ABSTRAK

Permasalahan kemanan jaringan akan selalu dikembangkan sejalan dengan perkembangan teknologi informasi. Hal ini dilakukan untuk meminimalisir tindakan yang dilakukan oleh orang-orang yang tidak bertanggung jawab. *IP Security (IPsec)* merupakan metode enkripsi untuk melindungi kerahasiaan, dan keutuhan data pengguna layanan di jaringan publik sehingga data yang bersifat sensitif akan tetap aman dilewatkan di jaringan. Hal ini merupakan penawaran yang sangat baik untuk pengguna yang membutuhkan tingkat keamanan lebih.

Sistem *Multi Protocol Label Switching – Virtual Private Network (MPLS-VPN)* banyak digunakan oleh organisasi yang membutuhkan kemanan ekstra. Namun pada kenyataannya sistem ini belum sepenuhnya aman, hal ini dikarenakan *MPLS-VPN* hanya membentuk saluran yang terpisah dari saluran lainnya pada jaringan internet sedangkan data yang dilewati belum terenkripsi sehingga kerahasiaan dan keutuhan data masih dipertanyakan. *IPSec* pada *MPLS-VPN* merupakan solusi yang sangat tepat untuk meningkatkan kemanan pada layanan berbasis *IP Multimedia Subsystem (IMS)*

Dari hasil pengujian didapat bahwa upaya *network scanning* untuk mendapatkan gambaran topologi dari luar *core* ke dalam *core MPLS-VPN* tidak berhasil, hal ini karena propagasi paket di dalam *core* menggunakan label pada jalur *Label Switching Path (LSP)* melalui proses *virtual routing and forwarding (vrf)* dan ditambahkannya *route distinguisher (rd)* pada MPLS-VPN. Dari upaya *sniffing* trafik voice dan chat di dalam *core MPLS-VPN* didapatkan bahwa paket-paket dapat di-*capture* dan isi komunikasi *client* dapat dibuka, namun dengan *IPSec tunnel* komunikasi *client* tidak dapat dibuka karena paket sudah dienkripsi menggunakan protokol *ESP*. Penyisipan paket dengan modifikasi jalur *MPLS* dapat dilakukan menggunakan *tools loki* dari dalam *core MPLS-VPN*, namun dengan adanya *IPSec tunnel* penyisipan paket menuju *client* tidak dapat dilakukan. Sistem keamanan *MPLS-VPN* dan *IPSec Tunnel* tidak menjamin dari serangan *Denial of Service (DoS)*, dari pengujian didapat *packet loss* mencapai kisaran 30 persen yang artinya masih dibawah standar ITU-T G.104 yang memiliki ambang batas maksimal 20 persen.

Kata Kunci : Keamanan Jaringan, *IPSec, MPLS-VPN, IP Multimedia Subsystem*