Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

Security and Performance Evaluation of PPTP-Based VPN with AES Encryption in Enterprise Network Environments

Ahmad Heryanto*[1], Deris Stiawan[2], Berby Febriana Audrey[3], Adi Hermansyah[4], Nurul Afifah[5], Iman Saladin B. Azhar[6], Mohd Yazid Bin Idris[7], Rahmat Budiarto[8]

[1,2,3,4,5,6]Department of Computer Science, Universitas Sriwijaya, Indonesia
[7]Department of Computer Science, University of Technology Malaysia
[8]Faculty of Computer Science, Albaha University, Saudi Arabia

Email: [1]hery@unsri.ac.id

Received : Jun 3, 2025; Revised : Jul 16, 2025; Accepted : Jul 19, 2025; Published : Aug 19, 2025

Abstract

In the context of the current digital era, Virtual Private Networks (VPNs) serve a critical function in ensuring the confidentiality and integrity of data transmitted across public networks, particularly within corporate environments. This study presents a comprehensive analysis of VPN security and performance, with a specific focus on the Point-to-Point Tunneling Protocol (PPTP) and the implementation of encryption algorithms such as AES-128 and AES-256. Despite the widespread adoption of PPTP due to its simplicity and broad compatibility, it exhibits significant security vulnerabilities, primarily stemming from its reliance on the outdated RC4-based Microsoft Point-to-Point Encryption (MPPE) and the susceptible MS-CHAP authentication protocol, which is highly vulnerable to brute-force and dictionary attacks. Empirical findings indicate that, although AES-128 and AES-256 introduce minor performance trade-offs compared to unencrypted configurations, AES-256 demonstrates markedly enhanced security, achieving a 98.9% authentication success rate and a threat detection time of 122 milliseconds. Nevertheless, increased user load adversely impacts network performance, with throughput declining from 95 Mbps to 40 Mbps as the user count rises from 5 to 50, accompanied by elevated latency and packet loss. Comparative analysis across three encryption scenarios AES-128, AES-256, and MPPE-PPTP reveals a consistent degradation in network performance as user load increases, with AES-256 offering the strongest security at the cost of slightly reduced throughput and increased latency under high-load conditions. MPPE-PPTP, while providing better throughput, lacks adequate security, making it unsuitable for high-risk environments. Based on these observations, this study recommends the implementation of AES-256 encryption in enterprise networks requiring high security, supported by continuous performance monitoring and strategic capacity planning. Furthermore, the adoption of a secure site-to-site VPN architecture is proposed to facilitate reliable and secure communication between geographically distributed office locations.

Keywords : *AES-256, Enterprise, Network Performance, PPTP, VPN*

1. INTRODUCTION

As a fundamental technology, the VPN is critical for upholding data communication integrity within today's digital framework. As the utilization of the internet and public networks continues to escalate, the demand for robust mechanisms that can effectively shield data against eavesdropping and unauthorized access has become increasingly imperative. VPN facilitates users in establishing secure and encrypted connections across public networks, thereby ensuring that the data being transmitted retains its confidentiality[1], [2]. The PPTP, or Point-to-Point Tunneling Protocol, has remarkably

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

increased its adoption across various VPN protocols since it was initially launched. Developed in the 1990s, PPTP garnered preference due to its straightforward implementation and extensive compatibility with a variety of operating systems. This method functions by wrapping Point-to-Point Protocol (PPP) data packets inside IP packets, thereby facilitating safe data communication across public networks[3].

This specialized protocol is crafted to fulfill diverse authentication requirements, including both variants of Microsoft Challenge Handshake Authentication Protocol (MS-CHAP v1 and v2), while it utilizes Microsoft Point-to-Point Encryption (MPPE) that applies the RC4 encryption algorithm to assure the privacy of data exchanged during the communication cycle. PPTP operates a control channel fundamentally connected to TCP, while simultaneously deploying a data channel utilizing GRE to achieve optimal data packet delivery across multiple networks[4]. However, despite these features and functionalities, it is crucial to acknowledge that this encryption mechanism exhibits significant limitations regarding its security strength, especially when it is juxtaposed with the more advanced and robust security measures offered by contemporary Virtual Private Network (VPN) protocols that are currently in widespread use.

The advancement of computer networks in contemporary society is undergoing a remarkably swift progression, characterized by the emergence of increasingly intricate and varied infrastructures that cater to a multitude of user needs and technological demands[5], [6]. Organizations today are tasked with the intricate management of networks that seamlessly integrate not only localized data centers but also an array of cloud services and mobile devices, which are dispersed across a diverse range of geographical locations and operational environments[7], [8]. This certain scenario demands the utilization of Virtual Private Network (VPN) protocols that not only furnish robust security measures to defend sensitive data but also display an impressive capacity for flexibility and adaptability when responding to the dynamic shifts that may arise in network architectures, all while complying with strict and thorough security guidelines that are essential to uphold data integrity and confidentiality[9].

The simplicity of configuration and extensive compatibility serve as the primary justifications for the ongoing utilization of PPTP. Consequently, it is imperative to undertake a comprehensive security assessment of the employment of PPTP within the framework of contemporary networks in order to ascertain and proficiently address prevailing vulnerabilities. The repercussions of PPTP weaknesses on the security of corporate networks can be profoundly consequential. Risks such as unauthorized intrusion, data exfiltration, and breaches of regulatory compliance may materialize if this protocol is implemented without supplementary protective measures. In settings that oversee sensitive information, including financial data, personal customer information, and proprietary trade secrets, the ramifications of an assault on a PPTP-based VPN can be both financially and reputationally catastrophic[10], [11].

Therefore, the execution of a comprehensive security analysis of VPNs utilizing the PPTP protocol is of paramount importance[12]. This investigation is designed to uncover vulnerabilities, comprehend potential methodologies of attack, and assess the efficacy of current security measures. The findings derived from this analysis will form a foundational basis for identifying suitable mitigation strategies and for formulating enhanced network security policies. Moreover, entities that continue to employ PPTP must adopt best practices in securing their VPNs, such as the implementation of robust passwords, the activation of multi-factor authentication, the continuous monitoring of network traffic, and the application of effective network segmentation. These initiatives should be bolstered by regular security audits and timely software updates to mitigate potential risks effectively.

