

ABSTRAK

Internet of things (IoT) merupakan konsep dimana suatu objek ditanamkan teknologi seperti sensor dan software yang bertujuan untuk berkomunikasi, mengendalikan, menghubungkan, serta bertukar data melalui perangkat lain selama masih terhubung ke internet. Namun, tantangan keamanan yang muncul dalam lingkungan yang semakin terhubung ini menuntut solusi yang efektif. Salah satu bentuk solusinya adalah menerapkan *Virtual Private Network* (VPN). Dalam konteks ini, penelitian ini bertujuan untuk menganalisis dan mengimplementasikan lapisan keamanan tambahan pada jaringan IoT menggunakan protokol Internet Protocol Security (IPSec) dan Generic Routing Encapsulation (GRE). Hasil pengujian menunjukkan bahwa penggunaan kombinasi protokol IPSec dan GRE memberikan hasil yang sangat baik dalam aspek keamanan dan QoS. Hal ini dilihat dari pengujian yang dilakukan dengan PING dan di analisa menggunakan aplikasi *Wireshark* dengan melihat parameter IP dan protokol, *Quality of Service* (QoS), keamanan data, dan rute. Penambahan protokol IPSec dan GRE tidak menyebabkan penurunan QoS pada jaringan yang signifikan. Hal ini berdasarkan data hasil perhitungan QoS yakni didapatkan rata – rata hasil *throughput*-nya adalah 986.5 bps, rata – rata hasil *delay*-nya adalah 1.03615 ms, rata – rata hasil *packet loss*-nya adalah 0%, dan rata – rata hasil *jitter*-nya adalah 3.35445 ms. Kesimpulannya, implementasi protokol IPSec dan GRE pada jaringan IoT menghasilkan lapisan keamanan yang efektif tanpa mengorbankan performa jaringan. Ini memberikan perlindungan yang memadai terhadap ancaman keamanan serta menjaga kualitas layanan dalam lingkungan jaringan yang semakin kompleks.

Kata Kunci: Internet of Things, IPSec, GRE, GNS3, Terowongan

ABSTRACT

Internet of things (IoT) is a concept where an object is embedded with technology such as sensors and software that aims to communicate, control, connect, and exchange data through other devices as long as they are connected to the internet. However, the security challenges that arise in this increasingly connected environment demand effective solutions. One form of solution is to implement a Virtual Private Network (VPN). In this context, this research aims to analyze and implement an additional security layer on IoT networks using Internet Protocol Security (IPSec) and Generic Routing Encapsulation (GRE) protocols. The test results show that the use of a combination of IPSec and GRE protocols provides excellent results in terms of security and QoS. This can be seen from tests conducted with PING and analyzed using the Wireshark application by looking at IP and protocol parameters, Quality of Service (QoS), data security, and routes. The addition of IPSec and GRE protocols does not cause a significant decrease in QoS on the network. This is based on the data from the QoS calculation results, namely the average throughput result is 986.5 bps, the average delay result is 1.03615 ms, the average packet loss result is 0%, and the average jitter result is 3.35445 ms. In conclusion, the implementation of IPSec and GRE protocols in IoT networks produces an effective security layer without sacrificing security.

Keywords: *Internet of Things, IPSec, GRE, GNS3, Tunnel*