# ASA/PIX 7.x en VPN-client-IPSec-verificatie met digitale certificaten met Microsoft CAconfiguratievoorbeeld

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Configureren Netwerkdiagram Configuraties ASA-configuratie ASA-configuratie ASA-configuratie VPN-clientconfiguratie Verifiëren Problemen oplossen Gerelateerde informatie

# **Inleiding**

Dit document beschrijft hoe u een digitaal certificaat van een derde partij voor verkoper handmatig kunt installeren op de Cisco security applicatie (ASA/PIX) 7.x en op VPN-clients, om IPSec-peers te authentiseren met Microsoft certificaatserver (CA).

# **Voorwaarden**

# **Vereisten**

Dit document vereist dat u toegang hebt tot een certificeringsinstantie (CA) voor de inschrijving van certificaten. Ondersteunde CA-verkopers van derden zijn onder meer Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA en VeriSign.

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

**N.B.:** Dit document gaat ervan uit dat er geen bestaande VPN-configuratie in de ASA/PIX is geïnstalleerd.

## Gebruikte componenten

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

- ASA 5510 dat softwareversie 7.2(2) en ASDM versie 5.2(2) draait.
- VPN-client met softwareversie 4.x en hoger

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 7.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 <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

## **Netwerkdiagram**

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 gebruikt zijn.

## **Configuraties**

Dit document gebruikt deze configuraties:

- <u>ASA-configuratie</u>
- <u>ASA-configuratiesoverzicht</u>
- <u>VPN-clientconfiguratie</u>

## ASA-configuratie

Voltooi deze 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. Generate RSA Key Pair

Stap 3. Maak het Trustpunt.

Stap 4. Generate the certificaatinschrijving.

Stap 5. Verifieer het Trustpoint

Stap 6. Installeer het certificaat

Stap 7. 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 **Properties**.
- 2. Apparaatbeheer uitvouwen en Kloktijd kiezen.
- 3. Controleer of de verstrekte informatie juist is.De waarden voor Datum, Tijd en Tijdzone moeten nauwkeurig zijn zodat een goede certificatie kan plaatsvinden.



Cisco ASA
CiscoASA# <b>show clock</b>
16:25:49.580 IST Fri Dec 28 2007

#### Stap 2. Generate RSA Key Pair

De gegenereerde openbare RSA-toets wordt gecombineerd met de identiteitsinformatie van de ASA om een PKCS#10-certificaataanvraag te vormen. U dient de sleutelnaam duidelijk te identificeren met het schaalpunt waarvoor u het sleutelpaar maakt.

#### ASDM-procedure

- 1. Klik op Configuration en vervolgens op Properties.
- 2. Vergroot Certificaat, en kies Toetsenbord.
- 3. Klik op

Toevoegen.

Configuration > Properties > Certifi	icate > Key Pair			
	ey Pair			
🗄 🖬 AAA Setup	Configure the here weive to be wood in and	Maskan		
	Configure the key pairs to be used in cen	incates.		
E-B ARP				
	Note: Operations on this screen are appli	ed immediately upon	completion and are irreve	ersible.
😑 🐼 Certificate				
- Authentication				
Enrolment	Key Pair Name	Usane	Modulus Size	b aba
- El Import Certificate	They Four House	osayo	11000003-0120	Add
- Star Key Pair				
Manage Cartificat				Show Details
🗄 🙀 Trustpoi 🚺 Add Key Pa	ir	×		
E f Device Acce				Delete
E 30 Device Admi	C Harden alexandre			
Banner Name:	<ul> <li>Use default key name</li> </ul>			Defrach
Boot Ime	G mu CA Inul			Reiresn
CLI Prom	(* my.c.A.key)			
Clock				
Console Size:	1024			
🛅 CSD Set	·			
Of Device Usage	🗧 🕝 General Purpose 🛛 C. Specia			
FTP Moc				
ICMP Ru				
Manager				
O NTP Generate N	Now Cancel He	4p di		
Passwo				

- 4. Voer de naam van de toets in, kies de modulegrootte en selecteer het gebruikte type.**Opmerking:** de aanbevolen grootte van een sleutelpaar is 1024.
- 5. Klik op **Generate Now**.Het sleutelpaar dat u hebt gemaakt, moet in de kolom Naam sleutelpaar worden vermeld.

Cisco ASA
CiscoASA#configure terminal
CiscoASA(config)#crypto key generate rsa label my.CA.key modulus 1024
<pre>! 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)#</pre>

#### Stap 3. Maak het Trustpunt

Trustpoints zijn vereist om de certificaatinstantie (CA) te verklaren die uw ASA zal gebruiken.

#### ASDM-procedure

- 1. Klik op Configuration en vervolgens op Properties.
- 2. Certificaat uitvouwen, en Trustpoint uitvouwen.
- 3. Kies **Configuration** en klik op **Add**.

Configuration > Properties > C	ertificate >	Trustpoint > Config	guration		
Startup Wizard	Configur	ation			
🖭 🚽 AAA Setup	1	imme e Cerdificate Aud	havity (CA) as a tructuralist		
	Con	igure a Certificate Aut	nonty (CA) as a trustpoint.		
🖭 🐻 ARP					
				(	
🖃 🔂 Certificate		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add
Authentication					
Enrolment					Edit
Import Certificate					
- 😽 Key Pair					
Manage Certificat					Delete
Arustpoint					
Configuration					Request (
Export					
import		1			

