ASA/PIX 8.x：带Microsoft CA的使用数字证书验证的站点至站点IPSec VPN配置示例

目录

简介

本文档介绍如何在站点到站点 VPN 中的 Cisco 安全设备 (ASA/PIX) 8.x 上手动安装第三方供应商数字证书，以利用 Microsoft 证书颁发机构 (CA) 服务器对 IPSec 对等体进行身份验证。

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。

本文档假设 ASA/PIX 中事先不存在 VPN 配置。

注意： 本文档使用 Windows 2003 服务器作为此方案的 CA 服务器。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 8.0(2) 及 ASDM 6.0(2) 版的 Cisco ASA 5510 自适应安全设备

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。

相关产品

ASA 配置也可用于运行软件版本 8.x 的 Cisco 500 系列 PIX。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

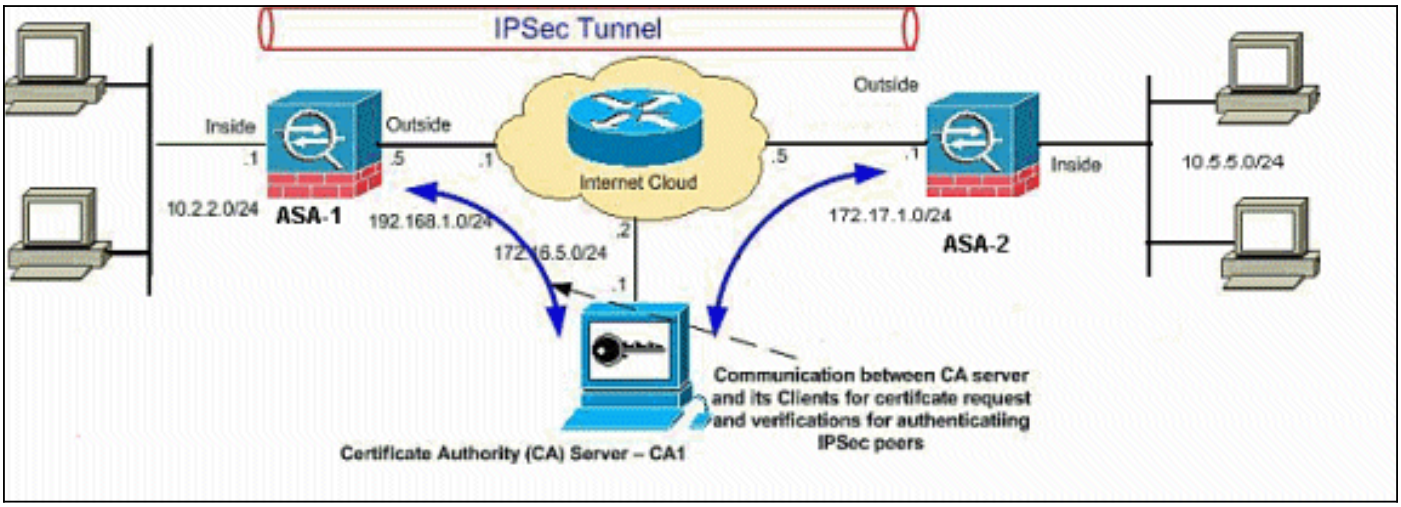
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置

本文档使用以下配置：

- ASA-1 分步配置
- ASA-1 配置概要

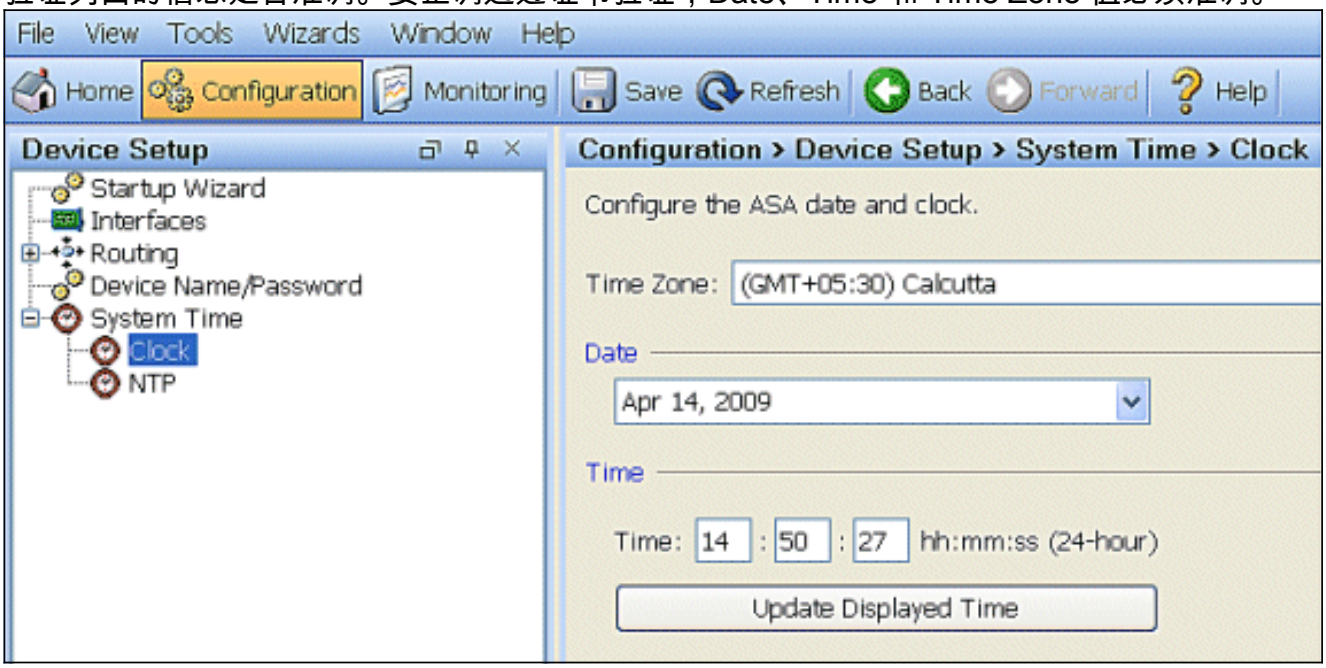
ASA-1 配置

要在 ASA 上安装第三方供应商数字证书，请执行下列步骤：

步骤 1. 验证 Date、Time 和 Time Zone 值是否准确

ASDM 步骤

1. 单击 **Configuration**，然后单击 Device Setup。
2. 展开 **System Time**，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

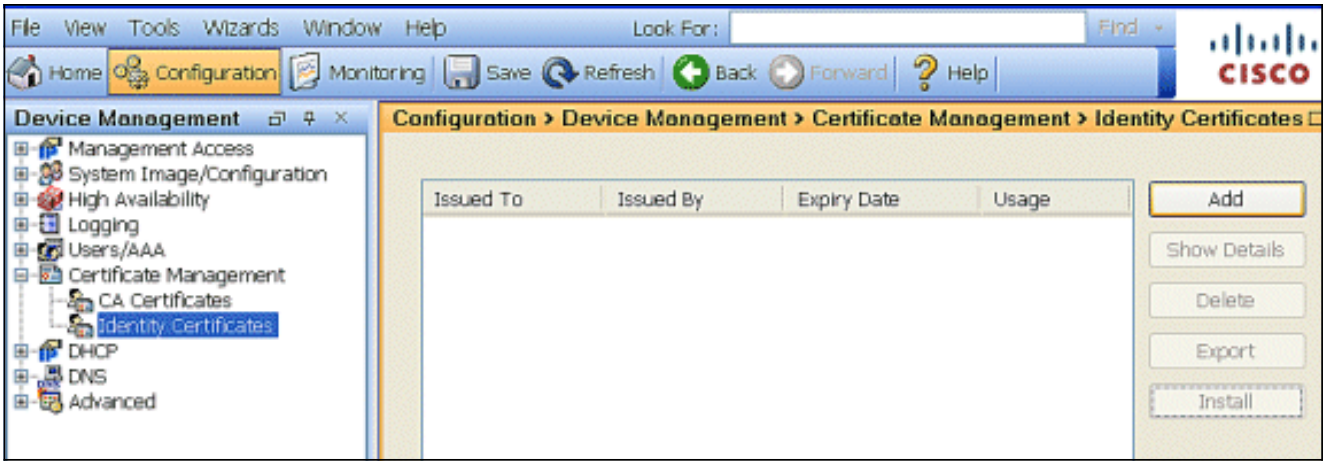
ASA-1
ASA-1# sh clock 14:53:15.943 IST Tue Apr 14 2009

步骤 2. 生成证书签名请求

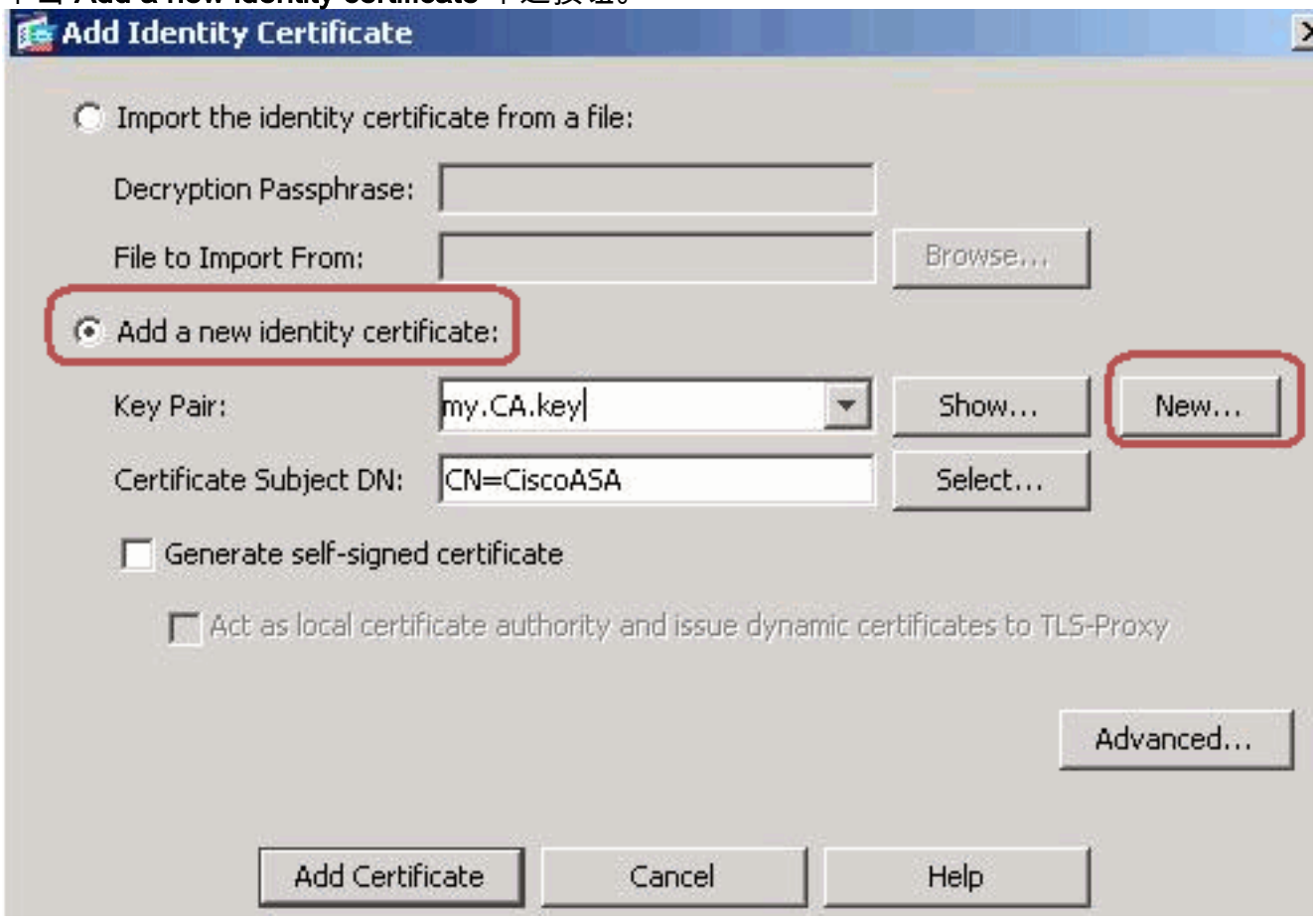
要让第三方 CA 发放身份证书，需要提供证书签名请求 (CSR)。CSR与其生成的公共密钥一起包含您的ASA特有名(DN)字符串。ASA 将使用生成的私钥对 CSR 进行数字签名。

ASDM 步骤

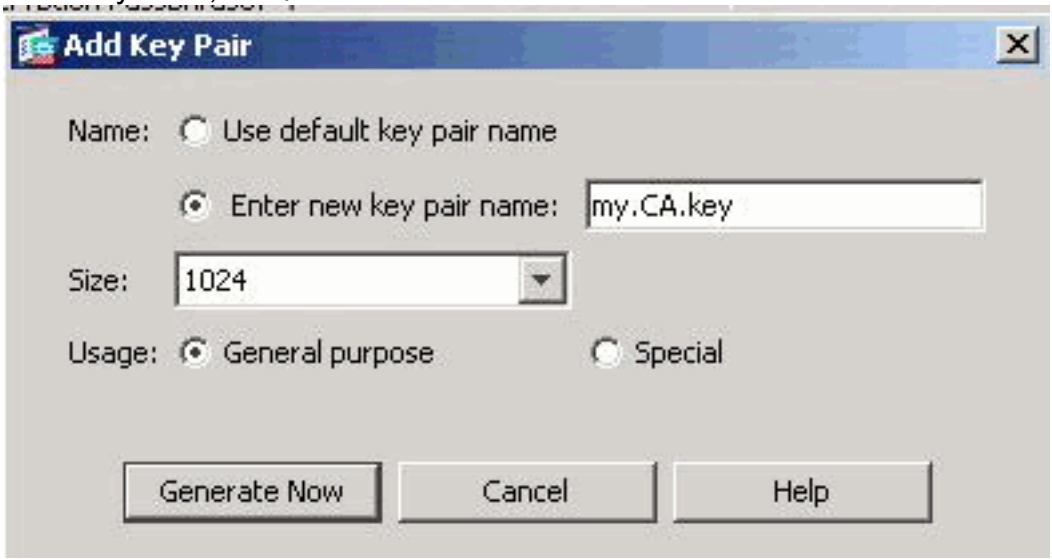
1. 转到 **Configuration > Device Management > Certificate Management > Identity Certificates**，然后单击 Add。



