IMPLEMENTASI DAN ANALISA PROFIL FUNGSI KONTROL DAN PERFORMANCE PADA OPENVPN (VPN) DAN OPENZITI (ZTNA)

1st Hafizh Al Fauzi
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
hafizhalfauzi@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 — Keamanan jaringan menjadi elemen vital dalam era digital, terutama menghadapi ancaman siber seperti pencurian data dan eksploitasi konfigurasi. Penelitian ini membandingkan dua pendekatan keamanan jaringan: OpenVPN sebagai representasi Virtual Private Network (VPN) dan OpenZiti sebagai implementasi Zero Trust Network Access (ZTNA) berbasis identitas. Fokus utama adalah bagaimana kedua sistem menerapkan fungsi kontrol IAAA (Identification, Authentication, Authorization, Accounting), merespons serangan, serta performa jaringan dalam kondisi diserang. Eksperimen dilakukan menggunakan pendekatan blackbox dengan simulasi serangan siber, seperti port scanning (Nmap), brute force login (ffuf), dan configuration manipulation (modifikasi JWT). Hasil menunjukkan bahwa OpenVPN unggul dalam log granularity dan pencatatan autentikasi, meskipun terbatas dalam otorisasi akses. Sebaliknya, OpenZiti memberikan kontrol akses yang lebih presisi dan cepat dalam mendeteksi serangan agresif, namun pencatatan log dan deteksi terhadap manipulasi JWT masih perlu ditingkatkan. Dari sisi performa jaringan, OpenZiti secara konsisten unggul dengan kecepatan unduh 6267.74 Mbps dibanding OpenVPN yang hanya mencapai 287.38 Mbps. Kesimpulannya, OpenVPN lebih sesuai untuk lingkungan yang membutuhkan akses jaringan luas dan pencatatan log teknis yang mendetail, sedangkan OpenZiti lebih tepat digunakan dalam sistem yang mengutamakan performa tinggi, kontrol akses berbasis identitas, dan segmentasi akses yang fleksibel.

Kata kunci — Keamanan Jaringan, VPN, ZTNA, OpenVPN, OpenZiti, IAAA, Profiling.

I. PENDAHULUAN

Isi Keamanan jaringan merupakan elemen krusial di era digital saat ini. Pertumbuhan teknologi informasi telah membuka potensi risiko terhadap keamanan data, seperti pencurian data, serangan brute force, dan eksploitasi konfigurasi sistem [1]. Secara tradisional, Virtual Private Network (VPN) menjadi solusi utama untuk menyediakan konektivitas terenkripsi, dengan OpenVPN sebagai salah satu implementasi open-source yang populer [2]. Namun, seiring berkembangnya kebutuhan akan manajemen akses yang lebih terkendali, konsep Zero Trust Network Access (ZTNA) muncul sebagai pendekatan baru yang mengelola akses secara ketat berdasarkan prinsip verifikasi berkelanjutan [3]. OpenZiti adalah salah satu platform ZTNA yang menerapkan pendekatan berbasis identitas untuk mengelola trafik jaringan [4].Penelitian ini bertujuan untuk melakukan analisis komparatif dan profiling terhadap fungsi kontrol dan performa dari kedua pendekatan tersebut. Dengan mensimulasikan berbagai ancaman siber seperti port scanning, brute force, dan configuration manipulation, penelitian ini akan mengevaluasi bagaimana setiap sistem menerapkan fungsi kontrol IAAA (Identification, Authentication, Authorization, Accounting) dan bagaimana profil performa keduanya dalam menghadapi serangan.

II. KAJIAN TEORI

A. Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah kerangka kerja jaringan yang berfungsi melalui jaringan publik untuk mengamankan data rahasia. VPN memanfaatkan internet terbuka untuk menciptakan media komunikasi yang sangat terlindungi antara kantor pusat dan pengguna jarak jauh [5].

B. OpenVPN

OpenVPN adalah perangkat lunak sumber terbuka yang mengimplementasikan VPN dan menyediakan fitur otentikasi serta enkripsi dalam komunikasi titik ke titik [6].

C. Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) adalah solusi keamanan yang menyediakan akses jarak jauh yang aman ke aplikasi

dan layanan berdasarkan kebijakan kontrol akses yang jelas [3]. Berbeda dengan VPN yang memberikan akses ke seluruh jaringan, ZTNA hanya memberikan akses ke layanan atau aplikasi tertentu [7].

D. OpenZiti

OpenZiti adalah proyek sumber terbuka yang menyediakan semua komponen yang diperlukan untuk membangun jaringan overlay Zero Trust dan mengintegrasikan konsepnya langsung ke dalam aplikasi [4].

E. Fungsi Kontrol (IAAA)

Fungsi kontrol IAAA adalah bagian dari Manajemen Identitas dan Akses (IAM) yang terdiri dari proses identifikasi, otentikasi, otorisasi, dan audit (accounting) untuk memastikan hanya pengguna berwenang yang mendapatkan akses [8].

F. Serangan Siber

Beberapa jenis serangan yang disimulasikan dalam penelitian ini meliputi:

1. Port Scanning: Proses memeriksa port pada alamat IP untuk mengetahui port yang terbuka atau tertutup, sering digunakan untuk persiapan serangan [9].

2. Brute Force: Teknik serangan yang mencoba semua kombinasi kunci yang mungkin untuk membobol sistem keamanan [10].

3. Configuration Manipulation: Jenis serangan yang memanipulasi file konfigurasi sistem untuk mengeksploitasi kelemahan desain yang ada [11].

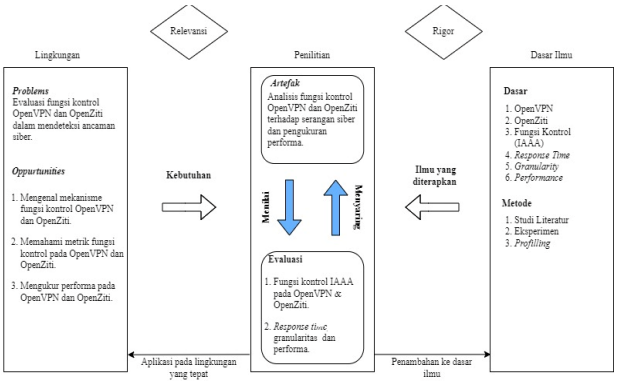
G. Metrik Performa

Metrik performa yang diukur meliputi Download/Upload Speed, Latency, Jitter, Packet Loss, dan Network Throughput untuk menilai kualitas dan efisiensi koneksi jaringan

III. METODE

A. Model Konseptual

Untuk memandu penelitian, digunakan model konseptual yang menggambarkan struktur dan hubungan antar elemen penelitian. Model ini mencakup tiga bagian utama: Lingkungan (masalah dan peluang), Penelitian (artefak dan evaluasi), dan Dasar Ilmu (teori dan metode).



Gambar 1 Model Konseptual

B. Sistematika Penyelesaian Masalah

Penelitian ini disusun melalui enam tahapan sistematis untuk memastikan pendekatan yang terstruktur dalam menyelesaikan masalah.

1. Tahap Awal: Dimulai dengan identifikasi masalah mengenai penerapan fungsi kontrol pada OpenZiti dan OpenVPN, dilanjutkan studi literatur mendalam.

2. Tahap Hipotesis: Melakukan profiling awal fungsi kontrol untuk memahami karakteristik masing-masing platform dan merumuskan hipotesis mengenai perbedaan efektivitasnya.

3. Tahap Desain: Mempersiapkan lingkungan pengujian, termasuk platform eksperimen dan pembuatan skenario serangan (Port Scanning, Brute Force, Configuration Manipulation) serta skenario pengujian performa.

4. Tahap Pengujian: Melaksanakan semua skenario pengujian yang telah dirancang, baik untuk keamanan maupun performa, dan mengumpulkan data output dari setiap platform.

