Analysis Quality of Service and Security of VoIP Communication System Using OpenVPN

Rusdiyansah[1] Sri Dianing Asri[2]

[1] *Faculty of informatics Engineering, Mercubuana University, Jl. Raya Meruya Selatan, Kembangan, Jakarta, 11650, Indonesia*
E-mail: rusdiansyahajah@gmail.com,

[2] *Faculty of informatics Engineering, Mercubuana University, Jl. Raya Meruya Selatan, Kembangan, Jakarta, 11650, Indonesia*
E-mail: dianing.asri@mercubuana.ac.id,

***Abstract*— Voice Over Internet Protocol (VoIP) is a telecommunications technology that is able to deliver communication services in Internet Protocol networks that enable voice communication between clients in an IP network [1]. And VPN (virtual private network) is an alternative to sending voice, which is private or secure, because of the use of encrypted connections and the use of private keys, certificates, usernames or passwords for authentication in establishing connections [2]. Quality of Service and Security Analysis of VoIP Communication System Using OpenVPN is to find out QoS (Delay, Jitter, Packet Loss and Throughput) whether it still meets the ITU-T standard or not. And to find out the security of the VoIP system after using OpenVPN and before using OpenVPN. The result of analysis and testing using Audio Codec G.711 and G729, it can be seen that the use of Audio Codec G.729 is more optimal. This can be seen from the results of Delay, Jitter and Packet Loss in both Audio Codecs. Although the results are not too much different but throughput or bandwidth used by Audio Codec G.729 is smaller than Audio Codec G.711. As for VoIP data security, OpenVPN can secure data from security threats of tapping. Unlike before using OpenVPN VoIP data can be recorded and played back. And before using OpenVPN VoIP data can be recorded and played back**

***Keywords*— VoIP, QoS, VPN, Audio Codec**

I. INTRODUCTION

With The rapid development in technology, Technology of IP-based communication is growing rapidly as well. Currently the internet is not only focused on data package services and standard applications such as the WWW (World Wide Web), HTTP, SMTP, FTP, or other data services that are non-real-time and do not have QoS. At present the need for multimedia-based services for IP networks has become possible because of the discovery of network QoS supporting technologies such as RTP, Streaming via the Internet which makes IP networks reliable for sending real-time data such as voice or video. But one obstacle in implementing VoIP, the data sent is not guaranteed so that anyone can capture and manipulate the data. one of the solution is use a VPN (Virtual Private Network). In this experiment the author will use OpenVPN. VPN itself is known as one of the reliable methods of dealing with network security issues, especially for sending important data. VPN (virtual private network) is an alternative to sending voice, which is private or secure, because of the use of encrypted connections and the use of private keys, certificates, usernames or passwords for authentication in establishing connections.

In general, VPN is a local communication network that is connected through public network media, the most widely used public infrastructure is the internet network. In the VPN there is a combination of tunneling and encryption technology that makes VPN a reliable technology to overcome security problems in the network.

In its implementation, the VPN is divided into remote access VPN and site-to-site VPN. Site-to-site VPN is used to connect between two places that are located in a row, such as a central office with a branch office. This remote access type of VPN is used by company employees who want to connect to their company's local network from various remote locations.

II. IMPLEMENTATION OF VoIP

In this section, we will first describe the VoIP protocol and service quality and security in the VoIP system that will be used in research.

A. Protocols

SIP (Session Initiation Protocol) is an application layer control protocol developed by the Internet Engineering Task Force (IETF) to establish a bidirectional session for multimedia conferences, telephone calls and distribution of multimedia attachments. Its greater support for mobility, interoperability and multimedia made it scalable beyond VoIP calls. It acts similar to HTTP with its request and response structure .This protocol is used to create sessions and to carry session descriptions that allow participants to agree on multimedia capability. The functions of this protocol are to :

1) determine the location of an endpoint or user to be used for communication.
2) synchronize connection between the caller and the destionation .
3) establishing media parameters for a successful connection
4) in Progress changing the features of a session
5) adding, dropping packets, terminating sessions and invoking services SIP works in conjunction with other protocols to provide for a complete multimedia architecture like RTP (Real Time Transport protocol) or transmitting real time data along with Quality of Service (QoS).

B. Quality Of Service

The definition of QoS according to the International Telecommunication Union (ITU): the collective effect of service performance which determines the degree of satisfaction of a user of the service.

