BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini akan dilakukan implementasi dan pengujian terhadap sistem *site-to-site* VPN yang dibangun. Implementasi dilakukan berdasarkan analisis dan perancangan yang telah dibuat. Setelah implementasi selesai, maka selanjutnya akan dilakukan pengujian untuk mengetahui kinerja dari jaringan VPN yang telah dibangun.

4.1 Implementasi sistem

Setelah melalui tahap analisis dan perancangan selesai, selanjutnya sistem yang telah di rancang akan di implementasikan.

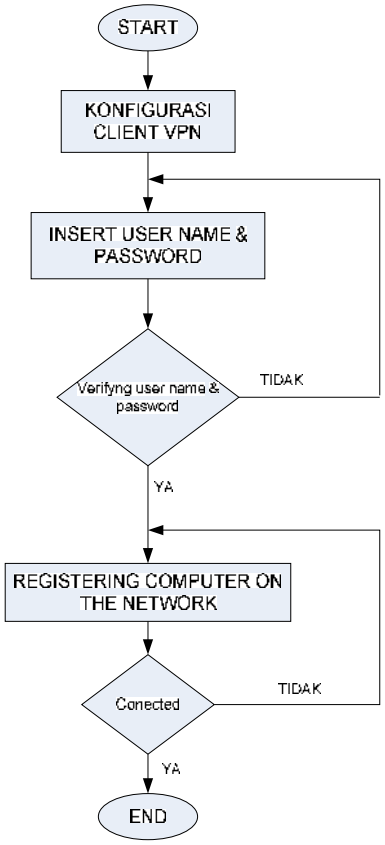
4.1.1 Konfigurasi client

Dalam mengkonfigurasi VPN *Client*, ada beberapa tahapan yang harus dilakukan diantaranya :

a. Tahap konfigurasi akses VPN.

b. Tahap *Connecting* VPN.

Untuk lebih memperjelas mengenai tahapan konfigurasi di sisi *client,* berikut akan disertakan gambar flowchart