This study aims to provide a comprehensive analysis of the security and performance characteristics of PPTP-based VPNs within modern network infrastructures. By scrutinizing various dimensions, including protocol mechanisms, vulnerabilities, ramifications, and mitigation tactics, this research aspires to make a significant contribution, thereby aiding organizations in making informed strategic decisions regarding the adoption of secure and effective VPN technologies. Unlike prior studies

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

that typically focus on either security or performance in isolation[13]–[15], this study integrates both aspects to provide a more holistic understanding of VPN implementation challenges. Furthermore, this research addresses the limited empirical benchmarking of AES-128 and AES-256 encryption within PPTP-based VPNs, particularly under simulated enterprise traffic conditions, thereby filling a critical gap in the existing body of knowledge.

2. METHOD

The proposed methodology presents a comprehensive framework for evaluating the security and performance of VPN implementations based on the Point-to-Point Tunneling Protocol (PPTP), utilizing Advanced Encryption Standard (AES) algorithms specifically AES 128 and AES 256 within enterprise network environments.

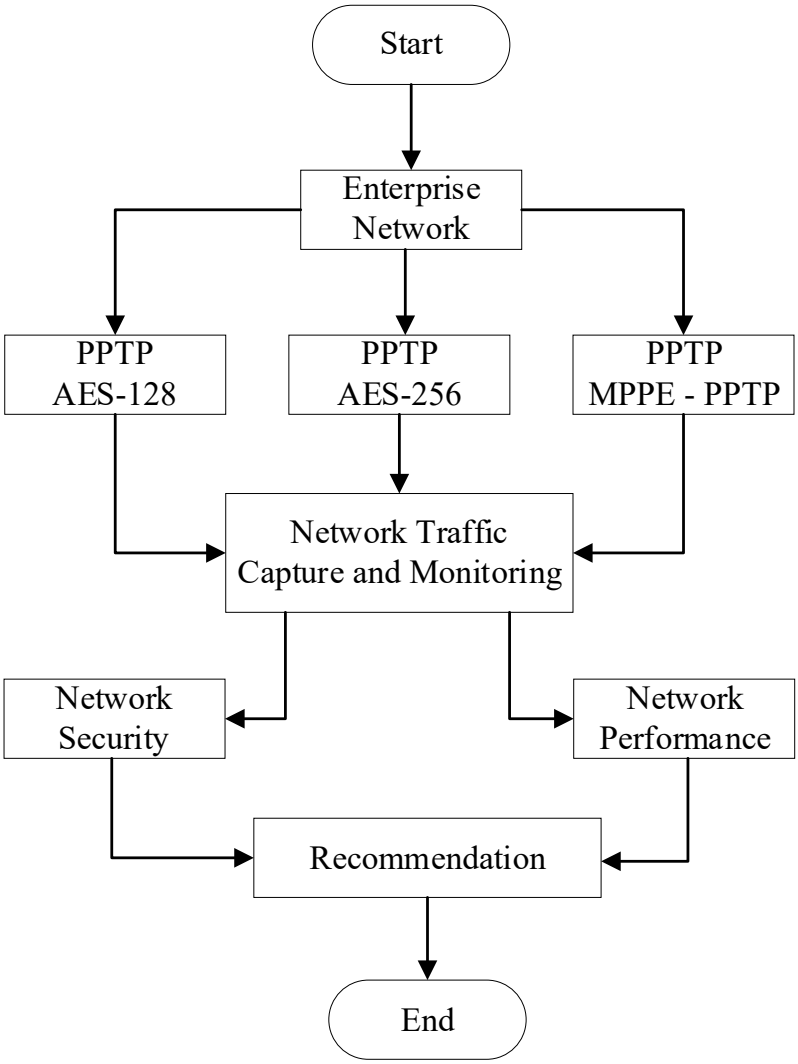

Figure 1. Proposed Research Methods

As illustrated in Figure 1, this approach follows a systematic sequence of key stages, including data preprocessing, system development, encryption testing, and network performance evaluation. The preprocessing phase encompasses data preparation activities such as the segmentation of test scenarios, configuration of network parameters, simulation of user loads, and implementation of encryption

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

protocols. During the system development stage, an experimental approach is employed to examine various network traffic scenarios in order to assess the impact of AES encryption on PPTP protocol performance. The experimental setup utilizes MikroTik RB750 and RB450G devices operating on RouterOS version 6.49, with a configured bandwidth capacity of 100 Mbps. Network performance is assessed using three principal metrics, each calculated using a corresponding equation: Throughput (Equation 1), which quantifies the rate of data transmission; Latency (Equation 2), which measures the delay in data transfer; and Packet Loss (Equation 3), which determines the proportion of data packets lost during transmission. In addition to performance evaluation, the testing model is designed to identify PPTP security vulnerabilities, particularly against brute-force and dictionary-based attacks, while also comparing the relative effectiveness of AES-128 and AES-256 encryption schemes. The final phase involves classifying security risk levels and conducting a comprehensive analysis of network performance based on the observed metrics, thereby offering a detailed assessment of PPTP-based VPN deployment within contemporary enterprise networks.

$$\text{Throughput} = \left(\frac{\text{Total Data Received (bits)}}{\text{Total Time (seconds)}}\right) \text{x } 10^8 \quad (1)$$

$$\text{Latency} = \left(\frac{\text{Total Round−Trip Time}}{\text{Number of Packets}}\right) \text{x } 1000 \quad (2)$$

$$\text{Packet Loss} = \left(\frac{\text{Packets Sent−Packets Received}}{\text{Packets Sent}}\right) \text{x } 100 \quad (3)$$

2.1. Site to Site VPN

The deployment of a Virtual Private Network (VPN) through the Point-to-Point Tunneling Protocol (PPTP) in a Site-to-Site layout aspires to fuse two or more geographically apart local networks into a cohesive network that is acknowledged as dwelling within a singular physical environment. In this scenario, main office and branch office are enabled to communicate and transfer data securely via the public internet[2], [16]. Figure 2 delineates the network topology of an organization comprising two operational sites: Main Office and the Branch Office. These two offices are interconnected through the public Internet, thereby facilitating connection and communication despite their separation by varying geographic locales. In main office, there exists a local network designated with the IP address range 192.168.10.0/24. This network is comprised of multiple computers that are linked to a router. The router operates as a conduit linking the internal local network to the vast expanse of the internet. The router stationed at main office possesses a public IP address of 103.241.x.x, which permits the local network within main office to engage with and communicate across external networks, including the branch office[17].

