Department of Digital Business
**Journal of Artificial Intelligence and Digital Business (RIGGS)**
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 16277-16284
P-ISSN: 2963-9298, e-ISSN: 2963-914X

# Perancangan VPN Site-to-Site pada Server Debian dengan Protokol Wireguard dan Metode Elliptic Curve Cryptography

Sonia Elvrida Saragih, Wilfred Raimond Zebua, Dwiki Prihatin Zalukhu, Lotar Mateus Sinaga
Teknik Informatika, Ilmu Komputer, Universitas Katolik Santo Thomas Medan
soniasaragih28@gmail.com, wilfredzeb@gmail.com, dwikizalukhu@gmail.com, lotarmateus88@gmail.com

***Abstrak***

*Virtual Private Network (VPN) merupakan teknologi yang digunakan untuk membangun komunikasi data yang aman melalui jaringan publik. Penelitian ini bertujuan untuk merancang dan mengimplementasikan VPN site-to-site pada server Debian menggunakan protokol WireGuard dengan metode Elliptic Curve Cryptography (ECC). WireGuard dipilih karena menggunakan algoritma kriptografi modern yang mampu memberikan tingkat keamanan tinggi dengan kompleksitas komputasi yang rendah. Metode ECC yang digunakan pada WireGuard adalah Curve25519 sebagai mekanisme pertukaran kunci untuk menjamin kerahasiaan dan integritas data. Penelitian dilakukan dengan membangun dua server Debian yang saling terhubung melalui tunnel WireGuard. Pengujian dilakukan menggunakan perintah wg show untuk memverifikasi koneksi, ping untuk mengukur delay dan packet loss, iperf3 untuk mengukur throughput, serta top untuk mengetahui penggunaan sumber daya sistem. Hasil pengujian menunjukkan bahwa koneksi VPN berhasil dibangun dengan baik melalui proses handshake yang sukses pada kedua server. Nilai packet loss yang diperoleh sebesar 0% dengan rata-rata delay sebesar 2,15 ms. Pengujian throughput menghasilkan kecepatan transfer data sebesar 41,1 Mbps, sedangkan pengujian penggunaan sumber daya menunjukkan nilai CPU idle sebesar 94% pada Server A dan 98,7% pada Server B. Hasil penelitian menunjukkan bahwa implementasi VPN site-to-site menggunakan WireGuard dengan metode Elliptic Curve Cryptography mampu memberikan koneksi yang aman, stabil, dan efisien dengan penggunaan sumber daya sistem yang rendah. Dengan demikian, WireGuard dapat menjadi solusi VPN modern yang sesuai untuk diterapkan pada lingkungan jaringan yang membutuhkan keamanan tinggi dan performa yang optimal.*

*Kata kunci: WireGuard, VPN, Site-to-Site, Elliptic Curve Cryptography, Curve25519, Debian Server.*

## 1. Latar Belakang

Perkembangan teknologi jaringan komputer menyebabkan kebutuhan terhadap komunikasi data yang aman semakin meningkat. Virtual Private Network (VPN) merupakan salah satu solusi yang banyak digunakan untuk menjamin kerahasiaan dan integritas data pada jaringan publik [1].

Protokol VPN tradisional seperti IPsec dan OpenVPN memiliki tingkat keamanan yang tinggi, namun membutuhkan konfigurasi yang kompleks dan sumber daya sistem yang relatif besar. WireGuard hadir sebagai protokol VPN modern yang dirancang dengan kode yang lebih sederhana dan penggunaan algoritma kriptografi terkini [2].

WireGuard menggunakan ChaCha20-Poly1305 untuk enkripsi data dan Curve25519 sebagai mekanisme pertukaran kunci berbasis Elliptic Curve Cryptography (ECC). Penggunaan ECC memungkinkan proses autentikasi dan pertukaran kunci dilakukan dengan cepat serta memiliki tingkat keamanan tinggi dengan ukuran kunci yang relatif kecil [3].

Penelitian sebelumnya menunjukkan bahwa WireGuard memiliki performa throughput dan latensi yang lebih baik dibandingkan beberapa protokol VPN konvensional [4]. Selain itu, penggunaan Curve25519 memberikan efisiensi komputasi yang tinggi dan sangat sesuai untuk sistem dengan sumber daya terbatas [5].

