ASA 8.X: AnyConnect SCEP-configuratievoorbeeld voor inschrijving

Inhoud

Inleiding

SCEP-inschrijvingsfunctionaliteit wordt geïntroduceerd in AnyConnect standalone client 2.4. Tijdens dit proces wijzigt u het AnyConnect XML-profiel om een SCEP-gerelateerde configuratie op te nemen en maakt u een specifiek groepsbeleid en verbindingsprofiel voor certificatie-inschrijving. Wanneer een AnyConnect-gebruiker op deze specifieke groep verbindingen maakt, stuurt AnyConnect een verzoek om inschrijving van het certificaat naar de CA-server en aanvaardt of ontkent de CA-server automatisch het verzoek.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 Series adaptieve security applicaties die softwareversie 8.x uitvoeren
- Cisco AnyConnect VPN versie 2.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Het doel van de automatische SCEP inschrijving voor AnyConnect is een certificaat aan de cliënt op een veilige en schaalbare manier af te geven. Gebruikers hoeven bijvoorbeeld geen certificaat bij een CA server aan te vragen. Deze functionaliteit is geïntegreerd in de AnyConnect-client. De schuldbewijzen worden aan de cliënten uitgegeven op basis van de in het XML - profielbestand vermelde certificatieparameters.

Overzicht van de vereiste wijzigingen

AnyConnect SCEP-inschrijvingsfunctie vereist dat bepaalde certificeringsparameters in het XML-profiel worden gedefinieerd. Er wordt een Groepsbeleid- en verbindingsprofiel gecreëerd op de ASA voor certificatie inschrijving, en het XML profiel wordt geassocieerd met dat beleid. De AnyConnect-client sluit aan op het verbindingsprofiel dat dit specifieke beleid gebruikt en stuurt een aanvraag voor een certificaat met de parameters die in het XML-bestand zijn gedefinieerd. Certificaat-instantie (CA) accepteert of ontkent het verzoek automatisch. De AnyConnect-client wint certificaten op met het SCEP-protocol als het <certificaatonderdeel> in een clientprofiel is gedefinieerd.

De verificatie van het clientcertificaat moet onjuist zijn voordat AnyConnect automatisch de nieuwe certificaten probeert op te halen, zodat er geen inschrijving plaatsvindt als u al een geldig certificaat hebt geïnstalleerd.

Wanneer gebruikers inloggen bij de specifieke groep, worden ze automatisch geregistreerd. Er is ook een handmatige methode beschikbaar voor het ophalen van certificaat, waarin gebruikers voorzien zijn van een knop **kraan**. Dit werkt alleen wanneer de client directe toegang heeft tot de CA server, niet door de tunnel.

Raadpleeg de Cisco AnyConnect VPN-clientbeheerdershandleiding, release 2.4 voor meer informatie.

XML-instellingen om de AnyConnect SCEP-functie in te schakelen

Dit zijn de belangrijke elementen die moeten worden gedefinieerd in het AnyConnect XML-bestand. Raadpleeg de Cisco AnyConnect VPN-clientbeheerdershandleiding, release 2.4 voor meer informatie.

- <AutomaticSCEPHost>-Specificeert de ASA host naam en het verbindingsprofiel (tunnelgroep) waarvoor SCEP certificaat ophalen is ingesteld. De waarde moet in het formaat van de volledig gekwalificeerde domeinnaam van de ASA\Connection-profielnaam of IP-adres

van de ASA\Connection-profielnaam zijn.
- <CAURL>-identificeert de SCEP CA server.
- <certificaatomvang>-definieert hoe de inhoud van het certificaat wordt gevraagd.
- <DisplayGetCertKnop>—Hiermee wordt bepaald of de AnyConnect GUI de knop Get Certificate weergeeft. Het stelt gebruikers in staat handmatig om verlenging of levering van het certificaat te verzoeken.

Hier is een voorbeeldprofiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Configureer het ASA om SCEP protocol te ondersteunen voor AnyConnect

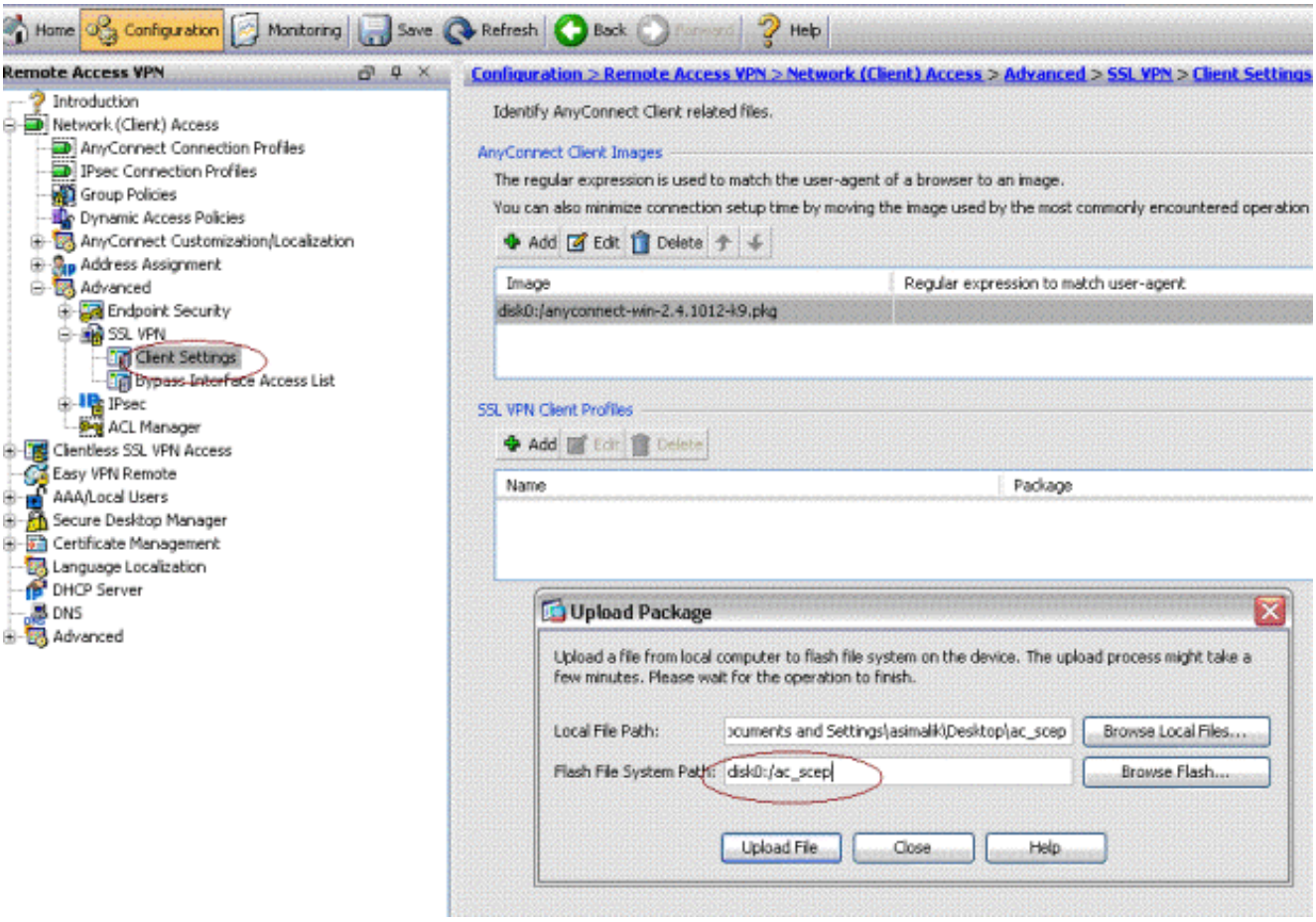
Om toegang te verlenen tot een particuliere Registratieautoriteit (RA), moet de ASA-beheerder een alias maken die een ACL heeft die de verbinding van het particuliere netwerk aan de gewenste RA beperkt. Om automatisch een certificaat op te halen, verbinden gebruikers zich aan en authentiseren ze deze alias.

