Microsoft Windows 2012和OpenSSL下帶 OCSP驗證的ASA遠端訪問VPN

目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 帶OCSP的ASA遠端訪問 Microsoft Windows 2012 CA 服務安裝 OCSP的CA配置模板 OCSP服務證書 OCSP服務節點 OCSP擴展的CA配置 **OpenSSL** 具有多個OCSP源的ASA 具有由不同CA簽名的OCSP的ASA 驗證 ASA — 通過SCEP獲取證書 AnyConnect — 通過網頁獲取證書 帶OCSP的ASA VPN遠端訪問驗證 具有多個OCSP源的ASA VPN遠端訪問 具有OCSP和已撤銷證書的ASA VPN遠端訪問 疑難排解 OCSP伺服器關閉 時間不同步 不支援簽名的Nonces IIS7伺服器身份驗證 相關資訊

簡介

本文檔介紹如何在Cisco Adaptive Security Appliance(ASA)上對VPN使用者提供的證書使用線上證 書狀態協定(OCSP)驗證。提供了兩個OCSP伺服器(Microsoft Windows Certificate Authority [CA]和OpenSSL)的配置示例。「驗證」部分描述資料包級別的詳細流程,「故障排除」部分重點 介紹典型錯誤和問題。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco自適應安全裝置命令列介面(CLI)配置和安全套接字層(SSL)VPN配置
- •X.509憑證
- Microsoft Windows Server
- Linux/OpenSSL

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Adaptive Security Appliance軟體8.4版及更高版本
- •搭載Cisco AnyConnect安全行動化使用者端的Microsoft Windows 7,版本3.1
- Microsoft Server 2012 R2
- 使用OpenSSL 1.0.0j或更高版本的Linux

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

註:使用<u>命令查詢工具(</u>僅限<u>註冊</u>客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

客戶端使用遠端訪問VPN。此訪問可以是Cisco VPN Client(IPSec)、Cisco AnyConnect Secure Mobility(SSL/Internet Key Exchange Version 2 [IKEv2])或WebVPN(門戶)。為了登入,客戶端提 供正確的證書以及在ASA本地配置的使用者名稱/密碼。客戶端證書通過OCSP伺服器進行驗證。



帶OCSP的ASA遠端訪問

ASA配置為SSL訪問。使用者端正在使用AnyConnect進行登入。ASA使用簡單證書註冊協定 (SCEP)來請求證書:

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

建立證書對映以標識其主題名稱包含單詞administrator(不區分大小寫)的所有使用者。這些使用 者已繫結到名為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

VPN配置需要成功授權(即經過驗證的證書)。它還要求本地定義的使用者名稱(身份驗證 aaa)具有正確的憑據:

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

Microsoft Windows 2012 CA

注意:有關通過CLI配置ASA的詳細資訊,請參閱<u>Cisco ASA 5500系列使用CLI的配置指南</u> 8.4和8.6:配置外部伺服器以進行安全裝置使用者授權。

服務安裝

以下過程介紹了如何為Microsoft伺服器配置角色服務:

 導覽至Server Manager > Manage > Add Roles and Features。Microsoft伺服器需要以下角 色服務:

證書頒發機構客戶端使用的證書頒發機構Web註冊線上響應程式,OCSP需要該程式網路裝 置註冊服務,包含ASA使用的SCEP應用程式 如果需要,可以新增帶策略的Web服務。

	AD CS Configuration	>
Role Services		DESTINATION SERVER WIN-35QVH03PQE3.lab.com
Credentials	Select Role Services to configure	
Role Services		
Setup Type	 Certification Authority 	
CA Type	Certification Authority Web Enrollment	
Private Key	Online Responder 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 Koles	
L.		
.0	< Previous Next >	Configure Cancel

2.

3.

