ASA 8.x:使用ASDM續訂和安裝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> 慣例 <u>程式</u> <u>驗證</u> <u>疑難排解</u> <u>如何將SSL證書從一個ASA複製到另一個ASA</u> <u>相關資訊</u>

<u>簡介</u>

本文檔中的過程是一個示例,可作為任何證書供應商或您自己的根證書伺服器的指南。您的證書供 應商有時需要特殊證書引數要求,但本文檔旨在提供續訂SSL證書並將其安裝在使用8.0軟體的 ASA上所需的一般步驟。

必要條件

需求

本文件沒有特定需求。

<u>採用元件</u>

此過程適用於ASA版本8.x和ASDM版本6.0(2)或更高版本。

本文檔中的過程基於安裝證書並用於SSL VPN訪問的有效配置。只要未刪除當前證書,此過程不會 影響您的網路。此程式是有關如何為當前憑證核發新的CSR的逐步程式,該當前憑證與核發原始根 CA的根憑證相同。

本文中的資訊是根據特定實驗室環境內的裝置所建立。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。

<u>慣例</u>

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。



請完成以下步驟:

1. 在Configuration > Device Management > Identity Certificates下選擇要續訂的證書,然後按一 下Add。圖1

🔂 Cisco ASDM 6.1 for ASA - 172	16.242.232				
Elle Yew Look Wigards Window	w Help		Look Par	:	⁶⁵
🚮 Home 🖓 Configuration 🔯 M	lonitoring 🔚 Sava 🔇 Refres	ih 🕜 Back 🕥 Forwa	а 🦻 нар		CISCO
Device Management 🗗 🕂 🔀	Configuration > Device Mana	agement > Certificate M	anagement > Identity Certific	cates	
Management Access System Unage(Configuration System Unage(Configuration Loging Subset (AAA Source) Cattricate Management Source) Cattricate Management Cattricate Management Source Source Cattricate Source Cattricate Source Dis Advanced	Issued To [cr=="xgcn1.com]	Issued By [(m=M5-CA]	Expiry Date 00:03:16 UTC Mar 11 20	Usage 09 General Purpose	Add Show Details Delete Export 3hstal Refresh
	Identity certificate can be use to make such configuration.	ed to authenticate SSL, such	as ADDM, access to the security a	pplance on a given interface. You can	oge to <u>19. Settines</u>
Revice Setup					
Firewall					
Ste-to-Ste VPN					
Device Menagement			Apply Reset		
Device configuration refreshed successfu	ly.		riscol 15	B B 6	8/29/08 8:52:53 PM UTC

2. 在Add Identity Certificate下,選擇Add a new identity certificate單選按鈕,然後從下拉選單中 選擇金鑰對。**注意:**不建議使用<Default-RSA-Key>,因為如果您重新生成SSH金鑰,則會使 證書無效。如果沒有RSA金鑰,請完成步驟a和b。否則,請繼續執行步驟3。**圖2**

🗲 Add Identity Certificat	e	×
O Import the identity certif	icate from a file:	
Decryption Passphrase:		
File to Import From:	Browse	
 Add a new identity certif 	icate:	
Key Pair:	CertKey Show New]
Certificate Subject DN:	ASA5540.company.com Select	
🔲 Generate self-signed	certificate	
Act as local certif	icate authority and issue dynamic certificates to TLS-Proxy	
	Advanced	
	Havancoarri	
Add Certifi	cate Cancel Help	
		_
(可選)如果尚禾配直RSA金 E <mark>nter new key pair name</mark> 欄位	讀,請完成這些步驟,否則跳到步驟3。按一下 新運 .在 □中輸入金鑰對名稱,然後按一下 Generate Now。圖3	-
🖆 Add Key Pair		
Name: 🔵 Use default key	y pair name	
💿 Enter new key	pair name: Certkey	
Size: 1024	✓	
Usage: 💿 General purpos	e 🔿 Special	
Generate Now	Cancel Help	

3. 按一下「**Select**」。

4. 輸入適當的證書屬性,如圖4所示。完成後,按一下OK。然後按一下「Add Certificate」。圖4

🗲 Certificate S	Subject DN				×
DN Attribu Attribute Value:	te to be Added Common Name (CN) Common Name (CN) Department (OU) Company Name (O) Country (C) State (St) Location (L) Email Address (EA)	Add>> Delete	Attribute Common Name (CN) Department (OU) Company Name (O) Country (C) State (St)	Value ASA5540.comp LAB Cisco Systems US CA	
			help		

CLI輸出:

to ca trustpoint ASDM_TrustPoint0
keypair CertKey
id-usage ssl-ipsec
fqdn 5540-uwe
<pre>subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA</pre>
enrollment terminal
pto ca enroll ASDM TrustPoint0

5. 在「Identity Certificate Request」彈出視窗中,將證書簽名請求(CSR)儲存到文本檔案,然後 按一下OK。圖5

🖆 Identity Certificate Request 🛛 🛛 🔀							
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.							
You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.							
Save CSR to file: C:\Certificates\ASACertCSR.txt Browse							
OK Cancel Help							

6. (可選)在ASDM中驗證CSR是否處於掛起狀態,如圖6所示。圖6

😼 Cisco ASDM 6.1 for ASA - 172.	16.242.232				
<u>File View Tools Wigards Window</u>	Help		Look Far:	6:	
🐴 Home 🙈 Configuration 🔯 Mo	nitoring 🛄 Save 💽 R	efresh 🙆 Back 🕥 Forwa	d 🦻 Help		cisco
Device Management P + X	Configuration > Device N	Innogement > Certificate M	anagement > Identity Certificate	3	
Management Access					_
🖶 🎉 System Image/Configuration		1	E - I - E - I -	L Harris	
High Availability	Issued to	Issued by	Expry Date 00:03:16 UTC Mar 11 2009	Ceneral Disage	
🖶 🎲 Users (AAA	[ASA5540.company.com	[Not Available]	Pending	Unknown	_ Show Details
Certificate Management					Delete
Identity Certificates					Expert
B 💕 DHOP					(
Advanced					Tuecal
-					Refresh
	Identity certificate can be to make such configuration	e used to authenticate SSL, such on	as ASDM, access to the security applia	nce on a given interface. You can g	o to <u>59. Settinos</u>
🛃 Device Setup					
📆 Firowali					
Remote Access VPN					
🙀 Ske-to-Site VPN					
Device Management					
20			Apply Reset		
Configuration changes saved successfully			ciscol 15	B 💀 🖪 🔒	(/29/08 9:56:23 PM UTC

- 7. 向證書管理員提交證書請求,證書管理員在伺服器上頒發證書。這可以通過Web介面和電子郵件進行,也可以直接到根CA伺服器進行證書頒發過程。
- 8. 完成以下步驟即可安裝續訂的憑證。在Configuration > Device Management > Identity Certificates下選擇掛起的證書請求,如圖6所示,然後按一下Install。在「安裝身份證書」視窗 中,選擇Paste the certificate data in base-64 format單選按鈕,然後按一下Install Certificate。注意:或者,如果證書是在.cer檔案中頒發,而不是在基於文本的檔案或電子郵件 中頒發,則您也可以選擇Install from a file,瀏覽到PC上的相應檔案,按一下Install ID certificate file,然後按一下Install Certificate。圖7

🖆 Install Identity certificate 🛛 🛛 🔀
Identity Certificate
Paste the certificate data in base-64 format:
Ng9SqvsXWWkJmS8ss9Qvz5D+K2uSLPcEAuuT7JhUVC1jbTZh1GLpqBheEeMk/8jY fui6ZdrSloUbodDEy6IiodF8QeQgCEdl1omR5W9bP5t2aTPT5J7lG3ckEM0kseqC wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== END CERTIFICATE
Install Certificate Cancel Help

CLI輸出:

crypto ca import ASDM_TrustPoint0 certificate

 $\tt WIID2DCCAsCgAwIBAgIKYb9 wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ$

!--- output truncated wPevLEO16TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit

9. 此時會出現一個視窗,確認已成功安裝證書。按一下「確定」確認。圖8

🕵 Informa	tion 🛛 🔀
į	Certificate import succeeded.
	OK

10. 確保新證書出現在「身份證書」下。圖9

🚰 Cisco ASDM 6.1 for ASA - 172.	16.242.232				
<u>File Yew Tools Wigards Window</u>	Help		Look P	ar:	🙃luulu
🛃 Home 🖓 Configuration 🔯 Mo	nitoring 🔚 Save 🔇 R	Refresh 🕜 Back 🕥 Forwa	rd 🦻 Help		cisco
Device Management 🗗 🕀 🗙	Configuration > Device !	Management > Certificate M	Innogement > Identity Certi	ficates	
E 🚰 Management Access					
🖶 🍰 System Image/Configuration	Tee red Te	Jacoust Ru	Evering Dates	Ukree	
H- Carling Availability	Im=".sont.com]	[m=MS-CA]	D:D3:16 UTC Mar 11 2	2009 General Prinnse	
🖶 🚮 Users/AAA	[cn=A5A5540.company.	.com, [cn=MS-CA]	22:49:31 UTC Aug 29:	2009 General Purpose	. Show Details
⊟ ∰ Certificate Management See CA Certificates					Delete
Identity Certificates					Export
⊕ (B) DHCP ⊕					Indal
🗉 🛐 Advanced					2.05.04
					Refresh
					_
	Edentity certificate can b to make such configurati	be used to authenticate SSL, such ion.	h as ASDM, access to the security	 appliance on a given interface. You can 	n go to <u>55. Settinos</u>
	-				
🛃 Device Setup					
👯 Frewal					
Remote Access VPN					
🔗 Site-to-Site VPN					
Device Management					
20			Apply Reset		
Configuration changes saved successfully.			disco1 15	B 🗟 🖬 🔒	8/29/08 10:05:53 PM UTC

11. 完成以下步驟,即可將新憑證繫結到介面:選擇Configuration > Device Management > Advanced > SSL Settings,如圖10所示。在Certificates下選擇您的介面,然後按一下Edit。 圖10

🚰 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
<u>File View Tools Wigards Window</u>	- Help			Look Far:	©lulu
🚮 Home 🦓 Configuration 📴 Mo	mitoring 🔚 Save 🔇 Refresh	🕒 Back 🕥 Forward 🧣	Нер		CISCO
Device Management 🗇 🕂 🔀	Configuration > Device Manage	ment > Advanced > SSL Se	ttings		
Management Access System Inage(Configuration Grift Availability Grift Availability Grift Availability Grift Cate Management Signa Grift Cate Management Signa Grift Cate Management Signa Grift Cate Grift Cate Grift Cate Grift Cate Grift Cate Grift Cate Signa HTP Redirect Signa	Configure SSL parameters. These parameters SSL Version: Any Encryption Available Algorithms RC4-M05 DES-SHAL Certificates	Clent 53L Version: A	SSL VPN access. ny V HJ >> A Remove 1	Active Algorithms RC4-SHA1 AES128-SHA1 AES256-SHA1 3DE5-SHA1	Move Up : : : Move Down
- 🔄 History Metrics	Specify which certificates, if any,	should be used for SSL authentic	ation on each int	terface. The fallback certificate will be	used on interfaces not
55. Settings	associated with a certificate of the	ar oan.			
E-W. ACCh	Interrace	Trustpoint		.oad Balancing Hustpoint	
	outside	jon-1.spil.com jon-66	GAL611)		
Device Setup					
Remote Access VPN	Falback Certificate: None			×	
🔗 Ske-to-Ste VPN					
Device Management					
2			Apply P	Reset	
Configuration changes saved successfully			cisco 1	15 🔝 🛃 🔂	🔒 8/29/08 10:08:53 PM UTC
松下垃 澡胃由澡煙菜	6.惑走 拉 てつい	/ 从这边 丁	Annly		

12. 從下拉選單中選擇新證書,按一下OK,然後按一下Apply。

ssl encryption rc4-shal aes128-shal aes256-shal 3des-shal

ssl	trust-point	ASDM_	_TrustPoint0	outside
-----	-------------	-------	--------------	---------

圖11

actest aan set tillingte		r:	Select	SSL	Certificate	
--------------------------	--	----	--------	-----	-------------	--

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the outside interface. To enroll a trustpoint, go to Configuration > Features > Device Administration > Certificate > Enrollment.

×

Interface:	outside
Primary Enrolled Certificate:	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems, 💟
Load Balancing Eprolled Certificate:	None
Eoda Balancing Enrolloa Contineator	[cn=*.vpn1.com]:[cn=MS-CA]: 611f863000000000026
	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems,

13. 在ASDM或CLI中儲存配置。



您可以使用CLI介面驗證新證書是否正確安裝到ASA,如以下輸出示例所示:

ASA(config) #**show crypto ca certificates** Certificate Status: Available Certificate Serial Number: 61bf707b000000000027 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name:

cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3basel\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage: Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---'old' certificate CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006 end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available Certificate Serial Number: 611f86300000000026 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009 Associated Trustpoints: test ASA(config)#

疑難排解

(可選)在CLI上驗證是否已向介面應用正確的證書:

ASA(config) #show running-config ssl

ssl trust-point ASDM_TrustPoint0 outside

!--- Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN.
ASA(config)#

如何將SSL證書從一個ASA複製到另一個ASA

如果已生成可匯出金鑰,則可以執行此操作。您需要將證書匯出到PKCS檔案。這包括匯出所有關 聯的金鑰。

使用以下命令通過CLI匯出證書:

ASA(config) #crypto ca export

注意:口令 — 用於保護pkcs12檔案。

使用以下命令通過CLI匯入證書:

SA(config) #crypto ca import

注意:此密碼應與匯出檔案時使用的密碼相同。

也可以通過ASDM為ASA故障轉移對執行此操作。請完成以下步驟以執行此操作:

1. 通過ASDM登入到主ASA並選擇Tools—> Backup Configuration。

2. 您可以備份所有內容或僅備份證書。

3. 在備用模式下,開啟ASDM並選擇Tools ---> Restore Configuration。

相關資訊

- Cisco Adaptive Security Appliance(ASA)支援頁面
- ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例
- 技術支援與文件 Cisco Systems