BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat menyebabkan pertumbuhan jumlah user internet dikalangan masyarakat menjadi semakin meningkat. Pada dasarnya hal ini disebabkan oleh mobilitas atau kegiatan yang mengharuskan terjadinya pertukaran informasi dengan cepat dan efisien. Dalam hal ini penggunaan internet dapat memudahkan user untuk mengakses data dan saling melakukan pertukaran informasi. Dan karena pertumbuhan pengguna internet yang semakin meningkat, dibutuhkan keamanan data yang baik untuk dapat mengirim data tanpa merubah keutuhan data yang dipertukarkan di dalam internet. Untuk memungkinkan terjaminnya keamanan data tersebut dibangun satu jaringan *private* di atas jaringan publik yang ada. Jaringan *private* yang digunakan untuk mengatasi masalah keamanan data tersebut adalah *Virtual Private Network* (VPN).

Virtual Private Network atau yang disebut sebagai VPN merupakan suatu koneksi antar dua jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan suatu metode enkripsi tertentu sebagai media pengamannya atau dengan kata lain VPN merupakan suatu jaringan private yang dibangun di atas jaringan public seperti internet yang menghubungkan satu jaringan ke jaringan lainnya. Dalam hal ini VPN yang di implementasikan pada jaringan *Virtual Private Server* dapat diakses dimanapun dengan menggunakan *remote access* untuk dapat memudahkan *user* dalam mengakses jaringan VPN dimanapun selama *user* masih terhubung dengan jaringan *access* VPN server. Pada dasarnya ketika user sudah berada pada jaringan VPN, dalam hal ini user sedang melakukan proses *tunnneling*. Proses *tunneling* merupakan suatu proses enkapsulasi transmisi dan decapsulasi paket yang dikomunikasikan. Metode tunneling menggunakan beberapa *protocol* yang terdapat pada VPN seperti *Point To Point Protocol* (PPTP) , *tunneling protocol* (L2TP), dan IP Sec.

Untuk itu implementasi pada jaringan VPN dibutuhkan *Virtual Private Server* sebagai wadah untuk VPN server. Pada proyek akhir ini akan diimplementasikan jaringan openvpn pada *virtual private server* (VPS) dan kemudian dilakukan pengujian

tes keamanan terhadap jaringan openvpn, serta mengidentifikasikan serangan-serangan yang terjadi pada jaringan openvpn.

1.2 Tujuan dan Maksud

Tujuan dan maksud penulisan proyek akhir ini adalah :

1 Mampu mengimplementasikan jaringan openvpn pada jaringan Virtual Private Server.

2 Mengetahui cara kerja openvpn .

3 Menganalisa tingkat kemanan jaringan openvpn terhadap berbagai macam serangan.

1.3 Rumusan Masalah

Berdasarkan tujuan dan maksud penelitian di atas, maka permasalahan yang akan dipecahkan dalam penelitian ini adalah :

1 Bagaimana cara mengkonfigurasi jaringan openvpn pada jaringan *Virtual Private Server*.

2 Bagaimana kemanan pada VPN dapat mengamankan user yang berada pada jaringan VPN.

3 Bagaimana melakukan pengujian keamanan pada jaringan openvpn yang terdapat pada *virtual private server*.

1.4 Batasan Masalah

Ruang lingkup batasan masalah dalam penulisan laporan proyek akhir ini hanya terbatas pada masalah-masalah sebagai berikut:

1. Pembuatan proyek akhir ini dilakukan dengan cara implementasi pada *virtual private server.*
2. Pengujian keamanan dilakukan pada *user* yang terhubung kedalam jaringan vpn.
3. Mengidentifikasi serangan-serangan yang terjadi pada jaringan vpn.
4. Mengidentifikasi hasil dari parameter pengujian.
5. Hanya membahas jaringan openvpn.
6. Tidak membahas detail mengenai enkripsi.

1.5 Metodologi Penelitian

Adapun dalam pelaksanaan proyek akahir ini, penulis menggunakan beberapa metode penelitian untuk merealisasikan proyek akhir ini, yaitu :

1. **Studi Pustaka**

   Metode ini dilakukan dengan membaca referensi dari buku - buku, majalah dan artikel di internet yang berkaitan dengan permasalahan yang akan dibahas.

2. **Studi Literatur**

   Metode ini dilakukan dengan membaca referensi dari jurnal ilmiah yang berkaitan dengan permasalahan yang akan di bahas dan pada tahap ini dilakukan pendalaman materi tentang VPN, keamanan jaringan, dan teori-teori yang mendukung tugas akhir ini.

3. **Perancangan Sistem dan Jaringan**

   Dalam tahap ini, dilakukan perancangan sistem dan jaringan yang sesuai dengan topik tugas akhir ini. Sistem nantinya akan terdiri dari *virtual private server* dengan *virtual private network* dan *client* sebagai user.

4. **Implementasi Sistem dan Jaringan**

   Dalam tahap ini, dilakukan implementasi dari perancangan system dan jaringan yang telah dibuat.

5. **Pengujian dan Pengukuran**

   Pengujian dan analisa dalam tahap ini dilakukan berdasarkan parameter-parameter pengujian pada keamanan jaringan vpn yang dijelaskan pada bab 3.

6. **Diskusi**

   Metode ini dilakukan dengan berdiskusi dengan pembimbing akademik dan staf yang telah ahli dibidangnya

1.6 Sistematika Penulisan

Secara umum sistematika penulisan Proyek Akhir ini terdiri dari bab-bab dengan metode penyampaian sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi tentang latar belakang penulisan proyek akhir, maksud dan tujuan penulisan proyek akhir, rumusan masalah, batasan masalah, metodologi penulisan serta sistematika yang digunakan dalam penulisan proyek akhir.

BAB II DASAR TEORI

Pada bab ini berisi tentang penjelasan teori penunjang penulisan proyek akhir mengenai VPN Server dan materi lain yang akan digunakan untuk mencapai tujuan

BAB III PEMBAHASAN

Pada bab ini berisi tentang proses installasi VPN server dan *firewall* pada sistem KVM pada *virtual private server* dengan sistem operasi centos.

BAB IV HASIL UJI COBA DAN PENGUKURAN KEAMANAN

Pada bab ini berisi tentang hasil uji coba dan penjelasan pengukuran hasil implementasi keamanan server VPN dari berbagai macam serangan-serangan.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dari hasil uji coba dan kemungkinan pengembangan akhir yang telah dibuat.