Voer de volgende stappen uit:

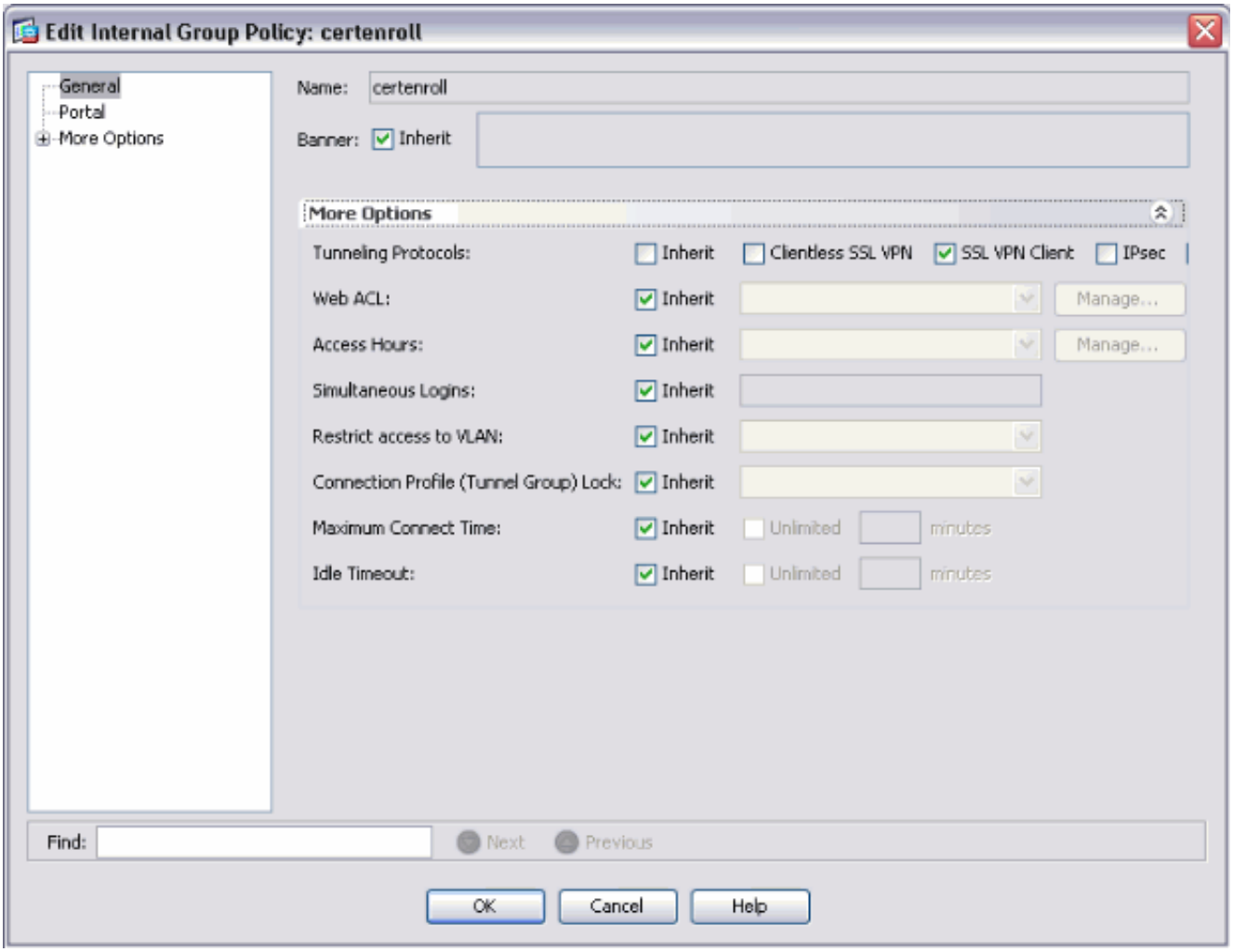
1. Maak een alias op de ASA om naar de specifieke geconfigureerde groep te wijzen.
2. Specificeer het alias in het element <AutomaticSCEPHost> in het clientprofiel van de gebruiker.
3. Hang het clientprofiel dat de sectie <certificaatinschrijving> in de specifieke geconfigureerde groep bevat.
4. Stel een ACL voor de specifieke geconfigureerde groep in om het verkeer te beperken tot de particuliere RA.

