IPsec の設定

IPsec の制約事項

IPsec の一般的な制約事項

- クリプトマップはサポートされていません。
- トンネルモードのみがサポートされています。
- ボリュームベースのキー再生成はサポートされていません。
- IPsec トンネルは、MPLS クラウドではサポートされていません。
- IPsec トンネルは、vrf lite ではサポートされていません。
- トンネルの送信元 IP アドレスとして、送信元 IPv4 アドレスを最大 4 つまで使用できます（ループバックアドレス）。
- トンネルの送信元 IP アドレスとして、送信元 IPv6 アドレスを最大 4 つまで使用できます（ループバックアドレス）。
- サポートされるトンネルの最大数は 128 です。これは一次元のスケール数です。同じリソースを共有する他の機能を有効にすると、スケール数が減少します。
- IPv4 トンネルモードと IPv6-overlay-IPv4 は、IPv6 アドレスを許可しません。
- IPv6 トンネルモードと IPv4-overlay-IPv6 は、IPv4 アドレスを許可しません。
- OSPFv3 認証は、IPsec でサポートされていません。

- IPsec 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）のみがサポートされています。

IPsec 仮想トンネル インターフェイスの制約事項

- 暗号化されたパケットのフラグメンテーションおよび暗号化されたフラグメントのリアセンブルはサポートされていません。SVTIのMTUは、物理インターフェイスよりも小さく設定する必要があります。フラグメンテーションは、暗号化の前または暗号解読の後に実行できます。
- インターネット キー交換（IKE）セキュリティ アソシエーション（SA）は VTI にバインドされています。
- デフォルトでは、スタティック VTI（SVTI）は、仮想トンネルインターフェイスに接続された 1 つの IPsec SA のみをサポートします。IPsec SA のトラフィックセレクタは、常に「IP any any」または「IPv6 any any」です。
- VTI は、トラフィックセレクタの絞り込みをサポートしません。
- SVTI は、"IP any any" プロキシのみをサポートします。
- IPsec ステートフル フェールオーバーは、IPsec VTI ではサポートされません。
- IPsec IPv4 モードで **tunnel mode ipsec ipv4** コマンドを使用する場合は、**shared** キーワードを設定しないでください。
- VTI での暗号化オフロードを使用したトレースルート機能はサポートされていません。
- **tunnel mode auto** で、混合モードはサポートされていません。**tunnel protection ipsec [shared]** で、混合モードはサポートされていません。
- トンネルの送信元をサブインターフェイスにすることはできません。

IPSec デッド ピア検出定期メッセージ オプションの制約事項

定期的 Dead Peer Detection（DPD; デッドピア検出）を使用した場合、デバイスはオンデマンド DPD よりも短い応答時間で、応答しない IKE ピアを検出できます。ただし、定期的な DPD では、余分なオーバーヘッドが発生します。10 を超える暗号化セッションで、大量の IKE ピアと通信する場合は、代わりにオンデマンドの DPD を使用することを検討してください。

IPsec についての情報

以降のトピックでは、IPsec に関する情報を示します。

IPsec の概要

（注） この機能は、Cisco Catalyst 9300X シリーズ スイッチでのみサポートされます。

（注） この機能を使用するには、HSECK9 キーを有効にする必要があります。HSECK9 キーを有効にするには、ポリシーを使用したスマートライセンスの章を参照してください。

安全なネットワークは、情報へのアクセスの自由度を定義し、ネットワーク内のセキュリティの展開を指示する強力なセキュリティポリシーから始まります。シスコは、インターネット、エクストラネット、イントラネット、およびリモート アクセス ネットワーク向けのカスタム セキュリティ ソリューションを構築するための多くのテクノロジーソリューションを提供しています。これらの拡張性の高いソリューションは、シームレスに相互運用し、エンタープライズワイドのネットワークセキュリティを展開します。シスコの IPsec は、総合的なセキュリティ ソリューションを提供するための主要なテクノロジーコンポーネントを提供します。シスコの IPsec サービスは、インターネット上を機密情報を送信するためのプライバシー、完全性、および真正性を提供します。

シスコのエンドツーエンドのサービスにより、お客様は個々のワークステーションに影響を与えることなく、ネットワーク インフラストラクチャに IPsec を透過的に実装できます。

IPSec は、インターネット上のプライベート通信のセキュリティを確保するためのオープンスタンダードのフレームワークです。インターネット技術特別調査委員会（IETF）によって開発された標準に基づく IPsec は、パブリックネットワーク全体におけるデータ通信の機密性、完全性、真正性を保証します。IPsec は、ネットワーク全体のセキュリティポリシーを展開するための、標準ベースの柔軟なソリューションに必要なコンポーネントを提供します。

