IPsec VPN 用インターネット キー交換の設定ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

強力な Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースは、コンバージド リリースの 1 つのバージョンに進化（マージ）しました。これは、単一のリリースでスイッチングおよびルーティング ポートフォリオにおいて幅広いアクセスおよびエッジ製品をカバーします。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

「Configuring Internet Key Exchange for IPsec VPNs」

この章では、基本的な IP Security（IPsec）バーチャル プライベート ネットワーク（VPN）用のインターネット キー エクスチェンジ（IKE）プロトコルの設定方法について説明します。IKE とは、IPsec 標準とともに使用されるキー管理プロトコル標準です。IPsec は、IP パケットに対して強力な認証や暗号化を実現する IP セキュリティ機能です。

IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

IKE は、Oakley キー交換や Skeme キー交換をインターネット セキュリティ アソシエーションおよびキー管理プロトコル（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（ISAKMP、Oakley、および Skeme は、IKE により実装されるセキュリティ プロトコルです）。

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

IKE 設定の前提条件

- 「Configuring Security for VPNs with IPsec」モジュールで説明している概念およびタスクを理解している必要があります。
- ご使用のアクセス コントロール リスト（ACL）が IKE と互換性があることを確認してください。IKE ネゴシエーションではポート 500 でUser Datagram Protocol（UDP）を使用するため、IKE および IPsec が使用するインターフェイスで UDP ポート 500 のトラフィックがブロックされないように ACL を設定しておく必要があります。場合によっては、UDP ポート 500 のトラフィックを明示的に許可するために、ACL にステートメントを追加する必要があります。

IKE 設定の制約事項

- 開始ルータでは、リモートピアに関連付けられた証明書がない状態にしてください。
- 事前共有キーは、両方のピアで完全修飾ドメイン名（FQDN）を使用する必要があります（事前共有キーを設定するには、**crypto isakmp key** コマンドを入力します）。
- 各通信ルータは、互いの FQDN ホスト エントリを設定に保持している必要があります。
- 通信ルータはホスト名で認証するように設定する必要があります（IPアドレスではありません）。このため、**crypto isakmp identity hostname** コマンドを使用する必要があります。
- **show crypto eli** コマンドを使用して、デバイスのソフトウェア暗号化制限事項を決定します。ハードウェア モジュールがない場合の制限事項は次のとおりです。
  - IPSec セキュリティ アソシエーション（SA）数：1000
  - IKE SA 数：100
  - Diffie-Hellman（DH）セッション キー数：50

IPsec VPN の IKE 設定に関する情報

IKE での使用でサポート対象となる標準

シスコでは次の標準を採用しています。

- IPsec：IP セキュリティ プロトコル。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。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のネゴシエーションおよびアルゴリズムを処理し、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。
- ISAKMP：インターネットセキュリティアソシエーションおよびキー管理プロトコル。ペイロード形式、キー交換プロトコル実装の方法、およびセキュリティアソシエーションのネゴシエーションを定義するプロトコル フレームワークです。
- Oakley：キー交換プロトコルの 1 つで、認証済みのキー関連情報を取得する方法を定義します。
- Skeme：キー交換プロトコルの 1 つで、キーをすばやく更新しながら認証済みのキー関連情報を取得する方法を定義します。

（注） シスコでは DES、3DES、MD5（HMAC バリアントを含む）、および Diffie-Hellman（Dh）グループ 1、2、および 5 の使用は推奨しなくなりました。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。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

IKE での使用に備えて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。

- 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、データ暗号規格（DES）に代わる規格として開発されました。AES は DES よりセキュリティを向上させるために設計されています。具体的には、AES は、キーのサイズが従来より大きく、侵入者が既知の方式でメッセージを解読するには、キーを総当たりで試すしかありません。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。IKE は Explicit IV 標準の 56 ビット DES-CBC 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。

また Cisco IOS ソフトウェアは、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。トリプル DES（3DES）は強力な暗号化方式であり、これにより、機密性の高い情報を非信頼ネットワーク上で送信できます。この暗号化方式を使用することで、（特に金融業界の）お客様はネットワーク層での暗号化を実現できます。

（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。

- SEAL：ソフトウェア暗号化アルゴリズム（SEAL）。ソフトウェア ベースの DES、3DES、および AES に代わるアルゴリズムです。SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムに比べて、CPU に与える影響は小さくなります。
- 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 サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。
- RSA シグニチャおよび RSA 暗号化ナンス：RSA は、ロナルド・リベスト、アディ・シャミア、レオナルド・エーデルマンの 3 人によって開発された公開キー暗号化システムです。RSA シグニチャは否認防止を実行し、RSA 暗号化ナンスは否認を実行します（否認および否認防止は追跡可能性と関係があります）。
- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、安全でない通信チャネルでの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。サポートされているのは、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 ビットの DH グループです。また、2048 ビット DH グループの 256 ビット サブグループ、および 256 ビットと 384 ビットの楕円曲線 DH（ECDH）をサポートします。Cisco では、2048 ビット以上の DH キー交換または ECDH キー交換を使用することを推奨します。
- MD5：Message Digest 5（ハッシュ ベースのメッセージ認証コード（HMAC））バリアント）。パケットデータの認証に使用するハッシュ アルゴリズム。HMAC は、追加レベルのハッシュを提供するバリアントです。

IKE は、X.509v3 証明書と相互運用されます。X.509v3 は、認証に公開キーが必要な場合に、IKE プロトコルに沿って使用されます。この証明書サポートを使用すると、各デバイスに同等のデジタル ID カードを付与することで、保護されたネットワークを拡張できます。2 つの装置が通信する際、デジタル証明書を交換することで ID を証明します（これにより、各ピアで公開キーを手動で交換したり、各ピアで共有キーを手動で指定したりする必要がなくなります）。

IKE の利点

IKE は自動で IPsec セキュリティ アソシエーション（SA）をネゴシエーションするため、手間のかかる手動の事前設定をすることなしに IPsec によるセキュアな通信を実現できます。特に、IKE には次のような利点があります。

- IPsec SA のライフタイムが指定可能。
- IPsec セッション中に暗号キーの変更が可能。
- IPsec でアンチ リプレイ サービスが使用可能。
- 認証局（CA）のサポートにより、管理可能でスケーラブルな IPsec を実現可能。
- ピアのダイナミック認証が可能です。

IKE のメイン モードとアグレッシブ モード

IKE では、キーのネゴシエーションにフェーズ 1 とフェーズ 2 の 2 つのフェーズがあります。フェーズ 1 では、2 つの IKE ピア間でセキュリティ アソシエーション（キー）のネゴシエーションをします。フェーズ 1 でキーのネゴシエーションをすることで、フェーズ 2 で IKE ピアが安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE が IPsec など他の適用でのキー（セキュリティ アソシエーション）を設定します。

フェーズ 1 のネゴシエーションは、メイン モードまたはアグレッシブ モードを使用して実行されます。メイン モードでは、ネゴシエーション中にすべての情報が保護されるため、攻撃者が情報にアクセスできなくなります。メイン モードを使用すると、2 つの IKE ピアの ID が非表示になります。このモードでの運用は非常にセキュアですが、ネゴシエーションの実行に比較的時間がかかります。アグレッシブ モードでは、メインモードよりも少ない時間でピア間のキーのネゴシエーションを実行します。ただし、メイン モードでのネゴシエーションでは可能なセキュリティが一部失われます。たとえば、セキュリティ アソシエーションを確立しようとしている 2 つの装置の ID が傍受者に見えてしまいます。

この 2 つのモードは異なった目的で使用し、それぞれ別の強みがあります。メイン モードは、アグレッシブ モードに比べると低速ですが、アグレッシブ モードよりも IKE ピアのセキュリティが高いため、セキュアで柔軟性があります。アグレッシブ モードは柔軟性とセキュリティの点で劣りますが、より高速です。

Cisco IOS ソフトウェアでは、この 2 つのモードの設定はできません。IKE 認証（rsa-sig、rsa-encr、または事前共有）ではデフォルトでメイン モードを起動しますが、認証の起動に対応する情報がなく、ピアのホスト名に関連づけられている事前共有キーがある場合、Cisco IOS ソフトウェアは

アグレッシブ モードを起動できます。Cisco IOS ソフトウェアでは、アグレッシブ モードを開始した IKE ピアには、アグレッシブ モードで応答します。

IKE ネゴシエーション用 IKE ポリシー セキュリティ パラメータ

IKE ポリシーを使い、IKE ネゴシエーション中に使用するセキュリティ パラメータの組み合わせを定義します。IKEエクスチェンジに参加する各ピアでIKEポリシーを作成する必要があります。

IKE ポリシーを 1 つも設定しない場合、ルータはデフォルトのポリシーを使用します。デフォルトのポリシーは、常にプライオリティが最低に設定されており、各パラメータはデフォルト値に設定されています。

IKE ポリシーについて

IKE ネゴシエーションは保護する必要があるため、各 IKE ネゴシエーションは、共有（共通）の IKE ポリシーについて両ピアが同意することで開始されます。このポリシーには、次の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータとピアの認証方法を記述します。

両ピアがポリシーに同意すると、各ピアに確立されている SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーションにおける以降すべての IKE トラフィックに適用されます。

各ピアには、パラメータ値の組み合わせをそれぞれ変えることでプライオリティをつけたポリシーを複数設定できます。ただし、そのうちの少なくとも 1 つのポリシーには、リモート ピアのポリシーのいずれかとまったく同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値が設定されている必要があります。作成する各ポリシーに対して、一意のプライオリティを割り当てます（1 ～ 10,000 で指定し、1 が最大のプライオリティ）。

ヒント サポートされているパラメータの値が1つしかないデバイスを使用する場合は、もう一方のデバイスでサポートされている値を設定する必要があります。この制限を別にすれば、セキュリティとパフォーマンスには通常トレードオフの関係があり、パラメータ値の多くにはこのトレードオフがあります。ネットワークのセキュリティ リスクのレベルと、そのリスクに対する許容度を評価する必要があります。

一致する IKE ポリシーでの IKE ピアの合意

IKE ネゴシエーションが開始されると、IKE は、両方のピアにある同じ IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、自分のプライオリティ 1 位のポリシーと、相手のピアから受け取ったポリシーを比較し、一致するポリシーを探します。一致するポリシーが見つかるまで、リモート ピアは優先順位が高い順に各ポリシーをチェックします。

一致が成立するのは、2 つのピアからの両方のポリシーに、同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータ値が含まれているときです。

一致した場合は、IKE がネゴシエーションを完了し、IPsec セキュリティアソシエーションが作成されます。一致するポリシーが見つからなかった場合は、IKE はネゴシエーションを拒否し、IPsec は確立されません。

（注） このパラメータ値は、IKE SA の確立後 IKE ネゴシエーションに適用されます。ポリシーに指定する認証方式によっては、追加の設定が必要な場合があります（IKE 認証, （9 ページ）のセクションを参照）。ピアのポリシーに必要な関連設定がされていないと、一致するポリシーをリモート ピアで検索するときに、ピアはポリシーを送信しません。

IKE 認証

IKE 認証は次のオプションで構成され、各認証方式には追加の設定が必要です。

RSA シグニチャ

RSA シグニチャでは、CA から証明書を取得するようにピアを設定できます（証明書を発行するよう、CA が正しく設定されている必要があります）。CA を使用すると、IPSec ネットワークの管理性と拡張性が大幅に改善されます。また、RSA シグニチャ ベースの認証で使用できる公開キー操作は 2 つだけです。これに対し、RSA 暗号化では 4 つの公開キー操作を使用しますが、その分だけ全体のパフォーマンスが下がります。CA サポートを正しく設定するには、モジュール「PKI 内での RSA キーの展開」を参照してください。

証明書は公開キーを安全に交換するために各ピアで使用されます（RSA シグニチャでは、各ピアに、リモート ピアの公開シグニチャ キーが必要です）。双方のピアに有効な証明書がある場合、RSA シグニチャを使用する IKE ネゴシエーションの一環として、ピア間で公開キーが自動的に交換されます。

公開キーは手動でエクスチェンジすることもできます。これについては、RSA 暗号化ナンスの RSA キーの手動設定, （17 ページ）の項を参照してください。

RSA シグニチャにより、IKE ネゴシエーションで否認防止が可能になりますさらに、リモート ピアとの IKE ネゴシエーションを実際に実行することで、第三者に対する証明が可能になります。

RSA 暗号化ナンス

RSA 暗号化ナンスを使用するには、各ピアが他のピアの公開キーを持つようにする必要があります。

RSA シグニチャとは異なり、RSA 暗号化ナンス方式では、証明書を使って公開キーを交換できません。その代わり、各ピアが他のピアの公開キーを持つようにします。それには次の方法のいずれかを実行します。

- RSA 暗号化ナンスの RSA キーの手動設定, （17 ページ）のセクションの説明に従って、手動で RSA キーを設定する。
- 証明書を使用する RSA シグニチャを使って IKE 交換がピア間で実行されていることを確認する（証明書を使用すると、RSA シグニチャ ベースの IKE ネゴシエーション中にピアの公開キーが交換されます）。IKE 交換が実行されるようにするには、RSA 暗号化ナンスによる高プライオリティのポリシーと、RSA シグニチャによる低プライオリティのポリシーの 2 つのポリシーを指定します。RSA シグニチャは IKE ネゴシエーションが実行されるときに初めて使用されます。これは、各ピアに他のピアの公開キーがまだないためです。公開キーが交換されることで、以後の IKE ネゴシエーションで RSA 暗号化ナンスを使用できるようになります。この方法では、CA サポートをあらかじめ設定しておく必要があります。

RSA 暗号化ナンスでは IKE ネゴシエーションを否認できます。ただし、RSA シグニチャとは異なり、リモート ピアと IKE ネゴシエーションを実行したことを第三者に対して証明はできません。

事前共有キー

事前共有キーの概要

事前共有キーは、大規模なセキュア ネットワークでは、成長するネットワークにうまく対応できないため、適していません。ただし、RSA シグニチャのように CA を使用する必要がないため、10 ノード未満の規模の小さいネットワークではセットアップが簡単です。また、事前共有キーによる認証に比べ、RSA シグニチャによる認証の方が安全です。

（注） RSA 暗号化を設定し、シグニチャ モードがネゴシエーションされ、シグニチャ モードに証明書が使用されると、ピアはシグニチャと暗号キーを要求します。基本的にルータは、コンフィギュレーションでサポートされているできる限り多くのキーを要求します。RSA 暗号化が設定されていない場合は、ルータはシグニチャ キーだけを要求します。

事前共有キーの ISAKMP ID の設定

IKE ポリシーで事前共有キーを使用するピアそれぞれについて ISAKMP ID を設定する必要があります。

2 つのピアが IKE を使って IPsec SA を確立する場合、各ピアが自分の ID をもう一方のピア（リモート ピア）に送信します。各ピアは、ルータの ISAKMP ID の設定に従い、ホスト名または IP アドレスを送信します。

デフォルトでは、ピアの ISAKMP ID はピアの IP アドレスになっています。必要に応じて ID をピアのホスト名に変更します。一般的に、すべてのピアの ID は同じ設定（すべてのピアで IP アドレスを設定するか、すべてのピアでホスト名を設定）にします。お互いの識別にホスト名を使うピアと IP アドレスを使うピアが混在していると、リモート ピアの ID が識別されない場合にドメイン ネーム システム（DNS）lookup で ID を解決できなくなり、IKE ネゴシエーションが失敗することがあります。

マスク事前共有キー

マスク事前共有キーを使用すると、認証レベルが同じリモート ユーザのグループで、IKE 事前共有キーを共有できます。IKE 認証を実行するには、リモート ピアの事前共有キーと、ローカル ピアの事前共有キーが一致している必要があります。

マスク事前共有キーは通常、アウトオブバンドの安全なチャネル経由で配信されます。リモート ピアとローカル ピアが通信する場合、IKE 事前共有キーが設定されているリモート ピアとローカル ピアとの間で、IKE SA を確立できます。

mask キーワードの指定を **crypto isakmp key** コマンドで行う場合、サブネット アドレスを使用するかどうかはユーザが決定します。使用すると、より多くのピアとの間で同じキーを共有できます。つまり、事前共有キーが 2 人のユーザ間の使用に制限されないということです。

（注） サブネット アドレスとして 0.0.0.0 の使用は推奨しません。この設定ではグループで事前共有キーを保持できるため（すべてのピアが同じグループ キーを持つことが可能）、ユーザ認証のセキュリティが低下するからです。

特定の IPsec ピアの Xauth の無効化

静的 IPsec ピアの拡張認証（Xauth）を無効にすると、ルータで Xauth 情報（ユーザ名とパスワード）が表示されなくなります。

IKE モード設定

Internet Engineering Task Force（IETF）によって定義されているように、IKE モード コンフィギュレーションでは、ゲートウェイにより、IP アドレス（およびその他のネットワーク レベルの設定）を、IKE ネゴシエーションの一環で、クライアントにダウンロードできます。このエクスチェンジを使用することで、IP アドレスはゲートウェイによって IKE クライアントに渡され、IPsec でカプセル化された「内部」IP アドレスとして使用されます。この方式では、IPsec ポリシーと一致する可能性のある、クライアントの既知の IP アドレスが渡されます。

ダイナミック IP アドレスと会社のゲートウェイが設定されたリモート アクセス クライアント間に IPsec VPN を実装するには、各クライアントが認証された後、拡張可能な IPsec ポリシーをゲートウェイでダイナミックに管理する必要があります。IKE モード コンフィギュレーションにより、各クライアントの IP アドレスに関係なく、非常に規模の大きいクライアント群に対して拡張可能なポリシーをゲートウェイでセットアップできます。

IKE モード コンフィギュレーションには次の 2 つのタイプがあります。

- ゲートウェイ始動：ゲートウェイがクライアントでコンフィギュレーション モードを開始する。クライアントが応答すると、IKE が送信者の ID を変更し、メッセージが処理され、クライアントが応答を受信します。
- クライアント始動：クライアントがゲートウェイでコンフィギュレーション モードを開始する。クライアントに割り当てた IP アドレスでゲートウェイが応答します。

IPsec VPN 用 IKE の設定方法

IPsec 実装で IKE を使用しない場合は、**no crypto isakmp** コマンドを使ってすべての IPsec ピアの IKE を無効にし、この章の残りは実行せずに、IPsec VPN を開始します。

IKE はデフォルトでイネーブルになっています。各インターフェイスについて IKE を個別にイネーブルにする必要はなく、ルータのすべてのインターフェイスについてグローバルにイネーブルになっています。

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

IPsec ピアの認証、IPsec SA のネゴシエーション、IPsec キーの確立を実行するには、次の作業を実行します。

IKE ポリシーの作成

はじめる前に

AES IKE ポリシーを設定している場合、次の制限事項が適用されます。

- デバイスが IPsec およびロング キー（「k9」サブシステム）をサポートしている必要がある。
- アクセラレーション カードを使用している場合、AES は IPsec および IKE トラフィックを暗号化できない。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **crypto isakmp policy***priority*
4. **encryption**{**des** | **3des** | **aes** | **aes192** | **aes256**}
5. **hash** {**sha**|**sha256**|**sha384** | **md5**}
6. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
7. **group** {**1** | **2** | **5** | **14** | **15** | **16**|**19**|**20**|**24**}
8. **lifetime***seconds*
9. **exit**
10. **exit**
11. **showcryptoisakmppolicy**
12. 作成するポリシーそれぞれについて上記の手順を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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 isakmp policy***priority* 例： `Router(config)# crypto isakmp policy 10`	IKE ポリシーを定義し、config-isakmp コンフィギュレーション モードを開始します。 • *priority*：IKE ポリシーを一意に識別し、ポリシーにプライオリティを割り当てます。有効な値：1 ～ 10,000。1 が最大プライオリティ。

