Atlantis Highlights in Engineering (AHE), volume 1
International Conference on Science and Technology (ICST 2018)

Point to Point Protocol Tunneling VPN Simulation and Analysis on Sniffing

Chrystia Aji Putra[1], Yisti Vita Via[2], Wahyu SJ Saputra[3]
Informatics Engineering
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya, Indonesia
[1]ajiputra@upnjatim.ac.id, [2]yistivia.if@upnjatim.ac.id

***Abstract*— PPTP (Point-to-Point Tunneling Protocol) is a network protocol used in the implementation of Virtual Private Networks (VPN). PPTP uses a client-server design that operates at Layer 2 of the OSI model. Network administrators require the existence of performance testing Point to point protocol and VPN network topology; this can be done with the result of simulation of computer networks. This research will discuss about the level of performance and security of PPTP to sniffing in VPN network. Simulations were performed with an average file packet delivery scenario of 500 MB. Graphical Network Simulator-3 (GNS3) is a network software emulator. This allows a combination of virtual and real devices, used to simulate complex networks. The simulation will be done using a VPN network and not using VPN by using GNS3 network simulation tool. Measurement of performance and security analysis is obtained by using Wireshark. The simulation results of the test will produce data to be used in the analysis process. PPTP performance analysis is performed in testing data transfer using FTP protocol when using the VPN network and not using VPN network. Performance parameters measured using Wireshark include throughput and delay. Testing is done by transferring data from the FTP protocol using a VPN network and not using a VPN network. The data transfer test results will get the parameters of output, delay, and data level of confidentiality. The best throughput values give results, data transfers that not use VPN are higher than using a VPN with an average yield of 153 KB and a delay in the network that does not use a VPN that is 0.0032 MS. Data transmission process from both methods shows the security of the FTP protocol, this concludes the security of the PPTP VPN protocol.**

Keywords— VPN; point-to-point; sniffing; FTP

I. INTRODUCTION

Computer networks need security management in data transmission. To facilitate the security of data transmission, it is necessary to have network management and security tunnel methods [1]. This aims to create a private network that is safe in sending a data packet to the destination. VPN can provide a solution in making the secure transfer process. One method is to use the point to point tunneling protocol (PPTP) protocol. With this method, data transfer can be done safely and to its destination [2].

The basic concept of a VPN is to create a private network through a public network. The choice of protocol in a VPN network is very influential on performance and security later. Point to Point Tunneling Protocol VPN is one of the communication protocols on the internet and local networks [3]. PPTP VPN has facilities to maintain confidentiality, integrity, and validity in a VPN network. This is important because when sending a data to a public network has the potential to be seen by a sniffer. VPN network implementation with Point to Point Tunneling Protocol method is an alternative solution. This method can help connect different networks in a private network that is safe against sniffers [4].

Making a private network (VPN) with the PPTP protocol is an advantage of infrastructure in an open communication network that is carried out. PPTP is a protocol that allows the transfer of data between the remote client and the enterprise server safely [5]. The transmission process uses a VPN based on an IP address. VPN is needed for security in the exchange of important data. Also, FTP is used as a transfer medium. FTP is one protocol that functions as a media file transfer. In VPN, data transmission security is in the layer two tunnels [6].

Previous research has discussed VPN in the internet network and WAN (Wide Area Network), which connects between two clients and can be accessed remotely safely [7]. VPN does not require expensive fees, and transfer rates are relatively fast and safe. The results of this research VPN can be connected properly, both remote access and using file transfer protocols [8].

This research was conducted to test VPN point to point tunneling protocol. This research simulates PPTP VPN security test against Sniffing, the purpose of this simulation is getting results that show the security of file transmission through the PPTP VPN protocol. The simulation will be done using a VPN network and not using VPN. Graphical Network Simulator-3 (GNS3) is a network software emulator. This allows a combination of virtual and real devices, used to simulate complex networks. This simulation is using GNS3 network simulation tool.

II. METHODOLOGY

First work is making VPN network design with PPTP protocol based on simulation using GNS3 Network Simulator. This work will get QOS which consist of delay, throughput and data transmission using VPN and not using VPN.

Furthermore, analyzing network traffic using VPN and not using VPN. This step will get information on the level of confidentiality of data transferring, and show sniffer activity during data transfer.

