BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi dan informasi untuk kelancaran proses kerja menuntut tersedianya media dan proses transfer data secara *real time*, juga fungsi keamanan yang terjamin. Maka dibutuhkan jaringan pribadi yang menghubungkan antar pengguna ataupun instansi. Hal ini membutuhkan investasi perangkat keras yang tidak murah dan dukungan teknis yang rumit dalam jaringan, sehingga pengguna membutuhkan jaringan publik yang bersifat pribadi untuk mengatasi hal tersebut. Teknologi MPLS (*Multi Protocol Label Switching*) merupakan sebuah metode transmisi data yang menggunakan informasi dalam label yang dilekatkan pada alamat IP untuk melakukan *forwarding* paket data. Teknologi ini membutuhkan konsep VPN (*Virtual Private Network*) untuk transfer data yang tinggi dan memungkinkan pengguna menggunakan jaringan publik yang bersifat pribadi dengan *network private IP* yang sama tanpa adanya link terpisah dan keamanan kualitas data yang terjamin, serta membatasi pemborosan link yang tidak dipakai bagi setiap pengguna pada jaringan yang sama. MPLS dapat menyederhanakan proses *routing* yang menjadi beban router karena harus menganalisa setiap header IP yang masuk, serta mengoptimalkan pemilihan *path* melalui kemampuan manajemen *class-of-service* dan *traffic-engineering.*

Salah satu jenis aplikasi yang digunakan pada MPLS adalah *Virtual Private Network* (VPN). MPLS-VPN biasanya dibangun dengan menggunakan protocol routing Border Gateway Protocol (BGP). BGP merupakan protocol routing yang beroperasi pada *Autonomous System* (AS) yang memiliki skalabilitas dan integritas yang tinggi sehingga dapat melayani pertukaran routing pada teknologi MPLS untuk mekanisme autentikasi dalam menjaga integritas suatu jaringan.

Jaringan MPLS tidak cukup aman bila diterapkan tanpa adanya mekanisme keamanan yang dapat melindungi paket data saat ditransmisikan melalui jaringan publik. Oleh sebab itu *IPSec* diimplementasikan pada setiap *end-to-end* router agar data yang mengalir dalam tunnel *IPSec* dienkripsi pada satu router dan didekripsi pada router yang lain sehingga menjamin keamanan dan kerahasiaan isi data dari

akses ilegal yang tidak diinginkan. *IPSec* melakukan proteksi lapisan jaringan dengan merancang mekanisme keamanan kriptografi. Sebuah perusahaan yang menggunakan layanan MPLS dari suatu ISP dan menerapkan *IPSec* di setiap routernya dapat membuat jalur aman yang didukung dengan manajemen *Quality of Service* (QoS) yang baik dalam berkomunikasi dengan kantor-kantor cabangnya.

Studi kasus yang penulis pelajari untuk penelitian ini diantaranya adalah Jurnal berjudul "*Performa Protokol Routing OSPF dan BGP pada jaringan VoIP MPLS dengan Tunneling L2TP/IPSec"* oleh Bekti Maryuni Susanto dan Ery Setiyawan Jullev Atmaji, tahun 2017. Mereka mensimulasikan jaringan VOIP berbasis MPLS VPN menggunakan software GNS3 dan Oracle Virtual Box. GNS3 digunakan untuk membuat model topologi jaringan sedangkan Virtual Box digunakan untuk menjalankan VOIP Server dan komputer klien. Kemudian jurnal berjudul "*Analisis QoS Pada Jaringan Internet (Studi Kasus: UPT Loka Uji Teknik Penambangan Jampang Kulon – LIPI)* oleh Rika Wulandari, tahun 2016, yang menganalisis jaringan internet di Satuan Kerja UPT Loka Uji Penambangan Jampang Kulon – LIPI dengan menggunakan parameter QoS (Quality of Service). Dan terakhir adalah skripsi Sdr. Roberto Sembiring Universitas Sumatera Utara tahun 2018 dengan judul "*Analisa Perbandingan OSPF dan BGP Jaringan MPLS untuk Video Streaming."* Sdr. Roberto Sembiring menganalisis perbandingan kinerja dua teknik routing yang berbeda yakni kinerja dari routing protocol OSPF dengan MPLS dan routing protocol BGP (Boarder Gateway Protocol) dengan MPLS pada layanan Video Streaming, dan mensimulasikan jaringan MPLS dengan dua teknik routing tersebut menggunakan simulator GNS3 untuk mengetahui perbandingan *Quality of Service* (QOS) dan hasil kualitas *video Streaming* dari suatu jaringan.

Pada Tugas Akhir ini penulis melakukan implementasi Layanan VoIP dan menganalisa QoS kinerja routing protocol BGP pada jaringan MPLS terhadap penerapan keamanan paket data *IPSec*. Data yang diujikan berupa trafik *audio IP-Based telephony*, yang merupakan jenis trafik *real-time*. Simulasi yang penulis lakukan adalah langsung mengimplementasikan jaringan skala kecil (lab) menggunakan perangkat jaringan Mikrotik dan server PBX berbasis Linux untuk menjalankan aplikasi VoIP secara nyata.

