Journal of Computer Science and Information Technology
https://jcsitech-upiyptk.org/ojs
2021 Volume 7 Issue 3 Hal: 64-69 e-ISSN: 2502-1486

Analysis of Ethernet Over Internet Protocol (EOIP) VPN Performance

Ahmad Purwana
Universitas Putra Indonesia YPTK Padang
wawanw807@gmail.com

Abstract

The need for interconnection between networks will be needed, especially in a company that has many branch offices, but companies usually demand a minimum use of resources in order to get maximum results. To overcome this problem, a Virtual Private Network (VPN) network is needed by utilizing the EOIP protocol, Ethernet Over IP (EOIP) is a protocol on Mikrotik RouterOS which functions to build a network tunnel between Mikrotik routers on a TCP / IP connection, namely by utilizing internet connection as a liaison. This study aims to analyze the performance of VPN by using the concept of Ethernet Over Internet Protocol (EOIP) on the existing network at PT. Energy Source Dempo. This analysis is needed to manage network access to connected data in each branch of the company. This is to anticipate access rights that enter the network owned by PT. Energy Source Dempo. The results of the analysis provide easy access rights and provide a sense of security from the data communication that occurs. In addition, the results of the analysis can also be used as network management control at PT. Dempo Sumber Energi so that the results of the analysis can maximize data communication performance.

Keywords: EOIP, VPN, Mikrotik, Communication, Network.

1. Introduction

Along with the rapid development of computer network technology today, especially in the field of the internet, causing everyone to be free to communicate with each other or exchange information in the internet world [1]. The negative side of this development arises when one's privacy begins to be disturbed. Because everyone has different interests and privacy. For example, a company that has many branches wants to send important confidential data to other branch offices via the internet, this is certainly very vulnerable to being hijacked or stolen by people who have other interests. One of the new technologies that are currently being developed to prevent this is Virtual Private Network (VPN)[2].

Virtual Private Network (VPN) is a way to make a network private and secure by using a public network such as the internet. A Virtual Private Network (VPN) can send data between two computers that pass through a public network so that it seems as if it is connected point to point so that data passes through a public network and can reach its final destination [3]. In other words, a Virtual Private Network (VPN) is able to create a private network within a public network. Virtual Private Network (VPN) is a technology that is widely used by large companies, especially in the banking world. There are various methods that can be used to build a Virtual Private Network (VPN), one of which is Ethernet Over Internet Protocol (EOIP) [4].

Computer networks are an important point in companies that have many branch offices for the coordination process of data transfer. PT Indo Matra Lestari connection uses a VPN system with the PPTP method [5]. The Data Center is used as a VPN server, the clients are the Head Office and Citereup Branch Offices. Between the Head Office and the Citereup Branch Offices there is no direct connection so that accessing data between the Head Office and the Citereup Branch Offices becomes slow, because the data must pass through the Data Center before reaching its destination. Moreover, the data accessed is private for the company and is only accessed on the local network. The solution used to create a direct and secure network path between the Head Office and Branch Offices is to use the EOIP Tunnel on a mikrotik router. The tunneling method on EOIP can create network bridging between Mikrotik devices, the EOIP Tunnel will turn into a Virtual Interface on the Mikrotik router so that it seems as if the Mikrotik routers are connected locally [6].

In this sophisticated era, an internet connection with reliable security is very much needed by business owners who deal with internet connections every day. The use of a Virtual Private Network (VPN) on a communication network aims to limit access from the public to the private network. Large organizations with several branch offices can use the internet to carry out the coordination process, so they can cut costs for business trips or for meetings between branch offices. Where the implementation of the Virual Private Network (VPN) network can be replaced by using the Ethernet over Internet Protocol (EOIP) Tunnel [7]. This EOIP tunnel feature is only available on Mikrotik routers. The routing protocols used in the EOIP tunnel network configuration are OSPF and RIPv2, then the results between these routing protocols are compared with their QoS to determine which one is better.

Recived 25 February 2021; Revised 27 March 2021; Accepted 20 June 2021| doi: 10.35134/jcsitech.v7i2.1

Simulation using GNS3 software is used to run an EOIP tunnel simulation between OSPF and RIPv2 and address devices that will communicate with each other using Internet Protocol version 4 (IPv4) then the simulation results are seen from the Quality of Service [8].

