IPsec を使用した VPN のセキュリティの設定

この部分では、基本的な IP VPN を設定する方法について説明します。IPsec は、IETF によって開発されたオープン規格のフレームワークです。インターネットなどの保護されていないネットワークを介して機密情報を伝達する場合にセキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（「ピア」）間の IP パケットを保護および認証します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IPsec を使用した VPN のセキュリティの設定に関する前提条件

IKE の設定

インターネット キー エクスチェンジ（IKE）は、「*Configuring Internet Key Exchange for IPsec VPNs*」の手順に従って設定する必要があります。

（注） IKE を使用しない場合でも、「*Configuring Internet Key Exchange for IPsec VPNs*」の手順に従って、IKE をディセーブルにする必要があります。

アクセス リストが IPsec と互換性があるか確認する

IKE は UDP ポート 500 を使用します。IPsec Encapsulating Security Payload（ESP）プロトコルと認証ヘッダー（AH）プロトコルは、それぞれ、プロトコル番号 50 と 51 を使用します。プロトコル 50、51、および UDP ポート 500 からのトラフィックが IPsec によって使用されるインターフェイスでブロックされないように、アクセス リストが設定されていることを確認します。場合によっては、これらのトラフィックを明示的に許可する文をアクセス リストに追加する必要があります。

IPsec を使用した VPN のセキュリティの設定に関する制約事項

Cisco IPsec ポリシー マップ MIB

MIB OID オブジェクトは、IPsec セッションが起動中にしか表示されません。

不連続アクセス制御リスト

不連続マスクを持つアクセス制御リスト（ACL）を使用する暗号マップはサポートされません。

物理インターフェイスと暗号マップ

物理インターフェイスがトンネル保護インターフェイスの送信元インターフェイスである場合、物理インターフェイスの暗号マップはサポートされません。

NAT の設定

ネットワークアドレス変換（NAT）を使用する場合は、IPsec が適切に動作するように、スタティック NAT を設定する必要があります。一般に、ルータが IPsec カプセル化を実行する前に、NAT が発生する必要があります。つまり、IPsec はグローバル アドレスと連動している必要があります。

ユニキャスト IP データグラム アプリケーションのみ

IPsec は、ユニキャスト IP データグラムにのみ適用できます。IPsec のワーキング グループがまだグループ キー配布の問題に対処していないため、IPsec は現在マルチキャストまたはブロードキャスト IP データグラムを処理しません。

サポートされないインターフェイス タイプ

- 暗号 VPN は、ブリッジ ドメイン インターフェイス（BDI）上でサポートされません。
- 暗号マップは、トンネルインターフェイスとポートチャネルインターフェイス上でサポートされません。例外として、GDOIの暗号マップは、トンネルインターフェイス上でサポートされます。
- 暗号マップは、ループバック インターフェイス上ではサポートされません。
- トンネルでトランスポートプロファイルが有効になっている場合、トンネル送信元インターフェイス上では暗号マップはサポートされません。
- 暗号マップは、MFR のトンネルインターフェイス上ではサポートされません。
- 暗号マップは、VLAN インターフェイス上ではサポートされません。
- GetVPN 暗号マップは、ポートチャネル インターフェイス上でサポートされます。

IPsec を使用した VPN のセキュリティの設定に関する情報

Supported Standards

シスコでは、この機能を使用して次の規格を実装しています。

- IPsec：IPsec は、参加しているピア間のデータ機密性、データ整合性、およびデータ認証を提供するオープン スタンダードのフレームワークです。IPsecは、これらのセキュリティ サービスを IP レイヤで提供します。IPsec は、IKE を使用して、ローカル ポリシーに基づいてプロトコルおよびアルゴリズムのネゴシエーションを処理し、IPsec で使用される暗号キーと認証キーを生成します。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

（注） IPsec という用語は、IPsec データ サービスのプロトコル全体およびIKEセキュリティ プロトコルを表す場合に使用されることがあります。また、データ サービスだけを表す場合にも使用されることがあります。

- IKE（IKEv1 と IKEv2）：Oakley キー交換や SKEME キー交換を Internet Security Association and Key Management Protocol（ISAKMP）フレームワーク内部に実装したハイブリッド プロトコルです。IKE は他のプロトコルで使用されますが、その初期実装は IPsec プロトコルで使用されます。IKE は、IPSec ピアを認証し、IPSec セキュリティ アソシエーションをネゴシエーションし、IPSec キーを確立します。

（注） Cisco IOS XE Bengaluru 17.6.x 以降、脆弱な暗号化アルゴリズムを設定すると警告が生成されますが、警告は無視しても問題はなく、アルゴリズムの動作には影響しません。次の例では、脆弱な暗号アルゴリズムに関する警告メッセージを表示します。

```
Device(config-ikev2-proposal)# group 5
%Warning: weaker dh-group is deprecated
```

次の表に、すべての脆弱なアルゴリズムを示します。

IKEv1	IKEv2	IPSec
DH_GROUP_768_MODP/Group 1	DH_GROUP_768_MODP/Group 1	ah-md5-hmac
DH_GROUP_1024_MODP/Group 2	DH_GROUP_1024_MODP/Group 2	ah-sha-hmac
DH_GROUP_1536_MODP/Group 5	DH_GROUP_1536_MODP/Group 5	esp-des
DES	DES	esp-3des
3DES	3DES	esp-sha-hmac
MD5	MD5	esp-gmac
DH_GROUP_2048_256_MODP/Group 24	DH_GROUP_2048_256_MODP/Group 24	esp-md5-hmac
		esp-null

IPsec のために実装されているコンポーネント テクノロジーには、次のものがあります。

（注） Cisco IOS XE 17.11.1a 以降、セキュリティ強化と弱い暗号の廃止の一環として、DES、3DES、MD5、および Diffie-Hellman（DH）グループ 1、2、5 を設定するオプションは廃止され、サポートされなくなりました。代わりに、AES、SHA、および DH グループ 14 以上を使用してください。さらに、esp-gmac トランスフォームも廃止されました。

弱い暗号を引き続き使用する場合は、**crypto engine compliance shield disable** コマンドを使用してデバイスで CSDL コンプライアンスを無効にし、再起動してください。

- AES：Advanced Encryption Standard（AES）。暗号アルゴリズムの 1 つで、重要ではあるが機密扱いではない情報を保護します。AES は、IPsec および IKE 用のプライバシー変換であり、DES に代わる規格として開発されました。AES は DES よりも安全度の高い設計となっています。AES ではキーのサイズが従来より大きく、侵入者がメッセージを解読するには、あらゆるキーを試してみるしか方法がありません。AES のキーは可変長であり、アルゴリズムは 128 ビット キー（デフォルト）、192 ビット キー、または 256 ビット キーを指定できます。
- DES：データ暗号規格（DES）。パケット データの暗号化に使用されるアルゴリズムです。シスコ ソフトウェアは、必須の 56 ビット DES-CBC with Explicit IV を実装していま

す。Cipher Block Chaining（CBC）では、暗号化の開始に初期ベクター（IV）が必要です。IV は IPSec パケットに明示的に指定されます。下位互換性を確保するために、Cisco IOS IPsec は ESP DES-CBC の RFC 1829 バージョンも実装します。

また、Cisco IOS は、特定のプラットフォームで使用可能なソフトウェア バージョンに応じて、Triple DES（168 ビット）暗号化も実装します。Triple DES（3DES）は推奨されていません。

（注） 強力な暗号化を使用する Cisco IOS イメージ（56 ビット データ暗号化フィーチャ セットを含むがこれに限定されない）は、米国輸出規制の対象となり、配布が制限されます。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- SHA-2 および SHA-1 ファミリ（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）の 1 および 2。SHA-1 および SHA-2 は、パケット データの認証および IKE プロトコルの整合性確認メカニズムの検証に使用されるハッシュ アルゴリズムです。HMAC は、追加レベルのハッシュを提供するバリアントです。SHA-2 ファミリには、SHA-256 ビットのハッシュ アルゴリズムと SHA-384 ビットのハッシュ アルゴリズムが加わっています。この機能は Suite-B の要件に含まれています。Suite-B は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco IOS での Suite-B サポートに関する詳細については、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。
- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、セキュアでない通信チャネルによる共有秘密を確立できます。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。これは、768 ビット（デフォルト）、1024 ビット、1536 ビット、2048 ビット、3072 ビット、および 4096 ビット DH グループをサポートします。また、256 ビット サブグループを含む 2048 ビット DH グループと、256 ビットと 384 ビットの Elliptic Curve DH（ECDH）もサポートします。2048 ビット以上の DH キー交換または ECDH キー交換の使用をお勧めします。
- MD5（ハッシュ ベースのメッセージ認証コード（HMAC）バリアント）：メッセージ ダイジェスト アルゴリズム 5（MD5）はハッシュ アルゴリズムです。HMAC はデータの認証に使用されるキー付きハッシュ バリアントです。

シスコ ソフトウェアに実装された IPsec は、さらに次の規格をサポートします。

- AH：認証ヘッダー。データ認証と、オプションとしてアンチ リプレイ サービスを提供するセキュリティ プロトコルです。AH は、保護対象のデータ（完全 IP データグラム）に埋め込まれます。
- ESP：Encapsulating Security Payload。データ プライバシー サービスと、オプションとしてデータ認証およびアンチ リプレイ サービスを提供するセキュリティ プロトコルです。ESP は保護対象のデータをカプセル化します。

サポートされるカプセル化

IPsec は、フレーム リレー、ハイ レベル データ リンク制御（HDLC）、および PPP のシリアル カプセル化と連動します。

また、IPsec は、Generic Routing Encapsulation（GRE）、IPinIP レイヤ 3、データリンクスイッチング +（DLSw+）、および Source Route Bridging（SRB）トンネリングプロトコルとも連動します。ただし、マルチポイントトンネルはサポートされません。他のレイヤ 3 のトンネリング プロトコルと IPSec の併用はサポートされない場合があります。

IPsec 機能の概要

IPSec は、次のネットワーク セキュリティ サービスを提供します。（一般に、ローカルセキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます）。

- データ機密性：ネットワークにパケットを伝送する前に IPSec 送信側がパケットを暗号化できます。
- データ整合性：IPSec 受信者は、IPSec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。
- データ送信元認証：IPsec 受信者は、送信された IPsec パケットの送信元を認証できます。このサービスは、データ整合性サービスに依存します。
- アンチ リプレイ：IPsec 受信者は、再送されたパケットを検出し、拒否できます。

IPsec は、2 つのピア（2 台のルータなど）間にセキュア トンネルを確立します。機密性が高く、セキュア トンネルを介して送信する必要があるパケットを定義し、セキュア トンネルの特性を指定することによって、機密性の高いパケットを保護するために使用するパラメータを定義します。IPsec ピアが機密パケットを認識すると、ピアは適切なセキュア トンネルを設定し、このトンネルを介してリモート ピアにパケットを送信します（この章で使用するトンネルという用語は、IPsec をトンネル モードで使用することではありません）。

正確には、このトンネルは、2 つの IPsec ピア間に確立されるセキュリティ アソシエーション（SA）のセットです。SA は、機密パケットに適用するプロトコルおよびアルゴリズムを定義し、2 つのピアが使用するキー関連情報を指定します。SA は単方向で、セキュリティ プロトコル（AH または ESP）ごとに確立されます。

2 つのピア間に複数の IPsec トンネルを設定し、トンネルごとに個別の SA のセットを使用することにより、さまざまなデータ ストリームを保護できます。たとえば、一部のデータ ストリームは認証だけが必要で、他のデータ ストリームは暗号化と認証の両方が必要な場合があります。

IKEv1 トランスフォーム セット

インターネット キー エクスチェンジ バージョン 1（IKEv1）トランスフォーム セットは、セキュリティ プロトコルとアルゴリズムの特定の組み合わせを表します。IPsec SA のネゴシエーション中に、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合意します。

IKEv2 トランスフォーム セット

インターネット キー エクスチェンジ バージョン 2（IKEv2）プロポーザルは、IKE_SA_INIT 交換の一部としての IKEv2 SA のネゴシエーションで使用されるトランスフォームのセットです。IKEv2 プロポーザルは、少なくとも 1 つの暗号化アルゴリズム、整合性アルゴリズム、および Diffie-Hellman（DH）グループが設定されている場合にのみ、完全であるとみなされます。プロポーザルが設定されておらず、IKEv2 ポリシーに接続されていない場合、ネゴシエーションではデフォルトのプロポーザルが使用されます。デフォルトのプロポーザルは、次のような通常使用されるアルゴリズムのコレクションです。

```
encryption aes-cbc-128 3des
integrity sha1 md5
group 5 2
```

crypto ikev2 proposal コマンドは **crypto isakmp policy priority** コマンドに似ていますが、IKEv2 プロポーザルには次のような違いがあります。

- IKEv2 プロポーザルを使用すると、各トランスフォーム タイプに対して 1 つ以上のトランスフォームを設定できます。
- IKEv2 プロポーザルには関連付けられた優先順位はありません。

（注） ネゴシエーションで IKEv2 プロポーザルを使用するには、それらを IKEv2 ポリシーにアタッチする必要があります。プロポーザルが設定されていない場合、デフォルトの IKEv2 プロポーザルとデフォルトの IKEv2 ポリシーが使用されます。

トランスフォーム セット：セキュリティ プロトコルとアルゴリズムの組み合わせ

トランスフォーム セットの概要

（注） h-md5-hmac、esp-md5-hmac、esp-des、または esp-3des の使用は推奨されていません。代わりに、ah-sha-hmac、esp-sha-hmac、または esp-aes を使用する必要があります。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsec SA のネゴシエーション中に、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合意します。

IKE との IPSec セキュリティ アソシエーション ネゴシエーションで、ピアは両方のピア用の同じトランスフォーム セットを探します。同一のトランスフォーム セットが検出された場合、そのトランスフォーム セットが選択され、両方のピアの IPsec SA の一部として、保護するト

ラフィックに適用されます。（手動で確立した SA は、ピアとネゴシエーションしないため、両方に同じトランスフォーム セットを指定する必要があります）。

次の表に、許可されるトランスフォームの組み合わせを示します。

表 *1:* 許可されるトランスフォームの組み合わせ

トランスフォーム タイプ	トランスフォーム	説明
AH Transform（*1* つ選択）	**ah-md5-hmac**	MD5（メッセージ ダイジェスト 5）（HMAC バリアント）認証アルゴリズムを使用する AH。（非推奨）。
	ah-sha-hmac	SHA（セキュア ハッシュ アルゴリズム）（HMAC バリアント）認証アルゴリズムを使用する AH。
ESP Encryption Transform（*1* つ選択）	**esp-aes**	128 ビット Advanced Encryption Standard（AES）暗号化アルゴリズムを使用する ESP。
	esp-aes 192	192 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-aes 256	256 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-des	56 ビットのデータ暗号規格（DES）暗号化アルゴリズムを使用する ESP。（非推奨）。
esp-3des	168 ビット DES 暗号化アルゴリズム（3DES、トリプル DES とも呼ばれる）を使用する ESP。（非推奨）。	
ESP Authentication Transform（*1* つ選択）	**esp-md5-hmac**	MD5（HMAC バリアント）認証アルゴリズムを使用する ESP。（非推奨）。
	esp-sha-hmac	SHA（HMAC バリアント）認証アルゴリズムを使用する ESP。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IKE および IPsec 暗号化アルゴリズムのための Cisco IOS Suite-B のサポート

Suite-B には次の暗号化アルゴリズムがあります。

- Suite-B-GCM-128：ESP 整合性保護、機密性、および RFC 4106 で規定されている 128 ビット AES using Galois and Counter Mode（AES-GCM）を使用する IPsec 暗号化アルゴリズムを提供します。ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。
- Suite-B-GCM-256：RFC 4106 で規定されている 256 ビット AES-GCM を使用して、ESP 整合性保護と機密性を提供します。ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。
- Suite-B-GMAC-128：RFC 4543 で規定されている 128 ビット AES-Galois Message Authentication Code（GMAC）を使用して、ESP 整合性保護を提供しますが、機密性は提供しません。このスイートは、ESP の暗号化が不要である場合のみに使用する必要があります。
- Suite-B-GMAC-256：RFC 4543 で規定されている 256 ビット AES-GMAC を使用して、ESP 整合性保護を提供しますが、機密性は提供しません。このスイートは、ESP の暗号化が不要である場合のみに使用する必要があります。

IPSec 暗号化アルゴリズムは、暗号化が必要な場合に AES-GCM を使用し、暗号化が不要な場合のメッセージの整合性には AES-GMAC を使用します。

IKE ネゴシエーションでは、AES 暗号ブロック連鎖（CBC）モードを使用して暗号化を行い、RFC 4634 に定義されている SHA-256 および SHA-384 ハッシュ アルゴリズムを含む Secure Hash Algorithm（SHA）-2 ファミリを使用してハッシュ機能を実行します。キー交換には RFC 4753 に定義されている Elliptic Curves（ECP）を使用した Diffie-Hellman が使用され、認証を行うには RFC 4754 に定義されている楕円曲線デジタル署名アルゴリズム（ECDSA）が使用されます。

Suite-B の要件

IKE および IPsec を使用する場合、Suite-B によって次のソフトウェア暗号エンジンに要件が課せられます。

- HMAC-SHA256 と HMAC-SHA384 は疑似ランダム関数として使用されます。また、IKE プロトコル内の整合性チェックが使用されます。必要に応じて、HMAC-SHA512 を使用することもできます。

- 楕円曲線グループ 19（256 ビットの ECP 曲線）および 20（384 ビットの ECP 曲線）は、IKE で Diffie-Hellman グループとして使用されます。必要に応じて、グループ 21（521 ビットの ECP 曲線）を使用できます。
- X.509 証明書内の署名操作で、楕円曲線デジタル署名アルゴリズム（ECDSA）（256 ビットおよび 384 ビットの曲線）が使用されます。
- ESP（128 ビットおよび 256 ビットのキー）には、GCM（16 バイトの ICV）および GMAC が使用されます。必要に応じて、192 ビットのキーを使用することもできます。
- ECDSA 署名を使用した X.509 証明書の確認に対する Public Key Infrastructure（PKI）サポートを使用する必要があります。
- ECDSA 署名を使用して証明書要求を生成する場合、および発行された証明書を IOS にインポートする場合に、PKI を使用する必要があります。
- 認証方式として ECDSA signature（ECDSA-sig）を使用できるようにする場合に、IKEv2 を使用する必要があります。

Suite-B の設定情報の入手先

Suite-B の設定のサポートについては、次のマニュアルで説明されています。

- SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キー ペアの設定の詳細については、「*Configuring Internet Key Exchange for IPsec VPNs*」機能モジュールを参照してください。
- 整合性アルゴリズム タイプのトランスフォームの設定の詳細については、「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」機能モジュールの「Configuring the IKEv2 Proposal」を参照してください。
- ECDSA-sig を IKEv2 の認証方式として設定する場合の詳細については、「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」機能モジュールの「Configuring IKEv2 Profile (Basic)」を参照してください。
- IPsec SA ネゴシエーション用の Elliptic Curve Diffie-Hellman（ECDH）サポートの設定の詳細については、「*Configuring Internet Key Exchange for IPsec VPNs*」および「*Configuring Internet Key Exchange Version 2 and FlexVPN*」機能モジュールを参照してください。

PKI の証明書登録での Suite-B のサポートの詳細については、「*Configuring Certificate Enrollment for a PKI*」機能モジュールを参照してください。

IPsec VPN の設定方法

クリプト アクセス リストの作成

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
   - **ip access-list extended** *name*
4. 作成するクリプト アクセス リストごとにステップ 3 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを実行します。
	• **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
	• **ip access-list extended** *name*
	例：
	`Device(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255`
	例：
	`Device(config)# ip access-list extended vpn-tunnel`
		保護する IP パケットを判別する条件を指定します。
		• 番号または名前によって指定された IP アクセスリストを使用して、条件を指定します。**access-list** コマンドでは、番号付き拡張アクセスリストを指定し、**ip access-list extended** コマンドでは、名前付きアクセスリストを指定します。
		• これらの条件に一致するトラフィックに対して暗号化をイネーブルまたはディセーブルにします。
		ヒント　IPsec で使用できるように "mirror image" クリプトアクセスリストを設定することを推奨します。また、**any** キーワードを使用することは推奨しません。

	コマンドまたはアクション	目的
ステップ 4	作成するクリプト アクセス リストごとにステップ 3 を繰り返します。	—

次の作業

クリプトアクセスリストを 1 つ以上作成したら、トランスフォームセットをIKEv1 および IKEv2 プロポーザルのトランスフォーム セットの設定 （12 ページ）の手順に従って定義する必要があります。

次に、クリプトマップセットを設定してインターフェイスに適用するときに、クリプトアクセスリストを特定のインターフェイスに関連付ける必要があります。（クリプト マップ セットの作成 （17 ページ）およびインターフェイスへのクリプト マップ セットの適用 （28 ページ）の指示に従ってください）。

IKEv1 および IKEv2 プロポーザルのトランスフォーム セットの設定

この作業は、IKEv1 および IKEv2 プロポーザルとの IPsec SA のネゴシエーション時に IPsec ピアが使用するトランスフォーム セットを定義するために実行します。

機能制限

SEAL 暗号化を指定する場合は、次の制約事項に注意してください。

- ルータと他のピアがハードウェア IPsec 暗号化を備えていないこと。
- ルータおよび他のピアが IPsec をサポートすること。
- ルータおよび他のピアが k9 サブシステムをサポートすること。
- SEAL 暗号化はシスコ製の装置だけで使用可能。したがって、相互運用性はありません。
- IKEv1 と異なり、認証方式と SA ライフタイムは IKEv2 ではネゴシエーション可能ではありません。そのため、これらのパラメータを IKEv2 プロポーザルで設定することはできません。

IKEv1 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]]
4. **mode** [**tunnel** | **transport**]
5. **end**
6. **clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map** *map-name* | **sa entry** *destination-address protocol spi*]

7. **show crypto ipsec transform-set** [**tag** *transform-set-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]] 例： `Device(config)# crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac`	トランスフォームセットを定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • transform 引数に使用できるエントリを定義する複合ルールがあります。これらルールについては、**crypto ipsec transform-set** コマンドのコマンド解説で説明します。また、「トランスフォームセットの概要」の表に、許可されるトランスフォームの組み合わせのリストを示します。
ステップ 4	**mode** [**tunnel** | **transport**] 例： `Device(cfg-crypto-tran)# mode transport`	（任意）トランスフォームセットに関連付けられたモードを変更します。 • このモード設定は、送信元アドレスと宛先アドレスが IPsec ピア アドレスであるトラフィックだけに適用され、その他すべてのトラフィックに対しては無視されます。（他のトラフィックはすべてトンネル モードです）。
ステップ 5	**end** 例： `Device(cfg-crypto-tran)# end`	暗号トランスフォーム コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map** *map-name* | **sa entry** *destination-address protocol spi*] 例： `Device# clear crypto sa`	（任意）既存の IPsec SA を消去して、その後確立された SA でトランスフォーム セットへの変更が有効になるようにします。 手動で確立した SA は、すぐに再確立されます。 • パラメータを指定せずに **clear crypto sa** コマンドを使用すると、SA データベースの内容が完全に消去されるので、アクティブなセキュリティセッションが消去されます。

	コマンドまたはアクション	目的
		• SA データベースのサブセットだけを消去するには、**peer**、**map**、または **entry** キーワードも指定します。
ステップ 7	**show crypto ipsec transform-set** [**tag** *transform-set-name*] 例： `Device# show crypto ipsec transform-set`	（任意）設定済みのトランスフォームセットを表示します。

次の作業

トランスフォーム セットを定義したら、「クリプト マップ セットの作成」の手順に従ってクリプト マップを作成する必要があります。

IKEv2 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal** *proposal-name*
4. **encryption** *transform1* [*transform2*] ...
5. **integrity** *transform1* [*transform2*] ...
6. **group** *transform1* [*transform2*] ...
7. **end**
8. **show crypto ikev2 proposal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 proposal** *proposal-name* 例： `Device(config)# crypto ikev2 proposal proposal-1`	プロポーザルの名前を指定し、暗号 IKEv2 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。 • IKEv2 ポリシーでは、プロポーザル名を使用してプロポーザルが参照されます。

	コマンドまたはアクション	目的
ステップ 4	**encryption** *transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# encryption aes-cbc-128`	（任意）次の暗号化タイプのトランスフォームを 1 つ以上指定します。 • AES-CBC 128：128 ビット AES-CBC • AES-CBC 192：192 ビット AES-CBC • AES-CBC 256：256 ビット AES-CBC • 3DES：168 ビット DES（非推奨。AES が推奨されている暗号化アルゴリズムです）。
ステップ 5	**integrity** *transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# integrity sha1`	（任意）次の整合性タイプのトランスフォームを 1 つ以上指定します。 • **sha256** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 256 ビット（HMAC バリアント）を指定します。 • **sha384** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 384 ビット（HMAC バリアント）を指定します。 • **sha512** キーワードは、ハッシュアルゴリズムとして SHA-2 ファミリ 512 ビット（HMAC バリアント）を指定します。 • **sha1** キーワードは、ハッシュアルゴリズムとして SHA-1（HMAC バリアント）を指定します。 • **md5** キーワードは、ハッシュアルゴリズムとして MD5（HMAC バリアント）を指定します。（非推奨。SHA-1 が推奨されている代替品です）。
ステップ 6	**group** *transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# group 14`	（任意）使用可能な DH グループ タイプのトランスフォームを 1 つ以上指定します。 • **1**：768 ビット DH（非推奨） • **2**：1024 ビット DH（非推奨） • **5**：1536 ビット DH（非推奨） • **14**：2048 ビット DH グループを指定します。 • **15**：3072 ビット DH グループを指定します。 • **16**：4096 ビット DH グループを指定します。

	コマンドまたはアクション	目的
		• **19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 • **20**：384 ビット ECDH グループを指定します。 • **24**：2048 ビット DH/DSA グループを指定します。
ステップ 7	**end** 例： `Device(config-ikev2-proposal)# end`	暗号 IKEv2 プロポーザル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show crypto ikev2 proposal** 例： `Device# show crypto ikev2 proposal`	（任意）各 IKEv2 プロポーザルのパラメータを表示します。

IKEv2 のトランスフォーム セットの例

次の例では、プロポーザルの設定方法を示しています。

各トランスフォーム タイプに対して 1 つのトランスフォームがある IKEv2 プロポーザル

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity sha1
Device(config-ikev2-proposal)# group 14
```

各トランスフォーム タイプに対して複数のトランスフォームがある IKEv2 プロポーザル

```
crypto ikev2 proposal proposal-2
encryption aes-cbc-128 aes-cbc-192
integrity sha1 sha256
group 14 15
```

トランスフォームの組み合わせのリストについては、「Configuring Security for VPNs with IPsec」を参照してください。

発信側と応答側の IKEv2 プロポーザル

発信側のプロポーザルは次のとおりです。

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-196
Device(config-ikev2-proposal)# integrity sha1 sha256
Device(config-ikev2-proposal)# group 14 16
```

応答側のプロポーザルは次のとおりです。

```
Device(config)# crypto ikev2 proposal proposal-2
```

```
Device(config-ikev2-proposal)# encryption aes-cbc-196 aes-cbc-128
Device(config-ikev2-proposal)# integrity sha256 sha1
Device(config-ikev2-proposal)# group 16 14
```

このシナリオでは、発信側のアルゴリズムの選択が優先されます。選択されたアルゴリズムは次のとおりです。

```
encryption aes-cbc-128
integrity sha1
group 14
```

次の作業

トランスフォーム セットを定義したら、「クリプト マップ セットの作成」の手順に従ってクリプト マップを作成する必要があります。

クリプト マップ セットの作成

スタティック クリプト マップの作成

IKE を使用して SA が確立されると、IPsec ピアは、新しいセキュリティ アソシエーションに使用する設定をネゴシエートできます。つまり、クリプト マップ エントリ内でリスト（許容されるトランスフォームのリストなど）を指定できます。

このタスクは、IKE を使用して SA を確立するクリプト マップ エントリを作成するために実行します。IPv6 クリプトマップエントリを作成するには、**crypto map** コマンドで **ipv6** キーワードを使用する必要があります。IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp**]
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
7. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
8. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}
9. **set security-association level per-host**
10. **set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
11. **end**

12. **show crypto map** [**interface** *interface* | **tag** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp**] 例： `Device(config)# crypto map static-map 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。 • IPv4 クリプトマップでは、**ipv6** キーワードなしでコマンドを使用します。
ステップ 4	**match address** *access-list-id* 例： `Device(config-crypto-m)# match address vpn-tunnel`	拡張アクセス リストに名前を付けます。 • このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要のあるトラフィックと IPsec セキュリティで保護する必要のないトラフィックを判別します。
ステップ 5	**set peer** {*hostname* | *ip-address*} 例： `Device(config-crypto-m)# set-peer 192.168.101.1`	リモート IPsec ピアを指定します。これは、IPsec 保護されたトラフィックの転送先となるピアです。 • 複数のリモート ピアに対して、同じ作業を繰り返します。
ステップ 6	**crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*} 例： `Device(config-crypto-m)# set security-association dummy seconds 5`	ダミー パケットの生成を有効にします。これらのダミー パケットは、クリプト マップ内で作成されたすべてのフローに対して生成されます。
ステップ 7	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] 例： `Device(config-crypto-m)# set transform-set aesset`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。 • 複数のトランスフォーム セット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。

	コマンドまたはアクション	目的
ステップ 8	**set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**} 例： `Device (config-crypto-m)# set security-association lifetime seconds 2700`	（任意）クリプト マップ エントリの SA ライフタイムを指定します。 • デフォルトでは、クリプト マップの SA はグローバル ライフタイムに従ってネゴシエーションされ、これはディセーブルにできます。
ステップ 9	**set security-association level per-host** 例： `Device(config-crypto-m)# set security-association level per-host`	（任意）送信元と宛先ホストのペアごとに、個別の SA を確立するよう指定します。 • デフォルトで、1 つの IPsec「トンネル」を使用して、複数の送信元ホストと複数の宛先ホストのトラフィックを伝送できます。 **注意** 特定のサブネット間の複数のストリームによって急速にリソースが消費される可能性があるので、このコマンドは注意して使用してください。
ステップ 10	**set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**] 例： `Device(config-crypto-m)# set pfs group14`	（任意）IPsec がこのクリプト マップ エントリの新しい SA を要求するときに Password Forward Secrecy（PFS）を要求するか、IPsec ピアから受信する要求に PFS を含めるように要求するかを指定します。 • グループ 1 は、768 ビット Diffie-Hellman（DH）識別子を指定します（デフォルト）。（非推奨）。 • グループ 2 は、1024 ビット DH 識別子を指定します。（非推奨）。 • グループ 5 は、1536 ビット DH 識別子を指定します。（非推奨） • グループ 14 は、2048 ビット DH 識別子を指定します。 • グループ 15 は、3072 ビット DH 識別子を指定します。 • グループ 16 は、4096 ビット DH 識別子を指定します。 • グループ 19 は、256 ビット Elliptic Curve DH（ECDH）識別子を指定します。 • グループ 20 は、384 ビット ECDH 識別子を指定します。

	コマンドまたはアクション	目的
		• グループ 24 は、2048 ビット DH/DSA 識別子を指定します。 • デフォルトでは、PFS は要求されません。このコマンドでグループが指定されなかった場合は、グループ 1 がデフォルトとして使用されます。
ステップ 11	**end** 例： `Device(config-crypto-m)# end`	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Device# show crypto map`	クリプト マップ コンフィギュレーションを表示します。

トラブルシューティングのヒント

特定の設定変更は、それ以後の SA をネゴシエーションする場合にだけ有効になります。新しい設定をすぐに有効にする場合は、既存の SA が変更後の設定で再確立されるように、これらの SA を消去する必要があります。ルータが活発に IPsec トラフィックを処理する場合は、設定変更によって影響を受ける SA データベースの一部だけを消去します（つまり、所定のクリプト マップ セットで確立されている SA だけを消去します）。大規模な変更を行う場合や、ルータが他の IPsec トラフィックをほとんど処理しない場合を除いて、SA データベースを完全に消去しないでください。

IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベースが完全に消去され、アクティブなセキュリティ セッションも消去されてしまいます）。

次の作業

スタティック クリプトマップを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。この作業を完了するには、インターフェイスへのクリプトマップセットの適用 （28 ページ） を参照してください。

ダイナミック クリプト マップの作成

ダイナミック クリプト マップ エントリにより、IPsec SA を確立できるトラフィックを制限するクリプト アクセス リストを指定します。トラフィックのフィルタリング中、アクセス リストを指定しないダイナミック クリプトマップ エントリは、無視されます。ダイナミック クリプトマップエントリに空のアクセスリストが含まれていると、トラフィックが廃棄されます。クリプト マップ セットにダイナミック クリプトマップ エントリが 1 つしかない場合、クリプト マップ セットは許容範囲内のトランスフォーム セットを指定する必要があります。

このタスクは、SA の確立に IKE を使用するダイナミック クリプト マップ エントリを作成するために実行します。

（注） IPv6 アドレスは、ダイナミック クリプト マップではサポートされません。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
4. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
5. **match address** *access-list-id*
6. **set peer** {*hostname* | *ip-address*}
7. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}
8. **set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
9. **exit**
10. **exit**
11. **show crypto dynamic-map** [**tag** *map-name*]
12. **configure terminal**
13. **crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* [**discover**]
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* 例： `Device(config)# crypto dynamic-map test-map 1`	ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] 例： `Device(config-crypto-m)# set transform-set aesset`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。 • 複数のトランスフォーム セット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。これは、ダイナミック クリプト マップ エントリで必要とされる唯一の設定文です。
ステップ 5	**match address** *access-list-id* 例： `Device(config-crypto-m)# match address 101`	（任意）拡張アクセス リストのリスト番号またはリスト名を指定します。 • このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと、IPsec セキュリティで保護しないトラフィックを決定します。 （注） ダイナミック クリプトマップでは、アクセス リストの使用は任意ですが、使用することを強く推奨します。 • アクセスリストが設定されている場合、IPsec ピアによって提示されるデータフロー ID は、このクリプトアクセスリストの **permit** ステートメントの範囲内である必要があります。 • アクセス リストが設定されていない場合、デバイスは、IPsec ピアが提示したデータ フロー ID を受け入れます。ただし、アクセス リストが設定されていても指定されたアクセス リストが存在しない、あるいは空である場合、デバイスはすべてのパケットを廃棄します。これは、アクセス リストを指定する必要のあるスタティック クリプト マップと同様です。 • アクセスリストはネゴシエーションだけでなくパケットフィルタリングでも使用されるため、**any** キーワードをアクセスリストで使用する場合には注意が必要です。 • 一致アドレスを設定する必要があります。設定しない場合、パケットがクリアテキスト（暗号解除されて）で送信されるため、動作が不安定になり、TED をイネーブルにできません。

	コマンドまたはアクション	目的
ステップ 6	**set peer** {*hostname* | *ip-address*} 例： `Device(config-crypto-m)# set peer 192.168.101.1`	（任意）リモート IPsec ピアを指定します。リモート ピアが複数ある場合、このステップを繰り返します。 （注） ダイナミック クリプト マップ エントリでは、これを設定することはまれです。ダイナミック クリプト マップ エントリは、多くの場合、未知のリモート ピアで使用されます。
ステップ 7	**set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**} 例： `Device(config-crypto-m)# set security-association lifetime seconds 7200`	（任意）IP セキュリティ SA をネゴシエーションするときに使用されるグローバル ライフタイム値を上書きします（特定のクリプト マップ エントリの場合）。 （注） 高帯域幅環境でのキーの再生成時にパケット損失が発生する可能性を最小限にするには、大量のライフタイム有効期限によってトリガーされるキーの再生成要求をディセーブルにできます。
ステップ 8	**set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**] 例： `Device(config-crypto-m)# set pfs group14`	（任意）IPsec がこのクリプトマップエントリの新しい SA を要求した場合、PFS を要求するように、または IPsec ピアから受信する要求に PFS が含まれることを要求するように指定します。 • グループ 1 は、768 ビット Diffie-Hellman（DH）識別子を指定します（デフォルト）。（非推奨）。 • グループ 2 は、1024 ビット DH 識別子を指定します。（非推奨）。 • グループ 5 は、1536 ビット DH 識別子を指定します。（非推奨） • グループ 14 は、2048 ビット DH 識別子を指定します。 • グループ 15 は、3072 ビット DH 識別子を指定します。 • グループ 16 は、4096 ビット DH 識別子を指定します。 • グループ 19 は、256 ビット Elliptic Curve DH（ECDH）識別子を指定します。

	コマンドまたはアクション	目的
		• グループ 20 は、384 ビット ECDH 識別子を指定します。 • グループ 24 は、2048 ビット DH/DSA 識別子を指定します。 • デフォルトでは、PFS は要求されません。このコマンドでグループが指定されなかった場合は、**group1** がデフォルトとして使用されます。
ステップ 9	**exit** 例： `Device(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto dynamic-map** [**tag** *map-name*] 例： `Device# show crypto dynamic-map`	（任意）ダイナミック クリプト マップに関する情報を表示します。
ステップ 12	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* [**discover**] 例： `Device(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map discover`	（任意）クリプト マップ セットにダイナミック クリプト マップを追加します。 • クリプト マップ セット内のプライオリティの最も低いエントリに、ダイナミック マップを参照するクリプト マップ エントリを設定する必要があります。 （注） TED を有効にするには、**discover** キーワードを入力する必要があります。
ステップ 14	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

トラブルシューティングのヒント

特定の設定変更は、それ以後の SA をネゴシエーションする場合にだけ有効になります。新しい設定をすぐに有効にする場合は、既存の SA が変更後の設定で再確立されるように、これらの SA を消去する必要があります。ルータが活発に IPsec トラフィックを処理する場合は、設定変更によって影響を受ける SA データベースの一部だけを消去します（つまり、所定のクリプト マップ セットで確立されている SA だけを消去します）。大規模な変更を行う場合や、ルータが最小の IPsec トラフィックを処理している場合を除いて、SA データベース全体のクリアを予約しないでください。

IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベースが完全に消去され、アクティブなセキュリティ セッションも消去されてしまいます）。

次の作業

クリプトマップセットを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプトマップセットを適用する必要があります。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用 （28 ページ） 」を参照してください。

手動による SA を確立するためのクリプト マップ エントリの作成

このタスクは、クリプト マップ エントリを作成して手動 SA を確立するため（つまり、SA の確立に IKE が使用されない場合）に実行します。IPv6 クリプトマップエントリを作成するには、**crypto map** コマンドで **ipv6** キーワードを使用する必要があります。IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** [**ipv6**] *map-name seq-num* [**ipsec-manual**]
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name*
7. 次のいずれかを実行します。
   - **set session-key inbound ah** *spi hex-key-string*
   - **set session-key outbound ah** *spi hex-key-string*
8. 次のいずれかを実行します。
   - **set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
   - **set session-key outbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
9. **exit**
10. **exit**
11. **show crypto map** [**interface** *interface* | **tag** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-manual**] 例： `Device(config)# crypto map mymap 10 ipsec-manual`	作成または変更するクリプト マップ エントリを指定して、クリプト マップ コンフィギュレーション モードを開始します。 • IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。
ステップ 4	**match address** *access-list-id* 例： `Device(config-crypto-m)# match address 102`	このクリプトマップエントリに照らして、IPsec で保護するトラフィックと、IPsec で保護しないトラフィックを決定する IPsec アクセス リストに名前を付けます • IKE を使用しない場合、アクセスリストは **permit** エントリを 1 つだけ指定できます。
ステップ 5	**set peer** {*hostname* | *ip-address*} 例： `Device(config-crypto-m)# set peer 10.0.0.5`	リモート IPsec ピアを指定します。これは、IPsec 保護されたトラフィックの転送先となるピアです • IKE を使用しない場合、ピアを 1 つだけ指定できます。
ステップ 6	**set transform-set** *transform-set-name* 例： `Device(config-crypto-m)# set transform-set someset`	使用するトランスフォーム セットを指定します。 • これは、リモート ピアの対応するクリプトマップ エントリで指定したトランスフォーム セットと同じである必要があります。 （注） IKE を使用しない場合、トランスフォーム セットを 1 つだけ指定できます。
ステップ 7	次のいずれかを実行します。 • **set session-key inbound ah** *spi hex-key-string* • **set session-key outbound ah** *spi hex-key-string* 例：	指定されたトランスフォーム セットに AH プロトコルが含まれている場合、保護対象の着信および発信トラフィックに適用する AH セキュリティ パラメータ インデックス（SPI）およびキーを設定します

	コマンドまたはアクション	目的

	`Device(config-crypto-m)# set session-key inbound ah 256 9876543210987654987654321098765 4`
	例：
	`Device(config-crypto-m)# set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc`
		• 保護するトラフィックに使用する AH セキュリティ アソシエーションを手動で指定します。

ステップ 8	次のいずれかを実行します。
	• **set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
	• **set session-key outbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
	例：
	`Device(config-crypto-m)# set session-key inbound esp 256 cipher 0123456789012345`
	例：
	`Device(config-crypto-m)# set session-key outbound esp 256 cipher abcdefabcdefabcd`
		指定されたトランスフォーム セットに ESP プロトコルが含まれている場合、保護対象の着信および発信トラフィックに適用する Encapsulating Security Payload（ESP）セキュリティ パラメータ インデックス（SPI）およびキーを設定します。
		または
		トランスフォーム セットに ESP 暗号化アルゴリズムが含まれている場合は、暗号キーを指定します。トランスフォーム セットに ESP 認証アルゴリズムが含まれている場合は、認証キーを指定します。
		• 保護するトラフィックに使用する ESP セキュリティ アソシエーションを手動で指定します。

ステップ 9	**exit** 例： `Device(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Device# show crypto map`	クリプト マップ コンフィギュレーションを表示します。

トラブルシューティングのヒント

手動で確立された SA の場合、変更を有効にするために SA を消去し、再初期化する必要があります。IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベース全体がクリアされ、アクティブなセキュリティ セッションもクリアされてしまいます）。

次の作業

クリプトマップセットを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプトマップセットを適用する必要があります。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用 （28 ページ）」を参照してください。

インターフェイスへのクリプト マップ セットの適用

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。インターフェイスにクリプト マップ セットを適用すると、デバイスに対して、トラフィックをクリプトマップで保護する代わりに、インターフェイスのトラフィックをクリプトマップセットに対して評価し、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するように指示されます。

インターフェイスにクリプト マップを適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **crypto map** *map-name*
5. **exit**
6. **crypto map** *map-name* **local-address** *interface-id*
7. **exit**
8. **show crypto map** [**interface** *interface*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type/number* 例： `Device(config)# interface FastEthernet 0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**crypto map** *map-name* 例： `Device(config-if)# crypto map mymap`	インターフェイスに対してクリプト マップ セットを適用します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**crypto map** *map-name* **local-address** *interface-id* 例： `Device(config)# crypto map mymap local-address loopback0`	（任意）冗長インターフェイスが同じローカルアイデンティティを使用して、同じクリプトマップを共有できるようにします。
ステップ 7	**exit** 例： `Device(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了します。
ステップ 8	**show crypto map** [**interface** *interface*] 例： `Device# show crypto map`	（任意）クリプト マップ コンフィギュレーションを表示します。

IPsec VPN の設定例

例：AES ベースのスタティック暗号マップの設定

この例は、スタティック クリプト マップを設定し、暗号化方式として AES を定義する方法を示しています。

```
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
 lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
 mode transport
!
crypto map aesmap 10 ipsec-isakmp
 set peer 10.0.110.1
 set transform-set aesset
 match address 120
!
!
!
voice call carrier capacity active
!
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
 ip address 10.0.110.2 255.255.255.0
 ip nat outside
 no ip route-cache
 no ip mroute-cache
 duplex auto
```

```
 speed auto
 crypto map aesmap
!
interface Serial0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 10.0.110.1 255.255.255.0
 ip nat inside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
ip nat inside source list 110 interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.5.1.1
ip route 10.0.110.0 255.255.255.0 FastEthernet0/0
ip route 172.18.124.0 255.255.255.0 10.5.1.1
ip route 172.18.125.3 255.255.255.255 10.5.1.1
ip http server
!
!
access-list 110 deny   ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
access-list 110 permit ip 10.0.110.0 0.0.0.255 any
access-list 120 permit ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
!
```

IPsec を使用した VPN のセキュリティの設定に関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IKE、IPsec、および PKI のコンフィギュレーション コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IKE 設定	「*Configuring Internet Key Exchange for IPsec VPNs*」

関連項目	マニュアル タイトル
Suite-B SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キー ペアの設定	「*Configuring Internet Key Exchange for IPsec VPNs*」
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	「*Configuring Internet Key Exchange Version 2 (IKEv2)*」
IKEv2 用の Suite-B の Elliptic Curve Digital Signature Algorithm（ECDSA）signature（ECDSA-sig）認証方式の設定	「*Configuring Internet Key Exchange Version 2 (IKEv2)*」
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	• 「*Configuring Internet Key Exchange for IPsec VPNs*」 • 「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」
PKI の証明書登録のための Suite-B サポート	「*PKI* の証明書登録の設定」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
なし	—

MIB

MIB	MIB のリンク
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』

RFC	タイトル
RFC 2402	『*IP Authentication Header*』
RFC 2403	『*The Use of HMAC-MD5-96 within ESP and AH*』
RFC 2404	『*The Use of HMAC-SHA-1-96 within ESP and AH*』
RFC 2405	『*The ESP DES-CBC Cipher Algorithm With Explicit IV*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet IP Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol (ISAKMP)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec を使用した VPN のセキュリティの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2 : IPsec VPN* のセキュリティ設定に関する機能情報

機能名	ソフトウェア リリース	機能情報
Advanced Encryption Standard		この機能により、新しい暗号化規格 AES に対するサポートが追加されます。AES は、DES の後継として開発された IPsec および IKE のプライバシー トランスフォームです。 この機能により、次のコマンドが変更されました。**crypto ipsec transform-set**、**encryption (IKE policy)**、**show crypto ipsec transform-set**、**show crypto isakmp policy**。
IOS ソフトウェア暗号での Suite-B のサポート		Suite-B には、IKE と IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートのサポートが追加されています。これは RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。 この機能により、**crypto ipsec transform-set** コマンドが変更されました。

（注） GetVPN 暗号マップは、IOS XE 16.9.1 以降のポートチャネル インターフェイスでサポートされています。

用語集

anti-replay：受信者が再送攻撃から自身を保護するために、古いパケットまたは重複するパケットを拒否できるセキュリティサービス。IPSec は、データ認証とシーケンス番号を組み合わせて使用することにより、このオプション サービスを提供します。Cisco IOS XE IPsec は、手動で確立された SA（IKE ではなく、設定によって確立された SA）を除いて、データ認証サービスを実行するときは必ずこのサービスを提供します。

data authentication：データの整合性および発信元の検証。データ認証は、整合性だけを意味する場合と、整合性と認証の両方の概念を意味する場合があります（ただし、データ発信元認証はデータの整合性に依存します）。

data confidentiality：保護されたデータが第三者に読み取られないようにするセキュリティサービス。

data flow：送信元アドレスまたはマスク、宛先アドレスまたはマスク、IP 次プロトコルフィールド、送信元および宛先ポートの組み合わせによって識別されるトラフィックの集まり。プロ

トコルフィールドおよびポートフィールドには **any** の値が含まれます。IPSec 保護はデータ フローに適用されます。

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）。IKE は、共有セキュリティ ポリシーを確立し、キーを必要とするサービス（IPSec など）のキーを認証します。IPSec トラフィックが通過する前に、各ルータ、ファイアウォール、およびホストはそのピアの ID を検証する必要があります。それには、事前共有キーを両ホストに手動で入力するか、CA サービスを使用します。

IPsec：IP Security（IP セキュリティ）。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPSec は、このようなセキュリティ サービスを IP レイヤで提供します。IPSec は IKE を使用して、プロトコルやアルゴリズムのネゴシエーションをローカル ポリシーに基づいて処理し、IPSec で使用される暗号キーや認証キーを生成します。IPSec では、一対のホスト間、一対のセキュリティ ゲートウェイ間、または一対のセキュリティ ゲートウェイとホストの間で 1 つ以上のデータ フローを保護できます。

peer：ここで使用する「ピア」とは、IPsec に参加するルータまたはその他のデバイスです。

PFS：Perfect Forward Secrecy。これは、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。

SA：Security Association（セキュリティ アソシエーション）。2 つ以上のエンティティが、特定のデータ フローにおいて安全に通信するために、特定のセキュリティ プロトコル（AH または ESP）と関連してセキュリティ サービスを使用する方法を記述します。トラフィックを保護するために、トランス フォームと共有秘密キーが使用されます。

SPI：Security Parameter Index（セキュリティ パラメータ インデックス）。これは、宛先 IP アドレスおよびセキュリティ プロトコルを組み合わせて、特定の SA を一意に識別する番号です。IKE を使用しない場合、SPI は、手動で各セキュリティ アソシエーションに指定されます。

transform：データ認証、データ機密性、およびデータ圧縮を実現するためにデータフローで実行される処理のリスト。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

tunnel：ここで使用する「トンネル」とは、2 つのピア間（2 台のルータなど）の安全な通信パスです。トンネル モードで IPsec を使用することではありません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。