ASA 8.X AnyConnect-verificatie met de Belgische eID-kaart

Inhoud

Inleiding

In dit document wordt beschreven hoe ASA 8.x moet worden ingesteld. AnyConnect-verificatie om de Belgische eID-kaart te gebruiken.

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:

- ASA 5505 met de juiste ASA 8.0-software
- AnyConnect-client
- ASDM 6.0

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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

De e-ID is een PKI (Public Key Infrastructure)-kaart die door de Belgische overheid is uitgegeven en die door gebruikers moet worden gebruikt om op een afgelegen Windows-PC te bevestigen. De AnyConnect-softwareclient wordt op de lokale pc geïnstalleerd en krijgt verificatiereferenties van de externe pc. Zodra de authenticatie is voltooid, krijgt de externe gebruiker toegang tot de centrale bronnen via een volledige SSL-tunnel. De externe gebruiker heeft een IP-adres dat afkomstig is van een pool die door de ASA wordt beheerd.

Local PC Setup

Besturingssysteem

Het besturingssysteem (Windows, MacOS, Unix of Linux) op uw lokale pc moet actueel zijn terwijl alle benodigde patches zijn geïnstalleerd.

Kaartlezer

Er moet een elektronische kaartlezer op uw lokale computer geïnstalleerd zijn om de e-ID-kaart te kunnen gebruiken. De elektronische kaartlezer is een hardware-instrument dat een communicatiekanaal vormt tussen de programma's op de computer en de chip op de ID-kaart.

Raadpleeg deze URL voor een lijst met goedgekeurde kaartlezers:
http://www.cardreaders.be/en/default.htm

Opmerking: Om de kaartlezer te kunnen gebruiken, dient u de stuurprogramma's te installeren die door de hardwareverkoper worden aanbevolen.

Software voor eID Runtime

U moet de eID-software installeren die door de Belgische regering is geleverd. Met deze software kan de externe gebruiker de inhoud van de eID-kaart lezen, valideren en afdrukken. De software is beschikbaar in het Frans en Nederlands voor Windows, MAC OS X en Linux.

Raadpleeg voor meer informatie deze URL:

- http://www.belgium.be/zip/eid_datacapture_nl.html

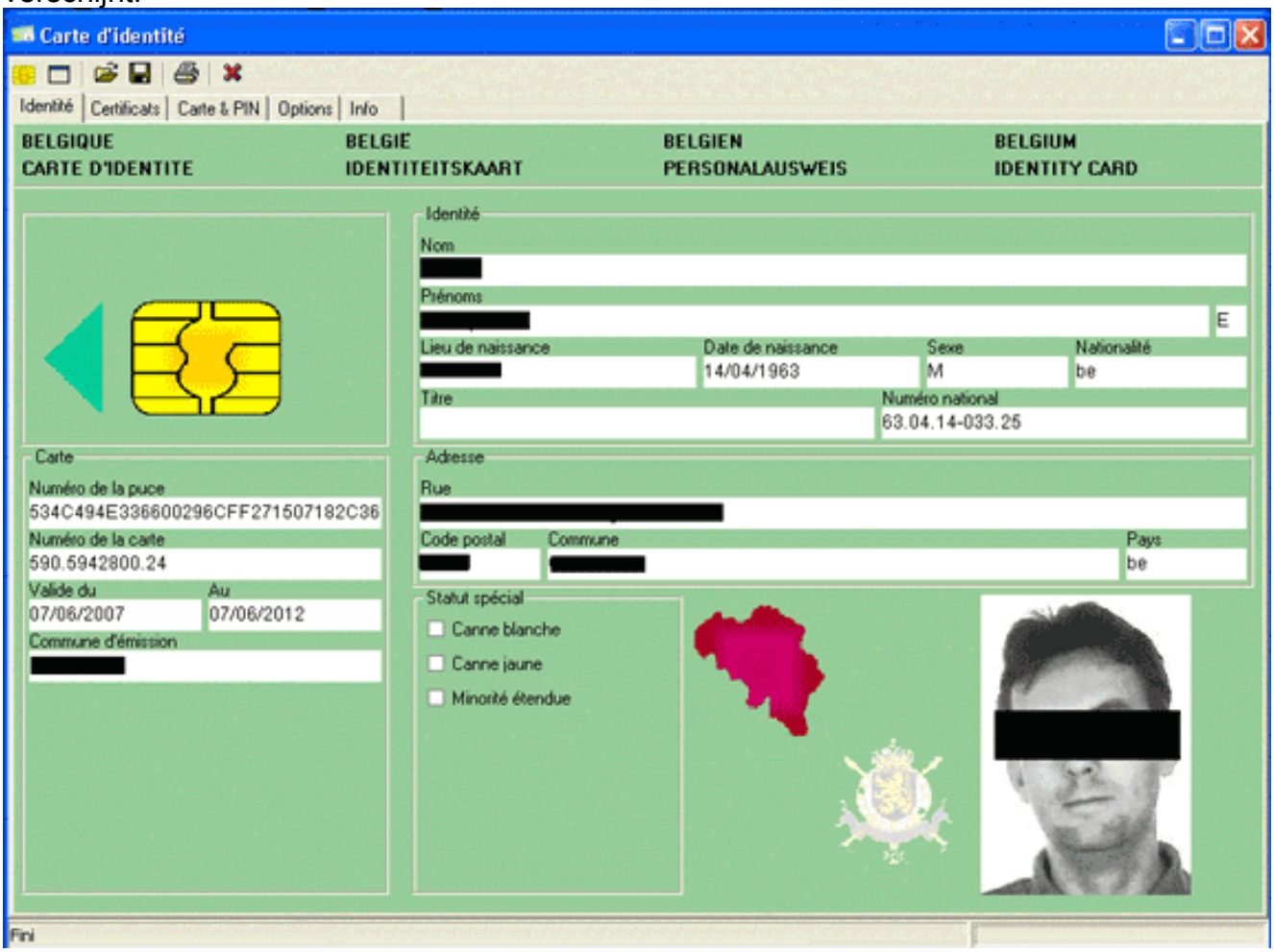
Verificatiebewijs

U moet het authenticatiecertificaat importeren in de Microsoft Windows-winkel op de lokale pc. Als u het certificaat niet in de winkel importeert, kan de AnyConnect-client geen SSL-verbinding met de ASA opzetten.

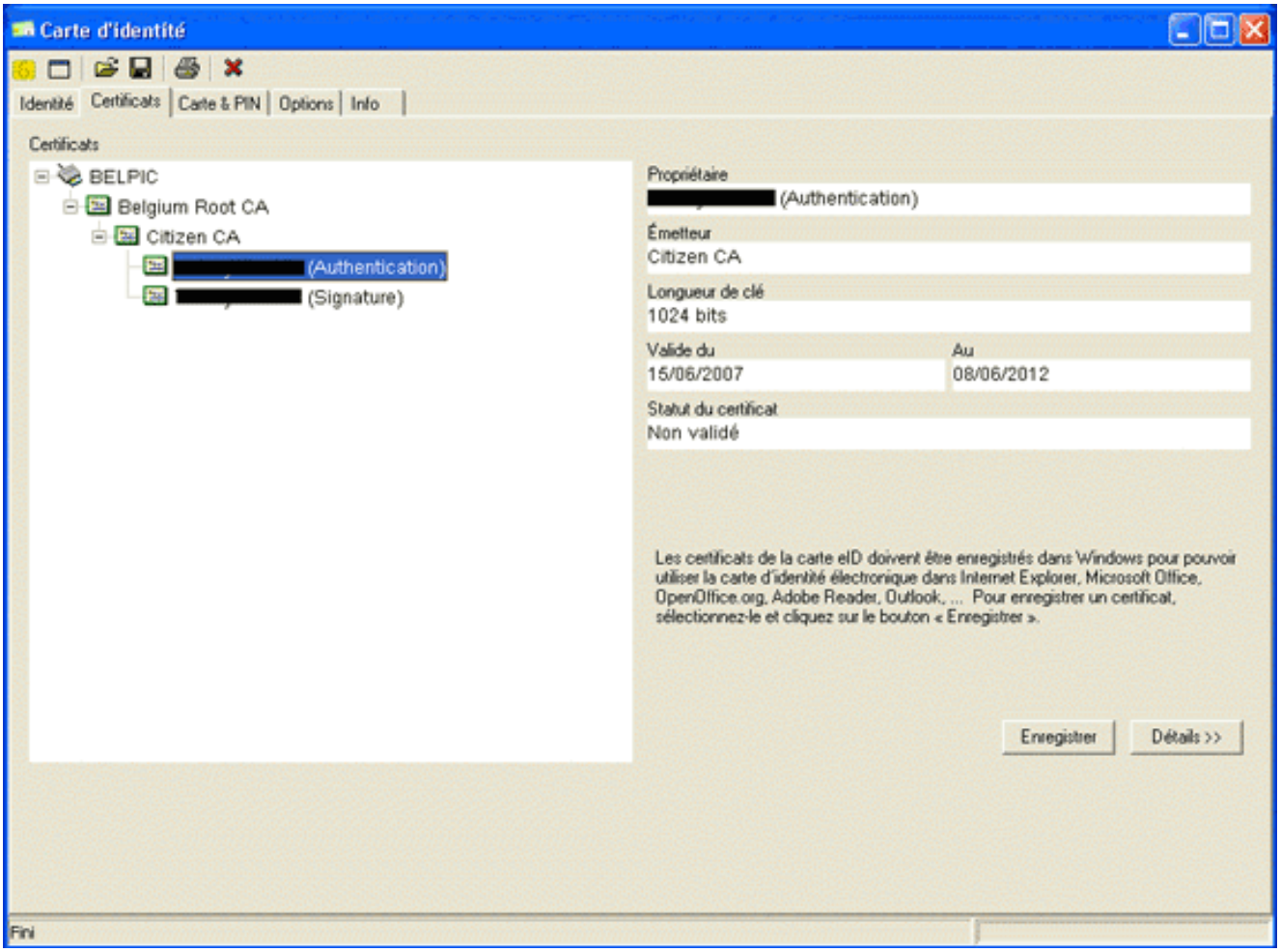
Procedure

Voltooi de volgende stappen om het echtheidscertificaat in de Windows-winkel te importeren:

1. Plaats uw e-id in de kaartlezer en start de middleware om toegang te krijgen tot de inhoud van de eID-kaart.De inhoud van de eID-kaart verschijnt.



2. Klik op het tabblad **Certificaten** (FR).De hiërarchie van certificaten wordt weergegeven.



3. Uitbreidt **België Root CA**, en vergroot vervolgens **Citizen CA**.
4. Kies de versie van **de** verificatie van uw benoemde certificaat.
5. Klik op de knop **Enregistrer** (FR).Het certificaat wordt naar de Windows-winkel gekopieerd.

