International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 58-65
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

Analysis of Security Virtual Private Network (VPN) Using OpenVPN

Muhammad Iqbal[1], Imam Riadi[2]
[1]*Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[2]*Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
(muhammad12018182@webmail.uad.ac.id, imam.riadi@is.uad.ac.id)

ABSTRACT

Data transmission on the network of Informatics Engineering Research Laboratory Universitas Ahmad Dahlan using an unsecured public internet network, in order to be able to access the network from crossing actions and search for data traffic. One solution that can be done is with Virtual Private Network techniques using OpenVPN in learning networks. This research describes attempts to make a Virtual Private Network using the OpenVPN network design in the research laboratory of Informatics Universitas Ahmad Dahlan and how big the level of security. The results of implementing Virtual Private Network using OpenVPN is that the attempt gives a positive result, this is evidenced by the sniffing of data that cannot detect the username and password sent. Quality of Service measurement results experienced a decline in network quality with delay parameters rising from 51.4 ms to 463.4 ms, packet loss rose from 7.8% to 20.2%, throughput dropped from 82.8% to 71.6%, and bandwidth dropped from 64786.6 bit/s to 55589 bit/s, it is due to the encryption process and encapsulation that takes time.

Keywords:
OpenVPN, Mikrotik, Analysis, Security, QoS.

1 INTRODUCTION

Informatics research laboratory of Universitas Ahmad Dahlan (UAD) which can be used for students to conduct research primarily in the field of the internet network, and research in the lab, lots of data are not allowed to be published and confidential, but nowadays the available networks in research laboratory have not completely safe from the action of tapping the data so that it gave rise to fears of impending attack by the attacker who can intercept this data from outside the area over a network the Internet. Therefore research laboratory needs a security system can protect data from the action of hacking and data-sniffing by using Virtual Private Network (VPN) with OpenVPN.

The basic idea of a private network VPN can be used as an advantage of an open communications network infrastructure. A VPN is needed to specify a certainty that the confidentiality of sensitive data can be kept transmitted on the network a Local Area Network (LAN) or workable so that only authorized users are able to access sensitive data. The VPN system integrated into the communication system is able to realize security is very high, so as to guarantee a secure VPN that has been realized by the use of encryption and decryption.

The advantage of a VPN using the OpenVPN is a local chain owned will be wide, the time it takes to connect the local network to other places also getting faster. Reduces operational costs when compared with the use of a leased line as a traditional way to implement WAN. A VPN can reduce the cost of making the network because it does not require wires (leased line). Increase scalability as well as giving ease to be accessed from anywhere because a VPN to connect to the internet (Remote Access). OpenVPN uses the mechanism of Secure Sockets Layer/Transport Layer Security (SSL/TLS), SSL/TLS uses one of the best encryption methods namely asymmetric encryption. On asymmetric encryption, each server and client has 2 keys, namely public key and private key.

Results of the network observation in this research laboratory are not using VPN so for the security of data sent and received is not fully safe from assault and tapping. According to a study of the literature, that the network security and data transfer security method can use VPN, therefore the author analyzes the network security and Quality of Service (QoS) from the VPN using the OpenVPN and analyze the level of eligibility OpenVPN's security itself.

2 BASIC THEORY

2.1 Computer Network

Computer networks there are a variety of the following types of computer network based on scope. The scope here is how big the computer network will be built. Based on spaces in scope, a computer network can be distinguished into three, namely [1] :

a) *Local Area Network (LAN),* is a computer network which is built in the room a small scope as a single building or group of buildings. LAN is built in a limited scope and usually owned by organizations that already have the devices installed. An internal data rate of the LAN is usually much greater than the WAN.
b) *Wireless Networks*, are widely used in environmental business. Wireless technology is also common for both large areas of voice and data network networks. It gives the advantage in the field of wireless mobility and ease of installation and configuration for its users.
c) *Wide Area Network* (WAN), is a network that covers a large geographic area requires delimiters and rely at least partly on the circuit provided by public operators. Typically, a WAN consists of a number of switching node interconnects. A transmission from one of the devices is channeled through the internal node to the device purpose. This node (including node limit) does not affect the contents of the data, their goal was to provide a switching facility will move data from node to node until they reach their destination. Traditionally, WAN has been implemented using one of the two technologies: circuit switching and packet switching. Recently, frame relay and ATM networks have assumed the lead role which uses it [2].

