

ABSTRACT

This thesis explores the implementation of GRE IPSec private networks as a secure and cost solution for data transmission in corporate environments, with a focus on addressing the challenges of ensuring secure data transfer over private networks. The primary objective is to investigate how GRE IPSec can enhance security, feasibility cost, and align with regulatory requirements, particularly in the context of Indonesia. The research adopts a multi-faceted methodology, which includes designing and simulating network topologies using GNS3 to assess the technical feasibility of the network configuration. This is followed by an in-depth economic feasibility analysis, incorporating CAPEX, OPEX, NPV, IRR, PI, and PP metrics, to evaluate the financial viability of implementing Private Networks in the corporate sector. Additionally, the study conducts a regulatory review based on Indonesia's Electronic Information and Transaction Law (UU ITE) to identify gaps and provide recommendations for enhancing the current legal framework governing private networks. By integrating the GRE tunneling protocol with IPSec encryption, this study evaluates the performance and security of corporate data when transmitted over public networks, addressing potential risks such as unauthorized access and data breaches. The findings highlight the technical performance, economic viability, and legal alignment of GRE IPSec private networks within Indonesia's current regulatory environment, offering valuable insights for businesses seeking to implement secure, scalable, and compliant private network infrastructures. This research not only provides a framework for enterprises to develop robust private network systems but also suggests regulatory improvements to foster more effective and fair governance of telecommunication networks in Indonesia.

Keywords: Private Network, GRE, IPSec, Techno Economic, Regulation.