BAB 4
IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Tahapan implementasi sistem merupakan tahap penerjemahan perancangan berdasarkan hasil analisis serta penerapan kebutuhan pada keadaan yang sebenarnya. Tahapan ini terdiri dari dua bagian yaitu implementasi *firewall* dan VPN pada sistem operasi IPCop.

4.1.1 Implementasi Perangkat Keras

Implementasi perangkat keras merupakan proses yang digunakan dalam implementasi kebutuhan, tujuannya adalah agar dapat mengoptimalkan performansi *firewall* dan VPN dalam penelitian. Berikut spesifikasi perangkat keras yang digunakan:

a. Spesifikasi Komputer *Server*

Tabel 4.1 Spesifikasi Komputer *Server*

Spesifikasi	Keterangan
Processor	Pentium 4
RAM	512 MB
Harddisk	80 GB
Sistem Operasi	IPCop (Linux)

b. Spesifikasi Komputer Client

Tabel 4.2 Spesifikasi Komputer *Client*

Spesifikasi	Keterangan
Processor	Pentium 4
RAM	512 MB

Harddisk	**40GB**
Sistem Operasi	**Windows 7, Windows XP**

4.1.2 Implementasi Perangkat Lunak

Implementasi perangkat lunak merupakan proses instalasi komponen-komponen perangkat lunak, sehingga dapat beroperasi dengan benar. Berikut ini merupakan perangkat lunak yang digunakan :

Tabel 4.3 Spesifikasi Perangkat Lunak

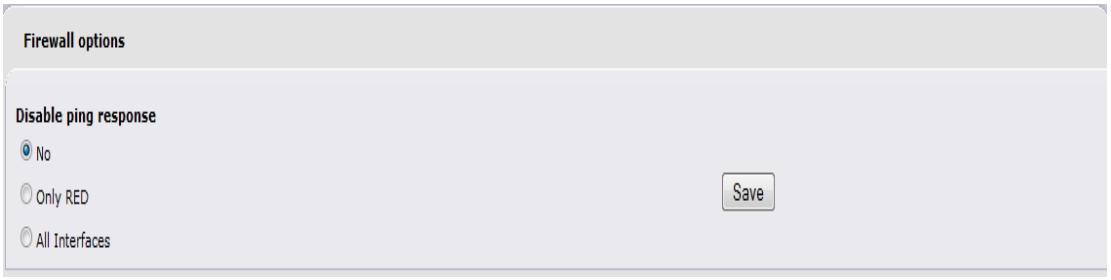
Spesifikasi	*Server*	Client
Sistem Operasi	IPCop (Linux)	Windows xp, Windows 7, Linux
Perangkat Lunak Pendukung	-	Putty, WinSCP
Web Browser	Mozilla Firefox dan google chrome	Mozilla Firefox dan Google chrome

4.1.3 Implementasi Firewall

Setelah mengetahui pengkat keras dan perangkat lunak yang dibutuhkan, maka selanjutnya akan dilakukan tahap konfigurasi *firewall* pada IPCop. Berikut adalah tahapan konfigurasi berdasarkan hasil analisis yang telah dilakukan sebelumnya.

Konfigurasi Firewall Administrasi Halaman Web

Bagian pertama memungkinkan untuk mengontrol akses administratif melalui https ke jaringan tertentu seperti RED dan All Interface yang tersedia.



Gambar 4.1 Firewall Options

Centang di samping untuk setiap antarmuka jaringan yang akan digunakan untuk akses administratif.

Aturan tambahan untuk menciptakan aturan-aturan firewall. Seperti Opsi untuk membatasi penebangan, pilihan untuk menambah jangka waktu ketika aturan akan aktif, membuat aturan untuk antarmuka, menambahkan *Source Port* aturan, dan menambahkan kemungkinan untuk 'membalikkan' *Source, Destination, Source Port* dan Layanan *Destination.*

Menetapkan nama-nama ke IP Address, jika menggunakan DHCP dapat menggunakan *Blue Network*, dan dapat mengizinkan semua perangkat untuk menghubungkan dan mengakses jaringan *Red*, harus menambahkan sebuah entri untuk setiap alamat IP dalam rentang DHCP yang akan digunakan ke daftar ini. Biarkan kolom Address MAC kosong ketika menambahkan setiap IP Address.

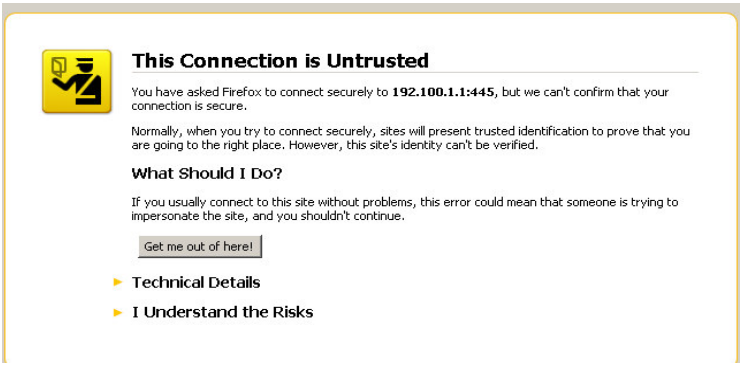


Gambar 4.2 Firewall Add New Rule

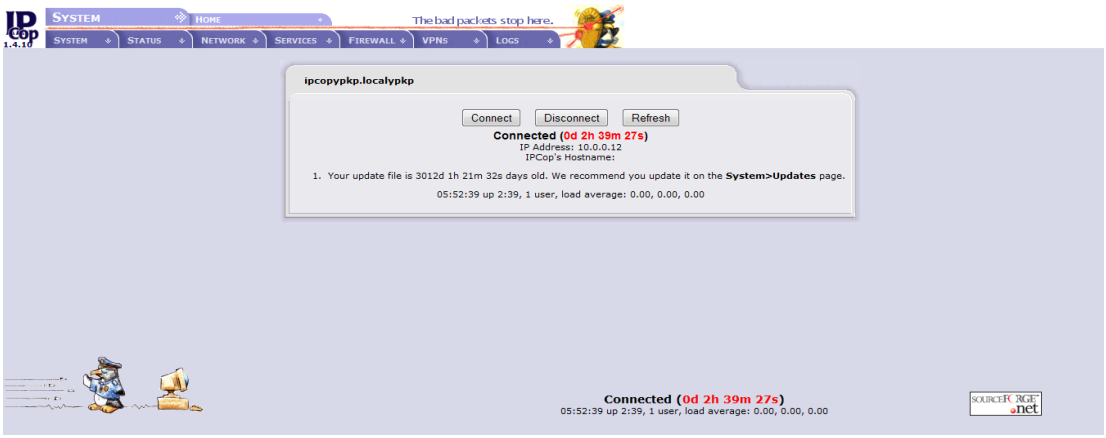
4.1.4 Implementasi VPN

Penggunaan IPCop sebagai *server* Universitas Sangga Buana YPKP Bandung memerlukan sedikitnya dua buah kartu jaringan sebagai penghubung antara jaringan lokal dengan jaringan publik. Kemudahan IPCop dan paket-paket yang sudah terangkum pada satu sistem sehingga menambah nilai tersendiri dalam penggunaan IPCop sebagai *server* VPN.

