



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 \(1 ページ\)](#)
- [VTI トンネルの作成 \(2 ページ\)](#)

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 VPN の代替策として、仮想トンネル インターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、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。これは、動的または静的なルートの使用が可能です。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 をサポートする静的 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。

仮想トンネル インターフェイスの注意事項

IPv6

- IPv6 はサポートされていません。

一般的な設定時の注意事項

- 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、動的または静的なルートを使用することができます。
- 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。
- ネットワークアドレス変換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。
- LAN-to-LAN 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。
- 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 インターフェイスにはセキュリティレベル設定はありません。
- 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リストを適用することができます。
- VTI では BGP のみサポートされます。
- ASA が IOS IKEv2 VTI クライアントを終端している場合は、IOS VTI クライアントによって開始されたこの L2L セッションのモード CFG 属性を ASA が取得できないため、IOS での設定交換要求を無効にします。

コンテキストモード

シングルモードでだけサポートされています。

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。

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。

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

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-des : 56 ビット DES-CBC を使用します。
- esp-3des : トリプル DES アルゴリズムを使用します。
- 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/al/sec-al-cr-book/sec-cr-c2.html#wp3456426280>」を参照してください。

- IPsec プロポーザ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 {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256
| aes-gmac | aes-gmac-192 | aes-gmac-256 | null} | integrity {md5 | sha-1 | sha-256 | sha-384 |
sha-512 | null}}
```

例 :

```
ciscoasa (config-ipsec-proposal) #protocol esp encryption 3des aes des
```

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нда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。
- IKEv1 を使用すると、IOS が継続的なチャンネル モードをサポートしていないため、IOS は常にレスポンド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、レスポンドのみのモードを解除して SA の確立を双方向にするか、レスポンドのみの端の 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 {group1 | group2 | group5}
```

例 :

```
ciscoasa(config-ipsec-profile)# set pfs group2
```

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
```

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*

例 :

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

トンネル ID を 0 ~ 100 の範囲で指定します。最大 100 の VTI インターフェイスがサポートされます。

(注) 他のデバイスから ASA 5506 に設定を移行する場合は、トンネル ID 範囲に 1 ~ 100 を指定します。これは、ASA 5506 デバイスで使用可能なトンネル範囲 1 ~ 100 に対応させるためです。

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 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*

例 :

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

ステップ 5 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 6 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 7 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
```

この新しい VTI は、IPsec サイト間 VPN の作成に使用できます。
