JURNAL LOCUS: Penelitian & Pengabdian
Volume 5 No. 6 June 2026
E-ISSN 2829-7334| P-ISSN 2829-5439
Hompage: https://locus.rivierapublishing.id/index.php/jl

Analisis *Quality of Service* pada Implementasi Multi VPN Tunnel dalam Infrastruktur SD -WAN

Feny Indriany*, Galura Muhammad Suranegara
Universitas Pendidikan Indonesia, Indonesia
Email: fnydriany@upi.edu*, galurams@upi.edu

Keywords:
SD-WAN; WireGuard, Tailscale; ZeroTier; *Quality of Service*; TIPHON.

Abstract
The growing need for data communication between locations has driven the adoption of SD-WAN as a solution to enhance the flexibility and efficiency of network management. In its implementation, SD-WAN utilizes VPNs as a means of communication between sites over the internet. However, differences in the communication mechanisms of WireGuard, Tailscale, and ZeroTier VPNs have the potential to result in varying network performance. This study aims to implement multi-VPN tunnels using WireGuard, Tailscale, and ZeroTier on an SD-WAN infrastructure and analyze performance based on QoS parameters, including throughput, latency, jitter, and packet loss. The research method used is an experimental approach, involving the implementation of the three VPNs within the SD-WAN environment, followed by testing using Ping, iPerf3, and Wireshark. The test results show that all VPNs successfully established communication between sites and achieved 0% packet loss. For the throughput parameter, Tailscale and ZeroTier achieved the highest values at 99 Mbps, while WireGuard reached 95 Mbps. However, WireGuard demonstrated the best performance in terms of latency 4 ms and jitter 2 ms, outperforming ZeroTier latency 7 ms, jitter 27 ms and Tailscale latency 17 ms, jitter 60 ms. Based on the research findings, WireGuard is the most optimal VPN for SD-WAN implementation as it provides more stable communication quality with lower latency and jitter.

Kata Kunci:
SD-WAN; WireGuard, Tailscale; ZeroTier; *Quality of Service*; TIPHON.

Abstrak
Perkembangan kebutuhan komunikasi data antar lokasi mendorong penerapan SD-WAN sebagai solusi untuk meningkatkan fleksibilitas dan efisiensi pengelolaan jaringan. Dalam implementasinya, SD-WAN memanfaatkan VPN sebagai media komunikasi antar *site* melalui jaringan internet. Namun perbedaan mekanisme komunikasi pada VPN WireGuard, Tailscale, dan ZeroTier berpotensi menghasilkan performa jaringan yang berbeda. Penelitian ini bertujuan mengimplementasikan multi VPN *tunnel* menggunakan WireGuard, Tailscale, dan ZeroTier pada infrastruktur SD-WAN serta menganalisis performa berdasarkan parameter QoS yang meliputi *throughput*, *latency*, *jitter*, dan *packet loss*. Metode penelitian yang digunakan adalah metode eksperimen dengan melakukan implementrasi ketiga VPN pada lingkungan SD-WAN, kemudian dilakukan pengujian menggunakan Ping, iPerf3, dan Wireshark. Hasil pengujian menunjukan bahwa seluruh VPN berhasil membangun komunikasi antar *site* dengan baik dan menghasilkan *packet loss* 0%. Pada parameter *throughput*, Tailscale dan ZeroTier memperoleh nilai tertinggi sebesar 99 Mbps, sedangkan WireGuard memperoleh 95 Mbps. Namun, WireGuard menunjukkan performa terbaik pada parameter *latency* 4 ms dan jitter 2 ms, lebih rendah ZeroTier *latency* 7 ms dan jitter 27 ms, serta Tailscale *latency* 17 ms dan jitter 60 ms. Berdasarkan hasil penelitian, WireGuard menjadi VPN yang paling optimal untuk implementasi SD-WAN karena mampu memberikan

kualitas komunikasi yang lebih stabil dengan *latency* dan *jitter* yang lebih rendah.

PENDAHULUAN

Perkembangan transformasi digital, layanan berbasis *cloud computing*, dan kebutuhan komunikasi data antar lokasi telah meningkatkan tuntutan terhadap infrastruktur jaringan yang fleksibel, aman, dan efisien (Dudczyk et al., 2025). Pada lingkungan enterprise, komunikasi antar kantor cabang, data center, dan layanan *cloud* membutuhkan konektivitas yang mampu menjaga kualitas layanan jaringan secara konsisten. Namun implementasi *Wide Area Network* (WAN) tradisional masih menghadapi berbagai keterbatasan, seperti tingginya biaya operasional, kompleksitas konfigurasi, serta kurangnya fleksibilitas dalam pengelolaan lalu lintas data (Petrović et al., 2025). Untuk mengatasi permasalahan tersebut, teknologi *Software Defined Wide Area Network* (SD-WAN) dikembangkan sebagai solusi yang memungkinkan pengelolaan jaringan dilakukan secara terpusat, dinamis, dan lebih efisien melalui pendekatan *Software Defined Networking* (SDN) (Fu et al., 2024).

Dalam implementasinya, SD-WAN umumnya memanfaatkan *Virtual Private Network* (VPN) sebagai media komunikasi *overlay network* yang berjalan di atas jaringan internet publik (Ibrahim et al., 2025). VPN memungkinkan komunikasi antar *site* dilakukan secara aman melalui mekanisme *tunneling* dan enkripsi data (Gentile et al., 2024). Seiring perkembangan teknologi, berbagai VPN modern seperti WireGuard, Tailscale, dan ZeroTier mulai banyak digunakan karena menawarkan kemudahan implementasi, keamanan yang tinggi, serta kemampuan membangun konektivitas antar perangkat secara fleksibel (Abdulazeez et al., 2020a). Meskipun memiliki fungsi yang sama, ketiga VPN tersebut menggunakan mekanisme komunikasi yang berbeda sehingga berpotensi menghasilkan performa jaringan yang berbeda.

Kualitas layanan jaringan pada implementasi SD-WAN dapat dievaluasi menggunakan parameter *Quality of Service* (QoS) yang meliputi *throughput*, *delay*, *jitter*, dan *packet loss*. Selain itu, analisis *packet behavior* menggunakan Wireshark, seperti TCP *Retransmission*, *Duplicate* ACK, dan *Previous Segment Not Captured*, dapat memberikan informasi mengenai kondisi lalu lintas jaringan selama proses transmisi berlangsung (Simargolang & Widarma, 2022). Kualitas layanan jaringan menjadi faktor penting pada implementasi SD-WAN karena dapat memengaruhi performa aplikasi berbasis *cloud*, komunikasi *real-time*, serta pertukaran data antar lokasi. Pemilihan teknologi VPN yang kurang sesuai berpotensi menyebabkan peningkatan *latency, jitter* maupun penurunan *throughput* yang dapat berdampak pada kualitas layanan jaringan.

