Design of Data Security for Remote Access Using IPsec- and SSL-Based VPN

Ahmad Fikri[1*]

Abstract

The rapid advancement of digital communication technologies has increased the need for secure remote access within corporate environments. This study develops and implements a secure network architecture for PT Tanjungenim Lestari Pulp & Paper using Virtual Private Network (VPN) mechanisms based on Internet Protocol Security (IPsec) and Secure Socket Layer (SSL). The existing network, which utilizes a star topology and file-sharing mechanisms, was found to lack sufficient security, particularly in protecting data transmission to external partner companies. The proposed system integrates IPsec-based VPN tunneling to ensure encrypted communication channels and SSL certificates to safeguard FTP authentication processes. Data were collected through action research and document studies, followed by network design, IP addressing, router configuration, VPN deployment, FTP server installation (VSFTPD), and file transfer testing. The results demonstrate successful establishment of secure tunnels, encrypted data exchange, and protection against credential interception during authentication. This study concludes that implementing IPsec VPN and SSL-secured FTP significantly enhances remote access security, maintains data confidentiality, and strengthens the overall network infrastructure of PT Tanjungenim Lestari Pulp & Paper.

Keywords

VPN, IPsec, SSL, network security, remote access, PT Tanjungenim Lestari Pulp & Paper.

Article History

Received 21 July 2025
Accepted 25 October 2025

How to Cite

Fikri, A. (2025). Design of Data Security for Remote Access Using IPsec- and SSL-Based VPN. ***Jurnal Jaringan Komputer dan Keamanan,*** *6*(3), 93-99.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: 201220013@students.binadarma.ac.id

Introduction

In an increasingly digitalized environment, remote access has become a fundamental requirement for organizations and individuals. The shift toward distributed communication systems, cloud-based services, and remote working arrangements demands seamless and secure access to internal networks. However, this convenience also expands the attack surface for cybercriminals. Sensitive data transmitted over public networks is susceptible to interception, monitoring, and manipulation. As communication infrastructures become more interconnected, implementing strong information security measures is essential to prevent unauthorized access, data breaches, and other cyber threats that could compromise business operations.

One widely adopted solution for securing remote communication is the Virtual Private Network (VPN). VPN technology establishes encrypted tunnels between remote users and internal networks, ensuring that data travels securely even across untrusted public networks. Ayu (2020) in Musril (2019) explains that VPNs often utilize GRE (Generic Routing Encapsulation) tunnels to connect multiple routers and transport encapsulated packets reliably. Cisco defines VPN as a secure communication method that encrypts transmitted data to maintain confidentiality, integrity, and authenticity. Through VPNs, users can safely retrieve internal files, access corporate applications, and communicate with devices within the organization's private network.

A prominent protocol used to strengthen VPN communication is Internet Protocol Security (IPsec). IPsec offers robust, multilayered protection by encrypting data packets and authenticating endpoints involved in communication. J. Safira, Hanafi, and Munawar (2021) emphasize that IPsec provides two types of protection simultaneously: secure point-to-point connectivity and end-to-end encryption. These features safeguard data integrity while preventing interception or tampering during transmission. IPsec has therefore become a preferred standard for organizations requiring secure and resilient remote communication infrastructures.

In addition to IPsec, SSL/TLS also serves as a crucial security mechanism, particularly for web-based communication. SSL encrypts data exchanged between clients and servers, protecting it from man-in-the-middle attacks or unauthorized interception. Apriyanto and Wahyuni (2019) describe SSL as a standard security technology that ensures secure and private online communication. Its widespread adoption in web browsers, applications, and online services demonstrates its importance in safeguarding digital transactions and maintaining trust in web communications.

Several studies have explored the implementation of VPNs and related security technologies to enhance organizational cybersecurity. Sulistiyono (2020) analyzed IPsec VPN deployment using MikroTik routers, while Ruwaida and Kurnia (2019) investigated SSL-secured FTP implementation over PPTP-based VPN connections. Meanwhile, Sumarna and Maulana (2021) conducted performance evaluations of L2TP/IPsec VPNs in a public health training institution. These studies demonstrate that VPN technology not only improves network security but also supports flexible and efficient remote connectivity. As Iswa (2019) states, VPNs provide important advantages such as enhanced privacy, expanded network

coverage, reduced long-distance communication costs, and increased scalability for business operations.

PT Tanjungenim Lestari Pulp & Paper, a major pulp and paper company located in Tanjung Enim, South Sumatra, depends heavily on continuous and secure data exchange with partner companies and internal divisions. However, existing security gaps—such as unencrypted transmissions, weak authentication, and insufficient encryption—expose the organization to cyber risks. Given its operational scale and sensitivity of its business processes, implementing a secure communication framework through IPsec-based VPN and SSL is critically important. Strengthening these security mechanisms will help safeguard confidential business information, protect communication channels, and support the company's efforts to maintain operational continuity in an increasingly threat-prone digital environment.

Methodology

This study employed the following methods:

Action Research

Action research was used to identify and solve network security issues at PT Tanjungenim Lestari Pulp & Paper. This method supports iterative problem-solving through planning, action, observation, and reflection.

Document Study

A literature-based approach was used to analyze relevant journals, documentation, and previous studies related to VPN, IPsec, SSL, and network security implementation.

Results

Company Network Structure and Architecture

PT Tanjungenim Lestari Pulp & Paper's existing infrastructure uses a star topology, which offers ease of maintenance and scalability. A central hub or switch mediates all data communication, simplifying troubleshooting and allowing efficient connectivity between computers, internet access points, and the data center.

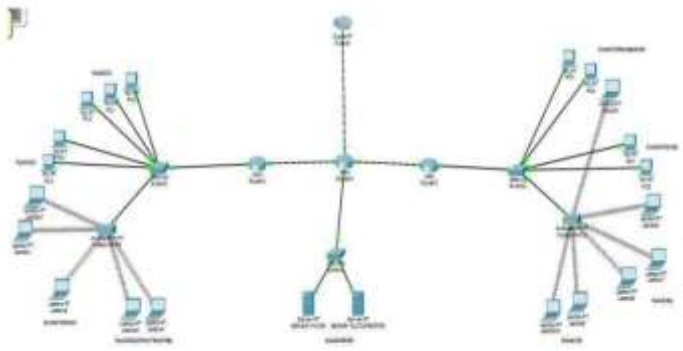

Figure .1 Star Topology

Network Design

Based on the analysis of the existing architecture, an enhanced network design was proposed to improve communication security, integrate encrypted tunnels, and strengthen internal resource access. The design focuses on proper IP allocation, router configuration, and VPN tunneling.

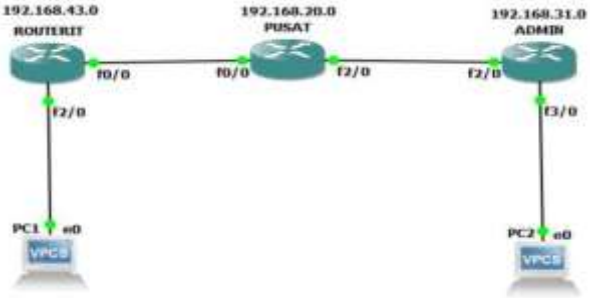

Figure 2. Proposed Network Design

IP Address Configuration

The initial setup involved assigning static IP addresses to each computer and network device to ensure unique identification. Proper IP allocation allows clients and servers to communicate seamlessly within the same network.

Router Configuration

Routers were configured by setting interface parameters, assigning IP addresses, adding necessary routing entries, and preparing devices for VPN tunneling. Console access was used to configure each router node, ensuring that devices could communicate within the defined network.

IPsec VPN Configuration and Results

After completing IP assignments and router configurations, IPsec VPN was implemented. The configuration establishes a secure tunnel for encrypted data exchange. Testing showed successful IPsec tunnel creation, although early stages experienced connection timeouts before final stability was achieved.

FTP Server Installation (VSFTPD)

An FTP server was installed to support centralized file distribution within the company. The VSFTPD service was configured through the /etc/vsftpd.conf file, including enabling local user access, activating SSL support, and defining security attributes. Verification showed successful service activation and readiness for file transfer operations.

File Transfer Testing

Testing focused on securing FTP authentication with and without SSL protection. FileZilla was used to log into the FTP server using controlled credentials. When SSL was enabled, the username and password could not be intercepted using Wireshark, demonstrating

secure authentication. Without SSL, credentials were exposed to interception attempts.Successful file transfers were conducted in both directions client to server and server to client confirming that the secure FTP setup functioned as expected.

Discussion

The results of this study demonstrate that the implementation of IPsec VPN combined with SSL encryption significantly improves the security of remote communication within the PT Tanjungenim Lestari Pulp & Paper network environment. IPsec provides robust packet-level encryption, ensuring that all data transmitted between remote devices and internal servers remains confidential and tamper-proof during transit. This encryption mechanism effectively prevents unauthorized parties from capturing or manipulating sensitive information—a critical requirement for organizations with high data exchange intensity. SSL complements this protection by securing the authentication stage, particularly during FTP login processes, thereby ensuring that usernames and passwords are not exposed to interception or man-in-the-middle attacks.

Furthermore, the IPsec-based VPN tunnel successfully establishes a secure and stable communication channel that maintains both data integrity and authenticity. The dual-layer protection described by J. Safira, Hanafi, and Munawar (2021) is evident in the system's ability to safeguard point-to-point connectivity while encrypting all transported packets. This layered security approach aligns with Cisco's definition of VPN as a secure connection that enhances confidentiality across public networks. Through encryption, hashing, and authentication, the implemented system ensures that only legitimate users can access internal resources, reducing the risk of unauthorized infiltration.

The study also finds that the existing star topology used by the organization is well-suited for the deployment of IPsec VPN and SSL. Because star topology centralizes network control, the VPN server configuration can be managed efficiently from a single point. This structural compatibility simplifies IPsec key exchange, SSL certificate distribution, and tunnel management. Previous studies—such as those by Sulistiyono (2020) and Ruwaida & Kurnia (2019)—also emphasize that centralized network designs improve the scalability and manageability of VPN solutions, particularly in organizations requiring controlled, secure access to internal systems.

In terms of functional performance, the integration of IPsec and SSL demonstrates clear improvements in safeguarding communication flows. SSL encryption supports the secure transmission of authentication credentials, eliminating vulnerabilities commonly associated with plaintext login mechanisms. Meanwhile, the GRE tunneling feature highlighted by Musril (2019) facilitates smooth packet encapsulation and forwarding between interconnected routers. Together, these technologies create a holistic security framework that not only protects data but also enhances the reliability of remote access services. This aligns with the advantages outlined by Iswa (2019), who identified privacy preservation, cost efficiency, scalability, and flexible remote access as key benefits of VPN adoption.

Despite the positive outcomes, the research also identifies several limitations. The system testing was conducted within a controlled, simulated environment, which does not fully capture real operational challenges such as fluctuating bandwidth usage, unpredictable user behavior, or external cyberattack attempts. Real-world networks often experience latency variation, packet loss, or peak traffic loads that can affect VPN performance. Additionally, the

study has not yet evaluated integration with intrusion detection systems (IDS), comprehensive logging analysis, or performance benchmarking under high-stress conditions.

Based on these limitations, future research is recommended to expand toward real-time network monitoring, the incorporation of IDS/IPS technologies, stress-testing under varied traffic conditions, and the deployment of multi-site IPsec VPNs across multiple branch offices. Studies focusing on certificate automation, auto-key exchange mechanisms, and VPN failover techniques would also enhance resilience and operational continuity. Through these further explorations, organizations like PT Tanjungenim Lestari Pulp & Paper can develop a fully optimized, resilient, and scalable secure communication infrastructure that meets the demands of modern digital ecosystems.

Conclusion and Recommendations

Designing a secure network architecture requires connecting multiple devices to support communication and data exchange. Implementing IPsec VPN enhances data security by encrypting transmissions and preventing third-party interference. PT Tanjungenim Lestari Pulp & Paper's existing star topology supports efficient integration of secure tunnels and centralized data distribution.

Additionally, implementing SSL certificates for FTP authentication provides strong protection against credential interception. Together, IPsec VPN and SSL-secured FTP create a robust and secure remote access framework suitable for enterprise environments.

Disclosure Statement

The authors declare no conflict of interest related to this study.

Acknowledgments

The authors express appreciation to PT Tanjungenim Lestari Pulp & Paper and Universitas Bina Darma for their support and cooperation throughout this research.

References

Apriyanto, & Wahyuni. (2019). Secure Socket Layer (SSL) technology for encrypted communication between servers and clients.

Iswa. (2019). Advantages of using VPN.

J. Safira, Hanafi, & Munawar. (2021). Implementation of L2TP/IPsec VPN network using Linux in a computer network laboratory. Jurnal TEKTRO, 5(1), 59–63.

Musril, H. A. (2019). Design of Virtual Private Network (VPN) based on Open Shortest Path First (OSPF). Info Tekjar: Jurnal Nasional Informatika dan Teknologi Jaringan.

Putra, O. D., Destiarini, & Rahman, A. (2022). Use of Virtual Private Network (VPN) at PT Semen Baturaja (Persero) Tbk. INTECH, 3(1).

Putri, R. R. Q. Y., Nusantara, H., Effendi, M. R., & Munir, A. (2019). Two-stage wideband waveguide BSF composed of CSRR-based dielectric frequency selective structures for X-band application. In 2019 International Conference on Electrical Engineering and Informatics (ICEEI) (pp. 653–656). IEEE.

Rasuanda, M. (2020). Comparison of VPN performance using PPTP and SSTP over SSL with Quality of Service method. Journal of Information System and Technology (JOINT), 1(2), 110–123.

Ruwaida, D., & Kurnia, D. (2018). Development of FTP with OpenSSL security on MikroTik VPN at SMK Dwiwarna. CESS: Journal of Computer Engineering, System and Science, 3(1), 45–49.

Subekti, R. (2020). Implementation of Virtual Private Network (VPN) as a security solution during work from home. JUNIF, 1(1).

Sulistiyono, S. (2020). Design of Virtual Private Network based on IP Security using MikroTik routers. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 7(2), 150–164.

Tamsir Ariyadi, T. (2022). Comparison of Virtual Private Network performance between VPN tunnel and IPsec. Journal of Network and Computer Applications, 1(1), 38–47.

Wicaksana, M. R. N. (2022). Design of Mikrotik-based Layer 2 Tunneling Protocol (L2TP) Virtual Private Network. Journal of Network and Computer Applications, 1(1), 38–47.

Biographical Notes

AHMAD FIKRI is a student in the Computer Engineering Study Program at Universitas Bina Darma, focusing on network security, VPN technology, and secure communication systems.