Voer de volgende stappen uit:

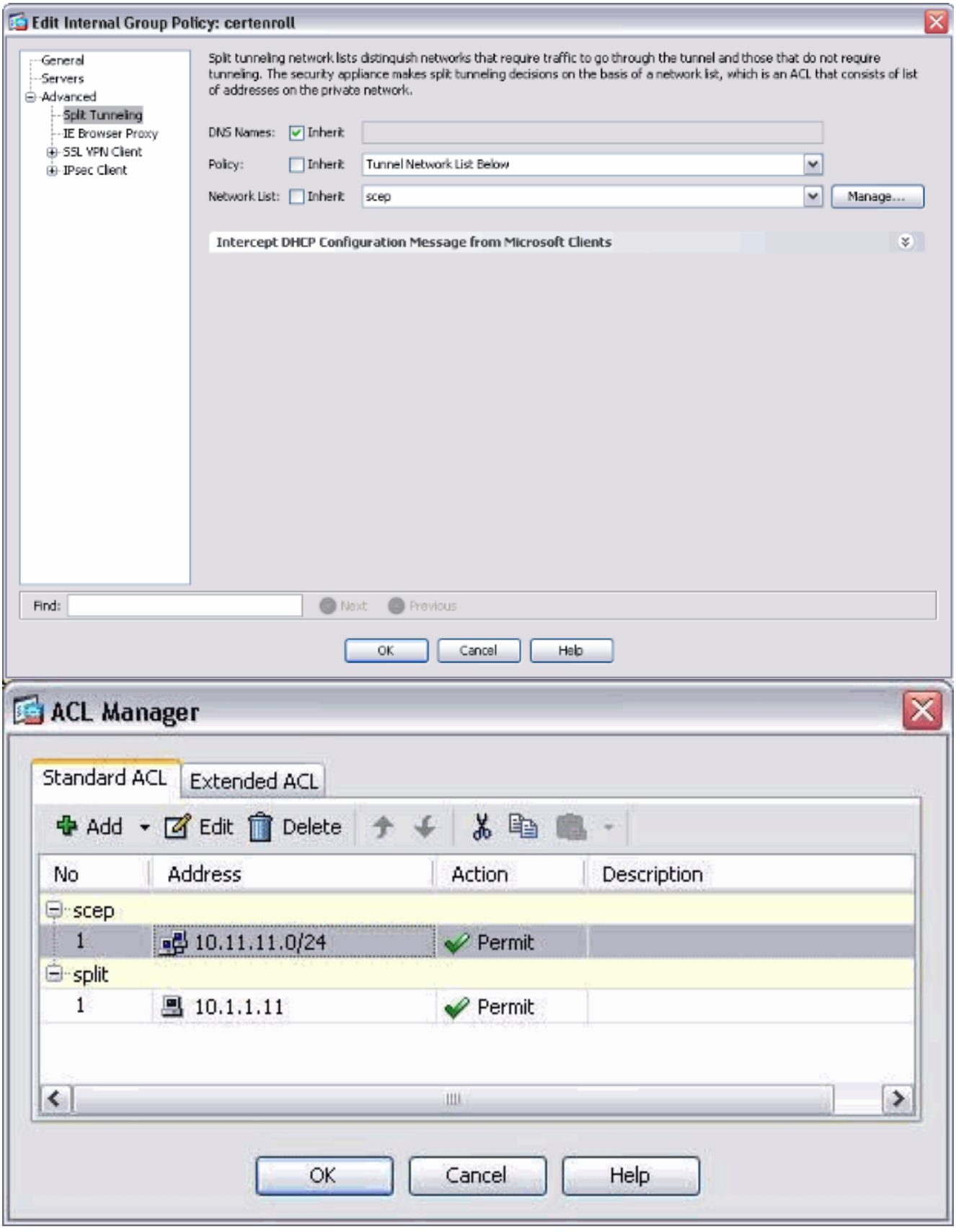
1. Upload het XML-profiel naar ASA.Kies **Remote Access VPN > Network (client) toegang > Advanced > SSL VPN > Clientinstellingen**.Klik onder SSL VPN-clientprofielen op **Toevoegen**.Klik op **Local Files Bladeren** om het profielbestand te selecteren en klik op **Bladeren** om de naam van het flitsbestand te specificeren.Klik op **Upload File**.