2.2 Virtual Private Network

Virtual Private Network (VPN) is a computer network where connections between its nodes utilize public networks (internet/WAN) as it may be in certain cases or conditions do not allow it to build its own infrastructure. When the Connect VPN, the interconnection between the node such as an independent network that has actually created a special line pass through connection or a public network. At every company site, workstations, servers, and databases connected by one or more local area network (LAN) a LAN is under the control of the network manager and can be configured and tuned for cost-effective. The Internet or other public networks can be used to connect the sites, provide cost savings over the use of private networks and reduction of the burden of wide area network traffic to providers of public networks [2].

2.3 Types of VPN Implementations

On the implementation, there are two types of VPN, namely Remote Access VPN and Site to Site VPN [2].

a) Remote access VPN

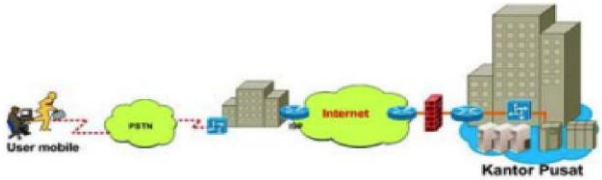

Figure 1. Remote access VPN

Figure 1 is Remote access VPN, Remote access VPN also called Virtual dial-up Network

(VPDN). VPDN is a type of user-to-LAN connection, the connection that connects a mobile user with a Local Area Network (LAN). This means that the user can access the private network from anywhere. Usually, this VPDN utilized by employees who are out of the Office and require a connection to the Office network of the company. Usually, companies that want to make this type of VPN network will work closely with Enterprise Service Provider (ESP). ESP will provide a Network Access Server (NAS) for the company. ESP will also provide special software to computers used by employees of the company[2].

b) Site-to-site VPN

Site-to-site VPN used to connect various areas that already fixed or fixed, this device utilizing a dedicated VPN are connected through the internet. Site-to-site VPN is divided into two, namely, extranet and intranet. An intranet that is where VPN is used only to connect various locations that are still one agency or one company. Like the Central Office is connected to the Branch Office. In other words, administrative control in control. While the extranet is where VPN is used to connect the company with other companies, such as partners, suppliers, or customers. In other words, administrative control is under the control of some of the relevant agencies.

2.4 Network Security

The security of computer networks is defined as a protection of resources against the efforts of change and destruction caused by someone who is not allowed, there are two things that are related to the security and confidentiality of data in computer networks namely representation of the data and data compression, which was later associated with the issue of encryption [3].

The security of computer networks namely the protection afforded to the automatic information system to achieve the goal, namely maintaining the availability, integrity, and confidentiality [4]. CIA triad can be seen in Figure 2.

Figure 2. CIA Triad

a. Availability

Availability means the system can ensure that the system works well and the service is not denied to users who are authorized. then ensure proper access and can be trusted to use the information. Loss of availability is the disruption of access to the use of information or information systems [4].

b. Confidentiality

Confidentiality means ensuring that personal or confidential information can not be accessed or used by another user or not on show to unauthorized users. Can then guarantee that user information can control information associated with the user as can be gathered and given to anyone. Then keep the limitations of authority information access such as protect personal privacy and the information that matters.

c. Integrity

Ensure that the information and the program can be changed only in a certain way and with full authority to the user. Ensure that the system functions as requested by users, there is no willful and intentional to manipulate the system. Then be able to guard against improper information modification or destruction, including ensuring the authenticity of the data.

2.5 Mikrotik RouterOS

Mikrotik on standards-based hardware Personal Computer (PC) known for their stability, quality control and flexibility for different types of data packets and handling of these processes (routing). Mikrotik created as a router-based

computer much benefit for an ISP that wants to run multiple applications ranging from the lightest to advance. In addition to routing, Mikrotik can be used as a management access capacity, bandwidth control, firewall, hotspot system, Virtual Private Network server and much more [5].

Mikrotik began to be established in 1995 that was originally intended for the company's Internet service (Internet Service Provider, ISP). Currently, MikroTik provides services to many wireless ISPs for Internet access services in many countries around the world and also very popular in Indonesia [6].