Conversely, on the branch office side, a distinct local network is established with the IP address range 192.168.100.0/24. Analogous to main office, this network is similarly composed of several computers connected to a router. This router is assigned a public IP address of 103.208.137.x, functioning as the conduit between the branch's local network and the internet. This configuration enables the computers in the branch office to reach the internet and communicate with main office seamlessly. Each office operates its own local area network (LAN), indicating that their IP addressing is private and exclusively utilized for internal communication within each respective site. In its essential capacity, the router controls data movement, ensuring smooth traffic within the local network while also directing the data exchange to and from the internet.

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

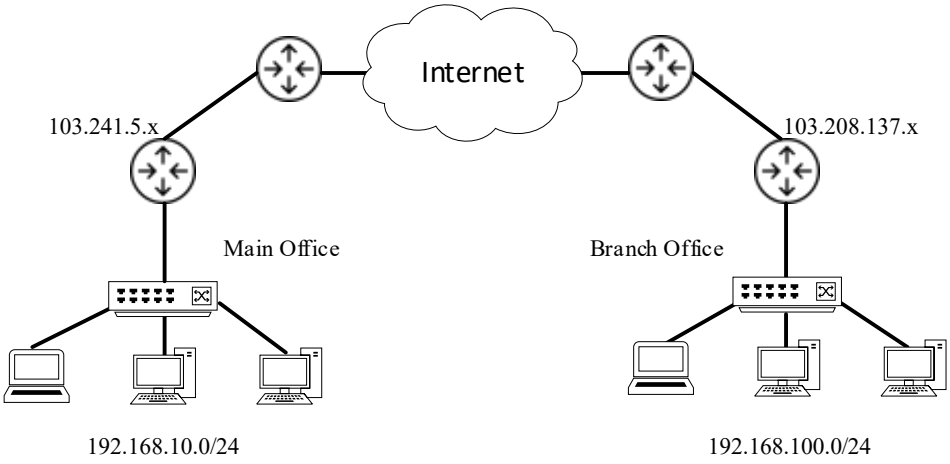

Figure 2. Enterprise Networks

Nevertheless, this network topology is also characterized by several constraints that may present challenges to the operational efficacy of the organization. A primary concern is that the local networks situated in both offices are unable to engage in direct communication with one another, due to the utilization of private IP addresses that are only recognized within their respective local contexts. In the absence of specific configurations such as address translation or supplementary devices computers located in main office are incapable of directly accessing devices within the branch office, and conversely. This predicament can obstruct collaboration, data exchange, or access to internal servers and services between the offices, which ideally ought to function seamlessly and efficiently. These constraints necessitate an additional solution to facilitate unimpeded communication between the local networks at both sites.

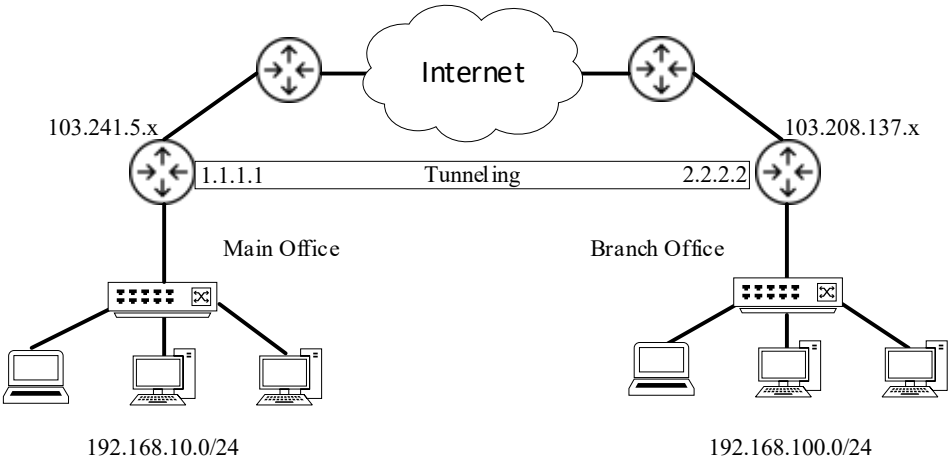

Figure 3. Site-to-Site VPN for Enterprise Networks

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

In the depicted network topology figure 3., the linkage between main office and branch office is facilitated via the internet utilizing a site-to-site Virtual Private Network (VPN) methodology incorporating tunneling. In this arrangement, main office serves as the VPN server endowed with a public IP address of 103.241.5.x, whereas branch office operates as the VPN client possessing a public IP address of 103.208.137.x. The VPN linkage is established as a virtual tunnel, with each endpoint designated a tunnel IP: 1.1.1.1 for main office and 2.2.2.2 for branch office. After establishing the VPN connection successfully and activating the tunnel, routing methods, either static or dynamic, are put into place between the two local networks. The primary office is affiliated with a local network segment of 192.168.10.0/24, while the branch office is prepared to engage 192.168.100.0/24. Through this routing configuration, the router at main office is directed to transmit traffic intended for 192.168.100.0/24 through the tunnel to IP 2.2.2.2. In contrast, the router at branch office is tasked with routing all traffic aimed at 192.168.10.0/24 through tunnel IP 1.1.1.1. With this configuration, devices located at both sites are enabled to communicate directly as though they resided on a unified network. For instance, a computer stationed at main office can access a file server or printer located at branch office, and reciprocally. This configuration enhances collaboration among teams situated in disparate locations without necessitating substantial alterations to the network infrastructure of either office. This routing architecture is fundamental to site-to-site connectivity and represents one of the primary advantages of employing a site-to-site VPN with tunneling.

