1. Pendahuluan

1.1 Latar Belakang

Virtual Private Network (VPN) merupakan suatu teknologi membangun jaringan *private* dalam jaringan publik [5]. Teknologi tersebut mampu meningkatkan keamanan komunikasi pada jaringan publik, karena komunikasi tersebut seolah-olah berada pada sebuah jaringan *private*. Karena keunggulan tersebut, VPN telah banyak diimplementasikan pada jaringan internet. Internet saat ini masih menggunakan standar pengalamatan *Internet Protocol version 4* (IPv4). Standar pengalamatan IPv4 akan digantikan dengan standar pengalamatan *Internet Protocol version* 6 (IPv6). Hal ini mengharuskan VPN yang merupakan suatu solusi keamanan pada jaringan IPv4 agar tetap bisa mengerjakan fungsinya pada jaringan IPv6.

Proses penggantian sistem pengalamatan ini tidak berlangsung serentak. Beberapa jaringan sudah mulai menggunakan standar pengalamatan IPv6, biasanya jaringan berstatus *Local Area Network* (LAN) . Salah satu penyebab beberapa jaringan masih menggunakan standar pengalamatan IPv4 seperti internet dikarenakan keterbatasan perangkat keras. Dimana perangkat keras yang digunakan sekarang masih banyak yang belum mendukung jaringan yang menggunakan sistem pengalamatan IPv6.

Standar pengalamatan IPv6 memiliki beberapa perbedaan dengan standar IPv4, misalnya pada panjangnya *header* dan *payload*. Perbedaan-perbedaan tersebut diperkirakan akan memberikan perbedaan kinerja antara VPN pada jaringan IPv4 dengan VPN pada jaringan IPv6.

Saat ini banyak kantor yang menerapkan metode *work-at-home* yaitu mengerjakan pekerjaan kantoran di rumah. Pegawai kantor yang bekerja di rumah tetap harus terhubung dengan jaringan internal kantor. Sehingga dibutuhkan sebuah VPN berjenis *remote access* agar pegawai tersebut bisa terhubung ke jaringan internal kantor melalui Internet.

Ada beberapa jenis protokol yang biasa digunakan pada VPN seperti *Internet Protocol Security* (IPSec), *Secure Socket Layer* (SSL), *Point-to-Point Tunnelling* (PPTP), dan *Layer 2 Tunneling Protocol* (L2TP). Namun dilihat dari segi dukungan keamanan protokol IPSec dan SSL merupakan protokol yang paling banyak digunakan [1].

Karena telah mampu memenuhi kriteria dukungan keamanan [13], maka akan digunakan kriteria *Quality of service* (QoS) dalam menetukan mana protokol keamanan yang lebih baik. Dimana dalam menganalisa QoS, akan digunakan parameter *throughput* dan *delay*. Pemilihan parameter tersebut karena diperkirakan protokol keamanan akan membebani performansi jaringan ketika proses pengamanan jaringan komunikasi.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, ditemukan beberapa masalah yang dirumuskan sebagai berikut:

1. Bagaimana mengimplementasikan VPN berbasis protokol IPSec dan VPN berbasis protokol SSL.
2. Bagaimana perbandingan performansi VPN berbasis protokol IPSec dengan VPN berbasis protokol SSL.

Batasan-batasan masalah dalam pengerjaan tugas akhir ini adalah:

1. Parameter performansi jaringan yang digunakan adalah *throughput* dan *delay*.
2. Menggunakan standar pengalamatan IPv6 pada LAN dimana *server* dipasang.
3. Menggunakan standar pengalamatan IPv4 pada jaringan antar router dan *client*.
4. Tidak membahas mengenai kemampuan VPN dari segi keamanan jaringan.

5. Tidak membahas enkripsi secara mendalam.
6. Layanan yang digunakan adalah *File Transfer Protocol* (FTP).
7. VPN yang dibangun dengan jenis pengimplementasian VPN remote access.
8. Pengimplementasian sistem dikerjakan berupa emulasi.

1.3 Tujuan

Tujuan yang ingin dicapai dalam pengerjaan tugas akhir ini adalah:

1. Mengimplementasikan remote access VPN berbasis IPsec dan berbasis SSL.
2. Menganalisis perbandingan performansi remote access VPN berbasis IPsec dengan berbasis SSL

1.4 Hipotesa

Tujuan dari IPSec yang merupakan protokol keamanan yang dirancang untuk IPv6. Hal tersebut tentunya memberikan suatu kemungkinan bahwa IPSec akan memiliki performansi yang lebih baik jika dibandingkan dengan protokol keamanan SSL.

Pada IPSec terdapat penambahan Header pada paket IP berupa penambahan AH Header dan/atau ESP Header, ESP trailer, ESP Auth, sehingga paketnya menjadi lebih besar. Sedangkan pada SSL mengirim paket yang telah dienkripsi dalam suatu sesi koneksi. Sehingga SSL akan memiliki throughput yang lebih baik. Dari segi parameter delay, protokol IPSec akan memiliki kemungkinan lebih buruk dibanding SSL. Hal tersebut dimungkinkan karena ukuran paket IPSec akan lebih besar karena IPSec akan menggunakan fungsi jumbo payload di IPv6.

1.5 Metodologi Penyelesaian Masalah

Metode yang digunakan untuk menyelesaikan masalah diatas adalah:

a. Studi Literatur

   Mencari dan mempelajari data mengenai IPv6, VPN, IPSec, SSL, dan keamanan jaringan dari berbagai sumber seperti jurnal, literatur, dan bacaan-bacaan lainnya.

b. Perancangan Sistem

   Merancang VPN berbasis IPSec dan VPN berbasis SSL pada jaringan IPv6 yang nantinya mampu diuji dengan skenario uji agar mampu membuktikan hipotesa.

c. Pengimplementasian Sistem

   Megimplemetasikan VPN berbasis IPSec dan VPN berbasis SSL pada jaringan IPv6 yang dikerjakan menggunakan aplikasi GNS3. Sehingga akan ada satu file *project* untuk masing-masing VPN. Serta akan membangun sebuah server FTP yang akan menjadi layanan pada jaringan yang di-*remote*.

d. Pengujian Sistem

   Melakukan pengujian performansi jaringan untuk masing-masing VPN yang telah diimplementasikan dengan cara mencoba menggunakan layanan FTP. Penggunaan layanan FTP dengan proses mengunduh dan menggunggah *file* , dimana ukuran dan banyaknya file akan divariasikan. Selanjutnya proses pengujian berupa pemantauan proses penggunaan layanan FTP tersebut dengan aplikasi *Wireshark*.

e. Analisis Hasil

   Data-data yang ditampilkan oleh *Wireshark* tersebut digunakan sebagai bahan analisis dalam menyimpulkan performansi dari masing-masing VPN.

f. Pembuatan Laporan Tugas Akhir

   Membuat laporan yang berisi semua kegiatan yang dilakakukan dalam penyelesaian tugas akhir ini.

1.6 Sistematika Penulisan

Tugas Akhir ini disusun berdasarkan sistematika penulisan sebagai berikut :

BAB I : Pendahuluan

Menjelaskan tentang permasalahan yang akan dibahas secara umum dengan memperhatikan latar belakang, perumusan masalah, tujuan, metodologi dan sistematika penulisan.

BAB II : Dasar Teori

Menjelaskan teori tentang IPv6, VPN, IPSec, SSL dan performansi yang berpengaruh dalam jaringan.

BAB III : Analisa dan Perancangan Sistem

Bab ini akan menjelaskan tentang analisa kebutuhan dan perancangan sistem yang akan dibangun.

BAB IV : Implementasi, Pengujian, Dan Analisa Hasil Pengujian

Bab ini akan menampilkan konfigurasi yang dilakukan dalam implementasi, skenario pengujian, dan analisa hasil pengujian dari perancangan sistem yang telah dibuat.

BAB V : Kesimpulan Dan Saran

Pada bab ini akan disebutkan kesimpulan yang telah didapatkan dari proses pengujian dan analisa sebelumnya beserta saran yang dapat digunakan sebagai masukan dalam penelitian berikutnya.