ASA/PIX 7.x and VPN クライアント Microsoft CA によるデジタル証明書を使用した IPSec 認証の設定例

目次

概要

このドキュメントでは、Cisco セキュリティ アプライアンス（ASA/PIX）7.x および VPN Client にサード パーティ ベンダーのデジタル証明書を手動でインストールして、Microsoft の認証局（CA）サーバで IPSec ピアの認証を行う方法について説明します。

前提条件

要件

このドキュメントでは、証明書を登録するために Certificate Authority（CA; 認証局）にアクセスする必要があります。 サポートされるサードパーティ CA ベンダーは、Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA、および VeriSign です。

注: このドキュメントは、シナリオに CA サーバとして Windows 2003 Server を使用しています。

注: このドキュメントは、ASA/PIX に既存の VPN 設定がないことを前提としています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 7.2(2) および ASDM バージョン 5.2(2) が稼働する ASA 5510
- ソフトウェア バージョン 4.x 以降が稼働する VPN Client

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

ASA の設定は、ソフトウェア バージョン 7.x が稼働する Cisco 500 シリーズ PIX にも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

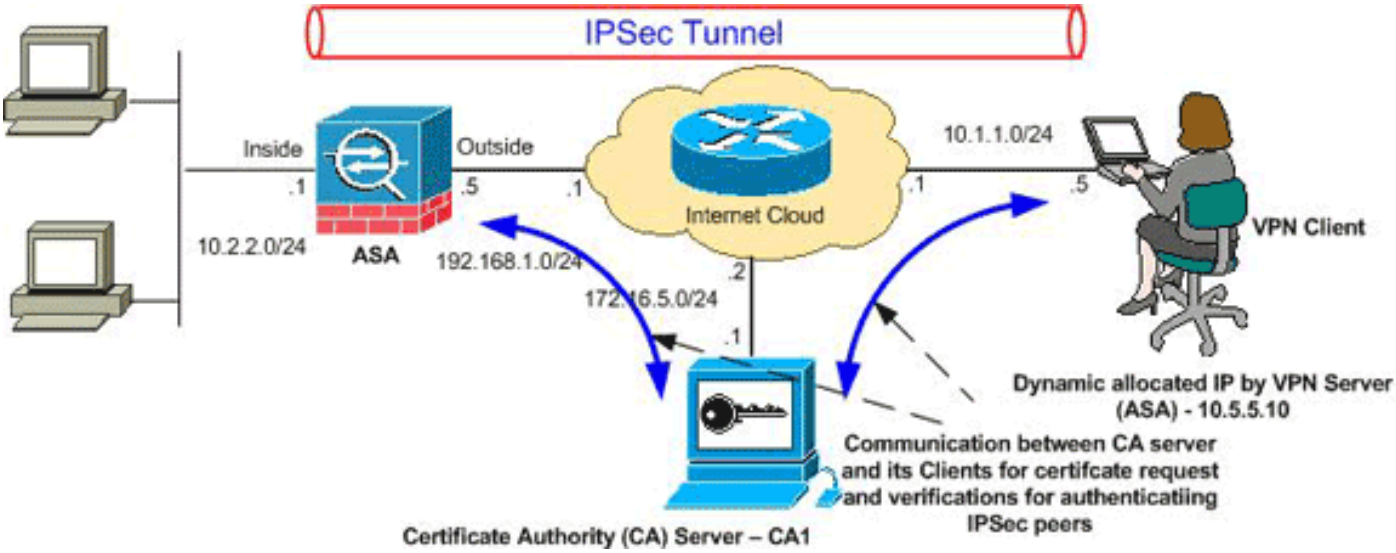
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

設定

このドキュメントでは、次の設定を使用します。

- ASA の設定
- ASA の設定の概要
- VPN Client の設定

ASA の設定

ASA にサードパーティ ベンダーのデジタル証明書をインストールするには、次の手順を実行します。

ステップ 1：日付、時刻、および時間帯（Time Zone）の値が正しいことを確認する

ステップ 2. RSA キー ペアを生成する

ステップ 3. トラストポイントを作成する

ステップ 4. 証明書登録を生成する

ステップ 5. トラストポイントを認証する

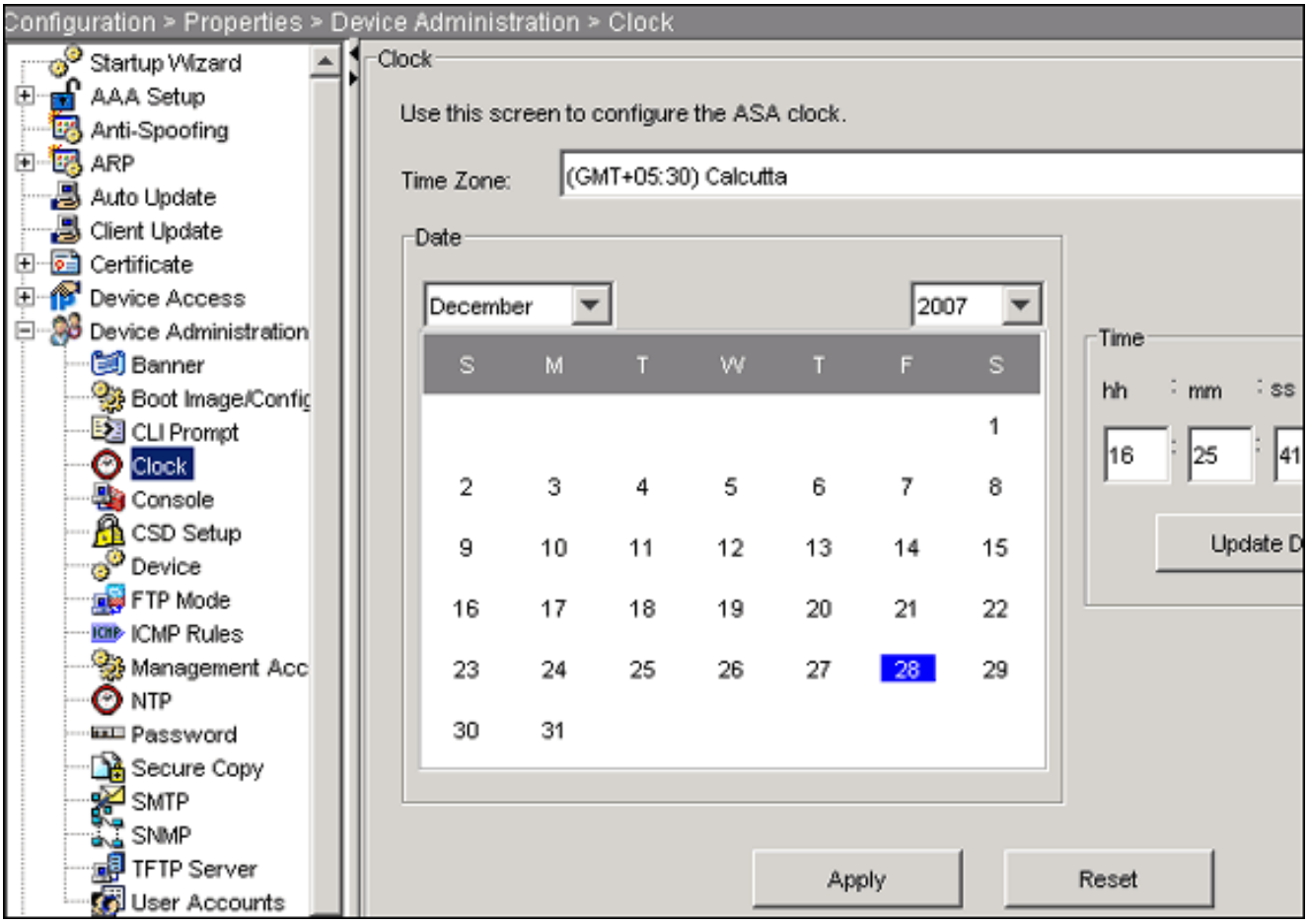
ステップ 6. 証明書をインストールする

ステップ 7. 新しくインストールした証明書を使用するようにリモート アクセス VPN（IPSec）を設定する

ステップ 1：日付、時刻、および時間帯（Time Zone）の値が正しいことを確認する

ASDM の手順

1. [Configuration]、[Properties] の順にクリックします。
2. [Device Administration] を展開し、[Clock] を選択します。
3. 表示されている情報が正しいことを確認します。証明書の検証が適切に行われるために、Date、Time、および Time Zone の値は正確である必要があります。



コマンドラインの例

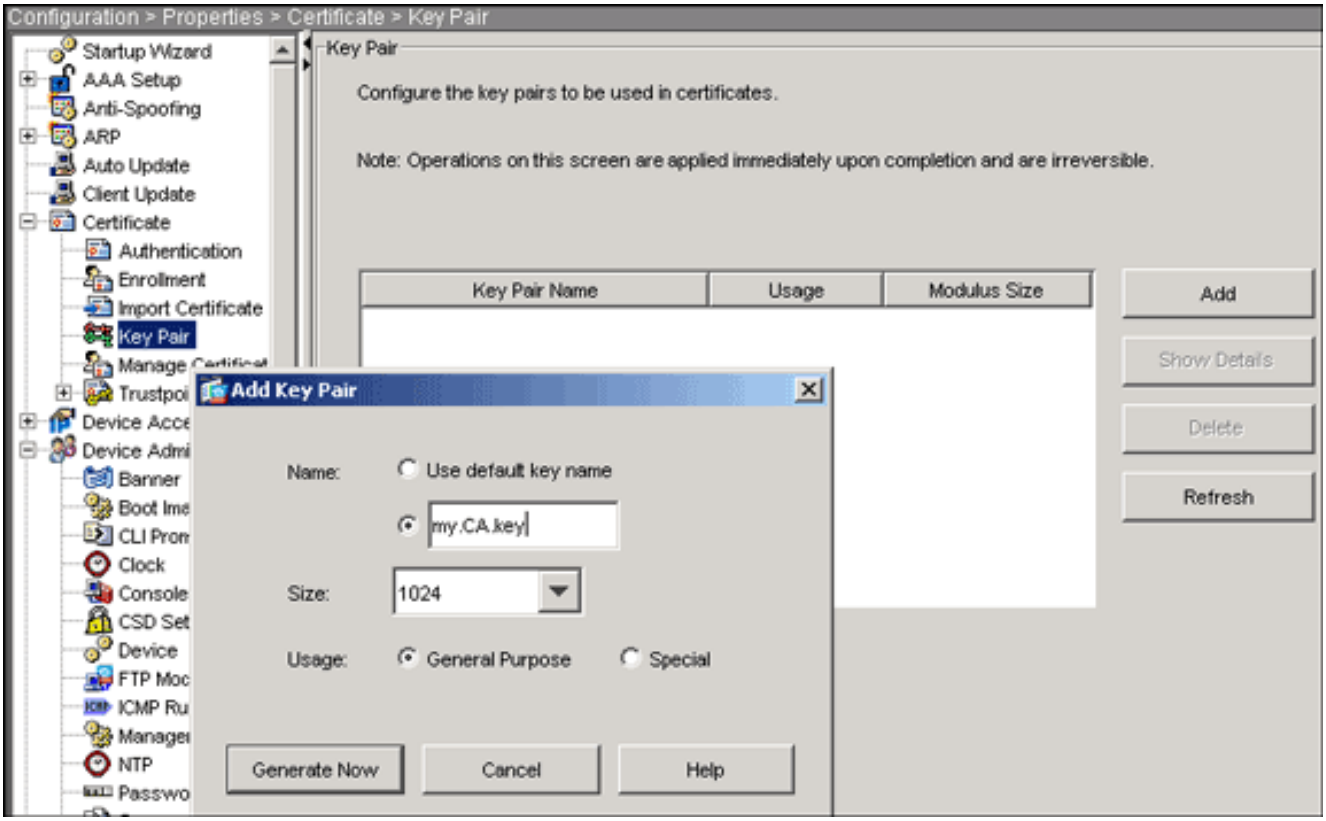
CiscoASA
CiscoASA#**show clock** 16:25:49.580 IST Fri Dec 28 2007

ステップ 2. RSA キー ペアを生成する

生成された RSA 公開キーは、ASA からの ID 情報と結合され、PKCS#10 証明書要求が形成されます。 キー ペアを作成するトラストポイントでキー名を明確に特定する必要があります。

ASDM の手順

1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Key Pair] を選択します。
3. [Add] をクリックします。



4. キー名を入力し、モジュール サイズを選択し、使用タイプを選択します。**注:** 推奨されるキー ペアのサイズは 1024 です。
5. [Generate Now] をクリックします。作成したキー ペアが [Key Pair Name] 列に表示されます。

コマンドラインの例

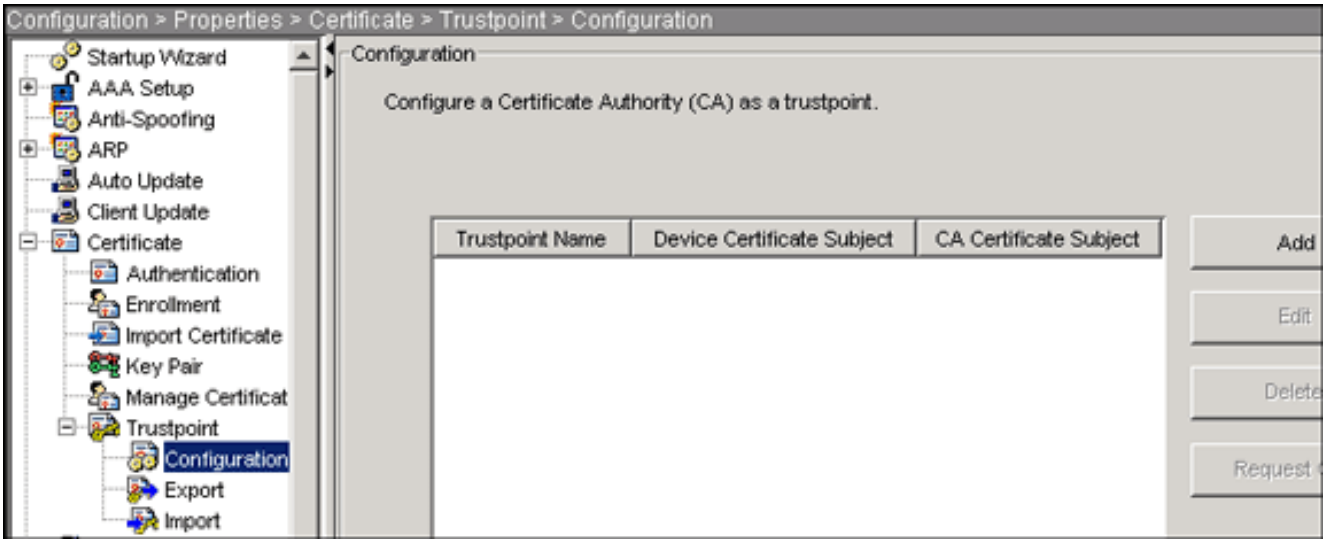
CiscoASA
CiscoASA#**configure terminal** CiscoASA(config)#**crypto key generate rsa label my.CA.key modulus 1024** *!--- Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.CA.key Keypair generation process begin. Please wait... ciscoasa(config)#