5. Tahap Analisis: Melakukan analisis komprehensif terhadap data hasil pengujian untuk mengevaluasi efektivitas fungsi kontrol dan dampak performa pada kedua platform.

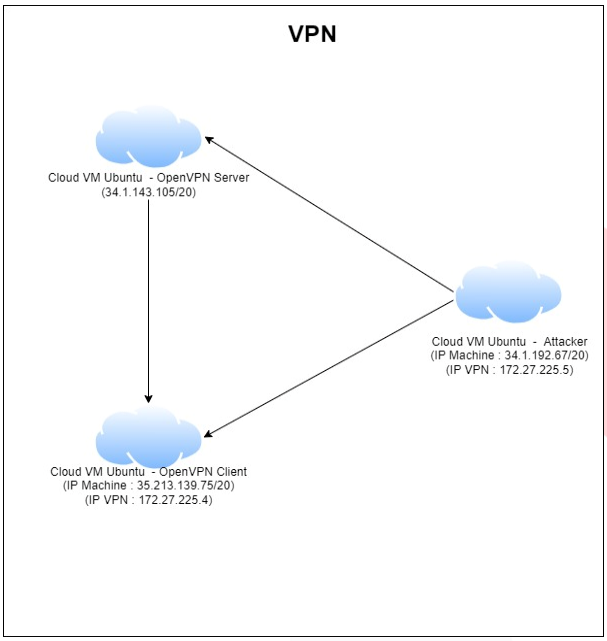
6. Tahap Akhir: Mendokumentasikan seluruh hasil penelitian, menarik kesimpulan, dan memberikan saran berdasarkan temuan yang diperoleh.

IV. HASIL DAN PEMBAHASAN

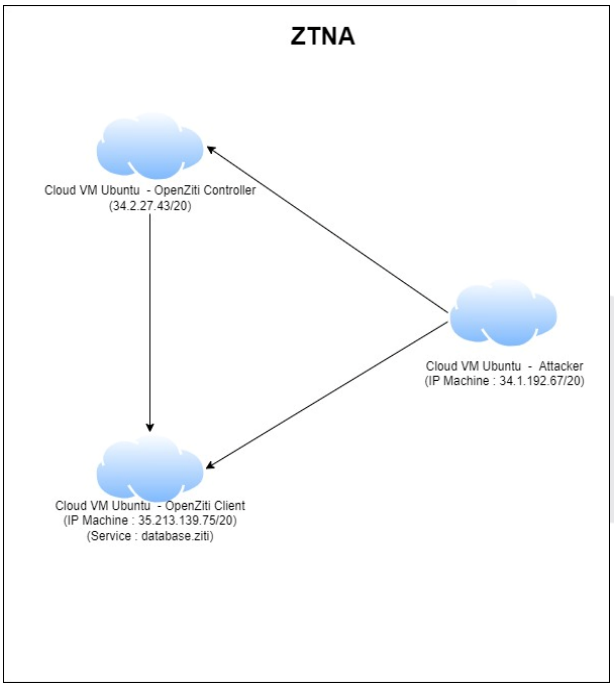
Bagian ini menjelaskan hasil eksperimen yang dilakukan, meliputi platform yang digunakan, skenario pengujian, serta analisis terhadap fungsi kontrol dan metrik yang diukur.

1. Platform Eksperimen

Platform eksperimen dibangun di lingkungan cloud menggunakan Virtual Machine (VM) Ubuntu. Untuk pengujian VPN, platform terdiri dari OpenVPN Server, OpenVPN Client, dan Attacker. Untuk ZTNA, platform terdiri dari OpenZiti Controller, OpenZiti Client (dengan tunneler), dan Attacker.