Beberapa peneliti terdahulu telah membahas implemantasi SD-WAN maupun VPN secara tepisah. Penelitian terkait WireGuard umumnya berfokus pada perbandingan performa dengan VPN tradisional (Anyam et al., 2025a), sedangkan penelitian Tailscale dan ZeroTier lebih banyak membahas kemudahan implementasi serta fleksibilitas konektivitas jaringan (Putra et al., 2025a). Namun, penelitian yang membandingkan WireGuard, Tailscale dan ZeroTier secara langsung pada implementasi multi VPN *tunnel* dalam satu lingkungan SD-WAN menggunakan parameter QoS yang sama masih relatif terbatas (Kjorveziroski et al., 2024a). Selain itu, sebagian besar penelitian sebelumnya belum mengombinasikan analisis

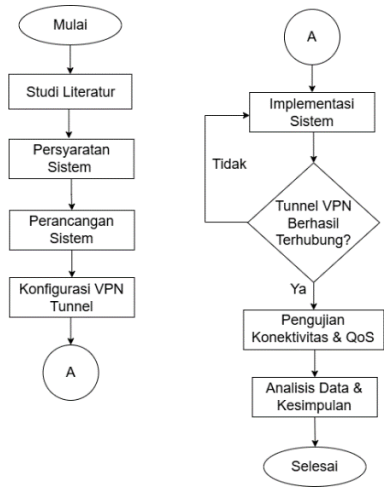
QoS dengan analisis *packet behavior* menggunakna Wireshark sehingga belum memberikan gambaran performa jaringan secara menyeluruh(Rahman & Harnaningrum, 2024a).

Kebaruan (*novelty*) penelitian ini terletak pada implementasi dan evaluasi komparatif tiga teknologi VPN modern WireGuard, Tailscale, dan ZeroTier dalam satu infrastruktur SD-WAN dengan menggunakan pendekatan *multi VPN tunnel* yang terintegrasi. Penelitian ini tidak hanya menganalisis parameter QoS secara kuantitatif, tetapi juga melakukan analisis mendalam terhadap *packet behavior* menggunakan Wireshark untuk mengidentifikasi indikator-indikator seperti *TCP Retransmission*, *Duplicate ACK*, dan *Previous Segment Not Captured*, yang jarang dibahas secara komprehensif dalam penelitian sebelumnya. Pendekatan holistik ini memberikan gambaran performa jaringan yang lebih lengkap, mulai dari aspek kuantitatif hingga karakteristik lalu lintas data selama transmisi berlangsung.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan mengimplementasikan multi VPN *tunnel* menggunakan WireGuard, Tailscale, dan ZeroTier pada infrastruktur SD-WAN serta menganalisis performanya berdasarkan parameter QoS yang meliputi *throughput*, *delay*, *jitter*, dan *packet loss* (Troia et al., 2021a). Selain itu, melakukan analisis *packet behavior* menggunakan Wireshark untuk mengevaluasi kondisi lalu lintas jaringan selama proses transmisi data berlangsung. Hasil penelitian diharapkan dapat memberikan kontribusi sebagai referensi dalam pemilihan teknologi VPN yang optimal pada implementasi SD-WAN serta menjadi acuan bagi peneliti selanjutnya dalam pengembangan jaringan berbasis multi VPN *tunnel*.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode eksperimen *(Experimental Method*). Metode ini dilakukan dengan merancang dan mengimplementasikan sistem SD-WAN menggunakan VPN WireGuard, Tailscale, dan Zerotier, kemudian melakukan pengujian QoS untuk menganalisis performa jaringan berdasarkan parameter *throughput*, *delay*, *jitter* dan *packet loss* (Putra et al., 2025b). Tahapan penelitian yang dilakukan secara keseluruhan ditunjukkan pada gambar 1.



Gambar 1. Diagram Alur Penelitian
Sumber: Hasil Perancangan Peneliti, (2026)

Studi Literatur

Software Defined Wide Area Network (SD-WAN) merupakan teknologi jaringan berbasis *Software Defined Networking* (SDN) yang digunakan untuk mengelola jaringan area luas secara terpusat dan dinamis (Ouamri et al., 2025). SD-WAN mampu melakukan proses *routing*, monitoring, dan optimasi trafik secara otomatis berdasarkan kondisi *Quality of Service* (QoS) sehingga komunikasi jaringaan menjadi lebih fleksibel dan efisien. Dalam implementasinya, SD-WAN memanfaatkan *controller, edge device*, *overlay network*, dan *underlay network* untuk mendukung komunikasi antar *site* melalui VPN *tunnel*. Teknologi ini memiliki kelebihan dalam hal *load balancing, failover*, efisiensi *bandwidth*, serta pengurangan biaya implementasi jaringan WAN (Troia et al., 2021b). Oleh karena itu, teknologi ini banyak diterapkan pada jaringan *enterprise* untuk menghubungkan kantor cabang, *data center*, dan *cloud service* secara aman dan optimal menggunakan multi VPN *tunnel*.

Virtual Private Network (VPN) merupakan teknologi jaringan yang digunakan untuk membangun komunikasi *private* melalui jaringan publik menggunakan mekanisme *tunneling* dan enkripsi data sehingga komunikasi antar perangkat dapat berjalan dengan aman melalui internet. VPN berfungsi untuk meningkatkan keamanan, privasi, serta mendukung komunikasi antar *site* dan *remote access* pada jaringan komputer (Arifwidodo, 2023).

Penelitian ini menggunakan tiga provider VPN yaitu WireGuard, Tailscale, dan ZeroTier. WireGuard merupakan teknologi VPN modern yang dirancang untuk menyediakan komunikasi jaringan yang aman, ringan, dan memiliki performa tinggi (Abdulazeez et al., 2020b). WireGuard menggunakan protokol UDP dengan mekanisme enkripsi modern sehingga mampu menghasilkan *throughput* tinggi, *delay* rendah, serta konsumsi *resource* yang lebih kecil dibandingkan VPN tradisional (Anyam et al., 2025b). Selain memiliki konfigurasi yang lebih sederhana, WireGuard juga stabil untuk komunikasi *real-time*, namun masih memiliki keterbatasan pada fitur manajemen dan memerlukan konfigurasi manual (Rahman & Harnaningrum, 2024b).

Tailscale merupakan VPN berbasis WireGuard yang menggunakan konsep *mesh network* dan *overlay network* untuk mempermudah komunikasi antar perangkat melalui internet (Kjorveziroski et al., 2024b). Tailscale mendukung *NAT traversal*, autentikasi *cloud*, dan konfigurasi otomatis sehingga lebih mudah diimplementasikan untuk *remote access*. Namun penggunaan *relay server* dan layanan *cloud* dapat meningkatkan *overhead* jaringan serta memengaruhi *delay* dan *jitter* komunikasi data (Mackey et al., 2020).

Sementara itu, ZeroTier merupakan teknologi virtual *networking* berbasis SDN yang memungkinkan perangkat tergabung dalam satu jaringan virtual melalui *overlay network*. ZeroTier mendukung komunikasi *peer-to-peer*, virtual LAN, dan multi platform sehingga fleksibel digunakan pada berbagai topologi jaringan. Meskipun mudah diimplementasikan, ZeroTier memiliki *overhead* jaringan yang lebih besar dan memerlukan proses otorisasi *node* sebelum perangkat dapat saling berkomunikasi (Haeruddin et al., 2023).

Dalam implementasi SD-WAN, VPN berperan sebagai media komunikasi *overlay network* antar *site* melalui jaringan internet. Penggunaan multi VPN *tunnel* memungkinkan sistem memilih jalur komunikasi terbaik berdasarkan kualitas jaringan sehingga komunikasi data dapat berjalan lebih aman, fleksibel, dan efisien.