IP データグラムを保護する IPsec のメソッドには、次の形式があります。

- データ発信者認証
- コネクションレス型のデータ完全性認証
- データコンテンツの機密性
- アンチリプレイ保護
- 限られたトラフィックフローの機密性

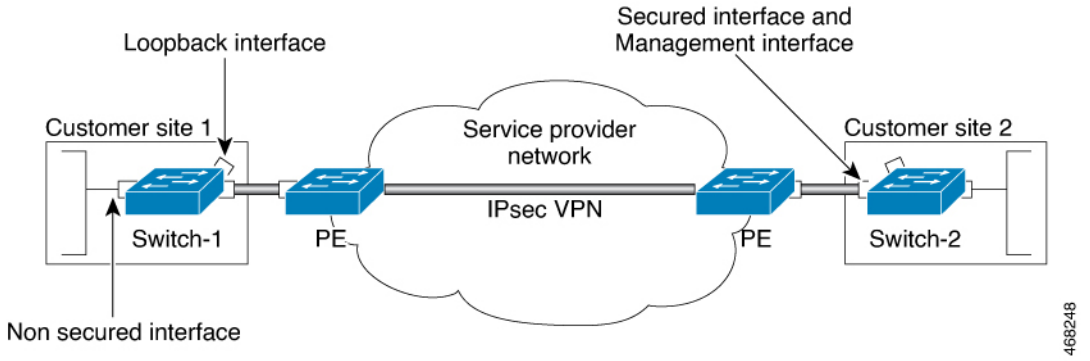
IPsec は、保護するトラフィックを指定する方法、そのトラフィックの保護方法、およびトラフィックの送信先を定義することにより、IP データグラムを保護します。

IP レベルでセキュリティを実装することにより、組織はセキュリティメカニズムを備えたアプリケーションだけでなく、セキュリティを無視した多くのアプリケーションに対しても、安全なネットワークを保証できます。IPsec は、LAN 全体、プライベートおよびパブリック WAN 全体、およびインターネット全体の通信を保護する機能を提供します。その使用例を次に示します。

- インターネット経由の安全な分散拠点の接続：企業は、インターネットまたはパブリック WAN 経由で、安全な仮想プライベートネットワークを構築できます。これにより、企業はインターネットに大きく依存し、プライベートネットワークの必要性を減らし、コストとネットワーク管理のオーバーヘッドを節約できます。
- インターネット経由の安全なリモートアクセス：IP セキュリティプロトコルを備えたシステムを使用するエンドユーザーは、インターネット サービス プロバイダー（ISP）にローカルコールを行い、企業ネットワークへの安全なアクセスを得られます。これにより、出張する従業員や在宅勤務者の移動費用を削減できます。
- パートナーとのエクストラネットおよびイントラネット接続の確立：IPsec を使用して、他の組織との通信を保護し、認証と機密性を保証し、鍵交換のメカニズムを提供できます。
- 電子商取引のセキュリティの強化：インターネット上での電子商取引を保護するためのこれまでの多くの方法は、Web ブラウザで一般的に使用され、設定と実行が簡単な、SSL を使用した Web トラフィックの保護に依存していました。ここに、電子商取引に IPsec を利用する新しい提案があります。

これらのさまざまなアプリケーションをサポートできるようにする IPsec の主な機能は、すべてのトラフィックを IP レベルで暗号化または認証できることです。これにより、リモートログオン、クライアント/サーバー、電子メール、ファイル転送、Web アクセスなどを含む、すべての分散アプリケーションを保護できます。

図 *1 : IPsec* ネットワーク



組織は通常、離れた場所の LAN を管理します。この典型的なビジネスシナリオでは、各 LAN 上のトラフィックに特別な保護は必要ありませんが、LAN 上のデバイスはファイアウォールにより、信頼できないネットワークから保護できます。

私たちは分散したモバイルの世界にいるため、各 LAN 上のサービスにアクセスする必要がある人が、インターネット上のサイトにいる可能性があります。この会社は、IPsec プロトコルを使用してアクセスを保護できます。これらのプロトコルは、各 LAN を外部に接続するルータやファイアウォールなどのネットワークデバイスで動作することも、ワークステーションやサーバーで直接動作することもできます。

