Virtual Private Network for Data and Information Communication Security:Testing on Zyxel USG 2200 Router

[1]Nurwahidah Jamal, [2]Ihsan, [3]Kety Lulu Agustin, [4]Andi Yasir Amsal, [5]Farida, [6]Mariatul Kiptiah
[12] Electrical Engineering Department, Balikpapan State Polytechnic, Balikpapan
[3] Business Department, Balikpapan State Polytechnic, Balikpapan
[45] Hospitality Department, Balikpapan State Polytechnic, Balikpapan
[6] Civil Engineering Department, Balikpapan State Polytechnic, Balikpapan
[1]nurwahidah.jamal@poltekba.ac.id, [2] ihsan@poltekba.ac.id

Abstract - This study evaluates the efficacy and security robustness of a Remote Terminal Unit (RTU) data connection protected by a Virtual Private Network (VPN) deployed on the Zyxel USG 2200 router. The aim is to evaluate the effects of IPsec and SSL VPN implementations on network performance, particularly in terms of latency and packet loss, and to assess system resilience against cyberattacks through penetration testing. An experimental methodology was employed, involving the configuration of IPsec/SSL on the Zyxel router and VA modem, conducting packet transmission tests, and performing a security evaluation using Kali Linux tools (Hydra, NMAP, and Metasploit). The performance test showed that the VPN connection was successfully established with packet transmission recorded between the source and destination. However, due to the second-level timestamp resolution, millisecond-level latency could not be accurately determined. The initial packet transmission test showed observed delay values of 2 ms for Packet 1 and 5 ms for Packet 2, with packet loss rates of 0.14% and 0.81%, signifying that the communication channel is exceptionally reliable and appropriate for real-time RTU applications. Port scanning revealed five open ports (21, 22, 53, 80, 443), but all penetration attempts were futile. Hydra faced failure due to a key-exchange mismatch; NMAP was unable to identify appropriate authentication keys despite numerous attempts, and Metasploit experienced connection issues during exploitation efforts. These findings validate that the established encryption and authentication systems offer sufficient defense against brute-force and fundamental exploitation threats. The research reveals that deploying IPsec and SSL VPN on the Zyxel USG 2200 enhances communication security while maintaining network performance. Future studies should incorporate long-term load testing and more sophisticated, multi-layered attack scenarios to achieve comprehensive security certification.

Keywords — IPsec, Cybersecurity, Zyxel USG 2200, Penetration Testing, Scada

I. Introduction

In the era of digitalized electric power systems, data communication between Remote Terminal Units (RTUs) and control centers has become a crucial component in ensuring the reliability of distribution network operations. RTUs transmit real-time field condition data to the Supervisory Control and Data Acquisition (SCADA) system, supporting the monitoring and control of electrical equipment. However, the connection of these systems via public networks and remote access increases risks to data and information security. Threats such as sniffing, unauthorized access, and man-in-the-middle attacks can result in operational disruptions, data manipulation, and even widespread failures of the distribution system [1]. This condition highlights the importance of research in developing an RTU communication security system that ensures data confidentiality, integrity, and availability (CIA Triad) through the application of Virtual Private Network technology [2]. The implementation of IPsec and SSL protocol-based VPN on industrial devices, such as the Zyxel USG 2200 Router, in the PLN UP2D Kaltimra environment is a strategic step to enhance critical data protection, strengthen the cyber resilience of the energy sector, and ensure safe and efficient electricity operations [3].

To address this issue, this study proposes implementing Virtual Private Network (VPN) technology, based on IPsec and SSL protocols, to secure data communications between the RTU and the control center. Through strong encryption and authentication mechanisms, VPNs can establish private communication channels that are protected from interception and cyberattacks [4]. The implementation of this system utilizes a Zyxel USG 2200 Router that supports industrial-grade security configurations, allowing its performance to be tested under real-world operational conditions at PLN UP2D Kaltimra. This research is expected to provide practical benefits in the form of increased reliability and security of RTU communications, as well as academic benefits in the form of a network security system model that can be used as a reference for the development of data communication security standards in the national electricity sector.

The primary challenge in implementing data communication between RTUs and control centers is the security and confidentiality of information transmitted over open networks. In practice, RTU data transmission often utilizes public IP-based connections without adequate encryption, making it vulnerable to eavesdropping, data forgery, and unauthorized access. This situation can be exploited by irresponsible parties to conduct man-in-the-middle attacks, data interception, and even command and control manipulation, potentially disrupting the stability of the electrical system [1]. Furthermore, the lack

of robust authentication and authorization mechanisms increases the risk of operational data leaks. Therefore, a data communication security mechanism is needed that can guarantee the integrity, authentication, and confidentiality of information across the RTU and the control center, ensuring the Safe and reliable operation of the electricity distribution system [5].

Several previous studies have examined the security of communication in Remote Terminal Unit (RTU) devices within SCADA systems and industrial networks. For example, in "Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis" [5], which conducted a vulnerability analysis and penetration testing on RTUs, it was demonstrated that RTU devices and their communication paths are highly vulnerable to interception, spoofing, and man-in-the-middle attacks in innovative grid environments.[5]. Meanwhile, a review study [6] on SCADA vulnerabilities and attacks noted that SCADA systems connected to public IP networks often still utilize legacy protocols without strong encryption, thereby opening up significant opportunities for cyberattacks against RTUs and other controller devices. [6]. Furthermore, the technical report "SCADA Security for Remote Site Operations and Remote Terminal Units" (2014) explains that one solution adopted in remote RTU operations is the use of Virtual Private Network (VPN) technology to strengthen communication channels, with authentication and encryption mechanisms to protect data that traverses public networks. [7]. However, these studies tend to focus on vulnerabilities and the need for security measures. Still, few evaluate network performance after implementing technologies like VPNs or comprehensively test them on real-world industrial devices (e.g., enterprise-class routers) in an RTU operational environment. Thus, a research gap remains regarding testing the effects of VPN implementation (including IPsec/SSL) on performance (delay, packet loss) and system resilience through real-world penetration tests in an industrial RTU context.

Table 1. Related works

No	Researcher & Year	Title	Research (summary)
1	Ghanem, K. et al. (2021)[8]	Bandwidth-Efficient Secure Auth & Encryption (IEC 60870-5-104)	There is a bandwidth trade-off between IPsec and TLS; overhead quantification for IEC-104 monitoring/control operations.
2	Ghanem, K. et al. (2022)[9]	Security vs Bandwidth: IPsec vs OpenVPN	IPsec increases protection but reduces bandwidth; OpenVPN is lighter but with certain compromises.
3	Bengs, F. (2023)[10]	Enhancement of Cyber Security in Substation Projects	IPsec server with certificate + username/password connects RTU & SCADA; emphasizing MFA and network segmentation.
4	Wai, E. et al. (2023)[11]	Seamless Industry 4.0 Integration: Multilayered Cybersecurity	Proposed layered framework to harden the SCADA environment; VPN/TLS is part of access control & network segmentation.
5	Setiawan, F. (2024)[12]	Implementasi SSL VPN (Secure Socket Layer Virtual Private Network) Pada Badan Bank Tanah	SSL VPN tunnel mode encrypts all client–gateway traffic (HTTPS); relevant as a secure access option.

A recent literature review suggests that research on Virtual Private Network (VPN)-based RTU (Remote Terminal Unit) data communication security is ongoing; however, several critical research gaps remain that need to be addressed. Studies such as [10] confirm the effectiveness of implementing IPsec and SSL VPNs in protecting data in SCADA and RTU systems; however, these tests are generally conducted in simulated environments, rather than on real-world distribution systems. Other studies by [9] focus on analyzing VPN performance and bandwidth efficiency, but have not yet linked these specifically to the characteristics of real-time RTU communication, which requires low latency and high availability.

This gap serves as the basis for the direction of this research development, specifically designing and testing a VPN-based RTU data communication security system (IPsec and SSL) directly in the operational environment of PLN UP2D Kaltimra, utilizing a Zyxel USG 2200 router. This research not only assesses the effectiveness of VPN, but also measures network performance (delay, packet loss, throughput) and resilience to cyber threats through penetration tests. The results are expected to provide an empirical contribution to enhancing the reliability of critical industrial communication systems and serve as a replicable model that can be implemented to strengthen cyber resilience in the national energy sector.

II. Research Method

This study uses an experimental approach to design and implement an RTU data communication security system with IPsec and SSL VPN protocols [13]. The methods used include the stages of system design, hardware and software implementation, performance testing, and penetration testing to evaluate the security and effectiveness of the implemented system [14].

A. Data and Information Security System Topology Design Scheme

The first step in network topology design is to design a network topology that connects the RTU device, the Zyxel USG2200 router, and the Master Station using two VPN protocols, IPsec and SSL[15] This system will secure the data communication path between the RTU and the Master Station [16]. Device and Protocol Selection: This study uses a Zyxel USG2200 router device and a VA GW2028 modem. The IPsec protocol will encrypt data sent between the RTU and the Master Station [17], [18], while SSL VPN will secure remote user access to the server that has been secured with IPsec, as in Figure 1 below.