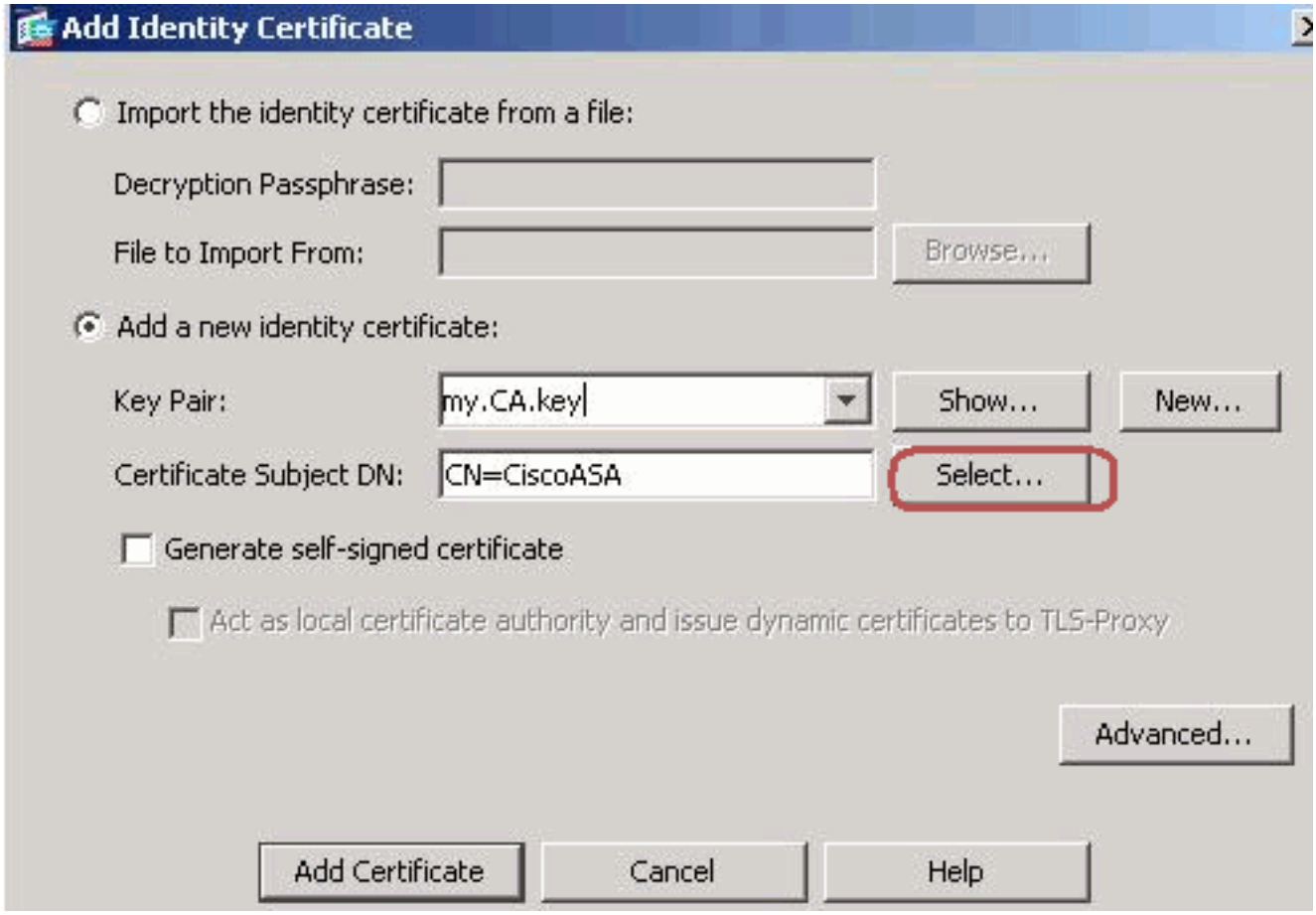
2. 单击 **Add a new identity certificate** 单选按钮。



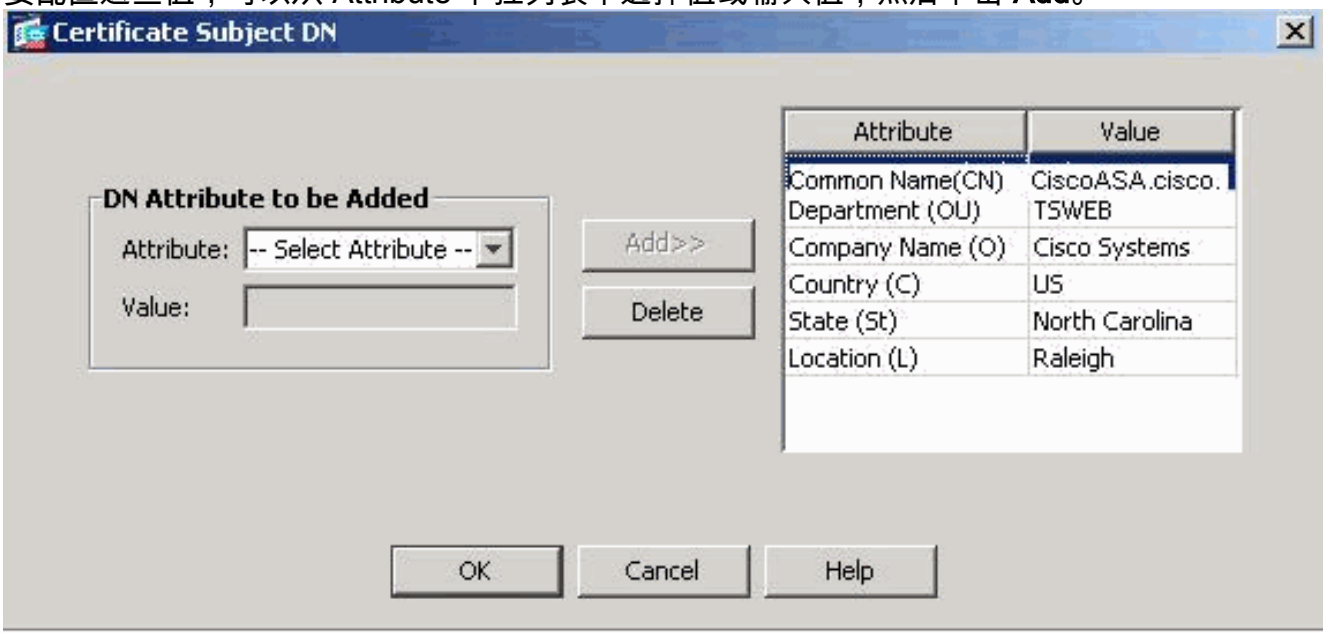
3. 对于 Key Pair，单击 **New**。



4. 单击 **Enter new key pair name** 单选按钮。您必须明确指出密钥对名称以进行识别。
5. 单击 **Generate Now**。这将立即创建密钥对。
6. 要定义 Certificate Subject DN，请单击 **Select**，然后配置下表中列出的属性：

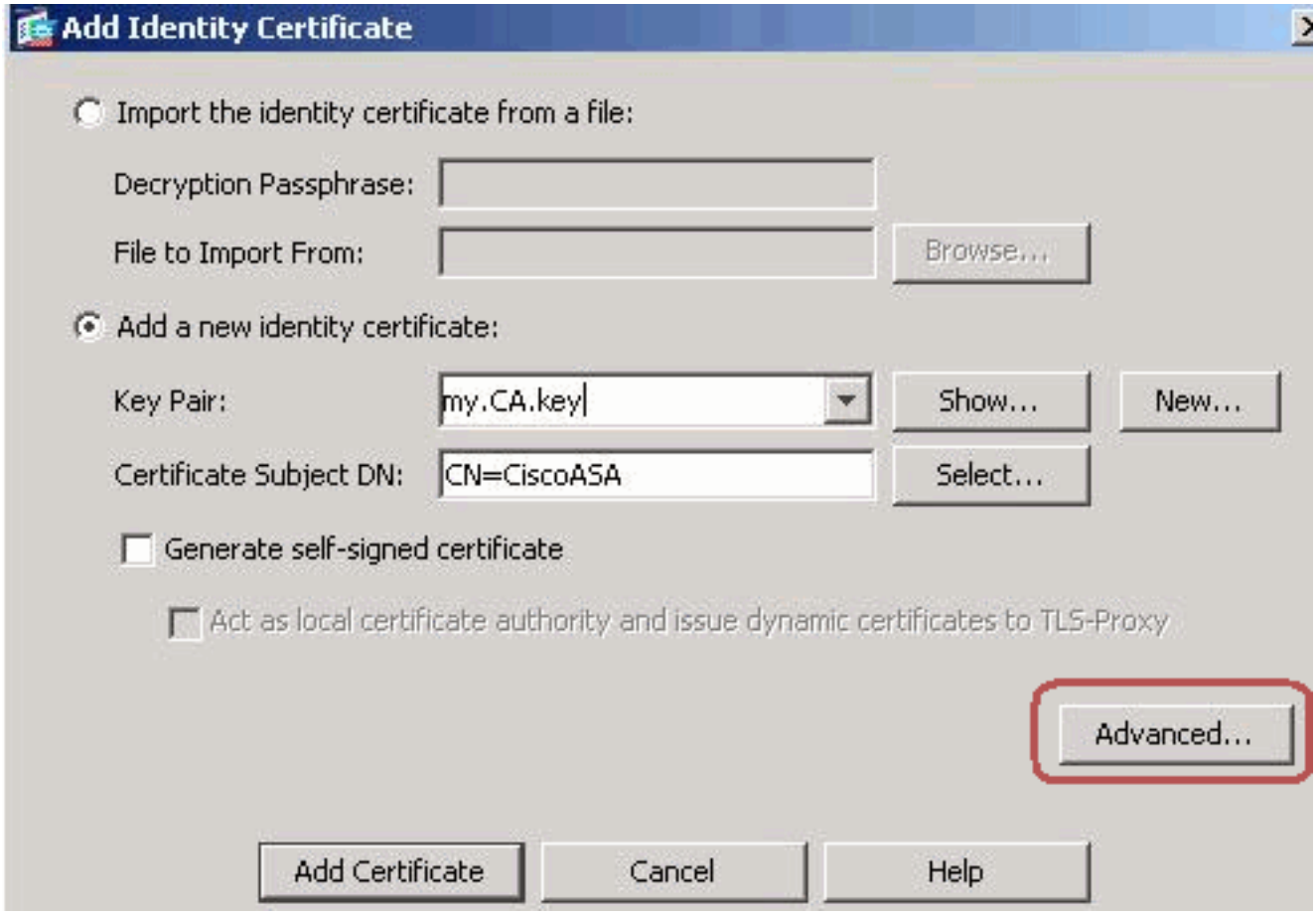


要配置这些值，可以从 Attribute 下拉列表中选择值或输入值，然后单击 **Add**。

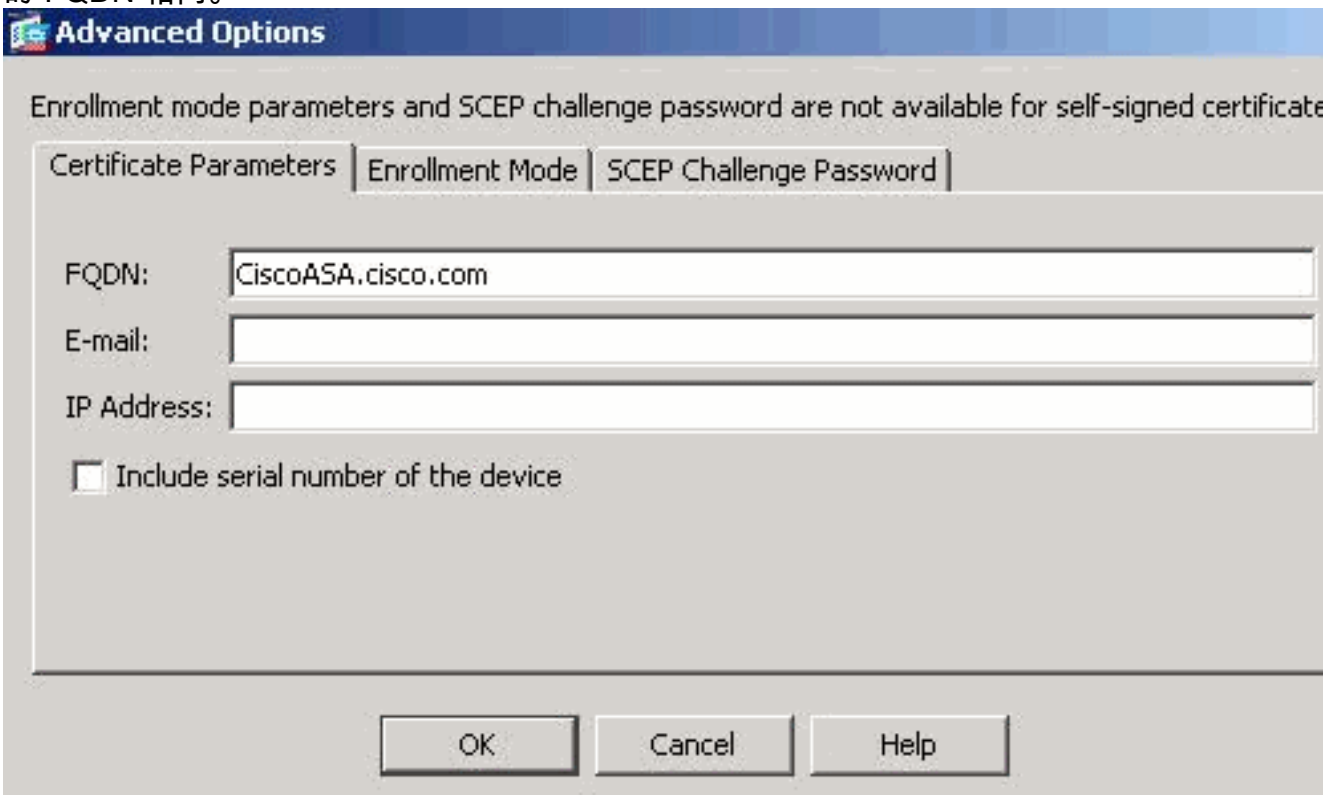


注意： 一些第三方供应商在发放身份证书之前要求提供特定属性。如果不确定需要提供什么属性，请与您的供应商联系以了解详细信息。

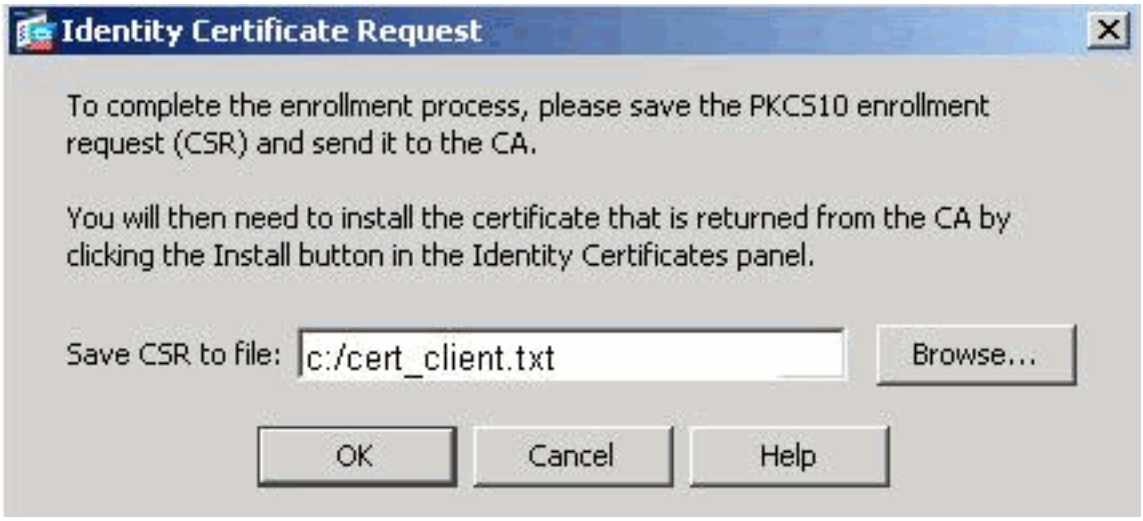
7. 添加相应的值之后，单击 **OK**。将会出现 Add Identity Certificate 对话框，并显示已填入的 Certificate Subject DN。
8. 单击 **Advanced**。



