MENGADMINISTRASI SERVER DALAM JARINGAN

A. PENDAHULUAN

Aplikasi Server adalah aplikasi komputer yang berfungsi melayani permintaan akses dari komputer klien. Berikut ini beberapa contoh aplikasi server:

1. **Web Server**

   Web server merupakan software yang memberikan layanan data yang berfungsi menerima permintaan HTTP atau HTTPS dari klien yang dikenal dengan browser web dan mengirimkan kembali hasilnya dalam bentuk halaman - halaman web yang umumnya berbentuk dokumen HTML. Hubungan antara Web Server dan Browser Internet merupakan gabungan atau jaringan Komputer yang ada di seluruh dunia. Setelah terhubung secara fisik, Protocol TCP/IP yg memungkinkan semua komputer dapat berkomunikasi satu dengan yg lainnya. Pada saat browser meminta data halaman web ke server, maka instruksi permintaan data tersebut di kemas dalam TCP yang merupakan protocol transport dan dikirim ke alamat protocol berikutnya yaitu Hyper Text Transfer Protocol (HTTP). HTTP merupakan protocol yg digunakan dalam World Wide Web (WWW) antar komputer yang terhubung dalam jaringan. Data yg di*passing* dari web browser ke web server disebut sebagai *HTTP request* yang meminta halaman web, kemudian web server akan mencari data HTML yang ada dan dikemas dalam protokol TCP dan dikirim kembali ke browser. Data yang dikirim dari server ke browser disebut sebagai *HTTP response*. Jika data yang diminta tidak ditemukan oleh web server maka akan menimbulkan error yang sering anda lihat di web page yaitu Error : 404 Page Not Found.

   Hal ini memberikan cita rasa dari suatu proses yang tridimensional, artinya pengguna internet dapat membaca dari satu dokumen ke dokumen yang lain hanya dengan mengklik beberapa bagian dari halaman web. Proses yang dimulai dari permintaan web browser, diterima web server, diproses, dan dikembalikan hasil prosesnya oleh web server ke web browser kembali dilakukan secara transparan. Setiap orang dapat dengan mudah mengetahui apa yang terjadi pada tiap-tiap proses. Secara garis besarnya web server hanya memproses semua masukan yang diperolehnya dari web browser.

   Web Server Apache

   Apache merupakan web server yang paling banyak digunakan di Internet. Program ini awalnya didesain untuk sistem operasi UNIX. Namun demikian, pada versi berikutnya Apache mengeluarkan program yang dapat dijalankan di Windows NT. Apache mempunyai program pendukung yang cukup banyak. Hal ini memberikan layanan yang cukup lengkap bagi penggunanya. Beberapa dukungan Apache :

   a) Kontrol Akses, kontrol ini dapat dijalankan berdasarkan nama host atau nomor IP.
   b) CGI (Common Gateway Interface), yang paling terkenal digunakan adalah PERL (Practical Extraction and Report Language), didukung oleh Apache dengan menempatkannya sebagai modul (mod_perl).
   c) PHP (Personal Home Page/PHP Hypertext Processor), merupakan program dengan metode semacam CGI, yang memproses teks dan bekerja di server. Apache mendukung PHP dengan menempatkannya dalam modul (mod_php).
   d) SSI (Server Side Includes).

   Kelebihan dari web server apache :

a. Apache termasuk dalam kategori freeware.
b. Proses instalasi lebih mudah jika dibanding web server lainnya seperti NCSA, IIS, dan lain-lain.
c. Mampu beroperasi pada berbagai platform sistem operasi.
d. Mudah mengatur konfigurasinya. Apache mempunyai hanya empat file konfigurasi.
e. Mudah dalam menambahkan peripheral lainnya ke dalam platform web servernya.

Fasilitas atau ciri khas dari web server Apache adalah :

- *Dapat dijadikan pengganti bagi NCSA web server.*
- *Perbaikan terhadap kerusakan dan error pada NCSA 1.3 dan 1.4.*
- *Apache merespon web client sangat cepat jauh melebihi NCSA.*
- *Mampu di kompilasi sesuai dengan spesifikasi HTTP yang sekarang.*
- *Apache menyediakan feature untuk multihomed dan virtual server.*
- *Kita dapat menetapkan respon error yang akan dikirim web server dengan menggunakan file atau skrip.*
- *Server apache dapat otomatis berkomunikasi dengan client browsernya untuk menampilkan tampilan terbaik pada client browsernya. Web server Apache secara otomatis menjalankan file index.html, halaman utamanya, untuk ditampilkan secara otomatis pada clientnya.*
- *Web server Apache mempunyai level-level pengamanan.*
- *Apache mempunyai komponen dasar terbanyak di antara web server lain.*
- *Ditinjau dari segi sejarah perkembangan dan prospeknya, Apache web server mempunyai prospek yang cerah. Apache berasal dari web server NCSA yang kemudian dikembangkan karena NCSA masih mempunyai kekurangan di bidang kompatibilitasnya dengan sistim operasi lain. Sampai saat ini, web server Apache terus dikembangkan oleh tim dari apache.org.*
- *Performasi dan konsumsi sumber daya dari web server Apache tidak terlalu banyak, hanya sekitar 20 MB untuk file-file dasarnya dan setiap daemonnya hanya memerlukan sekitar 950 KB memory per child.*
- *Mendukung transaksi yang aman (secure transaction) menggunakan SSL (secure socket layer).*
- *Mempunyai dukungan teknis melalui web.*
- *Mempunyai kompatibilitas platform yang tinggi.*
- *Mendukung third party berupa modul-modul tambahan.*

2. File Transfer Protocol (FTP) Server

FTP adalah sebuah protokol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas atau file komputer antar mesin-mesin dalam sebuah internetwork. FTP bersama dengan Transmission Control Protocol (TCP) digunakan untuk komunikasi data antara klien dan server, sehingga di antara kedua komponen tersebut akan dibuatlah sebuah sesi komunikasi sebelum transfer data dimulai. FTP hanya menggunakan metode autentikasi standar, yakni menggunakan username dan paswordnya yang dikirim dalam bentuk tidak terenkripsi. Pengguna terdaftar dapat menggunakan username dan password-nya untuk mengakses, men-download, dan meng-upload berkas-berkas yang dikehendaki.

Dua hal penting yang ada dalam FTP adalah :

a. FTP server yaitu software yang digunakan untuk tukar menukar file, yang selalu siap memberikan layanan FTP apabila mendapat request dari FTP client.
b. FTP client adalah komputer yang merequest koneksi ke FTP server untuk tujuan tukar menukar file.

Tujuan dari FTP server adalah sebagai berikut :
a) Untuk tujuan sharing data
b) Untuk menyediakan indirect atau implicit remote komputer
c) Untuk menyediakan media penyimpanan bagi para user
d) Untuk menyediakan transfer data yang reliable dan efisien

FTP sebenarnya cara yang tidak aman dalam mentransfer suatu file karena file dikirimkan tanpa di-enkripsi terlebih dahulu tetapi melalui clear text. Mode text yang dipakai untuk transfer data adalah format ASCII atau format binary. Secara default, FTP menggunakan mode ASCII dalam transfer data. Karena pengirimannya tanpa enkripsi, username, password, data yang di transfer, maupun perintah yang dikirim dapat di-sniffing oleh orang dengan menggunakan protocol analyzer (sniffer). Solusi yang digunakan adalah dengan menggunakan SFTP (SSH FTP) yaitu FTP yang berbasis pada SSH atau menggunakan FTPS (FTP over SSL) sehingga data yang dikirim terlebih dahulu di enkripsi.

3. Simple Mail Transfer Protocol (SMTP) Server

SMTP (Simple Mail Transfer Protocol) merupakan salah satu protokol yang umum digunakan untuk pengiriman surat elektronik di internet. Protokol ini dipergunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima. Protokol ini bekerja pada port 25. Dimana pada port ini digunakan aplikasi yang dinamakan MTA (Mail Transfer Agent). MTA ini berupa program email misalnya: sendmail, qmail atau postfix. ---→ TKJ 2

Protokol SMTP ini timbul karena desain sistem surat elektronik yang mengharuskan adanya server surat elektronik yang menampung sementara sampai surat elektronik diambil oleh penerima yang berhak. SMTP bisa dianalogikan sebagai kantor pos. Ketika kita mengirim sebuah e-mail, komputer kita akan mengarahkan e-mail tersebut ke sebuah SMTP server, untuk diteruskan ke mail-server tujuan. Mail-server tujuan ini bisa dianalogikan sebagai kotak pos di pagar depan rumah, atau kotak PO.BOX di kantor pos. Email-email yang terkirim akan tersimpan di tempat tersebut hingga si pemilik mengambilnya. Urusan pengambilan e-mail tersebut tergantung kapan si penerima memeriksa akun e-mailnya.

SMTP adalah protokol yang cukup sederhana, berbasis teks dimana protokol ini menyebutkan satu atau lebih penerima email untuk kemudian diverifikasi. Jika penerima email valid, maka email akan segera dikirim. SMTP menggunakan port 25 dan dapat dihubungi melalui program telnet. Agar dapat menggunakan SMTP server lewat nama domain, maka record DNS (Domain Name Server) pada bagian MX (Mail Exchange) digunakan.

4. Proxy Server

Proxy server adalah sebuah komputer server atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan request terhadap content dari Internet atau intranet. Proxy Server bertindak sebagai gateway terhadap dunia Internet

untuk setiap komputer klien. Proxy server tidak terlihat oleh komputer klien. Seorang pengguna yang berinteraksi dengan Internet melalui sebuah proxy server tidak akan mengetahui bahwa sebuah proxy server sedang menangani request yang dilakukannya. Web server yang menerima request dari proxy server akan menginterpretasikan request-request tersebut seolah-olah request itu datang secara langsung dari komputer klien, bukan dari proxy server.

Proxy server juga dapat digunakan untuk mengamankan jaringan pribadi yang dihubungkan ke sebuah jaringan publik (seperti halnya internet). Proxy server memiliki lebih banyak fungsi daripada router yang memiliki fitur packet filtering karena memang proxy server beroperasi pada level yang lebih tinggi dan memiliki kontrol yang lebih menyeluruh terhadap akses jaringan. Proxy server yang berfungsi sebagai sebuah "agen keamanan" untuk sebuah jaringan pribadi, umumnya dikenal sebagai firewall.

Keuntungan jaringan proxy server jika dibandingkan dengan hanya menggunakan sebuah proxy server adalah:

- Permintaan dari pengguna akan dapat dilayani dengan lebih cepat
- Kehandalan proxy server lebih terjamin, jika salah satu proxy server tidak berfungsi, maka proxy server lainnya akan menggantikan fungsinya.
- Lebih efisien dan menghemat bandwidth.

5. Simple Network Management Protocol (SNMP) Server

SNMP singkatan dari Simple Network Management Protocol. Protokol ini digunakan untuk memonitor device-device yang terhubung ke jaringan akan kondisi-kondisi systemnya yang penting. Sebagai contoh penggunaan CPU, penggunaan harddisk, penggunaan memory, traffic jaringan dan lain-lain. Untuk device-device yang dapat dipantau adalah device-device seperti PC, Server, atau router. Sedangkan Operating System bisa Linux, *Nix, Windows, atau yang lain.

Dengan Adanya SNMP tidak perlu memeriksa-memeriksa satu-satu server, tetapi anda cukup mengakses satu komputer untuk melihat kondisi seluruh server dan router. Hal ini disebabkan server dan router akan bertindak sebagai SNMP-server yang tugasnya yang menyediakan requset SNMP dari komputer lain. Satu PC akan bertindak sebagai **SNMP Agent** yaitu komputer yang mengumpulkan informasi-informasi dari SNMP-servers.

Selain digunakan untuk memonitoring sebetulnya SNMP dapat digunakan untuk melakukan perubahan dan memberikan konfigurasi baru ke server. Tetapi pengubahan konfigurasi system di server hanya dilakukan apabila ada perubahan infrastruktur di jaringan. Nilai-nilai variabel yang diakses menggunakan SNMP diatur dalam bentuk hirarki. Tipe hirarki dan metadata (seperti tipe dan deskripsi variabel) diatur oleh Management Information Bases (MIBs).

6. Internet Relay Chat Daemon (IRCD) Server

IRCd (Internet Relay Chat Development) adalah sebuah software yang dikembangkan untuk keperluan komunikasi antar komputer yang terhubung ke Internet. Salah satu software ircd yang cukup terkenal adalah "hybrid". Hybrid dikenalkan pertama kali oleh EFNET (Eris Free Network), adalah salah satu dari Network yang tertua di dunia.

Layanan IRC, atau biasa disebut sebagai "chat" saja adalah sebuah bentuk komunikasi di intenet yang menggunakan sarana baris-baris tulisan yang diketikkan melalui keyboard. Dalam sebuah sesi chat, komnunikasi terjalin melalui saling bertukar pesan-pesan singkat. kegiatan ini disebut chatting dan pelakunya disebut sebagai chatter. Para chatter dapat saling berkomunikasi secara berkelompok dalam suatu chat room dengan membicarakan topik tertentu atau berpindah ke modus private untuk mengobrol berdua saja dengan chatter lain. Kegiatan chatting membutuhkan software yang disebut IRC Client, diantaranya yang paling populer adalah software mIRC.

7. Post Office Protocol (POP) Server

POP adalah protokol untuk menerima email, sedang untuk mengirim email kita membutuhkan server SMTP (Simple Mail Transfer Protocol). Ada dua jenis mode pada POP3 yaitu mode offline dan mode inline. Pada mode offline, POP3 mengambil dan kemudian menghapus mail yang tersimpan dari server. POP3 bekerja dengan baik pada mode ini, karena terutama memang didisain untuk berlaku sebagai sebuah sistem mail yang memiliki sifat “store-and-forward”. Server, pada mode offline, berlaku seperti sebuah tempat penampungan yang menyimpan mail sampai user memintanya.

Pada mode inline, POP3 akan mengambil mail dari server tanpa menghapus mail yang sudah diambil tersebut. Mode ini lebih disukai oleh user yang sering berpindah tempat (nomadic user) karena memungkinkan mereka untuk melihat mail yang sama dari tempat atau komputer yang berbeda. Akan tetapi untuk nomadic user yang selalu bekerja dan bepergian dengan selalu membawa notebook, dan tetap menginginkan agar mail miliknya yang ada di server tidak dihapus, tentu saja menginginkan agar setiap kali mengambil mail tidak semua mail yang akan terambil, tapi hanya mail yang belum pernah dia lihat saja yang akan diambil. Keinginan user seperti ini dapat dipenuhi dengan menggunakan informasi pada client yang memungkinkan untuk memberi tanda mail yang sudah pernah dilihat.

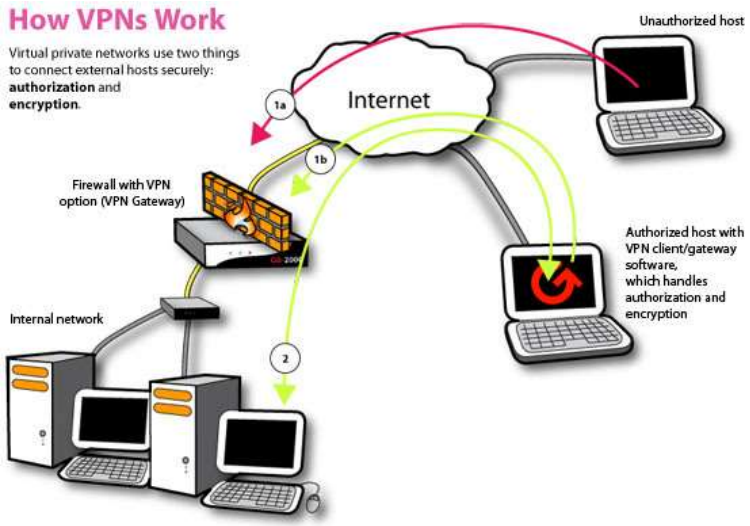
Dengan demikian untuk seseorang yang sering bekerja dengan email akan lebih baik jika menggunakan POP email daripada web email. Karena ada beberapa keuntungan menurut saya antara lain :

- Hemat waktu. Ketika menggunakan web email kita akan melakukan langkah – lahkah berikut ini. Menjalankan browser–> membuka halaman web email (misalnya di http://id.yahoo.com/ mail) –>memasukkan username & passwords –> memilih email yang ada di inbox –>membaca email. Sedangkan di POP yang dilakukan hanya menjalankan email client dan menunggu email selesai di download–>membaca email.
- Pengarsipan lebih mudah. Ketika kita ingin membuka email yang lama dengan web email kita perlu melakukan langkah yang sama dengan langkah diatas. Belum lagi kalau email yang sudah sangat lama di halaman inbox berikutnya kita perlu menunggu loading halaman web. Sedang dengan POP kita tinggal menjalankan email client dan tanpa harus terkoneksi ke internet karena email sudah di simpan di komputer kita.”

8. Virtual Private Network (VPN) Server

VPN adalah singkatan dari *virtual private network*, yaitu sebuah cara aman untuk mengakses local area network yang berada pada jangkauan, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara

pribadi, dengan enkripsi Perlu penerapan teknologi tertentu agar walaupun menggunakan medium 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 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 keamanan data.

Konsep kerja VPN

Pada dasarnya VPN Membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC. Jika digambarkan kira-kira seperti ini :

Internet <—> VPN Server <—-> VPN Client <—-> Client

Bila digunakan untuk menghubungkan 2 komputer secara private dengan jaringan internet maka seperti ini :

Komputer A <—> VPN Clinet <—> Internet <—> VPN Server <—> VPN Client <—> Komputer B

Jadi semua koneksi diatur oleh VPN Server sehingga dibutuhkan kemampuan VPN Server yang memadai agar koneksinya bisa lancar. Keamanan Dengan konsep demikian maka jaringan VPN ini menawarkan keamanan dan untraceable, tidak dapat terdeteksi sehingga IP kita tidak diketahui karena yang digunakan adalah IP Public milik VPN server. Dengan ada enkripsi dan dekripsi maka data yang lewat jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh server VPN dan Client yang terhubung. Enkripsi dan dekripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga keamananya terjamin. Untuk menjebol

data si pembajak data harus melalukan proses dekripsi tentunya untuk mencari rumus yang tepat dibutuhkan waktu yang sangat lama sehingga biasa menggunakan super computing untuk menjebol dan tentunya tidak semua orang memiliki PC dengan kemampuan super ini dan prosesnya rumit dan memakan waktu lama.

Kelebihan VPN

Ada beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN untuk implementasi WAN. *Pertama,* jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP terdekat di daerahnya. Sedangkan penggunaan leased line sebagai WAN akan membutuhkan waktu yang lama untuk membangun jalur koneksi khusus dari kantor cabang yang baru dengan perusahaan induknya. Dengan demikian penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.

Kedua, penggunaaan VPN dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN. VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (leased line) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya. VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan kabel dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.

Media internet telah tersebar ke seluruh dunia, karena internet digunakan sebagai media komunikasi publik yang bersifat terbuka. Artinya setiap paket informasi yang dikirimkan melalui internet, dapat diakses dan diawasi bahkan dimanipulasi, oleh setiap orang yang terhubung ke internet pada setiap saat. Setiap orang berhak menggunakan internet dengan syarat dia memiliki akses ke internet. Untuk memperoleh akses ke internet, orang tersebut dapat dengan mudah pergi ke warnet (warung internet) yang sudah banyak tersebar di Indonesia. Oleh karena itu untuk memperoleh komunikasi yang aman, perlu protokol tambahan yang khusus dirancang untuk mengamankan data yang dikirim melalui internet, sehingga data tersebut hanya dapat diakses oleh pihak tertentu saja.

Penggunaan VPN juga dapat mengurangi biaya telepon untuk akses jarak jauh, karena hanya dibutuhkan biaya telepon untuk panggilan ke titik akses yang ada di ISP terdekat. Pada beberapa kasus hal ini membutuhkan biaya telepon SLJJ (sambungan langsung jarak jauh), namun sebagian besar kasus cukup dengan biaya telepon lokal. Berbeda dengan penggunaan leased line, semakin jauh jarak antar terminal, akan semakin mahal biaya telepon yang digunakan.

Biaya operasional perusahaan juga akan berkurang bila menggunakan VPN. Hal ini disebabkan karena pelayanan akses dial-up dilakukan oleh ISP, bukan oleh perusahaan yang bersangkutan. Secara teori biaya operasional ISP yang dibebankan kepada perusahaan bisa jauh lebih kecil daripada biaya operasional akses dial-up tersebut ditanggung perusahaan itu sendiri karena biaya operasional ISP itu ditanggung bersama-sama oleh ribuan pelanggan ISP tersebut.

Ketiga, penggunaan VPN akan meningkatkan skalabilitas. Perusahaan yang tumbuh pesat akan membutuhkan kantor cabang baru di beberapa tempat yang terhubung dengan jaringan lokal kantor pusat. Bila menggunakan leased line, penambahan satu kantor cabang membutuhkan satu jalur untuk membangun WAN. Penambahan satu kantor cabang baru lagi (dua kantor cabang) akan membutuhkan dua tambahan jalur, masing-masing ke kantor pusat dan ke kantor cabang terdahulu. Jika mereka memiliki kantor cabang yang ke-3, dibutuhkan enam jalur untuk menghubungkan semua kantor. Jika ada empat kantor cabang, maka dibutuhkan 10 jalur.

Berbeda dengan penggunaan leased line, penambahan satu kantor cabang hanya membutuhkan satu jalur, yaitu jalur yang menhubungkan kantor cabang yang baru dengan ISP terdekat. Selanjutnya jalur dari ISP akan terhubung ke internet yang merupakan jaringan global. Dengan demikian penggunaan VPN untuk implementasi WAN akan menyederhanakan topologi jaringannya.

Keempat, VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang mobile dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan. Hal ini tidak dapat dilakukan jika menggunakan leased line yang hanya dapat diakses pada terminal tertentu saja.

Kelima, investasi pada VPN akan memberikan peluang kembalinya investasi tersebut (ROI = return on investment) yang lebih cepat daripada investasi pada leased line. Berdasarkan artikel "Delivering Profitable Virtual Private LAN Services – Business Case White Paper" bulan November 2003, telah dilakukan studi kasus pada kota berukuran medium di Amerika Utara. Artikel tersebut menunjukkan bahwa dengan beberapa asumsi parameter yang disimpulkan pada tabel 1, VPN dapat mengembalikan nilai investasi dalam 2.1 tahun. Bahkan dengan peningkatan penetrasi pasar dan perubahan kecenderungan pelanggan untuk menyewa bandwidth yang besar akan mempercepat jangka waktu ROI, yaitu dalam 1 tahun.

Kekurangan VPN

Salah satu kekurangan dari VPN adalah fakta bahwa penggunaan atau pengaplikasiannya membutuhkan pengetahuan jaringan tingkat tinggi, dan juga harus dapat memahami berbagai macam aspek pada jaringan seperti keamanan jaringan (network security). Keamanan VPN membutuhkan password dan enkripsi data. Network address mungkin juga dapat dienkripsi untuk keamanan tambahan. Untuk menghindari masalah keamanan dan pengembangan, perencanaan (planning) yang matang dan juga tindakan pencegahan yang tepat perlu dilakukan. Salah satu kekurangan signifikan dari VPN lainnya adalah ketersediaan (availability) dan performanya sulit untuk dikontrol. Biasanya, kecepatan VPN jauh lebih lambat dibandingkan dengan koneksi tradisional. Seringkali, beberapa VPN bahkan tidak dapat menyediakan koneksi karena alasan tertentu. Karena beberapa alasan tertentu juga, pengguna dapat kesulitan tetap berada pada VPN dari waktu ke waktu.

Fungsi VPN

Teknologi VPN memiliki tiga fungsi utama, di antaranya adalah :

- Confidentially (Kerahasiaan)

Teknologi VPN merupakan teknologi yang memanfaatkan jaringan publik yang tentunya sangat rawan terhadap pencurian data. Untuk itu, VPN menggunakan metode enkripsi untuk mengacak data yang lewat. Dengan adanya teknologi enkripsi itu, keamanan data menjadi lebih terjamin. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Jadi, confidentially ini dimaksudkan agar informasi yang ditransmisikan hanya boleh diakses oleh sekelompok pengguna yang berhak.

- Data Integrity (Keutuhan Data)
  Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.
- Origin Authentication (Autentikasi Sumber)
  Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

B. MENGINSTALASI SISTEM OPERASI SERVER

Sistem operasi adalah aplikasi yang berfungsi menghidupkan semua perangkat keras komputer dan sebagai penerjemah perintah pengguna ke bahasa mesin. Sehingga komputer dapat memproses permintaan pengguna dan menampilkan dalam bahasa yang dimengerti oleh pengguna pada layar monitor komputer. Berikut ini contoh sistem operasi yang dikenal oleh masyarakat luas.

1. Sistem Operasi Debian Server

Debian pertama kali diperkenalkan oleh Ian Murdock, seorang mahasiswa dari Universitas Purdue, Amerika Serikat, pada tanggal 16 Agustus 1993. Nama Debian berasal dari kombinasi nama Ian dengan mantan-kekasihnya Debra Lynn: Deb dan Ian. Pada awalnya, Ian memulainya dengan memodifikasi distribusi SLS (Softlanding Linux System). Namun, ia tidak puas dengan SLS yang telah dimodifikasi olehnya sehingga ia berpendapat bahwa lebih baik membangun sistem (distribusi Linux) dari nol (Dalam hal ini, Patrick Volkerding juga berusaha memodifikasi SLS. Ia berhasil dan distribusinya dikenal sebagai "Slackware").

Proyek Debian tumbuh lambat pada awalnya dan merilis versi 0.9x di tahun 1994 dan 1995. Pengalihan arsitektur ke selain i386 dimulai ditahun 1995. Versi 1.x dimulai tahun 1996. Ditahun 1996, Bruce Perens menggantikan Ian Murdoch sebagai Pemimpin Proyek. Dalam tahun yang sama pengembang debian Ean Schuessler, berinisiatif untuk membentuk Debian Social Contract dan Debian Free Software Guidelines, memberikan standar dasar komitmen untuk pengembangan distribusi debian. Dia juga membentuk organisasi "Software in Public Interest" untuk menaungi debian secara legal dan hukum.

Di akhir tahun 2000, proyek debian melakukan perubahan dalam archive dan managemen rilis. Serta di tahun yang sama para pengembang memulai konferensi dan workshop tahunan "debconf".

Di April 8, 2007, Debian GNU/Linux 4.0 dirilis dengan nama kode "Etch". Rilis versi terbaru Debian, 2009, diberi nama kode "Lenny". **deb** adalah perpanjangan dari paket perangkat lunak Debian format dan nama yang paling sering digunakan untuk paket-paket binari seperti itu. Paket debian adalah standar Unix pada arsip yang mencakup dua gzip, tar bzipped atau lzmaed arsip: salah satu yang memegang kendali informasi dan lain yang berisi data. Program kanonik untuk menangani paket-paket tersebut adalah dpkg, paling sering melalui apt/aptitude.

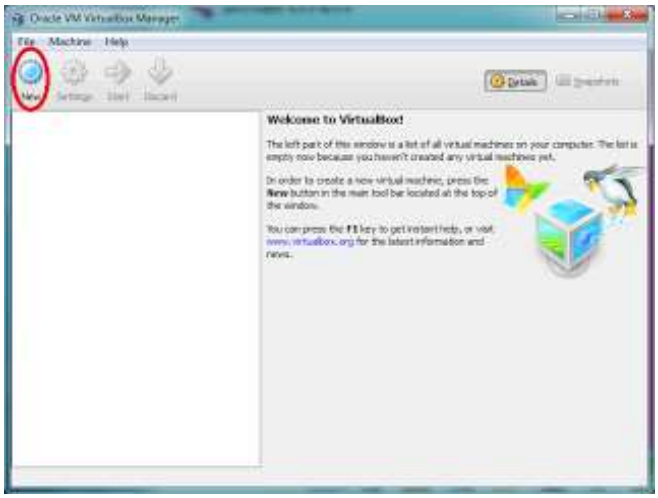
Beberapa paket Debian inti tersedia sebagai udebs ("mikro deb"), dan biasanya hanya digunakan untuk *bootstrap* instalasi Linux Debian. Meskipun file tersebut menggunakan ekstensi nama file udeb, mereka mematuhi spesifikasi struktur yang sama seperti biasa deb. Namun, tidak seperti rekan-rekan mereka deb, hanya berisi paket-paket udeb fungsional penting file. Secara khusus, file dokumentasi biasanyadihilangkan. udeb paket tidak dapat diinstal pada sistem Debian standar.Paket debian juga digunakan dalam distribusi berbasis pada Debian, seperti Ubuntu dan lain-lain. Saat initelah terdapat puluhan distribusi Linux yang berbasis kepada debian, salah satu yang paling menonjol danmenjadi fenomena adalah Ubuntu.

2. Instalasi Sistem Operasi Debian Server

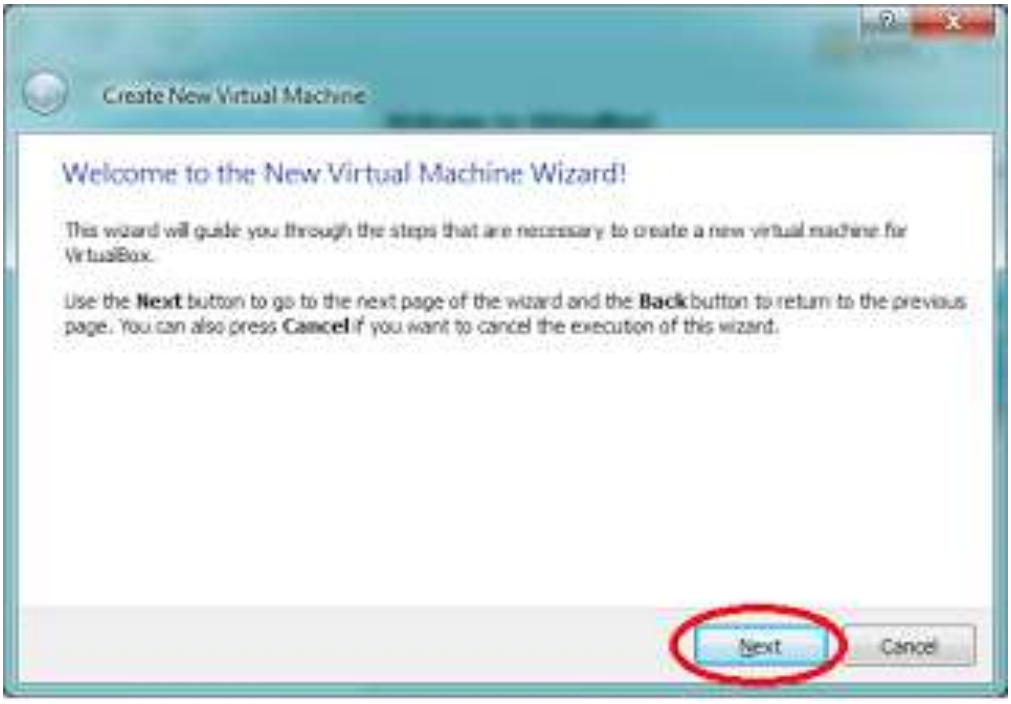
INSTALASI LINUX DEBIAN DI VIRTUALBOX

Langkah – langkah menginstal linux debian dari tahap awal :

