

Abstrak

Protokol keamanan *Internet Protocol Security* (IPSec) dan *Secure Socket Layer* (SSL) merupakan protokol keamanan yang paling banyak digunakan untuk meningkatkan keamanan VPN. Hal ini dikarenakan, kedua protokol mampu memenuhi kriteria dukungan keamanan dan memiliki tingkat keamanan yang lebih baik dari protokol-protokol keamanan lainnya.

Selain tingkat keamanan, performansi protokol keamanan juga bisa diuji dengan parameter seperti *throughput* dan *delay*. Parameter ini akan memberikan gambaran Quality of Service (QoS) protokol keamanan dari segi performansi jaringan.

Skenario pengimplementasian VPN dengan IPSec dan VPN dengan SSL adalah VPN *remote access*. Jenis pengimplementasian *remote access* memungkinkan pengguna VPN yang *mobile* untuk terhubung ke *private network*. Pada *private network* akan menggunakan standar pengalamatan IPv6 karena sudah banyak *Local Area Network* (LAN) yang mampu menjalankan standar IPv6.

Kata Kunci: *IPSec, SSL, IPv6, VPN, Remote Access.*