Quality of Service (QoS) merupakan metode pengukuran kualitas layanan jaringan berdasarkan performa komunikasi data untuk mengetahui kemampuan jaringan dalam

mengirimkan data secara stabil dan efisien. Pada penelitian ini, pengukuran QoS mengacu pada standar TIPHON dengan parameter *throughput*, *delay*, *jitter*, dan *packet loss*. *Throughput* digunakan untuk mengetahui kemampuan transfer data, *delay* menunjukkan waktu tempuh paket data, *jitter* merupakan variasi *delay* antar paket, sedangkan *packet loss* menunjukkan jumlah paket yang hilang selama transmisi. Nilai *throughput* yang tinggi serta *delay*, *jitter*, dan *packet loss* yang rendah menunjukkan kualitas jaringan yang lebih baik (Nisa et al., 2024). Rumus perhitungan QoS yang digunakan pada penelitian ini meliputi:

$$Latency = \frac{\text{Total Delay}}{\text{Jumlah Paket yang Diterima}} \quad (1)$$

$$Packet\ loss = \frac{\text{Paket Dikirim} - \text{Paket Diterima}}{\text{Jumlah Paket Dikirim}} \times 100\% \quad (2)$$

$$Throughput = \frac{\text{Jumlah Data yang Dikirim}}{\text{Waktu Pengiriman Data}} \quad (3)$$

$$Jitter = \frac{\text{Total Variasi Delay}}{\text{Total Paket Diterima} - 1} \quad (4)$$

Persyaratan Sistem

Penelitian ini menggunakan beberapa perangkat keras dan perangkat lunak sebagai pendukung proses implementasi dan pengujian. Spesifikasi sitem yang digunakan terdapat pada tabel berikut.

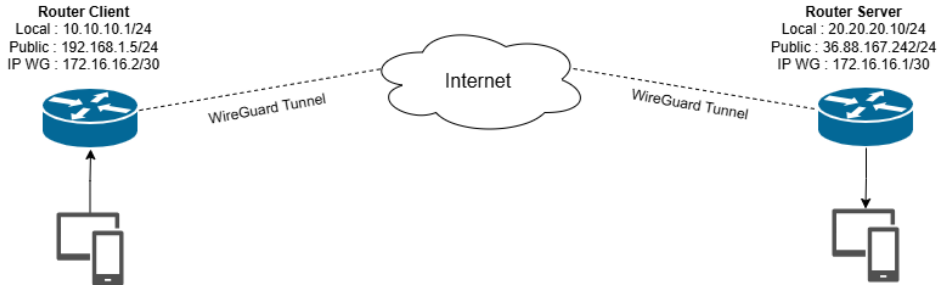
Tabel 1. *Tools* Pengujian

Komponen	Spesifikasi
Sistem Operasi	Windows 11
Prosesor (CPU)	Intel® Core™ i5-12500H
Memori (RAM)	8 GB
Router	Mikrotik RB750 Mikrotik RB952Ui-5ac2nD-TC (hAP-AC-Lite-TC)
Manajemen Router	Winbox (64-bit) v7.20.6 hAP ac^2 (arm) Winbox (64 bit) v7.12.1 on RB750 (mipsbe)
VPN	Wireguard Tailscale ZeroTier

Sumber: Data Penelitian (2026)

Implementasi Sistem Design dan Konfigurasi VPN Tunnel WireGuard

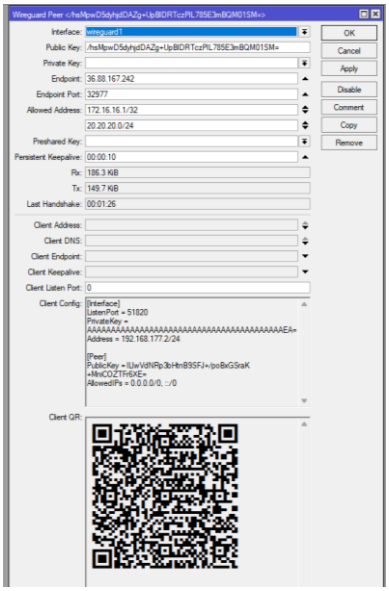
Sistem pada penelitian ini dirancang menggunakan konsep SD-WAN dengan memanfaatkan VPN WireGuard sebagai media komunikasi antar *site* melalui jaringan internet. Topologi jaringan terdiri dari router client dan router server yang saling terhubung menggunakan *tunnel* WireGuard. Masing-masing router memiliki alamat IP lokal, IP publik, dan IP WireGuard.



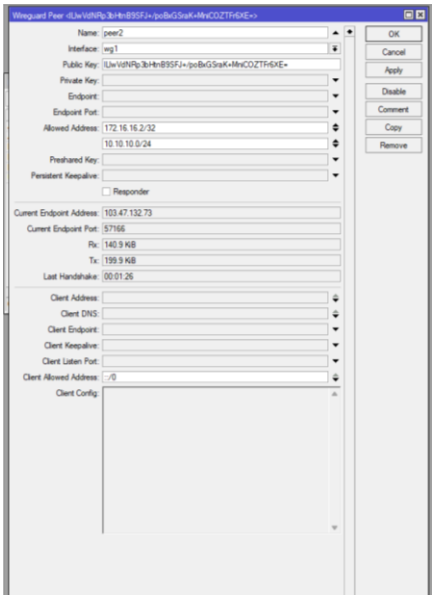
Gambar 2. Sistem Design WireGuard
Sumber: Hasil Perancangan Peneliti (2026)

Proses konfigurasi VPN *tunnel* dilakukan pada kedua router Mikrotik menggunakan aplikasi Winbox. Tahap konfigurasi meliputi pembuatan *interface* WireGuard, pengaturan *public key* dan *private key*, penambahan *peer*, serta konfigurasi *endpoint* dan *allowed address* pada masing-masing router. Router client dikonfigurasikan menggunakan alamat IP publik router server sebagai *endpoint* tujuan, sedangkan router server berfungsi sebagai responder untuk menerima konesi *tunnel* dari router client.

Selanjutnya, dilakukan konfigurasi routing untuk mengarahkan lalu lintas data dari jaringan lokal masing-masing *site* agar dapat melewati tunnel WireGuard. Dengan konfigurasi tersebut, perangkat pada jaringan lokal router client dapat berkomunikasi dengan perangkat pada jaringan lokal router server melalui jalur VPN terenkripsi menggunakan mekanisme *site-to-site* VPN.



Gambar 3. Konfigurasi Peer Router Server
Sumber: Hasil Tangkapan Layar Peneliti (2026)

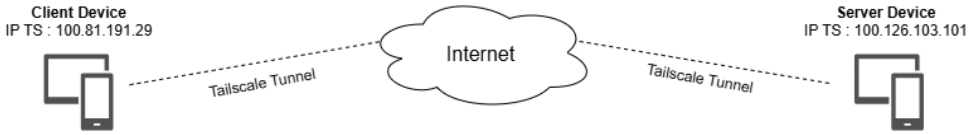


Gambar 4. Konfigurasi *Peer* Router Client
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Hasil implementasi menunjukkan bahwa tunnel VPN WireGuard berhasil terbentuk yang ditandai dengan adanya proses *handshake* antar *peer* serta aktivitas *transmit* (Tx) dan *receive* (Rx) pada *interface* WireGuard.