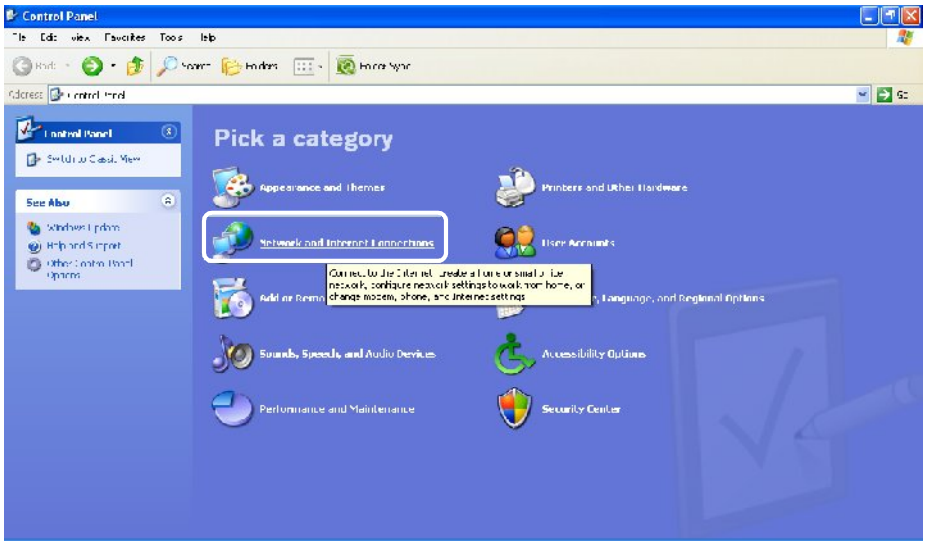


Gambar 4.1 Flowchart Konfigurasi *Client*

4.1.1.1 Tahap konfigurasi *client*

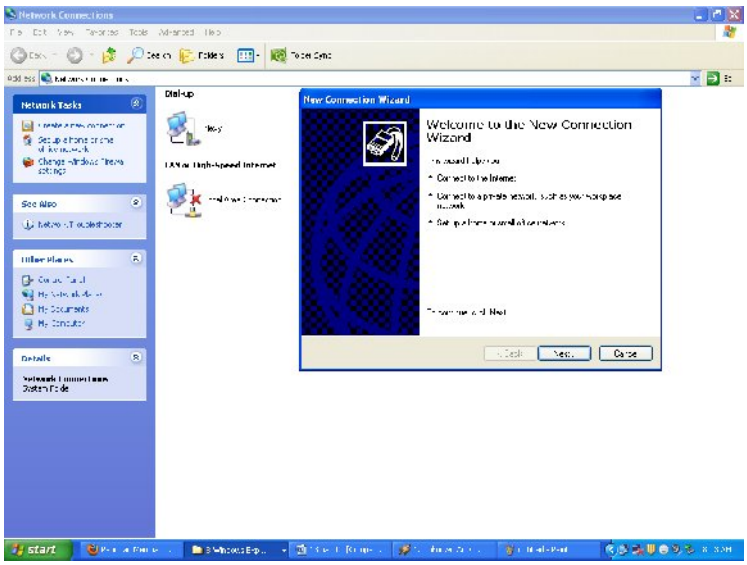
Untuk melakukan koneksi *client* dengan VPN *server* dibutuhkan beberapa tahapan konfigurasi pada komputer *client*, berikut adalah konfigurasi *client* VPN menggunakan Mocrosoft Windows XP SP3.

1. Masuk ke windows control panel kemudian klik *network and internet connections* seperti gambar dibawah.



Gambar 4.2 Windows control panel

2. Klik *network conecctions* kemudian Pilih " Buat koneksi baru dari sisi kiri jendela windows xp *new connection wizard* seperti gambar dibawah :



Gambar 4.3 Membuat koneksi baru VPN client

3. Tekan tombol next untuk memulai wizard, lalu pilih '*Connect to the at my workplace*' dari daftar dan klik *next.*



Gambar 4.4 Pemilihan type koneksi

4. Pada halaman koneksi jaringan *wizard*, pilih pilihan 'koneksi *virtual private network*' dan klik *next.*



Gambar 4.5 Pemilihan koneksi jaringan

4 Masukan nama untuk sambungan VPN, dalam penelitian ini peneliti menggunakan nama perusahaan (PT. Icky Corp) dan klik *next*.



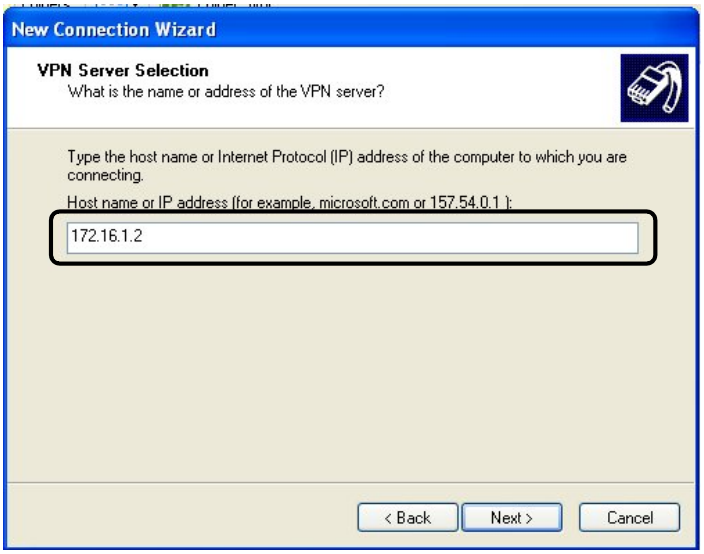
Gambar 4.6 Penamaan koneksi jaringan VPN

5 Kemudian pada 'layar jaringan publik' pilih *do not dial the initial connection* dan klik next. Pilihan default *automatically dial this initial connection,* dapat digunakan jika koneksi VPN akan dimulai pada saat komputer terhubung ke internet. Jika tidak, pilih opsi *do not dial the initial connection*.



