

Implementasi dan Analisis Keamanan VPN Menggunakan WireGuard pada Jaringan MikroTik di PT Jakarta International Security Service

Muhammad Bayram Arajeeba Tasdikin^{1*}, Ali Mulyanto², Anik Sri Wahyuningsih³
¹⁻³ Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Panca Sakti
Bekasi, Bekasi, Indonesia

*Corresponding Email: bisnisbayram@gmail.com¹, alimulyanto.6.psub@gmail.com²,
anikpsu79@gmail.com³

Abstrak: Penelitian ini bertujuan mengimplementasikan dan menganalisis keamanan Remote Access Virtual Private Network (VPN) menggunakan WireGuard pada jaringan MikroTik di PT Jakarta International Security Service. Permasalahan berawal dari lokasi perusahaan yang belum dapat dijangkau layanan ISP dengan IP Public langsung sehingga perangkat MikroTik dan jaringan internal sulit diakses dari luar lokasi, sedangkan akses jarak jauh tanpa pengamanan yang memadai berisiko terhadap penyadapan trafik dan akses tidak sah. Penelitian menggunakan metode eksperimen dengan pendekatan kuantitatif melalui tahapan analisis kebutuhan, perancangan, implementasi, pengujian, evaluasi, dan penyempurnaan konfigurasi. MikroTik RB5009UG+S+ dengan RouterOS 7.19.6 dikonfigurasi sebagai VPN Server dan laptop sebagai VPN Client yang terhubung melalui Internet, dengan konfigurasi interface WireGuard, pasangan public key dan private key, alamat IP tunnel, peer, routing, dan firewall. Hasil pengujian menunjukkan tunnel berstatus aktif dengan handshake berhasil, keempat paket ICMP ke alamat tunnel MikroTik diterima (packet loss 0%) dengan waktu tempuh rata-rata 66 ms melalui hotspot ponsel, dan client dapat mengakses jaringan internal sesuai konfigurasi routing dan firewall. Validasi ahli menghasilkan rata-rata skor 4,90 (Sangat Baik) dengan kesimpulan layak digunakan tanpa revisi. Sistem dinilai layak sebagai solusi akses jaringan jarak jauh, dengan keberhasilan yang tetap bergantung pada kualitas koneksi Internet serta ketelitian konfigurasi peer, alamat IP, routing, dan firewall. Evaluasi performa pada penelitian ini masih terbatas pada latensi dan packet loss.

Kata kunci: VPN; WireGuard; MikroTik; Keamanan Jaringan; Remote Access; Firewall

Abstract: This study aims to implement and analyze the security of a Remote Access Virtual Private Network (VPN) using WireGuard on the MikroTik network at PT Jakarta International Security Service. The research was motivated by the company's location, which cannot be directly served by an Internet Service Provider (ISP) offering a public IP address, making it difficult to access MikroTik devices and the internal network from outside the premises. Furthermore, remote access without adequate security measures poses risks of traffic interception and unauthorized access. This study employed an experimental method with a quantitative approach, consisting of several stages: requirements analysis, system design, implementation, testing, evaluation, and configuration refinement. A MikroTik RB5009UG+S+ running RouterOS 7.19.6 was configured as the VPN server, while a laptop served as the VPN client connected via the Internet. The configuration included the WireGuard interface, public and private key pairs, tunnel IP addresses, peers, routing, and firewall rules. The testing results demonstrated that the VPN tunnel was active with a successful handshake. All four Internet Control Message Protocol (ICMP) packets sent to the MikroTik tunnel address were successfully received, resulting in 0% packet loss and an average round-trip time of 66 ms over a mobile phone hotspot connection. The VPN client was also able to access the internal network in accordance with the configured routing and firewall rules. Expert validation yielded an average score of 4.90, categorized as "Very Good," indicating that the system was suitable for implementation without revision. The findings suggest that the proposed system is a feasible solution for secure remote network access, although its successful operation remains dependent on Internet connection quality and the accuracy of peer, IP addressing, routing, and firewall configurations. However, the performance evaluation in this study was limited to latency and packet loss measurements.