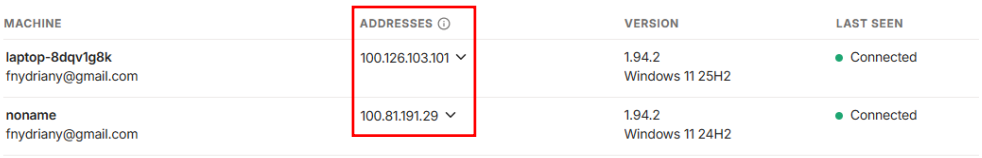
Tailscale

Implementasi sistem menggunakan teknologi VPN Tailscale sebagai media komunikasi antar perangkat melalui jaringan internet. Topologi jaringan terdiri dari *client device* dan *server device* yang saling terhubung menggunakan *tunnel* Tailscale. Kedua perangkat terhubung ke jaringan internet daan membentuk komunikasi virtual menggunakan alamat IP Tailscale yang diperoleh secara otomatis dari sistem Tailscale.



Gambar 5. Sistem Design Tailscale
Sumber: Hasil Perancangan Peneliti (2026)

Proses konfigurasi VPN *tunnel* dilakukan dengan menginstal aplikasi Tailscale pada masing-masing perangkat, kemudian menggunakan autentikasi menggunakan akun yang sama agar kedua perangkat dapat bergabung dalam satu jaringan virtual Tailscale. Setelah proses autentikasi berhasil dilakukan, sistem secara otomatis membentuk koneksi *peer-to-peer* dan memberikan alamat IP virtual Tailscale pada setiap perangkat yang digunakan sebagai jalur komunikasi *tunnel* VPN.

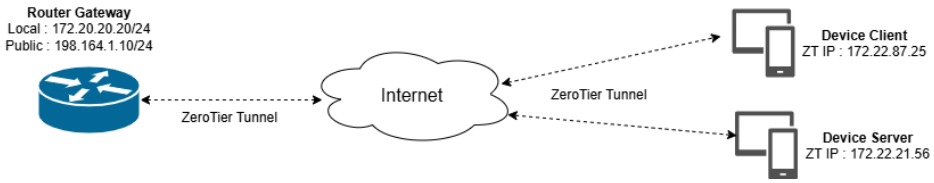


Gambar 6. Perangkat Tailnet
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Berdasarkan hasil implementasi, kedua perangkat berhasil terhubung yang ditandai dengan status *connected* pada dashboard Tailscale serta munculnya alamat IP Tailscale pada masing-masing perangkat. Dengan konfigurasi tersebut, komunikasi data antar perangkat dapat dilakukan secara aman melaluii *tunnel* terenkripsi menggunakan mekanisme *overlay network* Tailscale.

ZeroTier

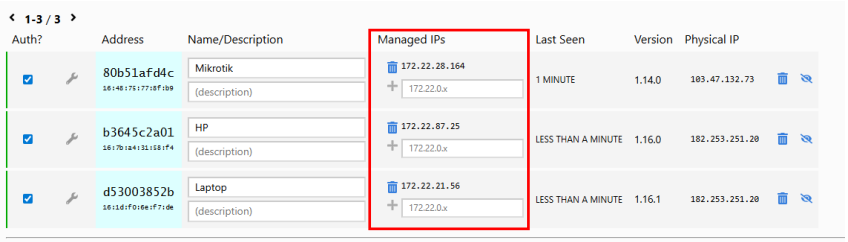
Topologi jaringan terdiri dari router *gateway* yang terhubung dengan *device client* dan *device server* melalui *tunnel* ZeroTier. Router *gateway* berfungsi sebagai perhubung jaringan lokal dengan jaringan virtual ZeroTier sehingga komunikasi antar perangkat dapat dilakukan secara aman melalui jaringan internet.



Gambar 7. Sistem Design ZeroTier
Sumber: Hasil Perancangan Peneliti (2026)

Router mikrotik dikonfigurasikan dengan memisahkan jaringan publik dan jaringan privat agar proses komunikasi dan pengujian jaringan dapat berjalan secara terkontrol. *Interface* ether1 menggunakan alamat IP 198.164.1.10/24 sebagai jalur koneksi ke internet, sedangkan *interface* ether2 menggunakan alamat IP 172.20.20.20/24 sebagai jaringan lokal. Selain itu, router dikonfigurasikan dengan *default route* menuju *gateway* 192.168.1.1 untuk akses internet, DNS publik 8.8.8.8 dan 8.8.4.4 untuk proses resolusi domain, serta DHCP server pada *interface* bridgeLocal agar perangkat *client* memperoleh alamat IP secara otomatis. Konfigurasi NAT menggunakan metode 'masquerade' untuk menerjemahkan alamat IP privat menjadi alamat IP publik sehingga perangkat lokal dapat terhubung ke internet.

Implementasi ZeroTier dilakukan melalui ZeroTierCentral dengan membuat jaringan virtual baru. Proses tersebut menghasilkan Network ID yang digunakan oleh perangkat router, *client*, dan server untuk bergabung ke jaringan virtual yang sama. Setelah perangkat berhasil terhubung, setiap *node* akan muncul pada dashboard ZeroTier Central dan harus melalui proses otorisasi oleh administrator sebelum dapat saling berkomunikasi. Perangkat yang telah terhubung akan memperoleh alamat IP virtual (Managed IP) dalam satu subnet yang sama sehingga komunikasi data dapat dilakukan melalui *tunnel* ZeroTier secara aman melalui jaringan internet.



Gambar 8. Node Perangkat ZeroTier
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Selanjutnya, dilakukan integrasi sistem dan konfigurasi routing untuk menghubungkan jaringan lokal router dengan jaringan virtual ZeroTier. Dengan konfigurasi tersebut, lalu lintas data dari jaringan lokal dapat diarahkan menuju jaringan virtual ZeroTier sehingga komunikasi antar perangkat dapat berlangsung melalui jalur *tunnel* terenkripsi menggunakan mekanisme *overlay network*.

Pengujian Konektivitas & QoS

Tahap pengujian konektivitas dilakukan untuk memastikan komunikasi antar *site* pada infrastruktur SD-WAN melalui *tunnel* VPN berjalan dengan baik. Pengujian konektivitas dilakukan menggunakan metode ping antar perangkat untuk memastikan setiap *node* dapat saling terhubung melalui jaringan virtual VPN. Selain itu, pengujian ping juga digunakan untuk mengukur parameter *delay*, *jitter*, dan *packet loss* pada VPN WireGuard, Tailscale, dan ZeroTier.

Pengujian *throughput* dilakukan menggunakan iperf3 dengan metode pengiriman data antara perangkat *client* dan server melalui *tunnel* VPN pada jaringan SD-WAN. Pada proses pengujian *throughput* menggunakan iPerf3, *bandwidth* dibatasi sebesar 100 Mbps untuk menjaga kestabilan trafik selama pengujian berlangsung. Hal tersebut dilakukan karena *bandwidth* aktual jaringan internet tidak selalu stabil pada nilai maksimum, terdapat *overhead*

pada *tunnel* VPN, serta kemungkinan terjadinya trafik *burst* selama proses transmisi data. Selain itu, analisis paket dilakukan menggunakan wireshark untuk mengamati kondisi lalu lintas jaringan selama pengujian berlangsung. Analisis dilakukan dengan mengidentifikasi paket *behavior* seperti TCP *retransmission, duplicate* ACK, dan *previous segment not captured* sebagai indikator terjadinya keterlambatan maupun kehilangan paket pada *tunnel* VPN.