2.2. Mechanisms of Virtual Private Network Operation

The initiation of the development process commences with a comprehensive needs analysis of the organization's network infrastructure, which encompasses the identification of the total number of sites requiring connectivity, the specific local IP addresses assigned at each distinct location, the various types of services anticipated to function over the network, as well as the hardware and software resources available to facilitate the VPN service. This analytical assessment serves as the fundamental basis for ascertaining the VPN network architecture design that is to be executed. Upon the identification of the requisite specifications, the subsequent phase involves the formulation of the Site-to-Site VPN network topology. Within this topology, one end will operate as the PPTP Server, located at main office, while the opposing end will function as the PPTP Client, positioned at the branch office[14], [18]. The PPTP Server is responsible for managing connection requests originating from the client and granting access to the local network of main office for the branch office. Both entities are interconnected via the internet, through which a VPN tunnel will be established, serving as an encrypted communication conduit between the two networks. This tunnel utilizes the GRE (Generic Routing Encapsulation) protocol to encapsulate data packets, along with TCP port 1723 for the purposes of connection initialization and control. The data frame structure of the Point-to-Point Tunneling Protocol (PPTP), as illustrated in Figure 4, consists of three main sequential components: the GRE Header, the PPP Header, and the PPP Payload. The first part, the GRE (Generic Routing Encapsulation) Header, functions as the initial encapsulation that wraps the PPP packet into a format suitable for transmission over public IP networks. This header contains critical information such as control flags, version, and session identifiers that facilitate tunnel connection management. Following this is the PPP (Point-to-Point Protocol) Header, which governs the communication session through control fields and protocol identification, ensuring that the data can be properly recognized and processed by the receiving device. The final part is the PPP Payload, which carries data to be transmitted ranging from IP packets and authentication information to application data and may be encrypted using Microsoft Point-to-Point Encryption (MPPE), depending on the security configuration applied. This layered structure enables PPTP to provide secure and efficient network communication between locations over public networks. To avert any interruptions in

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

the connection, it is imperative that firewall configurations at each site permit traffic for both the GRE protocol and TCP port 1723[12], [19], [20].

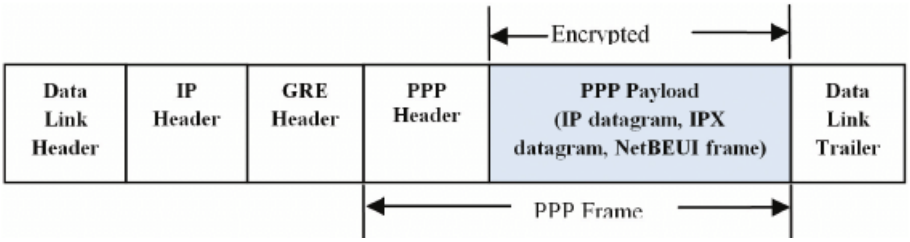

Figure 4. PPTP Tunnel Data Frame Format

During the third phase, we undertake the activation and establishment of the Virtual Private Network (VPN) setup, particularly leveraging MikroTik routers functioning as both the Point-to-Point Tunneling Protocol (PPTP) Server and the PPTP Client. At main office location, the MikroTik router is set up to operate as the PPTP Server. The PPTP server configuration is shown in Figure 5, and the configuration for the PPTP client is shown in Figure 6. To facilitate communication between the local networks of both locations, it is essential to configure static routing on both MikroTik devices. In the branch office, a pathway to main office network needs to be set up using the PPTP Client interface, while in main office, a pathway to branch office network ought to be configured through the active PPTP Client interface. With this arrangement, data packets from each network can be appropriately routed through the established VPN tunnel. This tunnel enables secure data transmission between the two locations, effectively creating the impression that they are part of a singular local network despite their geographical dispersion.

```
/interface pptp-server server set enabled=yes
/ip pool add name=pptp-pool ranges=2.2.2.2
/ppp profile add name=pptp-profile local-address=1.1.1.1 remote-address=pptp-pool use-encryption=yes
/ppp secret add name=branch password=123456 service=pptp profile=pptp-profile
/ip route add dst-address=192.168.100.0/24 gateway=1.1.1.1
```

Figure 5. PPTP Server

```
/interface pptp-client add name=pptp-to-main connect-to=103.241.5.x user=branch password=123456 \
disabled=no add-default-route=no use-peer-dns=no profile=default-encryption
/ip route add dst-address=192.168.10.0/24 gateway=2.2.2.2
```

Figure 6. PPTP Client

Upon the culmination of the configuration process, the subsequent phase entails executing connectivity assessments between the various sites. This assessment encompasses the verification of the successful establishment of the client-server connection, the accurate allocation of virtual (VPN) IP addresses, and the capability of devices from disparate networks to communicate with one another utilizing protocols such as ping, SSH, or any other relevant protocols as required. Should all functionalities operate as intended, the VPN connection may be deemed successful. Further examinations can be administered utilizing analytical tools such as Wireshark or tcpdump to ascertain that data transmission is indeed traversing through the VPN tunnel rather than an unencrypted public pathway. The concluding phase in the establishment of a Site-to-Site VPN involves the processes of maintenance and monitoring. The ongoing surveillance of the VPN connection is imperative to guarantee both the stability and availability of the inter-site network. Organizations may utilize network monitoring applications such as Zabbix, Nagios, etc to oversee traffic patterns, scrutinize connection logs, and promptly identify network anomalies[21]–[23]. Furthermore, the regular execution of

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

configuration backups alongside the maintenance of technical documentation pertinent to the server and client configurations constitutes a fundamental aspect of the long-term management of VPN infrastructure. This documentation also proves invaluable in circumstances of system interruptions or transitions in technical personnel in the future.

3. RESULT

3.1. Infrastructure Development

The investigation was executed utilizing two principal methodologies: configuration time assessment and user feedback collection. The testing cohort comprised 50 participants, whose expertise varied from novice to intermediate levels within the realm of network technology. The configuration steps were undertaken through two distinct avenues: the Command Line Interface (CLI) and Winbox. Each participant was assigned an identical task, which entailed configuring a PPTP VPN on a MikroTik device. The duration required for each approach was meticulously documented on an individual basis. Furthermore, the success rate of the preliminary configuration attempt was systematically recorded. Subsequent to the completion of the configuration, participants were solicited to complete a questionnaire aimed at evaluating the usability and satisfaction associated with the Winbox interface. The findings of the research indicated that the configuration process employing Winbox necessitated an average duration of 15 to 25 minutes, representing an approximate 40% enhancement in efficiency compared to the configuration via CLI. This level of efficiency is deemed noteworthy, particularly for novice users who may lack familiarity with text-based commands. Additionally, the success rate for initial configuration attempts among beginner users attained a remarkable 92%, signifying that Winbox affords a more user-centric experience relative to the CLI approach, which exhibited a heightened initial failure rate.