Keywords: VPN; WireGuard; MikroTik; Network Security; Remote Access; Firewall

PENDAHULUAN

Perkembangan teknologi informasi menuntut perusahaan memiliki jaringan komputer yang aman, stabil, dan dapat diakses secara fleksibel. Kebutuhan akses jaringan tidak hanya muncul dari dalam kantor, tetapi juga dari luar lokasi untuk mendukung kegiatan administrasi, pemantauan perangkat, pengelolaan server, dan akses terhadap sumber daya jaringan internal.

Oleh karena itu, perusahaan memerlukan mekanisme akses jarak jauh yang mampu menjaga keamanan komunikasi data ketika melewati jaringan Internet.

PT Jakarta International Security Service membutuhkan akses jaringan yang aman untuk mendukung kegiatan operasional dan pengelolaan perangkat teknologi informasi. Hasil pengamatan menunjukkan bahwa lokasi perusahaan belum dapat dijangkau layanan ISP yang menyediakan IP Public secara langsung, sehingga perangkat jaringan di lokasi tidak memperoleh IP Public statis yang dapat menjadi alamat tujuan akses dari Internet. Kondisi ini menyulitkan administrator mengakses perangkat MikroTik, server, dan jaringan internal dari luar lokasi. Di sisi lain, penggunaan koneksi Internet biasa tanpa pengamanan yang memadai meningkatkan risiko penyadapan trafik, pencurian data, akses tidak sah, dan serangan man-in-the-middle, sedangkan membuka layanan internal langsung ke Internet memperbesar risiko terhadap perangkat dan data perusahaan.

Virtual Private Network (VPN) dapat menjadi solusi karena membangun jalur komunikasi privat melalui jaringan Internet dengan mekanisme autentikasi dan enkripsi, sehingga client dari luar jaringan dapat terhubung ke jaringan internal tanpa membuka layanan internal secara langsung. Panduan NIST telah membahas pengamanan VPN berbasis IPsec dan SSL (Jansen & Scarfone, 2005; Frankel et al., 2008), sedangkan WireGuard merupakan protokol VPN yang lebih baru dengan rancangan sederhana, menggunakan pasangan public key dan private key untuk mengidentifikasi peer, serta berkomunikasi melalui UDP (Donenfeld, 2020). Keamanan protokol ini telah dianalisis melalui pembuktian kriptografis termekanisasi (Lipp et al., 2019), dan WireGuard tersedia pada MikroTik RouterOS versi 7 sehingga dapat dikonfigurasi langsung pada router (MikroTik, 2026b).

Beberapa penelitian telah membahas penerapan WireGuard pada MikroTik. Ikhwindi et al. (2025) mengimplementasikan WireGuard sebagai koneksi dengan routing MikroTik, dan Novianto et al. (2022) menerapkan WireGuard VPN pada RouterBoard MikroTik untuk mengamankan akses terhadap website. Muhajir dan Utami (2026) membandingkan performa WireGuard dan OpenVPN pada VPN berbasis MikroTik dengan parameter round-trip time, jitter, packet loss, throughput, serta penggunaan CPU dan memori. Penelitian tersebut menunjukkan bahwa analisis VPN perlu menilai kualitas koneksi setelah VPN diterapkan, tidak hanya keberhasilan koneksinya.

Penelitian ini memiliki perbedaan pada kondisi lokasi objek, yaitu perusahaan yang belum dapat memperoleh layanan IP Public langsung dari ISP. Oleh karena itu, penelitian ini mengimplementasikan Remote Access VPN WireGuard pada MikroTik yang tetap dapat dijangkau dari luar lokasi melalui endpoint perantara yang memiliki IP Public, serta menganalisis konfigurasi peer, alamat IP tunnel, routing, firewall, dan hasil pengujiannya.

Tujuan penelitian ini adalah: (1) merancang dan mengimplementasikan Remote Access VPN menggunakan WireGuard pada MikroTik RB5009UG+S+; (2) mengonfigurasi MikroTik sebagai VPN Server dan laptop sebagai VPN Client; (3) menguji kemampuan client terhubung dan mengakses jaringan internal melalui tunnel WireGuard; (4) menganalisis mekanisme keamanan komunikasi data yang diterapkan WireGuard; (5) mengevaluasi kualitas koneksi berdasarkan latensi dan packet loss; dan (6) menilai kelayakan sistem melalui validasi ahli.

METODE

Desain dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif. Metode eksperimen dipilih karena penelitian memberikan perlakuan berupa implementasi Remote Access VPN menggunakan WireGuard pada MikroTik RB5009UG+S+, kemudian melakukan pengujian untuk mengetahui keberhasilan implementasi serta pengaruhnya terhadap keamanan dan performa komunikasi jaringan. Pendekatan kuantitatif digunakan karena pengujian menghasilkan data berupa angka, seperti latensi dan packet loss.

Teknik penelitian berupa eksperimen dan observasi. Eksperimen dilakukan dengan mengimplementasikan WireGuard pada MikroTik dan menghubungkan laptop sebagai VPN Client melalui Internet, sedangkan observasi dilakukan terhadap hasil koneksi, status WireGuard, dan performa jaringan selama pengujian. Variabel bebas penelitian adalah implementasi Remote Access VPN menggunakan WireGuard, dan variabel terikatnya adalah keamanan serta performa komunikasi jaringan. Penelitian dilakukan melalui enam tahapan yang dirangkum pada Tabel 1.

Tabel 1. Tahapan Penelitian

Tahap	Kegiatan	Keluaran
Analisis kebutuhan	Menentukan perangkat, perangkat lunak, dan parameter konfigurasi	Daftar kebutuhan
Perancangan	Menyusun topologi, alamat IP, rancangan peer, dan firewall	Rancangan jaringan
Implementasi	Mengonfigurasi WireGuard pada MikroTik dan client	Tunnel WireGuard
Pengujian	Menguji handshake, konektivitas, dan akses jaringan internal	Data hasil uji
Evaluasi	Menganalisis hasil pengujian dan validasi ahli	Tingkat kelayakan
Penyempurnaan	Memperbaiki konfigurasi peer, routing, dan firewall	Konfigurasi akhir

Sumber: Data diolah peneliti, 2026

Tempat, Waktu, dan Sasaran Penelitian

Penelitian dilaksanakan di PT Jakarta International Security Service pada tahun 2026, mencakup studi pendahuluan, studi pustaka, analisis kebutuhan, perancangan jaringan, konfigurasi MikroTik, implementasi WireGuard, pengujian, pengumpulan dan analisis data, serta penyusunan laporan. Sasaran penelitian meliputi satu unit MikroTik RB5009UG+S+ sebagai VPN Server, satu unit laptop sebagai VPN Client, dan satu ahli sebagai validator sistem.

Kebutuhan Perangkat dan Teknologi

Kebutuhan perangkat ditentukan pada tahap analisis kebutuhan dan dirangkum pada Tabel 2. Selain perangkat, ditentukan pula kebutuhan konfigurasi berupa alamat IP, interface WireGuard, public key, private key, peer, endpoint, routing, dan firewall. WireGuard dipilih karena menggunakan kriptografi modern dengan konfigurasi yang relatif sederhana (Donenfeld, 2020), yaitu Curve25519 untuk pertukaran kunci, ChaCha20-Poly1305 untuk authenticated encryption, BLAKE2s sebagai fungsi hash, dan HKDF untuk derivasi kunci (WireGuard, n.d.).

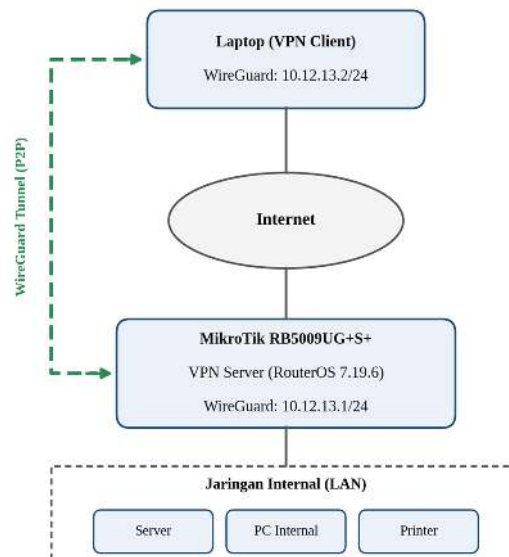
Tabel 2. Perangkat dan Perangkat Lunak Penelitian

