APPLICATION OF OPEN VPN AND WIREGUARD TO THE COMPUTER NETWORK OF ISPSC STA MARIA CAMPUS

ROSELYN S. DELMENDO

JUBILEO JB U. DIZON

HANNIE ROSE A. GARRIDO

RUBELYN R. RECOLCOLIN

JHENELLA MAE G. SAGUN

ILOCOS SUR POLYTECHNIC STATE COLLEGE

COLLEGE OF COMPUTING STUDIES

SANTA MARIA, ILOCOS SUR

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

FEBRUARY 2023

TABLE OF CONTENTS

		Page
TITLE PAGE	.....	i
APPROVAL SHEET	.....	ii
ABSTRACT	.....	iii
ACKNOWLEDGEMENT	.....	iv
DEDICATION	.....	vi
TABLE OF CONTENTS	.....	xi
LIST OF FIGURES	.....	xiii
LIST OF TABLES	.....	xiv

CHAPTER

1 INTRODUCTION

Background of the Study..... 1

Conceptual framework of the Study..... 5

Objectives of the Study..... 5

Scope and Limitation of the Study..... 6

Importance of the Study..... 6

2 METHODOLOGY

Research Design..... 7

Software Model..... 8

Project Plan..... 13

Project Assignments..... 14

Research Instrument..... 15

Data Analysis..... 16

3 RESULTS AND DISCUSSIONS

Findings..... 19

Conclusions..... 24

Recommendations 25

GLOSSARY 27

REFERENCES 28

APPENDICES 31

BIOGRAPHICAL SKETCH 38

Chapter 1

INTRODUCTION

Background of the Study

In today's interconnected world, computer networks play a crucial role in facilitating communication, data sharing, and resource access. Educational institutions, such as Ilocos Sur Polytechnic State College (ISPSC), rely heavily on computer networks to support various academic and administrative activities. As the demand for secure and private connectivity increases, the implementation of two well-known virtual private network (VPN) technologies, OpenVPN and WireGuard, to strengthen the computer network security of the institution is the main goal of this capstone project. ISPSC aims to establish secure and private communication channels within its network architecture by using these VPN solutions, protecting sensitive data and reducing potential security threats.

According to (Beritelli, F., La Corte, A., Sciuto, G.L., Rametta, and Scaglione 2015), VPN is becoming more and more popular as a way to send data securely over "insecure" public networks like the internet at a lower cost. The variety of advantages they provide is what makes VPNs so well-liked in today's society. The primary concept behind VPN and the reason why it gained popularity is that it takes advantage of the internet as a universal medium that is accessible everywhere. However, because everyone uses the internet, which is a common resource, the data is especially susceptible to numerous breaches. Unauthorized access is among those breaches that cause damage and eavesdropping, which can end up hurting the organization rather than helping it. However, the purpose of VPN is to deliver dependable, secure, and specified networks within the specified installation budget. By applying various security measures, the user can overcome the downsides, and in the end, he or she can decide whether the

technology is appropriate for their organization or use scope and whether the benefits outweigh the negatives.

The use of VPN technology has expanded beyond individual users to encompass businesses, educational institutions, and government entities. VPNs enable organizations to establish secure connections between geographically dispersed locations, facilitating seamless communication and collaboration. According to (Thompson et al. 2022), VPNs play a crucial role in safeguarding sensitive data and trade secrets, particularly for industries dealing with confidential information. By employing encryption protocols and authentication mechanisms, VPNs ensure that data transmitted over public networks remains confidential and protected from eavesdropping and unauthorized access. The increasing adoption of VPNs underscores their effectiveness in mitigating security risks and maintaining privacy in an interconnected world. Studies by (Maggi, F., Quarta, D., Pogliani, M., Polino, M., Zanchettin, A.M., and Zanero, S. 2017) because of OpenVPN's long-standing reputation for robustness and compatibility across various platforms, it has been widely implemented in numerous network environments, showcasing its effectiveness in enhancing security and enabling remote access. On the other hand, WireGuard's innovative design, with its streamlined codebase and improved performance, has been praised for reducing potential attack vectors and delivering efficient throughput.