2.6 OpenVPN

OpenVPN is an open source application for Virtual Private Networking (VPN), where the application can create a connection point to point tunnel that has been encrypted. OpenVPN using private keys, certificate, or username or password to perform authentication in building connections. Where to use OpenSSL encryption [7].

a. Layer 2 and Layer 3 VPN.
   OpenVPN offers two basic modes, which operates as both a VPN layer 2 or layer 3 tunnel so that OpenVPN can also run on Ethernet Frames, IPX packets and Windows Network (NETBIOS) Packet Browsing, all of which is a problem in the VPN solution [7].
b. Protecting field workers with the internal firewall.
   Users who connect to the VPN Server will make the tunnel and turn the laptop/computer network settings, so that network traffic is sent through the tunnel. If the tunnel is established then the firewall from the VPN Server will be able to protect your laptop/computer connected, even though it is not the local machine.
c. OpenVPN connections can be tunneled through almost every firewall tunnel.
   OpenVPN can work on sites that use HTTPS protocol.
d. Proxy support and configuration.
   OpenVPN has proxy support and can be configured to run as a service and TCP or UDP as server or client. As the OpenVPN server, just wait until the client connection requests, while as a client, it tries to make the connection that corresponds to the configuration.
e. Only one port in the firewall must be opened to allow incoming connections.
   Since the OpenVPN 2.0, a special server mode allows connection of multiple incoming TCP or UDP port of the same, while still using a different configuration for every single connection.
f. Virtual interfaces allow very specific networking and firewall rules.
   All regulations, restrictions, and forwarding mechanisms concepts like NAT can be used with OpenVPN tunnel.
g. High flexibility with extensive scripting possibilities.
   OpenVPN offers many starting points for individual scripts. This script can be used for a variety of purposes from authentication to failover or more.
h. Transparent, high-performance support for dynamic IPs.
   OpenVPN no longer needs to use static IP'S on both sides of the tunnel. The second point is the end of the tunnel can have cheap DSL, access with dynamic IP users will rarely see the IP changes on both sides. the second session is the Windows Terminal Server and the Secure Shell (SSH) will only be "hang" for a few seconds, but it will not stop the requested demand after a brief pause.
i. No problems with NAT.
   Both the OpenVPN server and clients can be in a network that uses private IP addresses only. Any firewall can be used to send traffic to another tunnel.
j. Simple installation on any platform.

Both installation and usage are very simple. Especially, if you've tried to set up IPsec connections with different implementations.

k. Modular design.
Modular design with a high degree of simplicity both in security and networking. There are no other VPN solutions that can offer different possibilities on the same security level.

3 RESEARCH METHOD

3.1 Method Of Data Collection

Data collection was conducted to obtain data or documents required in the research. Methods undertaken in this research are:

a. Literature Method

This method is done by means of the study of literature by reading and comparing the books, journals, and papers on Virtual Private Network, OpenVPN, sniffing Internet, and related articles.

b. Observation Method

This method is done by Observation or research directed towards the object being examined, with UAD research laboratory experimenting with network security against sniffing, then provide solutions for prevention use the new security system.

3.2 Design

The process of designing this system needed a structured scenario. To simplify the process of designing the implementation of required network topology and flowchart to help in understanding the process of designing an OpenVPN to be made. As for the topology of VPN using OpenVPN using two Mikrotik routers to connect between the server and the client.

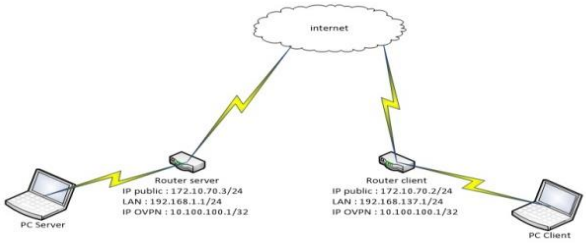

Figure 3. OpenVPN Network Topology

Figure 3 Is an OpenVPN Topology design, OpenVPN server located in research laboratory associated with Mikrotik router by taking an existing internet access, and then in the configuration of Mikrotik router to a client and also take the internet available in research laboratory, in this topology using the IP Public Server 172.10.70.3/24 and Client 172.10.70.2/24 and the IP OpenVPN Server 10.100.100.1/32 and Client 10.100.100.2/32.

3.3 Testing System

Testing of the system will be done by conducting an analysis of the QoS on the VPN network that includes Throughput, Packet loss, Delay, and Bandwidth, then conducted Security Test for linking among servers with a user for sharing data using VPN. To test security can be done an assault by sniffing the data using tools of Wireshark.

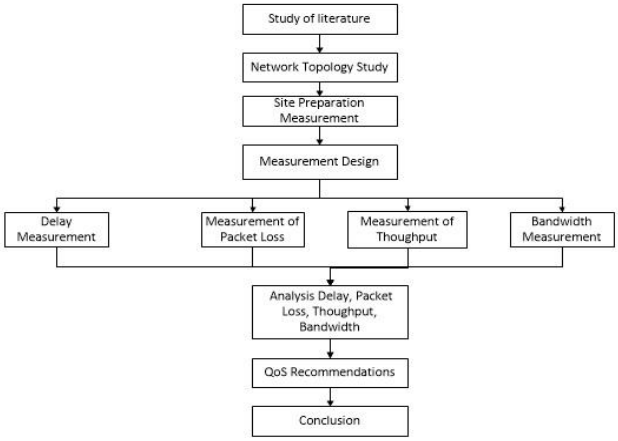

Figure 4. QoS analysis flowchart

Figure 4, is the flowchart in the analysis of the QoS, using Software Tools, namely Axance Net Tools to measure Delay, Packet lost, Throughput

and Bandwidth on the internet network Research Laboratory. The principle of work is to connect first to a network that will be the measure after that start the analysis with time, then note down the measurement results with the specified parameters.

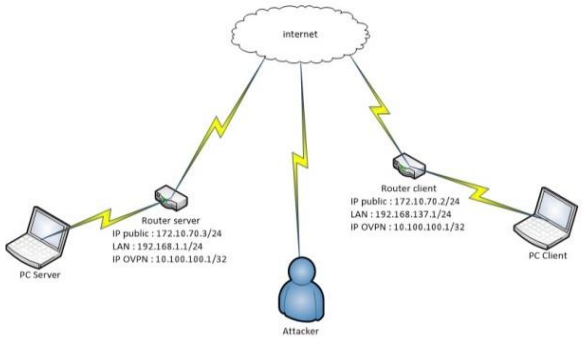

Figure 5. Attack Scenarios

In Figure 5, Assault scenario by using the tools of Wireshark, which an attacker can place his position in two machines communicate with each other, then the attacker will perform the action of sniffing data, and later in the analysis to get the difference between when OpenVPN is attacked and not attacked.

4 RESULTS AND DISCUSSION

4.1 Creation of OpenVPN

Creation of VPN with OpenVPN network of informatics research laboratory UAD after doing research on QoS and security network from sniffing action and known to the preliminary results of the parameter delay, packet loss, throughput, and bandwidth on the site www.google.com and the sniffing is done with the login to the website portal.uad.ac.id by sending the username and password data, sniffing data is done using the software Wireshark.

The first configuration on the proxy server is to enable OpenVPN on the main gateway, by entering the router configuration using the Winbox software and then configuring the PPP (Point to Point Protocol) menu.

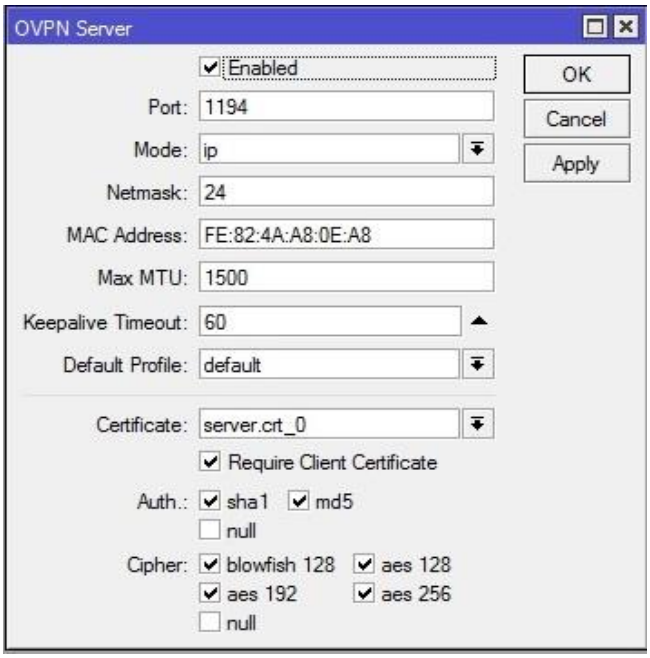

Figure 6. Enable OpenVPN

In Figure 6, this OVPN server tab is configured for the port used, enter the certificate to the server and choose security or encryption will be used. After that make a PPP connection to dial the secret from the OpenVPN client.

