インターネット キー エクスチェンジ バージョン 2

このモジュールには、基本および高度なインターネット キー エクスチェンジ バージョン 2（IKEv2）の情報と設定手順が含まれています。このモジュールの IKEv2 のタスクおよび設定例は、次のように分類されます。

- 基本の IKEv2：基本の IKEv2 コマンド、IKEv2 スマート デフォルト、基本の IKEv2 プロファイル、および IKEv2 キー リングに関する情報が示されています。
- 高度な IKEv2：グローバルな IKEv2 コマンドに関する情報と、IKEv2 スマート デフォルトのオーバーライド方法が示されています。

（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。

インターネット キー交換バージョン 2 の設定に関する前提条件

「Configuring Security for VPNs with IPsec」モジュールで説明している概念および作業を理解している必要があります。

インターネット キー エクスチェンジ バージョン 2 の設定に関する制約事項

特定のプラットフォーム上でサポートされないオプションを設定することはできません。たとえば、セキュリティ プロトコルでハードウェア クリプト エンジンの機能が重要である場合、エクスポート可能でないイメージ内で Triple Data Encryption Standard（3DES）または Advanced Encryption Standard（AES）の各タイプの暗号化トランスフォームを指定できず、暗号エンジンでサポートされない暗号化アルゴリズムを指定できません。

インターネット キー エクスチェンジ バージョン 2 に関する情報

IKEv2 のサポート対象規格

シスコでは、インターネット キー エクスチェンジ バージョン 2（IKEv2）で使用するための IP セキュリティ（IPsec）プロトコル規格を実装しています。

（注） DES または MD5（HMAC バリアントを含む）の使用は、現在推奨されていません。代わりに、AES および SHA-256 を使用してください。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。

IKEv2 で実装されるコンポーネント技術は、次のとおりです。

- AES-CBC：高度暗号化規格暗号ブロック連鎖（AES-CBC）。
- SHA（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）。
- Diffie-Hellman：公開キー暗号法プロトコル。
- DES：データ暗号規格（現在は推奨されていません）。

- MD5（HMAC（ハッシュベースのメッセージ認証コード）バリアント）：メッセージ ダイジェスト アルゴリズム 5（現在は推奨されていません）。

サポートされる規格およびコンポーネント技術の詳細については、『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の『Configuring Internet Key Exchange for IPsec VPNs』モジュールにある「Supported Standards for Use with IKE」の項を参照してください。

IKEv2 の利点

デッド ピア検出とネットワーク アドレス変換トラバーサル

インターネット キー エクスチェンジ バージョン 2（IKEv2）にはデッド ピア検出（DPD）とネットワーク アドレス変換トラバーサル（NAT-T）のサポートが組み込まれています。

証明書の URL

証明書はIKEv2パケット内で送信されるのではなくURLとハッシュを通じて参照できるため、フラグメンテーションを回避できます。

DoS 攻撃の復元力

IKEv2は、要求者を確認するまで要求を処理しません。これにより、偽の場所から大量の暗号化（高コスト）処理を実行するようにスプーフィングされる可能性があるIKEv1でのサービス妨害（DoS）の問題にある程度対処しています。

EAP のサポート

IKEv2 では認証に Extensible Authentication Protocol（EAP）を使用できます。

複数の暗号エンジン

ネットワークに IPv4 と IPv6 の両方のトラフィックがあり、複数の暗号エンジンがある場合、次のいずれかの設定オプションを選択します。

- 1 つのエンジンで IPv4 トラフィックを処理し、他方のエンジンで IPv6 トラフィックを処理する。
- 1 つのエンジンで IPv4 と IPv6 の両方のトラフィックを処理する。

信頼性と状態管理（ウィンドウイング）

IKEv2 では、信頼性を提供するためにシーケンス番号と確認が使用され、エラー処理ロジスティックと共有状態管理が要求されます。

インターネット キー エクスチェンジ バージョン 2 CLI の構成

IKEv2 プロポーザル

インターネット キー エクスチェンジ バージョン 2（IKEv2）のプロポーザルは、IKE_SA_INIT 交換の一部としてインターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（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コレクションです。ネゴシエーションで使用されるトランスフォームのタイプは、次のとおりです。

- 暗号化アルゴリズム
- 整合性アルゴリズム
- Pseudo-Random Function（PRF）アルゴリズム
- デフィーヘルマン（DH）グループ

デフォルト IKEv2 プロポーザルについては、「IKEv2 スマート デフォルト」の項を参照してください。デフォルト IKEv2 プロポーザルをオーバーライドする方法および新しいプロポーザルを定義する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

IKEv2 ポリシー

IKEv2 ポリシーには、IKE_SA_INIT 交換での暗号化、整合性、PRF アルゴリズム、および DH グループのネゴシエーションに使用されるプロポーザルが含まれています。これには match 文を含めることができ、ネゴシエーション時にポリシーを選択するための選択基準として使用されます。

デフォルト IKEv2 ポリシーについては、「IKEv2 スマート デフォルト」の項を参照してください。デフォルト IKEv2 ポリシーをオーバーライドする方法および新しいポリシーを定義する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

IKEv2 プロファイル

IKEv2 プロファイルは、IKE SA のネゴシエーション可能でないパラメータ（ローカル ID またはリモート ID および認証方式）と、そのプロファイルと一致する認証相手が使用できるサービスのリポジトリです。IKEv2 プロファイルは、発信側の暗号マップまたは IPsec プロファイルのいずれかにアタッチされる必要があります。IKEv2 プロファイルは、応答側では必須ではありません。

IKEv2 キー リング

IKEv2 キー リングは対称および非対称の事前共有キーのリポジトリであり、IKEv1 キー リングとは無関係です。IKEv2 キー リングは 1 つの IKEv2 プロファイルと関連付けられるため、その IKEv2 プロファイルに一致する一連のピアをサポートします。IKEv2 キー リングは、関連付けられた IKEv2 プロファイルから VPN ルーティングおよび転送（VRF）コンテキストを取得します。

IKEv2 スマート デフォルト

IKEv2 スマート デフォルト機能は、ほとんどの使用例に対応することで FlexVPN 設定を最小化します。IKEv2 スマートデフォルトは特定の使用例向けにカスタマイズできますが、これはお勧めしません。

デフォルト IKEv2 構造を変更する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

次のルールが IKEv2 スマート デフォルト機能に適用されます。

1. デフォルト設定は、**default** をキーワードとして指定して引数を指定しない、対応する **show** コマンドで表示されます。たとえば、**show crypto ikev2 proposal default** コマンドではデフォルト IKEv2 プロポーザルが表示され、**show crypto ikev2 proposal** コマンドではユーザー設定されたプロポーザルと共にデフォルト IKEv2 プロポーザルが表示されます。
2. デフォルト設定は、**show running-config all** コマンドで表示されます。**show running-config** コマンドでは表示されません。
3. **show running-config all** コマンドで表示されるデフォルト設定を変更できます。
4. コマンドの **no** 形式（**no crypto ikev2 proposal default** など）を使用して、デフォルト設定を無効にすることができます。無効化されたデフォルト設定はネゴシエーションで使用されませんが、設定は **show running-config** コマンドで表示されます。無効化されたデフォルト設定では、ユーザー変更が失われてシステム設定値が復元されます。
5. デフォルト設定は、コマンドのデフォルト形式（**default crypto ikev2 proposal** など）を使用すると再度有効にすることができ、システム設定値が復元されます。
6. デフォルト トランスフォーム セットのデフォルト モードは、トランスポートです。その他すべてのトランスフォーム セットのデフォルト モードは、トンネルです。

（注） MD5（HMAC バリアントを含む）や Diffie-Hellman（DH）グループ 1、2、および 5 の使用は、現在は推奨されていません。代わりに、SHA-256 および DH グループ 14 以降を使用してください。最新のシスコの暗号化の推奨事項の詳細については、『Next Generation Encryption』（NGE）のホワイト ペーパーを参照してください。

次の表に、IKEv2 スマートデフォルト機能によって有効化されるコマンドをデフォルト値と共に示します。

表 *1 : IKEv2* コマンドのデフォルト

コマンド名	デフォルト値

crypto ikev2 authorization policy	`Device# show crypto ikev2 authorization policy default`
	
	`IKEv2 Authorization policy: default`
	`route set interface`
	`route accept any tag: 1 distance: 2`

コマンド名	デフォルト値
crypto ikev2 proposal	Device# **show crypto ikev2 proposal** IKEv2 proposal: default Encryption: AES-CBC-256 Integrity: SHA512 SHA384 PRF: SHA512 SHA384 DH Group: DH_GROUP_256_ECP/Group 19 DH_GROUP_2048_MODP/Group 14 DH_GROUP_521_ECP/Group 21 DH_GROUP_1536_MODP/Group 5
crypto ikev2 policy	Device# **show crypto ikev2 policy default** IKEv2 policy: default Match fvrf: any Match address local: any Proposal: default

crypto ipsec profile	Device# **show crypto ipsec profile default**
	
	IPSEC profile default
	Security association lifetime: 4608000 kilobytes/3600 seconds
	Responder-Only (Y/N): N
	PFS (Y/N): N
	Transform sets={
	default: { esp-aes esp-sha-hmac },
	}

crypto ipsec transform-set	Device# **show crypto ipsec transform-set default** Transform set default: { esp-aes esp-sha-hmac } will negotiate = { Tunnel, },

（注） デフォルト IPsec プロファイルを使用する前に、**tunnel protection ipsec profile default** コマンドを使用してトンネル インターフェイスで **crypto ipsec profile** コマンドを明示的に指定します。

（注） 他の CLI への明示的なマッピングが必要な「デフォルト」キーワードは、YANG 設定で実行されているデバイスではサポートされていません。

IKEv2 Suite-B サポート

Suite-B は、暗号の近代化プログラムの一環として国家安全保障局によって交付された一連の暗号化アリゴリズムです。インターネット キー エクスチェンジ（IKE）および IPsec の Suite-B は、RFC 4869 で定義されます。Suite-B のコンポーネントは、次のとおりです。

- IKEv2 プロポーザルで設定された Advanced Encryption Standard（AES）の 128 ビット キーおよび 256 ビット キー。データ トラフィックの場合、AES は、IPsec トランスフォーム セットに設定されるガロア カウンタ モード（GCM）で使用する必要があります。
- IKEv2 プロファイルに設定された楕円曲線デジタル署名アルゴリズム（ECDSA）。
- IKEv2 プロポーザルおよび IPsec トランスフォーム セットに設定されたセキュア ハッシュ アルゴリズム 2（SHA-256 および SHA-384）。

Suite-B の要件は、IKE および IPSec で使用するために、暗号化アルゴリズムの 4 つのユーザー インターフェイス スイートで構成されています。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 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。

AES-GCM のサポート

認証済みの暗号化アルゴリズムは、暗号化と整合性の組み合わさった機能を提供します。このようなアルゴリズムは、連結モード アルゴリズムと呼ばれます。IOS 上における IKEv2 暗号としての AES-GCM サポート機能では、ガロア/カウンタ モードの Advanced Encryption Standard（AES-GCM）を追加することによって、IKEv2 プロトコルの暗号化メッセージに認証済みの暗号化アルゴリズムを使用できます。AES-GCM は、128 ビットおよび 256 ビットのキー サイズ（AES-GCM-128 および AES-GCM-256）をサポートします。

（注） 暗号化アルゴリズムが AES-GCM のみの場合、整合性アルゴリズムをプロポーザルに追加することはできません。

IKEv2 での自動トンネル モードのサポート

複数ベンダー シナリオで VPN ヘッドエンドを設定する場合は、ピアまたはレスポンダの技術的な詳細を認識しておく必要があります。たとえば、一部のデバイスは IPsec トンネルを使用しているが、他のデバイスは Generic Routing Encapsulation（GRE）または IPsec トンネルを使用している場合やトンネルが IPv4 または IPv6 の場合があります。最後のケースでは、インターネット キー エクスチェンジ（IKE）プロファイルと仮想テンプレートを設定する必要があります。

トンネル モード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセス インターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。この機能は、Cisco AnyConnect VPN Client や Microsoft Windows7 Client などのマルチベンダー リモート アクセスを集約しているデュアル スタック ハブ上で役に立ちます。

（注） トンネル モード自動選択機能は、レスポンダの設定のみを容易にします。トンネルはイニシエータに対して静的に設定する必要があります。

トンネル モードの自動選択機能は、IKEv2 プロファイル設定で **virtual-template** コマンドに **auto mode** キーワードを使用するとアクティブ化できます。

インターネット キー交換バージョン 2 の設定方法

基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定

暗号化インターフェイスで IKEv2 を有効にするには、インターネット キー エクスチェンジ バージョン 2（IKEv2）プロファイルをそのインターフェイスに適用される暗号マップまたは IPsec プロファイルにアタッチします。IKEv2 応答側では、この手順は任意です。

（注） IKEv1 と IKEv2 の違いは、IKEv1 はデバイス上のすべてのインターフェイスでグローバルに有効になっているため、個々のインターフェイスで IKEv1 を有効にする必要がないことです。

基本の IKEv2 構造を手動で設定するには、次のタスクを実行します。

IKEv2 キーリングの設定

このタスクは、ローカルまたはリモート認証方式が事前共有キーの場合に、IKEv2 キーリングを設定するために実行します。

IKEv2 キーリング キーは、ピア サブブロックを定義するピア コンフィギュレーション サブモードで設定する必要があります。IKEv2 キーリングには、複数のピア サブブロックを含めることができます。1 つのピア サブブロックには、ホスト名、ID、および IP アドレスの任意の組み合わせで識別される 1 つのピアまたはピア グループ用の単一の対称または非対称キー ペアが含まれています。

IKEv2 キーリングは IKEv1 キーリングと無関係です。主な違いは次のとおりです。

- IKEv2 キーリングは、対称事前共有キーと非対称事前共有キーをサポートします。
- IKEv2 キーリングは、Rivest、Shamir、および Adleman（RSA）公開キーをサポートしません。
- IKEv2 キーリングは、IKEv2 プロファイル内で指定され、ルックアップされないため、事前共有キー認証方式をネゴシエートするために MM1 の受信時にキーがルックアップされる IKEv1 とは異なります。IKEv2 では、認証方式がネゴシエートされません。

- IKEv2 キーリングは、設定時に VPN ルーティングおよび転送（VRF）と関連付けられません。IKEv2 キーリングの VRF は、そのキーリングを参照している IKEv2 プロファイルの VRF です。
- 複数のキー リングを指定できる IKEv1 プロファイルとは異なり、IKEv2 プロファイルでは 1 つのキー リングを指定できます。
- 同じキーが別々のプロファイルと一致するピア全体で共有されている場合は、1 つのキーリングを複数の IKEv2 プロファイルで指定できます。
- IKEv2 キーリングは 1 つ以上のピア サブブロックとして構造化されます。

IKEv2 イニシエータでは、ピアのホスト名またはアドレスを使用してその順に IKEv2 キーリング キー ルックアップが実行されます。IKEv2 レスポンダでは、ピアの IKEv2 ID またはアドレスを使用してその順にキー ルックアップが実行されます。

（注） 複数のピアで同じ ID を設定することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring** *keyring-name*
4. **peer** *name*
5. **description** *line-of-description*
6. **hostname** *name*
7. **address** {*ipv4-address* [*mask*] | *ipv6-address prefix*}
8. **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
9. **pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string*
10. **end**

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 keyring** *keyring-name* 例：	IKEv2 キーリングを定義し、IKEv2 キーリング 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
	`Device(config)# crypto ikev2 keyring kyr1`	
ステップ 4	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 5	**description** *line-of-description* 例： `Device(config-ikev2-keyring-peer)# description this is the first peer`	（任意）ピアまたはピア グループを記述します。
ステップ 6	**hostname** *name* 例： `Device(config-ikev2-keyring-peer)# hostname host1`	ホスト名を使用してピアを指定します。
ステップ 7	**address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} 例： `Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0`	ピアの IPv4 アドレス、IPv6 アドレス、または範囲を指定します。 （注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。

ステップ 8	**identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
	例：
	`Device(config-ikev2-keyring-peer)# identity address 10.0.0.5`
		次の ID を使用して IKEv2 ピアを特定します。
		• 電子メール
		• 完全修飾ドメイン名（FQDN）。
		（注） キーリング設定で、ピアを識別するために FQDN が使用されている場合は、FQDN とともにピアの IP アドレスを使用します。
		`crypto ikev2 keyring key1`
		`peer headend-1`
		`address 1.1.1.1 >>>>>>>>>`
		`identity fqdn NFVIS-headend-1.cisco.com`
		`pre-shared-key Cisco123`
		• IPv4 アドレスまたは IPv6 アドレス
		• キー ID
		（注） ID は IKEv2 レスポンダ上のキー ルックアップにしか使用できません。

ステップ 9	**pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string* 例：	ピアの事前共有キーを指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-keyring-peer)# pre-shared-key local key1`	
ステップ 10	**end** 例： `Device(config-ikev2-keyring-peer)# end`	IKEv2 キーリング ピア コンフィギュレーション モードを終了して、特権EXECモードに戻ります。

次の作業

IKEv2 キー リングの設定後、IKEv2 プロファイルを設定します。詳細については、「IKEv2 プロファイルの設定（基本）」セクションを参照してください。

IKEv2 プロファイルの設定（基本）

このタスクは、IKEv2 プロファイル用の必須コマンドを設定するために実行します。

IKEv2 プロファイルは、IKE セキュリティ アソシエーション（SA）（ローカル ID またはリモート ID と認証方式など）のネゴシエーション不能パラメータと、そのプロファイルと一致する認証されたピアが使用可能なサービスのリポジトリです。IKEv2プロファイルは、設定して、IKEv2 イニシエータ上のクリプト マップと IPSec プロファイルのどちらかに関連付ける必要があります。プロファイルを暗号マップまたは IPsec プロファイルに関連付けるには、**set ikev2-profile** *profile-name* コマンドを使用します。プロファイルの関連付けを解除するには、このコマンドの **no** 形式を使用します。

次のルールが match ステートメントに適用されます。

- IKEv2 プロファイルには、match identity ステートメントまたは match certificate ステートメントを含める必要があります。そうしないと、プロファイルが不完全と見なされ、使用されません。IKEv2 プロファイルには、複数の match identity ステートメントまたは match certificate ステートメントを含めることができます。
- IKEv2 プロファイルには、単一の match Front Door VPN routing and forwarding (FVRF) ステートメントを含める必要があります。
- プロファイルを選択すると、同じタイプの複数の match ステートメントが論理的に OR され、違うタイプの複数の match ステートメントが論理的に AND されます。
- match identity ステートメントと match certificate ステートメントは、同じタイプのステートメントと見なされ、OR されます。
- 重複したプロファイルの設定は、設定ミスと見なされます。複数のプロファイルが一致した場合は、どのプロファイルも選択されません。

IKEv2 プロファイルを表示するには、**show crypto ikev2 profile** *profile-name* コマンドを使用します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **description** *line-of-description*
5. **aaa accounting** {**psk** | **cert** | **eap**} *list-name*
6. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
7. **dpd** *interval retry-interval* {**on-demand** | **periodic**}
8. **dynamic**
9. **identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*}
10. **initial-contact force**
11. **ivrf** *name*
12. **keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
13. **lifetime** *seconds*
14. **match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}
15. **nat keepalive** *seconds*
16. **pki trustpoint** *trustpoint-label* [**sign** | **verify**]
17. **virtual-template** *number* **mode auto**
18. **shutdown**
19. **end**

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 モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
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 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	IKEv2プロファイルを定義し、IKEv2プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**description** *line-of-description* 例： `Device(config-ikev2-profile)# description This is an IKEv2 profile`	（任意）プロファイルを記述します。

	コマンドまたはアクション	目的
ステップ 5	**aaa accounting** {**psk** | **cert** | **eap**} *list-name* 例： `Device(config-ikev2-profile)# aaa accounting eap list1`	（任意）IPsec セッションの認証、認可、およびアカウンティング（AAA）アカウンティング方式リストを有効にします。 （注） **psk**、**cert**、または **eap** キーワードが指定されなかった場合は、ピア認証方式に関係なく、AAA アカウンティング方式リストが使用されます。
ステップ 6	**authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}} 例： `Device(config-ikev2-profile)# authentication local ecdsa-sig`	ローカルまたはリモートの認証方式を指定します。 • **rsa-sig**：認証方式として RSA-sig を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。 • **ecdsa-sig**：認証方式として ECDSA-sig を指定します。 • **eap**：リモート認証方式として EAP を指定します。 • **query-identity**：ピアに EAP ID を問い合わせます。 • **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。 （注） ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。
ステップ 7	**dpd** *interval retry-interval* {**on-demand** | **periodic**} 例： `Device(config-ikev2-profile)# dpd 30 6 on-demand`	この手順は任意です。（任意）プロファイルと一致したピアの Dead Peer Detection（DPD; デッドピア検出）をグローバルに設定します。デフォルトでは、Dead Peer Detection（DPD; デッドピア検出）は無効化されています。

	コマンドまたはアクション	目的
		（注） この手順の例では、着信 ESP トラフィックがない場合、最初の DPD が 30 秒後に送信されます。6 秒間（指定された再試行間隔）待機した後、DPD 再試行が 6 秒間隔でアグレッシブに 5 回送信されます。そのため、合計 66 秒（30 + 6 + 6 X 5 = 66）が経過すると、DPD によって暗号化セッションが切断されます。
ステップ 8	**dynamic** 例： `Device(config-ikev2-profile)# dynamic`	ダイナミック IKEv2 プロファイルを設定します。このキーワードは、Cisco IOS XE 17.2.1 リリースで導入されました。 （注） 動的プロファイルを設定する場合、コマンドラインインターフェイスを使用して、ローカルまたはリモートの認証とアイデンティティを設定することはできません。
ステップ 9	**identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# identity local email abc@example.com`	この手順は任意です。（任意）ローカル IKEv2 アイデンティティタイプを指定します。 （注） ローカル認証方式が事前共有キーの場合は、デフォルトのローカル ID が IP アドレスになります。ローカル認証方式が Rivest、Shamir、および Adleman（RSA）署名の場合は、デフォルトのローカル ID が識別名になります。
ステップ 10	**initial-contact force** 例： `Device(config-ikev2-profile)# initial-contact force`	初期連絡先通知が IKE_AUTH 交換で受信されなかった場合に、初期連絡先処理を強制します。
ステップ 11	**ivrf** *name* 例： `Device(config-ikev2-profile)# ivrf vrf1`	この手順は任意です。IKEv2 プロファイルがクリプトマップに適用されている場合に、ユーザー定義の VPN ルーティングおよび転送（VRF）またはグローバル VRF を指定します。 • IKEv2 プロファイルをトンネル保護に使用している場合は、トンネルインターフェイス上で内部 VRF（IVRF）を設定する必要があります。

	コマンドまたはアクション	目的
		（注） IVRF は、クリア テキスト パケット用の VRF を指定します。IVRF のデフォルト値は FVRF です。
ステップ 12	**keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] } 例： `Device(config-ikev2-profile)# keyring aaa keyring1 name-mangler mangler1`	ローカルまたはリモートの事前共有キー認証方式で使用する必要があるローカルまたは AAA ベースのキーリングを指定します。 （注） 1 つのキーリングしか指定することができません。ローカル AAA は AAA ベースの事前共有キーに対してサポートされません。 （注） リリースによっては、**local** キーワードと **name-mangler** *mangler-name* キーワード引数ペアを使用する必要があります。 （注） AAA を使用する場合、Radius アクセス要求のデフォルト パスワードは「cisco」です。パスワードを変更するには、**keyring** コマンド内で **password** キーワードを使用します。 （注） IKEv2 プロファイルからキーリングを削除するには、**no keyring** {**aaa** | **local** | **ppk**} *keyring-name* コマンドを使用します。
ステップ 13	**lifetime** *seconds* 例： `Device(config-ikev2-profile)# lifetime 1000`	IKEv2 SA のライフタイムを秒単位で指定します。
ステップ 14	**match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# match address local interface Ethernet 2/0`	match ステートメントを使用して、ピア用の IKEv2 プロファイルを選択します。
ステップ 15	**nat keepalive** *seconds* 例： `Device(config-ikev2-profile)# nat keepalive 500`	（任意）NAT キープアライブを有効にして、その期間を秒単位で指定します。 • デフォルトでは、NAT は無効になっています。

	コマンドまたはアクション	目的
ステップ 16	**pki trustpoint** *trustpoint-label* [**sign** | **verify**] 例： `Device(config-ikev2-profile)# pki trustpoint tsp1 sign`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。 （注） **sign** または **verify** キーワードが指定されていない場合、トラストポイントは署名と検証に使用されます。 （注） IKEv1 とは対照的に、証明書ベースの認証を成功させるためにトラストポイントを IKEv2 プロファイル内で設定する必要があります。このコマンドが設定内に存在しない場合は、グローバルに設定されたトラストポイントのフォールバックが存在しません。トラストポイント設定は IKEv2 イニシエータおよびレスポンダに適用されます。
ステップ 17	**virtual-template** *number* **mode auto** 例： `Device(config-ikev2-profile)# virtual-template 1 mode auto`	この手順は任意です。仮想アクセスインターフェイス（VAI）のクローニング用の仮想テンプレートを指定します。 • **mode auto**：トンネルモード自動選択機能を有効にします。 （注） IPsec ダイナミック仮想トンネル インターフェイス（DVTI）では、仮想テンプレートを IKEv2 セッションが開始されない IKEv2 プロファイル内で指定する必要があります。
ステップ 18	**shutdown** 例： `Device(config-ikev2-profile)# shutdown`	（任意）IKEv2 プロファイルをシャット ダウンします。
ステップ 19	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル 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。

高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定

この項では、グローバル IKEv2 CLI 構造について説明します。また、IKEv2 のデフォルト CLI 構造をオーバーライドする方法についても説明します。IKEv2 スマートデフォルトは、ほとん

どの使用例をサポートします。そのため、デフォルトで対応されない特定の使用例に必要な場合にのみ、デフォルトをオーバーライドすることをお勧めします。

高度な IKEv2 CLI 構造を設定するには、次のタスクを実行します。

グローバル IKEv2 オプションの設定

この作業は、ピアに依存しないグローバル IKEv2 オプションを設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 certificate-cache** *number-of-certificates*
4. **crypto ikev2 cookie-challenge** *number*
5. **crypto ikev2 diagnose error** *number*
6. **crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**}
7. **crypto ikev2 http-url cert**
8. **crypto ikev2 limit** { **max-in-negotiation-sa** *limit* | **max-sa** *limit*}
9. **crypto ikev2 nat keepalive** *interval*
10. **crypto ikev2 window** *size*
11. **crypto logging ikev2**
12. **end**

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 certificate-cache** *number-of-certificates* 例： `Device(config)# crypto ikev2 certificate-cache 750`	HTTP URL から取得した証明書を保存するためのキャッシュ サイズを定義します。
ステップ 4	**crypto ikev2 cookie-challenge** *number* 例： `Device(config)# crypto ikev2 cookie-challenge 450`	ハーフオープン セキュリティ アソシエーション（SA）の数が設定された値を超えた場合にだけ、IKEv2 cookie チャレンジを有効にします。 • Cookie チャレンジは、デフォルトで無効化されています。

	コマンドまたはアクション	目的
ステップ 5	**crypto ikev2 diagnose error** *number* 例： `Device(config)# crypto ikev2 diagnose error 500`	IKEv2 エラーの診断を有効にして終了パス データベースのエントリ数を定義します。 • IKEv2 エラー診断はデフォルトでは無効化されています。
ステップ 6	**crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**} 例： `Device(config)# crypto ikev2 dpd 30 6 on-demand`	ピアを次のようにライブでチェックできるようにします。 • Dead Peer Detection（DPD：デッドピア検出）はデフォルトでは無効化されています。 （注） この手順の例では、着信 ESP トラフィックがない場合、最初の DPD が 30 秒後に送信されます。6 秒間（指定された再試行間隔）待機した後、DPD 再試行が 6 秒間隔でアグレッシブに 5 回送信されます。そのため、合計 66 秒（30 + 6 + 6 X 5 = 66）が経過すると、DPD によって暗号化セッションが切断されます。
ステップ 7	**crypto ikev2 http-url cert** 例： `Device(config)# crypto ikev2 http-url cert`	HTTP CERT サポートを有効にします。 • HTTP CERT は、デフォルトで無効化されています。
ステップ 8	**crypto ikev2 limit** { **max-in-negotiation-sa** *limit* | **max-sa** *limit*} 例：	コネクション アドミッション制御（CAC）を有効にします。 • コネクション アドミッション制御はデフォルトで有効化されています。
ステップ 9	**crypto ikev2 nat keepalive** *interval* 例： `Device(config)# crypto ikev2 nat keepalive 500`	ネットワーク アドレス変換（NAT）のキープアライブを有効にして、インターネットキーエクスチェンジ（IKE）ピア間に NAT がある場合に、任意のトラフィックが欠けることによる NAT の削除を防ぎます。 • NAT キープアライブはデフォルトで無効化されています。
ステップ 10	**crypto ikev2 window** *size* 例： `Device(config)# crypto ikev2 window 15`	送信時に複数の IKEv2 要求と応答のピアを許可します。 • デフォルトのウィンドウ サイズは 5 です。

	コマンドまたはアクション	目的
ステップ 11	**crypto logging ikev2** 例： `Device(config)# crypto logging ikev2`	IKEv2 Syslog メッセージを有効にします。 • デフォルトでは、IKEv2 syslog メッセージは無効化されています。
ステップ 12	**end** 例： `Device(config)# end`	グローバル 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。

IKEv2 フラグメンテーションの設定

このタスクを実行して、大規模な IKEv2 パケットのラグメンテーションを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 fragmentation** [**mtu** *mtu-size*]
4. **end**

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 fragmentation** [**mtu** *mtu-size*] 例： `Device(config)# crypto ikev2 fragmentation mtu 100`	IKEv2 フラグメンテーションを設定します。 • MTU の範囲は 96 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。 （注） MTU のサイズは、IP または UDP でカプセル化された IKEv2 パケットを示します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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。

IKEv2 プロポーザルの設定

デフォルトの IKEv2 プロポーザルについては、「IKEv2 スマート デフォルト」の項を参照してください。

このタスクは、デフォルト プロポーザルを使用しない場合に、デフォルト IKEv2 プロポーザルをオーバーライドするか、手動でプロポーザルを設定するために実行します。

IKEv2 プロポーザルは、IKE_SA_INIT 交換の一部として IKEv2 SA のネゴシエーションに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 ポリシーにアタッチされていない場合は、デフォルト IKEv2 ポリシー内のデフォルト プロポーザルがネゴシエーションで使用されます。

（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。

IKEv2 プロポーザルは **crypto isakmp policy** 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal** *name*
4. **encryption** *encryption-type...*
5. **integrity** *integrity-type...*
6. **group** *group-type...*
7. **prf** *prf-algorithm*
8. **end**
9. **show crypto ikev2 proposal** [*name* | **default**]

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）。

	コマンドまたはアクション	目的
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** *name* 例： `Device(config)# crypto ikev2 proposal proposal1`	デフォルト IKEv2 プロポーザルをオーバーライドして、IKEv2 プロポーザル名を定義し、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。
ステップ 4	**encryption** *encryption-type...* 例： `Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-192`	1 つまたは複数の暗号化タイプのトランスフォームを指定します。タイプは次のとおりです。 • **3des**（非推奨） • **aes-cbc-128** • **aes-cbc-192** • **aes-cbc-256** • **aes-gcm-128** • **aes-gcm-256**
ステップ 5	**integrity** *integrity-type...* 例： `Device(config-ikev2-proposal)# integrity sha1`	次のように、整合性アルゴリズム タイプの 1 つ以上のトランスフォームを指定します。 • **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） • **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。 • **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。 （注） 暗号化タイプとして Advanced Encryption Standard（AES）in Galois/Counter Mode（AES GCM）を指定した場合は、整合性アルゴリズム タイプを指定できません。

	コマンドまたはアクション	目的
ステップ 6	**group** *group-type...* 例： `Device(config-ikev2-proposal)# group 14`	Diffie-Hellman（DH）グループ ID を指定します。 • デフォルトの DH グループ識別子は、IKEv2 プロポーザル内のグループ 2 および 5 です。 • **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。 • **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 グループを指定します。 選択するグループは、ネゴシエーション中の IPsec キーを保護するため、十分強力（十分なビット数がある）である必要があります。一般に受け入れられているガイドラインでは、2013 年以降（2030 年まで）は 2048 ビット グループの使用が推奨されています。このガイドラインを満たすために、グループ 14 とグループ 24 のどちらかを選択できます。より寿命の長いセキュリティ方式が必要な場合でも、楕円曲線暗号の使用をお勧めしますが、グループ 15 とグループ 16 も検討してください。
ステップ 7	**prf** *prf-algorithm* 例： `Device(config-ikev2-proposal)# prf sha256 sha512`	次のように、1 つ以上の擬似ランダム関数（PRF）アルゴリズムを指定します。 • **md5** • **sha1** • **sha256** • **sha384** • **sha512**

	コマンドまたはアクション	目的
		（注） この手順は、暗号化タイプが AES-GCM：**aes-gmc-128** または **aes-gmc-256** の場合に必須です。暗号化アルゴリズムが AES-GCM でない場合は、PRF アルゴリズムが指定された整合性アルゴリズムと同じになります。ただし、必要に応じて、PRF アルゴリズムを指定できます。
ステップ 8	**end** 例： `Device(config-ikev2-proposal)# end`	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 9	**show crypto ikev2 proposal** [*name* | **default**] 例： `Device# show crypto ikev2 proposal default`	（任意）IKEv2 プロポーザルを表示します。

次の作業

IKEv2 プロポーザルを作成した後、ポリシーと接続して、ネゴシエーションでプロポーザルを選択できるようにします。このタスクの完了について、詳細は「IKEv2 ポリシーの設定」セクションを参照してください。

IKEv2 ポリシーの設定

デフォルトの IKEv2 ポリシーについては、「IKEv2 スマート デフォルト」の項を参照してください。

このタスクは、デフォルト ポリシーを使用しない場合に、デフォルト IKEv2 ポリシーをオーバーライドするか、手動でポリシーを設定するために実行します。

IKEv2 ポリシーには、完全だと考えられる 1 つ以上のプロポーザルを含める必要があり、ネゴシエーション用のポリシーを選択するための選択基準として使用される match ステートメントを含めることができます。初期交換中に、ネゴシエートする SA のローカル アドレス（IPv4 または IPv6）と Front Door VRF（FVRF）がポリシーと照合され、プロポーザルが選択されます。

次のルールが match ステートメントに適用されます。

- match ステートメントを含まない IKEv2 ポリシーは、グローバル FVRF 内のすべてのピアと一致します。
- IKEv2 ポリシーには、match FVRF ステートメントを 1 つしか含めることができません。
- IKEv2 ポリシーには、match address local ステートメントを 1 つ以上含めることができます。
- ポリシーを選択すると、同じタイプの複数の match ステートメントが論理的に OR され、違うタイプの match ステートメントが論理的に AND されます。

- タイプが異なる match ステートメントの優先順位はありません。
- 重複したポリシーの設定は、設定ミスと見なされます。複数のポリシーが一致した場合は、最初のポリシーが選択されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 policy** *name*
4. **proposal** *name*
5. **match fvrf** {*fvrf-name* | **any**}
6. **match address local** {*ipv4-address* | *ipv6-address*}
7. **end**
8. **show crypto ikev2 policy** [*policy-name* | **default**]

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 policy** *name* 例： `Device(config)# crypto ikev2 policy policy1`	デフォルト IKEv2 ポリシーをオーバーライドして、IKEv2 ポリシー名を定義し、IKEv2 ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**proposal** *name* 例： `Device(config-ikev2-policy)# proposal proposal1`	このポリシーで使用する必要があるプロポーザルを指定します。 • プロポーザルは、一覧の順の優先順位になります。 （注） 少なくとも 1 つのプロポーザルを指定する必要があります。各プロポーザルを別々のステートメントに分けた追加のプロポーザルを指定できます。
ステップ 5	**match fvrf** {*fvrf-name*	**any**} 例： `Device(config-ikev2-policy)# match fvrf any`	（任意）ポリシーをユーザーが設定した FVRF または任意の FVRF に基づいて照合します。 • デフォルトはグローバル FVRF です。

	コマンドまたはアクション	目的
		（注） 任意の VRF と一致させるには、**match fvrf any** コマンドを明示的に設定する必要があります。FVRF には、IKEv2 パケットのネゴシエーションを行う VRF を指定します。
ステップ 6	**match address local** {*ipv4-address* | *ipv6-address*} 例： `Device(config-ikev2-policy)# match address local 10.0.0.1`	（任意）ローカル IPv4 または IPv6 アドレスに基づいてポリシーを照合します。 • デフォルトは、設定済みの FVRF 内のすべてのアドレスと一致します。
ステップ 7	**end** 例： `Device(config-ikev2-policy)# end`	IKEv2 ポリシー 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 policy** [*policy-name* | **default**] 例： `Device# show crypto ikev2 policy policy1`	（任意）IKEv2 ポリシーを表示します。

インターネット キー エクスチェンジ バージョン 2 の設定例

基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例

例：IKEv2 キー リングの設定

例：複数のピア サーバブロックを持つ IKEv2 キー リング

次の例は、複数のピア サブブロックを持つインターネット キー エクスチェンジ バージョン 2（IKEv2）キー リングを設定する方法を示します。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1
  address 209.165.200.225 255.255.255.224
  pre-shared-key key-1
 peer peer2
  description peer2
  hostname peer1.example.com
  pre-shared-key key-2
```

```
 peer peer3
  description peer3
  hostname peer3.example.com
  identity key-id abc
  address 209.165.200.228 255.255.255.224
  pre-shared-key key-3
```

例：IP アドレスに基づく対称型事前共有キーを使用した IKEv2 キー リング

次の例は、IP アドレスに基づく対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1
  address 209.165.200.225 255.255.255.224
  pre-shared-key key1
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer2
  description peer2
  address 209.165.200.228 255.255.255.224
  pre-shared-key key1
```

例：IP アドレスに基づく非対称型事前共有キーを使用した IKEv2 キー リング

次の例は、IP アドレスに基づく非対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1 with asymmetric keys
  address 209.165.200.225 255.255.255.224
  pre-shared-key local key1
  pre-shared-key remote key2
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer2
  description peer2 with asymmetric keys
  address 209.165.200.228 255.255.255.224
  pre-shared-key local key2
  pre-shared-key remote key1
```

例：ホスト名に基づく非対称型事前共有キーを使用した IKEv2 キー リング

次の例は、ホスト名に基づく非対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer host1
  description host1 in example domain
  hostname host1.example.com
  pre-shared-key local key1
  pre-shared-key remote key2
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer host2
  description host2 in abc domain
  hostname host2.example.com
  pre-shared-key local key2
  pre-shared-key remote key1
```

例：アイデンティティに基づく対称型事前共有キーを使用した IKEv2 キー リング

次の例は、アイデンティティに基づく対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。

```
crypto ikev2 keyring keyring-4
 peer abc
  description example domain
  identity fqdn example.com
  pre-shared-key abc-key-1
 peer user1
  description user1 in example domain
  identity email user1@example.com
  pre-shared-key abc-key-2
 peer user1-remote
  description user1 example remote users
  identity key-id example
  pre-shared-key example-key-3
```

例：ワイルドカード キーを使用した IKEv2 キー リング

次の例は、ワイルドカード キーを使用する IKEv2 キー リングの設定方法を示します。

```
crypto ikev2 keyring keyring-1
 peer cisco
  description example domain
  address 0.0.0.0 0.0.0.0
  pre-shared-key example-key
```

例：キー リングの照合

次の例は、キー リングの照合方法を示します。

```
crypto ikev2 keyring keyring-1
 peer cisco
  description example.com
  address 0.0.0.0 0.0.0.0
  pre-shared-key xyz-key
 peer peer1
  description abc.example.com
  address 10.0.0.0 255.255.0.0
  pre-shared-key abc-key
 peer host1
  description host1@abc.example.com
  address 10.0.0.1
  pre-shared-key host1-example-key
```

ここに示す例では、ピア 10.0.0.1 を照合するキーは最初にワイルドカード キー example-key と一致し、次にプレフィックス キー example-key と一致し、最後にホスト キー host1-example-key と一致します。最適な一致である host1-example-key が使用されます。

```
crypto ikev2 keyring keyring-2
 peer host1
 description host1 in abc.example.com sub-domain
 address 10.0.0.1
 pre-shared-key host1-example-key
 peer host2
  description example domain
  address 0.0.0.0 0.0.0.0
  pre-shared-key example-key
```

ここに示す例では、ピア 10.0.0.1 を照合するキーは最初にホスト キー host1-abc-key と一致します。これが固有の一致であることから、これ以上の照合は実行されません。

例：プロファイルの設定

例：リモート ID で照合する IKEv2 プロファイル

次のプロファイルは、完全修飾ドメイン名（FQDN）example.com を使用して自身を特定し、トラストポイントリモートを使用して RSA 署名で認証するピアをサポートします。ローカルノードは、keyring-1 を使用する事前共有キーでノード自体を認証します。

```
crypto ikev2 profile profile2
 match identity remote fqdn example.com
 identity local email router2@example.com
 authentication local pre-share
 authentication remote rsa-sig
 keyring keyring-1
 pki trustpoint trustpoint-remote verify
 lifetime 300
 dpd 10 5 on-demand
 virtual-template 1
```

例：2 つのピアをサポートする IKEv2 プロファイル

次の例は、異なる認証方式を使用する 2 つのピアがサポートする、IKEv2 プロファイルの設定方法を示します。

```
crypto ikev2 profile profile2
 match identity remote email user1@example.com
 match identity remote email user2@example.com
 identity local email router2@cisco.com
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 keyring keyring-1
 pki trustpoint trustpoint-local sign
 pki trustpoint trustpoint-remote verify
 lifetime 300
 dpd 10 5 on-demand
 virtual-template 1
```

例：証明書および IKEv2 スマート デフォルトを使用するダイナミック ルーティングによる FlexVPN の設定

次の例に、トンネルを介したダイナミック ルーティングによるブランチデバイス（発信者側、スタティック仮想トンネルインターフェイス（sVTI）を使用）と中央デバイス（応答側、ダイナミック仮想トンネルインターフェイス（dVTI）を使用）との間の接続を示します。この例ではIKEv2 スマートデフォルトを使用し、認証は証明書（RSA 署名）を使用して実行されます。

（注） 推奨される RSA モジュラス サイズは 2048 です。

ピアは IKEv2 ID として FQDN を使用し、応答側の IKEv2 プロファイルは ID FQDN のドメインと一致します。

発信側（ブランチ デバイス）での設定は、次のとおりです。

```
hostname branch
ip domain name cisco.com
!
crypto ikev2 profile branch-to-central
 match identity remote fqdn central.cisco.com
 identity local fqdn branch.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
!
crypto ipsec profile svti
 set ikev2-profile branch-to-central
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile svti
!
interface Ethernet0/0
 ip address 10.0.0.101 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.101.1 255.255.255.0
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 172.16.0.0
 network 192.168.101.0
 no auto-summary
```

応答側（中央ルータ）での設定は、次のとおりです。

```
hostname central
ip domain name cisco.com
!
crypto ikev2 profile central-to-branch
 match identity remote fqdn domain cisco.com
 identity local fqdn central.cisco.com
```

```
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 virtual-template 1
!
interface Loopback0
 ip address 172.16.0.100 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.100.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 172.16.0.0
 network 192.168.100.0
 no auto-summary
```

高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例

例：プロポーザルの設定

例：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

次の例は、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プロポーザルの設定方法を示します。

```
crypto ikev2 proposal proposal-1
 encryption aes-cbc-128
 integrity sha1
 group 14
```

例：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

次の例は、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プロポーザルの設定方法を示します。

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

（注） シスコは現在、3DES、MD5（HMAC バリアント含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨していません。代わりに、AES、SHA-256、および DH グループ 14 以降を使用する必要があります。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。

ここに示す IKEv2 プロポーザル proposal-2 では、次の組み合わせのトランスフォームの優先順位リストに変換されます。

- aes-cbc-128, sha1, 14
- aes-cbc-192, sha1, 14

例：発信側と応答側の IKEv2 プロポーザル

次の例は、発信側と応答側の IKEv2 プロポーザルの設定方法を示します。発信側のプロポーザルは次のとおりです。

```
crypto ikev2 proposal proposal-1
 encryption aes-cbc-192 aes-cbc-128
 integrity sha-256 sha1
 group 14 24
```

応答側のプロポーザルは次のとおりです。

```
crypto ikev2 proposal proposal-2
 encryption aes-cbc-128 aes-cbc-192
 peer
 integrity sha1 sha-256
 group 24 14
```

選択したプロポーザルは次のようになります。

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

発信側と応答側に示されるプロポーザルでは、発信側と応答側では設定が競合します。この場合、発信側が応答側よりも優先されます。

例：ポリシーの設定

例：VRF およびローカル アドレスで照合する IKEv2 ポリシー

次の例は、IKEv2 ポリシーが VRF およびローカル アドレスで照合する方法を示します。

```
crypto ikev2 policy policy2
 match vrf vrf1
 match local address 10.0.0.1
 proposal proposal-1
```

例：グローバル VRF 内のすべてのピアを照合する複数のプロポーザルがある IKEv2 ポリシー

次の例は、複数のプロポーザルがある IKEv2 ポリシーがグローバル VRF 内のピアを照合する方法を示します。

```
crypto ikev2 policy policy2
 proposal proposal-A
 proposal proposal-B
 proposal proposal-B
```

例：任意の VRF 内のすべてのピアを照合する IKEv2 ポリシー

次の例は、任意の VRF 内のピアを照合する IKEv2 ポリシーの方法を示します。

```
crypto ikev2 policy policy2
 match vrf any
 proposal proposal-1
```

例：ポリシーの照合

重複するポリシーは設定しないでください。一致する複数の可能性がポリシーにある場合、次の例に示すように、最適な照合が使用されます。

```
crypto ikev2 policy policy1
 match fvrf fvrf1
crypto ikev2 policy policy2
 match fvrf fvff1
 match local address 10.0.0.1
```

vrf1 という FVRF のプロポーザルと 10.0.0.1 というローカル ピアは policy2 および policy2 と一致しますが、policy1 が最適な一致であるためにこちらが選択されます。

次の作業

IKEv2 の設定後、IPsec VPN の設定に進みます。詳細については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。

インターネット キー エクスチェンジ バージョン 2（IKEv2）のその他の関連資料

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 Command List』、すべてのリリース

関連項目	マニュアル タイトル
セキュリティ 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』
IPsec の設定	『Configuring Security for VPNs with IPsec』
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』
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』
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』
PKI の証明書登録のための Suite-B サポート	『Configuring Certificate Enrollment for a PKI』
IKE での使用にサポートされている標準	『Internet Key Exchange for IPsec VPNs Configuration Guide』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

RFC

RFC	タイトル
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
RFC 4869	*Suite B Cryptographic Suites for IPsec*
RFC 5685	*Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*

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

インターネット キー エクスチェンジ バージョン 2（IKEv2）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*：インターネット キー エクスチェンジ バージョン *2*（*IKEv2*）の設定に関する機能情報

機能名	リリース	機能情報
IPsec と IKEv2 に対する IPv6 のサポート		この機能によって、IPv6 アドレスを IPsec および IKEv2 プロトコルに追加できます。 次のコマンドが導入または変更されました。 **address (IKEv2 keyring), identity (IKEv2 keyring), identity local, match (IKEv2 policy), match (IKEv2 profile), show crypto ikev2 session, show crypto ikev2 sa, show crypto ikev2 profile, show crypto ikev2 policy, debug crypto condition, clear crypto ikev2 sa.**

機能名	リリース	機能情報
IOS ソフトウェア暗号での Suite-B のサポート		パケットデータの認証およびIKEv2プロポーザル設定の整合性確認メカニズムの検証に使用される SHA-2 ファミリ（HMAC バリアント）のハッシュアルゴリズムに、Suite-Bのサポートが追加されました。HMACは、追加レベルのハッシュを提供するバリアントです。 Suite-B によって、RFC 4754 で定義されているように楕円曲線デジタル署名アルゴリズム（ECDSA）署名（ECDSA-sig）を IKEv2 の認証方式にすることもできます。 Suite-B の要件は、暗号化アルゴリズムの 4 つのユーザー インターフェイス スイートです。アルゴリズムは、RFC 4869 で説明されている IKE および IPSec で使用します。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、および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 上における Suite-B サポートの詳細については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。 次のコマンドが導入または変更されました。 **authentication, group, identity (IKEv2 profile), integrity, match (IKEv2 profile).**
IOS 上における IKEv2 暗号としての AES-GCM のサポート		IKEv2 機能の AES-GCM サポートでは、Galois/カウンタ モードの Advanced Encryption Standard（AES-GCM）の使用方法を説明します。インターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルの暗号化ペイロードと共に認証済みの暗号化アルゴリズムを使用することについても説明します。 次のコマンドが導入または変更されました。 **encryption (IKEv2 proposal), prf, show crypto ikev2 proposal.**
トンネルモード自動選択		トンネルモード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセスインターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。 次のコマンドが導入または変更されました。 **virtual-template (IKEv2 profile), show crypto ikev2 profile.**

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。