BAB III

ANALISIS DAN PERANCANGAN

3.1. Analisis Sistem

Analisa merupakan suatu tindakan untuk mengetahui lebih jauh tentang obyek yang akan diteliti. Bab ini akan menguraikan proses analisis pembangunan sistem VPN dengan Virtual Private Server juga keamanan sebelum dan sesudah menggunakan VPN. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan – kebutuhan pokok sistem VPN dengan Virtual Private Server yang akan dibangun.

3.1.1 Analisis Wifi

Wi-Fi merupakan kependekan dari *Wireless Fidelity*, yang memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal *Nirkabel* (*Wireless Local Area Networks* - WLAN) yang didasari pada spesifikasi *IEEE 802.11*. Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.11 g, saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya

Awalnya Wi-Fi ditujukan untuk penggunaan perangkat nirkabel dan Jaringan Area Lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinan seseorang dengan komputer dengan kartu nirkabel (*wireless card*) untuk terhubung dengan internet dengan menggunakan titik akses (atau dikenal dengan *hotspot*) terdekat. Wi-Fi dirancang berdasarkan spesifikasi *IEEE 802.11*. Sekarang ini ada empat variasi dari 802.11, yaitu:

1. 802.11a
2. 802.11b
3. 802.11g
4. 802.11n

3.1.2 Standarisasi Jaringan Wireless

Untuk sebuah teknologi yang bersifat massal sebuah standarisasi sangatlah dibutuhkan. Standarisasi akan memberikan banyak keuntungan di antaranya adalah :

1. Pembuatan hardware yang berbeda biasa saling bekerja sama. Tentunya tidaklah sangat efisien wireless di satu merek laptop hanya bisa berhubungan dengan perlatan yang berasal dari merek yang sama.

2. Pembuatan hardware tambahan biasa membuat perlatan yang berlaku untuk semua peraltan berdasarkan informasi dari standarisasi yang telah ada.

3. Penghematan dan perkembangan teknologi yang jauh lebih cepat.

Berdasarkan hasil penelitian yang diperoleh IEEE (*Institute Of Electrical Engineers*) merupakan organisasi non-profit yang mendedikasikan kerja kerasnya demi kemajuan teknologi. Pada tahun 1980 IEEE membuat sebuah bagian yang mengurusi standarisasi LAN dan MAN (*Metropolitan Area Network*). Bagian ini kemudian dinamakan sebagai 802, angka 80 menunjukkan tahun dan angka 2

(dua) menunjukkan bulan dibentuknya kelompok kerja ini. Berdasarkan hasil penelitian yang dilakukan diketahui bahwa internet wireless adalah sebagian dari hasil kerja 802. Bagian ini dibagi menjadi beberapa bagian yang lebih kecil dan lebih spesifik yang dinamakan sebagai unit kerja. Unit kerja ini diberikan nama berupa angka yang berurutan di belakang 802. Berikut adalah contoh unit kerja dan bidang yang ditangani.

Tabel 3.1 Unit kerja standarisasi LAN dan WAN

Unit Kerja	Bidang yang Ditangani
802.1	Higher Layar LAN Protokol
802.3	Ethernet Working Group
802.11	Wireless Working Group
802.15	Wireless Personal Area Network (WAPN) Working Group
802.16	Broadband Wireless Access Working Group
802.17	Reselient Pacet Ring Working Group
802.18	Radio Regulator TAG
802.19	Coexistence TAG

802.20	Mobile Broadcast Wireless Access (MBWA) Working Group
802.21	Media Independent Handoff Working Group
802.22	Wireless Region Area Network

3.1.3 Jenis keamanan wifi

1. Hide SSID

Banyak administrator menyembunyikan *Services Set Id* (SSID) jaringan *wireless* mereka dengan maksud agar hanya yang mengetahui SSID yang dapat terhubung ke jaringan mereka. Hal ini tidaklah benar, karena SSID sebenarnya tidak dapat disembuyikan secara sempurna. Pada saat saat tertentu atau khususnya saat client akan terhubung (*assosiate*) atau ketika akan memutuskan diri *(deauthentication)* dari sebuah jaringan wireless, maka *client* akan tetap mengirimkan SSID dalam bentuk plain text (meskipun menggunakan enkripsi), sehingga jika kita bermaksud menyadapnya, dapat dengan mudah menemukan informasi tersebut. Beberapa tools yang dapat digunakan untuk mendapatkan ssid yang di-*hidden* antara lain: *kismet* (kisMAC), ssid_*jack* (*airjack*).

2. WEP

Teknologi *Wired Equivalency Privacy* atau WEP memang merupakan salah satu standar enkripsi yang paling banyak digunakan. Namun, teknik enkripsi WEP ini memiliki celah keamanan yang cukup mengganggu. Bisa dikatakan, celah keamanan ini sangat berbahaya. Tidak ada lagi data penting yang bisa lewat dengan aman. Semua data yang telah dienkripsi sekalipun akan bisa dipecahkan oleh para penyusup. Kelemahan WEP antara lain :

a. Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
b. WEP menggunakan kunci yang bersifat statis
c. Masalah *Initialization Vector* (IV) WEP
d. Masalah integritas pesan *Cyclic Redundancy Check* (CRC-32)

WEP terdiri dari dua tingkatan, yakni kunci 64 bit, dan 128 bit. Sebenarnya kunci rahasia pada kunci WEP 64 bit hanya 40 bit, sedang 24 bit merupakan Inisialisasi Vektor (IV). Demikian juga pada kunci WEP 128 bit, kunci rahasia terdiri dari 104 bit.

3. WPA-PSK atau WPA2-PSK

WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS. Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline. Brute force dengan menggunakan

mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang digunakan wireless tersebut memang terdapat pada kamus kata yang digunakan si hacker. Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakanlah passphrase yang cukup panjang (satu kalimat).

3.1.4 Kelemahan dan Kekurangan wifi

Banyak pengguna jaringan *wifi* tidak menyadari jenis bahaya apa yang ada di jaringan *wireless (wifi)* misalnya seperti sinyal WLAN dapat disusupi oleh penyadap.Berikut ini dapat menjadi ancaman kekurangan dalam jaringan *wireless,* di antaranya:

A Sniffing to Eavesdrop

Paket yang merupakan data seperti akses HTTP, email, dan Iain-Iain, yang dilewatkan oleh gelombang *wireless* dapat dengan mudah ditangkap dan dianalisis oleh *attacker* menggunakan aplikasi Packet Sniffer seperti cain abel.

B Denial of Service Attack

Serangan jenis ini dilakukan dengan membanjiri *(flooding)* jaringan sehingga sinyal *wireless* berbenturan dan menghasilkan paket-paket yang rusak.

C Man in the Middle Attack

Peningkatan keamanan dengan teknik enkripsi dan authentikasi masih dapat ditembus dengan cara mencari kelemahan operasi protokol jaringan tersebut. Salah satunya dengan mengeksploitasi *Address Resolution Protocol* (ARP) pada TCP/IP sehingga penyadap dapat mengambil alih jaringan *wireless* tersebut. Contoh jika seorang administrator atau seorang yang ingin login ke data yang rahasia maka bisa disadap jika dilakukan di jaringan wifi yang publik umun Keamananan data dalam transmisi sebuah jaringan *wifi* merupakan faktor yang sangat penting.

3.2 Analisis VPN

VPN adalah singkatan dari *virtual private network*, yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar jaringan *komputer* secara aman. Perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi *traffic* (lalu lintas) antar jaringan *komputer* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya ke dalam *jaringan komputers*.

Menurut IETF, Internet Engineering Task Force, VPN is an emulation of a private Wide Area Network(WAN) using shared or public IP facilities, such as the Internet or private IP backbones.merupakan suatu bentuk private internet yang melalui publicnetwork (internet), dengan menekankan pada keamanan data dan

akses global melaluiinternet. Hubungan ini dibangun melalui suatu tunnel (terowongan) virtual antara 2 node.

3.2.1 Analisis Topologi

Remote Access VPN Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah s*ite-to-site*

VPN. *Remote access* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN).

Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *sotware* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara

jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

3.2.2 Analisis Protokol

L2TP dengan software OpenVpn adalah OpenVPN merupakan aplikasi VPN opensource yang gratis (bebas biaya). OpenVPN digunakan untuk membangun koneksi tunneling ter-enkripsi point to point atau server dengan beberapa komputer klien melalui jaringan internet.

L2TP tunneling protocol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft (Gupta, 2003). L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 53 dengan protocol UDP untuk mengirimkan L2TP *encapsulated* PPP frames sebagai data yang di tunnel.Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitu *compulsory*dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung tunnel berada pada ISP, sedangkan pada *voluntary* ujung tunnel berada pada client remote.

3.2.3 Analisis Enkripsi

Enkripsi merupakan teknik untuk mengamankan data yang dikirim dengan mengubah data tersebut ke dalam bentuk sandi-sandi yang hanya dimengerti oleh pihak pengirim dan pihak penerima data. Teknik enkripsi pada computer bedasarkan pada perkembangan ilmu kriptografi. Dahulu kriptografi banyak

digunakanpada bidang militer. Tujuannya adalah untuk mengirimkan informasi rahasia ke tempat yang jauh. Namun saat ini enkripsi telah banyak digunakan untuk aplikasi-aplikasi seperti informasi kartu kredit, PIN (personal identity number), informasi tabungan di bank dan lain sebagainya.

