

ABSTRAK

Dalam rangka efisiensi dan efektifitas kinerja dalam berkomunikasi, sistem komunikasi video conference melalui jalur internet menjadi suatu kebutuhan layanan yang sering digunakan untuk keperluan koordinasi, penyampaian laporan dan diskusi antar satuan era di Kementerian Luar Negeri di Jakarta dan Kantor Perwakilan RI di luar negeri. Namun video conference yang dilakukan pada jaringan umum (public network) ini memerlukan pengamanan.

Pada skripsi ini dilakukan scenario test pengamanan video *conference* menggunakan VPN SSL. Video conference dilakukan antara Kantor Pusat Kementerian Luar Negeri di Jakarta dengan Kantor Perwakilan RI di Canberra, Davao City dan Kopenhagen dan kemudian dilakukan analisa terhadap faktor keamanan maupun *Quality of Service* (QoS). Hasil pengujian untuk faktor keamanan menunjukkan bahwa video *conference* yang dilakukan dengan pengamanan VPN SSL tidak dapat dilihat informasi protocol seperti IP address, user ID, RTP dan SIP karena semua data telah dienkripsi dan dikapsulisasi. Selain itu hasil pengujian untuk *quality of service* menunjukkan bahwa hasil pengukuran parameter *throughput*, *delay*, *jitter* dan *packet loss* masih memenuhi persyaratan rekomendasi ITU dan menunjukkan tingkat performansi yang baik.

Kata Kunci : Video *Conference*, VPN SSL, Keamanan, *Quality of Service*