ق م ASA دعب نع لوصولل VPN ةكبش و OCSP بجومب Microsoft Windows 2012 نم OpenSSL

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة التكوين الرسم التخطيطي للشبكة الوصول عن بعد إلى ASA باستخدام OCSP نظام التشغيل Microsoft Windows 2012 CA تثبيت الخدمات تكوين CA لقالب OCSP شهادة خدمة OCSP <u>حالات عدم اتصال خدمة OCSP</u> تكوين CA لملحقات OCSP **OpenSSL** ASA مع مصادر OCSP متعددة ASA مع OCSP موقع من قبل CA مختلف التحقق من الصحة ASA - الحصول على الشهادة عبر SCEP AnyConnect - الحصول على شهادة عبر صفحة الويب <u>الوصول عن بعد إلى ASA VPN مع التحقق من OCSP</u> الوصول عن بعد إلى ASA VPN مع مصادر OCSP متعددة الوصول عن بعد إلى ASA VPN مع OCSP والشهادة الملغاة استكشاف الأخطاء وإصلاحها خادم OCSP معطل الوقت غير متزامن لا يتم دعم نقاط الاتصال الموقعة مصادقة خادم IIS7 معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية إستخدام التحقق من صحة بروتوكول حالة الشهادة عبر الإنترنت (OCSP) على جهاز الأمان القابل للتكيف (ASA) من Cisco للشهادات المقدمة من قبل مستخدمي شبكة VPN. يتم تقديم مثال لتكوينات خادمي OCSP (المرجع المصدق ل Microsoft Windows [CA] و OpenSSL). يصف قسم التحقق التدفقات التفصيلية على مستوى الحزمة، ويركز قسم أستكشاف الأخطاء وإصلاحها على الأخطاء والمشاكل النموذجية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين واجهة سطر الأوامر (CLI) الخاصة بجهاز الأمان القابل للتكيف (SSL) من Cisco وتكوين طبقة مأخذ التوصيل الآمنة (VPN (SSL
 - شهادات X.509
 - نظام التشغيل Microsoft Windows Server
 - Linux/OpenSSL •

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance، الإصدار 8.4 والإصدارات الأحدث
 - Microsoft Windows 7 مع Cisco AnyConnect Secure Mobility Client، الإصدار 3.1،
 - نظام التشغيل Microsoft Server 2012 R2
 - Linux مع OpenSSL 1.0.0j أو إصدار أحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم العميل شبكة VPN للوصول عن بعد. يمكن أن يكون هذا الوصول هو Cisco VPN Client (IPSec) أو WebVPN الإصدار Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange الإصدار [IKEv2]] أو WebVPN) portal)). لتسجيل الدخول، يوفر العميل الشهادة الصحيحة، بالإضافة إلى اسم المستخدم/كلمة المرور التي تم تكوينها محليا على ASA. يتم التحقق من شهادة العميل عبر خادم OCSP.



الوصول عن بعد إلى ASA باستخدام OCSP

تم تكوين ASA للوصول إلى SSL. يستخدم العميل AnyConnect لتسجيل الدخول. يستخدم ASA بروتوكول تسجيل الشهادة البسيط (SCEP) لطلب الشهادة:

```
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
guina خريطة شهادات لتحديد كافة المستخدمين الذين يحتوي اسم الموضوع الخاص بهم على كلمة مسؤول (غير
حساس لحالة الأحرف). هؤلاء المستخدمون موحدون بمجموعة أنفاق تحمل اسم AL
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable
tunnel-group-list enable
certificate-group-map MAP 10 RA
zirduب تكوين الشبكة الخاصة الظاهرية (VPN) تفويضا ناجحا (أي شهادة تم التحقق من صحتها). كما يتطلب بيانات
الاعتماد الصحيحة لاسم المستخدم المحدد محليا (المصادقة والتفويض والمحاسبة (AAA)):
```

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

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

نظام التشغيل Microsoft Windows 2012 CA

ملاحظة: راجع <u>دليل تكوين السلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6: تكوين خادم خارجي</u> <u>لتفويض مستخدم جهاز الأمان</u> للحصول على تفاصيل حول تكوين ASA من خلال CLI (واجهة سطر الأوامر).