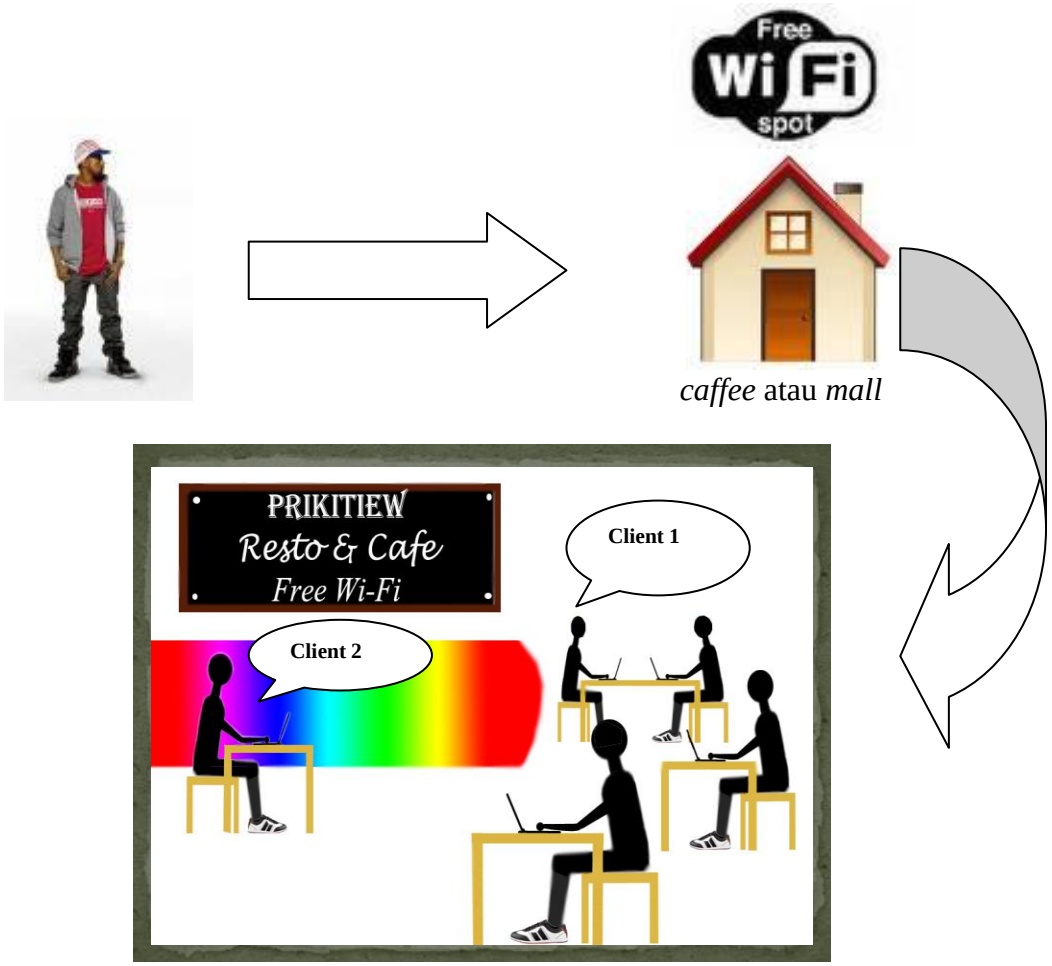
OpenVPN menggunakan algoritma kriptografi yang berbeda seperti 3DES, AES, RC5, Blowfish. mengimplementasikan algoritma AES yang sangat aman dengan kunci 256 bit.

3.3 Analisis masalah

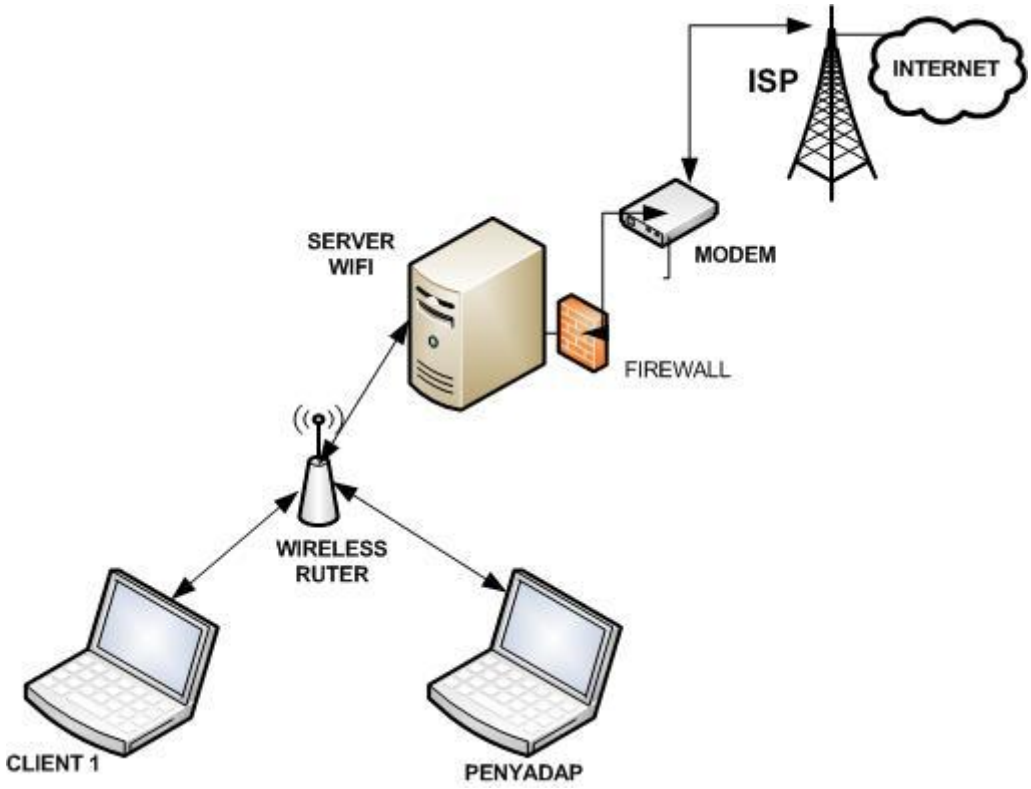
Jaringan Wireless memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Saat ini perkembangan teknologi wireless sangat signifikan sejalan dengan kebutuhan sistem informasi yang *mobile*. Banyak penyedia jasa wireless seperti *hotspot* komersil, ISP, Warnet, kampus,mall maupun perkantoran sudah mulai memanfaatkan wireless pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. Hal ini membuat para penyadap *sniffer* menjadi tertarik untuk mencoba keamampuannya untuk melakukan berbagai aktifitas yang biasanya ilegal menggunakan wifi.

