使用数字证书与Microsoft CA的ASA/PIX 7.x和VPN客户端IPSec认证配置示例

目录

简介

本文档介绍如何在 Cisco 安全设备 (ASA/PIX) 7.x 和 VPN Client 上手动安装第三方供应商数字证书，以利用 Microsoft 证书机构 (CA) 服务器验证 IPSec 对等体。

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 供应商包括 Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA 和 Verisign。

注意： 本文档使用 Windows 2003 服务器作为 CA 服务器方案。

注意： 本文档假设 ASA/PIX 中事先不存在 VPN 配置。

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 7.2(2) 和 ASDM 版本 5.2(2) 的 ASA 5510。
- 运行软件版本 4.x 及更高版本的 VPN Client。

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 7.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 配置
- ASA 配置概要
- VPN 客户端配置

ASA 配置

执行以下步骤以便在 ASA 上安装第三方供应商数字证书：

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. 配置远程访问 VPN (IPSec) 使用新安装的证书

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 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** 16:25:49.580 IST Fri Dec 28 2007

步骤 2. 生成 RSA 密钥对

生成的 RSA 公钥将与 ASA 的身份信息一起形成 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。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Certificate**，然后选择 Key Pair。
3. 单击 **Add**。
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 **Generate Now**。您创建的密钥对应在 Key Pair Name 列中列出。

命令行示例

Ciscoasa
CiscoASA#**configure terminal** CiscoASA(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... ciscoasa(config)#

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。

ASDM 步骤

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。
4. 配置以下值：**Trustpoint Name**:信任点名称应与目标用途相关。（本示例使用 *CA1*。）**Key pair**:选择在第 2 步中生成的密钥对 (my.CA.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**。
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。
10. 单击 **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。

命令行示例

Ciscoasa

```
CiscoASA(config)#crypto ca trustpoint CA1 !--- Creates
the trustpoint. CiscoASA(config-ca-
trustpoint)#enrollment terminal !--- Specifies cut and
paste enrollment with this trustpoint. CiscoASA(config-
ca-trustpoint)#subject-name
CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh !--- Defines
x.500 distinguished name. CiscoASA(config-ca-
trustpoint)#keypair my.CA.key !--- Specifies key pair
generated in Step 2. CiscoASA(config-ca-trustpoint)#fqdn
CiscoASA.cisco.com !--- Specifies subject alternative
name (DNS:). CiscoASA(config-ca-trustpoint)#exit
```

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。
3. 确认选择了在第 3 步中创建的信任点，然后单击 **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）。
4. 将 PKCS#10 注册请求复制到文本文件，然后将保存的 CSR 提交到第三方供应商（例如 Microsoft CA），如以下步骤所示：使用为 vpn 服务器提供的用户凭证登录到 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** 文本字段中，然后单击 Submit。单击 **Base 64 encoded** 单选按钮，然后单击 Download certificate。出现 File Download 对话框时，请使用文件名 **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

Ciscoasa

```
CiscoASA(config)#crypto ca enroll CA1 !--- 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=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]: 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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: 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。

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 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：** 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. 单击位于所发放的身份证书上方的 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。要从名为 *CA1* 的 CA 服务器中下载 CA 证书，请执行以下步骤：使用为 vpn 服务器提供的用户凭证登录到 CA 服务器 172.16.5.1。单击 **Download a CA certificate, certificate chain or CRL**，然后选择 Base 64 单选按钮以指定编码方法。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 Properties。
13. 展开 **Certificate**，然后选择 Authentication。
14. 单击 **Enter the certificate text in hexadecimal or base64 format** 单选按钮。
15. 将 base64 格式的 CA 证书从文本编辑器中粘贴到文本区域。
16. 单击 **Authenticate**。
17. 单击 **Ok**。

命令行示例

Ciscoasa

```
CiscoASA(config)#crypto ca authenticate CA1 !---
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
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 CiscoASA(config)#
```

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。
4. 单击 **Import**，然后单击 OK。

命令行示例

Ciscoasa

