IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* (VPN) DENGAN OTENTIKASI RADIUS *SERVER* PADA PT. ANUGERAH TUNGGAL MANDIRI JAKARTA

Rosmana[1], Fitri Latifah[2]
[1]Teknik Informatika, Sekolah Tinggi Manajemen Informatika & Komputer Nusa Mandiri
[2.] Komputerisasi Akuntansi AMIK BSI Jakarta

fitri.latifah25@gmail.com

Abstrak

Abstract

The principle of this research is un availability of secure data exchange lines, as well as the lack of authentication for users who join the PT network. Anugerah Tunggal Mandiri. To ensure the security of the VPN, the need for authentication process in which the adoption of restrictions on who is allowed to enter a network. Protocol that supports VPN authentication process on one of which is Service User Authentication Dial-In remote (RADIUS). This protocol is also often used for authentication of the wireless network, Ethernet switches and other devices. Application of VPN technology allows data exchange can be run safely and smoothly, as supported by the encryption technologies and tunnels. the RADIUS server is used as a centralized user management, which has the capacity in terms of authentication, authorization and accounting. The results showed the data sent through the VPN pass through a special line known as the tunnel name and therefore can not be detected by sniffing program.

***Key word** : VPN, RADIUS server, Tunneling*

PENDAHULUAN

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 dalam reliabilitas suatu jaringan. *Virtual Private Network* (VPN) merupakan salah satu cara yang dapat digunakan untuk membuat jaringan yang bersifat *private* dan koneksi jarak jauh (*remote access*) dengan tingkat keamanan yang tinggi diatas jaringan publik atau internet.

Teknologi VPN sendiri sebenarnya dapat didukung oleh beberapa protokol keamanan, salah satunya adalah *Remote Authentication Dial-In User Service* (RADIUS). RADIUS *server* digunakan dalam implementasi *remote-access* VPN karena pada RADIUS terdapat fungsi *authentication, authorization*, dan *accounting* (AAA). Pada proses *authentication* menawarkan proses otentikasi *user, authorization* menawarkan *access-control* untuk *user* dan *accounting* digunakan untuk melacak konsumsi *network-resource* yang dilakukan oleh *user*. Dengan adanya proses mekanisme tersebut dapat meningkatkan sistem keamanan jaringan.

Berdasarkan penelitian yang dilakukan Sahari (2008:46-54) dalam merancang dan mengimplementasikan VPN pada sebuah jaringan nirkabel Universitas Putra Indonesia menunjukan bahwa dengan gagasan awal seluruh dosen, karyawan dan mahasiswa dapat dengan mudah memperoleh data ataupun informasi dari internet dengan tetap memastikan bahwa kerahasiaan dari data yang sensitif dapat terjaga pada saat tranmsisi. Sehingga dibangun sebuah sistem baru dengan mempertimbahkan beberapa aspek keamanan dan hak akses. Sistem tersebut yaitu *Virtual Private Network* (VPN) yang memberikan fungsi dalam menjaga kerahasian data (*Confidentiality*), keutuhan data (*Data Integrity*) serta otentikasi sumber (*Origin Authentication*). PT Anugerah Tunggal Mandiri termasuk kedalam jenis perusahaan induk (*holding company*) dimana perusahaan ini memiliki beberapa anak perusahaan yang tersebar dibeberapa

tempat dengan jenis usaha yang berbeda. Jalur atau alat komunkasi untuk pertukaran data dan informasi antara kantor pusat dengan anak perusahaan masih dengan cara manual seperti menggunakan fasilitas internet melalui *email, messenger,* fax maupun *line* telepon. Hal ini menyebabkan setiap orang masih bisa masuk kedalam jaringan komunikasi dikarenakan masih belum tersedianya pembatasan hak akses. Karena itulah diharapkan melalui teknologi VPN dengan otentikasi RADIUS *server*, antara kantor pusat dan anak perusahaan maupun antara karyawan atau pimpinan yang sedang bertugas di luar kantor, terbentuk suatu jaringan komunikasi yang mudah dan tetap terjamin keamanannya.

BAHAN DAN METODE

Data yang melalui jaringan VPN akan terlebih dahulu dienkapsulasi (dibungkus) dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point to point* sehingga data dapat melewati jaringan publik, proses enkapsulasi sering disebut *tunneling* (Wendy dan Ramadhana, 2005a:1).

Secara mendasar *tunneling* merupakan suatu metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung. Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua *end point* atau ujung.

Menurut Hendriana (2012:132-141) dalam penelitiannya, sebuah jaringan VPN perlu dilakukan tahap pengujian keamanan dalam komunikasi data untuk mengetahui faktor-faktor yang mempengaruhi keamanan komunikasi data pada jaringan tersebut. Adapun mekanisme pengujian kemanan yang dilakukan meliputi penggunaan *software cain and abel* dan software *Wireshark.* Percobaan dalam penelitian tersebut salah satunya yaitu membandingkan dua keadaan jaringan setelah dilakukan *sniffing* sebelum dan sesudah mengaktifkan fasilitas VPN. Terbukti dalam penelitian tersebut ketika dilakukan *sniffing* dengan menggunakan *software cain & Abel* dan *Wireshark* dalam keadaan *service* VPN dimatikan maka akan terlihat aktifitas penyadapan. Berbeda ketika *sniffing* dikukan dalam keadaan *service* dari VPN diaktifkan, dari hasil percobaan menunjukan bahwa tidak ada aktivitas yang terlihat pada jaringan tersebut, karena pengguna jaringan sedang berada dalam *tunnel* jaringan VPN.

Untuk menjamin keamanan dalam jaringan VPN, perlu adanya proses otentikasi dimana diberlakukannya pembatasan siapa saja yang diperbolehkan masuk kejaringan. Protokol yang mendukung proses otentikasi pada VPN salah satunya yaitu *Remote Authentication Dial-In User Service* (RADIUS). Protokol ini juga sering digunakan untuk otentikasi jaringan nirkabel, switch Ethernet dan perangkat lainnya.

Dalam sebuah penelitian penerapan RADIUS *Server* pada jaringan WiFi yang dilakukan oleh Agus Prihanto, menunjukan bahwa user yang tidak terdaftar pada RADIUS *Server* tidak bisa memanfaatkan fasilitas jaringan.