1) Delay

Delay is a collection of various times from end to end on the internet network. The delay affects the quality of the QoS service because the delay time causes a packet to reach the destination longer. ITU-T G.114 Delay placement is not greater than 150ms for various applications, with a limit of 400ms for multimedia communication that is still acceptable. Meanwhile for Voice applications such as VoIP and Conference Calls, the maximum delay limit is 300ms.

2) Jitter

Jitter is the difference in time interval between packages at the destination terminal. Jitter can be caused by congestion, lack of network capacity, variations in packet size, and package inaccuracy.

3) Packet loss

Packet loss is the main cause of weakening audio and video streaming, VoIP and Conference Calls. Packet loss can be caused by the disposal of a packet in the network (network loss) or disposal at the gateway / terminal until the last arrival (late loss). Network loss is normally caused by congestion (buffer overflow routers), changes in routes instantly, link failures and lossy links such as wireless channels. Congestion on the network is the main cause of packet loss.

4) Throughput

This parameter concerns about the maximum number of bits received out of the total number of bits sent during an interval of time.

C. Virtual Private Network (VPN)

A Virtual Private Network (VPN) is communication technology to be able to connect to public networks and use it to join local network. In this way it will obtained the same rights and settings as the case is in the LAN itself, though actually uses a public network.

III. CONFIGURATIONS OF VOIP

In this research VoIP will be designed using AVAYA IP Office Server Edition Version 9 on a LAN (Local Area Network) and OpenVPN network on the MikroTik OS Router. This research will focus on the analysis of the QoS Audio codec G729 and G711 and the security of using VPN.

D. Topology

The design of VoIP networks in this study uses several IP subnets and different VLAN IDs. This is very important because with the implementation of different VLAN IDs and IPs, if something happens that is not desired, such as broadcast or flooding, the packet on a network does not affect other VLANs or IP subnets.

TABLE I
DESIGN IP ADDRESS OF NETWORK

Nama	VLAN	IP Address	Subnet Mask
Server VoIP	2	172.16.1.231	255.255.255.0
MikroTik	-	172.16.100.250	255.255.255.0
OpenVPN Client	-	192.168.30.x	255.255.255.0
VoIP Client	269	10.12.69.x	255.255.255.0

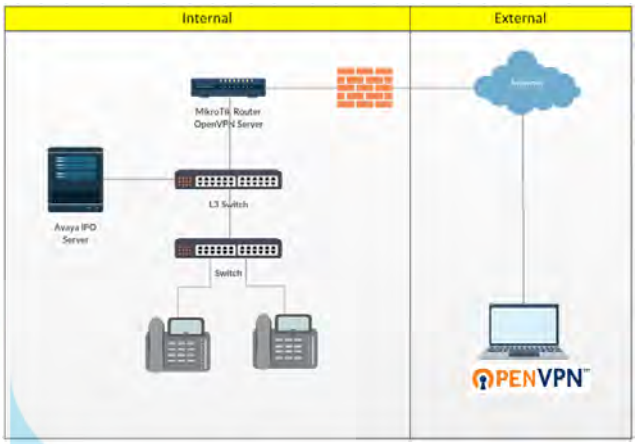

Fig. 1 Network Topology in this Research

E. VoIP Server

SIP user on VoIP Server AVAYA IP Office Server Edition Version 9 it should be configured. Making a SIP user that will be used on each client is made according to the VoIP server. As for what must be considered in making the user, among others, the user name, extension number, then the password from the extension. The extension number and password are used to authenticate the client to register. As well as on Avaya VoIP Server the extension number and user name must be unique cannot be the same.

TABLE 2
DESIGN THE IP ADDRESS AND EXTENTION CLIENT

Nama	IP Address	Extention
Client 1	10.12.69.11	9908
Client 2	10.12.69.12	9907
Client 3	192.168.30.1	9909

F. VoIP Client

The client configuration is done so that each client can be registered into the VoIP server so that it can make phone calls. In the configuration there is a configuration number extension that will be used on the client, the time server configuration used (NTP Server), and integrated address book into active directory.

