IPsec および ISAKMP

トンネリング、IPsec、および ISAKMP について

このトピックでは、バーチャルプライベートネットワーク（VPN）の構築に使用するインターネットプロトコルセキュリティ（IPsec）標準と Internet Security Association and Key Management Protocol（ISAKMP）標準について説明します。

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモートユーザとプライベートな企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

ASA は、ISAKMP と IPsec のトンネリング標準を使用してトンネルの構築と管理を行っています。ISAKMP と IPsec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション
- トンネルの確立
- ユーザとデータの認証
- セキュリティ キーの管理
- データの暗号化と復号化
- トンネル経由のデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、双方向のトンネル エンドポイントとして機能します。プライベート ネットワークからプレーン パケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネ

ルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリック ネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

IPsec の概要

ASA では、LAN-to-LAN VPN 接続に IPsec が使用され、client-to-LAN VPN 接続に IPsec を使用することもできます。IPsec 用語では、ピアとは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。どちらの接続タイプについても、ASA はシスコのピアだけをサポートします。シスコは VPN の業界標準に従っているので、ASA は他ベンダーのピアとの組み合わせでも動作しますが、シスコはこのことをサポートしていません。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションをネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

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。IPsec LAN-to-LAN 接続では、ASA は発信側または応答側として機能することができます。IPsec client-to-LAN 接続では、ASA は応答側としてのみ機能します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

IPsec トンネルの概要

IPsec トンネルとは、ASA がピア間に確立する SA のセットのことです。SA とは、機密データに適用するプロトコルとアルゴリズムを指定するものであり、ピアが使用するキー関連情報も指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

ピアは SA ごとに使用する設定をネゴシエートします。各 SA は次のもので構成されます。

- IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル
- クリプト マップ
- ACL
- トンネル グループ
- 事前フラグメンテーション ポリシー

ISAKMP および IKE の概要

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。このセキュリティ アソシエーションには、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。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。
- IKEv2 の場合は、別の疑似乱数関数（PRF）。IKEv2 トンネル暗号化などに必要な、キー関連情報とハッシュ操作を導出するためのアルゴリズムとして使用されます。
- ASA が暗号キーを使用する時間の制限。この時間が経過すると暗号キーを置き換えます。

IKEv1 ポリシーでは、各パラメータに対して 1 個の値を設定します。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。この並べ替えにより、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。

ASA は、IKEv2 の複数のセキュリティ アソシエーション（SA）をサポートしていません。ASA は現在、検出された最初の SA でのみインバウンド IPsec トラフィックを受け入れます。IPsec トラフィックが他の SA で受信された場合は、`vpn-overlap-conflict` のためドロップされます。複数の IPsec SA は 2 つのピア間の重複トンネル、または非対称トンネリングからの情報を取得できます。

IKEv1 トランスフォーム セットおよび IKEv2 プロポーザルの概要

IKEv1 トランスフォーム セットや IKEv2 プロポーザルは、ASA によるデータ保護の方法を定義するセキュリティ プロトコルとアルゴリズムの組み合わせです。IPsec SA のネゴシエート時に、ピアはそれぞれトランスフォーム セットまたはプロポーザルを指定しますが、これは両ピアで同一であることが必要です。ASA は、この一致しているトランスフォーム セットまたはプロポーザルを使用して SA を作成し、この SA によって暗号マップに対する ACL のデータフローが保護されます。

IKEv1 トランスフォーム セットでは、各パラメータに対して 1 個の値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに対して、複数の暗号化および認証のタイプ、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個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

SA の作成に使用されたトランスフォーム セットまたはプロポーザルの定義が変更された場合は、ASA はトンネルを切断します。詳細については、セキュリティ アソシエーションのクリア （49 ページ） を参照してください。

（注） トランスフォーム セットまたはプロポーザルの唯一の要素が消去または削除された場合は、ASA はそのトランスフォーム セットまたはプロポーザルを参照する暗号マップを自動的に削除します。

IPsec VPN のライセンス

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイト間 VPN では、基本ライセンスに付属の Other VPN ライセンスが使用されます。モデルごとの最大値については、「Cisco ASA Series Feature Licenses」を参照してください。

IPsec VPN のガイドライン

コンテキスト モードのガイドライン

シングルまたはマルチ コンテキスト モードでサポートされます。Anyconnect Apex ライセンスは、マルチコンテキスト モードのリモートアクセス VPN に必要です。ASA は AnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用 AnyConnect、Cisco VPN フォン用 AnyConnect、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フェールオーバーのガイドライン

IPsec VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。

その他のガイドライン

IKE を設定すると、システムは自動的に RADIUS UDP ポート 1645 および 1646 を予約します。この予約は syslog 713903 に記載され、ポート番号は 27910 および 28166 として示されます。この予約により、ポートが PAT 変換に使用されないように確保されます。

ISAKMP の設定

IKEv1 ポリシーと IKEv2 ポリシーの設定

IKEv1 と IKEv2 はどちらも、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

IKE ネゴシエーションが始まると、ネゴシエーションを開始したピアはそのすべてのポリシーをリモート ピアに送信し、リモート ピアは一致するポリシーを探します。リモート ピアは、一致するポリシーを見つけるまで、設定済みのポリシーに対してピアのすべてのポリシーを 1 つずつプライオリティ順に（最も高いプライオリティから）照合します。

一致と見なされるのは、2 つのピアからの両方のポリシーに、同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータ値が含まれているときです。IKEv1 では、リモート ピアのポリシーで指定されているライフタイムが、開始側から送信されたポリシーのライフタイム以下であることも必要です。ライフタイムが等しくない場合、ASA は短い方のライフタイムを使用します。IKEv2 では、ライフタイムはネゴシエートされませんが、各ピアの間でローカルに管理されるので、ライフタイムを各ピアで個別に設定できます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、SA は確立されません。

各パラメータに対して特定の値を選択するときは、セキュリティとパフォーマンスの間に暗黙のトレードオフが発生します。デフォルト値で得られるセキュリティ レベルは、ほとんどの組織のセキュリティ要件に十分に対応します。パラメータに対し 1 つの値だけをサポートしているピアと相互運用する場合は、相手のピアがサポートしている値に選択が制限されます。

ISAKMP コマンドには、それぞれプライオリティを指定する必要があります。プライオリティ番号によってポリシーが一意に識別され、IKE ネゴシエーションにおけるポリシーのプライオリティが決定されます。

手順

ステップ 1 IKE ポリシーを作成するには、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーション モードで **crypto***ikev1* | *ikev2* policy コマンドを入力します。プロンプトは、IKE ポリシー コンフィギュレーション モードを表示します。

例：

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

（注） 新しい ASA コンフィギュレーションには、デフォルトの IKEv1 や IKEv2 のポリシーはありません。

ステップ 2 暗号化アルゴリズムを指定します。デフォルトはトリプル DES です。

encryption[aes | aes-192 | aes-256 | des | 3des]

例：

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

ステップ 3 ハッシュ アルゴリズムを指定します。デフォルト値は SHA-1 です。

hash [md5 | **sha]**

例：

```
hostname(config-ikev1-policy)# hash md5
```

ステップ 4 認証方式を指定します。デフォルトは事前共有キーです。

authentication[**pre-shared**]**rsa-sig**]

例：

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

ステップ 5 Diffie-Hellman グループ識別番号を指定します。デフォルトはグループ 2 です。

group[**2** | **5**]

例：

```
hostname(config-ikev1-policy)# group 5
```

ステップ 6 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。

lifetime *seconds*

例：

この例では、4 時間（14400 秒）のライフタイムを設定します。

```
hostname(config-ikev1-policy)# lifetime 14400
```

ステップ 7 IKEv1 ポリシー キーワード、IKEv2 ポリシー キーワード、および IKE ポリシー キーワードと値 （7 ページ） で入力した値を使用して追加設定を指定します。所定のポリシー パラメータに値を指定しない場合、デフォルト値が適用されます。

IKE ポリシー キーワードと値

	キーワード	意味	説明
authentication	**rsa-sig**	RSA 署名アルゴリズムによって生成されたキー付きのデジタル証明書	各 IPSec ピアの ID を確立するために ASA が使用する認証方式を指定します。
	pre-share **(デフォルト)**	事前共有キー	事前共有キーは拡大するネットワークに対応して拡張が困難ですが、小規模ネットワークではセットアップが容易です。
encryption	**des** **3des**（デフォルト）	56 ビット DES-CBC 168 ビット Triple DES	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。
hash	**sha**（デフォルト）	SHA-1（HMAC バリアント）	データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。

	キーワード	意味	説明
group	**1**	グループ 1（768 ビット）	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。 Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 AES は、VPN-3DES のライセンスがあるセキュリティアプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman（DH）のグループ 5 を使用する必要があります。
	2（デフォルト）	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	
lifetime	**整数値** （86400 = デフォルト）	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA による IPsec SA のセットアップ機能が高速になります。

	キーワード	意味	説明
integrity	sha（デフォルト）	SHA-1（HMACバリアント）	データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。MD5 に対する攻撃の成功例がありますが（これは非常に困難ですが）、IKEが使用する HMAC バリアントがこの攻撃を防ぎます。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	null		AES-GCM が暗号化アルゴリズムとして指定されているときは、IKEv2整合性アルゴリズムとしてヌルを選択できます。
encryption	des 3des（デフォルト）	56 ビット DES-CBC 168 ビット Triple DES	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。

	キーワード	意味	説明
	aes aes-192 aes-256		Advanced Encryption Standard（AES）は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
	aes-gcm aes-gcm-192 aes-gcm-256 null	IKEv2 暗号化に使用する AES-GCM アルゴリズムのオプション	Advanced Encryption Standard（AES）は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
policy_index			IKEv2 ポリシー サブモードにアクセスします。
prf	sha（デフォルト）	SHA-1（HMAC バリアント）	疑似乱数関数（PRF）を指定します。これは、キー関連情報を生成するために使用されるアルゴリズムです。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
priority			ポリシー モードを拡張します。追加の IPsec V3 機能がサポートされ、AES-GCM および ECDH の設定が Suite B サポートに含まれるようになります。

