CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 2, November 2025, hlm. 107-113

Perbandingan Keamanan Dan Performa Protokol Vmess, Vless, Trojan, Dan Wireguard Pada Passwall Berbasis Openwrt

Fajar Siddik[1], Aulia Syarif Aziz[2]

[1]Program Studi Pendidikan Teknologi Informasi, Fakultas Tarbiyah dan Keguruan, Universitas Islam Negeri Ar-Raniry, Banda Aceh, Indonesia
Email: [1]210212027@student.ar-raniry.ac.id, [2]aulia.aziz@ar-raniry.ac.id

Abstrak

Penelitian ini membandingkan keamanan dan performa empat protokol *tunneling* modern Vmess, Vless, Trojan, dan WireGuard yang diimplementasikan melalui aplikasi *Passwall* versi 4.77-6 pada *firmware* ReyRe WRT berbasis OpenWRT 23.05.4, yang berjalan di perangkat *router* STB ZTE B860H. Metode eksperimen komparatif digunakan dengan pendekatan kuantitatif untuk mengevaluasi *throughput*, *latensi*, *jitter*, serta penggunaan CPU. Analisis keamanan dilakukan menggunakan Wireshark untuk menilai efektivitas enkripsi dan mendeteksi kebocoran *DNS*. Hasil menunjukkan bahwa *WireGuard* memiliki *throughput* tertinggi (45,2 Mbit/s) dan penggunaan CPU paling efisien (1,2%), menjadikannya ideal untuk aktivitas dengan kebutuhan *bandwidth* tinggi. *Trojan* mencatat *latensi* terendah (7,1 ms) dan *jitter* yang stabil (0,35 ms), cocok untuk aplikasi real-time seperti *VoIP* dan *gaming*. *Vmess* dan *Vless* menunjukkan performa sedang, dengan *Vmess* menonjol sebagai pilihan serbaguna yang seimbang. Dari sisi keamanan, semua protokol mampu mengenkripsi *payload* dengan baik, namun ditemukan kebocoran *DNS* ke *router* lokal pada konfigurasi default, yang menjadi perhatian serius dalam konteks privasi. Analisis statistik memperkuat perbedaan signifikan antar protokol. Penelitian ini memberikan wawasan berbasis data untuk pemilihan protokol *tunneling* yang sesuai dengan kebutuhan spesifik pengguna, serta menekankan pentingnya konfigurasi manual untuk mencegah kebocoran informasi.

Kata kunci: *tunneling*, *openWRT*, *passwall*, keamanan, performa, *DNS leak*

Comparison Of Security And Performance Of Vmess, Vless, Trojan, And Wireguard Protocols On Opwrt-Based Passwall

Abstract

This study compares the security and performance of four modern tunneling protocols Vmess, Vless, Trojan, and WireGuard implemented via Passwall version 4.77-6 on ReyRe WRT custom firmware based on OpenWRT 23.05.4, running on a ZTE B860H STB router. A quantitative approach using a comparative experimental method was applied to evaluate throughput, latency, jitter, and CPU usage. Security analysis was conducted using Wireshark to examine encryption effectiveness and detect DNS leaks. The results show that WireGuard achieved the highest throughput (45.2 Mbit/s) and the lowest CPU usage (1.2%), making it ideal for bandwidth-intensive activities. Trojan recorded the lowest latency (7.1 ms) and stable jitter (0.35 ms), making it suitable for real-time applications like VoIP and online gaming. Vmess and Vless performed moderately, with Vmess standing out as a balanced, versatile choice. From a security perspective, all protocols successfully encrypted payloads; however, DNS leaks to the local router were consistently detected under default configurations, posing a significant privacy concern. Statistical analysis confirmed that performance differences between protocols were significant. This study provides data-driven insights for selecting the most appropriate tunneling protocol based on specific user needs and highlights the importance of manual configuration to prevent information leakage.

Keywords*: tunneling, openWRT, passwall, security, performance, DNS leak*

1. PENDAHULUAN

Di era internet saat ini, di mana jejak digital menjadi bagian tak terpisahkan dari kehidupan sehari-hari, privasi dan keamanan dalam komunikasi data telah berevolusi dari sekadar kebutuhan teknis menjadi hak fundamental. Meningkatnya ketergantungan pada teknologi digital untuk transaksi perbankan, komunikasi pribadi, dan pekerjaan profesional telah secara eksponensial meningkatkan volume data sensitif yang ditransmisikan melalui jaringan publik. Hal ini menciptakan lanskap yang matang bagi aktor jahat untuk melakukan penyadapan, pencurian identitas, dan pengawasan massal. Untuk mengatasi tantangan ini, teknologi seperti *tunneling* dan *Virtual Private*

Network (VPN) telah muncul sebagai solusi utama, memungkinkan pengguna untuk membangun "terowongan" pribadi yang terenkripsi melalui infrastruktur internet publik, sehingga dapat menyembunyikan aktivitas online mereka dan melewati pembatasan akses geografis atau sensor(Abdulazeez *et al.*, 2020).