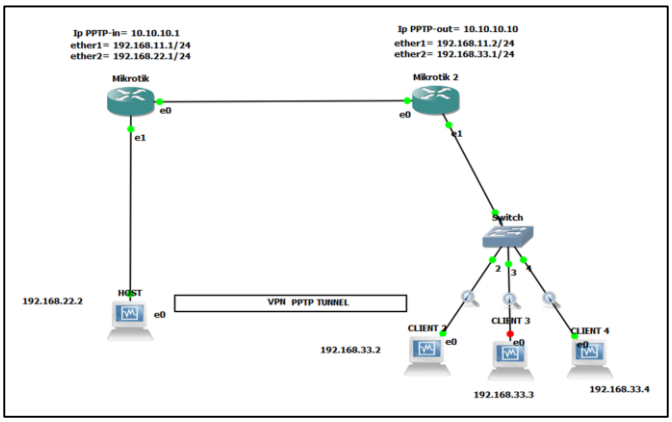

Fig. 1. Network Topology for Simulation.

In this step, the network topology is created as in Fig. 1, server and client is properly connected. In implementations on a VPN using 1 Server, 3 Clients and 2 MikroTik routers, plus a host as a Sniffer.

MikroTik 1 is configured as a server to manage VPN networks, MikroTik 1 also builds security on its internal network. The construction of this topology is done step by step; the first step is to configure IP addresses on MikroTik 1 as a server. Then MikroTik 2 can make access to the IP address of MikroTik 1. MikroTik 2 can start VPN server installation process. Next step is to manage VPN security with PPTP method.

List of IP addresses in static routing simulations has been created in Table I.

TABLE I. IP ADDRESS LIST FOR SIMULATION

Name	As	IP Adress	Ethernet
ROUTER 1	Router	192.168.11.1/24	Eth 1
GATEWAY	Router	192.168.22.1/24	Eth 2
ROUTER 2	Router	192.168.11.2/24	Eth 1
GATEWAY	Router	192.168.33.1/24	Eth 2
Host	Client	192.168.22.2/24	Eth0
Client User 2	Client	192.168.33.2/24	Eth0
Client User 3	Client	192.168.33.3/24	Eth0
Cllient User 4	Client	192.168.33.4/24	Eth0
Router 1/ PPTP in	VPN	10.10.10.1	TCP
Router 2/ PPTP out	VPN	10.10.10.10	TCP

Testing simulation in this research is using GNS3. Testing is carried out with several conditions in the network. File transfer traffic will be seen in VPN simulations. The focus of testing is on performance and security of file transfers. Test results are obtained from the comparison of delay and throughput.

First scenario testing is transferring files from the FTP server to the client and using a VPN network and PPTP tunnel. In this scenario, the average value of delay and throughput is taken. In this step also doing file transfer testing. Transfer files from all three clients simultaneously to HOST. Simultaneously, packet sniffer capture uses Wireshark between the client and HOST with a VPN-connected network.

Furthermore, analyzing includes Delay and Throughput values. In this test also carried out file transfers from the three clients but alternately. Moreover, the analysis consists of the value of Delay and Throughput.

Second scenario testing is transferring a file from all client to HOST using FTP. File transfers in this step are not using VPN. In this step, testing is also doing sniffing into the data transmission package. In this scenario then the average delay and throughput values are taken.

Last test scenario is checking confidentiality of data being transmitted. This file transfer testing was doing out on the VPN network, then sniffing using Wireshark. Wireshark is a free and open source network protocol analyzer that allows users to trace data traffic on a computer network interactively. This testing aims to test the confidentiality of data from data packet sending activities. Delivery of data packets from the host to the client without using a VPN network.

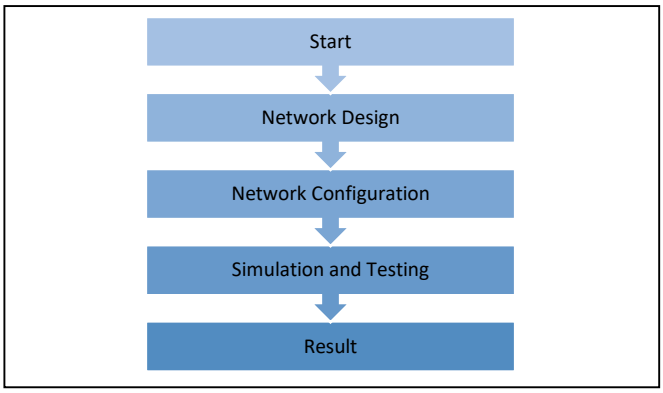

Fig. 2. Design Simulation Network.

Design of topology that using VPN consisting of two MikroTik routers and two clients. Configuring the IP address of each router with the aim of being able to connect with clients. This configuration of the router will have a VPN tunnel path. This path can also be accessed by both clients safely. Testing process to determine the level of security and performance of this VPN protocol. This testing process is also used with PPTP. Sniffing testing is carried out on traffic between host and client. Fig. 2 describes the step by step in this research. In other words, testing in the first scenario is getting the result of delay and throughput with transmission using VPN.

Meanwhile in the second scenario, testing data transmission using VPN. This test aims to obtain performance simulation results in PPTP tunneling. Another thing that is obtained is the quality of data transmission against sniffing. From the results of

this test, it will be concluded the quality and security level of PPTP VPN.

III. Result And Discussion

This implementation includes network configuration and testing according to the scenario that has been created. This simulation is using GNS3; testing is done with several conditions in a computer network. File transfer traffic is carried out on VPN simulations. This simulation is obtained performance rate and security of file transfers. Performance parameters are comparing delay time and throughput time during data transfer.

To determine results of performance testing via FTP, each file is downloaded simultaneously from three clients to VPN Network host. This simulation will get an average download transfer speed. Next simulation process of sending files via FTP. Files that will be used as testing simulation media is 191 MB with ISO extension, 412 MB with MP4 extension, and 712 MB with AVI extension. Wireshark shows the IP Source and the Destination IP from the package delivery activity. The third client packet delivery is carried out from the client to the host that has been configured on Router 1.

In this section will be presented delay value and throughput of data packet delivery. Testing is done using VPN or without using VPN. The delay value presented is the average delay value of each packet data delivery testing. The delay value is one of the comparison parameters that will be used in this study. The delay value is the delay time of a packet caused by the transmission process from one point to another.

To get results of throughput, specified file transfer was chosen. Obtaining throughput value is different by getting a delay value. The value of throughput in the FTP package is calculated from the total size of the package sent from beginning to end. The value obtained is compared to the total overall delay time.

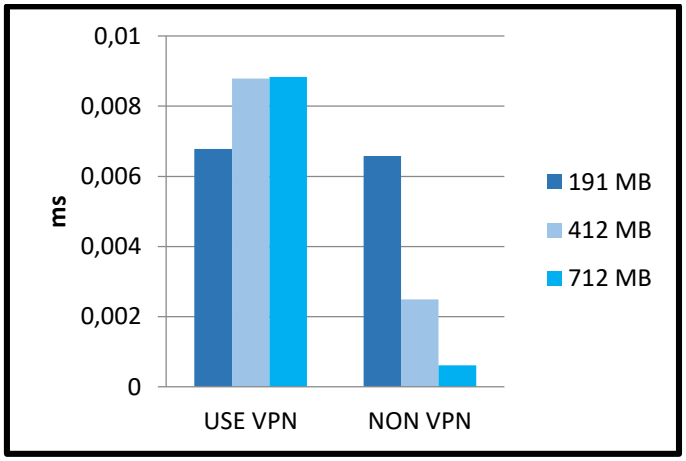

Fig. 3. Delay Value Result.

File delivery testing is divided into two, using VPN and not using VPN. Test results can be seen in Fig. 3. Different file sizes for each package delivery simulations. The first file is 191 MB, and ISO extension has a delay value of 0.0064 ms when using VPN, has a delay value of 0.0060 ms when not using VPN. The second file is 412 MB, and MP4 extension has a delay value of 0.0082 ms when using VPN, has a delay value 0.0025 ms when not using VPN. The third file is 712 MB, and ISO extension has a delay value of 0.0083 ms when using VPN, has a delay value of 0.0001 ms when not using VPN.

Fig. 4 is a throughput value from FTP transfer. File delivery testing is divided into two, using VPN and not using VPN. Test results can be seen in Fig. 4. Different file sizes for package delivery simulations.

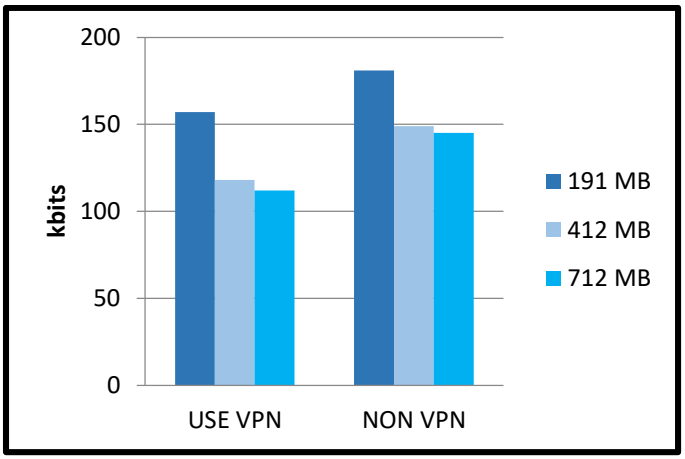

Fig. 4. Throughput Value Result.

The first file is 191 MB, and ISO extension has a throughput value 149 Kbits when using VPN, has a throughput value 180 Kbits when not using VPN. The second file is 412 MB, and MP4 extension has a throughput value 108 Kbits when using VPN, has a throughput value 142 Kbits when not using VPN. The third file is 712 MB, and ISO extension has a value 105 Kbits throughput when using VPN, has a throughput value 141 Kbits when not using VPN.

The last testing is comparing the two methods between PPTP VPN and Remote (non-Tunneling) Network. Remote networks that have been sniffed have the following results. Wireshark is installed between server and client, then captures each packet that passes through the second network. Also, contents of the package will be analyzed to analyze other security gaps. The scenario created is that the server and client communicate by sending data from the client to the server. During data transfer, sniffing will be done using Wireshark. The results of sniffing will show the data sent from the client to the server.

Simulation above can be known to network security vulnerabilities when sending data. Testing process of sending packets takes place with both IP seen between server 192.168.22.2 and client 192.168.33.2. At this time sniffing is done by filtering the FTP protocol. Testing gives results that package delivery can be seen by Wireshark. This means that the FTP protocol without tunneling still has a gap in sniffing activities. This is because package delivery does not use PPTP tunneling.

Next testing is the result of the package delivery process using PPTP VPN. Testing is carried out when packet delivery takes place, and sniffing is done by filtering FTP protocol. Testing simulation gives results that the package delivery is not

visible to Wireshark. This marking functioning of PPTP VPN feature so that sniffer can only see. The sniffer can only see PPP protocol activity with compressed data information. This indicates safe delivery of encrypted packages.

IV. CONCLUSION

From the description above, obtained a conclusion about this research. Results obtained of file transfer traffic testing based on delay parameters in the VPN network has an average delay value of 0.0076 ms. While file transfers that not use a VPN network have an average Delay value of 0.0028 ms. The result of the file transfer traffic test results based on the parameter throughput parameters in the VPN network has a value of 120.6 Kbits, while the non-VPN value is 154 Kbits. In both testing simulation, it can be concluded that a higher Delay value is poor quality in file transfer, while the smaller value throughput is better quality.

Security testing includes data confidentiality when file transfers are carried out. This testing result provides good results when using a VPN network. Sending of compressed data packages so that they are not visible to the sniffer. But when not using a VPN network the data transmitted can be seen by the sniffer.

The conclusion of these two methods is that remote networks are superior in data delivery performance. Download rate process is faster than a VPN network. But regarding network security, VPN is superior to sniffer because there is an encapsulation and decapsulation process.

REFERENCES

[1] J.D. McCabe, Network Analysis, Architecture, and Design, 3rd ed., Massachusetts: Morgan Kaufmann, 2007.

[2] D. F. Handriyanto, Use the Router MikroTik as a Network Router, 2009.

[3] I.G.L.P.E Prismana and B. Chilmi "Implementasi Simulasi Jaringan Komputer Multi Device Dengan Menggunakan GNS3," Jurnal Manajemen Informatika, 04(01), pp.77-84, May 2015.

[4] J. Biswas, "An Insight in to Network Traffic Analysis using Packet Sniffer," International Journal Computer Applications, 94(11), pp. 39-44, May 2014.

[5] Shrivastava, Anupriya, "Performance and Strength Comparison Of Various Encryption Protocol of PPTP VPN," International Journal of Advance Found. and Res. in Computer (IJAFRC), January 2014.

[6] F.D. Irnawan, "Compare of Analysis of VPN Network with Mikrotik Based," Jurnal of Computer Netw., 2014.

[7] Ritika kajal, Deepshikha Saini, Kusum Grewal, "Virtual Private Network," International Journal of Adv. Res. in Computer Sci. Softw. Eng., 2012.

[8] T.S. Sobh, Y. Aly, "Scientific Research. Effective and Extensive Virtual Private Network," Journal of Information Security, 2, pp. 39-49, January 2011.