ASA 7.x Installeer Verkrakers van 3 partijen handmatig voor gebruik met WebVPNconfiguratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten **Conventies** Configureren 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. De certificaatinschrijving genereren Stap 5. Verifieer het Trustpoint Stap 6. Installeer het certificaat Stap 7. Configuratie van WebVPN om het nieuw geïnstalleerd certificaat te gebruiken Verifiëren Vervang een zelfondertekend certificaat van ASA Geïnstalleerde certificaten bekijken Geïnstalleerde certificaten voor WebVPN verifiëren via een webbrowser Stappen om het SSL-certificaat te verlengen Opdrachten Problemen oplossen Gerelateerde informatie

Inleiding

In dit configuratievoorbeeld wordt beschreven hoe u een digitaal certificaat van een derde verkoper op de ASA handmatig kunt installeren voor gebruik met WebVPN. In dit voorbeeld wordt een gratis proefcertificaat gebruikt. Elke stap bevat de ASDM-toepassingsprocedure en een CLI-voorbeeld.

Voorwaarden

Vereisten

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

Gebruikte componenten

Dit document maakt gebruik van een ASA 5510 met softwareversie 7.2(1) en ASDM versie 5.2(1). De procedures in dit document werken echter op elk ASA-apparaat dat 7.x met een compatibele ASDM-versie draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

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

Configureren

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

- 1. Controleer of de waarden voor datum, tijd en tijdzone juist zijn.
- 2. Generate the RSA Key Pair.
- 3. Maak het trustpunt.
- 4. Generate de certificaatinschrijving.
- 5. Verifieer het Trustpoint.
- 6. Installeer het certificaat.
- 7. Configuratie van WebVPN om het Nieuw Geïnstalleerde 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. Sluit Apparaatbeheer uit en kies Kloktijd.
- 3. Controleer of de verstrekte informatie juist is.De waarden voor Datum, Tijd en Tijdzone moeten nauwkeurig zijn zodat een goede certificatie kan plaatsvinden.



Opdrachtlijnvoorbeeld

ciscoa
ciscoasa# show clock
11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

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 **Add**

(Toevoegen).

es.	E- Certificate		
65	Authentication		
NAT	Enrolment	Kev Pair Name Usage Modulus Size	bbb
-		They i all theme are a surger modeling and a	700
<u>23</u>	- Key Pair		1
VDN	- An Manage Certificates		Show Details
	E- 🙀 Trustpoint		
A	- S Configuration		Delete
	- Seport	😰 Add Key Pair 🔀	
CSD Manager	- Import		
12.	E-1 Device Access	Norman Calification & Income	Refresh
335	E-38 Device Administration	Name: Use detaut key name	
Routing	B-P DHC Services	G Investment and	
0.	E-ADNS 18	· my renage wey	
68	High Availability and Scal		
Global Objects	- 🧼 Failover	Size: 1024	
	- Stragment		
3		Usage: 🕑 General Purpose 🖤 Special	
Properties	HTTP.MTTPS		
rioperdes	E-10 IP Audit		
	E Logging		
	Priority Queue	Generate Now Cancel Help	
	SSL .		
	- SUNRPC Server		
	TCP Options		
	Timeouts		
1			

- 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**.Het sleutelpaar dat u hebt gemaakt, moet in de kolom Naam sleutelpaar worden vermeld.

Opdrachtlijnvoorbeeld

ciscoa
ciscoasa# conf t
ciscoasa(config)#crypto key generate rsa label my.verisign.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.verisign.key Keypair generation process begin. Please wait ciscoasa(config)#

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**.

l	Configuration > Properties > C	ertificate > Trustpoint > Configuration	
	Startup Wizard	Configuration	
	AAA Setup	Configure a Certificate Authority (CA) as a trustpoint.	
	E-B ARP		
I	Auto Update		
I			[
I	🔁 🐻 Certificate	Trustpoint Name Device Certificate Subject CA Certificate Subject	Add
I	- Authentication		
I			Edit
I	- El Import Certificate		5000
I			f
I			Delete
I	E-22 Trustpoint		
l	- Social Configuration		Request CRL
I			
I			
I	E Device Access		

- Configuratie van deze waarden: Naam van het schaalpunt: De naam van het trustpunt moet relevant zijn voor het beoogde gebruik. (Dit voorbeeld gebruikt *my.verising.trustpoint.*) Belangrijk paar: Selecteer het sleutelpaar dat in <u>Stap 2</u> gegenereerd is. (*my.verising.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:U kunt deze waarden configureren door een waarde te selecteren in de vervolgkeuzelijst Attribute (Kenmerk), de waarde in te voeren en te klikken op Add>>

		Common Name (CN)	webypn.cisco.com
Attribute to be Added		Department (OU)	TSWEB
	1	Company Name (O)	Cisco Systems
tribute: Select Attribute	Add >>	State (St)	North Carolina
	_	State (St)	US
alue:	Delete	Location (L)	Raleigh

- 8. Klik op **OK** wanneer u de juiste waarden heeft 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 naam

(CN).

🚰 Certificate Parameters	×
Enter the values for the parameters that are to be included in the certificate.	
Subject DN: ystems,St=North Carolina,St=US,L=Raleigh	
FQDN	
C Use FQDN of the device	
Specify FQDN webvpn.cisco.com	
C Use none	
E-mail:	
IP Address:	
Include device serial number	
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 Co	Generalize		
	nnguration		
Trustnoint Name:	my verision truspoi	int	
maspoint Name.	l'information and a second		
🔲 Generate a sel	f-signed certificate on a	enrollment	
If this option is	enabled, only Key Pair	and Certificate Parameters can be specified.	
Enrollment Settings	Revocation Check	CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced	#
Key Pair:	my.verisign.key 💌	Show Details New Key Pair	
Challenge		Confirm Challenge	
Password:		Password:	
C Lice at	tomatic aprollment		
· 030 at	atomatic enroiment		
Enrollme	nt URL: http://		
Enrollme Retry Pe	nt URL: http://	minutes	
Enrollme Retry Pe Retry Co	nt URL: http:// riod: 1 unt: 0	minutes (Use 0 to indicate unlimited retries)	
Enrollme Retry Pe Retry Co	nt URL: http://	Minutes (Use 0 to indicate unlimited retries) Certificate Parameters	
Retry Pe Retry Co	nt URL: http://	(Use 0 to indicate unlimited retries) Certificate Parameters	

Opdrachtlijnvoorbeeld

ciscoa					
ciscoasa(config)#crypto ca trustpoint my.verisign.trustpoint					
! Creates the trustpoint.					
ciscoasa(config-ca-trustpoint)# enrollment terminal					
<pre>! Specifies cut and paste enrollment with this trustpoint. ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,</pre>					
! Defines x.500 distinguished name. ciscoasa(config-ca- trustpoint)#keypair my.verisign.key					
! Specifies key pair generated in <u>Step 3</u> . ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com					
! Specifies subject alternative name (DNS:).					

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).



4. Kopieer het verzoek om inschrijving van PKCS#10 naar een tekstbestand en dien de CSR vervolgens naar de juiste verkoper van de derde partij toe.Nadat de verkoper van de derde partij de CSR heeft ontvangen, moet hij een identiteitsbewijs voor installatie afgeven.
Opdrachtlijnvoorbeeld

Apparaatnaam 1

```
ciscoasa(config)#crypto ca enroll my.verisign.trustpoint

! 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=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems, C=US, St=North Carolina, L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.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]: yes
! 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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczE0
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3vEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request --- Redisplay enrollment
request? [yes/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 weergegeven te worden als een certificaat.
- 4. Dubbelklik op het certificaatbestand.Het dialoogvenster Certificaat



rking: Als het *bericht "Windows niet voldoende informatie heeft om dit certificaat te controleren*" in het tabblad Algemeen verschijnt, moet u het certificaat van oorsprong CA of tussenpersoon voor CA van de derde verkoper 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 Certificaat

Certificate	? ×
General Details Certification Path	
Certification path VeriSign Trial Secure Server Test Root CA VeriSign Trial Secure Server Test CA Webvpn.cisco.com	
View Certificate	•
Certificate status:	
This certificate is OK.	
	ок Gedetai

bekijken.

lleerde informatie over het intermediaire CA-certificaat is te vinden. **Waarschuwing:** Installeer het certificaat van identiteit (apparaat) niet in deze stap. In deze stap worden alleen de wortel, de ondergeschikte wortel of het CA-certificaat toegevoegd. De identiteit (apparaat) certificaten zijn geïnstalleerd in <u>Stap 6</u>.

Certificate		<u>?</u> ×
General Details Certification Pa	h]	
		1
Show: <al></al>	▼	
Co.L.	University	
	Value V3	-
	•3 63 b1 a5 cd c5 9f 78 80 1d a0	
Signature algorithm	sha1RSA	
E Issuer	VeriSign Trial Secure Server Te	_
Valid from	Tuesday, February 08, 2005 8	
Valid to	Sunday, February 08, 2015 7:	
	VeriSign Trial Secure Server Te	
	RSA (2048 Bits)	-
		- 1
J		
	Edit Properties Copy to File	.
	01	<

- 7. Klik op Details.
- 8. Klik op Kopie naar bestand.
- 9. Klik in de Wizard Certificaat exporteren op Volgende.

 Klik in het dialoogvenster Exporteren File Format op de radioknop Base-64, gecodeerd X.509 (.CER) en klik op Volgende.

tificate Export Wizard	
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
Include all certificates in the certification path if possible	
C Personal Information Exchange - PKCS #12 (,PFX)	
\square Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
Delete the private key if the export is successful	
< Back Next > C	ancel

- 11. Voer de bestandsnaam en -locatie in waarop u het CA-certificaat wilt opslaan.
- 12. Klik op **Volgende** en vervolgens op **Voltooien**.

ertificate Export Wizard	
File to Export Specify the name of the file you want to export	
File name:	
c:\introotca	Browse
< Back	k Next > Cancel

- 13. Klik op **OK** in het dialoogvenster Met succes exporteren.
- 14. Bladeren naar de locatie waar u het CA-certificaat hebt opgeslagen.
- 15. Open het bestand met een teksteditor, zoals Kladblok. (Klik met de rechtermuisknop op het bestand en kies Verzenden naar > Kladblok.)Het Base64-gecodeerde bericht verschijnt evenveel als het certificaat in deze afbeelding:

File Edit Format View Help

----BEGIN CERTIFICATE--MIIFSjçCBDKqAwIBAqIQCECQ47aTdj6BtrI60/Vt6zANBqkqhkiG9w0BAQUFADCB yzelMA&GA1UEBhMCVVMxFzAVBqNVBAoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL ÉydGb3IqVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3R]c3RjYSAoYykwNTEtMCsGA1UEAXMkVmVyaVNpZ24gVHJpYWwqU2VjdXJ1FN] cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTkloVowgZ4x CZAJBGNVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q21zY28qU31zdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BqNVBAsUMVR1cm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PwYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRw0i8vb2NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9Tv]JTZWN1cmUtyW]hLnZ]cm]zaWduLmNvbS9Tv[JUcm]hbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAwIaBBRLa7ko]gYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTqIorIClawwwx+RHCcTqIrlzf0vfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvlXzŽjiOJ51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLKyja |idT1FmBvf02qaZS6S40= ----END CERTIFICATE----

- 16. Klik binnen ASDM op **Configuration** en vervolgens op **Properties.**
- 17. Vul Certificaat uit en kies Verificatie.
- 18. Klik op de radioknop Voer de certificaattekst in in in hexadecimaal of in basis64-formaat.
- 19. Plakt het basis64-geformatteerde CA-certificaat van uw teksteditor in het tekstgebied.
- 20. Klik op

Verifiëren.

Configuration > Properties > C	ertificate > Authentication					
Startup Wizard	Authentication					
🗄 🚅 AAA Setup	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with					
Anti-Spooting	trustpoint and installed on the device.					
C-EG ANP						
Auto Update	Trustpoint Name: wy.verisign.truspo Verilian Karal Kara					
Client Opdate						
Authentication	Fingerprint (optional):					
- Stanler Internet	a Marken delanation					
	The conditional fact and have been precisived if the content of the object in conditioned for every strengthered					
-88 Key Pair	The certificate text can be specified if the selected trustpoint is configured for manual enrolment.					
	Certificate Text					
🖃 🤯 Trustpoint						
- 👸 Configuration	C Import from a file: Browse					
- State Export						
	Enter the certificate text in hexadecimal or base64 format:					
E Device Access	A1UEAxMpVmVvaVNpZ24qVHJpVWvvqU2VidXJIFNIcnZIc/BUZXN0FJvb3					
Device Administration	ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/					
H-15" DHCP Services	Kqt234YROIL51ZS111oUZ2MANp2H4biw4ittsG5snDDlw/SRmiH3BA//SU6E					
High Auglishilly and Seal	Al9TXvRlcD5q0mB+nyK9fB2aBzOiaiHSiWzAJeQjuqA+Q93jNew+peuj4Ahc					
Fallower	n/KK/+1 Yv61w3+7g6ukFMARVBNg=					
Eragment	END CERTIFICATE					
HTTP/HTTPS						
😥 📲 🙇 IP Audit	Authentication Successful					
🕀 🔠 Logging						
- Priority Queue						
SSL 🚽	The trustpoint my verisign truspoint has been authenticated.					
SUNRPC Server						
TCP Options						
Timeouts	OK					
CRL Filtering	i					
MOCP						

21. Klik op OK. Opdrachtlijnvoorbeeld

ciscoa			
ciscoasa(config)#crypto ca authenticate			
my.verisign.trustpoint			
! 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			
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B			
AQUFADCB			
$\verb"jDelMakGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw"$			
LgYDVQQL			
${\tt EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x}$			
MjAwBgNV			
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290			
IENBMB4X			
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT			
AlVTMRcw			
FQYDVQQKEw5WZXJpU21nbiwgSW5jLjEwMC4GA1UECxMnRm9yIFR1c3Qg			
UHVycG9z			
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv			
ZiB1c2Ug			
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp			
MDUxLTAr			
${\tt BgNVBAMTJFZlcmlTaWdulFRyaWFslFNlY3VyZSBTZXJ2ZXIgVGVzdCBD}$			

QTCCASIW			
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu			
wElv6IJ/			
${\tt DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6}$			
1BBD6Zqk			
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45			
1P4qoyqS			
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1			
D/OCCmZO			
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo			
xjKfV6sb			
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6			
QMECAWEA			
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA			
BgpghkgB			
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu			
CHMVdGVZdGNhLZAOBGNVHQ8BA18EBAMCAQYWEQYJY1Z1AYD4QGEBBAQD			
AIUdDgQWBBRmI06B4DF23Sp/qUDFNgIGCCeHwjCBSgIDVRUjBIGqMIGn			
MIGMMQSWCQIDVQQGEWJVUZEAMBUGAIUECHMOVMVYAVNDZZ4SIEIUIY4X MDAuBeMU			
BAGTIOZUCI BUZINOIFB1 COBUCIUZIEQUEHEUICBOEUBECINICTEUVIUZ			
A1UEAxMpVmVvaVNpZ24gVHJpYWwgU2VidXJlIFNlcnZlciBUZXN0IFJy			
b30g00GC			
ECCol67bggLewTagTia9h3MwDOYJKoZIhvcNAOEFBOADgYEASz5v8s3/			
SjzRvY21			
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU			
6EEzD9oi			
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu			
j4AhdvGN			
n/KK/+1Yv61w3+7g6ukFMARVBNg=			
END CERTIFICATE			
quit			
! Manually pasted certificate into CLI. INFO:			
Certificate has the following attributes: Fingerprint:			
8de989db 7fcc5e3b fdde2c42 0813ef43 Do you accept this			
certificate? [yes/no]: yes Trustpoint			
'my.verisign.trustpoint' is a subordinate CA and holds a			
non self-signed certificate. Trustpoint CA certificate			
accepted. % Certificate successfully imported			
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.

Configuration > Properties > Certificate > Import Certificate						
Startup Wizard	Import Certificate					
🕀 🚮 AAA Setup	lastell as blastily contificate that uses years) and from a Cartificate Authority (CA) is years are to a manual					
- B Anti-Spoofing	enrolment request					
🟵 🐻 ARP	en onnen request.					
	Trusteeint Name					
E Certificate	Trustpoint ridme: my.verisign.truspo Edit New					
- Authentication						
-2 Enrolment	Certificate Text					
Import Certificate	C Insert from a file					
Key Pair	s importante.					
Manage Certificates						
E-82 Trustpoint	 Enter the certificate text in nexadecimal or base54 format; 					
Configuration						
- Seport	USDSUUSEPESHIYE GUAAPPIKOONKWO.000069H9322X.0pc2h05p20Votrus					
mport	nutkisisti Dio Forca a Yesi si su nu a n					
E Device Access	TFKFFSFbleCK/hh6MaMb40z6kFlzoVUmtdJDoU3B00U/vm+fa02eTWdz/WE					
P-R DHCP Services	0YVwM3kDQAO6EbAntUoAxovDbJucdxb6ZVTtyevMcgzCkXMHEVxa5/P>					
	ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4utcGgGZD8ltVGx26b5OWTz8K					
High Availability and Scal	8EvHm3grdbOZP+ISMotVVYE+CgfKpZb+CPAqH2Cdpz2aJiJih6CS6NM=					
Failover	END CERTIFICATE					
- K Fragment						
-12 History Metrics						
- TP/HTTPS	Tig Information					
🖲 📲 🔁 P Audit						
E- Logging						
- Priority Queue	Certificate import succeeded.					
SSL .						
SUNRPC Server						
TCP Options						
Timeours						
- Cikering						
C MUCP						
1						

4. Klik op Importeren en vervolgens op OK.

Opdrachtlijnvoorbeeld

ciscoa		
ciscoasa(config)#crypto ca import my.verisign.trustpoint certificate		
<pre>! Initiates prompt to paste the base64 identity certificate ! provided by the 3rd party vendor. % The fully-qualified domain name in the certificate will be: webvpn.cisco.com Enter the base 64 encoded certificate. End with the word "quit" on a line by itselfBEGIN CERTIFICATE</pre>		
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B		
AQUFADCB		
yzELMAKGA1UEBhMCVVMxFzAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMTAw		
LGYDVQQL EvdGb3IqVGVzdCB0dXJwb3N1cvBPbmx5LiAgTm8gYXNzdXJhbmN1cv4x		
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5j		
b20vY3Bz		
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj		
dxjlifnl		
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1		
OVowgbox		
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4G		
UmFsZW1naDEWMBQGA1UEChQNQ21zY28gU31zdGVtczEOMAwGA1UECxQF		
VFNARULX		

OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t			
L2Nwcy90			
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w			
gZ8wDQYJ			
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ			
/9ker2jQ			
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec			
rO+6aY1R			
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxS1Egry			
osBMMazg			
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF			
oDBDBgNV			
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJ1LWNybC52ZXJpc21n			
bi5jb20v			
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAE0zBBMD8GCmCGSAGG+EUBBxUw			
MTAvBggr			
BgEFBOcCARYjaHR0cHM6Lv93d3cudmVvaXNpZ24uY29tL2Nwcv90ZXN0			
Y2EwHOYD			
~ VR01BBYwFAYIKwYBBOUHAwEGCCsGAOUFBwMCMB8GA1UdIwOYMBaAFGYi			
ioHgMVnd			
Kn+rRsU2AgZwJ4daMHgGCCsGAOUFBwEBBGwwaiAkBggrBgEFBOcwAYYY			
aHR0cDov			
L29ic3AudmVvaXNpZ24uY29tMEIGCCsGAOUFBzAChiZodHRwOi8vU1ZS			
u2vidxj1			
LWFpYS52ZXJpc21nbi5ib20vU1ZSVHJpYWwyMDA1LWFpYS5iZXIwbgYI			
KwYBBOUH			
AOwEYiBqoV6qXDBaMFqwVhYJaW1hZ2UvZ21mMCEwHzAHBqUrDqMCGqOU			
S2u5KJYG			
DLvOUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVvaXNpZ24uY29t			
L3ZzbG9n			
bzEuZ21mMA0GCSgGSIb3D0EBB0UAA4IBA0Anvm4GVThPIvL/9v1DBd8N			
7/vW30v3			
blirHfHJvfPJ1znZOXvXdObpZkuA6Jvu03V2CYNnDomn4xRXOTUDD8g8			
6ZiKvMIj			
XM2VCmcHSaimMMRvjpvdxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/			
540021kB			
SmLzVV7crlYJEuhggu3Pz7gNRd8N0Un6c9sbw01BuM990xzIzdAo89FS			
ewy8MAIY			
rtab5F+oiTc5xGv8w7NARAfNgFXihgnLgWTtA35/oWuv86bje1IWbevg			
i8ePM9Td			
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0g0PBPx5FJSgMiUZGrviu50			
END CERTIFICATE			
guit			
-			
INFO: Certificate successfully imported			
ciscoasa(config)#			

Stap 7. Configuratie van WebVPN om het nieuw geïnstalleerd certificaat te gebruiken

ASDM-procedure

- 1. Klik op Configuration, klik op Properties en kies vervolgens SSL.
- 2. Selecteer in het gebied Trustpoints de interface die wordt gebruikt om WebVPN-sessies te beëindigen. (Dit voorbeeld gebruikt de externe interface.)
- 3. Klik op **Edit** (Bewerken).Het dialoogvenster SSL-trustpunt bewerken verschijnt.

Configuration > Properties > S	šL
Startup Wizard	SSL
🕀 🚽 🖌 AAA Setup	Configure SSI parameters. These parameters effect both ASDM and Moh DNI access
	Configure Sal parameters. These parameters affect out Asom and Web YPN access.
1 - 1 ARP	Server SSL Version: Any Client SSL Version: Any
	Encryption
	List (poor
🔁 🚰 Certificate	Available Algorithms Add >> Active Algorithms Move Up
E Device Access	30ES-SHA1
Device Administration	Read SSI Trustment
E-12 DHCP Services	
🕀 🚚 DNS	Specify an enrolled trusthoint to be used for SSL authentication on the outside interface. To enroll a trusthoint
High Availability and Scal	go to Configuration > Properties > Certificate > Enrolment.
- Failover	
- Fragment	
-22 History Metrics	
- M HTTP/HTTPS	Interface: outside
E-IQ IP Audit	
E Logging	Enroled Trustpoint: my.verisign.trustp
Priority Queue	
-Se SSL	
SUNRPC Server	
TCP Options	OK Cancel Help
imeouts	
CRL Fitering	Trustopints
MOOP	Search unkick enrolled tructure if any should be used for SSI authoritication on each interface. The fallency
	specify much encoded adapting, in any, and we doed to sole during the adapting of the one of each methods. The readow
	Fallpert Tructoriet
	Interface Trustmint Evil
	management
	management
	ownande (mytyternagen in watpoint
I I	

- 4. Kies in de vervolgkeuzelijst Invoegen punt het vertrouwen dat u in Stap 3 hebt gemaakt.
- 5. Klik op OK en vervolgens op Toepassen.

Uw nieuw certificaat zou nu gebruikt moeten worden voor alle WebVPN sessies die op de gespecificeerde interface eindigen. Zie de sectie Verifiëren in dit document voor informatie over het controleren van een succesvolle installatie.

Opdrachtlijnvoorbeeld

ciscoa
ciscoasa(config)# ssl trust-point my.verisign.trustpoint outside
! Specifies the trustpoint that will supply the SSL ! certificate for the defined interface. ciscoasa(config)#write memory
Building configuration Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08
8808 bytes copied in 3.630 secs (2936 bytes/sec) [OK] ciscoasa(config)#
! Save configuration.

Verifiëren

In dit hoofdstuk wordt beschreven hoe u kunt bevestigen dat het installeren van uw certificaat door een derde partij is geslaagd.

Vervang een zelfondertekend certificaat van ASA

In dit gedeelte wordt beschreven hoe het geïnstalleerde zelfgetekende certificaat van de ASA moet worden vervangen.

- 1. Geef een verzoek om ondertekening van een certificaat uit aan Verising.Nadat u het gevraagde certificaat van Versie hebt ontvangen, kunt u het rechtstreeks onder hetzelfde punt installeren.
- 2. Typ deze opdracht: **Versiering van crypto-coderingslijst**U wordt gevraagd vragen te beantwoorden.
- 3. Voer **ja** in **en** verstuur de uitvoer naar Verkennend voor verzoek om certificaat om de aansluiting te controleren.
- 4. Typ deze opdracht zodra u het nieuwe certificaat hebt ontvangen: verzegelcertificaat voor invoer

Geïnstalleerde certificaten bekijken

ASDM-procedure

- 1. Klik op **Configuration** en klik op **Properties**.
- 2. **Certificaat** uitvouwen en **Certificaten beheren**.Het CA-certificaat dat wordt gebruikt voor de verificatie van het schaalpunt en het identiteitsbewijs dat is afgegeven door de derde verkoper, moeten in het gebied van de beheerde certificaten worden vermeld.



Opdrachtlijnvoorbeeld

ciscoa
ciscoasa(config)# show crypto ca certificates
! Displays all certificates installed on the ASA.
Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d Certificate Usage:
General Purpose Public Key Type: RSA (1024 bits) Issuer
<pre>Name: cn=verisign Trial Secure Server Test CA ou=Terms of use at https://www.verisign.com/cps/testca (c)05 ou=For Test Purposes Only. No assurances. o=VeriSign</pre>

```
Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of
use at www.verisign.com/cps/testca (c)05 ou=TSWEB
o=Cisco Systems l=Raleigh st=North Carolina c=US OCSP
AIA: URL: http://ocsp.verisign.com CRL Distribution
Points: [1] http://SVRSecure-
crl.verisign.com/SVRTrial2005.crl Validity Date: start
date: 00:00:00 UTC Jul 19 2007 end date: 23:59:59 UTC
Aug 2 2007 Associated Trustpoints:
my.verisign.trustpoint ! Identity certificate received
from 3rd party vendor displayed above. CA Certificate
Status: Available Certificate Serial Number:
63b1a5cdc59f78801da0636cf975467b Certificate Usage:
General Purpose Public Key Type: RSA (2048 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test Root CA
ou=For Test Purposes Only. No assurances. o=VeriSign\,
Inc. c=US Subject Name: cn=VeriSign Trial Secure Server
Test CA ou=Terms of use at
https://www.verisign.com/cps/testca (c)05 ou=For Test
Purposes Only. No assurances. o=VeriSign\, Inc. c=US
Validity Date: start date: 00:00:00 UTC Feb 9 2005 end
date: 23:59:59 UTC Feb 8 2015 Associated Trustpoints:
my.verisign.trustpoint ! CA intermediate certificate
displayed above.
```

Geïnstalleerde certificaten voor WebVPN verifiëren via een webbrowser

Voer de volgende stappen uit om te verifiëren dat WebVPN het nieuwe certificaat gebruikt:

- 1. Connect met uw WebVPN-interface door een webbrowser. Gebruik https:// samen met de FQDN die u gebruikte om het certificaat aan te vragen (bijvoorbeeld https://webvpn.cisco.com).Als u een van deze beveiligingswaarschuwingen ontvangt, voert u de procedure uit die met die waarschuwing overeenkomt: De naam van het veiligheidscertificaat is ongeldig of komt niet overeen met de naam van de siteControleer dat u de juiste FQDN/CN hebt gebruikt om met de WebVPN-interface van de ASA te verbinden. U moet de FQDN/CN gebruiken die u op het moment dat u om het identiteitsbewijs verzoekt hebt gedefinieerd. U kunt de opdracht show crypto ca certificaten trustpointname gebruiken om de certificaten FQDN/CN te controleren. Het beveiligingscertificaat is afgegeven door een bedrijf dat u niet hebt gekozen om te vertrouwen. Voltooi deze stappen om het basiscertificaat van de derde verkoper aan uw webbrowser te installeren:Klik in het dialoogvenster Beveiligingswaarschuwing op Certificaat bekijken. Klik in het dialoogvenster Certificaat op het tabblad certificaatpad.Selecteer het CA-certificaat boven het door u afgegeven identiteitsbewijs en klik op Certificaat bekijken. Klik op Install Certificate (Certificaat installeren).Klik in het dialoogvenster Wizard Document installeren op Volgende.Selecteer de optie Automatisch de certificaatwinkel selecteren op basis van het selectieknop van het certificaat, klik op Volgende en klik vervolgens op Voltooien.Klik op Ja wanneer u de vraag installeert om het certificaat te bevestigen. Klik in de prompt Importeren op OK en vervolgens op Ja Opmerking: Aangezien dit voorbeeld het Verticaal Trial certificaatmodel gebruikt, moet het Verticaal Trial CA Root-certificaat worden geïnstalleerd om verificatiefouten te voorkomen wanneer gebruikers verbinding maken.
- 2. Dubbelklik op het slotpictogram dat rechtsonder in het WebVPN-aanmeldingspagina staat.De geïnstalleerde certificaatinformatie moet worden weergegeven.
- 3. Bekijk de inhoud om te controleren of deze overeenkomt met uw certificaat van

Ce	ertificate	<u>?</u> ×
	General Details Certification Path	1
	Certificate Information	
	This certificate is intended for the following purpose(s):	-
	•Ensures the identity of a remote computer	
	* Refer to the certification authority's statement for details.	
	Issued to: webvpn.cisco.com	
	Issued by: VeriSign Trial Secure Server Test CA	
	Valid from 8/14/2007 to 8/29/2007	
	, Install Certificate Issuer Statemer	ıt
	Ok	:

Stappen om het SSL-certificaat te verlengen

Voltooi deze stappen om het SSL-certificaat te verlengen:

- 1. Selecteer het vertrouwen dat u moet vernieuwen.
- 2. Kies **inschrijving**.Dit bericht verschijnt:*Als het opnieuw wordt geregistreerd, wordt de huidige cert vervangen door de nieuwe. Wil je doorgaan?*
- 3. Kies ja.Dit zal een nieuwe CSR genereren.
- 4. Verzend de CSR naar uw CA en voer vervolgens het nieuwe ID cert in wanneer u het terugkrijgt.
- 5. Verwijder het trust-point en pas het opnieuw toe op de externe interface.

Opdrachten

Op de ASA, kunt u verscheidene showopdrachten in de opdrachtregel gebruiken om de status van een certificaat te verifiëren.

- Toon crypto ca trustpoint— displays geconfigureerde trustpoints.
- toont het crypto-certificaat—Hier worden alle certificaten weergegeven die op het systeem zijn geïnstalleerd.
- Laat crypto kras zien-displays met gecached certificaat revocatielijsten (CRL).
- toon crypto toets mypubkey rsa-displays alle gegenereerde cryptosleutelparen.

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:

- % Waarschuwing: CA cert is niet gevonden. De geïmporteerde certs zijn mogelijk niet bruikbaar.INFO: Certificaat dat met succes is geïmporteerdCA-certificaat is niet correct gewaarmerkt. Gebruik de opdracht Strestpointname van het certificaat van show crypto ca om te controleren of het CA-certificaat is geïnstalleerd. Zoek de lijn die begint met CA certificaatcertificaat. Als het CA-certificaat is geïnstalleerd, controleert u of dit verwijst naar het juiste betrouwbaar punt.
- 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 doeleindenDeze 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 met *bijbehorende Trustpoints:* Als het foute vertrouwen in een lijst is opgenomen, gebruikt u de in het document beschreven procedures om dit te verwijderen en opnieuw te installeren op het juiste betrouwbaar punt. Controleer ook of het paar niet verandert sinds de CSR is gegenereerd.
- Fout: %PIX|ASA-3-717023 SSL is er niet in geslaagd om het apparaatcertificaat voor trustpoint in te stellen [naam van het betrouwbaar punt]Dit bericht wordt weergegeven wanneer er een fout optreedt wanneer u een apparaatcertificaat voor het gegeven trustpunt instelt om de SSL-verbinding te authentiseren. Wanneer de SSL-verbinding tot stand komt, wordt er gepoogd het apparaatcertificaat in te stellen dat wordt gebruikt. Als er een fout optreedt, wordt er een foutmelding opgeslagen die het geconfigureerde vertrouwde punt bevat dat moet worden gebruikt om het apparaatcertificaat te laden en de reden voor de fout.*naam van het betrouwbaar punt—naam van het vertrouwde punt waarvoor SSL er niet in is geslaagd om een apparaatcertificaat in te stellen.*Aanbevolen actie: Los het probleem op dat wordt aangegeven door de reden die voor de mislukking wordt gemeld.Zorg ervoor dat het gespecificeerde trustpoint is ingeschreven en beschikt over een apparaatcertificaat.Controleer of het certificaat van het apparaat geldig is.Roep desgewenst het trustpunt terug.

Gerelateerde informatie

- Een digitaal certificaat verkrijgen van een Microsoft Windows-certificeringsinstantie met ASDM op een ASA
- <u>Security-productmeldingen</u>
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie Cisco Systems