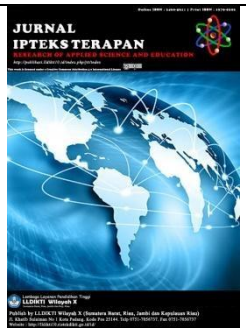

Vol.16 No.4 | Dec, 2022

IMPLEMENTATION OF VPN SERVER USING L2TP PROTOCOL AND IPSEC METHODS AS NETWORK SECURITY

Ruri Hartika Zain[1)], Retno Devita*[2)], Ipriadi[3)], Ondra Eka Putra[4)]
[1,2] Universitas Putra Indonesia YPTK Padang
* Corresponding Email: retnodevita@upiyptk.ac.id

Submit :
18/08/2022

Accept:
25/12/2022

Publish:
31/12/2022

Abstract

This think about points to plan a VPN arrange framework by utilizing a open organize, where this framework points to supply security by utilizing IPSec in giving private data through the L2TP burrow strategy from the server to the branch/client computer and bad habit versa. VPN is actualized utilizing layer 2 tunneling convention (L2TP) utilizing two Mikrotik routers. There are only many changes within the computer organize setup to play down costs and execution time. Tests are carried out to actualize security on the organize utilizing the command incite, where the admin watches bundle misfortune and delay parameters to discover out the increment in security quality on the organize.

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

doi : https://doi.org/10.22216/jit.v16i4 754-760
1979-9292 / 2460-5611 ©2021 © 2022 LLDIKTI Wilayah X
This is an open access article under the CC Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0/).
JIT is Sinta 3 Journal (https://sinta3.kemdikbud.go.id/journals/profile/2143) accredited by Ministry of Research & Technology, Republic Indonesia

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V16.i4 (754-760)
E-ISSN : 2460-5611

INTRODUCTION

The advancement of Data Innovation is right now exceptionally quick, particularly the Web, in any case, the improvement of innovation features a awful affect on offices that don't have solid sufficient security, particularly in terms of organize security, indeed in spite of the fact that the security has numerous sorts of security protocols. One of them is like an organization or company where there's so much vital data information that can be stolen due to unreliable people, in this manner a strategy is required to decrease indeed anticipate different acts of burglary of data or aggressors carried out by means of the Internet. Virtual Private Organize (VPN) is one way to prevent and protect the trade of data information through the web arrange. VPN itself could be a communication innovation that allows associations from open systems and employments them like a neighborhood organize and indeed joins the neighborhood arrange itself. By employing a open organize, clients can get to data on the neighborhood organize, get the same rights and settings [1].

One of the VPN administrations found on Mikrotik is Layer 2 Tunneling Convention (L2TP), particularly utilizing L2TP can offer assistance trade data and progress organize security between a few systems through a burrow that passes through the web arrange securely. L2TP is an expansion of PPTP additionally L2F. Arrange Security and encryption utilized for confirmation are the same as PPTP, more often than not for superior security with this VPN, data information security and organize security are way better than past VPN administrations [1]. The IPSec convention gives a Web Key Trade (IKE) that can fulfill the require for verification and make an assention between 2 computers, called the Security Affiliation (SA). Verification and assention between the 2 computers are put away in a advanced certificate that must be possessed by the server and client.System advancement is characterized as an exertion to get ready a unused framework to supplant the ancient framework as a entirety or make strides the existing system [2]. A computer arrange may be a relationship. The devices in question are PCs, laptops, smartphones, routers, switches, hubs and other connecting devices [4]. Internet is short for interconnection networking with computer network coverage that is wider than WAN. To get internet access, a separate protocol is needed, namely the TCP / IP (Transmission Control Protocol / Internet Protocol) protocol in order to exchange packets of users around the world [5]. VPN is a virtual connection that is private, so called because basically this network does not exist physically only in the form of a virtual network VPN connects computers to public networks or the internet but is private, because it is private so not everyone can connect to this network and access it. . Therefore, information security is needed in a VPN. In the

This work is licensed under a Creative Commons Attribution 4.0 International License

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V16.i4 (754-760)
E-ISSN : 2460-5611

VPN there is a tunnel, the tunnel itself is a generic term that explains that a connection between points on a computer network is carried out through a kind of tunnel between the two points [6].

