BAB III
PEMBAHASAN

3.1 Analisis

Analisis adalah pembagian suatu masalah menjadi komponen – komponen yang lebih kecil untuk mengidentifikasi dan mengevaluasi masalah dan hambatan yang ditemui, dan kebutuhan yang diharapkan sehingga nantinya dapat diusulkan perbaikan-perbaikannya. Bab ini menguraikan proses analisis pembangunan server VPN berbasis SSTP dan perancangan dan implementasi server VPN berbasis SSTP pada Jaringan PT Softex Indonesia Departemen Acounting. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan–kebutuhan server VPN berbasis SSTP yang akan dibangun.

3.1.1 Analisis Masalah

Di PT Softex Indonesia data hanya tersimpan di kantor saja dan hanya dapat diakses dengan jaringan internal. Hal ini mempersulit dalam berkomunikasi data untuk staff maupun rekan kantor ataupun antar Departemen yang mana antara Departemen Personalia dan Departemen Acounting berada di dua tempat yang berbeda yaitu yang satu di daerah Gajah Tunggal Km 7, Tangerang dan yang satu lagi berada di daerah Serpong, sehingga dalam komunikasi antar Divisi dilakukan lewat email, dan juga apabila Staff yang ditugaskan ke luar kota kadang lupa membawa data dari kantornya sehingga dapat menghambat pekerjaan. Rekan kantor juga harus datang langsung untuk mengambil data sehingga proses pekerjaan membutuhkan waktu yang lama.

Oleh karena itu, solusi yang lebih tepat adalah dengan munggunakan *Virtual Private Network* (VPN) berbasis Secure Socket Tunneling Protocol (SSTP). VPN merupakan suatu teknologi informasi yang komunikasi datanya dilewatkan pada jaringan publik Internet secara *private*.

SSTP merupakan bentuk baru dari VPN *tunnel* yang memiliki fitur mengizinkan trafik dapat melewati *firewall* yang memblok trafik PPTP dan trafik L2TP/IPsec. SSTP menyediakan mekanisme untuk mengenkapsulasi trafik PPP *over* SSL *channel* dari protokol HTTPS. Penggunaan PPP memungkinkan dukungan untuk metode autentikasi yang kuat dan handal seperti EAP-TLS.

Karena protokol SSTP baru dikembangkan oleh *Microsoft*, maka dalam implementasinya hanya dapat dikonfigurasi dan diakses oleh *client* dengan sistem operasi *windows*, dari *Windows Vista SP1* hingga yang terbaru saat ini. Kemudian akan dilakukan konfigurasi *routing* dan *remote access* untuk pengujian sistem agar berfungsi sebagai VPN *server* terhadap *client.*

Teknologi VPN membuat dunia semakin tak berbatas. Dengan hanya bermodalkan koneksi Internet, seluruh data dalam jaringan di kantor bisa di akses dengan mudah dengan keadaan data yang utuh. Staff dapat mengakses server kantor melalui VPN dimana saja, dirumah atau di luar kota secara aman meskipun menggunakan infrastruktur jaringan internet dalam penggunaannya. Diharapkan dengan diterapkannya Server VPN berbasis Protocol (SSTP) ini dapat mempermudah dan mempercepat dan mempermudah karyawan PT Softex Indonesia dalam menyelesaikan pekerjaanya.

3.1.2 Keuntungan Pembangunan Server VPN berbasis SSTP

Ada beberapa keuntungan yang dapat diperoleh PT Softex Indonesia dengan menggunakan server VPN berbasis SSTP.

1. Jangkauan jaringan lokal yang dimiliki perusahaan akan menjadi luas. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal juga semakin cepat karena proses instalasi infrastruktur jaringan dilakukan di kantor PT Softex dengan ISP terdekat. Dengan demikian, penggunaan VPN secara tidak langsung akan meningkatkan efektifitas dan efisiensi kerja.
2. Server VPN berbasis SSTP memberi kemudahan untuk mengakses data, program aplikasi, mail intranet yang ada di PT Softex Indonesia,

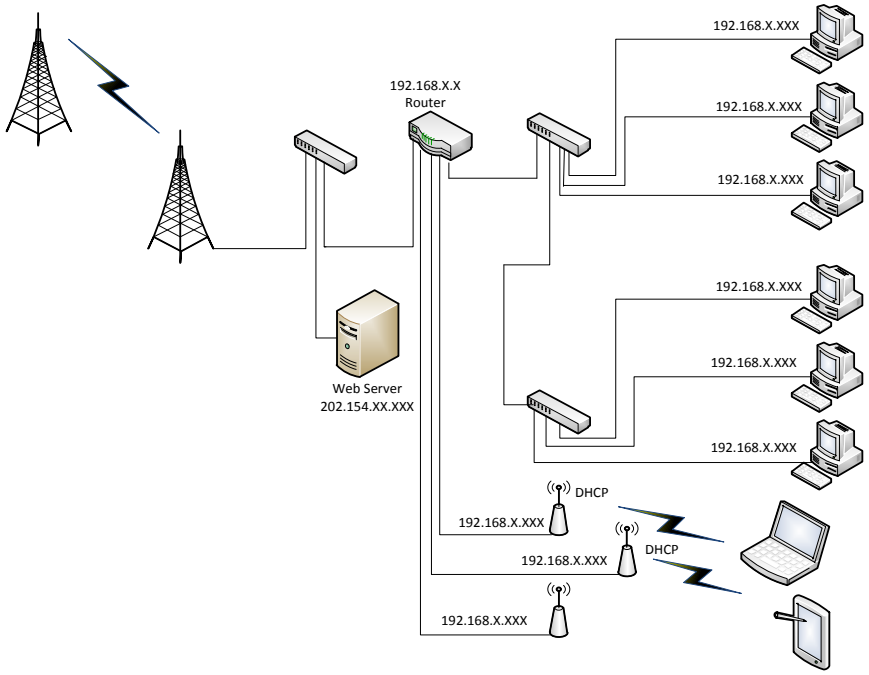
Departemen Acounting karena VPN terhubung ke internet, sehingga pegawai yang kebetulan bertugas diluar kantor dapat mengakses jaringan khusus perusahaan di mana pun dia berada. Selama dia bisa mendapatkan akses ke internet atau ke ISP terdekat.

Sebelum melakukan pembangunan server VPN berbasis SSTP di PT Softex Indonesia di bagian Departemen Acounting, akan diuraikan proses pembangunan server VPN berbasis SSTP dan perancangan dengan langkah-langkah sebagai berikut.

1. Analisis topologi jaringan.
2. Analisis kebutuhan sistem.
3. Skenario untuk Koneksi Remote Access VPN berbasis SSTP
4. Proses Koneksi Server VPN berbasis SSTP
5. Perancangan sistem VPN berbasis SSTP
6. Implementasi & Pengujian VPN berbasis SSTP

3.2 Analisis Topologi

Topologi jaringan merupakan tata letak serta struktur hubungan antara komponen-komponen (node) dalam suatu jaringan. Topologi jaringan berkaitan dengan mekanisme yang digunakan untuk mengelola cara station (komputer) dalam mengakses jaringan, sehingga tidak terjadi konflik. Berikut ini adalah topologi jaringan yang sedang berjalan di PT Softex Indonesia.



Gambar 3.1. Topologi Jaringan yang sedang berjalan.

3.2.1 Pengalamatan IP PT Softex Indonesia

Pengalamatan IP di jaringan PT Softex Indonesia bagian departemen Acounting menggunakan IP *static* berdasarkan DHCP *server*. Dimana setiap *client/user* yang sudah terdaftar atau memperoleh IP dari server dicatat *macaddressnya* oleh *server* supaya IP yang diperoleh tidak berubah lagi.

Range IP address yang dipakai oleh user antara 1 – 100 sedangkan *IP address* dibawah dipakai sebagian oleh *server* diantaranya:

1. *IP address* 192.168.1.1 di pakai oleh *server* windows 2008 server dimana di dalam windows 2003 server terdiri dari DHCP *server*, DNS *server*, *Activ directory server* (*Domain Contoller*), *File server*, dan *Data base Server*.

2. *IP address* 192.168.1.10 dipakai sebagai router dimana didalam router tersebut terdiri dari *gateway server* dan *proxy server*
3. *IP address* 192.168.1.5 digunakan untuk *email server*
4. *IP address* 192.168.1.4 digunakan untuk mikrotik VPN *server*

3.2.2 Server PT Softex Indonesia Departemen Acounting

Dalam jaringan di PT Softex Indonesia departemen Acounting terdapat 2 server. Server yang ada yaitu adalah.

1. Server Acounting

Menggunakan Windows Server 2008 mempunyai alamat IP 192.168.1.1 berfungsi sebagai :

1. DHCP Server

DHCP server pada jaringan PT Softex yang berfungsi menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua Client Acounting yang memintanya.

2. DNS Server

DNS* (*Domain Name System) pada PT Softex menyimpan informasi tentang nama *host* maupun nama *domain (softexindonesia.com)* dalam bentuk basis data tersebar (*distributed database*) di dalam jaringan komputer, DNS pada jaringan PT Softex menyediakan servis yang cukup penting untuk internet, karena penggunaan perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan pengalamatan dan penjaluran (*routing*)kurang optimal. Oleh karena itu, pada umumnya *user* lebih memilih menggunakan nama *host* dan nama *domain*.

3. Active Directory

Pada Server Acounting menginstal *Active Directory* pada Microsoft Windows Server 2008 untuk memaksimalkan kinerja. Dan Semua yang berhubungan dengan services dan domain ada dalam *Active Directory* ini.

4. **File Server**

Menyediakan layanan berupa pengelolaan dan pengaksesan *file* oleh Client Acounting

5. **Data Base Server**

Menyediakan ruang *(space)* bagi Client Acounting untuk penyimpanan data

2. Router Server

Menggunakan system operasi Mikrotik dan mempunyai alamat IP 202.154.10.1 yang berfungsi sebagai:

1. *Gateway Server*
2. *Proxy Server*

3.3 Analisis Kebutuhan Sistem VPN berbasis SSTP

Untuk analisis kebutuhan sistem, terdapat tiga komponen inti yang akan dijelaskan kebutuhan sistemnya dalam membangun *server* VPN berbasis SSTP ini. Komponen tersebut antara lain *client*, *domain controller*, dan *server* VPN berbasis SSTP. Untuk lebih jelasnya akan dijabarkan dibawah ini

3.3.1 Domain Controller

Domain controller menjadi *server* computer Departemen Acounting PT Softex yang menggunakan *windows server 2008*. Dalam proyek akhir ini *domain controller* akan diinstal beberapa kebutuhan sistem yang menyediakan *service-service* antara lain *Domain Name Sistem* (DNS) *server*, dan *file server* pada *private* (*intranet*) *network.*

1. *Active Directory*

Dalam proyek akhir ini *active directory* berfungsi sebagai *control network resources* secara terpusat. Hanya *user* yang berhak yang bisa mengakses *network resources* tersebut. *Administrator* bisa mengatur *network resources* dari lokasi terpusat atau bisa juga mendelegasikan pengelolaan sebagian atau seluruh *network resources* ke *administrator* lain.

2. *Domain Name Sistem* (DNS)

   Dalam proyek akhir ini dikonfigurasi DNS dan diberi nama *softexindonesia.com* yang berfungsi sebagai pengalamat dan penjaluran *routing* terhadap alamat IP *domain controller* dalam membantu *access client* ke *server*.

3. *File Sharing*

   Pada implementasinya, *Domain controller* merupakan *file sharing* yang harus dapat diakses oleh *remote user* setelah metode akses dan autentifikasi dikonfigurasi.

3.3.2 Server VPN Berbasis SSTP

Server VPN disini menggunakan *windows server 2008*. Dalam proyek akhir ini *server* VPN akan memiliki *service-service* antara lain.

1. *Active directory certificate service*

   Crtification Authority (CA) yang menerbitkan sertifikat komputer yang diperlukan untuk koneksi VPN berbasis SSTP pada PT Softex. *Active Directory Certificate Service* dalam *windows server operating system* berfungsi menyediakan layanan membuat dan mengelola *public key certificate* yang dapat disesuaikan dan digunakan dalam sistem keamanan software menggunakan teknologi kunci *public*. Suatu Organisasi dapat menggunakan AD CS untuk meningkatkan kemanan dengan mengidentifikasi seseorang, perangkat atau layanan *private key* lainnya.

2. *Certification Authority Web Enrollment*

   Sebuah *service* yang untuk mengaktifkan penerbitan dan sertifikat melalui *web browser*. Dalam implementasi proyek akhir ini, *certificate service* harus diinstal serta diterbitkan baik di *server* VPN maupun di *client* untuk autentifikasi protocol SSTP. *Service* ini juga digunakan oleh *client* untuk mengautentifikasi *server* VPN

3. *Web Server (IIS)*

Sebuah HTTP *web server* yang digunakan dalam sistem operasi *server windows* di PT Softex. Dimana layanan ini berfungsi sebagai pendukung protocol TCP/IP yang berjalan dalam *layer application*. Pada proyek akhir ini *web server* (IIS) diinstal dan diperlukan sebagai *service* untuk *Certification Authority Web Enrollment*.

4. *Network Policy* Dan *Access Service*

   Service untuk menyediakan dukungan koneksi VPN melalui *remote access service* pada jaringan PT softex.

5. *Routing* Dan *Remote Access*

   Layanan *routing* dan *remote* akses di dalam *windows server* menyediakan *remote user access* ke *resource* didalam jaringan *private* PT Softex melalui *Virtual Private Network* (VPN). *Server* yang dikonfigurasi *routing* dan *remote access service* dapat menyediakan layanan *Local Area Network* (LAN) dan *Wide Area Network* (WAN) layanan *routing* digunakan untuk menghubungkan segmen jaringan dalam kantor atau untuk menghubungkan dua *private network* melalui internet. Jadi *routing* dan *remote access* harus dikonfigurasi agar berfungsi sebagai *server* VPN.

3.3.3 Client

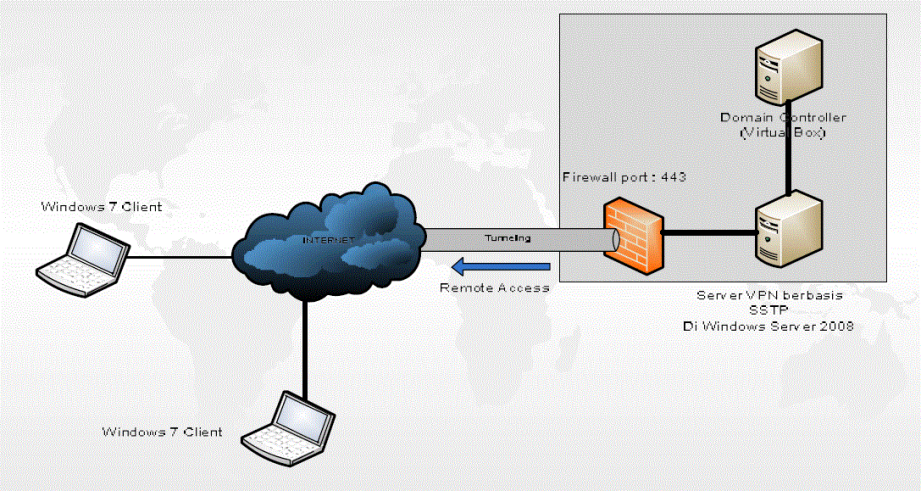
Client pada PT Softex Indonesia Departement Acounting menggunakan sistem operasi *windows* 7 yang berfungsi sebagai *remote access* VPN *client* untuk domain *wirecat.com*. *Client* terhubung pada jaringan *public*. VPN *client* yang menggunakan koneksi SSTP harus menginstal sertifikat *root CA certificate* computer dari *server* VPN. Selama fase autentifikasi berlangsung, VPN *client* memvalidasi *server* authentication *certificate* dengan menggunakan sertifikat yang diinstal pada *client*. *Root certificate* dapat diperoleh melalui *auto-enrollment*, jika *client* digabungkan ke domain *active directory*, atau melalui *web enrollment*

3.4 Skenario untuk Koneksi Remote Access VPN berbasis SSTP

Infrastruktur jaringan VPN berisi 3 komputer yang menjalankan masing-masing service berikut:

1. Satu server komputer yang menggunakan Windows Server 2008 diberi nama DC01 yang berperan sebagai domain controller, Domain Name System (DNS) server, dan file server pada private (intranet) network.
2. Satu server komputer yang menggunakan Windows Server 2008 diberi nama VPN01 yang dikonfigurasi dengan Routing and Remote Access dan berperan sebagai VPN server. Sebagai tambahan, VPN01 dikonfigurasi dengan Active Directory Certificate Services dan Internet Information Services (IIS) untuk kebutuhan Web enrollment dari computer certificate yang diperlukan untuk koneksi VPN berbasis SSTP. VPN01 memiliki dua network adapter.
3. Satu client komputer yang menjalankan Windows 7 diberi nama CLIENT01 yang berperan sebagai VPN client pada public (Internet) network.

   Diagram berikut menunjukkan konfigurasi dari test lab VPN tersebut :



Gambar 3.2. Access VPN berbasis SSTP [5]

3.5 Proses Koneksi Server VPN berbasis SSTP

Saat user yang menggunakan komputer Windows Server 2008 atau Windows 7 menginisiasi suatu koneksi VPN berbasis SSTP, maka terjadi proses sebagai berikut:

1. Client SSTP membentuk suatu koneksi TCP dengan server SSTP antara port TCP yang dialokasikan secara dinamis pada client SSTP dan port TCP 443 pada server SSTP.

2. Client SSTP mengirimkan sebuah *SSL Client-Hello message*, mengindikasikan bahwa client SSTP ingin membuat sebuah *SSL session* dengan server SSTP.
3. Server SSTP mengirimkan sertifikat komputernya ke client SSTP.
4. Client SSTP memvalidasi sertifikat komputer tersebut, menentukan metode enkripsi untuk SSL session, membuat sebuah *SSL session key* dan mengenkripsi-nya dengan *public key* yang berasal dari sertifikat milik server SSTP, dan kemudian mengirimkan *encrypted form* ini ke server SSTP.
5. Server SSTP men-dekrip *encrypted SSL session key* dengan private key yang berasal dari sertifikat komputernya.
6. Client SSTP mengirimkan pesan permintaan HTTP over SSL ke server SSTP.
7. Client SSTP melakukan negosiasi sebuah *SSTP tunnel* dengan server SSTP.
8. Client SSTP menegosiasi sebuah koneksi PPP dengan server SSTP. Dalam negosiasi ini termasuk di dalamnya proses melakukan autentikasi user credential dengan metode autentikasi PPP dan seting konfigurasi untuk trafik Internet Protocol version (IPv4) atau Internet Protocol version 6 (IPv6).
9. Client SSTP mulai mengirimkan trafik IPv4 atau trafik IPv6 melalui jalur PPP.

3.6 Perancangan Sistem

Pada bagian ini akan dibahas mengenai perencanaan infrastruktur server VPN berbasis SSTP di Jaringan PT Softex, inpementasi system pengujian, kebutuhan dari perangkat keras maupun perangkat lunak yang dipergunakan pada jaringan untuk implementasi server VPN berbasis SSTP tersebut.

3.6.1 Imlementasi Sistem Pengujian

Berdasarkan dari gambaran arsitektur system diatas, maka dalam implementasi pengujiannya, didalam komputer *server* VPN diinstal *virtual box*. Fungsi *virtual box* sendiri adalah tempat konfigurasi *domain controller*. *Domain controller* dan *server* VPN tergabung dalam satu komputer, tapi terpisah oleh dua

operating system. Hal ini mensimulasikan bahwa *domain controller* memiliki komputer yang terpisah dari *server* VPN. Dalam Analisis sistemnya, *domain controller* dapat lebih dari satu, namun dalam proyek akhir ini hanya menggunakan satu *domain controller*.

Untuk simulasi jaringannya sendiri, pada arsitektur sistem, *client* mengakses *server* melalui *tunneling* dalam jaringan internet WAN. Hal itu juga mensimulasikan bahwa *client* mengakses *server* dari jarak yang jauh. Namun dalam pengujiannya, jaringan internet itu sendiri diimplementasikan dengan jaringan LAN yang menggunakan *switch* dan menggunakan *ip address public* antara akses *client* ke *server* VPN

Pada pengujian proyek akhir ini mempunyai dua komputer sebagai *client* yang secara bersama akan mengakses *server* VPN berbasis SSTP. Setiap *client* SSTP harus menerbitkan sertifikat CA dikomputer masing-masing agar bisa melakukan *remote access*:

3.6.2 Kebutuhan Perangkat Keras dan Perangkat Lunak

Dari perngujian yang akan dilakukan tentang kebutuhan sistem, maka dibawah ini akan dijelaskan kebutuhan *hardware* dan *software* untuk pengimplementasian dan pengujian sistem serta bagaimana proses koneksi. Spesifikasi kebutuhan dibawah ini adalah berdasarkan pengujian, bisa saja diimplementasikan kepada spesifikasi yang lebih tinggi.

1. **Perangkat Keras**

Tabel 3.1. Kebutuhan Perangkat Keras

No	Perangkat	Unit	Spesifikasi Hardware
1	Server VPN	1	Prosesor, Memori 2.5 GB DDR2 Hardisk 100 GB

2	Client	1	Memory 2 Gb DDR2
		1	Prosesor Memory 2.5 Gb DDR2
3	Jaringan	1 3	Swich 8 Port Kabel UTP

2. Perangkat Lunak

Tabel 3.2. Kebutuhan Perangkat Lunak

No	Software	Implementasi	Keterangan
1	Virtual Box	Domain Controller	Domain controller dikonfigurasi pada virtual box
2	Windows Server 2008	Server VPN	Sistem Operasi Server
		Domain Controller	Sistem Operasi Domain Controller
3	Certificate SSTP	Server VPN	Untuk Menerbitkan sertifikat akses server VPN berbasis SSTP

3.7 Implementasi

Tahap implementasi dilakukan berdasarkan analisis dan perancangan yang telah dibuat, yaitu mengkonfigurasi berdasarkan analisis dan perancangan. Infrastruktur untuk implementasi jaringan VPN memiliki tiga komputer yang menjalankan masing-masing *service,* Setelah implementasi selesai dilakukan, maka

akan dilakukan pengujian terhadap *Remote Access Virtual Private Network* berbasis SSTP yang telah dibangun.

3.7.1 Konfigurasi Domain Controller

DC01 adalah komputer yang menjalankan Windows Server 2008 yang menyediakan service-service berikut:

1. Domain controller untuk Active Directory domain softexindonesia.com.
2. DNS server untuk DNS domain softexindonesia.com.
3. File server.

Konfigurasi dari DC01 memerlukan langkah-langkah berikut :

1. Instal sistem operasi.
2. Konfigurasi TCP/IP.
3. Instal Active Directory dan DNS.
4. Buat sebuah user account dengan remote access permission.
5. Buat sebuah shared folder dan file.

Langkah-langkah tersebut secara detail sebagai berikut.

Instalasi Sistem Operasi

Instalasi Windows server 2008

1. Pada DC01, menjalankan computer yang menggunakan Windows Server product disv
2. Ikuti intruksinya yang di layar, dan pada saat di minta untuk menggantikan password masukan **P@ssword**

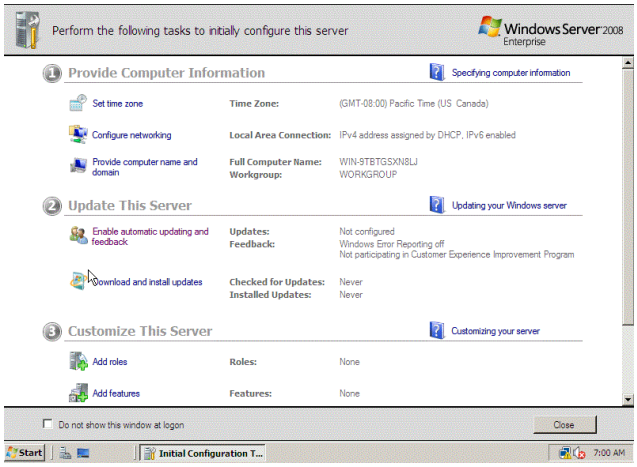
3.7.1.1 Konfigurasi TCP/IP

Konfigurasi property dari TCP/IP sedemikian sehingga DC01 memiliki static IP address 192.168.1.1 dengan subnet mask 255.255.255.0 dan default gateway 192.168.1.2.

