IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 May 2023, accepted 9 June 2023, date of publication 14 June 2023, date of current version 21 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3286032

RESEARCH ARTICLE

Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol

SETIYO BUDIYANTO[1] AND DADANG GUNAWAN[2], (Senior Member, IEEE)
[1]Department of Electrical Engineering, Universitas Mercu Buana, Jakarta 11650, Indonesia
[2]Department of Electrical Engineering, Universitas Indonesia, Depok, West Java 16424, Indonesia

Corresponding author: Setiyo Budiyanto (sbudiyanto@mercubuana.ac.id)

This work was supported by Universitas Mercu Buana, in 2022.

ABSTRACT Voice over Internet Protocols (VoIP) is an IP-based communication technology or commonly known as Internet Protocols (IP). In which, IP is currently widely used for mobile communication activities. However, the main concern in the application of VoIP technology is the system ability to maintain information confidentiality while guaranteeing protection to its primary users. For this reason, it requires to do the addition of Virtual Private Network (VPN) features. Conceptually, it aims to create connection lines in secret by utilizing the internal network structure (intranet) and to be accessed remotely using tunneling protocols in its security system. The purpose of this research is to compare the Quality of Service (QoS) on several tunneling protocols. Moreover, it is conducted to also analyze several security system mechanisms including Delay, Jitter, Throughput and Packet Loss. This analyzation is used for determining the best quality of some of the piloted tunneling security protocols. Furthermore, this work compares several methods of VoIP voice-call-testing in term of Generic Routing Encapsulation with IPSecurity (GRE+IPSec), Internet Protocol in Internet Protocol based Session Initiation Protocol (IPIP+SIP-based), Secure Socket Layer (SSL), and Layer 2 Tunneling Protocol IPSecurity (L2TP+IPSec). Accordingly, the comparative results show the better performance compared to the existing work, which is proven by the ability of the proposed method to provide the VoIP based on ITU-T.G.1010.

INDEX TERMS VoIP, GRE+IPsec, IPIP+SIP-based, SSL, L2TP, VPN security.

I. INTRODUCTION

The internet's need for the application of communication technologies (voice, video, and data) is bringing about a very vital change in modern times today [1], [2], [3]. This brings changes to the gadget industry to develop technologies that can facilitate current communication needs, one of which is using VoIP (Voice over Internet Protocol) [4], [5], [6]. VoIP is a technology that enables long-distance voice conversation over the internet. According to some VoIP research, there are new ways of communicating that enable users to initiate phone calls over IP networks [7], [8], [9]. The advantage of voip compared to PSTN (Public Switched Telephone Network) is the ability to send voice packets over packet-switched networks so that data-voice packets can use the best lines when compared to circuit-based PSTN technology that requires dedicated lines for telecommunication services.

Voice merging in traffic data can be added to voIP network infrastructure, but some risks include viruses, worms, denial of service (DoS), and other security threats. To secure VoIP communications from the security threats mentioned above, security system mechanisms are needed in data networks such as firewalls, encryption, and Virtual Private Networks (VPNs) [10], [11], [12], [13], [14], [15].

The research method used is an experimental method. That is, collecting some problems that have not been solved in previous research by creating phenomena under controlled conditions and then correlated by using observation techniques and some experiments conducted make this part of the research as a reference to compare some vpn network security methods located in Layer 2 in the VoIP network.

According to [16], [17], and [18], explaining the issue of VoIP research regarding the results of evaluation

The associate editor coordinating the review of this manuscript and approving it for publication was Hongli Dong.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

of performance investigations using IAX (Inter-Asterisk Exchange Protocol) and SIP (Session Initiation Protocol) by measuring QoS levels, then analysis of VoIP performance without VPN with VoIP that implements PPTP (Point-to-Point Tunneling Protocol) VPN. The test results showed that PPTP-VPN cannot be intercepted because the conversation data packet is encrypted by PPTP-VPN so that the codec for the deposit file cannot be read. This means that communication using the SIP protocol and PPTP-VPN is secure and has no loopholes for eavesdropping by irresponsible parties. As VPNs are not just PPTP, this research explores other VoIP-VPN techniques to be used as decision support for the best VoIP-VPN in the design of a built VoIP system.

According to [19] explaining voip research problems regarding QoS VoIP analysis based on measurements of major factors affecting QoS according to ITU (International Telecommunication Union) standards, including delay, jitter and packet loss. In this study, a comparison was conducted between several security mechanisms such as Packet Filter Firewall and Virtual Private Network (VPN).

According to [20] describes the problem of VoIP research regarding exploration and investigation of the rate and magnitude of decreased QoS VoIP traffic running through heterogeneous networks using the OPNET Tool Modeler simulation method.

According to [21] explaining his research problem about simulating IPSec-based VPN tunnel systems can be connected using EVE-NG simulator. The simulation results were calculated and analyzed by QoS on OSPF, RIPv2 and EIGRP routing. The simulation was conducted at EVE-NG by likening a company that has 1 headquarters and 2 branch offices with servers located in the data center. The simulation was conducted on a VoIP service with an asterisk server.

According to [22] describes his research issues regarding the use of the TRIXBOX CE System that allows users to implement VoIP services. One internet protocol (IP) based application is the 3CX Phone System for voice signal [23], [24], [25], video and PSTN (Public Switch Telephone Network). 3CX Phone System [26], [27] facilitates configuration and maintenance over the Web or GUI (Graphical User Interface), making it easier to use.

According to [28] explaining his research problem regarding QoS Tunneling Protocol PPTP and L2TP Performance Comparison on VPN networks using Mikrotik. Because tunneling methods vary, this study compares several methods including GRE+IPSec, IPIP-SIP based, L2TP+IPSec and SSL.

The decrease in QoS (Quality of Service) caused by the use of several complex encryption algorithms is an impact when upgrading the network security system mentioned above [10], [11], [12], [13], [14], [15]. Balance must be agreed between the security system and QoS as long as the security system solution is implemented by minimizing delays, jitters and packet losses to ensure that QoS has been successfully maintained. Thus, the recommendation of voip communication security system in this research is VPN (Virtual Private Network). A VPN is a method that uses tunneling to create a private network on a public network where network security is equivalent to the security provided by a leased line. VPNs have two types of classifications based on network topology: Remote Access VPN and Site-to-site VPN [16], [19], [20], [29]. VoIP communication security system using a VPN [26], [30], [31] such as Generic Routing Encapsulation IPSecurity (GRE+IPSec) [10], [21] Internet Protocol in Internet Protocol Session Initiation Protocol based (IPIP-SIP based) [23], [24], [25], Layer 2 Tunneling Protoocol IP security (L2TP+IPSec) and Secure Socket Layer (SSL) [28], [32], [33].

A. MOTIVATION

The purpose of this research is to analyze VoIP performance with QoS parameters, security in the network by tunneling and using several protocols to produce VoIP quality analysis data, as well as obtaining results from the influence of several security system mechanisms on QoS VoIP and analyzing based on measurement of key factors that affect including: delay, jitter, throughput and packet loss. The hypothesis in this research is to find the best QoS VoIP and ensure that packet delivery is not delayed or lost during transmission over the network.

B. CONTRIBUTION

Contribution to this research is expected to be one of the alternatives to the technical solution of VoIP-based telephony system connection with VPN in accordance with the recommendations of international Telecommunication Union Telecommunication Standardization Sector (ITU-T) and TIPHON standards to support government policies in running work form home and remote working without harming employee productivity and capabilities by utilizing available technologies and systems.

It is expected that this research is theoretically useful for development and knowledge, and the results can enrich the science in particular related to voice telephony connections with the mechanisms of VPN security systems.

II. VOIP AND PROTOCOLS

VoIP is a technology that enables conversations of voice, video and data remotely over internet media or LANs over an IP network. Voice data is converted into digital code and streamed over a network that sends data packets, rather than through the analog circuitry of a regular phone [7], [8], [9]. Multimedia sessions are exchanges between users that can include voice, video, or text. SIP provides communication services for users, for example with RTP (Real Time Transport Protocol) used for real-time data transfer, with SDP (Session Description Protocol) used to describe multimedia sessions, with MEGACO (Media Gateway Control Protocol) used for communication with PSTN (Public Switch Telephone Network).

A VPN is a communication technology that allows users to have the right and settings of connectivity to a public network and use it to join a local network and/or vice versa. A VPN network is built on a tunnel that serves as the path responsible for the security of the data running on it; the VPN tunnel that correlates with this research is L2TP [10], [34]. L2TP is a development of PPTP plus L2F. Network security protocol and encryption are used for the same authentication as PPTP, but in its data communication LTP uses UDP. UDP is one of the main protocols above IP and is a simpler transport protocol compared to TCP.

Internet Protocol Security (IPsec) is a network layer security control widely used to protect data communications [30]. IPSec is a set of specifications to secure communications over the Internet. Its main function is to secure IP communication by verifying each session with individual encryption through both transportation mode and canalization mode. Their primary function is to secure IP communications, encrypting each session in both transport and canalization modes. Transport mode means the message in the data packet is encrypted, while canalization is the data packet as a whole which is encrypted. IPsec supports two types of security communication: [10], [21], [30].

1) AUTHENTICATION HEADER PROTOCOL (AHP)

It provides data authentication and integrity, as well as user authentication and protection against multiple attacks (typically man-in-the-middle attacks). This protocol gives the recipient confidence in the identity of the sender and that the data has been unaltered in transit. The AH protocol provides no encryption against the data being transferred. AH information in the header of the delivered IP packet.

2) ENCAPSULATION SECURITY PAYLOAD (ESP)

This protocol encapsulates and encrypts user data for confidentiality. ESP can provide authentication and protection against multiple attacks. Like AH, ESP information is included in the header of the transmitted IP packet. IPIP works by encapsulating packets from one IP to another, forming a network tunnel. IPIP can be used on almost all routers that support IPIP. However, IPIP cannot be bridged locally. It must use different IP address segments [23], [24], [25].

Tunneling is an alternative for us to connect two or more sites that may be very distant from each other. Tunneling is simple and inexpensive compared to building physical media between sites [10], [21], [30].

III. PROPOSED METHOD

A. SYSTEM DEVELOPMENT METHODS

The steps taken in this research adopt / perform the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) method and become PDEA (Prepare, Design, Experiment and Analyze) steps method as shown in figure 1 [35], [36], [37]. This method was chosen because it contains the right elements to implement. The selection of PDEA method is

FIGURE 1. Research flowchart.

because the PDEA method has more advantages over the cycle of the method. In the PDEA method the method cycle will not stop until the work is completed, so there is continuous optimization until the work done can meet existing needs. This condition is very suitable for the development of VoIP, because VoIP must be reviewed and optimized continuously for a long period of time.

Security when conducting voice communication is very important because it concerns the privacy of its users on the VoIP architecture. VoIP servers using VPNs are a solution to close security gaps in data and voice. A VPN is a computer network that connects between nodes utilizing the public internet network at each site. When implementing a VPN, the interconnection between nodes will have a dedicated virtual path on top of an independent public network. This method is usually used to make communication secure, VPN is one alternative to send data and voice, which is private or secure.

Figure 1 shows that each stage of the PDEA method has an interrelated explanation with the next stage. The ''prepare'' stage starts from identifying problems, and planning the research that will be achieved from this research. In addition, it also prepares supporting devices including servers that serve as database centers, then router devices that create data transmission routes securely, and switches as distributions and connecting several devices either wired or wireless.

The data in this research were obtained from the performance of 1 VoIP server, 3 Routers, 3 Switch and hosts as shown at figure 2.

In the ''design'' step, the target to be achieved is the success of connecting / building communication in 3 different locations (Tangerang, Jakarta, Bandung). The reason is that this research location requires a network connection that is cheap, fast, secure and can communicate with clients in branch offices.

In the ''experiment'' step, the thing to do is to design a network architecture diagram, install forticlient VPN and install wireshark software to measure QoS parameters including delay, jitter, packet loss, and throughput to the protocol to be tested and compared to the best protocol between GRE+IPSec, IPIP-SIP based, L2TP+IPSec and Secure Socket Layer (SSL). Finally, implementation of hardware and software configurations.

In the ''analyze'' phase is the last stage in the PDEA method, the thing to do is to monitor, retrieve data and

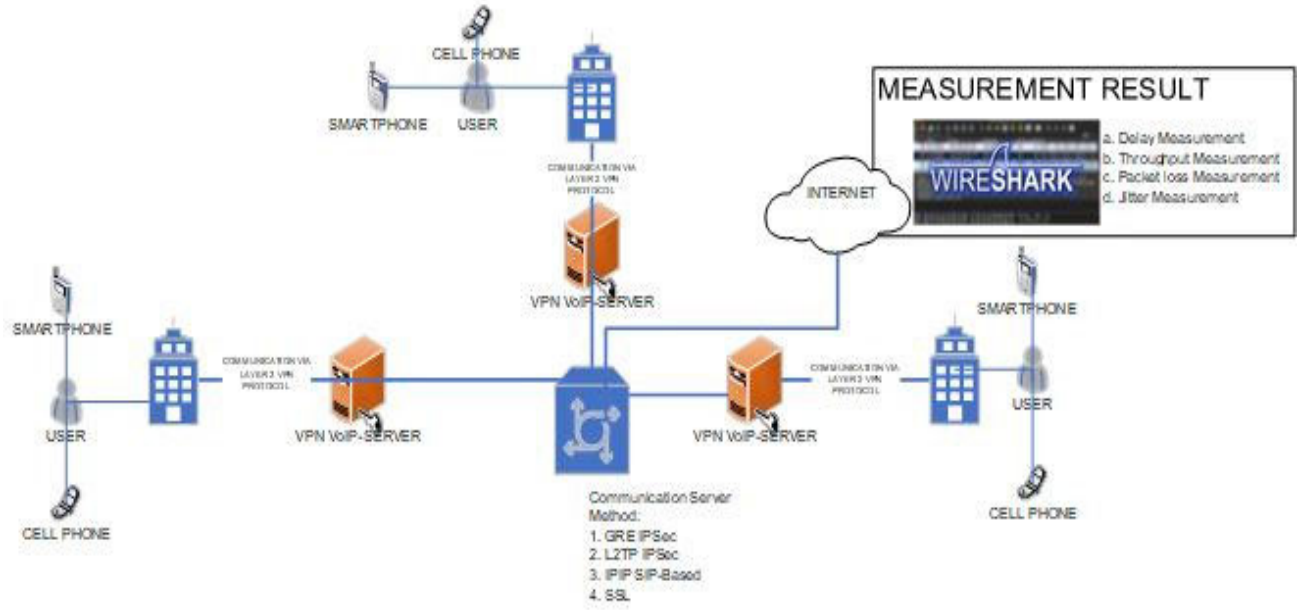

FIGURE 2. Research topology.

perform system analysis. The results are then analyzed and adjusted the best installation system to the protocol to be tested and evaluated.

1) GRE+IPSEC CONFIGURATION

After the server computer settings are successfully installed until the remote address parameters have been addressed to each client location, then add the Keepalive function that aims when the link from the tunnel down, the router will keep the tunnel interface running. IP address tunnel Rtr_Tgr (Router Tangerang) – Rtr_Jkt (Router Jakarta) is located at IP 118.22.85.0/24 as shown at Figure 3a and Figure 3b, then IP address tunnel Rtr_Jkt (Router Jakarta) – Rtr_Bdg (Router Bandung) is located at IP 119.85.22.0/24 as shown at Figure 3c and Figure 3d.

2) IPIP-BASED CONFIGURATION

Figure 4 shows the appearance of configuration settings on the IPIP tunnel. The parameters ''Local Address and Remote Address'' must be filled in and equipped by entering the Public IP on each router.

1. Figure 4a
   Local Address: 119.22.85.1
   Remote Address: 119.22.85.2
2. Figure 4b
   Local Address: 119.22.85.2
   Remote Address: 119.22.85.1
3. Figure 4c
   Local Address: 118.22.85.2
   Remote Address: 118.22.85.1

3) L2TP+IPSEC CONFIGURATION

Figure 5 shows the appearance of configuration settings in the L2TP+IPSec tunnel. The ''Destination Address Gateway'' parameter must be filled in and equipped with entering the Existing Public IP on each router.

4) SSLVPN CONFIGURATION

Figure 6 shows the appearance of configuration settings on the SSL tunnel. The parameters ''Remote Gateway and Customize Port'' must be filled and equipped.

B. QUALITY OF SERVICE PARAMETER

QoS is the ability to provide better network traffic services by providing throughput, packet loss, jitter and controlled delays. This research refers to the standardization of ITU-T. G.1010 regarding the value limit that has been determined in order to ensure QoS can be accepted or felt by both users. Some of the disruptions that occur in network wire and wireless can occur and are difficult to avoid. These disruptions can decrease the performance of a network. Here are some parameters used to determine the performance of a network and the value limit of the ITU-T standard. G.1010 [38], [39], [40].

1) DELAY

Delay is the time data takes to travel from source to destination. Delay can be affected by distance, physical congestion, or processing time. Delay category calculation using Eq. 1. Where Delay is equal to long observations (Lo) divided by the total packages received ($\sum$PR) Table 1 shows delay categories by ITU-T. G.1010 [38], [39], [40]:

$$Delay = \frac{Lo}{\sum PR} \tag{1}$$

2) JITTER

Jitter is a variation in queue length, data processing time, and also the time to re-evaluate packets at the end of the

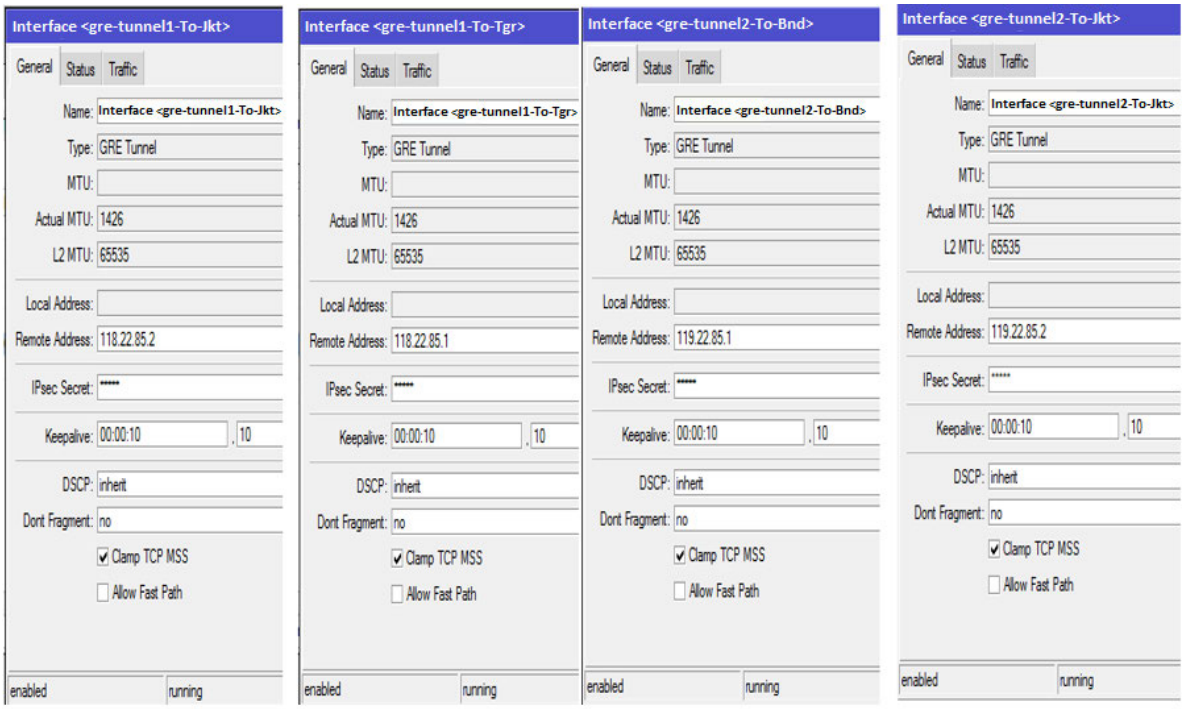

FIGURE 3. GRE+IPSec tunnel configuration.

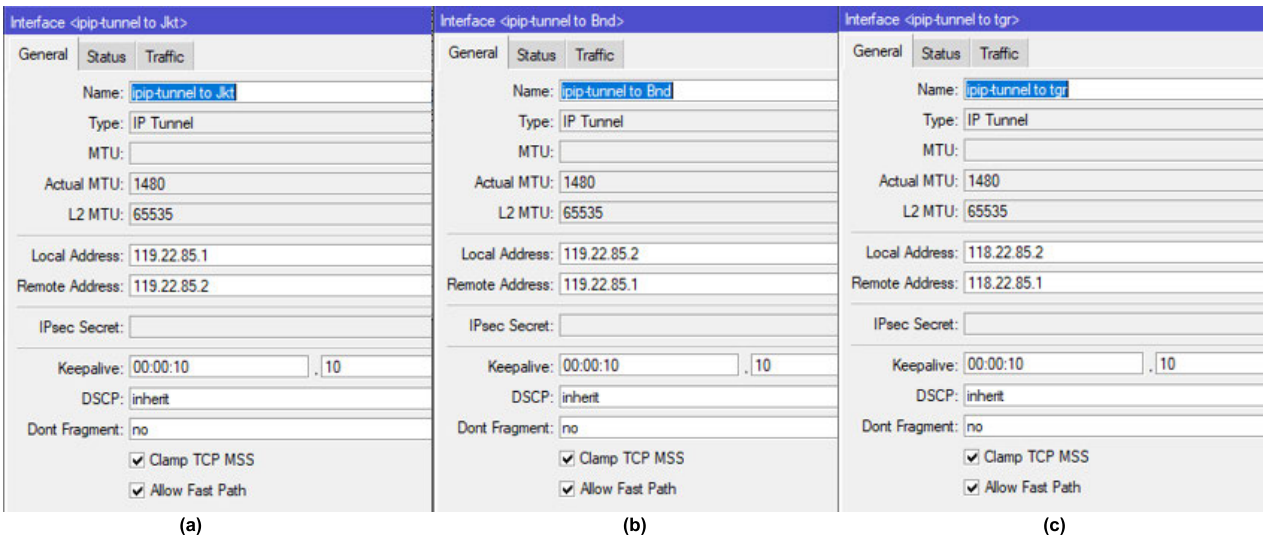

FIGURE 4. IPIP-SIP based configuration.

TABLE 1. Delay.

Category	Delay	Index
Very Good	< 150 ms	4
Good	150 up to 300 ms	3
Normal	300 up to 450 ms	2
Bad	> 450 ms	1

trip. The QoS calculation of the Jitter category as shown in Eq. 2. Where Jitter equals total Delay Variation ($\sum$DV) divided by total Packages Received ($\sum$PR). Table 2 shows jitter category by ITU-T. G.1010 [38], [39], [40]:

$$Jitter = \frac{\sum DV}{\sum PR} \tag{2}$$

3) PACKET LOSS

Packet loss is a parameter which describes the total number of packets lost because of collisions or network congestion. QoS calculation of Packet Loss Category as shown in Eq. 3. Where Packet Loss equals Send-Receive packets (SDP-RDP)

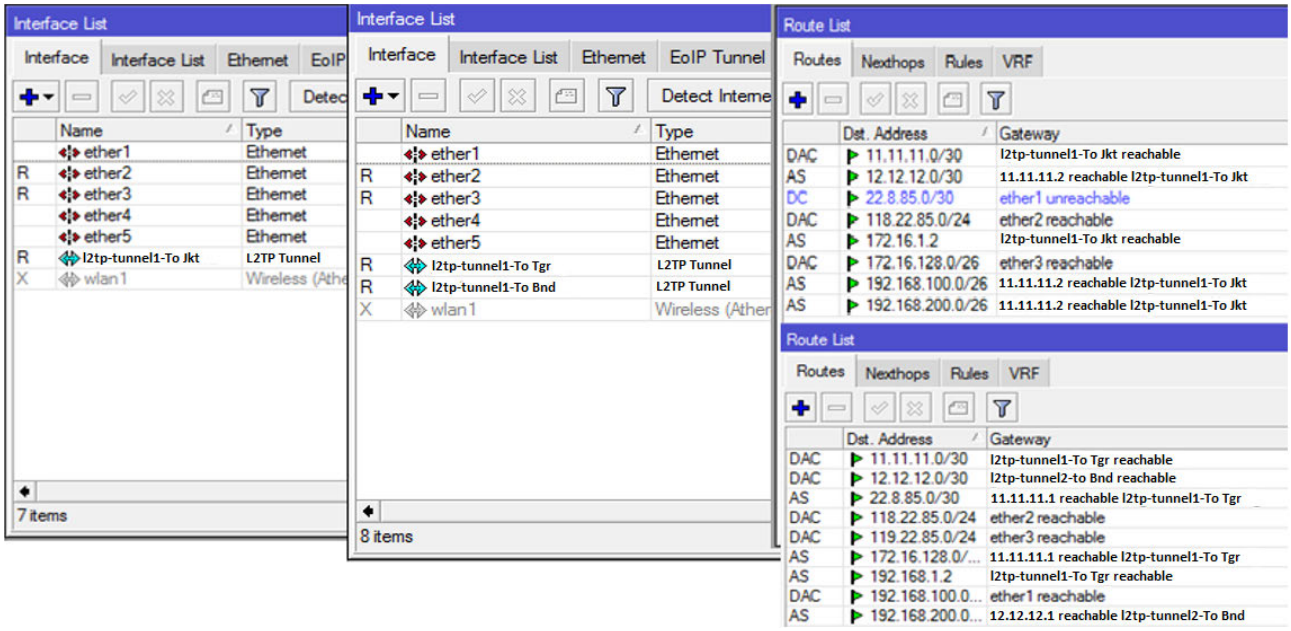

FIGURE 5. L2TP + IPSec configuration.