Opmerking: Wanneer u op de knop **Details** klikt, verschijnt er een venster met informatie over het certificaat. Selecteer in het tabblad Details het veld **Onderwerp** om het veld Serienummer weer te geven. Het veld Serienummer bevat een unieke waarde die wordt gebruikt voor de gebruikersautorisatie. Het serienummer "56100307215" vertegenwoordigt bijvoorbeeld een gebruiker waarvan de geboortedatum 3 oktober 1956 is, met een volgnummer van 072 en een controlecijfer van 15. *U moet een verzoek om goedkeuring bij de federale overheid indienen om deze nummers op te slaan. Het is uw verantwoordelijkheid om de juiste officiële verklaringen af te leggen in verband met het bijhouden van een gegevensbank van Belgische burgers in uw land.*

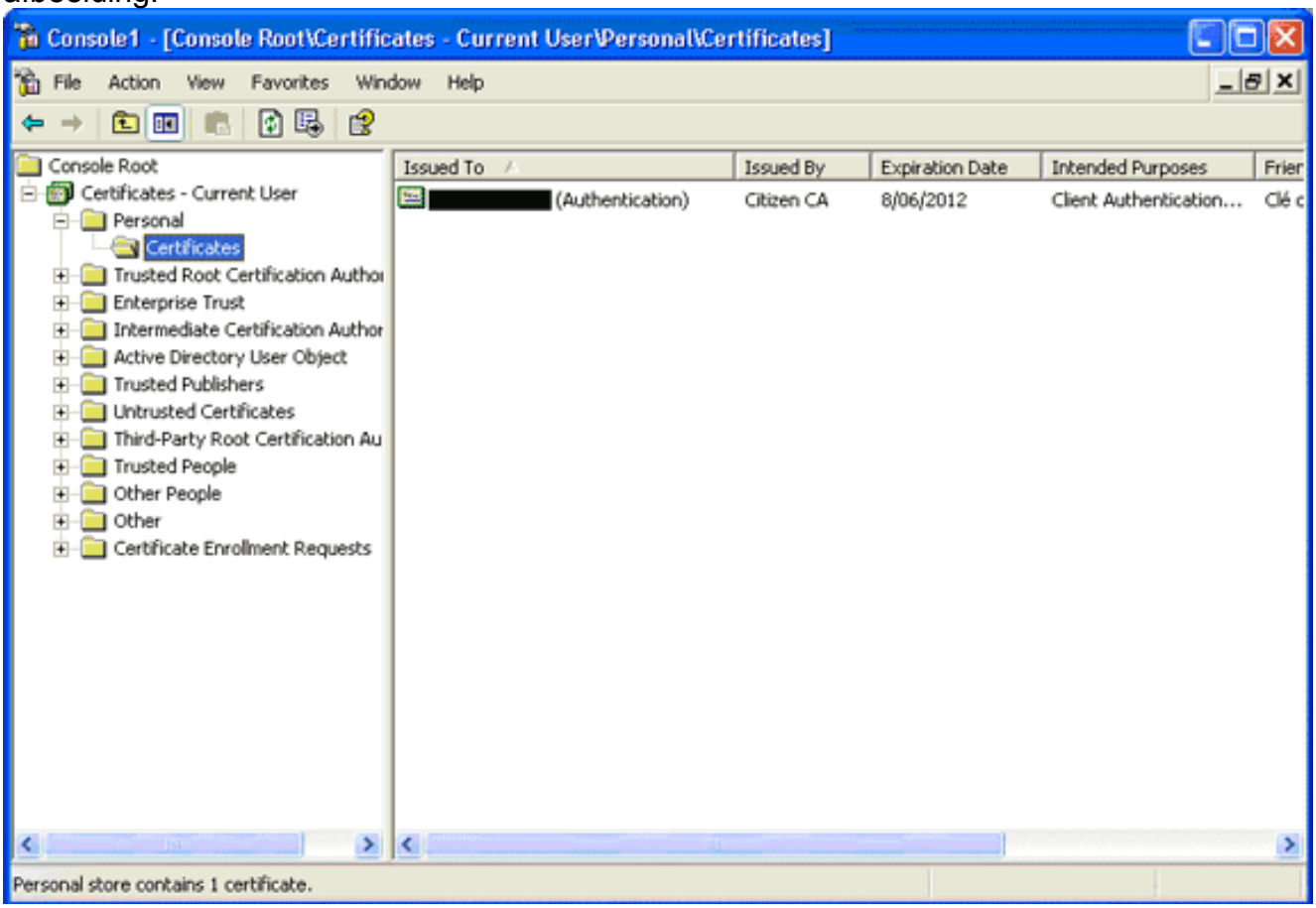
Verifiëren

Voltooi de volgende stappen om te controleren of het ingevoerde certificaat succesvol is:

1. Open in een Windows XP-machine een DOS-venster en typ de **mmc-**opdracht.De console-toepassing verschijnt.
2. Kies **Bestand > Magnetisch toevoegen/verwijderen** (of druk op Ctrl+M).Het dialoogvenster Magnetisch toevoegen/verwijderen verschijnt.
3. Klik op de knop **Toevoegen**.Het dialoogvenster Magnetisch-in toevoegen verschijnt.
4. Selecteer in de lijst Beschikbare standalone magnetisch-ins de optie **Certificaten** en klik op **Toevoegen**.
5. Klik op het keuzerondje **Mijn gebruikersaccount** en klik op **Voltooien**.Het programma Uitlijning van het certificaat verschijnt in het dialoogvenster Magnetisch toevoegen/verwijderen.
6. Klik op **Sluiten** om het dialoogvenster Magnetisch in-stand toevoegen te sluiten en

vervolgens op **OK** in het dialoogvenster Toevoegen/Verwijderen Magnetisch-in te klikken om uw wijzigingen op te slaan en naar de console-toepassing terug te keren.

7. Vul onder de map console Root de optie **Certificaten uit - Huidige gebruiker**.
8. **Persoonlijk** uitvouwen en **Certificaten** vervolgens uitvouwen.Het geïmporteerde certificaat moet in de Windows-winkel verschijnen zoals in deze afbeelding:



AnyConnect-installatie

U moet de AnyConnect-client op de externe pc installeren. De AnyConnect-software gebruikt een XML-configuratiebestand dat kan worden bewerkt om een lijst met beschikbare gateways vooraf in te stellen. Het XML bestand wordt in dit pad op de afstandsbediening opgeslagen:

C:\Documents and Settings*%USERNAME%*\Application Data\Cisco\Cisco AnyConnect VPN Client

waarbij *%USERNAME%* de naam van de gebruiker op de externe pc is.

De naam van het XML-bestand is *preferenties.xml*. Hier volgt een voorbeeld van de inhoud van het bestand:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

waar *192.168.0.1* het IP-adres van de ASA gateway is.

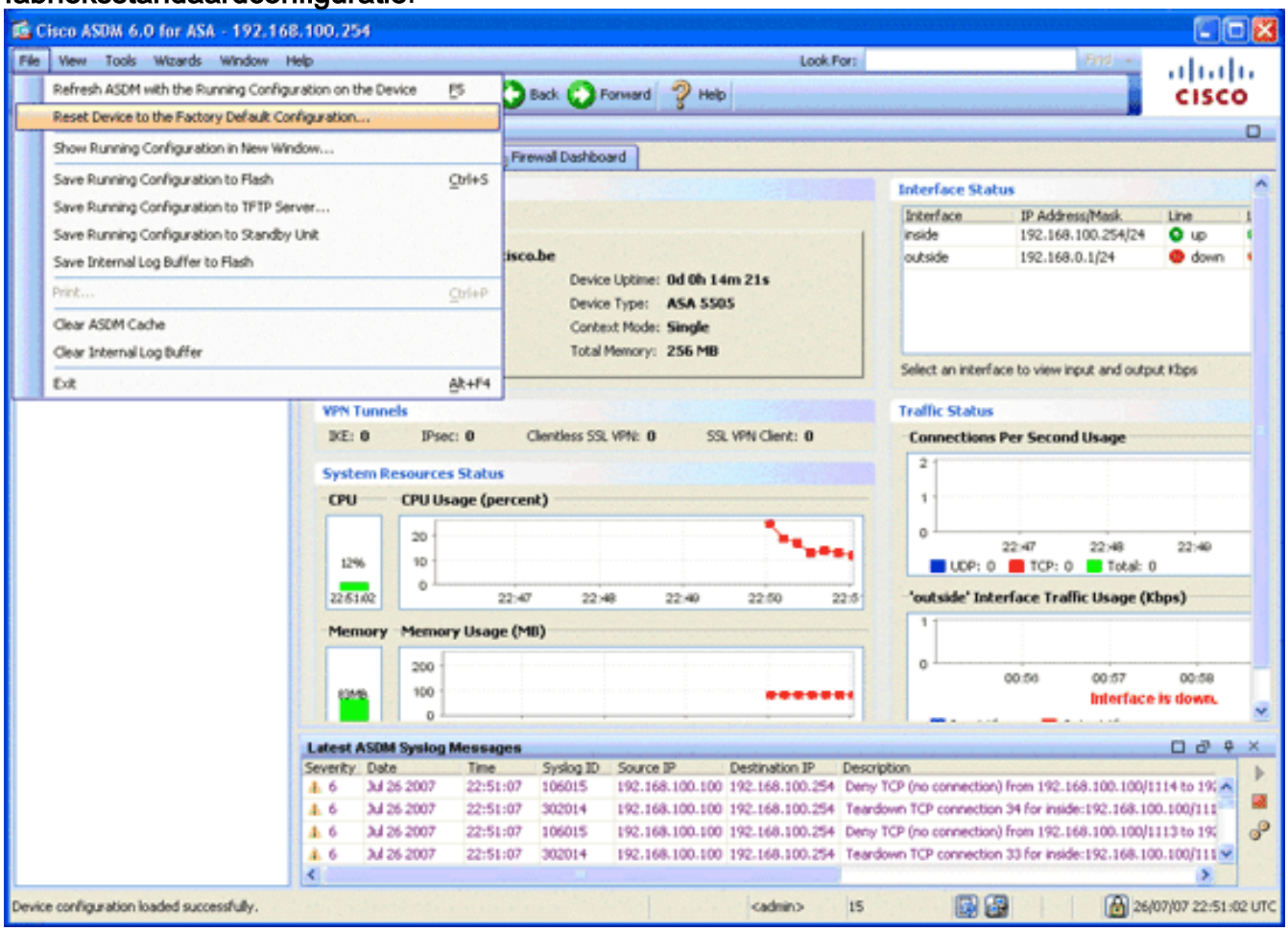
ASA-vereisten

Zorg ervoor dat de ASA aan deze eisen voldoet:

- AnyConnect en ASDM moeten in flitser worden uitgevoerd.Om de procedures in dit document te voltooien, gebruikt u een ASA 5505 met de juiste ASA 8.0 software geïnstalleerd. De AnyConnect- en ASDM-toepassingen moeten in flitser worden voorgeladen. Gebruik de opdracht **flitser tonen** om de inhoud van flitser te bekijken:

```
ciscoasa#show flash:
--#--  --length--  -----date/time------  path
   66  14524416    Jun 26 2007 10:24:02  asa802-k8.bin
   67  6889764     Jun 26 2007 10:25:28  asdm-602.bin
   68  2635734     Jul 09 2007 07:37:06  anyconnect-win-2.0.0343-k9.pkg
```

- ASA moet uitgevoerd worden met fabrieksinstellingen.U kunt deze eis overslaan als u een nieuw ASA-chassis gebruikt om de procedures in dit document te voltooien. Voltooi anders deze stappen om de standaardinstellingen van de ASA te herstellen:Sluit in de ASDM-toepassing aan op het ASA-chassis en kies **Bestand > Apparaat opnieuw instellen op de fabrieksstandaardconfiguratie**.



Laat de standaardwaarden in de sjabloon staan.Sluit uw PC op de Ethernet 0/1 binneninterface aan en vervang uw IP-adres dat voorzien zal worden door de DHCP-server van de ASA.**Opmerking:** Gebruik deze opdrachten om de standaardinstellingen van de ASA terug te stellen op de fabriek:

```
ciscoasa#conf t
ciscoasa#config factory-default 192.168.0.1 255.255.255.0
```

ASA-configuratie

Nadat u de standaardinstellingen van de ASA-fabriek hebt hersteld, kunt u ASDM op 192.168.0.1 starten om verbinding te maken met de ASA op de Ethernet 0/1 interne interface.

Opmerking: Uw vorige wachtwoord is bewaard gebleven (of het kan standaard leeg zijn).

Standaard accepteert de ASA een inkomende beheersessie met een bron IP-adres in het subsysteem 192.168.0.0/24. De standaard DHCP-server die is ingeschakeld op de interne interface van de ASA biedt IP-adressen in het bereik 192.168.0.2-129/24, geldig om verbinding te maken met de interne interface met ASDM.

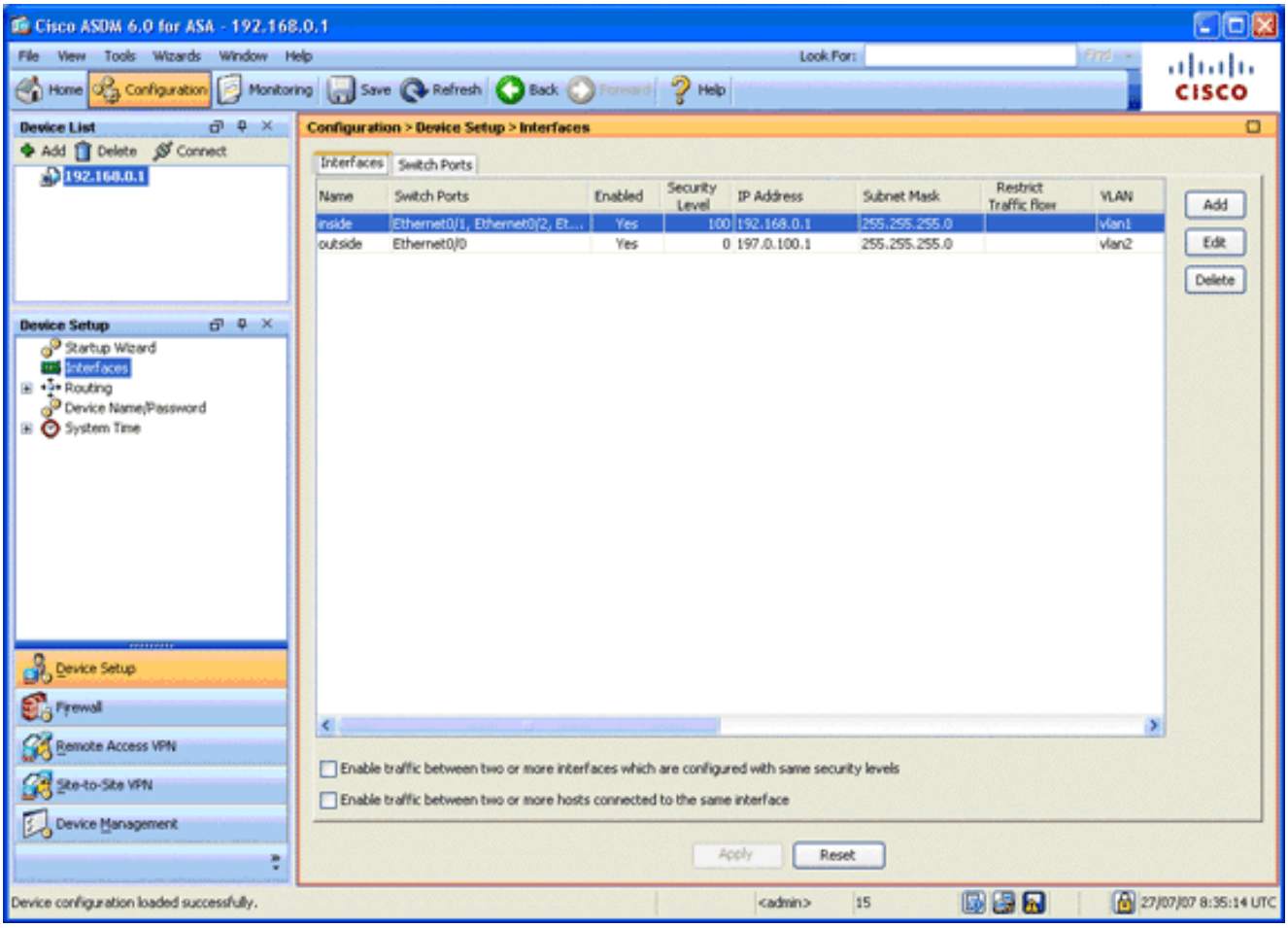
Voltooi deze stappen om de ASA te configureren:

1. Schakel de externe interface in
2. Domain Name, Password en System Time configureren
3. Een DHCP-server op externe interface inschakelen
4. De e-ID VPN-adresgroep configureren
5. Importeer het België Root CA-certificaat
6. Secure Socket Layer configureren
7. Het standaardgroepsbeleid definiëren
8. De certificaattoewijzing definiëren
9. Een lokale gebruiker toevoegen
10. Herstart de ASA

Stap 1. Schakel de buiteninterface in

In deze stap wordt beschreven hoe u de externe interface kunt inschakelen.

1. Klik in de ASDM-toepassing op **Configuration** en vervolgens op **Devices Setup**.
2. Kies in het gebied Setup-apparaat **interfaces** en klik vervolgens op het tabblad **Interfaces**.

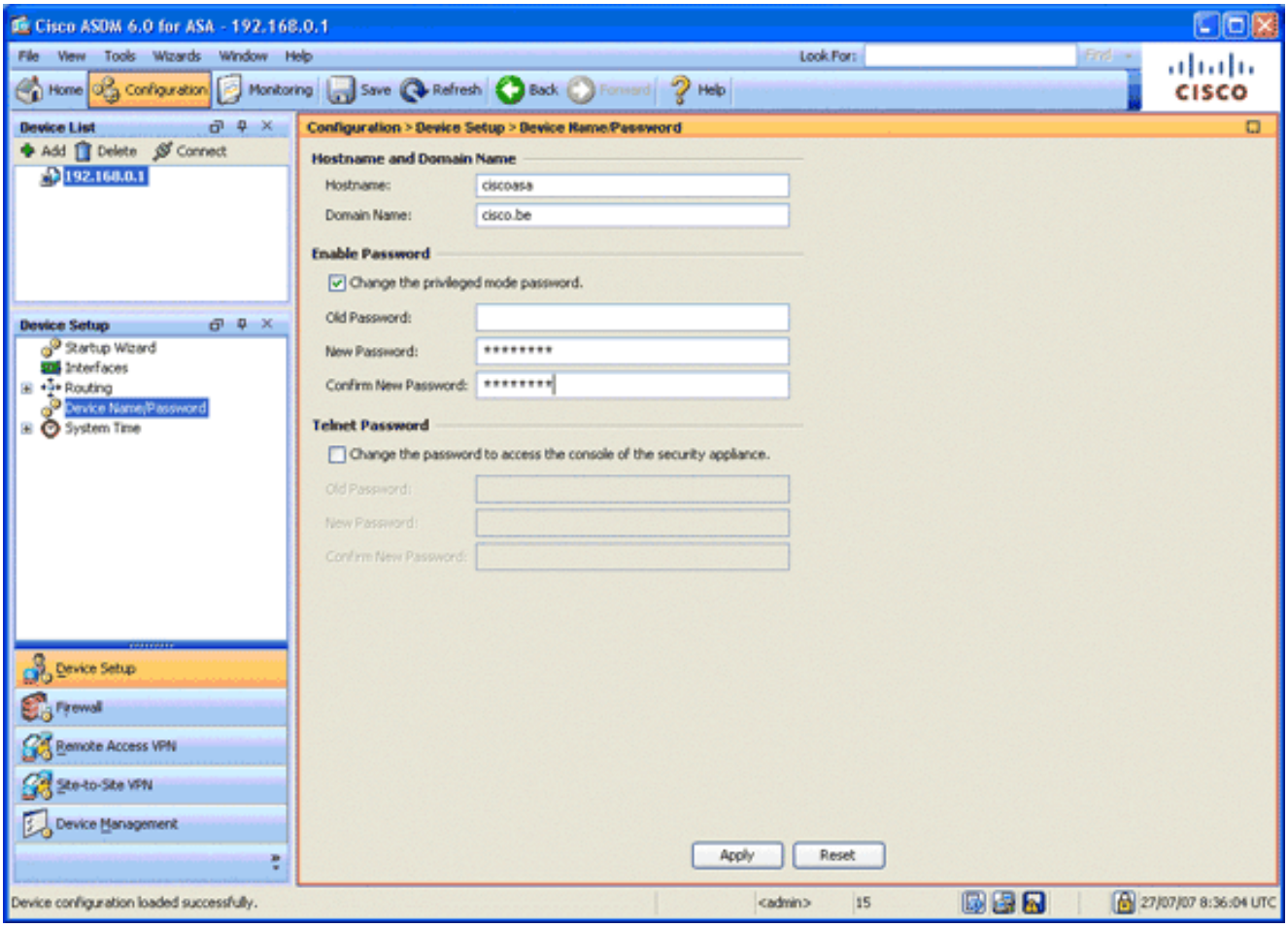


3. Selecteer de externe interface en klik op **Bewerken**.
4. Kies op het tabblad Algemeen de optie **Statische IP** gebruiken.
5. Voer **197.0.100.1 in** voor het IP-adres en **255.255.255.0** voor het subnetmasker.
6. Klik op **Apply** (Toepassen).

Stap 2. Configuratie van de domeinnaam, het wachtwoord en de systeemtijd

In deze stap wordt beschreven hoe u de domeinnaam, het wachtwoord en de systeemtijd kunt configureren.

1. Kies in het gebied Instellingen apparaat de **naam/het wachtwoord**.

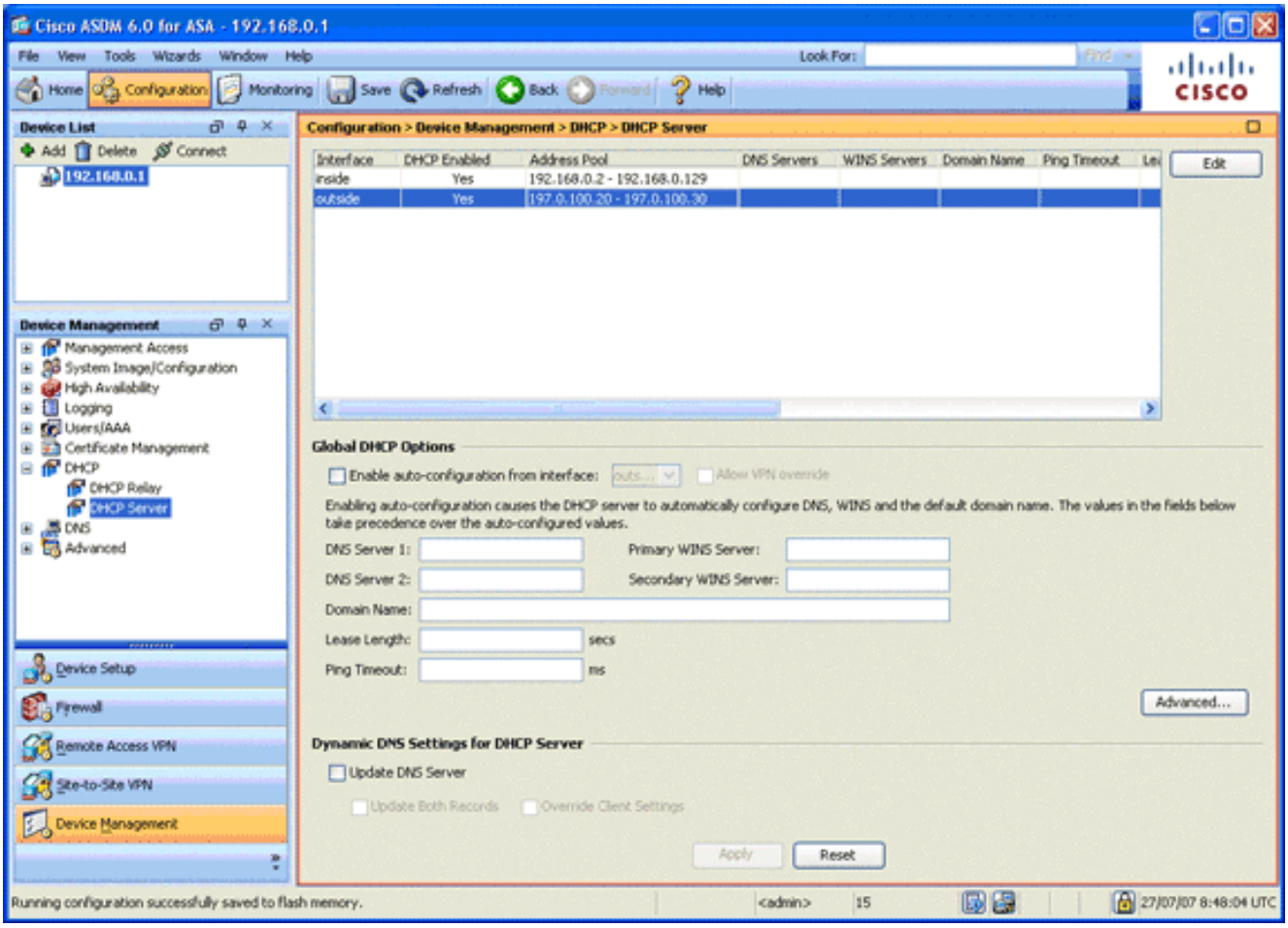


2. Voer **cisco.be in** voor de domeinnaam en voer **cisco123 in** voor de waarde Wachtwoord voor inschakelen.**Opmerking:** standaard is het wachtwoord leeg.
3. Klik op **Apply** (Toepassen).
4. Kies in het gebied Setup **Apparaat de optie Systeemtijd** en verander de klokwaarde (indien nodig).
5. Klik op **Apply** (Toepassen).