ステップ 4	**encryption** {**des** | **3des** | **aes** | **aes192** | **aes256**}
	
	例：
	`Router(config-isakmp)# encryption aes 256`
		暗号化アルゴリズムを指定します。
		• デフォルトでは **des** キーワードが使用されます。
		  • **des**：56 ビットDES-CBC（非推奨。推奨される暗号化アルゴリズムは AES）
		  • **3Des**：168 ビット DES（非推奨。推奨される暗号化アルゴリズムは AES）
		  • **aes**：128 ビット AES
		  • **aes 192**：192 ビット AES
		  • **aes 256**：256 ビット AES

ステップ 5	**hash** {**sha**|**sha256**|**sha384** | **md5**} 例： `Router(config-isakmp)# hash sha`	ハッシュ アルゴリズムを指定します。 • デフォルトでは SHA-1（**sha**）が使用されます。 • **sha256** キーワードは、ハッシュ アルゴリズムに SHA-2 ファミリの 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 アルゴリズムに SHA-2 ファミリの 384 ビット（HMAC バリアント）を指定します。 • **md5** キーワードは、ハッシュ アルゴリズムに MD5（HMAC バリアント）を指定します。（非推奨。代替として推奨されるのは SHA-256。）

	コマンドまたはアクション	目的
ステップ 6	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} 例： `Router(config-isakmp)# authentication pre-share`	認証方式を指定します。 • デフォルトでは RSA シグネチャが使用されます。 • **rsa-sig**：RSA シグネチャでは、CA から認証書を取得するようにピア ルータを設定する必要があります。 • **rsa-encr**：RSA 暗号化ナンスでは、各ピアが他のピアの RSA 公開キーを保持するように設定する必要があります。 • **pre-share**：事前共有キーでは、それらの事前共有キーを個別に設定する必要があります。
ステップ 7	**group** {**1** | **2** | **5** | **14** | **15** | **16**|**19**|**20**|**24**} 例： `Router(config-isakmp)# group 14`	Diffie-Hellman（DH）グループ ID を指定します。 • デフォルトでは DH グループ 1 が使用されます。 • **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。 • **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。一般的なガイドラインでは、2013 年より後（2030 年まで）、2048 ビット グループの使用を推奨しています。このガイドラインを満たすには、（可能な限り）group14 以上を選択してください。より長期にわたるセキュリティ方式が必要であっても、楕円曲線暗号の使用が推奨されますが、group15 と group16 も検討できます。
ステップ 8	**lifetime***seconds* 例： `Router(config-isakmp)# lifetime 180`	IKE SA のライフタイムを指定します。 • *seconds*：各 SA が満了するまでの時間（秒）。有効な値：60 ～ 86,400 秒、デフォルト値：86,400。

	コマンドまたはアクション	目的
		（注） ライフタイムを短くするほど（ポイントまで）、IKEネゴシエーションがセキュアになります。ただし、ライフタイムを長くすれば、以後の IPsec SA をそれだけ速くセットアップできます。
ステップ 9	**exit** 例： `Router(config-isakmp)# exit`	config-isakmp コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Router(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	**showcryptoisakmppolicy** 例： `Router# show crypto isakmp policy`	（任意）既存の IKE ポリシーをすべて表示します。
ステップ 12	作成するポリシーそれぞれについて上記の手順を繰り返します。	—

例

次に、**show crypto isakmp policy** コマンドからの出力で、ハードウェアがサポートしていない IKE 暗号化方式を設定しようとしたときに表示される警告メッセージの例を示します。

```
Router# show crypto isakmp policy
Protection suite of priority 1
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard 2 (256-bit)
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #14 (2048 bit)
        lifetime:              3600 seconds, no volume limit
```

トラブルシューティングのヒント

- **clearcryptosa** コマンドを使用して、IPsec SA を消去（および再初期化）します。

パラメータを指定せずに **clearcryptosa** 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。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。詳細については、『Cisco IOS Security Command Reference』の **clearcryptosa** コマンドを参照してください。

- デフォルト ポリシーおよび設定されているポリシーのデフォルト値は、**showrunning-config** コマンドの発行時には設定に表示されません。デフォルトポリシーおよび設定されているポリシーのデフォルト値を確認するには、**showcryptoisakmppolicy** コマンドを使用してください。
- 使用しているハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式はすべて無効にしてください。無効にしておくと、ピアとのネゴシエーションのときに常に無視されます。

ハードウェアがサポートしていないIPsecトランスフォームまたはIKE暗号化方式を入力すると、警告メッセージが表示されます。この警告メッセージはブート時にも表示されます。暗号化カードを挿入すると、現在の設定がスキャンされます。ハードウェアがサポートしていないIPsecトランスフォームまたは IKE 暗号化方式が検出されると、警告メッセージが表示されます。

次の作業

IKE ポリシーで指定した認証方式（RSA シグニチャ、RSA 暗号化ナンス、事前共有キー）によっては、IKE および IPsec が IKE ポリシーを正常に使用できるように、特定の設定作業を追加で実行する必要があります。この追加作業実行についての詳細は、IKE 認証の設定, （16 ページ）を参照してください。

AES ベースのトランスフォームセットを設定する方法については、モジュール「Configuring Security for VPNs with IPsec」を参照してください。

IKE 認証の設定

認証方式を指定（またはデフォルト方式を設定）したIKEポリシーを少なくとも1つ作成したら、認証方式を設定する必要があります。認証方式を正常に設定しなければ、IPsecがIKEポリシーを使用できません。

（注） IKE認証を設定する前に、認証方式を指定した（またはデフォルトのRSAシグニチャにした）IKE ポリシーを最低 1 つは設定しておく必要があります。

IKE 認証を設定するには、状況に応じて次の作業のいずれかを実行する必要があります。

前提条件

認証方式を指定した（またはデフォルトの RSA シグニチャを設定した）IKE ポリシーを最低 1 つは設定しておく必要があります。

RSA 暗号化ナンスの RSA キーの手動設定

（注） この作業を実行するのは、CA を使用していない場合だけです。

RSA キーを手動で設定するには、IKE ポリシーで RSA 暗号化ナンスを使用する IPsec ピアそれぞれについて、この作業を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **crypto key generate rsa**{**general-keys**} | **usage-keys**} [**label***key-label*] [**exportable**] [**modulus***modulus-size*]
4. **cryptokeygenerateeckeysize** [**256** | **384**] [**label***label-string*]
5. **exit**
6. **show crypto key mypubkey rsa**
7. **configure terminal**
8. **crypto key pubkey-chain rsa**
9. 次のいずれかを実行します。
   - **named-key***key-name*[**encryption** | **signature**]
   - **addressed-key***key-address* [**encryption** | **signature**]
10. **address***ip-address*
11. **key-string** key-string
12. **quit**
13. IKE ポリシーで RSA 暗号化ナンスを使用するピアそれぞれについて上記の手順を繰り返します。
14. **exit**
15. **exit**
16. **showcryptokeypubkey-chainrsa** [**name***key-name* | **address***key-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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 key generate rsa**{**general-keys**} | **usage-keys**} [**label***key-label*] [**exportable**] [**modulus***modulus-size*] 例： `Router(config)# crypto key generate rsa general-keys modulus 360`	RSA キーを生成します。 • *key-label* 引数を指定していない場合、ルータの完全修飾ドメイン名（FQDN）であるデフォルト値が使用されます。
ステップ 4	**cryptokeygenerateeckeysize** [**256** | **384**] [**label***label-string*] 例： `Router(config)# crypto key generate ec keysize 256 label Router_1_Key`	EC キーを生成します。 • 256 キーワードは、キーのサイズを 256 ビットに指定します。 • 384 キーワードは、キーのサイズを 384 ビットに指定します。 • **label** キーワードと *label-string* 引数を使用して、EC キーにラベルを指定できます。 （注） ラベルを指定しない場合は、FQDN の値が使用されます。
ステップ 5	**exit** 例： `Router(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 6	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）生成された RSA 公開キーを表示します。
ステップ 7	**configure terminal** 例： `Router# configure terminal`	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 8	**crypto key pubkey-chain rsa** 例： `Router(config)# crypto key pubkey-chain rsa`	公開キー コンフィギュレーション モード（他のデバイスの RSA 公開キーの手動設定が可能）にします。

	コマンドまたはアクション	目的

ステップ 9	次のいずれかを実行します。
	• **named-key***key-name*[**encryption** | **signature**]
	• **addressed-key***key-address* [**encryption** | **signature**]
	
	例：
	`Router(config-pubkey-chain)# named-key otherpeer.example.com`
	
	例：
	`Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption`
		どのリモート ピアの RSA 公開キーを指定するのかを示し、公開キー コンフィギュレーション モードを開始します。
		• リモート ピアが ISAKMP ID にホスト名を使用している場合は、**named-key** コマンドを使用し、リモート ピアの FQDN（somerouter.example.com など）を *key-name* に指定します。
		• リモート ピアが ISAKMP ID に IP アドレスを使用している場合は、**addressed-key** コマンドを使用し、リモート ピアの IP アドレスを *key-address* に指定します。

ステップ 10	**address***ip-address* 例： `Router(config-pubkey-key)# address 10.5.5.1`	リモート ピアの IP アドレスを指定します。 • **named-key** コマンドを使用するのは、このコマンドを使用してピアの IP アドレスを指定する必要がある場合です。

ステップ 11	**key-string** key-string
	
	例：
	`Router(config-pubkey-key)# key-string`
	
	例：
	`Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973`
	
	例：
	`Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5`
	
	例：
	`Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8`
	
	例：
	`Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB`
	
	例：
	`Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B`
		リモート ピアの RSA 公開キーを指定します。
		• （このキーは、リモート ルータの RSA キーが生成されたときに、リモート ピアの管理者が確認したキーです）

	コマンドまたはアクション	目的
	例： `Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21`	
ステップ 12	**quit** 例： `Router(config-pubkey-key)# quit`	公開キー チェーン コンフィギュレーション モードに戻ります。
ステップ 13	IKE ポリシーで RSA 暗号化ナンスを使用するピアそれぞれについて上記の手順を繰り返します。	—
ステップ 14	**exit** 例： `Router(config-pubkey-key)# exit`	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 15	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**showcryptokeypubkey-chainrsa** [**name***key-name* | **address***key-address*] 例： `Router# show crypto key pubkey-chain rsa`	（任意）ルータに保存されているすべての RSA 公開キーのリスト、またはルータに保存されている特定の RSA キーの詳細を表示します。

事前共有キーの設定

事前共有キーを設定するには、IKE ポリシーで事前共有キーを使用するピアそれぞれについて以下の手順を実行します。

（注） 事前共有は、規模が拡大しているネットワークではうまく拡張できない。マスク事前共有キーには次の制約事項があります。

- 同じ事前共有キーのすべての IPsec ピアを設定するまで、IPsec ピア間に SA を確立できない。
- マスク事前共有キーは、さまざまなレベルの認可を要求しているリモートユーザごとに、明確に異なっている必要がある。認証のレベルごとに新しい事前共有キーを設定し、適切なキーを適切なユーザに割り当てる必要があります。正しく設定しないと、認証を受けていない人物が、保護されているデータに対するアクセス権を取得する場合があります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **cryptoisakmpidentity**{**address** | **dn**|**hostname**}
4. **ip host***hostnameaddress1* [*address2...address8*]
5. 次のいずれかを実行します。
   - **cryptoisakmpkey***keystring***address***peer-address* [**mask**] [**no-xauth**]
   - **cryptoisakmpkey***keystring***hostname***hostname* [**no-xauth**]
6. 次のいずれかを実行します。
   - **cryptoisakmpkey***keystring***address***peer-address* [**mask**] [**no-xauth**]
   - **cryptoisakmpkey***keystring***hostname***hostname* [**no-xauth**]
7. IKE ポリシーで事前共有キーを使用するピアそれぞれについて以上の手順を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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	**cryptoisakmpidentity**{**address** | **dn**|**hostname**} 例： `Router(config)# crypto isakmp identity address`	ローカル ピアの IP アドレスまたは認定者名（DN）ホスト名を使ってピアの ISAKMP ID を指定します。 • **address**：通常は、ピアが IKE ネゴシエーションに使用するインターフェイスが 1 つだけ（したがって IP アドレスが 1 つだけ）で、IP アドレスがわかっている場合に使用します。 • **dn**：通常は、IKE 処理中、ISAKMP ID としてルータ証明書の DN が指定および選択される場合に使用します。dn キーワードは、証明書ベースの認証にだけ使用します。 • **hostname**：IKE ネゴシエーションに使用するインターフェイスがピアに複数ある場合か、（IP アドレスのダイナミック割り当てなどで）インターフェイスの IP アドレスが不明の場合に使用する必要があります。
ステップ 4	**ip host***hostnameaddress1* [*address2...address8*] 例： `Router(config)# ip host RemoteRouter.example.com 192.168.0.1`	ホスト名を使ってローカル ピアの ISAKMP ID を指定した場合、すべてのリモート ピアについて、ピアのホスト名を IP アドレスにマップします （ホスト名または IP アドレスが DNS サーバでマップ済みの場合はこの手順は不要）。

ステップ 5	次のいずれかを実行します。
	• **cryptoisakmpkey***keystring***address***peer-address* [**mask**] [**no-xauth**]
	• **cryptoisakmpkey***keystring***hostname***hostname* [**no-xauth**]
	
	例：
	`Router(config)# crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth`
	
	例：
	`Router(config) crypto isakmp key sharedkeystring hostname RemoteRouter.example.com`
		特定のリモート ピアで使用する共有キーをローカル ピアで指定します。
		• リモート ピアで ISAKMP ID を IP アドレスで指定した場合は、この手順で **address** キーワードを使用し、それ以外の場合は、この手順で **hostname** キーワードを使用します。
		  • **no-xauth**：ルータがピアに Xauth 情報のプロンプトを出力しないようにします。
		
		（注） 事前共有キーは、IKE メイン モードでの事前共有キー認証の設計に従い、ピアの IP アドレスを基にしている必要があります。事前共有キー認証の ID としてホスト名を送信できますが、キーはピアの IP アドレスを基に検索されます。（IP アドレスに基づいて）キーが検索されなかった場合、ネゴシエーションが失敗します。

	コマンドまたはアクション	目的

ステップ 6	次のいずれかを実行します。
	• **cryptoisakmpkey***keystring***address***peer-address* [**mask**] [**no-xauth**]
	• **cryptoisakmpkey***keystring***hostname***hostname* [**no-xauth**]
	
	例：
	`Router(config) crypto isakmp key sharedkeystring address 10.0.0.1`
	
	例：
	`Router(config) crypto isakmp key sharedkeystring hostname LocalRouter.example.com`
		ローカル ピアで使用する共有キーをリモート ピアで指定します。
		• これは、ローカル ピアで指定したキーと同じキーです。
		• ローカル ピアで ISAKMP ID を IP アドレスで指定した場合は、この手順で **address** キーワードを使用し、それ以外の場合は、この手順で **hostname** キーワードを使用します。

ステップ 7	IKE ポリシーで事前共有キーを使用するピアそれぞれについて以上の手順を繰り返します。	--

IKE モード コンフィギュレーションの設定

（注） IKE モード コンフィギュレーションには次の制約事項があります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip local pool***pool-namestart-addrend-addr*
4. **crypto isakmp client configuration address-pool local***pool-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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• 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： `Router# 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	**ip local pool***pool-namestart-addrend-addr* 例： `Router(config)# ip local pool pool1 172.16.23.0 172.16.23.255`	アドレス一式が定義されている既存のローカルアドレス プールを定義します。
ステップ 4	**crypto isakmp client configuration address-pool local***pool-name* 例： `Router(config)# crypto isakmp client configuration address-pool local pool1`	IKE コンフィギュレーションのローカルアドレス プールを参照します。

IPsec SA ネゴシエーションのための IKE 暗号マップの設定

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『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. イネーブル化
2. **configureterminal**
3. **cryptomap***tagsequence***ipsec-isakmp**
4. **setpfs** {**group1** | **group2** | **group5** | **group14** | **group15** | **group16**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptomap***tagsequence***ipsec-isakmp** 例： `Router(config)# crypto map example 1 ipsec-ipsec-isakmp`	クリプト マップを指定し、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。 • *tag* 引数には、暗号マップを指定します。 • *sequence* 引数には、暗号マップ エントリに挿入するシーケンスを指定します。 • **ipsec-isakmp** キーワードには、IKEv1 を使用する IPsec（ISAKMP）を指定します。

ステップ 4	**setpfs** {**group1** | **group2** | **group5** | **group14** | **group15** | **group16**}
	例：
	`Router(config-isakmp)# set pfs 14`
		IPSec SA ネゴシエーションの DH グループ ID を指定します。
		• デフォルトでは DH グループ 1 が使用されます。
		  • **group1**：768 ビット DH（非推奨）
		  • **group2**：1024 ビット DH（非推奨）
		  • **group5**：1536 ビット DH（非推奨）
		  • **group14**：2048 ビット DH グループを指定します。
		  • **group15**：3072 ビット DH グループを指定します。
		  • **group16**：4096 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。一般的なガイドラインでは、2013 年より後（2030 年まで）、2048 ビット グループの使用を推奨しています。このガイドラインを満たすには、いずれかの group14 を選択してください。より長期にわたるセキュリティ方式が必要であっても、楕円曲線暗号の使用が推奨されますが、group15 と group16 も検討できます。

IKE コンフィギュレーションの設定例

例：IKE ポリシーの作成

このセクションには、AES IKE ポリシーおよび 3DES IKE ポリシーの設定方法を示す次の例が含まれています。

（注） シスコでは、3DES の使用は推奨していません。代わりに、AES を使用してください。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

例：3DES IKE ポリシーの作成

この例では、2 つの IKE ポリシー（最大のプライオリティとして policy 15、次のプライオリティとして policy 20）を作成し、最小のプライオリティとして既存のデフォルト プライオリティを使用します。また、IP アドレスが 192.168.224.33 のリモート ピアに、policy 20 で使用する事前共有キーも作成します。

```
crypto isakmp policy 15
 encryption 3des
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
!
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
!
crypto isakmp key 1234567890 address 192.168.224.33
```

この例では、暗号化DESのポリシーのデフォルト値は、暗号化アルゴリズムパラメータのデフォルト値のため、記述した設定には表示されません。

この設定で **show crypto isakmp policy** コマンドを発行すると、出力は次のようになります。

```
Protection suite priority 15
encryption algorithm:3DES - Triple Data Encryption Standard (168 bit keys)
hash algorithm:Message Digest 5
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#2 (1024 bit)
lifetime:5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:preshared Key
Diffie-Hellman group:#1 (768 bit)
lifetime:10000 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
```

```
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
```

