# FlexVPN クライアントの設定

このモジュールでは、FlexVPN クライアント機能と FlexVPN クライアントの設定に必要なインターネット キー エクスチェンジ バージョン 2（IKEv2）コマンドについて説明します。

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



# FlexVPN クライアントの制限事項

## ローカル認証方式としての EAP

- ローカル認証方式としての Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）は、IKEv2 発信側でのみサポートされます。リモート認証としては、IKEv2 応答側でのみサポートされます。
- EAP がローカル認証方式として指定されている場合、リモート認証方式は証明書ベースである必要があります。
- FlexVPN サーバーで **authentication remote eap query-identity** コマンドが設定されていないと、IP アドレスを EAP 認証方式のユーザー名として使用することはできないため、クライアントはローカル ID として IPv4 アドレスまたは IPv6 アドレスを持つことはできません。

# デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec

VPN ルーティングおよび転送（VRF）認識 IPsec シナリオでデュアルスタック トンネル インターフェイスを設定する場合、**ip vrf forwarding** コマンドを使用して内部 VPN ルーティングおよび転送（IVRF）インスタンスを設定することはできません。これは有効な設定ではないためです。トンネル インターフェイスの IVRF を定義するには **vrf forwarding** *vrf-name* コマンドを使用します。ここで、*vrf-name* 引数は、定義内に IPv4 および IPv6 アドレス ファミリを指定した **vrf definition** コマンドを使用して定義されます。

### SSO の制約事項

- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピアルータは、予期されたシーケンス番号を持たないパケットをドロップします。単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。