Analisis Data dan Kesimpulan

Berdasarkan hasil implementasi dan pengujian QoS tabel 3 WireGuard menunjukkan performa terbaik dibandingkan Tailscale dan ZeroTier. Hal tersebut ditunjukkan melalui nilai *latency* dan *jitter* yang lebih rendah sehingga komunikasi jaringan menjadi lebih stabil dan efisien. Sementara itu, Tailscale dan ZeroTier mampu menghasilkan *throughput* yang tinggi, namun memiliki variasi *delay* yang lebih besar sehingga kualitas komunikasi jaringan menjadi kurang stabil dibandingkan WireGuard.

Tabel 2. Rekapitulasi Hasil QoS

VPN	*Latency*	*Packet Loss*	*Jitter*	*Throughput*
WireGuard	4 ms	0%	2 ms	95 Mbps
Tailscale	17 ms	0%	60 ms	99 Mbps
ZeroTier	7 ms	0%	27 ms	99 Mbps

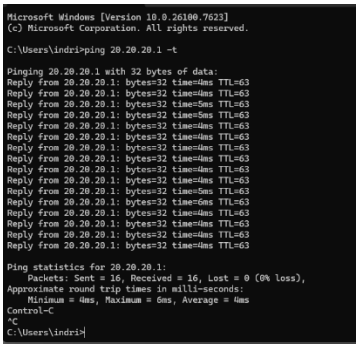
Sumber: Hasil Pengolahan Data Penelitian (2026)

HASIL DAN PEMBAHASAN

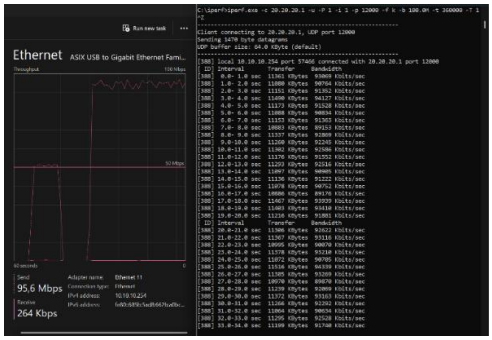
Pengujian QoS dilakukan pada implementasi SD-WAN menggunakan tiga provider VPN yaitu, WireGuard, Tailscale, dan ZeroTier. Parameter yang diukur meliputi *throughput, latency, jitter,* dan *packet loss*. Selain itu, dilakukan analisis *packet behavior* menggunakan Wireshark untuk mengamati kondisi lalu lintas jaringan selama proses pengujian berlangsung.

Hasil Pengujian WireGuard

Pengujian konektivitas pada VPN WireGuard dilakukan menggunakan metode ping antar perangkat melalui tunnel VPN.



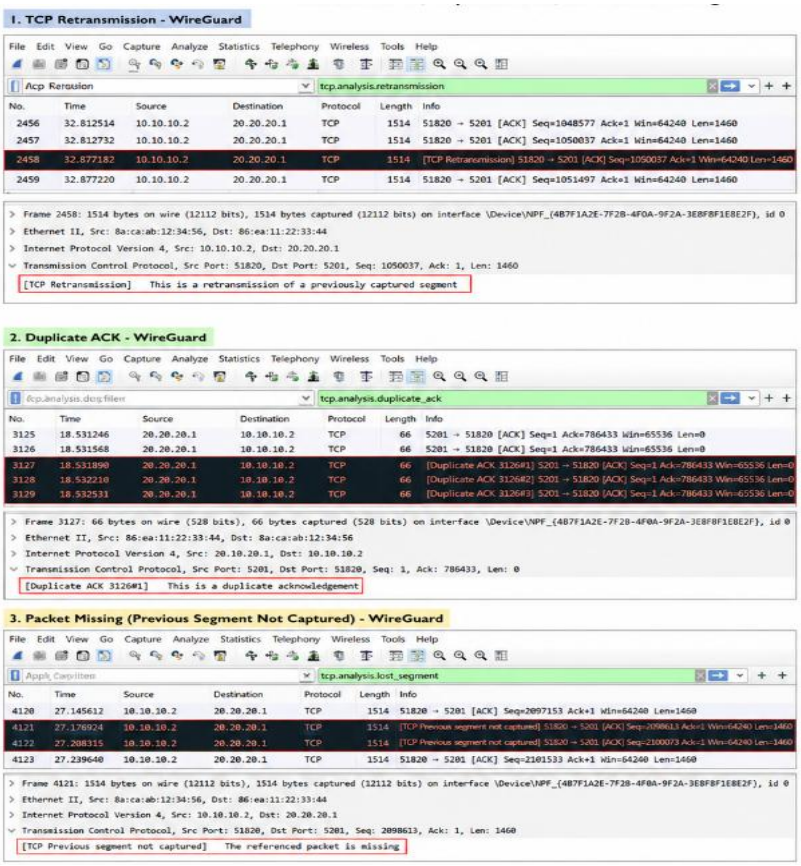
Gambar 9. Pengujian Ping WireGuard
Sumber: Hasil Tangkapan Layar Peneliti (2026)



Gambar 10. Pengujian Throughput WireGuard
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Berdasarkan hasil pengujian pada gambar 9, konektivitas menggunakan perintah ping ke alamat 20.20.20.1 melalui VPN WireGuard, 16 paket data berukuran 32 *byte* berhasil

dikirim dan diterima tanpa kehilangan paket (*Sent* = 16, *Receive* = 16, *Lost* = 0%). Menunjukkan nilai *round trip time* minimum 4 ms, maksimum 6 ms, dan rata-rata 4 ms. Menghasilkan latency 4 ms, packet loss 0% dan jitter 2 ms. Gambar 10, Hasil pengujian iperf3 pada WireGuard menghasilkan *throughput* rata-rata 95 Mbps dari *bandwidth* yang ditetapkan sebesar 100 Mbps. Gambar 11 menunjukkan kondisi lalu lintas jaringan selama proses pengujian berlangsung.



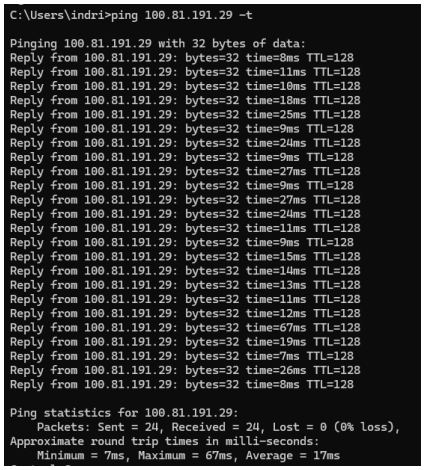
Gambar 11. *Packet Behavior* WireGuard
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Gambar 11, ditemukan bebrapa indikator *packet behavior* yaitu TCP *Retransmission*, *Duplicate* ACK, dan *Previous Segment Not Captured*. TCP *Retransmission* menunjukkan adanya paket yang dikirim ulang akibat ACK tidak diterima oleh pengirim. *Duplicate* ACK menunjukkan adanya paket yang terlambat atau hilang sehingga penerima mengirim ACK yang sama secara berulang. Sementara itu, *Previous Segment Not Captured* menunjukkan adanya paket yang hilang atau tidak tertangkap selama proses pengujian berlangsung.

