Journal of System & Technology
e-ISSN: XXXX-XXXX
Vol. 1, No. 1, Juni 2025

IMPLEMENTASI ZERO TRUST ARSITEKTUR PADA JARINGAN HYBRID WORK

Rakhmadi Rahman[1]*, Muhammad Faiz Ilyaz[1], Muhammad Syawal[1]
[1]Department of Information Systems, BJ. Habibie Institute of Technology, Parepare, South Sulawesi, Indonesia
rakhmadi.rahman@ith.ac.id, muhammadfaizilyas750@gmail.com, ssaawal123@gmail.com
*Corresponding author: rakhmadi.rahman@ith.ac.id

Abstract: The increasingly common hybrid working model poses significant challenges to network security and the protection of sensitive data. Traditional perimeter-based security approaches are no longer effective because they rely on the assumption that internal devices can be trusted. This research proposes a Zero Trust Architecture (ZTA)-based solution that promotes the principle of 'never trust, always verify' to address these challenges. The ZTA system is designed and implemented in a hybrid environment using components such as WireGuard as a VPN, UFW as a firewall, and Keycloak integrated with the Flask application as an OIDC-based identity management system. Through a pre-test and post-test experimental approach with controls, the effectiveness of the system was tested before and after the implementation of ZTA. The test results showed significant improvements in terms of unauthorized access detection, network communication protection through encryption, and user authentication reliability. Thus, the implementation of ZTA is proven to be able to increase system resilience to cyber threats in a dynamic and decentralized hybrid work environment.

Keywords—Authentication, Hybrid Work, Network Security, Network Segmentation, Zero Trust Architecture

I. PENDAHULUAN

Kemajuan teknologi informasi yang cepat telah mengubah cara kerja organisasi dan institusi. Salah satu tren paling signifikan dalam beberapa tahun terakhir adalah adopsi model kerja hibrida, yang mengintegrasikan kerja di tempat dan kerja jarak jauh. Meskipun model ini memberikan fleksibilitas dan efisiensi operasional, ia juga menghadirkan tantangan baru terkait keamanan jaringan dan perlindungan data sensitif. Menurut laporan IBM Cost of a Data Breach Report 2023, rata-rata biaya pelanggaran data mencapai USD 4,45 juta, dan 82% pelanggaran melibatkan data yang disimpan di cloud atau diakses dari lokasi kerja jarak jauh. Selain itu, laporan Cybersecurity Insiders 2023 menyebutkan bahwa 70% organisasi mengalami peningkatan serangan siber sejak menerapkan model kerja hybrid, dengan 53% dari mereka melaporkan serangan phishing sebagai ancaman utama. Hal ini menunjukkan pentingnya pergeseran ke model keamanan seperti Zero Trust [1], [2].

Secara historis, keamanan jaringan bergantung pada pendekatan berbasis perimeter, yang menganggap bahwa ancaman datang dari luar jaringan dan pengguna serta perangkat di dalamnya dapat dipercaya. Namun, dalam lingkungan kerja hybrid, asumsi ini tidak lagi valid, karena akses data terjadi dari berbagai lokasi, perangkat, dan jaringan yang mungkin tidak aman. Studi dari Gartner memprediksi bahwa hingga tahun 2025, 60% organisasi akan mengalami insiden keamanan besar karena kegagalan dalam mengadopsi model keamanan yang sesuai dengan lingkungan hybrid. Oleh karena itu, dibutuhkan strategi keamanan yang lebih fleksibel yang tidak lagi bergantung pada keandalan lokasi fisik perangkat atau jaringannya.

Zero Trust Architecture (ZTA) menjadi pendekatan yang menjawab tantangan ini dengan menerapkan prinsip "Jangan Pernah Percaya, Selalu Verifikasi". Prinsip ini memastikan bahwa setiap entitas, baik internal maupun eksternal, harus melalui proses verifikasi ketat dan mendapatkan otorisasi sebelum dapat mengakses sumber daya. Implementasi ZTA umumnya melibatkan otentikasi multifaktor yang kuat, segmentasi jaringan, enkripsi menyeluruh, dan pemantauan aktivitas secara terus-menerus. Dengan pendekatan ini, organisasi dapat secara signifikan mengurangi kemungkinan akses tidak sah, penyebaran malware, dan pelanggaran data yang semakin sering terjadi dalam lingkungan kerja hybrid. Laporan dari Forrester Research menunjukkan bahwa organisasi yang menerapkan ZTA mengalami penurunan insiden keamanan sebesar 50% dalam dua tahun pertama implementasi. Beberapa studi sebelumnya juga menunjukkan efektivitas pendekatan ini dalam lingkungan hybrid [3], [4], [5].

