RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN

SKRIPSI

Disusun Oleh :

HESTA SAPUTRA

NIM.0812515

PROGRAM STUDI TEKNIK ELEKTRO S-1

KONSENTRASI TEKNIK KOMPUTER

FAKULTAS TEKNOLOGI INDUSTRI

INSTITUT TEKNOLOGI NASIONAL MALANG

2012

LEMBAR PERSETUJUAN

RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN

SKRIPSI

Disusun dan diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Strata Satu (S-1)

Disusun oleh :

HESTA SAPUTRA
0812515

Mengetahui,
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y.1018800189

Diperiksa dan disetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Dr.Eng. Aryuanto Soetedjo, ST.MT	**Bima Aulia Firmandani, ST**
NIP.P.1030800417	**1121**

PROGRAM STUDI TEKNIK ELEKTRO S-1
KONSENTRASI TEKNIK KOMPUTER
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2012

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini :

Nama	: **Hesta Saputra**
NIM	: **08.12.515**
Program Studi	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini menyatakan bahwa Skripsi yang saya buat adalah hasil karya sendiri, tidak merupakan plagiasi dari karya orang lain. Dalam Skripsi ini tidak memuat karya orang lain, kecuali dicantumkan sumbernya sesuai dengan ketentuan yang berlaku.

Demikian surat pernyataan ini saya buat, dan apabila di kemudian hari ada pelanggaran atas surat pernyataan ini, saya bersedia menerima sangsinya.

Malang, 8 Agustus 2012

Yang membuat Pernyataan,

Hesta Saputra
0812515

ABSTRAK

RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN

Hesta Saputra, NIM 0812515

Dosen Pembimbing : Dr. Eng. Aryuanto Soetedjo, ST. MT dan Bima Aulia Firmandani, ST

VPN (Virtual Private Network) adalah sebuah cara aman untuk mengakses jaringan lokal yang berada diluar jangkauan, dengan menggunakan media internet atau jaringan umum lainnya untuk melakukan transmisi paket data secara pribadi. Perlu penerapan teknologi tertentu agar walaupun menggunakan media yang umum, tetapi traffic (lalu lintas) antar remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidak semestinya kedalam remote-site.

Pada tulisan ini akan dibahas tentang perancangan dan pembangunan sebuah server VPN yang dalam pengujiannya akan mengimplementasi sistem dari sebuah VPN. Padaimplementasinya server inimenggunakanperangkatlunak yang bersifat open source yaitu CentOS sebagai sistem operasi dan OpenVPN sebagai perangkat virtual dari sebuah VPN. Pengujian yang dilakukan meliputi :pengujian koneksi dan enkripsi data. Pengujian dilakukan untuk mengetahui apakah sistem yang dibuat sesuai dengan perancangan. Hasil yang diinginkan adalah sistem dapat berjalan atau berfungsi dengan baik.

Kata kunci : VPN, CentOS, OpenVPN.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala limpahan berkat dan rahmat-Nya sehingga penelitian yang berjudul "RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN" dapat terselesaikan.

Penelitian ini dibuat untuk memenuhi salah satu syarat dalam memperoleh gelar sarjana teknik. Ucapan terima kasih yang sebesar–besarnya kami ucapkan kepada :

1. Bapak Ir. Soeparno Jiwo, MT selaku Rektor ITN Malang.
2. Bapak Ir. H. Sidik Noertjahjono, MT selaku Dekan Fakultas Teknologi Industri ITN Malang.
3. Bapak Ir. Yusuf Ismail Nakhoda, MT selaku Ketua Program Studi Teknik Elektro S-1 ITN Malang.
4. Bapak Dr. Eng. Aryuanto Soetedjo, ST.MT selaku Dosen Pembimbing I.
5. Bapak Bima Aulia Firmandani, ST selaku Dosen Pembimbing II.
6. Kedua orang tua dan kedua saudara yang telah member motivasi dalam penyusunan penelitian ini.
7. Mahasiswa Elektro S-1 angkatan 2008 dan asisten Lab. P K&M.
8. Semua pihak yang telah membantu dalam penulisan dan penyusunan penelitian ini.

Penulis menyadari bahwa penelitian ini masih jauh dari sempurna, untuk itu kritik dan saran dari pembaca sangat penulis harapkan untuk perbaikan penelitian ini.

Malang, 2012

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

BAB I

PENDAHULUAN

1.1 Latar Belakang

Transmisi data melalui jaringan computer sudah menjadi kebutuhan vital suatu perusahaan atau instansi yang memiliki cabang atau divisi yang berada pada area local maupun area yang luas. Contoh, seorang karyawan yang berada di kantor cabang suatu perusahaan ingin memasukkan data ke sistem *database* pusat, tapi disini yang menjadi permasalahan adalah lokasi dari sistem *database* pusat terletak puluhan kilometer dari kantor cabang tersebut jika karyawan tersebut memutuskan untuk dating ke kantor pusat tentu sangat tidak efisien karena akan membuang waktu dan tenaga, disini jaringan komputer muncul sebagai solusi.

Untuk keamanan komunikasi atau transmisi data yang memanfaatkan jaringan komputer di area local mungkin lebih mudah ditangani oleh administrator, tapi jika jaringan tersebut sudah mencakup area yang luas tentu untuk membuat keamanan transmisi data tidak semudah dan sesederhana di area lokal.Tapi permasalahan ini dapat diatasi dengan *VPN (Virtual Private Network)*. *VPN* adalah jaringan privat yang secara fisik tidak ada, tapi mengapa disebut secara fisik tidak ada karena jaringan ini dibentuk dengan memanfaatkan infrastruktur internet yang telah ada kemudian dilakukan tunneling sehingga disebut privat karena tidak semua bisa mengakses *tunnel* tersebut.

Untuk mengimplementasikan *VPN* dibutuhkan *server VPN* yang akan digunakan untuk menyediakan *tunnel* dan enkripsi jalur transmisi data.

1.2 RumusanMasalah

Bagaimana merancang dan membangun *server VPN* yang dapat membuat *tunnel* dan melakukan enkripsi pada jalur transmisi data.

1.3 Tujuan

Menyediakan jalur komunikasi atau transmisi data yang terenkripsi tanpa harus

Membuat jalur komunikasi *point-to-point* secara fisik atau menyewa jasa perusahaan telekomunikasi, tapi dengan memanfaatkan infrastruktur internet yang telah tersedia.

1.4 Batasan Masalah

Pada pembuatan *Server VPN* berbasis *CentOS* dan *OpenVPN* ini, penulis membuat ruang lingkup pembahasan atau batasan masalah sebagai berikut :

1. Tidak membahas secara spesifik perangkat keras komputer.
2. Perangkat lunak yang digunakan adalah *CentOS* dan *OpenVPN*.
3. Pengujian dilakukan dengan satu *server* dan satu *client*.
4. Pada pengujian server *VPN* nantinya juga digunakan sebagai *file server* yang digunakan untuk menganalisa enkripsi pada protokol *FTP*.

1.5 Sistematika Penulisan

Pada penulisan skripsi ini terdiri atas lima pembahasan yaitu :

BAB I : PENDAHULUAN

Bab ini merupakan bagian pendahuluan dimana akan tercakup secara umum mengenai latar belakang penulisan laporan, ruang lingkup karya tulis skripsi ini, tujuan dan manfaat yang mau dicapai, metodologi yang dipakai dalam penyusunan laporan dan sistematika penulisan yang digunakan.

BAB II : TINJAUAN PUSTAKA

Bab ini berisi tentang teori – teori yang mendukung dan berhubungan dengan judul penulisan skripsi.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Bab ini berisi mengenai analisa kebutuhan sistem baik sofware maupun hardware yang di perlukan untuk membuat kerangka global yang

menggambarkan mekanisme dari sistem yang akan di buat.

BAB IV : IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi penjelasan pembahasan program sesuai dengan permasalahan yang diambil dalam penulisan skripsi.

BAB V : PENUTUP

Bab ini berisi kesimpulan dan saran dari penulisan skripsi.

BAB II
TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya , berkomunikasi dan dapat mengakses informasi.

Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti *Hub*, *Bridge*, *Switch*, *Router*, *Gateway* sebagai peralatan interkoneksinya.

Sejarah jaringan komputer bermula dari lahirnya konsep jaringan komputer pada tahun 1940-an di Amerika yang digagas oleh sebuah proyek pengembangan komputer MODEL I di laboratorium *Bell* dan *group riset Universitas Harvard* yang dipimpin profesor Howard Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian.

Kemudian ditahun 1950-an ketika jenis komputer mulai berkembang sampai terciptanya super komputer, maka sebuah komputer harus melayani beberapa tempat yang tersedia (*terminal*), untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama *TSS (Time Sharing System)*. Maka untuk pertama kalinya bentuk jaringan (*network*) komputer diaplikasikan. Pada sistem *TSS* beberapa terminal terhubung secara seri ke sebuah komputer atau perangkat lainnya yang terhubung dalam suatu jaringan komputer. Dalam proses *TSS* mulai terlihat perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.

Departemen Pertahanan Amerika, *U.S. Defense Advanced Research Projects Agency(DARPA)* memutuskan untuk mengadakan riset yang bertujuan untuk menghubungkan sejumlah komputer schingga membentuk jaringan organik pada tahun 1969. Program riset ini dikenal dengan nama *Arpanet.*

Pada tahun 1970, sudah lebih dari 10 komputer yang berhasil dihubungkan satu sama lain schingga mereka bisa saling berkomunikasi dan membentuk sebuah jaringan. Dan pada tahun 1970 itu juga setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (*Distributed Processing*). Dalam proses ini beberapa *host* komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa *terminal* yang tersambung secara seri disetiap *host* komputer.

Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua *host* komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.

Pada tahun 1972, Roy Tomlinson berhasil menyempurnakan program surat elektonik (*E-mail*) yang dibuatnya setahun yang lalu untuk *Arpanet*. Program tersebut begitu mudah untuk digunakan, schingga langsung menjadi populer.Pada tahun yang sama yaitu tahun 1972, ikon at (@) juga diperkenalkan sebagai lambang penting yang menunjukan "at" atau "pada". Tahun 1973, jaringan komputer *Arpanet* mulai dikembangkan meluas ke luar Amerika Serikat.

Komputer University College di London merupakan komputer pertama yang ada di luar Amerika yang menjadi anggota jaringan *Arpanet*. Pada tahun yang sama yaitu tahun 1973, dua orang ahli komputer yakni Vinton Cerf dan Bob Kahn mempresentasikan sebuah gagasan yang lebih besar, yang menjadi cikal bakal pemikiran *International Network(Internet)*. Ide ini dipresentasikan untuk pertama kalinya di Universitas Sussex. Hari bersejarah berikutnya adalah tanggal 26 Maret1976, ketika Ratu Inggris berhasil mengirimkan surat elektronik dari *Royal Signals and Radar Establishment* di Malvern. Setahun kemudian, sudah lebih dari 100 komputer yang bergabung di *Arpanet* membentuk sebuah jaringan atau *network*.

Tom Truscott, Jim Ellis dan Steve Bellovin, menciptakan *newsgroups* pertama yang diberi nama *USENET(User Network)* pada tahun 1979. Tahun 1981, France Telecom menciptakan sesuatu hal yang baru dengan meluncurkan telepon televisi pertama, di mana orang bisa saling menelepon yang juga berhubungan dengan *video link*.

Seiring dengan bertambahnya komputer yang membentuk jaringan, dibutuhkan sebuah protokol resmi yang dapat diakui dan diterima oleh semua jaringan. Untuk itu, pada tahun 1982 dibentuk sebuah *Transmission Control Protocol (TCP)* atau lebih dikenal dengan sebutan *Internet Protocol (IP)* yang kita kenal hingga saat ini. Sementara itu, di Eropa muncul sebuah jaringan serupa yang dikenal dengan *Europe Network (EUNET)* yang meliputi wilayah Belanda, Inggris, Denmark, dan Swedia. Jaringan *EUNET* ini menyediakan jasa surat elektronik dan *newsgroup USENET*.

Untuk menyeragamkan alamat di jaringan komputer yang ada, maka pada tahun 1984 diperkenalkan Sistem Penamaan Domain atau *domain name system*, yang kini kita kenal dengan *DNS*. Komputer yang tersambung dengan jaringan yang ada sudah melebihi 1000 komputer lebih.Pada 1987, jumlah komputer yang tersambung ke jaringan melonjak 10 kali lipat menjadi 10000 lebih.

Jaringan komputer terus berkembang pada tahun 1988, Jarkko Oikarinen seorang berkebangsaan Finlandia menemukan sekaligus memperkenalkan *Internet Relay Chat* atau lebih dikenal dengan *IRC* yang memungkinkan dua orang atau lebih pengguna komputer dapat berinteraksi secara langsung dengan pengiriman pesan (*Chatting*). Akibatnya, setahun kemudian jumlah komputer yang saling berhubungan melonjak 10 kali lipat.tak kurang dari 100000 komputer membentuk sebuah jaringan. Pertengahan tahun 1990 merupakan tahun yang paling bersejarah, ketika Tim Berners Lee merancang sebuah programe penyunting dan penjelajah yang dapat menjelajai komputer yang satu dengan yang lainnya dengan membentuk jaringan.Program inilah yang disebut *Waring Wera Wanua* atau *World Wide Web*.

Komputer yang saling tersambung membentuk jaringan sudah melampaui sejuta komputer pada tahun 1992. Dan pada tahun yang sama muncul istilah *surfing* (menjelajah). Dan pada tahun 1994, situs-situs di internet telah tumbuh menjadi 3000

alamat halaman, dan untuk pertama kalinya berbelanja melalui internet atau *virtual-shopping* atau *e-retail* muncul di situs.

2.2 Internet

Internet, kependekan dari *interconnection-networking*.secaraharfiah ialah sistem global dari seluruh jaringan komputer yang saling terhubung menggunakan standar *Internet Protocol Suite(TCP/IP)* untuk melayani miliaran pengguna di seluruh dunia. yang terhubung secara global dan menggunakan *TCP/IP* sebagai protokol pertukaran paket (*packet switching communication protocol*).Rangkaian internet yang terbesar dinamakan Internet.Cara menghubungkan rangkaian dengan kaedah ini dinamakan *internetworking*.

Internet dijaga oleh perjanjian bilateral atau multilateral dan spesifikasi teknikal (protokol yang menerangkan tentang perpindahan data antara rangkaian). Protokol-protokol ini dibentuk berdasarkan perbincangan *Internet Engineering Task Force* (IETF), yang terbuka kepada umum. Badan ini mengeluarkan dokumen yang dikenali sebagai *RFC* (Request for Comments). Sebagian dari *RFC* dijadikan Standar Internet (Internet Standard), oleh Badan Arsitektur Internet (Internet Architecture Board - IAB). Protokol-protokol Internet yang sering digunakan adalah seperti, *IP, TCP, UDP, DNS, PPP, SLIP, ICMP, POP3, IMAP, SMTP, HTTP, HTTPS, SSH, Telnet, FTP, LDAP,* dan *SSL*.

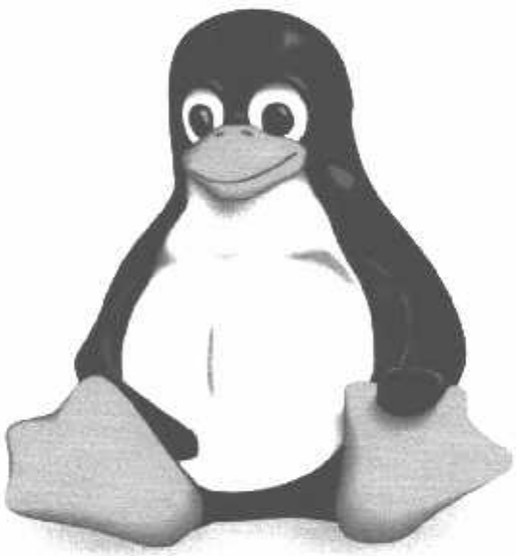
Internet memungkinkan adanya servis terkini *(Real-time service),* seperti *web radio,* dan *webcast,* yang dapat diakses di seluruh dunia. Selain itu melalui Internet dimungkinkan untuk berkomunikasi secara langsung antara dua pengguna atau lebih.

Jumlah pengguna Internet yang besar dan semakin berkembang, telah mewujudkan budaya Internet. Internet juga mempunyai pengaruh yang besar atas ilmu, dan pandangan dunia. Dengan hanya berpandukan mesin pencari seperti *Google,* pengguna di seluruh dunia mempunyai akses Internet yang mudah atas bermacam-macam informasi. Dibanding dengan buku dan perpustakaan, Internet melambangkan penyebaran *(decentralization)* / pengetahuan *(knowledge)* informasi dan data secara ekstrem.

Perkembangan Internet juga telah mempengaruhi perkembangan ekonomi. Berbagai transaksi jual beli yang sebelumnya hanya bisa dilakukan dengan cara tatap muka (dan sebagian sangat kecil melalui pos atau telepon), kini sangat mudah dan sering dilakukan melalui Internet.

2.3 Linux

Linux adalah nama yang diberikan kepada sistem operasi komputer bertipe *Unix*. *Linux* merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Seperti perangkat lunak bebas dan sumber terbuka lainnya pada umumnya, kode sumber*Linux* dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapa saja.



Gambar 2.1. Logo *linux*

Nama "*Linux*" berasal dari nama pembuatnya, yang diperkenalkan tahun 1991 oleh Linus Torvalds. Sistemnya, peralatan sistem dan pustakanya umumnya berasal dari sistem operasi *GNU*, yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi *GNU* adalah dasar dari munculnya nama alternatif *GNU/Linux*.

Linux telah lama dikenal untuk penggunaannya di *server*, dan didukung oleh perusahaan-perusahaan komputer ternama seperti Intel, *Dell, Hewlett-Packard, IBM, Novell, Oracle Corporation, Red Hat,* dan *Sun Microsystems. Linux* digunakan sebagai sistem operasi di berbagai macam jenis perangkat keras komputer, termasuk komputer *desktop, superkomputer*dan sistem benam seperti pembaca buku elektronik, sistem permainan video, telepon genggam dan *router*. Para pengamat teknologi informatika beranggapan kesuksesan *Linux* dikarenakan *Linux* tidak bergantung kepada *vendor* (*vendor independence*), biaya operasional yang rendah, dan kompatibilitas yang tinggi dibandingkan versi *UNIX,* serta faktor keamanan dan kestabilannya yang tinggi dibandingkan dengan sistem operasi lainnya seperti *Microsoft Windows*. Ciri-ciri ini juga menjadi bukti atas keunggulan model pengembangan perangkat lunak sumber terbuka (*opensource software*).

2.4 CentOS

CentOS adalah singkatan dari *Community Enterprise Operating System* (Sistem Operasi Perusahaan buatan Komunitas/Masyarakat) adalah sistem operasi gratis yang dibuat dari *source code Red Hat Enterprise Linux (RHEL).* Proyek ini berupaya untuk 100% kompatibel dengan produk hulunya *(RHEL).* Dan menggunakan paket *RPM.*

Gambar 2.2. Logo *CentOS*

CentOS ada untuk memberikan komputasi dengan *platform* kelas *enterprise* yang bebas untuk siapa saja yang ingin menggunakannya. *CentOS* dirancang untuk

orang yang membutuhkan sistem operasi kelas *enterprise* tanpa biaya .

2.5 VPN (Virtual Private Network)

VPN adalah singkatan dari *Virtual Private Network*, yaitu Sebuah cara aman untuk mengakses jaringan lokal yang berada diluar jangkauan, dengan menggunakan media internet atau jaringan umum lainnya untuk melakukan transmisi data secara pribadi, Perlu penerapan teknologi tertentu,agar walaupun menggunakan media yang umum, tetapi *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya ke dalam *remote-site*.

VPN adalah suatu jaringan privat (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet (publik), dimana jaringan privat ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik.

VPN adalah sebuah koneksi Virtual yang bersifat privat mengapa disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut privat karena jaringan ini merupakan jaringan yang sifatnya privat yang tidak semua orang bisa mengaksesnya. *VPN* Menghubungkan *PC* dengan jaringan publik atau internet namun sifatnya privat, karena bersifat privat maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya.Oleh karena itu diperlukan untuk keamanan data.

2.6 OpenVPN

OpenVPN adalah sebuah implementasi *VPN open source* yang didasarkan pada *SSL (Secure Socket Layer)*. Implementasi klien *OpenVPN* tersedia untuk banyak sistem operasi, termasuk *Linux, Windows 2000/XP* atau yang lebih tinggi, *OpenBSD, FreeBSD, NetBSD, Mac OS X,* dan *Solaris*. Pada sebuah *VPN, OpenVPN* akan meng-enkapsulasi semua trafik (termasuk protokol DNS dan protokol-protokol lain) di *tunnel* yang terenkripsi, jadi bukan hanya satu *port TCP* saja.

Gambar 2.3. Logo *OpenVPN*

OpenVPN juga mempunyai beberapa kerugian, seperti latensi yang cukup tinggi.Beberapa latensi tak terelakan karena semua enkripsi/dekripsi dilakukan di aplikasi *user*, dengan memakai komputer yang relatif baru kedua ujung tunnel dapat mengurangi latensi ini. Biarpun bisa memakai *shared key* yang tradisional, *OpenVPN*akan lebih baik jika digunakan bersama sertifikat *SSL* dan *Certificate Authority*. *OpenVPN* mempunyai banyak keuntungan yang membuatkannya pilihan yang baik untuk menyediakan keamanan *end-to-end*.

OpenVPN perlu menyambung sebuah *port TCP* atau *UDP* di *remote site*. Setelah tersambungkan, *OpenVPN*akan mengenkapsulasi semua data ke *Networking Layer*, atau bahkan sampai ke lapisan *Data-Link*.

2.7 Algoritma RSA

Algoritma RSA yang diciptakan oleh Ronald Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1977 merupakan salah satu algoritma kriptografi yang sukses dan sangat baik dimana algoritma ini berdasarkan pada sistem kriptografi yang menggunakan *public key* dengan faktorisasi dari bilangan integer dan modulus dalam nilai yang besar.

Algoritma *RSA* melibatkan dua kunci yaitu *private key* dan *public key*. Dimana *public key* dapat secara aman diketahui oleh semua pihak untuk digunakan sebagai kunci untuk melakukan enkripsi, sedangkan *private key* harus selalu di simpan secara rahasia untuk melakukan dekripsi data yang telah di enkripsi dengan menggunakan *public key*.

Data yang telah di enkripsi oleh *public key* hanya dapat di dekripsi oleh *private key*, hal ini lah yang membuat data yang dienkripsi dengan algoritma *RSA* aman walaupun Algoritma *RSA*-nya diketahui selama *private key* nya tidak diketahui oleh pihak lain. Algoritma *RSA* dapat dijelaskan sebagai berikut:

Penjelasan variabel-variabel yang digunakan :

1. P = bilangan prima 1.
2. Q = bilangan prima 2.
3. E = *public key* (kunci untuk enkripsi).
4. D = *private key* (kunci untuk dekripsi).
5. N = modulus pada *public* dan *private key*.

Langkah-langkah dalam algoritma RSA :

1. Menentukan suatu nilai-nilai prima rahasia *P* dan *Q*.
2. Menghitung nilai N dengan rumus sebagai berikut :

$$N = P.Q$$

3. Menentukan nilai yang akan digunakan untuk pencarian nilai *private key* dengan rumus berikut :

$$PQ = (P-1) * (Q-1)$$

4. Menentukan nilai *E* dengan syarat :

$$(1 < E < PQ) \text{ dan } (GCD\ (E, PQ) = 1)$$

5. Menentukan nilai D dengan syarat :

$$(D*E)\ Mod\ PQ = 1$$

Dalam *point* ke-4, terdapat fungsi *GCD*, dimana nilai fungsi ini ddigunakan untuk mencari nilai bagi terbesar (*Greatest common divisor*) yang biasanya telah terdapat pada fungsi matematika.

Contoh Kasus Pembuatan Kunci dengan bilangan yang kecil (hanya sebagai ilustrasi cara kerja algoritma *RSA*).

1. Memilih 2 bilangan prima yang berbeda untuk P dan Q. Misalnya :

   P = 61 dan Q = 53.

2. Menghitung N = PQ

   (61*53 = 3233)

3. Mengitung PQ = (P-1)*(Q-1)

   (61-1)*(53-1) = 3120

4. Memilih bilangan E dengan syarat (1 < E < 3120) dan GCD(E, 3120) = 1, mengambil E = 17, dimana 17 memenuhi syarat :

   (1 < 17 < 3120) dan (GCD(17, 3120) = 1)

5. Memilih nilai D, dimana (D*E) Mod PQ = 1. Mengambil D = 2753 dimana :

   (2753*17) Mod 3120 = 146801 Mod 3120 = 1

Dengan perhitungan tersebut telah didapatkan *private* dan *public key*, dimana *private key* adalah (N = 3233 dan D = 2753) dan *public key* adalah (N = 3233 dan E = 17).

RSA seringkali disebut dengan *RSA* - n bit,. di mana n menunjukkan jumlah digit kunci yang digunakan. Semakin tinggi bit *RSA* yang digunakan maka akan semakin besar nilai prima P dan Q yang akan digunakan dan akan semakin sulit untuk dipecahkan oleh pihak-pihak yang tidak diinginkan, karena pencarian nilai D, yang digunakan sebagai kunci untuk dekripsi juga akan semakin sulit. Keamanan data pada *RSA* sangat bergantung pada faktor kerja (*Work Factor*) yang mampu dilakukan oleh komputer dalam menghitung hasil dari 2 bilangan prima yang sangat besar. Misalkan digunakan kunci P = 23 (2 byte= 16 bit) dan Q = 29 (2 byte= 16 bit), maka metode *RSA* yang digunakan akan disebut *RSA* - 32 bit.

2.8 FTP Server

FTP (File Transfer Protocol) adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkaskomputer antar mesin-mesin dalam sebuah Antar jaringan.

FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan dan pengunggahanberkas-berkas komputer antara *client FTP* dan *server FTP*. Sebuah *client FTP* merupakan aplikasi yang dapat mengeluarkan perintah-perintah *FTP* ke sebuah *serverFTP*, sementara *server FTP* adalah sebuah *daemon* yang berjalan di atas sebuah komputer yang merespon perintah-perintah dari sebuah *client FTP*. Perintah-perintah *FTP* dapat digunakan untuk mengubah direktori, mengubah modus pengiriman antara *biner* dan *ASCII*, menggugah berkas komputer ke *server FTP*, serta mengunduh berkas dari *server FTP*.

Sebuah *serverFTP* diakses dengan menggunakan *Universal Resource Identifier (URL)* dengan menggunakan format *ftp://namaserver*. *Client FTP* dapat menghubungi *server FTP* dengan membuka *URL* tersebut.

FTP menggunakan protokol*Transmission Control Protocol (TCP)* untuk komunikasi data antara *client* dan *server*, sehingga di antara kedua komponen tersebut akan dibuatlah sebuah sesi komunikasi sebelum pengiriman data dimulai. Sebelum membuat koneksi, *port TCP* nomor 21 di sisi server akan "mendengarkan" percobaan koneksi dari sebuah *clientFTP* dan kemudian akan digunakan sebagai *port* pengatur *(control port)* untuk (1) membuat sebuah koneksi antara *client* dan *server*, (2) untuk mengizinkan klien untuk mengirimkan sebuah perintah *FTP* kepada *server* dan juga (3) mengembalikan respon*server* ke perintah tersebut. Sekali koneksi kontrol telah dibuat, maka *server* akan mulai membuka *port TCP* nomor 20 untuk membentuk sebuah koneksi baru dengan *client* untuk mengirim data aktual yang sedang dipertukarkan saat melakukan pengunduhan dan pengunggahan.

FTP hanya menggunakan metode autentikasi standar, yakni menggunakan *username* dan *password* yang dikirim dalam bentuk tidak terenkripsi. Pengguna terdaftar dapat menggunakan *username* dan password-nya untuk mengakses,

mengunduh, dan mengunggah berkas-berkas yang dikehendaki. Umumnya, para pengguna terdaftar memiliki akses penuh terhadap beberapa direktori, sehingga mereka dapat membuat berkas, membuat direktori, dan bahkan menghapus berkas. Pengguna yang belum terdaftar dapat juga menggunakan metode *anonymous login*, yakni dengan menggunakan nama pengguna *anonymous* dan *password* yang diisi dengan menggunakan alamat *e-mail*.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

BAB III

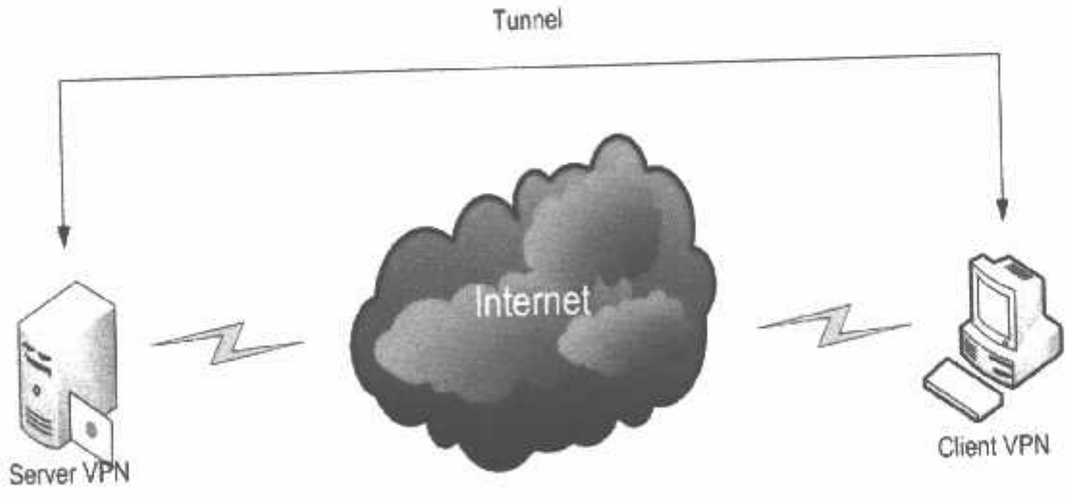
ANALISA DAN PERANCANGAN SISTEM

3.1 Gambaran Umum Sistem

Kebutuhan dalam akses data yang dilakukan kapanpu memerlukan sebuah teknologi yang dapat mendukung keamanan pengaksesan dalam jaringan secara jarak jauh. Salah satu teknologi yang menyediakan kebutuhan keamanan yang diperlukan *end user* adalah *VPN (Virtual Private Network)*, yaitu fasilitas yang memungkinkan *end-user* mengirimkan sebuah data dalam sebuah kanal jaringan dengan aman.

Rancang bangun *server VPN* ini merupakan suatu usaha untuk menyediakan keamanan transportasi perlewatan data pada jaringan komputer. Menyediakan jalur komunikasi atau transmisi data yang terenkripsi tanpa harus membuat jalur komunikasi *point-to-point* secara fisik atau menyewa jasa perusahaan telekomunikasi, tapi dengan memanfaatkan infrastruktur internet yang telah tersedia.

3.2 Desain Sistem



Gambar 3.1. Blok desain sistem

Dari desain sistem pada gambar 3.1, *tunnel VPN* akan terbentuk untuk melakukan koneksi ketika *client* telah memiliki *CA (Certificate Authority)* dan *key* yang diberikan oleh *server* yang dapat digunakan untuk melakukan autentikasi.

3.3 Analisa Kebutuhan Pada Server VPN

Untuk sistem dibutuhkan komponen-komponen yang nantinya diharapkan mampu memenuhi kebutuhan selama proses implementasi, dan komponen tersebut meliputi perangkat keras dan perangkat lunak.

3.3.1 Analisa Kebutuhan Perangkat Keras

Server VPN menggunakan sebuah *PC (Personal Computer)* untuk implementasinya. Berikut merupakan spesifikasi perangkat keras yang digunakan.

Tabel 3.1.Spesifikasi perangkat keras

No	Device	Keterangan
1	*Processor*	Intel Core 2 Duo E7400 2.8 GHz
2	*Memory*	1 GHz
3	*Hardisk*	80 GHz

Spesifikasi pada tabel 3.1 merupakan spesifikasi perangkat keras yang digunakan oleh penulis untuk mengimplementasi *server VPN*.

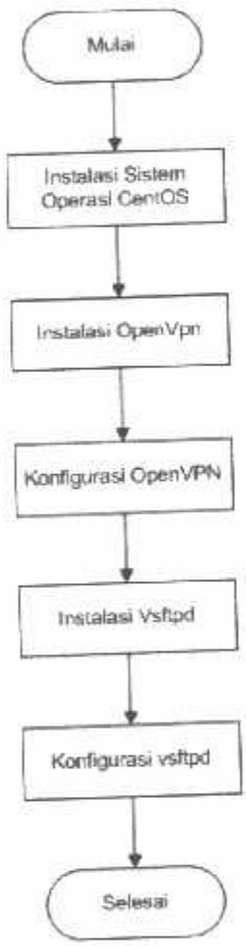
3.3.2 Analisa Kebutuhan Perangkat Lunak

Server VPN menggunakan sistem operasi berbasis *linux*. Penggunaan *linux* disini menggunakan *distro CentOS*. *Distro* ini dipilih karena kestabilan dan kehandalannya untuk digunakan sebagai *server*. Selain itu dibutuhkan perangkat–perangkat lunak lain seperti yang terdapat pada tabel 3.2.

Tabel 3.2.Spesifikasi perangkat lunak

No	Software	Keterangan
1	*CentOS 6.0*	Sistemoperasi
2	*OpenVPN*	*VPN*
3	*Vsftpd*	*Server FTP*

Setelah ditentukan spesifikasi perangkat lunak kemudian dilakukan instalasi dengan tahap – tahap seperti pada gambar 3.2.



Gambar 3.2. Diagram alir
tahap–tahap instalasi kebutuhan *server VPN*

Proses pertama adalah instalasi *CentOS* yang akan digunakan sebagai sistem operasi *server VPN*. Kemudian instalasi *OpenVPN* yang akan digunakan untuk penyedia layanan *VPN*, setelah *OpenVPN* diinstal maka harus dikonfigurasi untuk membuat *CA*

(Certificate Authority) dan *key* yang nantinya digunakan untuk membuka koneksi antara *client* dan *server VPN*.

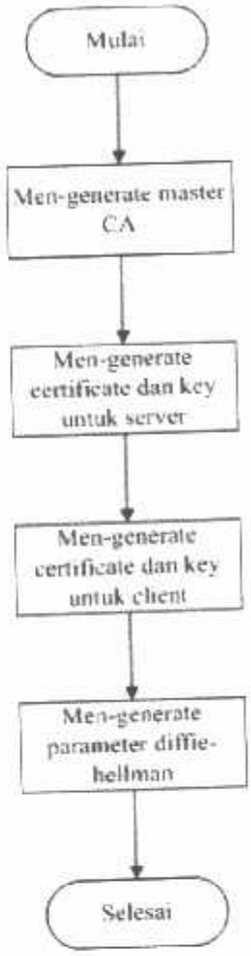
3.4 Perancangan Sistem

Untuk menyediakan transmisi data yang aman maka diperlukan proses enkripsi pada data yang dikirimkan, oleh karena itu proses enkripsi menjadi *point* penting dalam mengimplementasi sistem yang dibuat. Selain proses enkripsi sistem autentikasi dari *VPN* yang dibuat adalah langkah awal dari berhasilnya dalam mengimplementasi sistem.

3.4.1 Metode Autentikasi

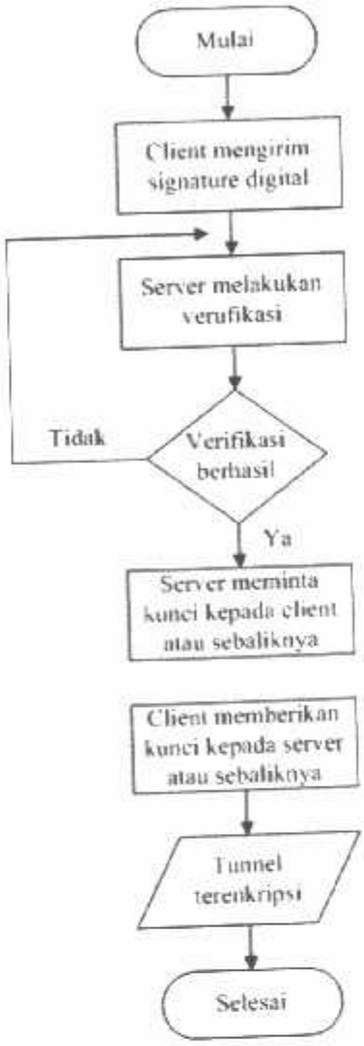
Metode autentikasi yang digunakan adalah menggunakan *PKI (Public Key Infrastructur)*, *PKI* adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah penyangkalan.

Sebelum metode autentikasi *PKI (Public Key Infrastructure)* dapat diimplementasikan perlu dilakukan pembuatan dengan tahap-tahap seperti pada gambar 3.3.



Gambar 3.3. Diagram alir pembuatan *PKI*

Setelah pembuatan *PKI* selesai, selanjutnya proses autentikasi menggunakan metode *PKI* dapat dilaksanakan. Berikut merupakan diagram alir proses autentikasi menggunakan *PKI* :

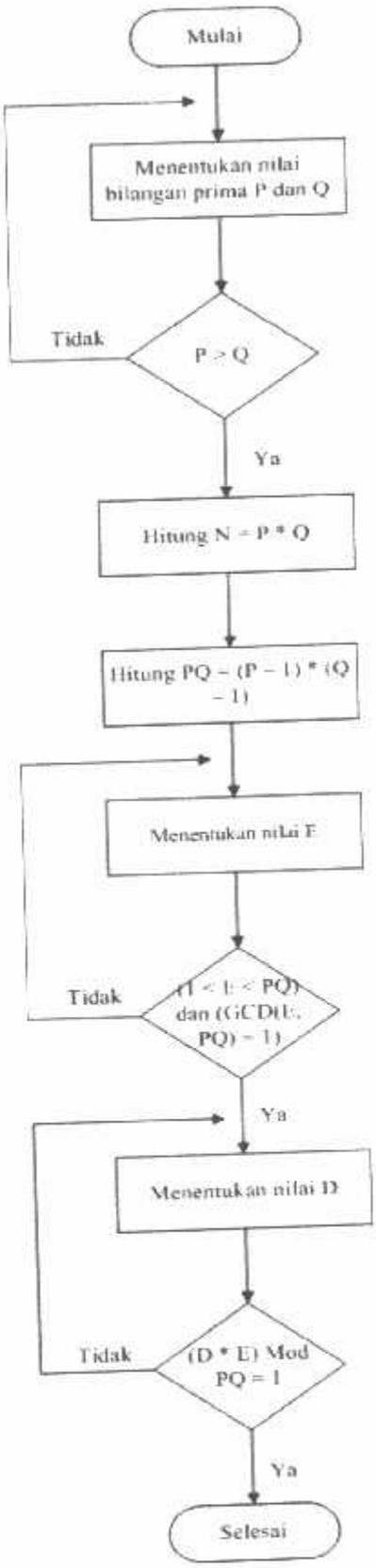


Gambar 3.4. Proses autentikasi

3.4.2 Enkripsi Dan Dekripsi

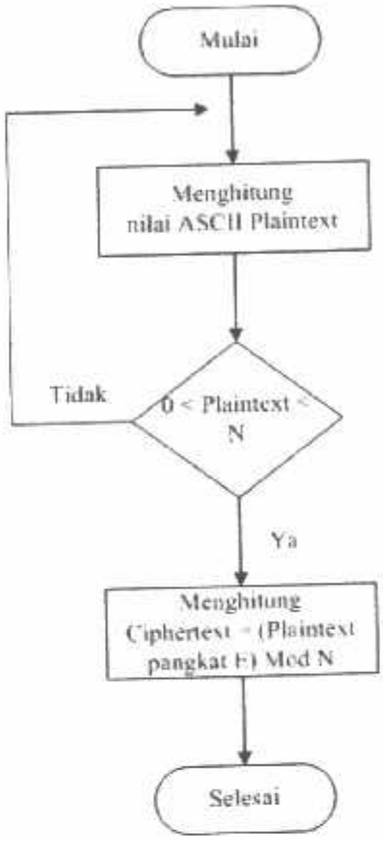
Untuk meningkatkan keamanan transmisi data maka perlu dilakukan proses enkripsi. Dalam sistem ini algoritma *RSA* digunakan untuk metode enkripsi.

Sebelum dapat melakukan proses enkripsi terlebih dahulu harus dibuat *public key* dan *private key*. Berikut merupakan tahap-tahap pembuatannya :

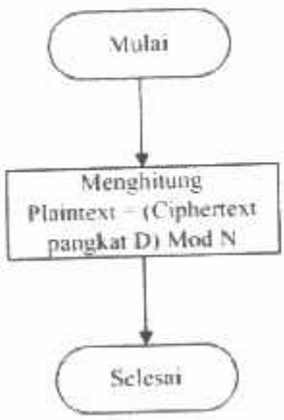


Gambar 3.5. Diagram alir
proses pembuatan *public key* dan *private key*

Setelah *public key* dan *private key* berhasil dibuat langkah selanjutnya adalah melakukan proses enkripsi seperti pada gambar 3.6.



Gambar 3.6. Proses enkripsi



Gambar 3.7. Proses dekripsi

Dari gambar 3.6 dan gambar 3.7 *ciphertext* merupakan data atau informasi yang telah mengalami proses enkripsi sedangkan *plaintext* merupakan data atau informasi yang belum mengalami enkripsi.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem

Dalam bab ini membahas tentang implementasi dan pengujian dari sistem yang dibuat. Secara umum implementasi dan pengujian ini bertujuan untuk mengetahui apakah piranti yang telah direalisasikan dapat bekerja sesuai dengan perencanaan yang telah direncanakan.

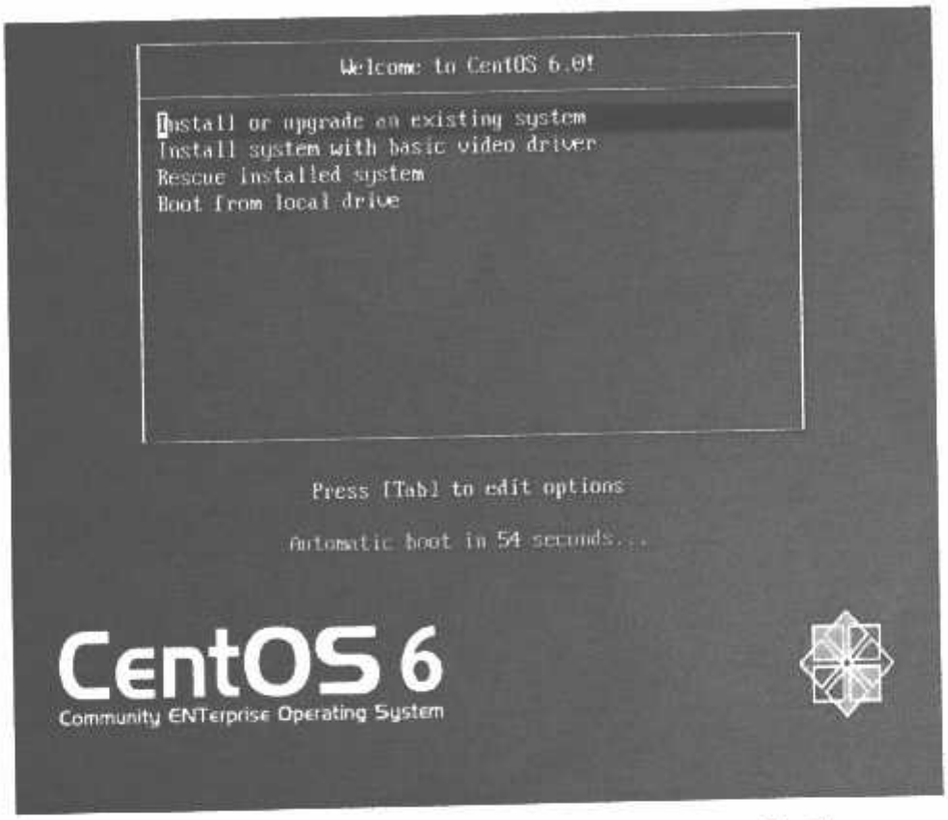
4.1.1 Konfigurasi Server VPN

Sesuai dengan perancangan yang telah dilakukan, berikut merupakan implementasi tahap – tahap instalasi kebutuhan pada sisi *server VPN*.

4.1.1.1 InstalasiCentOS

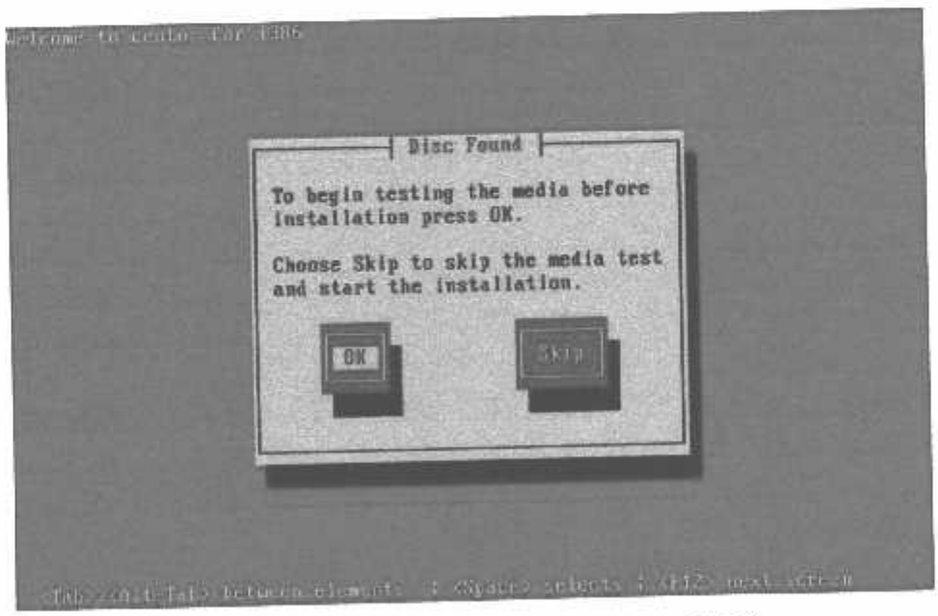
Berikut ini adalah langkah – langkah instalasi *CentOS* untuk sistem operasi *server VPN* :

1. Konfigurasi *boot device priority* pada *bios* agar melakukan *booting*pada *cd-room*.
2. Jika *booting*dari *cd-room* berhasil maka akan muncul dilayar seperti gambar 4.1.



Gambar 4.1. Tampilan pertama kali saat instalasi *CentOS 6.0*

3. Setelah booting akan muncul tampilan pengujian media instalasi seperti gambar 4.2.

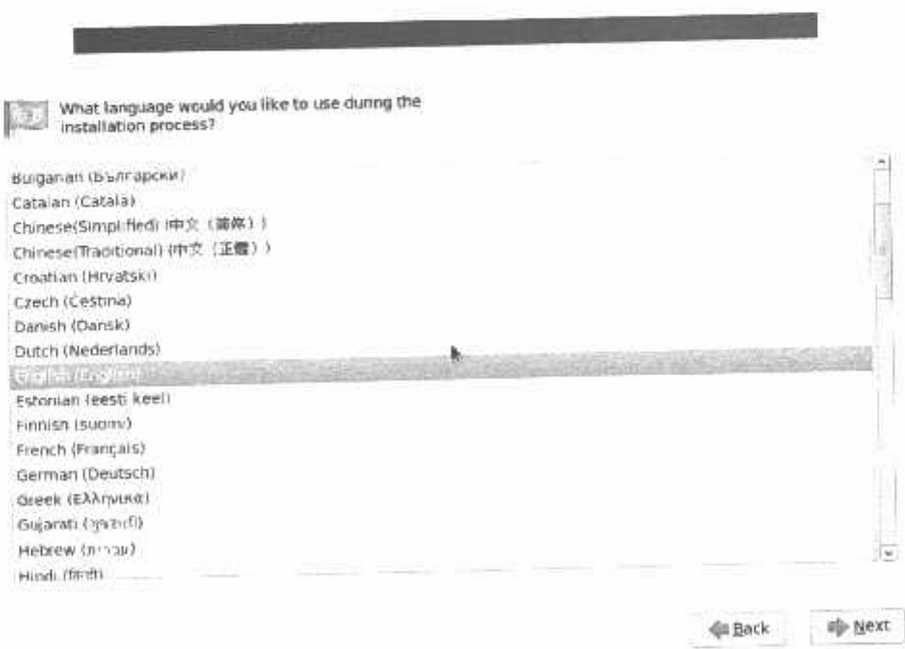


Gambar 4.2. Pengujian media instalasi *CentOS 6.0*

4. Setelah melakukan pengujian media instalasi akan muncul tampilan seperti gambar 4.3.

Gambar 4.3. Tampilan setelah melakukan pengujian media instalasi

5. Pemilihan bahasa yang akan digunakan selama proses instalasi *CentOS 6.0*



Gambar 4.4. Pemilihan bahasa yang digunakan

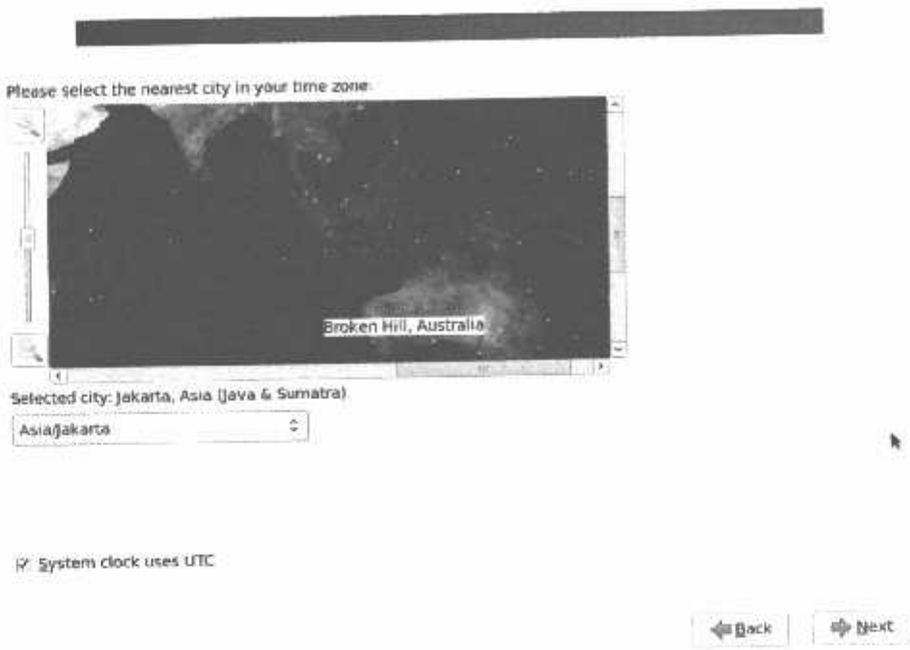
6. Memilih jenis *device* yang akan digunakan selama instalasi *CentOS 6.0*.

Gambar 4.5. Memilih jenis *device* yang digunakan

7. Memberi nama komputer agar dikenali di jaringan.

Gambar 4.6. Pemberian nama komputer

8. Memilih kota terdekat yang akan digunakan sebagai zona waktu.

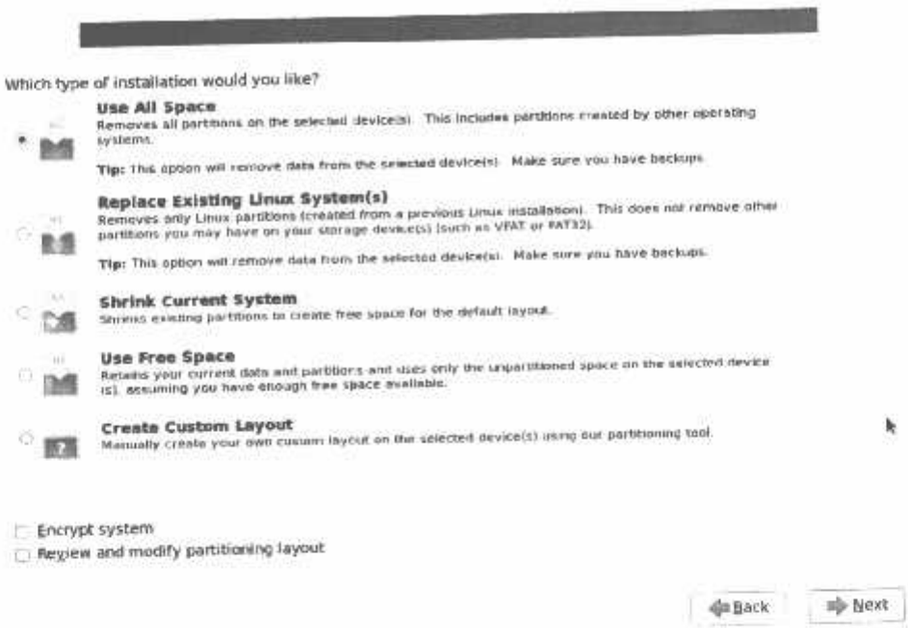


Gambar 4.7. Pemilihan zona waktu

9. Memberi *password* yang akan digunakan sebagai *super user (Root)*.

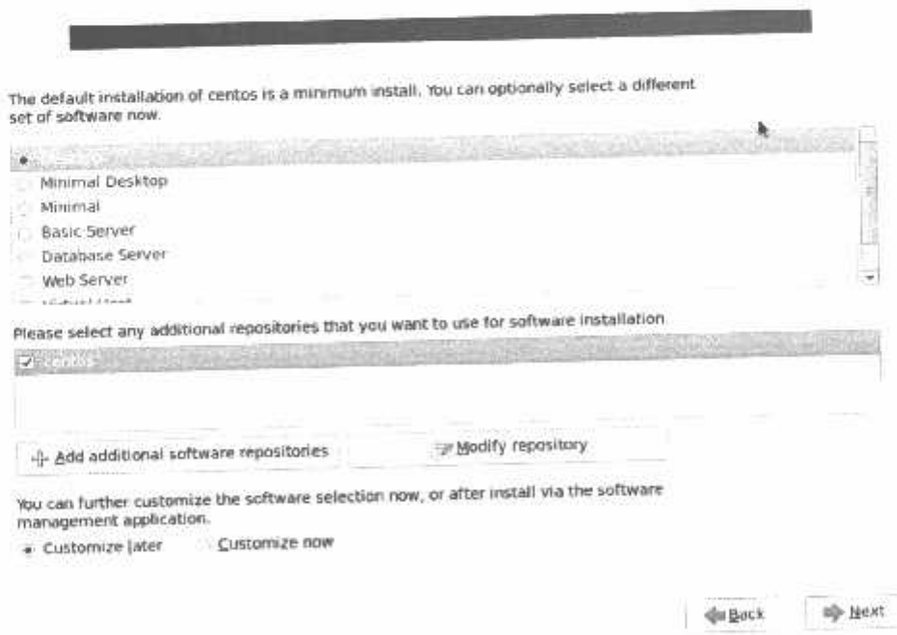
Gambar 4.8. Pemberian *password* untuk *super user*

10. Memilih jenis partisi yang diinginkan untuk instalasi *Centos 6.0.*



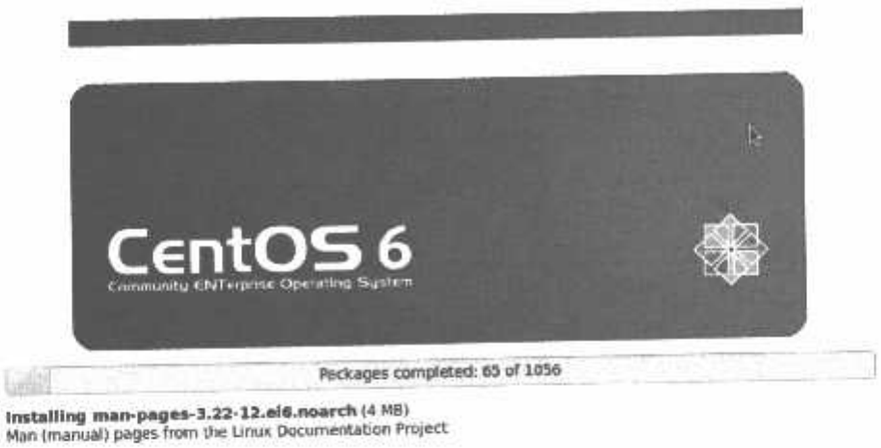
Gambar 4.9. Pemilihan jenis instalasi

11. Memilih jenis instalasi apakah *CentOS* akan digunakan untuk keperluan desktop biasa atau untuk fungsi yang lebih spesifik seperti sebuah *web server.*



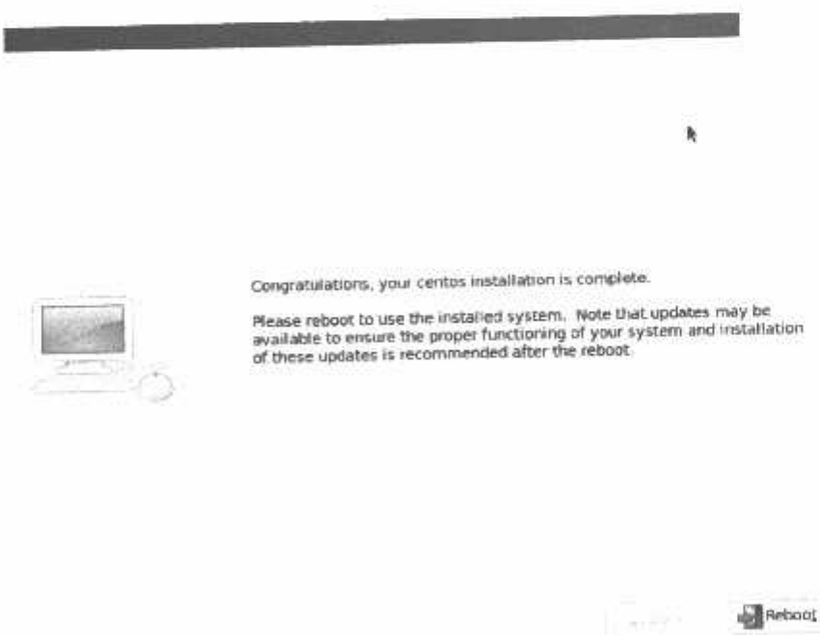
Gambar 4.10. Pemilihan jenis instalasi

12. Tampilan progress instalasi *CentOS 6.0*akan muncul seperti gambar 4.11



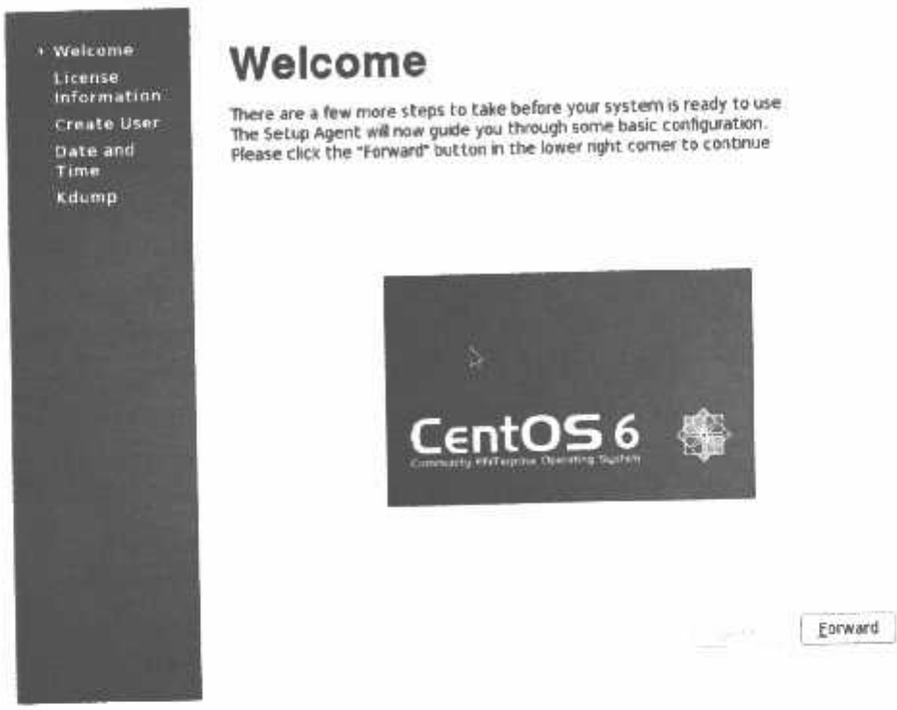
Gambar 4.11. Progres instalasi *CentOS 6.0*

13. Setelah instalasi *CentOS 6.0* selesai akan muncul tampilan untuk meminta *reboot* seperti gambar 4.12.



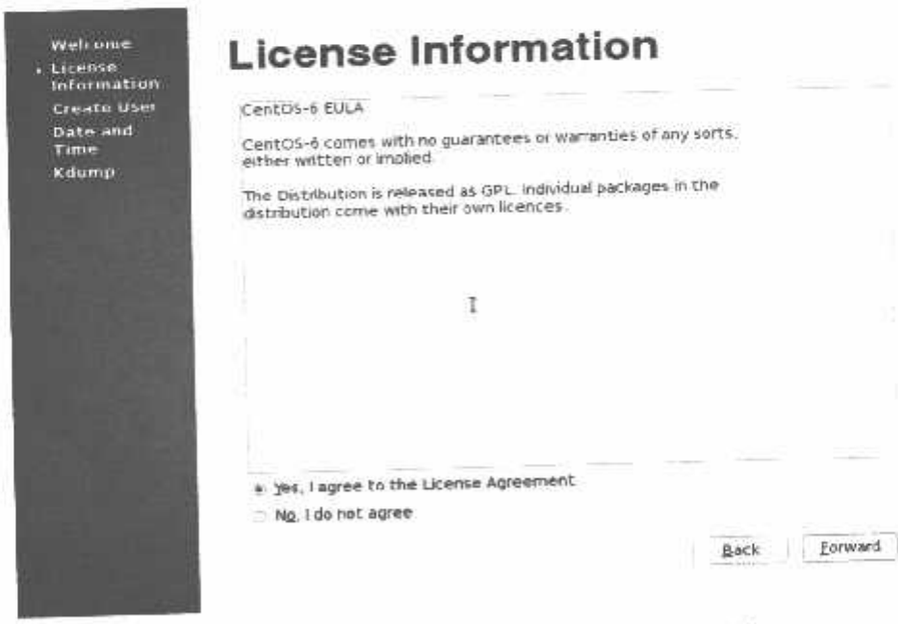
Gambar 4.12. Tampilan meminta *reboot* setelah instalasi

14. Setelah *reboot* akan muncul tampilan penyambut seperti gambar 4.13 berikut.



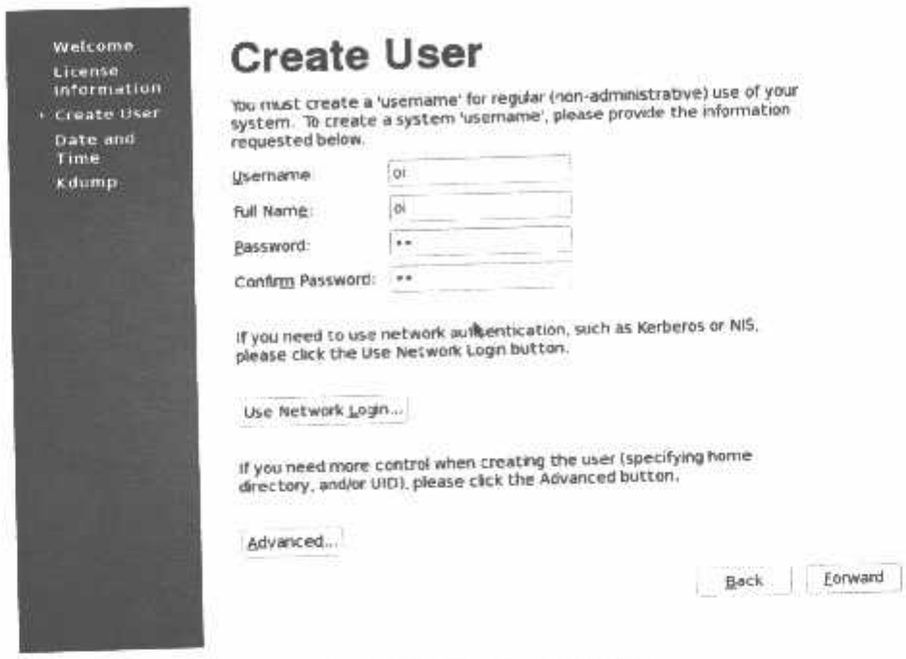
Gambar 4.13. Tampilan setelah *reboot*

15. Tampilan informasi tentang lisensi *CentOS 6.0.*



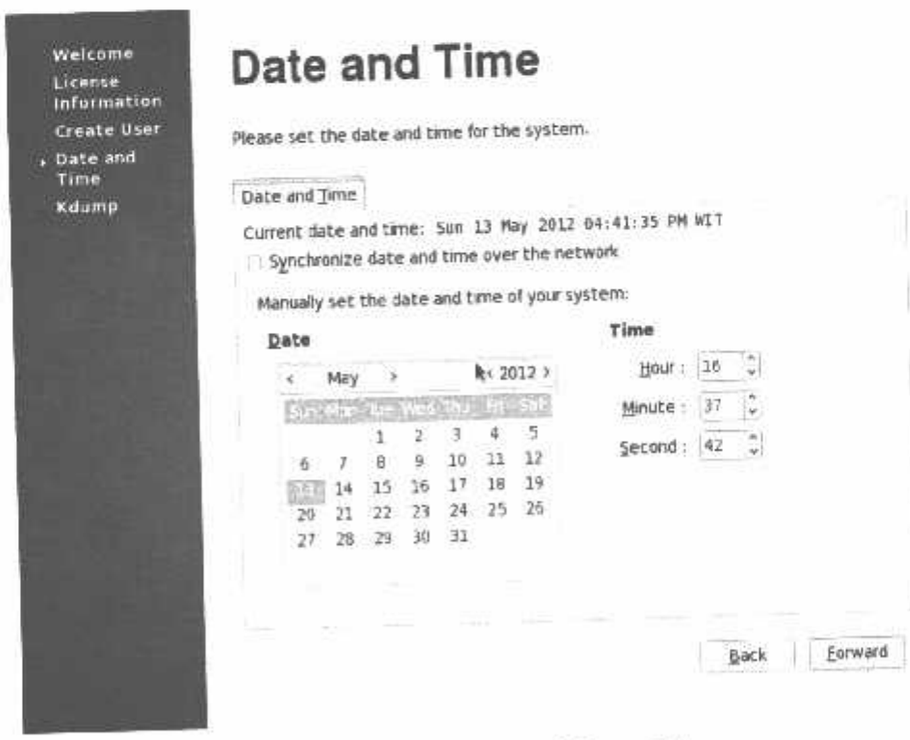
Gambar 4.14. Informasi tentang lisensi *CentOS 6.0*

16. Pembuatan *user* yang akan digunakan untuk *login* kedalam sistem operasi.



Gambar 4.15. Pembuatan *user*

17. Melakukan *setting* untuk tanggal dan waktu untuk sistem.

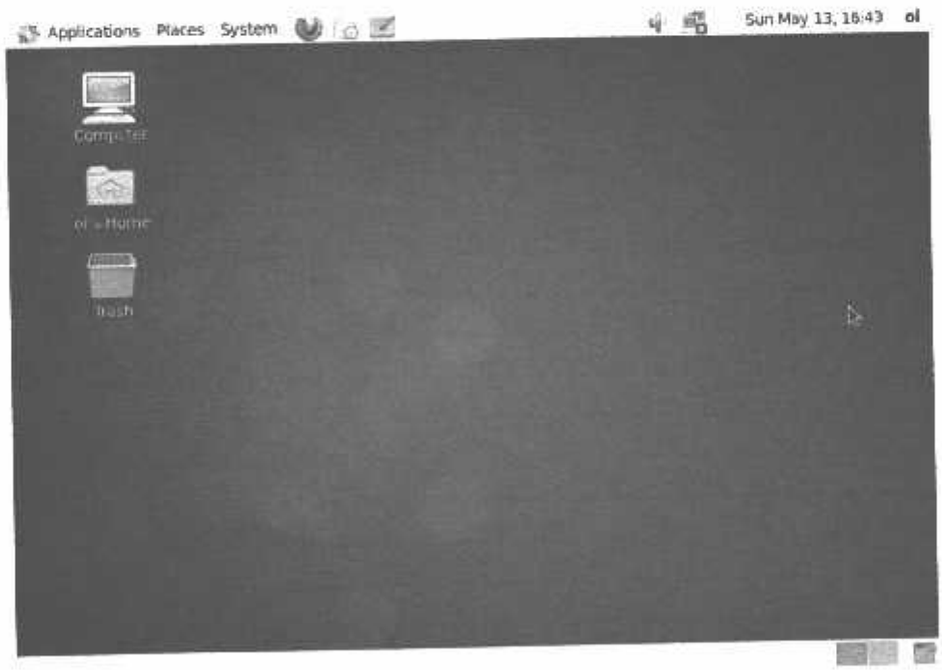


Gambar 4.16.*Setting* tanggal dan waktu

18. Jendela untuk *login* kedalam sistem.

Gambar 4.17.*Login* kedalam sistem

19. Setelah semua proses instalasi selesai dan melakukan *login*akan muncul tampilan seperti gambar 4.18.



Gambar 4.18. Tampilan *CentOS 6.0*

4.1.1.2 Instalasi Dan Konfigurasi OpenVPN Pada Server

Agar *server* dapat bekerja sesuai dengan yang diharapkan, maka pada tahap instalasi dan konfigurasi *OpenVPN* harus dilakukan dengan teliti.

4.1.1.2.1 Instalasi OpenVPN

Berikut ini adalah langkah – langkah instalasi *OpenVPN* untuk keamanan transmisi data :

1. Masuk ke terminal *CentOS* kemudian mengganti hak akses menjadi *super user*.
2. setelah hak akses menjadi *super user* kemudian mengetikkan *yum install openvpn* pada terminal Seperti pada gambar 4.19.

Gambar 4.19. Proses instalasi *OpenVPN* di *CentOS*

4.1.1.2.2 Pembuatan CA (Certificate Authority) dan Key

Setelah proses instalasi *OpenVPN* selesai maka akan dilakukan pembuatan *CA* dan *key* untuk autentikasi dengan langkah – langkah sebagai berikut :

1. Menginisialisasi *PKI (Public Key Infrastructure)* dengan perintah sebagai berikut :

   . ./vars

   ./clean-all

   ./build-ca

2. Kemudian membuat *CA* dan *key* untuk *server* dengan perintah ***./build-key-server server***.

```
oi@oi-PC:/etc/openvpn/easy-rsa/2.0
File  Edit  View  Search  Terminal  Help
[root@oi-PC 2.0]# ./build-key-server server
Generating a 2048 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) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [server]:server
Name [changeme]:
Email Address [mail@host.domain]:

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/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JT'
localityName          :PRINTABLE:'Malang'
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [server]:server
Name [changeme]:
Email Address [mail@host.domain]:

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/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JT'
localityName          :PRINTABLE:'Malang'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'mail@host.domain'
Certificate is to be certified until Jul 28 03:35:43 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
[root@oi-PC 2.0]#
```

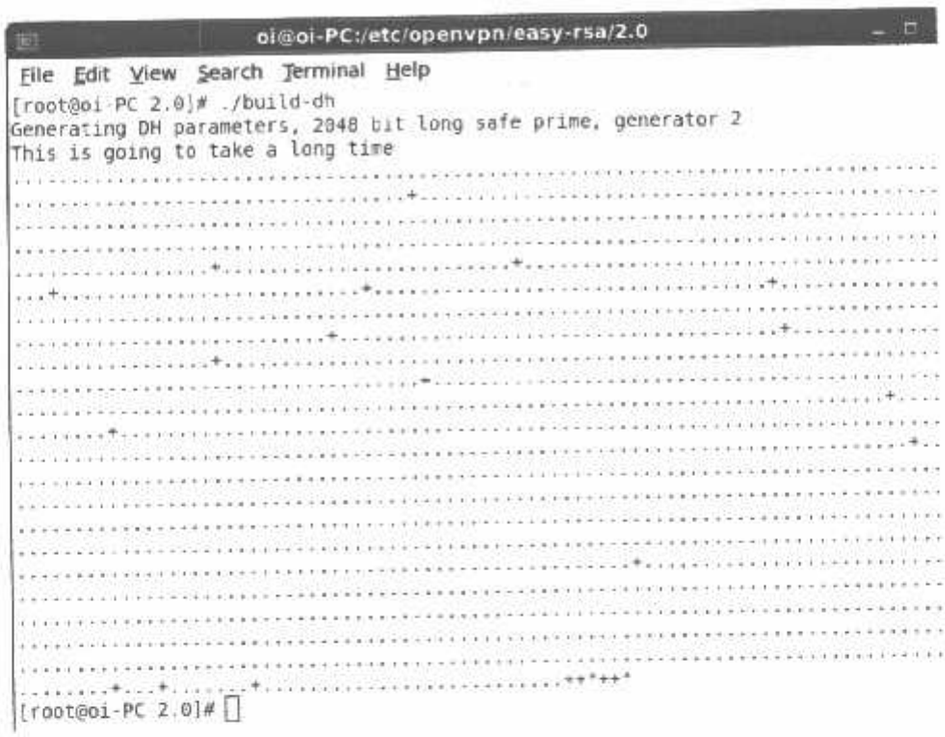
Gambar 4.20. Pembuatan *CA* dan *key*untuk *server*

3. Membuat *CA* dan *key* untuk client dengan perintah ***./build-key client1***.

```
oi@oi-PC:/etc/openvpn/easy-rsa/2.0
File  Edit  View  Search  Terminal  Help
[root@oi-PC 2.0]# ./build-key client1
Generating a 2048 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) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [client1]:client1
Name [changeme]:
Email Address [mail@host.domain]:

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/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JT'
localityName          :PRINTABLE:'Malang'
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [client1]:client1
Name [changeme]:
Email Address [mail@host.domain]:

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/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JT'
localityName          :PRINTABLE:'Malang'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'client1'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'mail@host.domain'
Certificate is to be certified until Jul 28 03:37:37 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
[root@oi-PC 2.0]#
```

Gambar 4.21. Pembuatan *CA* dan *key* untuk *client*

4. Selanjutnya membuat parameter *Diffie Hellman (DH)* dengan perintah ***./build-dh***.



Gambar 4.22. Pembuatan parameter *diffie-hellman*

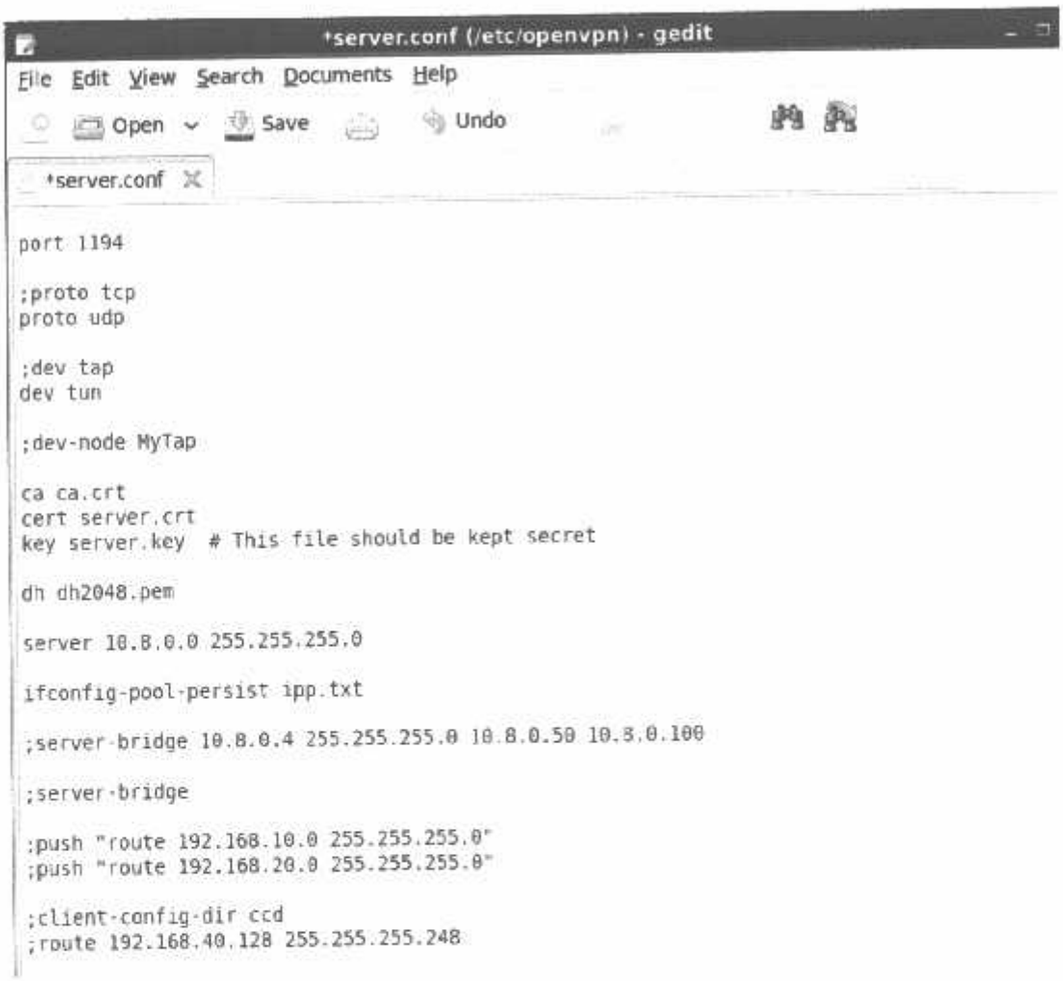
Berikut Hasil pembuatan *CA* dan *key* yang tersimpan pada direktori */etc/openvpn/easy-rsa/2.0/keys*.

Tabel 4.1. Hasil pembuatan *CA* dan *key* beserta penjelasannya

Nama	Dibutuhkan Oleh :	Fungsi	Rahasia
ca.crt	Server dan semua client	CA root	Tidak
ca.key	Server	Key CA root	Ya
dh{n}.pem	Server	Parameter diffie hellman	Tidak
server.crt	Server	Certificate server	Tidak
server.key	Server	Key server	Ya
client1.crt	Client	Certificate client	Tidak
client1.key	Client	Key client	Ya

4.1.1.2.3 Pembuatan Berkas Konfigurasi Server VPN

Berkas ini berjalan pada sisi *server VPN* dan berkas ini yang akan menjadi acuan untuk membuat konfigurasi disisi *client*. berikut merupakan isi dari berkas *server.conf* yang telah dibuat.



```
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252

;learn-address ./script

;push "redirect-gateway def1 bypass-dhcp"

;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

;client-to-client

;duplicate-cn

keepalive 10 120

;tls-auth ta.key 0 # This file is secret

;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

comp-lzo

;max-clients 100

;user nobody
;group nobody

persist-key
persist-tun

status openvpn-status.log
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

;client-to-client

;duplicate-cn

keepalive 10 120

;tls-auth ta.key 0 # This file is secret

;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

comp-lzo

;max-clients 100

;user nobody
;group nobody

persist-key
persist-tun

status openvpn-status.log

;log         openvpn.log
;log-append  openvpn.log

verb 3

;mute 20
```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 INS

Gambar 4.23. Berkas konfigurasi *server VPN*

Perangkat virtual seperti pada gambar merupakan perangkat yang akan digunakan untuk *tunneling* pada sistem *VPN*. *IP address* 10.8.0.1 yang ada pada perangkat virtual berfungsi sebagai *IP* yang akan memprivasi dari jaringan publik.

4.2 Pengujian Sistem

Karena konsep *VPN* yang menekankan tidak hanya koneksi tapi juga pada keamanan data, maka Pada pengujian sistem akan dilakukan beberapa pengujian sebagai berikut :

1. Pengujian koneksi antara *server* dan *client*.
2. Pengujian privasi jaringan.
3. Pengujian enkripsi *VPN*.

Perangkat pendukung pengujian terdiri dari beberapa perangkat keras dan perangkat lunak yang tertera pada tabel 4.1.

Tabel4.2. Perangkat pengujian sistem

Perangkat Keras	*PC* sebagai *server VPN* dan server FTP
	Laptop sebagai *client VPN*
	Modem ADSL sebagai akses internet dari *ISP* pada sisi *server VPN* menggunakan *IP* publik
	Modem ADSL sebagai akses internet dari *ISP*pada sisi *clientVPN*
Perangkat Lunak	*CentOS 6.0* sebagai *server VPN*
	OpenVPN sebagai protokol *VPN*
	Windows 7 sebagai sistem operasi *clientVPN*
	Wireshark sebagai *protocol analyzer*pada sisi *client*
	VSFTPD sebagai *server FTP* pada sisi *server*

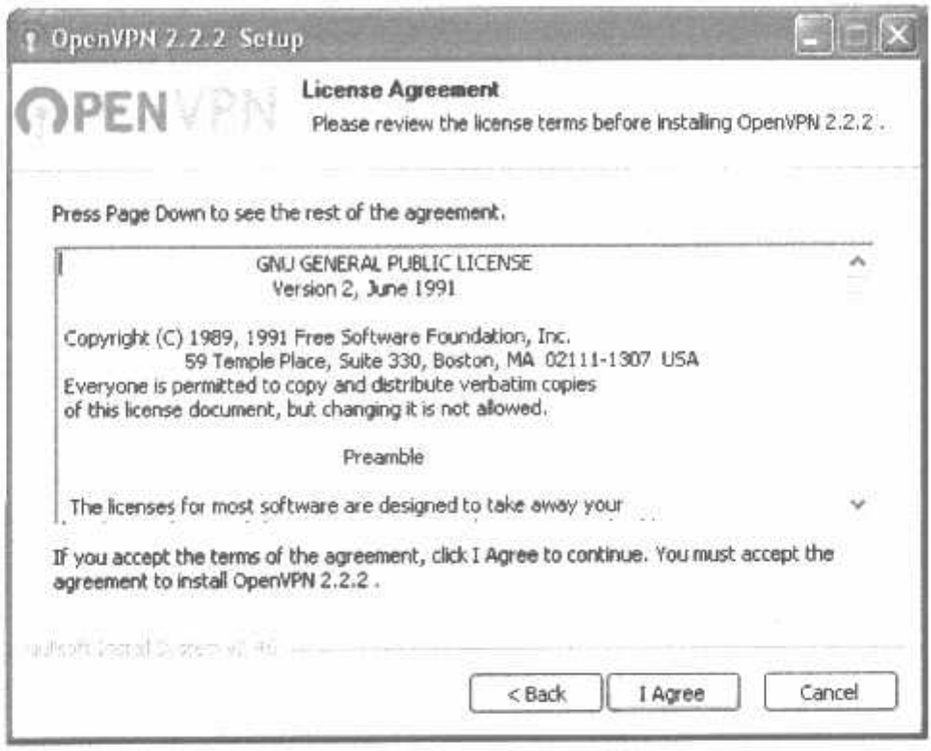
4.2.1 Instalasi Dan Konfigurasi OpenVPN Client

Sebelum dapat melakukan koneksi antara *client* dan *server*, *client* terlebih dahulu harus dilakukan instalasi dan konfigurasi *OpenVPNclient*.Berikut merupakan tahapan instalasi dan konfigurasi *OpenVPNclient*.

1. *Double* klik *berkas* instalasi *OpenVPNclient*, maka akan muncul tampilan seperti pada gambar.

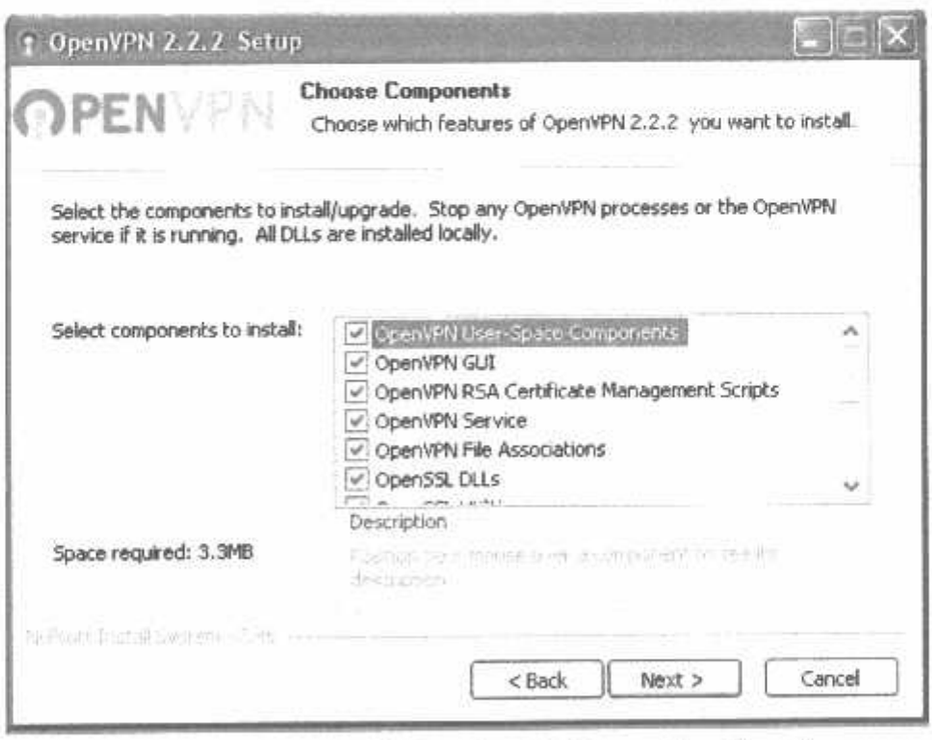
Gambar 4.26. Tampilan penyambut instalasi *OpenVPN*

2. Klik *Next*.



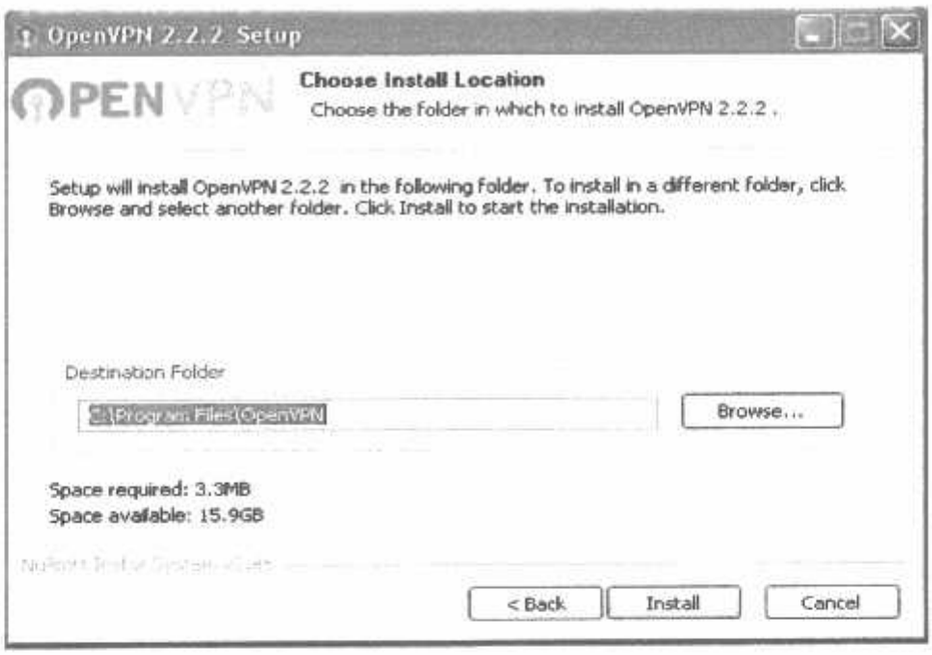
Gambar 4.27. Tampilan *license agreementOPenVPN*

3. Klik *I Agree*.



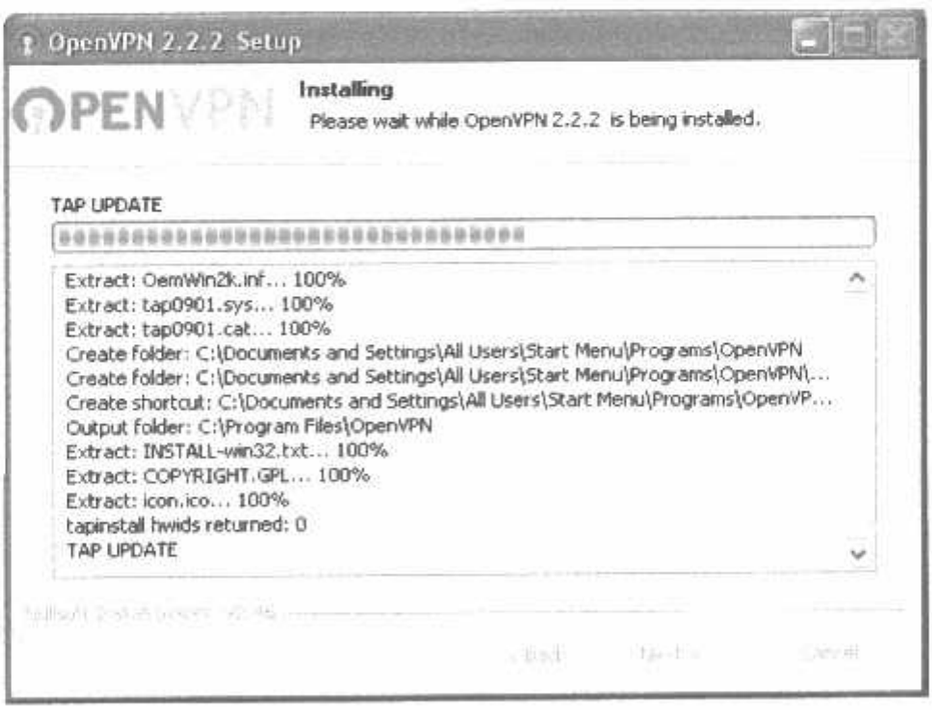
Gambar 4.28. Memilih fitur *OpenVPN* yang akan diinstal

4. Klik *Next.*



Gambar 4.29. Memilih lokasi instalasi *OpenVPN*

5. Tampilan *progress* instalasi.



Gambar 4.30. Progress instalasi OpenVPN

6. Klik *finish*.

Gambar 4.31.*OpenVPN* telah selesai diinstal

7. Meng-*copyCA* dan *key* hasil *generateOpenVPNserver* ke direktori *C:\Program Files\OpenVPN\config*. Berikut *CA* dan *key* yang diperlukan untuk konfigurasi *OpenVPNclient* :

   Ca.crt

   Client1.key

   Client1.crt

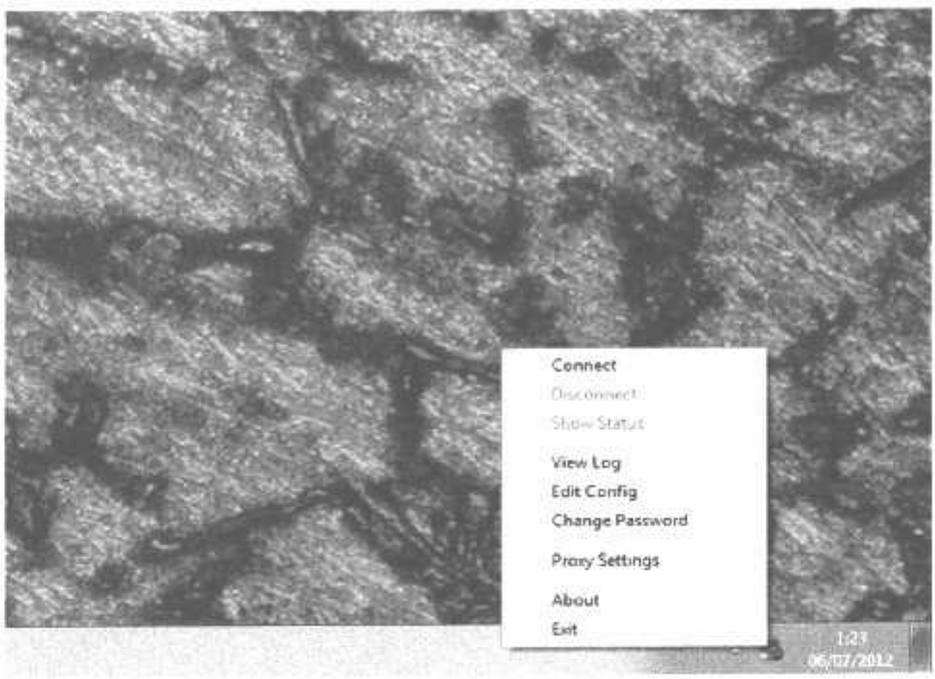
Setelah instalasi *OpenVPN* selesai kemudian dilakukan pembuatan *berkas* konfigurasi untuk *clientOpenVPN*. Berikut merupakan *berkas* konfigurasi untuk *OpenVPNclient* :

Gambar 4.32 *Berkas* konfigurasi *OpenVPNclient*

4.2.2 Membuat Koneksi Dan Melakukan Autentikasi CA dan Key

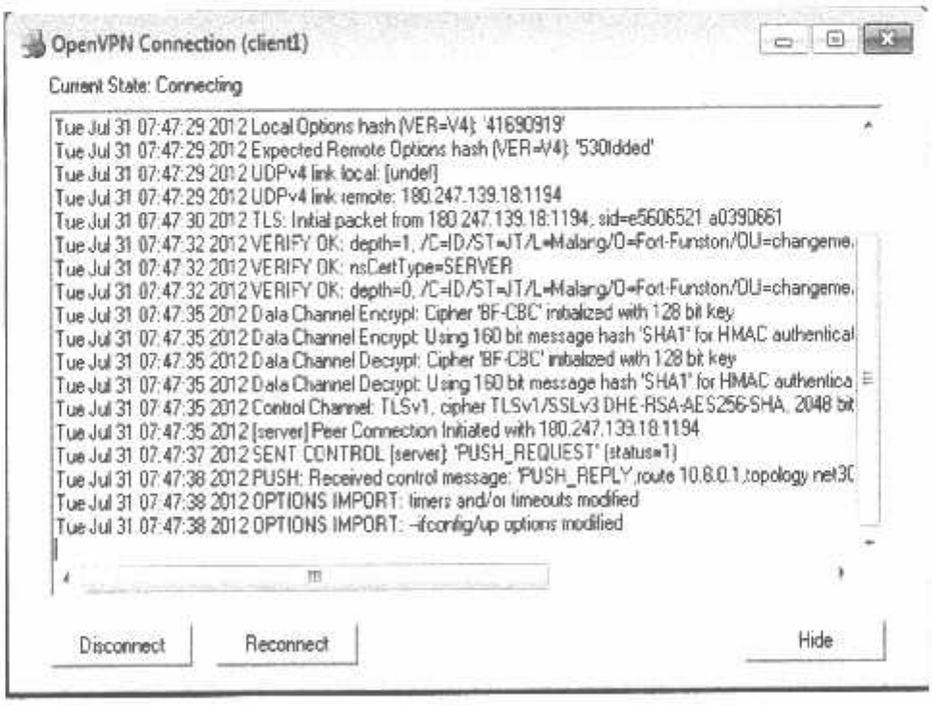
Berikut tahap –tahap pembuatan koneksi dan autentikasi *CA* dan *key* :

1. Masuk *Start menu -> All Programs -> openvpn -> openVPN GUI* kemudian klik.
2. Selanjutnya klik kanan *tray icon OpenVPN* seperti berikut :



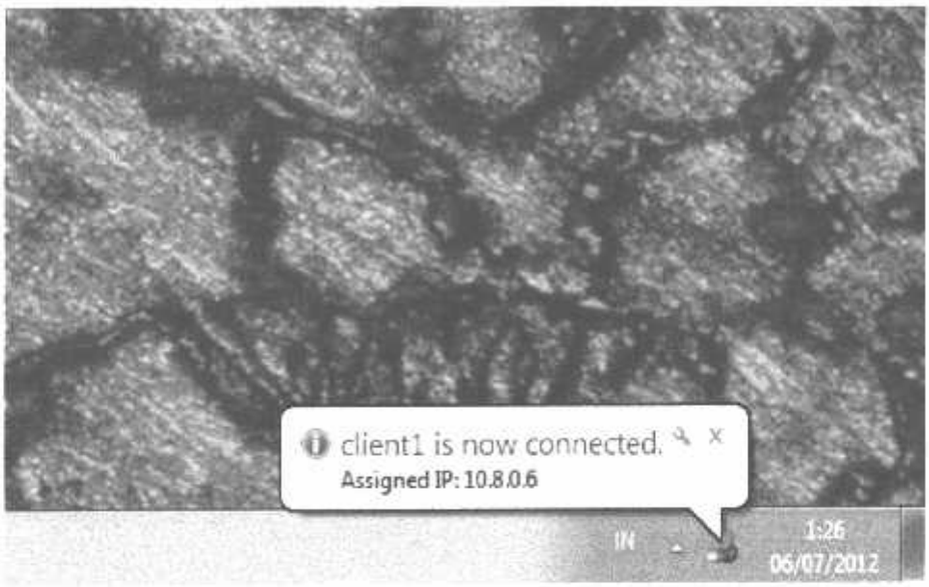
Gambar 4.33. Melakukan koneksi ke *serverVPN*

3. Kemudian klik *connect*. Maka akan muncul jendela autentikasi seperti pada gambar 4.34.



Gambar 4.34. Proses autentikasi *CA* dan *key*

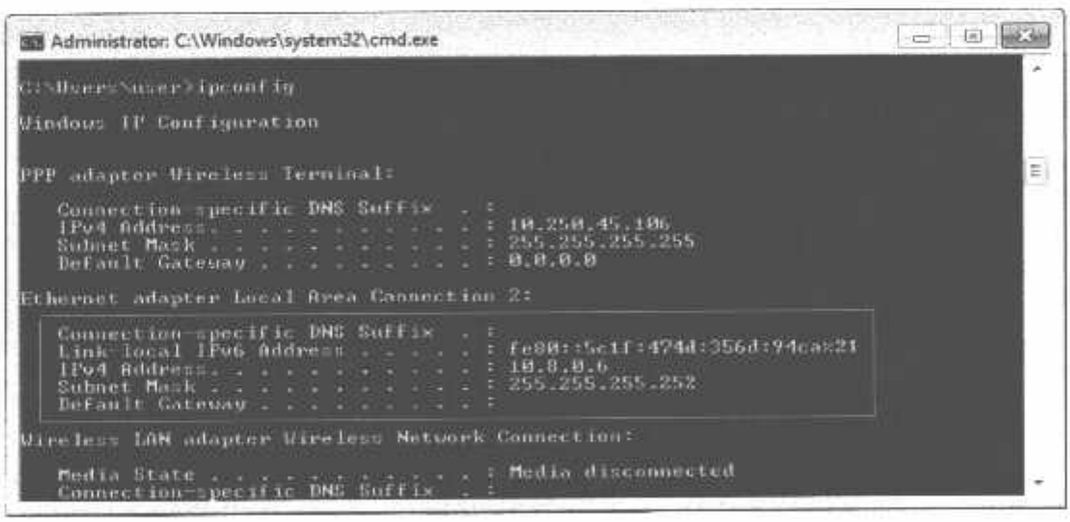
4. Jika proses autentikasi *CA* dan *key* berhasil, maka pada *tray icon OpenVPN* akan muncul notifikasi seperti pada gambar.



Gambar 4.35. Notifikasi bahwa *client* telah terhubung ke *serverVPN*

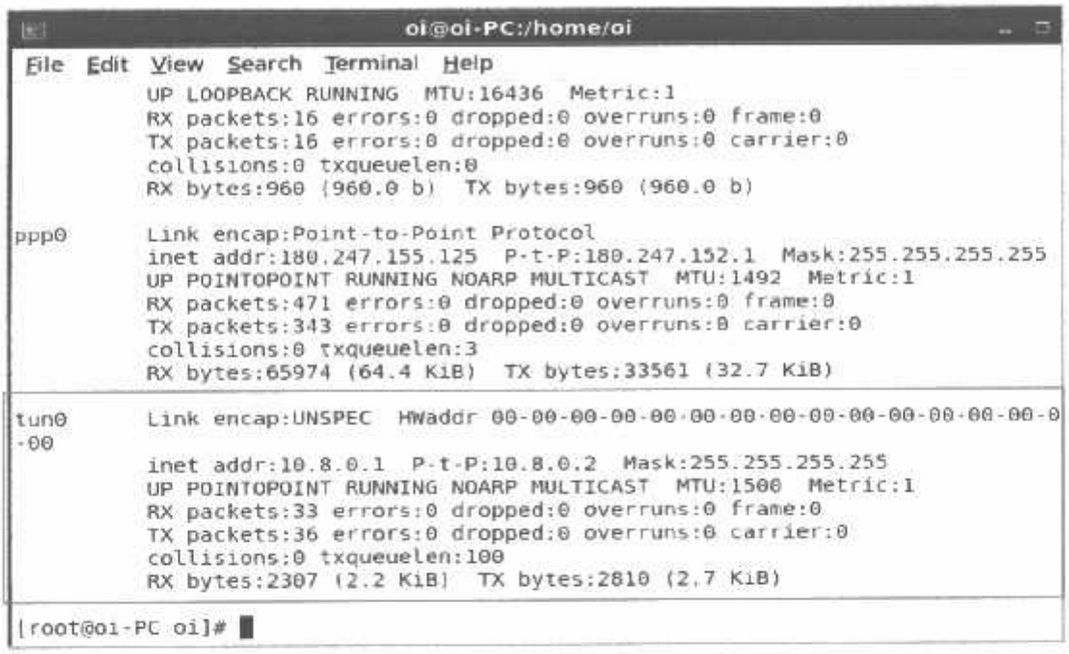
4.2.3 Pengujian KoneksiClient dan Server

Setelah dilakukan proses autentikasi *CA* dan *key* oleh *server* terhadap *client*, selanjutnya adalah mencoba melakukan pengujian koneksi. Rangkaian pengujian berikut adalah untuk mengetahui apakah koneksi *VPN* dapat berjalan dengan baik.



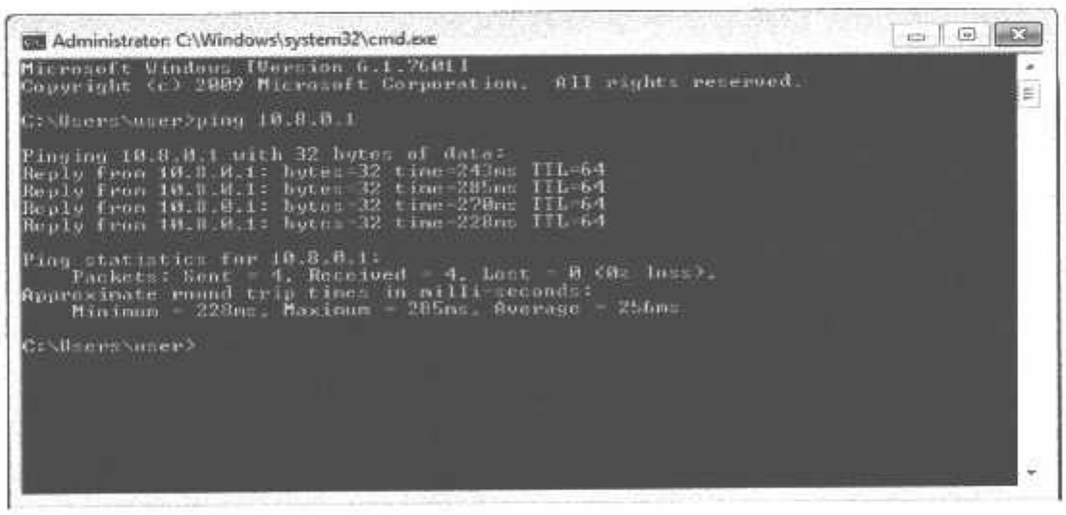
Gambar 4.36. Hasil *ipconfig* pada *client VPN*

Dari gambar 4.36, terlihat alamat *IP* yang didapat oleh *client* saat ini adalah 10.8.0.6 yang akan digunakan untuk koneksi melalui *tunnel*.

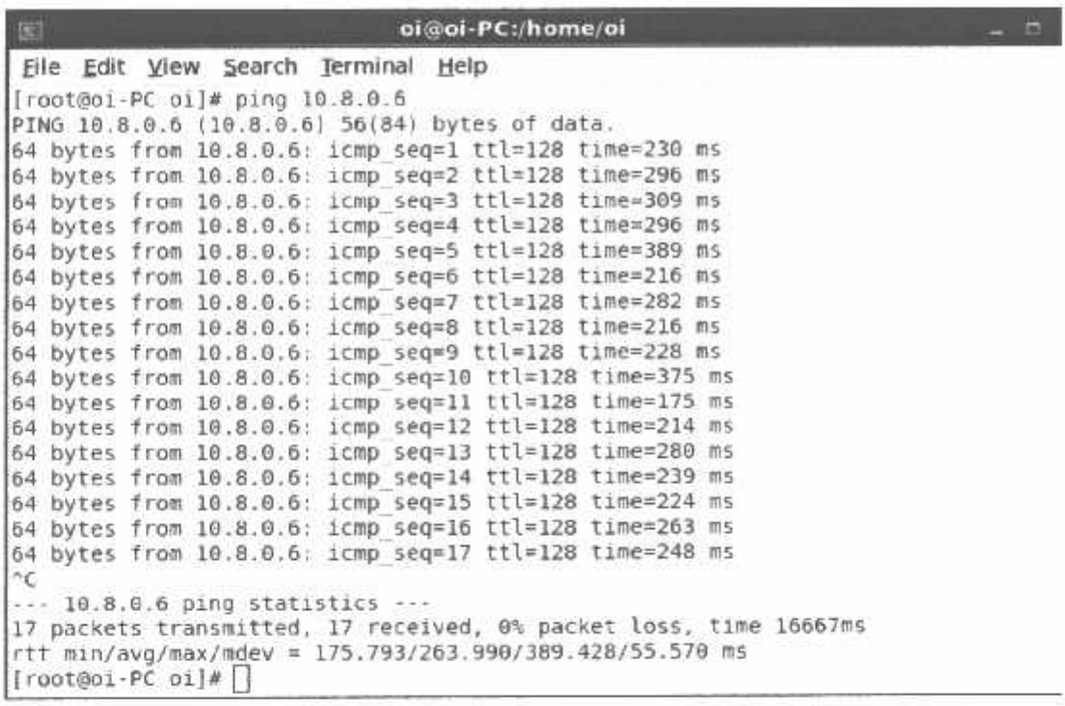


Gambar 4.37. Hasil *ifconfig* pada *server VPN*

Dari gambar 4.37, terlihat alamat *IP* yang digunakan oleh *server* saat ini adalah 10.8.0.1 yang akan digunakan untuk koneksi melalui *tunnel*.Selanjutnya adalah melakukan pengujian koneksi antara keduanya dengan melakukan *ping* dan *tracert* atau *traceroute*.

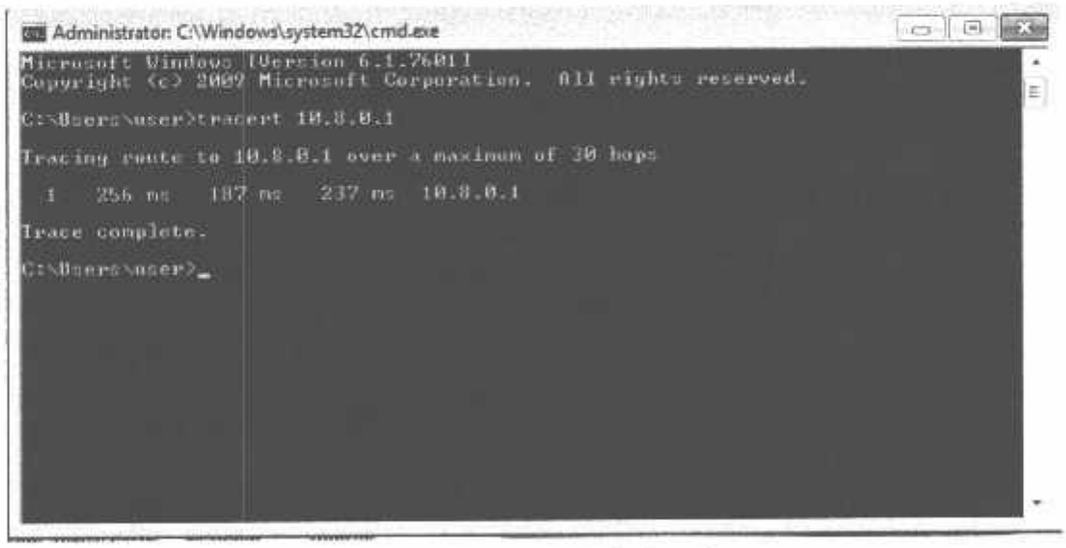


Gambar 4.38. Hasil *ping* dari *client* ke *server*



Gambar 4.39. Hasil *ping* dari *server* ke *client*

Dari pengujian dengan melakukan *ping* seperti pada gambar 4.38 dan gambar 4.39, koneksi antara keduanya dapat berjalan dengan baik karena paket dapat terkirim dengan baik. Selanjutnya adalah melakukan *tracert atau traceroute*, pengujian ini dimaksudkan untuk mengetahui apakah koneksi *point-to-point* melalui *tunnel* antara *client* dan *server* telah terbentuk.



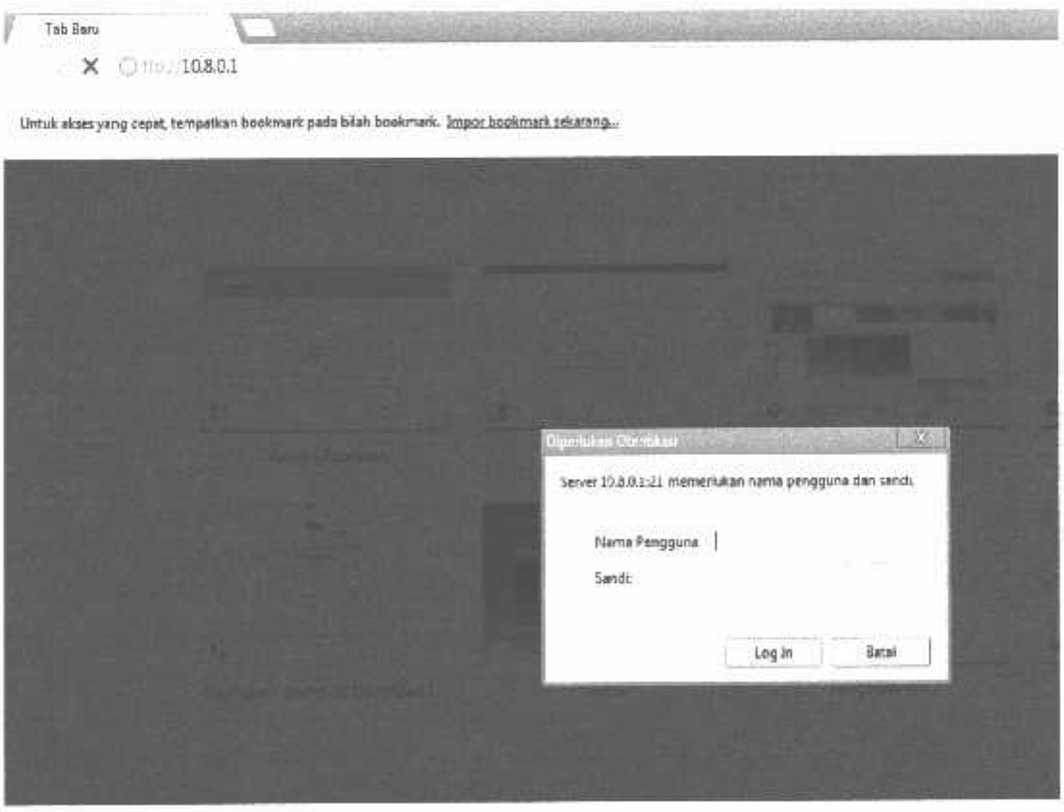
Gambar 4.40. Hasil *tracert* dari *client* ke *server*

```
oi@oi-PC:/home/oi
File  Edit  View  Search  Terminal  Help
[root@oi-PC oi]# traceroute 10.8.0.6
traceroute to 10.8.0.6 (10.8.0.6), 30 hops max, 60 byte packets
 1  10.8.0.6 (10.8.0.6)  404.230 ms  430.302 ms  484.150 ms
[root@oi-PC oi]#
```

Gambar 4.41. Hasil *traceroute* dari *server* ke *client*

Dari hasil pengujian dengan *tracert* atau *traceroute* seperti pada gambar 4.40 dan gambar 4.41, diketahui hanya mengalami satu kali *hops* dan ini membuktikan bahwa koneksi *point-to-point* melalui *tunnel* antara *client* dan *server* berhasil.

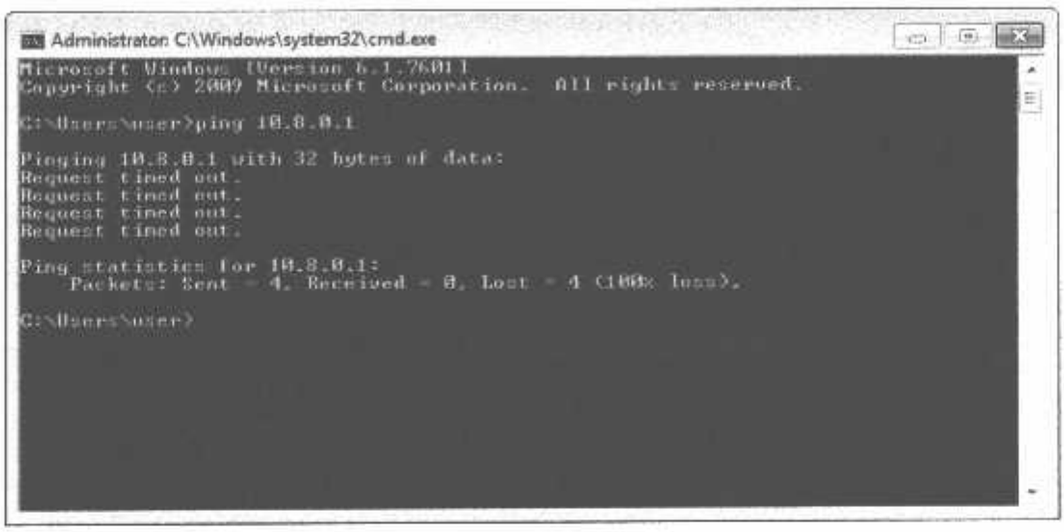
Setelah pengujian koneksi berhasil, kemudian akan dilakukan pengujian untuk mengakses *serverFTP* menggunakan alamat IP *tunnel* dengan memanfaatkan *web browser*.



Gambar 4.42. Akses ke *serverFTP*

4.2.4 Pengujian Privasi Jaringan

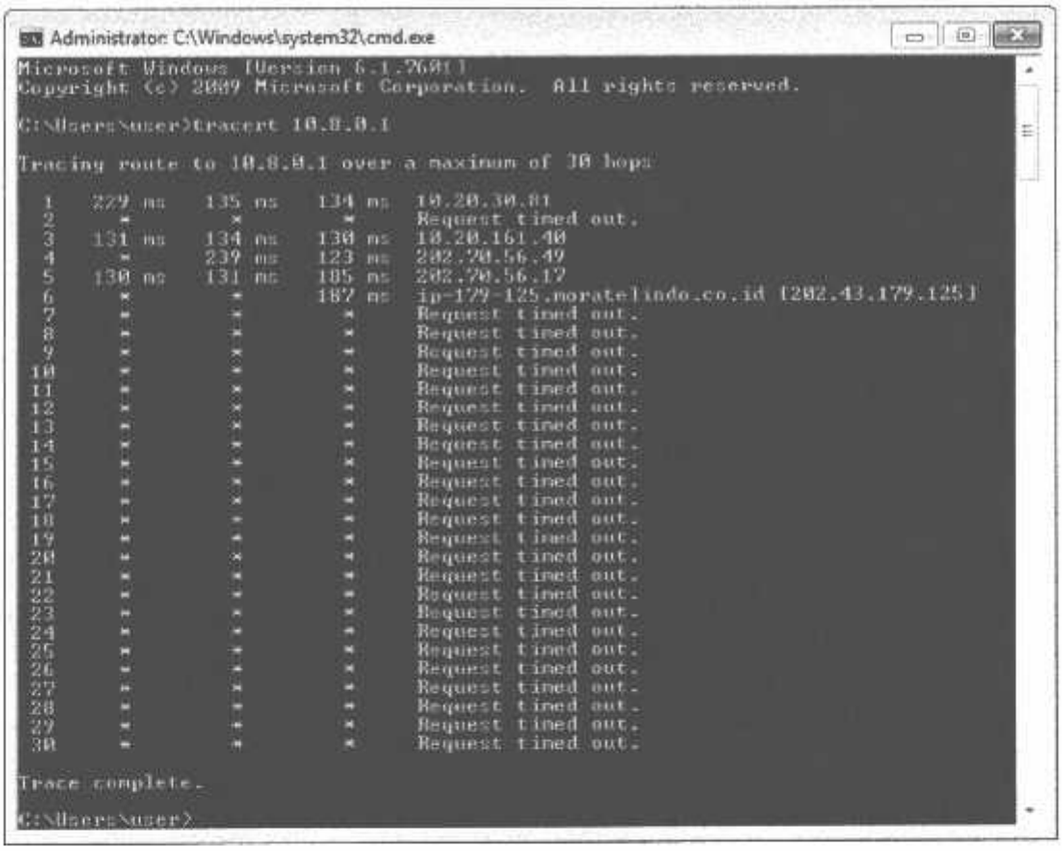
Pengujian ini dilakukan untuk mengetahui apakah *VPN* yang dibuat dapat diakses oleh selain *client VPN*.



Gambar 4.43. Hasil *ping* ke *server*

Dari gambar 4.43, diketahui *ping* ke *server* tidak berhasil karena paket tidak berhasil dikirim.

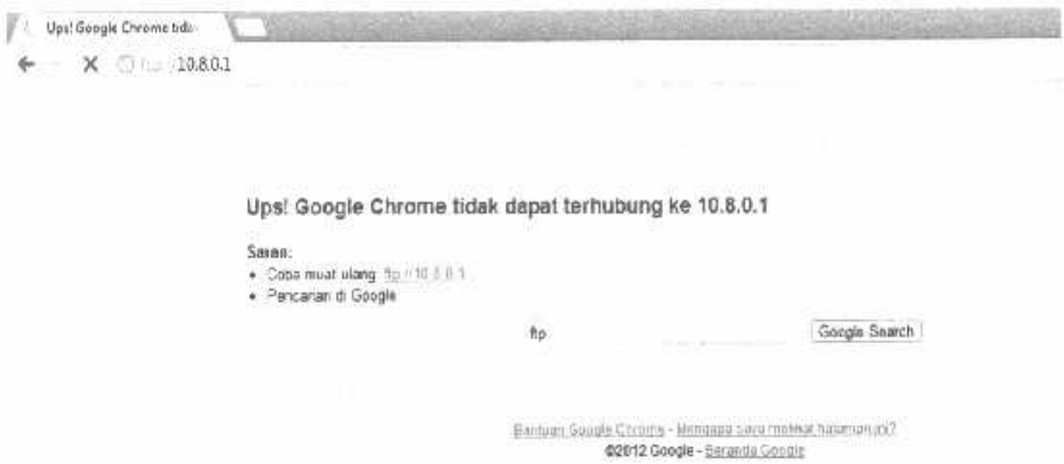
Selanjutnya akan dilakukan *tracert* untuk mengetahui apakah *server* dapat dijangkau atau tidak.



Gambar 4.44. Hasil *tracert* ke *server*

Seperti yang ditunjukkan gambar 4.44, *tracert* ke *server* tidak dapat dilakukan karena melebihi 30 *hops*.

Setelah dilakukan pengujian dengan melakukan *ping* dan *tracert*, sekarang dilakukan pengujian dengan langsung mengakses *serverFTP* dengan memanfaatkan *web browser*.



Gambar 4.45. Mengakses *server* FTP

Dari pengujian yang ditunjukkan gambar 4.45, *web browser* tidak dapat terhubung ke *server*.

Dari rangkaian pengujian yang dilakukan membuktikan bahwa *VPN* tidak dapat diakses oleh selain *clientVPN* meskipun melalui jaringan publik.

4.2.5 Pengujian Enkripsi VPN

Pada pengujian sistem ini merupakan pembuktian kehandalan *VPN* berbasis *OpenVPN*.Tahap – tahap skenario pengujian adalah dengan mengakses *serverFTP* kemudian melakukan *pengunduhan* berkas melalui *VPN* dan tanpa melalui *VPN*, kemudian melakukan *monitoring* data menggunakan perangkat lunak *wireshark*.

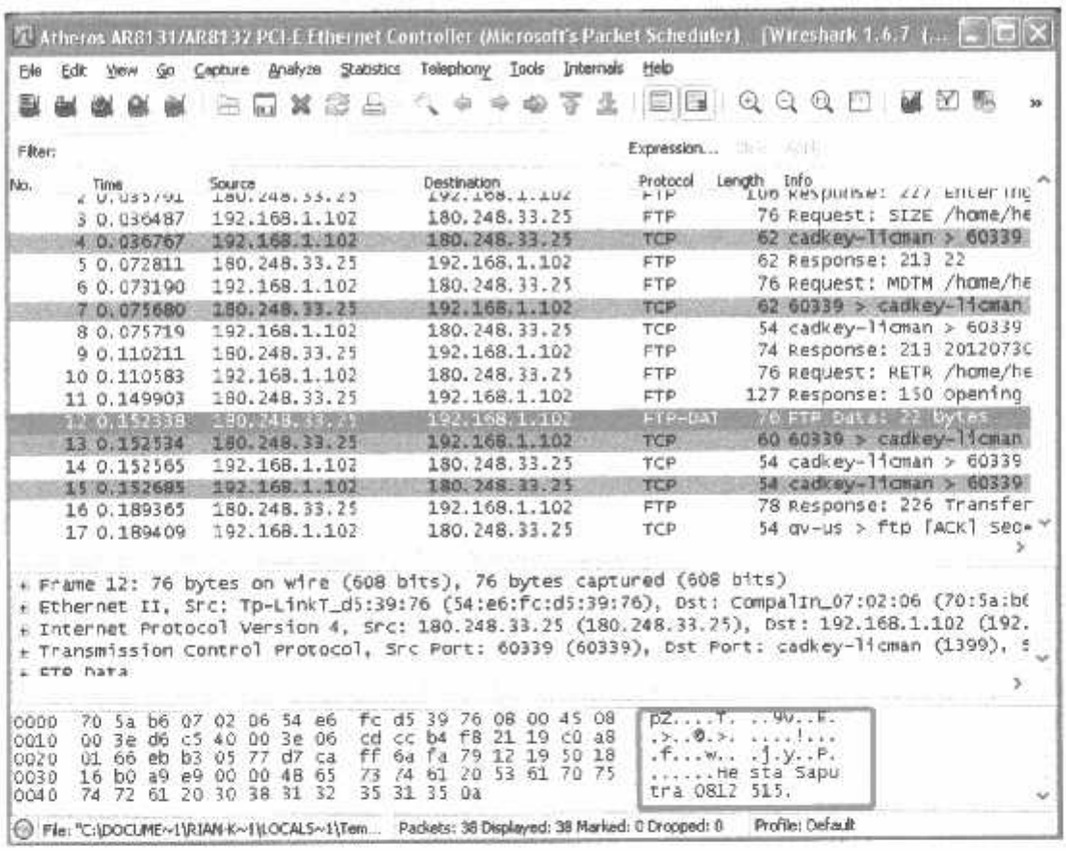
Dibawah ini merupakan gambar *berkas* yang akan digunakan sebagai pengujian enkripsi data.

Gambar 4.46.Berkas pengujian enkripsi data

Dari gambar 4.46.diketahui bahwa berkas memiliki nama *File tes*berisi data *Hesta Saputra 0812515*. Skenario pengujiannya adalah dengan melakukan *monitoring berkas* diatas menggunakan perangkat lunak *wireshark* selama proses pengunduhan dari *server FTP*, dari sana akan dilihat apakah isi dari *File Tes* terenkripsi atau tidak.

4.2.5.1 Monitoring Data Tanpa Menggunakan Layanan VPN

Berikut merupakan hasil *monitoring* data tanpa menggunakan layanan *VPN* yang nantinya akan dibandingkan dengan hasil *monitoring* data menggunakan layanan *VPN*.

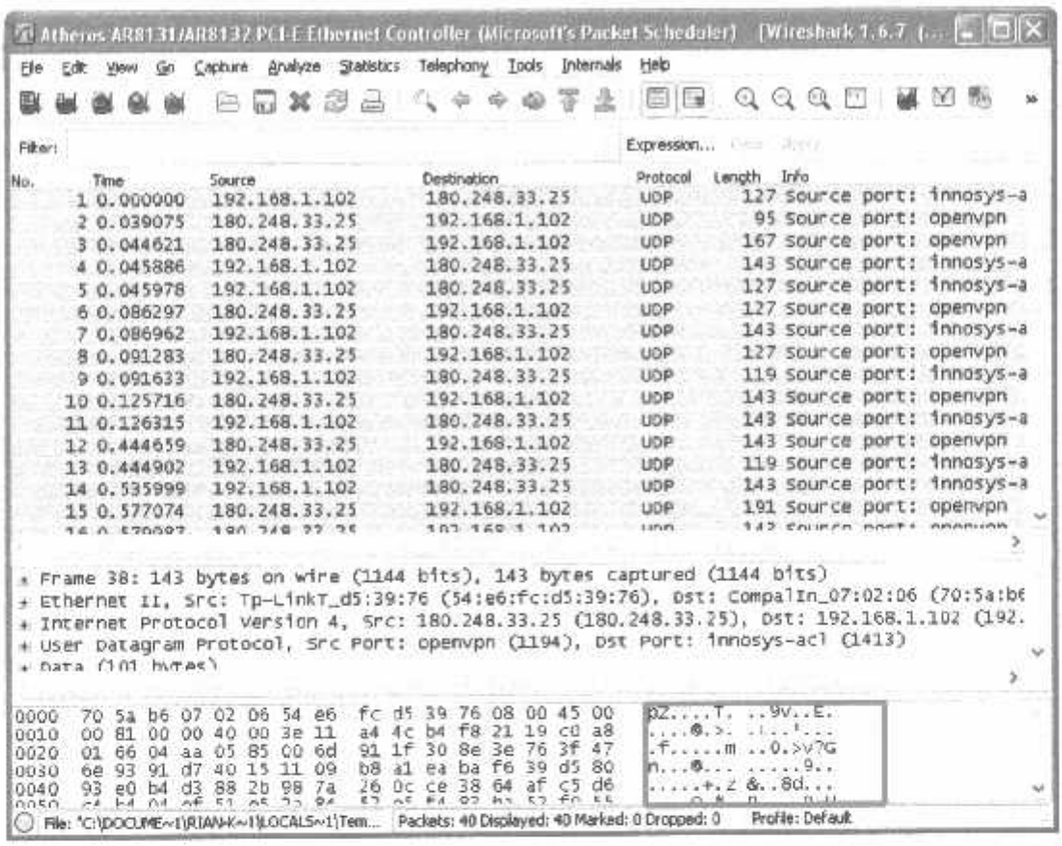


Gambar 4.47. Hasil *capturewireshark*

Dari hasil *capture* yang ditunjukkan gambar 4.47, pada bagian yang diberikan tanda merah merupakan data yang diunduh dari *server FTP*. Dapat disimpulkan bahwa transmisi data tanpa menggunakan layanan *VPN* adalah tidak aman karena dari hasil *monitoring*, data dapat dibaca dengan jelas.

4.2.4.2 Monitoring Data Menggunakan Layanan VPN

Berikut merupakan hasil *monitoring* data yang menggunakan layanan *VPN* yang akan dibandingkan dengan hasil *monitoring* tanpa menggunakan layanan *VPN*.



Gambar 4.48. Hasil *capturewireshark*

Dari hasil *capture* yang ditunjukkan pada gambar 4.48 dapat disimpulkan bahwa transmisi data melalui layanan VPN lebih aman karena data yang dikirimkan tidak dapat dibaca karena mengalami enkripsi.

BAB V

PENUTUP

5.1 Kesimpulan

Dari semua hasil pengujian yang telah dilakukan, maka dapat diambil kesimpulan bahwa :

1. Ketika proses autentikasi berhasil *client VPN* akan mendapatkan alamat *IP* dari *server VPN* yang akan digunakan untuk koneksi melalui *tunnel*.
2. Pada saat dilakukan pengujian dengan melakukan *tracert* atau *traceroute* koneksi yang terbentuk melalui *tunnel* antara *client* dan *server* adalah *point-to-point* karena hanya mengalami satu kali *hops*.
3. Ketika dilakukan pengujian privasi jaringan *VPN* diketahui bahwa *tunnel* tidak dapat diakses oleh selain *client VPN*.
4. Ketika dilakukan *monitoring* data melalui *VPN* diketahui bahwa data terenkripsi dan ini membuktikan bahwa menggunakan layanan *VPN* lebih aman.
5. *VPN* terbukti memberikan keamanan transmisi data dengan melakukan enkripsi.

5.2 Saran

1. Sebaiknya untuk alamat *IP* publik *server VPN* menggunakan *IP* statis. Karena jika menggunakan *IP* dinamis ketika *server restart* maka alamat *IP* akan berubah dan ini menyebabkan berkas konfigurasi pada sisi *client* tidak akan sesuai sehingga layanan *VPN* tidak dapat digunakan.

2. Diharapkan pada pengembangan selanjutnya dilakukan untuk mengamankan transmisi data yang bersifat *site-to-site*. Karena *OpenVPN* dapat digunakan oleh lebih dari satu *client*.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

DAFTAR PUSTAKA

http://id.wikipedia.org/wiki/CentOS. Diakses tanggal 04 April 2012.

http://id.wikipedia.org/wiki/VPN. Diakses tanggal 04 April 2012.

http://id.wikipedia.org/wiki/Linux. Diakses tanggal 19 Juni 2012

http://id.wikipedia.org/wiki/Jaringan_komputer. Diakses tanggal 19 Juni 2012.

http://id.wikipedia.org/wiki/Internet. Diakses tanggal 19 Juni 2012.

http://id.wikipedia.org/wiki/RSA. Diakses tanggal 19 Juni 2012.

http://blog.amarullz.com/mengenal-rsa.xm. Diakses tanggal 19 Juni 2012.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

LAMPIRAN

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

Nama	:	**Hesta Saputra**
Nim	:	**08.12.515**
Jurusan	:	**Teknik Elektro S-1**
Konsentrasi	:	**Teknik Komputer**
Masa Bimbingan	:	**Semester Genap 2011-2012**
Judul	:	**RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN**

Dipertahankan dihadapan Tim Penguji Skripsi Jenjang Program Strata Satu (S-1) pada :

Hari : Sabtu
Tanggal : 04 Agustus 2012
Dengan Nilai : 82 (A)

PANITIA UJIAN SKRIPSI

Ketua Majelis Penguji

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y.1018800189

Sekretaris Majelis Penguji

Dr. Eng. Aryuanto Soetedjo, ST.MT
NIP.P.1030800417

ANGGOTA PENGUJI

Penguji I

M.Ibrahim Ashari, ST.MT
NIP.P.1030100358

Penguji II

Irmalia Suryani Faradisa, ST.MT
NIP.P.1030000365

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

FORMULIR PERBAIKAN SKRIPSI

Dalam pelaksanaan Ujian Skripsi Jenjang Strata 1 Jurusan Teknik Elektro Konsentrasi Teknik Komputer, maka perlu adanya perbaikan skripsi untuk mahasiswa :

Nama	:	**Hesta Saputra**
Nim	:	**08.12.515**
Jurusan	:	**Teknik Elektro S-1**
Konsentrasi	:	**Teknik Komputer**
Masa Bimbingan	:	**Semester Genap 2011-2012**
Judul	:	**RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN**

No	Penguji	Tanggal	Uraian	Paraf
1.	Penguji II	04 Agustus 2012	• Metode enkripsi dicantumkan di bab III • Dasar teori enkripsi dicantumkan	

Disetujui :

Penguji I

M. Ibrahim Ashari, ST.MT
NIP.P.1030100358

Penguji II

Irmalia Suryani Faradisa, ST.MT
NIP.P.1030000365

Mengetahui :

Dosen Pembimbing I

Dr. Eng. Aryuanto Soetedjo, ST.MT
NIP.P.1030800417

Dosen Pembimbing II

Bima Aulia Firmandani, ST
1121

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

FORMULIR BIMBINGAN SKRIPSI

Nim : **Hesta Saputra**
Nama : **0812515**
Masa Bimbingan : **Semester Genap 2011 – 2012**
Judul : **RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN**

Tanggal	Uraian	Paraf Pembimbing
18 Juni 2012	Dasar teori VPN	
25 Juni 2012	Perangkat keras dan perangkat lunak sistem	
02 Juli 2012	Gambar Desain sistem	
09 Juli 2012	Keterangan atau penjelasan desain sistem	
14 Juli 2012	Pengujian privasi jaringan	
16 Juli 2012	Pembahasan proses pengujian server untuk VPN (public domain)	

Malang, 2/8/ 2012

Dosen Pembimbing

Dr. Eng. Aryuanto Soetedjo, ST.MT
NIP.P.1030800417

Form S-4b

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

FORMULIR BIMBINGAN SKRIPSI

Nim	:	**Hesta Saputra**
Nama	:	**0812515**
Masa Bimbingan	:	**Semester Genap 2011 – 2012**
Judul	:	**RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN**

Tanggal	Uraian	Paraf Pembimbing
09 Juli 2012	Dasar teori bab II	
12 juli 2012	Analisa dan perancangan sistem bab III	
12 Juli 2012	Proses enkripsi pada desain sistem bab III	
13 Juli 2012	Pengujian enkripsi data bab IV	

Malang, 2012

Dosen Pembimbing

Bima Aulia Firmandani, ST
1121

Form S-4b

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak/Ibu **Dr. Eng. Aryuanto Soetedjo, ST, MT**
Dosen Teknik Elektro S-1
ITN Malang

Yang bertanda tangan dibawah

Nama	: **HESTA SAPUTRA**
Nim	: **0812515**
Jurusan	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing untuk penyusunan Skripsi dengan judul :

"RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN "

Demikian permohonan kami buat dan atas kesediaan Bapak kami ucapkan terima kasih.

Mengetahui
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y.1018800189

Hormat Kami

HESTA SAPUTRA
NIM. 0812515

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai permohonan dari mahasiswa/i :

Nama	: **HESTA SAPUTRA**
Nim	: **0812515**
Semester	: **VIII (Delapan)**
Jurusan	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini menyatakan bersedia/~~tidak bersedia~~*) Membimbing skripsi dari mahasiswa tersebut, dengan judul :

" RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN "

Demikian surat pernyataan ini kami buat agar dapat dipergunakan seperlunya.

Hormat Kami

Dr. Eng. Aryuanto Soetedjo, ST, MT
NIP.P. 1030800417

*) Coret yang tidak perlu

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK

PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG

Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Nomor Surat : ITN-204/EL-FTI/2012
Lampiran : -
Perihal : BIMBINGAN SKRIPSI

Kepada : Yth. Bapak/Ibu **Dr. Eng. Aryuanto Soetedjo, ST, MT**
Dosen Teknik Elektro S-1
ITN MALANG

Dengan Hormat

Sesuai dengan permohonan dan persetujuan dalam Proposal Skripsi untuk mahasiswa :

Nama	: **HESTA SAPUTRA**
Nim	: **0812515**
Fakultas	: **Teknologi Industri**
Program Studi	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Maka dengan ini pembimbingan tersebut kami serahkan sepenuhnya kepada Saudara/i selama masa waktu :

" Semester Genap Tahun Akademik 2011 - 2012 "

Demikian agar maklum dan atas perhatian serta bantuannya kami sampaikan terima kasih.

Mengetahui
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y. 1018800189

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak/Ibu **Bima Aulia Firmandani, ST**
Dosen Teknik Elektro S-1
ITN Malang

Yang bertanda tangan dibawah

Nama	: **HESTA SAPUTRA**
Nim	: **0812515**
Jurusan	**Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing untuk penyusunan Skripsi dengan judul :

"RANCANG BANGUN SERVER VPN (VIRTUAL PRIVATE NETWORK) BERBASIS CentOS DAN OpenVPN "

Demikian permohonan kami buat dan atas kesediaan Bapak kami ucapkan terima kasih.

Mengetahui
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y. 1018800189

Hormat Kami

HESTA SAPUTRA
NIM. 0812515

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Nomor Surat : ITN-204/EL-FTI/2012
Lampiran : -
Perihal : BIMBINGAN SKRIPSI

Kepada : Yth. Bapak/Ibu **Bima Aulia Firmandani, ST**
Dosen Teknik Elektro S-1
ITN MALANG

Dengan Hormat

Sesuai dengan permohonan dan persetujuan dalam Proposal Skripsi untuk mahasiswa :

Nama	: **HESTA SAPUTRA**
Nim	: **0812515**
Fakultas	: **Teknologi Industri**
Program Studi	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Maka dengan ini pembimbingan tersebut kami serahkan sepenuhnya kepada Saudara/i selama masa waktu :

" Semester Genap Tahun Akademik 2011 - 2012 "

Demikian agar maklum dan atas perhatian serta bantuannya kami sampaikan terima kasih.

Mengetahui
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y. 1018800189

YUDISIUM PROGRAM STUDI TEKNIK ELEKTRO S-1
KONSENTRASI TEKNIK KOMPUTER
INSTITUT TEKNOLOGI NASIONAL MALANG
PERIODE II TAHUN 2012

YUDISIUM PROGRAM STUDI TEKNIK ELEKTRO S-1
ANGKATAN 2008
INSTITUT TEKNOLOGI NASIONAL MALANG
PERIODE II TAHUN 2012