Drawing from a survey of 50 participants possessing backgrounds in information technology, the satisfaction rating for the Winbox interface garnered an average score of 4.6 out of 5. The salient features appreciated by users included the intuitive organization of menus, ease of navigation, and the occurrence of minimal errors throughout the configuration process. In light of the outcomes, it can be inferred that the utilization of Winbox for PPTP VPN configuration is significantly more effective when juxtaposed with the CLI method. Given the reduced configuration time, elevated success rates, and favorable user satisfaction, Winbox is recommended as the primary instrument for VPN network management, especially for individuals operating at the beginner and intermediate levels in network technology.

3.2. Network Performance

The deployment of a Virtual Private Network (VPN) utilizing the Point-to-Point Tunneling Protocol (PPTP) on MikroTik exemplifies network efficiency that is contingent upon several pivotal technical metrics. The connection initiation time for PPTP on MikroTik is comparatively rapid, as the processes of tunneling setup and authentication transpire in a matter of seconds, particularly when the network configuration is meticulously optimized. With respect to throughput, PPTP has the capacity to provide relatively consistent upload and download velocities, albeit not at the level of more contemporary VPN protocols such as L2TP/IPsec or OpenVPN; the data transmission rate is subject to the relatively minimal encryption overhead. Latency associated with PPTP connections on MikroTik is also notably low, rendering it appropriate for remote access applications that require satisfactory responsiveness. Nevertheless, packet loss may manifest in instances of network instability or when the MikroTik apparatus encounters significant traffic loads, although under typical conditions, the incidence tends to remain minimal. The utilization of CPU and RAM on the MikroTik device during the execution of PPTP is relatively efficient; however, it may escalate as the client count or volume of encrypted data

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

increases. Consequently, resource monitoring emerges as an indispensable facet in sustaining overall system performance.

Table 1. VPN Network Performance

Parameter	Scenario 1 (AES-128)	Scenario 2 (AES-256)	Scenario 3 (No Encryption)
Connection Time (seconds)	3.2	3.5	2.8
Download Throughput (Mbps)	85	78	95
Upload Throughput (Mbps)	45	40	50
Latency (ms)	25	28	20
Packet Loss (%)	0.5	0.7	0.3
CPU Usage (%)	65	72	55
RAM Usage (MB)	128	135	120

Based on the evaluation of three VPN configuration scenarios (Table 1), the unencrypted scenario demonstrated the best performance, with a connection time of 2.8 seconds, download/upload throughput of 95/50 Mbps, 20 ms latency, 0.3% packet loss, and the lowest CPU and RAM usage (55% and 120 MB). The AES-128 encryption scenario recorded a connection time of 3.2 seconds, throughput of 85/45 Mbps, 25 ms latency, 0.5% packet loss, 65% CPU usage, and 128 MB RAM. Meanwhile, AES-256 showed decreased performance with a 3.5-second connection time, 78/40 Mbps throughput, 28 ms latency, 0.7% packet loss, 72% CPU usage, and 135 MB RAM. Although the unencrypted setup offers superior performance, it lacks data protection and is therefore unsuitable for network environments requiring high security.

Table 2. PPTP Advantages and Disadvantages

Scenario	Advantages	Disadvantages
Scenario 1 (AES-128)	- Adequate security - High performance - Moderate resource usage	- Slightly higher latency than without encryption - Higher CPU and RAM usage than without encryption
Scenario 2 (AES-256)	- Strongest security - Suitable for highly sensitive data environments	- Lower throughput - Slower connection time- Highest CPU and RAM usage
Scenario 3 (No Encryption)	- Highest throughput - Lowest latency - Most efficient CPU and RAM usage	- No data protection - Highly vulnerable to eavesdropping and network attacks

PPTP presents both advantages and Disadvantages that must be aligned with specific VPN network requirements (Table 2). The AES-128 scenario offers a balance between security and performance, making it suitable for SMEs or internal networks. AES-256 provides the highest level of security but results in reduced performance and increased system resource usage, thus recommended for highly sensitive environments. In contrast, the non-encryption scenario demonstrates optimal performance, yet its vulnerability to threats makes it unsuitable for public or sensitive networks.

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

3.3. VPN Network Security

From a security standpoint, the implementation of PPTP VPN on MikroTik devices presents several constraints when juxtaposed with contemporary VPN protocols. A significant limitation is associated with the deployment of the MPPE (Microsoft Point-to-Point Encryption) algorithm, which is often deemed less effective in strength relative to encryption standards like AES (Advanced Encryption Standard) found in protocols including L2TP/IPsec and OpenVPN. The reliance of MPPE on the RC4 cipher, which is known to be susceptible to various forms of exploitation, renders it inadequate for environments that necessitate elevated security measures. The authentication efficacy of MikroTik's PPTP is generally dependable, particularly when robust usernames and passwords are utilized in conjunction with the CHAP (Challenge Handshake Authentication Protocol) mechanism. However, this authentication model is still at risk from various attack methods, particularly when weak passwords are in play. The susceptibility to brute-force attacks constitutes a notable concern, as PPTP does not incorporate supplementary protective measures such as two-factor authentication or digital certificates. Consequently, while PPTP may be characterized by ease of implementation and minimal resource consumption, it exhibits heightened vulnerabilities from a security perspective and is not advocated for networks that emphasize high-level data protection.

