BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Internet merupakan sebuah jaringan global dan terbuka, dimana setiap pengguna dapat saling berkomunikasi dan bertukar informasi. Seiring dengan maraknya penggunaan *Internet*, banyak perusahaan yang kemudian beralih menggunakan *internet* sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama.

Untuk mengatasi masalah keamanan dalam komunikasi data pada jaringan umum (*public network / internet*) maka lahirlah *Virtual Private Network* (VPN). Secara umum VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik, infrastruktur publik yang paling banyak digunakan adalah jaringan *internet*. Didalam VPN terdapat perpaduan teknologi tunneling dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan.

Dalam implementasinya, VPN terbagi menjadi *remote access* VPN dan *site-to-site* VPN. *Site-to-site* VPN digunakan untuk menghubungkan antara 2 tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut *ekstranet*. Sedangkan bila VPN digunakan untuk

menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet *site-to-site* VPN.

Pada VPN terdapat beberapa protokol yang paling umum digunakan, yaitu *Point to Point Tunneling Protocol* (PPTP), SOCKS, *Layer 2 Tunneling Protocol* (L2TP), *Cryptographic IP Encapsulation* (CIPE), *Generic Routing Encapsulation* (GRE), dan *Internet Protocol Securuty* (IPSec). Protokol-protokol tersebut memiliki karakteristik yang berbeda-beda.

IPSec adalah sebuah pilihan tunneling protokol yang sangat tepat untuk digunakan dalam VPN level korporat. IPSec merupakan protokol yang dapat menyediakan keamanan data, keutuhan data, dan autentikasi data antara kedua *peer* yang berpartisipasi di dalamnya. IPSec menyediakan sistem keamanan data dengan menggunakan sebuah metode pengaman yang bernama *Internet Key Exchange* (IKE). IKE bertugas untuk menangani masalah negosiasi dari protokol-protokol dan algoritma pengamanan yang diciptakan berdasarkan dari *policy* yang diterapkan pada jaringan sipengguna. IKE pada akhirnya akan menghasilkan sebuah sistem enkripsi dan kunci pengamannya yang akan digunakan untuk autentikasi pada sistem IPSec ini.

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka penulis bermaksud mengambil topik tugas akhir ini dengan judul "**ANALISIS DAN PERANCANGAN *SITE-TO-SITE* VIRTUAL PRIVATE NETWORK (VPN) BERBASIS IP *SECURITY* MENGGUNAKAN MIKROTIK ROUTER OPERATING SYSTEM*"***

1.2 Rumusan Masalah

Dari latar belakang yang telah diuraikan, ditemukan beberapa masalah yang dirumuskan dalam suatu rumusan masalah yaitu :

1. Bagaimana merancang dan mengimplementasikan *site-to-site* VPN berbasis IPsec dengan MikroTik Router Operating System.
2. Bagaimana memberikan solusi keamanan data pada jaringan lokal atau *intranet* yang terhubung ke jaringan global atau *internet*.
3. Bagaimana perbandingan data yang diperoleh dari layanan yang menggunakan VPN dengan layanan yang tidak menggunakan VPN.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan tugas akhir ini adalah untuk menganalisis dan merancang *site-to-site* VPN berbasis IPsec dengan MikroTik Router Operating System.

Sedangkan yang menjadi tujuan penulisan tugas akhir ini adalah:

1. Menerapkan *site-to-site* VPN dengan protokol IP security
2. Membuktikan bahwa VPN memberikan solusi keamanan dalam trasmisi data atau informasi pada jaringan komputer.
3. Menganalisis perbandingan data yang diperoleh dari layanan yang menggunakan VPN dengan layanan yang tidak menggunakan VPN.

1.4 Batasan Masalah atau Ruang Lingkup kajian

Dalam Perancangan dan Implementasi sistem ini, terdapat batasan-batasan masalah yang meliputi :

1. Jenis implementasi VPN yang digunakan adalah *site-to-site* VPN
2. Implementasi *site-to-site* VPN menggunakan protokol IP Security
3. *Server* VPN menggunakan MikroTik *Router Operating System*.
4. Tidak menggunakan radius *server*
5. VPN di implementasikan dengan menggunakan IP *version 4* (*ipv4*).
6. Algoritma yang digunakan untuk authentikasi adalah MD5.
7. Algoritma yang digunakan untuk enkripsi adalah 3DES.
8. Penelitian ini tidak membahas mengenai enkripsi secara mandalam
9. Uji koneksi menggunakan *tool monitoring* jaringan, yaitu *ping*.
10. Simulasi VPN dilakukan secara Local Area Network (LAN).
    a. Arsitektur simulasi
        1) *Hardware* yang diperlukan yaitu dua buah PC (sebagai *server* VPN dan Router) dan dua buah Laptop (sebagai *client* dan web *server*)
        2) *Software* yang diperlukan yaitu Mikrotik Router Operation System versi 2.9.27, RidenDNSD 1.3.17, Xampp for windows 1.6.5, Filezilla dan *Protocol Analyzer* (wireshark –win32- 1.2.9).
        3) Sistem Operasi yang digunakan pada Laptop *server* dan *client* adalah Windows 7 Ultimate dan Windows XP Service Pack 3

b. Skenario simulasi

1) Menguji konektivitas VPN:

a. Mengakses web *server*

b. Melakukan *download* file dari file *server* menggunakan FTP *service*

2) Menguji kehandalan VPN:

a. Melakukan *download* file melalui VPN

b. Melakukan *download* file tanpa VPN

c. Melakukan monitoring data menggunakan wireshark dan menganalisa perbandinga datanya

1.5 Metodologi Penelitian

Metode penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

a. Studi Pustaka

Penulis mengumpulkan data dengan cara membaca literatur, jurnal, *browsing internet* dan bacaan-bacaan yang ada kaitannya dengan masalah yang akan diteliti sebagai bahan referensi tertulis.

b. Wawancara

Penulis melakukan pengumpulan data memalui tanya jawab kepada nara sumber yang ahli di bidang jaringan komputer.

c. Eksperimen

Eksperimen yang dilakukan penulis adalah mengumpulkan data mengenai kebutuhan sistem, merancang dan membangun arsitektur jaringan komputer dan mengimplementasikan teknologi site-to-site VPN.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang sistem yang akan dibuat. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini memaparkan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan beberapa hal yaitu landasan teori seperti pengertian jaringan komputer, pengertian keamanan jaringan, pengertian enkripsi, deskripsi VPN dan teknologi pendukungnya, deskripsi protokol VPN dan pembahasan mengenai *software* yang Mikrotik RouterOS dan sebagainya.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini memaparkan tentang analisis sistem, analisis masalah, analisis kebutuhan sistem VPN, analisis *hardware* dan *software*, analisis pengguna, perancangan sistem, arsitektur simulasi dan konfigurasi *site-to-site* VPN.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini diuraikan tentang lingkungan implementasi sistem, skenario pengujian sistem, dan sebagainya.

BAB V KESIMPULAN DAN SARAN

Pada bab terakhir ini akan berisikan kesimpulan-kesimpulan dari skripsi yang dibuat dan terdapat pula saran yang diberikan sebagai bahan pertimbangan dalam pengembangan sistem *site-to-site* VPN kedepannya.