Ethernet Over Internet Protocol (EOIP) is a feature of the Mikrotik Router OS that builds a network tunel between Mikrotik routers on a TCP/IP connection. Ethernet Over Internet Protocol (EOIP) protocol developed by MikroTik where this protocol is able to shorten the distance between Ethernet in an office and other branch offices by combining or bridging the Ethernet Over Internet Protocol (EOIP) tunel with the office Ethernet, so Ethernet Over Internet Protocol (EOIP) has a very fast data transfer rate from source to destination (throughput) even though it passes through two-three or even ten routers at once.

The work of EOIP as an intercity based on EOIP Tunnel between Bandung and Bekasi can be done well because both routers on the Bandung and Bekasi sides use Static IP Public and sufficient internet bandwidth [9]. The quality of the EOIP Tunnel connection is very dependent on the quality of the internet from both sides of the router, if one router experiences interference or degradation of bandwidth quality, it will affect the speed and capacity of the EOIP Tunnel [10].

This study aims to conduct research at PT. Dempo Sumber Energi which is engaged in Construction. Basic this company uses the internet as a medium for distributing data to support communication activities between existing branches of the company. This allows employees to access data remotely which of course must also be supported by a good, fast, reliable and secure computer network infrastructure to support activities. In this case PT. Dempo Sumber Energi requires a secure and stable connection when connecting or accessing data. So it is necessary to do a private network analysis process using the Ethernet Over IP (EOIP) protocol. The results are expected to make it easier for users to access data on the office server without having to be constrained by time and place to produce better performance.

2. Research Method

The research framework is a plot contained in the research. The research framework describes the stages and concepts that will be carried out in the research. The following stages of research can be seen in Figure.1 as follows:

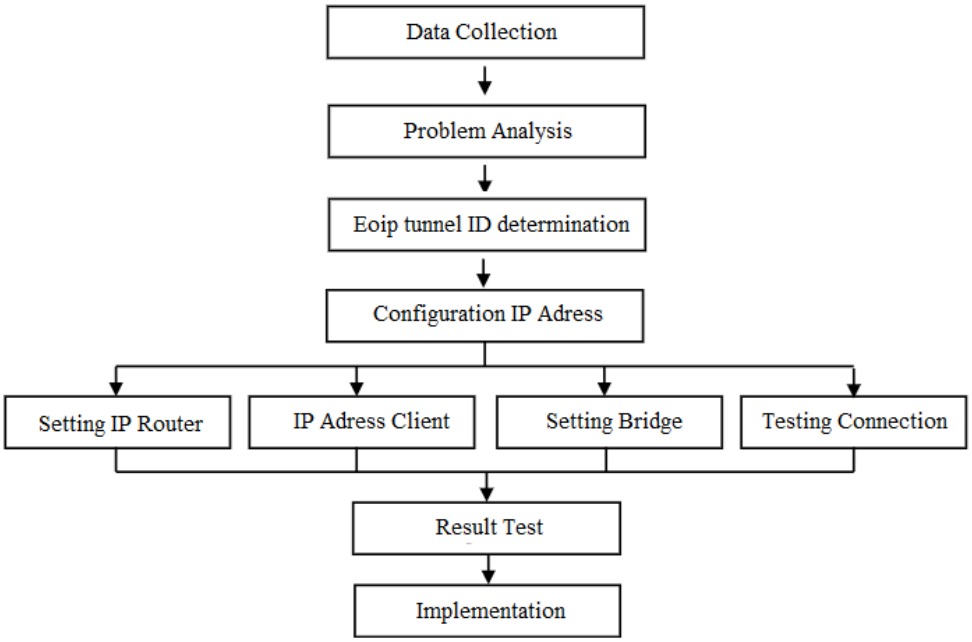

Figure.1 Research Stages

The research stages explain the steps in recording data and collecting several reports that are needed to be used as guidelines in making this research starting from preliminary research carried out by approaching the object of research. The purpose of this stage is to find out the problems that occur appropriately, so that research is expected to provide the most optimal solution to solving these problems.

The problem that has been successfully obtained is the use of internet network access at PT Dempo Sumber Energi which is less secure and unstable in connecting or accessing data from branch offices to their head office. Therefore, the author wants to do an analysis to get results and assess how the performance of the network quality at PT Dempo Sumber Energi and whether it is in accordance with the internet network category according to Ethernet Over Internet Protocol

(EOIP). At the analysis stage it becomes the basis for system design, such as determining the ID used in the EOIP tunnel, determining the virtual IP address used in the tunnel, using the client IP address for each branch office and designing the network topology used, In this EOIP configuration make it easier for branch offices to make long-distance connections using tunnels via the internet, in addition to being economical and efficient in equipment, security in the data communication process is easily affordable.

2.1 Network Basic Concepts

A computer network is the interconnection of several autonomous (independent) computers that can share information (and resources) with each other [11]. A network usually consists of two or more computers that are interconnected with each other, and share resources such as CD-ROMs, printers, file exchanges, or allow to communicate with each other electronically. The connected computers may be connected to cable media, telephone lines, radio waves, satellite or infrared [12]. Computer networks can also be interpreted as "interconnections" between 2 or more autonomous computers, which are connected by wired or wireless transmission media. Autonomous is when a computer does not control another computer with full access, so that it can make another computer, restart, shut down, lose files or damage the system [13].

2.2 Virtual Private Network (VPN)

Virtual Private Network (VPN) is a computer network technology developed by a large-scale company that connects networks over other networks using the internet that requires privacy lines in communication. In more technical terms, the link layer virtual network protocol is said to be a tunnel or tunnel that passes through the underlying transport network. The term VPN can be used to describe a wide variety of network configurations and protocols [14]. VPN networks can be called secure because all data transmitted through a tunnel (tunnel) is always encrypted using certain algorithms, depending on the protocol used. VPN components and technologies can be seen in Figure.2 below [15]:

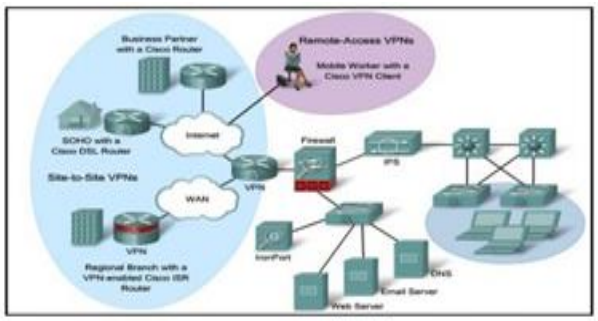

Figure. 2 VPN Components and Technology

VPN technology provides three main functions for its use, namely [16]:

A. Confidentially

VPN technology has a working system of encrypting all data that passes through it. With this encryption technology, the confidentiality of data becomes more awake. Although there are parties who can intercept data that passes through the internet and even the VPN line itself, they may not necessarily be able to read the data, because the data has been scrambled. By implementing this encryption system, no one can access and read the contents of the data network easily.

B. Data Integrity (Data Integrity/Data Authenticity)

When passing through the internet network, data actually has traveled very far across various countries. During the journey, various disturbances can occur to the contents, either lost, damaged, or manipulated by people who are not supposed to. VPN technology will maintain the authenticity of data by ensuring that the data that arrives is still the same as when it was sent.

C. Origin Authentication (Source Authentication)

VPN technology has the ability to authenticate the sources that send data to be received. The VPN will check all incoming data and retrieve information from the data source. Then the address of the data source will be approved if the authentication process is successful. Thus, a VPN guarantees that all data sent and received comes from the source it is supposed to be. No data is falsified or sent by other parties.

2.3 Ethernet Over Internet Protocol (EOIP)

Ethernet over Internet protocol is a protocol developed by Mikrotik OS that creates an Ether Tunnel connection between two routers using a TCP/IP connection [17]. The EOIP interface looks like a normal ethernet interface (logically). When the bridging function is enabled, all data transmitted via the ethernel protocol on the two routers will be bridged as if the two routers were connected by a cable. The order of encapsulation in the EOIP protocol is, first the internet protocol (IP) at layer 3 will be encapsulated using ethernet II technology at layer 2. The results of the encapsulation then encapsulate the GRE (Generic Routing Encapsulation) protocol. This EOIP uses the generic routing encapsulation protocol -GRE (RFC1701) [18]. It is in this way that the EOIP tunnel formation process occurs and is used to transmit and transmit data. The EOIP protocol tunnel works using a tunnel ID which must be the same value between the two routers that have an EOIP interface in forming an EOIP tunnel [19].

3. Result and Discussion

3.1 System analysis

Before doing the EOIP Test running on the Mikrotik network, hardware and software are needed so that the simulation can run well. To provide an overview of the

current working system on the old computer network system at PT Dempo Sumber Energi using a wireless router with a tree topology circuit with a total bandwidth of 100 mb, where all computers are connected to users using a wireless router. All computers can be connected to the internet, but due to the limited available bandwidth, on certain days and during peak operational hours there are often connection problems when communicating, sending company data.

3.2 Network Topology Design

The network topology image at PT Dempo Sumber Energi can be seen in Fig. 3 below:

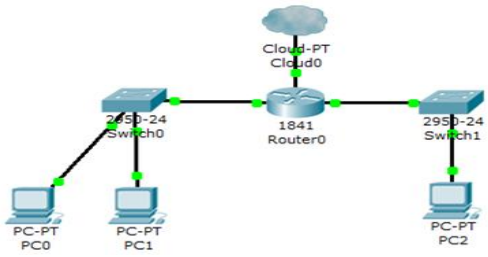

Figure. 3 Network Topology PT. Energy Source Dempo

From the topology obtained, it can be explained that the tree topology is a combination of two existing network topologies. The combination of these topologies, namely bus topology and start topology, consists of several groups of workstations using a start topology connected to the main cable (coaxial) using a bus topology.

3.3 Ethernet Over IP (EOIP) Analysis

This research will design Ethernet Over IP (EOIP) in a network using hardware and software. Researchers will compare before designing Ethernet Over IP (EOIP) and after designing Ethernet Over IP (EOIP) to identify and evaluate problems in the system. Before configuring each Mikrotik Router, the IP settings for each client are first made.

1. Set the IP on the client

Set the IP address according to their wishes using the Ip address 192.168.13.2 and because on router1 192.168.13.1 the gateway is filled according to the router1 owned:

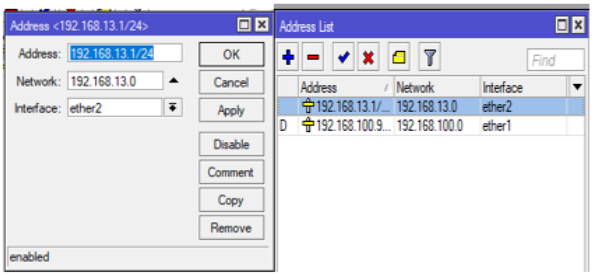

Figure. 4 Setting IP Adress

IP address is a unique addressing system for each host connected to a TCP/IP-based network, the IP address can be analogous to a home address.

2. DHCP Client Settings

DHCP Client is used to get an IP address allocation from the ISP, which can later be used to connect to the internet. The steps are by clicking the IP|DHCP Client + menu Click + blue.

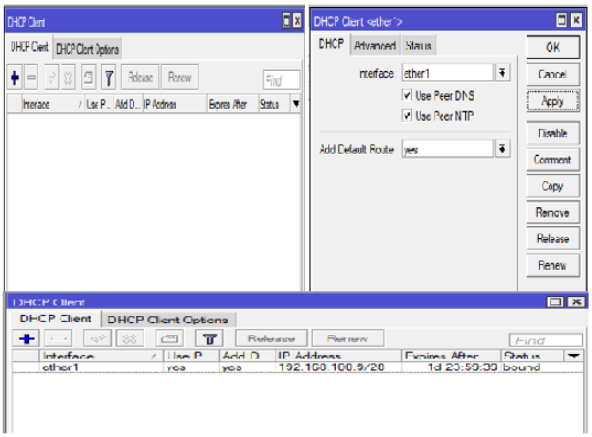

Figure. 5 Setting DHCP Client

3. NAT Firewall Settings

NAT or also known as Network Address Translation is a method of connecting more than one computer to the internet using one IP address. The results of the NAT Firewall settings can be seen in Fig. 6 below:

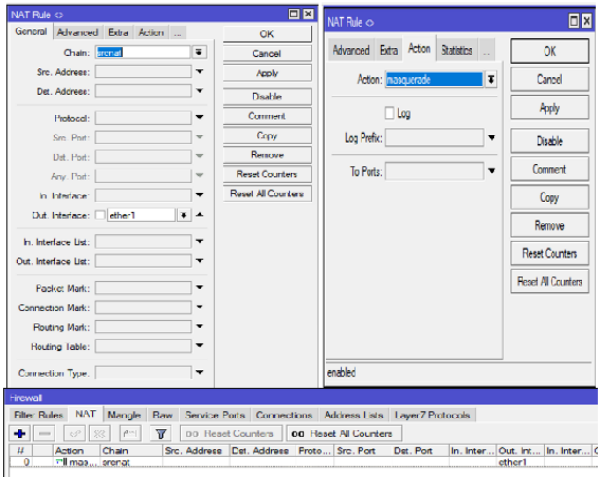

Figure. 6 Setting Firewall

4. Create an EOIP tunnel.

EOIP Tunnel is a protocol on Mikrotik that functions to build a network tunnel between Mikrotik routers over a TCP/IP connection. The steps, click the Interface menu | click + | fill in the name column with EOIP-tunnel1| on the remote address enter the opponent's public IP| in the Tunnel ID, enter the number to be generated:

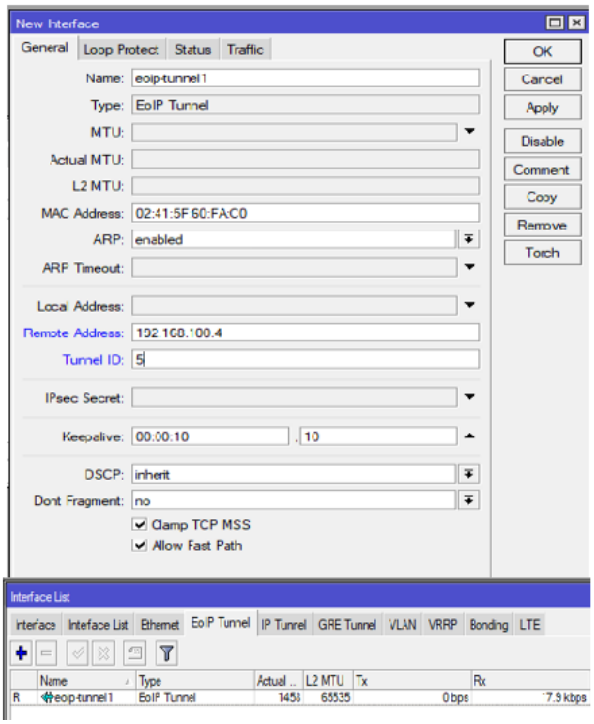

Figure. 7 Display of creating EOIP Tunnel

5. Make a Bridge

Bridge is a network component that is used to expand the network or create a network segment. The steps work, click the Bridge menu, click + apply + ok. The results of the work of making the Bridge can be seen in Fig. 8:

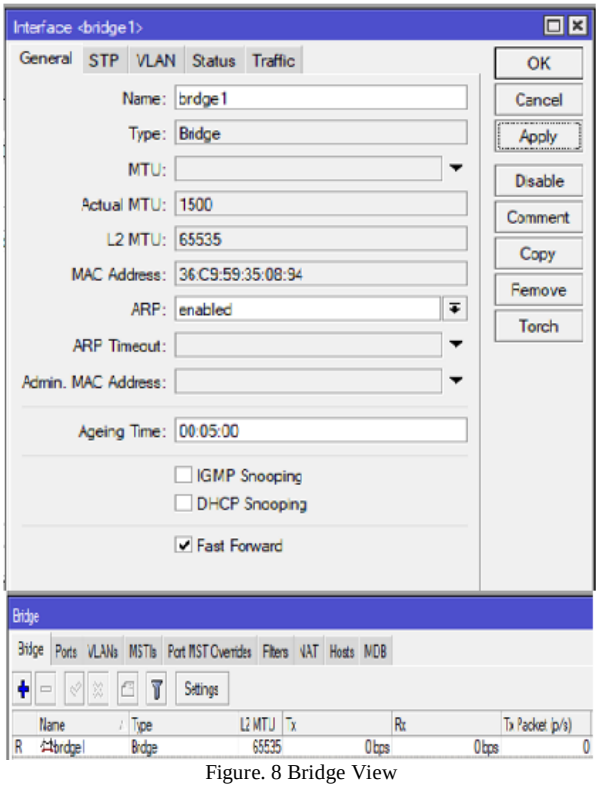

Figure. 8 Bridge View

3.3 EOIP Network Testing

Network testing is carried out after the EOIP Tunnel is created in the configuration above. The final result of the tests carried out is to perform a traceroute or jump from one host to another. Testing is done on the user side who is on a different router. In the final result, this network test was carried out based on ping and traceroute tests to the branch and central offices to find out that the data path sent either from the center to the branch or vice versa was the path through the pre-configured EOIP-tunnel gateway. At this testing stage, a connection test will be conducted to pcB, Router1, and Router2 by means of a ping test, for the IP address of Router2 with IP 192.168.13.254, IP address for Router1 with IP 192.168.13.1 and IP address for pcB with IP 192.168.13.253. Here are the results of the ping test capture.

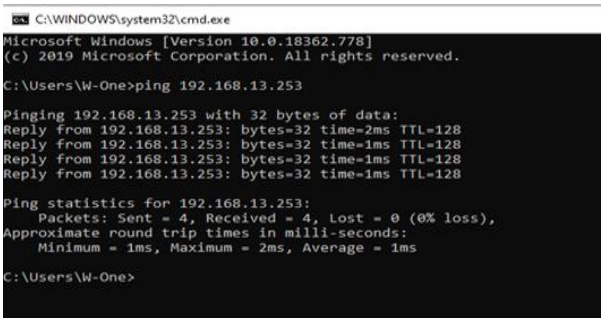

Figure. 9 Network Connection Test Results

After the occurrence of an existing intranet connection, the network can share access and then to form a Wide Area Network (WAN) scale network so that it can utilize the resources of the entire existing network to connect to the existing LAN network without having to make a user authentication first. Folder permissions can be set by the system administrator so that not all users can access folders that are not in the related division.

4. Conclusion

In the discussion described earlier, some conclusions that the author found in the form of a VPN design using the access built by EOIP that the author did can make it easier for employees of PT Dempo Sumber Energi to be able to access company data and systems remotely by connecting computers between branches through the network. Internet connection. The application of a VPN using the EOIP method can help make Point to Point connection lines between Mikrotik devices faster in data access because the data access goes directly to the destination so as to provide stable and secure network access. Not all applications can be passed to the internet network for reasons of application limitations and security itself to connect two or more offices, then a VPN using access built by EOIP can facilitate internet access at a relatively low cost and suitable for remote internet network access.

References

1. Farly, K. A., Najoan, X. B. N., & Lumenta, A. S. M. (2017). Perancangan Dan Implementasi Vpn Server Dengan Menggunakan Protokol Sstp (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *11*(1). https://doi.org/10.35793/jti.11.1.2017.16745.
2. Haryanto, M. D., & Riadi, I. (2014). Analisa Dan Optimalisasi Jaringan Menggunakan Teknik Load Balancing. *Jurnal Sarjana Teknik Informatika*, *2*, 1370–1378. http://www.mendeley.com/research/analisa-dan-optimalisasi-jaringan-menggunakan-teknik-load-balancing.
3. Hasibuan, M. S. (2016). Keylogger pada Aspek Keamanan Komputer. *Teknovasi*, *3*(1), 8–15.
4. Kuswanto, H. (2017). Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EOIP. *Paradigma*, *19*(1), 46–51.
5. Lan, K. B. (2019). *729-Article Text-2577-1-10-20190628*. *4*(1).
6. Madcoms (2015), Membangun Sistem Jaringan Komputer Untuk Pemula. Yogyakarta .
7. Mutaqin, A. F. (2016). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. *Jurnal Sistem Dan Teknologi Informasi*, *1*(1), 1–6.
8. Muzawi, R. (2018). Jurnal Edik Informatika Penelitian Bidang Komputer Sains dan Pendidikan Jurnal Edik Informatika Pengaturan Bandwidth dan QoS Pada PC Router Menggunakan Kernel Gnu / Linux dan FreeBSD. *Pengaturan Bandwidth Dan QoS Pada PC Router Menggunakan Kernel Gnu/Linux Dan FreeBSD*, *2*(January), 80–82. https://doi.org/10.13140/RG.2.2.10700.92809.
9. Oktivasari & Andri Budhi Utomo, P., & Andri Budhi Utomo, P. (2016). Analysis of Virtual Private Network Using Openvpn and Point to Point Tunneling Protocol - Analisa Virtual Private Network Menggunakan Openvpn Dan Point to Point Tunneling Protocol. *Jurnal Penelitian Komunikasi Dan Opini Publik*, *20*(2), 123903.
10. Rifkie Primartha (2019), Manajemen Jaringan Komputer Bandung: Informatika.
11. Sahari, & Putra, O. A. (2015). Implementasi Point to Point Tunneling Protocol (Pptp) Pada Jaringan Virtual Private Network (VPN) Dan Bandwidth Manajement Dengan Routerboard Mikrotik. *Prosiding Seminar Ilmiah Nasional Teknologi Komputer (SENATKOM)*, *1*(Senatkom), 610–619.
12. Sirait, F., Studi, P., Elektro, T., Teknik, F., Buana, U. M., Studi, P., Elektro, T., Teknik, F., & Buana, U. M. (2018). *Jurnal Teknologi Elektro, Universitas Mercu Buana ISSN: 2086 - 9479 Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan Fadli Sirait Program Studi Teknik Elektro, Fakultas Teknik ISSN: 2086 - 9479*. *9*(1), 16–22.
13. Sutara, B. & sutrisno. (2018). Layanan Jaringan Internet Pada Virtual Private Network (Vpn) Menggunakan L2Tp Untuk Peningkatan Keamanan Jaringan. *Jurnal ICT: Information Communication & Technology*, *16*(1), 1–6.
14. Suyuti Ma'sum, M., Azhar Irwansyah, M., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *5*(1), 56–60.
15. Umam, C., & Roza, E. (2016). Perancangan Jaringan Keamanan Virtual Private Network (VPN) Siteto Site. *Perancangan Jaringan Keamanan Virtual Private Network (VPN) Siteto Site Chairul*, 23–30.
16. VARIANTO, E., & MOHAMMAD BADRUL. (2015). Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt.Valdo International. *Jurnal Teknik Komputer Amik Bsi*, *1*(1), 55–56.
17. Warman, I., & Hanafi, A. (2019). Analisa Perbandingan Kinerja Generic Routing Encapsulation (GRE) Tunnel Dengan Point to Point Protocol over Ethernet (PPPoE) Tunnel Mikrotik Routeros. *Teknoif*, *7*(1), 58–66.
18. Watrianthos, R., & Nasution, M. (2019). Analisa Kemampuan Transver Data Vpn Berbasis Open Source Pada Kondisi Encripsi-Dekscripsi Dan Komprensi-Dekomprensi. *Jurnal Informatika*, *6*(1), 23–51. https://doi.org/10.36987/informatika.v6i1.740.
19. Wongkar, S., Sinsuw, A., Najoan, X., Studi, P., Informatika, T., Teknik, F., & Ratulangi, U. S. (2015). Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan Lan Dan Wlan Di Desa Kawangkoan Bawah Wilayah Amurang Ii. *Jurnal Teknik Elektro Dan Komputer*, *4*(6), 62–68. https://doi.org/10.35793/jtek.4.6.2015.10400.