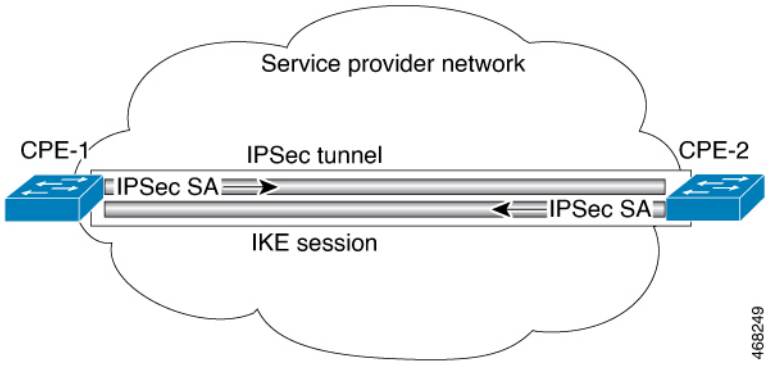
図 1 では、顧客サイトの CPE の 1 つに接続されているユーザーのワークステーションが、ネットワークデバイスとの IPsec トンネルを確立して、後続のすべてのセッションを保護できます。

このトンネルが確立されると、ワークステーションは、これらの IPsec ゲートウェイの背後にあるデバイスとさまざまなセッションを持つことができます。インターネットを通過するパケットは IPsec によって保護されますが、各 LAN には通常の IP パケットとして配信されます。

IPsec の機能

IPSec は 2 つのピア（2 つのスイッチなど）間で、セキュアなトンネル を提供します。機密性の高いパケット、およびこれらのセキュアなトンネルを介して送信されるべきパケットを定義します。これらのトンネルの特性を指定することによって、これらの機密性の高いパケットを保護するために使用すべきパラメータを定義します。マークされたパケットは、トンネルインターフェイスにローカルにリダイレクトされます。

図 *2 : IPSec* トンネル



より正確に言うと、これらのトンネルは、2 つの IPSec ピア間に確立されたセキュリティ アソシエーション（SA）のセットです。セキュリティ アソシエーションは、機密性の高い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、また 2 つのピアが使用するキー関連情報も指定します。セキュリティ アソシエーションは単一方向で、セキュリティプロトコルごとに確立されます。

IPsec がピアへのこのトラフィックを保護するために使用できるセキュリティ アソシエーションが存在しない場合、IPsec はインターネット キー エクスチェンジ（IKE）を使用してリモートピアとネゴシエーションし、データフローの代わりに必要な IPsec セキュリティ アソシエーションを設定します。

セキュリティアソシエーションのセット（ピアへの発信）は、一度確立されると、トリガーするパケット、および後続の適用可能なパケットに、これらのパケットがデバイスを出るときに適用されます。適用可能なパケットとは、元のパケットが一致したのと同じ基準に一致するパケットです。たとえば、すべての適用可能なパケットを、リモート ピアに転送する前に暗号化できます。そのピアからの着信トラフィックを処理する際、対応する着信セキュリティアソシエーションが使用されます。

IKE を使用してセキュリティアソシエーションを確立する場合、セキュリティアソシエーションが定期的に期限切れになり、再ネゴシエーションが必要になるようにライフタイムが設定されるため、追加のセキュリティ レベルが提供されます。

さまざまなデータ ストリームを保護するため、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セキュリティ アソシエーションのセットを使用できます。たとえば、一部のデータストリームは認証のみが行われ、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。

トランスフォーム セットは、IPsec 保護されたトラフィックに適用されるセキュリティ プロトコル、アルゴリズムおよびその他の設定の適切な組み合わせです。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。

IPsec は、ネットワーク層の暗号化と認証を実装し、ネットワークアーキテクチャ内にエンドツーエンドのセキュリティを組み込みます。これの利点は、強力なセキュリティを利用するために個々のアプリケーションを変更する必要がないことです。ネットワーク経由でルーティングされるすべてのパケットは、自動的に保護されます。

インターネット キー エクスチェンジ バージョン 2 に関する情報

以下のセクションでは、インターネット キー エクスチェンジ バージョン 2 に関する情報を示します。

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）。

（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。

IKEv2
DH_GROUP_768_MODP/Group 1
DH_GROUP_1024_MODP/Group 2
DH_GROUP_1536_MODP/Group 5
DES
DES
MD5

IKEv2 の利点

Dead Peer Detection

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、Dead Peer Detection（DPD; デッドピア検出）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。

（注） 応答側デバイスで、応答側のみの設定を行う必要があります。この設定を行わないと、IPsec プロセスが失敗する可能性があるためです。

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、設定手順を最小化します。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`