Tunneling is the basic foundation of a VPN system whose job is to establish, handle and provide point-to-point connections from the source to its destination where the process of this private network is useful for capturing all packets of information, and encapsulating them or wrapping them with other packets before sending them over a network[7]. In the tunneling process, three different protocols are involved, namely (1) Carrier Protocol, the protocol used by the network where information travels on it such as TCP/UDP, (2) Encapsulating Protoco, this protocol silences the original data in it such as IPSec, L2TP, (3) Passanger Protocol, a protocol that receives original data from servers such as IP[8]. *L2TP* is a development of PPTP plus L2F. The Network Protocol and encryption used for authentication is the same as PPTP. Usually for better security, L2TP is combined with IPSec, becoming L2TP/IPSec. However, the client side must also support IPSec when implementing L2TP/IPSec. In terms of encryption, L2TP/IPSec has a higher security level than PPTP which only uses MPPE. The L2TP protocol is also often referred to as a virtual dial-up protocol, because L2TP extends a Point to Point Protocol (PPP) dial-up session over the public internet network [9].

(IPSec)

IPSec is a protocol used to secure the transmission of datagrams on a TCP/IP-based network. IPSec is an open standards framework developed by the Internet Engineering Task Force (IETF). IPSec offers 3 main services, namely authentication and data integrity, confidentiality, and key management [10]. To be able to meet the security needs of L2TP, it is necessary to try the implementation of security by using the IPSec transport type protocol or better known as the L2TP over IPSec protocol, so that the information packets sent by the L2TP protocol will be encapsulated by the IPSec protocol [11].

RESEARCH METHODS

The method used in the development of the Network Development Life Cycle (NDLC) system which is a method that depends on the process of designing and developing a business network that allows network monitoring to occur to find out statistics and network mechanisms so that a top-down approach can be carried out. This method is a continuous improvement method where the results of the analysis will continue to be used as material for consideration to carry out continuous improvement research [3]. Based on the identification of the problems above, the researchers conducted data analysis first. This is so that the problem solving can produce a new solution. At the design stage of the

This work is licensed under a Creative Commons Attribution 4.0 International License

ISSN : 1979-9292

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V16.i4 (754-760)

E-ISSN : 2460-5611

network topology with the L2TP and IPSec methods as network security using the Cisco packet tracer application as a replica of the system to be run. This testing session is carried out to identify whether the simulation of the network can run successfully without errors with the initial planning. Testing is tried on only one server computer and several client computers for the purpose of identifying whether the design matches the initial plan. Testing the VPN server is tried by testing the connectivity of request reply information packets to the internet network via the proxy feature.

RESULTS

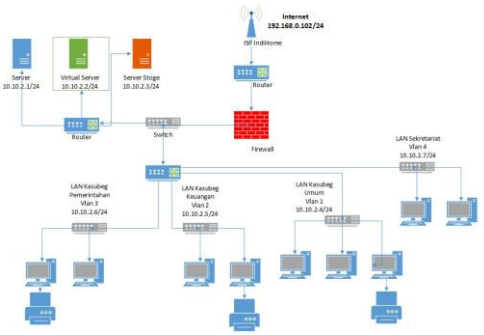

Figure 1. LAN Topology Schematic

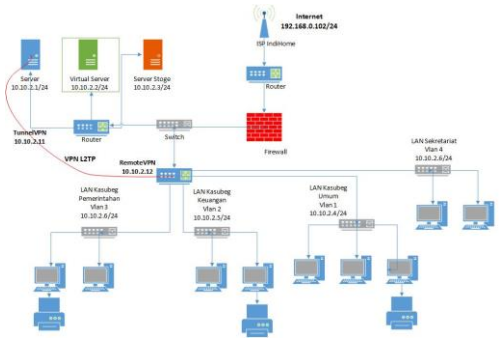

Figure 2. L2TP VPN Network Topology Schematic

In proposing a organize topology to be actualized, it'll not alter the shape of the existing topology, since the shape of the topology utilized is as of now exceptionally great. The topology used could be a star topology. And it is proposed to utilize a VPN to communicate or trade private information to be more secure. Within the L2TP VPN network plan, there are a few steps that must be carried out, a framework that's in agreement with the plan will make it simpler to oversee organize setup and not make an director not confounded in overseeing it.

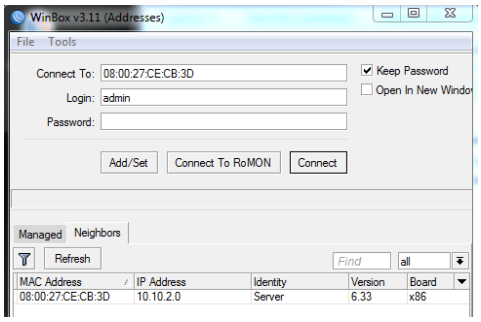

Figure 3. Configuration Shematic

Arrange NAT on the firewall. NAT is an IP address mapping so that numerous private IPs in a LAN can get to open IPs. After introducing the Mikrotik, the following step is to design NAT through the terminal. After shaping a server setup to be able to put through to the web, the following step is to make a intermediary arrangement to form VPN innovation. The primary menu determination is selecting the PPP menu on the cleared out side of the winbox until the PPP exchange box shows up. Within the PPP discourse

This work is licensed under a Creative Commons Attribution 4.0 International License

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V16.i4 (754-760)
E-ISSN : 2460-5611

box, select the L2TP server menu until the L2TP server discourse box shows.

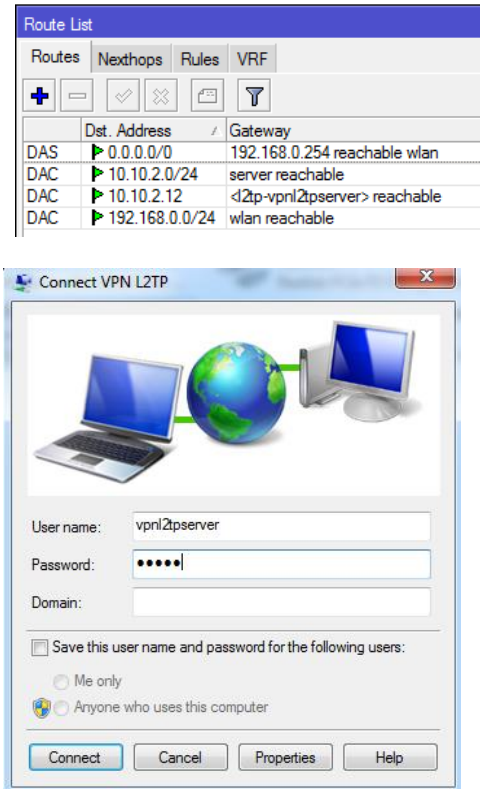

Figure 4. L2TP Secret Creation

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

This test is valuable to see association resistance when in ddos assault. Testing is done with the pingflood.exe application. After testing by sending 4 information bundles of 25 kb, the comes about appeared that the organize was not disengaged and the most extreme circular trip was 2ms. Parcel misfortune testing was carried out a few times with the "ping" command to the goal IP employing a command provoke to see the solidness of the association on a open organize utilizing L2TP/IPSec VPN. And the result is thatfor information max and normal circular trip a bundle is still inside a sensible. From the try of 9 parcels, max circular trip = 3ms and normal circular trip = 1ms. This test is valuable to see association resistance when in ddos assault. Testing is done with the pingflood.exe application. After donetesting by flooding the VPN server with 28 information bundles of 25kb. The information gotten for max and normal circular trips of a parcel are still inside sensible limits.

CONCLUSION

After completing the stages of carrying out exercises from needs examination from plan to testing and talking about the comes about, the taking after conclusions can be drawn: 1 Simulation plan utilizing Microsoft Visio 2013 application can be done for all intents and purposes as a shape of blue print some time recently the application of the organize framework is improved. 2

This work is licensed under a Creative Commons Attribution 4.0 International License

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V16.i4 (754-760)
E-ISSN : 2460-5611

Improved arrange security framework by actuating the IPSec include found on the switch so that the data backflow handle is ensured secrecy and security. IPSec can moreover be combined with other security frameworks such as intermediaries and firewalls, in arrange to actualize layered security on the arrange or too called numerous layer security. 3 By employing a VPN Server arrange with the L2TP/ IPSec strategy, the security of the organize framework will increment due to IPSec supporters who perform programmed encryption of data sent on the arrange. The usage of a VPN server arrange with the L2TP/IPSec strategy is decently simple and can be done effectively so that

BIBLIOGRAPHY

[1] Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. TEKNOKOM, 4(1), 30-36.

[2] 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.

[3] 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).

[4] Singh, K. K. V., & Gupta, H. (2016, March). A New Approach for the Security of VPN. In Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies (pp. 1-5).

[5] Singh, K. K. V., & Gupta, H. (2016, March). A New Approach for the Security of VPN. In Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies (pp. 1-5).

[6] 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.

[7] Zhou, Y., & Zhang, K. (2020, June). DoS vulnerability verification of IPSec VPN. In 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 698-702). IEEE.

[8] Luo, J., & Ji, Q. (2020, October). Password Acquisition and Traffic

This work is licensed under a Creative Commons Attribution 4.0 International License

Decryption Based on L2TP/IPSec. In 2020 IEEE 20th International Conference on Communication Technology (ICCT) (pp. 1567-1571). IEEE.

[9] Sawalmeh, H., Malayshi, M., Ahmad, S., & Awad, A. (2021, September). VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements. In 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT) (pp. 236-241). IEEE.

[10] Angelo, R. (2019). Secure Protocols And Virtual Private Networks: An Evaluation. Issues in Information Systems, 20(3).

This work is licensed under a Creative Commons Attribution 4.0 International License