1.2 Tujuan

Tujuan penelitian tugas akhir ini adalah untuk menganalisa performansi QoS dan mengetahui kualitas layanan VoIP dan *video streaming* pada jaringan MPLS menggunakan *protocol routing* BGP dengan membandingkannya pada jaringan yang sama, sebelum dan sesudah diimplementasikan *tunneling IPSec*.

1.3 Rumusan Masalah

Permasalahan yang dijadikan obyek penelitian dan pengembangan dalam pembuatan tugas akhir ini adalah :

1. Bagaimana simulasi jaringan MPLS-VPN membentuk jaringan internet sederhana di atas routing protocol BGP.
2. Bagaimana menerapkan teknik *tunneling IPSec* di setiap *end-to-end* router pada sebuah jaringan MPLS yang menggunakan protokol routing BGP.
3. Bagaimana mengukur parameter *QoS* seperti *delay, jitter, throughput,* dan *packet loss* yang dilewatkan pada jaringan MPLS-VPN dengan melakukan komunikasi VoIP antar *client* dan aplikasi *video streaming*.
4. Pengamatan terhadap kerja *IPSec* mengamankan paket data dengan melakukan enkripsi pada satu router dan dekripsi pada router yang lain.

1.4 Batasan Masalah

Dalam tugas akhir ini diteliti mengenai pengaruh *IPSec* terhadap *QoS* pada trafik *real-time* di atas jaringan MPLS VPN. Terdapat beberapa batasan masalah, yaitu:

1. Perancangan dilakukan dengan menggunakan 7 unit Router fisik Mikrotik dan 1 unit switch.
2. Jaringan menggunakan pengalamatan IPv4.
3. *Routing protocol* yang diimplementasikan hanya BGP, sebagai satu-satunya protokol penghubung antar jaringan di internet yang umum digunakan saat ini.
4. Jaringan yang diamankan adalah koneksi antara *end-to-end router*, yaitu dari router Kantor Pusat sampai dengan Kantor Cabang, sedangkan jaringan lokal di masing-masing site diasumsikan aman.
5. Aplikasi yang digunakan adalah *software* PBX Server dan VoIP *Client*.

6. Pengambilan data dilakukan pada jaringan berskala kecil, yang dirancang dengan skenario *Site-to-site IPSec VPN*.
7. Analisa performansi *QoS* didapatkan dari perbandingan antara sebelum dan sesudah penerapan tunneling *IPSec* antar dua router CE (*Customer Edge*).
8. Parameter yang diteliti, yaitu waktu tunda (*delay*), variasi waktui tunda (*jitter*), *throughput*, dan *packet loss*.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam menyelesaikan masalah pada tugas akhir ini, adalah sebagai berikut:

1. Studi Literatur

   Kegiatan pembelajaran dan pemahaman dengan mencari, mengumpulkan dan mempelajari referensi tentang teori dan konsep jaringan melalui berbagai sumber pustaka yang berkaitan dengan penelitian, meliputi: VPN, MPLS, *routing protocol* BGP, teknologi VoIP, *software* TrixBox, dan VoIP *Client*.
2. Perancangan dan Implementasi Sistem

   Merancang sistem jaringan MPLS-VPN dengan tunnel *IPSec*, kemudian implementasi dilakukan dengan meng-*configure* 7 unit RouterBoard Mikrotik dan sebuah switch *unmanaged* menggunakan konfigurasi dasar BGP.
3. Pengujian, Pengambilan data, dan Analisa

   Setelah dilakukan implementasi, dilakukan pengujian terlebih dahulu, kemudian mencatat data-data yang berhubungan dengan parameter QoS (*Quality of Service*) menggunakan *software tool* Wireshark untuk selanjutnya dianalisa.
4. Penarikan Kesimpulan

   Dari hasil analisa tersebut ditarik kesimpulan mengenai seberapa besar pengaruh implementasi enkripsi paket data pada tunneling *IPSec* terhadap kualitas layanan komunikasi *Voice over IP*.
5. Penulisan Laporan

   Penyusunan laporan dimaksudkan sebagai pertanggungjawaban secara tertulis atas tugas akhir yang telah dibuat dengan mengacu pada pedoman penulisan skripsi yang diatur oleh pihak Universitas Darma Persada.

1.6 Sistematika Penulisan

Untuk kemudahan dalam memahami tugas akhir yang dibuat, penulisan tugas akhir ini dibagi dalam beberapa bagian sebagai berikut:

BAB I Pendahuluan

Menjelaskan secara singkat tahapan awal penulisan dari latar belakang, tujuan, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II MPLS, VPN, *IPSEC*, *Internet Routing Protocol*, dan BGP

Berisi tentang penjelasan teoritis yang berhubungan dengan analisa tugas akhir yang dibuat, yang mendukung pencapaian tujuan tugas akhir ini.

BAB III Perancangan dan implementasi jaringan MPLS dengan Routing Protocol BGP dan OSPF

Bab ini memuat tentang proses perancangan simulasi hingga konfigurasi untuk implementasi sistem serta skenario yang digunakan untuk melakukan pengujian.

BAB IV Pengujian dan Analisa Sistem

Bab ini menjelaskan hasil pengujian, pengamatan proses transmisi paket data di dalam jaringan, dan pembahasan analisa hasil parameter QoS yang didapat.

BAB IV Kesimpulan

Memuat kesimpulan dan kemungkinan pengembangan untuk penelitian selanjutnya.