

ABSTRAK

Layanan VPN (*virtual private network*) merupakan koneksi jaringan pribadi melalui jaringan *public*. Pembangunan VPN menjadi sebuah solusi untuk menyediakan jaringan pribadi yang aman (*secure*). Pemilihan protokol VPN akan berpengaruh pada tingkat performansi dan keamanan jaringan tersebut. *IPSec* melakukan enkapsulasi terhadap data yang lewat dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan internet atau dalam jaringan intranet secara aman. Permasalahan yang ada ialah proses autentikasi pada layanan VPN lebih lama dibandingkan dengan proses autentikasi pada jaringan yang tidak menggunakan sistem tersebut. Hal itu dikarenakan adanya proses enkapsulasi paket sebelum dikirim dan proses pengecekan didalam *database*.

Dalam Tugas Akhir ini dibuat layanan VPN yang di implementasikan ke dalam jaringan *virtual* dan jaringan fisik. Dalam jaringan *virtual* hal ini memungkinkan proses kerja sistem menjadi lebih cepat dikarenakan teknologi yang diterapkan ke dalam *hardware* sudah mendukung teknologi *hypervisor*.

Dengan diterapkannya jaringan *virtualisasi*, jaringan *virtual* tetap memberikan keamanan data berupa enkapsulasi dengan protokol ESP dan kenaikan nilai sebesar 28.76% untuk *throughput* dan performa yang lebih baik daripada jaringan fisik.

Kata Kunci: *VPN, IPSec, Jaringan fisik, Jaringan virtual*