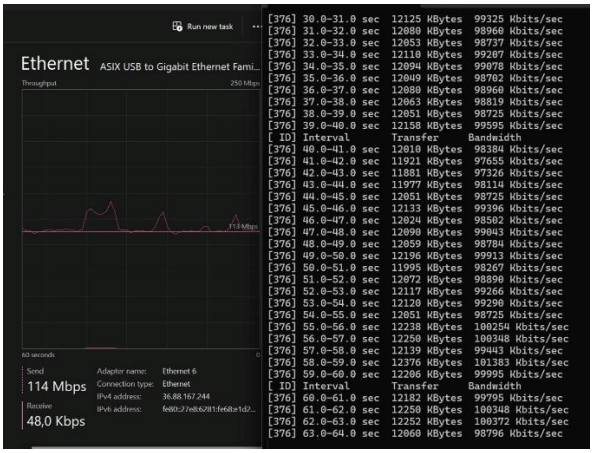
Hasil Pengujian Tailscale

Berdasarkan hasil pengujian pada gambar 12, konektivitas menggunakan ping ke alamat 100.81.191.29 melalui VPN Tailscale menunjukkan bahwa sebanyak 24 paket data berukuran 32 *byte* berhasil dikirim dan diterima tanpa kehilangan paket (*Sent* = 24, *Received* = 24, *Lost* = 0%). Berdasarkan hasil tersebut, diperoleh nilai *latency* sebesar 17 ms, *packet loss* 0%, dan *jitter* 60 ms menunjukkan adanya variasi waktu kedatangan paket yang cukup besar selama proses transmisi data. Gambar 13 menunjukkan pengujian *throughput* menggunakan

iPerf3 menunjukkan bahwa Tailscale mampu menghasilkan *throughput* sebesar 99 Mbps selama proses transmisi data berlangsung.

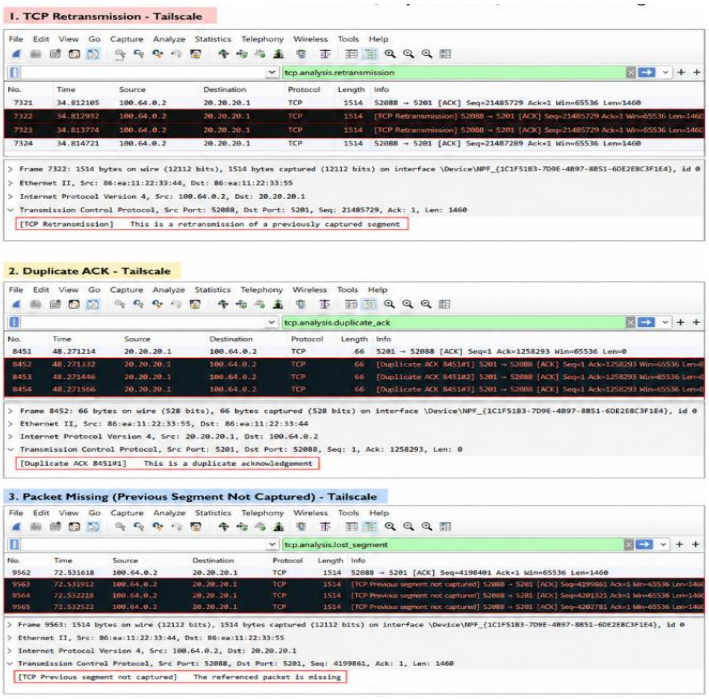


Gambar 12. Pengujian Ping Tailscale
Sumber: Hasil Tangkapan Layar Peneliti (2026)



Gambar 13. Pengujian Throughput Tailscale
Sumber: Hasil Tangkapan Layar Peneliti (2026)

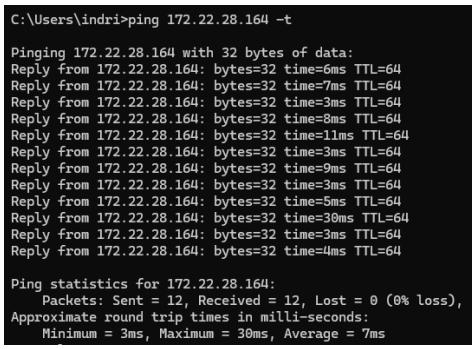
Hasil pengujian Wireshark pada gambar 14, menunjukkan adanya TCP *Retransmission*, *Duplicate* ACK, dan *Previous Segment Not Captured* yang menandakan terdapat paket yang dikirim ulang, ACK yang muncul berulang, serta paket yang tidak tertangkap selama proses *capture* jaringan berlangsung.



Gambar 14. *Packet Behavior* Tailscale
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Hasil Pengujian ZeroTier

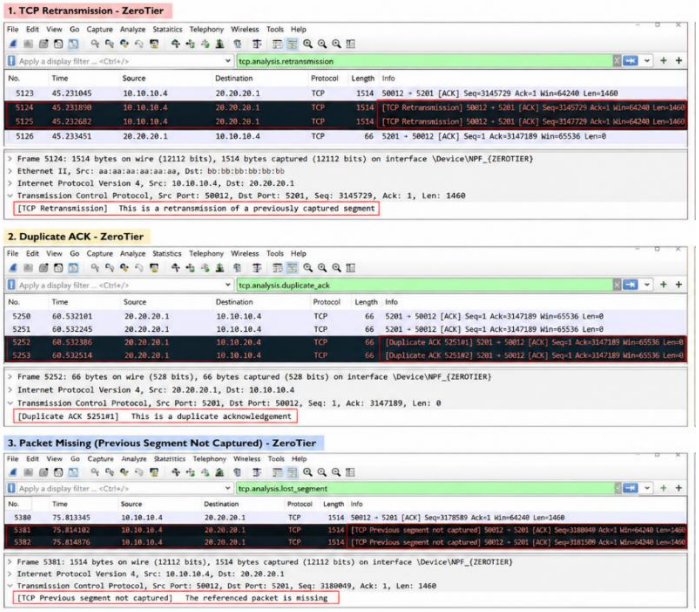
Berdasarkan hasil pengujian pada gambar 15, konektivitas menggunakan ping ke alamat 172.22.28.164 melalui VPN Zerotier menunjukkan bahwa sebanyak 12 paket data berukuran 32 *byte* menghasilkan *packet loss* sebesar 0%, rata-rata *delay* sebesar 7 ms, serta *jitter* sekitar 27 ms. Hasil pengujian *throughput* menggunakan iPerf3 menunjukkan gambar 16 bahwa ZeroTier mampu menghasilkan *throughput* sebesar 99 Mbps selama proses transmisi data berlangsung.



Gambar 15. Pengujian Ping ZeroTier
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Gambar 16. Pengujian Throughput ZeroTier
Sumber: Hasil Tangkapan Layar Peneliti (2026)

Gambar 17, hasil pengujian Wireshark menunjukkan adanya TCP *Retransmission*, *Duplicate* ACK, dan *Previous Segment Not Captured* yang menandakan terdapat paket yang dikirim ulang, ACK yang muncul berulang, serta paket yang tidak tertangkap selama proses *capture* jaringan berlangsung.

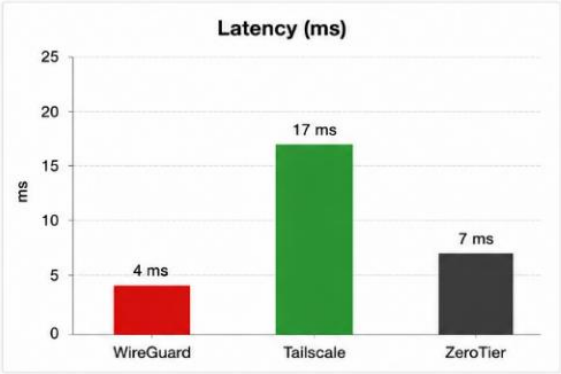


Gambar 17. *Packet Behavior* ZeroTier
Sumber: Hasil Tangkapan Layar Peneliti (2026)

ANALISIS QoS

Latency

Berdasarkan diagram *latency* pada gambar 18, diperoleh bahwa VPN WireGuard menghasilkan nilai *latency* paling rendah sebesar 4 ms, ZeroTier sebesar 7 ms, sedangkan Tailscale menghasilkan *latency* tertinggi sebesar 17 ms. Hasil ini menunjukkan bahwa WireGuard memiliki performa terbaik dalam hal waktu tunda pengiriman paket dibandingkan dengan Tailscale dan ZeroTier.



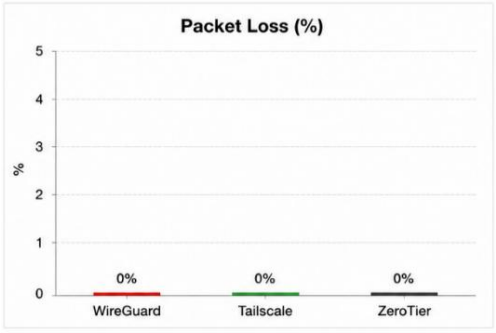
Gambar 18. Diagram *Latency*
Sumber: Hasil Pengolahan Data Penelitian (2026)

Rendahnya nilai *latency* pada WireGuard disebabkan oleh protokol yang lebih ringan dan mekanisme *tunneling* yang sederhana sehingga proses enkapsulasi dan dekripsi paket dapat dilakukan dengan lebih cepat. Sementara itu, Tailscale menghasilkan *latency* yang lebih tinggi karena menggunakan jaringan *overlay* berbasis WireGuard yang melibatkan proses koordinasi tambahan melalui *control plane* dan kemungkinan penggunaan *relay node* ketika koneksi *peer-to-peer* tidak dapat terbentuk secara langsung. ZeroTier menghasilkan nilai *latency* yang lebih rendah dibandingkan Tailscale, namun masih lebih tinggi daripada WireGuard karena adanya mekanisme virtualisasi jaringan yang menambah *overhead* selama proses transmisi data.

Secara keseluruhan, seluruh VPN masih menghasilkan nilai *latency* yang tergolong sangat baik (<150 ms berdasarkan standar TIPHON). Namun, WireGuard menjadi pilihan yang paling optimal untuk implementasi SD-WAN karena mampu memberikan waktu respon tercepat dan komunikasi jaringan yang lebih efisien dibandingkan Tailscale dan ZeroTier.

Packet Loss

Berdasarkan diagram gambar 19, seluruh VPN yaitu WireGuard, Tailscale, dan ZeroTier menghasilkan nilai *packet loss* sebesar 0%. Hasil tersebut menunjukkan bahwa tidak terdapat paket data yang hilang selama proses transmisi berlangsung sehingga komunikasi jaringan pada implementasi SD-WAN dapat berjalan dengan baik dan stabil.



Gambar 19. Diagram *Packet Loss*
Sumber: Hasil Pengolahan Data Penelitian (2026)

Jitter

Berdasarkan diagram *jitter* pada gambar 20, diperoleh bahwa VPN WireGuard menghasilkan nilai *jitter* paling rendah sebesar 2 ms, ZeroTier menghasilkan *jitter* sebesar 27 ms dan Tailscale sebesar 60 ms. Hasil ini menunjukkan bahwa WireGuard memiliki performa terbaik dalam menjaga kestabilan waktu kedatangan paket dibandingkan dengan Tailscale dan ZeroTier.

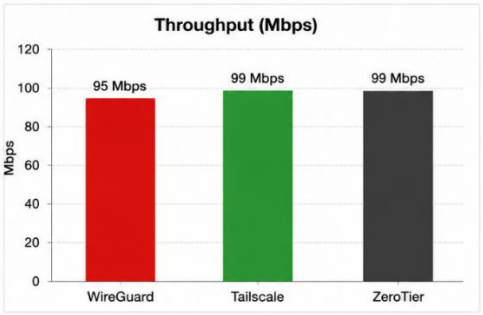
Gambar 20. Diagram *Jitter*
Sumber: Hasil Pengolahan Data Penelitian (2026)

Rendahnya nilai *jitter* pada WireGuard menunjukkan bahwa variasi waktu tunda antar paket sangat kecil, sehingga aliran data dapat ditransmisikan secara lebih konsisten dan stabil. Sebaliknya, nilai *jitter* yang lebih tinggi pada Tailscale mengindikasikan adanya fluktuasi *delay* yang lebih besar selama proses transmisi data. Hal ini dapat disebabkan oleh mekanisme jaringan *overlay* dan proses routing tambahan yang digunakan Tailscale. Sementara itu, ZeroTier menghasilkan nilai *jitter* yang lebih rendah dibandingkan Tailscale, namun masih lebih tinggi daripada WireGuard karena adanya *overhead* virtualisasi jaringan yang memengaruhi kestabilan pengiriman paket.

Berdasarkan standar TIPHON, nilai *jitter* WireGuard sebesar 2 ms, Tailscale sebesar 60 ms, dan ZeroTier sebesar 27 ms masih termasuk dalam kategori baik. Namun, WireGuard memberikan kualitas layanan yang paling optimal karena mampu menghasilkan variasi *delay* yang paling rendah, sehingga lebih sesuai untuk aplikasi yang sensitif terhadap perubahan waktu transmisi, seperti komunikasi *real-time* dan layanan multimedia.

Throughput

Berdasarkan diagram *throughput* pada gambar 21, diperoleh bahwa VPN Tailscale dan ZeroTier menghasilkan *throughput* tertinggi sebesar 99 Mbps, sedangkan WireGuard menghasilkan *throughput* sebesar 95 Mbps. Hasil ini menunjukkan bahwa ketiga provider VPN mampu memanfaatkan *bandwidth* jaringan secara optimal dengan perbedaan *throughput* yang relatif kecil.



Gambar 21. Diagram *Throughput*
Sumber: Hasil Pengolahan Data Penelitian (2026)

Tingginya nilai *throughput* pada Tailscale dan ZeroTier menunjukkan bahwa kedua VPN tersebut mampu mentransmisikan data dengan laju yang mendekati kapasitas *bandwidth* yang tersedia. Sementara itu, WireGuard menghasilkan *throughput* yang sedikit lebih rendah, yang dapat disebabkan oleh *overhead* proses enkapsulasi dan mekanisme pengamanan data selama transmisi. Namun demikian, selisih *throughput* yang dihasilkan tidak terlalu signifikan sehingga tidak memberikan pengaruh yang besar terhadap performa jaringan.

Secara keseluruhan, ketiga VPN menunjukkan performa *throughput* yang sangat baik karena mampu mencapai lebih dari 95% dari kapasitas *bandwidth* 100 Mbps yang digunakan pada pengujian. Berdasarkan hasil tersebut, Tailscale dan ZeroTier memiliki performa terbaik pada parameter *throughput* dengan nilai 99 Mbps, sedangkan WireGuard tetap menunjukkan kinerja yang baik dengan *throughput* sebesar 95 Mbps.

KESIMPULAN

Berdasarkan hasil implementasi dan pengujian QoS pada infrastruktur SD-WAN, seluruh VPN berhasil membangun komunikasi antar *site* dengan baik melalui *tunnel* VPN yang ditunjukkan oleh nilai *packet loss* 0%. Hasil pengujian *throughput* menunjukkan bahwa Tailscale dan ZeroTier menghasilkan *throughput* 99 Mbps, sedangkan WireGuard menghasilkan *throughput* 95 Mbps. Selain itu, hasil pengujian *latency* dan *jitter* menunjukkan bahwa Wireguard memiliki performa paling stabil dengan nilai *latency* 4 ms dan *jitter* 2 ms dibandingkan dengan VPN lainnya.

Hasil analisis *packet behavior* menggunakan Wireshark, ditemukan adanya TCP *Retransmission*, *Duplicate* ACK, dan *Previous Segment Not Captured* pada seluruh teknologi VPN selama proses transmisi data berlangsung. Kondisi tersebut menunjukkan adanya paket yang dikirim ulang, ACK yang muncul berulang, serta paket yang tidak tertangkap selama proses *capture* jaringan. Namun demikian, kondisi tersebut tidak memberikan pengaruh

signifikan terhadap kualitas komunikasi jaringan karena seluruh VPN masih mampu mempertahankan performa jaringan yang baik selama pengujian berlangsung.

Secara keseluruhan, implementasi multi VPN *tunnel* pada infrastruktur SD-WAN mampu mendukung komunikasi jaringan yang stabil dan efisien. Berdasarkan parameter QoS yang telah diuji, WireGuard menunjukkan kualitas komunikasi jaringan yang lebih baik dan stabil dibandingkan Tailscale dan ZeroTier karena menghasilkan *latency* dan *jitter* yang lebih rendah. Oleh karena itu, WireGuard dinilai lebih optimal untuk diterapkan pada implementasi SD-WAN yang membutuhkan performa komunikasi jaringan dengan tingkat kestabilan yang tinggi.

DAFTAR PUSTAKA

Abdulazeez, A. M., Salim, B. W., Zeebaree, D. Q., & Doghramachi, D. (2020a). Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol. *International Journal of Interactive Mobile Technologies (IJIM)*, *14*(18), 157. https://doi.org/10.3991/ijim.v14i18.16507

Abdulazeez, A. M., Salim, B. W., Zeebaree, D. Q., & Doghramachi, D. (2020b). Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol. *International Journal of Interactive Mobile Technologies (IJIM)*, *14*(18), 157. https://doi.org/10.3991/ijim.v14i18.16507

Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025a). Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions. *Computers*, *14*(8), 326. https://doi.org/10.3390/computers14080326

Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025b). Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions. *Computers*, *14*(8), 326. https://doi.org/10.3390/computers14080326

Arifwidodo, B. (2023). Mekanisme Keamanan Jaringan Menggunakan Protokol Wireguard Pada Jaringan Privat. *Journal of Informatics and Communication Technology (JICT)*, *5*(2), 78–86. https://doi.org/10.52661/j_ict.v5i2.211

Dudczyk, J., Sergiel, M., & Krygier, J. (2025). Analysis of SD-WAN Architectures and Techniques for Efficient Traffic Control Under Transmission Constraints—Overview of Solutions. *Sensors*, *25*(20), 6317. https://doi.org/10.3390/s25206317

Fu, C., Wang, B., Liu, H., & Wang, W. (2024). Software-Defined Virtual Private Network for SD-WAN. *Electronics*, *13*(13), 2674. https://doi.org/10.3390/electronics13132674

Gentile, A. F., Macrì, D., Greco, E., & Fazio, P. (2024). Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment. *Future Internet*, *16*(8), 283. https://doi.org/10.3390/fi16080283

Haeruddin, H., Wijaya, G., & Khatimah, H. (2023). Sistem Keamanan Work From Anywhere Menggunakan VPN Generasi Lanjut. *JITU : Journal Informatic Technology And Communication*, *7*(2), 102–113. https://doi.org/10.36596/jitu.v7i2.1086

Ibrahim, R., Khider, I., Edam, S., & Mukhtar, T. (2025). Comprehensive Strategies for Enhancing SD-WAN: Integrating Security, Dynamic Routing and Quality of Service Management. *IET Networks*, *14*(1). https://doi.org/10.1049/ntw2.70007

Kjorveziroski, V., Bernad, C., Gilly, K., & Filiposka, S. (2024a). 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

Kjorveziroski, V., Bernad, C., Gilly, K., & Filiposka, S. (2024b). 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

Mackey, S., Mihov, I., Nosenko, A., Vega, F., & Cheng, Y. (2020). A Performance Comparison of WireGuard and OpenVPN. *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy*, 162–164. https://doi.org/10.1145/3374664.3379532

Nisa, I. S. N., Rahmat Miyarno Saputro, Tegar Fatwa Nugroho, & Alfirna Rizqi Lahitani. (2024). Analisis Quality of Service (QoS) Menggunakan Standar Parameter Tiphon pada Jaringan Internet Berbasis Wi-Fi Kampus 1 Unjaya. *Teknomatika: Jurnal Informatika Dan Komputer*, *17*(1), 1–9. https://doi.org/10.30989/teknomatika.v17i1.1307

Ouamri, M. A., Alharbi, T., Singh, D., & Sylia, Z. (2025). A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges. *The Journal of Supercomputing*, *81*(1), 291. https://doi.org/10.1007/s11227-024-06718-1

Petrović, T., Vidaković, A., Doknić, I., Veinović, M., & Bojović, Ž. (2025). An Adaptive Application-Aware Dynamic Load Balancing Framework for Open-Source SD-WAN. *Sensors*, *25*(17), 5516. https://doi.org/10.3390/s25175516

Putra, F. P. E., Ilhamsyah, R. M., Efendy, S. A., & Rizki, A. (2025a). Implementation And Evaluation Of Zerotier-Based Virtual Network For Device Connectivity. *Brilliance: Research of Artificial Intelligence*, *5*(1), 281–290. https://doi.org/10.47709/brilliance.v5i1.5966

Putra, F. P. E., Ilhamsyah, R. M., Efendy, S. A., & Rizki, A. (2025b). Implementation And Evaluation Of Zerotier-Based Virtual Network For Device Connectivity. *Brilliance: Research of Artificial Intelligence*, *5*(1), 281–290. https://doi.org/10.47709/brilliance.v5i1.5966

Rahman, I. K., & Harnaningrum, L. N. (2024a). Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk mengamankan VoIP. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *7*(1), 10–20. https://doi.org/10.31598/jurnalresistor.v7i1.1553

Rahman, I. K., & Harnaningrum, L. N. (2024b). Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk mengamankan VoIP. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *7*(1), 10–20. https://doi.org/10.31598/jurnalresistor.v7i1.1553

Simargolang, M. Y., & Widarma, A. (2022). Quality of Service (QoS) for Network Performance Analysis Wireless Area Network (WLAN). *CESS (Journal of Computer Engineering, System and Science)*, *7*(1), 162. https://doi.org/10.24114/cess.v7i1.29758

Troia, S., Sapienza, F., Vare, L., & Maier, G. (2021a). On Deep Reinforcement Learning for Traffic Engineering in SD-WAN. *IEEE Journal on Selected Areas in Communications*, *39*(7), 2198–2212. https://doi.org/10.1109/JSAC.2020.3041385

Troia, S., Sapienza, F., Vare, L., & Maier, G. (2021b). On Deep Reinforcement Learning for Traffic Engineering in SD-WAN. *IEEE Journal on Selected Areas in Communications*, *39*(7), 2198–2212. https://doi.org/10.1109/JSAC.2020.3041385