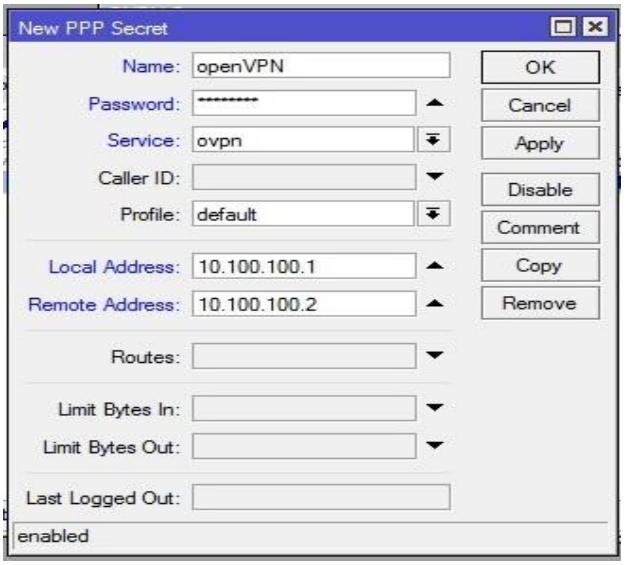

Figure 7. Configuring PPP Secret

Figure 7, is a secret PPP configuration that functions as an identity identifier when the client dials the connection on the OpenVPN server. The configuration with the name OpenVPN and password 12018182, OpenVPN service OVPN and local IP and remote IP IP later on this

remote be the IP of the client OpenVPN is connected.

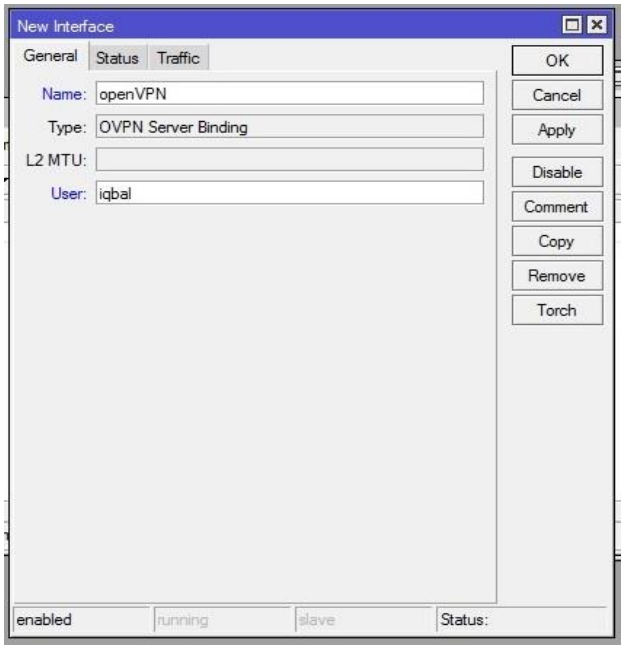

Figure 8. Static Interface Configuration

In Figure 8, the static interface configuration is used for the interface when the OpenVPN connection is formed, here also included user authentication when a client will connect to the server. Then proceed with the configuration on the router client.

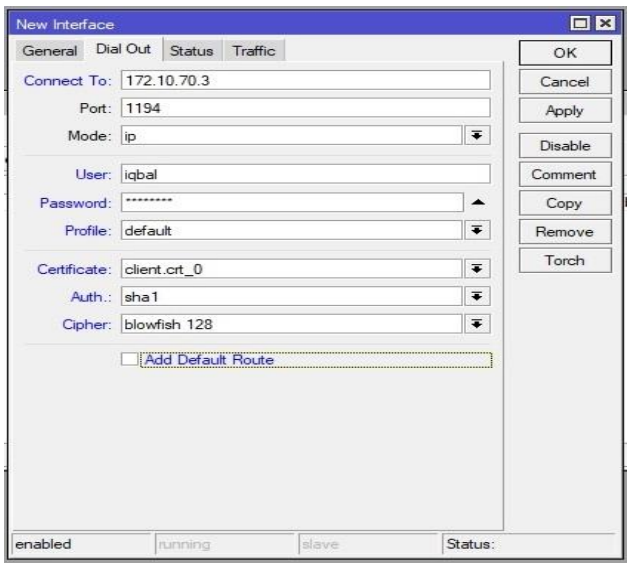

Figure 9. Configuring OpenVPN client

In Figure 9, OpenVPN client configuration is entered the IP address of the server's public IP, namely 172.10.70.3 then the port used, on the user and the password is entered with the appropriate name and password created on the PPP server secret, then put the certificate client for authentication to the server.

4.2 Security Analysis Results

Sniffing data on a network of research laboratory of Informatics UAD sniffing by performing against the network, the data is then sent in the form of a username and password from the client computer. Results of sniffing data before using a VPN with OpenVPN can be seen in Figure 10.

