1. Pendahuluan

1.1 Latar Belakang

SIP (RFC 3216) merupakan kesatuan komponen protokol multimedia yang memiliki tingkat fleksibilitas dan adaptasi yang tinggi terhadap protokol lainnya [4]. Struktur SIP mirip dengan HTTP yakni berupa *plain text* memiliki kelemahan karena protokol ini sangat rentan terhadap aktifitas *sniffing, spoffing* dan DoS *attack* sehingga tidak direkomendasikan penggunaan SIP tanpa protokol pengamanan tambahan [4][5]. RTP sebagai bagian dari transmisi VoIP memiliki kriteria *media path*, yakni ketersediaan bandwidth yang digunakan untuk komunikasi VoIP. Penggunaan bandwidth sesuai dengan kebutuhan minimal akan menghasilkan pengalaman komunikasi yang memuaskan.

Dengan implementasi VPN berbasis IPSec dan TLS tentu akan menambah ukuran paket data akibat penambahan 1 layer atau *header* diatas paket data asal. Implementasi ZRTP fokus pada pengamanan RTP payload dengan menggunakan teknik enkripsi memberikan peningkatan ukuran RTP payload. Sedangkan SIP-Secure mengamankan VoIP dari segi protokol inisialisasi yang digunakan, dimana dalam hal ini adalah SIP. VPN memberikan *overhead* yang lebih besar dibandingkan dengan ZRTP dan SIP-Secure sehingga diperlukan kebutuhan bandwidth minimal agar dapat mengakomodir aliran paket data.

Harus diakui bahwa kondisi Internet di Indonesia tidak bisa dikatakan memuaskan dalam hal *availability*, *reliability* dan *cost* untuk standar layanan ekonomis. Di lain pihak VoIP sangat sensitif terhadap kondisi traffic yang dilaluinya dan membutuhkan akses internet yang stabil (minim RTO) [13].

1.2 Perumusan Masalah

Dari latar belakang diatas maka terdapat hal-hal penting yang perlu diperhatikan diantaranya:

1. Bagaimana pengaruh ketersediaan bandwidth, traffic network dan protokol pengamanan diatas terhadap kualitas layanan VoIP SIP?
2. Bagaimana QoS VoIP berupa delay, jitter dan packet loss serta utilitas network pada setiap penggunaan protokol pengamanan tersebut?
3. Begaimana protokol pengamanan tersebut dapat melindungi paket data VoIP berupa *credential* dan media konten yang dibawanya?

1.3 Tujuan

Tujuan yang ingin dicapai dari penelitian ini adalah untuk menganalisis performansi dari VPN-IPSec, VPN-TLS, ZRTP dan SIP-Secure terhadap pengamanan yang diimplementasikan pada SIP dilihat dari aspek:

1. Kebutuhan minimal bandwidth.
2. Peningkatan ukuran paket data yang mempengaruhi kualitas VoIP diantaranya *delay*, *jitter* dan *packet loss*.
3. Unjuk kerja protokol pengamanan dalam mengamankan paket VoIP diantaranya *credential* dan konten media.

1.4 Batasan Masalah

Agar hasil simulasi sesuai dengan apa yang diharapkan, maka berikut adalah batasan masalah yang berkaitan dengan penelitian ini diantaranya:

1. Simulasi dilakukan dalam rekayasa jaringan network yang sudah terkontrol komposisinya (jumlah host, spesifikasi host dan topologi jaringan) yang akan dijelaskan pada subbab selanjutnya.
2. Model simulasi jaringan yang digunakan adalah *wired* dan menggunakan IPv4 sebagai pengalamatannya.
3. Topologi jaringan menggunakan skema SIP Proxy.
4. Paket yang dianalisa adalah paket RTP atau bentuk lainnya jika terdapat mekanisme enkripsi yang mewakili RTP. Paket lain yang tertangkap bersama paket RTP (beserta bentuk enkripsinya) tidak masuk dalam perhitungan analisa.
5. Codec yang digunakan pada tugas akhir ini adalah G.711.
6. Parameter kualitas layanan VoIP yang digunakan adalah *delay*, *jitter* dan *packet loss* dan *call setup*.
7. Range *bandwidth* yang digunakan pada simulasi adalah 128 kbps dan 64 kbps yang akan diimplementasikan pada 2 skenario yang akan dijelaskan pada subbab selanjutnya.

1.5 Metodologi

1. Studi literatur
   Tahap ini dilakukan pengumpulan referensi yang relevan berkaitan dengan VoIP, SIP, VPN, TLS, IPSec dan ZRTP baik itu berasal dari jurnal online maupun offline serta buku cetak.
2. Perancangan sistem
   Setelah memahami teori penelitian maka dilakukan perancangan sistem sesuai dengan tujuan yang telah didefinisikan
3. Implementasi
   Dengan mengaplikasikan teori-teori yang ada serta asumsi yang telah ditetapkan dan menggunakan perangkat pendukung simulasi baik itu hardware maupun software tertentu. Diharapkan hasil dari simulasi ini dapat mewakili kondisi nyata dilapangan.
4. Pengujian dan analisis
   Dalam tahap ini dilakukan pengujian performansi jaringan terhadap penggunaan protokol pengamanan yang digunakan pada pengamanan SIP. Kemudian didapatkan hasil numerik yang selanjutnya dilakukan analisis untuk menentukan protokol pengamanan mana yang memberikan performansi terbaik berdasarkan parameter yang telah ditetapkan.
5. Pembuatan laporan
   Setelah tahap-tahap sebelumnya diselesaikan maka dilakukan pembukuan dengan membuat laporan tertulis agar dapat disajikan secara formal.

1.6 Sistematika Penulisan

1. **Pendahuluan**
   Bab ini menjelaskan permasalahan yang akan dibahas secara khusus dengan memperhatikan latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, metodologi dan sistematika.
2. **Landasan Teori**
   Bab ini menjelaskan teori konsep SIP serta protokol pengamanan yang digunakan yakni VPN, TLS, IPSec dan ZRTP.
3. **Perancangan Sistem**
   Bab ini menjelaskan tentang kebutuhan sistem untuk mencapai target yang telah ditetapkan.
4. **Pengujian dan Analisis**
   Bab ini mengimplementasikan konfigurasi serta pengujian sistem.
5. **Kesimpulan dan Saran**
   Bab ini berisikan kesimpulan dan saran dari hasil penelitian yang diangkat.