ライフタイムに「no volume limit」と出力されていますが、time ライフタイム（86,400 秒など）だけは設定できます。volume limit ライフタイムは設定できません。

例：AES IKE ポリシーの作成

次に、**showrunning-config** コマンドからの出力例を示します。この例では、AES 256 ビット キーが有効になっています。

```
Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
 mode transport

.
.
.
```

例：IKE 認証の設定

次の例は、2 つの IPsec ピアの RSA 公開キーを手動で指定する方法を示しています。10.5.5.1 のピアは汎用キーを使用し、もう一方のピアは特殊な用途のキーを使用しています。

```
crypto key pubkey-chain rsa
 named-key otherpeer.example.com
 address 10.5.5.1
 key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4
 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
 D58AD221 B583D7A4 71020301 0001
 quit
 exit
 addressed-key 10.1.1.2 encryption
 key-string
 00302017 4A7D385B 1234EF29 335FC973
 2DD50A37 C4F4B0FD 9DADE748 429618D5
```

```
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
exit
addressed-key 10.1.1.2 signature
key-string
0738BC7A 2BC3E9F0 679B00FE 53987BCC
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
quit
exit
exit
```

次の作業

IKE ネゴシエーションを正常に設定したら、IPsec の設定を開始します。このタスクの実行についての詳細は、モジュール「Configuring Security for VPNs with IPsec」を参照してください。

その他の参考資料

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 Commands List, All Releases』
セキュリティコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	• 『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	IPsec を使用した VPN のセキュリティの設定
IKE バージョン 2	「Configuring Internet Key Exchange Version 2 and FlexVPN」
CA から証明書を取得するように RSA キーを設定	PKI 内での RSA キーの展開

関連項目	マニュアル タイトル
Suite-B の ESP トランスフォーム	IPsec を使用した VPN のセキュリティの設定
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 and FlexVPN」
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 Version 2 and FlexVPN」
PKI の証明書登録のための Suite-B サポート	「Configuring Certificate Enrollment for a PKI」
推奨される暗号化アルゴリズム	次世代暗号化

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
なし	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	Title
RFC 2408	『Internet Security Association and Key Management Protocol (ISAKMP)』
RFC 2409	『The Internet Key Exchange (IKE)』
RFC 2412	『The OAKLEY Key Determination Protocol』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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 VPN の IKE 設定の機能情報

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 *1*：*IPsec VPN* の *IKE* 設定の機能情報

機能名	リリース	機能情報
スタティック IPsec ピアの拡張認証を無効にする機能	12.2(4)T	この機能により、ルータ間 IPsec の事前共有キー設定中に Xauth を無効にできます。したがって、ルータによりピアのユーザ名およびパスワードは要求されません。これらは、VPN クライアント対 Cisco IOS IPsec の Xauth が発生するときに転送されます。 この機能により、**crypto isakmp key.** コマンドが変更されました。

機能名	リリース	機能情報
Advanced Encryption Standard（AES）	12.2(8)T	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、**crypto ipsec transform-set**、**encryption**（**IKE ポリシー**）、**show crypto ipsec transform-set**,**crypto ipsec transform-set**、**show crypto isa**、**kmp policy** の各コマンドが変更されました。
SEAL 暗号化	12.3(7)T	この機能により、IPsec での SEAL 暗号化に対するサポートが追加されました。 この機能により、**crypto ipsec transform-set.** コマンドが変更されました。

機能名	リリース	機能情報
IOS SW の暗号化での Suite-B のサポート	15.1(2)T	Cisco IOS で、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 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。この機能により、IPsec SA ネゴシエーションに Elliptic Curve Diffie-Hellman（ECDH）のサポートも追加されました。 Cisco IOS での Suite-B サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。 この機能により、**authentication**、**crypto key generate ec keysize**、**crypto map**、**group**、**hash**、**set pfs** の各コマンドが変更されました。

第 3 章

「Call Admission Control for IKE」

IKE 用コール アドミッション制御機能は、Cisco IOS ソフトウェアでのインターネット キー エクスチェンジ（IKE）プロトコルに対し、コール アドミッション制御（CAC）を適用したものです。CAC は、IKE と IPsec セキュリティ アソシエーション（SA）（つまり CAC へのコール）をルータが同時に確立できる数を制限します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

IKE 用コール アドミッション制御に関する前提条件

- このデバイスで IKE を設定します。

IKE 用コール アドミッション制御に関する情報

IKE セッション

デバイスが別のデバイスとの間で確立できるインターネット 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）の数を制限する方法には、次の 2 つがあります。

- **cryptocalladmissionlimit** コマンドを入力して、IKE SA の絶対制限値を設定します。設定された制限値に達すると、デバイスは新しい IKE SA 要求をドロップします。
- **calladmissionlimit** コマンドを入力して、システム リソース制限値を設定します。チャージ単位で設定されたレベルのシステム リソースが使用されている場合、デバイスは新しい IKE SA 要求をドロップします。

コール アドミッション制御（CAC）は新しい SA のみ（つまり、ピア間に SA がまだ存在しないとき）に適用されます。既存の SA を保存するためにあらゆる処置が行われます。新しい SA 要求が拒否されるのは、システム リソースが不足しているか、あるいは設定された IKE SA 制限値に達したことが原因です。

セキュリティ アソシエーション制限

SA（セキュリティ アソシエーション）は、2 つ以上のエンティティがセキュリティ サービスを使用して特定のデータ フローのために安全に通信する方法を記述したものです。IKE は接続のパラメータを識別するために、必ず SA を使用します。IKE では、独自に SA をネゴシエーションして確立できます。IKE SA は、IKE だけで使用され、双方向です。IKE SA は、IPsec を制限できません。

IKE は、ユーザが設定した SA 制限値に基づいて SA 要求をドロップします。IKE SA 制限値を設定するには、**crypto call admission limit** コマンドを入力します。ピア ルータから新しい SA 要求があると、IKE はアクティブな IKE SA の数とネゴシエーション中の SA の数が、設定された SA 制限値を満たしているか、超えているかを判別します。この数が制限値より大きい、または等しい場合、新しい SA 要求は拒否され、syslog が生成されます。このログには、SA 要求の送信元および宛先 IP アドレスが含まれます。

crypto call admission limit コマンドの **ipsec sa** *number* と **ike sa** *number* キーワードと引数のペアには、確立された IPsec SA と IKE SA の数の制限値を設定します。

ネゴシエーション時の IKE 接続数の制限

Cisco リリースに基づいて、デバイスで設定できる内部 IKE ネゴシエーション接続の数を制限できます。このタイプの IKE 接続は、認証および実際の確立前のアグレッシブ モード IKE SA またはメイン モード IKE SA を表します。IKEv2 の最大内部ネゴシエーション CAC のデフォルト値は 40 です。

cryptocalladmissionlimitikein-negotiation-sa *number* コマンドを使用すると、IKE が新しい SA 要求の拒否を開始する前にデバイスが確立できるインターネット キーエクスチェンジ（IKE）と IPsec セキュリティ アソシエーション（SA）の最大数を指定できます。

cryptocalladmissionlimit コマンドの **allin-negotiation-sa** *number* と **ikein-negotiation-sa** *number* のキーワードと引数のペアは、ネゴシエーション時のすべての SA とネゴシエーション時の IKE SA を制限します。

システム リソースの使用状況

ルータの CPU サイクルまたはメモリ バッファが不足した場合に、IKE がそのことを認識できるように、CAC はグローバル情報リソース モニタをポーリングします。システム リソースの使用量レベルを表す制限値を 1 ～ 100000 までの範囲で設定できます。設定レベルのリソースが使用されると、IKE は SA 要求を廃棄します（新たに受け入れません）。システム リソース使用量の制限を設定するには、**call admission limit** コマンドを入力します。

新しい着信 SA 要求ごとに、ルータにかかる現在の負荷が数値に変換され、システム リソースの使用量レベルが表示されます。また、この数値と、**call admission limit** コマンドによって設定されたリソース制限値が比較されます。現在の負荷が、設定されたリソース制限値を超えると、IKE は新しい SA 要求を廃棄します。ルータの負荷には、アクティブな SA、CPU の使用量、および考慮される SA 要求が含まれます。

call admission load コマンドを実行すると、現在のシステム リソース使用量の倍率を表す 0 ～ 1000 の乗数値と 1 ～ 32 秒の負荷メトリックのポーリング レートが設定されます。システム リソースの使用量レベルの数値は、（倍率 * 現在のシステム リソースの使用量）/ 100 という式で計算されます。Cisco Technical Assistance Center（TAC）技術者からの指示がないかぎり、 **call admission load** コマンドを使用することは推奨しません。

IKE 用コール アドミッション制御の設定方法

IKE セキュリティ アソシエーション制限の設定

IKE SA の絶対制限値を設定するには、次の作業を実行します。制限値に達すると、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptocalladmissionlimit** {**all in-negotiation-sa** *number* | **ipsec sa** *number* | **ike** {**in-negotiation-sa** *number* | **sa** *number*}}
4. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptocalladmissionlimit** {**all in-negotiation-sa** *number* | **ipsec sa** *number* | **ike** {**in-negotiation-sa** *number* | **sa** *number*}} 例： `Router(config)# crypto call admission limit ike sa 25`	ネゴシエーション時の IKE SA の最大数、合計 SA 数、または IKE が新しい SA 要求を拒否し始める前に確立できる IKE SA まはた IPsec SA の最大数を指定します。
ステップ 4	**exit** 例： `Router(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、特権 EXEC モードに戻ります。

システム リソース制限の設定

システム リソースの制限値を設定するには、次の作業を実行します。負荷単位で設定されたレベルのシステム リソースが使用されている場合、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **calladmissionlimit***charge*
4. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**calladmissionlimit***charge* 例： `Router(config)# call admission limit 1000`	システム リソースを使用する場合、システム リソースのレベルを設定して、IKE による新しい SA 要求の受け入れを停止します。 • *charge*：有効な値は 1 ～ 100000 です。
ステップ 4	**exit** 例： `Router(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、特権 EXEC モードに戻ります。

IKE の CAC の設定確認

IKE 設定の CAC を確認するには、次の手順を実行します。

手順の概要

1. **showcalladmissionstatistics**
2. **showcryptocalladmissionstatistics**

手順の詳細

ステップ 1 **showcalladmissionstatistics**

このコマンドを使用して、グローバル CAC コンフィギュレーション パラメータおよび CAC の動作をモニタします。

例：

```
Router# show call admission statistics
Total Call admission charges: 82, limit 1000
Total calls rejected 1430, accepted 0
Load metric: charge 82, unscaled 82%
```

ステップ 2 **showcryptocalladmissionstatistics**

このコマンドを使用して、暗号 CAC 統計情報をモニタします。

例：

```
Router# show crypto call admission statistics
----------------------------------------------------------------------
                Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
Total IKE SA Count:           0 active:          0 negotiating:     0
Incoming IKE Requests:        0 accepted:        0 rejected:        0
Outgoing IKE Requests:        0 accepted:        0 rejected:        0
Rejected IKE Requests:        0 rsrc low:        0 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0
Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0
Phase1.5 SAs under negotiation:         0
```

IKE 用コール アドミッション制御の設定例

IKE セキュリティ アソシエーション制限値の設定例

次の例では、IKE が新しい SA 要求を拒否し始めるまでの SA の最大値を 25 に指定する方法を示します。

```
Router(config)# crypto call admission limit ike sa 25
```

システム リソース制限値の設定例

次の例では、負荷単位で設定されたシステム リソースのレベルが 9000 に達したときに、IKE が SA 要求を廃棄するように指定する方法を示します。

```
Router(config)# call admission limit 9000
```

その他の参考資料

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 Commands List, All Releases』
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
IKE コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco 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	Title
RFC 2409	『*The Internet Key Exchange*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

IKE 用コール アドミッション制御の機能情報

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*：*IKE* 用コール アドミッション制御の機能情報

機能名	リリース	機能情報
「Call Admission Control for IKE」	12.3(8)T 12.2(18)SXD1 12.4(6)T 12.2(33)SRA 12.2(33)SXH	IKE用コールアドミッション制御機能は、Cisco IOS ソフトウェアでのインターネットキーエクスチェンジ（IKE）プロトコルに対し、コール アドミッション制御（CAC）を適用したものです。 この機能は、Cisco IOS Release 12.3(8)T で導入されました。 この機能は Cisco IOS Release 12.2(18)SXD1 に統合され、Cisco 6500 および Cisco 7600 ルータに実装されました。 Cisco IOS Release 12.4(6)T では、ネゴシエーション時の IKE 接続数の制限を設定する機能が追加されました。 この機能に関する詳細については、次の各項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。 **calladmissionlimit**、**clearcryptocalladmissionstatistics**、**cryptocalladmissionlimit**、**showcalladmissionstatistics**、**showcryptocalladmissionstatistics**

機能名	リリース	機能情報
IKEv1 の強化	15.1(3)T	IKEv1 の強化機能とは、IKE 機能のコール アドミッション制御（CAC）に対して行われた拡張機能を表します。 この機能は、Cisco IOS Release 15.1(3)T で導入されました。 この機能に関する詳細については、次の各項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。 **cryptocalladmissionlimit**、**showcryptocalladmissionstatistics**

第 4 章

証明書/ISAKMP プロファイルマッピング

証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを割り当てることができます。また、この機能では、ISAKMP プロファイルに割り当てられたピアにグループ名を割り当てることもできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

証明書/ISAKMP プロファイルマッピングの前提条件

- 証明書マップの設定を理解している必要があります。
- ISAKMP プロファイルの設定を理解している必要があります。

証明書/ISAKMP プロファイルマッピングの制約事項

証明書を交換しないで、Rivest、Shamir、Adelman（RSA）シグニチャまたはRSA暗号化認証を使用する場合は、この機能を適用できません。ISAKMP ピアは、証明書を使用して RSA シグニチャまたは RSA 暗号化認証を実行するように設定する必要があります。

同じ認証局（CA）サーバに登録された 2 つのトラストポイントを使用する IPsec はサポートされません。2 つ以上の ISAKMP プロファイルがあり、各プロファイルが、同じ CA サーバに登録されているが異なるトラストポイントを持っている場合、応答側は最後のグローバル トラストポイントを選択します（トラストポイントは、グローバルに定義された順序と逆の順序で選択されます）。ピアが IPsec トンネルの確立を成功させるには、発信側が選択したトラストポイントは、応答側が選択したトラストポイントと一致する必要があります。トラストポイントが一致しない場合、他のすべての IPsec トンネルは、接続の確立に失敗します。

証明書/ISAKMP プロファイルマッピングに関する情報

証明書/ISAKMP プロファイルマッピングの概要

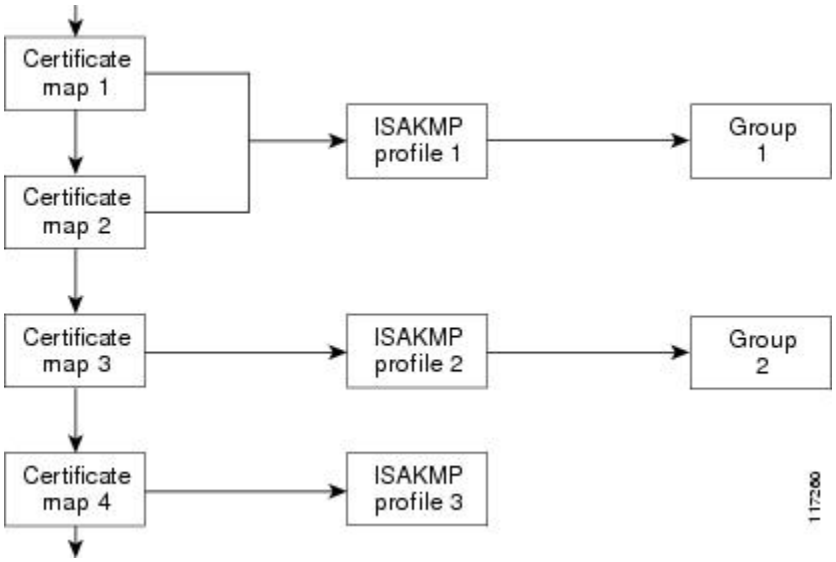
Cisco IOS Release12.3(8)T 以前では、ピアを ISAKMP プロファイルにマッピングする方法は、次の方法だけでした。ISAKMP 交換の ISAKMP ID フィールドは、ピアを ISAKMP プロファイルにマッピングするために使用されていました。証明書が認証に使用されるとき、ISAKMP ID ペイロードに証明書からの所有者名が含まれていました。CA が、要求されたグループ値を証明書の最初の組織ユニット（OU）フィールドに表示しなかった場合、ISAKMP プロファイルをピアに割り当てることはできませんでした。

Cisco IOS Release 12.3(8)T でも、上記のように、ピアをマッピングできます。証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに ISAKMP プロファイルを割り当てることができます。以前は、証明書の所有者名に基づいて ISAKMP プロファイルを割り当てるという方法しかありませんでした。また、この機能により、ISAKMP プロファイルが割り当てられたピアにグループを割り当てることができます。

証明書/ISAKMP プロファイルマッピングのしくみ

次の図に、証明書マップを ISAKMP プロファイルに接続し、証明書マップにグループ名を割り当てる方法を示します。

図 *1*：プロファイル グループ割り当てにマッピングされる証明書マップ



ISAKMP プロファイルには複数の証明書マップを接続できますが、証明書マップは 1 つの ISAKMP プロファイルにしか接続できません。

証明書マップにより、証明書を指定の一連の基準と照合できるようになります。ISAKMP プロファイルは、自身を証明書マップにバインドできます。また、提示された証明書が ISAKMP プロファイル内に存在する証明書マップと一致した場合、ピアに ISAKMP プロファイルが割り当てられます。ISAKMP プロファイルにクライアント設定グループ名が含まれている場合、同じグループ名がピアに割り当てられます。この ISAKMP プロファイル情報により、ID_KEY_ID アイデンティティまたは証明書の最初の OU フィールドの情報が上書きされます。

ピアへの ISAKMP プロファイルおよびグループ名の割り当て

証明書内の任意のフィールドに基づいて、ピアに ISAKMP プロファイルを割り当てるには、ISAKMP プロファイルを定義してから、**match certificate** コマンドを使用します。

ピアに割り当てられる ISAKMP プロファイルにグループ名を関連付けるには、ISAKMP プロファイルを定義してから、**client configuration group** コマンドを使用します。

証明書/ISAKMP プロファイルマッピングの設定方法

証明書/ISAKMP プロファイル マッピング

ISAKMPプロファイルに証明書をマッピングするには、次の手順を実行します。この設定により、証明書内の任意のフィールドの内容に基づいて、ピアにISAKMPプロファイルを割り当てることができます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpprofile***profile-name*
4. **matchcertificate***certificate-map*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoisakmpprofile***profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	ISAKMPプロファイルを定義し、暗号ISAKMP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	**matchcertificate***certificate-map* 例： `Router (conf-isa-prof)# match certificate map1`	証明書マップの名前を受け入れます。