Komponen	Spesifikasi	Fungsi
Router	MikroTik RB5009UG+S+, RouterOS 7.19.6	VPN Server
Perangkat client	Laptop berbasis Windows	VPN Client dan perangkat uji
Aplikasi client	WireGuard	Membuat koneksi ke MikroTik
Aplikasi konfigurasi	WinBox	Konfigurasi dan pemantauan router
Perangkat uji jaringan	ICMP ping dan tracert	Mengukur latensi dan packet loss

Sumber: Data diolah peneliti, 2026

Perancangan Sistem

Arsitektur sistem menempatkan MikroTik RB5009UG+S+ sebagai VPN Server dan laptop sebagai VPN Client yang terhubung melalui tunnel WireGuard peer-to-peer melalui Internet, sebagaimana ditunjukkan pada Gambar 1. Alamat tunnel MikroTik adalah 10.12.13.1/24 dan alamat client adalah 10.12.13.2/24. Karena lokasi perusahaan belum memperoleh IP Public langsung, ketersediaan endpoint dari Internet dibatasi pada penggunaan layanan penghubung pihak ketiga, seperti VPS/CHR atau Cloud VPN, sebagai endpoint perantara.



Gambar 1. Topologi Jaringan Remote Access VPN WireGuard

Sumber: Data diolah peneliti, 2026

Peer dirancang dengan parameter public key, allowed address, endpoint address, endpoint port, dan persistent keepalive apabila diperlukan. Rancangan firewall mencakup pengizinan port UDP yang digunakan WireGuard, pengizinan trafik VPN yang diperlukan, pembatasan akses terhadap router, pengaturan forwarding antara jaringan VPN dan jaringan

lokal, serta penolakan trafik yang tidak diperlukan, dengan mengacu pada panduan pengamanan router MikroTik (MikroTik, 2026a) dan prinsip kebijakan firewall (Scarfone & Hoffman, 2009).

Tahapan Implementasi

Implementasi dilakukan dengan membuat interface WireGuard pada MikroTik beserta private key dan public key, menentukan listen port, dan memberikan alamat IP pada interface. Selanjutnya dibuat peer untuk laptop dengan memasukkan public key client dan menentukan allowed address, kemudian dilakukan konfigurasi routing dan firewall. Pada sisi client, profil WireGuard dikonfigurasi pada laptop dan dihubungkan ke VPN Server, lalu status handshake diperiksa untuk memastikan koneksi berhasil.

Teknik Pengujian dan Validasi

Pengujian dilakukan pada perangkat fisik dalam tiga kelompok pemeriksaan. Pertama, pembentukan tunnel diperiksa melalui status interface pada client serta status peer dan last handshake pada MikroTik. Kedua, konektivitas diuji menggunakan ping dan tracert dari client ke alamat tunnel MikroTik, serta akses ke perangkat dan layanan pada jaringan internal untuk menilai routing dan firewall. Ketiga, lalu lintas data diamati pada interface WireGuard di MikroTik. Latensi dan packet loss diperoleh dari hasil ping.

Kelayakan sistem divalidasi melalui kuesioner berskala Likert 1–5 yang diisi oleh satu ahli dengan empat aspek, yaitu desain dan konfigurasi sistem, fungsionalitas dan kinerja VPN, keamanan VPN dan manajemen akses, serta kemudahan pengelolaan dan pemeliharaan, dengan total 21 pernyataan. Kategori penilaian ditentukan dengan interval $(5 - 1) \div 5 = 0,80$, sehingga rata-rata 4,21–5,00 dikategorikan Sangat Baik. Persentase kelayakan dihitung dengan rumus $(\text{rata-rata skor} \div \text{skor maksimum}) \times 100\%$. Validator juga memilih salah satu kesimpulan, yaitu layak digunakan tanpa revisi, layak digunakan dengan revisi, atau tidak layak digunakan.

HASIL DAN PEMBAHASAN

Hasil Implementasi Sistem

Implementasi menghasilkan tunnel WireGuard antara MikroTik RB5009UG+S+ sebagai VPN Server dan laptop sebagai VPN Client. Pada MikroTik dibuat interface WireGuard dengan alamat 10.12.13.1/24, kemudian dibuat peer untuk client dengan memasukkan public key client. Pada laptop dibuat profil WireGuard dengan alamat 10.12.13.2/24. Parameter konfigurasi yang digunakan dirangkum pada Tabel 3. Private key disimpan pada perangkat masing-masing, sedangkan public key digunakan pada konfigurasi peer sebagai identitas peer (Donenfeld, 2020).

Tabel 3. Parameter Konfigurasi WireGuard

Parameter	Nilai
VPN Server	MikroTik RB5009UG+S+ (RouterOS 7.19.6)
Interface WireGuard	Koneksi_Bayram, MTU 1420
Alamat tunnel server	10.12.13.1/24 (jaringan 10.12.13.0)
Alamat tunnel client	10.12.13.2/24
Autentikasi peer	Pasangan public key dan private key

Parameter	Nilai
Allowed address peer	10.12.13.0/24 dan 0.0.0.0/0
DNS client	8.8.8.8

Sumber: Data diolah peneliti, 2026

Hasil Pengujian Konektivitas

Setelah profil diaktifkan, aplikasi WireGuard pada client menampilkan status Active dengan latest handshake yang tercatat, sedangkan peer pada MikroTik menampilkan last handshake serta jumlah data yang dikirim dan diterima. Hal ini menunjukkan bahwa peer berhasil melakukan handshake dan bertukar data melalui tunnel.

Pengujian konektivitas dilakukan dengan client yang terhubung ke Internet melalui hotspot ponsel, sehingga pengujian berasal dari luar jaringan internal perusahaan. Hasilnya dirangkum pada Tabel 4. Keempat paket ICMP ke alamat tunnel MikroTik dibalas dengan waktu 54–80 ms (rata-rata 66 ms) tanpa packet loss, dan tracert menunjukkan tujuan dicapai pada satu hop, yang menandakan trafik menuju MikroTik dikirim langsung melalui tunnel. Halaman login aplikasi web perusahaan juga dapat dimuat pada peramban client. Pada pengamatan ping berkelanjutan melalui jaringan Wi-Fi yang berbeda, waktu balasan yang terekam berkisar 38–126 ms.

Tabel 4. Hasil Pengujian Konektivitas Client

Parameter	Hasil
Kondisi pengujian	Client melalui hotspot ponsel, tunnel aktif
Status tunnel pada client	Active
Handshake	Tercatat pada client dan peer MikroTik
Tujuan ping	10.12.13.1 (alamat tunnel MikroTik)
Paket dikirim / diterima	4 / 4
Packet loss	0%
RTT minimum / maksimum / rata-rata	54 ms / 80 ms / 66 ms
TTL	64
Tracert	1 hop (73 ms, 57 ms, 59 ms)
Akses aplikasi web perusahaan	Halaman login berhasil dimuat

Sumber: Data diolah peneliti, 2026

Hasil Validasi Ahli

Validasi oleh satu ahli menghasilkan rata-rata total 4,90 dengan kategori Sangat Baik dan persentase kelayakan sebesar 98% (Tabel 5). Nilai tertinggi (5,00) diperoleh pada aspek desain dan konfigurasi sistem serta aspek kemudahan pengelolaan dan pemeliharaan. Dari 21 pernyataan, 19 pernyataan bernilai 5 dan dua pernyataan bernilai 4, yaitu kinerja koneksi (kecepatan dan waktu respons) serta pembatasan koneksi hanya bagi perangkat atau pengguna yang terdaftar. Validator menyatakan sistem layak digunakan tanpa revisi.

Tabel 5. Hasil Validasi Ahli

Aspek Penilaian	Jumlah Butir	Rata-rata	Kategori
Desain dan Konfigurasi Sistem	5	5,00	Sangat Baik
Fungsionalitas dan Kinerja VPN	5	4,80	Sangat Baik
Keamanan VPN dan Manajemen Akses	6	4,83	Sangat Baik
Kemudahan Pengelolaan dan Pemeliharaan	5	5,00	Sangat Baik
Rata-rata Total	21	4,90	Sangat Baik

Sumber: Data diolah peneliti, 2026

Pembahasan

Hasil penelitian menunjukkan bahwa Remote Access VPN menggunakan WireGuard pada MikroTik RB5009UG+S+ dapat memberikan akses jaringan dari luar jaringan lokal. Dengan endpoint perantara, keterbatasan IP Public pada lokasi perusahaan dapat diatasi, tunnel dapat terbentuk dengan handshake berhasil, dan client dapat berkomunikasi dengan MikroTik serta mengakses jaringan internal sesuai konfigurasi routing dan firewall.

Dari sisi keamanan, WireGuard mengautentikasi peer berdasarkan pasangan kunci sehingga hanya peer dengan public key yang terdaftar pada konfigurasi yang dapat membentuk tunnel, sedangkan data pada tunnel dilindungi authenticated encryption (Donenfeld, 2020; WireGuard, n.d.). Pengaturan akses dilakukan melalui allowed address, routing, dan firewall pada MikroTik sehingga administrator dapat menentukan jaringan atau alamat IP yang dapat diakses client. Karena allowed address pada client diatur 0.0.0.0/0, pembatasan akses ke sumber daya internal perlu ditegaskan melalui aturan firewall yang sesuai (Scarfone & Hoffman, 2009; MikroTik, 2026a). Pada penilaian validator, satu-satunya pernyataan pada aspek keamanan yang tidak bernilai 5 adalah pembatasan koneksi hanya bagi perangkat atau pengguna terdaftar, sehingga aspek ini dapat menjadi fokus pengembangan konfigurasi firewall.

Dari sisi performa, tidak terdapat packet loss pada pengujian ping dengan latensi rata-rata 66 ms melalui hotspot ponsel. Latensi bergantung pada kualitas jaringan Internet yang digunakan client, sebagaimana terlihat dari variasi waktu balasan pada pengamatan melalui Wi-Fi, dan sejalan dengan penilaian validator yang memberi nilai 4 pada kinerja koneksi. Hal ini mendukung temuan Muhajir dan Utami (2026) bahwa evaluasi VPN perlu memperhatikan kualitas koneksi, tidak hanya keberhasilan koneksi.

Beberapa faktor mendukung penerapan sistem. MikroTik RB5009UG+S+ dapat berperan sebagai router sekaligus VPN Server sehingga tidak memerlukan perangkat tambahan khusus. Konfigurasi WireGuard relatif sederhana karena setiap client menggunakan peer yang telah ditentukan, sehingga penambahan client dilakukan dengan menambah peer pada MikroTik dan konfigurasi pada perangkat client, sebagaimana juga diterapkan pada MikroTik oleh Ikhwandi et al. (2025) dan Novianto et al. (2022). Aplikasi WireGuard pada client memudahkan pengguna mengaktifkan koneksi, dan akses setiap client dapat dikontrol dari MikroTik.

Faktor penghambat meliputi ketergantungan pada koneksi Internet, baik di sisi client maupun lokasi MikroTik, serta ketepatan konfigurasi alamat IP, peer, routing, dan firewall karena kesalahan pada bagian tersebut dapat membuat client tidak terhubung atau tidak dapat mengakses jaringan internal. Client juga dapat menggunakan jaringan yang berbeda, seperti Wi-Fi, jaringan seluler, atau jaringan publik, yang memengaruhi kualitas koneksi dan memiliki pertimbangan keamanannya sendiri (Souppaya & Scarfone, 2012). Selain itu, pengelolaan client dalam jumlah banyak memerlukan pencatatan peer yang teratur agar tidak terjadi kesalahan konfigurasi.

Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan. Pengujian dilakukan pada satu VPN Client di satu lokasi dan divalidasi oleh satu ahli, sehingga hasilnya belum menggambarkan penggunaan oleh banyak client secara bersamaan. Evaluasi performa terbatas pada latensi dan packet loss melalui ICMP. Pengukuran throughput, jitter, dan penggunaan CPU serta RAM MikroTik, perbandingan dengan kondisi tanpa VPN, serta analisis paket menggunakan Wireshark belum dilaporkan pada naskah ini, sehingga perlindungan enkripsi didasarkan pada mekanisme protokol WireGuard dan belum dibuktikan melalui pengamatan trafik. Cakupan pengujian dibatasi pada akses client menuju jaringan internal, dan pengaturan firewall dibatasi pada pembagian subnet tunnel, alokasi alamat IP, serta aturan hak akses dasar.

SIMPULAN

Penelitian ini berhasil mengimplementasikan Remote Access VPN menggunakan WireGuard pada MikroTik RB5009UG+S+ sebagai VPN Server dan laptop sebagai VPN Client di PT Jakarta International Security Service. Client dapat terhubung ke tunnel WireGuard dan mengakses jaringan internal, sedangkan akses setiap client dapat dikelola melalui konfigurasi peer, routing, dan firewall pada MikroTik sehingga pengelolaan jaringan menjadi lebih terpusat.

Tunnel berstatus aktif dengan handshake berhasil, pengujian ping ke alamat tunnel MikroTik tidak mengalami packet loss dengan latensi rata-rata 66 ms, dan validasi ahli menghasilkan rata-rata 4,90 (Sangat Baik; kelayakan 98%) dengan kesimpulan layak digunakan tanpa revisi. Hasil tersebut menunjukkan bahwa sistem layak digunakan sebagai solusi akses jaringan jarak jauh yang lebih aman, dengan keberhasilan yang tetap bergantung pada kualitas koneksi Internet dan ketelitian konfigurasi. Penelitian lanjutan disarankan menguji jumlah client yang lebih banyak pada beberapa kondisi jaringan Internet, mengukur throughput, jitter, serta penggunaan CPU dan RAM disertai analisis trafik menggunakan Wireshark, mengembangkan konfigurasi firewall untuk membatasi akses sesuai hak akses masing-masing client, dan membandingkan WireGuard dengan protokol VPN lain dari segi keamanan, kecepatan, dan kestabilan koneksi.

DAFTAR PUSTAKA

- Donenfeld, J. A. (2020). WireGuard: Next generation kernel network tunnel. WireGuard. Diakses pada 28 Agustus 2026, dari <https://www.wireguard.com/papers/wireguard.pdf>
- Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2008). Guide to SSL VPNs (NIST Special Publication 800-113). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-113>
- Ikhwandhi, M. I., Azinar, A. W., & Sumarno. (2025). Implementasi WireGuard sebagai koneksi menggunakan routing MikroTik. SMATIKA: STIKI Informatika Jurnal, 15(2), 292–301. <https://doi.org/10.32664/smatika.v15i02.1898>
- Jansen, W., & Scarfone, K. (2005). Guide to IPsec VPNs (NIST Special Publication 800-77). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-77>
- Lipp, B., Blanchet, B., & Bhargavan, K. (2019). A mechanised cryptographic proof of the WireGuard virtual private network protocol. Dalam Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (hlm. 231–246). IEEE. <https://doi.org/10.1109/EuroSP.2019.00026>
- MikroTik. (2026a). Securing your router. RouterOS Documentation. Diakses pada 28 Agustus 2026, dari <https://help.mikrotik.com/docs/spaces/ROS/pages/328353/Securing%20your%20router>
- MikroTik. (2026b). WireGuard. RouterOS Documentation. Diakses pada 28 Agustus 2026, dari <https://help.mikrotik.com/docs/spaces/ROS/pages/69664792/WireGuard>

- Muhajir, F., & Utami, E. (2026). Analisis performa WireGuard dan OpenVPN pada VPN perbankan berbasis MikroTik menggunakan ICMP, iPerf3, dan Mann–Whitney. *JURIKOM (Jurnal Riset Komputer)*, 13(1), 71–84. <https://doi.org/10.30865/jurikom.v13i1.9438>
- Novianto, D., Japriadi, Y. S., & Tommy, L. (2022). Implementasi keamanan akses terhadap website menggunakan WireGuard VPN di RouterBoard MikroTik. *Jurnal Ilmiah Informatika Global*, 13(2), 139–145. <https://doi.org/10.36982/jiig.v13i2.2308>
- Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy (NIST Special Publication 800-41 Revision 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-41r1>
- Souppaya, M., & Scarfone, K. (2012). Guidelines for securing wireless local area networks (WLANs) (NIST Special Publication 800-153). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-153>
- WireGuard. (n.d.). Protocol and cryptography. Diakses pada 28 Agustus 2026, dari <https://www.wireguard.com/protocol/>