تثبيت الخدمات

يوضح هذا الإجراء كيفية تكوين خدمات الأدوار لخادم Microsoft:

انتقل إلى **مدير الخادم > إدارة > إضافة أدوار وميزات**. يحتاج خادم Microsoft إلى خدمات الأدوار التالية: 1.

هيئة الشهاداتتسجيل ويب ل Certificate Authority الذي يستخدمه العميلOnline Responder، المطلوب ل OCSPخدمة تسجيل جهاز الشبكة، والتي تحتوي على تطبيق SCEP المستخدم من قبل ASA يمكن إضافة خدمة ويب ذات النهج إذا لزم الأمر.

a	AD CS Configuration	_ _ ×
Role Services		DESTINATION SERVER WIN-35QVH03PQE3.lab.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Authentication Type for C Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	
.2	More about AD CS Server Roles <pre></pre>	Configure Cancel

عندما تقوم بإضافة ميزات، تأكد من تضمين "أدوات المستجيب عبر الإنترنت" لأنها تتضمن أداة OCSP إضاف*ي*ة يتم إستخدامها لاحقا:

ña -	Add Roles and Features Wizard	_ D X
Select features	DEST WIN-35QVI	INATION SERVER H03PQE3.lab.com
Before You Begin Installation Type	Select one or more features to install on the selected server. Features Description	
Server Selection Server Roles Features AD CS Role Services Confirmation Results	 Conline Responder Tools Conline Responder Tools AD DS and AD LDS Tools (4 of 5 installed) Hyper-V Management Tools Remote Desktop Services Tools (1 of 3 instriction) Windows Server Update Services Tools Active Directory Certificate Services Tools Certification Authority Management Tools Certification Authority Management Service Active Directory Rights Management Service DHCP Server Tools (Installed) 	ols includes the nagement
	ONS Server Tools (Installed) Fax Server Tools File Services Tools Network Policy and Access Services Tools (V <	Cancel

تكوين CA لقالب OCSP

تستخدم خدمة OCSP شهادة لتوقيع إستجابة OCSP. يجب إنشاء شهادة خاصة على خادم Microsoft ويجب أن تتضمن:

- إستخدام المفتاح الموسع = توقيع OCSP
 - OCSP لا تدقيق إبطال

هذه الشهادة مطلوبة لمنع حلقات التحقق من صحة OCSP. لا يستخدم ASA خدمة OCSP لمحاولة التحقق من الشهادة المقدمة من خدمة OCSP.

إضافة قالب للشهادة على المرجع المصدق. انتقل إلى CA > قالب الشهادة > إدارة، حدد توقيع إستجابة 1. OCSP، وقم بمضاعفة القالب. قم بعرض خصائص القالب الذي تم إنشاؤه حديثا، وانقر فوق علامة التبويب أمان. تصف الأذونات الكيان المسموح له بطلب شهادة تستخدم هذا القالب، لذلك يلزم توفر أذونات صحيحة. في هذا المثال، الكيان هو خدمة OCSP التي يتم تشغيلها على المضيف نفسه (DC/DC) الكيان متوارت التعاري خدمة OCSP إلى امتيازات التسجيل التلقائي:

Ø	Certifi	cate Templates Cons	ole				- 0	x
File Action View Help								
File Action View Help	Template Display Name Administrator Authenticated Session Basic EFS CA Exchange CEP Encryption Code Signing Computer Copy of OCSP Response Signing Cross Certification Authority Directory Email Replication Domain Controller Domain Controller Domain Controller Domain Controller Domain Controller Domain Controller Domain Controller Ers Recovery Agent Enrollment Agent Enrollment Agent Exchange Enrollment Agent (Offline Exchange Signature Only Exchange User IPSec IPSec IPSec IPSec IPSec COSP Response Signing RAS and IAS Server Root Certification Authority Smattcard User Signatured User	Schama Varcino Prop Subject Name Compatibility General Superseded Templa Group or user names: Administrator DC (TEST-CISCO DD (TEST-CISCO DD (TEST-CISCO DD (TEST-CISCO DD (TEST-CISCO DC	Varzi Derties of New Server Request Handling tes Est rs DC\$) EST-CISCO\Domain (TEST-CISCO\Ente	Intended Ru Template Issuance R Cryptography ensions n Admins) prise Admins) Add Allow S, click	Remove Deny	e Ter ctions ctions	nplat ; ;	es ▲
< III >	Trust List Signing	1	3.1		>			

يمكن تعيين كافة الإعدادات الأخرى للقالب إلى الإعداد الافتراضي.

قم بتنشيط القالب. انتقل إلى **CA > قالب الشهادة > جديد > قالب الشهادة المراد إصداره**، ثم حدد القالب 2. المكرر:



شهادة خدمة OCSP

يصف هذا الإجراء كيفية إستخدام إدارة التكوين عبر الإنترنت من أجل تكوين OCSP:

انتقل إلى **مدير الخادم > الأدوات**.

انتقل إلى **تكوين الإبطال > إضافة تكوين الإبطال** لإضافة تكوين جديد:

.1

.2



يمكن ل OCSP إستخدام المرجع المصدق للمؤسسة نفسه. يتم إنشاء شهادة خدمة OCSP.

أستخدم المرجع المصدق للمؤسسة المحدد، واختر القالب الذي تم إنشاؤه مسبقا. تم تسجيل الشهادة تلقائيا: 3.

9		ocsp - [Online Responder: DC.test-cisco.com]
File Action	View Help	
🗢 🔿 🛛 🛛		
 Online Response 	onder: DC.test-cisco.cc on Configuration nfiguration	Online Responder Configuration Use this snap-in to configure and manage one or more certificate revocation responders.
		Add Revocation Configuration ? X
	Select Signi	ing Certificate
	Getting started with addi Name the Revocation Co Select CA Certificate Loca	Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.
	Choose CA Certificate	Automatically select a signing certificate
	Select Signing Certificate	Catification authority DC test sizes care/best sizes DC CA
	Revocation Provider	Browse
		Certificate Template: Copy 2 of OCSP Response Signing V
		 Manually select a signing certificate Note: You will need to specify a signing certificate for each member in the Online Responder Array. Use the CA certificate for the revocation configuration
	R	< Previous Next > Finish Cancel

.4

تأكد من تسجيل الشهادة ومن أن حالتها تعمل/موافق:





5. انتقل إلى CA > الشهادات الصادرة</mark> للتحقق من تفاصيل الشهادة:

i	certsrv - [Certification Authority (Local)\test-cisco-D	C-CA\I	ssued Certificat	es]
File Action View Help				
🗢 🔿 🙎 🙆 📓	Certificate X			
Certification Authority (Local) Certification Authority (Local) Certificates Service Certificates Service Certificates Service Certificates Service Certificates Certificate Templates Certificate Templates	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 Signing (1.3.6.1.5.5.7.3 @ Application/Policies [1]Application Certificate Polic @ OCSP No Revocation Checking 05 00 @ Authority Key Identifier KeyID=9f 99 7f b2 3b 61 90 0 v OCSP Signing (1.3.6.1.5.5.7.3.9) Edit Properties Copy to File OK</all>	late ler (ment (CEP ques ques ques ques	Serial Number 24000000206c 240000003d86 2400000057d8 2400000057d8 24000000057d8 24000000082d2 24000000082d2 24000000098d 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 10/11/2013 12:12 AM 10/10/2013 12:7 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 10/10/2013 2:06 PM 10/10/2013 6:51 PM

حالات عدم اتصال خدمة OCSP

يتوافق تنفيذ Microsoft ل OCSP مع <u>RFC 5019 ملف تعريف بروتوكول حالة الشهادة عبر الإنترنت (OCSP) خفيف</u> <u>الوزن للبيئات كبيرة الحجم</u>، وهو إصدار مبسط من <u>بروتوكول حالة الشهادة عبر الإنترنت الخاص ب RFC 2560 X.509 . Internet Key Public Infrastructure Certificate Protocol .</u>

يستخدم ASA RFC 2560 ل OCSP. أحد الفروق في شبكتي RFC هو أن RFC 5019 لا يقبل الطلبات الموقعة التي تم إرسالها من قبل ASA.

