

ABSTRAK

Pada era teknologi yang menuju *Next Generation Network*, IP Multimedia Subsystem (IMS) hadir sebagai suatu teknologi yang *support* untuk multimedia interaktif berbasis *IP* dengan mengatur *session* yang muncul untuk setiap layanan. Namun, Aspek keamanan sistem informasi berbasis *IP* pun harus diperhatikan, *Secure GRE tunnel* merupakan mekanisme *tunneling GRE* yang menggunakan metode keamanan dengan menggunakan *IP Security*. *Secure GRE Tunnel* mengimplementasikan *site-to-site VPN*, membuat lalulintas paket antara dua *site* yang terpisah dilalui pada suatu jalur *virtual point-to-point*.

Pada tugas akhir ini akan dilakukan implementasi *secure GRE tunnel*, kemudian melakukan komunikasi *VoIP* dan *VoD* berbasis *IMS*. Akan dilakukan *sniffing* untuk menguji *GRE tunnel* yang dilindungi dengan *IPSec* dan untuk membuktikan terbungkusnya *packet* dengan *GRE Header* dan *ESP Header*. Selain pengujian terhadap serangan tersebut, akan dilakukan uji performansi dan analisis pada layanan *VoIP* dan *VoD* yang berbasis *IMS* dengan mengimplementasikan *GRE tunnel* dan *Secure GRE tunnel* pada sisi *core*-nya dengan mengacu pada nilai *inter arrival delay*, *jitter*, *throughput* dan *packet loss*.

Dari hasil penelitian, didapat bahwa *Tunneling Secure GRE* merupakan *site-to-site VPN* dengan memberikan jaminan keamanan pada layer tiga, namun performansi jaringan lebih bagus jika diimplementasikan hanya *GRE Tunnel* saja. Pada *Secure GRE Tunnel* terjadi *overhead* pada *IPSec* dan proses enkripsi menyebabkan paket membutuhkan waktu pemrosesan yang lebih lama. Nilai *delay*, *jitter* dan *packet loss* pada *GRE Tunnel* layanan *VoIP* dan *VoD* jauh lebih kecil dibandingkan *tunneling GRE over IPSec*. Dan nilai *throughput* pada *tunneling GRE* pun lebih besar dibandingkan pada *tunneling GRE over IPSec*.

Kata kunci: *GRE, IPSEC, IMS, VoIP, VoD, sniffing*