ステップ 3. トラストポイントを作成する

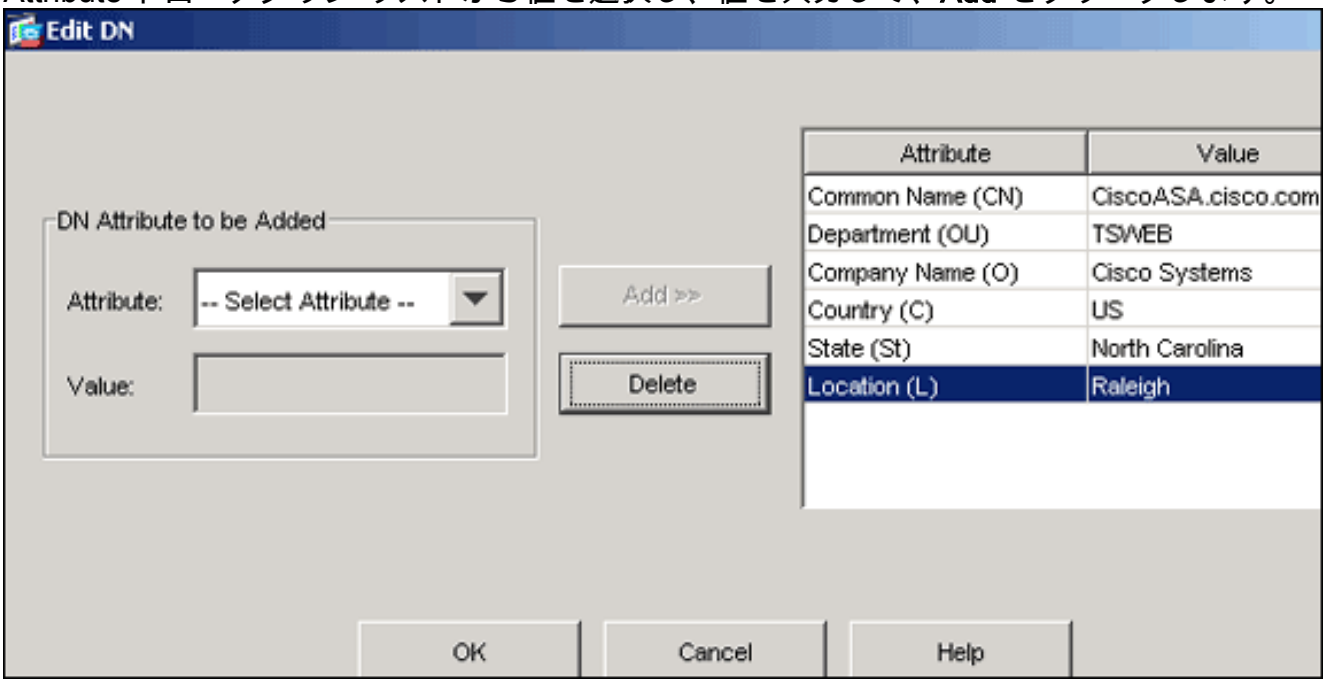
トラストポイントは、ASA が使用する認証局（CA）を宣言する必要があります。

ASDM の手順

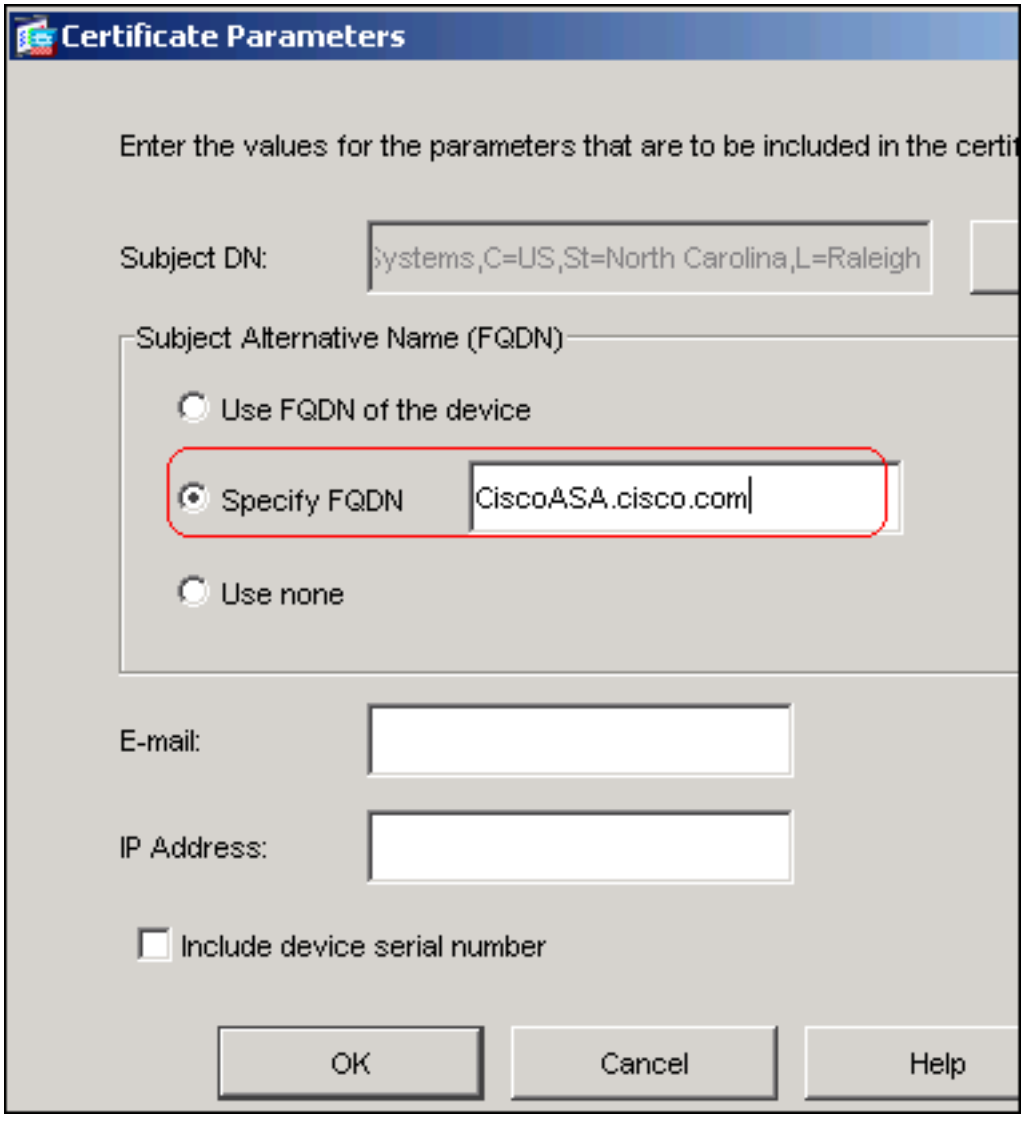
1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Trustpoint] を展開します。
3. [Configuration] を選択し、[Add] をクリックします。



4. 以下の値を設定します。**トラストポイント名**： トラストポイント名は目的の用途に関連する名前にします（この例では *CA1*）。**キー ペア**： ステップ 2. で生成したキー ペア（my.CA.key）を選択します。
5. [Manual Enrollment] を選択していることを確認します。
6. [Certificate Parameters] をクリックします。[Certificate Parameters] ダイアログ ボックスが表示されます。
7. [Edit] をクリックし、次の表に示す属性を設定します。これらの値を設定するために、Attribute ドロップダウン リストから値を選択し、値を入力して、**Add** をクリックします。

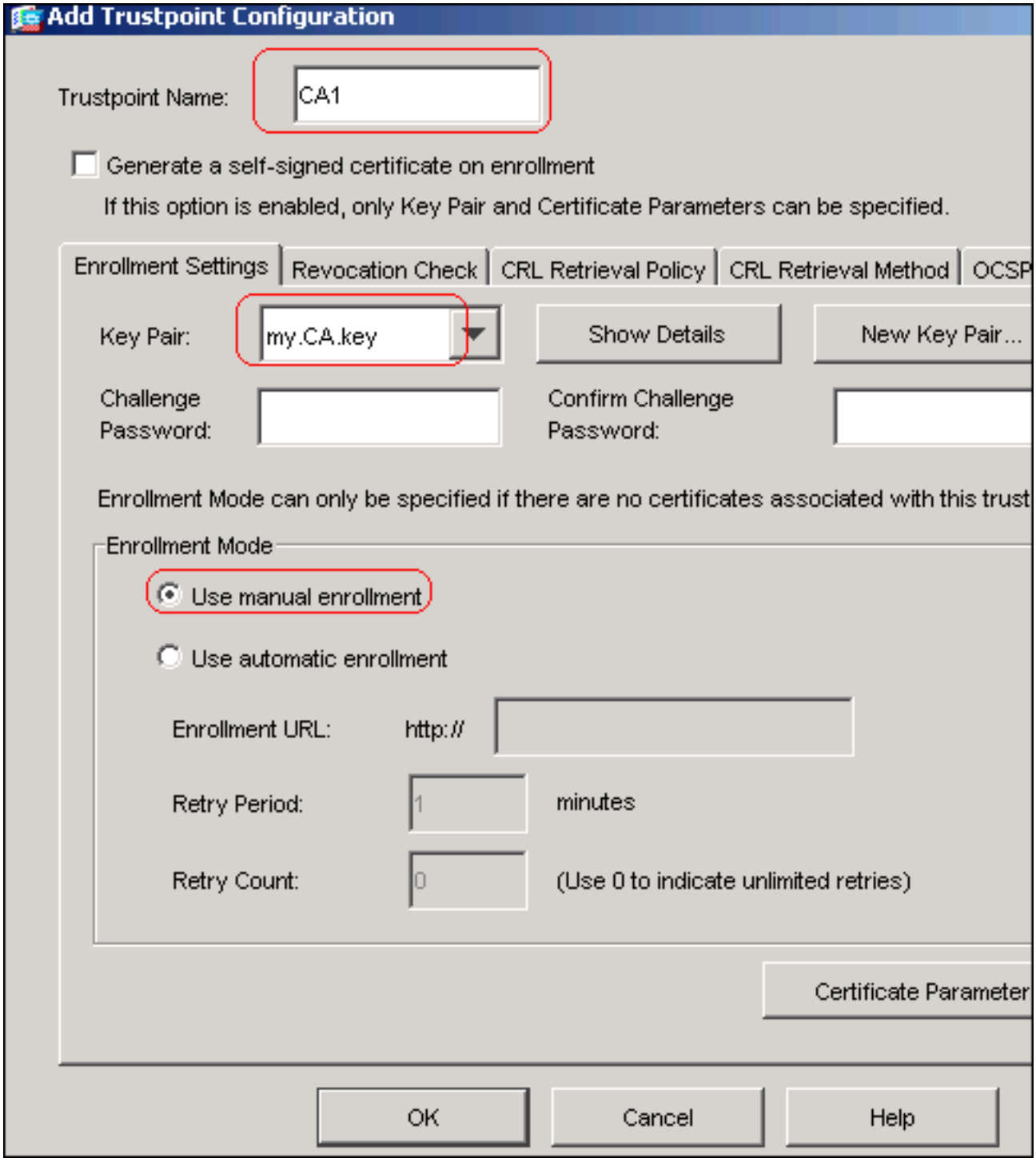


8. 適切な値を追加したら、**OK** をクリックします。
9. [Certificate Parameters] ダイアログボックスで、[Specify FQDN] フィールドに FQDN を入力します。この値は、Common Name（CN）に使用したものと同じ FQDN である必要があ



ります。

10. [OK] をクリックします。
11. 正しいキー ペアが選択されていることを確認し、[Use manual enrollment] オプション ボタンをクリックします。
12. [OK] をクリックして、[Apply] をクリックします。



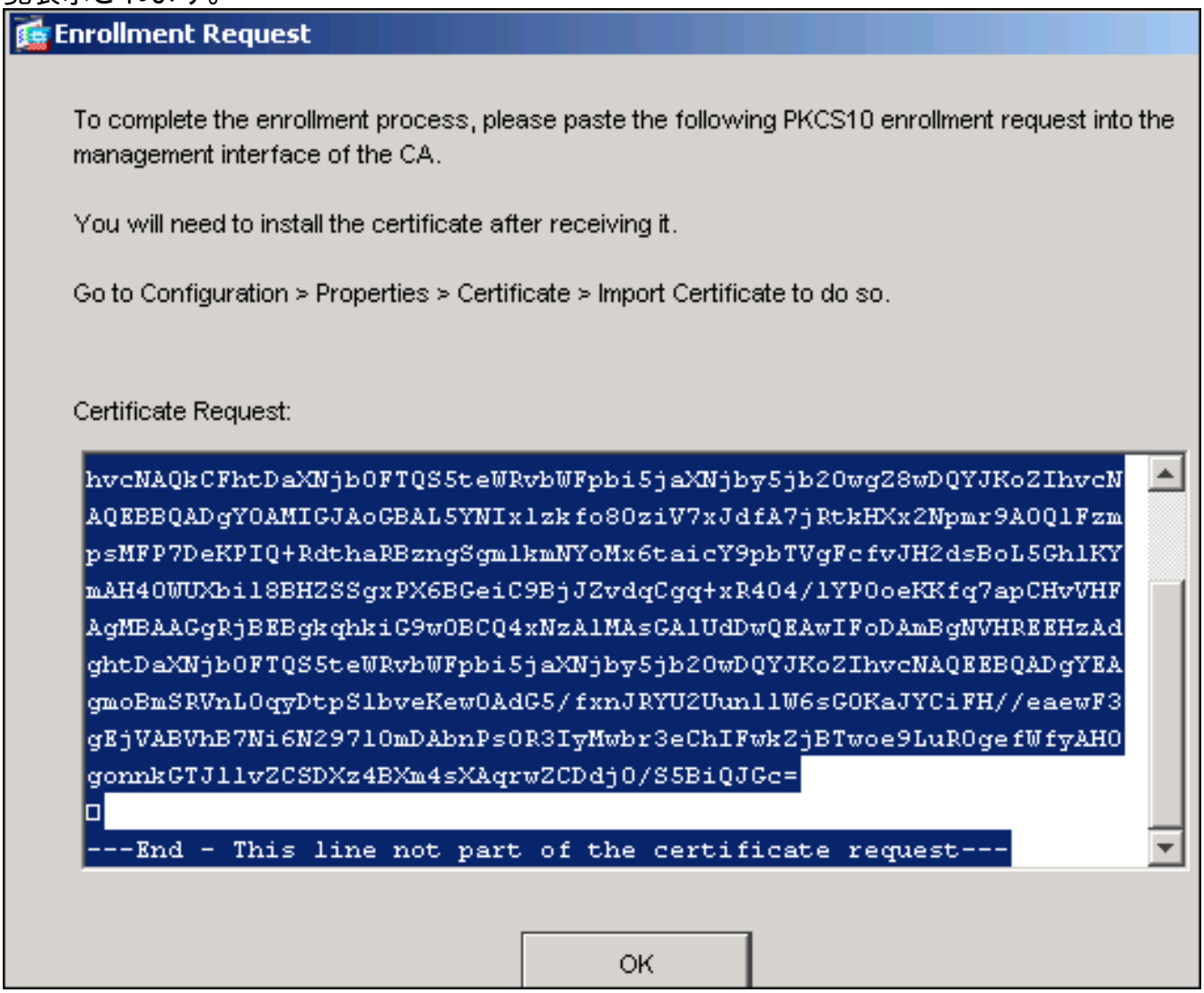
コマンドラインの例

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**

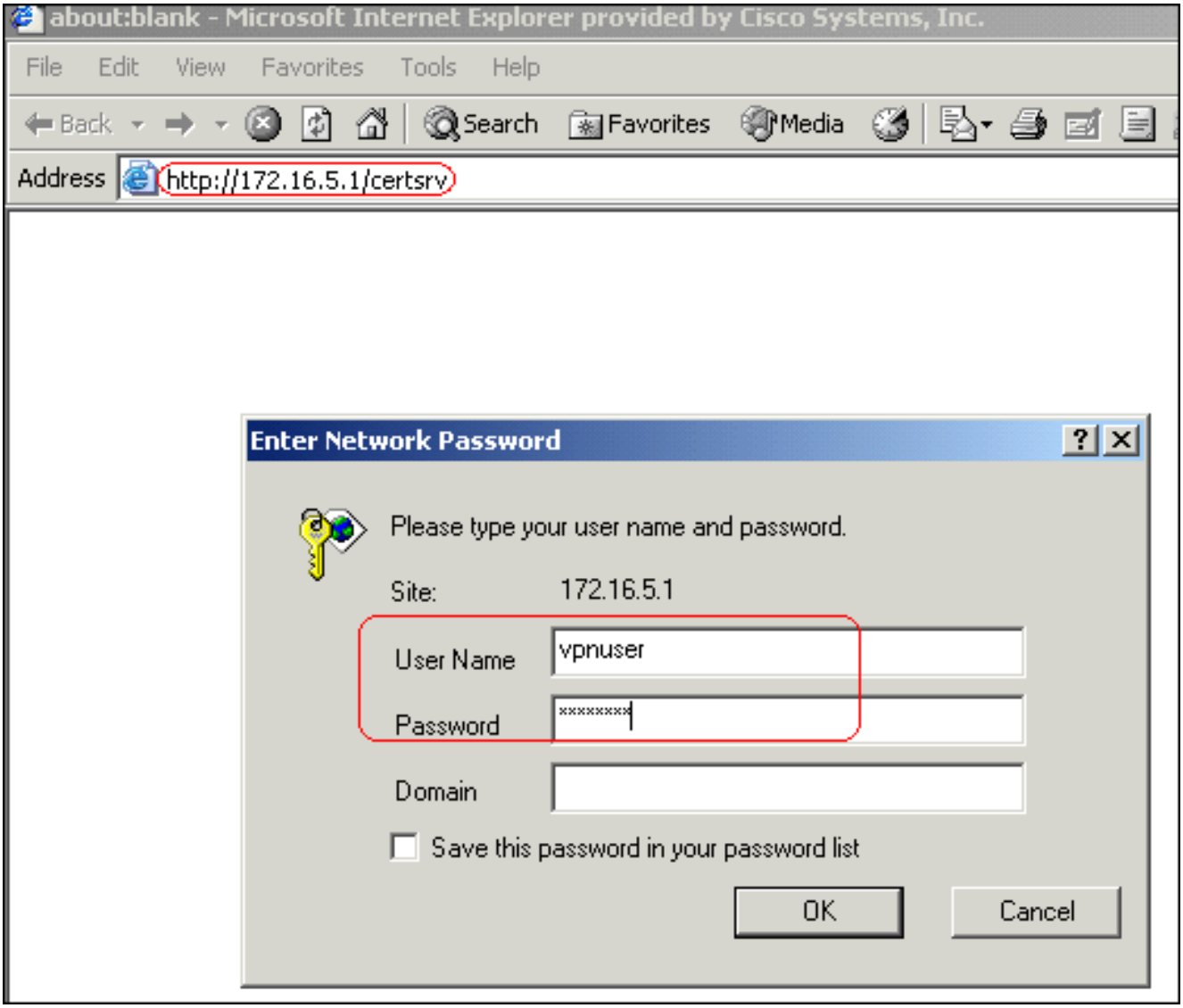
ステップ 4. 証明書登録を生成する

ASDM の手順

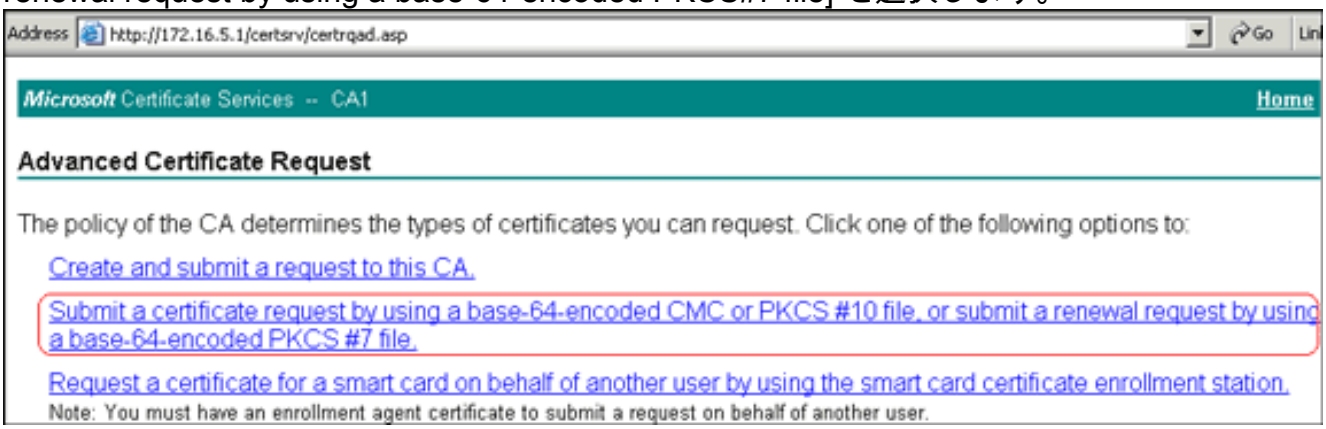
1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Enrollment] を選択します。
3. ステップ 3 で作成したトラストポイントが選択されていることを確認して、[Enroll] をクリックします。ダイアログ ボックスに証明書登録要求（証明書署名要求とも呼ばれる）が一覧表示されます。



