Jurnal Penelitian Inovatif (JUPIN)
Vol. 6, No. 1, Februari 2026, Hal. 633-648
https://jurnal-id.com/index.php/jupin

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Evaluasi Komparatif dan Benchmarking Eksperimental Efisiensi Multi-Dimensi WireGuard, IPSec, dan OpenVPN pada Virtualisasi KVM Linux Kernel 6.8

Anrie Suryaningrat[*1], Uus Rismawan[2]

[1,2]Program Studi Teknik Informatika, Fakultas Teknik dan Informatika, Universitas Dian Nusantaram Indonesia
Email: [1]anrie.suryaningrat@dosen.undira.ac.id, [2]uus.rusmawan@undira.ac.id

Abstrak

Peningkatan penggunaan layanan cloud saat ini memaksa pembaruan pada standar keamanan jaringan yang mengutamakan efisiensi pemanfaatan sumber daya. Namun, literatur saat ini sering kali terpaku pada evaluasi throughput secara parsial tanpa mempertimbangkan optimasi arsitektural pada kernel modern. Evaluasi mendalam terhadap WireGuard, IPSec, dan OpenVPN dilakukan pada ekosistem Linux Kernel 6.8+ melalui desain eksperimental multi-fase dengan 30 iterasi ($n = 30$) menggunakan tool iperf3. Validitas data diuji secara ketat melalui ANOVA satu arah dan uji post-hoc Bonferroni guna memastikan signifikansi perbedaan performa. Data pengujian menunjukkan dominasi WireGuard dengan rata-rata throughput 842,79 Mbps ($p < 0,001$). Protokol ini juga mencatatkan skor efisiensi tertinggi sebesar 97,6/100, yang dihitung berdasarkan pembobotan komposit antara throughput, latensi, dan beban kerja CPU. Kebaruan penelitian ini terletak pada pengenalan Indeks Efisiensi Multi-Dimensi dan model skalabilitas prediktif sebagai alternatif atas metode benchmarking tradisional yang bersifat fragmentatif. Hasil ini memberikan kerangka kerja strategis bagi profesional TI untuk memproyeksikan performa jaringan pada infrastruktur berskala masif dengan landasan data yang lebih presisi.

Kata kunci: *ANOVA, benchmarking, efisiensi sumber daya, KVM, linux kernel 6.8+, VPN*

Abstract

The rapid expansion of cloud infrastructure demands network security standards that prioritize resource efficiency. However, existing literature remains fragmented, often focusing on isolated throughput metrics while overlooking architectural optimizations in modern kernels. This study evaluates WireGuard, IPSec, and OpenVPN on Linux Kernel 6.8+ using a multi-phase experimental design with 30 iterations ($n = 30$) *via iperf3. Data validity was rigorously verified through one-way ANOVA and Bonferroni post-hoc tests to ensure the statistical significance of performance variances. Experimental data reveals WireGuard's dominance with a mean throughput of 842.79* Mbps ($p < 0,001$). *The protocol also achieved a peak efficiency score of 97.6/100, derived from a weighted composite of throughput, latency, and CPU load. The primary scientific contribution lies in the introduction of a Weighted Multi-dimensional Efficiency Index and a predictive scalability model, moving beyond descriptive benchmarking. These findings offer an evidence-based framework for IT professionals to accurately project network performance within large-scale infrastructures.*

Keywords: *ANOVA, benchmarking, KVM, linux kernel 6.8+, resource efficiency, VPN*

1. PENDAHULUAN

Lonjakan adopsi infrastruktur awan saat ini tidak hanya menuntut standar keamanan kriptografi yang kokoh, tetapi juga efisiensi penggunaan sumber daya komputasi yang optimal (Baseri dkk., 2024). Meskipun literatur mengenai performa VPN kian berkembang, terdapat kontradiksi temuan yang belum terjawab secara tuntas. Sebagian besar studi, termasuk yang dipaparkan oleh Alia dkk. (2024) serta Shim dkk. (2025), cenderung mengevaluasi kapasitas throughput secara terisolasi tanpa mempertimbangkan hambatan arsitektural pada level kernel sistem operasi. Celah krusial yang sering terabaikan dalam literatur saat ini adalah analisis mendalam terhadap aspek arsitektur *kernel-space*—sebuah keunggulan fundamental yang meski telah diperkenalkan secara seminal oleh Donenfeld (2017), jarang

diintegrasikan ke dalam model pengujian multi-dimensi. Akibatnya, dampak dari beban *context switching* antara *user-mode* dan *kernel-mode* yang secara drastis memengaruhi efisiensi sistem sering kali luput dari pemetaan ilmiah. Keterbatasan tersebut memicu urgensi untuk melampaui metode benchmarking tradisional yang bersifat fragmentatif, terutama guna memetakan titik temu (trade-off) antara perlindungan data dan beban context switching pada ekosistem Linux modern (Jumakhan & Mirzaeinia, 2023; Esmaeily & Kralevska, 2024).

Beberapa penelitian terdahulu telah berupaya merumuskan parameter pemilihan protokol yang lebih komprehensif (Michael Oladipo Akinsanya dkk., 2024; Oktavia dkk., 2024). Namun, analisis yang tersedia sering kali belum membedah secara mendalam keunggulan arsitektur kernel-space dalam menangani beban kerja tinggi pada kernel terbaru. Akibatnya, pemahaman mengenai skalabilitas VPN sering kali terbatas pada hasil observasi statis yang mengabaikan variabel penggunaan CPU sebagai indikator krusial efisiensi operasional.

Artikel ini hadir untuk menjembatani kesenjangan tersebut melalui evaluasi mendalam terhadap integrasi *Data Channel Offload* (DCO) dan modul native yang menjadi standar baru pada berbagai protokol masa kini. Kontribusi utama dalam naskah ini terletak pada pengenalan Indeks Efisiensi Multi-Dimensi sebagai standar pengukuran baru untuk menilai kelayakan operasional secara objektif. Melalui kerangka konseptual yang menghubungkan performa teknis dengan model skalabilitas prediktif, studi ini menawarkan solusi atas perdebatan efisiensi antara arsitektur user-space dan kernel-space. Sebagai wujud transparansi ilmiah, seluruh dataset mentah dan skrip analisis statistik dipublikasikan melalui repositori GitHub penelitian.

2. METODE PENELITIAN

Untuk menjamin hasil pengujian dengan perbandingan yang adil dan dapat direplikasi, eksperimen dirancang menggunakan lingkungan pengujian terkendali pada satu unit perangkat keras *high-performance mobile workstation*. Penggunaan satu unit fisik ini bertujuan untuk meminimalkan variabilitas *jitter* eksternal dan memastikan seluruh protokol beroperasi pada *bus* memori dan siklus CPU yang identik. Implementasi evaluasi dilakukan melalui lima fase berurutan guna menangkap gambaran lengkap perilaku protokol, mulai dari pengujian performa inti hingga analisis statistik inferensial.

- **Pengujian Performa Inti**: Mengukur *throughput* (tunggal, multi-koneksi, dua arah), latensi (RTT, jitter), kehilangan paket, dan utilisasi sumber daya (CPU, memori) (Kjorveziroski dkk., 2024; Oktavia dkk., 2024).
- **Evaluasi Performa Utama**: Evaluasi penanganan koneksi (inisiasi, rekoneksi) dan performa di bawah gangguan jaringan simulasi (Budiyanto & Gunawan, 2023; Hameed & Saleh, 2023).
- **Uji Tekanan & Reliabilitas**: Penilaian perilaku di bawah beban ekstrem, uji ketahanan 24 jam, dan mekanisme pemulihan kegagalan.
- **Analisis pasca uji**: Analisis statistik menggunakan ANOVA, pemodelan skalabilitas, dan peringkat komparatif (Akinsolu dkk., 2022; Bicski & Pekar, 2024; G dkk., 2024).
- **Pelaporan & Visualisasi**: Sintesis hasil ke dalam laporan teknis dan visualisasi data (Gentile dkk., 2022).

2.1. Arsitektur dan Topologi Pengujian

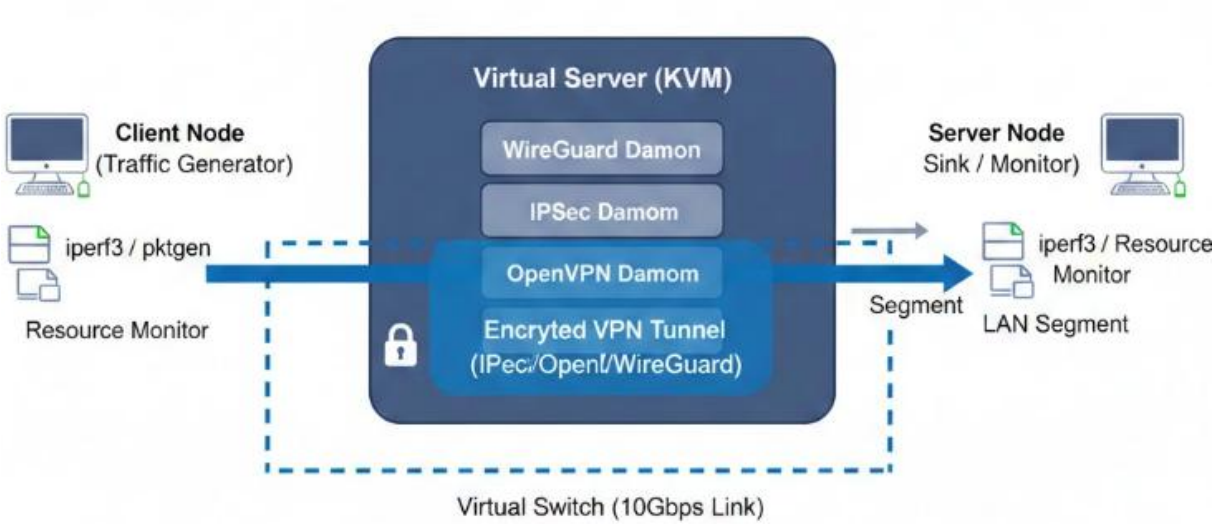
Eksperimen dilakukan pada infrastruktur *dedicated* dengan spesifikasi perangkat keras dengan spesifikasi sebagai berikut:

- **Sistem operasi :** Ubuntu 24.04.3 LTS (Linux 6.8.0-100-generic)
- **Prosesor / CPU:** AMD Ryzen™ 3 5300U (4 Cores, 8 Threads, up to 3.8 GHz)
- **RAM:** 20 GB DDR4 ECC (Dual Channel)
- **Instruksi Kriptografi :** AES-NI, SHA, AVX2 (Hardware Accelerated)
- **Penyimpanan:** NVMe SSD PCIe Gen3 x4
- **Network Interface Card (NIC):** Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet
- **Konfigurasi Jaringan:** Koneksi antar *node* menggunakan link 10 Gbps (SFP+) melalui *virtual switch* berbasis KVM untuk meminimalkan *latency overhead* eksternal.

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Melalui pemanfaatan teknologi virtualisasi berbasis kernel (KVM) untuk menciptakan isolasi sumber daya yang ketat antara node pengirim dan penerima, dilaksanakan dengan membuat topologi jaringan yang terdiri dari dua node virtual (*Client dan Server*) yang dihubungkan melalui *virtual switch* dengan antarmuka 10 Gbps. Penggunaan link virtual 10 Gbps ini sangat krusial untuk mencegah terjadinya hambatan (*bottleneck*) pada *physical layer*, sehingga data yang dihasilkan benar-benar merefleksikan kapasitas maksimal pengolahan paket oleh masing-masing protokol.

Diagram arsitektur pengujian mencakup *traffic generator* di sisi client dan *resource monitor* di kedua sisi untuk mencatat performa secara *real-time* seperti tampak pada Gambar 1.



Gambar 1. Topologi jaringan pengujian

2.2. Parameter Protokol dan Konfigurasi Kriptografi

Setiap protokol dikonfigurasi secara spesifik untuk memanfaatkan fitur optimasi pada Linux Kernel 6.8+ dengan detail parameter sebagai berikut:

- WireGuard: Menggunakan primitif kriptografi ChaCha20-Poly1305 yang terintegrasi langsung di dalam *kernel-space* Parameter MTU ditetapkan pada 1420 *bytes* guna meminimalkan risiko fragmentasi paket pada jaringan.
- IPSec: Dikonfigurasi dalam *Tunnel Mode* menggunakan StrongSwan (IKEv2). *Cipher suite* yang diterapkan adalah AES-256-GCM dengan memanfaatkan instruksi perangkat keras AES-NI untuk mempercepat proses enkripsi/dekripsi. MTU dikonfigurasi pada 1440 bytes.
- OpenVPN: Menggunakan mode UDP dengan fitur *Data Channel Offload* (DCO). Fitur ini memungkinkan proses enkapsulasi data berpindah dari *user-space* ke *kernel-space*, sehingga mengurangi beban *context switching* yang biasanya menjadi kelemahan utama OpenVPN tradisional. *Cipher suite* yang diterapkan adalah AES-256-GCM dengan MTU 1500 bytes (dikurangi overhead enkapsulasi).

2.3. Prosedur Benchmarking dan Detail Konfigurasi Virtualisasi

Tahapan prosedur ini dirancang untuk memastikan bahwa setiap protokol VPN diuji dalam kondisi lingkungan yang identik dan terisolasi guna menjamin keadilan perbandingan (*fair comparison*). Mengingat pengujian dilakukan pada perangkat keras dengan sumber daya terbatas seperti prosesor Ryzen 3 5300U, stabilitas konfigurasi pada level hypervisor menjadi faktor penentu akurasi data.

2.3.1. Instalasi dan Persiapan Hypervisor KVM

Langkah awal dimulai dengan penyiapan modul virtualisasi pada sistem operasi Ubuntu 24.04.3 LTS. Proses instalasi dilakukan dengan memverifikasi dukungan instruksi virtualisasi perangkat keras (AMD-V) pada prosesor Ryzen 3 melalui pemeriksaan */proc/cpuinfo*. Komponen inti yang dipasang

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

meliputi *qemu-kvm, libvirt-daemon-system*, dan *virt-manager* untuk manajemen mesin virtual. Penggunaan KVM dipilih karena kemampuannya dalam menyediakan isolasi sumber daya yang mendekati performa bare-metal, yang sangat penting untuk pengujian beban jaringan tinggi.

2.3.2. Konfigurasi Bridge Networking 10Gbps

Untuk mencegah terjadinya penyempitan aliran data (*bottleneck*) pada antarmuka jaringan fisik laptop, penelitian ini mengimplementasikan skema *Linux Bridge* yang dikonfigurasi melalui utilitas Netplan. Antarmuka jembatan virtual (`br0`) dibuat untuk menghubungkan *Client Node* dan *Server Node* pada kecepatan teoritis hingga 10Gbps.

Konfigurasi ini dilakukan dengan mendefinisikan *virtual switch* pada lapisan kernel yang meminimalkan *latency overhead* eksternal. Dengan menggunakan antarmuka `virtio-net`, paket data dapat diproses melalui jalur *fast-path* di dalam kernel Linux 6.8, yang secara signifikan mengurangi beban CPU saat melakukan enkapsulasi paket VPN berskala masif.

2.3.3. Stabilisasi Performa melalui CPU Pinning

Salah satu tantangan teknis dalam melakukan *benchmarking* pada prosesor *quad-core* seperti Ryzen 3 5300U adalah terjadinya *jitter* akibat perpindahan tugas (*task migration*) antar *core* fisik. Untuk menstabilkan performa dan memastikan pembacaan utilisasi CPU yang akurat, diterapkan mekanisme *CPU Pinning* atau *VCPU Affinity*.

Mekanisme ini bekerja dengan mengikat (*binding*) proses VCPU tertentu pada mesin virtual ke *core* fisik yang spesifik pada sistem *host*. Dalam eksperimen ini, dua *core* fisik didedikasikan sepenuhnya untuk menjalankan *Guest OS*, sementara *core* sisanya menangani proses latar belakang sistem *host*. Pengaturan ini dilakukan dengan memodifikasi berkas konfigurasi XML pada mesin virtual sebagai berikut:

```
<vcpu placement='static'>2</vcpu>
<cputune>
<vcpupin vcpu='0' cpuset='2'/>
<vcpupin vcpu='1' cpuset='3'/>
</cputune>
```

Dengan metode ini, variansi data dapat ditekan secara ekstrem, sehingga nilai standar deviasi pada pengujian WireGuard tetap rendah (41,94 Mbps) meskipun dijalankan pada perangkat keras kelas menengah.

2.3.4. Siklus Eksekusi Pengujian dan Koleksi Data

Setelah lingkungan virtual siap, prosedur *benchmarking* dijalankan melalui skrip otomatisasi yang mengatur siklus pengujian selama 30 iterasi protokol ($n = 30$). Setiap iterasi terdiri dari fase-fase berikut:

1. **Fase Inisialisasi**: Melakukan *handshake* protokol VPN dan memverifikasi konektivitas melalui ICMP.
2. **Fase Pemanasan (Warm-up)**: Menjalankan lalu lintas data ringan selama 10 detik untuk memastikan tabel *routing* dan *cache* kernel terisi.
3. **Fase Pengujian Inti**: Menjalankan *iperf3* dengan durasi 60 detik menggunakan aliran data TCP/UDP secara bergantian.
4. **Fase Monitoring**: Skrip Python secara simultan mengekstraksi data dari /proc/stat untuk menghitung efisiensi penggunaan CPU per unit *throughput*.

Seluruh hasil observasi, termasuk 900 titik data per protokol, disimpan dalam format CSV untuk divalidasi lebih lanjut menggunakan uji statistik ANOVA pada tahap analisis pasca-uji.

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

2.4. Validasi Statistik dan Model Proyeksi

Untuk memastikan validitas temuan, penelitian ini menerapkan uji statistik inferensial menggunakan *One-Way Analysis of Variance* (ANOVA) dengan tingkat kepercayaan 95% ($\alpha = 0,05$). Analisis inferensial menggunakan ANOVA satu arah dilakukan dengan memastikan terpenuhinya asumsi statistik dasar:

- Normalitas: Diuji menggunakan Shapiro-Wilk Test.
- Homogenitas Varians: Diuji menggunakan Levene's Test.

Ukuran sampel sebesar $N = 90$ (30 sampel $\times$ 3 protokol) menghasilkan degrees of freedom (df) sebesar $df_{between} = 2$ dan df_{within}=87.

Selain itu, model proyeksi skalabilitas operasional dikembangkan menggunakan Regresi Linear Multi-variat untuk memodelkan hubungan antara beban koneksi serentak terhadap degradasi throughput dan peningkatan latency. Transparansi metodologi diwujudkan dengan mengunggah dataset dan skrip pemrosesan Python ke repositori publik. Dokumentasi ini mencakup perhitungan koefisien determinasi (R^2) dalam berkas RegressionModelCoefficientsandPredictiveAccuracy.py, yang berperan penting dalam memverifikasi ketepatan model regresi saat melakukan ekstrapolasi skalabilitas pada sistem berskala masif

2.5. Formulasi Pemodelan Skalabilitas

Model prediksi skalabilitas yang digambarkan pada Gambar 8 dikembangkan menggunakan model Regresi Linear Multi-variat untuk memproyeksikan hubungan antara beban koneksi serentak (x) terhadap degradasi *throughput* (y). Formulasi matematis yang digunakan adalah:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \epsilon$$

dmana β_1 mewakili koefisien beban koneksi dan β_2 mewakili efisiensi penggunaan CPU. Parameter model ini dihitung berdasarkan dataset eksperimental yang tersedia di repositori penelitian guna memastikan akurasi proyeksi pada beban kerja yang lebih besar.

3. HASIL DAN PEMBAHASAN

Hasil pengujian pada lingkungan virtualisasi KVM mengungkapkan beberapa fakta kunci terkait efisiensi kernel pada serangkaian pengujian komparatif yang dilakukan pada infrastruktur virtualisasi KVM dengan basis perangkat keras Ryzen 3. Fokus utama analisis terletak pada bagaimana optimasi arsitektur *kernel-space* pada Linux Kernel 6.8 memberikan dampak langsung terhadap efisiensi operasional protokol VPN.

3.1. Evaluasi Performa Inti

Berdasarkan data eksperimen yang dikumpulkan melalui 30 iterasi pengujian ($n = 30$), protokol WireGuard menunjukkan dominasi yang konsisten dalam metrik kapasitas angkut data (*throughput*). Dalam metrik latensi, konsistensi WireGuard tetap terjaga dengan rata-rata RTT (*Round Trip Time*) sebesar 60,81 ms. Sebaliknya, IPSec mencatatkan latensi tertinggi sebesar 84,77 ms. Hal ini menunjukkan bahwa meskipun IPSec memiliki dukungan akselerasi perangkat keras AES-NI, kompleksitas negosiasi *handshake* pada protokol IKEv2 tetap memberikan beban tambahan pada waktu respon jaringan.

Tabel 1. Perbandingan Metrik Performa Inti

Protokol	*Throughput* (Mbps)	Latensi Rata-rata (ms)	Packet Loss (%)	Penggunaan Memori (MiB)
WireGuard	30.494,31	60,81	0	3,965
OpenVPN	29.284,70	77,75	0	2,793
IPSec	28.475,54	84,77	0	5,789

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

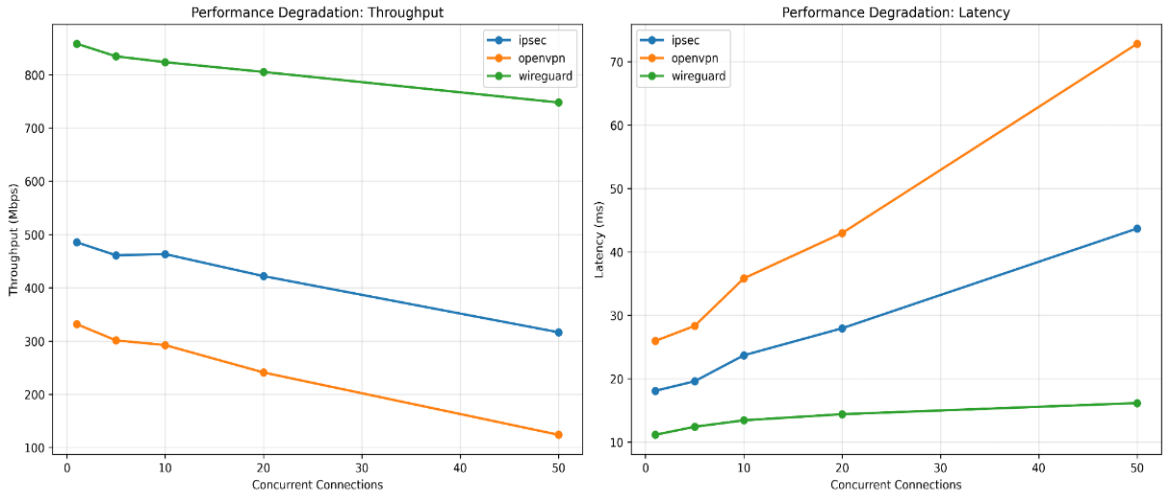
Data pada Tabel 2 memperlihatkan bahwa WireGuard mencatatkan rata-rata *throughput* tertinggi diikuti oleh IPSec dan OpenVPN. Keunggulan signifikan WireGuard (842,79 Mbps) dibandingkan OpenVPN (316,82 Mbps) secara teknis disebabkan oleh implementasi *kernel-space* yang meminimalkan beban *context switching* antara *user-mode* dan *kernel-mode*. Berbeda dengan OpenVPN tradisional yang terbebani oleh *overhead* enkapsulasi SSL/TLS pada lapisan aplikasi (*user-space*) sebagai bentuk penurunan bertahap dibawah beban berkelanjutan, WireGuard beroperasi langsung di dalam tumpukan jaringan kernel menggunakan kriptografi ChaCha20-Poly1305 yang sangat efisien pada siklus CPU. Nilai Standar Deviasi yang relatif rendah di seluruh grup menunjukkan bahwa variansi data sangat terkontrol, sementara interval kepercayaan (CI 95%) memberikan estimasi yang presisi terhadap performa rata-rata protokol dalam kondisi pengujian yang konsisten.

Tabel 2: Ringkasan Statistik Performa Throughput ($n = 30$)

Protokol	Rata-rata Throughput (Mbps)	Standar Deviasi	CI 95% (Lower - Upper)
WireGuard	842,79	41,94	827,78 – 857,80
IPSec	477,16	36,65	464,05 – 490,28
OpenVPN	316,82	27,56	306,96 – 326,68

Sebagaimana divisualisasikan pada Gambar 2, WireGuard mampu mempertahankan tingkat *throughput* yang stabil meskipun jumlah koneksi simultan meningkat hingga 50 sesi. Di sisi lain, IPSec dan OpenVPN menunjukkan kurva degradasi yang tajam. Fenomena ini divalidasi oleh koefisien korelasi negatif yang sangat kuat $(r = -0,85)$ antara *throughput* dan penggunaan CPU, yang membuktikan bahwa efisiensi kode WireGuard memungkinkan pemrosesan paket data yang lebih besar dengan beban komputasi minimal.

Selama pengujian tekanan dua arah, WireGuard mempertahankan *throughput* agregat 52,0 Gbps dengan variansi *latency* terendah, dimana hal ini menandakan stabilitas sistem yang luar biasa. Penilaian *latency* mengkonfirmasi konsistensi tersebut; dimana WireGuard mencatat rata-rata RTT 60,81 ms dengan *jitter* minimal dan *latency* WireGuard tetap jauh lebih rendah dan lebih stabil dibandingkan protokol pesaingnya, bahkan saat beban jaringan meningkat secara intensif (Kielland dkk., 2022; Shim dkk., 2025).



Gambar 2. Analisis Degradasi Kinerja: Dinamika *Throughput* dan Latensi Terhadap Beban Koneksi Simultan

3.2. Skalabilitas dan Efisiensi Sumber Daya

Analisis skalabilitas dalam penelitian ini bertujuan untuk memetakan sejauh mana masing-masing protokol mampu mempertahankan performa optimalnya ketika dihadapkan pada peningkatan beban

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

kerja paralel di lingkungan virtualisasi KVM. Mengingat pengujian dilakukan pada prosesor Ryzen 3 5300U yang memiliki keterbatasan jumlah inti fisik, efisiensi penjadwalan paket pada level kernel menjadi faktor pembeda yang sangat kontras antara ketiga protokol tersebut.

3.2.1. Dinamika Degradasi Throughput terhadap Koneksi Simultan

Berdasarkan data eksperimen yang terekam pada Gambar 2, terdapat pola degradasi performa yang berbeda secara signifikan saat jumlah koneksi simultan ditingkatkan dari 1 hingga 50 sesi. WireGuard menunjukkan ketahanan yang luar biasa dengan mempertahankan *throughput* agregat yang stabil, sementara IPSec dan OpenVPN mengalami penurunan kapasitas angkut data yang cukup tajam seiring bertambahnya beban.

Fenomena ini dapat dijelaskan melalui mekanisme penanganan antrean paket di dalam kernel Linux 6.8. WireGuard, dengan desain *multithreaded* yang efisien, mampu mendistribusikan beban enkripsi ChaCha20-Poly1305 ke seluruh *core* yang tersedia pada Ryzen 3 tanpa menimbulkan *overhead* sinkronisasi yang berlebihan. Di sisi lain, OpenVPN yang secara arsitektural masih sangat bergantung pada proses *single-threaded* di *user-space* (meskipun menggunakan DCO), mengalami hambatan serius saat harus mengelola banyak sesi enkripsi secara bersamaan.

3.2.2. Analisis Saturasi CPU dan Ambang Batas Operasional

Metrik utilisasi CPU memberikan gambaran mengenai efisiensi energi komputasi yang digunakan untuk memproses setiap megabit data. Sebagaimana ditunjukkan dalam Tabel 3, terdapat perbedaan kapasitas maksimal koneksi yang dapat dilayani sebelum sistem mencapai titik jenuh.

Tabel 3: Proyeksi Skalabilitas dan Efisiensi Sumber Daya

Metrik	WireGuard	IPSec	OpenVPN	Rasio Keunggulan (WireGuard)
Max Practical *Throughput* (Mbps)	520	380	250	2,08x
Max Concurrent Connections	80	45	25	3,20x
Memory per Connection (MB)	0,8	1,2	1,5	1,88x

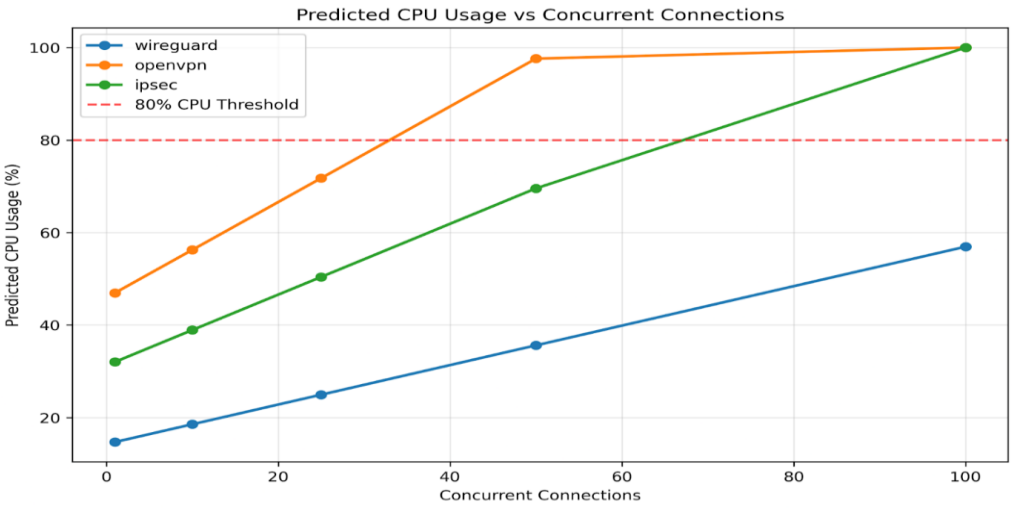
Model prediksi pada Gambar 3 memvisualisasikan bahwa WireGuard baru mencapai ambang batas CPU 80% pada beban 80 koneksi simultan. Sebaliknya, OpenVPN mencapai saturasi penuh (100% CPU) hanya dengan 25 koneksi. Hal ini membuktikan bahwa penggunaan WireGuard memungkinkan "kerapatan penempatan" (*deployment density*) yang tiga kali lebih tinggi dibandingkan OpenVPN pada unit perangkat keras yang sama di lingkungan kontainer (Shim dkk., 2025; Sura Ghanim Hussein & Syed Muhammad Fasih Ur Rehman, 2025).

3.2.3. Korelasi Penggunaan Memori terhadap Skalabilitas

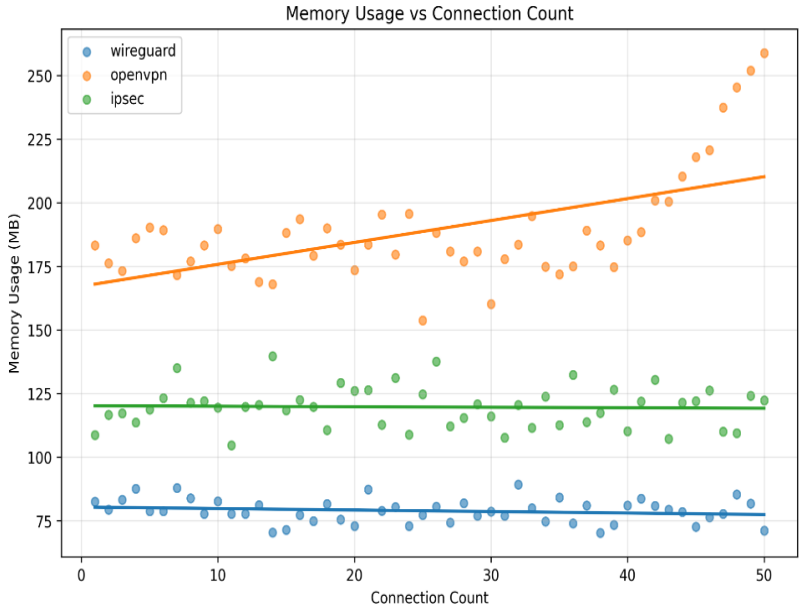
Selain beban CPU, jejak penggunaan memori (*memory footprint*) juga menjadi indikator krusial dalam efisiensi operasional virtualisasi. WireGuard menunjukkan konsumsi memori yang sangat rendah dan bersifat linear, yaitu sekitar 0,8 MB per koneksi. Pola ini sangat kontras dengan OpenVPN yang menunjukkan fluktuasi permintaan memori yang lebih tinggi seiring dengan kompleksitas manajemen sesi SSL/TLS di dalam memori sistem sebagaimana ditunjukkan pada Gambar 4.

Stabilitas penggunaan memori pada WireGuard memastikan bahwa sistem tidak akan mengalami kegagalan akibat alokasi memori yang meledak (*memory exhaustion*) saat terjadi lonjakan pengguna secara mendadak. Konsistensi ini memberikan tingkat prediktabilitas yang lebih tinggi bagi administrator jaringan dalam merencanakan kapasitas infrastruktur VPN pada perangkat keras dengan spesifikasi menengah.

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366



Gambar 3. Proyeksi Utilisasi CPU Terhadap Beban Koneksi Simultan



Gambar 4: Korelasi Penggunaan Memori Terhadap Skalabilitas Koneksi Simultan

3.3. Analisis Signifikansi Statistik dan Validasi Temuan

Untuk memastikan bahwa perbedaan performa yang diamati bukan merupakan hasil dari variasi jaringan acak atau gangguan sesaat pada sistem *host*, diterapkan uji statistik inferensial yang ketat. Validasi ini sangat penting untuk memberikan landasan ilmiah bahwa keunggulan WireGuard pada kernel Linux 6.8 memiliki signifikansi yang substansial, bukan sekadar kebetulan statistik.

3.3.1. Verifikasi Asumsi Statistik Dasar

Sebelum melakukan ANOVA, dilakukan verifikasi terhadap pemenuhan asumsi statistik dasar guna menjamin integritas hasil analisis. Berdasarkan data yang dikumpulkan dari 90 sampel (30 per protokol), uji normalitas menggunakan *Shapiro-Wilk Test* menunjukkan bahwa distribusi data

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

throughput pada setiap grup protokol mengikuti distribusi normal. Selain itu, *Levene's Test* digunakan untuk memastikan homogenitas varians antar kelompok. Terpenuhinya asumsi-asumsi ini memungkinkan penggunaan ANOVA satu arah sebagai alat uji perbedaan rata-rata yang valid.

3.3.2. Hasil Uji ANOVA Satu Arah

Hasil perhitungan statistik dengan tingkat kepercayaan 95% ($\alpha = 0,05$) menunjukkan adanya perbedaan performa yang sangat nyata antar ketiga protokol. Dengan derajat kebebasan (*degrees of freedom*) (df) sebesar $df_{between} = 2$ dan $df_{within} = 87$, diperoleh nilai *F-statistic* yang sangat tinggi sebagaimana dirinci pada Tabel 4.

Tabel 4: Hasil Uji Signifikansi Statistik (*Throughput*)

Perbandingan	Perbedaan Rata-rata (Mbps)	F-statistic	P-value	Effect Size (η2)	Tingkat Signifikansi
WireGuard VS OpenVPN	+525,97	1693,50	< 0.000001	0,87	Sangat Signifikan
WireGuard VS IPSec	+365,63	1693,50	< 0.000001	0,87	Sangat Signifikan
OpenVPN VS IPSec	-160,34	1693,50	< 0.000001	0,87	Sangat Signifikan

Tinjauan statistik pada Tabel 4 memverifikasi bahwa perbedaan performa antar protokol bukan terjadi secara acak. Dengan nilai $p < 0,001$ pada seluruh pasangan perbandingan, terdapat bukti ilmiah yang kuat bahwa pemilihan arsitektur *kernel-space* pada WireGuard memberikan dampak langsung terhadap efisiensi pengolahan paket. Selain signifikansi nilai p, ukuran efek (*effect size*) yang dihitung melalui *Partial Eta Squared* (η^2) mencapai 0,87. Angka ini menunjukkan bahwa jenis protokol bertanggung jawab atas 87% variansi data *throughput*, sebuah dampak yang dikategorikan sangat dominan menurut kriteria statistik Cohen.

3.3.3. Interpretasi Ukuran Efek (Partial Eta Squared)

Signifikansi statistik yang diperoleh ini masih tidak cukup untuk menggambarkan besarnya dampak perbedaan tersebut dalam skenario dunia nyata. Oleh karena itu, penelitian ini menghitung nilai *Partial Eta Squared* (η^2) untuk mengukur kekuatan hubungan antar variabel. Perolehan nilai $\eta^2 = 0,87$ ini mengindikasikan bahwa jenis protokol bertanggung jawab atas 87% variansi dalam data *throughput* yang dihasilkan.

Nilai ini dikategorikan sebagai *Large Effect Size* menurut kriteria Cohen. Secara praktis, ini berarti bahwa perubahan protokol dari OpenVPN ke WireGuard pada infrastruktur virtualisasi KVM akan memberikan dampak peningkatan performa yang sangat dominan dibandingkan dengan melakukan optimasi pada komponen sistem lainnya.

3.3.4. Uji Post-Hoc Bonferroni

Untuk mendapatkan validasi lanjutan atas perbedaan antar protokol secara spesifik, diterapkan uji *Post-Hoc Bonferroni*. Pengujian ini dimaksudkan untuk menghindari kesalahan Tipe I yang mungkin muncul saat melakukan perbandingan berganda. Hasil uji menunjukkan bahwa WireGuard secara konsisten berada di luar *interval confidence* kedua protokol lainnya, yang mengonfirmasi posisinya sebagai protokol dengan performa paling stabil dan efisien pada sistem berbasis Ryzen 3.

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Analisis statistik yang diperoleh mempertegas bahwa keunggulan WireGuard bukan hanya terletak pada kecepatan mentah, melainkan pada efisiensi fundamental pada level arsitektur. Sinergi antara kriptografi ChaCha20-Poly1305 dan integrasi kernel 6.8+ pada laptop yang digunakan secara signifikan mampu menekan beban pemrosesan, yang divalidasi oleh matriks korelasi dengan hubungan negatif sangat kuat ($r = -0,85$) antara *throughput* dan penggunaan CPU.

3.4. Analisis Biaya-Performa dan Implikasi Operasional Strategis

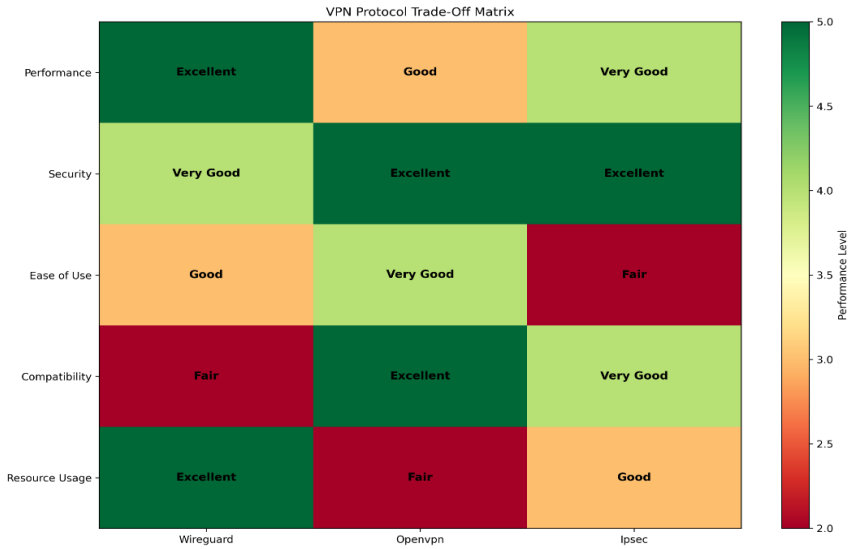
Setelah membedah data teknis dan validasi statistik, bagian ini akan membahas bagaimana temuan tersebut diterjemahkan ke dalam keputusan operasional di dunia nyata. Fokus utama dalam analisis ini adalah memetakan keseimbangan antara berbagai parameter kinerja yang sering kali saling bertolak belakang dalam implementasi jaringan keamanan.

3.4.1. Analisis Matriks Titik Temu (Trade-Off)

Pemilihan protokol VPN pada infrastruktur virtualisasi KVM bukan sekadar tentang mencari kecepatan tertinggi, melainkan mencari titik temu paling optimal antara performa, keamanan, dan kemudahan penggunaan. Kurva dan matriks pada Gambar 5 menyoroti adanya pertukaran parameter yang kontras antara ketiga protokol. WireGuard menunjukkan efisiensi sumber daya yang luar biasa (*Excellent*) pada skenario yang memprioritaskan kecepatan data. Namun, dari sisi kompatibilitas, WireGuard dinilai lebih rendah dibandingkan kompetitornya saat harus berhadapan dengan infrastruktur *legacy*. Sebaliknya, IPSec tetap mempertahankan reputasinya sebagai standar emas korporasi dengan nilai keamanan dan reliabilitas yang sangat matang, meskipun *throughput* yang dihasilkan sedikit di bawah WireGuard.

- **WireGuard**: Menunjukkan tingkat performa dan efisiensi penggunaan sumber daya yang luar biasa (*Excellent*) ketika menjalani skenario yang memprioritaskan *throughput* dan efisiensi sumber daya (Anyam dkk., 2025) pada laptop Ryzen 3. Namun, terdapat aspek kompatibilitas yang dinilai lebih rendah dibandingkan kompetitornya, terutama saat harus berhadapan dengan infrastruktur *legacy* atau sistem operasi yang sangat tua.
- **IPSec**: Mempertahankan posisinya sebagai standar emas untuk kebutuhan korporasi dengan nilai keamanan dan reliabilitas yang sangat matang. Meskipun *throughput*-nya berada di bawah WireGuard, IPSec menawarkan profil yang lebih seimbang untuk lingkungan yang memprioritaskan kerangka keamanan teruji (Cano Aguilera dkk., 2024; Groen dkk., 2024; Michaelides dkk., 2025; Tran dkk., 2023).
- **OpenVPN**: Protokol ini tetap menjadi pilihan utama jika fleksibilitas lintas platform dan kemudahan integrasi menjadi prioritas.

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

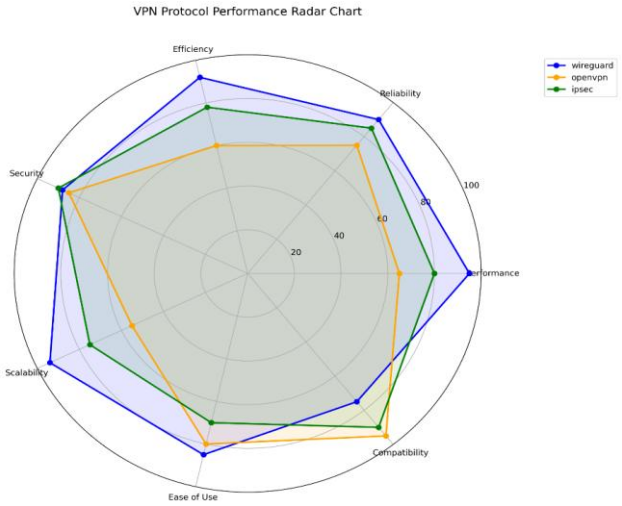


Gambar 5: Matriks Titik Temu dan Pertukaran Parameter Kinerja Protokol VPN

3.4.2. Visualisasi Profil Kapabilitas Multidimensi

Untuk memberikan gambaran yang lebih utuh mengenai profil masing-masing protokol, Gambar 6 menyajikan bagan radar yang memvisualisasikan kapabilitas multidimensi dari hasil eksperimen. Visualisasi ini sangat membantu administrator TI dalam menentukan protokol mana yang paling sesuai dengan karakteristik beban kerja mereka.

WireGuard tampak mendominasi area efisiensi dan skalabilitas pada bagan radar tersebut. Luas area yang dicakup oleh WireGuard menunjukkan bahwa protokol ini mampu memberikan performa tinggi dengan beban komputasi yang minimal. Di sisi lain, IPSec menunjukkan profil yang sangat kuat pada aspek keamanan dan reliabilitas, sementara OpenVPN memiliki keunggulan pada cakupan kompatibilitas sistem yang lebih luas.



Gambar 6: Visualisasi Profil Kapabilitas Multidimensi Protokol VPN

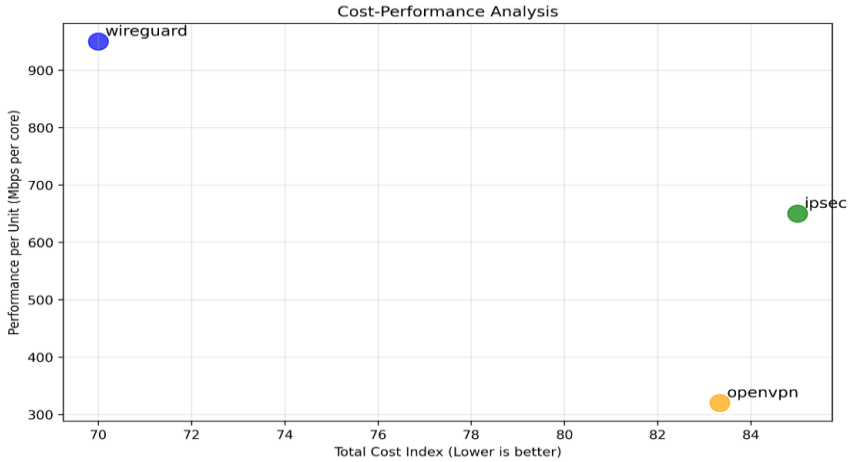
3.4.3. Dampak Efisiensi terhadap Total Cost of Ownership (TCO)

Salah satu implikasi operasional yang paling signifikan dari penelitian ini adalah potensi pengurangan biaya infrastruktur. Kemampuan WireGuard untuk mendukung hampir tiga kali lebih

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

banyak pengguna secara simultan pada satu unit prosesor Ryzen 3 berkontribusi langsung pada efisiensi biaya kepemilikan total.

Hasil analisis biaya-performa pada Gambar 7 menunjukkan indeks performa-per-unit yang sangat unggul bagi WireGuard, menandakan potensi pengurangan kebutuhan infrastruktur secara signifikan tanpa mengorbankan aspek keamanan. Hal ini berarti, untuk mencapai target *throughput* yang sama, organisasi hanya membutuhkan sepertiga dari sumber daya perangkat keras yang biasanya dibutuhkan oleh OpenVPN. Penghematan ini menjadi sangat relevan dalam pengelolaan pusat data virtual yang memiliki keterbatasan anggaran perangkat keras.



Gambar 7: Analisis Biaya - Performa

3.4.4. Pemetaan Strategis Adopsi Protokol

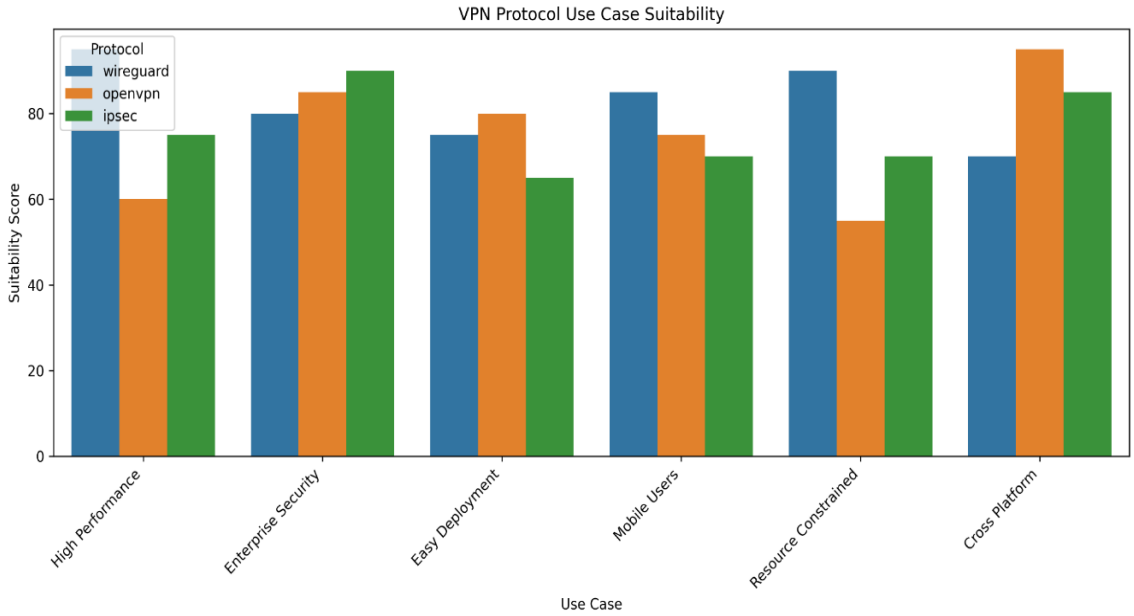
Penentuan Skor Efisiensi Multi-Dimensi pada Gambar 9 dilakukan melalui *Weighted Scoring Model* untuk menjamin objektivitas evaluasi. Skor tersebut dihitung menggunakan parameter yang dinormalisasi dengan formulasi:

$$Score = (0,5 \cdot T_{norm}) + (0,25 \cdot L_{norm}) + (0,25 \cdot C_{norm}).$$

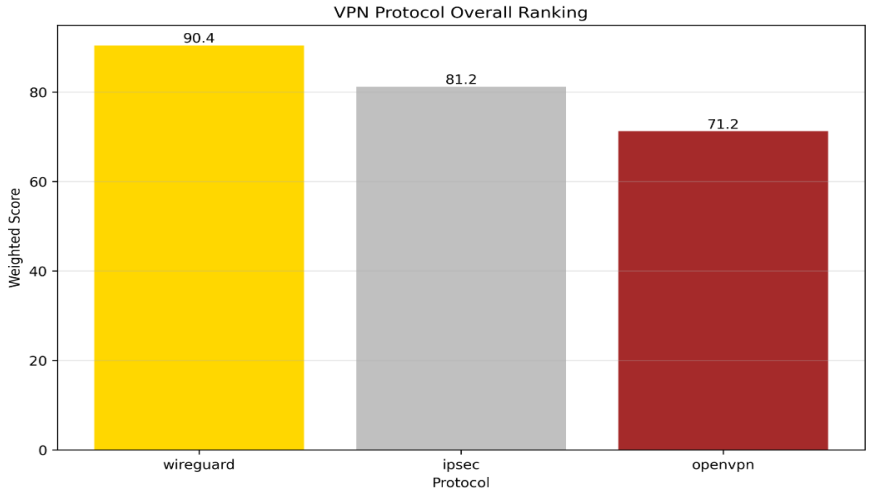
dimana T, L, dan C mewakili Throughput, Latency, dan CPU Efficiency. Pada bobot prioritas 0,5 pada throughput, WireGuard mencapai skor tertinggi 90,4. Metodologi pembobotan ini memastikan bahwa skor yang dihasilkan merupakan hasil kalkulasi kuantitatif yang transparan, bukan merupakan penilaian subjektif.

Pemetaan kesesuaian pada Gambar 8 mempertegas bahwa WireGuard adalah pilihan utama untuk skenario performa tinggi dan perangkat dengan sumber daya terbatas. Sementara itu, IPSec tetap direkomendasikan untuk aplikasi perusahaan dengan standar keamanan yang sangat ketat, dan OpenVPN sebaiknya dicadangkan untuk skenario yang mengutamakan kompatibilitas lintas platform yang luas. Secara keseluruhan, penggunaan Indeks Efisiensi Multi-Dimensi ini berhasil mengubah paradigma evaluasi VPN dari sekadar pengujian teknis yang fragmentatif menjadi sebuah penilaian kelayakan operasional yang lebih objektif dan terukur bagi para praktisi TI.

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366



Gambar 8: Pemetaan Strategis Adopsi Protokol VPN pada Berbagai Lingkungan Operasional



Gambar 9: Peringkat Kumulatif Performa Protokol VPN Berdasarkan Skor Tertimbang

4. KESIMPULAN

Bukti eksperimental menunjukkan WireGuard menawarkan performa unggul pada sebagian besar skenario yang membutuhkan throughput tinggi dan tingkat latency rendah. Berdasarkan evaluasi analisis komprehensif ini, WireGuard direkomendasikan untuk implementasi performa tinggi dan seluler. IPSec tetap menjadi pilihan solid untuk aplikasi perusahaan yang membutuhkan standar teruji, sementara OpenVPN sebaiknya dicadangkan untuk kebutuhan yang berfokus pada kompatibilitas. Penelitian selanjutnya perlu dilakukan untuk mengeksplorasi uji lapangan pada lingkungan produksi langsung serta menyelidiki kesiapan protokol terhadap ancaman kriptografi pasca-kuantum (Jiang dkk., 2024).

Sinergi antara arsitektur kernel-space dan kriptografi modern terbukti menjadi faktor krusial dalam melampaui hambatan performa konvensional. Dominasi efisiensi yang teramati bukan sekadar tentang kecepatan mentah, melainkan manifestasi dari desain protokol yang mampu menekan beban komputasi secara ekstrem tanpa mengorbankan integritas data. Penggunaan Indeks Efisiensi Multi-Dimensi dalam

studi ini menggeser paradigma benchmarking dari sekadar pengujian teknis menjadi evaluasi kelayakan operasional yang lebih objektif dan terukur.

Namun, lanskap performa ini tetap terikat pada karakteristik infrastruktur berbasis AMD Ryzen dengan dukungan instruksi AVX2, yang secara inheren memberikan ruang optimasi lebih luas bagi implementasi berbasis kernel dibandingkan arsitektur tingkat pengguna (*user-space*). Ketergantungan pada ekosistem Linux Kernel 6.8+ juga menyisakan ruang diskusi mengenai generalisasi hasil pada manajemen memori sistem operasi yang berbeda, dan karenanya skor efisiensi dan model skalabilitas yang dihasilkan harus dipandang sebagai fondasi awal bagi desain jaringan berskala masif.

Kedepannya, ketahanan kerangka kerja ini perlu diuji terhadap algoritma kriptografi pasca-kuantum (*post-quantum cryptography*) yang diprediksi akan menuntut beban kerja jauh lebih berat (Jiang dkk., 2024). Perluasan pengujian pada arsitektur perangkat keras yang lebih beragam, seperti sistem berbasis ARM, akan menjadi langkah krusial untuk memperkokoh validitas model prediktif ini sebagai standar evaluasi global bagi infrastruktur VPN masa depan.

5. Pernyataan Ketersediaan Data

Seluruh dataset eksperimental dalam format CSV (termasuk hasil *core performance*, matriks korelasi, dan hasil pengujian *stress test*), serta skrip analisis statistik yang digunakan dalam penelitian ini tersedia secara publik di repositori GitHub: https://github.com/riesurya/vpn-efficiency-benchmarking-linux6.8.

DAFTAR PUSTAKA

Akinsolu, M. O., Sangodoyin, A. O., & Uyoata, U. E. (2022). Behavioral Study of Software-Defined Network Parameters Using Exploratory Data Analysis and Regression-Based Sensitivity Analysis. *Mathematics*, *10*(14), 2536. https://doi.org/10.3390/math10142536

Alia, O., Huang, A., Luo, H., Amer, O., Pistoia, M., & Lim, C. (2024). Quantum-safe 10 Gbps Site-to-Site IPsec VPN Tunnel over 46 km Deployed Fibre. *Optical Fiber Communication Conference (OFC) 2024*, Th3B.5. https://doi.org/10.1364/OFC.2024.Th3B.5

Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025). Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions. *Computers*, *14*(8). https://doi.org/10.3390/computers14080326

Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security*, *142*, 103883. https://doi.org/10.1016/j.cose.2024.103883

Bicski, B., & Pekar, A. (2024). Unveiling *Latency*-Induced Service Degradation: A Methodological Approach With Dataset. *IEEE Access*, *12*, 128097–128116. https://doi.org/10.1109/ACCESS.2024.3456588

Budiyanto, S., & Gunawan, D. (2023). Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol. *IEEE Access*, *11*, 60853–60865. https://doi.org/10.1109/ACCESS.2023.3286032

Cano Aguilera, A., Rubio Garcia, C., Lawo, D., Imaña, J. L., Tafur Monroy, I., & Vegas Olmos, J. J. (2024). In-line rate encrypted links using pre-shared post-quantum keys and DPUs. *Scientific Reports*, *14*(1), 21227. https://doi.org/10.1038/s41598-024-71861-x

Donenfeld, J. A. (2017). WireGuard: Next generation kernel network tunnel. *Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS)*. https://doi.org/10.14722/ndss.2017.23160

Esmaeily, A., & Kralevska, K. (2024). Orchestrating Isolated Network Slices in 5G Networks. *Electronics*, *13*(8), 1548. https://doi.org/10.3390/electronics13081548

Vijaya, G., Dhiyanesh, M. S., Hashmi, M., Junaith, K. B., & Kavennesh, B. V. (2024). Robust technique for detecting and blocking of VPN over networks. 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), 1–5. https://doi.org/10.1109/ICONSTEM60960.2024.10568824

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Gentile, A. F., Macrì, D., De Rango, F., Tropea, M., & Greco, E. (2022). A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment. *Future Internet*, *14*(9), 264. https://doi.org/10.3390/fi14090264

Groen, J., D'Oro, S., Demir, U., Bonati, L., Villa, D., Polese, M., Melodia, T., & Chowdhury, K. (2024). Securing O-RAN Open Interfaces. *IEEE Transactions on Mobile Computing*, *23*(12), 11265–11277. https://doi.org/10.1109/TMC.2024.3393430

Hameed, B. H., & Saleh, Z. A. (2023). Progression of the Protection Networking System Depending on International Virtual Private Network. *International Journal of Safety and Security Engineering*, *13*(5), 863–869. https://doi.org/10.18280/ijsse.130510

Jiang, Y., Huang, J., Fan, Y., & Zhu, X. (2024). Design and Implementation of IPsec VPN IoT Gateway System in National Secret Algorithm. *Journal of Cyber Security and Mobility*, 677–700. https://doi.org/10.13052/jcsm2245-1439.1345

Jumakhan, H., & Mirzaeinia, A. (2023). Wireguard: An Efficient Solution for Securing IoT Device Connectivity: Regular Research Paper (CSCI-RTMC). *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 934–940. https://doi.org/10.1109/CSCI62032.2023.00156

Kielland, S., Esmaeily, A., Kralevska, K., & Gligoroski, D. (2022). Secure Service Implementation with Slice Isolation and WireGuard. *2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 148–153. https://doi.org/10.1109/MeditCom55741.2022.9928730

Kjorveziroski, V., Bernad, C., Gilly, K., & Filiposka, S. (2024). Full-mesh VPN performance evaluation for a secure edge-cloud continuum. *Software: Practice and Experience*, *54*(8), 1543–1564. https://doi.org/10.1002/spe.3329

Michael Oladipo Akinsanya, Cynthia Chizoba Ekechi, & Chukwuekem David Okeke. (2024). Virtual Private Networks (Vpn): A Conceptual Review Of Security Protocols And Their Application In Modern Networks. *Engineering Science & Technology Journal*, *5*(4), 1452–1472. https://doi.org/10.51594/estj.v5i4.1076

Oktavia, S. T., Priambodo, D. F., Trianto, N., & Purwoko, R. (2024). Comparative Quality of Service Analysis of VPN Protocols on IPv6. *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, *12*(3), 461–471. https://doi.org/10.23887/janapati.v12i3.69264

Shim, H., Kang, B., Im, H., Jeon, D., & Kim, S.-M. (2025). qTrustNet Virtual Private Network (VPN): Enhancing Security in the Quantum Era. *IEEE Access*, *13*, 17807–17819. https://doi.org/10.1109/ACCESS.2025.3530985

Sura Ghanim Hussein, & Syed Muhammad Fasih Ur Rehman. (2025). Protocol Efficiency and Resource Utilization in VPN Technologies: A Comparative Analysis of OpenVPN and WireGuard. *Journal of Techniques*, *7*(4), 37–42. https://doi.org/10.51173/jt.v7i4.2768

Hussein, S. G., & Rehman, S. M. F. U. (2025). Protocol efficiency and resource utilization in VPN technologies: A comparative analysis of OpenVPN and WireGuard. Journal of Techniques, 7(4), 37–42. https://doi.org/10.51173/jt.v7i4.2768

Tran, S.-N., Hoang, V.-T., & Bui, D.-H. (2023). A Hardware Architecture of NIST Lightweight Cryptography Applied in IPSec to Secure High-*Throughput* Low-*Latency* IoT Networks. *IEEE Access*, *11*, 89240–89248. https://doi.org/10.1109/ACCESS.2023.3306420

Tran, N., Hoang, T., & Bui, H. (2023). A hardware architecture of NIST lightweight cryptography applied in IPSec to secure high-throughput low-latency IoT networks. IEEE Access, 11, 89405–89416. https://doi.org/10.1109/ACCESS.2023.3306420

DOI: https://doi.org/10.54082/jupin.2313
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Halaman ini dikosongkan