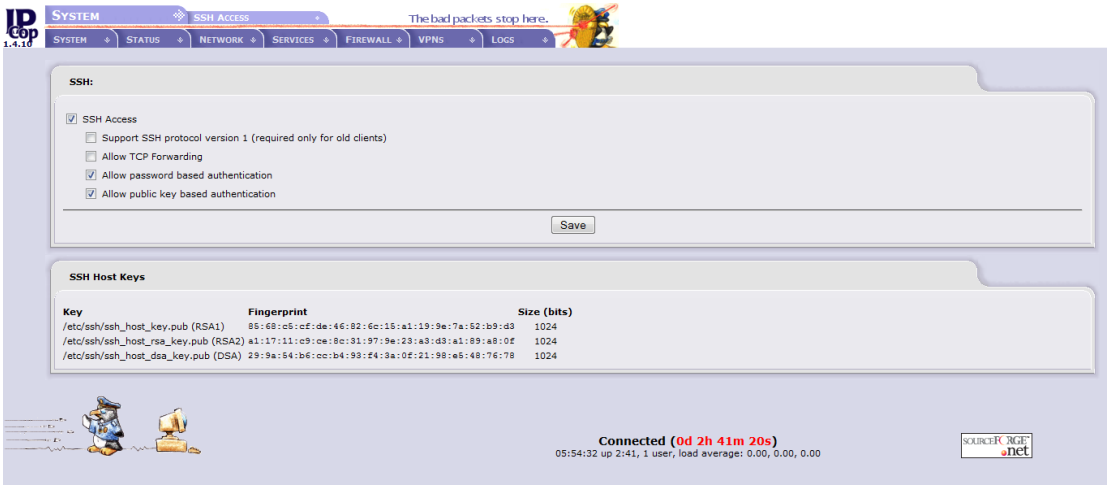
Akses pada *server* sendiri dapat dilakukan hanya sebatas pada proses instalasinya saja, setelah proses instalasi selesai konfigurasi selanjutnya dapat dilakukan secara *remote* pada komputer *client* yang akan melakukan koneksi lokal VPN dengan membuka aplikasi *browser* pada komputer *client* dan masuk ke halaman *website* dari IPCop tersebut dengan mengetikkan IP *interface* lokal (*green interface*), contohnya seperti https://192.168.0.89:445, jika muncul pernyataan tentang keamanan koneksi klik pada *I Understand the Risk* dan masuk sebagai *administrator* serta aktifkan SSH dengan memberi tanda *check* pada kotak SSH *Access*. Gambar berikut merupakan langkah-langkah konfigurasi dalam membangun koneksi VPN *server* dengan *client* yang akan dibangun di Universitas Sangga Buana YPKP Bandung.



Gambar 4.3 *Security Connection.*

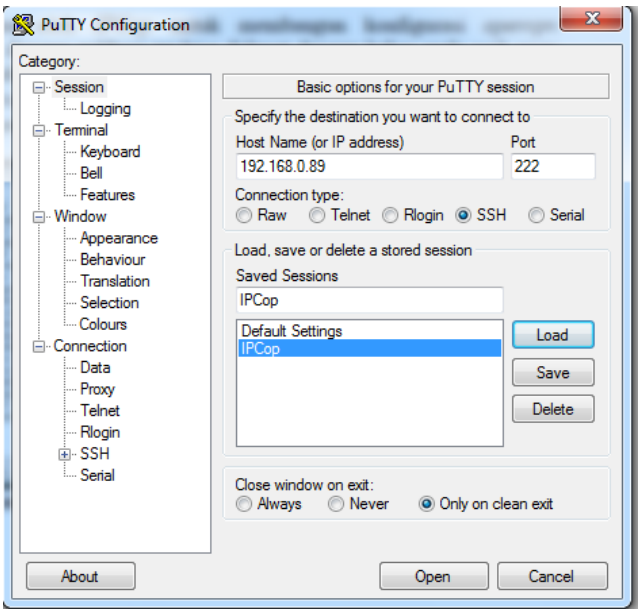


Gambar 4.4 Tampilan Halaman Awal IPCop *Web Browser*.

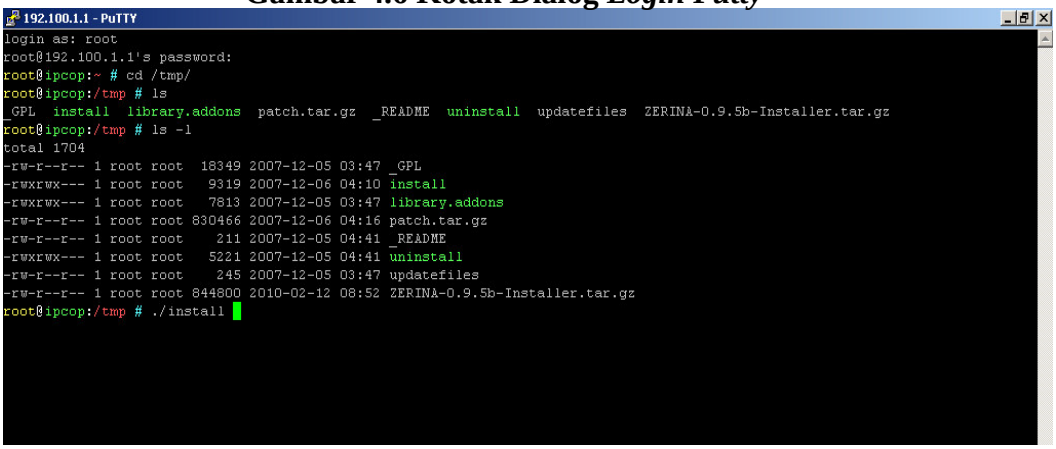


Gambar 4.5 Tampilan *System SSH*.

Tools yang digunakan oleh IPCop untuk membangun konfigurasi openvpn menggunakan aplikasi zerina, dimana aplikasi ini bisa didapat dengan bebas pada *web open source*. Membuka *port ssh* pada ipcop memungkinkan akses melalui komputer *client* untuk proses *install* aplikasi *zerina* yang akan digunakan membangun openvpn dengan menggunakan *tools* bantuan seperti *putty* dan *login* sebagai *root*.

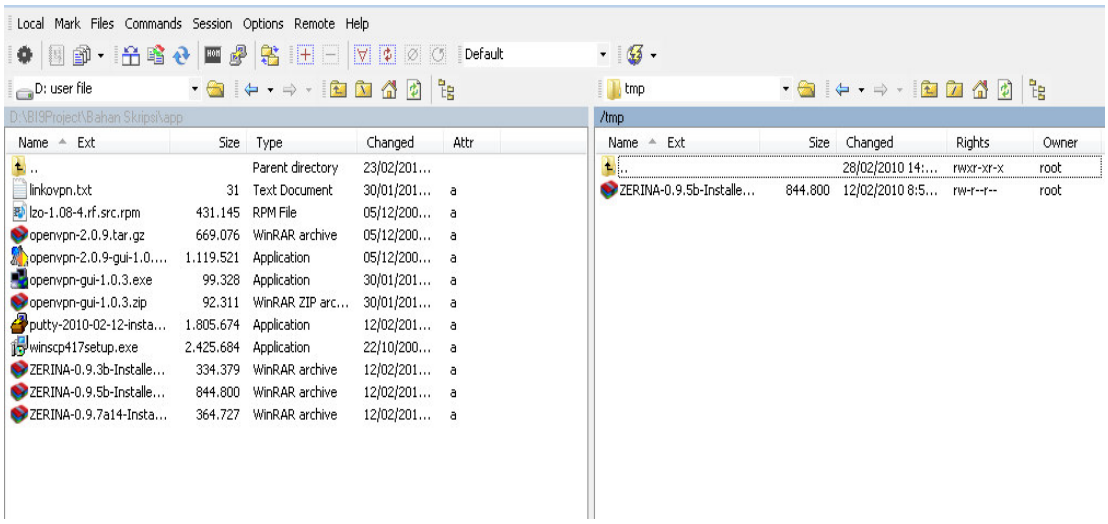


Gambar 4.6 Kotak Dialog *Login Putty*



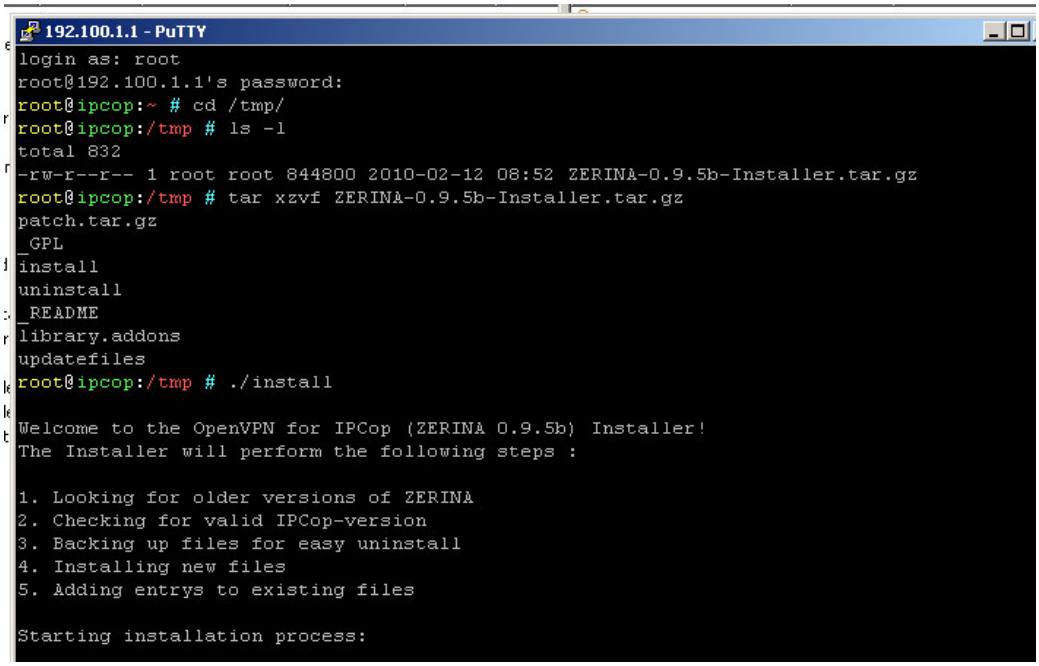
Gambar 4.7 Tampilan Awal *Putty*

Pemindahan *file* yang diperlukan dalam membangun konfigurasi openvpn ini dibantu dengan *Winscp* sebagai perantara antara sistem pada server maupun pada *client.*



Gambar 4.8 Penggunaan *Winscp*

Sebelum dilakukan instalasi aplikasi zerina ditempatkan sementara pada direktori /tmp pada server ipcop untuk kemudian di ekstrak lalu *install* dengan perintah : # tar xzvf ZERINA-0.9.5b-Installer.tar.gz # ./install

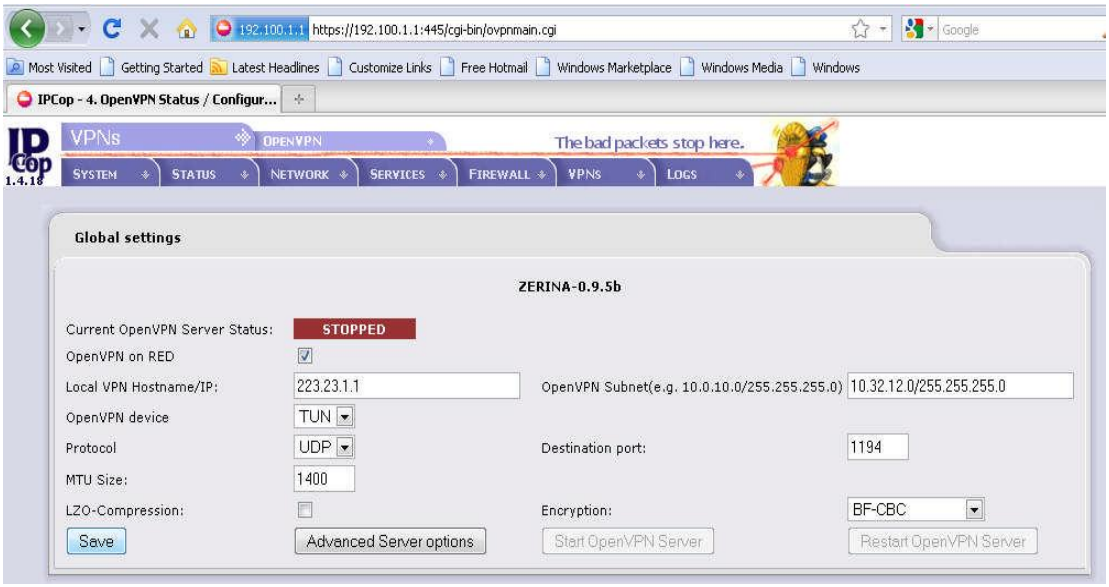


Gambar 4.9 Proses *Install Zerina*

Proses *install* aplikasi untuk openvpn pada ipcop yang telah selesai akan menambah satu *tool* pada menu *drop down* VPNS yang dapat dilihat pada tampilan *browser*, dan untuk memulai konfigurasi vpn klik openvpn pada menu *drop down* sehingga *browser* akan memulai tampilan awal dari aplikasi *zerina*.



Gambar 4.10 Tampilan Utama Web IPCop



Gambar 4.11 Tampilan *Zerina*

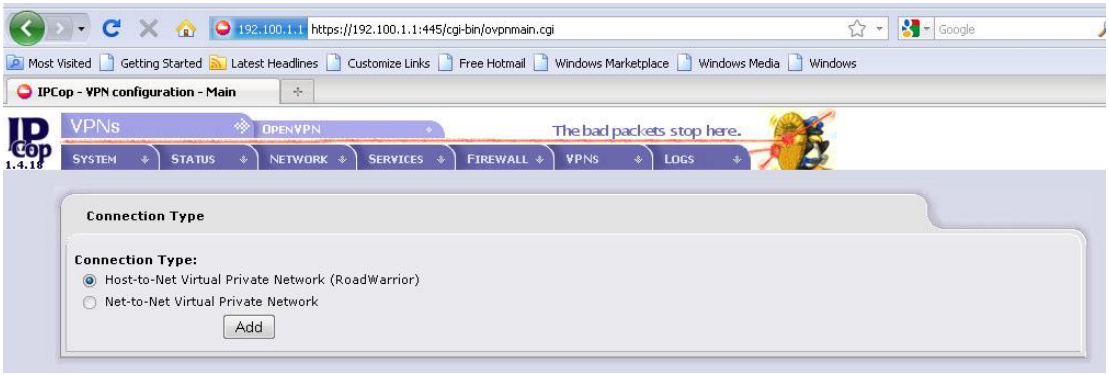
Perintah selanjutnya adalah meng-*generate* kunci (*key*) yang akan digunakan sebagai verifikasi antara *server* dan *client* pada saat proses *tunneling* berlangsung, klik tombol *Generate Root/Host certificate* dan isikan *field* yang ditampilkan dengan *setting*-an menurut kebutuhan organisasi/perusahaan.



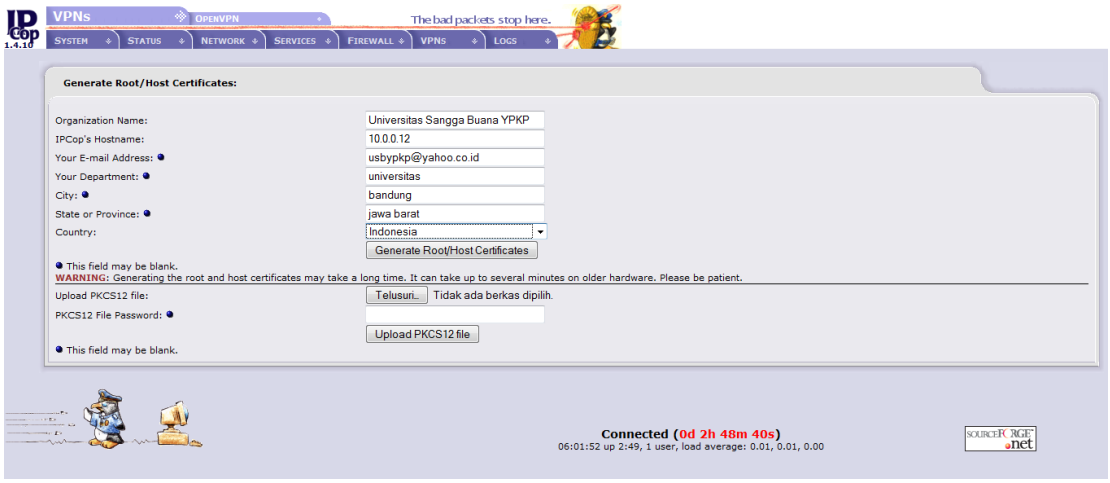
Gambar 4.12 Kotak Dialog *Generate Root Certificate*



Gambar 4.13 Tampilan Setelah *Root Certificate* Terbuat

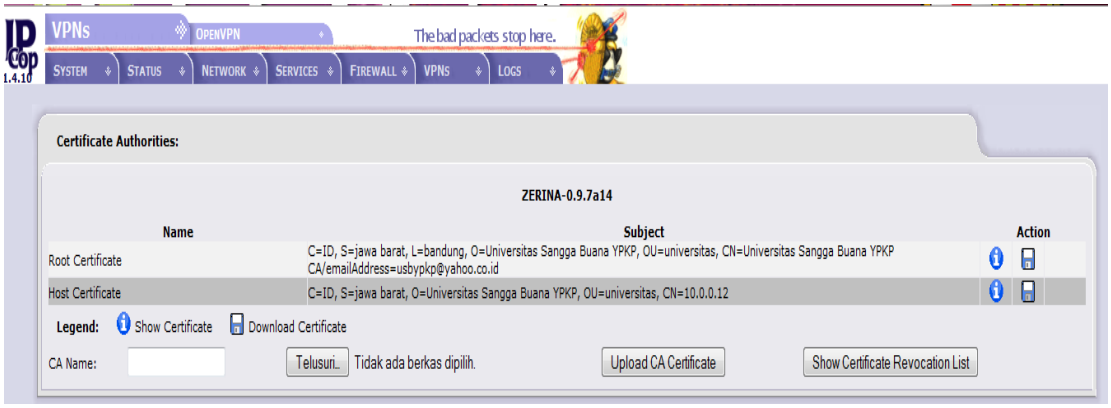


Gambar 4.14 Tampilan Pemilihan Tipe Koneksi *Client*



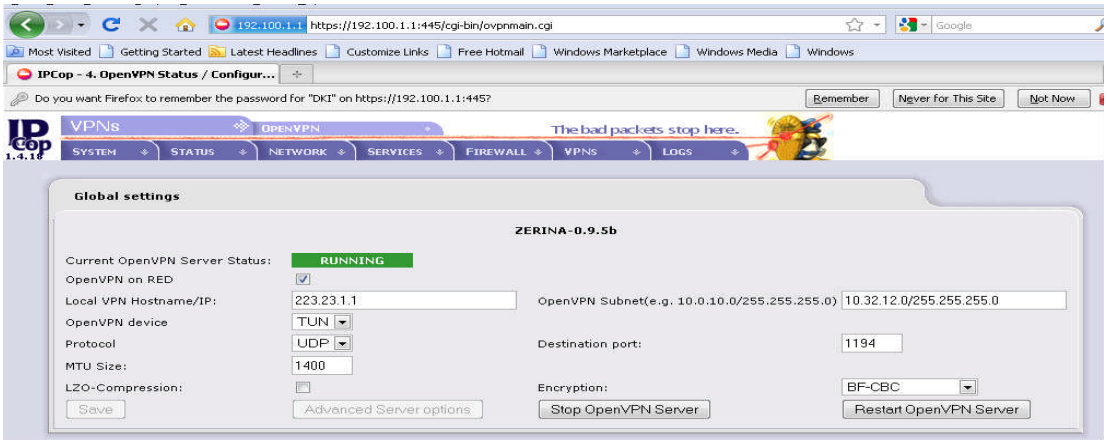
Gambar 4.15 Tampilan *Field* Isian Deskripsi *Client*

Sertifikat *client* yang terbuat akan membentuk satu *file zip* yang harus *didownload* yang nantinya di distribusikan kepada *client* yang ditujukan.



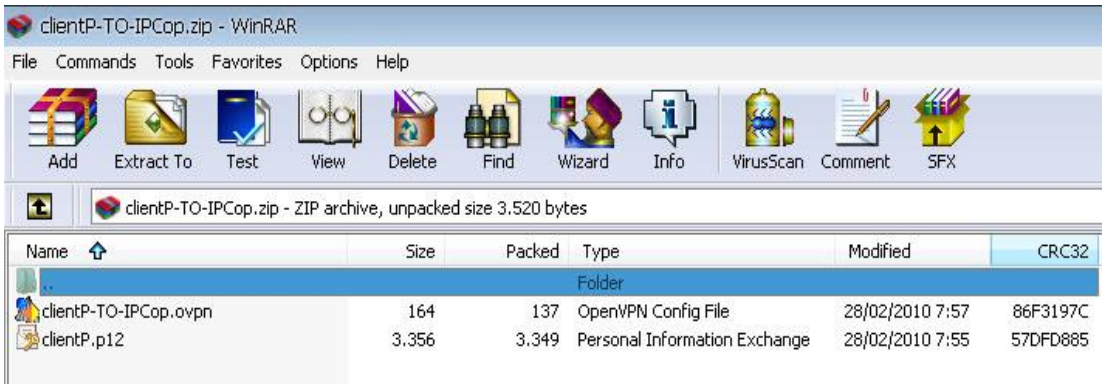
Gambar 4.16 Tampilan Hasil Pembentukan *Certificate Client*

Setelah semua *certificate* yang diperlukan telah terbentuk *vpn server* dapat dihidupkan dengan klik tombol *start* VPN *server*, dan pastikan *current* VPN *server status* berubah menjadi *running* dan berwarna hijau.



Gambar 4.17 Tampilan IPCop *Running.*

Mengkoneksikan *client* dapat mulai dilakukan dengan cara mendistribusikan *certificate* yang telah didownload pada *server* dengan cara di *copy*-kan melalui media *storage device* (*flashdisk*) ataupun dengan *tool* bantuan seperti *winscp*.



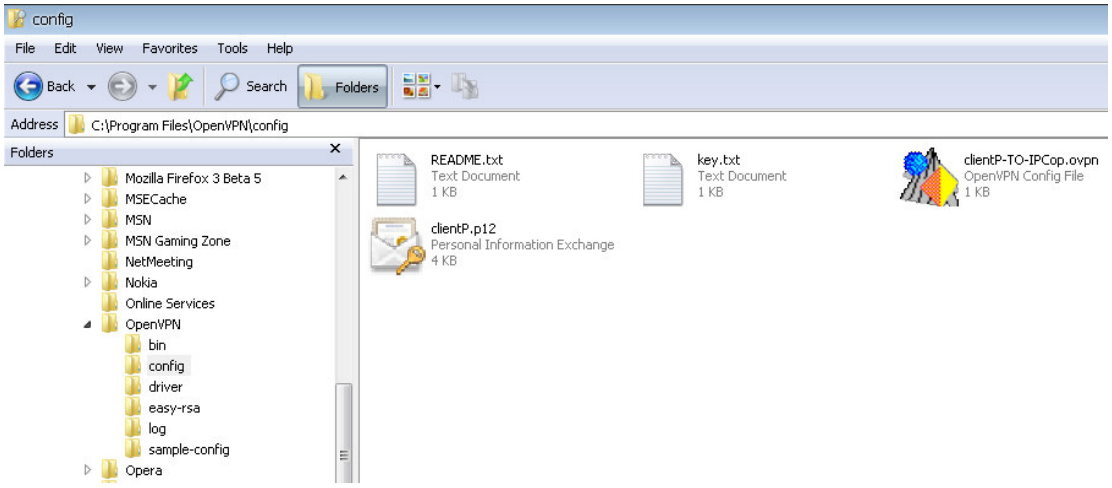
Gambar 4.18 File ZIP *Certficate Client*

Pengaturan openvpn pada sisi *client* yang menggunakan *windows* menggunakan aplikasi bantuan openvpn-2.0.9-gui-1.0.3-install.exe dan openvpn-gui-1.0.3.exe yang bisa di-*download* pada *web open source* yang bisa langsung dikonfigurasikan pada pengguna *windows* yang akan membentuk satu perangkat jaringan *virtual* baru, yaitu adapter Tap -32 yang akan digunakan sebagai pintu masuk antara *server* dengan *client*. Untuk mengaktifkan aplikasi ini cukup dengan melakukan *double click* pada *icon* openvpn-gui-1.0.3.exe hingga muncul applet koneksi pada *shortcut* menu di kanan bawah *taskbar*.



Gambar 4.19 *Icon* Openvpn Install.Exe

Secara *default* konfigurasi dari hasil installasi openvpn-2.0.9-gui- 1.0.3-install.exe berada pada folder C:\Program Files\OpenVPN, dimana *file* sertifikat yang telah di *download* diletakkan pada direktori config.

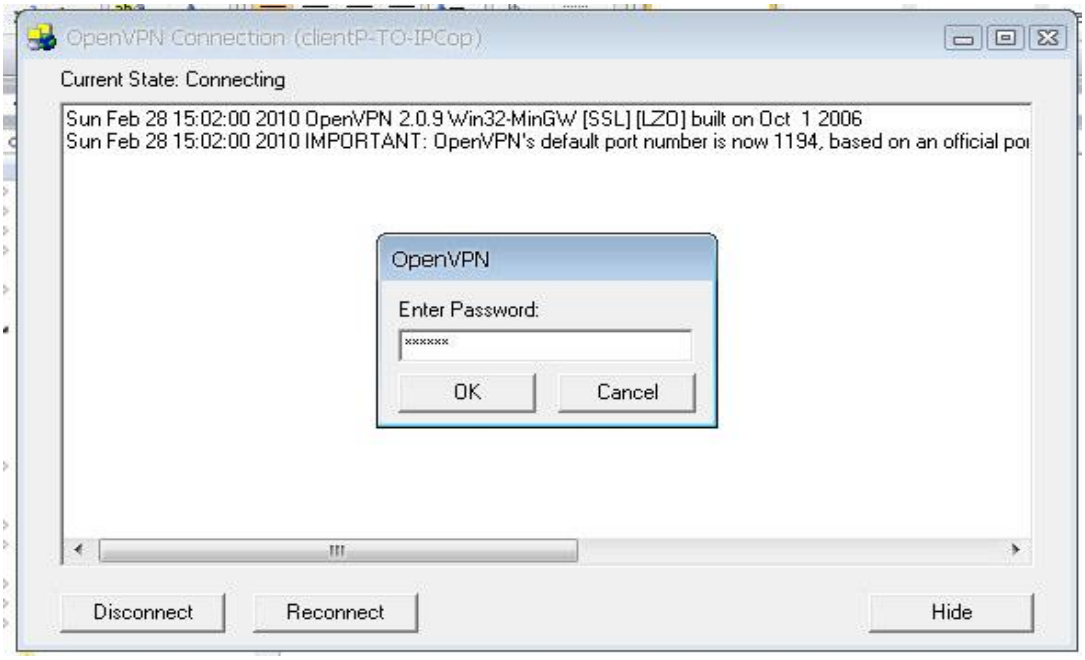


Gambar 4.20 Folder Penyimpanan *Certificate* Pada *Client*



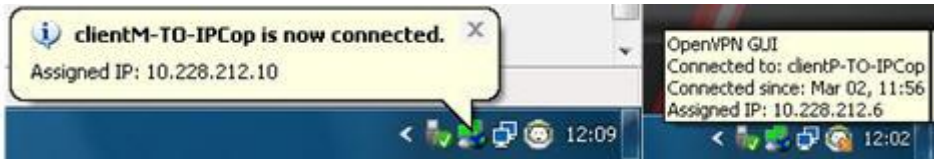
Gambar 4.21 Menu Openvpn

Selanjutnya jika koneksi vpn *server-client* dilakukan, openvpn akan meminta *password* yang telah dibuat sebelumnya pada saat pembuatan sertifikat untuk *client*.

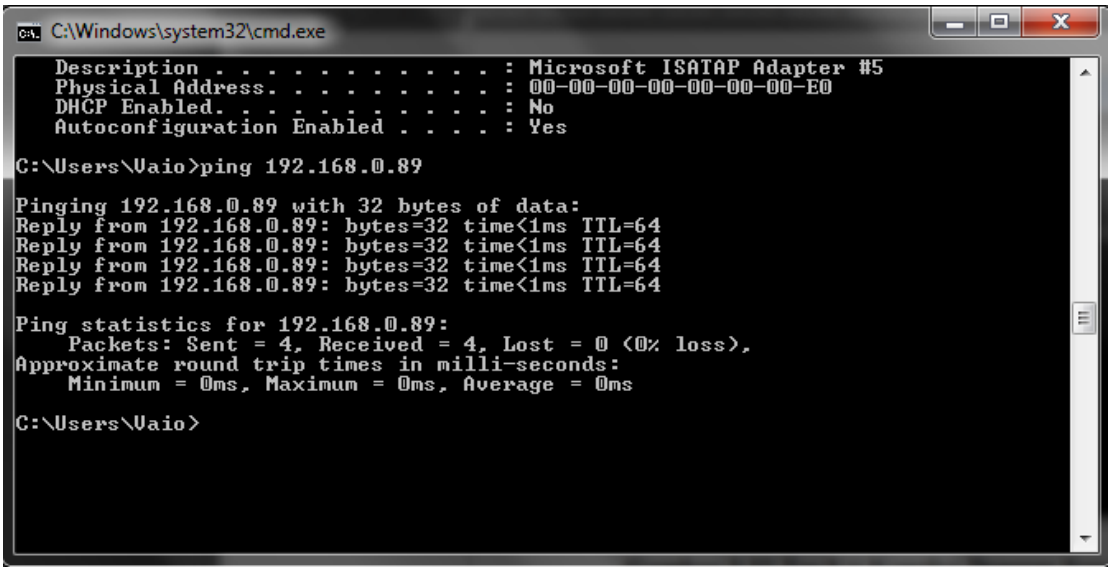


Gambar 4.22 Kotak Dialog Permintaan *Password*

Jika uji koneksi berhasil, openvpn *client* akan menerima *ip virtual* dari *server* yang bisa dilihat melalui *message box* yang muncul pada layar *desktop* apabila sistem *client* berhasil terkoneksi pada *server*, atau bisa juga dilihat dengan menggunakan perintah *ipconfig* pada *console* yang akan menampilkan *ip address* baru yang ditunjukkan pada pernyataan *Ethernet adapter Local Area Connection* 8 , dimana *ip virtual* tersebut akan digunakan sebagai alamat atau pintu dalam memasuki sistem pada *server*.



Gambar 4.23 Tampilan *Ip Virtual* Pada Layar *Console*



Gambar 4.24 Tes Uji Koneksi Dengan *Server* Menggunakan Perintah Ping

Penerapan VPN pada Universitas Sangga Buana YPKP Bandung terutama pada sektor teknologi informasi mampu memberikan jawaban akan pertanyaan-pertanyaan tentang bagaimana meningkatkan kinerja aktivitas dalam melakukan transfer data pada *client* ke *server* ataupun sebaliknya, sehingga tidak mengganggu pada aktivitas universitas.

4.2 Pengujian

Pada penelitian ini, dilakukan pengujian terhadap performansi *firewall* dan VPN yang ada di Universitas Sangga Buana YPKP dengan beberapa skenario pengujian. Pengujian menggunakan metode *Black Bos Testing*. *Black Box Testing* adalah pengujian yang mengabaikan mekanisme internal sistem atau komponen dan fokus hanya pada *output* yang dihasilkan yang merespon input yang dipilih dan kondisi tersebut.

4.2.1 Skenario Pengujian

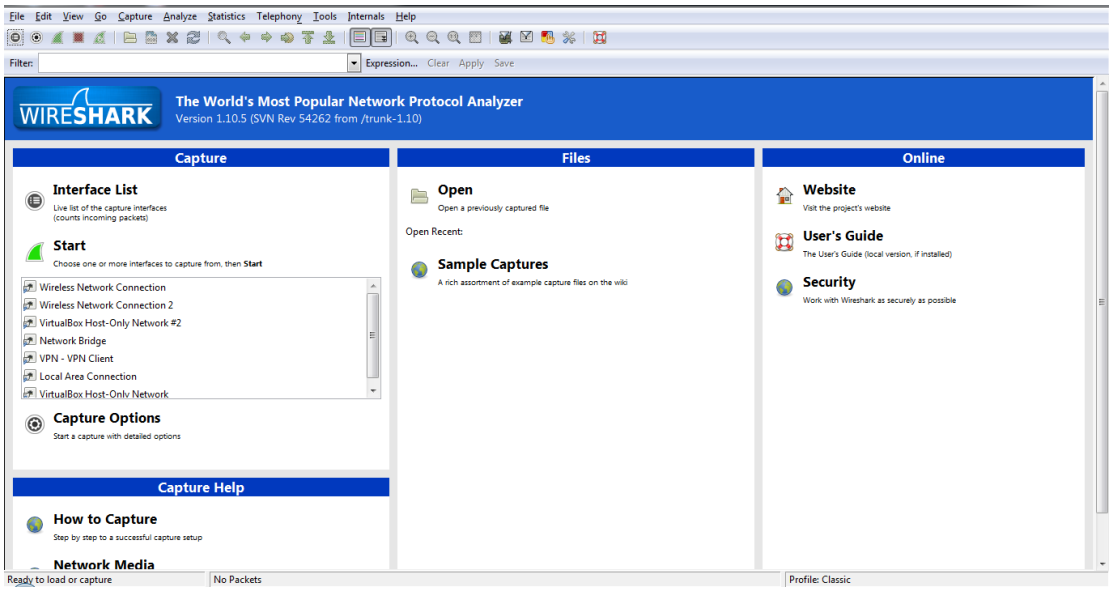
Pada skenario pengujian, dilakukan analisa kesesuaian performansi *firewall* dan VPN terhadap keamanan di Universitas Sangga Buana YPKP.

4.2.2 Pengujian Firewall

Pengujian keamanan Firewall di Universitas Sangga Buana YPKP menggunakan *tools-tools* yang dapat membuat seorang *attacker* bisa mengakses ke jaringan yang berada di Universitas Sangga Buana YPKP. *Tools* yang digunakan adalah *wireshark.*

a. *Wireshark* digunakan untuk mencari *service port* dan *operating system* yang berada pada ip target. Hal ini memudahkan seorang *attacker* untuk bisa mengakses ke jaringan Universitas Sangga Buana YPKP melalui *service-service* yang ada.

Berikut ini merupakan *interface wireshark.*



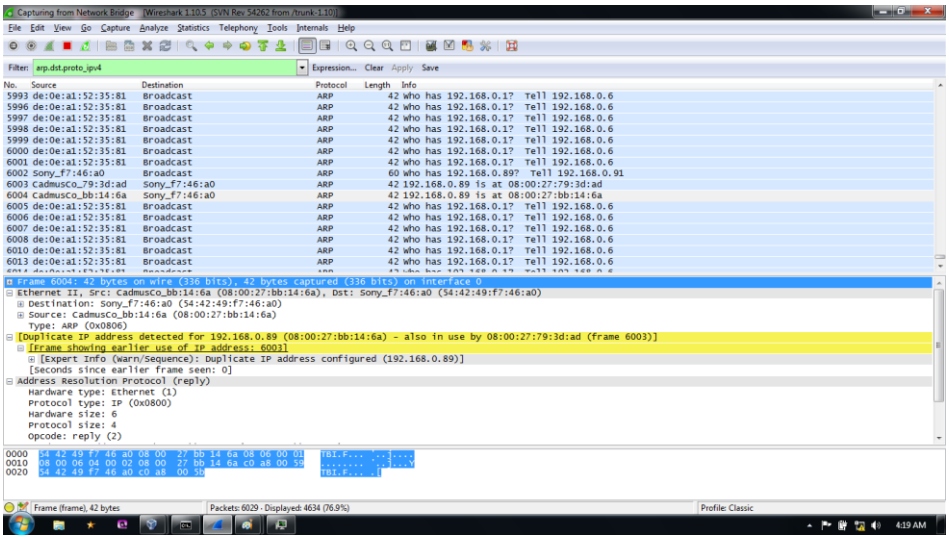
Gambar 4.25 *Interface Wireshark*

b. Serangan *spam DoS* ini sering membanjiri *server mail* dengan paket data yang tidak diminta dengan cara belum pernah terjadi sebelumnya. Hal ini menyebabkan '*Overflow* Kapasitas' terhadap *server mail* yang dimiliki Universitas Sangga Buana YPKP. Berikut pengujian sebelum diterapkan *firewall.*



Gambar 4.26 Ilustrasi *DoS*

Berikut pengujian setelah diterapkan *firewall.*



Gambar 4.27 Ilustrasi Firewall Memfilterisasi Protokol ARP

Protokol ARP dapat berasal dari berbagai sistem, baik itu secara sengaja maupun otomatis. ARP *padding* menunjukan adanya kelebihan data paket yang tidak sesuai dengan format data. Ada banyak penyebab terjadiya ARP padding ini, ada yang berasal dari kerusakan sistem atau bug akibat kesalahan proses hingga respon yang dikirim menjadi lebih banyak dari yang seharusnya.

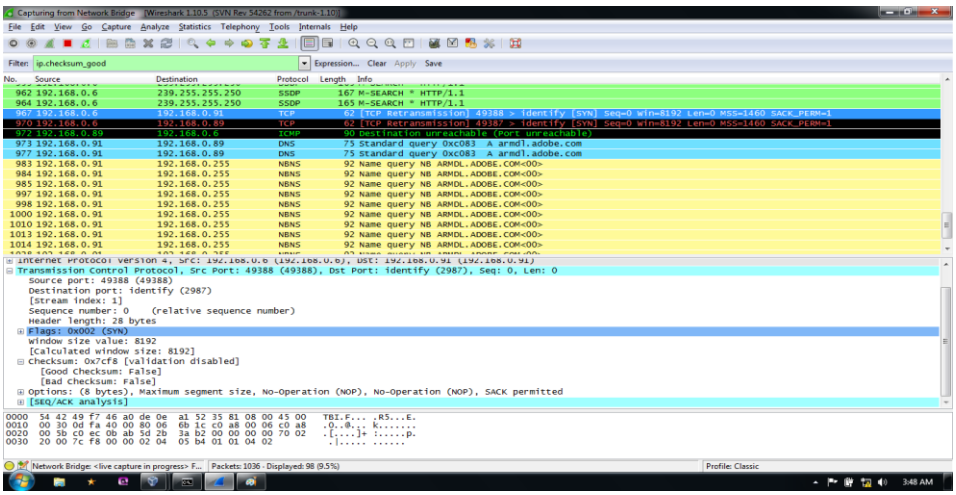
c. Paket-paket *flooding* adalah salah satu jenis paket dalam protokol *Transmission Control Protocol* yang dapat digunakan untuk membuat koneksi antara dua *host* dan dikirimkan oleh *host* yang hendak membuat

koneksi, sebagai langkah pertama pembuatan koneksi dalam proses "*TCP Three-way Handshake*". Dalam sebuah serangan *flooding*, penyerang mengirimkan paket-paket *flooding* ke dalam *port-port* yang sedang berada dalam keadaan "*Listening*" yang berada dalam *host* Universitas Sangga Buana YPKP. Berikut pengujian sebelum diterapkan *firewall.*



Gambar 4.28 Ilustrasi *Flooding*

Berikut pengujian setelah diterapkan *firewall.*

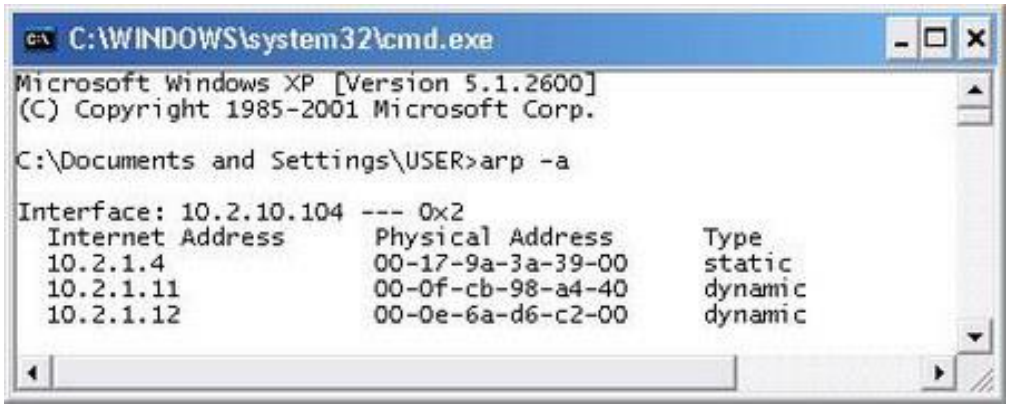


Gambar 4.29 Ilustrasi Firewall Memfilterisasi Protokol TCP

Protokol TCP adalah permasalahan pada *handshake* dan bisa terjadi karena lingkungan jaringan yang tidak bagus. Berikut protocol TCP yang sedang berjalan dan di *block firewall*.

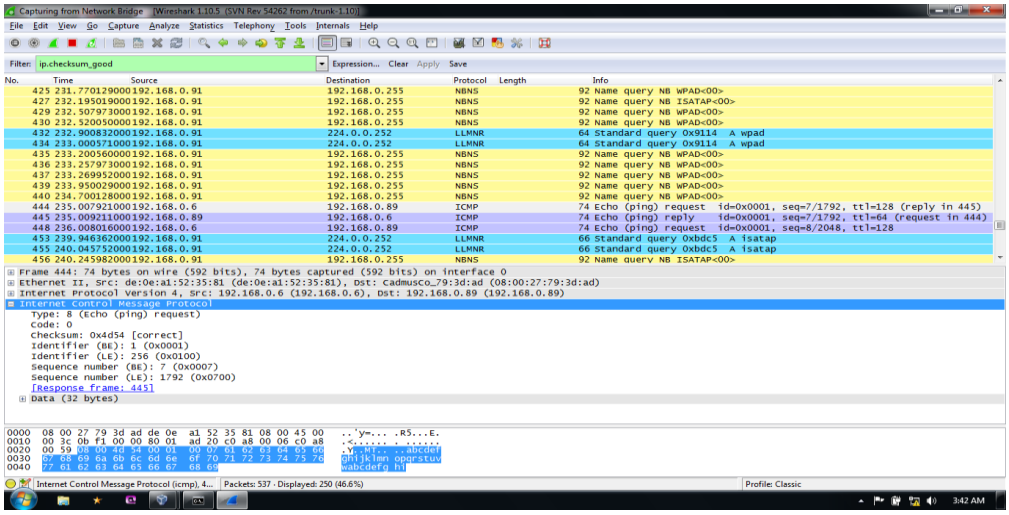
d. IP *spoofing* juga dikenal sebagai *Source Address Spoofing*. Yaitu pemalsuan IP *attacker* sehingga sasaran menganggap alamat IP *attacker*

adalah alamat IP dari *host* di dalam *network* bukan dari luar *network*. Berikut pengujian sebelum diterapkan *firewall.*



Gambar 4.30 Ilustrasi IP *Spoofing*

Berikut pengujian setelah diterapkan *firewall.*



Gambar 4.31 Ilustrasi Firewall Memfilterisasi Paket ICMP

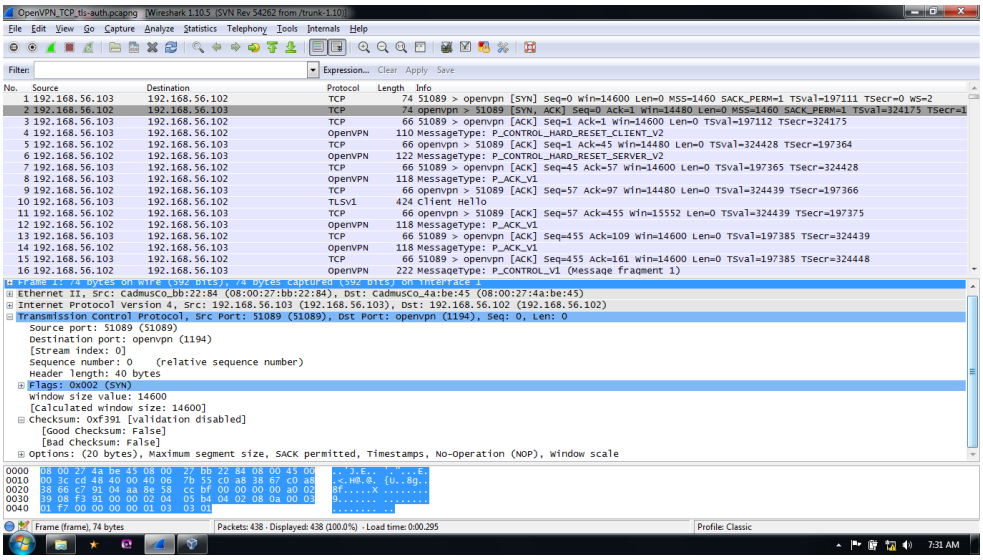
Dapat dilihat paket ICMP sedang berjalan. Permasalahan yang sering terjadi pada protocol ICMP adalah kegagalan mencapai alamat IP target yang diinginkan.

4.2.3 Pengujian VPN

Pengujian keamanan VPN di Universitas Sangga Buana YPKP melalui TCP dan UDP. Berikut analisis keamanan VPN.

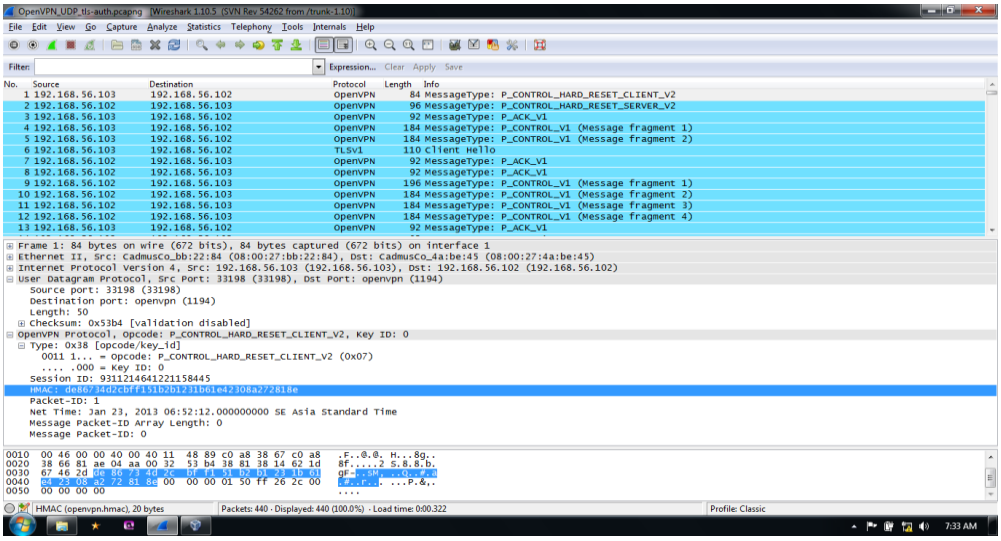
Protokol Tranmission Control Protocol (TCP) adalah protocol yang berada pada layer transport pada model OSI dan menyediakan keandalan pengiriman

paket secara *stream* dari layanan ke aplikasi dengan menerapkan beberapa mekanisme pengakuan dan retrains-misi paket pada kasus spesifikasi. Melalui pengiriman aliran ini, kita dapat mengirim data melalui TCP dengan format atau struktur data yang bebas. Berikut kasus pengiriman paket melalui protokol TCP.



Gambar 4.32 Ilustrasi VPN Memfilterisasi Protokol TCP

User Datagram Protocol (UDP) merupakan protokol berorientasi connectionless yang berada pada layer transport dari model OSI yang menawarkan kesederhanaan. UDP melakukan antarmuka antara protokol pada TCP. Berikut kasus pengiriman paket melalui protokol UDP.



Gambar 4.33 Ilustrasi VPN Memfilterisasi Protokol UDP

4.3 Hasil Pengujian

Berdasarkan pengujian keamanan pada *firewall* dan VPN Universitas Sangga Buana YPKP, maka dapat dijelaskan perbedaan tersebut. Pengujian keamanan *firewall* dan VPN dilakukan pada Universitas Sangga Buana YPKP.

4.3.1 Hasil Pengujian Keamanan

Berdasarkan hasil pengujian pada *server* dengan menggunakan *wireshark*, maka dapat disimpulkan bahwa pengujian keamanan firewall dan VPN, masih terdapat masalah yang terdapat pada protokol TCP/IP dan UDP.

4.3.2 Hasil Pengolahan Data Kuesioner

Berikut ini merupakan hasil pengolahan data kuesioner berdasarkan pertanyaan yang telah diajukan kepada 10 *client* dari Universitas Sangga Buana YPKP.

Tabel 4.4 Tabel Pengolahan Data Kuesioner

Pertanyaan Ke -	Sangat Setuju	Setuju	Ragu-ragu	Tidak Setuju	Jumlah
1	1	9	-	-	10
2	-	6	2	2	10
3	-	5	3	2	10
4	2	4	2	2	10
5	3	3	2	2	10

Berikut ini adalah hasil presentase masing-masing jawaban yang sudah dihitung nilainya. Hasil perhitungan presentase masing-masing jawaban adalah sebagai berikut :

1. **Apakah anda setuju bahwa kinerja *firewall* dan VPN dapat membantu kinerja pekerjaan anda?**

   Sangat Setuju : 1/10 = 0,1

   Setuju : 9/10 = 0,9

2. **Apakah anda setuju keamanan data menggunakan *firewall* dan VPN lebih aman?**

   Setuju : 6/10 = 0,6

   Ragu-ragu : 2/10 = 0,2

   Tidak Setuju : 2/10 = 0,2

3. **Setujukah anda jika *firewall* dan VPN digunakan untuk keamanan data di Universitas Sangga Buana YPKP?**

   Setuju : 5/10 = 0,5

   Ragu-ragu : 3/10 = 0,3

   Tidak Setuju : 2/10 = 0,2

4. **Apakah anda setuju jika *firewall* digunakan untuk mengatasi *spam* DoS, *flooding,* dan *spoofing*?**

   Sangat Setuju : 2/10 = 0,2

   Setuju : 4/10 = 0,4

   Ragu-ragu : 2/10 = 0,2

   Tidak Setuju : 2/10 = 0,2

5. **Apakah anda setuju jika VPN digunakan untuk membantu kinerja pekerjaan anda dalam mengakses data dimanapun berada tanpa terbatasi waktu dan tempat?**

   Sangat Setuju : 3/10 = 0,3

   Setuju : 3/10 = 0,3

   Ragu-ragu : 2/10 = 0,2

   Tidak Setuju : 2/10 = 0,2

4.4 Kesimpulan Hasil Pengujian

Berdasarkan kuesioner yang diajukan kepada *client* di Universitas Sangga Buana YPKP mulai dari pertanyaan 1 sampai 5, maka diperoleh hasil berikut :

1. *Firewall* dan VPN telah membantu *client* di Universitas Sangga Buana YPKP dalam membantu kebutuhan kinerja pekerjaan mereka.
2. *Client* Universitas Sangga Buana YPKP masih ragu-ragu dalam menggunakan *firewall* dan VPN untuk keamanan data.
3. *Client* Universitas Sangga Buana YPKP setuju untuk menetapkan *firewall* untuk mengatasi *spam* Dos, *flooding*, dan *spoofing*.
4. Berdasarkan pengujian keamanan *firewall* dan VPN masih terdapat celah-celah sehingga tidak ada jaminan keamanan yang sangat tinggi dalam mengamankan data.

4.5 Hasil Kesimpulan Perfomansi

Hasil kesimpulan performansi di Universitas Sangga Buana YPKP meliputi performansi *hardware,* dan *software* terhadap *firewall* dan VPN di Universitas Sangga Buana YPKP.

4.5.1 Hasil Perfomansi *Software* (Perangkat Lunak)

Berdasarkan pengujian *software* yang digunakan untuk mengimplementasikan *firewall* dan VPN pada komputer *server* dan komputer *client* meliputi *operating system (OS). Operating system* yang digunakan pada komputer *server* yaitu IPCop (Linux) telah mendukung *firewall* dan VPN. Sedangkan *operating system (OS)* yang digunakan pada komputer *client* yang telah mendukung *firewall* dan VPN adalah *windows* 7, dan *windows* xp.

4.5.2 Hasil Perfomansi *Hardware* (Perangkat Keras)

Berdasarkan pengujian *hadrware* terhadap implementasi *firewall* dan VPN di Universitas Sangga Buana YPKP, maka dapat disimpulkan bahwa *hardware* yang meliputi *server, router,* dan komputer *client* yang digunakan di Universitas Sangga Buana YPKP telah mendukung *firewall* dan VPN.