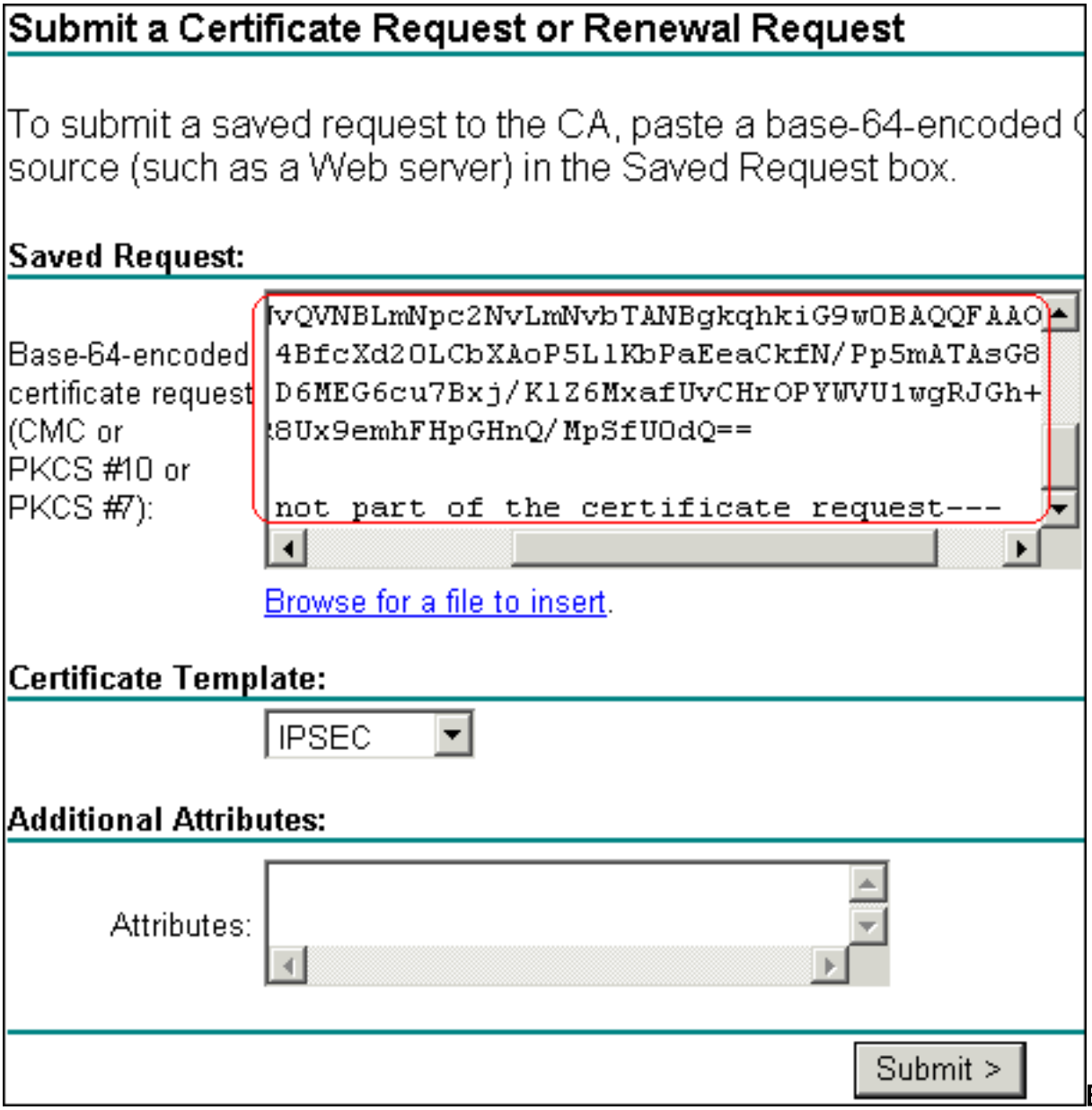
4. 次の手順に示すように、PKCS#10 登録要求をテキスト ファイルにコピーし、保存した CSR をサードパーティ ベンダー（Microsoft CA など）に送信します。VPN サーバに提供されたユーザ クレデンシャルを使用して、CA サーバ 172.16.5.1 にログインします。



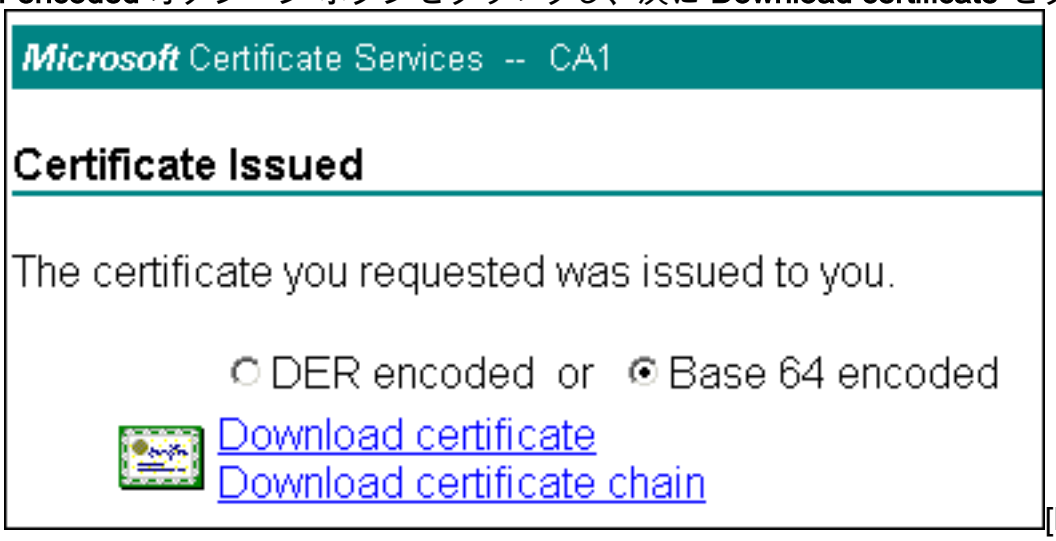
注: CA サーバで、ASA（VPN サーバ）のユーザ アカウントを所有していることを確認してください。[Request a certificate] > [advanced certificate request] の順にクリックし、[Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file] を選択します。



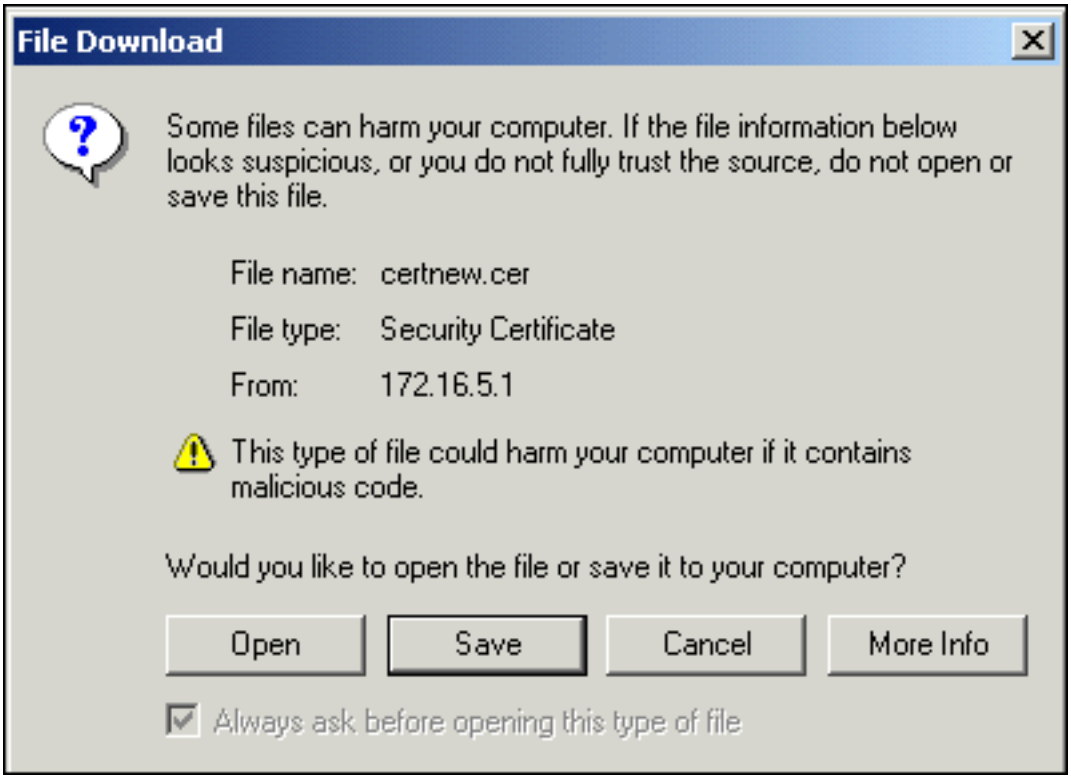
符号化された情報を [Saved Request] ボックスにコピー アンド ペーストし、[Submit] をクリックします。



Base 64 encoded オプション ボタンをクリックし、次に **Download certificate** をクリックします。



[File Download] ダイアログ ボックスが表示されたら、ASA にインストールする ID 証明書として **cert_client_id.cer** という名前で保存します。



