



# 仮想トンネル インターフェイス

この章では、VTI トンネルの設定方法について説明します。

- [仮想トンネル インターフェイスについて \(1 ページ\)](#)
- [仮想トンネル インターフェイスの注意事項 \(2 ページ\)](#)
- [VTI トンネルの作成 \(6 ページ\)](#)
- [仮想トンネル インターフェイスの機能履歴 \(14 ページ\)](#)

## 仮想トンネル インターフェイスについて

ASA は、仮想トンネル インターフェイス (VTI) と呼ばれる論理 インターフェイスをサポートします。ポリシーベースの VPN の代わりに、VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。動的ルートまたは静的ルートを使用できます。VTI からの出力トラフィックは暗号化されてピアに送信され、VTI への入力トラフィックは関連付けられた SA によって復号化されます。

VTI を使用することにより、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングすることが不要になります。すべてのリモートサブネットを追跡し、暗号マップのアクセスリストに含める必要がなくなります。展開が簡単になるほか、ダイナミックルーティングプロトコルのルートベースの VPN をサポートするステティック VTI があると、仮想プライベートクラウドの多くの要件を満たすこともできます。

### スタティック VTI

2 つのサイト間でトンネルが常にオンになっているサイト間接続用に、スタティック VTI 設定を使用できます。スタティック VTI インターフェイスの場合、物理インターフェイスをトンネルソースとして定義する必要があります。デバイスごとに最大 1024 の VTI を関連づけることができます。スタティック VTI インターフェイスを作成するには、[VTI インターフェイスの追加 \(9 ページ\)](#) を参照してください。

### Dynamic VTI

ダイナミック VTI は、サイト間 VPN に高度に安全でスケーラブルな接続を提供します。ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。

ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。ダイナミック VTI テクノロジーは、ダイナミック クリプト マップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。管理センターでは、ダイナミック VTI はハブアンドスポークトポロジのみをサポートします。

ダイナミック VTI では、IPsec インターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。ダイナミック VTI はダイナミック (DHCP) スポークもサポートします。ダイナミック VTI インターフェイスを作成するには、[ダイナミック VTI インターフェイスの追加 \(12 ページ\)](#) を参照してください。

### ASA で VPN セッションのダイナミック VTI トンネルを作成する方法

1. ASA で仮想テンプレートを作成します ([設定 (Configuration) ]>[デバイスの設定 (Device Setup) ]>[インターフェイス設定 (Interface Settings) ]>[インターフェイス (Interfaces) ]>[追加 (Add) ]>[DVTI インターフェイス (DVTI Interface) ] を選択)。

このテンプレートは、複数の VPN セッションに使用できます。

2. このテンプレートをトンネルグループに適用します。1 つの仮想テンプレートを複数のトンネルグループに適用することができます。
3. スポークは、ハブとのトンネル要求を開始します。
4. ハブはスポークを認証します。
5. ASA は、仮想テンプレートを使用して、スポークとの VPN セッション用にハブ上に仮想アクセスインターフェイスを動的に作成します。
6. ハブは、仮想アクセスインターフェイスを使用して、スポークとのダイナミック VTI トンネルを確立します。
7. IKEv2 交換で VTI インターフェイス IP をアドバタイズするように、IKEv2 route set interface オプションを設定します。このオプションにより、トンネルを介して機能する BGP またはパスモニタリングの VTI インターフェイス間のユニキャスト到達可能性が有効になります。
8. VPN セッションが終了すると、トンネルは切断され、ハブは対応する仮想アクセスインターフェイスを削除します。

## 仮想トンネルインターフェイスの注意事項

### コンテキストモードとクラスタリング

- シングル モードでだけサポートされています。

- クラスタリングはサポートされません。

#### ファイアウォール モード

ルーテッドモードのみでサポートされます。

#### BGP IPv4 および IPv6 のサポート

VTI を介した IPv4 および IPv6 BGP ルーティングをサポートします。

#### EIGRP サポート

VTI を介した IPv4 および IPv6 EIGRP ルーティングをサポートします。

#### OSPF IPv4 および IPv6 のサポート

VTI を介した IPv4 および IPv6 OSPF ルーティングをサポートします。

#### IPv6 のサポート

- IPv6 アドレスが指定された VTI を設定できます。
- VTI のトンネル送信元とトンネル接続先の両方に IPv6 アドレスを設定できます。
- パブリック IP バージョンを介した VTI IP（または内部ネットワーク IP バージョン）の次の組み合わせがサポートされています。
  - IPv6 over IPv6
  - IPv4 over IPv6
  - IPv4 over IPv4
  - IPv6 over IPv4
- トンネルの送信元および接続先としてサポートされるのは、静的 IPv6 アドレスだけです。
- トンネル送信元インターフェイスには IPv6 アドレスを設定できます。トンネルエンドポイントとして使用するアドレスを指定できます。指定しない場合、デフォルトでは、リスト内の最初の IPv6 グローバルアドレスがトンネルエンドポイントとして使用されます。
- トンネルモードを IPv6 として指定できます。指定した場合、VTI を介して IPv6 トラフィックをトンネリングできます。ただし、単一 VTI のトンネルモードは IPv4 または IPv6 のいずれかになります。

#### 一般的な設定時の注意事項

- LAN-to-LAN VPN でダイナミッククリプトマップとダイナミック VTI を使用する場合は、ダイナミック VTI トンネルのみが起動します。この動作は、クリプトマップとダイナミック VTI の両方がデフォルトのトンネルグループを使用しようとするために発生します。次のいずれかを実行することを推奨します。

- LAN-to-LAN VPN をダイナミック VTI に移行します。
- 独自のトンネルグループを持つ静的クリプトマップを使用します。
- VTI は IPsec モードのみで設定可能です。ASA で GRE トンネルを終了することはサポートされていません。
- トンネルインターフェイスを使用するトラフィックには、静的、BGP、OSPF、または EIGRP IPv4 ルートを使用できます。
- スタティックおよびダイナミック VTI の場合は、借用 IP インターフェイスを VTI インターフェイスのトンネルソース IP アドレスとして使用しないでください。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。ただし、VTI を有効にした後で物理インターフェイス MTU を変更した場合は、新しい MTU 設定を使用するために VTI を無効にしてから再度有効にする必要があります。
- ダイナミック VTI の場合、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。トンネル送信元インターフェイスを指定しない場合、仮想アクセスインターフェイスは、ASA が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。
- スタティック VTI の場合、デバイスには最大 1,024 の VTI を設定できます。VTI 数を計算する際は、次の点を考慮してください。
  - nameif サブインターフェイスを含めて、デバイスに設定できる VTI の総数を導き出します。
  - ポートチャネルのメンバーインターフェイスに nameif を設定することはできません。したがって、トンネル数は実際のメイン ポートチャネル インターフェイスの数だけ減少し、そのメンバーインターフェイスの数は減少しません。
  - プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、500 の VLAN をサポートしているモデルの場合、トンネル数は 500 から設定された物理インターフェイスの数を引いた数になります。
- ダイナミック VTI の場合、ダイナミックに作成された仮想アクセスインターフェイスの最大数は、1,024 またはプラットフォームの合計インターフェイス制限のいずれか少ない方です。
- VTI は IKE のバージョン v1 および v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- NAT を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- IKE および IPsec のセキュリティアソシエーションには、トンネル内のデータトラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。

- トンネルグループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。
- サイト間トンネルグループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブモードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。
- 暗号マップに設定されるピア アドレスと VTI のトンネル宛先が異なる場合、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセスルールを適用することができます。
- ICMP ping は、VTI インターフェイス間でサポートされます。
- IKEv2 サイト間 VPN トンネルのピアデバイスが IKEv2 設定要求ペイロードを送信した場合、ASA はデバイスとの IKEv2 トンネルを確立できません。ASA がピアデバイスとの VPN トンネルを確立するには、ピアデバイスで `config-exchange` 要求を無効にする必要があります。
- ダイナミック VTI は HA および IKEv2 をサポートします。

### デフォルト設定

- デフォルトでは、VTI 経由のトラフィックは、すべて暗号化されます。
- VTI インターフェイスのデフォルトのセキュリティレベルは 0 です。セキュリティレベルを設定することはできません。