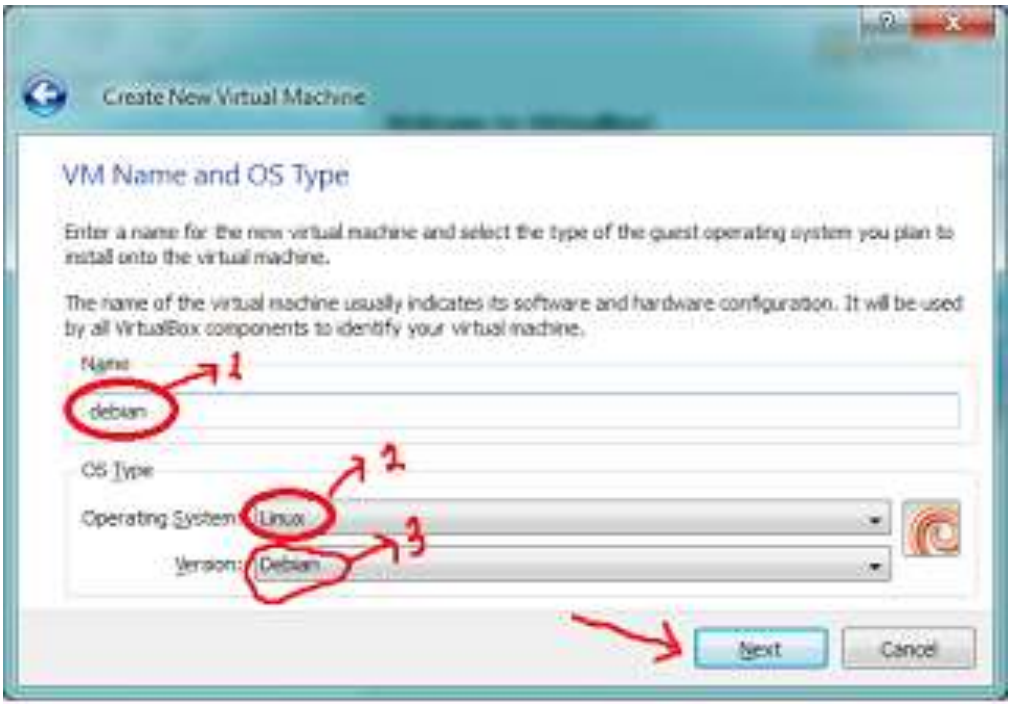
1) Langkah pertama klik new pada pojok kiri atas di virtualbox sepertia gambar di bawah.



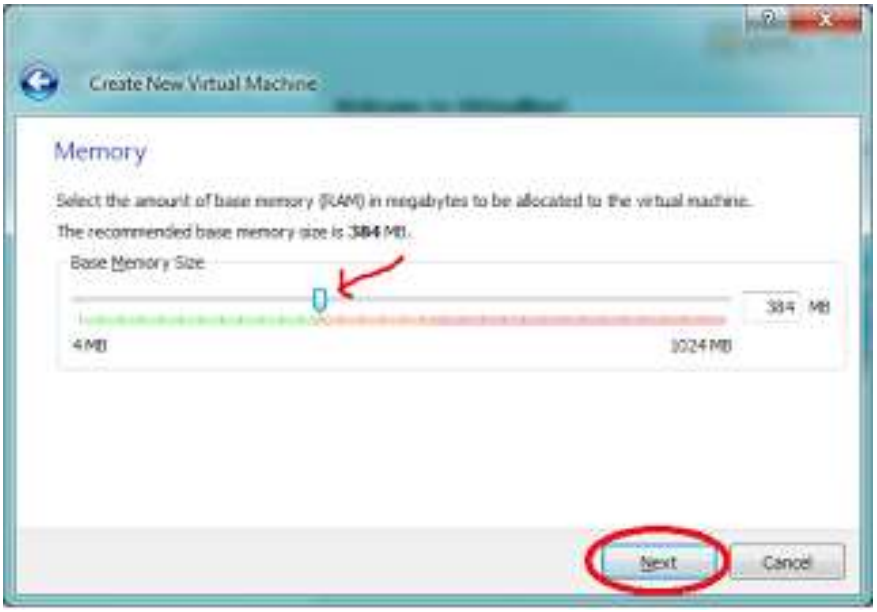
2) Kemudian Setelah muncul seperti gambar diatas, klik next untuk melanjutkan ke tahap selanjutnya



3) Selanjutnya isi nama seperti gambar di atas bagian No 1 sesuai nama yang diinginkan, pada bagian no 2 pilih Linux dan bagian 3 pilih debian dan klik next

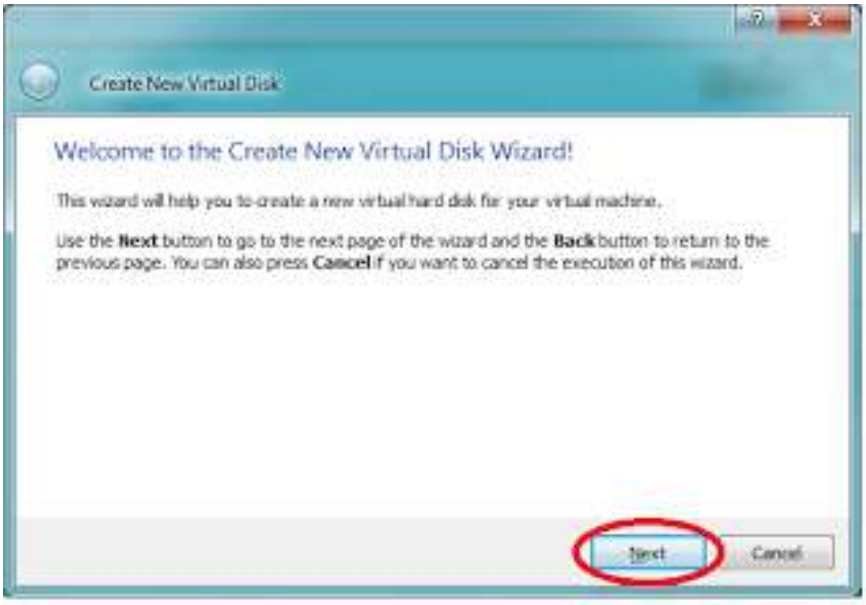


4) Gambar di bawah merupakan jendela memori, Berikan memori min 384 MB



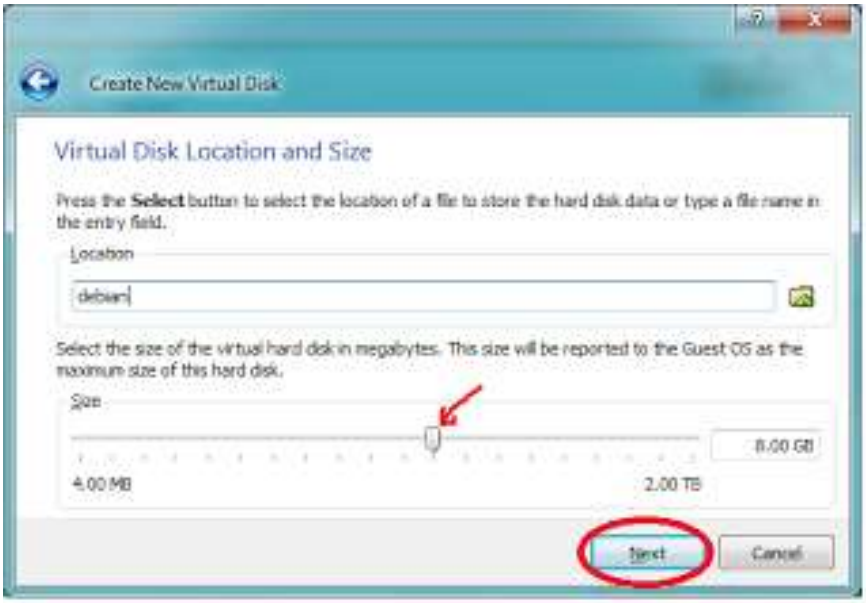
5) Selanjutnya akan muncul jendela hard disk virtual dan pilih create new hard disk lalau klik next, lihat gambar di bawah.

6) Kemudian akan muncul jendela welcome to the create Virtual Disk Wizard dan klik next seperti gambar di bawah.

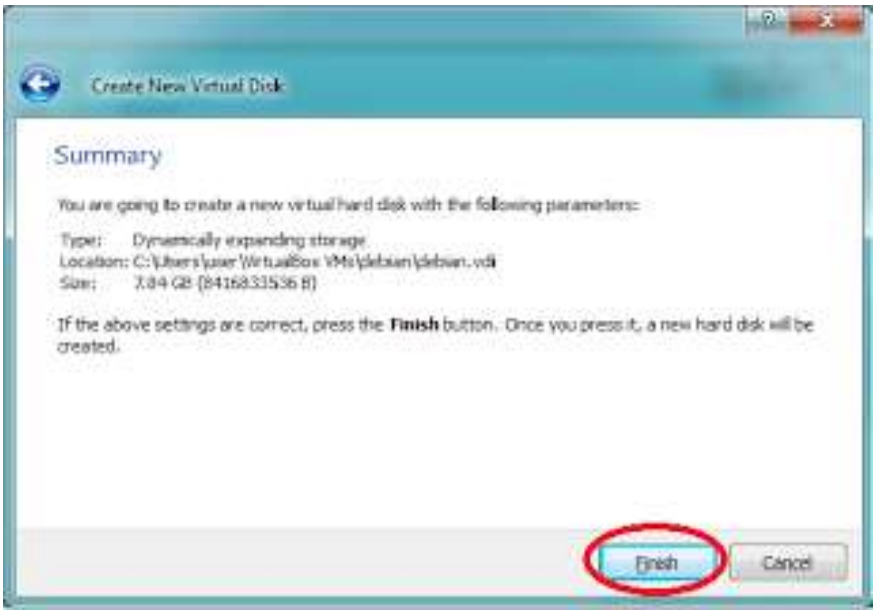


7) Kemudian akan muncul hard Disk storage Type lalu klik Dinamically expanding storage dan klik next.