Table 3. VPN Network Security

Parameter	Scenario 1 (AES-128)	Scenario 2 (AES-256)	Scenario 3 (MPPE - PPTP)
Authentication Success Rate (%)	97.8% (Failed: 2.2% wrong password, connection timeout)	98.9% (Failed: 1.1% – input error)	94.3% (Failed: 5.7% – partial brute-force success)
Attack Detection Time (ms)	135 ms (Brute-force detected after 8 attempts)	122 ms (Fast detection with login limit + log alert)	230 ms (Slow detection due to minimal logging)
Encryption Vulnerability	Medium (at risk if key reuse occurs)	Low (AES-256 is resistant to brute-force and cryptanalysis)	High (MPPE uses RC4, vulnerable to exploitation)
Authentication Method	CHAP with minimum 8-character password	CHAP + lockout policy after 5 attempts	PAP (vulnerable, not fully encrypted during login process)
Firewall Response Level	Medium (Blocks IP after 10 failed attempts)	High (Auto-blacklist + email alert)	Low (Logging only, no automatic blocking)

Based on the evaluation results presented in Table 3, Scenario 2 (AES-256) offers the most robust security framework, with the highest authentication success rate (98.9%) and the fastest attack detection time (122 ms), supported by a responsive firewall and automated notification systems. Scenario 1 (AES-128) demonstrates a balance between security and efficiency, with a 97.8% authentication rate and moderate vulnerability, making it suitable for environments requiring adequate protection without overloading system resources. In contrast, Scenario 3 (MPPE-PPTP), although relatively efficient in performance, exhibits the weakest security (94.3% authentication, 230 ms detection), uses the insecure PAP method, and is highly vulnerable to attacks, rendering it unsuitable for networks that demand strong data protection.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

3.4. Device Configuration

Creating a Virtual Private Network (VPN) with the Point-to-Point Tunneling Protocol (PPTP) on MikroTik platforms necessitates thorough hardware adjustments, essential for boosting network effectiveness and accommodating future expansion. MikroTik devices such as the RB750 and RB450G, operating on RouterOS version 6.49, are prevalent in the market, primarily due to their cost-effectiveness and adequate data processing capabilities tailored for small to medium-sized networks. The RB750, with its compact form and basic hardware, is well-suited for scenarios with a limited user base and moderate traffic demands. In contrast, the RB450G, equipped with a more advanced processor and enhanced RAM specifications, is proficient in managing a greater number of concurrent VPN sessions. The quantity of simultaneous users represents a significant factor in the configuration process, as each active connection necessitates CPU and RAM resources for the execution of encryption, authentication, and traffic management functions. On devices like the RB450G, PPTP can accommodate multiple simultaneous connections while maintaining a stable performance level, given the available bandwidth of 100 Mbps, provided that traffic surges do not exceed the device's operational limitations. Furthermore, bandwidth allocation must be meticulously regulated to guarantee that each user is afforded adequate access speed, thereby preventing network overload. The implementation of MikroTik functionalities such as Simple Queue or Queue Tree aids in the management of bandwidth on a per-user basis, thereby promoting efficient and regulated VPN connections.

Table 4. Network Users via PPTP

Users	AES 128			AES - 256			MPPE-PPTP		
	Throughput (Mbps)	Latency (ms)	Packet Loss (%)	Throughput (Mbps)	Latency (ms)	Packet Loss (%)	Throughput (Mbps)	Latency (ms)	Packet Loss (%)
5	92	22	0.2	90	24	0.3	95	20	0.1
10	85	26	0.5	82	28	0.6	88	23	0.3
20	68	40	1.2	65	42	1.5	70	38	1.0
30	53	48	2.0	50	50	2.3	55	45	1.8
40	47	58	3.2	44	61	3.5	50	55	3.0
50	38	68	4.8	36	72	5.2	40	65	4.5

Table 4 delineates the repercussions of increasing the number of concurrently connected users on network efficacy across three encryption scenarios: AES-128, AES-256, and MPPE-PPTP. The metrics examined include throughput, latency, and packet loss, which collectively illustrate the impact of encryption strength on network performance under varying load conditions. In the initial state with 5 users, MPPE-PPTP yields the highest throughput at 95 Mbps, with latency at 20 ms and minimal packet loss of 0.1%, signifying an optimal performance under light load. AES-128 and AES-256 follow closely with throughputs of 92 Mbps and 90 Mbps, respectively, accompanied by marginal increases in latency and packet loss. These results highlight that under minimal user load, all three encryption methods deliver acceptable performance, though stronger encryption slightly affects efficiency. As the number of users increases to 10, a gradual decline in throughput is observed across all scenarios. MPPE-PPTP sustains 88 Mbps, AES-128 drops to 85 Mbps, and AES-256 to 82 Mbps, while latency and packet loss remain within controllable limits. This phase reflects the network's ability to handle moderate user loads with only minor degradation. At 20 users, performance degradation becomes more evident. Throughput drops to 70 Mbps for MPPE-PPTP, 68 Mbps for AES-128, and 65 Mbps for AES-256, accompanied by increased latency (up to 42 ms) and packet loss reaching up to 1.5% for AES-256. This indicates the

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

onset of congestion effects, especially for networks using stronger encryption schemes. When reaching 30 users, the strain on the network intensifies. MPPE-PPTP throughput declines to 55 Mbps, while AES-128 and AES-256 decrease further to 53 Mbps and 50 Mbps, respectively. Latency ranges between 45–50 ms, and packet loss climbs up to 2.3%, particularly for AES-256. These figures suggest that the network is approaching overload conditions, especially when handling complex encryption under growing user demand. At 40 users, the downward trend continues with throughput values dropping to 50 Mbps (MPPE-PPTP), 47 Mbps (AES-128), and 44 Mbps (AES-256). Latency escalates to as high as 61 ms, and packet loss surges, notably reaching 3.5% for AES-256, highlighting significant performance strain. Finally, under the load of 50 users, the network experiences critical performance deterioration. MPPE-PPTP records 40 Mbps throughput with 4.5% packet loss, while AES-128 and AES-256 lag at 38 Mbps and 36 Mbps, respectively, with latency peaking at 72 ms in the AES-256 scenario. This condition clearly indicates that the network has surpassed its optimal operating capacity, resulting in substantial Quality of Service (QoS) degradation. In summary, the data reveals a strong correlation between user volume and network performance across encryption schemes. While stronger encryption (AES-256) offers superior security, it introduces measurable performance trade-offs, especially under high-load conditions. These findings underscore the importance of strategic network capacity planning that balances security requirements with performance expectations in multi-user environments.