Menurut Prihanto (2010:230) menyimpulkan dalam penelitiannya, bahwa "Hasil menunjukan dengan menggunakan RADIUS autentikasi user di jaringan WiFi Kampus dapat dikelola secara terpusat dan jika user tidak berhasil melakukan authentikasi ke *server* RADIUS, maka *user* tidak bisa memanfaatkan fasilitas jaringan kampus sekalipun hanya untuk intranet".

Ketika RADIUS diterapkan pada jaringan VPN, *user* dapat dengan mudah dikelola secara terpusat. Sehingga *user* yang telah terdaftar pada RADIUS *server* dapat melakukan koneksi kejaringan VPN dari mana saja dengan terlebih dahulu terkoneksi ke internet walaupun menggunakan *provider* yang beda-beda.

Konsep Dasar Jaringan

Menurut Aditya (2011a:3) Jaringan komputer adalah "sebuah sistem yang terdiri atas komputer, *software* dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama".

Pada awalnya, masing-masing komputer tersebut bekerja secara terpisah antara satu dengan yang lainnya, namun suatu saat komputer tersebut tentu perlu dikorelasikan untuk saling berhubungan membagi informasi.

Jaringan komputer dapat di klasifikasikan antara lain

Berdasarkan Jarak

1. Local Area Network (LAN)

Menurut Aditya (2011b:11) mendefinisikan, bahwa "LAN (Jaringan *Local Area Network*) adalah jaringan komputer yang jaringannya hanya mencakup jaringan kecil, seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil". Meskipun LAN sebenarnya mula-mula dikembangkan

di dunia *minicomputer*, tetapi justru menjadi populer setelah banyak digunakan PC (*Personal Computer*). Hal ini disebabkan kerena hal-hal sebagai berikut:

a. Pemakaian Bersama Sumber Daya (Resources Sharing)

Adanya LAN yang saling menghubungkan sistem komputer dan memungkinkan pengguna *communicaties server*, menyebabkan peralatan yang dihubungkan ke LAN dapat digunakan bersama. Adanya sistem seperti ini menyebabkan sebuah PC yang tadinya bekerja sendiri, kini dapat saling bekerja sama dalam batas-batas tertentu, bahkan juga dengan sistem komputer yang lebih besar. Kerjasama yang dapat dilakukan juga semakin berkembang dari pertukaran data sampai saling memakai peralatan yang dihubungkan dengan salah satu sistem komputer (*Resources Sharing*).

b. Memungkinkan Perbaikan untuk Pekerjaan.

LAN menyebabkan banyak pemakai satu tergantung kepada pemakai lainnya, atau hanya tergantung pada satu CPU saja, sehingga apabila CPU itu tidak bekerja, maka tidak semua pemakai terpaksa berhenti bekerja, tetapi hanya pemakai yang menggunakan CPU tersebut. Jika diperlukan, pemakai dapat juga mengalihkan pekerjaannya ke CPU lain.

c. Memungkinkan Pengiriman File (File Transfer)

Jika ada LAN menghubungkan sistem yang satu dengan yang lain, maka dimungkinkan pengiriman *file* dari sistem yang satu ke sistem yang lain. Hal ini bahkan mudah dilakukan antar sistem yang berbeda merk, dan yang berbeda merk dapat saling dihubungkan pada suatu LAN dan hubungan tersebut tidak hanya berhubungan secara fisik tetapi juga dapat saling berkomunikasi.

d. Memungkinkan Pertukaran Informasi

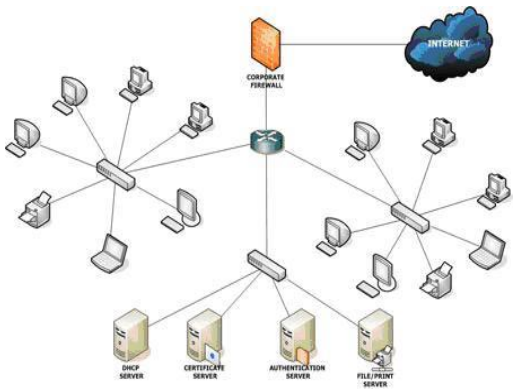
Keuntungan yang paling utama dari LAN yaitu dimungkinkannya pertukaran informasi antar sistem yang dihubungkan pada suatu jaringan LAN tersebut dengan sangat efisien.

e. Meningkatkan Produktivitas

Karena setiap pemakai dapat mempunyai suatu sistem dan bukan lagi terminal, maka pemakai dapat mengerjakan hal-hal yang tidak mungkin pemakai kerjakan karena harus menggunakan CPU yang digunakan bersama. Disamping itu karena pada dasarnya pemakai memiliki CPU sendiri, maka pemakai lebih bebas menggunakan *software* aplikasi sesuai dengan kebutuhanya, apabila sistem tersebut adalah PC yang *software*-nya mudah didapat dan harganya tidak terlalu mahal. Semua hal ini akan meningkatkan produktivitasnya.

f. Mengurangi atau Menghilangkan Ketidakaturan (Chaos)

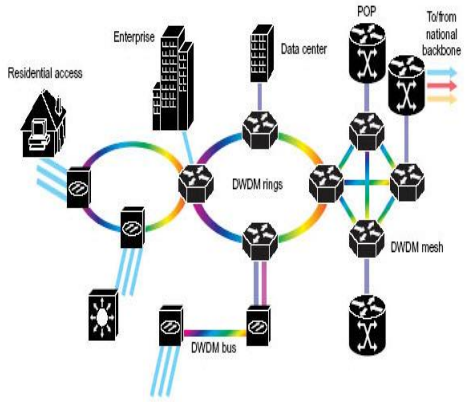
Salah satu dampak negatif dari perkembangan PC dalam suatu perusahaan adalah suatu ketidakaturan atau *chaos*, karena siapa saja atau bagian mana saja di dalam perusahaan ataupun instansi dapat membeli dan menggunakan PC (*Personal Computer*).



Gambar 2.1. Local Area Network
Sumber :
http://www.mysecurecyberspace.com/encyclopedia/index/lan.jpg

2. Metropolitan Area Network (MAN)

Menurut Aditya (2011c:12) mendefinisikan, bahwa "MAN (*Metropolitan Area Network*) suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan dan sebagainya". Komunikasi yang terjadi dilakukan melalui telepon, gelombang mikro atau bahkan satelit. Jaringan ini memiliki 10 – 50 km dan merupakan pilihan untuk membangun jaringan komputer antar kantor cabang dalam suatu kota.

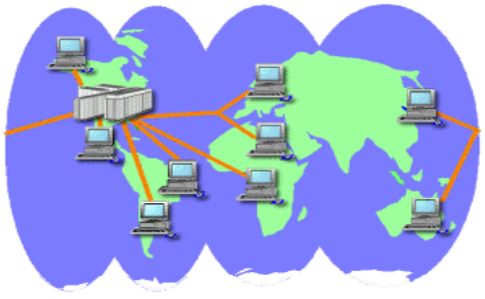


Gambar 2.2 Metropolitan Area Network (MAN)

Sumber : http://www.pulsewan.com/data101/images/metropolitan_area_network_diagram.jpg

3. Wide Area Network WAN)

Menurut Aditya (2011d:12) mendefinisikan, bahwa "WAN (*Wide Area Network*) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik. Jaringan ini merupakan pengembangan dari MAN yang dibutuhkan oleh instansi perusahaan yang membangun kantor-kantor cabang atau sentra-sentra produksi yang tempatnya berada diluar kota atau bahkan luar pulau dan luar negeri. Untuk membangun jaringan komputer ini dibutuhkan fasilitas infrastruktur publik, yaitu internet. Meskipun relatif lebih murah, namun belum banyak instansi atau perusahaan memanfaatkan fasilitas internet ini dengan optimal.

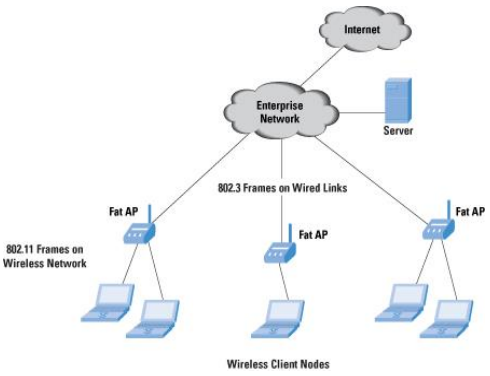


Gambar 2.3 Wide Area Network (WAN)
Sumber : http://www.jegsworks.com/lessons/lesson7/wan-world.gif

4. WLAN (*Wireless Local Area Network*)

Menurut Sugeng (2005:1) mendefiniksan WLAN *(Wireless Local Area Network*) adalah "teknologi jaringan yang tidak menggunakan perangkat kabel yang umumnya dijumpai di dalam sebuah jaringan komputer dewasa ini".

Pada dasarnya penggunaan WLAN pada suatu jaringan tidak berbeda dengan jaringan yang menggunakan kabel, hanya saja biaya pemasangan akan relatif lebih ringan terutama pada suatu jaringan yang jaraknya cukup berjauhan, sehingga walaupun perangkat tersebut relatif mahal dibanding menggunakan kabel tetapi jika dilihat kemudahan dan biaya instalasi jaringan total lebih murah khususnya jika jarak yang berjauhan dan atau medan yang sulit jika menggunakan kabel. Jika suatu hubungan antara sistem komputer dihubungkan dengan menggunakan media komunikasi gelombang *mikro* (gelombang radio), maka sistem tersebut lebih cocok jika disebut sebagai *Wireless Area Network* (WLAN), jarak yang didapat ditempuh tergantung dari sarana komunikasi radio yang dipasang. Dengan sistem ini, maka komunikasi dapat dilakukan dimana saja dan sering juga disebut sebagai komunikasi tanpa kabel.



Gambar 2.4. *Wirelees Local Area Network* (WLAN)

Sumber : http://www.ustudy.in/sites/default/files/images/wlan1.jpg

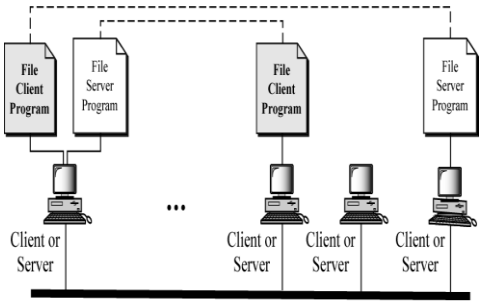
Berdasarkan Fungsi

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai *client* dan juga *server*. Tetapi ada jaringan yang memiliki komputer khusus didedikasikan sebagai *server* yang lain sebagai *client.* Ada juga yang tidak memiliki komputer yang khusus berfungsi sebagai *server* saja

1. Peer to Peer

Pada sebuah konektivitas jaringan, setiap terminal memiliki peran dan derajat yang sama. Jaringan lokal dengan konektivitas *Peer to Peer* ini dibentuk dengan menghubungkan setiap terminal secara langsung sehingga masing-masing terminal dapat berbagi data, aplikasi dan peripheral lainnya. Semua terminal dapat bertindak sebagai workstation atau server. Oleh karena itu, bentuk *Peer to Peer* ini tidak dirancang untuk WAN (*Wide Area Network*).

Pembangunan jaringan dengan arsitektur ini akan menghemat biaya untuk pembelian server dan dapat mengoptimalkan pemanfaatan sumber daya seperti harddisk, printer, processor dan memori dari masing-masing komputer yang ada. Namun memiliki sejumlah kelemahan, antara lain pengelola jaringan atau pengakses akan mengalami kesulitan untuk melacak keberadaan data atau file yang dibutuhkan, karena masing-masing komputer dapat berfungsi sebagai server yang memberikan layanan bagi komputer lainnya, proses pemeliharaan dan pengamanan data dan file aplikasi ini menjadi sulit dan rumit dan juga sangat rentan dari ancaman virus atau dari orang-orang yang tidak berhak.

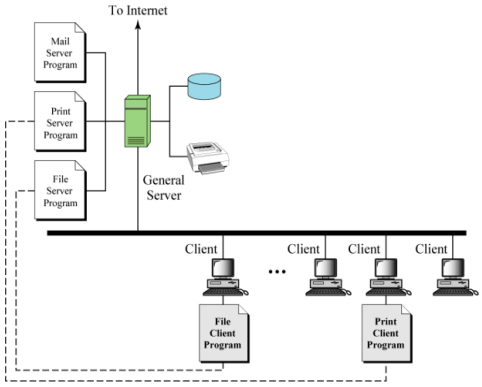


Gambar 2.5 Jaringan Peer to Peer
Sumber :
http://tukshareaja.files.wordpress.com/2010/08/peer.jpg

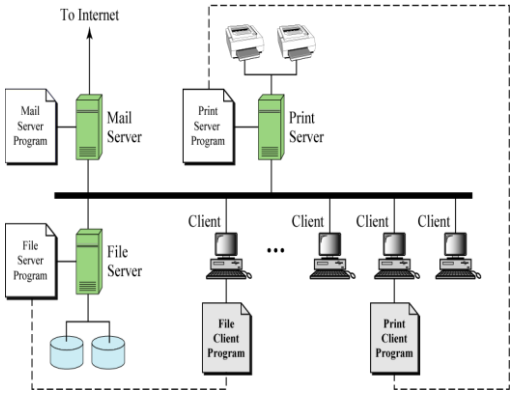
2. Client Server

Menurut Aditya (2011e:13) mendefinisikan, bahwa "jaringan komputer dengan komputer yang dedikasikan khusus sebagai server". Pada model ini, komputer *client* tidak dapat berfungsi sebagai server. Sementara itu, meskipun server dapat berfungsi sebagai client (*server non dedicated*), namun sebaliknya dihindari, agar tidak berubah menjadi arsitektur *Peer to Peer*. Prinsip kerjanya, *server* akan menunggu permintaan dari *client*, memproses dan memberikan hasilnya kepada *client*. Sedangkan *client* akan mengirimkan permintaan ke *server*. Menunggu proses dan melihat visualisasi hasil prosesnya. Model ini dirancang untuk jaringan komputer skala luas. Sistem ini menggunakan TCP/IP (*Transmission Control Protokol / Internet Protokol*), contohnya Unix dan Windows NT. Jenis layanan *client server* antara lain:

1. File Server : Memberikan layanan fungsi pengelolaan file
2. Print Server : Memberikan fungsi layanan pencetakan
3. Database Server : Proses fungsional mengenai database dijalankan pada mesin ini dan stasiun lain dapat meminta pelayanan
4. DIP : Memberikan pelayanan fungsi penyimpanan manajemen dan pengambilan data (*Document Information Processing*)



Gambar 2.6. Model Client Server dengan server yang berfungsi umum
Sumber
http://dc225.4shared.com/doc/9jZb2J55/preview_html_77141bd3.png

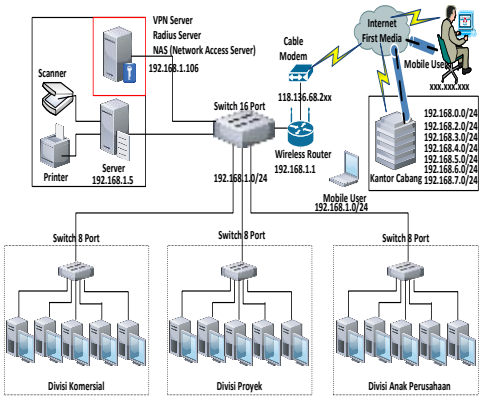


Gambar II.7. Model *Client Server* dengan *Dedicated Server*
Sumber :
http://dc225.4shared.com/doc/9jZb2J55/preview_html_m28422584.png

HASIL DAN PEMBAHASAN

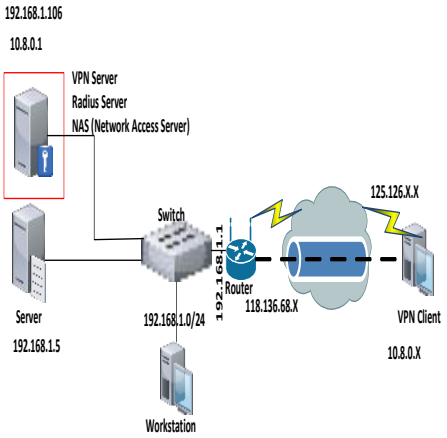
Skema Jaringan

Tidak terlalu banyak perubahan yang dilakukan pada implementasi VPN di PT. Anugerah Tunggal Mandiri ini. Berdasarkan analisa permasalahan yang dihadapi maka ditambahkan sebuah VPN Server dan RADIUS server sebagai usulan pemecahan masalah. Skema jaringan setelah penambahan VPN dan RADIUS Server yang dibangun adalah sebagai berikut:



Gambar 3.1. Skema Jaringan VPN
Sumber hasil penelitian

Komputer yang digunakan untuk instalasi VPN *Server*, Radius *Server* dan NAS merupakan komputer yang telah tersedia di kantor pusat jadi dalam penelitian ini tidak dibahas mengenai anggaran biaya untuk pengadaan komputer yang akan dijadikan *server*. Sebenarnya tiga aplikasi tersebut bisa diinstal ditempat yang berbeda, tetapi dengan di instal dalam satu komputer dapat menghemat dan menekan biaya untuk pengadaan barang baru. VPN *server* nantinya akan bertindak untuk merespon VPN yang masuk, dengan terlebih dahulu dilakukan otentikasi oleh RADIUS server. NAS (*Network Access server*) sendiri bertindak sebagai *client* dari RADIUS server atau sebagai jembatan penghubung antara VPN *client* yang akan melakukan koneksi ke VPN server dengan RADIUS server sebagai protokol yang akan melakukan otentikasi serta otoriasi sebelum akhirnya dapat terhubung ke jaringan. Pada konfigurasi Jaringan pertama dilakukan pengalamatan IP terhadap server dan client. Adapun pengalamatan IP terhadap VPN server, router dan client adalah sebagai berikut :



Gambar 3.1. Konfigurasi Jaringan VPN
Sumber hasil penelitian

Untuk alamat IP publik pada VPN *client* akan tergantung pada provider yang digunakan ketika mengakses internet, gambar di atas sebagai simulasi ketika *client* akan masuk kejaringan VPN. VPN *server* yang berfungsi sebagai infrastruktur komunikasi yang mempunyai mekanisme protokol komunikasi data SSL memberikan IP *Address* kepada *client* yang terkoneksi dengan VPN *server*, sehingga pada *client* akan mempunyai IP address VPN yang telah diberikan oleh *server*, sehingga apabila *client* melakukan *remote* terhadap *server* melalui koneksi internet, maka network yang digunakan untuk berkomunikasi dengan server yaitu menggunakan network VPN. Pada VPN server akan diberikan alamat IP 10.8.0.1 dengan subnet 255.255.255.0, sedangkan *client* akan dialokasikan alamat IP pada *range 10.8.0.2-10.8.0.254*. Berikut ini tabel alokasi IP *address* untuk jaringan VPN

Tabel :3.1. Konfigurasi IP

No	Hadware	IP Address	Subnet Mask
1	Router	*Public* : 118.136.68.2xx	255.255.0.0
		Private : 192.168.1.1	255.255.255.0
2	VPN Server	192.168.1.106	255.255.255.0
		IP VPN: 10.8.0.1	
3	PC Server	192.168.1.5	255.255.255.0
4	Workstation	192.168.1.0/24	255.255.255.0
5	VPN *Client*	*Public* : 126.125.x.x	255.255.0.0
		Private : 192.168.0.0/24	255.255.255.0
		IP VPN: 10.8.0.x	255.255.255.0

Instalasi Open VPN

Berikut dijelaskan langkah-langkah dalam penginstallan *software* OpenVPN pada Ubuntu 12.04.3 LTS dan pada komputer *client* dengan sistem operasi Windows XP Profesional sp3.

1. Instalasi Open VPN pada server

root@admin-atm:~# apt-get install openvpn

copy script konfigurasi open VPN kedalamfolder Open VPN

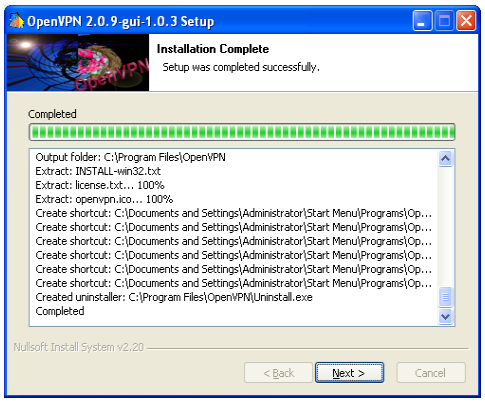
```
root@admin-atm:~# mkdir /etc/openvpn/easy-rsa/
root@admin-atm:~# cp -r
/usr/share/doc/openvpn/examples/easy-rsa/2.0/*
/etc/openvpn/easy-rsa/
```

2. Install Open VPN pada Chient

Untuk proses instalasi pada *client* dengan OS Windows, maka pertama kali download *software* OpenVPN berbasis GUI untuk windows pada laman :

http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

3. Install software



Gambar 3.2. Proses Instalasi OpenVPN GUI
Sumber hasil penelitian

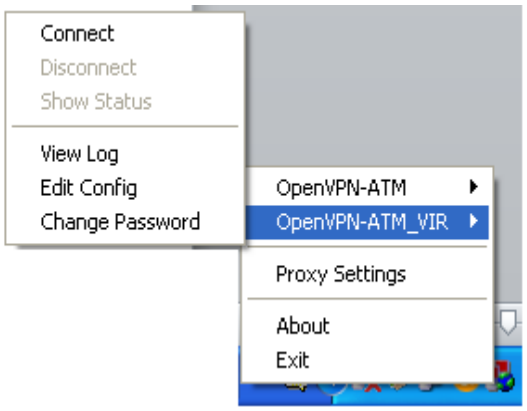
4. Akan berbentuk sebuah network adapter baru nama TAP-Win32

Adapter V8 pada *Network Connections*, juga akan terbentuk OpenVPN GUI di taskbar seperti gambar dibawah:

Gambar 3.3. OpenVPN GUI *Tray*
Sumber hasil penelitian

Konfigurasi Open VPN

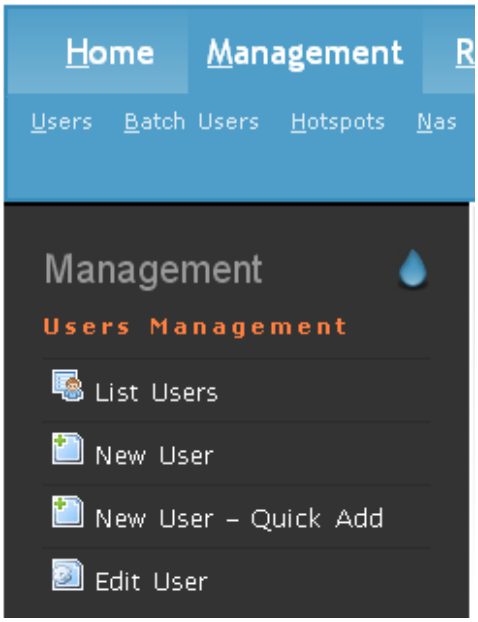
Setelah OpenVPN di instal pada *server* dan client, maka langkah berikutnya adalah konfigurasi OpenVPN baik *server* maupun *Client*. Jika proses konfigurasi selesai, maka akan terlihat adanya pilihan koneksi pada tray OpenVPN di taskbar.



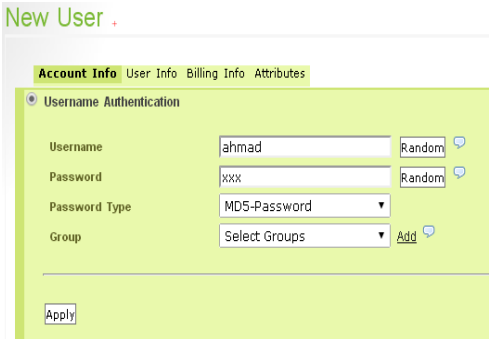
Gambar 3.4. Menu Koneksi pada *Client*
Sumber hasil penelitian

Membuat *client* VPN yang baru

Aplikasi daloradius memberikan kemudahan untuk manajemen *user* baik menambah ataupun menghapus. Untuk membuat user baru, buka halaman daloradius, pilih menu "Management – User" dan 'New User



