BAB I
PENDAHULUAN

1.1. Latar Belakang

Kebutuhan bisnis di masa sekarang didukung dengan variasi jaringan komunikasi yang luas. Para karyawan di perusahaan mengakses sumber daya perusahaan untuk mendukung pekerjaan mereka melalui jaringan komunikasi perusahaan. Belum lagi rekanan bisnis perusahaan juga turut mengakses sumber daya perusahaan dengan jaringan lain dalam rangka kerja sama membagi informasi bisnis, perencanaan bisnis bersama, dan lain sebagainya. Pada umumnya perusahaan mengunakan jaringan berbasis *leased line* atau *frame relay* untuk menghubungkan kantor pusat dengan kantor cabang. Hal tersebut tidak fleksibel mengingat saat ini sebuah perusahaan ingin cepat mempunyai jaringan komunikasi dengan rekanan bisnis atau untuk mendukung pekerja yang sedang mengerjakan proyek bersifat lapangan dan menuntut mobilitas. Perubahan gaya bekerja, seperti perusahaan yang mendukung *full-time remote worker*, yaitu karyawan yang mengantikan jam bekerja di kantor dengan bekerja pada PC (*personal computer*) di rumahnya, menyebabkan permintaan akan teknologi *remote access* semakin meningkat. Teknologi *remote access* tradisional seperti *dial-up* RAS (*remote access server*) saat ini telah terbukti tidak memadai untuk tugas itu. Penyebab utamanya rumitnya *deploymet*, tinggi biaya telepon, kurangnya implementasi keamanan, dan juga biaya pemeliharaan yang tinggi. (sumber: http://www.netilla.com/)

Oleh sebab itu, VPN (*Virtual Private Network*) muncul sebagai solusi alternative yang logis untuk memperluas akses sumber daya perusahaan dengan aman dan dengan biaya lebih murah melalui jaringan standar seperti internet.

Salah satu konsep umum yang salah pada VPN adalah VPN selalu dikaitkan dengan protokol IPSec (*Internet Protocol Security*), yaitu sebuah protokol enkripsi yang menyediakan tranmisi data terenkripsi yang aman pada *network lay*er dalam jaringan, Padahal, ada banyak lagi protokol enkripsi dan keamanan data yang dapat menyediakan fungsionalitas dari VPN. SSL (*Secure Socket Layer*) adalah salah satu protokol tersebut juga dapat bekerja pada *application layer* dan umum digunakan pada komunikasi aman berbasis web pada internet.

Untuk mengetahui lebih jelas tentang protokol IPSec dan SSL Pada VPN serta tinjauan operasional pada protokol tersebut, maka akan dilakukan studi literatur yang membahas protokol IPSec dan SSL pada VPN secara keseluruhan. Berdasarkan latar belakang tersebut, penulis tertarik membuat penelitian untuk Tugas Akhir ini dengan judul "Studi Analisis Perbandingan IPSec (Internet Protocol Security) dan SSL (Secure Socket Layer) Pada VPN (Virtual Private Network)".

1.2. Perumusan masalah

Perumusan masalah pada pembuatan tugas akhir ini adalah sebagai berikut :

a. Bagaimana tinjauan proses operasional protokol IPSec dan SSL?
b. Bagaimana mengetahui perbedaan antara IPSec dan SSL VPN?
c. Bagaimana mengetahui perbandingan protokol IPSec dan SSL pada VPN?

1.3. Batasan masalah

Adapun batasan masalah dalam penulisan tugas akhir ini adalah sebagai berikut :

a. Menjelaskan tentang protokol IPSec dan SSL.
b. Analisis terhadap perbandingan antara protokol IPSec dan SSL pada VPN.

c. Tidak membahas perhitungan algoritma enkripsi, seperti: (DES, 3DES, dan AES), algoritma hashing (MD5, SHA-1) pada protokol IPSec dan SSL.

1.4. Tujuan dan Manfaat

Tujuan dari penelitian ini adalah :

a. Untuk mengetahui VPN dan protokol IPSec dan SSL.
b. Untuk mengetahui solusi IPSec dan SSL VPN serta mengetahui kelebihan dan kekurangan dari masing-masing VPN tersebut.
c. Untuk mengetahui perbandingan protokol IPSec dan SSL pada VPN.

Manfaat akademik dari penelitian ini adalah :

a. Dapat memberikan referensi bahan bacaan mengenai protokol IPSec dan SSL kepada kalangan akademik.

1.5. Metode Penelitian

Metodologi penelitian yang digunakan dalam melakukan proses penelitian pada tahap pengumpulan data adalah sebagai berikut:

a. Studi literatur

   Data dan informasi yang diperoleh adalah dengan cara studi literatur, yaitu dengan mengadakan pengumpulan data teoritis dari beberapa buku, jurnal, *e-book*, *paper*, yang mendukung penyusunan Tugas
   Akhir ini, serta berbagai artikel yang diperoleh dari internet.

b. Observasi

   Melakukan observasi atau pemahaman mendalam pada data yang di peroleh dari tahap studi literatur, dan mendapatkan pembanding dari data yang diperoleh sebelumnya.

1.6. Sistematika Penulisan

Sistematika penulisan laporan akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan membahas latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini memuat kerangka teori dan tinjauan pustaka. Kerangka teori menjelaskan kerangka teoritis yang mendasari penelitian. Tinjauan pusataka berisi pengumpulan data dari buku-buku serta beberapa referensi dari hasil penelitian yang relevan dengan topik tugas akhir yang disajikan, yang diperoleh dari berbagai sumber.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metode yang digunakan untuk melakukan penelitian.

BAB IV ANALISIS PERBANDINGAN DAN PEMBAHASAN

Secara umum bab ini menyajikan data analisis perbandingan dan pembahasan dari protokol IPSec dan SSL serta solusi VPN berbasis IPSec dan VPN berbasis SSL juga data analisisnya untuk digunakan sebagai bahan pertimbangan dalam dunia nyata.

BAB V PENUTUP

Kesimpulan memuat secara singkat hasil penting yang diperoleh dari penelitian sesuai dengan masalah dan tujuan penulisan.