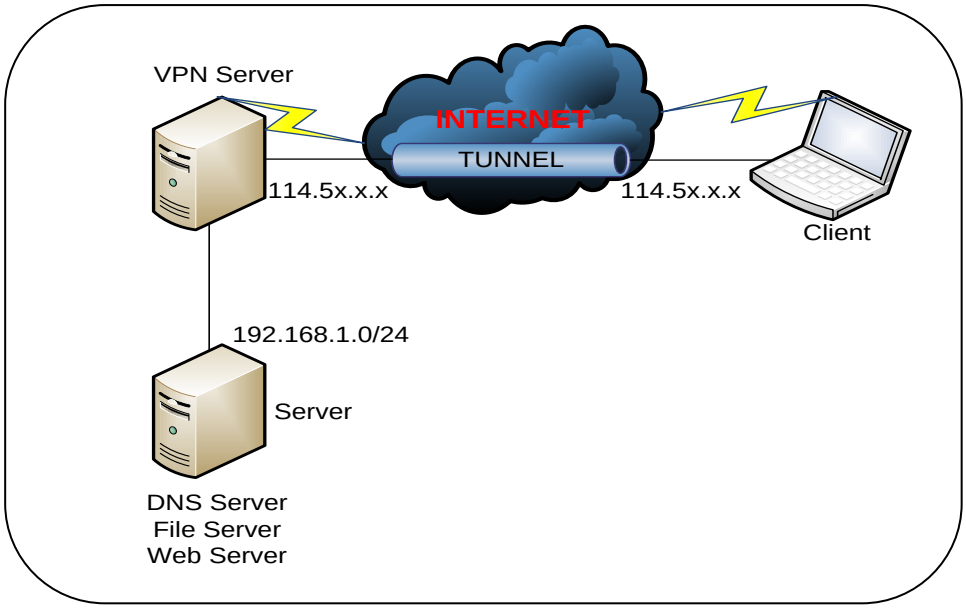
BAB IV
IMPLEMENTASI DAN PENGUJIAN

4.1 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.

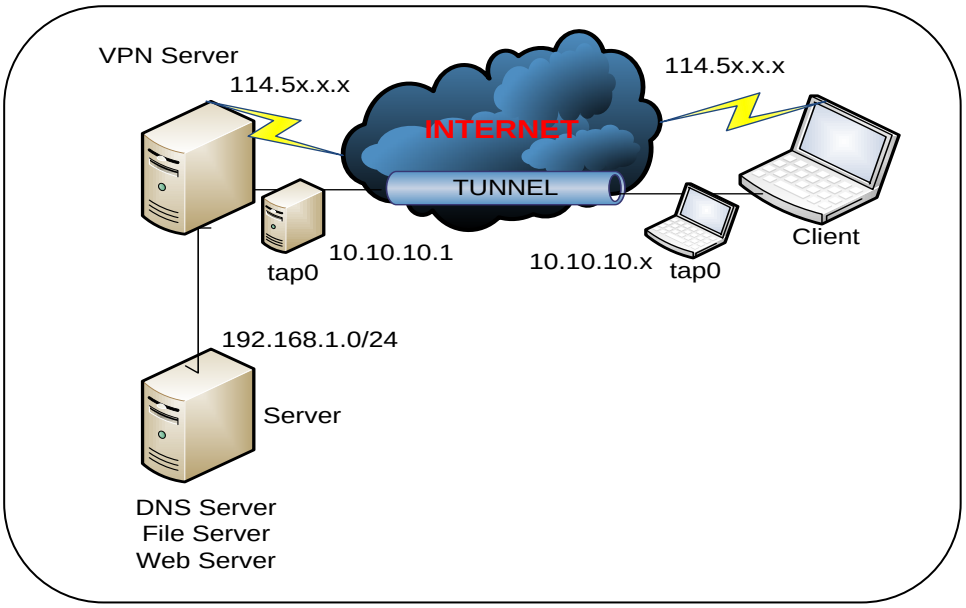
4.1.1 Konfigurasi Jaringan

Pada konfigurasi jaringan dilakukan pengalamatan IP terhadap *server* dan *client* sesuai dengan skema perancangan jaringan yang telah dilakukan pada bab sebelumnya. Adapun pengalamatan IP terhadap vpn *server*, *server* dan *client* adalah sebagai berikut:



Gambar 4.1 *Implementasi Jaringan Remote Access VPN Berbasis SSL*

Pada implementasi *network* vpn, vpn *server* akan diberikan IP *address*-nya yaitu 10.10.10.1 dengan *subnet* 255.255.255.0 dan IP *address client* akan berada pada *range* 10.10.10.2-10.10.10.254 dengan *subnet* 255.255.255.0. Sehingga akan terbentuk topologi logik seperti yang ditunjukkan pada Gambar 4.2 dibawah ini:



Gambar 4.2 *Topologi Logik Remote Access VPN Berbasis SSL*

Sehingga konfigurasi akan menghasilkan alamat-alamat IP *address* seperti yang ditunjukan pada Tabel 4.1 berikut:

Tabel 4.1 Alokasi IP Address

Device	IP Address	Publik/Private	Interface
VPN *Server*	114.5x.x.x.	IP Publik	Modem HSDPA
	192.168.1.1	IP Private	Eth0
	10.10.10.1	IP VPN	Tap0
Server	192.168.1.100	IP Private	Eth0
Client	114.5x.x.x	IP Publik	Modem HSDPA
	10.10.10.x	IP VPN	Tap0

4.1.2 Konfigurasi VPN *Server*

Pada VPN *Server* digunakan sistem operasi Linux Ubuntu Lucid Lynx 10.04. 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 4.2 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 4.3 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="h2s.cyber@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:

```
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) [JB]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [Learner]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Learner
CA]:
Name []:
Email Address [h2s.cyber@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) [JB]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [Learner]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [h2s.cyber@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:

```
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) [JB]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [Learner]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [h2s.cyber@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:'JB'
localityName          :PRINTABLE:'Bandung'
organizationName      :PRINTABLE:'Learner'
commonName            :PRINTABLE:'server'
emailAddress          :IA5STRING:'h2s.cyber@gmail.com'
Certificate is to be certified until May 25 12:07:54 2020 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) [JB]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [Learner]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [h2s.cyber@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

```
-rw-r--r-- 1 root root 3843 2010-05-28 19:07 01.pem
-rw-r--r-- 1 root root 3727 2010-05-28 19:09 02.pem
-rw-r--r-- 1 root root 1200 2010-05-28 19:07 ca.crt
-rw------- 1 root root  887 2010-05-28 19:07 ca.key
-rw-r--r-- 1 root root  207 2010-05-28 19:09 index.txt
-rw-r--r-- 1 root root   21 2010-05-28 19:09 index.txt.attr
-rw-r--r-- 1 root root   21 2010-05-28 19:07 index.txt.attr.old
-rw-r--r-- 1 root root  103 2010-05-28 19:07 index.txt.old
-rw-r--r-- 1 root root    3 2010-05-28 19:09 serial
-rw-r--r-- 1 root root    3 2010-05-28 19:07 serial.old
-rw-r--r-- 1 root root    0 2010-05-29 03:27 server.crt
-rw-r--r-- 1 root root  668 2010-05-29 03:27 server.csr
-rw------ 1 root root  887 2010-05-29 03:27 server.key
```

Sedangkan untuk pembuatan kunci untuk *client* yang akan dikoneksikan dengan VPN *server*, kunci untuk *client* diberi nama *client*1.

```
#. 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:

