PENERAPAN DAN PROFILING FUNGSI KONTROL DAN PERFORMANCE PADA FERRUMGATE (ZTNA) DAN WIREGUARD (VPN)

1st Sulthan Jihad
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
sulthanjihad@student.telkomuniversity.ac.id

2nd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd M. T. Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

***Abstrak* — Penelitian ini membahas implementasi dan analisis fungsi kontrol keamanan serta performa dua teknologi akses jaringan, yaitu FerrumGate sebagai representasi Zero Trust Network Access (ZTNA) dan WireGuard sebagai protokol VPN. Seiring transformasi digital dan meningkatnya ancaman siber, model keamanan tradisional berbasis perimeter dianggap kurang efektif. Pendekatan ZTNA, dengan prinsip "never trust, always verify", menawarkan kontrol akses ketat tanpa memandang lokasi perangkat, sedangkan WireGuard dikenal sebagai protokol VPN yang efisien dan ringan. Studi ini mengevaluasi kedua sistem melalui simulasi serangan jaringan (Brute Force dan Port Scanning) menggunakan alat seperti Nmap dan ffuf, serta pengukuran performa jaringan. Evaluasi fungsi keamanan mencakup aspek identification, authentication, authorization, dan accounting. Hasilnya, FerrumGate lebih unggul dalam deteksi dan cakupan kontrol, mampu mendeteksi port scanning dibawah 1 menit dan brute force dalam ~1 detik, dengan coverage completeness 75%. Sebaliknya, WireGuard gagal mendeteksi port scanning dan lambat dalam merespons brute force (45 detik), dengan coverage completeness yang terbatas (25%). Dalam performa, FerrumGate mencatat kecepatan tinggi (197 Mbit/s) namun latensi lebih besar (118 ms), sedangkan WireGuard memiliki latensi rendah (6,78 ms) dengan kecepatan lebih rendah (~31,2 Mbit/s). Hasil penelitian ini memberikan dasar dalam memilih solusi keamanan yang sesuai.**

***Kata kunci— Profiling, Performance,* Kontrol, FerrumGate, WireGuard.**

I. PENDAHULUAN

Dalam era transformasi digital yang semakin pesat, keamanan jaringan menjadi salah satu elemen kritis yang harus diperhatikan oleh organisasi. Semakin banyak munculnya pekerja jarak jauh dan adopsi teknologi berbasis cloud. Hal ini mendorong peningkatan perangkat terminal dan pertukaran data, yang memberikan kemudahan tetapi juga memunculkan ancaman internal dalam jaringan. Misalnya, Tim FireEye melaporkan bahwa ancaman internal meningkat dari 6% pada 2011 menjadi 53% pada 2021, sehingga diperlukan pertahanan yang lebih kuat terhadap ancaman internal [1].

Model keamanan tradisional, yang didasarkan pada perimeter jaringan, memiliki keterbatasan dalam menghadapi ancaman modern. Dalam konteks ini, pendekatan Zero Trust Network Access (ZTNA) muncul sebagai solusi yang menitikberatkan pada prinsip "never trust, always verify". ZTNA memberikan akses berdasarkan verifikasi ketat, tanpa memandang lokasi fisik pengguna atau perangkat, sehingga menghilangkan kepercayaan default yang rentan terhadap eksploitasi. Selain itu, protokol keamanan seperti WireGuard juga mendapatkan perhatian karena efisiensinya dalam menyediakan koneksi Virtual Private Network (VPN) yang aman dan sederhana.

Penelitian ini berfokus pada implementasi dan profiling fungsi kontrol keamanan dan performance pada dua platform, yaitu FerrumGate (ZTNA) dan WireGuard. FerrumGate, sebagai solusi ZTNA, menawarkan kemampuan kontrol akses granular dan segmentasi mikro yang memastikan bahwa hanya pengguna atau perangkat yang telah diverifikasi yang dapat mengakses sumber daya tertentu. Sementara itu, WireGuard menyediakan enkripsi kuat dan performa tinggi untuk komunikasi yang aman.

Untuk mendukung penelitian ini, eksperimen dilakukan menggunakan simulasi serangan berbasis jaringan, yang mencakup teknik seperti Brute Force Attack dan Port Scanning, serta dilakukan pengukuran metrik performance. Hasil eksperimen akan digunakan untuk mengevaluasi efektivitas fungsi kontrol yang diterapkan pada kedua platform ini. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam memahami perbandingan performa kedua teknologi dalam meningkatkan keamanan jaringan modern.

II. KAJIAN TEORI

A. Zero Trust Network Access (ZTNA)
Zero Trust Network Access (ZTNA) adalah model keamanan yang meniadakan kepercayaan default, menerapkan verifikasi berkelanjutan, prinsip hak akses minimum, dan segmentasi mikro untuk memastikan setiap permintaan akses divalidasi berdasarkan identitas, konteks, dan risiko [2]

B. Virtual Private Network (VPN)
Virtual Private Network (VPN) adalah kerangka kerja yang mengamankan pertukaran data sensitif melalui jaringan publik dengan membuat terowongan terenkripsi antara pengguna jarak jauh dan jaringan pusat [3]

C. FerrumGate
FerrumGate adalah implementasi ZTNA yang menyediakan kontrol akses granular, segmentasi mikro, dukungan multi-factor authentication (MFA) dan single sign-on (SSO), integrasi IdP, serta pemantauan dan pencatatan aktivitas secara real-time pada lingkungan on-premise, hybrid, atau multi-cloud [4].

D. WireGuard
WireGuard adalah protokol VPN modern berbasis kriptografi ringan yang dirancang untuk kinerja tinggi dan keamanan, namun memerlukan solusi eksternal untuk otentikasi berbasis kata sandi dan tidak menyembunyikan lalu lintas dari DPI [5].

E. WireGuard-Easy
Antarmuka web open-source untuk mengelola konfigurasi dan klien WireGuard secara grafis, menyederhanakan pembuatan dan distribusi profil VPN [6].

F. Fungsi Kontrol (IAAA)
Empat mekanisme—Identification, Authentication, Authorization, Accounting—yang menjamin hanya entitas berwenang mengakses sumber daya, sekaligus mencatat aktivitas untuk audit dan penegakan kebijakan [7].

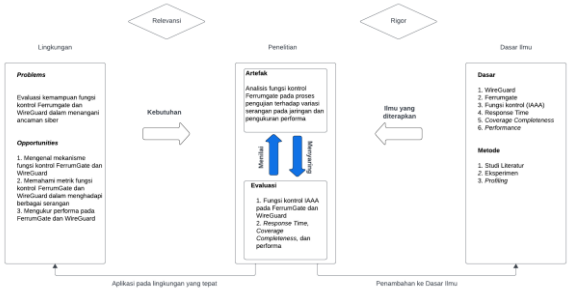
G. Port Scanning
Teknik mengirim paket ke berbagai port pada host untuk menentukan statusnya (terbuka, tertutup, difilter), dengan metode seperti SYN, UDP, dan aggressive scan untuk mengidentifikasi potensi kerentanan [8].

H. Brute Force
Strategi serangan yang mencoba semua kombinasi kata sandi atau kunci enkripsi secara sistematis hingga menemukan yang valid; efektif namun mudah terdeteksi dan membebani sistem [9].

I. Metrik Performance
Metrik performa yang diukur. Hal ini meliputi Download/Upload Speed, Latency, Jitter, Packet Loss, Network Throughput dan Data Transfer Rate untuk menilai kualitas dan efisiensi koneksi.

III. METODE

A. Model Konseptual
Definisikan singkatan dan akronim saat pertama kali digunakan dalam teks, bahkan setelah didefinisikan dalam abstrak. Jangan mengggunakan singkatan dalam judul kecuali jika tidak dapat dihindari.



Gambar 1 Model Konseptual

B. Sistematika Penyelesaian Masalah
Sistematika pemecahan masalah adalah rangkaian langkah terstruktur yang dirancang untuk menyelesaikan masalah yang telah diidentifikasi. Proses ini terdiri dari enam tahapan utama:

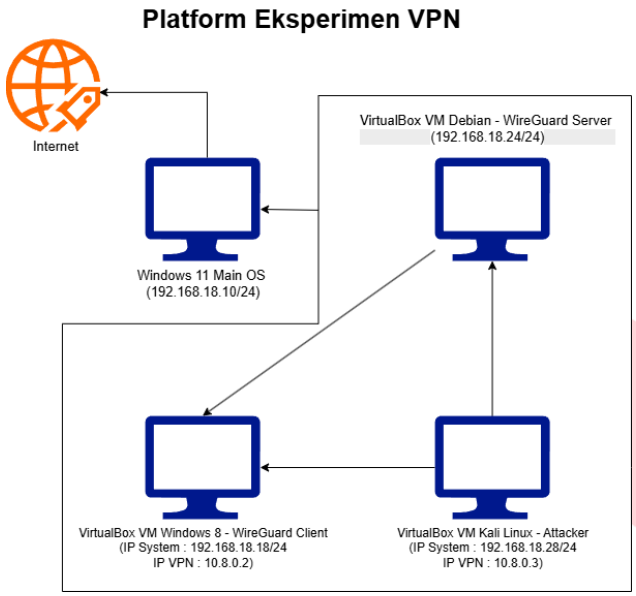
1. Tahap Awal: Identifikasi masalah penerapan fungsi kontrol dan performa pada FerrumGate (ZTNA) dan WireGuard (VPN), dilanjutkan dengan studi literatur mendalam tentang konsep fungsi kontrol keamanan dan metrik performa.
2. Tahap Hipotesis: Melakukan profiling awal fungsi kontrol pada FerrumGate dan WireGuard, lalu merumuskan hipotesis bahwa kedua platform memiliki mekanisme fungsi kontrol yang berbeda dengan tingkat efektivitas yang bervariasi, yang dapat diukur melalui pengujian.
3. Tahap Desain: Mempersiapkan lingkungan eksperimen Server, Attacker, dan Client, dan merancang skenario pengujian
4. Tahap Pengujian: Menjalankan setiap skenario pengujian (Brute Force, Port Scanning, dan Performance) pada FerrumGate dan WireGuard, sambil merekam data output, log, dan metrik performa.
5. Tahap Analisis: Data hasil eksperimen dianalisis secara mendalam untuk mengevaluasi mekanisme kontrol keamanan. Hasil analisis digunakan untuk menyusun profil FerrumGate dan WireGuard berdasarkan metrik fungsi kontrol dan performance.
6. Tahap Akhir: Dokumentasi keseluruhan proses penelitian. Penarikan kesimpulan dilakukan berdasarkan data yang diperoleh, disertai dengan rekomendasi untuk pengembangan lebih lanjut.

IV. HASIL DAN PEMBAHASAN

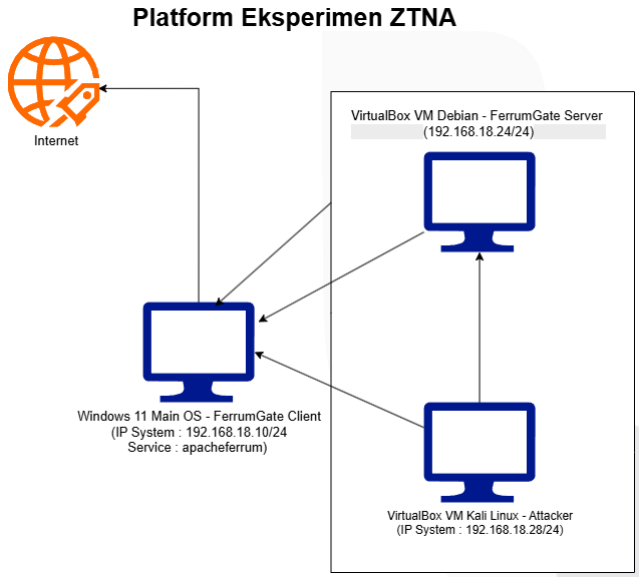
Bagian ini memaparkan hasil eksperimen, yang meliputi deskripsi platform eksperimen, skenario pengujian yang dijalankan, serta analisis terhadap fungsi kontrol dan metrik yang diukur.

1. Platform Eksperimen

Platform eksperimen dibangun di atas VirtualBox dengan tiga entitas utama server, klien, dan penyerang setiap teknologi. Untuk VPN, platform terdiri dari WireGuard Server, WireGuard Client, dan Attacker. Untuk ZTNA, platform terdiri dari



Gambar 2 Platform Eksperimen VPN



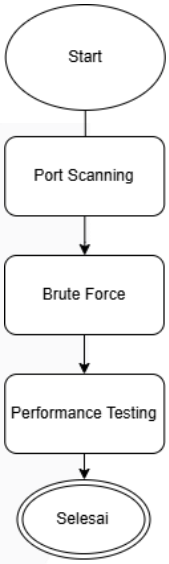
Gambar 3 Platform Eksperimen ZTNA

Spesifikasi perangkat keras platform eksperimen dibagi menjadi dua lingkungan pengujian—VPN dan ZTNA—yang masing-masing dijalankan di atas host Windows 11 Home (23H2, OS Build 22631.5335) dengan prosesor Ryzen 5 5600 (4 vCPU @ 3.5 GHz), 16 GB RAM, dan penyimpanan 2 TB. Untuk platform VPN (Gambar 2), lingkungan virtual dibangun dengan Oracle VirtualBox: OS menggunakan Debian 12.0 “Bookworm” (4 vCPU, 4 GB RAM, 50 GB disk) menjalankan WireGuard sebagai server, VM Windows 8 (2 vCPU, 4 GB RAM, 50 GB disk) berfungsi sebagai klien WireGuard, serta VM Kali Linux 2025.1a (2 vCPU, 2 GB RAM, 50 GB disk) digunakan sebagai mesin penyerang. Demikian pula, platform ZTNA (Gambar 2) terdiri dari VM Debian 12.0 “Bookworm” (4 vCPU, 4 GB RAM, 50 GB disk) yang menjalankan FerrumGate, Main OS Windows 11 (Ryzen 5 5600 8 CPU 16 Threads, 16 GB RAM, 2 TB disk) sebagai klien FerrumGate dan VM Kali Linux 2025.1a (2 vCPU, 2 GB RAM, 50 GB disk) sebagai penyerang.

Untuk mensimulasikan berbagai jenis serangan dan mengukur kinerja sistem, digunakan rangkaian alat uji sebagai berikut: Nmap (versi 7.95) untuk port scanning, ffuf (versi 2.1.0-dev) sebagai alat brute-force attack, serta Wister (versi 1.0.3) untuk pembuatan wordlist. Pengukuran performa download speed dan upload speed dilakukan menggunakan speedtest-cli (versi 1.2.0-win64), wget (versi 1.21.4) untuk file download time dan network throughput, dan iperf3 (versi 3.19) untuk pengujian data transfer rate antara klien dan server. Deteksi dan respons terhadap serangan dianalisis dengan memantau log yang dihasilkan langsung oleh WireGuard-Easy Server pada platform VPN dan FerrumGate pada platform ZTNA, kemudian dievaluasi berdasarkan metrik fungsi kontrol serta metrik performa sistem.

2. Skenario Eksperimen

Pengujian dilakukan dengan tiga jenis pengujian utama untuk mengevaluasi respons sistem VPN dan ZTNA.



Gambar 4 Skenario Eksperimen Penyerangan

Skenario pengujian yang dijalankan meliputi:

1. Pengujian dimulai dengan menggunakan Nmap sebagai alat port scanning untuk memetakan port terbuka dan layanan yang berjalan pada sistem target, sehingga permukaan serangan dapat diidentifikasi dan titik lemah potensial ditemukan.

2. Setelah melaksanakan penyerangan port scanning, menjalankan penyerangan brute force menggunakan alat seperti ffuf untuk mencoba berbagai kombinasi login dan memperoleh akses tidak sah.

3. Tahap akhir adalah melakukan pengukuran throughput dan kestabilan koneksi menggunakan speedtest, wget, dan iperf3 untuk menilai kualitas jaringan VPN dan ZTNA terhadap kecepatan dan kualitas transfer data.

3. Analisis Fungsi Kontrol

Analisis fungsi kontrol keamanan pada kedua platform dilakukan berdasarkan empat pilar IAAA (Identification, Authentication, Authorization, dan Accounting) untuk mengevaluasi bagaimana WireGuard (VPN) dan FerrumGate (ZTNA) mendeteksi serta merespons serangan port scanning dan brute force. Hasil analisis mencerminkan perbedaan mendasar dalam kemampuan logging dan kontrol akses antara arsitektur VPN tradisional dan model ZTNA modern.

A. WireGuard

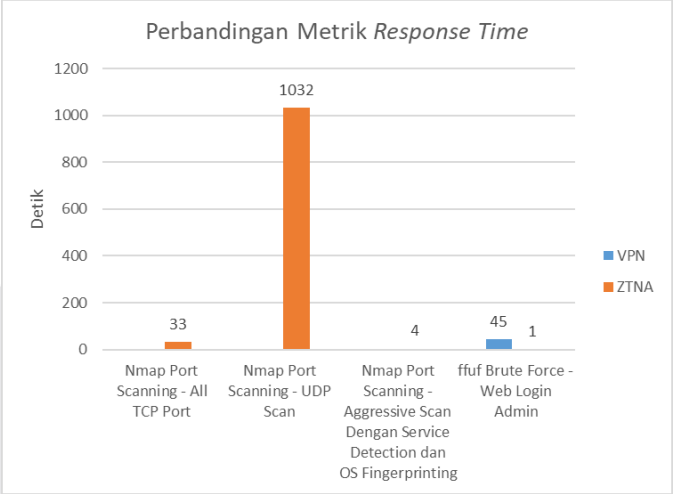
1. **Identification**
   WireGuard tidak mencatat detail serangan port scanning (TCP/UDP maupun agresif dengan Nmap). Log hanya menunjukkan metadata administratif seperti "New Session" tanpa menyertakan informasi IP penyerang, port yang dipindai, atau User-Agent alat serangan. Dengan demikian, aspek Identification sama sekali tidak terpenuhi untuk skenario port scanning.
2. **Authentication**
   Pada serangan brute force menggunakan ffuf terhadap antarmuka web, WireGuard hanya mencatat upaya koneksi baru, tetapi tidak menampilkan status autentikasi (gagal/sukses) maupun kredensial yang dicoba. Tidak ada mekanisme lockout atau throttling yang terekam di log, sehingga aspek Authentication tidak terekam secara eksplisit.
3. **Authorization**
   Karena tidak ada detail autentikasi, tidak ada pula entri otorisasi spesifik. Setelah sesi baru dibuka, log tidak mencatat apakah akses ke layanan atau resource tertentu diizinkan atau ditolak. Kontrol akses dinamis atau berbasis peran tidak diterapkan, sehingga Authorization juga tidak terlihat dalam log.
4. **Accounting**
   Satu-satunya pilar yang muncul adalah Accounting, yaitu pencatatan timestamp dan event "New Session" dengan kode sesi unik. Meski memadai untuk mengetahui jumlah koneksi, log ini tidak memberikan konteks siapa pengguna, asal koneksi, atau aktivitas apa yang dilakukan dalam sesi tersebut.

B. FerrumGate

1. **Identification**
   FerrumGate mencatat identitas pengguna (username, userId) serta IP sumber dan tujuan pada setiap aktivitas port scanning maupun brute force. Informasi ini terekam bersamaan metadata koneksi seperti requestId dan sessionId, sehingga Pilar Identification terpenuhi dengan baik.
2. **Authentication**
   Untuk port scanning, tidak ada autentikasi ulang karena pengguna sudah dalam sesi aktif. Pada brute force ffuf, log menampilkan jenis percobaan dan hasilnya (contoh: "login try → 401 ErrUserNotFound"), menandakan sistem memproses setiap upaya login dan mencatat kegagalannya. Aspek Authentication tercermin dari entri-entri ini.
3. **Authorization**
   Semua permintaan pemindaian port diizinkan dengan kode respons "200 NoError", sehingga Authorization bersifat permisif pada skenario port scanning. Pada brute force, karena gagal login, tidak ada entri otorisasi — serangan tidak mencapai tahap akses resource. Model policy-based FerrumGate memungkinkan kontrol yang lebih granular, tetapi dalam konfigurasi ini port scan tetap dibiarkan.
4. **Accounting**
   FerrumGate merekam metadata rinci untuk setiap kejadian: requestId, sessionId, timestamp, sourcePort, networkProtocol, destinationPort, dan IP sumber. Pilar Accounting terpenuhi secara penuh, menyediakan jejak audit lengkap untuk analisis pola serangan maupun forensik.

4. Analisis Metrik Response Time

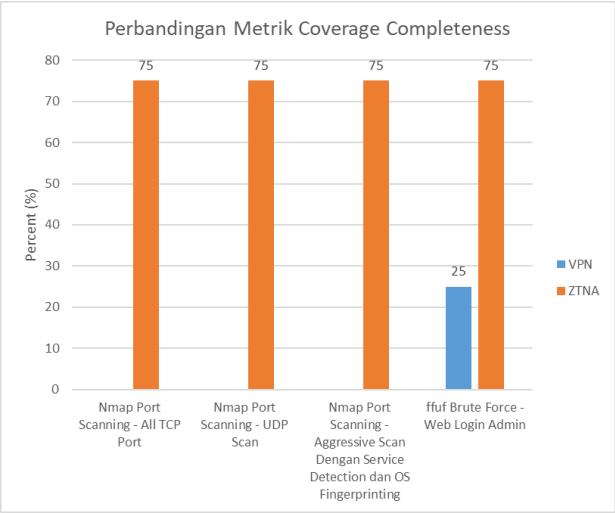
Pada metrik Response Time, WireGuard tidak mendeteksi semua bentuk port scanning sehingga tidak ada respons tercatat, dan baru mencatat brute-force ffuf setelah 45 detik. Sebaliknya, FerrumGate mendeteksi All TCP Ports dalam 33 detik, Aggressive Scan dalam 4 detik, dan brute-force ffuf dalam 1 detik—meski untuk UDP Scan responsnya relatif lama, yaitu 1 032 detik (17 menit 12 detik).



Gambar 5 Perbandingan Metrik Response Time

5. Analisis Metrik Coverage Completeness

FerrumGate secara konsisten mencapai nilai coverage completeness sebesar 75% untuk semua jenis serangan yang diuji, sedangkan WireGuard mencetak 0% pada serangan pemindaian port dan 25% pada serangan brute-force.

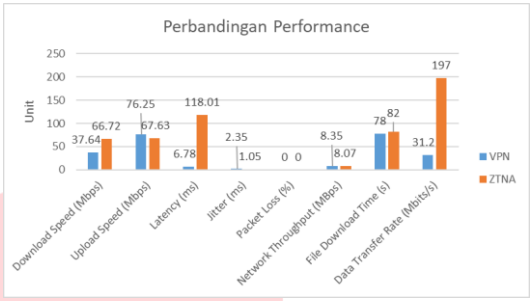


Gambar 6 Perbandingan Metrik Coverage Compleness

6. Analisis Perbandingan Performance

Jenis Performance	Throughput / Waktu
Download Speed (VPN)	37,64 Mbps
Upload Speed (VPN)	76,25 Mbps
Latency (VPN)	6,78 ms
Jitter (VPN)	2,35 ms
Packet Loss (VPN)	0,0 %
Network Throughput (VPN)	8,35 MBps
File Download Time (VPN)	78 s
Data Transfer Rate (VPN)	31,2 Mbit/s
Download Speed (ZTNA)	66,72 Mbps
Upload Speed (ZTNA)	67,63 Mbps
Latency (ZTNA)	118,01 ms
Jitter (ZTNA)	1,05 ms
Packet Loss (ZTNA)	0,0 %
Network Throughput (ZTNA)	8,07 MBps
File Download Time (ZTNA)	82 s
Data Transfer Rate (ZTNA)	197 Mbit/s

FerrumGate mencatatkan Download Speed 66,72 Mbps dibandingkan 37,64 Mbps pada WireGuard. Meskipun Upload Speed WireGuard sedikit lebih tinggi (76,25 Mbps vs 67,63 Mbps FerrumGate), FerrumGate unggul secara signifikan pada Data Transfer Rate (197 Mbit/s vs 31,2 Mbit/s). Latency WireGuard lebih rendah (6,78 ms vs 118,01 ms), sementara jitter FerrumGate lebih baik (1,05 ms vs 2,35 ms). Network Throughput (8,07 MBps vs 8,35 MBps) dan File Download Time (82 s vs 78 s) relatif setara, dan keduanya tidak mengalami packet loss.



Gambar 7 Perbandingan Performance

V. KESIMPULAN

Penelitian ini menunjukkan bahwa WireGuard dan FerrumGate memiliki kekuatan dan kelemahan yang berbeda. WireGuard unggul dalam kesederhanaan dan latency rendah, serta mampu mencatat event sesi (Accounting) untuk serangan brute force, sehingga cocok untuk organisasi yang mengutamakan respons jaringan cepat dan log teknis dasar. Namun, WireGuard tidak mendeteksi port scanning sama sekali dan hanya memiliki cakupan IAAA terbatas (25 % pada brute force).

Sebaliknya, FerrumGate menawarkan deteksi serangan yang jauh lebih komprehensif—mencakup Identification, Authentication, Authorization, dan Accounting—dengan response time di bawah satu menit untuk port scanning dan 1 detik untuk brute force (meski butuh 17 menit untuk UDP Scan). Dengan coverage completeness 75 % di seluruh kategori serangan dan data transfer rate tinggi (197 Mbit/s), FerrumGate ideal bagi organisasi yang membutuhkan visibilitas mendalam dan performa jaringan tinggi. Trade-off-nya adalah latency yang lebih tinggi (118 ms vs 6,78 ms pada WireGuard) dan konfigurasi kontrol akses yang permisif pada beberapa skenario scan.

REFERENSI

[1] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "*Theory and Application of Zero Trust Security: A Brief Survey*," Dec. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/e25121595.

[2] P. Assunção, "A Zero Trust Approach to Network Security," 2019, doi: 10.11228/dpsc.01.01.

[3] Z. Mahmood, "Virtual Private Networks: Fundamentals, security issues and solutions," Jun. 16, 2023. doi: 10.20944/preprints202306.1105.v1.

[4] FerrumGate, "FerrumGate: Open Source Zero Trust Access," FerrumGate. Accessed: Jun. 28, 2025. [Online]. Available: https://ferrumgate.com/

[5] A. Master and C. Garman, “A WireGuard Exploration,” 2023. doi: 10.5703/1288284317610.

[6] G. Nkolo, “How to Install Wg-Easy - An Opensource Web UI for WireGuard VPN.” Accessed: May 30, 2025. [Online]. Available: https://docs.vultr.com/how-to-install-wg-easy-an-opensource-web-ui-for-wireguard-vpn

[7] D. G. Rosado *et al.*, “*Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern*,” *Comput Ind*, vol. 142, Nov. 2022, doi: 10.1016/j.compind.2022.103715.

[8] M. Vivo, L. Ke, G. Isern, and G. Vivo, “*A review of port scanning techniques*,” *Computer Communication Review*, vol. 29, pp. 41–48, Apr. 1999, doi: 10.1145/505733.505737.

[9] S. Rahmah, “Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web,” *Journal of Computers and Digital Business*, vol. 2, pp. 112–119, Sep. 2023, doi: 10.56427/jcbd.v2i3.235.