```
CiscoASA(config)#crypto ca import CA1 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:
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 3rd 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
CiscoASA(config)#
```

步骤 7. 配置远程访问 VPN (IPSec) 使用新安装的证书

ASDM 步骤

执行下列步骤以配置远程访问 VPN：

1. 选择 **Configuration > VPN > IKE > Policies > Add** 以创建 ISAKMP 策略 65535，如下图所示。
2. 单击 **OK**，然后单击 Apply。
3. 选择 **Configuration > VPN > IPSec > Transform Sets >Add** 以创建转换集 (*myset*)，如下图所示：
4. 单击 **OK**，然后单击 Apply
5. 选择 **Configuration > VPN > IPSec > IPSec Rules >Add** 以使用优先级为 10 的动态策略创建加密映射，如下图所示：
6. 单击 **OK**，然后单击 Apply
7. 选择 **Configuration > VPN > General > Group Policy > Add Internal Group Policy** 以创建 Defaultgroup 组策略，如下图所示。

8. 单击 **OK**，然后单击 Apply
9. 选择 **Configuration > VPN > IP Address Management > IP Pools > Add** 以便为要动态指定的 VPN Client 用户配置地址池 vpnpool。
10. 单击 **OK**，然后单击 Apply
11. 选择 **Configuration > VPN > General > Users > Add** 以便为 VPN Client 访问创建用户帐户 vpnuser。
12. 将此用户添加到 **DefaultRAGroup**。
13. 单击 **OK**，然后单击 Apply
14. 根据以下步骤说明编辑 DefaultRAGroup：选择 **Configuration > VPN > General > Tunnel Group > Edit**。从 Group Policy 下拉列表中选择 **Defaultgroup**。从 Authentication Server Group 下拉列表中选择 **LOCAL**。从 Client Address Assignment 下拉列表中选择 **vpnpool**。
15. 单击 **OK**，然后单击 Apply

命令行示例

Ciscoasa

```
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5 CiscoASA(config-
isakmp-policy)#group 2 CiscoASA(config-isakmp-
policy)#lifetime 86400 CiscoASA(config-isakmp-
policy)#exit CiscoASA(config)#crypto isakmp identity
auto !--- Phase 1 Configurations CiscoASA(config)#crypto
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map outside_dyn_map 10
set transform-set myset CiscoASA(config)#crypto map
outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
CiscoASA(config)#crypto map outside_map interface
outside !--- Phase 2 Configurations
CiscoASA(config)#group-policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value
cisco.com CiscoASA(config-group-policy)#exit !--- Create
a group policy "Defaultgroup" with domain name !---
cisco.com CiscoASA(config)#username vpnuser password
password123 CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#group-lock value
DefaultRAGroup CiscoASA(config-username)#exit !---
Create an user account "vpnuser" and added to
"DefaultRAGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes !--- The Security
Appliance provides the default tunnel groups !--- for
remote access (DefaultRAGroup). CiscoASA(config-tunnel-
general)#address-pool vpnpool !--- Associate the vpnpool
to the tunnel group using the address pool.
CiscoASA(config-tunnel-general)#default-group-policy
Defaultgroup !--- Associate the group policy
"Defaultgroup" to the tunnel group. CiscoASA(config-
tunnel-general)#exit CiscoASA(config)#tunnel-group
DefaultRAGroup ipsec-attributes CiscoASA(config-tunnel-
ipsec)#trust-point CA1 CiscoASA(config-tunnel-
ipsec)#exit !--- Associate the trustpoint CA1 for IPSec
peer authentication
```

ASA 配置概要

Ciscoasa