Figure 10. Results of Sniffing before using OpenVPN

From the results, it can be stated that a network of research laboratory of Informatics UAD HTTP to access the web is not secure from eavesdropping, as can be seen in the username and password as shown in Figure 10, When the user performs the authentication to the address portal.uad.ac.id or 103.19.180.90 with the username 12018182 and the password Iqbal12018182. The results are then compared with sniffing the network against after using a VPN with OpenVPN.

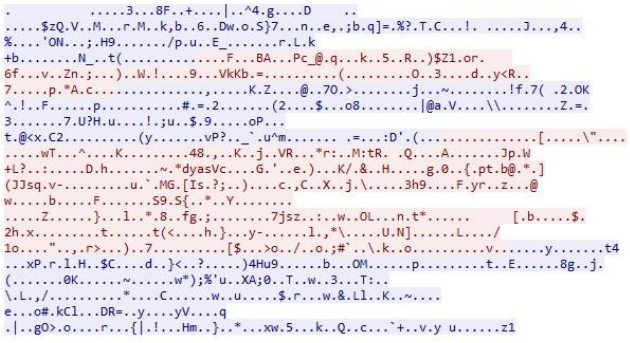

Figure 11. Results of Sniffing after using OpenVPN

Seen in Figure 11, results of sniffing after using a VPN with OpenVPN, the username and the password changed to row characters that can not be in the know or already in the encryption, so that the results from data sniffing after using

VPN with OpenVPN can be said to be safe from sniffing the network data.

5 CONCLUSION

The level of appropriateness of the use of VPN with OpenVPN is already quite worthy, this is due to increased data security than before using a VPN with OpenVPN, evidenced by the results of testing the action data sniffing is done using software Wireshark by sending data in the form of a username and password, the results obtained before using OpenVPN username and password can be seen and detected, then after using OpenVPN username and password data is not detected or has been encrypted by the OpenVPN so it is safe from the action of sniffing data. QoS measurement results experienced a decline in network quality with delay parameters rising from 51.4 ms to 463.4 ms, packet loss rose from 7.8% to 20.2%, throughput dropped from 82.8% to 71.6%, and bandwidth dropped from 64786.6 bit/s to 55589 bit/s, it is due to the encryption process and encapsulation that takes time.

REFERENCES

[1] Mains, John, "VPNs A Beginners Guide," McGraw Hill, 2001.
[2] Stallings, William., "Data and Computer Communications, Eighth Edition," Pearson Education, 2007.
[3] Kristanto, Andi., "Computer Network," Graha Ilmu, Yogyakarta, 2003.
[4] Stallings, William., "Cryptography and Network Security Principle and Practice, 5th Edition," Pearson Education, 2011.
[5] I. Riadi, "Network Security Optimization using Microtic Based Application Filtering Introduction Theoretical Basis," JUSI, Universitas Ahmad Dahlan Yogyakarta, vol. 1, no. 1, pp. 71–80, 2011.
[6] Setiawan, "Design and Implementation of Virtual Private Networks with PPTP Protocol on Cisco Router 2901 (UNTAN Informatics Engineering case study)," volume 1, JUSTIN, 2016.
[7] Purbo, Onno W., "Solution Mesh Network Building a Mutual Cooperation Wireless Network Without Access Points," Andi, Yogyakarta, 2013.
[8] Afrianto, Setiawan., "Study of Virtual Private Network as a Data Security System on Computer Networks," Vol.12, Scientific Magazine UNIKOM, 2013.
[9] I. Riadi, A. Luthfi, and M. Itqan, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," IJCSIS, vol. 15, no. 2, 2017.
[10] Irwan, Budhi, "Computer Network," Graha Ilmu, Yogyakarta, 2005.
[11] Wahyudi, "VPN Server Implementation using Slackware13 for Computer Network Security," STMIK Amikom Yogyakarta, 2011.
[12] Ulumuddin, "VPN Design and Application Using the OpenVPN Protocol for Hotspot User Authentication," Universitas Muhammadiyah Jember, 2015.
[13] R. Rizal, I. Riadi, Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," SDIWC, 2018.
[14] Supriyono, "Application of Virtual Private Network for data security PT. Mega Tirta Alami," WARTA, volume 16.
[15] Desti, I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," IJCSIS, vol. 15, no. 2, 2017.
[16] A.R. Caesarano, I. Riadi, "Network Forensics for Detecting SQL Injection Attacks Using NIST Method," SDIWC, 2018.