証明書がマッピングされたことの確認

次の **show** コマンドを使って、証明書マップの所有者名が正しく設定されているか確認できます。

手順の概要

1. イネーブル化
2. **showcryptocacertificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptocacertificates** 例： `Router# show crypto ca certificates`	証明書に関する情報を表示します。

ピアへのグループ名の割り当て

ピアを ISAKMP プロファイルにマッピングするときにグループ名をピアに関連付けるには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpprofile***profile-name*
4. **clientconfigurationgroup***group-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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router# enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoisakmpprofile***profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	ISAKMP プロファイルを定義し、ISAKMP 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	**clientconfigurationgroup***group-name* 例： `Router (conf-isa-prof)# client configuration group group1`	この暗号 ISAKMP プロファイルにピアを割り当てるときに、そのピアに割り当てられるグループ名を受け入れます。

証明書/ISAKMP プロファイルマッピングのモニタおよびメンテナンス

ISAKMP プロファイル マッピングに対応する証明書をモニタし、メンテナンスするには、次の **debug** コマンドを使用します。

手順の概要

1. イネーブル化
2. **debugcryptoisakmp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • 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	**debugcryptoisakmp** 例： `Router# debug crypto isakmp`	証明書が、証明書マップの照合を経て、ISAKMP プロファイルと一致することを示す出力を表示します。 このコマンドは、ピアにグループが割り当てられたことを確認する場合にも使用できます。

証明書/ISAKMP プロファイルマッピングの設定例

任意のフィールドに基づいた ISAKMP プロファイルへの証明書のマッピング：例

次の設定例では、証明書に「ou = green」が含まれているときは必ず、ISAKMP プロファイル「cert_pro」がピアに割り当てられる、ということを示します。

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   initiate mode aggressive
   match certificate cert_map
```

ISAKMP プロファイルに関連付けられたピアに割り当てられるグループ名の例

次の例は、グループ「some_group」が、ISAKMP プロファイルが割り当てられたピアに関連付けられていることを示しています。

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

ISAKMP プロファイルへの証明書のマッピング検証例

次の例は、ISAKMP プロファイルに証明書がマッピングされたことを示します。この例には、応答側および発信側の設定、証明書マップの所有者名が設定されたことを確認する**show コマンド**出

力、および証明書が証明書マップの照合を経てISAKMPプロファイルに一致したことを示す**debug**コマンド出力が含まれています。

応答側の設定

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
 subject-name co ou = green
! The above line shows that the subject name must have "ou = green."
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
of the peer matches cert_map (shown on third line below).
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   initiate mode aggressive
```

発信側の設定

```
crypto ca trustpoint LaBcA
 enrollment url http://10.76.82.20:80/cgi-bin/openscep
 subject-name ou=green,c=IN
! The above line ensures that the subject name "ou = green" is set.
 revocation-check none
```

発信側の **show crypto ca certificates** コマンド出力

```
Router# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 21
  Certificate Usage: General Purpose
  Issuer:
    cn=blue-lab CA
    o=CISCO
    c=IN
  Subject:
    Name: Router1.cisco.com
    c=IN
    ou=green
! The above line is a double check that "ou = green" has been set as the subject name.
    hostname=Router1.cisco.com
  Validity Date:
    start date: 14:34:30 UTC Mar 31 2004
    end   date: 14:34:30 UTC Apr 1 2009
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: LaBcA
```

応答側の **debug crypto isakmp** コマンド出力

```
Router# debug crypto isakmp
6d23h: ISAKMP (0:268435460): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
 MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
6d23h: ISAKMP:(0:4:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:4:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:4:HW:2): processing ID payload. message ID = 0
```

```
6d23h: ISAKMP (0:268435460): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : Router1.cisco.com
        protocol     : 17
        port         : 500
        length       : 28
6d23h: ISAKMP:(0:4:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:4:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:4:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:4:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:4:HW:2): OU = green
6d23h: ISAKMP:(0:4:HW:2): certificate map matches certpro profile
! The above line shows that the certificate has gone through certificate map matching and
that it matches the "certpro" profile.
6d23h: ISAKMP:(0:4:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:4:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:4:HW:2): CERT validity confirmed.
```

ピアに割り当てられたグループ名の検証例

次の設定およびデバッグ出力は、グループがピアに割り当てられたことを示します。

発信側の設定

```
crypto isakmp profile certpro
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   client configuration group new_group
! The statement on the above line will assign the group "new_group" to any peer that matches
 the ISAKMP profile "certpro."
   initiate mode aggressive
!
```

応答側の debug crypto isakmp プロファイル コマンド出力

次のデバッグ出力例は、ピアが「certpro」という ISAKMP プロファイルと照合され、「new_group」というグループが割り当てられたことを示します。

```
Router# debug crypto isakmp profile
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
 MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : Router1.cisco.com
        protocol     : 17
        port         : 500
        length       : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
```

```
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ISAKMP プロファイルの設定	VRF 認識 IPSec
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
なし	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	Title
なし	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

証明書/ISAKMP プロファイルマッピングの機能情報

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 *3*：証明書*/ISAKMP* プロファイルマッピングの機能情報

機能名	リリース	機能情報
証明書/ISAKMP プロファイルマッピング	12.3(8)T 12.2(33)SRA 12.2(33)SXH	証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを割り当てることができます。また、この機能では、ISAKMP プロファイルに割り当てられたピアにグループ名を割り当てることもできます。 この機能は、Cisco IOS Release12.3(8)T で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。

第 5 章

「Encrypted Preshared Key」

暗号化事前共有キー機能を使用すると、プレーンテキストのパスワードをタイプ6（暗号化）形式で NVRAM に安全に保管できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

暗号化事前共有キーの制約事項

- 古い ROM モニタ（ROMMON）およびブート イメージでは、新しいタイプ 6 パスワードが認識されません。そのため、旧来の ROMMON から起動すると、エラーが発生します。

- Cisco 836 ルータでは、Advanced Encryption Standard（AES）を使用できるのは IP Plus イメージ上に限ります。

暗号化事前共有キーに関する情報

暗号化事前共有キーの使用によるパスワードのセキュアな保存

暗号化事前共有キー機能を使用すると、コマンドライン インターフェイス（CLI）から、プレーンテキストのパスワードをタイプ 6 形式で NVRAM へセキュアに保存できます。タイプ 6 のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**keyconfig-key** コマンドおよび **passwordencryptionaes** コマンドを使用すると、パスワードを設定して有効化できます（キーの暗号化には、対称暗号である AES が使用されます）。**config-keypassword-encryption** コマンドを使用して設定されたパスワード（キー）は、ルータ内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

passwordencryptionaes コマンドを設定する際、同時に **keyconfig-key** コマンドを設定しないと、**showrunning-config** コマンドや **copyrunning-configstartup-config** コマンドなどが設定されている起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encryption コマンドを使用してパスワード（マスター キー）が変更された場合、または再暗号化された場合には、リスト レジストリから、タイプ 6 暗号が使用されているアプリケーション モジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

keyconfig-keypassword-encryption コマンドを使用して設定されたマスター キーがシステムから削除されると、タイプ 6 のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティ対策として、暗号化されたパスワードは、Cisco IOS XE ソフトウェアによって復号化されることはなくなります。ただし、すでに説明したように、パスワードを再暗号化することはできます。

注意 **keyconfig-keypassword-encryption** コマンドを使用して設定されたパスワードは、一度失われると回復できません。パスワードは、安全な場所に保存することを推奨します。

パスワード暗号化の設定解除

あとの段階で **no password encryption aes** コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encryption** コマンドを使用して設定したパスワード（マスター キー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。

パスワードの保存

（**key config-key password-encryption** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、ルータからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、ルータにはロードできません。設定をルータにロードする前後には、（**key config-key password-encryption** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカット アンド ペーストした暗号文は、それがマスター キーに適合しない場合やマスター キーが存在しない場合でも、受理または保存されます。ただしこの場合にはアラート メッセージが出力されます。アラート メッセージの内容は次のとおりです。

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

マスター キーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ 6 のキーになります。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスター キーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encryption** コマンドを使用してそのマスター キーを削除できます。**no key config-key password-encryption** コマンドを使用してマスター キーを削除しても、既存の暗号化パスワードは、暗号化された状態のままルータ設定内に保持されます。これらのパスワードは復号化されません。

暗号化事前共有キーのイネーブル化

password encryption aes コマンドを使用すると、暗号化されたパスワードを有効化できます。

暗号化事前共有キーの設定方法

暗号化事前共有キーの設定

暗号化事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **keyconfig-keypassword-encryption** [*text*]
4. **passwordencryptionaes**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**keyconfig-keypassword-encryption** [*text*] 例： `Router (config)# key config-key password-encryption`	タイプ 6 の暗号キーをプライベート NVRAM に保存します。 • （Enter キーを使用して）インタラクティブにキーボード操作を行う場合、暗号キーがすでに存在すれば、Old key、New key、Confirm key という 3 つのプロンプトが表示されます。 • インタラクティブにキーボード操作を行う場合、暗号キーが存在しなければ、New key、Confirm key という 2 つのプロンプトが表示されます。 • すでに暗号化されているパスワードを削除する場合は、次のプロンプトが表示されます。「WARNING: All type 6 encrypted keys will become unusable.Continue with master key deletion? [yes/no]:」

	コマンドまたはアクション	目的
ステップ 4	**passwordencryptionaes** 例： `Router (config)# password-encryption aes`	暗号化事前共有キーのイネーブル化

トラブルシューティングのヒント

「ciphertext >[for username bar>] is incompatible with the configured master key」という警告メッセージが表示された場合は、入力またはカット アンド ペーストした暗号文がマスター キーに適合しないか、またはマスターキーが存在しないと判断できます（暗号文は受理または保存されます）。この警告メッセージを手掛かりにすれば、設定の不具合箇所を特定できます。

暗号化事前共有キーのモニタリング

暗号化事前共有キーに関するロギングを出力するには、次の手順を実行します。

1 イネーブル化
2 **passwordlogging**

手順の概要

1. イネーブル化
2. **passwordlogging**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**passwordlogging** 例： `Router# password logging`	タイプ 6 パスワードの処理に関するデバッグ出力のログを表示します。

例

次に示すのは、**passwordlogging** によるデバッグ出力の表示例です。ここでは、マスター キーが新規に設定された場合と、その新しいマスター キーを使用してそのキーが暗号化された場合が表示されています。

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas
Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

次の作業

次に示す作業を実行できます。これらの各作業は、互いに独立したものです。

ISAKMP 事前共有キーの設定

ISAKMP 事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpkey***keystring***address***peer-address*
4. **cryptoisakmpkey***keystring***hostname***hostname*

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • 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	**configureterminal** 例： `Router# 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	**cryptoisakmpkey***keystring***address***peer-address* 例： `Router (config)# crypto isakmp key cisco address 10.2.3.4`	事前共有認証キーを設定します。 • *peer-address* 引数には、リモート ピアの IP アドレスを指定します。
ステップ 4	**cryptoisakmpkey***keystring***hostname***hostname* 例： `Router (config)# crypto isakmp key mykey hostname mydomain.com`	事前共有認証キーを設定します。 • *hostname* 引数には、ピアの完全修飾ドメイン名（FQDN）を指定します。

例

次に示すのは、暗号化事前共有キーが設定された場合の出力例です。

```
crypto isakmp key 6 _Hg[^^ECgLGGPF^RXTQfDDWQ][YAAB address 10.2.3.4
crypto isakmp key 6 `eR\eTRaKCUZPYYQfDgXRWi_AAB hostname mydomain.com
```

ISAKMP キーリングの ISAKMP 事前共有キーの設定

IPSec 仮想経路フォワーディング（VRF）で使用される ISAKMP リングの ISAKMP 事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptokeyring***keyring-name*
4. **pre-shared-keyaddress***address***key***key*
5. **pre-shared-keyhostname***hostname***key***key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptokeyring***keyring-name* 例： `Router (config)# crypto keyring mykeyring`	インターネット キー交換（IKE）認証で使用する暗号キーリングを定義し、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	**pre-shared-keyaddress***address***key***key* 例： `Router (config-keyring)# pre-shared-key address 10.2.3.5 key cisco`	IKE 認証に使用する事前共有キーを定義します。 • *address* 引数には、リモート ピアの IP アドレスを指定します。
ステップ 5	**pre-shared-keyhostname***hostname***key***key* 例： `Router (config-keyring)# pre-shared-key hostname mydomain.com key cisco`	IKE 認証に使用する事前共有キーを定義します。 • *hostname* 引数には、ピアの FQDN を指定します。

例

次に示すのは、ISAKMP キーリングの暗号化された事前共有キーが設定された場合の **show-running-config** による出力例です。

```
crypto keyring mykeyring
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname mydomain.com key 6 aE_REHDcOfYCPF^RXTQfDJYVVNSAAB
```

ISAKMP アグレッシブ モードの設定

ISAKMP アグレッシブ モードを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmppeerip-address***ip-address*
4. **setaggressive-modeclient-endpoint***client-endpoint*
5. **setaggressive-modepassword***password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoisakmppeerip-address***ip-address* 例： `Router (config)# crypto isakmp peer ip-address 10.2.3.4`	アグレッシブ モードのトンネル属性に関し、IP セキュリティ（IPSec）ピアによる認証、許可、アカウンティング（AAA）の IKE クエリーをイネーブルにし、ISAKMP ピア 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	**setaggressive-modeclient-endpoint***client-endpoint* 例： `Router (config-isakmp-peer)# set aggressive-mode client-endpoint fqdn cisco.com`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint 属性を指定します。
ステップ 5	**setaggressive-modepassword***password* 例： `Router (config-isakmp-peer)# set aggressive-mode password cisco`	ISAKMP ピア設定内で、Tunnel-Password 属性を指定します。

例

次に示すのは、ISAKMP アグレッシブ モードで、暗号化された事前共有キーが設定された場合の **show-running-config** による出力例です。

```
crypto isakmp peer address 10.2.3.4
 set aggressive-mode password 6 ^aKPIQ_KJE_PPF^RXTQfDTIaLNeAAB
 set aggressive-mode client-endpoint fqdn cisco.com
```

Unity サーバ グループ ポリシーの設定

Unity サーバ グループ ポリシーを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpclientconfigurationgroup***group-name*
4. **pool***name*
5. **domainname**
6. **key***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	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoisakmpclientconfigurationgroup***group-name* 例： `Router (config)# crypto isakmp client configuration group mygroup`	定義するグループのポリシープロファイルを指定し、ISAKMP グループ 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	**pool***name* 例： `Router (config-isakmp-group)# pool mypool`	ローカル プール アドレスを定義します。

	コマンドまたはアクション	目的
ステップ 5	**domainname** 例： `Router (config-isakmp-group)# domain cisco.com`	グループが属するドメイン ネーム サービス（DNS）ドメインを指定します。
ステップ 6	**key***name* 例： `Router (config-isakmp-group)# key cisco`	グループ ポリシー属性の定義に使用する IKE 事前共有キーを指定します。

例

次に示すのは、暗号化されたキーが Unity サーバ グループ ポリシーに対して設定された場合の **show-running-config** による出力例です。

```
crypto isakmp client configuration group mygroup
 key 6 cZZgDZPOE\dDPF^RXTQfDTIaLNeAAB
 domain cisco.com
 pool mypool
```

Easy VPN クライアントの設定

Easy VPN クライアントを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoipsecclientezvpn***name*
4. **peer***ipaddress*
5. **modeclient**
6. **group***group-name***key***group-key*
7. **connectmanual**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router# enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoipsecclientezvpn***name* 例： `Router (config)# crypto ipsec client ezvpn myclient`	Cisco Easy VPN Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote 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***ipaddress* 例： `Router (config-isakmp-peer)# peer 10.2.3.4`	VPN 接続に対して、ピアの IP アドレスを設定します。
ステップ 5	**modeclient** 例： `Router (config-isakmp-ezpvy)# mode client`	ネットワーク アドレス変換（NAT）またはピア アドレス変換（PAT）を使用する Cisco Easy VPN クライアント モードでの動作用にルータを自動設定します。
ステップ 6	**group***group-name***key***group-key* 例： `Router (config-isakmp-ezvpn)# group mygroup key cisco`	VPN 接続に使用するグループ名およびキー値を指定します。
ステップ 7	**connectmanual** 例： `Router (config-isakmp-ezvpn)# connect manual`	手動設定を指定して、Cisco Easy VPN Remote クライアントに対し、コマンドまたはアプリケーション プログラミング インターフェイス（API）のコールを待機してから、Cisco Easy VPN リモート接続の確立を試行するよう指示します。

例

次に示すのは、Easy VPN クライアントが設定された場合の **show-running-config** による出力例です。このキーは暗号化されています。

```
crypto ipsec client ezvpn myclient
 connect manual
 group mygroup key 6 gdMI`S^^[GIcPF^RXTQfDFKEO\RAAB
 mode client
 peer 10.2.3.4
```

暗号化事前共有キーの設定例

暗号化事前共有キー：例

次に示すのは、タイプ 6 の事前共有キーが暗号化された場合の設定例です。この中には、ユーザに対して表示されるプロンプトやメッセージも含まれています。

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show running-config | include crypto isakmp key
 crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# password encryption aes

Router (config)# key config-key password-encrypt

New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

キーが存在しない場合の例

次の設定例には、以前のキーがありません。

```
Router (config)#
```

キーが存在する場合の例

次の設定例には、キーがすでに存在しています。

```
Router (config)#
Old key:
Router (config)#
```

キーが存在する状況でユーザがインタラクティブにキーを入力する場合の例

次の設定例では、ユーザは対話形式の入力を求めていますが、キーはすでに存在しています。**keyconfig-key** コマンドを入力し、Enter キーを押してインタラクティブ モードを開始すると、画面には Old key、New key、Confirm key という 3 つのプロンプトが表示されます。

```
Router (config)#
Old key:
New key:
Confirm key:
```

キーが存在しない状況でユーザがインタラクティブにキーを入力する場合の例

次に示すのは、キーが存在しない状況でユーザがインタラクティブにキーボード操作を行う場合の設定例です。対話モードを開始すると、画面には New key および Confirm key という 2 つのプロンプトが表示されます。

```
Router (config)#

New key:
Confirm key:
```

パスワード暗号化の設定解除の例

次に示すのは、ユーザがパスワード暗号化の設定を解除する場合の設定例です。「WARNING: All type 6 encrypted keys will become unusable.Continue with master key deletion? [yes/no]:」 というプロンプトが画面に表示されます（インタラクティブ モードの場合）。

