BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Semakin canggihnya teknologi digital masa kini membuat perubahan besar terhadap dunia. Berbagai kalangan dimudahkan dalam mengakses suatu informasi melalui banyak cara, serta dapat menikmati fasilitas dari teknologi digital dengan bebas dan terkendali. Meski begitu, dunia digital tidak sepenuhnya aman dari serangan peretasan. Sehingga dibutuhkannya sistem keamanan yang tepat untuk mengatasi masalah tersebut.

Maka dari itu dilakukannya sebuah percobaan menggunakan sistem keamanan jaringan berbasis *Virtual Private Network* (VPN) pada mikrotik. VPN dipilih dikarenakan sebuah solusi hemat biaya untuk membangun koneksi *private* melalui jaringan publik atau internet. VPN digunakan untuk menghubungkan dua titik dengan satu kabel atau satu jalur internet yang terhubung langsung meskipun secara fisik jauh. Jenis VPN yang digunakan adalah *Open*VPN, dimana aplikasi tersebut bekerja membuat koneksi *point-to-point tunnel* yang telah ter-*enkripsi*. *Open*VPN menggunakan *private keys, certificate*, atau *username* dan *password* untuk melakukan authentifikasi dalam membangun sebuah koneksi [1]. Dengan adanya proses *enkripsi* dan *autentifikasi*, data yang melewati jaringan internet tidak mudah diketahui dan dimanipulasi oleh pihak yang tidak bertanggung jawab sehingga proses pertukaran informasi dapat berjalan dengan aman [2]. Ada beberapa teknologi VPN yang digunakan pada saat ini, diantaranya *Point -to-Point Tunneling Protocol* (PPTP), *Layer* 2 *Tunnel Protocol/IP Security* (L2TP/IPSec), OpenVPN, *Secure Socket Tunneling Protocol* (SSTP), dan *Internet Key Exchange version* 2 (IKEv2) [3].

VPN yang digunakan peneliti yakni VPN dengan metode (*Source Soucket Tunneling Protocol*) SSTP. Terdapat 2 *enkripsi* yang dapat digunakan dalam SSTP yakni tanpa menggunakan sertifikat yang pada umumnya menggunakan *port* jenis 80 dengan *encoding* AES256-CBC (HTTP) dan menggunakan sertifikat *port* yang digunakan yakni *port* 443 dengan *encoding Rivest Chipher* 4 (RC4) [1]. Port 443

digunakan untuk mengakses *Hypertext Transfer Protocol Secure* (HTTPS) melalui *Source Soucket Layers* (SSL) sertifikat, dimana ketika dilakukannya sebuah *scan* seolah-olah aksesnya ke *websit*e HTTPS sehingga jarang sekali *port* ini diblokir oleh *Internet Service Provider* (ISP) dan juga memiliki kemampuan untuk mencegah masalah *firewall NAT* karena dapat menerobos sebagian besar *firewall.* SSL beroperasi di layer 4-7 pada model referensi OSI [4]. Akan tetapi dalam proses penelitian ini dilakukan di kampus Institut Teknologi Telkom Purwokerto dengan menggunakan jaringan topologi yang ada pada BMKG Sultan Thaha Jambi. Meskipun dilakukan ditempat berbeda dengan alamat IP LAN dan IP WAN berbeda akan tetapi tujuan peneliti sama yakni menganalisis sistem keamanan jaringan VPN dengan metode SSTP pada mikrotik.

Penelitian yang dilakukan oleh Muhammad Naufal yang berjudul "Analisa *Quality of Service* Jaringan Vpn Menggunakan Protokol SSTP Dan *Open*VPN" meneliti tentang bagaimana QoS pada jaringan VPN yang menggunakan protokol SSTP dan *Open*VPN berdasarkan parameter *delay, jitter, throughput,* dan *packet loss* saat menggunakan layanan FTP (*File Transfer Protocol)* dan video *streaming.* Dari hasil yang didapat dapat diketahui bahwa Nilai *delay* pada OpenVPN lebih kecil dibandingkan dengan SSTP dengan selisih berturut-turut sebesar 8.2%, 9.2%, 15.3% dan 37.6% saat menggunakan layanan FTP. Sedangkan saat menggunakan layanan *video streaming*, nilai *delay* pada SSTP dan *Open*VPN bernilai hampir sama dengan selisih antara 0% sampai 1%. Nilai *jitter* pada OpenVPN lebih kecil dibandingkan dengan SSTP dengan selisih antara 33% hingga 39,02% saat menggunakan layanan FTP. Sedangkan saat menggunakan layanan video *streaming*, nilai *jitter* antara SSTP dan *Open*VPN bernilai hampir sama dengan selisih antara 1.03% sampai 1.12 %. 3. Nilai *throughput* pada *Open*VPN lebih besar dibandingkan dengan SSTP dengan selisih berturut-turut sebesar 7.3%, 11.6%, 14,6 dan 37% saat menggunakan layanan FTP. Sedangkan saat menggunakan layanan *video streaming*, nilai *throughput* pada SSTP dan *Open*VPN bernilai hampir sama dengan selisih antara 0% sampai 1.2%. 4. Nilai *packet loss* pada SSTP dan *Open*VPN bernilai sama sebesar 0% pada layanan FTP dan video *streaming* [2].

Selain itu penelitian yang dilakukan oleh Moezes Rasuanda dan Haeruddin yang berjudul "Perbandingan Performa VPN Menggunakan PPTP dan SSTP *Over* SSL dengan Metode *Quality of Service*" meneliti tentang menguji serta membandingkan performa *Quality of Service* dari PPTP dan SSTP untuk menngukur seberapa baiknya jaringan tersebut dan juga memastikan pengguna mendapatkan kualitas dari servis yang terbaik. Dari hasil penelitian dapat disimpulkan secara teori yaitu VPN PPTP memiliki kelebihan dimana mendukung semua sistem operasi desktop dan seluler, *set up* konfigurasi sederhana, dan memiliki kecepatan yang baik dengan kekurangan mudah untuk diblokir oleh ISP karena tingkat *enkripsi* tidak begitu tinggi. VPN SSTP memiliki kelebihan dimana mampu menembus *firewall*, dan terdukung penuh oleh sistem operasi *Windows*. Sedangkan kekurangan dari VPN ini ialah tidak bisa melakukan *backdoor*, dan sementara masih terfungsi hanya pada *platform Windows* [5].

Berdasarkan beberapa penelitian diatas maka penulis berinisiatif untuk melakukan penelitian mengenai tingkat keamanan yang terdapat pada SSTP. Penelitian ini dilakukan untuk mengetahui bagaimana rancangan sistem keamanan jaringan menggunakan SSTP serta mengetahui apakah sistem dengan metode SSTP mampu melakukan *enkripsi* data dengan baik. Keberhasilan peneliti dapat dinilai dari keberhasilan dalam membuktikan bahwa protokol SSTP mampu menjaga kerahasiaan data agar tidak bocor. Untuk membuktikan tingkat keamanan tersebut penulis menggunakan aplikasi *Wireshark.* Serta mencoba melakukan serangan menggunakan *Attacking DoS.* Dari hasil penelitian yang diperoleh dapat disimpulkan bahwa dengan menggunakan HTTPS maka akan meminimalisir adanya pencurian data dari pihak lain karena didalam sertifikat sudah memiliki tanda pengenal tersendiri seperti organisasi, wilayah, dan lain sebagainya.

1.2 RUMUSAN MASALAH

1. Apakah sistem jaringan SSTP mampu melakukan *enkripsi* data dengan baik?
2. Bagaimanakah rancangan pada sistem keamanan jaringan SSTP?

1.3 BATASAN MASALAH

1. Penelitian ini dilakukan di kampus Institut Teknologi Telkom Purwokerto dengan menggunakan topologi jaringan yang ada di BMKG Jambi.
2. Implementasi jaringan dilakukan secara langsung menggunakan jaringan internet kampus Institut Teknologi Telkom Purwokerto sebagai jaringan publik.
3. Dalam pengujian VPN SSTP dilakukan dengan menggunakan *certificate*.
4. Pengujian ini dilakukan dengan menganalisa cara kerja dari SSTP.
5. Mencoba melakukan serangan DoS dengan menggunakan *pingflooding.*
6. Dalam pengujian *wireshark* hanya melihat apakah jaringan SSTP ter-*enksripsi* atau tidak.

1.4 TUJUAN PENELITIAN

1. Menganalisa tingkat keamanan VPN SSTP pada mikrotik menggunakan *wireshark.*
2. Mengamati cara kerja dari sistem keamanan jaringan VPN SSTP.

1.5 MANFAAT PENELITIAN

Hasil dari penelitian dapat digunakan untuk mempertimbangkan sistem *enkripsi* keamanan jaringan VPN mana yang aman dan mudah digunakan oleh perusahaan-perusahaan lain.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian ini dibagi menjadi 4 bagian :

1. BAB 1 : PENDAHULUAN

   Bab ini berisi tentang latar belakang yang diambil dari judul proposal skripsi, rumusan masalah, Batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan proposal skripsi yang menjelaskan secara garis besar substansi yang diberikan pada masing-masing bab.
2. BAB 2 : DASAR TEORI

Pada bagian ini membahas dan menjelaskan teori yang berkaitan dengan judul/masalah di proposal skripsi ini.

3. BAB 3 : METODE PENELITIAN

   Bab ini membahas bagaimana cara perancangan infrastruktur dalam melakukan penelitian, serta parameter-parameter yang digunakan dalam penulisan judul proposal ini.

4. BAB 4 : HASIL DAN ANALISA

   Bab ini membahas tentang hasil dan analisa dari penelitian yang telah dilakukan.

5. BAB 5 : KESIMPULAN DAN SARAN

   Berisi tentang kesimpulan yang diperoleh dari penelitian dan saran yang ditunjukkan untuk perbaikan dalam melakukan penelitian.