Banyak pengguna jaringan *wifi* tidak menyadari jenis bahaya apa yang ada di jaringan *wifi* misalnya seperti sinyal wireless dapat disusupi oleh penyadap,untuk lebih jelasnya dapat digambarkan sebagai berikut

A . Wireless (*wifi)* dalam keadaan normal



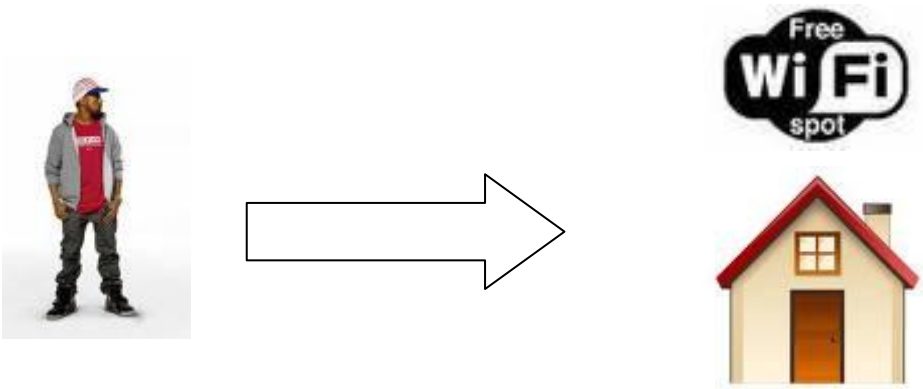
Gambar 3.1 Proses koneksi di jaringan wifi

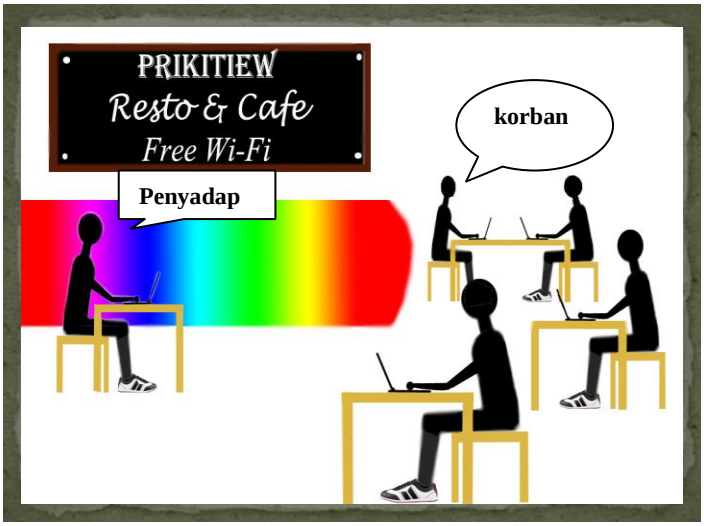


Gambar 3.2 Aliran Paket Data Normal Di jaringan wifi

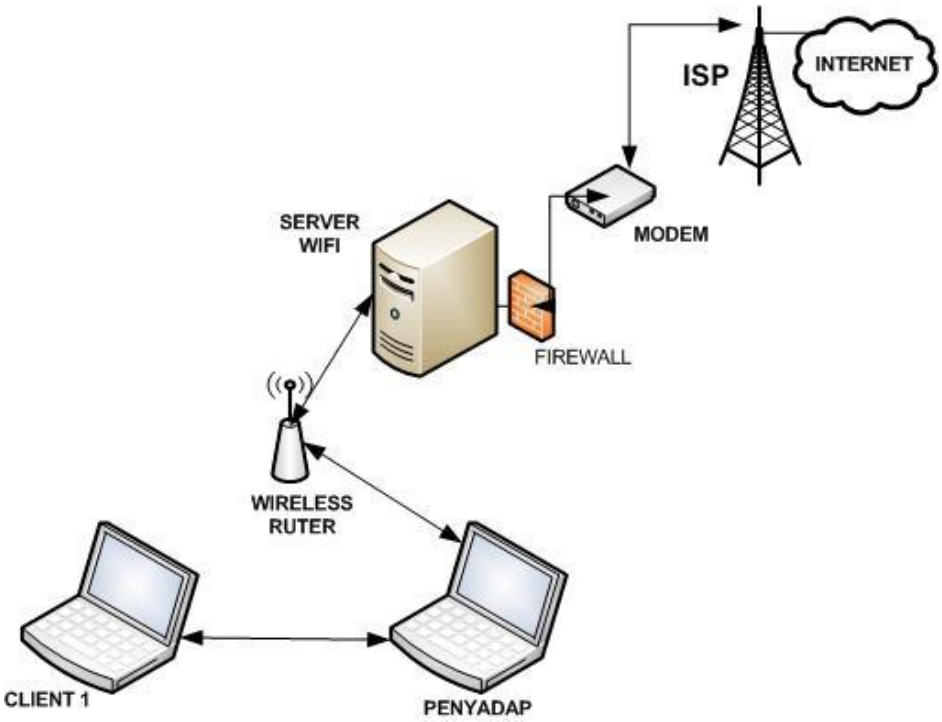
Dari gambar seorang administrator melakukan koneksi dengan wifi dimana disana juga ada banyak client yang melakukan koneksi yang sama dan digambarkan aliran data normal semua aliran data dari tiap client merequest ke server wifi dan server merequest replay ke client yang melakukan request dengan benar,karna keadaan wifi dalam keadaan normal.

B . Wireless (*wifi)* ketika terjadi penyadapan





Gambar 3.3 Proses Penyadapan koneksi di jaringan wifi

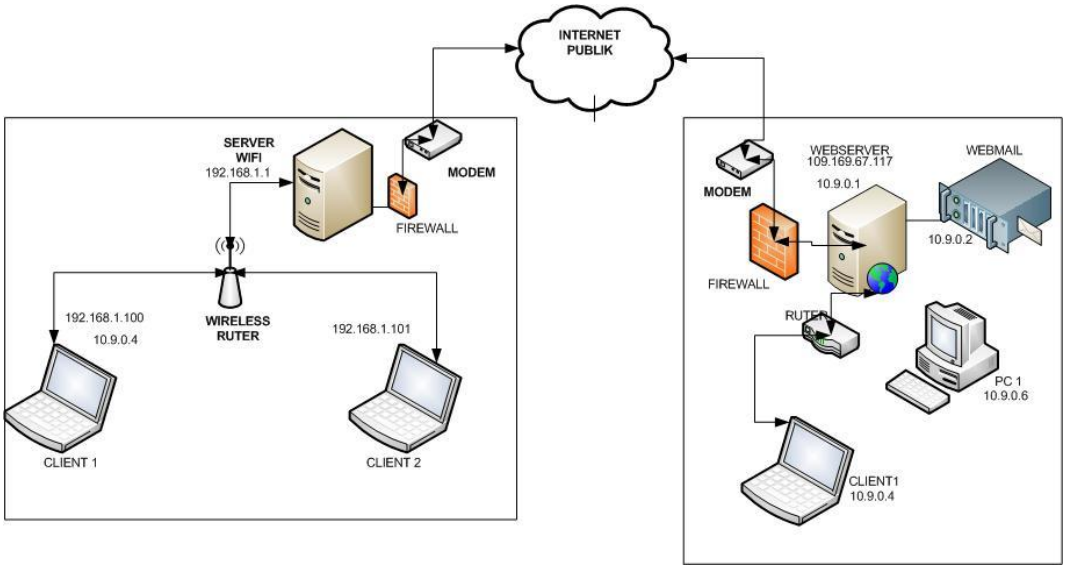


Gambar 3.4 Aliran Paket Data tidak normal Akan melalui Penyadap

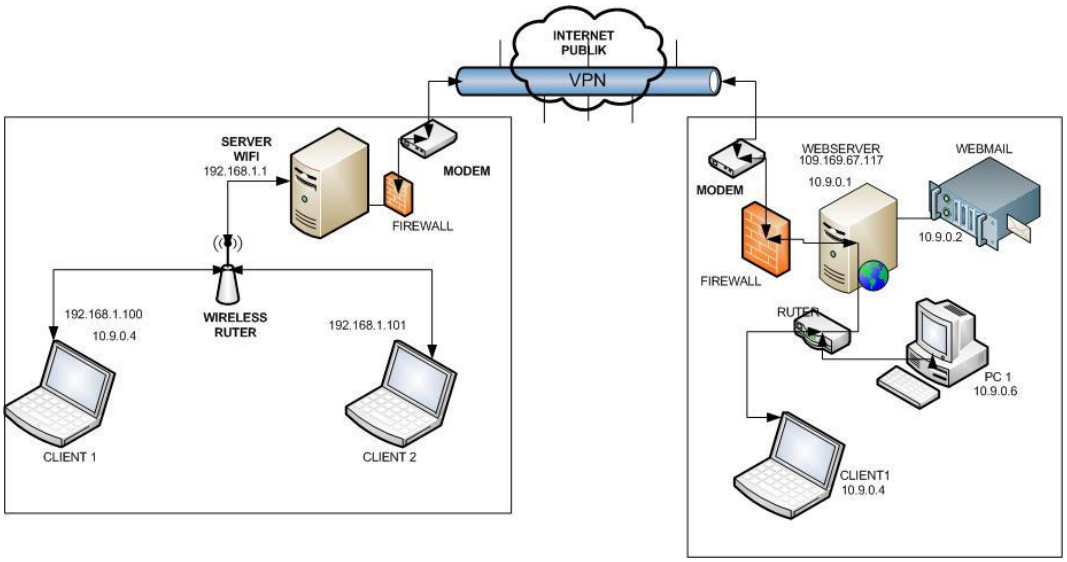
Dari gambar diatas jika seseorang administrator melakukan keneksi dijaringan wifi,umum (publik) dimana dalam satu jaringan tersebut,ada penyadap maka data –data akan melewati penyadap seperti pada Gambar 3.6 apalagi jika seorang administrator mengakses data-data penting maka dapat tersadap oleh penyadap seperti pada gambar aliran data yang seharusnya untuk server di lewatkan dulu ke penyadap hingga dapat disimpulkan betapa bahaya nya jika melakukan koneksi di jaringan wifi yang di dalam nya ada seorang yang menyadap data yang kira request ke server wifi.

3.3.1 Solusi Untuk menanggulangi kelemahan Wifi dan Penyadapan

Dari kekurangan diatas dibutuhkan suatu metode keamanan untuk menanggulangi permasalahan yang terjadi di jaringan wifi disini menggunakan VPN dengan Virtual Private Server sebagai solusi keamanan paket data di jaringan wifi agar data menjadi lebih aman dan bisa menyelsaikan permasalahan yang terjadi di jaringan wifi,dengan VPN dan tanpa VPN dapat digambarkan sebagai berikut

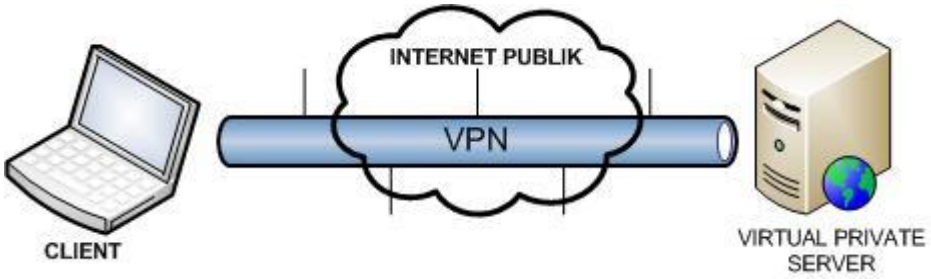


Gambar 3.5 Proses koneksi normal di jaringan wifi



Gambar 3.6 Proses koneksi VPN pada jaringan wifi

Dari Gambar 3.6 dan 3.7 dapat disimpulkan kalau menggunakan VPN bisa menjadi lebih aman karena paket data di kirim melalui VPN (Terowongan) atau jaringan *Private* sehingga paket data yang dikirim dan di terima menjadi lebih Aman



Gambar 3.7 Proses Koneksi VPN

3.4 Analisis kebutuhan sistem VPN

VPN merupakan perpaduan dari teknologi *tunneling* dengan teknologi enkripsi. Teknologi *tunneling* bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Sedangkan teknologi enkripsi menjamin kerahasiaan data yang berjalan di dalam *tunnel*. Untuk membangun VPN dibutuhkan perangkat keras dan perangkat lunak

3.4.1 Analisis Perangkat Keras

Di sini akan dibahas mengenai kebutuhan hardware apa saja yang diperlukan untuk VPN dengan menggunakan Virtual Private server.

A.Kebutuhan Perangkat Keras

Kebutuhan hardware pada skripsi ini terdiri dari beberapa perangkat keras meliputi PC sebagai VPN *server*, VPS sebagai *server*, PC sebagai *client*, dan modem.

1.VPN Server

Komputer VPN *server* pada *Remote Access Virtual Private Network* yaitu bertindak sebagai *server* VPN, *server* VPN bertugas membentuk *tunnel*,

melakukan validitas *certificate*, dan sebagai gateway antar vpn *client*. Komputer yang bertindak sebagai *server* VPN mempunyai spesifikasi sebagai berikut :

Processor : Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 1 cores

Memory : 512 MB

Harddisk : 15 GB

Operating System : Centos 5 x86_64

Bandwidth/Data Transfer : 1000 GB /bulan

Untuk server menggunakan *Virtual Private Server* (Turunan *Dedicated Server*) karena belum Mempunyai *Server* sendiri.

Virtual Private Server (VPS), juga dikenal dengan *Virtual Dedicated Server (*VDS) adalah teknologi *server side* tentang *sistem operasi* dan perangkat lunak yang memungkinkan sebuah mesin dengan kapasitas besar dibagi ke beberapa *virtual* mesin. Tiap *virtual* mesin ini melayani sistem operasi dan *perangkat lunak* secara mandiri dan dengan konfigurasi yang cepat.

1.Server Wifi

Adapun spesifikasi *hardware* yang digunakan sebagai komputer *client* VPN dalam simulasi yang dilakukan memiliki spesifikasi sebagai berikut :

Hardware :

Processor : intel core2duo P7200

Memory : 2 GB

Harddisk : 250 GB

Operating System : windows 7 ultimate

2.Client VPN

Adapun spesifikasi *hardware* yang digunakan sebagai komputer *client* VPN dalam simulasi yang dilakukan memiliki spesifikasi sebagai berikut :

Hardware :

Processor : intel atom 450

Memory : 1 GB

Harddisk : 160 GB

Operating System : windows XP home edition

3.Komputer Penyadap

Adapun spesifikasi *hardware* yang digunakan sebagai komputer Penyadap dalam simulasi yang dilakukan memiliki spesifikasi sebagai berikut :

Hardware :

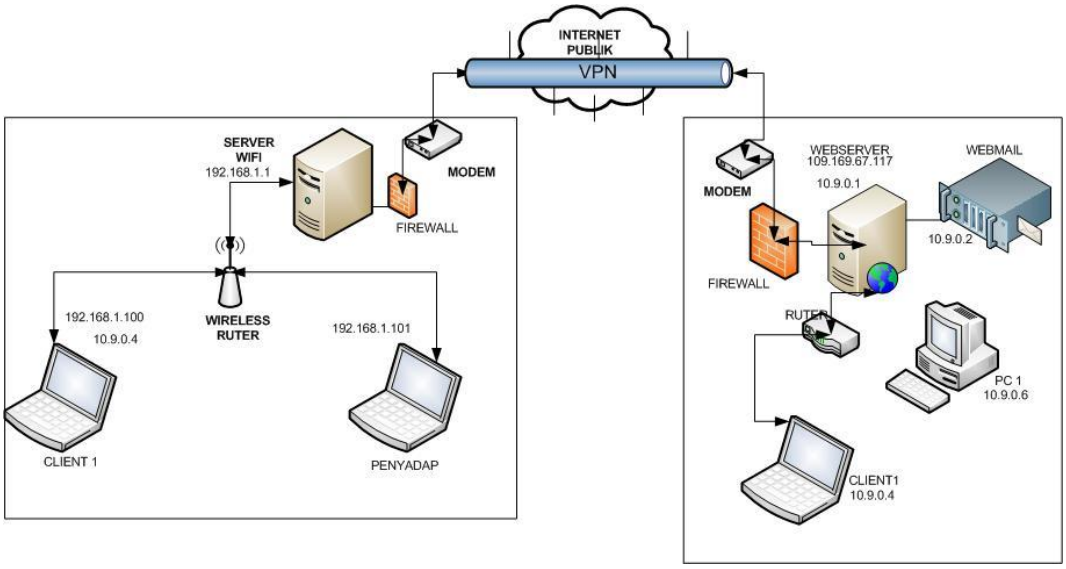
Processor : intel atom 450

Memory : 1 GB

Harddisk : 160 GB

Operating System : Windows XP Propesional

3.5 Analisis Perancangan lingkungan uji



Gambar 3.8 Perancangan lingkungan Kerja

Dari Gambar 3.9 jika seorang administrator terkoneksi ke jaringan wifi dengan ip 192.168.1.100 dan ada penyadap 192.168.1.101 aliran data yang di *request* ke *server* 192.168.1.1 tidak akan terbaca karena *client* melawatkan data melalui jaringan vpn 10.9.0.4 maka aliran data menjadi aman karena menggunakan vpn.

3.6 Analisis software

a. Putty (Untuk menjalankan command - command untuk setup VPS)
b. Winscp (untuk upload dan download)
c. OpenVPN Client (Untuk login ke VPN disisi klien)
d. Netscan
e. Cain & Abel

A.Putty

Putty adalah aplikasi pengganti remote login seperti telnet, rsh, dan rlogin, yang jauh lebih aman. Dikembangkan pertamakali oleh OpenBSD project dan kemudian versi rilis p (port) di-manage oleh team porting ke sistem operasi lainnya, termasuk sistem operasi Linux. Fungsi utama aplikasi ini adalah untuk mengakses mesin secara remote. Bentuk akses remote yang bisa diperoleh adalah akses pada mode teks maupun mode grafis/X apabila konfigurasinya mengijinkan. scp yang merupakan anggota keluarga ssh adalah aplikasi pengganti rcp yang aman, software lainnya adalah sftp yang dapat digunakan sebagai pengganti ftp. Dengan SSH, semua percakapan antara server dan klien di-enkripsi. Artinya, apabila percakapan tersebut disadap, penyadap tidak mungkin memahami isinya. Bayangkan seandainya sedang melakukan maintenance server dari jauh, tentunya dengan account yang punya hak khusus, tanpa setahu pengguna, account dan password tersebut disadap orang lain, kemudian server Akan diambil setelahnya.
Lebih jauh lagi, SSH memungkinkan kita mengamankan koneksi dari pembajakan (jika sedang terhubung sebagai root ke server, tiba-tiba di tengah jalan ada diambil alih, yang tanpa perlu tahu username maupun password nya bisa langsung melanjutkan sesi admin yang sedang aktif, dan tentu saja dengan hak sebagai root).

B.WinSCP

WinSCP adalah aplikasi *open source klien* SFTP, SCP ataupun FTP di Windows. Fungsi utamanya adalah menyediakan sarana pengiriman data yang aman antara komputer lokal dan komputer remote.

WinSCP (*Windows Secure CoPy*) open source SFTP dan klien FTP untuk Microsoft Windows. Fungsi utamanya adalah transfer file aman antara komputer lokal dan remote. Selain ini, WinSCP menawarkan file manager dasar dan file fungsi sinkronisasi. Untuk transfer aman, menggunakan Secure Shell (SSH) dan mendukung protokol SCP selain untuk SFTP.

Pengembangan WinSCP dimulai sekitar Mei 2000 dan terus berlanjut. Perayaan ini diselenggarakan oleh Universitas Ekonomi di Praha, dimana penulis bekerja pada saat itu.Sejak 16 Juli 2003 itu dilisensikan di bawah GNU GPL dan host di SourceForge.net.

WinSCP didasarkan pada pelaksanaan protokol SSH dari Putty dan protokol FTP dari filezilla.WinSCP juga tersedia sebagai *plugin* untuk dua manajer file, FAR dan Altap Salamander.Hal ini populer di kalangan masyarakat Jailbreak iPhone sebagai cara untuk mentransfer data ke dan dari perangkat.

C. Openvpn Client

Software VPN yang digunakan untuk Client agar bisa connect ke Server VPN

D .Netscan

SoftPerfect Network Scanner atau yang biasa dikenal dengan programnya yaitu NETSCAN merupakan program free multi-threaded IP, NetBIOS dan SNMP scanner dengan tampilan interface modern dan beberapa feature baru. Netscan akan melakukan pings computers, scans for listening TCP ports dan menampilkan tipe dari resource yang di share pada jaringam seperti folder .(including system and hidden). Program ini akan dengan mudah mencari semua komputer yang terhubung serta mencari data yang di share dan dapat digunakan untuk melihat MAC Address dan banyak juga fitur lainnya diantara nya seperti berikut :

A. Melakukan Pings computers.
B. Melihat file sharing.
C. Menditeksi MAC

E . Cain&Abel

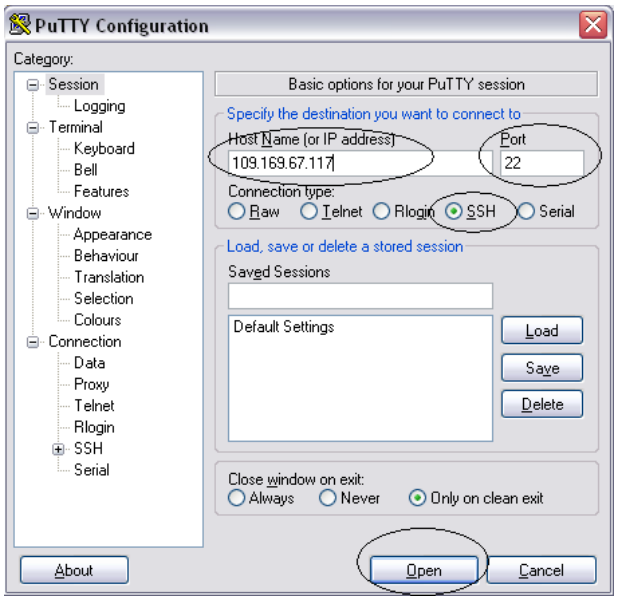
Cain & Abel adalah program yang berguna untuk memonitor (baca,menyadap) paket-paket data yang lewat di jaringan, termasuk paket yang berisi user,pasword dengan cain abel bisa digunakan untuk berbagai macam metode penyadapan,scanning,Crack dan lainnya

3.4.3 Langkah-Langkah Instalasi dan Konfigurasi Server VPN pada VPS

A. *Remote Server* dengan menggunakan putty untuk memulai instalasi di server VPS

1. Jalankan program *putty*
2. Login ke akses *Root SSH*
3. Pada kolom: *Hostname (or IP Address)* isi dengan IP address Virtual Private server.
4. Pada kolom *Port* isi dengan angka 22
5. Pada pilihan *Connection Type* pilih ke *SSH*
6. Dan *Click open*

Untuk lebih jelas lihat Gambar 3



Gambar 3.9 Tampilan Putty *Remote* Vps

Click Open, akan muncul tampilan



Gambar 3.10 Tampilan login ke server

7. Ketika melakukan *remote* pertama akan diminta *user* dan *password* disini menggunakan *user root* dan *password* sany18 yang telah ditentukan waktu Registrasi VPS , tekan *enter*.

   Maka akan muncul tampilan



Gambar 3.11 Tampilan *login* ke *server* VPS

8. Setelah masuk ke *root* Gambar 3.22 disini bisa langsung dilakukan instalasi untuk *Server* VPS

3.4.4 Tahapan Konfigurasi pada *Server* VPS

A. Aktifkan TUN/ TAP

Pada umumnya Default TUN/TAP sudah langsung aktif ketika melakukan registrasi,untuk melakukan pengecekan,ketikan perintah ini

```
# ls -al /dev/net/tun
```

Apabila sudah aktif maka akan muncul replay pada putty

```
crw------- 1 root root 10, 2010 May 10 16:21
/dev/net/tun
```

B. Instalasi aplikasi yang diperlukan untuk membuat vpn

1.Pada aplikasi putty ,ketikan perintah ini:

```
# yum install gcc rpm-build autoconf.noarch zlib-devel
pam-devel openssl-devel make
```

2.Secara otomatis akan terinstal paket-paket ini :

gcc, autoconf.noarch, zlib-devel, pam-devel, openssl-devel.

C.*Download* Paket OpenVPN dan Jadikan RPM

Pada Putty masukan *command* ini untuk *download* paket

```
# wget http://openvpn.net/release/openvpn-2.0.9.tar.gz
```

tekan *enter*,

```
#wget http://openvpn.net/release/lzo-1.08-4.rf.src.rpm
```

tekan *enter*,

Setelah itu masukan command ini untuk menjadikan RPM:

#rpmbuild --rebuild lzo-1.08-4.rf.src.rpm

tekan *enter*

#rpm -Uvh /usr/src/redhat/RPMS/i386/lzo-.rpm*

tekan *enter*

#rpmbuild -tb openvpn-2.0.9.tar.gz

tekan *enter*

#rpm -Uvh /usr/src/redhat/RPMS/i386/openvpn-2.0.9-1.i386.rpm

tekan *enter*

B. ***Copy* File Konfigurasi**

Untuk mempermudah pemeriksaan konfigurasi , copy file konfigurasi ke folder /etc/openvpn dengan perintah *command* ini:

#cp -r /usr/share/doc/openvpn-2.0.9/easy-rsa/ /etc/openvpn/

tekan enter

#cp/usr/share/doc/openvpn-2.0.9/sample-config-files/server.conf /etc/openvpn/

tekan enter

C. **Membuat *Key* RSA**

Masuk ke direktori /etc/openvpn/easy-rsa/2.0 dengan perintah sebagai berikut :

#cd /etc/openvpn/easy-rsa/2.0

#source ./vars

```
#./vars

#./clean-all

#./build-ca
```

Ketikan Perintah ini untuk membuat key servernya :

```
#./build-key-server server
```

Buat Diffie Hellman:

```
# ./build-dh
```

D. **Konfigurasi Server VPN**

Menuju direktori /etc/openvpn/ ketikan command dibawah:

```
# cd /etc/openvpn/
```

Untuk membuat konfigurasi ketikan perintah ini :

```
# vi server.conf
```

isi dengan sintak ini *dev tun*

E. **Membuat file konfigurasi UDP**

Ketikan command dibawah:

```
$ cat > 53.conf

konfigurasi

port 53

proto udp

dev tun

ca /etc/openvpn/keys/ca.crt

cert /etc/openvpn/keys/server.crt
```

```
key /etc/openvpn/keys/server.key
dh /etc/openvpn/keys/dh1024.pem

plugin /usr/share/openvpn/plugin/lib/openvpn-auth-
pam.so /etc/pam.d/login
client-cert-not-required
username-as-common-name
server 10.9.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1"
push "dhcp-option DNS 4.2.2.1"
push "dhcp-option DNS 4.2.2.2"
keepalive 5 30
comp-lzo
persist-key
persist-tun
status server-tcp.log
verb 3
```

konfigurasi simpan di

openvpn /etc/openvpn/53.conf

F. ***Setting Firewall***

Aktifkan *packet forwarding*:

```
#echo 1 > /proc/sys/net/ipv4/ip_forward
```

Edit NAT Table untuk MASQUERADING, setting untuk VPS:

```
#iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o
venet0 -j SNAT -to ip.address.vps.
```

G. **Membuat / Menambah *User* VPN**

Masukan command dibawah :

```
# adduser client -m -s /bin/false
```

Kemudian untuk password:

```
# passwd "client"
```

Akan diminta memasukan *password* :

Changing password for *user* .

New UNIX password:

Setelah dimasukan tekan *enter* dua kali.

Jika sewaktu - waktu ingin hapus user tertentu:

```
# userdel nama user
```