IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⪤ Impact Factor 7.105 ⪤ Vol. 9, Issue 8, August 2022

DOI: 10.17148/IARJSET.2022.9809

PPTP VPN and L2TP/IPsec VPN Performance as Voice Data Security in VoIP

Martono Dwi Atmadja[1], Farida Arinie Soelistianto[2], Harrij Mukti Khristiana[3]

Electrical Engineering Major Lecturer, Malang state Polytechnic, Malang, Indonesia[1,2,3]

Abstract: VoIP technology is a technology that allows long-distance voice communication by utilizing internet media. Communication between users through the internet requires a level of security that are confidential (private). However, using an open internet network requires a communication data security method with the implementation of network performance and security. This can be done with the application of the Virtual Private Network (VPN) method. VPN applications on VoIP are affected by the security system by encrypting data from VoIP communications. VPN PPTP computer network security technology in virtual private IP or as a tunnel as a secure data transmission medium. The PPTP VPN and L2TP/IPsec VPN methods are a Layer 2 (Layer 2 Tunnel Protocol) – L2TP protocol, while the PPTP protocol uses only IP addresses, usernames and passwords for authentication. L2TP uses an additional authentication system, namely a Pre-shared key or secret. The purpose of this study is to compare security based on the protocol used with sniffing techniques and to obtain the Quality of Service (QOS) parameter values that includes bandwidth and delay. Performance test for bandwidth from the largest upload side, when using L2TP/IPsec VPN The average bandwidth value when uploading the G.711 codec is 76kbit/sec. While the download is around 77kbit/sec.

Keywords: VoIP, VPN PPTP, VPN L2TP/IPsec, QoS

I. INTRODUCTION

The telecommunications technology industry is growing rapidly under customer service needs. The Telecommunications Operator must be able to read the customer's needs against the user's interests, and if it is unable to handle this then the Operator will only serve as a capacity provider. With the development of this service as well as optimization in financing and speed of access, the use of computer networks has also become one of the telecommunications technologies that develop in line with customer needs. IP-based communication technology that is embedded in the internet network is not only for data packet services and for word wide web, HTTP and FTP applications. One of the telecommunications technologies currently developing is voice communication via the internet. VoIP (Voice over Internet Protocol) telephone call technology via the internet [1]. The received voice is converted into a digital code and then passed through the network in the form of data packets [2]. The difference in telephone via VoIP lies in the security system compared to analogue voice [3]. In real-time packet data usage, call encryption is made so that it is not vulnerable to eavesdropping and the voice received by the recipient is clear. Disadvantages of VoIP need internet sender and receiver to be connected. When the network is experiencing bottlenecks, there are more and more communication connections via VoIP, so they are unable to access the server because of data overload. VoIP communication still needs a study on data security in voice communication when it takes place. When voice communication occurs, the possibility of eavesdropping, data content hijacking or not being able to access the server when the server is overloaded [4]. To handle this kind of condition, it is possible to apply a data security method to VoIP services using the PTPP VPN protocol security. VPN (Virtual Private Network) is a service that connects one network to another with a private system through the internet network [5]. Another capability of a VPN is to provide secure access through a server connection by hiding traces of personal data. VPN works by managing data encryption in the exchange of data before connecting to the public. Utilization of VPN as an alternative to using the internet network traversed by voice encryption by using private keys, certificates, or unique usernames so that they can authenticate in establishing connections. In network authentication with 80kbps (standard G.711) bandwidth requirement. VoIP communication between buildings requires security on the network (private) [6]. This can be done by using a VPN. Users can access information sources from outside that are in the local network. The importance of VPN security and privacy of data on transmission from unauthorized users in the same transmission can be limited by encryption and tunnelling of the VPN. The data that VPN receives and sends is guaranteed to be from a private source. VPN tunnelling creates a private connection path using other network infrastructure. VPN began with Swipe in 1993 with PPTP (Point to Point Tunnelling Protocol) then developed with IPsec until it was available in the form of Open VPN [7]. PPTP (Point to Point Tunnelling Protocol) is a network protocol that functions as a secure data transfer from a remote client to a company's private server by creating a VPN via TCP/IP. While Internet Protocol Security (IPsec) is a tunnelling protocol that works at layer 3. Provides the algorithm used in the service and places the cryptographic key according to the required service. This study aims to analyse the characteristics of voice security on VoIP by using a protocol that

DOI: 10.17148/IARJSET.2022.9809

supports encryption on a VPN network with PPTP (Point to Point Tunnel Protocol) and L2TP (Layer2 Tunnel Protocol) tunnelling methods.

II. Research Methods

This research is an experimental method of a case in a VoIP network on voice security in the use of the VPN method. The research variable is carried out by utilizing the intranet network and computer network within the scope of one company. The VoIP technology used is the use of long-distance voice communication through internet media and the server used VoIP Asterisk FreePBX. VPN design by planning tunnelling with encapsulated packets sent through the company intranet network [8]. Utilization of PPTP VPN and L2TP/IPsec VPN. While the VoIP server uses raspberry pi while the VPN uses a proxy. The design stage is to install the operating system on the raspberry pi, the OS used is the OS pack which contains Raspbian and raspbx. Furthermore, designing the proxy system by setting the server IP with the division on the VoIP server IP and IP settings for the VPN server. The VPN server configuration stage is set to PPTP and L2TP/IPsec VPN. L2TP VPN is also regulated by IPsec Proposal, as well as IPsec Policy connected to Ipsecpeer. While the VPN client is set for calls from VoIP. The design of the FreePBX and softphone configurations is divided by setting the codec on FreePBX as well as adding call extensions. On the softphone, it is used as a place to create call accounts from extensions that are on asterisk FreePBX. While testing the connection between networks by connecting the VPN server to the client or vice versa, to find out the configuration that is not connected. For security on VoIP, the test is by tapping login data. Stages of analysis of the test results from these stages with a comparison between VPN PPTP and VPN L2TP/IPsec. Figure 1 shows the design for testing voice security with the VPN method.

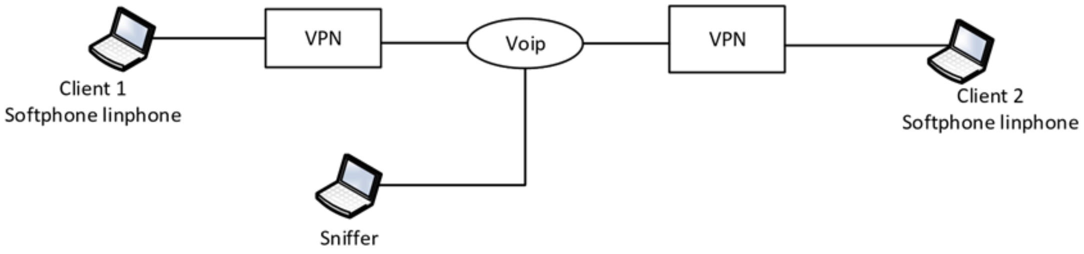
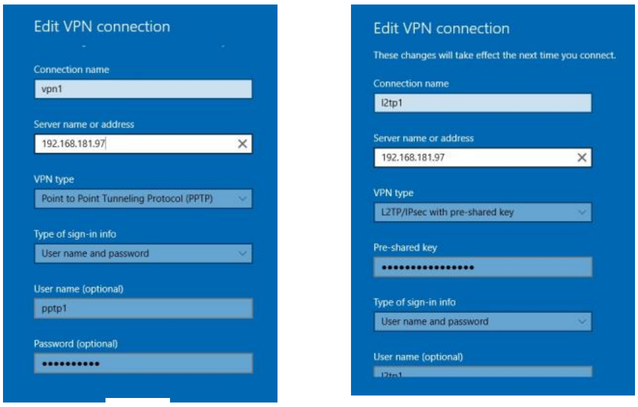


Figure 1. VoIP Voice Security System Design VPN Method

This method was tested for the stages of design, implementation and operation of the system following the research objectives. Testing between two VPN protocols with the same topology [9]. That is testing by pining between the proxy and the client's IP. The security system using calls between clients connected to the VPN is then captured from the Wireshark software. The results obtained from the capture are read the protocol for sending calls through the VoIP network. Part of the VoIP server on the raspberry pi is used for the proxy server IP. IP configuration is used to enter reboot command in putty terminal. Configure the VPN server with IP settings on the network in the inbox software. The local IP of the raspberry pi server and the IP on the router is configured as a VPN server, on ether 2 with IP 192.168.50.1(port2). While the VPN server IP is used on the DHCP client when the proxy router becomes the client of the access point on the company intranet. The VPN server IP is self-configured so as not to interfere with the company intranet. The configuration is IP→DHCP Client→(+). Next, configure the PPTP server by selecting the PPP→PPTP Server tab and marking it as “enabled”. In the L2TP server configuration is the authentication setting and activate the L2TP server using IPsec marked as use IPsec and set IPsec secret. At the time of configuration proposal., policies, and peer-selected IPsec for L2TP VPN. IPsec proposal selected the default proposal tab. Authalgorithm is marked in **sha 1** section and Encr.Algorithm in **3Des** section. Configuration on the VPN server is done first on the client side which is not limited to computers. The stages of the VPN client configuration are windows settings → Network & Internet → VPN then select **"add VPN connection"**. Figure 2 shows the configuration of PPTP VPN and L2TP VPN.



Edit VPN connection

Connection name: vpn1

Server name or address: 192.168.181.97

VPN type: Point to Point Tunneling Protocol (PPTP)

Type of sign-in info: User name and password

User name (optional): pptp1

Password (optional): •••••••••••

(a)

Edit VPN connection

These changes will take effect the next time you connect.

Connection name: l2tp1

Server name or address: 192.168.181.97

VPN type: L2TP/IPsec with pre-shared key

Pre-shared key: ••••••••••••••••

Type of sign-in info: User name and password

User name (optional): l2tp1

(b

Figure 2. Configuration (a) VPN PPTP and (b) VPN L2TP

From merging the client's VPN on the VPN server by ensuring that the client is connected to the corporate intranet network. While on the client's VPN from the android smartphone, go to settings, and select 'add VPN'. This study uses the G.711 Alaw codec. G.711 Ulaw [10]. GSM and Speex. This codec is used for the 'enable' and 'disable' modes for the active codec.

III. RESULT AND DISCUSSION

Based on connection, security and network testing using PPTP and L2TP/IPsec VPN tunnelling methods using sniffing techniques as login data acquisition. The performance of the call concerning bandwidth capacity, delay and packet loss. Network security with calls made between clients and wiretapping. The results obtained are data packet capture and VPN login data. When testing data packet capture using Wireshark software, while logging in VPN with Cain and Abel software as sniffing software. VPN PPTP login data on average is unreadable with two clients. Likewise, the L2TP login data is also unreadable. The data from the bandwidth was tested during the morning rush hour (08.00WIB) from table 1 for the download and upload conditions from the two VPNs, namely PPTP and L2TP. The average bandwidth value when uploading the G.711 codec is 76kbit/sec. Meanwhile, when downloading around 77kbit/sec.

Table 1. Average Bandwidth Score

VPN	CODEC	UPLOAD (Kbit/s)	DOWNLOAD (Kbit/s)
PPTP	G.711 ALAW	66	75.5
	G.711 ULAW	70	63
	GSM	19	26.2
	SPEEX	19.5	23.2
L2TP	G.711 ALAW	74.7	73.5
	G.711 ULAW	75.2	76.5
	GSM	28.5	25
	SPEEX	26.	24.9

In testing the ping-in connection on the PPTP VPN IP tunnel, which is 10.10.10.1, it shows accurate (successful) results. Likewise, the L2TP/IPsec VPN was also successfully connected. The VPN server and the client's VPN form a tunnel so that the client gets an IP tunnel. Security testing performs sniffing on data packets sent with Cain and Abel software. Wiretapping is done on the client using a VPN network. The login data encryption process is carried out when using PPTP VPN, the login data that is read is only the username while the password cannot be read. The authentication protocol used is MS-CHAPv2 and the encryption uses MPPE. The process of encapsulating and encrypting data packets sent from VPN PPTP in compressed form by the PPP protocol. Furthermore, encapsulation is carried out by the Generic Routing Encapsulation (GRE) protocol. At the time of L2TP eavesdropping, the username and password sections were not read with sha1 for authentication and 3des as encryption. Packets sent using L2TP VPN are encapsulated with the

DOI: 10.17148/IARJSET.2022.9809

Encapsulating Security Payload (ESP) protocol. The ESP protocol's function is a protocol owned by IPsec so the security method is better than PPTP. The daytime delay test with VPN PPTP is the codec G.711 ulaw about 26.9 ms, when using L2TP it is around 27 ms.

III. Conclusion

Based on the results of research on the security performance of L2TP/IPsec and PPTP VPNs, the results can be observed with delays, bandwidth testing is carried out during the day (peak hours). The L2TP/Ipse VPN security system is more optimal than the use of PPTP VPN, even though the upload and download bandwidths are significantly different. The encryption and encapsulation process in L2TP/IPsec VPN use Encapsulation Security Payload (ESP) with 3DES and SHA1 algorithms. Meanwhile, PPTP uses the MPPE protocol which changes the login data format in the form of MS-CHAPv2 and the encapsulation uses GRE. The highest data upload bandwidth value is on L2TP/IPsec VPN, on the other hand, the highest data download is with PPTP VPN. The biggest delay test is using VPNL2TP/IPsec with G.711 Ulaw codec. The sound performance test is classified as good (no interference/echo) with Absolutely Category Rating (ACR) 4 from the ITU-T standard rec.800.2.

References

[1] Meisel, J. B., & Needles, M. (2005). Voice over internet protocol (VoIP) development and public policy implications. info.

[2]. Yuniati, Y., Fitriawan, H., & Patih, D. F. J. (2014). VoIP Server Design Analysis (Voice Internet Protocol) with Opensource Asterisk and VPN (Virtual Private Network) as Network Security Between Clients. SITEKIN: Journal of Science, Technology and Industry, 12(1), 112-121.

[3]. Butcher, D., Li, X., & Guo, J. (2007). Security challenge and defense in VoIP infrastructures. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6), 1152-1162.

[4]. Kuhn, D. R., Walsh, T. J., & Fries, S. (2005). Security considerations for voice over IP systems. NIST special publication, 800.

[5]. Rohman, M. F. (2021). ANALISIS QOS (QUALITY OF SERVICE) PADA JARINGAN VOIP DENGAN MENGGUNAKAN PROTOKOL VPN SEBAGAI KEAMANAN JARINGAN (Doctoral dissertation, universitas muhammadiyah jember).

[6]. Gupta, P., & Shmatikov, V. (2007, July). Security analysis of voice-over-ip protocols. In 20th IEEE Computer Security Foundations Symposium (CSF'07) (pp. 49-63).

[7]. JEONG, J. H., KIM, G. W., PARK, S. H., & SOHN, S. W. Design and Implementation of the Ipsec-based Security System.

[8]. Wang, C., & Chen, J. Y. (2014, May). Implementation of GRE over IPsec VPN enterprise network based on cisco packet tracer. In 2nd International Conference on Soft Computing in Information Communication Technology (pp. 142-146).

[9]. Scott, C., Wolfe, P., & Erwin, M. (1999). Virtual private networks. " O'Reilly Media, Inc."

[10]. Denev, D. R. (2021). ANALYTICAL STUDY OF THE DELAY INTRODUCED AS A RESULT OF ENCRYPTION/DECRYPTION OF VOICE TRANSMITTED OVER A VPN NETWORK. Journal Scientific & Applied Research, (20).