# FlexVPN クライアントに関する情報

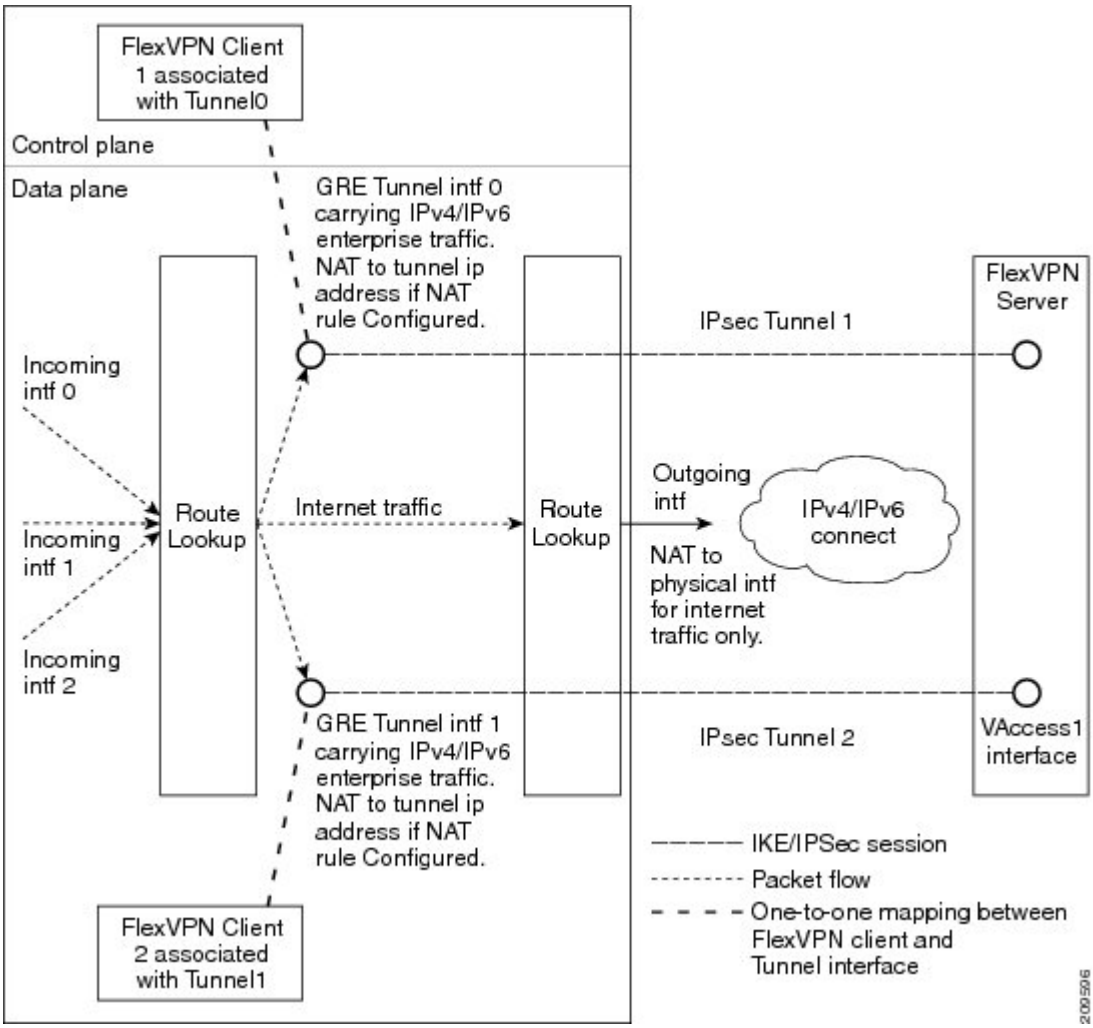
## IKEv2 FlexVPN クライアント

IKEv2 FlexVPN クライアント機能は、FlexVPN クライアントと FlexVPN サーバーの間にセキュアな IPsec VPN トンネルを確立します。IKEv2 FlexVPN クライアント機能の利点は、次のとおりです。

- トンネル インフラストラクチャの統合
- IPv4/IPv6 トランスポートを介した IPv4/IPv6 プロキシ サポート
- EasyVPN によってサポートされるいくつかの機能との下位互換性
- ダイナミック ルーティング プロトコルを実行するための柔軟性

各 FlexVPN クライアントは、一意のトンネルインターフェイスに関連付けられます。これは、特定の FlexVPN クライアントによって取得された IPsec セキュリティ アソシエーション（SA）がトンネル インターフェイスにバインドされていることを示します。次の図に、FlexVPN クライアントとトンネル インターフェイスとの間の関連付けを示します。

図 *1 : FlexVPN* クライアントとトンネル インターフェイスの関連付け




動作のシーケンスは、次のとおりです。

- ルーティング：FlexVPN サーバーは、モード設定応答の一部としてネットワーク リストをプッシュします。クライアントは、これらのネットワークにトンネルインターフェイスのルートを追加します。コンフィギュレーションモード設定の一部として、クライアントはネットワークにルートを送信します。サーバーがクライアント側ネットワークにルートを追加できるように、IP アドレスがトンネル インターフェイスに設定されます。
- NAT：ネットワーク アドレス変換（NAT）ルールは、ルート マップを使用して明示的に設定する必要があります。ルールが一致すると、FlexVPN クライアントの背後にあるホストはトンネルの IP アドレスに変換されます。この IP アドレスは、FlexVPN サーバーによるモード設定時にプッシュされる属性の 1 つとして取得できます。
- カプセル化および暗号化：Generic Routing Encapsulation（GRE）および IPSec カプセル化モードがサポートされます。GRE は、IPv4 と IPv6 の両方のトラフィックをサポートします。トンネル インターフェイスに到達するトラフィックは、GRE ヘッダーでカプセル化

され、その後に IPSec 保護が実行されます。その後、暗号化されたトラフィックは発信インターフェイスにルーティングされます。

FlexVPN クライアントによってサポートされる機能について、次の項で説明します。

## トンネル有効化

FlexVPN クライアントは、自動的にまたはユーザー操作によって手動で接続できます。FlexVPN 設定が完了すると、FlexVPN クライアントは、自動的にトンネルに接続します。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、接続を無制限に再試行します。自動トンネル接続を設定するには、IKEv2 FlexVPN プロファイルで **connect** コマンドに **auto** キーワードを使用します。