```
Router (config)#
WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion
 ? [yes/no]: y
```

次の作業

その他の事前共有キーを設定します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
パスワードの設定	『*Cisco IOS Security Command Reference*』

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
なし	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	Title
なし	--

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

第 6 章

識別名ベースのクリプト マップ

機能の履歴

リリース	変更内容
12.2(4)T	この機能が導入されました。

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

この章では、Cisco IOS Release 12.2(4)T の識別名ベースの暗号マップ機能について説明します。次のセクションで構成されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用の

プラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

機能の概要

識別名ベースのクリプト マップ機能により、証明書（特に特定の識別名（DN）持つ特定の証明書）を持つピアの選択された暗号化インターフェイスだけに、アクセスを制限するようにルータを設定できます。

以前まで、暗号化ピアからルータが証明書または共有秘密を受け入れる場合、Cisco IOS では暗号化ピアの IP アドレスによって制限する以外、暗号化されたインターフェイスとピアが通信するのを防ぐ方法がありませんでした。この機能により、ピアが自身の認証に使用した DN に基づいて、ピアが使用できるクリプト マップを設定し、特定の DN を持つピアがアクセスできる暗号化インターフェイスを制御できます。

利点

識別名ベースの暗号マップ機能では、暗号化インターフェイスを選択し、特定の証明書（なかでも特別な DN を持つ証明書）を持つピアがそのインターフェイスにアクセスしないよう、ルータに制限を設定できます。

機能制限

システム要件

この機能を設定するには、ルータが IP セキュリティをサポートする必要があります。

パフォーマンス上の影響

アクセスを制限する DN が多い場合、少数のアイデンティティ セクションを参照する多数のクリプト マップを指定するよりも、多数のアイデンティティ セクションを参照する少数のクリプト マップを指定することを推奨します。

関連資料

次のマニュアルには、識別名ベースのクリプト マップ機能の関連情報が記載されています。

- 『Cisco IOS Security Command Reference』

- 『Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T』
- Next Generation Encryption（NGE）ホワイト ペーパー。

サポートされるプラットフォーム

この機能は、次のプラットフォームでサポートされます。

- Cisco 1700 シリーズ
- Cisco 2600 シリーズ
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 シリーズ
- Cisco 7200 シリーズ
- Cisco uBR905 ケーブル アクセス ルータ
- Cisco uBR925 ケーブル アクセス ルータ

Feature Navigator を使用したプラットフォーム サポートの判別

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。

サポートされている規格 MIB および RFC

標準

なし

MIB

なし

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

RFC

なし

前提条件

DN ベースのクリプト マップを設定する前に、次の作業を実行する必要があります。

- ピアごとに IKE ポリシーを作成します。

IKE ポリシーの作成についての詳細は、『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Configuring Internet Key Exchange for IPsec VPNs」の章を参照してください。

- IPSec のクリプト マップ エントリを作成します。

暗号マップ エントリの作成についての詳細は、『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Configuring Security for VPNs with IPsec」の章を参照してください。

設定作業

クリプト マップ エントリの作成に関する詳細については、「IPsec VPN のセキュリティの設定」を参照してください。一覧内の各作業は、必須と任意に分けています。

- （DN によって認証された）DN ベースの暗号マップの設定, （74 ページ） （必須）
- （ホスト名によって認証された）DN ベースの暗号マップの設定, （75 ページ） （必須）
- DN ベースの暗号マップへの ID の適用, （75 ページ） （必須）
- DN ベースの暗号マップの確認, （76 ページ） （任意）

（DN によって認証された）DN ベースの暗号マップの設定

DN によって認証されたピアだけが使用できる DN ベースのクリプト マップを設定するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

手順の概要

1. Router(config)# **crypto identity** *name*
2. Router(crypto-identity)# **dn** *name=string* [,*name=string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **crypto identity** *name*	ルータの証明書内にある指定DNリストを使用してルータのアイデンティティを設定し、暗号アイデンティティ 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 2	Router(crypto-identity)# **dn** *name=string* [,*name=string*]	ルータの証明書内にあるDNに、ルータのアイデンティティを関連付けます。 （注） ピアのアイデンティティは、交換された証明書のアイデンティティと一致する必要があります。

（ホスト名によって認証された）DN ベースの暗号マップの設定

ホスト名によって認証されたピアだけが使用できるDNベースのクリプトマップを設定するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

手順の概要

1. Router(config)# **crypto identity** *name*
2. Router(crypto-identity)# **fqdn** *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	Router(config)# **crypto identity** *name*	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 2	Router(crypto-identity)# **fqdn** *name*	ピアの認証に使用したホスト名にルータのアイデンティティを関連付けます。 （注） ピアのアイデンティティは、交換された証明書のアイデンティティと一致する必要があります。

DN ベースの暗号マップへの ID の適用

（クリプトマップのコンテキスト内で）アイデンティティを適用するには、グローバルコンフィギュレーション モードの開始時に次のコマンドを使用します。

手順の概要

1. Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**
2. Router(config-crypto-map)# **identity** *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	Router(config)# **crypto map** *map-name seq-num* **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。
ステップ 2	Router(config-crypto-map)# **identity** *name*	クリプト マップに対して ID を適用します。 このコマンドを適用した場合、**identity** *name* でリストされているコンフィギュレーションと一致するホストだけが、指定した暗号マップを使用できます。 （注） 暗号マップ内に **identity** コマンドが表示されない場合は、暗号化ピアの IP アドレスを除き、暗号化接続に制約はありません。

DN ベースの暗号マップの確認

この機能が適切に設定されているかを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router#` **show crypto identity**	設定したアイデンティティを表示します。

トラブルシューティングのヒント

暗号化ピアが接続を確立しようと試み、それが DN ベースのクリプト マップ設定によってブロックされた場合、次のエラー メッセージが記録されます。

```
<time>: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted connection attempted with a peer without
 the configured certificate attributes.
```

設定例

DN ベースの暗号マップの設定例

次の例では、DN およびホスト名によって認証された DN ベースのクリプト マップを設定する方法を示します。間にコマンドを説明するためのコメントが含まれています。

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
 encryption aes
 hash sha
 authentication rsa-sig
 group 14
 lifetime 5000
crypto isakmp policy 20
 encryption aes
 hash sha
 authentication pre-share
 group 14
 lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

第 7 章

IPsec と Quality of Service

IPsec と Quality of Service 機能を使用すれば、Cisco IOS Quality of Service（QoS）ポリシーを、QoS グループに基づいて、IP Security（IPsec）パケット フローに適用できます。QoS グループは、現在の Internet Security Association and Key Management Protocol（ISAKMP）プロファイルに適用できます。

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の検索

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで **[Cancel]** をクリックし、表示される説明に従ってください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

IPsec と Quality of Service の前提条件

- IPsec、および ISAKMP プロファイルの概念についての知識が必要です。
- Cisco IOS QoS の知識が必要です。

IPsec と Quality of Service の制約事項

- この機能を適用できるのはISAKMPプロファイルを介してだけです。QoSアプリケーションに対して使用できる QoS グループは 128 個までという制限はこの機能にも当てはまります。
- IPsec QoS グループを適用できるのは、発信サービス ポリシーに対してだけです。
- QoS は、ソフトウェア暗号化に関してはサポートされません。

IPsec と Quality of Service に関する情報

IPsec と Quality of Service の概要

IPsec と Quality of Service 機能を使用すれば、QoS グループを ISAKMP プロファイルに追加することによって、トラフィック ポリシングおよびシェーピングなどの QoS ポリシーを QoS ポリシーに適用できます。QoS グループが追加されると、このグループの値が、QoS クラス マップ内で定義されたものと同じ QoS グループにマッピングされます。この QoS グループ タグを利用している現在の QoS 方式はすべて、IPsec パケット フローに適用できます。パケット フローの共通グルーピングには、IPsec QoS グループを QoS メカニズムにとって使用可能にすることによって、特定のポリシー クラスを適用できます。IPsec フローをマーキングすれば、QoS メカニズムを、特定のグループが使用可能な帯域幅の制限や特定のフロー上のタイプ オブ サービス（ToS）ビットのマーキングなどをサポート可能なトラフィックのクラスに適用できます。

ISAKMP プロファイルは、アイデンティティ照合基準方式によってデバイスを一意に識別できるプロファイルなので、QoS グループのアプリケーションは、ISAKMP プロファイル レベルで適用されます。これらの基準は、インターネット キー交換（IKE）IDに基づいています。このIDは、受信 IKE 接続によって提供され、IP アドレス、完全修飾ドメイン名（FQDN）、およびグループ（つまり、バーチャル プライベート ネットワーク [VPN] リモート クライアント グルーピング）などが格納されます。アイデンティティ照合基準の粒度によって、指定された QoS ポリシーの粒度に制約が課せられます。たとえば、「Engineering」という名前の VPN クライアント グループに所属するすべてのトラフィックを、「TOS 5」としてマーキングします。指定した QoS ポリシーの粒度に制約を課すその他の例としては、発信 WAN リンクの 30 パーセントをリモート VPN デバイスの特定のグループへ割り当てるなどがあります。

IPsec と Quality of Service の設定方法

IPsec と Quality of Service の設定

QoS ポリシーを ISAKMP プロファイルに適用するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmp-profile***profile-number*
4. **qos-group***group-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoisakmp-profile***profile-number* 例： `Router (config)# crypto isakmp-profile vpnprofile`	ISAKMP プロファイルを定義し、IPsec ユーザ セッションを監査し、ISAKMP 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	**qos-group***group-number* 例： `Router(config-isa-prof)# qos-group 1`	QoS グループ値を ISAKMP プロファイルに適用します。

IPsec と Quality of Service セッションの確認

IPsec and QoS セッションを確認するには、次の手順を実行します。**show** コマンドは、任意の順序か互いに独立させて使用できます。

手順の概要

1. イネーブル化
2. **showcryptoisakmpprofile**
3. **showcryptoipsecsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptoisakmpprofile** 例： `Router# show crypto isakmp profile`	QoS グループがプロファイルに適用されていることを表示します。

	コマンドまたはアクション	目的
ステップ 3	**showcryptoipsecsa** 例： `Router# show crypto ipsec sa`	QoS グループが、IPsec セキュリティ アソシエーション（SA）の特定のペアに適用されていることを表示します。

トラブルシューティングのヒント

IPsecセッションおよびQoSセッションに問題が発生した場合、次が実行されているかどうかを確認します。

- 『*Cisco IOS Quality of Service Solutions Command Reference*』に記載されている QoS 専用コマンドを使用して、QoS の適用を QoS サービスごとに確認している。
- クラスマップ一致基準に指定されたものと同じQoSグループと一致しているルータ上のQoSポリシーを設定している。
- クリプト マップが適用されるものと同じインターフェイスにサービス ポリシーを適用している。

IPsec と Quality of Service の設定例

リモート ユーザの 2 つのグループに適用された QoS ポリシーの例

次に、特定の QoS ポリシーがリモート ユーザの 2 つのグループに適用されている例を示します。2つのプロファイルが、IKE を介した最初の接続上でリモートユーザが特定のプロファイルにマッピングされるように設定されています。そのプロファイルから、そのリモートに対して作成されたすべての IPsec SA が特定の QoS グループでマーキングされます。トラフィックが発信インターフェイスを出ると、QoS サービスによって、その発信インターフェイス上で適用されているサービス ポリシーを構成するクラス マップ内で指定された QoS グループで IPsec 設定 QoS グループがマッピングされます。

```
version 12.3
!
aaa authentication login group group radius
aaa authorization network autho local
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
!
!
ip cef
no ip domain lookup
```

```
!
class-map match-all yellow
 match qos-group 3
class-map match-all blue
match qos-group 2
!
!
policy-map clients
 class blue
  set precedence 5
 class yellow
  set precedence 7
!
!
crypto isakmp policy 1
 encr aes
 hash sha
 authentication pre-share
 group 14
 lifetime 300
!
crypto isakmp keepalive 10 periodic
crypto isakmp xauth timeout 20
!
crypto isakmp client configuration group blue
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 pool blue
 save-password
 include-local-lan
 backup-gateway corky1.cisco.com
!
crypto isakmp client configuration group yellow
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.5
 pool yellow
!
crypto isakmp profile blue
   match identity group cisco
   client authentication list autho
   isakmp authorization list autho
   client configuration address respond
   qos-group 2
crypto isakmp profile yellow
   match identity group yellow
   match identity address 10.0.0.11 255.255.255.255
   client authentication list autho
   isakmp authorization list autho
   client configuration address respond
   qos-group 3
!
!
crypto ipsec transform-set combo ah-sha-hmac esp-aes esp-sha-hmac
crypto ipsec transform-set client esp-aes esp-sha-hmac comp-lzs
!
crypto dynamic-map mode 1
 set security-association lifetime seconds 180
 set transform-set client
 set isakmp-profile blue
 reverse-route
crypto dynamic-map mode 2
 set transform-set combo
 set isakmp-profile yellow
 reverse-route
!
crypto map mode 1 ipsec-isakmp dynamic mode
!
interface FastEthernet0/0
 ip address 10.0.0.110 255.255.255.0
 no ip redirects
 no ip proxy-arp
 no ip mroute-cache
```

```
 duplex half
 no cdp enable
 crypto map mode
 service-policy out clients
!
ip local pool yellow 192.168.2.1 192.168.2.10
ip local pool blue 192.168.6.1 192.168.6.6
no ip classless
!
radius-server host 10.0.0.13 auth-port 1645 acct-port 1646
radius-server key XXXXXX
radius-server vsa send accounting
radius-server vsa send authentication
```

show crypto isakmp profile コマンドの例

次の出力では、QoS グループ「2」が ISAKMP プロファイル「blue」に適用され、QoS グループ「3」が ISAKMP プロファイル「yellow」に適用されていることを示しています。

```
Router# show crypto isakmp profile
ISAKMP PROFILE blue
   Identities matched are:
    group blue
   QoS Group 2 is applied
ISAKMP PROFILE yellow
   Identities matched are:
    ip-address 10.0.0.13 255.255.255.255
    group yellow
   QoS Group 3 is applied
```

show crypto ipsec sa コマンドの例

次の出力では、QoS グループが IPsec SA の特定のペアに適用されていることを示しています。