コマンドラインの例

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:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgTDk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNvbTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKargwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeOHZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPIbkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
```

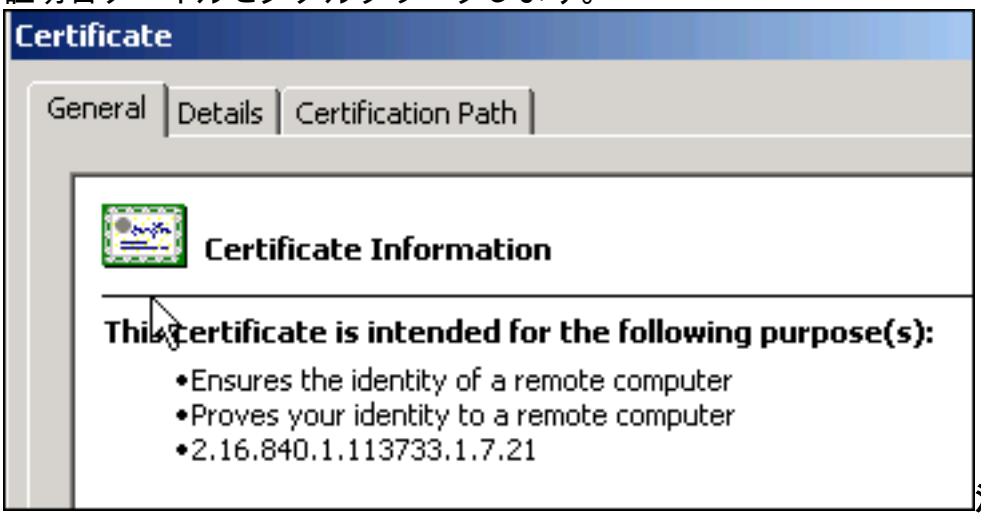
```
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no ciscoasa(config)#
```

ステップ 5. トラストポイントを認証する

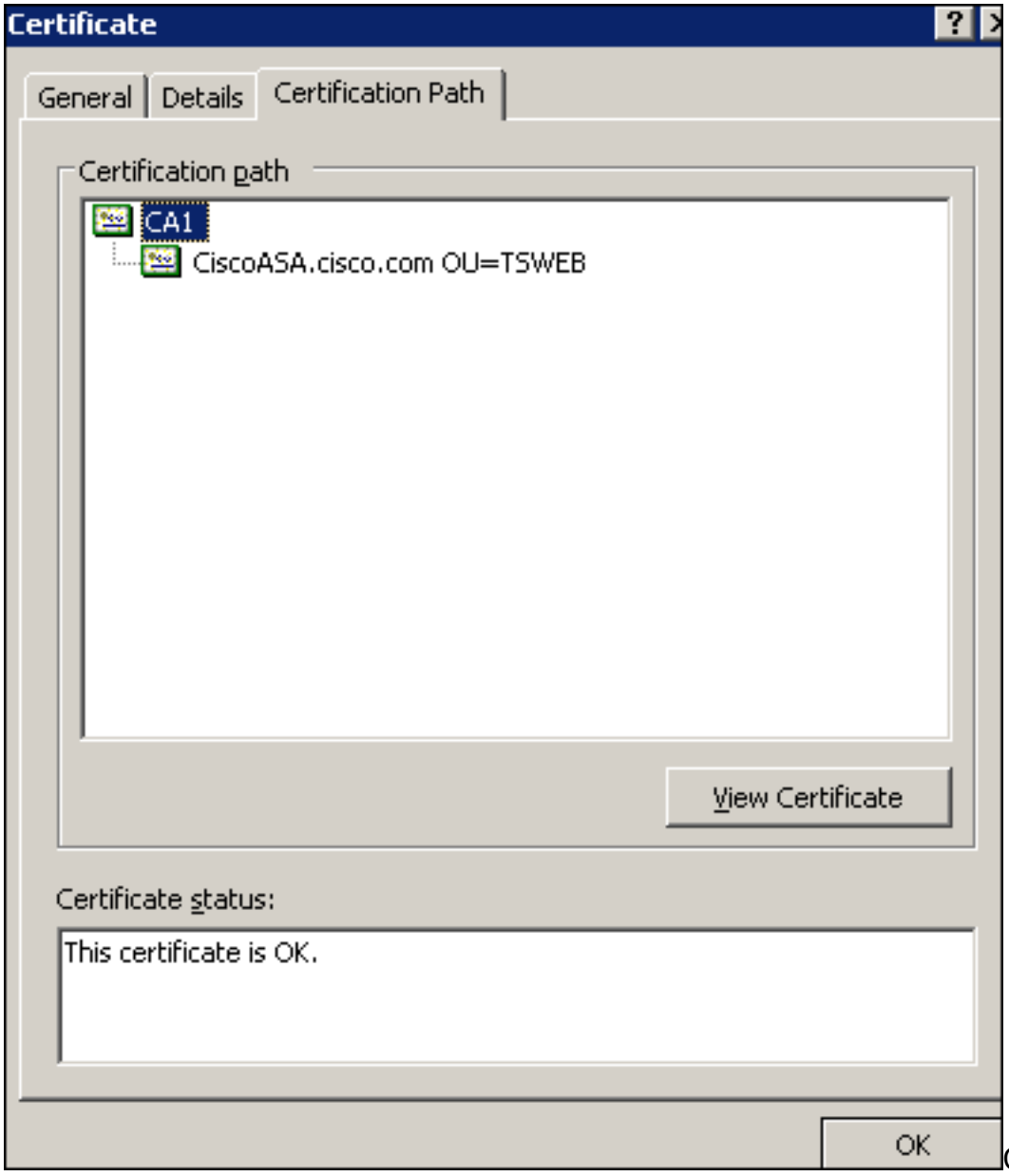
サードパーティ ベンダーから ID 証明書を受信したら、引き続きこのステップを実行します。

ASDM の手順

1. ID 証明書をローカル コンピュータに保存します。
2. ファイル形式ではない Base64 で符号化された証明書が提供された場合、Base64 メッセージをコピーし、テキスト ファイルに貼り付ける必要があります。
3. .cer 拡張子を使用してファイルの名前を変更します。**注:** .cer 拡張子を使用してファイルの名前を変更すると、ファイルのアイコンは証明書として表示されます。 

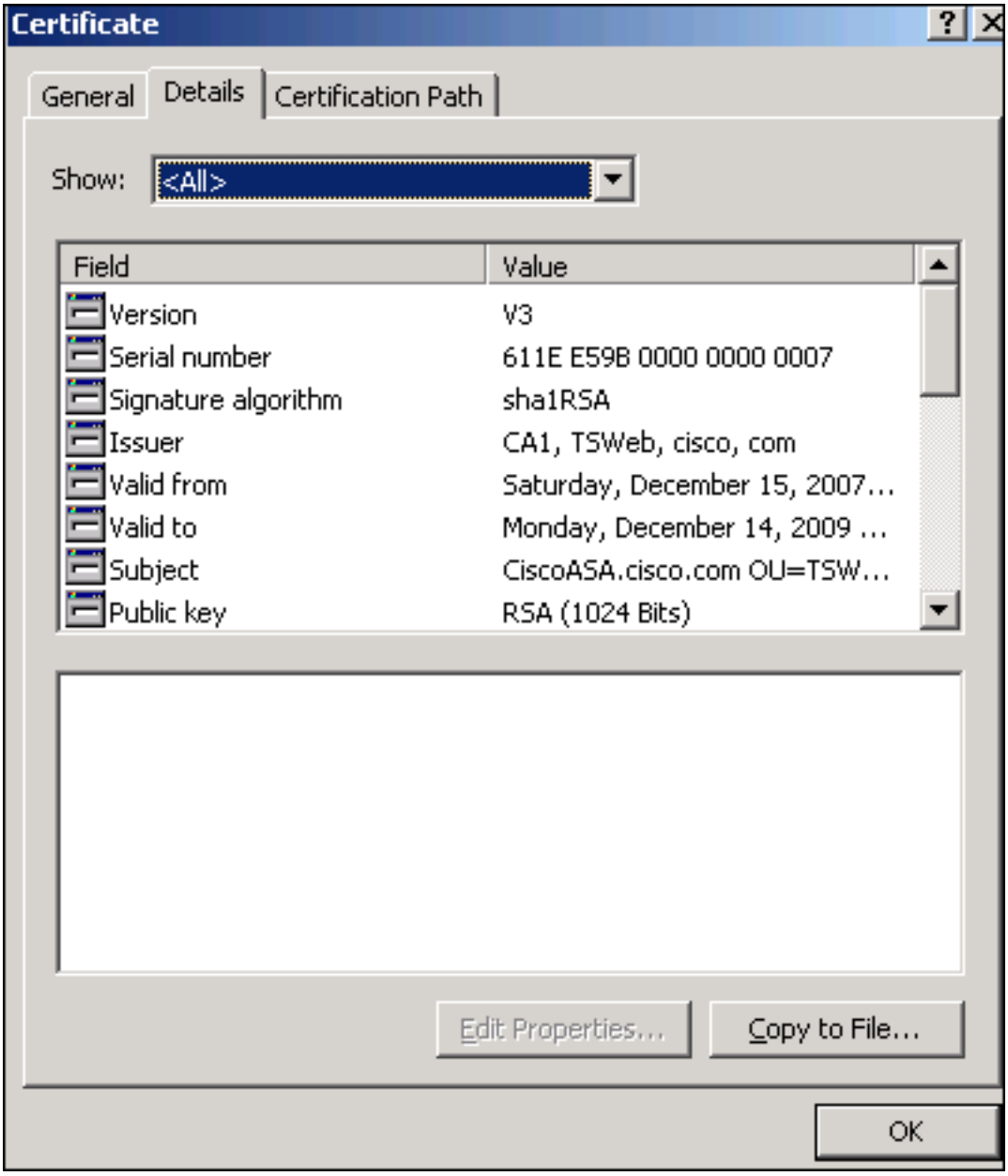
4. 証明書ファイルをダブルクリックします。 

注: General タブに「Windows does not have enough information to verify this certificate」というメッセージが表示された場合、この手順を継続する前に、サードパーティ ベンダーのルート CA または中間 CA 証明書を入手する必要があります。 ルート CA または中間 CA 証明書を入手するには、サードパーティ ベンダーまたは CA 管理者に問い合せてください。
5. [Certificate Path] タブをクリックします。
6. 発行された ID 証明書の上にある CA 証明書をクリックし、[View Certificate] をクリックし

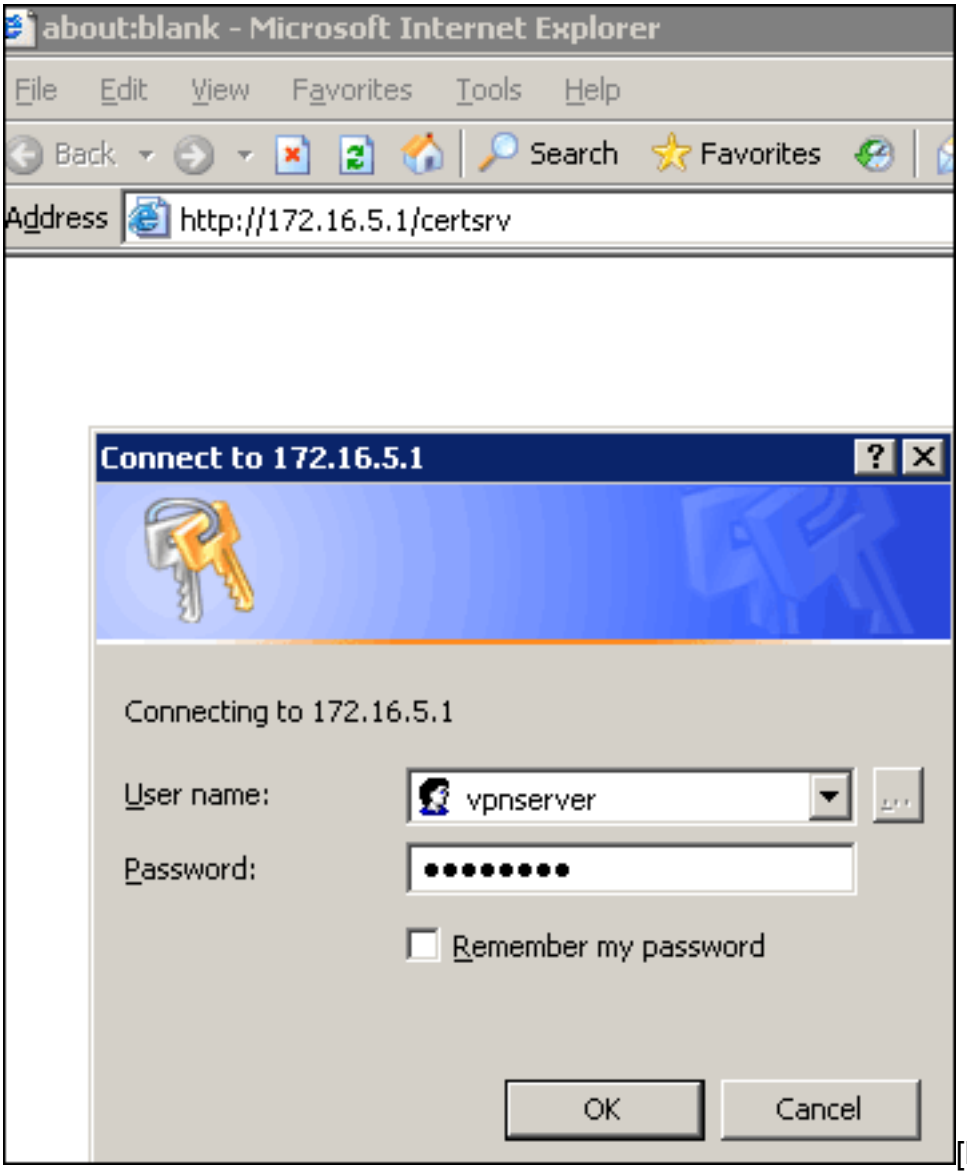


ます。CA 証明書に関する詳細情報が表示されます。

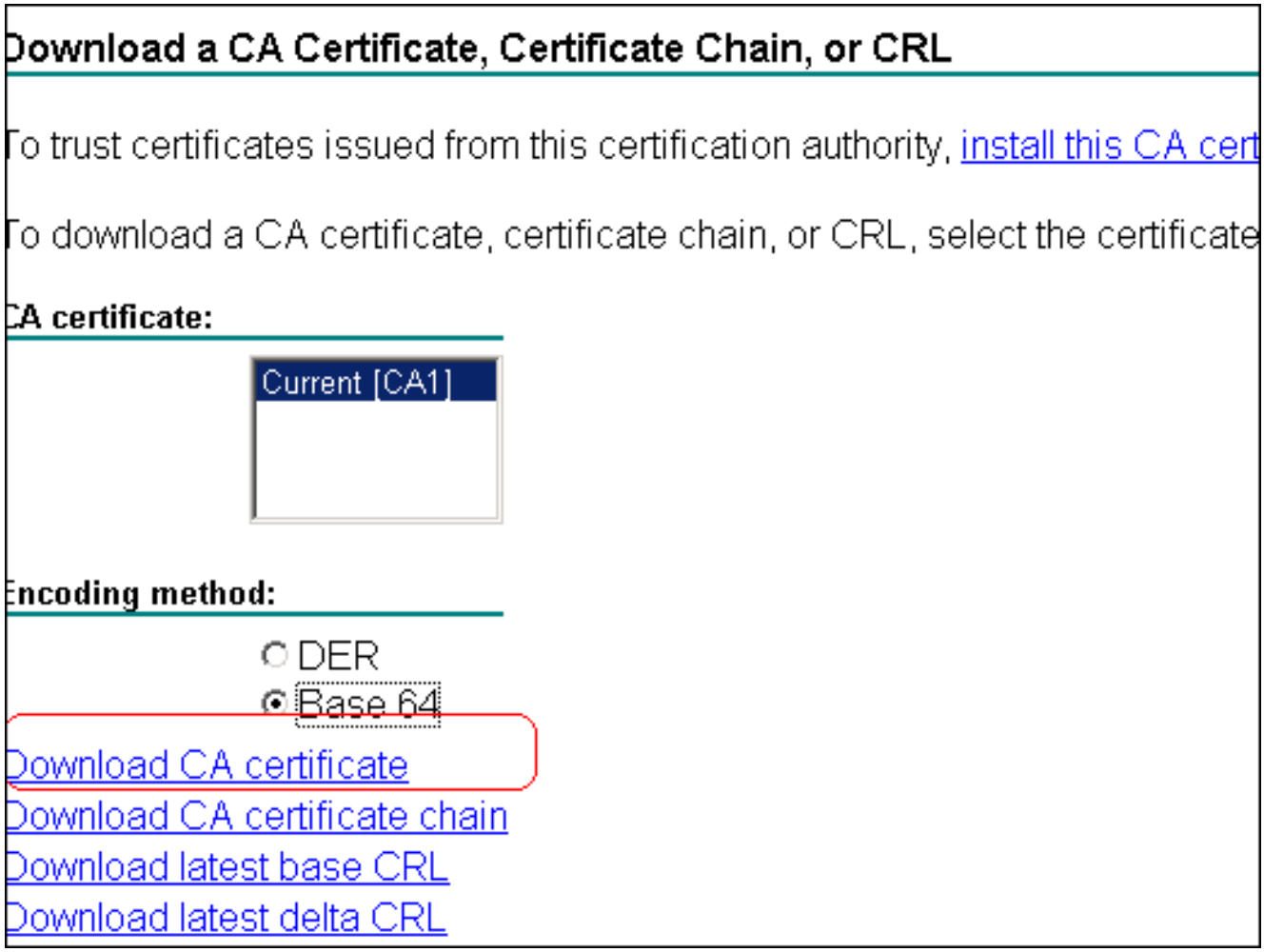
7. **Details** をクリックして、ID 証明書の詳細情報を確認します。



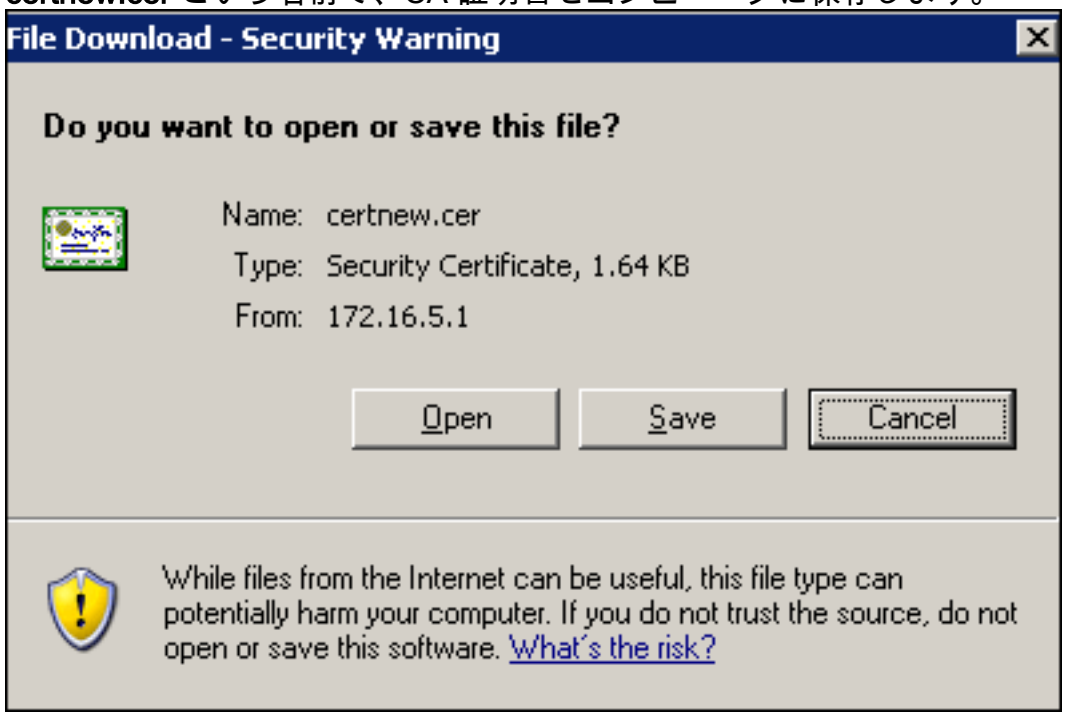
8. ID 証明書をインストールする前に、CA 証明書を CA サーバからダウンロードし、ASA にインストールする必要があります。 次の手順を実行して、*CA1* という名前の CA サーバから CA 証明書をダウンロードします。VPN サーバに提供されたユーザ クレデンシャルを使用して、CA サーバ 172.16.5.1 にログインします。



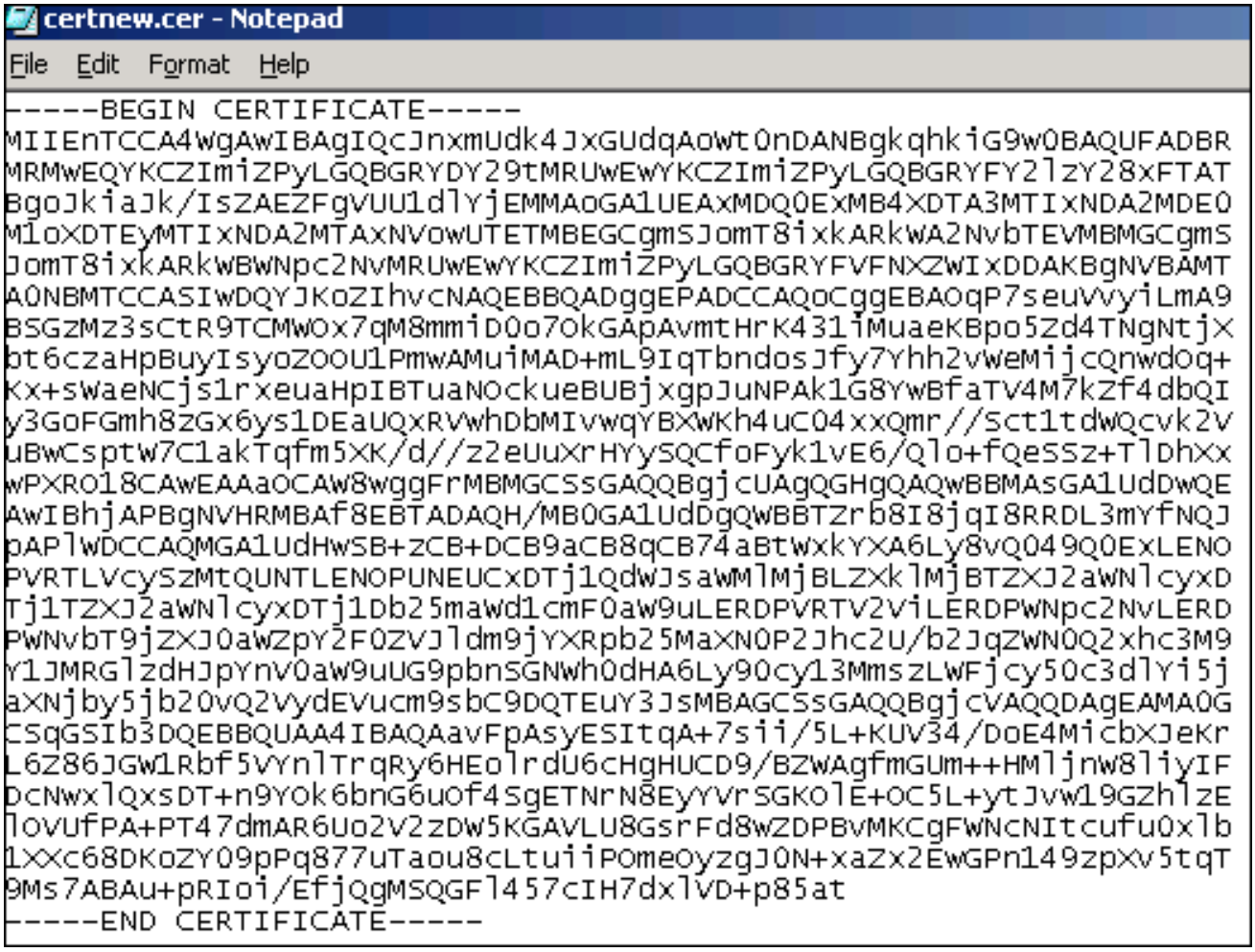
[Download a CA certificate, certificate chain or CRL] をクリックし、[Base 64] オプション ボタンを選択して符号化方式を指定します。[Download CA certificate] をクリックします。



certnew.cer という名前で、CA 証明書をコンピュータに保存します。



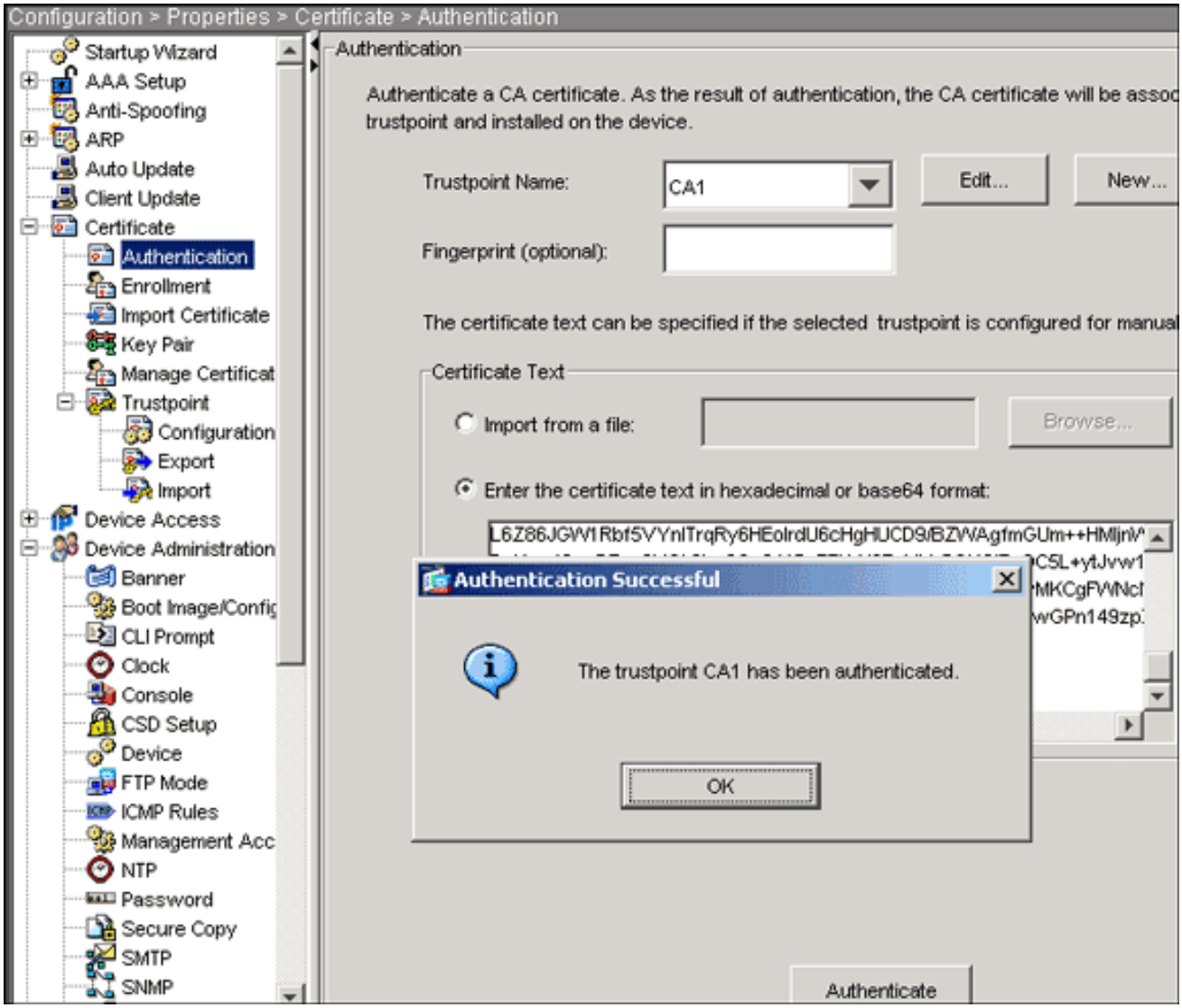
9. CA 証明書を保存した場所を表示します。
10. メモ帳などのテキスト エディタでファイルを開きます。（ファイルを右クリックし、[Send To] > [Notepad] の順に選択します）。
11. Base64 で符号化されたメッセージは、次の画像の証明書のようになります。


certnew.cer - Notepad

File Edit Format Help

```
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAKBgNVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuVvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMijcQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1tdWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMASGA1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNwh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMljnW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw19GZhlzE
lOvUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8WZDPBvMKCgFWNcNItcufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+p85at
-----END CERTIFICATE-----
```

12. ASDM で [Configuration] をクリックし、[Properties] をクリックします。
13. [Certificate] を展開し、[Authentication] を選択します。
14. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックします。
15. Base64 形式で作成された CA 証明書をテキスト エディタからテキスト領域に貼り付けます。
16. [Authenticate] をクリックします。



17. [OK] をクリックします。

コマンドラインの例

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
```

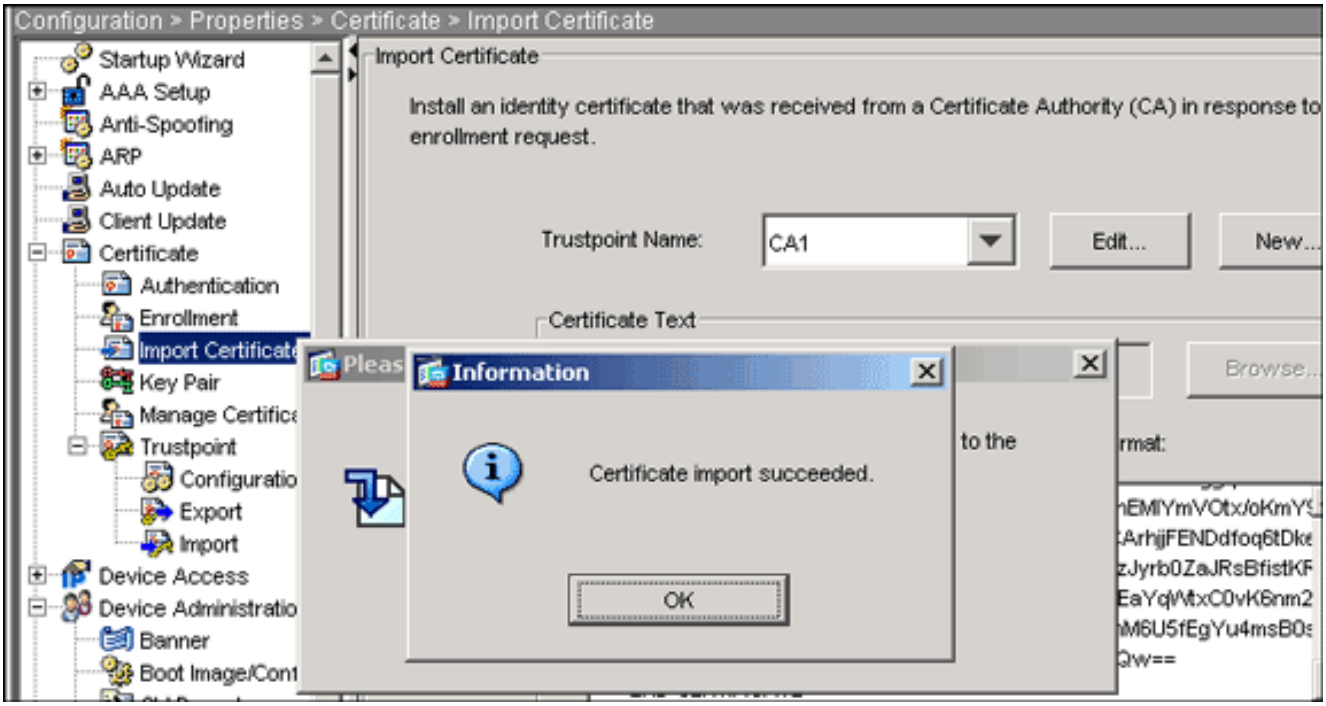
```
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSS
z+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
L3mYfNQJ
pAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
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)#
```

ステップ 6. 証明書をインストールする

ASDM の手順

次の手順を実行するには、サードパーティ ベンダーにより提供された ID 証明書を使用します。

1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Import Certificate] を選択します。
3. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックし、テキスト フィールドに Base64 ID 証明書を貼り付けます。



4. [Import] をクリックし、[OK] をクリックします。

コマンドラインの例

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
```

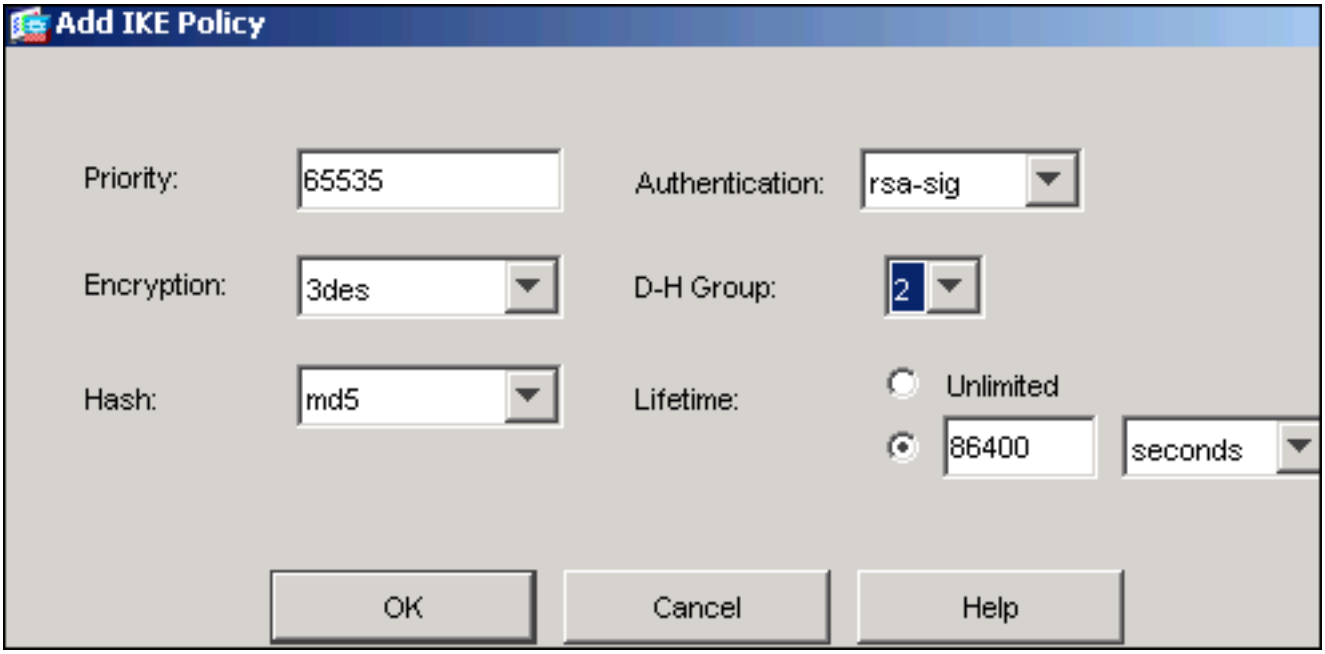
```
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
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)#
```

ステップ 7. 新しくインストールした証明書を使用するようにリモート アクセス VPN (IPSec) を設定する

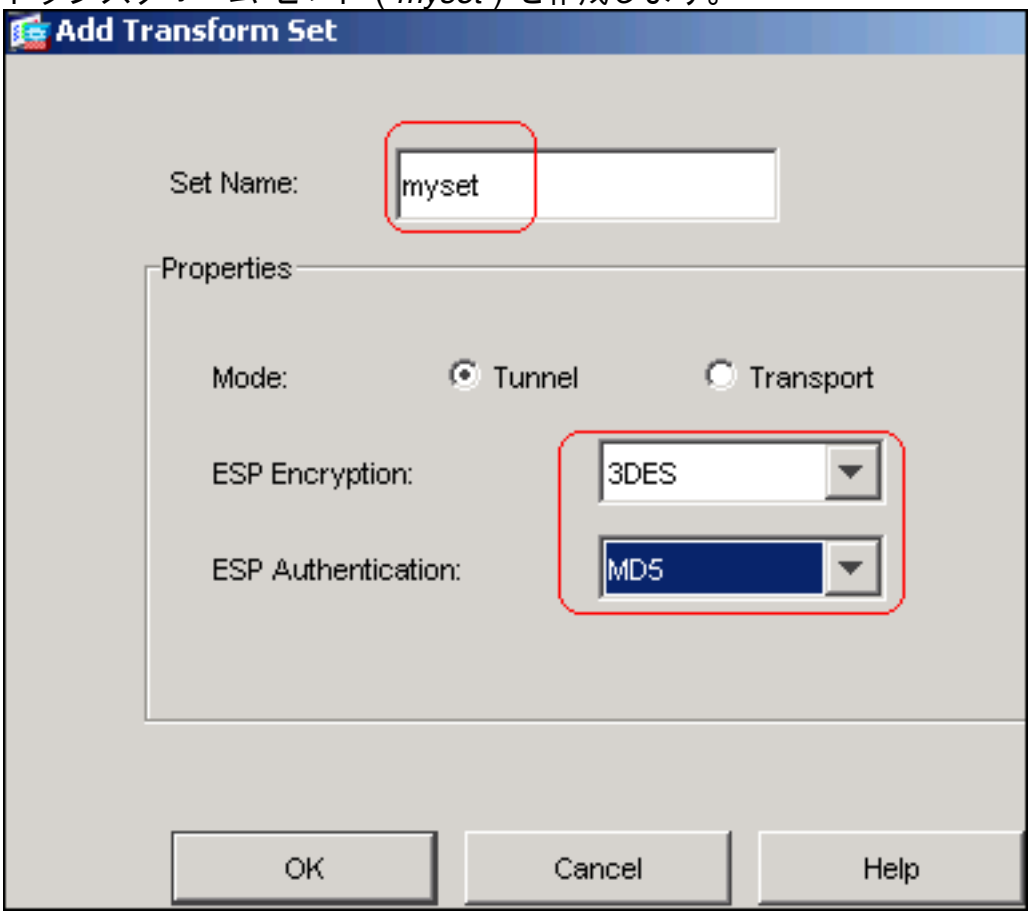
ASDM の手順

リモート アクセス VPN を設定するには、次の手順を実行します。

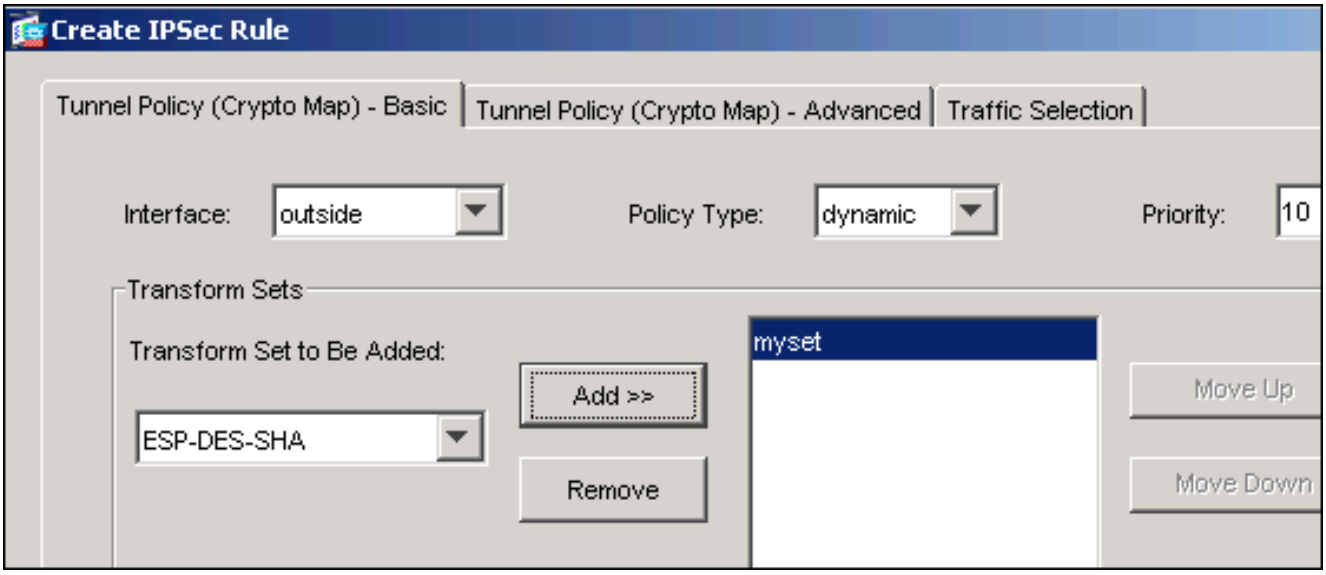
1. [Configuration] > [VPN] > [IKE] > [Policies] > [Add] の順に選択し、この図のように ISAKMP ポリシー 65535 を作成します。



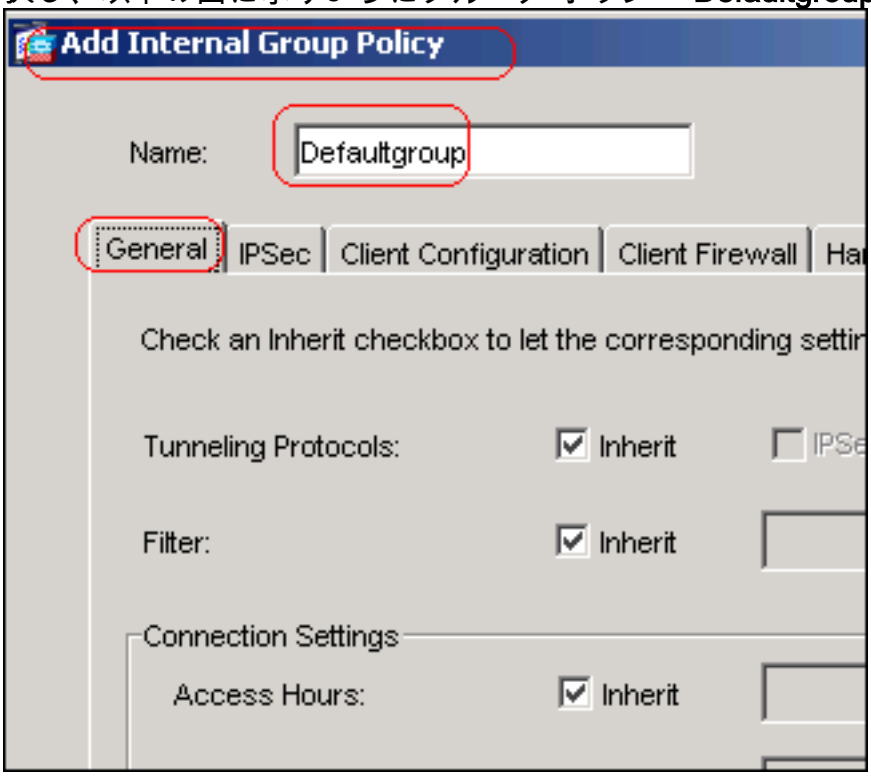
2. [OK] をクリックして、[Apply] をクリックします。
3. [Configuration] > [VPN] > [IPSec] > [Transform Sets] > [Add] の順に選択し、この図のようにトランスフォーム セット（*myset*）を作成します。

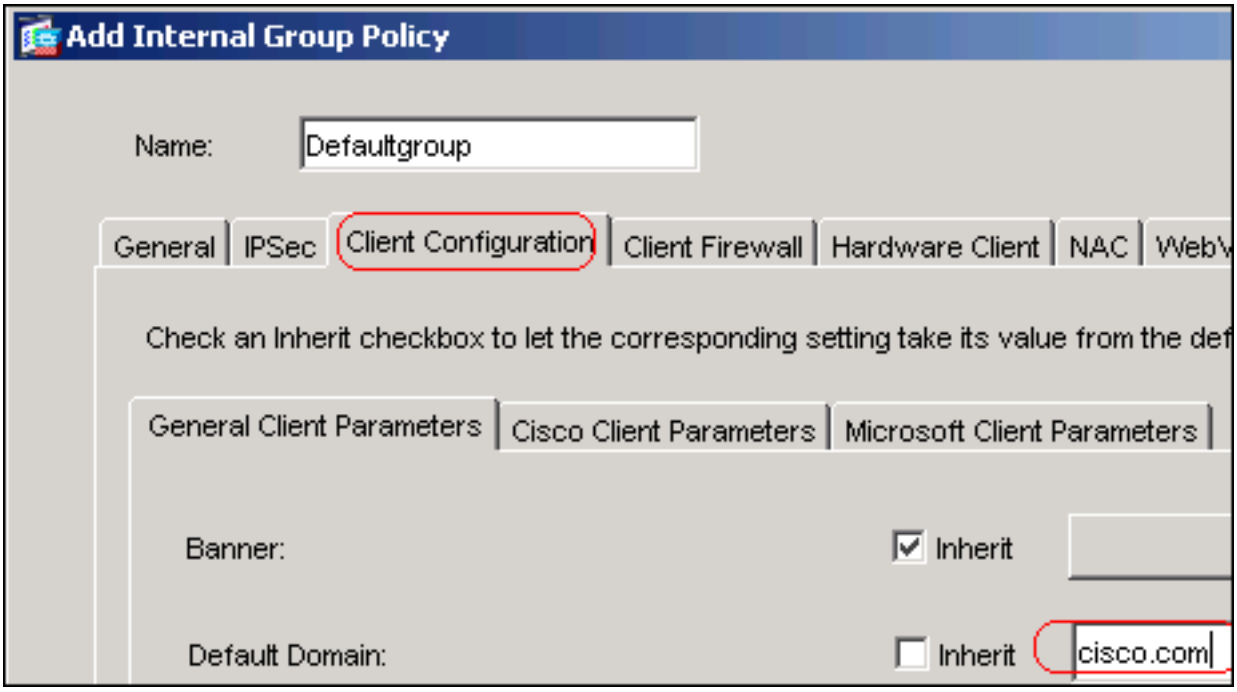


4. [OK] をクリックし、[Apply] をクリックします。
5. [Configuration] > [VPN] > [IPSec] > [IPSec Rules] > [Add] の順に選択し、この図のように、ダイナミック ポリシーのプライオリティが 10 であるクリプト マップを作成します。

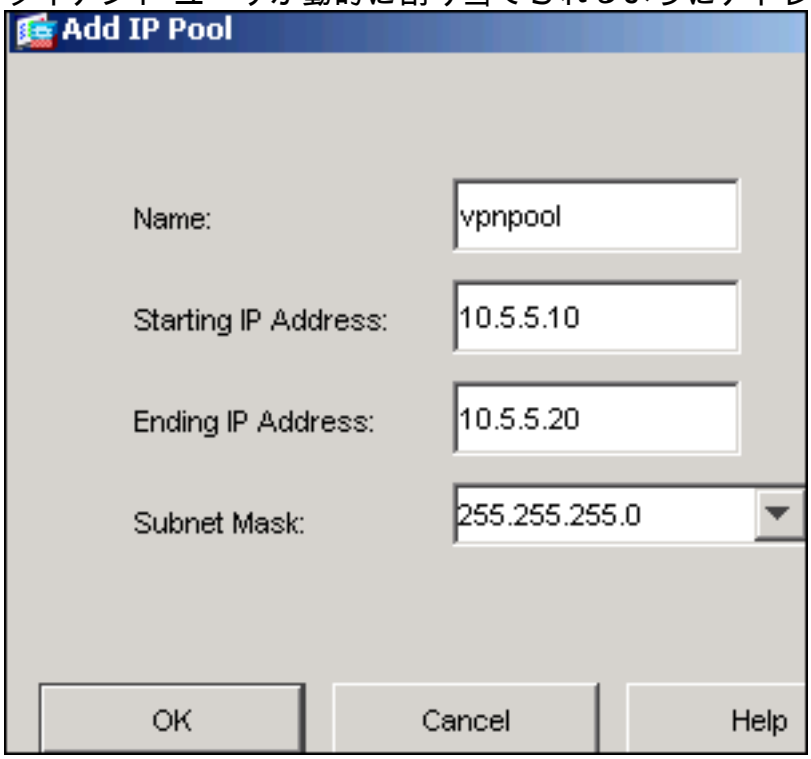


6. [OK] をクリックし、[Apply] をクリックします。
7. [Configuration] > [VPN] > [General] > [Group Policy] > [Add Internal Group Policy] の順に選択し、以下の図に示すようにグループ ポリシー **Defaultgroup** を作成します。



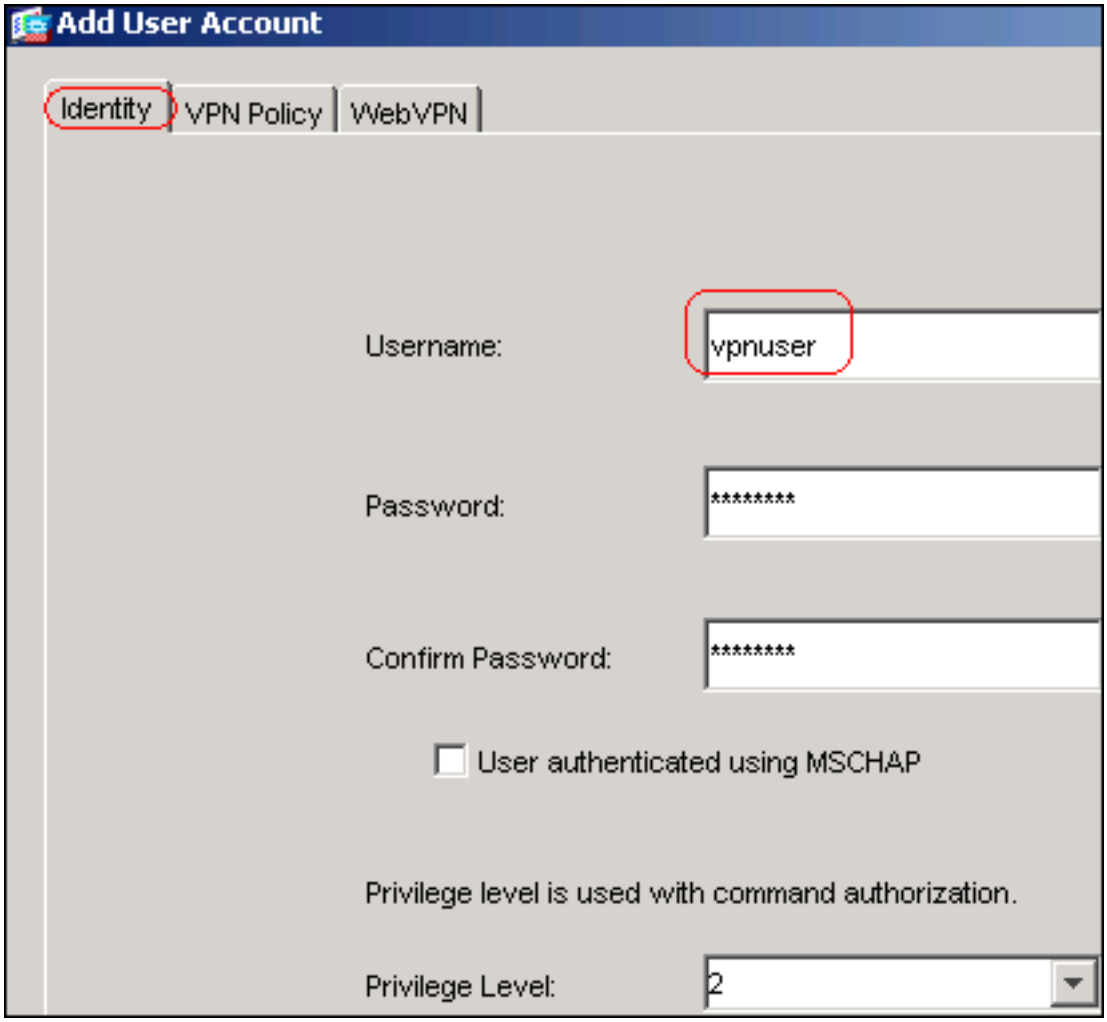


8. [OK] をクリックし、[Apply] をクリックします。
9. [Configuration] > [VPN] > [IP Address Management] > [IP Pools] > [Add] の順に選択し、VPN クライアント ユーザが動的に割り当てられるようにアドレス プール vpnpool を設定します

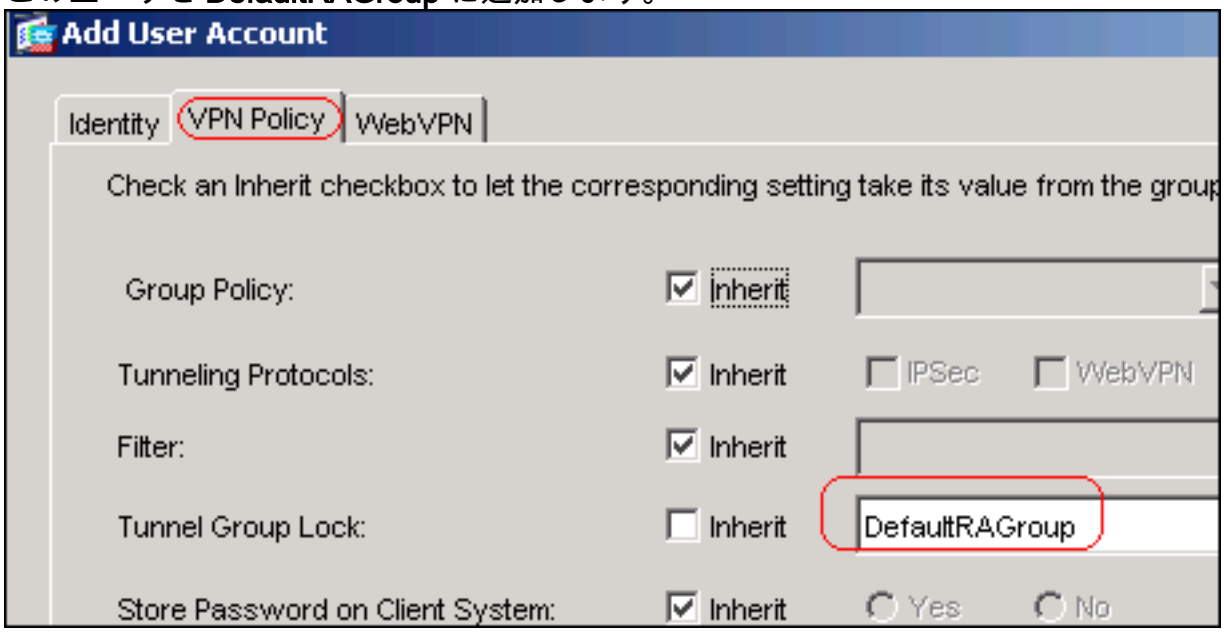


。

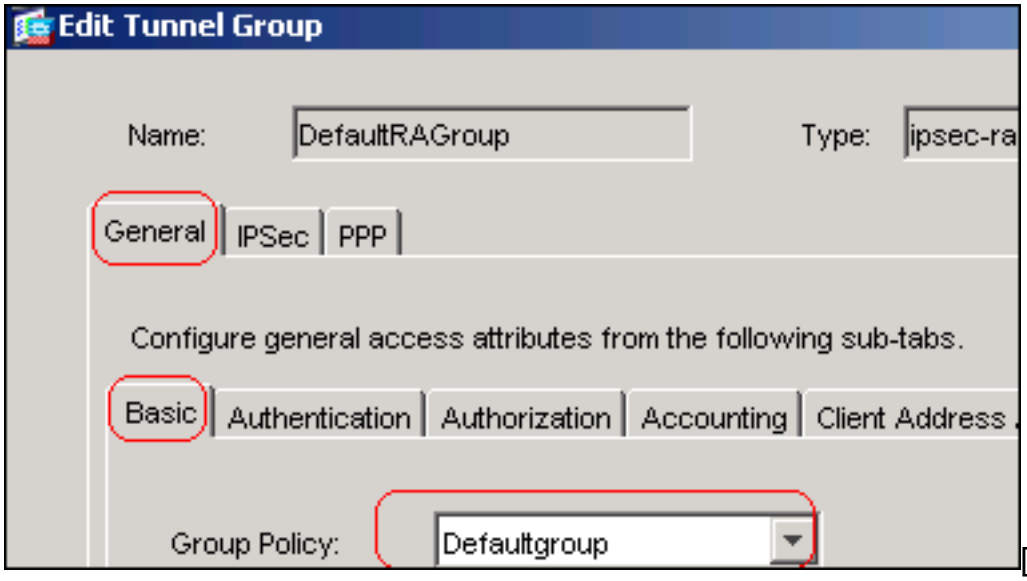
10. [OK] をクリックし、[Apply] をクリックします。
11. [Configuration] > [VPN] > [General] > [Users] > [Add] の順に選択し、VPN クライアント アクセス用のユーザ アカウント **vpnuser** を作成します。



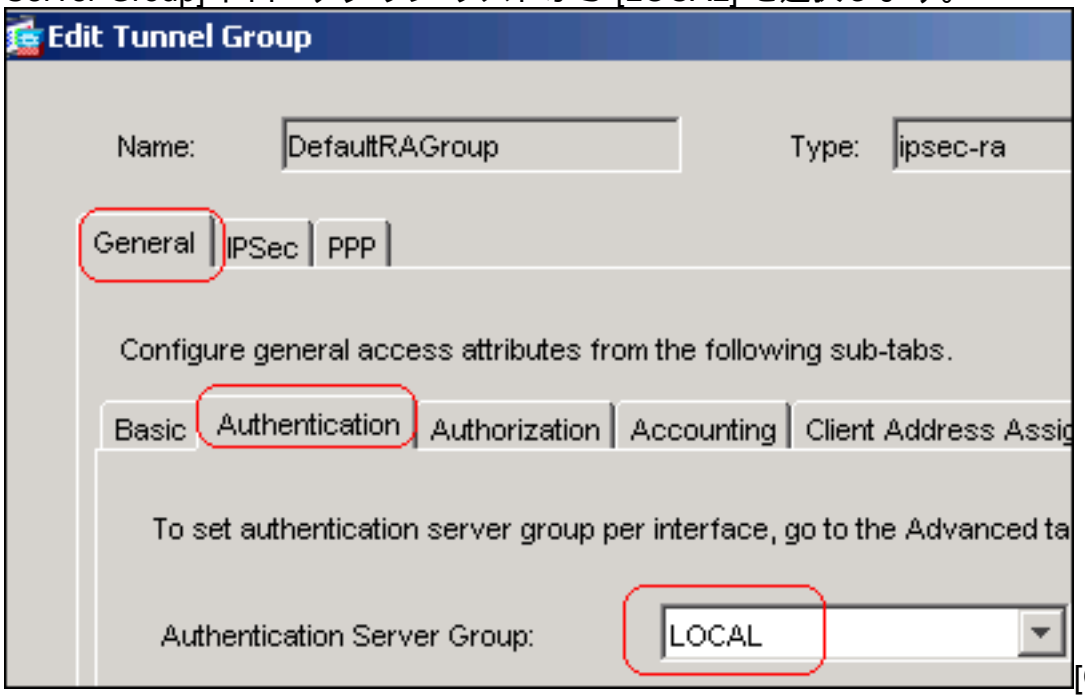
12. このユーザを **DefaultRAGroup** に追加します。



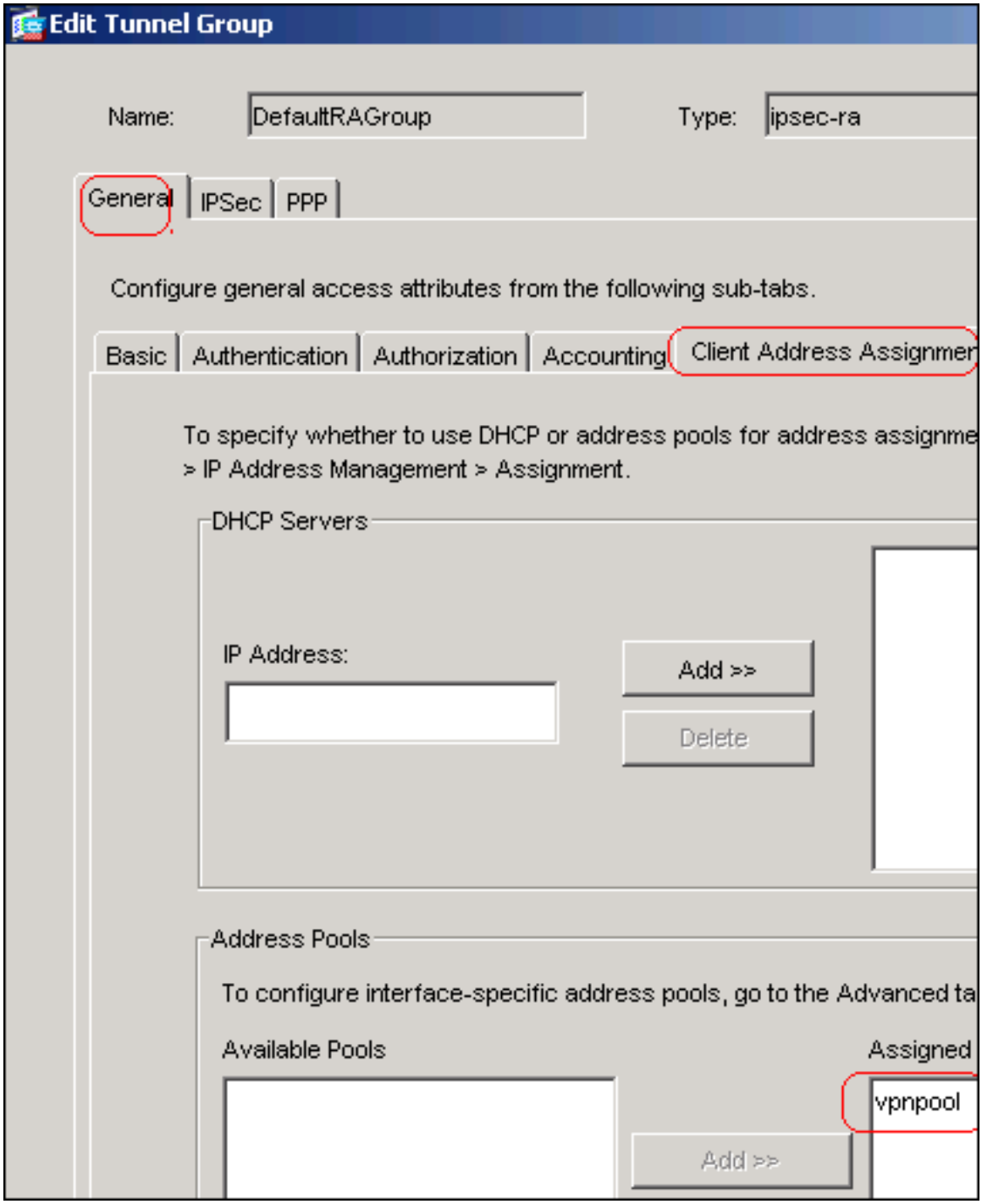
13. [OK] をクリックし、[Apply] をクリックします。
14. 次の手順を実行して DefaultRAGroup を編集します。[Configuration] > [VPN] > [General] > [Tunnel Group] > [Edit] の順に選択します。[Group Policy] ドロップダウン リストから [Defaultgroup] を選択します。



[Authentication Server Group] ドロップダウン リストから [LOCAL] を選択します。



[Client Address Assignment] ドロップダウン リストから [vpnpool] を選択します。



15. [OK] をクリックし、次に [Apply] をクリックします。

コマンドラインの例

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 の設定の概要

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
```

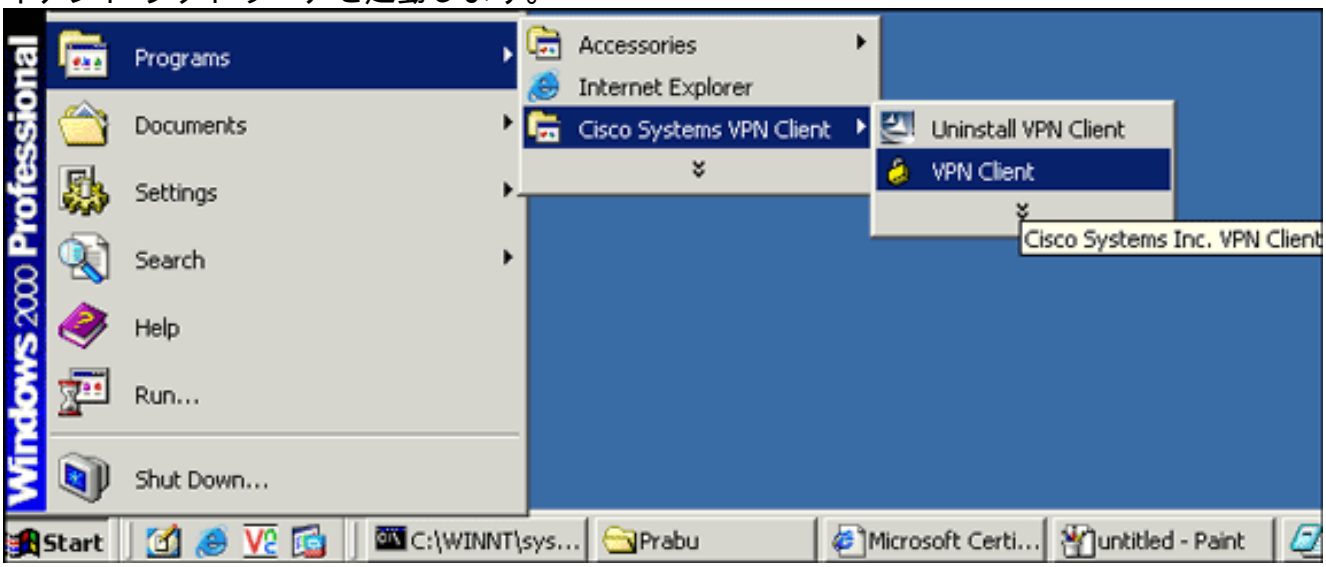
```
0d030730 0d06092a 864886f7 0d010105 05000382 010100bf
99b9daf2 e24f1bd6 ce8271eb 908fadb3 772df610 0e78b198
f945f379 5d23a120 7c38ae5d 8f91b3ff 3da5d139 46d8fb6e
20d9a704 b6aa4113 24605ea9 4882d441 09f128ab 4c51a427
fa101189 b6533eef adc28e73 fcfed3f1 f4e64981 0976b8a1
2355c358 a22af8bb e5194b42 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#
```

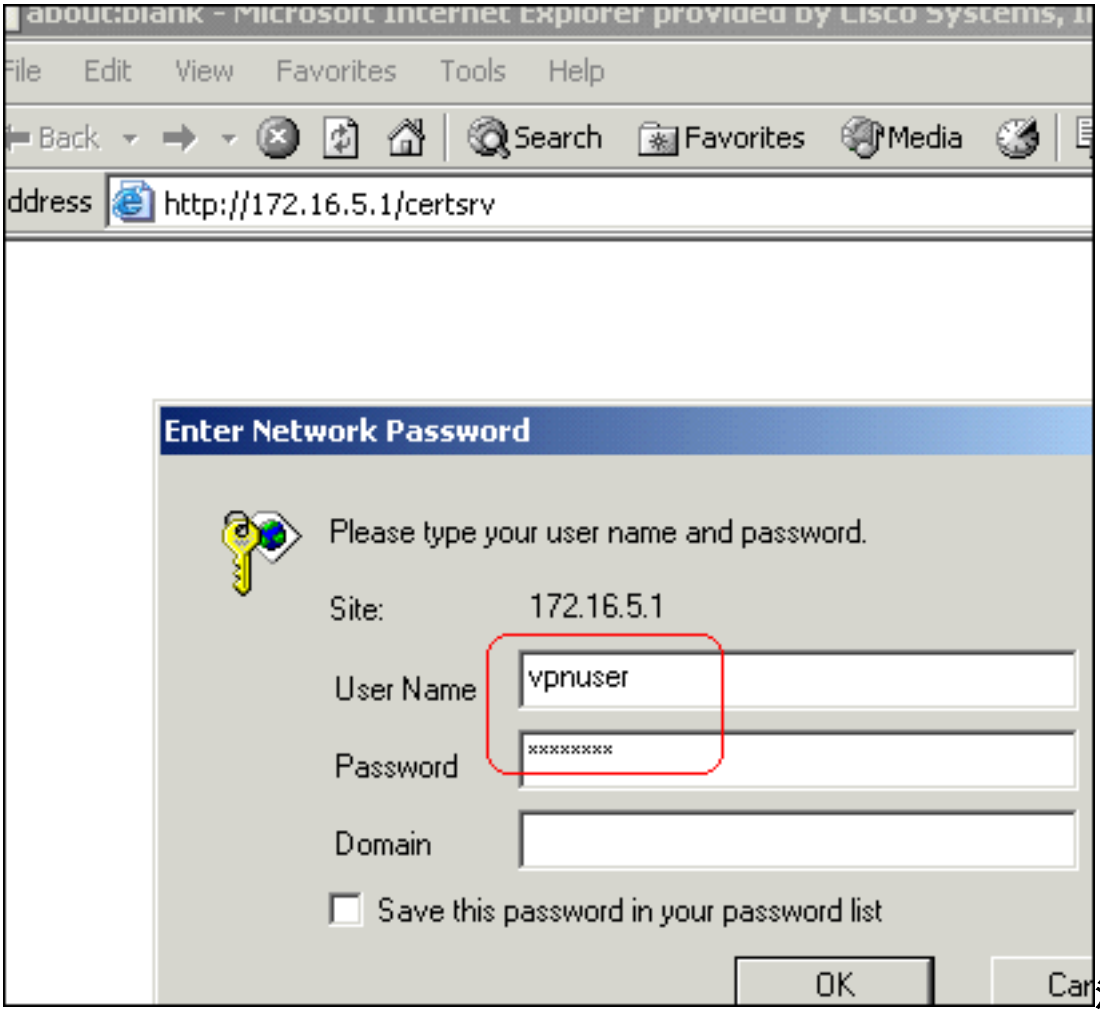
VPN Client の設定

次の手順を実行して、VPN Client を設定します。

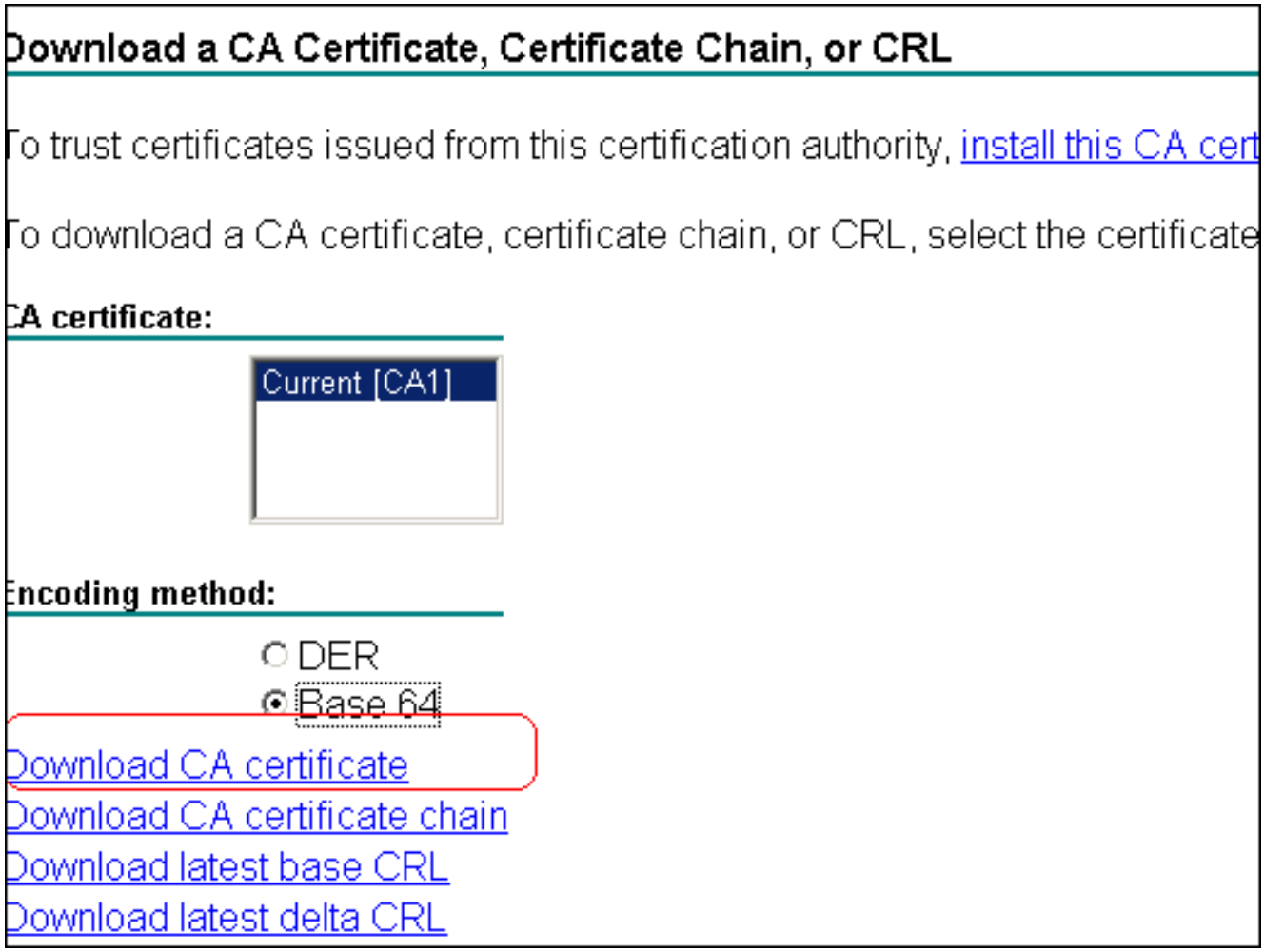
1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択し、VPN クライアント ソフトウェアを起動します。



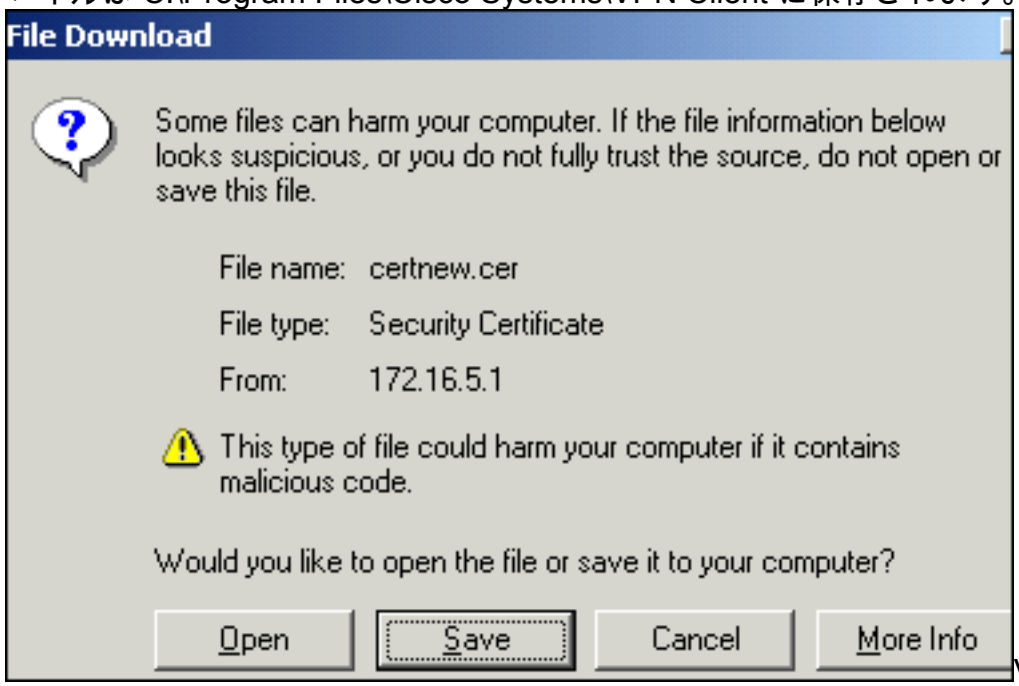
2. 次の手順を実行して、**CA1** という名前の CA サーバから CA 証明書をダウンロードし、Cisco VPN Client にインストールします。vpnuser に提供されたユーザ クレデンシャルを使用して、CA サーバ 172.16.5.1 にログインします。



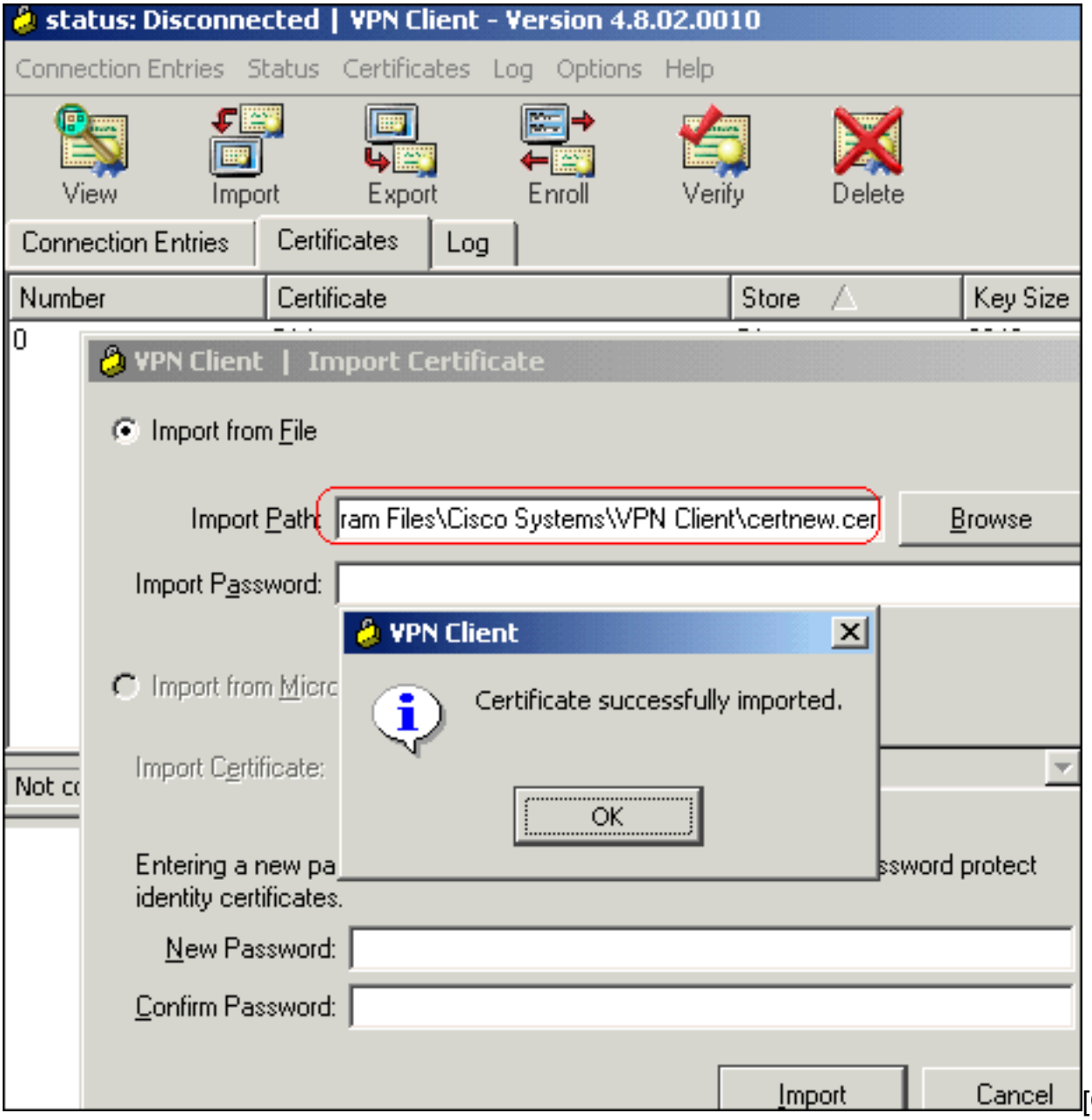
注: CA のサーバで、VPN Client ユーザのユーザ アカウントを持っていることを確認してください。[Download a CA certificate, certificate chain or CRL] をクリックし、[Base 64] オプション ボタンを選択して符号化方式を指定します。[Download CA certificate] をクリックします。



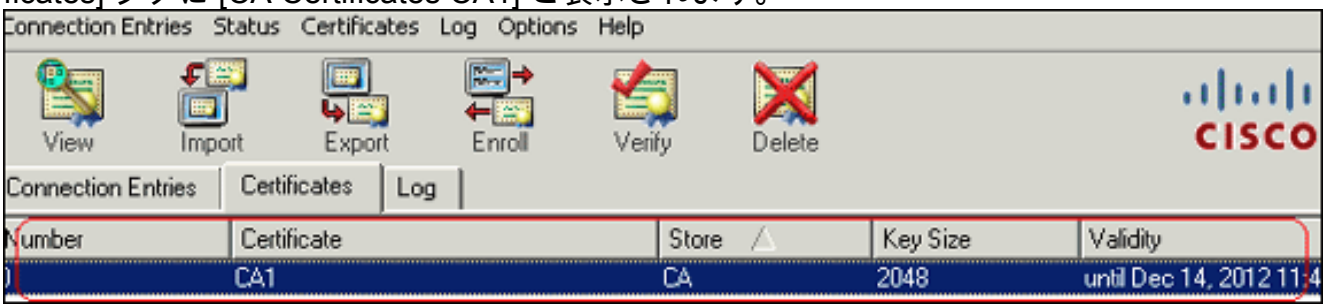
certnew.cer という名前で、CA 証明書をコンピュータに保存します。 デフォルトでは、ファイルは C:\Program Files\Cisco Systems\VPN Client に保存されます。



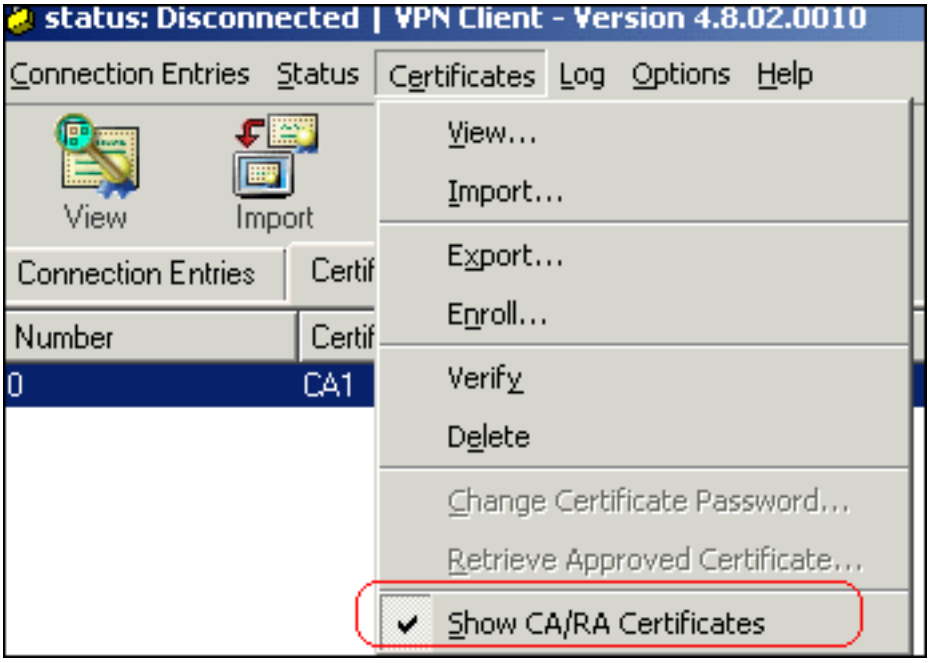
VPN Client で [Certificates] タブをクリックし、[Import] を選択します。[Import from File] オプション ボタンをクリックし、[Browse] をクリックして、保存場所の C:\Program Files\Cisco Systems\VPN Client から CA 証明書をインポートします。[Import] をクリックします。証明書が正常にインポートされたことを示すダイアログ ボックスが表示されます。



