

# ASA/PIX 8.x en VPN-client-IPSec-verificatie met digitale certificaten met Microsoft CA-configuratievoorbeeld

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[ASA-configuratie](#)

[ASA-configuratieoverzicht](#)

[VPN-clientconfiguratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document beschrijft hoe u een digitaal certificaat van een derde verkoper handmatig kunt installeren op de Cisco security applicatie (ASA/PIX) 8.x en VPN-clients om de IPSec-peers te authenticeren met de Microsoft certificaatserver (CA).

## [Voorwaarden](#)

### [Vereisten](#)

Voor dit document moet u toegang hebben tot een certificeringsinstantie voor de inschrijving van certificaten. Ondersteunde derden voor CA-verkopers zijn Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA en VeriSign.

Dit document gaat ervan uit dat er geen bestaande VPN-configuratie in de ASA/PIX-modus is.

**Opmerking:** Dit document gebruikt een Microsoft Windows 2003-server als CA-server voor het scenario.

**Opmerking:** Raadpleeg [CA op Windows server configureren](#) voor volledige informatie over hoe u een Windows 2003-server als CA kunt configureren.

## Gebruikte componenten

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

- ASA 5510 die softwareversie 8.0(2) en ASDM versie 6.0(2) draait
- VPN-client die softwareversie 4.x en hoger uitvoert

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.

## Verwante producten

De ASA-configuratie kan ook worden gebruikt met Cisco 500 Series PIX die softwareversie 8.x draait.

## Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

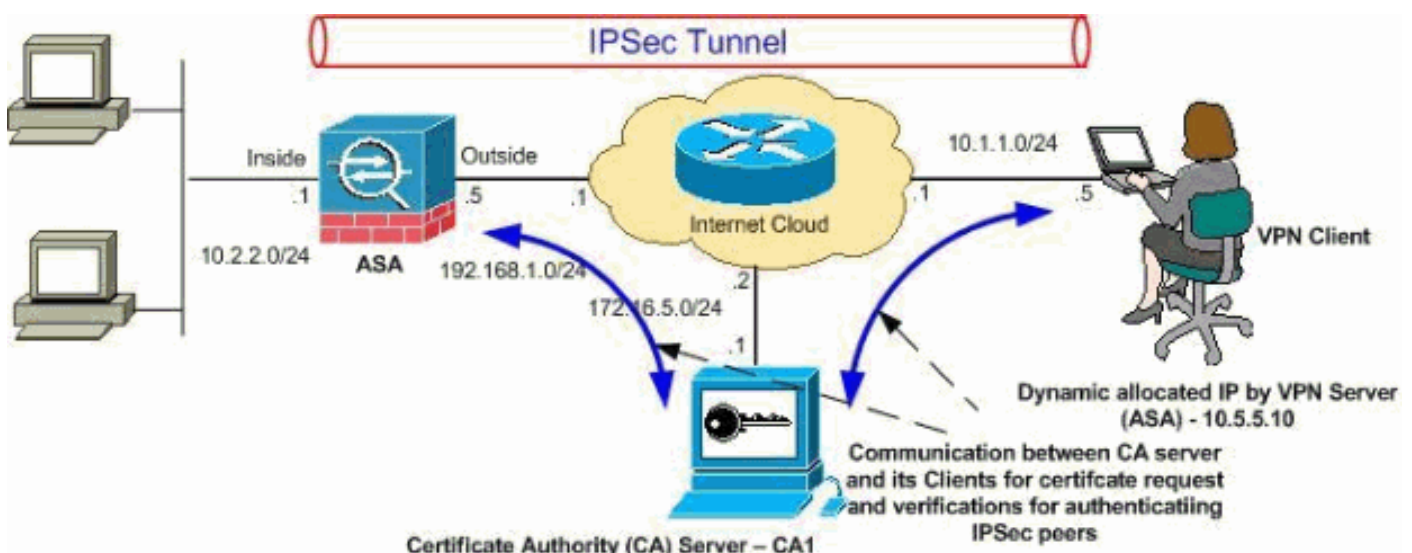
## Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**Opmerking:** Gebruik het [Opdrachtupgereedschap](#) (alleen [geregistreeerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

## Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



**Opmerking:** de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

## [Configuraties](#)

Dit document gebruikt deze configuraties:

- [ASA-configuratie](#)
- [ASA-configuratiesoverzicht](#)
- [VPN-clientconfiguratie](#)

## [ASA-configuratie](#)

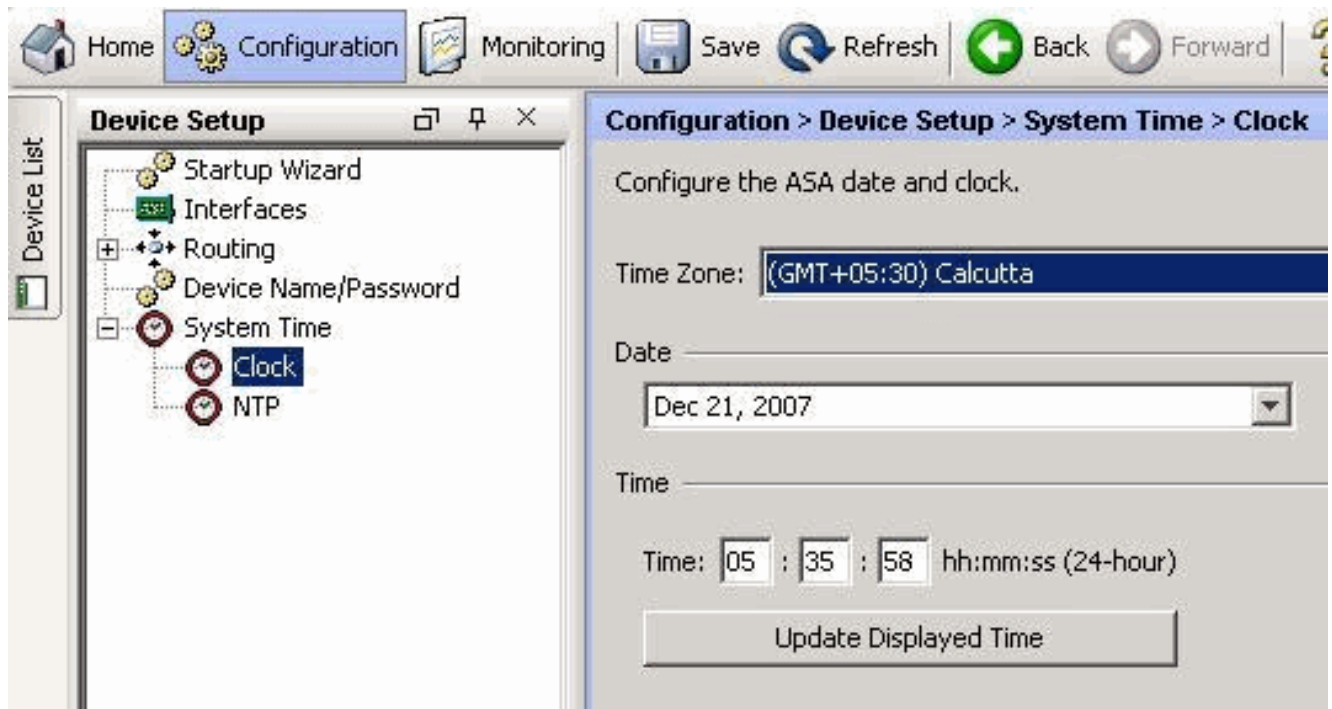
Voltooi de volgende stappen om een digitaal certificaat van een derde verkoper op de ASA te installeren:

- [Stap 1. Controleer dat de waarden voor Datum, tijd en tijd nauwkeurig zijn](#)
- [Stap 2: genereer een certificaataanvraag](#)
- [Stap 3. Verifieer het Trustpoint](#)
- [Stap 4. Installeer het certificaat](#)
- [Stap 5. Het configureren van VPN-toegang \(IPSec\) om het nieuw geïnstalleerd certificaat te gebruiken](#)

### [Stap 1. Controleer dat de waarden voor Datum, tijd en tijd nauwkeurig zijn](#)

#### **ASDM-procedure**

1. Klik op **Configuration** en vervolgens op **Devices Setup**.
2. Uitbreidt **systemtijd** en kiest **klok**.
3. Controleer of de verstrekte informatie juist is. De waarden voor Datum, Tijd en Tijdzone moeten nauwkeurig zijn zodat de juiste certificatie kan plaatsvinden.



### Opdrachtlijvoorbeeld

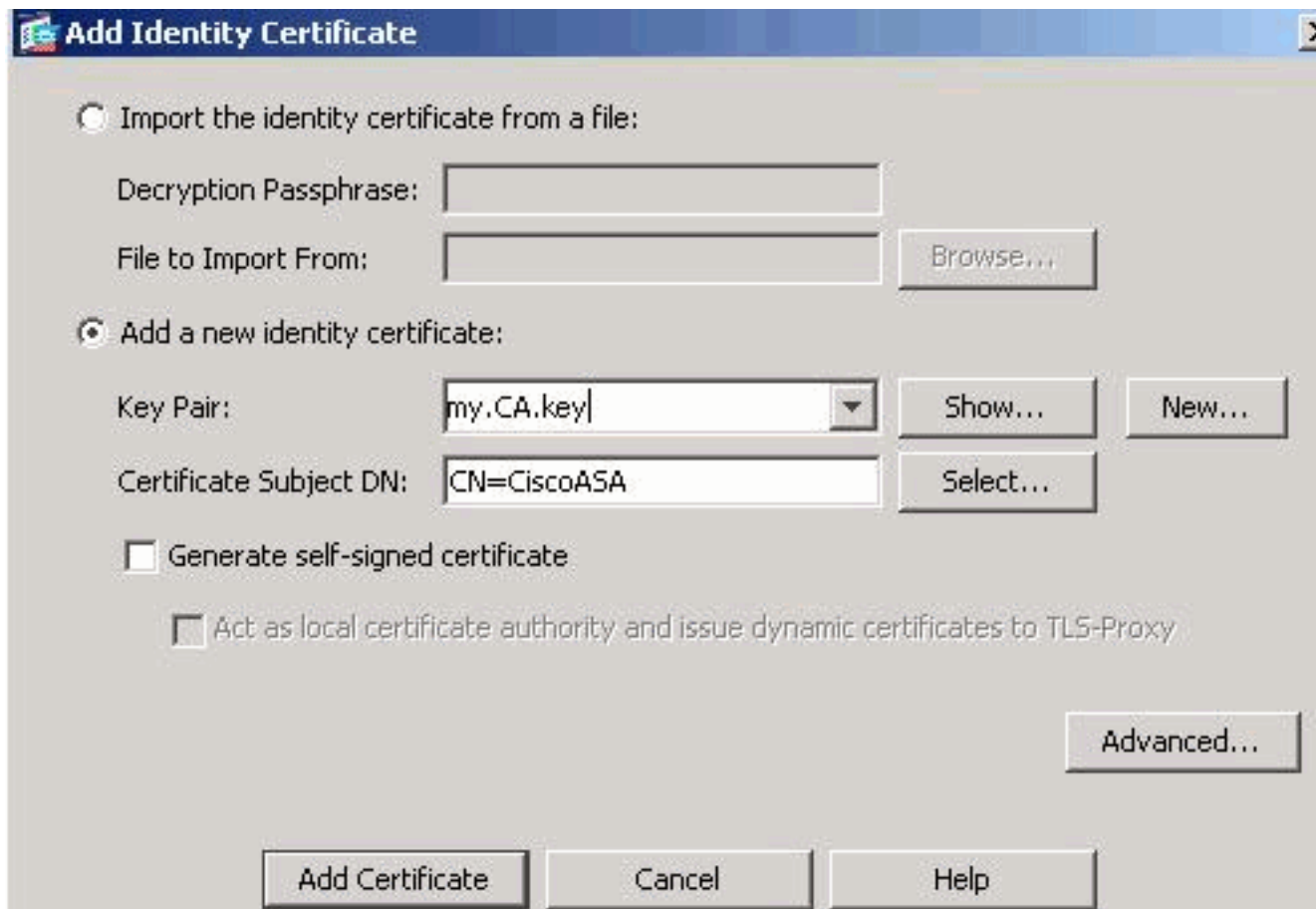
Cisco ASA
<pre>CiscoASA#show clock 05:37:37.904 UTC Fri Dec 21 2007</pre>

### Stap 2: genereer een certificaataanvraag

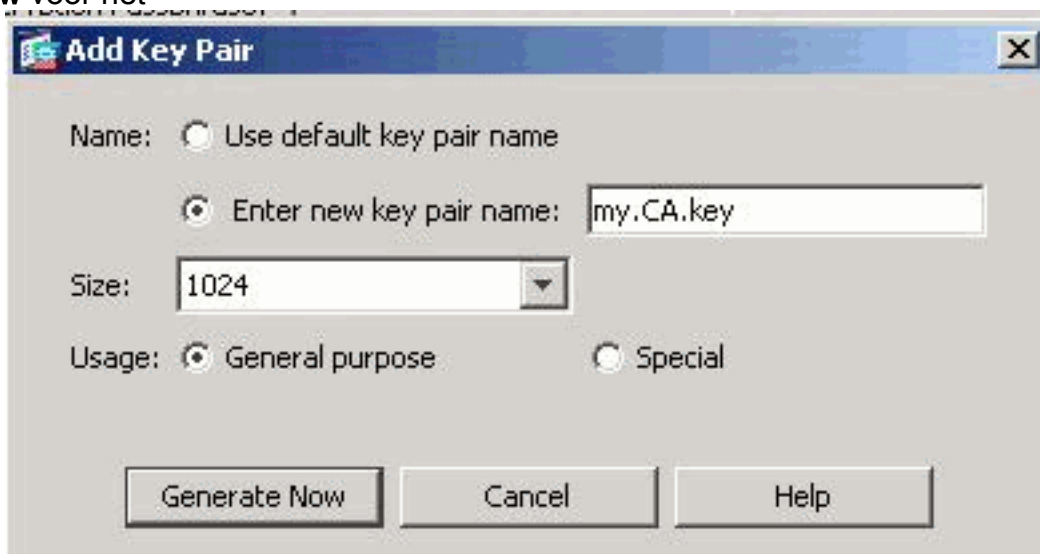
Er is een verzoek om ondertekening van een certificaat (CSR) vereist, zodat de derde partij een identiteitsbewijs kan afgeven. Het CSR bevat de naam van uw ASA (DN)-string samen met de ASA's genereerde openbare sleutel. De ASA gebruikt de gegenereerde privé-sleutel om digitaal de CSR te ondertekenen.

### ASDM-procedure

1. Klik op **Configuration** en vervolgens op **Apparaatbeheer**.
2. **certificaatbeheer** uitbreiden en **identiteitsbewijzen** kiezen.
3. Klik op **Toevoegen**.

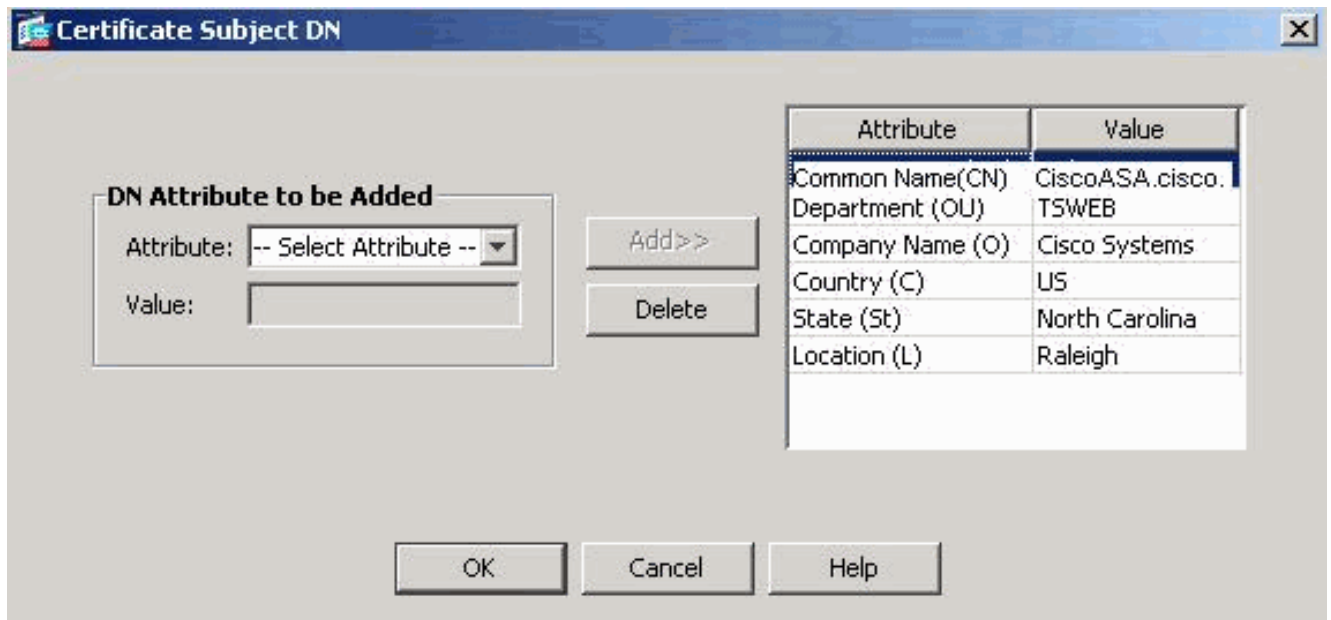


4. Klik op de knop **Een nieuw identiteitsbewijs** toevoegen.
5. Klik op **Nieuw** voor het



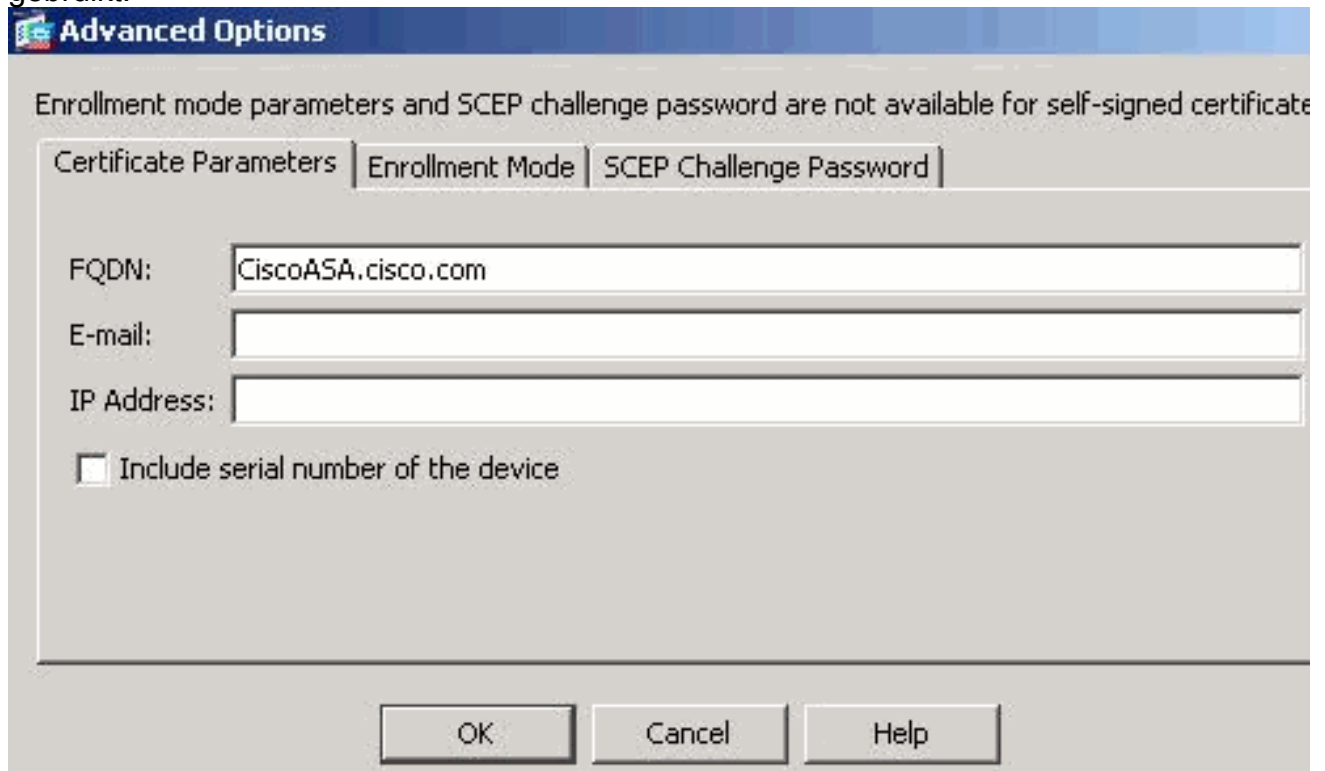
toetsenbord.

6. Klik op de radioknop **Voer de nieuwe naam van het sleutelpaar in**. U moet de naam van het sleutelpaar voor herkenningdoeleinden duidelijk herkennen.
7. Klik op **Generate Now**. Het sleutelpaar moet nu worden gemaakt.
8. Om het Onderwerp van het Certificaat te definiëren DN, klik **Selecteer**, en stel de eigenschappen in deze tabel in: Om deze waarden te configureren kiest u een waarde uit de vervolgkeuzelijst Eigenschappen, voert u de waarde in en klikt u op **Toevoegen**.

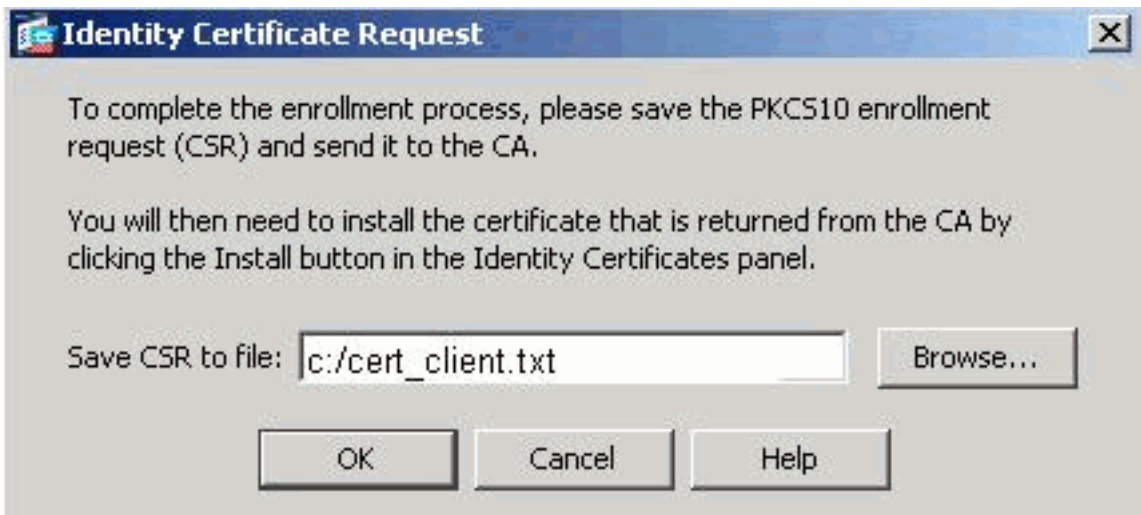


**Toelichting:** Sommige derde verkopers vereisen dat specifieke eigenschappen worden opgenomen voordat een identiteitsbewijs wordt afgegeven. Als u niet zeker weet welke eigenschappen u moet hebben, raadpleegt u de verkoper voor meer informatie.

9. Klik op **OK** als de juiste waarden zijn toegevoegd. Het dialoogvenster Identiteitscertificaat toevoegen wordt weergegeven met het veld Programma Onderwerp Certificaat ingevuld.
10. Klik op **Geavanceerd**.
11. Voer in het veld FQDN de FQDN in die wordt gebruikt om het apparaat van het internet te gebruiken. Deze waarde moet dezelfde FQDN zijn als u voor de gemeenschappelijke naam (CN) gebruikt.



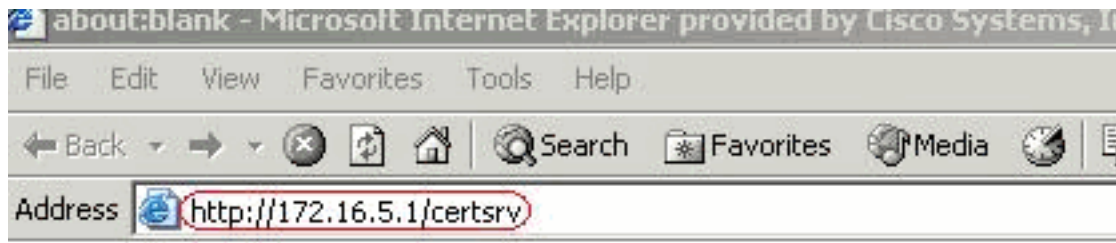
12. Klik op **OK** en vervolgens op **Certificaat toevoegen**. U wordt gevraagd de CSR op te slaan in een bestand op uw lokale



machine.

13. Klik op **Bladeren**, kies een plaats waar u de CSR wilt opslaan en slaat u het bestand op met de .txt-extensie.**Opmerking:** wanneer u het bestand opslaat met een .txt-extensie, kunt u het bestand openen met een teksteditor (zoals Kladblok) en het PKCS#10-verzoek bekijken.

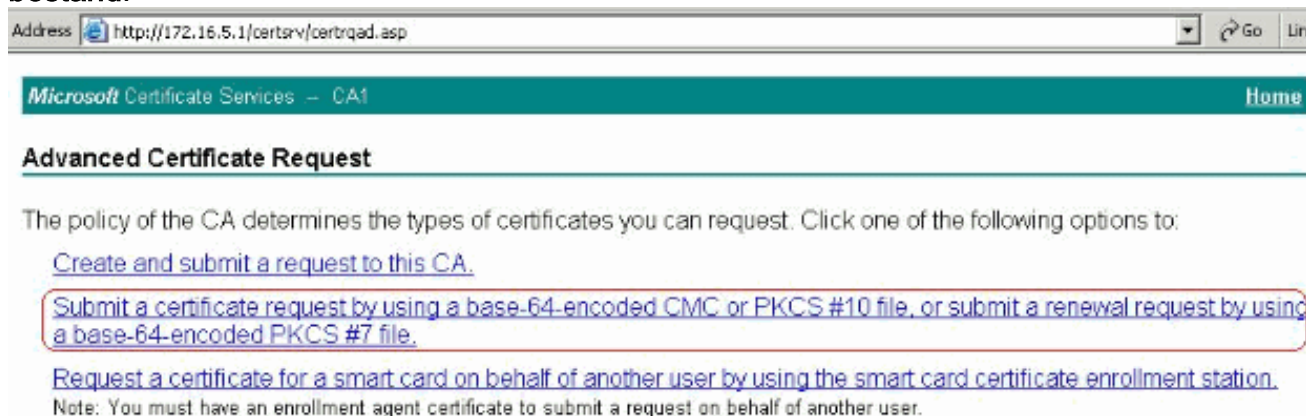
14. Geef de opgeslagen CSR door aan uw derde verkoper zoals Microsoft CA, zoals getoond. Voer de weblognaam in de CA Server 172.16.5.1 uit met behulp van de gebruikersreferenties die voor de VPN-server beschikbaar

A screenshot of a Windows dialog box titled 'Enter Network Password'. The dialog box has a blue title bar with a question mark icon and a close button. The main area contains a key icon and the text 'Please type your user name and password.'. Below this, the 'Site:' is listed as '172.16.5.1'. There are three input fields: 'User Name' containing 'vpnuser', 'Password' containing 'xxxxxxxx', and 'Domain' which is empty. A checkbox labeled 'Save this password in your password list' is unchecked. At the bottom, there are 'OK' and 'Cancel' buttons. A red rectangle highlights the 'User Name' and 'Password' fields.

zijn.

Opmerki

ng: Zorg ervoor dat u een gebruikersaccount hebt voor de ASA (VPN-server) met de CA-server. Klik op **Aanvragen van een certificaat > gevorderd certificaatverzoek** om te selecteren **Een certificaataanvraag in te dienen door gebruik te maken van een basisbestand van 64-gecodeerde CMC of PKCS#10-bestand of een vernieuwingsverzoek in te dienen door gebruik te maken van een basisbestand van 64-gecodeerde PKCS#7-bestand.**



Kopieer en plak de gecodeerde informatie naar het vakje **Opgeslagen aanvraag** en klik vervolgens op **Indienen**.



## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded (source such as a Web server) in the Saved Request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
vQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAO  
4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8  
D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+  
8Ux9emhFHpGHnQ/MpSfU0dQ==  
not part of the certificate request---
```

[Browse for a file to insert.](#)

### Certificate Template:

IPSEC

### Additional Attributes:

Attributes:

Submit >

Klik op

de radioknop **Base64 encoded** en klik op **Download**

**Microsoft** Certificate Services -- CA1

## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



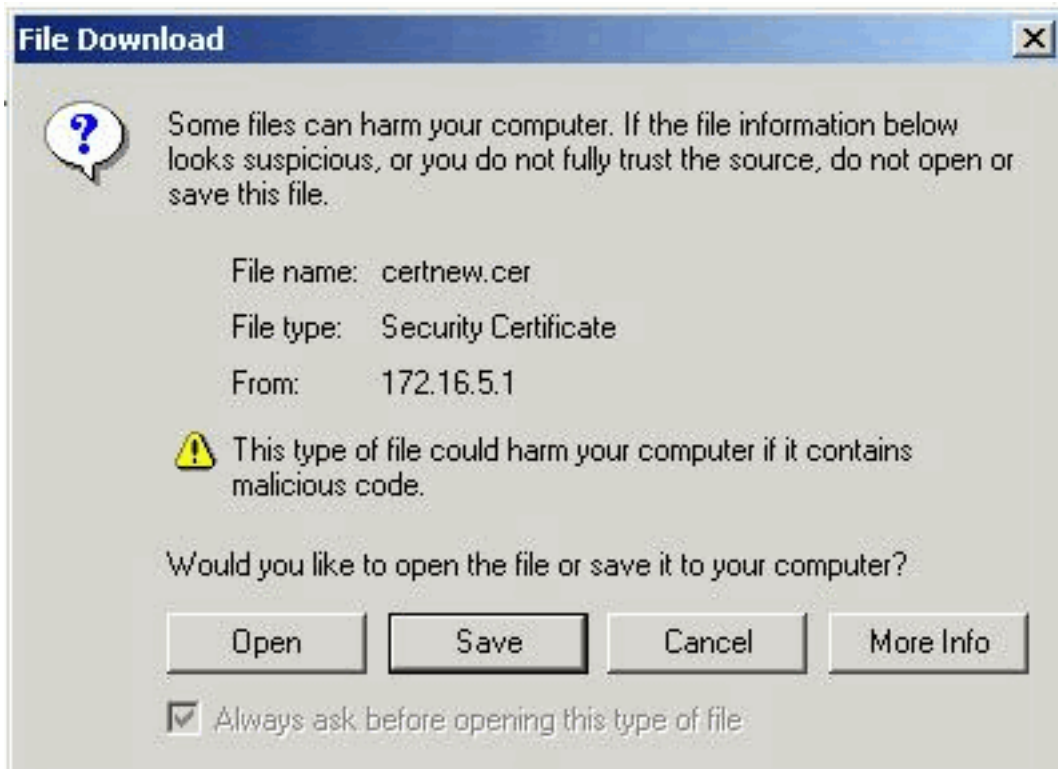
[Download certificate](#)

[Download certificate chain](#)

certificaat.

Het

venster File Download verschijnt. Sla het op met de naam **cert\_client\_id.cer**, dat is het identiteitsbewijs dat moet worden geïnstalleerd op de



ASA.

## Opdrachtlijvoorbeeld

### Cisco ASA

```
CiscoASA# configure terminal

CiscoASA(config)#crypto key generate rsa label my.ca.key
modulus 1024

!--- Generates 1024 bit RSA key pair. "label" defines
the name of the Key Pair. INFO: The name for the keys
will be: my.CA.key Keypair generation process begin.
Please wait... ciscoasa(config)#crypto ca trustpoint CA1
ciscoasa(config-ca-trustpoint)# subject-name
CN=CiscoASA.cisco.com,OU=TSWEB,
                                O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh

!--- Defines x.500 distinguished name. Use the
attributes defined in table as a guide. CiscoASA(config-
ca-trustpoint)#keypair my.CA.key

!--- Specifies key pair generated in Step 3
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com

!--- Specifies the FQDN (DNS:) to be used as the subject
alternative name CiscoASA(config-ca-
trustpoint)#enrollment terminal

!--- Specifies manual enrollment. CiscoASA(config-ca-
trustpoint)#exit
CiscoASA(config)#crypto ca enroll CA1

!--- Initiates certificate signing request. This is the
request to be !--- submitted via Web or Email to the
third party vendor. % Start certificate enrollment .. %
The subject name in the certificate will be:
cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems,
```

```

C=US,St=North Carolina,L=Raleigh % The fully-qualified
domain name in the certificate will be:
CiscoASA.cisco.com % Include the device serial number in
the subject name? [yes/no]: no
!--- Do not include the device's serial number in the
subject. Display Certificate Request to terminal?
[yes/no]: y
!--- Displays the PKCS#10 enrollment request to the
terminal. You will need to !--- copy this from the
terminal to a text file or web text field to submit to
!--- the third party CA. Certificate Request follows:
MIICKzCCAzQCAQAwga0xEDAObgNVBAcTB1JhbGVpZ2gxZzAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU31z
dGVtczEk
MCIGA1UEAxMbQ2l2Y29BU0EuY2l2Y28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDafBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXT1PgNAaFMwB2YsTIOh+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBxl/LVLTy3ORqcy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJJDjEuMCwwCwYDVR0PBAQD
AgWgMB0G
A1UdEQQWMBSEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF
AAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd20LCbXAoP5L1KbPaEeaCkFN/Pp5mATA
sG832TBm
bsxSvljSSXQsQ1Sb842D6MEG6cu7Bxj/K1Z6MxafUvCHROPYWVU1wgrJ
Gh+ndCZK j89/Y4S8XhQ79fvBwB8Ux9emhFHpGHnQ/MpSfU0dQ== --
--End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: n
CiscoASA(config)#

```

### Stap 3. Verifieer het Trustpoint

Zodra u het identiteitsbewijs van de derde verkoper ontvangt, kunt u met deze stap verder gaan.

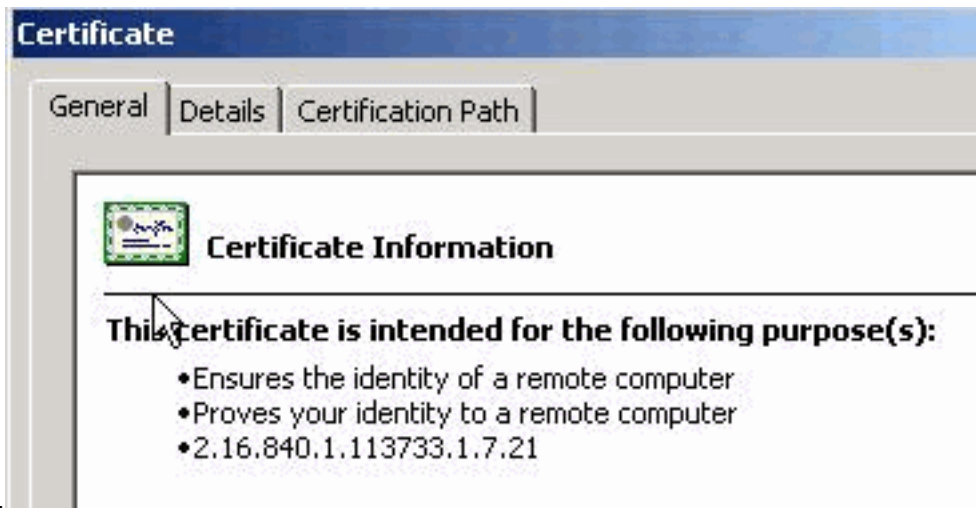
#### ASDM-procedure

1. Sla het identiteitsbewijs op de plaatselijke computer op.
2. Als uw basiscertificaat 64 niet als bestand is ingevuld, moet u het Base64-bericht kopiëren en het in een tekstbestand plakken.
3. Geef het bestand een andere naam met een .cer-extensie **Opmerking:** Zodra het bestand een andere naam heeft gekregen dan de .cer extensie, wordt het bestands pictogram



weergegeven als een certificaat, zoals wordt weergegeven.

4. Dubbelklik op het



certificaatbestand.

Opme

**rkning:** Als Windows niet genoeg informatie heeft om dit certificaatbericht in het tabblad Algemeen te controleren, moet u het certificaat van oorsprong CA of tussenpersoon CA van een derde verkoper verkrijgen voordat u met deze procedure doorgaat. Neem contact op met uw verkoper of CA-beheerder om de afgifte van de basiscertificaten voor CA of de tussenliggende CA-certificaten te verkrijgen.

5. Klik op het tabblad **certificaatpad**.

6. Klik op het CA-certificaat dat aan uw afgegeven identiteitsbewijs is gekoppeld en klik op **Certificaat**

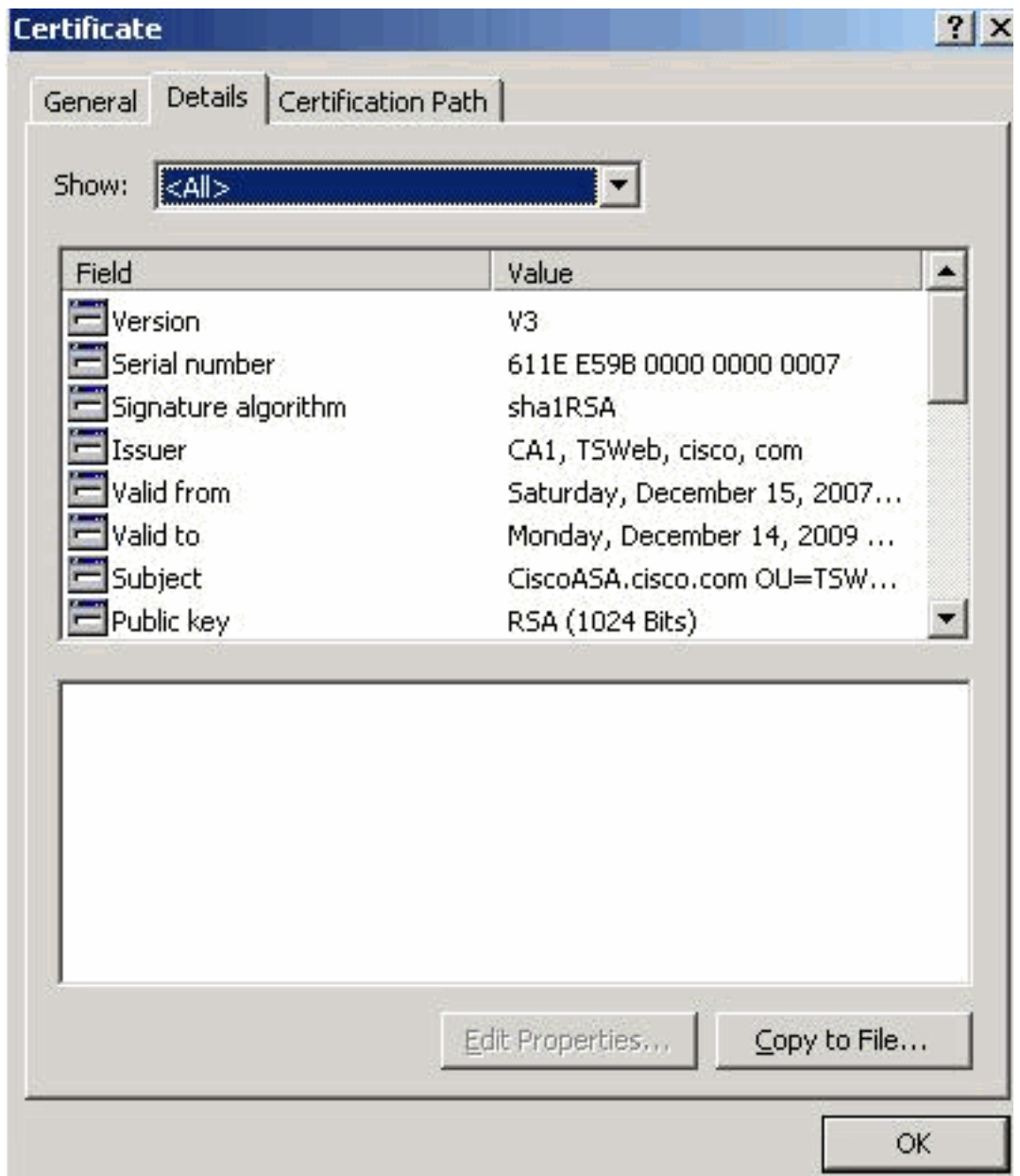


bekijken.

eerde informatie over het CA-certificaat verschijnt.

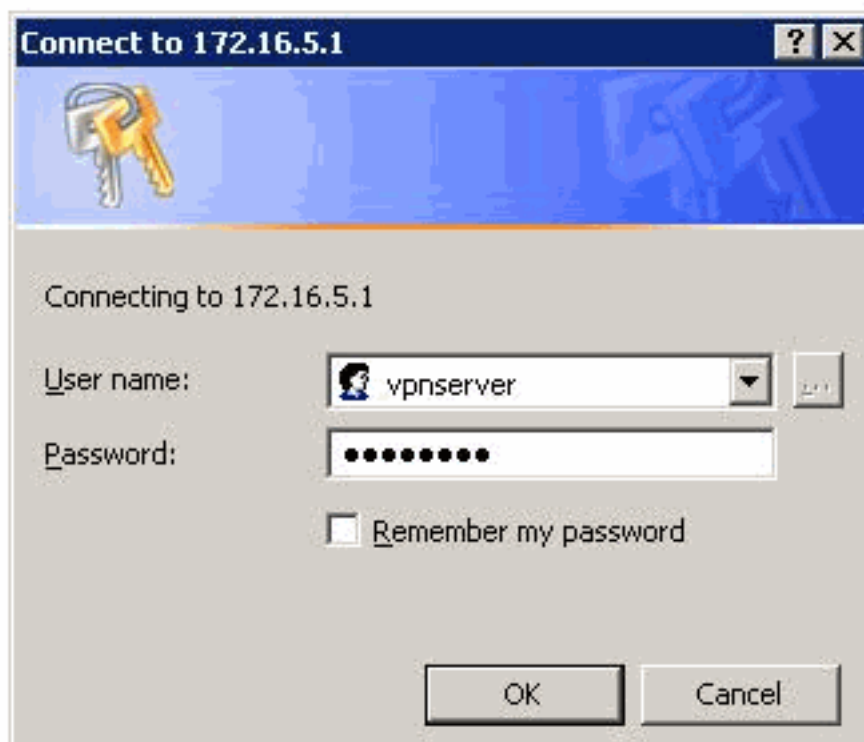
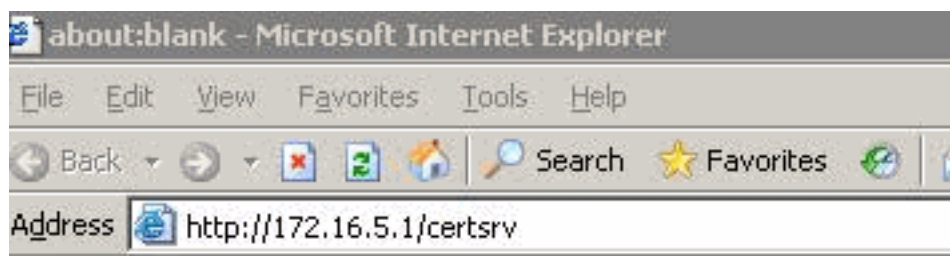
7. Klik op **Details** om meer informatie te krijgen over het

Gedetaill



identiteitsbewijs.

8. Voordat u het identiteitsbewijs installeert, moet het CA certificaat van de server van CA worden gedownload en in de ASA worden geïnstalleerd, zoals getoond. Voltooi deze stappen om het CA-certificaat te downloaden van de CA-server genaamd **CA1**. Voer de weblognaam in de CA-server 172.16.5.1 uit met behulp van de aanmeldingsgegevens die op de VPN-server worden



geleverd.

**Download een CA certificaat, certificaatketen of CRL** om het venster te openen, zoals weergegeven. Klik op de radioknop **Base64** als de coderingsmethode en klik op **CA-certificaat** downloaden.

Klik op

## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

### CA certificate:



### Encoding method:

- DER
- Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Sla het CA-certificaat op met de naam **certnew.cer** op uw



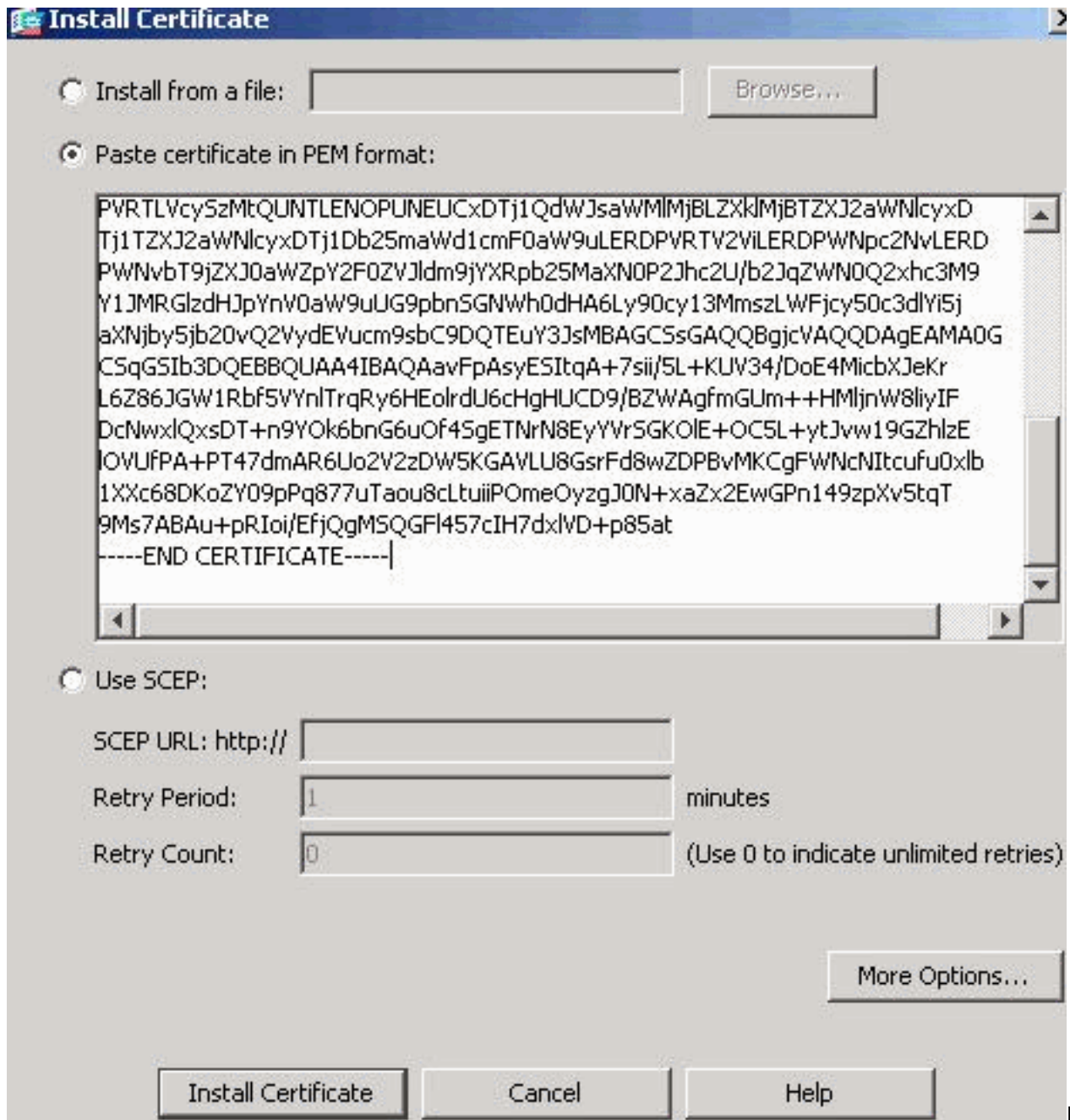
computer.

9. Bladeren naar de locatie waar u het CA-certificaat hebt opgeslagen.
10. Open het bestand met een teksteditor, zoals Kladblok. Klik met de rechtermuisknop op het bestand en kies **Verzenden naar > Kladblok**.
11. Het Base64-gecodeerde bericht vergelijkbaar met het certificaat in deze afbeelding verschijnt:



```
-----BEGIN CERTIFICATE-----
MIIEHTCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBR
MRMwEQYKZCZImiZPyLQBGGRYDY29tMRUwEwYKZCZImiZPyLQBGGRYFY2IzY28xFTAT
BgoJkiajk/IsZAEZFGVUU1dIYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
Ml0XDTEyMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCgms
JomT8ixkARKwBWNpc2NvMRUwEwYKZCZImiZPyLQBGGRYFVFNXZWIxDDAKBgnVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaekBpo5Zd4TNgntjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vweMijcQnwdOq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhdbMivwqYBXWkh4u04xxQmr//Sct1tdwQcvk2V
uBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wggFrMBMGCSSGAQQBggjCUAgQHgQAQwBBMASGA1UddwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZr68I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZXk1MjBTZXJ2awNlcYxD
Tj1TZXJ2awNlcYxDTj1Db25mawd1cmF0aw9uLERDPVRTV2ViLERDPWNpc2NvLERD
PWNvbT9jZXJ0awZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNWwh0dHA6Ly90cy13MmszLWwFjcy50c3dIYi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGCSGAQQBggjCVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MibXJekr
L6Z86JGw1Rbf5vynlTrqRy6HEo1rdU6cHgHUCD9/BZWagfmGUM++HMLjnw8liyIF
DcnwxlQxsDT+n9Yok6bnG6uof4SgETNrN8EyyVrSGK0lE+OC5L+ytJvw19Gzh1ze
lOVUFPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCGFWNCNItcufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPn149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
```

12. Klik binnen ASDM op **Configuration** en vervolgens op **Apparaatbeheer**.
13. Vergroot **certificaatbeheer** en kies **CA-certificaten**.
14. Klik op **Toevoegen**.
15. Klik het **certificaat van het plakken in de radioknop van het Formaat in PEM**, en plak het basis64 CA certificaat dat door de derde verkoper in het tekstveld wordt verstrekt.
16. Klik op **Installeer het certificaat**.



Er

verschijnt een dialoogvenster waarin wordt bevestigd dat de installatie geslaagd is.

### Opdrachtlijvoorbeeld

```

Cisco ASA
CiscoASA(config)#crypto ca authenticate CA1
!--- Initiates the prompt for paste-in of base64 CA
intermediate certificate. ! This should be provided by
the third party vendor. Enter the base 64 encoded CA
certificate. End with the word "quit" on a line by
itself -----BEGIN CERTIFICATE-----
MIIE nTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLQG BGRYDY29tMRUwEwYKCZImiZPyLQG BGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0E xMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNvowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgms
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQG BGRYFVFNXZWI xDDAK

```

```

BgNVBAMT
A0NBMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGAPAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuAhpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAQOQHQAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbTzrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMM1mjBLZXk1mjBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNO
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnsSGNWh0dHA6Ly90cy13MmszLWFwjcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAghmGUm++HM1j
nW8liYIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOLE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPvMKCGFWNCNIt
cufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqT
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dxlVD+p85at
-----END CERTIFICATE-----
quit
!--- Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
CiscoASA(config)#

```

## Stap 4. Installeer het certificaat

### ASDM-procedure

Gebruik het door de derde verkoper verstrekte identiteitsbewijs om deze stappen te voltooien:

1. Klik op **Configuration** en vervolgens op **Apparaatbeheer**.
2. vouwt **certificaatbeheer** uit en kies vervolgens **identiteitsbewijzen**.
3. Selecteer het identiteitsbewijs dat u in [Stap 2](#) hebt gemaakt. **Opmerking:** de verloopdatum is



```
aW5hMRAwDgYDVQOHEwdSYWxlaWdoMRYwFAYDVQOKEw1DaXNjbyBTeXNO
ZW1zMSQw
IgyYDVQOQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZlhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBAaAwHQYDVROBBYwFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDgQWBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfnQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxID
Tj1QdWJs
aWM1MjBLZXklMjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnsG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEgEgEPMIIBCzCBQQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUESQ049UHvibgljJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UuY1XmksZLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAWGA1Ud
EwEB/wQC
MAAwEwYDVRO1BAwwCgYIKwYBBQUHAWEdDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzCWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtzhz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpFv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
tlnwLpsc
lL5nuPsd8MaexBc=
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate successfully imported
CiscoASA(config)#
```

## [Stap 5. Het configureren van VPN-toegang \(IPSec\) om het nieuw geïnstalleerd certificaat te gebruiken](#)

## ASDM-procedure

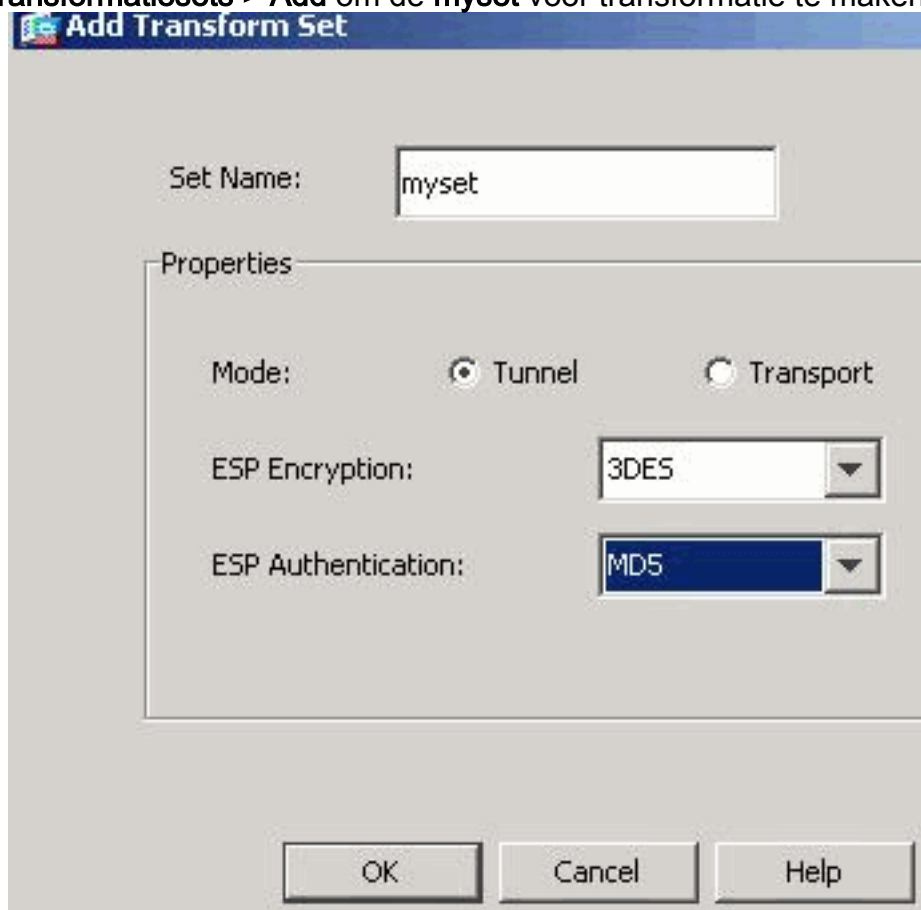
Voltooi deze stappen om de externe VPN-toegang te configureren:

1. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-beleid > Add** om een ISAKMP-beleid 65535 te maken, zoals getoond.



Klik op OK en Toepassen.

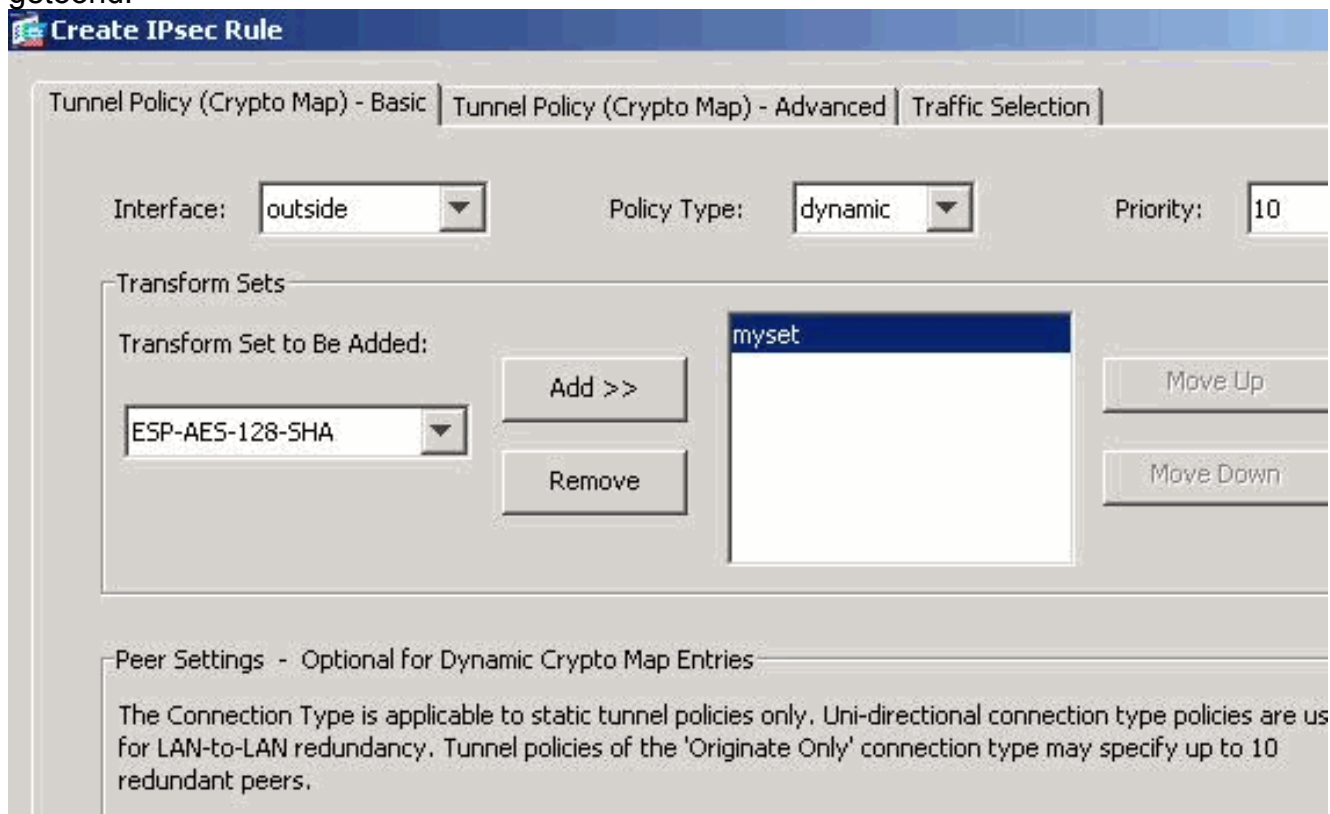
2. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transformatiesets > Add** om de myset voor transformatie te maken, zoals



getoond.  
Toepassen.

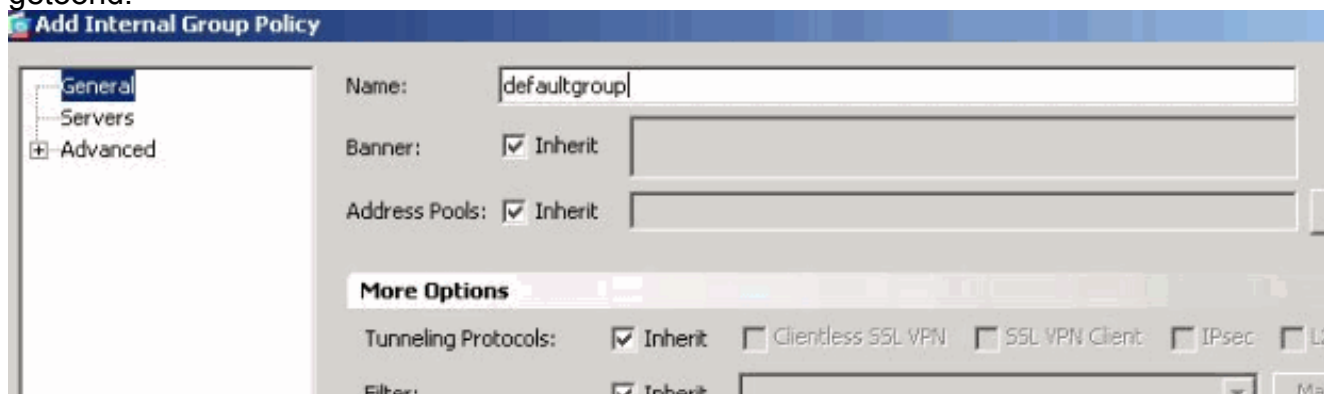
Klik op OK en

3. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps > Add** om een crypto-kaart te maken met dynamisch beleid van prioriteit 10, zoals getoond.



Klik op **OK** en **Toepassen**. **Opmerking:** ASA 8.0 ondersteunt SHA 2 niet. Ook IPsec-klienten die certificaten met een hash van 256 gebruiken worden niet ondersteund.

4. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policy > Add** om een **standaard** groepsbeleid te maken, zoals getoond.



Klik op **OK** en **Toepassen**.

5. Kies **Configuration > Remote Access VPN > Network (Client) Access > Address Assignatie > Address Pools > Add** om de VPN-adrespool te configureren zodat de VPN-clientgebruikers dynamisch toegewezen

**Add IP Pool**

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

OK Cancel Help

worden.

Klik op **OK** en **Toepassen**.

6. Kies **Configuration > Remote Access VPN > AAA-instelling > Local Gebruikers > Add** om de gebruikersaccount voor VPN-client te maken. Maak van deze gebruiker ook lid van **DefaultRAGroup**.

**Add User Account**

Identity

VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of

Member-of:  Add >> Delete

DefaultRAGroup

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.  
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)  
Privilege level is used with command authorization.  
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)  
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access  
This setting is effective only if AAA authenticate console command is configured.

7. Kies **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection**



**Profile > Bewerken** om de **DefaultRAGroup** te kunnen bewerken, zoals wordt getoond. Kies het juiste **identiteitsbewijs** uit de uitrollijst voor het veld IKE Peer Verificatie. Kies de servergroep als **LOCAL** voor het veld Gebruikersverificatie. Kies **vpool** als de clientadrespool voor het veld Toewijzing van clientadres. Kies **de standaardgroep** als het groepsbeleid voor het veld

Standaardbeleid.

Klik op OK en Toepassen.

### Opdrachtlijvoorbeeld

```

Cisco ASA

CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)#exit
CiscoASA(config)#crypto isakmp identity auto

!--- Phase 1 Configurations CiscoASA(config)#crypto
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map dynmap 10 set
transform-set myset
CiscoASA(config)#crypto map mymap 10 ipsec-isakmp
dynamic dynmap
CiscoASA(config)#crypto map mymap interface outside

