ABSTRAK

Keamananan data demi menjaga privasi komunikasi yang dilakukan setiap pengguna jasa layanan publik telah menjadi prioritas utama bagi penyedia jasa layanan tersebut. Sayangnya, keamanan tersebut masih terbatas pada akses *server*, tidak pada jaringan yang dilalui oleh pengguna menuju *server*. Oleh karena itu, VPN akan menjadi salah satu solusi dalam menangani permasalahan keamanan data dalam jaringan.

Virtual Private Network (VPN) menawarkan konsep pengamanan data dengan membentuk jalur komunikasi secara *private* dalam jaringan publik, misalnya internet. Salah satu implementasi jaringan VPN adalah dengan protokol *Secure Socket Layer* (SSL) yang menerapkan kunci keamanan berlapis sehingga mampu menjaga komunikasi secara *private*.

Enkripsi SSL pada teknologi VPN dapat menjaga paket data selama proses pengiriman. Hasil pengujian menunjukkan VPN-SSL lebih dapat menjaga keamanan data dari ancaman *sniffing* dan *disclosure attack*. Berbeda dengan jaringan IPv4 murni dan VPN-GRE yang performansi keamanan datanya masih rentan terhadap ancaman-ancaman tersebut. Di samping itu, dilihat dari segi performansi QoS pada layanan *video streaming*, VPN SSL memiliki performansi paling buruk jika dibandingkan dengan IPv4 murni dan VPN-GRE.

Kata kunci : VPN, SSL, keamanan, *sniffing*. d*isclosure*, QoS, GRE