Table 5. Comparison of PPTP with Other VPN Protocols

Protocol	Security	Performance	Compatibility & Advantages	References
PPTP	Very low	Very fast	Easy to configure, highly compatible	Proposed Method
L2TP/IPsec	High	Moderate	Built-in OS support, secure	[24]–[26]
OpenVPN	Very high	Moderate to high	Cross-platform, firewall/NAT traversal	[27]–[29]
SSTP	High	Moderate	Best suited for Windows environments	[30]–[32]

In the use of Virtual Private Networks (VPNs), each protocol offers different levels of security, speed, and compatibility. This study compares four main VPN protocols: PPTP, L2TP/IPsec, OpenVPN, and SSTP. PPTP is known for its high speed and ease of use, but it provides very low security due to outdated and vulnerable encryption. Because of its speed, PPTP is used in this method as a reference for performance testing. L2TP/IPsec provides strong security by combining tunneling and encryption, although its performance decreases due to double encapsulation. OpenVPN offers very high security, works across various operating systems, and is effective in bypassing firewalls and NAT, although its speed ranges from moderate to high depending on the configuration. Meanwhile, SSTP is suitable for Windows systems because of its good integration and use of port 443, which allows it to bypass most firewalls, while also maintaining a high level of security. A complete comparison of these four protocols is presented in Table 5. Comparison of PPTP with Other VPN Protocols, which summarizes each protocol's security, performance, and advantages. These findings, derived from both experimental results and literature studies, help identify the most appropriate protocol according to specific network requirements, especially in resource-constrained environments.

4. CONCLUSION

Based on the analysis conducted, it can be concluded that the deployment of a Virtual Private Network (VPN) using AES-128 and AES-256 encryption mechanisms results in a relatively minor decrease in connection speed and data transmission efficiency when compared to an unencrypted

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

system. Nevertheless, AES-256 offers the highest level of security, with performance trade-offs that remain within acceptable limits. Conversely, unencrypted VPNs exhibit superior performance metrics but are highly vulnerable to security threats. The use of the Point-to-Point Tunneling Protocol (PPTP) combined with Microsoft Point-to-Point Encryption (MPPE) employing RC4 encryption reveals significant security weaknesses, making it unsuitable for scenarios requiring elevated protection. Among the configurations tested, AES-256 demonstrated the highest authentication success rate (98.9%) and the fastest threat detection time (122 milliseconds), supported by features such as automatic blacklisting and email notifications. Furthermore, as the number of VPN users increases, network performance deteriorates significantly, as evidenced by reduced throughput, increased latency, and higher packet loss highlighting the critical importance of careful network capacity planning. Therefore, the implementation of AES-256 encryption is strongly recommended to ensure optimal network security, supplemented by continuous performance monitoring and capacity management to maintain service quality in response to growing user demand. Scientifically, this study provides a significant contribution to the understanding of security risks and mitigation strategies in the implementation of PPTP-based VPNs, particularly for organizations with limited infrastructure. By highlighting the inherent weaknesses of legacy protocols such as PPTP and MPPE-RC4, this research aids technology decision-makers in resource-constrained institutions to consider more secure alternatives that remain operationally efficient. These findings serve as a foundation for developing more adaptive network security policies in response to modern cyber threats, without overlooking the technical limitations faced by small to medium-sized organizations.

For future research, it is recommended to explore the implementation of more robust VPN protocols such as OpenVPN or IPSec, which are known to offer enhanced encryption standards and improved performance scalability, thereby further strengthening secure communications within enterprise environments.

REFERENCES

[1] D. Bringhenti, R. Sisto, and F. Valenza, "Automating VPN Configuration in Computer Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 22, no. 1, pp. 561–578, 2025, doi: 10.1109/TDSC.2024.3409073.

[2] M. Naas and J. Fesl, "A novel dataset for encrypted virtual private network traffic analysis," *Data Br.*, vol. 47, p. 108945, 2023, doi: 10.1016/j.dib.2023.108945.

[3] J. Li, B. Feng, and H. Zheng, "A survey on VPN: Taxonomy, roles, trends and future directions," *Comput. Networks*, vol. 257, p. 110964, 2025, doi: https://doi.org/10.1016/j.comnet.2024.110964.

[4] U. H. Rao and U. Nayak, "Virtual Private Networks," in *The InfoSec Handbook: An Introduction to Information Security*, Berkeley, CA: Apress, 2014, pp. 245–262.

[5] G. R. Chen, "Development Trend of Computer Network," in *Advances in Mechatronics and Control Engineering II*, 2013, vol. 433, pp. 1670–1673, doi: 10.4028/www.scientific.net/AMM.433-435.1670.

[6] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," *J. Netw. Comput. Appl.*, vol. 226, p. 103884, 2024, doi: https://doi.org/10.1016/j.jnca.2024.103884.

[7] N. A. Magnaye, "Advancements in computer network technologies: A review," *Metaverse*, vol. 5, no. 1, p. 2315, 2024, doi: 10.54517/m.v5i1.2315.

[8] L. Sun, H. Dong, F. K. Hussain, O. K. Hussain, and E. Chang, "Cloud service selection: State-of-the-art and future research directions," *J. Netw. Comput. Appl.*, vol. 45, pp. 134–150, 2014, doi: https://doi.org/10.1016/j.jnca.2014.07.019.

[9] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891.

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

[10] S. Budiyanto and D. Gunawan, "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol," *IEEE Access*, vol. 11, pp. 60853–60865, 2023, doi: 10.1109/ACCESS.2023.3286032.

[11] J. Jones, H. Wimmer, and R. J. Haddad, "PPTP VPN: An Analysis of the Effects of a DDoS Attack," in *2019 SoutheastCon*, 2019, pp. 1–6, doi: 10.1109/SoutheastCon42311.2019.9020514.

[12] M. A. Gunawan and S. Wardhana, "Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network)," *Resist. (Elektronika Kendali Telekomun. Tenaga List. Komputer)*, vol. 6, no. 1, p. 69, 2023, doi: 10.24853/resistor.6.1.69-78.

