ABSTRAK

Dalam lingkungan bisnis yang bergerak cepat saat ini, lingkungan bisnis didukung dengan variasi jaringan komunikasi yang luas. VPN (*Virtual Private Network*) adalah suatu teknologi komunikasi yang memungkinkan *remote user* dapat mengakses sebuah jaringan *private* yang tertutup dengan menggunakan jaringan publik standar seperti internet. Kebutuhan keamanan remote akses terhadap sumber daya perusahaan melalui penggunaan VPN telah menjadi kebutuhan penting perusahaan sekarang sebagai usaha memperluas akses jaringan untuk mendukung karyawan yang mengerjakan proyek dari PC (*personal computer*) rumah mereka, karyawan yang sedang mengerjakan proyek dilokasi lain (dilapangan) dan mitra bisnis yang berada ditempat yang jauh. Salah satu metode yang efisien dan hemat biaya untuk memenuhi kebutuhan remote akses perusahaan adalah menggunakan VPN, digunakan untuk memastikan keamanan transfer data penting melalui jaringan publik seperti internet. Salah satu konsep umum yang salah mengenai VPN adalah VPN selalu dikaitkan dengan protokol IPSec (*Internet Protocol Security*), yaitu sebuah protokol enkripsi yang menyediakan tranmisi data terenkripsi yang aman pada *network layer* dalam jaringan. Padahal ada banyak lagi protokol enkripsi keamanan yang dapat menyediakan fungsionalitas dari VPN. SSL (*Secure Socket Layer*) adalah salah satu protokol tersebut, yang bekerja pada *application layer* dan umum digunakan pada komunikasi aman berbasis web pada internet. protokol IPSec dan SSL memiliki kelebihan serta kekurangan masing-masing. Dalam membandingkan IPSec dan SSL, maka akan diketahui kelebihan dan kekurangan pada masing-masing protokol bila diterapkan pada VPN. Sehingga dari masalah-masalah tersebut akan dilakukan analisis dan kemudian dilakukan penelitian untuk Tugas Akhir ini.

Kata kunci : Jaringan, Enkripsi, Security, VPN, IPSec, SSL.