BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Dalam era digital yang terus berkembang, akses jarak jauh menjadi semakin penting bagi organisasi dan individu. Namun, seiring dengan kemudahan akses jarak jauh juga datang tantangan keamanan yang signifikan. Keamanan data dan informasi sensitif sangat penting untuk dijaga selama proses transmisi dan akses jarak jauh. Oleh karena itu, perancangan sistem keamanan yang andal diperlukan untuk melindungi data dari ancaman yang mungkin terjadi selama proses transmisi dan akses jarak jauh.

Virtual Private Network (VPN), merupakan salah satu alternatif untuk pengamanan data karena bersifat privat. VPN memungkinkan pengguna dapat masuk ke dalam jaringan lokal, memungkinkan pengguna untuk mengambil data dari dalam jaringan lokal serta melakukan remote pada perangkat yang ada di jaringan tersebut. Menurut (ayu 2020) dalam (Musril, 2019) bahwa Jaringan *Virtual Private Network (VPN)* merupakan pengguna teknologi GRE *Tunnel*, untuk menghubungkan lebih dari satu router lainnya. Dengan protokol GRE yang digunakan mampu menghantarkan paket. Sebagai tambahan, di definisikan oleh cisco.com virtual *private network* adalah suatu koneksi yang menggunakan internet sebagai media untuk menghubungkan suatu perangkat ke jaringan lokal. Koneksi ini terenkripsi untuk menjamin bahwa data dapat terkirim dengan aman.

VPN memungkinkan pengguna untuk membentuk koneksi aman melalui jaringan publik seperti internet, sehingga data yang dikirimkan antara pengguna dan sumber daya jaringan yang terhubung tetap terenkripsi dan terlindungi dari mata-mata yang tidak sah. Dalam konteks ini, peneliti ingin menggunakan protokol yang umum digunakan untuk membentuk koneksi VPN yang aman adalah IPsec *(Internet Protocol Security)*

IPsec dikenal sebagai Keamanan IP. Dalam IPsec, paket data yang dikirim melalui L2TP VPN dapat di enkapsulasi lebih lanjut untuk membuat komunikasi antara server dan klien lebih aman. Ada proteksi ganda dalam keamanan jaringan: proteksi pertama menciptakan koneksi *Point-to-Point* antar pengirim, sedangkan proteksi kedua adalah enkripsi untuk keamanan yang memanfaatkan IPsec . (J. Safira, Hanafi dan Munawar, 2021) Penggunaan IPsec dalam perancangan keamanan data pada jarak jauh melalui VPN akan memberikan lapisan keamanan tambahan yang kuat dan dapat diandalkan.

Menurut Apriyanto & Wahyuni (2019), SSL atau singkatan dari *Secure Socket Layer* adalah teknologi keamanan standar mendirikan sebuah link yang terenkripsi antara server dan klien, biasanya dikenal dengan server website dan browser atau email server dan email klien (umpamanya, *Microsoft Outlook*). SSL sendiri adalah teknologi yang dibutuhkan untuk mengamankan komunikasi dan transfer data di antara web server dan user. Penggunaan SSL/TLS dalam perancangan keamanan data pada jarak jauh melalui VPN akan memberikan tingkat enkripsi yang tinggi dan juga memberikan perlindungan terhadap serangan *man-in-the-middle*.

Beberapa penelitian terdahulu yang berhubungan dengan penelitian ini yaitu Perancangan Jaringan *Virtual Private Network* Berbasis Ip *Security* Menggunakan Router Mikrotik Penelitian ini membahas Tentang konfigurasi jaringan VPN (*Virtual Private Network*) menggunakan perangkat MikroTik. VPN digunakan untuk mengamankan komunikasi dan akses jaringan dari lokasi yang berbeda, termasuk koneksi antara perangkat lokal dan server yang terhubung ke internet (Sulistiyono 2020). Penelitian ini membahas tentang perbedaan antara IP Public (alamat-alamat IP yang digunakan untuk jaringan internet) dan IP Private (yang digunakan untuk jaringan lokal seperti sekolah, kantor, dan lainnya). Pengujian dilakukan untuk memastikan koneksi VPN berhasil terhubung, pengiriman data terenkripsi dengan IPsec, dan penggunaan aplikasi Winbox untuk meremote router lokal. Pengujian juga mencakup percobaan file *sharing* melalui VPN untuk mengakses file dari router server.

Penelitian berikutnya adalah Rancang Bangun *File Transfer Protocol* (FTP) Dengan Pengamanan *Open* SSL Pada Jaringan VPN Mikrotik di SMK Dwiwarna Judul ini membahas Tentang implementasi *File Transfer Protocol* (FTP) server dengan pengamanan menggunakan *Open* SSL pada jaringan VPN MikroTik di SMK SDwiwarna. Penelitian ini bertujuan untuk membangun FTP server dengan lapisan keamanan SSL (*Secure Socket Layer*) yang diintegrasikan dengan jaringan VPN PPTP (*Point-to-Point Tunneling Protocol*) menggunakan perangkat MikroTik di sekolah SMK Swiwarna. dengan nama Pengarang Devi Ruwaida dan Dian Kurnia (2019).

Implementasi *Virtual Private Network* Menggunakan L2TP/IPsec pada BBPK Jakarta Judul Ini Membahas Tentang implementasi jaringan Virtual Private Network (VPN) menggunakan Layer 2 *Tunneling Protocol* (L2TP) pada Balai Besar Pelatihan Kesehatan Jakarta (BBPK Jakarta). dengan nama Pengarang Sumarna dan Maulana (2021)

Menurut Iswa (2019), ada beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN:

1. Menjaga privasi dengan baik.
2. Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain.
3. Penggunaan VPN juga dapat mengurangi biaya telpon untuk akses jarak jauh, karena hanya dibutuhkan biaya telpon untuk panggilan ke titik akses yang ada di ISP terdekat.
4. Biaya operasional perusahaan juga akan berkurang bila menggunakan VPN. Hal ini disebabkan karena pelayanan akses dial-up dilakukan oleh ISP, buka oleh perusahaan yang bersangkutan.
5. Penggunaan VPN akan meningkatkan skalabilitas.
6. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang mobile dapat mengakses

7. jaringan khusus perusahaan di manapun selama bisa mendapatkan akses internet.

PT. Tanjungenim Lestari *Pulp & Paper* adalah perusahaan yang berfokus pada produksi kertas dan pulp. PT. Tanjungenim Lestari *Pulp & Paper* terletak di Tanjung Enim, Sumatera Selatan, Indonesia. Tanjung Enim adalah salah satu kota di Provinsi Sumatera Selatan yang terkenal sebagai pusat industri pulp dan kertas di Indonesia. Pabrik atau fasilitas produksi perusahaan ini mungkin berlokasi di daerah tersebut untuk memanfaatkan sumber daya alam seperti kayu dan serat yang diperlukan dalam proses produksi pulp dan kertas. Bagi pengguna internet yang memerlukan privasi dalam berkomunikasi tentunya ada masalah – masalah yang muncul dalam situasi sehari-hari. PT. Tanjungenim Lestari *Pulp & Paper* memiliki masalah pengiriman data yang tidak aman dapat mengancam tingkat kerahasiaan, terutama saat data dikirim ke perusahaan konsumen di daerah lain, yang dapat di pengaruhi oleh faktor-faktor seperti jaringan yang tidak aman, enkripsi yang lemah, kurangnya otentikasi, manajemen kunci yang buruk, kurangnya keamanan pada perangkat pengirim dan penerima, serta tidak di proteksikan terhadap ancaman *cyber*, sehingga perusahaan perlu menerapkan langkah-langkah keamanan seperti protokol keamanan kuat, enkripsi end-to-end, otentikasi ganda, dan kebijakan keamanan data untuk menjaga integritas dan kerahasiaan data. Selain itu perusahaan tersebut juga menggunakan jaringan yang terkoneksi ke internet yang memiliki kelemahan yaitu membutuhkan perhatian yang serius pada keamanan jaringan publik (internet).

Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan. Dengan merancang sistem keamanan data pada jarak jauh menggunakan VPN berbasis IPsec dan SSL, organisasi dan individu dapat mengoptimalkan akses jarak jauh sambil tetap menjaga keamanan dan integritas data. Dengan demikian, risiko ancaman keamanan dapat dikurangi dan informasi sensitif dapat dijaga dengan lebih baik selama proses transmisi dan akses jarak jauh. Berdasarkan Latar Belakang tersebut, Maka Penulis ingin mengangkat judul

"**PERANCANGAN KEAMANAN DATA PADA AKSES JARAK JAUH MENGGUNAKAN VPN BERBASIS IP SEC DAN SSL".**

1.2 RUMUSAN MASALAH

Berdasarkan informasi yang telah dijelaskan sebelumnya, masalah utama yang dapat difokuskan dalam penelitian ini adalah: "Bagaimana merancang dan mengimplementasikan arsitektur jaringan yang aman dan efektif menggunakan metode VPN berbasis IPsec dan SSL

1.3 BATASAN MASALAH

Agar penulis tidak menyimpang dan lebih mengarah pada permasalahan yang ada, maka masalah dibatasi adalah Merancang sistem keamanan data jarak jauh menggunakan VPN berbasis IPsec dan SSL.

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah untuk merancang system keamanan jarak jauh dengan menggunakan metode VPN berbasis IPsec dan SSL dalam bentuk simulasi untuk jaringan komputer PT. Tanjungenim Lestari *Pulp & Paper.*

1.5 MANFAAT PENELITIAN

Manfaat penelitian ini adalah agar mengetahui cara mengaplikasikan dan menggunakan VPN berbasis IPsec dan SSL dalam mengamankan data yang dikirim melalui jaringan publik (internet).

Penelitian ini juga dapat membantu menghindari pengeluaran yang tidak perlu dalam pemilihan dan implementasi solusi keamanan jarak jauh. Dengan pemahaman yang lebih baik tentang teknologi yang digunakan, Penulis dapat menghemat biaya dan sumber daya.

Penelitian ini juga akan memberikan wawasan mendalam tentang keamanan jaringan dan teknologi VPN kepada peneliti dan praktisi IT. Hal ini dapat meningkatkan pengetahuan dan keahlian mereka dalam mengelola keamanan informasi.

Manfaat bagi perusahaan yaitu membantu perusahaan menghindari pengeluaran yang tidak perlu dalam pemilihan dan implementasi keamanan jarak jauh. Manfaat bagi penulis selanjutnya. dapat di gunakan sebagai refrensi untuk pengembangan selanjutnya.