# ASA Remote Access VPN met OCSP-verificatie onder Microsoft Windows 2012 en OpenSSL

### Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram ASA externe toegang met OCSP Microsoft Windows 2012 CA Installatie van services CA-configuratie voor OCSP-sjabloon **OCSP-servicecertificaat OCSP-serviceleases** CA Configuration voor OCSP-uitbreidingen **OpenSSL** ASA met meerdere OCSP-bronnen ASA met OCSP ondertekend door verschillende CA Verifiëren ASA - Certificaat verkrijgen via SCEP AnyConnect - Certificaat verkrijgen via webpagina ASA VPN Remote Access met OCSP-validatie ASA VPN Remote Access met meerdere OCSP-bronnen ASA VPN Remote Access met OCSP en ingetrokken certificaat Problemen oplossen **OCSP-server** omlaag Tijd niet gesynchroniseerd Ondertekende nonces niet ondersteund **IIS7-serververificatie** Gerelateerde informatie

### Inleiding

Dit document beschrijft hoe u de bevestiging van Online Certificate Status Protocol (OCSP) op een Cisco adaptieve security applicatie (ASA) moet gebruiken voor certificaten die door VPNgebruikers worden aangeboden. Voorbeeldconfiguraties voor twee OCSP-servers (Microsoft Windows Certificate Authority [CA] en OpenSSL) worden weergegeven. In het gedeelte Verifiëren worden gedetailleerde stromen op pakketniveau beschreven en in het gedeelte Problemen oplossen wordt de nadruk gelegd op typische fouten en problemen.

### Voorwaarden

#### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco adaptieve security applicatie configuratie met opdrachtregel voor interface (CLI) en configuratie met Secure Socket Layer (SSL) VPN
- X.509-certificaten
- Microsoft Windows Server
- Linux/OpenSSL

#### Gebruikte componenten

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

- Software voor Cisco adaptieve security applicatie, versie 8.4 en hoger
- Microsoft Windows 7 met Cisco AnyConnect Secure Mobility Client, release 3.1
- Microsoft Server 2012 R2
- Linux met OpenSSL 1.0.0j of 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.

### Configureren

**Opmerking**: Gebruik de <u>Command Lookup Tool</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

#### Netwerkdiagram

De client maakt gebruik van externe VPN-toegang. Deze toegang kan zijn: Cisco VPN-client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange versie 2 [IKEv2]) of WebVPN (portal). Om in te loggen, geeft de client het juiste certificaat en de gebruikersnaam/wachtwoord die lokaal op de ASA zijn geconfigureerd. Het clientcertificaat wordt gevalideerd via de OCSP-server.



#### ASA externe toegang met OCSP

ASA wordt geconfigureerd voor SSL-toegang. De client maakt gebruik van AnyConnect om in te loggen. ASA gebruikt Simple Certificate Enrollment Protocol (SCEP) om het certificaat aan te vragen:

```
crypto ca trustpoint WIN2012

revocation-check ocsp

enrollment url http://10.147.25.80:80/certsrv/mscep/mscep.dll
```

crypto ca certificate map MAP 10 subject-name co administrator

Er wordt een certificaatkaart gemaakt om alle gebruikers te identificeren van wie de onderwerpnaam het woord beheerder bevat (hoofdlettergevoeligheid). Deze gebruikers zijn gebonden aan een tunnelgroep met de naam RA:

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable
certificate-group-map MAP 10 RA
```

De VPN-configuratie vereist een succesvolle autorisatie (dat wil zeggen een gevalideerd certificaat). Het vereist ook de juiste referenties voor de lokaal gedefinieerde gebruikersnaam (authenticatie aaa):

```
aaa authentication LOCAL
aaa authorization LOCAL
group-policy MY internal
group-policy MY attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
default-group-policy MY
authorization-required
tunnel-group RA webvpn-attributes
authentication aaa certificate
group-alias RA enable
```

### Microsoft Windows 2012 CA

**Opmerking**: Zie de <u>configuratiehandleiding voor Cisco ASA 5500 Series met behulp van de</u> <u>CLI, 8.4 en 8.6</u>: Configureer een externe server voor security applicatie gebruikersautorisatie voor informatie over de configuratie van de ASA via de CLI.

#### Installatie van services

Deze procedure beschrijft hoe u de rolservices voor de Microsoft server moet configureren:

1. Ga naar **Server Manager > Beheer > Rollen en functies toevoegen**. De Microsoft-server heeft deze rolservices nodig:

CertificeringsinstantieWebinschrijving voor certificeringsinstanties, die door de client wordt gebruiktOnline Responder, die nodig is voor OCSPService voor inschrijving van netwerkapparaten, die de SCEP-toepassing bevat die door de ASA wordt gebruikt Webservice met beleid kan indien nodig worden toegevoegd.

Role Services		DESTINATION SEF WIN-35QVH03PQE3.lab.
Credentials	Select Role Services to configure	
Role Services		
Setup Type	Certification Authority	
CA Type	Certification Authority Web Enrollment	
Private Key	Network Device Enrollment Service	
Cryptography	Certificate Enrollment Web Service	
CA Name	<ul> <li>Certificate Enrollment Policy Web Service</li> </ul>	
Validity Period		
Certificate Database		
Authentication Type for C		
Confirmation		
Progress		
	More about AD CS Server Roles	
1		

- 3.
- 4. Wanneer u functies toevoegt, dient u Online Responder Tools op te nemen omdat dit een OCSP-module bevat die later wordt gebruikt:

	Add Roles and Features Wizard	
Select features		DESTINATION SERVER WIN-35QVH03PQE3.lab.com
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection		Online Responder Tools includes the
Server Roles	<ul> <li>Role Administration Tools (12 of 28 installed)</li> </ul>	Online Responder Management
Features	AD DS and AD LDS Tools (4 of 5 installed)	snap-in.
AD CS	Hyper-V Management Tools	
Role Services	Kemote Desktop Services Tools (1 of 3 insta	
Confirmation	A Active Directory Certificate Services Tools	
	✓       Certification Authority Management Tools         ✓       Online Responder Tools         ✓       DHCP Server Tools (Installed)         ✓       DNS Server Tools (Installed)         ✓       File Services Tools         ✓       File Services Tools         ✓       Network Policy and Access Services Tools (Installed)	

#### CA-configuratie voor OCSP-sjabloon

De OCSP-service gebruikt een certificaat om de OCSP-respons te ondertekenen. Er moet een speciaal certificaat op de Microsoft-server worden gegenereerd, met inbegrip van:

- Uitgebreid sleutelgebruik = OCSP-ondertekening
- OCSP niet herroepingscontrole

Dit certificaat is nodig om OCSP-validatielussen te voorkomen. ASA gebruikt de OCSP-service niet om te proberen het certificaat te controleren dat door de OCSP-service wordt aangeboden.

 Voeg een sjabloon toe voor het certificaat op de CA. Navigeer naar CA > certificaatsjabloon > Beheer, selecteer OCSP Response Signing en dupliceer de sjabloon. Bekijk de eigenschappen voor de nieuwe sjabloon en klik op het tabblad Beveiliging. De toestemmingen beschrijven welke entiteit wordt toegestaan om een certificaat te verzoeken dat dat malplaatje gebruikt, zodat worden de correcte toestemmingen vereist. In dit voorbeeld is de entiteit de OCSP-service die op dezelfde host wordt uitgevoerd (TEST-CISCO\DC) en heeft de OCSP-service Autoenroll-rechten nodig:

<b>2</b>	Certific	ate Templates Cons	ole				- 1	• >	x
File Action View Help									
(+ +) 📷 📾 🔒 🖬 📷									
Certificate Templates (DC.test-c	Template Display Name	Schema Verring	Verri	Intended Ru	Actions				_
	Administrator	Pro	perties of New	Template	×	еT	empla	ates	*
	Authenticated Session	Authenticated Session Revic EFS Subject Name Server Issuance Requirements of					ons		۲
	CA Exchange	Compatibility General	Request Handing	Cryptography	Key Attestation	po	nse Si	ani	
	CEP Encryption	Superseded Temps	ates   Ext	ensions	Jecuny	ctic	ons	-	×
	Code Signing	& Authenticated Us	ers						
	Copy of OCSP Response Signing	& Administrator							
	Cross Certification Authority	Bornain Admins (1	/\DC\$) TEST-CISCO\Domai	n Admins)					
	Directory Email Replication	& Enterprise Admins	(TEST-CISCO\Ente	rprise Admins)					
	Domain Controller Authentication								
	EFS Recovery Agent								
	Enrollment Agent (Computer)			Add	Remove				
	Exchange Enrollment Agent (Offline	Permissions for DC		Allow	Deny				
	Exchange Signature Only	Full Control							
	IPSec	Write			8 11				
	IPSec (Offline request)	Enroll							
	Kerberos Authentication	Autoenroll							
	OCSP Response Signing								
	RAS and IAS Server	For special permissions	or advanced setting	s, click	Advanced				
	Router (Offline request)	Advanced.		_					
	Smartcard Logon								
	Subordinate Certification Authority	ОК	Cancel	Apply	Help				
	Trust List Signing	1	3.1						
< III >	<				>				

Alle andere instellingen voor de sjabloon kunnen op standaard worden ingesteld.

2. Activeer de sjabloon. Navigeer naar CA > certificaatsjabloon > Nieuw > Certificaatsjabloon voor afgifte, en selecteer de sjabloon voor het duplicaat:



#### **OCSP-servicecertificaat**

In deze procedure wordt beschreven hoe u Online Configuration Management kunt gebruiken om OCSP te configureren:

- 1. Navigeer naar Server Manager > Tools.
- 2. Navigeren naar Herroepingsconfiguratie > Herroepingsconfiguratie toevoegen om een nieuwe configuratie toe te voegen:

9	ocsp - [Online Responder: DC.test-cisco.com\Re	evocation Configuration]
File Action View Help		
🗢 🔿 🙍 🗟		
Ponline Responder: DC.test-cisco.cc	Name Signing Cert	ificate Selec Enrollment Ten
<ul> <li></li></ul>	There are no items to show in th	is view.
	Add Revocation Configuration	? X
Choose CA Ce	ertificate	
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate	In order to check the status of a certificate, a revocation configuration Responder must identify the CA that issued the certificate. You can identify this CA by selecting a CA certificate published in Ac by locating a CA computer.	n for the Online tive Directory or
Select Signing Certificate	<ul> <li>Browse CA certificates published in Active Directory</li> </ul>	Browse
Revocation Provider	Select Certification Authority	×
	Select a certification authority (CA) you want to use	rowse
	CA Computer	
	test-cisco-DC-CA DC.test-cisco.com	
	< III OK Cancel	Cancel

OCSP kan dezelfde Enterprise-CA gebruiken. Er wordt een certificaat voor OCSP-service gegenereerd.

3. Gebruik de geselecteerde Enterprise CA en kies de sjabloon die eerder is gemaakt. Het certificaat wordt automatisch ingeschreven:



4. Bevestig dat het certificaat is ingeschreven en dat de status werkt/OK is.



Revocation Configuration Status	
Signing Certificate: Ok	
<u>View Signing Certificate</u> Revocation Provider Status	
Type: Microsoft CRL-based revocation status provider	^
The revocation provider is successfully using the current configuration	
I	
	$\sim$

5. Navigeer naar CA > Afgegeven certificaten om de certificaatgegevens te verifiëren:

i 🖕	certsrv - [Certification Authority (Local)\test-cisco-D	C-CA\I	ssued Certificate	es]
File Action View Help				
🗢 🔿 🙎 🙆 📓	Certificate X			
<ul> <li>Certification Authority (Local)</li> <li>Certification Authority (Local)</li> <li>test-cisco-DC-CA</li> <li>Revoked Certificates</li> <li>Issued Certificates</li> <li>Pending Requests</li> <li>Failed Requests</li> <li>Certificate Templates</li> </ul>	Certificate       ×         General       Details       Certification Path         Show: <all>       ×         Field       Value       ^         Valid to       Thursday, October 24, 2013 6       ×         Subject       DC.test-cisco.com       ×         Public key       RSA (2048 Bits)       ×         Certificate Template Inform       Template=1.3.6.1.4.1.311.21       ×         Enhanced Key Usage       OCSP Spring (1.3.6.1.5.5.7.3       ×         OCSP No Revocation Checking       05 00       ×         Application/Policies       [1]Application Certificate Polic       ×         OCSP No Revocation Checking       05 00       ×         Authority Key Identifier       KeyID=9f 99 7f b2 3b 61 90 0       ×</all>	ilate ler ( ment (СЕР ques ques ques	Serial Number 24000000206c 240000003d86 2400000057d8 24000000639b 24000000639b 2400000082d2 24000000088d 24000000098d 24000000098d 240000000048 240000000cb0c 240000000cb0c	Certificate Effective Date 10/10/2013 7:25 AM 10/10/2013 7:33 AM 10/10/2013 7:33 AM 10/10/2013 11:54 AM 10/10/2013 11:54 AM 10/11/2013 12:05 AM 10/11/2013 12:12 AM 10/10/2013 1:27 PM 10/10/2013 1:27 PM 10/10/2013 1:28 PM 10/10/2013 1:30 PM 10/10/2013 1:31 PM
	OCSP Signing (1.3.6.1.5.5.7.3.9) Edit Properties Copy to File OK	ques .8.16	24000000e80d 240000001221c	10/10/2013 2:06 PM 10/10/2013 6:51 PM

#### **OCSP-serviceleases**

Microsoft-implementatie van OCSP is compatibel met <u>RFC 5019 The Lichtgewicht Online</u> <u>Certificate Status Protocol (OCSP) Profile for High-Volume Environments</u>, een vereenvoudigde versie van <u>RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -</u> <u>OCSP</u>.

ASA gebruikt RFC 2560 voor OCSP. Een van de verschillen tussen de twee RFC's is dat RFC 5019 geen ondertekende verzoeken van ASA accepteert.

Het is mogelijk om de Microsoft OCSP-dienst te dwingen deze ondertekende verzoeken te

aanvaarden en te antwoorden met de juiste ondertekende reactie. Navigeer naar Herroepingsconfiguratie > RevocationConfiguration1 > Eigenschappen bewerken en selecteer de optie om de uitbreidingsondersteuning van Nonce in te schakelen.

File Action View Help			
🗢 🔿 🙍 🗟			
Solution Presponder: DC.test-cisco.cc	Name	Signing Certificate Selec	- Enrollment Template
Revocation Configuration	RevocationConfiguration1	Automatically enrolled	Copy 2 of OCSP Response S
Array Configuration	Properties for Revocation Co	nfiguration: RevocationC 🗙	
	Local CRL Revocation Provider S	igning	
	The selected hash algorithm is used b responses sent to clients.	y the Online Responders to sign	
	Hash algorithm: SHA1	¥	
	Do not prompt for credentials for c	cryptographic operations	
	<ul> <li>Automatically use renewed signing</li> </ul>	g certificates.	
	<ul> <li>Enable NONCE extension support</li> </ul>	t	
	Use any valid OCSP signing certif	icate	
	Online Responder Identifiers All responses will include the follow	ing Online Responder identifier:	
	<ul> <li>Key hash of the signing certification</li> </ul>	ate	
	<ul> <li>Subject of the signing certificat</li> </ul>	e	
~			
	0	K Cancel Help	

De OCSP-service is nu klaar voor gebruik.

Hoewel Cisco dit niet aanraadt, kunnen verbindingen worden uitgeschakeld op de ASA:

BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce

#### CA Configuration voor OCSP-uitbreidingen

U moet nu de CA aanpassen om de OCSP-serveruitbreiding op te nemen in alle afgegeven certificaten. De URL van deze extensie wordt door ASA gebruikt om verbinding te maken met de OCSP-server wanneer een certificaat wordt gevalideerd.

- 1. Open het dialoogvenster Eigenschappen voor de server op de CA.
- Klik op het tabblad Uitbreidingen. De extensie Autoriteit Information Access (AIA) die verwijst naar de OCSP-dienst is nodig; in dit voorbeeld is het http://10.61.208.243/ocsp. Schakel beide opties voor de AIA-extensie in:

In de AIA-verlenging van afgegeven certificaten opnemenOmvat in de online extensie van het certificaatprotocol (OCSP)

ته c	tes	test-cisco-DC-CA Properties ?						
File Action View Help	Enrollment Agents	Auditing	Recover	y Agents	Security			
	General Policy Module Exit Modu Extensions Storage Certificate Manage							
↓ Certification Authority (Local) ↓ test-cisco-DC-CA	Select extension:							
Revoked Certificates	Authority Information	Access (AIA)			~			
Pending Requests	Specify locations from	which users car	n obtain the o	certificate for	this CA.			
Failed Requests	C:\Windows\mutam?							
	C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<caname:  dap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN=S http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce file://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert< td=""></cert<></caname></serverdnsname></serverdnsname></cert </caname></serverdnsname></serverdnsname></ce </caname></serverdnsname></serverdnsname></catruncatedname></caname: </serverdnsname>							
$\mathbf{k}$	< 111				>			
			Ado	d	Remove			
	<ul> <li>✓ Include in the AIA</li> <li>✓ Include in the online</li> </ul>	extension of issu e certificate stat	ed certificate us protocol (	es OCSP) exter	ision			

Dit waarborgt dat alle afgegeven certificaten een correcte uitbreiding hebben die naar de OCSP-dienst verwijst.

#### **OpenSSL**

**Opmerking**: Zie de <u>configuratiehandleiding voor Cisco ASA 5500 Series met behulp van de</u> <u>CLI, 8.4 en 8.6: Configureer een externe server voor security applicatie gebruikersautorisatie</u> voor informatie over de configuratie van de ASA via de CLI.

In dit voorbeeld wordt ervan uitgegaan dat de OpenSSL-server al is geconfigureerd. In dit gedeelte worden alleen de OCSP-configuratie en -wijzigingen beschreven die nodig zijn voor de CA-configuratie.

In deze procedure wordt beschreven hoe het OCSP-certificaat moet worden gegenereerd:

1. Deze parameters zijn nodig voor de OCSP-responder:

```
[ OCSPresponder ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSPSigning
```

2. Deze parameters zijn nodig voor gebruikerscertificaten:

```
[ UserCerts ]
authorityInfoAccess = OCSP;URI:http://10.61.208.243
```

- 3. Certificaten moeten worden gegenereerd en ondertekend door de CA.
- 4. Start de OCSP-server:

```
openssl ocsp -index ourCAwebPage/index.txt -port 80 -rsigner
ocspresponder.crt -rkey ocspresponder.key -CA cacert.crt -text -out
log.txt
```

5. Test het voorbeeldcertificaat:

```
openssl ocsp -CAfile cacert.crt -issuer cacert.crt -cert example-cert.crt -url http://10.61.208.243 -resp_text
```

Meer voorbeelden zijn beschikbaar op de OpenSSL website .

OpenSSL ondersteunt OCSP-nonces, net als ASA; de nonces kunnen worden bestuurd met behulp van de -nonce en -no\_nonce switches.

#### ASA met meerdere OCSP-bronnen

ASA kan de OCSP-URL overschrijven. Zelfs als het clientcertificaat een OCSP-URL bevat, wordt deze overschreven door de configuratie op de ASA:

crypto ca trustpoint WIN2012 revocation-check ocsp enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll

ocsp url http://10.10.10.10/ocsp

Het OCSP-serveradres kan expliciet worden gedefinieerd. Dit opdrachtvoorbeeld past alle certificaten aan met beheerder in onderwerpnaam, gebruikt een OPENSSL-trustpoint om OCSP-handtekening te valideren en gebruikt de URL van http://11.11.11.11/ocsp om het verzoek te verzenden:

crypto ca trustpoint WIN2012
revocation-check ocsp
enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map **MAP** 10 subject-name co administrator

De volgorde die wordt gebruikt om OCSP URL te vinden is:

- 1. Een OCSP-server die u met de opdracht matchcertificaat hebt ingesteld
- 2. Een OCSP-server die u met de opdracht OCSP-URL hebt ingesteld
- 3. De OCSP-server in het AIA-veld van het clientcertificaat

#### ASA met OCSP ondertekend door verschillende CA

Een OCSP-antwoord kan worden ondertekend door een andere CA. In een dergelijk geval is het

noodzakelijk om de opdracht **matchcertificaat** te gebruiken om een ander betrouwbaarheidspunt op de ASA te gebruiken voor OCSP-certificaatvalidatie.

crypto ca trustpoint WIN2012
revocation-check ocsp
enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map **MAP** 10 subject-name co administrator

crypto ca trustpoint **OPENSSL** enrollment terminal revocation-check none

In dit voorbeeld gebruikt de ASA de OCSP URL om alle certificaten te herschrijven met een onderwerpnaam die beheerder bevat. ASA wordt gedwongen om het OCSP-respondercertificaat te valideren tegen een ander trustpoint, OPENSSL. Gebruikerscertificaten worden nog steeds gevalideerd in de Win2012 trustpoint.

Aangezien het OCSP-antwoordcertificaat de extensie 'OCSP no revocation check' heeft, wordt het certificaat niet geverifieerd, zelfs als OCSP gedwongen is te valideren tegen het OPENSSLbetrouwbaarheidspunt.

Standaard worden alle trustpoints doorzocht wanneer de ASA het gebruikerscertificaat probeert te verifiëren. Validatie voor het OCSP-antwoordcertificaat is anders. De ASA zoekt alleen het trustpoint dat al is gevonden voor het gebruikerscertificaat (WIN2012 in dit voorbeeld).

Daarom is het noodzakelijk om de opdracht **matchcertificaat** te gebruiken om de ASA te dwingen een ander trustpoint te gebruiken voor OCSP-certificaatvalidatie (OPENSSL in dit voorbeeld).

Gebruikerscertificaten worden gevalideerd tegen het eerste overeenkomende trustpoint (WIN2012 in dit voorbeeld), dat vervolgens het standaard trustpoint voor OCSP-respondervalidatie bepaalt.

Als in de opdracht **matchcertificaat** geen specifiek trustpoint wordt verstrekt, wordt het OCSPcertificaat gevalideerd tegen hetzelfde trustpoint als de gebruikerscertificaten (WIN2012 in dit voorbeeld).

crypto ca trustpoint WIN2012
revocation-check ocsp
enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
match certificate MAP override ocsp 10 url http://11.11.11.11/ocsp

### Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

**Opmerking**: De <u>Output Interpreter Tool</u> (alleen geregistreerde klanten) ondersteunt bepaalde **show** opdrachten. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

#### ASA - Certificaat verkrijgen via SCEP

In deze procedure wordt beschreven hoe het certificaat via het SCEP kan worden verkregen:

1. Dit is het vertrouwde verificatieproces voor het verkrijgen van het CA-certificaat:

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction
BSNS-ASA5510-3(config-ca-crl)# crypto ca authenticate WIN2012
Crypto CA thread wakes up!
CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83
CRYPTO_PKI: http connection opened
INFO: Certificate has the following attributes:
Fingerprint:
               27dda0e5 e1ed3f4c e3a2c3da 6d1689c2
Do you accept this certificate? [yes/no]:
% Please answer 'yes' or 'no'.
Do you accept this certificate? [yes/no]:
ves
```

Trustpoint CA certificate accepted.

2. Om het certificaat aan te vragen moet de ASA een eenmalig SCEP-wachtwoord hebben dat kan worden verkregen bij de beheerdersconsole op http://IP/certsrv/mscep\_admin:



3. Gebruik dat wachtwoord om het certificaat bij de ASA aan te vragen:

Re-enter password: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

% The fully-qualified domain name in the certificate will be: BSNS-ASA5510-3.test-cisco.com % Include the device serial number in the subject name? [yes/no]: yes % The serial number in the certificate will be: JMX1014K16Y

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
BSNS-ASA5510-3(config)#

```
CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83
```

CRYPTO\_PKI: http connection opened

CRYPTO\_PKI: Found a subject match - inserting the following cert record into certList Een deel van de output is weggelaten voor de duidelijkheid.

4. Controleer zowel de CA- als ASA-certificaten:

```
BSNS-ASA5510-3(config)# show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 240000001cbf2fc89f44fe81970000000000
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
  cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Subject Name:
   hostname=BSNS-ASA5510-3.test-cisco.com
  serialNumber=JMX1014K16Y
CRL Distribution Points:
  [1] ldap:///CN=test-cisco-DC-CA,CN=DC,CN=CDP,
CN=Public%20Key%20Services,CN=Services,CN=Configuration,
DC=test-cisco,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
Validity Date:
  start date: 11:02:36 CEST Oct 13 2013
  end date: 11:02:36 CEST Oct 13 2015
Associated Trustpoints: WIN2012
CA Certificate
Status: Available
Certificate Serial Number: 3d4c0881b04c799f483f4bbe91dc98ae
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
   cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Subject Name:
  cn=test-cisco-DC-CA
```

```
dc=test-cisco
dc=com
Validity Date:
  start date: 07:23:03 CEST Oct 10 2013
  end date: 07:33:03 CEST Oct 10 2018
Associated Trustpoints: WIN2012
```

ASA toont niet de meeste certificaatuitbreidingen. Hoewel het ASA certificaat de 'OCSP URL in AIA' extensie bevat, wordt het door de ASA CLI niet getoond. Deze verbetering wordt aangevraagd door Cisco Bug ID <u>CSCui44335</u>, "ASA ENH Certificate x509 extensions displays".

#### AnyConnect - Certificaat verkrijgen via webpagina

Deze procedure beschrijft hoe het certificaat te verkrijgen door gebruik van de webbrowser op de client:

1. Via de webpagina kan een AnyConnect-gebruikerscertificaat worden aangevraagd. Gebruik op de client-pc een webbrowser om naar de CA te gaan op http://*IP*/certsrv:



 Het gebruikerscertificaat kan worden opgeslagen in de webbrowserwinkel en vervolgens worden geëxporteerd naar de Microsoft Store, die wordt doorzocht door AnyConnect. Gebruik certmgr.msc om het ontvangen certificaat te verifiëren:



AnyConnect kan ook het certificaat aanvragen zolang er een correct AnyConnect-profiel is.

#### ASA VPN Remote Access met OCSP-validatie

In deze procedure wordt beschreven hoe de OCSP-validering moet worden gecontroleerd:

1. Aangezien de ASA probeert verbinding te maken, meldt de ASA dat het certificaat wordt gecontroleerd op OCSP. In dit geval is het OCSP-ondertekeningscertificaat zonder controle uitgebreid en niet via OCSP gecontroleerd:

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction
%ASA-6-725001: Starting SSL handshake with client outside:
10.61.209.83/51262 for TLSv1 session.
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain.
serial number: 240000001B2AD208B1281168740000000001B, subject name:
cn=Administrator, cn=Users, dc=test-cisco, dc=com.
Found a suitable trustpoint WIN2012 to validate certificate.
%ASA-7-717035: OCSP status is being checked for certificate. serial
number: 240000001B2AD208B1281168740000000001B, subject name:
cn=Administrator, cn=Users, dc=test-cisco, dc=com.
%ASA-6-302013: Built outbound TCP connection 1283 for outside:
10.61.209.83/80 (10.61.209.83/80) to identity:10.48.67.229/35751
(10.48.67.229/35751)
%ASA-6-717033: CSP response received.
%ASA-7-717034: No-check extension found in certificate. OCSP check
bypassed.
%ASA-6-717028: Certificate chain was successfully validated with
revocation status check.
Een deel van de output is weggelaten voor de duidelijkheid.
```

2. De eindgebruiker geeft de gebruikersreferenties aan:

🕙 Cisco AnyConn	ect   10.48.67.229	
Username:	cisco	
Password:		
	OK Cancel	
🕥 Cisco AnyCon	nect Secure Mobility Client	
	VPN: Contacting 10.48.67.229. 10.48.67.229	Connect
Ö Ö		ajtajta

3. De VPN-sessie is correct voltooid:

%ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with serial number: 24000001B2AD208B128116874000000001B, subject name: cn=Administrator, cn=Users,dc=test-cisco,dc=com, issuer\_name: cn=test-cisco-DC-CA, dc=test-cisco,dc=com. %ASA-7-717038: Tunnel group match found. Tunnel Group: RA, Peer certificate: serial number: 24000001B2AD208B1281168740000000001B, subject name: cn=Administrator,cn=Users,dc=test-cisco,dc=com, issuer\_name: cn=test-cisco-DC-CA,dc=test-cisco,dc=com. %ASA-6-113012: AAA user authentication Successful : local database : user = cisco %ASA-6-113009: AAA retrieved default group policy (MY) for user = cisco %ASA-6-113039: Group <MY> User <cisco> IP <10.61.209.83> AnyConnect parent session started. 4. De sessie wordt aangemaakt:

4

BSNS-ASA5510-3(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username	: cisco	Index	:
----------	---------	-------	---

Assigned IP : 192.168.11.100 Public IP : 10.61.209.83 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 10540 Pkts Tx : 8 Bytes Rx : 32236 Pkts Rx : 209 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : MY Tunnel Group : RA Login Time : 11:30:31 CEST Sun Oct 13 2013 : 0h:01m:05s Duration Inactivity : 0h:00m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 4.1 Public IP : 10.61.209.83 Encryption : none Hashing : none TCP Src Port : 51401 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5270 Bytes Rx : 788 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 4.2 Assigned IP : 192.168.11.100 Public IP : 10.61.209.83 Hashing : SHA1 TCP Src Port : 51406 Auth Mode : Certificate and Encryption : RC4 Encapsulation: TLSv1.0 TCP Dst Port : 443 userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5270 Bytes Rx : 1995 Pkts Tx : 4 Pkts Rx : 10 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 4.3 Assigned IP : 192.168.11.100 Public IP : 10.61.209.83 Hashing : SHA1 UDP Src Port : 58053 Auth Mode : Certificate and Encryption : AES128 Encapsulation: DTLSv1.0 UDP Dst Port : 443 userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Rx : 29664 Bytes Tx : 0 Pkts Tx : 0 Pkts Rx : 201 Pkts Tx Drop : 0 Pkts Rx Drop : 0

#### 5. U kunt gedetailleerde debugs voor OCSP-validatie gebruiken:

CRYPTO\_PKI: Starting OCSP revocation CRYPTO\_PKI: Attempting to find OCSP override for peer cert: serial number: 2400000019F341BA75BD25E91A00000000019, subject name: cn=Administrator, cn=Users,dc=test-cisco,dc=com, issuer\_name: cn=test-cisco-DC-CA, dc=test-cisco,dc=com. CRYPTO\_PKI: No OCSP overrides found. <-- no OCSP url in the ASA config CRYPTO\_PKI: http connection opened CRYPTO\_PKI: OCSP response received successfully. CRYPTO\_PKI: OCSP found in-band certificate: serial number: 240000001221CFA239477CE1C000000000012, subject name: cn=DC.test-cisco.com, issuer\_name: cn=test-cisco-DC-CA,dc=test-cisco, dc=com CRYPTO\_PKI: OCSP responderID byKeyHash CRYPTO\_PKI: OCSP response contains 1 cert singleResponses responseData sequence. Found response for request certificate! CRYPTO\_PKI: Verifying OCSP response with 1 certs in the responder chain CRYPTO\_PKI: Validating OCSP response using trusted CA cert: serial number: 3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA, dc=test-cisco,dc=com, issuer\_name: cn=test-cisco-DC-CA,dc=test-cisco, dc=com CERT-C: W ocsputil.c(538) : Error #708h CERT-C: W ocsputil.c(538) : Error #708h CRYPTO\_PKI: Validating OCSP responder certificate: serial number: 240000001221CFA239477CE1C000000000012, subject name: cn=DC.test-cisco.com, issuer\_name: cn=test-cisco-DC-CA,dc=test-cisco, dc=com, signature alg: SHA1/RSA CRYPTO\_PKI: verifyResponseSig:3191 CRYPTO\_PKI: OCSP responder cert has a NoCheck extension CRYPTO\_PKI: Responder cert status is not revoked <-- do not verify responder cert CRYPTO\_PKI: response signed by the CA CRYPTO\_PKI: Storage context released by thread Crypto CA CRYPTO\_PKI: transaction GetOCSP completed CRYPTO\_PKI: Process next cert, **valid cert**. <-- client certificate validated correctly

Op het pakketopnameniveau is dit het OCSP-verzoek en de juiste OCSP-respons. Het antwoord bevat de juiste handtekening - nonce extensie ingeschakeld op Microsoft OCSP:

No.	Source	Destination	Protocol	Length	Info
24	10.48.67.229	10.61.208.243	0CSP	545	Request
31	10.61.208.243	10.48.67.229	0CSP	700	Response
۹.					
▶ Hy	pertext Transfer Prot	tocol			
<mark>⊽</mark> 0n	line Certificate Stat	tus Protocol			
	responseStatus: succe	ssful (0)			
⊽	responseBytes				
	ResponseType Id: 1.3	3.6.1.5.5.7.48.1.1 (	id-pkix-	ocsp-ba	sic)
~	BasicOCSPResponse				
	🔻 tbsResponseData				
	▷ responderID: byK	ey (2)			
	producedAt: 2013	-10-12 14:48:27 (UTC	.)		
	♭ responses: 1 ite	m			
	▼ responseExtensio	ns: 1 item			
	<pre>▼ Extension</pre>				
	Id: 1.3.6.1.5	.5.7.48.1.2 (id-pkix	.48.1.2	)	
	▹ BER: Dissecto	r for OID:1.3.6.1.5.	5.7.48.	1.2 not	implemented.
	▹ signatureAlgorithm	(shaWithRSAEncrypt:	ion)		
	Padding: 0				
	signature: 353fc46	1732dc47b1d167ebace6	677a0877	65b48ed	b3b284c
	⊳ certs: 1 item				

#### ASA VPN Remote Access met meerdere OCSP-bronnen

Als een matchcertificaat is geconfigureerd zoals in <u>ASA</u> wordt uitgelegd<u>met meerdere OCSP-</u> <u>bronnen</u>, krijgt het voorrang:

CRYPTO\_PKI: Processing map MAP sequence 10... CRYPTO\_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=Administrator,cn=Users,dc=test-cisco,dc=com, map rule: subject-name co administrator. CRYPTO\_PKI: Peer cert has been authorized by map: MAP sequence: 10. CRYPTO\_PKI: Found OCSP override match. Override URL: http://11.11.11.11/ocsp, Override trustpoint: OPENSSL

Wanneer een OCSP URL-overschrijving wordt gebruikt, zijn de debugs:

```
CRYPTO_PKI: No OCSP override via cert maps found. Override was found in trustpoint: WIN2012, URL found: http://10.10.10.10/ocsp.
```

#### ASA VPN Remote Access met OCSP en ingetrokken certificaat

In deze procedure wordt beschreven hoe het certificaat kan worden ingetrokken en de ingetrokken status kan worden bevestigd:

1. Trek het clientcertificaat in:

🗔 certsrv - [Cer	tificatio	n Autł	nority (Loc	al)\t	est-cisco-DC-CA\ls	sued
File Action View Help						
🗢 🔿 🙎 🗟 🗟						
🙀 Certification Authority (Local)	Request	ID	Requester Na	ame	Binary Certificate	Certif
⊿ 🚽 test-cisco-DC-CA	<b>5</b> 6		TEST-CISCO	\Ad	BEGIN CERTI	IPSec
Revoked Certificates	<b>-</b> 7		TEST-CISCO	∖Ad	BEGIN CERTI	IPSec
Issued Certificates	5		TEST-CISCO	∖Ad	BEGIN CERTI	IPSec
Pending Requests	5		TEST-CISCO	∖Ad	BEGIN CERTI	User
Failed Requests	🔄 10		TEST-CISCO	∖Ad	BEGIN CERTI	User
Certificate Templates	🔄 11		TEST-CISCO\Ad		BEGIN CERTI	User
	🔄 12		TEST-CISCO	∖Ad	BEGIN CERTI	User
	🔄 13		TEST-CISCO	∖Ad	BEGIN CERTI	User
	🔄 14		TEST-CISCO	∖Ad	BEGIN CERTI	IPSec
	🔄 18		TEST-CISCO	DC\$	BEGIN CERTI	Сору
	🔄 19		TEST-CISCO	∖Ad	BEGIN CERTI	IPSec
	iii 20		TEST-CISCO	∖Ad	BEGIN CERTI	IPSec
	21		TEST-CISCO	∖Ad	BEGIN CERTI	User
		0		Ad	BEGIN CERTI	User
		Open		Ad	BEGIN CERTI	User
		All Ta	sks 🕨 🕨		View Attributes/Extensi	ons
R	<b></b>	Refre	sh		Export Binary Data	
		Help			Revoke Certificate	
	28		TEST-CISCO	Ad	BEGIN CERTI	IPSec
	<		III			
Contains actions that can be performe	d on the it	em.				

2. Publiceer de resultaten:



3. [Optioneel] Stappen 1 en 2 kunnen ook worden uitgevoerd met het zekere CLIhulpprogramma in Power Shell:

```
c:\certutil -crl
CertUtil: -CRL command completed succesfully.
```

4. Wanneer de client probeert verbinding te maken, is er een fout bij de certificaatvalidatie:

Cisco AnyConnect	<b>EXE</b>		
<b>A</b> Certificate Validat	ion Failure		
	ОК		
Sisco AnyConnect Secure	e Mobility Client		
VPN: No valid cert 10.48.67.2	tificates available for au 29	uthentication.	ct
<b>\$</b> (i)			ajiaji. cisco

5. De AnyConnect-logbestanden geven ook de fout in de certificaatvalidatie aan:

[2013-10-13 12:49:53] Contacting 10.48.67.229. [2013-10-13 12:49:54] No valid certificates available for authentication. [2013-10-13 12:49:55] Certificate Validation Failure

6. De ASA meldt dat de certificaatstatus is ingetrokken:

```
CRYPTO_PKI: Starting OCSP revocation

CRYPTO_PKI: OCSP found in-band certificate: serial number:

240000001221CFA239477CE1C00000000012, subject name:

cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,

dc=com

CRYPTO_PKI: OCSP responderID byKeyHash

CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData

sequence.

Found response for request certificate!

CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain

CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:

3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
```

dc=test-cisco,dc=com, issuer\_name: cn=test-cisco-DC-CA,dc=test-cisco,

dc=com

CRYPTO\_PKI: verifyResponseSig:3191 CRYPTO\_PKI: OCSP responder cert has a NoCheck extension CRYPTO\_PKI: Responder cert status is not revoked CRYPTO\_PKI: response signed by the CA CRYPTO\_PKI: Storage context released by thread Crypto CA

CRYPTO\_PKI: transaction GetOCSP completed

CRYPTO\_PKI: Received OCSP response:Oct 13 2013 12:48:03: %ASA-3-717027: Certificate chain failed validation. Generic error occurred, serial number: 240000001B2AD208B1281168740000000001B, subject name: cn=Administrator,cn=Users,dc=test-cisco,dc=com.

CRYPTO\_PKI: Blocking chain callback called for OCSP response (trustpoint: WIN2012, status: 1) CRYPTO\_PKI: Destroying OCSP data handle 0xae255ac0 CRYPTO\_PKI: OCSP polling for trustpoint WIN2012 succeeded. Certificate status is REVOKED. CRYPTO\_PKI: Process next cert in chain entered with status: 13. CRYPTO\_PKI: Process next cert, Cert revoked: 13

7. Het pakket neemt een succesvolle OCSP-respons weer met de certificaatstatus van ingetrokken:

No.	Source	Destination	Protocol	Length	Info	
24	10.48.67.229	10.61.209.83	0CSP	544	Request	
31	10.61.209.83	10.48.67.229	0CSP	721	Response	
4						
▶ Hy	pertext Transfer Pro	tocol				
<b>⊽ 0n</b>	line Certificate Sta	tus Protocol				
1	responseStatus: succe	ssful (0)				
<b>⊽</b>	responseBytes					
	ResponseType Id: 1.	3.6.1.5.5.7.48.1.1 (	id-pkix-	ocsp-ba	sic)	
~	BasicOCSPResponse					
	▼ tbsResponseData					
	▷ responderID: byKey (2)					
	producedAt: 2013-10-13 10:47:02 (UTC)					
▼ responses: 1 item						
	▷ certID					
	▶ certStatus: r	evoked (1)				
thisUpdate: 2013-10-13 10:17:51 (UTC)						
nextUpdate: 2013-10-14 22:37:51 (UTC)						
<pre>&gt; singleExtensions: 1 item</pre>						
responseExtensions: 1 item						
	▷ signatureAlgorithm (shaWithRSAEncryption)					

### Problemen oplossen

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

#### **OCSP-server** omlaag

ASA meldt wanneer de OCSP-server is uitgeschakeld:

CRYPTO\_PKI: unable to find a valid OCSP server. CRYPTO PKI: OCSP revocation check has failed. Status: 1800. Packet-opnamen kunnen ook helpen bij het oplossen van problemen.

#### Tijd niet gesynchroniseerd

Als de huidige tijd op OCSP-server ouder is dan op ASA (kleine verschillen zijn acceptabel), stuurt de OCSP-server een ongeautoriseerde respons en de ASA rapporteert dit:

CRYPTO\_PKI: OCSP response status - unauthorized

Wanneer de ASA een OCSP-respons ontvangt van toekomstige tijdstippen, faalt dit ook.

#### Ondertekende nonces niet ondersteund

Als de fouten op de server niet worden ondersteund (wat de standaard is op Microsoft Windows 2012 R2), wordt een ongeautoriseerd antwoord teruggestuurd:

No.	Source	Destination	Protocol	Length	Info	
56	10.48.67.229	10.61.208.243	0CSP	545	Request	
59	10.61.208.243	10.48.67.229	0CSP	337	Response	
4						
▶ Fr	ame 59: 337 bytes on	wire (2696 bits), 3	37 bytes	captur	red (2696 bits)	
▶ Et	hernet II, Src: Cisco	_2a:c4:a3 (00:06:f6	:2a:c4:a	3), Dst	:: Cisco_b8:6b:25 (00:1	7:5
▶ In	ternet Protocol Vers	ion 4, Src: 10.61.20	8.243 (1	0.61.20	8.243), Dst: 10.48.67.2	229
▶ Tr	ansmission Control P	rotocol, Src Port: h	ttp (80)	, Dst P	ort: 14489 (14489), Se	q:
▶ Hy	pertext Transfer Pro	tocol				
⊽ 0n	line Certificate Sta	tus Protocol				
	responseStatus: unaut	horized (6)				

#### **IIS7-serververificatie**

Problemen met een SCEP/OCSP-verzoek zijn vaak het gevolg van onjuiste authenticatie op Internet Information Services 7 (IIS7). Zorg ervoor dat anonieme toegang is geconfigureerd:

File View Help					
Connections	Authentication				
<ul> <li>DC (TEST-CISCO\Administrat</li> <li>Application Pools</li> <li>Sites</li> <li>Opfault Web Site</li> <li>Opfault Web Site</li></ul>	Name Anonymous Authentication ASP.NET Impersonation Basic Authentication Digest Authentication Forms Authentication Windows Authentication	Status Enabled Disabled Disabled Disabled Disabled	Response Type HTTP 401 Challenge HTTP 401 Challenge HTTP 302 Login/Redirect HTTP 401 Challenge		

## Gerelateerde informatie

- Microsoft TechNet: handleiding voor installatie, configuratie en probleemoplossing van online responder
- Microsoft TechNet: Een CA configureren ter ondersteuning van OCSP-responders
- <u>Cisco ASA Series opdrachtreferentie</u>
- Technische ondersteuning en documentatie Cisco Systems

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.