DIJEMSS: Dinasti International Journal of Education Management and Social Science
E-ISSN: 2686-6331
P-ISSN: 2686-6358
https://dinastipub.org/DIJEMSS dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/dijemss.v7i1

Design and Simulation of VPN based Private Network with Regulatory Compliance and Economic Feasibility Analysis in Government WAN Infrastructure

Dara Kusumawati Ramadani Yasir[1], Rendy Munadi[2], Helni Mutiarsih Jumhur[3]
[1]School of Electrical Engineering, Telkom University Bandung, Indonesia, darakusumawati@student.telkomuniversity.ac.id
[2]Faculty of Electrical Engineering, Telkom University Bandung, Indonesia, rendymunadi@telkomuniversity.ac.id
[3]Faculty of Economics and Business, Telkom University Bandung, Indonesia, helnimj@telkomuniversity.ac.id

Corresponding Author: darakusumawati@student.telkomuniversity.ac.id[1]

Abstract: The increasing reliance on private networks in modern enterprise highlights the need for efficient and reliable network performance to support business operations. WAN is a backbone for connecting branch offices, enabling data exchange and coordination across geographically dispersed locations. However, maintaining optimal performance amidst growing traffic demands, latency issues, and packet loss remains a significant challenge. This study focuses on developing VPN technol ogy integrated with QoS management to enhance network reliability, scalability, and efficiency in WAN environments. By employing a simulated network emulator, the research evaluates key performance indicators such as latency, bandwidth utilization, and packet loss under varying network conditions. The study further integrates technoeconomic analysis to assess the feasibility of the proposed solution, considering capital expenditures, operational costs, and the financial viability of the implementation. Regulatory compliance is also considered, with a focus on ensuring that the proposed framework aligns with national and international laws and policies, particularly those governing private networks and WAN operations. The results aim to provide enterprises with a strategic approach to optimizing VPN and WAN performance while balancing operational demands, cost efficiency, and legal adherence. This comprehensive framework is expected to contribute to the development of sustainable network solutions for modern enterprise, ensuring improved productivity and business continuity in an increasingly connected digital landscape.

Keywords: Private Network, VPN, WAN, TechnoEconomy, Regulatory Compliance.

INTRODUCTION

In the rapidly evolving digital era, modern companies rely heavily on computer networks to support their business operations. Many companies with branch offices in various locations rely on a Wide Area Network (WAN) to stay connected efficiently.

However, the biggest challenge in using WAN is ensuring that network performance remains optimal, especially in the face of various conditions. One solution that is widely used by companies to overcome this challenge is to implement Virtual Private Network (VPN) technology. VPN allows companies to connect private networks through the public internet or WAN in a secure way through data encryption[1]. Using a VPN, companies can ensure that the data sent and received remains protected, even through unsecured channels. In addition, a VPN allows employees or business partners to access the company's internal network remotely, increasing flexibility and productivity.

VPN is a communication technology that makes it possible to connect to a public network and use it to join a local network [1]. However, the use of VPN on WAN networks often faces challenges related to Quality of Service (QoS). QoS is an important element in network management to prioritize bandwidth usage, reduce la tency, and improve connection reliability. Without good QoS management, critical applications and network usage can experience disruptions that negatively impact operations [2]. The challenge of maintaining network quality over WAN demands a more efficient and secure solution.

Therefore, this research focuses on the development and application of optimized VPN technology with QoS management to improve the performance of enterprise networks using WAN. By developing more effective methods of imple menting VPN and QoS, enterprises are expected to achieve higher levels of network reliability and efficiency, which in turn will improve productivity and business sus tainability. In this study, the QoS measurement will be based on practical usage scenarios within the company, such as the use of an attendance website. This appli cation serves as an example of realworld usage, where the website relies on VPN connectivity for data transmission and consistent access across various locations. As a result, the QoS methods implemented in this research will be tailored to meet the specific requirements of the attendance website, focusing on reducing latency, ensuring reliable bandwidth allocation, and minimizing packet loss to support opti mal user experience and operational efficiency. This research aims to formulate an appropriate strategy for developing an enterprise private network by utilizing VPN and QoS technologies within a WAN environment. The proposed solution will be tested and evaluated to see to what extent improvements in network service quality can be achieved, as well as how network security and efficiency can be further enhanced to support the increasingly complex operational needs of the enterprise.

In the growing digital era, computer networks have become the backbone of modern enterprise operations [3]. Reliance on WAN that allow branch offices in various locations to remain connected creates its challenges for companies, especially in maintaining optimal network performance. This condition is especially relevant for the Indonesian economy, which is increasingly driven by digitalization. Companies that are unable to maintain network quality risk losing productivity and competitiveness in an everevolving global market [4].

From an economic perspective, network optimization through the implementation of technologies such as VPN is crucial in supporting the efficiency and effectiveness of company operations. VPN allows companies to connect private networks through public internet lines securely while enabling remote access for employees and business partners [5]. With better network performance, companies can maximize bandwidth usage, reduce latency, and ensure that the network used can run smoothly. This will increase the productivity, operational efficiency, and profitability of the company. In addition, proper implementation of QoS management also has a significant economic impact. In the application of technology used to determine the feasibility of implementation in private network research, it is neces sary to analyze the economic feasibility that will be calculated using the Capital Ex penditure (CAPEX), Operational Expenditure (OPEX), Net Present Value (NPV), Internal Rate of Return (IRR), Profitability Index (PI), and Payback Period (PP) methods[6].

In terms of regulations, especially private networks, there are no regulations governing them because private networks are only used in internal cases. The ap plication of VPN and QoS technology must also comply with various regulations that apply in Indonesia. The Indonesian government through Law No. 11/2008 on Electronic Information and Transactions (ITE) regulates the safe and responsible use of information technology. In this context, companies must ensure that VPN use and QoS management are in line with personal data protection regulations as well as increasingly stringent cybersecurity policies. On the other hand, regulations relating to network management also require companies to ensure the security of the data they manage, especially in highly regulated industries such as finance and healthcare. By following the security standards set by the government, such as Government Regulation No. 82/2012 on the Implementation of Electronic Systems and Transactions, companies can not only ensure compliance with regulations but also protect themselves from potential legal sanctions that may arise from data protection violations. Therefore, this research focuses on developing VPN technology and QoS management that not only improves network performance and operational efficiency but also complies with applicable regulations, thus providing a compre hensive solution for enterprise in Indonesia.

