Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik

Fauzan Prasetyo Eka Putra[1], M. Khofikur R.A[2*], Moh. Wahid Ridho G[3], Valentino Huda[4]
[1,2,3,4] Program Studi Teknik Informatika, Universitas Madura
*khofipunya316@gmail.com

Abstrak

Virtual Private Network (VPN) telah menjadi solusi kritis untuk memastikan komunikasi yang aman melalui jaringan publik. Penelitian ini melakukan analisis komprehensif terhadap kinerja dan keamanan dua protokol VPN utama: Point-to-Point Tunneling Protocol (PPTP) dan Layer 2 Tunneling Protocol dengan Internet Protocol Security (L2TP/IPSec) yang diimplementasikan pada perangkat MikroTik. Metodologi penelitian menggunakan pendekatan eksperimental dengan menguji throughput, latency, packet loss, dan CPU utilization pada berbagai skenario jaringan. Hasil penelitian menunjukkan bahwa PPTP memberikan throughput yang lebih tinggi dengan overhead yang minimal, namun memiliki kelemahan signifikan dalam aspek keamanan. Sebaliknya, L2TP/IPSec menawarkan tingkat keamanan yang superior dengan enkripsi yang kuat, meskipun menghasilkan latency yang lebih tinggi dan throughput yang lebih rendah. Temuan ini memberikan wawasan penting bagi administrator jaringan dalam memilih protokol VPN yang sesuai dengan kebutuhan organisasi, dengan mempertimbangkan trade-off antara kinerja dan keamanan.

Kata kunci : L2TP/IPSec, MikroTik, PPTP, Quality of Service, VPN Security

Abstract

Virtual Private Network (VPN) has become a critical solution for ensuring secure communication over public networks. This research conducts a comprehensive analysis of the performance and security of two major VPN protocols: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol with Internet Protocol Security (L2TP/IPSec) implemented on MikroTik devices. The research methodology uses an experimental approach by testing throughput, latency, packet loss, and CPU utilization in various network scenarios. The results show that PPTP provides higher throughput with minimal overhead, but has significant weaknesses in security aspects. Conversely, L2TP/IPSec offers superior security levels with strong encryption, although it results in higher latency and lower throughput. These findings provide important insights for network administrators in choosing VPN protocols that suit organizational needs, considering the trade-off between performance and security.

Keywords : *L2TP/IPSec, MikroTik, PPTP, Quality of Service, VPN Security.*

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mengubah cara organisasi mengelola infrastruktur jaringan mereka. Dalam era digital yang semakin terhubung, kebutuhan akan akses jarak jauh yang aman dan reliable menjadi sangat krusial. Virtual Private Network (VPN) telah menjadi solusi standar industri untuk memfasilitasi koneksi aman melalui jaringan publik, memungkinkan pengguna untuk mengakses sumber daya internal organisasi dari lokasi yang berbeda dengan tingkat keamanan yang tinggi.

Menurut penelitian terbaru, implementasi VPN telah mengalami peningkatan signifikan, terutama dalam konteks remote working dan digitalisasi proses bisnis. Namun, pemilihan protokol VPN yang tepat masih menjadi

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

tantangan bagi banyak organisasi, mengingat setiap protokol memiliki karakteristik kinerja dan keamanan yang berbeda. Dua protokol yang paling umum digunakan adalah Point-to-Point Tunneling Protocol (PPTP) dan Layer 2 Tunneling Protocol dengan Internet Protocol Security (L2TP/IPSec).

Studi sebelumnya telah mengidentifikasi berbagai aspek teknis dari implementasi VPN, namun masih terdapat gap dalam analisis komprehensif yang membandingkan kinerja dan keamanan protokol VPN pada platform MikroTik. Penelitian yang dilakukan oleh Sari dan Helena menunjukkan bahwa implementasi L2TP pada MikroTik dapat memberikan keamanan yang memadai untuk jaringan enterprise, namun belum mengeksplorasi aspek kinerja secara mendalam[3]. Sementara itu, analisis oleh Budiyanto dan Gunawan fokus pada perbandingan protokol VPN dalam konteks Voice over Internet Protocol, yang memiliki karakteristik traffic yang spesifik[11].

Kebaruan penelitian ini terletak pada pendekatan analisis komprehensif yang mengintegrasikan aspek kinerja dan keamanan dalam satu framework evaluasi. Penelitian ini menggunakan metodologi pengujian yang sistematis dengan berbagai skenario jaringan untuk memberikan pemahaman yang lebih mendalam tentang trade-off antara kinerja dan keamanan. Selain itu, implementasi pada platform MikroTik memberikan nilai praktis yang tinggi mengingat popularitas perangkat tersebut di kalangan enterprise dan service provider.

Fokus penelitian ini adalah melakukan evaluasi komprehensif terhadap kinerja dan keamanan protokol PPTP dan L2TP/IPSec pada jaringan MikroTik, dengan tujuan memberikan panduan praktis bagi administrator jaringan dalam memilih protokol VPN yang optimal sesuai dengan kebutuhan organisasi mereka

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Beberapa penelitian terdahulu telah mengeksplorasi aspek - aspek implementasi VPN dalam berbagai konteks diantaranya antara lain :

- Penelitian oleh Fitrian et al. melakukan analisis manajemen traffic jaringan pada VPN menggunakan protokol PPTP, L2TP/IPSec, dan OpenVPN, namun fokus utama mereka adalah pada aspek manajemen traffic tanpa analisis keamanan yang mendalam[1].
- Yaqoob et al. mengembangkan sistem deteksi anomali berbasis deep learning untuk jaringan IoVs yang menggunakan fog-assisted architecture, memberikan perspektif keamanan dari sudut pandang machine learning[2].
- Studi yang dilakukan oleh Kim et al.

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

mengembangkan framework systematic security guideline melalui analisis kerentanan otomatis yang dapat diterapkan dalam konteks VPN security assessment[4].

- Penelitian oleh Chen menggunakan improved RBF neural network algorithm untuk prediksi situational awareness dalam konteks internet security[6]. Penelitian - penelitian ini memberikan foundation teoritis yang kuat untuk pengembangan metodologi keamanan dalam implementasi VPN. Dalam konteks implementasi praktis.
- Penelitian oleh Gunawan dan Wardhana melakukan perbandingan keamanan antara PPTP dan L2TP/IPSec VPN, namun terbatas pada aspek implementasi tanpa analisis kinerja yang komprehensif[[18].
- Arianti, Jamaluddin, dan Kuswanto menggunakan topologi Mesh - Wireless pada RT - RW Net untuk meningkatkan pemahaman administrasi sistem jaringan siswa, memberikan perspektif pedagogis dalam pembelajaran jaringan komputer melalui praktik langsung dengan teknologi Mikrotik dan Winbox[19].
- Penelitian terbaru oleh Oktavia et al. melakukan analisis komparatif Quality of Service protokol VPN pada IPv6, menunjukkan pentingnya evaluasi kinerja dalam implementasi modern[44].
- Rahman et al. mengimplementasikan VPN pada VPS server menggunakan OpenVPN dan Raspberry Pi, memberikan perspektif implementasi pada low-cost hardware[22]. Park et al. mengembangkan enhanced AI-based network intrusion detection system menggunakan generative adversarial networks untuk meningkatkan keamanan jaringan VPN[21].

2.2. Landasan Teori

1. Virtual Private Network (VPN)

VPN merupakan teknologi yang menciptakan koneksi aman dan terenkripsi antara dua atau lebih perangkat melalui jaringan publik. VPN bekerja dengan membuat tunnel virtual yang mengenkapsulasi data dan menyediakan mekanisme autentikasi serta enkripsi untuk melindungi integritas dan confidentiality data yang ditransmisikan. Implementasi sistem monitoring jaringan VPN memerlukan pendekatan yang komprehensif untuk memastikan kontinuitas layanan yang optimal[35].

2. Point-to-Point Tunneling Protocol (PPTP)

PPTP merupakan salah satu protokol VPN tertua yang dikembangkan oleh Microsoft. PPTP bekerja pada layer 2 model OSI dan menggunakan port TCP 1723 untuk establishing control connection serta Generic Routing Encapsulation (GRE) untuk data transmission. Meskipun PPTP menawarkan kemudahan konfigurasi dan overhead yang minimal, protokol

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

ini memiliki kelemahan keamanan yang signifikan karena menggunakan enkripsi Microsoft Point-to-Point Encryption (MPPE) yang relatif lemah[41]. Layer 2 Tunneling Protocol (L2TP) dikombinasikan dengan Internet Protocol Security (IPSec) memberikan solusi VPN yang lebih aman. L2TP berfungsi sebagai tunneling protocol yang bekerja pada layer 2, sementara IPSec menyediakan enkripsi dan autentikasi yang kuat. Kombinasi ini menghasilkan overhead yang lebih besar dibandingkan PPTP, namun menawarkan tingkat keamanan yang superior dengan dukungan berbagai algoritma enkripsi seperti AES dan 3DES [23], [26].

3. MikroTik RouterOS

Mikrotik Router OS merupakan sistem operasi berbasis Linux yang dirancang khusus untuk perangkat networking. Platform ini menyediakan implementasi lengkap berbagai protokol VPN termasuk PPTP dan L2TP/IPSec dengan konfigurasi yang fleksibel dan monitoring yang komprehensif [39].

2.3. Tahapan Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan tahapan yang sistematis. Pertama, dilakukan setup laboratorium dengan konfigurasi jaringan yang terdiri dari MikroTik RouterBoard sebagai VPN server, client devices, dan network monitoring tools. Kedua, implementasi dan konfigurasi protokol PPTP dan L2TP/IPSec pada perangkat MikroTik dengan parameter yang konsisten. Ketiga, pelaksanaan pengujian kinerja menggunakan berbagai tools seperti iperf3 untuk throughput testing, ping untuk latency measurement, dan SNMP monitoring untuk resource utilization. Keempat, analisis keamanan menggunakan penetration testing tools dan vulnerability assessment[30]. Kelima, pengumpulan dan analisis data menggunakan statistical analysis untuk memvalidasi hasil pengujian.

3. Metode Penelitian

3.1. Desain Penelitian

Penelitian ini menggunakan desain eksperimental komparatif dengan pendekatan kuantitatif untuk menganalisis kinerja dan keamanan protokol PPTP dan L2TP/IPSec pada jaringan MikroTik. Desain ini dipilih karena memungkinkan peneliti untuk melakukan kontrol yang ketat terhadap variabel-variabel yang diuji dan memberikan hasil yang objektif serta dapat direplikasi.

3.1 Prosedur Penelitian

Prosedur penelitian dimulai dengan persiapan infrastruktur laboratorium yang terdiri dari MikroTik RouterBoard RB4011iGS + RM sebagai VPN server, dua unit komputer sebagai VPN client, dan satu unit komputer sebagai network monitoring station. Selanjutnya, dilakukan konfigurasi baseline jaringan dengan pengaturan

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

IP addressing, routing protocol, dan firewall rules yang konsisten untuk kedua protokol VPN. Tahap berikutnya adalah implementasi dan konfigurasi protokol VPN. Untuk PPTP, konfigurasi meliputi pengaturan PPP profile, PPTP server settings, dan user authentication [49]. Untuk L2TP/IPSec, konfigurasi mencakup L2TP server settings, IPSec policies, encryption algorithms, dan authentication methods[38]. Setiap konfigurasi didokumentasikan secara detail untuk memastikan reproducibility.

3.2 Populasi dan Sampel

Populasi penelitian ini adalah semua implementasi protokol VPN pada perangkat MikroTik dalam environment enterprise. Sampel penelitian terdiri dari dua protokol VPN utama (PPTP dan L2TP/IPSec) yang diimplementasikan pada MikroTik RouterOS versi 7.1.5. Pemilihan sampel ini didasarkan pada popularitas dan adoption rate protokol tersebut dalam implementasi real-world [42].

3.3 Instrumen Penelitian

Instrumen penelitian yang digunakan meliputi software tools untuk performance testing seperti iperf3 untuk throughput measurement, ping dan traceroute untuk latency testing, Wireshark untuk packet analysis, dan PRTG Network Monitor untuk continuous monitoring. Untuk security assessment, digunakan tools seperti Nmap untuk port scanning, Metasploit framework untuk penetration testing, dan OpenVAS untuk vulnerability scanning [46].

