BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Suatu jaringan idealnya dapat menghubungkan antartitik secara *any to any*. Di masa lalu, perusahaan yang hendak menghubungkan cabang-cabang kantornya dalam suatu jaringan akan mengunakan saluran sewa secara titik ke titik (*point to point*) yang tentu saja biayanya sangat besar.

Dalam sebuah jaringan komputer, keamanan di dalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga, terutama jika data tersebut bersifat rahasia. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan. Banyak metode yang dapat diimplementasikan, seperti penggunaan tanda tangan digital, enkripsi ataupun pemasangan firewall.

Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama dalam reabilitas dalam suatu jaringan. *Virtual Private Network* (VPN) adalah salah satu cara untuk membuat sambungan *any to any* di atas jaringan publik seperti internet, tanpa klien yang satu dengan klien yang lain saling mengetahui yang merupakan suatu cara untuk membuat sebuah jaringan bersifat "*private*" dan aman dengan menggunakan jaringan publik.

Dewasa ini ada beberapa teknik yang dikenal untuk mengembangkan VPN di atas jaringan Internet yaitu *Point to Point Tunnelling Protocol* (PPTP), *Layer* 2

Tunneling Protocol (L2TP), *Secure Socket Layer/ Transport Layer Security* (SSL/TLS) dan *Internet Protocol Security* (IPSec). Kelompok kerja IPSec (di bawah area keamanan) berkonsentrasi pada proteksi lapisan jaringan dengan merancang mekanisme keamanan pengacakan (kriptografi). Mekanisme secara fleksibel dapat mendukung kombinasi dari autentifikasi, integritas, kontrol akses, dan kerahasiaan.

Pada VPN yang berbasis SSL, SSL VPN menggunakan algoritma *cryptographic* untuk mengenkripsi data sehingga hanya komputer-komputer yang berkomunikasi yang dapat membaca dan mengerti pesan yang dikirim. SSL mendukung berbagai algoritma enkripsi sehingga modifikasi terhadap aplikasi tidak dibutuhkan dan pengguna tidak perlu membuat sistem keamanan untuk setiap aplikasi atau setiap komputer. SSL merupakan salah satu solusi yang baik bagi *remote access* VPN atau pengguna yang bergerak (*mobile*). Sehingga dengan dibangunnya suatu layanan VPN yang berbasis SSL merupakan alternatif yang efektif untuk solusi keamanan untuk suatu jaringan.

Berdasarkan pertimbangan dari beberapa permasalahan diatas, maka penulis melakukan kajian judul **"PROTOTYPE LAYANAN REMOTE ACCESS VIRTUAL PRIVATE NETWORK (VPN) DENGAN METODE SECURE SOCKET LAYER (SSL)"**.

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang masalah yang dikemukakan di atas, maka permasalahan yang dikaji dalam penelitian ini adalah:

1. Bagaimana mengkonfigurasi *Remote Access* VPN dengan metode SSL.
2. Bagaimana membangun suatu layanan *Remote Access* VPN dengan metode SSL.
3. Bagaimana perbandingan layanan yang menggunakan *Remote Access* VPN yang menggunakan metode SSL dengan layanan yang tidak menggunakan VPN.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan skripsi ini adalah untuk membangun suatu prototype layanan dari *Remote Access* VPN dengan metode SSL.

Sedangkan tujuan yang akan dicapai dalam penelitian ini adalah:

1. Untuk menganalisis arsitektur dari VPN, terutama *Remote Access* VPN dengan metode SSL.
2. Untuk Mengimplementasikan suatu layanan yang berbasiskan *Remote Access* VPN dengan metode SSL.
3. Untuk membandingkan layanan yang menggunakan *Remote Access* VPN yang menggunakan metode SSL dengan jaringan yang tidak menggunakan VPN.

1.4 Batasan Masalah

Penulis membatasi permasalahan dalam penulisan ini dengan maksud agar pembahasan dan penyusunan laporan dapat dilakukan secara terarah dan tidak menyimpang serta sesuai dengan apa yang diharapkan. Batasan-batasan masalah tersebut antara lain adalah:

1. Konfigurasi *Remote Access* VPN dengan metode SSL berupa konfigurasi pada sistem operasi.
2. Sistem operasi yang digunakan pada VPN *server* adalah Linux.
3. Implementasi konfigurasi *Remote Access* VPN dengan metode SSL berupa simulasi jaringan (*real network*) dengan menggunakan 2-4 komputer.
4. Koneksi *Remote Access* VPN apabila melewati internet pada bandwidth maksimal 256 Kbps.
5. VPN (*Virtual Private Network*) diimplementasikan dengan menggunakan IP versi 4 (IPv4).

1.5 Metodologi Penelitian

Metodologi Penelitian yang digunakan dalam penulisan skripsi ini adalah sebagai berikut:

1. Studi Literatur

   Studi literatur yaitu membaca dan memahami referensi-referensi sumber, serta mempelajari dokumentasi-dokumentasi yang mendukung penelitian.

2. Studi Eksperimen

   Studi eksperimen yaitu dengan melakukan pemahaman proses konfigurasi *Virtual Private Network* (VPN) dengan *Secure Socket Layer* (SSL).

1.6 Sistematika Penulisan

Sitematika penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, asumsi, serta sistematika penulisan.

BAB II LANDASAN TEORI

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan, serta menjelaskan teori-teori yang berhubungan dengan masalah yang dibahas.

BAB III. ANALISIS DAN PERANCANGAN SISTEM

Menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Merupakan tahapan yang dilakukan dalam penelitian secara garis besar sejak dari tahap persiapan sampai penarikan hipotesis. Serta menjelaskan tentang implementasi hasil dari analisis dan perancangan sistem ke dalam bentuk konfigurasi *Remote Access* VPN. Serta kebutuhan perangkat keras dan perangkat lunak yang diperlukan dalam membangun *Remote Access* VPN dengan metode SSL. Selain itu akan dibahas tentang masalah pengujian terhadap *Remote Access* VPN yang dibangun.

BAB V. KESIMPULAN DAN SARAN

Berisi kesimpulan dari pengujian yang dilakukan serta saran-saran pengembangan sistem kedepannya.

DAFTAR PUSTAKA

LAMPIRAN