ABSTRAKSI

Jaringan komputer telah menjadi salah satu kebutuhan yang sangat penting bagi kelangsungan bisnis di banyak perusahaan. Di masa lalu, banyak perusahaan yang membangun sendiri jaringan backbone antar cabang yang membutuhkan biaya yang sangat tinggi. Keamanan data internal perusahaan, reabilitas serta ketersediaan jaringan menjadi alasan mengapa mereka membangun jaringan internal yang tertutup.

Internet merupakan jaringan publik yang telah berkembang sangat pesat. Saat ini POP (point of presence) telah ada di berbagai kota. Namun protokol internet sejak awal dirancang tanpa memperhatikan aspek keamanan secara mendalam. Virtual private network dikembangkan untuk menjawab kebutuhan tersebut. Dengan menggunakan tunneling, VPN memungkinkan untuk membangun komunikasi antar komputer melalui jaringan publik namun seolah-olah berkomunikasi dalam suatu jaringan private. Keamanan data terjamin dengan digunakannya enkripsi dan autentikasi.

Terdapat berbagai macam metode yang digunakan untuk membangun jaringan VPN, diantaranya yang berbasis IPsec dan SSL. Tugas akhir bertujuan untuk menguji performansi jaringan dari kedua macam metode tersebut. Karena peningkatan level keamanan merupakan trade off dengan performansi jaringan. Tingginya level keamanan berbanding terbalik dengan performansi jaringan yang dihasilkan.

Hasil dari penelitian ini menyimpulkan bahwa implementasi VPN berbasis IPsec memiliki performansi jaringan yang lebih baik dibandingkan dengan implementasi menggunakan SSL dari segi troughput, dan delay. Implementasi VPN IPsec dan VPN SSL tidak memiliki pengaruh terhadap packet loss.