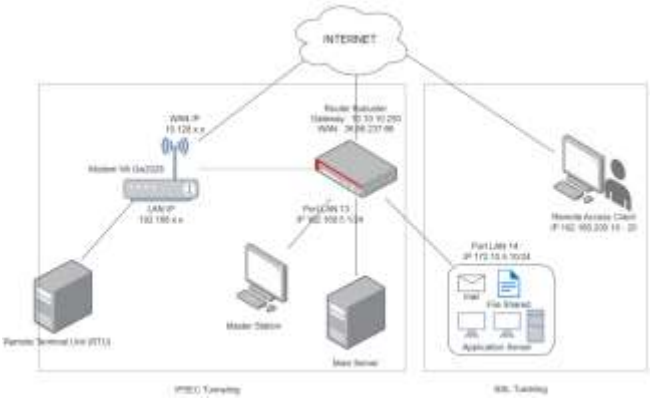

Figure 1. VPN-based Security System Design and Topology

Figure 1 above is illustrates two secure communication protocols: IPsec Tunnelling and SSL Tunnelling. Route 1 IPsec Tunnelling. The data route is Remote Terminal Unit (RTU) → Modem VA GW02 → Internet → Router Site → Main Server / Master Station. This route is used for secure site-to-site communication. IPsec is suitable for gateway-to-gateway connections because it provides data confidentiality, integrity, authentication, and protection against unauthorised access across public networks. Route 2 SSL Tunnelling The data route is Remote Access Client → Internet → Router Site → Application Server / File Share. This route is used for secure remote-user access to internal applications and files. SSL VPN is appropriate for individual remote access because it enables secure application-level communication through encrypted sessions. Thus, IPsec Tunnelling is primarily for site-to-site network security, while SSL Tunnelling is primarily for remote client access.

Meanwhile, to explain SSL VPN from the topology image, the User or Client who wants to do Remote must be connected to the Internet network in the Office, such as WIFI or LAN. Then, after connecting, the User will get a private IP provided by the Router between 192.168.200.10 and 192.168.200.20. To access the Web or Server that has been permitted, the User can use the IP 10.10.10.250 or 172.10.5.10 to enter the Zyxel Web SSL VPN [19]. The User enters the Username and Password that has been registered [20]. After entering the Username and Password, the User will be directed to a Web Page that contains several Web links that have been permitted, such as Web Email, File Shared, or Applications on the Server [21], [22].

The following is a Flowchart of the VPN-based RTU (Remote Terminal Unit) Data Security System, which can be seen in Figure 2 below.

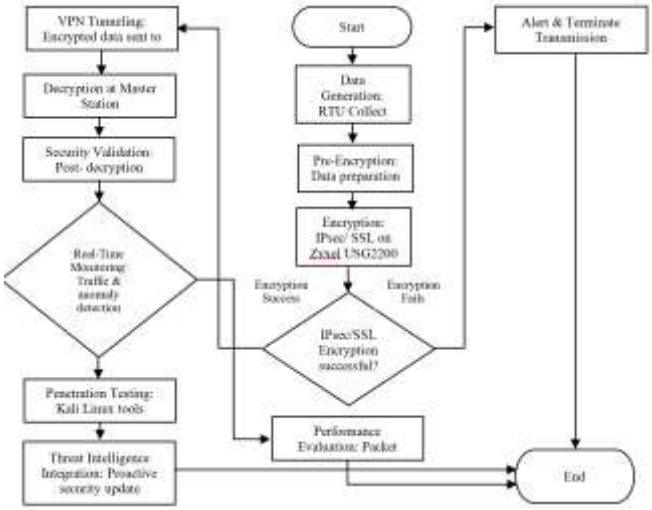

Figure 2. RTU Data Security System Flowchart

B. Creating IPsec and SSL VPN on Zyxel Router and VA GW2028 Modem

In the process of creating a security system using the Internet Protocol Security (IPsec) VPN method in the Zyxel USG2200 Router and VA GW2028 Modem [23], several configuration stages must be carried out to ensure that the security system is successfully created and can be used efficiently [24]. These stages involve various technical steps that must be followed carefully to optimize network security and performance [25].

The first thing to do is to connect the laptop to the router using a LAN cable connected to the Ethernet LAN port of the Zyxel router. Then, set the laptop IP to Obtain an IP address Automatically so that the laptop can immediately get the router's default IP. After configuring the Ethernet port, the next step is to configure the VPN Gateway. After that, the address configuration is done to register a single IP address or range of IP addresses on the router by entering the name, IP, netmask, and address type. After creating the VPN Gateway and Address Object, the next step is to create and configure the VPN Connection Tunnel. Next, create and configure IPsec on the Zyxel Router. The next thing to do is to create and configure IPsec on the VA GW2028 Modem, followed by seeing the results of the VPN that has been created working, before configuring the Secure Socket Layer (SSL) VPN on the Zyxel Router. The router must be connected to the Internet in the office. To connect the router, several configuration steps are required. In Full Tunnel Mode on Socket Layer (SSL) VPN on the Zyxel Router, a virtual connection is created for remote users with the same private IP address subnet as the local network. The last step is testing the SSL VPN and monitoring the results [26].

C. Determining attributes for Penetration Testing and Final Analysis

After successfully creating, configuring, and implementing a VPN-based security system with two methods, namely IPsec and SSL [27]. The last step taken by the researcher was to conduct Penetration Testing and Final Analysis of the security system created using software and hardware such as Kali Linux, Hydra, NMAP, Metasploit, and System Log Modem VA GW2028 [28].

The purpose of conducting this Penetration Testing and Final Analysis is to determine several parameters, such as Delay, Packet Loss, Port Scanning, and vulnerabilities, in VPN IPSec Tunnel Connections. In this test, Connections were created between the Zyxel Router and the VA Modem in the field. The following explains the results of the Testing and Analysis carried out [29].

1. Delay

The amount of time it takes for data to move from one location to another is known as the delay. Distance, traffic congestion, and the quality of the distribution network may all have an impact on delay [30]. The following is Table 1 of Delay Value Parameters.

Table 2. Parameter Delay

Delay Category	Total Delay	Index
Very Good	< 150 ms	4
Good	150 to 300 ms	3
Average	300 to 450 ms	2
Bad	> 450 ms	1

To calculate the average delay, use the formula:

$$Delay_i = T_{received,i} - T_{sent,i} \quad (1)$$

$$AverageDelay = \frac{\sum_{i=1}^{n}(T_{received,i} - T_{sent,i})}{n} \quad (2)$$

2. Packet Loss

The criterion to show the total number of packets lost in delivery is described by the parameter "Packet Loss," which might be brought on by network congestion and conflicts [31]. The following is a table of packet loss value parameters.

Table 3. Parameter Packet Lost

Delay Category	Total Delay	Index
Very Good	< 0%	4
Good	0 s.d 3 %	3
Average	3 s.d 15 %	2
Bad	> 25 %	1

To calculate Packet Loss, use the formula:

$$\text{Packet Loss} = \frac{Packet\ sent - \text{Package Received}}{Packet\ sent}\ x\ 100\% \quad (3)$$

3. Penetration Testing

The technique of mimicking a cyberattack to find weaknesses in a system or network is known as penetration testing. It involves two main steps: scanning the device to identify services or ports running on it and finding system vulnerabilities. This process uses open-source tools such as Kali Linux, Hydra, and NMAP to detect security holes. In addition , brute force is used as an attack method by systematically trying various combinations of passwords or encryption keys until finding the right one. This method tests the system's strength against attacks by trying password combinations in bulk [32].

III. Results and Discusion

Results

A. Zyxel Router and VA Modem Connection Testing

Below, Figure 3 is a screenshot of the results of testing the delivery of packets 1 and 2 to calculate the delay value and packet loss value.

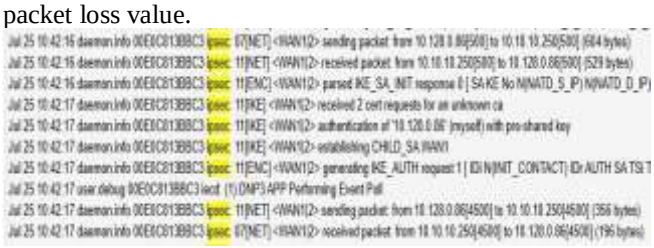

Figure 3. Packet Delivery Data

Based on the test results above, it can be presented in Table 4. Data packet delivery testing is as follows:

Table 4. Packet Delivery Testing

Packet	Source IP	Destination IP	Sent Time	Received Time	Delay
1	10.128.0.86	10.10.10.250	10:42:16.123	10:42:16.125	2 ms
2	10.128.0.86	10.10.10.250	10:42:17.210	10:42:17.215	5 ms

Based on the results of packet delivery testing in Table 4 above, Table 5 below shows the results of delay and packet loss testing.