Stap 3. Schakel een DHCP-server in op de externe interface.

In deze stap wordt beschreven hoe een DHCP-server op de externe interface kan worden ingeschakeld om het testen te vergemakkelijken.

1. Klik op **Configuration** en vervolgens op **Apparaatbeheer**.
2. In het gebied van het Apparaatbeheer, breid **DHCP uit** en kies **DHCP Server**.

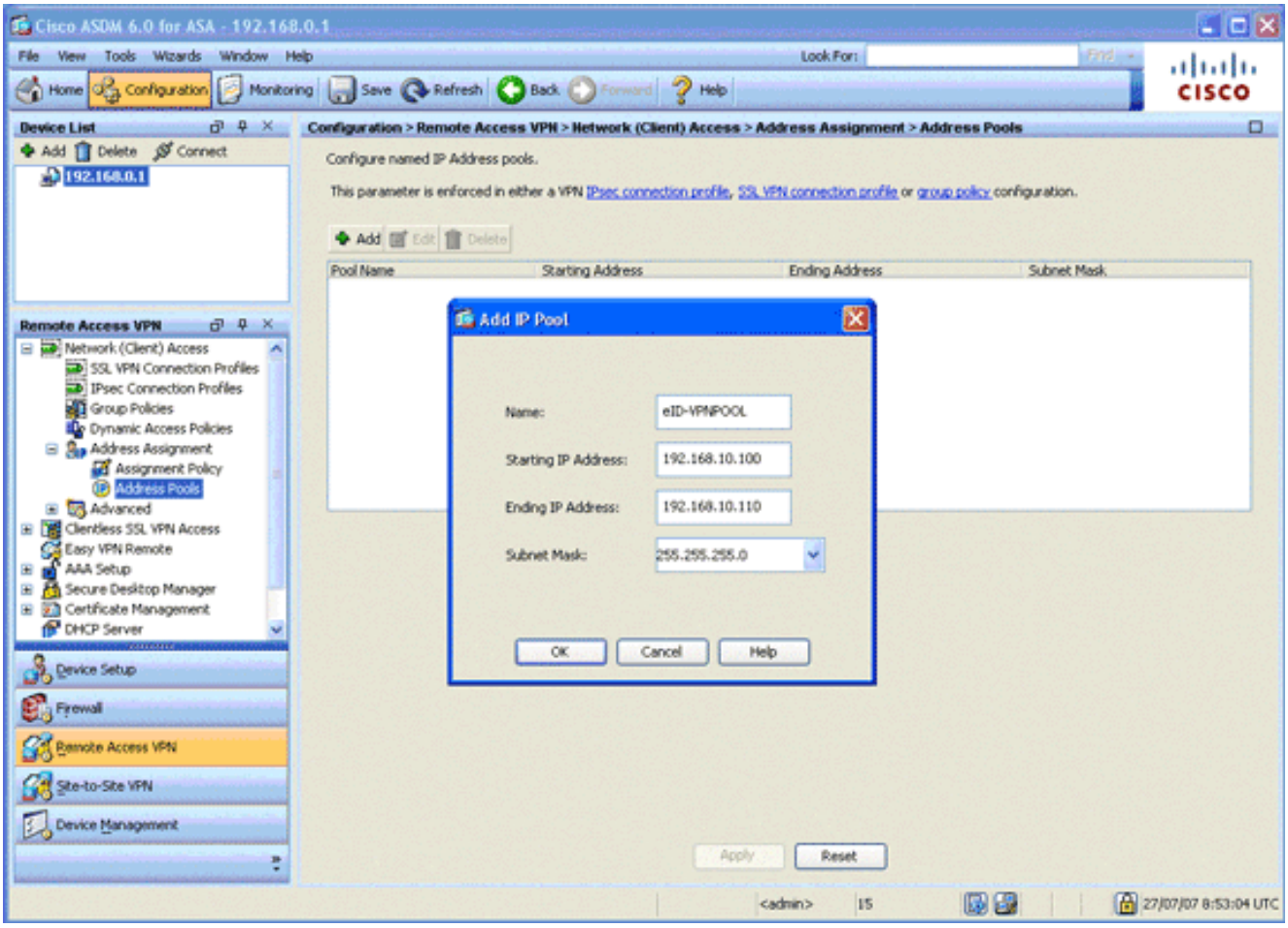


3. Selecteer de externe interface in de lijst Interface en klik op **Bewerken**.Het dialoogvenster DHCP-server bewerken verschijnt.
4. Controleer het vakje **DHCP-server inschakelen**.
5. Voer in de DHCP-adresgroep een IP-adres in van 197.0.100.20 tot 197.0.100.30.
6. Schakel in het gebied Global DHCP-opties de **automatische configuratie inschakelen uit** om het vakje **te** controleren.
7. Klik op **Apply** (Toepassen).

Stap 4. Configuratie van de e-ID VPN-adresgroep

In deze stap wordt beschreven hoe u een pool van IP-adressen kunt definiëren die gebruikt worden om de externe AnyConnect-clients aan te bieden.

1. Klik op **Configuration** en klik vervolgens op **Remote Access VPN**.
2. In het gebied Access VPN verwijderen, **dient u Network (Client) Access** uit te vouwen en vervolgens **adrestoewijzing** uit te vouwen.
3. Kies **Adres Pools**, en klik dan de **Add** knop in het gedeelte Configure genoemde IP Address pools.Het dialoogvenster Wol toevoegen
verschijnt.



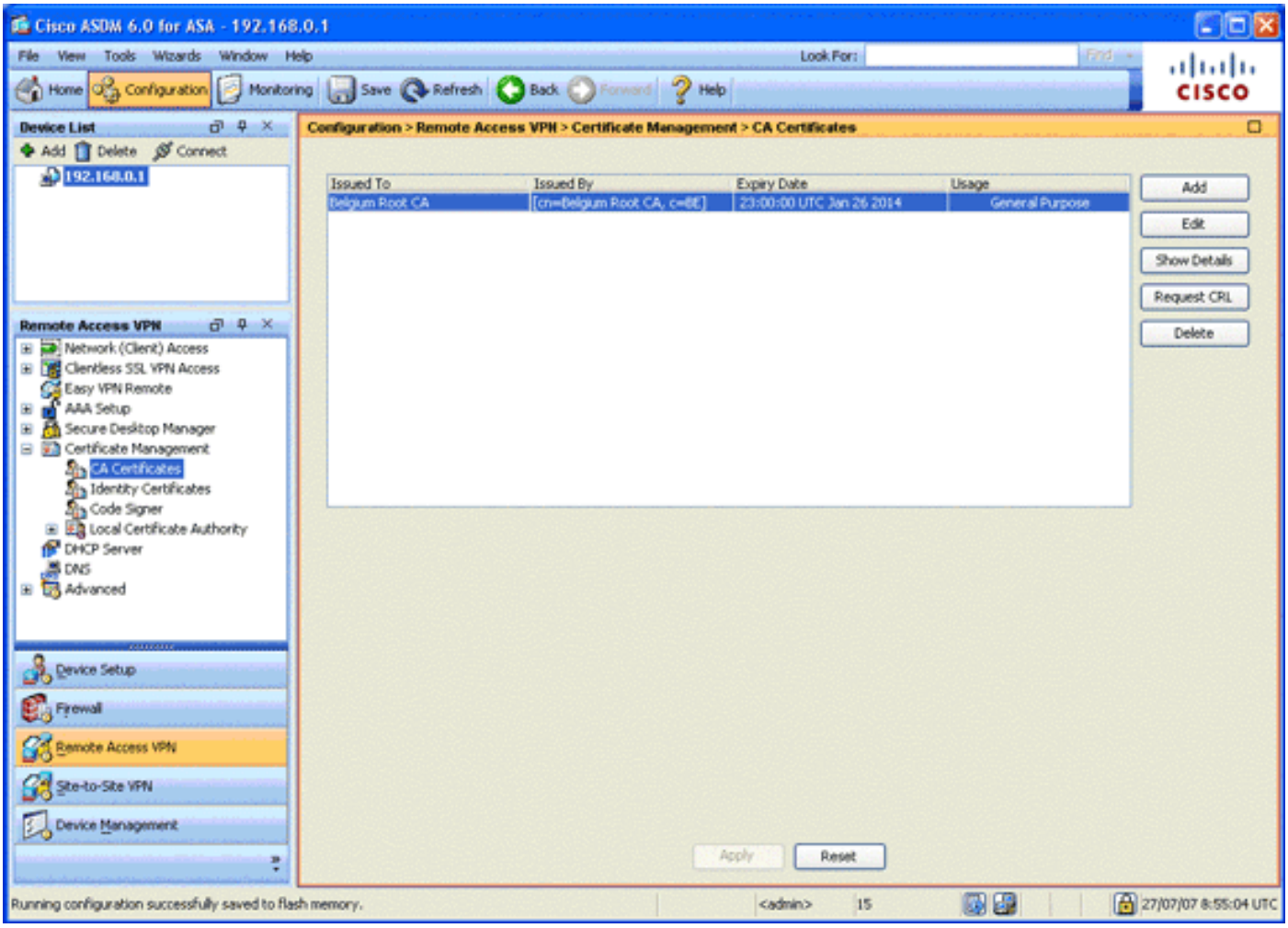
4. Voer in het veld Naam **eID-VPL in**.
5. Voer in de velden IP-adres starten en eindigen een bereik van IP-adres in van 192.168.10.100 tot 192.168.10.110.
6. Kies **255.255.255.0** uit de vervolgkeuzelijst Subnetmasker, klik op **OK** en klik vervolgens op **Toepassen**.

Stap 5. Importeer het Belgische Root CA-certificaat

In deze stap wordt beschreven hoe in de ASA het Belgisch Root CA-certificaat wordt ingevoerd.

1. Download en installeer de Belgische Root CA-certificaten (belgiumrca.crt en belgiumrca2.crt) van de overheidswebsite en bewaar deze op uw lokale pc.De Belgische overheidswebsite bevindt zich op deze URL: http://certs.eid.belgium.be/
2. In het gebied van de Externe Toegang VPN, breid **certificaatbeheer uit** en kies **CA-certificaten**.
3. Klik op **Add** en vervolgens op **Install uit bestanden**.
4. Bladeren naar de locatie waar u het Belgie Root CA-certificaat (belgiumrca.crt) hebt opgeslagen en op **Installeer certificaatdocument** klikken.
5. Klik op **Toepassen** om de wijzigingen op te slaan.

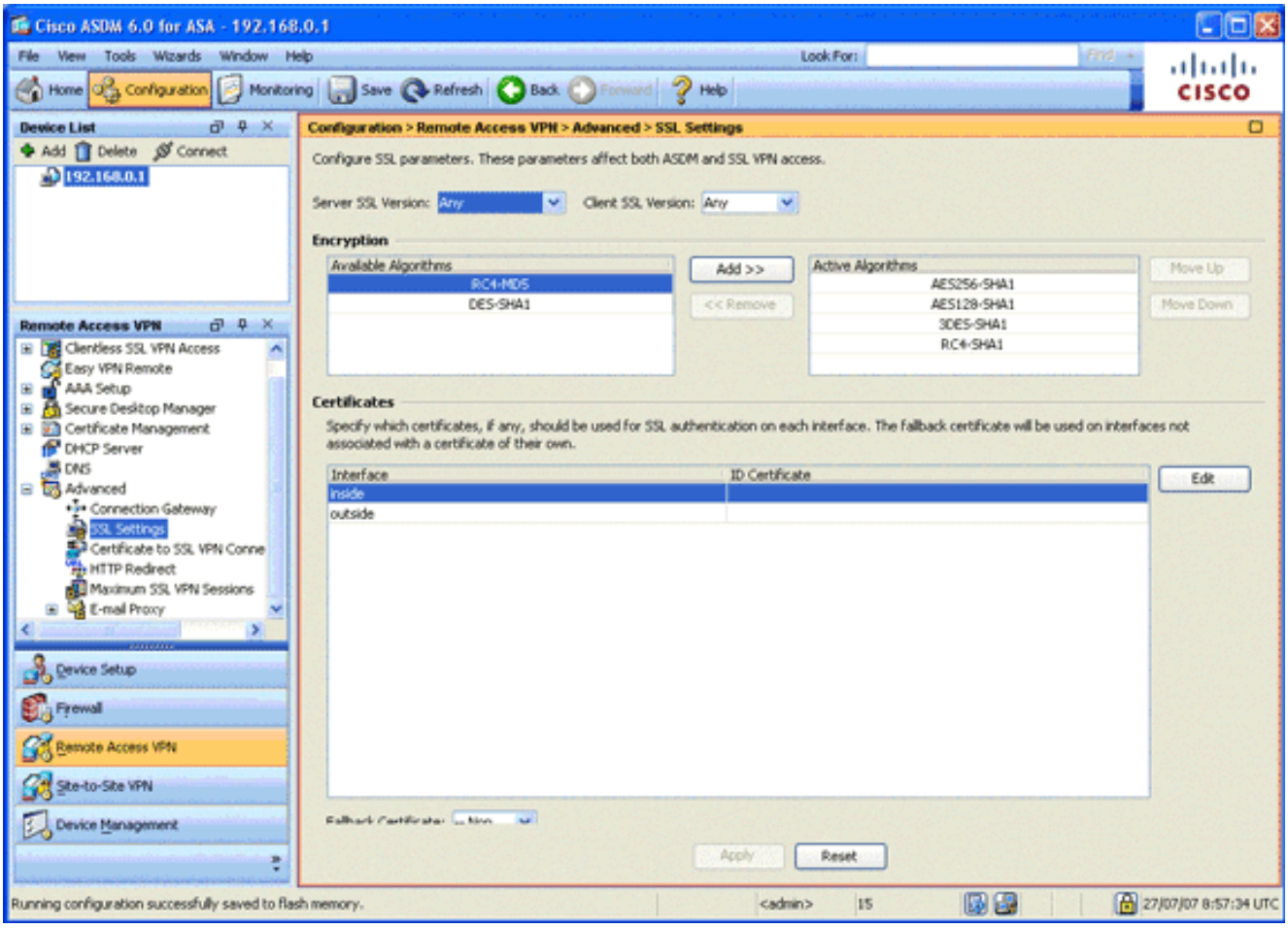
Deze afbeelding toont het certificaat dat op de ASA is geïnstalleerd:



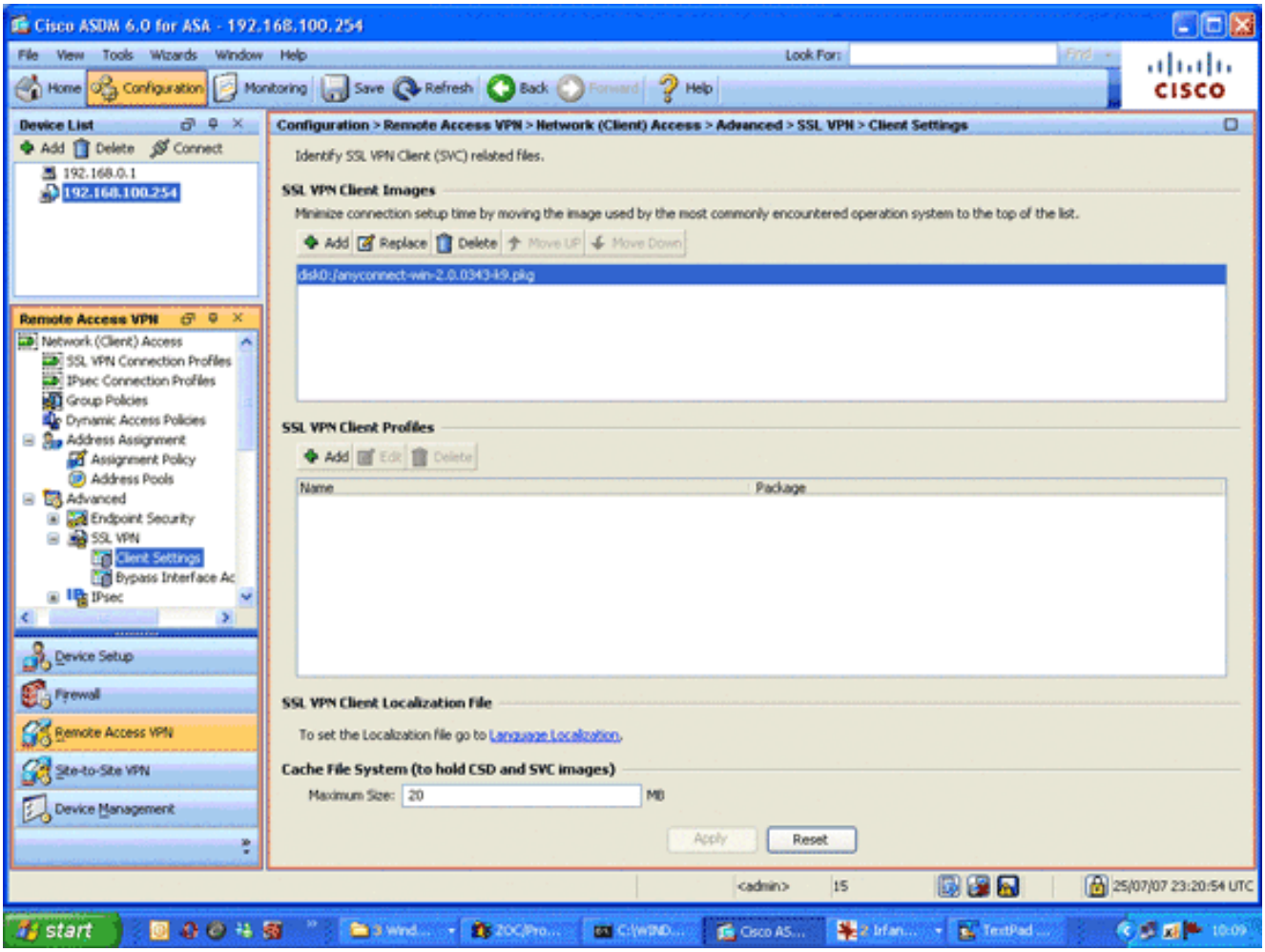
Stap 6. Het configureren van beveiligde contactdoos

In deze stap wordt beschreven hoe u prioriteit geeft aan beveiligde encryptieopties, hoe u het SSL VPN-clientbeeld definieert en het verbindingsprofiel definieert.

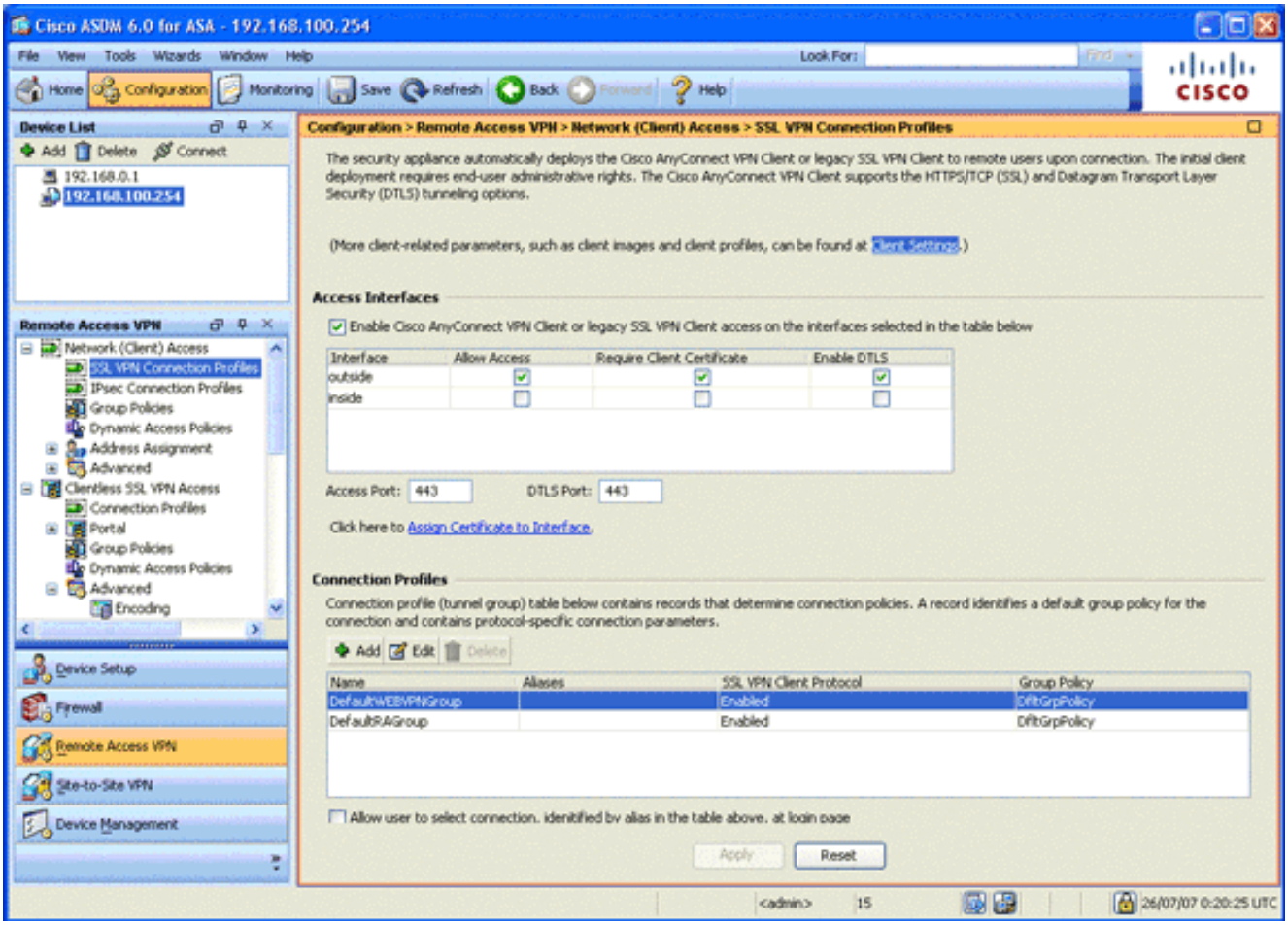
1. Prioriseer de best beveiligde encryptieopties.In het gebied van de Toegang van Afstandsbediening VPN, uitvouwen **Geavanceerd** en kies **SSL Instellingen**. In het gedeelte Encryptie worden de actieve algoritmen gestapeld, bovenaan als volgt:AES256-SHA1AES128-SHA13DES-SHA1RC4-
SHA1