```
CiscoASA#show running-config : Saved : ASA Version
7.2(2) ! hostname CiscoASA domain-name cisco.com enable
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
shutdown nameif inside security-level 100 ip address
10.2.2.1 255.255.255.0 ! interface Ethernet0/2 nameif
DMZ security-level 90 ip address 10.77.241.142
255.255.255.192 ! interface Ethernet0/3 shutdown no
nameif no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa722-k8.bin ftp mode passive dns server-group
DefaultDNS domain-name cisco.com access-list 100
extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 mtu DMZ 1500 ip local pool vpnpool 10.5.5.10-
10.5.5.20 mask 255.255.255.0 no failover icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-522.bin no asdm history enable arp timeout
14400 nat (inside) 0 access-list 100 route outside
10.1.1.0 255.255.255.0 192.168.1.1 1 route outside
172.16.5.0 255.255.255.0 192.168.1.1 1 route DMZ 0.0.0.0
0.0.0.0 10.77.241.129 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 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout uauth 0:05:00 absolute group-policy
Defaultgroup internal group-policy Defaultgroup
attributes default-domain value cisco.com username
vpnuser password TXttW.eFqbHusJQM encrypted username
vpnuser attributes group-lock value DefaultRAGroup http
server enable http 0.0.0.0 0.0.0.0 outside http 0.0.0.0
0.0.0.0 DMZ no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart crypto ipsec transform-set
myset esp-3des esp-md5-hmac crypto dynamic-map
outside_dyn_map 10 set transform-set myset crypto map
outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
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=Raleigh keypair my.CA.key crl
configure crypto ca certificate chain CA1 certificate
3f14b70b00000000001f 308205eb 308204d3 a0030201 02020a3f
14b70b00 00000000 1f300d06 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 37313232 37313430
3033365a 170d3038 31323236 31343030 33365a30 67311330
11060a09 92268993 f22c6401 19160363 6f6d3115 3013060a
09922689 93f22c64 01191605 63697363 6f311530 13060a09
92268993 f22c6401 19160554 53576562 310e300c 06035504
03130555 73657273 31123010 06035504 03130976 706e7365
72766572 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 0001a382
03313082 032d300b 0603551d 0f040403 02052030 34060355
1d11042d 302ba029 060a2b06 01040182 37140203 a01b0c19
76706e73 65727665 72405453 5765622e 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 74301506 092b0601
04018237 14020408 1e060045 00460053 300c0603 551d1301
01ff0402 30003015 0603551d 25040e30 0c060a2b 06010401
82370a03 04304406 092a8648 86f70d01 090f0437 3035300e
06082a86 4886f70d 03020202 0080300e 06082a86 4886f70d
03040202 00803007 06052b0e 03020730 0a06082a 864886f7
0d030730 0d06092a 864886f7 0d010105 05000382 010100bf
99b9daf2 e24f1bd6 ce8271eb 908fadb3 772df610 0e78b198
f945f379 5d23a120 7c38ae5d 8f91b3ff 3da5d139 46d8fb6e
20d9a704 b6aa4113 24605ea9 4882d441 09f128ab 4c51a427
fa101189 b6533eef adc28e73 fcfed3f1 f4e64981 0976b8a1
2355c358 a22af8bb e5194b42 69a7c2f6 c5a116f6 d9d77fb3
a7f3d201 e3cff8f7 48f8d54e 243d2530 31a733af 0e1351d3
9c64a0f7 4975fc66 a017627c cfd0ea22 2992f463 9412b388
84bf8b33 bd9f589a e7087262 a4472e69 775ab608 e5714857
4f887163 705220e3 aca870be b107ab8d 73faf76d b3550553
1a2b873f 156f9dff 5386c839 1380fda8 945a7f6c c2e9d5c8
83e2e761 394dd4da 63eaefc6 a44df5 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
65535 authentication rsa-sig encryption 3des hash md5
group 2 lifetime 86400 crypto isakmp identity auto
tunnel-group DefaultRAGroup general-attributes address-
pool vpnpool default-group-policy Defaultgroup tunnel-
group DefaultRAGroup ipsec-attributes trust-point CA1
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0 : end
CiscoASA#
```

VPN 客户端配置

执行以下步骤以配置 VPN Client：

1. 选择 **Start > Programs > Cisco Systems VPN Client > VPN Client** 以启动 VPN Client 软件。
2. 执行以下步骤，以便从名为 **CA1** 的 CA 服务器中下载 CA 证书，然后将其安装到 Cisco VPN Client 中：使用为 vpnuser 提供的用户凭证登录到 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 VPN Client 用户帐户。单击 **Download a CA certificate, certificate**

chain or CRL，然后选择 Base 64 单选按钮以指定编码方法。单击 **Download CA certificate**。使用文件名 **certnew.cer** 将 CA 证书保存到计算机中。默认情况下，文件将保存到 C:\Program Files\Cisco Systems\VPN Client。在 VPN Client 软件中，单击 **Certificates Tab**，然后选择 Import。单击 **Import from File** 单选按钮，然后单击 Browse 以便从存储位置 C:\Program Files\Cisco Systems\VPN Client 中导入 CA 证书。单击 **Import**。将会出现一个提示导入成功的对话框。在 Certificates 选项卡中将会出现 CA 证书 CA1。**注意：** 请确保选中 **Show CA/RA Certificates** 选项；否则，CA 证书将不会出现在证书窗口中。

3. 执行以下步骤以下载身份证书，并将其安装到 VPN Client 中：在 CA 服务器 CA1 中，选择 **Request a Certificate > advanced certificate request > Create and submit a request to this CA** 以注册身份证书。单击 **submit**。单击 **Yes** 以继续执行。单击 **Install this certificate**。单击 **Yes** 以继续执行。您必须收到证书已安装的消息，如下图所示：退出然后重新启动 VPN Client，以使已安装的身份证书出现在 VPN Client 的 Certificates 选项卡中，如下图所示：
4. 执行以下步骤以创建连接项 (*vpnuser*)：单击 Connection Entries 选项卡，然后单击 **New**。在 Host 字段中输入远程对等体 IP 地址（可路由）。选择 **Certificate Authentication** 单选按钮，然后从下拉列表中选择身份证书。单击 **Save**。
5. 单击 **Connect**。
6. 出现提示时，输入 xauth 的用户名和口令信息，然后单击 **OK** 以连接远程网络。
7. VPN Client 即会连接 ASA，如下图所示。

验证

在 ASA 上，您可以在命令行中使用一些 show 命令以验证证书的状态。

使用本部分可确认配置能否正常运行。

- **show crypto ca trustpoint** — 显示已配置的信任点。`CiscoASA#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** — 显示系统上安装的所有证书。`CiscoASA#show crypto ca certificates 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=Configuratio n,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 UTC Dec 27 2007 end date: 14:00:36 UTC Dec 26 2008 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=Configuratio n,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 UTC Dec 14 2007 end date: 06:10:15 UTC Dec 14 2012 Associated Trustpoints: CA1`
- **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。`CiscoASA#show crypto key mypubkey rsa Key pair was generated at: 01:43:45 UTC Dec 11 2007 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 UTC Dec 15 2007 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 UTC Dec 21 2007
CiscoASA#
```

