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 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

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。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。
- 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 インターフェイスのデフォルトのセキュリティレベルは 0 です。
- 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 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。

IPv6 のサポート

IPv6 はサポートされていません。

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。

DHCP リレー

DHCP リレーは、仮想トンネルインターフェイス（VTI）ではサポートされていません。

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

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ンダ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。
- 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 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 [OK] をクリックします。

ステップ 10 [IPsec Proposals (Transform Sets)] メイン パネルで [Apply] をクリックします。

ステップ 11 [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、**VTI ID** と入力します。0 ー 10413 の任意の値を指定できます。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 4 [Interface Name] を入力します。

[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。

ステップ 5 トンネルの送信元 **IP アドレス**と **サブネット マスク**を入力します。

ステップ 6 [Advanced] タブをクリックします。

すべてのフィールドに有効な値が入力または選択されていないと、トンネルは、VPN ウィザードに表示されません。

ステップ 7 **宛先 IP** アドレスを入力します。

ステップ 8 **送信元インターフェイス**を選択します。

ステップ 9 [Tunnel Protection with IPsec Profile] フィールドで、IPsec プロファイルを選択します。

ステップ 10 [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 11 [OK] をクリックします。

ステップ 12 [Interfaces] 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。

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。