JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Analisis Performa WireGuard dan OpenVPN pada VPN Perbankan Berbasis MikroTik menggunakan ICMP, iPerf3, dan Mann–Whitney

Fadhil Muhajir*, Ema Utami

Fakultas Ilmu Komputer, Prodi S2 PJJ Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
Email: [1]*fadhilmuhajir@students.amikom.ac.id, [2]ema.u@amikom.ac.id
Email Penulis Korespondensi: fadhilmuhajir@students.amikom.ac.id
Submitted **22-12-2025;** Accepted **27-01-2026;** Published **24-02-2026**

Abstrak

Industri perbankan membutuhkan konektivitas site-to-site yang aman dan andal antara data center dan kantor cabang untuk mendukung transaksi, replikasi data, dan monitoring yang sensitif terhadap latensi, jitter, serta packet loss. Pada praktiknya, VPN gateway sering berjalan bersamaan dengan fungsi routing dan keamanan, sehingga muncul masalah spesifik berupa trade-off antara kualitas layanan jaringan dan overhead pemrosesan pada perangkat gateway. Karena OpenVPN masih luas digunakan sementara WireGuard semakin diadopsi sebagai protokol yang lebih ringkas, diperlukan bukti terukur untuk menentukan protokol yang paling sesuai pada lingkungan perbankan berbasis router MikroTik. Penelitian ini bertujuan membandingkan kinerja WireGuard dan OpenVPN pada tiga dimensi yaitu kualitas koneksi melalui ICMP Ping (min/avg/max RTT, jitter, packet loss), kapasitas transfer menggunakan iPerf3 pada skenario TCP/UDP (download dan upload), serta efisiensi pemrosesan melalui pemantauan CPU dan memori. Data dirangkum menggunakan statistik deskriptif dan diuji dengan Mann–Whitney U pada kondisi uji setara. Hasil menunjukkan WireGuard memberikan kestabilan delay yang lebih baik (Avg/Max RTT dan jitter lebih rendah) serta penggunaan CPU yang lebih hemat dibanding OpenVPN, sementara throughput bersifat kontekstual yang mana WireGuard cenderung unggul pada skenario UDP dan OpenVPN dapat lebih baik pada TCP tertentu. Kontribusi penelitian ini adalah metodologi uji yang replikatif dan bukti kuantitatif sebagai dasar rekomendasi pemilihan protokol VPN bagi perbankan berdasarkan performa jaringan, efisiensi resource, dan keberlangsungan layanan.

Kata Kunci: WireGuard; OpenVPN; VPN; MikroTik; ICMP; RTT; Jitter; Packet Loss; iPerf3; Throughput; Mann–Whitney

Abstract

The banking industry necessitates secure and reliable site-to-site connectivity between data centres and branch offices to support transactions, data replication, and monitoring that is sensitive to latency, jitter, and packet loss. In practice, VPN gateways often operate concurrently with routing and security functions, leading to specific issues characterised by a trade-off between network service quality and processing overhead on gateway devices. Given that OpenVPN remains widely used while WireGuard is increasingly adopted as a more streamlined protocol, there is a need for measurable evidence to determine the most suitable protocol in a banking environment based on MikroTik routers. This study aims to compare the performance of WireGuard and OpenVPN across three dimensions: connection quality via ICMP Ping (minimum/average/maximum round-trip time, jitter, packet loss), transfer capacity using iPerf3 in TCP/UDP scenarios (download and upload), and processing efficiency through monitoring of CPU and memory usage. Data will be summarised using descriptive statistics and tested with the Mann–Whitney U test under equivalent test conditions. The results indicate that WireGuard provides better delay stability (lower average/maximum round-trip time and jitter) and more efficient CPU utilisation compared to OpenVPN, whereas throughput is context-dependent, with WireGuard generally excelling in UDP scenarios and OpenVPN performing better in certain TCP situations. The contribution of this research lies in the replicable testing methodology and quantitative evidence that serves as a foundation for recommending VPN protocol selection for banking based on network performance, resource efficiency, and service continuity.

Keywords: WireGuard; OpenVPN; VPN; MikroTik; ICMP; RTT; Jitter; Packet Loss; iPerf3; Throughput; Mann–Whitney

1. PENDAHULUAN

Transformasi digital pada industri perbankan menuntut konektivitas antarlokasi (*data center*, *disaster recovery*, kantor cabang, dan titik layanan) yang aman, stabil, dan berperforma tinggi untuk menopang transaksi, sinkronisasi basis data, monitoring, serta aplikasi operasional yang sensitif terhadap latensi, *jitter*, *throughput*, dan *packet loss*. Permasalahan utama pada implementasi *VPN site-to-site* di perbankan adalah munculnya *bottleneck* kinerja akibat *trade-off* antara kebutuhan *QoS* (latensi rendah, *throughput* tinggi, *loss* minimal) dan *overhead* komputasi enkripsi/enkapsulasi pada perangkat *gateway*. Kondisi ini krusial karena *VPN gateway* pada operasional perbankan umumnya berjalan bersamaan dengan fungsi *routing*, *firewall*, kontrol akses, dan pemantauan jaringan sehingga ketika sumber daya *gateway* terbatas atau *overhead* protokol tinggi, dampaknya dapat berupa lonjakan latensi (*tail latency*), *jitter* yang tidak stabil, penurunan *throughput*, hingga degradasi layanan pada jam sibuk. Solusi yang diharapkan dari penelitian ini adalah tersedianya dasar keputusan teknis berbasis bukti untuk memilih protokol *VPN* yang paling sesuai, bukan sekadar berdasarkan popularitas, tetapi berdasarkan kinerja terukur dan efisiensi *resource* pada skenario yang merepresentasikan kebutuhan jaringan perbankan, sejalan dengan kajian arsitektur *VPN gateway* berperforma tinggi yang menekankan pentingnya efisiensi pemrosesan paket dan kriptografi [1].

Dalam praktik, organisasi kerap dihadapkan pada pilihan protokol *VPN* yang berbeda karakteristiknya. *OpenVPN* luas digunakan karena fleksibilitas dan ekosistem dukungan yang matang, namun literatur terbaru juga mengangkat potensi eksposur *OpenVPN* terhadap teknik *fingerprinting* pada kondisi tertentu [2]. Sementara itu, *WireGuard* muncul sebagai alternatif modern dengan desain lebih ringkas dan pilihan kriptografi yang minimalis; bahkan analisis formal menunjukkan *WireGuard* lebih mudah dipelajari dan diverifikasi secara sistematis dibanding rancangan yang kompleks [3]. Dari sisi performa, beberapa studi komparatif melaporkan bahwa *WireGuard* dan *OpenVPN* dapat menunjukkan

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

perbedaan kinerja pada beragam skenario uji, termasuk pada lingkungan *cloud* atau virtualisasi dan kondisi jaringan tersimulasi [4], [5]. Namun, hasil komparasi tersebut tidak selalu dapat digeneralisasi langsung ke konteks operasional perbankan yang memiliki karakteristik link antarcabang dinamis, beban transaksi fluktuatif, dan *SLA* internal yang ketat maka dari itu, diperlukan pengujian yang menempatkan kedua protokol pada kondisi implementasi yang relevan.

Kinerja *VPN* tidak semata ditentukan oleh protokol, tetapi merupakan interaksi antara konfigurasi, karakteristik trafik, kondisi jaringan, serta kemampuan perangkat keras. Studi pada konteks *IoT* dan perangkat *constrained* menegaskan bahwa *overhead* enkripsi dan proses *encapsulation* dapat menurunkan kapasitas layanan, sehingga evaluasi harus memasukkan keterbatasan komputasi *gateway* [6], [7]. Perspektif ini relevan bagi organisasi yang menggunakan *router* sebagai *VPN gateway* atas pertimbangan biaya, ketersediaan, dan kemudahan operasional. *Router MikroTik* juga umum digunakan pada berbagai implementasi *VPN*, termasuk *WireGuard* maupun *tunneling* lain berbasis *MikroTik* [8], [9], serta studi *QoS* pada *MikroTik* menunjukkan pengukuran metrik jaringan dapat menjadi dasar keputusan teknis [10]. Selain itu, pada layanan yang bersifat interaktif, latensi dan *jitter* dapat memengaruhi persepsi kualitas layanan [11], sedangkan *packet loss* dapat menurunkan reliabilitas transmisi pada aplikasi sensitif [12], sehingga parameter kestabilan koneksi menjadi faktor penting pada jaringan perbankan.

Agar evaluasi performa bersifat objektif dan replikatif, diperlukan metodologi uji yang terukur. Pengukuran *ICMP Ping* digunakan untuk menangkap latensi dan variasi *delay* (*jitter*), sedangkan *iPerf3* digunakan untuk menilai *throughput* pada skenario *TCP*/*UDP* karena mampu menghasilkan trafik uji terkontrol [13]. Validasi perilaku trafik dapat didukung dengan analisis paket menggunakan *Wireshark* [14]. Namun, literatur juga mengingatkan potensi ketidakandalan hasil eksperimen apabila lingkungan uji tidak dikendalikan dengan baik, sehingga desain eksperimen harus memastikan konsistensi konfigurasi dan pengulangan pengukuran yang memadai [15]. Oleh karena itu, penelitian ini diposisikan sebagai eksperimen terkontrol dengan konfigurasi yang konsisten untuk membandingkan karakteristik protokol secara lebih adil.