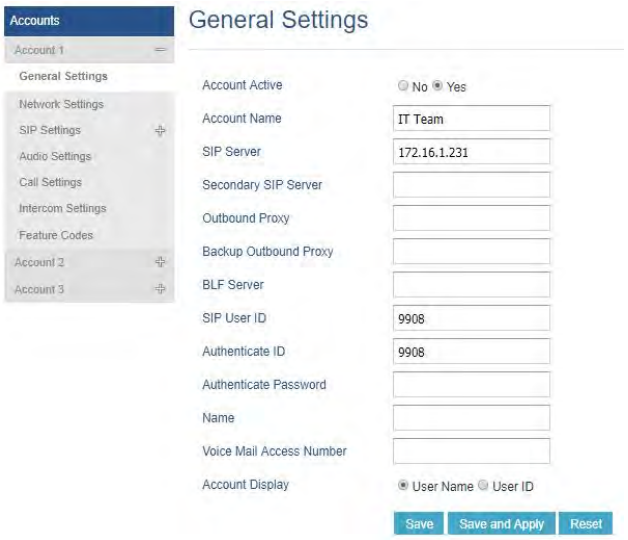

Fig. 2 IP Phone Grandstream Extension configuration via Web base

```
<?xml version="1.0" encoding="utf-8"?>
<gs_provision version="1">
  <config version="1">

<!-- Line 1 - Button Label     --> <P270> IT Team </P270>
<!-- Line 1 - SIP Server IP    --> <P47>172.16.1.231</P47>
<!-- Line 1 - SIP User ID      --> <P35>9908</P35>
<!-- Line 1 - Auth ID          --> <P36>9908</P36>
<!-- Line 1 - Auth Password    --> <P34>9908</P34>

<!-- Line 2 - Button Label     --> <P417></P417>
<!-- Line 2 - SIP Server IP    --> <P402></P402>
<!-- Line 2 - SIP User ID      --> <P404></P404>
<!-- Line 2 - Auth ID          --> <P405></P405>
<!-- Line 2 - Auth Password    --> <P406></P406>

<!-- Firmware Server Path      --> <P192>172.16.1.15/gs-provisioning</P192>
<!-- Config Server Path        --> <P237>172.16.1.15/gs-provisioning</P237>
<!-- Firmware Upgrade Via      --> <P212>1</P212>
<!-- Automatic Upgrade Daily   --> <P194>2</P194>
<!-- Automatic Upgrade Time    --> <P285>1</P285>

<!-- Phonebook Key (ldap )     --> <P1526>1</P1526>
<!-- LDAP Directory            --> <P8020>172.16.1.7</P8020>
<!-- LDAP Server Port          --> <P8021>389</P8021>
<!-- LDAP search base          --> <P8022>OU=4. Users,OU=Luminary Prima,DC=luminaryprima,DC=com</P8022>
<!-- User Name                 --> <P8023>CN=ldap,CN=Users,DC=luminaryprima,DC=com</P8023>
<!-- Password                  --> <P8024>directory</P8024>
<!-- LDAP Number Filter        --> <P8025>(|(telephoneNumber=%)(mobile=%)(ipPhone=%))</P8025>
<!-- LDAP Name Filter          --> <P8026>(&(telephoneNumber=*)(cn=%))</P8026>
<!-- LDAP Version              --> <P8027>3</P8027>
<!-- LDAP Name Attributes      --> <P8028>cn sn</P8028>
<!-- LDAP Number Attributes    --> <P8029>mobile telephoneNumber</P8029>
<!-- LDAP Display Name         --> <P8030>cn</P8030>
<!-- Max Hits                  --> <P8031>500</P8031>
<!-- Search Timeout            --> <P8032>30</P8032>
<!-- Sort Results              --> <P8033>0</P8033>
<!-- Incoming calls            --> <P8035>1</P8035>
<!-- Outgoing calls            --> <P8034>1</P8034>
<!-- Lookup Display Name       --> <P8036>cn</P8036>

<!-- NTP Server                --> <P30>10.254.254.1</P30>
<!-- Time Zone                 --> <P64>WIB-7</P64>
<!-- Date (dddd, MMMM dd)      --> <P102>3</P102>

<!-- Weather Update Interval   --> <P1378>360</P1378>
<!-- Temperature Unit          --> <P1379>c</P1379>
<!-- Currency Code             --> <P1381>USD/IDR;EUR/IDR;GBP/IDR;CNY/IDR;AUD/IDR</P1381>

  </config>
</gs_provision>
```

Fig. 3 IP Phone Grandstream Extension configuration via XML Code

Fig. 4 IP Phone Grandstream audio codec configuration

G. *Configuration OpenVPN*

- Certificate CA

/certificate
add name=CA common-name=CA country=ID state=Jakarta locality=Thamrin organization=”Luminary Prima” unit=UOB days-valid=3650 key-size=2048

- Certificate OpenVPN Server

/certificate
add name=Server common-name=Server country=ID state=Jakarta locality=Thamrin organization=”Luminary Prima” unit=UOB days-valid=3650 key-size=2048