Penelitian ini bertujuan merancang VPN site-to-site pada server Debian menggunakan WireGuard dan menganalisis performanya berdasarkan parameter konektivitas, throughput, delay, dan penggunaan sumber daya server.

## 2. Metode Penelitian

### 2.1. *Tahapan Penelitian*

Penelitian menggunakan metode eksperimen dengan membangun dua server Debian sebagai Server A dan Server B.

Server A menggunakan alamat lokal 192.168.18.200 dan Server B menggunakan alamat 192.168.18.201. Kedua server dikonfigurasi menggunakan WireGuard pada interface wg0 dengan jaringan virtual 10.0.0.0/24.

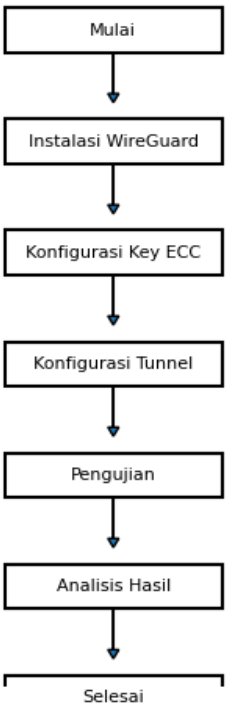
Tahapan penelitian meliputi:

1. Instalasi WireGuard pada kedua server Debian.
2. Pembuatan public key dan private key menggunakan Curve25519.
3. Konfigurasi interface WireGuard.
4. Implementasi tunnel VPN site-to-site.
5. Pengujian konektivitas menggunakan ping.
6. Pengujian throughput menggunakan iperf3.
7. Pengujian penggunaan sumber daya menggunakan top.

Parameter pengujian terdiri atas:

- Delay
- Packet loss
- Throughput
- Penggunaan CPU
- Penggunaan memori

Dibawah ini merupakan gambar diagram alur penelitian




Gambar 2.1. diagram alur penelitian

DOI: https://doi.org/10.31004/riggs.v5i2.11610

### 2.2. *Metode Pengumpulan Data*

Pengumpulan data dilakukan melalui beberapa metode sebagai berikut:

2.2.1. Studi Literatur

Studi literatur dilakukan dengan mengumpulkan referensi berupa jurnal, prosiding, buku, dan standar internasional yang berkaitan dengan WireGuard, VPN, dan Elliptic Curve Cryptography.

2.2.2. Observasi

Observasi dilakukan terhadap proses instalasi, konfigurasi, dan pengoperasian WireGuard pada kedua server Debian.

2.2.3. Eksperimen

Eksperimen dilakukan dengan mengimplementasikan VPN *site-to-site* pada dua server yang terhubung melalui jaringan lokal untuk mengetahui performa protokol WireGuard.

### 2.3. Perancangan Topologi Jaringan

Topologi yang digunakan pada penelitian ini adalah topologi site-to-site VPN yang menghubungkan dua server Debian menggunakan protokol WireGuard.

Tabel 2.1. Konfigurasi Alamat IP

| **Perangkat** | **Alamat IP** |
|---|---|
| Server A | 192.168.18.200 |
| Server B | 192.168.18.201 |
| VPN Server A | 10.0.0.1 |
| VPN Server B | 10.0.0.2 |
| Port WireGuard | 51820 |

Kedua server berfungsi sebagai *peer* yang saling terhubung melalui tunnel WireGuard.

### 2.4. *Implementasi WireGuard*

Implementasi WireGuard dilakukan dengan langkah-langkah berikut:

2.4.1. Menginstal paket WireGuard pada kedua server Debian.

2.4.2. Membuat private key dan public key menggunakan Curve25519.

2.4.3. Mengkonfigurasi interface wg0.

2.4.4. Menentukan alamat IP virtual VPN.

2.4.5. Menambahkan konfigurasi peer pada masing-masing server.

2.4.6. Mengaktifkan layanan WireGuard.

DOI: https://doi.org/10.31004/riggs.v5i2.11610

Contoh perintah aktivasi WireGuard:

sudo systemctl enable wg-quick@wg0

sudo systemctl start wg-quick@wg0

### 2.5. *Teknik Analisis Data*

Data hasil pengujian dianalisis secara deskriptif dengan membandingkan hasil pengukuran konektivitas, throughput, dan penggunaan sumber daya terhadap penelitian terdahulu yang berkaitan dengan WireGuard dan Elliptic Curve Cryptography.

