ASA/PIX 8.x： Microsoft CA とデジタル証明書を使用するサイト間の IPSec VPN の認証の設定例

目次

概要

このドキュメントでは、サイト間 VPN の Cisco Security Appliance (ASA/PIX) 8.x 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 Certificate Authority (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。

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。

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。

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 8.0(2) および ASDM バージョン 6.0(2) を実行する Cisco ASA 5510 適応型セキュリティ アプライアンス

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 8.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 RFC 1918 でのアドレスであり、ラボ環境で使用されたものです。

設定

このドキュメントでは、次の設定を使用します。

- Step-by-Step ASA-1 の設定
- ASA-1 の設定の概要

ASA-1 の設定

次の手順を実行して、ASA 上にサード 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：証明書署名要求を生成する
- ステップ 3：トラストポイントを認証する

- ステップ 4：証明書をインストールする
- ステップ 5：新しくインストールした証明書を使用するためのサイト間 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** をクリックし、次に **Device Setup** をクリックします。
2. [System Time] 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は、Date、Time、および Time Zone の値が正確である必要があります。

コマンドラインの例

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

ステップ 2：証明書署名要求を生成する

サード パーティ CA で ID 証明書を発行するには、Certificate Signing Request（CSR; 証明書署名要求）が必要です。 CSR には、ASA の識別名（DN）と生成された公開鍵が含まれています。 ASA は、生成された秘密鍵を使用して、CSR のデジタル署名を行います。

ASDM の手順

1. [Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] にアクセスして [Add] をクリックします。
2. **Add a new identity certificate** オプション ボタンをクリックします。
3. Key Pair で **New** をクリックします。
4. [Enter new key pair name] オプション ボタンをクリックします。 認識できるように、鍵ペアの名前を明確に特定する必要があります。
5. [Generate Now] をクリックします。この時点で鍵ペアが作成されます。
6. **Select** をクリックし、次の表に表示されているアトリビュートを設定して、Certificate Subject DN を定義します。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。**注:** 一部のサード パーティ ベンダーでは、ID 証明書を発行する前に、特定のアトリビュートを追加する必要があります。 必要な属性が明確でない場合は、ベンダーに詳細を問い合せてください。
7. 適切な値を追加したら、**OK** をクリックします。Certificate Subject DN フィールドにデータが入力された状態で、Add Identity Certificate ダイアログ ボックスが表示されます。
8. [Advanced] をクリックします。
9. [FQDN] フィールドに、インターネットからデバイスにアクセスするために使用される 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、次に **Add Certificate** をクリックします。ローカル マシン上のファイルに CSR を保存するプロンプトが表示されます。
11. **[Browse]** をクリックし、CSR を保存する場所を選択し、.txt 拡張子を付けてファイルを保存します。**注:** .txt 拡張子を付けてファイルを保存すると、（メモ帳などの）テキスト エデ

ィタを使用してファイルを開き、PKCS#10 要求を表示できます。

12. 次に示すように、保存した CSR を Microsoft CA などのサードパーティ ベンダーに送信します。VPN サーバ用に提供されたユーザのクレデンシャルを使用して、CA のサーバ 172.16.5.1 への Web ログインを実行します。**注:** CA サーバで、ASA (VPN サーバ) 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。[Request a certificate] > [advanced certificate request] をクリックし、[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 ウィンドウが表示されます。 それを cert_client_id.cer という名前で保存します。これが ASA にインストールされる ID 証明書となります。

コマンドラインの例

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)#
```

ステップ 3：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 証明書を受け取ったら、引き続き次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く Base 64 で符号化された証明書が提供された場合は、Base 64 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、次のように、ファイルのアイコンが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。 サード パーティ ベンダーまたは CA 管理者に問い合せて、ルート CA または中間 CA 証明書を入手してください。
5. [Certificate Path] タブをクリックします。
6. 発行済み ID 証明書に関連付けられた 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、次に示すように 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クレデンシャルを使用して、CA のサーバ 172.16.5.1 への Web ログインを実行します。[Download a CA certificate, certificate chain or CRL] をクリックし、次に示すウィンドウを開きます。 符号化の方式として **Base 64** オプション ボタンをクリックし、**Download CA certificate** をクリックします。CA 証明書を certnew.cer という名前でローカル 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. Base 64 で符号化されたメッセージは、次の図の証明書のようになります。
12. ASDM 内で **Configuration** をクリックし、次に **Device Management** をクリックします。
13. [Certificate Management] を展開し、[CA Certificates] を選択します。
14. [Add] をクリックします。
15. [Paste certificate in PEM Format] オプション ボタンをクリックし、サード パーティ ベンダーにより提供された Base 64 の CA 証明書をテキスト フィールドに貼り付けます。

16. Install Certificate をクリックします。インストールが成功したことを確認するダイアログボックスが表示されます。

コマンドラインの例

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-----
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----- 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)#
```

ステップ 4：証明書をインストールする

ASDM の手順

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

1. **Configuration** をクリックし、次に **Device Management** をクリックします。
2. **Certificate Management** を展開し、**Identity Certificates** を選択します。
3. ステップ 2 で作成した ID 証明書を選択します。**注:** [Expiry Date] には [Pending] と表示されています。
4. [Install] をクリックします。[Paste the certificate data in base-64 format] オプション ボタンをクリックし、サード パーティ ベンダーにより提供された ID 証明書をテキスト フィールドに貼り付けます。
5. **Install Certificate** をクリックします。ダイアログボックスが現れ、インポートが成功であることを確認します。

コマンドラインの例

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)#
```

ステップ 5：新しくインストールした証明書を使用するためのサイト間 VPN（IPSec）を設定する

VPN トンネルを作成するには、次の手順を実行します。

1. ブラウザを開き、**https://<ASDM にアクセスするように設定された ASA のインターフェイスの IP アドレス>** を入力して、ASA 上の ASDM にアクセスします。
2. [Download ASDM Launcher and Start ASDM] をクリックして、ASDM アプリケーションのインストーラをダウンロードします。
3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連のステップを実行し、該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。
4. **http -** コマンドで設定したインターフェイスの IP アドレス、およびユーザ名とパスワード（指定した場合）を入力します。
5. ASDM アプリケーションが ASA に接続したら、[IPsec VPN Wizard] を実行します。
6. IPSec VPN トンネル タイプとして [Site-to-Site] を選択し、次のように [Next] をクリックします。
7. リモート ピアの外部 IP アドレスを指定します。 使用する認証情報（今の場合は事前共有鍵）を入力します。 次の例では、**cisco123** という事前共有鍵を使用しています。 [Tunnel Group Name] は、L2L VPN を設定する場合、デフォルトでは外部 IP アドレスになります。 [Next] をクリックします。
8. IKE（フェーズ 1 ともいう）で使用する属性を指定します。 それらの属性は、ASA および

IOS ルータの両方で同じでなければなりません。 [Next] をクリックします。

9. IPSec（フェーズ 2 ともいう）で使用する属性を指定します。 それらの属性は、ASA および IOS ルータの両方で同じでなければなりません。 [Next] をクリックします。
10. VPN トンネルを通過できるようなトラフィックのホストを指定します。 このステップでは、VPN トンネルに対して [Local Networks] および [Remote Networks] を指定します。 [Local Networks] の横にあるボタンを次の図のようにクリックして、ドロップ ダウン リストからローカル ネットワーク アドレスを選択します。
11. ローカル ネットワーク アドレスを選択し、図のように [OK] をクリックします。
12. [Remote Networks] の横にあるボタンを次の図のようにクリックして、ドロップ ダウン リストからリモート ネットワーク アドレスを選択します。
13. リモート ネットワーク アドレスを選択し、図のように [OK] をクリックします。**注:** リモート ネットワークがリスト内にない場合は、ネットワークをリストに追加する必要があります。 [Add] をクリックします。
14. [Exempt ASA side host/network from address translation] チェック ボックスをオンにします。このようにすると、トンネルのトラフィックに対する **Network Address Translation** は行われません。 [Next] をクリックします。
15. VPN Wizardによって定義された属性が、次の要約画面に表示されます。. 設定を再確認し、設定が正しいことを確認したら [Finish] をクリックします。

ASA-1 の設定の概要

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 の設定

ASA-2 のセキュリティ アプライアンスについても、同様の設定を行います。

確認

ASA では、コマンドラインで各種の show コマンドを発行し、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 コマンド**は、設定されているトラストポイントを表示します。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 コマンド**は、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。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 コマンド**は、キャッシュされている証明書失効リスト（CRL）を表示します。
- **show crypto key mypubkey rsa コマンド**は、生成済みのすべての暗号鍵ペアを表示します。

```
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 コマンド**を使用すると、ピアにおける現在の IKE SA をすべて表示できます。`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 コマンド**を使用すると、ピアにおける現在の IPSec SA をすべて表示できます。`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`

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。

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。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』および『**IP Security のトラブルシューティング：debug コマンドの説明と使用**』を参照してください。

- **debug crypto ipsec 7**：フェーズ 2 の IPSec ネゴシエーションを表示します。**debug crypto isakmp 7**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。

サイト間 VPN のトラブルシューティングの詳細は、『一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について』を参照してください。

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**
- **テクニカルサポートとドキュメント - Cisco Systems**