

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital perkembangan teknologi saat ini sangat pesat terkait dengan komunikasi data dalam jaringan komputer adalah salah satu perkembangan teknologi yang paling cepat pada saat ini. Seperti dapat ditandai dengan perkembangan perangkat lunak baru untuk mendukung aktivitas di bidang jaringan. Oleh karena itu tugas dari jaringan komputer akan semakin berat, karena semakin banyak aplikasi berbasis jaringan. Ini menyebabkan ketersediaan jaringan komputer dan internet yang tangguh menjadi hal yang sangat penting (Wijayaet al., 2019).

Virtual Private Network (VPN) adalah sebuah *channel* komunikasi yang mampu terotentifikasi dan terenskripsi melalui bentuk suatu *network* yang bersifat mendunia atau bisa disebut dengan internet. *Network* yang bersifat umum atau mendunia dianggap memiliki keamanan yang kurang terjamin. Dari masalah tersebut kemudian muncul sebuah *enkripsi* dan *otentikasi* yang digunakan untuk melindungi sebuah data saat berlangsungnya proses pengiriman maupun pertukaran data, sebuah vpn bersifat *service independent*, atau tidak memiliki ketergantungan pada suatu jenis *service* yang menggunakannya (Umaroh & Rifauddin, 2020).

Keamanan jaringan (*Network Security*) dalam sebuah jaringan komputer sangat penting supaya dapat dikelola dengan baik dan benar sehingga tidak bisa memberikan celah untuk penyalahgunaan sumber daya jaringan. Tugas untuk mengontrol keamanan jaringan adalah admin jaringan, dengan tujuan keamanan

jaringan untuk mengantisipasi resiko berupa bentuk ancaman fisik maupun logika baik secara langsung maupun tidak langsung yang dapat mengganggu aktivitas yang sedang berlangsung dalam sebuah jaringan komputer pada perusahaan. Suatu perusahaan yang memiliki banyak perangkat komputer yang terhubung kedalam jaringan intranet dan memiliki beberapa *server* yang digunakan dalam operasional, beberapa *server* tersebut terdiri dari, *web server*, *database server* dan *server file*. admin jaringan melakukan tugas monitoring trafik jaringan komputer intranet dan trafik yang masuk dan keluar pada *server* (Mukiman et al., 2023).

pada penelitian sebelumnya yang dilakukan oleh Ikhwan Ruslianto dan Uray Ristian, pada tahun 2019 dengan judul perancangan dan *implementasi virtual private network* (VPN) menggunakan protokol SSTP (*secure socket tunneling protocol*) mikrotik di fakultas MIPA Universitas Tanjungpura. Pada penelitian ini dilakukan suatu perancangan dan implementasi *virtual private network* (VPN) untuk melakukan pengaksesan informasi yang bersifat kredensial dengan protokol SSTP (*secure socket tunneling protocol*) yang ada pada sebuah mikrotik sehingga dapat mengurangi permasalahan internet yang kurang maksimal dari sisi kecepatan akses serta keamanan lalu lintas data di lingkungan MIPA Universitas Tanjungpura (Ruslianto & Ristian, 2019).

PT. PLN (PERSERO) ULP BELANTI PADANG merupakan salah satu unit layanan pelanggan PLN yang bertanggung jawab atas distribusi listrik di wilayah tertentu. Sebagai bagian dari infrastruktur energi yang krusial, keamanan jaringan menjadi faktor penting dalam memastikan kelancaran operasi dan ketersediaan layanan bagi pelanggan. Dalam konteks ini, implementasi jaringan VPN (*Virtual Private Network*) dapat menjadi solusi yang efektif untuk

memastikan keamanan komunikasi data antara berbagai lokasi PT. PLN ULP Belanti Padang. Metode SSTP (*Secure Socket Tunneling Protocol*) dipilih karena menawarkan tingkat keamanan yang tinggi melalui enkripsi SSL/TLS, yang sangat penting dalam melindungi data sensitif dan rahasia perusahaan. Dengan adanya jaringan VPN yang terenkripsi, PT. PLN ULP Belanti Padang dapat memastikan bahwa komunikasi antar lokasi, termasuk data pelanggan dan informasi operasional, tetap aman dan terjamin. Hal ini akan membantu meningkatkan keandalan sistem, mengurangi risiko kebocoran informasi, dan meningkatkan efisiensi dalam pengelolaan jaringan. Oleh karena itu saya mengangkat judul perancangan dan implementasi jaringan VPN menggunakan metode SSTP berbasis MikroTik di PT. PLN ULP Belanti Padang ini guna untuk menjadi langkah strategis dalam meningkatkan keamanan jaringan dan mendukung kelancaran operasi perusahaan dalam menjalankan misi penyediaan layanan energi yang handal dan terpercaya.

Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan jaringan VPN menggunakan metode SSTP. Dengan pemahaman yang mendalam tentang karakteristik dan kelebihan SSTP, diharapkan dapat dikembangkan solusi yang efektif dan efisien untuk menyediakan koneksi VPN yang aman dan dapat diandalkan bagi pengguna yang mengakses jaringan dari lokasi yang berbeda.

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu:

"PERANCANGAN DAN IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* MENGGUNAKAN METODE SSTP (*SECURE SOCKET*

***TUNNELING PROTOCOL*) UNTUK KEAMANAN JARINGAN PADA PT. PLN (PERSERO) ULP BELANTI PADANG”.**

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dapat disimpulkan permasalahan yang akan dibahas pada laporan ini sebagai berikut:

1. Bagaimana merancang jaringan VPN menggunakan metode SSTP dengan mempertimbangkan kebutuhan keamanan dan kinerja?
2. Bagaimana langkah-langkah implementasi jaringan VPN menggunakan metode SSTP pada platform jaringan yang sudah ada?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut :

1. Diharapkan perancangan dan implementasi jaringan vpn menggunakan metode SSTP dapat membantu keamanan jaringan pada PT.PLN (Persero) ULP Belanti Padang .
2. Diharapkan perancangan dan implementasi jaringan vpn menggunakan metode SSTP dapat membantu trafik jaringan tetap stabil pada PT.PLN (Persero) ULP Belanti Padang.

1.4 Batasan Masalah

Agar untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka penelitian memberikan batasan masalah yaitu, peneliti akan melakukan analisis terhadap jaringan yang ada pada PT.PLN(persero) ULP Belanti padang untuk mempermudah pihak pengguna dalam pekerjaan. Dengan menggunakan mikrotik sebagai pengujiannya .

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya adalah:

1. Merancang jaringan VPN yang memanfaatkan metode SSTP untuk menyediakan koneksi aman bagi pengguna yang mengakses jaringan dari jarak jauh.
2. Mengevaluasi kinerja jaringan VPN yang diimplementasikan menggunakan metode SSTP, termasuk keandalan koneksi dan tingkat keamanannya.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini yaitu :

1. Memberikan panduan praktis bagi organisasi atau perusahaan yang ingin mengimplementasikan jaringan VPN menggunakan metode SSTP.
2. Meningkatkan pemahaman tentang penggunaan metode SSTP dalam menyediakan koneksi VPN yang aman dan andal.

1.7 Gambaran Umum objek penelitian

1.7.1 Lokasi PT.PLN (PERSERO) Rayon Belanti Padang

PT. PLN (Persero) Wilayah Sumbar Area Padang Rayon Belanti Padang beralamat di Jl. Khatib Sulaiman No.44, Padang, Sumatera Barat, Indonesia. Kontak nomor telepon yang dapat dihubungi melalui telepon (0751)455220.

1.7.2 Visi , Misi , Dan Moto PT.PLN (PERSERO) Rayon Belanti Padang

Visi

Menjadi Perusahaan Listrik Terkemuka se-Asia Tenggara dan #1 Pilihan Pelanggan untuk Solusi Energi.

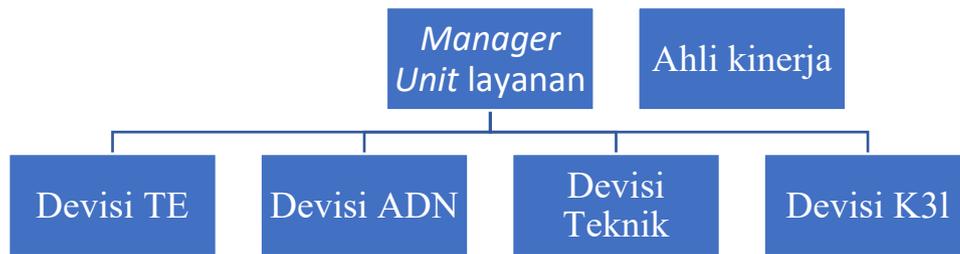
Misi

1. Menjalankan bisnis kelistrikan dan bidang lain yang terkait, berorientasi pada kepuasan pelanggan, anggota perusahaan dan pemegang saham.
2. Menjadikan tenaga listrik sebagai media untuk meningkatkan kualitas
3. kehidupan masyarakat.
4. Mengupayakan agar tenaga listrik menjadi pendorong kegiatan ekonomi.
5. Menjalankan kegiatan usaha yang berwawasan lingkungan.

Moto

“Listrik untuk Kehidupan yang Lebih Baik”

1.7.3 Susunan Kepegawaian PT.PLN (persero) Belanti Padang



Sumber : PT.PLN(Persero)

Gambar 1. 1 susunan kepegawaian PT.PLN (persero) Belanti padang

1.7.4 Tugas pokok fungsi

1. Manager unit layanan
 - a. *Managerial cycle* atau siklus pengambilan keputusan, membuat rencana, menyusun organisasi, pengarahan organisasi, pengendalian, penilaian dan pelaporan.
 - b. Menyusun laporan kinerja Rayon.
 - c. Menyusun data perusahaan yang berhubungan dengan target kinerja.
 - d. Menyusun langkah-langkah strategis untuk mencapai target kinerja.
 - e. Manajer harus membina bawahannya agar dapat bekerja secara efektif dan efisien.
2. Ahli kinerja
 - a. Menganalisa kerja ulp.
 - b. Manajemen Kualitas Layanan.
3. Devisi Transaksi Energi
 - a. Pengelolaan Pembelian dan Penjualan Energi.
 - b. Perencanaan Pasokan Energi.
 - c. Pengaturan Pasokan Listrik.
 - d. Manajemen Kontrak dan Tarif.

- e. Pengembangan Rantai Pasok Energi.
 - f. Pelaporan dan Analisis Kinerja.
4. Divisi Administrasi Niaga
 - a. Menghitung hasil laba dan rugi jual beli listrik.
 - b. Melayani pelanggan baru listrik.
 - c. Pengelolaan Tarif Listrik.
 5. Divisi Teknik
 - a. Untuk pelayanan gangguan jaringan listrik.
 - b. Operasi Jaringan Listrik.
 - c. Pengembangan Infrastruktur Listrik.
 - d. Pengukuran dan Analisis Kinerja Jaringan.
 6. Divisi K3L
 - a. Manajemen Bahan Berbahaya dan Limbah.
 - b. Investigasi Kecelakaan dan Insiden.
 - c. Menyediakan kelengkapan APD (Alat Pelindung Diri).