BAB I

PENDAHULUAN

1.1. Latar Belakang

Jumlah pengguna Internet yang besar dan semakin berkembang, telah mewujudkan budaya Internet. Internet juga mempunyai pengaruh yang besar atas ilmu, informasi dan pendidikan.pengguna internet dapat mudah mencari bermacam-macam informasi dari internet. Selain dengan media buku dan perpustakaan, Internet menjadikan penyebaran pengetahuan informasi dan data secara cepat dan menyeluruh.

Perkembangan Internet juga telah mempengaruhi perkembangan ekonomi. Berbagai transaksi jual beli yang sebelumnya hanya bisa dilakukan dengan cara tatap muka dan sebagian melalui pos atau telepon, kini sangat mudah dan sering dilakukan melalui Internet. Transaksi keuangan juga sekarang bisa dilakukan dengan ada nya internet banking,melihat data karyawan bisa lewat remote desktop,ménage website bisa darimana saja asal ada jaringan internet,cek email atau mengambil data penting bisa dilakukan di jaringan internet.

seiring dengan peningkatan perkembangan itu,muncul masalah baru yaitu dari segi keamanan berinternet,apalagi untuk akses internet yang umum atau public atau sering disebut Wi-fi,biasanya rentan sekali terhadap keamanan,masalah yang timbul biasanya berupa penyadapan account internet,pencuruan data yang berada di computer kita,pengambil alihan suatu akses,penyebaran *virus*,dan lain-lain yang sering dilakukan di jaringan

internet,untuk penanganan saat ini kebanyakan orang menggunakan,anti Iyang *free* dan tidak *terupdate*, sehingga sangat rentan untuk terinfeksi I dan penyadapan data.

Disini vpn dengan menggunakan virtual private server akan di coba solusi untuk menanggulangi hal-hal yang terjadi dalam menggunakan jaringan wifi,dengan cara menggunakaan Vpn (*Virtul private network),* yaitu jaringan pribadi yang menggunakan medium nonpribadi (misalnya internet) untuk berkoneksi, Vpn merupakan suatu cara untuk membuat sebuah jaringan bersifat "private" dan aman dengan menggunakan jaringan publik misalnya internet. Dengan VPN Data *dienkapsulasi* (dibungkus) dengan *header* yang berisi informasi routing untuk mendapatkan koneksi ke server sehingga data dapat melewati jaringan publik dengan aman dan dapat mencapai akhir tujuan.Sedangkan untuk data yang dikirimkan telah dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi.

untuk membuat Vpn dibutuhkan suatu server yang selalu terkoneksi ke *internet*,dikarnnakan harga server yang mahal, maka disini VPN yang dibangun akan menggunakan *Virtual Private server* sebagai solusi untuk *server* dari vpn. Semoga dengan **Pembangunan vpn dengan Menggunakan *Virtual Private Server* untuk menjaga keamanan *internet* publik** ini, bisa menanggulangi masalah penyadapan *account* internet,pencuruan data ,pengambil alihan suatu *akses*,penyebaran *virus*,dan lain-lain.

1.2. Identifikasi Masalah

Permasalahan yang akan dibahas pada Konfigurasi VPN dengan menggunakan *Virtual Private Server* untuk menjaga keamanan internet public ini adalah sebagai berikut :

1. Melakukan konfigurasi vpn pada *server*
2. Melakukan konfigurasi vpn pada *client*
3. Simulasi keamanan pada jaringan *internet* tanpa vpn dan dengan vpn
4. Membahas dan mendefinisikan masalah-masalah keamanan yang terjadi pada jaringan *internet*,baik penyadapan dan pencurian *account* di jaringan *internet*.
5. Simulasi keamanan *website* sebelum dan setelah menggunakan vpn
6. *Virtual Private Server* sebagai solusi server Vpn yang harganya murah untuk mendapatkan fasilitas vpn,Beberapa keuntungan dan mengapa menggunakan *Virtual Private Server*, diantaranya adalah sebagai berikut :

   1) Biaya :

   Sebuah *virtual private server* memberi kegunaan layaknya *dedicated server* dengan harga yang lebih rendah.

   2) *Management* :

   Dengan VPS u*ser* bisa *memanage* semua aspek dari *upgrading* dan *patching software*, tidak perlu kuatir tentang *updating paket*,karena hal tersebut sudah terkontrol.

   3) *Fungsionality* :

   Sebuah VPS berfungsi hampir sama seperti *dedicated server* dan memiliki Os yang berdiri sendiri.

4) *Resource Efficient* :

Memiliki *resource* yang yang besar.

5) *Control* :

sebuah VPS memberikan anda *access root* untuk *system*, hal tersebut juga mengijinkan kita untuk memodifikasi *file server* konfigurasi, *install* aplikasi atau memodifikasi *software system*.

6) Keamanan :

Dengan VPS, *file system* kita tidak akan bisa diakses oleh pemilik VPS lain, tidak seperti *shared evironments* dimana siapapun dengan *sheell access* bisa mencari jalan ke *file* kita, sebuah VPS memastikan *privacy* dan keamana penuh penggunanya.

1.3. Maksud dan Tujuan

Maksud dan Tujuan utama dari pelaksanaan tugas akhir ini adalah mengembangkan *Virtual Private Server* untuk vpn sehingga mampu menyelsaikan masalah yang terjadi di jaringan internet. Adapun tujuannya sebagai berikut :

a. Mampu mengurangi penyadapan dan pencurian *account* di jaringan internet *wifi.*
b. Memberikan solusi VPS bagi yang ingin menggunakan Vpn dengan pengeluaran yang murah
c. Mampu membarikan keamanan pada jarinagn internet dan Menanggulangi penyadapan dan pencurian *account* di jaringan *internet wifi.*
d. Diharapkan Vpn bisa menjadi solusi keamanan yang baik di jaringan wifi

e. Mengamankan *website* dari kemungkinan terjadinya penyadapan data

1.4. Batasan Masalah

Adapun yang menjadi beberapa batasan masalah adalah sebagai berikut :

a. Vpn yang dibahas diutamakan pada Keamanan dalam jaringan internet sebagai solusi untuk mengurangi masalah yang ada pada jaringan internet .
b. Menggunakan kartu jaringan yang *support promiscuous* mode dan monitor.
c. membahas *Virtual Private server* yang digunakan untuk Vpn.
d. Menggunakan *protocol L2TP* dengan software Openvpn karena opensource
e. Menggunakan Putty untuk melakukan konfigurasi pada *Virtual Private Server*.
f. *Server* menggunakan *Centos Os* 5 (32 bit) karena *lisensi*

1.5. Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Observasi

Yaitu pencarian data/informasi dengan melakukan pengamatan langsung terhadap objek yang diteliti.

2. Studi Literatur

Pengumpulan data dengan cara mengumpulkan buku-buku yang ada kaitannya dengan judul penelitian.

3. Interview

Teknik pengumpulan data dengan mengadakan Tanya jawab secara langsung yang berkaitan dengan topik yang diambil.Melakukan Tanya jawab dengan Pakar jaringan,dan dengan intansi terkait

4. Tahap Penggunaan

A. Analisis

Merupakan tahapan menganalisis hal-hal yang diperlukan dalam pelaksanaan proyek pembangunan VPN dengan *Virtual Private Server*.

B. *Design*

Tahap penerjemahan dari data yang dianalisis ke dalam bentuk yang lebih mudah dimengerti oleh *user*.

C. Pengujian

Merupakan tahap pengujian pada pembangunan VPN dengan *Virtual private Server.*

D. *Maintenance*

Tahap Akhir Dimana Suatu jaringan,Perangkat lunak dapat digunakan untuk melakukan perubahan sesuai dengan permintaan *user*.

1.6. Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi penjelasan mengenai latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, serta sistematika pembahasan yang digunakan untuk menyusun laporan tugas akhir.

BAB II LANDASAN TEORI

Berisi dasar teori yang digunakan dalam Pembuatan Tugas akhir, pembangunan Vpn dengan Private Virtual Server ini.

BAB III ANALISIS MASALAH DAN PERANCANGAN

Berisi analisis tentang pembangunan Vpn dengan *Virtual Private Server* dan alur kerjanya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Berisi hasil Perancangan dan pengujian pembangunan Vpn dengan *Virtual Private Server* dan koneksi Vpn nya terhadap keamanan jaringan internet.

BAB V KESIMPULAN DAN SARAN,

Berisi kesimpulan dan saran yang didapatkan selama pelaksanaan Tugas Akhir.