```
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) [JB]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [Learner]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client1]:
Name []:
Email Address [h2s.cyber@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:'JB'
localityName          :PRINTABLE:'Bandung'
organizationName      :PRINTABLE:'Learner'
commonName            :PRINTABLE:'client1'
emailAddress          :IA5STRING:'h2s.cyber@gmail.com'
Certificate is to be certified until May 25 12:09:02 2020 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) [JB]:
Locality Name (eg, city) [Bandung]:
Organization Name (eg, company) [Learner]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [h2s.cyber@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 *client*1.crt, *client*1.key, dan *client*1.csr.

```
-rw-r--r-- 1 root root 3843 2010-05-28 19:07 01.pem
-rw-r--r-- 1 root root 3727 2010-05-28 19:09 02.pem
-rw-r--r-- 1 root root 1200 2010-05-28 19:07 ca.crt
-rw------- 1 root root  887 2010-05-28 19:07 ca.key
-rw-r--r-- 1 root root 3727 2010-05-28 19:09 client1.crt
-rw-r--r-- 1 root root  668 2010-05-28 19:09 client1.csr
-rw------- 1 root root  887 2010-05-28 19:09 client1.key
-rw-r--r-- 1 root root  207 2010-05-28 19:09 index.txt
-rw-r--r-- 1 root root   21 2010-05-28 19:09 index.txt.attr
-rw-r--r-- 1 root root   21 2010-05-28 19:07 index.txt.attr.old
-rw-r--r-- 1 root root  103 2010-05-28 19:07 index.txt.old
-rw-r--r-- 1 root root    3 2010-05-28 19:09 serial
-rw-r--r-- 1 root root    3 2010-05-28 19:07 serial.old
-rw-r--r-- 1 root root    0 2010-05-29 03:27 server.crt
-rw-r--r-- 1 root root  668 2010-05-29 03:27 server.csr
-rw------- 1 root root  887 2010-05-29 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 4.4 Parameter Konfigurasi Server

Parameter	Keterangan
Server	Menunjukan sebagai *server*
Port 1194	*Port* yang akan dibuka untuk vpn (1194 merupakan *port* default untuk openvpn)

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 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
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 192.168.1.0/24 melalui alamat tunnel *server* 10.10.10.1
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*

4.1.3 Konfigurasi *Client*

4.1.3.1 Konfigurasi *Client* Linux

Konfigurasi *client* yang berbasis linux harus meng-*copy*-kan sertifikat dan kunci *client* yang telah dibuat dari *server*, yaitu ca.crt, client1.crt, client1.csr client1.key, simpan file-file tersebut di folder /etc/openvpn/

Copy file client.conf yang berada di folder /usr/share/doc/openvpn/examples/sample-config-files ke folder /etc/openvpn, kemudian sesuaikan file konfigurasi client.conf dengan file konfigurasi yang terdapat pada *server* dengan parameter sebagai berikut:

Tabel 4.5 Parameter Konfigurasi Client Linux

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 114.59.105.35 1194	IP Address *server* dan *port* yang dibuka untuk VPN (Pada saat ujicoba IP Public *Server* yaitu 114.59.105.35)
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.*

4.1.3.2 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 4.6 sebagai berikut:

Tabel 4.6 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 114.59.105.35 1194	IP Address *server* dan *port* yang dibuka untuk VPN. (Pada saat ujicoba IP Public *Server* yaitu 114.59.105.35)
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.*

4.2 Pengujian

Pada penelitian ini dilakukan pengujian terhadap *remote access virtual private network* dengan beberapa skenario. Simulasi akan dilakukan melalui jaringan internet, dengan arsitektur simulasi seperti yang telah dirancang pada Gambar 4.1.

4.2.1 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.

4.2.2 Pengujian Startup VPN

4.2.2.1 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@musashi-laptop:/etc/openvpn# /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@musashi-laptop:/etc/openvpn# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:d4:9c:81:af
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::216:d4ff:fe9c:81af/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:301 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31927 (31.9 KB)  TX bytes:43936 (43.9 KB)
          Interrupt:16 Base address:0x2000

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:885 errors:0 dropped:0 overruns:0 frame:0
          TX packets:885 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:76550 (76.5 KB)  TX bytes:76550 (76.5 KB)


tap0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-
```

```
00-00-00-00
          inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1680 (1.6 KB)  TX bytes:1344 (1.3 KB)

wlan0     Link encap:Ethernet  HWaddr 00:18:de:cf:ad:10
          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)
```

4.2.2.2 Pengujian Startup *Client* Linux

Untuk memulai startup openvpn pada *client*, lakukan inialisasi *client*.

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

Pada komputer remote (*client*) mengeluarkan output sebagai berikut:

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

Apabila status pada layar menunjukan tampilan [OK], maka vpn *client* berhasil melakukan inialisasi awal terhadap file konfigurasi *client*, apabila menunjukan tampilan [FAIL], maka pada konfigurasi *client* masih terdapat kesalahan.

Apabila vpn *client* telah dilakukan startup, maka *client* dapat melakukan koneksi dengan vpn *server* untuk membentuk suatu tunnel.

```
#/etc/openvpn/openvpn --config client1.conf
```

Pada komputer remote akan melakukan inialisasi terhadap koneksi sampai muncul Initialization Sequence Completed seperti yang ditunjukan dibawah ini:

```
root@herwan-laptop:/etc/openvpn# openvpn client.conf
Fri May 28 19:38:43 2010 us=130780 Current Parameter Settings:
Fri May 28 19:38:43 2010 us=131090   config = 'client.conf'
Fri May 28 19:38:43 2010 us=131165   mode = 0
Fri May 28 19:38:43 2010 us=131232   persist_config = DISABLED
Fri May 28 19:38:43 2010 us=131298   persist_mode = 1
Fri May 28 19:38:43 2010 us=131364   show_ciphers = DISABLED
Fri May 28 19:38:43 2010 us=131429   show_digests = DISABLED
Fri May 28 19:38:43 2010 us=131495   show_engines = DISABLED
Fri May 28 19:38:43 2010 us=131560   genkey = DISABLED
Fri May 28 19:38:43 2010 us=131625   key_pass_file = '[UNDEF]'
Fri May 28 19:38:43 2010 us=131690   show_tls_ciphers = DISABLED
Fri May 28 19:38:43 2010 us=131755   Connection profiles [default]:
Fri May 28 19:38:43 2010 us=131822   proto = udp
Fri May 28 19:38:43 2010 us=131887   local = '[UNDEF]'
Fri May 28 19:38:43 2010 us=131952   local_port = 0
Fri May 28 19:38:43 2010 us=132017   remote = '192.168.1.10'
Fri May 28 19:38:43 2010 us=132082   remote_port = 1194
                              .
                              .
                              .
                              .
                              .
                              .
                              .
Fri May 28 19:38:46 2010 us=70513 ROUTE: default_gateway=UNDEF
Fri May 28 19:38:46 2010 us=83052 TUN/TAP device tun0 opened
Fri May 28 19:38:46 2010 us=83187 TUN/TAP TX queue length set to 100
Fri May 28 19:38:46 2010 us=83334 /sbin/ifconfig tun0 10.10.0.6 pointopoint
10.10.0.5 mtu 1500
Fri May 28 19:38:46 2010 us=88601 /sbin/route add -net 10.10.0.0 netmask
255.255.255.0 gw 10.10.0.5
Fri May 28 19:38:46 2010 us=128000 Initialization Sequence Completed
```

