# 使用數位證書和Microsoft CA的ASA/PIX 8.x和 VPN客戶端IPSec身份驗證配置示例

## 目錄

## <u>簡介</u>

本文說明如何手動在思科安全裝置(ASA/PIX)8.x以及VPN客戶端上安裝第三方供應商數位證書,以 便使用Microsoft證書頒發機構(CA)伺服器驗證IPSec對等體。

## <u>必要條件</u>

## <u>需求</u>

本文檔要求您擁有證書註冊證書頒發機構的訪問許可權。支援的第三方CA供應商包括Baltimore、 Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA和VeriSign。

本文檔假設ASA/PIX中沒有預先存在的VPN配置。

注意:本文檔使用Microsoft Windows 2003伺服器作為方案的CA伺服器。

**注意:**有關如何將Windows 2003伺服器配置為CA的完整資訊,請參閱<u>在Windows伺服器上配置CA</u> 。

## <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- ASA 5510(運行軟體版本8.0(2)和ASDM版本6.0(2))
- 運行軟體版本4.x及更高版本的VPN客戶端

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。

### 相關產品

ASA配置還可以與運行軟體版本8.x的Cisco 500系列PIX一起使用。

#### 慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

## <u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

#### 網路圖表

本檔案會使用以下網路設定:



**注意:**此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

#### <u> 組態</u>

本檔案會使用以下設定:

• <u>ASA配置</u>

• <u>ASA配置摘要</u>

• <u>VPN客戶端配置</u>

### <u>ASA配置</u>

要在ASA上安裝第三方供應商數位證書,請完成以下步驟:

- 步驟1.檢驗日期、時間和時區值是否準確
- 步驟2.生成證書簽名請求
- 步驟3.驗證信任點
- <u>步驟4.安裝證書</u>
- •步驟5.將遠端訪問VPN(IPSec)配置為使用新安裝的證書

#### 步驟1.檢驗日期、時間和時區值是否準確

#### ASDM過程

- 1. 按一下Configuration,然後按一下Device Setup。
- 2. 展開System Time, 然後選擇Clock。
- 3. 驗證列出的資訊是否準確。Date、Time和Time Zone的值必須準確無誤,才能進行正確的證書 驗證。

	Device Setup $\Box + \times$	Configuration > Device Setup > System Time > Clock
vice List	Startup Wizard	Configure the ASA date and clock.
De		Time Zone: (GMT+05:30) Calcutta
	System Time	Date
		Dec 21, 2007
		Time
		Time: 05 : 35 : 58 hh:mm:ss (24-hour)
		Update Displayed Time

命令列示例

CiscoASA
CiscoASA#show clock
05:37:37.904 UTC Fri Dec 21 2007

### 步驟2.生成證書簽名請求

需要證書簽名請求(CSR),第三方CA才能頒發身份證書。CSR包含您的ASA的可分辨名稱(DN)字串 以及ASA生成的公鑰。ASA使用生成的私鑰對CSR進行數位簽章。

### ASDM過程

- 1. 按一下Configuration,然後按一下Device Management。
- 2. 展開Certificate Management, 然後選擇Identity Certificates。

C Import the identity certi	ificate from a file:			
Decryption Passobrase:				
File to Import From:			Browse	ŕ
C Add a naw identify carti	i i i - ka i			
<ul> <li>Add a new identity certi</li> </ul>		1000	(i	() 
Key Pair:	my.CA.key	<u> </u>	Show	New
Certificate Subject DN:	CN=CiscoASA		Select	<i>y</i>
Act as local certi	ficate authority and i	ssue dynamic ce	ertificates to TLS	Proxy Advanced.
Act as local certi	ficate authority and i	ssue dynamic ce	ertificates to TLS	-Proxy Advanced.
▲ Generate seir-signer ▲ Act as local certi Add Certil 一下Add a new identity cert 於金鑰對,按一下New。	ficate authority and i ficate Can tificate單選按鈕。	ssue dynamic ce	ertificates to TLS	-Proxy Advanced.
C Act as local certi Add Certil 一下Add a new identity cert 於金鑰對,按一下New。 Add Key Pair	ficate authority and i ficate Can tificate單選按鈕。	ssue dynamic ca	ertificates to TLS Help	-Proxy Advanced.
C Act as local certi Add Certil 一下Add a new identity cert 於金鑰對,按一下New。 Add Key Pair Name: ① Use default key	ficate authority and i ficate Can tificate單選按鈕。	ssue dynamic ca	ertificates to TLS Help	-Proxy Advanced.
C Act as local certi Add Certil 一下Add a new identity cert 於金鑰對,按一下New。 Add Key Pair Name: ○ Use default key ⓒ Enter new key	ficate authority and i ficate Can tificate單選按鈕。	ssue dynamic ca	ertificates to TLS	Proxy Advanced.
C Act as local certi Add Certil →下Add a new identity certi 於金鑰對,按一下New。 Add Key Pair Name: ○ Use default key ⓒ Enter new key Size: 1024	ficate authority and i ficate Can tificate單選按鈕。	ssue dynamic ca	ertificates to TLS Help	-Proxy Advanced.
C Act as local certil Add Certil 一下Add a new identity cert 於金鑰對,按一下New。 Add Key Pair Name: ○ Use default key ⓒ Enter new key Size: 1024	ficate authority and i ficate Can tificate單選按鈕。	ssue dynamic ce cel	ertificates to TLS	Proxy Advanced.

- 6. 按一下Enter new key pair name單選按鈕。出於識別目的,必須明確標識金鑰對名稱。
- 7. 按一下「Generate Now」。現在必須建立金鑰對。
- 8. 要定義證書使用者DN,請按一下**選擇**,然後配置下表列出的屬性:若要設定這些值,請從「 屬性」下拉式清單中選擇一個值,輸入該值,然後按一下Add。

		Attribute	Value
DN Attribute to be Added		Common Name(CN)	CiscoASA.cisco.
Attribute: Select Attribute	✓ Add>>	Company Name (O)	Cisco Systems
		Country (C)	US
vaue:	Delete	State (St)	North Carolina
	]	Location (L)	Raleigh
ОК	Cancel	Help	
一下「 <b>Advanced」。</b> FQDN欄位中,輸入用於從Inte QDN相同。	rnet訪問裝置的FQ	DN。此值必須與用	於公用名(CN)的
一下「 <b>Advanced</b> 」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S	rnet訪問裝置的FQ CEP challenge passw	DN。此值必須與用 ord are not available	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte DN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Chal	DN。此值必須與用 vord are not available llenge Password	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte DN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Chai	DN。此值必須與用 vord are not available llenge Password	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte DN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.com	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Cha m	DN。此值必須與用 word are not available llenge Password	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor E-mail:	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Cha n	DN。此值必須與用 vord are not available llenge Password ]	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor E-mail: IP Address:	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Chai	DN。此值必須與用 word are not available llenge Password ]	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor E-mail: IP Address: 「Include serial number of the	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Chal m	DN。此值必須與用 oord are not available llenge Password	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor E-mail: IP Address: Include serial number of the	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Cha m	DN。此值必須與用 word are not available llenge Password	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor E-mail: IP Address: 「Include serial number of the	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Cha n	DN。此值必須與用 word are not available llenge Password	於公用名(CN)的 for self-signed ce
一下「Advanced」。 FQDN欄位中,輸入用於從Inte QDN相同。 Advanced Options Enrollment mode parameters and S Certificate Parameters Enrollme FQDN: CiscoASA.cisco.cor E-mail: IP Address: Include serial number of the	rnet訪問裝置的FQ CEP challenge passw nt Mode   SCEP Chal n	DN。此值必須與用 ord are not available llenge Password	於公用名(CN)的 for self-signed ce