- Certificate OpenVPN Client

/certificate
add name=Client common-name=Client country=ID state=Jakarta locality=Thamrin organization=”Luminary Prima” unit=UOB days-valid=3650 key-size=2048

- Sign Certificate CA, Client dan Server

/certificate
sign cacert ca-crl-host=IP_PUBLIC
sign Server ca=CA
sign Client ca=CA
set Server trusted=yes
set Client trusted=yes

- Eksport Certificate Client and Private Key

/certificate
export-certificate Client export-passphrase=ovpnclient

- Address Pool Client OpenVPN

/ip pool add name=pool_openvpn ranges=192.168.30.1-192.168.30.10

- Profile OpenVPN

/ppp profile
add dns-server=172.16.100.1 local-address=172.16.100.1 name=OVPN remote-address=pool_openvpnMembuat Username dan Password untuk OpenVPN Client

- Activate Service OpenVPN Server

/interface ovpn-server server
set certificate=Server cipher=aes256 default-profile=OVPN enabled=yes require-client-certificate=yes

IV. SYSTEM TEST RESULTS

There are several scenarios that will be carried out to test the security holes and performance of the VoIP over VPN network.

1. First Scenario. in the first scenario a call is made between the VoIP Client 1 to the VoIP Client 2 using the IP Phone. Two audio codecs are used as a comparison, audio codecs G.711 codec with 64 Kbps bitrate and audio codec G729 codec which has an 8 Kbps bitrate with different call duration, which is 1 minute, 5 minutes and 15 minutes. When client 1 and 2 have communicated, the conversation

that occurs will be captured (tapping), and analyzed the data in it and played (played back) with Wireshark software to find out whether the voice from the speaker on the client 1 and client 2 can be tapped.

2. In the second scenario a VoIP over VPN (OpenVPN) network is built. OpenVPN is used to secure clients outside the office environment and use the Softphone PortGo for the SIP Client and the encryption key used in OpenVPN. If the packet can be played back (play) then the security level of using the VPN is not secure but if it cannot be played back then the level of security is secure.

Analysis and Results QoS for scenario 1

- Delay

Latency is the time required by the package from the sending terminal to get to the receiving terminal. Delay is an important parameter for determining the quality of a VoIP network. Based on the standards of ITU-T for good VoIP quality, the delay must be <150 ms so there is no overlap in communication. Results of the delay calculation in scenario 1, when making a call using the G.711 Codec with a duration of 1 minute it has a delay of 19,990 ms. 5 minutes has a throughput of 19,996 ms and 15 minutes has a delay of 19,997 ms. While the G.729 Codec with a duration of 1 minute has a delay of 19,990 ms. 5 minutes has a delay of 19,996 ms and 15 minutes has a delay of 19,997 ms. From the comparison, it can be seen that the delay that occurs during a conversation or call using the G.729 Codec or using the G.711 Codec is still in good category.

TABLE 3
DELAY CALCULATION RESULT IN SCENARIO 1

No	Codec	Duration	Delay (ms)
1	G.711	1 Minutes	19.990
		5 Minutes	19.996
		15 Minutes	19.997
2	G.729	1 Minutes	19.990
		5 Minutes	19.996
		15 Minutes	19.997

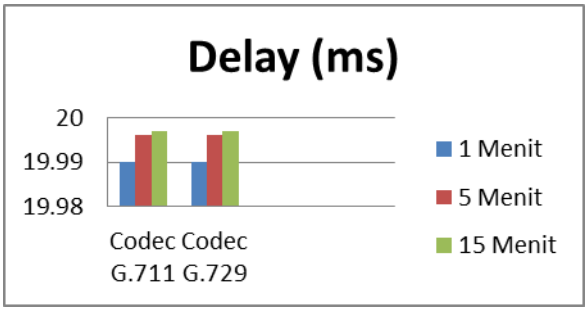

Fig. 5 Graph of Delay Calculation Result in Scenario 1

- Jitter

Jitter measurements are carried out simultaneously with measurements of delay and packet loss. Passing VoIP packages are captured and analyzed. ITU-T recommends is <20 ms. Calculation results of the jitter on the RTP packet it is known that all experiments performed when using Codec G.711 and Codec G.729 around 1.986 ms and 2.030 (ms). that jitter occur are still in the good category

TABLE 4
JITTER CALCULATION RESULT IN SCENARIO 1

No	Codec	Durasi	Jitter (ms)
1	G.711	1 Menit	1.986
		5 Menit	2.097
		15 Menit	2.104
2	G.729	1 Menit	2.008
		5 Menit	2.013
		15 Menit	2.030

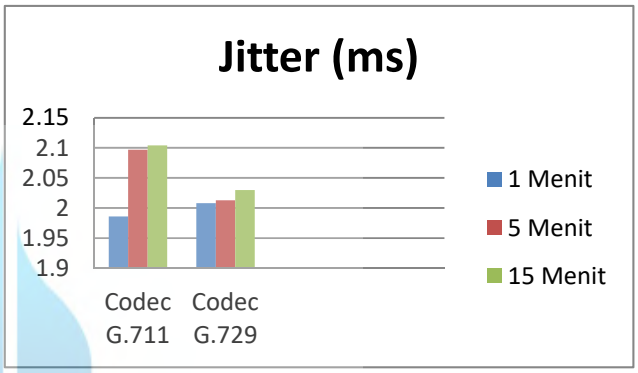

Fig. 6 Graph of Jitter Calculation Result in Scenario 1

Jitter affects to the sound quality. The greater value jitter make sound will be unclear. Jitter value affected when the RTP packet that came will be processed into the sound. When the jitter value is smaller than the data packet processing time, So that the sound produced is good too.

- Packet Loss

Packet loss determines the amount of packet lost on the way from the source address to the destination address. The greater packet loss causes the sound sent will not be heard (lost). According to ITU-T standard, good packet loss is less than 5%. The results of testing for packet loss show that all experiments performed on both the G.711 and G.729 codecs for the duration of 1 Minute, 5 Minutes, and 15 Minutes have a percentage of 0%. which is still in the Good category. The results of packet loss are displayed as shown below:

TABLE 5
RESULT OF PACKET LOSS IN SCENARIO 1

No	Codec	Durasi	Packet Loss (%)
1	G.711	1 Menit	0
		5 Menit	0
		15 Menit	0
2	G.729	1 Menit	0
		5 Menit	0
		15 Menit	0

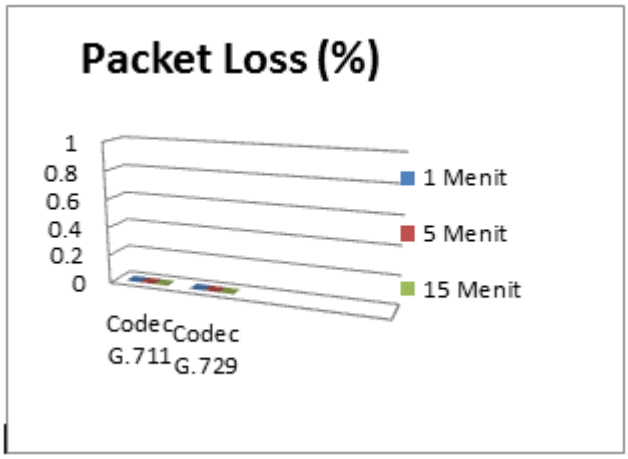

Fig. 7 Graph of Packet loss in Scenario 1

- Throughput

Throughput is to determine the amount of bandwidth needed in the process from the source address to the destination address when the conversation is in progress. From the results of calculation of throughput in scenario 1, when making a call using the G.711 Codec with a duration of 1 minute, it has a 169 Kbps throughput. 5 minutes has a throughput of 170 Kpbs and 5 minutes has a throughput of 171 Kbps. While the G.729 Codec with a duration of 1 minute has a throughput of 58 Kbps. 5 minutes has a throughput of 59 Kpbs and 15 minutes has a throughput of 59 Kbps. Of the bandwidth needed when conducting a conversation or using the G.729 Codec is lower than using the G.711 Codec. The results of througput are displayed as shown below:

TABLE 6

- THROUGHPUT CALCULATION RESULT IN SCENARIO 1

No	Codec	Durasi	Throughput (kpbs)
1	G.711	1 Menit	169
		5 Menit	170
		15 Menit	171
2	G.729	1 Menit	58
		5 Menit	59
		15 Menit	59