3.4 Teknik Pengumpulan Data

Data dikumpulkan melalui automated testing scripts yang menjalankan series of tests dengan durasi pengujian 24 jam untuk setiap protokol. Parameter yang diukur meliputi throughput (Mbps), latency (ms), packet loss (%), jitter (ms), CPU utilization (%), memory usage (%), dan connection establishment time (s). Setiap test scenario diulang sebanyak 10 kali untuk memastikan validitas statistik [31].

3.5 Teknik Analisis Data

Analisis data menggunakan statistical analysis dengan descriptive statistics untuk merangkum hasil pengujian, comparative analysis menggunakan independent t-test untuk membandingkan performa kedua protokol, dan correlation analysis untuk mengidentifikasi hubungan antar variabel. Software yang digunakan untuk analisis data adalah SPSS versi 28 dan Microsoft Excel dengan Analysis ToolPak.

3.6 Lokasi Penelitian

Penelitian dilaksanakan di Laboratorium Jaringan Komputer Program Studi Teknik Informatika Universitas Madura, dengan infrastruktur jaringan

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

yang terisolasi untuk memastikan validitas hasil pengujian tanpa interferensi dari traffic eksternal

4. Hasil dan Pembahasan

4.1. Analisis Kinerja Protokol VPN

Hasil pengujian kinerja menunjukkan perbedaan yang signifikan antara protokol PPTP dan L2TP/IPSec dalam berbagai aspek. Pengujian throughput menggunakan iperf3 dengan duration 300 detik menunjukkan bahwa PPTP mampu mencapai throughput rata-rata 847.3 Mbps, sementara L2TP/IPSec mencapai 621.7 Mbps pada koneksi 1 Gbps. Perbedaan ini disebabkan oleh overhead enkripsi yang lebih besar pada L2TP/IPSec dibandingkan dengan MPPE encryption yang digunakan oleh PPTP [15].

Tabel 1. Perbandingan Kinerja Protokol VPN

Parameter	PPTP	L2TP/IPSec	Selisih (%)
Throughput (Mbps)	847.3	621.7	26.6
Latency (ms)	3.42	5.78	69.0
Packet Loss (%)	0.12	0.08	-33.3
CPU Usage (%)	23.5	41.2	75.3

Analisis latency menunjukkan bahwa PPTP memiliki rata-rata latency 3.42 ms, sedangkan L2TP/IPSec memiliki latency 5.78 ms. Peningkatan latency pada L2TP/IPSec disebabkan oleh proses enkripsi dan dekripsi yang lebih kompleks, serta overhead dari dual encapsulation (L2TP dan IPSec) [20]. Namun, dari segi packet loss, L2TP/IPSec menunjukkan performa yang sedikit lebih baik dengan tingkat packet loss 0.08% dibandingkan PPTP yang mencapai 0.12%.

Penggunaan CPU menunjukkan perbedaan yang dramatis, dimana L2TP/IPSec mengkonsumsi CPU hingga 41.2% dibandingkan PPTP yang hanya 23.5%. Hal ini mengindikasikan bahwa implementasi L2TP/IPSec memerlukan resource komputasi yang lebih besar, yang perlu dipertimbangkan dalam capacity planning untuk deployment skala besar [14].

4.2. Analisis Keamanan Protokol VPN

Evaluasi keamanan dilakukan menggunakan multiple approach termasuk vulnerability assessment, penetration testing, dan cryptographic analysis. Hasil assessment menunjukkan bahwa PPTP memiliki beberapa kerentanan kritikal yang telah diidentifikasi oleh security community, termasuk weaknesses dalam MS-CHAP authentication dan MPPE encryption [37]. Testing menggunakan dictionary attack terhadap PPTP authentication berhasil dilakukan dalam waktu rata-rata 4.7 jam menggunakan wordlist standar, sementara L2TP/IPSec dengan pre-shared key yang kuat tidak dapat dipenetrate dalam testing period 72 jam. Hal ini menunjukkan superioritas L2TP/IPSec dalam aspek authentication security [32].

Analisis encryption strength menunjukkan bahwa

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

PPTP menggunakan RC4 cipher dengan key length maksimal 128-bit, yang saat ini dianggap tidak memadai untuk high-security environment. Sebaliknya, L2TP/IPSec mendukung AES encryption dengan key length hingga 256-bit, yang masih dianggap cryptographically secure untuk jangka waktu yang panjang [17].

Pengujian resistance terhadap man-in-the-middle attack menunjukkan bahwa PPTP vulnerable terhadap serangan ini karena lemahnya authentication mechanism dan absence of certificate-based verification. L2TP/IPSec dengan proper certificate configuration menunjukkan resistance yang tinggi terhadap MITM attacks [50].

4.3. Perbandingan Trade-off Kinerja vs Keamanan

Analisis komprehensif menunjukkan adanya clear trade-off antara kinerja dan keamanan. PPTP menawarkan kinerja yang superior dengan throughput tinggi dan latency rendah, namun dengan significant security compromises. L2TP/IPSec memberikan security yang robust namun dengan cost berupa reduced performance dan increased resource consumption [29]. Untuk environment yang mengutamakan kinerja dan tidak menangani sensitive data, PPTP masih dapat dipertimbangkan dengan additional security measures seperti network-level protection dan strict access control [40]. Namun, untuk enterprise environment yang menangani confidential data, L2TP/IPSec menjadi pilihan yang lebih appropriate meskipun memerlukan additional infrastructure investment [13].

Result menunjukkan bahwa pemilihan protokol VPN harus didasarkan pada comprehensive risk assessment yang mempertimbangkan nature of data yang ditransmisikan, compliance requirements, available bandwidth, dan hardware capabilities[48]. Implementasi hybrid approach dengan multiple VPN protocols untuk different use cases juga dapat menjadi strategi yang optimal [47].

5. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa terdapat perbedaan signifikan dalam kinerja dan keamanan antara protokol PPTP dan L2TP/IPSec pada implementasi MikroTik. PPTP menunjukkan keunggulan dalam aspek kinerja dengan throughput yang lebih tinggi (847.3 Mbps vs 621.7 Mbps), latency yang lebih rendah (3.42 ms vs 5.78 ms), dan penggunaan CPU yang lebih efisien (23.5% vs 41.2%). Namun, dari aspek keamanan, PPTP memiliki kerentanan yang signifikan terhadap berbagai jenis serangan siber, termasuk dictionary attack dan man-in-the-middle attack.

Sebaliknya, L2TP/IPSec menawarkan tingkat keamanan yang superior dengan enkripsi AES hingga 256-bit dan resistance yang tinggi terhadap berbagai attack vectors, meskipun

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

memerlukan resource komputasi yang lebih besar dan menghasilkan throughput yang lebih rendah. Trade-off ini mengindikasikan bahwa pemilihan protokol VPN harus didasarkan pada analisis kebutuhan spesifik organisasi, dengan mempertimbangkan sensitivitas data, compliance requirements, dan available resources.

Kontribusi penelitian ini adalah memberikan framework evaluasi komprehensif untuk pemilihan protokol VPN dan quantitative comparison yang dapat digunakan sebagai reference untuk decision making. Keterbatasan penelitian meliputi scope testing yang terbatas pada dua protokol VPN dan single vendor platform, serta duration testing yang relatif terbatas. Penelitian future dapat diperluas dengan mengincludkan protokol VPN lainnya seperti OpenVPN dan WireGuard, serta testing dalam multi-vendor environment untuk generalizability yang lebih luas.

6. Daftar Pustaka

[1] H. P. Fitrian, A. A. Nurani, I. Mulhakim, N. Maesaroh, and P. Raharja, "Analisis Manajemen Trafik Jaringan pada Virtual Private Network (VPN) Menggunakan Protokol PPTP, L2TP/IPSec, dan OpenVPN," 2025.

[2] S. Yaqoob, A. Hussain, F. Subhan, G. Pappalardo, and M. Awais, "Deep Learning Based Anomaly Detection for Fog-Assisted IoVs Network," *IEEE Access*, vol. 11, pp. 19024–19038, 2023, doi: 10.1109/ACCESS.2023.3246660.

[3] [3] L. O. Sari and H. Helena, "Implementasi Virtual Private Network Menggunakan Layer 2 Tunneling Protocol Berbasis Mikrotik," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 4, pp. 1496–1504, Sep. 2024, doi: 10.57152/malcom.v4i4.1651.

[4] D. Kim, N. Kim, and J. Ahn, "Systematic Security Guideline Framework through Intelligently Automated Vulnerability Analysis," *Computers, Materials and Continua*, vol. 78, no. 3, pp. 3867–3889, 2024, doi: 10.32604/cmc.2024.046871.

[5] J. Deep Q-Learning, H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection," 2022, doi: 10.3390/computers.

[6] Z. Chen, "Research on Internet Security Situation Awareness Prediction Technology Based on Improved RBF Neural Network Algorithm," *Journal of Computational and Cognitive Engineering*, vol. 1, no. 3, pp. 103–108, Aug. 2022, doi: 10.47852/bonviewJCCE149145205514.

[7] A. Fatani, A. Dahou, M. A. A. Al-Qaness, S. Lu, and M. A. Elaziz, "Advanced Feature Extraction and Selection Approach Using Deep Learning and Aquila Optimizer for IoT Intrusion Detection System," *Sensors*, vol. 22, no. 1, Jan. 2022, doi: 10.3390/s22010140.

[8] A. Ali et al., "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020572.

[9] A. Esmaeily and K. Kralevska, "Orchestrating Isolated Network Slices in 5G Networks," *Electronics*, vol. 13, no. 8, Apr. 2024, doi: 10.3390/electronics13081548.

[10] A. K. Balyan et al., "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method,"

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

Sensors, vol. 22, no. 16, Aug. 2022, doi: 10.3390/s22165986.

[11] S. Budiyanto and D. Gunawan, "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol," *IEEE Access*, vol. 11, pp. 60853–60865, 2023, doi: 10.1109/ACCESS.2023.3286032.

[12] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks - Current Research Solutions," *IEEE Access*, vol. 12, pp. 17982–18011, 2024, doi: 10.1109/ACCESS.2024.3360868.

[13] P. Krishnan, K. Jain, A. Aldweesh, P. Prabu, and R. Buyya, "OpenStackDP: A Scalable Network Security Framework for SDN-based OpenStack Cloud Infrastructure," *Journal of Cloud Computing*, vol. 12, no. 1, Dec. 2023, doi: 10.1186/s13677-023-00406-w.

[14] C. Fu et al., "A Generic High-Performance Architecture for VPN Gateways," *Electronics*, vol. 13, no. 11, Jun. 2024, doi: 10.3390/electronics13112031.

[15] D. Setya Aji, F. Wahyu Christanto, J. Arteri Soekarno-Hatta Tlogosari, K. Semarang, and J. Tengah, "Analisis dan Perbandingan QoS Jaringan Internet dengan Metode PPPoE, PPTP, dan L2TP pada Implementasi Hotspot RT/RW Net," 2023.

[16] D. Soldani et al., "E-BPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond)," *IEEE Access*, vol. 11, pp. 57174–57202, 2023, doi: 10.1109/ACCESS.2023.3281480.

[17] F. Hauser, M. Haberle, and M. Menth, "P4sec: Automated Deployment of 802.1X, IPsec, and MACsec Network Protection in P4-Based SDN," *IEEE Access*, vol. 11, pp. 56300–56309, 2023, doi: 10.1109/ACCESS.2023.3283428.

[18] M. A. Gunawan and S. Wardhana, "Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network)," vol. 6, no. 1.

[19] B. D. D. Arianti, Jamaluddin, and H. Kuswanto, "Analisis penerapan RT-RW Net menggunakan Topologi Mesh-Wireless untuk meningkatkan pemahaman Administrasi Sistem Jaringan Siswa," Infotek : Jurnal Informatika dan Teknologi, vol. 7, no. 1, pp. 236-245, Jan. 2024, doi: 10.29408/jit.v7i1.24809.

[20] P. Bidang, K. Sains, P. Informatika, and A. Maulana, "Analisa Performa Interkoneksi VPN Menggunakan Metode L2TPv3," *Jurnal Edik Informatika*, vol. 10, no. 2, 2024, doi: 10.22202/ei.2024.v10i2.7538.

[21] C. Park, J. Lee, Y. Kim, J. G. Park, H. Kim, and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2330–2345, Feb. 2023, doi: 10.1109/JIOT.2022.3211346.

[22] T. Rahman, G. M. V. T. Mariatmojo, H. Nurdin, and H. Kuswanto, "Implementasi VPN Pada VPS Server Menggunakan OpenVPN dan Raspberry Pi," *Teknika*, vol. 11, no. 2, pp. 138–147, Jul. 2022, doi: 10.34148/teknika.v11i2.482.

[23] D. Zaldiyanto and I. Rofni Wulandari, "Implementasi VPN Menggunakan Protokol L2TP untuk Pengelolaan NAS (Network Attached Storage) pada STB," *Bulletin of Information Technology*, vol. 5, no. 4, pp. 387–395, 2024, doi: 10.47065/bit.v5i2.1770.

[24] L. O. Sari, E. Safrianti, and D. Wahyuningtias, "Analisis Keamanan Jaringan Berbasis Point to Point Protocol Over Ethernet (PPPoE) Menggunakan Mikrotik," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 3, pp. 943–954, May 2024, doi: 10.57152/malcom.v4i3.1301.

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

[25] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session Management for Security Systems in 5G Standalone Network," *IEEE Access*, vol. 10, pp. 73421–73436, 2022, doi: 10.1109/ACCESS.2022.3187053.

[26] L. M. Silalahi et al., "Application of MPLS Tunnel Services L2TP-VPN Optimization Concept with Traffic Engineering Method for Looping-Protection Services Analysis," *International Journal of Electronics and Telecommunications*, vol. 69, no. 1, pp. 115–120, 2023, doi: 10.24425/ijet.2023.144339.

[27] X. J. Li, M. Ma, and Y. Sun, "An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids," *Algorithms*, vol. 16, no. 6, Jun. 2023, doi: 10.3390/a16060288.

[28] R. Elsya Putra et al., "Nomor 2," *Agustus*, vol. 22, pp. 340–347, 2023. [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jis/index

[29] A. F. Gentile, D. Macrì, F. De Rango, M. Tropea, and E. Greco, "A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment," *Future Internet*, vol. 14, no. 9, Sep. 2022, doi: 10.3390/fi14090264.

[30] G. Jekateryńczuk, D. Jankowski, R. Veyland, and Z. Piotrowski, "Detecting Malicious Devices in IPsec Traffic with IPv4 Steganography," *Applied Sciences*, vol. 14, no. 9, May 2024, doi: 10.3390/app14093934.

[31] E. P. Saputra, A. Saryoko, M. Maulidah, N. Hidayati, and S. Dalis, "Analisis Quality of Service (QoS) Performa Jaringan Internet Wireless LAN PT. Bhineka Swadaya Pertama," *Jurnal Sains dan Manajemen*, vol. 11, no. 1, 2023.

[32] S. W. Nourildean, "Virtual Private Network Firewall Integration for Wireless Local Area Network Improvement against Jammers," *International Journal of Electrical and Electronic Engineering and Telecommunications*, vol. 13, no. 1, pp. 58–66, 2024, doi: 10.18178/ijeetc.13.1.58-66.

[33] E. Elkana, D. Djoko, and A. Widodo, "Application of VPN Based on L2TP untuk Mengakses e-Rapor di SMKN 5 Semarang." [Online]. Available: https://elektroda.uho.ac.id/

[34] Z. Sui, H. Shu, F. Kang, Y. Huang, and G. Huo, "A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches," *Applied Sciences*, vol. 13, no. 3, Feb. 2023, doi: 10.3390/app13031974.

[35] M. Wahyu, A. S. Fitrani, and Hindarto, "Penerapan Bot Telegram untuk Sistem Monitoring Jaringan Intranet Daerah di Instansi Pemerintahan," Infotek : Jurnal Informatika dan Teknologi, vol. 7, no. 1, pp. 112-122, Januari 2024, doi: 10.29408/jit.v7i1.24014.

[36] T. Kemendikbud, A. Dwi Prameswari, and R. D. Marcus, "Peningkatan Keamanan Jaringan Virtual Private Network Menggunakan Protokol IKE/IPSec Berbasis Mikrotik," *J-INTECH (Journal of Information and Technology)*.

[37] D. N. Amadi, A. Budiman, and P. Utomo, "Analysis of the Effectiveness of VPN and PPTP Protocol in E-Link Health Report Application Using NDLC Method," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 949–958, Jun. 2024, doi: 10.51519/journalisi.v6i2.746.

[38] I. K. Rahman and L. N. Harnaningrum, "Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk Mengamankan VoIP." [Online]. Available: https://s.id/jurnalresistor

[39] M. Munaza Fathsyah et al., "Implementasi Virtual Private Network Failover Menggunakan Mikrotik Pada Jaringan

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 334-344

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30230 Link : https://dx.doi.org/10.29408/jit.v8i2.30230

Lokal Politeknik Negeri Sriwijaya," *Jurnal Teknik Komputer AMIK BSI*, vol. 7, no. 2, 2021, doi: 10.31294/jtk.v4i2.

[40] Y. N. Sari, D. Irfan, and A. Huda, "Network Security Analysis Using Virtual Private Network in Vocational School," *Jurnal Paedagogy*, vol. 9, no. 3, p. 582, Jul. 2022, doi: 10.33394/jp.v9i3.5346.

[41] R. Febrianti, E. Rikardo Nainggolan, U. Radiyah, T. Informatika, and S. Tinggi Manajemen Informatika dan Komputer Nusa Mandiri, "Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board." [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/infortech46

[42] Ubaidi and N. Puspa Dewi, "Analisis dan Implementasi VPN pada VPS untuk Peningkatan Aksesibilitas Jaringan di Lingkungan Perguruan Tinggi," *Jurnal Informasi dan Teknologi*, pp. 131–140, Nov. 2023, doi: 10.60083/jidt.v5i3.409.

[43] R. D. Gulo and M. Raharjo, "Implementasi Jaringan VPN PPTP Menggunakan IP Publik VPS Untuk Web Server Pada SMK Yadika 2," *Media Jurnal Informatika*, vol. 15, no. 2, p. 117, Dec. 2023, doi: 10.35194/mji.v15i2.3388.

[44] S. T. Oktavia, D. F. Priambodo, N. Trianto, and R. Purwoko, "Comparative Quality of Service Analysis of VPN Protocols on IPv6," *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, vol. 12, no. 3, pp. 461–471, Jan. 2024, doi: 10.23887/janapati.v12i3.69264.

[45] R. Elsya Putra et al., "Nomor 2," *Agustus*, vol. 22, pp. 340–347, 2023. [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jis/index

[46] F. P. E. Putra, Ubaidi, S. A. A. Sugi, K. Mufidah, and Y. R. Febriani, "Analysis of Cyber Attacks on Network Security," *Jurnal Informasi dan Teknologi*, vol. 6, no. 2, pp. 204–208, 2024, doi: 10.60083/jidt.v6i2.569.

[47] E. Suhadi and T. Arifin, "Rancangan Virtual Private Network Pada Kantor Prolov Menggunakan ZeroTier," *JIKA (Jurnal Informatika)*, vol. 8, no. 1, p. 66, Jan. 2024, doi: 10.31000/jika.v8i1.9979.

[48] I. W. Yudik Pradnyana, K. Y. E. Aryanto, and I. G. Aris Gunadi, "Desain Data Center Perbankan dengan Metode Network Development Life Cycle (NDLC) (Studi Kasus PT. BPR XYZ)," *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 21, no. 2, 2024.

[49] L. Oktaviana Sari, T. Dwi Kharisma, K. H. Binawidya Jl Sobrantas KM, and S. Baru, "Implementation of VPN Using the PPTP Method to Access CCTV Monitoring Data at the Bukit Raya District Office," vol. 9, no. 2, p. 2024.

[50] Z. Gao, F. Chen, Y. Wang, W. He, X. Shi, and G. Xie, "MVPN: A Defense Architecture against VPN Traffic Hijacking Based on MTD," *Electronics*, vol. 12, no. 3, Feb. 2023, doi: 10.3390/electronics12030711..