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。

IPSec 仮想トンネル インターフェイス

IPsec VTI の使用により、リモートアクセスの保護を提供する必要がある場合の設定プロセスが簡素化され、カプセル化に Generic Routing Encapsulation（GRE）またはレイヤ 2 トンネリング プロトコル（L2TP）トンネルを使用する代替手段が提供されます。IPsec VTI を使用するメリットは、設定において物理インターフェイスに対する IPsec セッションのスタティックマッピングが必要ないことです。IPsec トンネル エンドポイントは実際（仮想）のインターフェイスに関連付けられます。トンネルエンドポイントにはルーティング可能なインターフェイスがあるので、多くの共通インターフェイス機能を IPsec トンネルに適用できます。

IPsec VTI によって、複数パスの場合のように、物理インターフェイス上における IP ユニキャストおよびマルチキャスト制御パケット両方の暗号化トラフィックの送受信の柔軟性が高まります。トラフィックは、トンネルインターフェイスから転送されるときに暗号化され、トンネル インターフェイスに転送されると復号化されます。また、IP ルーティング テーブルによって管理されます。IP ルーティングを使用してトラフィックをトンネルインターフェイスに転送することで、IPsec VPN 設定が簡素化されます。

IPsec 仮想トンネル インターフェイスを使用するメリット

IPsec VTI によって、機能を適用できる仮想インターフェイスを設定できます。暗号化されていないテキスト パケットの機能は VTI 上で設定されます。暗号化されたパケットの機能は、物理インターフェイス上で適用されます。

スタティック VTI（SVTI）と DVTI という 2 つのタイプの VTI インターフェイスが存在します。

（注） 現在、SVTI のみがサポートされています。現在、DVTI はサポートされていません。

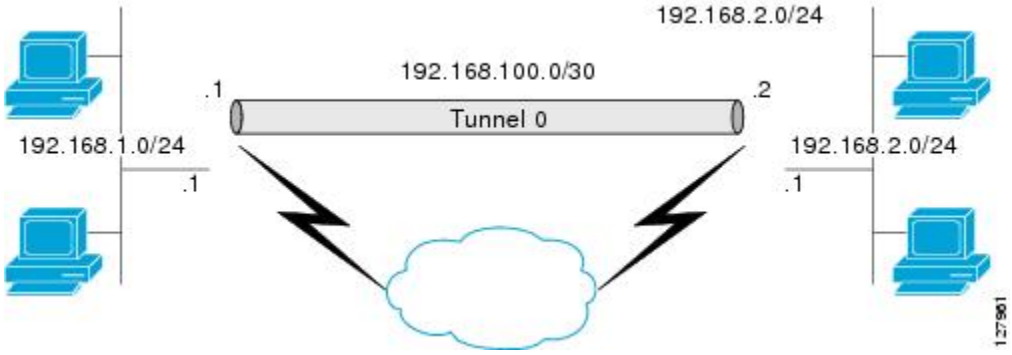
スタティック仮想トンネル インターフェイス

SVTI 設定は、トンネルによって 2 つのサイト間の常にオンであるアクセスが提供される、サイト間接続用に使用できます。

SVTI を使用することの利点は、ユーザーが、GRE ヘッダーに必要な追加の 24 バイトなしで、トンネルインターフェイス上のダイナミック ルーティング プロトコルをイネーブルにでき、その結果、暗号化データ送信用の帯域幅を削減できることです。