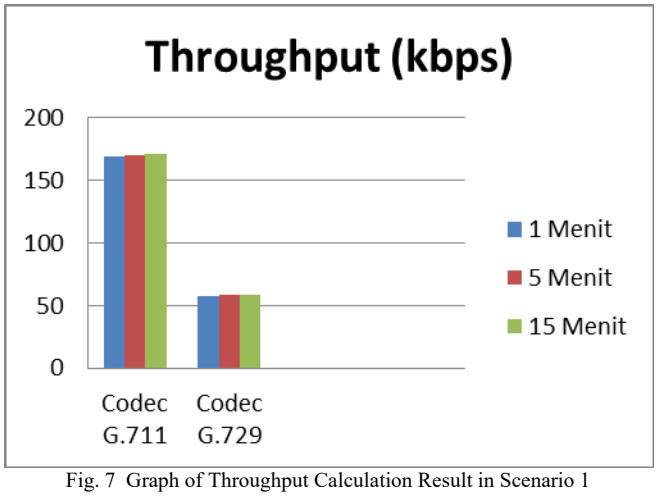

Fig. 7 Graph of Throughput Calculation Result in Scenario 1

ANALYSIS AND RESULTS SECURITY FOR SCENARIO 1

Security threats on VoIP networks can consist of various ways. starting from call piracy, spoofing, Man in the midlle attack, capturing.tapping file. In this scenario, the wiretapping method will be used using Windows-based software, Wireshark. This software will be installed on a laptop that is connected to a hub and connects every packet that passes it. From the results of tapping that can be seen in the wireshark software, a conversation package (RTP) is required between IP Address 10.12.69.12 (Ext. 9908) and IP Address 10.12.69.11 (EXT. 9907).

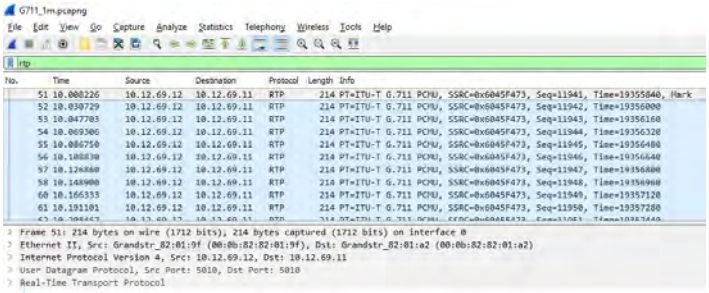

Fig. 8 RTP Packet captured in Wireshark

It was found that the call was between IP Address 10.12.69.12 (Ext. 9908) and IP Address 10.12.69.11 (EXT. 9907). The SIP server (Avaya IP Office Server Edition) is known to have IP Address 172.16.1.231. which can be seen in SIP packet flow sequences captured by wireshark.

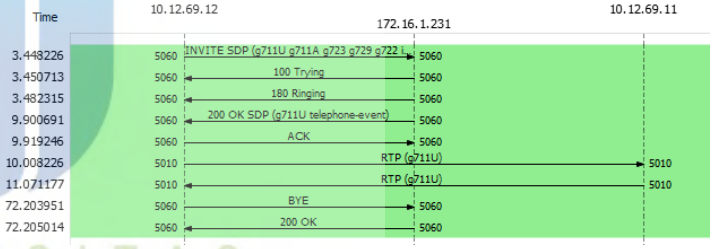

Fig. 9 Flow Diagram SIP Voice Call

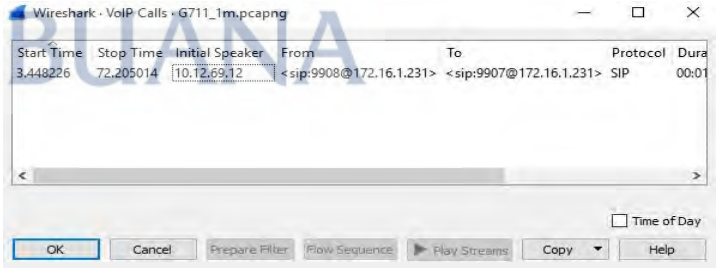

Fig. 10 Voice Call Packet in Wireshark

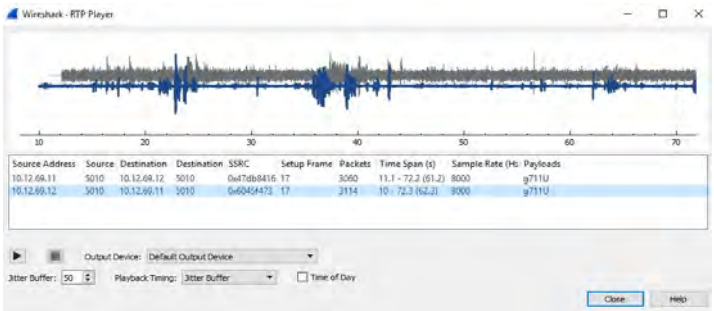

Fig. 11 RTP Player Voice Call in Wireshark

From the packet captured on the wireshark that the conversation carried out by EXT. 9908 and 9907 can be played back again using the RTP Player in the Wireshark application.

ANALYSIS AND RESULTS QOS FOR SCENARIO 2

Analysis of VoIP security using OpenVPN is almost the same as the first scenario. Conversations conducted by client 3 and 1 are tapped using wireshark. From the results of the tapping, there is no RTP package like happened when before using OpenVPN, all that is visible is OpenVPN packets.

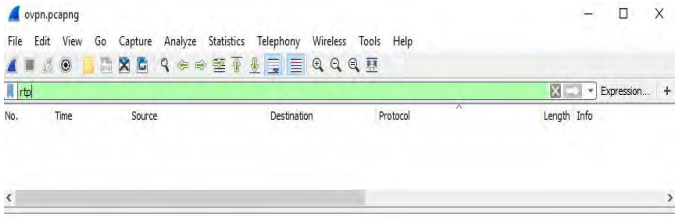

Fig. 12 No RTP Packet captured in Wireshark

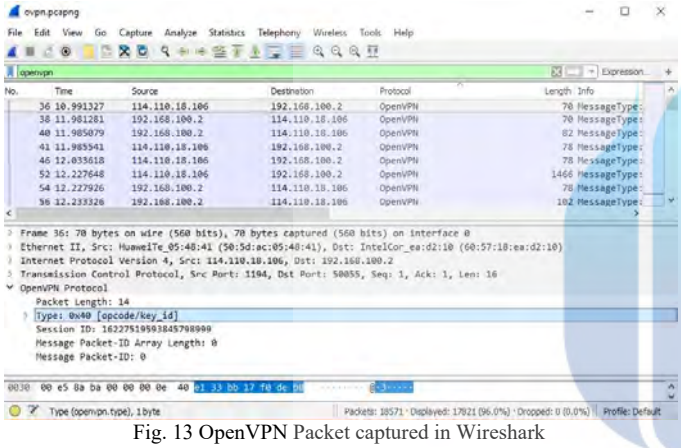

Fig. 13 OpenVPN Packet captured in Wireshark

From the packet captured on the wireshark, there is also no VoIP Call that can be played back by conversations carried out by EXT. 9909 and 9907 can be played back again using the RTP Player that is in the Wireshark application.

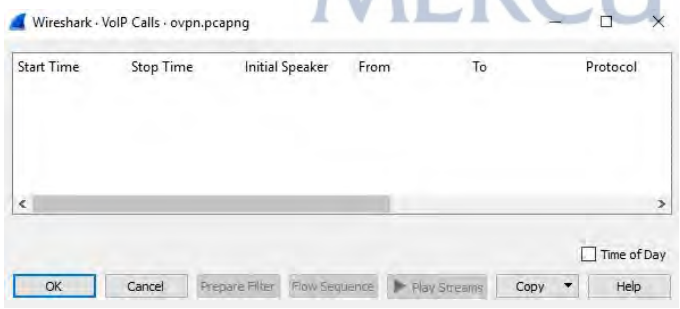

Fig. 14 OpenVPN Packet captured in Wireshark

From the results of security testing when using OpenVPN, it can be seen that when a call is made from the client 3 to the client 1, the RTP packet is not captured. only OpenVPN packets are captured, so they cannot be played back. This shows that making calls using OpenVPN outside the office is safe because packet voice has been encapsulated by OpenVPN.

V. CONCLUSIONS

The results of all experiments that have been carried out in the calculation of QoS and security, the VoIP system using Audio Codec G.711 and G.729 can be concluded that:

1. QoS performance on the VoIP system using Avaya IPO Server at PT. XYZ in the category of Good. This is seen from the results of calculating the average Delay, Jitter, Packet Loss and Throughput into the ITU-T standard.
2. Audio Codec G.711 when compared to Audio Codec G.729, Audio Codec G.729 is more optimal. This can be seen from the results of the average Delay, Jitter and Packet Loss in both Audio Codecs. Although the average results from the two are not too much different but throughput or bandwidth used Audio Codec G.729 is smaller than Audio G.711 Codec. This is very useful for those who have bandwidth limitations.
3. VoIP system security testing at PT. XYZ before using OpenVPN is relatively insecure. Because the conversation data packet (RTP Packet) can still be tapped or captured and played back using the RTP Player conversation.
4. VoIP system security testing at PT. XYZ after using OpenVPN can be said to be safe. Because the RTP packet or conversation data cannot be seen and played back because it has been encapsulated and encrypted.

REFERENCES

[1] Handayani R. Voice over Internet Protocol (VOIP) on Raspberry Pi-based Wireless Networks. Kinetik. 2017;2(2):82. doi:10.22219/kinetik.v2i2.146

[2] Umam C, Roza E, Irfan. Site to Site Virtual Private Network (VPN) Security Network Design. 2016:23-30.

[3] Forda G, Septana HD. Performance Analysis of Voice Over Internet Protocol (VOIP) Based on Session Initiation Protocol (SIP) on IEEE 802.11 Wireless LAN Networks at Lampung University.. Elektro, Fak Tek Lampung, Bandar. 2014:85-96

[4] D. N. R. Ahmad Sven Heddin Timoryansyah, Hafidudin, "Implementation of Voip Server Using Mini Pc," E-Proceeding Applied Science., Vol. 1, No. 3, Pp. 1–8, 2015.

[5] Kango R, Ibrahim I. Quality of Service Analysis of Voice Over Internet Protocol Applications on the AdHoc Mobile Network. 2018;1(November):21-27. doi:http://dx.doi.org/10.31314/jsig.v1i2.175

[6] Basri H, Mulyani A, Budihartanti C. Designing a Wide Area Network at PT. Vizta Pratama Jakarta Branch. J PROSISKO. 2017;4(2):38-43.

[7] Seta HB, Ridwan M, Wati T. Comparison of Virtual Private Network Protocols Using Point to Point Tunnel Protocol and OpenVPN. Konf Nas Sist Inform. 2015;(Perbandingan VPN):1-6.

[8] Wahyu AP, Informatika T, Teknik F, Widyatama U, Kidul C. Local Area Network Optimization Using VLAN and VOIP. J Inform J Pengemb IT Poltek Tegal. 2017;2(1):54-57

[9] Risnandar M, Hendrawan AH, Prakosha BA, Goeritno A. Implementation of Voice Over Internet Protocol (VOIP) Based on Session Initiation Protocol (SIP) using Briker Version 1.4 for Measurement of Quality of Services in Computer Networks at the Faculty of Engineering, Uika Bogor. 2016;(November):1-8.

[10] Maryanto, Maisyaroh, Santoso B. Method of Internet Protocol Security (IPSec) with Virtual Private Network (VPN) for Data Communication. Embed and Logic Systems Computational Science Research. 2018;6(2):179-188.http://jurnal.unismabekasi.ac.id/index.php/piksel/article/view/1508.

[11] Jalendry S, Verma S. A Detail Review on Voice over Internet Protocol (VoIP). Int J Eng Trends Technol. 2015;23(4):161-166. doi:10.14445/22315381/ijett-v23p232

[12] Roy A, Chen X, Dsouza J. Evaluation of VoIP and IPv6 with Jairou. Int J Adv Eng Res Sci. 2018;5(5):333-335. doi:https://dx.doi.org/10.22161/ijaers.5.5.44

[13] Jasim AF, Jasim AD. Simulation analysis of real-time video QoS over IP and IP / MPLS networks. Int J Enhanc Res Sci Technol Eng. 2014;3(6):477-483. www.erpublications.com
[14] Rajput TS, Maheshwar K. VOIP PACKET ANALYZER FOR DETECTING THREATS. Int J Adv Res Comput Sci. 2017;8:613-618. doi:http://dx.doi.org/10.26483/ijarcs.v8i9.5167
[15] Forda G, Septana HD. Analisis Performansi Voice Over Internet Protocol (VOIP) Berbasis Session Initiation Protocol (SIP) Pada Jaringan Wireless LAN IEEE 802 . Universitas Lampung. Elektro, Fak Tek Lampung, Bandar. 2014:85-96
[16] Ida, N. (2019). Quality of Service for Traffic Monitoring System based on Static Routing using EoIP Tunnel over IPSec. Proceedings of the 2019 Asia Pacific Information Technology Conference (pp. 91-99). ACM.
[17] E. Ramadhan, A. Firdausi and S. Budiyanto, "Design and analysis QoS VoIP using routing Border Gateway Protocol (BGP)," 2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), Jakarta, 2017, pp. 1-4. doi: 10.1109/BCWSP.2017.8272556
[18] Karya, O. T., Saesaria, S. S., Budiyanto, S., “RTP analysis for the video transmission process on WhatsApp and Skype against signal strength variations in 802.11 network environments”,2018 IOP Conference Series: Materials Science and Engineering, Volume 453, Issue 1, pp. 012062 (2018).