Gambar
Menu Management User Daloradius
Sumber hasil penelitian



Gambar IV.12. Membuat User Baru
Sumber hasil penelitian

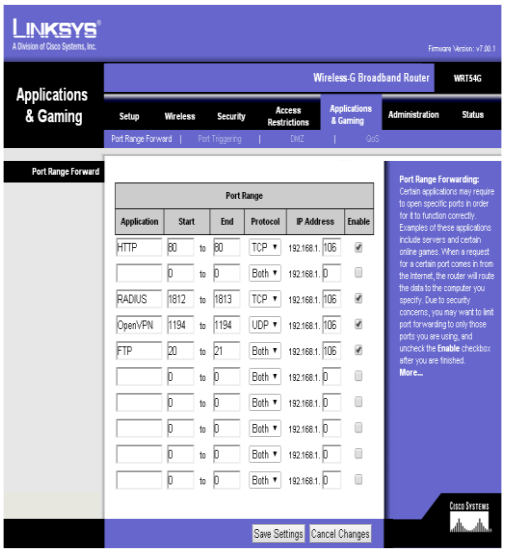
Konfigurasi Port Forwading Pada Router

Setelah semua langkah instalasi dan konfigurasi VPN baik pada sisi server maupun *client*, langkah berikutnya yang tidak kalah pentng yaitu konfigurasi *port forwading* pada *router*. Hal ini dimaksudkan karena server VPN berada di belakang *router*, sehingga jika tidak dilakukan *port forwad* maka koneksi *client* tidak dapat mencapai *server*.

Adapun *port* yang di arahkan ke *server* dari *router* yaitu:

1. Port 1194 : VPN
2. Port 1812 dan 1813 : RADIUS *Server*
3. Port 80 : Web
4. Port 20 dan 21 : FTP

Adapun langkah yang dilakukan yaitu akses web administrator router melalui web browser dengan memasukan user name dan password, kemudian konfigurasi sesuai kebutuhan.



Gambar IV.13. Konfigurasi *Port Forwading*

Keamanan Jaringan

Sistem keamanan yang diterapkan dan telah terintegrasi dengan OpenVPN meliputi:

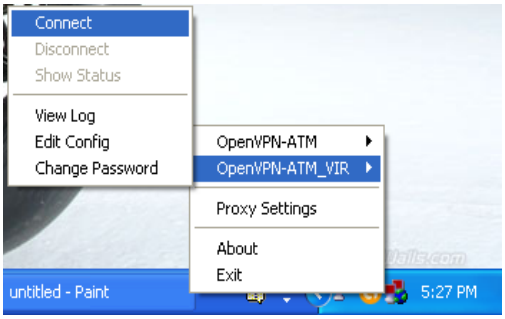
1. Metode *Tunneling* (terowongan)
   Dengan metode ini terbentuk terowongan virtual diatas jaringan publik dengan protokol *Secure Socket Layer* (SSL)
2. Metode Enkripsi
   Untuk *Encapsulations* (membungkus) data yang melawati *tunnel*, maka data tersebut akan dirubah dengan metode algoritma kriptograpi AES-128-CBC .
3. Metode otentikasi pengguna
   Mekanisme otentikasi pengguna diemplementasikan pada VPN server yang digunakan untuk memfilter pengguna ketika mengakses jaringan VPN. Sebagai hasilnya hanya pengguna yang berwenang mengakses sumber jaringan. Adapun otentikasi pengguna yang diterapkan pada penelitian ini adalah menggunakan RADIUS *Server*

Berikut ini gambaran proses otentikasi, otorisasi dan akuntasi yang dipakai dalam sistem RADIUS, proses yang menjelaskan ketika RADIUS *server* menerima permintaan dari *user* ketika melakukan login sampai user menghentikan koneksnya ke jaringan.

Pengujian Jaringan

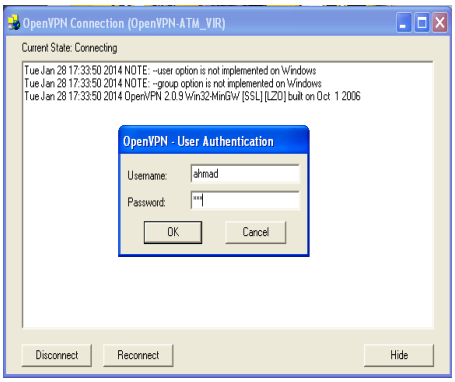
Pengujian jaringan dilakukan untuk mengetahui apakah proses instalasi baik di *server* maupun di *client* sudah sesuai dengan yang diharapkan, yaitu dengan cara melakukan koneksi dari client ke server. Adapun langkah-langkahnya adalah sebagai berikut:

1. Klik kanak pada icon tray Open VPN kemudian pilih VPN server dan pilih “Connect”



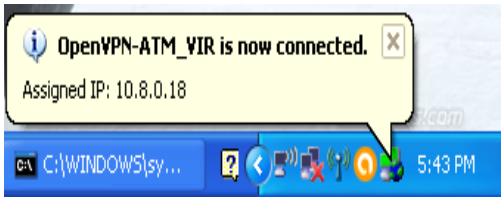
Gambar 3. Proses Koneksi VPN
Sumber Hasil Penelitian

2. Maka adakn tampil form untuk login sebagai otentikasi yang di berikan RADIUS server untuk bisa mengakses VPN



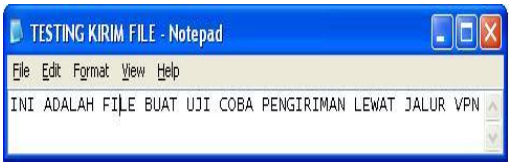
Gambar 3. Form Login VPN
Sumber Hasil Penelitan

3. Jika berhasil akan ditampil seperti gambar berikut



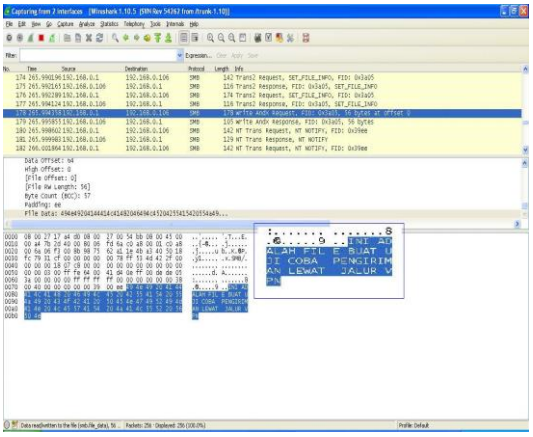
Gambar 3 Client Terkoneksi Ke server
Sumber Hasil Penelitian

Terlihat pada gambar, ketika *client* telah mendapat otentikasi dan otorisasi dari RADIUS *server* maka client mendapatkan ip address otomatis dari server VPN
Ketika komputer dikonfigurasi sebagai server VPN dan akan di jalankan maka komputer tersebut akan mendapatkan satu *buah virtual interface network* baik model TUN maupun TAP yang digunakan sebagai jalur khusus untuk komunikasi antar server dengan *client* VPN atau sebaliknya Virtual interface tersebut akan menghasilkan *ip address* baru yang dapat dikonfigurasi pada file *server conf* di komputer server VPN
Pada saat pengujian dilakukan komunikasi data tidak melalui virtual interface dari VPN, artinya komunikasi data dilakukan tanpa menjalankan server VPN. Pada pengujian ini akan dilakukan pengirimkan data dari client ke server dan dengan bantuan software wireshark akan dilakukan snifing terhadap data yang dikirimkan tersebut. Pertama tama dibuat satu buah file dengan format txt dan akan diberi nama " TESTING KIRIM FILE.txt.



Gambar 3 File Uji Coba
Sumber hasl penelitian

File tersebut akan dikirim dari client ke server melalui file sharing samba, kemudian dilakukan sniffing dengan software wireshart terhadap data yang dikirm tersebut



Gamber 3 Sniffing Data Tanpa VPN
Sumber Hasil Penelitian

Terlihat bahwa data yang dikirimkan masih bisa dibaca, artinya data tersebut tidak ada proses enkripsi dan sangat tidak aman apabila file tersebut merupakan file penting kemudian diakses oleh orang yang tidak bertanggung jawab.
Percobaab berikutnya adalah mengirimkan file denga ukuran cukup besar meluli email, seperti yang biasa dilakukan oleh user

Gambar 3. File Uji Coba Ukuran Besar
Sumber Hasil Penelitian

Maka yang terjadi adalah penyedia layanan email seperti yahoo dan gmail tidak bisa melakukan pengiriman data tersebut karena kapasitas dari file yang dikirimkan terlalu besar. Hal ini akan menjadi masalah jika data tersebut adalah penting dan harus segera dikirimkan

Gambar 3 Konfirmasi dari Yahoo Mail
Sumber Hasil Penelitian

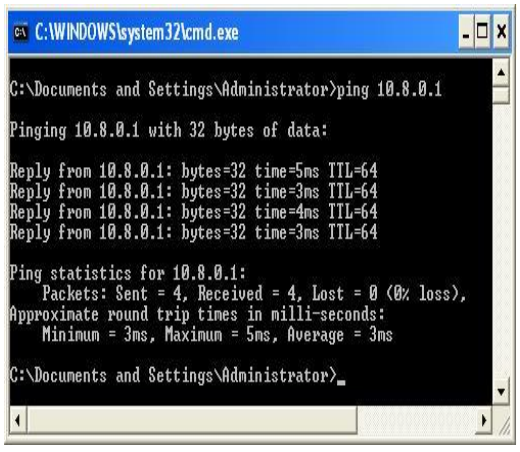
Gambar 3. Konfigurasi dari Gmail
Sumber hasil penelitian

Pada pengujian implementasi VPN ini juga akan dilakukan beberapa parameter pengujian yaitu :

Pengujian Kokentivitas

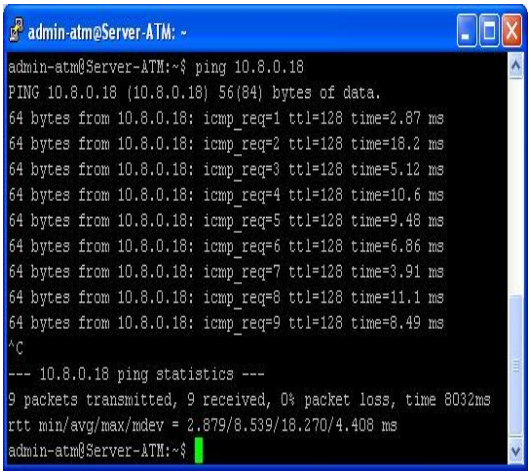
1. Pengiriman paket ping dan client ke server

Dilakukan dengan cara membuka commend promt pada komputer client kemudaian melakukan ping terhadap ip address server yaitu ip address yang di konfigurasi pada file server conf di OpenVPN server yaitu 10.8.0.1



Gambar 3. Ping dari Client ke Server
Sumber Hasil Penelitian

2. Pengiriman paket ping dari server ke client

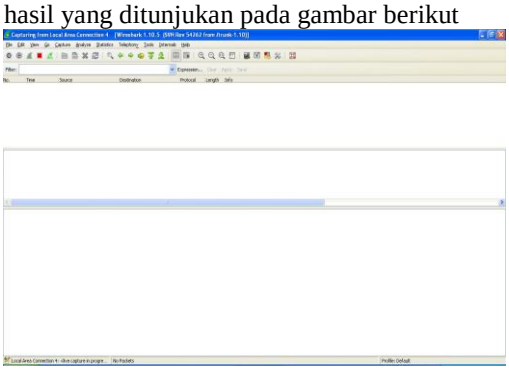


Gambar 3. Ping dari Server ke Client
Sumber Hasil Penelitian

Terlihat pada gambar antara client dengan server sudah terhubung dengan baik ditandai dengan respon repply dari kedua sisi

Penguji Keamanan

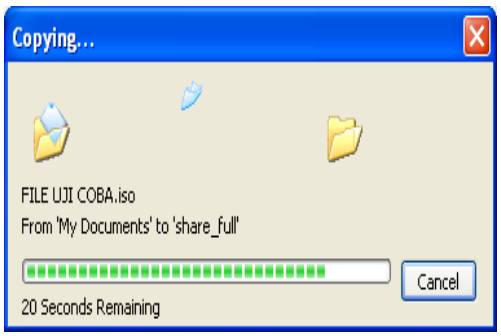
Posedur yang dilakukan dama dengan pengujian pada tahap awal yaitu dilakukan pengiriman data dari client ke server, kemudaian dilakukan sniffing terhadap paket data yang dikirim tersebut dengan hasil yang ditunjukan pada gambar berikut



Gambar 3 Sniffing Data Pada Koneksi VPN
Sumber hasil penelitian

Terlihat perbedaan yang cukup besar yaitu ketika *sniffing* dilakukan tanpa adanya koneksi VPN dengan koneksi menggunakan VPN. Paket data yang dikirim karena sudah melalui jalur *tunneling* dan proses enkripsi, maka ketika di ambil *capture* terlihat seperti tidak ada aktifitas yang dilakukan antara *client* dengan *server*. Hal ini menunjukan VPN memberikan konektifitas yang aman dalam hal pertukaran data dan informasi.

Pengujian Kecepatan Tranfer Data

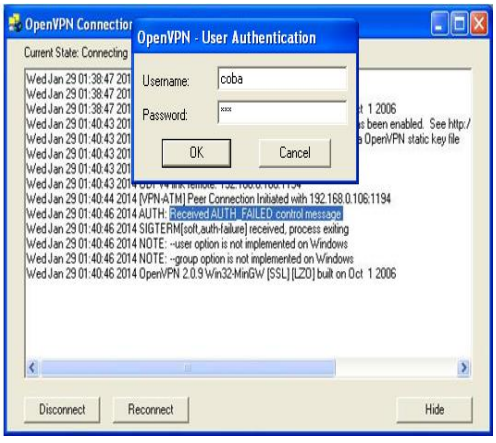


Gambar 3. Proses Transfer Data
Sumber pengolahan data

Jalur VPN ini memberikan keleluasaan dalam hal pengiriman data seperti layaknya berada dalam jaringan lokal. Sehingga dapat membantu memecahkan masalah dalam hal pertukaran data.

Uji Privasi dan Hak Akses

Pada perancangan jaringan VPN ini, ditambahkan juga modul untuk otentikasi menggunakan RADIUS *server*. Sehingga tidak begitu saja semua orang bisa masuk kejaringan. RADIUS *server* memberikan kemudahan dalam mengatur hak akses siapa saja yang bisa bergabung dan siapa saja yang tidak bisa.
Ketika ada user yang mencoba untuk masuk kejaringan VPN, maka sistem akan langsung menolaknya. Hal tersebut terjadi karena *user* tersebut belum terdaftar sebagai *user* yang di perbolehkan masuk ke jaringan VPN.



Gambar 3.
Sumber Hasil Penelitian

KESIMPULAN

Pada penelitian yang dilakukan terdapat beberapa kesimpulan yang dapat diambil, diantaranya sebagai berkut:

1. VPN merupakan solusi aman dalam hal pertukaran data yang menggunakan jalur publik.
2. Hasil *sniffing* menunjukan bahwa data yang ditransmisikan melalui jalur VPN tidak dapat terdeteksi, sehingga seolah-olah tidak ada aktifitas pada jaringan tersebut.
3. Dengan di implementasikannya VPN, akan memberikan kemudahan dalam transfer data karena tidak terbatas seberapa besar data yang akan di transmisikan. Berbeda dengan transfer data melalui email yang mempunyai keterbatasan..
4. RADIUS server memberikan kemudahan dalam mengatur otentikasi pada *user*¸ sehingga hanya user yang terdaftar saja yang bisa terhubung ke jaringan VPN.

Adapun saran yang dapat diberikan pada PT. Anugerah Tunggal Mandiri antara lain:

1. Aktifitas pertukaran data dan informasi yang dilakukan antar cabang yang selama ini masih menggunakan cara-cara manual, disarankan beralih menggunakan teknologi VPN untuk mencegah kebocoran data selama proses pertukaran informasi melalui jalur publik.
2. Informasi yang di kirimkan dari pusat ke cabang atau sebaliknya terkadang mengandung informasi yang sangat sensitif, penggunaan VPN akan memberikan rasa aman karena informasi yang dikirimkan melalui jalur VPN tidak akan terdeteksi oleh proses *sniffing* sekalipun.
3. Penggunaan *email*, *fax* atau cara yang lain dalam pengiriman data terutama data yang besar selain faktor kurang aman juga terkendala akan keterbatasan ukuran data yang dapat dikirimkan. Maka untuk mengatasi permasalahan tersebut penggunaan teknologi VPN merupakan salah satu solusi yang dapat diterapkan pada perusahaan.
4. Terdapat banyak *user* pada perusahaan yang dapat dengan mudah mengakses jaringan baik lokal maupun internet, hal ini menjadi suatu masalah bagi administrator jaringan dalam mengelola *user-user* tersebut. Terutama pengelolaan terhadap *user* siapa saja yang boleh mengakses dan tidak terhadap jaringan tersebut. penambahan modul *Remote Authentication Dial-In User Service* (RADIUS) pada jaringan

VPN akan memberikan kemudahan dalam mengelola *user-user* tersebut.

DAFTAR PUSTAKA

Aditya, Alan Nur. 2011. Mahir Membuat Jaringan Otodidak. Jakarta. Dunia Komputer

Feilner, Markus. 2006. OpenVPN *Building and Integrating Virtual Private Networks*. Birmingham. Packt Publishing

Hendriana, Yana. 2012. Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Studi Kasus pada CV. Pangestu Jaya). Yogyakarta: Jurnal Teknologi, Volume 5, Nomor 2 Desember 2012: 132-142

Kuswayatno, Lia. 2005. Mahir Dan Terampil Berkomputer. Bandung. Grafindo Media Pratama

Prihanto, Agus. 2010. Membangun Radius Server Untuk Keamanan Wifi Kampus. ISSN: 2088-2130. Surabaya: Jurnal Simantec, Volume 1, Nomor 3 Desember 2010: 230-235

Sahari. 2008. Perancangan Dan Implementasi Virtual Private Network (VPN) Pada Jaringan Nirkabel (Studi Kasus: UPI-YPTK Padang). ISSN: 1858 3709. Padang: Poli Rekayasa, Volume 4, Nomor 1 Oktober 2008: 48 55

Sugeng, Winarno. 2005. Instalasi Wireless LAN. Bandung. Informatika Bandung

Wendy, Aris dan Ahmad Ramadhana. 2005. Membangun VPN Linux Secara Cepat. Jakarta. Andi Publisher