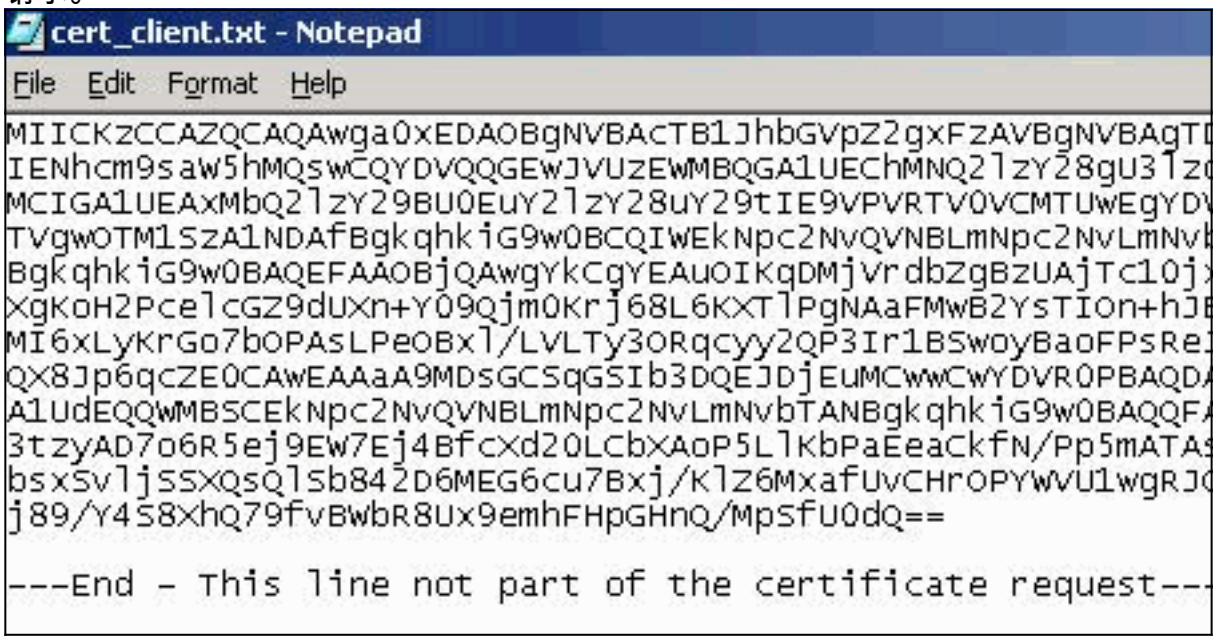
9. 在 FQDN 字段中，输入要用于从 Internet 访问设备的 FQDN。此值必须与用于公用名称 (CN) 的 FQDN 相同。



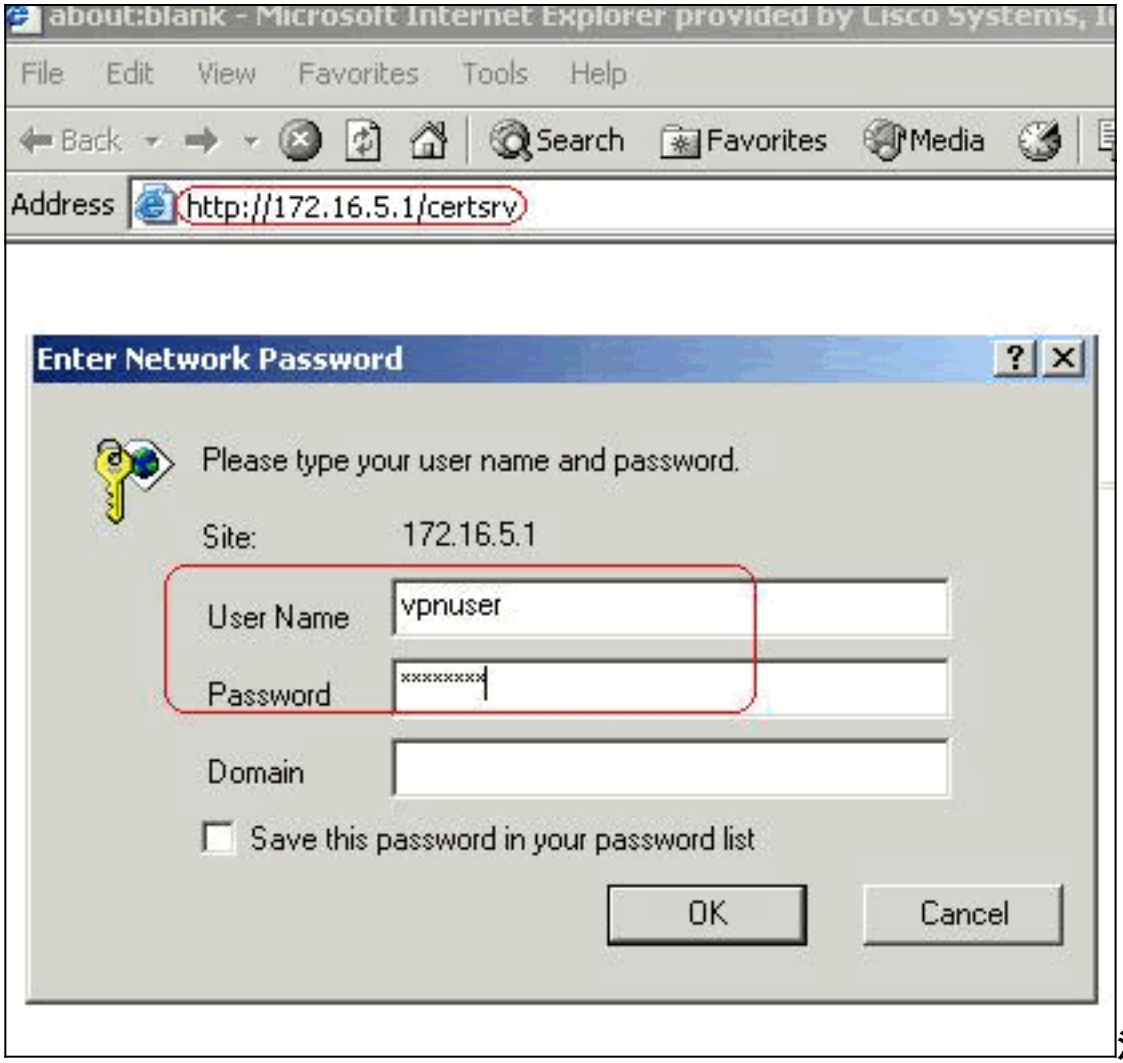
10. 单击 **OK**，然后单击 Add Certificate。系统会提示您将 CSR 保存到本地计算机上的文件中。



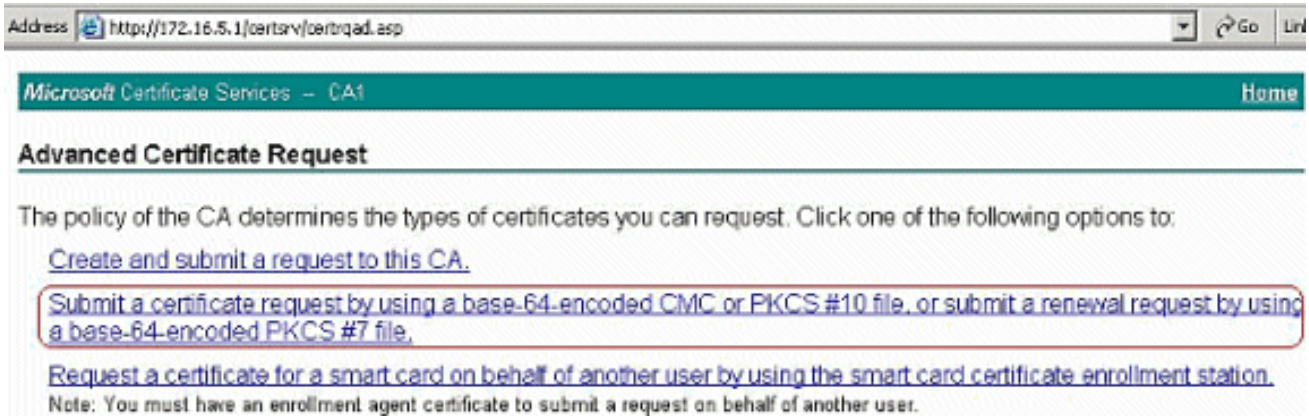
11. 单击 **Browse**，选择用于保存 CSR 的位置，然后使用 .txt 扩展名保存文件。**注意：** 使用 .txt 扩展名保存文件后，您可以使用文本编辑器（例如记事本）打开此文件，并查看 PKCS#10 请求。



12. 将保存的 CSR 提交到第三方供应商（例如 Microsoft CA），如下所示。使用为 VPN 服务器提供的用户凭证通过 Web 登录到 CA 服务器 172.16.5.1。

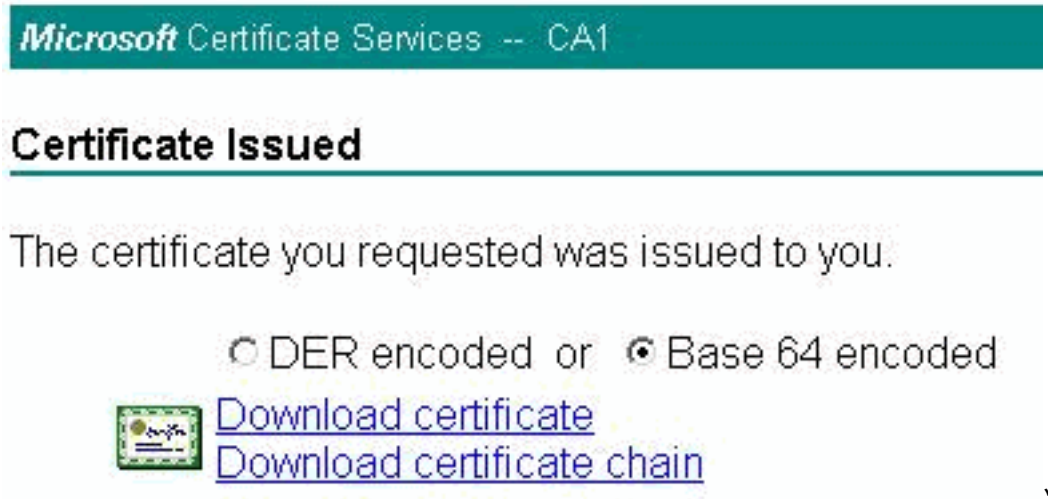


注意： 请确保您具有用于登录 CA 服务器的 ASA（vpn 服务器）用户帐户。单击 **Request a certificate > advanced certificate request**，然后选择 Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file。

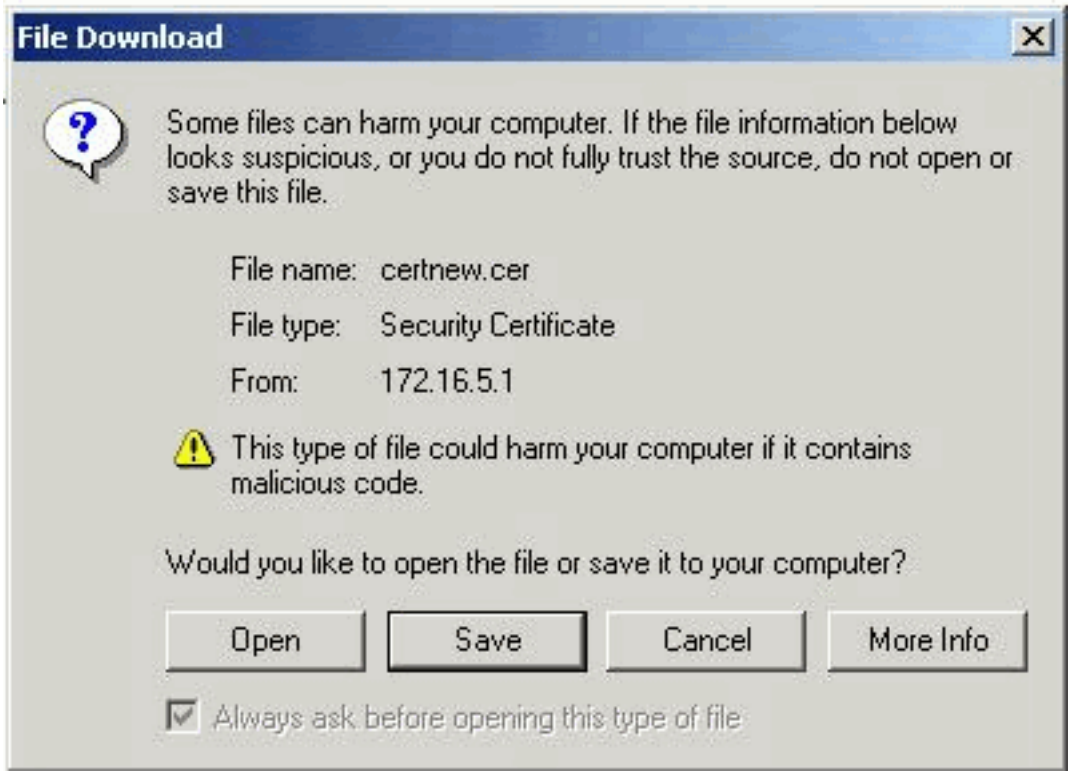


复制编码信息，并将其粘贴到 **Saved Request** 框中，然后单击 Submit。

单击 **Base 64 encoded** 单选按钮，然后单击 Download certificate。



将会出现 File Download 窗口。使用文件名 **cert_client_id.cer** 保存文件，这是要安装在 ASA 上的身份证书



-

命令行示例

ASA-1

```
ASA-1# configure terminal

ASA-1(config)#crypto key generate rsa label my.ca.key
modulus 1024 !--- 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... ASA-1(config)#crypto ca
trustpoint CA1 ASA-1(config-ca-trustpoint)# subject-name
CN=CiscoASA.cisco.com,OU=TSWEB, O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh !--- Defines
x.500 distinguished name. Use the attributes defined in
table as a guide. ASA-1(config-ca-trustpoint)#keypair
my.CA.key !--- Specifies key pair generated in Step 3
ASA-1(config-ca-trustpoint)#fqdn CiscoASA.cisco.com !---
Specifies the FQDN (DNS:) to be used as the subject
alternative name ASA-1(config-ca-trustpoint)#enrollment
terminal !--- Specifies manual enrollment. ASA-1(config-
ca-trustpoint)#exit ASA-1(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,
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]: no !--- Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: y !---
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 third
party CA. Certificate Request follows:
MIICKzCCAZQCAQAwga0xEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
```

```
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEk
MCIGA1UEAxMbQ2lzY29BU0EuY2lzY28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkcr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXTlPgNAaFMwB2YsTIOn+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBxl/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]: n ASA-1(config)#
```

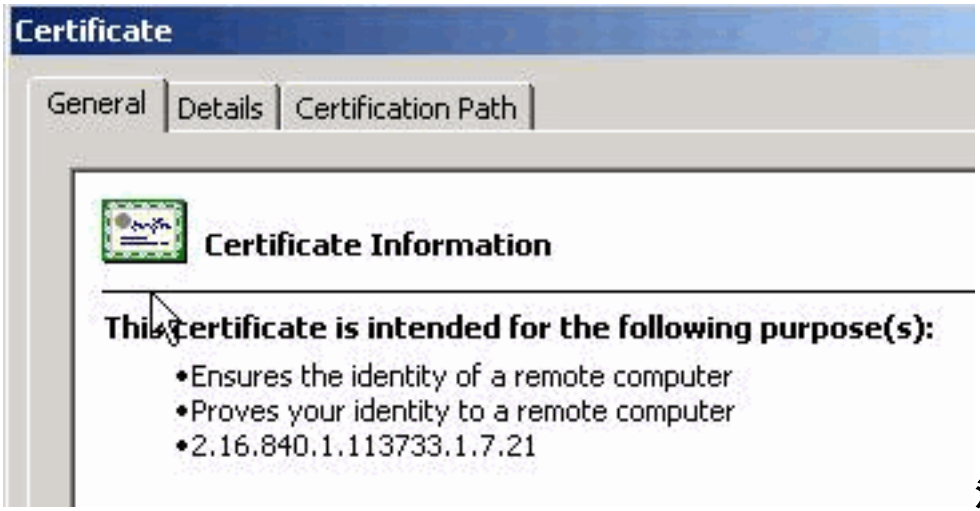
步骤 3. 验证信任点

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。

ASDM 步骤

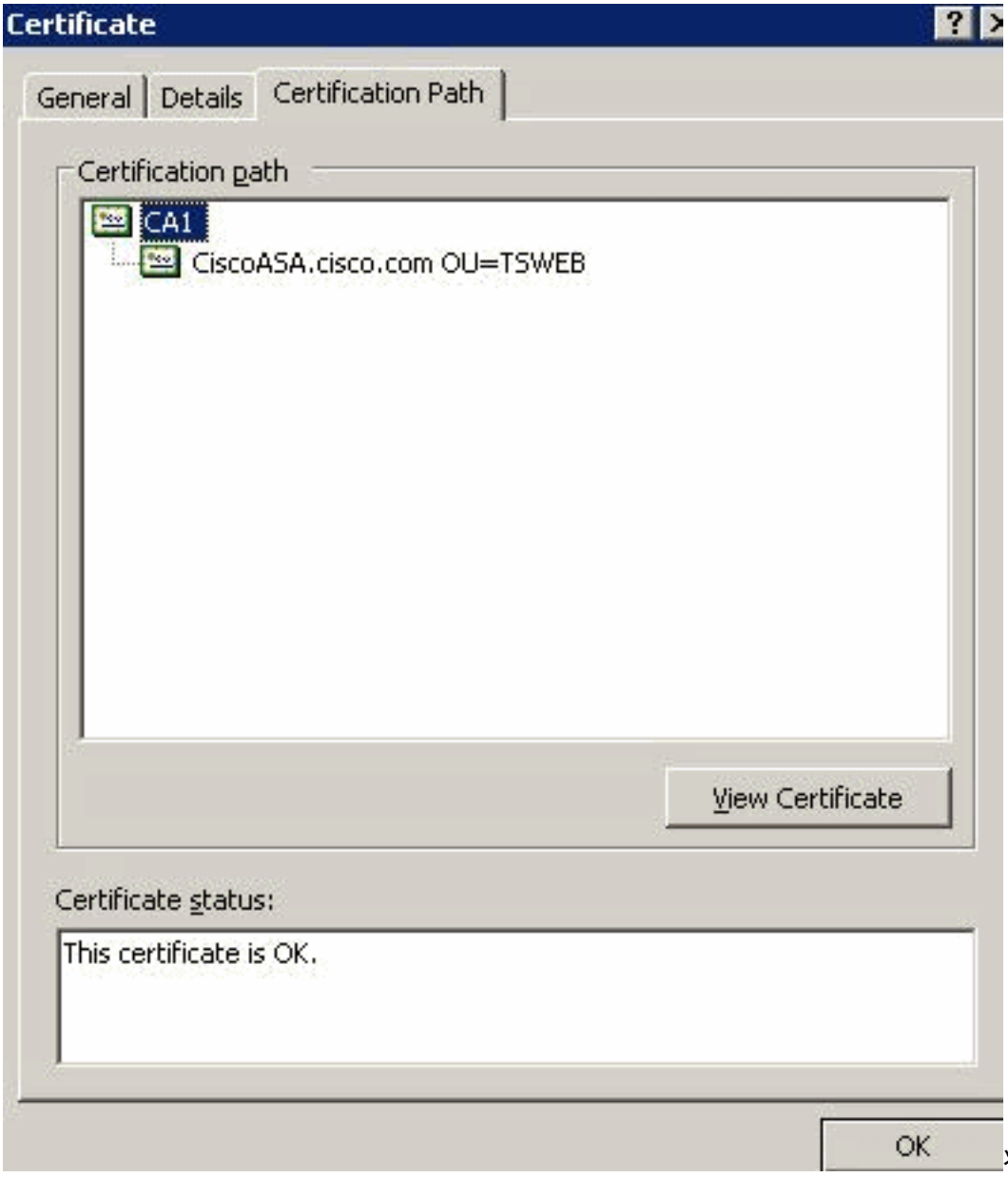
1. 将身份证书保存到本地计算机中。
2. 如果您收到的是非文件形式的 base64 编码证书，则必须复制此 base64 信息，并将其粘贴到文本文件中。
3. 将文件扩展名改为 .cer**注意：** 将文件扩展名改为 .cer 后，文件图标将显示为证书，如下所示。

4. 双击此证书文件。



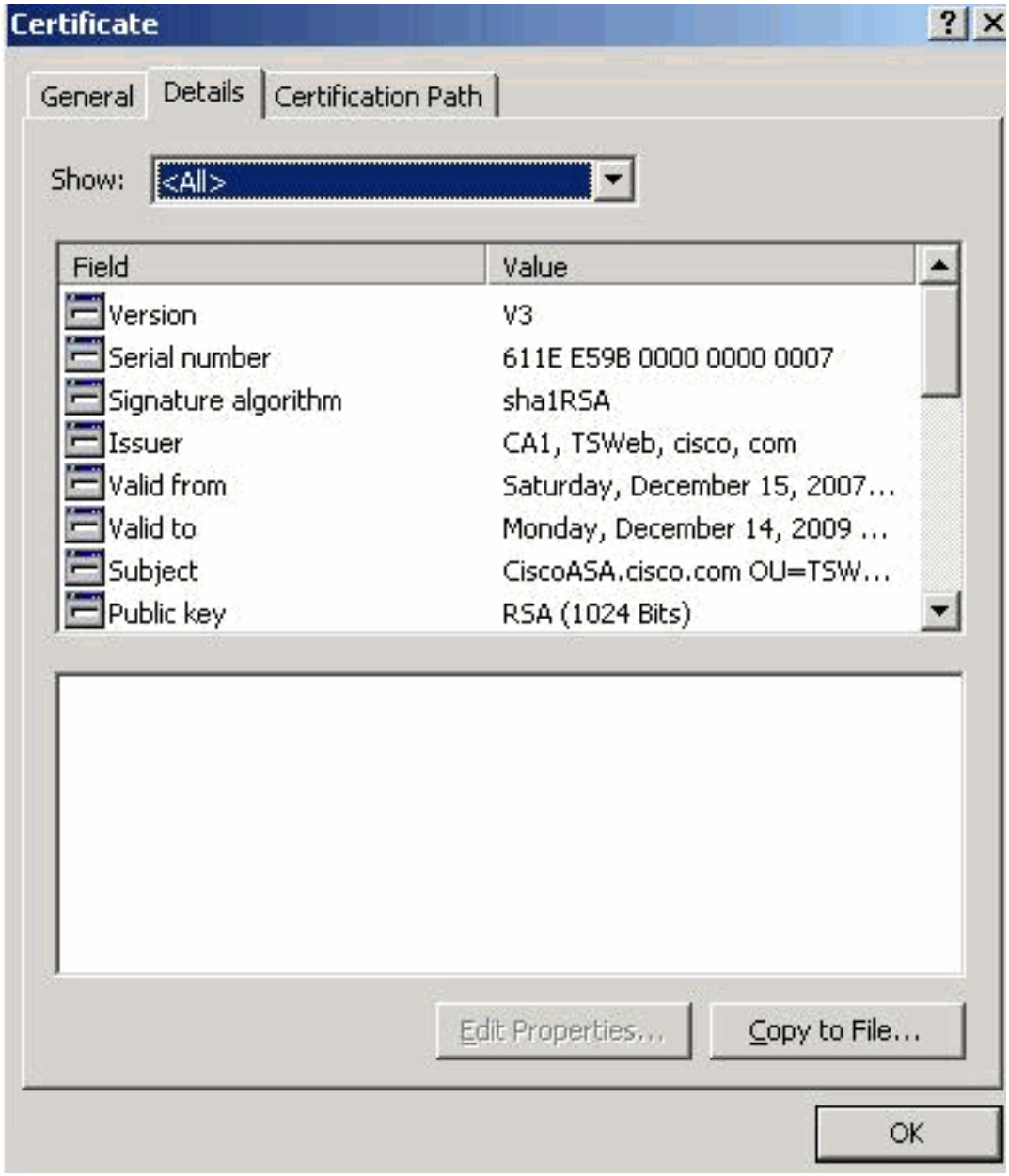
注意： 如果 General 选项卡中显示 Windows does not have enough information to verify this certificate 信息，则在继续执行此步骤之前，您必须获取第三方供应商的根 CA 或中间 CA 证书。请与第三方供应商或 CA 管理员联系，以获得其发放的根 CA 或中间 CA 证书。

5. 单击 **Certificate Path** 选项卡。
6. 单击与所发放的身份证书关联的 CA 证书，然后单击 **View Certificate**。

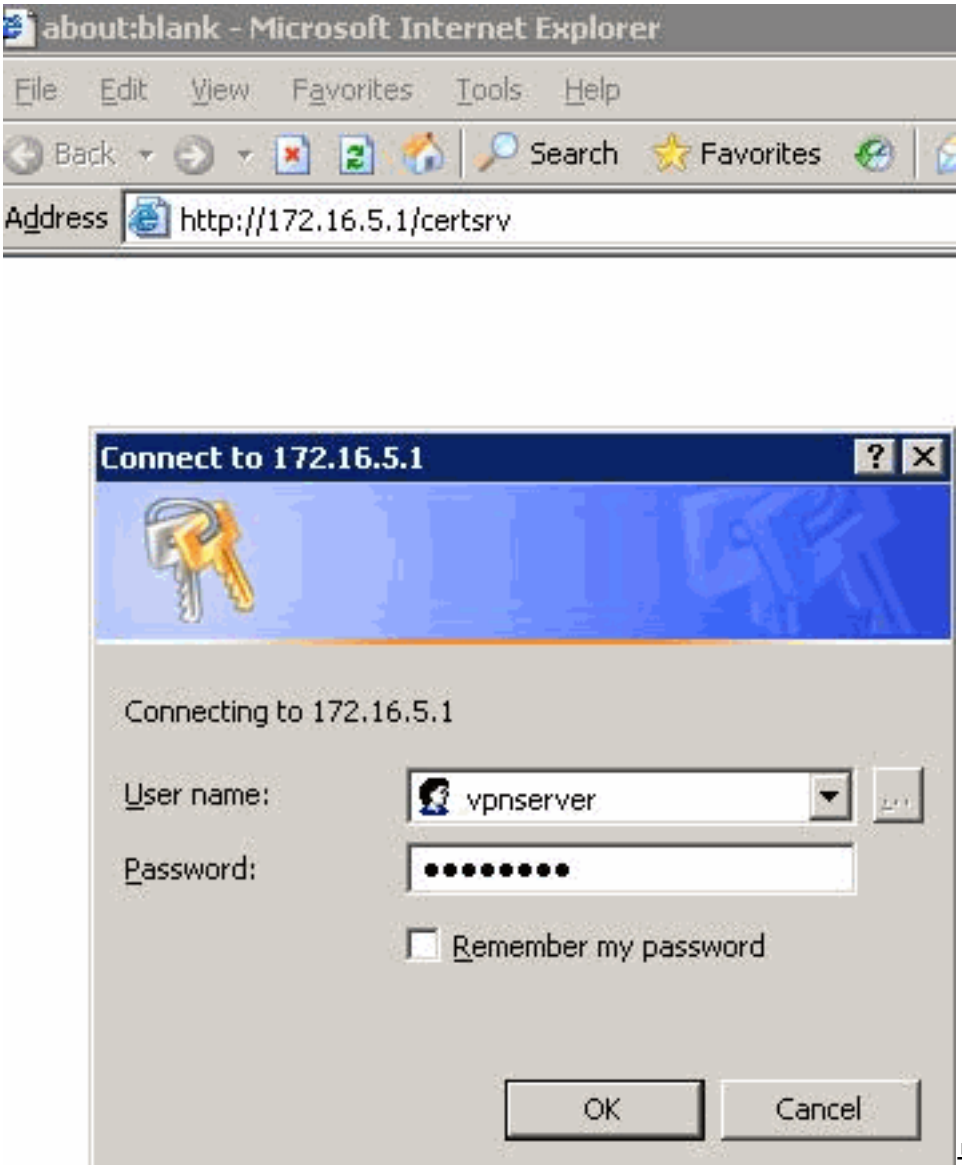


将会出现 CA 证书的详细信息。

7. 单击 **Details** 以查看身份证书的详细信息。



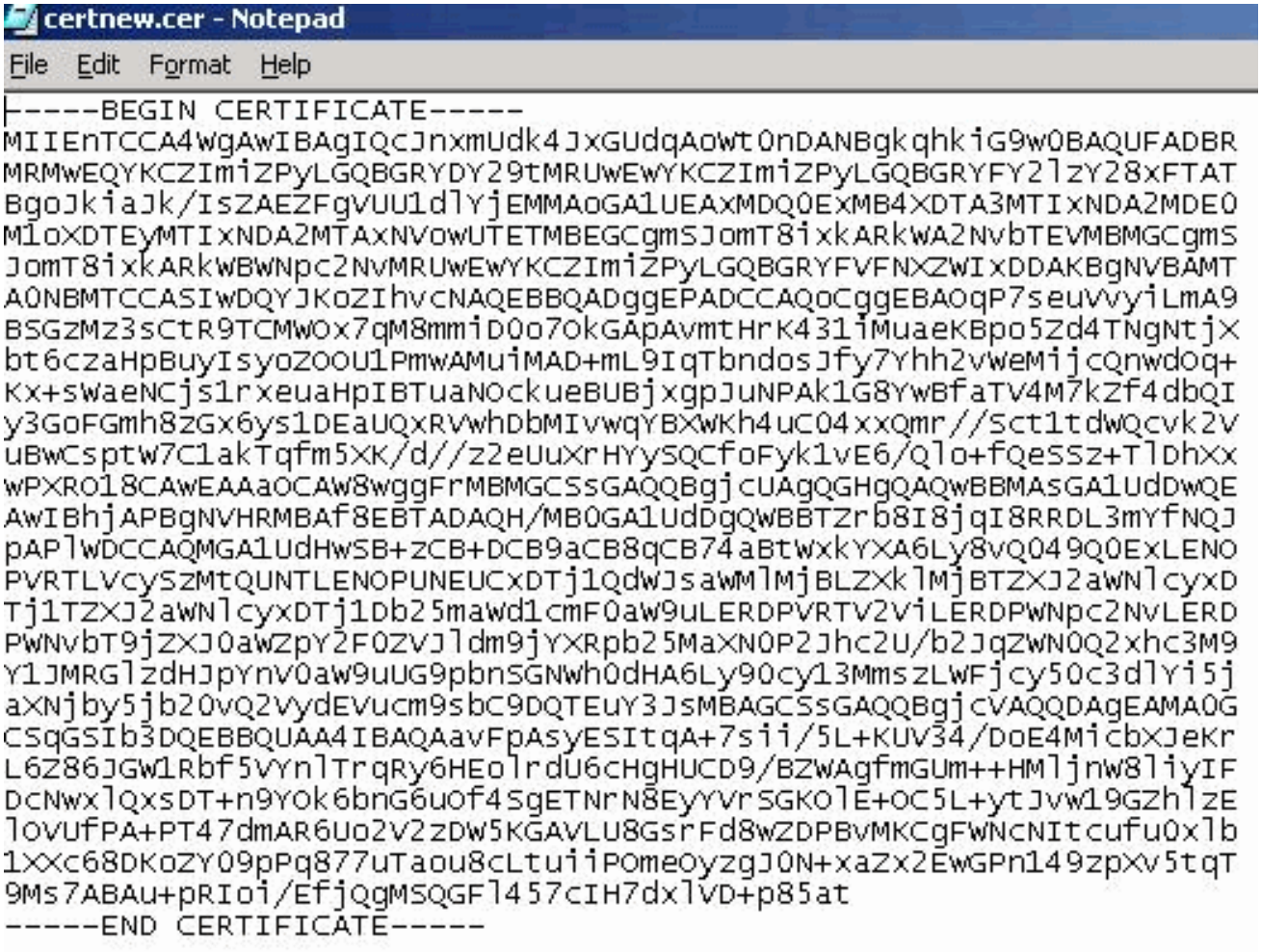
8. 在安装身份证书之前，您必须从 CA 服务器中下载 CA 证书，并将其安装到 ASA 中，如下所示。要从名为 **CA1** 的 CA 服务器中下载 CA 证书，请执行下列步骤。使用为 VPN 服务器提供的凭证通过 Web 登录到 CA 服务器 172.16.5.1。



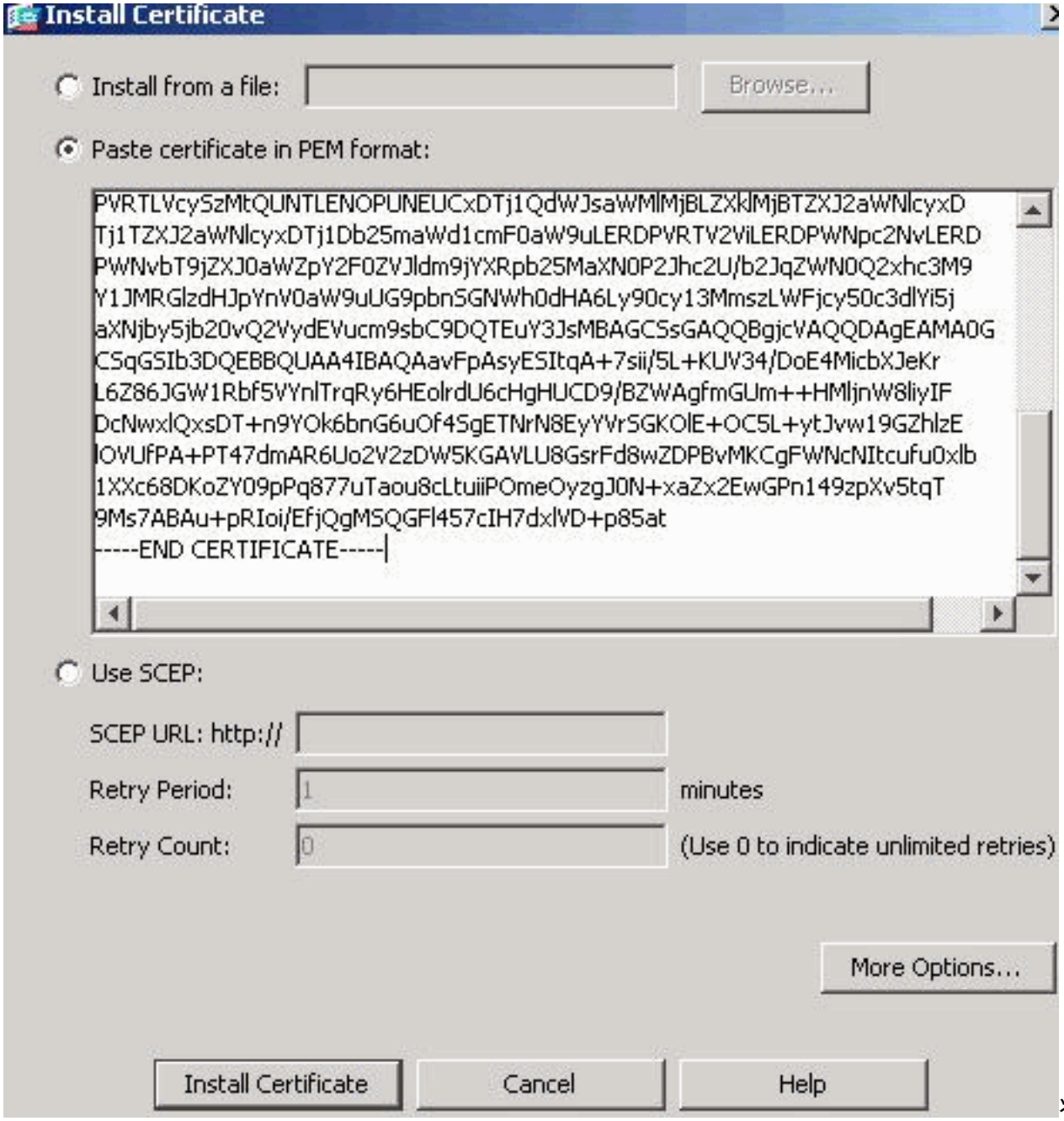
单击 **Download a CA certificate, certificate chain or CRL** 以打开如下所示的窗口。单击 **Base64** 单选按钮以选择其作为编码方法，然后单击 Download CA certificate。

使用文件名 **certnew.cer** 将 CA 证书保存到计算机中。

9. 浏览到 CA 证书的保存位置。
10. 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**。
11. 将会显示类似于下图中证书的 base64 编码信息
    :



12. 在 ASDM 中，单击 **Configuration**，然后单击 Device Management。
13. 展开 **Certificate Management**，然后选择 CA Certificates。
14. 单击 **Add**。
15. 单击 **Paste certificate in PEM Format** 单选按钮，然后将第三方供应商提供的 base64 CA 证书粘贴到文本字段中。
16. 单击 **Install Certificate**。



将会出现一个确认安装成功的对话框。

命令行示例

ASA-1
ASA-1(config)#**crypto ca authenticate CA1** *!--- Initiates the prompt for paste-in of base64 CA intermediate certificate. ! This should be provided by the third party vendor.* Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself **-----BEGIN CERTIFICATE-----** **MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B AQUFADBR** **MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lz Y28xFTAT** **BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx NDA2MDE0** **M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV MBMGCgmS** **JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK BgNVBAMT** **A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu**

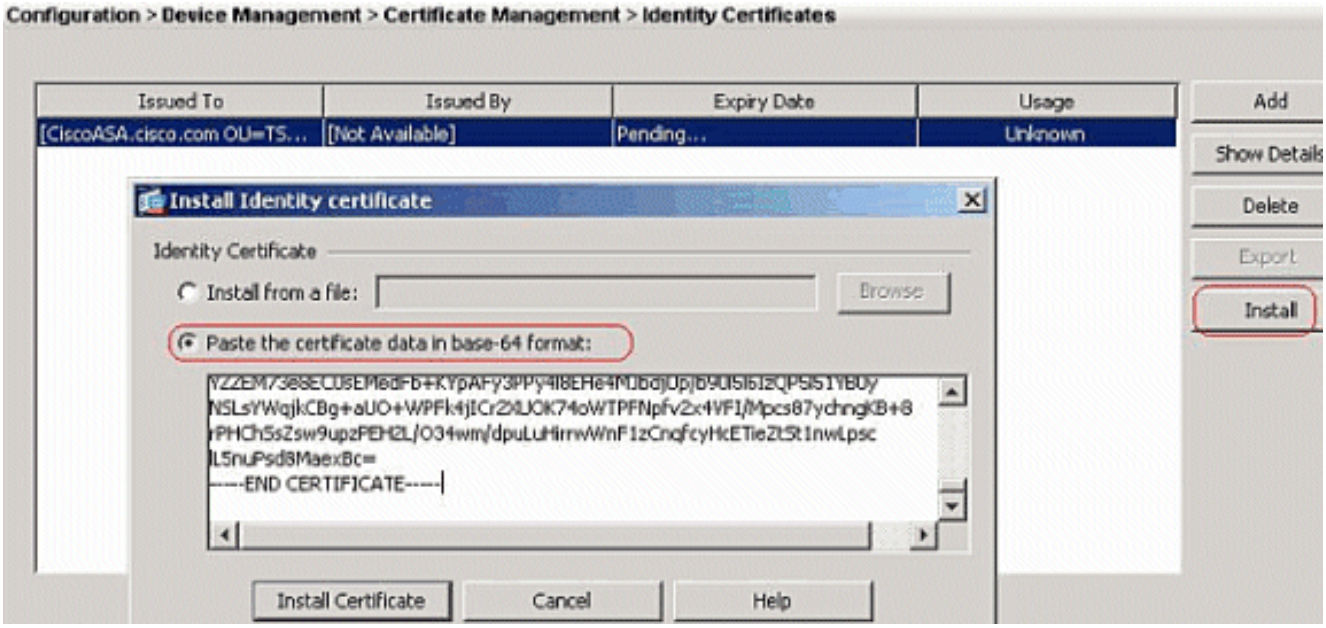
```
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSS
z+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
L3mYfNQJ
pAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2
aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMlj
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
cufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+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]: yes Trustpoint CA certificate accepted. %
Certificate successfully imported ASA-1(config)#
```

步骤 4. 安装证书

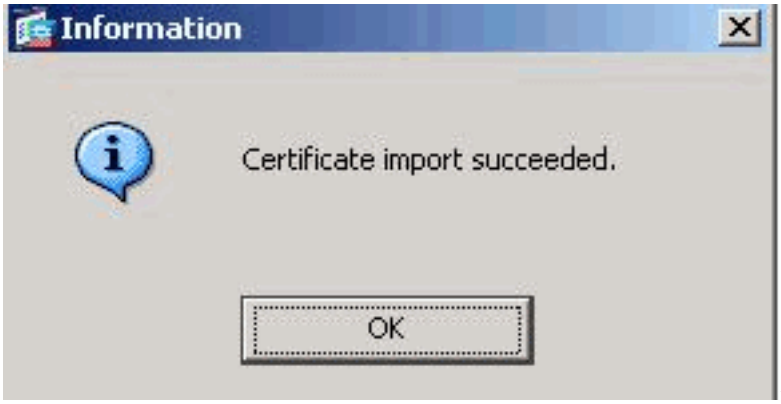
ASDM 步骤

使用第三方供应商提供的身份证书执行下列步骤：

1. 单击 **Configuration**，然后单击 Device Management。
2. 展开 **Certificate Management**，然后选择 Identity Certificates。
3. 选择您在步骤 2 中创建的身份证书。**注意：** Expiry Date 将显示 *Pending*。
4. 单击 **Install**。



单击 **Paste the certificate data in base-64 format** 单选按钮，然后将第三方供应商提供的身份证书粘贴到文本字段中。

5. 单击 **Install Certificate**。 

将会出现一个确认导入成功的对话框。

命令行示例

ASA-1

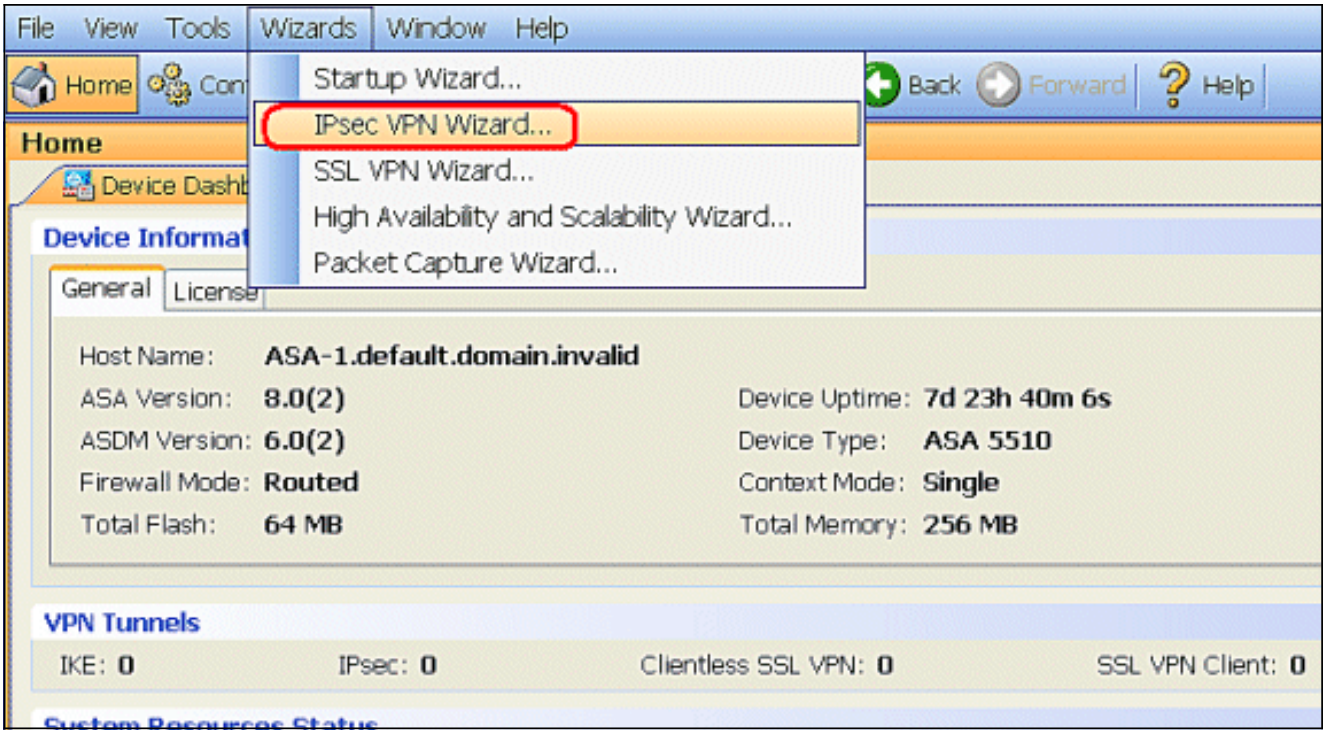
```
ASA-1(config)#crypto ca import CA1 certificate !---
Initiates prompt to paste the base64 identity !---
certificate provided by the third party vendor. %The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself !--- Paste the base 64 certificate provided by
the third party vendor. -----BEGIN CERTIFICATE-----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoXDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0
ZW1zMSQw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZIhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
```

```
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ2lz
Y29BU0Eu
Y2lzY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KMl0xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAPlWDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy4l8EHe4MJbdjUp/b90l5l6IzQP
5l51YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc lL5nuPsd8MaexBc= -----END CERTIFICATE----- quit
INFO: Certificate successfully imported ASA-1(config)#
```

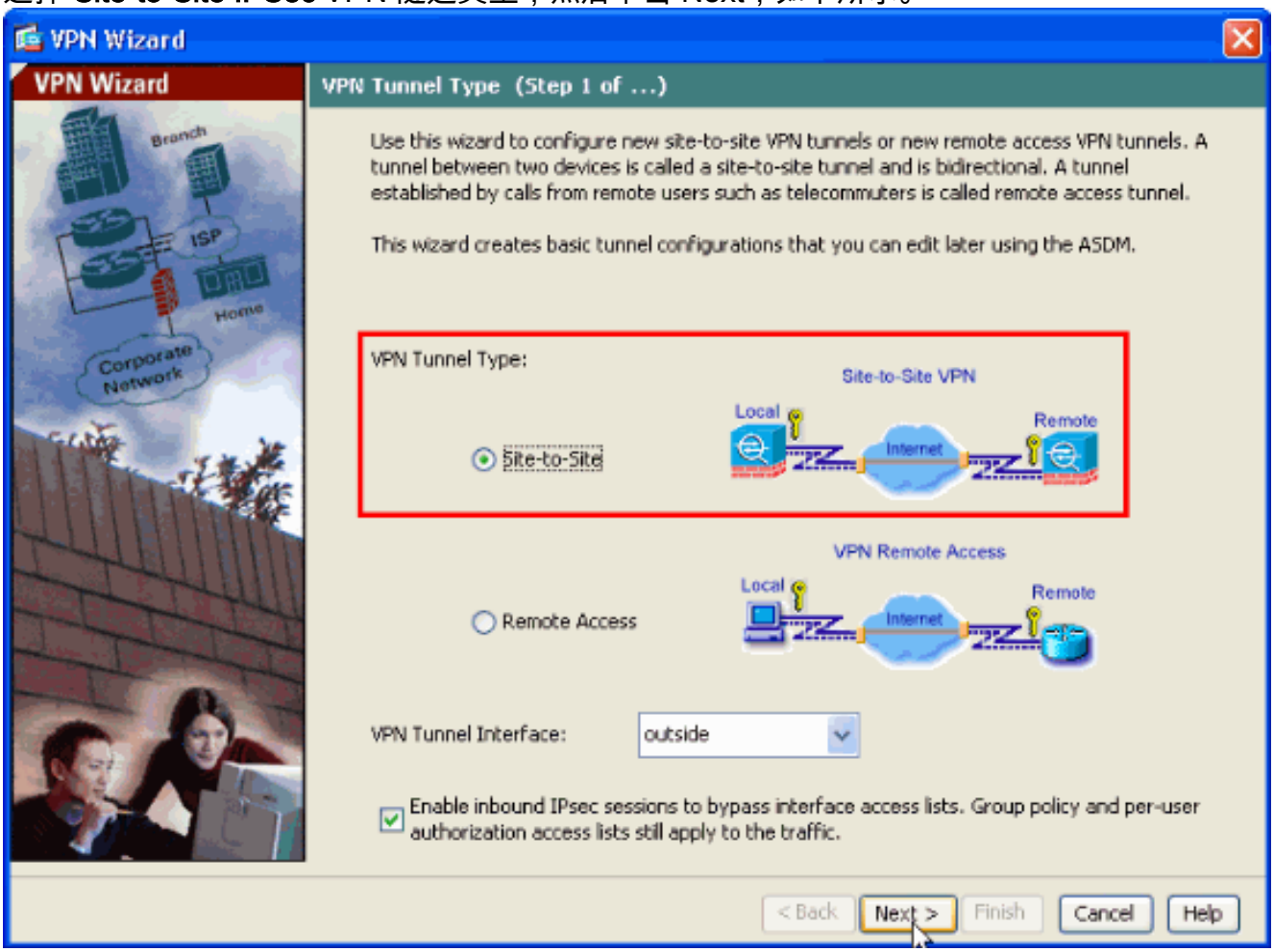
步骤 5. 配置站点到站点 VPN (IPSec) 以使用新安装的证书

完成以下步骤以创建 VPN 隧道：

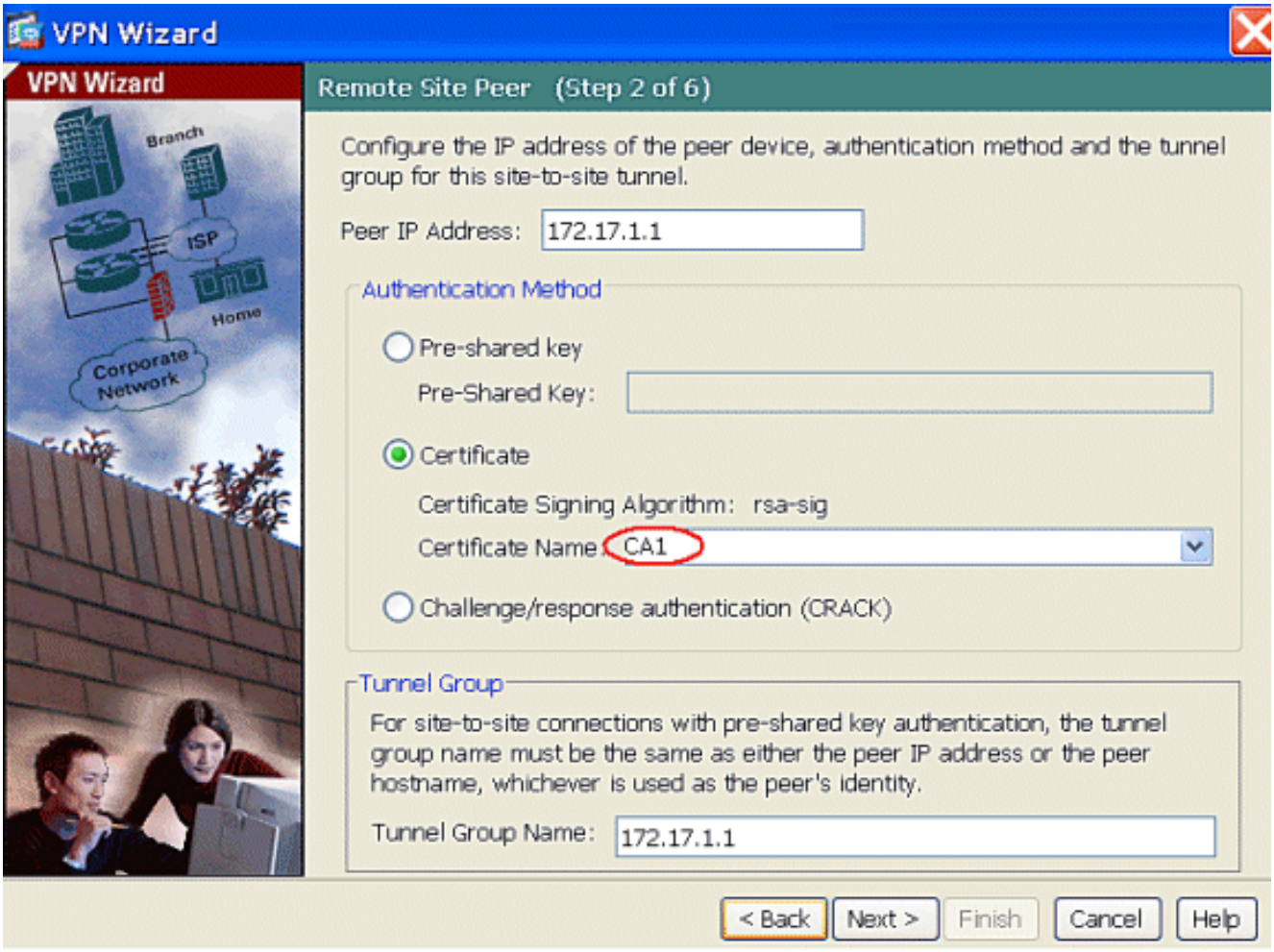
1. 打开浏览器并输入 **https://<为访问 ASDM 而配置的 ASA 接口的 IP 地址>**，以访问 ASA 上的 ASDM。
2. 单击 **Download ASDM Launcher and Start ASDM** 以下载 ASDM 应用程序的安装程序。
3. 下载 ASDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco ASDM 启动程序。
4. 输入使用 **http -** 命令配置的接口的 IP 地址，以及用户名和口令（如果已指定）。
5. 在 ASDM 应用程序连接到 ASA 之后，运行 **IPsec VPN Wizard**。



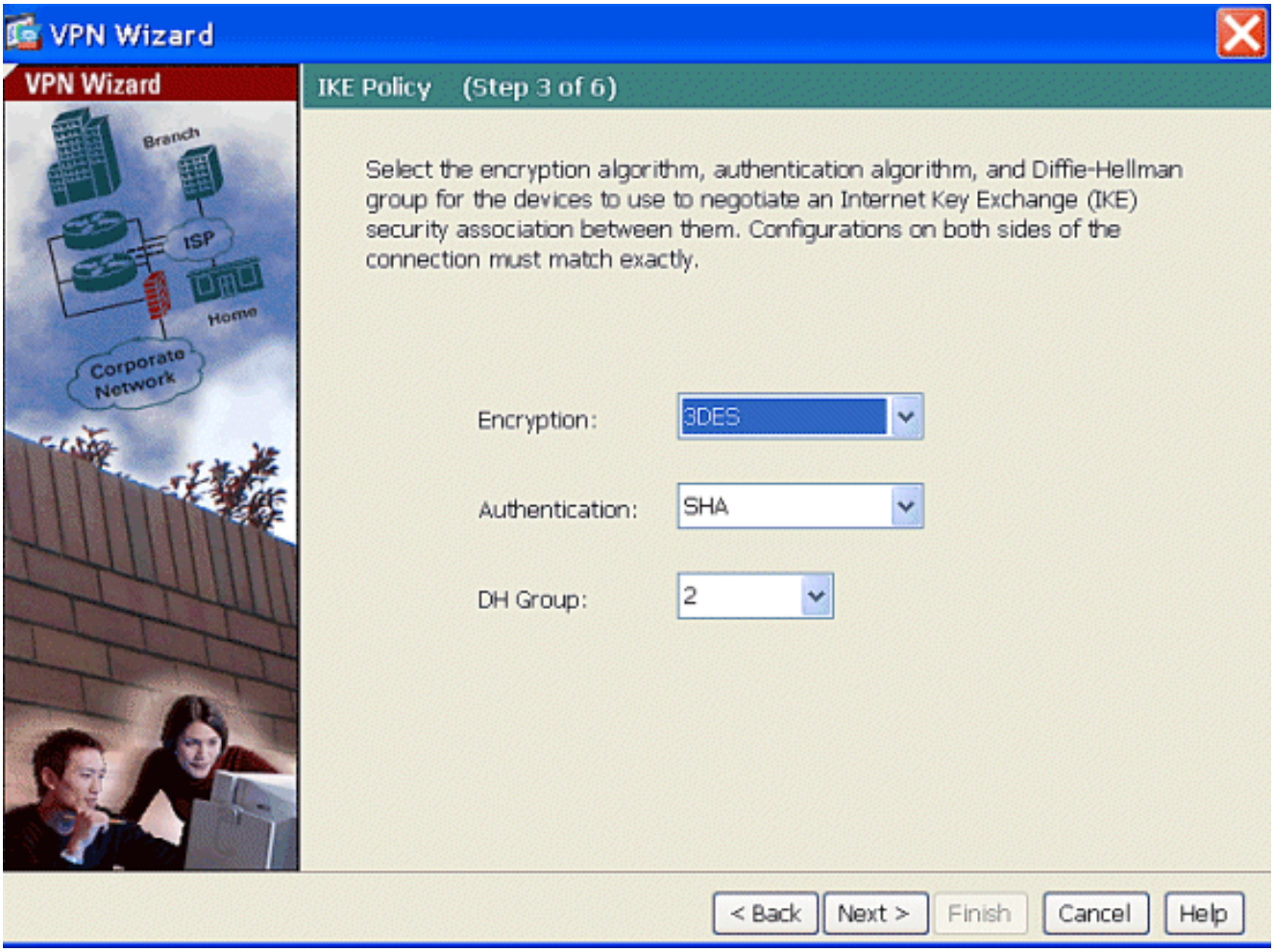
6. 选择 **Site-to-Site IPSec** VPN 隧道类型，然后单击 Next，如下所示。



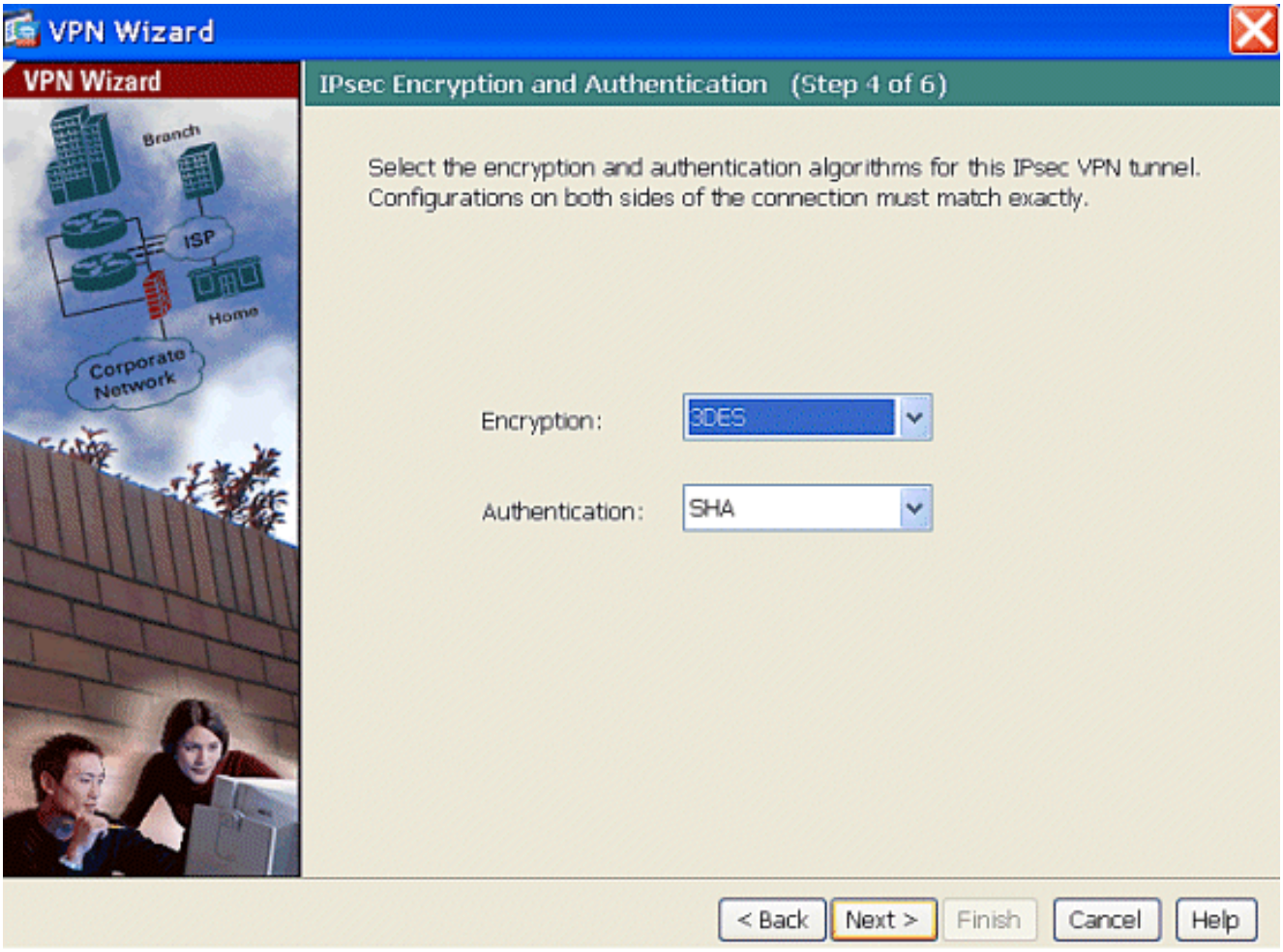
7. 指定远程对等体的外部 IP 地址。输入要使用的身份验证信息，在本示例中是预共享密钥。本示例中使用的预共享密钥是 **cisco123**。如果您配置 L2L VPN，默认情况下 **Tunnel Group Name** 为外部 IP 地址。单击 **Next**。



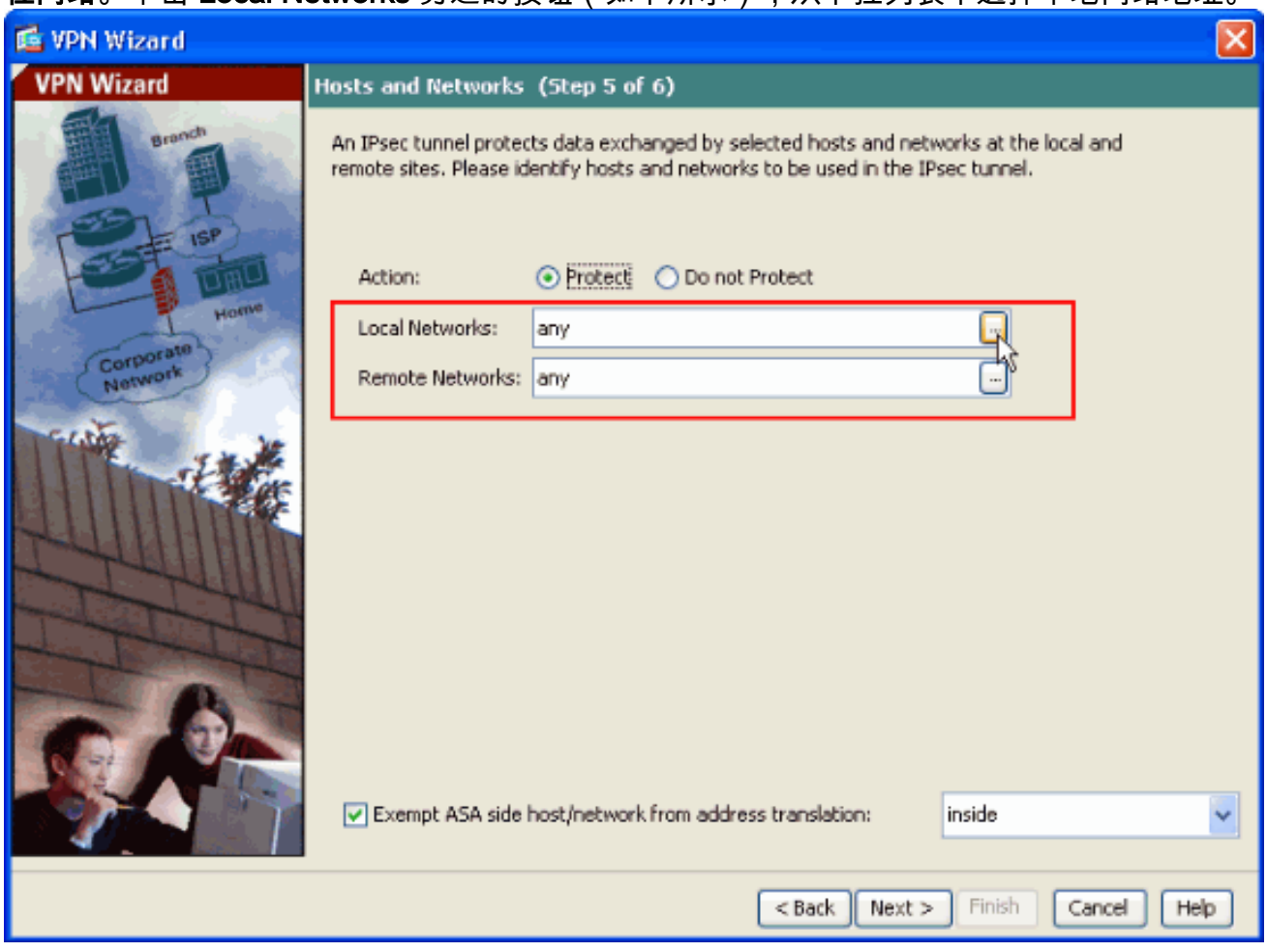
8. 指定要用于 IKE 的属性，也称为“第 1 阶段”。这些属性在 ASA 和 IOS 路由器上必须相同。单击 **Next**。



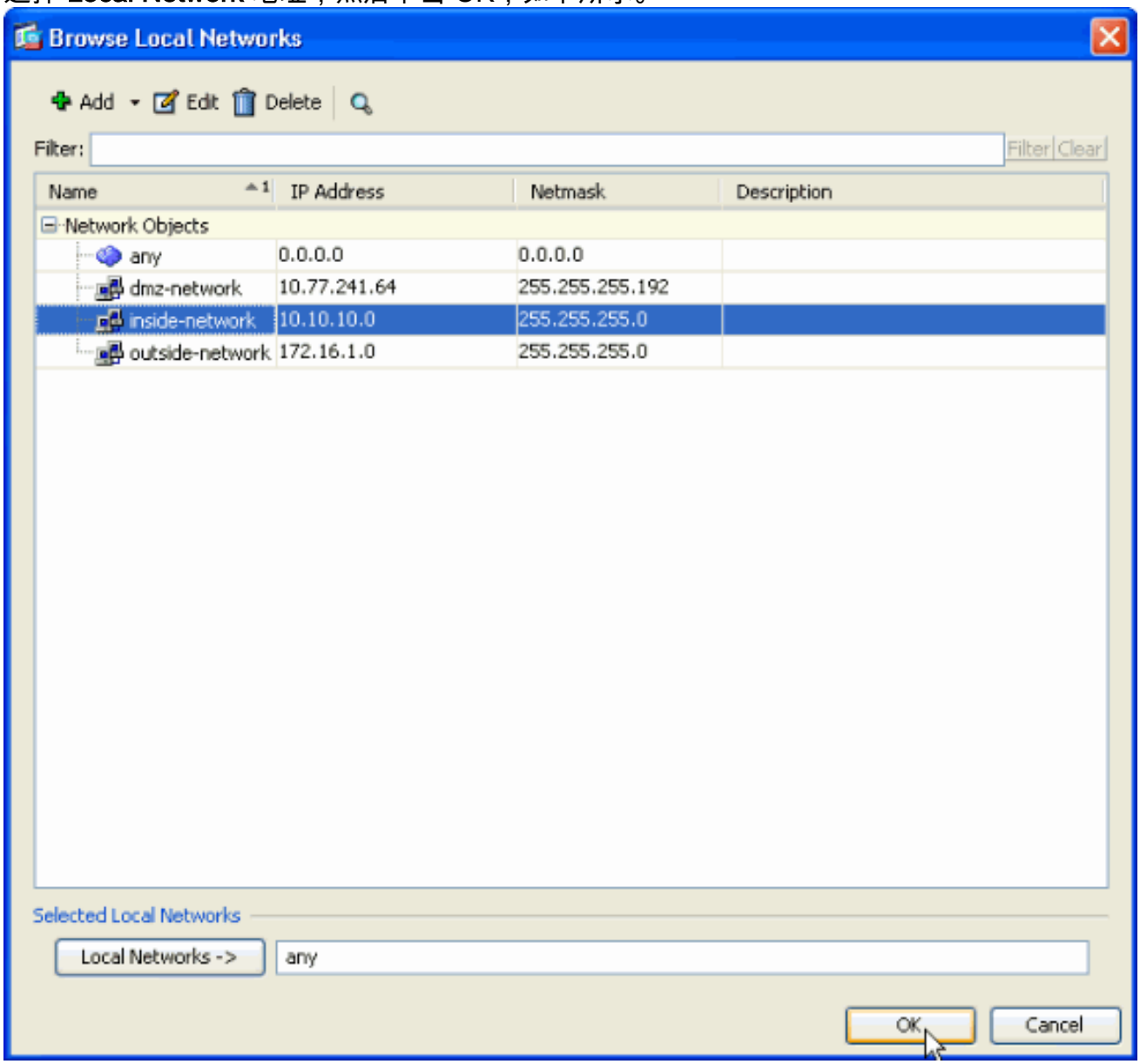
9. 指定要用于 IPsec 的属性，也称为“第 2 阶段”。这些属性在 ASA 和 IOS 路由器上必须匹配。单击 **Next**。



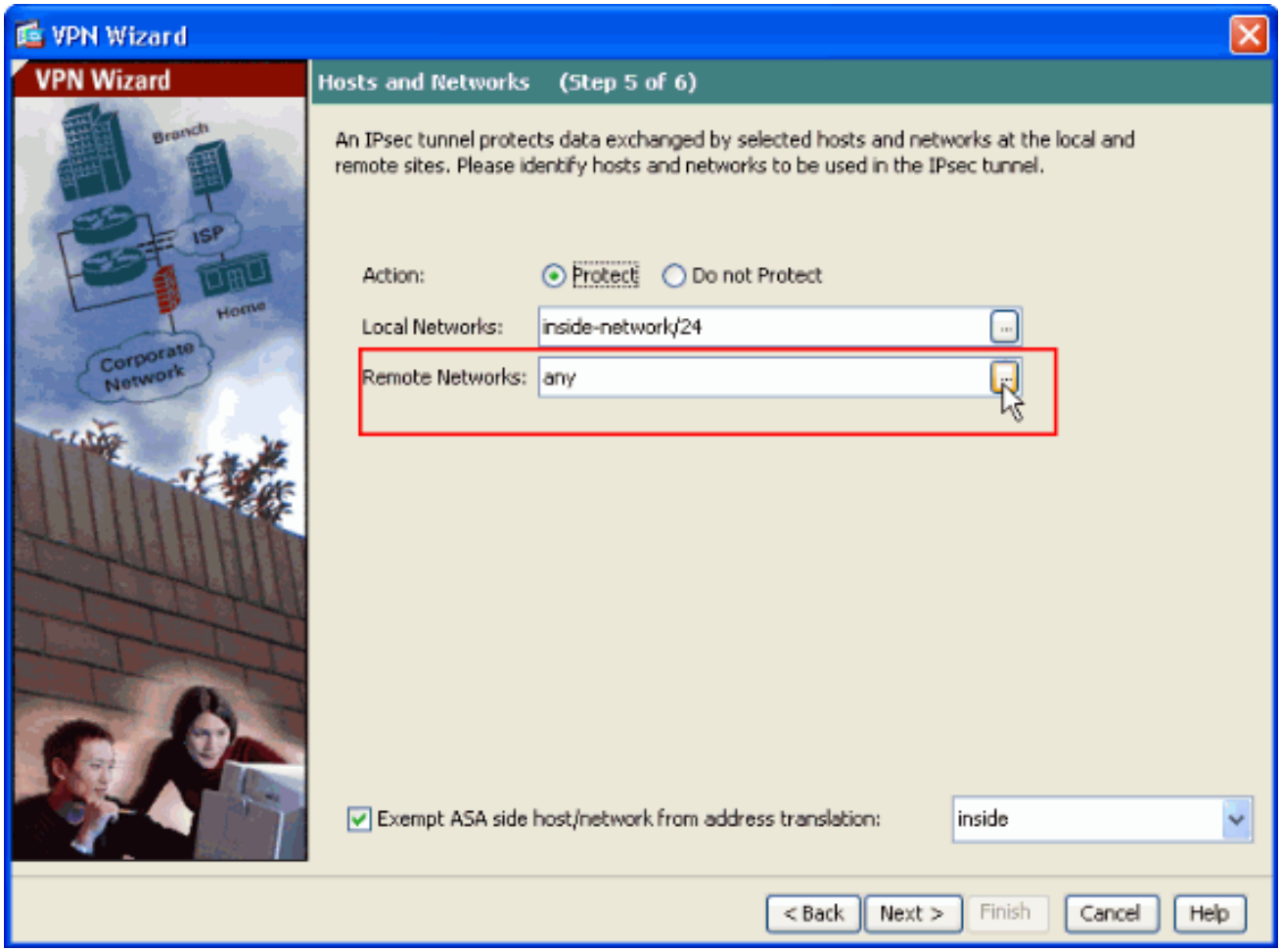
10. 指定必须允许其数据流通过 VPN 隧道的主机。在此步骤中，必须提供 VPN 隧道的**本地和远程网络**。单击 **Local Networks** 旁边的按钮（如下所示），从下拉列表中选择本地网络地址。



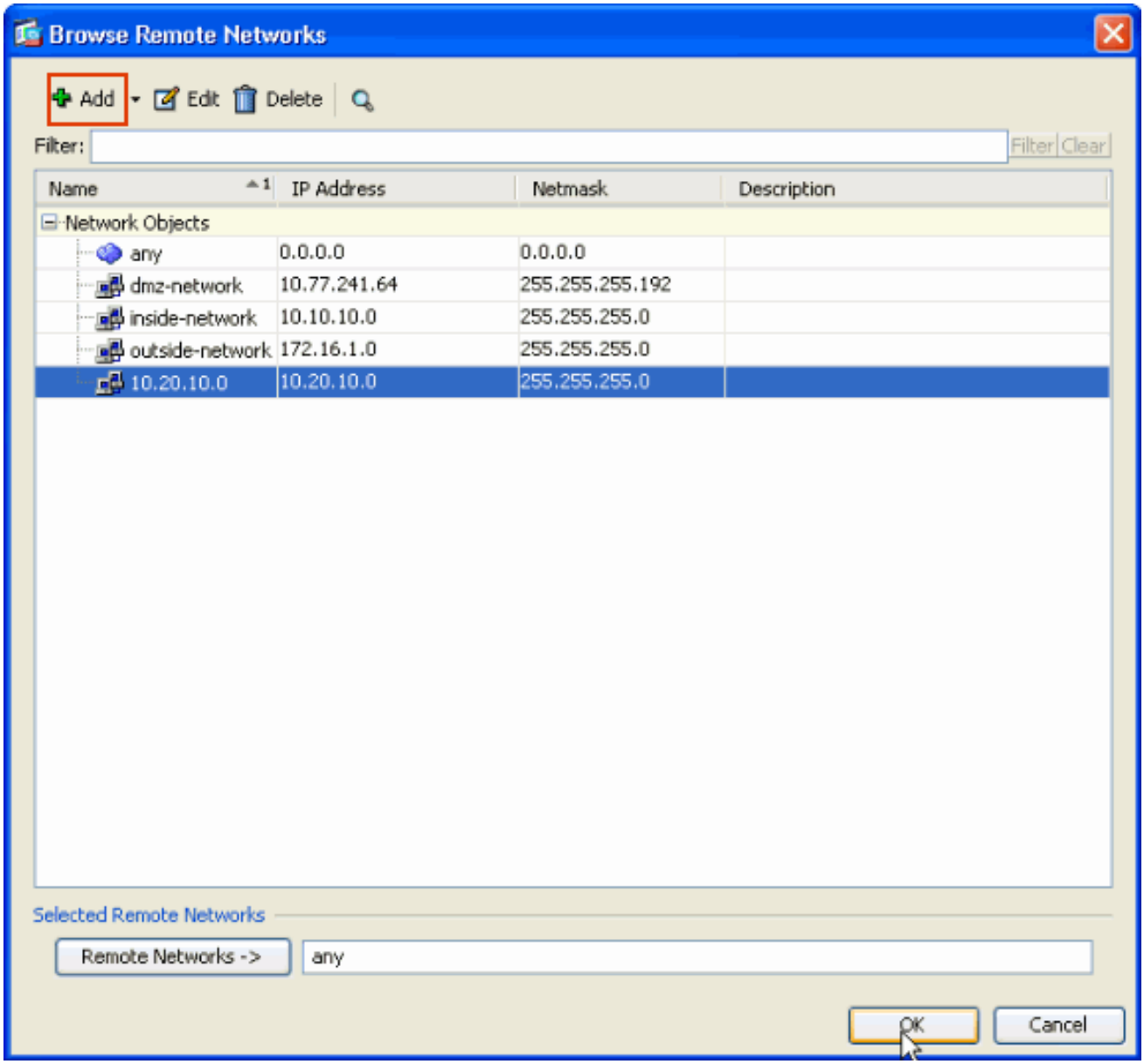
11. 选择 **Local Network** 地址，然后单击 OK，如下所示。



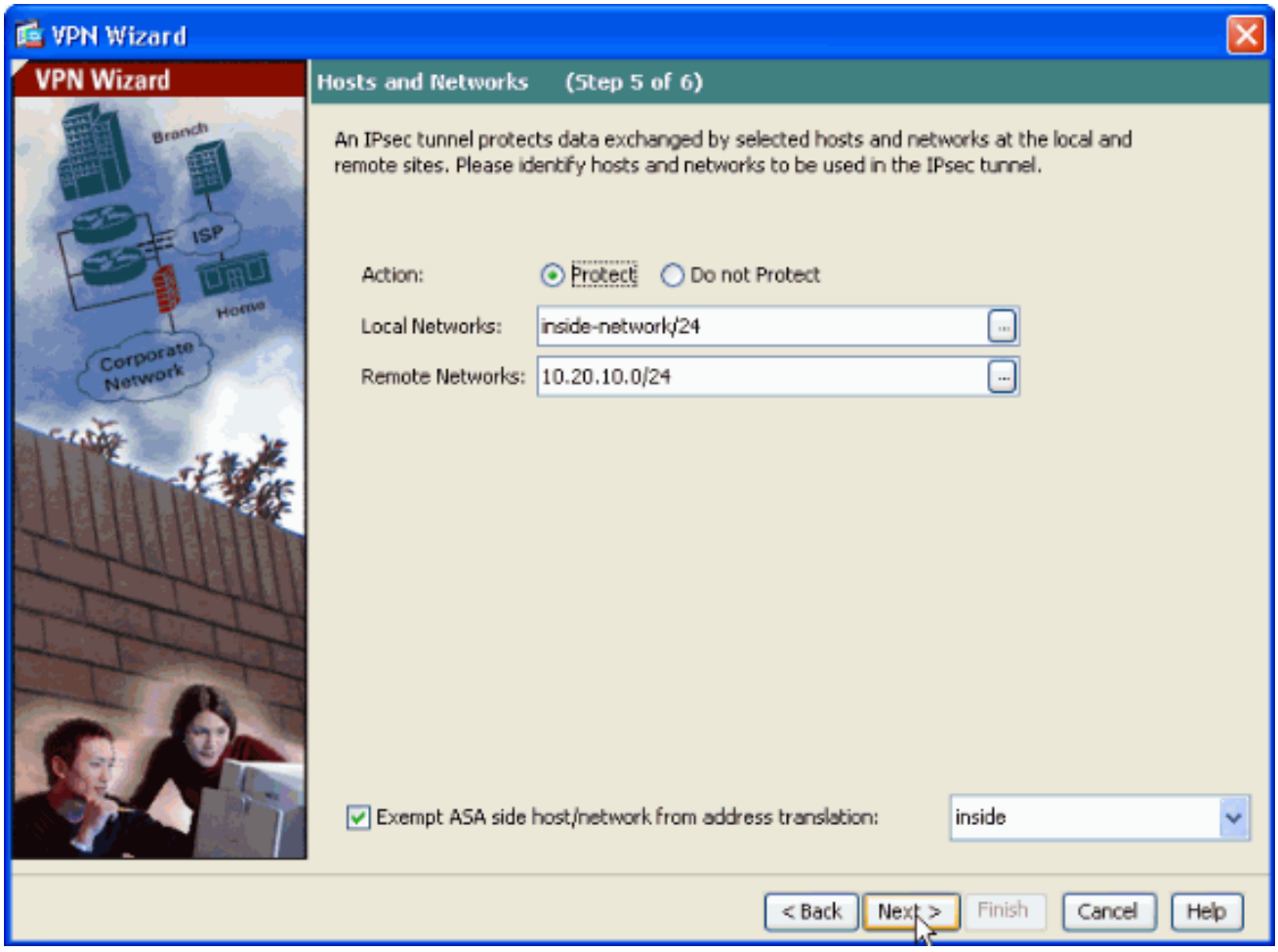
12. 单击 **Remote Networks** 旁边的按钮（如下所示），从下拉列表中选择远程网络地址。



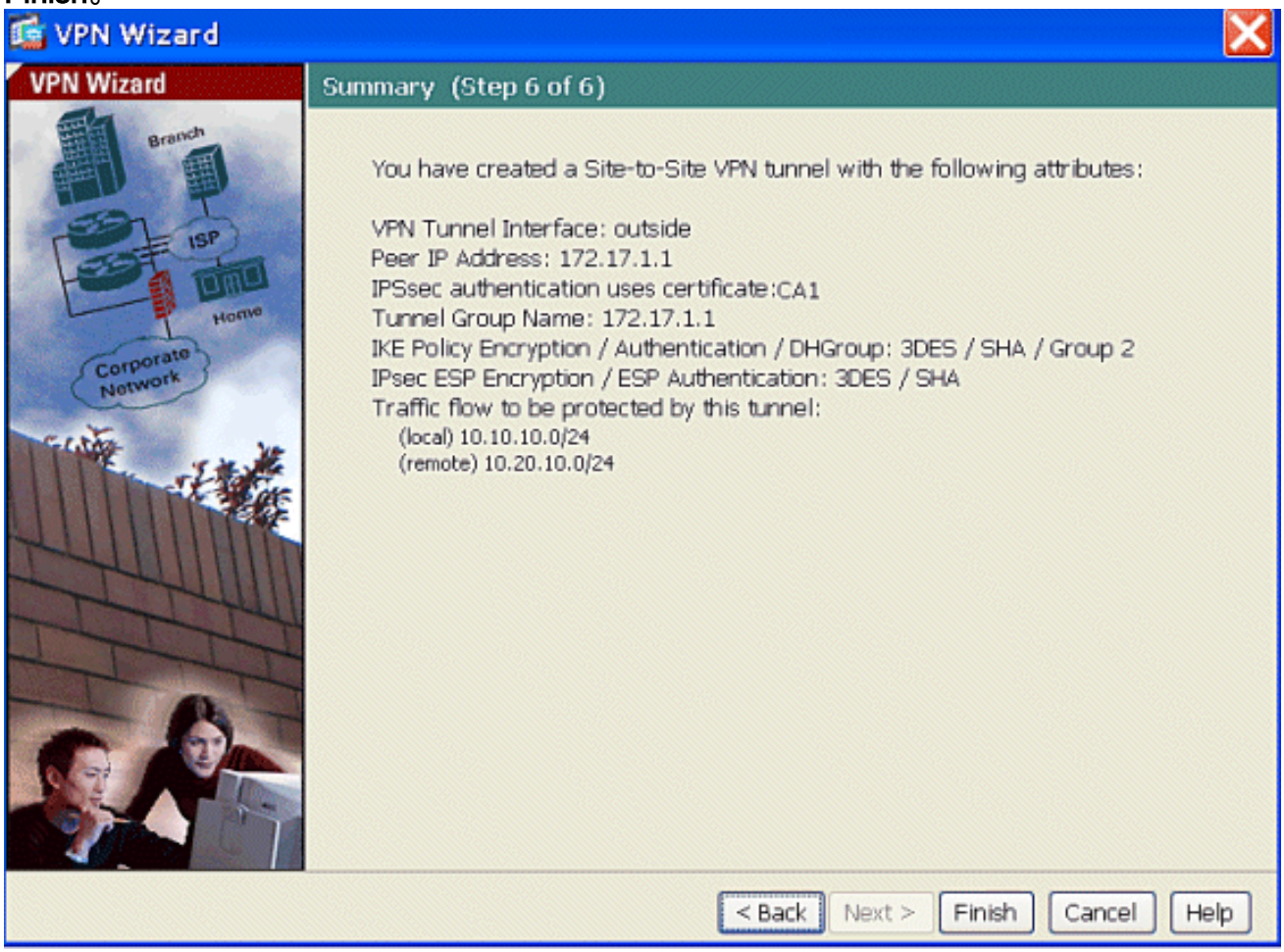
13. 选择 **Remote Network** 地址，然后单击 OK，如下所示。**注意：** 如果列表中没有“远程网络”，则必须将该网络添加到列表中；单击 **Add**。



14. 选中 **Exempt ASA side host/network from address translation** 复选框，以防止隧道数据流进行网络地址转换。单击 **Next**。



15. 此概要中显示了通过 VPN 向导定义的属性。再次检查配置，如果您确定设置正确，请单击 **Finish**。



ASA-1 配置概要

ASA-1

```
ASA-1#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ASA-1
domain-name cisco.comenable password 8Ry2YjIyt7RRXU24
encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0!
interface Ethernet0/2
 nameif DMZ
 security-level 50
 ip address 10.77.241.142 255.255.255.192
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
encryptedftp mode passive dns server-group DefaultDNS
domain-name cisco.com access-list inside_nat0_outbound
extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0
255.255.255.0 access-list outside_1_cryptomap extended
permit ip 10.2.2.0 255.255.255.0 10.5.5.0 255.255.255.0
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover asdm image disk0:/asdm-613.bin asdm history
enable arp timeout 14400 global (outside) 1 interface
nat (inside) 1 10.2.2.0 255.255.255.0 nat (inside) 0
access-list inside_nat0_outbound route outside 0.0.0.0
0.0.0.0 192.168.1.3 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media
0:02:00 timeout uauth 0:05:00 absolute http server
enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location
no snmp-server contact ! crypto ipsec transform-set ESP-
3DES-SHA esp-3des esp-sha-hmac crypto map outside_map 1
match address outside_1_cryptomap crypto map outside_map
1 set peer 172.17.1.1 crypto map outside_map 1 set
transform-set ESP-3DES-SHA crypto map outside_map
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 1ee59b00 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 1e170d30 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 1e1fb28c 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 b1e15148 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 a1e906ec
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 1e01d408 3f7f0595
8081f986 526fbe1c 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
10 authentication rsa-sig encryption 3des hash sha group
1 lifetime 86400 telnet timeout 5 ssh timeout 5 console
timeout 0 threat-detection basic-threat threat-detection
statistics access-list ! class-map inspection_default
match default-inspection-traffic ! !-- Output
suppressed! tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes trust-point CA1
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

ASA-2 配置

对 ASA-2 安全设备进行类似的配置。

验证

在 ASA 上，您可以在命令行中发出一些 show 命令以检验证书的状态。

使用本部分可确认配置能否正常运行。

- **show crypto ca trustpoint** 命令可显示已配置的信任点。`ASA-1#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** 命令可显示系统上安装的所有证书。`ASA-1# show crypto ca certificate`

```
Certificate
  Status: Available
  Certificate Serial Number: 3f14b70b00000000001f
  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 IST Apr 14 2009
    end   date: 14:00:36 IST Apr 15 2010
  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 IST Apr 14 2009
    end   date: 06:10:15 IST Apr 14 2014
  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** 命令可显示缓存的证书撤销列表 (CRL)。
- **show crypto key mypubkey rsa** 命令可显示所有生成的加密密钥对。`ASA-1# show crypto key mypubkey rsa`

```
Key pair was generated at: 01:43:45 IST Apr 14 2009
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 IST Apr 15 2009
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 IST Apr 16 2009
ASA-1#
```

- **show crypto isakmp sa** 命令可显示对等体上的所有当前 IKE SA。`ASA#`**`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 1 IKE Peer: 172.17.1.1 Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
```

- **show crypto ipsec sa** 命令可显示对等体上的所有当前 IPSec SA。`ASA#`**`show crypto ipsec sa`**

```
interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 192.168.1.1 local
ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0) current_peer: 172.17.1.1 #pkts encaps:
9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #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.: 192.168.1.1, remote crypto endpt.: 172.17.1.1 path mtu
1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp sas: spi:
0xB7C1948E (3082917006) transform: esp-3des esp-sha-hmac none in use settings ={L2L, Tunnel,
PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key
lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y outbound esp
sas: spi: 0x434C4A7F (1129073279) transform: esp-3des esp-sha-hmac none in use settings
={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing:
```

```
    remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y
```

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

本部分提供的信息可用于对配置进行故障排除。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 debug 命令的重要信息和 IP 安全故障排除 - 了解和使用 debug 命令。

- **debug crypto ipsec 7** - 显示第 2 阶段的 IPsec 协商。**debug crypto isakmp 7** - 显示第 1 阶段的 ISAKMP 协商。

有关站点到站点 VPN 故障排除的详细信息，请参阅最常见的 L2L 和远程访问 IPsec VPN 故障排除解决方案。

相关信息

- **Cisco 自适应安全设备支持页**
- **Cisco VPN 客户端支持页**
- **技术支持和文档 - Cisco Systems**