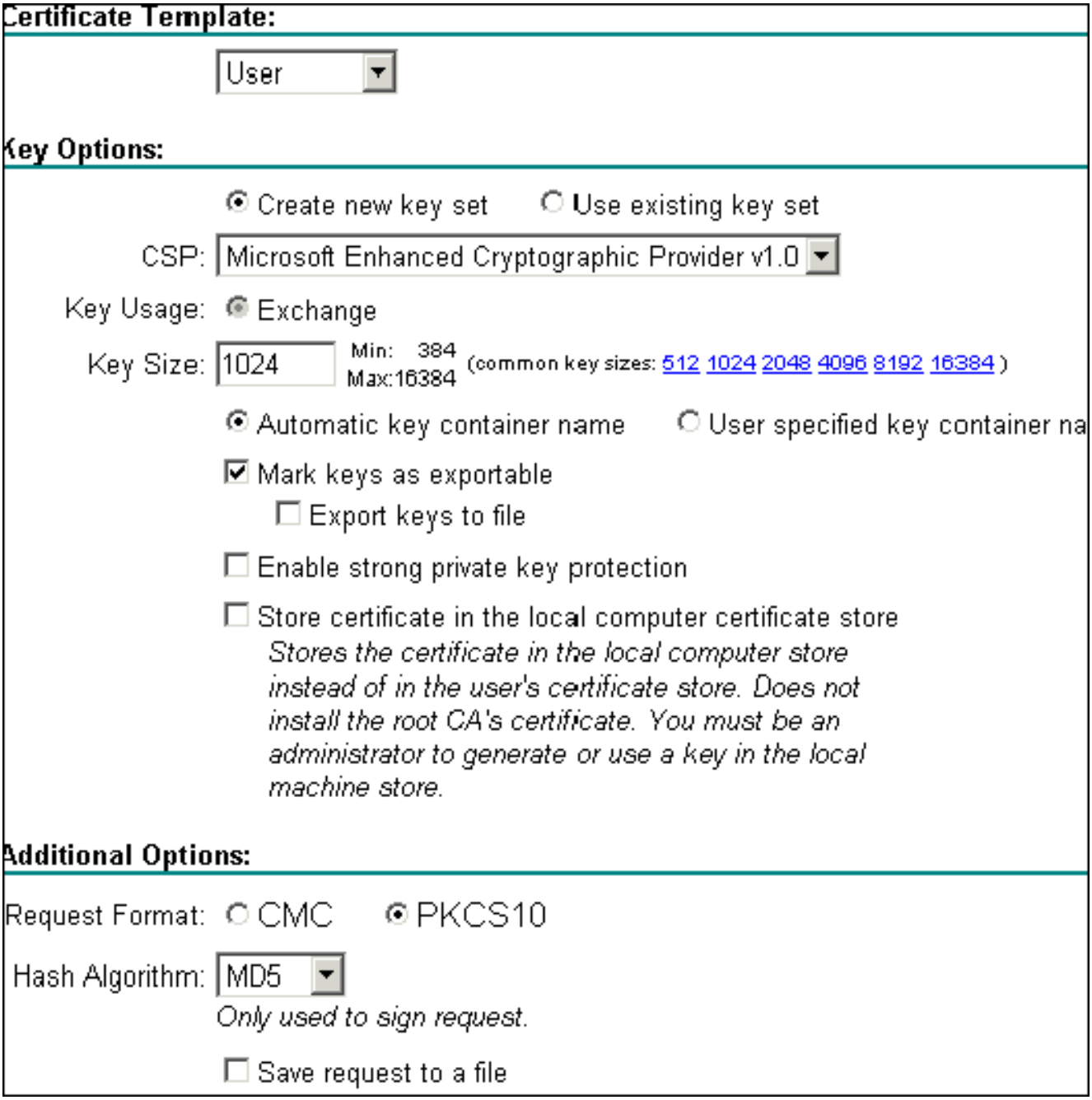
[Certificates] タブに [CA Certificates CA1] と表示されます。



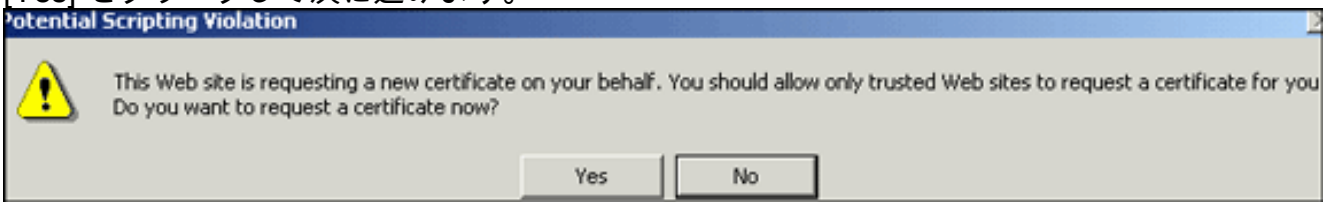
注: [Show CA/RA Certificates] オプションを選択していることを確認します。 選択されていないと、証明書ウィンドウに CA 証明書が表示されません。



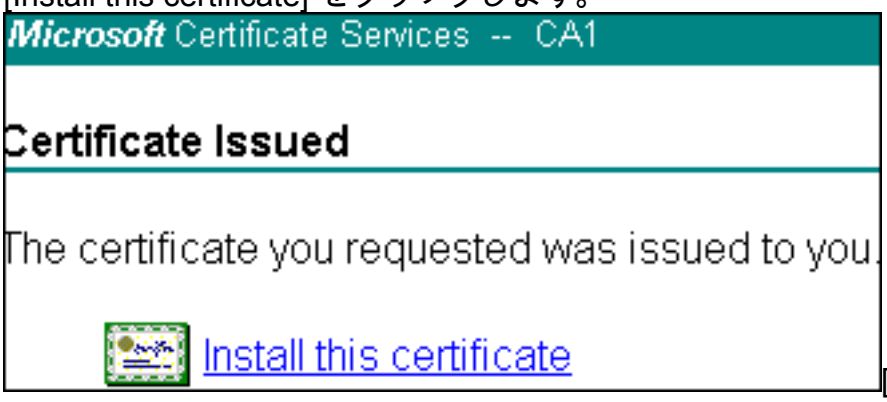
3. 次の手順を実行して、ID 証明書をダウンロードし、VPN Client にインストールします。CA のサーバ CA1 で、[Request a Certificate] > [advanced certificate request] > [Create and submit a request to this CA] の順に選択し、ID 証明書を登録します。[Submit] をクリックします。



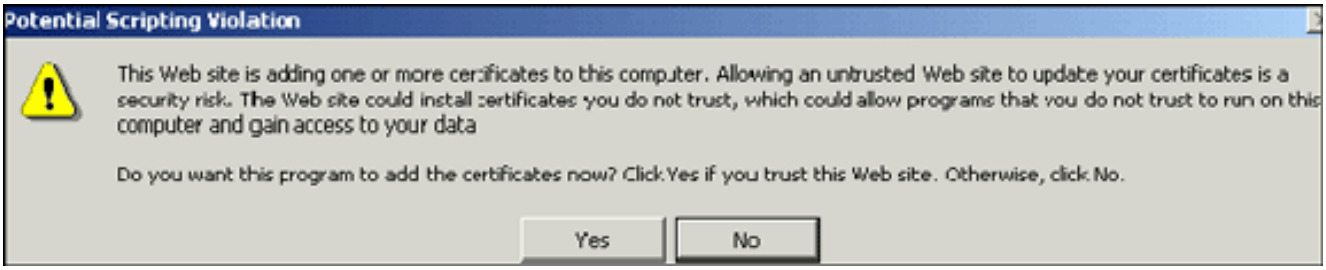
[Yes] をクリックして次に進みます。



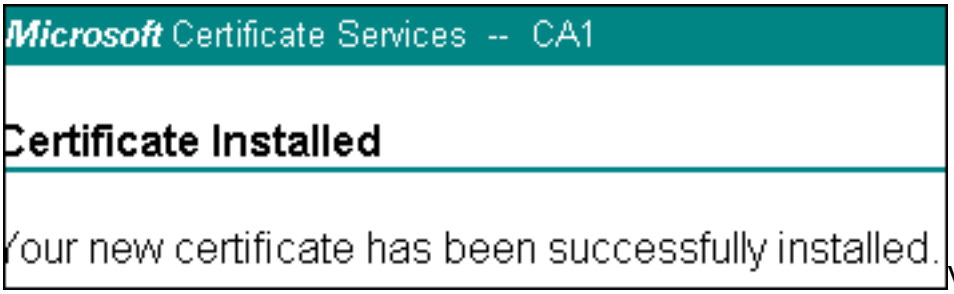
[Install this certificate] をクリックします。



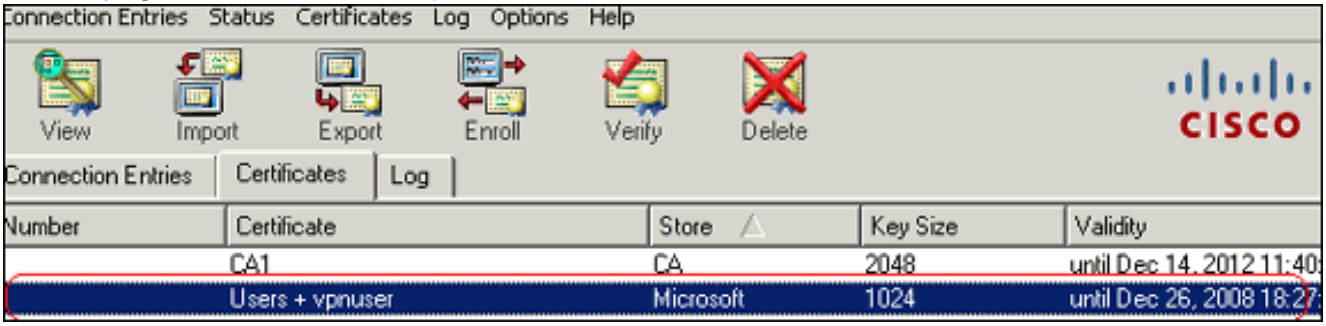
[Yes] をクリックして次に進みます。



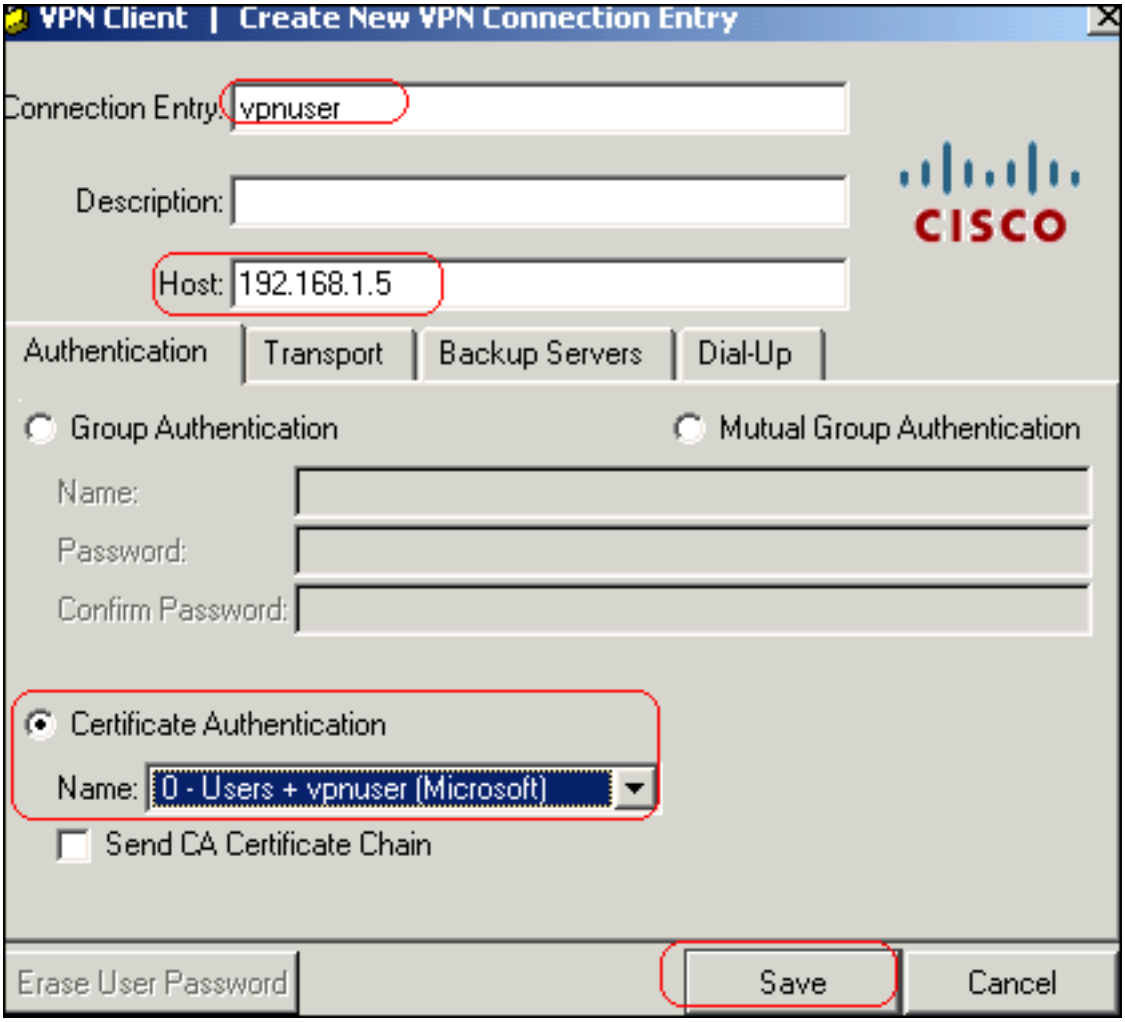
次の図のように、証明書がインストールされたことを示すメッセージが表示されます。



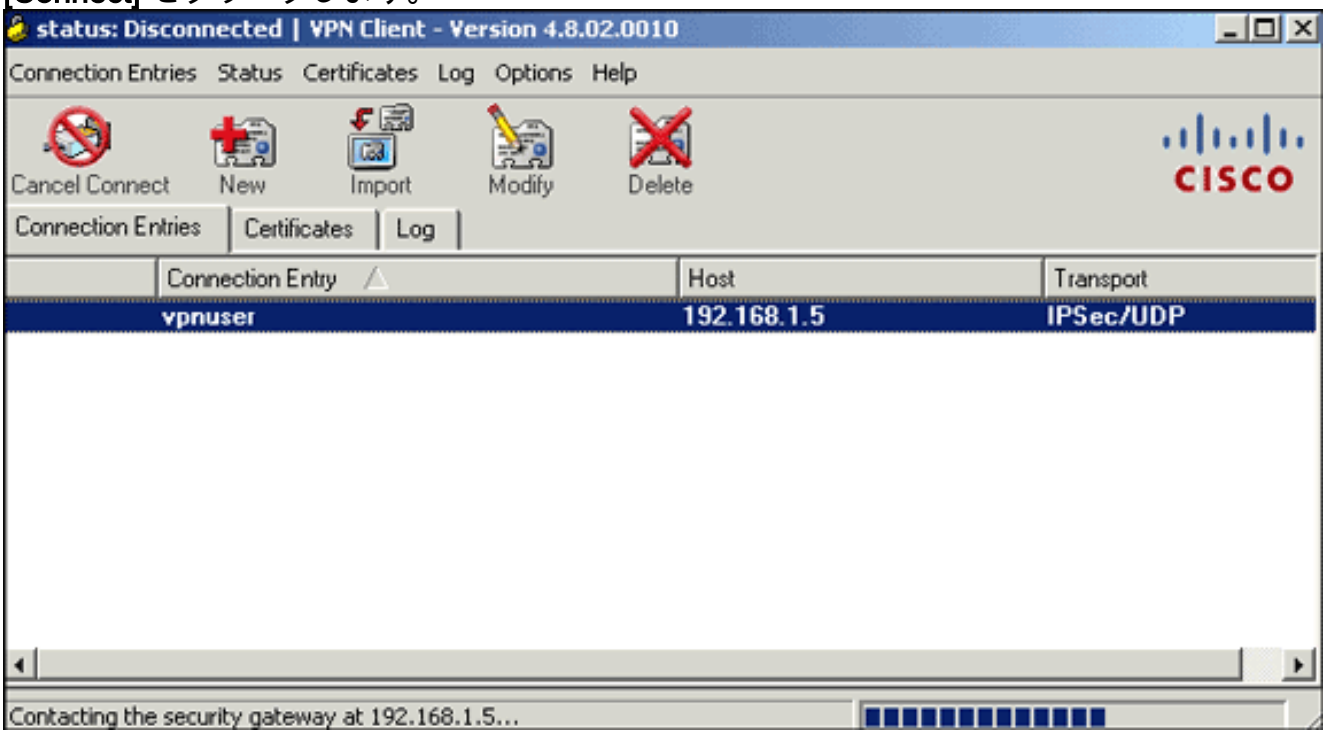
VPN Client を終了して再起動し、インストールされた ID 証明書が、次の図に示すように VPN Client の [Certificates] タブに表示されるようにします。



4. 次の手順を実行して、接続エントリ (*vpnuser*) を作成します。[Connection Entries] タブをクリックし、[New] をクリックします。Host フィールドにルーティング可能なリモート ピアの IP アドレスを入力します。[Certificate Authentication] オプション ボタンを選択し、ドロップダウン リストから ID 証明書を選択します。[Save] をクリックします。



5. [Connect] をクリックします。



6. ダイアログボックスが表示されたら、xauth のユーザ名とパスワード情報を入力して、[OK] をクリックし、リモート ネットワークに接続します。

7. 次の図に示すように、VPN Client が ASA に接続されます。

確認

ASA では、コマンドラインで各種の show コマンドを使用して、証明書の状況を確認できます。

ここでは、設定が正常に動作していることを確認します。

- **show crypto ca trustpoint** — 設定されているトラストポイントを表示します。`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** — システムにインストールされているすべての証明書を表示します。`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=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 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=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 UTC Dec 14 2007 end date: 06:10:15 UTC Dec 14 2012 Associated Trustpoints: CA1`
- **show crypto ca crls** — キャッシュされている Certificate Revocation List（CRL; 証明書失効リスト）を表示します。
- **show crypto key mypubkey rsa** — 生成されたすべての暗号鍵ペアを表示します。`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** — IKE 1 トンネル情報を表示します。`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** — IPSec トンネル情報を表示します。

```
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
```

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

発生する可能性のあるエラーを次に示します。

- **ERROR : Failed to parse or verify imported certificate**このエラーが発生する可能性があるのは、ID 証明書をインストールしたけれども、関連付けられたトラストポイントで認証された正しい中間証明書またはルート CA 証明書がない場合です。 正しい中間証明書またはルート CA 証明書を使用して削除と再認証を行う必要があります。 正しい CA 証明書を受け取っていることを確認するには、サードパーティ ベンダーに問い合せてください。
- **Certificate does not contain general purpose public key**このエラーが発生する可能性があるのは、正しくないトラストポイントに ID 証明書をインストールしようとした場合です。 無効な ID 証明書をインストールしようとしているか、トラストポイントと関連付けられた鍵ペアが ID 証明書に含まれている公開鍵と合致しません。 正しいトラストポイントに ID 証明書をインストールしたことを確認するには、**show crypto ca certificates trustpointname** コマンドを使用します。 **Associated Trustpoints** がある行を探します。 正しくないトラストポイントが表示されている場合は、このドキュメントで説明されている手順に従って、トラストポイントを削除して適切なトラストポイントを再インストールします。 また、CSR が生成されてから鍵ペアが変更されていないことを確認します。
- **ERROR : ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:**認証中に証明書の問題が発生した場合に、VPN Client でこのエラーが表示される場合があります。 この問題を解決するには、ASA/PIX 設定で **crypto isakmp identity auto** コマンドを使用します。

関連情報

- Cisco 適応型セキュリティ アプライアンスに関するサポート ページ（英語）
- Cisco VPN Client に関するサポート ページ
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）

- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems