BAB III
PEMBAHASAN

3.1 Analisis

Analisis adalah pembagian suatu masalah menjadi komponen – komponen yang lebih kecil untuk mengidentifikasi dan mengevaluasi masalah dan hambatan yang ditemui, dan kebutuhan yang diharapkan sehingga nantinya dapat diusulkan perbaikan-perbaikannya. Bab ini menguraikan proses analisis pembangunan VPN dan perancangan dan implementasi VPN sistem. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan–kebutuhan pokok sitem VPN yang akan dibangun.

3.1.1 Analisis Masalah

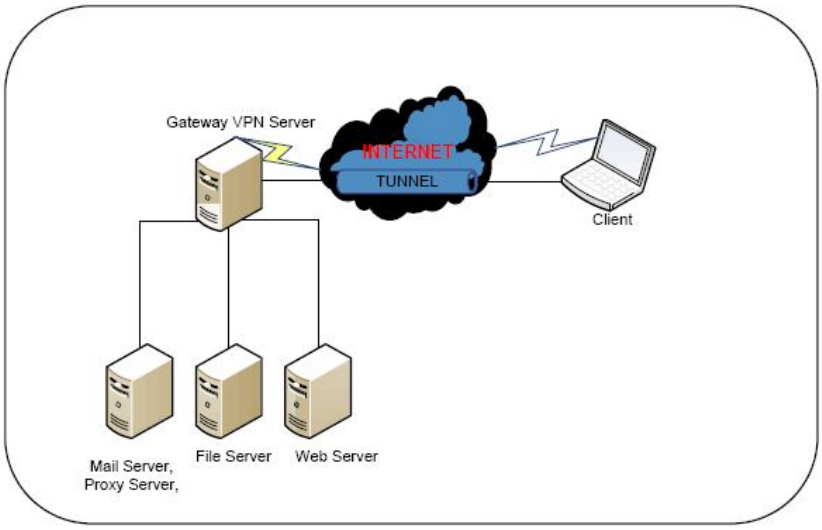
Di Dinas Permukiman dan Perumahan, data hanya tersimpan di kantor saja dan hanya dapat diakses dengan jaringan internal. Staff yang di tugaskan ke luar kota kadang lupa membawa data dari kantornya sehingga dapat menghambat pekerjaan. Rekan kantor yang bertugas diluar kantor juga harus datang langsung ke kantor untuk mengambil data sehingga proses pekerjaan membutuhkan waktu yang lama. Komunikasi data di Diskimrum dilakukan dengan media email kalau staff atau rekan kantor tidak berada di kantor. Hal ini, belum tentu data yang dikirim akan sampai dengan aman dan utuh. Kerahasiaan data tersebut juga belum tentu terjaga.

Solusi yang diusulkan untuk mempermudah berkomunikasi data di Dinas Permukiman dan Perumahan adalah dengan diterapkannya security VPN. VPN (*Virtual Private Net work*) memungkinkan terbentuknya sebuah jaringan data *private* pada jaringan publik dengan menerapkan autentikasi dan enkripsi sehingga akses terhadap jaringan tersebut hanya dapat dilakukan oleh pihak-pihak tertentu. Sistem ini menjadikan komunikasi data yang aman dapat dilakukan dimana saja dan kapan saja. VPN merupakan sebuah teknologi komunikasi yang memungkinkan terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal. Dengan

menggunakan jaringan publik ini, dapat tergabung dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti ketika berada di kantor.

VPN adalah singkatan dari *virtual private network*, yaitu jaringan pribadi (bukan untuk akses umum) dengan internet untuk menghubungkan antar jaringan komputer secara aman. Perlu digunakan teknologi tertentu untuk menggunakan medium yang umum, agar 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 komputer.

Biasanya VPN digunakan oleh pegawai yang ingin terhubung ke jaringan lokal perusahaannya dari berbagai lokasi yang jauh. Biasanya perusahaan bekerja sama dengan *enterprise service provider* (ESP) untuk membangun jaringan vpn ini. Kemudian ESP akan memberikan *network access server* (NAS) bagi perusahaan tersebut. Selain itu ESP akan menyediakan *software client* 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 client*, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.



Gambar 3.1. Remote Access VPN secara umum

Pegawai perusahaan yang berada 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. Akan tetapi kebutuhan akan tingkat keamanan data yang tinggi dan solusi membangun keamanan jaringan yang handal yang tidak mengeluarkan dana tidak begitu besar masih sangat mungkin dilakukan. Oleh karena itu bagaimana membangun suatu jaringan VPN dengan tidak banyak mengeluarkan dana yang besar, maka dapat dilakukan konfigurasi VPN pada tingkat sistem operasi, dengan tetap mempunyai kehandalan dalam keamanan.

3.1.2 Keuntungan Pembangunan VPN

Ada beberapa keuntungan yang dapat diperoleh Dinas Permukiman dan Perumahan dengan menggunakan VPN.

1. Jangkauan jaringan lokal yang dimiliki perusahaan akan menjadi luas. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal juga semakin cepat karena proses instalasi infrastruktur jaringan dilakukan di kantor Dinas Permukiman dan Perumahan dengan ISP terdekat. Dengan demikian, penggunaan VPN secara tidak langsung akan meningkatkan efektifitas dan efisiensi kerja.
2. VPN memberi kemudahan untuk mengakses data, program aplikasi, mail intranet yang ada di Dinas Permukiman dan Perumahan dari mana saja karena VPN terhubung ke internet, sehingga pegawai yang kebetulan bertugas diluar kantor dapat mengakses jaringan khusus perusahaan di mana pun dia berada. Selama dia bisa mendapatkan akses ke internet atau ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan.

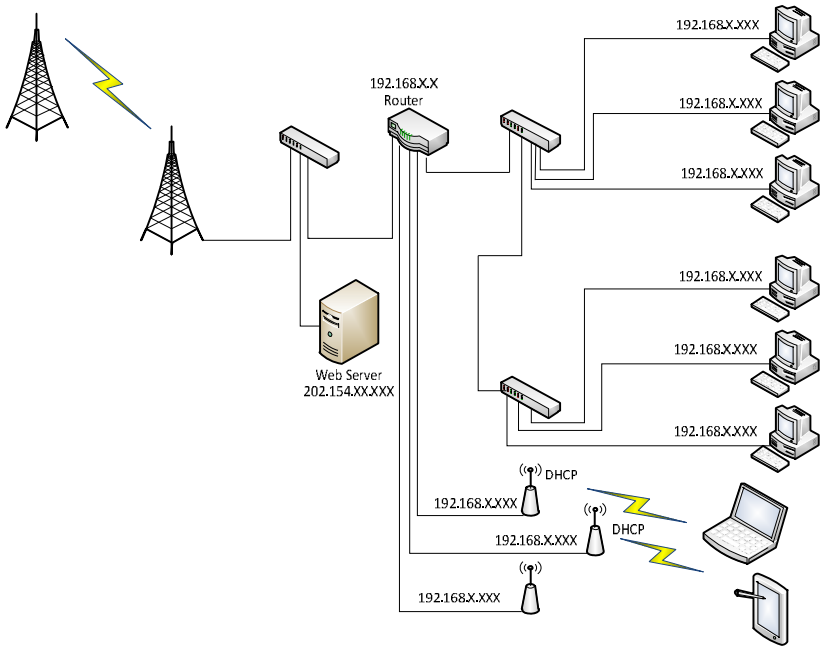
Sebelum melakukan pembangunan VPN di PT Dinas Permukiman dan Perumahan, akan diuraikan proses pembangunan sistem VPN dan perancangan dengan langkah-langkah sebagai berikut.

1. Analisis topologi jaringan.
2. Analisis kebutuhan sistem VPN.

3. Analisis kebutuhan *server* mencakup *software* dan *hardware* untuk implementasi VPN.
4. Analisis kebutuhan *client* mencakup *software* dan *hardware.*
5. Analisis Pengguna.
6. Perancangan sistem VPN.

3.2 Analisis Topologi

Topologi jaringan merupakan tata letak serta struktur hubungan antara komponen-komponen (node) dalam suatu jaringan. Topologi jaringan berkaitan dengan mekanisme yang digunakan untuk mengelola cara station (komputer) dalam mengakses jaringan, sehingga tidak terjadi konflik. Berikut ini adalah topologi jaringan yang sedang berjalan di Dinas Permukiman dan Perumahan.



Gambar 3.2. Topologi Jaringan yang sedang berjalan.

3.2.1 Pengalamatan IP Dinas Permukiman dan Perumahan

Pengalamatan IP di jaringan Dinas Permukiman dan Perumahan menggunakan IP *dynamic* berdasarkan DHCP *server*. Dimana setiap *client/user* yang

sudah terdaftar atau memperoleh IP dari server dicatat *macaddressnya* oleh *server* supaya IP yang diperoleh tidak berubah lagi.

Range IP address yang dipakai oleh user antara – sedangkan *IP address* dibawah dipakai sebagian oleh *server* diantaranya:

1. *IP address* 10.88.1.1 di pakai oleh *server* windows 2003 server dimana di dalam windows 2003 server terdiri dari DHCP *server*, DNS *server, Activ directory server* (*Domain Contoller*), *File server*, dan *Data base Server*.
2. *IP address* 10.88.1.15 dipakai sebagai router dimana didalam router tersebut terdiri dari *gateway server* dan *proxy server*
3. *IP address* 10.88.1.4 digunakan untuk *email server*
4. *IP address* 10.88.1.9 digunakan untuk mikrotik VPN *server*

3.2.2 Server Dinas Permukiman dan Perumahan

Dalam jaringan di Dinas Permukiman dan Perumahan terdapat beberapa server yang berbeda fungsi dan kegunaanya. Server yang ada diantaranya adalah.

1. Diskimrum Server

Menggunakan Linux Ubuntu 11.04 mempunyai alamat IP 202.154.42.132 berfungsi sebagai :

a. DHCP Server

DHCP server merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti Windows NT Server, Windows 2000 Server, Windows Server 2003, atau GNU/Linux memiliki layanan seperti ini

b. DNS Server

DNS (***Domain Name System)***, adalah sebuah sistem yang menyimpan informasi tentang nama *host* maupun nama *domain* dalam bentuk basis data tersebar (*distributed database*) di dalam jaringan komputer, DNS menyediakan servis yang cukup penting untuk internet, karena penggunaan perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan

pengalamatan dan penjaluran (*routing*)kurang optimal. Oleh karena itu, pada umumnya *user* lebih memilih menggunakan nama *host* dan nama *domain*.

c. Active Directory

Microsoft Windows Server 2003 tidak akan bekerja maksimal apabila *Active Directory* belum diinstalasi. Semua yang berhubungan dengan services dan domain ada dalam *Active Directory* ini.

d. File Server

Menyediakan layanan berupa pengelolaan dan pengaksesan *file*

e. Data Base Server

Menyediakan ruang *(space)* untuk penyimpanan data

2. Router Server

Menggunakan system operasi Mikrotik dan mempunyai alamat IP 202.154.42.145 yang berfungsi sebagai:

a. *Gateway Server*

b. *Proxy Server*

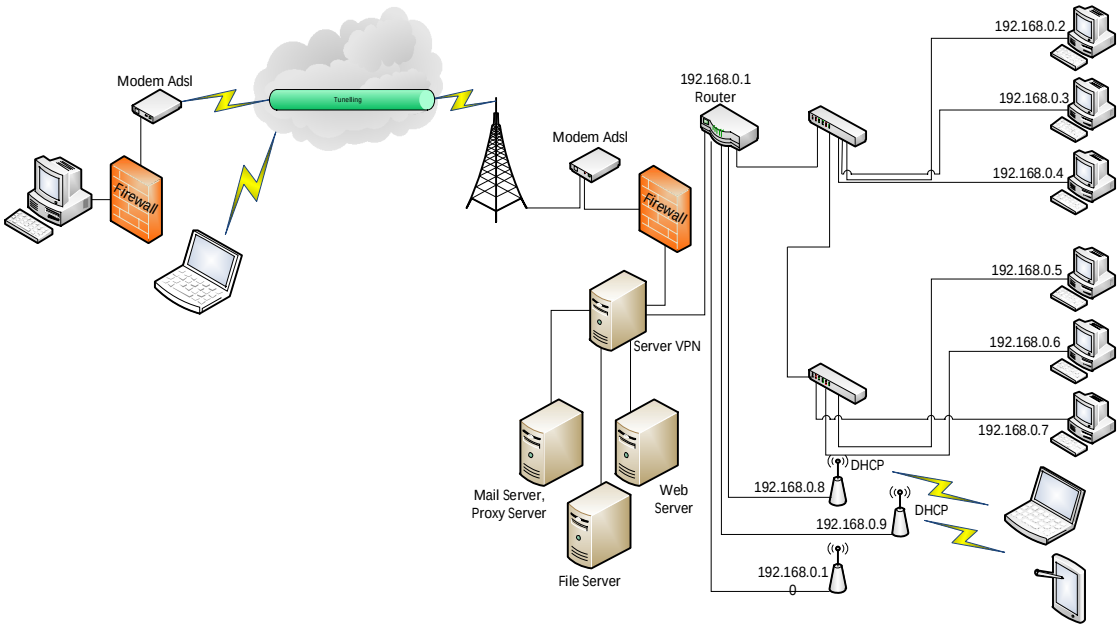
3.3 Analisis Kebutuhan Sistem VPN

VPN memberikan keamanan serta *reliabilitas* yang sama seperti jaringan *private*. Oleh karena itu, pengguna VPN dapat mengakses *Local Area Network* suatu perusahaan atau organisasi dengan mengunakan jaringan *internet*.

