

Abstrak

SIP merupakan protokol negosiasi multimedia yang dikirimkan dengan mode *plain text* sehingga memiliki isu dalam hal keamanan baik itu dari segi *credential* yang terdiri atas *user extension* dan password pada SIP message maupun konten media yang terdapat pada RTP payload. Komunikasi VoIP SIP yang tidak aman ini dapat diamankan dengan implementasi VPN, ZRTP dan SIP-Secure.

Tugas akhir ini akan membahas QoS VoIP setelah dilakukan implementasi protokol pengamanan. Hal yang perlu diperhatikan dalam VoIP adalah kebutuhan bandwidth minimal agar dapat menghasilkan komunikasi yang memuaskan. Dengan implementasi protokol pengamanan baik itu VPN, ZRTP dan SIP-Secure maka akan menambah ukuran paket data yang ditransmisikan. Penggunaan bandwidth yang tidak sesuai dengan kebutuhan minimal akan mengakibatkan QoS yang buruk diakibatkan kapasitas bandwidth tidak mengakomodir *overhead* paket data. Parameter QoS yang digunakan pada VoIP diantaranya *delay*, *jitter* dan *packet loss*.

Dari hasil pengujian terlihat bahwa dengan asumsi penggunaan *codec* G.711, implementasi VPN baik itu IPSec/TLS, ZRTP dan SIPS memberikan performa yang baik pada bandwidth 128/128. Dilihat dari faktor keamanan, VPN memberikan perlindungan menyeluruh baik itu *credential* dan konten media. Sedangkan ZRTP hanya melindungi konten media dan SIPS hanya melindungi *credential* yang ada pada SIP message.

Kata kunci: SIP, VPN, TLS, IPSec, ZRTP, bandwidth, QoS, TCP, UDP