International Journal of Computer Technology and Science

E-ISSN: 3048-1961
Print ISSN: 3048-1899

(Research) Article

Implementation of Cloudflare's Zero Trust Network Access at PT FHI

Rizky Febriyan*, Boy Yuliadi

Informatics Engineering Study Program, Faculty of Engineering and Informatics, Universitas Dian Nusantara, West Tanjung Duren Street 2 No. 1, West Jakarta City, Special Capital Region of Jakarta, Indonesia, 11470.
* Corresponding Author: rizky.febriyan1902@gmail.com

Abstract: The increasing vulnerabilities of modern enterprise network security systems highlight the necessity of adopting a more comprehensive and adaptive security approach than traditional VPN infrastructures. This study explores the design and implementation of Zero Trust Network Access (ZTNA) using the Cloudflare platform at PT FHI, focusing on addressing the weaknesses caused by uncontrolled remote access and legacy security models. The research adopts an experimental methodology based on the Network Development Life Cycle (NDLC), which includes systematic phases such as needs analysis, architectural design, system implementation, testing, and performance evaluation. Data were collected through structured interviews with IT managers and security specialists, direct observation of network logs, and comprehensive testing involving three different categories of end users. The findings demonstrate significant improvements in role-based access control, granular authentication, and the elimination of unrestricted access to internal resources. Additionally, real-time monitoring and alerting features available through the Cloudflare dashboard enhance visibility and responsiveness to potential threats. The implemented system successfully applies the "never trust, always verify" principle by blocking unauthorized access attempts, enforcing continuous validation, and producing detailed audit logs. Performance evaluation results confirm stable connections, acceptable latency for critical business applications, and an overall improvement in network security posture while maintaining operational productivity across departments..

Keywords: Cloudflare; Network Access; Network Security; Role-based Access; Zero Trust.

1. Introduction

The vulnerability of security systems in the modern corporate environment has become a major concern that comes not only from external threats, but also from internal parties including the company's own employees (Deta Mediana et al., 2023). Technological developments Virtual Private Network (VPN) allows employees to access the company's internal network from a remote location as if they were in the office over a public internet connection (et al., 2024). However, conventional VPN implementations often don't come with mechanisms in place Filtering or role-based access restrictions (Role-based access control) such as Network Engineer, Developer, or Staff. This condition allows employees who work from outside the office to access the entire internal network without any restrictions or adequate supervision.

PT FHI as a leading healthcare company in Indonesia faces significant challenges in maintaining the security of customer data and internal company data. The company's commitment to maintaining customer trust and protecting digital assets drives continuous efforts to fix security gaps in network systems, especially when employees access internal networks from outside the office (Listartha & Saskara, 2024). The company strives to bring advanced security measures to ensure optimal data protection while supporting work flexibility for employees.

Received: June 02, 2025;
Revised: June 30, 2025;
Accepted: July 27,2025;
Published : July 31, 2025;
Curr. Ver.: July 31, 2025

Security concept Zero Trust emerged as a solution to overcome the security weaknesses of traditional remote access. Zero Trust Prioritizing the principle "Never Trust, Always Verify" which emphasizes the importance of identity verification and access regardless of the user's location (Marni Purnama Sari et al., 2025). This approach conducts thorough checks on each access request to minimize the risk of unauthorized access (Scott, 2023). Implementation of principles Zero Trust allows PT FHI to minimize the risk of data leakage due to improper access from internal parties who should not have obtained such access permissions.

This study aims to analyze the implementation of Zero Trust Network Access (ZTNA) at PT FHI to address remote access vulnerabilities that currently occur. The research focus includes designing a Zero Trust solution that can secure remote access from vulnerability issues as well as evaluating the effectiveness of ZTNA on enterprise systems. The scope of research is limited to the implementation of ZTNA as the main solution, with a focus on enterprise infrastructure including network devices, databases, webservers, authentication processes, and access log monitoring. The contribution of this research is expected to provide an analytical framework and formal documentation regarding the adoption of Zero Trust architecture that can serve as a conceptual foundation for PT FHI in formulating strategic and adaptive corporate cybersecurity policies. The implementation of ZTNA will practically strengthen the company's security posture, particularly in mitigating remote access risks through continuous validation of each access request to significantly minimize the attack surface.

2. Literature Review

2.1. Zero Trust Architecture Concept

Traditional security models relying on security perimeters have proven inadequate against modern cyber threats. Zero Trust Architecture (ZTA) emerged as a more effective solution. (Muchlisin & Yuliadi, 2024) defines ZTA's conceptual framework with the basic principle of "never trust, always verify", resulting in vendor-neutral architectural standards. This architecture details logical components such as Policy Engine, Policy Administrator, and Policy Enforcement Point as organizational security implementation references. Zero Trust implements continuous verification against every network entity, without providing implicit trust based on previous location or status, differing significantly from conventional security models assuming trust after initial authentication.

2.2. Zero Trust Network Access in the Enterprise Context

Research (Muhammad Altoumi Alsyaibani et al., 2021) demonstrates Enterprise network infrastructure transformation from traditional Virtual Private Network (VPN) to Zero Trust Network Access (ZTNA). VPN Security Framework implementation at Mewar University successfully developed systems with Stuart T management features and stricter access verification. Policy Control Plane application shows significant increases in access control and user activity monitoring. (End, 2020) explores Secure Socket Shell (SSH) protocol integration with Zero Trust architecture using Kerberos and OpenLDAP protocols, creating more secure centralized authentication systems.

2.3. Challenges and Applications in Modern Networks

This paper analyzes the core principles of ZTS, including micro-segmentation, least privileged access, and continuous monitoring, while critically examining four major controversies: scalability issues, economics, integration issues with existing systems, and compliance to legal requirements." (Oladimeji, 2024)

Implementation of Zero Trust in latest generation networks faces complexities. (Naurah Lisnarini & Gessan Kurnia Dewi, 2025) conduct comprehensive surveys on Zero Trust architecture application in 6G networks, identifying traditional security architecture inadequacies for future network technologies. Integration with Artificial Intelligence (AI) for threat detection and Blockchain technology for authentication demonstrates potential effective solutions, though implementation faces scalability and complexity challenges.

2.4. IT Infrastructure Security Framework

The framework uses Ethereum smart contracts to enforce Multi Factor Authentication (MFA), Role-Based Access Control (RBAC), and Just-In-Time (JIT) access privileges, effectively mitigating credential theft and insider threats (Singh, Pareek, & Sharma, 2025). IT infrastructure security requires comprehensive approaches encompassing multiple dimensions. (Sari et al., 2024) conclude that IT infrastructure security success requires holistic approaches including technical, policy, and human resource training aspects, establishing basic security principles (confidentiality, integrity, availability) as cybersecurity practitioners' knowledge foundation.

3. Proposed Method

3.1. Research Design

This study uses an experimental approach to implement and evaluate the effectiveness of Zero Trust Network Access (ZTNA) by leveraging Cloudflare services on enterprise network infrastructure. The experimental design focuses on testing network security and access modifications through ZTNA implementations compared to traditional VPN methods, providing empirical evidence of improved safety and operational effectiveness in a controlled enterprise environment.

3.2. Research Location and Time

The research was conducted at PT FHI, located at Cibis Park, Jl. TB Simatupang No.25 5th Floor, Cilandak Tim., Cilandak District, South Jakarta City, Special Capital Region of Jakarta 12560. This strategic location provides access to comprehensive enterprise network infrastructure suitable for ZTNA implementation testing.

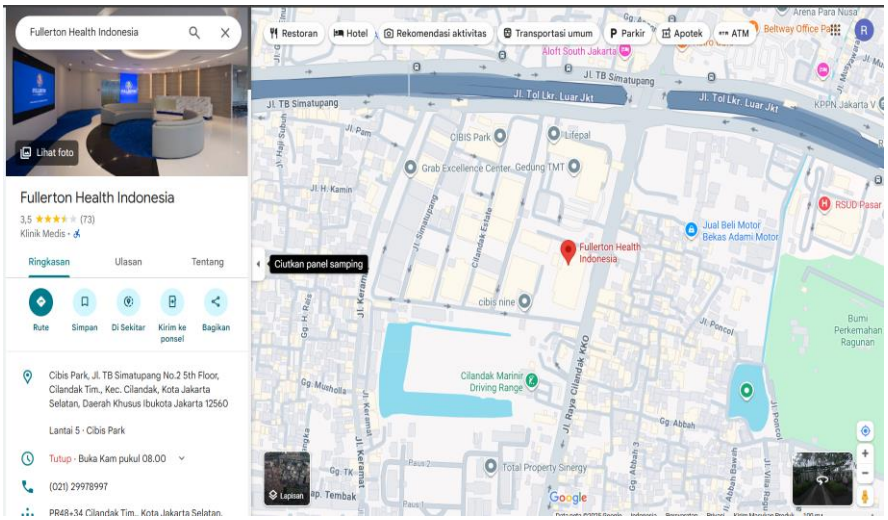

Figure 1. Research Location.

The study duration lasted two months, from September 2024 to October 2024, providing sufficient time for implementation, testing, and initial evaluation of the performance of the ZTNA system.

3.3. Data Collection Methods

Data collection uses complementary techniques to ensure comprehensive evaluation of the implementation process and results obtained.

3.4. Structured Interviews

In-depth interviews were conducted with the Head of Infrastructure at PT FHI to assess existing network security policies and challenges prior to ZTNA implementation. A structured interview with developer representatives on October 21, 2024, covered current working setups, server access methods, connectivity challenges, authentication requirements, security incidents, and perspectives on role-based access policies.

Table 1. Summary of the Interview.

No.	Stakeholders	Question Topics	Key Findings
1	Developer	Work Arrangement	Hybrid model with office visits for urgent meetings and remote development work
2	Developer	Server Access Methods	Exclusive *VPN* access using *FortiClient VPN* for internal server connectivity
3	Developer	The Challenges of Remote Work	Unstable connectivity and communication misunderstandings during *User Acceptance Testing* (*UAT*)
4	Developer	Authentication Requirements	Basic credentials: username, password, and *public* VPN IP
5	Developer	Security Incidents	Junior developer accidentally accesses the wrong server environment due to *unlimited VPN* access
6	Developer	The Importance of Role-Based Access	High priority to prevent unauthorized access and enforce user-specific restrictions

Interview results revealed that VPNs currently serve as the only remote access method, with security primarily dependent on host-level protection through antivirus software and network device firewalls.

3.5. Direct Observation

Systematic observation of network logs documented cases where employees using VPNs accessed environments outside their authorization scope. Additional data collection included security documentation review, analysis of traditional VPN configurations (IPSec), and security incident reports prior to ZTNA implementation.

3.6. Research Framework

This research utilizes the Network Development Life Cycle (NDLC) methodology for network development and design. The NDLC framework includes systematic steps: needs analysis, design, prototyping, implementation, monitoring, and management phases (Haeruddin et al., 2024).

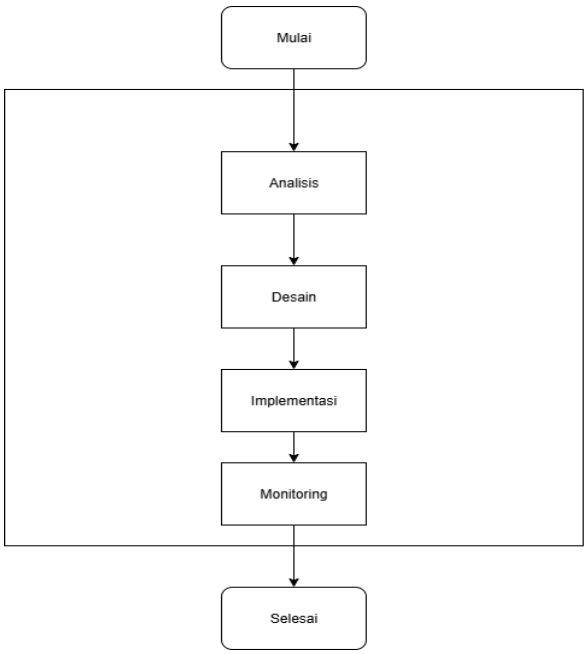

Figure 2. Research Methodology Framework

3.7. Analysis Phase

The analysis phase identifies comprehensive needs to ensure secure access to internal systems for all FHI employees, especially remote workers. This approach integrates interviews and direct observation of current access methods, complemented by infrastructure surveys. Results indicate significant vulnerability to internal attacks, as VPN users can access internal networks without strict authentication, establishing ZTNA implementation needs.

3.8. Design Phase

The design phase develops Zero Trust Network Access architecture using Cloudflare technology to address identified internal network security issues. This phase creates structured topology representation allowing precise Cloudflare ZTNA implementation, reducing risks through traffic segregation based on user roles and administrator-defined access requirements.

3.9. Implementation Phase

Implementation includes configuring Cloudflare's systems for secure user access, testing verification policies, and adjusting security settings according to FHI requirements, including initial testing to ensure optimal verification mechanism performance.

3.10. Monitoring Phase

The monitoring phase ensures security access mechanisms operate according to established company policies, including brief user education on secure access practices and identity verification importance. However, optimal monitoring implementation is constrained by research time limitations.

4. Results and Discussion

4.1. Result

4.1.1. Initial Network Infrastructure Condition Analysis

Analysis conducted at PT FHI revealed critical security vulnerabilities in existing traditional VPN infrastructure. Prior to the implementation of Zero Trust Network Access, companies used conventional VPN systems without additional authentication and authorization mechanisms once the user connected to the network. This condition is evidenced through comprehensive network monitoring and security assessments.

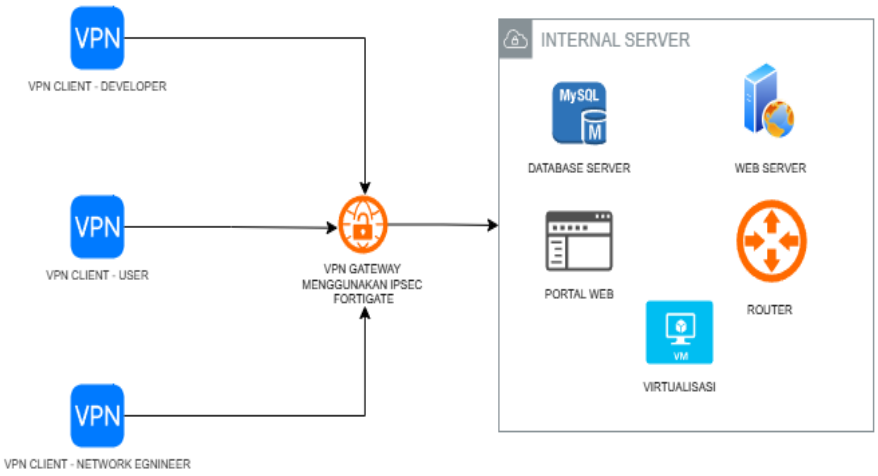

Figure 3. Ongoing business processes.

The existing network infrastructure shows significant security gaps where users with different roles can access the company's internal systems without any additional verification process, relying solely on VPN access. The investigation revealed that users who should not have access to the router and database could potentially log in, indicating the absence of a comprehensive *role-based access control* implementation at both the VPN and internal system levels.

4.1.2. *Identify Security Issues*

The analysis stage identifies security needs in PT FHI's corporate network. Some of the problems found include: network access from VPN *users* that is not well restricted, increasing the risk of cyberattacks such as *malware*, *ransomware*, and *command inject* due to the negligence of *VPN users* who are not properly monitored; lack of layered authentication on the login system that allows unauthorized users to enter the internal server network; and the absence of a system real-time monitoring of VPN user activity.

Incident ID	Date	Summary	Severity	Status	Remarks	Endpoint / Server / Unknown	IP ADDRESS
[SOC-NEOTECH]-1031	9/12/2024	WIN-EXE-PRC-PROCESS-IN-SUSPICIOUS-USERS-FOLDER-1	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	10.96.130.111
[SOC-NEOTECH]-1032	9/12/2024	WIN-EXE-PRC-PROCESS-IN-SUSPICIOUS-USERS-FOLDER-1	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	10.96.140.71
[SOC-NEOTECH]-1033	9/13/2024	WIN-PROT-WEB-MALWARE-MAL-FBJACK-1	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	10.96.80.72
[SOC-NEOTECH]-1034	9/13/2024	WIN-PROT-WEB-MALWARE-MAL-HTMLGEN-A	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	10.96.160.88
[SOC-NEOTECH]-1035	9/13/2024	WIN-PROT-WEB-MALWARE-MAL-HTMLGEN-A	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	192.168.101.70
[SOC-NEOTECH]-1036	9/13/2024	WIN-PROT-WEB-MALWARE-MAL-HTMLGEN-A	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	10.96.130.148
[SOC-NEOTECH]-1037	9/13/2024	WIN-PROT-WEB-MALWARE-MAL-ISINJECT-AB	Medium	CLOSED	blokir domain dari firewall jika di perlukan	[redacted]	10.96.222.109
[SOC-NEOTECH]-1038	9/13/2024	WIN-PROT-WEB-MALWARE-TROJ-HTMLINJ-A	Medium	CLOSED	blokir domain dari firewall jika di perlukan dan [redacted]	[redacted]	10.96.170.132

Figure 4. Incident alert reports on users.

Incident reports from *the company's firewall* show that some *hostnames* owned by *users* were detected accessing websites or applications that are indicated to be *malware* and malicious. This condition creates a security risk if *users* who are not in the company access *the malware* website and accidentally download, then *the malware* makes *lateral movements* to the internal network through a VPN without any further access control.

4.1.3. *Zero Trust Network Access Implementation*

Cloudflare's *implementation of Zero Trust Network Access* successfully addresses identified security vulnerabilities through the systematic implementation of access controls and monitoring mechanisms. The solution architecture integrates *Cloudflare Edge* as the primary gateway, replacing *the traditional* Fortigate VPN infrastructure.

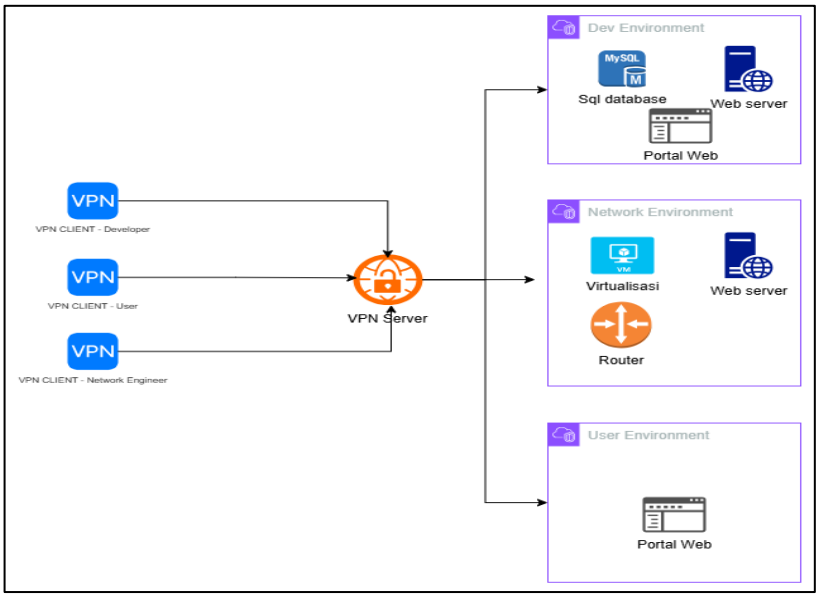

Figure 5. Network proposal business process.

4.1.4. User Role Configuration and Access Control

Implementations assign different access permissions based on user roles, as documented in the access control matrix. The following table shows the access configuration by role:

Table 3. Access Role User.

Yes	Role	Access	Yes	Not
1.	Infrastructure	Server Web	✓	
		Server Database	✓	
		Virtualization Server	✓	
		Portal Web	✓	
		Network Devices	✓	
2.	Developer	Server Web	✓	
		Server Database	✓	
		Virtualization Server		✓
		Portal Web	✓	
		Network Devices		✓
3.	E-Mail	Server Web		✓
		Server Database		✓
		Virtualization Server		✓
		Portal Web	✓	
		Network Devices		✓
4.	Network Engineer	Server Web		✓
		Server Database		✓
		Virtualization Server	✓	
		Portal Web	✓	
		Network Devices	✓	

4.1.5. System Configuration and Testing

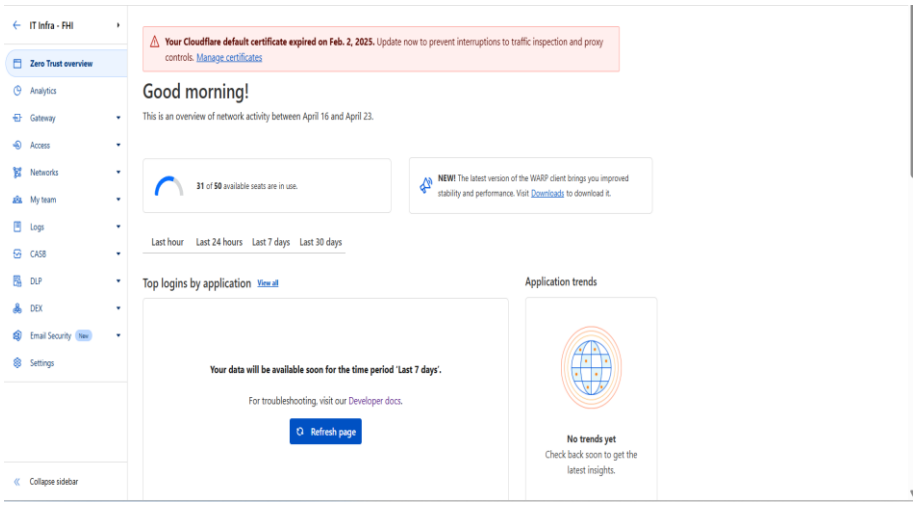

Figure 6. Cloudflare Zero Trust Network Access Dashboard.

The configuration process involves creating *a tunnel connector* that connects the company's internal network with *Cloudflare proxies*. Administrators can define access rules and policies centrally through *the Cloudflare dashboard.*

Table 4. Server, IP, and User Role.

Yes	Server Name	IP Address	Role
1	Web Portal Learning	10.96.210.150	E-Mail
2	Ubuntu Server	10.96.221.43	Developer
3	Switch Web Management	172.18.0.78	Network Engineer

4.1.6. Security Test Results

Comprehensive testing was conducted using three different user accounts representing different organizational roles. The testing protocol involves verifying authentication, monitoring access efforts, and validating policy enforcement.

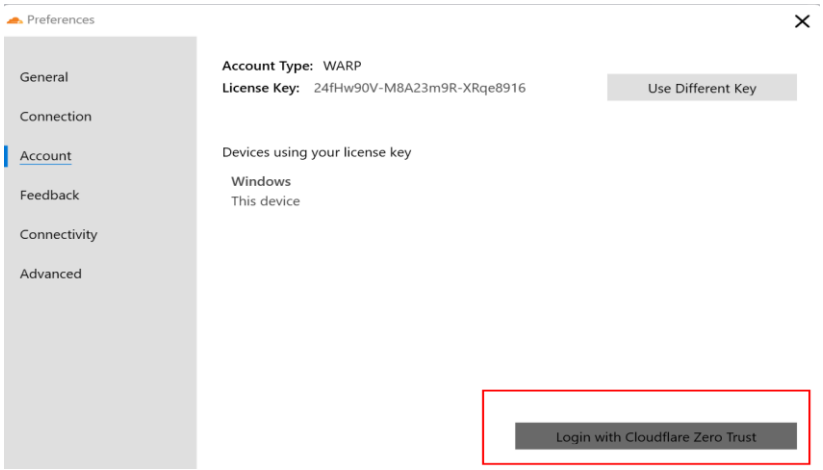

Figure 7. Zero Trust Login.

The test results show successful policy enforcement across all user categories. When a user tries to access an unauthorized resource, *the Zero Trust* system instantly blocks access and generates comprehensive audit logs.

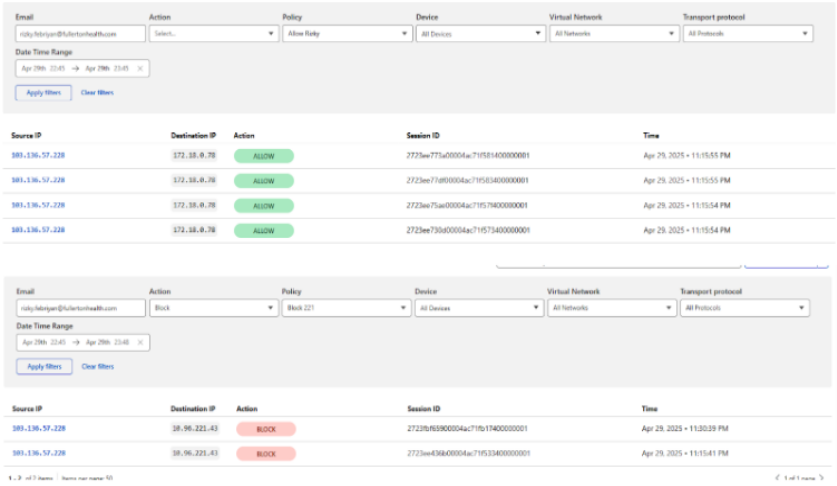

Figure 8. Log Policy Rizky

Cloudflare's dashboard provides real-time *monitoring capabilities*, allowing administrators to track access attempts, successful authentication, and policy violations.

4.1.7. System Performance Evaluation

System performance evaluation focuses on connection latency, *packet loss assessment*, and connection stability during operational periods. Cloudflare *Zero Trust implementations* demonstrate stable performance metrics with minimal impact on user productivity. Response times remain within acceptable parameters for critical business applications, and connection reliability meets organizational requirements for remote access operations.

4.2. Discussion

4.2.1. Enhanced Security and Risk Mitigation

Implementation Zero Trust Network Access at PT FHI successfully addressed fundamental security challenges in traditional VPN infrastructure. Results showed significant improvements in access control mechanisms, user authentication processes, and security monitoring capabilities. The transition from implicit trust to explicit verification protocol substantially reduces organizational exposure to cyber threats, particularly lateral movement attacks and unauthorized system access (Novianti, 2024). Implementation of comprehensive Role-based access control aligns with established security frameworks emphasizing Least privilege principles. By restricting user access to required resources based on organizational roles, this effectively minimizes attack vectors while maintaining operational efficiency. This corresponds to findings by (Suparman & Sugiyanto, 2022) regarding Zero Trust optimization in digital security environments.

4.2.2. Comparative Analysis with Traditional VPN Systems

Results clearly demonstrate Zero Trust Network Access superiority over traditional VPN implementations regarding security effectiveness and administrative controls. Traditional VPN systems provide unrestricted network access post-authentication, creating significant vulnerabilities. The Zero Trust model's continuous verification ensures dynamic access decisions based on user identity, device status, and resource sensitivity. Elimination of implicit trust relationships represents a fundamental network security philosophy shift. While traditional systems assume internal network security after perimeter defense bypass, Zero Trust implementations treat any access request as potentially dangerous, requiring explicit verification and authorization.

4.2.3. Implementation Effectiveness and Operational Impact

Successful Cloudflare Zero Trust Network Access implementation demonstrates practical viability of modern security frameworks in enterprise environments. Implementation achieves primary goals of limiting unauthorized access, implementing comprehensive monitoring capabilities, and maintaining operational continuity. Cloud-based architecture provides scalability benefits while reducing infrastructure management overhead compared to traditional on-premises security solutions. User acceptance proved successful with minimal workflow disruption. WARP client applications provide seamless connectivity while transparently implementing security policies. This balance between improved security and user experience represents critical success factors, as noted by (Azmi Fauziah Suanda & Tajul Arifin, 2024) in their Zero Trust application analysis.

4.2.4. Technical Architecture and Performance Considerations

Cloudflare Edge infrastructure exhibits robust performance characteristics suitable for enterprise-scale deployments. Tunneling technology effectively creates secure communication channels without sacrificing system responsiveness. Performance metrics remain within acceptable parameters for critical business applications. Centralized policy management through Cloudflare's dashboard significantly improves administrative efficiency. Real-time monitoring and logging enable proactive security management and rapid incident response capabilities.

4.2.5. Limitations and Future Research Opportunities

Despite achieving main objectives, limitations require consideration for future research. Reliance on Cloudflare's infrastructure introduces potential single point of failure requiring careful disaster recovery planning. Solution effectiveness depends on proper policy configuration and maintenance. Future research opportunities include investigating hybrid Zero Trust implementations combining multiple security vendors, testing artificial intelligence integration in access control decisions, and evaluating scalability in complex multi-cloud environments.

4.2.6. Managerial Implications and Strategic Considerations

Successful implementation provides critical insights for organizational security strategy development. Results show comprehensive security improvements achievable without significant business operation disruption when properly planned. Enhanced auditability and policy enforcement provide management better security posture visibility and compliance status. Implementation positions organizations well for future security challenges and regulatory requirements. Zero Trust Network Access foundations provide platforms for additional security enhancements supporting digital transformation initiatives while maintaining robust security standards (Aripradono et al., 2021).

5. Conclusions

This study successfully demonstrated the effectiveness of the implementation of Zero Trust Network Access using Cloudflare in overcoming traditional network security vulnerabilities at PT FHI. The transformation from conventional VPN systems to a Zero Trust architecture resulted in significant improvements in role-based access control, multi-layered authentication mechanisms, and comprehensive real-time monitoring capabilities. The implementation of role-based access control successfully restricts user access according to their organization's responsibilities, reducing the risk of lateral movement and unauthorized access to the company's critical systems. Performance evaluations show that Cloudflare's solutions maintain optimal system responsiveness without sacrificing operational productivity, while centralized management dashboards improve administrative efficiency in security policy enforcement. Nonetheless, the study has limitations in terms of relatively short evaluation periods and reliance on a single cloud infrastructure that has the potential to create a single point of failure. The limited research time also limits the ability to conduct long-term evaluations of system stability and in-depth analysis of operational cost impacts. Further research is recommended to explore hybrid Zero Trust implementations with multiple vendors, integration of artificial intelligence in decision engines, and evaluation of scalability in complex multi-cloud environments.

References

Altoumi Alsyaibani, O., Utami, E., & Hartanto, A. D. (2021). Survey on deep learning based intrusion detection system. Telematics, 14(2), 86–100. https://doi.org/10.35671/telematika.v14i2.1317

Aripradono, H. W., Tjahyadi, S., Yap Rui Qi, K. O., Nursudiono, N., Galang, Y. P., Hirawan, J., Te, C., Ariadi, C., & Elvin, E. (2021). Integration of Digital Ethics in Culture in Companies Doing Work-From-Home (WFH) during the Pandemic. Journal of Entrepreneurship, Management and Industry (JEMI), 4(2), 56–64. https://doi.org/10.36782/jemi.v4i2.2202

Ayu, R. S., Rivai, M. M., Mubarak, N. Al, & Pratama, D. (2025). Information Technology Infrastructure Security: Cyber Threat Analysis and Mitigation Approaches. 4(2), 195–222. https://doi.org/10.1201/9781032622408-13

Ayu, R. S., Rivai, M. M., Mubarak, N. Al, & Pratama, D. (2025). Information technology infrastructure security: Cyber threat analysis and mitigation approaches. Journal of Information Infrastructure Security, 4*(2), 195–222. https://doi.org/10.1201/9781032622408-13

Azmi Fauziah Suanda, & Tajul Arifin. (2024). The Significance of Historical Hadith in Handling Negative Content on Social Media. Equator: Journal of Educational and Social Humanities, 4(2), 288–298. https://doi.org/10.55606/khatulistiwa.v4i2.3576

Deta Mediana, S., Lindawati, & Fadhli, M. (2023). Implementation of the Zero Trust Model on SSH Security with the Kerberos and OpenLDAP Protocols. SYSTEMATICS: Journal of Information Systems, 12(3), 981–995. http://sistemasi.ftik.unisi.ac.id

Fitra, E. (2014). Violation of servitude rights (yard devotion) in Lengkong Gudang Serpong – South Tangerang as viewed from the Civil Code. Undergraduate thesis, Universitas Trisakti.

Haeruddin, H., Prasetyo, S. E., & Kaharuddin, A. W. (2024). Network Security Optimization in the Digital Era using the Zero Trust method. Journal of Information System and Technology, 5(3), 15–24. https://doi.org/10.37253/joint.v5i3.9986

Haeruddin, H., Prasetyo, S. E., & Kaharuddin, A. W. (2024). Network security optimization in the digital era using the Zero Trust method. Journal of Information System and Technology, 5(3), 15–24. https://doi.org/10.37253/joint.v5i3.9986

Listartha, I. M. E., & Saskara, G. A. J. (2024). Security testing with the PenetrationTesting Execution Standard (Ptes) method to find vulnerabilities in network devices. Electro Luceat, 10(2), 32–40. https://jurnal.poltekstpaul.ac.id/index.php/jelekn/article/view/821

Listartha, I. M. E., & Saskara, G. A. J. (2024). Security testing with the Penetration Testing Execution Standard (PTES) method to find vulnerabilities in network devices. Electro Luceat, 10(2), 32–40. https://jurnal.poltekstpaul.ac.id/index.php/jelekn/article/view/821

Marni Purnama Sari, Sukmawarti Sukmawarti, & Hidayat Hidayat. (2025). Integrating Computational Thinking (CT) in Solving AKM Numeracy Problems at SDN 2 Kutapanjang. Equator: Journal of Education and Social Humanities, 5(3), 819–832. https://doi.org/10.55606/khatulistiwa.v5i3.7246

Mihit, Y. (2023). Dynamics and Challenges in Pancasila Education in the Era of Globalization: A Literature Review. EDUCATIONIST: Journal of Educational and Cultural Studies, 2023(1), 357–366.

Muchlisin, M., & Yuliadi, B. (2024). Improving Network Performance of Headquarters and Branches Using Software-Defined Network WAN (SD-WAN). PIXEL: Embedded Systems and Logic Computer Science Research, 12(1), 23–34. https://doi.org/10.33558/piksel.v12i1.8115

Muchlisin, M., & Yuliadi, B. (2024). Improving network performance of headquarters and branches using software-defined network WAN (SD-WAN). PIXEL: Embedded Systems and Logic Computer Science Research, 12(1), 23–34. https://doi.org/10.33558/piksel.v12i1.8115

Muhammad Altoumi Alsyaibani, O., Utami, E., & Dwi Hartanto, A. (2021). Survey on Deep Learning Based Intrusion Detection System. Telematics, 14(2), 86–100. https://doi.org/10.35671/telematika.v14i2.1317

Mungkasa, O. (2020). Telecommuting: Concepts, Applications and Learning. Bappenas Working Papers, 3(1), 1–32. https://doi.org/10.47266/bwp.v3i1.52

Naurah Lisnarini, & Gessan Kurnia Dewi. (2025). Motivation and Obstacles to the Work of State Civil Apparatus in the Work From Home (WFH) System. SPEECH: Journal of Communication, Social and Humanities Sciences, 3(1), 235–250. https://doi.org/10.47861/tuturan.v3i1.1586

Novianti, L. (2024). Theoretical Analysis of Work From Home Trends in the Digital Era: Advantages and Disadvantages. ACADEMIC: Journal of Humanist Students, 4(1), 31–40. https://doi.org/10.37481/jmh.v4i1.656

Sari, J. A., Yuliani, I., Akadira, T., Sunarya, A., & Ating, R. (2024). Data Security and Individual Privacy from the Perspective of Public Administration. International Journal of Social Science, 5(3), 818–830. https://doi.org/10.61194/ijss.v5i3.1297

Suparman, R. C., & Sugiyanto, E. (2022). The Influence of Digital Culture and Work Discipline on Employee Performance in the WFH Period at the Directorate General of Civil Defense in 2020-2021. Populist : Journal of Social and Humanities, 7(2), 244–260. https://doi.org/10.47313/pjsh.v7i2.1967