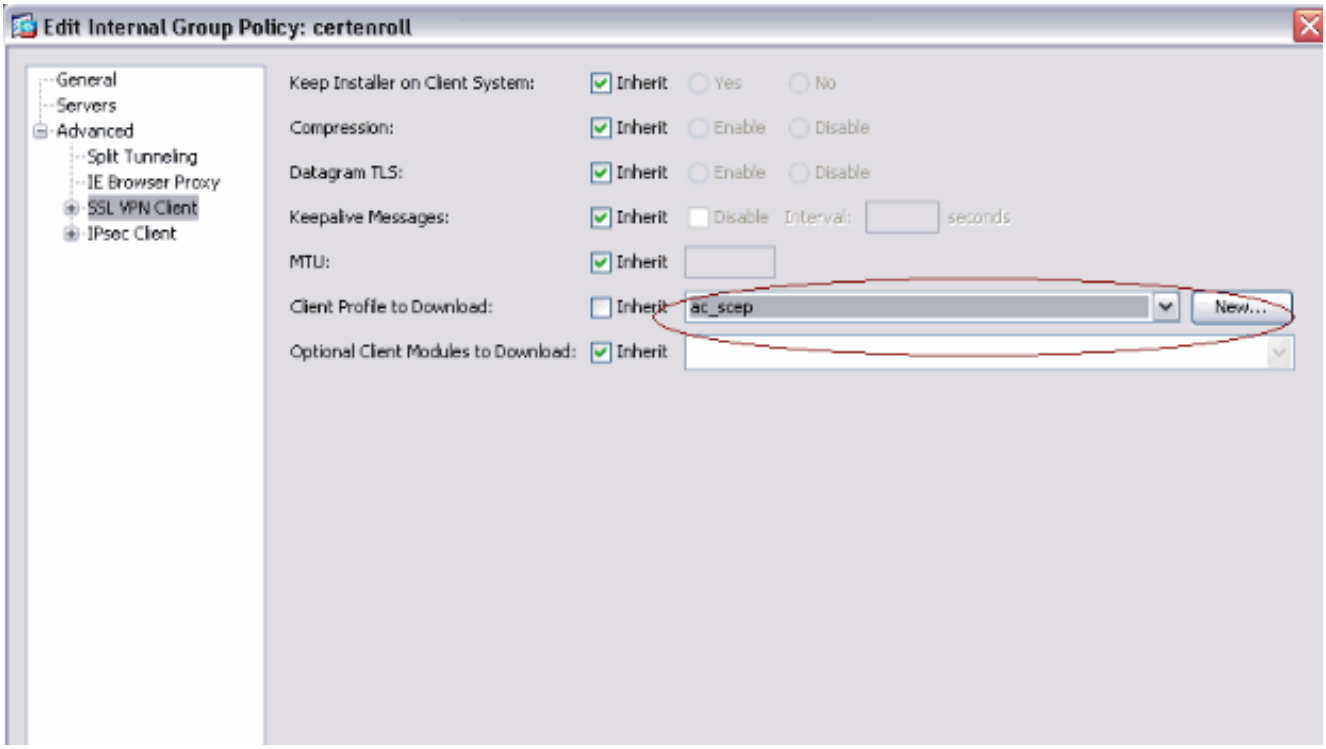
2. Stel een groepsbeleid voor de inschrijving van certificaten in.Kies **externe toegang VPN > Toegang tot netwerkclient > Groepsbeleid** en klik op **Toevoegen**.



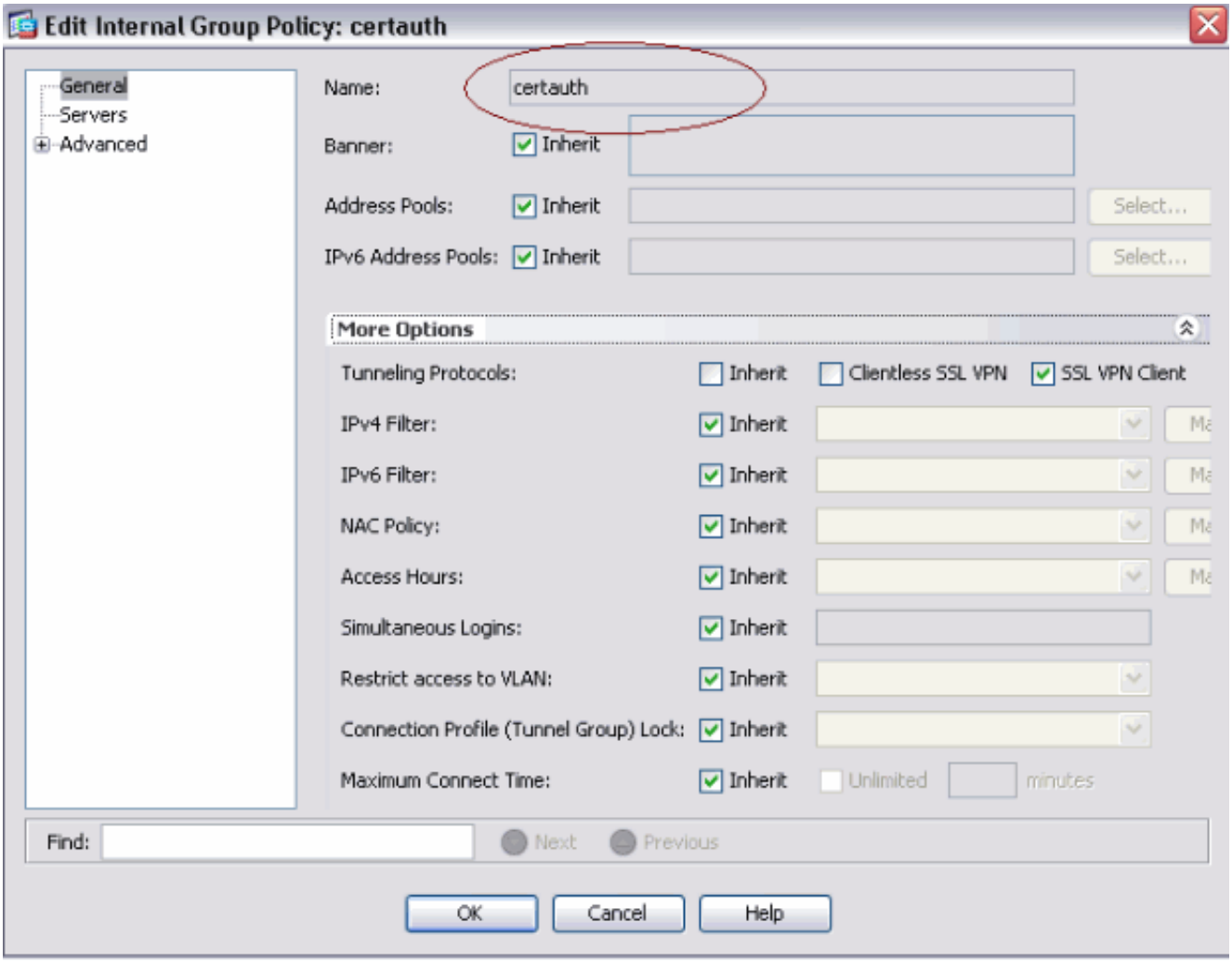
Voeg een gesplitste tunnel toe voor CA server.Vul **Geavanceerd uit** en selecteer vervolgens **Split-tunneling**.Klik op **de** onderstaande **lijst met tunnelnetwerken** in het beleidsmenu en klik op **Bewerken** om de toegangscontrolelijst toe te
voegen.



