配置Cisco VPN 3000 Concentrator 4.7.x以獲取 數位證書和SSL證書

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>在VPN集中器上安裝數位證書</u> <u>在VPN集中器上安裝SSL證書</u> <u>在VPN集中器上續訂SSL證書</u> 相關資訊

<u>簡介</u>

本文檔包含有關如何配置Cisco VPN 3000系列集中器以使用數字或身份證書和SSL證書進行身份驗 證的逐步說明。

注意:在VPN集中器中,必須在生成另一個SSL證書之前禁用負載平衡,因為這樣可以防止證書生成。

請參閱<u>如何使用ASA上的ASDM從Microsoft Windows CA獲取數位證書</u>,以瞭解有關PIX/ASA 7.x的 相同方案的詳細資訊。

請參閱<u>使用增強型註冊命令的Cisco IOS證書註冊配置示例</u>,以瞭解更多有關Cisco IOS®平台相同 方案的資訊。

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文檔中的資訊基於運行版本4.7的Cisco VPN 3000集中器。

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。

<mark>請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u></mark>

在VPN集中器上安裝數位證書

請完成以下步驟:

1. 選擇Administration > Certificate Management > Enroll 以選擇數位證書或身份證書請求。

Administration Certificate Management Enroll
This section allows you to create an SSL or identity certificate request. The identity certificate request allows the VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, which will issue a certificate. The CA's certificate must be installed as a Certificate Authority before installing the certificate you requested.
Choose the type of certificate request to create:
Identity certificate SSL certificate
<< Go back to Certificate Management

2. 選擇Administration > Certificate Management > Enrollment > Identity Certificate,然後按一下 Enroll via PKCS10 Request(Manual)。

Administration | Certificate Management | Enroll | Identity Certificate

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. <u>Click here to install a new CA using SCEP before enrolling</u>.

Enroll via PKCS10 Request (Manual)

- Enroll via SCEP at RSAv57RootMD5srvCN
- Enroll via SCEP at TestCA6-8 at Cisco

<< Go back and choose a different type of certificate

 填寫請求的欄位,然後按一下Enroll。本示例中填寫了這些欄位。常用名稱 — altiga30組織單 位 — IPSECCERT(OU應與配置的IPsec組名匹配)組織- Cisco Systems位置- RTP州/省 — 北卡羅萊納國家 — 美國完全限定域名 — (此處未使用)金鑰大小 — 512注意:如果使用「 簡單證書註冊協定」(SCEP)請求SSL證書或身份證書,則只有這些RSA選項可用。RSA 512位RSA 768位RSA 1024位RSA 2048位DSA 512位DSA 768位DSA 1024位

Administration Certificate Management Enroll Identity Certificate PKCS10				
Enter the information to be included in the certificate request. The CA's certificate must be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.				
Common Name (CN) altiga30	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.			
Organizational Unit (OU) IPSECCERT	Enter the department.			
Organization (O) Cisco Systems	Enter the Organization or company.			
Locality (L) RTP	Enter the city or town.			
State/Province (SP) NorthCarolina.	Enter the State or Province.			
Country (C) US	Enter the two-letter country abbreviation (e.g. United States = US).			
Subject AlternativeName (FQDN)	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.			
Subject AlternativeName (E- Mail Address)	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.			
Key Size RSA 512 bits 💌	Select the key size for the generated RSA/DSA key pair.			
Enroll Cancel				

4. 按一下Enroll後,將顯示多個視窗。第一個視窗確認您已請求證書。

Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated. In a few seconds, a new browser window will open up with the certificate request. The request can be saved as a file, or copied then pasted into a CA's management interface.

The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file; go to the <u>File Management page</u> to delete the certificate request.

- Go to Certificate Management
- · Go to Certificate Enrollment

Г

Go to Certificate Installation

還會開啟一個新的瀏覽器視窗,並顯示您的PKCS請求檔案。

https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer	-DX
File Edit View Favorites Tools Help	- 19
(← Back - → - 🔘 🛐 🚮 🔞 Search 💿 Favorites ଔMedia 🔇 🖏 - 🚑 🗐 🗐 🔞	
Address 🙆 https://172.18.124.214/FILE/pkcs0001.txt 🔹 🔗 Go	Links »
iwon - 🗞 - 📕 🔽 🔤 Search - 🚧 🏧 Won - 🖂 Email 🐼 Money -	More [⊉]
NASCAQ®	
BEGIN NEW CERTIFICATE REQUEST MIIBKDCBOwIBADByMREwDwYDVQQDEwhhbHRpZ2EzMDESMBAGA1UECxMJSVBTRUND RVJUMRYwFAYDVQQKEw1DaXNjbyBTeXNOZW1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAgTDUSvcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQYJKoZIhvcNAQEBBQAD SQAwRgJBAIaj+mtJ/UozTMMwO1oNMiqw4kmgIhIG2E/BIZc+xokG4rBpl1rq4DkM J3XOVB8y1Ukzjvdlgh+ckmjBaiqy3I8CAQUwDQYJKoZIhvcNAQEEBQADQQAurnDB DOdRWJg/dVvGAMZHKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqaSNv1cdLsQFPxV1 zV1eLhhpRf0A4hw1 END NEW CERTIFICATE REQUEST	4
	-
🕘 Done	

5. 在證書頒發機構(CA)伺服器上,突出顯示請求並將其貼上到CA伺服器以提交請求。按「 Next」(下一步)。

Microsoft Certificate Services - Microsoft Internet Explorer		1
File Edit View Pavorites Tools Help		
4-Back + + · () [] [] [] Search @Favorites @History] +]		
Address Dhttp://172.10.124.96/certsrv/	-	10 C
Microsoft Certificate Services - jfrahim-pc	tit in in	Home
Welcome		
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once yo will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-m depending upon the type of certificate you request.	ou acquire a certifica nail messages, and	ate, you more
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate		
	N	< txel

6. 選擇Advanced request,然後按一下Next。

Microsoft Certificate Services - Microsoft Internet Explorer	_ii
File Edit View Favorites Tools Help	
4-Back + + - ◎ ③ ④ ④ Search ⊕Favorites @History ◎ + @	
Address Abhtp://172.18.124.96/certsrv/certrqus.asp	
Microsoft Certificate Services jfrahim-pc	Home
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request.	
Web Browser Centionte E-Mail Protection Certificate	
Advanced request	
	Next >

7. 選擇Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file, 然後按一下Next。

Microsoft Certificate Services - Microsoft Internet Explorer			-10
File Edit View Favorites Tools Help			
4+Back + → - ② (2) (2) Search (a) Favorites (3)History (2) + (3)			
Address R http://172.18.124.96/certsrv/certrgad.asp	٠	PG	Lin
Microsoft Certificate Sentces jfrahim-pc		-)	fome
Advanced Certificate Requests			
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of authority (CA) will determine the certificates that you can obtain.	the ce	rtifica	ation
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS	#7 file	í,	
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user. 			
	N	< bos	

8. 將PKCS檔案剪下並貼上到Saved Request部分下的文本欄位中。然後按一下Submit。

Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		
4-Back - → - ◎ 3 ④ @Search @Favorites @History 03- @		
Address 🖉 http://172.18.124.96/certsrv/certrqut.asp		(2 GO 11
Microsoft Certificate Services ifrahim-pc		Hom
Submit A Saved Request		
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external as server) into the request field to submit the request to the certification authority (CA).	pplication (such as a	i web
Saved Request:		
Bace64 Encoded Certificate Request (PWCS #10 or #?): *		
Etowse for a file to insert.		
Additional Attributes:		
	Su	bmit≯

9. 在CA伺服器上頒發身份證書。

Certification Authority							_ 5
Action Yew ↓ 💠 → 💽 💽		ľ					
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
Certification Authority (Local)	167 1	BEGIN M	Takan Iboles Schoolstop Al Tasks I Issue Refresh Help	3/23/2001 9:13 AM	GHOSTEMUSR	. 05	Cisco Syste

10. 下載根和身份證書。在CA伺服器上,選擇**Check on a pending certificate**,然後按一下 Next。

Microsoft Certilicate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
\$+8ad - + - O 2 2 2 Caserth @Favorites Gristory 03- 3	
dåress 🕘 http://172.18.324.96/certsrv/	- eres
Microsoft Centificate Services Itrahim-pc	Hor
Nelcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. O will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt yo depending upon the type of certificate you request.	Once you acquire a certificate, you our e-mail messages, and more
Select a task:	
C Retrieve the CA certificate or certificate revocation list	
Request a certificate	
Check on a pending certificate	
	Next >

11. 選擇Base 64 encoded,然後按一下Download CA certificate on the CA server。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
2-Back + + - 2 2 3 3 2 Search Braverites Steatory 2- 3	
Address Attp://172.18.124.96/certsrv/certfrsh.asp	
Microsoft Certificate Services jfrahm-pc	Home
Certificate Issued	
The certificate you requested was issued to you. C DER encoded or C Base 64 encoded Download CA certificate Download CA certification path	
·	

12. 將身份證書儲存在本地驅動器上。

Save As					? ×
Save in:	🛃 Desktop		•	+ 🖻 💣 🗉	•
History History Desktop My Documents	My Documents	:es			
My Computer	File name: Save as type:	certnew.cer Security Certificate		•	Save Cancel

13. 在CA伺服器上,選擇**Retrieve the CA certificate or certificate revocation list**以取得根憑證。 然後按一下**Next**。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
4-Back - → - () () () () Search () Favortes () History 1 - ()	
Address @ http://172.10.124.96/certarv/	
Microsoft Certificate Services – jitahim-pc	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. O will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt yo depending upon the type of certificate you request.	Drice you acquire a certificate, you our e-mail messages, and more
Select a task: Retrieve the CA certificate or certificate revocation list C Request a certificate C Check on a pending certificate	
	Next >

Save As						?×
Save in:	Desktop		•	+ 📾 🔿	•	
History History Desktop My Documents My Documents My Computer	My Document My Computer My Network F Certnew, cer	is Places				
	File name:	certroot.cer		•		Save
My Network P	Save as type:	Security Certificate				Cancel

15. 在VPN 3000 Concentrator上安裝根和身份證書。若要執行此操作,請選擇**管理 > Certificate** Manager > Installation > 安裝通過註冊獲取的證書。在Enrollment Status下,按一下Install。

Select a enrollment request to install.							
Enrollment Status							
Subject	Issuer	Date	Use	Reason	Method	Status	Actions
altiga30 at Cisco Systems	N/A	05/22/2003	D	Initial	Manual	In Progress	View Install Delete

16. 按一下「Upload File from Workstation」。



17. 按一下**Browse**,然後選擇儲存到本地驅動器中的根證書檔案。選擇**安裝**以在VPN集中器上安 裝身份證書。行政部門 | Certificate Management視窗顯示為確認,新的身份證書出現在 Identity Certificates表中。

Administration Certificate Management Install Id	entity Certificate Upload File from Workstation					
Enter the name of the identity certificate file.						
Filename	Browse					
Install Cancel						

注意:如果證書失敗,請完成以下步驟以生成新證書。選擇Administration > Certificate Management。在SSL Certificate清單的Actions框中按一下Delete。選擇Administration > System Reboot。選擇Save the active configuration at time of reboot,選擇Now,然後按一 下Apply。現在,您可以在重新載入完成後產生新憑證。

在VPN集中器上安裝SSL證書

如果您在瀏覽器和VPN集中器之間使用安全連線,則VPN集中器需要SSL證書。您還需要在用於管理VPN集中器和WebVPN的介面以及終止WebVPN隧道的每個介面上獲得SSL證書。

升級VPN 3000集中器軟體後,當VPN 3000集中器重新啟動時,將自動生成介面SSL證書(如果不存在)。因為自簽名證書是自生成的,所以此證書不可驗證。沒有證書頒發機構保證其身份。但是此證書允許您使用瀏覽器與VPN集中器進行初始聯絡。如果要將其替換為另一個自簽名SSL證書 ,請完成以下步驟:

1. 選擇Administration > Certificate Management。

Administ	ration Certificate	Managen	nent				Mo	ndav M	5. January 2004	16-3
PAGININ	auton certificati	: managen	ilein				110	nuay, ea	R	etres
This section • <u>Cli</u> • <u>Cli</u>	on lets you view and ck here to enroll with ck here to install a ce	manage cert <u>a Certificate</u> rtificate	ificates on the VPN 1 Authority	3000 Concer	ntrator.					
Certifica	te Authorities [<u>V</u> Subject	iew All CRL	Caches <u>Clear All CRI</u> Issuer	L Caches] (c	urrent: 1, maxi Expirati	muum ion	: 20) SCEP Issuer		Actions	
ms-root-s	ha-06-2001 at cisco	ms-	root-sha-0é-2001 at	cisco	06/04/202	2	No	View 0	Configure Delete	
	Subject			Issuer			Expiration		Actions	
Gateway.	A at Cisco Systems		ms-root-sha-D6-	2001 at cisc	0		02/04/2004	View R	enew Delete	
SSL Cer Interface	tificates Subject	1	Issuer		Expiration			Actions		
Private	10.5.6.1 at Cisco Sm	stems Inc	10.5.6.1 at Cisco Str	stems Inc.	02/01/2006	Uieur	Renew Dalata Evnort Ganarata Ennill Junn			norf
SSH Ho	st Key	1		16						
	Key Size	1	Кеу Туре		Date G	ener	ated		Actions	
1024 bits		RSA		01/05/2004				Goz	iczato	
按一下 配置VF	「Generate」 N集中器自動	可在「 9生成的9	SSL Certifica SSL證書的欄	te」表中 位。這些	P顯示新₰ 些SSL證著	 透き 書月	^登 並替換現有 目於介面和負	「憑證。 〕載均	。此視窗允 衡。	,許:
Administr You are a	ation Certificate f	fanagemer ertificate for	nt Generate SSL (r the Public Interfac	Certificate ce . The cer	tificate will ha	ive t	he following DN	for both	Subject and Iss	uer.
The certifi	cate will be valid for	r 3 years fro	m yesterday.							
Com	mon Name (CN)	10.86 194 17	<u>г</u> ,	Enter	the Common	Man	ne usually the TP	or DMS	address of this	inter

Common Name (CN)	10.86.194.175	Enter the Common Name, usually the IP or DNS address of this interface
Organizational Unit (OU)	VPN 3000 Concentrator	Enter the department.
Organization (O)	Cisco Systems, Inc.	Enter the Organization or company.
Locality (L)	Franklin	Enter the city or town.
State/Province (SP)	Massachusetts	Enter the State or Province.
Country (C)	US	Enter the two-letter country abbreviation (e.g. United States = US).
RSA Key Size	1024-bits 💌	Select the key size for the generated RSA key pair.
Generate Cancel		

如果要獲取可驗證的SSL證書(即由證書頒發機構頒發的證書),若要使用獲取身份證書所使 用的相同過程,請參閱本文檔的<u>在VPN集中器上安裝數位證書</u>部分。但這一次,在 Administration > Certificate Management > Enroll視窗中,按一下SSL certificate(而不是 Identity Certificate)。注意:請參閱管理 <u>VPN</u> 3000集中器參考<u>卷II的證書管理部分:管理和</u> <u>監控版本4.7</u>瞭解有關數位證書和SSL證書的完整資訊。

在VPN集中器上續訂SSL證書

本節介紹如何續訂SSL證書:

如果這是針對VPN集中器生成的SSL證書,請轉到SSL部分上的**管理>證書管理**。按一下「**renew**」 選項,就會更新SSL憑證。

如果這是外部CA伺服器授予的憑證,請完成以下步驟:

1. 在*SSL Certificates*下選擇Administration > Certificate Management >Delete,以便從公共介面 刪除過期的證書。

Administration | Certificate Management

Wednesday, 19 September 2007 00:01:4 Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- · Click here to enroll with a Certificate Authority
- Click here to install a certificate

Certificate Authorities [View All CRL Caches] Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut at Equifax	08/16/2008	View Renew Delete) Export Generate Enroll Import

按一下「Yes」以確認刪除SSL憑證。

No

Yes

Administration | Certificate Management | Delete

Subject

CN=pearlygates.ocp.org OU=Domain Control Validated - QuickSSL Premium(R) OU=See www.geotrust.com/resources/cps (c)07 OU=GT94824223 O=pearlygates.ocp.org C=US

Issuer

OU=Equifax Secure Certificate Authority O=Equifax C=US

	Serial Number 07E267
	Signing Algorithm SHA1WithRSA
	Public Key Type RSA (1024 bits)
	Certificate Usage Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
	MD5 Thumbprint 2C:EC:8D:8B:FE:59:9D:F8:04:A6:B2:1B:C5:09:9A:27
	SHA1 Thumbprint 6E:9A:7C:D3:02:FE:10:1C:75:79:00:AA:6A:73:84:54:C2:DC:BE:95
	Validity 8/16/2007 at 17:26:35 to 8/16/2008 at 17:26:35
	CRL Distribution Point http://crl geotrust.com/crls/secureca.crl
Are you s	way want to delete this certificate?
ac you s	

2. 選擇Administration > Certificate Management > Generate以生成新的SSL證書。

Refresh(

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- · Click here to enroll with a Certificate Authority
- <u>Click here to install a certificate</u>

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	No Certificate Installed.		(Generate) Enroll Import
				$\hat{\mathbf{n}}$

系統將顯示公共介面的新SSL證書。

Administration Certificate Management	Wednesday, 19 September 2007 00:06
	Refresh
This section lets you view and manage certificates on the VPN 3000 Concentrator.	

- · Click here to enroll with a Certificate Authority
- · Click here to install a certificate

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	10.1.1.5 at Cisco Systems, Inc.	10.1.1.5 at Cisco Systems, Inc.	09/18/2010	<u>View Renew Delete Export Generate Enroll Import</u>

相關資訊

- <u>Cisco VPN 3000系列集中器支援頁面</u>
- IPSec 協商/IKE 通訊協定
- 技術支援與文件 Cisco Systems