VPN menjamin keamanan karena koneksi yang dilakukan oleh VPN menggunakan peranti yang menerapkan metode autentikasi, serta data yang dikirimkan dienkripsi.

3.3.1 Tipe Jaringan VPN

Model topologi jaringan Remote Access Virtual Private Network yang umum digunakan biasanya terdiri dari sebuah komputer sebagai server VPN, server pendukung lain seperti web server, file server, dan server-server yang lain dan komputer client dengan bentuk topologi seperti pada gambar berikut:



Gambar 3.3. Topologi Jaringan VPN

Pada skema diatas, client akan melakukan remote access terhadap layanan-layanan yang terdapat pada server. Dimana client memerlukan untuk mengakses file yang memerlukan koneksi langsung ke server. Sebelum client dapat mengakses file maupun layanan-layanan yang terdapat pada server jaringan lokal, client membuat koneksi dengan sebuah VPN Server sebagai mekanisme kemananan komunikasi data, untuk menjaga keamanan data pada saat koneksi dengan server, kemudian pada VPN Server akan melakukan forwading kepada layanan yang diinginkan oleh client, kemudian layanan yang diinginkan oleh client yang telah terkoneksi vpn akan me-reply layanan yang diinginkan tersebut. Dengan menggunakan koneksi VPN untuk mengakses layanan yang terdapat pada jaringan lokal, koneksi dari client ke server dapat dilakukan dengan aman.

Client dapat mengakses server-server seperti file server, web server, dan server-server yang lain setelah client melakukan koneksi melalui vpn, sehingga pengaksesan server-server tersebut dilakukan melalui network interface vpn, sehingga pengaksesan data dari server dapat dilakukan dengan aman.

3.3.2 Bandwidth

Bandwidth adalah besaran yang menunjukkan banyaknya data yang dapat dilewatkan disuatu saluran komunikasi pada *network* dalam satuan waktu tertentu. Dalam perancangan VPN, *Bandwidth* sangat perlu diperhitungkan karena kecepatan transfer *file* tergantung pada *bandwidth* yang kita gunakan. Jenis *Bandwidth* ini biasanya diukur dalam bps (*bits per second*). Perancangan pembangunan VPN Dinas Permukiman dan Perumahan menggunakan *Internet Service Provider* (ISP) Radnet.

Dinas Permukiman dan Perumahan kurang lebih memiliki 50 client (komputer), dengan menggunakan kapasitas bandwidth sebesar 512 Mbps. Jaringan Dinas Permukiman dan Perumahan menggunakan IP Public 202.154.xx.xxx, IP Public tersebut dapat dimanfaatkan sebagai Web Server, akses VPN, Remote Server, Dll. sedangkan pada sisi client menggunakan IP Address 192.168.x.xxx dimana IP Address tersebut tergolong pada IP kelas C yang umum digunakan untuk skala kecil seperti LAN.

3.4 Analisis Kebutuhan Server VPN

Perancangan sistem VPN di Dinas Permukiman dan Perumahan membutuhkan sebuah server VPN. Analisis kebutuhan server mencakup *hardware* dan *software* untuk implementasi VPN.

3.4.1 Perangkat Keras

Spesifikasi perangkat keras yang digunakan sebagai komputer server memiliki spesifikasi sebagai berikut :

a. Procesor : Intel P4 2,4 GHz
b. RAM : 512 Mb DDR2
c. VGA : Onboard
d. Ethernet : - Onboard
   : - DFE-528 TX Ethernet
   : - DFE-528 TX Ethernet
e. HDD : ATA 40 Gb

f. Monitor : LG 710S
g. Keyboard : Standar
h. Mouse : Optic standar
i. Optical disc : CD Room

3.4.2 Perangkat Lunak

Spesifikasi perangkat lunak yang digunakan pada server adalah Linux Distro Ubuntu 11.10 sebagai server VPN. Sedangkan software pendukung yang digunakan pada laporan ini meliputi openvpn, tcpdump, nmap dan wireshark.

a. Openvpn

Openvpn adalah salah satu aplikasi VPN berbasiskan *open source* untuk membuat koneksi *encrypted tunnels* secara *virtual* dengan menggunakan autentikasi dengan yang lainnya menggunakan *pre-shared secret key*, *certificates*, atau *username* OpenVPN memiliki beberapa kelebihan untuk membuat VPN *server* seperti berbasiskan *open source*, keamanan, kestabilan, mekanisme *autentikasi* dan *enkripsi*.

b. TCP DUMP

TCPdump adalah tools yang berfungsi meng*capture*, membaca atau men*dump*ing paket yang sedang ditransmisikan melalui jalur TCP. TCPdump diciptakan untuk menolong programmer ataupun administrator dalam menganalisa dan *troubleshooting* aplikasi *networking*. Seperti pisau yang bermata dua, TCPdump bisa digunakan untuk bertahan dan juga bisa digunakan untuk menyerang.

TCPDump seringkali digunakan oleh para cracker untuk melaksanakan perkerjaannya, karena TCPdump bisa meng-*capture* atau men-*sniff* semua paket yang diterima oleh *network interface*. Sebagai contoh, digunakan *network* yang terdiri dari tiga komputer yang dihubungkan menggunakan *hub*. Komputer pertama, menggunakan sistem operasi Windows XP dengan IP *address* 192.0.0.1, sedang melakukan koneksi melalui telnet ke komputer kedua yang menggunakan Slackware 8.0 dengan IP *address* 192.168.0.2 dan *host* ketiga

komputer Redhat 7.1 dengan IP *address* 192.168.0.3 yang menggunakan *utility* TCPdump. Alasan untuk membedakan *Operating System* yang digunakan adalah untuk menunjukkan bahwa TCP/IP dapat berkomunikasi dengan baik pada dua platform yang berbeda.

Untuk menjalankan TCPdump, ketik perintah tcpdump di *console* pada *host* 192.168.0.3 sebagai root. *Output* yang diperlihatkan di bawah ini adalah *output* yang bergulir *non-stop*, terus berganti baris tanpa henti hingga menekan Ctrl+C (^C) untuk menghentikan *utility* ini.

c. NMAP

Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning, eksplorasi dan audit keamanan jaringan. Nmap dirancang untuk memeriksa jaringan besar secara cepat, meskipun dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan

d. Wireshark

Wireshark adalah program yang berfungsi untuk mengetahui kejadian yang terjadi pada saat kita melakukan interaksi pada suatu jaringan komputer. Wireshark merupakan salah satu network analysis tool, atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis, pengembangan software dan protokol, serta untuk keperluan edukasi.

Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam suatu jaringan yang dimonitor. Hampir semua jenis paket informasi dalam berbagai format protokol dapat ditangkap dan dianalisa.

3.5 Analisis Kebutuhan *Client*

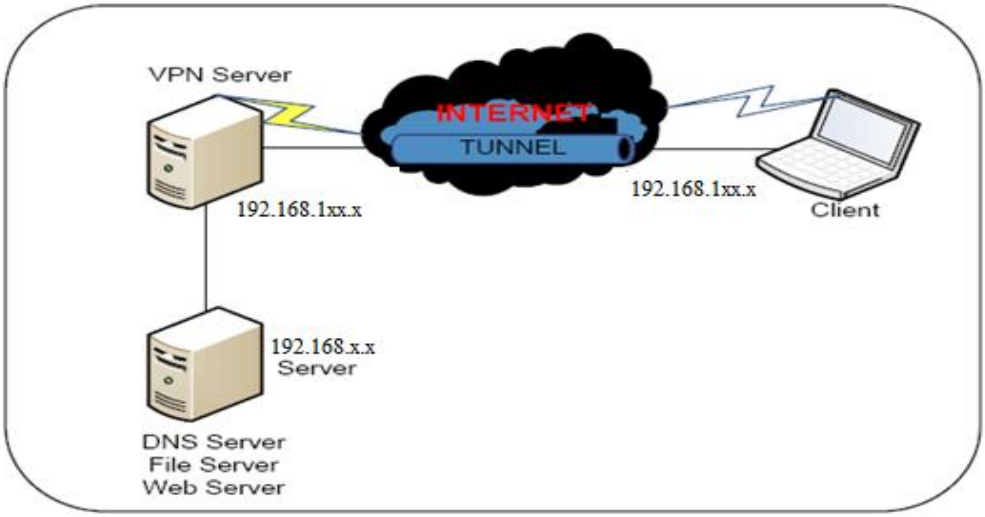
Perangkat yang bisa dipergunakan oleh *client* yaitu berupa komputer yang mempunyai koneksi jaringan dengan internet dan mempunya spesifikasi perangkat lunak sistem operasi berbasis windows.

3.6 Perancangan Sistem

Pada bagian ini akan dibahas mengenai perencanaan infrastruktur VPN, konfigurasi, dan instalasi dari perangkat keras maupun perangkat lunak yang dipergunakan pada jaringan untuk implementasi VPN tersebut. Infrastruktur yang mendukung untuk jaringan ini terdiri dari *server* dan *client* yang berupa PC, *hub*/*switch*, dan perangkat lunak pendukung.

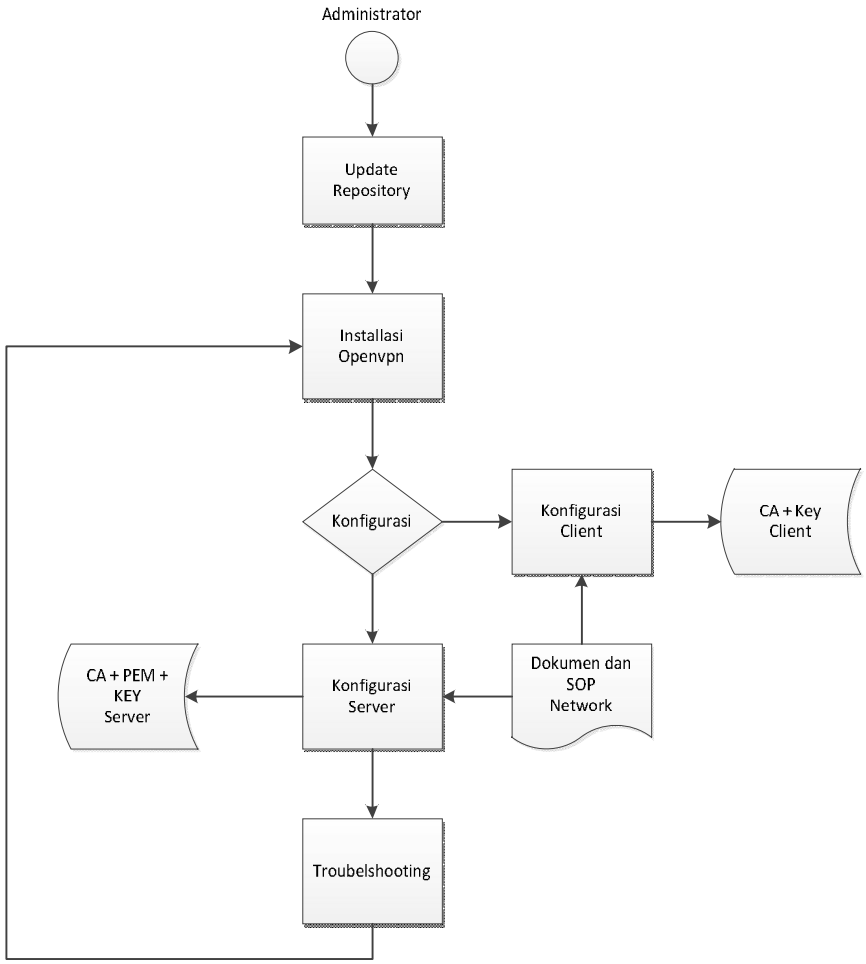
3.6.1 Arsitektur Simulasi

Perancangan Jaringan yang akan digunakan terdiri dari sebuah komputer sebagai *server* VPN, *server* dan komputer *client* dengan bentuk topologi seperti yang ditunjukan pada gambar 3.3:



Gambar 3.4. Gambar Arsitektur Simulasi

Berikut ini adalah langkah – langkah atau prosedur installasi dan konfigurasi openvpn :



Gambar 3.5. Prosedur Installasi dan Konfigurasi Openvpn

3.7 Implementasi

Tahap implementasi dilakukan berdasarkan analisis dan perancangan yang telah dibuat, yaitu mengkonfigurasi berdasarkan analisis dan perancangan. Setelah implementasi selesai dilakukan, maka akan dilakukan pengujian terhadap *Remote Access Virtual Private Network* berbasis SSL yang telah dibangun.

3.7.1 Konfigurasi VPN *Server*

Pada VPN *Server* digunakan sistem operasi Linux Ubuntu 11.04. Sebelum mengkonfigurasi VPN *Server*, sangat penting untuk mengcopikan berbagai script dan dokumentasi yang dibutuhkan untuk konfigurasi ke folder /etc/openvpn/, dikarenakan pada folder /etc/openvpn merupakan folder untuk inialisasi file konfigurasi dari openvpn

```
#cp –R /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn
```

Dekompress file server.conf.gz yang berada di folder /usr/share/doc/openvpn/examples/sample-config-files/ ke folder /etc/openvpn/. File server.conf digunakan sebagai file eksekusi yang menandakan bahwa komputer tersebut merupakan vpn *server*.

```
#gzip –d /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
/etc/openvpn/
```

Sebelum mengkonfigurasi Remote Access Virtual Private Network melalui software openvpn yang berbasis SSL, file openssl.cnf harus disesuaikan dengan kebutuhan yang akan digunakan, openssl.cnf dibutuhkan konfigurasi untuk menentukan besar bits yang akan dienkripsi, masa validasi dan jenis enkripsi yang akan digunakan pada koneksi remote access VPN.

File openssl.cnf merupakan file konfigurasi yang berbasis SSL yang digunakan oleh file-file konfigurasi yang lain sebagai parameternya. Openssl.cnf yang terdapat di direktori /usr/share/doc/openvpn/examples/easy-rsa/2.0/openssl.cnf Pada file openssl.cnf untuk menentukan besar bits yang akan di enkripsi, masa validasi dan jenis enkripsi yang akan digunakan dari koneksi *remote access* VPN terdapat pada bagian seperti yang ditunjukkan Tabel 4.2 di bawah ini:

Tabel 3.1 Parameter Openssl Yang Dibutuhkan

Parameter	**Keterangan**
Default_days = 3650	Untuk menentukan lama aktif dari sertifikat dan kunci yang digunakan
Default_crl_days = 30	Untuk menentukan lama aktif dari crl yang digunakan
Default_md = **md5**	Jenis enkripsi yang akan digunakan
Preserve = no	

File konfigurasi yang paling dasar dalam openvpn adalah vars, yang berisi informasi penting openvpn yang akan dibuat, dalam hal ini openvpn akan dikonfigurasi menggunakan easy-rsa (sertifikat digital yang menggunakan konfigurasi dari openssl.cnf). Parameter vars yang dibutuhkan antara lain:

Tabel 3.2 Key Konfigurasi Vars

Kunci	**Keterangan**
export KEY_SIZE=1024	Ukuran kunci yang akan dibuat (dalam bit)
export KEY_COUNTRY="ID"	Informasi identitas negara
export KEY_PROVINCE="JB"	Informasi identitas provinsi
export KEY_CITY="Bandung"	Informasi identitas kota
export KEY_ORG="Learner"	Informasin identitas organisasi
export KEY_EMAIL="diskimrum@gmail.com"	Informasi identitas email

Apabila file vars telah dikonfigurasi, maka file vars dapat dijalankan untuk menginialisasi pembuatan sertifikat dan kunci yang dibutuhkan.

```
#cd /etc/openvpn/
#. ./vars
#./clean-all
```

Perintah clean-all akan menghapus semua konfgurasi lama yang pernah dibuat pada folder keys.

Implementasi pada skripsi akan menggunakan 3 jenis kunci, kunci dan sertifikat ini merupakan implementasi dari konsep Asymmetric Encription dari SSL, dimana kunci dan key akan bertindak sebagai kunci dan kunci privat pada komputer server dan komputer client yang akan terkoneksi melalui remote access VPN, kunci dan sertifikat tersebut yaitu: CA (Certificate Authority), Key, dan Kunci DH (Diffie-Hellman). CA (Certificate Authority) merupakan sertifikat yang digunakan untuk authentikasi yang menandakan bahwa itu berasal dari server yang sah. CA dapat dibuat dengan perintah:

```
#./build-ca
```

Proses pembuatan CA akan mengeneralisasi informasi-informasi yang dibutuhkan, seperti yang ditunjukan pada hasil proses pembuatan CA di bawah ini:

```
root@kimrum-asus:/etc/openvpn# ./build-ca
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JABAR]:
```

```
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [DISKIMRUM]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [DISKIMRUM CA]:
Name []:
Email Address [diskimrum.jabar@gmail.com]:
```

Pada proses pembuatan CA, akan diminta konfirmasi terhadap bagian seperti yang ditunjukkan dibawah ini:

```
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JABAR]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [DISKIMRUM]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [DISKIMRUM CA]:
Name []:
Email Address [diskimrum.jabar@gmail.com]:
```

Bagian diatas merupakan hal yang diubah pada file vars sebelumnya, yaitu Country Name, State or Province, Locality Name, Organization Name, Organizational Unit Name, Common Name, Name, dan Email Address, apabila informasi-informasi tersebut telah sesuai, maka tidak perlu untuk mengisi ulang informasi tersebut. Akan tetapi apabila informasi terdapat kesalahan, maka dapat mengisi ulang dengan informasi yang benar dan sesuai.

Proses pembuatan kunci(key), terdapat 2 jenis, yaitu kunci untuk server dan kunci untuk client, kunci untuk server hanya diperbolehkan mempunyai satu kunci, sedangkan kunci client dapat dibuat lebih dari satu. Kunci server maupun kunci client merupakan kunci private asymmetric encryption yang harus dimiliki oleh server maupun client. Kunci pada client merupakan sinkronisasi dari kunci server yang terdapat pada komputer vpn server, dan menandakan bahwa client tersebut

merupakan client dari vpn server tersebut. Kunci server dapat dibuat dengan menggunakan perintah:

```
#. Build-key-server server
```

Proses pembuatan kunci akan mengeneralisasi informasi yang dibutuhkan, seperti yang ditunjukan pada hasil proses pembuatan kunci di bawah ini:

```
root@kimrum-asus:/etc/openvpn# ./build-key-server server
Generating a 1024 bit RSA private key
.............++++++
.......++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JABAR]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [DISKIMRUM]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [diskimrum.jabar@gmail.com]:


Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JABAR'
localityName          :PRINTABLE:'Bandung'
organizationName      :PRINTABLE:'DISKIMRUM'
commonName            :PRINTABLE:'server'
emailAddress          :IA5STRING:'diskimrum.jabar@gmail.com'
Certificate is to be certified until Jan 13 14:31:34 2022 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Pada proses pembuatan kunci untuk server, menunjukkan bahwa kunci server dibuat dengan menggunakan parameter-parameter yang berasal dari file openssl.cnf yang berbasis SSL.

(Using configuration from /etc/openvpn/openssl.cnf)

Pada proses pembuatan kunci untuk server, akan diminta konfirmasi terhadap bagian seperti yang ditunjukkan dibawah ini:

```
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JABAR]:
```

```
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [DISKIMRUM]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [diskimrum.jabar@gmail.com]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Bagian diatas merupakan hal yang diubah pada file vars sebelumnya, yaitu Country Name, State or Province, Locality Name, Organization Name, Organizational Unit Name, Common Name, Name, dan Email Address, apabila informasi tersebut telah sesuai, maka tidak perlu untuk mengisi ulang informasi tersebut. Akan tetapi apabila informasi terdapat kesalahan, maka dapat mengisi ulang dengan informasi yang benar dan sesuai. Dengan tambahan yang akan dimasukan sebagai atribut ekstra yaitu: A Challenge Password dan optional Company Name maka hanya mengkonfirmasikan dan apabila diperlukan untuk mengisi dari atribut ekstra yang akan dimasukan. Dan generalisasi kunci menggunakan konfigurasi dari file openssl.cnf.

Setelah proses pembuatan kunci server, kunci server maka akan terdapat file sertifikat server pada folder /etc/openvpn/keys.

- 01.pem
- ca.key
- server.crt
- server.key
- ca.crt
- server.csr

Sedangkan untuk pembuatan kunci untuk client yang akan dikoneksikan dengan VPN server, kunci untuk client diberi nama client1.

```
#. Build-key client1
```

Sama halnya dengan proses pembuatan kunci pada server, proses pembuatan kunci pada client akan mengeneralisasi informasi-informasi yang dibutuhkan, seperti yang ditunjukan pada hasil proses pembuatan kunci di bawah ini:

```
root@kimrum-asus:/etc/openvpn# . build-key client1
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JABAR]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [DISKIMRUM]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client1]:
Name []:
Email Address [diskimrum.jabar@gmail.com]:

Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
A challenge password []:12345
An optional company name []:
Using configuration from /etc/openvpn/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JABAR'
localityName          :PRINTABLE:'Bandung'
organizationName      :PRINTABLE:'DISKIMRUM'
commonName            :PRINTABLE:'client1'
emailAddress          :IA5STRING:'diskimrum.jabar@gmail.com'
Certificate is to be certified until Jan 13 14:37:51 2022 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Sama halnya dengan proses pembuatan kunci untuk server, Pada proses pembuatan kunci untuk client, menunjukkan bahwa kunci kunci dibuat dengan menggunakan parameter-parameter yang berasal dari file openssl.cnf yang berbasis SSL.

(Using configuration from /etc/openvpn/openssl.cnf)

Dan pada proses pembuatan kunci untuk, akan diminta konfirmasi terhadap bagian seperti yang ditunjukkan dibawah ini:

```
Country Name (2 letter code) [ID]:
```

```
State or Province Name (full name) [JABAR]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [DISKIMRUM]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client1]:
Name []:
Email Address [diskimrum.jabar@gmail.com]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Bagian diatas merupakan hal yang diubah pada file vars sebelumnya, yaitu Country Name, State or Province, Locality Name, Organization Name, Organizational Unit Name, Common Name, Name, dan Email Address, apabila informasi tersebut telah sesuai, maka tidak perlu untuk mengisi ulang informasi tersebut. Akan tetapi apabila informasi terdapat kesalahan, maka dapat mengisi ulang dengan informasi yang benar dan sesuai. Dengan tambahan yang akan dimasukan sebagai atribut ekstra yaitu: A Challenge Password dan Optional Company Name maka hanya mengkonfirmasikan dan apabila diperlukan untuk mengisi dari atribut ekstra yang akan dimasukan. Dan generalisasi kunci menggunakan konfigurasi dari file openssl.cnf.

Setelah pembuatan kunci client maka akan terdapat file sertifikat client pada folder /etc/openvpn/keys, yaitu client1.crt, client1.key, dan client1.csr.

```
-rw-r--r-- 1 root root 3843 2012-01-08 19:07 01.pem
-rw-r--r-- 1 root root 3727 2012-01-08 19:09 02.pem
-rw-r--r-- 1 root root 1200 2012-01-08 19:07 ca.crt
-rw------- 1 root root 887 2012-01-08 19:07 ca.key
-rw-r--r-- 1 root root 3727 2012-01-08 19:09 client.crt
```

```
-rw-r--r-- 1 root root 668 2012-01-08 19:09 client.csr
-rw------- 1 root root 887 2012-01-08 19:09 client.key
-rw-r--r-- 1 root root 207 2012-01-08 19:09 index.txt
-rw-r--r-- 1 root root 21 2012-01-08 19:09 index.txt.attr
-rw-r--r-- 1 root root 21 2012-01-08 19:07 index.txt.attr.old
-rw-r--r-- 1 root root 103 2012-01-08 19:07 index.txt.old
-rw-r--r-- 1 root root 3 2012-01-08  19:09 serial
-rw-r--r-- 1 root root 3 2012-01-08 19:07 serial.old
-rw-r--r-- 1 root root 0 2012-01-08 03:27 server.crt
-rw-r--r-- 1 root root 668 2012-01-08 03:27 server.csr
-rw------- 1 root root 887 2012-01-08 03:27 server.key
```

Kunci DH(Diffie-Hellman) merupakan metode enkripsi dengan algoritma kunci publik (public key distribution system), yang memungkinkan dua pihak yang tidak memiliki koneksi sebelumnya satu sama lain untuk dapat membentuk suatu kunci rahasia untuk menciptakan komunikasi yang aman.

```
#. /Build-dh
```

Setelah semua kunci telah terbentuk, maka server dapat dikonfigurasi dengan mengedit isi file server.conf yang berada di folder /etc/openvppn/server.conf

Tabel 3.3 Parameter Konfigurasi Server

Parameter	**Keterangan**
Server	Menunjukan sebagai *server*
Proto tcp	Protokol yang digunakan adalah tcp
Dev tap	“dev tun” akan menciptakan tunnel routing IP. “dev tap” akan menciptakan tunnel Ethernet.
Ca /etc/openvpn/keys/ca.crt	Sertifikat dan kunci-kunci yang

Cert /etc/openvpn/keys/server.crt Key /etc/openvpn/keys/server.key	digunakan *server* serta tempat beradanya sertifikat dan kunci tersebut
Dh /etc/openvpn/keys/dh1024.pem	Parameter Diffie-Hellman dan tempat beradanya parameter Diffie-Hellman
Server 10.10.10.0 255.255.255.0	Mode koonfigurasi *server* dan suplai dari subnet VPN. Dengan ditentukan parameter tersebut, maka IP *server* yaitu 10.10.0.1 dan sisanya adalah untuk *client*.
Ifconfig-pool-persist ipp.txt	Record perbaikan dari *client*.
Push “route 192.168.1.0 255.255.255.0”	Melakukan routing ke jaringan intranet dengan alamat 192.168.1.2/24 melalui alamat tunnel *server* 192.168.111.1
Client-to-client	Mengizinkan *client* agar dapat melihat satu sama lain
Keepalive 10 120	Menjaga agar pesan aktif antara pihak yang berhubungan dapat terjaga, dengan asumsi sistem akan ping selama 10 detik apabila pada jangka waktu 120 detik tidak diterima ping.
Comp-lzo	Meng-*enable*-kan kompresi pada jalur VPN
Max-clients	Jumlah *client* yang diizinkan
User nobody	Untuk mengurangi hak istimewa
Group nogroup	daemon openvpn
Persist-key Persist-tun	Berguna untuk menghindari mengakses sumber daya tertentu pada *restart* yang mungkin tidak dapat diakses lagi karena *downgrade* hak istimewa

Status /var/log/opnvpn-status.log	Log dari status koneksi vpn
Verb 4	Untuk penggunaan umum
Mute 10	Tidak mengulangi pesan. Maksimal 10 pesan dari kategori pesan yang sama akan menjadi output untuk log
Plugin /usr/lib/openvpn/openvpn-authpam.so login	Menggunakan plugin untuk authentifikasi *client*

3.7.2 Konfigurasi *Client* Windows

Konfigurasi client yang berbasis windows harus meng-copy-kan sertifikat dan kunci client yang telah dibuat dari server, yaitu ca.crt, client1.crt, client1.csr client1.key, simpan file tersebut di folder C:/ProgramFiles/openVPN/config dan sesuaikan file konfigurasi client.ovpn dengan file konfigurasi yang terdapat pada server dengan parameter yang ditunjukan Tabel 3.5 sebagai berikut:

Tabel 3.4 Parameter Konfigurasi Client Windows

Parameter	**Keterangan**
Client	Menunjukan sebagai *client*
Dev tap	"dev tun" akan menciptakan tunnel routing IP. "dev tap" akan menciptakan tunnel Ethernet.
Proto tcp	Protokol yang digunakan adalah tcp
Remote 192.168.x.x 1194	IP Address *server* dan *port* yang dibuka untuk VPN. (Pada saat ujicoba IP *Server* yaitu 192.168.x.x)
Resolve-retry infinite	Untuk mencoba menjaga koneksi dengan *server*.
Nobind	*Client* tidak perlu mengikat *port*

Persist-key Persist-tun	Berguna untuk menghindari mengakses sumber daya tertentu pada *restart* yang mungkin tidak dapat diakses lagi karena *downgrade* hak istimewa
Ca /etc/openvpn/keys/ca.crt Cert /etc/openvpn/keys/server.crt Key /etc/openvpn/keys/server.key	Sertifikat dan kunci-kunci yang digunakan *server* serta tempat beradanya sertifikat dan kunci tersebut
Comp-lzo	Meng-*enable*-kan kompresi pada jalur VPN
Verb 4	Untuk penggunaan umum
Auth-user-pass	Menggunakan authentikasi untuk *client* yang berupa *username* dan *password*

Berikut ini adalah isi dari file client.ovpn

```
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap
; dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
```

```
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
; dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
proto tcp
;proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
;remote my-server-1 1194
;remote my-server-2 1194
remote 192.168.x.x 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite
```

```
# Most clients don't need to bind to
# a specific local port number.
nobind

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca keys/ca.crt
```

```
cert keys/client1.crt
key keys/client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x
;cipher AES-128-CBC



# Enable compression on the VPN link.
# Don't enable this unless it is also
```

```
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 4

# Silence repeating messages
;mute 20
```

3.8 Pengujian

Pada penelitian ini dilakukan pengujian terhadap virtual private network dengan beberapa skenario. Simulasi akan dilakukan melalui jaringan internet, dengan arsitektur simulasi seperti yang telah dirancang pada Gambar 3.4.

3.8.1 Skenario Pengujian

Pada skenario pengujian akan dilakukan terhadap konektivitas remote access VPN yang berbasis SSL. Adapun skenario-skenario yang akan dilakukan adalah sebagai berikut:

1. Pengujian Startup VPN (Startup Server dan Startup Client), pengujian bertujuan apakah konfigurasi yang telah dilakukan pada server maupun client telah benar atau tidak.
2. Pengujian Koneksi VPN yang berupa tes koneksi PING dan TCPdump.
3. Pengujian Akses *Server* dimana *client* melakukan akses terhadap layanan yang terdapat pada *server*, seperti Web Server, FTP Server dan DNS Server.
4. Pengujian Keamanan yang berupa tes *port scanning* terhadap VPN *server*, memonitoring data dan analisis perbandingan datanya.

3.8.2 Pengujian Startup VPN

3.8.2.1 Pengujian Startup *Server*

Untuk memulai startup openvpn pada *server* dilakukan perintah :

```
#/etc/init.d/openvpn start
```

Pada komputer server dan komputer remote (client) mengeluarkan output sebagai berikut:

```
root@kimrum-asus:/# sudo /etc/init.d/openvpn start
 * Starting virtual private network daemon(s)...
*   Autostarting VPN 'server'                          [ OK ]
```

Apabila status pada layar menunjukan tampilan [OK], maka vpn server tidak terjadi kesalahan konfigurasi, apabila menunjukan tampilan [FAIL], maka pada konfigurasi server masih terdapat kesalahan.

Network tap0 terbentuk dikomputer server dengan IP Address 10.10.10.1. sesuai dengan konfigurasi awal vpn server. Hal ini menandakan bahwa network vpn telah terbentuk.

```
root@kimrum-asus:/etc/openvpn# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:01:39:03:16:69
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::201:39ff:fe03:1669/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8113579 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15512541 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:511408841 (511.4 MB)  TX bytes:1406335472 (1.4 GB)
          Interrupt:20 Base address:0xe800

eth1      Link encap:Ethernet  HWaddr 00:24:8c:88:d3:8d
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:42 Base address:0xa000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:180 errors:0 dropped:0 overruns:0 frame:0
          TX packets:180 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:69710 (69.7 KB)  TX bytes:69710 (69.7 KB)

tap0      Link encap:Ethernet  HWaddr 06:09:19:d8:7e:bc
          inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::409:19ff:fed8:7ebc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2696 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
RX bytes:396129 (396.1 KB)  TX bytes:218984 (218.9 KB)
```

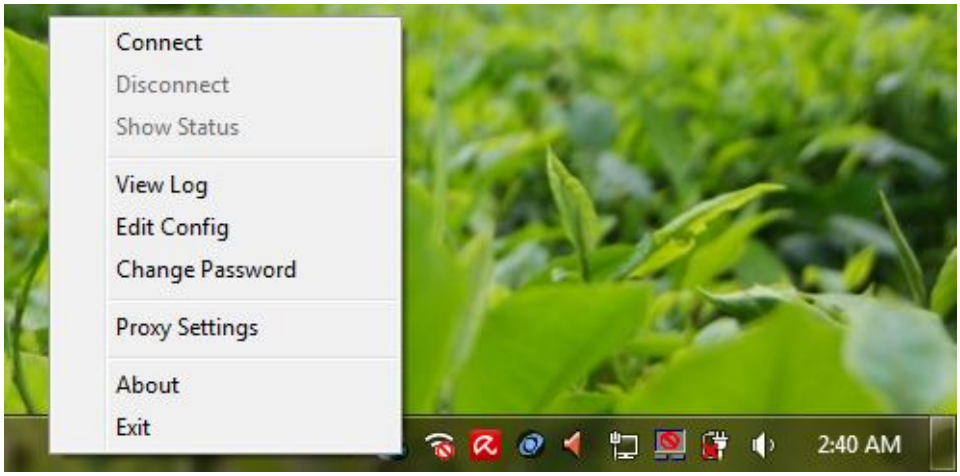
3.8.2.2 Pengujian Startup *Client* Windows

Pada pengujian startup client berbasis windows menggunakan openvpn versi GUI. Kondisi apabila belum terkoneksi dengan VPN server, indikator openvpn akan menunjukkan warna merah.



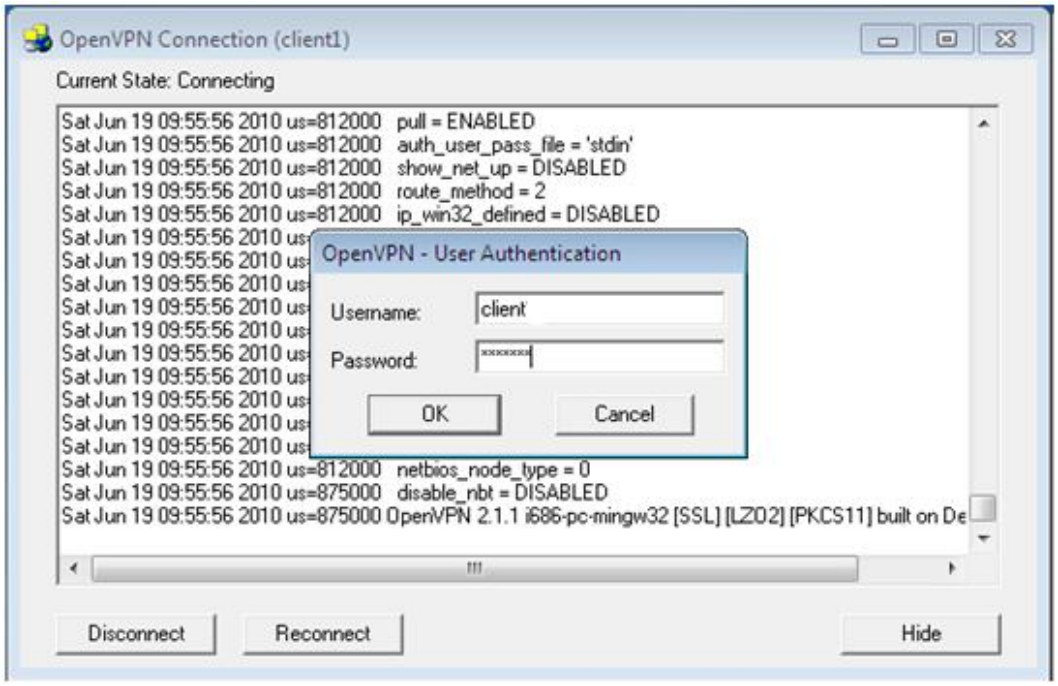
Gambar 3.6 Kondisi Tidak Terkoneksi Dengan VPN Server

Klik kanan pada openvpn dan lakukan koneksi sesuai dengan client yang diizinkan oleh server (nama client pada saat pengujian bernama client1).



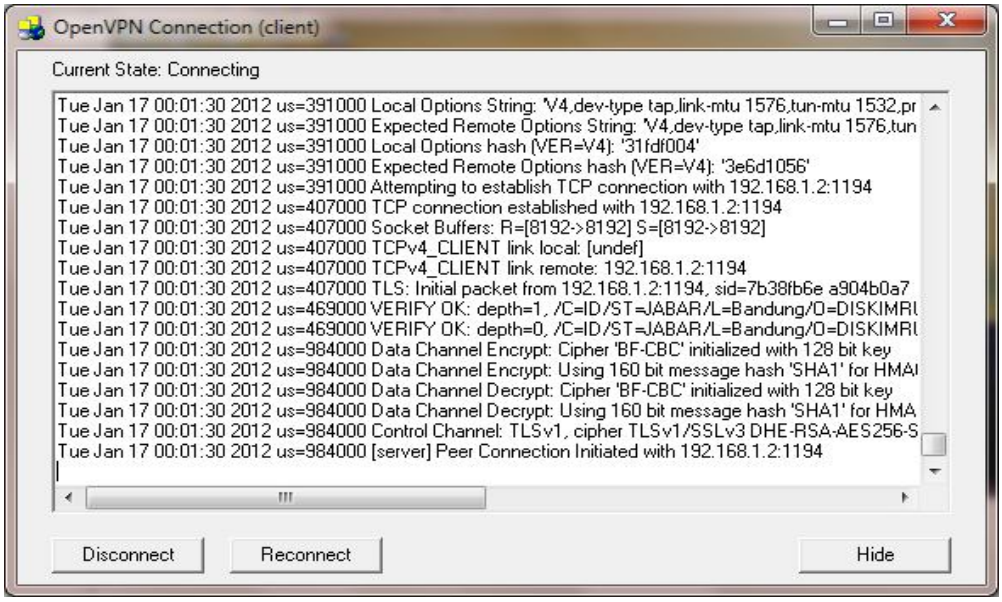
Gambar 3.7 Mengkoneksikan ke VPN Server

Maka openvpn akan melakukan inialisasi dan meninta client memasukan username dan password.



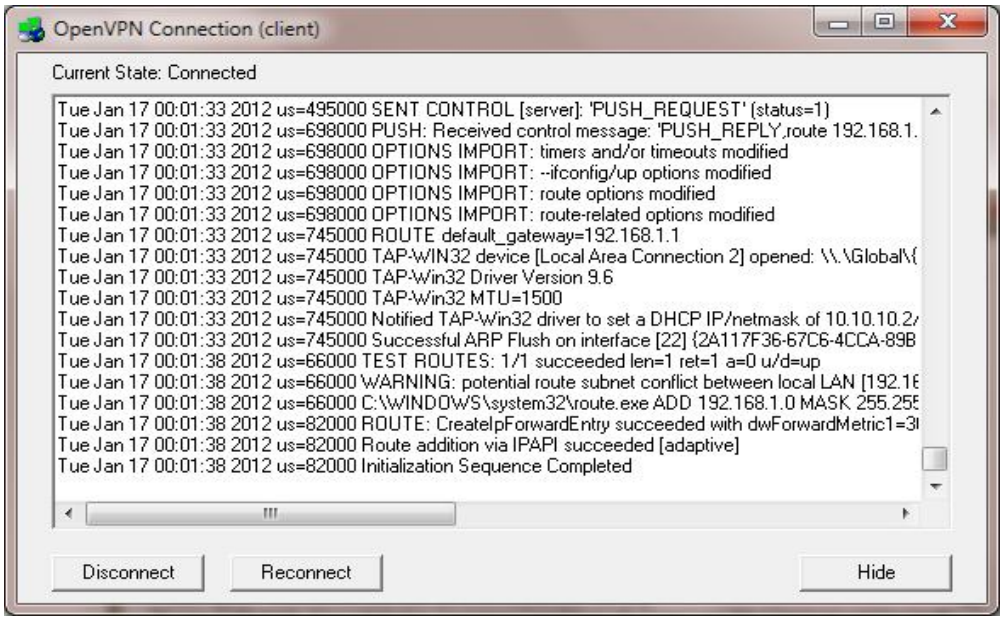
Gambar 3.8 Autentikasi Client

Apabila username dan password sesuai, maka openvpn akan mencoba koneksi kepada vpn server sampai inialisasi tersebuat berhasil dikoneksikan.

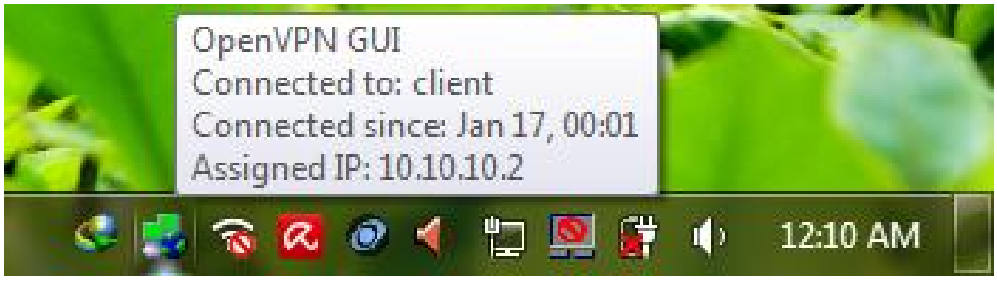


Gambar 3.9 Proses Inialisasi Ke VPN Server

Apabila proses inialisasi berhasil dilakukan, maka indikator openvpn akan berubah menjadi warna hijau.



Gambar 3.10 VPN Client berhasil dikoneksikan dengan VPN Server



Gambar 3.11 VPN Client terkoneksi ke VPN server

Maka akan terbentuk network baru pada VPN Client dengan alamat IP 10.10.10.2

```
C:\Users\Nazy>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6449:d35:e247:127c%22
   IPv4 Address. . . . . . . . . . . : 10.10.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f447:d7b5:eae9:c487%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.121
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

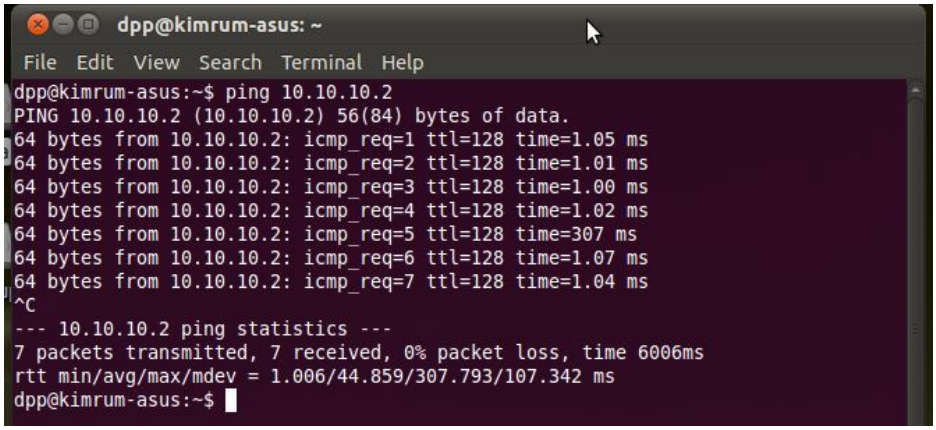
Tunnel adapter isatap.{E22E9665-307D-442C-941D-C968A57CA6C3}:
```

Gambar 3.12 Terbentuk Network Baru Untuk VPN Client

3.8.3 Pengujian Koneksi VPN

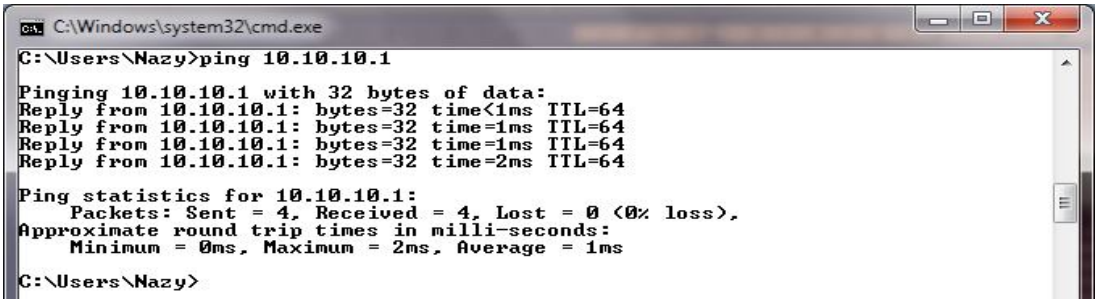
3.8.3.1 Pengujian Ping

Pada pengujian koneksi dilakukan tes ping dan tcpdump kepada vpn. Tes ping dari komputer server kepada komputer client berhasil dan menghasilkan log seperti yang ditunjukan dibawah ini:



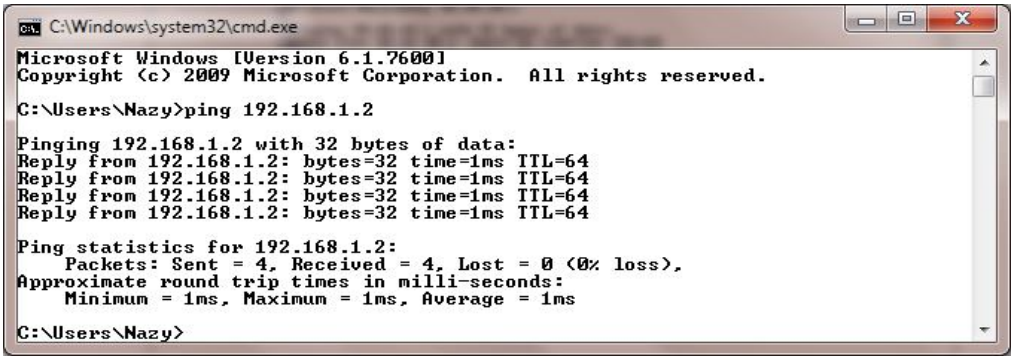
Gambar 3.13 Ping vpn server ke client

Sedangkan ping dari komputer remote (Linux Client) kepada komputer vpnserver berhasil dan menghasilkan log seperti yang ditunjukan dibawah ini:



Gambar 3.14 Ping Client ke vpn server

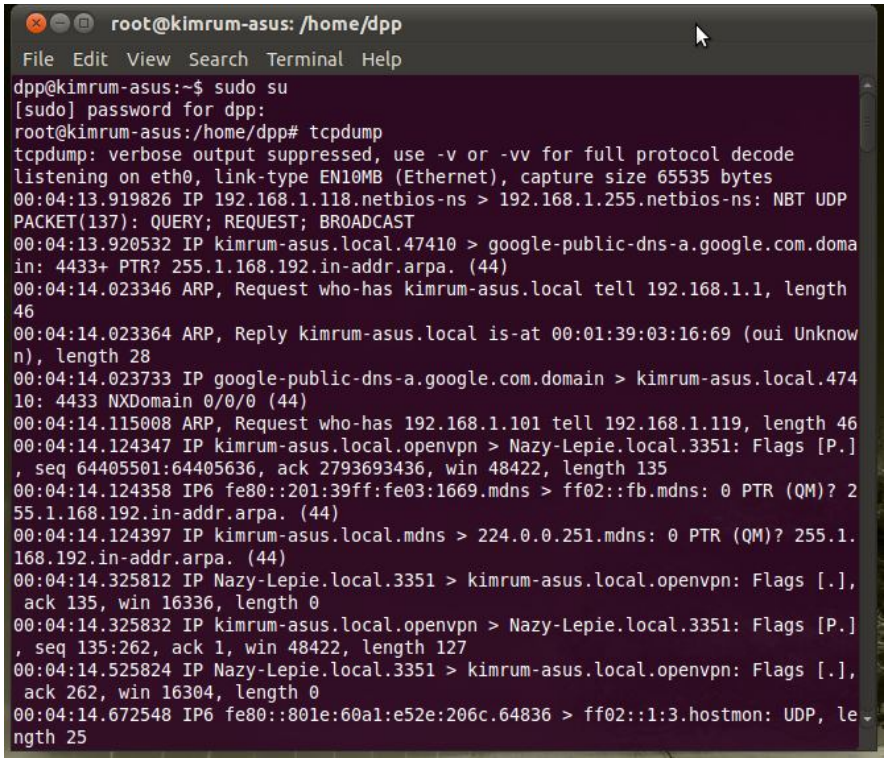
Ping dari komputer remote (Windows Client) kepada komputer server berhasil dan menghasilkan log seperti yang ditunjukan dibawah ini:



Gambar 3.15 Ping client ke komputer server

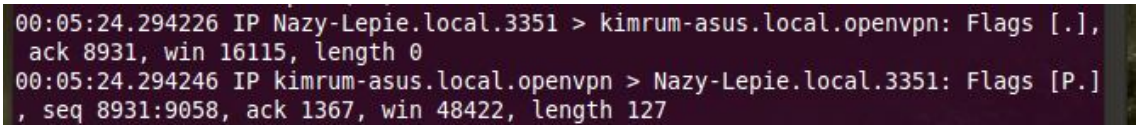
3.8.3.2 Pengujian TCPDUMP

Tes koneksi dengan menggunakan tcpdump dari komputer server ke komputer remote untuk mengecek koneksi dan melihat paket data yang diambil dan port yang diakses, tes koneksi tcpdump berhasil dilakukan dan menghasilkan log seperti dibawah ini



Gambar 3.16 Hasil Scanning TCPDUMP

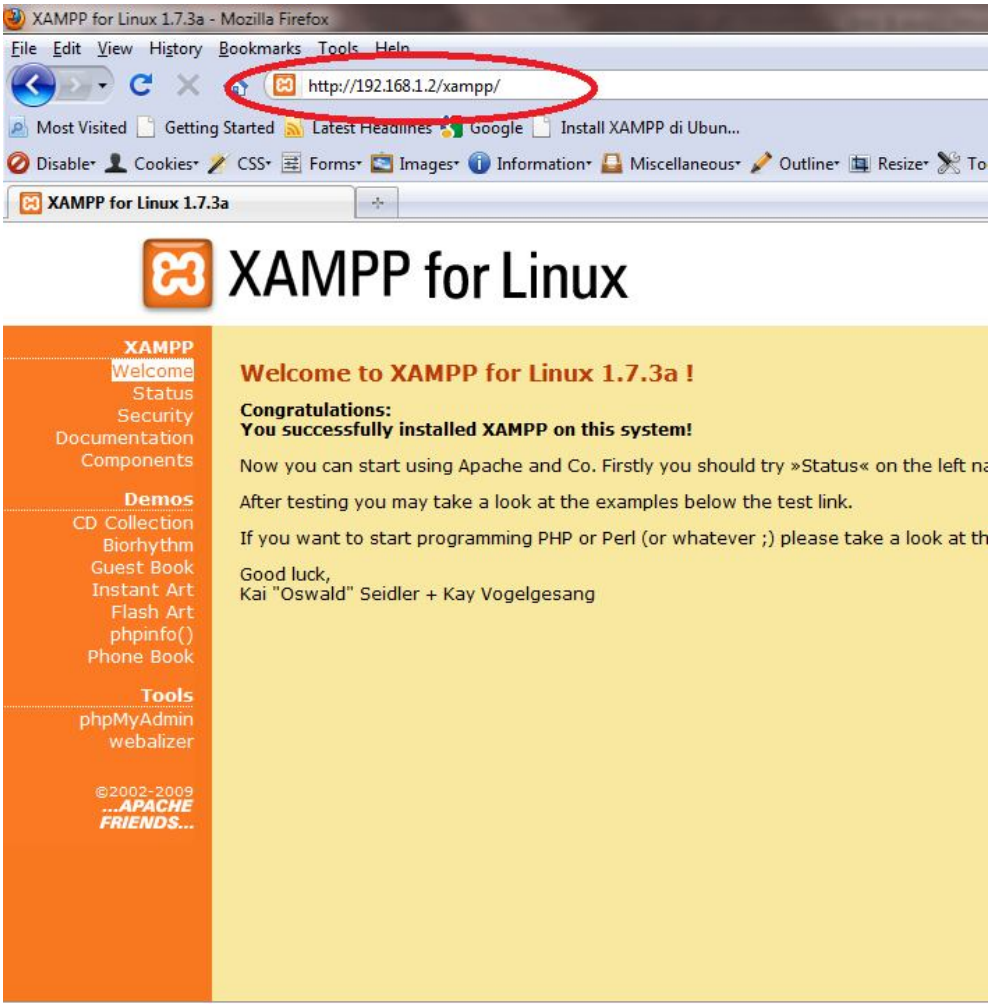
Pada log diatas, tcpdump mencatat koneksi dari server ke client dan port yang di akses sebagai contoh port 3315



Gambar 3.17 Rincian Scanning TCPDUMP

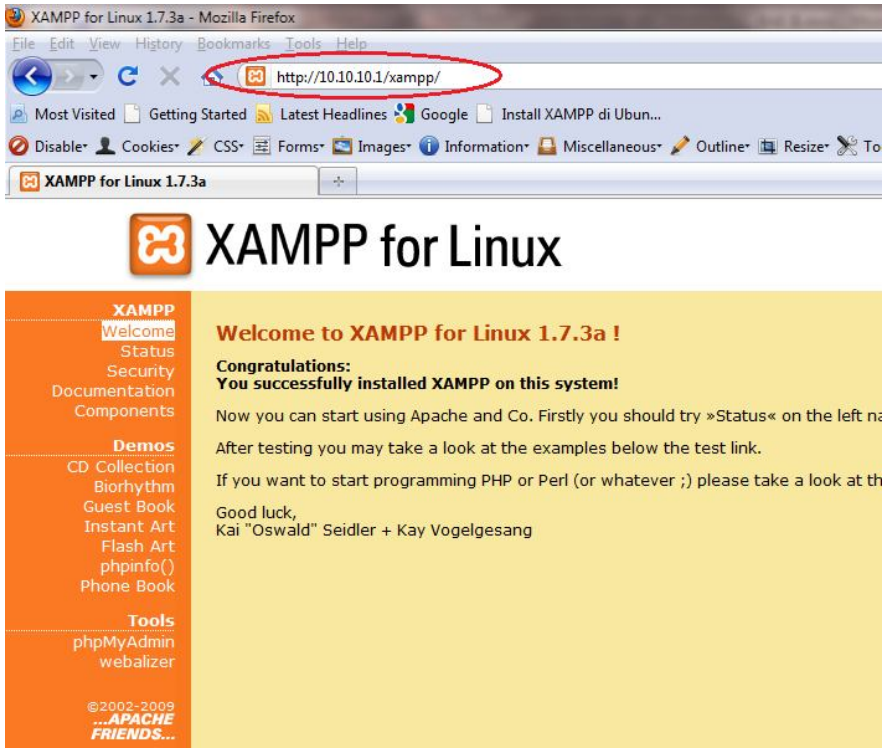
3.8.3.3 Pengujian Akses Server

Pengujian dilakukan pada akses web server yang terdapat di komputer server, akses web server dilakukan web browser dengan mengetikan alamat IP dari komputer server (192.168.1.2).



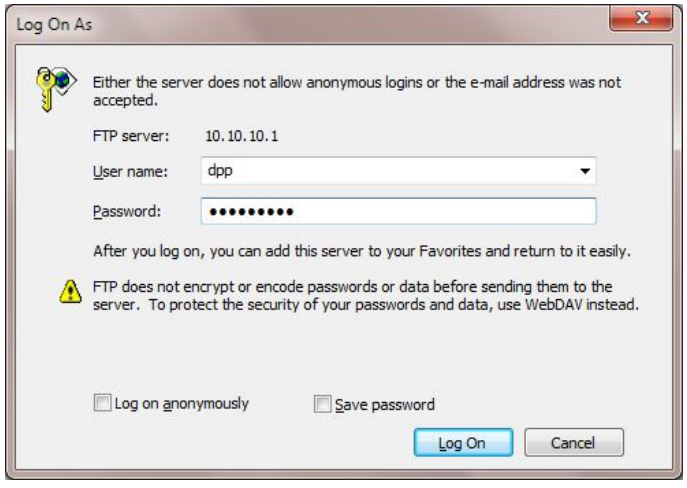
Gambar 3.18 Koneksi Web Server

Sedangkan untuk akses web server yang terdapat pada komputer server, akses web server dapat dilakukan melaui web browser dengan mengetikan IP Address komputer server VPN, pengujian akses web server berhasil dan akan menampilkan hasil seperti yang ditunjukkan Gambar 3.18 dibawah ini:

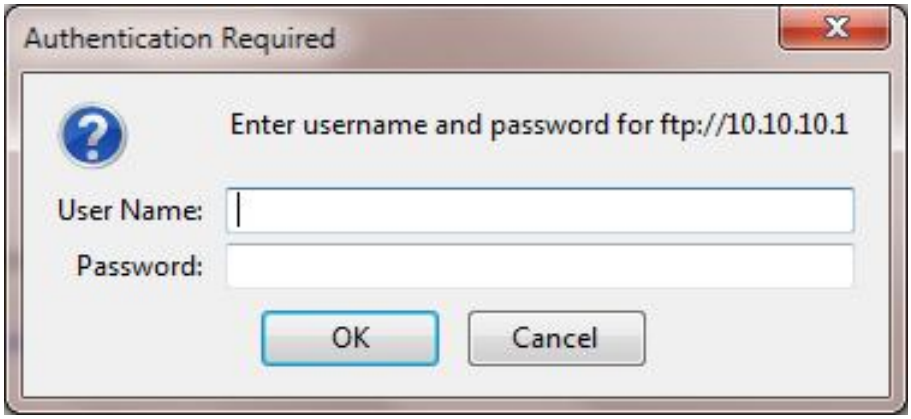


Gambar 3.19 Akses Web Server di VPN Server

Pada akses ftp server, sebelum terkoneksi dengan ftp server, client akan diminta untuk mengisi autentikasi seperti yang ditunjukkan pada Gambar 3.20 di bawah ini:

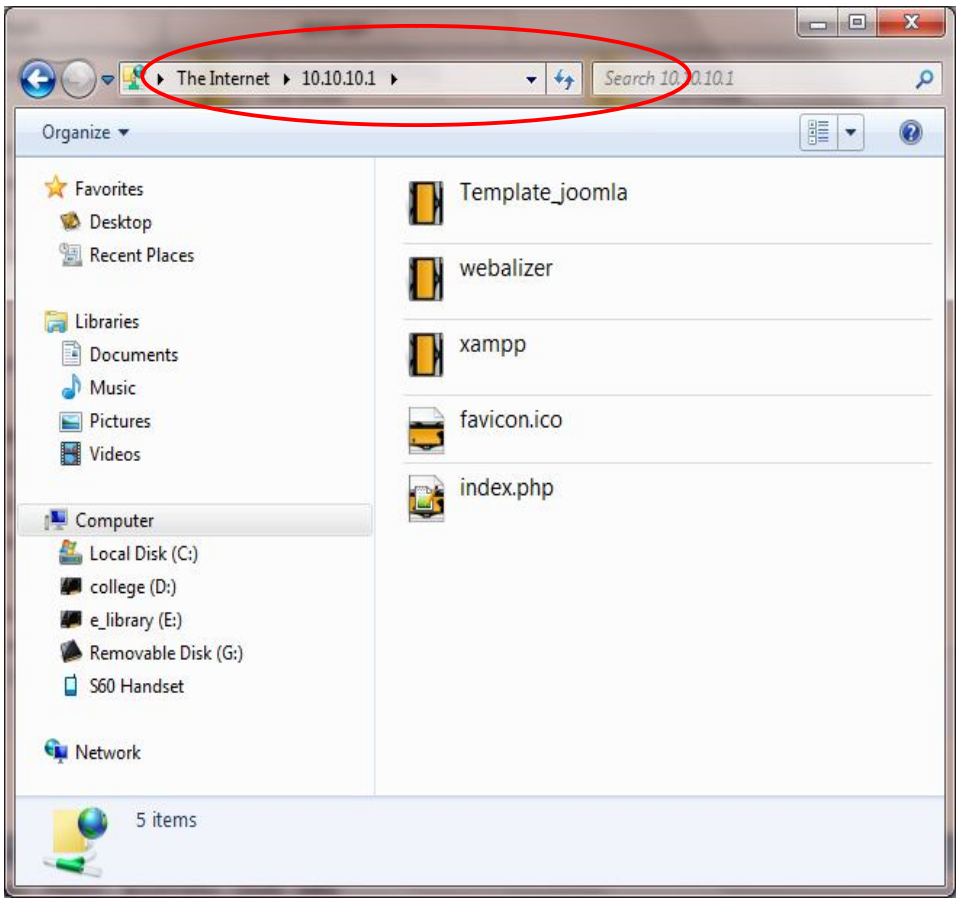


(a)

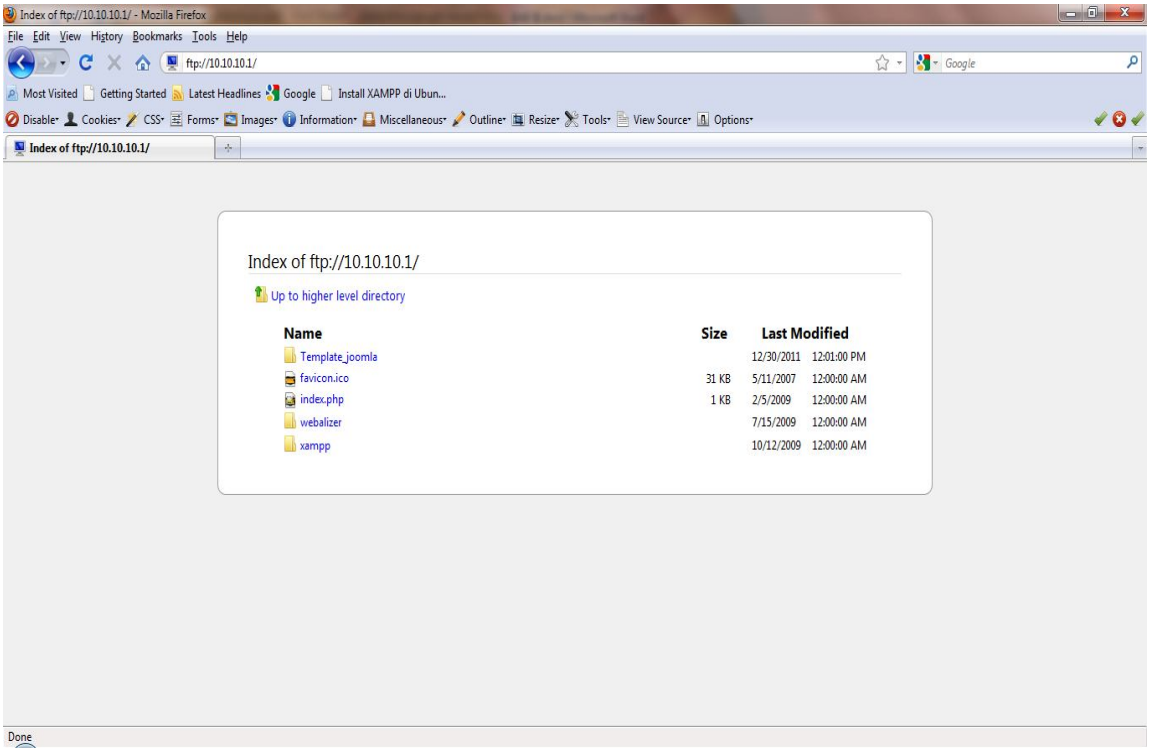


(b)

Gambar 3.20 (a) authentikasi windows explorer; (b) authentikasi web browser



(a)



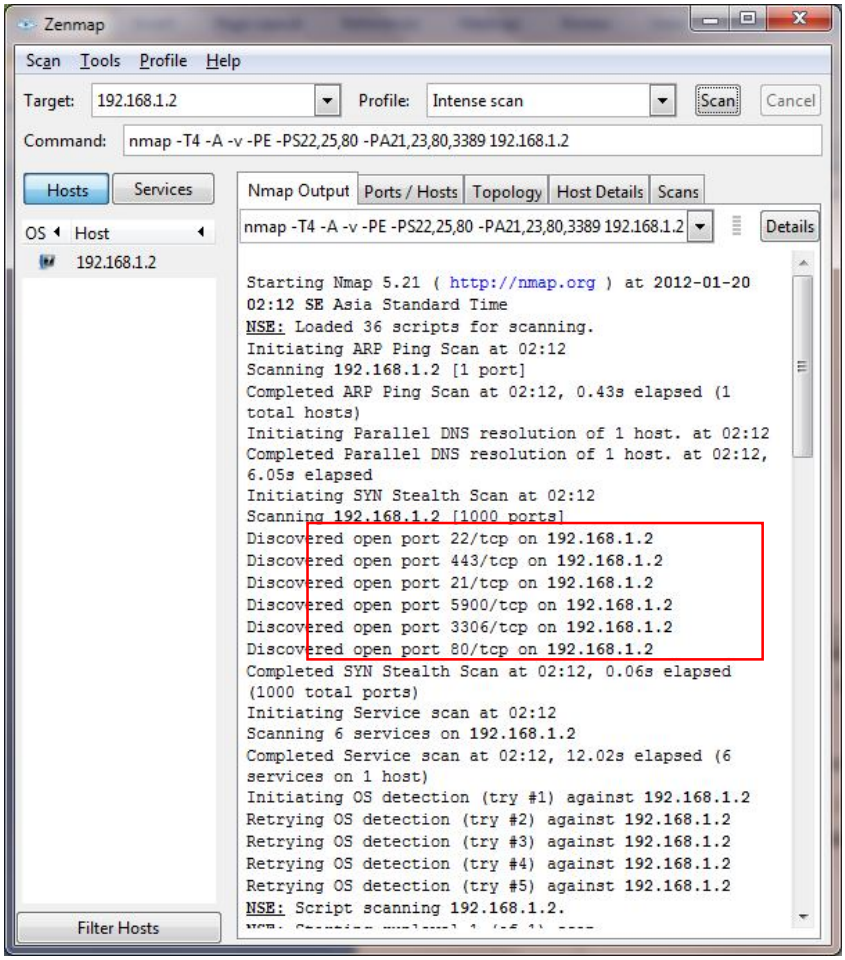
(b)

Gambar 3.21 (a) akses melalui windows explorer; (b) akses melalui web browser

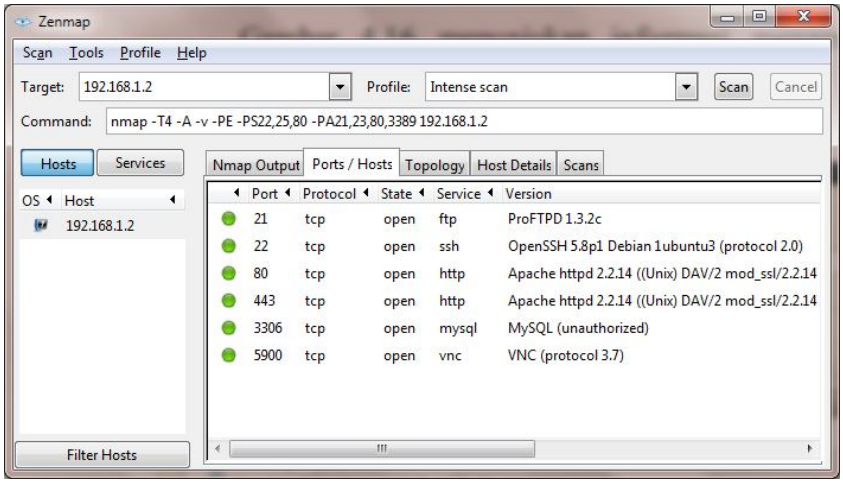
Setelah login berhasil, maka client dapat mengakses file yang berada pada ftp server.

3.8.3.4 Pengujian *Scanning Port*

Pada pengujian scanning port dilakukan terhadap vpn server menggunakan mode *intense scan* dan *intense scan all TCP Scan*, scanning terhadap vpn server menggunakan aplikasi Zenmap, adapun hasil dari scanning adalah sebagai berikut:

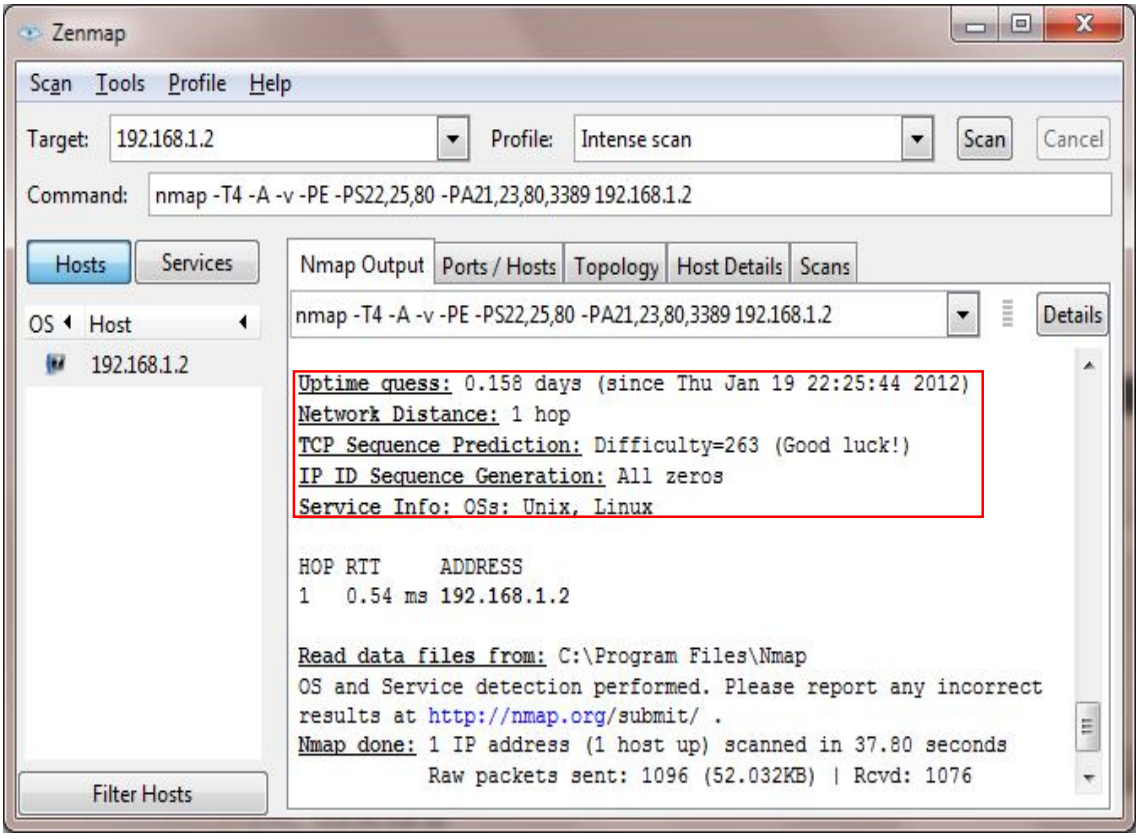


Gambar 3.22 *Scanning Port Server* VPN mode *intense scan*



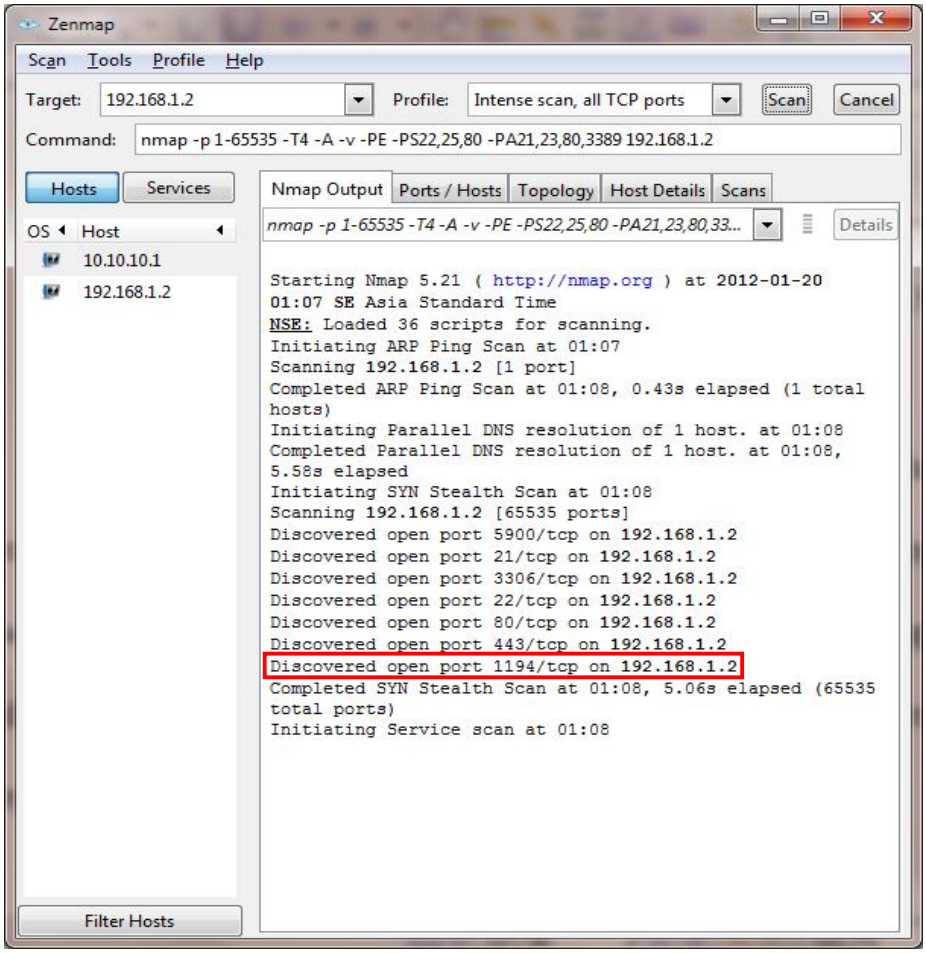
Gambar 3.23 Informasi *Ports/Hosts* yang aktif

Pada hasil scanning port menggunakan mode *intense scan* menunjukan bahwa terdapat 6 port yang terbuka, dan port VPN yang telah dibuat sebelumnya, yaitu port 1194 tidak tidak terdeteksi oleh Zenmap.



Gambar 3.24 Informasi *Host* pada *server* VPN

Sedangkan apabila melakukan scanning port terhadap vpn server dengan menggunakan mode *intense scan all TCP Scan*, maka akan terdeteksi 7 port yang terbuka, dan port vpn server (1194) terdeteksi oleh aplikasi Zenmap.



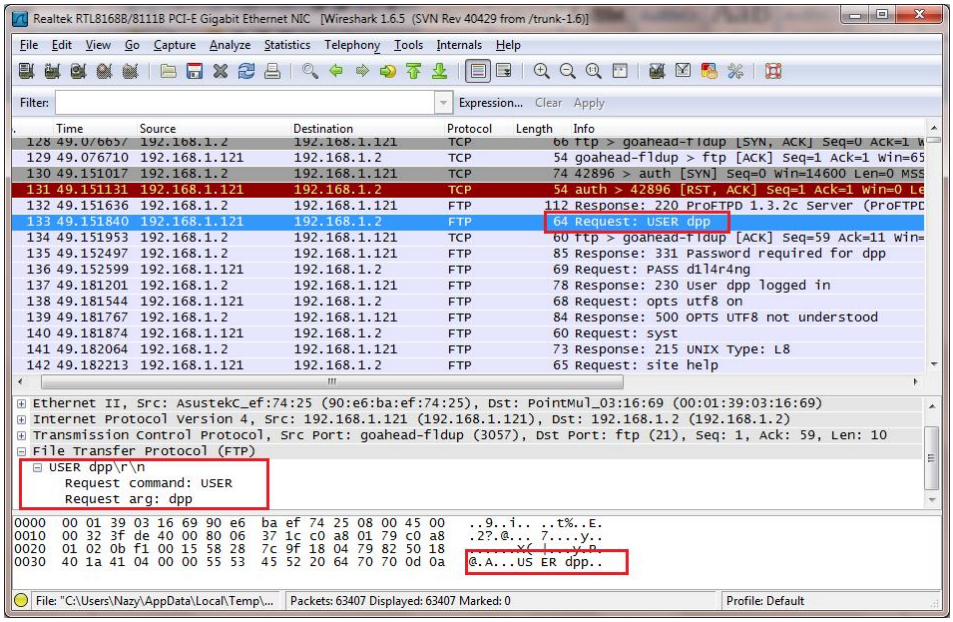
Gambar 3.25 Scanning mode *intense scan all TCP Scan*

3.8.3.5 Pengujian Monitoring Data

Pada pengujian monitoring data dilakukan monitoring data dari proses transfer yang dilakukan, baik yang melalui remote access VPN yang berbasis SSL maupun tidak, dan membandingkan hasil dari monitoring data yang dilakukan tesebut. Proses akses dilakukan client untuk mendownload data dari server melaui ftp server. Adapun hasil yang diperoleh adalah sebagai berikut:

a. Monitoring Data Tidak melalui Remote Access VPN Berbasis SSL

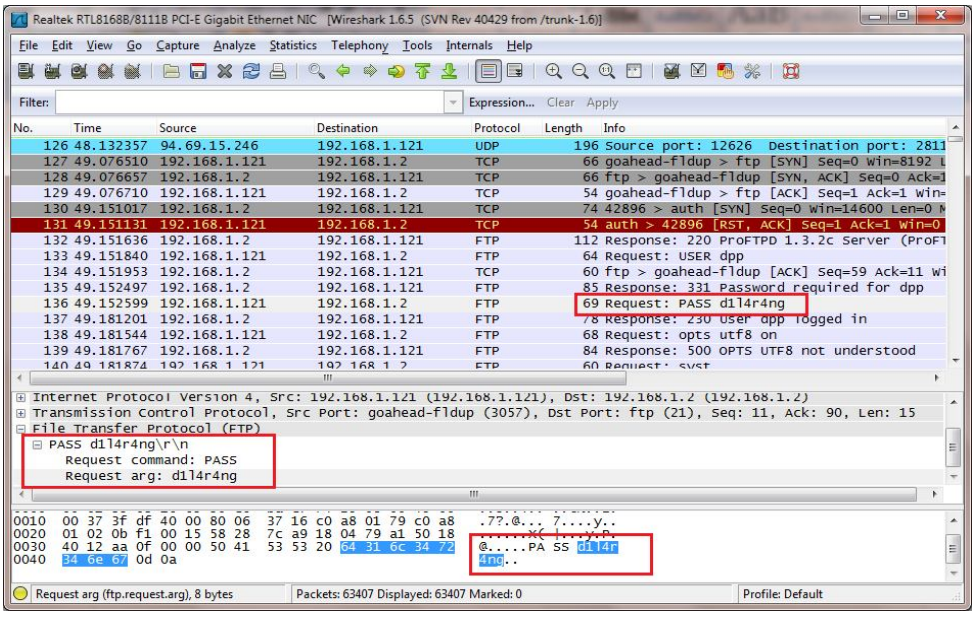
Monitoring data yang tidak melalui remote access vpn yang berbasis SSL, akan menampilkan hasil seperti Gambar 3.25 berikut ini.



Gambar 3.26 Monitoring tanpa melalui remote akses VPN berbasis SSL

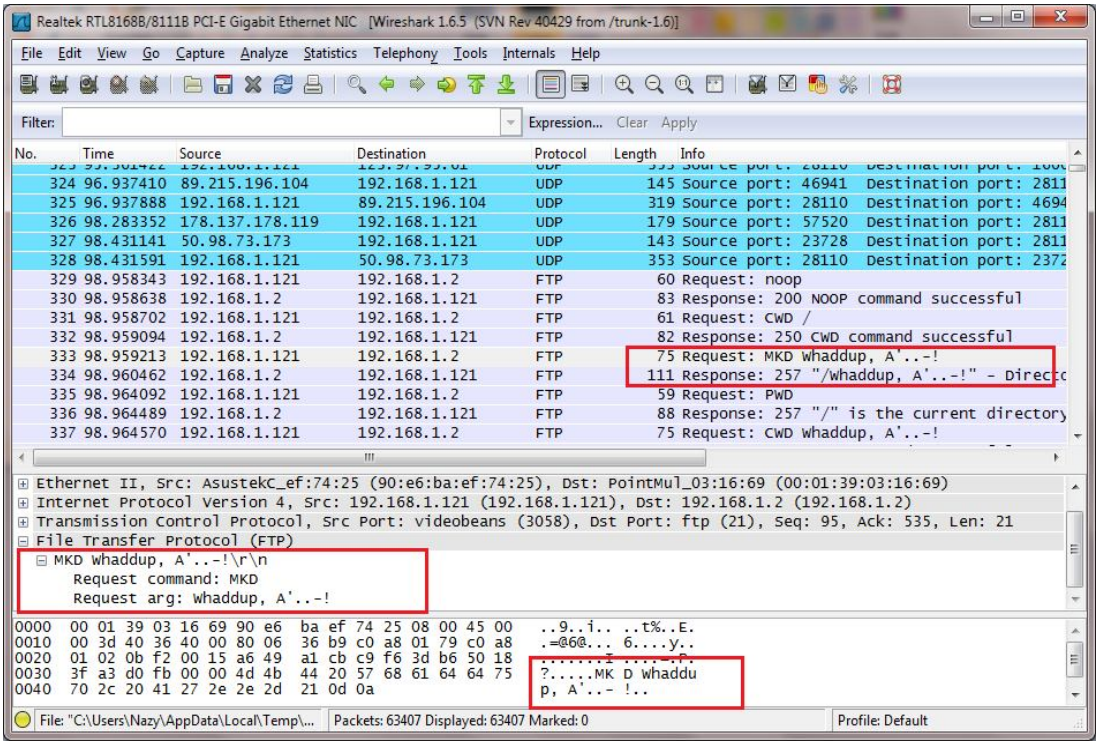
Gambar 3.26 menunjukkan client “dpp” yang melakukan akses terhadap ftp server, dapat diketahui username yang melakukan akses terhadap ftp server.

Pada Gambar 3.27 menunjukkan bahwa user yang melakukan akses terhadap ftp server dapat juga diketahui password yang digunakan oleh user tersebut.



Gambar 3.27 Monitoring tanpa melalui remote akses VPN berbasis SSL (2)

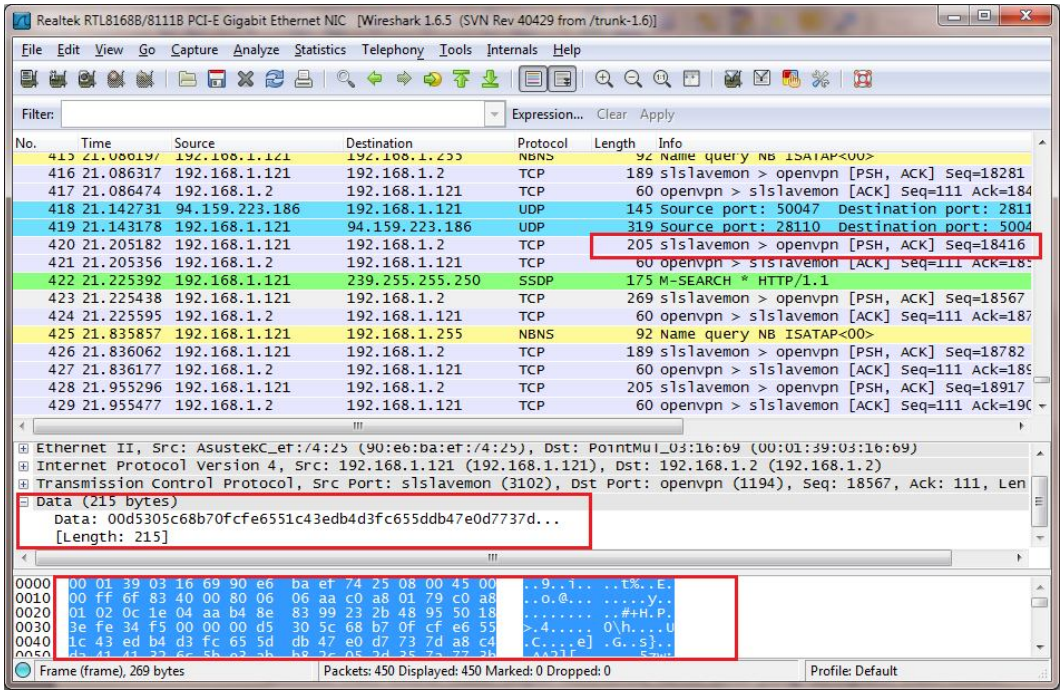
Pada gambar 3.27 menunjukan bahwa client yang melakukan transfer file (berupa folder) terhadap ftp server, dapat diketahui pula file yang transfer oleh user yang melakukan akses terhadap ftp server.



Gambar 3.28 Monitoring tanpa melalui remote akses VPN berbasis SSL (3)

A. Monitoring Data Melalui Remote Access VPN Berbasis SSL

Pada proses monitoring data yang melalui remote access vpn yang berbasis SSL, username dan password yang digunakan oleh client untuk mengakses ftp server tidak diketahui, serta data yang di-request oleh client tidak dapat dimonitor oleh wireshark, seperti yang ditunjukkan pada Gambar 3.28 dibawah ini:



Gambar 3.29 Monitoring data melalui VPN

Pada Gambar 3.29, dapat diperoleh hasil bahwa dengan menggunakan remote access VPN yang berbasis SSL terbukti data yang ditransfer akan terlebih dahulu dilakukan enkripsi, sehingga informasi tentang username, password yang dimiliki oleh client tidak dapat diketahui, serta data yang direquest oleh client tidak dapat diketahui, sehingga proses transfer data melalui remote access virtual private network yang berbasis secure socket layer menjadi aman.