METHOD

Overview

This research focuses on developing and optimizing VPN technology, integrated with QoS management, to enhance network performance on WAN in enterprise environments. The study explores how VPN can be optimized to ensure secure communication across public or wide-area networks, improving flexibility, productivity, and data security. As VPN are widely used to connect multiple branch offices se- curely, this research is essential to address the limitations in maintaining consistent network performance.

The implementation is carried out using a network emulator that simulates a real-world corporate WAN environment, connecting various branch offices through VPN technology with QoS optimization. The performance and reliability of the proposed system will be evaluated through technical analysis, operational efficiency assessments, and network performance tests.

System Model and Scenarios

This study utilizes a simulated environment to test the effectiveness of VPN combined with QoS management. The network model includes the design and implementation of a WAN architecture that uses VPN technology to connect several branch offices. The proposed solution focuses on optimizing the use of bandwidth, reducing latency, and improving connection reliability by integrating QoS. The topology designed for the network simulator includes the following compo- nents:

- **Central Router**: Serves as the VPN hub, managing connections across branch networks and distributing QoS controls.
- **Branch Routers and Hosts**: Five edge routers represent branch offices, configured with QoS settings to prioritize data flow.
- **QoS Mechanisms**: QoS performance is monitored by observing key parameters—such as latency, jitter, packet loss, and bandwidth utilization—during real-time application usage to ensure the network can maintain reliable ser- vice quality for essential applications and services.

Simulation Scenarios

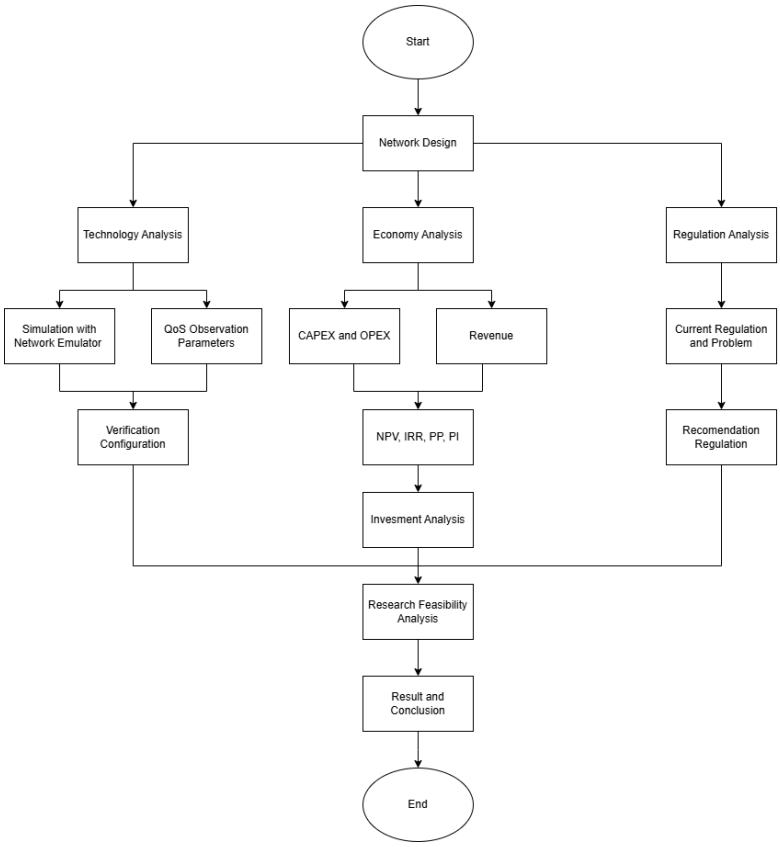

Figure 1. Research Methodology Flowchart

The simulation is conducted using network emulator software to represent a WAN connecting multiple branch offices. The system utilizes VPN as the private communication channel and implements QoS management to ensure high performance and reliability. The overall process is illustrated in Figure 1, which presents the research methodology flowchart with QoS observation, encompassing technological, economic, and regulatory analyses. The simulation steps are as follows:

1. Initial Setup
   Establish a VPN connection across the WAN, simulating the network archi- tecture between the central office and branch offices. This step involves configuring the VPN software and setting up basic network parameters.
2. QoS Optimization
   Optimize QoS by monitoring key performance indicators such as latency, jitter, packet loss, and bandwidth utilization to ensure critical applications receive adequate network resources. This process involves evaluating application behavior under simulated traffic conditions and verifying that network performance remains stable and reliable across all endpoints.
3. Network Performance Evaluation
   Measure network performance, including latency, bandwidth utilization, and packet loss, to evaluate the integration of VPN and QoS. The collected data is analyzed to gain insights into optimal network performance.
   The emulator generates network performance data to reflect the response to realworld challenges such as bandwidth allocation, latency, and network stability. The analysis results will inform the development of more efficient network strategies

RESULT AND DISCUSSION

Technical Analysis

Network Topology

The network topology illustrated in this study was designed using Cisco Packet Tracer to simulate a secure communication infrastructure between two government offices. It represents the practical implementation of a private Wide Area Network (WAN) supported by VPN tunneling to ensure secure inter-site data exchange. This simulation highlights the logical and physical arrangement of routers, switches, servers, and end devices across two buildings (provincial and municipal offices), connected via a GRE over IPsec VPN. The topology provides a clear visualization of how encrypted traffic flows between the two locations, reinforcing the security, reliability, and scalability of a VPN-based WAN deployment in a government envi- ronment.

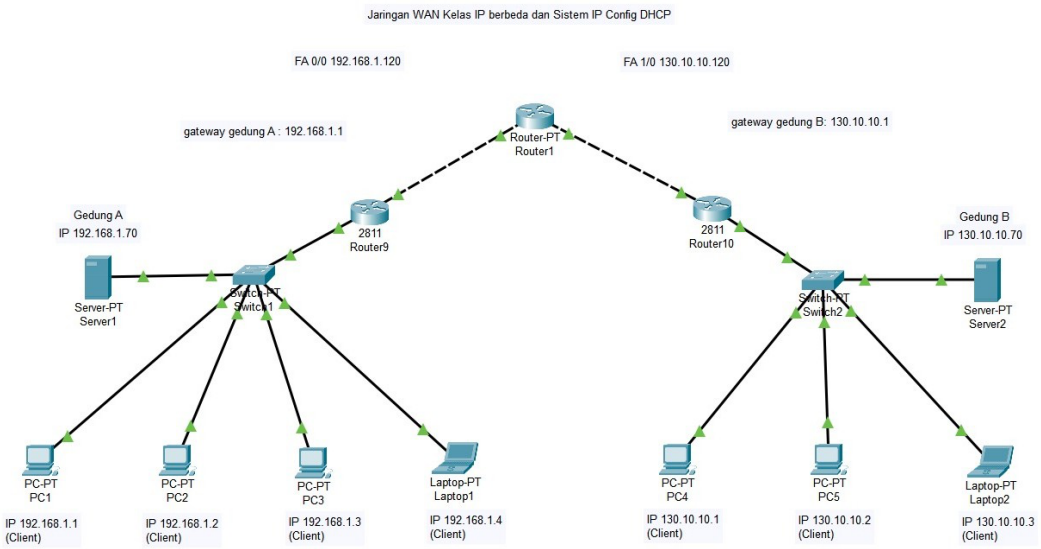

Figure 2. Network Topology

Cisco Packet Tracer was used to design the network topology presented in Figure 2, which illustrates a secure communication infrastructure between two gov- ernment offices: Building A (Provincial Diskominfo) and Building B (Municipal Diskominfo). These two sites are connected via a public network using a VPN (Virtual Private Network) configuration that implements GRE over IPsec tunneling. The main objective of this network setup is to secure data transmission across the WAN (Wide Area Network), ensuring confidentiality and integrity of government communications.

In this simulation, each building operates under a different IP address class, with Building A using the 192.168.1.0/24 network and Building B using the 130.10.10.0/24 network. Routers are statically configured to route traffic through a secure VPN tunnel established between the two Cisco 2811 routers. Router1 functions as the central point in the public network, facilitating site-to-site VPN communication.

Building A hosts a web server used to manage a simple HTMLbased attendance application. This server is not publicly accessible and can only be reached from within the local network or remotely from Building B through the VPN tunnel.

This setup enhances data security by restricting access to sensitive information and ensuring all traffic is encrypted before crossing the public network.

Local switches connect multiple end-user devices such as PCs and laptops within each building, allowing internal access to the web application and network resources. Building B also contains a backup server to support failover operations or to synchronize data with the main server.

The VPN configuration uses GRE over IPsec to encapsulate and encrypt data, which ensures that the information exchanged between both locations remains protected from interception or tampering. Static routing enhances network stability by minimizing routing overhead, while IPsec provides robust authentication, encryption, and integrity checks.

Overall, this topology supports a resilient digital infrastructure for government offices. It enables secure inter-office communication, supports the implementation of electronic-based government systems (SPBE), and protects mission-critical applications such as attendance tracking and internal data management services.

IP Addressing Scheme

To ensure effective communication and seamless data transmission across all nodes in the VPN-based WAN topology, a structured IP addressing scheme is implemented. Each device, including routers, tunnel interfaces, firewalls, web servers, and client PCs, is assigned a specific IP address according to its location and network role. The IP scheme supports logical segmentation between the central office (Gedung A), intermediary router (Router Tengah), and branch office (Gedung B), enabling secure tunneling via GRE over IPsec. Table 1 presents the detailed device list with corresponding IP addresses and physical locations within the simu- lated network. By clearly defining the addressing plan, the system ensures efficient routing, easier troubleshooting, and better control over traffic flow across the net-work. This structure also plays a crucial role in supporting the VPN configuration, as each IP assignment contributes to accurate tunnel establishment, access control, and secure data forwarding. Such clarity in addressing enhances the overall security posture and operational efficiency of the WAN environment deployed across the two sites.

Table 1 presents the IP addressing scheme used across all devices in the simulated VPN-based WAN topology. Each device is assigned a unique IP address corresponding to its function and physical location, whether in the central office (Gedung A), intermediary router (Router Tengah), or branch office (Gedung B). The addressing plan covers web servers, LAN and WAN interfaces of routers, GRE.

Table 1. Device List with IP Addresses and Locations

Device	IP Address	Location
Web Server	192.168.1.10	Gedung A
Router Gedung A (LAN)	192.168.1.120	Gedung A
Router Gedung A (WAN)	192.168.2.1	Gedung A
Tunnel Interface Gedung A	10.10.10.1	Gedung A
Router Tengah (to Gedung A)	192.168.2.2	Router Tengah
Router Tengah (to Gedung B)	9.9.9.1	Router Tengah
Router Gedung B (WAN)	9.9.9.2	Gedung B
Router Gedung B (LAN)	130.10.10.120	Gedung B
Tunnel Interface Gedung B	10.10.10.2	Gedung B
PC Client Gedung B	130.10.0.1	Gedung B

Tunnel interfaces, and end-user client PCs. This structured IP configuration ensures seamless data routing, secure VPN tunneling, and clear segmentation between network zones, forming the foundation for stable and encrypted communication across the WAN infrastructure.

Conclusion of Analytical Technical

Based on the simulation results and technical analysis, it can be concluded that the proposed VPNbased private network topology is technically feasible and operates effectively in a simulated WAN environment. The implementation of site to site VPN ensures secure

communication between branch offices and enables centralized access to web-based services such as the internal attendance system.

The network simulation using Cisco Packet Tracer successfully demonstrates that the infrastructure is capable of maintaining stable and reliable performance. This is evidenced by the acceptable values of key QoS parameters, including latency, jitter, packet loss, and bandwidth utilization, which were observed during realtime application testing.

Furthermore, the integration of VPN and web application services reflects a practical enterprise network scenario, where data protection and service availability are essential. The topology design and its successful implementation provide a strong foundation for proceeding to the economic and regulatory feasibility evalua- tions, ensuring that the network is not only secure and efficient but also suitable for real-world deployment.

Economic Analysis

CAPEX and OPEX Fee Plan

In planning the development of a private enterprise network using a VPNbased Wide Area Network (WAN) topology, the budget is categorized into two primary components: Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). CAPEX encompasses all upfront costs required for building and deploying the physical and digital infrastructure needed to support the system's core functionality. Table 2 CAPEX list for deploying VPN Technology over WAN.

Table 2. CAPEX Cost for Private VPN-Based WAN Infrastructure

Item	**Item Price**	**Qty**	**Total**
Cisco Router 2811	Rp5.000.000	3	Rp15.000.000
Web Server (Intel Xeon, 16GB RAM)	Rp7.500.000	2	Rp15.000.000
Switch Layer 2 (TP-Link TL-SG1024DE)	Rp900.000	2	Rp1.800.000
UPS Backup (Prolink 650VA)	Rp1.000.000	2	Rp2.000.000
Mini Server Rack	Rp2.000.000	1	Rp2.000.000
LAN Cable, Patch Panel, RJ- 45	Rp1.000.000	1	Rp1.000.000
Admin Laptop (Core i5, 8GB RAM)	Rp6.500.000	2	Rp13.000.000
PC Client (Core i5, 8GB RAM, SSD)	Rp4.500.000	5	Rp22.500.000
Monitor 24" (AOC / LG LED)	Rp1.300.000	5	Rp6.500.000
Office Desk + Chair	Rp1.000.000	7	Rp7.000.000
Printer Shared (HP DeskJet All-in-One)	Rp2.000.000	1	Rp2.000.000
Mini Projector 2800 Lumens	Rp3.500.000	1	Rp3.500.000
Installation & Configuration	Rp5.000.000	1	Rp5.000.000
Contingency Fee (10%)			Rp9.330.000
Grand Total			**Rp102.630.000**

These include procurement of routers, switches, servers, power supply equipment, and other supporting hardware, as well as network installation and configuration. As a one-time investment, these assets serve as the foundation for establishing secure interbranch communication via VPN tunneling across the WAN topology.

Meanwhile, OPEX represents the recurring expenses required for the operation and maintenance of the network infrastructure throughout the life cycle of the project, typically five years. This includes electricity consumption, Internet subscriptions, hardware maintenance, and IT support services. Categorizing costs in this way enables structured and predictable financial planning, ensuring that the network remains sustainable and efficient over time.

Table 2 outlines the detailed CAPEX required for implementing a simple but reliable VPN-based WAN infrastructure. Cisco 2811 routers are selected to serve as core routing devices at each VPN endpoint, enabling IPsec-based site-to-site tunneling and static routing for secure data exchange. Web server machines powered by Intel Xeon processors with 16GB RAM function as internal application servers, such as for attendance tracking. TP-Link TL-SG1024DE switches are deployed to manage Layer 2 traffic at each node, ensuring seamless communication among local devices.

To protect against power failures, Prolink 650VA UPS units are installed, while a mini server rack organizes critical equipment centrally. The network's physical layer is supported by LAN cables, patch panels, and RJ-45 connectors to ensure structured cabling. Admin laptops and PC clients with Core i5 processors and SSD storage are provided to IT staff and end users, while 24-inch monitors improve usability and monitoring accuracy.

Basic office facilities such as desks, ergonomic chairs, shared printers, and a mini projector support day-to-day operations and documentation. A dedicated cost for configuration and installation is also allocated, ensuring all hardware is prop- erly connected and tested. Every component listed has been selected based on compatibility, performance efficiency, and cost-effectiveness to support the secure, scalable, and maintainable deployment of a private VPNbased network that meets enterprise-level standards for Quality of Service (QoS) across a multi-site WAN topology.

In summary, the capital expenditures detailed above lay a robust foundation for a secure, high-performance private network infrastructure that enables seamless interoffice communication through VPN tunneling and QoS enforcement. With all critical components strategically selected to balance functionality and cost, this investment ensures long-term operational stability. Following this CAPEX breakdown, the next section presents a comprehensive OPEX cost table, which outlines the anticipated annual operating expenses necessary to sustain and manage the network infrastructure throughout the five-year project lifecycle.

Table 3. Annual OPEX Cost for VPN-Based WAN Network

Item	**Item Price**	**Qty**	**Period (Months)**	**Total**
Internet Subscription (20 Mbps/site)	Rp1.500.000	2 sites	12	Rp36.000.000
Electricity for Network De- vices	Rp300.000	2 sites	12	Rp7.200.000
Hardware Maintenance (Router, Server)	Rp2.500.000	1 package	12	Rp2.500.000
IT Support Services (Free- lance / SLA)	Rp1.500.000	1 person	12	Rp18.000.000
Software License & An- tivirus Updates	Rp1.000.000	1 license	12	Rp1.000.000
Cloud Backup Storage (100GB/site)	Rp250.000	2 sites	12	Rp6.000.000
VPN License (IPsec/SSL Paid)	Rp500.000	2 sites	12	Rp1.000.000
Air Conditioner Mainte- nance	Rp500.000	2 units	12	Rp1.000.000
Travel Allowance (IT site visit)	Rp300.000	per visit	6	Rp1.800.000
Total				**Rp74.500.000**

This table outlines the annual operational costs required to maintain the private network based on VPN. The main components include technical support, hardware maintenance, as well as Internet service and electricity consumption, which ensure the continuous functionality of the infrastructure. Additional expenses cover software licenses, cloud backup

storage, and technician travel for on-site monitoring. The total estimated operating cost per year is IDR 74,500,000.