	キーワード	意味	説明
group	**1**	グループ 1（768 ビット）	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。 Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 AnyConnect クライアントは、非 FIPS モードで DH グループ 1、2、および 5 をサポートし、FIPS モードではグループ 2 だけをサポートします。 AES は、VPN-3DES のライセンスがあるセキュリティアプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman（DH）のグループ 5 を使用する必要があります。
	2（デフォルト）	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	
	14 19 20 21 24		
lifetime	**整数値** （86400 = デフォルト）	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA による IPsec SA のセットアップ機能が高速になります。

外部インターフェイスでの IKE のイネーブル化

VPN トンネルの終端となるインターフェイスで、IKE をイネーブルにする必要があります。通常は外部（つまり、パブリック）インターフェイスです。IKEv1 または IKEv2 を有効にするには、crypto [**ikev1** | **ikev2**] **enable***interface-name* コマンドを、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーション モードで実行します。

次に例を示します。

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

IKEv1 アグレッシブ モードのディセーブル化

フェーズ 1 の IKEv1 ネゴシエーションでは、メイン モードとアグレッシブ モードのどちらも使用できます。どちらのモードも同じサービスを提供しますが、アグレッシブ モードではピア間の交換が 2 回だけ必要で、合計 3 メッセージとなります（交換が 3 回で、合計 6 メッセージではありません）。Agressive モードの方が高速ですが、通信パーティの ID は保護されません。このため、セキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。アグレッシブ モードは、デフォルトでイネーブルになっています。

（注） アグレッシブ モードをディセーブルにすると、Cisco VPN Client は、ASA へのトンネルを確立するための事前共有キー認証を使用できなくなります。ただし、証明書に基づく認証（つまり ASA または RSA）を使用してトンネルを確立できます。

アグレッシブ モードをディセーブルにするには、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

```
hostname(config)# crypto ikev1 am-disable
```

アグレッシブ モードをいったんディセーブルにした後でイネーブルに戻すには、このコマンドの no 形式を使用します。次に例を示します。

```
hostname(config)#  no crypto ikev1 am-disable
```

IKEv1 および IKEv2 ISAKMP ピアの識別方式の決定

IKEv1 または IKEv2 ISAKMP フェーズ I ネゴシエーションでは、ピアが相互に相手を識別する必要があります。この識別方式は、次のオプションから選択できます。

Address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。

Automatic （デフォルト）	接続タイプによって ISAKMP ネゴシエーションが決まります。 • 事前共有キーの IP アドレス • 証明書認証の証明書認定者名
Hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
Key ID *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

ASA は、ピアに送信するフェーズ I の ID を使用します。これは、事前共有キーで認証を行うメイン モードでの LAN-to-LAN IKEv1 接続を除いて、すべての VPN シナリオで行われます。

ピア識別方式を変更するには、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

crypto isakmp identity {*address* | *hostname* | **key-id** *id-string* | **auto**}

たとえば、次のコマンドはピア識別方式を「ホスト名」に設定します。

```
hostname(config)# crypto isakmp identity hostname
```

INVALID_SELECTORS 通知

IPsec システムが SA 上で着信パケットを受信し、そのパケットのヘッダー フィールドが SA 用のセレクタに適合しなかった場合は、そのパケットを廃棄する必要があります。このイベントの監査ログ エントリには、現在の日時、SPI、IPsec プロトコル、パケットの送信元と宛先、その他の入手可能なパケットのベクトル値、および関連 SA エントリのセレクタ値が含まれます。システムは、セレクタ チェックに合格しなかったために受信パケットが破棄されたことを示す INVALID_SELECTORS の IKE 通知を生成して、送信元（IPsec ピア）に送信します。

ASA は、次に示す既存の syslog を使用して、CTM 内にこのイベントのロギングを実装しています。

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
 the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

管理者は、SA 用のトラフィック セレクタと一致しない着信パケットが SA 上で受信された場合に、ピアへの IKEv2 通知の送信を有効または無効にできるようになりました。有効にした場

合は、IKEv2 通知メッセージが 5 秒ごとに SA あたり 1 つの通知メッセージに制限されます。IKEv2 通知は、IKEv2 情報交換でピアに送信されます。

16 進数の IKEv2 事前共有キーの設定

ローカルとリモートの両方の事前共有キー コマンドにキーワードの *hex* を追加することによって、16 進数の IKEv2 事前共有キーを設定することができます。

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

IKE 通知の送信の有効化または無効化

管理者は、IKEv2 IPsec VPN 接続上でその接続用のトラフィック セレクタと一致しない着信パケットが受信された場合に、ピアへの IKE 通知の送信を有効または無効にすることができます。この通知の送信はデフォルトで無効になっています。ASDM 証明書でユーザ名を認可する場合の IKE INVALID_SELECTORS 通知の送信は、次の CLI を使用して有効または無効にします。

[**no**] **crypto ikev2 notify invalid-selectors**

証明書認証の実行時は、証明書内の CN がユーザ名であり、認可がローカル サーバに対して実行されます。"service-type" 属性が取得された場合は、前述のように処理されます。

IKEv2 フラグメンテーション オプションの設定

ASA では、IKEv2 フラグメンテーションをイネーブルまたはディセーブルにすることができ、IKEv2 パケットのフラグメント化で使用する MTU（最大伝送ユニット）を指定できます。また、管理者は次のコマンドを使用して、優先するフラグメンテーション方式を設定できます。

[**no**] **crypto ikev2 fragmentation** [**mtu** <*mtu-size*>] | [**preferred-method** [**ietf** | **cisco**]]

デフォルトでは、すべての IKEv2 フラグメンテーション方式がイネーブルになり、MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）、優先される方式は IETF 標準 RFC-7383 となります。

次の点を考慮して、[**mtu** <*mtu-size*>] を指定してください。

- 使用する MTU 値には、IP（IPv4/IPv6）ヘッダー + UDP ヘッダーのサイズを含める必要があります。
- 管理者によって指定されていない場合、デフォルトの MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）となります。
- 指定すると、同じ MTU が IPv4 と IPv6 の両方で使用されます。
- 有効範囲は 68 ～ 1500 です。

（注） MTU の設定時に ESP オーバーヘッドを考慮する必要があります。暗号化中に MTU に追加される ESP オーバーヘッドにより、暗号化後にパケットサイズが増加します。「packet too big」エラーが表示された場合は、MTU サイズを確認し、より低い MTU を設定してください。

次のサポートされているフラグメンテーション方式のいずれかを、IKEv2 の優先フラグメンテーション方式 [**preferred-method**[**ietf** | **cisco**]] として設定できます。

- IETF RFC-7383 標準ベースの IKEv2 フラグメンテーション。
  - この方式は、両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
  - この方式を使用すると、フラグメンテーションの後に暗号化が実行され、各 IKEv2 フラグメント メッセージが個別に保護されます。
- シスコ独自のフラグメンテーション。
  - この方式は、これが AnyConnect クライアントなどのピアによって提供される唯一の方法である場合、または両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
  - この方式を使用すると、暗号化の後にフラグメンテーションが実行されます。受信側のピアは、すべてのフラグメントを受信するまで、メッセージを復号することも認証することもできません。
  - この方式は、シスコ以外のピアとの相互運用性はありません。

show running-config crypto ikev2 コマンドは現在の設定を表示し、**show crypto ikev2 sa detail** コマンドは、SA に対してフラグメンテーションが使用された場合に符号化された MTU を表示します。

始める前に

- パス MTU ディスカバリはサポートされていません。MTU は、ネットワークのニーズに合わせて手動で設定する必要があります。
- この設定はグローバルであり、設定の適用後に確立される SA に影響を及ぼします。適用以前の SA は影響を受けません。フラグメンテーションがディセーブルになっている場合でも同様です。
- 最大 100 のフラグメントを受信できます。

例

- IKEv2 フラグメンテーションをディセーブルにする場合：

```
no crypto ikev2 fragmentation
```

- デフォルト動作に戻す場合：

```
crypto ikev2 fragmentation
```

または

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- MTU の値を 600 に変更する場合：

```
crypto ikev2 fragmentation mtu 600
```

- デフォルトの MTU 値に戻す場合：

```
 no crypto ikev2 fragmentation mtu 576
```

- 優先するフラグメンテーション方式をシスコ方式に変更する場合：

```
crypto ikev2 fragmentation preferred-method cisco
```

- 優先するフラグメンテーション方式を IETF に戻す場合：

```
no crypto ikev2 fragmentation preferred-method cisco
```

または

```
 crypto ikev2 fragmentation preferred-method ietf
```

AAA 認証と認可

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

AAA 認証は、ユーザが入力したユーザ名とパスワードを使用して、ローカル サーバに対して実行されます。追加の認証は、同じユーザ名を使用して、*radius* サーバに対して実行されます。*service-type* 属性を取得した場合、すでに説明したように処理されます。

IPsec over NAT-T のイネーブル化

NAT-T を使用すると、IPsec ピアは NAT デバイスを介した接続を確立できます。このことを実現するために、IPsec トラフィックが UDP データグラムとしてカプセル化されます。これにはポート 4500 が使用されるので、これによって、NAT デバイスにポート情報が提供されます。NAT-T は NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。

（注） AnyConnect クライアントの制限により、AnyConnect クライアントが IKEv2 を使用して接続できるようにするには NAT-T のイネーブル化が必要になります。この要件は、クライアントが NAT-T デバイスの背後になくても適用されます。

ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-T、および IPSec over UDP を同時にサポートできます。

各オプションがイネーブルのときの接続の状態を次に示します。

オプション	イネーブルの機能	クライアントの位置	使用する機能
オプション 1	NAT-T がイネーブル	およびクライアントが NAT の背後にある場合は、	NAT-T が使用される
		および NAT が存在しない場合は	ネイティブ IPsec（ESP）が使用される
オプション 2	IPsec over UDP がイネーブル	およびクライアントが NAT の背後にある場合は、	IPsec over UDP が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される
オプション 3	NAT-T と IPsec over UDP の両方がイネーブル	およびクライアントが NAT の背後にある場合は、	NAT-T が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される

（注） IPsec over TCP がイネーブルになっている場合は、その他のすべての接続方式よりも優先されます。

NAT-T をイネーブルにすると、ASA は自動的に、IPsec がイネーブルになっているすべてのインターフェイス上でポート 4500 を開きます。

ASA は、LAN-to-LAN とリモート アクセス ネットワークの両方ではなく、どちらかで動作する単一の NAT/PAT デバイスの背後に設置された複数の IPsec ピアをサポートします。混合環境では、リモート アクセス トンネルのネゴシエーションに失敗します。これは、すべてのピアが同じパブリック IP アドレス、つまり NAT デバイスのアドレスから発信されたように見えるためです。また、リモート アクセス トンネルは、LAN-to-LAN トンネル グループ（つまり NAT デバイスの IP アドレス）と同じ名前を使用することが多いため、混合環境では失敗します。この名前の一致により、NAT デバイスの背後にあるピアの LAN-to-LAN とリモート アクセスの混合ネットワークでは、複数のピア間のネゴシエーションが失敗する場合があります。

NAT-T を使用するには、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手順を実行します。

手順

ステップ 1 次のコマンドを入力して、ASA 上でグローバルに IPsec over NAT-T をイネーブルにします。

crypto isakmp nat-traversal *natkeepalive*

natkeepalive 引数の範囲は 10 ～ 3600 秒です。デフォルトは 20 秒です。

例：

次のコマンドを入力して、NAT-T をイネーブルにし、キープアライブ値を 1 時間に設定します。

```
hostname(config)# crypto isakmp nat-traversal 3600
```

ステップ 2 IPsec フラグメンテーション ポリシーに対して暗号化前オプションを選択するために、次のコマンドを入力します。

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。

IPsec with IKEv1 over TCP のイネーブル化

IPsec over TCP は、IKEv1 と IPsec の両方のプロトコルを TCP に似たパケットの中にカプセル化するものであり、NAT と PAT の両方のデバイスとファイアウォールを通過するセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。IPsec/IKEv1 over TCP を使用すると、標準の ESP や IKEv1 が機能できない環境や、既存のファイアウォール ルールを変更した場合に限って機能できる環境で、Cisco VPN クライアントが動作できるようになります。

（注） この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモート アクセス クライアントで動作します。ASA とその接続先クライアントの両方で IPsec over TCP をイネーブルにします。ASA では、すべての IKEv1 対応インターフェイス上で動作するようにグローバルにイネーブルにされます。LAN-to-LAN 接続では機能しません。

ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-Traversal、および IPSec over UDP を同時にサポートできます。IPsec over TCP は、イネーブルになっている場合、その他のすべての接続方式よりも優先されます。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などの周知のポートを入力すると、そのポートに関連付けられているプロトコルがパブリック インターフェイスで機能しなくなることを示すアラートが表示されます。その結果、パブリック インターフェイスを介して ASA を管理するためにブラウザを使用することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

デフォルトのポートは 10000 です。

ASA だけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、ASA 用に設定したポートを少なくとも 1 つ含める必要があります。

IKEv1 の IPsec over TCP を ASA でグローバルにイネーブルにするには、次のコマンドをシングルまたはマルチ コンテキスト モードで実行します。

crypto ikev1 ipsec-over-tcp [port *port 1...port0]*

次の例では、IPsec over TCP をポート 45 でイネーブルにしています。

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

IKEv1 の証明書グループ照合の設定

トンネル グループは、ユーザの接続条件とアクセス権を定義します。証明書グループ照合では、ユーザ証明書のサブジェクト DN または発行者 DN を使用して、ユーザとトンネル グループを照合します。

（注） 証明書グループ照合は IKEv1 と IKEv2 LAN-to-LAN 接続だけに適用されます。IKEv2 リモートアクセス接続は、トンネルグループの webvpn 属性および certificate-group-map の webvpn コンフィギュレーション モードなどに設定されるグループ選択のプルダウンをサポートしています。

証明書のこれらのフィールドに基づいてユーザをトンネル グループと照合するには、まず照合基準を定義したルールを作成し、次に各ルールを目的のトンネル グループに関連付ける必要があります。

証明書マップを作成するには、**use the crypto ca certificate map**コマンドを使用します。トンネル グループを定義するには、tunnel-group コマンドを使用します。

また、証明書グループ照合ポリシーも設定する必要があります。これには、ルールからグループを照合する、Organizational Unit (OU) フィールドからグループを照合する、すべての証明書ユーザにデフォルトのグループを使用する、という方式があります。これらの方式のいずれかまたはすべてを使用できます。

手順

ステップ 1 証明書ベースの ISAKMP セッションをトンネル グループにマッピングするためのポリシーとルールを設定し、証明書マップエントリをトンネル グループに関連付けるには、tunnel-group-map コマンドをシングルまたはマルチ コンテキスト モードで入力します。

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

ポリシー	証明書からトンネル グループ名を取得するためのポリシーを指定します。policyは次のいずれかです。 *ike-id*：トンネル グループがルール ルックアップに基づいて特定されず、OUからも取得されない場合に、証明書ベースのISAKMPセッションをフェーズ 1 ISAKMP ID の内容に基づいてトンネル グループにマッピングすることを示します。 *ou*：トンネル グループをルール検索によって決定しない場合、サブジェクト識別名（DN）の OU の値を使用することを示します。 *peer-ip*：トンネル グループをルール検索によって決定しない場合やOU またはike-id 方式で取得しない場合、ピアの IP アドレスを使用することを示します。 *rules*：証明書ベースのISAKMPセッションが、このコマンドによって設定された証明書マップの関連付けに基づいて、トンネル グループにマッピングされることを示します。
rule index	（オプション）**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

次のことに注意してください。

- 各呼び出しが一意であり、マップインデックスを2回以上参照しない限り、このコマンドを複数回実行できます。
- ルールは 255 文字以下です。
- 1 つのグループに複数のルールを割り当てられます。複数のルールを割り当てるには、まずルールのプライオリティを追加し、グループ化します。次に、各グループに必要な数だけ基準文を定義します。1 つのグループに複数のルールを割り当てた場合、テストされる最初のルールの照合結果は一致します。

- ルールを 1 つだけ作成すると、すべての条件に一致したときにのみユーザを特定のトンネル グループに割り当てることができるようになります。すべての照合基準が必要であることは、論理 AND 操作に相当します。または、ユーザを特定のトンネル グループに割り当てる前にすべての照合基準が必要な場合は、基準ごとに 1 つのルールを作成します。照合基準が 1 つだけ必要であることは、論理 OR 操作に相当します。

ステップ 2 コンフィギュレーションでトンネル グループが指定されていない場合に使用する、デフォルト トンネル グループを指定します。

コマンドの構文は、**tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name* です。*rule-index* はルールの優先順位で、tunnel-group name は既存のトンネル グループでなければなりません。

例

次の例では、フェーズ 1 の ISAKMP ID の内容に基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ike-id
```

次の例では、ピアの IP アドレスに基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable peer-ip
```

次の例では、サブジェクト認定者名（DN）の組織ユニット（OU）に基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ou
```

次の例では、設定されたルールに基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable rules
```

IPsec の設定

ここでは、IPsec を使用して VPN を実装するときの ASA の設定に必要な手順について説明します。

暗号マップの定義

クリプト マップは、IPsec SA でネゴシエートされる IPsec ポリシーを定義します。使用できるキーワードには次のものがあります。

- IPsec 接続が許可および保護するパケットを識別するための ACL。
- ピア ID。
- IPsec トラフィックのローカル アドレス（詳細については、クリプト マップのインターフェイスへの適用 （33 ページ） を参照してください）。
- 最大 11 個の IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル。ピアのセキュリティ設定の照合に使用されます。

クリプト マップ セットは、同じマップ名を持つ 1 つまたは複数のクリプト マップで構成されます。最初のクリプト マップを作成したときに、クリプト マップ セットを作成します。次のサイトツーサイト タスクでは、シングルまたはマルチ コンテキスト モードで暗号マップを作成または暗号マップに追加します。

crypto map *map-name seq-num* **match address** *access-list-name*

access-list-name では、ACL ID を、最大 241 文字の文字列または整数として指定します。

ヒント　すべて大文字にすると、ACL ID がコンフィギュレーション内で見つけやすくなります。

このコマンドを続けて入力すると、クリプトマップをクリプトマップセットに追加できます。次の例では、暗号マップを追加する暗号マップ セットの名前は *mymap* です。

crypto map mymap 10 match address 101

上記の構文に含まれるシーケンス番号（*seq-num*）によって、同じ名前を持つ暗号マップがそれぞれ区別されます。暗号マップに割り当てられているシーケンス番号によって、暗号マップセット内の暗号マップ間のプライオリティが決まります。シーケンス番号が小さいほど、プライオリティが高くなります。暗号マップセットをインターフェイスに割り当てると、ASA は、そのインターフェイスを通過するすべての IP トラフィックと暗号マップ セット内の暗号マップを、シーケンス番号が低い順に照合して評価します。

[no] crypto map *map_name map_index* **set pfs [group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

暗号化マップの完全転送秘密（PFS）に使用する ECDH グループを指定します。暗号マップに対して group14 および group24 オプションを設定することはできなくなります（IKEv1 ポリシーを使用するとき）。

[no] crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

このクリプトマップエントリに基づく接続に対して逆ルート注入（RRI）をイネーブルにします。ダイナミックが指定されていない場合、RRI は設定時に行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。さらに、RRI ルートが、静的ルートがすでに存在する同じ宛先で設定されると、既存の静的ルートは廃棄され、RRI ルートがインス

トールされます。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。

ダイナミックが指定されている場合、ルートはIPsecセキュリティ アソシエーション（SA）の確立成功時に作成され、IPsec SA が削除されると削除されます。

暗号マップの1つが実際に使用されていない場合でも、スタティック暗号マップと同じ名前のダイナミック暗号マップを設定することはできません。その逆も同様です。

（注） ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

[no] crypto map *name priority* **set validate-icmp-errors**

または

[**no**]**crypto dynamic-map** *name priority* **set validate-icmp-errors**

着信ICMPエラーメッセージを、暗号化マップとダイナミック暗号化マップのどちらに対して検証するかを指定します。

[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}

または

[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]

暗号化マップまたはダイナミック暗号化マップの、既存のDo Not Fragment（DF）ポリシー（セキュリティ アソシエーション レベル）を設定します。

- *clear-df* : DF ビットを無視します。
- *copy-df* : DF ビットを維持します。
- *set-df* : DF ビットを設定して使用します。

[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

または

[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

管理者は、IPsecセキュリティ アソシエーションにおける、ランダムな長さおよび間隔のダミーのトラフィック フローの機密性（TFC）パケットをイネーブルにできます。TFC をイネーブルにするには、IKEv2 IPsec プロポーザルが設定されている必要があります。

暗号マップに割り当てられているACLは、同じACL名を持つすべてのACEで構成されます。コマンドの構文は次のとおりです。

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

最初の ACE を作成したときに、ACL を作成します。ACL を作成または追加するコマンドの構文は次のとおりです。

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

次の例では、ASA は 10.0.0.0 サブネットから 10.1.1.0 サブネットへのすべてのトラフィックに対して、暗号マップに割り当てられている IPsec 保護を適用します。

access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0

パケットが一致する暗号マップによって、SA ネゴシエーションで使用されるセキュリティ設定が決定します。ローカルの ASA がネゴシエーションを開始する場合は、スタティック暗号マップで指定されたポリシーを使用して、指定のピアに送信するオファーを作成します。ピアがネゴシエーションを開始する場合は、ASA はポリシーに一致するスタティック暗号マップを探しますが、見つからない場合は、暗号マップセット内のダイナミック暗号マップの中で見つかるものを探します。これは、ピアのオファーを受け入れるか拒否するかを決定するためです。

2 つのピアが SA の確立に成功するには、両方のピアが互換性のあるクリプト マップを少なくとも 1 つ持っている必要があります。互換性が成立するには、クリプトマップが次の条件を満たす必要があります。

- クリプト マップに、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。応答側ピアがダイナミック暗号マップを使用している場合は、ASA 側でも互換性のある暗号 ACL が含まれていることが、IPsec を適用するための要件の 1 つです。
- 各クリプト マップ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 マップに、共通のトランスフォーム セットまたはプロポーザルが少なくとも 1 つある。

1 つのインターフェイスに適用できるクリプトマップセットは 1 つだけです。次の条件のいずれかが当てはまる場合は、ASA 上の特定のインターフェイスに対して複数の暗号マップを作成します。

- 特定のピアに異なるデータ フローを処理させる。
- さまざまなタイプのトラフィックにさまざまな IPsec セキュリティを適用する。

たとえば、暗号マップを 1 つ作成し、2 つのサブネット間のトラフィックを識別する ACL を割り当て、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを 1 つ割り当てます。別の暗号マップを作成し、別の 2 つのサブネット間のトラフィックを識別する ACL を割り当て、VPN パラメータが異なるトランスフォーム セットまたはプロポーザルを適用します。

1 つのインターフェイスに複数のクリプト マップを作成する場合は、クリプト マップ セット内のプライオリティを決めるシーケンス番号（seq-num）を各クリプトマップエントリに指定します。

各 ACE には permit 文または deny 文が含まれます。次の表に、暗号マップに適用される ACL での許可 ACE と拒否 ACE の特別な意味を示します。

クリプト マップ評価の結果	応答
permit 文が含まれている ACE の基準と一致	パケットを暗号マップセットの残りの ACE と照合して評価することを停止し、パケット セキュリティ設定を、暗号マップに割り当てられている IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの中の設定と照合して評価します。セキュリティ設定がトランスフォーム セットまたはプロポーザルのセキュリティ設定と一致したら、ASA は関連付けられた IPsec 設定を適用します。一般に発信トラフィックの場合、IPsec 設定の適用とはパケットの復号化、認証、ルーティングを行うことを意味します。
deny 文が含まれている ACE の基準と一致	パケットを評価中のクリプト マップの残りの ACE と照合して評価することを中断し、次のクリプトマップ（クリプトマップに割り当てられているシーケンス番号で判断する）の ACE との照合と評価を再開します。
クリプトマップセット内のテスト済みのすべての許可 ACE と不一致	パケットを暗号化せずにルーティングします。

deny 文が含まれている ACE は、IPsec 保護が不要な発信トラフィック（たとえば、ルーティング プロトコル トラフィックなど）をフィルタリングして除外します。したがって、暗号 ACL の permit 文と照合して評価する必要のない発信トラフィックをフィルタリングするために、最初の deny 文を挿入します。

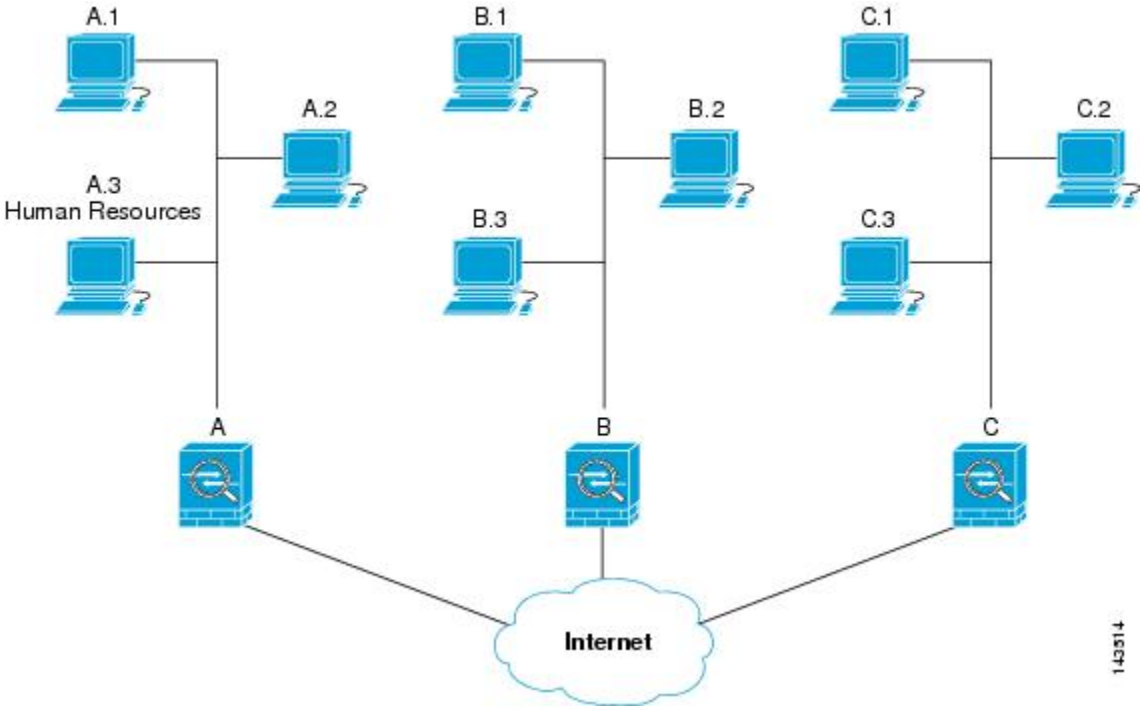
暗号化された着信パケットに対しては、セキュリティアプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティ アプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティアプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティ アプライアンスはそのパケットをルーティングします。

暗号化されていない着信パケットの内部ヘッダーを比較する場合は、セキュリティアプライアンスはすべての拒否ルールを無視します。これは、拒否ルールによってフェーズ 2 の SA の確立が妨げられるためです。

（注） 暗号化されていない着信トラフィックをクリア テキストとしてルーティングするには、ACE の許可の前に ACE の拒否を挿入します。ASA は、スプリットトンネル アクセスリストで 28 を超える ACE をプッシュすることはできません。

LAN-to-LAN 暗号マップの例

この LAN-to-LAN ネットワークの例において、セキュリティ アプライアンス A、B、および C を設定する目的は、ホストのいずれか 1 台から発信され、別のホストを宛先とするすべてのトラフィックのトンネリングを許可することです。ただし、ホスト A.3 から発信されるトラフィックには人事部の機密データが含まれるため、他のトラフィックよりも強固な暗号化と頻繁なキー再生が必要です。そのため、ホスト A.3 から発信されるトラフィックには特別なトランスフォーム セットを割り当てます。



この図に示され、また以下の説明で使用されている単純なアドレス表記は、抽象化したものです。実際の IP アドレスを使用した例は、この説明の後に示します。

セキュリティ アプライアンス A を発信トラフィック用に設定するには、2 つの暗号マップを作成します。1 つはホスト A.3 からのトラフィック用で、もう 1 つはネットワーク A の他のホストからのトラフィック用です。次に例を示します。

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

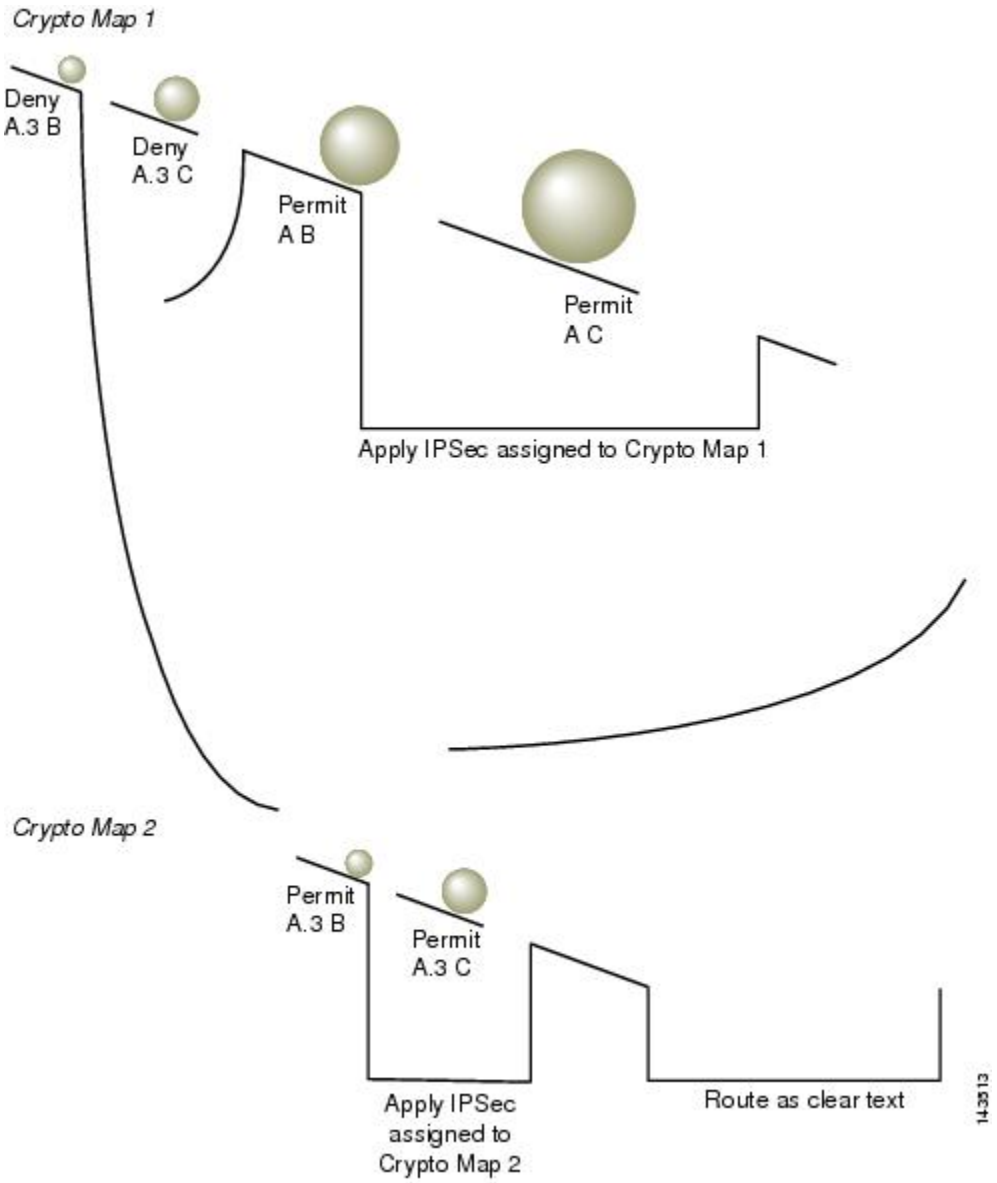
ACL を作成したら、一致するパケットごとに必要な IPsec を適用するためのトランスフォーム セットを各暗号マップに割り当てます。

カスケードACLとは、拒否ACEを挿入することで、ACLの評価をバイパスし、クリプトマップ セット内の次の ACL の評価を再開するものです。クリプト マップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応するクリプト マップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプト マップ、または異なるセキュリティを必要とする別のクリプト マップの permit 文と特別なトラフィックを照合することができます。暗号ACLに割り当てられているシーケンス番号によって、暗号マップ セット内の評価の順序が決まります。

次の図に、この例の概念的なACEから作成されたカスケードACLを示します。各記号の意味は、次のとおりです。

	クリプトマップセット内のクリプトマップ。
	（すき間がある直線）パケットがACEに一致した時点でクリプト マップの照合を終了します。
	1 つの ACE の説明と一致したパケット。それぞれの大きさのボールは、図中の別々の ACE に一致する異なるパケットを表しています。大きさの違いは、各パケットの発信元と宛先が異なることを示しています。
	クリプト マップ セット内での次のクリプト マップへのリダイレクション。
	パケットがACEに一致するか、またはクリプト マップ セット内のすべての許可 ACE に一致しない場合の応答。

図 *1:* 暗号マップ セット内のカスケード *ACL*



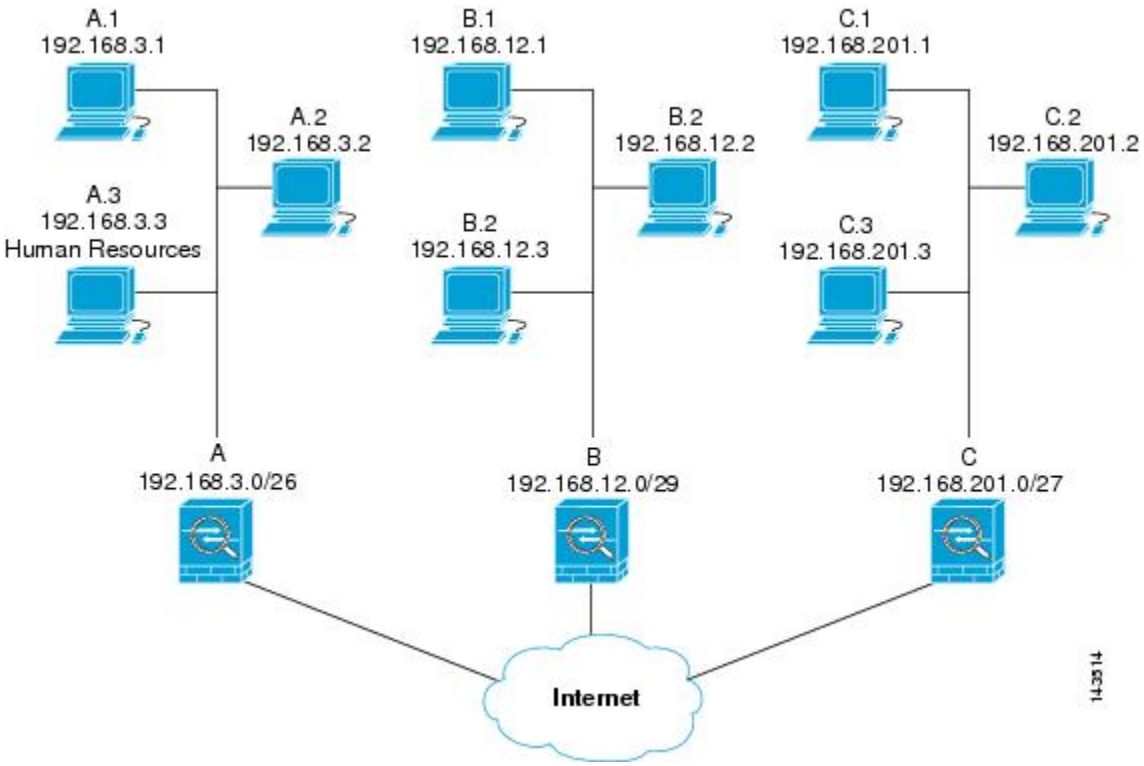
セキュリティ アプライアンス A は、ホスト A.3 から発信されたパケットが許可 ACE と一致するまで評価し、クリプト マップに関連付けられている IPsec セキュリティの割り当てを試行します。このパケットが拒否 ACE と一致すると、ASA はこの暗号マップの残りの ACE を無視し、次の暗号マップ（暗号マップに割り当てられているシーケンス番号で判断する）との照合と評価を再開します。この例では、セキュリティ アプライアンス A がホスト A.3 から発信されたパケットを受信すると、このパケットを最初のクリプト マップの拒否 ACE と照合し、次のクリプト マップでの照合と評価を再開します。パケットが 2 番目のクリプト マップの許可 ACE と一致すると、関連付けられた IPsec セキュリティ（強固な暗号化と頻繁なキー再生）がパケットに適用されます。

ネットワーク例の ASA 設定を完了するために、ASA B と C にミラー暗号マップを割り当てますが、ASA は、暗号化された着信トラフィックの評価時に deny ACE を無視するため、deny A.3 B ACE と deny A.3 C ACE のミラーに相当するものを除外できます。したがって、暗号マップ 2 のミラーに相当するものは必要ありません。このため、ASA B と C のカスケード ACL の設定は不要です。

次の表に、ASA A、B、および C のすべてに設定された暗号マップに割り当てられる ACL を示します。

セキュリティ アプライアンス A		セキュリティ アプライアンス B		セキュリティ アプライアンス C	
クリプト マップ シーケンス 番号	ACE パターン	クリプト マップ シーケンス 番号	ACE パターン	クリプト マップ シーケンス 番号	ACE パターン
1	A.3 B を拒否	1	B A を許可	1	C A を許可
	A.3 C を拒否				
	A B を許可				
	A C を許可		B C を許可		C B を許可
2	A.3 B を許可				
	A.3 C を許可				

次の図は、上で示した概念上のアドレスを実際の IP アドレスにマッピングしたものです。



次の表に示す実際の ACE では、そのネットワーク上で評価されるすべての IPsec パケットに適切な IPsec 設定が適用されます。

セキュリティアプライアンス	クリプトマップシーケンス番号	ACE パターン	実際の ACE
A	1	A.3 B を拒否	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を拒否	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		A B を許可	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		A C を許可	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224
	2	A.3 B を許可	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を許可	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
B	必要なし	B A を許可	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		B C を許可	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224

セキュリティ アプライアンス	クリプト マップ シーケンス 番号	ACE パターン	実際の ACE
C	必要なし	C A を許可	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192
		C B を許可	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248

この例のネットワークで示した論法を応用すると、カスケード ACL を使用して、1 台の ASA で保護されているさまざまなホストまたはサブネットにそれぞれ異なるセキュリティ設定を割り当てることができます。

（注） デフォルトでは、ASA は、IPsec トラフィックが入ってきたインターフェイスと同じインターフェイスを宛先とする IPsec トラフィックはサポートしません。このタイプのトラフィックには、U ターン、ハブアンドスポーク、ヘアピニングなどの名称があります。ただし、U ターン トラフィックをサポートするように IPsec を設定できます。それには、そのネットワークとの間のトラフィックを許可する ACE を挿入します。たとえば、セキュリティ アプライアンス B で U ターン トラフィックをサポートするには、概念上の「B B を許可」ACE を ACL1 に追加します。実際の ACE は次のようになります。**permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248**

公開キー インフラストラクチャ（PKI）キーの設定

キー ペアを生成またはゼロ化するときに Suite-B ECDSA アルゴリズムを選択できるようにするには、公開キー インフラストラクチャ（PKI）を設定する必要があります。

始める前に

RSA または ECDSA のトラストポイントを認証に使用するように暗号化マップを設定する場合は、最初にキー セットを生成する必要があります。これで、そのトラストポイントを作成して、トンネル グループ コンフィギュレーションの中で参照できるようになります。

手順

ステップ 1 キー ペアを生成するときに Suite-B ECDSA アルゴリズムを選択します。

crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]

ステップ 2 キー ペアをゼロ化するときに Suite B ECDSA アルゴリズムを選択します。

crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]

クリプト マップのインターフェイスへの適用

暗号マップ 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割り当てる必要があります。ASA は、すべてのインターフェイスで IPsec をサポートします。暗号マップ セットをインターフェイスに割り当てると、ASA は、すべてのトラフィックを暗号マップ セットと照合して評価し、接続中またはネゴシエーション中は指定されたポリシーを使用します。

クリプト マップをインターフェイスに割り当てると、SA 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 データ構造も初期設定されます。クリプト マップを修正してインターフェイスに再割り当てすると、ランタイム データ構造はクリプト マップ設定と再同期化されます。また、新しいシーケンス番号を使用して新しいピアを追加し、クリプト マップを再割り当てしても、既存の接続が切断されることはありません。

インターフェイス ACL の使用

ASA では、デフォルトで IPsec パケットがインターフェイス ACL をバイパスするようになっています。インターフェイス ACL を IPsec トラフィックに適用する場合は、**no** 形式の **sysopt connection permit-vpn** コマンドを使用します。

発信インターフェイスにバインドされている暗号マップ ACL は、VPN トンネルを通過する IPsec パケットの許可と拒否を行います。IPsec は、IPsec トンネルから来たパケットの認証と解読を行い、トンネルに関連付けられている ACL とパケットを照合して評価します。

ACL は、どの IP トラフィックを保護するかを定義します。たとえば、2 つのサブネット間または 2 台のホスト間のすべての IP トラフィックを保護するための ACL を作成できます（これらの ACL は、**access-group** コマンドで使用される ACL とよく似ています。ただし、**access-group** コマンドでは、ACL がインターフェイスで転送するトラフィックと阻止するトラフィックを決めます）。

暗号マップを割り当てるまで、ACL は IPsec の使用に限定されません。各暗号マップは ACL を参照し、パケットが ACL のいずれか 1 つで permit と一致した場合に適用する IPsec プロパティを決めます。

IPsec 暗号マップに割り当てられている ACL には、次の 4 つの主要機能があります。

- IPSec で保護する発信トラフィックを選択する（permit に一致したものが保護の対象）。
- 確立された SA がない状態で移動するデータに対して ISAKMP ネゴシエーションをトリガーする。
- 着信トラフィックを処理して、IPSec で保護すべきであったトラフィックをフィルタリングして廃棄する。

- ピアからの IKE ネゴシエーションを処理するときに、IPsec SA の要求を受け入れるかどうかを決定する（ネゴシエーションは **ipsec-isakmp crypto map** エントリにだけ適用されます）。ピアは、**ipsec-isakmp crypto map** コマンド エントリが関連付けられているデータフローを許可する必要があります。これは、ネゴシエーション中に確実に受け入れられるようにするためです。

（注） ACL の要素を 1 つだけ削除すると、ASA は関連付けられている暗号マップも削除します。

現在1つまたは複数の暗号マップが参照している ACL を修正する場合は、**crypto map interface** コマンドを使用してランタイム SA データベースを再初期化します。詳細については、**crypto map** コマンドを参照してください。

ローカル ピアで定義するスタティック暗号マップに対して指定するすべての暗号 ACL について、リモート ピアで「ミラー イメージ」暗号 ACL を定義することを推奨します。また、クリプトマップは共通トランスフォームをサポートし、他のシステムをピアとして参照する必要があります。これにより、両方のピアで IPsec が正しく処理されます。

（注） すべてのスタティック暗号マップで ACL と IPsec ピアを定義する必要があります。どちらかが定義されていないと、暗号マップは不完全なものになり、ASA は、前の完全な暗号マップにまだ一致していないトラフィックをドロップします。show conf コマンドを使用して、すべての暗号マップが完全なものになるようにします。不完全なクリプトマップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

暗号 ACL で送信元アドレスまたは宛先アドレスの指定に **any** キーワードを使用すると問題が発生するため、このキーワードの使用は避けてください。**permit any any** コマンド文を使用すると次の現象が発生するため、使用は極力避けてください。

- すべての発信トラフィックが保護されます。これには、対応するクリプトマップで指定されているピアに送信される保護済みのトラフィックも含まれます。
- すべての着信トラフィックに対する保護が必要になります。

このシナリオでは、ASA は IPsec 保護されていないすべての着信パケットを通知なしでドロップします。

保護するパケットを定義したことを必ず確認してください。**permit** 文に **any** キーワードを使用する場合は、その文の前に一連の **deny** 文をおき、保護対象外のトラフィックをすべてフィルタリングして排除します。これを行わないと、その **permit** 文に保護対象外のトラフィックが含まれることになります。

（注） **no sysopt connection permit-vpn** が設定されているときに、外部インターフェイスのアクセス グループが deny ip any any アクセス リストを呼び出すように設定されていたとしても、クライアントからの復号化された通過トラフィックは許可されます。

保護されたネットワークへの、サイトツーサイトまたはリモート アクセス VPN 経由でのアクセスをコントロールするために、**no sysopt permit** コマンドを外部インターフェイス上のアクセス コントロール リスト（ACL）と組み合わせて使用しようとしても、うまくいきません。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザはまだセキュリティ アプライアンスへの SSH を使用して接続できます。内部ネットワーク上のホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックできません。

ssh および **http** コマンドは、ACL よりもプライオリティが高くなります。つまり、VPN セッションからデバイスへの SSH、Telnet、または ICMP トラフィックを拒否するには、IP ローカル プールを拒否する **ssh**、**telnet**、および **icmp** コマンドを追加する必要があります。

トラフィックが着信か発信かに関係なく、ASA は、インターフェイスに割り当てられている ACL とトラフィックを照合して評価します。インターフェイスに IPsec を割り当てるには、次の手順を実行します。

手順

ステップ 1 IPsec に使用する ACL を作成します。

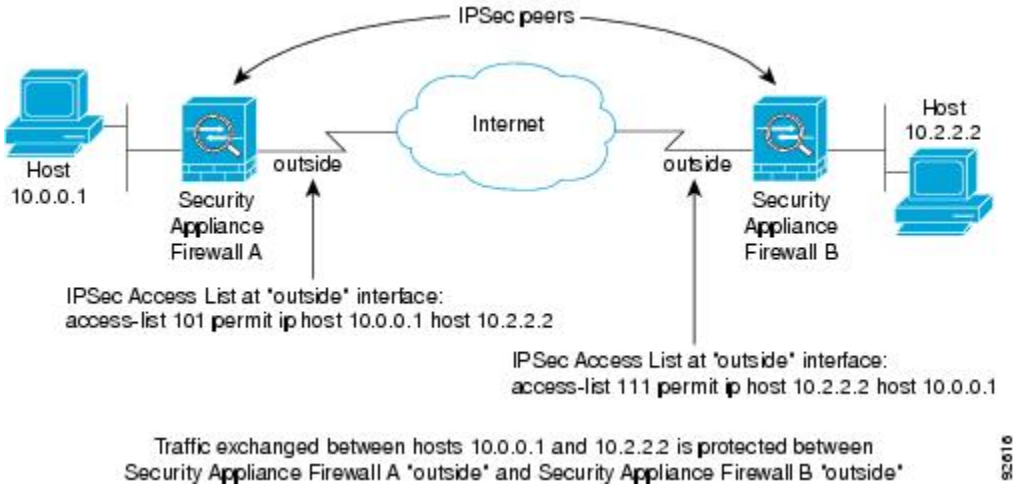
ステップ 2 作成したアクセス リストを、同じクリプトマップ名を使用して 1 つまたは複数のクリプトマップにマッピングします。

ステップ 3 データ フローに IPsec を適用するために、暗号マップに IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルをマッピングします。

ステップ 4 共有するクリプトマップ名を割り当てて、クリプトマップを一括してクリプトマップ セットとしてインターフェイスに適用します。

例

この例では、データが ASA A 上の外部インターフェイスを出てホスト 10.2.2.2 に向かうときに、ホスト 10.0.0.1 とホスト 10.2.2.2 の間のトラフィックに IPsec 保護が適用されます。



ASA A は、ホスト 10.0.0.1 からホスト 10.2.2.2 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.0.0.1
- 宛先 = ホスト 10.2.2.2

また、ASA A は、ホスト 10.2.2.2 からホスト 10.0.0.1 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.2.2.2
- 宛先 = ホスト 10.0.0.1

評価中のパケットと最初に一致した permit 文によって、IPsec SA のスコープが決まります。

IPsec SA のライフタイムの変更

ASA が新しい IPSec SA とネゴシエートするときに使用する、グローバル ライフタイム値を変更できます。特定のクリプト マップのグローバル ライフタイム値を上書きできます。

IPsec SA では、取得された共有秘密キーが使用されます。このキーは SA に不可欠な要素です。キーは同時にタイムアウトするので、キーのリフレッシュが必要です。各 SA には、「指定時刻」と「トラフィック量」の 2 種類のライフタイムがあります。それぞれのライフタイムを過ぎると SA は失効し、新しい SA のためのネゴシエーションが開始します。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。

グローバル ライフタイムを変更すると、ASA はトンネルをドロップします。変更後に確立された SA のネゴシエーションでは、新しい値が使用されます。

暗号マップに設定されたライフタイム値がなく、ASA から新しい SA を要求された場合、暗号マップは、ピアに送信される新しい SA 要求に、既存の SA で使用されているグローバル ライ

フタイム値を挿入します。ピアがネゴシエーション要求を受け取ると、このピアが提案するライフタイム値とローカルに設定されているライフタイム値のうち小さい方の値を、新しい SA のライフタイム値として使用します。

既存 SA のライフタイムのしきい値を超える前に、ピアは新しい SA をネゴシエートします。このようにして、既存 SA の有効期限が切れる前に、新しい SA の準備が整います。既存 SA の残りのライフタイムが約 5 ～ 15% になると、ピアは新しい SA をネゴシエートします。

VPN ルーティングの変更

デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係ルックアップが行われ、IPSec トンネル経由で送信されるパケットに対してはルックアップが行われません。

一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカルIPsecトンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。

これを防止するには、IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。

始める前に

この機能がデフォルトでディセーブルになっているのは、こうしたルックアップによるパフォーマンスの低下を回避するためです。この機能は、必要な場合にのみイネーブルにしてください。

手順

IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。

[no] [crypto] ipsec inner-routing-lookup

（注） このコマンドが設定されている場合、非VTIベースのトンネルにのみ適用されます。

例

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
 crypto ipsec ikev2 ipsec-proposal GCM
 protocol esp encryption aes-gcm
 protocol esp integrity null
 crypto ipsec inner-routing-lookup
```

スタティック暗号マップの作成

スタティック クリプトマップを使用する基本的なIPsecコンフィギュレーションを作成するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力して、保護するトラフィックを定義する ACL を作成します。

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

access-list-name では、ACL ID を、最大 241 文字の文字列または整数として指定します。*destination-netmask* と *source-netmask* では、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。この例では、**permit** キーワードによって、指定の条件に一致するトラフィックすべてが暗号で保護されます。

例：

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

ステップ 2 トラフィックを保護する方法を定義する IKEv1 トランスフォーム セットを設定するには、次のコマンドを入力します。

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

encryption では、IPsec データ フローを保護するための暗号化方式を指定します。

- esp-aes：AES と 128 ビット キーを使用します。
- esp-aes-192：AES と 192 ビット キーを使用します。
- esp-aes-256：AES と 256 ビット キーを使用します。
- esp-des：56 ビット DES-CBC を使用します。
- esp-3des：トリプル DES アルゴリズムを使用します。
- esp-null：暗号化なし。

authentication では、IPsec データ フローを保護するための暗号化方式を指定します

- esp-md5-hmac：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。
- esp-sha-hmac：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
- esp-none：HMAC 認証なし。

例：

この例では、myset1、myset2、aes_set がトランスフォーム セットの名前です。

```
hostname(config)#  crypto ipsec ikev1 transform-set myset1 esp-des esp-sha-hmac
```

```
hostname(config)# crypto ipsec ikev1 transform-set myset2 esp-3des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

ステップ 3 トラフィックを保護する方法も定義するIKEv2プロポーザルを設定するには、次のコマンドを入力します。

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

proposal tag は IKEv2 IPsec プロポーザルの名前で、1 ～ 64 文字の文字列です。

プロポーザルを作成し、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。このコンフィギュレーション モードでは、プロポーザルに対して複数の暗号化タイプと整合性タイプを指定できます。

例：

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

この例では、secure がプロポーザルの名前です。プロトコルおよび暗号化タイプを入力します。

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

例：

このコマンドでは、どの AES-GCM または AES-GMAC アルゴリズムを使用するかを選択します。

[**no**] **protocol esp encryption** [**3des** |**aes** |**aes-192** |**aes-256** |**aes-gcm** |**aes-gcm-192** |**aes-gcm-256** |**aes-gmac** |**aes-gmac-192** |**aes-gmac-256** |**des** |**null**]

SHA-2 またはヌルが選択されている場合は、どのアルゴリズムを IPsec 整合性アルゴリズムとして使用するかを選択する必要があります。AES-GCM/GMACが暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

[**no**] **protocol esp integrity** [**md5** |**sha-1** |**sha-256** |**sha-384** |**sha-512** |**null**]

（注） AES-GCM/GMACが暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。SHA-256はIKEv2トンネルを確立するために整合性や PRF に使用できますが、ESP 整合性保護にも使用できます。

ステップ 4 （任意）管理者はパス最大伝送単位（PMTU）エージングをイネーブルにして、PMTU 値を元の値にリセットする間隔を設定することができます。

[**no**] **crypto ipsec security-association pmtu-aging** *reset-interval*

ステップ 5 暗号マップを作成するには、シングルまたはマルチ コンテキスト モードを使用して、次のサイトツーサイト手順を実行します。

a) ACL を暗号マップに割り当てます。

crypto map *map-name seq-num* **match address** *access-list-name*

暗号マップセットとは、暗号マップエントリの集合です。エントリはそれぞれ異なるシーケンス番号（*seq-num*）を持ちますが、*map name* が同じです。*access-list-name* では、ACL ID を、最大 241 文字の文字列または整数として指定します。次の例では、mymap がクリ

プトマップセットの名前です。マップセットのシーケンス番号は10です。シーケンス番号は、1つのクリプトマップセット内の複数のエントリにランクを付けるために使用します。シーケンス番号が小さいほど、プライオリティが高くなります。

例：

この例では、ACL 101 が暗号マップ mymap に割り当てられます。

```
crypto map mymap 10 match address 101
```

b) IPsec で保護されたトラフィックの転送先となるピアを指定します。

crypto map *map_name sequence number***set peer** *ip_address*

例：

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA は、ピアに IP アドレス 192.168.1.100 が割り当てられている SA をセットアップします。

c) このクリプトマップに対して、IKEv1 トランスフォーム セットと IKEv2 プロポーザルのどちらを許可するかを指定します。複数のトランスフォーム セットまたはプロポーザルを、プライオリティ順（最高のプライオリティのものが最初）に列挙します。1 つの暗号マップに最大 11 個のトランスフォーム セットまたはプロポーザルを指定できます。次の 2 つのいずれかのコマンドを使用します。

crypto map *map-name seq-num* **set ikev1 transform-set** *transform-set-name1 [transform-set-name2, …transform-set-name11*]

または

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

proposal-name1 と *proposal-name11* では、IKEv2 の IPsec プロポーザルを 1 つ以上指定します。各暗号マップ エントリは、最大 11 個のプロポーザルをサポートします。

例：

IKEv1 の場合のこの例では、トラフィックが ACL 101 に一致したときに、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

d) （任意）IKEv2 では、トンネルに ESP 暗号化と認証を適用するための **mode** を指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

crypto map *map-name seq-num* **set ikev2 mode** [**transport | tunnel | transport-require**]

- [Tunnel mode]（デフォルト）：カプセル化モードがトンネル モードになります。トンネル モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）

に適用されるため、本来の送信元アドレスと宛先アドレスが非表示になります。元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。

このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。

トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- [Transport mode]：ピアがサポートしていない場合、カプセル化モードは、トンネル モードにフォールバックするオプション付きの転送モードになります。transport モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。

  このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理（たとえばQoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。

- [Transport Required]：カプセル化モードは転送モードにしかなりません。トンネル モードにフォールバックすることはできません。

デフォルトは **tunnel** カプセル化モードです。**transport** カプセル化モードは、ピアがこのモードをサポートしていない場合に tunnel モードにフォールバックできる転送モードであり、**transport-require** カプセル化モードでは、転送モードのみが適用されます。

（注） 転送モードは、リモート アクセス VPN には推奨されません。

カプセル化モードのネゴシエーションの例は次のとおりです。

- イニシエータが転送モードを提案し、レスポンダがトンネル モードで応答した場合、イニシエータはトンネル モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport モードで応答した場合、応答側は tunnel モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport-require モードの場合、応答側はプロポーザルを送信しません。
- 同様に、イニシエータが transport-require モードで、レスポンダがトンネル モードの場合は、レスポンダから NO PROPOSAL CHOSEN が送信されます。

e) （任意）グローバル ライフタイムを上書きする場合は、クリプト マップの SA ライフタイムを指定します。

crypto map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

map-name では、暗号マップセットの名前を指定します。*seq-num* では、暗号マップエントリに割り当てる番号を指定します。時間または送信されたデータに基づいて両方のライフタイムを設定できます。ただし、データ送信ライフタイムはサイト間 VPN にのみ適用され、リモート アクセス VPN には適用されません。

例：

この例では、クリプト マップ mymap の指定時刻ライフタイムを 10 ～ 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

f) （任意）IPsec がこのクリプト マップに対して新しい SA を要求するときに PFS を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

crypto map *map_name seq-num* **set pfs** [**group1** | **group2** | **group5**|**group14**]

例：

この例では、暗号マップ mymap 10 に対して新しい SA をネゴシエートするときに PFS が必要です。ASA は、1024 ビット Diffie-Hellman プライム モジュラス グループを新しい SA で使用します。

```
crypto map mymap 10 set pfs group15
```

g) （任意）このクリプト マップ エントリに基づく接続に対して逆ルート注入（RRI）をイネーブルにします。

crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

ダイナミックが指定されていない場合、RRI は設定時に行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。

ダイナミックが指定されている場合、ルートはIPsecセキュリティアソシエーション（SA）の確立成功時に作成され、IPsec SA が削除されると削除されます。

（注） ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

例：

```
crypto map mymap 10 set reverse-route dynamic
```

ステップ 6 IPsec トラフィックを評価するために、クリプト マップ セットをインターフェイスに適用します。

crypto map *map-name* **interface** *interface-name*

map-name では、暗号マップセットの名前を指定します。*interface-name* では、ISAKMP IKEv1 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

例：

この例では、ASA は外部インターフェイスを通過するトラフィックを暗号マップ mymap と照合して評価し、保護が必要かどうかを判断します。

```
crypto map mymap interface outside
```

ダイナミック暗号マップの作成

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、不足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。ASA は、スタティック暗号マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック暗号マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。ASA は、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベートIPアドレスを持っています一般に、LAN-to-LAN トンネルには事前に決定されたプライベート ネットワークのセットがあります。これがスタティック マップの設定に使用されるので、結果として IPsec SA の確立にも使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントには、スタティック IP アドレスがなく、IPsec ネゴシエーションを発生させるためのダイナミック クリプト マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当て、クライアントはこのアドレスを使用して IPsec SA をネゴシエートします。

（注） ダイナミック クリプト マップには **transform-set** パラメータだけが必要です。

ダイナミック暗号マップを使用すると、IPsec のコンフィギュレーションが簡単になります。ピアが常に事前に決定されるとは限らないネットワークで使用することを推奨します。ダイナ

ミック クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。

ヒント　ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリを ACL に挿入します。ネットワークとサブネット ブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。ASA は、ダイナミック暗号マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック暗号マップでは、発信トラフィックが ACL の permit エントリと一致しても、対応する SA がまだ存在しない場合、ASA はそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック暗号マップのセットには、暗号マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、ASA が他の暗号マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック クリプト マップを含めます。dynamic-seq-num によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック暗号マップを設定する場合は、IPsec ピアのデータ フローを暗号 ACL で識別するために、ACL の許可を挿入します。このように設定しないと、ASA は、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

注意　ダイナミック暗号マップ セットを使用して設定された、ASA インターフェイスにトンネリングされるトラフィックに対して、モジュールのデフォルト ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

シングル コンテキスト モードとマルチ コンテキスト モードのどちらかを使用して、ダイナミック暗号マップのエントリを作成します。1 つのクリプト マップ セット内で、スタティック マップ エントリとダイナミック マップ エントリを組み合わせることができます。

手順

ステップ 1　（任意） ACL をダイナミック暗号マップに割り当てます。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *access-list-name*

これによって、保護するトラフィックと保護しないトラフィックが決まります。*dynamic-map-name* では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

例：

この例では、ACL 101 がダイナミック暗号マップ dyn1 に割り当てられます。マップのシーケンス番号は 10 です。

```
crypto dynamic-map dyn1 10 match address 101
```

ステップ 2 このダイナミック暗号マップに対して、どの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを許可するかを指定します。複数のトランスフォームセットまたはプロポーザルをプライオリティ順に（最高のプライオリティのものが最初）指定します。IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルに応じたコマンドを使用してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1*, ［*transform-set-name2*, …*transform-set-name9*］

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。*transform-set-name* は、作成または変更するトランスフォーム セットの名前です。*proposal-name* では、IKEv2 の IPsec プロポーザルの名前を 1 つ以上指定します。

例：

IKEv1 の場合のこの例では、トラフィックが ACL 101 に一致したときに、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

ステップ 3 （任意）グローバル ライフタイム値を無効にする場合は、暗号ダイナミック マップ エントリの SA ライフタイムを指定します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。時間または送信されたデータに基づいて両方のライフタイムを設定できます。ただし、データ送信ライフタイムはサイト間 VPN にのみ適用され、リモート アクセス VPN には適用されません。

例：

この例では、ダイナミック クリプト マップ dyn1 の指定時刻ライフタイムを 10 ～ 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

ステップ 4 （任意） IPsec がこのダイナミック暗号マップに対して新しい SA を要求するときに PFS を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group7**]

dynamic-map-name では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

例：

```
crypto dynamic-map dyn1 10 set pfs group5
```

ステップ 5 ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加します。

ダイナミック マップを参照するクリプト マップは、必ずクリプト マップ セットの中でプライオリティ エントリを最低（シーケンス番号が最大）に設定してください。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

map-name では、暗号マップセットの名前を指定します。*dynamic-map-name* では、既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。

例：

```
crypto map  mymap 200 ipsec-isakmp dynamic dyn1
```

サイトツーサイト冗長性の実現

暗号マップを使用して複数の IKEv1 ピアを定義すると、冗長性を持たせることができます。このコンフィギュレーションはサイトツーサイト VPN に便利です。この機能は、IKEv2 ではサポートされません。

あるピアが失敗すると、ASA は、暗号マップに関連付けられている次のピアへのトンネルを確立します。ネゴシエーションが成功したピアにデータが送信され、そのピアがアクティブ ピアになります。アクティブ ピアとは、後続のネゴシエーションのときに、ASA が常に最初に試みるピアのことです。これは、ネゴシエーションが失敗するまで続きます。ネゴシエーションが失敗した時点で、ASA は次のピアに移ります。暗号マップに関連付けられているすべてのピアが失敗すると、ASA のサイクルは最初のピアに戻ります。

IPsec VPN の管理

IPsec コンフィギュレーションの表示

これらは、IPsec コンフィギュレーションに関する情報を表示するためにシングルまたはマルチ コンテキスト モードで入力できるコマンドです。

表 *1 : IPsec* コンフィギュレーション情報を表示するためのコマンド

show running-configuration crypto	IPsec、クリプトマップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。
show running-config crypto ipsec	IPsec コンフィギュレーション全体を表示します。
show running-config crypto isakmp	ISAKMP コンフィギュレーション全体を表示します。
show running-config crypto map	クリプトマップ コンフィギュレーション全体を表示します。
show running-config crypto dynamic-map	ダイナミック クリプトマップのコンフィギュレーションを表示します。
show all crypto map	すべてのコンフィギュレーション パラメータ（デフォルト値を持つパラメータも含む）を表示します。
show crypto ikev2 sa detail	暗号化統計情報での Suite-B アルゴリズム サポートを表示します。
show crypto ipsec sa	シングルまたはマルチ コンテキスト モードでの Suite-B アルゴリズム サポートおよび ESPv3 IPsec 出力を表示します。
show ipsec stats	シングルまたはマルチ コンテキスト モードでの IPsec サブシステムに関する情報を表示します。ESPv3 統計情報は、受信した TFC パケットおよび有効および無効な ICMP エラーに表示されます。

リブートの前にアクティブ セッションの終了を待機

すべてのアクティブ セッションが自発的に終了した場合に限り ASA をリブートするように、スケジュールを設定できます。この機能はデフォルトで無効に設定されています。

reload コマンドを使用して、ASA をリブートします。**reload-wait** コマンドを設定すると、**reload quick** コマンドを使用して **reload-wait** 設定を無効にできます。**reload** コマンドと **reload-wait** コマンドは特権 EXEC モードで使用できます。どちらにも **isakmp** プレフィックスは付けません。

手順

すべてのアクティブ セッションが自発的に終了するのを待って ASA をリブートする機能をイネーブルにするには、次のサイトツーサイトタスクをシングルまたはマルチコンテキストモードで実行します。

crypto isakmp reload-wait

例：

```
hostname(config)# crypto isakmp reload-wait
```

接続解除の前にピアに警告する

リモート アクセスや LAN-to-LAN のセッションがドロップする理由には、さまざまなものがあります。たとえば、ASA のシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、管理者による停止です。

ASA では、（LAN-to-LAN コンフィギュレーションまたは VPN クライアントの）限定されたピアに対して、セッションが接続解除される直前に通知できます。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ ペインに表示します。この機能はデフォルトで無効に設定されています。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス
- Cisco VPN Client のうち、バージョン 4.0 以降のソフトウェアを実行しているもの（コンフィギュレーションは不要）

IPsec ピアへの切断通知をイネーブルにするには、**crypto isakmp disconnect-notify** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

セキュリティ アソシエーションのクリア

一部のコンフィギュレーション変更は、後続の SA をネゴシエートしている間だけ有効になります。新しい設定をただちに有効にするには、既存の SA をクリアして、変更後のコンフィギュレーションで SA を再確立します。ASA がアクティブに IPsec トラフィックを処理している場合は、SA データベースのうち、コンフィギュレーション変更の影響を受ける部分だけをクリアします。SA データベースを完全にクリアするのは、大規模な変更の場合や、ASA が処理している IPsec トラフィック量が少ない場合に限定するようにしてください。

次の表に示すコマンドを入力すると、シングルまたはマルチ コンテキスト モードで IPsec SA をクリアして再初期化することができます。

表 *2 : IPsec SA* のクリアおよび再初期化用のコマンド

clear configure crypto	IPsec、クリプトマップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を削除します。
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
clear configure crypto dynamic-map	すべてのダイナミック クリプトマップを削除します。特定のダイナミック クリプトマップを削除できるキーワードもあります。
clear configure crypto map	すべてのクリプト マップを削除します。特定のクリプト マップを削除できるキーワードもあります。
clear configure crypto isakmp	ISAKMP コンフィギュレーション全体を削除します。
clear configure crypto isakmp policy	すべての ISAKMP ポリシーまたは特定のポリシーを削除します。
clear crypto isakmp sa	ISAKMP SA データベース全体を削除します。

暗号マップ コンフィギュレーションのクリア

clear configure crypto コマンドには、IPsec、暗号マップ、ダイナミック暗号マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーションの要素を削除できる引数が含まれます。

引数を指定しないで **clear configure crypto** コマンドを入力すると、暗号コンフィギュレーション全体（すべての認証も含む）が削除されることに注意してください。

詳細については、『*Cisco ASA Series Command Reference*』の **clear configure crypto** コマンドを参照してください。