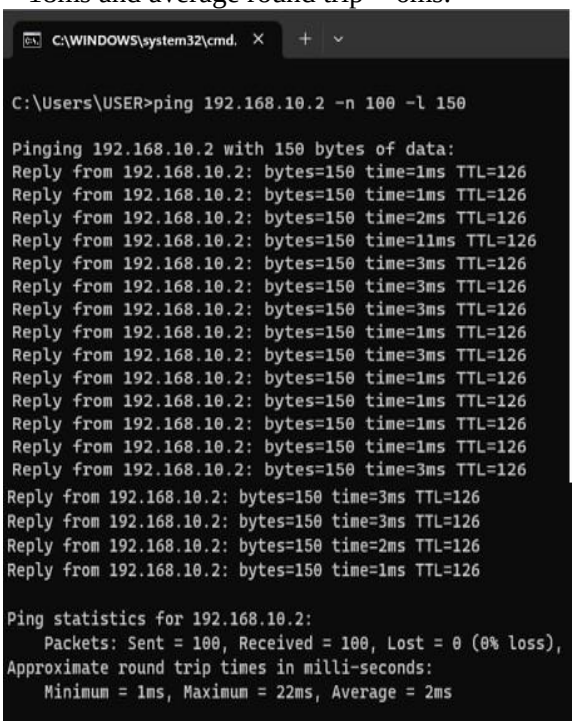

Figure 5. DoS Attack Network VPN Server to Client

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.

4. 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.

1. 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.
2. 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.
3. 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.

References

[1] Zhang, Z., Zhang, Y. Q., Chu, X., & Li, B. (2004). An overview of virtual private network (VPN): IP VPN and optical VPN. Photonic network communications, 7, 213-225.

[2] Knight, P., & Lewis, C. (2004). Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts. IEEE Communications Magazine, 42(6), 124-131.

[3] Bhat, A. Z., Al Shuaibi, D. K., & Singh, A. V. (2016, September). Virtual private network as a service—A need for discrete cloud architecture. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 526-532). IEEE.

[4] Cheung, K. H., & Mišić, J. (2002). On virtual private networks security design issues. Computer Networks, 38(2), 165-179.

[5] 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.

[6] Iqbal, M., & Riadi, I. (2019). Analysis of security virtual private network (VPN) using openVPN. International Journal of Cyber-Security and Digital Forensics, 8(1), 58-65.

[7] Iqbal, M., & Riadi, I. (2019). Analysis of security virtual private network (VPN) using openVPN. International Journal of Cyber-Security and Digital Forensics, 8(1), 58-65.

[8] 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.

[9] Duffield, N. G., Goyal, P., Greenberg, A., Mishra, P., Ramakrishnan, K. K., & van der Merive, J. E. (1999, August). A flexible model for resource management in virtual private networks. In Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication (pp. 95-108).

[10] Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN's protocols and security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(5), 919-932.