次の図に、SVTI の使用方法を示します。

図 *3 : IPsec SVTI*



IPsec VTI は、ネイティブ IPsec トンネリングをサポートします。

IPsec 仮想トンネル インターフェイスを使用したルーティング

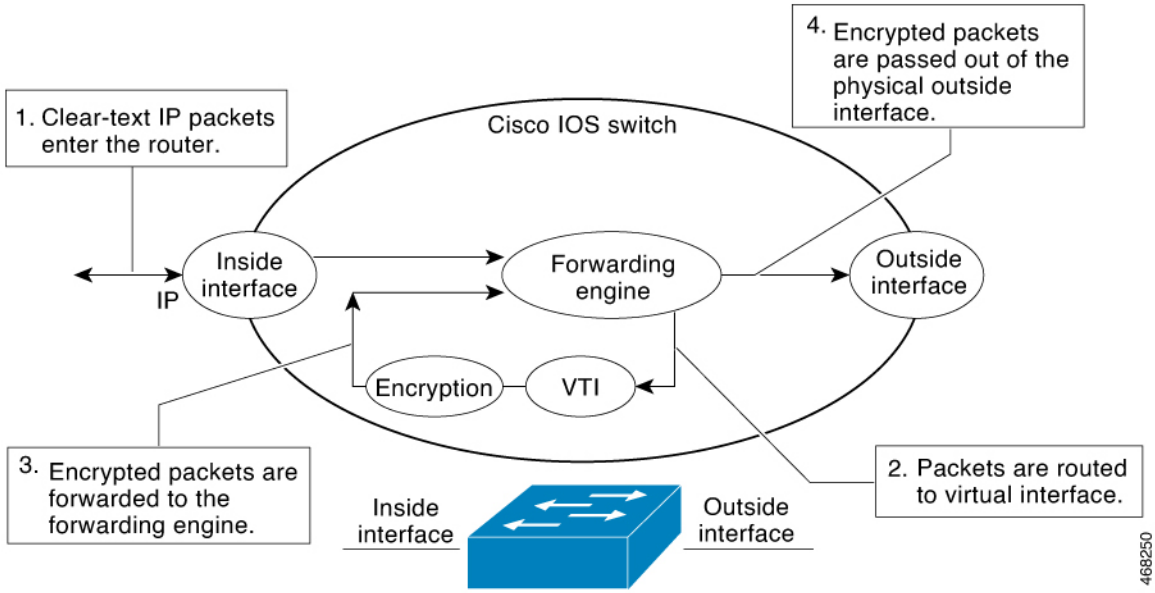
VTI はルーティング可能なインターフェイスなので、暗号化プロセスにおけるルーティングの役割は重要です。トラフィックは、VTI の外に転送される場合にだけ暗号化され、VTI に到着するトラフィックは、適宜、復号化およびルーティングされます。VTI を利用すれば、実際のインターフェイスをトンネルエンドポイントとして使用することによって、暗号化トンネルを確立できます。インターフェイスをモニターし、それにルーティングできます。このインターフェイスは実際のインターフェイスであるため、より有益で、他の Cisco IOS XE インターフェイスと同様のメリットを提供します。

IPsec 仮想トンネル インターフェイスを使用したトラフィックの暗号化

IPsec VTI が設定されると、暗号化がトンネル内で実行されます。トラフィックがトンネル インターフェイスに転送されると、そのトラフィックが暗号化されます。トラフィック転送は、IP ルーティングテーブルによって処理され、トラフィックを SVTI にルーティングします。IP ルーティングを使用してトラフィックを暗号化に転送することで、IPsec VPN 設定が簡素化されます。さらに、IPsec 仮想トンネルを使用すれば、IPsec によってマルチキャスト トラフィックを暗号化できます。

次の図に、IPsec トンネルへの IPsec パケット フローを示します。

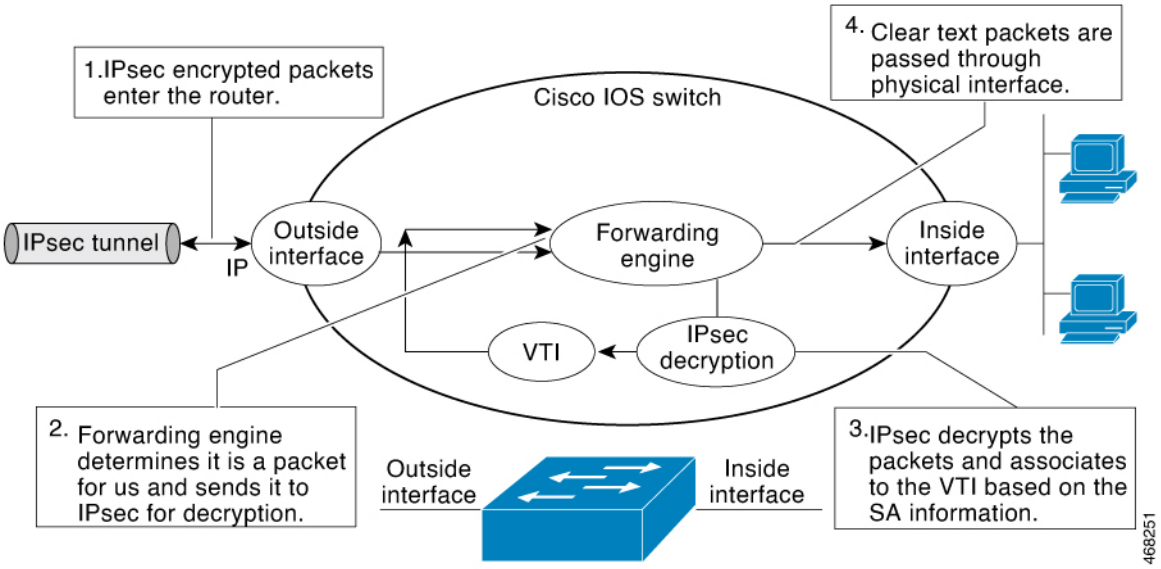
図 *4 : IPsec* トンネルへのパケット フロー



パケットが内部インターフェイスに到着すると、転送エンジンによってパケットが VTI にスイッチングされ、そこで暗号化されます。暗号化されたパケットは転送エンジンに戻され、そこで外部インターフェイスを介してスイッチングされます。

次の図に、IPsec トンネルからのパケット フローを示します。

図 *5 : IPsec* トンネルからのパケット フロー



IPsec アンチ リプレイ ウィンドウ

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます（セキュリティ アソシエーション（SA）アンチリプレイは、受信側がリプレイ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パケットを拒否できるセキュリティ サービスです）。復号機能によって、以前に認識したシーケンス番号が除外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値Xはデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X（N はウィンドウ サイズ）までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットが廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

IPsec の設定方法

次のセクションでは、IPsec を設定するために実行できる手順に関する情報を示します。

インターネット キー交換バージョン 2 の設定方法

次のセクションでは、インターネット キー エクスチェンジ バージョン 2 の構造を設定するために実行できる手順を示します。

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。

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

	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： `Device(config)# crypto ikev2 keyring kyr1`	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。
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）。

	コマンドまたはアクション	目的

		（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 10.1.1.1 >>>>>>>>>`
		`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： `Device(config-ikev2-keyring-peer)# pre-shared-key local key1`	ピアの事前共有キーを指定します。
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。

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 プロファイルを設定し、クリプトマップ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

	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。
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）方式リストを有効にします。

	コマンドまたはアクション	目的
		（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。
ステップ 8	**dynamic** 例：	ダイナミック IKEv2 プロファイルを設定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-profile)# dynamic`	（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。 （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。

	コマンドまたはアクション	目的
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） 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。
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	**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。

	コマンドまたはアクション	目的
		（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 16	**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。
ステップ 17	**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 18	**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

	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。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 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。
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。

	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 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* [**incoming** | **outgoing**] | **max-sa** *limit*} 例： `Device(config)# crypto ikev2 limit max-in-negotiation-sa 5000 incoming`	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 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。
ステップ 10	**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 11	**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

	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** *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**

	コマンドまたはアクション	目的
		• **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。
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。

	コマンドまたはアクション	目的
		• **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。

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

	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。

スタティック IPsec 仮想トンネル インターフェイスの設定

静的 IPsec 仮想トンネルインターフェイスを設定するには、次の手順を実行します。

手順

	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。

	コマンドまたはアクション	目的
ステップ 3	**crypto ipsec transform-set** *transform-set-name* 例： `Device(config)# crypto ipsec transform-set tfs esp-gcm`	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。
ステップ 4	**mode tunnel** 例： `Device(cfg-crypto-tran)#mode tunnel`	（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。
ステップ 5	**crypto IPsec profile** *profile-name* 例： `Device(cfg-crypto-tran)# crypto IPsec profile PROF`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec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 6	**set transform-set** *transform-set-name* 例： `Device(ipsec-profile)# set transform-set tfs esp-gcm`	クリプトマップエントリで使用可能なトランスフォーム セットを指定します。
ステップ 7	**set ikev2-profile** *profile-name* 例： `Device(ipsec-profile)#set ikev2-profile ikev2_prof`	IKEv2 プロファイルを IPSec プロファイルに適用します。
ステップ 8	**exit** 例： `Device(ipsec-profile)# exit`	IPsec プロファイル コンフィギュレーションモードを終了して、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 9	**interface** *tunnel number* 例： `Device(config)# interface tunnel 0`	トンネルが設定されるインターフェイスを指定し、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 10	**ip address** *address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	IP アドレスおよびマスクを指定します。
ステップ 11	**no interface** *interface-name* 例：	インターフェイス設定を削除します。

	コマンドまたはアクション	目的
	`Device(config-if)# no interface loopback 1`	
ステップ 12	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 13	**tunnel source** *interface-type interface-number* 例： `Device(config-if)# tunnel source loopback 0`	トンネルの送信元をループバック インターフェイスとして指定します。
ステップ 14	**tunnel destination** *ip-address* 例： `Device(config-if)# tunnel destination 172.16.1.1`	トンネルの宛先のIPアドレスを指定します。
ステップ 15	**tunnel protection IPsec profile** *profile-name* 例： `Device(config-if)# tunnel protection IPsec profile PROF`	トンネル インターフェイスを IPsec プロファイルに関連付けます。
ステップ 16	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

IPsec アンチ リプレイ ウィンドウの拡張と無効化のグローバル設定

IPsec アンチリプレイウィンドウを設定する：グローバルに展開および無効化する（これにより、作成されるすべてのセキュリティアソシエーションに影響を与える）には、次の手順を実行します。

手順

	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 ipsec security-association replay window-size** ［なし］ 例： `Device (config)# crypto ipsec security-association replay window-size 64`	セキュリティ アソシエーション リプレイ ウィンドウのサイズをグローバルに設定します。デフォルトのウィンドウ サイズは 64 で、64 パケットのウィンドウサイズのみがサポートされています。 （注） このコマンドまたは **crypto ipsec security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 4	**crypto ipsec security-association replay disable** 例： `Device (config)# crypto ipsec security-association replay disable`	検査をグローバルにイネーブルにします。アクティブなセキュリティ アソシエーションで **show crypto ipsec sa** コマンドを使用して、crypto ipsec セキュリティ アソシエーションの再生のステータスを確認できます。 （注） このコマンドまたは **crypto ipsec security-association replay window-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

IPsec の設定例

次のセクションでは、IPsec の設定例を示します。

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

次のセクションでは、インターネット キー エクスチェンジ バージョン 2 構成の設定例を示します。

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 10.165.200.225 255.255.255.224
  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 10.165.200.228 255.255.255.224
  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 10.165.200.225 255.255.255.224
  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 10.165.200.228 255.255.255.224
  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 10.165.200.225 255.255.255.224
  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 10.165.200.228 255.255.255.224
  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 10.0.0.0 10.0.0.0
  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 10.0.0.0 10.0.0.0
  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 10.0.0.0 10.0.0.0
  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。

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：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
```

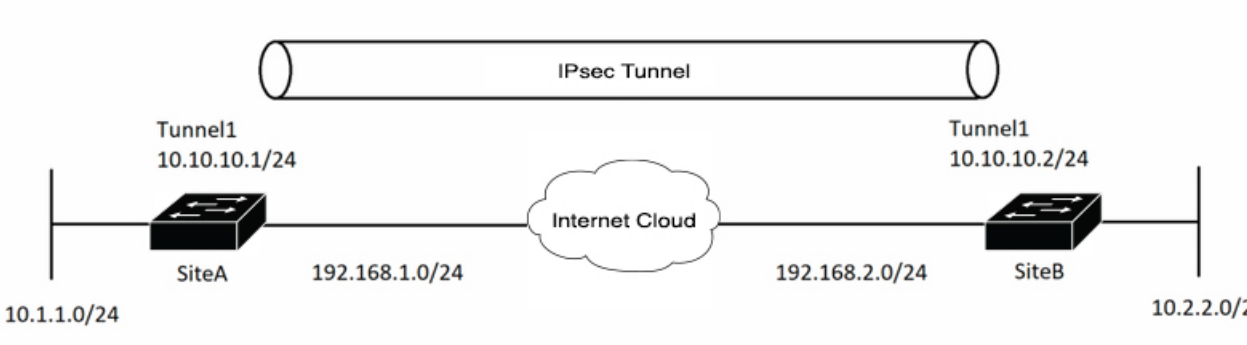
選択したプロポーザルは次のようになります。

```
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：分散型ゲートウェイでの IPsec の設定

次の例では、IPsec トンネルを設定する方法について説明します。



IKEv2 トンネルを起動するために必要なパラメータを設定します。まず、IKEv2 プロポーザルとキーリングを作成します。次に、暗号キーリングが呼び出される IKEv2 プロファイルを設定します。IPSEC トランスフォームセットと IKEv2 プロファイルを含む IPSEC プロファイルを設定して、暗号設定を完了します。

サイト A の設定例

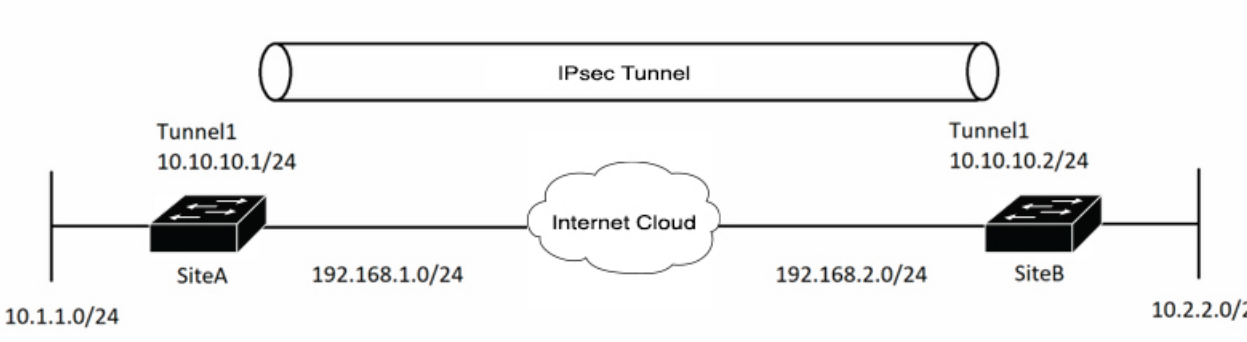
```
! —— IKEv2 Proposal

crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha512
 group 5

! --- IKEv2 Policy

crypto ikev2 policy policy-1
 match fvrf any
 match address local 192.168.1.1
 proposal prop-1

! —— IKEv2 Keyring

crypto ikev2 keyring keyring-1
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco123

! —— IKEv2 Profile

crypto ikev2 profile IKEv2-Profile-1
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-1

! —— IPSEC Transform set

crypto ipsec transform-set transform-1 esp-aes 256 esp-sha-hmac
 mode transport

! —— IPSEC Profile

crypto ipsec profile IPSEC-Profile-1
 set transform-set transform-1
 set ikev2-profile IKEv2-Profile-1
```

サイト B の設定例

```
! —— IKEv2 Proposal

crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha512
 group 5

! -- IKEv2 Policy

crypto ikev2 policy policy-1
 match fvrf any
 match address local 192.168.2.1
 proposal prop-1

! —— IKEv2 Keyring

crypto ikev2 keyring keyring-1
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco123

! —— IKEv2 Profile

crypto ikev2 profile IKEv2-Profile-1
 match fvrf internet
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-1

! —— IPSEC Transform set

crypto ipsec transform-set transform-1 esp-aes 256 esp-sha-hmac
 mode transport

! —— IPSEC Profile

crypto ipsec profile IPSEC-Profile-1
 set transform-set transform-1
 set ikev2-profile IKEv2-Profile-1
```

例：IPsec を使用したスタティック仮想トンネル インターフェイス

以下の例では、VPN トラフィックが暗号化のために IPsec VTI に転送され、その後物理インターフェイスに送信されます。サブネット 10 のトンネルでは、IPsec ポリシーに関してパケットがチェックされ、IPsec 暗号化のために暗号エンジン（CE）に渡されます。次の図に、IPSec VTI 設定を示しています。



サイト A のデバイス設定

```
! ── Interface Configuration

interface Tunnel1
 ip address 10.10.10.1 255.255.255.0
 tunnel source 192.168.1.1
 tunnel destination 192.168.2.1
 tunnel mode IPsec ipv4
 tunnel protection ipsec profile IPSEC-Profile-1

 interface Loopback 1
 ip address 192.168.1.1 255.255.255.0
```

サイト B のデバイス設定

```
! ── Interface Configuration


interface Tunnel1
 ip address 10.10.10.2 255.255.255.0
 tunnel source 192.168.2.1
 tunnel destination 192.168.1.1
 tunnel mode IPsec ipv4
 tunnel protection ipsec profile IPSEC-Profile-1

interface Loopback 1
 ip address 192.168.2.1 255.255.255.0
```

例：IPsec スタティック仮想トンネル インターフェイスの結果の確認

ここでは、設定が正しく動作しているか確認するうえで利用可能な情報を示します。次の出力では、Tunnel 0 およびライン プロトコルが「up」状態です。ライン プロトコルが「down」状態の場合、セッションは非アクティブです。

IPsec スタティック仮想トンネルインターフェイスの確認

```
Device# show interface tunnel 0

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
```

```
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport ipsec/ip, key disabled, sequencing disabled
Tunnel TTL 255
Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

Device# show crypto session

Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4, origin: crypto map

Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

例：アンチリプレイウィンドウのグローバル拡張と無効化

次の例は、アンチリプレイウィンドウサイズがグローバルに64に設定されていることを示しています。

```
Device(config)#crypto ipsec security-association replay window-size 64
```

IPsec の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.2	IPSec	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 仮想トンネルインターフェイスの設定	IPsec 仮想トンネル インターフェイス（VTI）では、IPsecトンネルを終了するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。
	IPSecアンチリプレイウィンドウの設定	IPsecアンチリプレイウィンドウの機能を使用すると、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護のウィンドウサイズを拡張できます。デフォルトのウィンドウサイズは64パケットです。64パケットのウィンドウサイズのみがサポートされます。

Cisco Feature Navigatorを使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigatorには、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。