Selain performa, aspek operasional juga penting pada jaringan berskala perbankan. Kesalahan konfigurasi *VPN* dapat memicu risiko keamanan maupun gangguan layanan. Penelitian mengenai otomasi konfigurasi *VPN* menunjukkan bahwa otomasi dapat meningkatkan konsistensi dan mengurangi risiko *human error* pada konfigurasi jaringan [16]. Di sisi lain, keamanan layanan perbankan modern juga berkembang melalui pemanfaatan analitik data real-time untuk mendeteksi dan merespons ancaman secara cepat [17]. Bahkan, diskursus keamanan *VPN* terus bergerak hingga pada isu keamanan era komputasi kuantum [18]. Walaupun fokus penelitian ini adalah kinerja, konteks keamanan tersebut menguatkan urgensi pemilihan protokol *VPN* yang tidak hanya aman, tetapi juga efisien dan stabil untuk mendukung layanan berkelanjutan. Dengan kata lain, protokol yang efisien secara komputasi berpotensi memberi ruang untuk aktivasi kontrol tambahan (misalnya *logging*, inspeksi, atau kebijakan akses) tanpa mengorbankan kualitas layanan.

Tujuan penelitian ini adalah menganalisis dan membandingkan kinerja *VPN WireGuard* dan *OpenVPN* pada konteks jaringan perbankan dengan *router MikroTik* sebagai *VPN gateway* berdasarkan tiga dimensi yaitu kualitas koneksi (*min*/*avg*/*max RTT*, *jitter*, *packet loss*) melalui *ICMP Ping*, kapasitas transfer data melalui *iPerf3* pada skenario *TCP*/*UDP* untuk arah *download* dan *upload*, serta efisiensi *resource gateway* (*CPU* dan memori) sebagai indikator *overhead* komputasi. Hasil pengujian dirangkum menggunakan statistik deskriptif dan diperkuat dengan uji inferensial nonparametrik (*Mann–Whitney U*) untuk menilai signifikansi perbedaan kinerja. Harapan yang ingin dicapai adalah tersusunnya rekomendasi teknis yang dapat dijadikan rujukan institusi perbankan dalam memilih protokol *VPN* yang paling sesuai untuk kebutuhan layanan aman, stabil, dan berkelanjutan, dengan mempertimbangkan performa jaringan, efisiensi *resource*, serta konteks keamanan yang relevan.

2. METODOLOGI PENELITIAN

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini merupakan penelitian kuantitatif dengan pendekatan eksperimental-komparatif untuk membandingkan kinerja protokol *VPN WireGuard* dan *OpenVPN* pada skenario jaringan perbankan. Pendekatan kuantitatif dipilih karena evaluasi dilakukan menggunakan data numerik (misalnya nilai *ping* atau *ICMP*, *throughput*, serta pemakaian *CPU* dan memori) sehingga dapat dianalisis secara objektif. Model komparatif digunakan untuk menilai perbedaan performa kedua protokol pada kondisi uji yang setara, sebagaimana diterapkan dalam studi perbandingan *WireGuard* dan *OpenVPN* pada berbagai lingkungan [4], [19], [5].

Secara eksperimental, pengujian dilakukan pada lingkungan terkontrol dengan konfigurasi yang konsisten agar hasil pengukuran dapat direplikasi. Fokus pengujian mengacu pada kebutuhan performa *gateway VPN* dan karakteristik implementasi nyata, termasuk aspek efisiensi pemrosesan gateway [1] serta dampak keterbatasan perangkat terhadap performa *VPN* [7]. Pengukuran kinerja meliputi *ping* berbasis *ICMP* untuk latensi/stabilitas, throughput menggunakan *iPerf3* (*TCP*/*UDP*) [13], dan pemantauan *resource* perangkat selama *tunnel* aktif. *Wireshark* dapat digunakan sebagai alat bantu verifikasi trafik dan parameter jaringan [14], dengan tetap memperhatikan potensi bias alat atau simulasi sehingga kontrol eksperimen dan pengulangan pengukuran menjadi penting [15].

Data dianalisis menggunakan Statistik Deskriptif untuk merangkum kecenderungan dan sebaran performa, kemudian diuji menggunakan Statistik Inferensial melalui uji nonparametrik *Mann–Whitney U* untuk menentukan signifikansi perbedaan kinerja *WireGuard* dan *OpenVPN* [4], [5].

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

2.2 Tahapan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksperimental–komparatif dengan lingkungan uji terkontrol untuk membandingkan kinerja WireGuard dan OpenVPN pada kondisi yang setara. Tahapan penelitian disusun untuk memastikan proses pengujian replikatif, mulai dari perancangan testbed, implementasi dua skenario VPN, pengukuran parameter (ICMP Ping, iPerf3 TCP/UDP, serta resource gateway), hingga analisis statistik deskriptif dan inferensial menggunakan uji Mann–Whitney U.

Gambar 1. Alur Tahapan Penelitian

Pada Gambar 1 menunjukkan alur penelitian secara berurutan yaitu identifikasi masalah dan tujuan, studi literatur untuk menetapkan variabel uji, perancangan testbed dan skenario eksperimen, implementasi serta pengecekan *baseline* tanpa *VPN*, kemudian pengujian *WireGuard* dan *OpenVPN* secara simetris (*ICMP Ping*, *iPerf3 TCP*/*UDP*, *monitoring CPU*/*memori*). Seluruh data dikumpulkan dan divalidasi, lalu dianalisis dengan statistik deskriptif dan uji *Mann–Whitney U* untuk menentukan signifikansi perbedaan kinerja, sebelum ditarik kesimpulan dan rekomendasi.

Tabel 1. Rincian Tahapan Penelitian, Instrumen, dan Output

Tahap	Aktivitas inti	Input	Output	Instrumen	Kontrol & Validasi
1	Identifikasi masalah, ruang lingkup, dan tujuan	Kebutuhan konektivitas perbankan, isu *QoS* vs *overhead*	Rumusan masalah, tujuan, kontribusi	Dokumen kebutuhan, catatan awal	Batasan penelitian jelas (*VPN site-to-site*; *MikroTik* sebagai *gateway*)
2	Studi literatur & penetapan variabel	Literatur *WireGuard*/*OpenVPN*, metrik performa	Variabel uji: *RTT*/*jitter*/*loss*, *throughput TCP*/*UDP*, *CPU*/memori	Referensi jurnal	Menetapkan parameter dan definisi pengukuran yang konsisten
3	Desain eksperimen & *testbed*	Variabel uji & skenario	Desain topologi *DC*–Cabang, skenario *WireGuard* vs *OpenVPN*	Diagram/topologi	Menyamakan kondisi uji (*link*, *host*, *routing*, *firewall* dasar)
4	Implementasi lingkungan uji + *baseline*	Konfigurasi IP, rute, *firewall* dasar	Konektivitas dasar stabil tanpa *VPN*	*MikroTik*, *host* uji	Uji *ping baseline*; memastikan tidak ada *bottleneck non-VPN*
5	Implementasi skenario WireGuard	Parameter *WireGuard* & *routing*	*Tunnel WireGuard* aktif & terverifikasi	*MikroTik RouterOS*, utilitas *ping*	Verifikasi koneksi *end-to-end* sebelum uji beban
6	Pengujian *WireGuard* (pengumpulan data)	*Tunnel WireGuard* aktif	*Dataset WireGuard*: *ICMP*, *iPerf3 TCP*/*UDP*, *CPU*/memori	*Ping*/*ICMP*, *iPerf3*, *monitoring CPU*/mem	Pengulangan uji (replikasi) & kondisi uji stabil
7	Implementasi skenario *OpenVPN*	Parameter *OpenVPN* & *routing*	*Tunnel OpenVPN* aktif & terverifikasi	*MikroTik RouterOS*	Menyelaraskan tingkat keamanan mendekati *WireGuard*
8	Pengujian *OpenVPN* (pengumpulan data)	*Tunnel OpenVPN* aktif	*Dataset OpenVPN*: *ICMP*, *iPerf3 TCP*/*UDP*, *CPU*/memori	*Ping*/*ICMP*, *iPerf3*, *monitoring CPU*/mem	Menjaga jam uji, beban lain, dan konfigurasi semirip mungkin

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

9	Pencatatan & pengelolaan data	*Log* hasil uji	Data terstruktur per parameter & skenario	*CSV*/*log*, *spreadsheet*	Validasi trafik (opsional *via Wireshark*)
10	Analisis statistik deskriptif	*Dataset WG & OVPN*	Ringkasan *mean*/*median*/*std*/*min*/*max* & visualisasi	*Excel*/*SPSS*/*R*/*Python*	Cek outlier & konsistensi satuan/format
11	Analisis inferensial (*Mann–Whitney U*)	Ringkasan + *dataset*	Keputusan signifikansi per parameter	Uji *Mann–Whitney U*	α=0,05; interpretasi p-value terhadap H0/H1
12	Interpretasi & rekomendasi	*Output* analisis	Kesimpulan & rekomendasi protokol *VPN*	Penulisan *paper*	Konsisten dengan tujuan & konteks perbankan

Pada Tabel 1 merangkum setiap tahap penelitian beserta *input–output*, *tools* yang digunakan, dan kontrol validasi. Tabel ini menegaskan bagaimana kondisi uji dijaga tetap setara (*baseline* stabil, konfigurasi inti sama, pengulangan pengukuran, serta penyelarasan keamanan) sehingga perbedaan hasil lebih merefleksikan perbedaan protokol *WireGuard* dan *OpenVPN*, bukan faktor lingkungan.

2.3 Lingkungan Penelitian dan Topologi Jaringan

Penelitian ini dilaksanakan pada lingkungan uji yang merepresentasikan jaringan perbankan (konektivitas *data center*–kantor cabang) dengan fokus pada evaluasi kinerja VPN gateway. Lingkungan penelitian dirancang sebagai *testbed* terkontrol agar perbandingan *WireGuard* dan *OpenVPN* dilakukan pada kondisi yang setara, selaras dengan rekomendasi penelitian arsitektur *high-performance VPN gateway* yang menekankan pentingnya konsistensi desain dan jalur pemrosesan paket pada *gateway* [1]. Selain itu, rancangan *testbed* mempertimbangkan bahwa performa *VPN* dipengaruhi oleh karakteristik perangkat dan beban trafik, sebagaimana ditemukan pada studi evaluasi *VPN* di lingkungan *IoT* dan perangkat dengan keterbatasan sumber daya [6], [7].

a. Lingkungan Penelitian

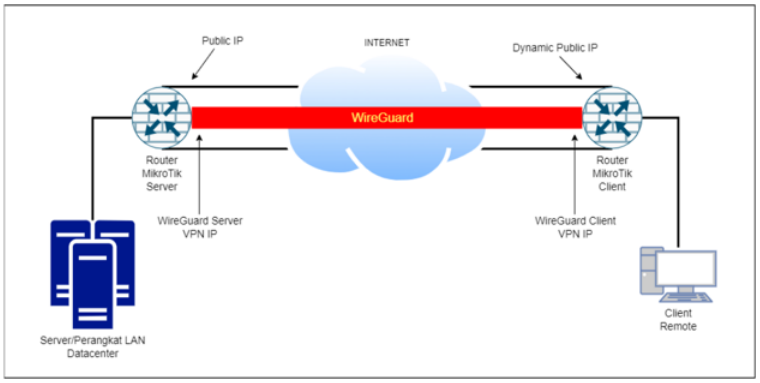
Lingkungan penelitian terdiri dari komponen utama berikut:

1. Dua titik jaringan: sisi *Data Center* (*DC*) dan sisi Cabang, yang dihubungkan melalui jaringan *WAN*/*Internet* (atau jaringan pengganti yang dikondisikan). Model dua titik ini umum digunakan pada studi perbandingan *WireGuard* dan *OpenVPN* untuk mengukur performa *end-to-end* secara objektif [4], [5].
2. *VPN Gateway*: masing-masing sisi menggunakan *router MikroTik* sebagai terminasi *VPN* (*endpoint*) sehingga skenario menyerupai implementasi riil pada organisasi yang memanfaatkan *router* komersial untuk *tunneling* terenkripsi [10], [8], [9].
3. Host penguji (*traffic endpoints*): perangkat klien/server di belakang gateway *DC* dan Cabang yang digunakan untuk menghasilkan trafik uji (*iPerf3*) dan pengukuran *ping*/*ICMP*. Penggunaan *iPerf3* untuk pengukuran *throughput* merupakan pendekatan yang lazim dan relevan dalam evaluasi kapasitas transfer jaringan [13].
4. Perangkat monitoring/analisis: pencatatan parameter performa dan validasi trafik dapat didukung oleh *Wireshark* untuk mengamati karakteristik paket serta memastikan skenario uji berjalan sesuai desain [14].

Agar hasil tidak bias, penelitian ini memperhatikan prinsip kontrol eksperimen seperti konfigurasi *IP*, rute, kebijakan *firewall* dasar, dan parameter *VPN* dibuat konsisten antara skenario *WireGuard* dan *OpenVPN*. Hal ini penting karena literatur menunjukkan hasil performa dapat bergantung pada konfigurasi dan lingkungan uji, bahkan pada pengujian berbasis simulasi dapat terjadi ketidakandalan bila kontrol tidak memadai [15]. Pada konteks operasional, konsistensi konfigurasi juga sejalan dengan tren otomasi konfigurasi *VPN* untuk mengurangi risiko misconfiguration pada jaringan [16].

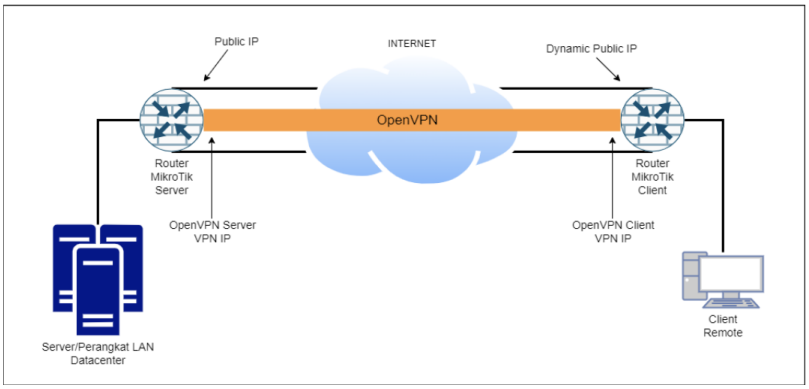
b. Topologi Jaringan Penelitian

Topologi yang digunakan adalah *site-to-site VPN* (*DC*–Cabang) dengan pola *router-to-router*, karena model ini paling relevan untuk interkoneksi antar lokasi pada institusi yang memiliki banyak cabang [16], [17]. Secara konseptual, topologi dapat ditunjukkan pada Gambar 2 dan Gambar 3 sebagai berikut:



Gambar 2. Topologi Jaringan *WireGuard*

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom



Gambar 3. Topologi Jaringan *OpenVPN*

Berdasarkan Gambar 2 dan Gambar 3, host uji ditempatkan pada LAN untuk memastikan pengukuran mencerminkan *end-to-end* setelah melewati proses enkripsi, *encapsulation*, dan *routing* pada *gateway*. Desain ini sesuai dengan praktik evaluasi performa *VPN* yang menempatkan generator trafik di belakang *gateway* agar metrik yang dihasilkan merefleksikan *overhead* protokol secara nyata [4], [5], [20]. Untuk menguji performa secara komprehensif, topologi ini mendukung:

1. Pengujian latensi/kestabilan menggunakan *Ping* (*ICMP*) dari *host DC* ke *host* Cabang melalui *tunnel VPN*.
2. Pengujian throughput menggunakan *iPerf3* (*TCP*/*UDP*) antar *host DC*–Cabang melalui *tunnel VPN* [13].
3. Pengamatan *resource* pada *router MikroTik* (*CPU* dan memori) selama tunnel aktif dan saat beban trafik berjalan, mengingat studi pada perangkat terbatas menegaskan pentingnya menilai *overhead* komputasi selain metrik jaringan [7].

2.4 Perangkat Keras dan Perangkat Lunak

a. Perangkat Keras

Secara umum, perangkat keras yang digunakan dalam penelitian ini meliputi :

1. Dua unit *router Mikrotik* yang berfungsi sebagai *VPN gateway* pusat dan cabang.
2. Dua unit komputer/host uji (*server* dan *client*) untuk menjalankan *ping* dan *iPerf3*.
3. Perangkat pendukung lainnya seperti *switch* dan kabel jaringan sesuai kebutuhan.

Spesifikasi rinci (model, kapasitas *CPU*, *RAM*, dan versi perangkat) dicatat untuk mendukung replikasi penelitian dan interpretasi hasil, mengingat keterbatasan sumber daya perangkat dapat memengaruhi performa *VPN* pada lingkungan *constrained hardware* [3].

b. Perangkat Lunak

Perangkat lunak utama yang digunakan adalah sebagai berikut :

1. Sistem operasi pada *host* uji (misalnya *Linux*/*Windows*) yang mendukung utilitas *ping* dan *iPerf3*.
2. Implementasi *WireGuard* dan *OpenVPN* pada *Mikrotik* sesuai dukungan *RouterOS*.
3. Aplikasi *iPerf3* sebagai sebuah *benchmarking tool* jaringan yang digunakan untuk mengukur *throughput* (kecepatan transfer data) antara dua *host* secara akurat menggunakan protokol *TCP* atau *UDP*.
4. *Traffic*/*Resource monitor* pada *Mikrotik* (misalnya *CPU usage*, *memory usage*, dan *interface traffic*) untuk mengamati pemanfaatan *resource*.
5. Perangkat lunak analisis data dan statistik (misalnya *Microsoft Excel*, *SPSS*, *R*, atau *Python*) untuk pengolahan Statistik Deskriptif dan uji *U Mann-Whitney*.

2.5 Parameter Pengukuran

Penelitian ini memfokuskan pengukuran pada tiga kelompok utama parameter performa :

a. Parameter *ICMP*/*Ping* (*Latency* dan *Packet Loss*)
   1. Pengukuran dilakukan menggunakan perintah ping (*ICMP Echo Request*/*Reply*) dari host cabang ke host pusat melalui *tunnel VPN*.
   2. Nilai yang dicatat mencakup minimum *RTT*, rata-rata *RTT*, maksimum *RTT*, *standard deviation RTT* (jika tersedia), serta persentase *packet loss*.
   3. Pengukuran diulang beberapa kali dalam jangka waktu tertentu (misalnya beberapa putaran ping dengan jumlah paket tertentu) untuk mendapatkan distribusi data yang memadai.

b. Parameter *Throughput* (*iPerf3*)
   1. *Throughput* diukur menggunakan *iPerf3* dengan konfigurasi satu *host* sebagai *server* dan *host* lainnya sebagai *client*.
   2. Pengujian dilakukan dalam mode *TCP* (dan dapat diperluas ke *UDP* jika diperlukan), dengan durasi uji tertentu per sesi (misalnya 30–60 detik) dan jumlah pengulangan yang cukup.
   3. Nilai yang dicatat berupa *throughput* rata-rata per sesi pengujian (dalam *Mbps*) untuk masing-masing protokol *VPN*.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

c. Parameter *Resource Mikrotik*
   1. Penggunaan *CPU* dan memori pada *router Mikrotik* dipantau selama pengujian ping dan *iPerf3* berlangsung.
   2. Nilai yang dicatat dapat berupa rata-rata penggunaan *CPU*, puncak (maksimum) penggunaan *CPU*, serta rata-rata penggunaan memori, untuk masing-masing protokol.
   3. Pengukuran dilakukan untuk menilai efisiensi pemanfaatan *resource* ketika *router* menjalankan *tunnel WireGuard* maupun *OpenVPN*, relevan dengan studi yang menyoroti pengaruh protokol *VPN* terhadap perangkat berdaya terbatas [1], [6], [3].