手動接続では、FlexVPN クライアントは、接続を確立する前にコマンドを実行するユーザーの操作を待ちます。クライアントがタイムアウトするか、接続に失敗すると、後続の接続ではユーザーの操作が必要になります。手動接続を設定するには、特権 EXEC モードで、**crypto ikev2 client flexvpn connect** コマンドに *flexvpn-name* 引数を使用します。接続を終了するには、**clear crypto ikev2 client flexvpn connect** コマンドに *flexvpn-name* 引数を使用します。

### 追跡ベースのトンネル有効化

追跡ベースのトンネル有効化機能は、主にバックアップ シナリオで使用されます。FlexVPN クライアントは、オブジェクトの状態変更に関する通知を取得するため、追跡システムに登録されます。この通知はクライアントに、トンネル有効化のための適切なアクションを実行するよう要求します。**connect** コマンドの **track** キーワードによって、クライアントがオブジェクト番号で特定されるオブジェクトの追跡に関心があることを示す、追跡プロセスを通知します。次に、追跡プロセスはクライアントに、オブジェクトの状態がいつ変更されたかを通知します。

**connect** コマンドの **track** キーワードでトンネル有効化が設定されている場合、オブジェクトが起動すると、オブジェクトがアップ状態にあることを示す通知を受信したクライアントは、接続をトリガーします。**connect** コマンドの **track** キーワードでトンネル有効化が設定されている場合、オブジェクトが停止すると、オブジェクトがダウン状態にあることを示す通知を受信したクライアントは、接続をトリガーします。

## バックアップ機能

FlexVPN クライアントは、事前に決定された順序で複数のピアまたはサーバーに接続できます。ピアのリストはゲートウェイ リストまたはバックアップ ゲートウェイ リストと呼ばれ、次のリストを使用して作成されます。

- スタティック バックアップ ゲートウェイ リストまたはスタティック リスト
- ダウンロード バックアップ ゲートウェイ リストまたはダウンロード リスト

スタティック バックアップ ゲートウェイ リストは、シーケンス番号の付いたピアのリストを提供することによって FlexVPN プロファイルで設定されます。ダウンロード バックアップ ゲートウェイ リストは、動的にダウンロードされ、モード設定の応答時に取得されます。ダウンロード リストは、スタティック ゲートウェイ リストを補完してバックアップ ゲートウェイ

リストを作成します。ダウンロードリストは、リストがダウンロードされるピアの後に挿入されます。

ゲートウェイ リストのピアとの既存の接続がダウンすると、クライアントはゲートウェイ リストにある次のピアとの接続を確立しようとします。ダウンロード リストが使用可能でスタティック ピアとの接続に失敗すると、クライアントはダウンロード リストのピアと順番に接続しようとします。クライアントがダウンロードリストのすべてのピアとの接続の確立に失敗すると、クライアントはスタティック リストにある次のピアに接続を試みて、ダウンロードリストは削除されます。

## バックアップ ゲートウェイ

バックアップ ゲートウェイ リストにピアを追加するには、**peer** コマンドを使用します。バックアップ ゲートウェイ リストを削除するには、**no peer** コマンドを使用します。

ピアは、優先順に並べられています。シーケンス番号が小さいほど、優先順位が高くなります。

新しいピアとの接続が確立され、そのピアがダウンロードリストに含まれていない場合、ピアはバックアップ ゲートウェイ リストにダウンロード リストを追加し、既存のバックアップ ゲートウェイ リストが新しいリストに置き換えられます。

スタティック ピアを設定して、トラック オブジェクトにアタッチすることができます。ピアのトラック オブジェクトがアップ状態の場合、ピアは「可能なピア」になります。

（注） ダウンロード リストのピアを含め、トラック オブジェクトにアタッチされていないピアは、これらのピアが常にアップ状態であるため「可能なピア」に分類されます。

ピアの選択プロセスは、次のように機能します。接続が確立されると、ゲートウェイ リストが検索され、最初の可能なピアが選択されます。ピアは次のルールに従って選択されます。スタティック ピアは、希望するステータス（アップまたはダウン）のトラック オブジェクトに関連付けることができます。トラック オブジェクトのステータスが設定されたステータスと一致すると、ピアは「可能なピア」と呼ばれます。

（注） ピアがドメイン ネーム サービス（DNS）の名前または完全修飾ドメイン名（FQDN）のいずれかによって識別される場合、名前は動的に解決されます。

ピアの選択プロセスの後に、新しいピアが選択されます。また、既存の条件が満たされない場合は、次のシナリオが発生します。

- アクティブなピアが、活性チェックに応答しなくなります。
- ピア名の DNS 解決が失敗します。
- ピアとの IKE ネゴシエーションが失敗します。
- ピアが「可能なピア」でなくなります（対応するトラック オブジェクトがダウンします）。

（注） 複数の FlexVPN ピアを FlexVPN クライアントで設定したり、プライマリ ピアで IKEv2 SA をクリアすると、そのクリアによってクライアントでの新しいピアの選択がトリガーされます。

### プライマリ ピアの再アクティブ化

プライマリ ピアの再アクティブ化機能は、最高優先度のピアが常に接続されるようにします。最高優先度のピアのトラック オブジェクトがオブジェクト ステータスと一致する場合、優先度が低いピアがある既存の接続が切断され、最高優先度のピアへの接続が確立されます。この機能を有効にするには、**peer reactivate** コマンドを使用します。

（注） トラック オブジェクトは、静的に設定されたピアに関連付ける必要があります。

### ダイヤル バックアップ（プライマリまたはバックアップ トンネル）

オブジェクトの状態の変化ついて通知を受けるように、FlexVPN クライアントを追跡システムに登録します。クライアントがオブジェクトを追跡したい追跡プロセス（オブジェクト番号で識別）について通知するには、**connect track** コマンドを使用します。追跡プロセスでは、このオブジェクトの状態が変わったときにクライアントに順番に通知されます。追跡しているオブジェクトの状態がアップまたはダウンの場合、この通知によってクライアントは、プライマリまたはバックアップ接続を開始または停止するために対処するよう促されます。

ダイヤル バックアップ機能は、次のように設定できます。

- プライマリおよびバックアップ トンネルの両方が FlexVPN トンネルの場合：
  - アクティブなトンネルは、一度に 1 つのみです。
  - 両方のクライアント プロファイルは **connect track** コマンドを使用して設定され、同じトラック オブジェクトを参照します。
  - オブジェクトがアップしているときにプライマリ トンネルがステータスを追跡する場合、セカンダリ トンネルはオブジェクトがダウンしているときにオブジェクトのステータスを追跡します。
- 1 つのトンネルが FlexVPN トンネルの場合：
  - 残りのトンネルは、セキュアな接続上に存在します。
  - プライマリ接続は FlexVPN ではなく、バックアップ接続が FlexVPN です。
  - クライアント プロファイルは、オブジェクトを指定した **connect track** コマンドを使用して設定され、プライマリ発信インターフェイスを介してプライマリ ピアに到達する能力をトレースします。

### バックアップ グループ

バックアップ グループ機能によって、FlexVPN クライアントは、グループに属する FlexVPN クライアントが同じピアとのセッションを確立しているときにピアを省略することができま

す。グループに属している FlexVPN クライアントがピアとの接続を開始すると、FlexVPN クライアントは同じグループ内の別の FlexVPN クライアントが同じピアとのセッションを確立しているかどうかを確認します。接続が存在する場合、FlexVPN クライアントはこのピアを省いて、順番に次のピアを確認します。バックアップ グループを設定するには、*group-number* 引数を指定して **backup group** コマンドを使用します。

## デュアル FlexVPN のサポート

デュアル FlexVPN サポート機能によって、同じ内部および外部インターフェイスを共有する 2 つの FlexVPN トンネルを設定することができます。2 つの FlexVPN トンネルは、ルート インジェクションを使用し、対応するトンネルインターフェイスを介して適切なトラフィックを送信します。トンネルがアップしているとき、トンネルはサーバーからネットワーク リストを「学習」します。サーバーがネットワーク リストを転送すると、FlexVPN は特定のルートをそのルーティング テーブル内の宛先ネットワークにインストールし、トンネル インターフェイスからこれらのネットワークにトラフィックを送信します。

