ASA 8.x:使用 ASDM 续订并且安装 SSL 证书

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 规则 步骤 <u>验证</u> <u>故障排除</u> <u>如何复制从一个ASA的SSL证书到另一个</u> <u>相关信息</u>

<u>简介</u>

本文档中介绍的步骤仅作示例用途,可用于在与证书供应商协作或使用您自己的根证书服务器时提供指导。有时,证书供应商会提出特殊证书参数要求,但本文档旨在提供续订 SSL 证书并将其安装 在使用 8.0 软件的 ASA 上所需要的一般步骤。

<u>先决条件</u>

要求

本文档没有任何特定的要求。

使用的组件

这些步骤适用于采用 ASDM 6.0(2) 版或更高版本的 ASA 8.x 版。

本文档中的步骤基于通过安装并用于 SSL VPN 访问的证书所进行的有效配置。只要不删除当前证书,此过程就不会影响您的网络。此过程逐步介绍了如何为当前证书发出新的 CSR,这些证书有发出原始根 CA 的相同的根证书。

本文档中的信息都是基于特定实验室环境中的设备编写的。如果您使用的是真实网络,请确保您已 经了解所有命令的潜在影响。

<u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则</u>。



完成这些步骤:

1. 在 Configuration > Device Management > Identity Certificates 下选择要续订的证书,然后单 击 Add。图

1					
🖆 Cisco ASDM 6.1 for ASA - 172	2.16.242.232				
<u>File View Tools Wizards Window</u>	w <u>H</u> elp		Look P	ar:	©
🚮 Home 🖓 Configuration 🔯 M	lonitoring 🔚 Sava 🔇 P	Refresh 🕜 Back 🕥 Forw	ad 🦻 Help		CISCO
Device Management 🗗 🕀 🔀	Configuration > Device	Management > Certificate !	tanagement > Identity Cert	ficates	
🖶 🜈 Management Access]				
H 😸 🥵 System Image/Configuration	Issued To	Issued By	Expiry Date	Usage	Add
🖽 🚺 Logging	[cn=*.spn1.com]	[cn=MS-CA]	00:03:16 UTC Nar 11 (2009 General Purp	Show Details
🖶 🚮 Certificate Management					C. PORTAGON,
CA Certificates					Delete
B B DHCP					Export
🖶 🚑 DNS					Instal
					Refresh
	Identity certificate can b	be used to authenticate SSL, suc	h as ASDM, access to the security	appliance on a given interface.	You can go to \$5. Settings
	to make such configurat	ion.			
💑 Device Setup					
Frowall					
Remote Access VPN					
Ske-to-Site VPN					
Device Management					
20 7			Apply Reset		
Device configuration refreshed successfu	uly.		riscol 15	🗟 🚨 🚾	🔒 8/29/08 8:52:53 PM UTC

2. 在 Add Identity Certificate 下,选中 Add a new identity certificate 单选按钮,然后从下拉菜单中选择密钥对。注意:不建议使用 <Default-RSA-Key>,因为一旦重新生成 SSH 密钥,就会使证书失效。如果没有 RSA 密钥,请完成步骤 a 和 b。如果有,则继续进行步骤 3。图2

🖆 Add Identity Certificat	ie	$\mathbf{\times}$
 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	
Add Certifi	cate Cancel Help	

(可选)如果还没有配置 RSA 密钥,请完成以下步骤;反之则跳到步骤 3。单击 New...。在 Enter new key pair name 字段中输入密钥对的名称,然后单击 Generate Now。图

is Add Ku	O Use default key pair name	×
. I amor	Enter new key pair name: Certkey	
Size:	1024 💌	
Usage:	⊙ General purpose O Special	
G	enerate Now Cancel Help	

- 3. 单击**选择**。
- 4. 如图 4 所示,输入相应的证书属性。完成后单击 OK。然后单击 Add Certificate。图 4

🖆 Certificate Subject DN 🛛 🔀
DN Attribute to be Added Attribute: Common Name (CN) Value: Common Name (CN) Department (OU) Delete Company Name (O) Country (C) State (St) CA Location (L) Email Address (EA) OK Cancel

CLI 输出:

crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec fqdn 5540-uwe subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA enrollment terminal crypto ca enroll ASDM_TrustPoint0

5. 在身份证书请求弹出窗口,请保存您的证书签名请求(CSR)到文本文件,并且点击OK键。图

To comple	te the enrollment process, please save the PKCS10 enrollment
request ((ISR) and send it to the CA.
You will th	en need to install the certificate that is returned from the CA by
clicking the	e Install button in the Identity Certificates panel.
Save CSR	to file: C:\Certificates\ASACertCSR.txt Browse
	OK Cancel Help

🔂 Cisco ASDM 6.1 Ior ASA - 172.	16.242.232				
<u>File Yew Tools Wizards Window</u>	Help		Look Far:	Go	ahaha
🚮 Home 🙈 Configuration 🔯 Mor	nitoring 🔚 Save 💽 R	efresh 🔇 Back 🕥 Forma	rd 🦻 Help		cisco
Device Management P P X	Configuration > Device N	Management > Certificate M	Innogement > Identity Certificate		
🗟 🍞 Management Access					
🖶 🍰 System Image/Configuration	Top and To	Terrined For	Evering Dates	1 threes	
H Cooing	[cn=".sont.com]	[m=MS-CA]	D:03:16 UTC Mar 11 2009	General Purpose	
🖶 🚮 Users(AAA	[ASA5540.company.com] [Not Available]	Panding	Unknown	. Show Details
Certificate Management Say CA Certificates					Delete
Identity Certificates					Export
E (P DHCP DHCP					Inital
🗊 🛐 Advanced					
					Refresh
	Identity certificate cap b	e used to authenticate 550 , such	as 450M, arress to the security apple	oce op a given interface. You can or	to SN. Settings
	to make such configurati	on.			
0					
Device Setup					
👯 Firoval					
Remote Access VPN					
🙀 Site-to-Site VPN					
Device Management					
20			Apply Reset		
Configuration changes saved successfully.			riscot 15		29/08 9:56:23 PM UTC

- 7. 向在服务器上签发证书的证书管理员提交证书请求。可通过 Web 界面或电子邮件方式提交 ,也可直接提交到用于证书签发过程的根 CA 服务器。
- 8. 请完成以下步骤,以便安装续订的证书。如图 6 所示,在 Configuration > Device Management > Identity Certificates 下选择挂起的证书请求,然后单击 Install。在 Install Identity Certificate 窗口中,选中 Paste the certificate data in base-64 format 单选按钮,然后 单击 Install Certificate。注意:或者,如果证书是以.cer 文件而非基于文本的文件或电子邮件 方式签发,您也可以选择 Install from a file,然后浏览到 PC 上的相应文件,再依次单击 Install ID certificate file 和 Install Certificate。图

🖆 Ins	stall Identity certificate	×
Identi	ity Certificate	
0	Install from a file: Browse	
	Paste the certificate data in base-64 format:	
	Ng9SqvsXWWkJmS8ss9Qvz5D+K2uSLPcEAuuT7JhUVC1jbTZh1GLpqBheEeMk/8jY fui6ZdrSloUbodDEy6IiodF8QeQgCEdl1omR5W9bP5t2aTPT5J7lG3ckEM0kseqC wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== END CERTIFICATE	<
	<	
7	Install Certificate Cancel Help	

CLI 输出:

crypto ca import ASDM_TrustPoint0 certificate

WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit

9. 此时将出现一个窗口,确认已成功安装证书。单击"OK"进行确认。图

	🕵 Informati	on	×
	¢	Certificate import succeeded.	
8		ОК	

10. 确保新证书出现在 Identity Certificates 下。图 9

🚰 Cisco ASDM 6.1 for ASA - 172	.16.242.232					
Ele Yew Look Wigards Window	v ∐elp			Look Par:		© alate
🚮 Home 🖓 Configuration 🔯 Mo	onitoring 🔚 Save 🔇 Re	efresh 🔇 Back 🕥 Forwar	а 🦻 нөр			cisco
Device Management D & X	Configuration > Device M	Innovement > Certificate M	anagement > Iden	tity Certificates		
Management Access						_
🖶 🎉 System Image/Configuration						
🖶 🤐 High Availability	Issued To	Issued By	Expiry Date	I IC M~ 11 0000	Usage Control Discours	Add
H 🙀 Users (AAA	[or=A5A5540.company.c	com[cn=MS-CA]	22:49:31 UT	IC Aug 29 2009	General Purpose	. Show Details .
😑 🛃 Certificate Management						Delete
🕀 🗗 ОНСР						Ester
DNS Advanced						Instal
						Refresh
	Identity certificate can be	e used to authenticate SSL, such	as ASDM, access to th	he security appliand	e on a given interface. You c	an go to <u>55. Settinos</u>
	to make such configuratio	on.				
💑 Device Setup						
👯 Fyrowali						
Remote Access VPN						
🙀 Site-to-Site VPN						
Device Management						
34 *			Apply .	Reset		
Configuration changes saved successfully			cisco 1	15	B 🗟 🖪 🛛 🔓	8/29/08 10:05:53 PM UTC

11. 请完成以下步骤,以便将新证书绑定到接口上:如图 10 所示,选择 Configuration > Device Management > Advanced > SSL Settings。在 Certificates 下选择接口,然后单击 Edit。图 10

🚰 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
Ele Yew Look Wizards Window	∕ Help			Look.Par: Go	alada
🐇 Home 🦓 Configuration 🔯 Mo	onitoring 🔚 Sava 🔇 Re	ilresh 🔇 Back 🕥 Forward			cisco
Device Management 🗗 🕀 🔀	Configuration > Device M	lanagement > Advanced > 5	SL Settings		
Management Access System Unexce/Configuration Gravity High Availability Users/AAA Graviticate Management Source Management Graviticate Management Graviticates DetCP Graviticates Advanced Graviticates Graviticates Management SSL Certificates History Metrics History Metrics History Metrics Success	Configure SSL parameters, 1 Server SSL Version: Any Encryption Available Algorithms RC DC Certificates Specify which certificates, accessible with certificates,	Clent 55L Versio	M and SS, VPN acce m: Any Add >> << Remove : thentication on each	Active Algorithms RC4-SHA1 AES128-SHA1 AES256-SHA1 3DE5-SHA1 3DE5-SHA1	Move Up (;) Move Down
- SS. Settings	associated with a certifica	te of their own.			
	inside outside	(cr1.ven).com)(c	n=M3-CA] 6115		
💑 Device Setup					
Remote Access VPN	Failback Certificate:	00 -		~	
Sterto-Ste VPN		a a		- 152)	
*			Apply .	Reset	
Configuration changes saved successfully			cisco 1	15 📑 🛃 🔂 8/2	9/08 10:08:53 PM UTC

12. 从下拉菜单中选择新证书,然后单击 OK,再单击 Apply。ssl encryption rc4-shal aes128shal aes256-shal 3des-shal

ssl trust-point ASDM_TrustPoint0	outside
11	
🖆 Select SSL Certificate	
Specify enrolled trustpoints to be us interface. To enroll a trustpoint, go Certificate > Enrollment.	ed for SSL authentication and VPN load balancing on the outside to Configuration > Features > Device Administration >
Interface:	outside
Primary Enrolled Certificate:	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems, 💟
Load Balancing Enrolled Certificate:	None
	[cn=*.vpn1.com]:[cn=MS-CA]: 6111863000000000026
ОК	[cn=*.vpn1.com]:[cn=MS-CA]: 611f86300000000000026 [cn=ASA5540.company.com, ou=LAB, o=Cisco Systems,

13. 将配置保存在 ASDM 中或 CLI 上。

<u>验证</u>

您可以使用 CLI 界面验证新证书是否已正确安装到 ASA,如以下示例输出所示:

ASA(config)#show crypto ca certificates Certificate Status: Available Certificate Serial Number: 61bf707b00000000027 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-base1/CertEnroll/MS-CA.crl [2] file:///\win2k3-base1\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-base1/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-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\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)#

<u>故障排除</u>

(可选)在 CLI 上验证是否已对界面应用正确的证书:

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)**#**

<u>如何复制从一个ASA的SSL证书到另一个</u>

如果生成可导出密钥,这可以执行。您需要导出证书到PKCS文件。这包括导出所有相关的密钥。

请使用此命令通过CLI导出您的证书:

ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase> 注意: 密码短语-曾经保护pkcs12文件。

请使用此命令通过CLI导入您的证书:

SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase> **注意:** 当导出文件时,此密码短语应该是相同的象使用。

这可能通过ASA故障切换对的ASDM也执行。完成这些步骤执行此:

- 1. 登陆对主要的ASA通过ASDM并且选择工具-->备份配置。
- 2. 您能备份一切或证书。
- 3. 在待机,开放ASDM和选择工具-->恢复配置。

相关信息

- Cisco 自适应安全设备 (ASA) 支持页
- 在 ASA 8.x 上手动安装第三方供应商证书以便与 WebVPN 一起使用的配置示例
- <u>技术支持和文档 Cisco Systems</u>