Eduvest – Journal of Universal Studies
Volume 6 Number 1, January, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Development of GRE IPSec for Enhancing Private Network Scalability: Performance, Cost, and Regulatory Framework

Mochammad Iqbal Fahriza, Rendy Munadi, Helni Mutiarsih Jumhur
Telkom University, Indonesia
Email: mochammadiqbalf@student.telkomuniversity.ac.id,
rendymunadi@telkomuniversity.ac.id, helnimj@telkomuniversity.ac.id

ABSTRACT

This research explores the implementation of GRE IPSec private networks as a secure and cost-effective solution for data transmission in corporate environments. The primary objective is to address the challenges of ensuring secure data transfer over private networks while meeting technical, economic, and regulatory requirements, particularly within the context of Indonesia. Despite the growing adoption of private networks globally, there remains a significant research gap in understanding the techno-economic viability and regulatory compliance of GRE IPSec implementation in developing countries, particularly Indonesia, where regulatory frameworks for commercial private networks are still evolving. The research employs a comprehensive methodology that includes network topology design and simulation using GNS3, along with a regulatory review based on Indonesia's Electronic Information and Transaction Law (UU ITE). By examining the integration of GRE and IPSec protocols, this study evaluates their effectiveness in safeguarding sensitive corporate data when transmitted over public networks. The quantitative analysis reveals significant findings regarding technical performance and economic viability of GRE IPSec private networks. Metrics such as NPV, IRR, and profitability ratios indicate that the implementation of this network is economically feasible, yielding a positive return on investment. Furthermore, the study confirms enhanced data transmission security and compliance with legal standards, providing a robust framework for enterprises to develop secure, scalable, and compliant private network infrastructures in Indonesia. However, this study is limited by its reliance on simulated data rather than real-world deployment scenarios, and the regulatory analysis is confined to the Indonesian context, which may limit generalizability to other jurisdictions.

KEYWORDS *Private Network, GRE, IPSec, Techno Economic, Regulation.*

INTRODUCTION

In the era of digital transformation, organizations across various sectors face increasing challenges in ensuring information and communication security (Gebremeskel et al., 2023; Nowicka et al., 2024; Saeed et al., 2023). The rise in online transactions and interactions demands that companies safeguard the integrity, privacy, and security of data exchanged internally and with external partners (Wylde et al., 2022). The growing frequency and sophistication of cyberattacks have exposed the vulnerabilities of public networks, especially unsecured public Wi-Fi, where data is often transmitted without encryption (Sombatruang et al., 2022).

The implementation of Private Network technology using GRE (Generic Routing Encapsulation) IPSec provides a secure solution by encrypting and authenticating data transmitted over public networks such as the Internet (Kumar et al., 2020; Nair, 2024; Ogudo, 2019; Uddin et al., 2021). This technology enables secure communication channels between business partners and corporate systems, protecting sensitive information like financial transactions from unauthorized access (Sargiotis, 2024). Moreover, GRE IPSec supports network scalability and integration without requiring complex infrastructure, helping companies maintain operational quality and customer trust amid rising digital security threats (Bitbit et al., 2023).

In Indonesia, the regulatory context presents particular urgency due to the country's rapid digital transformation. Indonesia has experienced exponential growth in digital economy activities, with e-commerce, fintech, and digital services expanding at unprecedented rates. This rapid digitalization has intensified the need for secure private network infrastructures that can protect sensitive data while supporting business scalability. However, the existing regulatory frameworks have not kept pace with these technological advancements, creating legal uncertainties for enterprises seeking to implement commercial private networks. The government's efforts to strengthen cybersecurity through various regulations, including the Electronic Information and Transaction Law (UU ITE) and data protection requirements, underscore the critical need for clear guidelines on private network implementation.

Furthermore, the use of GRE IPSec aligns with regulatory requirements in Indonesia related to data privacy and information security, including the Electronic Information and Transaction Law (ITE) and telecommunications regulations (Parulian & Putranto, 2022). Although specific regulations governing private network use remain limited, existing laws provide a legal framework to ensure compliance. Nevertheless, there is a need for clearer regulations addressing private network implementation to support secure and lawful operations.

Previous research has explored various aspects of private network security and implementation. Karstensen et al. (2022) examined spectrum allocation challenges for private networks in Denmark, highlighting regulatory complexities in different jurisdictions. Rey (2024) demonstrated the effectiveness of IPsec protocols in law enforcement security systems, though focused primarily on public sector applications. Horisaki et al. (2024) proposed secure end-to-end communication architectures that traverse firewalls and NATs, addressing technical implementation challenges. However, these studies have not comprehensively addressed the intersection of technical performance, economic viability, and regulatory compliance in developing country contexts. This research gap is particularly significant for Indonesia, where commercial private network regulations remain underdeveloped, and enterprises require evidence-based guidance on implementation strategies.

