BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya teknologi saat ini yang sangat pesat membuat masyarakat membutuhkan banyak informasi khususnya didalam jaringan internet dan menjadikan internet sebagai salah satu kebutuhan utama melakukan kegiatan sehari-hari. Berbagai aktivitas manusia menurut aspek Pendidikan, Kesehatan, Sosial dan Ekonomi. Namun banyak yang tidak mengetahui bahwa menjalankan komunikasi secara online sebenarnya bukan tanpa gangguan [1]. Adapun gangguan yang mengakibatkan data dari pengguna menjadi tidak aman dikarenakan akses dari jaringan public sehingga data dapat dicuri oleh pihak lain. Secara umun jaringan terbagi menjadi dua yaitu jaringan public dan jaringan local. Jaringan public adalah jaringan yang menghubungkan interface jaringan secara global, sedangkan untuk jarigan local adalah jaringan yang menghubungkan client-client dalam satu jaringan local, seperti instansi atau perkantoran. Permasalahan yang terjadi disebabkan komunikasi yang dilakukan secara tidak langsung (online). Oleh sebab itu data serta jaringan menjadi tidak aman [2].

Dari masalah diatas ada beberapa cara untuk mengatasi permasalahan tersebut, dalam keamanan jaringan berbagai keamanan diterapkan, hadirnya *firewall* telah banyak membantu dalam pengamanan, akan tetapi seiring berkembangnya teknologi saat ini hanya dengan *firewall* keamanan tersebut belum dapat dijamin sepenuhnya. Dengan demikian perlu ditambahkan keamanan jaringan tambahan diantaranya dengan penggunaan VPN *(Virtual Private Network)* yang bisa autentikasi, menjaga keamanan dan kerahasiaan data. VPN *(Virtual Private Network)* merupakan suatu jaringan komunikasi local yang menumpang dalam jaringan public. Dengan VPN, keamanan jaringan akan lebih mudah diatur dan dikontrol. Teknologi VPN memungkinkan setiap orang dapat mengakses jaringan local dari luar dengan menggunakan internet. VPN merupakan suatu bentuk metode yang

menggunakan enkripsi keamanan data menjadi terjamin. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data sudah teracak, jaringan VPN merupakan jaringan yang dibangun di atas sebuah Tunnel. Tunnel VPN mempunyai fungsi sebagai jalur yang bertanggung jawab atas keamanan dari data yang berjalan di dalamnya. Pada penerapan VPN ini juga terdapat fitur metode *tunnel* yang dapat di kombinasikan [3].

Istilah *Tunnel* atau sering disebut juga dengan Teknik *tunneling*. Dalam proses *tunneling* data yang di kirim akan di bungkus *(encapsulation)* oleh protocol lain. Untuk melakukan pembungkusan suatu paket data dapat digunakan berbagai protocol yang memang dirancang untuk melakukan *tunneling*. Protocol *tunnel* yang sering digunakan ialah PPTP, L2TP, SSTP, IPSEC dan OPEN VPN. Dari berbagai macam protocol tersebut L2TP *(Layer 2 Tunneling Protocol)* dan IPSEC *(Internet Protocol Security)* akan di pilih untuk digunakan pada penelitian ini, dimana L2TP berfungsi sebagai *Tunneling* dan IPSec yang berfungsi sebagai mekanisme keamanannya. L2TP merupakan pengembangan dari PPTP yang ditambah L2F. *Network security protocol* dan *enkripsi* yang digunakan untuk melakukan autentikasi yang sama dengan PPTP. L2TP *(Layer 2 Tunneling Protocol)* merupakan terowongan atau saluran yang aman *(Tunnel Secure)* yang berguna untuk mengatur alur IP yang menggunakan PPP *(Point-to-point Protocol)* untuk di transmisikan melalui jaringan TCP/IP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk melakukan keamanan yang lebih baik, L2TP akan dikombinasikan dengan IPSec. IPSec sendiri menggunakan *kriptografi* untuk melindungi komunikasi data yang melewati jaringan Internet Protocol (IP). Dengan menggunakan IPSec dapat memberikan tingkat keamanan yang tinggi [4]. Pada Implementasi VPN L2TP kali ini menggunakan IPSec yang biasa disebut L2TP/IPSec. Penggunaan L2TP/IPSec pada Mikrotik adalah untuk lebih menjaga keamanan data yang melalui VPN, suatu metode seperti enkripsi data menjadi salah satu kemampuan yang harus dimiliki oleh VPN. IPSec *(Internet Protocol Security)* merupakan suatu protocol pertukaran data pada IP

secara aman. IPSec dapat digunakan untuk memproteksi satu atau lebih jalur antara sepasang host, antara sepasang *security gateway*, atau antara *security gateway* dengan *host*. Jadi pada penelitian kali ini *router* akan digunakan sebagai VPN *server* dan VPN *client*. Router yang digunakan adalah Mikrotik router, yang merupakan salah satu router yang mendukung L2TP dan IPSec serta dengan menggunakan metode *Quality of Service* untuk mendukung mekanisme pada jaringan yang menentukan bahwa layanan dapat beroperasi sesuai dengan standart kualitas layanan yang telah diterapkan untuk mendapatkan hasil packet data *streaming, browsing* dan *download file* yang akan dianalisa untuk memperoleh nilai *throughput, packet loss, delay* dan *jitter*.

1.2 Perumusan Masalah

Bagian ini memuat penjelasan tentang permasalahan sehingga memerlukan solusi penelitian. Permasalahan yang diuraikan dalam latar belakang masalah dirumuskan kembali secara tegas dan jelas dalam bentuk poin-poin yang terinci yang berisi masalah-masalah yang akan dikaji pada penelitian.

1. Bagaimana cara membangun dan mengetahui tingkat keamanan jaringan VPN menggunakan protokol L2TP/IPSec menggunakan mikrotik ?
2. Bagaimana cara mengetahui kualitas kinerja jaringan VPN dengan protocol L2TP/IPSec dengan menggunakan parameter *Quality of Service* ?
3. Bagaimana mengimplementasikan jaringan VPN L2TP/IPSec pada keamanan Mikrotik ?

1.3 Batasan Masalah

Adapun batasalan masalah dari penelitian ini, sebagai berikut :

1. Perangkat yang digunakan Mikrotik Router RB941-2 nD-TC
2. Konfigurasi Mikrotik menggunakan aplikasi WinBox pada perangkat laptop.

3. *Virtual Private Network* yang dirancang menggunakan protokol *Layer 2 Tunneling Protocol* dan IPSec (L2TP/IPSec).
4. Implementasi serta pengujian jaringan VPN dilakukan dengan menggunakan metode QoS *(Quality of Service)*.
5. Menggunakan IP *address* versi 4.
6. Metode *Tunneling* yang digunakan adalah L2TP/IPSec.
7. Konfigurasi akan di Implementasikan pada Mikrotik.

1.4 Tujuan Penelitian

Adapun maksud dan tujuan penelitian ini, sebagai berikut :

1. Penelitian ini bertujuan untuk mengamankan jaringan pada saat bertukar informasi secara *online*.
2. Untuk mengimplementasikan jaringan *Virtual Private Network* (VPN) L2TP/IPSec pada Mikrotik.
3. Untuk mengetahui cara menyetting IP publik di Mikrotik agar terhubung ke jaringan internet.
4. Untuk mengetahui tingkat keamanan data menggunakan aplikasi yang terdapat pada *Virtual Private Network* (VPN) yaitu L2TP/IPSec.
5. Untuk menghasilkan perancangan *Virtual private Network* (VPN) *server* menggunakan IP *Tunneling* sehingga dapat memberikan keamanan dan kemudahan koneksi antar *client server*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini, sebagai berikut :

1. Sebagai acuan untuk mengembangkan fitur pada perangkat jaringan seperti Router.
2. Untuk meningkatkan kualitas suatu jaringan sesuai kebutuhannya diantara L2TP maupun IPSec.
3. Supaya dapat membedakan kualitas layanan *(service)* jaringan pada protocol terkait.
4. Sebagai sarana mengaplikasikan ilmu yang sudah didapat dalam perkuliahan.

1.6 Metode Penelitian

Penelitian ini menjabarkan cara-cara memperoleh data yang digunakan sebagai hasil dari penelitian untuk memecahkan masalah yang akan dibahas. Peneliti menggunakan beberapa metode dalam penelitian yaitu sebagai berikut:

1.6.1 Metode pengumpulan data

Pada tahap ini pengumpulan data sangatlah penting, karena tujuannya adalah mengalisa tingkat keamanan data dan jaringan. Oleh karena itu untuk mendapatkan data yang valid perlu adanya pengumpulan data. Pengumpulan informasi melalui Studi Pustaka dengan cara memahami metode-metode pada penelitian sebelumnya yang sidah diteliti lalu di implementasikan melalui literatur, buku ataupun jurnal yang membahas tentang keamanan jaringan menggunakan VPN dan *Tunneling*.

1.6.2 Metode Analisis

Analisis merupakan tahapan awal yang dilakukan dalam menganalisa kebutuhan dan menganalisa permasalahan yang muncul, pada tahap ini yang dilakukan adalah menganalisis secara teknis serta mencari tahu dimana letak kelemahan jaringan serta data yang terjadi pada internet.

1.6.3 Metode Perancangan

Dalam metode ini perlu dilakukan Langkah-langkah perancangan jaringan agar mendukung perkembangan jaringan. Dalam melakukan perancangan jaringan harus menentukan layanan jaringan agar dapat mendukung perancangan arsitektur yang bertujuan untuk menghasilkan desain jaringan yang signifikan.

1.6.4 Metode Implementasi

Pada tahap ini akan dilakukan konfigurasi pada Mikrotik untuk menentukan IP *address* pada perangkat yang ada pada VPN, melakukan konfigurasi *gateway* dan konfigurasi L2TP/IPSec.

1.7 Sistematika Penulisan

Sesuai dengan petunjuk penulisan laporan skripsi yang berlaku di Universitas Amikom Yogyakarta, sistematika penulisan laporan ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pendahuluan merupakan bab pertama yang berisi latar belakang, rumusan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori yang di gunakan dalam penelitian, implementasi dan pembuatan sistem.

BAB III METODE PENELITIAN

Berisi tentang penjelasan alat, bahan, alur penelitian, dan desain yang dibutuhkan untuk penyelesaian skripsi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang pembahasan yang di peroleh dari semua penelitian yang telah dilakukan, sehingga dapat dilakukan pembuktian hasil.

BAB V PENUTUP

Menguraikan kesimpulan dari hasil penelitian dan saran untuk bahan pertimbangan agar penelitian ini dapat di kembangkan di penelitian berikutnya.

DAFTAR PUSTAKA

Bagain ini berisikan daftar referensi yang telah digunakan dalam penelitian dan penulisan.