II. TINJAUAN PUSTAKA

A. *Zero Trust Arsitektur (ZTA)*

Zero Trust Architecture (ZTA) adalah pendekatan keamanan jaringan yang menolak kepercayaan otomatis terhadap pengguna atau perangkat, baik yang berasal dari dalam maupun luar jaringan organisasi. Setiap permintaan akses harus melalui verifikasi identitas, perangkat, serta konteks secara menyeluruh. Pendekatan ini bertujuan untuk mencegah penyusupan dan kebocoran data dengan cara mengurangi hak akses yang berlebihan dan menerapkan segmentasi keta[6].

B. *Hybrid Work*

Hybrid work merupakan model kerja campuran yang menggabungkan kerja di kantor dan dari lokasi lainnya, seperti rumah. Model ini mengalami peningkatan pesat sejak pandemi COVID-19 karena memungkinkan fleksibilitas tinggi bagi pekerja. Namun, implementasinya menimbulkan tantangan baru, terutama dalam hal pengelolaan keamanan jaringan yang kini harus melindungi data dari berbagai titik akses.

C. *Tools dan Teknologi Terkait*

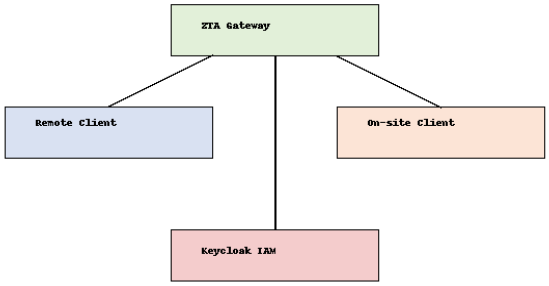
Untuk mendukung pelaksanaan Zero Trust

Architecture (ZTA) sekaligus menerapkan konsep kerja hybrid yang kini banyak digunakan oleh organisasi modern, diperlukan beragam alat dan teknologi yang terintegrasi dengan baik untuk memastikan keamanan, fleksibilitas, dan efisiensi dalam pengelolaan akses serta sumber daya IT[6].

Beberapa teknologi kunci yang sangat diperlukan antara lain adalah Identity and Access Management (IAM) yang berperan untuk mengelola dan mengatur hak akses pengguna secara ketat berdasarkan prinsip least privilege, serta Virtual Private Network (VPN) yang menyediakan koneksi aman bagi pengguna yang bekerja dari jarak jauh atau lokasi yang berlainan.

Di samping itu, dalam tahap pengembangan dan pengujian prototipe serta penerapan solusi, alat seperti bahasa pemrograman Python digunakan untuk mengotomatisasi beragam tugas dan membuat skrip keamanan, sedangkan Docker Desktop mempermudah pengelolaan kontainer agar aplikasi dapat dioperasikan secara konsisten di berbagai lingkungan.

Sama pentingnya, sistem operasi Ubuntu Server biasanya dipilih untuk menjalankan layanan server yang aman dan stabil, sementara WSL (Windows Subsystem for Linux) dengan distribusi ubuntu menawarkan lingkungan Linux yang komprehensif dan kuat di Windows, sangat bermanfaat untuk kebutuhan pengujian penetrasi dan keamanan siber. Dengan pemanfaatan alat dan teknologi tersebut, organisasi bisa menerapkan Zero Trust Architecture yang solid dan mendukung model kerja hybrid secara efektif.



Gambar 1. Diagram Blok Zero Trust Architecture dalam Lingkungan Hybrid

III. METODOLOGI

A. *Jenis dan Pendekatan Penelitian*

Penelitian ini menggunakan pendekatan eksperimental, yang bertujuan untuk menguji secara empiris efektivitas penerapan Zero Trust Architecture (ZTA) dalam meningkatkan keamanan sistem jaringan pada model kerja hybrid. Metode eksperimental memungkinkan peneliti untuk memanipulasi variabel bebas secara terkontrol dan mengamati pengaruhnya terhadap variabel terikat. Pendekatan ini dianggap tepat karena mendukung penilaian berbasis bukti terhadap sistem keamanan TI yang kompleks. Dalam konteks penelitian ini, eksperimen dilakukan dengan membandingkan kondisi sistem sebelum dan sesudah penerapan ZTA terhadap jenis-jenis ancaman siber seperti akses tidak sah (unauthorized access), sniffing, serta serangan man-in-the-middle.