What distinguishes this study from prior work is its integrated approach that simultaneously evaluates technical feasibility through network simulation, economic viability through comprehensive financial modeling, and regulatory compliance within Indonesia's evolving legal framework. Unlike previous studies that focus on isolated aspects, this research provides a holistic assessment that directly addresses the decision-making needs of enterprises and policymakers. The GRE IPSec approach examined here offers advantages over alternative solutions by combining the routing flexibility of GRE with the robust security of IPSec, providing a scalable solution suitable for multi-site corporate deployments. This integrated methodology fills a critical gap in understanding how private networks can be successfully deployed in emerging markets where regulatory clarity, cost constraints, and security requirements must all be simultaneously satisfied.

This study aims to evaluate the implementation of GRE IPSec in private network design from technical, economic, and regulatory perspectives. Technical evaluation includes topology design and network simulation to ensure optimal and secure operation, while economic feasibility is assessed through financial indicators such as CAPEX, OPEX, NPV, IRR, PI, and PP. This comprehensive analysis intends to support enterprises in developing secure, efficient, and regulationcompliant network infrastructures that meet growing demands in digital security. The implementation and feasibility of GRE IPSec will assist the government in determining and making regulatory recommendations on private networks.

METHOD

This research analyzed the feasibility of implementing GRE IPSec for private network design, particularly for companies related to the project using the GNS3 network simulator. A techno-economic analysis determined its viability as a private network solution. Additionally, the study evaluated relevant regulations and proposed improvements to Indonesia's legal framework regarding commercial private networks. The goal was to align these regulations with current technological and business needs, providing recommendations to regulators and the government to better support IPSec-based private networks in Indonesia.

Table 1 illustrates the research process, which was initiated by obtaining basic information through a literature review focused on understanding the parameters and operational mechanisms of the GRE IPSec protocol in a network simulator environment. This step was critical to accurately designing the network architecture.

Table 1. Research Scenario Parameter

Technical Simulation	Three routers to represent three regional clients with different IP versions.
Network Simulator	GNS3 2.2.54
Router	Cisco 2811
Method	GRE IPSec and IPv6 over IPv4

Regarding the regulatory aspects, the study involved collecting and analyzing relevant Indonesian laws and regulations on private networks. Once the initial data had been obtained, a technical analysis was performed by simulating the GRE IPSec network architecture using a network simulator. The topology consisted of three interconnected routers representing different areas in Jakarta, with each client router connected to client devices. The economic analysis involved combining all expenses incurred during implementation to obtain CAPEX and OPEX values. To further evaluate the feasibility of the investment, revenue modeling techniques were applied by calculating financial metrics such as net present value (NPV), internal rate of return (IRR), profitability index, and payback period. The regulatory analysis involved examining existing regulations that were directly relevant to the implementation of private networks within companies. Based on this review, refined regulatory recommendations for private networks in Indonesia were developed.

RESULT AND DISCUSSION

Technical, Techno-Economic, And Regulation Analysis of GRE IPSec Implementation

A. Technical Analysis

In the technical analysis process, the design and implementation of a private network simulation were carried out using GRE IPSec technology, operated through the GNS3 network simulator. The designed network topology underwent comprehensive research to ensure that it meets the requirements of a private network, while also guaranteeing an optimal level of system availability and reliability. The success of the simulation provides evidence of the effectiveness and robustness of the proposed network solution. Furthermore, the results from this stage serve as an important foundation for proceeding to the economic analysis.

B. Network Topology

Figure 1 illustrates the topology of a private network scenario, which includes a central router responsible for managing the entire network of routers, including those owned by service providers, and implementing a label based mechanism to direct data traffic. Client routers are connected to this central router, each representing a branch of the company located in various areas of Jakarta. This configuration ensures that data traffic from each region is routed efficiently and securely. This private network configuration utilizes the concept of GRE tunneling for IPv6 over IPv4, combined with additional security provided by IPSec. This allows sensitive data from each branch office to remain secure and isolated from one another.

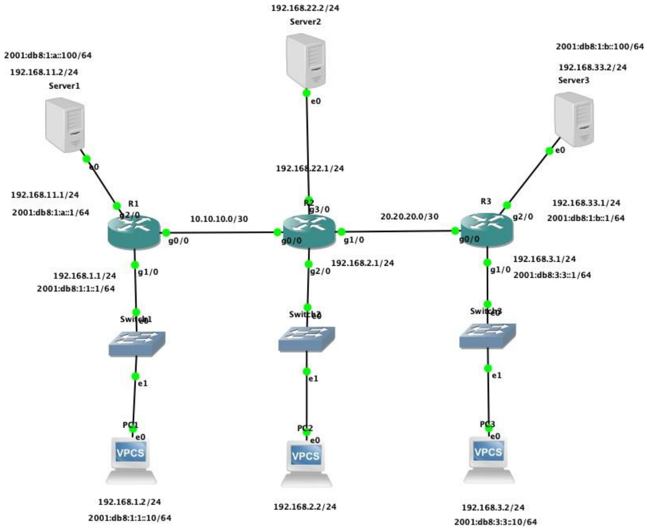


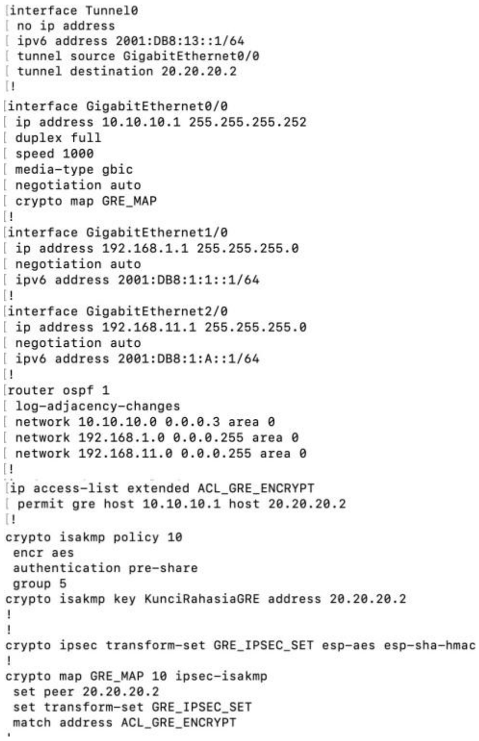
Fig. 1. GRE IPSec Network Topology

C. Configuration Between Router and End Device

In this section, the configuration process involves assigning IP addresses to each router interface connected to the end device, followed by setting up GRE tunneling to facilitate communication between networks. OSPF will be used for routing information exchange, ensuring fast convergence and optimal traffic management for larger networks (Huda & Andriyani, 2025). IPSec with ISAKMP will be implemented to secure data communication between the router and the end devices. Figure 2 shows the configuration of Router 1, Figure 3 shows the configuration of Router 2, and Figure 4 will show the configuration of Router 3. After the configuration is complete, the ’show run’ command will be used to verify that all settings have been applied correctly, with the results displayed below as proof of successful configuration.

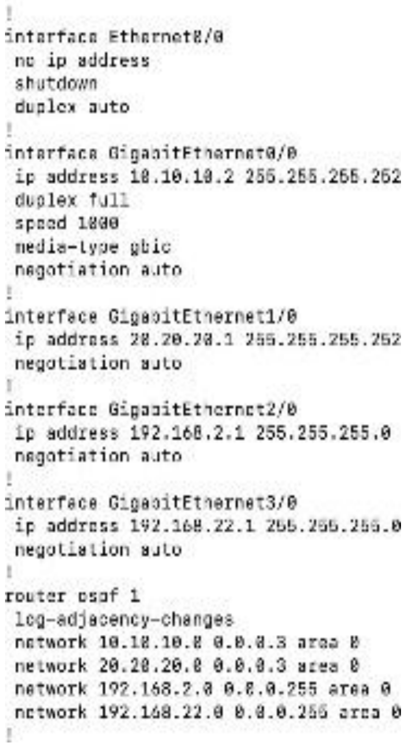
D. Simulation Result

In this simulation, connections between devices on the network were established using IPv6 over IPv4 tunneling, with the GRE protocol enabling the transmission of IPv6 packets over IPv4. The security of communication between end devices was ensured by implementing IPSec, which encrypts data and guarantees security during data exchange. Network performance testing was conducted by measuring Quality of Service (QoS) parameters, including delay, jitter, and throughput. This QoS testing was performed by capturing data from each end device to obtain an overview of latency, connection stability, and data transmission capacity. The test results showed that network quality between devices could be effectively controlled, even when using tunneling. Overall, the simulation results indicate that the implementation of GRE tunneling with IPSec security successfully establishes secure connections between end devices.



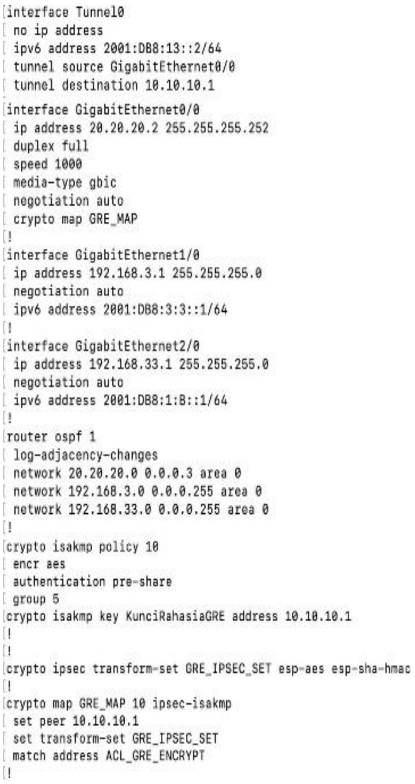
```
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8:13::1/64
 tunnel source GigabitEthernet0/0
 tunnel destination 20.20.20.2
!
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 crypto map GRE_MAP
!
interface GigabitEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:1:1::1/64
!
interface GigabitEthernet2/0
 ip address 192.168.11.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:1:A::1/64
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended ACL_GRE_ENCRYPT
 permit gre host 10.10.10.1 host 20.20.20.2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
crypto isakmp key KunciRahasiaGRE address 20.20.20.2
!
!
crypto ipsec transform-set GRE_IPSEC_SET esp-aes esp-sha-hmac
!
crypto map GRE_MAP 10 ipsec-isakmp
 set peer 20.20.20.2
 set transform-set GRE_IPSEC_SET
 match address ACL_GRE_ENCRYPT
```

Fig. 2. Router 1 Validation



```
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 10.10.10.2 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 20.20.20.1 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 192.168.2.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet3/0
 ip address 192.168.22.1 255.255.255.0
 negotiation auto
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 20.20.20.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.22.0 0.0.0.255 area 0
!
```

Fig. 3. Router 2 Validation



```
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8:13::2/64
 tunnel source GigabitEthernet0/0
 tunnel destination 10.10.10.1
interface GigabitEthernet0/0
 ip address 20.20.20.2 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 crypto map GRE_MAP
!
interface GigabitEthernet1/0
 ip address 192.168.3.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:3:3::1/64
!
interface GigabitEthernet2/0
 ip address 192.168.33.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:1:B::1/64
!
router ospf 1
 log-adjacency-changes
 network 20.20.20.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.33.0 0.0.0.255 area 0
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
crypto isakmp key KunciRahasiaGRE address 10.10.10.1
!
!
crypto ipsec transform-set GRE_IPSEC_SET esp-aes esp-sha-hmac
!
crypto map GRE_MAP 10 ipsec-isakmp
 set peer 10.10.10.1
 set transform-set GRE_IPSEC_SET
 match address ACL_GRE_ENCRYPT
!
```

Fig. 4. Router 3 Validation

E. Conclusion of Technical Analysis

GRE IPSec with IPv4 over IPv6 offers significant advantages in providing secure and efficient network services, with encrypted virtual connections between locations that ensure high data security. This technology supports more flexible data transmission and better network address management on a large scale, improving productivity and network infrastructure performance between offices. Based on simulation results and technical analysis, the GRE IPSec private network topology has proven to be feasible and effective to operate based on its network quality. This implementation also prepares the company to adapt to future IPv6 usage, with stable and reliable performance in GNS3 simulations. While there are many technical advantages, an economic analysis covering initial implementation costs, operational costs, and long-term benefits is crucial for assessing financial viability and its impact on the company's business growth strategy.

F. Techno Economic Analysis

In this techno-economic analysis, economic projections will be made regarding the construction of data centers in companies connected using the GRE IPSec topology over the next five years. The projection is carried out by calculating detailed expenditure costs, including the initial investment required to set up a data center, such as physical infrastructure, hardware, and software. In addition, it will estimate the operational and maintenance costs incurred over the five-year period, which include the costs necessary to ensure the continuity and stability of the data center's operations, as well as the calculation of asset costs associated with this project. This study aims to provide a comprehensive overview of the financial viability and potential benefits of implementing a private network project within the company.

G. Investment and Operational Cost Analysis

In developing the initial cost plan for the project of creating an enterprise data center interconnected through a private network using the GRE IPSec topology, costs will be divided into two main categories CAPEX and OPEX. CAPEX includes all expenses related to the initial long-term investment. Meanwhile, OPEX covers the operational and maintenance costs of the data center that are routinely incurred over the next five years in the short term. This cost separation aims to facilitate more systematic budget planning and improve the overall financial management of the project. Table II and III present the details of the CAPEX and OPEX costs used in the private network implementation.

H. Projected Cost and Revenue

Table IV shows the operating expenses per year that a company would incur when building data centers for three offices, including the additional annual depreciation costs of the equipment used. Depreciation is recalculated based on the updated CAPEX multiplied by three offices (total Rp 291.462.000) minus residual value 10% (Rp 29.146.200). Depreciation calculations are carried out using the Straight Line

Table 2. Capex Cost for Data Center Development

Item	Item Price (IDR)	Quantity	Total (IDR)
Router Cisco 1941	4.570.000	3	**13.710.000**
Switch Cisco Catalyst 2960	13.900.000	3	**41.700.000**
Server HP DL380 Gen9	22.450.000	3	**67.350.000**
Lenovo PC Monitor	2.552.000	3	**7.656.000**
Indorack Server IR11542D 42U	13.000.000	3	**39.000.000**
UTP Cable CAT 6	1.500.000	9	**13.500.000**
Fiber Optic Cable	400.000	6	**2.400.000**
APC UPS Electric	28.000.000	3	**84.000.000**
Air Conditioner LG 1 PK	3.399.000	3	**10.197.000**
CCTV Smart Camera	358.000	6	**2.148.000**
Security Smart Door Lock	1.200.000	3	**3.600.000**
Temperature Measuring Device	210.000	3	**630.000**
Portable Fire Extinguisher	488.000	3	**1.464.000**
Smoke Detector	600.000	3	**1.800.000**
Cable Terminal	17.000	6	**102.000**
Linear Lighting LED Blok	245.000	9	**2.205.000**
		Grand Total	**291.462.000**

Table 3. Opex Cost for Data Center Operations

Element	Monthly Cost	Period (Month)	Total
IT Employee Salary	5.300.000	12	**190.800.000**
Monitoring and Maintenance of Equipment	1.000.000	4	**12.000.000**
Infrastructure and Facilities Operations	1.000.000	4	**12.000.000**
Patch System Upgrade and Customization	500.000	4	**6.000.000**
Remote System Subscription	249.000	12	**8.964.000**
Information Security Audit and Regulation	15.000.000	1	**45.000.000**
		Grand Total	**274.764.000**

Depreciation (SLD) method. The formula used to calculate annual depreciation is:

$$\text{Depreciation} = \frac{291.462.000 - 29.146.200}{5} = 52.463.160$$

This calculation method assumes that the asset will depreciate evenly over its useful life. These operational costs include components such as employees, routine maintenance, electricity related to energy consumption, equipment maintenance, system upgrades, remote system subscriptions, and regulatory audit requirements. Other operating costs are expected to increase annually according to the inflation rate, with an estimated cost increase of 5% per year. Therefore, the annual cost projections accurately reflect changes in operating costs as well as depreciation allocation.

Table 5 estimates the potential revenue from data transmission over private networks using a tiered pricing model based on data volume. Transactions up to 500 MB are charged Rp 8.000, those between 501 MB and 1.000 MB are charged Rp 11.000, and those over 1 GB are charged Rp 13.000. In the first year, the projected monthly revenue is Rp 570.850.000. With a 10% annual growth in transaction volume, the total projected revenue over five years is Rp 3.485.096.335. This projection highlights the monetization potential and strategic value of implementing a private network for secure data transmission.

Table 4. Projected Cost of Operations

Period	Expense (Idr)	Depreciation (Idr)	Total (Idr)
First Year	274.764.000	52.463.160	**327.227.160**
Second Year	288.502.200	52.463.160	**340.965.360**
Third Year	302.927.310	52.463.160	**355.390.470**
Fourth Year	318.073.676	52.463.160	**370.536.836**
Fifth Year	**333.977.359**	**52.463.160**	**386.440.519**

Table 5. Projected Revenue Based on Data Transactions

Period	Total Transaction	Annual Income (IDR)
First year	54.350	**570.850.000**
Second year	59.785	**627.935.000**
Third year	65.764	**690.728.500**
Fourth year	72.340	**759.801.350**
Fifth year	79.574	**835.781.485**
Total	**331.213**	**3.485.096.335**

Table 6. Projection Tax for Data Center Development

Period	EBITDA (IDR)	EBIT (IDR)	Tax 10% (IDR)	Net Income (IDR)
First-year	296.086.000	243.622.840	24.362.284	**219.260.556**
Second year	339.432.800	286.969.640	28.696.964	**258.272.676**
Third year	387.801.190	335.338.030	33.533.803	**301.804.227**
Fourth year	441.727.675	389.264.515	38.926.451	**350.338.063**
Fifth year	**501.804.126**	**449.340.966**	**44.934.097**	**404.406.869**

Table 6 presents a detailed overview of the company's financial performance, focusing on income before tax and key profitability metrics. The EBITDA grows from Rp 296.086.000 in the first year to Rp 501.804.126 in the fifth year, reflecting revenue growth and effective cost management. EBIT, after accounting for depreciation, rises from Rp 243.622.840 to Rp 449.340.966, demonstrating improved operational efficiency. Taxes are calculated at 10% of EBIT, increasing from Rp 24.362.284 to Rp 44.934.097. Finally, net income after tax shows a significant increase from Rp 219.260.556 to Rp 404.406.869, highlighting the company's improved financial condition and sustainability over the first five years. This projection offers valuable insights into the financial viability of companies adopting private networks.

Feasibility Analysis

The feasibility analysis was conducted to provide an overview of the potential success and risks of the research, allowing for a conclusion on whether the research can be continued, modified, or discontinued. NPV is an economic valuation method that calculates the difference between the present value of discounted future cash flows and the initial investment cost, assessing the added value generated by a project. IRR is the project's rate of return that indicates the feasibility of an investment if it exceeds the cost of capital. PI is a financial indicator that measures the feasibility of a project by comparing the present value of future cash flows to the initial investment cost. PP is an investment appraisal method that measures the time required to recover the initial investment cost from project cash flows.

a. Net Present Value (NPV):

NPV is calculated using the following formula:

$$NPV = \sum_{t=0} \frac{CF_t}{(1+i)^t}$$

Where:

1) CF0 is the initial investment (usually a negative value),
2) CFt is the net cash flow at year t,
3) i is the discount rate,
4) n is the length of the evaluation period (in years).

Based on the updated data, the initial investment is Rp 291.462.000, and the net cash flow over five years are as follows:

Table 7. Net Cash Flow on Investments

Year (*t*)	**Net Cash Flow (*CFt*)**	**Discount Factor (*i* = 10%)**	**Present Value**
0	-291.462.000	1.0000	**-291.462.000**
1	219.260.556	0.9090	**199.307.845**
2	258.272.676	0.8260	**213.333.230**
3	301.804.227	0.7510	**226.654.974**
4	350.338.063	0.6830	**239.280.897**
5	**404.406.869**	**0.6200**	**250.732.258**

The total present value of the net cash flows over five years is: 199.307.845 + 213.333.230 + 226.654.974 + 239.280.897+250.732.258 = 1.129.309.206

Therefore, the project's NPV is:

NPV= −291.462.000 + 1.129.309.206 = 837.847.206

NPV is used to evaluate the economic feasibility of the project by calculating the difference between the present value of expected cash inflows and outflows. In this project, the NPV is calculated by discounting net cash flows over five years at a 10% rate of return. The resulting positive NPV of IDR 837.847.206 indicates that the project is expected to generate value beyond the initial investment, making the implementation of the private network economically viable.

b. Internal Rate of Return (IRR):

The formula used to calculate IRR is:

$$IRR = i_1 + \frac{NPV_1}{NPV_1 - NPV_2}(i_2 - i_1)$$

Where:

1) i1 = first discount rate (with NPV1 > 0)
2) i2 = second discount rate (with NPV2 < 0)
3) NPV1 = NPV at i1
4) NPV2 = NPV at i2

i1 = 10% = 0.10, NPV1 = 837.847.206

i2 = 85% = 0.85, NPV2 = −1.242.490

Therefore:

$$IRR = 0.10 + \frac{837.847.206}{837.847.206 - (-1.242.490)} \times (0.85 - 0.10)$$

$$= 0.10 + \frac{837.847.206}{837.847.206 + 1.242.490} \times 0.75$$

$$= 0.10 + \frac{837.847.206}{839.089.696} \times 0.75$$

$$= 0.10 + 0.9974 \times 0.75$$

$$= 0.10 + 0.7480$$

$$= 0.8480 = 84.80\%$$

The IRR is the discount rate at which the project's NPV equals zero, indicating the expected rate of return. By interpolating between discount rates of 10% (positive NPV) and 85% (negative NPV), the IRR was estimated at 84.80%. Since this rate exceeds the project's cost of capital (10%), it suggests that the investment is financially attractive and can generate returns above the required threshold. The IRR supports the project's feasibility and profitability.

c. Profitability Index (PI):

PI is the ratio between the present value of cash inflows and the present value of cash outflows. The formula is:

PI = PV of Cash Inflows
PV of Cash Outflows

Based on the available data:

1) The present value of cash inflows over 5 years (years 1 to 5) is IDR 2.594.772.727.
2) The present value of cash outflows, which is the initial investment (year 0), is IDR 291.462.000.

Thus, the calculation of PI is:

1.129.309.206
PI = = 3.87 291.462.000

PI is the ratio of the present value of future cash flows to the initial investment cost, used to evaluate the attractiveness of a project. A PI greater than 1 indicates that the project is feasible and creates value for the company. In this case, for every IDR 1 invested, the project generates IDR 3.87 in cash inflows. This makes the private network project financially profitable and supports the decision to proceed with the investment.

d. Payback Period (PP):

PP is the time required for the initial investment to be recovered from the annual net cash flows. The formula is:

Initial Investment
PP = Average Annual Net Cash Flow

Based on the data:

1) The initial investment (CAPEX) is IDR 291.462.000.
2) The average annual net cash flow over 5 years is calculated as follows:

Policy Brief Analysis

With the rise of digital technology, the demand for data security has made private networks an essential solution for protecting critical information in Indonesia. Private networks offer superior security compared to public networks, ensuring 219.260.556 + 258.272.676+ stricter control over internal data. While the initial cost is Average Net Cash Flow 301.804.227+ higher, the long-term benefits in terms of efficiency and = 350.338.063 + 404.406.869 : 5 risk reduction make them a popular choice. However, the Thus, the Payback Period is: 291.462.000 = 684.019.067 implementation of private networks in Indonesia faces regulatory challenges (Sankaran, 2023; López-Millán et al., 2023).. Current laws classify private networks as special telecommunications, creating an imbalance with public telecommunications providers, who are subject to additional fees, such as Non-Tax State Revenue (PNBP) and Universal

PP = = 0.95 years ≈ 11 months

306.816.478

PP measures how long it takes for the project to recover its initial investment from net cash inflows. The average annual net cash flow is IDR 306.816.478, leading to a PP of approximately 0.95 years or 11 months. This relatively short payback period implies quick recovery of invested capital, which reduces the financial risk and improves liquidity during the early years of the project.

Conclusion of Techno Economic Analysis

This study concludes that the proposed project is both technologically and economically viable. The financial analysis, using key indicators such as NPV, IRR, PI, and PP, confirms the project's profitability. The positive NPV of IDR 837,847,206 indicates a net return on investment, while the IRR of 84.80% exceeds the cost of capital, ensuring high returns. A PI of 3.87 further underscores the project's financial benefits, and the quick payback period of 0.95 years (approximately 11 months) minimizes financial risk. With projected annual revenue growth reaching IDR 3.49 billion by the fifth year, the project demonstrates long-term profitability. Additionally, the private network's strategic value lies in enhancing data security, making it a critical investment for the company's infrastructure and financial management.

Regulation Analysis

In Indonesia, although private networks are widely used by companies, the regulations governing them are still limited. Private networks are regulated as special telecommunications under Law No. 36 of 1999, but there are no regulations that specifically address private networks. Several regulations, such as Government Regulation No. 52/2000 and No. 71/2019, provide guidelines related to operational permits, electronic transaction systems, data protection, and network security. However, supervision and compliance with security and service quality standards remain a challenge because the existing regulations focus more on public service providers and do not comprehensively cover commercial private network operators. Therefore, a more comprehensive policy is needed to support sustainable technological and economic development while maintaining data security.

Service Obligation (USO) requirements. In contrast, commercial private network operators are not subject to these fees (Akinsanya et al., 2024). This regulatory gap hinders the growth of private networks. Existing regulations, such as Law No. 36/1999, Government Regulations No. 52/2000, and others, need to be updated to better align with technological advancements. Clear policies, fair enforcement, and improved data protection are needed. Updating these regulations is crucial to fostering sustainable investment and ensuring the long-term viability of private networks in Indonesia, while also balancing innovation with compliance to security standards.

Problem Identification in Policy Brief

a. Unclear Regulations Regarding Private Networks

Regulations governing the use of private networks in Indonesia remain unclear, particularly with regard to commercial use. This has led to legal uncertainty that could hinder development.

b. Differences in Treatment Between Private Networks and Public Services

Private networks in Indonesia are still classified as special telecommunications, subject to the same regulations as public telecommunications service providers. This creates an imbalance, where private network operators are not subject to the same obligations as PNBP (Non-Tax State Revenue) or USO (Universal Service Obligation), despite being able to operate commercially.

c. Limitations in Supervision and Law Enforcement

Supervision of private network operators is still limited, as most regulations focus more on public telecommunications service providers. This results in potential abuse or violations of security and service quality standards by private network providers.

d. Limitations in Data Protection and Security in the Financial Sector

Although private networks offer higher security, inadequate regulations can hinder optimal data protection. This is especially crucial in sectors such as finance and government, where it is important to ensure that data transmitted through private networks remains secure.

Private Network Financial Obligations: BHP and KPU/USO

After the economic analysis, the next step is to calculate the BHP and USO costs for the implementation of private networks in Indonesia, in accordance with the Minister of Communication and Information Technology Regulations No. 17 of 2016 and No. 5 of 2021. Telecommunications service providers with operational licenses are required to pay a BHP contribution of 0.50% and a KPU/USO contribution of 1.25% of gross revenue. Payments can be made quarterly or semiannually, in line with applicable regulations. The contribution amount is determined based on audited financial statements. This calculation ensures compliance with PNBP and USO obligations, supports the sustainability of the telecommunications sector, and guarantees that contributions are used to strengthen Indonesia's telecommunications infrastructure.

Table 8. Projection BHP & USO Contribution

Year	Revenue	BHP (0.50%)	KPU/USO (1.25%)
1	570.850.000	2.854.250	7.135.625

2	627.935.000	3.139.675	7.849.188
3	690.728.500	3.453.642	8.634.106
4	759.801.350	3.799.006	9.497.517
5	835.781.485	4.178.907	10.447.276

Table 8 illustrates the BHP and USO costs associated with the implementation of commercial private networks. It details the costs that must be borne by private network operators in accordance with applicable regulations. The calculations include the allocation of costs for BHP Telecommunications Services and contributions to the Universal Service Obligation (USO), which is a financial obligation that must be fulfilled by every private network operator in accordance with regulations established by the government. This ensures that all cost components have been calculated accurately and in accordance with applicable regulations, thereby supporting the sustainable operation of private networks. Additionally, accurate calculations are crucial to ensure that operators comply with existing legal regulations, avoid potential violations that could harm relevant parties, and maintain the trust of regulators and end-users. These calculations also serve as a reference for operators in planning budgets and facilitating more transparent financial management, which ultimately supports operational efficiency and strengthens the telecommunications ecosystem in Indonesia.

Policy Recommendation

1) Updating Law No. 36 of 1999 Regarding Regulations on Private Networks for Commercial Purposes

An update to Law No. 36 of 1999 is necessary to align the regulations on the use of commercial private networks with the same obligations as public service providers, including PNBP and USO. This update will reduce legal uncertainty and ensure that all parties comply with fair obligations, creating equity between the public and private sectors.

2) Adjustment of Tariffs and PNBP Payments

The PNBP tariff update for commercial private network operators needs to be adjusted according to the scale and type of service provided, ensuring a fair contribution to state revenue. This will also provide clarity regarding the financial obligations of operators, as well as increasing transparency and fairness in the taxation system.

3) Enhancement of Supervision and Enforcement of Laws for Private Network Operators

Regulations should include stricter supervision and enforcement for commercial private network operators, with more effective reporting and auditing mechanisms. This will ensure compliance with service quality and data security standards, reducing the risk of misuse and protecting consumers from poor service or data breaches. Enhanced oversight will also help maintain high standards and minimize legal risks for companies.

4) Strengthening Security Standards and Data Protection for the Financial Sector

The financial sector requires stricter security standards and data protection regulations for private network operators to prevent data leaks. Operators must comply with tighter security guidelines and certifications to ensure optimal protection, enhancing consumer trust, safeguarding the financial system, and reducing risks from cyberattacks.

CONCLUSION

This study demonstrates that implementing private networks using GRE IPSec technology in Jakarta is viable from technical, economic, and regulatory perspectives. Through comprehensive methodologies like GNS3 simulations and regulatory reviews, it confirms the architecture's robustness for secure corporate data transmission, ensuring high integrity, availability, and operational reliability. Economically, positive NPV, IRR, and profitability ratios highlight significant long-term returns despite initial costs, driven by efficiency gains and threat mitigation. Regulatorily, it identifies imbalances in Indonesia's laws treating private networks as specialized telecommunications, recommending revisions for fair competition, equivalent obligations to public providers, and enhanced compliance to foster industry growth and security. For future research, real-world deployments beyond simulations could validate performance in live Jakarta environments, while comparative analyses across other Indonesian regions or developing countries would strengthen generalizability.

REFERENCES

Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual private networks (VPN): A conceptual review of security protocols and their application in modern networks. *Engineering Science Technology Journal*, *5*(4), 1452–1472. https://doi.org/10.51594/estj.v5i4.1076

Bitbit, E. D., Gampoy, M. A. B., Ricafort, T. S., Tinio, R. D., Pula, R. L., Leona, R. F., & Olipas, C. N. P. (2023). Crafting a network plan for a microfinancing establishment and its branch network through virtual private network (VPN) implementation. *European Journal of Theoretical and Applied Sciences*, *1*(3), 441–448. https://doi.org/10.59324/ejtas.2023.1(3).43

Gebremeskel, B. K., Jonathan, G. M., & Yalew, S. D. (2023). Information security challenges during digital transformation. *Procedia Computer Science*, *219*, 44–51.

Horisaki, S., Matama, K., Naito, K., & Suzuki, H. (2024). CYPHONIC-overQUIC: Secure end-to-end communication architecture traversing firewalls/NATs. *Journal of Information Processing*, *32*, 509–519. https://doi.org/10.2197/ipsjjip.32.509

Huda, M., & Andriyani, W. (2025). Multi-area OSPF analysis using virtual link and GRE tunnel. *Eduvest Journal of Universal Studies*, *5*(2), 1804–1819. https://doi.org/10.59188/eduvest.v5i2.1710

Karstensen, A., Kolding, T., Rosa, C., Uzeda Garcia, L. G., Pedersen, K. I., & Hathiramani, N. (2022). Spectrum for private networks: Challenges and opportunities—A case study based on Danish regulation. *IEEE Access*, *10*, 69346–69353. https://doi.org/10.1109/ACCESS.2022.3186441

Kumar, J., Kumar, M., Pandey, D. K., & Raj, R. (2020). Encryption and authentication of data using the IPSEC protocol. *Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems: MCCS 2019*, 855–862.

López-Millán, G., Marín-López, R., Perenıguez-García, F., Canovas, O., & Parra Espín, J. A. (2023). Analysis and practical validation of a standard SDN-based framework for IPsec management. *Computer Standards & Interfaces*, *83*, 103665. https://doi.org/10.1016/j.csi.2022.103665

Nair, A. J. (2024). Securing Data Communication: An InDepth Exploration of IPsec Protocol Integration for Enhanced Data Security. *Journal of Network & Information Security*, *12*(1).

Nowicka, J., Ciekanowski, Z., Kudins, J., & Dąbrowski, P. J. (2024). *Managing organizational security in the era of digital transformation*.

Ogudo, K. A. (2019). Analyzing generic routing encapsulation (GRE) and IP Security (IPSec) tunneling protocols for secured communication over public networks. *2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (IcABCD)*, 1–9.

Parulian, H., & Putranto, R. D. (2022). Pidana ujaran kebencian melalui media sosial ditinjau dalam perspektif Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik (UU ITE). *Jurnal Pendidikan dan Konseling (JPDK)*, *4*(4), 4909–4919. https://doi.org/10.31004/jpdk.v4i4.6415

Rey, W. (2024). Enhancing law enforcement security: Implementing MABIS overlay with virtual tunnel interface over IPsec protocols for robust integration. In *2024 7th International Conference on Electronics, Communications, and Control Engineering (ICECC)* (pp. 87–93). IEEE. https://doi.org/10.1109/ICECC63398.2024.00023

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Sankaran, A. S. (2023). Cross protocol attack on IPSec-based VPN. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISDFS58141.2023.10131787

Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In *Data Governance* (pp. 137–150). Springer. https://doi.org/10.1007/978-3-031-67268-26

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2022). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In *2022 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1–11). IEEE. https://doi.org/10.1109/PST.2022.8514208

Uddin, M. R., Evan, N. A., Alam, M. R., & Arefin, M. T. (2021). Analysis of generic routing encapsulation (GRE) over IP security (IPSec) VPN tunneling in IPv6 network. *International Conference on Ubiquitous Communications and Network Computing*, 3–15.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Kamalasanan, V., Sankaranarayanan, S., David, L. A., & Chadha, A. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, *3*(127). https://doi.org/10.1007/s42979-022-01020-4