# ANALISIS KOMPARASI PROTOKOL *VIRTUAL PRIVATE NETWORK* (VPN) PADA METODE PPTP, L2TP, SSTP, DAN OPEN VPN

**Jerico Sola Reinier Sumbayak[1],Jeremia Siregar[2],Ruth Meivera[3]**

Prodi Teknik Informatika, Fakultas Teknologi Industri
Institut Sains dan Teknologi TD.Pardede,Jl.DR. TD. Perdede No.8 Medan 20153

*Email : jericosumbayak@gmail.com[1], jeremiasiregar@istp.ac.id[2], v_manut@yahoo.com[3]*

## ABSTRAK

*Virtual Private Network (VPN)* merupakan teknologi jaringan yang memungkinkan terjadinya pertukaran data terenkripsi antara dua atau lebih pengguna secara aman. Dari hasil pengujian, metode *OpenVPN* menunjukkan kinerja enkripsi paling kuat dibandingkan *PPTP, L2TP*, dan *SSTP*, karena proses pengacakan kodenya membutuhkan waktu lebih lama sehingga lebih sulit ditembus. Keunggulan utama *VPN* adalah setiap data yang dikirim akan melewati jalur terowongan (*tunnel*), sehingga memberikan tingkat keamanan yang lebih baik. *Tunneling* sendiri merupakan teknik untuk memindahkan data dari satu jaringan ke jaringan lain dengan memanfaatkan internet sebagai media tersembunyi. Berdasarkan uji serangan *DoS, protokol PPTP* dan *L2TP* menghasilkan waktu pengiriman 100 ms dengan jumlah paket relatif besar, sementara *SSTP* dan *OpenVPN* mencatat waktu lebih singkat yaitu 2 ms dengan 28 paket data. Hasil pengukuran menggunakan parameter *QoS* memperlihatkan bahwa *OpenVPN* memiliki nilai *Packet Loss* 0% (kategori memuaskan), *Delay* rata-rata 0 ms (memuaskan), *Jitter* 17 ms (bagus), serta *Throughput* yang stabil. Dari keempat metode, *PPTP* memperoleh nilai *throughput* tertinggi sebesar 3,428 Mbps, namun *OpenVPN* dinilai lebih seimbang karena mendukung keamanan dan performa transfer data sekaligus.

**Kata Kunci** : NDLC, Mikrotik, *VPN*, *Quality of Service*

## ABSTRAK

*Virtual Private Network (VPN) is a network technology that allows encrypted data exchange between two or more users securely. From test results, the OpenVPN method shows the strongest encryption performance compared to PPTP, L2TP, and SSTP, because its code scrambling process takes longer, making it harder to breach. The main advantage of VPN is that every data sent will pass through a tunnel, providing a better level of security. Tunneling itself is a technique for moving data from one network to another by leveraging the internet as a hidden medium. Based on DoS attack tests, the PPTP and L2TP protocols produce a delivery time of 100 ms with a relatively large number of packets, while SSTP and OpenVPN record a shorter time of 2 ms with 28 data packets. Measurement results using QoS parameters show that OpenVPN has a Packet Loss value of 0% (satisfactory category), Average delay 0 ms (satisfactory), Jitter 17 ms (good), and stable Throughput. Among the four methods, PPTP achieved the highest throughput score of 3.428 Mbps, however, OpenVPN is rated more balanced because it supports both security and data transfer performance*

***Keywords** : NDLC, Mikrotik, VPN, Quality of Service*

## 1. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi tidak terlepas dari perubahan pola pikir manusia yang terus berkembang seiring dengan zaman. Bagi negara berkembang seperti Indonesia, kemajuan hanya dapat

dicapai jika kualitas sumber daya manusianya juga meningkat. Pendidikan yang terstruktur dan berkualitas akan melahirkan individu yang mampu berpikir kritis, kreatif, dan produktif, sehingga berkontribusi pada peningkatan kesejahteraan bangsa (Putra et al., 2018).

*VPN* menjadi alasan bagi orang dalam menjaga keamanan komunikasi datanya dikarenakan *VPN* dapat membentuk jaringan privat di atas infrastruktur publik dengan mekanisme yang dimilikinya yaitu autentikasi dan enkripsi, yang mana hal ini membuat pihak yang berwenang saja dapat mengakses data tersebut. Salah satu protokol yang dimiliki *VPN* yang digunakan untuk menjaga kerahasiaan data yaitu *IPSec*, sebuah protokol yang bekerja pada lapisan jaringan untuk memastikan keamanan transmisi data melalui enkripsi yang kuat.

Selain itu, teknologi seperti *OpenSSL* juga dapat digunakan untuk mengamankan komunikasi melalui autentikasi kunci dan enkripsi data, baik dengan *IP* statis maupun dinamis. Dengan adanya dukungan tersebut, *VPN* menjadi solusi yang andal dalam menjaga keamanan komunikasi data, baik pada jaringan lokal maupun saat mengakses internet publik (Juma et al., 2020).

## 2. TINJAUAN PUSTAKA

### 2.1 VPN (*Virtual Private Network*)

*Virtual Private Network* atau *VPN* merupakan salah satu sebuah cara yang dapat mengakses *LAN* atau *Local Ara Network* pada jarak tertentu melalui koneksi jaringan internet untuk melakukan transmisi data secara pribadi sehingga penggunaan *VPN* dapat dipastikan keamannnya yang mana kita dapat menggunakan jaringan publik tapi kita sifatnya privat atau tidak terlihat di jaringan secara fisik (Oktivasari & Utomo, 2016).

Keamanan dalam *VPN* dicapai dengan membangun *tunnel*, yaitu jalur komunikasi virtual yang mengenkripsi data yang ditransmisikan. Dengan cara ini, data yang dikirimkan akan terlindungi dari pihak yang tidak berwenang (Watmah, 2020).

### *2.2 Tunneling*

*Tunneling* sendiri adalah konsep dasar dari *VPN* yang memungkinkan pembentukan jaringan lokal secara virtual melalui internet yang mana ini adalah sebuah cara untuk memungkinkan proses pengitiman data dapat dipastikan aman dan tenkripsi dari jaringan yang bahaya. Proses ini bekerja dengan cara melakukan enkapsulasi, yaitu membungkus protokol tertentu ke dalam paket protokol lain. Saat server dan klien membangun komunikasi melalui internet, jalur khusus (tunnel) terbentuk untuk mengalirkan data secara privat.

Agar tunnel dapat bekerja, diperlukan protokol komunikasi seperti *IPSec, L2TP (Layer 2 Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol),* atau *GRE (Generic Routing Encapsulation).* Pada proses enkapsulasi, ditambahkan header tunnel yang berfungsi sebagai identitas jalur transmisi, sehingga data dapat sampai ke tujuan dengan aman (Yumin et al., 2019).

## 3. METODOLOGI PENELITIAN

### 3.1 Desain Sistem

Dengan perancangan Analisis *Quality of Service* dan Implementasi metode *PPTP, L2TP, SSTP,* dan *OpenVPN* dengan menggunakan *IPSec VPN*, penulis ingin menganalisa beberapa parameter meliputi *Delay, Throughput, Packet Loss,* dan *Jitter.* Dari analisa *Quality of Service* ini akan diketahui bagaimana *Quality of Service* yang telah menggunakan metode keamanan *IPSec* dan bagaimana cara untuk mengoptimalkan *Quality of Service* yang telah menggunakan metode keamanan Jaringan di *server* Mikrotik

### 3.2 Desain Arsitektur Jaringan

Rancangan arsitektur jaringan dalam penelitian ini menggunakan *Local Area Network* (LAN) dan *Wireless Local Area Network* (WLAN), dimana *server* Mikrotik dan dua *user* terhubung di dalam satu jaringan menggunakan *Access Point.*

## 4. HASIL DAN PEMBAHASAN

Hasil perhitungan rata-rata dari pengujian parameter QoS dapat dilihat pada Tabel Perbandingan Qos berikut ini

| NO | PROTOKOL | | | |
|---|---|---|---|---|
| | PPTP | | | |
| | THROUGHPUT | DELAY | PACKET LOSS | JITTER |
| 1 | 898 | 7.004 | 0.02% | 11.646 |
| 2 | 5579 | 0.884 | 0.03% | 1.748 |
| 3 | 1500 | 4.414 | 0.00% | 8.725 |
| 4 | 3567 | 1.703 | 0.00% | 3.349 |
| 5 | 2180 | 2.7 | 0.49% | 5.17 |
| 6 | 5853 | 0.924 | 0.01% | 4.296 |
| 7 | 565 | 11.278 | 0.00% | 23.373 |
| 8 | 3613 | 1.591 | 0.02% | 118.026 |
| 9 | 3957 | 1.229 | 0.03% | 29.843 |
| 10 | 4039 | 1.396 | 0.00% | 14.094 |
| **JML** | 31751 | 33 | 0.606 | 220 |
| RATA | 3428 | 3 | 0.006 | 23 |

**Tabel 1** ***QoS PPTP***

| NO | PROTOKOL | | | |
|---|---|---|---|---|
| | L2TP | | | |
| | THROUGHPUT | DELAY | PACKET LOSS | JITTER |
| 1 | 2658 | 4.525 | 0.82% | 4.525 |
| 2 | 1131 | 7.303 | 0.38% | 7.303 |
| 3 | 1351 | 59.163 | 0.36% | 110.374 |
| 4 | 1689 | 4.705 | 0.37% | 8.896 |
| 5 | 805 | 9.303 | 1.41% | 18.16 |
| 6 | 1169 | 6.548 | 0.68% | 27.686 |
| 7 | 524 | 14.042 | 0.94% | 5.111 |
| 8 | 2623 | 2.75 | 0.66% | 12.205 |
| 9 | 1125 | 6.248 | 0.25% | 18.049 |
| 10 | 852 | 9.223 | 0.19% | 15.849 |
| **JML** | 13926 | 124 | 0.61 | 228 |
| RATA | 1252 | 13 | 0.061 | 25 |

**Tabel 2** ***QoS L2TP***

| NO | PROTOKOL | | | |
|---|---|---|---|---|
| | SSTP | | | |
| | THROUGHPUT | DELAY | PACKET LOSS | JITTER |
| 1 | 1093 | 5.132 | 0.22% | 7.303 |
| 2 | 1770 | 24.312 | 0.38% | 110.374 |
| 3 | 1499 | 2.811 | 0.36% | 8.896 |
| 4 | 1870 | 11.013 | 0.37% | 18.16 |
| 5 | 1138 | 9.728 | 1.41% | 12.139 |
| 6 | 1544 | 6.882 | 0.60% | 12.783 |
| 7 | 259 | 4.521 | 0.75% | 22.686 |
| 8 | 2548 | 4.997 | 1.75% | 5.111 |
| 9 | 677 | 4.287 | 0.70% | 12.205 |
| 10 | 833 | 6.756 | 0.68% | 16.049 |
| **JML** | 13230 | 80 | 0.72 | 226 |
| RATA | 1349 | 8 | 0.072 | 24 |

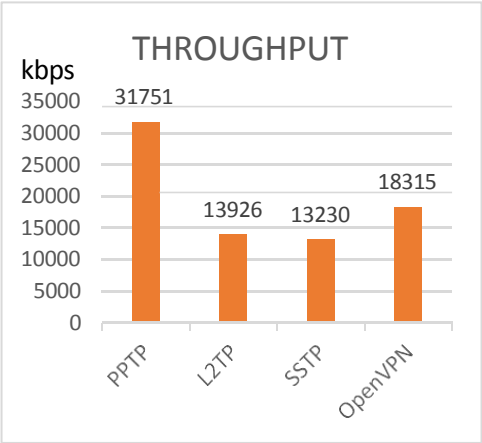
**Tabel 3** ***QoS SSTP***

| NO | PROTOKOL | | | |
|---|---|---|---|---|
| | Open VPN | | | |
| | THROUGHPUT | DELAY | PACKET LOSS | JITTER |
| 1 | 3207 | 0.01 | 0% | 23.9 |
| 2 | 1689 | 0.12 | 0% | 22.533 |
| 3 | 805 | 0.01 | 0% | 12.654 |
| 4 | 1169 | 0.01 | 0% | 18.2 |
| 5 | 1544 | 0.01 | 0% | 17.2 |
| 6 | 259 | 0.01 | 0% | 9.3 |
| 7 | 2548 | 0.01 | 0% | 20.3 |
| 8 | 677 | 0.01 | 0% | 10.4 |
| 9 | 5853 | 0.05 | 0% | 28.3 |
| 10 | 565 | 0.01 | 0% | 10.1 |
| **JML** | 18315 | 0.25 | 0 | 172.887 |
| RATA | 1679 | 0.025 | 0 | 17 |

**Tabel 4** ***QoS OPEN VPN***

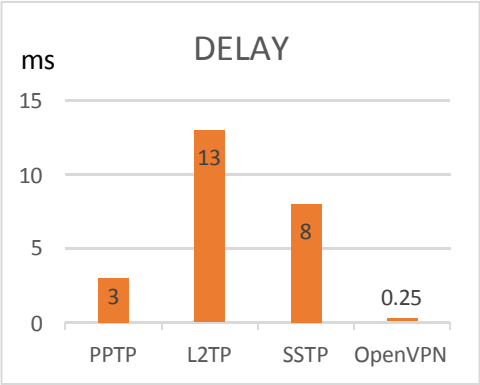
Pada Tabel 1,2,3,4 Perbandingan QoS menjelaskan setelah perhitungan terhadap metode VPN yang telah di hitung performanya dengan standart perhitungan TIPHON.

Grafik perbandingan rata-rata parameter QoS VPN dapat dilihat pada Gambar 1 Trougput , Gambar 2 Delay, Gambar 3 Paket Loss, dan Gambar 4 Jitter berikut ini.



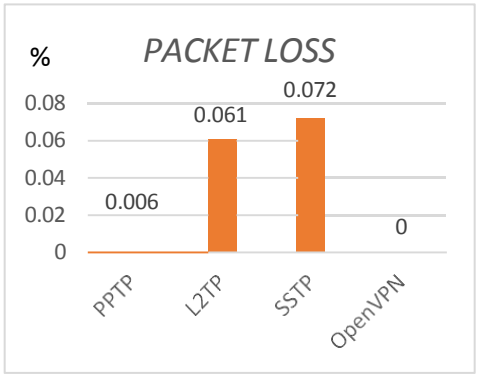

**Gambar 1 *Throughput***

Kondisi throughput dari masing-masing protokol menunjukkan perbedaan , yakni PPTP 3428 kbps, L2TP 1252kbps, SSTP 1349 kbps dan OpenVPN 1679 kbps. Hal ini menunjukkan bahwa throughput PPTP lebih baik dibandingkan dengan throughput metode lainnya karena throughput PPTP lebih besar.



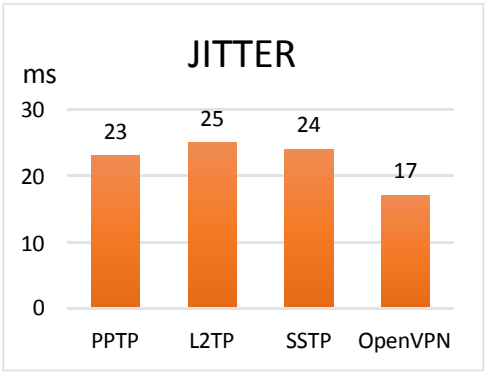

**Gambar 2 *Delay***

Berdasarkan grafik perbedaan rata-rata delay yang ditunjukkan pada Gambar 2, nilai rata-rata delay dari PPTP berjumlah 3 ms, L2TP 13 ms, SSTP 8ms dan sedangkan nilai rata-rata delay dari OpenVPN berjumlah 0.25 ms. Metode OpenVPN masuk dalam kategori latency "Sangat Bagus". Maka, dapat diketahui bahwa delay dari OpenVPN lebih baik dibanding dari metode VPN lainnya karena nilai delay OpenVPN lebih kecil.




**Gambar 3 *Packet Loss***

Berdasarkan grafik perbedaan rata-rata packet loss yang ditunjukkan pada Gambar 4.33 Paket Loss keempat metode masuk dalam indeks 4, yaitu perfect. Nilai packet loss dari PPTP sebanyak 0.006%, L2TP sebanyak 0.061%, SSTP adalah sebanyak 0.72%, sedangkan nilai packet loss dari OpenVPN sebanyak 0%. Hal ini berarti packet loss Protokol OpenVPN lebih baik karena nilai packet loss OpenVPN lebih kecil.




**Gambar 4 *Jitter***

Kondisi jitter dari masing-masing protokol menunjukkan perbedaan yang tidak terlalu signifikan, keempat metode VPN masuk kedalam indeks 3 "Bagus", dengan nilai PPTP 23 ms, L2TP 25 ms, SSTP 23 ms, dan OpenVPN dengan 17 ms. Lebih baik dibandingkan dengan metode VPN lainnya.

Hasil pengukuran QoS yang di dapatkan metode tersebut didapatkan Paket Loss dengan metode Open VPN

dengan nilai indeks QoS yaitu 0% dengan kategori memuaskan. Untuk metode Delay rata – rata sebesar 0 ms dengankategori memuaskan, untuk nilai Jitter metode OpenVPN nilai 17 ms bernilai bagus ,sedangkan untuk nilai

Trounghput dari keempat metode tersebut nilai terbaik adalah metode PPTP Server rata – rata nilai sebesar 3,428 Mbps dengan kategori memuaskan. Dari nilai-nilai parameter tersebut metode OpenVPN dapat disimpulkan lebih bagus, dengan mengacu pada standard TIPHON keempat metode tersebut masih layak digunakan akan tetapi motode OpenVPN lebih efektif.

## 5. KESIMPULAN DAN SARAN

1. PPTP (Point-to-Point Tunneling Protocol**)**
- Kelebihan: Memiliki nilai throughput tertinggi di antara keempat protokol, serta waktu pengiriman data yang cepat (3428 kbps).
- Kekurangan: Tingkat keamanan relatif lebih rendah karena enkripsi yang lemah dan sudah dianggap usang oleh banyak vendor keamanan.
- Cocok Digunakan Untuk sistem jaringan yang mengutamakan kecepatan transfer data dan tidak terlalu kritis terhadap tingkat keamanan tinggi, seperti penggunaan internal pada jaringan lokal tertutup.

2. L2TP (Layer 2 Tunneling Protocol)
- Kelebihan: Mendukung enkripsi tambahan melalui protokol IPSec, dan waktu pengiriman data cepat.
- Kekurangan: Lebih lambat dibanding PPTP karena proses enkripsi ganda (tunneling dan IPSec).
- Cocok Digunakan Untuk kebutuhan jaringan yang membutuhkan keamanan lebih baik dari PPTP, misalnya untuk penggunaan kantor kecil hingga menengah, dengan trafik tidak terlalu padat.

3. SSTP (Secure Socket Tunneling Protocol)
- Kelebihan: Menggunakan port HTTPS (443) sehingga mudah menembus firewall dan proxy.
- Kekurangan: Hanya tersedia secara optimal di sistem operasi Windows, dan fleksibilitasnya terbatas di platform lain.
- Cocok Digunakan Untuk lingkungan jaringan yang mengandalkan Windows sebagai OS utama, serta kondisi jaringan yang membatasi port atau menggunakan firewall ketat.

4. OpenVPN
- Kelebihan: Memiliki nilai QoS terbaik (packet loss 0%, delay 0 ms, jitter 17 ms), mendukung banyak platform, dan menggunakan enkripsi tingkat tinggi.
- Kekurangan: Konfigurasi awal lebih kompleks dibanding protokol lain, dan waktu enkripsi sedikit lebih tinggi .
- Cocok Digunakan Untuk sistem jaringan yang mengutamakan keamanan tinggi dan stabilitas koneksi, seperti akses jarak jauh, perkantoran skala besar, atau akses data sensitif.

Sebagai tindak lanjut dari penelitian ini, disarankan untuk melakukan pengujian yang lebih mendalam terhadap keamanan jaringan Virtual Private Network (VPN) dengan menggunakan metode PPTP, L2TP, SSTP, dan OpenVPN. Berdasarkan hasil yang diperoleh, metode OpenVPN menunjukkan performa yang lebih baik dibandingkan metode lainnya, dengan kecepatan transfer data di atas 2 Mbps, tingkat kehilangan paket sebesar 0%, serta waktu pengiriman

data sebesar 0 ms. Oleh karena itu, metode OpenVPN direkomendasikan untuk digunakan dalam mendukung keamanan, distribusi informasi, dan optimalisasi transfer data.

Untuk pengembangan lebih lanjut, sistem ini dapat ditingkatkan dengan spesifikasi perangkat keras yang lebih tinggi, sehingga mampu melayani lebih banyak klien secara bersamaan dan menjaga stabilitas serta kinerja jaringan VPN secara optimal

DAFTAR PUSTAKA

Juma, M., Monem, A. A., & Shaalan, K. (2020). Hybrid End-to-End VPN Security Approach for Smart IoT Objects. Journal of Network and Computer Applications, 158. https://doi.org/10.1016/j.jnca.2020.102598

Agung, R., Adam, F., & Hidayatulloh, S. (2020). Implementasi intercity berbasis tunneling mikrotik menggunakan metode eoip tunnel. 14(1), 66–70.

Akbar, F., & Napiah, M. (2021). Metode Point to Point Tunneling Protocol Untuk Keamanan Jaringan Studi Kasus Kantor Walikota Administrasi Jakarta Barat. 1(2), 85–91.

Khasanah, S. N., & Utami, L. A. (2018). Implementasi Failover Pada Jaringan WAN Berbasis VPN. Jurnal Teknik Informatika STMIK Antar Bangsa, 4(1), 62–66.

Mahardani, A. A., & Asmunin. (2017). Implementasi Openvpn Menggunakan Ldap Sebagai Manajemen User. Jurnal Manajemen Informatika, 7(1), 29–