



LAN-to-LAN IPsec VPN の設定

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。

2つのピアの内部および外部ネットワークが IPv4 の場合（内部および外部インターフェイス上のアドレスが IPv4 の場合）、ASA で、シスコまたはサードパーティのピアとの LAN-to-LAN VPN 接続がサポートされます。

IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 アドレッシングの LAN-to-LAN 接続については、両方のピアが ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、および両方の内部ネットワークのアドレッシング方式が一致している場合（両方が IPv4 または両方が IPv6 の場合）は、セキュリティ アプライアンスで VPN トンネルがサポートされます。

具体的には、両方のピアが ASA 5500 シリーズの場合、次のトポロジがサポートされます。

- ASA の内部ネットワークが IPv4 で、外部ネットワークが IPv6（内部インターフェイス上のアドレスが IPv4 で、外部インターフェイス上のアドレスが IPv6）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv4（内部インターフェイス上のアドレスが IPv6 で、外部インターフェイス上のアドレスが IPv4）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv6（内部および外部インターフェイス上のアドレスが IPv6）



(注) ASA は、シスコのピアや、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続をサポートしています。

この章では、LAN-to-LAN VPN 接続の構築方法について説明します。内容は次のとおりです。

- 「[コンフィギュレーションのまとめ](#)」 (P.10-2)
- 「[マルチコンテキスト モードでのサイトツーサイト VPN の設定](#)」 (P.10-2)
- 「[インターフェイスの設定](#)」 (P.10-3)
- 「[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](#)」 (P.10-4)
- 「[IKEv1 トランスフォーム セットの作成](#)」 (P.10-6)
- 「[IKEv2 プロポーザルの作成](#)」 (P.10-7)
- 「[ACL の設定](#)」 (P.10-8)
- 「[トンネル グループの定義](#)」 (P.10-8)
- 「[クリプト マップの作成とインターフェイスへの適用](#)」 (P.10-10)

コンフィギュレーションのまとめ

ここでは、この章で説明するサンプルの LAN-to-LAN コンフィギュレーションの概要を説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0/0
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 ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list 121_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-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfX
hostname(config)# crypto map abcmap 1 match address 121_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

マルチコンテキスト モードでのサイトツーサイト VPN の設定

5505 を除くすべてのプラットフォームについて、マルチモードのサイトツーサイト サポートを許可するには、次の手順に従います。これらの手順を実行して、リソース割り当てがどのように分解されるのかを確認できます。

- ステップ 1** マルチモードの VPN を設定し、リソース クラスを設定し、許可されたリソースの一部として VPN ライセンスを選択します。一般的な操作のコンフィギュレーション ガイドの“[Configuring a Class for Resource Management](#)” section on page 5-16 でこれらの設定手順について説明しています。
- ステップ 2** コンテキストを設定し、VPN ライセンスを許可する設定したクラスのメンバーにします。一般的な操作のコンフィギュレーション ガイドの“[Configuring a Security Context](#)” section on page 5-19 でこれらの設定手順について説明しています。
- ステップ 3** [Configuration] > [Site-to-Site VPN] > [Connection Profiles] の順に進みます。
- ステップ 4** コンテキスト設定およびサイトツーサイト VPN タブで、サイトツーサイト VPN のシングル コンテキスト VPN 設定と同様に、接続プロファイル、ポリシー、クリプトマップなどを設定します。

メイン ホーム パネルには、VPN セッション数を表示するサマリー パネルがあります。[Details] をクリックすると、VPN トンネルの詳細ビューが表示されます。

インターフェイスの設定

ASA には、少なくとも 2 つのインターフェイスがあり、これらをここでは外部と内部と言います。一般に、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ます。一方、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、一般のアクセスから保護されます。

最初に、ASA の 2 つのインターフェイスを設定し、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。オプションで、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操作を設定します。



(注) ASA の外部インターフェイス アドレス (IPv4 と IPv6 の両方) は、プライベート側のアドレス空間と重複してはなりません。

インターフェイスを設定するには、例に示すコマンド構文を使用して、次の手順を実行します。

- ステップ 1** インターフェイス コンフィギュレーション モードに入るには、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指定して **interface** コマンドを入力します。次の例で、インターフェイスは **ethernet0** です。
- ```
hostname(config)# interface ethernet0/0
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** コマンドを入力します。次の例で、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** インターフェイスに名前を付けるには、**nameif** コマンドを入力します。最大 48 文字です。この名前は、設定した後での変更はできません。次の例で、ethernet0 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** 形式を入力します。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** 変更を保存するには、**write memory** コマンドを入力します。
- ```
hostname(config-if)# write memory
hostname(config-if)#
```
- ステップ 6** 同じ手順で、2 番目のインターフェイスを設定します。

# 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 台のホストで IPsec Security Association (SA; セキュリティ アソシエーション) の構築方法を一致させるためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。これには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。ISAKMP のネゴシエーションは 2 つのフェーズ (フェーズ 1 とフェーズ 2) に分かれています。フェーズ 1 は、以後の 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を作成します。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。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー (PSK) です。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code (HMAC) 方式。
- 暗号キー決定アルゴリズムの強度を決定するデフィーヘルマン グループ。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。
- IKEv2 では、別個の Pseudo-Random Function (PRF; 疑似乱数関数) をアルゴリズムとして使用して、IKEv2 トンネルの暗号化などに必要なキー関連情報とハッシュ操作を取得していました。
- この暗号キーを使用する時間の上限。この時間が経過すると ASA は暗号キーを置き換えます。

IKEv1 ポリシーを使用して、パラメータごとに 1 つの値を設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

ここでは、IKEv1 および IKEv2 ポリシーを作成して、インターフェイスでイネーブルにする手順について説明します。

- 「IKEv1 接続の ISAKMP ポリシーの設定」 (P.10-4)
- 「IKEv2 接続の ISAKMP ポリシーの設定」 (P.10-5)

## IKEv1 接続の ISAKMP ポリシーの設定

IKEv1 接続の ISAKMP ポリシーを設定するには、`crypto ikev1 policy priority` コマンドを使用して IKEv1 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv1 のパラメータを設定できます。

次の手順を実行し、ガイドとして次の例で示すコマンド構文を使用します。

- ステップ 1** IPsec IKEv1 ポリシー コンフィギュレーション モードを開始します。たとえば、次のように入力します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

- ステップ 2** 認証方式を設定します。次の例では、事前共有キーを設定します。

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

- ステップ 3** 暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)#
```

- ステップ 4** HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

- ステップ 5** Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)#
```

- ステップ 6** 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

- ステップ 7** シングル コンテキスト モードまたはマルチ コンテキスト モードで、**outside** というインターフェイス上の IKEv1 をイネーブルにします。

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

- ステップ 8** 変更を保存するには、**write memory** コマンドを入力します。

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

## IKEv2 接続の ISAKMP ポリシーの設定

IKEv2 接続の ISAKMP ポリシーを設定するには、**crypto ikev2 policy priority** コマンドを使用して IKEv2 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv2 のパラメータを設定できます。

次の操作を行ってください。

- ステップ 1** IPsec IKEv2 ポリシー コンフィギュレーション モードを開始します。たとえば、次のように入力します。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

- ステップ 2** 暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)#
```