Hasil analisis digunakan untuk mengetahui tingkat keamanan, efisiensi, dan performa protokol WireGuard dalam implementasi VPN *site-to-site* pada server Debian.

## 3. Hasil dan Diskusi

### 3.1. *Pengujian Koneksi WireGuard*

Pengujian koneksi WireGuard dilakukan untuk memastikan bahwa tunnel VPN site-to-site yang dibangun antara Server A dan Server B dapat beroperasi dengan baik. Pengujian dilakukan menggunakan perintah wg show pada masing-masing server untuk melihat status interface, proses pertukaran kunci (*handshake*), serta jumlah data yang berhasil ditransmisikan melalui tunnel VPN.

```
root@sonia:/etc/wireguard# wg show
interface: wg0
  public key: uqQCzu0SJRtT9PpMB/ss6OYARR148Ggs86deFRylxFA=
  private key: (hidden)
  listening port: 51820

peer: 5WXJtGlPQ6sLVksJ98MzmcwMAomg4L4YnlnyaQ+tvXc=
  endpoint: 192.168.18.201:51820
  allowed ips: 10.0.0.2/32
  latest handshake: 1 minute, 12 seconds ago
  transfer: 212 B received, 5.07 KiB sent
  persistent keepalive: every 25 seconds
```

Gambar 3.1. hasil wg show pada server A

```
root@wilfred:/etc/wireguard# wg show
interface: wg0
  public key: 5WXJtGlPQ6sLVksJ98MzmcwMAomg4L4YnlnyaQ+tvXc=
  private key: (hidden)
  listening port: 51820

peer: uqQCzu0SJRtT9PpMB/ss6OYARR148Ggs86deFRylxFA=
  endpoint: 192.168.18.200:51820
  allowed ips: 10.0.0.1/32
  latest handshake: 1 minute, 4 seconds ago
  transfer: 156 B received, 212 B sent
  persistent keepalive: every 25 seconds
```

Gambar 3.2. hasil wg show pada server B

Hasil pengujian menunjukkan bahwa kedua server berhasil membangun koneksi WireGuard melalui interface wg0. Selain itu, proses *handshake* antar server berhasil dilakukan, yang menandakan bahwa mekanisme pertukaran kunci menggunakan algoritma Curve25519 pada metode Elliptic Curve Cryptography (ECC) berjalan dengan baik.

DOI: https://doi.org/10.31004/riggs.v5i2.11610

Tabel 3.1. Status WireGuard

| Parameter | Server A | Server B |
|---|---|---|
| Interface | wg0 | wg0 |
| Status Interface | Aktif | Aktif |
| Listening Port | 51820 | 51820 |
| Peer | Terdeteksi | Terdeteksi |
| Latest Handshake | Berhasil | Berhasil |
| Transfer Data | Ada trafik | Ada trafik |
| Persistent Keepalive | 25 detik | 25 detik |

Keberhasilan handshake menunjukkan bahwa pertukaran kunci menggunakan Curve25519 berhasil dilakukan.

Berdasarkan hasil perintah wg show, kedua server berhasil mendeteksi *peer* masing-masing dan melakukan proses *handshake*. Status *latest handshake* menunjukkan bahwa pertukaran kunci publik dan kunci privat telah berhasil dilakukan.

Proses *handshake* pada WireGuard menggunakan algoritma Curve25519, yang merupakan implementasi Elliptic Curve Diffie-Hellman (ECDH). Algoritma ini memungkinkan kedua server melakukan pertukaran kunci secara aman tanpa mengirimkan kunci rahasia melalui jaringan.

Selain itu, adanya nilai transfer data pada kedua server menunjukkan bahwa paket data telah berhasil melewati tunnel VPN. Fitur Persistent Keepalive yang dikonfigurasi selama 25 detik juga membantu menjaga koneksi tetap aktif sehingga tunnel tidak terputus ketika tidak ada lalu lintas data.