B. *Desain Eksperimen*

Penelitian ini berfokus pada implementasi Zero Trust Architecture (ZTA) pada lingkungan jaringan kerja hybrid berbasis sistem operasi Ubuntu Server 22.04. Sistem dibangun menggunakan WSL (Windows Subsystem for Linux) dengan Ubuntu sebagai server utama dan dua mesin client sebagai simulasi pengguna hybrid (on-site dan remote).

Beberapa komponen utama yang digunakan dalam arsitektur sistem ini meliputi:

1) UFW (Uncomplicated Firewall) digunakan untuk menerapkan kontrol akses berbasis IP dan port, memastikan hanya lalu lintas yang sah yang diizinkan mengakses server.
2) WireGuard digunakan sebagai solusi VPN ringan dan aman untuk mengamankan koneksi dari klien ke server, khususnya bagi pengguna yang bekerja secara remote.
3) Keycloak diimplementasikan sebagai Identity & Access Management (IAM) server, menyediakan autentikasi berbasis token (JWT), integrasi SSO, serta otorisasi berbasis peran (RBAC).

Dengan pendekatan langsung implementatif ini, penelitian lebih difokuskan pada penyusunan konfigurasi dan integrasi antar komponen sistem untuk menciptakan infrastruktur Zero Trust yang dapat direplikasi oleh organisasi kecil hingga menengah.

C. *Teknik Analisis Data*

Analisis sistem dilakukan secara deskriptif dengan meninjau kinerja keamanan jaringan pasca implementasi arsitektur Zero Trust menggunakan berbagai alat pemantauan. Fokus utama analisis adalah bagaimana sistem merespons dan mencatat aktivitas jaringan secara real time setelah penerapan firewall, VPN, serta manajemen identitas dan akses. Data dikumpulkan melalui Log sistem Ubuntu yang merekam aktivitas pengguna dan proses penting, Catatan firewall UFW untuk melihat lalu lintas yang diblokir atau diizinkan,

Selain itu, Keycloak mencatat aktivitas autentikasi dan otorisasi pengguna, memungkinkan pengelolaan akses berbasis peran (Role-Based Access Control/RBAC) yang lebih aman. Seluruh data log digunakan untuk mengevaluasi stabilitas sistem, upaya akses ilegal, serta efektivitas autentikasi dan enkripsi koneksi jaringan.

Pendekatan ini sejalan dengan praktik modern dalam penerapan dan audit Zero Trust Architecture di lingkungan hybrid [6], [7], di mana visibilitas menyeluruh, segmentasi, dan kontrol berbasis identitas menjadi fondasi utama dalam membangun sistem yang tahan terhadap industri.

