基本的な IPSec VPN トンネルの構築

次の項では、CLI コマンドと ASDM を使用して LAN 間トンネルおよびリモート アクセス トンネルを作成する方法と、事前共有鍵またはデジタル証明書を使用してそれらを認証する方法について説明します。

- デジタル証明書の登録
- LAN 間トンネルの設定
- リモート アクセス トンネルの設定

（注） ASDM には、完全なオンラインヘルプ システムが付属しています。パネルのフィールド定義を参照する場合は、**Help** をクリックしてください。

この章で使用するコマンドの完全なシンタックスについては、『*Cisco Security Appliance Command Reference*』を参照してください。

デジタル証明書の登録

この項では、CLI コマンドと ASDM を使用してデジタル証明書を登録する方法を説明します。登録が完了すると、その証明書を使用して VPN の LAN 間トンネルおよびリモート アクセス トンネルを認証できます。認証に事前共有鍵だけを使用する場合は、この項を読む必要はありません。

鍵ペア

各ピアには、公開鍵と秘密鍵の両方を含む鍵ペアが 1 つあります。これらの鍵は補完的に動作します。一方の鍵で暗号化された通信は、もう一方の鍵で復号化されます。

鍵ペアは RSA 鍵です。ASA では今後は DSA 鍵をサポートしなくなります。RSA 鍵には次の特性があります。

- RSA 鍵は、セキュリティ アプライアンスへの SSH アクセスまたは SSL アクセスをサポートします。
- SCEP 登録は、RSA 鍵の証明書でサポートされます。
- 鍵の生成が目的の場合、RSA 鍵の最大絶対値は 2048 です。デフォルトのサイズは 1024 ビットです。
- シグニチャ操作の場合、サポートされている鍵の最大サイズは RSA 鍵では 4096 ビットです。
- 生成した*汎用目的の* RSA 鍵ペアは、署名と暗号化の両方に使用できます。*特定用途向けの* RSA 鍵ペアの場合は、それぞれの目的に応じて分かれるため、対応する ID ごとに 2 つの証明書が必要です。デフォルトの設定は、汎用目的です。

証明書に鍵ペアを設定するには、生成する鍵ペアを識別するラベルを指定します。次の項では、CLI を使用してデフォルト ラベル付きの RSA 鍵ペアを生成する方法、ASDM を使用して指定のラベル付きの RSA 鍵ペアを生成する方法、およびその他のパラメータのデフォルト設定を使用する方法を説明します。

コンフィギュレーション手順の概要

CA に登録し、トンネルを認証するための ID 証明書を取得するには、次の手順を実行します。

（注） この例では、自動（SCEP）登録を示します。

1. ID 証明書の RSA 鍵ペアを作成します。
2. トラストポイントを作成します。この例のトラストポイントの名前は newmsroot です。
3. 登録 URL を設定します。この例で使用している URL は、http://10.20.30.40/certsrv/mscep/mscep.dll です。
4. CA を認証します。
5. CA に登録し、ID 証明書を ASA 上に取得します。

CLI コマンドを使用した手順

show crypto key mypubkey RSA コマンドを入力すると、現在実行されている鍵ペアを表示できます。

鍵ペアを生成する CLI コマンドの完全なシンタックスは、次のとおりです。

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*]

たとえば、グローバル コンフィギュレーション モードの場合、デフォルト名 <Default-RSA-Key> を持つ RSA 鍵ペアを生成するには、次のコマンドを入力します。

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

ASDM を使用した手順

ASDM を使用して RSA 鍵ペアを生成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Key Pair** パネルで、**Add** をクリックします。

ステップ 2　**Add Key Pair** ダイアログボックスで情報を設定します。

a. **Name**：デフォルト名を使用する場合はクリックします。または、鍵ペアの名前を入力します。この例では、key1 という名前を使用します。

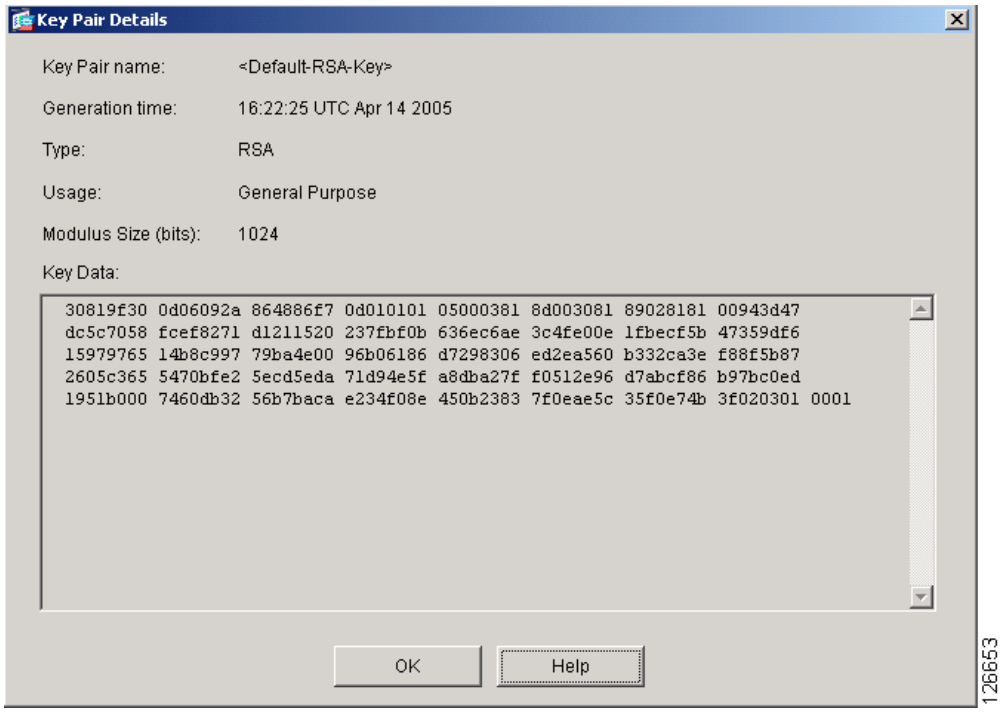
b. **Size** リスト：RSA 鍵ペアの場合、**Size** リストには、オプションとして 512、768、1024、または 2048 が表示されます。デフォルト サイズは 1024 です。この例では、デフォルト設定を受け入れます。

c. **Usage** オプション：Type が RSA の場合だけ使用できます。オプションは、General Purpose（署名および暗号化の両方に 1 つのペアを使用）と Special（機能ごとに 1 つのペアを使用）です。この例では、デフォルト設定（General Purpose）を受け入れます。

ステップ 3　**Generate Now** をクリックします。

ステップ 4　生成された鍵ペアを表示するには、**Show Details** をクリックします。ASDM に、鍵ペアに関する情報が表示されます。図 4-1 に出力例を示します。

図 4-1　鍵ペアの詳細表示



トラストポイントの作成

トラストポイントは CA と ID のペアを表し、CA の ID、CA 固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。トラストポイントを作成するには、使用するインターフェイスの項を参照してください。

CLI コマンドを使用した手順

トラストポイントの作成には、**crypto ca trustpoint** CLI コマンドを使用します。このコマンドを使用すると、config-ca-trustpoint モードに移行し、トラストポイント情報を管理できるようになります。このコマンドの後に必要なコマンドは、2 つのトラストポイント コマンド **enrollment url** および **subject-name** だけです。

次の手順に従って、コマンド例のシンタックスを使用します。

ステップ 1　グローバル コンフィギュレーション モードから config-ca-trustpoint モードに移行して、新しいトラストポイントを作成します。この例では、トラストポイントの名前は newmsroot です。

```
hostname(config)# crypto ca trustpoint newmsroot
```

ステップ 2　自動登録（SCEP）を指定し、このトラストポイントに登録して登録 URL を設定するには、**enrollment url** コマンドを使用します。次に、証明書の認定者（X.500）の名前を指定するために、**subject-name** コマンドを使用します。これが、この証明書を使用するユーザまたはシステムになります。DN フィールドは、グループ マッチングをサポートしていません。この例では、Common Name（CN; 通常名）と Organizational Unit（OU; 組織ユニット）を使用します。

```
hostname(config-ca-trustpoint)# enrollment url
http://10.20.30.40/certsrv/mscep/mscep.dll
hostname(config-ca-trustpoint)# subject-name CN=Pat, OU=Techpubs
```

ステップ 3　（オプション）トラストポイントの設定（デフォルト パラメータと値など）を表示します。

```
hostname(config-ca-trustpoint)# show run all crypto ca trustpoint newmsroot
crypto ca trustpoint newmsroot
 crl nocheck
 enrollment retry period 1
 enrollment retry count 0
 enrollment url http://10.20.30.40/certsrv/mscep/mscep.dll
 fqdn hostname.ciscopix.com
 no email
 subject-name CN=Pat, OU=Techpubs
 serial-number
 no ip-address
 no password
 id-cert-issuer
 accept-subordinates
 support-user-cert-validation
 crl configure
  policy cdp
  cache-time 60
  enforcenextupdate
  protocol http
  protocol ldap
  protocol scep
```

ASDM を使用した手順

ASDM を使用してトラストポイントを作成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Trustpoint > Configuration** パネルで、**Add** をクリックします。

ステップ 2　**Add Trustpoint Configuration** ダイアログボックスで、基本情報を設定します。その他のすべてのパラメータについては、デフォルト値を受け入れます。

a. **Trustpoint Name** ボックス：**Trustpoint Name** ボックスにトラストポイントの名前を入力します。この例では、名前は newmsroot です。

b. **Enrollment URL** ボックス：**Enrollment Settings** パネルの **Enrollment Mode** グループ ボックスで、**Use automatic enrollment** オプションをクリックします。次に、このボックスに登録 URL を入力します。この例では、**10.20.30.40/certsrv/mscep/mscep.dll** と入力します。

ステップ 3　CN と OU の名前を使用して、サブジェクト名を設定します。

a. **Enrollment Settings** パネルの **Key Pair** リストから、このトラストポイントに対して設定した鍵ペアを選択します。この例では、鍵ペアは key1 です。

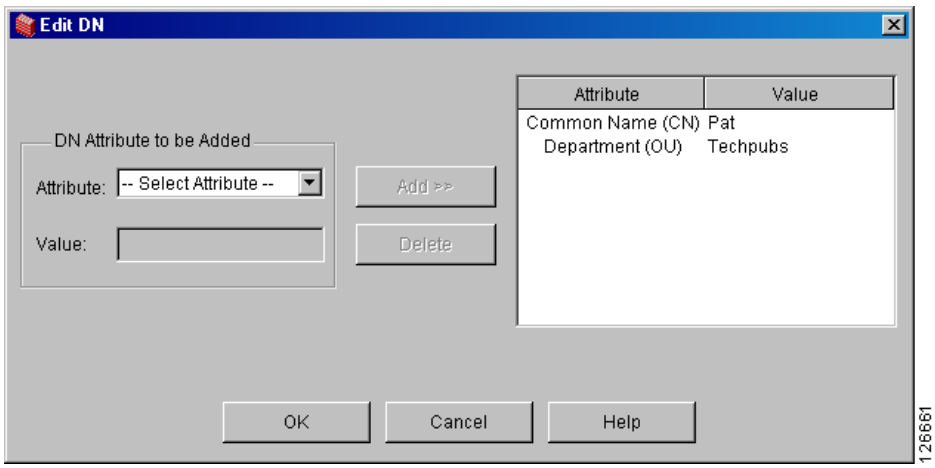
b. **Enrollment Settings** パネルで、**Certificate Parameters** をクリックします。

c. サブジェクト認定者（X.500）の名前の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** をクリックします。

d. **Edit DN** ボックスで、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** ボックスに値を入力します。次に **Add** をクリックします。DN 情報を入力したら **OK** をクリックします。

この例では、まず **Common Name (CN)** を選択し、**Value** ボックスに **Pat** と入力します。次に Add をクリックしてから **Department (OU)** を選択して、**Value** ボックスに **Techpubs** と入力します。図 4-2 は、**Edit DN** ダイアログボックスに入力した内容を示しています。

図 4-2　サブジェクト名のアトリビュートと値



ステップ 4　ダイアログボックスを確認したら **OK** をクリックして、残りの 2 つのダイアログボックスで **OK** をクリックします。

SCEP による証明書の取得

ここでは、SCEP を使用した証明書の設定方法を説明します。自動登録の場合は、設定するトラストポイントごとに手順を繰り返します。各トラストポイントに対する手順が完了すると、ASA は CA 証明書をトラストポイント用に 1 つ、そして署名および暗号化用に 1 つまたは 2 つを受信します。これらの手順を実行しない場合、ASA によって base-64 形式の CA 証明書をテキストボックスに貼り付けるよう求められます。

汎用目的の RSA 鍵を使用する場合、受信した証明書は署名と暗号化を目的としたものです。署名と暗号化に別個の RSA 鍵を使用すると、セキュリティ アプライアンスは目的ごとに別個の証明書を受信します。

CLI コマンドを使用した手順

証明書を取得するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。オプションとして、英数字で構成されたフィンガープリントを ASA に提供し、CA 証明書の認証に使用することもできます。このコマンドを発行すると、対話モードに移行します。証明書のフィンガープリントが表示され、その証明書を受け入れるかどうかを確認するプロンプトが表示されます。この証明書を受け入れるには、**yes**（または **y**）と入力します。

（注） この例では、「フィンガープリント」を使用した証明書の確認方法を示します。ただし、すべての CA でこの確認が必要なわけではありません。

```
hostname(config)# crypto ca authenticate newmsroot
INFO: Certificate has the following attributes:
Fingerprint:     3736ffc2 243ecf05 0c40f2fa 26820675

Do you accept this certificate? [yes/no]: y

Trustpoint 'newmsroot' is a subordinate CA and holds a non self signed cert.
Trustpoint CA certificate accepted.
```

ASDM を使用した手順

ASDM を使用して証明書を取得するには、次の手順を実行します。

ステップ 1　**Configuration >Properties > Certificate > Authentication** パネルに移動します。

ステップ 2　**Trustpoint Name** リストで、トラストポイントの名前を選択します。この例では、**newmsroot** を選択します。

ステップ 3　**Authenticate** をクリックします。

ステップ 4　**Apply** をクリックします。**Authentication Successful** ダイアログが表示されたら、**OK** をクリックします。

認証局への登録

トラストポイントを設定して認証したら、ID 証明書を登録できます。

CLI コマンドを使用した手順

show running-config crypto ca certificates *trustpoint_name* コマンドおよび **show running-config crypto ca trustpoint** *trustpoint_name* コマンドを使用すると、特定のトラストポイントの実行コンフィギュレーションを表示できます。

SCEP 登録のためにトラストポイントを設定した場合、次の例に示すように、ASA に CLI プロンプトが表示され、コンソールにステータス メッセージが表示されます。

登録を開始するには、**crypto ca enroll** コマンドを使用します。シンタックスは、**crypto ca enroll** *trustpoint* [**noconfirm**] です。開始する前に、パスワードを決定してください。

（注）　対話型のプロンプトは、参照されるトラストポイントの設定状態によって異なります。

```
hostname(config)# crypto ca enroll newmsroot
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: v$bx8*c

Re-enter password: v$bx8*c
% The subject name in the certificate will be: CN=Pat, OU=Techpubs
% The fully-qualified domain name in the certificate will be: hostname.ciscopix.com

% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: P3000000098

Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
hostname(config)# The certificate has been granted by CA!
```

これで、CA と ID 証明書の両方を入手できました。

ASDM を使用した手順

ASDM を使用して ID 証明書を登録するには、次の手順を実行します。

ステップ 1　**Configuration >Properties > Certificate > Enrollment** パネルに移動します。

ステップ 2　**Trustpoint Name** リストでトラストポイントを選択します。この例では、**newmsroot** を選択します。

ステップ 3　**Enroll** をクリックします。

ASDM での証明書の管理

証明書を管理するには、**Configuration > Properties > Certificate > Manage Certificates** パネルに移動します。

新しい証明書の追加や証明書の削除には、このパネルを使用します。**Show Details** をクリックすると、証明書に関する情報を表示することもできます。Certificate Details ダイアログには、General、Subject、および Issuer という 3 つのテーブルがあります。

General パネルには、次の情報が表示されます。

- Type：CA、RA、または ID
- Serial number：証明書のシリアル番号
- Status：Available または Pending
  - Available は、CA が登録要求を受け入れて、ID 証明書を発行したことを意味します。
  - Pending は、登録要求が処理中であるため、CA が ID 証明書をまだ発行していないことを意味します。

- Usage：General purpose または Signature
- CRL distribution point (CDP)：証明書を検証するために CRL を取得する URL
- Dates/times within which the certificate is valid：発効日、有効期限

Subject テーブルには、次の情報が表示されます。

- Name：証明書を所有しているユーザまたはエンティティの名前
- Serial number：ASA のシリアル番号
- Distinguished (X.500) name fields for the subject of the certificate：cn、ou、など
- 証明書保有者のホスト名

Issuer テーブルには、証明書を付与したエンティティの認定者名のフィールドが表示されます。

- 通常名（cn）
- 組織ユニットまたは部門（ou）
- 組織（o）
- 地名（l）
- 州（st）
- 国番号（c）
- 発行者の電子メール アドレス（ea）

LAN 間トンネルの設定

ASA とピア デバイスとの間に IPSec LAN 間トンネルを設定する最も容易な方法は、VPN ウィザードを使用することです。このウィザードの使用方法の詳細については、「VPN ウィザードを使用した VPN トンネルの設定」を参照してください。ここでは、ウィザードを実行する前に収集しておく必要のある情報のリストが示されています。

ウィザードを使用しないでトンネルを設定するか、または初期設定の後に変更を行う場合は、この項の手順を使用してください。この項では、CLI と ASDM を使用して LAN 間トンネルを設定する方法を説明します。この項ではさらに、ASA で使用する VPN の用語の一部についても説明します。この用語は、VPN 3000 コンセントレータのものとは異なります。

LAN 間 VPN 接続を構築するには、次のタスクを実行する必要があります。

- インターフェイスの設定
- ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化
- トランスフォーム セットの作成
- ACL の設定
- トンネル グループの定義
- 暗号マップの作成とインターフェイスへの暗号マップの適用
- IPSec トラフィックの許可

設定例

次のコマンドは、LAN 間接続の設定方法を示しています。以降の項では、この接続を設定する方法をステップごとに示します。また、事前共有鍵と証明書を使用した認証方法についても説明します。

```
hostname(config)# interface g0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto isakmp policy 1 authentication pre-share
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)# crypto isakmp policy 1 lifetime 43200
```

（注）　次のコマンドは、1 回だけ実行します。これは、トンネルごとに実行する必要はありません。

```
hostname(config)# crypto isakmp enable outside
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
```

（注）　別のインターフェイスにトンネルを構築するのでない限り、次の 2 つのコマンドは 1 回だけ実行します。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)# sysopt connection permit-vpn
hostname(config)# write mem
```

インターフェイスの設定

ASA には、少なくとも 4 つのインターフェイスがあり、ここではそのうち 2 つを外部インターフェイスと内部インターフェイスと呼びます。通常、外部インターフェイスはパブリック インターネットに接続され、内部インターフェイスはプライベート ネットワークに接続されてパブリック アクセスから保護されます。

ASA で 2 つのインターフェイスを設定およびイネーブル化し、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションとして、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重化操作を設定します（この例では示されていません）。

CLI コマンドを使用した手順

CLI でインターフェイスを設定するには、次の手順を実行します。上記の例のコマンド シンタックスを指針として使用します。

ステップ 1　グローバル コンフィギュレーション モードで、**interface** コマンド、および設定するインターフェイスのデフォルト名を入力します（たとえば g0/0）。この操作により、セッションがインターフェイス コンフィギュレーション モードに移行します。次に例を示します。

```
hostname(config)# interface g0/0
hostname(config-if)#
```

ステップ 2　**ip address** コマンド、およびインターフェイスの IP アドレスとサブネット マスクを入力します。次の例では、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

ステップ 3　インターフェイス名を指定するには、**nameif** コマンドを使用します。最大 48 文字使用できます。この名前は、設定後に変更できません。この例では、g0/0 インターフェイスの名前は outside です。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

ステップ 4　インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** バージョンを使用します。デフォルトでは、インターフェイスはディセーブルです。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ステップ 5　変更内容を保存するには、**write memory** コマンドを使用します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

ステップ 6　2 番目のインターフェイスを設定する場合も、同じ手順を使用します。

ASDM を使用した手順

ASDM がデバイスに送信する CLI コマンドを表示するには、**Options** メニューをクリックし、**Preferences** をクリックして、**Preview commands before sending to the device** を選択します。

ASDM を使用してこの例のインターフェイスを設定するには、次の手順を実行します。

ステップ 1　**Configuration > Interfaces** パネルで、**Add** をクリックします。**Add Interface** ダイアログボックスが開きます。

ステップ 2　**Hardware Port** リストでインターフェイスをクリックします。この例では、**g0/0** を選択します。

ステップ 3　**Enable Interface** をクリックします。

ステップ 4　**Interface Name** ボックスに名前を入力します。この例では、名前は outside です。

ステップ 5　**IP Address** ボックスに IP アドレスを入力します。この例では、IP アドレスは 10.10.4.100 です。

ステップ 6　**Subnet Mask** リストで、サブネット マスクをクリックします。この例では、**255.0.0.0** をクリックします。

ステップ 7　**Use Static IP** をクリックし（この例の場合）、次に **OK** をクリックします。

ステップ 8　コンフィギュレーションを保存するには（定期的に行う必要があります）、ツールバーで **Save** をクリックし、**Yes** をクリックします。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

Internet Security Association and Key Management Protocol（ISAKMP）は IKE とも呼ばれるもので、2 つのホストが IPSec セキュリティ アソシエーションの構築方法について合意するためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 およびフェーズ 2 と呼ばれる 2 つのセクションに分かれています。

フェーズ 1 では、最初のトンネルが作成されます。これは後で ISAKMP ネゴシエーション メッセージを保護します。フェーズ 2 では、データを保護するトンネルが作成されます。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。これには、次が含まれます。

- ピアの ID を保証するための認証方式（事前共有鍵または証明書のいずれか）。
- データを保護し、プライバシーを確保するための暗号化方式。
- メッセージと送信者の ID の整合性を確保するための Hashed Message Authentication Code（HMAC; ハッシュ メッセージ認証コード）方式。
- 暗号鍵を決定するアルゴリズムの強度を確立するための Diffie-Hellman グループ。ASA は、このアルゴリズムを使用して暗号鍵とハッシュ鍵を導出します。
- ASA が置換するタイミングを決定するための暗号鍵の期限満了タイマー。

表 4-1 は、IKE ポリシーのキーワードとそれらの値に関する情報を示しています。

表 4-1　フェーズ 1：CLI コマンドの IKE ポリシー キーワード

コマンド	キーワード	意味	説明
crypto isakmp policy authentication	rsa-sig	RSA シグニチャ アルゴリズムによって生成された鍵を持つデジタル証明書	ASA が各 IPSec ピアの ID を保証するために使用する認証方式を指定します。
	pre-share	事前共有鍵	
crypto isakmp policy encryption	des	56 ビットの DES-CBC	2 つの IPSec ピア間で伝送されるデータを保護する対称暗号アルゴリズムを指定します。デフォルトは 56 ビットの DES-CBC で、これは他のアルゴリズムより安全性は劣りますが高速です。
	3des	168 ビットの Triple DES	
	aes aes-192 aes-256	Advanced Encryption Standard では、128 ビット、192 ビット、および 256 ビットの鍵長をサポートしています。	
crypto isakmp policy hash	sha	SHA-1（HMAC バリアント）	データ整合性を確保するために使用するハッシュ アルゴリズムを指定します。これは、想定した相手から着信したパケットであることと、そのパケットが中継の間に変更されていないことを保証するものです。デフォルトは SHA-1 です。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。
	md5	MD5（HMAC バリアント）	
crypto isakmp policy group	1	グループ 1（768 ビット）	Diffie-Hellman グループ識別子を指定します。2 つの IPSec ピアは、互いに送信を行うことなく、これを使用して共有秘密鍵を導出します。デフォルトは、グループ 2（1024 ビットの Diffie-Hellman）です。
	2	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	
	7	グループ 7（楕円曲線フィールドのサイズは 163 ビット）	
crypto isakmp policy lifetime	整数値	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは、86400 秒（24 時間）です。一般的な規則として、ライフタイムが短い方が（ある程度まで）、より安全な IKE ネゴシエーションになります。ただし、ライフタイムが長い方が、ASA は後の IPSec セキュリティ アソシエーションをよりすばやくセット アップします。

CLI コマンドを使用した手順

show run crypto isakmp コマンドを入力すると、現在実行されている ISAKMP コンフィギュレーションを表示できます。システム応答の「policy」の後ろに *優先順位*が表示されます。それに後続するコマンドでは、関連付けられている IKE ポリシーが一意に識別され、そのポリシーに割り当てられている優先順位が表示されます。これは、1 ～ 65,534 の整数になります。1 は優先順位が最も高く、65,534 が最も低くなります。

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、さまざまな引数を付けて **crypto isakmp policy** コマンドを使用します。isakmp policy コマンドのシンタックスは、次のとおりです。

crypto isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

次の手順を実行します。上記の例のコマンド シンタックスを指針として使用します。

ステップ 1　認証方式を設定します。この例では、認証方式として、RSA シグニチャを指定します。デフォルトの設定は、**pre-share** です。この手順および後続の手順での優先順位は 1 です。

```
hostname(config)# crypto isakmp policy 1 authentication rsa-sig
hostname(config)#
```

ステップ 2　暗号化方式を設定します。この例では、デフォルト設定（**3des**）を示します。

```
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)#
```

ステップ 3　HMAC 方式を設定します。この例では、デフォルト設定（**sha**）を示します。

```
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)#
```

ステップ 4　Diffie-Hellman グループを設定します。この例ではグループ 2 を設定します。

```
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)#
```

ステップ 5　暗号鍵のライフタイムを設定します。この例では、43,200 秒（12 時間）を設定します。デフォルト設定は、**86400** です。

```
hostname(config)# crypto isakmp policy 1 lifetime 43200
hostname(config)#
```

ステップ 6　outside という名前のインターフェイス上で ISAKMP をイネーブルにします（このアトリビュートには、デフォルト設定がありません）。

```
hostname(config)# crypto isakmp enable outside
hostname(config)#
```

ステップ 7　**write mem** コマンドを使用して、変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM で ISAKMP ポリシーを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IKE > Policies** パネルで、**Add** をクリックします。

ステップ 2　上記の例のコンフィギュレーションから情報を入力します。

a. **Priority** ボックスに **1** と入力します。
b. 事前共有鍵の場合、**Authentication** リストで **pre-share** をクリックします。証明書認証の場合、**rsa-sig** をクリックします。
c. **Encryption** リストで **3des** をクリックします。
d. **Hash** リストで **sha** をクリックします。
e. **D-H group** リストで **2** をクリックします。
f. **Lifetime** ボックスに 43200 と入力し、**Lifetime** リストで **Seconds** をクリックします。

ステップ 3　**OK** をクリックします。

ステップ 4　次に、インターフェイスで ISAKMP をイネーブルにします。**Configuration > Features > VPN > IKE > Global Parameters** パネルで、**Enable IKE** グループ ボックス内で対象のインターフェイスをクリックしてから、**Enable** をクリックします。

ステップ 5　**Apply** をクリックします。

トランスフォーム セットの作成

トランスフォーム セットは、暗号化方式と認証方式を組み合せたものです。ISAKMP との IPSec セキュリティ アソシエーションのネゴシエート中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットを複数作成して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。ASA はそのトランスフォーム セットを使用して、暗号マップ エントリのアクセス リストで指定されているデータ フローを保護します。

有効な暗号化方式は次のとおりです。

- esp-des
- esp-3des
- esp-aes（128 ビット暗号化）
- esp-aes-192
- esp-aes-256
- esp-null

有効な認証方式は次のとおりです。

- esp-md5-hmac
- esp-sha-hmac

IPSec はトンネル モードで動作します。これは、パブリック インターネットなど、信頼できないネットワークを介して接続されている 2 つの ASA の間に IPSec を実装する方法です。これにはコンフィギュレーションは必要ありません。

CLI コマンドを使用した手順

show run crypto ipsec コマンドを入力すると、現在実行されているトランスフォーム セットのコンフィギュレーションを表示できます。

CLI を使用してトランスフォーム セットを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。シンタックスは次のとおりです。

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

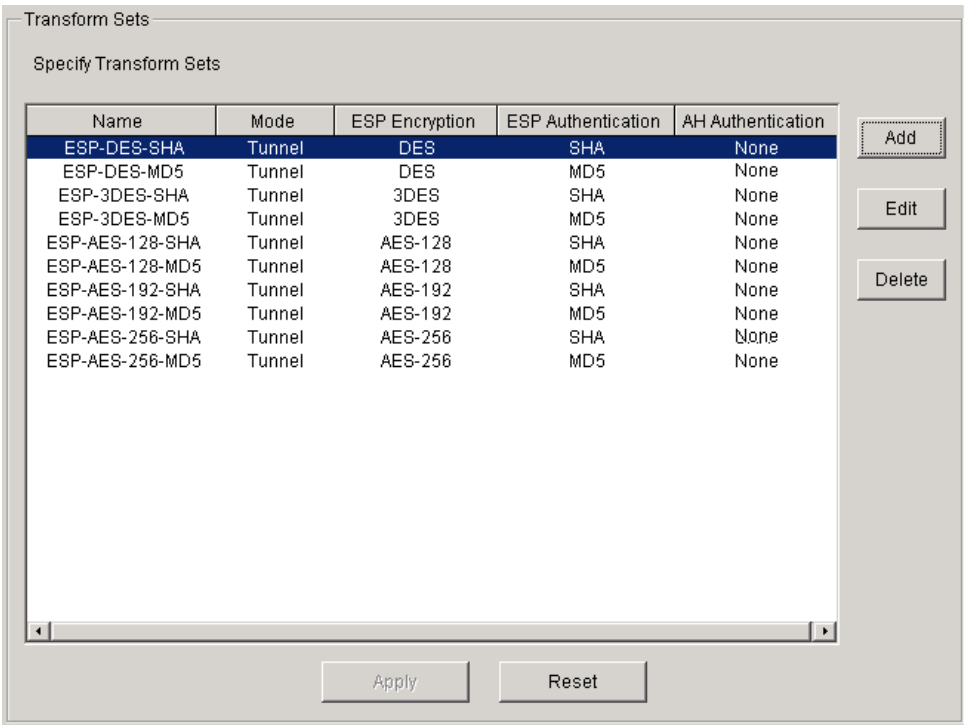
この例では、FirstSet という名前のトランスフォーム セット、esp-3des 暗号化、および esp-md5-hmac 認証を設定しています。

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

ASDM を使用した手順

ASDM には、あらかじめ、標準のトランスフォーム セットがすべて設定されています。ほとんどの場合は、リストにトランスフォーム セットを追加する必要はありません。これらのトランスフォーム セットを表示するには、**Configuration** > **VPN** > **IPSec** > **Transform Sets** パネルに移動します。

図 4-3　Transform Sets テーブル



ACL の設定

ASA は Access Control List（ACL; アクセス コントロール リスト）を使用して、ネットワーク アクセスを制御します。デフォルトでは、ASA はすべてのトラフィックを拒否します。トラフィックを許可する ACL を設定する必要があります。

LAN 間 VPN 用に設定する ACL は、送信元および宛先の IP アドレスに基づいて接続を制御します。接続の両側で互いに反映するように ACL を設定します。

CLI コマンドを使用した手順

ステップ 1　ACL を設定するには、**access-list extended** コマンドを使用します。次の例では、l2l_list という名前の ACL を作成します。この ACL は、IP アドレスが 192.168.0.0 のネットワークから 150.150.0.0 のネットワークへのトラフィックの伝送を許可します。シンタックスは、次のとおりです。**access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

ステップ 2　上に示す ACL が反映される接続のもう一方の側で、ASA 用の ACL を設定します。この例では、ピアのプロンプトは hostname2 で、コマンドによってトラフィックを 150.150.0.0 ネットワークから 192.168.0.0 ネットワークに伝送できるようになります。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname2(config)#
```

ASDM を使用した手順

ASDM を使用して ACL を設定するには、次の手順を実行します。

ステップ 1　**Configuration > Security Policy > Access Rules** パネルで、**Add** をクリックします。

ステップ 2　ほとんどのフィールドで、デフォルトを受け入れることができます。次の情報は入力する必要があります。

- 送信元ホストまたはネットワークの IP アドレスとマスク（たとえば、150.150.0.0/255.255.0.0）。
- 宛先ネットワークの IP アドレスとマスク（たとえば、192.168.0.0/255.255.0.0）。

トンネル グループの定義

トンネル グループとは、トンネル接続ポリシーが含まれたレコードのセットです。トンネル グループを設定して AAA サーバを識別し、接続パラメータを指定して、デフォルトのグループ ポリシーを定義します。ASA はトンネル グループを内部に格納します。

ASA システムには、次の 2 つのデフォルト トンネル グループがあります。

- DefaultRAGroup：デフォルトの IPSec リモート アクセス トンネル グループ
- DefaultL2LGroup：デフォルトの IPSec LAN 間トンネル グループ

これらのグループは変更できますが、削除はできません。また、環境に適応させるため、新しいトンネル グループを 1 つ以上作成できます。トンネル ネゴシエーションの間に特定のトンネル グループが識別されない場合、ASA はこれらの新しいトンネル グループを使用して、リモート アクセスおよび LAN 間のトンネル グループ用にデフォルトのトンネル パラメータを設定します。

基本の LAN 間接続を確立するには、トンネル グループに 2 つのアトリビュートを設定する必要があります。

- 接続タイプを IPSec LAN 間に設定します。
- 認証方式を設定します。この例では、事前共有鍵と証明書の両方のコンフィギュレーションが示されています。

CLI コマンドを使用した手順

show run all tunnel コマンドを入力して、現在実行されているトンネル グループ コンフィギュレーションを表示できます。

次の手順のように、**tunnel-group** コマンドを使用して、接続タイプを IPSec LAN 間に設定します。

ステップ 1　接続タイプを IPSec LAN 間に設定するには、**tunnel-group** コマンドを使用します。シンタックスは、**tunnel-group** *name* ***type*** *type* です。ここで、*name* はトンネル グループに割り当てる名前、*type* はトンネルのタイプです。CLI で入力するトンネル タイプは、次のとおりです。

- ipsec_ra（IPSec リモート アクセス）
- ipsec_l2l（IPSec LAN 間）

この例では、トンネル グループの名前は、LAN 間ピアの IP アドレスである 10.10.4.108 です。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)#
```

ステップ 2　認証方式を設定するには、ipsec-attributes モードに移行し、次に **pre-shared-key** コマンドを使用して事前共有鍵を作成します。この LAN 間接続では、両方の ASA に同一の事前共有鍵を使用する必要があります。証明書認証の場合、**trust-point** コマンドを使用します。

事前共有鍵は、1 ～ 127 文字の英数字文字列です。この例では、事前共有鍵は xyzx です。証明書認証の場合、トラストポイント名を指定します。この例では、newmsroot です。

事前共有鍵認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

また、デジタル証明書認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

ASDM を使用した手順

この例の情報を使用して ASDM でトンネル グループを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > General > Tunnel Group** パネルで、**Add** をクリックします。**Add Tunnel Group** ダイアログボックスが表示されます。これは、VPN 3000 Concentrator Manager の User Management セクションに似ています。

ステップ 2　**Identity** パネルで、**Name** ボックスにトンネル グループの名前を入力し、次に **IPSec for LAN to LAN** オプションをクリックします。この名前には、LAN 間ピアのホスト名または IP アドレス（この例では 10.10.4.108）を使用できます。

ステップ 3　**IPSec** パネルで、事前共有鍵認証の場合は **Pre-shared Key** ボックスに事前共有鍵を入力します。この例では、**xyzx** と入力します。証明書認証の場合、**Trustpoint Name** リストからトラストポイント名（**newmsroot**）を選択します。

暗号マップの作成とインターフェイスへの暗号マップの適用

暗号マップ エントリは、次のような IPSec セキュリティ アソシエーションの各種の要素をまとめたものです。

- IPSec で保護する必要があるトラフィック（アクセス リスト内で定義）
- IPSec によって保護されたトラフィックの送信先（ピアを特定することで指定）
- このトラフィックに適用される IPSec セキュリティ（トランスフォーム セットによって指定）
- IPSec トラフィックのローカル アドレス（インターフェイスに暗号マップを適用することで特定）

IPSec を成功させるには、設定に互換性のある暗号マップ エントリを両方のピアに用意する必要があります。このエントリは、IPSec リモート アクセス（ipsec-ra）または LAN 間（ipsec-l2l）です。2 つの暗号マップ エントリに互換性を持たせるには、少なくとも次の条件を満たす必要があります。

- 暗号マップ エントリに互換性のある暗号アクセス リスト（たとえば、ミラー イメージのアクセス リスト）が含まれている。応答ピアがダイナミック暗号マップを使用している場合、ASA 暗号アクセス リスト内のエントリは、ピアの暗号アクセス リストによって*許可*されている必要があります。
- 暗号マップ エントリはそれぞれ、他のピアを識別する（応答ピアがダイナミック暗号マップを使用していない場合）。
- 各ピアの暗号マップ エントリは、共通のトランスフォーム セットを少なくとも 1 つ持っている。

指定したインターフェイスに複数の暗号マップ エントリを作成する場合、各エントリのシーケンス番号（seq-num）を使用して、順位付けをします。小さいシーケンス番号の方が優先順位は高くなります。暗号マップ セットを持つインターフェイスでは、ASA は優先順位が最も高いマップのエントリから順にトラフィックを評価します。

次の条件のいずれかが存在する場合は、指定のインターフェイスに複数の暗号マップ エントリを作成します。

- 別個のピアが別個のデータ フローを処理する場合。
- 別個の IPSec セキュリティを異なるタイプのトラフィックに適用する場合（同一または別個のピアに対して）。たとえば、あるサブネットのセット間のトラフィックは認証し、別のサブネットのセット間のトラフィックは認証も暗号化も行う場合など。このケースでは、別個のタイプのトラフィックを 2 つの別個のアクセス リストで定義し、それぞれの暗号アクセス リストに別個の暗号マップ エントリを作成します。

CLI コマンドを使用した手順

show run crypto map コマンドを入力すると、現在実行されている暗号マップ コンフィギュレーションを表示できます。

グローバル コンフィギュレーション モードで暗号マップを作成し、その暗号マップを外部インターフェイスに適用するには、いくつかの **crypto map** コマンドを使用します。これらのコマンドではさまざまな引数を使用しますが、シンタックスはすべて **crypto map** *map-name-seq-num* で始まります。このコマンドの例では、マップ名は abcmap、シーケンス番号は 1 です。これらのコマンドをグローバル コンフィギュレーション モードで入力します。

ステップ 1　アクセス リストを暗号マップ エントリに割り当てるには、**crypto map match address** コマンドを使用します。

シンタックスは、**crypto map** *map-name seq-num* **match address** *aclname* です。この例では、マップ名は abcmap、シーケンス番号は 1、アクセス リスト名は xyz です。

```
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)#
```

ステップ 2　IPSec 接続に対してピア（複数可）を指定するには、**crypto map set peer** コマンドを使用します。

シンタックスは、**crypto map** *map-name seq-num* **set peer** {*ip_address1* | *hostname1*}[*... ip_address10* | *hostname10*] です。この例では、ホスト名は 10.10.4.108 です。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

ステップ 3　暗号マップ エントリにトランスフォーム セットを指定するには、**crypto map set transform-set** コマンドを使用します。

シンタックスは、**crypto map** *map-name seq-num* **set transform-set** *transform-set-name* です。この例では、トランスフォーム セットの名前は FirstSet です。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

ASDM を使用した手順

このコンフィギュレーション例の情報を使用して ASDM で暗号マップ機能を設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IPSec > Tunnel Policy** パネルで、**Add** をクリックします。

ステップ 2　インターフェイスとポリシー タイプを選択します。

a. **Interface** リストで **outside** をクリックします。
b. **Policy Type** リストで **Static** をクリックします。

ステップ 3　**Priority** ボックスに、優先順位（1）を入力します。

ステップ 4　**Transform Set to Be Added** リストでトランスフォーム セットをクリックし、**Add** をクリックします。この例では、**ESP-3DES-MD5** をクリックします。

ステップ 5　接続タイプを選択します。LAN 間の場合は、**Connection Type** リストから **Bidirectional** を選択します。

ステップ 6　ピア デバイスの IP アドレスを入力します。接続タイプが双方向の場合は、入力できるピア デバイスは 1 つだけです。**IP Address of Peer to be Added** ボックスに IP アドレス（この例では 192.168.1.1）を入力し、**Add** をクリックします。

インターフェイスへの暗号マップの適用

CLI インターフェイスを使用している場合は、IPSec トラフィックが経由するインターフェイスそれぞれに暗号マップ セットを適用する必要があります。ASA は、すべてのインターフェイスで IPSec をサポートしています。暗号マップ セットをインターフェイスに適用することにより、ASA はすべてのインターフェイス トラフィックを暗号マップ セットと対照させて評価し、接続中またはセキュリティ アソシエーション ネゴシエーション中に、指定されたポリシーを使用します。ASDM は、これらの操作を自動的に実行します。

インターフェイスに暗号マップをバインドすると、セキュリティ アソシエーション データベースやセキュリティ ポリシー データベースなど、実行時のデータ構造も初期化されます。後でどのように暗号マップを変更しても、ASA はその変更内容を実行コンフィギュレーションに自動的に適用します。この場合、既存の接続はドロップされ、新しい暗号マップが適用された後で再度確立されます。

設定済みの暗号マップを外部インターフェイスに適用するには、**crypto map interface** コマンドを使用します。

シンタックスは、**crypto map** *map-name* **interface** *interface-name* です。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

IPSec トラフィックの許可

ASA は、デフォルトで IPSec トラフィックを許可します。

IPSec トラフィックがディセーブルの場合は、**sysopt connection permit-vpn** コマンドを使用して IPSec トラフィックを許可します。これは、IPSec トラフィックを受け入れるために、トンネル型トラフィックがインターフェイス ACL をバイパスすることによって実現されます。これは、復号化されたトラフィックがインターフェイス ACL の対象ではないことを意味します。

CLI コマンドを使用した手順

CLI コマンドを使用する場合は、次のようにして、IPSec トラフィックを許可してから、コンフィギュレーションを保存します。

ステップ 1　グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用し、ASA で IPSec トラフィックを許可します。

```
hostname(config)# sysopt connection permit-vpn
hostname(config)#
```

ステップ 2　変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM では、IPSec トラフィックをイネーブルにしてから、コンフィギュレーションを保存します。次の手順を実行します。

ステップ 1　**Configuration > VPN > General > VPN System Options** パネルに移動します。

ステップ 2　**Enable IPSec authenticated inbound sessions to bypass interface access lists** オプションをクリックします。

ステップ 3　実行コンフィギュレーションをフラッシュ メモリに保存するには、ツールバーで **Save** をクリックし、確認を求められたら **Yes** をクリックします。

リモート アクセス トンネルの設定

リモート アクセス VPN トンネルを構築するには、次の手順を実行します。

- インターフェイスの設定
- ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化
- アドレス プールの設定
- ユーザの追加
- トランスフォーム セットの作成
- トンネル グループの定義
- ダイナミック暗号マップの作成
- ダイナミック暗号マップを使用するための暗号マップ エントリの作成（CLI のみ）
- IPSec トラフィックの許可

設定例の概要

このマニュアルでは、次の設定を使用して、リモート アクセス接続の設定方法を説明します。以降の項では、手順をステップごとに示します。ここでは、事前共有鍵と証明書を使用した認証方法を説明します。

```
hostname(config)# interface g0/0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# # no shutdown
hostname(config)# crypto isakmp policy 1 authentication pre-share
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)# crypto isakmp policy 1 lifetime 43200
hostname(config)# crypto isakmp enable outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# sysopt connection permit-vpn
hostname(config)# write mem
```

インターフェイスの設定

セキュリティ アプライアンスには、少なくとも 2 つのインターフェイスがありますが、このマニュアルではそれらを外部と内部と呼んでいます。通常、外部インターフェイスはパブリック インターネットに接続され、内部インターフェイスはプライベート ネットワークに接続されてパブリック アクセスから保護されます。

まず、ASA で 2 つのインターフェイスを設定してイネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションとして、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重化操作を設定します。

CLI コマンドを使用した手順

インターフェイスを設定するには、次の手順に従って、例に示したコマンド シンタックスを使用します。

（注）　すべてのインターフェイスの設定を表示するには、**show interface** コマンドを入力します。

ステップ 1　インターフェイス コンフィギュレーション モードに移行するには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を使用して **interface** コマンドを実行します。この例では、インターフェイスは g0/0 です。

```
hostname(config)# interface g0/0
hostname(config-if)#
```

ステップ 2　インターフェイスの IP アドレスとサブネット マスクを設定するには、**ip address** コマンドを使用します。この例では、IP アドレスは 10.10.4.200、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)#
```

ステップ 3　インターフェイス名を指定するには、**nameif** コマンドを使用します。最大 48 文字使用できます。この名前は、設定後に変更できません。この例では、g0/0 インターフェイスの名前は outside です。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

（注）　インターフェイスに「outside」という名前を付けた場合、ASA はデフォルト設定の g0/0 と Security Level 0 を割り当てます。インターフェイスに「inside」という名前を付けた場合、ASA はデフォルト設定の g0/1 と Security Level 100 を割り当てます。

ステップ 4　インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** バージョンを使用します。デフォルトでは、インターフェイスはディセーブルです。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ステップ 5　変更内容を保存するには、**write memory** コマンドを使用します。

```
hostname(config-if)# write memory
```

ステップ 6　同じ手順を使用して、2 番目のインターフェイスを設定します。

ASDM を使用した手順

ASDM を使用してこの例のインターフェイスを設定するには、次の手順を実行します。

ステップ 1　**Configuration > Interfaces** パネルで、**Add** をクリックします。**Add Interface** ダイアログボックスが開きます。

ステップ 2　**Hardware Port** リストでインターフェイスをクリックします。この例では、**g0/0** を選択します。

ステップ 3　**Enable Interface** をクリックします。

ステップ 4　**Interface Name** ボックスに名前を入力します。この例では、名前は outside です。

ステップ 5　**IP Address** ボックスに IP アドレスを入力します。この例では、IP アドレスは 10.10.4.200 です。

ステップ 6　**Subnet Mask** リストで、サブネット マスクをクリックします。この例では、サブネット マスクは 255.0.0.0 です。

ステップ 7　**Use Static IP** をクリックし（この例の場合）、次に **OK** をクリックします。

ステップ 8　コンフィギュレーションを保存するには（定期的に行う必要があります）、ツールバーで **Save** をクリックし、**Yes** をクリックします。

ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

ISAKMP は、2 つのホストが IPSec セキュリティ アソシエーションの構築方法について合意するためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 およびフェーズ 2 と呼ばれる 2 つのセクションに分かれています。

フェーズ 1 では、後で ISAKMP ネゴシエーション メッセージを保護する最初のトンネルが作成されます。フェーズ 2 では、データを保護するトンネルが作成されます。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。これには、次が含まれます。

- ピアの ID を保証するための認証方式。

  この項では、事前共有鍵と証明書の両方のコンフィギュレーションについて説明します。
- データを保護し、プライバシーを確保するための暗号化方式。
- 送信者の ID を保証し、また、中継の間にメッセージが変更されていないことを保証するための HMAC 方式。
- 暗号鍵のサイズを設定するための Diffie-Hellman グループ。セキュリティ アプライアンスは、このアルゴリズムを使用して暗号鍵とハッシュ鍵を導出します。
- 暗号鍵の期限満了タイマー。

その他の情報については、この章の LAN 間トンネルに関する項の表 4-1 を参照してください。

CLI コマンドを使用した手順

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、さまざまな引数を付けて **crypto isakmp policy** コマンドを使用します。isakmp policy コマンドのシンタックスは、次のとおりです。

crypto isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

次の手順を実行します。上記の例のコマンド シンタックスを指針として使用します。

ステップ 1　認証方式を設定します。デフォルトの設定は、pre-share です。その他のオプションは、RSA シグニチャを認証方式として使用する **rsa-sig** です。

次に例を示します。

```
hostname(config)# crypto isakmp policy 1 authentication pre-share
hostname(config)#
```

ステップ 2　暗号化方式を設定します。この例では 3DES を設定します。

```
hostname(config)# crypto isakmp policy 1 encryption 3des
hostname(config)#
```

ステップ 3　HMAC 方式を設定します。この例では SHA を設定します。

```
hostname(config)# crypto isakmp policy 1 hash sha
hostname(config)#
```

ステップ 4　Diffie-Hellman グループを設定します。この例ではグループ 2 を設定します。

```
hostname(config)# crypto isakmp policy 1 group 2
hostname(config)#
```

ステップ 5　暗号鍵のライフタイムを設定します。この例では、43,200 秒（12 時間）を設定します。

```
hostname(config)# crypto isakmp policy 1 lifetime 43200
hostname(config)#
```

ステップ 6　outside という名前のインターフェイス上で ISAKMP をイネーブルにします。

```
hostname(config)# crypto isakmp enable outside
hostname(config)#
```

ステップ 7　**write mem** コマンドを使用して、変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM で ISAKMP ポリシーを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IKE > Policies** パネルで、**Add** をクリックします。

ステップ 2　上記の例のコンフィギュレーションから情報を入力します。

a. **Priority** ボックスに **1** と入力します。
b. 事前共有鍵の場合、**Authentication** リストで **pre-share** をクリックします。証明書認証の場合、**rsa-sig** をクリックします。
c. **Encryption** リストで **3des** をクリックします。
d. **Hash** リストで **md5** をクリックします。
e. **D-H group** リストで **2** をクリックします。
f. **Lifetime** ボックスに 43200 と入力し、**Lifetime** リストで **Seconds** をクリックします。

ステップ 3　インターフェイスで ISAKMP をイネーブルにするには、**Configuration > Features > VPN > IKE > Global Parameters** パネルに移動し、**Enable IKE** ボックスで対象のインターフェイスをクリックしてから、**Enable** をクリックします。

アドレス プールの設定

セキュリティ アプライアンスでは、ユーザに IP アドレスを割り当てる方式が必要です。一般的な方式は、アドレス プールを使用するというものです。代替方式として、DHCP サーバでアドレスを割り当てるか、または AAA サーバでアドレスを割り当てることもできます。この例では、アドレス プールを使用します。

CLI コマンドを使用した手順

アドレス プールを設定するとき、VPN クライアントに割り当てられている IP アドレスが標準以外のネットワークに所属する場合は、マスク値を入力する必要があります。デフォルト マスクを使用すると、データが正しくルーティングされない可能性があります。一般的な例は、IP ローカル プールに 10.10.10.0/255.255.255.0 というアドレスが含まれている場合です。これはデフォルトでクラス A ネットワークです。そのため、VPN クライアントが別のインターフェイスを介して 10 ネットワーク内の異なるサブネットにアクセスする必要が生じた場合に、ルーティング上の問題が発生することがあります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 経由で使用可能な一方で、10.10.10.0 ネットワークが VPN トンネル（インターフェイス 1）経由で使用可能である場合、VPN クライアントには、プリンタを宛先とするデータをどこにルーティングするかという混乱が生じます。サブネット 10.10.10.0 と 10.10.100.0 はどちらも 10.0.0.0 クラス A ネットワーク内にあるため、プリンタ データは VPN トンネル経由で送信される可能性があります。

アドレス プールを設定するには、**ip local pool** コマンドを使用します。シンタックスは、**ip local pool** *poolname first_address-last_address* [**mask** *mask*] です。次のコマンド例では、firstpool という名前の IP アドレス プールを設定します。開始アドレスは 10.20.30.40 で、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)#
```

アドレス プール コンフィギュレーションを表示するには、**show running-config ip local pool** コマンドを使用します。

ASDM を使用した手順

ASDM でアドレス プールを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IP Address Management > IP Pools** パネルで、**Add** をクリックします。

ステップ 2　名前、開始 IP アドレス、および終了 IP アドレスを入力します。この例では、次のように入力します。

a. **Name** ボックスに、testpool と入力します。
b. **Start IP** ボックスに、**192.168.0.10** と入力します。
c. **End IP** ボックスに、**192.168.0.15** と入力します。

ステップ 3　**Subnet Mask** リストで、標準ネットワーク マスクの 1 つをクリックします。この例では、**255.255.255.0** をクリックします。

ユーザの追加

ASA にリモート アクセス ユーザを設定するには、ユーザ名とパスワードを指定します。

CLI コマンドを使用した手順

各ユーザ用の内部データベースのエントリを設定するには、**username** コマンドを使用します。シンタックスは、**username** *username* **password** *password* です。この例では、ユーザ名は testuser で、パスワードは 12345678 です。外部認証の設定方法の詳細については、「外部サーバを使用する認証」を参照してください。

```
hostname(config)# username testuser password 12345678
hostname(config)#
```

ASDM を使用した手順

ASDM でユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1　**Configuration > Properties> Device Administration > User Accounts** パネルで、**Add** をクリックします。

ステップ 2　ユーザ名とパスワードを入力し、パスワードを確認します。オプションとして特権レベルを入力します。この例では、次のように入力します。

a. **Identity** パネルで、**User Name** ボックスに **testuser** と入力します。
b. **Password** ボックスに **12345678** と入力します。
c. **Confirm Password** ボックスにパスワードをもう一度入力します。

トランスフォーム セットの作成

トランスフォーム セットは、暗号化方式と認証方式を組み合せたものです。ISAKMP との IPSec セキュリティ アソシエーションのネゴシエート中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

異なるアトリビュートを含むトンネルの組み合せをサポートできるようにトランスフォーム セットを複数設定して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。ASA はそのトランスフォーム セットを使用して、暗号マップ エントリのアクセス リストで指定されているデータ フローを保護します。有効な暗号化方式や認証方式など、その他の情報については、LAN 間トンネルに関する項にある「トランスフォーム セットの作成」を参照してください。

CLI コマンドを使用した手順

トランスフォーム セットを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。シンタックスは次のとおりです。

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

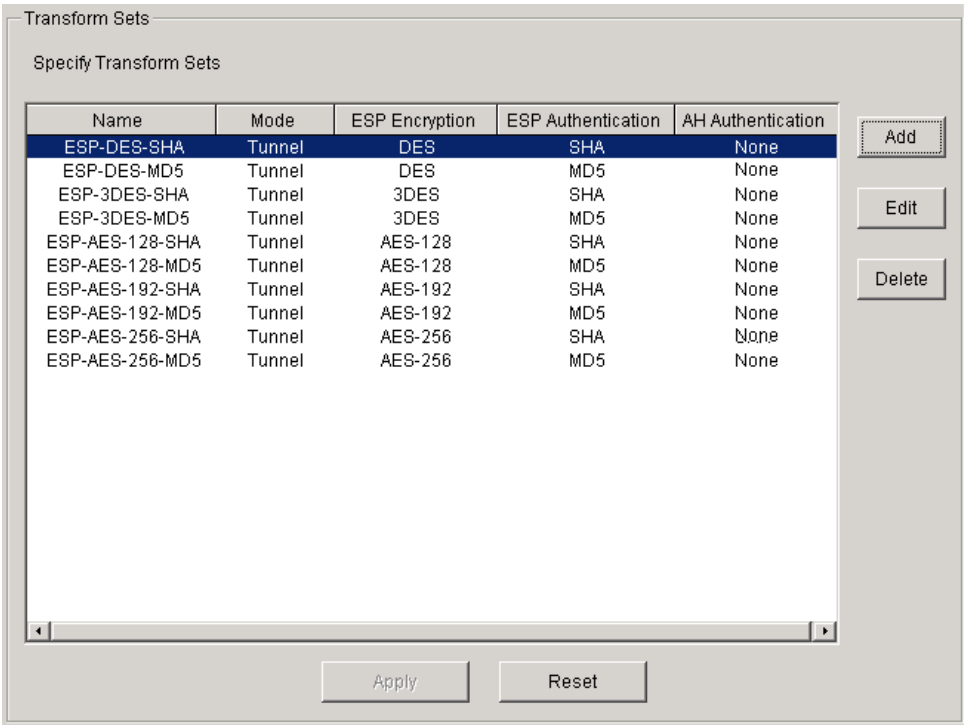
この例では、FirstSet という名前のトランスフォーム セット、esp-3des 暗号化、および esp-md5-hmac 認証を設定しています。

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

ASDM を使用した手順

ASDM には、あらかじめ、標準のトランスフォーム セットがすべて設定されています。ほとんどの場合は、リストにトランスフォーム セットを追加する必要はありません。これらのトランスフォーム セットを表示するには、**Configuration > VPN > IPSec > Transform Sets** パネルに移動します。

図 4-4　Transform Sets テーブル



トンネル グループの定義

トンネル グループとは、トンネル接続ポリシーが含まれたレコードのセットです。トンネル グループを設定して AAA サーバを識別し、接続パラメータを指定して、デフォルトのグループ ポリシーを定義します。ASA はトンネル グループを内部に格納します。

ASA システムには 2 つのデフォルト トンネル グループがあります。DefaultRAGroup（デフォルトの IPSec リモート アクセス トンネル グループ）と、DefaultL2LGroup（デフォルトの IPSec LAN 間トンネル グループ）です。これらを変更することはできますが、削除はできません。トンネル ネゴシエーションの間に特定のトンネル グループが識別されない場合、ASA はこれらのトンネル グループを使用してリモート アクセスおよび LAN 間のトンネル グループ用にデフォルトのトンネル パラメータを設定します。

基本のリモート アクセス接続を確立するには、トンネル グループに 3 つのアトリビュートを設定する必要があります。

- 接続タイプを IPSec_RA（リモート アクセス）に設定します。
- アドレス割り当て方式を設定します。次の手順ではアドレス プールを示します。
- 認証方式を設定します。次の手順では事前共有鍵とデジタル証明書を示します。

CLI コマンドを使用した手順

show run all tunnel コマンドを入力して、現在実行されているトンネル グループ コンフィギュレーションを表示できます。

CLI を使用してトンネル グループを設定するには、次の手順を実行します。

ステップ 1　接続タイプを IPSec リモート アクセスに設定するには、**tunnel-group** コマンドを使用します。コマンド シンタックスは、**tunnel-group** *name* ***type*** *type* です。ここで、*name* はトンネル グループに割り当てる名前、*type* はトンネルのタイプです。CLI で入力するトンネル タイプは、次のとおりです。

- ipsec_ra（IPSec リモート アクセス）
- ipsec_l2l（IPSec LAN 間）

この例では、トンネル グループの名前は testgroup で、タイプは ipsec_ra です。

```
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)#
```

ステップ 2　トンネル グループのアドレス プールを設定するには、一般アトリビュート モードに移行し、次に **address-pool** コマンドを使用してアドレス プールを作成します。この例では、グループの名前は testgroup で、アドレス プールの名前は testpool です。

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
```

ステップ 3　認証方式を設定するには、ipsec-attributes モードに移行し、次に **pre-shared-key** コマンドを使用して事前共有鍵を作成します。このリモート アクセス接続では、両方のデバイスに同一の事前共有鍵を使用する必要があります。証明書認証の場合、**trust-point** コマンドを使用します。

事前共有鍵は、1 ～ 127 文字の英数字文字列です。この例では、事前共有鍵は xyzx です。証明書認証の場合、トラストポイント名を指定します。この例では、newmsroot です。

事前共有鍵認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

デジタル証明書認証の場合、コマンドは次のとおりです。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

ASDM を使用した手順

ASDM を使用してトンネル グループを設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN** > **General** > **Tunnel Group** パネルに移動して、**Add** をクリックします。

ステップ 2　**Identity** パネルで、**Name** ボックスにトンネル グループの名前を入力します。この例では、名前は testgroup です。

ステップ 3　**Type** グループで、**IPSec for Remote Access** オプションをクリックします。

ステップ 4　**Client Address Assignment** パネルの **Address Pool** グループから、追加済みのアドレス プールを選択して、**Add** をクリックします。

ステップ 5　**IPSec** パネルで、事前共有鍵認証の場合は **Pre-shared Key** ボックスに事前共有鍵を入力します。この例では、事前共有鍵は xyzx です。証明書認証の場合は、**Trustpoint Name** リストからトラストポイント名を選択します。この例では、名前は newmsroot です。

ダイナミック暗号マップの作成

ASA では、ダイナミック暗号マップを使用してポリシー テンプレートを定義します。これらのダイナミック暗号マップを使用すると、ASA は IP アドレスが不明な場合でもピアから接続を受信できます。リモートアクセス クライアントは、このカテゴリに入ります。

ダイナミック暗号マップ エントリは、接続のトランスフォーム セットを識別します。また、Reverse Route Injection（RRI）をイネーブルにすると、ASA は接続クライアントのルーティング情報を取得できます。ASA は RIP または OSPF 経由でこの情報をアドバタイズする必要があります。アドレスをすべての方式（AAA、IP プール、および DHCP プロキシ）から取得するクライアントについては、ASA は設定済みのルートを通知します。他のアドレス割り当て方式の場合、ASA はグローバル イネーブル / ディセーブル フラグを使用して、クライアント ルートのアドバタイズメントを決定します。

CLI コマンドを使用した手順

show run all crypto dynamic-map コマンドを入力すると、現在実行されている暗号ダイナミック マップ コンフィギュレーションを表示できます。

このコンフィギュレーション例の情報を使用して CLI でダイナミック暗号マップ機能を設定するには、次の手順を実行します。

ステップ 1　ダイナミック暗号マップ エントリのトランスフォーム セットを指定するには、次のコマンド シンタックスを使用します。

crypto dynamic -map *dynamic-map-name seq-num* **set transform-set** *transform-set-name*

次の例では、ダイナミック マップの名前は dyn1、シーケンス番号は 1、トランスフォーム セットの名前は FirstSet です。

```
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)#
```

ステップ 2　この暗号マップ エントリに基づく任意の接続に対して RRI をイネーブルにするには、次のように **crypto dynamic-map set reverse route** コマンドを使用します。

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)#
```

ステップ 3　変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

このコンフィギュレーション例の情報を使用して ASDM でダイナミック暗号マップ機能を設定するには、次の手順を実行します。

ステップ 1　**Configuration > VPN > IPSec > Tunnel Policy** パネルで、**Add** をクリックします。

ステップ 2　**Interface** ボックスでインターフェイスをクリックします。この例では、**outside** をクリックします。

ステップ 3　**Policy Type** ボックスで **dynamic** をクリックします。

ASDM は、インターフェイスとポリシー タイプを組み合せてダイナミック マップの名前を付けます。この例では、暗号ダイナミック マップの名前は dyn1 になります。

ステップ 4　**Priority** ボックスに、優先順位（**1**）を入力します。

ステップ 5　**Transform Set to Be Added** リストでトランスフォーム セットをクリックし、**Add** をクリックします。この例では、**ESP-3DES-MD5** をクリックします。

ステップ 6　**Advanced** をクリックします。

ステップ 7　**Enable Reverse Route Injection** オプションをクリックします。

ステップ 8　**OK** をクリックして、**Tunnel Policy Advanced Settings** ダイアログボックスを閉じ、次にもう一度 **OK** をクリックして **Add Tunnel Policy** ダイアログボックスを閉じます。

ステップ 9　**Apply** をクリックします。

図 4-5 は、トンネル ポリシー コンフィギュレーションによって生成された CLI コマンドを示しています。暗号ダイナミック マップ dyn1 を参照する暗号マップ コマンドを ASDM が生成していることに注意してください。

図 4-5　トンネル ポリシー

```
crypto dynamic-map outside_dyn_map 1 set transform-set ESP-3DES-MD5
crypto dynamic-map outside_dyn_map 1 set security-association lifetime seconds 28800 kilobyte
crypto dynamic-map outside_dyn_map 1 set nat-t-disable
crypto dynamic-map outside_dyn_map 1 set reverse-route
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
```

ダイナミック暗号マップを使用するための暗号マップ エントリの作成（CLI のみ）

CLI を使用している場合、ASA がダイナミック暗号マップを使用して IPSec セキュリティ アソシエーションのパラメータを設定できるように、暗号マップ エントリを作成する必要があります。

（注）　ASDM を使用している場合は、ダイナミック暗号マップを使用するための暗号マップを作成する必要はありません。ASDM は暗号マップを自動的に作成します。

このコマンド例では、前の項「ダイナミック暗号マップの作成」で作成したのと同様、暗号マップの名前は mymap、シーケンス番号は 1、ダイナミック暗号マップの名前は dyn1 になります。これらのコマンドをグローバル コンフィギュレーション モードで入力します。

ステップ 1　ダイナミック暗号マップを使用する暗号マップ エントリを作成するには、**crypto map** コマンドを使用します。シンタックスは、**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* です。

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)#
```

ステップ 2　暗号マップを外部インターフェイスに適用するには、**crypto map interface** コマンドを使用します。

シンタックスは、**crypto map** *map-name* **interface** *interface-name* です。

```
hostname(config)# crypto map mymap interface outside
hostname(config)#
```

IPSec トラフィックの許可

ASA は、デフォルトで IPSec トラフィックを許可します。

IPSec トラフィックがディセーブルの場合は、**sysopt connection permit-vpn** コマンドを使用して IPSec トラフィックを許可します。これは、IPSec トラフィックを受け入れるために、トンネル型トラフィックがインターフェイス ACL をバイパスすることによって実現されます。これは、復号化されたトラフィックがインターフェイス ACL の対象ではないことを意味します。

CLI コマンドを使用した手順

CLI コマンドを使用する場合は、次のようにして、IPSec トラフィックを許可してから、コンフィギュレーションを保存します。

ステップ 1　グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用し、ASA で IPSec トラフィックを許可します。

```
hostname(config)# sysopt connection permit-vpn
hostname(config)#
```

ステップ 2　変更内容を保存します。

```
hostname(config)# write mem
hostname(config)#
```

ASDM を使用した手順

ASDM では、IPSec トラフィックをイネーブルにしてから、コンフィギュレーションを保存します。次の手順を実行します。

ステップ 1　**Configuration > VPN > General > VPN System Options** パネルに移動します。

ステップ 2　**Enable IPSec authenticated inbound sessions to bypass interface access lists** オプションをクリックします。

ステップ 3　実行コンフィギュレーションをフラッシュ メモリに保存するには、ツールバーで **Save** をクリックし、確認を求められたら **Yes** をクリックします。