VPN d'accès à distance ASA avec vérification OCSP sous Microsoft Windows 2012 et OpenSSL

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Configurer Diagramme du réseau Accès à distance ASA avec OCSP AC Microsoft Windows 2012 Installation des services Configuration CA pour le modèle OCSP Certificat de service OCSP Nonces de service OCSP Configuration CA pour les extensions OCSP **OpenSSL** ASA avec plusieurs sources OCSP ASA avec OCSP signé par une autre autorité de certification Vérifier ASA - Obtenir un certificat via SCEP AnyConnect - Obtenir un certificat via la page Web Accès à distance VPN ASA avec validation OCSP Accès à distance VPN ASA avec plusieurs sources OCSP Accès à distance VPN ASA avec OCSP et certificat révogué Dépannage Serveur OCSP arrêté Heure non synchronisée Nonces signées non prises en charge Authentification du serveur IIS7 Informations connexes

Introduction

Ce document décrit comment utiliser la validation OCSP (Online Certificate Status Protocol) sur un dispositif de sécurité adaptatif Cisco (ASA) pour les certificats présentés par les utilisateurs VPN. Des exemples de configuration pour deux serveurs OCSP (Autorité de certification Microsoft Windows [CA] et OpenSSL) sont présentés. La section Vérifier décrit les flux détaillés au niveau des paquets et la section Dépannage se concentre sur les erreurs et les problèmes typiques.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de l'interface de ligne de commande (CLI) du dispositif de sécurité adaptatif Cisco et configuration VPN SSL (Secure Socket Layer)
- Certificats X.509
- Microsoft Windows Server
- Linux/OpenSSL

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco Adaptive Security Appliance, versions 8.4 et ultérieures
- Microsoft Windows 7 avec Cisco AnyConnect Secure Mobility Client, version 3.1
- Microsoft Server 2012 R2
- Linux avec OpenSSL 1.0.0j ou version ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Remarque : utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Le client utilise un VPN d'accès à distance. Il peut s'agir de Cisco VPN Client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange Version 2 [IKEv2]) ou WebVPN (portail). Afin de se connecter, le client fournit le certificat correct, ainsi que le nom d'utilisateur/mot de passe qui ont été configurés localement sur l'ASA. Le certificat client est validé via le serveur OCSP.



Accès à distance ASA avec OCSP

L'ASA est configuré pour l'accès SSL. Le client utilise AnyConnect afin de se connecter. L'ASA utilise le protocole SCEP (Simple Certificate Enrollment Protocol) afin de demander le certificat :

```
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

Un mappage de certificat est créé afin d'identifier tous les utilisateurs dont le nom de sujet contient le mot administrateur (insensible à la casse). Ces utilisateurs sont liés à un groupe de tunnels nommé 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
```

La configuration VPN nécessite une autorisation réussie (c'est-à-dire un certificat validé). Il nécessite également les informations d'identification correctes pour le nom d'utilisateur défini localement (authentication aaa) :

username cisco password xxxxxx ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0

```
aaa authorization LOCAL
group-policy MY internal
group-policy MY attributes
vpn-tunnel-protocol ikev1 ikev2 12tp-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
```

AC Microsoft Windows 2012

Remarque : reportez-vous au <u>Guide de configuration de la gamme Cisco ASA 5500 à l'aide</u> <u>de l'interface de ligne de commande, 8.4 et 8.6 : Configuration d'un serveur externe pour</u> <u>l'autorisation utilisateur d'appliance de sécurité</u> pour obtenir des détails sur la configuration de l'ASA via l'interface de ligne de commande.

Installation des services

Cette procédure décrit comment configurer les services de rôle pour le serveur Microsoft :

1. Accédez à Gestionnaire de serveur > Gestion > Ajouter des rôles et des fonctionnalités. Le serveur Microsoft a besoin des services de rôle suivants :

autorité de certificationInscription Web de l'autorité de certification, utilisée par le clientRépondeur en ligne, nécessaire pour OCSPNetwork Device Enrollment Service, qui contient l'application SCEP utilisée par ASA Un service Web avec des stratégies peut être ajouté si nécessaire.

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

- 3.
- 4. Lorsque vous ajoutez des fonctionnalités, veillez à inclure les outils de répondeur en ligne, car ils incluent un composant logiciel enfichable OCSP utilisé ultérieurement :

elect features		DESTINATION SERVER WIN-35QVH03PQE3.Jab.com
Before You Begin	Select one or more features to install on the selected server.	
Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Features Image: Role Administration Tools (12 of 28 installed) Image: Role Administration Tools (12 of 28 installed) Image: Role Administration Tools (14 of 5 installed) Image: Role Administration Tools (16 of 3 installed) Image: Role Administration Tools (16 of 3 installed) Image: Role Administration Tools (16 of 3 installed) Image: Role Administration Tools (10 of 3 installed) Image: Role Administration Authority Management Tools Image: Role Administration Authority Management Tools Image: Role Administration Authority Management Service Image: Role Administration Authority Rights Management Service Image: Role Administration Tools (Installed) Image: Role Administration Tools (Installed)	Description Online Responder Tools includes the Online Responder Management snap-in.

Configuration CA pour le modèle OCSP

Le service OCSP utilise un certificat pour signer la réponse. Un certificat spécial sur le serveur Microsoft doit être généré et doit inclure :

- Utilisation de la clé étendue = signature OCSP
- OCSP sans contrôle de révocation

Ce certificat est nécessaire afin d'empêcher les boucles de validation OCSP. ASA n'utilise pas le service OCSP pour essayer de vérifier le certificat présenté par le service OCSP.

 Ajoutez un modèle pour le certificat sur l'autorité de certification. Accédez à CA > Modèle de certificat > Gérer, sélectionnez Signature de réponse OCSP, et dupliquez le modèle. Affichez les propriétés du modèle nouvellement créé, puis cliquez sur l'onglet Sécurité. Les autorisations décrivent l'entité autorisée à demander un certificat qui utilise ce modèle. Des autorisations correctes sont donc requises. Dans cet exemple, l'entité est le service OCSP qui s'exécute sur le même hôte (TEST-CISCO\DC), et le service OCSP a besoin des privilèges d'inscription automatique :

2	Certific	ate Templates Cons	ole				- 1		x
File Action View Help									
🔶 🔿 📷 🖾 📷 👘									
Certificate Templates (DC.test-c	Template Display Name	Schema Verrion	Verri	Intended Ru	ni A detions				_
	Administrator	Pro	perties of New	Template	×	e T	empla	ates	
	Authenticated Session	Cubinat Name	Canuar	heuranne P	an immede	cti	ans		
	Basic EFS	Compatibility General	Request Handling	Cryptography	Key Attestation				
	CA Exchange	Superseded Templa	stes Ext	ensions	Security	pc	nse Si	igni	-
	Code Signing	Group or user names:				cti	ons		•
	Computer	& Authenticated Use	ars						
	Copy of OCSP Response Signing	Administrator							
	Cross Certification Authority	DC (TEST-CISCO)	DCS)						
	Directory Email Replication	St. Enterprise Admins	(TEST-CISCO\Domain (TEST-CISCO\Ente	n Aamins) rorise Admins)					
	Domain Controller			, ,					
	EFS Recovery Agent								
	Enrollment Agent								
	Enrollment Agent (Computer)		1	Add	Remove				
	Exchange Enrollment Agent (Offline	Permissions for DC		Allow	Deny				
	Exchange Signature Only	Full Control							
	Exchange User	Read		✓					
	IPSec (Offline requert)	Write							
	Reperos Authentication	Atoenmi			8 1				
	Key Recovery Agent	1000000		(11)	-				
	OCSP Response Signing								
	RAS and IAS Server	For special permissions	or advanced setting	s, click	Advanced				
	Root Certification Authority	Advanced.			- and to be				
	Kouter (Offline request) Smartcard Lenge								
	Smartcard User								
	Subordinate Certification Authority	OK	Cancel	Apply	Help				
	Trust List Signing	1	3.1		~				
< III >	< III				>				

Tous les autres paramètres du modèle peuvent être définis par défaut.

2. Activez le modèle. Accédez à CA > Modèle de certificat > Nouveau > Modèle de certificat à émettre, et sélectionnez le modèle dupliqué :



Certificat de service OCSP

Cette procédure décrit comment utiliser la gestion de la configuration en ligne afin de configurer OCSP :

- 1. Accédez à Gestionnaire de serveur > Outils.
- 2. Accédez à **Revocation Configuration > Add Revocation Configuration** afin d'ajouter une nouvelle configuration :

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
 	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	 Browse CA certificates published in Active Directory 	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 peut utiliser la même autorité de certification d'entreprise. Le certificat du service OCSP est généré.

3. Utilisez l'autorité de certification d'entreprise sélectionnée et choisissez le modèle créé précédemment. Le certificat est inscrit automatiquement :



4. Vérifiez que le certificat est inscrit et que son état est En cours/OK :



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. Accédez à CA > Issued Certificates afin de vérifier les détails du certificat :

File Action View Help Image: Second S			
← ⇒ 2			
Certification Authority (Local)	x		
Image: Second Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates Value Valid to Thursday, Oc Subject DC.test-cisco Public key RSA (2048 Bit) Certificate Templates Certificate Template Inform Tenhanced Key Usage OCSP Signing OCSP No Revocation Checking 05 00 Authority Key Identifier KeyID=9f 99 OCSP Signing (1.3.6.1.5.5.7.3.9) Edit Properties	Iate Iate <	Serial Number 24000000206c 240000003d86 2400000057d8 2400000057d8 24000000039b 24000000082d2 24000000098d 24000000099f 240000000cb0c 240000000cb0c 240000000cb0c 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 12:05 AM 10/10/2013 12:7 PM 10/10/2013 1:27 PM 10/10/2013 1:27 PM 10/10/2013 1:30 PM 10/10/2013 1:31 PM 10/10/2013 2:06 PM 10/10/2013 6:51 PM

Nonces de service OCSP

La mise en oeuvre Microsoft d'OCSP est conforme à la <u>RFC 5019 The Lightweight Online</u> <u>Certificate Status Protocol (OCSP) Profile for High-Volume Environments</u>, qui est une version simplifiée du <u>RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol</u> <u>- OCSP</u>.

L'ASA utilise RFC 2560 pour OCSP. L'une des différences entre les deux RFC est que le RFC 5019 n'accepte pas les requêtes signées envoyées par ASA.

Il est possible de forcer le service Microsoft OCSP à accepter ces demandes signées et à

répondre avec la réponse signée correcte. Accédez à **Revocation Configuration > RevocationConfiguration1 > Edit Properties**, et sélectionnez l'option pour **Enable NONCE extension support**.

File Action View Help			
se e la constante de la consta			
P Online Responder: DC.test-cisco.cc	Name	Signing Certificate Selec	Enrollment Template
Revocation Configuration	RevocationConfiguration1	Automatically enrolled	Copy 2 of OCSP Response S
▲ Prray Configuration DC.test-cisco.com	Properties for Revocation Configuration: Local CRL Revocation Provider Signing The selected hash algorithm is used by the Online Responses sent to clients. Hash algorithm: SHA1 Image: Do not prompt for credentials for cryptographic operation of the signing certificates. Image: Automatically use renewed signing certificates. Image: Do not prompt for Credentials for cryptographic operation operation of the signing certificates. Image: Do not prompt for Credentials for cryptographic operation operation of the signing certificates. Image: Do not prompt for Credentials for cryptographic operation operation operation of the signing certificate. Image: Do not prompt for Credentials for cryptographic operation operation of the signing certificate. Image: Do not prompt for Credentials for cryptographic operation of the signing certificate. Image: Do not prompt for Credentials for cryptographic operation of the signing certificate. Image: Do not prompt for Credentials for cryptographic operation of the signing certificate. Image: Do not prompt for Credentials for cryptographic operation of the signing certificate. Image: Do not prompt for Credentials for cryptographic operation of the signing certificate.	sponders to sign	
R	ОК Са	ncel Help	

Le service OCSP est maintenant prêt à être utilisé.

Bien que Cisco ne le recommande pas, les nonces peuvent être désactivés sur l'ASA :

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

Configuration CA pour les extensions OCSP

Vous devez maintenant reconfigurer l'autorité de certification pour inclure l'extension du serveur OCSP dans tous les certificats émis. L'URL de cette extension est utilisée par ASA afin de se connecter au serveur OCSP lorsqu'un certificat est validé.

- 1. Ouvrez la boîte de dialogue Propriétés du serveur sur l'autorité de certification.
- Cliquez sur l'onglet Extensions. L'extension AIA (Authority Information Access) qui pointe vers le service OCSP est nécessaire ; dans cet exemple, il s'agit de http://10.61.208.243/ocsp. Activez les deux options suivantes pour l'extension AIA :

Inclure dans l'extension AIA des certificats délivrésInclure dans l'extension OCSP (Online Certificate Status Protocol)

c لھ	test-cisco-DC-CA Properties ?						
File Action View Help 	Enrollment Agents General Extensions Select extension:	Auditing Policy Mo Storage	Recover	y Agents Exit Certificate N	Security Module lanagers		
 Revoked Certificates Issued Certificates Pending Requests Failed Requests 	Authority Information Access (AIA) Specify locations from which users can obtain the certificate for this CA.						
Certificate Templates	C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<caname: Idap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN=S http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce file://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce http://10.61.208.243/ocsp</ce </caname></serverdnsname></serverdnsname></ce </caname></serverdnsname></serverdnsname></catruncatedname></caname: </serverdnsname>						
	✓ Include in the AIA e ✓ Include in the onlin	extension of issu	ied certificate	es (OCSP) exter	nsion		

Cela garantit que tous les certificats émis ont un poste correct qui pointe vers le service OCSP.

OpenSSL

Remarque : reportez-vous au <u>Guide de configuration de la gamme Cisco ASA 5500 à l'aide</u> <u>de l'interface de ligne de commande, 8.4 et 8.6 : Configuration d'un serveur externe pour</u> <u>l'autorisation utilisateur d'appliance de sécurité</u> pour obtenir des détails sur la configuration de l'ASA via l'interface de ligne de commande.

Cet exemple suppose que le serveur OpenSSL est déjà configuré. Cette section décrit uniquement la configuration OCSP et les modifications nécessaires à la configuration de l'autorité de certification.

Cette procédure décrit comment générer le certificat OCSP :

1. Ces paramètres sont nécessaires pour le répondeur OCSP :

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

2. Ces paramètres sont nécessaires pour les certificats utilisateur :

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

- 3. Les certificats doivent être générés et signés par l'autorité de certification.
- 4. Démarrez le serveur OCSP :

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

5. Testez l'exemple de certificat :

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

D'autres exemples sont disponibles sur le site Web d'OpenSSL .

OpenSSL, comme ASA, prend en charge les nonces OCSP ; les nonces peuvent être contrôlés à l'aide des commutateurs -nonce et -no_nonce.

ASA avec plusieurs sources OCSP

ASA peut remplacer l'URL OCSP. Même si le certificat client contient une URL OCSP, il est remplacé par la configuration sur l'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/ocsp

L'adresse du serveur OCSP peut être définie explicitement. Cet exemple de commande fait correspondre tous les certificats avec l'administrateur dans le nom du sujet, utilise un point de confiance OPENSSL afin de valider la signature OCSP, et utilise l'URL de http://11.11.11.11/ocsp afin d'envoyer la requête :

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

L'ordre utilisé pour rechercher l'URL OCSP est le suivant :

- 1. Un serveur OCSP que vous définissez avec la commande match certificate
- 2. Un serveur OCSP que vous définissez avec la commande ocsp url
- 3. Serveur OCSP dans le champ AIA du certificat client

ASA avec OCSP signé par une autre autorité de certification

Une réponse OCSP peut être signée par une autre autorité de certification. Dans ce cas, il est nécessaire d'utiliser la commande **match certificate** afin d'utiliser un point de confiance différent sur la validation de certificat ASA pour OCSP.

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

Dans cet exemple, l'ASA utilise la réécriture de l'URL OCSP pour tous les certificats avec un nom de sujet qui contient « administrator ». L'ASA est forcé de valider le certificat du répondeur OCSP par rapport à un autre point de confiance, OPENSSL. Les certificats utilisateur sont toujours validés dans le point de confiance WIN2012.

Puisque le certificat du répondeur OCSP a l'extension « OCSP no revocation checking », le certificat n'est pas vérifié, même lorsque OCSP est forcé de se valider par rapport au point de confiance OPENSSL.

Par défaut, tous les points de confiance sont recherchés lorsque l'ASA tente de vérifier le certificat utilisateur. La validation du certificat du répondeur OCSP est différente. L'ASA recherche uniquement le point de confiance qui a déjà été trouvé pour le certificat utilisateur (WIN2012 dans cet exemple).

Par conséquent, il est nécessaire d'utiliser la commande **match certificate** afin de forcer l'ASA à utiliser un point de confiance différent pour la validation de certificat OCSP (OPENSSL dans cet exemple).

Les certificats utilisateur sont validés par rapport au premier point de confiance correspondant (WIN2012 dans cet exemple), qui détermine ensuite le point de confiance par défaut pour la validation du répondeur OCSP.

Si aucun point de confiance spécifique n'est fourni dans la commande **match certificate**, le certificat OCSP est validé par rapport au même point de confiance que les certificats utilisateur (WIN2012 dans cet exemple) :

```
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
```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Remarque : l'outil Output Interpreter Tool (clients enregistrés uniquement) prend en charge

certaines commandes **show**. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

ASA - Obtenir un certificat via SCEP

Cette procédure décrit comment obtenir le certificat via l'utilisation du SCEP :

1. Il s'agit du processus d'authentification du point de confiance pour obtenir le certificat CA :

```
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]:
yes
```

Trustpoint CA certificate accepted.

 Pour demander le certificat, l'ASA doit disposer d'un mot de passe SCEP à usage unique qui peut être obtenu à partir de la console d'administration à l'adresse http://IP/certsrv/mscep_admin:



3. Utilisez ce mot de passe pour demander le certificat sur l'ASA :

```
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
 password to the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the
configuration.
 Please make a note of it.
Password: **************
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
```

Certains résultats ont été omis pour plus de clarté.

4. Vérifiez les certificats CA et ASA :

```
BSNS-ASA5510-3(config) # show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 240000001cbf2fc89f44fe81970000000001c
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
```

L'ASA n'affiche pas la plupart des extensions de certificat. Bien que le certificat ASA contienne l'extension 'URL OCSP dans AIA', l'interface de ligne de commande ASA ne la présente pas. L'ID de bogue Cisco <u>CSCui44335</u>, « Extensions x509 du certificat ASA ENH affichées », demande cette amélioration.

AnyConnect - Obtenir un certificat via la page Web

Cette procédure décrit comment obtenir le certificat à l'aide du navigateur Web sur le client :

1. Un certificat utilisateur AnyConnect peut être demandé via la page Web. Sur le PC client, utilisez un navigateur Web pour accéder à l'autorité de certification à l'adresse http://*IP*/certsrv:



 Le certificat utilisateur peut être enregistré dans le magasin du navigateur Web, puis exporté vers le magasin Microsoft, dans lequel AnyConnect effectue une recherche. Utilisez certmgr.msc afin de vérifier le certificat reçu :



AnyConnect peut également demander le certificat tant qu'il existe un profil AnyConnect correct.

Accès à distance VPN ASA avec validation OCSP

Cette procédure décrit comment vérifier la validation OCSP :

 Lorsqu'il tente de se connecter, l'ASA signale que le certificat est vérifié pour OCSP. Ici, le certificat de signature OCSP a une extension sans vérification et n'a pas été vérifié via OCSP :

```
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.
```

Certains résultats ont été omis pour plus de clarté.

2. L'utilisateur final fournit les informations d'identification :

🔇 Cisco AnyConr	×		
Username:	cisco		
Password:			
	OK Cancel		
🕥 Cisco AnyCon	nect Secure Mobility Client		
	VPN: Contacting 10.48.67.229.		Grout
	10.48.67.229		Connect

3. La session VPN s'est terminée correctement :

%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: 24000001B2AD208B12811687400000000001B, 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. La session est créée :

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

 Username
 : cisco
 Index
 : 4

 Assigned IP
 : 192.168.11.100
 Public IP
 : 10.61.209.83
 Index Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Premium License 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 Bytes Rx : 32236 Pkts Rx : 209 Pkts Tx : 8 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 Encryption : RC4 Encapsulation: TLSv1.0 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle TO Left : 29 Minutes Idle Time Out: 30 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 Tx : 0 Pkts Tx : 0 Bytes Rx : 29664 Pkts Rx : 201

Pkts Rx Drop : 0

5. Vous pouvez utiliser des débogages détaillés pour la validation OCSP :

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

6. Au niveau de capture de paquets, il s'agit de la requête OCSP et de la réponse OCSP correcte. La réponse inclut la signature correcte - extension nonce activée sur Microsoft OCSP :

No.	Source	Destination	Protocol	Length	Info		
24	10.48.67.229	10.61.208.243	0CSP 545 Red		Request		
31	10.61.208.243	10.48.67.229	0CSP	700	Response		
4							
▶ Hy	Hypertext Transfer Protocol						
⊽ 0n	line Certificate Stat	tus Protocol					
1	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: Dissector for OID:1.3.6.1.5.5.7.48.1.2 not implemented.						
	signatureAlgorithm (shaWithRSAEncryption)						
	Padding: 0						
	signature: 353fc46	1732dc47b1d167ebace6	677a0877	65b48ed	b3b284c		
	⊳certs: 1 item						

Accès à distance VPN ASA avec plusieurs sources OCSP

Si un certificat de correspondance est configuré comme expliqué dans <u>ASA avec plusieurs</u> <u>sources OCSP</u>, il a priorité :

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

Lorsqu'un remplacement d'URL OCSP est utilisé, les débogages sont les suivants :

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

Accès à distance VPN ASA avec OCSP et certificat révoqué

Cette procédure décrit comment révoquer le certificat et confirmer l'état révoqué :

1. Révoquez le certificat client :

certsrv - [Certification Authority (Local)\test-cisco-DC-CA\Issued							
File Action View Help							
🗢 🔿 🙎 🗟 🗟							
🙀 Certification Authority (Local)	Request	ID	Requester	Na	ame	Binary Certificate	Certif
⊿ 🚽 test-cisco-DC-CA	-		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
Revoked Certificates	5 7		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
Issued Certificates	58 💭		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
Pending Requests	5 9		TEST-CISC	0	\Ad	BEGIN CERTI	User
Failed Requests	🔄 10		TEST-CISC	0	∖Ad	BEGIN CERTI	User
Certificate Templates	🔄 11		TEST-CISC	0	\Ad	BEGIN CERTI	User
	🔄 12		TEST-CISC	0	∖Ad	BEGIN CERTI	User
	🔄 13		TEST-CISC	0	∖Ad	BEGIN CERTI	User
	🔄 14		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
	🔄 18		TEST-CISC	0	\DC\$	BEGIN CERTI	Сору
	🔄 19		TEST-CISC	0	∖Ad	BEGIN CERTI	IPSec
	iii 20		TEST-CISC	0	∖Ad	BEGIN CERTI	IPSec
	l 🔄 21		TEST-CISC	0	∖Ad	BEGIN CERTI	User
	-	0			Ad	BEGIN CERTI	User
		Open		_	Ad	BEGIN CERTI	User
		All Ta	sks	۲		View Attributes/Extensi	ons
R		Refre	sh			Export Binary Data	
		Help				Revoke Certificate	
	28		TEST-CISC	0	∖Ad	BEGIN CERTI	IPSec
	<						
Contains actions that can be performed on the item.							

2. Publier les résultats :



3. [Facultatif] Les étapes 1 et 2 peuvent également être effectuées à l'aide de l'utilitaire de ligne de commande certutil dans Power Shell :

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

4. Lorsque le client tente de se connecter, il y a une erreur de validation de certificat :

Cisco AnyConnect	
Certificate Validation Failure	
ОК	
Scisco AnyConnect Secure Mobility Client	
VPN: No valid certificates available for 10.48.67.229	or authentication. → Connect
\$ (i)	athalis cisco

5. Les journaux AnyConnect indiquent également l'erreur de validation du certificat :

[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. L'ASA signale que le certificat est révoqué :

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: OCSP response received successfully.
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. Les captures de paquets affichent une réponse OCSP réussie avec l'état de certificat révoqué :

No.	Source	Destination	Protocol	Length	Info			
24	4 10.48.67.229	10.61.209.83	0CSP	544	Request			
3	1 10.61.209.83	10.48.67.229	0CSP	721	Response			
4								
⊳ Hy	Hypertext Transfer Protocol							
⊽ 0r	Online Certificate Status Protocol							
	responseStatus: successful (0)							
~	▼ responseBytes							
	ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)							
	✓ Basic0CSPResponse							
	✓ tbsResponseData							
	▷ responderID: byKey (2)							
	producedAt: 2013-10-13 10:47:02 (UTC)							
	⊽ responses: 1 item							
	▼ SingleResponse							
	⊳ certID							
▶ certStatus: revoked (1)								
thisUpdate: 2013-10-13 10:17:51 (UTC)								
nextUpdate: 2013-10-14 22:37:51 (UTC)								
▷ singleExtensions: 1 item								
responseExtensions: 1 item								
	signatureAlgorithm (shaWithRSAEncryption)							

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Serveur OCSP arrêté

```
ASA signale la panne du serveur OCSP :
```

CRYPTO_PKI: unable to find a valid OCSP server. CRYPTO PKI: OCSP revocation check has failed. Status: 1800. Les captures de paquets peuvent également faciliter le dépannage.

Heure non synchronisée

Si l'heure actuelle sur le serveur OCSP est plus ancienne que sur ASA (de petites différences sont acceptables), le serveur OCSP envoie une réponse non autorisée, et l'ASA la signale :

CRYPTO_PKI: OCSP response status - unauthorized Lorsque l'ASA reçoit une réponse OCSP de temps futurs, il échoue également.

Nonces signées non prises en charge

Si les nonces sur le serveur ne sont pas pris en charge (ce qui est la valeur par défaut sur Microsoft Windows 2012 R2), une réponse non autorisée est renvoyée :

No.	Source	Destination	Protocol	Length	Info		
- 56	5 10.48.67.229	10.61.208.243	0CSP	545	Request		
59	0 10.61.208.243	10.48.67.229	0CSP	337	Response		
4							
▶ Frame 59: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)							
Ethernet II, Src: Cisco_2a:c4:a3 (00:06:f6:2a:c4:a3), Dst: Cisco_b8:6b:25 (00:17:5)							
⊳ In	Internet Protocol Version 4, Src: 10.61.208.243 (10.61.208.243), Dst: 10.48.67.229						
⊳ Tr	Transmission Control Protocol, Src Port: http (80), Dst Port: 14489 (14489), Seq:						
Hypertext Transfer Protocol							
• Online Certificate Status Protocol							
responseStatus: unauthorized (6)							

Authentification du serveur IIS7

Les problèmes liés à une demande SCEP/OCSP sont souvent le résultat d'une authentification incorrecte sur Internet Information Services 7 (IIS7). Assurez-vous que l'accès anonyme est configuré :

File View Help								
Connections	Authentication							
 DC (TEST-CISCO\Administrat Application Pools Sites Opfault Web Site APolicyProvider_ ADPolicyProvider_ CertEnroll CertSrv CertSrv DomainHRA HCAP NonDomainHRA ocsp 	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					

Informations connexes

- Microsoft TechNet : Guide d'installation, de configuration et de dépannage du répondeur en ligne
- Microsoft TechNet : Configurer une autorité de certification pour prendre en charge les répondeurs OCSP
- <u>Référence des commandes de la gamme Cisco ASA</u>
- <u>Technical Support & Documentation Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.