Strong Swan and OpenVPN are well-known VPN solutions that provide secure connections between two endpoints. However, these usages are typical, acknowledged as being complicated and easily misconfigured Both implementations are also built on established protocols. While standardized procedures undoubtedly have their benefits, Standardization takes time, and as a result, such implementations frequently have to

maintain antiquated features like weak cryptographic algorithms. The difference between conventional, unreliable Internet and dependable Internet. As more businesses provide internal services for their customers and employees, the intranet is losing relevance. As a result, it is frequently necessary to contact these internal offices online. This data must be backed up in order to assure data security. A virtual private network is a frequently employed method to accomplish this (Dekker, E., & Spaans, P. 2020).

In order to replace both IPsec and popular user space and/or TLS-based alternatives like OpenVPN, WireGuard, a secure network tunnel running at layer 3 and implemented as a kernel virtual network interface for Linux, aspires to be more secure, faster, and simpler to use. The association between a peer public key and a tunnel source IP address is the virtual tunnel interface's foundational tenet for secure tunnels. It is built on NoiseIK, uses a single round-trip key exchange, and uses a cutting-edge timer state machine technique to handle session generation invisibly to the user. Mutual authentication is carried through using short pre-shared static keys (Curve25519 points) in the same manner as OpenSSH. Strong perfect forward secrecy is provided by the protocol (Tolley, W.J., Kujath, B., Khan, M.T., Vallina-Rodriguez, N. and Crandall, J.R., 2021).

In Linux, IPsec, which makes use of the Linux transform ("xfrm") layer, is the default method for creating encrypted tunnels. For each set of packets passing the subsystem, users fill out a kernel structure specifying the cipher suite, key, or other transforms (such as compression) to apply. These data structures are typically updated by a user space daemon in response to the findings of a key exchange, which is typically conducted using IKEv2, a convoluted protocol with a wide range of options and flexibility. This solution has a sizable amount of code and is somewhat sophisticated.

For firewalling semantics and secure labeling for IPsec packets, administrators have a totally different set of rules (Markettos, A.T., Rothwell, C., Gutstein, B.F.,Pearce, A., Neumann, P.G., Moore, S.W. and Watson, R.N., 2019).

According to (Jones and Smith, 2020), OpenVPN and WireGuard have gained significant attention due to their unique features, high-security standards, and ease of implementation. By integrating these protocols into the ISPSC network, we aim to enhance network security, improve remote access efficiency, and streamline network management processes. In relation to this, the ISPSC network serves as a vital platform for various educational activities, including research, administrative operations, and student information management. However, the existing network infrastructure may lack adequate security measures to protect against unauthorized access, eavesdropping, and data breaches. As a result, it increases the risk of file corruption when it comes to important office files. OpenVPN and WireGuard offer robust VPN solutions that can address these security concerns by establishing encrypted tunnels between network devices, effectively shielding data from potential attackers. To fill a such gap in the literature and to further understand the concept of the involvement of VPN within the institution, this study was conducted to focus in enhancing the computer network of locos Sur Polytechnic State College, Santa Maria, Ilocos Sur, hence the reason for its implementation.To be more precise, it was conducted to achieve the following goals: a.) to improve remote access efficiency for staff, students, and other authorized users of the ISPSC network; b.) to enhance security, flexibility, and accessibility; c.) to establish secure and private communication channels within its network infrastructure, safeguarding sensitive data and mitigating potential security risks. Additionally, the

study can be a reference for other institutions that wish to enhance their security when it comes to network connectivity.

Conceptual Framework of the Study

A conceptual framework was a versatile analytical tool with several usages. It was used to arrange concepts and draw mental distinctions. Hence, it served as the visual representation for the study and can be significantly more systematic and logical. It could be utilized to show the relationship between the various variables in the developed Application of Open Vpn and Wireguard.

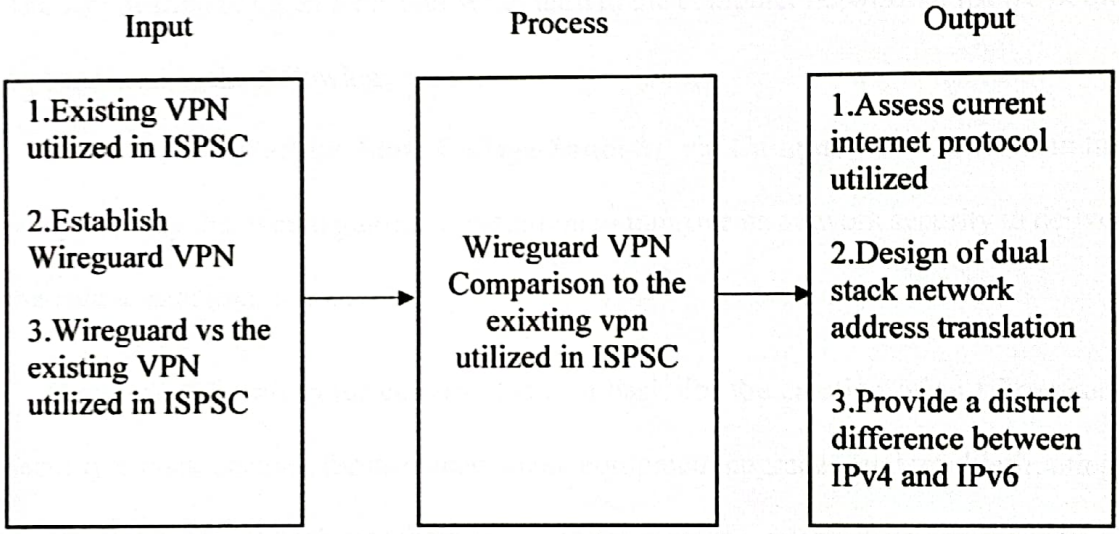

Figure 1. Conceptual Framework

Objectives of the Study

This project aimed to compare the OpenVPN and WireGuard to determine the performance of it and to identify the security features.

Specifically, it aimed to answer the following objectives:

1. To determine the existing VPN used in Ilocos Sur Polytechnic State College Sta. Maria Campus.
2. To establish Wireguard VPN in ISPSC Sta. Maria Campus.

3. To assess distinct difference between Wireguard and existing Vpn in ISPSC.

Scope and Limitation of the Study

The study focused to assess the existing Application of OpenVPN and Wireguard to the Computer Network of Ilocos Sur Polytechnic State College for Santa Maria Campus test capability and performance to the security of it.

This research is conduct to compare the performance of the OpenVPN and Wireguard in terms of being fast, secure, stable, and reliability.

Importance of the Study

The Application of Open VPN and Wireguard to the computer network of ISPSC could be beneficial to the following:

Ilocos Sur Polytechnic State College-Santa Maria Campus will benefit from the study in a way that would guide the institution to improve its network security to deliver the data to safe transaction.

Network Administrator can use this as a basis for the creation of an IT network security implementation for its management, equipment upgrades, and troubleshooting.

Employees would enhance their data security, remote work facilitation, streamlined network management, and potential professional growth, positively impacting their work experience and career development.

The Researchers can use this study to enhance their capabilities and skills in designing a Data Security with a network mechanism for the ISPSC.

Future Researchers could use this study as a reference for the conduct of similar studies in connection with advanced IT computer networking and security.

Chapter 2

METHODOLOGY

This chapter outlines the process followed in gathering the data and doing the analysis that was important to the study. The study research design, software model, population and locale, research instrument, and data analysis tools are all discussed. It also provides information about who the respondents are, and how they were sampled for the research.

Research Design

The researchers design employed in this study is a descriptive experimental design. This design, proposed by Johnson and Christensen (2019), allows for a comprehensive exploration and development of a particular phenomenon while also incorporating experimental elements to evaluate the effectiveness of the implemented solution. In the descriptive phase, the current state of ISPSC's computer network infrastructure was examined, including its architecture, security measures, and network services. This involved conducting a thorough assessment of the existing network infrastructure, identifying potential vulnerabilities, and understanding the specific requirements and challenges faced by the institution. Which sought to learn more about the status of a phenomenon at a given time. This form of study aimed to produce an accurate profile of circumstances, individuals, or events (Rahi, 2017). The developmental study design could provide a comparison of two separate but related randomized experiments and repeated observations of the same occurrences over time. (Mehran, 2017). In addition to using an experimental study approach, the researchers also used a purposive sample technique where customers can allow to operate and test the developed system and operate to ensure its smooth performance. By all means, the data were unbiasedly collected from the respondents that simply express their experience and ratings

throughout the acceptability of the Application of OpenVPN and Wireguard to the computer network of ISPSC through having a complete and deep observation in terms of the security and connection. Hence, this approach served as the way for the analysis, interpretation, and integration of the data within the application of OpenVPN and Wireguard to the computer network of ISPSC. This method benefited the developers of the researchers wherein different programming languages and software packages were applied. Generally, the data flow efficiently works to the point that the optimum user interface was built and incorporated into the web application.

The developmental phase involved designing and implementing the selected VPN protocols, OpenVPN and WireGuard, within the context of the Zero Trust model. The Zero Trust model, pioneered by Forrester Research (Brown & Kindervag, 2010), challenges the traditional security approach by assuming zero inherent trust and systematically verifying every access attempt within the network. By adopting this model, ISPSC aimed to enhance the security, access control, and overall performance of its computer network. The experimental phase focused on evaluating the performance, security, and user satisfaction aspects of the implemented VPN solution. This involved conducting tests and measurements to assess factors such as throughput, latency, and encryption capabilities. Additionally, a questionnaire survey using the WAMMI instrument was administered to gather user feedback on the usability, connectivity reliability, and overall satisfaction with the OpenVPN and WireGuard implementation within the Zero Trust model.

Software Model

The study used Zero Trust, an iterative procedure that systematically ensure that users and devices can safely connect to the internet, regardless of where the access

request is from, without the complexity associated with legacy approaches. They also need to proactively identify, block, and mitigate targeted threats such as malware, ransomware, phishing, DNS data exfiltration, and advanced zero-day vulnerabilities for users. Zero Trust security can improve security postures while reducing the risk of malware. Imagine a scenario where ISPSC's computer network is evolving to accommodate an increasing number of users, devices, and services. Traditional network security measures, which typically rely on perimeter defenses and trust within the internal network, may no longer provide adequate protection against sophisticated cyber threats (Collier, Z.A. and Sarkis, J., 2021).

In response to these challenges, the researchers adopted the Zero Trust model as a robust security framework. The Zero Trust model, introduced by Forrester Research, operates on the principle that no connection or user should be inherently trusted, regardless of their identity or device location. Instead, each network connection must be thoroughly authenticated, authorized, and continuously verified, ensuring that only trusted entities can access network resources. The Zero Trust model implements rigorous verification steps for remote staff members to access sensitive information. This reduces the attack surface and minimizes the risk of unauthorized access or lateral movement within the network. This approach is particularly useful for MIS office staff members who need to access sensitive information from a remote location. Every network traffic request, regardless of its origin or destination, undergoes continuous monitoring and verification. This ensures that each connection is validated based on its adherence to defined security policies, allowing only legitimate and authorized traffic to flow within the network.

Figure 2. The Zero Trust Model

Figure 2 presents the Zero trust Model for identities are given access to the programs, networks, systems, and data they require to perform their employment, and this trust is regularly verified to ensure the employee is who they say they are. Zero trust model that consist of five phases and several procedures that help the project progress.

The five phases utilized to implement Zero Trust Model are as follows:

User: As the researchers focused on enhancing user access and authentication within the computer network of ISPSC, they recognized the significance of going beyond traditional username and password combinations to verify user identities. Embracing the principles of the zero trust model, they implemented multi-factor authentication (MFA) as an additional layer of verification. This required users to provide a unique code generated by an authenticator app on their smartphones. Additionally, the researchers integrated an identity and access management (IAM) solution to enforce precise user permissions and restrictions. With the IAM system in place, users were granted access only to the resources relevant to their roles and responsibilities. By adopting this approach, the researchers minimized the potential attack surface and

ensured that each user's trustworthiness was continually evaluated, regardless of their network location or device used.

Device: The researchers shifted their focus to the security and management of devices within the ISPSC network. Embracing the zero trust principle that no device should be inherently trusted, they implemented robust device authentication mechanisms. This involved the deployment of device certificates and a device identity management solution to verify the authenticity and authorization of devices accessing the network. Furthermore, they enforced stringent security policies on devices, ensuring they remained updated with the latest software patches and adhered to predefined security configurations. By taking a proactive approach, the researchers minimized the risk of compromised or vulnerable devices compromising the integrity of the network and data.

Network Traffic: With a focus on network traffic management aligned with the zero trust model, the researchers directed their attention to securing the flow of data within the ISPSC network. They implemented network segmentation, strategically dividing the network into isolated segments, which served as barriers to prevent threats from spreading laterally across the network. By implementing this approach, they effectively limited the potential impact of a security breach.

Application: By focusing on securing applications and services, the researchers strengthened the overall security posture of the ISPSC network. Their implementation of robust authentication and authorization mechanisms, adherence to secure coding practices, and proactive vulnerability management contributed to the protection of sensitive data and ensured a resilient and secure application environment.

Data: Recognizing the value of data as a critical asset requiring special attention, the researchers implemented the zero trust model to ensure its protection. They adopted data encryption techniques to safeguard sensitive information during transit and while at rest. This approach ensured that even if data was intercepted or compromised, it would remain inaccessible without the appropriate decryption keys. Furthermore, stringent data access controls were implemented, granting permissions on a need-to-know basis. To actively monitor and prevent unauthorized access or leakage of sensitive data, the researchers deployed data loss prevention (DLP) solutions. Additionally, data classification policies were established, enabling them to prioritize protection measures based on the level of sensitivity. These measures further strengthened the zero trust model's data-centric approach.

Through the phased implementation of the zero trust model, leveraging open VPN **and** Wireguard.

Internet. The researchers prioritized securing the connection between the network and the internet by implementing encrypted VPN technologies like open VPN and WireGuard. This created secure tunnels over public networks, encrypting data transmission and preventing unauthorized access. The zero trust approach ensured rigorous security principles, verifications, and access controls were applied, ensuring consistent protection regardless of the network's physical location. The VPN tunnels channeled all network traffic, ensuring robust protection for all traffic.

Experimentation. Researchers conducted experiments to compare OpenVPN and WireGuard networks, focusing on security differences. They allocated a phase for experimentation, encouraging innovation and exploration. Controlled experiments and pilots assessed the feasibility and effectiveness of emerging security solutions aligned

with the zero trust model. This allowed for informed decisions about implementing novel security measures within the ISPSC network. Regular evaluations and assessments improved security strategies and enhanced the overall security posture. The implementation of the zero trust model using open VPN and WireGuard was comprehensive and dynamic, fostering a secure and trusted computing environment within ISPSC.

Project Plan

Table 1 presented the methods and procedures that were used to collect information required to clearly illustrate the status of the development of the Application of Open VPN and Wireguard to the computer network of Ilocos Sur Polytechnic State College, which could lessen the burden on the managers. It also shows the pattern and time frame for each of the five phases of the Zero Trust Model during the experimentation phase, we actively collaborated with industry partners, participated in cybersecurity conferences, and engaged with research institutions to stay abreast of the latest advancements in security technologies and methodologies. This allowed us to leverage external expertise and gather valuable insights, enriching our experimentation process. By fostering an environment of collaboration and knowledge sharing, we were able to evaluate cutting-edge solutions such as AI-driven threat detection systems, blockchain-based identity management, and behavior analytics tools. Through these endeavors, we aimed to identify innovative approaches that could further strengthen our zero trust implementation, ensuring that our network remained resilient against emerging cyber threats while enabling us to continuously adapt and evolve our security strategies.

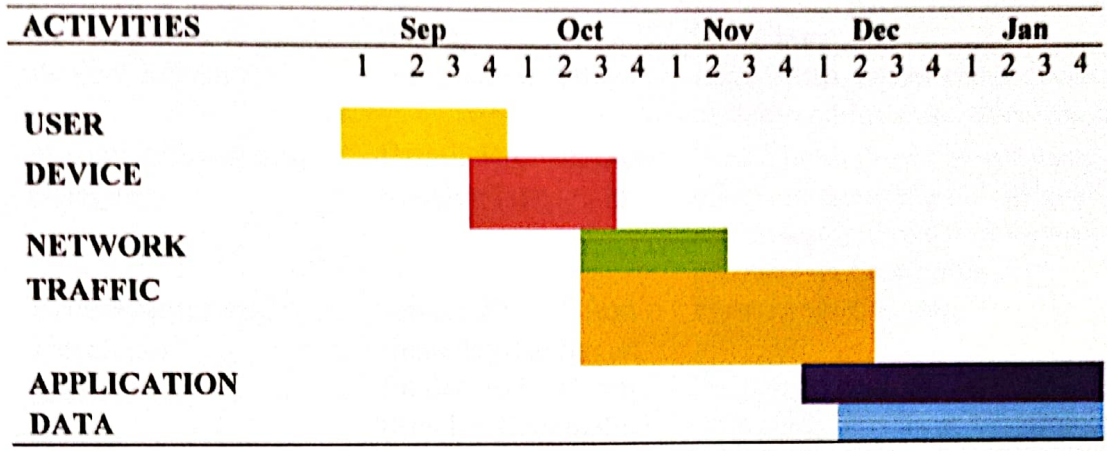

Table 1. The Project Schedule Gantt Chart

Project Assignments

The roles and responsibilities of the project team members within the proposed application, entitled Application of Open VPN and Wireguard to the computer network of ISPSC Sta. Maria Campus.

Table 2 shows the role requirements and responsibilities of the members of the team. It was show that each member had different tasks and responsibilities assigned. The project manager was the one who provided the assignments to the member according to their skills and was responsible for the overall management of the project and building cooperative teamwork in the group. The developer was responsible for the analysis and design, the rest of the members are documenters or planners of the team who provides teamwork in the overall development and status of the project and lastly, the testers are responsible for the performance test of the development of the technology that was done in this project.

Roles	Name	Functions
Project Manager	Jubileo Jb U. Dizon	Lead Team, report status review of deliverables and assure quality
System Analyst and Designer	Hannie Rose Garrido Roselyn Delmendo	Coordinates the technical team's efforts in resolving challenges and ensuring that solutions are practical and consistent.
Programmer and Developer	Jubileo Jb U. Dizon Jhenella Mae Sagun	Framework Content
QA / Tester	Jubileo Jb U. Dizon Rubelyn Recolcolin	Responsible for checking the debugging queries of the project. Test the performance of the project.
Documenter/Technical Writer	Hannie Rose Garrido Roselyn Delmendo	Design the project performance management

Table 2. The Role Requirements and Responsibility of the Team Population and Locale

The researchers utilized purposive sampling that helped them determine the distribution of respondents, which included students, teaching staff, non-teaching staff from the different colleges of Ilocos Sur Polytechnic State College, and customers outside the institution was within the municipality of Santa Maria, Ilocos Sur.

Table 3 presented the distribution of the respondents selected to participate to measure the Level of Acceptability of the proposed application which is composed of 5 respondents, namely 2 teaching-staff and 3 non-teaching staff of Ilocos Sur Polytechnic State College Sta. Maria Campus.

Respondents	N
MIS Staff	**5**
TOTAL	**5**

Table 3. Distribution of Respondents

Research Instruments

The researchers embarked on an extraordinary journey guided by the invaluable tool of survey forms in their quest to enhance the computer network of ISPSC. They

recognized the significance of capturing the insights and requirements of the five dedicated staff members from the MIS office. Through engaging with the MIS staff and fostering trust, they encouraged active participation in the survey, recognizing the importance of their input in shaping the network transformation. As survey responses poured in, the power of data unfolded, offering a rich tapestry of insights into the thoughts, experiences, and aspirations of the MIS staff. Meticulous data collection and analysis allowed the researchers to identify patterns and unique perspectives that informed their decision-making process. The voices of the MIS staff became a compass, influencing choices and strategies, ultimately leading to an implementation phase grounded in their collective wisdom. Armed with the survey findings and a clear vision, the researchers integrated OpenVPN and WireGuard to address the challenges and aspirations of the MIS office, ensuring a network transformation that exceeded expectations. The successful journey, fueled by collaboration and the power of their voices, resulted in a network infrastructure that truly served the needs of ISPSC.

Data Analysis

The researchers conduct a questionnaires, surveys, and user feedback among the staff of the MIS office to gather information. Performance tests also included. During the interview with the Management Information Systems (MIS) staff at ISPSC Sta. Maria Campus, valuable insights were obtained regarding the existing VPN infrastructure. It was revealed that Open VPN is the primary VPN solution used within the campus network. Open VPN was chosen due to its widespread adoption, security features, and compatibility with various operating systems. Dr. Barayuga mentioned that the implementation of Open VPN has been successful over the years, providing secure connectivity for remote users and branch campuses to the central network. It allows access to internal resources, ensuring the confidentiality of sensitive data during

transmission. While Open VPN has generally met the institution's requirements, Dr. Barayuga acknowledged occasional challenges related to latency and bandwidth constraints during periods of high usage. Users also expressed a moderate level of satisfaction with the existing VPN implementation, while some users found the VPN easy to use and appreciated its secure connectivity, others reported challenges in the configuration process and occasional disruptions in connectivity. In terms of performance, users generally perceived the VPN to have acceptable data transfer speeds and latency. However, there were suggestions for improvements to enhance speed and reduce occasional lags or disconnections. Regarding security, users indicated a high level of trust in the VPN's security measures, including encryption and authentication protocols. However, there were a few suggestions for reinforcing security awareness and providing additional information about the VPN's security features.

To address these issues, ongoing efforts have been made to optimize the network infrastructure. The researchers perform a comparative study between Open VPN and Wireguard by evaluating the performance, security, and user satisfaction of both VPN solutions to determine their suitability for the network infrastructure needed by the institution. To assess performance, the researchers conducted tests measuring speed, latency, and throughput of OpenVPN and WireGuard connections. Statistical analysis, such as t-tests or ANOVA, was employed to compare their performance metrics and identify significant differences. In terms of security, the researchers assessed features, protocols, encryption strength, authentication mechanisms, and vulnerability assessment for both VPN solutions. Qualitative feedback from the MIS staff was considered to understand their perceptions of security. User satisfaction and usability surveys provided data on ease of use, performance, and overall satisfaction, with descriptive statistics summarizing the results. The features and functionality of

OpenVPN and WireGuard were compared, considering ease of configuration, compatibility, and support for various network protocols. Feedback from the MIS staff and network administrators was crucial in gauging experiences and preferences.