1. Pendahuluan

Latar Belakang

Teknologi *Virtual Private Network* (VPN) dengan menggunakan IPSec merupakan solusi secara umum yang diterapkan untuk menjaga kerahasiaan, integritas dan ketersedian pada jaringan. Teknologi VPN memiliki kelemahan dalam waktu implementasi konfigurasi statis dan memiliki latency yang tinggi. Penyebab dari tinggi latency adalah karena terjadinya peningkatan beban *traffic* di *Hub* utama. Pada VPN juga memiliki pengurangan dalam paket *Routing* yang overhead disebabkan tingginya *traffic* dari *client* ke *hub* sehingga menghasilkan kinerja jaringan yang lebih tinggi dan bahkan mengurangi daya konsumsi jaringan [1], [2].

Untuk mengatasi keterbatasan VPN, maka perusahaan Cisco memperkenalkan *Dynamic Multipoint Virtual Private Network* (DMVPN). DMVPN merupakan teknik *Routing* pemodelan yang menggunakan topologi jaringan mesh pada sebuah *hub* (*Server*) yang ter*hub*ung antara *spoke* (*Client*) router yang saling ter*hub*ung satu sama lain dan mengizinkan *traffic* antara *spoke* router yang dikirim tanpa melalui *hub*. Selain itu juga pada DMVPN tidak perlu melakukan konfigurasi ulang pada lokasi *client* baru yang ter*hub*ung pada *hub* dan memiliki skalabilitas yang luas dibandingkan VPN[1]–[4].

DMVPN memiliki *protocol Routing* dinamis yang digunakan untuk melakukan manipulasi pembaruan paket *Routing* pada *spoke* dan *hub*. Jenis – jenis *Routing* dinamis yang digunakan antaranya adalah RIP, OSPF, EIGRP, IS – IS, dan BGP [1], [3]. Pada tugas akhir ini menggunakan *protocol Routing* BGP yang bisa digunakan dengan jangkauan skalabilitas yang tinggi dan cocok digunakan pada *protocol* DMVPN yang memiliki skalabilitas yang luas [5].

Encryption dari *traffic* antar *hub* penting untuk melindungi sistem dari *cyber criminals*. Penggunaan algoritma enkripsi yang tepat penting karena akan berbanding lurus dengan performa komunikasi jaringan. Ipsec adalah metode enkapsulasi yang digunakan untuk mengamankan lalu lintas antar *client*. Untuk membangun dan melindungi jaringan DMVPN, konfigurasi dasar IPsec dengan mGRE dan NHRP harus diimplementasikan di setiap node untuk memastikan tingkat dasar kerahasiaan dan integritas agar dapat membentuk perlindungan pada jaringan DMVPN [1], [6],[13],[15].

Permasalahan yang diangkat pada tugas akhir ini adalah untuk mengetahui dampak IPSec pada *protocol* DMVPN terhadap Quality of service di *Routing* BGP dengan parameter performansi *delay*, *throughput*, *jitter* dan packet *loss* [7]–[10]. Pada tugas akhir ini akan melakukan perbandingan analisis IPSec dan tanpa IPSec pada DMVPN menggunakan *Protocol Routing* BGP. Pada implementasi tugas akhir ini menggunakan aplikasi simulator GNS3 untuk melakukan rancangan jaringan, *configuration* jaringan dan pada pengujian kinerja jaringan memakai tools D-ITG[14].

Topik dan Batasannya

Batasan masalah dalam tugas akhir ini yaitu penelitian ini menggunakan protokol DMVPN, *Routing* BGP dan IPSec. Penelitian ini menggunakan simulator GNS3, aplikasi *Virtual Box*, system operasi ubuntu dan router cisco 7200. Dan Parameter performansi yang digunakan yaitu *delay*, *throughput*, packet *loss* dan *jitter* [7]–[11].

Tujuan

Tujuan dari penelitian ini adalah untuk memodelkan IPSec pada DMVPN khusus menggunakan protokol *Routing* BGP, menganalisis kinerja IPSec dan tanpa IPsec pada DMVPN menggunakan protokol BGP pada parameter kinerja seperti *delay*, *throughput*, *jitter* dan paket *loss*.

Organisasi Tulisan

Penelitian ini disusun berdasarkan struktur sebagai berikut: bagian awal menjelaskan tentang pendahuluan, bagian kedua menjelaskan studi terkait yang dibahas, bagian tiga memaparkan mengenai sistem model yang dibangun, bagian empat memaparkan hasil konfigurasi DMVPN, IPsec, *Routing* BGP, analisis dan hasil pengujian, dan kesimpulan daripenelitian ini dituliskan pada bagian lima.

.