（注） トンネル インターフェイスを介してデフォルト ルートと確立できる FlexVPN 接続は、1 つのみです。

## スプリット DNS のサポート

スプリット DNS 機能では、FlexVPN クライアントはドメイン ネーム システム（DNS）プロキシとして動作できます。FlexVPN ネゴシエーションの間、DNS リストはモード設定中にダウンロードされます。このリストは、FlexVPN プロファイルと関連付けられた内部インターフェイスで、DNS ビュー リストとして設定されます。ビュー リストは、ドメイン名に基づいて要求と DNS クエリを照合し、一致した要求を DNS サーバーに転送するために使用されます。他の DNS クエリは、デフォルト ビュー（グローバル DNS 設定）を照合するために使用され、ISP DNS に転送されます。

FlexVPN クライアント プロファイル内に 内部インターフェイスについての記載がない場合、DNS ビューはすべてのインターフェイスに適用されますが、設定されたすべてのプロファイルのトンネル インターフェイスとトンネル ソース インターフェイスを除きます。DNS クエリ要求が内部インターフェイスに受信されると、一致する DNS ビューが取得され、要求は DNS IP アドレスに転送されます。

## NAT

FlexVPN のネットワーク アドレス変換（NAT）機能では、トラフィックがルーティングされるインターフェイスに基づいて、トラフィックを IP アドレスに変換できます。パケットが、**ip nat inside** コマンドで設定された 1 つのインターフェイスで受信され、**ip nat outside** コマンドで設定された別のインターフェイスに送信される場合、そのパケットは 2 番目のインターフェイスで設定された IP アドレスに変換されます。

### サーバーのネットワーク リスト

企業トラフィックのルートは、トンネルインターフェイスを使用して、クライアントによってダイナミックインストールされます。このトラフィックは、発信する物理インターフェイス経由でデフォルトのルートをたどります。企業トラフィックはトンネルIPアドレスに変換され、インターネット トラフィックは外部の発信インターフェイス IP アドレスに変換されます。

### サーバーからのデフォルト ルート リスト

デフォルト ルートは、トンネル インターフェイスを介してシーケンス番号がより高いデバイスで設定する必要があります。トンネル インターフェイスは **ip nat outside** コマンドで設定されます。また、トンネルインターフェイスのIPアドレスは、クライアントが送信したIPアドレスによって割り当てられます。内部インターフェイスからの企業トラフィックは、送信アドレスに変換されます。NATは、ルートマップを使用してNATルールを設定することによって実現されます。ルートマップでは、発信インターフェイスに基づいてルールが定義されます。グローバルに設定されたNATルールは、ルーティングに基づいて適用されます。

トンネル インターフェイスから送信されたIPv4トラフィックは、IPv4送信アドレスに変換されます。

（注） NATが不要な場合、トンネル インターフェイスに関連付けられたNATルールを設定する必要はありません。

## FlexVPN クライアントのネットワーク リストの学習方法

FlexVPNクライアントは、次のいずれかの方法でピアの背後にあるネットワークのリストを学習します。

- モード設定プッシュ：FlexVPN サーバーは、ネットワーク属性のリストをコンフィギュレーション モードのパラメータとしてクライアントに送信します。FlexVPN クライアントは、メトリックが最も高いトンネルインターフェイスを介してこれらのネットワークにルートをインストールします。クライアントは、サーバーが仮想アクセスインターフェイスを介してそれらのルートを追加できるように、モード設定セットまたは確認応答（SET/ACK）の交換でサーバーにそのネットワークを伝達します。
- ルーティング プロトコルの実行：FlexVPN クライアントおよびサーバーはトンネル インターフェイスを介してルーティング プロトコルを実行し、ネットワーク ルートを確立します。これによって、クライアントおよびサーバーは、既存のセッションを切断せずに柔軟にネットワークを追加または削除できます。トンネルアドレスは、ピアとのルートを確立するためにモード設定時に伝達されます。

## WINS NBNS およびドメイン名

モード設定中、FlexVPN サーバーはドメイン名、Windows Internet Naming Service（WINS）、またはNetBIOS ネーム サーバー（NBNS）属性をプッシュします。これらの属性は、FlexVPN クライアントで実行されている DHCP サーバーに、動的に更新されます。