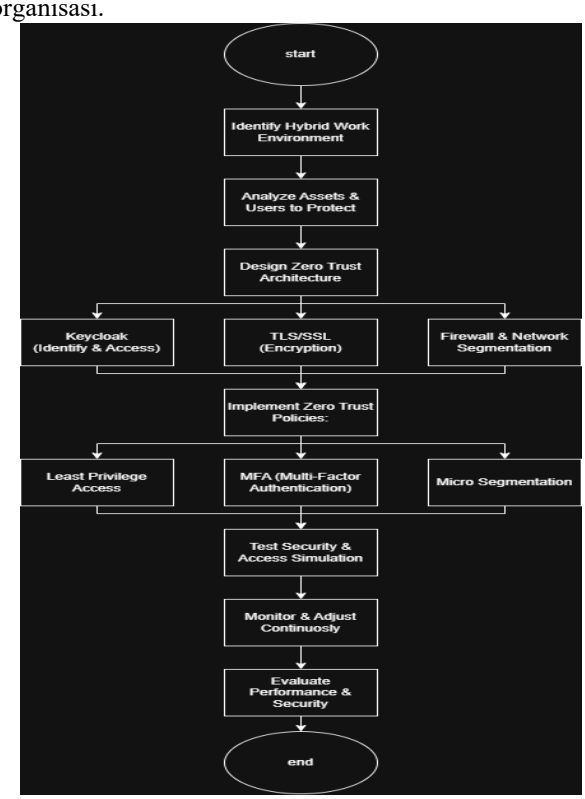
IV. GAMBARAN UMUM

Diagram alur yang ada pada gambar. 2 menunjukkan proses kerja menyeluruh dalam menerapkan arsitektur Zero Trust untuk lingkungan kerja hybrid. Proses dimulai dengan penentuan lingkungan kerja hybrid yang perlu diamankan, diikuti dengan analisis menyeluruh terhadap aset digital dan pengguna yang harus dilindungi. Langkah selanjutnya adalah merancang arsitektur Zero Trust yang mencakup beberapa elemen penting seperti Keycloak

untuk pengelolaan identitas dan akses, penerapan TLS/SSL untuk enkripsi data, serta konfigurasi firewall dan segmentasi jaringan.

Setelah merancang arsitektur, diterapkan kebijakan Zero Trust yang mencakup prinsip akses hak minimum, penggunaan autentikasi multi-faktor (MFA), dan microsegmentation untuk membatasi pergerakan lateral dalam jaringan. Tahap pengujian kemudian dilaksanakan melalui simulasi keamanan dan akses guna memastikan efektivitas sistem. Proses dilanjutkan dengan tahap pemantauan terus-menerus dan penyesuaian kebijakan sesuai kebutuhan, kemudian diakhiri dengan evaluasi menyeluruh terhadap kinerja dan tingkat keamanan yang telah dicapai.

Proses kerja ini bersifat siklus, menekankan pada prinsip kelangsungan dan peningkatan berkelanjutan yang menjadi karakteristik dari pendekatan Zero Trust, di mana sistem keamanan harus selalu dipantau dan ditingkatkan seiring dengan perkembangan ancaman dan kebutuhan organisasi.

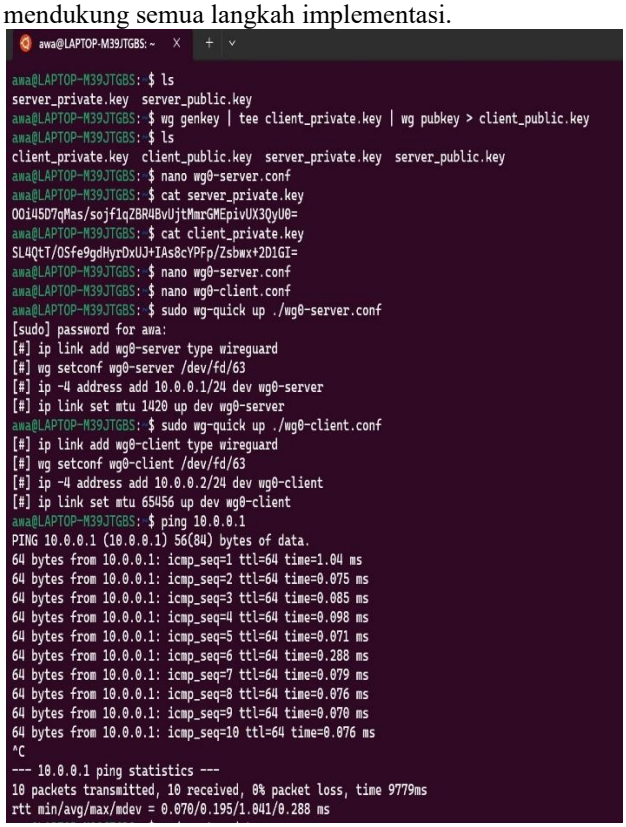


Gambar 2. Diagram alur implementasi Zero Trust dalam lingkungan hybrid

V. HASIL IMPLEMENTASI TEKNIS

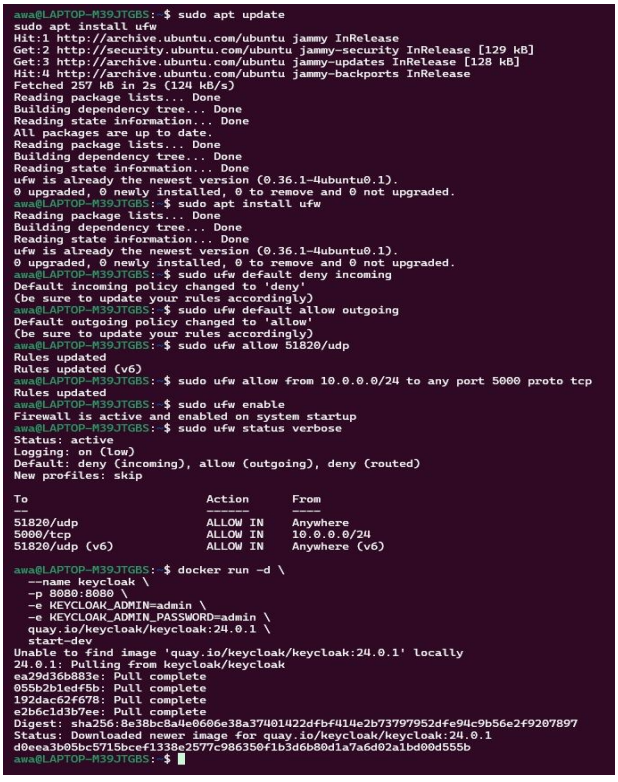
A. Lingkungan pengujian

Tampilan gambar 3 ini menggambarkan antarmuka awal dari WSL (Windows Subsystem for Linux) yang menggunakan distribusi Kali Linux. Lingkungan ini berfungsi sebagai basis utama dalam proses pengembangan dan evaluasi prototipe arsitektur Zero Trust untuk lingkungan kerja hibrida. Dengan menggunakan WSL, saya dapat menjalankan sistem operasi berbasis Linux secara langsung di Windows tanpa harus melakukan dual-boot atau menggunakan mesin virtual tambahan, sehingga pengujian dapat dilakukan dengan efisien dan terintegrasi. Ini adalah langkah awal yang krusial karena WSL berfungsi sebagai platform berbasis antarmuka baris perintah (CLI) yang handal dan fleksibel untuk mengelola berbagai perangkat keamanan siber. Oleh karena itu, dapat disimpulkan bahwa WSL ini berfungsi sebagai dasar pengujian sistem Zero Trust berbasis CLI yang mendukung semua langkah implementasi.



Gambar 3. Antarmuka awal lingkungan WSL

B. Pembaruan sistem dan Pengerasan Lingkungan



Gambar 4. Proses pembaruan sistem pada Kali Linux di WSL.

Pada gambar. 4 ini menunjukkan proses pembaruan dan peningkatan sistem di Kali Linux yang dioperasikan melalui WSL. Langkah ini diambil untuk memastikan bahwa semua paket dan dependensi sistem berada dalam versi terbaru dan stabil sebelum memulai instalasi komponen penting yang diperlukan untuk penerapan Zero Trust Architecture (ZTA), seperti Keycloak, konfigurasi TLS (Transport Layer Security), serta berbagai alat pendukung keamanan jaringan lainnya. Melakukan pembaruan sistem secara menyeluruh adalah bagian dari praktik terbaik dalam bidang keamanan siber, karena berfungsi untuk mengurangi kemungkinan kerentanan akibat versi perangkat lunak yang ketinggalan zaman. Dalam konteks proyek ini, langkah awal yang penting adalah proses pembaruan dan peningkatan sistem untuk menjamin bahwa lingkungan pengujian aman, terpercaya, dan siap untuk digunakan. Kamu dapat menyampaikan ini dalam presentasi sebagai wujud kepatuhan terhadap prinsip keamanan dasar: “Jamin sistem dalam keadaan aman dan terbaru sebelum merancang solusi keamanan jaringan yang lebih rumit.”

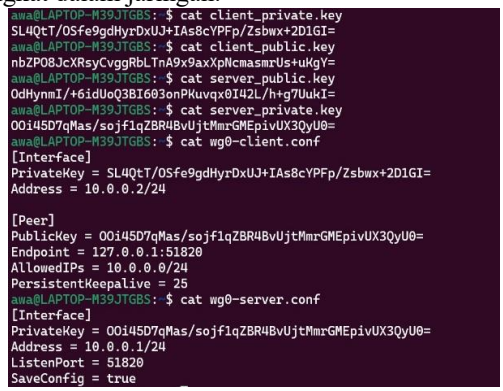
Gambar 5 ini menunjukkan tahapan instalasi OpenSSL atau pengaturan awal TLS (Transport Layer Security) di lingkungan Kali Linux. Langkah ini adalah elemen krusial dalam penerapan prinsip-prinsip Zero Trust Architecture (ZTA), terutama dalam memastikan keamanan komunikasi antara elemen-elemen sistem. TLS berfungsi untuk mengenkripsi lalu lintas data, sehingga informasi yang ditransmisikan melalui jaringan tidak dapat dijangkau atau diubah oleh pihak yang tidak berwenang, meskipun komunikasi tersebut terjadi di jaringan publik atau yang tidak kredibel. Penerapan TLS merupakan salah satu dasar teknis dari pendekatan Zero Trust, karena sistem dianggap selalu berada dalam situasi rentan terhadap serangan. Dalam presentasi, Anda bisa menegaskan bahwa penggunaan TLS bertujuan untuk memastikan setiap koneksi terenkripsi secara end-to-end, melindungi kerahasiaan, integritas, dan keaslian data, serta membangun kepercayaan antara perangkat dan layanan dalam arsitektur jaringan yang rumit.

Gambar 5. Halaman konfigurasi klien Keycloak.

C. *Implementasi Enkripsi dan Otentikasi dalam Arsitektur Zero Trust*

Gambar 6 ini menunjukkan sesi terminal di Kali Linux yang digunakan untuk menyiapkan dan mengkonfigurasi protokol VPN WireGuard. Pengaturan ini adalah elemen krusial dari implementasi Zero Trust Architecture (ZTA) karena mendukung prinsip dasar Zero Trust, yaitu mengenkripsi interaksi antar entitas dan mengonfirmasi setiap koneksi.

Implementasi Zero Trust Architecture ini memberikan kontribusi penting dalam penguatan sistem keamanan jaringan hybrid karena berhasil menyatukan autentikasi terpusat, enkripsi komunikasi, dan kontrol akses mikro. Berbeda dari pendekatan tradisional, sistem ini tidak mengandalkan perimeter statis, melainkan terus-menerus memverifikasi identitas dan perilaku pengguna serta perangkat dalam jaringan.



Gambar 6. Protokol VPN WireGuard

VI. HASIL DAN PEMBAHASAN

A. *Struktur Zero Trust Network*

Zero Trust Network mengadopsi prinsip dasar bahwa tidak ada entitas yang secara otomatis dipercaya, baik yang berasal dari dalam maupun luar jaringan. Dalam konteks sistem ini, struktur jaringan dibentuk dengan segmentasi yang jelas, memisahkan area publik, area otentikasi, serta akses internal ke layanan sensitif. Pembatasan akses ini diterapkan dengan pendekatan yang selektif dan berbasis kebijakan, sehingga pengguna hanya dapat mengakses sumber daya sesuai dengan hak akses yang telah ditetapkan. Skema ini memberikan kontrol yang lebih kuat terhadap lalu lintas data dan mengurangi risiko perpindahan lateral ketika terjadi kompromi.

Dengan struktur Zero Trust ini, setiap permintaan yang datang ke sistem akan diperlakukan sebagai tidak dipercaya hingga terbukti sebaliknya. Sistem tidak hanya memeriksa kredensial awal pengguna, tetapi juga terus memantau konteks akses, seperti lokasi, perangkat, dan perilaku. Pendekatan ini sangat relevan dalam lingkungan digital modern yang dinamis dan terdistribusi, terutama ketika aplikasi dan data tidak lagi berada di dalam satu perimeter tunggal. Hasilnya, struktur jaringan ini memperlihatkan peningkatan dalam kontrol akses dan pengamanan data. Hasil serupa juga ditemukan dalam tinjauan sistematis oleh Gambo dan Almulhem [4].

B. *Konfigurasi WireGuard VPN*

WireGuard digunakan sebagai tulang punggung dalam koneksi antar layanan dan perangkat, memberikan jalur komunikasi yang terenkripsi dan aman. Implementasi WireGuard bersifat ringan namun kuat, dirancang untuk menyederhanakan proses pengamanan jaringan tanpa mengorbankan performa. Dalam konteks sistem ini, WireGuard dikonfigurasikan antara dua entitas utama: server dan klien. Server VPN bertindak sebagai titik pusat, sementara klien terhubung melalui interface virtual yang telah dikonfigurasi dengan kunci privat dan publik. Model ini mendukung pendekatan Zero Trust dengan memastikan bahwa semua lalu lintas jaringan terenskripsi dan hanya

bisa diakses oleh pihak yang telah diotorisasi.

Konfigurasi WireGuard dalam sistem ini dilakukan dengan parameter-parameter yang disesuaikan agar koneksi tetap stabil dan terenkripsi setiap saat. Salah satu aspek penting adalah penerapan PersistentKeepalive pada klien, untuk menjaga koneksi tetap aktif bahkan di balik NAT. Kunci publik dan privat digunakan untuk autentikasi antar pihak yang terlibat. Tabel berikut merangkum konfigurasi inti WireGuard baik pada sisi klien maupun server: Evaluasi penggunaan WireGuard juga pernah dilakukan dalam studi oleh Rahman dan Harnaningrum [8], [9].

Tabel 1. Konfigurasi Inti Wireguard

Parameter	Konfigurasi Klien	Konfigurasi Server
Interface IP	10.0.0.2/24	10.0.0.1/24
Private Key	client_private.key	server_private.key
Public Key (Peer)	server_public.key	client_public.key
Endpoint	127.0.0.1:51820	-
AllowedIPs	10.0.0.0/24	10.0.0.0/24
PersistentKeepalive	25	-
SaveConfig	-	true

C. *Penempatan Keycloak sebagai Identity Provider*

Sebagai Identity Provider, Keycloak menyediakan pusat autentikasi yang memungkinkan pengelolaan pengguna, peran, dan kebijakan login secara terpusat. Ketika pengguna melakukan login, Keycloak akan memverifikasi kredensial dan mengeluarkan token yang dapat digunakan oleh layanan lain sebagai dasar untuk memberikan akses. Dengan demikian, layanan tidak perlu lagi menyimpan data pengguna secara langsung, melainkan cukup melakukan validasi terhadap token yang dikeluarkan oleh Keycloak.

Penempatan Keycloak pada sistem ini menunjukkan efisiensi dan keamanan dalam manajemen akses. Keberadaan Keycloak memungkinkan penggunaan Single Sign-On (SSO) serta penerapan autentikasi berbasis token. Seluruh sistem dapat berbagi mekanisme autentikasi yang sama, mengurangi kompleksitas dan meningkatkan konsistensi. Berikut adalah tabel yang menunjukkan hasil konfigurasi utama dari Keycloak untuk sistem ini: Pendekatan ini banyak digunakan dalam sistem Zero Trust berbasis identitas terpusat [3], [10], [11].

Tabel 2. Konfigurasi Utama dari Keycloak

Komponen	Nilai Pengaturan
Realm	ZTA-REALM
Nama Client	flask-client
Protocol	openid-connect
Root URL	http://localhost:5000
Valid Redirect URI	http://localhost:5000/login/callback
Web Origins	*
Peran (Role)	user, admin
Token Format	JWT
Login Theme	keycloak.v2

VII. KESIMPULAN

Penelitian ini memberikan kontribusi nyata dalam penerapan Zero Trust Architecture (ZTA) secara langsung di lingkungan kerja hybrid dengan pendekatan implementatif yang mudah direplikasi oleh organisasi kecil hingga menengah. Novelty dari penelitian ini terletak pada integrasi Keycloak sebagai manajemen identitas berbasis OIDC, WireGuard untuk enkripsi VPN ringan, serta UFW sebagai firewall berbasis aturan IP/port yang dikombinasikan dalam sistem kerja hybrid berbasis Linux WSL. Berdasarkan analisis dan penerapan yang disajikan dalam laporan ini, dapat disimpulkan bahwa Zero Trust Architecture (ZTA) adalah pendekatan keamanan yang sangat cocok dan efisien untuk diterapkan pada jaringan dengan model kerja hybrid. Tidak seperti model tradisional yang mengandalkan perimeter keamanan, ZTA mengutamakan prinsip "never trust, always verify", yang berarti setiap entitas, baik yang berasal dari dalam maupun luar, harus diverifikasi sebelum diizinkan mengakses sumber daya jaringan.

Dengan penerapan berbagai elemen ZTA seperti identitas dan akses yang didasarkan pada kebijakan, autentikasi multifaktor (MFA)[12], [13], enkripsi data, pemantauan lalu lintas, serta manajemen identitas terpusat seperti Keycloak, sistem menjadi lebih mampu menghadapi ancaman siber modern seperti pencurian kredensial, pergerakan lateral, dan akses yang tidak sah. Dalam konteks jaringan hibrid, yang melibatkan akses dari berbagai lokasi dan perangkat, ZTA menawarkan kontrol yang mendetail dan respons yang dapat beradaptasi terhadap risiko keamanan [14].

Untuk pengembangan selanjutnya, ZTA harus diuji pada organisasi yang memiliki infrastruktur dan kebijakan yang berbeda-beda. Integrasi IDS dan analitik AI dapat meningkatkan reaksi terhadap ancaman. Pelatihan untuk pengguna dan dokumentasi otomasi sangat penting bagi efektivitas serta pemeliharaan. Organisasi disarankan untuk menerapkan kebijakan keamanan yang ketat, termasuk prinsip keistimewaan paling sedikit, manajemen akses berbasis risiko, serta evaluasi secara berkala agar dapat beradaptasi dengan ancaman siber.

VIII. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada para pembimbing dan pengajar di Jurusan Teknik Informatika atas dukungan dan bimbingan yang diberikan selama pembuatan tesis ini. Terima kasih juga diberikan kepada semua orang yang telah memberikan ide, masukan, atau akses ke infrastruktur untuk menguji Arsitektur Zero Trust dalam lingkungan kerja hybrid. Terima kasih yang sebesar-besarnya kepada tim teknis dan rekan-rekan yang telah berpartisipasi dalam diskusi mengenai Keycloak, WireGuard, dan keamanan jaringan, yang secara signifikan meningkatkan kedalaman penelitian ini.

Dikirim 30-Mei-2025 | Revisi 01-Jun-2025 | Selesai Revisi 04-Jun-2025 | Diterima 05-Jun-2025

REFERENCES

[1] P. S. Emmanni, "Implementing a Zero Trust Architecture in Hybrid Cloud Environments," Int. J. Comput. Trends Technol., vol. 72, no. 5, pp. 33–39, 2024.

[2] V. R. K. Adapa, "Zero Trust Architecture Implementation in Critical Infrastructure: A Framework for Resilient Enterprise Security," Int. J. Adv. Res. Eng. Technol., vol. 15, no. 6, pp. 76–89, 2024.

[3] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," J. Eng. Res. Rep., vol. 26, no. 2, pp. 215–228, 2024.

[4] M. L. Gambo and A. Almulhem, "Zero Trust Architecture: A Systematic Literature Review," arXiv:2503.11659, 2025.

[5] H. Sharma, "Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security," ESP J. Eng. Technol. Adv., vol. 2, no. 2, pp. 78–91, 2022.

[6] A. A. Süzen and O. Ceylan, "The Advantages and Implementation Challenges within the Scope of the Basic Principles of Transition to Zero Trust Architecture," Int. J. 3D Print. Technol. Digit. Ind., vol. 8, no. 3, pp. 416–427, 2024.

[7] M. Nasiruzzaman, M. Ali, I. Salam, and M. H. Miraz, "The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation," arXiv:2504.11984, 2025.

[8] C. Itodo and M. Ozer, "Multivocal Literature Review on Zero-Trust Security Implementation," Comput. Secur., vol. 141, p. 103827, 2024.

[9] I. K. Rahman and L. N. Harnaningrum, "Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk mengamankan VoIP," J. RESISTOR, vol. 7, no. 1, pp. 1–10, 2023.

[10] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," Wireless Commun. Mob. Comput., vol. 2022, Art. no. 6476274, 2022.

[11] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust," Comput. Secur., vol. 110, p. 102436, 2021.

[12] L. Williams, T. M. Jones, and S. Patel, "Enhancing Network Security in Hybrid Workplaces through Zero Trust Implementation," J. Cybersecurity Res. Dev., vol. 9, no. 1, pp. 42–55, 2023.

[13] B. K. Singh and M. Gupta, "A Comparative Study of Identity Management Systems in Zero Trust Networks," Int. J. Secure Softw. Eng., vol. 14, no. 3, pp. 63–78, 2023.

[14] J. M. Keller and P. L. Dawson, "Zero Trust Network Access (ZTNA): Deployment Challenges and Strategic Benefits in Cloud-Based Enterprises," IEEE Access, vol. 11, pp. 34789–34802, 2023.