Gambar 2 Platform Eksperimen VPN

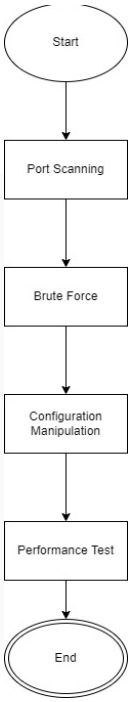


Gambar 3 Platform Eksperimen ZTNA

Platform eksperimen pada penelitian ini dikembangkan di atas infrastruktur berbasis cloud menggunakan layanan Google Cloud Platform (GCP). Seluruh entitas dalam eksperimen, yaitu server, klien, dan penyerang, diimplementasikan dalam bentuk Virtual Machine (VM) yang menjalankan sistem operasi Ubuntu 24.04.2 LTS. Setiap VM dikonfigurasi dengan spesifikasi perangkat keras seragam, terdiri dari prosesor AMD EPYC 7B12 (2 vCPU), memori sebesar 2 GB RAM, serta kapasitas penyimpanan antara 15 GB hingga 20 GB. Perangkat lunak utama yang menjadi objek pengujian mencakup OpenVPN versi 2.14.2 sebagai representasi dari Virtual Private Network (VPN) dan OpenZiti versi 1.5.4 sebagai implementasi dari Zero Trust Network Access (ZTNA). Untuk menyimulasikan berbagai jenis serangan siber, digunakan beberapa alat uji, antara lain Nmap (versi 7.94SVN) untuk port scanning, ffuf (versi 2.1.0-dev) untuk brute force attack, serta jwt_tool (versi 2.2.7) untuk manipulasi token JWT. Deteksi dan respons terhadap serangan dianalisis melalui pemantauan data log yang dihasilkan secara langsung oleh OpenVPN Access Server dan OpenZiti Controller, yang kemudian dievaluasi berdasarkan parameter fungsi kontrol dan performa sistem.

2. Skenario Eksperimen Penyerangan

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



Gambar 4 Skenario Eksperimen Penyerangan

Skenario serangan yang dijalankan meliputi:

1. Port Scanning: Menggunakan Nmap dengan berbagai metode (All TCP Ports, UDP Scan, Aggressive Scan) untuk mengidentifikasi port dan layanan yang terekspos.
2. Brute Force: Menggunakan FFUF untuk menyerang endpoint login web pada OpenVPN dan OpenZiti.
3. Configuration Manipulation: Memodifikasi file konfigurasi .ovpn pada klien VPN (misalnya, downgrade cipher suite, disable certificate verification) dan memanipulasi token JWT pada ZTNA ("none" algorithm bypass, algorithm downgrade, token lifetime extension).

3. Analisis Fungsi Kontrol

Analisis fungsi kontrol keamanan pada kedua platform dilakukan dengan menggunakan pendekatan IAAA (Identification, Authentication, Authorization, dan Accounting) untuk mengevaluasi secara sistematis bagaimana OpenVPN dan OpenZiti mendeteksi dan merespons berbagai skenario serangan. Hasil analisis menunjukkan perbedaan mendasar dalam penerapan fungsi-fungsi ini, yang mencerminkan filosofi desain yang berbeda antara arsitektur VPN dan ZTNA.

A. OpenVPN

1. Identification: OpenVPN menunjukkan kemampuan identifikasi yang sangat baik. Dalam semua skenario serangan, log server berhasil mencatat informasi krusial seperti alamat IP sumber penyerang , protokol yang digunakan (TCP/UDP) , dan port yang dituju. Lebih dari itu, pada serangan yang menggunakan alat spesifik, log mampu mengidentifikasi User-Agent dari alat tersebut, seperti "Nmap Scripting Engine" atau "Fuzz Faster U Fool", yang memberikan bukti konkret mengenai jenis aktivitas yang sedang berlangsung.
2. Authentication: Fungsi autentikasi pada OpenVPN terbukti kuat dan tangguh. Selama serangan brute force, sistem tidak hanya mencatat setiap upaya login yang gagal dengan pesan "Local auth failed", tetapi juga secara proaktif mengaktifkan mekanisme lockout untuk memblokir pengguna setelah beberapa kali percobaan gagal. Pada serangan configuration manipulation, sistem secara tegas menolak koneksi yang mencoba menonaktifkan verifikasi sertifikat server, yang ditandai dengan pesan error "certificate verify failed" dan "TLS Error: handshake failed".
3. Authorization: Aspek otorisasi pada OpenVPN bersifat terbatas. Setelah klien berhasil diautentikasi, server akan memberikan akses jaringan berdasarkan konfigurasi yang telah ditetapkan dalam PUSH_REPLY, seperti rute jaringan dan server DNS. Namun, model ini tidak menyediakan kontrol akses dinamis atau berbasis peran (role-based) ke aplikasi spesifik. Sekali berada di dalam jaringan VPN, seorang pengguna umumnya memiliki akses yang luas, yang menjadi kelemahan utama dibandingkan model ZTNA.
4. Accounting: OpenVPN unggul dalam aspek accounting berkat log granularity yang tinggi. Setiap peristiwa, mulai dari koneksi awal hingga pemutusan, dicatat dengan timestamp yang presisi, tingkat keparahan (severity), dan komponen sumber log. Sistem juga mampu mencatat anomali konfigurasi, seperti peringatan "DEPRECATED OPTION" saat klien mencoba menggunakan cipher yang usang, memberikan visibilitas yang mendalam untuk keperluan audit dan analisis forensik.

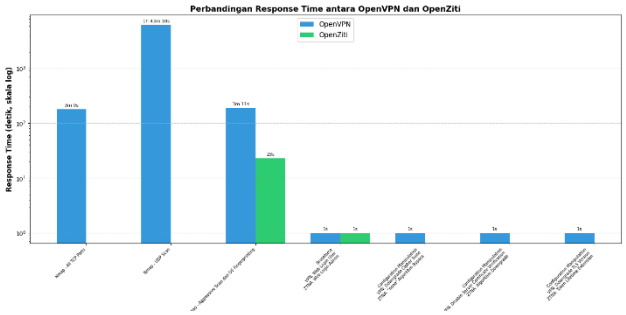
.

B. OpenZiti

1. Identification: OpenZiti mengidentifikasi setiap entitas melalui identitas digital unik yang digunakan saat proses enrollment (.jwt). Dalam log, setiap sesi koneksi dapat dilacak melalui apisessionId dan circuitId yang unik. Namun, kemampuannya untuk mengidentifikasi alat penyerang lebih terbatas; tidak ada pencatatan User-Agent seperti pada OpenVPN, sehingga identifikasi serangan lebih bergantung pada analisis pola daripada metadata eksplisit.
2. Authentication: Fungsi autentikasi sangat ketat untuk koneksi yang sah, karena setiap akses memerlukan identitas yang telah terverifikasi. Namun, pada skenario serangan manipulasi JWT, fungsi ini menunjukkan kelemahan. Ketika menerima JWT yang dimanipulasi (misalnya dengan algoritma "none" atau lifetime extension), sistem gagal memprosesnya dengan baik dan seringkali mengalami crash (Segmentation fault) daripada menghasilkan log kegagalan autentikasi yang jelas. Ini menunjukkan kurangnya exception handling yang robust untuk input yang tidak valid.
3. Authorization: Ini adalah keunggulan utama OpenZiti. Akses tidak diberikan ke seluruh jaringan, melainkan hanya ke layanan spesifik yang telah diizinkan melalui service policies. Prinsip least privilege diterapkan secara ketat, di mana identitas hanya dapat melakukan dial (mengakses) atau bind (menyediakan) layanan sesuai dengan peran yang telah ditetapkan. Hal ini secara efektif mencegah pergerakan lateral oleh penyerang, bahkan jika mereka berhasil mengkompromi satu identitas.
4. Accounting: Pencatatan log pada OpenZiti terpusat pada controller, namun detailnya bervariasi. Sistem berhasil mencatat upaya brute force pada API manajemen dengan pesan "could not authenticate". Namun, pada serangan port scanning berbasis UDP, tidak ada log yang dihasilkan sama sekali, dan pada serangan manipulasi JWT, log yang ada bersifat generik (seperti handshake failure) dan tidak secara spesifik menunjukkan adanya upaya manipulasi token. Keterbatasan ini mengurangi visibilitas untuk analisis insiden pada jenis serangan tersebut.

4. Analisis Metrik Response Time

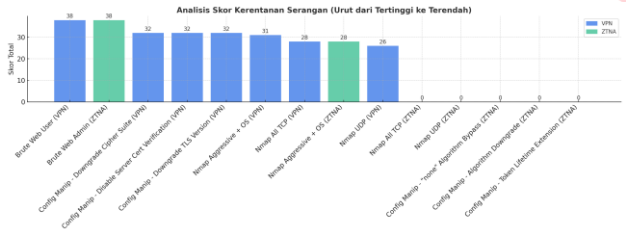
Waktu respons (deteksi) bervariasi tergantung jenis serangan. OpenVPN lambat mendeteksi UDP Scan (>1 jam) tetapi cepat untuk Brute Force (1 detik). OpenZiti lebih cepat mendeteksi Aggressive Scan (23 detik) dibandingkan OpenVPN (3 menit 11 detik). Namun, beberapa serangan manipulasi JWT pada OpenZiti tidak terdeteksi sama sekali.



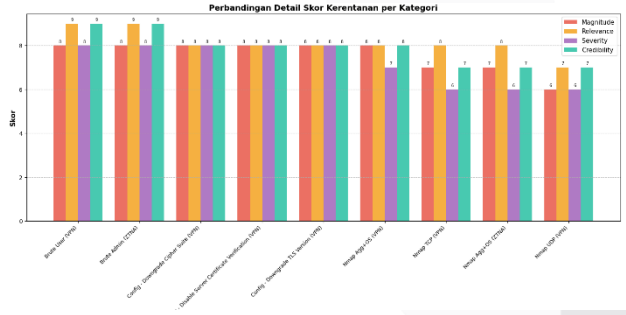
Gambar 5 Perbandingan Response Time antara OpenVPN dan OpenZiti

5. Analisis Metrik Granularity

Metrik Granularity, yang diukur melalui skor kerentanan, menunjukkan bahwa log OpenVPN secara umum lebih detail dan terstruktur. OpenVPN secara konsisten mendapatkan skor tinggi pada dimensi Credibility dan Severity. Sebaliknya, skor ZTNA lebih rendah pada serangan manipulasi JWT, yang menandakan kurangnya detail log untuk investigasi.



Gambar 6 Analisis Skor Kerentanan Serangan (Urut dari Tertinggi ke Terendah)



Gambar 7 Perbandingan Detail Skor Kerentanan per Kategori

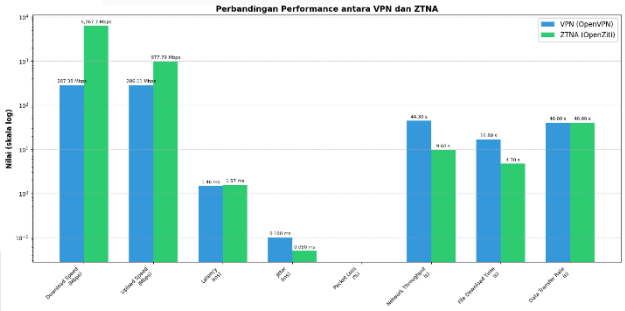
6. Analisis Perbandingan Performance

Pengujian performa menunjukkan keunggulan signifikan OpenZiti dibandingkan OpenVPN di hampir semua metrik.

Tabel 1 Analisis Perbandingan Performance OpenVPN dan OpwnZiti

Jenis Performance	Output Speed / Time
Download Speed (VPN)	287.38 Mbps
Upload Speed (VPN)	286.11 Mbps
Latency (VPN)	1.46 ms
Jitter (VPN)	0.10 ms
Packet Loss (VPN)	0.0%
Network Throughput (VPN)	44,3s
File Download Time (VPN)	16.8s
Data Transfer Rate (VPN)	40s
Download Speed (ZTNA)	6267.74 Mbps
Upload Speed (ZTNA)	977.79 Mbps
Latency (ZTNA)	1.57 ms
Jitter (ZTNA)	0.05 ms
Packet Loss (ZTNA)	0.0%
Network Throughput (ZTNA)	9,6s
File Download Time (ZTNA)	4.7s
Data Transfer Rate (ZTNA)	40s

OpenZiti mencatatkan Download Speed 6267.74 Mbps dibandingkan 287.38 Mbps pada OpenVPN. Begitu pula pada Upload Speed, Network Throughput, dan File Download Time, OpenZiti menunjukkan hasil yang jauh lebih superior. Latency dan Jitter pada kedua platform relatif setara dan sangat rendah.



Gambar 8 Perbandingan Performance antara VPN dan ZTNA

B. KESIMPULAN

Penelitian ini menunjukkan bahwa OpenVPN dan OpenZiti memiliki kekuatan dan kelemahan yang berbeda. OpenVPN unggul dalam pencatatan log teknis yang mendalam (granularity) dan deteksi serangan konvensional seperti brute force, menjadikannya pilihan solid untuk organisasi yang membutuhkan visibilitas jaringan luas. Di sisi lain, OpenZiti unggul secara signifikan dalam hal performa jaringan dan menawarkan kontrol akses berbasis identitas yang lebih granular dan fleksibel, sesuai dengan prinsip ZTNA. Namun, OpenZiti masih memiliki keterbatasan dalam mendeteksi serangan manipulasi token JWT. Pilihan antara kedua solusi ini sangat bergantung pada prioritas organisasi: apakah visibilitas log yang mendetail (OpenVPN) atau performa tinggi dan kontrol akses berbasis identitas (OpenZiti) yang menjadi fokus utama.

REFERENSI

[1] Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. Journal of Business and Entrepreneurship, 11(1), 23–33.
[2] Akinsanya, E. O., & Okeke, P. D. (2024). VIRTUAL PRIVATE NETWORKS (VPN): A CONCEPTUAL REVIEW OF SECURITY PROTOCOLS AND THEIR APPLICATION IN MODERN NETWORKS. Engineering Science & Technology Journal, 5(4), 1452–1472.
[3] Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors, 24(4).
[4] OpenZiti. (n.d.). Introduction to OpenZiti. Diakses pada 29 November 2024, dari https://openziti.io/docs/learn/introduction/
[5] Sharma, S., & Kaur, P. (2020). A Comprehensive Review on VPNs and its Security protocols. International Journal of Computer Applications, 175(11), 25-29.
[6] Brinsley, C., & Fernando, Y. (2018). Rancang Bangun Jaringan Pribadi Menggunakan OpenVPN. SYNTAX Jurnal Informatika, 7(2).
[7] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105–116.
[8] Gemawaty, C. A., & Yuliani, Y. (2024). MANAJEMEN IDENTITAS DAN AKSES DALAM KEAMANAN SISTEM INFORMASI (PENDEKATAN LITERATURE REVIEW). Jurnal Manajemen Informatika Jayakarta, 4(4), 396–403.
[9] Pandey, N. G., & Thakur, R. S. (2015). Port Scanning and Its Detection in Physical Network. Journal of Advance Research in Computer Science & Engineering, 2(3), 12–16.
[10] Gunawan, I. A. (2016). PENGGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYA PADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS. Jurnal TIMES, V(2).
[11] Zhang, Q., Zhu, X., Zhang, M., & Morley Mao, Z. (2022). Automated Runtime Mitigation for Misconfiguration Vulnerabilities in Industrial Control Systems. ACM International Conference Proceeding Series, 333–349.
[12] Kurose, J. F., & Ross, K. W. (2017). Computer networking: a top-down approach. Pearson.
[13] Stallings, W. (2014). Data and computer communications. Pearson. [14] Peterson, L. L., & Davie, B. S. (2011). Computer Networks: A Systems Approach. Morgan Kaufmann.