من الممكن إجبار خدمة OCSP ل Microsoft على قبول هذه الطلبات الموقعة والرد باستخدام الاستجابة الصحيحة الموقعة. انتقل إلى **تكوين الإبطال>RevocationConfiguration1>تحرير الخصائص**، وحدد الخيار **لتمكين دعم**

File Action View Help			
🧢 🔿 🖄 🗟			
Online Responder: DC.test-cisco.cc	Name	Signing Certificate Selec Automatically enrolled	Enrollment Template
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 o	anyptographic operations	
	Enable NONCE extension support	t	
	Use any valid OCSP signing certif	icate	
	Online Responder Identifiers All responses will include the follow	ing Online Responder identifier:	
	Key hash of the signing certification	ate	
	 Subject of the signing certificate 	e	
2			
	0	K Cancel Help	

خدمة OCSP جاهزة الآن للاستخدام.

على الرغم من أن Cisco لا توصي بهذا، يمكن تعطيل الاتصالات على ASA:

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

تكوين CA لملحقات OCSP

أنت ينبغي الآن reconfigure ال CA أن يتضمن ال OCSP نادل ملحق في كل شهادة صدرت. يتم إستخدام عنوان URL من هذا الملحق من قبل ASA للاتصال بخادم OCSP عند التحقق من صحة شهادة.

افتح مربع الحوار "خصائص" للخادم الموجود على المرجع المصدق.

- .1
- 2. انقر فوق علامة التبويب **الملحقات**. هناك حاجة إلى توسيع Authority Information Access (AIA) الذي يشير إلى خدمة OCSP، وهو في هذا المثال http://10.61.208.243/ocsp. مكنت كلا من هذا خيار ل ال AIA ملحق:

تضمين ملحق AIA للشهادات الصادرةتضمين في ملحق بروتوكول حالة الشهادة عبر الإنترنت (OCSP)

م ا	tes	test-cisco-DC-CA Properties ? X						
Image: Second system C File Action View Help Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system </td <td>tes Enrollment Agents General Extensions Select extension: Authority Information / Specify locations from C:\Windows\system3 Idap:///CN=<catrun http://<serverdnsn;< td=""><td colspan="5">test-cisco-DC-CA Properties ? × Enrollment Agents Auditing Recovery Agents Security General Policy Module Exit Module Extensions Storage Certificate Managers Select extension: </td></serverdnsn;<></catrun </td>	tes Enrollment Agents General Extensions Select extension: Authority Information / Specify locations from C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsn;< td=""><td colspan="5">test-cisco-DC-CA Properties ? × Enrollment Agents Auditing Recovery Agents Security General Policy Module Exit Module Extensions Storage Certificate Managers Select extension: </td></serverdnsn;<></catrun 	test-cisco-DC-CA Properties ? × Enrollment Agents Auditing Recovery Agents Security General Policy Module Exit Module Extensions Storage Certificate Managers Select extension:						
₽	Idap:///CN= <catrun http://<serverdnsna file://<serverdnsna http://10.61.208.243 < Ⅲ Include in the AIA of Include in the online</serverdnsna </serverdnsna </catrun 	extension of issue	I=AIA,CN=P(/ <serverdns ServerDNS Add</serverdns 	ublic Key Se SName>_ <c Name>_<ca d</ca </c 	nvices,CN=S aName> <ce Name><cer< th=""></cer<></ce 			

وهذا يضمن أن جميع الشهادات الصادرة لها ملحق صحيح يشير إلى خدمة OCSP.

OpenSSL

ملاحظة: راجع <u>دليل تكوين السلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6: تكوين خادم خارجي</u> <u>لتفويض مستخدم جهاز الأمان</u> للحصول على تفاصيل حول تكوين ASA من خلال CLI (واجهة سطر الأوامر).

يفترض هذا المثال أن خادم OpenSSL تم تكوينه بالفعل. يصف هذا القسم تكوين OCSP والتغييرات اللازمة لتكوين CA فقط.

يوضح هذا الإجراء كيفية إنشاء شهادة OCSP:

1. هذه المعلمات مطلوبة لمستجيب OCSP:

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

2. هذه المعلمات مطلوبة لشهادات المستخدم:

```
UserCerts ]
authorityInfoAccess = OCSP;URI:http://10.61.208.243
3. يجب إنشاء الشهادات وتوقيعها من قبل المرجع المصدق.
```

4. بدء تشغيل خادم OCSP:

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

5. إختبار نموذج الشهادة:

```
openssl ocsp -CAfile cacert.crt -issuer cacert.crt -cert example-cert.crt
url http://10.61.208.243 -resp_text-
يتوفر المزيد من الأمثلة على <u>موقع OpenSSL على الوب</u> .
```

يدعم OpenSSL، مثل ASA، طرق OCSP، ويمكن التحكم في المنافذ باستخدام محولات -nonce و-nonce.

ASA مع مصادر OCSP متعددة

يمكن أن يتجاوز ASA عنوان OCSP URL. حتى إذا كانت شهادة العميل تحتوي على عنوان OCSP URL، فإنه تتم الكتابة فوقها بواسطة التكوين الموجود على 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
يمكن تعريف عنوان خادم OCSP بشكل صريح. يتطابق مثال الأمر هذا مع كل الشهادات مع المسؤول في اسم
الموضوع، ويستخدم لاللال العلب:
http://11.11.11/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 الترتيب المستخدم للبحث عن OCSP URL هو:

شرييب المستحدم شبخت عن ١٠٢٠ ١٥٥٥ هو.

- 1. خادم OCSP الذي قمت بضبطه باستخدام الأمر **مطابقة الشهادة**
 - 2. خادم OCSP الذي قمت بضبطه باستخدام الأمر ocsp url
 - 3. خادم OCSP في حقل AIA لشهادة العميل

ASA مع OCSP موقع من قبل CA مختلف

يمكن توقيع إستجابة OCSP من قبل مرجع مصدق مختلف. في مثل هذه الحالة، من الضروري إستخدام الأمر **match certificate** لاستخدام نقطة ثقة مختلفة على ASA للتحقق من شهادة 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

في هذا المثال، يستخدم ASA إعادة كتابة عنوان OCSP URL لجميع الشهادات ذات اسم الموضوع الذي يحتوي على المسؤول. يتم فرض ASA على التحقق من صحة شهادة المستجيب OCSP مقابل نقطة ثقة أخرى، OpenSSL. لا تزال شهادات المستخدم معتمدة في Win2012 TrustPoint.

بما أن شهادة المستجيب OCSP تحتوي على الملحق 'OCSP no revocation check'، فلا يتم التحقق من الشهادة، حتى عندما يتم فرض التحقق من صحة OCSP مقابل OpenSSL TrustPoint.

بشكل افتراضي، يتم البحث في جميع نقاط الثقة عندما يحاول ASA التحقق من شهادة المستخدم. التحقق من صحة شهادة المستجيب OCSP مختلف. يبحث ASA فقط في TrustPoint التي تم العثور عليها بالفعل لشهادة المستخدم (WIN2012 في هذا المثال).

وبالتالي، من الضروري إستخدام الأمر **match certificate** لإجبار ASA على إستخدام نقطة ثقة مختلفة للتحقق من شهادة OCSP (OpenSSL في هذا المثال).

يتم التحقق من صحة شهادات المستخدم مقابل أول TrustPoint (WIN2012 في هذا المثال)، والذي يحدد بعد ذلك النقطة الموثوق بها الافتراضية للتحقق من إستجابة OCSP.

إذا لم يتم توفير أي نقطة ثقة محددة في الأمر match certificate، يتم التحقق من صحة شهادة OCSP مقابل نفس نقطة الثقة مثل شهادات المستخدم (WIN2012 في هذا المثال).:

```
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://11.11.11.0csp
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ملاحظة: <u>تدعم أداة مترجم الإخراج</u> (<u>العملاء المسجلون</u> فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر show.

ASA - الحصول على الشهادة عبر SCEP

يوضح هذا الإجراء كيفية الحصول على الشهادة من خلال إستخدام SCEP:

1. هذه هي عملية مصادقة TrustPoint للحصول على شهادة 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 eled3f4c 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

من أجل طلب الشهادة، يحتاج ASA إلى وجود كلمة مرور SCEP مرة واحدة يمكن الحصول عليها من وحدة 2. تحكم المسؤول على http://IP/certsrv/mscep_admin:



3. استعملت أن كلمة أن يطلب الشهادة على ال ASA:

```
BSNS-ASA5510-3(config)# crypto ca enroll WIN2012
                                      .. 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 **certList caded** cert.