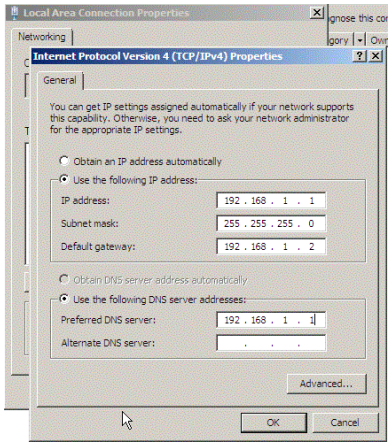
Langkah-langkah mengkonfigurasi TCP/IP adalah sebagai berikut :

1. Pada DC01, pada window **Initial Configuration Tasks**, pada bagian **Provide Computer Information**, klik **Configure networking**.

Catatan : Jika window **Initial Configuration Tasks** belum terbuka, kita dapat membukanya dengan cara klik **Start**, klik **Run**, dan ketikkan oobe dan klik **OK**.



2. Pada Windows Network Connections, klik-kanan **Local Area Connection,** dan kemudian klik **Properties**
3. Pada tab **Networking,** klik Internet Protocol Version 4 (TCP/IPv4), dan kemudian klik Properties
4. Klik Use the folloing IP address. Ketikan 192.168.1.1 untuk IP address, ketikan 255.255.255.0 untuk subnet mask, ketikan 192.168.1.2 untuk default geteway. Dan ketikan 192.168.1.1 untuk preferrend DNS server.



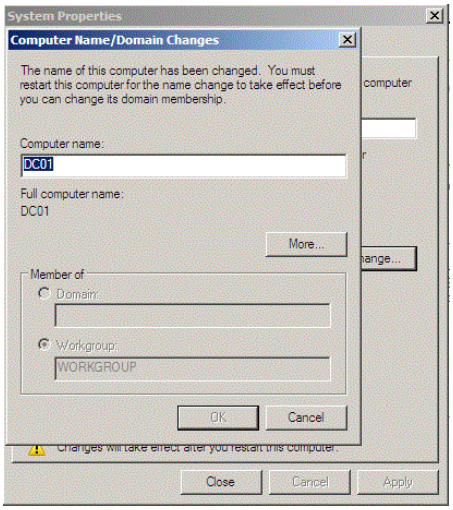
5. Klik OK. Dan kemudian close.

3.7.1.2 Instalasi Active Directory dan DNS

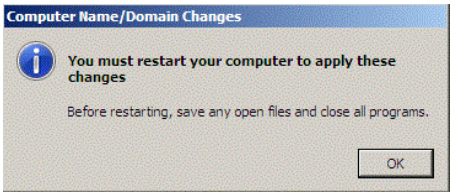
Konfigurasi computer DC01 sebagai domain controller untuk domain softexindonesia.com. computer DC01 akan menjadi DC yang pertaman dan satu-satunya DC pada jaringan yang akan dibuat ini.

Langkah-langkah komfigurasi DC01 sebagai domain Controller.

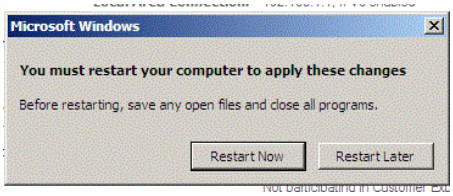
1. Pada DC01, pada windows initial configuration Tasks, pada bagian Provide Computer Information, klik Provide **Computer name and Doamain.**
2. Pada kotak dialog System Properties, Pada Tab Computer Namae, klik Change.
3. Ubah computer namae menjadi DC01, dan kemudian klik Ok.



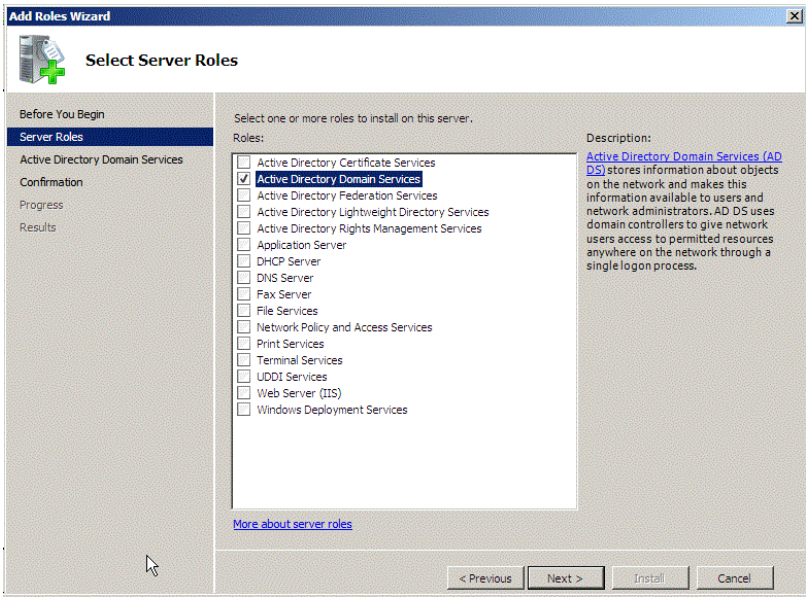
4. Pada kotak dialog Computer Name/domain Changes, klik Ok.



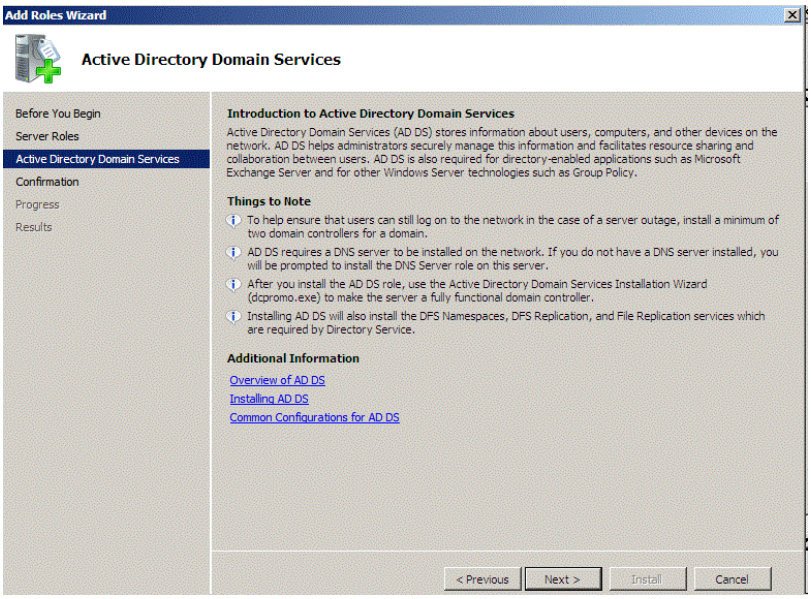
5. Klik Close, dan kemudian klik **Restart Now**.



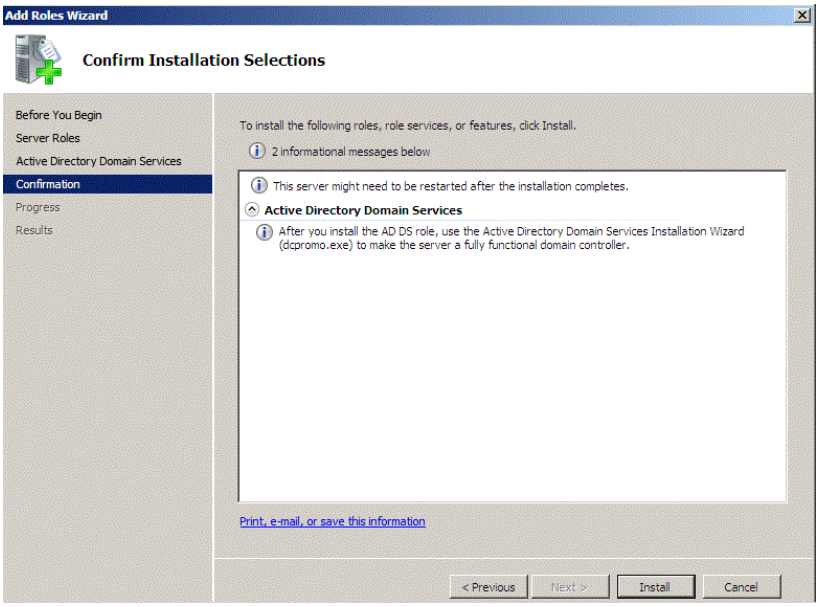
6. Setelah server restart, pada window initial configuration Task, pada bagian Costumize Thi server, klik **Add Roles**
7. Pada kotak dialog Add Roles Wizard, pada Before You Begin, Klik Next.
8. Pilih kotak cek Active Directory Domain Services dan kemudian klik Next.



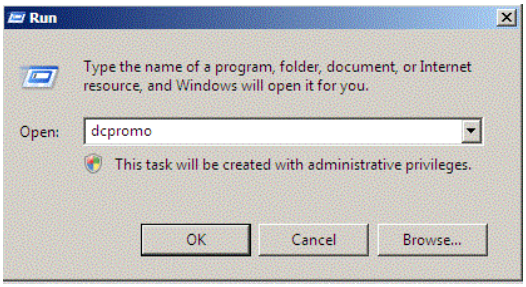
9. Pada kotak dialog Active Directory Domain Services, klik Next.



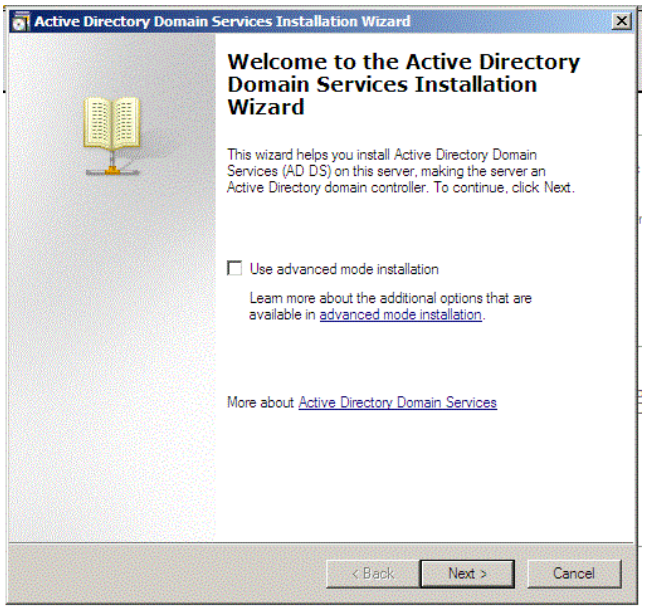
10. Pada Kotak dialog Confirm Instalation, Klik Instal.



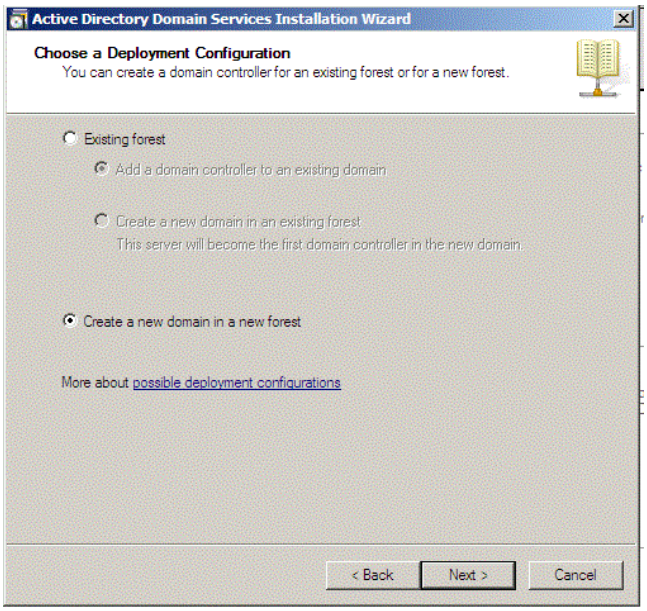
11. Pada kotak dialog Instalation Result, Klik Close.
12. Klik Start, dan kemudian klik run. Pada Open, Ketikan **DCPROMO,** dan kemudian klik Ok.



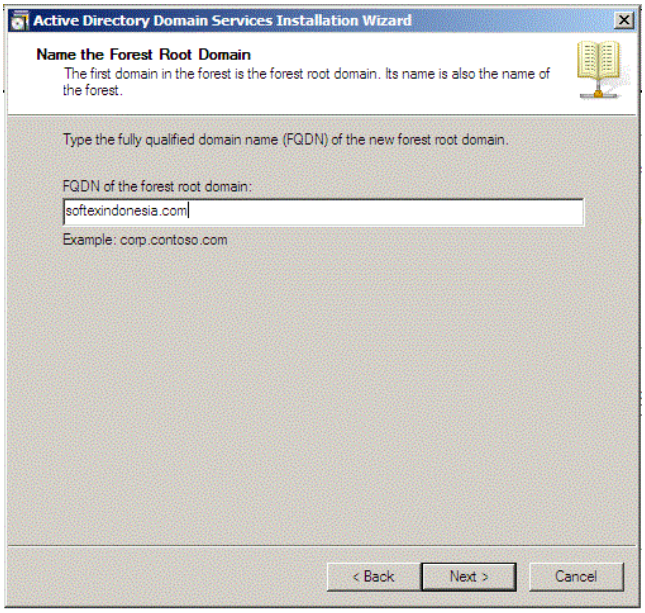
13. Pada halaman Welcome to the Active Directory Domani Services Instalation Wizard, Klik Next.



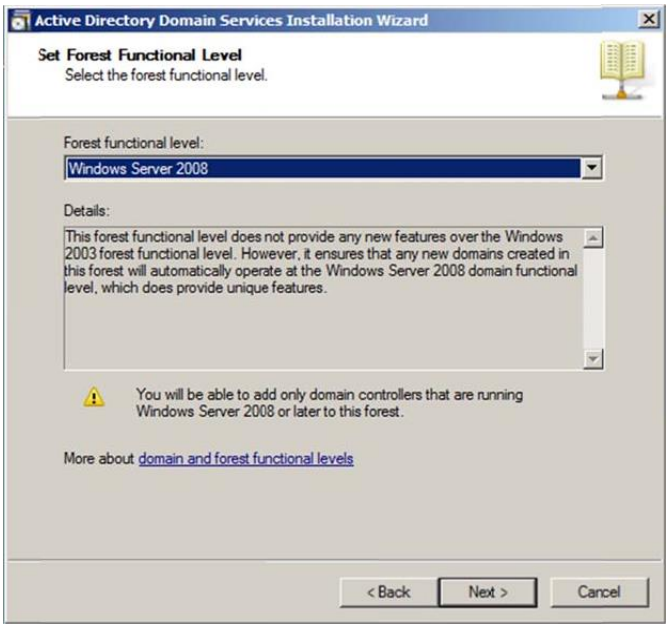
14. Klik Create a new domain in a new forest, dan kemudian klik Next. (masukan domain : *softexindonesia.com*)



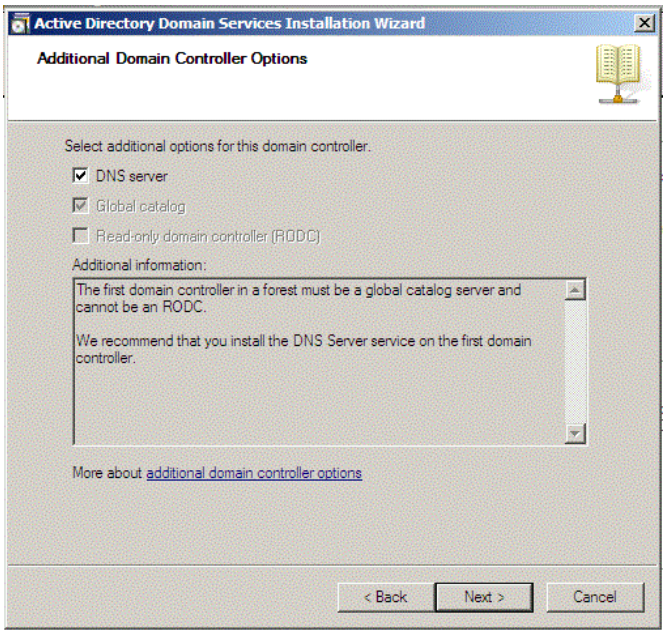
15. Pada FQDN of the forest root domain, ketikan *softexindonesia.com*, kemudian klik Next.



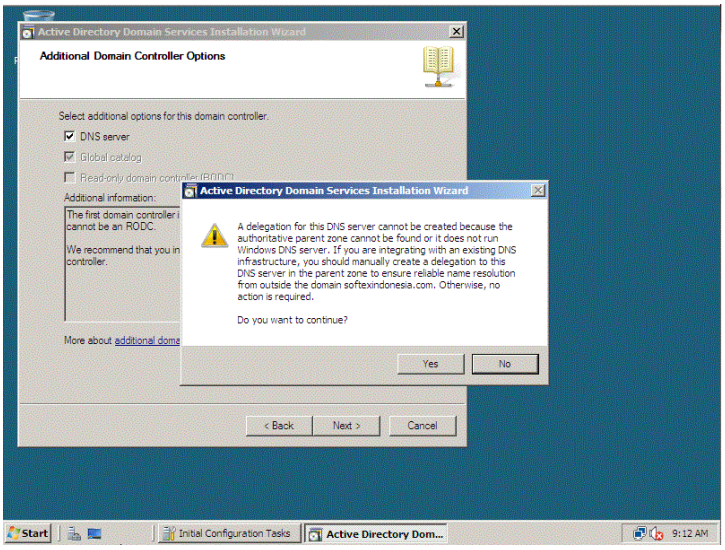
16. Pada forest functional level, pilih **Windows Server 2008,** dan kemudian Next.



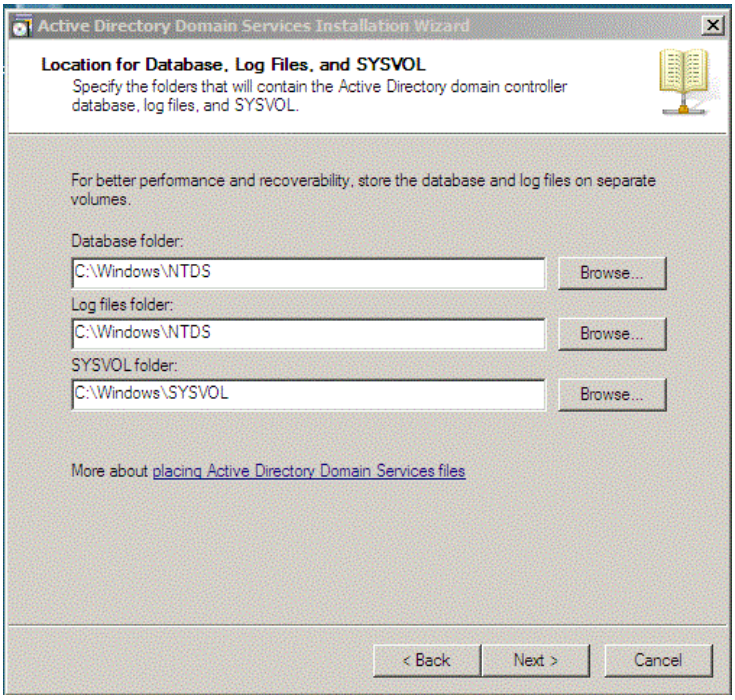
17. Pada h alaman Additional Domain Controller Options, Klik Next.



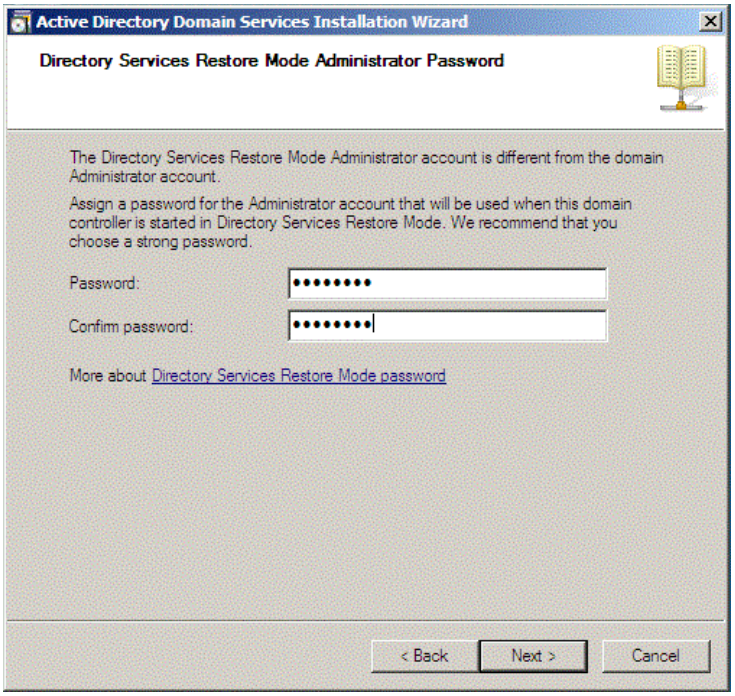
18. Selanjutnya Klik Yes



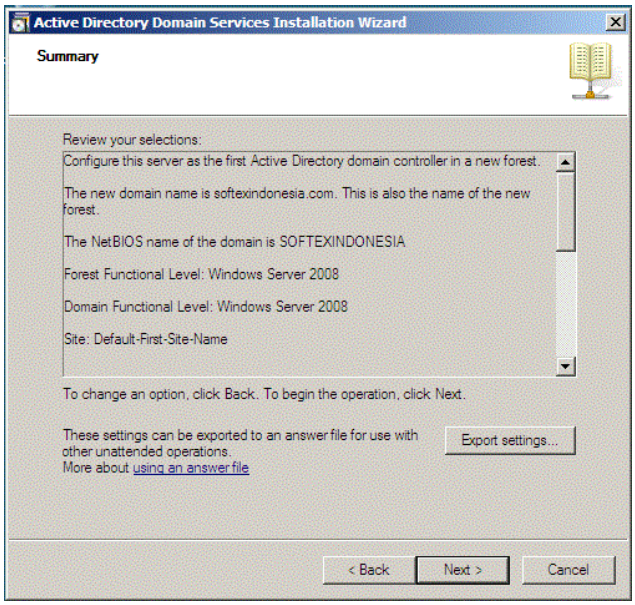
19. Untuk Lokasi datavase folder, log files forlder, dan SYSVOL folder, biarkan lokasi defaultnya dan klik Next.



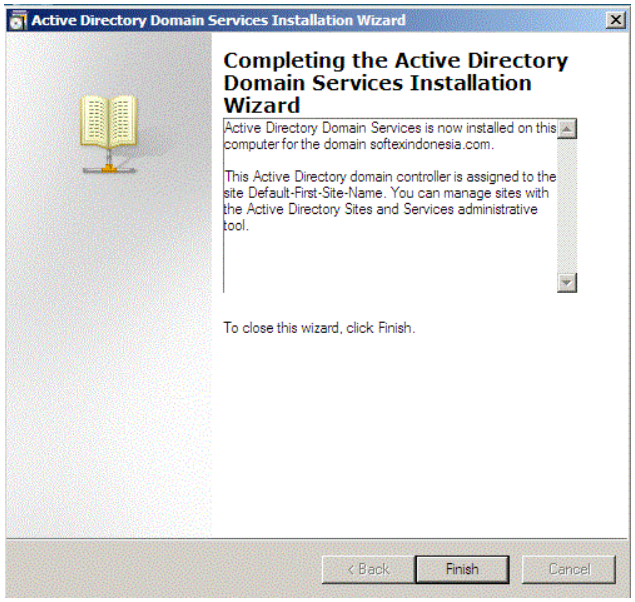
20. Berikan password untuk Directory Services Restore Mode Administrator Password, klik Next.

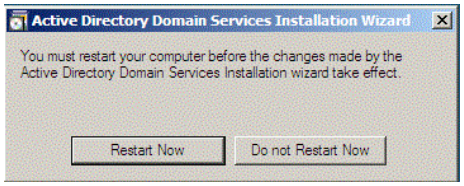


21. Pada hlaman Summary klik Next.



22. Active Directory domain services Instalation Wizard akan memulai melakukan konfigurasi Active Derectory. Saat konfigurasi selesai, klik Finish, dan kemudian klik Restart Now.





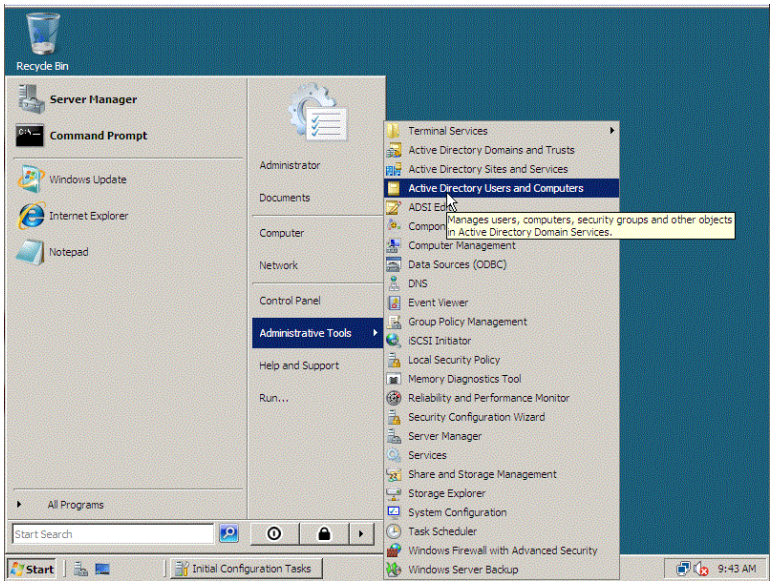


3.7.1.3 Membuat User Account dengan Remote Access Permission

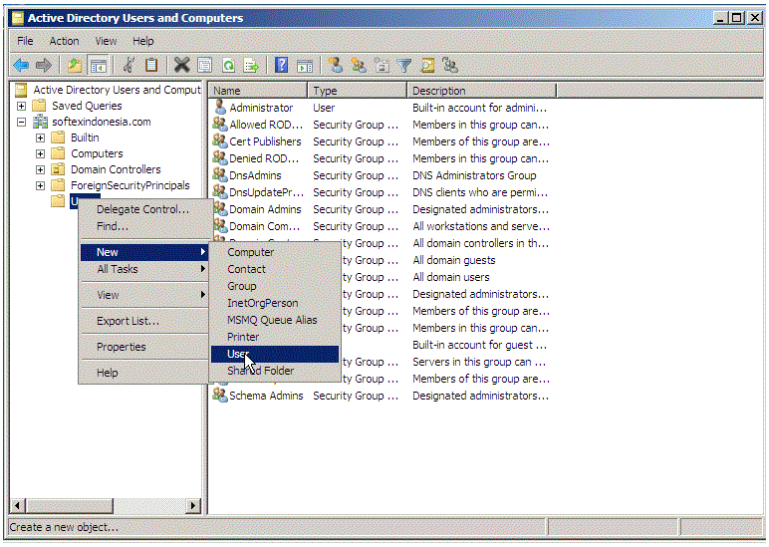
Membuat sebuah user account dan konfigurasi account tersebut dengan remote access permission.

Langkah-langkah membuat dan memberikan permission ke user account di Active Directory:

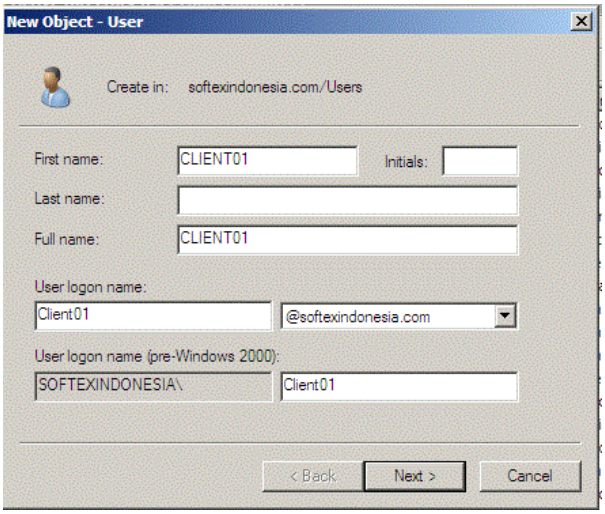
1. Pada DC01, klik Start, kemudian klik Administrative Tools, dan klik Active Directory Users dan Computers.



2. Buka *softeiIndonesia.com*, klik kanan Users, polih New, dan kemudian klik User.

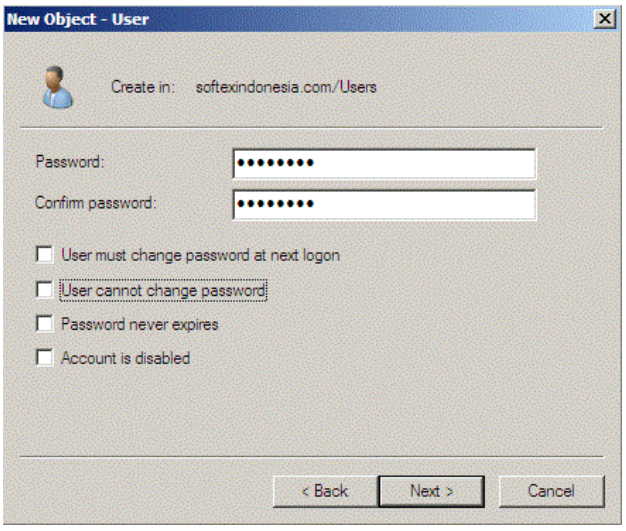


3. Pada Fullname, ketikan Client01, dan pada user logon name, ketika Client01.



4. Klik Next.
5. Pada Password, ketikan P@ssword dan pda confrime password, ketikan hal yang sama
6. Bersihkan pilihan tanda cek pada User must change at next login, dan kemudian juga pada tanda cek pada User cannot change password and

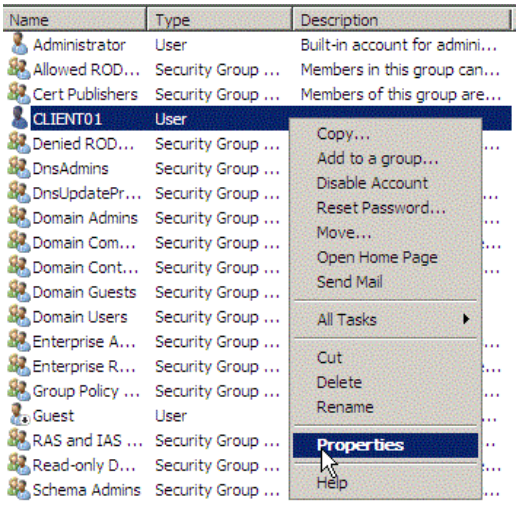
password never expires.



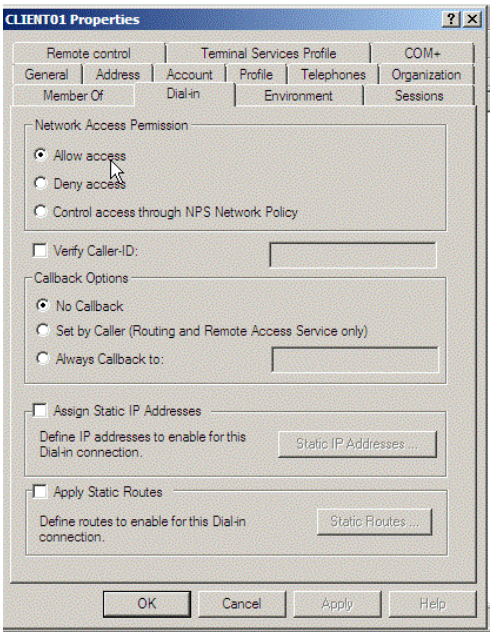
7. Klik Next. Dan kemudian klik Finish.

Langkah-langkah untuk memberikan remote access pemission ke Client01.

1. Pada Users. Klik –kanan Client01, dan kemudian pilih Properties.



2. Pada tab Dial-in, pada Network Access Permission, klik Allow Access, dan klik Ok,



Catatan : Pada scenario production, sebaiknya kita menggunakan Network Policy server (NSP) untuk mengkonfigurasi dan mengaktifkan remote access policies.

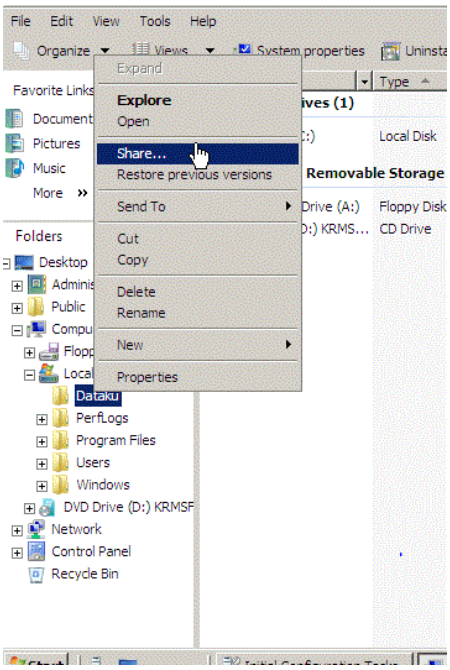
3. Tutup Active Directoru Users dan Computers.

3.7.1.4 Membuat Sebuah Shared Folder dan File

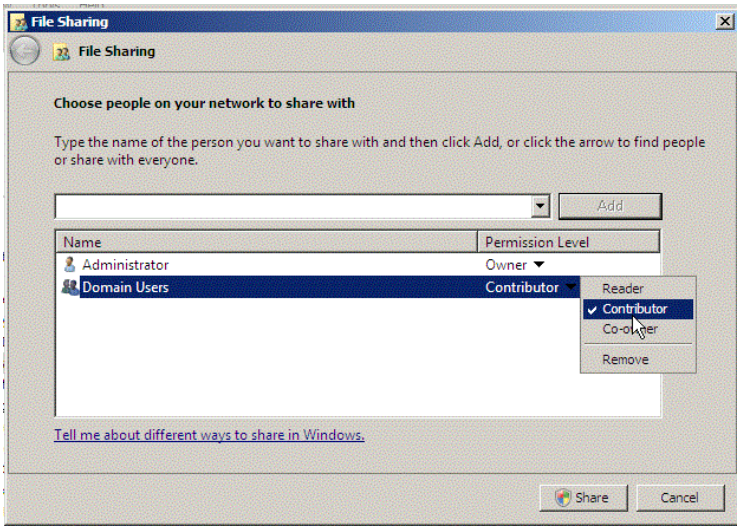
DC01 adalah file server yang harus dapat diakses oleh remote user setelah metode akses dan autentikasi dikonfigurasi.

Langkah-langkah membuat shared folder dan file.

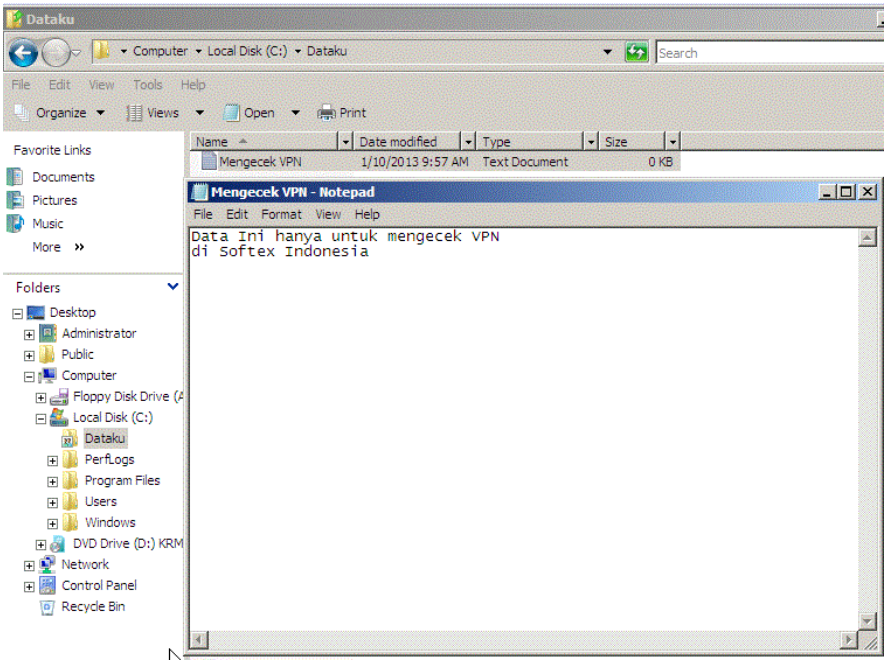
1. Pada DC01, klik Start, dan kemudian klik Computer.
2. Klik ganda Local Disk (C:).
3. Klik-kanan di dalam riang kosong dari windows explorer, pilih New, dan kemudian klik folder.
4. Beri nama foldernya : **Dataku.**
5. Klik kanan dari folder Dataku, dan kemudian klik Share.



6. Ketikan domain users, dan kemudian klik Add
7. Klik Domain Users, dan kemudian klik Contributor permission level.



8. Klik Share, dan kemudian klik Done.
9. Klik-ganda folder dataku, klik-kanan di ruang kosong dari folder, pilih new, dan kemudian klik Text Document.
10. Beri nama dokumen tersebut : MengecekVPN
11. Buka Mengecek VPN dan berikan beberapa kata teks.



12. Simpan dan tutup Mengecek VPN.

3.7.2 Konfigurasi Server VPN

VPN01 adalah komputer yang menggunakan Windows Server 2008 yang berperan sebagai berikut:

1. **Active Directory Certificate Services**, sebuah *certification authority (CA)* yang menerbitkan sertifikat komputer yang diperlukan untuk koneksi VPN berbasis SSTP.
2. **Certification Authority Web Enrollment**, sebuah service yang mengaktifkan penerbitan dari sertifikat melalui Web browser.
3. **Web Server (IIS)**, yang diinstal dan diperlukan sebagai service untuk *Certification Authority Web Enrollment*.
4. **Network Policy and Access Services**, yang diperlukan untuk menyediakan dukungan untuk koneksi VPN melalui Remote Access Service.

Konfigurasi VPN01 meliputi langkah-langkah berikut:

3.7.2.1 Instalasi Sisten Operasi

Instalasi Windows server 2008 pada VPN01:

1. Pada VPN01, menjalankan computer yang menggunakan Windows Server product disc
2. Ikuti intruksinya yang di layar, dan pada saat di minta untuk menggantikan password masukan **P@ssword**

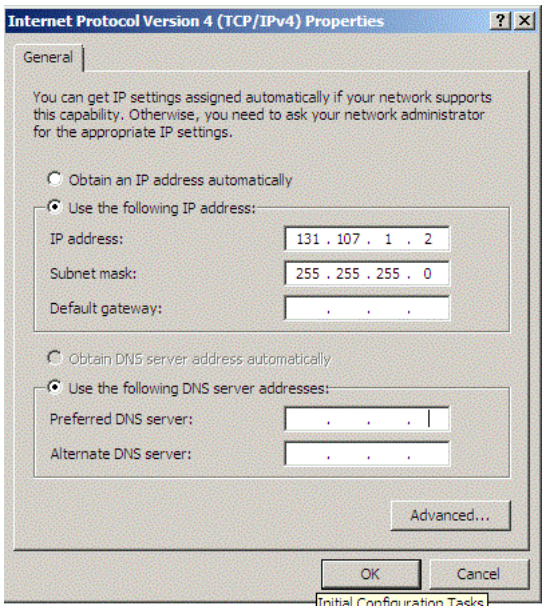
3.7.2.2 Konfigurasi TCP/IP Untuk Internet Dan Intranet Networks.

Langkah selanjutnya lakukan konfigurasi properti TCP/IP sedemikian sehingga VPN01 memiliki IP address 131.107.1.2 untuk public (Internet) connection dan 192.168.1.2 untuk private (intranet) connection.

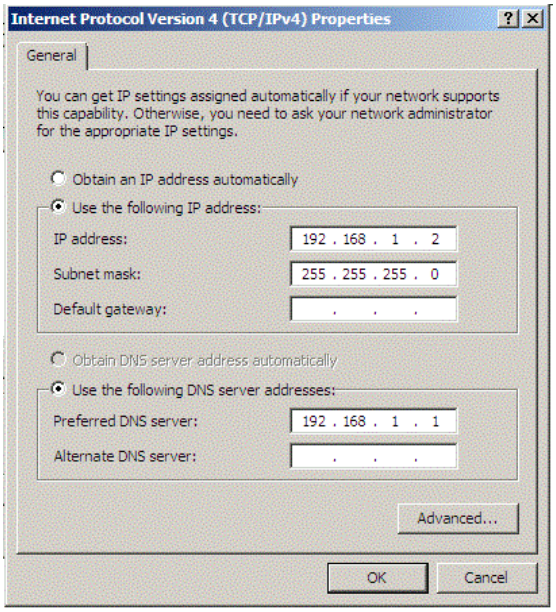
Tahanpan mengkonfigurasi property dari TCP/IP:

1. Pada VPN01, pada window **Initial Configuration Tasks**, pada bagian **Provide Computer Information**, klik **Configure networking**.

   Catatan : Jika window **Initial Configuration Tasks** belum terbuka, kita dapat membukanya dengan cara klik **Start**, klik **Run**, dan ketikkan oobe dan klik **OK**.
2. Pada Windows Network Connections, klik-kanan **Local Area Connection,** dan kemudian klik **Properties**
3. Pada tab **Networking,** klik Internet Protocol Version 4 (TCP/IPv4), dan kemudian klik Properties
4. Klik Use the folloing IP address.
5. Lakukan Konfigurasi IP address dan subnet mask dengan nilai-nilai berikut
   - Pada interface yang terkoneksi ke public (internet) Network, ketikan 131.107.1.2 untuk Ip address, dan ketikan 255.255.255.0 untuk subnet mask.



- Pada interface yang terkoneksi ke private (intranet) network, ketikan 192.168.1.2 untuk Ip address, ketikan 255.255.255.0 untuk subnet mask, dan ketikan 192.168.1.1 untuk preferren DNS server.



6. Klik OK. Dan kemudian close.
7. Untuk mengganti nama dari network connection, klik-kanan dari network connection yang ingin diganti namanya, dan kemudian klik Rename.

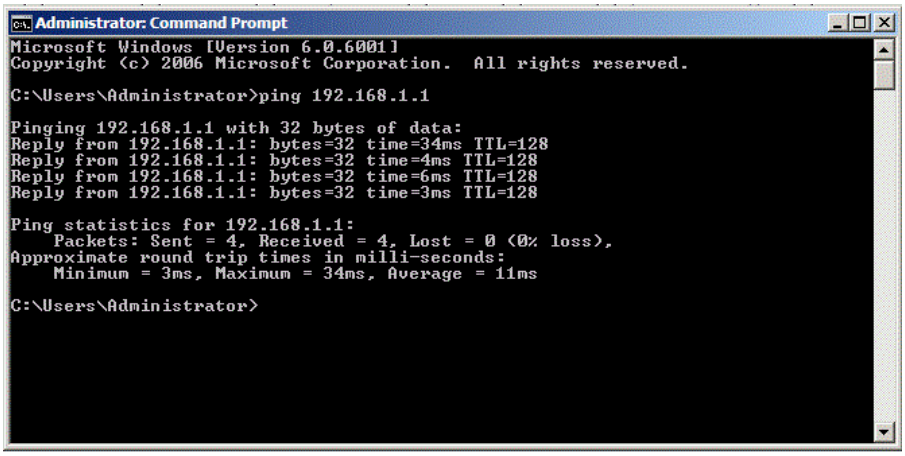
8. Lakukan konfigurasi penggantian nama network connection dengan nama-nama berikut:
    - Pada interface yeng terkoneksi ke public (internet) network, ketikan Public
    - Pada interface yeng terkoneksi ke private (intranet) network, ketikan Private
9. Tutup window Network Connectios.

Jalankan perintah ping dari VPN01 untuk memeriksa komunikasi jaringan antara VPN01 dengan DC01

3.7.2.3 Memeriksa Koneksivitas Jaringan

Gunakan perintah ping untuk memeriksa koneksifitas jaringan dengan langka-langkah berikut :

1. Pada VPN01, klik strart, klik Run, pada kotak Open, ketikan cmd, dan kemudian klik Ok. Pada windows command, ketikan ping 192.168.1.1



2. Hasilnya dapat dilihat di bawah ini hubungan antara VPN01 dengan DC01.
3. Tutup windows command.

3.7.2.4 Gabungkan ke domain *softexindonesia.com*

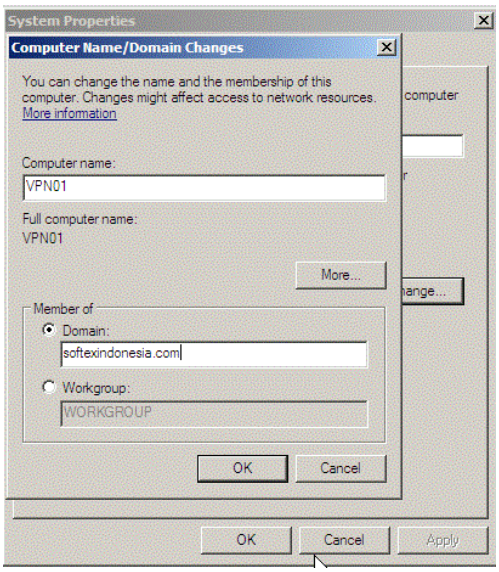
Konfigurasi VPN01 untuk menjadi member server di domain

softexindonesia.com.

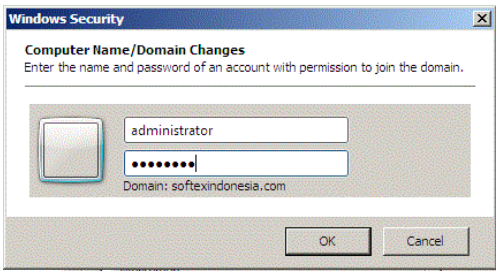
Berikut adalah langkah-langkah yang dilakukan untuk menggabungkan untukVPN01 ke domain *softexindonesia.com*

1. Pada VPN01, pada windows initial configuration tasks, pada bagian Provide Computer Information, klik Provide computer name and doamain.
2. Pada kotak dialog system Properties, pada tab Computer Name, klik Change.

3. Pada Computer name, berisikan text dan ketikan VPN01.
4. Pada Member of, klik domain, dan ketikan *softexindonesia.com*, dan kemudian klik Ok.



5. Masukan Administrator untuk name dan P@ssword untuk password



6. Dan pada saat melihat dialog "welcoming". Ke domain

softexindonesia.com, klik Ok.



7. Setelah itu ada pemberitahuan bahwa kita harus merestart computer, klik OK, klik Close, dan kemudian klik Restart Now.



3.7.2.5 Instalasi Active Directory Certificate Services dan Web Server (IIS) Server Roles.

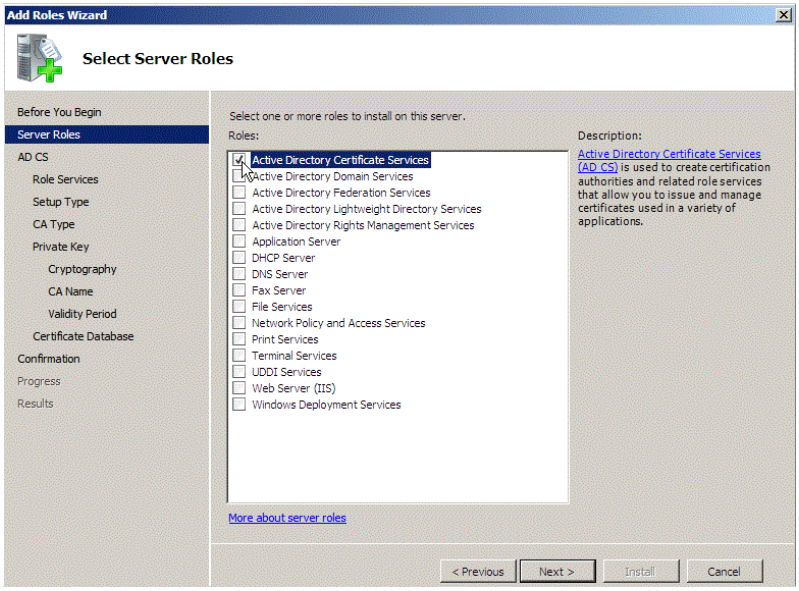
Untuk mendukung koneksi VPN yang menggunakan SSTP, langkah pertama adalah dengan menginstal Active Directory Certificate Service dan Web Server (ISS) untuk mengaktifkan Web enrollment untuk sertifikat komputer.

Langkah-langkah yang harus dilakukan adalah:

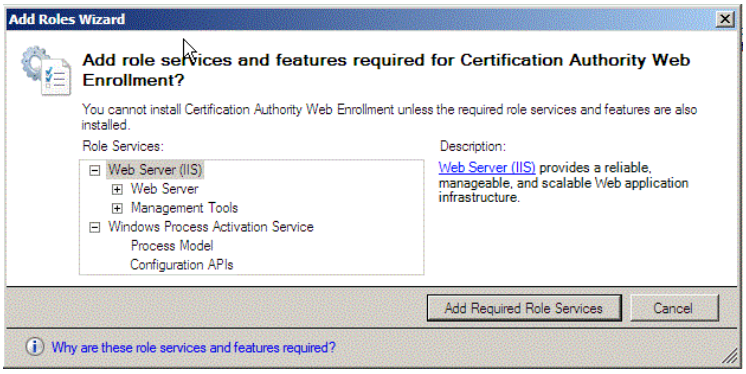
1. Pada VPN01, log on sebagai administrator@softexindonesia,com dengan

password P@ssword.

2. Pada window Intial Configuration Task, di bagian Costumize This Server, klik Add Roles. (bisa membuka window initial configuration dengan polih start → run dan tulis oobe.
3. Pada kotak dialog Add Roles Wizard, pada Before you begin, klik next.
4. Pilih kotak cek **Active Directory Certificate Services.**

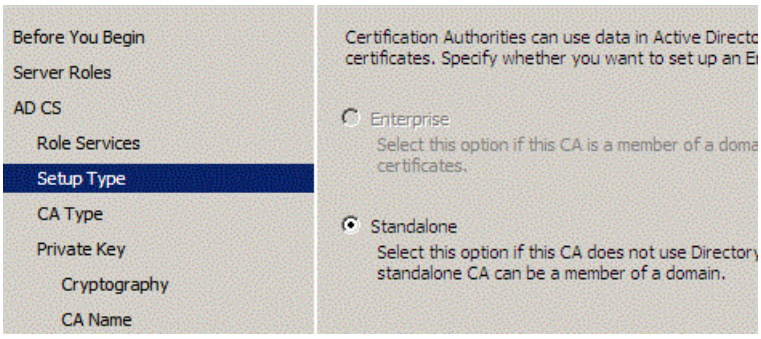


5. Klik next, dan klik next lagi.
6. Pada kotak dialog Reles services, pada bagian Rore Services, pilih kotak cek Certificate Authority Web Enrollment.
7. Pada kotak dialog Add Wizard, klik Add Required Role Services.

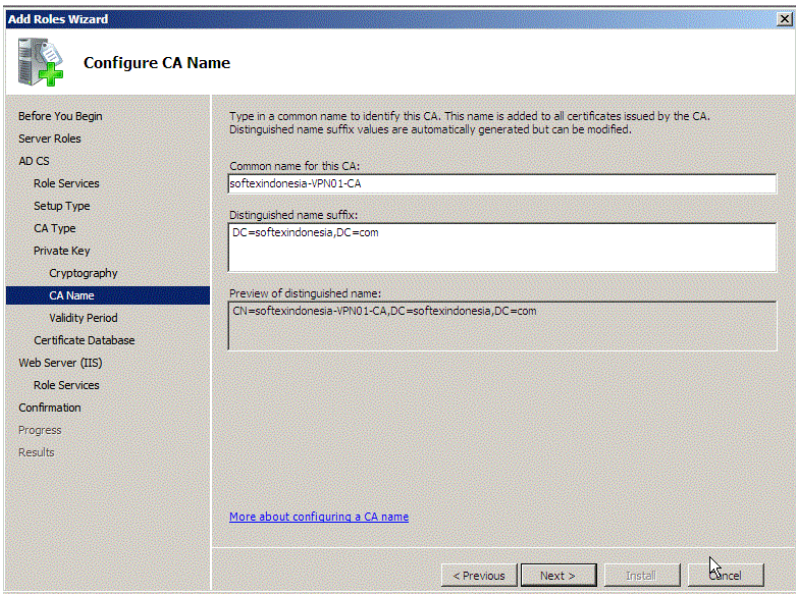


8. Klik Next.

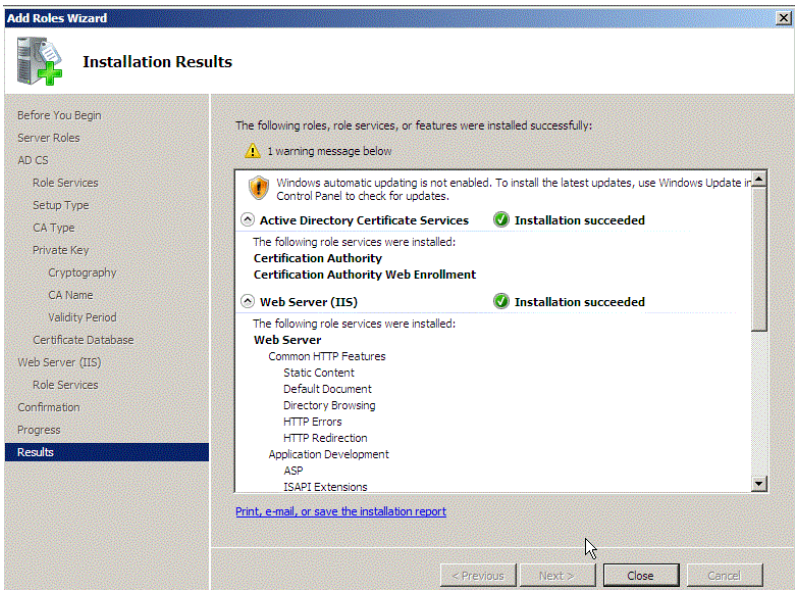
9. Klik Standalone, dan kemudian klik Next.



10. Klik Root CA (recommended), dan klik Next.
11. Klik create a new private key, dan kemudian klik Next.
12. Klik Next untuk menerima setting dari default cryptographic.
13. Pada kotak dialog Configure CA name, klik **Next** untuk menerima default dari CA.



14. Klik Next terus untuk menerima setting default.
15. Pada kotak dialog Confirm Instalation Selections, klik install. Proses Instalasinya akan memakan waktu beberapa menit.
16. Pada kotak dialog Instalation Results, klik Close.

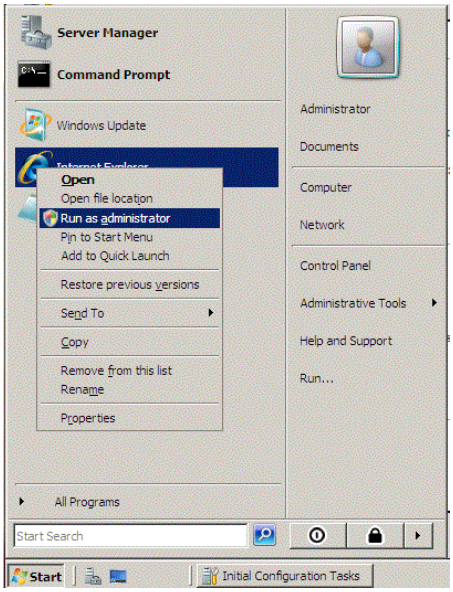


3.7.2.6 Membuat dan menginstalasi sertifikat Server Authentication.

Sertifikat Server Authentication digunakan oleh Clien01 untuk mengautentikaso VPN01. Sebelum instalasi sertifikat, kita harus mengkonfigurasi Internet Eksplore untuk mengizinkan publikasi sertifikat (sertificate publishing).

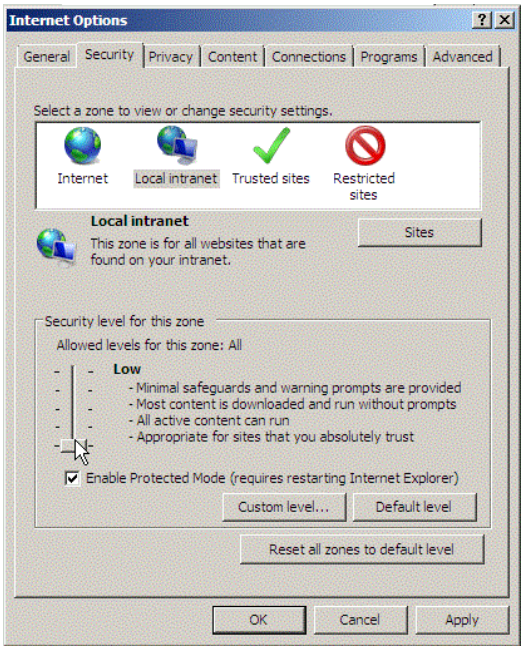
Berikut adalah langkah konfigurasi Internet Explorer:

1. Pada VPN01, klik Start, klik-kanan Internet Eksplorer, dan kemudian klik Run as Administrator



2. Jika muncul suatu Phishing Filter alert, klik turn off automatic Phishing Filter, dan kemudian Klik OK.
3. Klik menu Tools, dan kemudian klik Internet Options.
4. Pada ktak dialog Internet Options, klik tab Security.
5. Pada bagian select a zone to view or change security setting, klik local intranet.
6. Ubah level dari Security level untuk Local Intranet dari Medium-low ke low, dan kemudian klik OK.

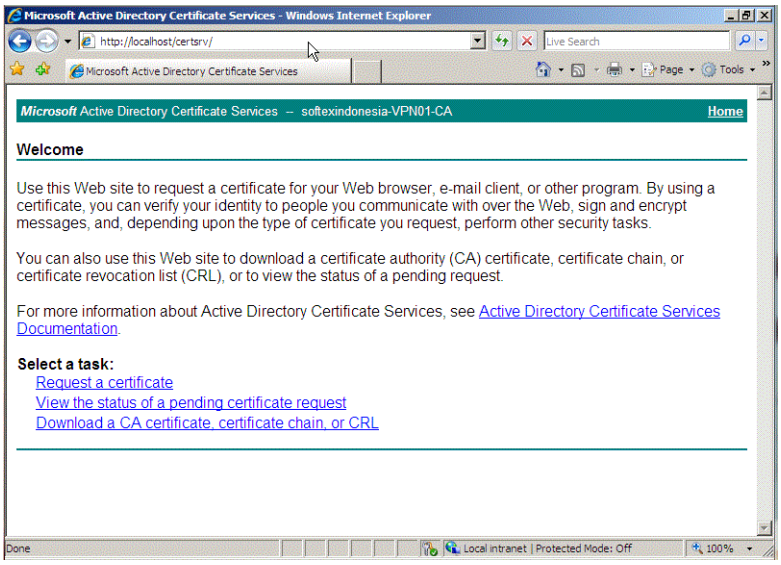
   Catatan : Pada Skenario Production, kita harus konfigurasi setting ActiveX control dengan menggunakan Costum level dan bukan dengan cara menurunkan Securuty level-nya.



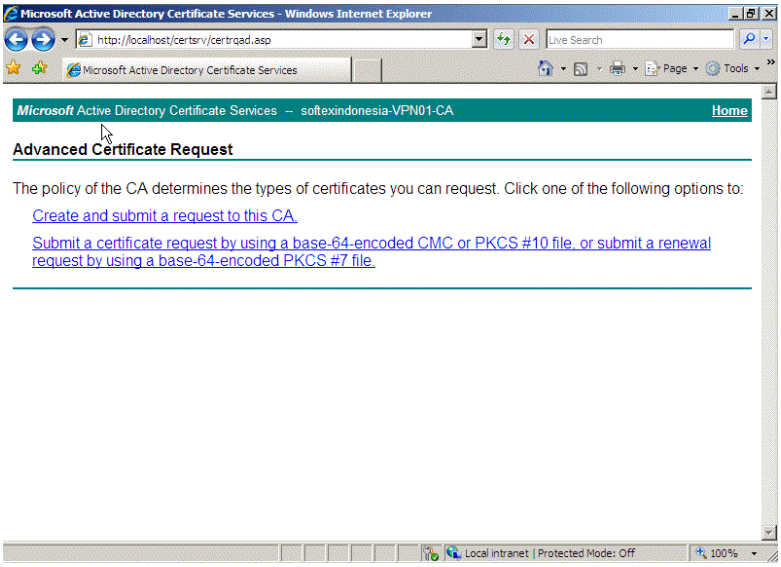
Gunakan Internet Explorer untuk memperoleh sertifikat Server Authentication.

Langkahnya adalah sebagai berikut :

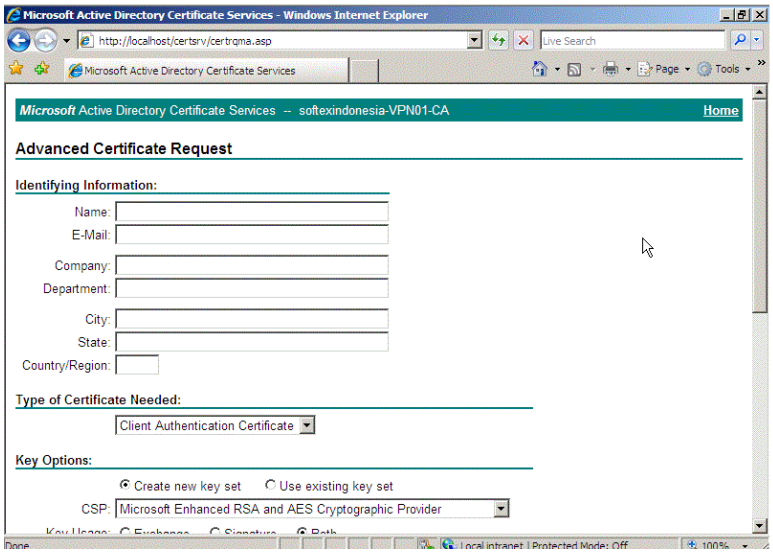
1. Pada VPN01, pada bar Internet Explorer Address, ketikan http://localhost/cerrtsrv, dan kemudian tekan enter.



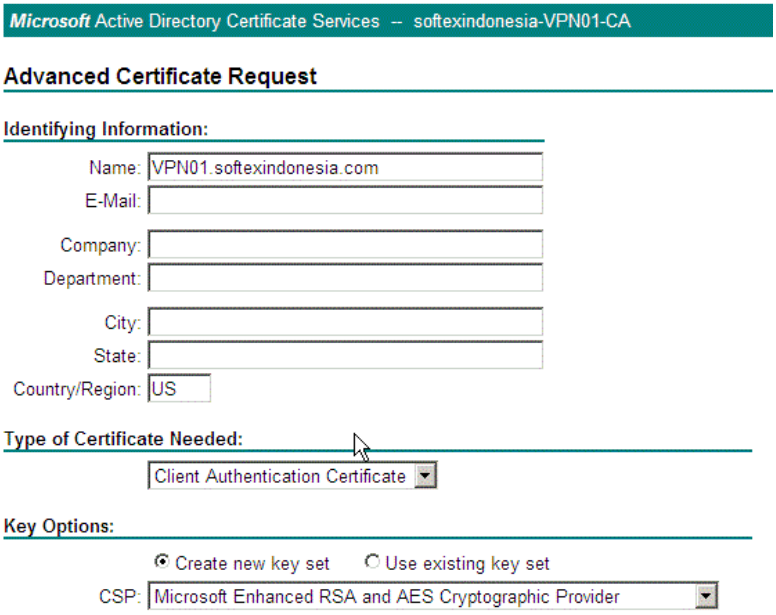
2. Pada bagian select a task, klik request a certificate.
3. Pada bagian request a certificate, klik advanced certificate request.
4. Pada bagian Advanced certificate request, klik create and submit a request to this CA.



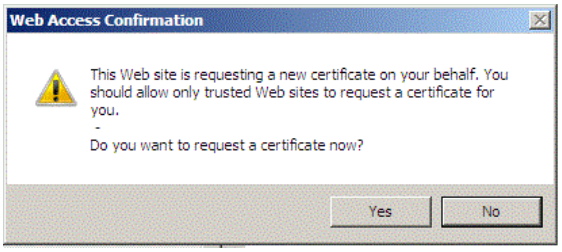
5. Klik Yes untuk mengizinkan ActiveX control.



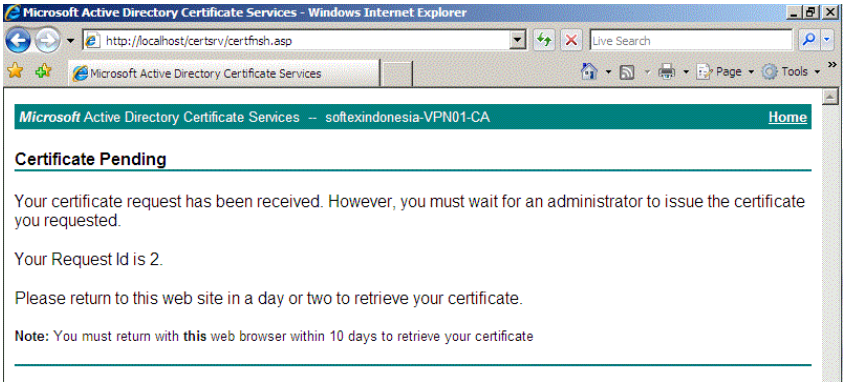
6. Pada bagian Identifying Information, pada bagian Name, ketikan VPN01.softexindonesia.com, dan pada Country/Region ketikan US.
7. Pada bagian Type of Certificate Needed, pilih Server Authentication Certificate.
8. Pada bagiankey Options, pilih kotak cek Mark keys as exportable, dan kemudian klik Submit.



9. Klik Yes pada kotak dialog konfirmasi.

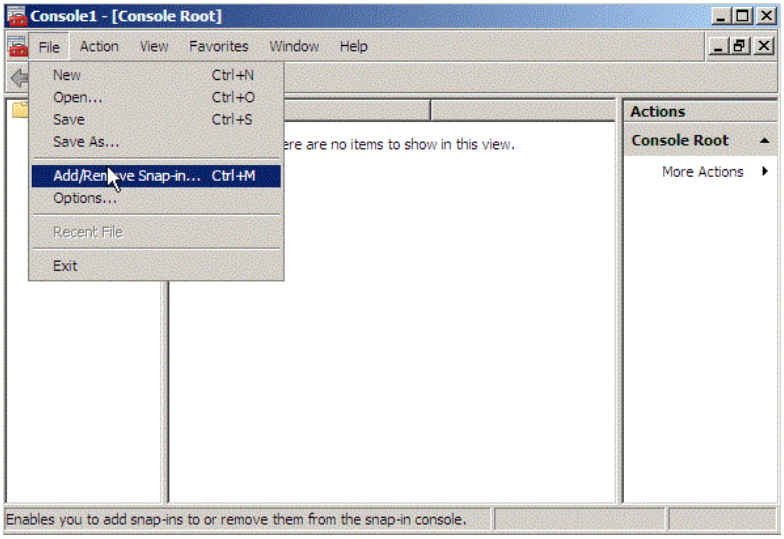


Sertificate Server Authentication sekarang berstatus tunda (pending). Sertifikat ini harus di terbitkan sebelum diinstal.

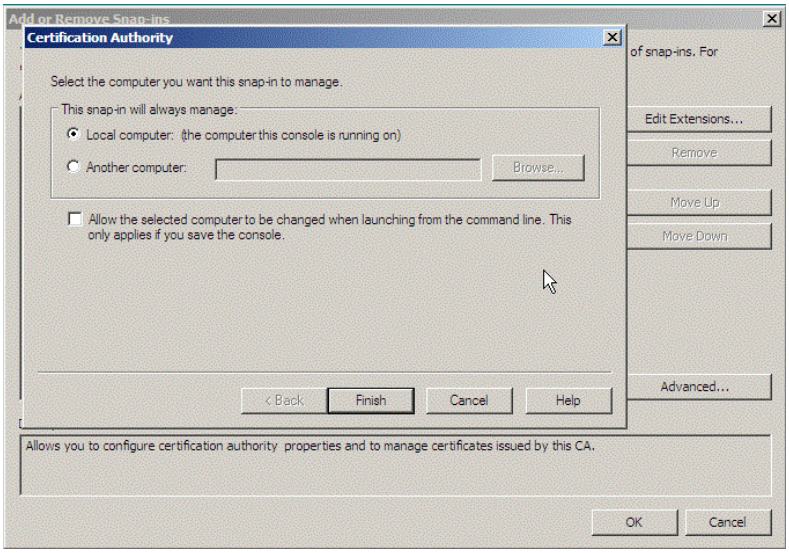


Step-step penerbitan dan Instalasi sertifikat Server Authentication

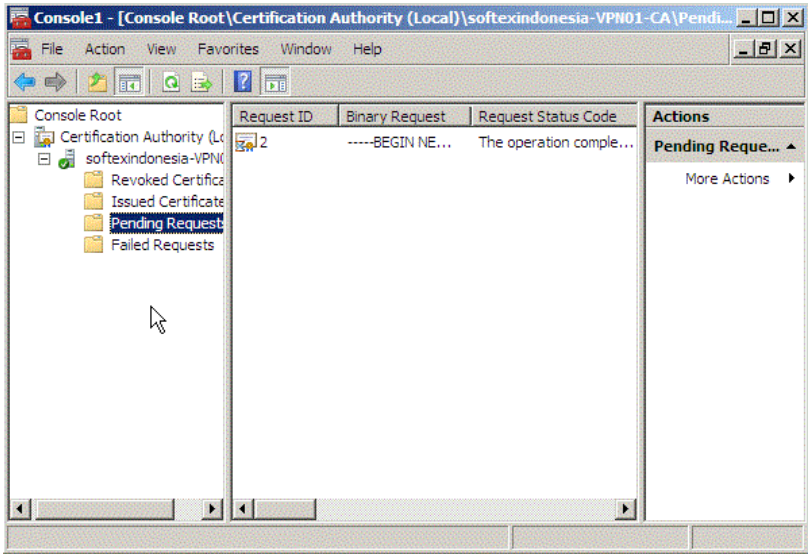
1. Pada VPN01, klik Start, dan kemudian Run.
2. Pada Open, ketikan mmc, dan kemudian klik Ok.
3. Pada Console snap-in, klik File, dan kemudian klik Add/Remove Snap-in.



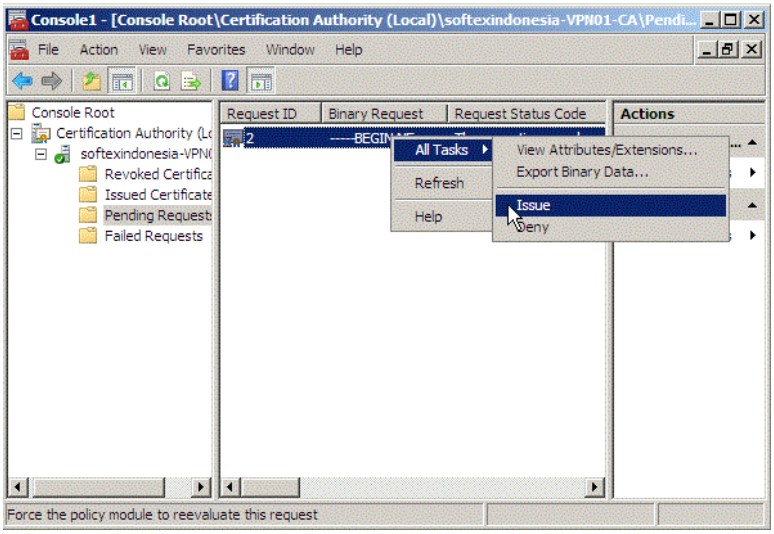
4. Bagian available snap-in, klik Certification Authority, dan kemudian klik Add.
5. Klik Finish untuk menerima setting default dari Local Computer.



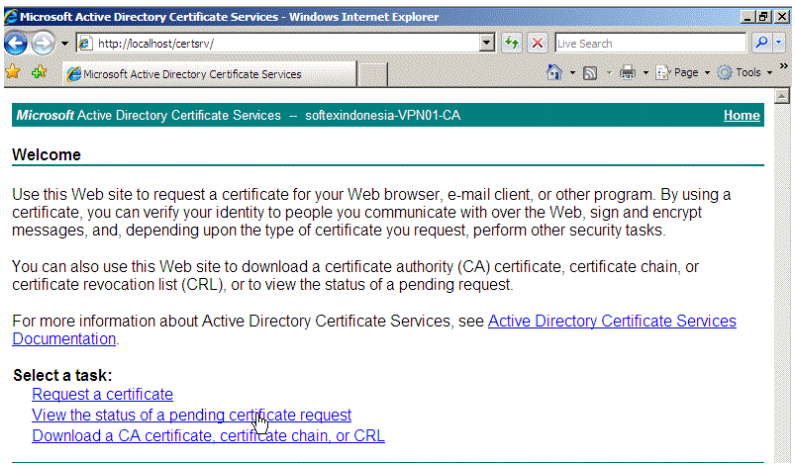
6. Klik Ok untuk menutup kotak dialog Add or Remove Snap-ins.
7. Pada MMC console yang baru saja terbentuk, di bagian kirinya, klik-ganda Certification Authority (Local).
8. Klik-ganda softexindonesia-VPN01-CA, dan kemudian klik Pending Requests.



9. Pada bagian panel tengah, klik-kanan *pending request*, pilih All Tasks, dan kemudian klik Issue.

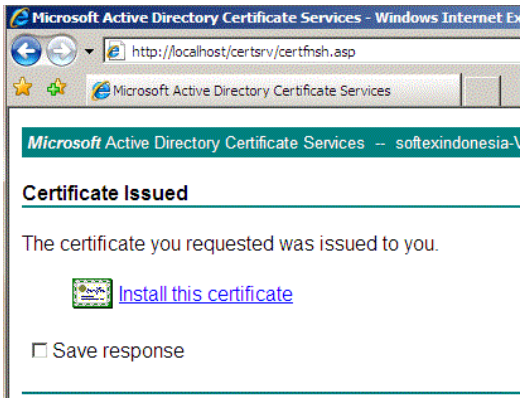


10. Pada bagian Internet Explorer, pada halaman Cercitificate, Pending, klik Home, jika halaman ini tidak terlihat, lakukan browsing ke http://localhost/certsv
11. Pada bagian Select atask, klik Viev the status of a pending cercitificate request.
12. Pada bagian View the Status of a Pending Certificate Request, pilih sertifikat yang baru saja diterbitkan

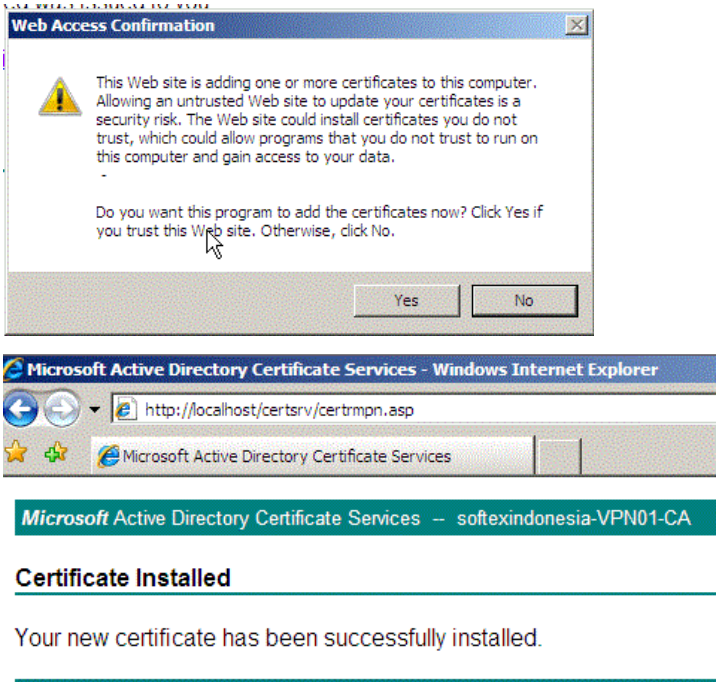


13. Klik Yes untuk mengizinkan ActiveX control

14. Pada bagian Cercitificate Issue, klik Instal this cercificate.

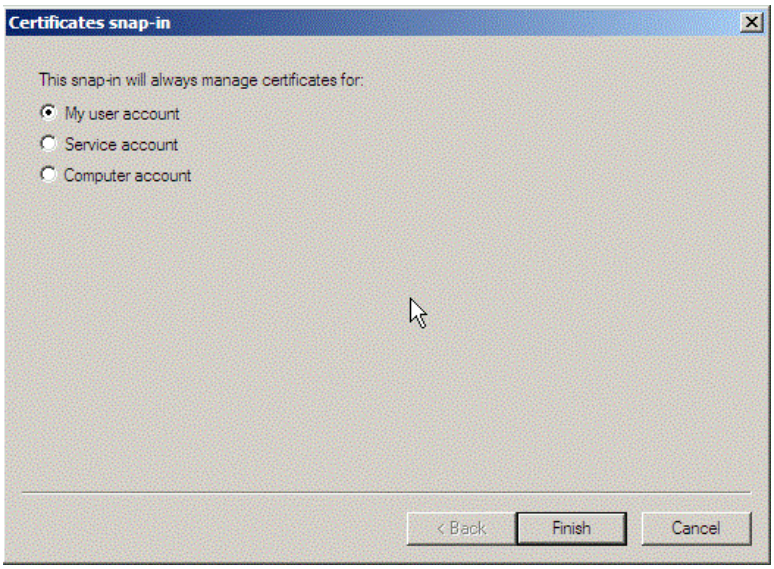


15. Klik Yes pada kotak dialog konfirmasi.

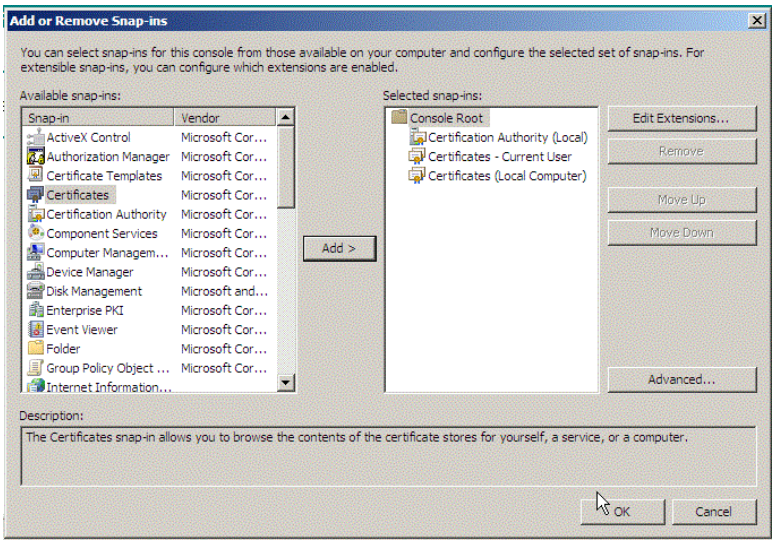


Memindahkan sertificate yang terinstal dari lokasi penyimpanan default.

1. Pada VPN01, pada MMC console yang dibuat sebelumnya klik file, dan kemudan klik Add/remove Snap-in.
2. Pada bagian Available snap-ins, klik Certificate dan kemudian klik Add.

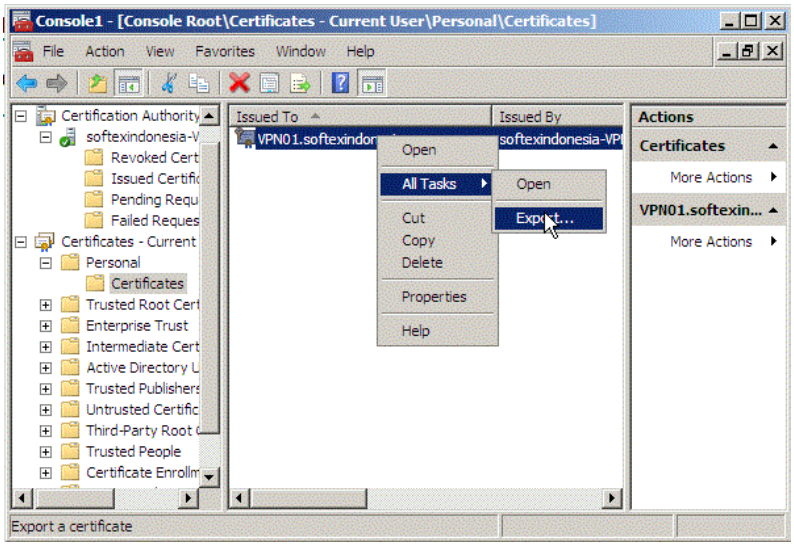


3. Klik Finish untuk menerima setting default dari My User Acount.
4. Klik Add, klik Computer Acount, dan kemudian klik Next.
5. Pada kotak dialog select computer, klik Finish untuk menerima seting default dari Local Computer.



6. Klik OK untuk menutup kotak dialog Add or Remove Snap-isd.
7. Kemudian klik-ganda Certificates – Current User, klik-ganda Personal, dan kemudian klik Certificates.
8. Pada bagian tengah, klik-kanan sertifikat VPN01.softexindonesia.com,

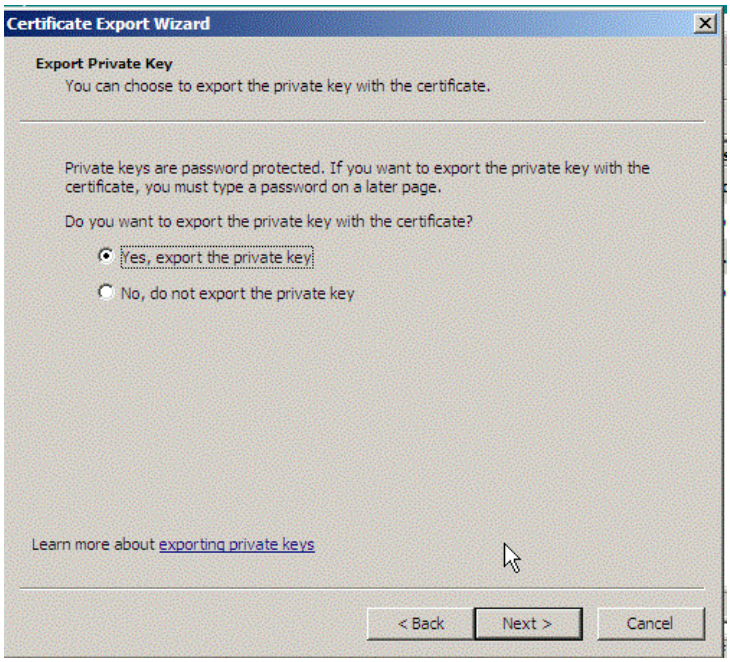
pilih All Tasks, dan kemudian klik Export.



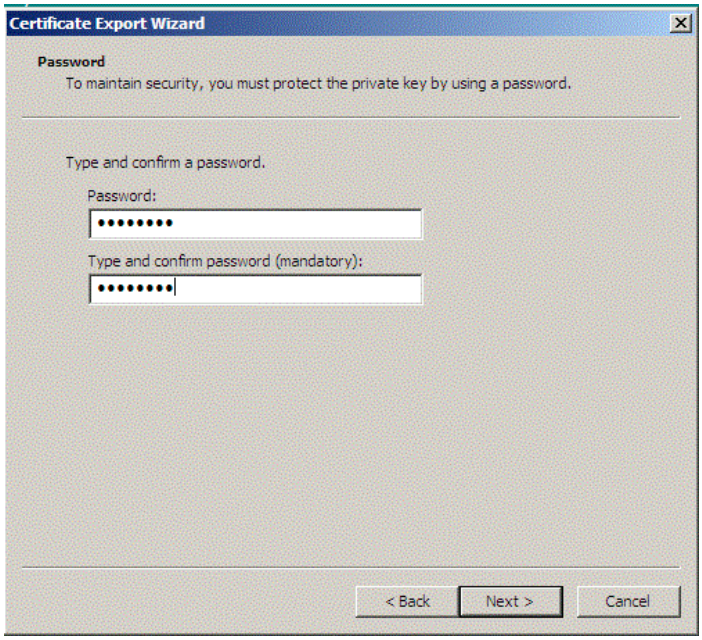
9. Pada halaman Welcome klik Next.



10. Klik Yes, export the private key, dan kemudian klik Next.

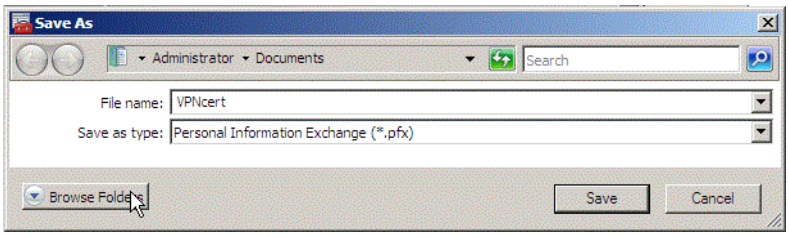


11. Klik Next untuk meneriman format file default.
12. Ketikan P@ssword di kedua kotak text, dan kemudian klik Next.

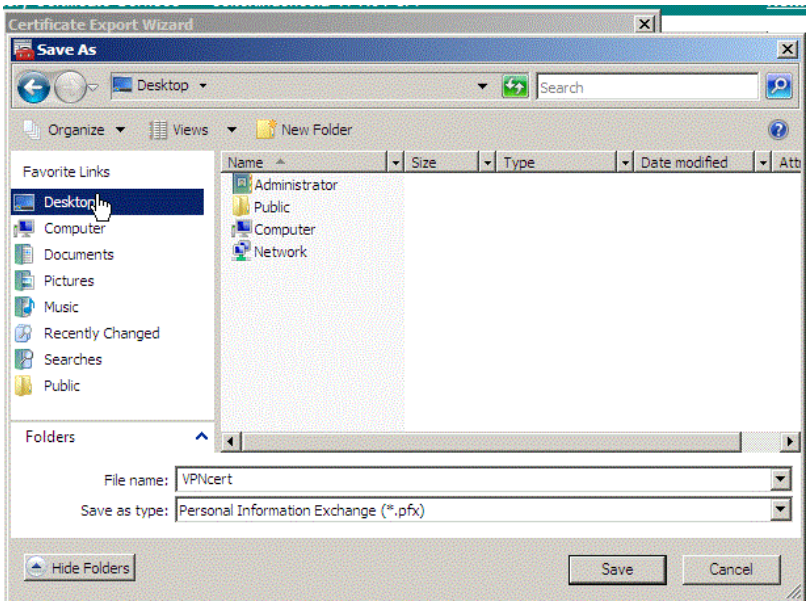


13. Pada halaman File to Export, klik Browse.
14. Pada kotak text file name, ketikan VPN01cert, dan kemudian klik Browse

Folder.

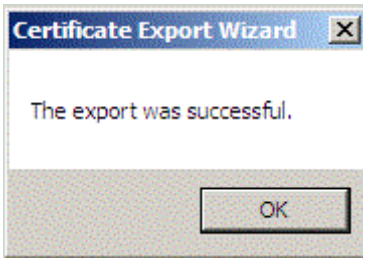


15. Pada bagian Faforite Links, klik Desktop, dan kemudian klik Save untuk menyimpan sertifikat tersebut ke Desktop.

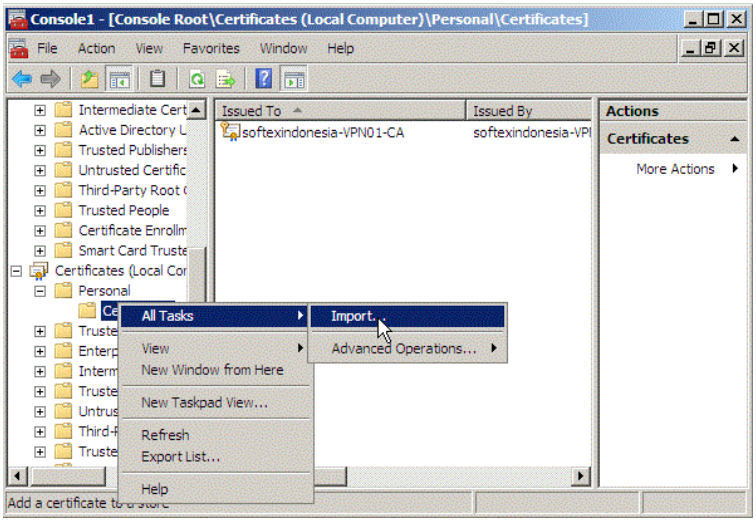


16. Pada halaman File to export, klik Next.
17. Klik Finish untuk menutup Certificate Export Wizard, dan kemudian klik OK pada kotak dialog konfirmasi.

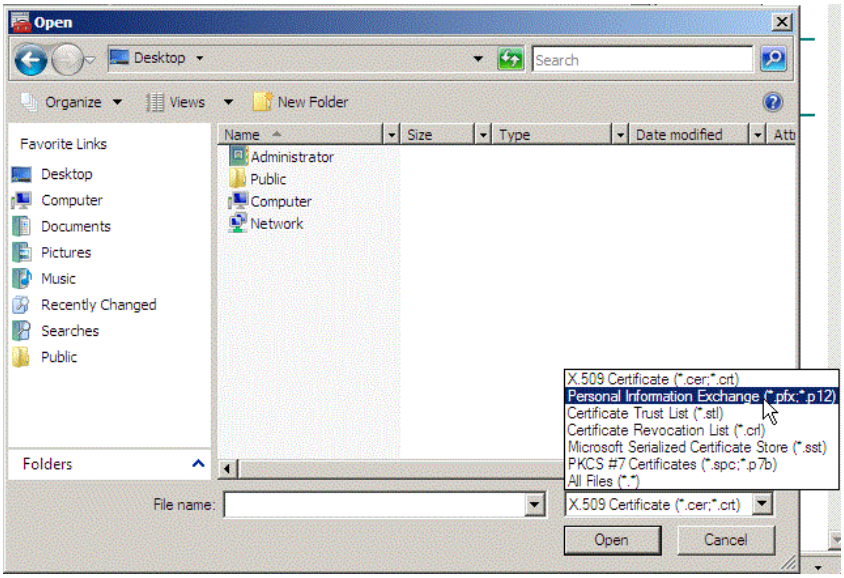




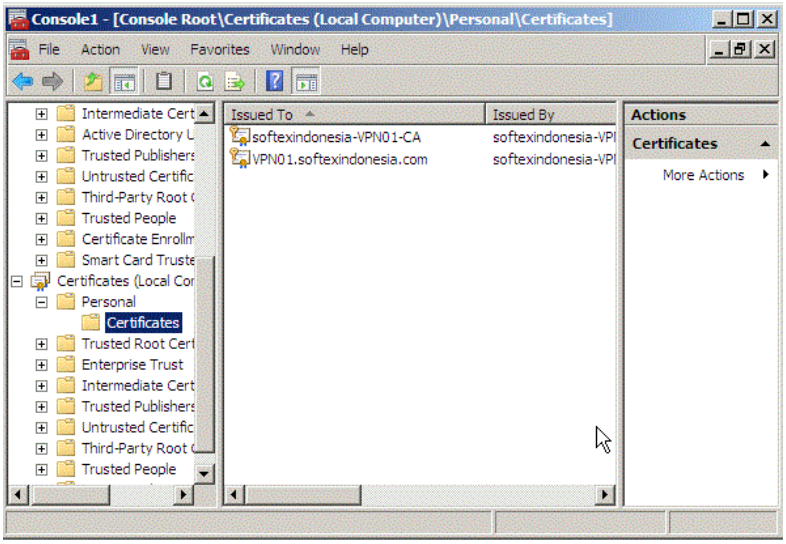
18. Kemudian klik-ganda Certificates (Local Computer), dan kemudian klik-ganda Personal.
19. Klik Certificates, dan kemudian klik-kanan Certificates, pilih All Tasks, dan kemudian klik Import.



20. Pada halaman welcome, klik Next.
21. Pada halaman Import, klik Browse.
22. Pada bagian Faforite Links, klik Desktop, dan pada *drop-down list,* pilih Personal Imformation Exchange untuk tipe filenya.



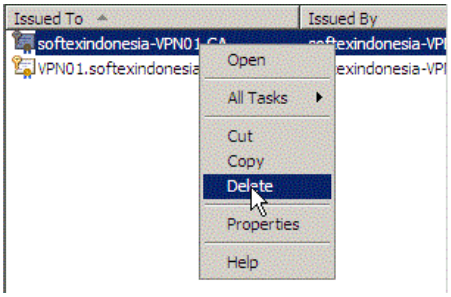
23. Kemudian klik-ganda VPN01cert.
24. Pada halaman File to import, klik Next.
25. Pada kotak text Password, ketikan P@ssword, dan kemudiann klik Next.
26. Pada halaman Certificate Store, klik Next untuk menerima lokasi Personal Store.
27. Klik Finish untuk menutup Certificate Import Wizard, dan kemudian nklik OK pada kotak dialog Konfirmasi.



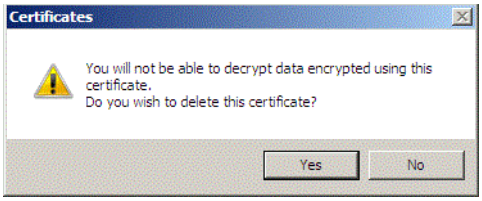
Catatan: jika procedure dalam laporan ini tidak diikuti dalam urutan yang disajikan, keberadaan sertificate tujuan semua (softexindonesia-VPN01-CA) dapat menimbulkan masalah, Hapus sertificate softexindonesia-VPN01-CA di Local Computer Store untuk memastikan **SSTP Linier** mengikat ke server authentication certificate (VPN01.softexindonesia.com)

Berikut langkah untuk menghapus sertificate

1. Klik-ganda Certificates, klik-kanan softexindonesia-VPN01-CA, dan kemudian klik Delete.



2. Klik yes pada kotak dialog Konfirmasi.

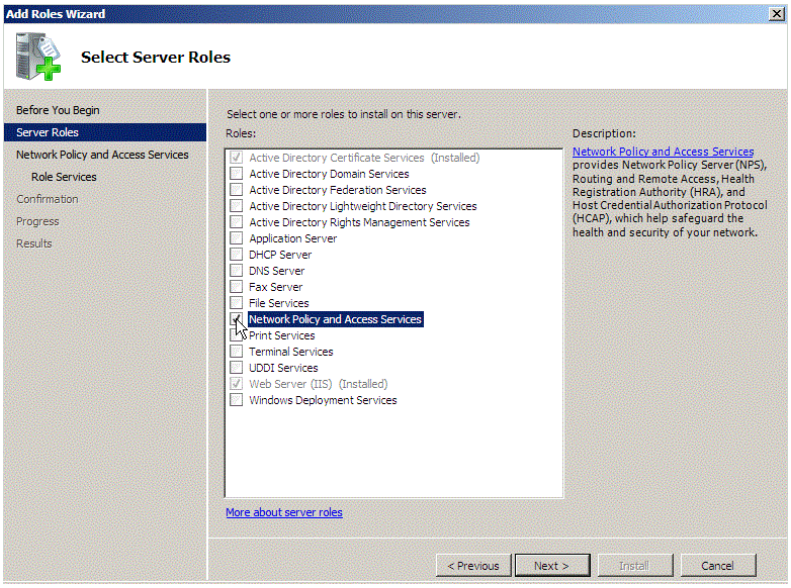


3.7.2.7 Instalasi Network Policy and Access Services (Routing and Remote Access) Server Role.

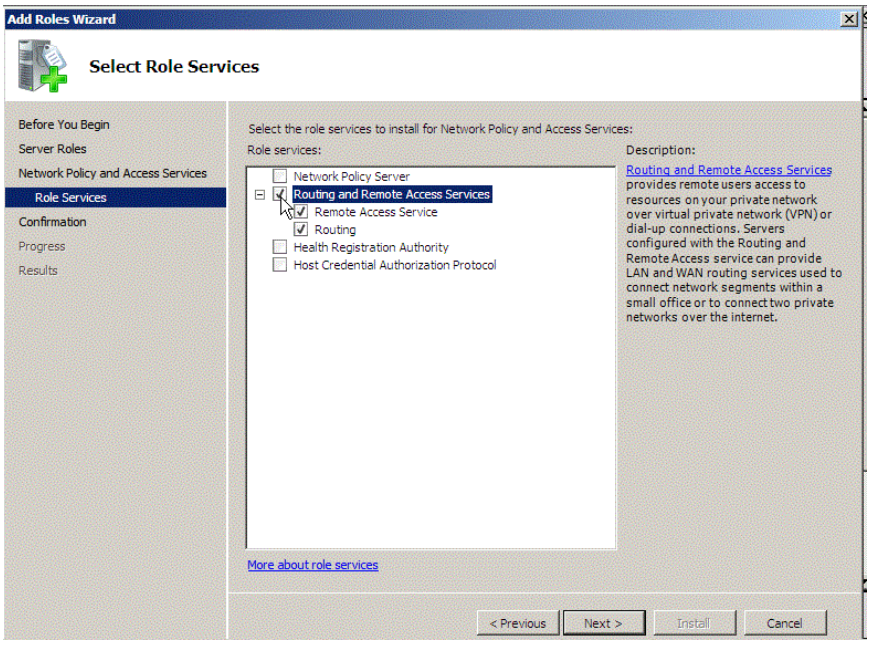
Konfigurasi VPN01 dengan Routing and Remote Access agar berfungsi sebagai VPN server.

Langkah Instalasi VPN dan certificate services Roles

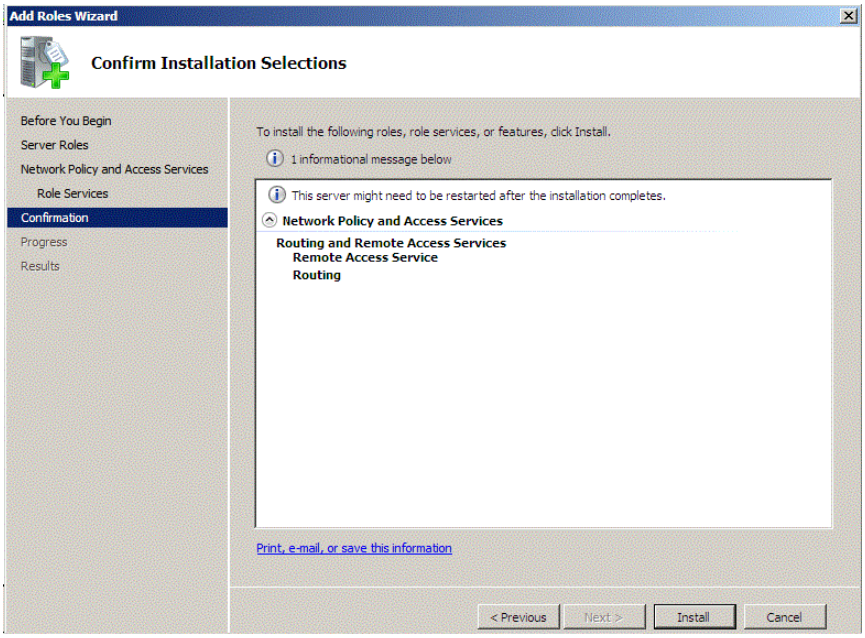
1. Pada VPN01, pada windows Initial Configuration Task, pada bagian Costumize This Server, klik Add Roles.
2. Pada kotak dialog Roles Wizard, pada bagian Before You Begin, klik Next.
3. Pilih kotak cek Network Policy and Access Services, klik Next, dan kemudian klik Next lagi.



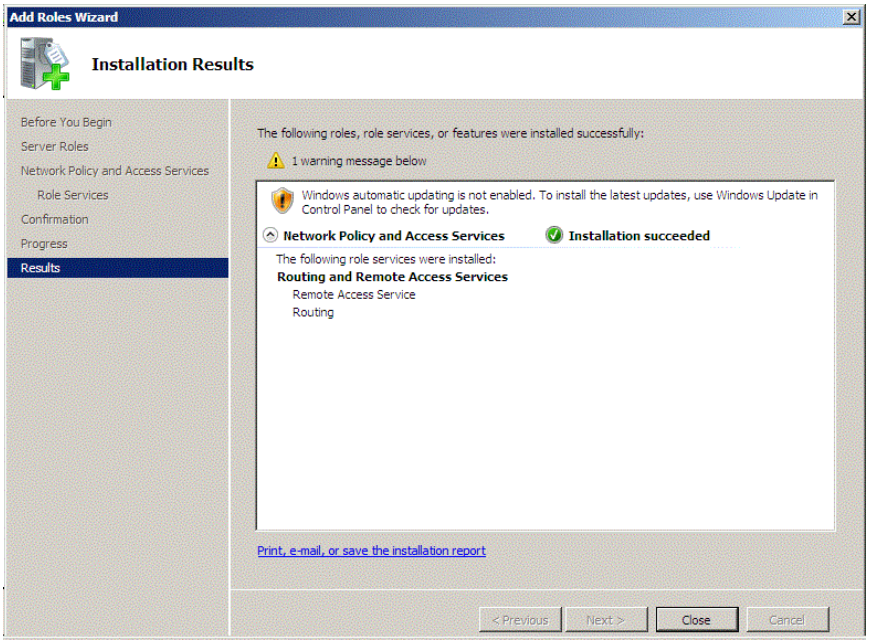
4. Pada kotak dialog Select Role Services, pada bagian Role services, pilih kotak cek Routing and Remote Access Services.



5. Klik Next, dan kemudian klik Instal.



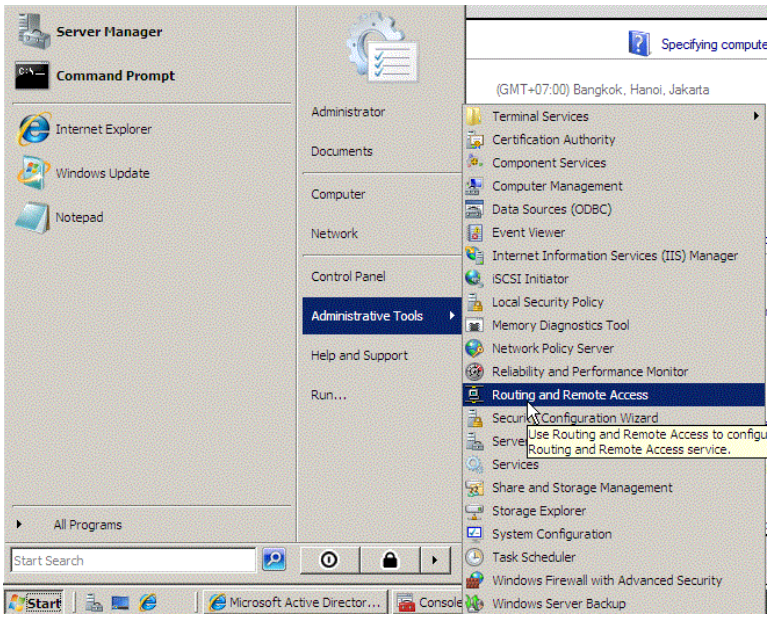
6. Pada kotak dialog Instalation Resuls, klik Close.



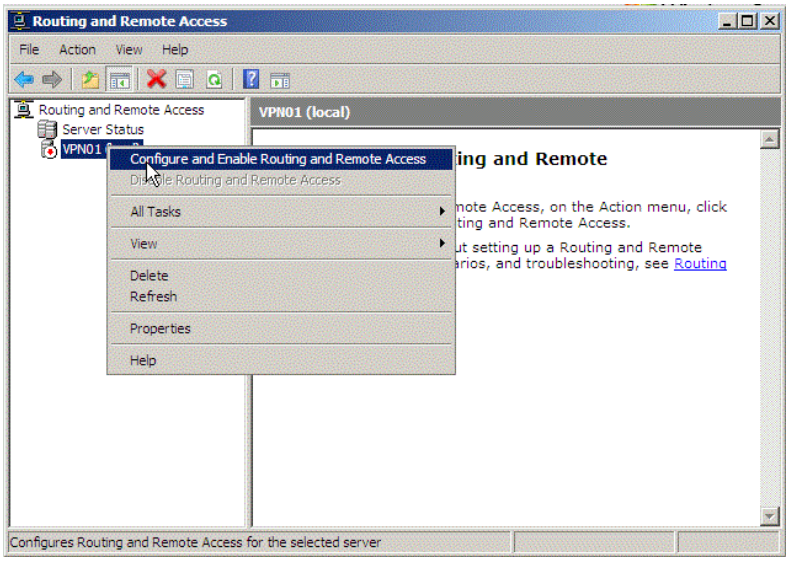
3.7.2.8 Konfigurasi VPN01 sebagai VPN server

Konfigurasi VPN01 sebagai VPN Server yang menyediakan Remote Access untuk Cliebt VPN.

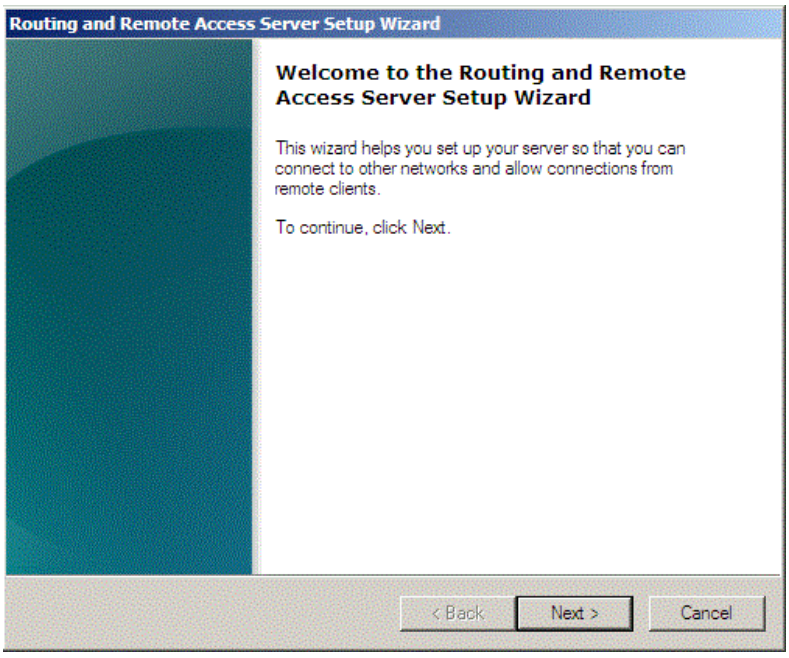
1. Pada VPN01, klik Start, pilih Administrative Tools, dan kemudian klik Routing and Remote Access.



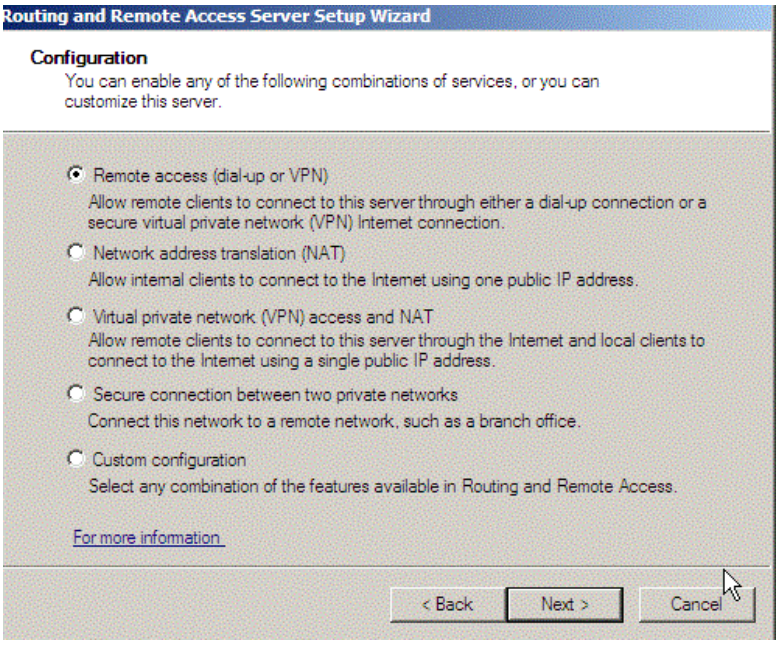
2. Pada Routing and Remote Access, klik kanan VPN01, dan kemudian klik Configure and Enable Routing and Remote Access.



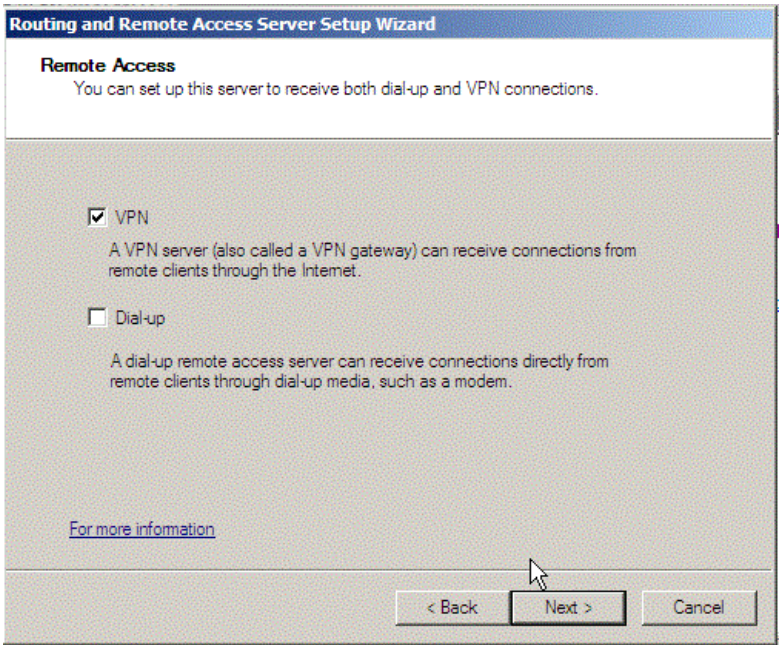
3. Pada halaman Welcome to the Routing and Remote Access Servver Setup Wizarrd, klik Next.



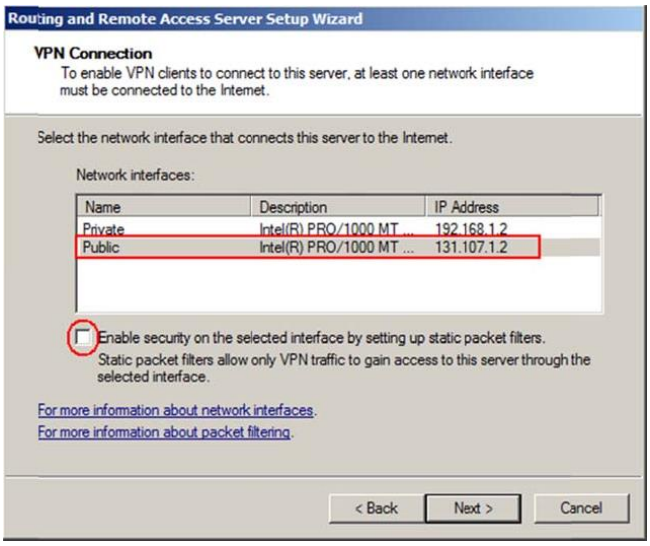
4. Pada halaman Configuration, klik Next untuk menerima seting default dari Remote Access (dial-up or VPN)



5. Pada halaman Remote Access, klik VPN, dan kemudian klik Next.

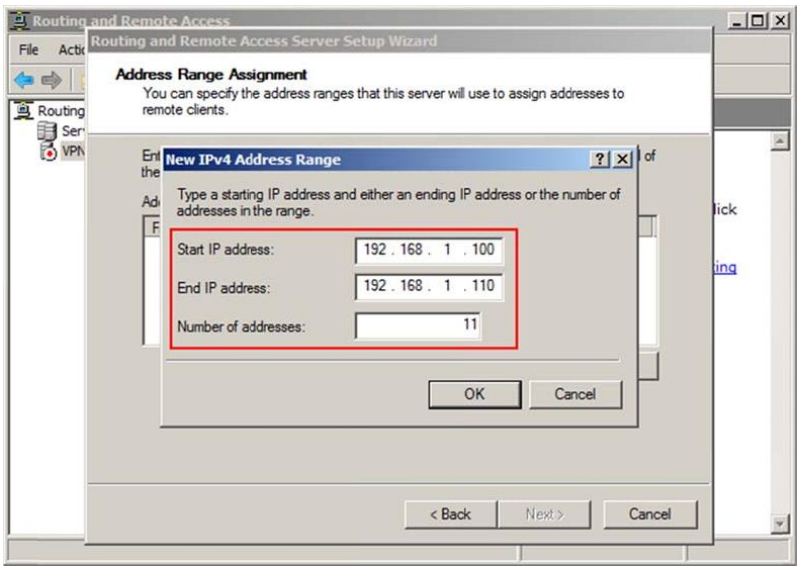


6. Pada hlaman VPN Connection, pada bagian Network Interfacesm kli Public. Interface ini yang akan melakukan koneksi VPN01 ke Internet.
7. Klik Enable Securuy ann the selected Interface by setting up static packet filters untuk membersihkan setingan ini, dan kemudian klik Next.



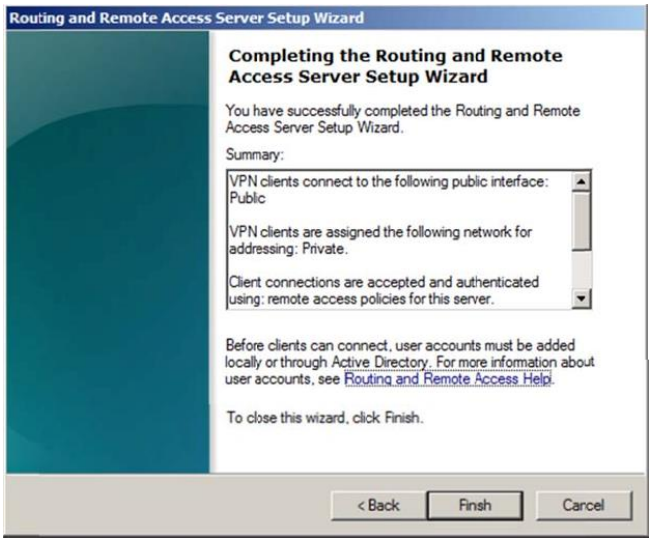
Catatan : untuk kondisi Normal, seting keamanan untuk pilihan Enable security on the selected interface by setting up static dibiarkan aktif pada public interface.

8. Klik From a specifired range af addresses, and then klik Next.
9. Klik New, ketikan 192.168.1.100 untuk IP address, ketikan 192.168.1.110 untuk IP address, klik OK, dan kemudian klik Next.



10. Klik Next untuk menerima seting default, yang artinya VPN01 tidak menggunakan RADIUS server, pada scenario ini, Routing and Remote Access Server akan menggunakan Windows Authentication

11. Pada halaman Completing the Routing and Remote Access Server Setup Wizard, klik Finish.



12. Jika kotak dialog yang menggambarkan kebutuhan untuk menambahkan computer ini ke dalam daftar remote Access Server muncul, klik Ok.
13. Pada kotak dialog yang menggambarkan kebutuhan untuk mengkonfogurasi DHCP Relay Agent, klik Ok.
14. Tutup Snap-in Routing and Remote Access.

3.7.3 Konfigurasi Client VPN

CLIENT01 adalah computer yang menggunakan Windows 7 yang berfungsi sebagai remote access VPN client untuk domain softexindonesia.com.

Konfigurasi CLIENT01 meliputi langkah-langkah berikut:

- Instalasi sistem operasi.
- Konfigurasi TCP/IP.

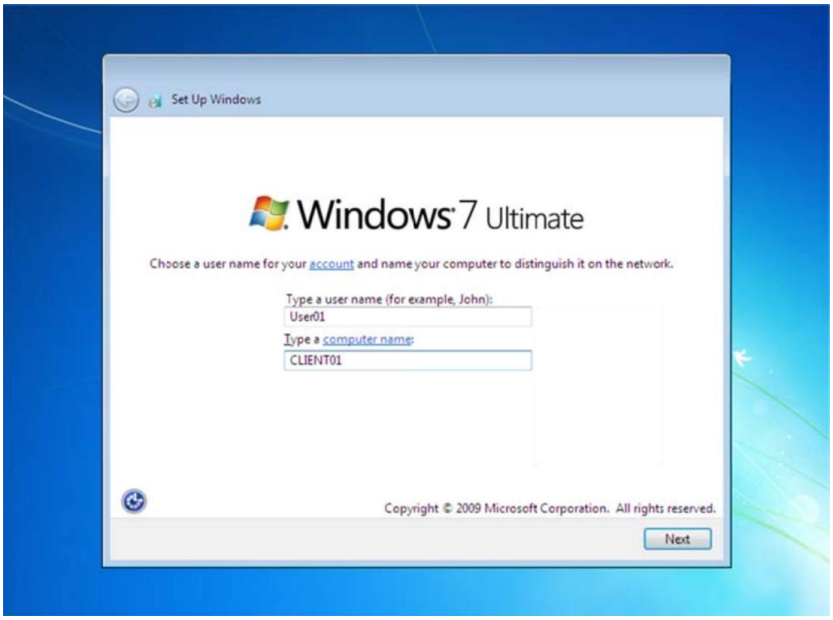
Langkah-langkahnya secara detail sebagai berikut:

3.7.3.1 Instalasi system Operasi

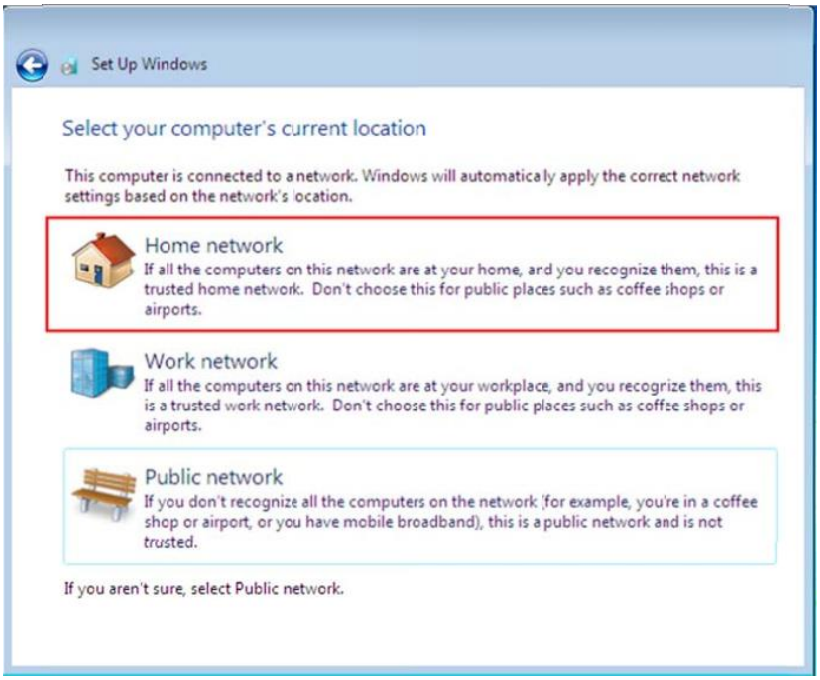
Untuk menginstal Windows 7 pada CLIENT01:

Langkah-langkah instalasi Windows 7

1. Pada CLIENT01, jalankan computer dengan dengan menggunakan Windows product disc. Ikuti instruksi yang muncul pada layar monitor.
2. Saat ditanya untuk tipe instalasinya, pilih **Custom**.
3. Saat ditanya untuk user name, ketikkan **user01**.
4. Saat ditanya untuk computer name, ketikkan CLIENT01



5. Saat ditanya unntuk computer location, pilih Home.

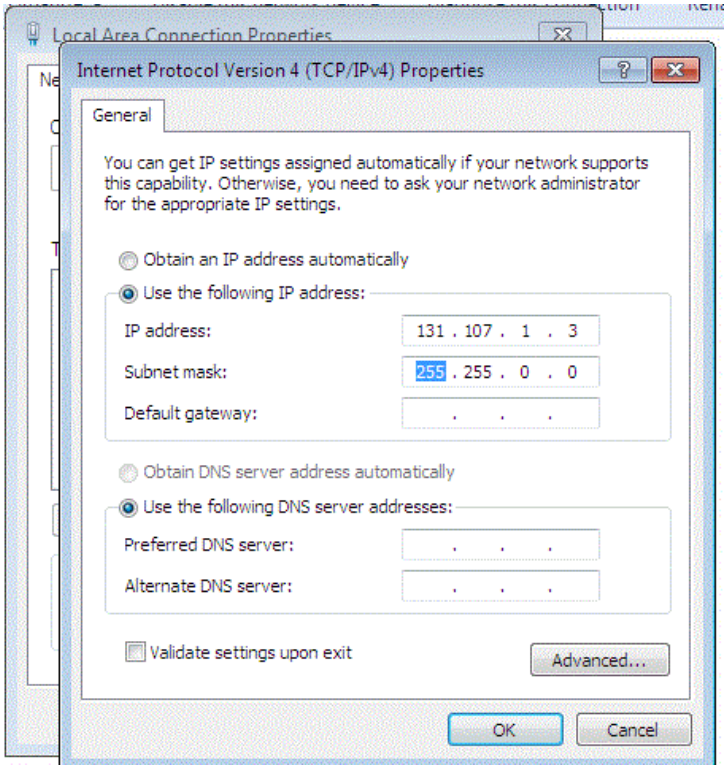


3.7.3.2 Konfigurasi TCP/IP

Konfigurasi property dari TCP IP agar Client01 memiliki IP address 131.107.1.3 untuk public (Internet) connection.

Langkahmengkonigurasi property TCP/IP:

1. Pada Client01, klik Start, dan kemudian klik Control Panel.
2. Klik Network and Internet, klik Network and Sharing Center, dan kemudian klik Manage network Connection.
3. Klik-kanan Local area Connection, dan kemudian klik Properties, jika terdapat kotak dialog yang muncul untuk meminta izin akses untuk menjalankan operasi ini klik Continue.
4. Pada kotak dialog Local Area Connection Properties, klik Internet Protocol Version 4 (TCP/IPv4) dan kemudian Klik Properties.
5. Klik Use the following IP address, pada IP address, ketikan 131.107.1.3 untuk IP address, dan ketikan 255.255.255.0 untuk subnet mask.



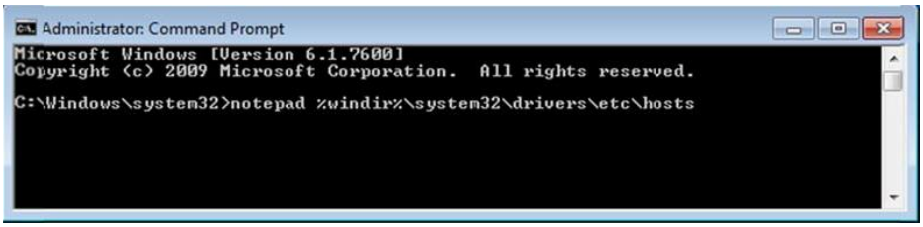
6. Klik Ok, dan kemudian klik Close.

Konfigurasi Host file untuk memiliki record untuk VPN01. Hal ini mensimulasikan scenario yang sesungguhnya dimana server VPN perusahaan memiliki host yang dipublikasikan.

Mengkonfigurasi Host file :

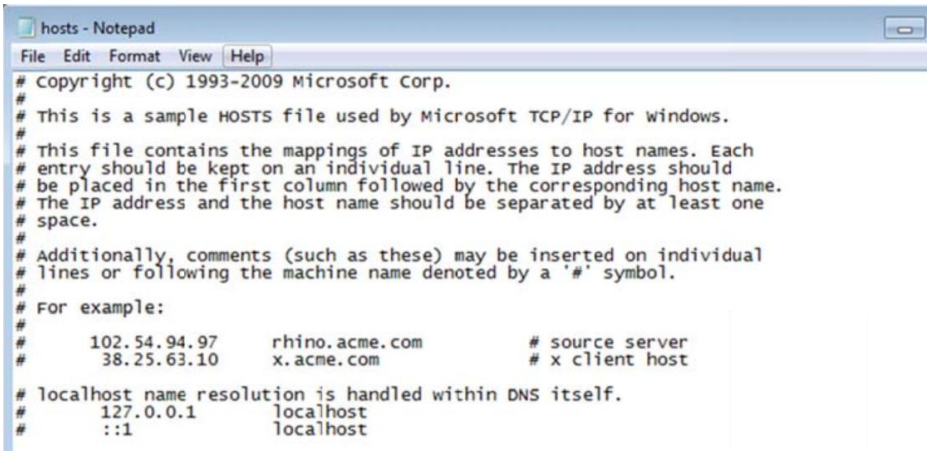
1. Pada client01, klik Start, klik All Programs, klik Accessories, klik kanan Comand Prompt, dan kemudian klik Run as Administrator.
2. Pada kotak sialog User Acound Control, klik Continue.
3. Pada windows Command, ketikan text berikut dan kemudian tekan Enter.

   `Notepad%windir%\system32\drivers\etc\host`



4. Tambahkan text berikut pada baris baru pada akhir document :

   `131.107.1.2VPN01.softexindonesia.com`

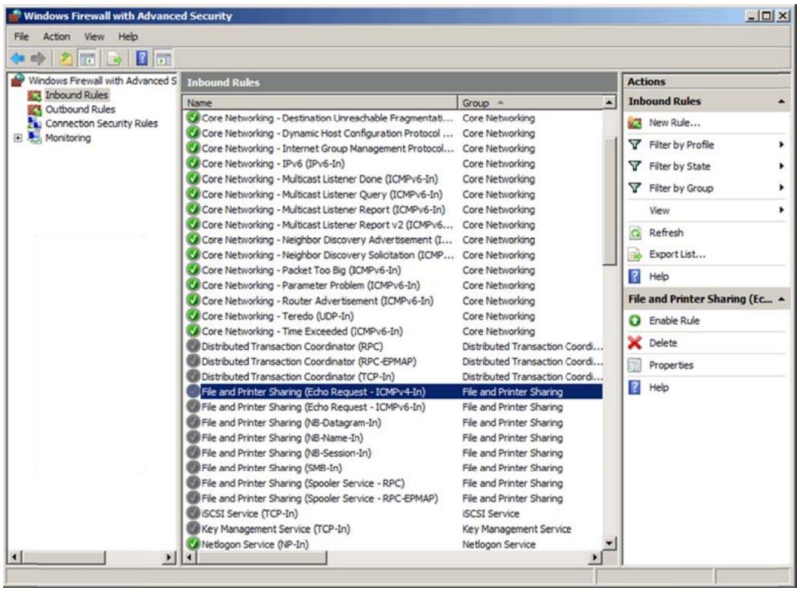


5. Simpan dan tutup host file

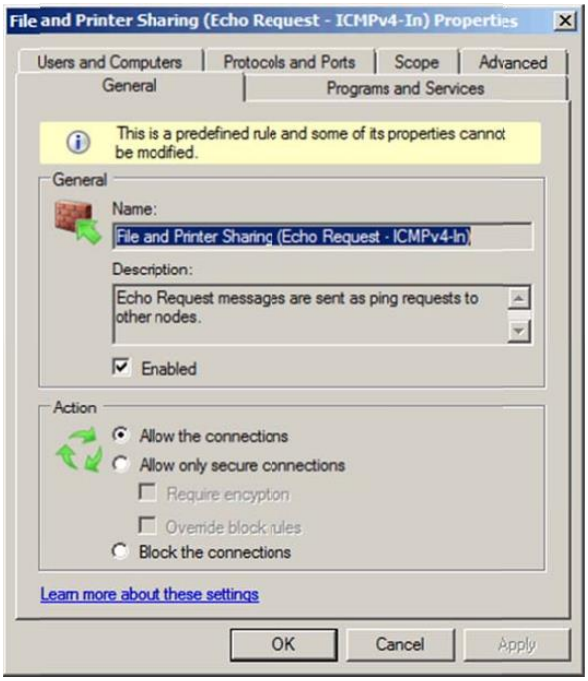
Jalankan perintah ping dari Client01 untuk memeriksa komunikasi jaringan antara Client01 dengan VPN01.

Langkah menggunakan perintah ping untuk memeriksa konektivitas jaringan:

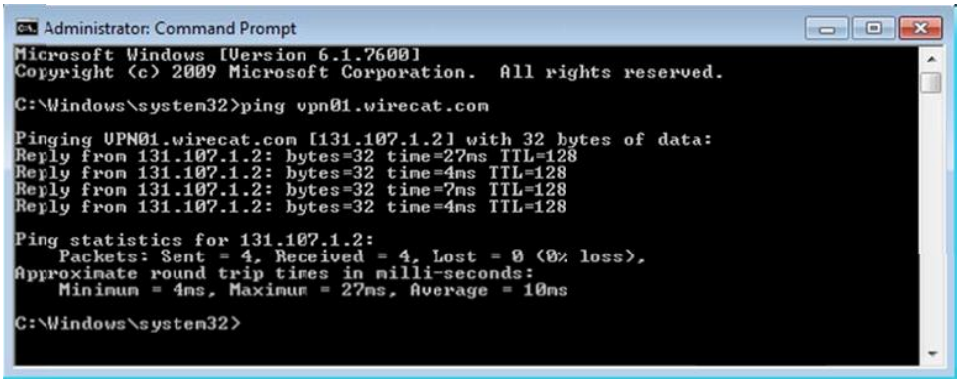
1. Pada VPN01, klik start, pilih Administrative Tools, dan kemudian klik windows Firewall with Advanve Security
2. Kemudian klik Inbound Rules.



3. Kemudan lakukan *scrolling down* dan klik-ganda File and Printer Sharing (Ecjo Request –ICMPv4-In) untuk Public profile. Pastikan rule ini aktif/enabled.



4. Pada bagin General, pastikan kotak cek Enable, dan kemudian klik OK.
5. Pada Client01, pada windows command window, ketikan ping VPN01.softexindonesia.com, dan kemudian tekan Enter.
6. Pastikan kita sukses melakukan ping ke VPN01



7. Tutup windows Command

3.8 Pengujian Koneksi VPN

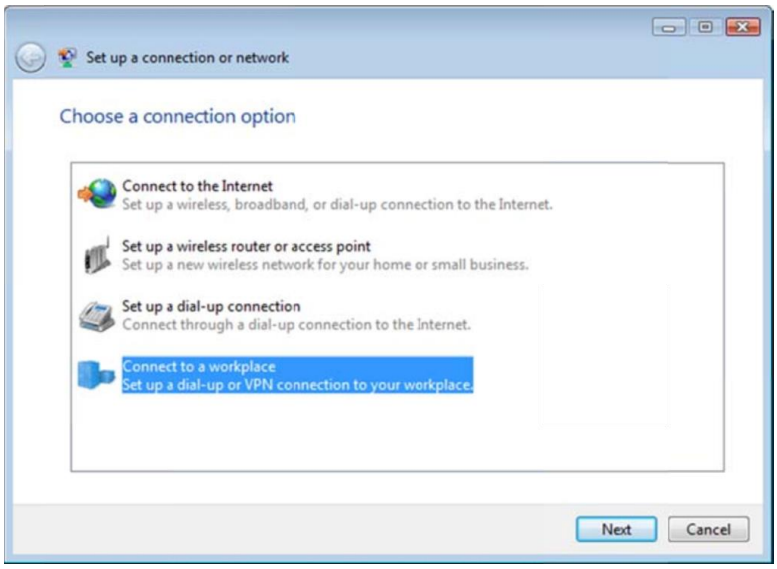
3.8.1 Simulasi Kegagalan Koneksi berbasis PPTP

Setelah melengkapi berbagai langkah konfigurasi yang. Pada bagian ini akan di jelaskan bagainmana mengkonfigurasi semua komponen yang sudah lengkap sehingga koneksi berbasis PPTP akan gagal. Simulasi ini merupakan scenario production dimana remote Access Server berada dibelakang firewall yang memblok koneksi PPTP. Berikut akan menggunakan Windows Firewall with Advance Securuty pada VPN01 yang berperan untuk *perimeter firewall.*

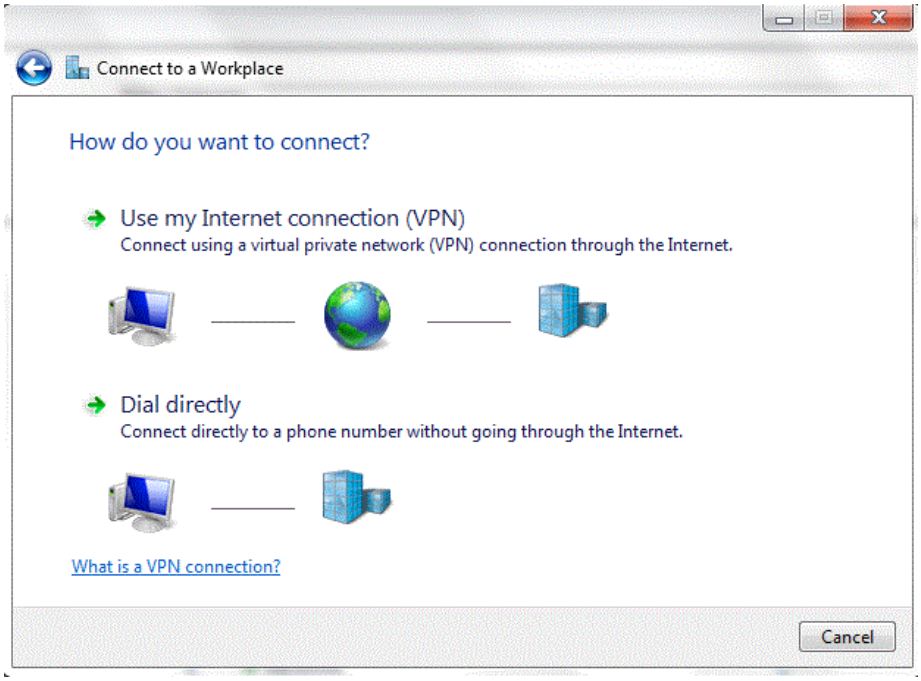
Konfigurasi Koneksi VPN berbasis PPTP

Langkah membuat Koneksi VPN berbasis PPTP:

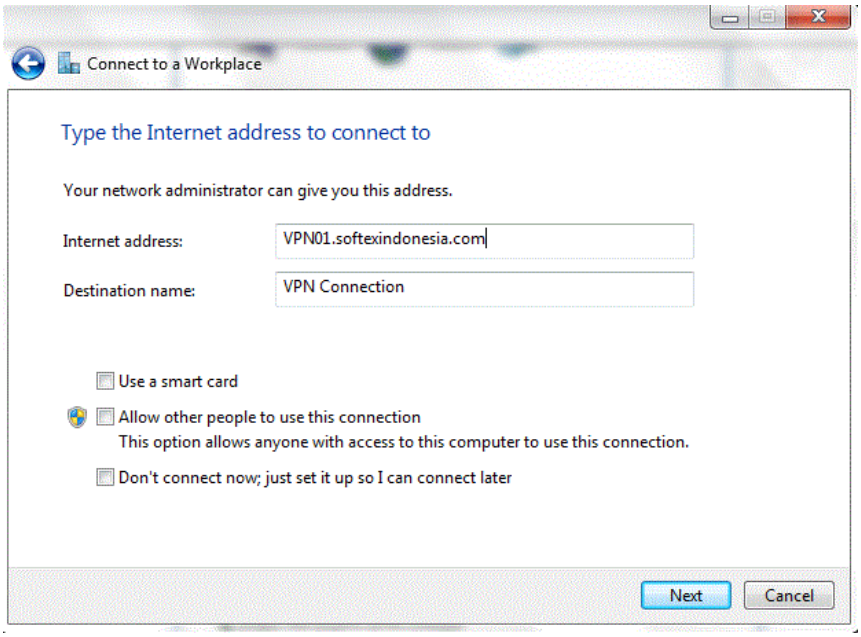
1. Pada Cllient01, klik Start, dan kemudian klik Control Panel.
2. Klik Network and Internet, klik Network and Sharing Center, dan kemudian klik set up a conneon or network.



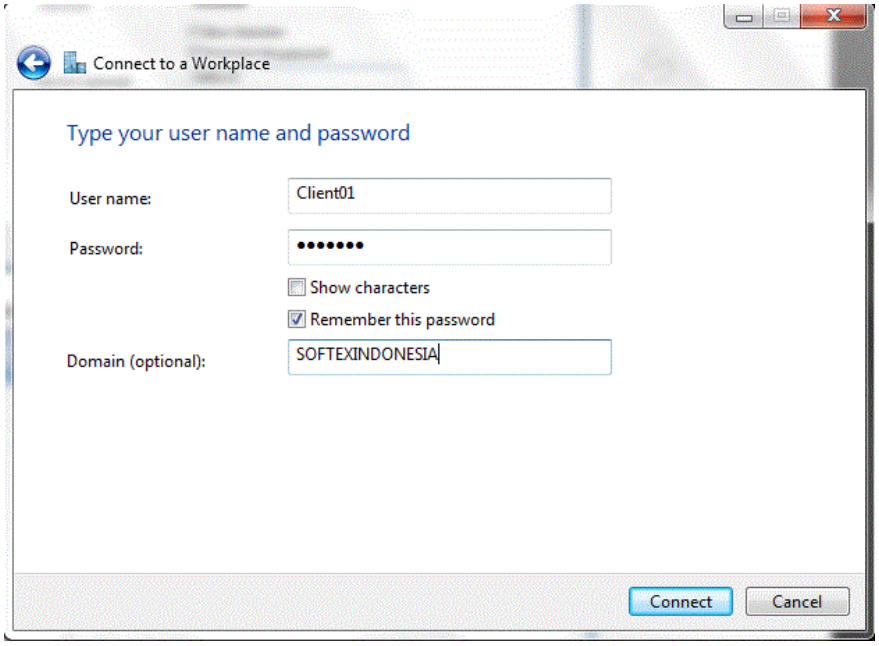
3. Klik Connect to a workplace, dan kemudian klik Next.
4. Klik Use My Internet Connection (VPN)



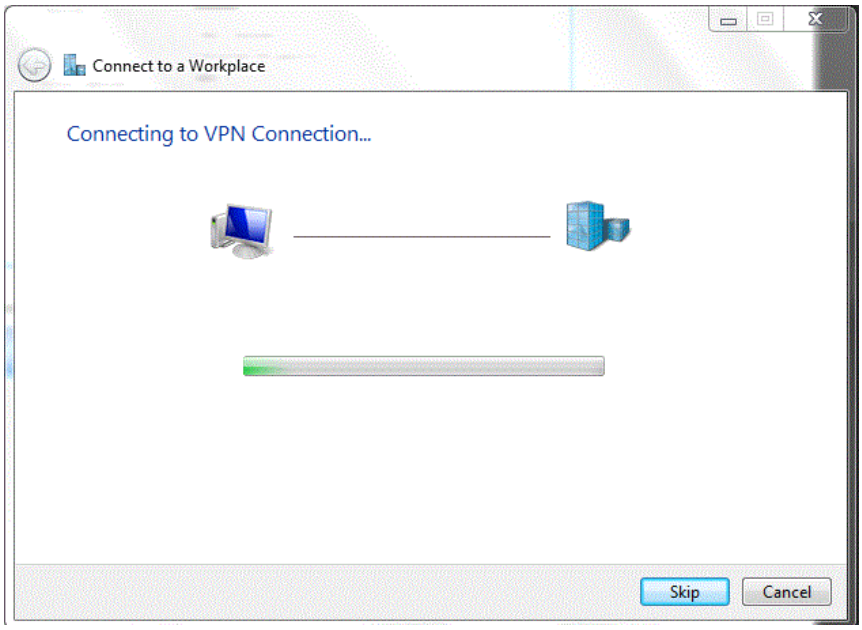
5. Klik I'll set up an Internet Connection later.
6. Pada Internet address, ketikan VPN01.softexindonesia.com, dan kemudian klik Next.



7. Pada kotak dialog type your user name and password, ketikan informasi berikut:
   - Pada UserName, keikkan Client01.
   - Pada Password, ketikkan P@ssword
   - Klik Remember this password
   - Pada domain (optional), ketikan softexindonesia.



8. Klik Create, dan apabila sudah selesai kemudian klik Close.



Pengujian Koneksi berbasis PPTP

Setelah selesai maka selanjutnya adalah melakukan pengujian koneksi PPTP. Dan pada pengujian ini harus sekses melakukan koneksi ke VPN01 dengan menggunakan koneksi VPN berbasis PPTP yang dibuat pada Client01.

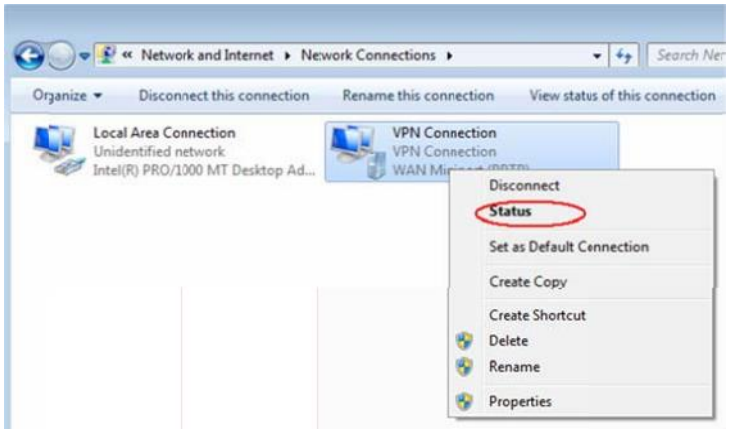
Langkah pengujiannya adalah

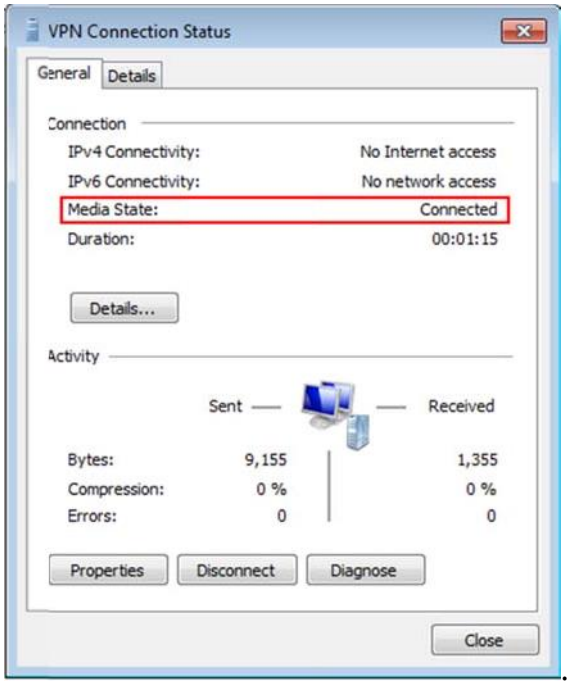
1. Pada Client01, pada Network And Sharing Center, klik Manage Network Connection.





2. Klik Ganda VPN Connection, dan kemudian klik Connect.
3. Pastikan bahwa koneksi sukses dilakukan dengan cara klik-kanan VPN Connection, dan kemudian klik Status, *Media State* pastikan "Connected"





4. Pada kotak dialog VPN Connection Status , Klik Disconnect.

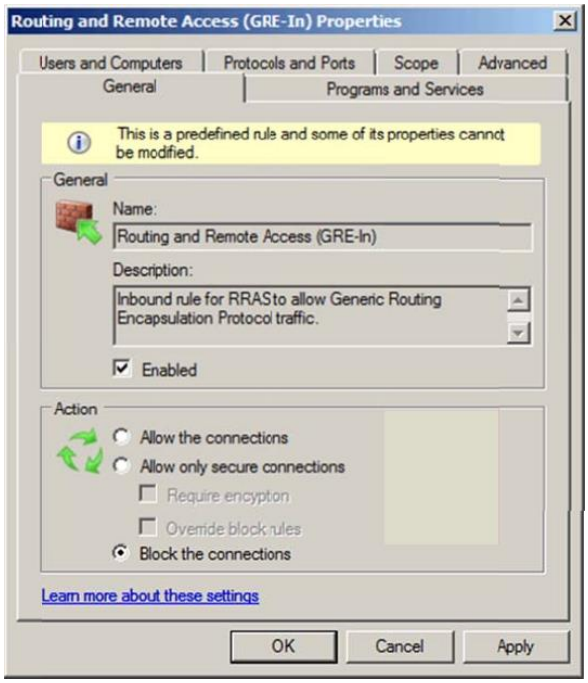
Konfigurasi Windows Firewall with Advanced Securuty

Trafik data PPTP berisi trafik yang melalui TCP port 1723 untuk *Tunnel maintenance* dan trafik yang melalui IP protocol 47 untuk *Generic Routing Encapsulation (GRE)* yang digunakan untuk tunneling data. Lakukan

komfigurasi Windows Firewall With Advanced Securuty untuk memblok trafik inbound GRE ke VPN01. Hal ini mensimulaikan remote access server yang berada di belakang firewall yang memblok koneksi PPTP.

Langkah mengkonfigurasi Windows Firewall with Adfanced Security untuk memblok koneksi berbasis PPTP:

1. Pada VPN01, klik Start, pilih Administative Tools, dan kemudian klik Windows Firewall with Advanced Security.
2. Kemudian klik Inbound Rules.
3. *Scrolling down* dan klik-ganda Routing and Remote Access (GRE-In)
4. Pada bagian Action, pilih Block the Connection, dan kemudian klik OK.



Menguji Koneksi berbasis SSTP

Berikut langkah menguji bahwa koneksi PPTP ke VPN01 telah di blok.

1. Pada Client01, pada Network and Sharing Center, klik Manage Network Connections.
2. Klik-ganda VPN Connection, dan kemudian klik Connect.
3. Periksa kembali untuk memastikan bahwa koneksi gagal, kita pastilah memeperoleh dialog seperti berikut :



4. Klik Close.

3.8.2 Konfigurasi Koneksi Berbasis SSTP

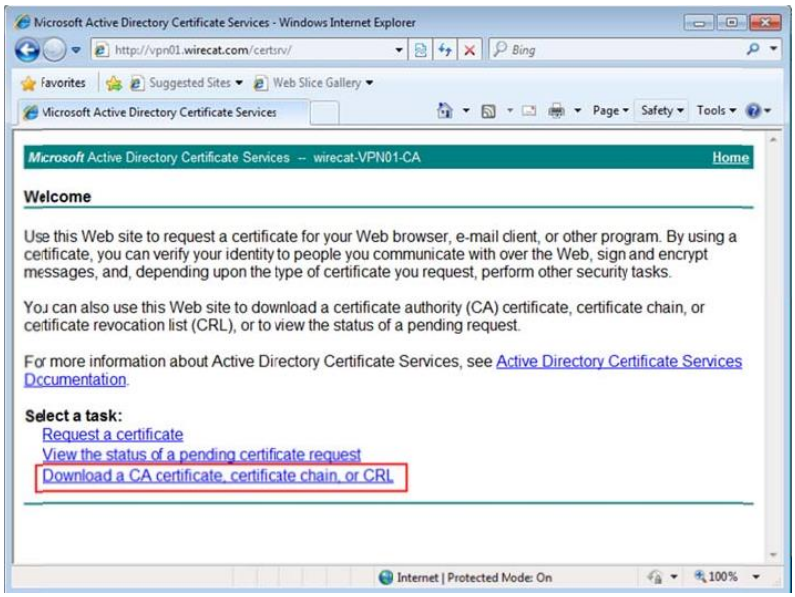
VPN Client yang menggunakan koneksi SSTP harus mengistal Sertifikat root CA sertifikat computer dari VPN server. Selama fase autentikasi berlangsung, VPN ZClient memvalidasi Server Authentication cercificate menggunakan sertifikat yang diindtal pada client**.**

Perolehan Trusted Root CA certificate

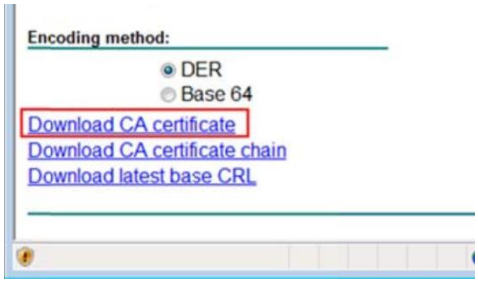
Root certificate dapaat diperoleh melalui *auto-enrollment,* jika client digabungkan ke domain Active Directory, atau melalui Web enrollment dari website yang menerbitkan sertifikat CA. disini Client01 akan memperoleh sertifikat root CA dari VPN01 dengan menggunakan Web Enrollment dengan langkah :

1. Pada Client01, klik start, dan kemudian klik internet Ekxplorer.
2. Pada internet explorer, bersihkan URL dan ketikan http://VPN01.softexindonesia/certsrv, dan kemudan tekan enter.
3. Jika Muncul peringatan *phishing filter,* klik turn off automatic Phishing Filter, dan kemudian OK.

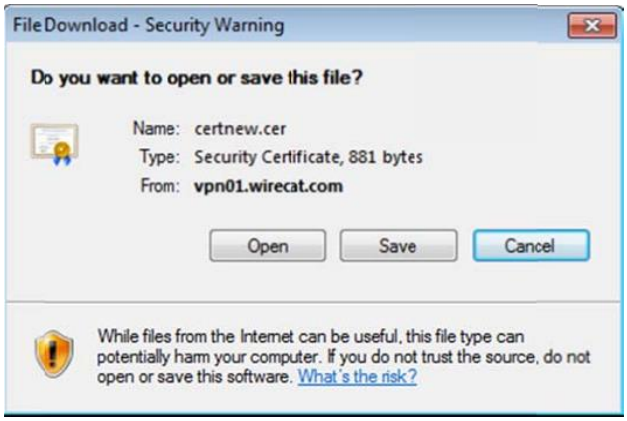
4. Pada halawan Welcome, pada bagian Select atask, klik Download a CA certificate, certificate chain, or CRL.



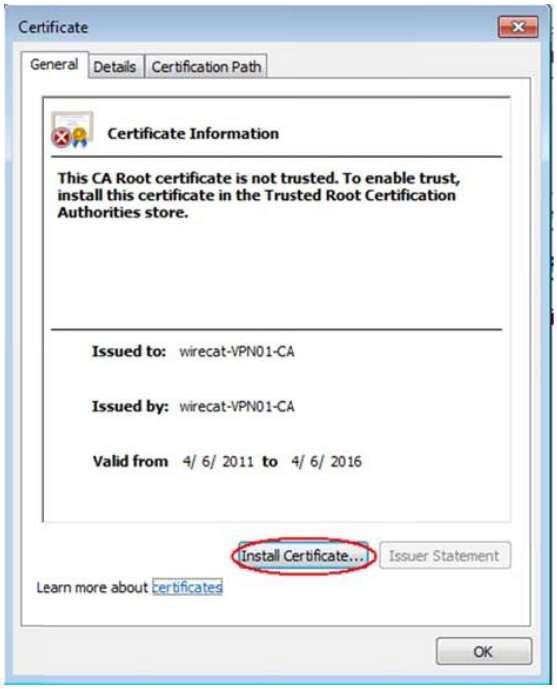
5. Jika menerima sebuah peringatan tentang *Information Bar*, klik Close.
6. Klik **Download CA Certificate.**



7. Pada kotak dialog File Download, klik Open.



8. Pada Kotak dialog security alert, klik Allow.
9. Klik Instal Certificate.



10. Pada Certificate Import Wizard, klik Next.
11. Pada kotak dialog Certificate Store, Klik Nenxt untuk menerima lokasi penyimpanan default automatis.
12. Klik Finish.
13. Pada kotak dialog konfirmasi, klik Ok.
14. Klik OK untuk menutup kotak dialog Certificate.

Sertifikat sudah terinstal dan harus dipindahkan ke lokasi penyimpanan yang benar, lokasi default secara automatis untuk setiap sertifikat yang diinstal adalah di **current user,** Intermediate Certification Authority, Sertifikat tersebut harus dipindahkan ke Local Computer, Trusted Root Certification Authority pada Clien01. Prosesnya diawali dengan mengkonfigurasi sebuah MMC dengan snap-in yser and Computer Certificate.

Langkah mengkonfigurasinya sebuah MMC:

1. Pada Client01, klik start, klik All Programs, klik Accessories, dan kemudian

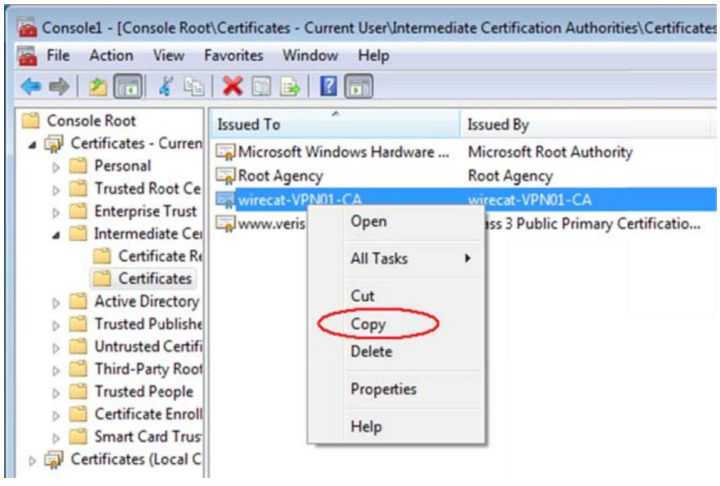
klik Run.

2. Pada Open, ketikan mmc, dan kemudian klik OK.
3. Pada Kotak dialog User Account Control , klik Continue.
4. Pada snap-in Console1, klik File, dan kemudian klik Add/Remove Snap-in.
5. Pada bagian Available snap-ins, klik certificates, dan kemudian klik Add.
6. Klik Finish untuk menerima seting default dari My User Account.
7. Klik Add, klik Computer Account, dan kemudian klik Next.
8. Pada kotak dialog Select Computer, klik Finish untuk menerima seting default dari Local Computer.
9. Klik OK untuk menutup kotak dialog Add or Remove Snap-ins.

Pindahkan sertifikat yang telah di install dari lokasi penyimpanan default. Karena sertifikat ini tidak melibatkan *private key building*, kita dapat lakukan *proses Copy* dan *paste* sertifikat tersebut ke lokasi penyimpanan sertifikat baru.

Langkah memindahkan sertifikat :

1. Pada Client01, pada MMC yang dibuat tadi, klik-ganda Crtificate –Current User, klik-ganda Intermediate Certification Authorities, dan kemudian klik Certificates.
2. Pada bagian tengah panel, kli-kanan sertifikat softexindonesia-VPN01-CA, dan kemudian klik Copy.



3. Kemudian klik-ganda Certificates (local Computer), klik-ganda Trusted Root

Certification Authorities, dan kemudian klik Certificates.

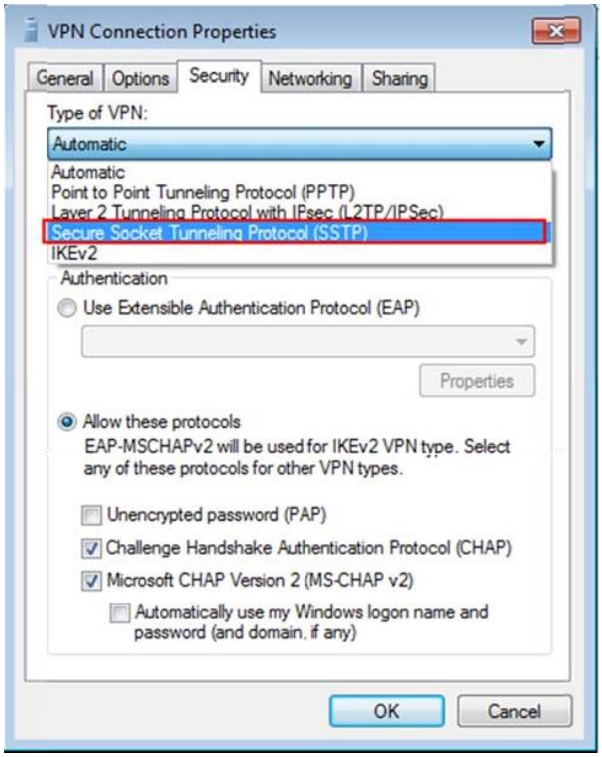
4. Pada bagian tengah panel, klik-kanan dan kemudian klik paste.
5. Lakukan *refresh* untuk memastikan sertificate tersebut telah ditambahkan ke lokasi penyimpanan ini.

Konfigurasi dan Pengujian Koneksi VPN berbasis SSTP

Setelah Sertificatk root CA dari sertifikat computer milik VPN Server telah berada di lokasi Trusted Root Certification Authorities pada Client01, sekarang tinggal melakukan konfigurasi dan pengujian koneksi SSTP.

Berikut adalah-langkah-langkahnya:

1. Pada Client01, pada Network and Sharing Center, klik Manage network Connection.
2. Klik-ganda VPN Connection, dan kemudian klik Properties.
3. Klik tab security.
4. Dari *drop-down list Type* of VPN, pilih Secure Socket Tunneling Protocol (SSTP), dan kemudian klik OK.

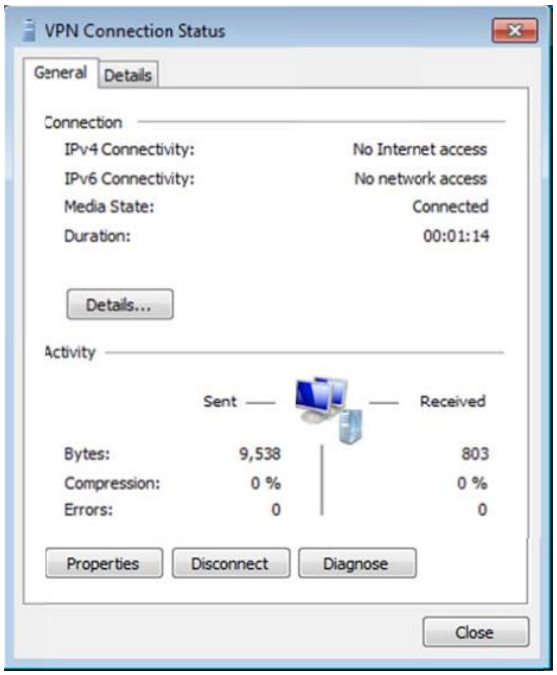


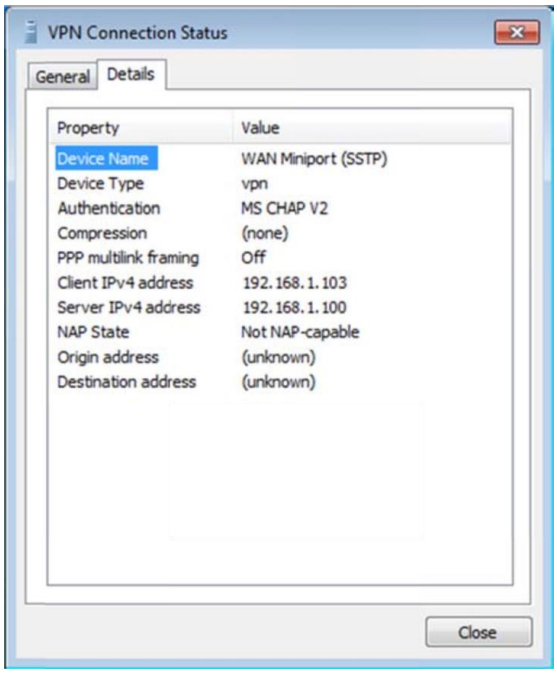
5. Pada dialog Connect VPN Connection, klik Connect.



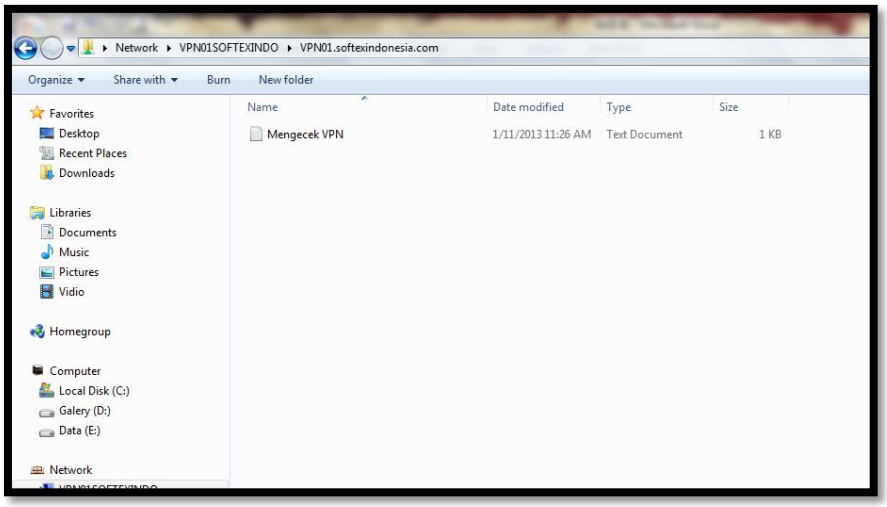
Client harus sukses melakukan koneksi VPN01 dengan menggunakan koneksi SSTP. Pastikan kita mengaksesn corporate fil server dari lokasi remote. Dan melakukan pengecekan pada VPN Connection Statusnya, periksa pada bagian tab General dan Detalnya.

6. Klik Start, klik All Program, klik Accessories, dan kemudian klik Run.

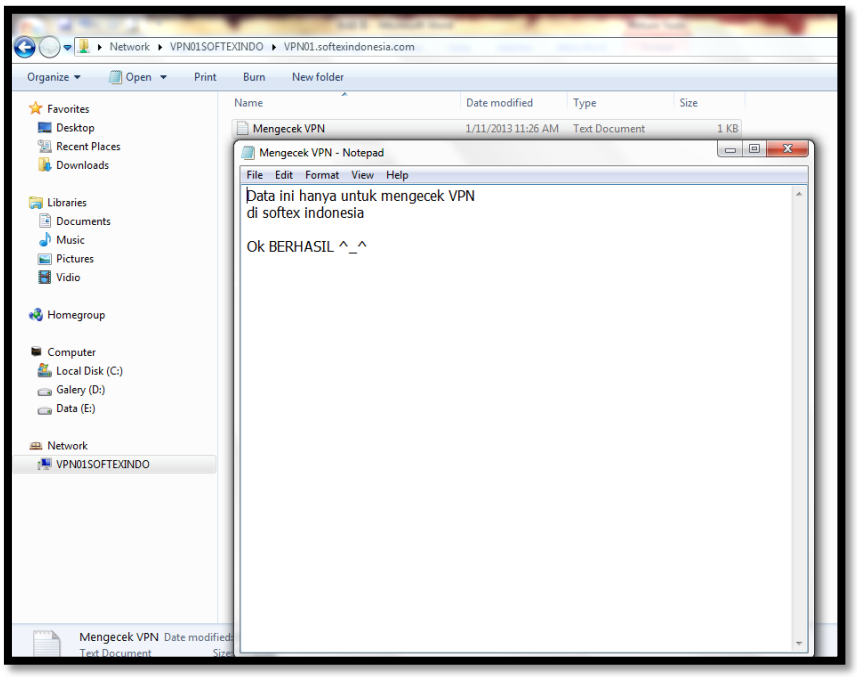




7. Pada Open, ketikan `\\DC01.softexindonesia.com\Dataku`. dan kemudian OK.



8. Klik-ganda (Mengecek VPN) untuk membukanya, tambahkan beberapa teks secara bebas dan kemudian simpan file tersebut.



9. Tutup (Mengecek VPN.txt)

Dengan begitu koneksi VPN berbasi Protocol SSTP ini berjalan dengan baik dan dapat di terapkan dengan menambahkan user-user di Departemen Acounting PT Softex Indonesia.