2.6 Prosedur Pengumpulan Data

Prosedur pengumpulan data dilakukan melalui beberapa tahapan berikut :

a. Konfigurasi Awal Jaringan
   1. Mengkonfigurasi alamat *IP*, rute, dan *firewall* dasar pada kedua *router Mikrotik*.
   2. Memastikan konektivitas dasar (tanpa *VPN*) antara host pusat dan cabang berjalan dengan baik.

b. Konfigurasi Skenario *WireGuard*
   1. Mengkonfigurasi *interface WireGuard* dan parameter kriptografi pada kedua *router*.
   2. Menambahkan rute agar trafik antara jaringan pusat dan cabang melewati *tunnel WireGuard*.
   3. Melakukan uji konektivitas awal (*ping test*) untuk memastikan *tunnel* berfungsi.

c. Pengukuran pada Skenario WireGuard
   1. Menjalankan *ping* (*ICMP*) dari *host* cabang ke *host* pusat dengan jumlah paket dan interval tertentu.
   2. Menjalankan *iPerf3* untuk mengukur throughput sesuai konfigurasi yang ditetapkan.
   3. Mencatat *log* hasil *ping*, hasil *iPerf3*, serta *data resource Mikrotik* (*CPU*, memori) selama pengujian.
   4. Mengulang pengujian sesuai jumlah replikasi yang telah direncanakan untuk memperoleh data yang cukup secara statistik.

d. Konfigurasi Skenario *OpenVPN*
   1. Menonaktifkan tunnel *WireGuard* dan mengkonfigurasi *tunnel OpenVPN* pada kedua *router*.
   2. Menyelaraskan parameter kriptografi *OpenVPN* agar tingkat keamanan mendekati skenario *WireGuard*.
   3. Menguji kembali konektivitas awal melalui *ping* untuk memastikan *tunnel* berfungsi.

e. Pengukuran pada Skenario *OpenVPN*
   1. Mengulangi rangkaian pengujian yang sama seperti pada skenario *WireGuard* (*ICMP*/*ping*, *iPerf3*, dan pemantauan *resource*).
   2. Menjamin bahwa kondisi lingkungan (jam pengujian, beban trafik lain, dan konfigurasi jaringan) dibuat semirip mungkin agar hasil komparasi valid.

f. Pencatatan dan Pengelolaan Data
   1. Seluruh hasil pengukuran disimpan dalam format *log* atau *CSV*.
   2. Data kemudian diorganisasikan ke dalam tabel per parameter dan per skenario (*WireGuard* vs *OpenVPN*) sebagai dasar analisis lebih lanjut.

2.6 Teknik Analisis Data

Analisis data dalam penelitian ini dibagi menjadi dua kelompok, yaitu Statistik Deskriptif dan Statistik Inferensial.

a. Statistik Deskriptif

Statistik Deskriptif digunakan untuk menyajikan gambaran umum karakteristik data performa yang diukur pada masing-masing protokol *VPN*. Parameter statistik yang dihitung antara lain :

1. Nilai rata-rata (*mean*)
2. Nilai tengah (*median*)
3. *Standard deviation*
4. Nilai minimum dan maksimum

Perhitungan dilakukan untuk setiap parameter (*RTT*, *throughput*, *CPU usage*, dan memori) pada masing-masing protokol. Hasil Statistik Deskriptif disajikan dalam bentuk tabel dan visualisasi (misalnya grafik batang atau *boxplot*) untuk memudahkan interpretasi perbedaan pola distribusi data antara *WireGuard* dan *OpenVPN*.

b. Statistik Inferensial dengan Uji *U Mann-Whitney*

Karena data performa jaringan sering kali tidak berdistribusi normal dan dapat dipengaruhi oleh fluktuasi trafik maupun kondisi jaringan yang dinamis, penelitian ini menggunakan uji non-parametrik *U Mann-Whitney* sebagai bagian dari Statistik Inferensial untuk menguji perbedaan performa antara *WireGuard* dan *OpenVPN*. Formulasi hipotesis yang digunakan adalah :

1. H_0 : Tidak terdapat perbedaan yang signifikan secara statistik antara performa *WireGuard* dan *OpenVPN* untuk parameter yang diuji (distribusi data kedua kelompok sama).
2. H_1 : Terdapat perbedaan yang signifikan secara statistik antara performa *WireGuard* dan *OpenVPN* untuk parameter yang diuji.

Uji *U Mann-Whitney* diterapkan untuk setiap parameter (*RTT*, *throughput*, *CPU usage*, memori) dengan tingkat signifikansi (α) yang ditetapkan (misalnya 0,05). Hasil uji yang menunjukkan *p-value* < α diinterpretasikan sebagai adanya perbedaan performa yang signifikan secara statistik antara kedua protokol. Dengan demikian, keputusan

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

pemilihan protokol *VPN* pada konteks infrastruktur jaringan perbankan dapat didasarkan pada temuan yang tidak hanya deskriptif, tetapi juga teruji secara inferensial.

2.7 Kajian Literatur

Studi komparatif *WireGuard* dan *OpenVPN* telah menjadi fokus penelitian karena kedua protokol banyak digunakan dan menunjukkan karakteristik performa yang berbeda. Mackey dkk. [4] memberikan rujukan awal yang secara langsung membandingkan *WireGuard* vs *OpenVPN* melalui pengujian performa. Paper ini relevan sebagai *baseline* karena menegaskan bahwa perbedaan protokol dapat memengaruhi hasil metrik kinerja, sehingga pendekatan eksperimen dan pengukuran kuantitatif diperlukan untuk memperoleh kesimpulan yang objektif.

Anyam dkk. [5] memperluas pembandingan tersebut pada lingkungan *cloud* dan virtualisasi dengan kondisi jaringan tersimulasi. Temuan utamanya menunjukkan bahwa hasil komparasi performa sangat dipengaruhi oleh kondisi jaringan dan lingkungan implementasi, sehingga studi perbandingan perlu dilakukan pada skenario yang sesuai konteks (misalnya jaringan perbankan) dengan kontrol variabel dan pengulangan yang memadai.

Selain metrik jaringan, Gentile dkk. [7] menekankan pentingnya evaluasi *overhead* komputasi pada perangkat *gateway*, terutama pada *hardware* terbatas. Perspektif ini mendukung pengukuran *resource* (*CPU*/memori) sebagai indikator penting, karena keterbatasan perangkat dapat menjadi faktor pembatas *throughput* maupun kestabilan koneksi ketika *tunnel* aktif.

Dari sisi arsitektur sistem, Fu dkk. [1] menyoroti bahwa *VPN gateway* dapat menjadi *bottleneck* sehingga desain pemrosesan paket dan efisiensi implementasi berpengaruh terhadap *throughput* dan latensi. Ini menguatkan alasan mengapa evaluasi performa harus mempertimbangkan kemampuan gateway memproses trafik secara konsisten.
Terakhir, Xue dkk. [2] menambahkan konteks keamanan dengan menunjukkan potensi *VPN fingerprinting* pada *OpenVPN*. Walau fokusnya bukan performa, paper ini relevan untuk perbankan karena rekomendasi pemilihan protokol sebaiknya mempertimbangkan aspek kinerja sekaligus risiko implementasi. Kombinasi literatur [1], [4], [5], [7], dan [2] menjadi dasar untuk merancang uji komparatif yang terukur pada jaringan perbankan menggunakan metrik *ping*/*ICMP*, *throughput* (*iPerf3*), serta *resource gateway*.

3. HASIL DAN PEMBAHASAN

3.1 Statistik Deskriptif

Statistik deskriptif pada penelitian ini digunakan untuk menyajikan gambaran umum mengenai karakteristik data performa jaringan yang diperoleh dari pengujian *VPN WireGuard* dan *OpenVPN*. Analisis ini mencakup perhitungan nilai rata-rata (*mean*), deviasi standar (*standard deviation*), nilai minimum (*min*), dan nilai maksimum (*max*) untuk beberapa parameter utama, yaitu :

a. Parameter kualitas layanan jaringan berbasis *ICMP* (*ping*) seperti *Min RTT*, *Avg RTT*, *Max RTT*, *jitter*, dan *packet loss*.
b. Parameter *throughput* (rata-rata dan maksimum) berdasarkan arah trafik (*Download*/*Upload*) dan jenis protokol (*TCP*/*UDP*).
c. Parameter *resource Mikrotik* seperti pemakaian *CPU* dan memori.

Hasil statistik deskriptif disajikan dalam bentuk tabel untuk menampilkan nilai-nilai numerik secara rinci, serta grafik batang dan boxplot untuk memvisualisasikan perbandingan antara *WireGuard* dan *OpenVPN* secara lebih intuitif.

3.1.1 *Ping* (*ICMP*)

Pengujian Ping berbasis *ICMP* digunakan untuk menggambarkan kualitas konektivitas dasar pada jalur *VPN*, khususnya dari sisi latensi (*RTT*), kestabilan *delay* (*jitter*), serta keandalan pengiriman paket (*packet loss*). Dalam konteks jaringan perbankan, metrik ini penting karena transaksi, akses layanan inti, dan aplikasi operasional membutuhkan *delay* yang stabil serta kehilangan paket minimal. Secara konseptual, *VPN gateway* yang berorientasi performa dituntut mampu menjaga *overhead* enkapsulasi dan kriptografi agar tidak memicu lonjakan *RTT* yang berulang [1], sementara studi komparatif *WireGuard* vs *OpenVPN* umumnya menilai keunggulan dari sisi efisiensi protokol dan dampaknya pada latensi/*jitter* [4], [5].

Tabel 2. Statistik Deskriptif Parameter *Ping* (*WireGuard* dan *OpenVPN*)

Parameter	Mean	Std Dev	Min	Max
Min RTT (ms)	98.238	6.397	91.00	133.0
Avg RTT (ms)	113.423	10.902	98.74	158.0
Max RTT (ms)	323.976	387.525	120.00	2614.0
Jitter (ms)	23.361	42.566	4.70	278.9
Packet Loss (%)	0.262	0.734	0.00	3.0

Tabel 2 merangkum karakteristik data ping secara global (gabungan seluruh pengujian). Nilai *Min RTT* memiliki *mean* 98,238 ms dengan rentang 91–133 ms, menunjukkan *baseline delay* jaringan relatif berada di kisaran ~100 ms.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Nilai *Avg RTT* memiliki *mean* 113,423 ms (*min* 98,74 ms, *max* 158 ms), yang menegaskan bahwa rata-rata *delay* umumnya masih terkendali namun terdapat variasi antar-sampel.
Temuan paling menonjol pada level global muncul pada *Max RTT* yaitu *mean* 323,976 ms dengan maksimum mencapai 2614 ms dan deviasi standar 387,525 ms. Ini mengindikasikan adanya *spike*/*latency burst* pada sebagian observasi. Pada layanan perbankan, lonjakan *RTT* seperti ini berpotensi menurunkan respons aplikasi (*timeout*, retransmisi, atau penurunan pengalaman pengguna), sejalan dengan literatur yang menekankan sensitivitas pengalaman layanan terhadap latensi.

Selanjutnya, *jitter* global memiliki *mean* 23,361 ms dengan maksimum 278,9 ms (*Std Dev* 42,566 ms). *Jitter* tinggi menandakan *delay* yang tidak konsisten. Pada aplikasi *real-time* (misalnya komunikasi suara/*video* operasional), *jitter* sering lebih kritis dibanding rata-rata *RTT* [13]. Untuk *packet loss*, *mean* global tercatat 0,262% dengan maksimum 3%. Walau nilai rata-ratanya kecil, literatur menunjukkan bahwa *loss* (terutama bila terjadi beruntun) dapat berdampak signifikan pada kualitas layanan tertentu [12].

Tabel 3. Statistik Deskriptif *Min*, *AVG*, *Max RTT* per *VPN* (*WireGuard vs OpenVPN*)

VPN	Min RTT (ms) mean	Min RTT (ms) std	Min RTT (ms) min	Min RTT (ms) max	Avg RTT (ms) mean	Avg RTT (ms) std	Avg RTT (ms) min	Avg RTT (ms) max	Max RTT (ms) mean	Max RTT (ms) std	Max RTT (ms) min	Max RTT (ms) max
OpenVPN	97.667	3.307	92.0	104.0	118.192	11.187	105.33	158.0	466.857	503.807	155.0	2614.0
WireGuard	98.810	8.501	91.0	133.0	108.654	8.411	98.74	141.0	181.095	105.675	120.0	520.0

Tabel 3 memecah *RTT* berdasarkan protokol *VPN* sehingga perbandingan menjadi lebih jelas. Pada *Min RTT*, *OpenVPN* memiliki *mean* 97,667 ms, sedangkan *WireGuard* 98,810 ms. Perbedaannya kecil sehingga dapat diinterpretasikan bahwa *baseline* jalur (propagasi + kondisi jaringan) relatif sama pada kedua skenario.
Perbedaan mulai terlihat pada *Avg RTT* yang mana *OpenVPN* memiliki *mean* 118,192 ms, sedangkan *WireGuard* lebih rendah yaitu 108,654 ms. Artinya, secara rata-rata *WireGuard* memberikan latensi yang lebih baik (lebih responsif) pada kondisi uji ini. Temuan ini konsisten dengan banyak studi komparatif yang sering melaporkan *WireGuard* lebih efisien untuk beban tertentu dibanding *OpenVPN* [4], [5].

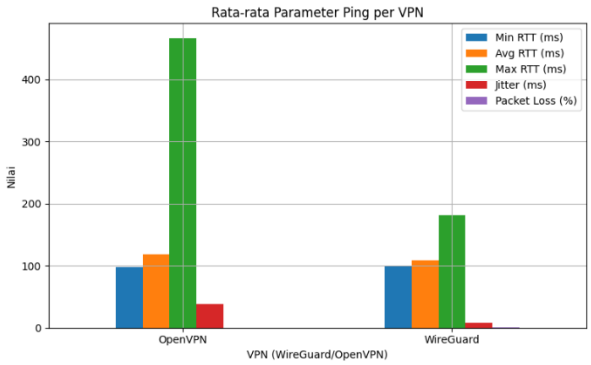
Kontras paling besar ada pada *Max RTT*. *OpenVPN* menunjukkan *mean* 466,857 ms dengan maksimum 2614 ms serta deviasi standar 503,807 ms, sedangkan *WireGuard mean* 181,095 ms dengan maksimum 520 ms dan standar standar 105,675 ms. Ini menguatkan indikasi bahwa pada pengujian ini, *OpenVPN* mengalami *spike* latensi jauh lebih ekstrem dan lebih sering, sementara *WireGuard* lebih stabil dan "*bounded*" (lonjakan tertinggi masih relatif jauh lebih rendah). Dari sudut pandang *gateway VPN*, lonjakan *RTT* yang besar bisa terkait dengan *overhead* pemrosesan/enkripsi, antrean, atau kondisi jaringan sesaat; karena itu pendekatan arsitektur *gateway* berperforma tinggi menekankan efisiensi jalur pemrosesan paket untuk mengurangi *delay burst* [1].

Tabel 4. Statistik Deskriptif *Jitter* dan *Packet Loss* per *VPN* (*WireGuard vs OpenVPN*)

VPN	Jitter (ms) mean	Jitter (ms) std	Jitter (ms) min	Jitter (ms) max	Packet Loss (%) mean	Packet Loss (%) std	Packet Loss (%) min	Packet Loss (%) max
OpenVPN	39.050	56.485	9.73	278.90	0.000	0.000	0.0	0.0
WireGuard	7.672	2.601	4.70	14.47	0.524	0.981	0.0	3.0

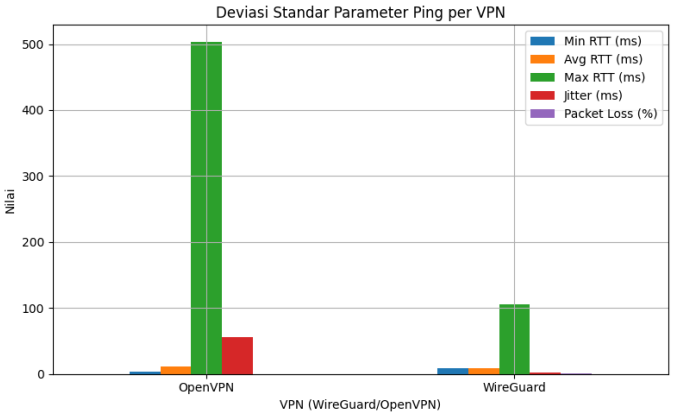
Tabel 4 memperlihatkan kualitas kestabilan *delay* dan reliabilitas paket. *Jitter OpenVPN* memiliki *mean* 39,050 ms (maks 278,90 ms, *Std Dev* 56,485 ms), sedangkan *WireGuard mean* 7,672 ms (maks 14,47 ms, *Std Dev* 2,601 ms). Secara praktis, *jitter WireGuard* jauh lebih rendah dan lebih konsisten. Ini penting karena jitter tinggi berpotensi memicu penurunan kualitas aplikasi sensitif *delay* (misalnya sesi interaktif), walaupun rata-rata *RTT* terlihat "cukup baik".

Untuk *packet loss*, *OpenVPN* pada *dataset* ini tercatat 0% di seluruh observasi (mean 0, min 0, max 0), sedangkan *WireGuard* memiliki *mean* 0,524% dengan maksimum 3%.



Gambar 4. Rata-Rata Parameter *Ping* per *VPN*

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom



Gambar 5. Deviasi Standar Parameter *Ping* per *VPN*

Gambar 5 merangkum perbandingan nilai rata-rata semua parameter *ping* per *VPN*. Visualisasi ini memperjelas pola dari Tabel 2–3, batang *Avg RTT*, *Max RTT*, dan *Jitter* pada *OpenVPN* lebih tinggi dibanding *WireGuard*, sedangkan *packet loss* terlihat hanya muncul pada *WireGuard* (*OpenVPN* ≈ 0). Sementara itu, Gambar 5 menampilkan deviasi standar per parameter yang merepresentasikan kestabilan. *OpenVPN* menunjukkan deviasi standar yang sangat besar terutama pada *Max RTT* dan *jitter*, sejalan dengan adanya lonjakan ekstrem (*outlier*). *WireGuard* memperlihatkan deviasi standar yang lebih kecil, artinya performa *delay* lebih konsisten.

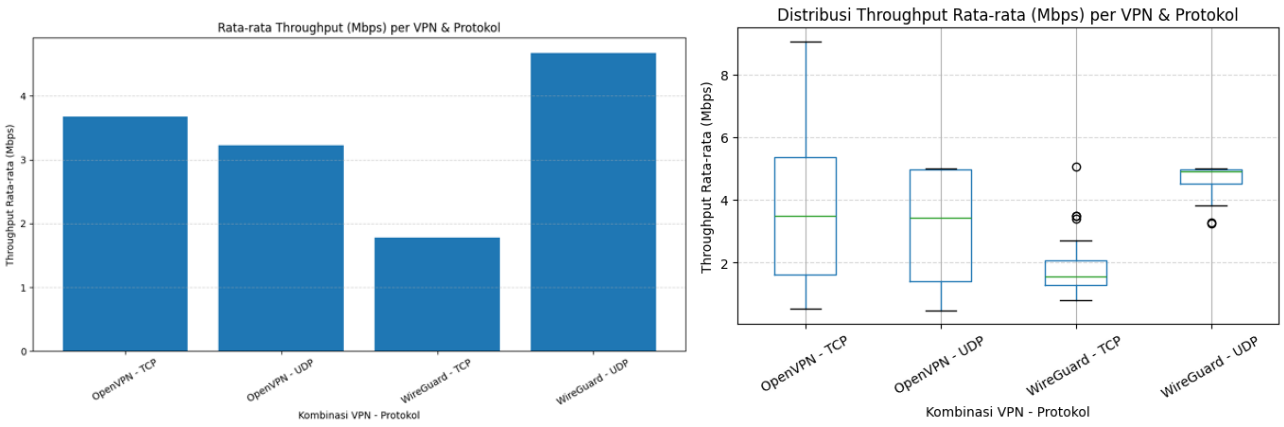
3.1.2 *Throughput*

Berdasarkan Tabel 5, *throughput* rata-rata menunjukkan pola yang berbeda ketika dipisahkan menurut protokol *transport* (*TCP*/*UDP*). Pada *OpenVPN–TCP*, *throughput* rata-rata tercatat 3,678 Mbps dengan variasi yang tinggi (*StdDev* 2,150) dan rentang nilai yang lebar (0,52–9,06 Mbps). Pada *OpenVPN–UDP*, *throughput* rata-rata sedikit lebih rendah (3,222 Mbps) dengan variasi yang juga cukup besar (StdDev 1,684) dan rentang 0,46–5,00 Mbps. Sebaliknya, *WireGuard–UDP* memberikan *throughput* rata-rata tertinggi yaitu 4,677 Mbps serta paling stabil (*StdDev* 0,456) dengan rentang 3,23–5,00 Mbps. Namun pada *WireGuard–TCP*, *throughput* rata-rata justru menjadi yang terendah (1,780 Mbps) walaupun variasinya relatif lebih kecil (*StdDev* 0,825) dengan rentang 0,80–5,07 Mbps.

Tabel 5. Statistik *Throughput* Rata-rata (Mbps) per *VPN,* Protokol dan Arah Tes

#	VPN	Jenis Protokol	N	Mean	StdDev	Min	Max	Arah Tes	N	Mean	StdDev	Min	Max
0	OpenVPN	TCP	42	3.678	2.150	0.52	9.06	Download	42	1.913	1.123	0.46	4.16
1	OpenVPN	UDP	42	3.222	1.684	0.46	5.00	Upload	42	4.987	1.210	3.05	9.06
2	WireGuard	TCP	42	1.780	0.825	0.80	5.07	Download	42	3.260	1.515	0.80	5.07
3	WireGuard	UDP	42	4.677	0.456	3.23	5.00	Upload	42	3.196	1.700	1.01	5.00

Pada Tabel 5, terlihat adanya asimetri performa antara arah *download* dan *upload*. Untuk *OpenVPN*, *throughput download* rata-rata hanya 1,913 Mbps (*StdDev* 1,123, rentang 0,46–4,16 Mbps), sedangkan *upload* rata-rata jauh lebih tinggi yaitu 4,987 Mbps (*StdDev* 1,210, rentang 3,05–9,06 Mbps). Untuk *WireGuard*, nilai *download* rata-rata 3,260 Mbps (*StdDev* 1,515, rentang 0,80–5,07 Mbps) dan *upload* rata-rata 3,196 Mbps (*StdDev* 1,700, rentang 1,01–5,00 Mbps).



Gambar 6. Rata-rata dan Distribusi Throughput (Mbps) per VPN dan Protokol

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Gambar 6 menegaskan temuan Tabel 4 melalui visualisasi distribusi (*boxplot*). Kombinasi *OpenVPN–TCP* dan *OpenVPN–UDP* tampak memiliki sebaran yang lebih lebar (variabilitas tinggi), sedangkan *WireGuard–UDP* memperlihatkan sebaran paling rapat (stabil/konsisten) di sekitar ~5 Mbps. Sementara itu *WireGuard–TCP* cenderung berada pada *throughput* yang lebih rendah dengan beberapa *outlier* bernilai lebih tinggi.

3.1.3 *Resource Mikrotik*

Secara umum, penggunaan *resource Mikrotik* selama pengujian pada Tabel 6 menunjukkan beban yang relatif rendah dimana *CPU Avg* rata-rata 1,444% dengan *CPU Max* rata-rata 3,595%. Sementara itu, *Memory Used Avg* rata-rata 20,465 dan *Memory Used Max* rata-rata 20,810 (sesuai satuan pada *RouterOS*/monitoring yang digunakan). Ini mengindikasikan bahwa perbedaan performa yang muncul lebih dominan berasal dari efisiensi pemrosesan (*CPU*) dibanding perubahan konsumsi memori.

Tabel 6. Statistik Deskriptif Global (semua *VPN*)

Parameter	Mean	Std Dev	Min	Max
CPU Avg (%)	1.444	0.510	0.57	2.71
CPU Max (%)	3.595	1.531	1.00	6.00
Memory Used Avg (%)	20.465	0.769	18.80	22.00
Memory Used Max (%)	20.810	0.671	20.00	22.00

Berdasarkan Tabel 7 menjelaskan:

a. *CPU Avg*: *OpenVPN* memiliki *mean* 1,806%, sedangkan *WireGuard mean* 1,082%. Artinya, *WireGuard* ~40% lebih hemat *CPU* rata-rata dibanding *OpenVPN* pada skenario ini.
b. *CPU Max*: *OpenVPN* memiliki *mean* 4,857%, sedangkan *WireGuard mean* 2,333% sehingga puncak beban *CPU WireGuard* ~52% lebih rendah.
c. Dari sisi kestabilan, deviasi standar *WireGuard* juga lebih kecil (*CPU Avg std* 0,283 vs 0,423; *CPU Max std* 0,730 vs 0,964) sehingga fluktuasi beban *CPU* cenderung lebih stabil.

Tabel 7. Statistik Deskriptif *CPU Avg* dan *CPU Max* per *VPN* (*WireGuard vs OpenVPN*)

VPN	CPU Avg (%) mean	CPU Avg (%) std	CPU Avg (%) min	CPU Avg (%) max	CPU Max (%) mean	CPU Max (%) std	CPU Max (%) min	CPU Max (%) max
OpenVPN	1.806	0.423	1.10	2.71	4.857	0.964	3.0	6.0
WireGuard	1.082	0.283	0.57	1.67	2.333	0.730	1.0	4.0

Pada Tabel 8 Perbedaan konsumsi memori terlihat lebih kecil dibanding *CPU*:

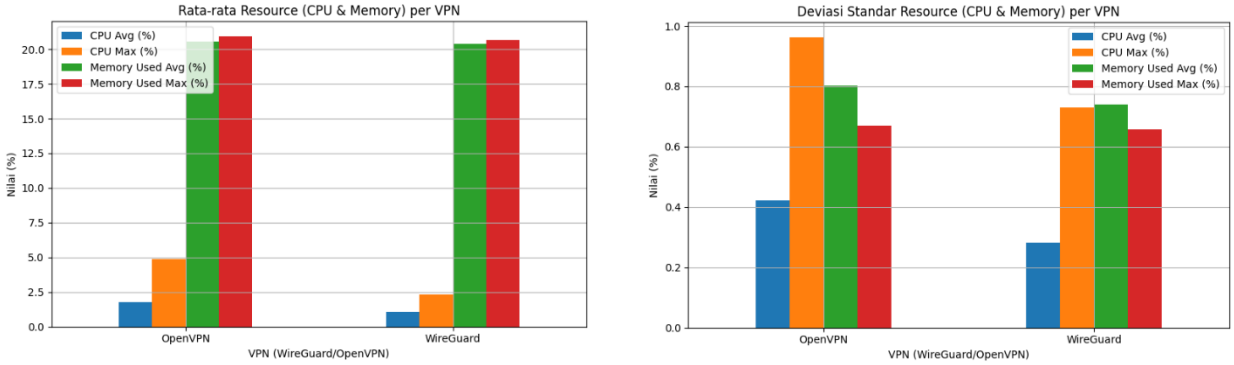
a. *Memory Used Avg*: *OpenVPN mean* 20,566 *vs WireGuard mean* 20,365 (selisih sekitar 0,201).
b. *Memory Used Max*: *OpenVPN mean* 20,952 *vs WireGuard mean* 20,667 (selisih sekitar 0,285).
c. Deviasi standar keduanya relatif mirip (misalnya *Memory Used Max std* 0,669 vs 0,658), menandakan penggunaan memori relatif stabil dan tidak menjadi faktor pembeda utama.

Tabel 8. Statistik Deskriptif *Memory Avg* dan *Memory Max* per *VPN* (*WireGuard vs OpenVPN*)

VPN	Memory Used Avg (%) mean	Memory Used Avg (%) std	Memory Used Avg (%) min	Memory Used Avg (%) max	Memory Used Max (%) mean	Memory Used Max (%) std	Memory Used Max (%) min	Memory Used Max (%) max
OpenVPN	20.566	0.802	18.80	22.0	20.952	0.669	20.0	22.0
WireGuard	20.365	0.740	19.13	21.3	20.667	0.658	20.0	22.0

Gambar 7 merangkum dua hal utama: rata-rata (mean) dan deviasi standar *resource CPU* dan memori untuk masing-*masing VPN*. Pola visualnya menegaskan bahwa *OpenVPN* lebih tinggi pada *CPU Avg* dan *CPU Max*, sedangkan *WireGuard* lebih rendah dan lebih stabil (*error bar*/variasi lebih kecil); untuk memori, perbedaan kedua protokol tampak tipis.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom



Gambar 7. Rata-rata dan Deviasi Standar Resource (*CPU* & Memori) per *VPN*

3.2 Statistik Inferensial

Analisis statistik inferensial dilakukan untuk memastikan apakah perbedaan kinerja *WireGuard* dan *OpenVPN* yang terlihat pada statistik deskriptif benar-benar merepresentasikan perbedaan populasi (bukan sekadar fluktuasi sampel pengukuran). Dalam konteks *VPN gateway*, variasi performa sangat dipengaruhi oleh jalur pemrosesan paket, *overhead* protokol, serta efisiensi implementasi pada perangkat jaringan oleh karena itu, pengujian signifikansi menjadi relevan untuk memperkuat kesimpulan komparatif [1].