## ■ IKEv1 トランスフォーム セットの作成

**ステップ 3** Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)#
```

**ステップ 4** アルゴリズムとして使用する疑似乱数関数 (PRF) を設定し、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得します。次の例では、SHA-1 (HMAC バリエーション) を設定します。

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

**ステップ 5** 暗号キーのライフタイムを設定します。次の例では、43,200 秒 (12 時間) に設定します。

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

**ステップ 6** outside というインターフェイス上の IKEv2 をイネーブルにします。

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

**ステップ 7** 変更を保存するには、**write memory** コマンドを入力します。

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

## IKEv1 トランスフォーム セットの作成

IKEv1 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わせたものです。特定のデータフローを保護する場合、ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエーション中に、特定のトランスフォーム セットを使用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 セットにより、関連付けられたクリプト マップ エントリで指定された ACL のデータフローが保護されます。ASA 設定でトランスフォーム セットを作成して、クリプト マップまたはダイナミック クリプト マップ エントリでトランスフォーム セットの最大数 11 を指定できます。

表 10-1 に、有効な暗号化方式と認証方式を示します。

表 10-1 有効な暗号化方式と認証方式

| 有効な暗号化方式             | 有効な認証方式              |
|----------------------|----------------------|
| esp-des              | esp-md5-hmac         |
| esp-3des (デフォルト)     | esp-sha-hmac (デフォルト) |
| esp-aes (128 ビット暗号化) |                      |
| esp-aes-192          |                      |
| esp-aes-256          |                      |
| esp-null             |                      |

パブリック インターネットなどの非信頼ネットワークを介して接続された 2 つの ASA 間で IPsec を実装する通常の方法は、トンネル モードです。トンネル モードはデフォルトであり、設定は必要ありません。

トランスフォーム セットを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のサイト間タスクを実行します。

- 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、**crypto ipsec ikev1 transform-set** コマンドを入力します。次の例では、名前が **FirstSet** で、暗号化と認証にそれぞれ **esp-3des** と **esp-md5-hmac** を使用するトランスフォーム セットを設定しています。構文は次のようになります。

```
crypto ipsec ikev1 transform-set transform-set-name encryption-method authentication-method
```

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

- ステップ 2** 変更を保存します。

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

## IKEv2 プロポーザルの作成

IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

表 10-2 に、有効な IKEv2 暗号化方式と整合性方式を示します。

表 10-2 有効な IKEv2 暗号化方式と整合性方式

| 有効な暗号化方式     | 有効な整合性方式    |
|--------------|-------------|
| des          | sha (デフォルト) |
| 3des (デフォルト) | md5         |
| aes          |             |
| aes-192      |             |
| aes-256      |             |

IKEv2 プロポーザルを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のタスクを実行します。

- 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 **crypto ipsec ikev2 ipsec-proposal** コマンドを使用して、プロポーザルの複数の暗号化および整合性タイプを指定できる IPSec プロポーザル コンフィギュレーション モードを開始します。この例では、プロポーザルの名前は **secure** です。

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```

- ステップ 2** 次に、プロトコルおよび暗号化タイプを入力します。サポートされている唯一のプロトコルは ESP です。たとえば、次のように入力します。

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)#
```

- ステップ 3** 整合性タイプを入力します。たとえば、次のように入力します。

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

ステップ 4 変更を保存します。

## ACL の設定

ASA は、アクセス コントロール リストを使用してネットワーク アクセスをコントロールします。デフォルトでは、適応型セキュリティ アプライアンス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。詳細については、一般的な操作のコンフィギュレーション ガイドの [Chapter 18, “Information About Access Control Lists,”](#) を参照してください。

この LAN-to-LAN VPN 制御接続で設定する ACL は、送信元 IP アドレスと変換された宛先 IP アドレスに基づいています。接続の両側に、互いにミラーリングする ACL を設定します。

VPN トラフィック用の ACL は、変換アドレスを使用します。詳細については、一般的な操作のコンフィギュレーション ガイドの [“IP Addresses Used for ACLs When You Use NAT” section on page 18-3](#) を参照してください。

ACL を設定するには、次の手順を実行します。

ステップ 1 **access-list extended** コマンドを入力します。次の例では、192.168.0.0 のネットワーク内にある IP アドレスから 150.150.0.0 のネットワークにトラフィックを送信する、l2l\_list という名前の ACL を設定します。構文は、**access-list listname extended permit ip source-ipaddress source-netmask destination-ipaddress destination-netmask** です。

```
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 接続のもう一方の側の ASA に、ACL をミラーリングする ACL を設定します。次の例では、該当ピアのプロンプトは hostname2 です。

```
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)#
```



(注) vpn-filter を使用した ACL の設定方法の詳細については、「[リモートアクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルール](#)」(P.4-49) を参照してください。

## トンネル グループの定義

トンネル グループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバを識別するトンネル グループを設定し、接続パラメータを指定し、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 グループを内部的に保存します。

ASA には、2 つのデフォルト トンネル グループがあります。1 つはデフォルトの IPsec リモート アクセス トンネル グループである DefaultRAGroup で、もう 1 つはデフォルトの IPsec LAN-to-LAN トンネル グループである DefaultL2Lgroup です。これらは変更可能ですが、削除はできません。

IKE バージョン 1 および 2 の主な相違点は、使用できる認証方式にあります。IKEv1 では、両方の VPN エンドで 1 つのタイプの認証のみが許可されます (つまり、事前共有キーまたは証明書)。しかし、IKEv2 では、別のローカルおよびリモート認証 CLI を使用して非対称認証方式を設定できます



(つまり、送信元に対しては事前共有キー認証を設定し、応答側に対しては証明書認証を設定できません)。したがって、IKEv2 では、一方があるクレデンシャルを使用して認証し、他方が別のクレデンシャルを使用する非対称認証となります (事前共有キーまたは証明書)。

また、環境に合った新しいトンネル グループを 1 つ以上作成することもできます。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、ASA は、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

基本的な LAN-to-LAN 接続を確立するには、次のように 2 つの属性をトンネル グループに設定する必要があります。

- 接続タイプを IPsec LAN-to-LAN に設定します。
- IP の認証方式を設定します。次の例では、IKEv1 および IKEv2 に事前共有キーを設定します。



(注) トンネル グループなどの VPN を使用するには、ASA はシングル ルーテッド モードでなければなりません。トンネルグループ パラメータを設定するためのコマンドは、他のどのモードにも表示されません。

**ステップ 1** 接続タイプを IPsec LAN-to-LAN に設定するには、**tunnel-group** コマンドを入力します。構文は、**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であり、*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。

- **remote-access** (IPsec、SSL、およびクライアントレス SSL リモート アクセス)
- **ipsec-l2l** (IPsec LAN-to-LAN)

次の例では、トンネル グループの名前は、LAN-to-LAN 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)#
```



(注) IP アドレス以外の名前が付いている LAN-to-LAN トンネル グループは、トンネル認証方式がデジタル証明書である、またはピアが Aggressive モードを使用するように設定されている (あるいはその両方) の場合に限り使用できます。

**ステップ 2** 認証方式を事前共有キーに設定するには、ipsec 属性モードに入り、**ikev1 pre-shared-key** コマンドを入力して事前共有キーを作成します。この LAN-to-LAN 接続の両方の ASA で、同じ事前共有キーを使用する必要があります。

キーは、1 ~ 128 文字の英数字文字列です。

次の例で、IKEv1 事前共有キーは 44kkaol59636jnfxf です。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfxf
```

次の例で、IKEv2 事前共有キーも 44kkaol59636jnfxf に設定されています。

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfxf
```



(注) **ikev2 remote-authentication pre-shared-key** または証明書を設定して、認証を完了する必要があります。

**ステップ 3** 変更を保存します。

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

```
hostname(config)#
```

トンネルが稼働中であることを確認するには、**show vpn-sessiondb summary**、**show vpn-sessiondb detail l2l**、または **show cry ipsec sa** コマンドを使用します。

## クリプト マップの作成とインターフェイスへの適用

クリプト マップ エントリは、IPsec セキュリティ アソシエーションの次のような各種要素をまとめたものです。

- IPsec で保護する必要のあるトラフィック (ACL で定義)
- IPsec で保護されたトラフィックの送信先 (ピアで指定)
- 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 セットで指定)
- 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クリプト マップを適用して指定)

IPsec が成功するためには、両方のピアに互換性のあるコンフィギュレーションを持つクリプト マップ エントリが存在する必要があります。2 つのクリプト マップ エントリが互換性を持つためには、両者が少なくとも次の基準を満たす必要があります。

- クリプト マップ エントリに、互換性を持つ暗号 ACL (たとえば、ミラー イメージ ACL) が含まれている。応答するピアがダイナミック クリプト マップを使用している場合は、ASA の暗号 ACL のエントリがピアの暗号 ACL によって「許可」されている必要があります。
- 各クリプト マップ エントリが他のピアを識別する (応答するピアがダイナミック クリプト マップを使用していない場合)。
- クリプト マップ エントリに、共通のトランスフォーム セットが少なくとも 1 つ存在する。

所定のインターフェイスに対して複数のクリプト マップ エントリを作成する場合は、各エントリのシーケンス番号 (seq-num) を使用して、エントリにランクを付けます。seq-num が小さいほど、プライオリティが高くなります。クリプト マップ セットを持つインターフェイスでは、ASA はまずトラフィックをプライオリティの高いマップ エントリと照合して評価します。

次の条件のいずれかに当てはまる場合は、所定のインターフェイスに対して複数のクリプト マップ エントリを作成します。

- 複数のピアで異なるデータ フローを処理する場合。
- 異なるタイプのトラフィック (同一または個別のピアへの) に異なる IPsec セキュリティを適用する場合。たとえば、あるサブネット セット間のトラフィックは認証し、別のサブネット セット間のトラフィックは認証および暗号化するような場合です。この場合は、異なるタイプのトラフィックを 2 つの個別の ACL で定義し、各暗号 ACL に対して個別にクリプト マップ エントリを作成します。

クリプト マップを作成して **outside** インターフェイスに適用するには、グローバル コンフィギュレーション モードで、シングル コンテキスト モードまたはマルチ コンテキスト モードで次の手順を実行します。

**ステップ 1** ACL をクリプト マップ エントリに割り当てるには、**crypto map match address** コマンドを入力します。

構文は、**crypto map map-name seq-num match address aclname** です。次の例では、マップ名は **abcmap**、シーケンス番号は **1**、ACL 名は **l2l\_list** です。

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

**ステップ 2** IPsec 接続用のピアを指定するには、**crypto map set peer** コマンドを入力します。

構文は、**crypto map map-name seq-num set peer {ip\_address1 | hostname1} [... ip\_address10 | hostname10]** です。次の例では、ピア名は 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** クリプト マップ エントリに IKEv1 トランスフォーム セットを指定するには、**crypto map ikev1 set transform-set** コマンドを入力します。

構文は、**crypto map map-name seq-num ikev1 set transform-set transform-set-name** です。次の例では、トランスフォーム セット名は *FirstSet* です。

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

**ステップ 4** クリプト マップ エントリに IKEv2 プロポーザルを指定するには、**crypto map ikev2 set ipsec-proposal** コマンドを入力します。

構文は、**crypto map map-name seq-num set ikev2 ipsec-proposal proposal-name** です。次の例では、プロポーザル名は *secure* です。

**crypto map** コマンドでは、1 つのマップ インデックスに複数の IPsec プロポーザルを指定できます。この場合、複数のプロポーザルがネゴシエーションの一部として IKEv2 ピアに送信され、プロポーザルの順序はクリプト マップ エントリの順序付け時に管理者が決定します。



**(注)** 連結モード (AES-GCM/GMAC) および通常モード (その他すべて) のアルゴリズムが IPsec プロポーザルにある場合、ピアに単一のプロポーザルを送信できません。この場合、2 つのプロポーザルが必要となります (連結モードのアルゴリズムに 1 つ、通常モードのアルゴリズムに 1 つ)。

```
hostname (config) # crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname (config) #
```

## クリプト マップのインターフェイスへの適用

クリプト マップ セットは、IPsec トラフィックが通過する各インターフェイスに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 をサポートします。クリプト マップ セットをインターフェイスに適用すると、ASA はすべてのインターフェイス トラフィックをクリプト マップ セットと照合して評価し、接続時やセキュリティ アソシエーションのネゴシエーション時に、指定されたポリシーを使用します。

また、クリプト マップをインターフェイスにバインドすると、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 データベースなどのランタイム データ構造も初期化されます。クリプト マップを後から変更すると、ASA は自動的にその変更を実行コンフィギュレーションに適用します。既存の接続はすべてドロップされ、新しいクリプト マップの適用後に再確立されます。

設定済みのクリプト マップを *outside* インターフェイスに適用するには、次の手順を実行します。

**ステップ 1** **crypto map interface** コマンドを入力します。構文は、**crypto map map-name interface interface-name** です。

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

**ステップ 2** 変更を保存します。

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

---