**JURNAL TEKNOLOGI DAN OPEN SOURCE**
Vol. 8, No. 2, December 2025, pp. 629~638
e-ISSN: 2622-1659, accredited Four Grade by Kemenristekdikti, Decree No: 152/E/KPT/2023
DOI: https://doi.org/10.36378/jtos.v8i2.4369

# Defguard Implementation for Remote Access Management Using WireGuard VPN at PT. Esta Dana Ventura

**Ervan Jefferson Bany [1], Muhamad Hadi Arfian[2]**
[1,2]Department of Informatics Engineering, Esa Unggul University, Indonesia

**Article Info**

***Article history:***

Received 05 20, 2025
Revised 08 15, 2025
Accepted 11 28, 2025

***Keywords:***

Access Management
VPN
Defguard
Wireguard

**ABSTRACT**

This study examines the development and deployment of a remote access management system by integrating Defguard with the WireGuard VPN at PT. Esta Dana Ventura. The company previously faced unstable connections and inefficient user administration due to the limitations of its MikroTik-based PPTP and L2TP VPN solutions. To overcome these challenges, a new architecture was designed using WireGuard for its lightweight performance and Defguard for centralized and streamlined access control. The system was implemented within a Docker environment and evaluated using key performance indicators such as latency, throughput, packet loss, and connection stability across multiple internet service providers. The results demonstrated that the WireGuard-based configuration delivered lower latency, zero packet loss, and secure connections without DNS leakage, while token-based authentication significantly simplified user management. Overall, the new system enhanced connection reliability, improved security, and provided scalable remote access for geographically distributed users, making it an effective replacement for the legacy VPN infrastructure.

*This is an open access article under the CC BY-SA license.*

***Corresponding Author:***

Muhamad Hadi Arfian
Department of Informatics Engineering
Esa Unggul University
Jakarta, Indonesia
Email: muhamad.arfian@esaunggul.ac.id
© The Author(s) 2025

## 1. Introduction

In today's evolving digital landscape, the need for secure and efficient remote access systems has become increasingly critical, especially with the growing trend of remote work and workforce mobility. A report from Gartner (2020) stated that over 74% of organizations planned to retain remote work policies permanently after the COVID-19 pandemic. This condition drives companies to adopt technology solutions that can ensure secure access to internal infrastructure without compromising network performance[1-3] .

*Virtual Private Networks* (VPNs) have long served as the standard solution for this purpose[4]. However, traditional VPN protocols such as OpenVPN and IPsec are often considered complex to configure and manage[5-6] . WireGuard, developed by Jason Donenfeld[7], emerged as a modern alternative that offers simplified cryptographic architecture and lightweight design[8], providing both high performance and strong security[9]. A study published by IEEE highlighted that WireGuard outperforms traditional VPNs in terms of latency and throughput, making it a promising option for remote network access needs[10].

At PT. Esta Dana Ventura, the existing VPN infrastructure based on *MikroTik* and the *Point-to-Point Tunneling Protocol* (PPTP) faced several issues, including unreliable connectivity with certain Internet Service Providers (ISPs). Additionally, the complexity in configuration and user management hindered operational efficiency and internal network maintenance.

To address these limitations, the company evaluated modern VPN alternatives, specifically *WireGuard* and *OpenVPN*. The assessment concluded that WireGuard offered notable advantages, including:

1. Performance Efficiency: WireGuard is designed with fewer lines of code, allowing it to run more efficiently and deliver lower latency[7].
2. Advanced Security: WireGuard applies cutting-edge cryptographic algorithms such as *ChaCha20* for encryption, *Poly1305* for authentication, and *Curve25519* for key exchange, which are more efficient than the TLS protocol used by OpenVPN*[5]*.
3. Simplified Configuration: WireGuard requires only a simple key pair for authentication, avoiding the need for complex certificate setups found in OpenVPN*[5]*.

Despite these strengths, WireGuard's deployment in enterprise environments still presents challenges primarily the lack of centralized user management and support for multi-user access control across multiple branches or departments.

To overcome these challenges, an *Identity and Access Management* (IAM) system is required to provide structured access control[11-12] . In this research, *Defguard* is selected as the IAM solution, offering native integration with WireGuard. *Defguard* supports security features such as *Single Sign-On* (SSO), *Multi-Factor Authentication* (MFA), and *Role-Based Access Control* (RBAC), allowing organizations to securely and efficiently manage user permissions. In addition to its technical advantages, this solution was chosen for its cost-effectiveness. Both *Defguard* and *WireGuard* are open-source platforms that do not require commercial licenses, aligning with the company's policy to utilize license-free technologies[13].

This study aims to explore how the integration of Defguard and WireGuard can provide a secure, manageable, and cost-effective remote access solution within PT. Esta Dana Ventura. Furthermore, it investigates the challenges encountered during the implementation and evaluates how the solution can be tailored to the company's specific operational needs.

The implementation process involves various supporting technologies such as *Docker*, *Portainer*, and performance testing tools, with evaluations based on parameters including latency, throughput, packet loss, jitter, and other relevant indicators[14-17] .

## 2. Research Method

This study was conducted through a structured sequence of stages to design and implement a secure and scalable remote access system. The main objective was to integrate the *WireGuard VPN* protocol with *Defguard*, an *open-source* IAM platform.[18]

A. Research Design

The research began by identifying the limitations of the existing VPN infrastructure at PT. Esta Dana Ventura, particularly concerning unstable ISP connectivity and inefficient manual user management. Based on this problem, a solution was designed by adopting *WireGuard* for its cryptographic performance and simplicity, and *Defguard* for centralized user access management[19]. In figure 1 taken from defguard documentation the architecture of Defguard[18].

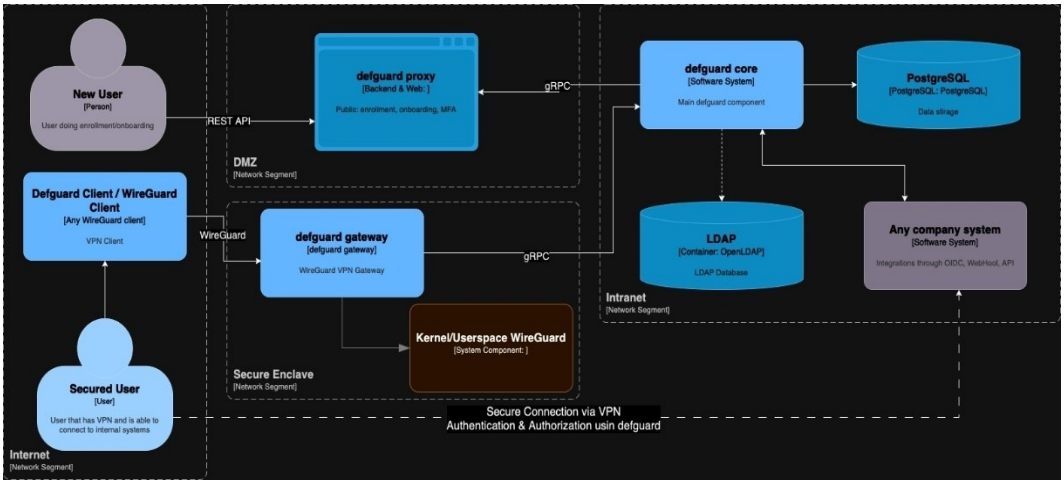

Figure 1. Defguard Architecture

B. Research Procedure

The system development and testing followed the steps below:

1. System Environment Setup

The server environment was built using *Ubuntu Server 20.04*, and the *Defguard* application was containerized using *Docker*. *Nginx* was used as a reverse proxy to manage application traffic.[16-17], [20]

Table 1. Server Specification

| Component | Specification |
|---|---|
| CPU | Intel(R) Xeon(R) CPU E3-1220 v5 @ 3.00GHz x 4 Core |
| RAM | 16 GB DDR4 ECC |
| Storage | HDD 500 GB |
| Operating System | Ubuntu Server 20.04 LTS |
| Virtualization | Docker Engine CE |
| Network Connectivity | Gigabit Ethernet LAN |

Table 1 presents the server specifications used in this study, detailing the hardware and software components that support system deployment. The table outlines essential elements such as processor type, memory capacity, storage configuration, and operating system, providing a clear overview of the server's capability to handle remote access management operations efficiently.

Table 2. Docker Container

| Services | Docker Image | Port |
|---|---|---|
| Defguard Core | ghcr.io/defguard/defguard:0.11.0 | 50055/TCP, 50055/UDP, 8000/TCP |
| Defguard Proxy | ghcr.io/defguard/defguard-proxy:0.5 | 50051/TCP, 8080/TCP |
| Defguard Gateway Admin | ghcr.io/defguard/gateway:0.7 | Internal GRPC |
| Defguard Gateway HO | ghcr.io/defguard/gateway:0.7 | Internal GRPC |
| Defguard Gateway Branch | ghcr.io/defguard/gateway:0.7 | Internal GRPC |
| PostgreSQL | postgres:latest | 5432/TCP |
| Nginx | nginx:latest | 443/TCP, 444/TCP, 445/TCP, 80/TCP |
| Defguard Core | ghcr.io/defguard/defguard:0.11.0 | 50055/TCP, 50055/UDP, 8000/TCP |
| Defguard Proxy | ghcr.io/defguard/defguard-proxy:0.5 | 50051/TCP, 8080/TCP |

Table 3. System Technology

| Component | Technology |
|---|---|
| Sistem Operasi | Ubuntu Server 20.04 LTS |
| Virtualisasi | Docker Standalone |
| VPN Server | Wireguard |
| IAM Platform | Defguard |
| Database | PostgreSQL |
| Web Server | Nginx |

2. User Role Management

Three user roles were defined: Admin (full access), Head Office (file-sharing access), and Branch (limited SFTP server access). Port forwarding was configured on the *MikroTik* router using separate UDP ports (50565, 50566, and 50567) for each user role.

Table 3. User Access Configuration

| Role | VPN Port | Access |
|---|---|---|
| Admin | 50567 | Full Access |
| Head Office | 50565 | File Sharing |
| Branch | 50566 | SFTP Server |

Three user roles were defined to organize access and strengthen security within the system: Admin, Head Office, and Branch. The Admin role holds full control over all system configurations and user management. The Head Office role is granted access specifically for file sharing and coordination between departments, while the Branch role receives restricted access limited only to the SFTP server for operational needs. To support secure and structured connectivity, port forwarding was configured on the MikroTik router

using dedicated UDP ports—50565 for Admin, 50566 for Head Office, and 50567 for Branch. This separation ensures clear traffic segmentation and prevents unauthorized cross-access between roles.

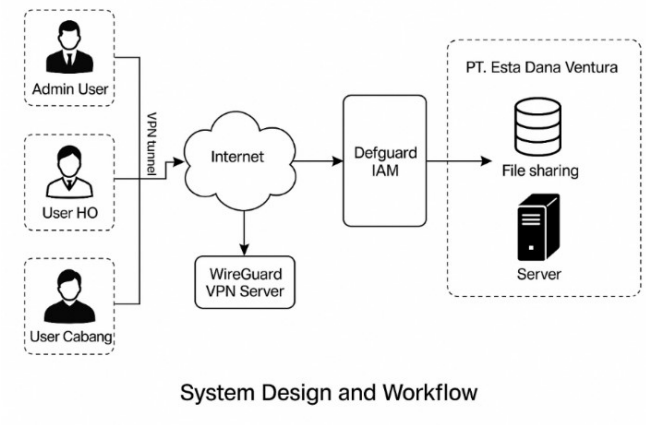


Figure 2. New User Role Workflow

3. Performance Testing

The system was evaluated based on latency, jitter, throughput, and packet loss using tools such as *iperf3* and *ping* command to be compared to general network performance standards.[21-23]

Table 4. QoS Parameter Index

| Parameter | Unit | Ideal Point | Maximum Limit | Category |
|---|---|---|---|---|
| Latency | ms | < 150 ms | ≤ 300 ms | Response time |
| Jitter | ms | 0 ms | ≤ 75 ms | Connection stability |
| Packet Loss | % | 0% | ≤ 3% | Network reliability |
| Throughput | % | 100% | ≥75% | Data capacity |
| Availability | % | ≥ 99.9% (3-nines) | ≥ 95% | Service availability |

Table 5. Jitter Classification

| Category | Jitter |
|---|---|
| Ideal | 0 ms |
| Baik | 0 - 75 ms |
| Sedang | 75 – 125 ms |
| Buruk | 125 - 225 ms |

Table 6. Latency Classification

| Category | Delay |
|---|---|
| Ideal | < 150 ms |
| Baik | 150 – 300 ms |
| Sedang | 300 – 450 ms |
| Buruk | > 450 ms |

Table 7. Packet Loss Classification

| Category | Packet Loss |
|---|---|
| Ideal | 0% |
| Baik | ≤ 3% |
| Sedang | > 3% - 15% |
| Buruk | > 25% |

Table 8. Availability Classification

| Category | Availability |
|---|---|
| Ideal | ≥ 99.99% |
| Baik | 98.99% – 95% |
| Sedang | 94.99% – 85% |
| Buruk | < 85% |

Table 9. Throughput Classification

| Category | Throughput |
|---|---|
| Ideal | 100% |
| Baik | < 100% – 75% |
| Sedang | < 75% – 50% |
| Buruk | < 50% |

4. Security Testing

Encryption visibility and DNS leakage were analyzed through packet inspection using *Wireshark* to ensure secure tunneling of all traffic.[8], [24-26]

5. Availability Testing

Connectivity tests were performed across various ISP commonly used by home users and branch (Indihome, Telkomsel, Tri, XL, CBN, iForte, and Oxygen) to measure reliability and access success rates. In table 10 is the value for ISP connectivity status.[21]

Table 10. Availability Point

| Status | Point |
|---|---|
| Connected | 1 |
| Connected not stable | 0.5 |
| Not connected | 0 |

6. Data Acquisition and Analysis

Each test was repeated five times, The average value ($\bar{X}$) for parameters such as latency, jitter, throughput, and packet loss was calculated by summing all measurement values and dividing by the number of observations ($n$)[27] using equation (1):

$$\bar{X} = \frac{X_1+X_2+X_3+\cdots+X_n}{n} \quad (1)$$

Where:

- $\bar{X}$ = Average value
- $n$ = Total number of measurements
- $X_n$ = Measured value at the $n$-th observation

## 3. Result and Discussion

This section presents the experimental results of the implementation and evaluation of the Defguard-WireGuard VPN system, compared with the previous MikroTik PPTP VPN solution. The discussion covers key performance indicators including latency, throughput, jitter, packet loss, encryption and DNS behavior, and ISP connectivity availability. Each metric is evaluated against accepted performance standards to assess the effectiveness of the solution in a real-world enterprise environment.

### *3.1. New System Implementation*

The system implemented in this research integrates two core components: Defguard, serving as the IAM platform, and WireGuard, acting as the VPN protocol that ensures secure and encrypted remote connections. This integration aims to provide a scalable, manageable, and secure remote access solution for PT. Esta Dana Ventura.

The system architecture adopts a client–server model, where users from various remote locations access the company's internal network over the Internet through a WireGuard-encrypted VPN tunnel. The connection process begins at the client side, where users authenticate through Defguard using a one-time

registration token. Once verified, Defguard assigns access rights based on predefined roles configured by the system administrator.

Defguard functions as the identity management center, providing a web interface for administrators to register users, manage VPN keys, and assign roles. It is hosted on a server alongside supporting services such as PostgreSQL for user data storage and Nginx as a reverse proxy to secure access to the web-based services.

All users establish connections through the WireGuard VPN tunnel, which ensures end-to-end data confidentiality and integrity while traversing public networks. This tunnel effectively bridges the user's device to the internal services of the company, enabling remote operations to be conducted securely and reliably. The new user workflow can be seen in figure 3.

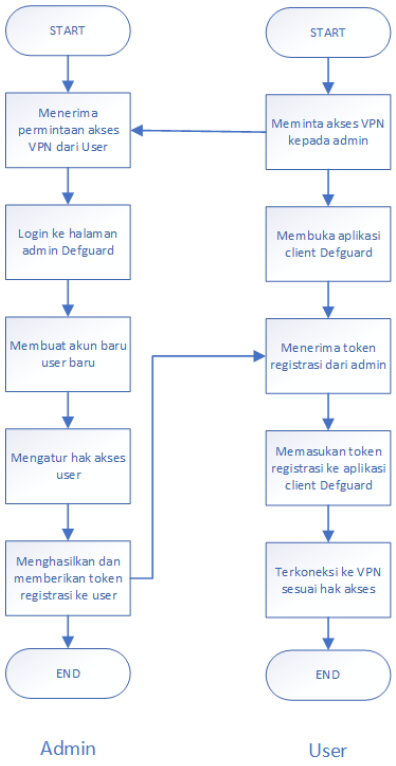


Figure 3. User and Admin Registration Process

## *3.2. Performance Evaluation*

The VPN system was tested based on four core Quality of Service (QoS) metrics: latency, throughput, jitter, and packet loss. Each test was performed five times and the average values were calculated. Throughput results were converted into percentage values against the theoretical maximum bandwidth of 10 Mbps. The evaluation results are shown in Table 11.

Table 11. Performance Comparison Between MikroTik VPN and WireGuard VPN

| Parameter | PPTP VPN (Mikrotik) | WireGuard VPN (Defguard) | Standard |
|---|---|---|---|
| Latency (avg) | 9.2 ms | 7.47 ms | ≤ 300 ms |
| Throughput (avg) | 92.94% | 93.52% | ≥ 75% |
| Jitter (avg) | 0.5125 ms | 0.5558 ms | ≤ 75 ms |
| Packet Loss (avg) | 0% | 0% | < 3% |

The results show that both VPN solutions comply with the performance standards. However, WireGuard VPN slightly outperforms MikroTik in terms of latency and throughput. Jitter and packet loss remained within excellent ranges for both systems, indicating consistent and reliable performance.

## *3.3. Security Analysis Using Wireshark*

Security evaluation was conducted using Wireshark packet inspection. The goal was to verify the integrity of data encryption and detect any DNS leakages. As shown in Table 12, both VPNs successfully encrypted payload data—no readable information was found in the captured packets. However, the MikroTik VPN exhibited DNS leaks, while WireGuard encapsulated all DNS traffic within the VPN tunnel.

Table 12. Security Evaluation Using Wireshark

| Metric | MikroTik VPN | WireGuard VPN (Defguard) | Standard |
|---|---|---|---|
| Encryption Visibility | Not Readable | Not Readable | Not Readable |
| DNS Leak | Detected | Not Detected | Not Detected |

This indicates that WireGuard provides a more secure transmission channel, fully tunneling both data and DNS requests, reducing the risk of data interception and DNS spoofing.

## *3.4. ISP Availability Testing*

The VPN connection availability was tested across seven ISP in Indonesia: Indihome, Telkomsel, Tri, XL, CBN, iForte, and Oxygen. This test aimed to determine the real-world usability and reliability of each VPN solution across diverse network infrastructures.

The results indicate that the MikroTik VPN was only accessible on three providers (42.9%), while WireGuard VPN with Defguard successfully connected on six providers (85.7%).

Table 13. ISP Availability Evaluation

| No | ISP / Provider | PPTP (Mikrotik) | Bobot | WireGuard (Defguard) | Bobot |
|---|---|---|---|---|---|
| 1 | Indihome | Terkoneksi | 1 | Terkoneksi | 1 |
| 2 | CBN | Terkoneksi | 1 | Terkoneksi | 1 |
| 3 | iForte | Tidak terkoneksi | 0 | Terkoneksi | 1 |
| 4 | Oxygen | Terkoneksi | 1 | Terkoneksi | 1 |
| 5 | XL (Tethering) | Tidak terkoneksi | 0 | Terkoneksi tidak stabil | 0.5 |
| 6 | Telkomsel (Tethering) | Tidak terkoneksi | 0 | Terkoneksi tidak stabil | 0.5 |
| 7 | Tri (Tethering) | Tidak terkoneksi | 0 | Terkoneksi | 1 |

Based on these results, WireGuard VPN outperformed MikroTik PPTP, showing greater compatibility with current ISP infrastructures. According to the ETSI EG 202 009-1 availability classification[22]:

- WireGuard VPN with 85.7% availability is categorized as "Moderate"
- PPTP VPN with only 42.9% is considered "Poor"

Although WireGuard has not yet reached the "Standard" category (≥95%), it represents a significant improvement over the legacy PPTP MikroTik implementation.

## *3.5. Role-Based Access Control Evaluation*

To ensure secure and structured access to internal network resources, the implemented system utilizes RBAC as provided by the Defguard platform. RBAC enables administrators to define user roles and assign access permissions accordingly, ensuring that each user can only interact with systems relevant to their responsibilities. This significantly reduces the attack surface and simplifies access management. In the implemented system at PT. Esta Dana Ventura, three distinct user roles were established:

1. Admin User: has unrestricted access to all system components, including Defguard's web dashboard, user management, server configurations, and monitoring tools. This role is reserved for IT administrators responsible for maintaining and managing the overall infrastructure.
2. Head Office User: has limited access restricted to internal file-sharing services within the head office network. This ensures that operational staff working from remote locations can securely access shared documents without exposing other internal systems.
3. Branch User: is granted access only to designated servers and services based on specific IP subnets configured through WireGuard. This role is designed for employees or teams working at remote branches, enabling controlled access to only the necessary backend systems.

The enforcement of RBAC is facilitated through Defguard's web-based management interface, where administrators can register users, assign them to predefined roles, and issue VPN key pairs. Notably,

the system employs a one-time token registration mechanism, which enhances security during user provisioning by preventing static credential reuse. Testing showed that each user role was effectively restricted to its assigned network scope. Admins had full visibility and access across all subsystems, while HO and Branch users encountered access limitations consistent with their roles. These results confirm the proper implementation of RBAC policies and demonstrate that Defguard can enforce granular access control without adding complexity to the user experience.

## 4. Conclusion

This study has successfully designed and implemented a secure and scalable remote access solution by integrating Defguard, an open-source Identity and Access Management (IAM) system, with the WireGuard VPN protocol. The objective was to address the connectivity issues, security limitations, and user management inefficiencies found in the legacy MikroTik-based VPN system used at PT. Esta Dana Ventura.

The implementation phase introduced a new system architecture that utilizes a client–server model, in which users authenticate through Defguard using a one-time token and connect via WireGuard tunnels. This design ensures that all data traversing public networks is encrypted and integrity-protected. The use of Docker, PostgreSQL, and Nginx allowed for a modular, secure, and maintainable deployment environment.

A significant enhancement was observed in **Role-Based Access Control (RBAC)**. Users were divided into three roles—Admin, Head Office, and Branch—each receiving access only to the systems they were authorized for. Admins managed the infrastructure, HO users accessed shared files, and Branch users were limited to designated internal servers. Testing confirmed that RBAC policies were correctly enforced, improving both security and operational control.

The experimental results showed that WireGuard outperforms the legacy MikroTik VPN in several aspects:

1. Latency decreased from 9.2 ms to 7.47 ms,
2. Throughput improved from 92.94% to 93.52%,
3. Packet loss remained at 0%,
4. DNS leak was eliminated, and
5. ISP connectivity increased from 42.9% to 85.7%.

The findings demonstrate that the integration of Defguard and WireGuard meets the goals established in the study: delivering secure, efficient, and user-friendly remote access while resolving previous limitations, by delivering improved performance, enhanced security, and better compatibility across ISPs.
The system has potential for further development, including:

1. Integration with additional authentication methods (e.g., OAuth2, LDAP),
2. Expansion to larger-scale multi-branch deployments,
3. Real-time monitoring and alerting,
4. And formal security certification for enterprise-level compliance.,

This research contributes not only a working implementation but also a practical reference for other organizations aiming to adopt open-source, secure remote access infrastructure tailored to enterprise needs.

## Acknowledgement

The author would like to express sincere gratitude to PT. Esta Dana Ventura for providing the opportunity and support throughout the research and implementation of this project. Special thanks are also extended to the supervising lecturer and academic advisors whose guidance, feedback, and encouragement have been invaluable throughout the writing of this paper.

Appreciation is also given to fellow students and colleagues who provided moral and technical support during the data collection, testing, and analysis phases. Finally, the author thanks their family and loved ones for their continuous motivation and understanding throughout the completion of this research.

## References

[1] J. Lavelle, “Shifting Some Employees to Remote Work Permanently,” 2020.

[2] D. F. Priambodo, Amiruddin, and N. Trianto, “Hardening a Work from Home Network with Wireguard and Suricata,” in *Proceedings - 2nd International Conference on Computer Science and Engineering: The Effects of the Digital World After Pandemic (EDWAP), IC2SE 2021*, 2021, pp. 1–4. doi: 10.1109/IC2SE52832.2021.9791983.

[3] B. Schneier, *Applied Cryptography*, vol. 1, no. [32. John Wiley & Sons, 1996. doi: 10.1.1.99.2838.

[4] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, "Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work," *Information (Switzerland)*, vol. 15, no. 11, pp. 1–25, 2024, doi: 10.3390/info15110734.

[5] S. Mackey, I. Mihov, A. Nosenko, F. Vega, and Y. Cheng, "A performance comparison of WireGuard and OpenVPN," in *Proceedings of the Tenth ACM Conference on data and application security and privacy*, 2020, pp. 162–164.

[6] E. Barker, Q. Dang, F. Sheila, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs," *Special Publication (Nist SP) - 800-77r1*, p. 166, 2020, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf%0Ahttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

[7] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," *24th Annual Network and Distributed System Security Symposium, NDSS 2017*, pp. 1–20, 2017, doi: 10.14722/ndss.2017.23160.

[8] B. Dowling and K. G. Paterson, "A cryptographic analysis of the WireGuard protocol," in *International Conference on Applied Cryptography and Network Security*, 2018, pp. 3–21.

[9] B. Schneier, *Applied Cryptography*, vol. 1, no. [32. John Wiley & Sons, 1996. doi: 10.1.1.99.2838.

[10] D. F. Priambodo, Amiruddin, and N. Trianto, "Hardening a Work from Home Network with Wireguard and Suricata," in *Proceedings - 2nd International Conference on Computer Science and Engineering: The Effects of the Digital World After Pandemic (EDWAP), IC2SE 2021*, 2021, pp. 1–4. doi: 10.1109/IC2SE52832.2021.9791983.

[11] V. Kumar and A. Bhardwaj, "Identity Management Systems," *International Journal of Strategic Decision Sciences*, vol. 9, no. 1, pp. 63–78, 2018, doi: 10.4018/ijsds.2018010105.

[12] J. Anderson, "The Role of Identity and Access Management (IAM) in Securing Cloud Workloads," 2022.

[13] "Introduction | defguard," 2025. [Online]. Available: https://docs.defguard.net/

[14] ETSI, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)," *Etsi Tr 101 329 V2.1.1*, vol. 1, pp. 1–37, 2020.

[15] O. Bartunov, "What is PostgreSQL."

[16] D. Merkel, "Docker : Lightweight Linux Containers for Consistent Development and Deployment Docker : a Little Background Under the Hood," *Linux Journal*, vol. 2014, no. 239, pp. 2–7, 2014, [Online]. Available: http://delivery.acm.org.ezproxy.library.wisc.edu/10.1145/2610000/2600241/11600.html?ip=128.104.46.196&id=2600241&acc=ACTIVE SERVICE&key=066E7B0AFE2DCD37.066E7B0AFE2DCD37.4D4702B0C3E38B35.4D4702B0C3E38B35&__acm__=1557803890_216b4a0168a6b29b8f2e7a74

[17] D. Aivaliotis, *Mastering Nginx*. 2013. [Online]. Available: https://www.packtpub.com/networking-and-servers/mastering-nginx

[18] "Architecture | defguard," 2025. [Online]. Available: https://docs.defguard.net/in-depth/architecture

[19] A. V Ostroukh, C. B. Pronin, A. A. Podberezkin, J. V Podberezkina, and A. M. Volkov, "Enhancing Corporate Network Security and Performance: A Comprehensive Evaluation of WireGuard as a Next-Generation VPN Solution," in *2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2024, pp. 1–5. doi: 10.1109/SYNCHROINFO61835.2024.10617501.

[20] X. Wang, H. Zhao, and J. Zhu, "GRPC: A communication cooperation mechanism in distributed systems," *ACM SIGOPS Operating Systems Review*, vol. 27, no. 3, pp. 75–86, 1993.

[21] A. Basri and B. Yuliadi, "Wireless Network Bandwidth Quality Measurement Using Qos Standard Tiphon," *PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic*, vol. 11, no. 2, pp. 283–292, 2023.

[22] ETSI, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)," *Etsi Tr 101 329 V2.1.1*, vol. 1, pp. 1–37, 2020.

[23] "30 Network Performance Metrics to Measure Network Health." [Online]. Available: https://research.aimultiple.com/network-performance-metrics/

[24] S. Kent and K. Seo, "RFC 4301: Security Architecture for the Internet Protocol," 2005, *RFC Editor, USA*.

[25] B. Schneier and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 132–141, 1998, doi: 10.1145/288090.288119.

[26] P. Arora, P. R. Vemuganti, and P. Allani, "Comparison of VPN Protocols – IPSec , PPTP , and L2TP," vol. ECE 646, no. Fall (2021), pp. 1–45, 2021, [Online]. Available: https://ece.gmu.edu/coursewebpages/ECE/ECE646/F09/project/reports_2001/arveal.pdf
[27] D. C. Montgomery, *Design and analysis of experiments*. John wiley & sons, 2017.