ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

COMPARATIVE QUALITY OF SERVICE ANALYSIS OF VPN PROTOCOLS ON IPV6

Sabela Trisiana Oktavia[1], Dimas Febriyan Priambodo[2], Nanang Trianto[3], Rahmat Purwoko[4]

[1,2,3,4]Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Jl Raya H. Usa, Bogor, Indonesia

email: sabela.trisiana@student.poltekssn.ac.id[1], dimas.febriyan@poltekssn.ac.id[2], nanang.trianto@poltekssn.ac.id[3], rahmat.purwoko@poltekssn.ac.id[4]

Abstract

The increase in internet users has led to the depletion of IPv4 supplies and the increase in cyber attacks, one of which is data leakage incidents. Several innovations were created such as switching to IPv6 which provides more addresses and implementing VPN technology to secure internet communications. The solution using VPN is believed to secure the network from various types of attacks from outside the network by creating a tunnel with a certain encryption algorithm as a data exchange path. Some studies reveal that using VPN can cause delay which will affect QoS performance. Therefore, this research will be conducted to provide evidence as well as a comparison between the WireGuard and L2TP / IPSec VPN protocols on IPv6 based on Quality of Service parameters which include delay, jitter, packet loss, throughput, and MOS with three tests namely iPerf3, FTP, and remote desktop . The measurement is done by making a sample model with mikrotik and 6to4 tunnel. From the series of tests, it is known that the L2TP/IPSec protocol is better than the WireGuard protocol judging by the performance generated in tests with FTP and remote desktop. This discovery can be used by end users or other researchers to use VPN more objectively based on the technology.

Keywords : IPv6, Quality of Service, VPN

Received: 06-11-2023 | **Revised:** 27-12-2023 | **Accepted:** 02-01-2024
DOI: https://doi.org/10.23887/janapati.v12i3.69264

INTRODUCTION

Internet Protocol (IP) addresses act as a host's identity when communicating on the Internet. The IP address of each host must be identical, in other words, each host has a different IP address [1]. Currently, internet users are increasing, based on APJJI data, internet users in Indonesia have reached 210 million [2]. According to the We Are Social report, the number of internet users will increase to 4.95 billion by early 2022, representing 62.5% of the world's population [3]. As the number of Internet users grows, the availability of IPv4 is becoming increasingly scarce. According to data from the Asia Pacific Network Information Centre (APNIC), only 0.3% of APNIC's IPv4 addresses are currently available, out of the 99.5% of addresses that will be available by September 2022 [4]. According to APJII, only 3.7 billion IPv4 addresses remain available for use on the Internet, while the theoretical number of IPv6 addresses available is 340 trillion [5]. Therefore, Kominfo prepared the Minister of Communication and Information Regulation No. 13 of 2014 on the Roadmap Policy for the Implementation of IPv6 in Indonesia [4]. According to APJII, the use of IPv6 can reduce the data processing overhead, making connections faster, because it does not require Network Address Translation (NAT) [6].

Increasingly, technology means that many jobs are done remotely. However, behind the ease of technology lies a vulnerability: exchanging information over the internet can be a major risk, as the sensitive information sent can be exploited by unauthorised parties [7]. Based on Surfshark data from January to August 2022, 196.26 million accounts experienced data breaches [8]. n Indonesia, 13.89 million accounts had their data leaked this year [8]. Virtual Private Network (VPN) is a technology that functions to secure communications [9]. VPN is a public network data communications technology that uses encryption to provide secure and reliable communications between users [10]. VPN networks are based on a tunnel that acts as a path to protect data during the data exchange process [11]. When using VPN technology, you can use existing VPN services or create your own VPN. A VPN can be created using the VPN feature provided by the Mikrotik router. Using a

VPN can cause increased latency on the network because the encryption and decryption process on the VPN takes time, so data security on the VPN affects QoS performance [11]. The quality of performance of a service, such as telephony, computer networks and cloud computing services, can be measured quantitatively with Quality of Service [12].

A Virtual Private Network (VPN) is a data communications technology used on public networks that uses encryption to ensure secure and reliable communications between users [10]. VPN networks are built over a tunnel, which acts as a protected path for data during the data exchange process [11]. Various VPN protocols can be implemented, such as PPTP, L2TP, IPSec, MPLS, OpenVPN, IKEv2, SSTP, and WireGuard [13]. Implementing VPN technology can leverage existing VPN services or build a VPN from scratch. VPNs can be established using the VPN features provided by Mikrotik routers. The use of VPNs can introduce network latency due to encryption and decryption processes, affecting data security and Quality of Service (QoS) performance [11]. The quality of service for services such as telephony, computer networks and cloud computing can be measured quantitatively through various aspects including delay, jitter, packet loss, throughput, Mean Opinion Score (MOS), echo cancellation and Post Dial Delay (PDD) [12].

There are related studies that address VPN protocols. In a study by M. Syahyuti Abjar [14], an analysis and performance comparison of PPTP VPN and L2TP VPN protocols in IPv6-based networks was conducted, considering QoS parameters such as delay, jitter, throughput and packet loss. The results of this research indicate that L2TP tunnels outperform PPTP in terms of QoS delay and jitter. Another study conducted by Wa Ode, Fid Aksara and Muh. Yamin [11] compared the performance of the VPN protocols PPTP, L2TP, SSTP and IPSec on Mikrotik based on QoS and concluded that IPSec provides better security and performance compared to PPTP, L2TP and SSTP. In addition, a study by Steven Mackey et al [15] presented a performance comparison of WireGuard and OpenVPN protocols on AWS instances and local virtual machines. The results of this research show that WireGuard outperforms OpenVPN, especially on multi-core machines, due to its lightweight code base.

This research will perform a comparative analysis of VPN protocols on IPv6 based on Quality of Service. The VPN protocols analysed are WireGuard and L2TP/IPSec. WireGuard is the latest lightweight [16] and secure VPN protocol. WireGuard is designed to simplify the connection setup process, utilise multi-threading capabilities and minimise bandwidth usage [15]. WireGuard is claimed to have capabilities above the OpenVPN and IPsec protocols [15]. The QoS parameters used in this research are the values of delay, jitter, packet loss, throughput and Mean Opinion Score (MOS). It is hoped that the results of this research will make it easier for network administrators to determine which protocol is better to use on IPv6 by knowing the performance of each VPN protocol on IPv6. The findings can also be used by end users and other researchers to make VPNs more objective and reduce confusion for users when choosing from the many VPN products on the market, making it easier for users to choose based on the technology used rather than being locked into a particular brand.

LITERATURE REVIEW

IPv6

The Internet Protocol (IP) is a set of rules that defines how communication takes place between computer devices operating at the network layer in the OSI model and the Internet layer in the TCP/IP model [1]. There are several types of IP, such as IPv4, IPv6 and IPv10, but the most popular are IPv4 and IPv6 [1]. IPv6 is a standard protocol for communicating on networks like IPv4, but IPv6 has more IP addresses, a better address structure, provides greater security and supports mobile devices [17]. The length of an IPv6 address is 128 bits, divided into eight parts, each of which is 16 bits long. IPv6 uses a prefix written after the address, such as the prefix /64, which means that of the 128 bits, the first 64 bits are network and the rest are host. The prefix is useful for describing the many bits used to store network information.

Wireguard

WireGuard is a VPN protocol that offers speed, ease of use, and security to users [18]. WireGuard employs the AEAD cipher ChaCha20 in combination with Poly1305 to provide privacy and integrity to users [19]. WireGuard only supports the use of the UDP protocol on port 51820. The WireGuard implementation uses a more efficiently written cipher with a kernel size of less than 4000 lines of source code, making it easier to audit and ensuring greater security. WireGuard is peer-to-peer only and does not require certificates [16]. Figure 1 illustrates the handshake process in WireGuard.

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

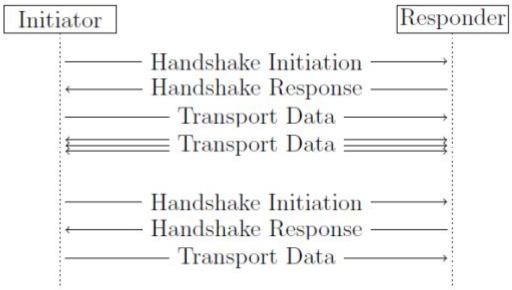


Figure 1. wireguard handshake [20]

L2TP/IPSec

The Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol for VPNs and standard tunnels between routers or from clients to hosts through the Internet Service Provider's (ISP's) Network Access Server (NAS) in a point-to-point fashion. L2TP uses the UDP protocol on port 1702 [11]. However, L2TP does not include a protocol for encrypting the packets being transmitted, so it requires another protocol, IPSec [9]. IPSec provides network layer security services, including access control, data integrity, authentication, protection against replay attacks and confidentiality. The security protocols for IP datagrams provided by IPSec are the Authentication Header (AH) and the Encapsulating Security Payload (ESP) [21]. IPSec supports encryption algorithms such as AES, ChaCha, Blowfish, DES-CBC, and Triple DES [22]. IPSec implements both asymmetric and symmetric encryption, increasing both the speed and security of data transfer [22].

Delay

Delay refers to the amount of time it takes for a packet to reach its destination [11]. The causes of delay include traffic overload, collisions, errors in the physical media, and failures on the receiving end [23]. Delay in a network consists of packetization delay, processing delay, jitter buffer delay, serialization delay, and network delay [24]. Table 1 provides a classification of delay parameters that categories various factors related to latency issues [11]. Delay measurement can be performed using Formula 1.

Table 1. delay classification

Category	ms	Scale
Excellent	<150	A
Good	150-300	B
Median	300-450	C
Poor	>450	D

$$Delay = \frac{total\ delay}{Total\ paket\ yang\ diterima - 1} \quad (1)$$

Jitter

Jitter is a form of delay variation caused by queue length and data processing during the packet transmission process [13]. The amount of jitter is affected by variations in traffic load and network congestion. Increased network traffic increases the likelihood of collisions [24]. Jitter is caused by the length of queues during data transmission, sudden spikes in traffic causing bandwidth constraints and queuing, and the speed at which packets are sent and received at each [25]. Jitter is caused by the length of queues during data transmission, sudden spikes in traffic causing bandwidth congestion and queuing, and the speed at which packets are sent and received at each link using Formula 2.

Table 2. jitter classification

Category	ms	Scale
Excellent	0	A
Good	0-75	B
Median	75-125	C
Poor	125-225	D

$$Jitter = \frac{total\ variasi\ delay}{Total\ paket\ yang\ diterima - 1} \quad (2)$$

Packet loss

Packet loss is the number of packets lost during the transmission of data from source to destination [25]. The lower the packet loss value, the better the network performance [26]. A lower value of packet loss indicates better network performance [25]. Packet loss typically occurs due to traffic congestion, receiver-side failures, physical media failures, router buffer overflows, congestion, signal degradation and overload [24]. Packet loss parameters are categorized and presented in Table 3 [11]. Measurement of packet loss can be carried out using Formula 3.

Table 3. jitter classification

Category	%	Scale
Excellent	0	A
Good	3	B
Median	15	C
Poor	25	D

$$Packet\ Loss = \frac{PTT - PT}{PTT} X\ 100\% \quad (3)$$

PTT = Total Package Captured
PT = Package Sent

Throughput

Throughput refers to the effective speed of data transfer, measured in bits per second (bps). Throughput is the total number of packets successfully received during a time interval

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

divided by the duration of that time interval [13]. Throughput represents the actual ability of a network to transmit data [27]. Throughput parameters are categorized and presented in Table 4 [13] and measurement of throughput can be carried out using Formula 4.

Table 4. Packet loss classification

Category	ms	Scale
Excellent	75-100	A
Good	75-50	B
Median	50-25	C
Poor	<25	D

$$Throughput = \frac{Jumlah\ data\ yang\ dikirim}{lama\ pengiriman} \quad (4)$$

Mean opinion score (MOS)

The Mean Opinion Score (MOS) is a unit used to assess voice quality [28]. MOS scores are obtained using both direct methods and mathematical approaches. Direct methods can include questionnaires designed to gather opinions from respondents. Meanwhile, the mathematical approach is carried out using the E-Model based on delay and packet loss values [26]. The E-Model is obtained by calculating the R-Factor, which ranges from 0 to 100 [28]. MOS parameters are categorized and presented in Table 5.

Table 5. MOS classification

Grade	MOS	Scale	E-Model (R)
Excellent	4,2<=M<=5	A	89<=R<=100
Very Good	3,9<=M<=4,2	B	79<=R<=89
Acceptable	3,5<=M<=3,9	C	70<=R<=79
Concerning	3<=M<=3,5	D	59<=R<=70
Poor	2,5<= M<=3	E	49<=R<= 59
Very Poor	0<=M<=2,5	F	0<=R<=49

The process of measuring MOS begins with the calculation of the delay and packet loss experienced during the test. The results of these delay and packet loss calculations are then used as a basis for obtaining the value of I_d (the logarithm of the delay) using the formula in Formula 5 and the value of I_{ef} (the logarithm of the effect of the lost packets) using the formula in Formula 6. The values of Id and Ief are then used as references to calculate the R-Factor value using the formula in Formula 7. This R-Factor value is used as the basis for calculating the MOS value using the formula in Formula 8. Thus, the MOS measurement can be obtained through a series of calculations based on the previously mentioned parameters.

$$I_d = 0{,}024d + 0{,}11(d - 177{,}3)\,H(d - 177{,}3) \quad (5)$$

$$H = \begin{cases} 0, x < 0 \\ 1, x \geq 0 \end{cases}$$

$$I_{ef} = 7 + 30\ln(1 + 15\rho) \quad (6)$$

$$R = 94{,}2 - I_d - I_{ef} \quad (7)$$

$$MOS = 1 + 0{,}035\,R + 7 \times 10^{-6}\,R\,(R - 60)(100 - R) \quad (8)$$

R = R-Factor
Id = decrease in quality due to delay
Ief = quality degradation due to packet loss
H = heavyside function
ρ = probability of packet loss
MOS = Mean Opinion Score

Related Works

The research [14] conducted an analysis and comparison of the performance of PPTP VPN and L2TP VPN protocols on an IPv6-based network based on QoS parameters, including Delay, Jitter, Throughput, and Packet loss. The performance comparison was evaluated through testing by sending files using FTP. The results of the research showed that the QoS values for Delay and Jitter in the L2TP tunnel were superior to those in the PPTP tunnel.

Research [11] conducted an analysis comparing the performance of VPN protocols PPTP, L2TP, SSTP, and IPSec using MikroTik based on QOS parameters, including packet loss, delay, and throughput. Testing was performed using Wireshark tools with two scenarios: all clients accessing web-based downloads and all clients accessing web video streaming. The results of this research showed that the security and performance of the IPsec protocol were better than PPTP, L2TP, and SSTP protocols.

Research [15] presented a performance comparison of the WireGuard and OpenVPN VPN protocols implemented on AWS instances and local virtual machines. The research environment was designed with two nodes, one as a server and one as a client. Testing was conducted using iPerf3 and Python's Psutil Library to determine CPU usage, RTT, and throughput. The results of this research showed that the WireGuard protocol outperformed OpenVPN on multi-core machines, and its code base was lightweight.

Research related to VPN protocols has been conducted by several authors, but none have addressed a comparative analysis of WireGuard and L2TP/IPSec in IPv6. For instance, in the research by M. Syahyuti Abjar [14], only the L2TP and PPTP protocols were examined on IPv6-based networks. Additionally, the research conducted by Wa Ode Zamalia et al [11] analyzed the QoS performance of PPTP, L2TP, SSTP, and IPSec on IPv4-based networks.

METHOD

The subject of this research is Mikrotik's WireGuard and L2TP/IPSec VPN protocols implemented on IPv6. The research carried out was comparative research, where a comparison of the WireGuard and L2TP/IPSec VPN protocols was carried out using a quantitative approach to data collection. This research phase begins with the creation of a network topology design, then continues with the implementation of the topology design created and configured to form a research environment. Next, data is collected through three tests, namely iPerf3, FTP and Remote Desktop. The test result data will be analysed based on QoS parameters. The results of the analysis are presented in tabular form to facilitate comparison of the test results.

Network Topology Design

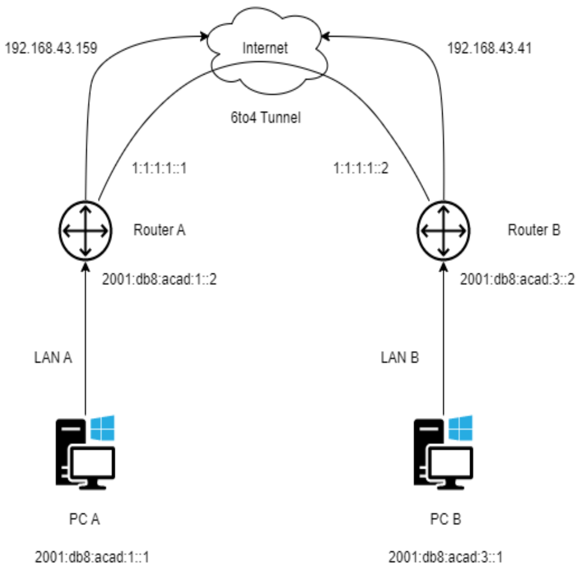


Figure 2. Network Topology

The test environment was set up using two Mikrotik routers and two PCs. There are two LANs, LAN A and LAN B, using IPv6 as shown in Figure 2. The two routers are connected via an Internet intermediary using the IP provided by the ISP in the form of IPv4. So a transition mechanism is needed to connect IPv6 to IPv4 using 6to4 tunnel [29]. In this research, communication can only take place between LAN A and LAN B. Meanwhile, the Internet is only used as a connection medium between Router A and Router B and only to illustrate that it is actually only a closed loop network between the two routers. Table 5 is the hardware detail and Table 6 is the software detail in this research.

Table 5. Hardware Detail

No	Hardware	Spesification
1	Router Mikrotik RB941	Processor 650Mhz 4 port Fast Ethernet NAND 16MB RAM 32MB
2	PC A	Processor intel core i7 HDD 1 TB dan SSD 256GB RAM 16 GB
3	PC B	Processor intel core i7 SSD 512GB RAM 8 GB

Table 6. Software Detail

No	Software	Version
1	IPerf3	3.1.3
2	FileZilla Client	3.63.2.1
3	XAMPP	3.3.0
4	Wireshark	4.0.6

Implementation and Configuration

The implementation starts by connecting the two routers over the Internet so that the router obtains an IP from the ISP in the form of IPv4. Once the router is connected, the configuration is done on each LAN with IPv6. Then add a 6to4 tunnel configuration to translate IPv4 to IPv6. Next, a VPN is created using the VPN protocol feature available from Mikrotik on a peer-to-peer basis and the specification details are shown in Table 7.

Table 7. VPN Configuration

No	Software	Version
1	WireGuard	listen-port : 13231 mtu : 1420 allowed-address : IP/IPv6 prefix endpoint-address : IP/Hostname endpoint-port : integer:0..65535
2	L2TP	connect-to : IP max-mtu : 1450 use-ipsec : require ipsec-secret : string

Data Retrieval

Data retrieval was carried out using iPerf3, FTP and Remote Desktop. The first test is

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

carried out with iPerf3 installed on each PC. PC A acts as the iPerf3 server and PC B as the iPerf3 client. The second test is with the FTP service, which aims to determine the quality of sending file packets over the VPN network. During the packet sending process, the data exchange traffic is captured by Wireshark. The final test is with Remote Desktop, where PC B is remotely controlled by PC A, then a video is played from PC B while data is exchanged. During the video playback process, the data exchange traffic is captured by Wireshark.

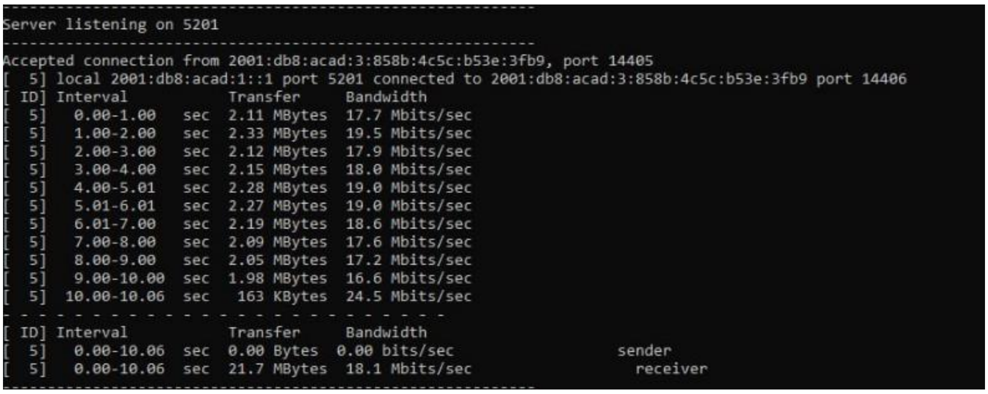
Analysis Based on QoS

The analysis is based on quality of service parameters including delay, jitter, packet loss, throughput and Mean Opinion Score (MOS). In this phase, the data obtained during the testing process is analysed according to the service where the iPerf3 test results show high values of received packets and high bandwidth. Wireshark capture results in the FTP test are analysed to obtain delay, jitter, packet loss and throughput values. The Wireshark capture results in the Remote Desktop test are analysed to obtain delay and packet loss values. These two values are then used as the basis for calculations to obtain the R-Factor value, and from the R-Factor value it is calculated again to obtain the MOS value. The following is a data analysis based on QoS in each test.

