在 ASA 7.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

目录

简介 先决条件 要求 使用的组件 规则 配置 步骤 1. 验证 Date、Time 和 Time Zone 值是否准确 步骤 2. 生成 RSA 密钥对 步骤 3. 创建信任点 步骤 4. 生成证书注册 步骤 5. 验证信任点 步骤 6. 安装证书 步骤 7. 将 WebVPN 配置为使用新安装的证书 验证 替换 ASA 的自签名证书 查看已安装的证书 使用 Web 浏览器验证为 WebVPN 安装的证书 续订 SSL 证书的步骤 命令 故障排除 相关信息

简介

此配置示例描述如何在 ASA 上手动安装第三方供应商数字证书,以便与 WebVPN 一起使用。此示 例中使用 Verisign Trial Certificate。每个步骤都包含 ASDM 应用程序步骤和 CLI 示例。

先决条件

要求

本文档要求您能够访问证书机构 (CA) 以便进行证书注册。支持的第三方 CA 供应商有 Baltimore、 Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA 和 Verisign。

使用的组件

本文档使用运行软件版本 7.2(1) 和 ASDM 版本 5.2(1) 的 ASA 5510。 但是,本文档中的过程对于 运行 7.x 和任何可兼容 ASDM 版本的任何 ASA 设备都有效。 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。本文档中使用的所有设备最初均采用原 始(默认)配置。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。

规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

配置

要在 PIX/ASA 上安装第三方供应商数字证书,请完成以下步骤:

- 1. 验证日期、时间和时区值是否准确。
- 2. <u>生成 RSA 密钥对。</u>
- 3. <u>创建信任点</u>。
- 4. <u>生成证书注册</u>。
- 5. <u>验证信任点</u>。
- 6. <u>安装证书</u>。
- 7. 配置WebVPN以使用新安装的证书。

步骤 1. 验证 Date、Time 和 Time Zone 值是否准确

- 1. 单击 Configuration, 然后单击 Properties。
- 2. 展开 Device Administration, 然后选择 Clock。
- 3. 验证列出的信息是否准确。要正确通过证书验证,Date、Time 和 Time Zone 值必须准确。



命令行示例

ciscoasa
ciscoasa# show clock
11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

步骤 2. 生成 RSA 密钥对

生成的 RSA 公钥将与 ASA 的身份信息组合在一起形成 PKCS#10 证书请求。您应明确指出要为其 创建密钥对的信任点的密钥名称。

- 1. 单击 Configuration,然后单击 Properties。
- 2. 展开 Certificate, 然后选择 Key Pair。
- 3. 单击 Add。

a.	E- Certificate				
68	- Authentication				
NAT		Key Pair Nam	e Usage	Modulus Size	Add
-		100 / 101 1101	n couge	modular size	
L 🕰	- Still Key Pair				1
VDN	- An Manage Certificates				Show Details
100	E- 🔂 Trustpoint				
A			entrett andt Joney als and	1001	Delete
	- Export	📴 Add Key Pair		×	
CSD Manager	- Import				
12.	E P Device Access	C. Hand	inford have a series		Refresh
25	E-86 Device Administration	Nome: Ose d	erault key hame		
Routing	E P DHC Services	G	arision had		
0	🕀 🚚 DNS 🕫	in history	ensignities)		
68	High Availability and Scal				
Global Objects	- 🙀 Fallover	Size: 1024	•		
	- 🥸 Fragment				
3	-12 History Metrics	Usage: 📀 Gener	ral Purpose C Special		
Properties	HTTP/HTTPS	-			
Propercies	E-Ito IP Audit				
	🔁 🚺 Logging			-	
	Priority Queue	Generate Now	Cancel Help		
	- 🙀 SSL				
	SUNRPC Server				
	TCP Options				
	- Timeouts				

- 4. 输入密钥名称,选择系数大小,然后选择使用类型。注意:推荐的密钥对大小是 1024。
- 5. 单击生成。您创建的密钥对应在 Key Pair Name 列中列出。

命令行示例



步骤 3. 创建信任点

要声明 ASA 将使用的证书机构 (CA),必须提供信任点。

- 1. 单击 Configuration,然后单击 Properties。
- 2. 展开 Certificate, 然后展开 Trustpoint。
- 3. 选择 Configuration, 然后单击 Add。

Configuration > Properties > C	ertificate > Trustpoint > Configuration				
Startup Wizard	Configuration				
🕀 🚮 AAA Setup	Configure a Certificate Authority (CA) as a trustroint				
	comigare a continente marierary (con) as a traciporte.				
🔁 🐯 ARP					
E- Certificate	Trustpoint Name Device Certificate Subject CA Certificate Subject	Add			
Authentication					
Enrolment		Edit			
Import Certificate	-				
		0.00			
Manage Certificates		Delete			
- A Trustpoint					
- Configuration	10	Request CRL			
Export	-				
- import					
Device Access					

- 4. 配置以下值: **Trustpoint Name**:信任点名称应与目标用途相关。(此示例使用 *my.verisign.trustpoint*。)**Key pair**:选择在<u>步骤 2 中生成的密钥对 (</u>*my.verisign.key*)。
- 5. 确保选中 Manual Enrollment。
- 6. 单击 Certificate Parameters。将会出现 Certificate Parameters 对话框。
- 7. 单击 Edit, 然后配置下表中列出的属性:要配置这些值,可以从 Attribute 下拉列表中选择值 或输入值, 然后单击 Add。

			Common Name (CN)	webvpn.cisco.com
Attribute to I	be Added	7	Department (OU)	TSWEB
			Company Name (O)	Cisco Systems
ttribute: :	Select Attribute	Add >>	State (St)	North Carolina
_			State (St)	US
alue:		Delete	Location (L)	Raleigh

- 8. 添加相应的值之后,单击 OK。
- 9. 在 Certificate Parameters 对话框的 Specify FQDN 字段中,输入 FQDN。此值应与用于公用 名称 (CN) 的 FQDN 相同。

🚰 Certificate Parameters	×
Enter the values for the parameters that are to be included in the certificate.	
Subject DN: ystems,St=North Carolina,St=US,L=Raleigh	
FQDN	
C Use FQDN of the device	
Specify FQDN webvpn.cisco.com	
C Use none	
E-mail:	
IP Address:	
Include device serial number	
OK Cancel Help	

- 10. Click **OK**.
- 11. 验证是否选择了正确的密钥对,然后单击 Use manual enrollment 单选按钮。
- 12. 单击 **OK**,然后单击 Apply。

Indication rustpoint Name: my.verisign.truspoint Generate a self-signed certificate on enrollment If this option is enabled, only Key Pair and Certificate Parameters can be specified. Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Key Pair: my.verisign.key Show Details New Key Pair Challenge Confirm Challenge Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode Mode Generate are no certificates associated with this trustpoint.
rustpoint Name: my.verisign.truspoint Generate a self-signed certificate on enrollment If this option is enabled, only Key Pair and Certificate Parameters can be specified. Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Key Pair: my.verisign.key Show Details New Key Pair Challenge Confirm Challenge Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode
Generate a self-signed certificate on enrollment If this option is enabled, only Key Pair and Certificate Parameters can be specified. Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced Key Pair: my.verisign.key Show Details New Key Pair Challenge Confirm Challenge Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode Guide an only be specified if there are no certificates associated with this trustpoint.
Generate a self-signed certificate on enrollment If this option is enabled, only Key Pair and Certificate Parameters can be specified. Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced Key Pair: my.verisign.key Show Details New Key Pair Challenge Password: Confirm Challenge Password: Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode
If this option is enabled, only Key Pair and Certificate Parameters can be specified. Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced Key Pair: my.verisign.key Show Details New Key Pair Challenge Password: Confirm Challenge Password: Confirm Challenge Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode
Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced Key Pair: my.verisign.key Show Details New Key Pair Challenge Confirm Challenge Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode
Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced Key Pair: my.verisign.key
Key Pair: my.verisign.key Show Details New Key Pair Challenge Confirm Challenge Password: Password: Password: Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode
Challenge Password: Confirm Challenge Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode
Challenge Password: Confirm Challenge Password: Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint. Enrollment Mode Confirm Challenge Confirm Challenge Password: Passwo
Password: Password: Password: Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.
Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.
Enrollment Mode
Enrollment Mode
C the week and a set
 Use manual enrollment
C the extended and head
Use automatic enrollment
Enrollment URL: http://
·]
Retry Period: 1 minutes
Retry Count: 0 (Use 0 to indicate unlimited retries)
Certificate Parameters
OK Cancel Help

命令行示例

ciscoasa
ciscoasa(config)# crypto ca trustpoint my.verisign.trustpoint
! Creates the trustpoint.
ciscoasa(config-ca-trustpoint)# enrollment terminal
<pre>! Specifies cut and paste enrollment with this trustpoint. ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,</pre>
Systems,C=US,St=North Carolina,L=Raleigh
<i>! Defines x.500 distinguished name.</i> ciscoasa(config-ca- trustpoint)# keypair my.verisign.key
<i>! Specifies key pair generated in <u>Step 3</u>.</i> ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
! Specifies subject alternative name (DNS:).

步骤 4. 生成证书注册

ASDM 步骤

- 1. 单击 Configuration, 然后单击 Properties。
- 2. 展开 Certificate, 然后选择 Enrollment。
- 确认选择了在<u>第3步中创建的信任点,然后单击</u> Enroll。将会出现一个对话框,并列出证书注 册请求(也称为证书签名请求)。

iroiment kequest	
o complete the enrollment p nanagement interface of the	rocess, please paste the following PKCS10 enrollment request into the CA.
/ou will need to install the c	ertificate after receiving it.
o to Configuration > Proper	ties > Certificate > Import Certificate to do so.
ertificate Request:	
hvcNAQkCFhtDaXNjbOF AQEBBQADgYOAMIGJAoC	TQS5teWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvcN BAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm
psMFP7DeKPIQ+RdthaF mAH40WUXbi18BH2SSgx AgMBAAGgRjBEBgkqhki ghtDaXNjb0FTQS5teWF gmoBmSRVnL0qyDtpS1F gEjVABVhB7Ni6N29710 gonnkGTJ11v2CSDXz4E	BzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY PX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF G9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd wbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA veKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 cXm4sXAqrwZCDdj0/S5BiQJGc=
psMFP7DeKPIQ+RdthaF mAH40WUXbi18BH2SSgx AgMBAAGgRjBEBgkqhki ghtDaXNjb0FTQS5teWF gmoBmSRVnL0qyDtpS1F gEjVABVhB7Ni6N29710 gonnkGTJ11v2CSDXz4E	BzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY PX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF G9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd wbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA oveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 Xm4sXAqrwZCDdj0/S5BiQJGc=
psMFP7DeKPIQ+RdthaF mAH40WUXbi18BHZSSgx AgMBAAGgRjBEBgkqhki ghtDaXNjb0FTQS5teWF gmoBmSRVnL0qyDtpS1F gEjVABVhB7Ni6N29710 gonnkGTJ11vZCSDXz4F D End - This line	BzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY PX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF G9w0BCQ4xNzA1MAsGA1UdDwQBAwIFoDAmBgNVHREEHzAd wbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA vveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 Xm4sXAqrwZCDdj0/S5BiQJGc=

 4. 将 PKCS#10 注册请求复制到一个文本文件中,然后将 CSR 提交给相应的第三方供应商。第 三方供应商在收到 CSR 后应颁发一个用于安装的身份证书。

命令行示例

设备名称1 ciscoasa(config)#crypto ca enroll my.verisign.trustpoint ! Initiates CSR. This is the request to be ! submitted via web or email to the 3rd party vendor. % Start certificate enrollment .. % The subject name in the certificate will be: CN=webvpn.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The fully-qualified domain name in the certificate will be: webvpn.cisco.com % Include the device serial number in

```
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes
! Displays the PKCS#10 enrollment request to the
terminal. ! You will need to copy this from the terminal
to a text ! file or web text field to submit to the 3rd
party CA. Certificate Request follows:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVt.czE0
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4vTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
30MXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3vEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BM05lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5Q1Kx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request --- Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#
```

步骤 5. 验证信任点

从第三方供应商处收到身份证书后,您可以继续执行此步骤。

- 1. 将身份证书保存到本地计算机中。
- 如果您收到的是非文件形式的 base64 加密证书,则您必须复制此 base64 信息,并将其粘贴 到文本文件中。
- 3. 将文件扩展名改为 .cer。注意:一旦文件以.cer扩展名重命名,文件图标应显示为证书。
- 4. 双击此证书文件。此时,将显示"Certificate"对话框。

Certificate	? ×
General Details Certification Path	
	_
Certificate Information	
This certificate is intended for the following purpose(s):	-
 Ensures the identity of a remote computer Proves your identity to a remote computer 2.16.840.1.113733.1.7.21 	
"Windows没有足够的信息来验证此证书"消息显示在"堂规"选项卡中。	你心须

"Windows没有足够的信息来验证此证书"消息显示在"常规"选项卡中,您必须先获取第三方供 应商根CA或中间CA证书,然后才能继续执行此过程。请与第三方供应商或 CA 管理员联系 ,以获得其发放的根 CA 或中间 CA 证书。

- 5. 单击 Certificate Path 选项卡。
- 6. 单击位于所发放的身份证书上方的 CA 证书,然后单击 View Certificate。

Certificate	? ×
General Details Certification Path	1
Certification path	_
VeriSign Trial Secure Server Test Root CA VeriSign Trial Secure Server Test CA Webvpn.cisco.com	
View Certificate	
Certificate status:	
This certificate is OK.	
0	

比时,将显示中

间 CA 证书的详细信息。警告:请勿在此步骤中安装身份(设备)证书。在此步骤中仅添加根 、辅助根或 CA 证书。身份(设备)证书在步骤 6 中安装。

ertificate	?
General Details Certification Pa	ath
Show: <a>All>	
Field	Value 🔺
Version	V3
Serial number	63 b1 a5 cd c5 9f 78 80 1d a0
Signature algorithm	sha1RSA
	VeriSign Trial Secure Server Te
Valid from	Tuesday, February 08, 2005 8
Valid to	Sunday, February 08, 2015 7:
Subject	VeriSign Trial Secure Server Te
	KOA (2010 BICS)
	Edit Properties Copy to File
	ОК

- 7. 单击 Details。
- 8. 单击 Copy to File。
- 9. 在"Certificate Export Wizard"中,单击 Next。
- 10. 在"Export File Format"对话框中,单击 Base-64 encoded X.509 (.CER) 单选按钮,然后单击 "Next"。

Certificate Export Wizard	X
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
C Personal Information Exchange - PKCS #12 (.PFX)	
\square Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
Delete the private key if the export is successful	
< Back Next > Cance	 el

- 11. 输入文件名以及要用于保存 CA 证书的位置。
- 12. 单击 **Next**,然后单击"Finish"。

	Browse
	Browse
	Browse

- 13. 在"Export Successful"对话框中,单击 OK。
- 14. 浏览到 CA 证书的保存位置。
- 15. 使用文本编辑器打开文件,例如记事本。(右键单击文件,然后选择 Send To > Notepad。)将会显示类似于下图中证书的 base64 编码信息 :

File Edit Format View Help

----BEGIN CERTIFICATE---MIIFSjçCBDKqAwIBAqIQCECQ47aTdj6BtrI60/Vt6zANBqkqhkiG9w0BAQUFADCB yzelMA&GA1UEBhMCVVMxFzAVBqNVBAoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24qVHJpYWwqU2VjdXJlIFNl cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTk1OVowgZ4x CZAJB9NVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q2lzY28qU3lzdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BgNVBAsUMVRlcm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PWYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBWIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRw0i8vb2NzcC52zXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9TvljTZWN1cmUtyWlhLnZlcmlzaWduLmNvbS9TvljUcmlhbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAwIaBBRLa7ko]gYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zxJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKozIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTqIorIC1aWwWx+RHCcTqIrlzf0vfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvl×zŹji0J51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLKyja |idT1FmBvf02qaZS6S40= ----END CERTIFICATE-----

- 16. 在 ASDM 中,单击 Configuration,然后单击 Properties。
- 17. 展开 Certificate, 然后选择 Authentication。
- 18. 单击 Enter the certificate text in hexadecimal or base64 format 单选按钮。
- 19. 将 base64 格式的 CA 证书从文本编辑器中粘贴到文本区域。
- 20. 单击 Authenticate。

Configuration > Properties > C	ertificate > Authentication				
Startup Wizard	Authentication				
AAA Setup AAA Setup Societary Anti-Spoofing ARP	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with a trustpoint and installed on the device.				
Auto Update	Trustpoint Name: wy.verisign.truspo Edit New				
Certificate	Fingerprint (optional):				
Import Certificate	The certificate text can be specified if the selected trustpoint is configured for manual enrolment.				
Annage Certificates Annage Certificates Trustpoint Configuration	C Import from a file: Browse				
Bevice Access	Enter the certificate text in hexadecimal or base64 format: A11E State VerYoux //bis 724e//of by2004 by2004 verYoux //bis 71e/2014//				
Device Administration DHCP Services	ECCol67bggLewTagTia9h3MwDQYJKoZhvcNAQEFBQADgYEASz5v8s3/ Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDIwSRmiH3B///SU6E				
High Availability and Scal	Ai9TXvRicD5q0mB+nyK9fB2aBzOiaiHSiMVzAJeQjuqA+Q93jNew+peuj4Ahc n/KK/+1 Yv61 w3+7g6ukFMARVBNg= END CERTIFICATE				
Fragment Bistory Metrics HITP/HTTPS					
⊕-100 IP Audit ⊕-100 Logging	Authentication Successful				
- Briority Queue - Briority Queue - Briority Queue - SSL - Server	The trustpoint my.verisign.truspoint has been authenticated.				
TCP Options Timeouts URL Filtering	OK				

21. Click **OK**. **命令行示例**

ciscoasa
ciscoasa(config)# crypto ca authenticate
my.verisign.trustpoint
! Initiates the prompt to paste in the base64 CA root !
or intermediate certificate. Enter the base 64 encoded
CA certificate. End with the word "quit" on a line by
itselfBEGIN CERTIFICATE
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
${\tt jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMTAw}$
LGYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT
AlvTMRcw
FQYDVQQKEw5WZXJpU21nbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
${\tt BgNVBAMTJFZ1cmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD}$

QTCCASIW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8D0Pv0fGRu1wpfUUZC8v+WKC20+sK6
QMECAWEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu
CHMVdGVzdGNhLzAOBgNVHQ8BA18EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
AludDgQWBBRm106B4DFZ3Sp/qUDFNg1GcCeHwjCBsgYDVRUjB1GqM1Gn
MIGMMQSWCQYDVQQGEWJVUZEXMBUGAIUEChMOVmVyaVNpZ24SIEIUYy4x
BASTJUZVCIBUZXNUIFBICNBVCZVZIEJUDHKUICBODYBNCJNICMFUIZVZ
AlliEAxMoVmVvaVNpZ24gVHJpVWwgU2VidXJ]IFN]cpZlciBUZXN0IFJv
b30g00GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY21
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNg=
END CERTIFICATE
quit
! Manually pasted certificate into CLL. INFO:
Certificate has the following attributes: Fingerprint:
ouerorum /Iccoesu Iddezc42 UNISEI43 Do you accept this
certificate: [yes/no]: yes trustpoint
my.verisign.trusipoint is a subordinate CA and holds a
non serr-signed certificate. Trustpoint CA certificate
accepted. & Certificate successfully imported
CISCOASA(COILLY)#

步骤 6. 安装证书

ASDM 步骤

使用第三方供应商提供的身份证书执行以下步骤:

- 1. 单击 Configuration,然后单击 Properties。
- 2. 展开 Certificate, 然后选择 Import Certificate。
- 3. 单击 Enter the certificate text in hexadecimal or base64 format 单选按钮,然后将 base64 身 份证书粘贴到文本字段中。

Configuration > Properties > C	ertificate > Import Certificate						
- 39 Startup Wizard	mport Certificate						
🕀 🚮 AAA Setup	Install an identity cartificate that was received from a Cartificate Authority (CA) in resource to a merual						
- 🐯 Anti-Spoofing	enrolment request.						
🟵 🐻 ARP	er a service à l'expension						
	Trustenist Name						
E Certificate	my vensign truspo Edit New						
Authentication							
- 2 Enrolment	Certificate Text						
Import Certificate	C hand from a flat						
Key Pair	Compare and the						
Manage Certificates							
E-82 Trustpoint	1. Enter the certificate text in nexadecimal or baseb4 format:						
Configuration							
Export	USSA SALVAR DV VICA THE NOT RECOVERY OF A DARGE & MORE AND A DARGE						
import	matkets photo and a state of the second state						
Device Access	tFkFFSFbleCK/hh6MaMb40z6kiFizoVUmtdJDoU3800U/vm+fq02eTWdz/WF.						
B-SD Device Administration	0YVwM3KDQAO6EbAntUoAxovDbJucdxb6ZVTtyevMcgzCkXMHEVxa5/P>						
P-B DNS	ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4ufcGgGZD8tVGx26b5OWTz8K						
High Availability and Scal	BEvHm3grdbDZP+iSMotWYE+CgfKpZb+CPAqH2Cdpz2aJljhb6CS6NM=						
Failover	END CERTIFICATE						
- K Fragment							
HTTP/HTTPS	To Information						
🕀 📲 🔁 IP Audit							
🐑 🛅 Logging							
- Priority Queue	Certificate import succeeded.						
- 📲 SSL							
SUNRPC Server							
TCP Options							
Timeouts							
ORL Fittering							
1							

4. 单击 **Import**,然后单击 OK。

命令行示例

ciscoasa
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate
! Initiates prompt to paste the base64 identity certificate ! provided by the 3rd party vendor. % The fully-qualified domain name in the certificate will be: webvpn.cisco.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itselfBEGIN
CERTIFICATE MIIFZiCCBE6aAwIBAaIOMs/oXuu9K14eMGSf0mYifTANBakahkiG9w0B
AOUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
${\tt EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x}$
QjBABgNV
BAsTOVR1cm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5j
dxJ11FN1
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4G AlUEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ21zY28gU31zdGVtczEOMAwGA1UECxQF VFNXRUIx

OjA4BgNVBAsUMVR1cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgrv
osBMMazg
5 5 1 2 1 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
oDBDBgNV
HR8EPDA6MDigNgA0hiJodHRwOi8vII1ZSII2VidXJILWNvbC52ZXJpc21n
hi5ib20v
IIIZSVH.ToYWwwMD&1LmNvbDBKBcMVHS&E0zBBMD8CCmCGS&GG+EIIBByIW
MTAuBaar
MIRVDYGI BAFFBOACNPY ja HPOAHMELIKO 3 d 3 au dmikka YND 7 2 4u Y2 0 t L 2 Novak 0 7 YNO
BGEF BQCCART JARKOCHMOLY 9505CUUMVYARNPZZ40125CUZNWCY 90ZRWO
VKUIBBIWFAIIKWIBBQUHAWEGCCSGAQUFBWMCMBOGAIUUIWQIMBAAFGII
KII+FRSUZAGZWJ4daMHgGCCSGAQUFBWEBBGWWaJARBggFBgEFBQCWAIII
L29JC3AudmvyaXNp224uY29tMEIGCCsGAQUFBZAChJ20dHRw018v012S
LWFpYS52ZXJpC2Inb15jb20v01ZSVHJpYWwyMDA1LWFpYS5jZX1wbgY1
KWYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ21mMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9y1DBd8N
7/yW30v3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
540021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0gQPBPx5FJSqMiUZGrvju50
END CERTIFICATE
quit
INFO: Certificate successfully imported
ciscoasa(config)#

步骤 7. 将 WebVPN 配置为使用新安装的证书

- 1. 单击 Configuration,单击 Properties,然后选择 SSL。
- 2. 在 Trustpoints 区域中,选择将用于终止 WebVPN 会话的接口。(本示例使用外部接口。)
- 3. 单击 Edit。此时将显示 Edit SSL Trustpoint 对话框。

Configuration > Properties > S	3L						
	SSL						
🕀 🖬 AAA Setup	Configure CCI assessments These exceptions official both ACDM and MANN (CAI assess						
-B Anti-Spoofing	Configure SSL parameters. These parameters affect both ASDM and WebVPN access.						
E-B ARP	Server SSL Version: Any Client SSL Version: Any						
🛃 Auto Update	Formation						
	Line year						
🔁 🔂 Certificate	Available Algorithms Add >> Active Algorithms Move Up						
E f Device Access	30ES-SHA1						
1 Device Administration	See Edit SSI Taustaniat						
E BHCP Services							
🔄 🚚 DNS	Specify an enrolled trustopint to be used for SSL at theritication on the outside interface. To enroll a trustopint						
High Availability and Scal	go to Configuration > Properties > Certificate > Enrolment.						
- Failover							
- Fragment							
-22 History Metrics							
HTTP/HTTPS	Interface: outside						
E-IQ IP Audit							
E Logging	Enrolled Trustpoint: my.verisign.trustp 💌						
Priority Queue							
SUNKPC Server							
Thread to	Circei nep						
LIFL Effering							
H- VALCE	Trustpoints						
a woor	Specify which enrolled trustopints if any should be used for SSL authentication on each interface. The fallback						
	trustpoint will be used on interfaces not associated with a trustpoint of their own.						
	Fallback Trustmint						
	Palback Hospore						
	Interface Trustpoint Edit						
	management						
	outside my, verisign trustpoint						

4. 从 Enrolled Trustpoint 下拉列表中,选择在<u>步骤 3 中创建的信任点。</u>

5. 单击 **OK**,然后单击 Apply。

现在,在指定接口上终止的所有 WebVPN 会话应该已使用新的证书。有关如何验证安装是否成功 的信息,请参阅本文档中的验证部分。

<mark>命</mark>令行示例

Ciscoasa ciscoasa(config)#ssl trust-point my.verisign.trustpoint outside ! Specifies the trustpoint that will supply the SSL ! certificate for the defined interface. ciscoasa(config)#write memory Building configuration... Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08 8808 bytes copied in 3.630 secs (2936 bytes/sec) [OK] ciscoasa(config)# ! Save configuration.

验证

本部分描述如何确认已成功安装第三方供应商证书。

替换 ASA 的自签名证书

本部分描述如何替换已安装的 ASA 自签名证书。

- 1. 向 Verisign 发送证书签名请求。从 Verisign 收到请求的证书后,便可在同一个信任点下直接 安装它。
- 2. 键入以下命令: crypto ca enroll Verisign系统将提示您回答问题。
- 3. 对于 Display Certificate Request to terminal, 输入 yes, 并将输出发送给 Verisign。
- 4. 在他们为您提供新证书后,键入以下命令: crypto ca import Verisign certificate

查看已安装的证书

ASDM 步骤

- 1. 单击 Configuration, 然后单击 Properties。
- 2. 展开 **Certificate**,然后选择 Manage Certificates。用于信任点身份验证的 CA 证书和由第三方 供应商颁发的身份证书应显示在 Manage Certificates 区域中。

Configuration > Properties > Certificate > Manage Certificates						
Startup Wizard	Manage Certificates					
🕀 🚮 AAA Setup	Manana the Cartificates associated with trustopists					
-B Anti-Spoofing	wanage ne cenncales associated with trasports.					
E-B ARP			[(1
🛃 Auto Update	Subject	Туре	Trustpoint	Status	Usage	Add
	VeriSign Trial	CA	my.verisign.tru	Available	General Purpo	
E-E Certificate	webvpn.cisco	Identity	my.verisign.tru	Available	General Purpo	Show Details
Authentication						
- Enrolment						Refresh
- Import Certificate						Nellosit
- Eng Key Pair						
Manage Certificates						Delete
E-lea Trustpoint						
Configuration						

命令行示例

ciscoasa
ciscoasa(config)# show crypto ca certificates
L Displays all contificates installed on the ACA
: Displays all certificates installed on the ASA.
Certificate Status: Available Certificate Serial Number:
32cfe85eebbd2b5e1e30649fd266237d Certificate Usage:
General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test CA ou=Terms
of use at https://www.verisign.com/cps/testca (c)05
ou=For Test Purposes Only. No assurances. o=VeriSign $$
Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of
use at www.verisign.com/cps/testca (c)05 ou=TSWEB
o=Cisco Systems l=Raleigh st=North Carolina c=US OCSP
AIA: URL: http://ocsp.verisign.com CRL Distribution
Points: [1] http://SVRSecure-
crl.verisign.com/SVRTrial2005.crl Validity Date: start
date: 00:00:00 UTC Jul 19 2007 end date: 23:59:59 UTC
Aug 2 2007 Associated Trustpoints:
my.verisign.trustpoint ! Identity certificate received
from 3rd party vendor displayed above. CA Certificate
Status: Available Certificate Serial Number:
63b1a5cdc59f78801da0636cf975467b Certificate Usage
Ceneral Durnose Public Key Type, RSA (2018 bits) Issuer
General rathoge rantic well the. Wey (2040 DICS) ISSUEL

Name: cn=VeriSign Trial Secure Server Test Root CA ou=For Test Purposes Only. No assurances. o=VeriSign\, Inc. c=US Subject Name: cn=VeriSign Trial Secure Server Test CA ou=Terms of use at https://www.verisign.com/cps/testca (c)05 ou=For Test Purposes Only. No assurances. o=VeriSign\, Inc. c=US Validity Date: start date: 00:00:00 UTC Feb 9 2005 end date: 23:59:59 UTC Feb 8 2015 Associated Trustpoints: my.verisign.trustpoint ! CA intermediate certificate displayed above.

使用 Web 浏览器验证为 WebVPN 安装的证书

要验证 WebVPN 是否使用新证书,请完成以下步骤:

- 1. 通过 Web 浏览器连接到 WebVPN 接口。将 https:// 以及用于请求证书的 FQDN(例如
 - ,https://webvpn.cisco.com)。如果收到下列安全警报之一,请执行与该警报对应的过程

: The Name of the Security Certificate Is Invalid or Does Not Match the Name of the Site验 证您使用的 FQDN/CN 是否正确,以便连接到 ASA 的 WebVPN 接口。必须使用请求身份证 书时定义的 FQDN/CN。可以使用 show crypto ca certificates trustpointname 命令验证证书 FQDN/CN。The security certificate was issued by a company you have not chosen to trust...要将第三方供应商根证书安装到 Web 浏览器,请完成以下步骤:在"Security Alert"对话 框中,单击 View Certificate。在"Certificate"对话框中,单击 Certificate Path 选项卡。选择位 于为您颁发的身份证书上方的 CA 证书,然后单击 View Certificate。单击 Install Certificate。 在"Certificate Install Wizard"对话框中,单击 Next。选择 Automatically select the certificate store based on the type of certificate 单选按钮,单击"Next",然后单击"Finish"。当收到安装 证书确认提示时,单击 Yes。显示 Import operation was successful 提示时,单击 OK,然后 单击"Yes"。注意:由于此示例使用Verisign试用证书,因此必须安装Verisign试用CA根证书 ,以避免用户连接时出现验证错误。

- 2. 双击 WebVPN 登录页右下角显示的锁图标。此时应显示已安装证书的信息。
- 3. 查看这些内容,以验证是否与您的第三方供应商证书相匹配。

Cert	tificate	<u>?</u> ×		
Ge	eneral Details Certification Path	_ 1		
	Certificate Information			
	This certificate is intended for the following purpose(s): •Ensures the identity of a remote computer			
	* Refer to the certification authority's statement for details.			
	Issued to: webypn.cisco.com	-		
	Issued by: VeriSign Trial Secure Server Test CA			
Valid from 8/14/2007 to 8/29/2007				
	Install Certificate Issuer Statemer	nt		
	0			

续订 SSL 证书的步骤

要续订 SSL 证书,请完成以下步骤:

- 1. 选择需要续订的信任点。
- 2. 选择 enroll。将显示以下消息:If it is successfully enrolled again, the current cert will be replaced with the new ones.是否要继续?
- 3. 选择 Yes。这将生成一个新 CSR。
- 4. 将此 CSR 发送给您的 CA,在返回证书后导入新 ID 证书。
- 5. 在外部接口上删除并重新应用信任点。

命令

在 ASA 上,可以在命令行中使用一些 show 命令来验证证书的状态。

• show crypto ca trustpoint — 显示已配置的信任点。

• show crypto ca certificate — 显示系统上安装的所有证书。

• show crypto ca crls — 显示缓存的证书撤销列表 (CRL)。

• show crypto key mypubkey rsa — 显示所有生成的加密密钥对。

故障排除

本部分提供的信息可用于对配置进行故障排除。

以下是您可能会遇到的一些可能的错误:

- % 警告: CA cert is not found. The imported certs might not be usable. INFO: Certificate successfully imported 对 CA 证书的身份验证不正确。请使用 show crypto ca certificate trustpointname 命令验证是否安装了 CA 证书。查找以 CA Certificate 开头的行。如果已安装 CA 证书,请验证它是否引用了正确的信任点。
- 错误:Failed to parse or verify imported certificate在安装身份证书时,如果您不具有通过相关 信任点验证的正确的中间或根 CA 证书验证,则可能会出现此错误。您必须删除此身份证书 ,然后使用正确的中间或根 CA 证书重新验证身份。请与您的第三方供应商联系以验证您收到 的 CA 证书是否正确。
- Certificate does not contain general purpose public key当您尝试将身份证书安装到错误的信任 点时,可能会出现此错误。这是因为您尝试安装无效的身份证书,或者与信任点关联的密钥对 不匹配身份证书中包含的公钥。请使用 show crypto ca certificates trustpointname 命令以验证 您是否将身份证书安装到正确的信任点。请查找以 Associated Trustpoints 开头的行:如果列出 了错误的信任点,则使用本文档中所述的过程删除并重新安装适当的信任点,并验证密钥对自 生成 CSR 以来是否未发生过更改。
- •错误消息:%PIX[ASA-3-717023 SSL无法为信任点[信任点名称]设置设备证书当为给定信任点 设置设备证书以对 SSL 连接进行身份验证时,如果发生故障,则会显示此消息。当 SSL 连接 恢复正常时,会尝试设置将要使用的设备证书。如果发生故障,则会记录一条错误消息,其中 包括将用于加载设备证书的已配置信任点以及发生故障的原因。信任点名称—SSL 未能设置设 备证书的信任点名称。建议操作:解决所报告的故障原因指出的问题。确保指定的信任点已注 册并具有设备证书。确保设备证书有效。重新注册信任点(如果需要)。

相关信息

- <u>如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书</u>
- 安全产品现场通知
- <u>请求注解 (RFC)</u>
- <u>技术支持和文档 Cisco Systems</u>