Koneksi pada VPN *client* berhasil apabila proses inialiasasi selesai seperti yang ditunjukkan pada log diatas. Pada komputer remote tap0 mempunyai IP Address 10.10.10.2, seperti yang ditunjukan dibawah ini:

```
root@herwan-laptop:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:26:9e:ed:ed:93
          inet addr:192.168.2.100  Bcast:192.168.2.255
Mask:255.255.255.0
          inet6 addr: fe80::226:9eff:feed:ed93/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:231 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20037 (20.0 KB)  TX bytes:30119 (30.1 KB)
          Interrupt:27 Base address:0x8000

eth1      Link encap:Ethernet  HWaddr c4:17:fe:7a:e1:cb
          inet6 addr: fe80::c617:feff:fe7a:e1cb/64 Scope:Link
          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:17

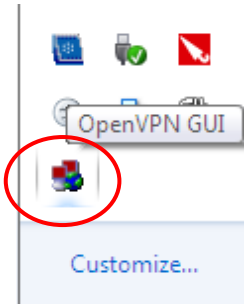
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:984 errors:0 dropped:0 overruns:0 frame:0
          TX packets:984 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

```
          RX bytes:67804 (67.8 KB)  TX bytes:67804 (67.8 KB)

tap0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-
00-00-00-00
          inet addr:10.10.10.2  Bcast:10.10.10.255 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:588 (588.0 B)  TX bytes:1092 (1.0 KB)
```

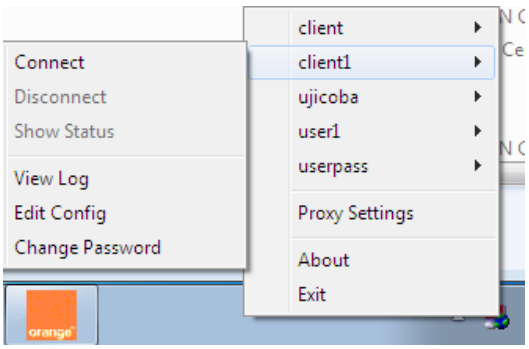
4.2.2.3 Pengujian Startup *Client* Windows

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



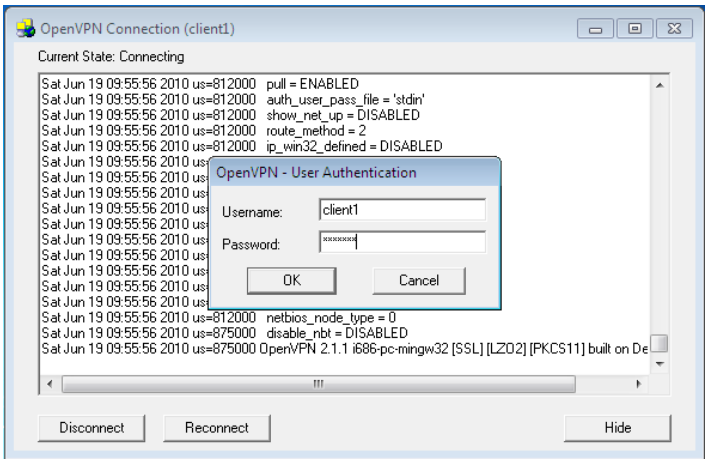
Gambar 4.3 *Kondisi Tidak Terkoneksi Dengan VPN Server*

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



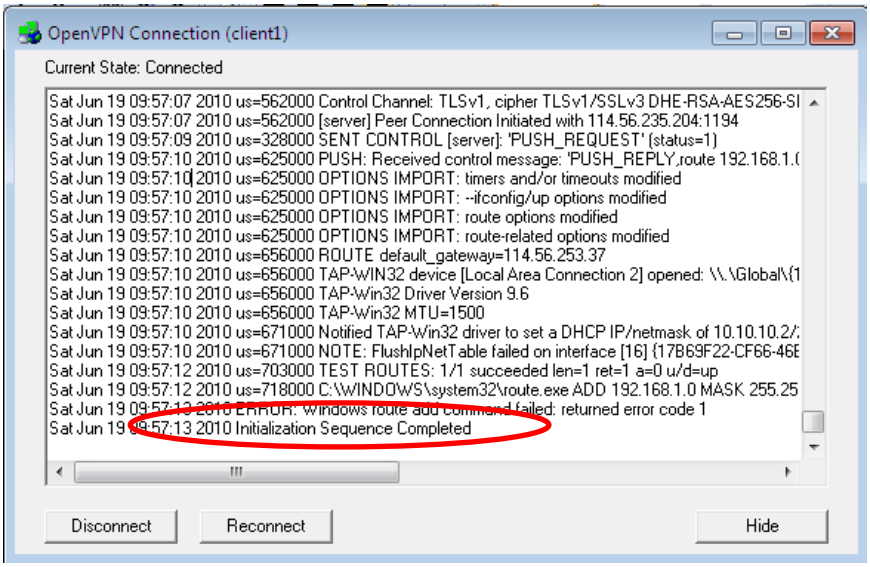
Gambar 4.4 *Mengkoneksikan ke VPN Server*

Maka openvpn akan melakukan inialisasi dan meninta client1 memasukan username dan password.



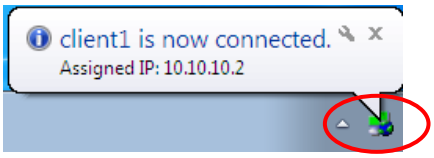
Gambar 4.5 *Autentikasi Client*

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



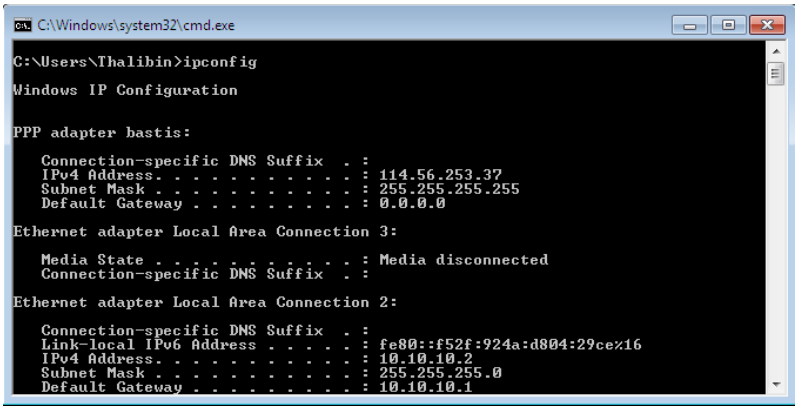
Gambar 4.6 *Proses Inialisasi Ke VPN Server*

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



Gambar 4.7 *VPN Client berhasil dikoneksikan dengan VPN Server*

Maka akan terbentuk network baru pada VPN *Client* dengan nama tap0 dengan alamat IP 10.10.10.2 dan *broadcast address* 10.10.10.255



Gambar 4.8 *Terbentuk Network Baru Untuk VPN Client*

4.2.3 Pengujian Koneksi VPN

4.2.3.1 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:

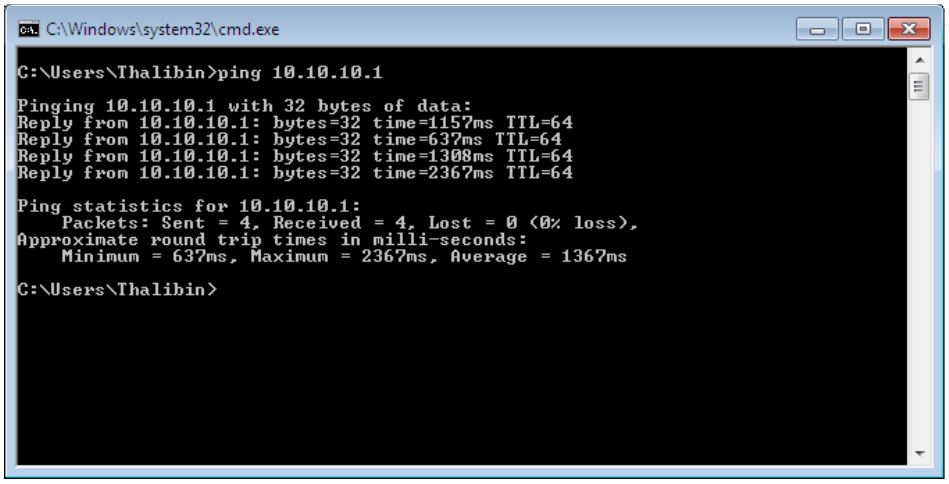
```
root@herwan-laptop:/etc/openvpn# ping 10.10.10.2
PING 10.10.10.2 (10.10.0.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.747 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.701 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.706 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=0.759 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=64 time=0.677 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=64 time=0.811 ms
64 bytes from 10.10.10.2: icmp_seq=7 ttl=64 time=0.675 ms
```