RESULT AND DISCUSSION

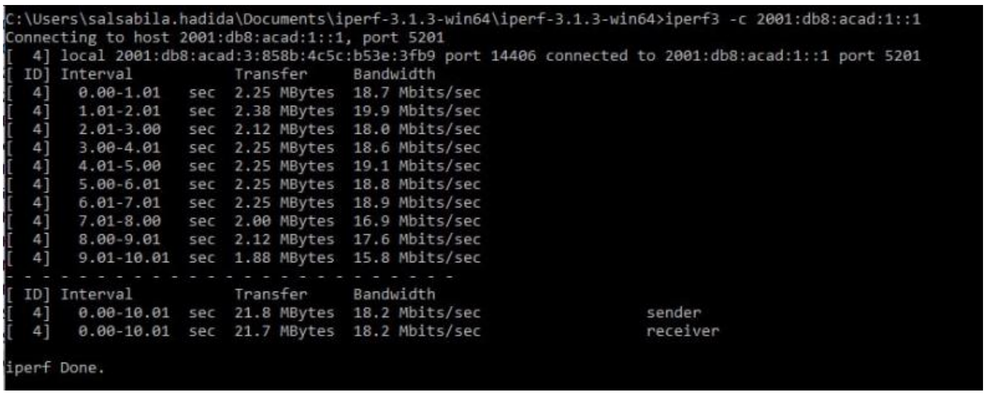
Iperf3

Testing with iPerf3 is done by installing the iPerf3 application on PC A and PC B. Then PC A runs iPerf3 in server mode and PC B runs iPerf3 in client mode. PC B will contact PC A by entering the IP of PC A. During the communication process a large transfer value and bandwidth are recorded. The resulting values are displayed on both the server and client side, so data is collected from both the server and the client. The Wireguard test is shown in Figure 3, with values displayed from the server side and Figure 4 from the client side. iPerf3 tests on each VPN protocol are detailed in Table 8.



```
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 2001:db8:acad:3:858b:4c5c:b53e:3fb9, port 14405
[  5] local 2001:db8:acad:1::1 port 5201 connected to 2001:db8:acad:3:858b:4c5c:b53e:3fb9 port 14406
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.00   sec  2.11 MBytes  17.7 Mbits/sec
[  5]   1.00-2.00   sec  2.33 MBytes  19.5 Mbits/sec
[  5]   2.00-3.00   sec  2.12 MBytes  17.9 Mbits/sec
[  5]   3.00-4.00   sec  2.15 MBytes  18.0 Mbits/sec
[  5]   4.00-5.01   sec  2.28 MBytes  19.0 Mbits/sec
[  5]   5.01-6.01   sec  2.27 MBytes  19.0 Mbits/sec
[  5]   6.01-7.00   sec  2.19 MBytes  18.6 Mbits/sec
[  5]   7.00-8.00   sec  2.09 MBytes  17.6 Mbits/sec
[  5]   8.00-9.00   sec  2.05 MBytes  17.2 Mbits/sec
[  5]   9.00-10.00  sec  1.98 MBytes  16.6 Mbits/sec
[  5]  10.00-10.06  sec   163 KBytes  24.5 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-10.06  sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-10.06  sec  21.7 MBytes  18.1 Mbits/sec                  receiver
```

Figure 3. wireguard iperf test from server side



```
C:\Users\salsabila.hadida\Documents\iperf-3.1.3-win64\iperf-3.1.3-win64>iperf3 -c 2001:db8:acad:1::1
Connecting to host 2001:db8:acad:1::1, port 5201
[  4] local 2001:db8:acad:3:858b:4c5c:b53e:3fb9 port 14406 connected to 2001:db8:acad:1::1 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  2.25 MBytes  18.7 Mbits/sec
[  4]   1.01-2.01   sec  2.38 MBytes  19.9 Mbits/sec
[  4]   2.01-3.00   sec  2.12 MBytes  18.0 Mbits/sec
[  4]   3.00-4.01   sec  2.25 MBytes  18.6 Mbits/sec
[  4]   4.01-5.00   sec  2.25 MBytes  19.1 Mbits/sec
[  4]   5.00-6.01   sec  2.25 MBytes  18.8 Mbits/sec
[  4]   6.01-7.01   sec  2.25 MBytes  18.9 Mbits/sec
[  4]   7.01-8.00   sec  2.00 MBytes  16.9 Mbits/sec
[  4]   8.00-9.01   sec  2.12 MBytes  17.6 Mbits/sec
[  4]   9.01-10.01  sec  1.88 MBytes  15.8 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  21.8 MBytes  18.2 Mbits/sec                  sender
[  4]   0.00-10.01  sec  21.7 MBytes  18.2 Mbits/sec                  receiver

iperf Done.
```

Figure 4. wireguard iperf test from client side

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

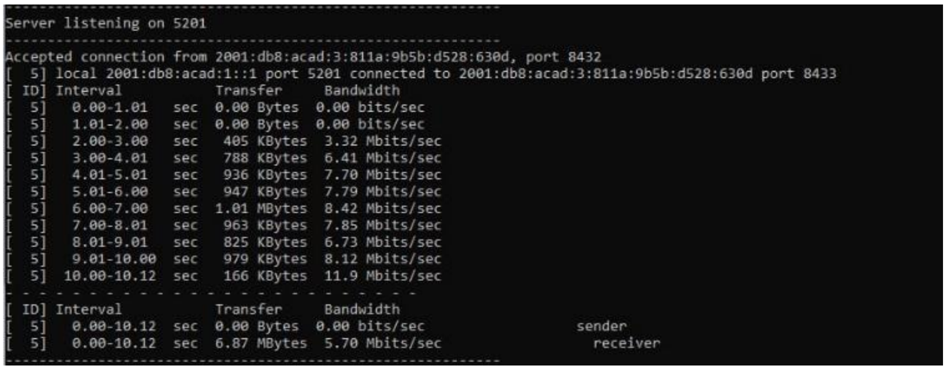


Figure 5. L2TP iperf test from server side

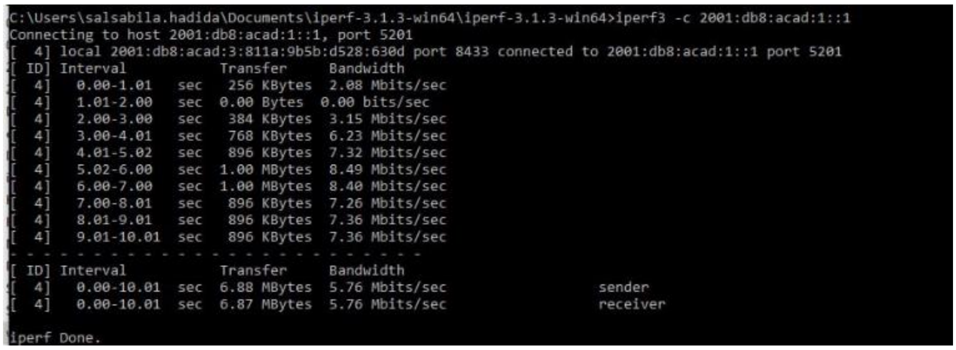


Figure 6. Test Results with iPerf3

Table 8. Comparison of Test Results with iPerf3

WireGuard		**L2TP/IPSec**	
Transfer	***Bandwidth***	***Transfer***	***Bandwidth***
21,7	18,1	6,87	5,70
21,8	18,2	6,88	5,76
21,7	18,2	6,87	5,76

FTP

Testing with FTP starts by creating an FTP server on PC A using the xampp application, then PC B acts as the recipient or FTP client using the filezilla client application. PC B will download data from PC A and upload data of the same size and type to PC A. The data exchange traffic is then captured using the Wireshark application, which is taken from the client side, as the process of downloading and uploading data takes place on the client. There are 4 files sent via FTP as explained in Table 9.

Table 9. Specifications for Files Sent Via FTP

No	**File Name**	**File Extensions**	**Size**
1	Audio	MP3	348 KB
2	Document	PDF	68 KB
3	Picture	JPG	160 KB
4	Video	MP4	5,13 MB

The process of sending files over FTP using the WireGuard VPN protocol is shown in Figure 7. In this figure, all files are successfully transferred from the server to the client, and the reverse process from the client to the server is also successful. The data exchange process is captured by Wireshark running on the client, as shown in Figure 8. Sending files via FTP using the L2TP/IPSec protocol is shown in Figure 9. In this figure, all files are successfully transferred from the server to the client, and the reverse process from the client to the server is also successful. The data exchange process is captured by Wireshark running on the client, as shown in Figure 10. All comparisons of this test are shown in Table 10.

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

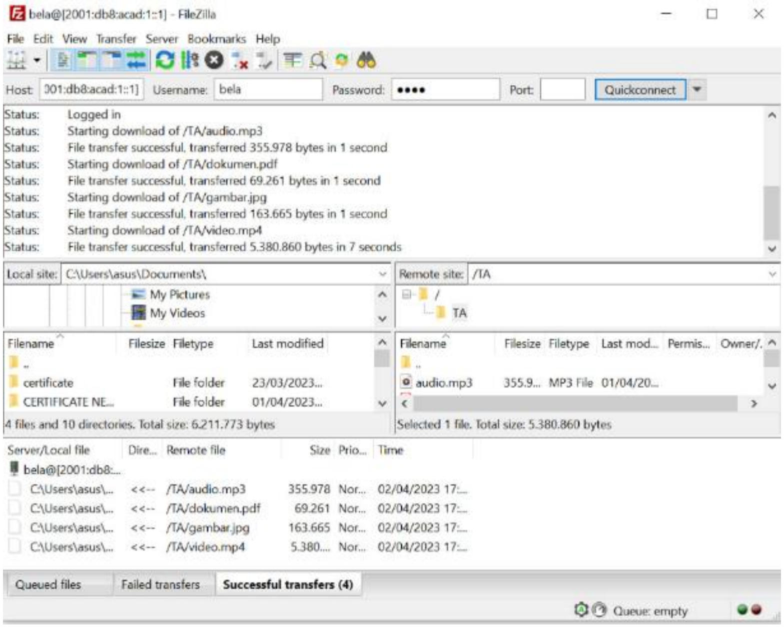


Figure 7. FTP test with WireGuard

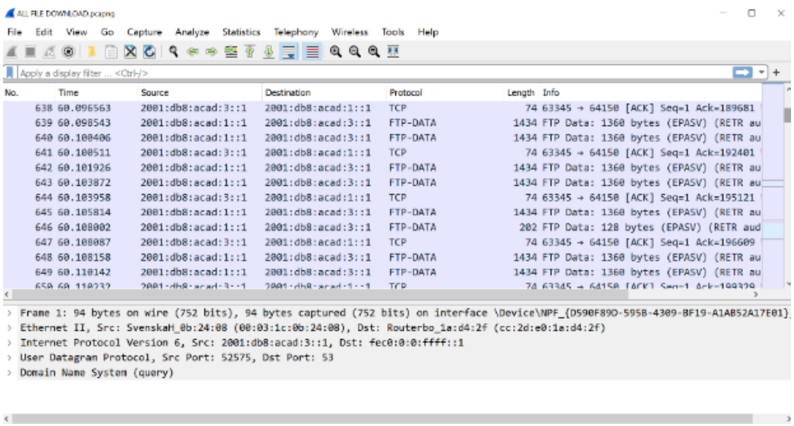


Figure 8. Wireshark FTP WireGuard test

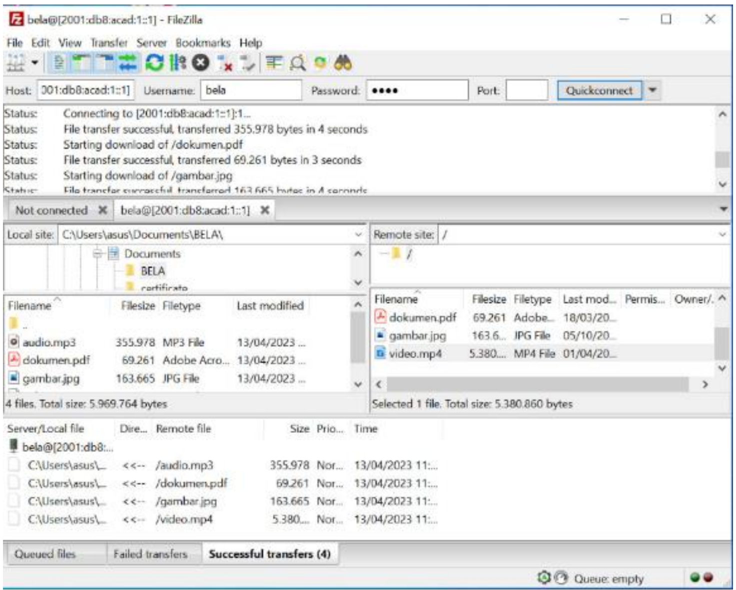


Figure 9. FTP L2TP test

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

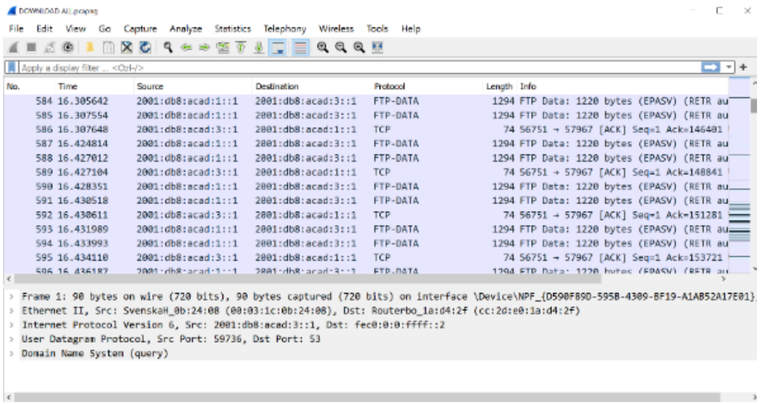


Figure 10. Wireshark FTP L2TP test

Table 10. Comparison of Test Results with FTP

File	Wireguard				L2TP/IPSec			
	Avg Delay (ms)	**Avg Jitter (ms)**	**Packet loss (%)**	**Throughput (kbps)**	**Avg Delay (ms)**	**Avg Jitter (ms)**	**Packet loss (%)**	**Throughput (kbps)**
Audio	12,94	12,94	0,04	578	6,26	6,26	0,042	1104
Document	104,99	83,58	0	36	106,1	106,1	0,719	30
Picture	68,71	85,08	0,408	77	49,44	53,54	0,19	105
Video	4,79	4,71	0,027	1567	4,53	4,52	0	1527

Remote Desktop

The remote desktop test was performed by playing videos of different durations on the remote PC, PC B. During the video playback process, the data exchange was captured by Wireshark, as shown in Figure 11. Table 11 shows the specifications of the video to be played, including the duration and size of the video, and Table 12 shows the result of the remote desktop test.

Table 11. Video Specifications

No	File Name	Duration	Size
1	Video 10S	10s	948 KB
2	Video 15S	20s	1,42 MB
3	Video 30S	30s	3,60 MB

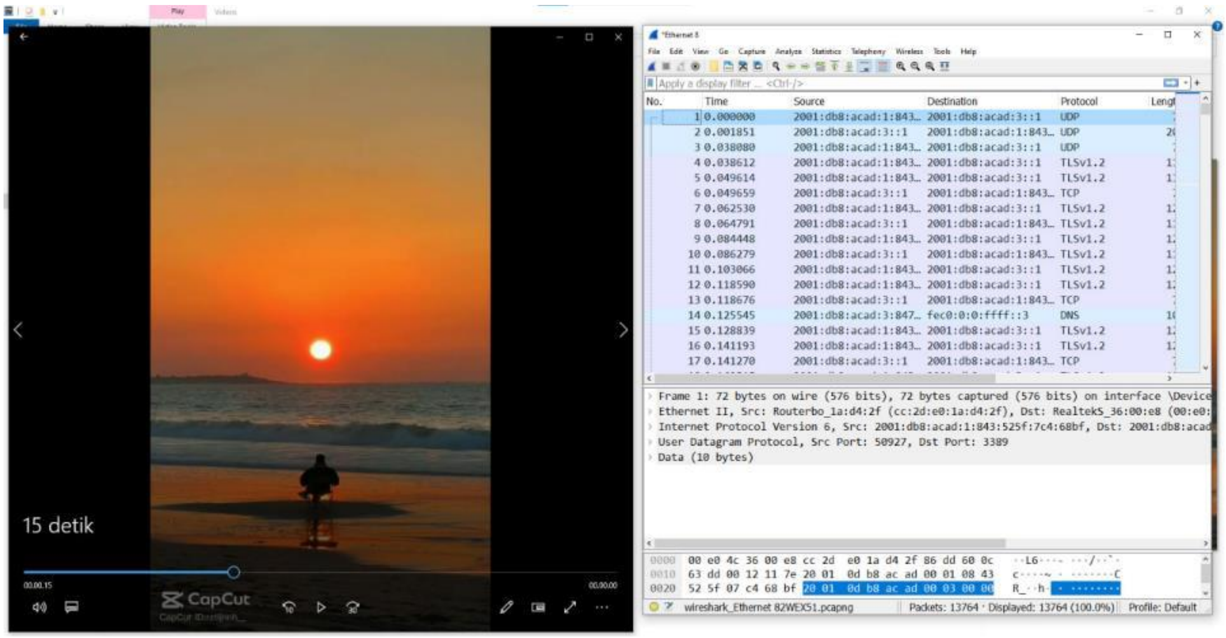


Figure 11. Video playing in remote desktop

Table 12. Comparison of Test Results with Remote Desktop

Duration	WireGuard		L2TP/IPSec	
	R-Faktor	**MOS**	**R-Faktor**	**MOS**
10 Second	87,168	4,26359	87,161	4,26339
15 Second	87,169	4,26362	87,156	4,26325
30 Second	87,166	4,26354	87,159	4,26334

CONCLUSION

Implementing the VPN protocol on IPv6 requires additional 6to4 tunneling which acts as an interconnection between IPv6 and IPv4 networks. The main purpose of using 6to4 tunneling is to overcome the limitations of using IPv6 and deal with the current situation of ISPs that have not yet adopted IPv6. After configuring 6to4 tunneling, the next step is to build a VPN protocol. The VPN protocol can be easily implemented using the VPN feature available in Mikrotik. VPN protocol configuration is carried out on each router that will be connected to the network. The WireGuard protocol uses public keys and private keys as a security layer. So when the WireGuard protocol is activated, each router will automatically obtain a public key and a private key. While the L2TP protocol requires IPSec as a security protocol and it is important to ensure that the IPSec secret used between the server and client is the same.

Test results and analysis based on the quality of service of the WireGuard and L2TP/IPSec protocols show that the L2TP/IPSec protocol outperforms the WireGuard protocol in FTP tests. This can be seen from the QoS values produced when sending audio, image and video files using the L2TP/IPSec protocol, which are superior to the WireGuard protocol. The WireGuard protocol only excels when sending document files. Apart from that, the WireGuard protocol shows better performance in the remote desktop test, but the difference in performance is not very significant because the percentage difference in the resulting MOS value is very small and the MOS values for WireGuard and L2TP/IPSec are both within class. B. Therefore, the overall conclusion is that the L2TP/IPSec protocol is better than the WireGuard protocol.

Although this research is limited to Wireguard and L2TP, it would be better to compare other protocols that are supported by the device used, namely Mikrotik with supported protocols including PPTP, L2TP / IPsec, OpenVPN, and SSTP and even better if compare more protocols and are used in general devices other than Mikrotik.

ACKNOWLEDGMENT

Thanks to National Cyber and Crypto for funding this paper submission.

REFERENCES

[1] G. K. Ordabayeva, M. Othman, B. Kirgizbayeva, Z. D. Iztaev, and A. Bayegizova, “A systematic review of transition from IPV4 to IPV6,” in *ACM International Conference Proceeding Series*, 2020. doi: 10.1145/3410352.3410735.

[2] APJII, “Laporan Survei Internet Indonesia APJII 2021-2022,” 2022.

[3] “Digital 2022: Another Year of Bumper Growth - We Are Social,” *2022*. [Online]. Available: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/

[4] Kementrian Komunikasi dan Informatika, “Atasi Keterbatasan Kapasitas IPv4, Kominfo Dorong Migrasi ke IPv6.” https://www.kominfo.go.id/content/detail/45021/atasi-keterbatasan-kapasitas-ipv4-kominfo-dorong-migrasi-ke-ipv6/0/berita_satker (accessed Sep. 25, 2023).

[5] “Gunakan IPv6 | IDNIC - APJII.” [Online]. Available: https://idnic.net/community/ipv6

[6] “Asosiasi Penyelenggara Jasa Internet Indonesia.” [Online]. Available: https://apjii.or.id/berita/detail/kebutuhan-ip-address-meningkat-apjii-dukung-rencana-penerapan-ipv6_874

[7] P. E. Kristianto and A. T. Putra, “Comparative Analysis of IPv4 and IPv6 OpenVPN Protocol Performance Based on QoS Parameters,” *J. Adv. Inf. Syst. Technol.*, vol. 3, no. 1, 2021, [Online]. Available: https://journal.unnes.ac.id/sju/index.php/jaist

[8] “Peta Kebocoran Data Global Sepanjang 2022, Termasuk Indonesia.” [Online]. Available: https://dataindonesia.id/digital/detail/peta-kebocoran-data-global-sepanjang-2022-

ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 12, Issue 03, December 2023

termasuk-indonesia
[9] M. Hickey and J. Arcuri, “Hands on Hacking,” 2020.
[10] D. Yang, H. Wei, Y. Zhu, P. Li, and J. C. Tan, “Virtual Private Cloud Based Power-Dispatching Automation System-Architecture and Application,” *IEEE Trans. Ind. Informatics*, vol. 15, no. 3, pp. 1756–1766, 2019, doi: 10.1109/TII.2018.2849005.
[11] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, “Analisis Perbandingan Performa QoS, PPTP, L2TP, SSTP Dan IPSec pada Jaringan Vpn Menggunakan Mikrotik,” *semanTIK*, vol. 4, pp. 1–8, 2018.
[12] B. Dwi Satoto, M. Khoironi, J. P. O. Raya Telang BOX, and K. pos, “Pemilihan Prioritas Layanan Qos Dengan Pendekatan Metode Fuzzy Analytical Hierarchy Process (Fahp) Dan Topsis.”
[13] M. Rasuanda *et al.*, “Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode Quality of Service,” 2020.
[14] M. S. Abjar, “Analisis Perbandingan Protokol Point-to-Point Tunneling Protocol VPN Dengan Protokol Layer Two Tunneling Protocol VPN pada Jaringan IPV6,” 2020.
[15] S. Mackey, I. Mihov, A. Nosenko, F. Vega, and Y. Cheng, “A Performance Comparison of WireGuard and OpenVPN,” in *CODASPY 2020 - Proceedings of the 10th ACM Conference on Data and Application Security and Privacy*, 2020, pp. 162–164. doi: 10.1145/3374664.3379532.
[16] D. F. Priambodo, Amiruddin, and N. Trianto, “Hardening a Work from Home Network with Wireguard and Suricata,” in *2021 International Conference on Computer Science and Engineering (IC2SE)*, 2021, vol. 1, pp. 1–4. doi: 10.1109/IC2SE52832.2021.9791983.
[17] Purti, “IPv6 Addresses,” *IJRAR- Int. J. Res. Anal. Rev.*, vol. 5, no. 3, pp. 1–3, 2018.
[18] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree, and D. Doghramachi, “Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol,” *Int. J. Interact. Mob. Technol.*, vol. 14, no. 18, pp. 157–177, 2020, doi: 10.3991/ijim.v14i18.16507.
[19] E. Dekker and P. Spaans, “Performance comparison of VPN implementations WireGuard, strongSwan, and OpenVPN in a 1 Gbit/s environment.”
[20] P. A. Wu supervised by Tanja Lange Jacob Appelbaum Jason Donenfeld, “Analysis of the WireGuard protocol,” 2019.
[21] V. Bollapragada, M. Khalid, and S. Wainner, *IPSec VPN design : the definitive design and deployment guide for secure virtual private networks*. Cisco Press, 2005.
[22] “Apa itu IPSec - IPSec di Amazon Web Services.” [Online]. Available: https://aws.amazon.com/id/what-is/ipsec/
[23] A. Budiman, M. Ficky Duskarnaen, and H. Ajie, “Analisis Quality Of Service (QoS) pada Jaringan Internet SMK Negeri 7 Jakarta,” 2020.
[24] M. Purwahid and J. Triloka, “Analisis Quality of Service (QoS) Jaringan Internet untuk Mendukung Rencana Strategis Infrastruktur Jaringan Komputer di SMK N I Sukadana,” 2019.
[25] F. Rianda, A. Gautama, P. Satwiko, and S. A. Karimah, “Perbandingan Mean Opinion Score (MOS) pada Jaringan VoIP Menggunakan Proportional Integral Controller Enhanced (PIE) dan Droptail.”
[26] I. W. A. P. Ardent Religian Putra. M.Sc., Dwi Fadilla K., ST., MT, “Performansi Layanan Video Conference Pada Jaringan Wide Area Network (WAN) Di Chevron Indonesia Company”.
[27] I. Kadek, S. Satwika, and M. Sukafona, “Analisis Quality of Service Jaringan Virtual Private Network (VPN) di STMIK STIKOM Indonesia,” 2019.
[28] R. FITRIYANTI, L. LINDAWATI, and A. ARYANTI, “Analisis Perbandingan Mean Opinion Score Aplikasi VoIP Facebook Messenger dan Google Hangouts menggunakan Metode E-Model pada Jaringan LTE,” *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 6, no. 3, p. 379, 2018, doi: 10.26760/elkomika.v6i3.379.
[29] S. Narayan, S. Ishrar, A. Kumar, R. Gupta, and Z. Khan, *Performance Analysis of 4to6 and 6to4 Transition Mechanisms over Point to Point and IPSec VPN Protocols*. 2016.