BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemudahan akses internet saat ini terdapat hal positif dan negatif yang timbul, karena internet banyak digunakan dalam sarana bertukar informasi dan komunikasi dalam jaringan. Salah satunya dikarenakan jaringan bersifat publik, maka data yang dikirim dan diterima juga akan terbuka. Hal ini sangat rentan dari ancaman pencurian data hingga ancaman yang bersifat merusak jaringan, ancaman tersebut dapat berasal dari dalam maupun dari luar jaringan tersebut [1].

Ditambah lagi setelah masa pandemi COVID-19 tempat kerja bisa di mana saja dan kapan saja baik secara WFO (*Work From Office*), WFH (*Work From Home*) maupun WFA (*Work From Anywhere*) yang mana bekerja dapat dilakukan di tempat umum dan menggunakan internet dengan jaringan *public* [2].

Dari hal tersebut di atas tentunya menggunakan jaringan *public* terdapat peluang adanya berbagai macam keamanan data. Ada beberapa cara untuk mengatasi hal tersebut, salah satunya menggunakan tambahan berupa *Virtual Private Network* (VPN) yang bisa melakukan otentikasi guna menjaga keamanan data. VPN menggunakan sistem *end-to-end* atau *point-to-point* dari sumber ke tujuan maupun sebaliknya secara *real time* sehingga dapat meminimalisir berbagai ancaman yang mungkin terjadi pada jaringan. Pada penerapan nya VPN menggunakan fitur *tunnel* yang terdapat protocol-protokol yang dapat dikombinasikan dalam penggunaan nya [3].

Tunnel atau sering disebut teknik *tunneling* yang pada prosesnya merupakan pembungkusan data yang akan dikirim (*encapsulation*) menggunakan protokol. Protokol *tunnel* yang dapat digunakan antara lain PPPOE, PPTP, SSTP, L2TP, Ipsec serta OpenVPN. Dari berbagai protokol tersebut dipilih protokol yang popular yaitu L2TP+IPsec dan SSTP, selain itu juga dikarenakan L2TP+Ipsec merupakan kombinasi tunneling L2TP ditambah IP *Security* berupa *secret* yang mana menggunakan 2 buah *password/secret* serta bisa digunakan di

seluruh sistem operasi. Sedangkan untuk SSTP yang hanya menggunakan 1 buah *password/secret* serta hanya untuk sitem operasi Windows. Hal tersebut yang membuat penulis untuk melakukan uji coba dengan kedua protokol tersebut [4].

Tidak hanya keamanan saja yang perlu diperhatikan, kualitas pengguna dalam menerima layanan juga harus diperhatikan. Oleh karena itu kualitas layanan yang diberikan kepada pengguna atau sering disebut dengan istilah QoS (*Quality Of Service*) juga perlu diperhatikan. QoS dalam pengujiannya menggunakan acuan dari ETSI (*Europan Telecommunication Standard Institute*) yang menggunakan beberapa parameter sebagai acuan pengujian kualitas pada jaringan [5].

Dalam analisis QoS akan dilakukan pengujian dengan *streaming* pada situs penyedia video YouTube menggunakan *browser* Google Chrome. Hasil data dari *streaming* kemudian akan di analisis dengan variabel nilai *Throughput, Packet Loss, Delay* dan *Jitter*. Penelitian ini akan dilakukan dengan membandingkan *client* yang terhubung dengan protocol VPN *tunneling* yang berbeda [4].

Selain beberapa hal tersebut pengujian pada penelitian-penelitian sebelumnya hanya dilakukan dalam waktu yang singkat, rata-rata dilakukan pengambilan nilai hanya dalam kurun waktu 5 menit dalam satu kali pengambilan data saja. Pemilihan waktu pengujian tentu juga akan menambah variasi jumlah data yang bisa di dapatkan, sehingga presisi data yang di uji akan lebih mendalam kajiannya dalam setiap waktu [6].

Dari latar belakang permasalahan di atas maka peneliti membuat topik penelitian berjudulkan **"*Analisis Perbandingan Kinerja Protokol Virtual Private Network (VPN) L2TP+IPSec & SSTP Pada MikroTik Menggunakan Metode Quality of Service (QoS)*"**, dengan penelitian ini harapannya bisa mendapatkan kesimpulan perbandingan dari kinerja kedua protocol yang akan diuji dari segi kualitas dengan parameter QoS di atas.

1.2 Rumusan Masalah

Agar arah penelitian menjadi sesuai yang diharapkan maka masalah yang dapat dirumuskan adalah bagaimana perbandingan kualitas protokol VPN L2TP+Ipsec dan SSTP pada MikroTik menggunakan metode *Quality of Service* dengan parameter *Throughput, Packet Loss, Delay* dan *Jitter*.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini :

1. Pengujian dilakukan menggunakan penyedia layanan internet kabel IndiHome dengan kecepatan 32Mbps.
2. Metode *tunneling* yang digunakan adalah protokol L2TP+Ipsec dan SSTP menggunakan router MikroTik RB951Ui-2HnD.
3. Pengambilan data pada kedua protokol VPN menggunakan *software* wireshark.
4. Pengujian QoS pada kedua protokol VPN dilakukan dengan variabel *Throughput, Packet Loss, Delay* dan *Jitter*.
5. Pengujian performa dengan *streaming* video di situs YouTube menggunakan kualitas 720p menggunakan *browser* Google Chrome pada kedua protocol VPN, dengan mengabaikan *cache*.
6. Pengujian kedua protokol dilakukan dalam waktu yang tidak bersamaan.
7. Pengujian kedua protokol menggunakan system operasi windows 10.
8. Pengujian kedua protokol mengabaikan faktor x dalam jaringan.

1.4 Tujuan Penelitian

Maksud dan tujuan dilakukannya penelitian ini adalah melakukan analisis perbandingan nilai kualitas kinerja pada protokol VPN L2TP+IPsec dan SSTP paka MikroTik dengan parameter QoS yaitu *Throughput, Packet Loss, Delay* dan *Jitter*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Sebagai perbandingan kinerja kedua protokol VPN pada perangkat jaringan.
2. Sebagai data bahan acuan perbandingan kualitas layanan jaringan pada kedua protokol.
3. Implementasi dan pengembangan teori yang telah di dapatkan selama perkuliahan.

1.6 Sistematika Penulisan

Sistematika dalam penulisan skripsi ini sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi gambaran umum penelitian tentang Latar Belakang Masalah, Batasan Masalah, Maksud dan Tujuan Penelitian, Manfaat penelitian, dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi mengenai tinjauan pustaka yang berkaitan dengan VPN (*Virtual Private Network*), *tunneling*, L2TP, IPsec, SSTP, QoS, serta teori yang mendukung dalam penelitian ini.

BAB III METODE PENELITIAN

Bab ini memaparkan metode yang akan digunakan dalam penelitian serta pengujian perbandingan kedua protokol sebagai landasan pengetahuan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan implementasi dari pengujian perbandingan kinerja L2TP+IPsec dan SSTP serta analisis perbandingan hasil uji coba kinerja kedua protokol dengan metode QoS.

BAB V PENUTUP

Bab ini adalah penutup penelitian dari penulisan skripsi yang terdapat simpulan dari penelitian yang dilakukan berdasarkan data yang telah diproses, serta terdapat saran untuk mengembangkan penelitian dan analisis lebih dalam.