!--- Phase 2 Configurations CiscoASA(config)#group-
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value

```

```

cisco.com
CiscoASA(config-group-policy)# exit

!--- Create a group policy "defaultgroup" with domain
name !--- cisco.com CiscoASA(config)#username vpnuser
password Cisco123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#memberof DefaultRAGroup
CiscoASA(config-username)#exit

!--- Create a user account "vpnuser" and added to !---
"DefaultGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes

!--- The Security Appliance provides the default tunnel
groups !--- for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)#address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the
address pool. CiscoASA(config-tunnel-general)#default-
group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the
tunnel group. CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-
attributes
CiscoASA(config-tunnel-ipsec)#trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer !---
authentication

```

## ASA-configuratieoverzicht

### Cisco ASA

```

CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ

```

```
security-level 90
ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
access-list 100 extended permit ip 10.2.2.0
255.255.255.0 10.5.5.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ip local pool vpnpool 10.5.5.10-10.5.5.20
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
route outside 172.16.5.0 255.255.255.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
crypto ca trustpoint CA1
enrollment terminal
subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco
Systems, C=US,
St=North Carolina,L=Rale
serial-number
keypair my.CA.key
crl configure
```

```
crypto ca certificate chain CA1
certificate 611ee59b000000000007
  308205a7 3082048f a0030201 02020a61 1ee59b00
00000000 07300d06 092a8648
  86f70d01 01050500 30513113 3011060a 09922689
93f22c64 01191603 636f6d31
  15301306 0a099226 8993f22c 64011916 05636973
636f3115 3013060a 09922689
  93f22c64 01191605 54535765 62310c30 0a060355
04031303 43413130 1e170d30
  37313231 35303833 3533395a 170d3039 31323134
30383335 33395a30 76310b30
  09060355 04061302 55533117 30150603 55040813
0e4e6f72 74682043 61726f6c
  696e6131 10300e06 03550407 13075261 6c656967
68311630 14060355 040a130d
  43697363 6f205379 7374656d 73312430 22060355
0403131b 43697363 6f415341
  2e636973 636f2e63 6f6d204f 553d5453 57454230
819f300d 06092a86 4886f70d
  01010105 0003818d 00308189 02818100 b8e20aa8
332356b7 5b660073 5008d373
  5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754
5e7f98d3 d4239b42 ab8faf0b
  e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a
b94b18ef 308eb12f 22ab1a8e
  db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9
03f722bd 414b0a32 05aa053e
  c45e2464 80606f8e 417f09a7 aa9c644d 02030100
01a38202 de308202 da300b06
  03551d0f 04040302 05a0301d 0603551d 11041630
14821243 6973636f 4153412e
  63697363 6f2e636f 6d301d06 03551d0e 04160414
2c242ddb 490cde1a fe2d63e3
  1e1fb28c 974c4216 301f0603 551d2304 18301680
14d9adbf 08f23a88 f114432f
  79987cd4 09a403e5 58308201 03060355 1d1f0481
fb3081f8 3081f5a0 81f2a081
  ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43
4e3d5453 2d57324b 332d4143
  532c434e 3d434450 2c434e3d 5075626c 69632532
304b6579 25323053 65727669
  6365732c 434e3d53 65727669 6365732c 434e3d43
6f6e6669 67757261 74696f6e
  2c44433d 54535765 622c4443 3d636973 636f2c44
433d636f 6d3f6365 72746966
  69636174 65526576 6f636174 696f6e4c 6973743f
62617365 3f6f626a 65637443
  6c617373 3d63524c 44697374 72696275 74696f6e
506f696e 74863568 7474703a
  2f2f7473 2d77326b 332d6163 732e7473 7765622e
63697363 6f2e636f 6d2f4365
  7274456e 726f6c6c 2f434131 2e63726c 3082011d
06082b06 01050507 01010482
  010f3082 010b3081 a906082b 06010505 07300286
819c6c64 61703a2f 2f2f434e
  3d434131 2c434e3d 4149412c 434e3d50 75626c69
63253230 4b657925 32305365
  72766963 65732c43 4e3d5365 72766963 65732c43
4e3d436f 6e666967 75726174
  696f6e2c 44433d54 53576562 2c44433d 63697363
6f2c4443 3d636f6d 3f634143
  65727469 66696361 74653f62 6173653f 6f626a65
6374436c 6173733d 63657274
```

69666963 6174696f 6e417574 686f7269 7479305d  
06082b06 01050507 30028651  
68747470 3a2f2f74 732d7732 6b332d61 63732e74  
73776562 2e636973 636f2e63  
6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b  
332d4143 532e5453 5765622e  
63697363 6f2e636f 6d5f4341 312e6372 74302106  
092b0601 04018237 14020414  
1e120057 00650062 00530065 00720076 00650072  
300c0603 551d1301 01ff0402  
30003013 0603551d 25040c30 0a06082b 06010505  
07030130 0d06092a 864886f7  
0d010105 05000382 0101008a 82680f46 fbc87edc  
84bc45f5 401b3716 0045515c  
2c81971d 0da51fe3 96870627 b41b4319 23284b30  
5eafcedb 10c1ef05 d0686a61  
cd1ab877 100b965d 499088e1 7de418fb b5529199  
46129b81 9c4353a2 1761b61c  
f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433  
bddef040 b4b0431e 7456fe29  
8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74  
97997a23 340fe65e 75601d32  
3522ec61 6aa39020 60f9a50e f963c593 88c80abd  
9750e2bb e285933c 53697efd  
b1e15148 fcca5cb3 cef27219 e0281fbc acf1c285  
2b19b30f 6ea733c4 1f62ff3b  
7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87  
7044e279 9b52b759 f02e9b1c  
94be67b8 fb1df0c6 9ec417  
quit  
certificate ca 7099f1994764e09c4651da80a16b749c  
3082049d 30820385 a0030201 02021070 99f19947  
64e09c46 51da80a1 6b749c30  
0d06092a 864886f7 0d010105 05003051 31133011  
060a0992 268993f2 2c640119  
1603636f 6d311530 13060a09 92268993 f22c6401  
19160563 6973636f 31153013  
060a0992 268993f2 2c640119 16055453 57656231  
0c300a06 03550403 13034341  
31301e17 0d303731 32313430 36303134 335a170d  
31323132 31343036 31303135  
5a305131 13301106 0a099226 8993f22c 64011916  
03636f6d 31153013 060a0992  
268993f2 2c640119 16056369 73636f31 15301306  
0a099226 8993f22c 64011916  
05545357 6562310c 300a0603 55040313 03434131  
30820122 300d0609 2a864886  
f70d0101 01050003 82010f00 3082010a 02820101  
00ea8fee c7ae56fc a22e603d  
0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d  
28ece906 02902f9a d1eb2b8d  
f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd  
ale906ec 88b32a19 38e5353e  
6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621  
876bd678 c8a37109 f074eabe  
2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7  
24b9e054 063c60a4 9b8d3c09  
351bc630 05f69357 833b9197 f875b408 cb71a814  
69a1f331 b1eb2b35 0c469443  
1455c210 db308bf0 a9805758 a878b82d 38c71426  
afffd272 dd6d7564 1cbe4d95  
b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67  
94b97ac7 63249009 fa05ca4d  
6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b

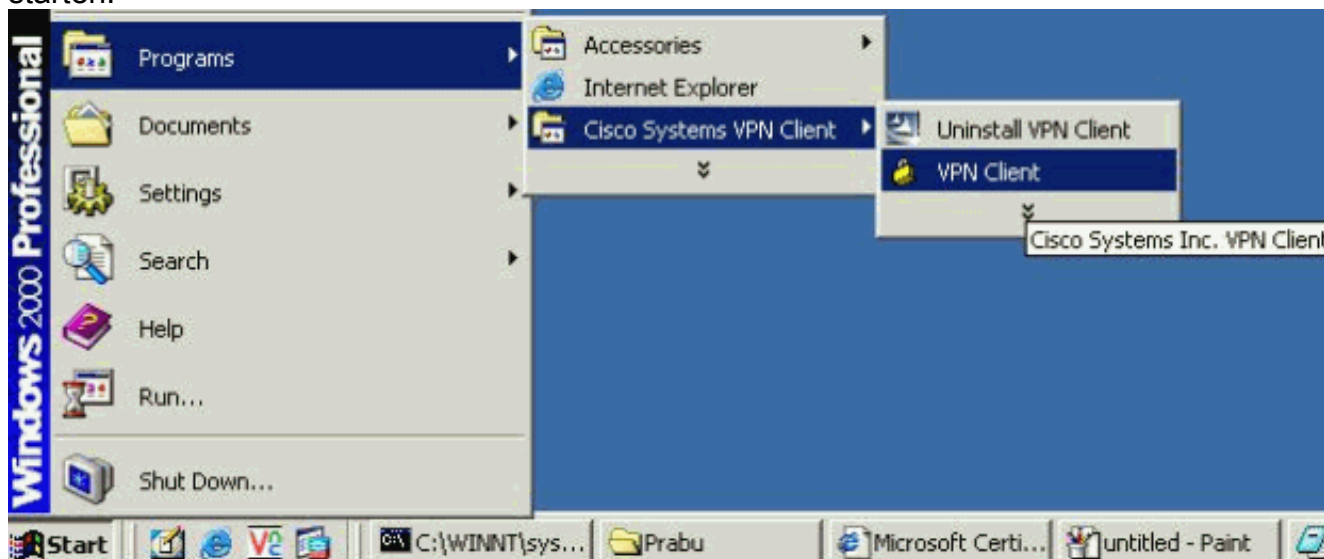
```
5f020301 0001a382 016f3082
  016b3013 06092b06 01040182 37140204 061e0400
43004130 0b060355 1d0f0404
  03020186 300f0603 551d1301 01ff0405 30030101
ff301d06 03551d0e 04160414
  d9adbf08 f23a88f1 14432f79 987cd409 a403e558
30820103 0603551d 1f0481fb
  3081f830 81f5a081 f2a081ef 8681b56c 6461703a
2f2f2f43 4e3d4341 312c434e
  3d54532d 57324b33 2d414353 2c434e3d 4344502c
434e3d50 75626c69 63253230
  4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f
  6e666967 75726174 696f6e2c 44433d54 53576562
2c44433d 63697363 6f2c4443
  3d636f6d 3f636572 74696669 63617465 5265766f
63617469 6f6e4c69 73743f62
  6173653f 6f626a65 6374436c 6173733d 63524c44
69737472 69627574 696f6e50
  6f696e74 86356874 74703a2f 2f74732d 77326b33
2d616373 2e747377 65622e63
  6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f
4341312e 63726c30 1006092b
  06010401 82371501 04030201 00300d06 092a8648
86f70d01 01050500 03820101
  001abc5a 40b32112 22da80fb bb228bfe 4bf8a515
df8fc3a0 4e0c89c6 d725e2ab
  2fa67ce8 9196d516 dfe55627 953aea47 2e871289
6b754e9c 1e01d408 3f7f0595
  8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b
  ab8e7f84 a011336b 37c13261 5ad218a3 a513e382
e4bfb2b4 9bf0d7d1 99865cc4
  94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92
860152d4 f06b2b15 df306433
  c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d
  aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76
13018f9f 5e3dce95 efe6da93
  f4cb3b00 102efa94 48a22fc4 7e342031 2406165e
39edc207 eddc6554 3fa9f396 ad
quit
crypto isakmp enable outside
crypto isakmp policy 65535
  authentication rsa-sig
  encryption 3des
  hash md5
  group 2
  lifetime 86400
crypto isakmp identity auto
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
```

