BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Saat ini semakin banyak perusahaan industri yang mengunakan layanan *internet* sebagai media untuk melakukan *transfer data* atau informasi sehari – hari seperti perusahaan manufaktur, distribusi dan retail, pertambangan minyak dan gas, telekomunikasi, finansial, pemerintahan serta industri transportasi [1]. Penggunaan *internet* memiliki resiko tersendiri karena *internet* bersifat publik, maka kerahasiaan dan authentikasi atas informasi juga terbuka [2]. Oleh karena itu pentingnya suatu perlindungan atas data merupakan suatu keniscayaan yang tidak bisa dipungkiri lagi.

Teknologi VPN dapat menjawab kebutuhan tersebut, menjaminnya dengan suatu *protocol* untuk enkripsi data. Ada beberapa jenis *protocol* VPN pada mikrotik yang bisa digunakan seperti PPTP, L2TP, SSTP, dan OpenVPN. Pada fitur authentikasi VPN terdapat beberapa metode diantaranya metode *pre shared key* dan *digital certificate*.

Perbedaan dari *pre shared key* yaitu pada pembentukan keamanan dukungan kunci yang berupa *string* teks dan merupakan metode authentikasi yang lemah. Sedangkan *digital certificate* adalah pertukaran sertifikat komputer dengan router, metode authentikasi *digital certificate* ini lebih baik dan manajemen lebih mudah dari pada *pre shared key* dalam jangka panjang [3].

Selain keamanan data, kualitas dari kinerja jaringan tentu merupakan suatu hal yang wajib diperhatikan. Kinerja dari sebuah jaringan merupakan salah satu faktor penting dalam keberhasilan bisnis suatu perusahaan industri.

Beberapa dari itu penulis bermaksud untuk melakukan analisa kualitas performa *protocol* VPN yang berbasis *digital certificate* SSL yaitu *Secure Socket Tunneling Protocol* (SSTP) dan OpenVPN yang mengacu pada *Quality of Service* dengan parameter pengujian yaitu *Delay, Throughput, Jitter, Packet Loss* dan sebagai tambahan dilakukan analisa terhadap ancaman *sniffing* pada kedua *protocol*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka perlu dirumuskan suatu masalah yang akan dipecahkan pada penelitian ini yaitu bagaimana perbandingan *Quality of Service* (QoS) VPN menggunakan protokol *Secure Socket Tunneling Protocol* (SSTP) dan OpenVPN dengan memanfaatkan *Cloud Computing* berdasarkan parameter *Delay, Throughput, Jitter, dan Packet Loss*.

1.3 Batasan Masalah

Agar penelitian ini fokus pada tujuan, maka lingkup dari Tugas Akhir ini adalah sebagai berikut:

1. Implementasi jaringan site – to – site VPN menggunakan protokol SSTP dan OpenVPN pada Router Mikrotik dengan memanfaatkan *Cloud Computing* sebagai *server*.
2. Menggunakan *Laptop* sebagai *SSTP dan OpenVPN Client*.
3. Bentuk pengalamatan jaringan menggunakan *IP Version 4* (IPv-4).

4. Parameter *Quality of Service* (QoS) berdasarkan *Delay, Throughput, Jitter, dan Packet Loss.*
5. Tidak menganalisis algoritma yang digunakan dalam autentikasi dan enkripsi pada kedua protokol VPN yang digunakan.
6. Ancaman keamanan yang digunakan adalah *Sniffing* dengan menggunakan *Wireshark.*
7. Software untuk pengukuran *Quality of Service* (QoS) menggunakan *Wireshark.*
8. VPS *(Virtual Private Server)* menggunakan sistem operasi *Mikrotik Cloud Hosted Router.*

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Penelitian ini bermaksud untuk mengetahui perbandingan *Quality of Service* (QoS) pada jaringan VPN yang menggunakan protokol *Secure Socket Tunneling Protocol* (SSTP) dan *OpenVPN* berdasarkan parameter *Delay, Throughput, Jitter, dan Packet Loss* dengan memanfaatkan *Cloud Computing* sebagai *Server VPN.*

1.4.2 Tujuan Penelitian

Tujuan yang ingin dicapai oleh penulis dalam penelitian dan penyusunan tugas akhir ini diharapkan dapat menjadi bahan referensi pada saat memilih protokol VPN yang sesuai dengan layanan yang akan digunakan.

1.5 Manfaat Penelitian

Dengan adanya penelitian ini, diharapkan dapat memberi gambaran tentang kualitas jaringan VPN pada protokol *Secure Socket Tunneling Protocol* (SSTP) dan OpenVPN berdasarkan parameter *Delay, Jitter, Throughput*, dan *Packet Loss*.

1.6 Metode Penelitian

1.6.1 Metode Pengumpulan Data

Agar mendapatkan data yang akurat dan relevan tentang penelitian yang akan dilakukan, maka dari itu diperlukan adanya metode untuk mencapai tujuan penelitian, berikut metode penelitian yang digunakan :

1.6.1.1 Studi Pustaka

Penulis mengumpulkan data dengan cara membaca artikel, buku, browsing internet serta bacaan – bacaan yang ada kaitannya dengan masalah yang akan diteliti sebagai bahan referensi tertulis.

1.6.1.2 Studi Literatur

Pada studi literatur, penulis mempelajari literatur penelitian sejenis yang memiliki keterkaitan dengan permasalahan yang dibahas. Studi literatur ini bertujuan untuk meningkatkan pemahaman terhadap topik yang sedang diusung.

1.6.2 Metode Pengembangan Sistem

Penelitian ini menggunakan metode NDLC *(Network Development Life Cycle)* sebagai acuan dalam membuat penelitian ini. Tahapan dalam metode NDLC meliputi :

1.6.2.1 Analisis

Tahap ini merupakan tahap analisa permasalahan yang muncul. Analisa dilakukan terhadap data dari penelitian sebelumnya.

1.6.2.2 Design

Dari data – data yang didapatkan sebelumnya, tahap design ini akan membuat gambar topologi jaringan VPN yang akan dibangun. Dengan gambar ini diharapkan akan memberi gambaran seutuhnya yang nanti akan digunakan dalam penelitian.

1.6.2.3 Simulasi

Pada tahap ini penulis akan membuat simulasi dengan bantuan tools khusus dibidang jaringan yaitu Cisco Packet Tracer.

1.6.2.4 Implementasi

Pada tahap implementasi ini, penulis menerapkan semua yang telah direncanakan dan didesign sebelumnya.

1.6.2.5 Monitoring

Pada tahap ini penulis akan melakukan pengawasan terhadap lalu lintas data pada jaringan yang telah dibuat agar sesuai dengan keinginan dan tujuan.

1.6.2.6 Manajemen

Pada tahap ini penulis akan membuat kebijakan untuk mengatur agar sistem yang telah dibangun dapat berjalan dengan baik.

1.7 Sistematika Penulisan

Untuk membuat penyajian dalam penelitian ini menjadi terstruktur dan mudah dimengerti, maka dibuat sistematika penulisan yaitu sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan pada penelitian ini.

BAB II LANDASAN TEORI

Bab ini menjelaskan tentang landasan teori yang digunakan diantaranya tinjauan pustaka, konsep dan teori, serta perangkat lunak yang akan digunakan pada penelitian ini.

BAB III ANALISIS DAN PERANCANGAN

Bab ini menjelaskan tentang tinjauan umum tentang objek permasalahan, analisis dan perancangan VPN yang meliputi analisis SWOT *(Strengths, Weaknes, Opportunity, Threats)*, analisis kebutuhan, dan desain.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan tentang tahapan pembuatan, implementasi VPN yang telah dilakukan, komparasi antara tunnel SSTP dan OpenVPN berdasarkan QoS dan pembahasannya.

BAB V PENUTUP

Terdapat dua bagian, yaitu :

1. Kesimpulan yang berisi jawaban terhadap pertanyaan atau pernyataan kebutuhan yang dikemukakan sebelumnya di bab 1 tentang identifikasi masalah.
2. Saran yang berupa pemantapan terhadap kesimpulan yang telah dibuat. Dengan demikian memantapkan hubungan antara masalah, analisis,

pengembangan dan kesimpulan. Pada bagian akhir saran ditambahkan saran untuk penelitian lanjutan karena masalah yang dikaji pada penelitian umumnya merupakan bagian keci dari keseluruhan masalah yang bersifat komperatif.

DAFTAR PUSTAKA

Daftar pustaka berisi referensi – referensi yang digunakan dalam pembuatan Tugas Akhir ini.