### VTI の制限事項

ASA は、VTI 復号の後にセキュリティグループタグ (SGT) フレームとパケットをドロップします。

ダイナミック VTI は以下をサポートしていません。

- ECMP と VRF
- クラスタリング
- IKEv1
- QoS

ダイナミック VTI では、トンネル送信元が指定されていないと、管理専用インターフェイスとフェールオーバーインターフェイスを除くデバイスのすべてのインターフェイスで、IKEv2 が有効になります。

## VTI トンネルの作成

VTI トンネルを設定するには、IPsec プロポーザル（トランスフォームセット）を作成します。IPsec プロポーザルを参照する IPsec プロファイルを作成した後で、IPsec プロファイルを持つ VTI インターフェイスを作成します。リモートピアには、同じ IPsec プロポーザルおよび IPsec プロファイルパラメータを設定します。SA ネゴシエーションは、すべてのトンネルパラメータが設定されると開始します。



(注) VPN および VTI ドメインの両方に属し、物理インターフェイス上で BGP 隣接関係を持つ ASA では、次の動作が発生します。

インターフェイスヘルスチェックによって状態の変更がトリガーされると、物理インターフェイスでのルートは、新しいアクティブなピアとの BGP 隣接関係が再確立されるまで削除されます。この動作は、論理 VTI インターフェイスには該当しません。

VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセス制御リストを適用することができます。IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバルコンフィギュレーションモードで `sysopt connection permit-vpn` コマンドを入力します。

ACL をチェックせずに ASA を通過する IPsec トラフィックをイネーブルにするための次のコマンドを使用できます。

**hostname(config)# sysopt connection permit-vpn**

外部インターフェイスと VTI インターフェイスのセキュリティレベルが 0 の場合、VTI インターフェイスに ACL が適用されていても、`same-security-traffic` が設定されていなければヒットしません。

この機能を設定するには、グローバルコンフィギュレーションモードで **intra-interface** 引数を指定して **same-security-traffic** コマンドを実行します。

### 手順

- ステップ 1 IPsec プロポーザル（トランスフォームセット）を追加します。
- ステップ 2 IPsec プロファイルを追加します。
- ステップ 3 VTI トンネルを追加します。

## IPsec プロポーザル（トランスフォームセット）の追加

トランスフォームセットは、VTIトンネル内のトラフィックを保護するために必要です。これは、VPN内のトラフィックを保護するためのセキュリティプロトコルとアルゴリズムのセットであり、IPsecプロファイルの一部として使用されます。

### 始める前に

- VTIに関連付けられたIKEセッションを認証するには、事前共有キーまたは証明書のいずれかを使用できます。IKEv2では、非対称認証方式とキーが使用できます。IKEv1とIKEv2のどちらも、VTIに使用するトンネルグループの下に事前共有キーを設定する必要があります。
- IKEv1を使用した証明書ベースの認証には、イニシエータで使用されるトラストポイントを指定する必要があります。レスポндаについては、`tunnel-group` コマンドでトラストポイントを設定する必要があります。IKEv2では、イニシエータとレスポндаの両方について、認証に使用するトラストポイントを `tunnel-group` コマンドで設定する必要があります。

### 手順

---

**ステップ 1** [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] を選択します。

**ステップ 2** セキュリティアソシエーションを確立するための IKEv1 または IKEv2 を設定します。

- IKEv1 を設定します。
    - a) [IKEv1 IPsec Proposals (Transform Sets)] パネルで [Add] をクリックします。
    - b) [Set Name] を入力します。
    - c) [Tunnel] チェックボックスは、デフォルトの選択のままにします。
    - d) [ESP Encryption] および [ESP Authentication] を選択します。
    - e) [OK] をクリックします。
  - IKEv2 を設定します。
    - a) [IKEv2 IPsec Proposals] パネルで [Add] をクリックします。
    - b) [Name] と [Encryption] を入力します。
    - c) [Integrity Hash] を選択します。
    - d) [OK] をクリックします。
-

## IPsec プロファイルの追加

IPsec プロファイルには、その参照先の IPsec プロポーザルまたはトランスフォーム セット内にある必要なセキュリティプロトコルおよびアルゴリズムが含まれています。これにより、2つのサイト間 VTI VPN ピアの間でセキュアな論理通信パスが確保されます。

### 手順

- ステップ 1** [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] を選択します。
- ステップ 2** [IPsec Profile] パネルで [Add] をクリックします。
- ステップ 3** [Name] に IPsec プロファイル名を入力します。
- ステップ 4** [IKE v1 IPsec Proposal] または [IKE v2 IPsec Proposal] に、IPsec プロファイルのために作成する IKE v1 IPsec プロポーザルまたは IKE v2 IPsec プロポーザルを入力します。IKEv1 トランスフォーム セットまたは IKEv2 IPsec プロポーザルのいずれかを選択できます。
- ステップ 5** VTI トンネルの一端をレスポндаとしてのみ動作させる必要がある場合は、[Responder only] チェックボックスをオンにします。
- VTI トンネルの一端をレスポндаとしてのみ動作するように設定できます。レスポндаのみの端は、トンネルまたはキー再生成を開始しません。
  - IKEv2 を使用する場合、セキュリティ アソシエーションのライフタイム期間は、イニシエータ側の IPsec プロファイルのライフタイム値より大きく設定します。こうすることで、イニシエータ側での正常なキー再生成が促進され、トンネルのアップ状態が保たれます。
  - イニシエータ側のキー再生成の設定が不明の場合、レスポндаのみのモードを解除して SA の確立を双方向にするか、レスポндаのみの端の IPsec ライフタイム値を無期限にして期限切れを防ぎます。
- ステップ 6** (任意) [Enable security association lifetime] チェックボックスをオンにして、セキュリティ アソシエーションの期間の値をキロバイトおよび秒で入力します。
- ステップ 7** (任意) [PFS Settings] チェックボックスをオンにして、必要な Diffie-Hellman グループを選択します。

Perfect Forward Secrecy (PFS) は、暗号化された各交換に対し、一意のセッション キーを生成します。この一意のセッションキーにより、交換は、後続の復号化から保護されます。PFS を設定するには、PFS セッション キーを生成する際に使用する Diffie-Hellman キー導出アルゴリズムを選択する必要があります。キー導出アルゴリズムは、IPsec セキュリティ アソシエーション (SA) キーを生成します。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。Diffie-Hellman グループは、両方のピアで一致させる必要があります。

これにより、暗号キー決定アルゴリズムの強度が確立されます。ASAはこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。

- ステップ 8** (任意) [Enable sending certificate] チェックボックスをオンにして、VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを選択します。必要に応じて、[Chain] チェックボックスをオンにします。
- ステップ 9** この IPsec プロファイルのリバースルートインジェクション (RRI) を有効にするには、[リバースルートインジェクションを有効にする (Enable Reverse Route Injection)] チェックボックスをオンにします。
- RRI は、ASA を実行している場合は OSPF、EIGRP などのダイナミック ルーティング プロトコルを実行する内部ルータのルーティングテーブルを入力します。それ以外の場合は、リモート VPN クライアントまたは LAN-to-LAN セッションの RIP を実行する内部ルータのルーティングテーブルを入力します。RRI は設定で行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティングテーブルにスタティックルートを自動的に追加し、OSPF を使用してそれらのルートをプライベートネットワークまたは境界ルータに通知します。送信元/宛先 (0.0.0.0/0.0.0.0) を保護ネットワークとして指定する場合は、RRI をイネーブルにしないでください。デフォルトルータを使用するトラフィックに影響しません。
- ステップ 10** [ダイナミック (Dynamic)] チェックボックスをオンにして、リバースルートをダイナミック ルートとして設定します。
- ステップ 11** [OK] をクリックします。
- ステップ 12** [IPsec Proposals (Transform Sets)] メイン パネルで [Apply] をクリックします。
- ステップ 13** [Preview CLI Commands] ダイアログボックスで、[Send] をクリックします。

## VTI インターフェイスの追加

新しい VTI インターフェイスを作成して VTI トンネルを確立するには、次の手順を実行します。



- (注) アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。<http://www.cisco.com/go/asa-config> の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

### 手順

- ステップ 1** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。
- ステップ 2** [Add] > [VTI Interface] の順に選択します。[Add VTI Interface] ウィンドウが表示されます。
- ステップ 3** [General] タブで次の手順を実行します。
- VTI ID** を入力します。範囲は 0 ~ 10413 です。最大 10413 の VTI インターフェイスがサポートされます。
  - [Interface Name] を入力します。

- c) [インターフェイスの有効化 (Enable Interface)] チェックボックスがオンになっていることを確認します。
- d) [パスモニタリング (Path Monitoring)] ドロップダウンリストから [IPv4] または [IPv6] を選択し、ピアの IP アドレスを入力します。
- e) [コスト (Cost)] を入力します。指定できる範囲は 1 ~ 65535 です。  
コストは、複数の VTI 間でトラフィックを負荷分散するための優先順位を決定します。最も小さい番号が最も高い優先順位になります。
- f) IP アドレスの設定：  
[アドレス (Address)] オプションボタンをクリックして、IP アドレスとサブネットマスクを設定します。  
または  
[アンナンバード (Unnumbered)] オプションボタンをクリックし、[IP アンナンバード (IP Unnumbered)] ドロップダウンリストからインターフェイスを選択して、その IP アドレスを借用します。リストからループバックインターフェイスまたは物理インターフェイスを選択することができます。

ステップ 4 [詳細 (Advanced)] タブで次の操作を実行します。

- a) [Cisco TrustSec に対してセキュリティグループタグ付けを有効にする (Enable secure group tagging for Cisco TrustSec)] チェックボックスをオンにして、VPN トポロジの SVTI および DVTI 経由でのセキュリティグループタグ (SGT) 伝達を有効にします。
- b) 出力パケットに SGT でタグを付けるには、[出力パケットにセキュリティグループタグでタグ付けする (Tag egress packets with secure group tags)] チェックボックスをオンにします。
- c) スタティック SGT をすべての入力パケットに割り当てるには、[スタティック セキュリティグループタグをすべての入力パケットに割り当てる (Assign a static secure group tag to all ingress packets)] チェックボックスをオンにします。
- d) [セキュリティグループタグ (Secure Group Tag)] フィールドで、VTI インターフェイスの SGT を入力します。範囲は 2 ~ 65519 です。
- e) 必要に応じて、[これは信頼されているインターフェイスであるため既存のセキュリティグループタグをオーバーライドしない (This is a trusted interface. Do not override existing security group tags)] チェックボックスをオンにします。
- f) SVTI 経由の SGT 伝達を必須にするには、[セキュリティグループタグインラインを適用 (Security group tag inline force)] チェックボックスをオンにします。
- g) [Destination IP] に入力します。
- h) [送信元インターフェイス (Source Interface)] ドロップダウンリストから、トンネル送信元インターフェイスを選択します。  
ループバック インターフェイスまたは物理インターフェイスを選択することもできます。
- i) [IPsec ポリシーによるトンネル保護 (Tunnel Protection with IPsec Policy)] フィールドで、IPsec ポリシーを選択します。
- j) [Tunnel Protection with IPsec Profile] フィールドで、IPsec プロファイルを選択します。

k) [Ensure the Enable Tunnel Mode IPv4 IPsec] チェックボックスをオンにします。

**ステップ 5** [OK] をクリックします。

**ステップ 6** [Interfaces] パネルで [Apply] をクリックします。

**ステップ 7** [Preview CLI Commands] ダイアログボックスで、[Send] をクリックします。

更新された設定が読み込まれると、新しいVTIがインターフェイスのリストに表示されます。  
この新しいVTIは、IPsec サイト間VPNの作成に使用できます。

## 例

ASA と IOS デバイスの間の VTI トンネル (IKEv2 を使用) の設定例

```
ASA □  
  
crypto ikev2 policy 1  
  encryption aes-gcm-256  
  integrity null  
  group 21  
  prf sha512  
  lifetime seconds 86400  
!  
crypto ipsec ikev2 ipsec-proposal gcm256  
  protocol esp encryption aes-gcm-256  
  protocol esp integrity null  
!  
crypto ipsec profile asa-vti  
  set ikev2 ipsec-proposal gcm256  
!  
interface Tunnel 100  
  nameif vti  
  ip address 10.10.10.1 255.255.255.254  
  tunnel source interface [asa-source-nameif]  
  tunnel destination [router-ip-address]  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile asa-vti  
!  
tunnel-group [router-ip-address] ipsec-attributes  
  ikev2 remote-authentication pre-shared-key cisco  
  ikev2 local-authentication pre-shared-key cisco  
!  
crypto ikev2 enable [asa-interface-name]  
  
IOS □  
  
!  
crypto ikev2 proposal asa-vti  
  encryption aes-gcm-256  
  prf sha512  
  group 21  
!
```

```

crypto ikev2 policy asa-vti
match address local [router-ip-address]
proposal asa-vti
!
crypto ikev2 profile asa-vti
match identity remote address [asa-ip-address] 255.255.255.255
authentication local pre-share key cisco
authentication remote pre-share key cisco
no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
set ikev2-profile asa-vti
set transform-set gcm256
!
interface tunnel 100
ip address 10.10.10.0 255.255.255.254
tunnel mode ipsec ipv4
tunnel source [router-interface]
tunnel destination [asa-ip-address]
tunnel protection ipsec profile asa-vti
!

```

## ダイナミック VTI インターフェイスの追加

ダイナミック VTI の仮想テンプレートを作成するには、次の手順を行います。



- (注) アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。<http://www.cisco.com/go/asa-config> の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

### 始める前に

IPsec プロファイルと IP アンナンバード インターフェイスが設定されていることを確認します。

### 手順

- ステップ 1 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に選択します。
- ステップ 2 [追加 (Add)] > [DVTI インターフェイス (DVTI Interface)] の順に選択します。[DVTI インターフェイスの追加 (Add DVTI Interface)] ウィンドウが表示されます。
- ステップ 3 [General] タブで次の手順を実行します。
  - a) **DVTI ID** を入力します。この ID には 1 ~ 10413 の任意の値を指定できます。デバイスごとに最大 1024 の VTI インターフェイスがサポートされます。

- b) [Interface Name] を入力します。
- c) [アラートの有効化 (Enable Alert)] チェックボックスがオンになっていることを確認します。
- d) [IPアンナンバード (IP Unnumbered)] ドロップダウンリストからインターフェイスを選択します。

仮想テンプレートは、選択したインターフェイスの IP アドレスを継承します。トンネル送信元 IP アドレスとは異なる IP アドレスを使用していることを確認してください。任意の物理インターフェイスまたはデバイスに設定されているループバックアドレスを選択できます。

- e) [説明 (Description)] フィールドにダイナミック VTI の説明を入力します。

**ステップ 4** [Advanced] タブで、次の手順を実行します。

- a) [Cisco TrustSec に対してセキュリティグループタグ付けを有効にする (Enable security group tagging for Cisco TrustSec)] チェックボックスをオンにして、VPN トポロジのスタティック VTI 経由でのセキュリティグループタグ (SGT) 伝達を有効にします。
- b) 出力パケットに SGT でタグを付けるには、[出力パケットにセキュリティグループタグでタグ付けする (Tag egress packets with security group tags)] チェックボックスをオンにします。
- c) スタティック SGT をすべての入力パケットに割り当てるには、[スタティックセキュリティグループタグをすべての入力パケットに割り当てる (Assign a static security group tag to all ingress packets)] チェックボックスをオンにします。
- d) [セキュリティグループタグ (Security Group Tag)] フィールドで、スタティック VTI インターフェイスの SGT を入力します。範囲は 2 ~ 65519 です。
- e) [送信元インターフェイス (Source Interface)] ドロップダウンリストから、トンネル送信元インターフェイスを選択します。インターフェイスの IP アドレスは、スポークの宛先 IP アドレスになります。リストから選択できるのは、物理インターフェイスとループバックインターフェイスだけです。
- f) トンネル送信元 IP アドレスが設定されたインターフェイスのみから VPN セッション要求を受け入れるには、[IPv6 送信元アドレスの有効化 (Enable IPv6 Source Address)] チェックボックスをオンにします。このオプションを有効にしない場合、ASA はすべてのインターフェイスからの VPN セッション要求を受け入れます。

また、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。上記のオプションを有効にしない場合、仮想アクセスインターフェイスは、ASA が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。

- g) [IPsec プロファイルによるトンネル保護 (Tunnel Protection with IPsec Profile)] ドロップダウンリストから、IPsec プロファイルを選択します。
- h) [IPsec のトンネルモード IP オーバーレイの有効化 (Enable Tunnel Mode IP Overlay for IPsec)] チェックボックスをオンにし、[IPv4] または [IPv6] オプションボタンを選択して、IPsec トンネルモードを有効にします。

**ステップ 5** [IPv6] タブで次の操作を実行します。

- a) [IPv6 アドレスアンナumberド (IPv6 Address Unnumbered) ] 参照ボタンをクリックし、リストから IPv6 アドレスを選択します。

仮想テンプレートから複製されたすべての仮想アクセスインターフェイスは、同じ IP アドレスを持つことになります。

- b) [OK] をクリックします。

**ステップ 6** [CLI コマンドのプレビュー (Preview CLI Commands) ] ダイアログボックスで、仮想テンプレートコマンドを表示できます。

**ステップ 7** [送信 (Send) ] をクリックします。

### 次のタスク

このテンプレートをトンネルグループに適用します。詳細については、[Site-to-Site トンネルグループ](#)を参照してください。

## 仮想トンネルインターフェイスの機能履歴

機能名	リリース	機能情報
ダイナミック仮想トンネルインターフェイスのサポート	9.19(1)	<p>ダイナミック VTI を作成し、それを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できます。ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。</p> <p>新規/変更された画面：[設定 (Configuration) ]&gt;[デバイスのセットアップ (Device Setup) ]&gt;[インターフェイスの設定 (Interface Settings) ]&gt;[インターフェイス (Interfaces) ]&gt;[追加 (Add) ]&gt;[DVTI インターフェイス (DVTI Interface) ]&gt;[詳細 (Advanced) ]</p>
OSPF IPv4 および IPv6 のサポート	9.19(1)	VTI 経由の OSPF IPv4 および IPv6 ルーティングプロトコルをサポートします。
EIGRP のサポート	9.19(1)	VTI 経由の EIGRP IPv4 および IPv6 ルーティングプロトコルをサポートします。

機能名	リリース	機能情報
スタティックおよびダイナミック VTI のループバックインターフェイスのサポート	9.19(1)	<p>ループバックインターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。</p> <p>新規/変更された画面：[設定 (Configuration)] &gt; [デバイスのセットアップ (Device Setup)] &gt; [インターフェイスの設定 (Interface Settings)] &gt; [インターフェイス (Interfaces)] &gt; [VTI インターフェイスの追加 (Add VTI Interface)] &gt; [詳細 (Advanced)]</p>
ローカルトンネル ID のサポート	9.17(1)	<p>ASA は、ASA が NAT の背後に複数の IPsec トンネルを持ち、Cisco Umbrella Secure Internet Gateway (SIG) に接続できるようにする、一意のローカルトンネル ID をサポートしています。ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。</p>
スタティック VTI での IPv6 のサポート	9.16(1)	<p>ASA は、仮想トンネルインターフェイス (VTI) の設定で IPv6 アドレスをサポートしています。</p> <p>VTI トンネル送信元インターフェイスには、トンネルエンドポイントとして使用するように設定できる IPv6 アドレスを設定できます。トンネル送信元インターフェイスに複数の IPv6 アドレスがある場合は、使用するアドレスを指定できます。指定しない場合は、リストの最初の IPv6 グローバルアドレスがデフォルトで使用されます。</p> <p>トンネルモードは、IPv4 または IPv6 のいずれかです。ただし、トンネルをアクティブにするには、VTI で設定されている IP アドレスタイプと同じである必要があります。IPv6 アドレスは、VTI のトンネル送信元インターフェイスまたはトンネル宛先インターフェイスに割り当てることができます。</p>
デバイスあたり 1024 個の VTI インターフェイスのサポート	9.16(1)	<p>デバイスに設定できる VTI の最大数が、100 個から 1024 個に増加しました。</p> <p>プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、ASA 5510 は 100 個の VLAN をサポートしているため、トンネル数は 100 から設定された物理インターフェイスの数を引いた数になります。</p> <p>新規/変更された画面：なし</p>
VTI での DHCP リレーサーバーのサポート	9.14(1)	<p>ASA は、インターフェイスを接続する DHCP リレーサーバーとして VTI インターフェイスを設定することを可能にします。</p> <p>DHCP リレーに VTI インターフェイスを指定できるように次の画面が変更されました。</p> <p>[Configuration] &gt; [Device Management] &gt; [DHCP] &gt; [DHCP Relay] &gt; [DHCP Relay Interface Servers]</p>

機能名	リリース	機能情報
VTI での IKEv2、証明書ベース認証、および ACL のサポート	9.8(1)	<p>仮想トンネルインターフェイス (VTI) は、BGP (静的 VTI) をサポートするようになりました。スタンドアロンモードとハイアベイラビリティモードで、IKEv2 を使用できます。IPsec プロファイルにトラストポイントを設定することにより、証明書ベースの認証を使用できます。また、入力トラフィックをフィルタリングする access-group コマンドを使用して、VTI 上でアクセスリストを適用することもできます。</p> <p>次の画面で、証明書ベース認証のトラストポイントを選択するオプションが導入されました。</p> <p>[設定 (Configuration)] &gt; [サイト間VPN (Site-to-Site VPN)] &gt; [詳細 (Advanced)] &gt; [IPsec プロポーザル (トランスフォームセット) (IPsec Proposals (Transform Sets))] &gt; [IPsec プロファイル (IPsec Profile)] &gt; [追加 (Add)]</p>
仮想トンネルインターフェイス (VTI) のサポート	9.7(1)	<p>ASA が、仮想トンネルインターフェイス (VTI) と呼ばれる新しい論理インターフェイスによって強化されました。VTI はピアへの VPN トンネルを表すために使用されます。これは、トンネルの各終端に接続されている IPsec プロファイルを利用したルートベースの VPN をサポートします。VTI を使用することにより、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングすることが不要になります。</p> <p>次の画面が導入されました。</p> <p>[設定 (Configuration)] &gt; [サイト間VPN (Site-to-Site VPN)] &gt; [詳細 (Advanced)] &gt; [IPsec プロポーザル (トランスフォームセット) (IPsec Proposals (Transform Sets))] &gt; [IPsec プロファイル (IPsec Profile)]</p> <p>[設定 (Configuration)] &gt; [サイト間VPN (Site-to-Site VPN)] &gt; [詳細 (Advanced)] &gt; [IPsec プロポーザル (トランスフォームセット) (IPsec Proposals (Transform Sets))] &gt; [IPsec プロファイル (IPsec Profile)] &gt; [追加 (Add)] &gt; [IPsec プロファイルの追加 (Add IPsec Profile)]</p> <p>[設定 (Configuration)] &gt; [デバイスのセットアップ (Device Setup)] &gt; [インターフェイスの設定 (Interface Settings)] &gt; [インターフェイス (Interfaces)] &gt; [追加 (Add)] &gt; [VTI インターフェイス (VTI Interface)]</p> <p>[設定 (Configuration)] &gt; [デバイスのセットアップ (Device Setup)] &gt; [インターフェイスの設定 (Interface Settings)] &gt; [インターフェイス (Interfaces)] &gt; [追加 (Add)] &gt; [VTI インターフェイス (VTI Interface)] &gt; [全般 (General)]</p> <p>[設定 (Configuration)] &gt; [デバイスのセットアップ (Device Setup)] &gt; [インターフェイスの設定 (Interface Settings)] &gt; [インターフェイス (Interfaces)] &gt; [追加 (Add)] &gt; [VTI インターフェイス (VTI Interface)] &gt; [詳細 (Advanced)]</p>

## 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。