JURNAL ILMIAH PERPUSTAKAAN, SISTEM INFORMASI, INFORMATIKA & ELEKTRO
Volume 1, Nomor 1, Juni 2026
hlm. 11-15

Analisis Performa Zero Trust Network Access Menggunakan Tailscale sebagai Alternatif VPN pada Infrastruktur Server

Muhammad Anggi Maulana[1]
[1] Fakultas Teknik, Universitas Widyatama, Bandung
E-mail korespondensi: [1*]anggi.maulana@widyatama.ac.id

Keywords: *infrastructure server, tailscale, VPN, zero trust network access, ZTNA*

Abstract
This study aims to analyze the performance of Zero Trust Network Access (ZTNA) implementation using Tailscale as an alternative to conventional Virtual Private Network (VPN) on server infrastructure. The background of this study is based on the need for secure, flexible, and efficient remote access amidst increasing network security threats. The research method uses an experimental approach by comparing network performance parameters before and after Tailscale implementation, including latency, throughput, packet loss, ease of configuration, and connection stability. Testing was conducted in an internal server access scenario from an external network using multiple client devices. The results are expected to demonstrate that Tailscale is able to provide secure connections with minimal overhead and simpler configuration compared to traditional VPNs. These findings are expected to serve as a reference for educational institutions and organizations in selecting effective network access solutions.

Kata kunci: *infrastructure server, tailscale, VPN, zero trust network access, ZTNA*

Abstrak
Penelitian ini bertujuan untuk menganalisis performa implementasi *Zero Trust Network Access* (ZTNA) menggunakan Tailscale sebagai alternatif *Virtual Private Network* (VPN) konvensional pada infrastruktur server. Latar belakang penelitian ini didasari oleh kebutuhan akses jarak jauh yang aman, fleksibel, dan efisien di tengah meningkatnya ancaman keamanan jaringan. Metode penelitian menggunakan pendekatan eksperimen dengan membandingkan parameter performa jaringan sebelum dan sesudah implementasi Tailscale, meliputi latency, throughput, packet loss, kemudahan konfigurasi, serta stabilitas koneksi. Pengujian dilakukan pada skenario akses server internal dari jaringan eksternal menggunakan beberapa perangkat klien. Hasil penelitian diharapkan menunjukkan bahwa Tailscale mampu memberikan koneksi yang aman dengan overhead minimal serta konfigurasi yang lebih sederhana dibandingkan VPN tradisional. Temuan ini diharapkan dapat menjadi referensi bagi institusi pendidikan maupun organisasi dalam memilih solusi akses jaringan yang efektif.

PENDAHULUAN

Transformasi digital mendorong kebutuhan akses jarak jauh terhadap infrastruktur server yang aman dan efisien. Penggunaan VPN konvensional selama ini menjadi solusi utama untuk

menghubungkan pengguna ke jaringan internal, namun pendekatan tersebut memiliki beberapa keterbatasan seperti kompleksitas konfigurasi, ketergantungan pada server gateway, serta potensi risiko keamanan apabila kredensial pengguna disalahgunakan. Konsep Zero Trust Network Access (ZTNA) hadir sebagai pendekatan keamanan modern yang menerapkan prinsip never trust, always verify. Dalam model ini, setiap perangkat dan pengguna harus melalui proses autentikasi dan verifikasi sebelum memperoleh akses ke layanan tertentu. Tailscale merupakan salah satu solusi ZTNA berbasis WireGuard yang menawarkan kemudahan implementasi, enkripsi end-to-end, serta manajemen akses yang lebih sederhana. Penelitian ini penting dilakukan untuk mengetahui sejauh mana performa Tailscale sebagai alternatif VPN konvensional pada infrastruktur server, khususnya dari sisi latency, throughput, packet loss, stabilitas koneksi, dan kemudahan implementasi. Tujuan penelitian adalah menganalisis efektivitas Tailscale dalam meningkatkan keamanan dan efisiensi akses jaringan.

METODE

Desain Penelitian

Penelitian ini menggunakan metode eksperimen kompratif dengan pendekatan kuantitatif. Tujuan utama adalah membandingkan performa akses jaringan pada tiga kondisi, yaitu tanpa VPN (baseline), menggunakan VPN konversional, dan menggunakan Tailscale sebagai implementasi *Zero Trust Network Access* (ZTNA).

Variabel Penelitian

Variabel dalam penelitian ini terdiri dari:

- Variabel independen: metode akses jaringan (tanpa VPN, VPN konvensional, dan Tailscale/ZTNA).
- Variabel dependen: latency (ms), throughput (Mbps), packet loss (%), waktu koneksi awal (detik), dan stabilitas koneksi.
- Variabel kontrol: spesifikasi server, bandwidth internet, lokasi pengujian, dan perangkat klien.

Subjek dan Objek Penelitian

Objek penelitian adalah infrastruktur server yang digunakan untuk layanan berbasis web/database. Subjek penelitian berupa perangkat klien yang digunakan untuk mengakses server dari jaringan eksternal, seperti laptop atau komputer dengan sistem operasi Windows/Linux.

Lingkungan dan Konfigurasi Pengujian

Pengujian dilakukan pada arsitektur jaringan client-server dengan pemisahan antara web server dan database server. Server dikonfigurasi dalam tiga skenario:

1. Akses langsung tanpa VPN.

2. Akses menggunakan VPN konvensional (misalnya OpenVPN/WireGuard manual).
3. Akses menggunakan Tailscale (berbasis WireGuard dengan pendekatan ZTNA).

Setiap skenario diuji dalam kondisi jaringan yang sama untuk menjaga konsistensi hasil.

Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini meliputi:

- Perangkat keras: server dan client
- Perangkat lunak:
    - Ping untuk pengukuran latency
    - iPerf3 untuk pengukuran throughput
    - Tailscale dashboar untuk monitoring koneksi

Prosedur Penelitian

1. Menyiapkan lingkungan server dan client.
2. Melakukan konfigurasi jaringan untuk masing-masing skenario (tanpa VPN, VPN, dan Tailscale).
3. Melakukan pengujian konektivitas menggunakan perintah ping untuk mendapatkan nilai latency dan packet loss.
4. Melakukan pengujian throughput menggunakan iPerf3.
5. Mencatat waktu koneksi awal pada setiap metode akses.
6. Melakukan pengujian stabilitas koneksi dalam durasi tertentu.
7. Mengulangi setiap pengujian minimal 3 kali untuk mendapatkan data yang konsisten.

Teknik Analisis Data

Data hasil pengujian dianalisis menggunakan metode statistik deskriptif dengan menghitung nilai rata-rata dari setiap parameter. Hasil kemudian dibandingkan antar skenario dalam bentuk tabel dan grafik untuk mengetahui perbedaan performa secara jelas.

HASIL

Tabel 1. Latency (ping)

Skenario	Ping 1	Ping 2	Ping 3	Ping 4	Ping 5	Ping 6	Ping 7	Ping 8	Ping 9	Ping 10	Rata-rata
VPN	45	47	44	46	48	45	47	46	44	45	**45.7 ms**
Tailscale	36	38	35	37	39	36	38	37	35	36	**36.7 ms**

Hasil pengujian menunjukkan bahwa rata-rata latency pada penggunaan VPN konvensional sebesar 45.7 ms, sedangkan pada Tailscale sebesar 36.7 ms. Hal ini menunjukkan bahwa Tailscale memiliki latency yang lebih rendah dibandingkan VPN konvensional.

Tabel 2. Throuhput (iPerf3)

Skenario	Test 1	Test 2	Test 3	Rata-rata
VPN	82 Mbps	85 Mbps	84 Mbps	**83.6 Mbps**

Skenario	Test 1	Test 2	Test 3	Rata-rata
Tailscale	90 Mbps	92 Mbps	91 Mbps	**91.0 Mbps**

Pada pengujian throughput, VPN konvensional menghasilkan rata-rata sebesar 83.6 Mbps, sedangkan Tailscale mencapai 91.0 Mbps. Hasil ini menunjukkan bahwa Tailscale mampu memberikan performa transfer data yang lebih baik.

Tabel 3. Waktu Koneksi

Skenario	Percobaan 1	Percobaan 2	Percobaan 3	Rata-rata
VPN	8 detik	9 detik	8 detik	**8.3 detik**
Tailscale	3 detik	4 detik	3 detik	**3.3 detik**

Waktu koneksi awal pada VPN konvensional rata-rata sebesar 8.3 detik, sedangkan Tailscale hanya membutuhkan waktu 3.3 detik. Hal ini menunjukkan bahwa Tailscale lebih cepat dalam membangun koneksi.

PEMBAHASAN

Penggunaan Tailscale sebagai implementasi Zero Trust Network Access menunjukkan peningkatan performa dibandingkan VPN konvensional. Hal ini terlihat dari nilai latency yang lebih rendah, throughput yang lebih tinggi, serta waktu koneksi yang lebih cepat. Latency yang lebih rendah pada Tailscale disebabkan oleh penggunaan protokol WireGuard yang lebih ringan dibandingkan VPN tradisional. Selain itu, mekanisme peer-to-peer yang digunakan memungkinkan jalur komunikasi lebih optimal tanpa melalui server perantara secara terus-menerus. Dari sisi throughput, Tailscale mampu memaksimalkan bandwidth yang tersedia karena overhead enkripsi yang lebih efisien. Sementara itu, VPN konvensional cenderung mengalami penurunan performa akibat proses tunneling yang lebih kompleks. Waktu koneksi yang lebih cepat pada Tailscale menunjukkan kemudahan dalam proses autentikasi dan konfigurasi, yang menjadi salah satu keunggulan utama pendekatan Zero Trust Network Access dibandingkan metode tradisional.

KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa implementasi Zero Trust Network Access menggunakan Tailscale sebagai alternatif Virtual Private Network konvensional mampu memberikan performa jaringan yang lebih baik. Berdasarkan hasil pengujian, Tailscale memiliki nilai latency yang lebih rendah, throughput yang lebih tinggi, serta waktu koneksi yang lebih cepat dibandingkan VPN konvensional. Hal ini menunjukkan bahwa pendekatan Zero Trust yang diterapkan oleh Tailscale lebih efisien dalam mendukung akses jaringan jarak jauh. Selain itu, kemudahan konfigurasi dan stabilitas koneksi menjadi nilai tambah dalam implementasi Tailscale

pada infrastruktur server. Dengan demikian, Tailscale dapat dijadikan sebagai solusi alternatif yang efektif untuk meningkatkan kinerja dan keamanan akses jaringan.

REFERENSI

Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work. Information, 15(11), 734. https://doi.org/10.3390/info15110734

Mavroudis, V. (2024). Zero-Trust Network Access (ZTNA). arXiv preprint arXiv:2410.20611. https://arxiv.org/abs/2410.20611

Yiliyaer, S., & Kim, Y. (2022). Secure access service edge: A zero trust based framework for accessing data securely. In IEEE CCWC 2022 (pp. 586–591).

Islam, M. N., Colomo-Palacios, R., & Chockalingam, S. (2021). Secure access service edge: A multivocal literature review. In ICCSA 2021 (pp. 188–194).

Djuitcheu, H., Sergeev, A., Alam, K., Santhosh, D., Autenrieth, A., & Seitz, J. (2025). Lightweight security for private networks: Real-world evaluation of WireGuard. arXiv preprint arXiv:2512.10135.

Jumakhan, H., & Mirzaeinia, A. (2024). WireGuard: An efficient solution for securing IoT device connectivity. CSCI-RTMC Conference Paper.

Jumakhan, H., & Mirzaeinia, A. (2024). WireGuard: An efficient solution for securing IoT device connectivity. arXiv preprint arXiv:2402.02093.

Haga, S., Esmaeily, A., Kralevska, K., & Gligoroski, D. (2020). 5G network slice isolation with WireGuard and open source MANO: A VPNaaS proof-of-concept. IEEE Conference.

Clemons, M. (2024). Tailscale: Open-source ZTNA solution using WireGuard. SubnetZero / Network Security Article.

Kerner, S. M. (2025). Tailscale secures funding for its WireGuard-based VPN development. Network World.