- **show crypto isakmp sa** — 显示 IKE 1 隧道信息。`CiscoASA#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: 10.1.1.5 Type : user Role : responder Rekey : no State : MM_ACTIVE`
- **show crypto ipsec sa** — 显示 IPSec 隧道信息。`CiscoASA#show crypto ipsec sa interface: outside Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0) current_peer: 10.1.1.5, username: vpnuser dynamic allocated peer ip: 10.5.5.10 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 #pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #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.: 192.168.1.5, remote crypto endpt.: 10.1.1.5 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: FF3EEE7D inbound esp sas: spi: 0xEFDF8BA9 (4024404905) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 4096, crypto-map: dynmap sa timing: remaining key lifetime (sec): 28314 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xFF3EEE7D (4282314365) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 4096, crypto-map: dynmap sa timing: remaining key lifetime (sec): 28314 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。

以下是您可能会遇到的一些可能的错误：

- **ERROR: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。如果所列出的信任点是错误的，请使用本文档中介绍的步骤删除信任点，然后重新安装正确的信任点。同时，请验证在生成 CSR 之后密钥对是否未更改。
- **ERROR:ASA/PIX.Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:**如果在验证证书时出现问题，您可能会在 VPN Client 中收到此错误。要解决此问题，请在 ASA/PIX 配置中使用 **crypto isakmp identity auto** 命令。

相关信息

- Cisco 自适应安全设备支持页
- Cisco VPN 客户端支持页
- Cisco PIX 500 系列安全设备

- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems