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

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された 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 （10 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（13 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（**インターフェイス virtual-Template** template_number **type tunnel**）。

   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 コマンドを設定します。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 1024 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、1024 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 復号化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。

詳細については、インターフェイス内トラフィックの許可（ヘアピニング）を参照してください。

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。レスポンダについては、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ンダの両方について、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

セキュリティ アソシエーションを確立するための IKEv1 トランスフォーム セットまたは IKEv2 IPsec プロポーザルを追加します。

IKEv1 トランスフォーム セットを追加します。

crypto ipsec ikev1 transform-set {*transform-set-name* | *encryption* | *authentication*}

例：

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

encryption では、IPsec データ フローを保護するための暗号化方式を指定します。

- esp-aes：AES と 128 ビット キーを使用します。
- esp-aes-192：AES と 192 ビット キーを使用します。
- esp-aes-256：AES と 256 ビット キーを使用します。
- esp-null：暗号化なし。

authentication では、IPsec データ フローを保護するための暗号化方式を指定します

- esp-md5-hmac：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。
- esp-sha-hmac：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
- esp-none：HMAC 認証なし。

IKEv2 IPsec プロポーザルを追加します。

（注）
IOS プラットフォームについては、IKEv2 プロファイル コンフィギュレーション モードで **no config-exchange request** コマンドを使用し、設定の交換のオプションをディセーブルにします。詳細については、「http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280」を参照してください。

- IPsec プロポーサルの名前を指定します。

crypto ipsec ikev2 ipsec-proposal *IPsec proposal name*

例：

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- crypto IPsec ikev2 ipsec-proposal コンフィギュレーション モードで、セキュリティ パラメータを指定します。

  protocol esp {encryption {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null} | integrity {sha-1 | sha-256 | sha-384 | sha-512 | null}

例：

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption aes aes-192
```

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 プロファイル名を設定します。

crypto ipsec profile *name*

例：

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

ステップ 2 IKEv1 または IKEv2 プロポーザルを設定します。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。

a) IKEv1 トランスフォーム セットを設定します。

- IKEv1 プロポーザルを設定するには、crypto ipsec profile コマンド サブモードで次のコマンドを入力します。

  set ikev1 transform set *set_name*

  この例の SET1 は、以前に作成された IKEv1 プロポーザル セットです。

  ```
  ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
  ```

b) IKEv2 プロポーザルを設定します。

- IKEv2 プロポーザルを設定するには、crypto ipsec profile コマンド サブモードで次のコマンドを入力します。

  set ikev2 ipsec-proposal *IPsec_proposal_name*

この例では、SET1 は、以前に作成された IKEv2 IPsec プロポーザルです。

```
ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
```

ステップ 3 （任意）セキュリティ アソシエーションの期間を指定します。

set security-association lifetime { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

例：

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

ステップ 4 （任意）VTI トンネルの一端をレスポンダとしてのみ動作するように設定します。

responder-only

- VTI トンネルの一端をレスポンダとしてのみ動作するように設定できます。レスポンダのみの端は、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。
- IKEv1 を使用すると、IOS が継続的なチャネル モードをサポートしていないため、IOS は常にレスポンダのみのモードになります。ASA は、イニシエータ、セッション、キーの再生成になります。
- イニシエータ側のキー再生成の設定が不明の場合、レスポンダのみのモードを解除して SA の確立を双方向にするか、レスポンダのみの端の 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 5 （任意）PFS グループを指定します。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。

set pfs { **group14** }

例：

```
ciscoasa(config-ipsec-profile)# set pfs group14
```

ステップ 6 （任意）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指定します。

set trustpoint *name*

例：

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

ステップ 7 （任意）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）を有効にし、リバースルートをダイナミックに設定します。

set reverse-route [dynamic]

例：

```
ciscoasa(config-ipsec-profile)#set reverse-route dynamic
```

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 新しいトンネル インターフェイスを作成します。

interface tunnel *tunnel_interface_number*

トンネル ID を 0 ～ 10413 の範囲で指定します。最大 10413 の VTI インターフェイスがサポートされます。

例：

```
ciscoasa(config)#interface tunnel 100
```

ステップ 2 VTI インターフェイス の名前を入力します。

interface tunnel コマンド サブモードで、次のコマンドを入力します。

nameif *interface name*

例：

```
ciscoasa(config-if)#nameif vti
```

ステップ 3 VTI インターフェイスの IP アドレスを入力します。

ip address *IP addressmask*

例：

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

ステップ 4 仮想テンプレートが継承するインターフェイスの IPv4 アドレスまたは IPv6 アドレスを入力します。

デバイスに設定されている任意の物理インターフェイスかループバックアドレスを選択できます。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。

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

ステップ 5 トンネル送信元のインターフェイスを指定します。

tunnel source interface *interface_name*

送信元インターフェイスとして、物理インターフェイスかループバック インターフェイスを使用できます。

例：

```
ciscoasa(config-if)#tunnel source interface outside
```

ステップ 6 トンネル宛先の IP アドレスを指定します。

tunnel destination *ip_address*

例：

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

ステップ 7 トンネルにトンネル モード IPsec IPv4 を設定します。

tunnel mode ipsec *ipv4*

例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

ステップ 8 トンネルに IPsec プロファイルを割り当てます。

tunnel protection ipsec *IPsec profile*

例：

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

ステップ 9 スタティック VTI インターフェイスのトラフィックセレクタを割り当てます。

tunnel protection policy *acl_name*

アクセスリストには、1 つまたは複数のリストセレクタを含めることができます。このコマンドを設定しない場合、スタティック VTI インターフェイスは any-any セレクタを提案します。これがデフォルトの動作です。

例：

```
ciscoasa(config)# access-list Spoke-to-Hub extended permit ip 209.165.200.225
255.255.255.224 any
```

```
ciscoasa(config-if)# tunnel protection ipsec policy Spoke-to-Hub
```

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 新しい仮想テンプレートを作成します。

interface virtual-Template *template_number* **type tunnel**

template_number は、仮想テンプレート固有の番号です。範囲は 0 ～ 10413 です。

インターフェイス テンプレートはシャットダウン状態ではない必要があります。仮想テンプレートの必須パラメータは次のとおりです。

- インターフェイス名
- トンネル IPsec モード
- トンネル IPsec プロファイル

例：

```
ciscoasa(config)#interface virtual-Template 101 type tunnel
```

ステップ 2 ダイナミック VTI 仮想テンプレート インターフェイスの名前を指定します。

interface コンフィギュレーション モードで、次のコマンドを使用します。

nameif *interface_name*

ASA は、仮想アクセスインターフェイスを <*Virtual_Template_name*>_va<*n*> として動的に作成します。たとえば、仮想テンプレートの名前が dVTI101 の場合、仮想アクセスインターフェイスは dVTI101_va1、dVTI101_va2 などになります。仮想テンプレートを変更する場合は、**shutdown** コマンドを使用して仮想テンプレートをシャットダウンする必要があります。

例：

```
ciscoasa(config-if)#nameif dVTI101
```

ステップ 3 仮想テンプレートが継承するインターフェイスの IPv4 アドレスまたは IPv6 アドレスを設定します。

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

仮想テンプレートは、任意の物理インターフェイスの IP アドレスまたはデバイスに設定されたループバックアドレスを継承できます。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。

例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

ステップ 4 （任意）トンネル送信元インターフェイスを指定します。

tunnel source interface *interface_name*

発信元インターフェイスは、物理インターフェイスかループバック インターフェイスです。

ASA は、トンネル送信元 IP アドレスとして設定されたインターフェイスからのみ VPN セッション要求を受け入れます。このインターフェイスを指定しない場合、ASA は任意のインターフェイスから受信した VPN セッション要求を受け入れます。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。

例：

```
ciscoasa(config-if)#tunnel source interface outside1
```

ステップ 5 トンネル保護モードを IPv4 または IPv6 として指定します。

tunnel mode ipsec {**ipv4** | **ipv6**}

例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

ステップ 6 トンネルに IPsec プロファイルを割り当てます。

tunnel protection ipsec profile *ipsec_profile*

この IPsec プロファイルは、交換のネゴシエーションに必要な IPSec/IKE パラメータを設定します。

例：

```
ciscoasa(config-if)#tunnel protection ipsec profile Profile1
```

ステップ 7 仮想テンプレートをトンネルグループに適用します。

tunnel-group *tunnel_group_name* **type** *type*

tunnel-group *tunnel_group_name* **ipsec-attributes**

virtual-template *template_number*

同じ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。ASA は、仮想テンプレートを使用して、VPN セッションごとに個別の仮想アクセスインターフェイスを作成します。

例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 type ipsec-l2l
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#virtual-template 101
```

ステップ 8 トンネルグループのダイナミックルーティングを有効にします。

tunnel-group *tunnel_group_name* **ipsec-attributes**

ikev2 route accept any

ikev2 route set interface

ikev2 route accept any コマンドを使用すると、ASA は、IKEv2 交換中に受信したすべてのトンネルインターフェイス IP アドレスを受け入れることが可能になります。デフォルトで、このオプションは有効になっています。

ikev2 route set interface コマンドを使用すると、ASA は、IKEv2 交換中にトンネルインターフェイスの IP アドレスを送信できるようになります。このオプションにより、BGP がトンネル経由で機能するための 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。

BGP/OSPF/EIGRP を使用して、トンネルグループに対して動的ルーティングが有効になっています。仮想テンプレートを設定した後、VTI トンネルを介してデバイス間のダイナミック VTI トラフィックをルーティングするようにルーティングポリシーを設定する必要があります。また、暗号化されたトラフィックを許可するアクセスコントロールルールを設定する必要があります。

例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ikev2 route set interface
ciscoasa(config-tunnel-ipsec)#ikev2 route accept any
```

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)	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。 新規/変更されたコマンド：**interface virtual-Template**、**ip unnumbered**、**ipv6 unnumbered**、**tunnel protection ipsec policy**
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。
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)	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。 新規/変更されたコマンド：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**
ローカルトンネル ID のサポート	9.17(1)	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。 新規/変更されたコマンド：**local-identity-from-cryptomap** 、
スタティック VTI での IPv6 のサポート	9.16(1)	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。 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。 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。 新規/変更されたコマンド：**tunnel source interface**、**tunnel destination**、**tunnel mode**

機能名	リリース	機能情報
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)	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。 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。 新規/変更されたコマンド：なし
VTI での DHCP リレーサーバーのサポート	9.14(1)	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。 次のコマンドが変更されました。**dhcprelay server** *ip_address vti_ifc_name*。
VTI での IKEv2、証明書ベース認証、および ACL のサポート	9.8(1)	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。 IPsec プロファイルのコンフィギュレーション モードに次のコマンドが導入されました。**set trustpoint**
仮想トンネルインターフェイス（VTI）のサポート	9.7.(1)	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。 次のコマンドが導入されました。**crypto ipsec profile**、**interface tunnel**、**responder-only**、**set ikev1 transform-set**、**set pfs**、**set security-association lifetime**、**tunnel destination**、**tunnel mode ipsec**、**tunnel protection ipsec profile**、**tunnel source interface**。

仮想トンネルインターフェイスの機能履歴

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。