```
Router# show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: mode, local addr. 10.0.0.110
   protected vrf:
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.12.12.0/255.255.255.0/0/0)
   current_peer: 10.0.0.11:500
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     qos group is set to 2
```

その他の参考資料

ここでは、IPsec と Quality of Service 機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IPSec	IPsec を使用した VPN のセキュリティの設定
QoS オプション	『*Cisco IOS Quality of Service Solutions Configuration Guide*』（Cisco.com）
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	次世代暗号化

標準

標準	Title
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec と Quality of Service の機能情報

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 *4*：*IPsec* と *Quality of Service* の機能情報

機能名	リリース	機能情報
IPsec と Quality of Service	Cisco IOS XE Release 3.9S	IPsec と Quality of Service 機能を使用すれば、Cisco IOS Quality of Service（QoS）ポリシーを、QoS グループに基づいて、IP Security（IPsec）パケットフローに適用できます。QoS グループは、現在の Internet Security Association and Key Management Protocol（ISAKMP）プロファイルに適用できます。 次のコマンドが導入または変更されました。**qos-group**

第 8 章

VRF 認識 IPSec

VRF-Aware IPsec 機能には、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）に対する IP Security（IPsec）トンネル マッピングが導入されています。VRF-Aware IPsec 機能を使用すれば、シングル パブリック方向アドレスによって、VPN ルーティング/転送（VRF）に対して IPsec トンネルをマッピングできます。

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

VRF-Aware IPsec に関する制約事項

- クリプト マップ設定を使用して VRF-Aware IPsec 機能を設定し、Inside VRF（IVRF）が Front Door VRF（FVRF）とは異なる場合、ユニキャスト RPF（uRPF）がクリプト マップ インターフェイス上でイネーブルになっていると、この機能と uRPFの相互運用はできなくなります。ネットワークに URPF が必要な場合、クリプト マップではなく、IPsec の Virtual Tunnel Interface（VTI）を使用することを推奨します。
- VRF-Aware IPsec 機能では、VRF 間における IPsec トンネル マッピングはできません。たとえば、VRF vpn1 から VRF vpn2 への IPsec トンネル マッピングはできません。
- VRF-Aware IPsec 機能をクリプト マップと使用した場合、このクリプト マップではグローバル VRF を IVRF として使用し、非グローバル VRF を FVRF として使用することはできません。しかし、仮想トンネル インターフェイスに基づく設定にその制限はありません。VTI またはダイナミック VTI（DVTI）を使用した場合、グローバル VRF を IVRF と使用すると同時に、非グローバル VRF を FVRF として使用できます。
- ISAKMP プロファイルおよびキーリングで VRF とともにローカル アドレスを使用する場合は、VRFを **local-address** コマンドに含める必要があります。

VRF-Aware IPsec に関する情報

VRF インスタンス

VRF は、VPN ごとのルーティング情報リポジトリであり、プロバイダー エッジ（PE）ルータに接続されたカスタマー サイトの VPN メンバーシップが定義されています。VRF は、IP ルーティング テーブル、派生シスコ エクスプレス フォワーディング（CEF）テーブル、転送テーブルを使用するインターフェイスのセット、ルーティング テーブルに含まれる情報を制御するルールおよびルーティング プロトコル パラメータのセットで構成されています。各 VPN カスタマーに対して、別個の一連のルーティング テーブルおよび Cisco Express Forwarding（CEF）テーブルが維持されます。

MPLS 配信プロトコル

MPLS 配信プロトコルは、高性能のパケット転送テクノロジーであり、データ リンク層スイッチングのパフォーマンスおよびトラフィック管理機能と、ネットワーク層ルーティングのスケーラビリティ、柔軟性、およびパフォーマンスが統合されています。

VRF-Aware IPsec 機能の概要

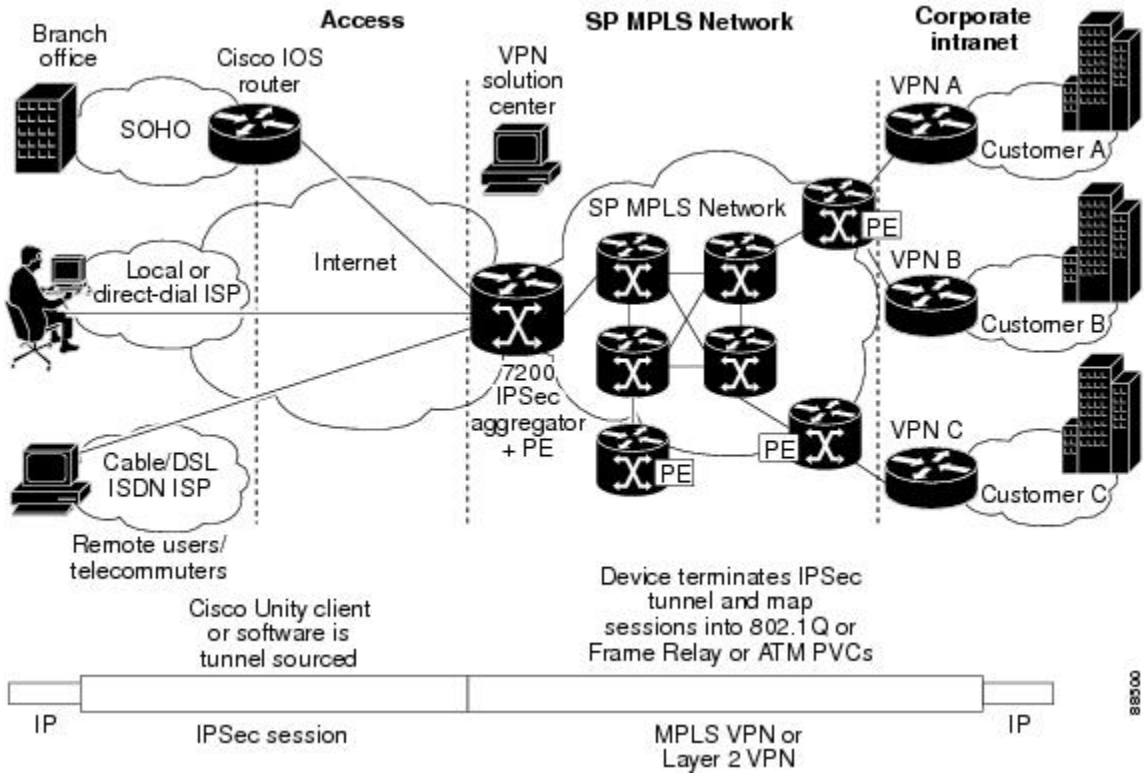
Front Door VRF（FVRF）と Inside VRF（IVRF）が、この機能を理解するうえで重要な概念となります。

各 IPsec トンネルは、2 つの VRF ドメインに関連付けられます。外部のカプセル化されたパケットは 1 つの VRF ドメイン（本マニュアルでは FVRF と呼びます）に所属し、内部の保護された IP パケットは IVRF と呼ばれる別のドメインに所属します。言い換えると、IPsec トンネルのローカル エンドポイントは FVRF に所属し、内部パケットの発信元および宛先アドレスは IVRF に所属します。

1 つ以上の IPsec トンネルを、単一のインターフェイス上で終了できます。これらのトンネルのすべての FVRF は同じものであり、そのインターフェイス上で設定されている VRF に設定されます。これらのトンネルの IVRF は異なる可能性があり、クリプト マップ エントリに付加された Security Association and Key Management Protocol（ISAKMP）プロファイル内で定義されている VRF に依存します。

次の図は、MPLS およびレイヤ 2 VPN に対する IPsec のシナリオを示しています。

図 *2*：***MPLS*** およびレイヤ ***2 VPN*** に対する ***IPsec***



IPsec トンネルへのパケット フロー

- VPN パケットが、サービス プロバイダー MPLS のバックボーン ネットワークから PE へ到着し、インターネット方向のインターフェイスを介してルーティングされます。
- パケットが Security Policy Database（SPD）と照合され、IPsec カプセル化されます。SPD には、IVRF とアクセス コントロール リスト（ACL）が格納されています。
- 次に、IPsec カプセル化パケットが、FVRF ルーティング テーブルによって転送されます。

IPsec トンネルからのパケット フロー

- IPsec カプセル化パケットが、リモート IPsec エンドポイントから PE ルータに到着します。
- IPsec によって、セキュリティ パラメータ インデックス（SPI）、宛先、およびプロトコルのセキュリティ アソシエーション（SA）検索が実行されます。
- パケットが、SA によってカプセル開放され、IVRF に関連付けられます。
- パケットが、IVRF ルーティング テーブルによって、さらに転送されます。

VRF-Aware IPsec の設定方法

暗号化キーリングの設定

暗号化キーリングは、事前共有キーおよび Rivest, Shamir, and Adelman（RSA）公開キーのリポジトリです。Cisco IOS ルータ上には、0 以上のキーリングを設定できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptokeyring***keyring-name*[**vrf** *fvrf-name*]
4. **description***string*
5. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key*
6. **rsa-pubkey** {**address** *address* | **name** *fqdn*} [**encryption** | **signature**]
7. **address***ip-address*
8. **serial-number***serial-number*
9. **key-string**
10. **text**
11. **quit**
12. **exit**
13. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptokeyring***keyring-name*[**vrf** *fvrf-name*] 例： `Router (config)# crypto keyring VPN1`	キーリングの名前として *keyring-name* を指定してキーリングを定義し、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。 • （任意）**vrf** キーワードおよび *fvrf-name* 引数は、キーリングが Front Door Virtual Routing and Forwarding（FVRF）にバインドされることを意味します。ローカル エンドポイントが FVRF 内にある場合、キーリング内のキーが検索されます。**vrf** を指定しない場合、キーリングはグローバルにバインドされます。

	コマンドまたはアクション	目的
ステップ 4	**description***string* 例： 例： `Router (config-keyring)# description The keys for VPN1`	（任意）キーリングに関する 1 行の説明です。
ステップ 5	**pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key* 例： `Router (config-keyring)# pre-shared-key address 10.72.23.11 key VPN1`	（任意）アドレスまたはホスト名によって、事前共有キーを定義します。
ステップ 6	**rsa-pubkey** {**address** *address* | **name** *fqdn*} [**encryption** | **signature**] 例： `Router(config-keyring)# rsa-pubkey name host.vpn.com`	（任意）アドレスまたはホスト名によって RSA 公開キーを定義し、rsa-pubkey コンフィギュレーション モードを開始します。 • オプションの **encryption** キーワードでは、キーが暗号化のために使用されることが指定されます。 • オプションの **signature** キーワードでは、キーがシグニチャ用に使用されることが指定されます。デフォルトでは、キーはシグニチャ用に使用されます。
ステップ 7	**address***ip-address* 例： `Router(config-pubkey-key)# address 10.5.5.1`	（任意）RSA 公開キーの IP アドレスを定義します。
ステップ 8	**serial-number***serial-number* 例： `Router(config-pubkey-key)# serial-number 1000000`	（任意）公開キーのシリアル番号を指定します。値は 0 から始まり、無制限です。
ステップ 9	**key-string** 例： `Router (config-pubkey-key)# key-string`	公開キーを定義するためのテキスト 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 10	**text** 例： `Router (config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973`	公開キーを指定します。 （注） この手順で追加できる公開キーは 1 つだけです。
ステップ 11	**quit** 例： `Router (config-pubkey)# quit`	公開キー コンフィギュレーション モードを終了します。
ステップ 12	**exit** 例： `Router (config-pubkey)# exit`	キーリング コンフィギュレーション モードに戻ります。
ステップ 13	**exit** 例： `Router(config-keyring)# exit#`	グローバル コンフィギュレーション モードに戻ります。

ISAKMP プロファイルの設定

ISAKMP プロファイルは、一連のピアのインターネット キー交換（IKE）フェーズ 1 および IKE フェーズ 1.5 設定のリポジトリです。ISAKMP プロファイルでは、IKE フェーズ 1 およびフェーズ 1.5 交換中に、キープアライブ、トラストポイント、ピアの ID、および XAUTH AAA リストなどのアイテムが定義されます。Cisco IOS ルータ上には、0 以上の ISAKMP プロファイルを設定できます。

（注） ルータから認証局（CA）へのトラフィック（認証および登録用、または、証明書失効リスト（CRL）取得用）、または Lightweight Directory Access Protocol（LDAP）サーバへのトラフィック（CRL 取得用）を VRF を介してルーティングする必要がある場合、トラストポイントに **vrf** コマンドを追加する必要があります。追加しない場合、トラフィックはデフォルトのルーティング テーブルを使用します。

- プロファイルに 1 つ以上のトラストポイントが指定されていない場合、ルータ内のすべてのトラストポイントが使用されて、ピアの証明書の確認が試行されます（IKE メイン モードま

たはシグニチャ認証）。1 つ以上のトラストポイントが指定されている場合、それらのトラストポイントだけが使用されます。

（注） IKE を開始するルータと IKE 要求に応答するルータのトラストポイント設定は互いに対称的である必要があります。たとえば、RSA シグニチャ暗号化および認証を実行中の応答ルータ（IKE メイン モード）では、CERT-REQ ペイロードの送信時に、グローバル コンフィギュレーション内で定義されたトラストポイントが使用されている場合があります。しかし、そのルータでは、証明書の確認のために ISAKMP プロファイル内で定義されたトラストポイントの制限リストが使用されている場合があります。ピア（IKE の発信側）が、トラストポイントが応答ルータのグローバル リスト内に存在するが、応答ルータの ISAKMP プロファイル内には存在しない証明書を使用するように設定されている場合、その証明書は拒否されます（ただし、開始ルータによって、応答ルータのグローバル コンフィギュレーション内のトラストポイントが認識されていない場合は、その証明書は認証されます）。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpprofile***profile-name*
4. **description***string*
5. **vrf***ivrf-name*
6. **keepalive***seconds***retry***retry-seconds*
7. **self-identity** {**address** | **fqdn**| **user-fqdn** *user-fqdn*}
8. **keyring***keyring-name*
9. **catrust-point** {*trustpoint-name*}
10. **matchidentity** {**group** *group-name* | **address** *address* [*mask*] [*fvrf*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
11. **clientconfigurationaddress** {**initiate** | **respond**}
12. **clientauthenticationlist***list-name*
13. **isakmpauthorizationlist***list-name*
14. **initiatemodeaggressive**
15. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptoisakmpprofile***profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを定義し、isakmp 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***string* 例： `Router (conf-isa-prof)# description configuration for VPN profile`	（任意）ISAKMP プロファイルの 1 行の説明を指定します。
ステップ 5	**vrf***ivrf-name* 例： `Router (conf-isa-prof)# vrf VPN1`	（任意）IPsec トンネルを Virtual Routing and Forwarding（VRF）インスタンスにマッピングします。 （注） VRF は、Security Policy Database（SPD）の照合のためのマッチングのためのセレクタにもなります。VRF が ISAKMP プロファイル内で指定されていない場合、IPsec トンネルの IVRF は、その FVRF と同じになります。
ステップ 6	**keepalive***seconds***retry***retry-seconds* 例： `Router (conf-isa-prof)# keepalive 60 retry 5`	（任意）ゲートウェイに対して、Dead Peer Detection（DPD）メッセージのピアへの送信を許可します。 • 定義しない場合、ゲートウェイではグローバルコンフィギュレーション値が使用されます。 • *seconds*：DPD メッセージ間の秒数。指定できる範囲は 10 ～ 3600 秒です。 • **retry***retry-seconds*：DPD メッセージがエラーになった場合の、リトライ間の秒数指定できる範囲は 2 ～ 60 秒です。

	コマンドまたはアクション	目的
ステップ 7	**self-identity** {**address** | **fqdn**| **user-fqdn** *user-fqdn*} 例： `Router (conf-isa-prof)# self-identity address`	（任意）ローカル IKE によって、リモート ピアに対して IKE 自身を識別させるために使用される、ID を指定します。 • 定義しない場合、IKE ではグローバル コンフィギュレーション値が使用されます。 • **address**：出力インターフェイスの IP アドレスを使用します。 • **fqdn**：ルータの完全修飾ドメイン名（FQDN）を使用します。 • **user-fqdn**：指定した値を使用します。
ステップ 8	**keyring***keyring-name* 例： `Router (conf-isa-prof)# keyring VPN1`	（任意）フェーズ1認証用に使用するキーリングを指定します。 • キーリングを指定しない場合、グローバル キー定義が使用されます。
ステップ 9	**catrust-point** {*trustpoint-name*} 例： `Router (conf-isa-prof)# ca trustpoint VPN1-trustpoint`	（任意）Rivest、Shamir、Adelman（RSA）証明書を確認するためのトラストポイントを指定します。 • ISAKMP プロファイル内でトラストポイントが指定されていない場合、Cisco IOS ルータ上で設定されているすべてのトラストポイントが証明書の確認に使用されます。
ステップ 10	**matchidentity** {**group** *group-name* | **address** *address* [*mask*] [*fvrf*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*} 例： `Router (conf-isa-prof)# match identity address 10.1.1.1`	照合されるクライアント IKE の ID を指定します。 • **group***group-name*：*group-name* と ID タイプ ID_KEY_ID を照合します。また、*group-name* と認定者名（DN）の組織ユニット（OU）フィールドも照合します。 • **address***address* [*mask*] *fvrf*：*address* と ID タイプ ID_IPV4_ADDR を照合します。*Mask* 引数を使用して、アドレスの範囲を指定できます。*fvrf* 引数では、アドレスが Front Door Virtual Routing and Forwarding（FVRF）にあることを指定します。 • **host***hostname*：*hostname* と ID タイプ ID_FQDN を照合します。 • **hostdomain***domain-name*：*domain-name* を、ドメイン名が *domain-name* と同じ IP タイプ ID_FQDN と照合します。このコマンドを使用して、ドメイン内のすべてのホストを照合します。

	コマンドまたはアクション	目的
		• **user***username*：*username* と ID タイプ ID_USER_FQDN を照合します。 • **userdomain***domainname*：ドメイン名が *domainname* と一致する ID タイプ ID_USER_FQDN を照合します。
ステップ 11	**clientconfigurationaddress** {**initiate** | **respond**} 例： `Router (conf-isa-prof)# client configuration address initiate`	（任意）モード設定交換を開始するか、モード設定要求に応答するかを指定します。
ステップ 12	**clientauthenticationlist***list-name* 例： `Router (conf-isa-prof)# client authentication list xauthlist`	（任意）Extended Authentication（XAUTH）交換中にリモート クライアントを認証するために使用する AAA（認証、許可、アカウンティング）。
ステップ 13	**isakmpauthorizationlist***list-name* 例： `Router (conf-isa-prof)# isakmp authorization list ikessaaalist`	（任意）フェーズ 1 キーおよびその他の AV のペアを受信するためのネットワーク認証サーバ。
ステップ 14	**initiatemodeaggressive** 例： `Router (conf-isa-prof)# initiate mode aggressive`	（任意）アグレッシブ モード交換を開始します。 • 指定しない場合、IKE によって、メイン モード交換が常に開始されます。
ステップ 15	**exit** 例： `Router (conf-isa-prof)# exit`	グローバル コンフィギュレーション モードに戻ります。

次の作業

セクション「暗号マップ上における ISAKMP プロファイルの設定，（100 ページ）」に進みます。

暗号マップ上における ISAKMP プロファイルの設定

ISAKMP プロファイルを、クリプト マップに適用する必要があります。ISAKMP プロファイル上の IVRF は、VPN トラフィックの照合時にセレクタとして使用されます。ISAKMP プロファイル上に IVRF が存在しない場合、IVRF は FVRF と同じになります。クリプト マップ上の ISAKMP プロファイルを設定するには、次の作業を実行します。

はじめる前に

クリプト マップ上で ISAKMP プロファイルを設定する前に、ルータに対して基本 IPsec の設定を行っておく必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptomap***map-name***isakmp-profile***isakmp-profile-name*
4. **setisakmp-profile***profile-name*
5. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptomap***map-name***isakmp-profile***isakmp-profile-name* 例： `Router (config)# crypto map vpnmap isakmp-profile vpnprofile`	（任意）クリプト マップ セット用に Internet Key Exchange and Key Management Protocol（ISAKMP）プロファイルを指定し、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。 • ISAKMP プロファイルは、IKE 交換中に使用されます。

	コマンドまたはアクション	目的
ステップ 4	**setisakmp-profile***profile-name* 例： `Router (config-crypto-map)# set isakmp-profile vpnprofile`	（任意）トラフィックがクリプト マップ エントリと一致した際に使用する ISAKMP プロファイルを指定します。
ステップ 5	**exit** 例： `Router (config-crypto-map)# exit`	グローバル コンフィギュレーション モードに戻ります。

IKE フェーズ 1 ネゴシエーション中に拡張認証を無視する設定

IKE フェーズ 1 ネゴシエーション中に XAUTH を無視するには、**no crypto xauth** コマンドを使用します。Unity クライアントの拡張認証が不要な場合、 **no crypto xauth** コマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **nocryptoxauth***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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**nocryptoxauth***interface* 例： `Router(config)# no crypto xauth ethernet0`	インターフェイスの IP アドレスを宛先とする要求の XAUTH 提案を無視します。デフォルトでは、IKE によって、XAUTH 提案が処理されます。

VRF-Aware IPsec の確認

VRF-Aware IPsec の設定を確認するには、次の **show** コマンドを使用します。これらの **show** コマンドによって、設定情報およびセキュリティ アソシエーション（SA）を表示できます。

手順の概要

1. イネーブル化
2. **showcryptoipsecsa** [**map** *map-name*| **address** | **identity** | **interface** *interface* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name*] [**detail**]
3. **showcryptoisakmpkey**
4. **showcryptoisakmpprofile**
5. **showcryptokeypubkey-chainrsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptoipsecsa** [**map** *map-name*| **address**	**identity**	**interface** *interface*	**peer** [**vrf** *fvrf-name*] **address**	**vrf** *ivrf-name*] [**detail**] 例： `Router# show crypto ipsec sa vrf vpn1`	現在の SA によって使用される設定の表示を許可します。

	コマンドまたはアクション	目的
ステップ 3	**showcryptoisakmpkey** 例： `Router# show crypto isakmp key`	すべてのキーリングおよびその事前共有キーを一覧表示します。 • このコマンドを使用して、クリプト キーリング設定を確認します。
ステップ 4	**showcryptoisakmpprofile** 例： `Router# show crypto isakmp profile`	すべての ISAKMP プロファイルおよびその設定を一覧表示します。
ステップ 5	**showcryptokeypubkey-chainrsa** 例： `Router# show crypto key pubkey-chain rsa`	ルータに保存されている、ピアの RSA 公開キーを表示します。 • 出力が、公開キーが所属するキーリングを表示するように拡張されます。

セキュリティ アソシエーションのクリア

次の **clear** コマンドによって、SA をクリアできます。

手順の概要

1. イネーブル化
2. **clearcryptosa** [**counters** | **map** *map-name* | **peer**[**vrf** *fvrf-name*] *address* | **spi** *address* {**ah** | **esp**} *spi* | **vrf** *ivrf-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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearcryptosa** [**counters** | **map** *map-name* | **peer**[**vrf** *fvrf-name*] *address* | **spi** *address* {**ah** | **esp**} *spi* | **vrf** *ivrf-name*]	IPsec SA をクリアします。

	コマンドまたはアクション	目的
	例： `Router# clear crypto sa vrf VPN1`	

VRF-Aware IPsec のトラブルシューティング

VRF-Aware IPsec のトラブルシューティングを行うには、次の **debug** コマンドを使用します。

手順の概要

1. イネーブル化
2. **debugcryptoipsec**
3. **debugcryptoisakmp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugcryptoipsec** 例： `Router# debug crypto ipsec`	IP セキュリティ（IPsec）イベントを表示します。
ステップ 3	**debugcryptoisakmp** 例： `Router(config)# debug crypto isakmp`	IKE に関するメッセージを表示します。

VRF-Aware IPsec のデバッグ例

次に、VRF-aware IPsec 設定のサンプル デバッグ出力を示します。

IPsec PE

```
Router# debug crypto ipsec
Crypto IPSEC debugging is on
IPSEC-PE#debug crypto isakmp
Crypto ISAKMP debugging is on
IPSEC-PE#debug crypto isakmp d
04:31:28: ISAKMP (0:12): purging SA., sa=6482B354, delme=6482B354
04:31:28: ISAKMP: Unlocking IKE struct 0x63C142F8 for declare_sa_dead(), count 0
IPSEC-PE#debug crypto isakmp detail
Crypto ISAKMP internals debugging is on
IPSEC-PE#
IPSEC-PE#
IPSEC-PE#
04:32:07: ISAKMP: Deleting peer node by peer_reap for 10.1.1.1: 63C142F8
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DC887D4E
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.68.1.1
04:32:55: ISAKMP cookie AA8F7B41 49A60E88
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DBC8E125
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 B4BDB5B7
04:32:55: ISAKMP (0:0): received packet from 10.1.1.1 dport 500 sport 500 Global (N) NEW
SA
04:32:55: ISAKMP: local port 500, remote port 500
04:32:55: ISAKMP: hash from 729FA94 for 619 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0:                   B91E2C70 095A1346          9.,p.Z.F
64218CD0: 0EDB4CA6 8A46784F B314FD3B 00        .[L&.FxO.};.
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 F7ACF384
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 0C07C670
04:32:55: ISAKMP: insert sa successfully sa = 6482B354
04:32:55: ISAKMP (0:13): processing SA payload. message ID = 0
04:32:55: ISAKMP (0:13): processing ID payload. message ID = 0
04:32:55: ISAKMP (0:13): peer matches vpn2-ra profile
04:32:55: ISAKMP: Looking for a matching key for 10.1.1.1 in default
04:32:55: ISAKMP: Created a peer struct for 10.1.1.1, peer port 500
04:32:55: ISAKMP: Locking peer struct 0x640BBB18, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
04:32:55: ISAKMP (0:13): Setting client config settings 648252B0
04:32:55: ISAKMP (0:13): (Re)Setting client xauth list and state
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13) Authentication by xauth preshared
04:32:55: ISAKMP (0:13): Checking ISAKMP transform 1 against priority 1 policy
04:32:55: ISAKMP:      encryption AES-CBC
04:32:55: ISAKMP:      hash SHA
04:32:55: ISAKMP:      default group 14
04:32:55: ISAKMP:      auth XAUTHInitPreShared
04:32:55: ISAKMP:      life type in seconds
04:32:55: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
04:32:55: ISAKMP (0:13): atts are acceptable. Next payload is 3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13): processing KE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing NONCE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is DPD
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 175 mismatch
04:32:55: ISAKMP (0:13): vendor ID is XAUTH
```

```
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): claimed IOS but failed authentication
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is Unity
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
04:32:55: ISAKMP (0:13): Old State = IKE_READY  New State = IKE_R_AM_AAA_AWAIT
04:32:55: ISAKMP cookie gen for src 11.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 7AE6E1DF
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 4 AA 31 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP (0:13): SKEYID state generated
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
        next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D70:                           0D000014               ....
63E66D80: 12F5F28C 457168A9 702D9FE2 74CC0100  .ur.Eqh)p-.btL..
63E66D90: 00                                   .
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
        next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D90: 0D000014 AFCAD713 68A1F1C9 6B8696FC  ..../JW.h!qIk..|
63E66DA0: 77570100 00                          wW...
04:32:55: ISAKMP (0:13): constructed NAT-T vendor-03 ID
04:32:55: ISAKMP (0:13): SA is doing pre-shared key authentication plus XAUTH using id type
 ID_IPV4_ADDR
04:32:55: ISAKMP (13): ID payload
        next-payload : 10
        type         : 1
        addr         : 172.16.1.1
        protocol     : 17
        port         : 0
        length       : 8
04:32:55: ISAKMP (13): Total payload length: 12
04:32:55: ISAKMP (0:13): constructed HIS NAT-D
04:32:55: ISAKMP (0:13): constructed MINE NAT-D
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
04:32:55: ISAKMP (0:13): Old State = IKE_R_AM_AAA_AWAIT  New State = IKE_R_AM2
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B D99DA70D
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 9C69F917
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 00583224
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 C1B006EE
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
AG_INIT_EXCH
04:32:55: ISAKMP: hash from 7003A34 for 132 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0:                   D1202D99 2BB49D38          Q -.+4.8
64218CD0: B8FBB1BE 7CDC67D7 4E26126C 63        8{1>|\gWN&.lc
04:32:55: ISAKMP (0:13): processing HASH payload. message ID = 0
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc my hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match MINE hash
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc his hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match HIS hash
04:32:55: ISAKMP (0:13): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = 0, sa = 6482B354
04:32:55: ISAKMP (0:13): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.16.1.1 remote 10.1.1.1 remote port
```

```
500
04:32:55: ISAKMP (0:13): returning IP addr to the address pool
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 05D315C5
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 041A85A6
04:32:55: ISAKMP (0:13): SA has been authenticated with 10.1.1.1
04:32:55: ISAKMP: Trying to insert a peer 172.16.1.1/10.1.1.1/500/,  and inserted
successfully.
04:32:55: ISAKMP: set new node -803402627 to CONF_XAUTH
04:32:55: IPSEC(key_engine): got a queue event...
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

04:32:55: ISAKMP (0:13): purging node -803402627
04:32:55: ISAKMP: Sending phase 1 responder lifetime 86400
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
04:32:55: ISAKMP (0:13): Old State = IKE_R_AM2  New State = IKE_P1_COMPLETE
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.168.1.1
04:32:55: ISAKMP cookie AA8F7B41 25EEF256
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): Need XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
04:32:55: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State =
IKE_XAUTH_AAA_START_LOGIN_AWAIT
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 2CCFA491
04:32:55: ISAKMP:        isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP: set new node -1447732198 to CONF_XAUTH
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
04:32:55: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = -1447732198
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) CONF_XAUTH

04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
04:32:55: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT  New State =
IKE_XAUTH_REQ_SENT
04:33:00: ISAKMP (0:13): retransmitting phase 2 CONF_XAUTH    -1447732198 ...
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): retransmitting phase 2 -1447732198 CONF_XAUTH
04:33:00: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) CONF_XAUTH

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 124D4618
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B0C91917
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 0E294692
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 091A7695
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292D74 for 92 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   84A1AF24 5D92B116          .!/$].1.
64218CD0: FC2C6252 A472C5F8 152AC860 63        |,bR$rEx.*H`c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
-1447732198
04:33:03: ISAKMP: Config payload REPLY
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
04:33:03: ISAKMP (0:13): deleting node -1447732198 error FALSE reason "done with xauth
```

```
request/reply exchange"
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_REQ_SENT  New State =
IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 A1B3E684
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP: set new node 524716665 to CONF_XAUTH
04:33:03: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = 524716665
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) CONF_XAUTH

04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT  New State =
IKE_XAUTH_SET_SENT
004:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 5C83A09D
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 2BEBEFD4
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B DA00A46B
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 FDD27773
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292A34 for 68 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   5034B99E B8BA531F          P49.8:S.
64218CD0: 6267B8BD F3006989 DC118796 63        bg8=s.i.\...c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID = 524716665
04:33:03: ISAKMP: Config payload ACK
04:33:03: ISAKMP (0:13):        XAUTH ACK Processed
04:33:03: ISAKMP (0:13): deleting node 524716665 error FALSE reason "done with transaction"
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_SET_SENT  New State = IKE_P1_COMPLETE
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 E0BB50E9
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 7794EF6E
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 C035AAE5
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B F1FCC25A
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 31744F44
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R) QM_IDLE

04:33:03: ISAKMP: set new node -1639992295 to QM_IDLE
04:33:03: ISAKMP: hash from 7293A74 for 100 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   9D7DF4DF FE3A6403          .}t_~:d.
64218CD0: 3F1D1C59 C5D138CE 50289B79 07        ?..YEQ8NP(.y.
04:33:03: ISAKMP (0:13): processing transaction payload from 10.1.1.1. message ID =
-1639992295
```

```
04:33:03: ISAKMP: Config payload REQUEST
04:33:03: ISAKMP (0:13): checking request:
04:33:03: ISAKMP:    IP4_ADDRESS
04:33:03: ISAKMP:    IP4_NETMASK
04:33:03: ISAKMP:    IP4_DNS
04:33:03: ISAKMP:    IP4_DNS
04:33:03: ISAKMP:    IP4_NBNS
04:33:03: ISAKMP:    IP4_NBNS
04:33:03: ISAKMP:    SPLIT_INCLUDE
04:33:03: ISAKMP:    DEFAULT_DOMAIN
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B02E0D67
04:33:03: ISAKMP:        isadb_post_process_list: crawler: C 27FF 12 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP (0:13): attributes sent in message:
04:33:03:         Address: 10.2.0.0
04:33:03: ISAKMP (0:13): allocating address 10.4.1.4
04:33:03: ISAKMP: Sending private address: 10.4.1.4
04:33:03: ISAKMP: Sending DEFAULT_DOMAIN default domain name: vpn2.com
04:33:03: ISAKMP (0:13): responding to peer config from 10.1.1.1. ID = -1639992295
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) CONF_ADDR

04:33:03: ISAKMP (0:13): deleting node -1639992295 error FALSE reason ""
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
04:33:03: ISAKMP (0:13): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT  New State = IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 881D5411
04:33:03: ISAKMP cookie gen for src 11.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 6FD82541
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 8A94C1BE
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 F3BA766D
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R) QM_IDLE

04:33:03: ISAKMP: set new node 17011691 to QM_IDLE
04:33:03: ISAKMP: hash from 70029F4 for 540 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   AFBA30B2 55F5BC2D          /:02Uu<-
64218CD0: 3A86B1C9 00D2F5BA 77BF5589 07        :.1I.Ru:w?U..
04:33:03: ISAKMP (0:13): processing HASH payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing SA payload. message ID = 17011691
04:33:03: ISAKMP (0:13): Checking IPSec proposal 1
04:33:03: ISAKMP: transform 1, ESP_AES
04:33:03: ISAKMP:   attributes in transform:
04:33:03: ISAKMP:      encaps is 1
04:33:03: ISAKMP:      SA life type in seconds
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP:      SA life type in kilobytes
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
04:33:03: ISAKMP:      authenticator is HMAC-SHA
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
```

```
04:33:03: IPSEC(validate_transform_proposal): transform proposal not supported for identity:

    {esp-aes esp-sha-hmac}
04:33:03: ISAKMP (0:13): IPSec policy invalidated proposal
04:33:03: ISAKMP (0:13): Checking IPSec proposal 2
04:33:03: ISAKMP: transform 1, ESP_AES
04:33:03: ISAKMP:   attributes in transform:
04:33:03: ISAKMP:      encaps is 1
04:33:03: ISAKMP:      SA life type in seconds
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP:      SA life type in kilobytes
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
04:33:03: ISAKMP:      authenticator is HMAC-SHA
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: ISAKMP (0:13): processing NONCE payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): asking for 1 spis from ipsec
04:33:03: ISAKMP (0:13): Node 17011691, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
04:33:03: ISAKMP (0:13): Old State = IKE_QM_READY  New State = IKE_QM_SPI_STARVE
04:33:03: IPSEC(key_engine): got a queue event...
04:33:03: IPSEC(spi_response): getting spi 2749516541 for SA
        from 172.18.1.1     to 10.1.1.1        for prot 3
04:33:03: ISAKMP: received ke message (2/1)
04:33:04: ISAKMP (13): ID payload
        next-payload : 5
        type         : 1
        addr         : 10.4.1.4
        protocol     : 0
        port         : 0
04:33:04: ISAKMP (13): ID payload
        next-payload : 11
        type         : 4
        addr         : 0.0.0.0
        protocol     : 0
        port         : 0
04:33:04: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
04:33:04: ISAKMP (0:13): Old State = IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B 93DE46D2
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 088A0A16
04:33:04: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04:       crawler my_cookie AA8F7B41 F7ACF384
04:33:04:        crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B A8F23F73
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 93D8D879
04:33:04: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04:       crawler my_cookie AA8F7B41 F7ACF384
04:33:04:        crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R) QM_IDLE

04:33:04: ISAKMP: hash from 7290DB4 for 60 bytes
04:33:04: ISAKMP: Packet hash:
64218CC0:                    4BB45A92 7181A2F8          K4Z.q."x
64218CD0: 73CC12F8 091875C0 054F77CD 63        sL.x..u@.OwMc
04:33:04: ISAKMP: Locking peer struct 0x640BBB18, IPSEC refcount 1 for stuff_ke
04:33:04: ISAKMP (0:13): Creating IPSec SAs
04:33:04:         inbound SA from 10.1.1.1 to 172.18.1.1 (f/i)  0/ 2
        (proxy 10.4.1.4 to 0.0.0.0)
```

```
04:33:04:         has spi 0xA3E24AFD and conn_id 5127 and flags 2
04:33:04:         lifetime of 2147483 seconds
04:33:04:         lifetime of 4608000 kilobytes
04:33:04:         has client flags 0x0
04:33:04:         outbound SA from 172.18.1.1     to 10.1.1.1        (f/i)  0/ 2 (proxy
0.0.0.0         to 10.4.1.4       )
04:33:04:         has spi 1343294712 and conn_id 5128 and flags A
04:33:04:         lifetime of 2147483 seconds
04:33:04:         lifetime of 4608000 kilobytes
04:33:04:         has client flags 0x0
04:33:04: ISAKMP (0:13): deleting node 17011691 error FALSE reason "quick mode done (await)"
04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
04:33:04: ISAKMP (0:13): Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLETE
04:33:04: IPSEC(key_engine): got a queue event...
04:33:04: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac ,
    lifedur= 2147483s and 4608000kb,
    spi= 0xA3E24AFD(2749516541), conn_id= 5127, keysize= 0, flags= 0x2
04:33:04: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac,
    lifedur= 2147483s and 4608000kb,
    spi= 0x50110CF8(1343294712), conn_id= 5128, keysize= 0, flags= 0xA
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:04: IPSEC(rte_mgr): VPN Route Added 10.4.1.4 255.255.255.255 via 10.1.1.1 in vpn2
04:33:04: IPSEC(add mtree): src 0.0.0.0, dest 10.4.1.4, dest_port 0
04:33:04: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.1.1, sa_prot= 50,
    sa_spi= 0xA3E24AFD(2749516541),
    sa_trans= esp-aes esp-sha-hmac, sa_conn_id= 5127
04:33:04: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0x50110CF8(1343294712),
    sa_trans= esp-aes esp-sha-hmac, sa_conn_id= 5128
04:33:53: ISAKMP (0:13): purging node -1639992295
04:33:54: ISAKMP (0:13): purging node 17011691
```

VRF-Aware IPsec の設定例

例：静的 IPsec-to-MPLS VPN

次のサンプルでは、IPsec トンネルを MPLS VPN にマッピングするスタティック設定を示しています。この設定により、IPsec トンネルが MPLS VPN、「VPN1」および「VPN2」にマッピングされます。IPsec トンネルは両方とも、シングルパブリック方向インターフェイス上で終了します。

IPsec PE の設定

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
```

```
!
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
crypto ipsec transform-set vpn2 esp-aes esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route 10.1.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
ip route vrf vpn2 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

VPN1 用 IPsec Customer Provided Edge（CPE）設定

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
crypto isakmp key vpn1 address 172.18.1.1
!
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
```

```
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

VPN2 用 IPsec CPE 設定

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
!
crypto isakmp key vpn2 address 172.18.1.1
!
!
crypto ipsec transform-set vpn2 esp-aes esp-sha-hmac
!
crypto map vpn2 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn2
 match address 101
!
interface FastEthernet0
 ip address 10.1.1.1 255.255.255.0
 crypto map vpn2
!
interface FastEthernet1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
```

例：RSA 暗号化を使用した IPsec-to-MPLS VPN

次の例では、RSA 暗号化を使用した IPsec-to-MPLS VPN 設定を示します。

PE ルータ設定

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto isakmp policy 10
 authentication rsa-encr
!
crypto keyring vpn1
 rsa-pubkey address 172.16.1.1 encryption
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DBF381 00DDECC8
   DC4AA490 40320C52 9912D876 EB36717C 63DCA95C 7E5EC02A 84F276CE 292B42D7
   D664F324 3726F4E0 39D33093 ECB81B95 482511A5 F064C4B3 D5020301 0001
   quit
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
```

```
 match address 101
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

VPN1 用 IPsec CPE 設定

```
crypto isakmp policy 10
 authentication rsa-encr
!
crypto key pubkey-chain rsa
 addressed-key 172.18.1.1 encryption
 key-string
  3082011B 300D0609 2A864886 F70D0101 01050003 82010800 30820103 0281FB00
  C90CC78A 6002BDBA 24683396 B7D7877C 16D08C47 E00C3C10 63CF13BC 4E09EA23
  92EB8A48 4113F5A4 8796C8BE AD7E2DC1 3B0742B6 7118CE7C 1B0E21D1 AA9724A4
  4D74FCEA 562FF225 A2B11F18 E53C4415 61C3B741 3A06E75D B4F9102D 6163EE40
  16C68FD7 6532F660 97B59118 9C8DE3E5 4E2F2925 BBB87FCB 95223D4E A5E362DB
  215CB35C 260080805 17BBE1EF C3050E13 031F3D5B 5C22D16C FC8B1EC5 074F07A5
  D050EC80 7890D9C5 EC20D6F0 173FE2BA 89F5B5F9 2EADC9A6 D461921E 3D5B60016
  ABB8B6B9 E2124A21 93F0E4AE B487461B E7F1F1C4 032A0B0E 80DC3E15 CB268EC9
  5D76B9BD 3C78CB75 CE9F68C6 484D6573 CBC3EB59 4B5F3999 8F9D0203 010001
  quit
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

例：RSA シグニチャを使用した IPsec-to-MPLS VPN

次のに、RSA シグニチャを使用した IPsec-to-MPLS VPN 設定を示します。

PE ルータ設定

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
```

```
!
crypto ca certificate chain bombo
 certificate 03C0
 308203BF 308202A7 A0030201 02020203 C0300D06 092A8648 86F70D01 01050500
 . . .
 quit
 certificate ca 01
 30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 . . .
 quit
!
crypto isakmp profile vpn1
 vrf vpn1
 ca trust-point bombo
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/1
 ip address 172.31.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
!
```

VPN1 用 IPsec CPE 設定

```
crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
 !
crypto ca certificate chain bombo
 certificate 03BF
  308203BD 308202A5 A0030201 02020203 BF300D06 092A8648 86F70D01 01050500
  . . .
  quit
 certificate ca 01
  30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  . . .
  quit
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

例：IPsec Remote Access-to-MPLS VPN

次に、IPsec Remote Access-to-MPLS VPN 設定を示します。この設定により、IPsec トンネルが MPLS VPN にマッピングされます。IPsec トンネルが、シングル パブリック方向インターフェイス上で終了します。

PE ルータ設定

```
aaa new-model
!
aaa group server radius vpn1
 server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn1
!
aaa group server radius vpn2
 server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn2
!
aaa authorization network aaa-list group radius
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
!
crypto isakmp profile vpn1-ra
   vrf vpn1
   match identity group vpn1-ra
   client authentication list vpn1
   isakmp authorization list aaa-list
   client configuration address initiate
   client configuration address respond
crypto isakmp profile vpn2-ra
   vrf vpn2
   match identity group vpn2-ra
   client authentication list vpn2
   isakmp authorization list aaa-list
   client configuration address initiate
   client configuration address respond
!
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
crypto ipsec transform-set vpn2 esp-aes esp-sha-hmac
!
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
```