3.2.1 Dasar pemilihan uji dan perumusan hipotesis

Uji yang digunakan adalah *Mann–Whitney U* (*non*-parametrik) untuk membandingkan dua kelompok pengukuran yang independen, yaitu hasil uji pada *WireGuard* dan *OpenVPN*, terutama ketika data tidak selalu memenuhi asumsi normalitas atau memiliki sebaran yang tidak simetris. Secara umum, hipotesis yang diuji pada setiap parameter adalah:

a. H0 : tidak terdapat perbedaan distribusi/median kinerja antara *WireGuard* dan *OpenVPN*.
b. H1 : terdapat perbedaan distribusi/median kinerja antara *WireGuard* dan *OpenVPN*.

Kriteria keputusan ditetapkan pada $\alpha = 0{,}05$. Apabila p-value < 0,05 maka H0 ditolak (perbedaan signifikan); sebaliknya apabila p-value ≥ 0,05 maka tidak terdapat bukti yang cukup untuk menolak H0. Pendekatan ini selaras dengan praktik komparasi performa *WireGuard* dan *OpenVPN* pada berbagai studi eksperimen sebelumnya [4].

3.2.2 *Ping* (*ICMP*)

Berdasarkan Tabel 9, hasil uji *Mann–Whitney* menunjukkan bahwa *Min RTT* tidak berbeda signifikan antara *WireGuard* dan *OpenVPN* (*p-value* = 0,809), dengan *median Min RTT WireGuard* 19,36 ms dan *OpenVPN* 19,28 ms. Dengan demikian, nilai "minimum" delay pada kondisi terbaik cenderung setara pada kedua protokol.

Tabel 9. Hasil uji *Mann–Whitney U* untuk setiap parameter

Parameter	Median WG	Median OVPN	Statistik U	p-value	Keterangan
Min RTT (ms)	97,00	98,00	210,50	0,809 > 0,05	Tidak berbeda signifikan
Avg RTT (ms)	107,16	116,59	62,50	p < 0,001	Berbeda signifikan
Max RTT (ms)	138,00	409,00	43,50	p < 0,001	Berbeda signifikan
Jitter (ms)	6,70	24,60	8,50	p < 0,001	Berbeda signifikan
Packet Loss (%)	0,00	0,00	283,50	0,010 < 0,05	Berbeda signifikan

Namun, untuk metrik yang lebih merepresentasikan kualitas layanan "rata-rata" dan "kondisi terburuk", diperoleh perbedaan yang bermakna. *Avg RTT*, *Max RTT*, dan *Jitter* menunjukkan perbedaan signifikan (*p-value* < 0,001) dengan *median WireGuard* lebih rendah (*Avg RTT* 20,78 ms; *Max RTT* 23,04 ms; *Jitter* 0,43 ms) dibanding *OpenVPN* (*Avg RTT* 21,98 ms; *Max RTT* 34,68 ms; *Jitter* 1,38 ms). Temuan ini mengindikasikan bahwa *WireGuard* memberikan *delay* yang lebih stabil dan lebih kecil pada dinamika trafik normal hingga kondisi puncak. Secara konseptual, hasil tersebut sejalan dengan literatur yang menempatkan *WireGuard* sebagai protokol yang cenderung efisien untuk latensi dan kestabilan karena desain yang lebih ringkas, sedangkan *OpenVPN* memiliki *overhead* lebih besar akibat mekanisme *tunneling* dan kontrol koneksi yang lebih kompleks [4].

Pada *Packet Loss*, perbedaan juga terdeteksi signifikan (*p-value* = 0,010), meskipun median kedua protokol sama-sama 0%. Hal ini umum terjadi ketika sebagian besar sampel bernilai nol, tetapi distribusi kejadian *loss* kecil (sporadis) lebih sering muncul pada salah satu protokol, sehingga uji peringkat tetap menangkap perbedaan distribusi. Dari perspektif layanan perbankan yang sensitif terhadap kualitas sesi (mis. transaksi *real-time*), *jitter* dan *tail latency* (*Max RTT*) yang lebih rendah umumnya lebih krusial dibanding sekadar *Min RTT*, karena lebih mencerminkan risiko keterlambatan dan retransmisi pada jam sibuk [5].

3.2.3 *Throughput*

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Pada *Throughput* rata-rata di Tabel 10, hasil uji menunjukkan pola yang tidak sepenuhnya "menang tunggal", melainkan bergantung pada jenis trafik dan arah komunikasi.

a. *TCP Download* tidak signifikan (*p-value* = 0,573), *median WireGuard* 232,01 Mbps dan *OpenVPN* 224,53 Mbps.
b. *UDP Download* signifikan (*p-value* = 0,030), dengan *median WireGuard* 203,34 Mbps lebih tinggi daripada *OpenVPN* 195,91 Mbps.
c. *TCP Upload* signifikan (*p-value* = 0,019), namun *median OpenVPN* 366,58 Mbps lebih tinggi daripada *WireGuard* 363,38 Mbps.

UDP Upload tidak signifikan (*p-value* = 0,604), *median WireGuard* 203,48 Mbps dan *OpenVPN* 208,58 Mbps.

Tabel 10. Hasil Uji *Mann–Whitney* untuk *Throughput* Rata-rata (Mbps) dan Maksimum (Mbps)

Arah Tes	Protokol	Median WG (Mbps)	Median OVPN (Mbps)	Statistik U	p-value	Keterangan	Median WG (Mbps)	Median OVPN (Mbps)	Statistik U	p-value	Keterangan
Download	TCP	1,68	1,54	228,00	0,860 > 0,05	Tidak berbeda signifikan	4,22	3,16	259,50	0,332 > 0,05	Tidak berbeda signifikan
Download	UDP	4,77	1,38	429,50	p < 0,001	Berbeda signifikan (WireGuard > OpenVPN)	6,35	2,77	391,00	p < 0,001	Berbeda signifikan (WireGuard > OpenVPN)
Upload	TCP	1,50	5,38	0,00	p < 0,001	Berbeda signifikan (OpenVPN > WireGuard)	4,16	9,43	17,00	p < 0,001	Berbeda signifikan (OpenVPN > WireGuard)
Upload	UDP	4,98	4,95	247,00	0,508 > 0,05	Tidak berbeda signifikan	5,09	5,13	163,50	0,149 > 0,05	Tidak berbeda signifikan

Sementara itu, pada *Throughput* maksimum di Tabel 10 pola yang mirip juga muncul yaitu *UDP Download* kembali signifikan (*WireGuard* lebih tinggi), *TCP Upload* signifikan (*OpenVPN* lebih tinggi), sedangkan *TCP Download* dan *UDP Upload* tidak signifikan.

Secara interpretatif, hasil ini menunjukkan bahwa *performance gap* kedua protokol dapat bersifat spesifik skenario (transport *TCP*/*UDP* dan arah trafik). Literatur komparatif juga melaporkan bahwa *WireGuard* sering unggul pada banyak skenario, tetapi *OpenVPN* dapat kompetitif atau lebih baik pada kondisi tertentu (misalnya profil jaringan/latensi tertentu atau konfigurasi tertentu), sehingga kesimpulan throughput sebaiknya dinyatakan "kontekstual" mengikuti rancangan eksperimen dan karakteristik jaringan [5]. Selain itu, karena pengujian *throughput* umumnya mengandalkan *iPerf3*, kehati-hatian terhadap faktor implementasi/lingkungan uji (mis. konfigurasi paralel *stream*, *MTU*, dan beban perangkat) tetap diperlukan agar interpretasi tidak *over*-generalisasi [7].

3.2.4 *Resource Mikrotik*

Pada metrik resource, fokus utama adalah efisiensi penggunaan *CPU* dan memori pada *MikroTik* sebagai *VPN gateway*. Berdasarkan Tabel 11, baik *CPU Average* maupun *CPU Max* berbeda signifikan (*p-value* < 0,001), dengan *median WireGuard* lebih rendah (*CPU Avg* 1,00%; *CPU Max* 2,00%) dibanding *OpenVPN* (*CPU Avg* 1,75%; *CPU Max* 5,00%).

Tabel 11. Hasil Uji *Mann–Whitney Resource Mikrotik* – Parameter *CPU*

Parameter	Median WG (%)	Median OVPN (%)	Statistik U	p-value	Keterangan
CPU Avg (%)	1,00	1,75	27,50	p < 0,001	Berbeda signifikan (WireGuard < OpenVPN)
CPU Max (%)	2,00	5,00	12,00	p < 0,001	Berbeda signifikan (WireGuard < OpenVPN)

Tabel 12. Hasil Uji *Mann–Whitney Resource Mikrotik* – Parameter *Memory*

Parameter	Median WG (%)	Median OVPN (%)	Statistik U	p-value	Keterangan
Memory Used Avg (%)	20,67	21,00	184,00	0,350 > 0,05	Tidak berbeda signifikan
Memory Used Max (%)	21,00	21,00	170,50	0,168 > 0,05	Tidak berbeda signifikan

Perbedaan ini mendukung argumentasi bahwa beban komputasi *OpenVPN* cenderung lebih tinggi, sedangkan *WireGuard* lebih efisien dari sisi pemrosesan, yang pada praktik operasional dapat berdampak pada headroom kapasitas perangkat ketika terjadi lonjakan sesi/tunnel atau trafik. Temuan ini konsisten dengan laporan penelitian perbandingan *WireGuard–OpenVPN* yang menemukan penggunaan *CPU WireGuard* lebih hemat dalam banyak skenario uji [4].

Sebaliknya, Tabel 1 menunjukkan penggunaan memori tidak berbeda signifikan baik untuk *Memory Used Average* (*p-value* = 0,350) maupun *Memory Used Max* (*p-value* = 0,168). Artinya, pada kondisi pengujian ini, perbedaan protokol

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 1, Februari 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i1.9438
Hal 71-84
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

lebih dominan tercermin pada konsumsi *CPU* daripada memori. Dalam konteks desain *VPN gateway* berperforma tinggi, hasil tersebut relevan karena bottleneck sering kali muncul pada *pipeline* pemrosesan paket dan *CPU path*, sehingga optimasi arsitektur dan pemilihan protokol dapat diarahkan untuk memaksimalkan efisiensi komputasi [1].

3.3 Pembahasan

Berdasarkan hasil pengujian, terdapat tiga temuan utama. Pertama, *WireGuard* menunjukkan kualitas koneksi yang lebih stabil daripada *OpenVPN*, terlihat dari kecenderungan *Avg RTT* dan terutama *Max RTT* (*tail latency*) yang lebih rendah serta *jitter* yang lebih kecil, sehingga risiko *delay burst* yang dapat mengganggu respons aplikasi perbankan menjadi lebih rendah. Kedua, pada sisi *throughput* hasilnya bersifat kontekstual: *WireGuard* cenderung lebih unggul dan stabil pada skenario *UDP*, sementara *OpenVPN* dapat lebih baik pada *TCP* tertentu, sehingga pemilihan protokol perlu mempertimbangkan profil trafik dominan (*TCP*/*UDP*) dan arah trafik layanan. Ketiga, *WireGuard* lebih efisien terhadap *resource gateway*, ditunjukkan oleh penggunaan *CPU* yang lebih rendah dibanding *OpenVPN*, yang penting untuk menjaga *headroom* ketika perangkat *gateway* juga menjalankan fungsi *routing* dan keamanan.

Jika dibandingkan dengan penelitian sejenis, pola temuan ini selaras dengan literatur yang menekankan bahwa efisiensi jalur pemrosesan paket di *VPN gateway* berpengaruh kuat terhadap latensi dan performa keseluruhan [1], serta studi komparatif yang kerap melaporkan *WireGuard* lebih efisien dibanding *OpenVPN* pada berbagai skenario uji [4], termasuk pada lingkungan *cloud*/virtualisasi dengan kondisi jaringan tersimulasi [5]. Selain aspek performa, literatur juga menyoroti dimensi keamanan-operasional: *OpenVPN* dapat diekspos pada *fingerprinting* pada kondisi tertentu [2], sedangkan *WireGuard* memiliki dukungan kajian analisis formal protokol [3]. Dengan demikian, hasil penelitian ini memperkuat rekomendasi berbasis bukti bahwa *WireGuard* lebih menguntungkan untuk stabilitas koneksi dan efisiensi *gateway* pada skenario uji, dengan tetap mempertimbangkan kebutuhan aplikasi, pola trafik, serta kebijakan keamanan institusi.

4. KESIMPULAN

Penelitian ini membandingkan kinerja *WireGuard* dan *OpenVPN* pada skenario jaringan perbankan menggunakan *router MikroTik* sebagai *VPN gateway* dengan metrik *ICMP* (*min*/*avg*/*max RTT*, *jitter*, *packet loss*), *throughput iPerf3 TCP*/*UDP* (*download*/*upload*), serta *resource* (*CPU* dan memori), kemudian dianalisis melalui statistik deskriptif dan uji *Mann–Whitney U*. Hasilnya menunjukkan *WireGuard* unggul signifikan pada latensi dan kestabilan *delay* (*Avg*/*Max RTT* dan *jitter* lebih rendah), *throughput* bersifat kontekstual (*WireGuard* cenderung lebih baik pada *UDP* sementara *OpenVPN* dapat lebih kompetitif pada *TCP* tertentu), dan dari sisi efisiensi *gateway WireGuard* lebih hemat *CPU* sedangkan memori tidak menunjukkan perbedaan berarti. Secara praktis, *WireGuard* direkomendasikan sebagai kandidat kuat untuk konektivitas *site-to-site* perbankan yang menuntut latensi rendah dan stabilitas tinggi, dengan tetap mempertimbangkan aspek keamanan atau operasional. Keterbatasan penelitian ini adalah penggunaan satu kelas perangkat dan satu rancangan topologi atau parameter uji, sehingga penelitian lanjutan disarankan memperluas variasi kondisi jaringan (mis. *impairment*, *MTU*, beban simultan), skenario *multi-user* atau *full-mesh*, serta otomasi konfigurasi untuk menjaga konsistensi eksperimen.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Universitas AMIKOM Yogyakarta, khususnya Program Magister Teknik Informatika dan Fakultas Ilmu Komputer, atas dukungan akademik, arahan ilmiah, serta fasilitas yang menunjang terlaksananya penelitian ini. Penulis juga menyampaikan apresiasi kepada pihak institusi tempat skenario studi kasus direpresentasikan, serta tim teknis yang membantu menyiapkan lingkungan uji, mendukung proses konfigurasi, dan memastikan ketersediaan data pengukuran sehingga rangkaian eksperimen dapat berjalan secara konsisten.
Selain itu, penulis berterima kasih kepada para reviewer/penyunting atas masukan konstruktif yang membantu meningkatkan kualitas naskah. Pada akhirnya, penulis menyampaikan terima kasih kepada seluruh pihak yang telah mendukung terlaksananya penelitian ini, baik secara langsung maupun tidak langsung, selama proses pengujian hingga penulisan laporan

REFERENCES

[1] C. Fu et al., “A Generic High-Performance Architecture for VPN Gateways,” Electronics (Basel), vol. 13, no. 11, p. 2031, May 2024, doi: 10.3390/electronics13112031.
[2] D. Xue et al., “OpenVPN is Open to VPN Fingerprinting,” Commun ACM, vol. 68, no. 1, pp. 79–87, Jan. 2025, doi: 10.1145/3618117.
[3] S. Ruhault, P. Lafourcade, and D. Mahmoud, “A Unified Symbolic Analysis of WireGuard,” in Proceedings 2024 Network and Distributed System Security Symposium, Reston, VA: Internet Society, Feb. 2024. doi: 10.14722/ndss.2024.24364.
[4] S. Mackey, I. Mihov, A. Nosenko, F. Vega, and Y. Cheng, “A Performance Comparison of WireGuard and OpenVPN,” in Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, New York, NY, USA: ACM, Mar. 2020, pp. 162–164. doi: 10.1145/3374664.3379532.
[5] J. Anyam, R. R. Singh, H. Larijani, and A. Philip, “Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions,” Computers, vol. 14, no. 8, p. 326, Aug. 2025, doi: 10.3390/computers14080326.

[6] D.-F. HRITCAN, A. GRAUR, D. G. BALAN, and E. M. TIMOFTE, "A Performance Analysis of VPN Technologies Used in an IoT Environment," Advances in Electrical and Computer Engineering, vol. 25, no. 2, pp. 81–88, 2025, doi: 10.4316/AECE.2025.02009.
[7] 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, p. 264, Sep. 2022, doi: 10.3390/fi14090264.
[8] D. Novianto, Y. S. Japriadi, and L. Tommy, "Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik," Jurnal Ilmiah Informatika Global, vol. 13, no. 2, Aug. 2022, doi: 10.36982/jiig.v13i2.2308.
[9] L. O. Sari and H. Helena, "Implementasi Virtual Private Network MenggunakanLayer 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.
[10] Surono and G. Guntoro Setiaji, "Analisa Perbandingan Quality of Service Protokol VPN antara Protokol SSTP Dan Open VPN Berbasis Router Mikrotik," Indonesian Journal of Computer Science, vol. 11, no. 1, Apr. 2022, doi: 10.33022/ijcs.v11i1.3034.
[11] D. L. Amenyo Fiase, K. Opoku Attah, S. Lartey, D. Adjin, and M. M.- Lisa Allotey, "Evaluating the Impact of Network Latency on user Experience in Telecommunication Industries in Ghana," International Journal of Innovative Science and Research Technology (IJISRT), pp. 2861–2869, Sep. 2024, doi: 10.38124/ijisrt/IJISRT24AUG1437.
[12] J. Bienik, M. Uhrina, L. Sevcik, and A. Holesova, "Impact of Packet Loss Rate on Quality of Compressed High Resolution Videos," Sensors, vol. 23, no. 5, p. 2744, Mar. 2023, doi: 10.3390/s23052744.
[13] B. Zieliński, "Assessment of iPerf as a Tool for LAN Throughput Prediction," International Journal of Electronics and Telecommunications, vol. 69, pp. 523–528, Sep. 2023, doi: 10.24425/ijet.2023.146501.
[14] R. Tuli, "Analyzing Network Performance Parameters using Wireshark," International Journal of Network Security & Its Applications, vol. 15, no. 01, pp. 01–13, Jan. 2023, doi: 10.5121/ijnsa.2023.15101.
[15] B. Hardin, D. Comer, and A. Rastegarnia, "On the Unreliability of Network Simulation Results FROM Mininet and iPerf," International Journal of Future Computer and Communication, pp. 5–13, Mar. 2023, doi: 10.18178/ijfcc.2023.12.1.596.
[16] D. Bringhenti, R. Sisto, and F. Valenza, "Automating VPN Configuration in Computer Networks," IEEE Trans Dependable Secure Comput, vol. 22, no. 1, pp. 561–578, Jan. 2025, doi: 10.1109/TDSC.2024.3409073.
[17] K. Sathupadi, S. Achar, S. V. Bhaskaran, N. Faruqui, and J. Uddin, "BankNet: Real-Time Big Data Analytics for Secure Internet Banking," Big Data and Cognitive Computing, vol. 9, no. 2, p. 24, Jan. 2025, doi: 10.3390/bdcc9020024.
[18] H. Shim, B. Kang, H. Im, D. Jeon, and S.-M. Kim, "qTrustNet Virtual Private Network (VPN): Enhancing Security in the Quantum Era," IEEE Access, vol. 13, pp. 17807–17819, 2025, doi: 10.1109/ACCESS.2025.3530985.
[19] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree, and D. Doghramachi, "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol," International Journal of Interactive Mobile Technologies (iJIM), vol. 14, no. 18, p. 157, Nov. 2020, doi: 10.3991/ijim.v14i18.16507.
[20] V. Kjorveziroski, C. Bernad, K. Gilly, and S. Filiposka, "Full-mesh VPN performance evaluation for a secure edge-cloud continuum," Softw Pract Exp, vol. 54, no. 8, pp. 1543–1564, Aug. 2024, doi: 10.1002/spe.3329.