```
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
group-policy defaultgroup internal
group-policy defaultgroup attributes
 default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
 memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
 address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
 trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#
```

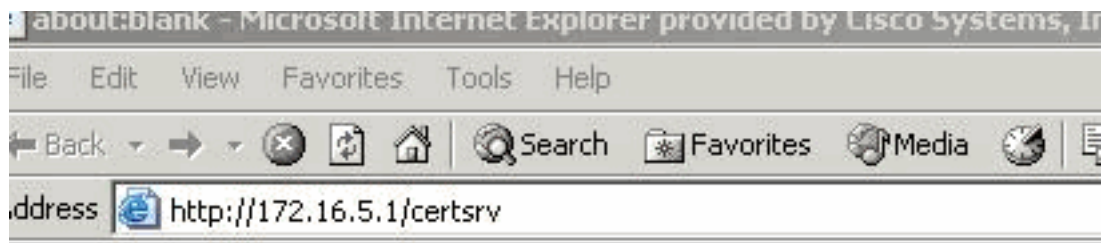
## VPN-clientconfiguratie

Voltooi deze stappen om de VPN-client te configureren.

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client** om de VPN-clientsoftware te starten.



2. Voltooi deze stappen om het CA-certificaat te downloaden van de CA-server genaamd **CA1** en het te installeren in Cisco VPN-client. Voer de weblognaam in de CA-server 172.16.5.1 uit met behulp van de aanmeldingsgegevens die aan de gebruiker worden



**Enter Network Password**

Please type your user name and password.

Site: 172.16.5.1

User Name: vpnuser

Password: xxxxxxxx

Domain:

Save this password in your password list

OK Cancel

geleverd.

**Opmerking:** Zorg dat u een gebruikersaccount hebt voor de VPN-clientgebruiker bij de CA-server. Klik op **Download een CA certificaat, certificaatketen of CRL** om het venster te openen, zoals weergegeven. Klik op de radioknop **Base64** als de coderingsmethode en klik op **CA-certificaat downloaden**.



## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

### CA certificate:



### Encoding method:

- DER
- Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

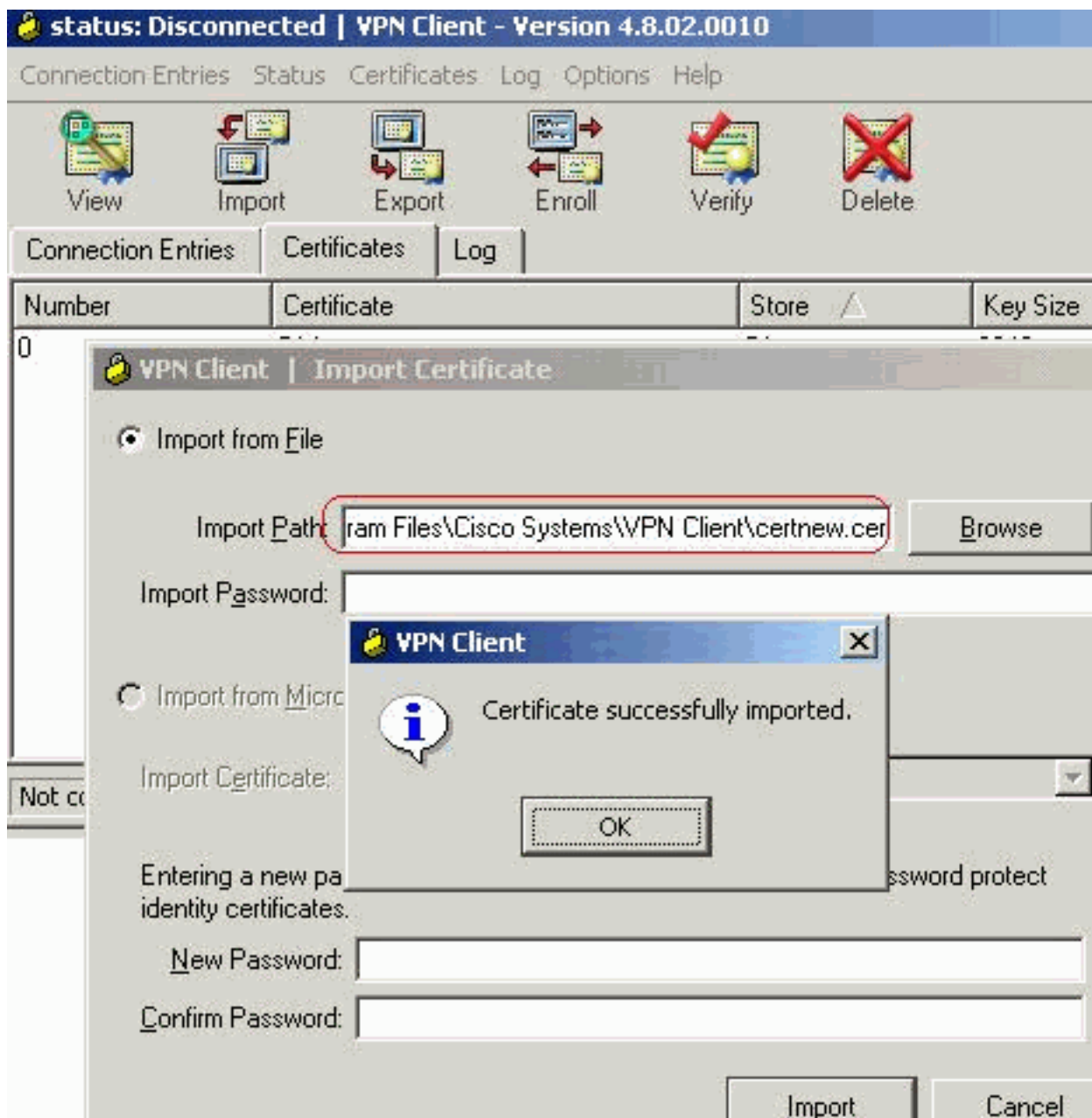
[Download latest delta CRL](#)

Sla het CA-certificaat op met de naam **certnew.cer** op uw computer. Standaard wordt de software opgeslagen in het C:\Program Files\Cisco Systems\VPN Client-



pad.

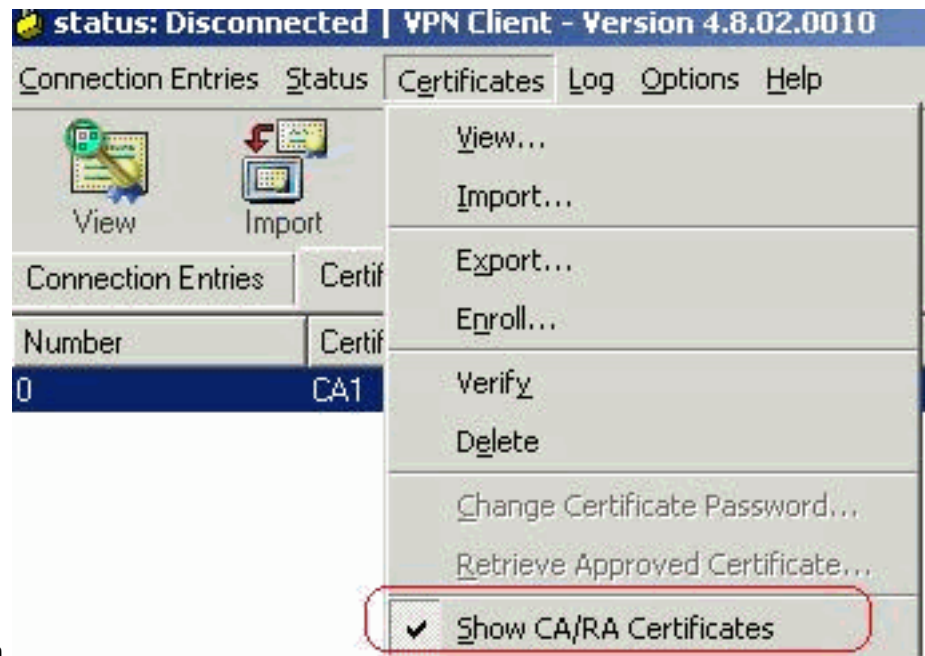
Kies in de VPN-client het tabblad **Certificaten > Importeren** en klik vervolgens op de knop **Importeren uit Fildio**. Klik op **Bladeren** om het CA-certificaat te importeren van de opgeslagen locatie C:\Program Files\Cisco Systems\VPN Client, zoals getoond. Klik op **Importeren**. Er verschijnt een succesvenster, zoals wordt getoond.



het tabblad Certificaten verschijnt de CA1-certificaten, zoals aangegeven.



**Opmerking:** Zorg ervoor dat de optie **CA/RA-certificaten** weergegeven is geselecteerd, zoals aangegeven, anders worden de CA-certificaten niet in het certificaatvenster



weergegeven.

3. Voltooi deze stappen om het identiteitsbewijs te downloaden en het in de VPN-client te installeren. Kies in de CA1-server een **certificaataanvraag > een geavanceerd certificaatverzoek > Aanvragen** en dien een verzoek in bij deze CA om zich in te schrijven voor het identiteitsbewijs. Klik op **Inzenden**.

## Certificate Template:

---

User ▼

## Key Options:

---

Create new key set     Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Key Usage:  Exchange

Key Size:     Min: 384    Max: 16384    (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name     User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

## Additional Options:

---

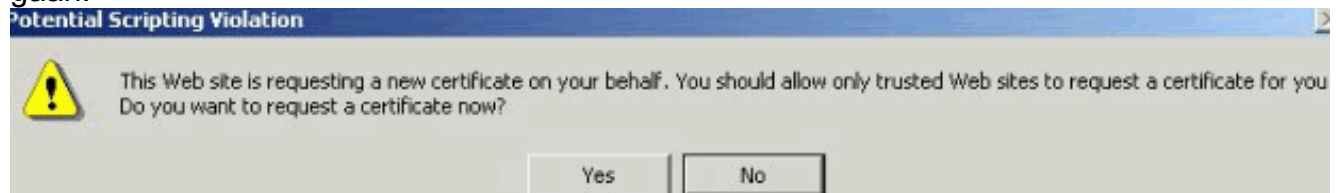
Request Format:  CMC     PKCS10

Hash Algorithm:  ▼

*Only used to sign request.*

Save request to a file

Klik op **Ja** om verder te gaan.



Klik op **Installeer dit**

**Microsoft Certificate Services -- CA1**

## Certificate Issued

---

The certificate you requested was issued to you.

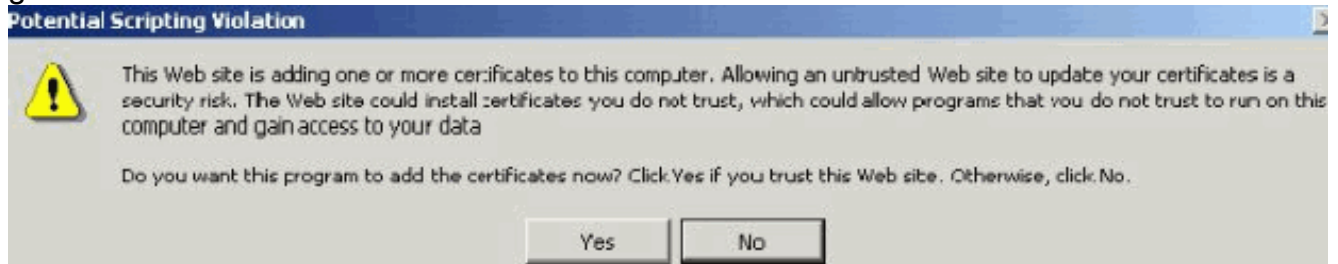
certificaat.



[Install this certificate](#)

Klik op **Ja** om verder

te  
gaan.



U moet het geïnstalleerde bericht van het certificaat ontvangen, zoals wordt

**Microsoft Certificate Services -- CA1**

## Certificate Installed

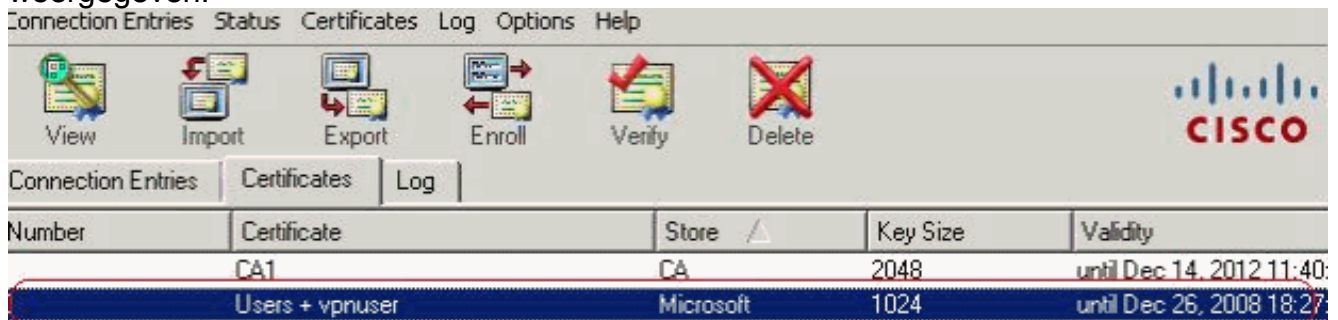
Your new certificate has been successfully installed.

weergegeven.

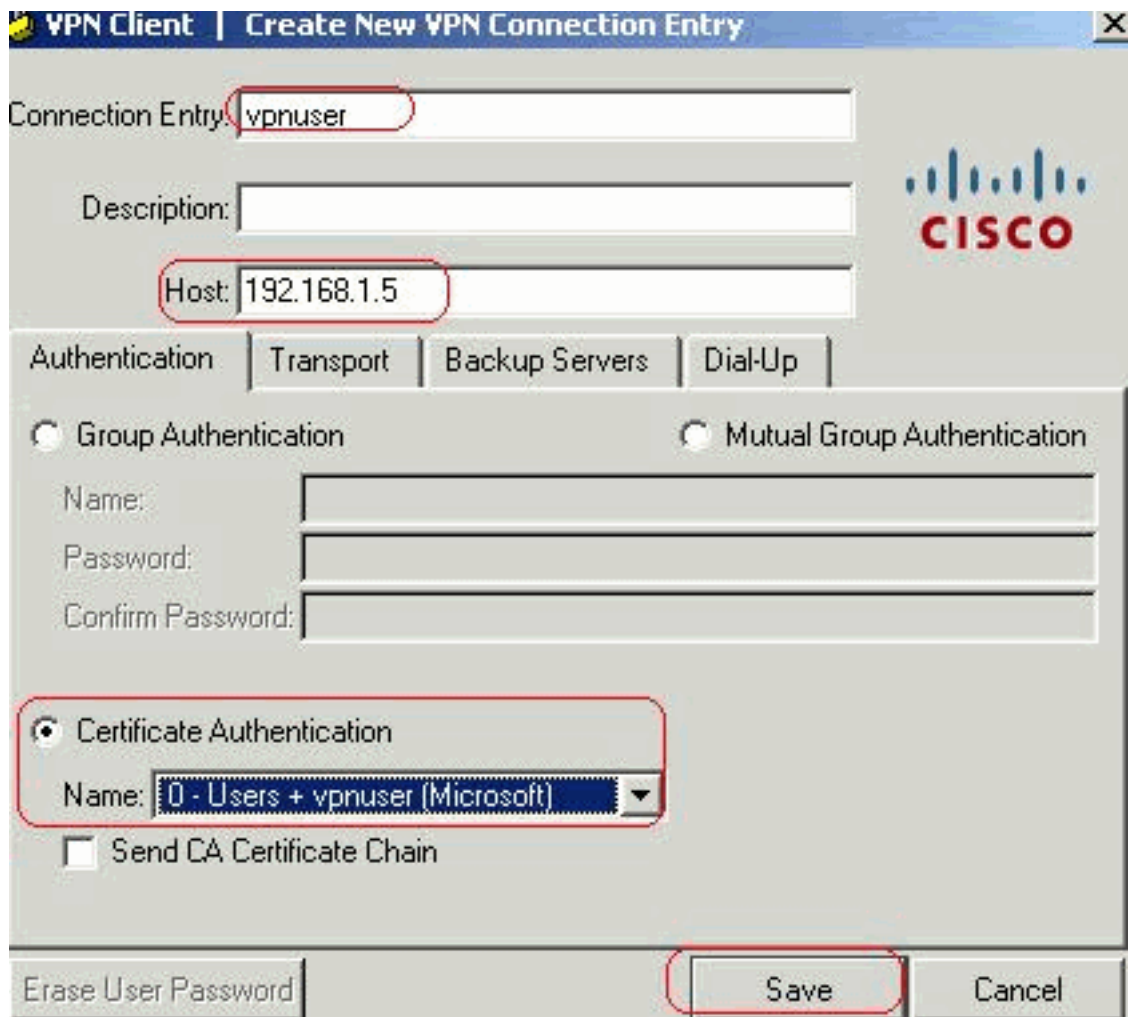
Sluit de

VPN-client af en start de client opnieuw om het geïnstalleerde identiteitsbewijs te laten  
verschijnen in het tabblad certificaat van de VPN-client, zoals

weergegeven.

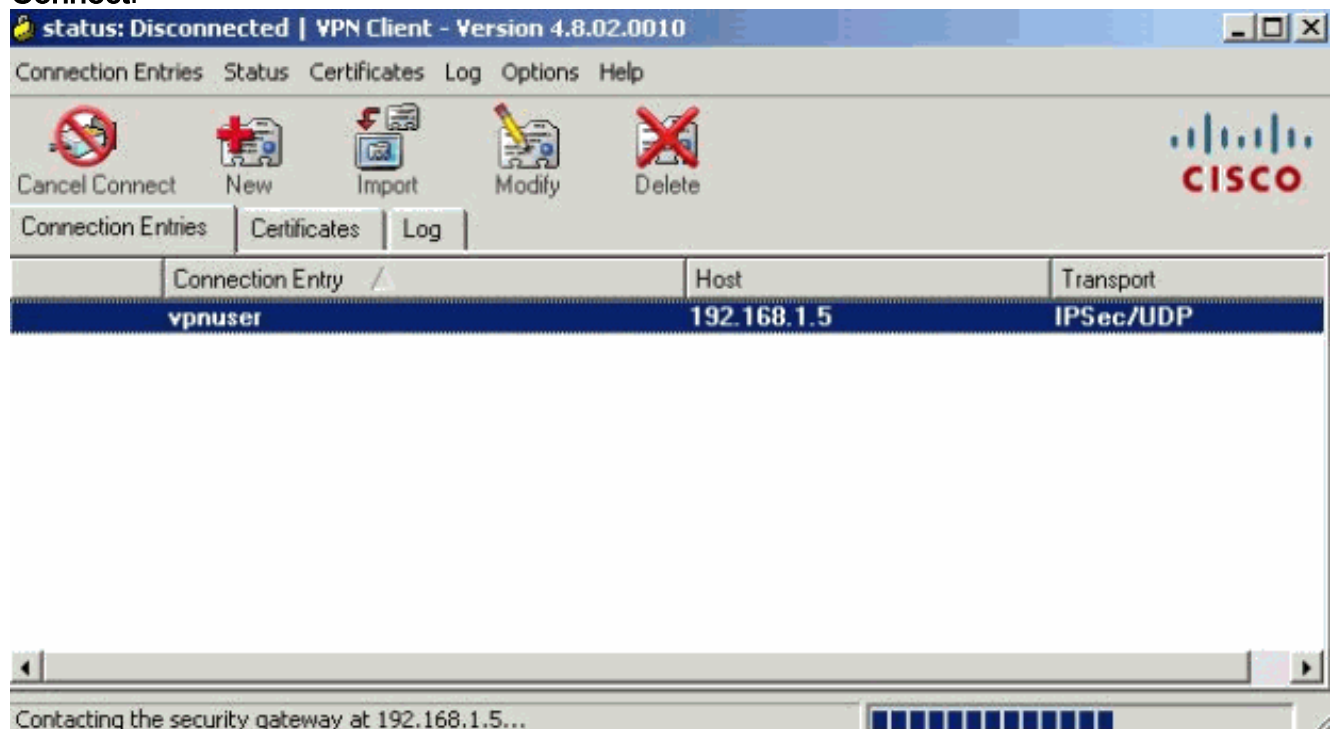


- In het tabblad Connection klikt u op **Nieuw** om een **videogebruiker** voor verbinding **te maken**, zoals aangegeven in de afbeelding. Voer het externe IP-adres (routeerbaar) in het veld Host in. Klik op het radioknop **certificaatverificatie** en kies het identiteitsbewijs in de vervolgkeuzelijst, zoals weergegeven. Klik op



Opslaan.

5. Klik op Connect.

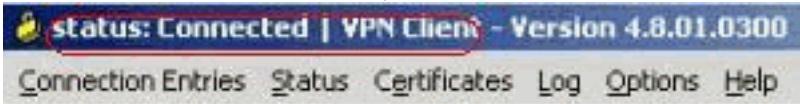


6. Voer desgevraagd de informatie over de naam van de gebruiker en het wachtwoord in voor de volledige tekst en klik vervolgens op OK om verbinding te maken met het externe



netwerk.

7. De VPN-client verbindt met de ASA, zoals wordt



getoond.

## Verifiëren

In de ASA kunt u verschillende show opdrachten op de opdrachtregel uitvoeren om de status van een certificaat te verifiëren.

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

- De **show crypto ca trustpoint** opdracht toont geconfigureerde kruispunten.

```
CiscoASA#show crypto ca trustpoints
```

```
Trustpoint CA1:
```

```
Subject Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Serial Number: 7099f1994764e09c4651da80a16b749c
```

```
Certificate configured.
```

- De opdracht **Encrypt** alle certificaten die op het systeem zijn geïnstalleerd, worden weergegeven.

```
CiscoASA# show crypto ca certificate
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 3f14b70b00000000001f
```

```
Certificate Usage: Encryption
```

```
Public Key Type: RSA (1024 bits)
```

```
Issuer Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Subject Name:
```

```
cn=vpnserver
```

```
cn=Users
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
PrincipalName: vpnserver@TSWeb.cisco.com
```

```
CRL Distribution Points:
```

```
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

```
[2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
```

```
Validity Date:
```

start date: 14:00:36 UTC Dec 27 2007  
end date: 14:00:36 UTC Dec 26 2008  
Associated Trustpoints: CA1

#### CA Certificate

Status: Available  
Certificate Serial Number: 7099f1994764e09c4651da80a16b749c  
Certificate Usage: Signature  
Public Key Type: RSA (2048 bits)  
Issuer Name:  
cn=CA1  
dc=TSWeb  
dc=cisco  
dc=com  
Subject Name:  
cn=CA1  
dc=TSWeb  
dc=cisco  
dc=com  
CRL Distribution Points:  
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,  
CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,  
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint  
[2] http://ts-w2k3-ac.s.tsweb.cisco.com/CertEnroll/CA1.crl  
Validity Date:  
start date: 06:01:43 UTC Dec 14 2007  
end date: 06:10:15 UTC Dec 14 2012  
Associated Trustpoints: CA1

#### Certificate

Subject Name:  
Name: CiscoASA.cisco.com  
Status: Pending terminal enrollment  
Key Usage: General Purpose  
Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345  
Associated Trustpoint: CA1

- De opdracht **Encrypt CMS toont** gecacheerde certificeringslijsten (CRL).
- De **show crypto key mypubkey rsa** opdracht geeft alle gegenereerde crypto sleutelparen weer.

```
CiscoASA# show crypto key mypubkey rsa
Key pair was generated at: 01:43:45 UTC Dec 11 2007
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
Key pair was generated at: 06:36:00 UTC Dec 15 2007
Key name: my.CA.key
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
Key pair was generated at: 07:35:18 UTC Dec 21 2007
```



CiscoASA#

- De opdracht **show crypto isakmp sa** geeft de IKE 1 tunnelinformatie weer.

```
CiscoASA#show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 10.1.1.5
  Type      : user           Role      : responder
  Rekey     : no            State     : MM_ACTIVE
```

- De **show crypto ipsec sa** opdracht toont de IPsec tunnelinformatie.

```
CiscoASA#show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
current_peer: 10.1.1.5, username: vpnuser
dynamic allocated peer ip: 10.5.5.10
```

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FF3EEE7D
```

```
inbound esp sas:
```

```
spi: 0xEFDF8BA9 (4024404905)
  transform: esp-3des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28314
  IV size: 8 bytes
  replay detection support: Y
```

```
outbound esp sas:
```

```
spi: 0xFF3EEE7D (4282314365)
  transform: esp-3des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28314
  IV size: 8 bytes
  replay detection support: Y
```

Het [Uitvoer Tolk \(uitsluitend geregistreeerde klanten\)](#) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

## [Problemen oplossen](#)

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Hier zijn een paar mogelijke fouten die u kunt tegenkomen:

- **FOUT: Kan geïmporteerd certificaat niet verwijderen of controleren** Deze fout kan voorkomen wanneer u het identiteitsbewijs installeert en niet het juiste tussenpersoon of de wortel CA certificaat heeft dat met het verbonden trustpunt voor authentiek is verklaard. U moet het juiste tussenpersoon- of basiscertificaat verwijderen en opnieuw bevestigen. Neem contact op met uw derde verkoper om te controleren of u het juiste CA-certificaat hebt ontvangen.
- **Het certificaat bevat geen openbare sleutel voor algemene doeleinden** Deze fout kan voorkomen wanneer u probeert om uw identiteitsbewijs te installeren op het verkeerde schaalpunt. U probeert een ongeldig identiteitsbewijs te installeren, of het sleutelbaar dat aan het Trustpoint is gekoppeld, komt niet overeen met de openbare sleutel in het identiteitsbewijs. Geef de opdracht **show crypto ca certificaten trustpointname uit** om te controleren of u uw identiteitsbewijs op het juiste punt hebt geïnstalleerd. Kijk naar de regel met **bijbehorende trustpoints**: Als het foute vertrouwen in een lijst staat, gebruikt u de in dit document beschreven procedures om het juiste punt van vertrouwen te verwijderen en opnieuw te installeren. Controleer ook of het sleutelbaar niet is gewijzigd sinds de CSR is gegenereerd.
- **FOUT : ASA/PIX. Sev=Waarschuwing/3 IKE/0xE300081 Ongeldig id voor extern certificaat:** Als u verificatieproblemen hebt met certificaten, kan deze foutmelding in de VPN-client verschijnen. Gebruik de opdracht **crypto isakmp Identity auto** in de ASA/PIX configuratie om het probleem op te lossen.

## Gerelateerde informatie

- [Cisco-pagina voor adaptieve security applicatie](#)
- [Cisco VPN-clientondersteuningspagina](#)
- [Microsoft Server configureren als certificeringsinstantie \(CA\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)