```
 ip address 172.18.1.1 255.255.255.0
 crypto map ra
!
ip local pool vpn1-ra 10.4.1.1 10.4.1.254 group vpn1-ra
ip local pool vpn2-ra 10.4.1.1 10.4.1.254 group vpn2-ra
!
```

Cisco Network-Based IPsec VPN Solution の旧バージョンからのアップデート

Cisco Network-Based IPsec VPN Solution リリース 1.5 における VRF-Aware IPsec 機能では、既存の設定を変更する必要があります。次のサンプル設定では、既存の設定に対して行う必要がある変更を示します。

Site-to-Site 設定のアップグレード

次の設定では、旧バージョンの Network-Based IPsec VPN Solution から Cisco Network-Based IPsec VPN Solution リリース 1.5 への Site-to-Site 設定のアップグレードに必要な変更を示します。

旧バージョンの Site-to-Site 設定

```
crypto isakmp key VPN1 address 172.21.25.74
 crypto isakmp key VPN2 address 172.21.21.74
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
!
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
  encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

新バージョンの Site-to-Site 設定

次に、同じ Site-to-Site 設定の、Cisco Network-Based IPsec VPN Solution リリース 1.5 ソリューションへアップグレードされたバージョンを示します。

（注） 2 つのキーリングを変更する必要があります。VRF-Aware Upset 機能では、IKE ローカル エンドポイントが VRF 内に存在している場合、キーを VRF に関連付ける必要があります。

```
crypto keyring VPN1-KEYS vrf VPN1
 pre-shared-key address 172.21.25.74 key VPN1
!
 crypto keyring VPN2-KEYS vrf VPN2
  pre-shared-key address 172.21.21.74 key VPN2
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
  set transform-set VPN1
 match address 101
!
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
  set transform-set VPN2
 match address 102
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

リモート アクセス設定のアップグレード

次の設定では、旧バージョンの Network-Based IPsec VPN Solution から Cisco Network-Based IPsec VPN Solution リリース 1.5 へのリモート アクセス設定のアップグレードに必要な変更を示します。

旧バージョンのリモート アクセス設定

```
crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
 pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
  set transform-set VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
  reverse-route
!
!
```

```
 crypto map VPN1 client authentication list VPN1-RA-LIST
 crypto map VPN1 isakmp authorization list VPN1-RA-LIST
 crypto map VPN1 client configuration address initiate
 crypto map VPN1 client configuration address respond
 crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 client authentication list VPN2-RA-LIST
 crypto map VPN2 isakmp authorization list VPN2-RA-LIST
 crypto map VPN2 client configuration address initiate
 crypto map VPN2 client configuration address respond
 crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
  encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

新バージョンのリモート アクセス設定

次のインスタンスでは、アップグレードはありません。次の設定を変更することを推奨します。

```
crypto isakmp client configuration group VPN1-RA-GROUP
  key VPN1-RA
  pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto isakmp profile VPN1-RA
 match identity group VPN1-RA-GROUP
  client authentication list VPN1-RA-LIST
 isakmp authorization list VPN1-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto isakmp profile VPN2-RA
 match identity group VPN2-RA-GROUP
 client authentication list VPN2-RA-LIST
 isakmp authorization list VPN2-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
 set transform-set VPN1-RA
 set isakmp-profile VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
 set isakmp-profile VPN2-RA
 reverse-route
!
 crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
```

```
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

Site-to-Site とリモート アクセスの設定の組み合わせのアップグレード

次の設定では、旧バージョンの Network-Based IPsec VPN Solution から Cisco Network-Based IPsec VPN Solution リリース 1.5 への Site-to-Site およびリモート アクセス設定のアップグレードに必要な変更を示します。

旧バージョンの Site-to-Site およびリモート アクセスの設定

```
crypto isakmp key VPN1 address 172.21.25.74 no-xauth
crypto isakmp key VPN2 address 172.21.21.74 no-xauth
!
 crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
 pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
 set transform-set VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
 reverse-route
!
 crypto map VPN1 client authentication list VPN1-RA-LIST
 crypto map VPN1 isakmp authorization list VPN1-RA-LIST
 crypto map VPN1 client configuration address initiate
 crypto map VPN1 client configuration address respond
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
 crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 client authentication list VPN2-RA-LIST
 crypto map VPN2 isakmp authorization list VPN2-RA-LIST
 crypto map VPN2 client configuration address initiate
 crypto map VPN2 client configuration address respond
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
 crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
```

```
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

新バージョンの Site-to-Site およびリモート アクセスの設定

この設定をアップグレードする必要があります。

（注） Site-to-Site 設定に XAUTH が不要な場合、XAUTH 設定なしで ISAKMP プロファイルを設定します。リモート アクセス設定に XAUTH が必要な場合、XAUTH ありで ISAKMP プロファイルを設定します。

```
crypto keyring VPN1-KEYS vrf VPN1
 pre-shared-key address 172.21.25.74 key VPN1
!
 crypto keyring VPN2-KEYS vrf VPN2
 pre-shared-key address 172.21.21.74 key VPN2
!
 crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
 pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto isakmp profile VPN1
 keyring VPN1-KEYS
 match identity address 172.21.25.74 VPN1
!
 crypto isakmp profile VPN2
 keyring VPN2-KEYS
 match identity address 172.21.21.74 VPN2
!
 crypto isakmp profile VPN1-RA
 match identity group VPN1-RA-GROUP
 client authentication list VPN1-RA-LIST
 isakmp authorization list VPN1-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto isakmp profile VPN2-RA
 match identity group VPN2-RA-GROUP
 client authentication list VPN2-RA-LIST
 isakmp authorization list VPN2-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
 set transform-set VPN1-RA
 set isakmp-profile VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
```

```
 set isakmp-profile VPN2-RA
 reverse-route
!
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 set isakmp-profile VPN1
 match address 101
 crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 set isakmp-profile VPN2
 match address 102
 crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPsec の設定作業	「Configuring Security for VPNs with IPsec」
IPsec コマンド	『*Cisco IOS Security Command Reference*』
IKE フェーズ 1 とフェーズ 2、アグレッシブ モード、およびメイン モード	「Configuring Internet Key Exchange for IPsec VPNs」
IKE DPD	「Easy VPN Server」
推奨される暗号化アルゴリズム	次世代暗号化

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco 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	Title
なし	--

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

VRF-Aware IPsec の機能情報

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 *5*：*VRF-Aware IPsec* の機能情報

機能名	リリース	機能情報
VRF 認識 IPSec	12.2(15)T	

機能名	リリース	機能情報
		VRF-Aware IPsec 機能には、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）に対する IP Security（IPsec）トンネル マッピングが導入されています。VRF-Aware IPsec 機能を使用すれば、シングル パブリック方向アドレスによって、VPNルーティング/転送（VRF）に対して IPsec トンネルをマッピングできます。 この機能は、Cisco IOS Release 12.2(15)T で導入されました。 この機能に関する詳細については、次の各項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。**address**、**catrust-point**、**clientauthenticationlist**、**clientconfigurationaddress**、**cryptoisakmpprofile**、**cryptokeyring**、**cryptomapisakmp-profile**、**initiate-mode**、**isakmpauthorizationlist**、**keepalive**（**isakmp** プロファイル）、**keyring**、**key-string**、**matchidentity**、**nocryptoxauth**、**pre-shared-key**、**quit**、**rsa-pubkey**、**self-identity**、**serial-number**、**setisakmp-profile**、**showcryptoisakmpkey**、**showcryptoisakmpprofile**、**vrf**、**clearcryptosa**、**cryptoisakmppeer**、**cryptomapisakmp-profile**、**showcryptodynamic-map**、**showcryptoipsecsa**、

機能名	リリース	機能情報
		showcryptoisakmpsa、**showcryptomap**（**IPsec**）.
	15.1(1)S	この機能は、Cisco IOS Release 15.1(1)S に統合されました。

用語集

CA：Certification Authority（認証局）。CA はデジタル証明書を発行するエンティティ（特に X.509 証明書）で、証明書のデータ項目間のバインディングを保証します。

CLI：コマンドライン インターフェイス。CLI は、ユーザが、コマンドおよびオプションの引数を入力することによって、オペレーティング システムとやり取りをすることを可能にするインターフェイスです。UNIS オペレーティング システムと DOS では、CLI が使用できます。

クライアント：マルチ プロトコル ラベル スイッチング（MPLS）ネットワーク内の UUT の対応する IPsec IOS ピア。

dead peer：到達できなくなった IKE ピア。

DN：識別名（DN）。オープン システム インターコネクション（OSI ディレクトリ（X.500））内のエントリの、グローバルな権威ある名前です。

FQDN：完全修飾ドメイン名。FQDN は、単なるホスト名ではなく、システムにおける正式な名前です。たとえば、aldebaran はホスト名で、aldebaran.interop.com は FQDN です。

FR：フレーム リレー。FR は、接続されたデバイス間におけるハイレベルデータ リンク（HDLC）カプセル化を使用して、複数の仮想回線を処理するための、業界標準の、スイッチデータリンク層プロトコルです。フレーム リレーは、一般的に置き代替可能と考えられているプロトコルである X.25 より効率的です。

FVRF：前面扉 Virtual Routing and Forwarding（VRF）のリポジトリ。FVRF は、暗号化されたパケットをピアにルーティングするために使用される VRF です。

IDB：インターフェイス記述子ブロック。IDB サブブロックは、アプリケーションに対してプライベートとなっているメモリ領域です。この領域には、アプリケーションにとって IDB またはインターフェイスに関連付ける必要があるプライベート情報およびステートが格納されます。アプリケーションによって IDB が使用されてポインタがそのサブブロックに登録されますが、サブブロック自体の内容には登録されません。

IKE：インターネット キーエクスチェンジ。IKE によって、キーが必要なサービス（IPsec など）のための共有セキュリティ ポリシーおよび認証キーが確立されます。IPsec トラフィックを通過させる前に、ルータ、ファイアウォール、ホストそれぞれでピアの 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。

IKEキープアライブ：IKE ピアの活性を判断するための双方向メカニズム。

IPsec：IP 用セキュリティ プロトコル。

IVRF：Inside Virtual Routing and Forwarding。IVRF は、暗号化されていないテキスト パケットの VRF です。

MPLS：マルチプロトコル ラベル スイッチング。MPLS は、ラベルを使用して IP トラフィックを転送するスイッチング方式です。このラベルによって、ネットワーク内のルータおよびスイッチが、事前に確立された IP ルーティング情報に基づくパケットの転送先を指示されます。

RSA：Rivest、Shamir、Adelman は、RSA 技術の発明者です。RSA 技術は、暗号化および認証に使用可能な公開キー暗号化システムです。

SA：セキュリティ アソシエーション。SA は、データ フローに適用されるセキュリティ ポリシーおよびキー関連情報のインスタンスです。

VPN：バーチャル プライベート ネットワーク。VPN を使用すると、ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

VRF：Virtual Route Forwarding。VRF は、VPN ルーティングおよび転送インスタンスです。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

XAUTH：拡張認証。XAUTH は、IKE フェーズ 1 と IKE フェーズ 2 の間における任意の交換です。XAUTH では、ルータが、（ピアの認証ではなく）実際のユーザの認証試行において、追加の認証情報を要求します。

第 9 章

IKE アグレッシブ モードの開始

IKE アグレッシブ モードの開始機能を使用すれば、IP Security（IPsec）ピアの RADIUS トンネル属性を指定して、トンネル属性とのインターネット キー エクスチェンジ（IKE）アグレッシブ モード ネゴシエーションを開始できます。この機能は、暗号ハブアンドスポーク シナリオでの実装に最適です。これにより、スポークが、AAA サーバ上にトンネル属性として指定され保存されている事前共有キーを使用することによって、ハブとの IKE アグレッシブ モード ネゴシエーションを開始します。このシナリオは、事前共有キーが中央リポジトリ（AAA サーバ）に保管され、複数のハブ ルータと 1 つのアプリケーションによるキーの情報の使用が可能になるので、容易に拡張できます。

（注） セキュリティに対する脅威も、その脅威から保護するための暗号化技術も、常に変化しています。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

IKE アグレッシブ モードの開始の前提条件

IKE：アグレッシブ モードの開始機能を設定する前に、次の作業を実行する必要があります。

- AAA の設定
- IPsec トランスフォームの設定
- 静的暗号マップの設定
- Internet Security Association and Key Management Protocol（ISAKMP）ポリシーの設定
- ダイナミック暗号マップの設定

IKE アグレッシブ モードの開始の制約事項

TED の制約事項

この機能は、トンネル セットアップを開始するために Tunnel Endpoint Discovery（TED）が使用されているダイナミック クリプトマップで使用するものではありません。TED は、各サイトにピアの事前共有キーを保管するための AAA サーバが必要なフル メッシュ セットアップの設定に便利ですが、この設定をこの機能と共に使用するのは実用的ではありません。

Tunnel-Client-Endpoint ID タイプ

この機能では次の ID タイプだけを使用できます。

- ID_IPV4（IPV4 アドレス）
- ID_FQDN（「foo.cisco.com」などの完全修飾ドメイン名）
- ID_USER_FQDN（E メール アドレス）

IKE アグレッシブ モードの開始に関する情報

概要

IKE：アグレッシブ モードの開始機能を使用すれば、IPSec ピアの RADIUS トンネル属性として IKE 事前共有キーを設定できます。これにより、ハブアンドスポーク トポロジ内で IKE 事前共有キーを拡張できます。

IKE 事前共有キーは理解しやすく、簡単に導入できるものですが、ユーザの数が増えると拡張が難しくなり、セキュリティ上の脅威が発生しやすくなります。ハブ ルータに事前共有キーを保管するのではなく、この機能を利用すれば、事前共有キーを、認証、許可、アカウンティング（AAA）サーバに保存し、またそこから取得することによって拡張できます。事前共有キーは、Internet Engineering Task Force（IETF）RADIUS トンネル属性として AAA サーバに保存され、ユーザがハブ ルータに「スピーク」を試行する際に取得されます。ハブ ルータによって AAA サーバから事前共有キーが取得され、スポーク（ユーザ）が、Internet Security Association Key Management Policy（ISAKMP）ピア ポリシー内に RADIUS トンネル属性として指定されている事前共有キーを使用して、ハブに対してアグレッシブ モードを開始します。

RADIUS トンネル属性

IKE アグレッシブ モード ネゴシエーションを開始するには、Tunnel-Client-Endpoint（66）および Tunnel-Password（69）属性を、ISAKMP ピア ポリシー内に設定する必要があります。Tunnel-Client-Endpoint 属性は、該当する IKE ID ペイロード内で符号化されることによって、サーバに伝達されます。Tunnel-Password 属性は、アグレッシブ モード ネゴシエーション用 IKE 事前共有キーとして使用されます。

IKE アグレッシブ モードの開始の設定方法

RADIUS トンネル属性の設定

ISAKMP ピア設定内の Tunnel-Client-Endpoint および Tunnel-Password 属性を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptomap***map-name***isakmpauthorizationlist***list-name*
4. **cryptoisakmppeer** {**ip-address** *ip-address* | **fqdn** *fqdn*}
5. **setaggressive-modeclient-endpoint***client-endpoint*
6. **setaggressive-modepassword***password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**cryptomap***map-name***isakmpauthorizationlist***list-name* 例： `Router (config)# crypto map testmap10 isakmp authorization list list ike`	アグレッシブ モードで、トンネル属性に関する AAA の IKE クエリー生成をイネーブルにします。
ステップ 4	**cryptoisakmppeer** {**ip-address** *ip-address* | **fqdn** *fqdn*} 例： `Router (config)# crypto isakmp peer ip address 10.10.10.1`	アグレッシブ モードで、トンネル属性に関する AAA の IKE クエリー生成のための IPsec ピアを有効化して、ISAKMP 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 5	**setaggressive-modeclient-endpoint***client-endpoint* 例： `Router (config-isakmp)# set aggressive-mode client-endpoint user-fqdn user@cisco.com`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint 属性を指定します。

	コマンドまたはアクション	目的
ステップ 6	**setaggressive-modepassword***password* 例： `Router (config-isakmp)#set aggressive-mode password cisco123`	ISAKMP ピア設定内で、Tunnel-Password 属性を指定します。

RADIUS トンネル属性設定の確認

Tunnel-Client-Endpoint 属性および Tunnel-Password 属性が ISAKMP ピア ポリシー内で設定されていることを確認するには、 **show running-config** グローバル コンフィギュレーション コマンドを使用します。

トラブルシューティングのヒント

IKE：アグレッシブ モードの開始機能のトラブルシューティングを行うには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **debugaaaauthorization**
3. **debugcryptoisakmp**
4. **debugradius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugaaaauthorization** 例： `Router# debug aaa authorization`	AAA 認証の情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**debugcryptoisakmp** 例： `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。
ステップ 4	**debugradius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

IKE アグレッシブ モードの開始の設定例

ハブの設定例

次に、アグレッシブ モードがサポートされているハブアンドスポーク トポロジのハブを、RADIUS トンネル属性を使用して設定する方法の例を示します。

```
!The AAA configurations are as follows:
aaa new-model
aaa authorization network ike group radius
aaa authentication login default group radius
!
! The Radius configurations are as follows:
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key rad123
!
! The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPsec configurations are as follows:
crypto ipsec transform-set trans1 esp-aes esp-sha-hmac
!
crypto dynamic-map Dmap 10
 set transform-set trans1
!
crypto map Testtag isakmp authorization list ike
crypto map Testtag 10 ipsec-isakmp dynamic Dmap
!
interface FastEthernet0
 ip address 10.4.4.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.2.2.1 255.255.255.0
```

スポークの設定例

次に、アグレッシブ モードがサポートされているハブアンドスポーク トポロジのスポークを、RADIUS トンネル属性を使用して設定する方法の例を示します。

```
!The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPsec configurations are as follows:
crypto ipsec transform-set trans1 esp-aes esp-sha-hmac
 access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 10.4.4.1
 set transform-set trans1
 match address 101
!
interface FastEthernet0
 ip address 10.5.5.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.3.3.1 255.255.255.0
```

RADIUS ユーザ プロファイルの例

次に、Tunnel-Client-Endpoint および Tunnel-Password 属性がサポートされている RADIUS サーバ上のユーザ プロファイルの例を示します。

```
user@cisco.com  Password = "cisco", Service-Type = Outbound
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Type = :1:ESP,
    Cisco:Avpair = "ipsec:tunnel-password=cisco123",
    Cisco:Avpair = "ipsec:key-exchange=ike"
```

その他の参考資料

次の項では、IKE アグレッシブ モードの開始機能に関連した関連資料を示します。

関連資料

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*』
認証の設定	「Configuring Authentication」

関連項目	マニュアル タイトル
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
推奨される暗号化アルゴリズム	次世代暗号化

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
• RFC 2409 • RFC 2868	• RFC 2409、『The Internet Key Exchange』 • RFC 2868、『RADIUS Attributes for Tunnel Protocol Support』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IKE アグレッシブ モードの開始の機能情報

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 *6*：*IKE* アグレッシブ モードの開始の機能情報

機能名	リリース	機能情報
IKE：アグレッシブ モードの開始	Cisco IOS XE Release 2.1	IKE アグレッシブ モードの開始機能を使用すれば、IPsec ピアの RADIUS トンネル属性を指定し、トンネル属性での IKE アグレッシブ モード ネゴシエーションを開始できます。 次のコマンドが導入または変更されました。 **cryptoisakmppeer**、**setaggressive-modeclient-endpoint**、**setaggressive-modepassword**