Gambar 4.7 Pemilihan jaringan publik

6 Masukan *IP address* dari *serve*r VPN untuk terhubung, dan klik *next.*



Gambar 4.8 Memasukan *IP address server* VPN

7 Klik *finish* untuk menyelesaikan *wizard*. Informasi koneksi VPN baru telah disimpan.

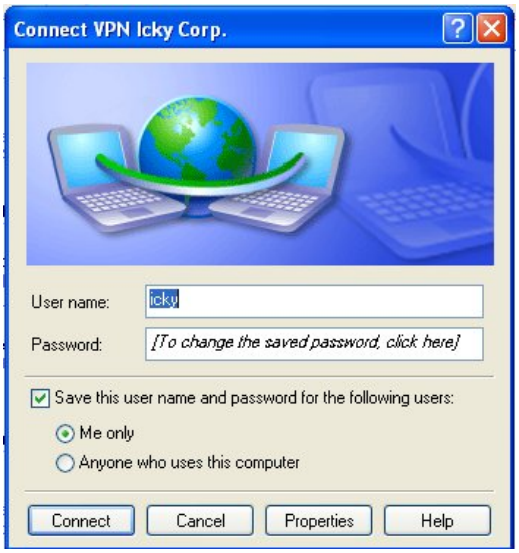


Gambar 4.9 *Finishing* dan Pembuatan shortcut

4.1.1.2 Tahap dialing VPN / koneksi VPN

Langkah selanjutnya adalah koneksi ke *server* VPN. Adapun langkah-langkahnya sebagai berikut :

1. Double klik pada kotak dialog *network connection* atau pilih *connect* dari menu, akan muncul seperti gambar di bawah



Gambar 4.10 *Dialog Network connection*

2. Masukan *user name* dan *password* yang sudah terdaftar di VPN server, kemudian klik *connect*.

   Proses *verifying username* dan *password*



Gambar 4.11 Dialog *verifying username and password*

Proses *Authetincated* komputer pada jaringan



Gambar 4.12 Dialog *Authenticated computer*

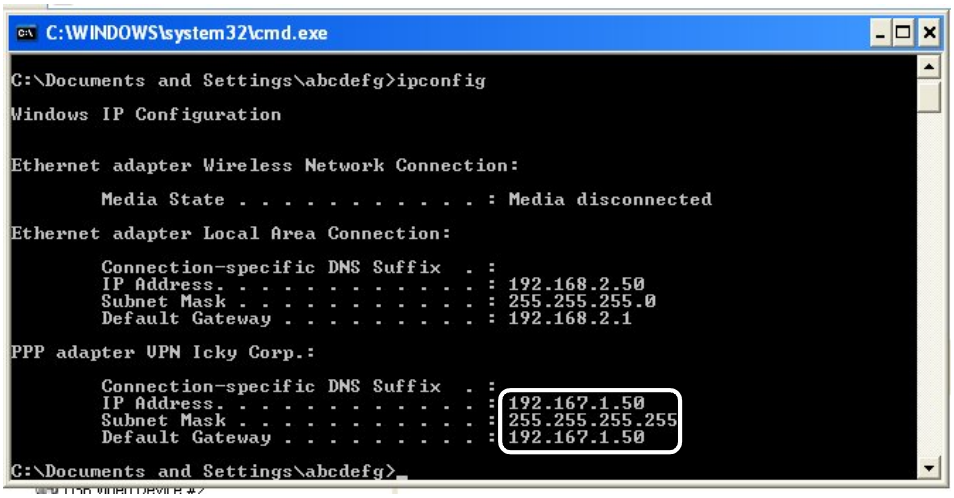
Setelah proses *Authentication* sukses, maka VPN Icky Corp. sudah terkoneksi dan muncul ikon seperti dibawah ini.



Gambar 4.13 Informasi koneksi VPN

4.1.1.3 Tahap Ping Test

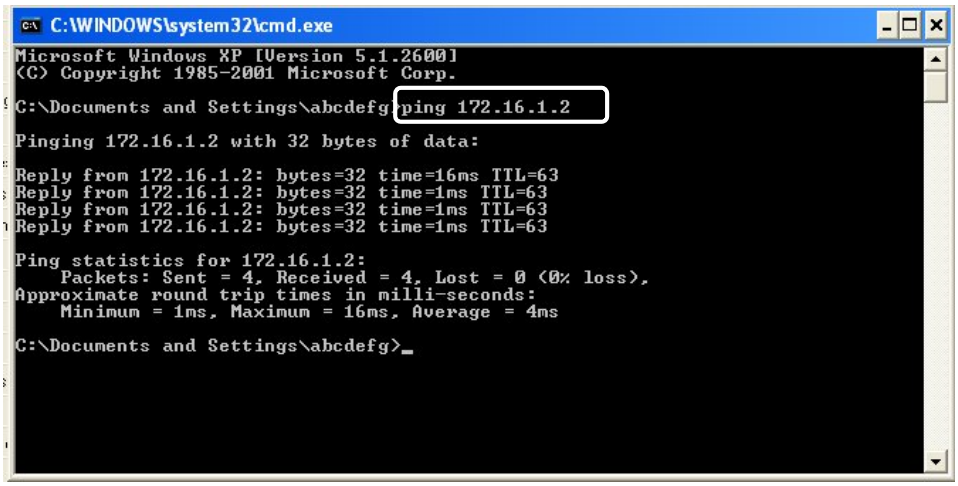
Setelah proses *dial* atau *connect* ke VPN untuk membuktikan koneksi VPN berjalan, maka selanjutnya akan dilakukan pengujian koneksi. Pertama kita chek *IP address* yang didapat dengan cara ketik ipconfig di *command promt*.



Gambar 4.14 Cek IP Address dengan Ipconfig

Setelah proses ipconfig, dapat diketahui bahwa *ip address* yang didapat oleh *client* VPN adalah 192.167.1.50 untuk koneksi saat ini, ip address yang didapat bisa berubah – ubah karena VPN *server* menggunakan DHCP *server Range IP address* untuk VPN adalah 192.167.1.1-192.167.1.50

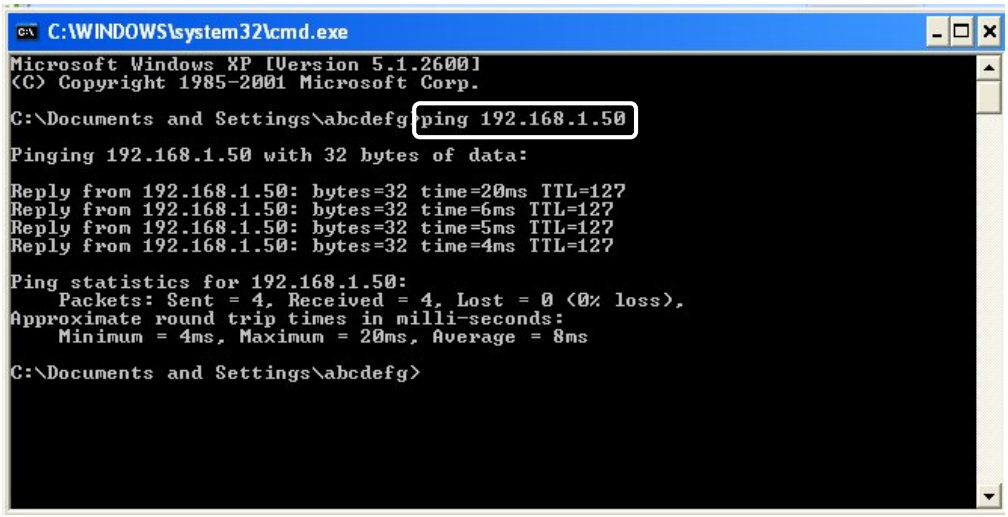
Tahap selanjutnya pengujian koneksi dengan tes ping ke *IP adress server* VPN yang mempunyai IP address 172.16.1.2 seperti gambar di bawah.



Gambar 4.15 Cek IP Address ke *server* VPN

Gambar diatas menunjukkan bahwa *client* telah terkoneksi dengan VPN *server.*

Selanjutnya, kita akan melakukan pengujian koneksi dengan *file server* yaitu dengan melakukan ping IP address *file server* yang memiliki IP Address 192.168.1.50. Berikut tampilan pada saat dilakukan *test ping* :

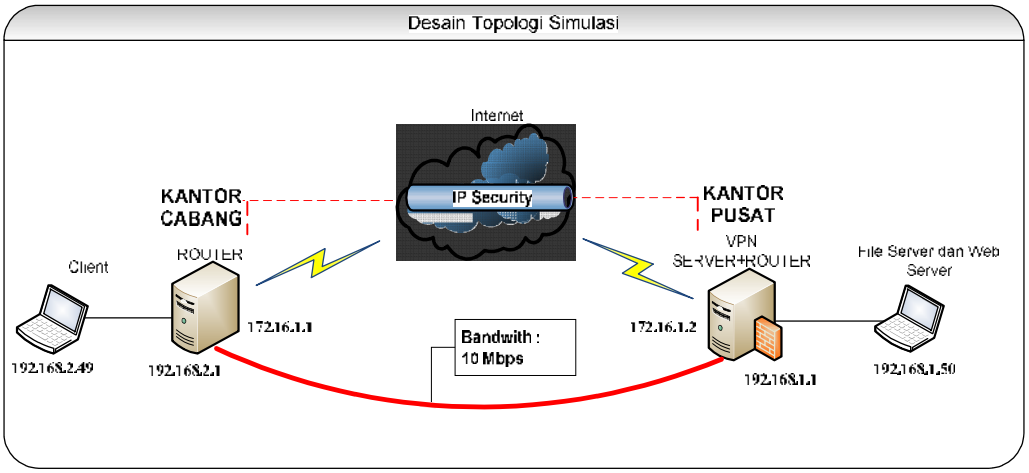


Gambar 4.16 Ping Tes ke *File server*

4.2 Pengujian sistem

4.2.1 Simulasi *site-to-site* VPN

Pada tahap pengujian ini, akan dilakukan simulasi *site-to-site* VPN kemudian dilakukan pengujian dengan beberapa skenario. Simulasi akan dilakukan melalui jaringan LAN, dan adapun desain topologi jaringan yang digunakan adalah sebagai berikut :



Gambar 4.17 Desain Topologi Simulasi

Perangkat pendukung pada simulasi diatas terdiri dari beberapa *hardware* dan *software* yang tertera dalam tabel di bawah ini :

Tabel 4.1 Perangkat Pendukung infrastruktur Simulasi

Hardware	PC Sebagai *Server* VPN dan Router
	PC Sebagai Router
	Laptop sebagai File S*erver*
	Laptop sebagai *Client* VPN
	Kabel UTP category 5e dan konektor RJ-45.
Software	Mikrotik Router OS v. 2.9.27 sebagai *server* VPN dan Router
	Windows 7 ultimate sebagai *server* dan Windows XP SP 3 sebagai *client*
	Wireshark –win32- 1.2.9 sebagai *protocol analyzer*
	Xampp for windows 1.6.5 (Web *server*)
	File zilla (FTP *Server*)
	RaidenDNSD 1.3.17 (DNS *server*)

Selain kebutuhan *hardware* dan *software* yang tertera pada tabel di atas, terdapat pembagian alokasi IP address yang tertera dalam tabel di bawah ini :

Selain kebutuhan *hardware* dan *software* yang tertera pada tabel di atas, terdapat pembagian alokasi IP address yang akan digunakan pada saat simulasi. Pada server VPN telah dilakukan konfigurasi DHCP, sehingga IP Address *client* akan bersifat dinamis. Dibawah ini merupakan tabel alokasi IP Address pada saat simulasi:

Tabel 4.2 Alokasi IP address untuk Router

Device	IP Address	Interface
PC sebagai VPN router	192.168.2.1	Lokal
	172.16.1.1	Publik
Laptop sebagai VPN *client*	192.167.1.50	Lokal

Tabel 4.3 Alokasi IP address untuk *Server* VPN dan File *Server*

Device	IP Address	Interface
PC sebagai VPN *Server* + router	192.168.1.2	Lokal
	172.16.1.2	Publik
Laptop sebagai HFS	192.168.1.50	Lokal

4.2.2 Skenario pengujian

Pada pengujian sistem ini, akan dilakukan pembuktian terhadap konektifitas dan kehandalan VPN berbasis IPSec. Adapun skenario-skenario yang akan dilakukan yaitu :

1) Menguji konektivitas VPN:

   a. Mengakses web *server*

   b. Melakukan *download* file dari file *server* menggunakan FTP *service*

2) Menguji kehandalan VPN:

   a. Melakukan *download* file melalui VPN, kemudian melakukan monitoring data menggunakan wireshark

   b. Melakukan *download* file tanpa VPN, kemudian melakukan monitoring data menggunakan wireshark

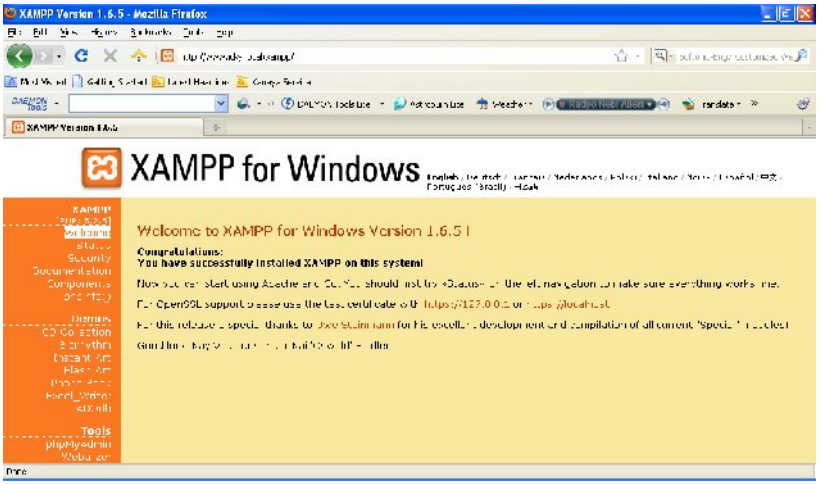
   c. Menganalisis perbandingan data layanan VPN dengan tanpa VPN

4.2.3 *Capture* skenario pengujian

1) Menguji konektivitas VPN:

   a. Mengakses web *server*

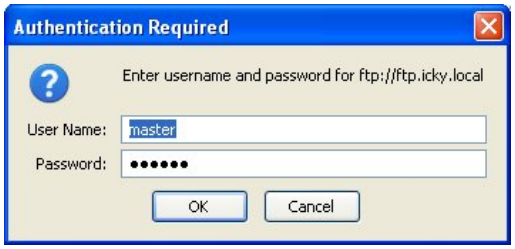
   Dibawah ini merupakan gambar pada saat user mengakses web *server*



Gambar 4.18 Tampilan interface web *server*

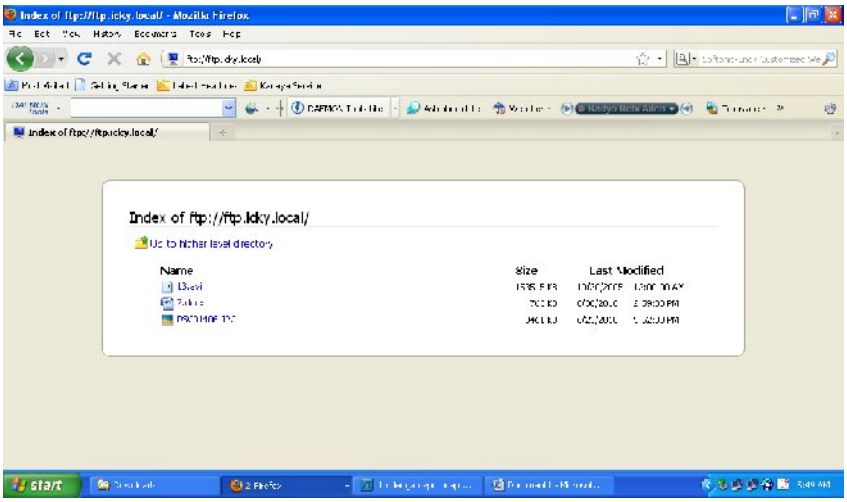
b. Melakukan *download* file dari file *server* menggunakan FTP *service*

Dibawah ini merupakan gambar pada saat user mengakses file *server*



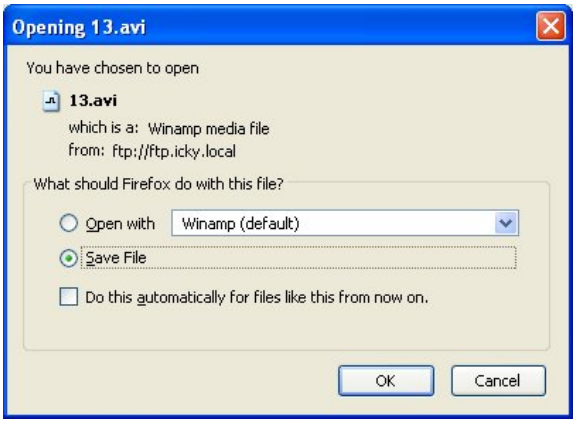
Gambar 4.19 Login FTP

Setelah user mengisi user name dan password, maka user akan masuk ke direktori *file server,* seperti gambar dibawah ini :

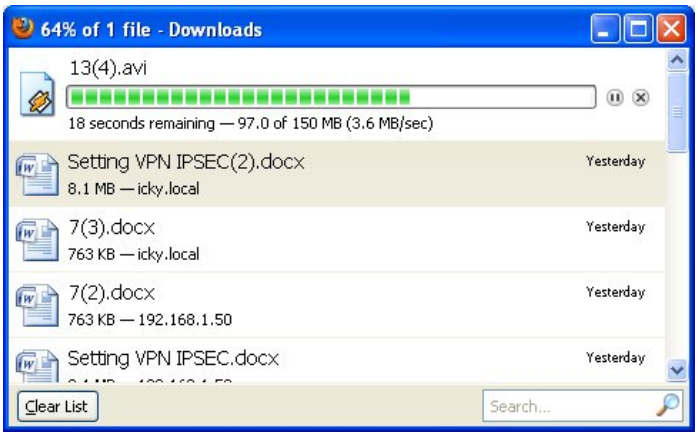


Gambar 4.20 Direktori *file server*

User dapat melakukan *download* pada file yang diinginkan, seperti pada gambar dibawah ini :



Gambar 4.21 Proses penyimpanan file

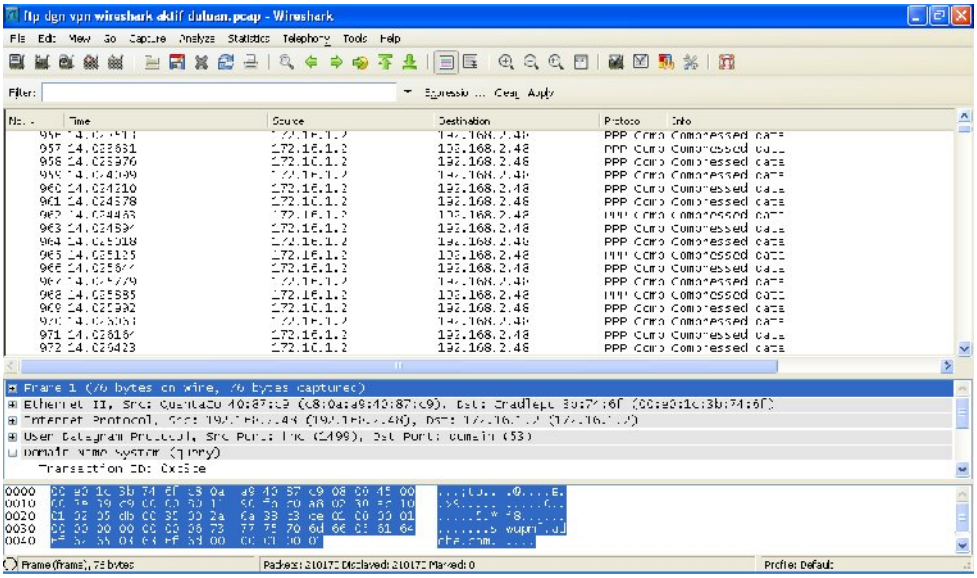


Gambar 4.22 Proses *download* file

2) Menguji kehandalan VPN:

Untuk dapat menguji kehandalan VPN berbasis IPsec, diperlukan analisa mengenai perbandingan data yang diperoleh dari monitoring FTP *service* melalui VPN dan tanpa VPN.

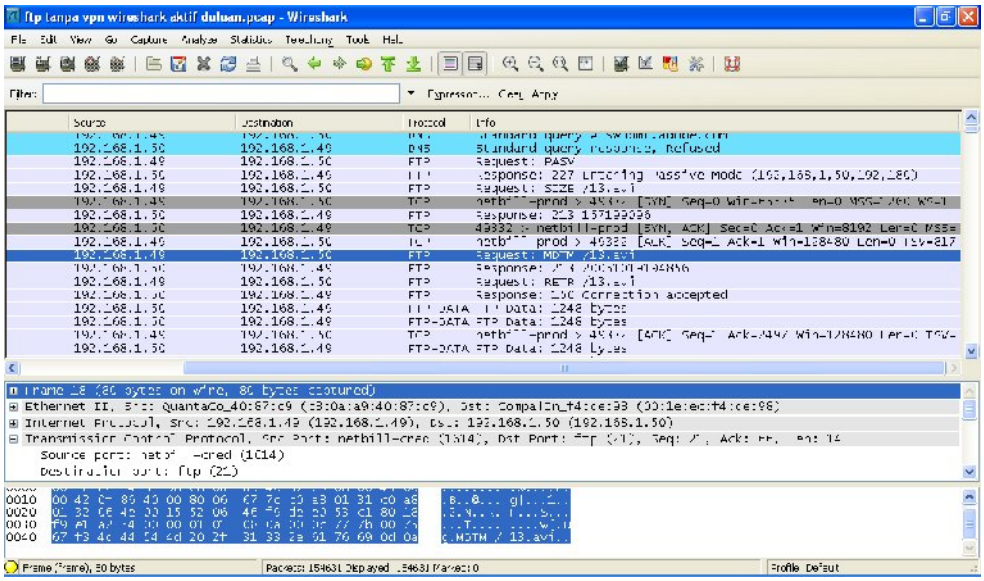
a. Dibawah ini merupakan gambar monitoring data melalui VPN



Gambar 4.23 Monitoring data melalui VPN

Hasil monitoring data diatas menyimpulkan bahwa, dengan teknologi VPN, protokol FTP tidak dapat di monitor dan data yang di transmisikan melalui *tunnel* mengalami kompresi dan file terenkripsi. Dengan demkian VPN terbukti dapat meningkatkan keamanan dalam transmisi data.

b. Dibawah ini merupakan gambar monitoring tanpa melalui VPN



Gambar 4.24 Monitoring data tanpa melalui VPN

Hasil monitoring data diatas menyimpulkan bahwa, ketika file ditransmisikan tanpa melalui VPN, protokol FTP dapat di monitor dan data yang di transmisikan dapat dilihat dengan jelas.