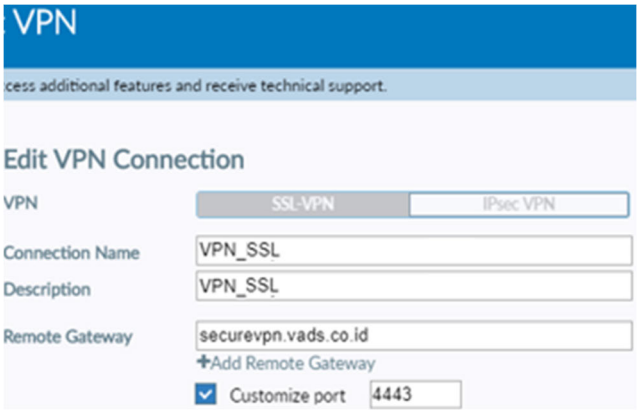

FIGURE 6. SSL VPN configuration.

TABLE 2. Jitter.

Category	Jitter	Index
Very Good	0 ms	4
Good	0 up to 75 ms	3
Normal	75 up to 125 ms	2
Bad	125 up to 225 ms	1

divided by SDP. Table 3 shows packet loss category by ITU-T.G.1010 [38], [39], [40]:

$$Packet\ Loss = \frac{SDP - RDP}{SDP} \tag{3}$$

4) THROUGHPUT

Throughput is the total number of successful packet arrivals observed at the destination during a given time interval,

TABLE 3. Packet loss.

Category	Packet Loss	Index
Very Good	0%	4
Good	3%	3
Normal	15%	2
Bad	25%	1

TABLE 4. Throughput.

Category	Throughput	Index
Very Good	> 1200 Kbps	4
Good	700-1200 Kbps	3
Normal	338-700 Kbps	2
Bad	0-338 Kbps	1

divided by the duration of that time interval. QoS calculation of throughput category as per Eq. 4. Where throughput is equal to RDP divided by Lo. Throughput is measured in bits per second. Table 4 shows throughput category by ITU-T.G.1010 [38], [39], [40]:

$$Throughput = \frac{RDP}{Lo} \tag{4}$$

IV. RESULT AND DISCUSSION

These tests examine QoS in VoIP communications networks using 4 tunnel techniques. Delay, packet loss, jitter and throughput are the QoS parameters tested. VoIP servers are used for call testing and softphones on client side. GRE Tunnel+IPSec, IPIP-SIP based, SSL and L2TP IPsec methods configured at each site are used for VoIP call testing. Each active site is tested with 5 calls per tunnel in turn. Each

parameter affecting QoS performance on a VoIP network can be analysed against ITU-T.

A. TUNNEL+IPSEC

QoS GRE Tunnel+IPSec data experiments were performed on all tunnels used and data is known from Wireshark in each client. Table 5 presents the average test results.

Data collection has been carried out with respect to the results shown in Table 5. The packet loss results show 0 (zero) which is categorized as ''Very Good'' indicating that no packets are lost during transmission. This shows a positive characteristic towards the reliability of the voice communication (VoIP) designed is very good when working on the GRE IPsec protocol.

The delay results produced an average of 10.1018ms during the 5 (five) days of monitoring, categorized as ''Very Good'' based on the ITU-T.G.1010 standard. This implies that the delay experienced by the transmitted packets is low. This becomes very important for real-time services designed today. Therefore, it is beneficial and ensures that the communication that has been designed is efficient and responsive.

The jitter results show an average of 10.333ms during the 5 (five) day monitoring, this is categorized as ''Good'' based on the ITU.T.G.1010 standard. That is, it indicates that the variation in delay between packets is minimal. A ''good'' level of jitter implies a stable and predictable delay, which is desirable for maintaining the quality of time-sensitive applications.

The throughput results show an average of 139.8Kbps during the 5 (five) days monitoring, this is categorised as ''Bad'' based on the ITU.T.G.1010 standard. This indicates that the data transfer rate is to focus on voice communication (VoIP).

Analysis of the GRE IPsec protocol shows success based on the merging of two technologies, namely GRE and IP security (IPsec). This combination provides secure and private communication over IP-VPN networks. Analysis of GRE IPsec shows positive aspects such as ''zero'' packet loss, ''Low'' delay, and ''Good'' jitter, but ''Bad'' throughput due to limitations in design and infrastructure in the design still supports VoIP communication.

B. IPIP-SIP BASED

QoS IPIP-SIP based VPN data experiments were performed on all tunnels used and data is known from Wireshark in each client. Table 6 presents the average test results.

The IPIP-SIP protocol is a combination of IPIP and SIP protocols used to tunnel IP packets and manage communication sessions. Compared to GRE IPsec, IPIP-SIP shows promising characteristics with zero packet loss, excellent delay, and good jitter. However, the identified issues with throughput indicate limitations in design and infrastructure.

The packet loss results show 0 (zero) which is categorized as ''Very Good'' indicating that this protocol design has been reliable in ensuring data transmission with no loss of

TABLE 5. Average QoS test of VoIP calls using GRETUNNEL+IPSEC.

Information	Call	Delay (ms)	Throughput (Kbps)	Packet Loss (%)	Jitter (ms)
Average TGR to JKT		10.1116	141.52	0	9.83752
Day 1					
08.00-12.00	1	10.552	149	0	10.512
	2	10.43	138	0	10.495
	3	10.351	135	0	10.481
13.00-16.00	4	9.985	130	0	9.97
	5	9.848	129	0	9.86
Day 2					
08.00-12.00	1	10	180	0	10.5
	2	10.11	145	0	10.27
	3	11.11	140	0	10.93
13.00-16.00	4	9.99	127	0	10.00
	5	9.05	130	0	10.01
Day 3					
08.00-12.00	1	9.03	150	0	9.46
	2	9.99	147	0	9.33
	3	10.017	135	0	9.99
13.00-16.00	4	10.223	135	0	10.45
	5	10.313	130	0	10.52
Day 4					
08.00-12.00	1	11	160	0	10.45
	2	10.87	155	0	10.79
	3	10.771	150	0	9.87
13.00-16.00	4	10.69	147	0	10.15
	5	10.39	135	0	10.27
Day 5					
08.00-12.00	1	10.11	150	0	10.33
	2	9.18	127	0	10
	3	9.77	138	0	10.27
13.00-16.00	4	10.01	141	0	10.15
	5	8.99	135	0	9.88
Average JKT to BDG		10.1712	140.96	0	10.24232
Day 1					
08.00-12.00	1	10.565	150	0	10.615
	2	10.443	139	0	10.598
	3	10.364	136	0	10.584
13.00-16.00	4	10.565	131	0	10.073
	5	A9.861	130	0	9.963
Day 2					
08.00-12.00	1	10.555	155	0	10.61
	2	10.433	140	0	10.588
	3	10.354	139	0	10.578
13.00-16.00	4	10.55	132	0	10.173
	5	9.851	131	0	9.973
Day 3					
08.00-12.00	1	10.5	149	0	10.6
	2	10.47	147	0	10.5
	3	10.29	148	0	10.21
13.00-16.00	4	10.555	130	0	10.37
	5	9.13	133	0	9.98
Day 4					
08.00-12.00	1	10.523	147	0	10.5
	2	10.42	150	0	10.47
	3	10.331	141	0	10.43
13.00-16.00	4	9.05	137	0	9.97
	5	9.50	142	0	9.47
Day 5					
08.00-12.00	1	10.54	145	0	10.64
	2	10.547	149	0	10.647
	3	10.413	138	0	10.513
13.00-16.00	4	9	148	0	9.233
	5	9.47	137	0	9.57

TABLE 5. *(Continued.)* **Average QoS test of VoIP calls using GRETUNNEL+IPSEC.**

Average TGR to JKT to BDG		10.0226	136.92	0	10.0192
Day 1					
08.00-12.00	1	10.191	155	0	10.192
	2	10.069	144	0	10.175
	3	9.99	141	0	10.161
13.00-16.00	4	10.191	136	0	9.65
	5	9.487	135	0	9.54
Day 2					
08.00-12.00	1	10.181	153	0	10.292
	2	10.169	140	0	10.275
	3	10.19	143	0	10.261
13.00-16.00	4	10.211	139	0	9.75
	5	9.497	137	0	9.64
Day 3					
08.00-12.00	1	10.211	150	0	10
	2	10.177	138	0	10.150
	3	10.12	133	0	10.117
13.00-16.00	4	10.311	151	0	10.123
	5	9.5	142	0	10.135
Day 4					
08.00-12.00	1	10.197	157	0	10.35
	2	10.277	135	0	10.21
	3	10.01	139	0	9.99
13.00-16.00	4	10.271	127	0	9.87
	5	9.671	141	0	9.77
Day 5					
08.00-12.00	1	10.187	149	0	10.127
	2	10.073	137	0	10.232
	3	9.89	140	0	10.15
13.00-16.00	4	10.177	133	0	9.57
	5	9.317	128	0	9.75
Average		10.1018	139.8	0	10.033

information data packets. This is a positive analysis, as the design has ensured the integrity of the transmitted data.

Analysis of packet loss indicates that the design of this protocol ensures reliable data delivery without loss. This is a positive aspect, as it guarantees the integrity of the transmitted data.

The resulting delay averaged 9.734ms during 5 (five) days of monitoring, this is categorized as ''Very Good'' based on the ITU.T.G.1010 standard. This shows that the protocol design has been successfully optimized with low delay results.

The resulting jitter averaged 9.78776ms during 5 (five) days of monitoring, this is categorized as ''Good'' based on the ITU.T.G.1010 standard. This shows that the protocol design has successfully minimized the delay variation between packets. This delay stability is beneficial for maintaining consistent and smooth transmission, especially for real-time applications.

The resulting throughput averaged 146.17Kbps during the 5 (five) days of monitoring, which is categorized as ''Bad'' based on the ITU.T.G.1010 standard. This indicates that the network infrastructure cannot efficiently handle large-scale data transfer rates because this research focuses on voice communication (VoIP).

TABLE 6. **Average QoS test of VoIP calls using IPIP-SIP based.**

Information	Call	Delay (ms)	Throughput (Kbps)	Packet Loss (%)	Jitter (ms)
Average TGR to JKT		9.64248	142.44	0	9.688
Day 1					
08.00-12.00	1	9.98	148	0	9.87
	2	9.858	137	0	9.853
	3	9.779	134	0	9.839
13.00-16.00	4	9.413	129	0	9.328
	5	9.276	128	0	9.218
Day 2					
08.00-12.00	1	10.273	150	0	9.981
	2	9.98	148	0	9.89
	3	9.863	137	0	9.971
13.00-16.00	4	9.776	144	0	9.813
	5	9.67	127	0	9.757
Day 3					
08.00-12.00	1	9.67	152	0	9.77
	2	9.71	151	0	9.81
	3	9.55	149	0	9.65
13.00-16.00	4	9.83	131	0	9.93
	5	8.99	147	0	9.89
Day 4					
08.00-12.00	1	9.91	151	0	10.21
	2	9.67	149	0	9.77
	3	8.817	131	0	8.92
13.00-16.00	4	9.53	140	0	9.67
	5	9.77	145	0	9.87
Day 5					
08.00-12.00	1	9.78	155	0	9.88
	2	9.51	150	0	9.61
	3	9.877	149	0	9.94
13.00-16.00	4	9.73	138	0	8.85
	5	8.85	141	0	8.91
Average JKT to BDG		9.81512	141.8	0	9.86136
Day 1					
08.00-12.00	1	10.38	164	0	10.35
	2	10.258	153	0	10.333
	3	10.179	150	0	10.319
13.00-16.00	4	9.813	145	0	9.808
	5	9.676	144	0	9.698
Day 2					
08.00-12.00	1	9.985	148	0	10.01
	2	10.43	148	0	10.33
	3	10.552	150	0	10.417
13.00-16.00	4	8.99	129	0	9.123
	5	9.861	128	0	9.99
Day 3					
08.00-12.00	1	10.565	150	0	10.65
	2	9.851	137	0	9.76
	3	9.05	129	0	9.13
13.00-16.00	4	10.4	128	0	10.287
	5	9.85	131	0	9.95
Day 4					
08.00-12.00	1	9.317	140	0	9.41
	2	9.671	145	0	9.57
	3	9.5	127	0	9.55
13.00-16.00	4	10.01	143	0	10.13
	5	9.317	147	0	9.42
Day 5					
08.00-12.00	1	9.98	131	0	9.88
	2	9.99	140	0	10.19
	3	9.487	151	0	9.56
13.00-16.00	4	9.276	149	0	9.349
	5	8.99	138	0	9.32

TABLE 6. *(Continued.)* **Average QoS test of VoIP calls using IPIP-SIP based.**

Average TGR to JKT to BDG		9.744	149.88	0	9.81392
Day 1					
08.00-12.00	1	10.191	166	0	10.192
	2	10.069	155	0	10.175
	3	9.99	152	0	10.161
13.00-16.00	4	9.624	147	0	9.65
	5	9.487	146	0	9.54
Day 2					
08.00-12.00	1	9.962	150	0	10.13
	2	9.847	156	0	9.95
	3	9.98	145	0	9.79
13.00-16.00	4	10.01	151	0	9.99
	5	9.487	155	0	9.49
Day 3					
08.00-12.00	1	9.313	153	0	9.43
	2	9.258	150	0	9.33
	3	9.871	144	0	9.97
13.00-16.00	4	9.808	143	0	9.91
	5	9.698	144	0	9.71
Day 4					
08.00-12.00	1	9.71	150	0	9.81
	2	9.83	151	0	9.93
	3	9.67	149	0	9.77
13.00-16.00	4	9.813	150	0	9.91
	5	9.676	148	0	9.77
Day 5					
08.00-12.00	1	9.069	147	0	9.3
	2	9.675	148	0	9.77
	3	9.926	145	0	9.84
13.00-16.00	4	9.837	150	0	9.94
	5	9.799	152	0	9.89
Average		9.734	144.71	0	9.78776

The steps that have been taken to optimize and succeed better than GRE IPsec analysis is to evaluate the network infrastructure has been done mitigation process and reconfiguration using IPIP-SIP based protocol and it can be seen that on day-3 there is a very significant improvement that has been done between VoIP communication from site TGR to JKT, JKT to BDG, TGR to JKT to BDG.

The application of QoS mechanisms to prioritize IPIP-SIP traffic by ensuring that it receives sufficient bandwidth and higher priority than other traffic. Compared to GRE IPsec, IPIP-SIP shows better performance in terms of packet loss, delay, and jitter. By assessing and optimizing the infrastructure, implementing QoS mechanisms, optimizing protocols, and using load-balancing techniques, the throughput of IPIP-SIP can be improved, leading to an overall improvement in performance.

C. L2TP IPSEC

QoS L2TP IPSec data experiments were performed on all tunnels used and data is known from Wireshark in each client. Table 7 presents the average test results.

L2TP IPsec refers to a combination of two protocols: Layer 2 Tunneling Protocol (L2TP) which functions as a tunneling and data encapsulation process, and IP Security (IPsec) which functions to provide security and encryption

TABLE 7. Average QoS test of VoIP calls using L2TP+IPSEC.

Information	Call	Delay (ms)	Throughput (Kbps)	Packet Loss (%)	Jitter (ms)
Average TGR to JKT		9.839704	148	0	9.89004
Day 1					
08.00-12.00	1	9.98	148	0	9.87
	2	9.858	137	0	9.853
	3	9.779	134	0	9.839
13.00-16.00	4	9.413	129	0	9.328
	5	9.276	128	0	9.218
Day 2					
08.00-12.00	1	10.2332	136	0	10.264
	2	10.3596	137	0	10.367
	3	9.9856	142	0	9.9436
13.00-16.00	4	10.1928	138	0	10.191
	5	9.77	141	0	9.87
Day 3					
08.00-12.00	1	9.6612	135	0	9.6216
	2	10.0612	151	0	10.102
	3	9.8722	153	0	9.943
13.00-16.00	4	9.864	146	0	9.88
	5	9.94	152	0	10.1
Day 4					
08.00-12.00	1	9.6612	142	0	9.6216
	2	9.9856	151	0	9.9856
	3	9.8722	153	0	9.943
13.00-16.00	4	9.84	148	0	9.85
	5	9.91	145	0	10.032
Day 5					
08.00-12.00	1	9.6612	167	0	9.6216
	2	9.743	171	0	10.102
	3	9.6216	183	0	9.943
13.00-16.00	4	9.67	173	0	9.88
	5	9.782	160	0	9.882
Average JKT to BDG		9.75188	144.08	0	9.67908
Day 1					
08.00-12.00	1	10.38	164	0	10.35
	2	10.258	153	0	10.333
	3	10.179	150	0	10.319
13.00-16.00	4	9.813	145	0	9.808
	5	9.676	144	0	9.698
Day 2					
08.00-12.00	1	9.877	150	0	9.756
	2	9.777	159	0	9.689
	3	9.666	147	0	9.547
13.00-16.00	4	9.012	144	0	8.912
	5	9.121	155	0	9.001
Day 3					
08.00-12.00	1	9.97	132	0	9.879
	2	9.847	154	0	9.751
	3	9.514	145	0	9.651
13.00-16.00	4	9.628	123	0	9.897
	5	9.532	132	0	9.632
Day 4					
08.00-12.00	1	9.786	134	0	9.123
	2	9.869	136	0	9.258
	3	9.237	139	0	9.159
13.00-16.00	4	9.547	128	0	9.357
	5	9.236	129	0	9.267
Day 5					
08.00-12.00	1	9.897	140	0	9.987
	2	10.012	155	0	9.978
	3	10.21	151	0	10.12
13.00-16.00	4	9.97	149	0	9.847
	5	9.78	144	0	9.658