Salah satu platform yang paling fleksibel dan kuat untuk mengimplementasikan solusi ini adalah OpenWRT(Pratama and Rasyid, 2022). Sebagai sistem operasi berbasis Linux untuk perangkat *embedded* seperti *router*, OpenWRT mengubah perangkat keras jaringan konsumen yang terbatas menjadi alat yang dapat dikustomisasi sepenuhnya. Fleksibilitas ini memungkinkan instalasi aplikasi pihak ketiga seperti Passwall, sebuah *toolset* canggih yang berfungsi sebagai panel kontrol terpusat untuk mengelola berbagai protokol *tunneling* modern. Di antara protokol yang didukung, Vmess, Vless, Trojan, dan WireGuard menonjol karena pendekatan inovatif mereka terhadap keamanan dan performa. Vmess dan Vless adalah protokol yang dikembangkan oleh Proyek V2Ray dengan fokus pada fleksibilitas dan penghindaran deteksi. Trojan mengambil pendekatan unik dengan meniru lalu lintas HTTPS untuk membuatnya tidak dapat dibedakan dari lalu lintas web biasa. Sementara itu, WireGuard adalah protokol VPN yang lebih baru, dirancang dengan basis kode yang minimalis untuk kecepatan dan kemudahan penggunaan.

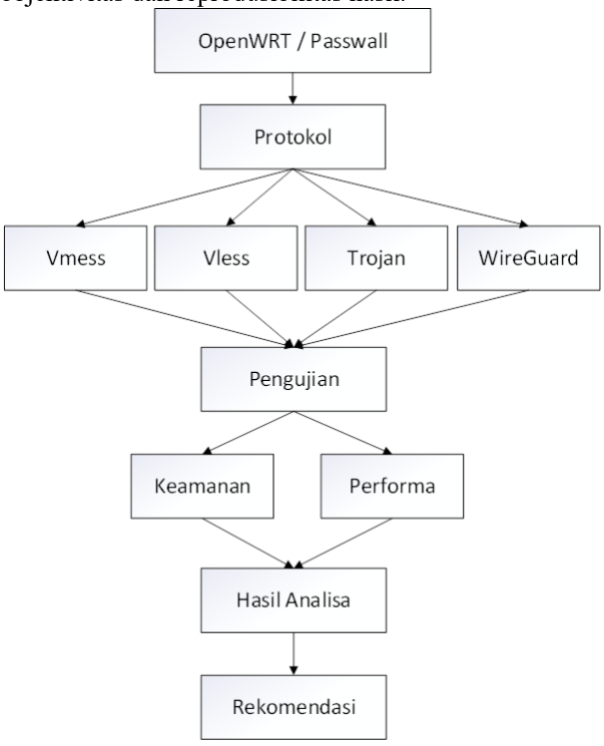
Meskipun terdapat berbagai ulasan pengguna yang bersifat anekdotal, hingga saat ini belum ada penelitian akademis yang melakukan perbandingan performa dan keamanan secara head-to-head antara Vmess, Vless, Trojan, dan WireGuard dalam satu lingkungan pengujian yang identik dan terkontrol, khususnya pada perangkat keras STB yang populer di komunitas OpenWRT. Penelitian ini secara spesifik mengisi kekosongan tersebut dengan menyediakan data kuantitatif dan analisis keamanan yang sistematis, yang tidak ditemukan pada penelitian sebelumnya.

Kedua penelitian ini berkontribusi pada pemahaman kinerja protokol tunneling pada OpenWRT, namun dengan fokus dan protokol yang berbeda. Penelitian ini lebih baru dan menguji protokol yang lebih modern (Vmess, Vless, Trojan, WireGuard) yang relevan untuk skenario circumvention dan VPN pribadi, serta menyertakan analisis keamanan. Sementara itu, artikel Justus Beyer lebih tua, berfokus pada protokol jaringan dasar dan VPN tradisional, serta menyoroti pentingnya efisiensi enkapsulasi data pada router kelas bawah. Perbedaan versi OpenWRT dan perangkat keras juga memengaruhi hasil kinerja yang diperoleh.

Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan melakukan analisis komparatif yang sistematis untuk: (1) Menganalisis dan membandingkan tingkat keamanan aktual dari protokol Vmess, Vless, Trojan, dan WireGuard, dengan fokus pada efektivitas enkripsi dan potensi kebocoran data. (2) Menganalisis dan membandingkan secara kuantitatif metrik performa kunci (*throughput, latensi, jitter, penggunaan CPU*) dari keempat protokol tersebut. (3) Memberikan rekomendasi berbasis bukti mengenai protokol yang paling optimal untuk berbagai skenario penggunaan, mulai dari *streaming* hingga *gaming* dan penggunaan umum(Pratama and Rasyid, 2022).

2. METODOLOGI PENELITIAN

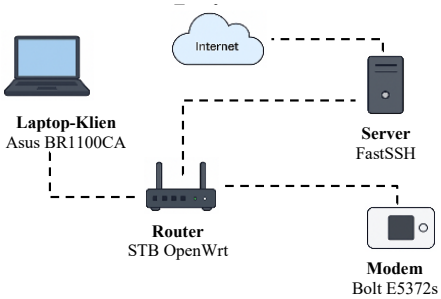
Penelitian ini menggunakan pendekatan kuantitatif dengan desain metode eksperimental komparatif yang ketat untuk memastikan objektivitas dan reprodusibilitas hasil.



Gambar 1 Diagram Alur

Subjek dan Lingkungan Penelitian:

Diagram Topologi



Gambar 2 Topologi Jaringan

Subjek penelitian adalah empat protokol tunneling Vmess, Vless, Trojan, WireGuard yang diimplementasikan pada router Set-Top Box (STB)

ZTE B860H v1. Perangkat ini dipilih karena popularitasnya di kalangan penggemar OpenWRT sebagai platform yang hemat biaya namun cukup kuat, ditenagai oleh CPU Amlogic S905X (Quad-core ARM Cortex-A53) dan RAM 1GBSutanto and Alfianto, 2022). Router ini menjalankan firmware kustom ReyRe WRT, sebuah varian yang dioptimalkan berbasis OpenWRT versi 23.05.4, dengan aplikasi Passwall versi 4.77-6 sebagai antarmuka manajemen protokol(Aminah, Raharjo and Budiman, 2021). Konfigurasi endpoint server untuk setiap protokol diperoleh dari layanan FastSSH, dengan server yang berlokasi di Singapura untuk menjaga konsistensi geografis dalam pengujian latensi(Marzuqon and Prihanto, 2022). Perangkat klien yang digunakan untuk pengujian adalah laptop yang terhubung ke router melalui koneksi Ethernet untuk menghilangkan variabel ketidakstabilan Wi-Fi.

2.1. Prosedur Pengumpulan Data

Sebelum pengujian dengan protokol, kondisi jaringan dasar (baseline) didokumentasikan dengan melakukan ping ke server Google (8.8.8.8) dan pengukuran kecepatan menggunakan Speedtest untuk mendapatkan data throughput, latensi, dan jitter tanpa tunnel. Seluruh pengujian dilakukan pada waktu yang konsisten, yaitu antara pukul 02:00 - 05:00 WIB untuk menghindari jam sibuk dan memastikan stabilitas koneksi dari penyedia layanan internet. Setiap pengujian untuk setiap metrik diulang sebanyak 30 kali untuk memenuhi syarat validitas statistik dan memastikan hasil yang lebih andal. Data yang terkumpul kemudian dianalisis untuk dihitung nilai rata-ratanya.

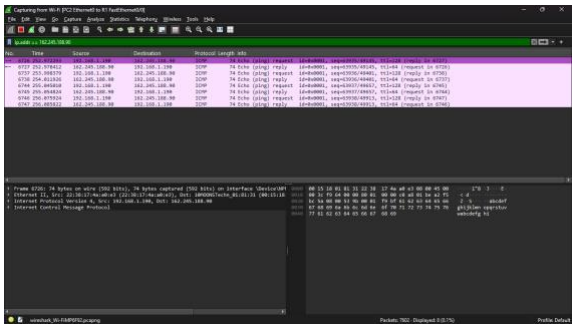
1. **Analisis Keamanan (Wireshark)**: Pengujian keamanan dilakukan dengan menangkap paket jaringan menggunakan Wireshark pada perangkat klien. Tujuannya adalah untuk memverifikasi secara visual bahwa *payload* data dari lalu lintas HTTP dan HTTPS benar-benar terenkripsi dan tidak dapat dibaca. Selain itu, analisis difokuskan pada identifikasi pola lalu lintas yang unik dari setiap protokol dan yang terpenting, untuk mendeteksi adanya *DNS leak*, di mana kueri DNS dikirim di luar *tunnel* terenkripsi(Hashim *et al.*, 2023).
2. **Throughput (iperf3)**: Throughput, atau kecepatan transfer data maksimum, diukur menggunakan *tool* iperf3. Pengujian dilakukan dengan menjalankan server iperf3 pada *endpoint* VPN dan klien iperf3 pada laptop lokal. Perintah iperf3 -c [server_ip] -p [port] -t 30s -i 5s digunakan untuk menjalankan tes selama 30 detik, memberikan gambaran yang stabil tentang kapasitas *bandwidth* yang dapat ditangani oleh setiap protokol(Zieliński, 2023).
3. **Latensi dan Jitter (mtr)**: Latensi (*round-trip time*) dan *jitter* (variasi latensi) diukur menggunakan *tool* mtr (My Traceroute). Mtr dipilih karena kemampuannya menggabungkan fungsionalitas ping dan traceroute untuk memberikan gambaran yang berkelanjutan tentang kualitas koneksi di setiap *hop* menuju server. Perintah mtr -r -c 100 [server_ip] digunakan untuk mengirim 100 paket ICMP dan melaporkan nilai latensi dan *jitter* terburuk, rata-rata, dan terbaik(Wahyuni, 2020).
4. **Penggunaan CPU (LuCI Realtime Graphs)**: Beban kerja pada CPU *router* dipantau secara *real-time* menggunakan fitur *Realtime Graphs* yang terintegrasi dalam antarmuka web LuCI OpenWRT. Penggunaan CPU dicatat selama pengujian *throughput* iperf3 untuk mensimulasikan beban maksimum, memberikan data tentang seberapa efisien setiap protokol dalam memanfaatkan sumber daya perangkat keras(Patil *et al.*, 2020).

Data mentah yang terkumpul dari serangkaian pengujian ini kemudian ditabulasi dan dianalisis secara komparatif untuk mengidentifikasi kekuatan dan kelemahan relatif dari masing-masing protokol, yang menjadi dasar untuk pembahasan dan kesimpulan penelitian.

Data performa yang diperoleh akan dianalisis secara statistik menggunakan *software SPSS*. Uji normalitas *Shapiro-Wilk* akan dilakukan untuk memeriksa distribusi data. Selanjutnya, untuk membandingkan perbedaan rata-rata performa antar keempat protokol, akan digunakan uji *Analysis of Variance* (*ANOVA*) satu arah. Jika ditemukan perbedaan yang signifikan, uji *post-hoc Tukey* akan dilakukan untuk mengidentifikasi protokol mana yang berbeda secara signifikan satu sama lain.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Keamanan



Gambar 3 Enkripsi Kemanan di Wireshark

Tabel 1 Analisis Keamanan

Protokol	*Payload* Data	TLS/Keamanan	DNS *Request*
Vmess	Terenkripsi	Aman	Bocor ke jaringan lokal (192.168.1.1)
Vless	Terenkripsi	Aman	Bocor ke jaringan lokal (192.168.1.1)
Trojan	Terenkripsi	Aman	Bocor ke jaringan lokal (192.168.1.1)
WireGuard	Terenkripsi	Aman	Bocor ke

	jaringan lokal (192.168.1.1)

Hasil analisis paket menggunakan Wireshark memberikan wawasan penting. Secara positif, keempat protokol (Vmess, Vless, Trojan, dan WireGuard) menunjukkan kemampuan enkripsi yang kuat(Aziz and Safriatullah, 2021). Saat lalu lintas HTTP dan HTTPS dilewatkan melalui *tunnel*, *payload* data yang ditangkap oleh Wireshark tampak sebagai data acak yang tidak dapat dibaca, yang mengonfirmasi bahwa fungsi enkripsi inti dari setiap protokol bekerja sebagaimana mestinya untuk melindungi konten komunikasi(Pandari and Sulistyo, 2023).

Namun, analisis yang lebih dalam mengungkap sebuah temuan kritis: kebocoran DNS (*DNS leak*) terdeteksi secara konsisten pada semua protokol yang diuji dalam konfigurasi *default* Passwall(Wangchuk and Rathod, 2021). Permintaan DNS dari perangkat klien, yang seharusnya dienkapsulasi dan dikirim ke server DNS melalui *tunnel* terenkripsi, malah dialihkan ke server DNS *default* dari *router* lokal (192.168.1.1). Ini merupakan celah privasi yang signifikan. Meskipun isi lalu lintas pengguna terenkripsi, ISP atau administrator jaringan lokal masih dapat memantau dan mencatat setiap situs web yang dikunjungi pengguna dengan menganalisis kueri DNS ini. Hal ini secara efektif merusak anonimitas yang seharusnya disediakan oleh layanan *tunneling*. Temuan ini menyoroti pentingnya konfigurasi manual oleh pengguna untuk memastikan semua lalu lintas, termasuk DNS, diarahkan dengan benar.

Selain itu, setiap protokol menunjukkan karakteristik lalu lintas yang berbeda. Lalu lintas Trojan, seperti yang dirancang, sangat mirip dengan koneksi TLS/SSL standar, membuatnya sulit dibedakan dari lalu lintas HTTPS biasa. Vmess dan Vless memiliki sidik jari yang lebih unik, sementara WireGuard menggunakan paket UDP yang dapat diidentifikasi.

Analisis Performa

Hasil pengujian performa kuantitatif menunjukkan perbedaan yang jelas dalam kapabilitas setiap protokol dan diuraikan di bawah ini.

Tabel 2 Rangkuman Hasil Uji Performa

Parameter	Vmess	Vless	Trojan	WireGuard
Throughput Rata-rata (Mbit/s)	23,6	27,8	36,3	45,2
Latensi Rata-rata (ms)	8,7	9	7,1	10,7
Jitter Rata-rata (ms)	0,60	0,45	0,35	0,25
Penggunaan CPU Rata-rata (%)	3,3	2,8	2,6	1,2

Analisis Statistik Hasil Uji Performa

Tabel 3 Uji ANOVA Satu Arah

Parameter	F	p-value	Kesimpulan
Throughput	31927.932	< 0.001	Signifikan
Latensi	3928.406	< 0.001	Signifikan
Jitter	3878.750	< 0.001	Signifikan
Penggunaan CPU	1407.950	< 0.001	Signifikan

Tabel 4 Hasil Uji Tukey HSD - Throughput

Perbandingan	Selisih Rata-rata	p-value	Signifikan?
Vmess - Vless	+0.206	0.001	Ya
Vmess - Trojan	+0.348	< 0.001	Ya
Vmess - WireGuard	+0.476	< 0.001	Ya
Vless - Trojan	+0.142	0.003	Ya
Vless - WireGuard	+0.270	< 0.001	Ya
Trojan - WireGuard	+0.128	0.005	Ya

WireGuard secara signifikan memiliki throughput tertinggi di antara semua protokol lainnya. Vmess memiliki throughput paling rendah dibanding yang lain. Semua pasangan perbandingan menunjukkan perbedaan signifikan secara statistik.

Tabel 5 Hasil Tukey HSD – Latensi

Perbandingan	Selisih Rata-rata	p-value	Signifikan?
Vmess - Vless	-0.30	< 0.001	Ya
Vmess - Trojan	+1.73	< 0.001	Ya
Vmess -WireGuard	-2.17	< 0.001	Ya
Vless - Trojan	+2.03	< 0.001	Ya
Vless - WireGuard	-1.87	< 0.001	Ya
Trojan - WireGuard	-3.90	< 0.001	Ya

Trojan adalah protokol dengan latensi paling rendah. WireGuard memiliki latensi paling tinggi. Semua pasangan perbandingan menunjukkan perbedaan signifikan secara statistik.

Tabel 6 Hasil Tukey HSD – Jitter

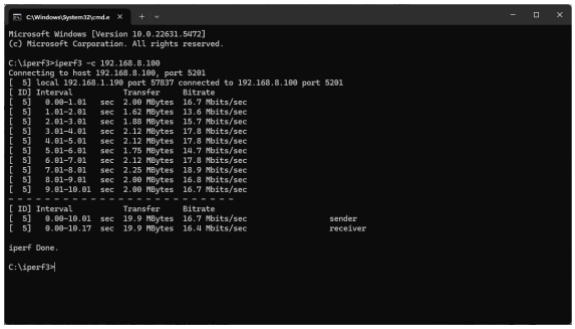
Perbandingan	Selisih Rata-rata	p-value	Signifikan?
Vless - Vmess	-0.1	<0.001	Ya
Trojan - Vmess	-0.2	<0.001	Ya
WireGuard - Vmess	-0.3	<0.001	Ya
Trojan - Vless	-0.1	<0.001	Ya
WireGuard - Vless	-0.2	<0.001	Ya
WireGuard - Trojan	-0.1	<0.001	Ya

WireGuard memiliki jitter paling rendah, diikuti oleh Trojan**,** lalu Vless**,** dan Vmess paling tinggi. Selisih jitter antar semua protokol adalah signifikan secara statistik.

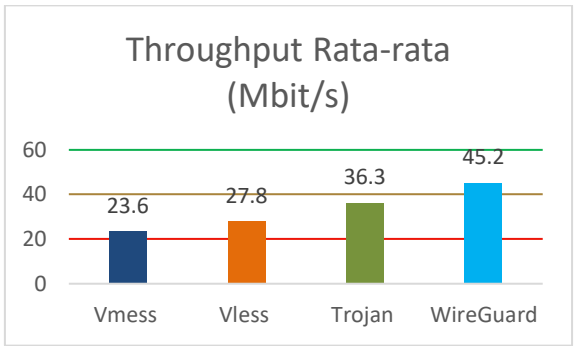
Tabel 7 Hasil Tukey HSD – Penggunaan CPU

Perbandingan	Selisih Rata-rata	p-value	Signifikan?
Vless - Vmess	-0.5	<0.001	Ya
Trojan - Vmess	-0.7	<0.001	Ya
WireGuard -Vmess	-2.1	<0.001	Ya
Trojan - Vless	-0.2	<0.001	Ya
WireGuard - Vless	-1.6	<0.001	Ya
WireGuard - Trojan	-1.4	<0.001	Ya

WireGuard menggunakan CPU paling efisien (terendah). Vmess paling tinggi penggunaan CPU-nya. Semua perbedaan antara pasangan protokol signifikan secara statistik.

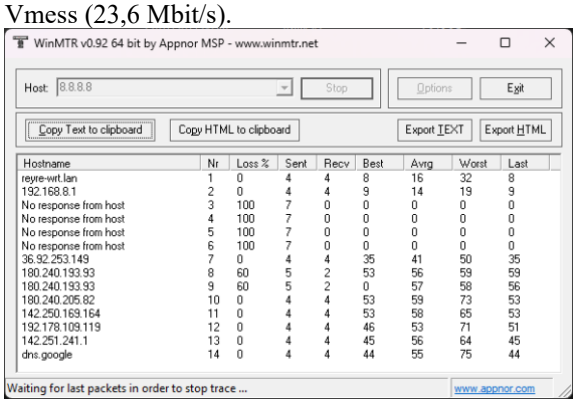


Gambar 4 Pegujian Throughput

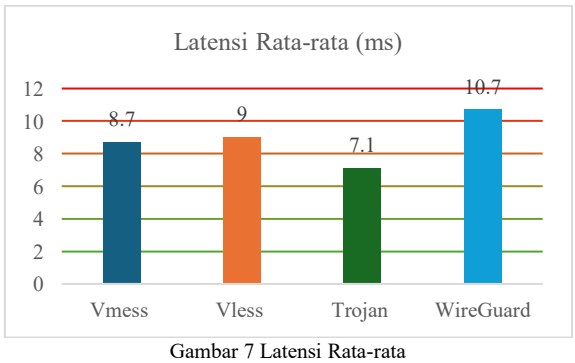


Gambar 5 Throughput Rata-rata

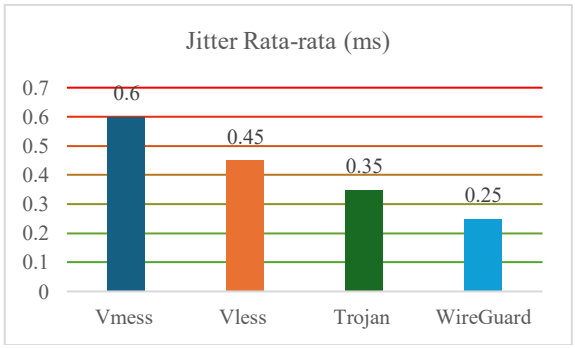
Throughput: WireGuard (45,2 Mbit/s) memiliki rata-rata throughput yang secara signifikan lebih tinggi daripada Vless (27,8 Mbit/s), Vmess (23,6 Mbit/s), dan Trojan (36,3 Mbit/s). Kecepatan ini cukup untuk melakukan *streaming* beberapa video 4K secara bersamaan atau mengunduh file besar dengan cepat. WireGuard (45,2 Mbit/s) menunjukkan keunggulan signifikan dibandingkan Trojan (36,3 Mbit/s), Vless (27,8 Mbit/s), dan Vmess (23,6 Mbit/s).



Gambar 6 Latensi & Jitter di MTR



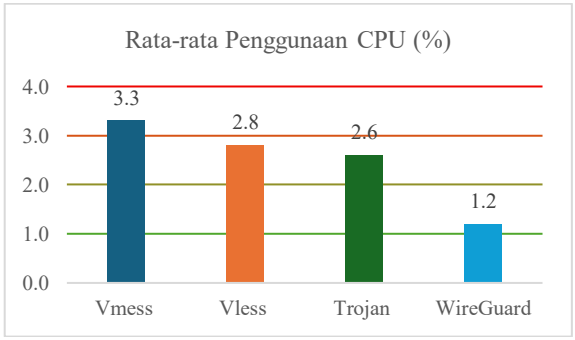
Gambar 7 Latensi Rata-rata



Gambar 8 Jitter Rata-rata

Stabilitas Koneksi (Latensi dan Jitter): Trojan memiliki latensi rata-rata terendah (7,1 ms). WireGuard memiliki jitter rata-rata terendah (0,25 ms), diikuti oleh Trojan dengan jitter yang juga sangat rendah (0,35 ms). Kestabilan ini sangat penting untuk aplikasi interaktif seperti *game online*, di mana penundaan yang tidak konsisten (*jitter*) dapat menyebabkan *lag* yang mengganggu, atau untuk panggilan VoIP dan konferensi video(Indrajaya *et al.*, 2022), di mana *jitter* yang tinggi dapat menyebabkan suara terputus-putus.

Gambar 9 Penggunaan CPU di LuCi Realtime



Gambar 10 Grafik Penggunaan CPU Raat-rata

Efisiensi Sumber Daya (Penggunaan CPU): WireGuard memiliki penggunaan CPU rata-rata terendah (1,2%). Trojan adalah yang terendah kedua (2,6%). Ini menjadikannya pilihan ideal untuk perangkat keras berdaya rendah seperti STB atau *router* generasi lama, memastikan perangkat tetap responsif untuk tugas-tugas lain.

3.2. Pembahasan

Hasil penelitian ini secara komprehensif mengonfirmasi bahwa tidak ada "protokol terbaik" yang universal; pilihan yang optimal sangat

bergantung pada skenario penggunaan dan prioritas pengguna. Analisis ini menyoroti *trade-off* yang jelas antara kecepatan, stabilitas, dan efisiensi sumber daya(Yang *et al.*, 2025).

Kasus Penggunaan untuk Kecepatan: Bagi pengguna yang prioritas utamanya adalah *bandwidth* mentah untuk mengunduh file besar, melakukan *torrenting*, atau *streaming* konten berkualitas sangat tinggi. WireGuard secara signifikan lebih cepat.

Kasus Penggunaan untuk Stabilitas: Trojan memiliki latensi terendah, dan baik Trojan maupun WireGuard memiliki jitter yang sangat rendah.

Pilihan Serbaguna: Vmess menempatkan dirinya sebagai pilihan serbaguna yang solid. Ia tidak memuncaki kategori mana pun tetapi memberikan kinerja yang sangat kompeten di semua metrik, menawarkan keseimbangan yang baik antara kecepatan yang layak dan stabilitas yang baik. Ini menjadikannya pilihan yang aman bagi pengguna yang tidak memiliki kebutuhan spesifik dan menginginkan protokol yang berkinerja baik di berbagai aktivitas.

Temuan mengenai DNS leak adalah masalah keamanan universal yang melintasi semua protokol dan tidak boleh diabaikan. Ini menyoroti bahwa keamanan *out-of-the-box* dari banyak solusi *tunneling* mungkin tidak selengkap yang diasumsikan pengguna. Untuk mitigasi, pengguna harus secara proaktif mengkonfigurasi pengaturan DNS di dalam Passwall untuk menggunakan server DNS terenkripsi (seperti DNS over HTTPS atau DNS over TLS) dan memastikan bahwa semua kueri dialihkan melalui *tunnel*.

4. KESIMPULAN DAN SARAN

Berdasarkan analisis keamanan dan performa yang komprehensif, dapat disimpulkan bahwa setiap protokol Vless, Trojan, Vmess, dan WireGuard menawarkan profil keunggulan yang unik. WireGuard terbukti paling unggul dalam throughput (45,2 Mbit/s) dan paling efisien dalam penggunaan CPU (1,2%). Trojan menonjol dengan latensi terendah (7,1 ms) dan jitter yang sangat stabil (0,35 ms), menjadikannya pilihan ideal untuk aplikasi yang sensitif terhadap penundaan. Vmess dan Vless memiliki throughput yang serupa, lebih rendah dari WireGuard, dan Vmess masih merupakan pilihan yang seimbang. Sementara semua protokol berhasil mengenkripsi lalu lintas data, kerentanan *DNS leak* yang konsisten pada konfigurasi *default* merupakan masalah keamanan signifikan yang memerlukan intervensi pengguna. Dengan demikian, rekomendasi protokol sangat bergantung pada kebutuhan spesifik: WireGuard untuk aktivitas yang haus bandwidth karena data throughput WireGuard adalah yang tertinggi., dan Trojan untuk aplikasi yang menuntut stabilitas dan efisiensi tertinggi.

Melakukan pengujian terhadap sistem *Deep Packet Inspection* (DPI) yang canggih untuk secara kuantitatif mengevaluasi seberapa efektif kemampuan penyamaran (*obfuscation*) dari Vmess, Vless, dan Trojan dalam lingkungan jaringan yang restriktif. Variasi Perangkat Keras dan Jaringan: Mengulangi eksperimen pada berbagai platform perangkat keras misalnya, *router* berbasis x86 atau model ARM yang lebih baru dan dalam kondisi jaringan yang berbeda misalnya, jaringan seluler dengan latensi tinggi atau koneksi dengan *packet loss* untuk menguji ketahanan dan skalabilitas protokol. Menyelidiki dampak dari berbagai parameter konfigurasi dalam setiap protokol misalnya, algoritma enkripsi yang berbeda pada Vmess atau pengaturan *congestion control* TCP terhadap performa dan keamanan.

DAFTAR PUSTAKA

Abdulazeez, A.M. et al. (2020) 'Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol', International Journal of Interactive Mobile Technologies, 14(18). Available at: https://doi.org/10.3991/ijim.v14i18.16507.

Aminah, N.S., Raharjo, M.R.R. and Budiman, M. (2021) 'Low-cost wireless mesh communications based on OpenWRT and voice over internet protocol', International Journal of Electrical and Computer Engineering, 11(6). Available at: https://doi.org/10.11591/ijece.v11i6.pp5119-5126.

Aziz, A.S. and Safriatullah (2021) 'Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius Design And Security Analysis On Freeradius Centralized Authentication System', Journal of Informatics and Computer Science, 7(2).

Hashim, S.R. et al. (2023) 'The facilities of detection by using a tool of Wireshark', Indonesian Journal of Electrical Engineering and Computer Science, 31(1). Available at: https://doi.org/10.11591/ijeecs.v31.i1.pp329-336.

Indrajaya, Muh.A. et al. (2022) 'Penerapan dan Analisis Perbandingan Metode Antrian Jaringan (Network Queuing) Pada Jaringan Local Area Network Fakultas Teknik Universitas Tadulako', Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering), 9(1). Available at: https://doi.org/10.33019/jurnalecotipe.v9i1.2921.

Marzuqon, M.W. and Prihanto, A. (2022) 'Analisis Perbandingan Behavior User Menggunakan Low Interaction Honeypot dan IDS pada Sistem Edge Computing', Journal of Informatics and Computer Science (JINACS), 3(04). Available at:

https://doi.org/10.26740/jinacs.v3n04.p471-480.

Pandari, J.L.J. and Sulistyo, W. (2023) 'Implementasi Intrusion Detection System (IDS) untuk Mendeteksi serangan Metasploit Exploit Menggunakan Snort dan Wireshark', Jurnal Pendidikan Teknologi Informasi (JUKANTI), 6(1 SE-Artikel).

Patil, L. et al. (2020) 'Virtual Private Network Implementation on PC as a Router for Privacy of Data Transfer', International Research Journal of Engineering and Technology [Preprint].

Pratama, Y. and Rasyid, R.M.A.K. (2022) 'PERBANDINGAN KUALITAS LAYANAN KINERJA PERANGKAT JARINGAN TP-LINK WIRELESS N ROUTER DAN GL- INET WIRELESS ROUTER BERBASIS FIRMWARE OPENWRT', Journal of Information System Management (JOISM), 4(1). Available at: https://doi.org/10.24076/joism.2022v4i1.760.

Sutanto, Y. and Alfianto, D.R. (2022) 'Analisis Perbandingan Quality of Service (QoS) Firmware Original TL-WR 840N Dengan Firmware OpenWRT Berbasis Open Source di Kos Larissa', Respati, 17(3). Available at: https://doi.org/10.35842/jtir.v17i3.469.

Wahyuni, S. (2020) 'Kajian Implementasi TWAMP Untuk Evaluasi Performa Dan Optimalisasi Desain Pada Jaringan LTE', JINTECH: Journal Of Information Technology, 1(2). Available at: https://doi.org/10.22373/jintech.v1i2.591.

Wangchuk, T. and Rathod, D. (2021) 'FORENSIC AND BEHAVIOR ANALYSIS OF FREE ANDROID VPNS', Journal of Applied Engineering, Technology and Management, 1(1). Available at: https://doi.org/10.54417/jaetm.v1i1.27.

Yang, M. et al. (2025) 'A new energy-aware resources scheduling method for mobile Internet of thing using a hybrid optimization algorithm', International Journal of Mobile Communications, 1(1). Available at: https://doi.org/10.1504/ijmc.2025.100626455.

Zieliński, B. (2023) 'Assessment of iPerf as a Tool for LAN Throughput Prediction', International Journal of Electronics and Telecommunications, 69(3). Available at: https://doi.org/10.24425/ijet.2023.146501.