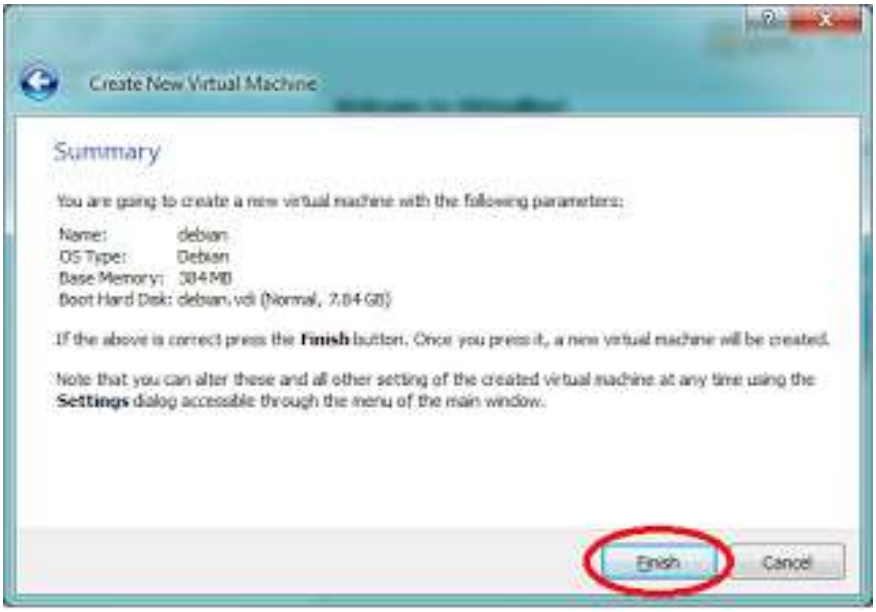
8) Kemudian pada virtual Disk location and size atur-atur ukuran seperti gambar di bawah .



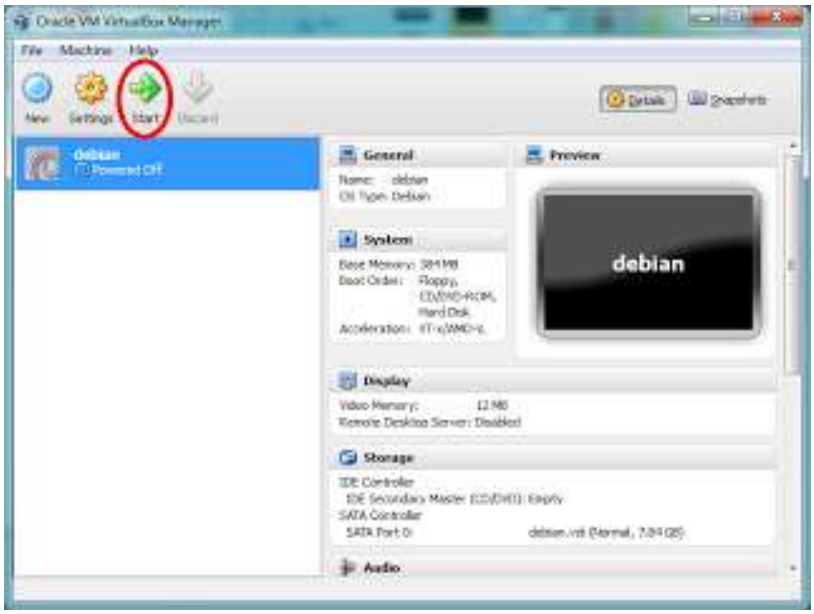
9) Kemudian akan muncul jendela seperti gambar di bawah lalu klik Finish.



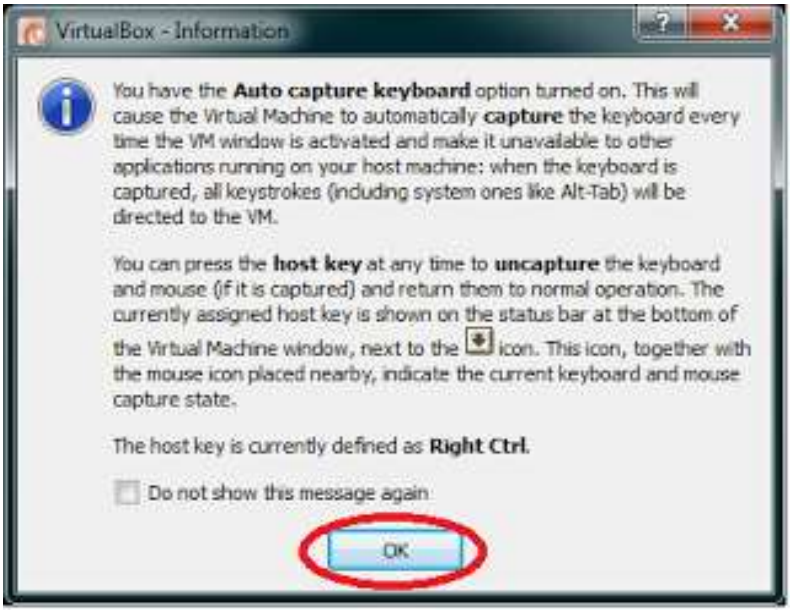
10) Lalu klik Finish lagi setelah muncul gambar seperti di bawah.



11) Kemudian klik Start setelah muncul jendela seperti ini.



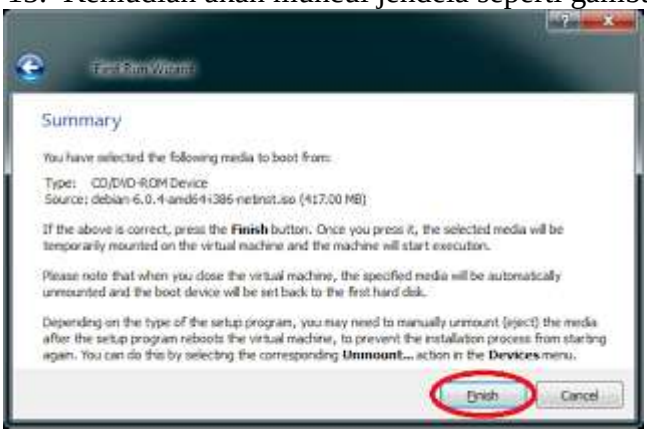
12) Kemudian akan muncul jendela VirtualBox-Information seperti gambar di bawah dan klik Ok .



13) Kemudaian akan muncul Welcome to the First Run wizard lalu klik Next.

14) Kemudian akan muncul select installation media ,lalu klik yang di tunjukkan pada tanda panah, masukan SO debian yang anda punya pada computer anda kemudian klik next

- 15. Kemudian akan muncul jendela seperti gambar di bawah lalu klik Finish.



- 16. Kemudian akan muncul starting virtual machine dan tunggu sampai proses selesai 100%

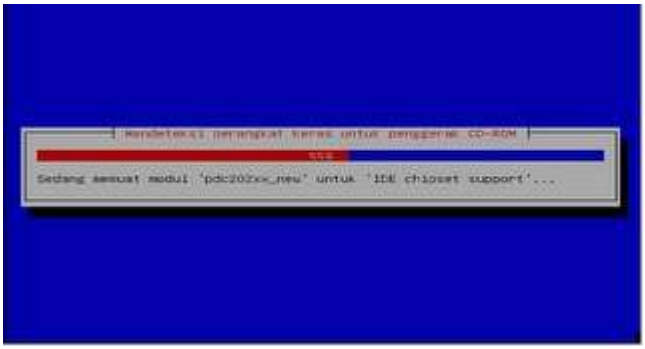
- 17. Kemudian setelah proses selesai akan muncul gambar seperti di bawah lalu klik Ok

- 18. lalu akan muncul gambar seperti di bawah ini.

- 19. Lalu pilih bahasa yang akan digunakan, pilih yang Indonesia, lalu tekan enter

- 20. Selanjutnya muncul pilih layout keyboard, pilih yang Inggris Amerika, lalu tekan enter.

- 21. Setelah itu tunggu proses deteksi hardware untuk penggerak CD-ROM.

- 

-

22. Selanjutnya muncul deteksi hardware jaringan,pilih yang tanpa kartu Ethernet**,** lalu enter.

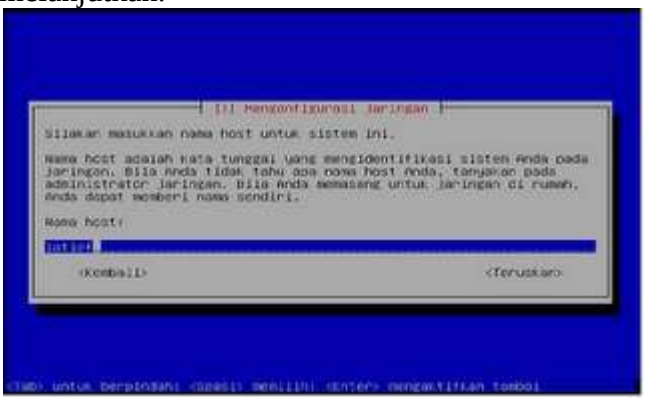
- 

-

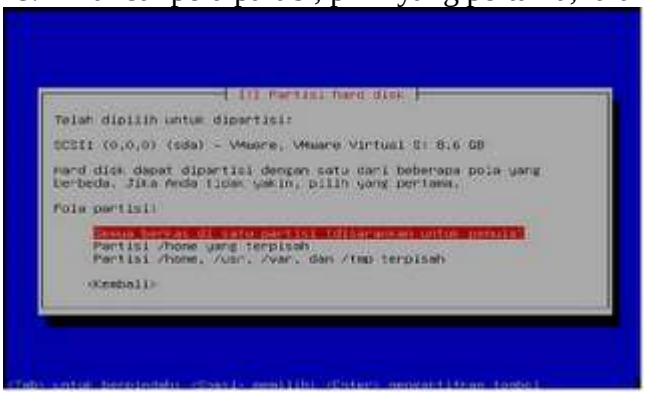
23. Setelah itu akan muncul mengkonfigurasi jaringan, lalu pilih teruskan,kemudian pilih untuk melanjutkan proses instalasi.

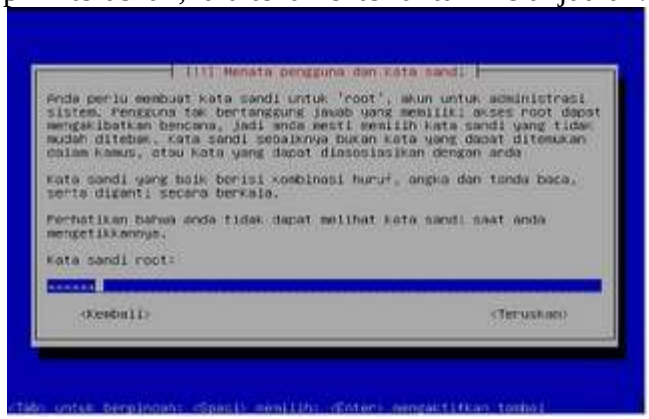
- 

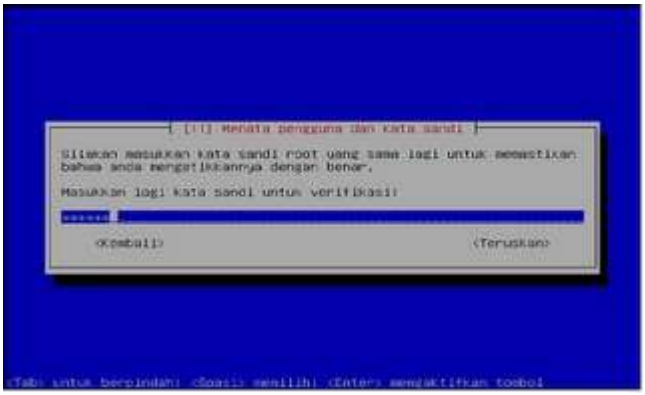
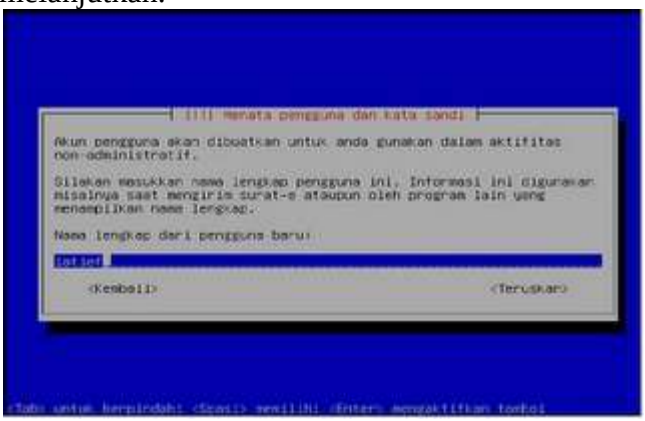
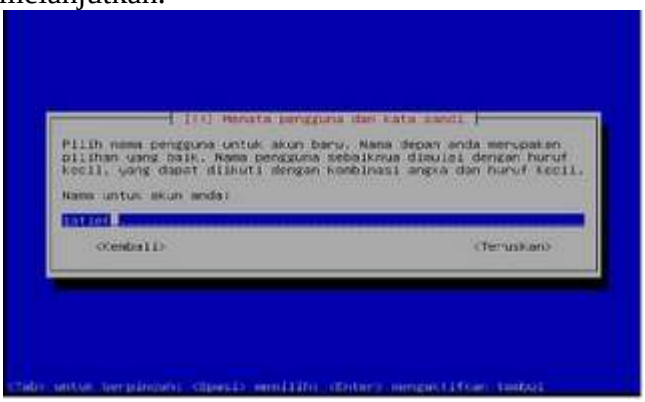
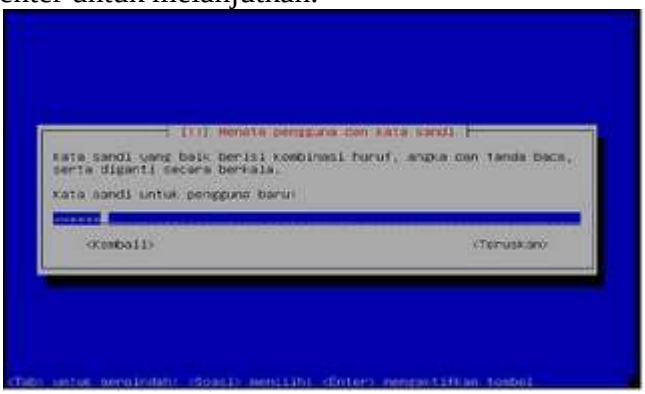
- 24. Setelah itu isi nama host untuk sistem ini, lalu pilih teruskan dan enter untuk melanjutkan.

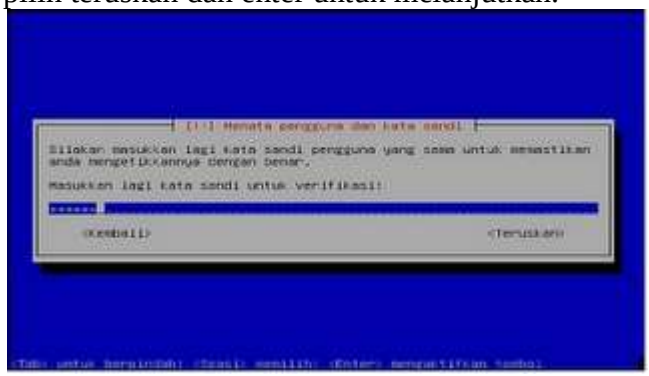
- 

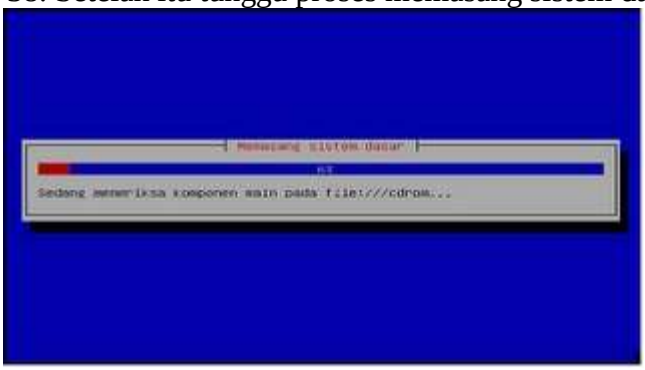
- 25. itu tunggu proses untuk memulai program pemartisi harddisk.

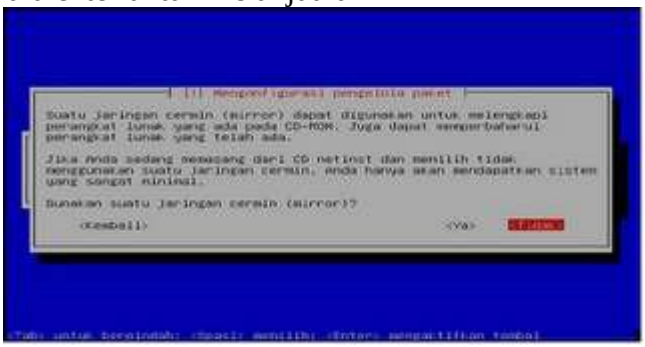
- 
- 26. Selanjutnya muncul partisi harddisk, pilih terpadu gunakan seluruh harddisk, lalu tekan enter
- 
- 27. Selanjutnya muncul pilih harddisk yang akan dipartisi, lalu tekan enter.
- 
- 28. Muncul pola partisi, pilih yang pertama, lalu tekan enter**.**
- 
- 29. Setelah itu muncul panduan tentang proses partisi pilih yang kedua, lalu enter untuk melanjutkan.

- 
- 30. Selanjutnya tuliskan perubahan yang terjadi pada harddisk, kita pilih ya, lalu enter untuk melanjutkan.
- 
- 31. Setelah itu muncul mengkonfigurasi zona waktu, pilih zona waktu yang sesuai dengan zona waktu anda, lalu enter untuk melanjutkan.
- 
- 32. Selanjutnya membuat password untuk root, kita tulis sesuai yang kita inginkan, lalu pilih teruskan, lalu tekan enter untuk melanjutkan.
- 
- 33. Selanjutnya tulis ulang kembali password yang barusan anda buat untuk mengkonfirmasi kebenaran password tersebut, lalu pilih teruskan dan enter untuk melanjutkan.

- 
- 34.Setelah itu tulis nama lengkap dari pengguna lalu pilih teruskan dan enter untuk melanjutkan.
- 
- 35. Selanjutnya tulis nama untuk akun anda, lalu pilih teruskan dan enter untuk melanjutkan.
- 
- 36.Setelah itu masukan password untuk pengguna baru, lalu pilih teruskan dan enter untuk melanjutkan.
- 

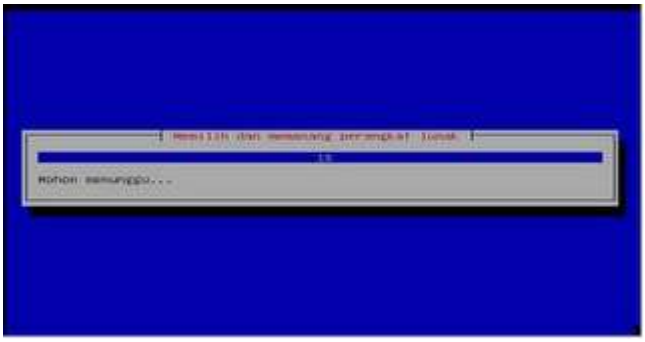
- 37. Lalu masukan kembali password untuk mengkonfrmasi kebenaran password, lalu pilih teruskan dan enter untuk melanjutkan.
- 

- 38. Setelah itu tunggu proses memasang sistem dasar.
- 

- 39. Setelah itu muncul jendela gunakan suatu jaringan cermin, kita pilih tidak**,** lalu enter untuk melanjutkan
- 

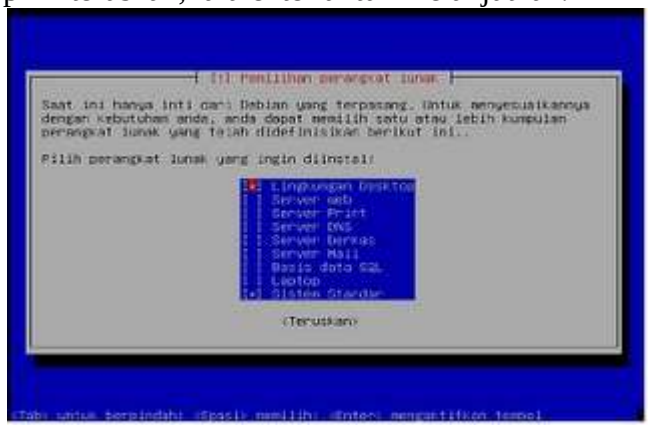
- 40. Setelah itu muncul jendela seperti gambar di bawah ini, kita pilih teruskan dan enter untuk melanjutkan.
- 

- 41. Setelah itu tunggu proses memilih dan memasang perangkat lunak.

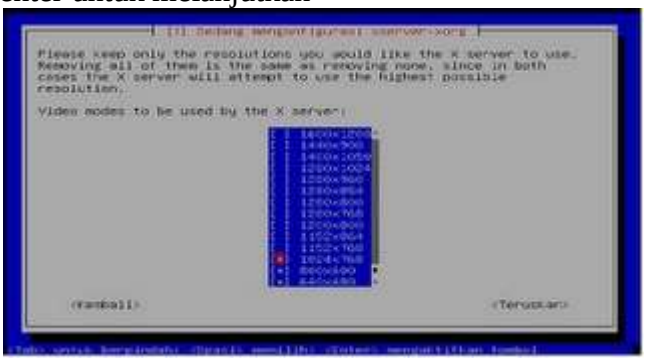


- 42. Setelah itu muncul survey penggunaan paket debian, kita pilih ya**,** lalu enter untuk melanjutkan.

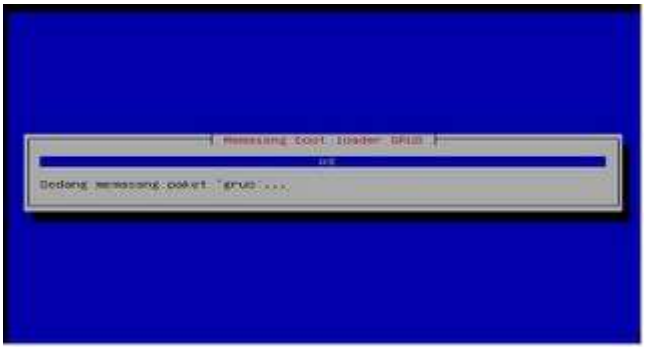
- 43. Selanjutnya memilih perangkat lunak yang akan diinstall (sudah tertera), kita pilih teruskan, lalu enter untuk melanjutkan.



- 44. Selanjutnya memilih resolusi gambar (sudah tertera), kita pilih teruskan, lalu enter untuk melanjutkan



- 45. Selanjutnya tunggu proses memasang boot loader GRUB.

- 
- 46. Selanjutnya memasang boot loader GRUB, kita pilih ya, lalu enter untuk melanjutkan.
- 
- 47. Setelah itu instalasi selesai, kita pilih teruskan, lalu enter untuk melanjutkan.
- 
- 48. S etelah proses instalasi selesai, nanti akan muncul tampilan nama pengguna, lalu kita masukan nama pengguna seperti yang kita buat pada saat proses instalasi , lalu enter untuk melanjutkan.
- 

- 49. Selanjutnya kita akan diminta untuk memasukan password, kita masukan password sesuai yang kita buat pada saat proses instalasi, lalu enter untuk melanjutkan

- 

-
- 50. Setelah proses instalasi yang begitu lama akhirnya instalasi Debian selesai juga dan Debian siap digunakan.
-