Table 5. Delay and Packet Loss Test Results

Testing	Calculation of test results	Delay Category	Index
Delay 1	10:42:16.125 − 10:42:16.123 = 0.002 s / 2 ms	Very Good	4
Delay 2	10:42:17.215 − 10:42:17.210 = 0.005 s / 5 ms	Very Good	4
Packet Loss 1	$\frac{604-529}{529} = 100\% = 0{,}14\%$	Good	3
Packet Loss 1	$\frac{356-196}{196} = 100\% = 0{,}81\%$	Good	3

The delay was calculated based on the difference between receiving time and sending time. The delay was calculated based on the difference between receiving time and sending time using millisecond-level timestamps. Based on Table 4, Packet 1 produced a delay of 2 ms, while Packet 2 produced a delay of 5 ms. However, because only two packets were tested, these results should be interpreted as preliminary observations rather than a comprehensive performance evaluation. In the delay category, the value is in the excellent range because it is less than 150 ms, with an index of 4. Based on the limited packet transmission test, the connection between the Zyxel router and the VA modem was successfully established and showed low observed delay and packet loss values. However, because only two packets were tested, these results should be

interpreted as preliminary observations rather than a comprehensive performance evaluation. Overall, this excellent delay value provides an optimal user experience regarding speed and responsiveness.

Meanwhile, in the packet loss parameter, packets 1 and 2 also show “good” results at index value 3, with a few packets lost. With results of 0.14% and 0.81% respectively.

B. Security System Testing

Data and information security testing uses penetration testing, scanning devices, and brute force techniques to identify potential vulnerabilities. Using Hydra, NMAP, and Metasploit, this test assesses how well the system can be defended against external threats. Hydra will identify vulnerabilities in the login system. NMAP is used for network mapping and vulnerability detection, while Metasploit is used for the exploitation and testing of security holes found. Below in Figure 4 are the results of the Port Scanning test using Kali Linux.

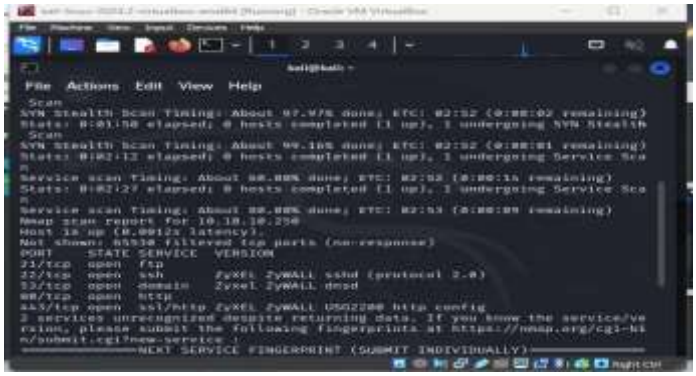

Figure 4. Port Successfully Scanned

Judging from the Scanning results, there are five open ports, namely 21,22,53,80 and 443. The presence of Port 21 indicates that the FTP service was open during the scanning process. This condition should be considered a potential security risk because FTP is commonly associated with unencrypted file transfer and may expose authentication credentials or data if not properly restricted. In this implementation, the FTP service should be enabled only when operationally required, for example, for device management or internal file transfer. If it is not required, Port 21 should be disabled. If FTP access is necessary, it should be restricted to trusted internal IP addresses or VPN-only access, monitored through system logs, and preferably replaced with a more secure alternative such as SFTP or FTPS. On ports 22 and 53, there are Zyxel ZyWALL sshd and dnsd versions, where sshd is a program that runs in the background on the server to allow incoming SSH connections. At the same time, DNSD is a program that runs in the background on the server to enable communication via DNS. After knowing which ports are open, the next step is to do Brute Force by creating a Wordlist.txt file. The port to be tested is port 22. The following can be seen in Figure 5 Test results with Hydra, Figure 6 NMAP test results, and Figure 7 Metasploit test results.

Figure 5. Hydra Test Results

The test results in the image above show that the penetration carried out using Hydra was unsuccessful due to the incompatibility of the key exchange algorithm between the server and Hydra.

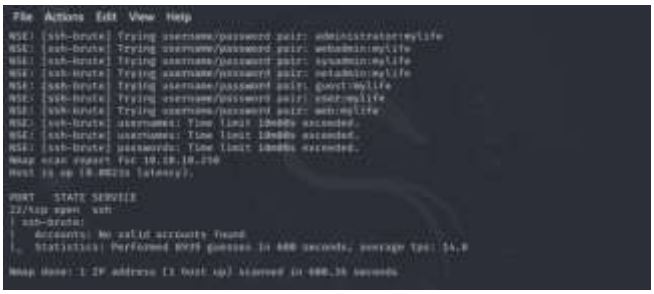

Figure 6: NMAP Testing Results

The test results in the image above show that the penetration carried out using NMAP was unsuccessful because within 600 seconds, NMAP conducted 8939 attempts, and the results did not find a single correct or matching key.

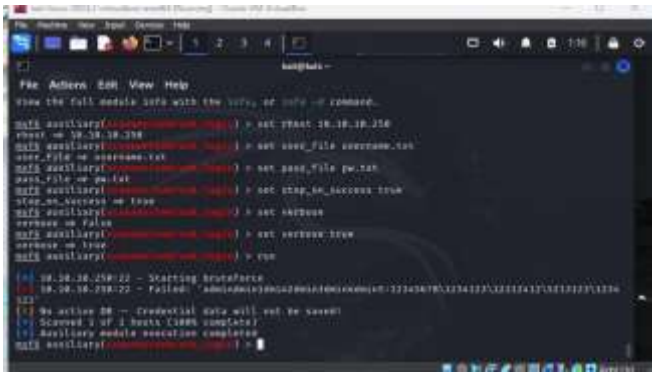

Figure 7: Metasploit Test Results

The test results showed that the penetration carried out using Metasploit was unsuccessful because of a Failed Connection when trying to use the owned key. This was caused by none of the keys being suitable or correct.

Discussion

Based on the packet transmission test, the connection between the Zyxel router and the VA modem was successfully established. The timestamp-based calculation showed observed delay values of 2 ms for Packet 1 and 5 ms for Packet 2, respectively and very low packet loss (0.14% and 0.81%), so as

not to disrupt real-time service performance and network throughput. These values are far below the critical threshold (150 ms for delay) and indicate adequate responsiveness and stability of the communication path for RTU operational applications. In terms of security, the port scan results identified five open ports, namely 21, 22, 53, 80, and 443, standard configurations for FTP, SSH, DNS, HTTP, and HTTPS services, but penetration testing using Hydra, NMAP, and Metasploit failed to penetrate the system, the Hydra attempt failed due to a mismatch in the key exchange algorithm, NMAP did not find a matching key despite conducting thousands of attempts within 600 seconds, and Metasploit experienced a connection failure when attempting exploitation. The results of this study indicate that the authentication and encryption mechanisms on the devices are pretty robust, and the service configuration has limited the possibility of attempts using brute-force methods or simple exploits. However, although the test results show excellent network quality and high security resilience, attention is still needed for ongoing further research, such as port and log monitoring, firmware/patch updates, traffic anomaly monitoring, implementation of access policies, such as SSH restrictions, DNS hardening, and regular testing with more sophisticated scenarios to ensure there are no gaps that the current test has missed. Overall, the test can be concluded that the tested infrastructure can support communication needs with minimal latency and packet loss, and has effective basic defences against external attacks. However, security and performance must be maintained proactively. A limitation of this performance evaluation is the small number of tested packets. Since the delay and packet loss measurements were based on only two packet samples, the results cannot be generalized to represent overall VPN performance under different traffic loads, time periods, or network congestion conditions. Therefore, the findings should be considered preliminary. Future testing should involve a larger number of packets, repeated measurement sessions, different packet sizes, and longer observation periods to obtain statistically stronger and more reliable performance results.

IV. Conslusion

1. The VPN connection between the Zyxel router and the VA modem was successfully established. The initial packet transmission test showed low observed delay values, namely 2 ms for Packet 1 and 5 ms for Packet 2, with packet loss values of 0.14% and 0.81%, respectively. However, because the performance test was conducted using only two packet samples, these findings should be interpreted as preliminary results rather than definitive evidence of overall VPN performance.
2. The communication channel showed promising initial performance for supporting RTU data transmission. Nevertheless, further testing with larger packet samples, different packet sizes, various traffic loads, and longer observation periods is required before drawing a strong conclusion regarding its suitability for operational RTU applications.
3. From a security perspective, the port scanning process identified five open ports, namely 21, 22, 53, 80, and 443. Although penetration attempts using Hydra, NMAP, and Metasploit were unsuccessful, the open Port 21 for FTP should be further reviewed because FTP may pose security risks if it is not operationally required or properly restricted.
4. The unsuccessful penetration attempts indicate that the authentication and encryption mechanisms implemented in the device provide initial resistance against brute-force attacks and basic exploitation attempts. However, these results do not fully represent the overall security posture because the attack scenarios were still limited.
5. For future research, it is recommended to expand the number and variety of tested packets, perform repeated performance measurements, conduct long-term load testing, and implement more comprehensive penetration testing scenarios, including layered attacks and advanced threat simulations. In addition, mitigation strategies such as FTP restriction or replacement with SFTP/FTPS, SSH hardening, port access control, firmware updates, VPN encryption review, continuous logging, and regular security audits should be applied to improve operational network resilience.

V. References

[1] C. I. Toma, M. Popescu, and I. C. Popa, “Application of SCADA System in an Electrical Substation and Remote Terminal Unit Parametrization,” *2023 International Conference on Electromechanical and Energy Systems, SIELMEN 2023 - Proceedings*, 2023, doi: 10.1109/SIELMEN59038.2023.10290773.

[2] D. Zela, B. Mema, and K. Zela, “VPN VIRTUAL PRIVATE NETWORK APPLICATIONS IN DATA PREDICTION,” *Smart Cities and Regional Development (SCRD) Preprints*, vol. 1, no. 1, Dec. 2024, Accessed: May 28, 2025. [Online]. Available: https://www.scrd.eu/index.php/scrd-pp/article/view/576

[3] H. Gunleifsen, T. Kemmerich, and V. Gkioulos, “Dynamic setup of IPsec VPNs in service function chaining,” *Computer Networks*, vol. 160, pp. 77–91, Sep. 2019, doi: 10.1016/J.COMNET.2019.05.015.

[4] V. G, D. M S, M. Hashmi, J. R. K, and K. B V, “Robust Technique for Detecting and Blocking of VPN over Networks,” in *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, IEEE, Apr. 2024, pp. 1–5. doi: 10.1109/ICONSTEM60960.2024.10568824.

[5] E. Rencelj Ling, J. E. Urrea Cabus, I. Butun, R. Lagerström, and J. Olegard, “Securing Communication and Identifying Threats in RTUs: A Vulnerability

Analysis," *ACM International Conference Proceeding Series*, Aug. 2022, doi: 10.1145/3538969.3544483.
[6] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues," *Comput. Secur.*, vol. 125, p. 103028, Feb. 2023, doi: 10.1016/J.COSE.2022.103028.
[7] K. L. Finnan, "SCADA Security for Remote Site Operations and Remote Terminal Units."
[8] *The 2021 International Conference on Smart Applications, Communications and Networking (SmartNets 2021) : October 22-23, 2021 - Glasgow, UK (virtual)*. [IEEE], 2021.
[9] K. Ghanem, S. Ugwuanyi, J. Hansawangkit, R. McPherson, R. Khan, and J. Irvine, "Security vs Bandwidth: Performance Analysis between IPsec and OpenVPN in Smart Grid," in *2022 International Symposium on Networks, Computers and Communications, ISNCC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ISNCC55209.2022.9851717.
[10] F. Bengs, "Enhancement of Cyber Security in Substation Projects."
[11] E. ; Wai *et al.*, "Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS," *Applied Sciences 2023, Vol. 13, Page 12008*, vol. 13, no. 21, p. 12008, Nov. 2023, doi: 10.3390/APP132112008.
[12] F. Setiawan, F. Siddik Chaniago, and A. Wibowo, "Implementasi SSL VPN (Secure Socket Layer Virtual Private Network) Pada Badan Bank Tanah," *Syntax Idea*, vol. 6, no. 6, pp. 2505–2516, Jun. 2024, doi: 10.46799/SYNTAX-IDEA.V6I6.3438.
[13] J. Y. Chen, K. C. Tai, and G. C. Chen, "Application of Programmable Logic Controller to Build-up an Intelligent Industry 4.0 Platform," *Procedia CIRP*, vol. 63, pp. 150–155, Jan. 2017, doi: 10.1016/J.PROCIR.2017.03.116.
[14] O. Purchina, A. Poluyan, and D. Fugarov, "Securing an Information System via the SSL Protocol," *International Journal of Safety and Security Engineering*, vol. 12, no. 5, p. 563, Oct. 2022, doi: 10.18280/IJSSE.120503.
[15] J. Antonio, P. Espín, R. Marín-López, G. López-Millán, F. Pereñíguez-García, and O. Canovas, "SDN-based automated rekey of IPsec security associations: Design and practical validations," *Elsevier*, 2023, Accessed: May 27, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S138912862300350X
[16] S. Amaldeep and S. S.-2023 11th I. Symposium, "Cross Protocol Attack on IPSec-based VPN," *ieeexplore.ieee.org*, 2023, Accessed: May 27, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10131787/
[17] by sandip patel, G. bhatt, and J. Graham, "Data Security at Cloud Storage using PGP in conjunction with IPsec VPN," *dl.acm.org*, vol. 52, no. 7, p. 139, Jul. 2023, doi: 10.1145/1538788.1538820.
[18] J. Kumar, M. Kumar, D. K. Pandey, and R. Raj, "Encryption and authentication of data using the IPSEC protocol," *Springer*, vol. 673, pp. 855–862, 2021, doi: 10.1007/978-981-15-5546-6_71.
[19] P. Gunda and S. Datta Voleti, "Performance evaluation of wireguard in kubernetes cluster." [Online]. Available: www.bth.se
[20] S. Murthy Pedapudi and N. Vadlamani, "A Comprehensive Network Security Management in Virtual Private Network Environment," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, IEEE, May 2022, pp. 1362–1367. doi: 10.1109/ICAAIC53929.2022.9793196.
[21] A. Yeboah-Ofori and A. Ganiyu, "Big Data Security Using RSA Algorithms in A VPN Domain," *International Conference on Artificial Intelligence, Computer, Data Sciences, and Applications, ACDSA 2024*, 2024, doi: 10.1109/ACDSA59508.2024.10467364.
[22] S. Biradar, P. S. Parsewar, N. Mishra, A. A. Galakatu, and S. S. Gandewar, "A Survey on: Design, Implementation, and Evaluation of a Secure and Anonymous Communication Platform Utilizing the TOR Network for Enhanced Privacy and Data Protection," *2024 IEEE 4th International Conference on ICT in Business Industry and Government, ICTBIG 2024*, 2024, doi: 10.1109/ICTBIG64922.2024.10911520.
[23] N. Q. Tran, K. D. L. Nguyen, and C. D. T. Thai, "Implementation and Evaluation of IPSec in an NFV-Based Network," *Lecture Notes in Networks and Systems*, vol. 967 LNNS, pp. 53–65, 2024, doi: 10.1007/978-981-97-2053-8_4.
[24] S. * Balachandran, Dominic, and J. Sivankalai, "A Comparative Analysis of VPN and Proxy Protocols in Library Network Management," *Library Progress International*, vol. 44, no. 3, pp. 17006–17020, Oct. 2024, doi: 10.48165/BAPAS.2024.44.2.1.
[25] Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols," *Comput. Secur.*, vol. 142, p. 103883, Jul. 2024, doi: 10.1016/J.COSE.2024.103883.
[26] Md. Z. Islam, M. A. Rahman Khan, and Md. I. Hossain, "Analysis the importance of VPN for Creating a Safe Connection Over the World of Internet," *IJARCCE*, vol. 10, no. 10, Oct. 2021, doi: 10.17148/ijarcce.2021.101017.

[27] L. Firdaouss, B. Ayoub, B. Manal, and Y. Ikrame, "Automated VPN configuration using DevOps," *Procedia Comput. Sci.*, vol. 198, pp. 632–637, Jan. 2022, doi: 10.1016/J.PROCS.2021.12.298.

[28] J. A. Parra-Espín, R. Marín-López, G. López-Millán, F. Pereñíguez-García, and O. Canovas, "SDN-based automated rekey of IPsec security associations: Design and practical validations," *Computer Networks*, vol. 233, p. 109905, Sep. 2023, doi: 10.1016/J.COMNET.2023.109905.

[29] J. Harmening, "Virtual Private Networks," *Computer and Information Security Handbook, Fourth Edition: Volumes 1-2*, vol. 2, pp. 979–992, Jan. 2025, doi: 10.1016/B978-0-443-13223-0.00059-X.

[30] G. López-Millán, R. Marín-López, F. Pereñíguez-García, O. Canovas, and J. A. Parra Espín, "Analysis and practical validation of a standard SDN-based framework for IPsec management," *Comput. Stand. Interfaces*, vol. 83, p. 103665, Jan. 2023, doi: 10.1016/J.CSI.2022.103665.

[31] O. Abolade *et al.*, "Overhead effects of data encryption on TCP throughput across IPSEC secured network," *Sci. Afr.*, vol. 13, p. e00855, Sep. 2021, doi: 10.1016/J.SCIAF.2021.E00855.

[32] D. Zielinski and H. A. Kholidy, "An Analysis of Honeypots and their Impact as a Cyber Deception Tactic," Dec. 2022, Accessed: Nov. 26, 2025. [Online]. Available: https://arxiv.org/pdf/2301.00045