Selecteer **SSL VPN-client** en kies het profiel voor certenroll in het **clientprofiel** van **het** menu **Downloaden**.

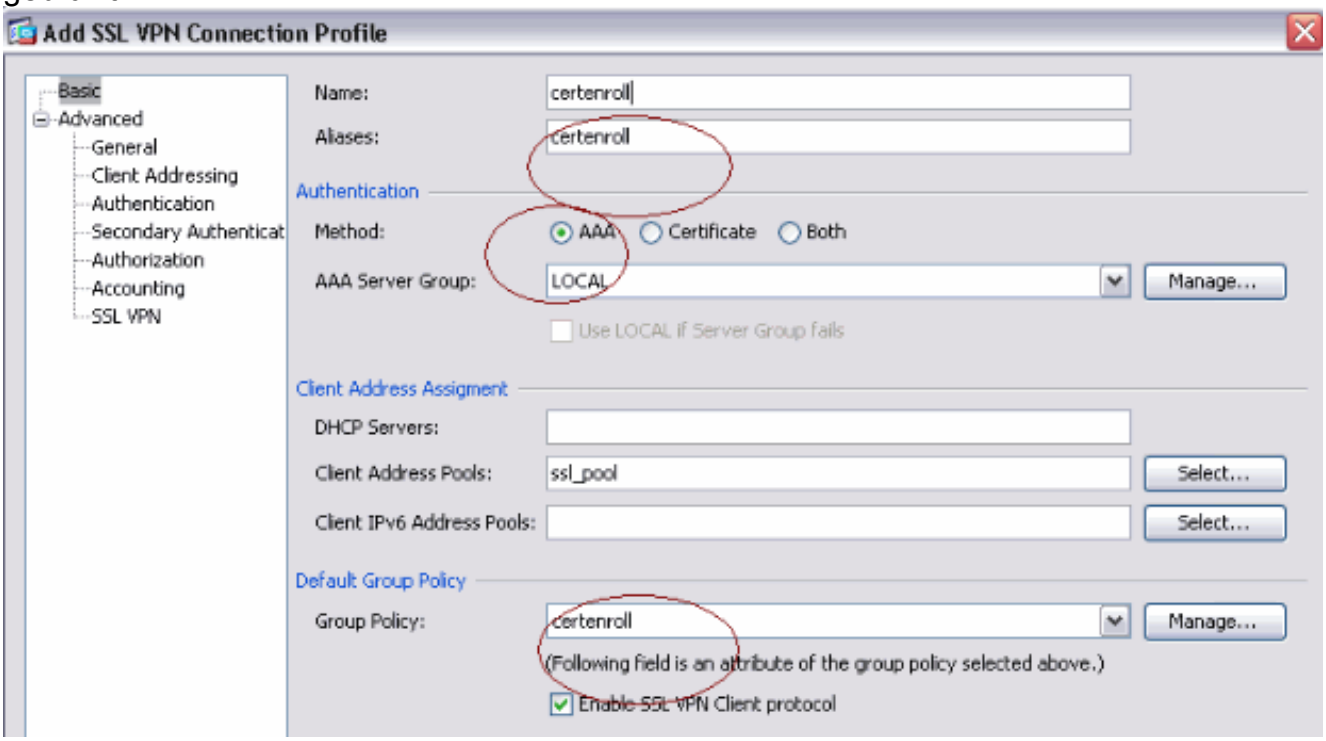


3. Maak een andere groep die **certauth** heet voor certificatie.

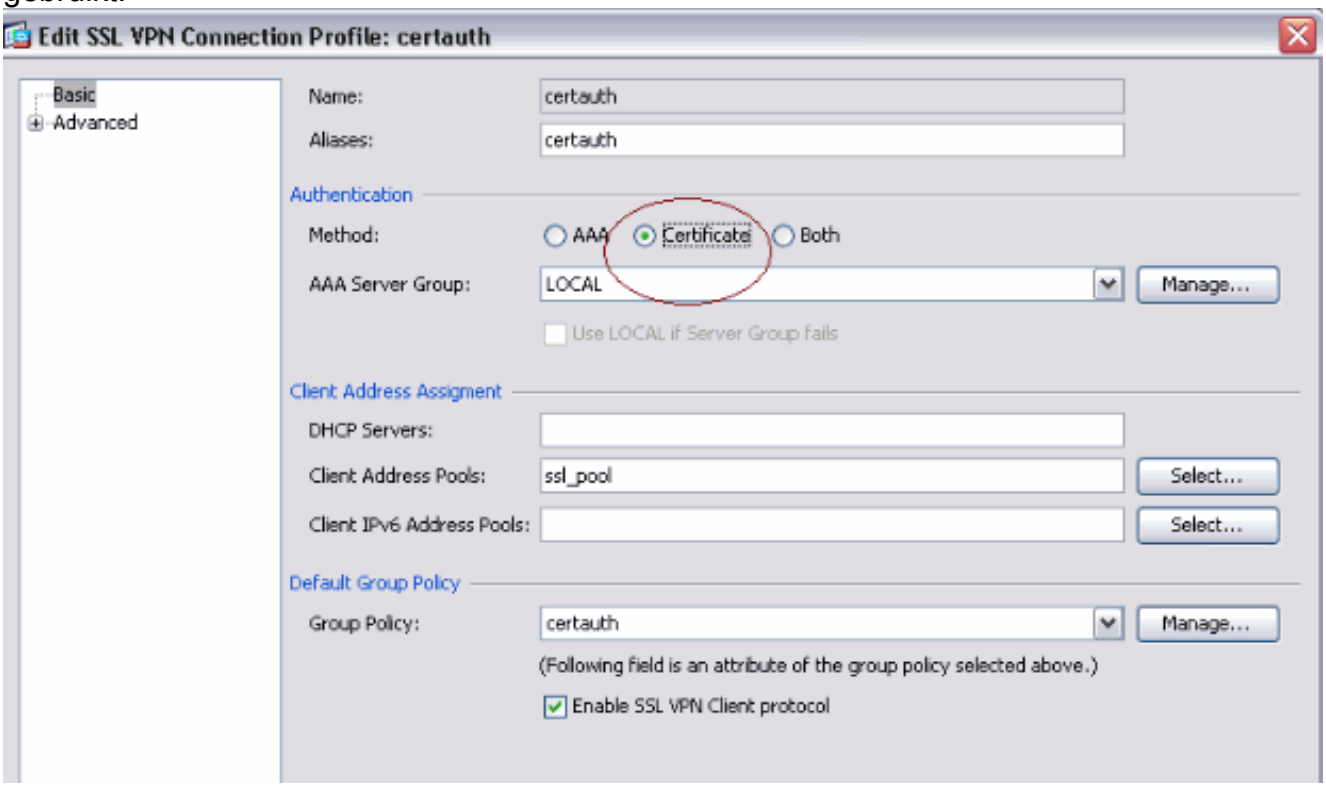


4. Maak een verbindingsprofiel.Kies **externe toegang VPN > Toegang tot netwerkclient > AnyConnect-verbindingsprofielen** en