12. 按一下「**OK**」,然後按一下「**Add Certificate**」。系統將提示您將CSR儲存到本地電腦上的

To complete request (CSF	the enrollment pro () and send it to th	ocess, please save t ne CA.	he PKCS10 enrollment
YOU WILL THEN	need to install the	e certificate that is r	eturned from the ( 0 by
clicking the Ir	ostall button in the	e Identity Certificate	es nanel
clicking the Ir	nstall button in the	e Identity Certificate	es panel.
clicking the Ir	file: c:/cert_cli	ent txt	es panel. Browse

檔案中。

13. 按一下「**Browse**」,選擇要儲存CSR的位置,並以.txt副檔名儲存檔案。**注意:**使用.txt副檔 名儲存檔案時,可以使用文本編輯器(如記事本)開啟該檔案並檢視PKCS#10請求。

<pre>@ cert_client.txt - Notepad</pre>
<u>File Edit Format H</u> elp
MIICKZCCAZQCAQAwga0xEDAOBgNVBACTB1JhbGVpZ2gxFzAVBgNVBAgTI IENhcm9saw5hMQswCQYDVQQGEwJVUZEWMBQGA1UEChMNQ21zY28gU31zc MCIGA1UEAxMbQ21zY29BU0EuY21zY28uY29tIE9VPVRTV0VCMTUwEgYDV TVgwOTM1szA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNvk BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j> XgKoH2Pce1cGZ9dUXn+Y09Qjm0Krj68L6KXT1PgNAaFMwB2YsTIOn+hJE MI6xLyKrGo7b0PAsLPeOBx1/LVLTy3ORqcyy2QP3Ir1BSwoyBaoFPsRe: QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJDjEuMCwwCwYDVR0PBAQD/ A1UdEQQWMBSCEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF/ 3tzyAD7o6R5ej9Ew7Ej4BfcXd20LCbXAoP5L1KbPaEeaCkfN/Pp5mATAs bsxSv1jSSXQsQ1Sb842D6MEG6cu7Bxj/K1Z6MxafUvCHr0PYWVU1wgRJC j89/Y4S8XhQ79fvBwbR8Ux9emhFHpGHnQ/MpSfU0dQ==

---End - This line not part of the certificate request---

14. 將儲存的CSR提交給您的第三方供應商(例如Microsoft CA),如下所示。使用為 vpnserver提供的使用者憑據執行Web登入CA伺服器172.16.5.1。

File	Edit	View	Fa	voriti	es	Tools	Help				
🔶 В	ack 🔻	÷ -	۲	¢	<b>a</b>	0	Search	🙀 Favorites	Media	۹	

Site:	172.16.5.1	
User Name	vpnuser	
Password	*******	
Domain		

**注意:**確保

您在CA伺服器中擁有ASA(vpn伺服器)的使用者帳戶。按一下「Request a certificate > advanced certificate request」,以選擇「Submit a certificate request by using a base-64encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file」。

Address 🙋 http://172.16.5.1/certsrv/certrqad.asp	*	∂Go Lin
Microsoft Certificate Services - CA1		Home

#### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

將編碼的資訊複製並貼上到Saved Request框中,然後按一下Submit。

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded ( source (such as a Web server) in the Saved Request box.

## Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	VQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAO 4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8 D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+ 8Ux9emhFHpGHnQ/MpSfU0dQ== not part of the certificate request	
	Browse for a file to insert.	
Certificate Temp	late:	
	IPSEC 🗾	
Additional Attrib	utes:	
Attributes:		
-	Submit >	
<sup>F</sup> Base 64 encoded	」單選按鈕,然後按一下「Download certificate」。	. Г
Microsoft Certific	ate Services CA1	
Certificate Iss	ued	
The certificate	you requested was issued to you.	
¢ [	ER encoded or @Base 64 encoded	
Dov Dov	<u>vnload certificate</u> <u>vnload certificate chain</u>	
Download(檔案下載 ASA上的身份證書。	或)」視窗。使用 <b>cert_client_id.cer</b> 名稱儲存該證書,該名稱是要安裝	돈

File Dow	nload			×
?	Some files can H looks suspicious save this file.	narm your compute s, or you do not ful	er. If the file inform ly trust the source	ation below ;, do not open or
	File name:	certnew.cer		
	File type:	Security Certifica	te	
	From:	172.16.5.1		
	This type of malicious of malicious of the second secon	if file could harm y ode.	our computer if it (	contains
	Would you like	to open the file or	save it to your cor	mputer?
	Open	Save	Cancel	More Info
		before opening thi	s tupe of file	
	It way up to	bererer operning dri	o ope of the	

### 命令列示例

CiscoASA
CiscoASA# configure terminal
CiscoASA(config)#crypto key generate rsa label my.ca.key modulus 1024
<pre>! Generates 1024 bit RSA key pair. "label" defines the name of the Key Pair. INFO: The name for the keys will be: my.CA.key Keypair generation process begin. Please wait ciscoasa(config)#crypto ca trustpoint CA1 ciscoasa(config-ca-trustpoint)# subject-name CN=CiscoASA.cisco.com,OU=TSWEB,</pre>
Systems, C=US, St=North Carolina, L=Raleign
<pre>! Defines x.500 distinguished name. Use the attributes defined in table as a guide. CiscoASA(config- ca-trustpoint)#keypair my.CA.key</pre>
<pre>! Specifies key pair generated in Step 3 CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com</pre>
<pre>! Specifies the FQDN (DNS:) to be used as the subject alternative name CiscoASA(config-ca- trustpoint)#enrollment terminal</pre>
<pre>! Specifies manual enrollment. CiscoASA(config-ca- trustpoint)#exit CiscoASA(config)#crypto ca enroll CA1 ! Initiates certificate signing request. This is the request to be ! submitted via Web or Email to the third party vendor. % Start certificate enrollment % The subject name in the certificate will be: cn=CiscoASA.cisco.com OU=TSWEB. O=Cisco Systems</pre>

C=US,St=North Carolina,L=Raleigh % The fully-qualified
domain name in the certificate will be:
CiscoASA.cisco.com % Include the device serial number in
the subject name? [yes/no]: <b>no</b>
<pre>! Do not include the device's serial number in the</pre>
subject. Display Certificate Request to terminal?
[yes/no]: <b>y</b>
<pre>! Displays the PKCS#10 enrollment request to the</pre>
terminal. You will need to ! copy this from the
terminal to a text file or web text field to submit to
! the third party CA. Certificate Request follows:
MIICKzCCAZQCAQAwga0xEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEk
MCIGA1UEAxMbQ21zY29BU0EuY21zY28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkcr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXTlPgNAaFMwB2YsTIOn+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBx1/LVLTy3ORqcyy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJDjEuMCwwCwYDVR0PBAQD
AgWgMB0G
A1UdEQQWMBSCEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF
AAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd20LCbXAoP5LlKbPaEeaCkfN/Pp5mATA
sG832TBm
bsxSvljSSXQsQlSb842D6MEG6cu7Bxj/KlZ6MxafUvCHrOPYWVU1wgRJ
Gh+ndCZK j89/Y4S8XhQ79fvBWbR8Ux9emhFHpGHnQ/MpSfU0dQ==
-End - This line not part of the certificate request
Redisplay enrollment request? [yes/no]: <b>n</b>
CiscoASA(config)#

### 步驟3.驗證信任點

收到來自第三方供應商的身份證書後,您可以繼續執行此步驟。

#### ASDM過程

- 1. 將身份證書儲存到本地電腦。
- 2. 如果為您提供了base64編碼的證書,並且該證書不是作為檔案提供的,則必須複製base64消 息並將其貼上到文本檔案中。
- 3. 使用.cer副檔名重新命名檔案注意: 使用.cer副檔名重新命名檔案後, 檔案圖示將顯示為證書



icate Information		
ite is intended for	he following	purpose(s):
the identity of a rem	ote computer	
your identity to a rem	ote computer	
Fi	ficate Information ate is intended for t s the identity of a remo your identity to a remo	ficate Information ate is intended for the following s the identity of a remote computer your identity to a remote computer

4. 按兩下證書檔案。

**:如果**Windows沒有足夠的資訊來驗證此證書消息出現在「常規」選項卡**中,則必須先獲取第 三方供應商根CA或中間CA證書,然後才能繼續此過程。**請聯絡您的第三方供應商或CA管理員 ,以獲取頒發的根CA或中間CA證書。

- 5. 按一下Certificate Path頁籤。
- 6. 點選與您頒發的身份證書關聯的CA證書,然後點選檢視證書。

CiscoASA.cisco.com OU=TSWEB	ral Details Certification Path ertification path	
<u>V</u> iew Certificate	CiscoASA.cisco.com OU=TSWEB	
View Certificate		
<u>V</u> iew Certificate		
		View Certificate
tificate <u>s</u> tatus:	tificate <u>s</u> tatus:	
ate <u>s</u> tatus: rtificate is OK.	ate <u>s</u> tatus: rtificate is OK.	0

CA證書的詳細資訊。

7. 按一下Details以瞭解有關身份證書的詳細資訊。

	Value
- Version	V3
Serial number	611E E59B 0000 0000 0007
Signature algorithm	shalkSA
Suer Suer	CAI, ISweb, cisco, com
Valid Fo	Monday, December 13, 2007
Subject	CiscoASA.cisco.com OLI=TSW.
Public kev	RSA (1024 Bits)

8. 在安裝身份證書之前,必須從CA伺服器下載CA證書並將其安裝在ASA中,如圖所示。完成這些步驟,從名為**CA1**的CA伺服器下載CA憑證。使用提供給VPN伺服器的憑據執行Web登入



Connecting to 172	.16.5.1
User name:	🖸 vpnserver
Password:	•••••
	Remember my password

一下「Download a CA certificate, certificate chain or CRL」以開啟視窗,如下所示。按一下 Base 64單選按鈕作為編碼方法,然後按一下Download CA certificate。

CA伺服器172.16.5.1。

## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA cert

To download a CA certificate, certificate chain, or CRL, select the certificate

## CA certificate:

Curre	nt [CA1]	ſ
10000		
ļ		

Encoding method:

	O D O F	)ER Jase 64		
<u>Download</u> Download Download Download	CA certi CA certi latest ba latest de	<u>ficate</u> ficate chain ise CRL ita CRL		
在電腦上使用	月 <b>certnew</b> .c	er名稱儲存CA證	書。	
File Downloa	ad - Securi	ty Warning		×
Do you w	v <b>ant to ope</b> Name: ( Type: S From:	en or save this f certnew.cer Security Certificate 172.16.5.1	fi <b>le?</b> e, 1.64 KB	
		<u>O</u> pen	<u>S</u> ave	Cancel
U P	/hile files fro otentially ha pen or save	m the Internet can rm your computer. this software. <u>Wh</u> a	be useful, this fi If you do not trus at's the risk?	le type can st the source, do not
9. 瀏覽到儲存C	A證書的位	置。		

- 10. 使用文字編輯器(例如記事本)開啟檔案。按一下右鍵該檔案,然後選擇**「傳送到」>「記事 本**」。
- 11. 系統會顯示與圖中的憑證類似的base64編碼訊息

1

🛃 certnew.cer - Notepad

<u>File Edit Format Help</u>

----BEGIN CERTIFICATE----

MIIEnTCCA4wgAwIBAgIQcJnxmUdk4JxGUdqAowt0nDANBgkqhkiG9w0BAQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT Bqojkiajk/IszAEZFqVUU1dlyjEMMAoGA1UEAxMDQ0ExMB4xDTA3MTIxNDA2MDE0 M1oxDTEyMTIxNDA2MTAxNVowUTETMBEGCqmSJomT8ixkARkWA2NvbTEVMBMGCqmS JOMT8ixkARkWBWNpc2NvMRUwEwYKCZImiŹPyLGQBGRYFVFNXZWIXDDAKBgNVBĀMT A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuvvyiLmA9 BSGzMz3sCtR9TCMw0x7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMijcQnwdOq+ Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXwKh4uC04xxQmr//Sct1tdwQcvk2V uBwCsptW7c1akTqfm5×K/d//z2eUu×rHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDh×x wPXR018CAwEAAaoCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQE AWIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYfNQJ pAP1wDccAQMGA1udHwSB+zcB+DcB9acB8qcB74aBtwxkYXA6Ly8vQ049Q0ExLENO PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdwJsawM]MjBLZXk]MjBTZXJ2aWN]cyxD Tj1TZXJ2aWN]cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9 Y1JMRGlzdHJpYnV0aw9uUG9pbnSGNwh0dHA6Ly90cy13MmszLwFjcy50c3dlYi5j aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHqHUCD9/BZWAqfmGUm++HMljnW8liyIF DCNwxlqxsDT+n9Y0k6bnG6u0f4SgETNrN8EyYVrSGK0lE+0C5L+ytJvw19GZhlzE lovufpa+pt47dmar6uo2v2zbw5kGavLu8GsrFd8wZbpBvMkCqFwNcNItcufu0x1b 1xxc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at ----END CERTIFICATE----

- 12. 在ASDM中,按一下Configuration,然後按一下Device Management。
- 13. 展開Certificate Management, 然後選擇CA Certificates。
- 14. 按一下「**Add**」。
- 15. 按一下**Paste certificate in PEM Format**單選按鈕,然後將第三方供應商提供的base64 CA證書貼上到文本欄位中。
- 16. 按一下「Install Certificate」。

PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPW PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN Y1JMRGlzdHJpYnV0aW9uUG9pbn5GNWh0dHA6Ly90cy13MmszLWFjcy aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQ4 CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HM DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVr5GKOIE+OC5L+ytJv IOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWN4	MjBTZXJ2aWNlcyxD ERDPWNpc2NvLERD 2JqZWN0Q2xhc3M9 zLWFjcy50c3dlYi5j 8gjcVAQQDAgEAMA00 4/DoE4MicbXJeKr m++HMljnW8liyIF 5L+ytJvw19GZhlzE CgFWNcNItcufu0xlb iGPn149zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+p85at	
C Use SCEP:	
SCEP URL: http://	
SCEP URL: http:// Retry Period: 1 minutes	;

命令列示例



BgNVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMW0x7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOg+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUOxRVwhDbMIvwqYBXWKh4uC04xxOmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTgfm5XK/d//z2eUuXrHYvS0CfoFvk1vE6/01o+f0eSS
z+TlDhXx
wPXR018CAwEAAaOCAW8wggFrMBMGCSsGA00BgjcUAg0GHg0A0wBBMAsG
AludDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jgI8RRD
L3mYfNQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWM1MjBLZXk1MjBTZXJ2
aWNlcyxD
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYn1TrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HM1j
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGK0lE+OC5L+ytJvw
19GZhlzE
10VUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
cufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
END CERTIFICATE
quit
! Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: <b>yes</b>
Trustpoint CA certificate accepted.
<pre>% Certificate successfully imported</pre>
CiscoASA(config)#

### <u>步驟4.安裝證書</u>

#### ASDM過程

使用第三方供應商提供的身份證書來完成以下步驟:

- 1. 按一下Configuration,然後按一下Device Management。
- 2. 展開Certificate Management,然後選擇Identity Certificates。
- 3. 選擇您在步驟2中建立的身份證書。註:到期日期顯示為待定。

4. 按一下「Install」。 Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Usage	Add
ASA.cisco.com OU=TS	[Not Available]	Pending	Unknown	Show De
💼 Install Identity	r certificate		×	Delet
Identity Certificate				Expo
C Install from a	file:	Brows	80	Insta
Paste the cer	rtificate data in base-64 forma	st:)		
YZZEM/388E NSLsYWqjkC rPHCh5sZsw IL5nuPsd8Mz END CEF	CUSEMedFb+KYpAFy3PPy4I8 Bg+aUO+WPFk4jICr2XUOK74 9up2PEH2L/O34wm/dpuLuHirr sexBc= RTIFICATE	EHe4MJbdjUp/b9U5I612QP5I51YBUy toWTPFNpfv2x4VF1/Mpcs87ychingKB+6 wWnF1zCnqfcyHcETieZtSt1nwLpsc		
4			<b>&gt;</b>	

按一下Paste the certificate data in base-64 format單選按鈕,然後將第三方供應商提供的身份 證書貼上到文本欄位中。

付 Informat	ion	×	
<b>i</b>	Certificate import succeeded.		
	ОК	÷	將出現

5. 按一下「Install Certificate」。

一個對話方塊,以確認匯入成功。

### 命令列示例

CiscoASA
CiscoASA(config)#crypto ca import CA1 certificate
<pre>! Initiates prompt to paste the base64 identity ! certificate provided by the third party vendor. %The fully-qualified domain name in the certificate will be: CiscoASA.cisco.com Enter the base 64 encoded certificate. End with the word "quit" on a line by itself ! Paste the base 64 certificate provided by the third party vendorBEGIN CERTIFICATE MIIFpzCCBI+gAwIBAgIKYR71mwAAAAAABzANBgkqhkiG9w0BAQUFADBR</pre>
MRMwEQYK CZTmiZDyr COBCEVDV20+MEIWEWVECZTmiZDyr COBCEVEV21zV28vEmam
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0 ZW1zMSOw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ KoZIhvcN

AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWgBTZrb818jq18RRDL3mYfNQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
TjlQdWJs
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJ1dm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3d1Yi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/02xDB
7wXQaGph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/034wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
tlnwLpsc
1L5nuPsd8MaexBc=
END CERTIFICATE
quit
INFO: Certificate successfully imported
CiscoASA(config)#

## 步驟5.將遠端訪問VPN(IPSec)配置為使用新安裝的證書

### ASDM過程

完成以下步驟以配置遠端訪問VPN:

1. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Policies > Add以建立ISAKMP策略配置,如65535所示。

Add IKE Policy					
Priority:	65535	Authentication:	rsa-sig 💌		
Encryption:	3des 💌	D-H Group:	2 💌		
Hash:	md5	Lifetime:	C Unlimited	seconds	•
	ОК	Cancel	Help		

按一下「OK」和「Apply」。

ο

2. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IPSec Transform Sets > Add以建立myset轉換集,如下所示。

Properties			-
Mode:	Tunnel	C Transport	
ESP Encryptio	n: 3D	ES 💌	
ESP Authentic	ation:	>5 💌	

3. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > Crypto Maps > Add,以便使用優先順序為10的動態策略建立加密對映,如下所示。

Interface: outside	-	Policy Type:	dynamic 💌	Priority:	[
Transform Sets					
Transform Set to Be Ad	ded:	m	/set		0006212
ESP-AES-128-SHA	A	dd >>		Mo	ve up
JEST RES 120 STR	R	emove		Moy	e Dov
				D	
-Peer Settings - Option	al for Dynamic Cr	ypto Map Entries			

按一下「**OK**」和「**Apply**」。**注意:**ASA 8.0不支援SHA 2。此外,不支援使用具有256雜湊值 的證書的IPSec客戶端。

4. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > Group Policies > Add以建立Defaultgroup組策略,如下所示。 Add Internal Group Policy

General	Name: defa	ultgroup				
Servers     Advanced	Banner: 🔽 Ir	herit				
	Address Pools: 🔽 In	herit				
	More Options					
	Tunneling Protocols	: 🔽 Inherit	Clientless SSL VPN	F SSL VPN Client	🕅 IPsec	
	Filter	🔽 Inherit			T	Ma

按一下「OK」和「Apply」。

5. 選擇Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools > Add, 為要動態分配的VPN客戶端使用者配置vpnpool地址池。

Name:	vpnpool
Starting IP Address:	10.5.5.10
Ending IP Address:	10.5.5.20
Subnet Mask:	255.255.255.0
ОК	Cancel Help

6. 選擇Configuration > Remote Access VPN > AAA Setup > Local Users > Add,以便為VPN客 戶端訪問建立vpnuser使用者帳戶。此外,將此使用者設為DefaultRAGroup的成員。

Image: Image
WPN Policy Username: Vpnuser Password: ****** Confirm Password: *******  User authenticated using MSCHAP Member-of Member-of: Delete Delete
Password: ****** Confirm Password: ****** Confirm Password: ****** User authenticated using MSCHAP Member-of Member-of Member-of: Delete Delete
Confirm Password: ******  Confirm Password: ******  User authenticated using MSCHAP  Member-of  Member-of:  DefaultRAGroup
User authenticated using MSCHAP       Member-of       Add >>       Member-of:
Member-of Member-of: DefaultRAGroup DefaultRAGroup
Add >>     DefaultRAGroup       Member-of:     Delete
Access Pectriction
Select one of the options below to sectivist ACDM, CSH, Telephined Consele access
Select one or the options below to restrict ASDM, SSH, Teinet and Console access.
Note: All users have network access, regardless or these settings.
<ul> <li>Full access(ASDM, SSH, Telnet and Console)</li> </ul>
Privilege level is used with command authorization.
Privilege Level: 2
C CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.
C No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

7. 選擇Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Edit以編輯DefaultRAGroup,如下所示。從IKE Peer Authentication欄位的下拉選單

# 中選擇適當的身份證書。在User Authentication欄位中選擇伺服器組作為LOCAL。選擇 vpnpool作為Client Address Assignment欄位的Client Address Pool。為「預設組策略」欄位 選擇defaultgroup作為「組策略」。

选择Gelauli	JIOUPTE	向 祖宋『	「白」。	
💼 Add IPsec	Remote A	Access Coni	nection Profile	2

Basic	Name:	DefaultRAGroup
General Client Addressing Authentication Authorization	IKE Peer Authentication Pre-shared Key: Identity Certificate:	[cn=CiscoASA.cisco.com OU\=TSWEB, o=Cisco Systems,▼
Accounting PPP	User Authentication — Server Group: Fallback:	LOCAL  Use LOCAL if Server Group fails
	Client Address Assigmer DHCP Servers: Client Address Pools:	it vpnpool
	Default Group Policy — Group Policy: Client Protocols:	defaultgroup

按一下「OK」和「Apply」。

## 命令列示例

CiscoASA
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)#exit
CiscoASA(config)#crypto isakmp identity auto
<pre>! Phase 1 Configurations CiscoASA(config)#crypto</pre>
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map dynmap 10 set
transform-set myset
CiscoASA(config)#crypto map mymap 10 ipsec-isakmp
dynamic dynmap
CiscoASA(config)#crypto map mymap interface outside
<pre>! Phase 2 Configurations CiscoASA(config)#group-</pre>
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)# <b>default-domain value</b>
cisco.com
CiscoASA(config-group-policy)# exit
<pre>! Create a group policy "defaultgroup" with domain</pre>



## <u>ASA配置摘要</u>

#### CiscoASA

```
CiscoASA#show running-config
: Saved
ASA Version 8.0(2)
1
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
1
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
1
interface Ethernet0/2
 nameif DMZ
 security-level 90
 ip address 10.77.241.142 255.255.255.192
1
interface Ethernet0/3
```

shutdown no nameif no security-level no ip address I interface Management0/0 shutdown no nameif no security-level no ip address 1 passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name cisco.com access-list 100 extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0 255.255.255.0 pager lines 24 mtu outside 1500 mtu inside 1500 mtu DMZ 1500 ip local pool vpnpool 10.5.5.10-10.5.5.20 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 nat (inside) 0 access-list 100 route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1 route outside 10.1.1.0 255.255.255.0 192.168.1.1 1 route outside 172.16.5.0 255.255.255.0 192.168.1.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 DMZ http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set myset esp-3des esp-md5-hmac crypto dynamic-map dynmap 10 set transform-set myset crypto map mymap 10 ipsec-isakmp dynamic dynmap crypto map mymap interface outside crypto ca trustpoint CA1 enrollment terminal subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems, C=US, St=North Carolina,L=Rale serial-number keypair my.CA.key crl configure crypto ca certificate chain CA1 certificate 611ee59b000000000007 308205a7 3082048f a0030201 02020a61 lee59b00 00000000 07300d06 092a8648

86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31 15301306 0a099226 8993f22c 64011916 05636973 636f3115 3013060a 09922689 93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 le170d30 37313231 35303833 3533395a 170d3039 31323134 30383335 33395a30 76310b30 09060355 04061302 55533117 30150603 55040813 0e4e6f72 74682043 61726f6c 696e6131 10300e06 03550407 13075261 6c656967 68311630 14060355 040a130d 43697363 6f205379 7374656d 73312430 22060355 0403131b 43697363 6f415341 2e636973 636f2e63 6f6d204f 553d5453 57454230 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 b8e20aa8 332356b7 5b660073 5008d373 5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754 5e7f98d3 d4239b42 ab8faf0b e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a b94b18ef 308eb12f 22ab1a8e db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9 03f722bd 414b0a32 05aa053e c45e2464 80606f8e 417f09a7 aa9c644d 02030100 01a38202 de308202 da300b06 03551d0f 04040302 05a0301d 0603551d 11041630 14821243 6973636f 4153412e 63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb 490cde1a fe2d63e3 lelfb28c 974c4216 301f0603 551d2304 18301680 14d9adbf 08f23a88 f114432f 79987cd4 09a403e5 58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081 ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453 2d57324b 332d4143 532c434e 3d434450 2c434e3d 5075626c 69632532 304b6579 25323053 65727669 6365732c 434e3d53 65727669 6365732c 434e3d43 6f6e6669 67757261 74696f6e 2c44433d 54535765 622c4443 3d636973 636f2c44 433d636f 6d3f6365 72746966 69636174 65526576 6f636174 696f6e4c 6973743f 62617365 3f6f626a 65637443 6c617373 3d63524c 44697374 72696275 74696f6e 506f696e 74863568 7474703a 2f2f7473 2d77326b 332d6163 732e7473 7765622e 63697363 6f2e636f 6d2f4365 7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06 01050507 01010482 010f3082 010b3081 a906082b 06010505 07300286 819c6c64 61703a2f 2f2f434e 3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230 4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143 65727469 66696361 74653f62 6173653f 6f626a65 6374436c 6173733d 63657274 69666963 6174696f 6e417574 686f7269 7479305d 06082b06 01050507 30028651 68747470 3a2f2f74 732d7732 6b332d61 63732e74 73776562 2e636973 636f2e63

6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b 332d4143 532e5453 5765622e 63697363 6f2e636f 6d5f4341 312e6372 74302106 092b0601 04018237 14020414 1e120057 00650062 00530065 00720076 00650072 300c0603 551d1301 01ff0402 30003013 0603551d 25040c30 0a06082b 06010505 07030130 0d06092a 864886f7 0d010105 05000382 0101008a 82680f46 fbc87edc 84bc45f5 401b3716 0045515c 2c81971d 0da51fe3 96870627 b41b4319 23284b30 5eafcedb 10c1ef05 d0686a61 cd1ab877 100b965d 499088e1 7de418fb b5529199 46129b81 9c4353a2 1761b61c f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433 bddef040 b4b0431e 7456fe29 8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74 97997a23 340fe65e 75601d32 3522ec61 6aa39020 60f9a50e f963c593 88c80abd 9750e2bb e285933c 53697efd ble15148 fcca5cb3 cef27219 e0281fbc acf1c285 2b19b30f 6ea733c4 1f62ff3b 7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87 7044e279 9b52b759 f02e9b1c 94be67b8 fb1df0c6 9ec417 quit certificate ca 7099f1994764e09c4651da80a16b749c 3082049d 30820385 a0030201 02021070 99f19947 64e09c46 51da80a1 6b749c30 0d06092a 864886f7 0d010105 05003051 31133011 060a0992 268993f2 2c640119 1603636f 6d311530 13060a09 92268993 f22c6401 19160563 6973636f 31153013 060a0992 268993f2 2c640119 16055453 57656231 0c300a06 03550403 13034341 31301e17 0d303731 32313430 36303134 335a170d 31323132 31343036 31303135 5a305131 13301106 0a099226 8993f22c 64011916 03636f6d 31153013 060a0992 268993f2 2c640119 16056369 73636f31 15301306 0a099226 8993f22c 64011916 05545357 6562310c 300a0603 55040313 03434131 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101 00ea8fee c7ae56fc a22e603d 0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d 28ece906 02902f9a d1eb2b8d f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd ale906ec 88b32a19 38e5353e 6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621 876bd678 c8a37109 f074eabe 2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7 24b9e054 063c60a4 9b8d3c09 351bc630 05f69357 833b9197 f875b408 cb71a814 69a1f331 b1eb2b35 0c469443 1455c210 db308bf0 a9805758 a878b82d 38c71426 afffd272 dd6d7564 1cbe4d95 b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67 94b97ac7 63249009 fa05ca4d 6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b 5f020301 0001a382 016f3082 016b3013 06092b06 01040182 37140204 061e0400 43004130 0b060355 1d0f0404 03020186 300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414 d9adbf08 f23a88f1 14432f79 987cd409 a403e558 30820103 0603551d 1f0481fb 3081f830 81f5a081 f2a081ef 8681b56c 6461703a 2f2f2f43 4e3d4341 312c434e 3d54532d 57324b33 2d414353 2c434e3d 4344502c 434e3d50 75626c69 63253230 4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f636572 74696669 63617465 5265766f 63617469 6f6e4c69 73743f62 6173653f 6f626a65 6374436c 6173733d 63524c44 69737472 69627574 696f6e50 6f696e74 86356874 74703a2f 2f74732d 77326b33 2d616373 2e747377 65622e63 6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f 4341312e 63726c30 1006092b 06010401 82371501 04030201 00300d06 092a8648 86f70d01 01050500 03820101 001abc5a 40b32112 22da80fb bb228bfe 4bf8a515 df8fc3a0 4e0c89c6 d725e2ab 2fa67ce8 9196d516 dfe55627 953aea47 2e871289 6b754e9c le01d408 3f7f0595 8081f986 526fbelc c9639d6f 258b2205 0dc370c6 5431b034 fe9fd60e 93a6e71b ab8e7f84 a011336b 37c13261 5ad218a3 a513e382 e4bfb2b4 9bf0d7d1 99865cc4 94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92 860152d4 f06b2b15 df306433 c1bcc282 80558d70 d22d72e7 eed3195b d575dceb c0caa196 34f693ea f3beee4d aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76 13018f9f 5e3dce95 efe6da93 f4cb3b00 102efa94 48a22fc4 7e342031 2406165e 39edc207 eddc6554 3fa9f396 ad quit crypto isakmp enable outside crypto isakmp policy 65535 authentication rsa-sig encryption 3des hash md5 group 2 lifetime 86400 crypto isakmp identity auto telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection\_default match default-inspection-traffic 1 1 policy-map type inspect dns preset\_dns\_map parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns preset\_dns\_map inspect ftp inspect h323 h225

inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
1
service-policy global_policy global
group-policy defaultgroup internal
group-policy defaultgroup attributes
default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#

## <u>VPN客戶端配置</u>

完成以下步驟以配置VPN客戶端。

- . Accessories Programs Internet Explorer Cisco Systems VPN Client 🔸 🚰 Uninstall VPN Client Documents ¥ VPN Client Settings Cisco Systems Inc. VPN Client Search Help Run... Shut Down... 🕄 Start 🛛 🧭 🚾 🔂 🖉 🖾 C:\WINNT\sys... 🔂 Prabu Microsoft Certi... Muntitled - Paint Ø
- 1. 選擇Start > Programs > Cisco Systems VPN Client > VPN Client以啟動VPN客戶端軟體。

2. 完成這些步驟,從名為**CA1**的CA伺服器下載CA憑證,並將其安裝到Cisco VPN使用者端。使 用提供給vpnuser的憑據執行Web登入CA伺服器172.16.5.1。

=ile	Edit	View	Favorites	Tools	Help				
<b>H</b> Ba	ack 🔻	÷ -	🛞 🙆 🙆	3 Q S	Search	😹 Favorites	Media	3	

	Enter Net	vork Passwor	ʻd				
	<u> (</u>	Please type yo	our user name a	nd password.			
	8	Site:	172.16.5.1	_			
		User Name	vpnuser				
		Password	*****	J			
		Domain					
		🗖 Save this j	password in you	ır password lis	t		
				OK		Car <mark>注意:</mark>	蹜保您在
CA伺服器 <b>certificate</b>	中擁有VPN <sup>s</sup> chain or CR	客戶端使用者的 L」以開啟視習	的使用者帳戶。 窗,如下所示。	按一下「D 按一下Base	ownload a e 64單選按	CA certificat 鈕作為編碼	<b>'e,</b> 方法,然

後按一下Download CA certificate。

## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA cert

To download a CA certificate, certificate chain, or CRL, select the certificate

### CA certificate:

[CA1]	
	[CA1]

Encoding method:

	O DER O Base 64
Download	CA certificate
Download	CA certificate chain
Download	latest base CRL
Download I	latest delta CRL

在電腦上使用certnew.cer名稱儲存CA證書。預設情況下,它儲存在C:\Program Files\Cisco Systems\VPN Client路徑中。

File Dow	nload	and the second second				
?	Some files can H looks suspicious save this file.	arm your computer. If th ;, or you do not fully trust	e file informatio the source, do	on below o not open or		
	File name:	certnew.cer				
	File type:	Security Certificate				
	From:	172.16.5.1				
	A This type of malicious of	f file could harm your co ode.	mputer if it con	tains		
	Would you like (	o open the file or save it	to your compu	iter?		
	<u>O</u> pen	<u>Save</u> (	Cancel	More Info	在VPN客戶端中	. 選
擇 <b>Certific</b> 位置c:\Pr	ates頁籤> Impo	rt,然後按一下Import	t <b>from</b> Filerad 匯入CA證書	io按鈕。按一 ,如下所示。	下Browse以從信 按一下「Import	, <u>一</u> 諸存 」

(匯入)。此時將顯示成功視窗,如圖所示。

👌 status: Disco	nnected   VI	PN Client	- Version 4.	8.02.0010		
Connection Entrie	s Status Ce	rtificates	Log Option:	; Help		
View Connection Entrie	Import I	Export	Enroll	Verify	Delete	
Number	Certificat	-   <sup>20</sup> 9		Sto	10 /	Keu Size
	lient   Impo	ort Certifi	cate	n		i key size
In	nport Path	n Files\Cisc	co Systems\V	PN Client\cei	thew.cer	<u>B</u> rowse
C Impor	t from <u>M</u> icrc Certificate:	VPN Clie	ent Certificate suc	cessfully imp	orted.	¥.
Enterin identity	ig a new pa certificates.		OK.		sswo	ord protect
<u>N</u> ev <u>C</u> onfim	v Password:   n Password:					
Certificates頁籤F	中,出現CA C	ertificates	s CA1,如下	所示。	Import	Cancel 在
Connection Entries Sta View Import	atus Certificates	Log Option	ns Help Yerify	Delete		cisco
Connection Entries	Certificates Log	]				LV P.D.
	Certificate		CA	2	ley Size 048	until Dec 14, 2012 11 4

**注意:**確保已選擇**Show CA/RA Certificates**選項(如圖所示),否則CA證書不得出現在證書

실 status: Disconn	ected	VPI	N Client	- Yei	sion 4.8	.02.0010
Connection Entries	<u>S</u> tatus	Cer	tificates	Log	Options	Help
<b>S</b>	7		View			
View Imp Connection Entries	iort Certif		Export.			
0	CA1		Verif <u>y</u> D <u>e</u> lete			
			⊆hange <u>R</u> etriev/	Certi e App	ficate Pas roved Cer	sword tificate
	1	~	Show C	A/RA	Certificat	es )

視窗中。

 完成以下步驟,即可下載身份證書並將其安裝到VPN客戶端。在CA伺服器CA1中,選擇 Request a Certificate > advanced certificate request > Create並向此CA提交請求以註冊身份 證書。按一下「Submit」。

Certificate Template:
User
Key Options:
Create new key set C Use existing key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0 💌
Key Usage: 🧔 Exchange
Key Size: 1024 Min: 384 (common key sizes: <u>512 1024 2048 4096 8192 16384</u> ) Max:16384
Automatic key container name O User specified key container name
✓ Mark keys as exportable □ Export keys to file
Enable strong private key protection
I Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.
Additional Options:
Request Format: CCMC © PKCS10
Hash Algorithm: MD5 💽 Only used to sign request.
Save request to a file
按一下「 <b>Yes</b> 」以繼續。
Potential Scripting Violation
This web site is requesting a new certificate on your behair. You should allow only trusted web sites to request a certificate for you behair. You should allow only trusted web sites to request a certificate for you behair.
Yes No
按一下「I <b>nstall this Certificate」。</b> <i>Microsoft</i> Certificate Services CA1
Certificate Issued

The certificate you requested was issued to you.

Install this certificate

#### Potential Scripting Violation

This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

	Yes	No	
您必須收到證書安裝消息,如圖所示。	0		
Microsoft Certificate Services	CA1		

## Certificate Installed

Your new certificate has been successfully installed. 退出VPN客戶端並重新啟 動它,以使安裝的身份證書開始顯示在VPN客戶端的證書頁籤中,如下所示。

View Imp	Status Certific	ates Log Option:	s Help	te	ululu cisco
Connection Entries	Certificates	Log			
Number	Certificate		Store /	Key Size	Validity
	CA1		CA	2048	until Dec 14, 2012 11:40:
	Users + vpnu	ser	Microsoft	1024	until Dec 26, 2008 18:27:

4. 在Connection entries頁籤中,按一下New以建立連線條目vpnuser,如下所示。在Host欄位中 輸入遠端對等IP地址(可路由)。按一下Certificate Authentication單選按鈕,然後從下拉式清 單中選擇身分憑證,如下所示。按一下「Save」。

onnection Entrys	vpnuser					
				Sec. 1	Variation	
Description:				- IIII	0	
Host:	192.168.1.5	)				
Authentication	Transport	Backup Servers	: Dial-Up			
C Group Authe	ntication		C Mutual G	iroup Authentica	tion	
Name:						
Password:					_	
Confirm Passo	vord:					
Certificate A	uthentication		1			
Certificate A	uthentication					
<ul> <li>Certificate Ar</li> <li>Name: 0 - 0:</li> </ul>	uthentication sers + vpnuser (	Microsoft)				
<ul> <li>Certificate Au Name: 0 - U</li> <li>Send CA</li> </ul>	uthentication sers + vpnuser ( Certificate Chair	Microsoft)				
<ul> <li>Certificate Ar</li> <li>Name: 0 - U</li> <li>Send CA</li> </ul>	uthentication sers + vpnuser Certificate Chair	Microsoft)				
<ul> <li>Certificate Ar</li> <li>Name: 0 - U</li> <li>Send CA</li> </ul>	uthentication sers + vpnuser Certificate Chair	Microsoft)			-	
<ul> <li>Certificate Ar</li> <li>Name: 0 - U</li> <li>Send CA</li> <li>Erase User Pass</li> </ul>	uthentication sers + vonuser Certificate Chair word	Microsoft)	Save	Canc	el	
<ul> <li>Certificate Ar Name: 0-U</li> <li>□ Send CA</li> <li>Erase User Pass</li> <li>安一下「Conne</li> </ul>	uthentication sers + vonuser Certificate Chair word st_l	Microsoft)	Save	Canc	el	
<ul> <li>Certificate Ar Name: 0-U</li> <li>Name: 0-U</li> <li>Send CA</li> <li>Erase User Pass</li> <li>安一下「Conne</li> <li>status: Disconne</li> <li>connection Entries S</li> </ul>	uthentication sers + vonuser Certificate Chair word cto cted   VPN Client tatus_Certificates	Microsoft)	Save	Canc	el	
<ul> <li>Certificate Ar Name: 0・U</li> <li>Name: 0・U</li> <li>Send CA</li> <li>Erase User Pass</li> <li>安一下「Conne</li> <li>status: Disconne</li> <li>Connection Entries S</li> </ul>	uthentication ers + vonuser Certificate Chair word ct_J o cted   VPN Client tatus Certificates	Microsoft)	Save	Canc	el	
<ul> <li>Certificate Ar Name: 0・U</li> <li>Name: 0・U</li> <li>Send CA</li> <li>Erase User Pass</li> <li>安一下「Conne</li> <li>status: Disconne</li> <li>Connection Entries S</li> <li>Connection Entries S</li> </ul>	uthentication sers + vonuser Certificate Chair word ot_J o cted   VPN Client tatus Certificates EXAMPLE IN CLIENT tatus Certificates	Microsoft)	Save	Canc	el	
<ul> <li>Certificate Ar Name: 0・U</li> <li>Name: 0・U</li> <li>Send CA</li> <li>Erase User Pass</li> <li>安一下「Conne</li> <li>status: Disconne</li> <li>connection Entries S</li> <li>Connection Entries</li> </ul>	uthentication sers + vonuser Certificate Chair word ct_l o cted   VPN Client tatus Certificates ew Import Certificates   Lo	Microsoft)	DIO Save	Canc	el	
<ul> <li>Certificate Ar Name: 0・U</li> <li>Name: 0・U</li> <li>Send CA</li> <li>Erase User Pass</li> <li>安一下「Conne</li> <li>status: Disconne</li> <li>Connection Entries S</li> <li>Connection Entries</li> <li>Connection Entries</li> </ul>	uthentication sers + vonuser Certificate Chair word ot_l o cted   VPN Client tatus Certificates www	Microsoft)	D10 Host	Canc	el	

6. 出現提示時,輸入xauth的使用者名稱和密碼資訊,然後按一下OK以運線到遠端網路。

Enter Username and Password.	user	
Password:	****	
	ОК	Cancel
. VPN客戶端連線到ASA,如圖所示 logstatus: Connected   VPN Client	• - Version 4.8.01.0300	

Connection Entries Status Certificates Log Options Help



在ASA上,您可以在命令列發出幾個show命令,以驗證證書的狀態。

使用本節內容,確認您的組態是否正常運作。

```
• show crypto ca trustpoint命令顯示已配置的信任點。
 CiscoASA#show crypto ca trustpoints
 Trustpoint CA1:
     Subject Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
           Serial Number: 7099f1994764e09c4651da80a16b749c
     Certificate configured.

    show crypto ca certificate命令會顯示系統上安裝的所有證書。

 CiscoASA# show crypto ca certificate
 Certificate
   Status: Available
   Certificate Serial Number: 3f14b70b0000000001f
   Certificate Usage: Encryption
   Public Key Type: RSA (1024 bits)
   Issuer Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
   Subject Name:
     cn=vpnserver
     cn=Users
     dc=TSWeb
     dc=cisco
     dc=com
   PrincipalName: vpnserver@TSWeb.cisco.com
   CRL Distribution Points:
     [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
     CN=Services, CN=Configuration, DC=TSWeb, DC=cisco,
     DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
     [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
   Validity Date:
     start date: 14:00:36 UTC Dec 27 2007
     end date: 14:00:36 UTC Dec 26 2008
   Associated Trustpoints: CA1
```

```
CA Certificate
   Status: Available
   Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
   Certificate Usage: Signature
   Public Key Type: RSA (2048 bits)
   Issuer Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
   Subject Name:
     cn=CA1
     dc=TSWeb
     dc=cisco
     dc=com
   CRL Distribution Points:
     [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
     CN=Services, CN=Configuration, DC=TSWeb, DC=cisco,
     DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
     [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
   Validity Date:
     start date: 06:01:43 UTC Dec 14 2007
     end date: 06:10:15 UTC Dec 14 2012
   Associated Trustpoints: CA1
 Certificate
   Subject Name:
     Name: CiscoASA.cisco.com
   Status: Pending terminal enrollment
   Key Usage: General Purpose
   Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
   Associated Trustpoint: CA1
• show crypto ca crls命令會顯示快取的憑證撤銷清單(CRL)。

    show crypto key mypubkey rsa命令顯示所有生成的加密金鑰對。

 CiscoASA# show crypto key mypubkey rsa
 Key pair was generated at: 01:43:45 UTC Dec 11 2007
 Key name: <Default-RSA-Key>
  Usage: General Purpose Key
  Modulus Size (bits): 1024
  Key Data:
   30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
   99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
   f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
   4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
   2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
 Key pair was generated at: 06:36:00 UTC Dec 15 2007
 Key name: my.CA.key
  Usage: General Purpose Key
  Modulus Size (bits): 1024
  Key Data:
   30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
   a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
   545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
   5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
   d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
 Key pair was generated at: 07:35:18 UTC Dec 21 2007
 CiscoASA#
```

#### show crypto isakmp sa命令顯示IKE 1隧道資訊。

CiscoASA#show crypto isakmp sa

```
Active SA: 1
       Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
    Total IKE SA: 1
      IKE Peer: 10.1.1.5
    1
       Type : user
                                 Role
                                        : responder
                                       : MM_ACTIVE
        Rekey
               : no
                                 State

    show crypto ipsec sa命令顯示IPSec隧道資訊。

    CiscoASA#show crypto ipsec sa
    interface: outside
        Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5
         local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
         remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
          current_peer: 10.1.1.5, username: vpnuser
         dynamic allocated peer ip: 10.5.5.10
          #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
          #pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
          #pkts compressed: 0, #pkts decompressed: 0
          #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
          #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
          #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
          #send errors: 0, #recv errors: 0
         local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5
         path mtu 1500, ipsec overhead 58, media mtu 1500
         current outbound spi: FF3EEE7D
        inbound esp sas:
          spi: 0xEFDF8BA9 (4024404905)
            transform: esp-3des esp-md5-hmac none
            in use settings ={RA, Tunnel, }
            slot: 0, conn_id: 4096, crypto-map: dynmap
            sa timing: remaining key lifetime (sec): 28314
             IV size: 8 bytes
            replay detection support: Y
        outbound esp sas:
          spi: 0xFF3EEE7D (4282314365)
            transform: esp-3des esp-md5-hmac none
            in use settings ={RA, Tunnel, }
            slot: 0, conn_id: 4096, crypto-map: dynmap
            sa timing: remaining key lifetime (sec): 28314
             IV size: 8 bytes
            replay detection support: Y
輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show指令輸出的分析
```

```
o
```

## <u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

以下是您可以遇到的一些可能錯誤:

 錯誤:無法分析或驗證匯入的證書安裝身份證書並且沒有用關聯的信任點進行身份驗證的正確 的中間或根CA證書時,可能出現此錯誤。您必須移除並使用正確的中間CA或根CA證書重新進 行身份驗證。請與您的第三方供應商聯絡,以驗證您是否收到了正確的CA證書。

- •證書不包含通用公鑰當您嘗試將身份證書安裝到錯誤的信任點時,可能會發生此錯誤。您試圖 安裝無效的身份證書,或者與信任點關聯的金鑰對與身份證書中包含的公鑰不匹配。發出show crypto ca certificates trustpointname命令,以驗證您是否將身份證書安裝到正確的信任點。查 詢說明Associated Trustpoints:如果列出的信任點不正確,請使用本文檔中介紹的過程來刪除並 重新安裝適當的信任點。此外,請確認自產生CSR後,金鑰對沒有變更。
- 錯誤:ASA/PIX。Sev=Warning/3 IKE/0xE:3000081程憑證ID無效:如果證書存在身份驗證問 題,此錯誤消息可能出現在VPN客戶端中。在ASA/PIX配置中使用命令crypto isakmp identity auto以解決此問題。

## 相關資訊

- <u>思科自適應安全裝置支援頁面</u>
- Cisco VPN使用者端支援頁面
- 將Microsoft Server配置為證書頒發機構(CA)
- 技術支援與文件 Cisco Systems