TABLE 7. *(Continued.)* **Average QoS test of VoIP calls using L2TP+IPSEC.**

Average TGR to JKT to BDG		9.701	146.44	0	9.6175
Day 1					
08.00-12.00	1	10.191	166	0	10.192
	2	10.069	155	0	10.175
	3	9.99	152	0	10.161
13.00-16.00	4	9.624	147	0	9.65
	5	9.487	146	0	9.54
Day 2					
08.00-12.00	1	9. 6612	150	0	9. 6216
	2	9. 9856	151	0	9. 35
	3	9. 84	145	0	9. 319
13.00-16.00	4	9. 9856	148	0	9. 191
	5	9. 276	146	0	9. 102
Day 3					
08.00-12.00	1	9.77	147	0	9. 9856
	2	9. 8722	140	0	9. 943
	3	9. 6216	145	0	9. 882
13.00-16.00	4	9. 782	138	0	9. 333
	5	9. 258	137	0	9. 319
Day 4					
08.00-12.00	1	9. 743	150	0	9. 689
	2	9. 6612	154	0	9. 912
	3	9.67	147	0	9. 001
13.00-16.00	4	9. 782	136	0	9. 179
	5	9.877	135	0	9. 676
Day 5					
08.00-12.00	1	9. 3596	141	0	9. 777
	2	9. 012	142	0	9. 813
	3	9. 847	146	0	9. 666
13.00-16.00	4	9. 628	148	0	9. 121
	5	9. 532	149	0	9. 84
Average		9.76	146.17	0	9.73

process on the transmitted data that has been working within the VPN network.

Data collection has been carried out with respect to the results shown in Table 7. The packet loss results show 0 (zero) which is categorized as ''Very Good'' indicating that all transmitted packets have perfectly reached their destination without any information being lost. This shows a positive characteristic towards the reliability of the voice communication (VoIP) design is very good when working on the L2TP IPsec protocol.

The resulting delay averaged 9.76ms during 5 (five) days of monitoring, this is categorized as ''Very Good'' based on the ITU.T.G.1010 standard. This shows that the transmitted delay is low, meaning that in real-time the results of this design have been carried out and have successfully worked in the L2TP IPsec network.

The resulting jitter averaged 9.73ms during the 5 (five) days of monitoring, which is categorized as ''Good'' based on the ITU.T.G.1010 standard. This implies that the delay variation between packets is minimal. This is very important in maintaining consistent and smooth transmission in VoIP voice communication networks.

The resulting throughput averaged 146.17Kbps during the 5 (five) days of monitoring, this is categorized as ''Bad'' based on the ITU.T.G.1010 standard. This shows that the speed of data transfer on the network is due to the communication that is carried out being limited to cross-voice communication so this shows that this design is not effective in sending data on a large scale because the tests carried out are in the voice communication channel.

So the analysis of L2TP IPsec shows a positive analysis of packet loss, delay, and jitter. However, the throughput results show limitations on bandwidth, the implementation of QoS mechanisms is optimal and can help improve the overall performance of L2TP IPsec and increase throughput better than the conditions in testing on GRE IPsec and IPIP-SIP based as evidenced on day-2.

D. SSL

QoS SSL VPN data experiments were performed on all tunnels used and data is known from Wireshark in each client. Table 8 presents the average test results.

SSL is a cryptographic protocol that provides secure communication over networks. Analysis based on table 8 shows:

Strengths:

1. Security: SSL ensures the confidentiality, integrity, and authenticity of data transmitted over the network.
2. Zero Packet Loss: There is no packet loss, indicating that SSL has successfully maintained the integrity of transmitted packets.
3. Delay that results in an average of 9.574ms during 5 (five) days of monitoring, is categorized as ''Very Good'' based on the ITU.T.G.1010 standard: Describing delay as ''Very Good'', this shows that SSL is designed to minimize latency.
4. The resulting jitter averaged 9.671ms during the 5 (five) days of monitoring, categorized as ''Good'' based on the ITU.T.G.1010 standard: Indicates that SSL effectively minimizes variations in delay between packets. This delay stability contributes to consistent and smooth transmission, especially for real-time applications.

Weakness:

The resulting throughput averaged 154.61Kbps over the 5 (five) days of monitoring, which is categorized as ''Bad'' based on the ITU.T.G.1010 standard: This weakness identified in throughput suggests that SSL may struggle to efficiently handle high data transfer rates and in reality, this test is a voice communication (VoIP) test.

Opportunities:

1. Protocol Upgrades: The SSL protocol can be enhanced or upgraded to increase throughput without compromising security, as well as offer better performance optimization and throughput.
2. Hardware Acceleration: Utilising hardware acceleration techniques, such as SSL/TLS offloading or dedicated cryptographic processors, can help improve SSL throughput by offloading cryptographic operations from the main server CPU.

TABLE 8. Average QoS test of VoIP calls using SSL.

Information	Call	Delay (ms)	Throughput (Kbps)	Packet Loss (%)	Jitter (ms)
Average TGR to JKT		9.662232	158.9788	0	9.77046
Day 1					
08.00-12.00	1	9.6612	167.2	0	9.6216
	2	9.743	171.2	0	10.102
	3	9.6216	183.2	0	9.943
13.00-16.00	4	9.67	173.87	0	9.88
	5	9.66	170	0	9.99
Day 2					
08.00-12.00	1	9.73	160	0	9.63
	2	9.99	151	0	10.11
	3	9.844	156	0	9.944
13.00-16.00	4	9.89	170	0	9.99
	5	9.77	168	0	9.88
Day 3					
08.00-12.00	1	9.66	150	0	9.77
	2	9.57	170	0	9.67
	3	9.441	155	0	9.541
13.00-16.00	4	9.377	165	0	9.477
	5	9.258	169	0	9.358
Day 4					
08.00-12.00	1	9. 191	150	0	9.291
	2	9. 624	151	0	9.724
	3	9. 9856	153	0	9.77
13.00-16.00	4	9. 77	154	0	9.88
	5	9. 6216	148	0	9.72
Day 5					
08.00-12.00	1	9. 743	147	0	9.84
	2	9. 6612	148	0	9.76
	3	9. 67	147	0	9.77
13.00-16.00	4	9. 782	148	0	9.88
	5	9. 6216	149	0	9.72
Average JKT to BDG		9.454784	153.68	0	9.54824
Day 1					
08.00-12.00	1	9.456	157	0	9.556
	2	9.567	158	0	9.667
	3	9.678	157	0	9.778
13.00-16.00	4	9.123	155	0	9.223
	5	9.321	154	0	9.421
Day 2					
08.00-12.00	1	9.165	148	0	9.265
	2	9.258	157	0	9.358
	3	9.367	154	0	9.467
13.00-16.00	4	9.368	147	0	9.468
	5	9.355	149	0	9.455
Day 3					
08.00-12.00	1	9.111	158	0	9.222
	2	9.255	160	0	9.355
	3	9.377	157	0	9.477
13.00-16.00	4	9.668	158	0	9.768
	5	9.555	154	0	9.666
Day 4					
08.00-12.00	1	9.987	150	0	9.99
	2	9.458	151	0	9.54
	3	9.478	157	0	9.55
13.00-16.00	4	9.234	154	0	9.34
	5	9.123	148	0	9.28
Day 5					
08.00-12.00	1	9. 3596	149	0	9.48
	2	9. 777	149	0	9.75
	3	9. 813	150	0	9.92
13.00-16.00	4	9. 84	157	0	9.94
	5	9. 676	154	0	9.77
Average TGR to JKT to BDG		9.605624	151.16	0	9.69444
Day 1					
08.00-12.00	1	9. 844	150	0	9.94
	2	9. 6216	150	0	9.72
	3	9. 63	157	0	9.763
13.00-16.00	4	9.77	155	0	9.87
	5	9.94	154	0	9.84
Day 2					
08.00-12.00	1	9.541	148	0	9.641
	2	9.67	150	0	9.77
	3	9.77	151	0	9.87
13.00-16.00	4	9.441	155	0	9.541
	5	9.57	152	0	9.67
Day 3					
08.00-12.00	1	9.66	147	0	9.76
	2	9.89	149	0	9.99
	3	9.57	145	0	9.67
13.00-16.00	4	9.74	146	0	9.84
	5	9.67	142	0	9.77
Day 4					
08.00-12.00	1	9.57	148	0	9.67
	2	9.99	150	0	9.89
	3	9.441	151	0	9.541
13.00-16.00	4	9.377	156	0	9.477
	5	9.258	156	0	9.358
Day 5					
08.00-12.00	1	9.66	155	0	9.77
	2	9.441	154	0	9.64
	3	9.258	153	0	9.35
13.00-16.00	4	9.377	153	0	9.47
	5	9.441	152	0	9.54
Average		9.574	154.61	0	9.671

Threats:

1. Network Infrastructure Limitations: SSL performance can be affected by network infrastructure limitations, bandwidth limitations, network congestion, or non-optimal routing.
2. Increased Computational Overhead: SSL involves additional computational overhead due to encryption and decryption operations.

Compared to GRE IPSec, IPIP-SIP, and L2TP IPSec, SSL showed better performance in terms of packet loss, delay, and jitter. Network infrastructure evaluation based on the results of identifying and overcoming bottlenecks or limitations that affect throughput in other protocol schemes has been improved so that it shows optimal results. Then, network equipment (routers and switches) has been successful to increase capacity and performance. To optimise network configuration, including routing protocols and QoS settings.

E. ANALYSIS DATA

Table 9 shows the average results of QoS parameter testing that has been conducted for 5 days in the working time span (08.00 AM – 04.00 PM), obtained the smallest average delay in VoIP call testing using the VPN SSL method of 9.574ms, compared to the IPIP SIP based VPN method of 9.734ms,

TABLE 9. System analysis.

Method	Delay (ms)	Throughput (Kbps)	Packet Loss (%)	Jitter (ms)
VPN GRE+IPSec Tunnel	10.108	139.8	0	10.033
VPN IPIP SIP Based	9.734	144.71	0	9.78776
VPN L2TP IPSec	9.76	146.17	0	9.73
VPN SSL	9.574	154.61	0	9.671

compared to the IPsec L2TP VPN method of 9.864ms, compared to the GRE +IPsec Tunnel method of 10.108ms. The system and method used have been successful and work optimally, so it can be analyzed that ***Delay*** is cumulatively **very good (< 150 ms)** refers to the QoS ITU-T standardization table (Table 1). **Delay** can be caused by several factors that affect it and including distance, physical media, or also a long process time.

In ***Jitter*** testing, the average jitter result that has been done for 5 days in the working time span (08.00 AM – 04.00 PM), it can be analyzed that the smallest jitter uses ssl VPN method of 9.671ms. The cause of ***Jitter*** occurrence is due to failures that occur on the receiving side. Although each of these VPN methods is equally a **good category (0 up to 75 ms)** refers to the QoS ITU-T standardization table (Table 2).

In ***Packet Loss*** testing, the final results showed that each of these VPN methods was equally a **very good category (0%)** referring to the QoS ITU-T (Table 3) standardization table.

In ***Throughput*** testing, the best results when communicating VoIP using the VPN SSL method of 154.61 Kbps compared to VoIP communication using the other three VPN tunneling methods. Although the results have a difference that is not too large, but with a large throughput value can be analyzed that the quality of VoIP communication running on networks that utilize the VPN SSL method is better because the number of packets received is greater than using other VPN tunneling methods. The final results show that each of these VPN methods is equally a **bad category (0 up to 338 Kbps)** referring to the QoS ITU-T.G.1010 (Table 4) standardization table. Some ***Throughput*** factors in bad category research due to several factors that affect it and including distance factors, the type of data transferred is voice data, and weather conditions that cannot be predicted during research.

Based on the final results of the analysis in table 9 shows that the SSL protocol has successfully outperformed the other protocols this is because SSL shows strength in security, no packet loss, excellent delay, and good jitter overall can be significantly improved as follows:

1) Applying data compression techniques to reduce the amount of data transmitted over the network, thereby increasing throughput.
2) Utilising caching mechanisms to store frequently accessed data, thereby reducing the need for retransmissions and improving overall performance.
3) Implementing load-balancing techniques to distribute SSL traffic across multiple servers.
4) Utilising a CDN to offload SSL processing and caching to geographically distributed servers, thereby reducing the load on the main infrastructure and improving performance.

V. CONCLUSION

The results of the experiment that has been analyzed in a system and PDEA method that has been implemented against several VoIP VPN tunneling mechanisms, then in this research concluded that the four voIP tunneling methods can work optimally and run according to the scenario. The best VoIP call quality results are SSL VPN methods that have a delay of 9,574 ms, jitter of 9,671, throughput of 154.61 Kbps and packet loss of 0%. Another method is due to the addition of IPSec, causing the performance of the server CPU is harder caused by the encryption process for security.

REFERENCES

[1] E. E. Cranmer, M. Papalexi, M. C. T. Dieck, and D. Bamford, "Internet of Things: Aspiration, implementation and contribution," *J. Bus. Res.*, vol. 139, pp. 69–80, Feb. 2022, doi: 10.1016/j.jbusres.2021.09.025.
[2] Y. Yin, L. Tan, and X. Zhang, "Commercial application of big data technology in internet economy," in *Innovative Computing*, J. C. Hung, J.-W. Chang, Y. Pei, and W.-C. Wu, Eds. Singapore: Springer, 2022, pp. 991–998, doi: 10.1007/978-981-16-4258-6_121.
[3] R. K. Dudeja, R. S. Bali, and G. S. Aujla, "Internet of Everything: Background and challenges," in *Software Defined Internet of Everything*, G. S. Aujla, S. Garg, K. Kaur, and B. Sikdar, Eds. Cham, Switzerland: Springer, 2022, pp. 3–15, doi: 10.1007/978-3-030-89328-6_1.
[4] A. Sourav, "Data security and privacy concern in the healthcare system," in *Internet of Healthcare Things*. Hoboken, NJ, USA: Wiley, 2022, pp. 1–25, doi: 10.1002/9781119792468.ch1.
[5] J. Bailey, "Communication: Telephone, computers and WWW," in *Inventive Geniuses Who Changed the World*. Cham, Switzerland: Springer, 2022, pp. 363–401, doi: 10.1007/978-3-030-81381-9_15.
[6] T. D. Mou and G. Srivastava, "Network protocols for the Internet of Health Things," in *Intelligent Internet of Things for Healthcare and Industry*, U. Ghosh, C. Chakraborty, L. Garg, and G. Srivastava, Eds. Cham, Switzerland: Springer, 2022, pp. 21–66, doi: 10.1007/978-3-030-81473-1_2.
[7] T. H. Lenhard, "Telephone systems," in *Data Security*, Wiesbaden, Germany: Springer, 2022, pp. 45–49, doi: 10.1007/978-3-658-35494-7_8.
[8] Y. D. Alava, D. M. Zambrano, E. C. Palma, L. C. Garcia, and M. C. Felipe, "Evaluation of quality of service in VoIP traffic using the E model," in *Advanced Research in Technologies, Information, Innovation and Sustainability*, T. Guarda, F. Portela, and M. F. Santos, Eds. Cham, Switzerland: Springer, 2021, pp. 34–43, doi: 10.1007/978-3-030-90241-4_3.
[9] D. Strz, "Performance analysis of VoIP data over IP networks," *Int. J. Electron. Telecommun.*, vol. 67, no. 4, pp. 743–750, 2021, doi: 10.24425/ijet.2021.139801.
[10] F. W. P. Dharma, "Enhancing branch office network availability using cloud EoIP gateway," *Proc. Comput. Sci.*, vol. 179, pp. 574–581, Jan. 2021, doi: 10.1016/j.procs.2021.01.042.
[11] J. H. Snyman, "Landlines, cellular, and internet protocol subscribership," *J. Strategic Innov. Sustainability*, vol. 16, no. 4, pp. 1–12, 2021.
[12] W. Amalou and M. Mehdi, "An approach to mitigate DDoS attacks on SIP based VoIP," *Eng. Proc.*, vol. 14, no. 1, pp. 1–20, 2022, doi: 10.3390/engproc2022014006.
[13] M. D'Arienzo and G. Musto, "A comparative analysis of protocols for VoIP services," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 26, no. 2, pp. 159–175, 2021, doi: 10.1504/IJCNDS.2021.113013.
[14] F. Hauser, M. Häberle, M. Schmidt, and M. Menth, "P4-IPsec: Site-to-site and host-to-site VPN with IPsec in P4-based SDN," *IEEE Access*, vol. 8, pp. 139567–139586, 2020, doi: 10.1109/ACCESS.2020.3012738.
[15] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid end-to-end VPN security approach for smart IoT objects," *J. Netw. Comput. Appl.*, vol. 158, May 2020, Art. no. 102598, doi: 10.1016/j.jnca.2020.102598.

[16] T. Surasak and S. C. Huang, "Enhancing VoIP security and efficiency using VPN," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 180–184, doi: 10.1109/ICCNC.2019.8685553.

[17] M. D. Atmadja, F. A. Soelistianto, A. Aisah, and Y. Ratnawati, "Design and implementation of analog telephone on IPPBX network interconnection," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 732, no. 1, Jan. 2020, Art. no. 012101, doi: 10.1088/1757-899x/732/1/012101.

[18] B. Saboka, "Improving the quality of service of voice over internet protocol in ethio telecom service level agreement customers," St. Mary's Univ., Twickenham, U.K., Tech. Rep., 2021.

[19] H. A. Mohammed and A. H. Ali, "Effect of some security mechanisms on the Qos VoIP application using OPNET," *Int. J. Curr. Eng. Technol.*, vol. 3, no. 5, pp. 1–10, 2013.

[20] M. H. Miraz, S. A. Molvi, M. A. Ganie, M. Ali, and A. H. Hussein, "Simulation and analysis of quality of service (QoS) parameters of voice over IP (VoIP) traffic through heterogeneous networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 1–7, 2017, doi: 10.14569/ijacsa.2017.080732.

[21] M. R. Uddin, N. A. Evan, M. R. Alam, and M. T. Arefin, "Analysis of generic routing encapsulation (GRE) over IP security (IPSec) VPN tunneling in IPv6 network," in *Ubiquitous Communications and Network Computing*, 2021, pp. 3–15.

[22] A. Jaenul, M. Yusro, and B. Maruddani, "Implementation of voice over internet protocol (VoIP) using softphone applications based on session initiation protocol (SIP)," in *Empowering Science and Mathematics for Global Competitiveness*. Boca Raton, FL, USA: CRC Press, 2019, pp. 562–568.

[23] A. Aimen, S. Hamid, S. Ahmad, M. A. Chisti, S. S. Khurana, and A. Kaur, "Handover between Wi-Fi and WiMAX technologies using GRE tunnel," in *Progress in Advanced Computing and Intelligent Engineering*, 2019, pp. 473–484.

[24] S. K. Das, "Mobility management—A personal perspective," *Comput. Commun.*, vol. 131, pp. 26–31, Oct. 2018, doi: 10.1016/j.comcom.2018.08.012.

[25] B. D. Deebak and F. Al-Turjman, "Robust lightweight privacy-preserving and session scheme interrogation for fog computing systems," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102689, doi: 10.1016/j.jisa.2020.102689.

[26] I. Nurhaida, "Quality of service for traffic monitoring system based on static routing using EoIP tunnel over IPSec," in *Proc. Asia Pacific Inf. Technol. Conf.*, Jan. 2019, pp. 91–99, doi: 10.1145/3314527.3314543.

[27] R. Chinna Rao, K. M. Lakshmi, C. Raja, P. B. S. Varma, G. R. K. Rao, and A. Patibandla, "Real-time implementation and testing of VoIP vocoders with asterisk PBX using wireshark packet analyzer," *J. Interconnection Netw.*, vol. 22, no. 1, Mar. 2022, Art. no. 2142030, doi: 10.1142/S0219265921410309.

[28] S. T. Aung and T. Thein, "Comparative analysis of site-to-site layer 2 virtual private networks," in *Proc. IEEE Conf. Comput. Appl. (ICCA)*, Feb. 2020, pp. 1–5, doi: 10.1109/ICCA49400.2020.9022848.

[29] D. Alvanos, K. Limniotis, and S. Stavrou, "On the cryptographic features of a VoIP service," *Cryptography*, vol. 2, no. 1, p. 3, Jan. 2018, doi: 10.3390/cryptography2010003.

[30] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2020, doi: 10.6028/NIST.SP.800-77r1.

[31] J. Prasetyo and I. W. Suardinata, "Comparison of voice over internet protocol (VoIP) performances in various network topologies," *Bul. Pos dan Telekomun.*, vol. 18, no. 1, pp. 65–74, 2020. [Online]. Available: https://online.bpostel.com/index.php/bpostel/article/view/180105

[32] H. Akter, S. Jahan, S. Saha, R. H. Faisal, and S. Islam, "Evaluating performances of VPN tunneling protocols based on application service requirements," in *Proc. 3rd Int. Conf. Trends Comput. Cognit. Eng.*, 2022, pp. 433–444.

[33] F. Ul Islam, G. Liu, and W. Liu, "Identifying VoIP traffic in VPN tunnel via flow spatio-temporal features," *Math. Biosci. Eng.*, vol. 17, no. 5, pp. 4747–4772, 2020.

[34] K. Gaur, A. Kalla, J. Grover, M. Borhani, A. Gurtov, and M. Liyanage, "A survey of virtual private LAN services (VPLS): Past, present and future," *Comput. Netw.*, vol. 196, Sep. 2021, Art. no. 108245, doi: 10.1016/j.comnet.2021.108245.

[35] R. Goldara and J. Patacsil, "An optimized wireless network architecture for department of agriculture, region 1," *Data Sci., J. Comput. Appl. Informat.*, vol. 6, no. 1, pp. 12–34, Jan. 2021, doi: 10.32734/jocai.v6.i1-7873.

[36] A. P. Lalengke and I. Nurhaida, "Performance analysis of CloudLinux-based web server at the embassy of the kingdom of Morocco in Jakarta," *Jurnal Sisfokom*, vol. 10, no. 2, pp. 250–258, Aug. 2021.

[37] M. Y. B. Rasyiidin, "Wireless network uses RSSI (received signal strength indication) mechanism for smart office concept," in *Proc. 4th Int. Conf. Comput. Informat. Eng. (IC2IE)*, Sep. 2021, pp. 441–446, doi: 10.1109/IC2IE53219.2021.9649351.

[38] L. M. Silalahi, I. U. V. Simanjuntak, S. Budiyanto, F. A. Silaban, A. D. Rochendi, and G. Osman, "Analysis of LTE 900 implementation to increase coverage and capacity of 4G LTE network on Telkomsel provider," in *Proc. Conf. Broad Exposure Sci. Technol.*, vol. 210, 2022 pp. 166–172.

[39] E. Ramadhan, A. Firdausi, and S. Budiyanto, "Design and analysis QoS VoIP using routing border gateway protocol (BGP)," in *Proc. Int. Conf. Broadband Commun., Wireless Sensors Powering (BCWSP)*, Nov. 2017, pp. 1–4, doi: 10.1109/BCWSP.2017.8272556.

[40] S. Budiyanto and I. Pratama, "Classification of network status in academic information systems using naive Bayes algorithm method," in *Proc. 2nd Int. Conf. Broadband Commun., Wireless Sensors Powering (BCWSP)*, Sep. 2020, pp. 107–112, doi: 10.1109/BCWSP50066.2020.9249398.

SETIYO BUDIYANTO received the Ph.D. degree in electrical engineering from the University of Indonesia, in 2016. He is currently an Associate Professor with the Department of Electrical Engineering, Universitas Mercu Buana, Jakarta, Indonesia. He has published 100 of academic papers as a first author or a coauthor in conference proceedings and international journals. His research interests include genetic algorithms, wireless, and telecommunications technology.

DADANG GUNAWAN (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the University of Indonesia, in 1983, the master's degree from Keio University, Japan, in 1989, and the Ph.D. degree from the University of Tasmania, Australia, in 1995. He is currently a Professor with the Department of Electrical Engineering, Universitas Indonesia. He has published 100 of academic papers as a first author or a coauthor in conference proceedings and international journals. His research interest includes wireless and signal processing technology.