klik op **Add**.Voer de certenroll-groep in in het veld Aliassen.**Opmerking:** De naam van het alias moet overeenkomen met de waarde die in het AnyConnect-profiel onder AutomaticSCEPHost wordt

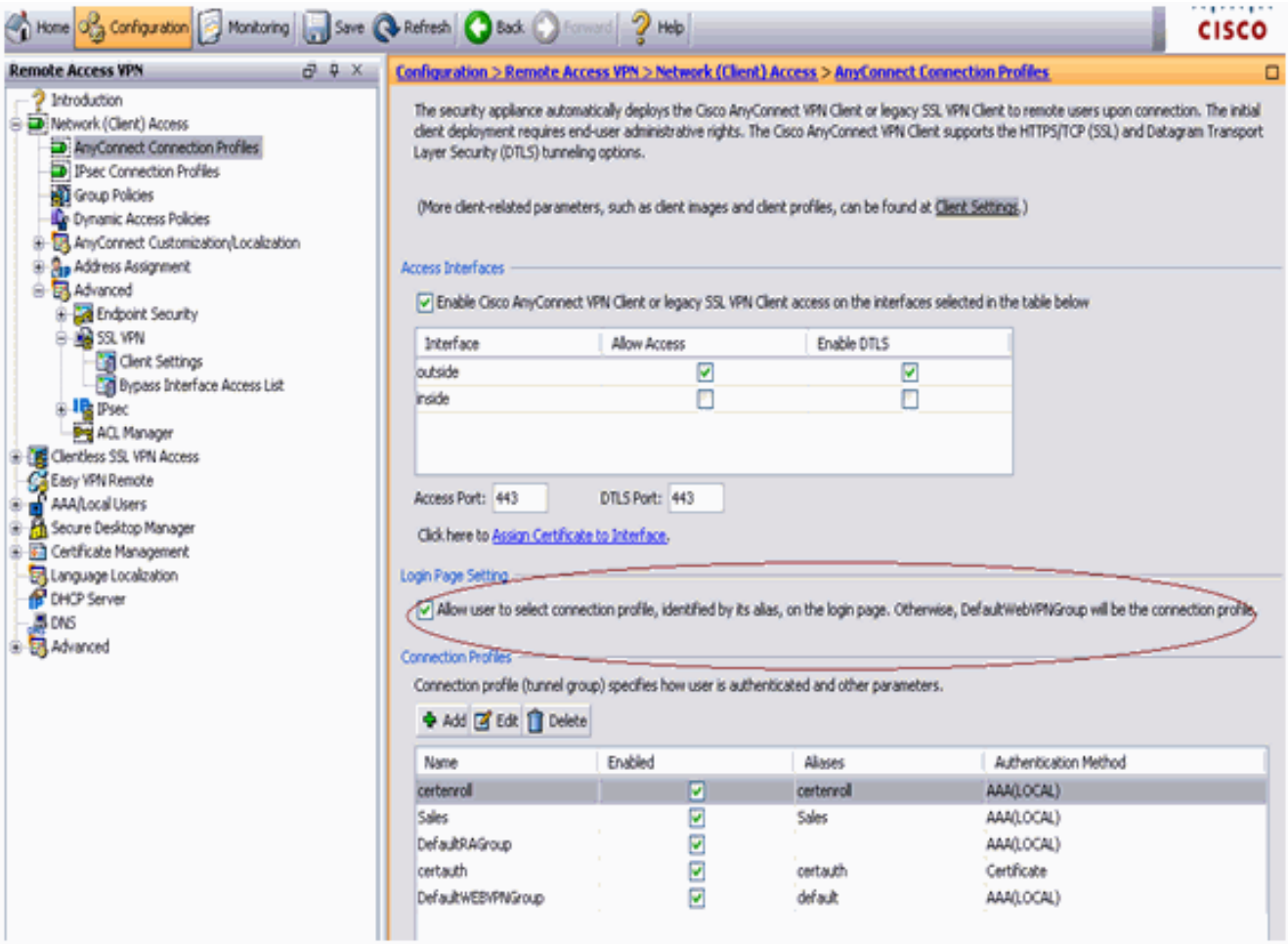
gebruikt.



5. Maak een ander verbindingsprofiel genaamd **certauth** met certificatie. Dit is het eigenlijke verbindingsprofiel dat na inschrijving wordt gebruikt.



6. Om er zeker van te zijn dat het gebruik van alias is ingeschakeld, controleert u **op de loginpagina de gebruiker toestemming geven om het verbindingsprofiel te selecteren dat door zijn alias is geïdentificeerd. Anders is DefaultWebVPNroup het verbindingsprofiel.**



AnyConnect SCEP testen

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

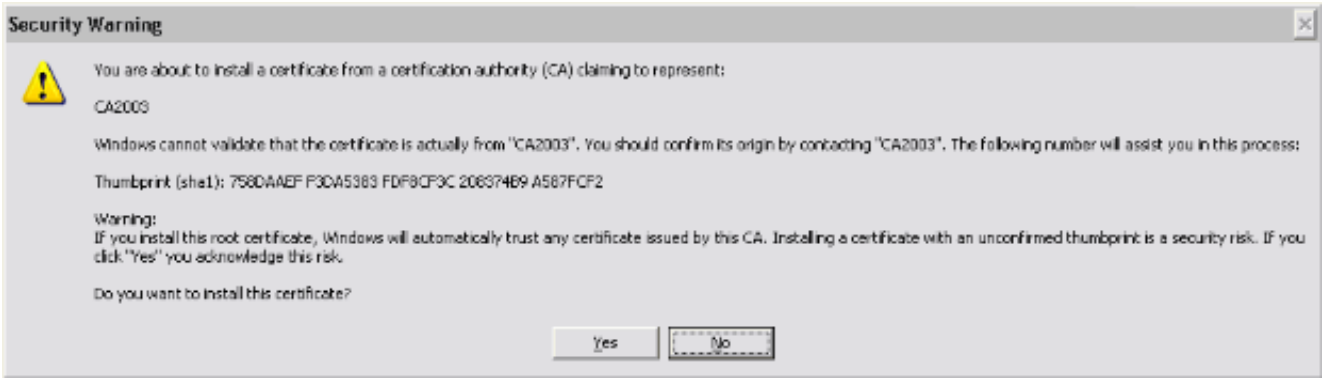
1. Start de AnyConnect-client en sluit u aan op het profiel van de

certenroll. AnyConnect geeft het inschrijvingsverzoek door aan de CA-server via

SCEP.AnyConnect gaat het inschrijvingsverzoek rechtstreeks in en gaat niet door de tunnel, als de knop **Get certificaatnummer** wordt

gebruikt.

2. Deze waarschuwing verschijnt. Klik op **Ja** om de gebruiker en het basiscertificaat te installeren



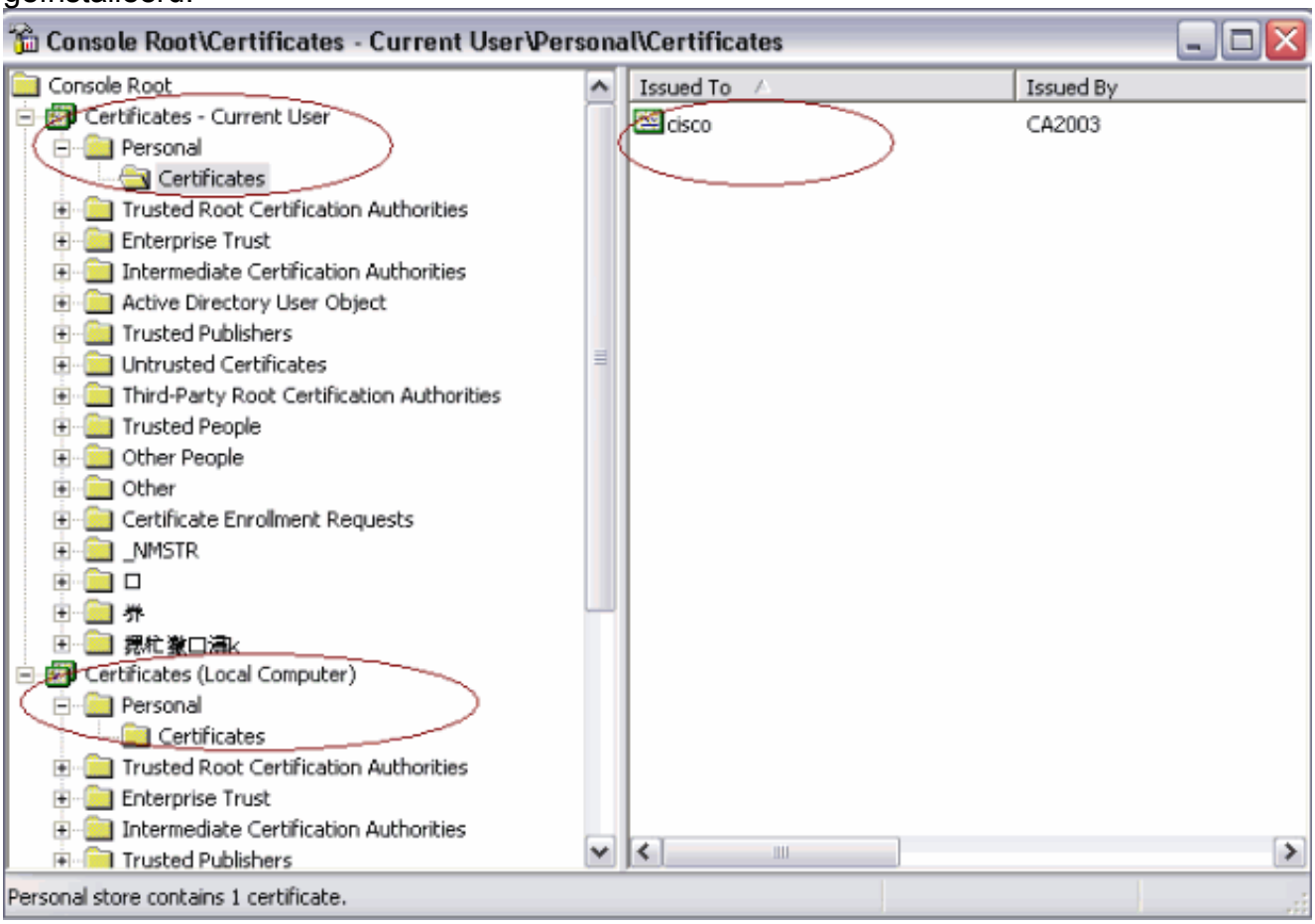
3. Zodra het certificaat is ingeschreven, sluit u het **veiligheidsprofiel aan**.