4. 新增功能時,請確保包含聯機響應程式工具,因為它包含稍後使用的OCSP管理單元:

h	Add Roles and Features Wizard	_ _ X
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Add Roles and Features Wizard Select one or more features to install on the selected server. Features Image: Role Administration Tools (12 of 28 installed) Image: Role Administration Tools (12 of 28 installed) Image: Role Administration Tools (12 of 5 installed) Image: Role Administration Tools (12 of 5 installed) Image: Role Administration Tools (12 of 5 installed) Image: Role Administration Tools (10 of 5 installed) Image: Role Administration Tools (1 of 6 installed) Image: Role Administration Tools (1 of 6 installed) Image: Role Administration Tools (1 of 6 installed) Image: Role Administration Tools (1 of 7 installed) Image: Role Administration Tools (1 of 7 installed) Image: Role Administration Tools (1 of 8 installed) Image: Role Administration Tools (1 of 8 installed) Image: Role Administration Tools (1 of 9 installed) Image: Role Administration Tools (1 of 9 installed) Image: Role Administration Tools (1 of 9 installed) Image: Role Administration Authority Management Tools Image: Role Administration Authority Management Servic Image: Role Administration Authority Management Servic	DESTINATION SERVER WIN-35QVH03PQE3.Jab.com Description Online Responder Tools includes the Online Responder Management snap-in.
	DHCP Server Tools (Installed) DNS Server Tools (Installed) Fax Server Tools File Services Tools Network Policy and Access Services Tools (Ivertice) Comparison of the service of	Install Cancel

OCSP服務使用證書對OCSP響應進行簽名。必須在Microsoft伺服器上生成特殊證書,並且必須包括:

- 擴展金鑰用法= OCSP簽名
- OCSP無吊銷檢查

需要此證書以防止OCSP驗證循環。ASA不使用OCSP服務嘗試檢查OCSP服務提供的證書。

 為CA上的證書新增模板。導航到CA > Certificate Template > Manage,選擇OCSP Response Signing,然後複製模板。檢視新建立的模板的屬性,然後按一下Security頁籤。許可權描述允 許哪個實體請求使用該模板的證書,因此需要正確的許可權。在本示例中,實體是在同一主機 上運行的OCSP服務(TEST-CISCO\DC),並且OCSP服務需要自動註冊許可權:

模板的所有其他設定都可以設定為預設值。

2. 啟用模板。導覽至CA > Certificate Template > New > Certificate Template to Issue,然後選 擇重複模板:



OCSP服務證書

以下過程介紹了如何使用聯機配置管理來配置OCSP:

- 1. 導覽至Server Manager > Tools。
- 2. 導覽至**吊銷配置 > 新增吊銷配置**,以便新增新配置:

P	ocsp - [Online Responder: DC.test-cisco.com\Revocatio	n Configuration]
File Action View Help		
🗢 🔿 🙍 🗟		
Ponline Responder: DC.test-cisco.cc	Name Signing Certificate Sele	ec Enrollment Ten
 	There are no items to show in this view.	
	Add Revocation Configuration	? X
Choose CA C	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 for the C Responder must identify the CA that issued the certificate. You can identify this CA by selecting a CA certificate published in Active Direct by locating a CA computer.	Inline ory or
Select Signing Certificate	Browse CA certificates published in Active Directory Browse	se
Revocation Provider	Select Certification Authority ? ×	
	Select a certification authority (CA) you want to use. CA Computer CA DC.test-cisco-DC-CA DC.test-cisco.com	ie
	< III > OK Cancel	Cancel

OCSP可以使用相同的企業CA。生成OCSP服務的證書。

3. 使用選定的企業CA,並選擇之前建立的模板。自動註冊證書:



4. 確認憑證已註冊,且其狀態為工作/正常:



Revocation Configuration Status	
Signing Certificate: Ok	
View Signing Certificate	
Revocation Provider Status:	
Type: Microsoft CRL-based revocation status provider The revocation provider is successfully using the current configuration	^
Т	
	~

5. 導覽至CA > Issued Certificates,以驗證憑證詳細資訊:

i 🖕	certsrv - [Certification Authority (Local)\test-cisco-D	C-CA\I	ssued Certificate	es]
File Action View Help				
* 🔿 🖄 🙆 📓	Certificate X			
Pile Action View Pile Image: Action Action Authority (Local) Image: Actiot	Certificate X General Details Certification Path Show: <all> V 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 _ Financed Key Usage OCSP Symng (1.3.6.1.5.5.7.3 _ OCSP No Revocation Checking 05 00 _ Authority Key Identifier KeyID=9f 99 7f b2 3b 61 90 0 _ OCSP Signing (1.3.6.1.5.5.7.3.9) _ _</all>	late ler (ment (CEP ques ques ques ques	Serial Number 24000000206c 240000003486 240000004971 2400000057d8 24000000639b 2400000082d2 2400000082d2 2400000098d 24000000098d 240000000648 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 12:12 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 10/10/2013 2:06 PM 10/10/2013 6:51 PM
	Edit Properties Copy to File OK			

OCSP服務節點

OCSP的Microsoft實施符合RFC 5019適用於高容量環境的輕型線上證書狀態協定(OCSP)配置檔案 (這是簡化版本的RFC 2560 X.509 Internet公鑰基礎設施線上證書狀態協定 — OCSP)。

ASA對OCSP使用RFC 2560。這兩個RFC的區別之一是RFC 5019不接受ASA傳送的簽名請求。

可以強制Microsoft OCSP服務接受這些已簽名的請求,並使用正確的已簽名的響應進行回覆。導航 到Revocation Configuration > RevocationConfiguration1 > Edit Properties,然後選擇選項以**啟用** NONCE**擴展支援**。

File Action View Help				
🗢 🤿 🙍 🗟				
Part Online Responder: 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 Config			
	Local CRL Revocation Provider Signing	1		
	The selected hash algorithm is used by the responses sent to clients.	Online Responders to sign		
	Hash algorithm: SHA1	~		
	Do not prompt for credentials for crypto	graphic operations		
	Automatically use renewed signing cert	ficates.		
	 Enable NONCE extension support 			
	Use any valid OCSP signing certificate			
	Online Responder Identifiers All responses will include the following O	nine Responder identifier		
		nine rresponder identifier.		
	Key hash of the signing certricate			
	 Subject of the signing certificate 			
N .				
12				
	ок	Cancel Help		

OCSP服務現已可供使用。

雖然Cisco不建議這樣做,但是可以在ASA上禁用nonces:

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

OCSP擴展的CA配置

現在,必須重新配置CA,以便在所有頒發的證書中包括OCSP伺服器擴展。驗證證書時,ASA使用 該擴展的URL以連線到OCSP伺服器。

- 1. 開啟CA上伺服器的屬性對話方塊。
- 2. 按一下**Extensions**頁籤。需要指向OCSP服務的授權資訊訪問(AIA)擴展;在本示例中,該擴展 為http://10.61.208.243/ocsp。為AIA擴展啟用以下兩個選項:

包括在已頒發證書的AIA擴展中包括在線上證書狀態協定(OCSP)擴展中

ته c	test-cisco-DC-CA Properties ?					
File Action View Help	Enrollment Agents	Auditing	Recover	y Agents	Security	
🖾 🚈 🛄 🔼 🦛 🗢	General	Policy Mo	dule	Exit	Module	
Certification Authority (Local)	Extensions	Storage		Certificate N	lanagers	
⊿ 👼 test-cisco-DC-CA	Select extension:					
Revoked Certificates	Authority Information	Access (AIA)			~	
Issued Certificates	Specify locations from	which users car	obtain the (certificate fo	r this CA	
Pending Requests	opeony received from			oonanooto to		
Failed Requests				DNIGN		
	; C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<cana Idap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname> file://<serverdnsname>/CertEnroll/<serverdnsname>_<caname></caname></serverdnsname></serverdnsname></caname></serverdnsname></serverdnsname></catruncatedname></cana </serverdnsname>				>_ <canname. ervices,CN=S CaName><ce aName><cert< th=""></cert<></ce </canname. 	
	< 111				>	
			Ad	d	Remove	
	 Include in the AIA extension of issued certificates Include in the online certificate status protocol (OCSP) extension 					

這可確保所有簽發的證書都有一個指向OCSP服務的正確擴展。

OpenSSL

注意:有關通過CLI配置ASA的詳細資訊,請參閱<u>Cisco ASA 5500系列使用CLI的配置指南</u> 8.4和8.6:配置外部伺服器以進行安全裝置使用者授權。

此範例假設已設定OpenSSL伺服器。本節僅介紹OCSP配置和CA配置所需的更改。

以下過程介紹了如何生成OCSP證書:

1. OCSP響應程式需要以下引數:

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

2. 使用者證書需要以下引數:

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

3. 證書需要由CA生成並簽名。

4. 啟動OCSP伺服器:

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

5. 測試示例證書:

openssl ocsp -CAfile cacert.crt -issuer cacert.crt -cert example-cert.crt -url http://10.61.208.243 -resp_text 更多示例可在OpenSSL網站上找到。

與ASA一樣, OpenSSL支援OCSP會話; 可以使用 — nonce和 — no_nonce開關控制nonce。

具有多個OCSP源的ASA

ASA可以覆蓋OCSP URL。即使客戶端證書包含OCSP URL,它也會被ASA上的配置覆蓋:

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 可以顯式定義OCSP伺服器地址。此命令示例匹配主題名稱中帶有管理員的所有證書,使用 OPENSSL信任點驗證OCSP簽名,並使用http://11.11.11.11/ocsp的URL傳送請求:

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 用於查詢OCSP URL的順序為:

- 1. 使用match certificate命令設定的OCSP伺服器
- 2. 使用ocsp url命令設定的OCSP伺服器
- 3. 客戶端證書的AIA欄位中的OCSP伺服器

具有由不同CA簽名的OCSP的ASA

OCSP響應可以由其他CA簽名。在這種情況下,必須使用**match certificate**命令才能在ASA上使用不同的信任點進行OCSP證書驗證。

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

在此示例中,ASA對包含管理員的使用者名稱的所有證書使用OCSP URL重寫。ASA被迫根據另一個信任點OPENSSL驗證OCSP響應方證書。使用者證書仍在WIN2012信任點中驗證。

由於OCSP響應方證書具有「OCSP無撤銷檢查」擴展,因此即使強制對OPENSSL信任點進行 OCSP驗證,也不會驗證證書。

預設情況下,當ASA嘗試驗證使用者證書時,將搜尋所有信任點。OCSP響應方證書的驗證不同。 ASA僅搜尋已找到的使用者證書的信任點(在本例中為WIN2012)。

因此,必須使用**match certificate**命令來強制ASA使用不同的信任點進行OCSP證書驗證(在此示例 中為OPENSSL)。

根據第一個匹配的信任點(本例中為WIN2012)驗證使用者證書,然後確定用於OCSP響應方驗證 的預設信任點。

如果**match certificate**命令中未提供特定信任點,則會根據與使用者證書相同的信任點驗證OCSP證 書(在本示例中為WIN2012):

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

驗證

使用本節內容,確認您的組態是否正常運作。

註:<u>Output Interpreter Tool</u>(僅<u>供</u>已註冊客戶)支援某些**show**命令。使用Output Interpreter工具 檢視**show**指令輸出的分析。

ASA — 通過SCEP獲取證書

以下程式說明如何使用SCEP取得憑證:

1. 這是用於獲取CA證書的信任點身份驗證過程:

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:

← → × 192.168.10.100/certsrv/mscep_admin/

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP). To complete certificate enrollment for your network device you will need the following information: The thumbprint (hash value) for the CA certificate is: 27DDA0E5 E1ED3F4C E3A2C3DA 6D1689C2 The enrollment challenge password is: 3F9E646BB159FB0F This password can be used only once and will expire within 60 minutes. Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password. For more information see Using Network Device Enrollment Service.

