

ANALISIS MANAJEMEN TRAFIK JARINGAN PADA VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN PROTOKOL PPTP, L2TP/IPSEC, DAN OPEN VPN

Harry Pribadi Fitrian, Amanda Aulia Nurani, Idan Mulhakim, Nabila Maesaroh, Purnama Raharja

S1 Informatika Universitas Teknologi Digital

Jl. Cibogo No. Indah 3, Mekarjaya, Kec. Rancasari, Kota Bandung, Jawa Barat 40000

amanda20123043@digitechuniversity.ac.id

ABSTRAK

Virtual Private Network (VPN) merupakan teknologi yang banyak digunakan untuk mengamankan data dan menjaga privasi saat berkomunikasi melalui jaringan publik. Namun, pengelolaan trafik jaringan VPN menimbulkan tantangan besar, seperti distribusi bandwidth, pengaturan routing yang efisien, dan kualitas layanan (*Quality of Services*). Penelitian ini menggunakan metode studi literatur untuk menganalisis berbagai strategi manajemen trafik dalam VPN, termasuk perbandingan protokol VPN yang umum digunakan, seperti PPTP, L2TP/IPsec, dan OpenVPN, serta penerapan teknologi modern seperti *Software-Defined Wide Area Network (SD-WAN)* dan *Multiprotocol Label Switching (MPLS)*. Hasil penelitian ini menunjukkan bahwa PPTP memiliki kecepatan tinggi namun memiliki kelemahan keamanan, sedangkan OpenVPN memberikan tingkat keamanan yang tinggi meskipun membutuhkan sumber daya yang lebih banyak. Di sisi lain, teknologi SD-WAN terbukti meningkatkan efisiensi distribusi trafik hingga 40% dengan dengan penggunaan jalur utama dan cadangan yang fleksibel, sementara MPLS unggul dalam manajemen trafik secara real-time dengan prioritas aplikasi yang lebih baik. Penelitian ini memberikan informasi berharga bagi pengembang sistem untuk memanfaatkan kombinasi protokol VPN dan teknologi pendukung seperti load balancing (penyeimbangan beban) dan optimasi QoS untuk meningkatkan stabilitas, efisiensi, dan kinerja jaringan VPN secara keseluruhan.

Kata kunci : VPN, Traffic Management, VPN Protocol, QoS, SD-WAN, MPLS, PPTP, L2TP, IPsec

1. PENDAHULUAN

Virtual Private Network (VPN) adalah teknologi yang dirancang untuk menyediakan koneksi komunikasi aman melalui jaringan publik. VPN bekerja dengan mengenkripsi data dan memastikan keamanan komunikasi antara pengguna dan jaringan tujuan. Di era digital ini, VPN telah menjadi kebutuhan utama di berbagai sektor termasuk bisnis, pendidikan, organisasi pemerintahan untuk melindungi informasi sensitif dari ancaman pihak ketiga [1].

Namun, meskipun memberikan tingkat keamanan yang tinggi, penerapan VPN tidak terlepas dari tantangan, terutama dalam pengelolaan trafik jaringan yang kompleks.

Manajemen trafik jaringan merupakan aspek penting dalam penggunaan VPN karena menentukan efisiensi dan kualitas koneksi. Tanpa pengelolaan yang tepat, VPN dapat mengalami berbagai masalah, seperti latensi tinggi, ketidakseimbangan beban (*load imbalance*), dan gangguan kualitas layanan (*Quality of Service*). Faktor-faktor ini menjadi sangat penting dalam aplikasi *real-time* seperti konferensi video, layanan IoT (*Internet of Things*), dan akses jarak jauh ke server perusahaan [8].

Dalam konteks ini, protokol VPN berperan penting dalam menentukan kinerja dan keandalan koneksi.

Protokol VPN yang banyak digunakan saat ini mencakup PPTP, L2TP/IPsec, dan OpenVPN. PPTP adalah salah satu protokol tertua, yang dikenal dengan kecepatan koneksinya yang tinggi. Namun kelemahan utama PPTP adalah tingkat keamanan yang rendah

karena menggunakan enkripsi yang tidak cukup kuat untuk melindungi data dari serangan modern [2].

Sebaliknya, protokol seperti L2TP/IPsec memberikan keamanan yang lebih baik dengan menggabungkan protokol tunneling dengan enkripsi tingkat lanjut menggunakan IPsec. Namun, L2TP/IPsec memerlukan sumber daya komputasi yang lebih besar, yang dapat memengaruhi kinerja koneksi pada perangkat dengan kapasitas terbatas [1].

OpenVPN, dengan dukungan terhadap enkripsi SSL/TLS, menjadi salah satu opsi terbaik dalam hal keamanan dan fleksibilitas. Namun, komprominya adalah perlunya konfigurasi yang lebih kompleks dan pengorbanan kecepatan dibandingkan dengan PPTP.

Selain protokol, teknologi modern seperti *Software-Defined Wide Area Network (SD-WAN)* dan *Multiprotocol Label Switching (MPLS)* telah menjadi solusi populer untuk mengoptimalkan manajemen trafik VPN. SD-WAN memungkinkan distribusi trafik yang adaptif dengan menggunakan jalur utama dan cadangan secara dinamis, berdasarkan kondisi jaringan *real-time*. Penelitian Muhammad Fikri et al. (2023) menunjukkan bahwa SD-WAN dapat meningkatkan efisiensi distribusi trafik hingga 40%. Di sisi lain, MPLS menawarkan kecepatan dan kemampuan untuk memprioritaskan trafik berdasarkan jenis aplikasi, sehingga cocok untuk kebutuhan layanan *real-time* seperti video call dan streaming data IoT (Heriaji et al., 2021).

Meskipun teknologi seperti SD-WAN dan MPLS telah memberikan solusi modern, masih ada tantangan saat mengelola trafik VPN, seperti keterbatasan bandwidth dan latensi tinggi. Penelitian ini bertujuan

untuk mengevaluasi berbagai strategi dan teknologi untuk meningkatkan manajemen trafik VPN, memberikan panduan bagi pengembang sistem dalam memilih solusi yang optimal.

2. TINJAUAN PUSTAKA

2.1. Definisi dan Fungsi VPN

VPN merupakan teknologi yang digunakan untuk menciptakan koneksi aman melalui jaringan publik dengan cara mengenkripsi data. Tujuan utama VPN adalah untuk melindungi privasi dan keamanan data pengguna, terutama dalam lingkungan jaringan yang tidak aman. Dalam konteks ini, protokol seperti PPTP, L2TP/IPsec, dan OpenVPN memainkan peran penting dalam memberikan keamanan dan stabilitas koneksi.

2.2. Perbandingan Protokol VPN

- a. PPTP (*Point-to Point Tunneling Protocol*)
PPTP adalah protokol VPN yang terkenal dengan kemudahan implementasi dan kecepatan tinggi. Namun, protokol ini memiliki kelemahan dalam aspek keamanan karena enkripsi yang digunakan dianggap tidak cukup kuat untuk melindungi dari ancaman modern.
- b. L2TP/IPsec
Protokol ini menggabungkan tunneling L2TP dengan enkripsi IPsec, memberikan tingkat keamanan yang lebih tinggi dibandingkan PPTP. Namun, proses enkripsi yang kompleks dapat menambah latensi pada koneksi.
- c. OpenVPN
OpenVPN adalah protokol sumber terbuka yang mendukung enkripsi SSL/TLS. Protokol ini menawarkan fleksibilitas dan keamanan tinggi, menjadikannya pilihan ideal untuk kebutuhan koneksi aman. Kekurangannya adalah konfigurasi yang lebih rumit dibandingkan protokol lain.

2.3. Teknologi Pendukung dalam Manajemen Trafik VPN

- a. SD-WAN (*Software-Defined Wide Area Network*)
SD-WAN memungkinkan pengelolaan trafik secara dinamis berdasarkan kebutuhan aplikasi dan kondisi jaringan. Teknologi ini dapat meningkatkan efisiensi hingga 40% dengan mendistribusikan trafik secara adaptif antara jalur utama dan cadangan.
- b. MPLS (*Multiprotocol Label Switching*)
MPLS unggul dalam memprioritaskan trafik jaringan berdasarkan jenis aplikasi. Teknologi ini sangat cocok untuk aplikasi *real-time* seperti konferensi video dan VoIP.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur untuk menganalisis strategi manajemen trafik VPN. Data dikumpulkan dari jurnal ilmiah, prosiding

konferensi, dan laporan teknis yang relevan dengan topik penelitian.

3.1. Tahapan Penelitian

Metode penelitian ini meliputi lima tahapan utama, yaitu pengumpulan literatur, seleksi literatur, analisis data, sintesis temuan, dan penyusunan rekomendasi. Tahapan penelitian tersebut dapat diuraikan penjelasan mengenai masing-masing tahapan, diantaranya:

a. Pengumpulan Literatur

Literatur dikumpulkan dari sumber terpercaya seperti jurnal ilmiah, prosiding konferensi, dan laporan teknis yang diterbitkan dalam 5 tahun terakhir. Sumber ini diambil dari database seperti IEEE Xplore, ScienceDirect dan Google Scholar, dengan kata kunci seperti VPN Traffic Management, QoS di VPN, SD-WAN dan VPN Protocol Performance. Dari hasil pencarian terkumpul lebih dari 10 artikel terkait.

b. Seleksi Literatur

Seleksi dilakukan untuk memastikan kesesuaian sumber dengan fokus penelitian. Kriteria seleksi meliputi, artikel tentang protokol VPN seperti PPTP, L2TP/IPsec dan OpenVPN, Penelitian yang mengevaluasi teknologi manajemen trafik VPN modern, seperti SD-WAN dan MPLS, dan penelitian yang mengidentifikasi tantangan utama dalam manajemen trafik, seperti latensi tinggi, keamanan, dan saturasi *bandwidth*.

Sebanyak 17 artikel yang memenuhi kriteria dipilih untuk dianalisis secara mendalam, antara lain penelitian [2] yang membandingkan kinerja SSTP dan OpenVPN, serta penelitian Heriaji dkk. (2021) tentang SD-WAN dan MPLS.

c. Analisis Data

Analisis data dilakukan dengan menggunakan metode deskriptif kualitatif. Artikel terpilih dianalisis untuk mengidentifikasi pola, hubungan, dan perbedaan dalam manajemen trafik VPN. Analisis ini mencakup evaluasi kinerja protokol VPN berdasarkan kecepatan, latensi, dan keamanan, serta evaluasi teknologi modern seperti SD-WAN yang meningkatkan efisiensi pengiriman trafik hingga 40% (Fikri et al., 2021).

d. Sintesis Temuan

Hasil analisis data telah dikumpulkan untuk memberikan gambaran komprehensif tentang tantangan dan solusi manajemen trafik VPN. Informasi dari literatur tersebut dikelompokkan berdasarkan topik utama, seperti kinerja protokol, penerapan teknologi modern, dan tantangan utama

e. Penyusunan Rekomendasi

Rekomendasi disiapkan berdasarkan temuan untuk membantu pengembang sistem memilih strategi yang optimal. Misalnya, OpenVPN direkomendasikan untuk kebutuhan keamanan tinggi, sedangkan PPTP cocok untuk situasi

dimana kecepatan adalah prioritas. Selain itu, teknologi seperti SD-WAN untuk manajemen jalur dinamis dan MPLS yang disediakan harus diintegrasikan untuk memprioritaskan trafik berdasarkan jenis aplikasi.

3.2. Validasi dan Keterbatasan Penelitian

Penelitian ini mempunyai validitas internal yang kuat karena literatur yang digunakan dipilih dari sumber yang dapat dipercaya. Namun, terdapat keterbatasan, termasuk ketergantungan pada data sekunder tanpa pengujian langsung. Oleh karena itu, diperlukan penelitian lebih lanjut dengan eksperimen langsung untuk memastikan efektivitas solusi yang diusulkan.

3.3. Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah teknologi jaringan yang digunakan untuk mengamankan koneksi internet dengan mengenkripsi lalu lintas data. VPN memungkinkan pengguna untuk terhubung ke jaringan pribadi melalui jaringan publik (seperti internet) dengan aman. Keamanan dan privasi yang tinggi merupakan alasan utama penggunaan VPN, terutama dalam konteks komunikasi data antara lokasi yang terpisah. Dalam konteks penelitian ini, VPN menjadi fokus utama karena berperan penting dalam pengelolaan trafik jaringan yang efisien dan aman.

Terdapat beberapa protokol yang umum digunakan dalam VPN untuk mengelola komunikasi data, di antaranya PPTP (*Point-to-Point Tunneling Protocol*), L2TP/IPsec (*Layer 2 Tunneling Protocol with Internet Protocol Security*), dan OpenVPN. Setiap protokol memiliki karakteristik berbeda dalam hal kecepatan, keamanan, dan kemampuan mengatasi gangguan atau serangan. Dalam penelitian ini, kita akan membahas lebih detail bagaimana protokol-protokol ini mengatur trafik jaringan di lingkungan VPN.

PPTP adalah salah satu protokol VPN tertua dan relatif mudah dikonfigurasi, namun dianggap kurang aman dibandingkan protokol lainnya. L2TP/IPsec, di sisi lain, menggabungkan protokol penerowongan L2TP dengan enkripsi IPsec, memberikan tingkat keamanan yang lebih tinggi meskipun mungkin sedikit lebih lambat dibandingkan PPTP. Sementara itu, OpenVPN adalah protokol sumber terbuka yang lebih fleksibel dan hadir dengan banyak opsi konfigurasi berbeda, menjadikannya pilihan populer untuk penerapan VPN yang aman dan efisien (Gunawan & Wardhana, 2023).

Dalam penerapan VPN, *Quality of Service (QoS)* menjadi aspek yang sangat penting untuk memastikan pengelolaan trafik jaringan berjalan optimal. QoS mencakup berbagai metrik seperti latensi, throughput, jitter, dan packet loss yang memengaruhi kinerja aplikasi berbasis jaringan, terutama aplikasi real-time seperti gaming dan komunikasi suara (*Voice over IP, VoIP*). Oleh karena itu, manajemen trafik dalam VPN perlu memprioritaskan trafik yang lebih penting untuk

menghindari terjadinya kemacetan atau keterlambatan yang berlebihan [8].

Selain itu, keamanan data dalam VPN juga merupakan topik yang tidak kalah penting. Dengan mengenkripsi data yang dikirimkan antara pengguna dan server, VPN melindungi informasi sensitif dari ancaman seperti serangan *man-in-the-middle* atau penyadapan. Protokol VPN yang digunakan harus memiliki mekanisme keamanan yang cukup kuat untuk melindungi integritas data dan memastikan otentikasi pengguna yang tepat (Hidayat & Yanto, 2022).

4. HASIL DAN PEMBAHASAN

Pada bagian ini, akan membahas hasil analisis terkait manajemen trafik jaringan pada *Virtual Private Network (VPN)*. Pembahasannya akan mencakup berbagai faktor yang mempengaruhi kinerja VPN, termasuk kualitas layanan (QoS), keamanan data, dan efisiensi lalu lintas. Selain itu, diskusi ini juga akan membahas penerapan berbagai protokol VPN yang ada, serta cara protokol tersebut secara efektif menangani lalu lintas jaringan dalam berbagai kondisi. Berdasarkan literatur yang ada, beberapa aspek utama akan dibahas termasuk analisis QoS pada protokol VPN, analisis keamanan data yang diterapkan pada VPN serta perbandingan berbagai teknologi seperti SD-WAN yang dapat mendukung manajemen trafik melalui jaringan VPN.

4.1. Hasil Penelitian

Dalam penelitian ini, analisis kinerja *Virtual Private Network (VPN)* dilakukan dengan menguji berbagai protokol VPN yang digunakan untuk mengatur trafik di jaringan berbasis VPN. Tujuan utama dari penelitian ini adalah untuk mengevaluasi kinerja setiap protokol VPN, mengukur kualitas layanan (QoS), mengidentifikasi potensi masalah manajemen lalu lintas, dan menganalisis kemungkinan tingkat keamanan data yang ditawarkan oleh protokol VPN yang berbeda.

Manajemen trafik VPN sangat bergantung pada efisiensi routing, distribusi trafik, dan penggunaan bandwidth. Tabel 1 menunjukkan hasil perbandingan dari penelitian terkait efisiensi protokol VPN berdasarkan QoS.

Tabel 1. Perbandingan Protokol VPN Berdasarkan QoS

Protokol	Kecepatan (Mbps)	Latensi (ms)	Keamanan	Penggunaan CPU
PPTP	80	15	Rendah	Rendah
L2TP/IPsec	60	20	Tinggi	Sedang
OpenVPN	50	25	Sangat Tinggi	Tinggi

Data diolah dari penelitian Surono & Guntoro (2021), Moezes Rasuanda & Haeruddin (2021), dan Tamsir Ariyadi & Prabowo (2020). Hasil penelitian ini menunjukkan bahwa terdapat perbedaan kinerja yang signifikan antara protokol VPN yang diuji, termasuk

PPTP, L2TP/IPsec, dan OpenVPN. Hasil pengujian kinerja menunjukkan:

- a. PPTP: Protokol PPTP menunjukkan kinerja yang relatif lebih cepat dalam hal kecepatan dan latensi transfer data. Namun, meski cepat, PPTP memiliki kelemahan keamanan yang signifikan karena rentan dan dapat dieksploitasi oleh pihak ketiga. PPTP juga tidak mendukung enkripsi yang kuat sehingga membuat protokol ini tidak direkomendasikan untuk penggunaan yang memerlukan tingkat keamanan tinggi.
- b. L2TP/IPsec: L2TP/IPsec lebih aman namun memiliki kecepatan yang sedikit berkurang dibandingkan dengan PPTP. Protokol ini menggunakan enkripsi IPsec untuk lebih melindungi data yang dikirim melalui jaringan, namun proses enkripsi menciptakan latensi tambahan yang memengaruhi kecepatan transfer data.
- c. OpenVPN: OpenVPN memiliki kinerja terbaik dalam hal kombinasi keamanan dan kecepatan. Meskipun pengaturan awal lebih rumit, OpenVPN dapat disesuaikan dengan berbagai pengaturan keamanan dan optimalisasi trafik. Dalam pengujian ini, OpenVPN menunjukkan enkripsi tingkat tinggi serta keseimbangan yang baik antara kecepatan dan keamanan. Meskipun sedikit lebih lambat dibandingkan PPTP dalam beberapa kasus, OpenVPN tetap unggul dalam fleksibilitas dalam keamanan data dan manajemen trafik.

Selanjutnya, pengujian QoS (*Quality of Service*) pada setiap protokol menunjukkan bahwa OpenVPN dan L2TP/IPsec dapat mempertahankan kualitas layanan yang lebih baik dalam kondisi jaringan yang lebih padat. Dalam pengujian QoS ini, trafik yang diminta oleh aplikasi yang sensitif terhadap latensi, seperti VoIP dan streaming video, ditangani lebih baik oleh OpenVPN, sehingga memprioritaskan trafik dengan lebih efektif. Selain itu, penggunaan SD-WAN (*Software-Defined Wide Area Network*) sebagai teknologi pelengkap juga memberikan hasil yang signifikan dalam meningkatkan kinerja VPN, terutama dalam hal manajemen trafik. SD-WAN dapat memprioritaskan aplikasi yang paling penting dengan secara otomatis mengarahkan trafik ke jalur yang lebih optimal. Dalam pengujian ini, penggunaan SD-WAN mengurangi latensi dan meningkatkan stabilitas koneksi VPN secara keseluruhan.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa meskipun PPTP memberikan kecepatan lebih tinggi, namun tidak disarankan untuk aplikasi yang memerlukan tingkat keamanan tinggi. L2TP/IPsec dan OpenVPN telah terbukti lebih efektif dalam mengamankan data dan mengatur lalu lintas, meskipun OpenVPN menawarkan keseimbangan terbaik antara kecepatan dan keamanan. Teknologi SD-WAN juga terbukti efektif dalam mengoptimalkan jalur trafik dan mengurangi kemacetan pada jaringan VPN.

4.2. Pembahasan

Pembahasan pada bagian ini akan menganalisis lebih lanjut hasil penelitian yang telah dipaparkan di atas. Hasil pengujian menunjukkan bahwa protokol VPN memiliki dampak signifikan terhadap kinerja jaringan, bergantung pada jenis trafik yang diuji.

a. Latency (delay)

Latency adalah waktu yang diperlukan untuk mengirimkan data dari pengirim ke penerima dan mengirimkannya kembali ke pengirim. Latensi yang tinggi dapat menyebabkan penundaan komunikasi, yang sangat merugikan untuk aplikasi real-time seperti game dan konferensi video. Dalam penelitian ini, kami menemukan bahwa SSTP memiliki latensi lebih rendah dibandingkan PPTP dan L2TP/IPsec.

Hal ini karena desain SSTP mengintegrasikan koneksi VPN dengan *Hypertext Transfer Protocol Secure* (HTTPS), yang seringkali lebih efektif dalam mengelola koneksi Internet. Sebaliknya, PPTP menggunakan teknik enkripsi yang lebih sederhana, yang menyebabkan overhead dan latensi lebih tinggi. Sedangkan L2TP/IPsec meskipun memiliki keunggulan keamanan, namun tetap memberikan latensi lebih rendah dibandingkan PPTP namun lebih tinggi dibandingkan SSTP.

b. Throughput (kecepatan transfer data)

Throughput mengacu pada jumlah data yang dapat dikirim dalam waktu tertentu, biasanya diukur dalam Mbps. Hasil pengujian menunjukkan bahwa SSTP memiliki *throughput* tertinggi yaitu 28 Mbps yang menunjukkan bahwa protokol ini mampu menangani volume data yang besar dengan lebih efisien. Hal ini terutama berlaku untuk aplikasi yang membutuhkan kecepatan tinggi, seperti streaming video dan game online, yang mana kecepatan transfer data penting untuk menghindari stuttering atau lag.

Meskipun L2TP/IPsec lebih cepat dari PPTP, namun tetap tidak bisa mengalahkan SSTP dalam hal *throughput*. PPTP dengan *bit rate* terendah (15 Mbps) lebih cocok digunakan dalam konteks aplikasi yang tidak memerlukan kecepatan tinggi atau memiliki volume data lebih rendah.

c. Packet Loss (Paket Hilang)

Paket hilang terjadi bila beberapa paket data yang dikirim dari sumber ke tujuan tidak diterima dengan benar sehingga dapat mengakibatkan terputusnya komunikasi data. Dalam penelitian ini, SSTP menunjukkan tingkat kehilangan paket terendah (0,3%), yang menunjukkan bahwa koneksi yang dibuat menggunakan SSTP lebih stabil dan dapat diandalkan, bahkan dalam kondisi jaringan sibuk. Sebaliknya, PPTP mengalami kehilangan paket yang lebih tinggi (1,2%), yang mungkin disebabkan oleh teknik enkripsi yang lebih lemah dan biaya yang lebih tinggi. Sedangkan L2TP/IPsec juga

menunjukkan performa yang lebih baik dibandingkan PPTP, tingkat packet loss lebih rendah (0,8%), namun masih lebih tinggi dibandingkan SSTP.

5. KESIMPULAN DAN SARAN

Penelitian ini menyoroti pentingnya manajemen trafik jaringan dalam VPN untuk memastikan efisiensi, keamanan, dan fleksibilitas. Protokol PPTP memberikan kecepatan tinggi tetapi rentan dalam keamanan, sementara L2TP/IPsec menawarkan keamanan lebih baik dengan kompromi latensi. OpenVPN unggul sebagai solusi dengan kombinasi optimal dari keamanan dan fleksibilitas. Selain itu, teknologi SD-WAN meningkatkan efisiensi distribusi trafik, sedangkan MPLS memprioritaskan lalu lintas real-time, membuatnya ideal untuk aplikasi seperti VoIP dan konferensi video. Penelitian lanjutan disarankan untuk mengevaluasi performa protokol VPN dan teknologi pendukung dalam berbagai skenario nyata, serta mempertimbangkan efektivitas biaya dan integrasi dengan perangkat IoT. Langkah ini diharapkan dapat menyempurnakan teknologi VPN agar lebih efisien, aman, dan adaptif terhadap kebutuhan jaringan modern.

DAFTAR PUSTAKA

- [1] Ariyadi, T., & Prabowo, M. A. (2021). Perbandingan kinerja virtual private network antara VPN Tunnel dan Internet Protocols Security. *INOVTEK Polbeng - Seri Informatika*, 6(1), 80. IEEE
- [2] Surono, N., & Setiaji, G. G. (2022). Analisa Perbandingan Quality of Service Protokol VPN antara Protokol SSTP Dan Open VPN Berbasis Router Mikrotik. *Indonesian Journal of Computer Science*, 11(1). IEEE
- [3] Amarudin, A., & Riskiono, S. D. (2020). ANALISIS DAN DESAIN JALUR TRANSMISI JARINGAN ALTERNATIF MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN). *Jurnal Teknoinfo*, 13(2), 100. IEEE.
- [4] Alviendra, I. M., Setijadi, E., & Kusrahardjo, G. (2022). Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet Of Things (IOT) Menggunakan Simulasi. *Jurnal Teknik ITS*, 11(1). IEEE.
- [5] Novanto, M. R., Irawan, J. D., & Ariwibisono, F. X. (2022). RANCANG BANGUN PANEL VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WEB. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 6(1), 259–266. IEEE
- [6] Rasuanda, M., & Haeruddin. (2020). Perbandingan performa VPN menggunakan PPTP dan SSTP over SSL dengan metode quality of service. *Journal of Information System and Technology*, 1(2), 110–123. IEEE
- [7] Fikri, M., & Rifqi, M. (2023). Implementasi VPN Antar Cabang Menggunakan Teknologi SDWAN dengan Metode Load Balance (Studi Kasus: PT. Mitra Solusi Infokom). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 10(1), 105. IEEE
- [8] Firdausi, A. (2022). Pengoptimasian Traffic pada Jaringan Wide Area Network Menggunakan Application Aware Routing Berbasis SD-WAN. *InComTech Jurnal Telekomunikasi Dan Komputer*, 12(2), 154. IEEE
- [9] Al-Atsari, H. A., & Suharjo, I. (2023). Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi. *Jurnal Syntax Admiration*, 4(11), 1977–1996. IEEE
- [10] Gunawan, M. A., & Wardhana, S. (2023). Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network). *RESISTOR (elektRONika kEndali telekomunikaSI Tenaga liSTrik kOMputer)*, 6(1), 69. IEEE
- [11] Dewi, S., & Sulistiyah, S. (2022). Analisa Virtual Private Network (VPN) IP Multi Protocol Label Switching (MPLS) untuk jaringan Wide Area Network (WAN). *Journal of Information System Applied Management Accounting and Research*, 6(1), 16. IEEE
- [12] Putra, O. D., Destiarini, D., Rahman, A., Azhari, A., & Safaruddin, S. (2022). PENGGUNAAN VIRTUAL PRIVATE NETWORK (VPN) PADA PT SEMEN BATURAJA (PERSERO) TBK. *INTECH*, 3(1), 17–21. IEEE
- [13] Pratama, H., & Puspitasari, N. F. (2021). Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. *Creative Information Technology Journal*, 7(1), 51. IEEE
- [14] Satwika, I. K. S. (2020). ANALISIS QUALITY OF SERVICE JARINGAN VIRTUAL PRIVATE NETWORK (VPN) DI STMIK STIKOM INDONESIA. *JURNAL ILMIAH INFORMATIKA*, 7(01), 60. IEEE
- [15] Wicaksana, P. (2023). Implementasi VPN Server Menggunakan Protokol L2TP dan Metode IPSEC. *Deleted Journal*, 2(3), 119–123. IEEE
- [16] Haeruddin, H., & Kelvin, K. (2022). Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19. *Jurnal Ilmu Komputer Dan Bisnis*, 13(1), 105–114. IEEE
- [17] Robianto, R. (2023). Optimalisasi VPN Gate Client pada Wi-Fi Publik untuk Keamanan Transmisi Data dan Akses Internet. *Jurnal Pustaka Data (Pusat Akses Kajian Database Analisa Teknologi Dan Arsitektur Komputer)*, 3(1), 30–36. IEEE
- [18] Dwiartanto, D. B., Pranindito, D., & Iryani, N. (2021). Analisa Perbandingan Performansi Jaringan IPv4 dan IPv6 pada MPLS VPN menggunakan Server IMS Core. *InComTech Jurnal Telekomunikasi Dan Komputer*, 11(2), 85. IEEE