ABSTRAK

Abstrak - *VoIP Quality of Service (QoS) distandarisasikan karena sangat sensitif terhadap kehilangan dan keterlambatan paket informasi. QoS VoIP diperlukan untuk memastikan bahwa paket suara tidak tertunda atau hilang selama transmisi melalui jaringan. Penggunaan Virtual Private Network (VPN) merupakan salah satu solusi untuk data enkripsi dan menutup celah keamanan. Tujuan dari penelitian ini adalah untuk mempelajari pengaruh beberapa mekanisme sistem keamanan VPN pada QoS VoIP dan menganalisa berdasarkan pengukuran faktor-faktor utama yang mempengaruhi menurut standarisasi meliputi: delay, jitter, throughput dan packet loss serta pengukuran MOS (Mean Opinion Score). Perbandingan performa yang dihasilkan dengan beberapa mekanisme sistem keamanan VPN yang menggunakan metode Layer 2 tunnelling protocol (L2TP IPSEC) dan Secure Soclet Layer (SSL). Penelitian ini mengahasilkan kesimpulan bahwa hasil QoS kedua metode VPN adalah Sangat Baik sesuai rekomendasi Telecommunications and Internet Protocol Harmonization Over Network (TIPHON) dan ITU Telecommunication Standardization Sector (ITU-T). Performansi VoIP VPN metode L2TP IPSec dengan authtentication algorithm sha1 enkripsi (aes-256) mendapatkan hasil lebih baik untuk delay dan jitter jika dibandingkan dengan metode VPN metode SSL enkripsi Transport Layer Security (TLS 1.2) . Rata rata delay untuk VPN SSL Forticlient sebesar 10,014 ms sedangkan Rata rata delay untuk VPN L2TP IPSEC 9,841 ms serta rata rata jitter VPN SSL Forticlient sebesar 10,007 ms sedangkan rata rata jitter untuk VPN L2TP IPSEC 9,842 ms. MOS 4,2576 untuk VPN L2TP dan MOS 4,2575 untuk VPN SSL dengan kategori standarisasi Baik. Hasil pengujian ini dapat dijadikan referensi untuk menentukan perancangan implementasi sistem kemanan VoIP yang terbaik dengan mekanisme system keamanan VPN metode L2TP IPSEC dan SSL.*

Keyword – VoIP, VPN, QoS, L2TP, IPSEC, SSL, MOS

ABSTRACT

Abstract - Quality of Service (QoS) is required and standardized because VoIP is very sensitive to loss and delay of information packets. VoIP QoS is required to ensure that voice packets are not lost during transmission over the network. The use of a Virtual Private Network (VPN) is one solution to close vulnerable security gaps for data confidentiality. The purpose of this research is to study the effect of several VPN security system mechanisms on VoIP QoS and analyze them based on the measurement of the main factors that influence it according to standardization, including: delay, jitter, throughput, and packet loss, as well as MOS (Mean Opinion Score). Comparison of the resulting performance with VPN security system mechanisms that use L2TP IPSEC and SSL methods. This study concludes that the QoS results of the two VPN methods are very good according to the recommendations of TIPHON and ITU-T. However, VoIP performance L2TP IPSec method with encryption AES-256 gets better results for delay and jitter compared to the VPN encryption method SSL TLS 1.2. The average delay for VPN SSL Forticlient is 10,014 ms while the average delay for VPN L2TP IPSEC is 9,841 ms and the average jitter for VPN SSL Forticlient is 10,007 ms while the average jitter for VPN L2TP IPSEC is 9,842 ms. MOS 4.2576 for L2TP VPN and MOS 4.2575 for SSL VPN with standardization category Good. The results of this simulation comparative analysis can be used as a reference to determine the design of the best VoIP security system implementation with a VPN security system mechanism using L2TP IPSEC and SSL methods.

Keywords – VoIP, VPN, QoS, L2TP, IPSEC, SSL, MOS