3. 使用該密碼在ASA上請求證書:

```
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: Found a subject match - inserting the following cert record into certList 為清楚起見,省略了部分輸出。

4. 驗證CA和ASA證書:

```
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
ASA不顯示大多數證書擴展。即使ASA證書包含「AIA中的OCSP URL」擴展,ASA CLI也不
```

會顯示它。思科錯誤ID <u>CSCui44335</u>、「ASA ENH Certificate x509 extensions displayed(已 顯示ASA增強型證書x509擴展)」請求此增強功能。

AnyConnect — 通過網頁獲取證書

以下程式說明如何在使用者端上使用Web瀏覽器來取得憑證:

1. 可以通過網頁請求AnyConnect使用者證書。在客戶端PC上,使用Web瀏覽器轉到CA,地址 為http://*IP*/certsrv:

← → C □ 192.168.10.100/certsrv/
Microsoft Active Directory Certificate Services test-cisco-DC-CA
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you ca depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation li
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

2. 使用者證書可以儲存在Web瀏覽器儲存中,然後匯出到Microsoft儲存中,AnyConnect將搜尋 該儲存區。使用certmgr.msc驗證收到的證書:

Certificates - Current User	\Personal\Certificates]	1	
 certmgr - [Certificates - Current User/ File Action View Help File Action View Help Certificates - Current User Certificates - Current User Personal Certificates Trusted Root Certification Au Enterprise Trust Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Certificates 	\Personal\Certificates] Image: Certificates Image: Certificates ssued To Image: Certificates Image: Certificates Ssued To Image: Certificates Image: Certificates	Certificate General Details Certification Path Show: <al>> Field Value CRL Distribution Points [1]CRL Distribution Point: Distr Authority Information Access [1]Authority Info Access: Acc Certificate Template Name User Enhanced Key Usage Encrypting File System (1.3.6 Subject Alternative Name Other Name:Principal Name =A</al>	
 Third-Party Root Certification Trusted People Other People Certificate Enrollment Reques Smart Card Trusted Roots 		SMIME Capabilities [1]SMIME Capability: Object I Key Usage Digital Signature, Key Encipher Thumborint algorithm sha 1 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	•

AnyConnect還可以請求證書,只要有正確的AnyConnect配置檔案。

帶OCSP的ASA VPN遠端訪問驗證

以下過程介紹了如何檢查OCSP驗證:

1. 在嘗試連線時,ASA報告正在檢查證書的OCSP。此處,OCSP簽名證書具有無檢查副檔名 ,且尚未通過OCSP檢查:

```
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.
為清楚起見,省略了部分輸出。
```

2. 終端使用者提供使用者憑證:

🔇 Cisco AnyConne	ect 10.48.67.229	×		
Username:	cisco			
Password:				
	OK Cancel			
🕥 Cisco AnyConn	ect Secure Mobility Client			8
	/PN: Contacting 10.48.67.229. 10.48.67.229	-	Connect	
\$ ()				dijulju cisco

3. VPN作業階段已正確完成:

%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. 會話已建立:

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

Session Type: AnyConnect Detailed

Username	:	cisco	Ind	ex	:	4	
Assigned IP	:	192.168.11.100	Pub	lic IP	:	10.61.209.83	
Protocol	:	: AnyConnect-Parent SSL-Tunnel DTLS-Tunnel					
License	:	AnyConnect Premium					
Encryption	:	AnyConnect-Parent: (1)	none	SSL-Tuni	ne	l: (1)RC4	
DTLS-Tunnel:	(1)AES128					
Hashing	:	AnyConnect-Parent: (1)	none	SSL-Tuni	ne	l: (1)SHA1	
DTLS-Tunnel:	(1)SHA1					
Bytes Tx	:	10540	Byt	es Rx	:	32236	
Pkts Tx	:	8	Pkt	s Rx	:	209	
Pkts Tx Drop	:	0	Pkt	s Rx Drop	:	0	
Group Policy	:	MY	Tun	nel Group	:	RA	
Login Time	:	11:30:31 CEST Sun Oct	13 2	013			
Duration	:	0h:01m:05s					
Inactivity	:	0h:00m:00s					
NAC Result	:	Unknown					
VLAN Mapping	:	N/A	VLA	N	:	none	
AnyConnect-Pa Tunnel ID	are :	ent: 4.1					
Public IP	:	10.61.209.83					
Encryption	:	none	Ha	shing		: none	
TCP Src Port	; ;	51401	TC	P Dst Port	t	: 443	
Auth Mode	:	Certificate and user	assw	ord			
Idle Time Ou	it:	30 Minutes	Id	le TO Left	t	: 29 Minutes	
Client OS	:	Windows					
Client Type	:	AnyConnect					
Client Ver	:	Cisco AnyConnect VPN	Agen	t for Wind	do	ws 3.1.02040	
Bytes Tx	:	5270	Ву	tes Rx		: 788	
Pkts Tx	:	4	Pk	ts Rx		: 1	
Pkts Tx Drop		0	Pk	ts Rx Drop	2	: 0	
SSL-Tunnel:							
Tunnel ID	:	4.2					
Assigned IP		192.168.11.100	Pu	blic IP		: 10.61.209.83	
5							

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

 Encryption : AES128
 Hashing : SHA1

 Encapsulation: DTLSv1.0
 UDP Src Port : 58053

 Encapsulation: DTLSv1.0 UDP Dst Port : 443 Auth Mode : Certificate and userPassword Idle TO Left : 29 Minutes Idle Time Out: 30 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 Tx : 0 Pkts Rx : 201 Pkts Tx Drop : 0 Pkts Rx Drop : 0

5. 您可以使用詳細調試進行OCSP驗證:

CRYPTO_PKI: Starting OCSP revocation CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number: 240000019F341BA75BD25E91A0000000019, 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: 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

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
```

 在資料包捕獲級別,這是OCSP請求和正確的OCSP響應。響應包含在Microsoft OCSP上啟用 的正確簽名 — nonce擴展:

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							
⊳ Hy	pertext Transfer Prot	tocol					
<mark>∀</mark> 0n	line Certificate Sta	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)		
~	▼ Basic0CSPResponse						
	▼ tbsResponseData						
	▷ responderID: byKey (2)						
	producedAt: 2013-10-12 14:48:27 (UTC)						
	▷ responses: 1 item						
	✓ responseExtensions: 1 item						
	▼ Extension						
	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: 353fc461732dc47b1d167ebace677a087765b48edb3b284c						
	⊳certs: 1 item						

具有多個OCSP源的ASA VPN遠端訪問

如果按照<u>具有多個OCSP源的ASA</u>中的說明配置匹配證書,則優先使用:

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 体用OCCDUDE 要求性 ==??口一方.

使用OCSP URL覆蓋時,調試程式為:

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

具有OCSP和已撤銷證書的ASA VPN遠端訪問

以下過程介紹了如何撤銷證書和確認撤銷狀態:

1. 吊銷客戶端證書:

📮 certsrv - [Cer	rtification	n Authoi	rity (Loc	al)\t	est-cisco-DC-CA\ls	sued
File Action View Help						
🗢 🔿 🙎 🙆 😫						
🙀 Certification Authority (Local)	Request	ID Red	quester N	ame	Binary Certificate	Certif
⊿ 🛃 test-cisco-DC-CA	-	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
Revoked Certificates	F 7	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
Ssued Certificates	58 💭	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
Pending Requests	l 🔄 9	TES	ST-CISCO	\Ad	BEGIN CERTI	User
Failed Requests	🔄 10	TES	ST-CISCO	\Ad	BEGIN CERTI	User
Certificate Templates	🔄 11	TES	ST-CISCO	\Ad	BEGIN CERTI	User
	🔄 12	TES	ST-CISCO	\Ad	BEGIN CERTI	User
	🔄 13	TES	ST-CISCO	\Ad	BEGIN CERTI	User
	🔄 14	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
	🔄 18	TES	ST-CISCO	\DC\$	BEGIN CERTI	Сору
	🔄 19	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
	l 🔄 20	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
	l 🔄 21	TES	ST-CISCO	\Ad	BEGIN CERTI	User
	🚎 r	0		`Ad	BEGIN CERTI	User
		Open		Ad	BEGIN CERTI	User
		All Tasks	•		View Attributes/Extensi	ons
A		Refresh			Export Binary Data	
		Help			Revoke Certificate	
	28	TES	ST-CISCO	\Ad	BEGIN CERTI	IPSec
	<	III				
Contains actions that can be performed on the item.						

2. 發佈結果:

📮 certs	srv - [Certi	ification Au	thority (Local)\tes	t-cisco-DC-CA\Revoked	Certificates]	
File Action View H	Help					
🙀 Certification Authority	(Local)	Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester
∡		27	10/13/2013 12:21	10/13/2013 12:21 PM	Unspecified	TEST-CISC
Ssued Cer	All Tasks	•	Publish			
Pending R	View	•				
Certificate	Refresh Export Lis	t				
	Properties	;				
	Help					

3. [可選]步驟1和2也可以使用Power Shell中的certutil CLI實用程式來完成:

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

4. 使用者端嘗試連線時,存在憑證驗證錯誤:

Cisco AnyConnect	
Certificate Validation Failure	
ОК	
Scisco AnyConnect Secure Mobility Client	
VPN: No valid certificates available for 10.48.67.229	r authentication. → Connect
‡ (j)	altala cisco

5. AnyConnect日誌還指示證書驗證錯誤:

[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. ASA報告證書狀態已吊銷:

CRYPTO_PKI: Starting OCSP revocation 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 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. 封包擷取顯示成功的OCSP回應,且憑證狀態為已撤銷:

No.	Source	Destination	Protocol	Length	Info		
2	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							
⊳ H	ypertext Transfer Pro	tocol					
⊽ 0	nline Certificate Sta	tus Protocol					
	responseStatus: succe	essful (0)					
~	responseBytes						
	ResponseType Id: 1.	3.6.1.5.5.7.48.1.1 (id-pkix-	ocsp-ba	nsic)		
	▼ Basic0CSPResponse						
	✓ tbsResponseData						
	▷ responderID: byKey (2)						
	producedAt: 2013-10-13 10:47:02 (UTC)						
	⊽ responses: 1 ite	m					
	⊳ certID						
	⊳certStatus: r	evoked (1)					
	thisUpdate: 2	2013-10-13 10:17:51	(UTC)				
	nextUpdate: 2	2013-10-14 22:37:51	(UTC)				
	⊳ singleExtensi	ons: 1 item					
	responseExtensio	ns: 1 item					
	▹ signatureAlgorithm	n (shaWithRSAEncrypt:	ion)				

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

OCSP伺服器關閉

ASA在OCSP伺服器關閉時報告:

CRYPTO_PKI: unable to find a valid OCSP server. CRYPTO PKI: OCSP revocation check has failed. Status: 1800. 封包擷取也有助於進行疑難排解。

時間不同步

如果OCSP伺服器上的當前時間早於ASA上的時間(可以接受較小的差異),則OCSP伺服器將傳送未經授權的響應,ASA將報告該響應:

CRYPTO_PKI: OCSP response status - unauthorized 當ASA收到來自未來時間的OCSP響應時,也會失敗。

不支援簽名的Nonces

如果伺服器上的nonces不受支援(這是Microsoft Windows 2012 R2的預設設定),則會返回未經 授權的響應:

No.	Source	Destination	Protocol	Length	Info	
5	5 10.48.67.229	10.61.208.243	0CSP	545	Request	
5	9 10.61.208.243	10.48.67.229	0CSP	337	Response	
4						
▶ F	ame 59: 337 bytes on	wire (2696 bits), 33	37 bytes	captur	red (2696 bits)	
▶ E	thernet II, Src: Cisco	_2a:c4:a3 (00:06:f6	:2a:c4:a	3), Dst	:: Cisco_b8:6b:25 (00:17:5	
ÞΙ	nternet Protocol Vers	ion 4, Src: 10.61.20	8.243 (1	0.61.20	8.243), Dst: 10.48.67.229	
ÞΤ	ransmission Control P	rotocol, Src Port: h	ttp (80)	, Dst P	ort: 14489 (14489), Seq:	
▶ H	/pertext Transfer Pro	tocol				
	nline Certificate Sta	tus Protocol				
	responseStatus: unauthorized (6)					

IIS7伺服器身份驗證

SCEP/OCSP請求的問題通常是由於Internet資訊服務7(IIS7)上的身份驗證不正確造成的。確保配置 了匿名訪問:





- Microsoft TechNet: Online Responder安裝、配置和故障排除指南
 Microsoft TechNet: 配置CA以支援OCSP響應程式
- <u>Cisco ASA系列命令參考</u>
- 技術支援與文件 Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。