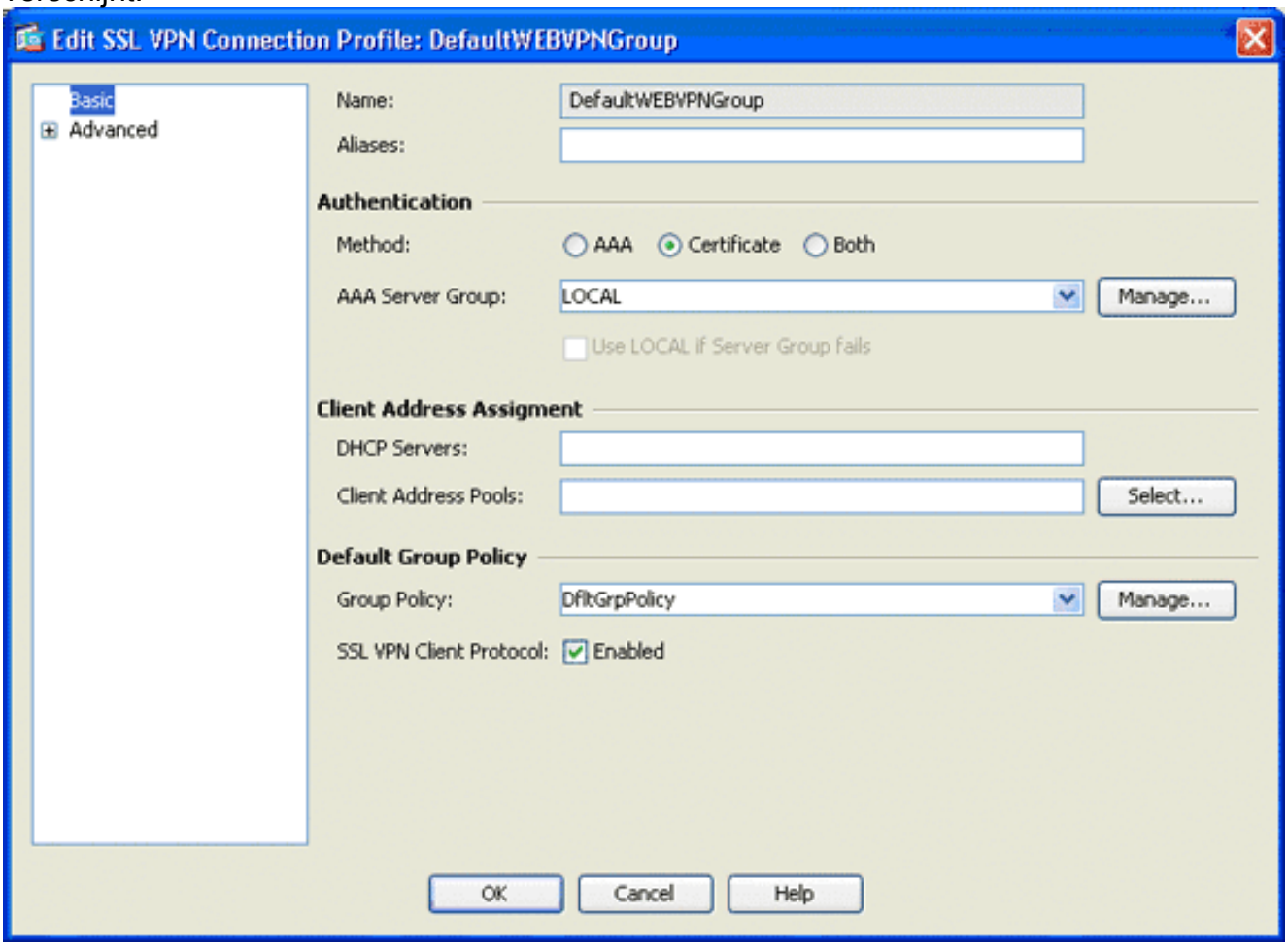
2. Defineert het SSL VPN-clientbeeld voor de AnyConnect-client.In het gebied Externe Toegang VPN vouwt u **Advanced** uit, vouwt u **SSL VPN uit** en kiest u **Clientinstellingen**.Klik in het gebied SSL VPN-clientafbeeldingen op **Toevoegen**.Kies het AnyConnect-pakket dat in flitser is opgeslagen.Het AnyConnect-pakket verschijnt in de lijst SSL VPN-clientafbeeldingen zoals in deze
afbeelding:



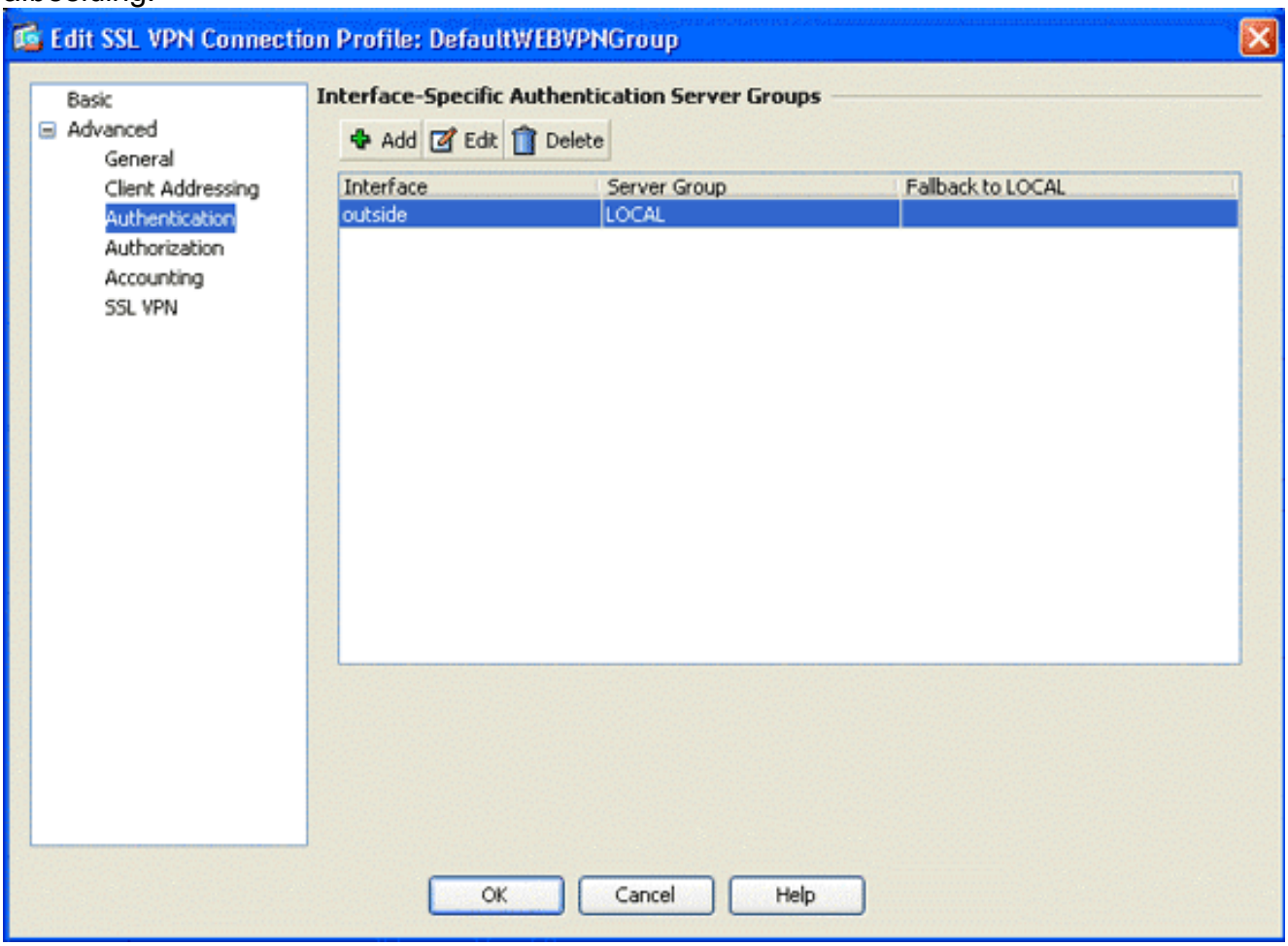
3. Defineert het verbindingsprofiel DefaultWEBVPL.In het gebied van de Afstandstoegang VPN, **breid** de **Toegang tot het netwerk (van de client) uit** en kies **SSL VPN Connection profielen**.Controleer in het gebied Access Interfaces het **vakje Cisco AnyConnect VPN-client inschakelen**.Controleer voor de externe interface de vinkjes **Toegang toestaan**, **Clientcertificaat eisen** en **DTLS inschakelen** zoals in dit beeld wordt weergegeven:



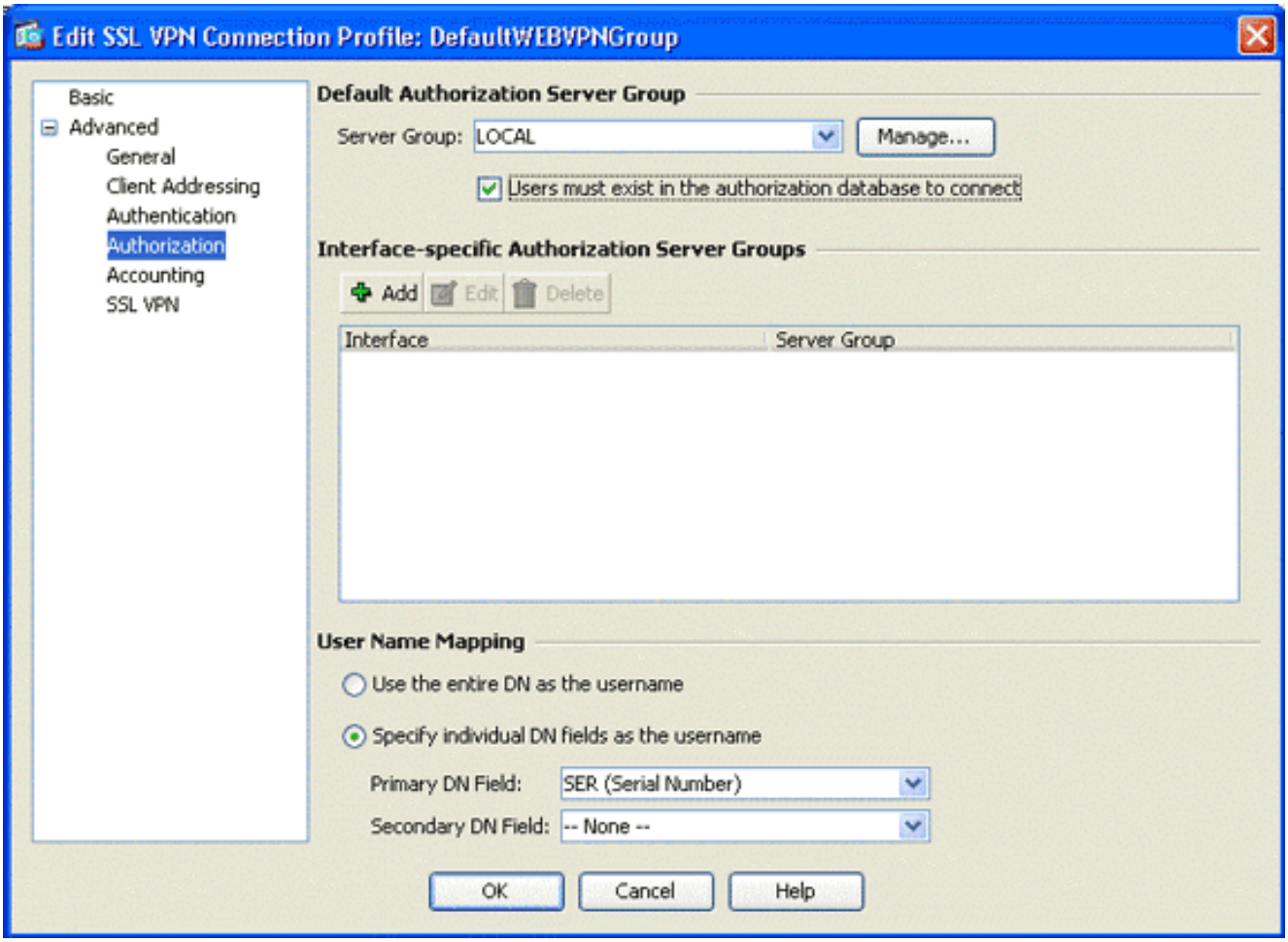
Kies in het gebied **verbindingsprofielen** de optie **DefaultWEBVPN** en klik op **Bewerken**.Het dialoogvenster SSL VPN-verbindingsprofiel bewerken verschijnt.



Kies in het navigatiegebied **basis**.Klik in het verificatiegebied op de knop **certificaatradio**.Controleer in het gedeelte Default Group Policy het vakje **SSL VPN-clientprotocol**.**Geavanceerde** uitvouwen, en kiezen **Verificatie**.Klik op **Add** en voeg de externe interface toe met een lokale servergroep zoals in deze afbeelding:



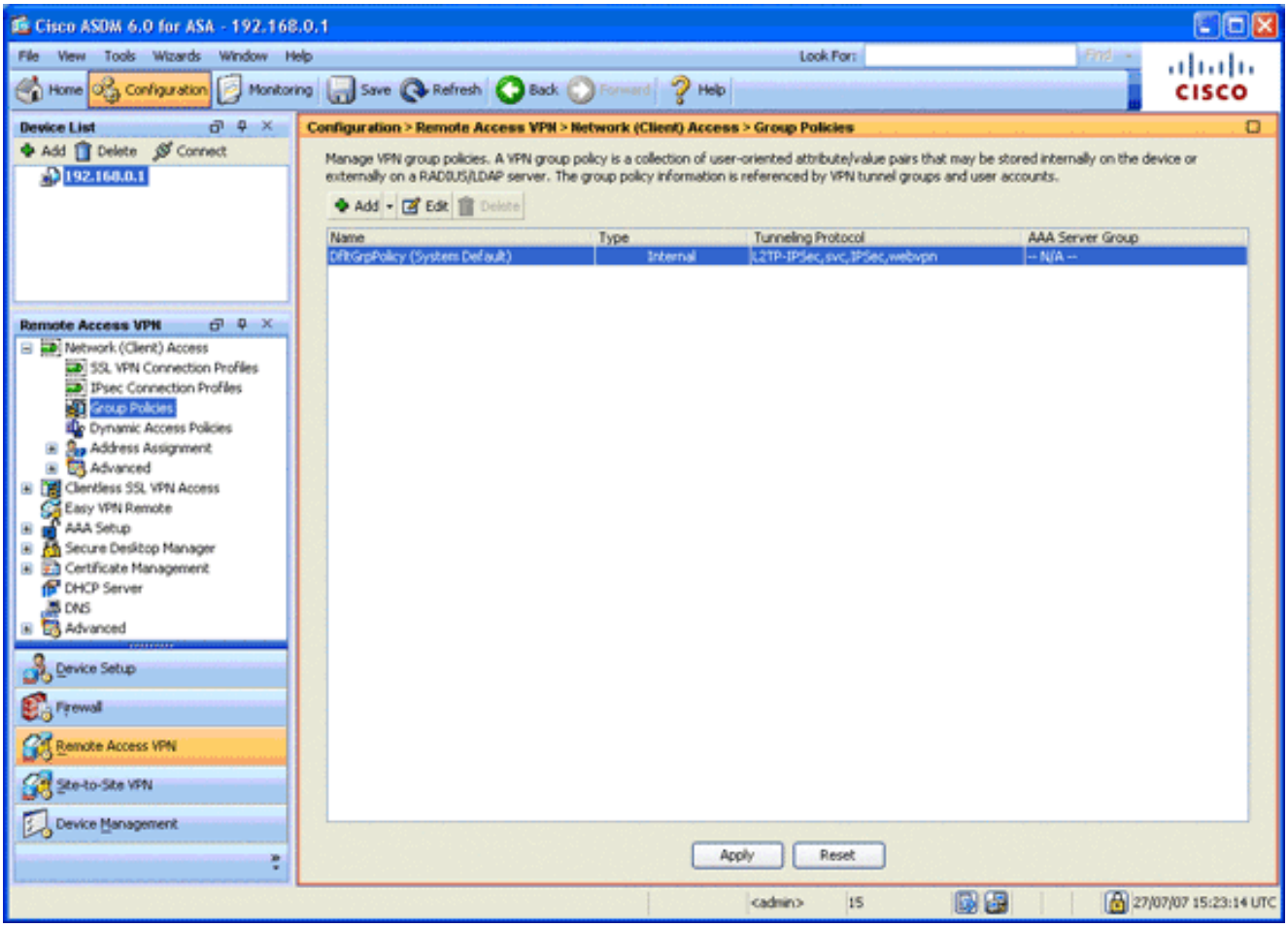
Kies in het navigatiegebied de **autorisatie**.In het gebied Group voor standaard autorisatie server kiest u **LOKAAL** uit de vervolgkeuzelijst servergroep en controleert u of de **gebruikers in de database van autorisatie moeten bestaan om** het aankruisvakje **aan te sluiten**.In het gedeelte Gebruikersnaam Toewijzing kiest u **SER (Serienummer)** uit de vervolgkeuzelijst Primair DNA-veld, kiest u **Geen** uit het veld Secundaire DN en klikt u op **OK**.



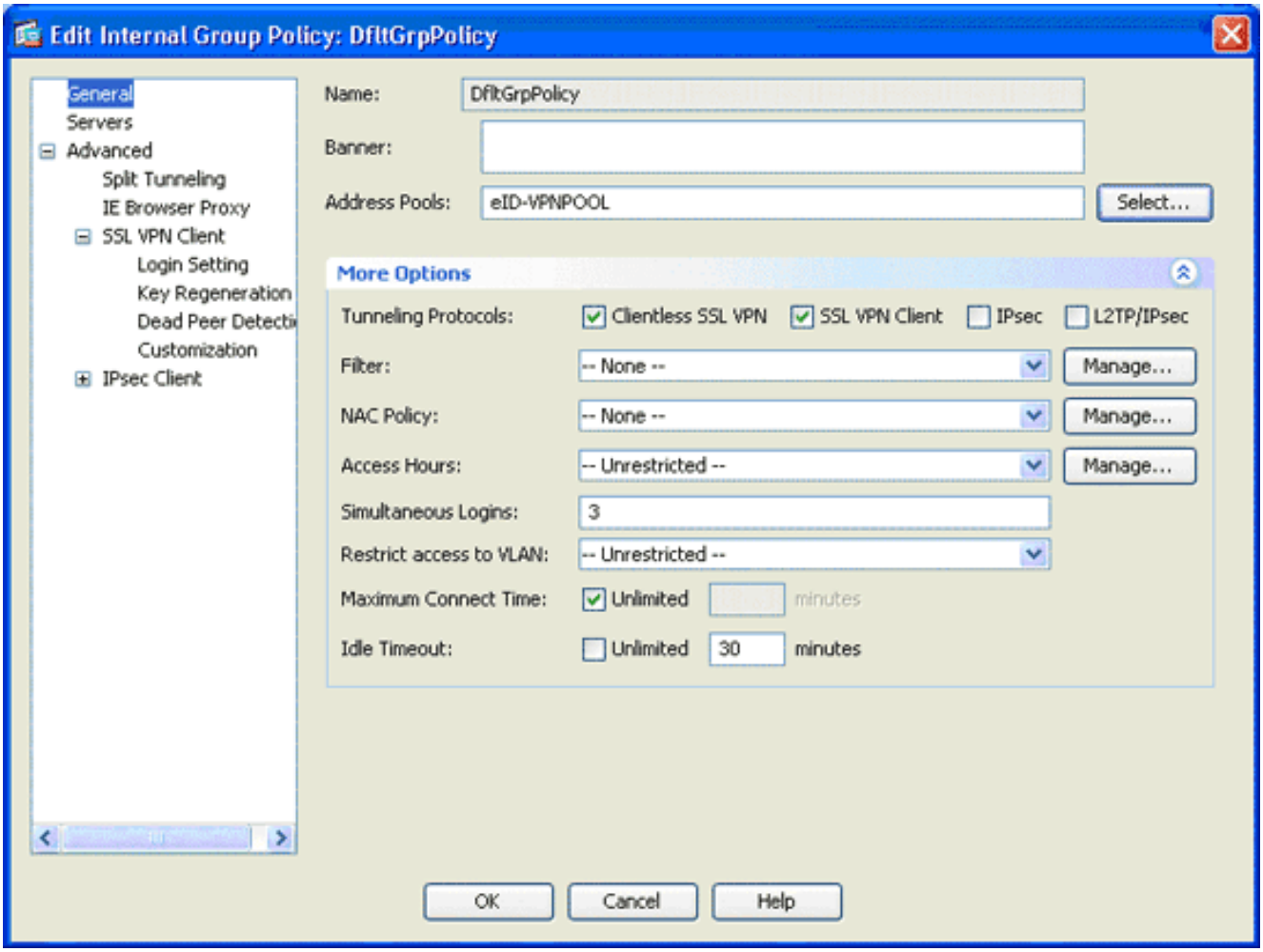
Stap 7. Bepaal het standaardbeleid van de groep

Deze stap beschrijft hoe u het standaardgroepsbeleid kunt definiëren.

1. In het VPN-gebied Externe toegang **vouwt** u **Network (Client) Access** uit en kiest u **groepsbeleid**.



2. Kies de optie **DfltGrpPolicy** in de lijst met groepsbeleid en klik op **Bewerken**.
3. Het dialoogvenster Intern groepsbeleid bewerken verschijnt.

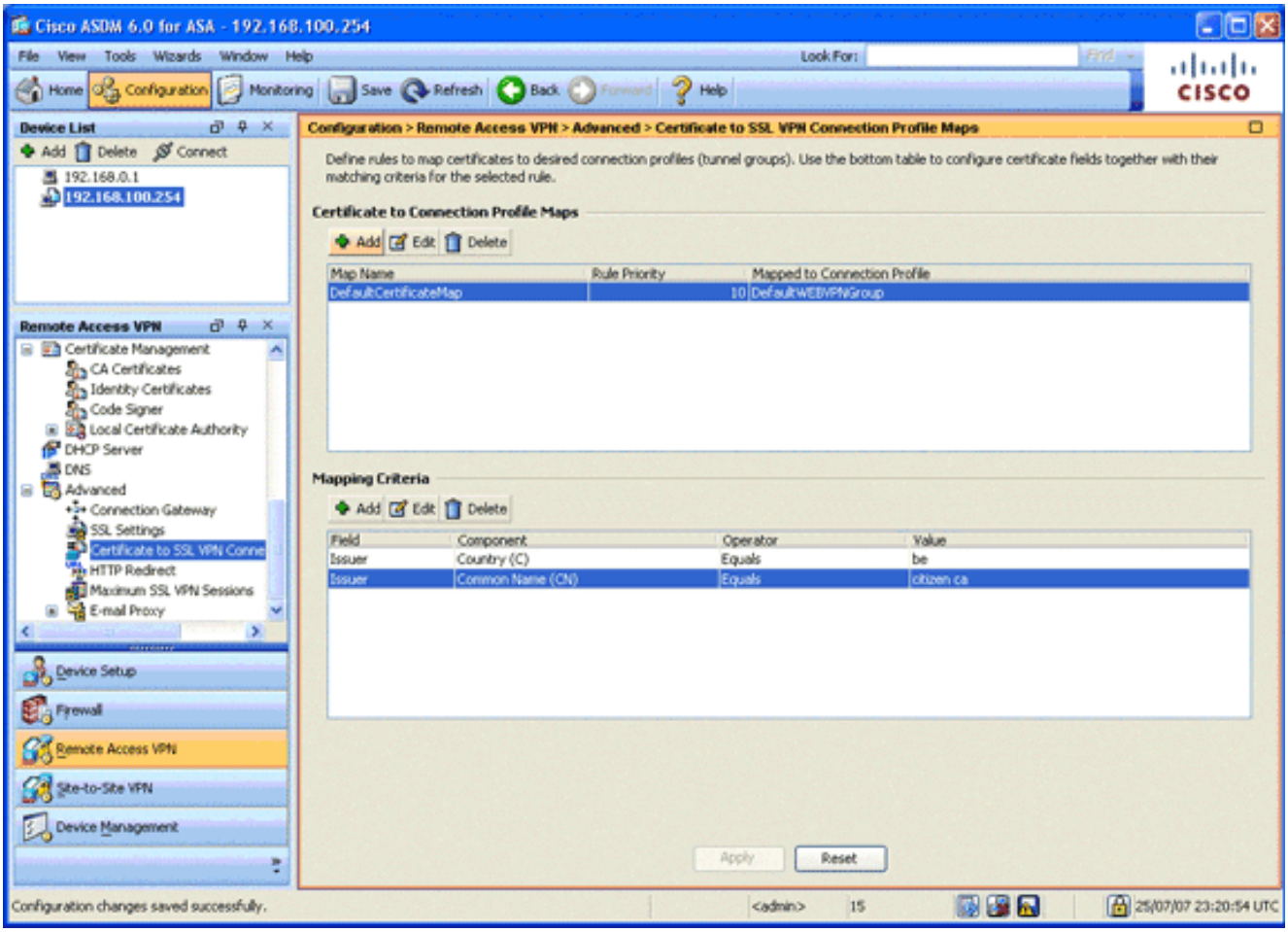


4. Selecteer in het navigatiegebied de optie **Algemeen**.
5. Voor adresgroepen klikt u op **Selecteren** om een pool van adressen te kiezen en kiest u **eID-VPL**.
6. In het gebied Meer opties controleert u de vinkjes **IPsec** en **L2TP/IPsec** en vervolgens klikt u op **OK**.

Stap 8. Bepaal de certificaattoewijzing

In deze stap wordt beschreven hoe de criteria voor het in kaart brengen van certificaten worden gedefinieerd.

1. Klik in het VPN-gebied Externe toegang op **Geavanceerd** en kies **certificaataanvraag voor SSL VPN-verbindingsprofiel**.
2. Klik in het gebied Certificaat om Profielkaarten te verbinden op **Toevoegen** en kies **Defaultcertificaatkaart** van de kaartlijst.Deze kaart moet overeenkomen met *DefaultWEBP.profiel* in het veld Map op verbindingen.
3. Klik in het gebied Kwaliteitscriteria op **Toevoegen** en voeg deze waarden toe:Veld: Uitgever, land (C), gelijk aan, "be"Veld: Afgiftester, gemeenschappelijke naam (GN), gelijken, "burgerkaart"De toekenningscriteria dienen in deze afbeelding te worden weergegeven:

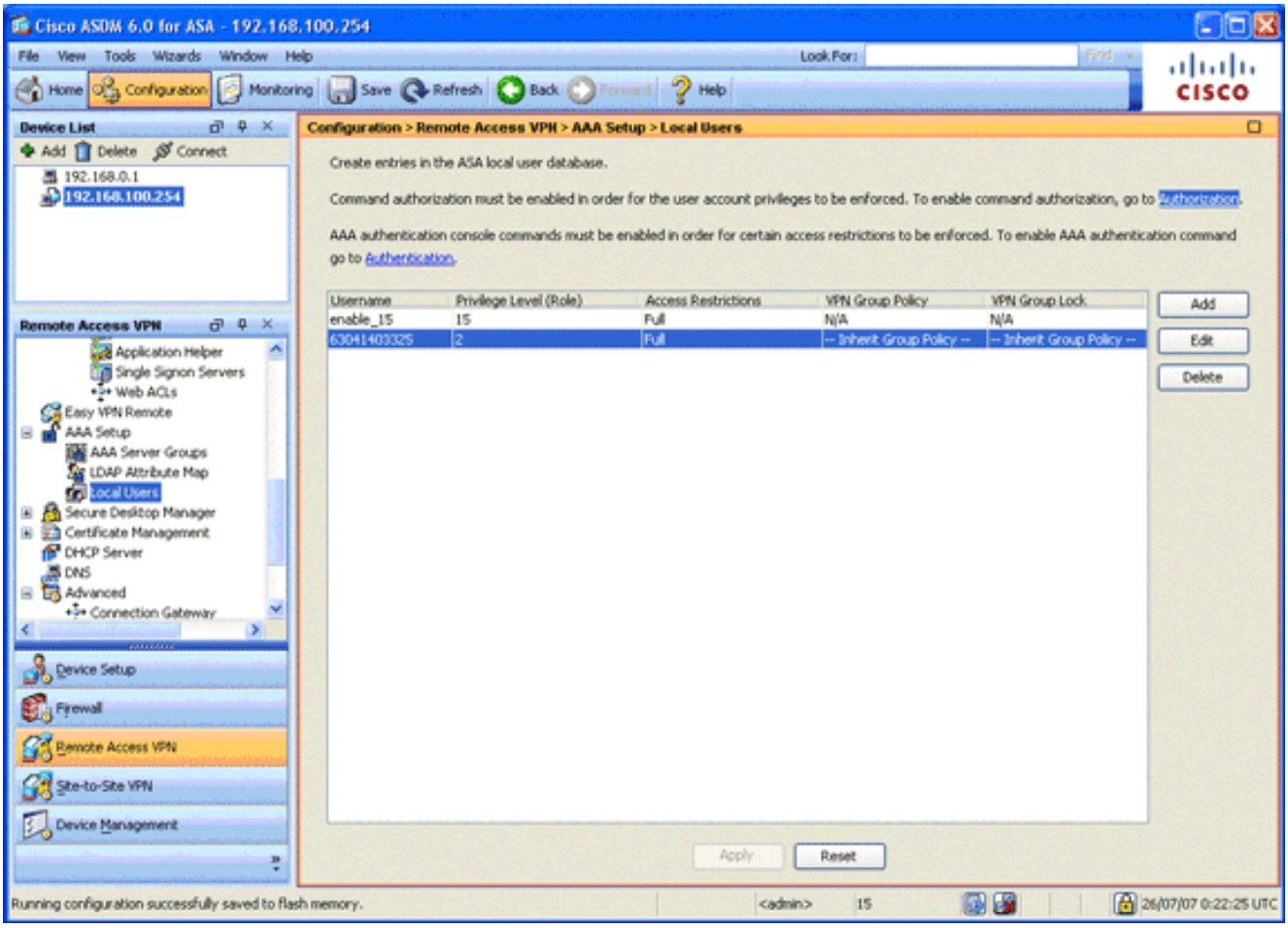


4. Klik op **Apply** (Toepassen).

Stap 9. Voeg een lokale gebruiker toe

In deze stap wordt beschreven hoe u een lokale gebruiker kunt toevoegen.

1. In het gebied van de Afstandstoegang VPN, **uitgebreid AAA-instelling** en kies **Lokale gebruikers**.
2. Klik in het gebied Local Gebruikers op **Add**.
3. Typ in het veld Naam van de gebruiker het serienummer van het gebruikerscertificaat. Bijvoorbeeld 56100307215 (zoals beschreven in het gedeelte Verificatiecertificaat van dit document).



4. Klik op **Apply** (Toepassen).

Stap 10. Herstart de ASA

Herstart de ASA om te verzekeren dat alle veranderingen van toepassing zijn op de systeemservices.

Fine Tune

Tijdens het testen, kunnen sommige SSL tunnels niet goed sluiten. Aangezien de ASA ervan uitgaat dat de AnyConnect-client de verbinding kan verbroken en opnieuw kan aansluiten, wordt de tunnel niet verbroken, waardoor deze de kans krijgt om terug te keren. Tijdens laboratoriumtesten echter met een basislicentie (2 SSL-tunnels standaard) kunt u de licentie uitputten als SSL-tunnels niet goed zijn gesloten. Als dit probleem zich voordoet, gebruikt u de opdracht **vpn-sessiondb <*optie*>** om alle actieve SSL-sessies op te heffen.

Configuratie één minuut

Om snel een werkende configuratie te maken, stelt u uw ASA in op de fabrieksstandaard en voegt u deze configuratie toe in de configuratiemodus:

ciscoa
ciscoasa#**conf t** ciscoasa#**clear configure all** ciscoasa#**domain-name cisco.be**

```
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
interface Ethernet0/1
 no shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
 domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 crl configure
crypto ca certificate map DefaultCertificateMap 10
 issuer-name attr c eq be
 issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
 certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
    16060355 0403130f 42656c67 69756d20 526f6f74
20434130 1e170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
30e8efc4 ab935e07 de328f12
    74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf
6ce3841d de872e33 0b3c74e2
    21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b
a7210687 1d27d3c4 a1c94cb0
```

```
    6f020301 0001a381 bb3081b8 300e0603 551d0f01
01ff0404 03020106 300f0603
    551d1301 01ff0405 30030101 ff304206 03551d20
043b3039 30370605 60380101
    01302e30 2c06082b 06010505 07020116 20687474
703a2f2f 7265706f 7369746f
    72792e65 69642e62 656c6769 756d2e62 65301d06
03551d0e 04160414 10f00c56
    9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
60864801 86f84201 01040403
    02000730 1f060355 1d230418 30168014 10f00c56
9b61ea57 3ab63597 6d9fddb9
    148edbe6 300d0609 2a864886 f70d0101 05050003
82010100 c86d2251 8a61f80f
    966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
48a74c49 37d773a1 6a01655e
    32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
5d0f37ba 76d240bd cc2d3fd3
    4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
45f4dae7 b5634544 110d2a7f
    337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
60f2d787 f6572e7a 7e6a1380
    1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
755481f3 1bad779c e8b28fdb
    83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
ba218c97 1a21d4ea 2d3bacba
    eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
fff26e87 7d46c974 d6efeb3d
    7de6596e 069404e4 a2558738 286a225e e2be7412
b004432a
  quit
no crypto isakmp nat-traversal
!
dhcpd address 192.168.0.2-192.168.0.129 inside
dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside
dhcpd enable outside
!
service-policy global_policy global
ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
sha1
ssl certificate-authentication interface outside port
443
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
 svc enable
certificate-group-map DefaultCertificateMap 10
DefaultWEBVPNGroup
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol svc webvpn
 address-pools value eID-VPNPOOL
username 63041403325 nopassword
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group (outside) LOCAL
 authorization-server-group LOCAL
 authorization-required
 authorization-dn-attributes SER
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
exit
copy run start
```

Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems