JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 3 No 1 – April 2020 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk mengamankan VoIP

Ikhwanul Kurnia Rahman[1], L.N. Harnaningrum[2]

[1,2]Magister Teknologi Informasi, Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia
Jl. Majapahit No.143 Jaranan Banguntapan Banguntapan Bantul, Yogyakarta, Indonesia

e-mail: ikhwanulkurniarahman@gmail.com[1], ningrum@utdi.ac.id[2]

Received : Maret, 2024	Accepted : April, 2024	Published : April, 2024

Abstract

Data security when using VoIP services is very important to prevent leaks of sensitive information, so VPN technology is needed that can be secure to avoid eavesdropping. In this research, testing was carried out by making calls using VoIP on a network without VPN, using L2TP IPSec VPN and Wireguard VPN. The results of this research prove that the use of L2TP IPSec VPN and Wireguard is successful in securing VoIP data communications from eavesdropping. The delay test results found that L2TP IPSec had an average delay of 19.9997ms while Wireguard had a better delay of 19.9994ms. After carrying out a series of VoIP development tests based on the scenarios described in the previous section it can be deduced, that VoIP communication systems that do not have security measures are vulnerable to potential eavesdropping on ongoing conversations and interception of voice data through VoIP Call Detection and RTP Player.

Keywords: *VoIP, IPSec, Wireguard, VPN*

Abstrak

Keamanan data dalam penggunaan layanan VoIP sangat penting untuk mencegah kebocoran informasi yang sensitive, sehingga dibutuhkan teknologi VPN yang dapat mengamankan agar terhindar dari penyadapan. Pada penelitian ini dilakukan pengujian dengan cara melakukan telpon menggunakan voip pada jaringan tanpa vpn, menggunakan L2TP IPSec VPN dan wireguard VPN. Hasil penelitian ini membuktikan, bahwa penggunaan VPN L2TP IPSec dan Wireguard berhasil mengamankan komunikasi data VoIP dari penyadapan. Adapun hasil pengujian delay didapati bahwa L2TP IPSec memiliki rata-rata delay 19,9997ms sedangkan wireguard memiliki delay lebih baik sebesar 19,9994ms. Setelah melakukan serangkaian pengujian pengembangan VoIP berdasarkan skenario yang diuraikan di bagian sebelumnya dapat dideduksi, bahwa sistem komunikasi VoIP yang tidak memiliki langkah-langkah keamanan rentan terhadap potensi penyadapan pada percakapan yang sedang berlangsung dan intersepsi data suara melalui Deteksi Panggilan VoIP dan Pemutar RTP.

Kata Kunci: *VoIP, IPSec, Wireguard, VPN*

1. PENDAHULUAN

Voice Over Internet Protocol (VOIP) adalah teknologi yang menggunakan Protokol Internet untuk mengirimkan komunikasi suara secara digital secara instan. VoIP menawarkan biaya yang lebih rendah dan fleksibilitas tinggi, sehingga banyak orang memilihnya sebagai pengganti telepon tradisional untuk berkomunikasi [1].

Keamanan data dalam penggunaan layanan VoIP sangat penting untuk mencegah kebocoran informasi yang sensitif. Seperti yang telah dibuktikan pada penelitian [3] bahwa komunikasi VoIP sangat rentan dan mudah sekali disadap, sehingga dibutuhkan teknologi yang dapat mengamankan agar terhindar dari penyadapan. Pada penelitian tersebut, penulis menerapkan VPN PPTP untuk mengamankan jalur komunikasi VoIP sehingga tidak dapat disadap lagi karena komunikasi voip di-enkripsi dan di-enkapsulasi oleh *protocol* VPN PPTP.

Virtual Private Network (VPN) berfungsi untuk mengamankan komunikasi antara perangkat *client* dan *server* yang melalui internet, sehingga tidak dapat dideteksi atau disadap oleh pihak yang tidak berwenang. Pada penelitian [5], peneliti mengimplementasikan VPN untuk melindungi data pada komunikasi pembayaran *online* dengan mengenkripsi data yang dikirim dari perangkat *client* ke *server* Bank, sehingga menyulitkan peretas untuk menyadap komunikasi data tersebut.

Beberapa penelitian sebelumnya telah membahas Implementasi VoIP, seperti pada penelitian [2] Penulis menggunakan VoIP sebagai media komunikasi antara 3 unit kampus di Universitas Muhammdiyah Metro. Penulis menyimpulkan, bahwa penggunaan VoIP memiliki beberapa manfaat seperti biaya yang lebih murah daripada telepon tradisional serta pemeliharaan yang lebih mudah karena koneksi internet atau data dan telepon bisa menggunakan media jaringan yang sama.

Pada penelitian [4] juga disimpulkan, bahwa VPN dapat mengamankan komunikasi data VoIP. Hal ini karena, VPN membuat koneksi terenkripsi yang aman dan menyediakan jalur private untuk data dan komunikasi saat menggunakan jaringan internet.

Jenis VPN yang digunakan pada penelitian [3] adalah PPTP, namun berdasarkan penelitian [6] setelah dilakukan pengujian perbandingan performa PPTP dan L2TP IPSec didapati, bahwa pada pengujian upload file 30MB, L2TP IPSec dengan enkripsi camelia 128 memiliki *delay* dan *jitter* lebih baik dibandingan PPTP.

Pada penelitian [7] Peneliti melakukan implementasi L2TP IPSec pada jaringan sebuah perusahaan sehingga kantor cabang dan kantor pusat dapat berkomunikasi dengan aman. Pengujian keamanan juga dilakukan dengan mencoba menyadap komunikasi dari kantor cabang ke kantor pusat, hasil dari pengujian menampilkan bahwa data komunikasi dari kantor cabang ke kantor pusat berhasil diamankan setelah mengimplementasikan L2TP IPSec ini sehingga data yang terkirim akan terenkripsi sehingga menyulitkan *hacker* untuk menyadap komunikasi data tersebut.

Selain L2TP IPSec, ada teknologi VPN yang lebih baru yaitu Wireguard VPN. Pada penelitian [8] dilakukan implementasi Keamanan Akses Terhadap *Website* Menggunakan *Wireguard*. Hasil dari pengujian tersebut, *Wireguard* berhasil mengamankan komunikasi data sehingga tidak bisa disadap oleh pihak yang tidak berwenang.

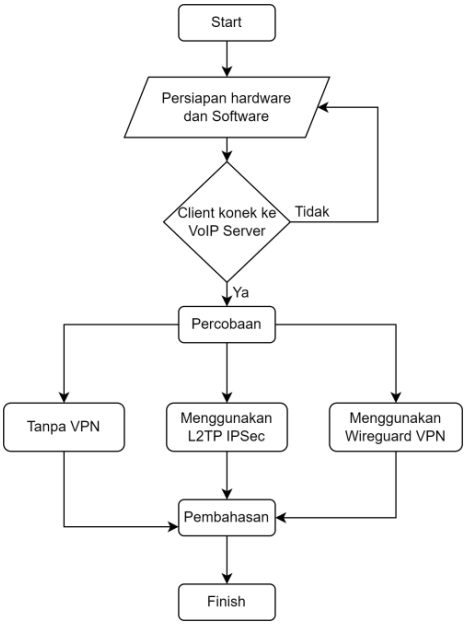
Pada penelitian [9] berdasarkan beberapa pengujian dapat disimpulkan, bahwa *Wireguard* memiliki tingkat keamanan lebih baik dan juga performa kecepatan data yang lebih baik dibandingkan dengan IPSec. Sehingga pada penelitian ini perlu dilakukan pengujian apakah *Wireguard* juga memiliki performa yang baik untuk diterapkan pada komunikasi data VoIP.

Pengujian pada penelitian ini akan memfokuskan pada analisis performa QoS VoIP dalam jaringan yang menggunakan protokol keamanan IPSec dan *WireGuard*. Melalui penelitian ini diharapkan dapat mengetahui perbandingan performa QoS antara IPSec dan *WireGuard* dalam mengamankan komunikasi data VoIP.

2. METODE PENELITIAN

Pada penelitian ini dilakukan pengujian dengan cara melakukan telepon menggunakan VoIP pada jaringan tanpa VPN, menggunakan L2TP

IPSec VPN dan *Wireguard* VPN. Adapun langkah-langkah yang dilakukan yaitu:



Gambar 1. Diagram Alir Penelitian

Gambar 1 di atas adalah diagram alir penelitian. Pertama kali yang dilakukan yaitu memulai persiapan seperti menyiapkan perangkat keras dan perangkat lunak yang diuperlukan seperti *Mikrotik Router*, *winbox*, dan *microsip*. Selanjutnya lakukan percobaan telepon menggunakan VoIP pada jaringan tanpa VPN, pada jaringan L2TP IPSec, dan *Wireguard* VPN. Selanjutnya dilakukan pembahasan dari data hasil pengujian tersebut.

Pengujian ini menggunakan standart TIPHON seperti yang dilakukan pada penelitian [10] untuk mengetahui *troughput*, *Packet Loss*, *Delay*, dan *jitter*. TIPHON (*Telecommunications and Internet Protokol Harmonization over Network*) adalah standar untuk mengevaluasi parameter QoS yang dikeluarkan oleh ETSI (*European Telecommunications Standards Institute*). ETSI adalah organisasi yang didirikan pada tahun 1988 di Eropa yang memiliki tanggungjawab menetapkan standar teknis telekomunikasi.

2.1 Troughput

Throughput jaringan mengacu pada jumlah data yang dapat ditransmisikan melalui jaringan dalam jangka waktu tertentu. Ini adalah metrik kinerja penting yang mengukur efisiensi dan kapasitas infrastruktur jaringan.

Throughput jaringan mengukur kecepatan perjalanan data dari satu titik ke titik lain melalui jaringan.

$$\boldsymbol{Throughput} = \frac{\boldsymbol{Total\ Data\ yang\ diterima}}{\boldsymbol{Total\ Waktu}} \quad \ldots\ldots (\mathbf{1})$$

Tabel 1: Indeks *Throughput*

Kategori	*Throughput*	Indeks
Sangat Bagus	76% - 100%	4
Bagus	51% - 75%	3
Sedang	26% - 50%	2
Buruk	< 25%	1

2.2 *Packet Loss*

Packet loss mengukur seberapa banyak paket yang hilang selama proses transmisi data ke tujuan. Ada beberapa faktor yang menyebabkan paket yang hilang ketika dikirim seperti koneksi yang buruk, *protocol* yang digunakan, dan sebagainya.

Tabel 2: Indeks *Packet Loss*

Kategori	Packet Loss (%)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Buruk	25	1

$$\text{Packet Loss} = \frac{\text{Paket yang dikirim} - \text{Paket data diterima}}{\text{Paket data dikirim}} x\,100\% \quad (2)$$

2.3 Delay

Delay mengukur jeda waktu yang digunakan data untuk melakukan pengiriman dari sumber menuju ke tujuan. Dengan parameter *delay* bisa kita melihat *performance* pengiriman data dari titik A ke B.

$$\text{Delay rata} - \text{rata} = \frac{\text{Total Delay}}{\text{Jumlah paket yang diterima}} \quad \ldots\ldots\ldots (3)$$

Tabel 3: Indeks *Delay*

Kategori	Besar *Delay* (ms)	Indeks
Sangat Bagus	< 150ms	4
Bagus	150ms - 300ms	3
Sedang	300ms - 450ms	2
Buruk	> 450ms	1

2.4 Jitter

Jitter adalah variasi waktu *delay* antara saat sinyal dikirim dan saat sinyal diterima melalui koneksi jaringan. Dengan kata lain, jitter pada jaringan komputer adalah perbedaan latensi antara paket yang dikirim melalui jaringan.

$$\text{Jitter rata} - \text{rata} = \frac{\text{Total variasi delay}}{\text{Total paket yang diterima}} \quad \ldots\ldots (4)$$

Tabel 4: Indeks *Jitter*

Kategori	Besar *Jitter* (ms)	Indeks
Sangat Bagus	0ms	4
Bagus	0ms - 75ms	3
Sedang	75ms - 125ms	2
Buruk	125ms - 225ms	1

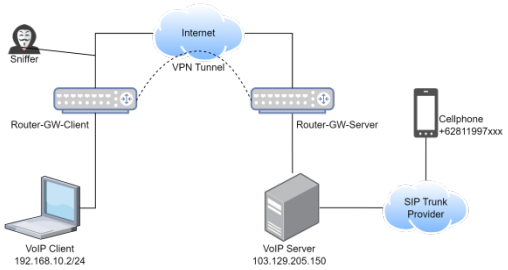
3. HASIL DAN PEMBAHASAN

3.1 Deskripsi Data

Tujuan utama penelitian ini adalah mencari tipe VPN mana yang memiliki performa QoS terbaik untuk mengamankan VoIP. Uji coba ini melibatkan tiga Langkah: Perancangan jaringan, konfigurasi L2TP IPSec, dan konfigurasi Wireguard VPN, serta pengujian awal dan pengujian akhir.

A. Desain Topologi Jaringan

Topologi jaringan komputer diatas memiliki empat buah perangkat yaitu VoIP Client dengan IP Address 192.168.10.2 yang terhubung ke internet melalui Router-GW-Client, dan VoIP Server dengan alamat IP 103.129.205.150 yang terhubung ke internet melalui Router-GW-Server. VoIP Server juga terhubung ke SIP Trunk Provider agar dapat melakukan panggilan ke nomor telepon seluler.



Gambar 2. Topologi Jaringan

Topologi jaringan komputer di atas memiliki empat buah perangkat yaitu VoIP *Client* dengan IP Address 192.168.10.2 yang terhubung ke internet melalui Router-GW-Client, dan VoIP *Server* dengan alamat IP 103.129.205.150 yang terhubung ke internet melalui Router-GW-*Server*. VoIP *Server* juga terhubung ke SIP Trunk *Provider* agar dapat melakukan panggilan ke nomor telpon seluler.

Sniffer adalah pihak yang memiliki kemungkinan menjadi sumber masalah dan ancaman keamanan,seperti melakukan penyadapan pada lalu lintas data VoIP.

Pada pengujian ini, *internet service provider* yang digunakan di sisi *client* adalah Biznethome dengan kecepatan 100mbps, dan di sisi server menggunakan ISP Indonet Colocation IP Transit dengan kecepatan 1000mbps.

Pada perancangan ini, penulis menerapkan VPN/*Tunneling* untuk mengamankan lalu lintas data VoIP dari client ke VoIP *server* menggunakan L2TP IPSec dan *Wireguard* VPN. Sistem keamanan ini ditujukan untuk melindungi dari ancaman keamanan seperti penyadapan lalu lintas data VoIP yang sedang berlangsung. Cara ini diharapkan, data VoIP akan terenkapsulasi dan terenkripsi, sehingga tidak ada pihak yang dapat melakukan penyadapan terhadap lalu lintas data VoIP tersebut.

B. Konfigurasi L2TP IPSec Tunnel

Berikut ini script konfigurasi L2TP IPSec pada Router-GW-Client dan Router-GW-Server

```
# Router-GW-Server
/interface l2tp-server server set enabled=yes use-ipsec=yes ipsec-secret=Ips3c!@#$%
/ppp secret add local-address=10.32.32.1 remote-address=10.32.32.4 name=voip-client1 password=Jos123$%^
/ip route add comment=route-via-ipsec dst-address=192.168.10.0/24 gateway=10.32.32.4

# Router-GW-Client
/interface l2tp-client add connect-to=103.129.205.145 name=l2tp-out1 user=voip-client1 password=Jos123$%^ use-ipsec=yes ipsec-secret=Ips3c!@#$%
/ip route add comment=route-via-ipsec dst-address=103.129.205.150/32 gateway=10.32.32.1
```

Berikut ini pengetesan *traceroute* untuk memastikan lalu lintas data dari voip client ke voip client melalui L2TP IPSec:

VoIP-Client> tracert -d 103.129.205.150
Tracing route to 103.129.205.150
1 1 ms 1 ms 1 ms 192.168.10.1
2 15 ms 9 ms 9 ms 10.32.32.1
3 8 ms 10 ms 8 ms 103.129.205.150

Pada hasil traceroute di atas terlihat rute pada hop kedua mengarah ke 10.32.32.1, ini adalah IP Address Interface L2TP IPSec di Router-VoIP-Server, sehingga bisa dipastikan traffic di atas sudah melalui L2TP IPSec tunnel.

C. Konfigurasi Wireguard VPN

Berikut ini *script* konfigurasi *Wireguard* pada Router-GW-Client dan Router-GW-Server

```
# Router-GW-Server
/interface wireguard add listen-port=51820 name=wireguard1
/ip route add comment=route-via-wireguard dst-address=192.168.10.0/24 gateway=10.50.0.2
/interface wireguard peers add allowed-address=10.50.0.2/32,192.168.10.0/24 endpoint-port=51820 interface=wireguard1 preshared-key=\
"QJD44KlvQVVvI2EUqkiMI9j4FbKqZAu41iEGks8THF8=" private-key=\
```

```
"YP7oGySQ4mHQHbJ29UhbHMaL+JGJ9G83Gny
/GwUF+l4=" public-key=\
"fXYhEKyWe7Zlqvqrc0iThxTowzJQUbJXhv3
CPhAJklE="

# Router-GW-Client
/interface wireguard add listen-
port=51820 name=wireguard1
/ip route add comment=route-via-
wireguard dst-
address=103.129.205.150/32
gateway=10.50.0.1
/interface wireguard peers
add allowed-address=\
10.50.0.1/32,103.129.205.150/32 \
endpoint-address=103.129.205.145
endpoint-port=51820
interface=wireguard1 preshared-key=\
"QJD44KlvQVVvI2EUqkiMI9j4FbKqZAu41iE
Gks8THF8=" private-key=\
"YP7oGySQ4mHQHbJ29UhbHMaL+JGJ9G83Gny
/GwUF+l4=" public-key=\

"ZFHt53e/ItZcQ3URNNPo1TXu6qSyGGVUu4X
A+KItCm8="
```

Berikut ini pengetesan traceroute untuk memastikan lalu lintas data dari voip client ke voip client melalui L2TP IPSec:

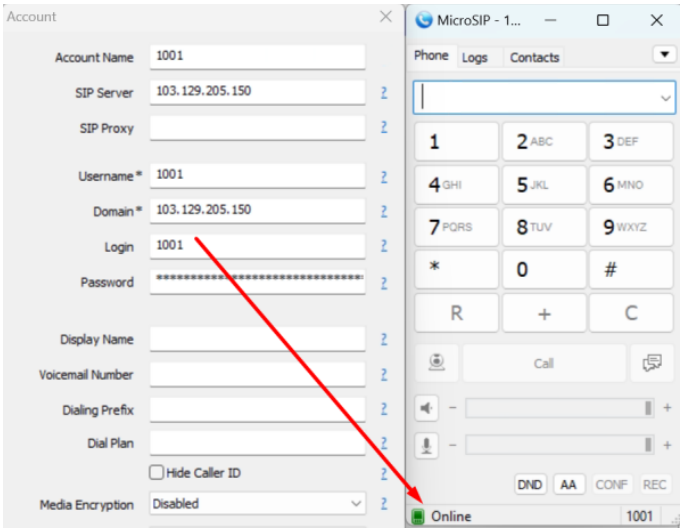
VoIP-Client> tracert -d 103.129.205.150
Tracing route to 103.129.205.

1 1 ms 1 ms 1 ms 192.168.10.1
2 11 ms 10 ms 12 ms 10.50.0.1
3 9 ms 9 ms 11 ms 103.129.205.150
Trace complete.

Pada hasil *traceroute* di atas terlihat lalu lintas data sudah melalui wireguard VPN.

D. Menghubungkan VoIP Client ke VoIP Server

Pada pengujian kali ini, VoIP client menggunakan aplikasi *softphone* yaitu MicroSIP. Pada tampilan berikut, tampilan konfigurasi MicroSIP dan status *online* yang berarti sudah berhasil terhubung ke VoIP *Server*.



Gambar 3. Konfigurasi MicroSIP

Berikut ini status koneksi voip di VoIP *Server*:

VoIP-Server# asterisk -rx "sip show peers"

Name/username	*Host*	*Status*
1001/1001	*192.168.10.2*	*OK (22 ms)*
Trunk-FR	*103.129.205.228*	*OK (1 ms)*

Hasil pengetesan status koneksi VoIP di atas menunjukan bahwa konek sudah sudah OK dengan latency 22ms untuk user 1001 dan latency 1ms untuk koneksi ke SIP Trunk Provider.

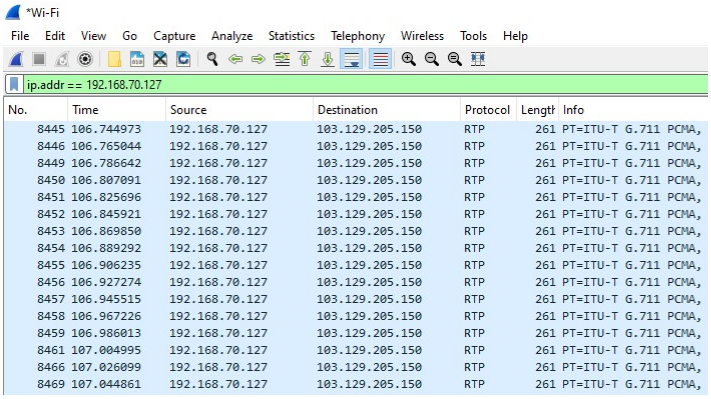
3.2 Pembahasan

Setelah VoIP Client terhubung ke VoIP Server maka dilakukan pengujian menggunakan MicroSIP VoIP untuk melakukan panggilan telpon ke nomor seluler. Pengujian terdiri dari pengujian keamanan lalu lintas data voip dan Performa QoS pada lalu lintas data VoIP.

A. Pengujian Kemanan Lalu Lintas Data VoIP

Setelah VoIP *Client* terhubung ke VoIP *Server* dan dilakukan pengujian telepon menggunakan MicroSIP VoIP, maka didapati bahwa koneksi VoIP tanpa VPN mengakibatkan *sniffer* dapat menyadap isi telepon yang dilakukan. Gambar *wireshark* dengan kondisi tanpa VPN, dapat

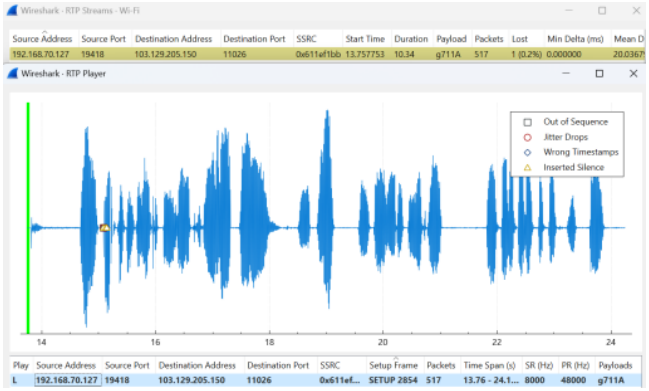
dilihat bahwa traffic RTP terdeteksi Ketika tools sniffing dijalankan.



No.	Time	Source	Destination	Protocol	Lengt	Info
8445	106.744973	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8446	106.765044	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8449	106.786642	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8450	106.807091	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8451	106.825696	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8452	106.845921	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8453	106.869850	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8454	106.889292	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8455	106.906235	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8456	106.927274	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8457	106.945515	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8458	106.967226	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8459	106.986013	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8461	107.004995	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8466	107.026099	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,
8469	107.044861	192.168.70.127	103.129.205.150	RTP	261	PT=ITU-T G.711 PCMA,

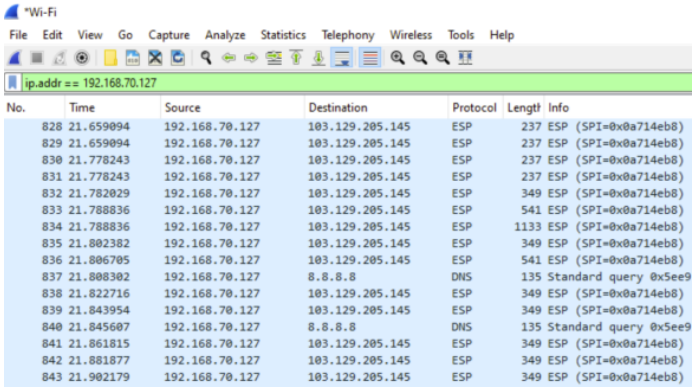
Gambar 4. Packet VoIP tanpa VPN

Dikarenakan data VoIP dapat dibaca oleh sniffer, maka percakapan VoIP dapat didengarkan.



Gambar 5. Rekaman VoIP tanpa VPN

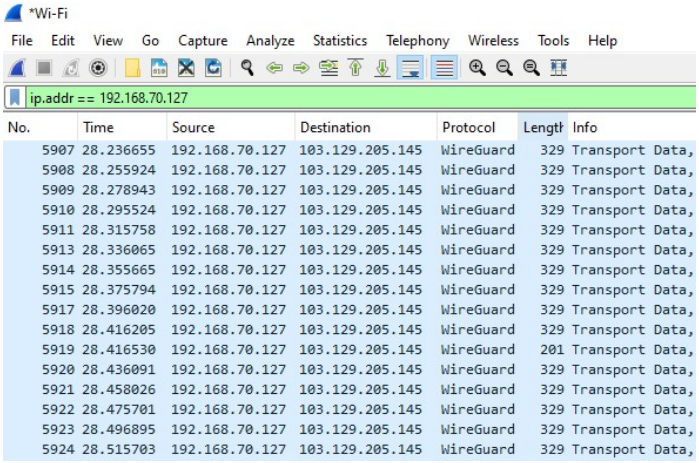
Adapun Ketika menggunakan L2TP IPSec sniffer tidak dapat menyadap lalu lintas data VoIP tersebut, dan traffic yang terdeteksi adalah protocol ESP seperti yang tersaji pada Gambar 6:



No.	Time	Source	Destination	Protocol	Lengt	Info
828	21.659094	192.168.70.127	103.129.205.145	ESP	237	ESP (SPI=0x0a714eb8)
829	21.659094	192.168.70.127	103.129.205.145	ESP	237	ESP (SPI=0x0a714eb8)
830	21.778243	192.168.70.127	103.129.205.145	ESP	237	ESP (SPI=0x0a714eb8)
831	21.778243	192.168.70.127	103.129.205.145	ESP	237	ESP (SPI=0x0a714eb8)
832	21.782029	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)
833	21.788836	192.168.70.127	103.129.205.145	ESP	541	ESP (SPI=0x0a714eb8)
834	21.788836	192.168.70.127	103.129.205.145	ESP	1133	ESP (SPI=0x0a714eb8)
835	21.802382	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)
836	21.806705	192.168.70.127	103.129.205.145	ESP	541	ESP (SPI=0x0a714eb8)
837	21.808302	192.168.70.127	8.8.8.8	DNS	135	Standard query 0x5ee9
838	21.822716	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)
839	21.843954	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)
840	21.845607	192.168.70.127	8.8.8.8	DNS	135	Standard query 0x5ee9
841	21.861815	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)
842	21.881877	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)
843	21.902179	192.168.70.127	103.129.205.145	ESP	349	ESP (SPI=0x0a714eb8)

Gambar 6. Packet VoIP dengan L2TP IPSec VPN

Sedangkan ketika menggunakan *Wireguard* VPN, *sniffer* tidak dapat menyadap lalu lintas data VoIP tersebut, dan *traffic* yang terdeteksi adalah *protocol wireguard*:



Gambar 7. Packet VoIP dengan *Wireguard* VPN

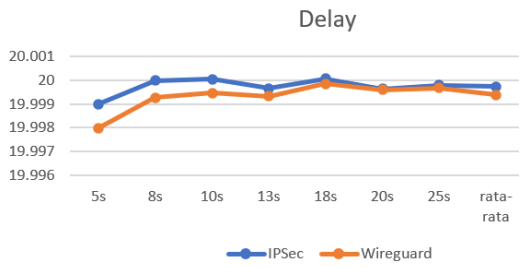
B. Pengujian Quality of Service (QoS)

Peneliti melakukan pengujian terhadap 10 dataset yang disiapkan untuk melihat hasil berdasarkan rumus TIPHON. Setelah dilakukan pengujian, bisa disimpulkan bahwa performa QoS L2TP IPSec lebih baik dibandingkan *Wireguard*.

Pada pengujian *delay*, tes yang dilakukan mengungkapkan bahwa L2TP IPSec menunjukkan delay rata-rata 19.9997ms, sedangkan *Wireguard* menunjukkan *delay* lebih baik sebesar 19.9994ms.

Tabel 5: Delay (ms)

Pengujian Call	IPSec	Wireguard
5s	19.9990	19.9980
8s	20.0000	19.9993
10s	20.0001	19.9995
13s	19.9997	19.9993
18s	20.0001	19.9999
20s	19.9996	19.9996
25s	19.9998	19.9997
rata-rata	19.9997	19.9994

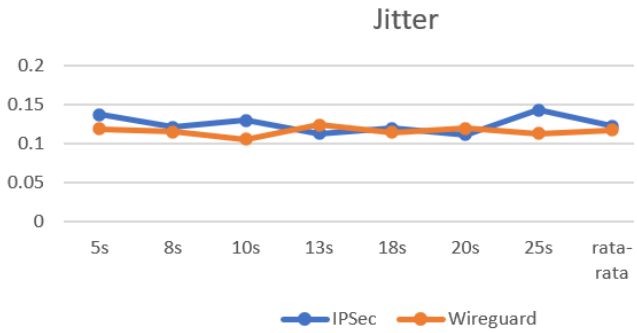


Gambar 8. Grafik delay

Selanjutnya, jitter yang diamati pada L2TP IPSec adalah sekitar 0.122839 ms, sementara Wireguard menunjukkan jitter yang lebih bagus yaitu 0.117597ms.

Tabel 6: Jitter (ms)

Pengujian Call	IPSec	Wireguard
5s	0.137364	0.118622
8s	0.121371	0.115092
10s	0.12992	0.10535
13s	0.113005	0.123768
18s	0.11966	0.11451
20s	0.111628	0.119828
25s	0.143133	0.113157
rata-rata	0.122839	0.117597

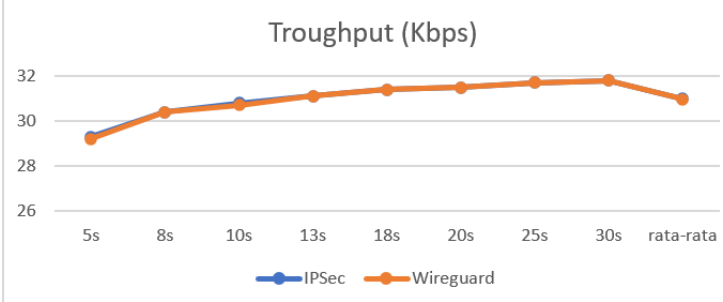


Gambar 9. Grafik Jitter

pada pengujian troughput IPSec memiliki troughput lebih tinggi sebesar 31kbps sedangkan *Wireguard* memiliki troughput 30.975kbps

Tabel 7: Troughput (kbps)

Pengujian Call	IPSec	Wireguard
5s	29.3	29.2
8s	30.4	30.4
10s	30.8	30.7
13s	31.1	31.1
18s	31.4	31.4
20s	31.5	31.5
25s	31.7	31.7
30s	31.8	31.8
rata-rata	31	30.975

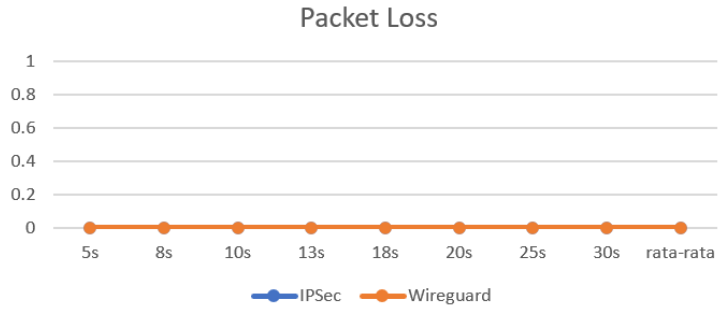


Gambar 10. Grafik Troughput

Dan pada pengujian packet loss keduanya memiliki 0% packet loss.

Tabel 8: Packet Loss (%)

Pengujian Call	IPSec	Wireguard
5s	0 %	0 %
8s	0 %	0 %
10s	0 %	0 %
13s	0 %	0 %
18s	0 %	0 %
20s	0 %	0 %
25s	0 %	0 %
30s	0 %	0 %
rata-rata	0 %	0 %



Gambar 11. Grafik Packet Loss

4. KESIMPULAN

Setelah melakukan serangkaian pengujian pengembangan VoIP berdasarkan skenario yang diuraikan di bagian sebelumnya, dapat dideduksi bahwa sistem komunikasi VoIP yang tidak memiliki langkah-langkah keamanan rentan terhadap potensi penyadapan pada percakapan yang sedang berlangsung dan intersepsi data suara melalui Deteksi Panggilan VoIP dan Pemutar RTP.

Sebaliknya, dalam konteks serangan, sistem komunikasi VoIP VPN yang memanfaatkan L2TP IPSec dan Wireguard mampu menjaga kerahasiaan komunikasi yang sedang berlangsung, sehingga mencegah intersepsi data suara melalui VoIP Call Detection dan RTP Player.

Pada kinerja jaringan, tes yang dilakukan mengungkapkan bahwa L2TP IPSec menunjukkan delay rata-rata 19.9997ms, sedangkan Wireguard menunjukkan delay lebih baik sebesar 19.9994ms. Selanjutnya, jitter yang diamati pada L2TP IPSec adalah sekitar 0.122839 ms, sementara Wireguard menunjukkan jitter yang lebih bagus yaitu 0.117597ms. Pada pengujian packet loss keduanya memiliki 0% packet loss, dan pada pengujian troughput IPSec memiliki troughput lebih tinggi sebesar 31kbps sedangkan wireguard memiliki troughput 30.975kbps.

DAFTAR PUSTAKA

[1] Berlian, "Membangun Server Voip Berbasis Asterisk," *Jurnal Media Infotama*, Vol. 16, No. 1, 2020.

[2] A. Hidayat And I. P. Saputra, "Implementation Voice Over Internet Protocol (Voip) As A Communication Media Between Unit At University Muhammadiyah Metro," *Ijiscs (International Journal Of Information System And Computer Science)*, Vol. 5, No. 3, 2023.

[3] D. P. Putra, "Analisis Keamanan Voice Over Internet Protocol (Voip) Over Virtual Private Network (Vpn)," *Jurnal Informatika Dan Rekayasa Perangkat*

Lunak (Jatika), Vol. 2, No. 3, Pp. 324–333, 2021, [Online]. Available: Http://Jim.Teknokrat.Ac.Id/Index.Php/Informatika

[4] M. Zaharaddeen Bello, B. Alhaji Buhari, B. Aminu Bodinga, And M. Malami Umar, "Secure And Optimize Voip Communication Using Qos Technologies And Vpn," *Journal Of Network Security And Data Mining*, Vol. 5, No. 3, 2022.

[5] Y. Bhatt, Dr. P. Sharma, And J. Patel, "Securing Online Payment Using Virtual Private Network (Vpn)," *Int J Sci Res Sci Eng Technol*, Vol. 8, No. 3, Pp. 65–70, May 2021, Doi: 10.32628/Ijsrset218311.

[6] M. A. Gunawan And S. Wardhana, "Implementasi Dan Perbandingan Keamanan Pptp Dan L2tp/Ipsec Vpn (Virtual Private Network)," *Resistor (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer)*, Vol. 6, No. 1, 2023.

[7] B. Santoso, A. Sani, T. Husain, And N. Hendri, "Vpn Site To Site Implementation Using Protocol L2tp And Ipsec," *Teknokom*, Vol. 4, No. 1, Pp. 30–36, Jun. 2021, Doi: 10.31943/Teknokom.V4i1.59.

[8] D. Novianto, Y. S. Japriadi, And L. Tommy, "Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard Vpn Di Routerboard Mikrotik," *Jurnal Ilmiah Informatika Global*, Vol. 13, No. 2, Aug. 2022, Doi: 10.36982/Jiig.V13i2.2308.

[9] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree, And D. Doghramachi, "Comparison Of Vpn Protocols At Network Layer Focusing On Wire Guard Protocol," *International Journal Of Interactive Mobile Technologies*, Vol. 14, No. 18, Pp. 157–177, 2020, Doi: 10.3991/Ijim.V14i18.16507.

[10] Subektiningsih, Renaldi Renaldi, Dan Ferdiansyah, Pramudhita. "Analisis Perbandingan Parameter Qos Standar Tiphon Pada Jaringan Nirkabel Dalam Penerapan Metode Pcq," *Jurnal Informatika Dan Komputer Explore*, Vol. 12, No. 1, 2022.