- 4. Configuratie van deze waarden: Naam van het schaalpunt: De naam van het trustpunt moet relevant zijn voor het beoogde gebruik. (Dit voorbeeld gebruikt CA1.)Belangrijk paar: Selecteer het sleutelpaar dat in <u>Stap 2</u> gegenereerd is. (my.CA.key)
- 5. Zorg ervoor dat handmatige inschrijving is geselecteerd.
- 6. Klik op certificaatparameters. Het dialoogvenster certificaatparameters verschijnt.
- 7. Klik op **Bewerken** en stel de kenmerken 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

roevoegen.					
🔂 Edit DN					
				Attribute	Value
				Common Name (CN)	CiscoASA cisco.com
DN Attribute	to be Added			Department (OU)	TSWEB
			1	Company Name (O)	Cisco Systems
Attribute:	Select Attribute	▼	Add >>	Country (C)	US
				State (St)	North Carolina
Value:			Delete	Location (L)	Raleigh
	, ,				
				J	
	0	к	Cancel	Help	

- 8. Klik op **OK** als de juiste waarden zijn toegevoegd.
- 9. Typ in het dialoogvenster certificaatparameters de FQDN in het veld FQDN specificeren.Deze waarde moet gelijk zijn aan FQDN dat u gebruikt voor de gezamenlijke

	💼 Certificate Parameters
	Enter the values for the parameters that are to be included in the certi
	Subject DN: Systems,C=US,St=North Carolina,L=Raleigh
	Subject Alternative Name (FQDN)
	O Use FQDN of the device
	Specify FQDN     CiscoASA.cisco.com
	O Use none
	E-mail:
	IP Address:
	Include device serial number
naam (CN).	OK Cancel Help

- 10. Klik op OK.
- 11. Controleer of het juiste paar is geselecteerd en klik op de radioknop **Handmatige inschrijving** gebruiken.
- 12. Klik op **OK** en vervolgens op **Toepassen**.

💼 Add Trustpoint Configuration	
Trustpoint Name:	
Generate a self-signed certificate on enrollment	
If this option is enabled, only Key Pair and Certific	cate Parameters can be specified.
Enrollment Settings Revocation Check CRL Retrie	eval Policy CRL Retrieval Method OCSP
Key Pair: my.CA.key 🗾 S	how Details New Key Pair
Challenge Confi Password: Passv	rm Challenge word:
Enrollment Mode can only be specified if there are	e no certificates associated with this trust
Enrollment Mode	
Use manual enrollment	
C Use automatic enrollment	
Enrollment URL: http://	
Retry Period: 1 minur	tes
Retry Count: 0 (Use	e 0 to indicate unlimited retries)
	Certificate Parameter
ок	Cancel Help

Cisco ASA
CiscoASA(config)#crypto ca trustpoint CA1
<pre>! Creates the trustpoint. CiscoASA(config-ca- trustpoint)#enrollment terminal</pre>
! Specifies cut and paste enrollment with this
<pre>trustpoint. CiscoASA(config-ca-trustpoint)#subject-name</pre>
CN=wepvpn.cisco.com,OU=TSWEB,
O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh
! Defines x.500 distinguished name. CiscoASA(config-



#### Stap 4. De certificaatinschrijving genereren

#### ASDM-procedure

- 1. Klik op Configuration en vervolgens op Properties.
- 2. Vul Certificaat uit en kies Invoegen.
- 3. Controleer het schaalpunt dat in <u>Stap 3</u> is gemaakt, en klik op **Invoegen**.Er verschijnt een dialoogvenster dat een lijst geeft van het verzoek om inschrijving voor het certificaat (ook aangeduid als een aanvraag voor ondertekening van het certificaat)

付 Enro	ollment Request	
To ma	complete the enrollment process, please paste the following PKCS10 enrollment request into th magement interface of the CA.	e
Yo	ou will need to install the certificate after receiving it.	
Go	to Configuration > Properties > Certificate > Import Certificate to do so.	
Cei	rtificate Request:	
h	vcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvcN	
A	QEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm	
p	SMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJHZdsBoLSGhlKY MH40WFVbil9PHZSSgrpV6PCoiC9Pil7wdgCggtrD404/lYD0ooFVfg7opCWwWFV	
A	m40w0AB118BH2SSGxFA8BGE1C5Bj62VdqCgq+xk404/11F60eRk1q/apch00HF gMBAAGgR1BEBgkghkiG9w0BC04xNzA1MAsGA1UdDw0EAw1FoDAmBgNVHREEHzAd	
gi	htDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA	
gn	moBmSRVnLOqyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3	
gi	EjVABVhB7Ni6N29710mDAbnPsOR3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0	
g	onnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=	
		4
	End - This line not part of the certificate request	<b>•</b>
	ок	

4. Kopieer het registratieverzoek van PKCS#10 naar een tekstbestand en dien vervolgens de opgeslagen CSR naar uw verkoper van een derde partij (zoals Microsoft CA) in zoals in deze procedure:Meld u aan bij de CA-server 172.16.5.1 met de gebruikerswoordenboeken die op de VPN-server zijn meegeleverd.

👰 about:blank - Microsoft I	nternet Explore	r provided by	' Cisco Sys	tems, Inc.	
File Edit View Favorites	Tools Help				
🖛 Back 🔻 🔿 👻 🙆 🐔	ථු 🛛 🔕 Search	🚡 Favorites	Media	🎯   🖏 -	4 e e
Address (http://172.16.5.1)	certsry				
Enter Net	work Password				? ×
<b>e</b> -2					
P 20	Please type you	r user name and	l password.		
V	Site:	172.16.5.1			
	User Name	vpnuser			
	Password	******		)	
	Domain				
	🔲 Save this pa	assword in your p	password list	t	
			ОК		Cancel

**Opmerking:** Zorg ervoor dat u een gebruikersaccount hebt voor de ASA (VPN-server) met de CA-server.Klik op **Aanvragen van een certificaat > Geavanceerd certificaatverzoek** en selecteer **Een certificaataanvraag indienen door een basis-64-gecodeerde CMC of PKCS#10** bestand te gebruiken of een hervernieuwingsaanvraag in te dienen door een basis-64-gecodeerd PKCS#7-bestand te

gebruiken.

Address 🗃 http://172.16.5.1/certsrv/certrqad.asp	i∂iso Ur
Microsoft Certificate Services CA1	Home
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options to:	
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request a base-64-encoded PKCS #7 file.	by using
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment st Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	ation.
Kopieer en plak de gecodeerde informatie naar het veld <b>Opgeslagen aanvraag</b> en klik (	эр

Kopieer en plak de gecodeerde informatie naar het veld **Opgeslagen aanvraag** en klik 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	
Certificate Temp	late:	
	IPSEC -	
Additional Attrib	utes:	
Attributes:		
	Submit >	≺lik op

de radioknop Base64 encoded en klik op Download

het dialoogvenster Bestand downloaden verschijnt, slaat u dit op met de naam **cert\_client\_id.cer**, het identiteitsbewijs dat op de ASA moet worden

	File Down	load	X
	?	Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open o save this file.	ır
		File name: certnew.cer	
		File type: Security Certificate	
		From: 172.16.5.1	
		This type of file could harm your computer if it contains malicious code.	
		Would you like to open the file or save it to your computer?	
		Open Save Cancel More Info	
		✓ Always ask before opening this type of file	
geïnstalleerd.			

Cisco ASA
CiscoASA(config)#crypto ca enroll CA1
<pre>! Initiates CSR. This is the request to be submitted ! via web or email to the 3rd 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</pre>
<pre>! Do not include the device's serial number in the subject. Display Certificate Request to terminal? [yes/no]: yes</pre>
<pre>! 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 3rd party CA. Certificate Request follows: MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT Dk5vcnRo</pre>
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3 DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB 9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt 3oMXSNPO
mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw

```
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BM05lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpf0kjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no
ciscoasa(config)#
```

## Stap 5. Verifieer het Trustpoint

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

#### ASDM-procedure

- 1. Sla het identiteitsbewijs op de plaatselijke computer op.
- 2. Als u een basis64 gecodeerd certificaat kreeg dat niet als bestand kwam, moet u het Base64-bericht kopiëren en het in een tekstbestand plakken.
- 3. Hernoemen het bestand met een .cer-extensie.**Opmerking:** Zodra het bestand een andere naam heeft gekregen dan de .cer extensie, dient het bestands pictogram weer te geven als



een certificaat zoals weergegeven.

4. Dubbelklik op het

Certificate	
General Details Certification Path	
Certificate Information	_
Thile certificate is intended for the following purpose(s):	
<ul> <li>Ensures the identity of a remote computer</li> <li>Proves your identity to a remote computer</li> <li>2.16.840.1.113733.1.7.21</li> </ul>	

certificaatbestand.

**rking:** Als het bericht "Windows niet voldoende informatie heeft om dit certificaat te controleren" in het tabblad Algemeen verschijnt, moet u het certificaat van de derde krachtoplossing CA of tussenpersoon CA verkrijgen voordat u doorgaat met deze procedure. Neem contact op met uw derde verkoper of CA-beheerder om de afgifte van de basiscertificaat voor CA of een tussenstation voor CA te verkrijgen.

- 5. Klik op het tabblad certificaatpad
- 6. Klik op het CA-certificaat boven het door u afgegeven identiteitsbewijs en klik op **Weergavecertificaat**.

Certificate		?	>
General Details Certification Path			
Certification path			
	<u>V</u> iew Cer	tificate	
Certificate <u>s</u> tatus:			
This certificate is OK.			
		ОК	Gedetailleerde

informatie over het CA-certificaat verschijnt.

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

General Details Certification P	Path	<u> </u>
Show: <a href="https://www.show-angle-show-a</th> <th></th> <th></th>		
Field	Value	<b>_</b>
Version	V3	
Serial number	611E E59B 0000 0000 0007	
Signature algorithm	sha1RSA -	
Issuer	CA1, TSWeb, cisco, com	
Valid from	Saturday, December 15, 2007	
Valid to	Monday, December 14, 2009	
Subject	CiscoASA.cisco.com OU=TSW	_
	RSA (1024 Bits)	<b>-</b>
	Edit Properties Copy to File	
	ОК	

identiteitsbewijs.

8. Voordat u het identiteitsbewijs installeert, moet het CA certificaat van de server van CA worden gedownload en in de ASA worden geïnstalleerd. Voltooi deze stappen om het CA-certificaat te downloaden van de CA-server genaamd *CA1*:Meld u aan bij de CA-server 172.16.5.1 met gebruikerswoordenboeken die aan de VPN-server zijn

🎒 abo	out:blank - Micro	soft Internet Explor	er	
Eile	<u>E</u> dit <u>V</u> iew F <u>a</u> v	vorites <u>T</u> ools <u>H</u> elp		
🕞 Bar	:k 🔻 🕘 👻 📕	😰 🏠 🔎 Search	☆ Favorites	1
A <u>d</u> dres	s 🥘 http://172.1	6.5.1/certsrv		
	c 11 (70			
	Connect to 172.	16.5.1	12/10	ŶX
	Connecting to 17	72.16.5.1		
	<u>U</u> ser name:	🕵 vpnserver	-	
	Password:	•••••		
		Remember my	password	
		ОК	Cano	:el

**Download een CA certificaat, certificeringsketen of CRL** en selecteer vervolgens de **Base 64** radioknop om de coderingsmethode te specificeren.Klik op het **CA-certificaat downloaden**.



Sla het CA-certificaat op uw computer op met de naam

File D	own	load - Secu	rity Warning				×
Do	) you	want to op	en or save th	is file?			
		Name: Type: From:	certnew.cer Security Certifi 172.16.5.1 <u>O</u> pen	cate, 1.	64 KB <u>S</u> ave	Cancel	
r		While files fr potentially h open or sav	om the Internet ( arm your comput e this software, <u>)</u>	can be u :er. If yo <u>What's t</u>	useful, this fil u do not trus <u>he risk?</u>	e type can t the source, do r	not

#### certnew.cer.

- 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 verschijnt evenveel als het certificaat in deze afbeelding:

📝 certnew.cer - Notepad <u>File Edit Format Help</u> ----BEGIN CERTIFICATE--MIIEnTCCA4WqAwIBAqIQcJnxmUdk4JxGUdqAoWt0nDANBqkqhkiG9w0BAQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT Bqojkiajk/IszaezFqvuu1dlyjeMMAoGA1uEAxMDQ0ExMB4xDTA3MTIxNDA2MDE0 MÍoXDTEVMTIXNDA2MTAXNVOWUTETMBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmS DomT8ixkARkwBwNpc2NvMRUwEwYKCZImiŹPyLGQBGRYFVFNXZWIXDDAKBgNVBĀMT AONBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuvvyiLmA9 BSGzMz3sCtR9TCMwOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5zd4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vŴeMijcQnŵdOq+ kx+sWaeNCjš1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI //3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXwKh4uC04xxQmr//Sct1tdwQcvk2V µBwCsptw7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDhXX wPXR018CAwEAAa0CAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQE AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYfNQJ pAP1wDccAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsawM]MjBLZXk]MjBTZXJ2aWN]cyxD Tj1TZXJŽaWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD PŴNvbT9jZXJ0aŴZpYŹF0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9 Y1JMRGlźdHJpYnV0aw9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j aXNjby5jb20vQ2vydEVucm9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHqHUCD9/BZWAqfmGUm++HMljnW8liyIF pcNwxlqxsDT+n9Y0k6bnG6u0f4SgETNrN8EyYVrSGK0lE+0C5L+ytJvw19GZhlzE 10VUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCqFWNcNItcufu0x1b 1xxc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlvD+p85at ----END CERTIFICATE-----

- 12. Klik binnen ASDM op Configuration en vervolgens op Properties.
- 13. Vul Certificaat uit en kies Verificatie.
- 14. Klik op de radioknop Voer de certificaattekst in in in hexadecimaal of in basis64-formaat.
- 15. Plakt het basis64-geformatteerde CA-certificaat van uw teksteditor in het tekstgebied.
- 16. Klik op

Verifiëren.

Configuration > Properties > Ce	rtificate > Authentication
Startup Wizard	Authentication
🗄 🚽 🖌 AAA Setup	Authenticate a CA cartificate. As the vacuit of authentication, the CA cartificate will be account
Anti-Spoofing	Authenticate a CA certificate. As the result of authentication, the CA certificate will be assor trustpoint and installed on the device
🖭 📆 ARP	a aspoint and installed on the device.
	Trustnaist blaver
	CA1
E- Certificate	
Authentication	Fingerprint (optional):
Enrollment	
	The certificate text can be specified if the selected trustpoint is configured for manual
- 🚟 Key Pair	
Manage Certificat	Certificate Text
🖻 🔯 Trustpoint	
Configuration	C Import from a file: Browse
🔛 Export	
- 🖗 Import	<ul> <li>Enter the certificate text in hexadecimal or base64 format:</li> </ul>
E 👔 Device Access	6786.IGM/LRhf5//VplTraRv6HEpirdLl6cHpHLICD9/B70/AptmGLlm++HMin/A
E 🛞 Device Administration	DCSL+v4.lvvv1
- 🗐 Banner	Authentication Successful
Boot Image/Config	wGPn149zp.
CLI Prompt	
Clock —	The trustpoint CA1 has been authenticated.
Console	
CSD Setup	<u>•</u>
Device	
FTP Mode	OK
ICMP Rules	
Management Acc	
O NTP	
Password	
Secure Copy	
SMTP	
SNMP I	Authenticate

# 17. Klik op **OK**.

Opdrachtlijnvoorbeeld

Cisco ASA
CiscoASA(config)#crypto ca authenticate CA1
<pre>! Initiates the prompt to paste in the base64 CA root ! or intermediate certificate. Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itselfBEGIN CERTIFICATE MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B AQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21z Y28xFTAT BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx NDA2MDE0 M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV MBMGCgmS JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK BgNVBAMT A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu VvyiLmA9 BSGZMZ3sCtR9TCMWOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd 4TNgNtjX</pre>
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij

KX+SWAENCJSIIXEUANDIBTUANOCKUEBOBJXGDJUNPAKIGGIWBIATV4M/
x21=uDQ1 x3GoFGmb8zGw6yg1DFallOvBVwbDbMIyzwwVBYWKb4ycO4wwOmr//Sct1t
uWgcvkzv uBwCentW7C1abTafm5XK/d//z2eUuXrHVvS0CfoFvk1vF6/01o+f0eSS
z+mlDhYy
WPXR018CawEAAaOCAW8wggFrMBMGCSsGAOOBgicUAgOGHgOAOwBBMAsG
A1IIdDwOF
AWIBh jAPBGNVHRMBAf8EBTADAOH/MB0GA1UdDgOWBBTZrb818jg18RRD
L3mYfNOJ
pAP1WDCCAOMGA1UdHwSB+zCB+DCB9aCB8gCB74aBtWxkYXA6Lv8v0049
O0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWM1MjBLZXk1MjBTZXJ2
aWNlcyxD
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dl¥i5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYn1TrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HM1j
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKO1E+OC5L+ytJvw
19GZhlzE
10VUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
1XXC68DKoZY09pPq877uTaou8CLtu11POmeOyzgJ0N+xaZX2EwGPn149
JMS/ADAU+DKIOI/EIJQGMSQGF145/CIH/GXIVD+D85aC
END CERTIFICATE
quit
Manually pasted certificate into CLT. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do vou accept this
certificate? [ves/no]: <b>yes</b>
Trustpoint CA certificate accepted.
<b>*</b>
<pre>% Certificate successfully imported</pre>
CiscoASA(config)#

#### Stap 6. Installeer het certificaat

#### ASDM-procedure

Gebruik het door de verkoper van de derde partij verstrekte identiteitsbewijs om deze stappen te ondernemen:

- 1. Klik op Configuration en vervolgens op Properties.
- 2. Vul het certificaat uit en kies vervolgens het invoercertificaat.
- 3. Klik op het radioknop **Voer de certificaattekst in in in het hexadecimaal of de** basisbestandsindeling, en plak het basis64-identiteitsbewijs in het tekstveld.



4. Klik op Importeren en vervolgens op OK.

#### Opdrachtlijnvoorbeeld

Cisco ASA
CiscolSl(config)#crupto ca import Cll certificate
! Initiates prompt to paste the base64 identity
certificate ! provided by the 3rd party vendor. % The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself ! Paste the base 64 certificate provided by
the 3rd party vendorBEGIN CERTIFICATE
MIIFpzCCBI+gAwIBAgIKYR71mwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoXDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWx1aWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0
ZW1zMSQw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZIhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zC0
sS8iqxqO
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ21z
Y212Y28UY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
GDAWGBTZrb&1&jqI&RRDL3mYiNQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
/4abtwxkixAbly8vQ049Q0ExLENOPVRTLVCySzMtQUNTLENOPUNEUCxD
TJIQAWJS

aWM1MjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJ1dm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3d1Yi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1d1Yi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/02xDB
7wXQaGph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/034wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc
1L5nuPsd8MaexBc=
END CERTIFICATE
quit
INFO: Certificate successfully imported
CiscoASA(config)#

# Stap 7. 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:

 Kies Configuratie > VPN > IKE > Beleid > Add om een ISAKMP beleid 65535 zoals in deze afbeelding te maken.

🎼 Add IKE Policy				
Priority:	85535	Authentication:		
r nonky.		Aumentication.	rsa-sig ·	
Encryption:	3des 💌	D-H Group:	2 💌	
Hash:	md5	Lifetime:	C Unlimited	seconds
	ок	Cancel	Help	

- 2. Klik op **OK** en vervolgens op **Toepassen**.
- 3. Kies **Configuratie > VPN > IPSec > TransforMS >** Toevoegen om een transformatieset (*myset*) te maken zoals in deze

Add Ir	ansform Set				
	Set Name: Properties	myset			
	Mode: ESP Encryptior	⊙ Tur n:	inel 3DES	C Transp	ort
	ESP Authentica	ation:	MD5		<b>-</b>
	ок	7	Cancel		Help
afbeelding:					

- 4. Klik op OK en Toepassen
- 5. Kies **Configuratie > VPN > IPSec > IPSec-regels >** om een crypto kaart te maken met dynamisch beleid van prioriteit 10 zoals in deze afbeelding getoond wordt:

Crea	te IPSec R	tule							
Tunn	el Policy (Cr	rypto Map) - Ba	sic   Tuni	nel Policy (Crypto Ma	ap) - Adv	anced Traff	ic Selectio	n	
	Interface:	outside	•	Policy Typ	e: dy	namic 💌		Priority:	10
	Transform	Sets							
	Transform	) Set to Be Add	ed:		myset				
		SHA		Add >>				Move	Up
				Remove				Move D	)ovvn

- 6. Klik op OK en Toepassen
- 7. Kies Configuratie > VPN > Algemeen > Groepsbeleid > Intern groepsbeleid toevoegen om een groep beleids Standaard te maken zoals in deze afbeeldingen wordt

	🚰 Add Internal Group Policy	
	Name: Defaultgroup	
	General IPSec Client Configuration	n Client Firewall Hai
	Check an Inherit checkbox to let th	e corresponding settir
	Tunneling Protocols:	Inherit 🗖 IPSe
	Filter:	Í Inherit
	Connection Settings	lnherit
getoond.		

📬 A	dd Internal Group Policy			
	Name: Defaultgroup			
	General PSec Client Configura	tion Client Firewall	Hardware Client	NAC VebV
	Check an Inherit checkbox to le	t the corresponding se	etting take its value	e from the def
	General Client Parameters Ci	sco Client Parameters	Microsoft Client I	Parameters
	Banner:		🔽 Inherit	
	Default Domain:		🗆 Inherit 🤇	cisco.com

- 8. Klik op OK en Toepassen
- 9. Kies Configuration > VPN > IP-adresbeheer > IP-pools > Add om de adrespool te configureren zodat de VPN-clientgebruikers dynamisch kunnen worden

configureren	Add IP Pool		
	Name:	vpnpool	
	Starting IP Addr	ess: 10.5.5.10	
	Ending IP Addre	ss: 10.5.5.20	
	Subnet Mask:	255.255.25	5.0 💌
toegewezen.	ок	Cancel	Help

- 10. Klik op OK en Toepassen
- 11. Kies Configuratie > VPN > Algemeen > Gebruikers > Toevoegen om een gebruikersaccount voor VPN-clienttoegang te

<b>1</b>	Add User Account	
	(dentity) VPN Policy VebVPN	
	Username:	vpnuser
	Password:	****
	Confirm Password:	****
	🔲 User authenticat	ed using MSCHAP
	Privilege level is used wit	h command authorization.
	Privile no Leonal	h =
(en.L	Privilege Level:	r 🔽

12. Voeg deze gebruiker toe aan

Def	aultRAGGroup.			
	Add User Account			
	Identity VPN Policy WebVPN			
	Check an Inherit checkbox to let the cor	responding settir	ng take its valı	ue from the group
	Group Policy:	Minherit		<u>-</u>
	Tunneling Protocols:	🔽 Inherit	🗖 IPSec	VVebVPN
	Filter:	🔽 Inherit		
	Tunnel Group Lock:	🗌 Inherit	DefaultRA	Group
	Store Password on Client System:	🔽 Inherit	C Yes	C No

- 13. Klik op OK en Toepassen
- 14. Bewerk de DefaultRAGgroup zoals in deze procedure wordt beschreven:Kies Configuratie
   > VPN > Algemeen > Tunnelgroep > Bewerken.Kies de standaardgroep in de vervolgkeuzelijst

🧱 Edi	it Tunnel Gro	up				
	Name:	DefaultRA	AGroup		Type:	jipsec-ra
	General IPS	ec   PPP   eneral acci	ess attribute:	s from the r	following sub	-tabs.
	Basic Auth	nentication	Authorizati	on Accou	unting Client	Address .
Groepsbeleid.	Group Po	olicy:	Defaultgro	qr	<u> </u>	Kies
LOCAL in de vervolg	keuzelijst					
Verificatieservergroe	p.					
Edit Tunnel Grou	P					
Name:	DefaultRAGrou	q		Type: ip	sec-ra	
General						
	11					
Configure ger	ieral access a	ttributes fro	om the follow	ing sub-tal	os.	
Basic Auther	ntication Aut	norization	Accounting	Client Ad	ldress Assig	
To set auth	entication serv	er group p	er interface,	go to the A	dvanced ta	
Authentica	tion Server Gr	oup:	LOCAL		T	(ies <b>VPN</b> in de

vervolgkeuzelijst Clientadrestoewijzing.

薩 Edit Tunnel Group	
Name: DefaultRAGroup	Type: ipsec-ra
Genera PPP	
Configure general access attributes from	the following sub-tabs.
Basic Authentication Authorization A	ccounting Client Address Assignmer
To specify whether to use DHCP or > IP Address Management > Assign	r address pools for address assignme nment.
DHCP Servers	
ID (Indexees)	
ir Address.	Add >>
	Delete
Address Pools	
To configure interface-specific	address pools, go to the Advanced ta
Available Pools	Assigned
	vpnpool
	Add >>

15. Klik op **OK** en **pas** vervolgens **toe**.

# Opdrachtlijnvoorbeeld

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)# <b>exit</b>
CiscoASA(config)#crypto isakmp identity auto
<pre>! Phase 1 Configurations CiscoASA(config)#crypto</pre>
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map outside_dyn_map 10

```
set transform-set myset
CiscoASA(config)#crypto map outside_map 65535 ipsec-
isakmp dynamic outside_dyn_map
CiscoASA(config)#crypto map outside_map 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 password123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#group-lock value
DefaultRAGroup
CiscoASA(config-username)#exit
!--- Create an user account "vpnuser" and added to
"DefaultRAGroup" 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
```

## ASA-configuratiesoverzicht

authentication

Cisco ASA

#### CiscoASA#**show running-config** : Saved : ASA Version 7.2(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
boot system disk0:/asa722-k8.bin
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 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
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
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 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
group-policy Defaultgroup internal
group-policy Defaultgroup attributes
default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
group-lock value DefaultRAGroup
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 DMZ
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 outside\_dyn\_map 10 set transform-set myset crypto map outside\_map 65535 ipsec-isakmp dynamic outside dyn map crypto map outside\_map 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=Raleigh keypair my.CA.key crl configure crypto ca certificate chain CA1 certificate 3f14b70b0000000001f 308205eb 308204d3 a0030201 02020a3f 14b70b00 00000000 1f300d06 092a8648 86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31 15301306 0a099226 8993f22c 64011916 05636973 636f3115 3013060a 09922689 93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 le170d30 37313232 37313430 3033365a 170d3038 31323236 31343030 33365a30 67311330 11060a09 92268993 f22c6401 19160363 6f6d3115 3013060a 09922689 93f22c64 01191605 63697363 6f311530 13060a09 92268993 f22c6401 19160554 53576562 310e300c 06035504 03130555 73657273 31123010 06035504 03130976 706e7365 72766572 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 0001a382 03313082 032d300b 0603551d Of040403 02052030 34060355 1d11042d 302ba029 060a2b06 01040182 37140203 a01b0c19 76706e73 65727665 72405453 5765622e 63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb 490cdela fe2d63e3 le1fb28c 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 74301506 092b0601 04018237 14020408 1e060045 00460053 300c0603 551d1301 01ff0402 30003015 0603551d 25040e30 0c060a2b 06010401 82370a03 04304406 092a8648 86f70d01 090f0437 3035300e 06082a86 4886f70d 03020202 0080300e 06082a86 4886f70d 03040202 00803007 06052b0e 03020730 0a06082a 864886f7 0d030730 0d06092a 864886f7 0d010105 05000382 010100bf 99b9daf2 e24f1bd6 ce8271eb 908fadb3 772df610 0e78b198 f945f379 5d23a120 7c38ae5d 8f91b3ff 3da5d139 46d8fb6e 20d9a704 b6aa4113 24605ea9 4882d441 09f128ab 4c51a427 fa101189 b6533eef adc28e73 fcfed3f1 f4e64981 0976b8a1 2355c358 a22af8bb e5194b42 69a7c2f6 c5a116f6 d9d77fb3 a7f3d201 e3cff8f7 48f8d54e 243d2530 31a733af 0e1351d3 9c64a0f7 4975fc66 a017627c cfd0ea22 2992f463 9412b388 84bf8b33 bd9f589a e7087262 a4472e69 775ab608 e5714857 4f887163 705220e3 aca870be b107ab8d 73faf76d b3550553 la2b873f 156f9dff 5386c839 1380fda8 945a7f6c c2e9d5c8 83e2e761 394dd4da 63eaefc6 a44df5 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 526fbelc 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 cOcaa196 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
tunnel-group DefaultRAGroup general-attributes
address-pool vpnpool
default-group-policy Defaultgroup
tunnel-group DefaultRAGroup ipsec-attributes
trust-point CA1
telnet timeout 5
ssh timeout 5
console timeout 0
!
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
prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0
: end
CiscoASA#
```

## **VPN-clientconfiguratie**

Voltooi deze stappen om de VPN-client te configureren:

 Selecteer Start > Programma's > Cisco Systems VPN-client > VPN-client om de VPNclientsoftware 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:Meld u aan bij de CA-server 172.16.5.1 met de gebruikerswoordenboeken die aan de gebruiker zijn

	aD	ouce	liank		rosorc	Ince	rneci	Explor	er prov	laea by	/ LISCO Sy	stems	5, II
	ile	Edit	Vie	w F	avorite	es '	Tools	Help					
	Ba	rck 🔻	>	- (2	) 🔹	<b>a</b>	Q	iearch	🛞 Fav	vorites	( Media	• 3	E
c	ddre	ss [	🔰 http	o://17:	2.16.5.	1/cer	tsrv						
			Ent	er Ne	twork	Pas	sword						
				<u> </u>	> Plea	ase ty	pe you	ır user r	name and	d passw	ord.		
				1×	Site			172.16	51				
					JIC	•	G	112.10					- 1
					Use	er Nai	me	vpnuse	;r				
					Pa	sswor	аЧ	*****					
					Do	main							
						Save	this n	300141010	t in your	Dassino	rd liet		
						Jave	uns pe	33399010	rinyour				
everd.L										(	эк		<u>Car</u> Op

**rking:** Zorg ervoor dat u een gebruikersaccount hebt voor de VPN-clientgebruiker bij de CAserver.Klik op **Download een CA certificaat, certificeringsketen of CRL** en selecteer vervolgens de **Base 64** radioknop om de coderingsmethode te specificeren.Klik op het **CAcertificaat** 

downloaden.

Download a CA Certificate, Certificate Chain, or CRL
For trust continuates issued from this continuation outbority, install this $CA$ cont
To trust certificates issued from this certification authority, <u>install this CA cert</u>
To download a CA certificate, certificate chain, or CRL, select the certificate
CA certificate:
Current [CA1]
ncoding method:
O DER
Base 64
<u>Download CA certificate</u>
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Sla het CA-certificaat op uw computer op met de naam certnew.cer. Standaard slaat het

File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: certnew.cer
File type: Security Certificate
From: 172.16.5.1
This type of file could harm your computer if it contains malicious code.
Would you like to open the file or save it to your computer?
Client. Open Save Cancel More Info

client op het tabblad **Certificaten** en kies vervolgens **Importeren**.Klik op de knop **Importeren uit bestand** en klik vervolgens op **Bladeren** om het CA-certificaat te importeren vanuit de opgeslagen locatie c:\Program Files\Cisco Systems\VPN Client.Klik op **Importeren**.Het dialoogvenster verschijnt dat aangeeft dat het certificaat is geïmporteerd.

👶 sta	atus: Disconn	ected	VPN Clier	nt - Ye	rsion 4.8	.02.00	10		
Conne	ection Entries	Status	Certificate	s Log	Options	Help			
<b>(</b>	iew Im	port	Export	<b>E</b>	<b>- →</b> Inroll	<b>V</b> eri	fy	XX Delete	
Conn	ection Entries	Certif	ficates L	og 📔					
Numb	ber	Certif	ficate				Store	$\Delta$	Key Size
0	👌 ¥PN Clier	nt   In	nport Cerl	ificate					
	<ul> <li>Import fr</li> </ul>	om <u>F</u> ile							
	Impo	ort <u>P</u> ath	ram Files\C	isco Sy	stems\VP	N Clien	t\certne	w.cer	<u>B</u> rowse
	Import P <u>a</u>	ssword:							
	C Import fr	om <u>M</u> icro	VPN C	lient Certifi	icate succ	essfully	' importe	× ed.	
Not co	Import C <u>e</u>	rtificate:			ОК			F	<b>v</b>
	Entering a identity ca	a new pa ertificate:	a S.			_		ssv	vord protect
	<u>N</u> ew P	assword	:						
	<u>C</u> onfirm P	assword	:						
						Γ	lmp	oort	Cancel

# CA1-certificaten worden weergegeven in het tabblad

Certificaten.					
Connection Entries	Status Certificate	s Log Options	Help		
View Imp	ort Export	Finol	Verify D	X Velete	cisco
Connection Entries	Certificates L	.og			
Number	Certificate		Store /	Key Size	Validity
)	CA1		CA	2048	until Dec 14, 2012 11

**Opmerking:** Controleer of de optie **CA/RA-certificaten** tonen is ingeschakeld. anders worden de CA-certificaten niet in het certificaatvenster

👶 status: Disconnecte	d   VP	N Client	- Yei	sion 4.8	.02.0010	
Connection Entries Statu	is C <u>e</u> r	tificates	Log	Options	<u>H</u> elp	
		<u>⊻</u> iew				
View Import		Import.				
Connection Entries Ce	ertif	Export.				
Number Ce	ertif	E <u>n</u> roll				
0 CA	1	Verify				
		D <u>e</u> lete				
		⊆hange	Certi	ficate Pas	sword,	
		<u>R</u> etrieve	е Арр	roved Cer	tificate,,,	
		<u>S</u> how Cr	A/RA	Certificat	es	

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 O Use existing key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0 💌
Key Usage: 🔎 Exchange
Key Size: 1024 Min: 384 Max:16384
Automatic key container name O 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: MD5 💌 Only used to sign request.
Save request to a file
Klik op <b>Ja</b> om verder te
gaan. Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you want to request a certificate now?
Yes No
Klik op <b>Installeer dit</b> Microsoft Certificate Services CA1
Certificate Issued
The certificate you requested was issued to you.
certificaat. Install this certificate Klik op Ja om verde

te



detoond: Your new certificate has been successfully installed.

Sluit de client

weer uit en start de VPN-client opnieuw om het geïnstalleerde identiteitsbewijs te laten verschijnen in het tabblad Certificaten van de VPN-client zoals in deze

afbeelding:

Connection Entries S	itatus Certificates	Log Options	Help				
View Impo	ort Export	Enroll	Veril	) y	X Delete		uluilu cisco
Connection Entries	Certificates Log	3					
Number	Certificate			Store	Δ	Key Size	Validity
	CA1			CA		2048	until Dec 14. 2012 11:40:
Users + vpnuser				Microso	ft	1024	until Dec 26, 2008 18:27:

4. Voltooi deze stappen om een verbindingsingang (gebruiker) te maken:Klik op het tabblad Connection Vermeldingen en vervolgens op Nieuw.Voer het externe IP-adres (routeerbaar) in het veld Host in.Selecteer de radioknop certificaatverificatie en kies het identiteitsbewijs in de vervolgkeuzelijst.Klik op

	🗦 VPN Client	Create New	VPN Connecti	on Entry	<u>×</u>	2
	Connection Entru	vonuser )	1			
	Connection Endys	vpriuser				
	Description:				cisco	
	(Host:	192.168.1.5				
	Authentication	Transport	Backup Serve	ers Dial-Up		
	C Group Auther	ntication		C Mutual Gro	up Authentication	
	Name:					
	Password:	Í				
	Confirm Passy	vord:				
				_		
	<ul> <li>Certificate Au</li> </ul>	Ithentication				
	Name: 0-Us	ers + vpnuser	(Microsoft)	<u> </u>		
	🔲 Send CA (	Certificate Cha	in			
Opslaan	Erase User Passy	vord		Save	Cancel	
Klik op						-
Connect. 💪 status: [	Disconnected   VPN	Client - Version	4.8.02.0010		_	
Connection I	Entries Status Certifi	cates Log Opti	ions Help			
8	- 📩 🎁		a 💥		alo alo	$\mathbf{d}_{11}$
Cancel Conr	nect New Ir	nport Modi	fy Delete		CIS	co
Lonnection	Connection Entru		Host		Transport	
	vpnuser	-	192.	68.1.5	IPSec/UDP	
•						Þ
Contacting t	the security gateway at	192.168.1.5				

5.

6. Voer na de indiening de naam van de gebruiker en de wachtwoordinformatie in voor de breedte en klik op **OK** om verbinding te maken met het externe

	Enter Username and Password.  CISCO SYSTEMS Username: Vpnuser Password: *******	
netwerk.	OK Cancel	
7. De VPN-	client sluit aan op de ASA zoals in deze afbeelding wordt	
	👶 status: Connected   VPN Clieny - Version 4.8.01.0300	
getoond:	Connection Entries Status Certificates Log Options Help	

# **Verifiëren**

dc=TSWeb dc=cisco dc=com

CRL Distribution Points:

In de ASA kunt u verschillende show opdrachten in de opdrachtregel gebruiken om de status van een certificaat te controleren.

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

• Laat crypto ca trustpoint-displays de geconfigureerde kruispunten zien. CiscoASA#show crypto ca trustpoints

```
Trustpoint CA1:
     Subject Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
           Serial Number: 7099f1994764e09c4651da80a16b749c
     Certificate configured.
• toont het crypto-certificaat—Hier worden alle certificaten weergegeven die op het systeem zijn
 geïnstalleerd.
 CiscoASA#show crypto ca certificates
 Certificate
   Status: Available
   Certificate Serial Number: 3f14b70b0000000001f
   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
```

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

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

PrincipalName: vpnserver@TSWeb.cisco.com

```
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=Configuratio
 n,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: 06:01:43 UTC Dec 14 2007
     end date: 06:10:15 UTC Dec 14 2012
   Associated Trustpoints: CA1

    Laat crypto kras zien-displays met gecached certificaat revocatielijsten (CRL).

    toon crypto toets mypubkey rsa-displays alle gegenereerde cryptosleutelparen.

 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#

    Laat crypto isakmp sa-displays de IKE 1 tunnelinformatie zien.

 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
```

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

    toon crypto ipsec sa-Geeft de tunnelinformatie van IPSec weer.

 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 <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

# Problemen oplossen

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

Hier zijn een paar mogelijke fouten die u zou kunnen tegenkomen:

- FOUT: Kan geïmporteerd certificaat niet verwijderen of controlerenDeze 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 sleutelpaar dat aan het Trustpoint is gekoppeld, komt niet overeen met de openbare sleutel in het identiteitsbewijs. Gebruik de opdracht **show crypto ca certificaten trustpointname** om te controleren of u uw identiteitsbewijs op het juiste betrouwbaar punt hebt geïnstalleerd. Kijk naar de regel die **Associated Trustpoints** noemt. 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 sleutelpaar niet is gewijzigd sinds de CSR is gegenereerd.

• FOUT : ASA/PIX. Sev=Waarschuwing/3 IKE/0xE300081 Ongeldig id voor extern certificaat:U kunt deze fout in de VPN-client ontvangen als er een probleem is met de certificaten tijdens de verificatie. Om dit probleem op te lossen, gebruikt u de automatische opdracht van de crypto-isakmp-identiteit in de ASA/PIX-configuratie.

# Gerelateerde informatie

- <u>Cisco-pagina voor adaptieve security applicatie</u>
- <u>Cisco VPN-clientondersteuningspagina</u>
- <u>Cisco PIX 500 Series security applicaties</u>
- Opdrachtreferenties van Cisco Secure PIX-firewall
- <u>Security meldingen uit het veld (inclusief PIX)</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>