Table 4. Projected Cost of Operations

Period (Year)	Expense (IDR)	Depreciation (IDR)	Total (IDR)
1	Rp177.630.000	Rp20.526.000	Rp198.156.000
2	Rp79.715.000	Rp20.526.000	Rp100.241.000
3	Rp85.294.050	Rp20.526.000	Rp105.820.050
4	Rp91.264.634	Rp20.526.000	Rp111.790.634
5	Rp97.654.158	Rp20.526.000	Rp118.180.158

Table 4 presents the projected operational costs over a five-year period for maintaining a VPN-based WAN infrastructure implemented across one central office and several connected branch offices. The projection accounts for both annual OPEX and asset depreciation. Operating costs are expected to rise progressively each year to reflect inflation and the scaling needs of IT services. Specifically, technical support and laborrelated services are estimated to increase by 10% annually, while other components such as electricity, internet subscriptions, auditing, train- ing, maintenance, and software licensing are projected to grow at a more stable rate of 5% per year. This escalation reflects a sustainable and realistic model of ongoing operational expenditure. Alongside OPEX, depreciation of capital expenditures is calculated using the straightline method, which distributes the total cost of equipment evenly across its useful life of five years. This allows for a consistent recognition of asset value reduction over time. The figures in the table combine both OPEX and depreciation to provide a comprehensive view of the total annual financial commitment required to sustain the infrastructure.

To estimate the depreciation of the investment, a straightline depreciation method is used. The investment cost is based on the total capital expenditure of IDR 102,630,000. The residual value is estimated to be 10% of the total investment, or IDR 10,263,000. The useful life of the assets is assumed to be 5 years.

$$\text{Annual Depreciation} = \frac{\text{Investment Cost} - \text{Residual Value}}{\text{Useful Life}} = \frac{102,630,000 - 10,263,000}{5} = 18,473,400 \quad (4.1)$$

This depreciation estimate ensures a structured spread of the capital investment over time, allowing the organization to allocate costs consistently and predictably throughout the useful life of the assets. By distributing the capital expenditure evenly over five years using the straight-line method, the institution can avoid sudden budgetary shocks and maintain a stable financial outlook. This approach supports clear visibility into annual accounting for asset value reduction, enabling better tracking of equipment aging and facilitating compliance with standard accounting principles. Moreover, it improves longterm financial planning and cost control by providing a reliable basis for forecasting replacement cycles, optimizing investment timing, and supporting sustainability in infrastructure management.

Revenue Projection

In the implementation of a private network using VPN technology across multiple government offices, revenue projection plays a critical role in evaluating the financial viability of the project. Revenue in this context refers to the estimated eco- nomic value generated from the delivery of network-based services, such as VPN site-to-site access,

application hosting, and technical support. These services are assumed to be utilized by internal stakeholders, including provincial and municipal Diskominfo offices, as well as affiliated institutions, either as direct cost-recovery mechanisms or in lieu of outsourcing to third party providers. Proposed revenue helps determine return on investment (ROI) and supports long-term planning for infrastructure sustainability, particularly in publicly funded ICT projects.

Table 5. Security Service Revenue Projection

Service Category	**Unit Price (IDR)**	**Quantity**	**Total (IDR)**
VPN Site-to-Site Access Service	1.000.000	600	600.000.000
Web-Based Application Hosting (Absensi)	1.200.000	300	360.000.000
Technical Support and Maintenance	1.500.000	200	300.000.000
Total Transactions			**1.100**
Total Revenue			**1.260.000.000**

Illustrates the projected revenue generated from core services offered through the VPN-based private network infrastructure, including VPN site-to-site access, web-based application hosting, and technical support and maintenance services. These services represent essential components derived directly from the implemented network architecture and are aligned with the capital and operational expenditures of the project. The quantity for each category reflects a realistic estimate of service usage within interagency communication environments, such as provincial and municipal Diskominfo offices. The total transactions are projected to reach 1,100 in the first year, resulting in an estimated revenue of IDR 1,260,000,000.

Table 6. Projected Revenue

Year	**Service Transactions (est.)**	**Annual Revenue (IDR)**
1	1.100	1.260.000.000
2	1.210	1.386.000.000
3	1.331	1.524.600.000
4	1.464	1.677.060.000
5	1.610	1.844.766.000
Total Revenue (5 years)		**7.692.426.000**

Presents the projected revenue over a five-year period based on a 10% annual growth assumption in service usage. This increase reflects expanding demand for secure and reliable network services among government agencies as digital transformation accelerates. The projection assumes proportional growth in all service categories from the baseline year. As a result, the revenue increases from IDR 1,260,000,000 in the first year to IDR 1,844,766,000 in the fifth year. Over the full period, the total projected revenue is expected to reach IDR 7,692,426,000, providing a solid financial foundation for evaluating the long-term viability of the infrastructure.

Table 7. Projection Tax

Year	**EBITDA (IDR)**	**EBIT (IDR)**	**Tax 10% (IDR)**	**Net Income (IDR)**
1	441.000.000	422.526.600	42.252.660	380.273.940
2	485.100.000	466.626.600	46.662.660	419.963.940
3	533.610.000	515.136.600	51.513.660	463.622.940
4	586.971.000	568.497.600	56.849.760	511.647.840
5	645.668.100	627.194.700	62.719.470	564.475.230

Table 7 presents the financial projection of tax-related performance over the next five years, focusing on four key financial indicators: EBITDA, EBIT, Tax, and Net Income. EBITDA (Earnings Before Interest, Taxes, Depreciation, and Amortization) represents the organization's gross operational earnings before non operating expenses are deducted, and is calculated as a fixed proportion 35% of the total annual revenue derived from the VPN-based WAN services. EBITDA reflects the profitability of the system's core operations, excluding capital structure and non-cash expenses.

$$\text{EBIT} = \text{EBITDA} - \text{Depreciation}$$

EBIT (Earnings Before Interest and Taxes) is calculated by subtracting the annual depreciation expense from EBITDA. The depreciation follows the straightline method, using an initial capital expenditure of IDR 102,630,000 with a 10% residual value and a five-year useful life, resulting in an annual depreciation of IDR 18,473,400. EBIT provides a more refined insight into operational performance by factoring in the aging and usage of fixed assets. The projection indicates steady growth in EBIT from IDR 422,526,600 in the first year to IDR 627,194,700 in the fifth year, demonstrating the system's increasing operational efficiency.

$$\text{Net Cash Flow} = \text{EBIT}\,(1 - \text{Tax Rate}) - \Delta\text{CAPEX} - \Delta\text{Working Capital}$$

Taxes are calculated at a fixed rate of 10% of EBIT, representing the organization's annual tax liability. As EBIT increases over time, tax obligations also grow proportionally from IDR 42,252,660 in the first year to IDR 62,719,470 in the fifth year. Net income, which represents the remaining profit after tax, reflects the fi- nancial health and sustainability of the project. The projection shows net income rising consistently from IDR 380,273,940 in the first year to IDR 564,475,230 in the fifth year. This trend illustrates the positive return potential of the investment and the financial viability of maintaining and operating a private VPN network across multiple sites. Overall, the projection underscores strong and stable financial per- formance, driven by efficient cost management and increasing service demand.

Feasibility Analysis

To evaluate the financial feasibility of the proposed VPN-based private network, this study uses several investment appraisal techniques. Net Present Value (NPV), Internal Rate of Return (IRR), Profitability Index (PI), and Payback Period (PP). These metrics are used to determine the value, risk, and return of the project over the five-year period. NPV measures the present value of future cash flows against the initial investment, while IRR indicates the discount rate at which the NPV becomes zero. The payback period estimates how long it takes to recover the initial capital. These indicators provide a comprehensive financial perspective to support decisionmaking and assess the project's economic viability.

Conclusion Techno-Economic Analysis

The techno-economic analysis conducted for the VPN-based private network over WAN implementation in government offices provides a comprehensive assessment of the project's financial viability. By applying key financial metrics such as NPV, IRR, PI, and PP, the evaluation demonstrates the economic benefits and investment feasibility of the project under a 10% discount rate assumption. These indicators offer valuable insights into the return on investment and risk mitigation for long-term infrastructure planning in the public sector.

Table 8. Economic Analysis Results

Discount Rate	10%
NPV	IDR 1,534,500,796
IRR	43.92%
PI	15.95
PP	0.22 years

Based on the results of the economic analysis in Table 8, this study shows that the proposed project is highly feasible and provides significant financial benefits. This conclusion was obtained through an in-depth evaluation using key economic indicators. A positive NPV of IDR 1,534,500,796 demonstrates that the project will yield returns exceeding its initial investment when evaluated at a 10% discount rate. Additionally, an IRR of 43.92% far surpasses the assumed cost of capital, indicating a strong return-generating capacity. The PI value of 15.95, well above the threshold of 1, confirms that the project's benefits substantially outweigh the costs. Furthermore, the very short Payback Period of just 0.22 years indicates that the initial investment can be recovered quickly, thus minimizing financial risk and supporting efficient capital allocation. Overall, these results confirm the project's viability and strategic value as a long-term infrastructure investment.

Regulation Analysis

Policy Brief Introduction

In the era of digital transformation, particularly in the public sector, data se- curity and inter-agency communication have become critical aspects in supporting efficient and integrated public services. To address these challenges, implementing a private network based on VPN (Virtual Private Network) with QoS (Quality of Service) support through WAN (Wide Area Network) infrastructure is a strategic solution to ensure confidentiality, integrity, and efficient data communication between provincial and municipal government offices.

VPN technology enables encrypted and secure data transmission between government institutions, thus minimizing the risk of cyberattacks and data breaches. The integration of QoS functions to maintain the performance of essential services, such as attendance applications, employee information systems, and SPBE (Electronic Based Government System) platforms, ensures prioritization of critical network traffic.

This regulation analysis focuses on two main areas: (1) security and data protection aspects for all stakeholders involved in VPN and QoS implementation within government infrastructure, and (2) licensing and fiscal impact on non-tax state rev- enue (PNBP), aligned with the Electronic-Based Government System (SPBE) reg- ulatory framework and related digital governance policies.

Problem Identification

Despite the availability of technology, the implementation of VPN and QoSbased private networks in government infrastructure faces several regulatory and policy-related challenges:

1. Lack of National Technical Standards

   Although the SPBE Presidential Regulation emphasizes security and interoperability, there is no technical standard specifically governing VPN and QoS usage at the regional government level. This results in inconsistent implementation and potential performance gaps between regions.

   Risk of Data Breach and Cyber Threats While VPN provides secure data paths, poor configuration and lack of security audits increase the risk of data leaks. The Personal Data

Protection (PDP) Law mandates end-to-end pro- tection with lawful, fair, and transparent principles—many of which remain unfulfilled in regional governments.
2. Unclear Funding and Budget Responsibilities Budgetary responsibility between central and regional governments for infrastructure costs is ambiguous. Additionally, obligations related to frequency usage fees (BHP) and universal service obligations (USO) for government-owned private networks are not clearly regulated.
3. Weak Oversight and Security Auditing VPN usage and QoS performance monitoring remain weak, especially at the city/district level. This opens up the possibility for network misconfigurations, misuse, or undetected ineffi- ciencies.
4. Regulatory Overlap Between Public and Commercial Sectors The Telecommunications Law still classifies private networks under "special telecommunications," but lacks explicit provisions for government implementation. This may lead to legal ambiguity and varying interpretations.

SWOT Analysis of Regulation

The implementation of VPN and QoS-based private networks in government infrastructures offers strategic benefits but also faces regulatory and operational challenges. A SWOT analysis in table 9 highlights key internal and external factors. Internally, strengths include enhanced inter-government communication and support for digital services like SPBE, while weaknesses involve a lack of technical standards and overlapping regulations. Externally, opportunities lie in regulatory reform and improved cybersecurity, whereas threats include policy ambiguity, fragmented budgets, and misuse risks. Recognizing these factors is essential to ensure alignment between technology strategies and sustainable governance.

Table 9. SWOT Analysis of VPN and QoS-Based Private Network

Strengths	**Weaknesses**
- Enhances secure communication between government institutions through VPN. - QoS guarantees priority for critical services such as employee systems and SPBE. - Supports efficient and integrated SPBE.	- No national standard for VPN-QoS use at local government levels. - Overlapping regulations between public and commercial telecommunication services.
Opportunities	**Threats**
- Potential for regulatory reform (e.g., revision of SPBE and PSTE) to support infrastructure. - Strengthening regional cyber- - security through private network standardization.	- Potential misuse of VPN by internal users. - Budget fragmentation between central and local governments may hinder implementation.

Related Regulations

The deployment of VPN and QoS technologies within government settings must adhere to a variety of regulatory frameworks that govern electronic systems, data protection, and telecommunication infrastructure. These regulations form the legal foundation ensuring secure, lawful, and efficient network operations. Among them are laws on electronic transactions (ITE), personal data protection (PDP), and governance of electronic-based government systems (SPBE), alongside ministerial and telecommunications regulations. These instruments guide licensing requirements, data governance practices, and infrastructure classification. The following table summarizes the key legal frameworks relevant to this study, highlighting their relevance to the secure implementation of government-wide VPN-

based networks. These frameworks also support alignment with national digital transformation goals. Table 10 outlines the primary regulations relevant to this study. As government services continue to digitize, regulatory compliance becomes increasingly critical for sustainable and secure network infrastructure.

Table 10. Policy Brief Related Regulation

No	Regulation	Relevance
1	Law No. 11 Year 2008 on Electronic Information and Transac-tions (ITE)	Security of electronic systems and data transactions
2	Law No. 27 Year 2022 on Personal Data Protection (PDP)	Protection of personal data of civil servants and citizens
3	Government Regulation No. 71 Year 2019 on Electronic Systems and Transactions (PSTE)	Obligations of government sys-tem providers
4	Presidential Regulation No. 95 Year 2018 on SPBE	Governance of digital government systems
5	Law No. 36 Year 1999 on Telecommunications	Classification and regulation of private networks
6	Ministerial Regulation No. 5 Year 2021 by Kominfo	Licensing and operation of telecommunication networks

Regulatory Impact

1. Increased Compliance with SPBE Indicators VPN and QoS support SPBE goals, particularly in infrastructure and information security.
2. Harmonization of Budgeting Central and local governments must coordinate budget mechanisms to finance secure private network infrastructure.
3. Potential Increase in Operational Costs If BHP/USO obligations are applied to government networks, additional costs will arise.
4. Expansion of Service Coverage A well-structured private network will enhance SPBE service delivery, especially to remote areas.

Policy Recommendations

1. Development of National Technical Guidelines for VPN and QoS Jointly issued by BSSN, Kominfo, and SPBE Coordination Team to standardize infrastructure for regional use.
2. Revision of PP 71/2019 and SPBE Indicators To include VPN and QoS as official components in evaluating digital government security.
3. VPN Compliance with PDP Law VPN usage must include encryption, access logging, and data retention policies aligned with data protection principles.
4. Strengthening SPBE Monitoring and Auditing Real-time monitoring mechanisms for VPN usage and network performance should be integrated to ensure accountability and operational efficiency.

Regulation Analysis on Licensing and PNBP Potential of VPN Technology in Government

Policy Brief Introduction

The Government of Indonesia, through Government Regulation No. 43 of 2023, has defined the classification and tariffs for types of Non-Tax State Revenue (PNBP) originating from digital activities, including the use of VPN-based networks within government agencies. The deployment of VPN systems with encryption, logging, and sensitive data processing features is subject to PNBP when classified under Electronic System Operators (PSE).

Revenue from this sector can strengthen national digital infrastructure funding. However, gaps remain regarding regulatory clarity on PNBP obligations, budget governance, and institutional compliance with reporting and payment mechanisms.

Problem Identification in Policy Brief

1. Absence of Specific Regulation for PNBP on Government-Owned Private Networks
   Agencies like Diskominfo, which intensively utilize VPNs, currently lack formal guidelines for managing related PNBP obligations.
2. PNBP May Increase Operational Costs for Local Governments
   If PNBP calculations are based on the number of endpoints or VPN nodes, regions with more branches or municipalities may bear heavier financial burdens.
3. Lack of Transparency in PNBP Utilization
   There is no clear regulation on how collected PNBP from IT-related services is reinvested into enhancing public digital infrastructure.
4. Overlap in Legal Status of Commercial vs. Government PSE
   Government VPN providers need to be regulated separately from commercial PSEs to avoid unfair tariff burdens.

SWOT Analysis of PNBP Regulation for Government VPNs

Table 11. SWOT Analysis of VPN-Based PNBP Regulation in Government

Strengths	**Weaknesses**
- Provides additional national revenue source from technology infrastructure. - Promotes accountability in government IT systems.	- Imposes additional operational costs on regional governments. - Absence of specific PNBP framework for public institutions.
Opportunities	**Threats**
- PNBP funds can be allocated for training, village digitalization, or cybersecurity upgrades.	- VPN adoption might decline due to perceived high costs. - Legal uncertainty over VPN classification as a PSE.

Related Regulations

The imposition of PNBP on government networks is guided by various legal instruments. These regulations determine the types, rates, governance, and reinvestment of state revenue from digital services. Table 12 summarizes the relevant rules and policies.

Table 12. Policy Brief Related Regulation on VPN and PNBP

No	**Regulation**	**Relevance**
1	Government Regulation No. 43 Year 2023	Classification and tariff of PNBP in the ICT sector
2	Law No. 9 Year 2018 on Non-Tax State Revenue (PNBP)	Legal basis for state revenue collection from public services

3	Presidential Regulation No. 95 Year 2018 on SPBE	Reinvestment of PNBP to strengthen digital governance
4	Ministerial Regulation No. 10 Year 2021 by Kominfo	Regulation of public and private Electronic System Operators (PSE)

Policy Recommendations

1. Revision of Government Regulation No. 43/2023 to Include Government Networks
   Update the regulation to specifically cover VPN, firewall, and network management systems used in public infrastructure.
2. Utilization of PNBP for Strengthening Local Digital Infrastructure
   Allocate PNBP funds to support cybersecurity training, public digital literacy, and secure hardware procurement at the regional level.
3. Classification of VPN as a Special PSE for Government Use
   This prevents the application of commercial tariffs and ensures fairness in regulation.
4. Transparency in Digital Sector PNBP Utilization
   Mandate all Diskominfo agencies to upload PNBP allocation reports into the national SPBE dashboard for public access and monitoring.

CONCLUSION

This thesis presents a comprehensive simulation and evaluation of a private enterprise network using VPN technology integrated with Quality of Service (QoS) mechanisms over a Wide Area Network (WAN). The simulation using Cisco Packet Tracer demonstrated that GRE over IPsec VPN successfully enables secure and stable communication between dispersed office branches. Key QoS metrics—such as throughput, latency, jitter, and packet loss—were measured, showing significant improvements after VPN activation, aligning with ITU-T standards. These results confirm the technical feasibility of the proposed model in supporting real-time, web-based enterprise applications, such as an internal attendance system.

From an economic perspective, the techno-economic analysis reveals that the project is financially viable and sustainable. With a total five-year investment of IDR 102 million and projected revenues exceeding IDR 7.6 billion, the analysis produced a positive Net Present Value (NPV) of IDR 1.53 billion, an Internal Rate of Return (IRR) of 43.92%, and a high Profitability Index (PI) of 15.95. These financial indicators, coupled with a short payback period, validate the economic efficiency of the VPN-based WAN model and support its adoption for secure and cost-effective digital infrastructure, particularly in government and enterprise environments.

Regulatory analysis further reinforces the project's alignment with Indonesian cybersecurity and data protection laws, including UU ITE, PP No. 71/2019, and UU PDP No. 27/2022. While specific regulations for private networks remain limited, this research ensures compliance with existing frameworks and provides a proactive approach toward responsible and secure network implementation. Overall, the proposed design offers a technically robust, economically sound, and legally compliant solution for modern enterprises seeking to enhance operational performance through secure and optimized WAN connectivity.

REFERENCES

A. T. Atmoko, A. S. Budiman, and N. Nuraeni, "Perancangan dan pengem- bangan virtual private network (vpn) menggunakan pptp pada pt indobinatu mitra sejati," *Jurnal Teknologi dan Sistem Informasi (JTSI)*, vol. 5, no. 1, pp. 160–170, April 2024.

M. Z. Chowdhury, M. N. Islam, Y. M. Seo, Y. K. Lee, S. B. Kang, S. W. Choi, and Y. M. Jang, "Characterizing qos parameters and application of soft- qos scheme for 3g wireless networks," *Neural Computing and Applications*, vol. 33, no. 8, pp. 3871–

3879, 2021.

B. W. Aulia, M. Rizki, P. Prindiyana, and Surgana, "Peran krusial jaringan komputer dan basis data dalam era digital," *JUSTINFO (Jurnal Sistem Infor- masi dan Teknologi Informasi)*, vol. 1, no. 1, pp. 160–170, December 2023.

A. Dresch, D. C. Collatto, and D. P. Lacerda, "Theoretical understanding between competitiveness and productivity: Firm level," *Ingenier´ıa y Competitividad*, vol. 20, no. 2, pp. 1–15, 2018. [Online]. Available: http://www.redalyc.org/articulo.oa?id=291361225007

S. Frankel, P. Hoffman, A. Orebaugh, and R. Park, "Guide to ssl vpns," National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-113, July 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf

A. A. of Port Authorities and U. D. of Transportation, "Port planning and investment toolkit," Maritime Administration (MARAD), United States, Tech. Rep., 2017. [Online]. Available: https://www.marad.dot.gov/ports/ strongports/port-planning-and-investment-toolkit/

C. B. D. R. Mauro Belgiovine, Kunal Sankhe and K. R. Chowdhury, "Deep learning at the edge for channel estimation in beyond-5g massive mimo," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 19–25, April 2021.

M. J. Fischer, D. M. B. Masi, and J. F. Shortle, "Simulating the performance of a class-based weighted fair queueing system," in *2008 Winter Simulation Conference*, 2008, pp. 2901–2908.

C. Huang and Z. Zhu, "Complex communication application identification and private network mining technology under a large-scale network," *Neural Com- puting and Applications*, vol. 33, no. 8, pp. 3871–3879, 2021.

NetworkLessons.com, "Introduction to wans (wide area network),"Network Lessons CCNA Routing & Switching ICND1 100-105, 2018. [Online]. Available: http://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ introduction-to-wans-wide-area-network

C. O. Corp., "What is vpn and how it works? vpn network diagram creating," April 2024.

C. Mancas and M. Mocanu, "Enhancing qos/qoe in multimedia networks," *IEEE International Conference on Communications: Workshop on Immersive & Interactive Multimedia Communications over the Future Internet*, pp. 637– 641, 2013.

D. A. Salman, R. Munadi, and R. Mayasari, "Analisis quality of service (qos) algoritma antrian cbwfq dan llq pada jaringan mpls-te," *e-Proceeding of Engineering*, vol. 3, no. 3, pp. 4585–4592, December 2016. [Online]. Available: https://repository.telkomuniversity.ac.id

W. Mulya, "Capital expenditure dan operational expenditure dalam perancangan instalasi pengolahan air di kota balikpapan," *Info Teknik*, vol. 23, no. 1, pp. 15–28, July 2022. [Online]. Available: http://ppjp.ulm.ac.id/journal/index.php/infoteknik

H. L.-V. Assche and T. Compernolle, "Economic feasibility studies for carbon capture and utilization technologies: A tutorial review," *Clean Technologies and Environmental Policy*, vol. 24, pp. 467–491, 2022. [Online]. Available: https://doi.org/10.1007/s10098-021-02128-6