### 3.2. *Pengujian Delay dan Packet Loss*

Tabel 3.2. Hasil Ping

| Parameter | Server A | Server B |
|---|---|---|
| Packet Loss | 0% | 0% |
| RTT Minimum | 1,328 ms | 1,167 ms |
| RTT Rata-rata | 2,174 ms | 2,140 ms |
| RTT Maksimum | 4,757 ms | 3,932 ms |

Nilai rata-rata delay sebesar 2,15 ms menunjukkan bahwa WireGuard memiliki latensi yang rendah.

Berdasarkan hasil pengujian menggunakan iPerf3, diperoleh nilai throughput sebesar 42,3 Mbps pada sisi pengirim (*sender*) dan 41,1 Mbps pada sisi penerima (*receiver*). Perbedaan nilai throughput antara kedua sisi relatif kecil sehingga menunjukkan bahwa proses transmisi data berlangsung secara stabil.

Jumlah data yang berhasil ditransmisikan selama pengujian mencapai 50,5 MB pada Server A dan 49,2 MB pada Server B. Selisih data yang kecil menunjukkan bahwa sebagian besar paket berhasil diterima dengan baik melalui tunnel VPN.

Selain itu, nilai retransmission sebesar 0 menunjukkan bahwa tidak terjadi pengiriman ulang paket akibat kehilangan data ataupun gangguan jaringan. Kondisi tersebut mengindikasikan bahwa koneksi VPN yang dibangun memiliki tingkat stabilitas yang baik.

DOI: https://doi.org/10.31004/riggs.v5i2.11610

### 3.3. Pengujian Throughput

Pengujian throughput dilakukan menggunakan aplikasi iPerf3 untuk mengukur kemampuan transfer data pada jaringan VPN site-to-site yang telah dibangun menggunakan WireGuard. Pengujian dilakukan dengan mengirimkan data selama 10 detik melalui tunnel VPN antara Server A dan Server B.

Tabel 3.3. Hasil iPerf3

| Parameter | Nilai |
|---|---|
| Transfer | 49,2 MB |
| Throughput | 41,1 Mbps |
| Retransmission | 0 |

Throughput yang diperoleh mencapai 41,1 Mbps dengan retransmission sebesar 0 sehingga menunjukkan stabilitas tunnel VPN.

Rendahnya penggunaan CPU dan memori pada kedua server menunjukkan bahwa WireGuard merupakan protokol VPN yang efisien dalam penggunaan sumber daya sistem. Efisiensi tersebut dipengaruhi oleh penggunaan algoritma Curve25519 pada mekanisme Elliptic Curve Cryptography (ECC) yang memiliki kompleksitas komputasi lebih rendah dibandingkan algoritma kriptografi konvensional seperti RSA.

Selain itu, desain WireGuard yang sederhana dengan jumlah kode yang relatif sedikit juga berkontribusi terhadap rendahnya konsumsi sumber daya. Hasil penelitian ini sejalan dengan penelitian Anyam et al. [1] yang menyatakan bahwa WireGuard mampu memberikan performa jaringan yang tinggi dengan penggunaan CPU yang lebih rendah dibandingkan OpenVPN.

Dengan demikian, implementasi VPN site-to-site menggunakan WireGuard pada server Debian terbukti mampu memberikan keamanan komunikasi tanpa memberikan beban yang signifikan terhadap sumber daya server. Hal ini menjadikan WireGuard sangat sesuai diterapkan pada lingkungan jaringan perusahaan, server berspesifikasi menengah, maupun perangkat dengan sumber daya terbatas.

### 3.4. Penggunaan Sumber Daya

Pengujian penggunaan sumber daya server dilakukan menggunakan perintah top pada masing-masing server Debian untuk mengetahui seberapa besar konsumsi CPU, memori, dan beban sistem selama VPN WireGuard beroperasi. Parameter yang diamati meliputi penggunaan CPU (*CPU usage*), penggunaan memori (*memory usage*), dan *load average*.

Tabel 4. Penggunaan Sistem

| Parameter | Server A | Server B |
|---|---|---|
| CPU Idle | 94% | 98,70% |
| RAM Digunakan | 1,6 GB | 1,2 GB |
| Load Average | 0,21 | 0,48 |

Penggunaan CPU yang rendah menunjukkan bahwa algoritma ECC pada Curve25519 memberikan efisiensi komputasi yang baik.

Rendahnya penggunaan CPU dan memori pada kedua server menunjukkan bahwa WireGuard merupakan protokol VPN yang efisien dalam penggunaan sumber daya sistem. Efisiensi tersebut dipengaruhi oleh penggunaan algoritma Curve25519 pada mekanisme Elliptic Curve Cryptography (ECC) yang memiliki kompleksitas komputasi lebih rendah dibandingkan algoritma kriptografi tradisional.

DOI: https://doi.org/10.31004/riggs.v5i2.11610

Selain itu, desain WireGuard yang sederhana dengan jumlah kode yang relatif sedikit turut berkontribusi terhadap rendahnya konsumsi sumber daya. Penelitian Anyam et al. [1] menunjukkan bahwa WireGuard mampu menghasilkan penggunaan CPU yang lebih rendah dibandingkan OpenVPN pada lingkungan virtualisasi. Penelitian lain oleh Demirdelen dan Kırmızı [2] juga menyatakan bahwa WireGuard memiliki efisiensi komputasi yang lebih baik dibandingkan IPSec.

Berdasarkan hasil pengujian tersebut, implementasi VPN site-to-site menggunakan WireGuard pada server Debian mampu memberikan keamanan komunikasi tanpa memberikan beban yang signifikan terhadap sumber daya server. Hal ini menjadikan WireGuard sangat sesuai diterapkan pada jaringan perusahaan maupun lingkungan dengan keterbatasan sumber daya perangkat.

### 3.5. Pembahasan

Berdasarkan hasil pengujian yang telah dilakukan, implementasi VPN *site-to-site* menggunakan protokol WireGuard pada server Debian berhasil membangun koneksi yang aman dan stabil. Hal ini dibuktikan melalui keberhasilan proses *handshake*, pengujian konektivitas, pengujian *throughput*, serta pengamatan terhadap penggunaan sumber daya sistem.

Pada pengujian koneksi menggunakan perintah wg show, kedua server berhasil melakukan proses *handshake* dan mendeteksi *peer* masing-masing. Keberhasilan proses tersebut menunjukkan bahwa mekanisme pertukaran kunci menggunakan algoritma Curve25519 berjalan dengan baik. Curve25519 merupakan algoritma berbasis Elliptic Curve Cryptography (ECC) yang dirancang untuk memberikan keamanan tinggi dengan kompleksitas komputasi yang rendah. Penggunaan algoritma ini memungkinkan proses autentikasi dan pertukaran kunci dilakukan secara efisien tanpa memberikan beban yang besar pada sistem [5], [9].

Hasil pengujian konektivitas menggunakan perintah ping menunjukkan bahwa komunikasi antara Server A dan Server B berjalan dengan baik dengan packet loss sebesar 0%. Nilai *round trip time* (RTT) rata-rata yang diperoleh sebesar 2,15 ms menunjukkan bahwa WireGuard mampu memberikan latensi yang rendah. Nilai delay yang kecil mengindikasikan bahwa proses enkripsi dan dekripsi yang dilakukan oleh WireGuard tidak memberikan tambahan waktu transmisi yang signifikan. Temuan ini sejalan dengan penelitian Anyam et al. [1] yang menyatakan bahwa WireGuard memiliki latensi yang lebih rendah dibandingkan OpenVPN.

Pada pengujian *throughput* menggunakan aplikasi iPerf3, diperoleh kecepatan transfer data sebesar 41,1 Mbps. Nilai tersebut menunjukkan bahwa tunnel VPN yang dibangun mampu memanfaatkan kapasitas jaringan dengan baik meskipun seluruh lalu lintas data telah dienkripsi. Selain itu, tidak ditemukan adanya *retransmission* selama proses pengujian, yang menunjukkan bahwa koneksi VPN memiliki tingkat stabilitas yang tinggi. Penelitian Kjorveziroski et al. [2] juga menunjukkan bahwa WireGuard mampu menghasilkan *throughput* yang lebih baik dibandingkan beberapa protokol VPN tradisional pada lingkungan jaringan modern.

Pengujian penggunaan sumber daya sistem menunjukkan bahwa WireGuard memiliki konsumsi CPU dan memori yang relatif rendah. Pada Server A, nilai CPU idle mencapai 94%, sedangkan pada Server B mencapai 98,7%. Kondisi tersebut menunjukkan bahwa sebagian besar sumber daya prosesor masih tersedia meskipun layanan VPN sedang aktif. Penggunaan memori yang rendah juga menunjukkan bahwa WireGuard memiliki arsitektur yang ringan (*lightweight*), sehingga cocok diterapkan pada perangkat dengan sumber daya terbatas maupun server skala menengah.

Keunggulan performa WireGuard tidak terlepas dari penggunaan algoritma kriptografi modern yang terdiri atas ChaCha20 sebagai algoritma enkripsi, Poly1305 untuk autentikasi pesan, BLAKE2s untuk fungsi *hashing*, dan Curve25519 untuk pertukaran kunci. Kombinasi algoritma tersebut memungkinkan WireGuard menghasilkan keamanan yang tinggi dengan *overhead* komputasi yang lebih rendah dibandingkan protokol VPN konvensional seperti OpenVPN dan IPSec [3], [10].

Hasil penelitian ini juga menunjukkan bahwa penerapan metode Elliptic Curve Cryptography (ECC) memberikan kontribusi yang signifikan terhadap efisiensi sistem. ECC menawarkan tingkat keamanan yang setara dengan algoritma kriptografi asimetris lainnya tetapi menggunakan ukuran kunci yang lebih kecil, sehingga proses komputasi menjadi lebih cepat dan penggunaan sumber daya dapat diminimalkan [9], [14].

DOI: https://doi.org/10.31004/riggs.v5i2.11610

Secara keseluruhan, implementasi VPN *site-to-site* menggunakan WireGuard pada server Debian mampu memberikan keamanan komunikasi, performa jaringan yang baik, serta efisiensi penggunaan sumber daya sistem. Dengan karakteristik tersebut, WireGuard dapat menjadi solusi yang efektif untuk membangun jaringan privat antar lokasi (*site-to-site VPN*) baik pada lingkungan perusahaan, institusi pendidikan, maupun organisasi yang membutuhkan komunikasi data yang aman dan andal.

## 4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, implementasi Virtual Private Network (VPN) site-to-site menggunakan protokol WireGuard pada server Debian dengan metode Elliptic Curve Cryptography (ECC) berhasil diterapkan dan berfungsi dengan baik. Proses konfigurasi pada kedua server menunjukkan bahwa tunnel VPN dapat dibangun dengan sukses melalui mekanisme handshake yang memanfaatkan algoritma Curve25519 sebagai metode pertukaran kunci. Hasil pengujian konektivitas menunjukkan bahwa komunikasi antara Server A dan Server B dapat berjalan dengan baik dengan packet loss sebesar 0% dan rata-rata delay sebesar 2,15 ms. Kondisi tersebut menunjukkan bahwa WireGuard mampu menyediakan koneksi yang stabil dengan latensi yang rendah. Pengujian throughput menggunakan aplikasi iPerf3 menghasilkan kecepatan transfer data sebesar 41,1 Mbps tanpa terjadinya retransmission, sehingga menunjukkan bahwa WireGuard mampu mempertahankan kualitas transmisi data meskipun seluruh lalu lintas jaringan telah melalui proses enkripsi. Selain itu, pengujian penggunaan sumber daya sistem menunjukkan bahwa WireGuard memiliki konsumsi CPU dan memori yang relatif rendah. Nilai CPU idle sebesar 94% pada Server A dan 98,7% pada Server B menunjukkan bahwa implementasi VPN tidak memberikan beban yang signifikan terhadap sistem. Penggunaan metode Elliptic Curve Cryptography (ECC) melalui algoritma Curve25519 turut berkontribusi terhadap efisiensi komputasi karena mampu memberikan tingkat keamanan yang tinggi dengan ukuran kunci yang lebih kecil dan proses perhitungan yang lebih cepat. Berdasarkan hasil tersebut, dapat disimpulkan bahwa WireGuard dengan metode Elliptic Curve Cryptography merupakan solusi VPN site-to-site yang aman, ringan, dan efisien untuk diterapkan pada server Debian. Protokol ini mampu memberikan performa jaringan yang baik, penggunaan sumber daya yang rendah, serta keamanan komunikasi yang tinggi sehingga layak digunakan pada lingkungan jaringan perusahaan maupun institusi yang membutuhkan koneksi antarjaringan yang aman dan andal.