[13] R. Arfind, H. Supendar, and R. Fahlapi, "Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik," *J. Komput. Antart.*, vol. 1, no. 3 SE-Articles, pp. 108–116, Sep. 2023, doi: 10.70052/jka.v1i3.28.

[14] D. A. Pangestu, A. S. Budiman, and S. Sartini, "Rancangan Site-to-Site VPN dengan PPTP pada Interkoneksi Antar Kantor PT. Indosis Integrasi," *Semantik*, vol. 8, no. 1, 2024, doi: 10.55679/semantik.v8i1.9189.

[15] U. Bina, S. Informatika, U. Mohammad, and H. Thamrin, "Penerapan Sistem Keamanan Jaringan Menggunakan Vpn Dengan Metode Pptp Pada Pt Hinoka Sinergi Tanyo," *J. Sist. Inf. Univ. Suryadarma*, vol. 11, no. 2, pp. 185–196, 2014, doi: 10.35968/jsi.v11i2.1252.

[16] R. F. Syarif and I. A. Sobari, "Implementasi Virtual Private Network (VPN) menggunakan Metode PPTP pada PT. Sinar Quality Internusa," *J. Pendidik. Tambusai*, vol. 6, no. 2, pp. 15165–15184, 2022.

[17] F. Hauser, M. Häberle, M. Schmidt, and M. Menth, "P4-IPsec: Site-to-Site and Host-to-Site VPN With IPsec in P4-Based SDN," *IEEE Access*, vol. 8, pp. 139567–139586, 2020, doi: 10.1109/ACCESS.2020.3012738.

[18] I. K. Rahman, D. I. Mulyana, and Y. Akbar, "Optimasi IPSec Site to Site VPN Mikrotik menggunakan Algoritme Enkripsi Blowfish," *Progresif*, vol. 19, no. 1, 2024, doi: 10.35889/progresif.v19i1.1092.

[19] A. K. M. Hadood, "Implementation of Site to Site IPsec VPN Tunnel using GNS3 Simulation," no. November, 2024, [Online]. Available: https://doi.org/10.22214/ijraset.2024.65635.

[20] M. T. Roseno, "Analisis Perbandingan Protokol Virtual Private Network (VPN) – PPTP, L2TP, IPSEC – Sebagai Dasar Perancangan VPN pada Politeknik Negeri Sriwijaya Palembang," pp. 1–7, 2013.

[21] M. Y. Ishaq and F. Firmansyah, "Implementasi Sistem Monitoring Menggunakan Zabbix dan Notifikasi Realtime Telegram," *JINSAN J. Inform. Sist. dan Apl.*, vol. 3, no. 2, 2019, doi: 10.31294/jinsan.v3i2.2432.

[22] A. Muttaqin, F. Chahyadi, and N. Hayati, "Network Monitoring System Menggunakan Nagios dengan Event Handler Notifikasi Whatsapp," vol. 11, no. 02, pp. 55–64, 2022.

[23] R. Sugeng, "Implementasi Zabbix Monitoring Dengan Integrasi Sistem Notifikasi Discord, Teams, Telegram Untuk Monitoring Infrastruktur Jaringan pada PT. Pundi Mas Berjaya (PMB)," *NACOSPRO J. Nas. Komput. dan Sist. Terdistribusi*, vol. 6, no. 1, 2024, doi: 10.37253/nacospro.v6i1.9721.

[24] Y. Chen, Q. Li, L. Tian, and Y. Jiang, "Navigating the VPN Landscape: A Comparative Study of L2TP, IPSec, and MPLS VPN Technologies," in *2024 4th International Conference on Electronic Information Engineering and Computer Science (EIECS)*, 2024, pp. 614–617, doi: 10.1109/EIECS63941.2024.10800571.

[25] Y. Niu, J. Li, and L. Li, "Research on Authentication Security of Wireless Local Area Network Based on L2TP Protocol," in *2009 IITA International Conference on Services Science, Management and Engineering*, 2009, pp. 491–494, doi: 10.1109/SSME.2009.30.

[26] A. F. Gentile, D. Macrì, F. De Rango, M. Tropea, and E. Greco, "A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment," in *Proceedings of the Future Internet Conference (hypothetical placeholder)*, 2022, vol. 14, no. 9, p. 264, [Online]. Available: https://www.proquest.com/scholarly-j@INPROCEEDINGS%7B6300807,%0A author=%7BQu, Junhua and Li, Tao and Dang, Fangfang%7D,%0A booktitle=%7B2012 Fourth International Conference on Computational and Information Sciences%7D, %0A title=%7BPerformance Evaluat.

Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818

[27] J. Qu, T. Li, and F. Dang, "Performance Evaluation and Analysis of OpenVPN on Android," in *2012 Fourth International Conference on Computational and Information Sciences*, 2012, pp. 1088–1091, doi: 10.1109/ICCIS.2012.203.

[28] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, "Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment," in *2015 International Conference on Computing, Communication and Security (ICCCS)*, 2015, pp. 1–4, doi: 10.1109/CCCS.2015.7374130.

[29] R. M. Pandurang and D. C. Karia, "Performance measurement of WEP and WPA2 on WLAN using OpenVPN," in *2015 International Conference on Nascent Technologies in the Engineering Field (ICNTE)*, 2015, pp. 1–4, doi: 10.1109/ICNTE.2015.7029939.

[30] J. B. R. Lawas, A. C. Vivero, and A. Sharma, "Network performance evaluation of VPN protocols (SSTP and IKEv2)," in *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, 2016, pp. 1–5, doi: 10.1109/WOCN.2016.7759880.

[31] S. Narayan, C. J. Williams, D. K. Hart, and M. W. Qualtrough, "Network performance comparison of VPN protocols on wired and wireless networks," in *2015 International Conference on Computer Communication and Informatics (ICCCI)*, 2015, pp. 1–7, doi: 10.1109/ICCCI.2015.7218077.

[32] Y.-J. Kim, V. Kolesnikov, H. Kim, and M. Thottan, "SSTP: A scalable and secure transport protocol for smart grid data collection," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 161–166, doi: 10.1109/SmartGridComm.2011.6102310.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, Agustus 2025, Page. 2171-2186
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4818