certificaatopslag op Microsoft Windows na SCEP-aanvraag

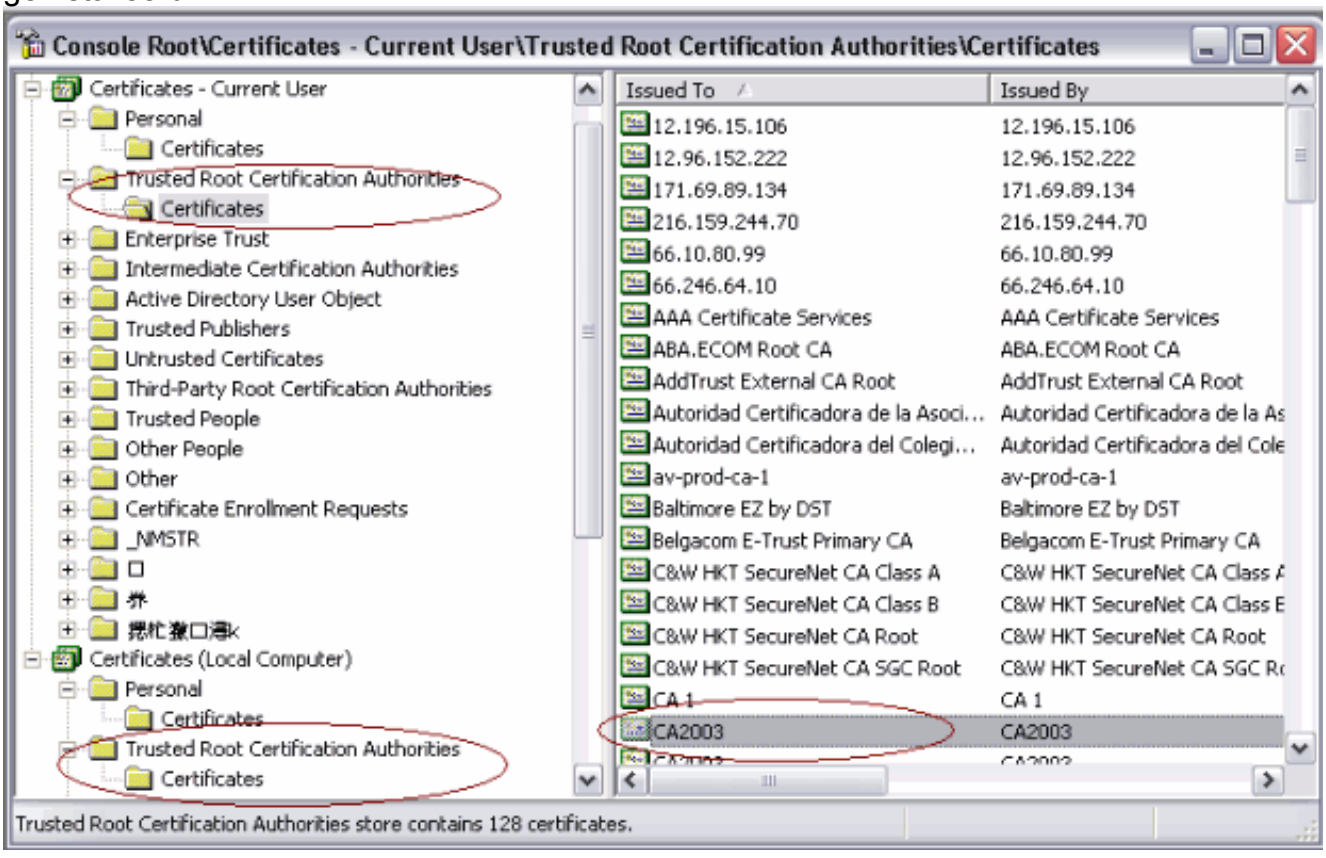
Voer de volgende stappen uit:

1. Klik op **Start > run > mmc**.
2. Klik op **Toevoegen/verwijderen**.

3. Klik op **Toevoegen** en kies **certificaten**.
4. Voeg de certificaten **van mijn gebruikersaccount** en **computeraccount toe**.In deze afbeelding is het gebruikerscertificaat weergegeven dat in de Windows-certificaatwinkel is geïnstalleerd:



In deze afbeelding is het CA-certificaat weergegeven dat in de Windows-certificaatwinkel is geïnstalleerd:



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- AnyConnect SCEP-inschrijving werkt alleen wanneer certificatie mislukt. Als dit niet het geval is, controleert u de certificaatwinkel. Als de certificaten al zijn geïnstalleerd, verwijdert u deze en test u het nogmaals.
- SCEP-inschrijving werkt niet tenzij de **ssl-certificatie interface buiten port 443** opdracht wordt gebruikt.Raadpleeg deze Cisco-pc's voor meer informatie:Cisco Bug ID CSCtf0678 (alleen geregistreerde klanten) —AnyConnect SCEP-inschrijving werkt niet bij Per Group Cert 2Cisco Bug ID CSCtf0684 (alleen geregistreerde klanten) —AnyConnect SCEP-inschrijving niet met ASA per groep werkt
- Als de CA server buiten ASA is, zorg er dan voor dat u het haarspelden toestaat met de **verbinding van de** vergunning **van het zelfde veiligheidsverkeer**. Voeg ook de buiten- en toegangslijst opdrachten toe zoals in dit voorbeeld:
  ```
  nat (outside) 1
  access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
  ```
  Waar 172.16.1.0 het AnyConnect-pool is en 171.69.89.87 het CA server IP-adres.
- Als de CA server binnen is, zorg ervoor dat deze in de gesplitste tunneltoegangslijst voor groepbeleid staat. In dit document wordt aangenomen dat de CA server binnen is.
  ```
  group-policy certenroll attributes
  split-tunnel-policy tunnelspecified
   split-tunnel-network-list value scep

  access-list scep standard permit 171.69.89.0 255.255.255.0
  ```

Gerelateerde informatie

- Cisco AnyConnect VPN-clientbeheerdershandleiding, release 2.4
- Technische ondersteuning en documentatie – Cisco Systems