## Referensi

[1] Streun, F., Wanner, J., & Perrig, A. (2022). Evaluating susceptibility of VPN implementations to DoS attacks using adversarial testing. In *Network and Distributed Systems Security Symposium 2022 (NDSS'22)*. Internet Society.

[2] Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025). Empirical performance analysis of WireGuard vs. OpenVPN in cloud and virtualised environments under simulated network conditions. *Computers*, *14*(8), 326.

[3] V. Kjorveziroski, A. Gusev, and S. Ristov, "Full-Mesh VPN Performance Evaluation for a Secure Edge–Cloud Continuum," *Software: Practice and Experience*, 2024. DOI: 10.1002/spe.3329

[4] G. T. Jucha and A. Yeboah-Ofori, "Evaluation of Security and Performance Impact of Cryptographic and Hashing Algorithms in Site-to-Site Virtual Private Networks," *IEEE ICECER*, 2024. DOI: 10.1109/ICECER62944.2024.10920332

[5] Banerjee, A., & Banerjee, U. (2024, September). A High-Performance Curve25519 and Curve448 Unified Elliptic Curve Cryptography Accelerator. In *2024 IEEE High Performance Extreme Computing Conference (HPEC)* (pp. 1-7). IEEE. [6] H. Djuitcheu et al., "Lightweight Security for Private Networks: Real-World Evaluation of WireGuard," 2025.

[7] Jumakhan, H., & Mirzaeinia, A. (2024). Wireguard: An Efficient Solution for Securing IoT Device Connectivity. *arXiv preprint arXiv:2402.02093*.

[8] Wøien, M. C., Catak, F. O., Kuzlu, M., & Cali, U. (2024, December). Neural Networks Meet Elliptic Curve Cryptography: A Novel Approach to Secure Communication. In *2024 IEEE Virtual Conference on Communications (VCC)* (pp. 1-6). IEEE.

[9] T. Demirdelen and S. Kırmızı, "Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations," 2025. DOI: 10.47495/okufbed.1660352

[10] Mallick, T., Kundu, A., & Kompella, R. (2026). Study of Post Quantum status of Widely Used Protocols. *arXiv preprint arXiv:2603.28728*. [11] D. J. Bernstein, "Curve25519 and X25519 Standards," RFC 7748.

[11] A. Banerjee and U. Banerjee, "A High-Performance Curve25519 and Curve448 Unified ECC Accelerator," *IEEE Transactions on VLSI Systems*, 2025. DOI: 10.1109/TVLSI.2025.3535157

[12] M. Wøien, A. Solberg, and T. Snekkenes, "Neural Networks Meet Elliptic Curve Cryptography," *Cryptography*, vol. 8, no. 2, 2024. DOI: 10.3390/cryptography8020019

[13] H. Jumakhan and A. Mirzaeinia, "WireGuard as an Efficient Security Solution for IoT Connectivity," *Sensors*, 2024. DOI: 10.3390/s24154831

[14] M. Al-Shaer and A. Aljuhani, "Performance Evaluation of VPN Technologies in Cloud Computing Environments," *Future Internet*, 2023.DOI: 10.3390/fi15030094

[15] Y. Li and H. Wang, "Elliptic Curve Cryptography for Modern Secure Communications," *IEEE Communications Surveys & Tutorials*, 2022. DOI: 10.1109/COMST.2022.3145638

[16] S. K. Singh and R. Kumar, "Comparative Analysis of Modern VPN Protocols: WireGuard, OpenVPN, and IPSec," *IEEE Access*, 2023. DOI: 10.1109/ACCESS.2023.3284412

DOI: https://doi.org/10.31004/riggs.v5i2.11610