4. دققت على حد سواء ال CA و ASA شهادة:

```
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
                                           ,ldap:///CN=test-cisco-DC-CA,CN=DC,CN=CDP [1]
                                    ,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
                                                         date: 11:02:36 CEST Oct 13 2015
                                                    end
                                                            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
لا يعرض ASA معظم ملحقات الشهادة. على الرغم من أن شهادة ASA تحتوي على URL 'OCSP في امتداد
    AIA'، إلا أن ASA CLI لا يقدمها. يتطلب معرف تصحيح الأخطاء من ASA ENH'، إلا أن ASA CLI'، إلا أن
```

Certificate x509 Extensions المعروض" هذا التحسين.

AnyConnect - الحصول على شهادة عبر صفحة الويب

يوضح هذا الإجراء كيفية الحصول على الشهادة من خلال إستخدام مستعرض الويب على العميل:

يمكن طلب شهادة مستخدم AnyConnect من خلال صفحة الويب. على جهاز الكمبيوتر العميل، أستخدم 1. مستعرض ويب للانتقال إلى المرجع المصدق على http://*IP*/CERTSRV:



2. يمكن حفظ شهادة المستخدم في مخزن مستعرض الويب، ثم تصديرها إلى مخزن Microsoft، والذي يتم البحث فيه بواسطة AnyConnect. أستخدم certmgr.msc للتحقق من الشهادة المستلمة:

🚡 certmgr - [Certificates - Current User\Personal\Certificates]		
File Action View Help	Certificate	×
Certificates - Current User Certificates Certificates Trusted Root Certification Au	General Details Certification Path Show: <all></all>	
 Enterprise Trust Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certificatior Trusted People Other People 	Image Value Image Value Image CRL Distribution Points Image Cartificate Template Name Image Certificate Template Name Image Certificate Template Name Image Encrypting File System (1.3.6) Image Subject Alternative Name Image Other Name:Principal Name = A Image SMIME Capabilities Image Digital Signature, Key Encipher Image Thumborint algorithm Image Shall	н н
Certificate Enrollment Reque: Smart Card Trusted Roots	URL=Idap:///CN=test-cisco-DC-CA,CN=AIA,CN=Public% 20Key%20Services,CN=Services,CN=Configuration,DC=test- cisco,DC=com?cACertificate?base?objectClass=certificationAuthority [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://10.61.208.243/ocsp	* III +

كما يمكن ل AnyConnect طلب الشهادة طالما كان هناك توصيف AnyConnect صحيح.

الوصول عن بعد إلى ASA VPN مع التحقق من OCSP

يصف هذا الإجراء كيفية التحقق من صحة OCSP:

بينما تحاول الاتصال، يبلغ ASA أنه يتم التحقق من الشهادة ل OCSP. هنا، تحتوي شهادة توقيع OCSP علـ1. ملحق بدون فحص ولم يتم فحصها عبر OCSP:

> debug crypto ca debug crypto ca messages debug crypto ca transaction :ASA-6-725001: Starting SSL handshake with client outside% .for TLSv1 session 10.61.209.83/51262 .(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% to identity:10.48.67.229/35751 (10.61.209.83/80) 10.61.209.83/80 (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 تم حذف بعض المخرجات من أجل الوضوح.

> > يقدم المستخدم النهائي مسوغات المستخدم:

🕙 Cisco AnyConr	×		
Username:	cisco		
Password:			
	OK Cancel		
Sisco AnyCon	nect Secure Mobility Client		
	VPN: Contacting 10.48.67.229. 10.48.67.229	.	Connect

3. انتهت جلسة VPN بشكل صحيح:

: AnyConnect Premium

DTLS-Tunnel: (1)AES128

```
ASA-7-717036: Looking for a tunnel group match based on certificate maps*
                                  :for peer certificate with serial number
   ,240000001B2AD208B1281168740000000001B, 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: 240000001B2AD208B1281168740000000001B
             ,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. خلقت الحلسة:
              BSNS-ASA5510-3(config) # show vpn-sessiondb detail anyconnect
                                         Session Type: AnyConnect Detailed
                                : cisco
                    Username
                                                          Index
                                                                      : 4
         Assigned IP : 192.168.11.100
                                              Public IP
                                                          : 10.61.209.83
                   Protocol
                            : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

License

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Rx : 32236 Bytes Tx : 10540 Pkts Tx : 8 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 Duration : 0h:01m:05s 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 Pkts Rx : 1 : 4 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 Encryption : RC4 Hashing : SHA1 TCP Src Port : 51406 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 Pkts Rx : 10 : 4 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 UDP Src Port : 58053 Encryption : AES128 Encapsulation: DTLSv1.0 UDP Dst Port : 443 Auth Mode : Certificate and 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 Bytes Rx : 29664 Pkts Rx : 201 Pkts Tx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 5. يمكنك إستخدام تصحيح الأخطاء التفصيلي للتحقق من OCSP: :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

:240000001221CFA239477CE1C00000000012, 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

في مستوى التقاط الحزمة، هذا هو طلب OCSP واستجابة OCSP الصحيحة. تتضمن الاستجابة التوقيع 6. الصحيح - تم تمكين الملحق مرة واحدة على 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			
4								
▶ Hvi	pertext Transfer Prot	tocol						
	<pre> Online Certificate Status Protocol </pre>							
r	esponseStatus: succe	ssful (0)						
⊽ r	esponseBytes							
	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						
	▼ Extension							
	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							

الوصول عن بعد إلى ASA VPN مع مصادر OCSP متعددة

إذا تم تكوين شهادة مطابقة كما هو موضح في <u>ASA مع مصادر OCSP متعددة</u>، فإنها تأخذ الأسبقية:

```
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

aic jurice in the constant of the constan
```

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

الوصول عن بعد إلى ASA VPN مع OCSP والشهادة الملغاة

يوضح هذا الإجراء كيفية إبطال الشهادة وتأكيد الحالة الملغاة:

إبطال شهادة العميل:

🧔 certsrv - [Cer	tificatior	n Aut	hority	/ (Loc	al)\te	est-cisco-DC-CA\ls	sued
File Action View Help							
🗢 🔿 🙍 🗟							
🙀 Certification Authority (Local)	Request	ID	Reque	ester N	ame	Binary Certificate	Certif
⊿ 🚽 test-cisco-DC-CA	5 6		TEST-	CISCO	\Ad	BEGIN CERTI	IPSec
Revoked Certificates	5 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
	III 21		TEST-	CISCO	\Ad	BEGIN CERTI	User
		0			Ad	BEGIN CERTI	User
		Oper	1		Ad	BEGIN CERTI	User
		All Ta	asks	•		View Attributes/Extensi	ons
R		Refre	sh			Export Binary Data	
		Help				Revoke Certificate	
	28		TEST-	cisco	\Ad	BEGIN CERTI	IPSec
	<		III				

Contains actions that can be performed on the item.

.2

نشر النتائج:

違 ce	rtsrv - [Certi	ification Aut	hority (Local)\test	t-cisco-DC-CA\Revoked	Certificates]	
File Action View	Help					
(* •) 2 🖾 Q	🔒 🛛					
🙀 Certification Author	rity (Local)	Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester
test-cisco-DC-CA Revoked Certificates		27	10/13/2013 12:21	10/13/2013 12:21 PM	Unspecified	TEST-CISC
Issued Cer	All Tasks	•	Publish			
Pending R	View	•				
Certificate	Refresh					
	Export Lis	t				
	Properties	5				
	Help					

3. [إختياري] يمكن أيضا تنفيذ الخطوات 1 و 2 باستخدام الأداة المساعدة لواجهة سطر الأوامر (CLI) الرئيسية في Power Shell: c:\certutil -crl CertUtil: -CRL command completed succesfully. عندما يحاول العميل الاتصال، يوجد خطأ في التحقق من صحة الشهادة:

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

5. تشير سجلات AnyConnect أيضا إلى خطأ التحقق من صحة الشهادة:

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

6. يبلغ ASA عن إبطال حالة الشهادة:

CRYPTO_PKI: Starting OCSP revocation .CRYPTO_PKI: OCSP response received successfully :CRYPTO_PKI: OCSP found in-band certificate: serial number :24000001221CFA239477CE1C00000000012, 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: 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. تظهر حزم الالتقاط إستجابة OCSP ناجحة بحالة الشهادة لإبطال:

No.	Source	Destination	Protocol	Length	Info		
24	10.48.67.229	10.61.209.83	OCSP	544	Request		
31	10.61.209.83	10.48.67.229	0CSP	721	Response		
4	101011200100	101101071220	0001	722	neoponoe		
b Hv	nortoxt Transfor Prot	tocol					
v IIV	nypertext fransfer Frotocot						
	On the certificate status protocot						
		SSIUL (0)					
× I	esponseby les		dal adadas				
	ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)						
~	BasicOCSPResponse						
	✓ tbsResponseData						
	▷ responderID: byKey (2)						
	producedAt: 2013-10-13 10:47:02 (UTC)						
	▼ responses: 1 item						
	▷ certID						
	CertStatus: r	evoked (1)					
	thisUpdate: 2	013-10-13 10:17:51 (UTC)				
nextUpdate: 2013-10-14 22:37:51 (UTC)							
▷ singleExtensions: 1 item							
<pre>> responseExtensions: 1 item</pre>							
	▹ signatureAlgorithm	(shaWithRSAEncrypt	ion)				

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

خادم OCSP معطل

تقرير ASA عند تعطل خادم OCSP:

CRYPTO_PKI: **unable to find a valid OCSP server**. CRYPTO PKI: OCSP revocation check has failed. **Status: 1800**. يمكن أن تساعد عمليات التقاط الحزم أيضا في أستكشاف الأخطاء وإصلاحها.

الوقت غير متزامن

إذا كان الوقت الحالي على خادم OCSP أقدم من الوقت على ASA (الفوارق الصغيرة مقبولة)، يرسل خادم OCSP إستجابة غير مصرح بها، ويبلغ ASA عنها:

> CRYPTO_PKI: OCSP response status - unauthorized عندما يتلقى ASA إستجابة OCSP من أوقات المستقبل، فإنه يفشل أيضا.

لا يتم دعم نقاط الاتصال الموقعة

إذا لم يتم دعم عمليات عدم الاتصال على الخادم (وهو الإعداد الافتراضي على نظام التشغيل Microsoft Windows 2012 R2)، يتم إرجاع إستجابة غير معتمدة:

No.	Source	Destination	Protocol	Length	Info		
- 56	0.48.67.229	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: Cisc	_2a:c4:a3 (00:06:f6	:2a:c4:a	3), Dst	:: Cisco_b8:6b:25 (00:17:5		
▶ In	ternet Protocol Vers	ion 4, Src: 10.61.20	8.243 (1	0.61.20	8.243), Dst: 10.48.67.229		
⊳ Tr	ansmission Control P	rotocol, Src Port: h	ttp (80)	, Dst P	ort: 14489 (14489), Seq:		
▶ Hy	Hypertext Transfer Protocol						
▼ 0n	line Certificate Sta	tus Protocol					
	responseStatus: unaut	horized (6)					

مصادقة خادم IIS7

غالبا ما تكون المشاكل المتعلقة بطلب SCEP/OCSP ناتجة عن مصادقة غير صحيحة على Internet Information Services 7 (IIS7). تأكد من تكوين الوصول المجهول:

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

معلومات ذات صلة

- Microsoft TechNet: دليل تثبيت Online Responder وتكوينه واستكشاف الأخطاء وإصلاحها
 - Microsoft TechNet: تكوين مرجع مصدق لدعم مستجيبي OCSP
 - مرجع أوامر سلسلة ASA من <u>Cisco</u>
 - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما