BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia Teknologi Informasi saat ini sudah sangat pesat khususnya untuk Internet, begitu banyak Aktifitas manusia yang banyak menjadi lebih cepat diselesaikan dengan adanya Teknologi Internet tersebut. Pertukaran informasi dari satu tempat ke tempat lain menjadi mudah dan sangat cepat berkat adanya internet. Akan tetapi dari segi keamanan walaupun internet memiliki berbagai Jenis *Protocol* keamanan akan tetapi masih banyak orang-orang dapat menembus keamanan jaringan sehingga terjadi pencurian data-data pada sebuah perusahaan.

Contohnya seperti di Perusahaan, Kampus, Rumah Sakit dan lain-lain begitu banyak informasi penting yang bisa dicuri oleh orang yang tidak bertanggung jawab tentu akan sangat merugikan pihak tersebut oleh karena itu dibutuhkan sebuah cara atau metode yang dapat mengurangi bahkan menghilangkan berbagai tindak pencurian data informasi yang dilakukan melalui Jaringan internet dengan menggunakan *Virtual Private Network* (VPN). *Virtual Private Network* (VPN) merupakan salah satu cara untuk melindungi pertukaran data informasi melalui Jaringan internet, khususnya dengan menggunakan Protokol *Secure Socket Tunneling Protokol* (SSTP) dapat membuat komunikasi antar beberapa Jaringan melalui sebuah *Tunneling* yang melewati Jaringan internet dengan aman. (Kaseger Arthur Farly, Xaverius B. N. Najoan,Arie S. M. Lumenta : 2017).

Secure Socket Tunneling Protokol (SSTP) adalah tembusan protokol yang tersedia pada platform Microsoft. Protokol ini berbasis pada kombinasi kedua teknologi, SSL dan TCP. Teknologi SSL menjaminkan tingkat keamanan transportasi dan integritas lalu lintas. SSL pada server kami dikonfigurasikan

sedemikian rupa sehingga hanya metode enkripsi terkuatlah yang diaktifkan. SSTP bisa digunakan melalui firewall atau ISP throttling. Sejak SSTP beroperasi melalui TCP, dalam beberapa kasus akan dikendalikan IKEv2 atau protokol berbasis UDP lainnya. Secara keseluruhan, SSTP adalah pilihan terbaik dan dapat membantu menyelesaikan masalah konektivitas ataupun masalah kecepatan yang dimiliki. SSTP memiliki keunggulan dalam hal keamanan (Secure) dibanding dengan L2TP, PPTP dan PPP. (Ikhwan Ruslianto, Uray Ristian : 2019).

Pada router gateway menggunakan Mikrotik dilakukan konfigurasi meliputi pembuatan template Certificate Authority (CA), Serverdan Client Certificate, export certificateyang telah dibuat yang digunakan oleh PC Client Internetyang bertindak sebagai SSTP Client, pengaktifan fitur SSTP Serverdan pembuatan akun pengguna untuk koneksi dari SSTP Client.Hasil pengaktifan SSTP Server. (I Putu Hariyadi1, Raisul Azhar : 2017).

Salah satu fitur VPN yang ada di MikroTik adalah SSTP (*Secure Socket Tunneling protocol*). SSTP merupakan sebuah *PPP Tunnel* dengan *TLS 1.0 Channel*. Fitur ini berjalan pada protokol TCP dan *Port* 443. Supaya dapat memanfaatkan SSTP secara optimal dengan keamanan yang baik, maka diharuskan menambahkan sertifikat SSL untuk koneksi antara *server* dan *client*. (Wa Ode Zamalia, L.M. Fid Aksara, Muh. Yamin : 2018).

Dalam metode SSTP memiliki kelebihan yakni kemampuan untuk menerobos kebanyakan firewall, sehingga mudah untuk mengamankan data-data yang ada pada rumah sakit tersebut.

Penelitian ini dilakukan untuk mengetahui kualitas layanan (QoS) pada jaringan yang menerapkan site to site VPN. Penelitian ini dilakukan guna memperoleh apakah terdapat pengaruh yang significant apabila suatu file dengan

type yang berbeda dilewatkan pada jarfingan yang menerapkan VPN terutama pada saat menerapkan protocol SSTP. Penekanan hasil penelitian diutaman pada unjuk kerja performa jaringan berdasarkan parameter QoS *(Quality of Serfice)* antara jaringan yang tidak menerapkan VPN dengan jaringan yang menerapkan VPN terutama pada pemanfaatan protocol SSTP pada jaringan kantor pusat dan kantor cabang. VPN atau jaringan dengan dua tempat yang saling berjauhan dengan menetapkan paramter-paramter tersebut untuk mengetahui apakah aspek keamanan telah dapat terpenuhi. (Raisul Azhar : 2017).

Hasil implementasi VPN SSTP di Data Utama Semarang diambil kesimpulan tunnel SSTP dapat dipakai dalam pembangunan komunikasi VPN untuk me*remote* jaringan dapat berjalan dengan baik. NOC dapat mengatur konfigurasi jaringan diluar kantor sehingga dapat mengatasi trouble pada jaringan. Dari hasil uji delay dapat disimpulkan bahwa delay yang dilakukan dengan cara ping setelah terkoneksi VPN lebih lama karena dilakukan proses encasulasi dan decapsulasi. (Fendy Febrianto : 2016).

Dari masalah tersebut, maka penulis ingin mencoba membuat jaringan VPN agar data-data keuangan, data dan informasi pada rumah sakit tersebut dapat di amankan dengan menggunakan VPN metode *Secure Socket Tunneling Protokol* (SSTP). Maka dibuatlah penilitian tentang **"PERANCANGAN DAN IMPLEMENTASI VPN *SERVER* DENGAN MENGGUNAKAN METODE SSTP (*SECURE SOCKET TUNNELING PROTOCOL*) DI RSUD KOTA SAWAHLUNTO"**

1.2 Rumusan Masalah

Dari uraian latar belakang masalah diatas dapat dirumuskan masalah yang dihadapi, yaitu :

1. Bagaimana *Virtual Private Network* (VPN) metode *Secure Socket Tunneling Protocol* (SSTP) memberikan solusi jaminan keamanan data pada RSUD Sawahlunto ?
2. Bagaimana perancangan dan implementasi jaringan *Virtual Private Network* (VPN) pada RSUD Sawahlunto dapat diterapkan dengan maksimal ?
3. Bagaimana keamanan data yang di peroleh setelah diimplementasikan *Virtual Private Network* (VPN) metode *Secure Socket Tunneling Protocol* (SSTP) pada RSUD Sawahlunto ?

1.3 Hipotesa

Berdasarkan rumusan masalah diatas, maka dapatlah hipotesa sebagai berikut:

1. Dengan adanya *Virtual Private Network* (VPN) metode *Secure Socket Tunneling Protocol* (SSTP) ini diharapkan dapat memberikan solusi dalam keamanan data pada RSUD Sawahlunto .
2. Dengan adanya *Virtual Private Network* (VPN) metode *Secure Socket Tunneling Protocol* (SSTP) ini diharapkan dapat diimplementasikan intuk keamanan data pada RSUD Sawahlunto.
3. Dengan adanya *Virtual Private Network* (VPN) metode *Secure Socket Tunneling Protocol* (SSTP) hasil implementasi metode ini diharapkan dapat berfungsi sebagai keamanan data pada RSUD Sawahlunto.

1.4 Batasan Masalah

Agar penilitian ini terarah dan tepat sasaran sehingga tujuan penulis tercapai, maka perlu adanya batasan masalah yang diteliti, yaitu :

1. Penilitan ini hanya menggunakan metode SSTP (*Secure Socket Tunneling Protocol*) dalam pengimplementasian *Virtual Private Network* (VPN) di RSUD Sawahlunto.
2. Pada penilitian implementasi *Virtual Private Network* (VPN) menggunakan Mikrotik *Router Operating System*.
3. Pada penilitian ini tidak membahas bagaimana cara untuk membobol jaringan *Virtual Private Network* (VPN).
4. Penilitian dilakukan khusus untuk perancangan jaringan *Virtual Private Network* (VPN).

1.5 Tujuan Penilitian

Adapun tujuan dari penilitan ini adalah sebagai berikut :

1. Dapat mengimplementasikan *Virtual Private Network* (VPN) dengan metode *Secure Socket Tunneling Protocol* (SSTP) pada RSUD Sawahlunto.
2. Untuk memberikan solusi keamanan dalam trasmisi data atau informasi jaringan komputer yang diterapkan pada RSUD Sawahlunto.
3. Untuk mengetahui perbandingan data yang di peroleh setelah menggunakan *Virtual Private Network* (VPN) dengan yang tidak menggunakan *Virtual Private Network* (VPN).

1.6 Manfaat Penilitian

Manfaat dari penilitian ini adalah sebagai berikut :

1. Memberikan kenyamanan bagi instansi rumah sakit dalam masalah data-data agar tidak diketahui maupun dicuri pihak luar.
2. Mendapatkan koneksi yang aman serta stabil saat download data maupun upload data setelah diimplementasikan *Virtual Private Network* (VPN) metode SSTP di RSUD Sawahlunto .
3. Mengetahui lebih jauh tingkat efektivitas, efisiensi dan keamanan komunikasi data di internet menggunakan *Virtual Private Network* (VPN) dengan metode SSTP di RSUD Sawahlunto.