## イベント トレース

イベント トレース機能は、デバッグのために使用されます。FlexVPN クライアントに通知されたイベントは記録され、その情報はデバッグに使用されます。イベント トレースは、バッファ領域に数バイトのトレース情報を記録する高速メカニズムと、デバッグデータを抽出および復号する表示メカニズムを組み合わせたものです。FlexVPNクライアントは、バッファを保持して、通常の動作時に有効にすることができます。

## ローカル認証方式としての Extensible Authentication Protocol

FlexVPN クライアントは、ローカル認証方式として EAP をサポートします。サポートされる EAP 認証方式は、Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）、メッセージ ダイジェスト アルゴリズム 5（MD5）、および Generic Token Card（GTC：汎用トークン カード）です。EAP 認証プロセスは、次のとおりです。

- EAP を使用して FlexVPN クライアントを認証するには、IKEv2 プロファイル コンフィギュレーション モードで **authentication local eap** コマンドを使用します。
- FlexVPN クライアントがピアから IKE_AUTH 応答を受信した後、**crypto eap credentials** コマンドを入力します。
- EAP ID 要求を IKE_AUTH 応答で受信した場合、EAP ユーザー名とパスワードを指定する必要があります。
- EAP ID 要求を IKE_AUTH 応答で受信していない場合、ローカル IKEv2 ID をユーザー名として使用するため、パスワードのみを指定します。

（注） ローカル認証方式としての EAP は FlexVPN クライアントと一緒に使用する必要がありますが、IKEv2 発信側では EAP を使用することもできます。EAP サーバーがサポートされていない認証方式を最初に指定すると、FlexVPN EAP 発信側は EAP 否定応答（NAK）パケットで応答し、希望の認証方式として EAP-MSCHAPv2、EAP-MD5、または EAP-GTC を要求します。FlexVPN EAP 応答側で、いずれかの認証方式を選択します。

# FlexVPN クライアントの設定方法

## IKEv2 VPN クライアント プロファイルの設定

このタスクでは、FlexVPN クライアントの設定に必要な IKEv2 コマンドと基本の IKEv2 コマンドについて説明します。基本の IKEv2 プロファイルの設定については、『*Configuring Internet Key Exchange Version 2 (IKEv2)*』モジュールの「Configuring Basic Internet Key Exchange Version 2 CLI Constructs」タスクを参照してください。

（注） IKEv2プロファイルの認証リストに入力ミスがある場合は、自動的にデフォルトのリストに戻ります。

FlexVPN サーバーの IKEv2 プロファイル設定については、「FlexVPN クライアントの設定方法」の項を参照してください。

## トンネル インターフェイスの設定

このタスクを実行して、FlexVPN クライアントが参照するトンネル インターフェイスを設定します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** {*ipv4-address* | **negotiated**}
5. **tunnel mode gre ip**
6. **tunnel mode ipsec ipv4**
7. **tunnel source** {*ip-address* | *interface* | **dynamic**}
8. **tunnel destination dynamic**
9. **tunnel protection ipsec-profile** *profile-name*
10. **end**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface tunnel** *number*<br>例：<br>`Device(config)# interface tunnel 1` | トンネルインターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip address** {*ipv4-address* | **negotiated**}<br>例：<br>`Device(config-if)# ip address negotiated` | （オプション）IPv4 アドレスをトンネル インターフェイスに割り当てます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **tunnel mode gre ip**<br>例：<br>`Device(config-if)# tunnel mode gre ip` | （オプション）トンネル インターフェイスの Generic Route Encapsulation（GRE）モードを有効にします。 |
| ステップ 6 | **tunnel mode ipsec ipv4**<br>例：<br>`Device(config-if)# tunnel mode ipsec ipv4` | （オプション）IPSec カプセル化を有効にします。 |
| ステップ 7 | **tunnel source** {*ip-address* \| *interface* \| **dynamic**}<br>例：<br>`Device(config-if)# tunnel source 10.0.0.1` | トンネルインターフェイスの送信元を指定します。 |
| ステップ 8 | **tunnel destination dynamic**<br>例：<br>`Device(config-if)# tunnel destination dynamic` | トンネル インターフェイスの宛先を指定します。 |
| ステップ 9 | **tunnel protection ipsec-profile** *profile-name*<br>例：<br>`Device(config-if)# tunnel protection ipsec-profile ipsecprofile1` | トンネルインターフェイスを IPsec プロファイルに関連付けます。 |
| ステップ 10 | **end**<br>例：<br>`Device(config-if)# end` | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

## FlexVPN クライアントの設定

**monitor event-trace flexvpn** コマンドを使用して、イベント トレースを有効にします。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 client flexvpn** *client-name*
4. **peer** *sequence* {*ipv4-address* | *ipv6-address* | **fqdn** *fqdn-name* [**dynamic** | **ipv6**]} [ **track** *track-number* [**up** | **down**]]
5. **connect** {**manual** | **auto** | **track** *track-number* [**up** | **down**]}
6. **client inside** *interface-type interface-number*
7. **client connect tunnel** *interface-number*
8. **source** *sequence-number interface-type interface-number* **track** *track-number*
9. **peer reactivate**
10. **backup group** {*group-number* | **default**}
11. **end**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **crypto ikev2 client flexvpn** *client-name*<br>例：<br>`Device(config)# crypto ikev2 client flexvpn client1` | IKEv2 FlexVPN クライアント プロファイルを定義し、IKEv2 FlexVPN クライアント 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 | **peer** *sequence* {*ipv4-address* \| *ipv6-address* \| **fqdn** *fqdn-name* [**dynamic** \| **ipv6**]} [ **track** *track-number* [**up** \| **down**]]<br>例：<br>`Device(config-ikev2-flexvpn)# peer 1 10.0.0.1` | IP アドレスまたはホスト名を使用して、静的ピアを定義します。 |
| ステップ 5 | **connect** {**manual** \| **auto** \| **track** *track-number* [**up** \| **down**]}<br>例：<br>`Device(config-ikev2-flexvpn)# connect track 10 up` | FlexVPN トンネルを接続します。<br>（注） このコマンドに変更を加えると、アクティブなセッションが終了します。 |
| ステップ 6 | **client inside** *interface-type interface-number*<br>例：<br>`Device(config-ikev2-flexvpn)# client inside GigabitEthernet 0/1` | （オプション）内部インターフェイスを指定します。<br>• FlexVPN クライアント プロファイルには、複数の内部インターフェイスを指定できます。内部インターフェイスは、FlexVPN クライアント プロファイル全体で共有できます。<br>（注） このコマンドに変更を加えると、アクティブなセッションが終了します。 |
| ステップ 7 | **client connect tunnel** *interface-number*<br>例：<br>`Device(config-ikev2-flexvpn)# client connect tunnel 1` | 「トンネル インターフェイスの設定」タスクで作成したトンネル インターフェイスを、FlexVPN クライアントに割り当てます。<br>• FlexVPN クライアント プロファイルに対して、設定できるトンネル インターフェイスは 1 つのみです。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | （注） このコマンドに変更を加えると、アクティブなセッションが終了します。 |
| ステップ 8 | **source** *sequence-number interface-type interface-number* **track** *track-number*<br>例：<br>`Device(config-ikev2-flexvpn)# source 1 GigabitEthernet 0/1 track 11` | トンネルの送信元アドレスにシーケンス番号を追加します。<br>• トンネルの送信元アドレスには、トラック オブジェクト番号がアップ状態の最小シーケンス番号があります。<br>（注） このコマンドに変更を加えると、アクティブなセッションが終了します。 |
| ステップ 9 | **peer reactivate**<br>例：<br>`Device(config-ikev2-flexvpn)# peer reactivate` | プライマリ ピア機能の再アクティベートを有効にします。 |
| ステップ 10 | **backup group** {*group-number* \| **default**}<br>例：<br>`Device(config-ikev2-flexvpn)# backup group default` | バックアップ グループにクライアントを割り当てます。<br>• デフォルトでは、すべてのクライアントがバックアップ グループ 0 に属しています。<br>（注） このコマンドに変更を加えると、アクティブなセッションが終了します。 |
| ステップ 11 | **end**<br>例：<br>`Device(config-ikev2-flexvpn)# end` | IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

## ローカル認証方式としての EAP の設定

このタスクを実行して、FlexVPN クライアントのローカル認証方式として Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）を設定します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **authentication local eap**
5. **end**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **crypto ikev2 profile** *profile-name*<br>例：<br>`Device(config)# crypto ikev2 profile profile1` | IKEv2 プロファイルを定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。 |
| ステップ 4 | **authentication local eap**<br>例：<br>`Device(config-ikev2-profile)# authentication local eap` | ローカル認証方式として EAP を指定します。<br>（注） このコマンドは、IKEv2 の発信側でのみサポートされます。 |
| ステップ 5 | **end**<br>例：<br>`Device(config-ikev2-profile)# end` | IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

# FlexVPN クライアントの構成例

## 例：IKEv2 FlexVPN クライアント プロファイルの設定

次の例は、IKEv2 FlexVPN クライアント プロファイルを設定する方法を示します。

```
crypto ikev2 client flexvpn flex
  peer 1 10.0.0.1
  connect manual
  client connect Tunnel0
!
crypto ikev2 authorization policy flex
 subnet-acl 199
 route set interface
 route accept any
!
crypto ikev2 keyring key
 peer dvti
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof
 match identity remote address 10.0.0.1 255.0.0.0
 authentication local pre-share
```

```
 authentication remote pre-share
 keyring key
 aaa authorization group psk list local-group-author-list flex
 config-mode set
!
crypto ipsec transform-set trans esp-aes
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set pfs group2
 set ikev2-profile prof
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec-profile ipsecprof
!
interface Ethernet0/0
 ip address 172.16.0.1 255.240.0.0
 ip virtual-reassembly in
!
 ip route 0.0.0.0 0.0.0.0 2.2.2.2
access-list 199 permit ip 10.20.20.20 0.0.0.255 any
access-list 199 permit ip 10.30.30.30 0.0.0.255 any
```

## 例：ローカル認証方式としての EAP の設定

次の例は、EAP をローカル認証方式として設定する方法を示します。

```
crypto ikev2 profile profile1
 authentication remote rsa-sig
 authentication local eap
```

セッションが起動すると、次のように、EAP の認証情報を入力するプロンプトが表示されます。

```
Enter the command "crypto eap credentials profile1"
Device# crypto eap credentials profile1

Enter the Username for profile profile1: cisco
Enter the password for username cisco
```

# FlexVPN クライアントの設定に関する追加情報

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| Cisco IOS コマンド | 『Cisco IOS Master Command List, All Releases』 |

| 関連項目 | マニュアル タイトル |
|---|---|
| セキュリティ コマンド | • 『Cisco IOS Security Command Reference Commands A to C』<br>• 『Cisco IOS Security Command Reference Commands D to L』<br>• 『Cisco IOS Security Command Reference Commands M to R』<br>• 『Cisco IOS Security Command Reference Commands S to Z』 |
| IPsec の設定 | 『*Configuring Security for VPNs with IPsec*』 |
| 推奨される暗号化アルゴリズム | 『Next Generation Encryption』 |

### シスコのテクニカル サポート

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

# FlexVPN クライアントの設定の機能情報

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 : FlexVPN* クライアントの設定の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IKEv2 リモートアクセス ハードウェア クライアント | | IKEv2 リモートアクセス ハードウェア クライアント機能は、モビリティ、NAT トラバーサル、およびサービス妨害（DoS）攻撃からの復元など、さまざまなソリューションのサポートに必要な、リモートアクセス接続と拡張機能をサポートします。<br>次のコマンドが導入または変更されました。 **backup group, client connect tunnel, client inside, connect, crypto ikev2 client flexvpn, interface, ip address, peer, peer reactivate, source tunnel destination, tunnel mode, tunnel protection, tunnel source.** |
| IPsec VPN の IPv6 リモート アクセス | | IPsec VPN の IPv6 リモート アクセス機能は、IPv6 サポートと、IKEv2 FlexVPN クライアントのローカル認証方式としての EAP をサポートします。<br>次のコマンドが変更されました。 **authentication (IKEv2 profile), peer.** |

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