```
--- 10.10.0.6 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5997ms
rtt min/avg/max/mdev = 0.675/0.725/0.811/0.048 ms
```

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

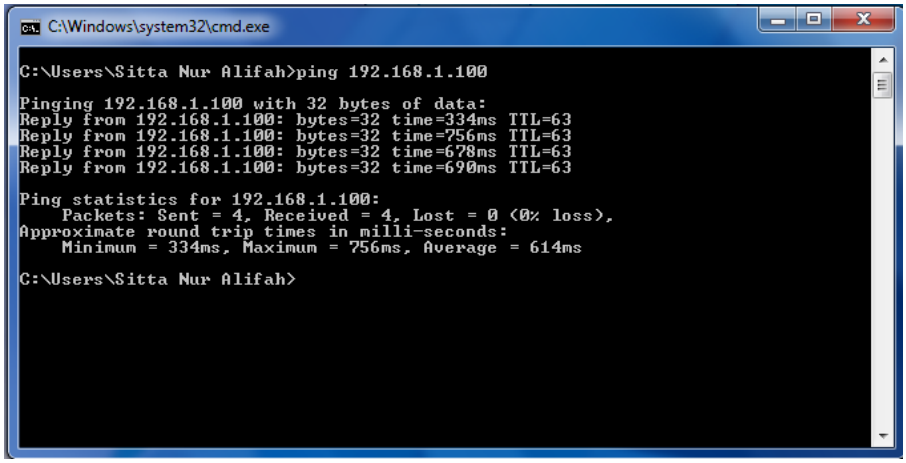
```
root@herwan-laptop:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.768 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.684 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.774 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.848 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=64 time=0.700 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=64 time=0.577 ms
64 bytes from 10.10.10.1: icmp_seq=7 ttl=64 time=0.711 ms
--- 10.10.10.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6000ms
rtt min/avg/max/mdev = 0.577/0.723/0.848/0.080 ms
```

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



Gambar 4.9 *Ping Ke VPN Server*

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



Gambar 4.10 *Ping Ke Server*

4.2.3.2 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(lengkap terdapat pada lampiran):

```
root@herwan-laptop:/etc/openvpn# tcpdump -ni tun0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 96 bytes
22:25:21.879305 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [S], seq 3752542502,
win 5840, options [mss 1352,sackOK,TS val 8537217 ecr 0,nop,wscale 6], length 0
22:25:21.889262 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [P.], seq 403:811, ack
350, win 108, options [nop,nop,TS val 8537219 ecr 8821608], length 408
22:25:21.891958 IP 10.10.10.1.80 > 10.10.10.6.44826: Flags [P.], seq 350:1250, ack
811, win 124, options [nop,nop,TS val 8821610 ecr 8537219], length 900
22:25:21.936907 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [P.], seq 811:1261, ack
1250, win 154, options [nop,nop,TS val 8537231 ecr 8821610], length 450
22:25:21.937920 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [.], seq 1250:2590, ack
1261, win 141, options [nop,nop,TS val 8821622 ecr 8537231], length 1340
22:25:21.937934 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [P.], seq 2590:2925,
ack 1261, win 141, options [nop,nop,TS val 8821622 ecr 8537231], length 335
22:25:21.944951 IP 10.10.10.6.44826 > 10.10.10.1.80: Flags [P.], seq 1261:1711,
ack 2925, win 241, options [nop,nop,TS val 8537233 ecr 8821622], length 450
22:25:21.949900 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [.], seq 2925:4265, ack
1711, win 158, options [nop,nop,TS val 8821625 ecr 8537233], length 1340
                                    .
                                    .
                                    .
                                    .
                                    .
22:25:21.950372 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [P.], seq 5605:5695,
ack 1711, win 158, options [nop,nop,TS val 8821625 ecr 8537233], length 90
22:25:22.146885 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [P.], seq 5275:5799,
ack 8497, win 628, options [nop,nop,TS val 8537283 ecr 8821646], length 524
22:25:22.148021 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [P.], seq 8497:8780,
ack 5799, win 292, options [nop,nop,TS val 8821674 ecr 8537283], length 283
22:25:22.164371 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [P.], seq 5799:6332,
ack 8780, win 670, options [nop,nop,TS val 8537288 ecr 8821674], length 533
22:25:22.164920 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [P.], seq 8780:9064,
```

```
ack 6332, win 309, options [nop,nop,TS val 8821679 ecr 8537288], length 284
22:25:22.170933 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [P.], seq 6332:6859,
ack 9064, win 712, options [nop,nop,TS val 8537290 ecr 8821679], length 527
22:25:22.171367 IP 10.10.10.1.80 > 10.10.10.2.44826: Flags [P.], seq 9064:9347,
ack 6859, win 325, options [nop,nop,TS val 8821680 ecr 8537290], length 283
```

Pada log diatas, tcpdump mencatat koneksi dari *server* ke *client* dan *port* yang di akses yaitu *port* 80(Web Server).

```
22:25:21.889262 IP 10.10.10.2.44826 > 10.10.10.1.80: Flags [P.],
seq 403:811, ack 350, win 108, options [nop,nop,TS val 8537219
ecr 8821608], length 408
```

Sedangkan tcpdump dari komputer *client* kepada komputer *server* untuk mengecek koneksi dan melihat paket data yang diambil dan *port* yang diakses oleh komputer *client*, tes koneksi tcpdump berhasil dilakukan dan menghasilkan log seperti yang ditunjukan dibawah ini(lengkap terdapat pada lampiran):

```
root@herwan-laptop:~# tcpdump -ni tun0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 96 bytes
22:10:19.041671 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.], seq 403:811, ack
350, win 108, options [nop,nop,TS val 8311578 ecr 8595901], length 408
22:10:19.047258 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [P.], seq 350:1250, ack
811, win 124, options [nop,nop,TS val 8595905 ecr 8311578], length 900
22:10:19.090832 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.], seq 811:1261, ack
1250, win 154, options [nop,nop,TS val 8311590 ecr 8595905], length 450
22:10:19.094259 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [.], seq 1250:2590, ack
1261, win 141, options [nop,nop,TS val 8595916 ecr 8311590], length 1340
22:10:19.098535 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.], seq 1261:1711,
ack 2925, win 241, options [nop,nop,TS val 8311592 ecr 8595917], length 450
22:10:19.106074 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [.], seq 2925:4265, ack
1711, win 158, options [nop,nop,TS val 8595919 ecr 8311592], length 1340
22:10:19.106236 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [.], seq 4265:5605, ack
1711, win 158, options [nop,nop,TS val 8595920 ecr 8311592], length 1340
22:10:19.168766 IP 10.10.10.1.80 > 10.10.10.2.44952: Flags [P.], seq 1383:1667,
ack 1504, win 141, options [nop,nop,TS val 8595935 ecr 8311609], length 284
22:10:19.178957 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.], seq 2752:3282,
ack 6264, win 415, options [nop,nop,TS val 8311612 ecr 8595933], length 530
22:10:19.182136 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [P.], seq 6264:6548,
ack 3282, win 208, options [nop,nop,TS val 8595938 ecr 8311612], length 284
22:10:19.228382 IP 10.10.10.2.44952 > 10.10.10.1.80: Flags [P.], seq 1504:1994,
ack 1667, win 206, options [nop,nop,TS val 8311624 ecr 8595935], length 490
22:10:19.233079 IP 10.10.10.1.80 > 10.10.10.2.44952: Flags [P.], seq 1667:1951,
ack 1994, win 158, options [nop,nop,TS val 8595950 ecr 8311624], length 284
                                        .
                                        .
                                        .
                                        .
                                        .
22:10:19.357616 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.], seq 3282:3806,
ack 6548, win 457, options [nop,nop,TS val 8311657 ecr 8595938], length 524
22:10:19.359389 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [P.], seq 6548:6831,
ack 3806, win 225, options [nop,nop,TS val 8595983 ecr 8311657], length 283
22:10:19.375879 IP 10.10.10.2.44952 > 10.10.10.1.80: Flags [P.], seq 1994:2527,
ack 1951, win 240, options [nop,nop,TS val 8311661 ecr 8595950], length 533
22:10:19.384168 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.], seq 3806:4333,
ack 6831, win 499, options [nop,nop,TS val 8311663 ecr 8595983], length 527
22:10:19.385049 IP 10.10.10.1.80 > 10.10.10.2.44952: Flags [P.], seq 1951:2235,
ack 2527, win 175, options [nop,nop,TS val 8595989 ecr 8311661], length 284
22:10:19.387455 IP 10.10.10.1.80 > 10.10.10.2.44951: Flags [P.], seq 6831:7114,
ack 4333, win 242, options [nop,nop,TS val 8595990 ecr 8311663], length 283
```

Pada log diatas, tcpdump mencatat koneksi dari *server* ke *client* dan *port* yang di akses yaitu *port* 80(Web Server).

```
22:10:19.041671 IP 10.10.10.2.44951 > 10.10.10.1.80: Flags [P.],
seq 403:811, ack 350, win 108, options [nop,nop,TS val 8311578
ecr 8595901], length 408
```

4.2.4 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*(192.168.1.100).



Gambar 4.11 *Koneksi Web Server*

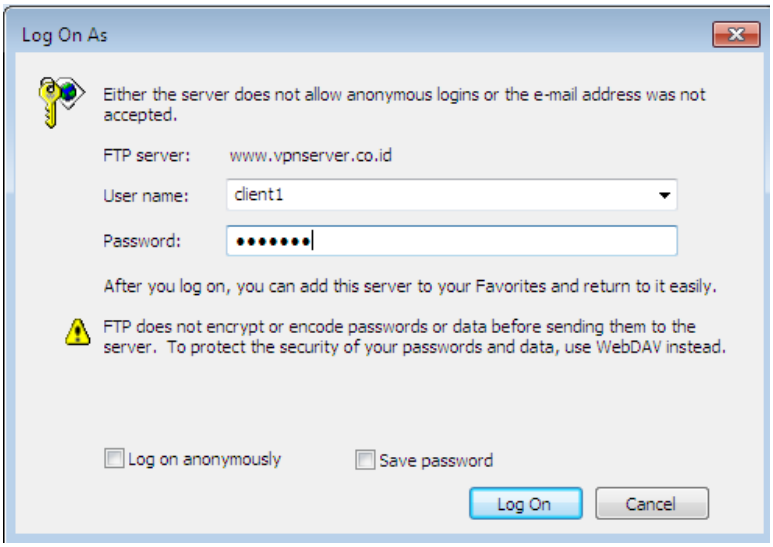
Sedangkan untuk akses web server yang terdapat pada komputer *server*, akses web server dapat dilakukan melaui web browser dengan mengetikan alamat

DNS dari komputer *server*, pengujian akses web server berhasil dan akan menampilkan hasil seperti yang ditunjukkan Gambar 4.12 dibawah ini:

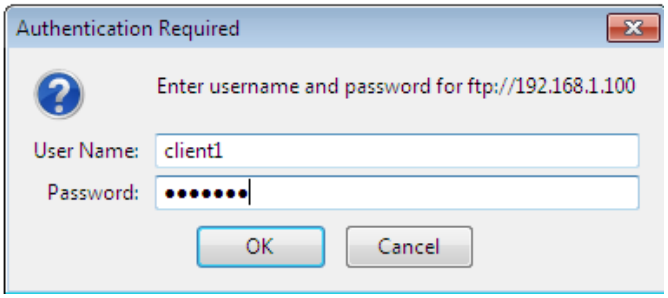


Gambar 4.12 *Akses Web Server Via DNS*

Pada akses ftp server, sebelum terkoneksi dengan ftp server, *client* akan diminta untuk mengisi autentikasi seperti yang ditunjukkan pada Gambar 4.13 di bawah ini:

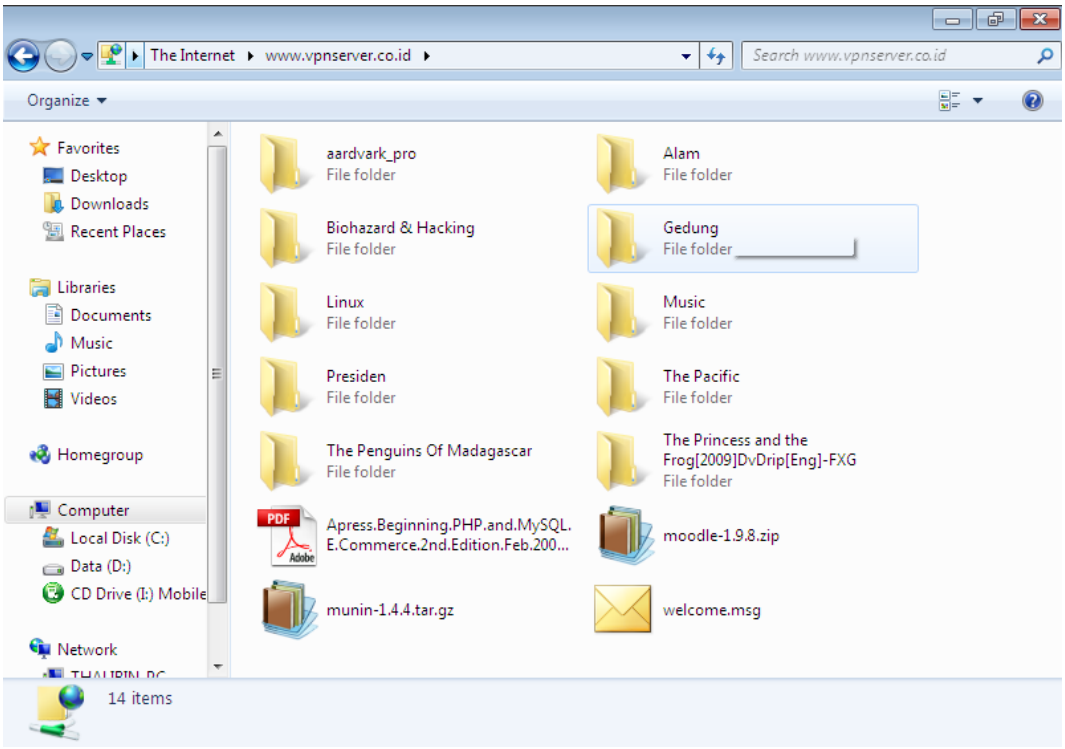


(a)

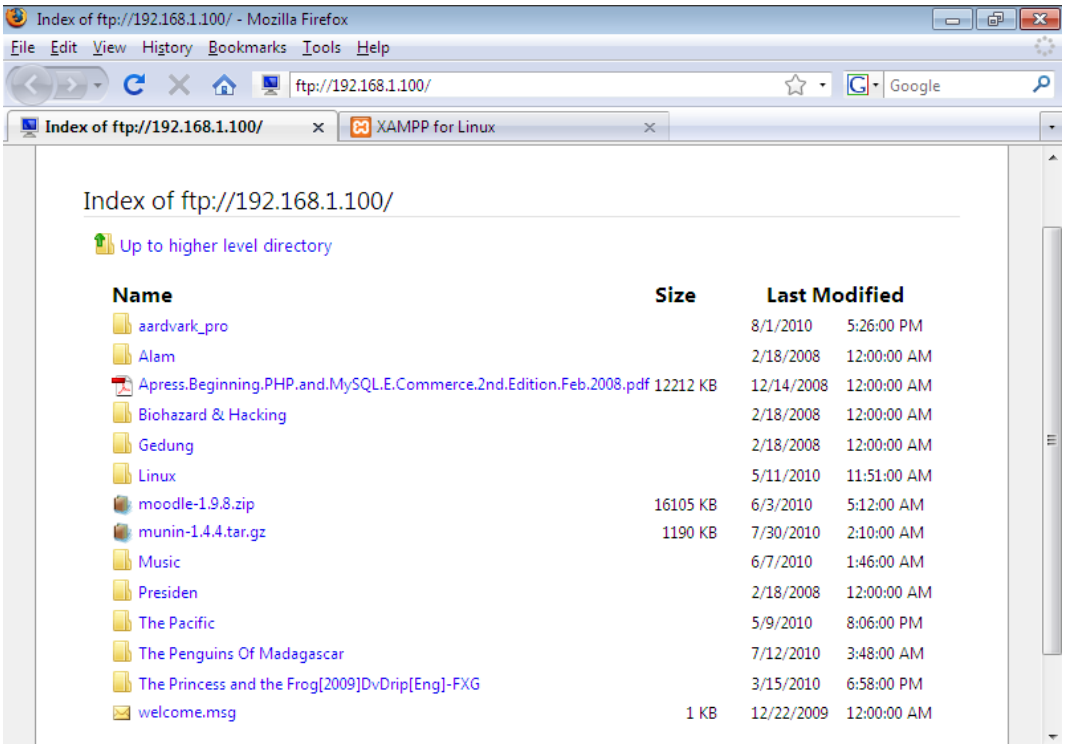


(b)

Gambar 4.13 *(a)autentikasi melalui windows explorer; (b)autentikasi melalui web browser*



(a)



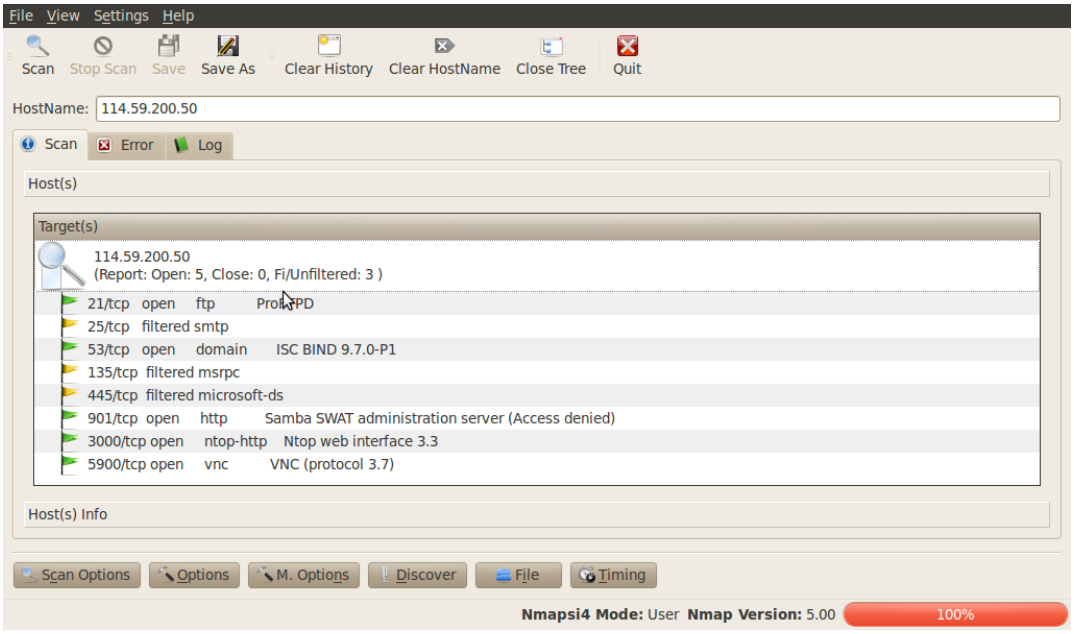
(b)

Gambar 4.14 *(a)akses melalui windows explorer; (b)akses melalui web browser*

Setelah login berhasil, maka *client* dapat mengakses layanan file pada ftp server.

4.2.5 Pengujian *Scanning Port*

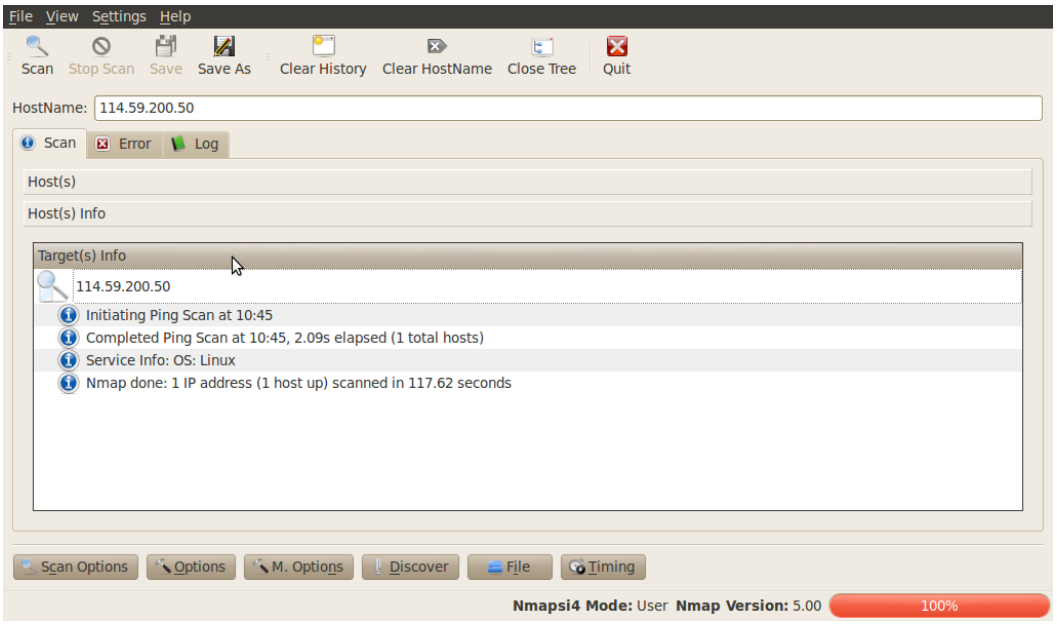
Pada pengujian *scanning port* dilakukan terhadap vpn *server* dengan menggunakan 2 mode, yaitu mode normal dan mode all, *scanning* dilakukan melalui akses internet terhadap vpn *server* menggunakan aplikasi Nmap, adapun hasil dari scanning *port* mode normal adalah sebagai berikut:



Gambar 4.15 *Scanning Port Mode Normal Host*

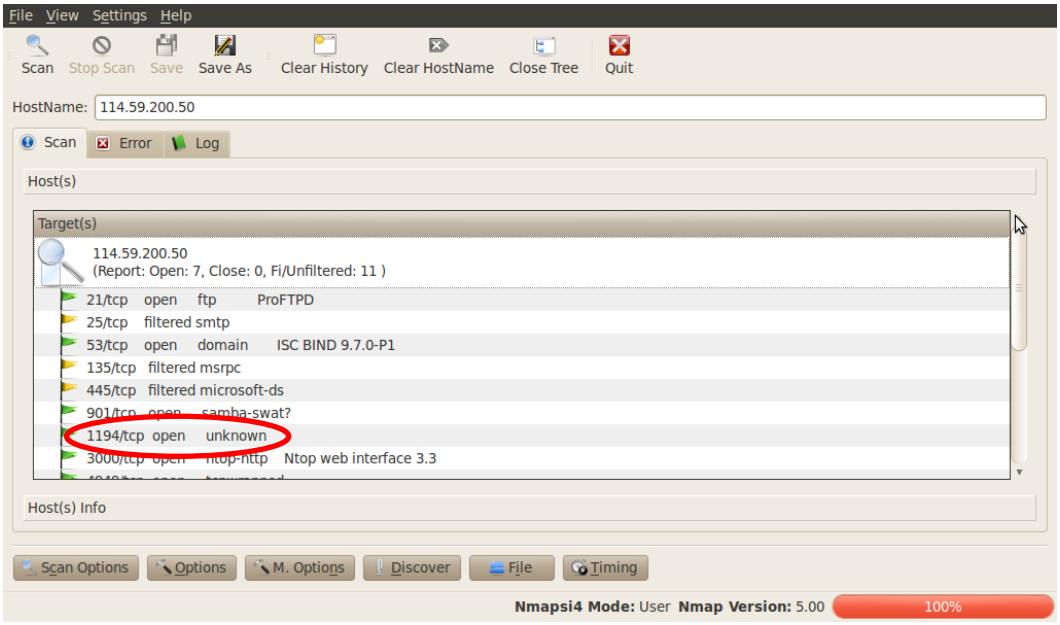
Pada hasil *scanning port* mode normal menunjukan bahwa terdapat 5 *port* yang terbuka, dan *port* VPN yang telah dibuat sebelumnya, yaitu *port* 1194 tidak tidak terdeteksi oleh Nmap.

Gambar 4.16 menunjukan informasi mengenai *host* yang dilakukan *scanning*.



Gambar 4.16 *Info Scanning Port Mode Normal*

Sedangkan apabila melakukan *scanning port* terhadap vpn *server* dengan menggunakan mode all, maka akan terdeteksi 7 *port* yang terbuka, dan *port* vpn *server* (1194) terdeteksi oleh aplikasi Nmap, akan tetapi, aplikasi Nmap tidak dapat mengetahui informasi *port* 1194 tersebut dengan memnentukan jenis *port*-nya merupakan *port unknown*.



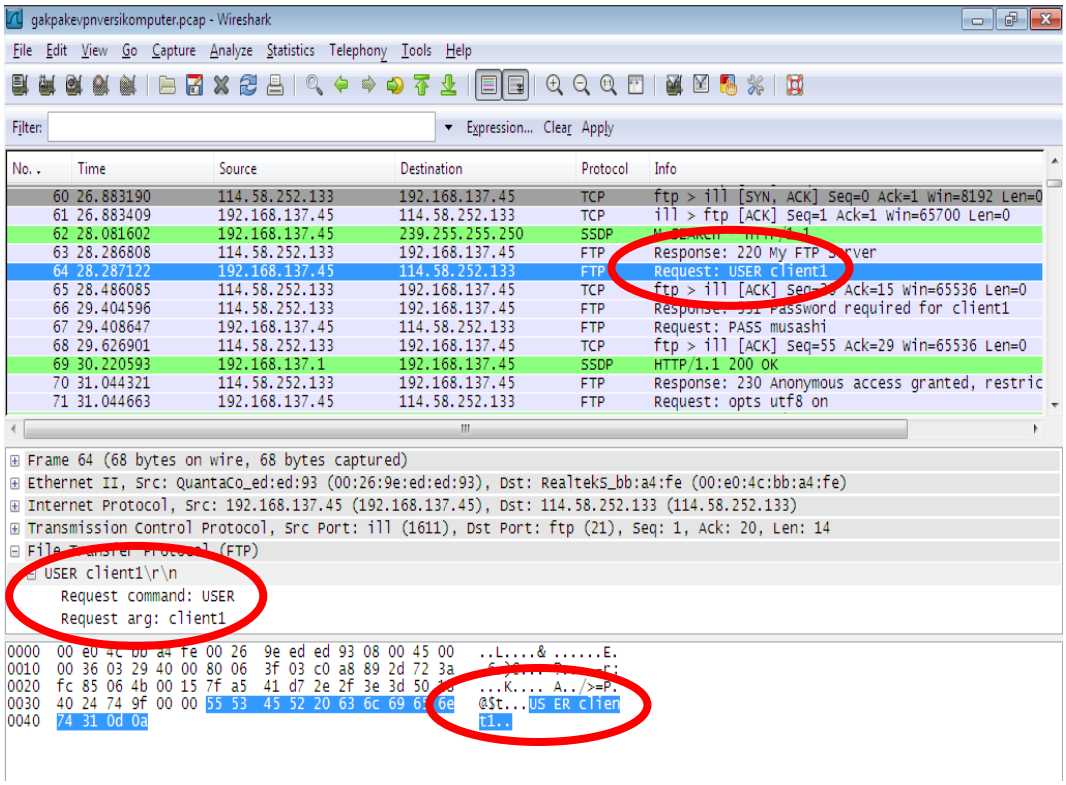
Gambar 4.17 *Scanning Port Mode All*

4.2.6 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

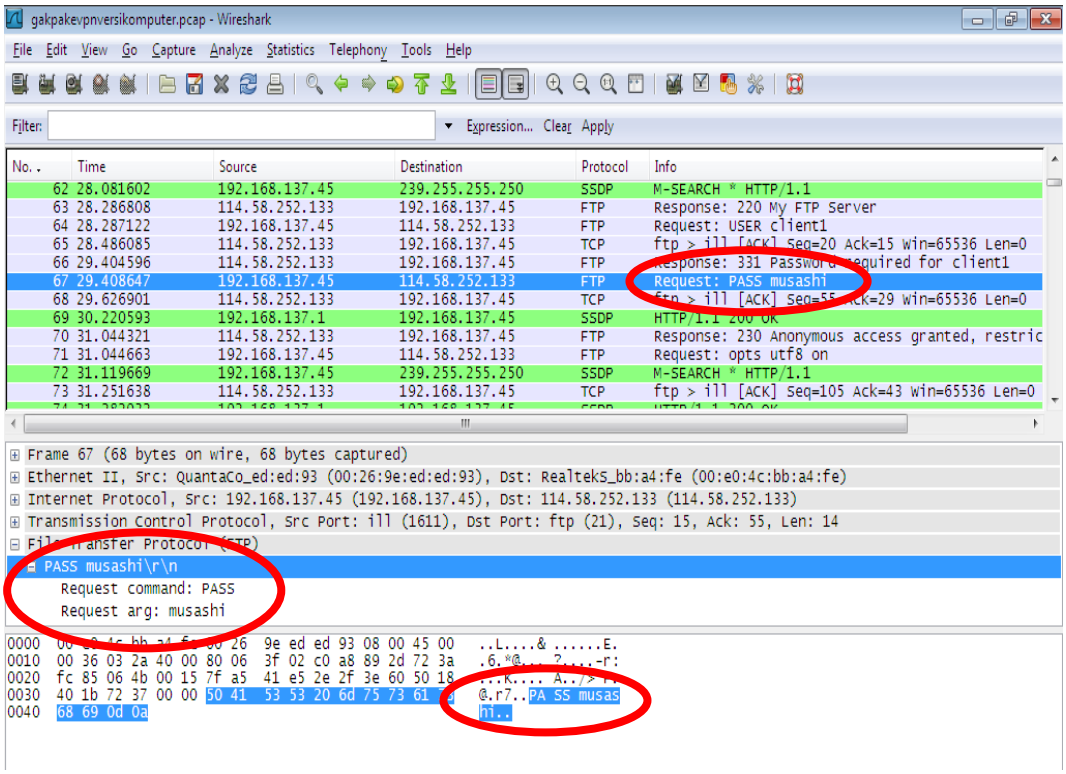
Monitoring data yang tidak melalui *remote access* vpn yang berbasis SSL, akan menampilkan hasil seperti yang ditunjukkan Gambar 4.18 sampai Gambar 4.20 berikut:



Gambar 4.18 *Monitoring Tanpa Melalui Remote Access VPN Berbasis SSL*

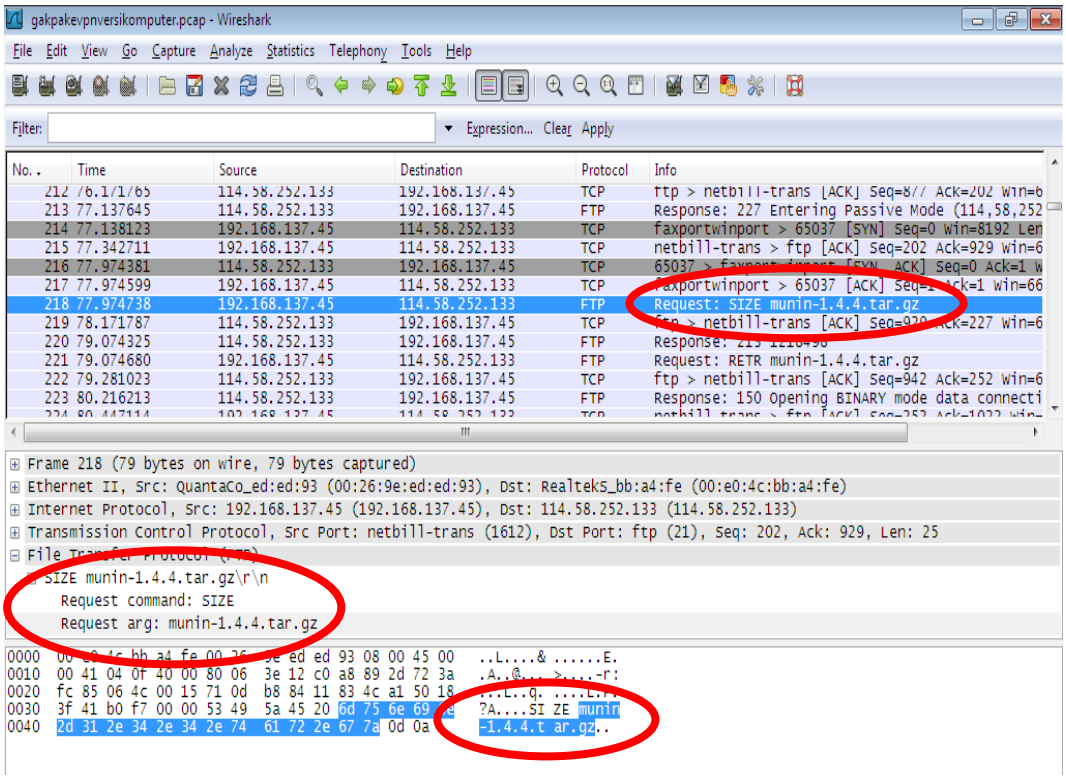
Pada gambar 4.18 menunjukkan bahwa *client* yang melakukan akses terhadap ftp server, dapat diketahui username yang melakukan akses terhadap ftp server.

Pada Gambar 4.19 menunjukkan bahwa user yang melakukan akses terhadap ftp server dapat juga diketahui password yang digunakan oleh user tersebut.



Gambar 4.19 *Monitoring Tanpa Melalui Remote Access VPN Berbasis SSL(2)*

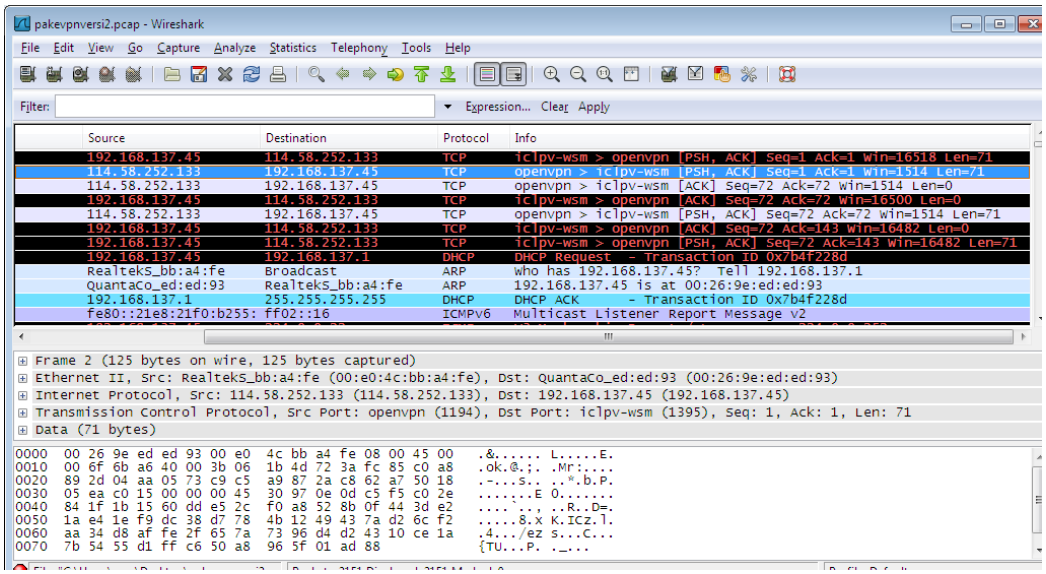
Pada gambar 4.20 menunjukan bahwa *client* yang melakukan akses terhadap ftp server, dapat diketahui pula file yang diakses oleh user yang melakukan akses terhadap ftp server.



Gambar 4.20 *Monitoring Tanpa Melalui Remote Access VPN Berbasis SSL(3)*

b. 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 4.21 dibawah ini:



Gambar 4.21 *Monitoring Data Melalui VPN*

Pada Gambar 4.21, 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 melaui *remote access virtual private network* yang berbasis *secure socket layer* menjadi aman.