IPsec 仮想トンネル インターフェイス

IP security（IPsec; IP セキュリティ）Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）では、IPsec トンネルを終了するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。IPsec VTI によって、リモート リンクを保護するための IPsec の設定が簡素化され、マルチキャストがサポートされ、さらには、ネットワーク管理およびロード バランシングが簡単に実現できるようになります。

機能情報の入手

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPsec 仮想トンネル インターフェイスの機能情報」（P.24）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

IPsec 仮想トンネル インターフェイスの制約事項

IPsec トランスフォーム セット

IPsec トランスフォーム セットを設定できるのは、トンネル モードでだけです。

IKE セキュリティ アソシエーション

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）Security Association（SA; セキュリティ アソシエーション）は VTI にバインドされています。IKE SA は VTI にバインドされているので、同じ IKE SA をクリプト マップに対して使用することは不可能です。

IPsec SA トラフィック セレクタ

スタティック VTI では、VTI インターフェイスに接続している単一の IPsec SA だけがサポートされます。IPsec SA のトラフィック セレクタは常に「IP any any」です。

Dynamic VTI（DVTI; ダイナミック VTI）も、単一の IPsec SA だけがサポートされるポイント間インターフェイスですが、DVTI は、発信側によって提案された IPsec セレクタを受け入れられるという点で柔軟性があります。

IPv4 および IPv6 パケット

この機能では、IPv4 パケットまたは IPv6 パケットをカプセル化するように設定されている SVTI がサポートされますが、IPv4 パケットによって IPv6 パケットを搬送すること、および IPv6 パケットによって IPv4 パケットを搬送することは不可能です。

プロキシ

SVTI では、「IP any any」プロキシだけがサポートされます。

DVTI では 1 つのプロキシだけがサポートされます。このプロキシは、「IP any any」かその何らかのサブセットになる可能性があります。

QoS トラフィック シェーピング

シェイプド トラフィックは交換されるプロセスです。

ステートフル フェールオーバー

IPsec ステートフル フェールオーバーは、IPsec VTI ではサポートされていません。

トンネル保護

shared キーワードは不要です。IPsec IPv4 モードで **tunnel mode ipsec ipv4** コマンドを使用する場合には設定しないでください。

スタティック VTI と GRE トンネル

IPsec VTI は、GRE トンネルとは逆に、IP ユニキャストおよびマルチキャストだけに制限されています。GRE トンネルには、IPsec 実装用の幅広いアプリケーションがあります。

VRF 認識 IPsec の設定

SVTI または DVTI を使用した VRF 認識 IPsec 設定では、VRF を Internet Security Association and Key Management Protocol（ISAKMP）プロファイル内で設定*しないでください*。代わりに、VRF は、SVTI のトンネル インターフェイス上で設定する必要があります。DVTI の場合、VRF を **ip vrf forwarding** コマンドを使用して vtemplate に適用する必要があります。

IPsec 仮想トンネル インターフェイスに関する情報

IPsec VTI の使用により、リモート アクセスの保護を提供する必要がある場合の設定プロセスが大幅に簡易化され、また、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）または、カプセル化および IPsec を使用したおよびクリプト マップ用の Layer 2 Tunneling Protocol（L2TP; レイヤ 2 プロトコル トンネリング）を使用するよりも簡単な代替手段を利用できます。IPsec VTI に関連した大きな利点は、設定に、物理インターフェイスに対する IPsec セッションのスタティック マッピングが不要であることです。IPsec トンネル エンドポイントは実際（仮想）のインターフェイスに関連付けられます。トンネル エンドポイントにはルーティング可能なインターフェイスがあるので、多くの共通インターフェイス機能を IPsec トンネルに適用できます。

IPsec VTI によって、複数パスの場合のように、物理インターフェイス上における IP ユニキャストおよびマルチキャストの両方の暗号化トラフィックの送受信の柔軟性が高まります。トラフィックがトンネル インターフェイスから、またはトンネル インターフェイスに対して転送されると、そのトラフィックは暗号化または復号化され、IP ルーティング テーブルで管理されます。IP ルーティングを使用してトラフィックをトンネル インターフェイスに転送すると、ネイティブの IPsec 設定内においてクリプト マップ付き Access Control List（ACL; アクセス コントロール リスト）を使用する複雑なプロセスと比較して、IPsec VPN 設定が簡単になります。DVTI は、他の現実のインターフェイスと同様に機能するので、トンネルがアクティブになるのと同時に、Quality of Service（QoS）、ファイアウォール、およびその他セキュリティ サービスを適用できます。

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Acceleration Module2+（VAM2+）が仮想インターフェイスを加速しない場合、IPsec 仮想インターフェイスを通過するパケットは、カプセル化用の Router Processor（RP）に直接送信されます。この方式は処理が遅くなる傾向があるので、スケーラビリティが制限されています。ハードウェアクリプト マップでは、すべての IPsec VTI が VAM2+ 暗号化エンジンによって加速され、トンネルを通過するすべてのトラフィックが VAM2+ によって暗号化または復号化されます。

IPsec VTI に関する詳細については、次の各項を参照してください。

- 「IPsec 仮想トンネル インターフェイスを使用する利点」（P.3）
- 「スタティック仮想トンネル インターフェイス」（P.4）
- 「ダイナミック仮想トンネル インターフェイス」（P.4）
- 「ダイナミック仮想トンネル インターフェイスのライフ サイクル」（P.6）
- 「IPsec 仮想トンネル インターフェイスを使用したルーティング」（P.6）
- 「IPsec 仮想トンネル インターフェイスを使用したトラフィックの暗号化」（P.6）

IPsec 仮想トンネル インターフェイスを使用する利点

IPsec VTI によって、機能を適用できる仮想インターフェイスを設定できます。暗号化されていないテキスト パケットの機能は VTI 上で設定されます。暗号化されたパケットの機能は物理外部インターフェイス上で適用されます。IPsec VTI を使用すると、NAT、ACL、および QoS などの各種機能のアプリケーションを分離して、それらを暗号化されていないテキストまたは暗号化されたテキスト、あるいはその両方に適用できます。クリプト マップを使用する場合、暗号化機能を IPsec トンネルに適用するための簡単な方法はありません。

Static VTI（SVTI; スタティック VTI）と DVTI という 2 つのタイプの VTI インターフェイスが存在します。

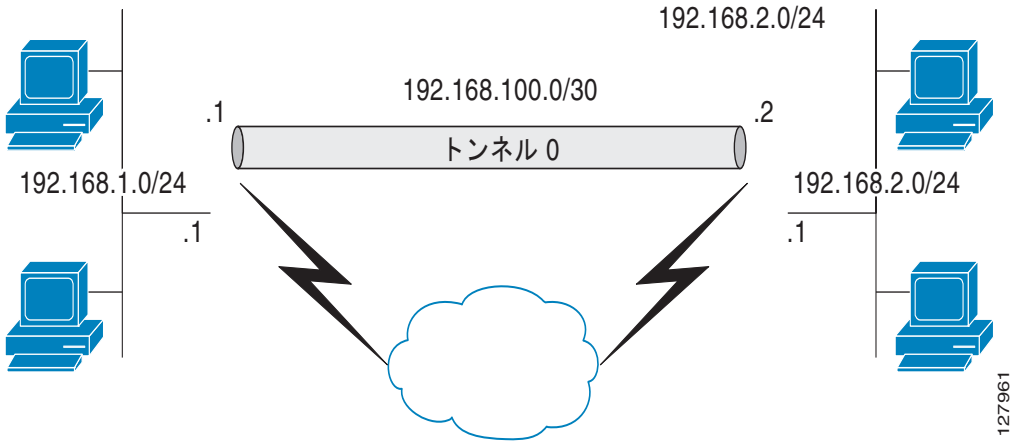
スタティック仮想トンネル インターフェイス

SVTI 設定は、トンネルによって 2 つのサイト間の常にオンであるアクセスが提供される、サイト間接続用に使用できます。SVTI を使用することの利点は、クリプト マップ設定とは逆に、ユーザが、GRE ヘッダーに必要な追加の 24 バイトなしで、トンネル インターフェイス上のダイナミック ルーティング プロトコルをイネーブルにでき、その結果、暗号化データ送信用の帯域幅を削減できることです。

さらに、複数の Cisco IOS ソフトウェア機能を、トンネル インターフェイス上、およびトンネル インターフェイスの物理出力インターフェイス上で直接設定できます。この直接設定によって、ユーザは、暗号化前または暗号化後のパスにおける機能のアプリケーションを確実に管理できます。

図 1 に SVTI の使用方法を示します。

図 1　　IPsec SVTI



IPsec VTI によって、ネイティブの IPsec トンネリングがサポートされ、物理インターフェイスのプロパティの大部分が示されます。

ダイナミック仮想トンネル インターフェイス

DVTI によって、リモートアクセス VPN 用接続のセキュリティ保護とスケーラビリティが向上します。DVTI 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。

DVTI は、サーバと、リモート設定の両方に対して使用可能です。トンネルによって、各 VPN セッション用に、個別のオンデマンド仮想アクセス インターフェイスが提供されます。仮想アクセス インターフェイス設定は、仮想テンプレート設定からコピーされます。このコピーには、IPsec 設定と、QoS、NetFlow、ACL といった、仮想テンプレート インターフェイス上で設定されたすべての Cisco IOS ソフトウェア機能が含まれています。

DVTI は、他の現実のインターフェイスと同様に機能するので、トンネルがアクティブになるのと同時に、QoS、ファイアウォール、およびその他セキュリティ サービスを適用できます。QoS 機能を使用して、ネットワーク上の各種アプリケーションのパフォーマンスを向上させることが可能です。Cisco IOS ソフトウェア内で提供される各種 QoS 機能の組み合せを使用して、音声、ビデオ、またはデータ アプリケーションをサポートできます。

DVTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。DVTI によって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーを RADIUS サーバ上で設定できます。グループごとまたはユーザごとの定義を、Extended Authentication（Xauth; 拡張認証）User または Unity グループを使用して作成するか、証明書から取得できます。DVTI は、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。IPsec DVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）と組み合せて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。DVTI によって、Virtual Route Forwarding（VRF; VPN ルーティングおよび転送）認識 IPsec の導入が簡単になります。VRF は、インターフェイス上で設定されます。

DVTI には、ルータ上での最小限の設定が必要です。単一の仮想テンプレートを設定およびコピーできます。

DVTI によって、IPsec セッション用のインターフェイスが作成され、ダイナミック IPsec VTI の動的なインスタンス化および管理のための仮想テンプレート インフラストラクチャが使用されます。仮想テンプレート インフラストラクチャは、ダイナミック仮想アクセス トンネル インターフェイスを作成するために拡張されます。DVTI は、ハブアンドスポーク設定で使用されます。単一の DVTI で複数のスタティック VTI をサポートできます。

（注） DVTI は、Easy VPN でだけサポートされます。つまり、DVTI エンドを、Easy VPN として設定する必要があります。

図 2 に、DVTI 認証パスを示します。

図 2　　ダイナミック IPsec VTI

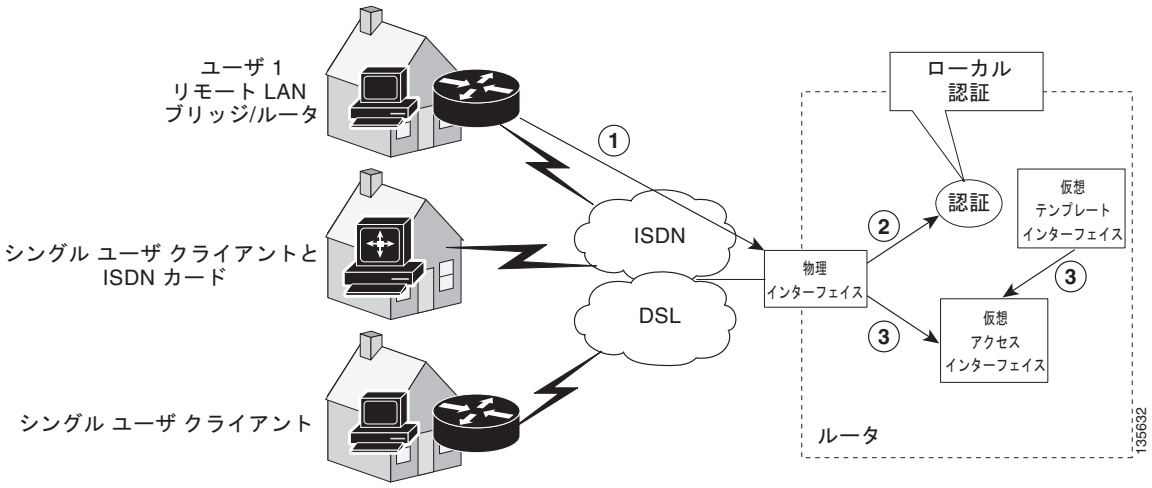


図 2 に示した認証は次のパスに従います。

1. ユーザ 1 がルータを呼び出します。
2. ルータ 1 によって ユーザ 1 が認証されます。
3. IPsec によって、仮想テンプレート インターフェイスから仮想アクセス インターフェイスがコピーされます。

ダイナミック仮想トンネル インターフェイスのライフ サイクル

IPsec プロファイルによって、DVTI のポリシーが定義されます。ダイナミック インターフェイスが、IKE フェーズ 1 および IKE フェーズ 1.5 の終了時に作成されます。ピアに対する IPsec セッションが終了すると、インターフェイスが削除されます。ピアに対する IKE と IPsec SA の両方が削除されると、IPsec セッションが終了します。

IPsec 仮想トンネル インターフェイスを使用したルーティング

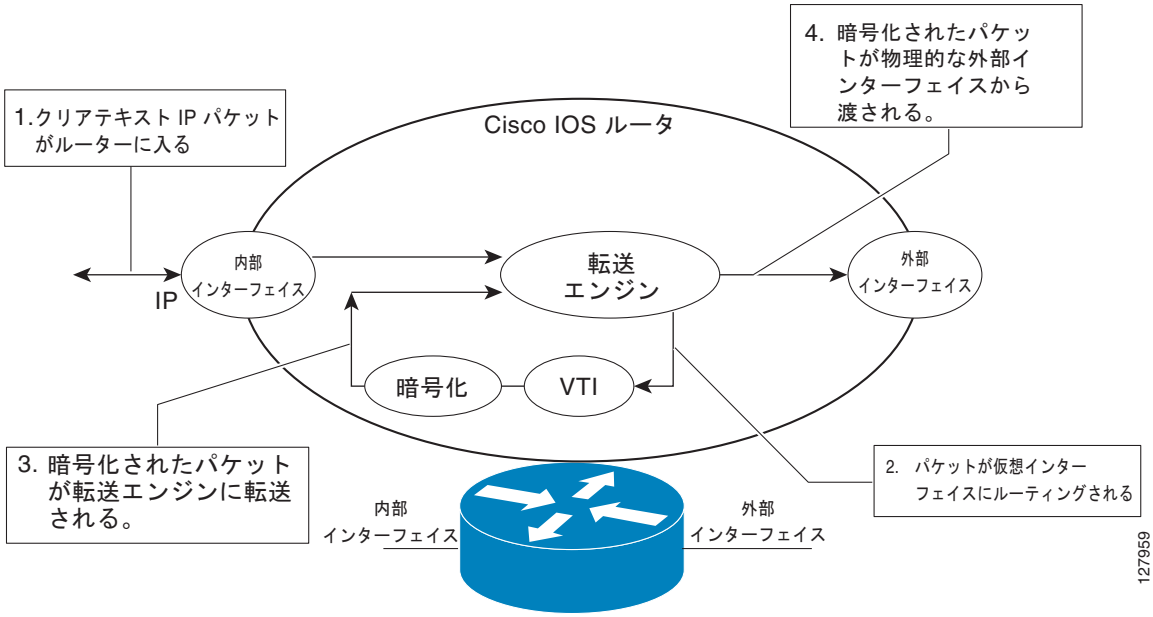
VTI はルーティング可能なインターフェイスなので、暗号化プロセスにおけるルーティングの役割は重要です。トラフィックは、VTI の外に転送される場合にだけ暗号化され、VTI に到着するトラフィックは、適宜、復号化およびルーティングされます。VTI を利用すれば、実際のインターフェイスをトンネル エンドポイントとして使用することによって、暗号化トンネルを確立できます。インターフェイスに対してルーティングしたり、QoS、ファイアウォール、ネットワーク アドレス変換、および Netflow 統計情報などのサービスを必要に応じて他のインターフェイスに適用したりできます。インターフェイスをモニタリングし、そのインターフェイスにルーティングできます。そのインターフェイスは、実際のインターフェイスであり、他のすべての通常の Cisco IOS インターフェイスの利点を備えているので、クリプト マップよりも有利です。

IPsec 仮想トンネル インターフェイスを使用したトラフィックの暗号化

IPsec VTI が設定されると、暗号化がトンネル内で実行されます。トラフィックがトンネル インターフェイスに転送されると、そのトラフィックが暗号化されます。トラフィックの転送は、IP ルーティング テーブルによって処理され、ダイナミックまたはスタティック ルーティングを使用してトラフィックを SVTI にルーティングできます。DVTI では、逆ルート注入が使用されるので、ルーティングの設定がさらに簡単になっています。IP ルーティングを使用してトラフィックを暗号化に転送すると、ネイティブの IPsec 設定内のクリプト マップを持つ ACL を使用する必要がなくなるので、IPsec VPN 設定が簡単になります。さらに、IPsec 仮想トンネルを使用すれば、IPsec によってマルチキャスト トラフィックを暗号化できます。

図 3 に、IPsec トンネルへの IPsec パケット フローを示します。

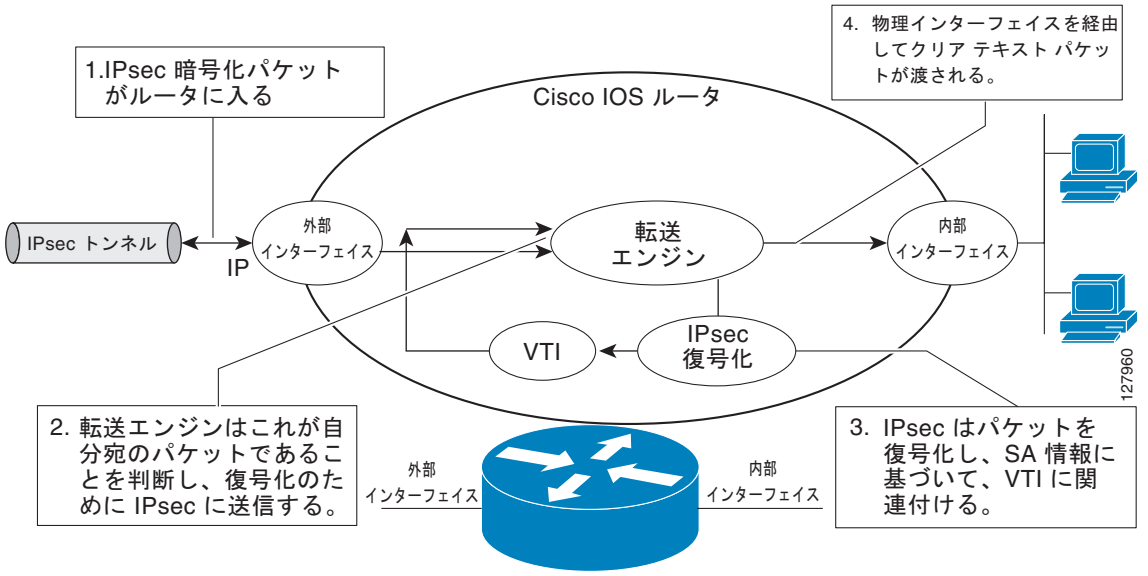
図 3　　IPsec トンネルへのパケット フロー



パケットが内部インターフェイスに到着すると、転送エンジンによってパケットが VTI にスイッチングされ、そこで暗号化されます。暗号化されたパケットは転送エンジンに戻され、そこで外部インターフェイスを介してスイッチングされます。

図 4 に、IPsec トンネルの外へのパケット フローを示します。

図 4　　IPsec トンネルの外へのパケット フロー



IPsec 仮想トンネル インターフェイスの設定方法

スタティック IPsec 仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface** *type number*
6. **ip address** *address mask*
7. **tunnel mode ipsec ipv4**
8. **tunnel source** *interface*
9. **tunnel destination** *ip-address*
10. **tunnel protection IPsec profile** *profile-name* [**shared**]

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** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 IPsec profile** *profile-name* **例：** `Router(config)# crypto IPsec profile PROF`	2 つの IPsec ルータ間における IPsec 暗号化のために使用される IPsec パラメータを定義します。
ステップ 4	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **例：** `Router(config)# set transform-set tset`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* **例：** `Router(config)# interface tunnel0`	トンネルが設定されるインターフェイスを指定し、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 6	**ip address** *address mask* **例：** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	IP アドレスおよびマスクを指定します。
ステップ 7	**tunnel mode ipsec ipv4** **例：** `Router(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 8	**tunnel source** *interface* **例：** `Router(config-if)# tunnel source loopback0`	トンネルの送信元をループバック インターフェイスとして指定します。
ステップ 9	**tunnel destination** *ip-address* **例：** `Router(config-if)# tunnel destination 172.16.1.1`	トンネルの宛先の IP アドレスを指定します。
ステップ 10	**tunnel protection IPsec profile** *profile-name* [**shared**] **例：** `Router(config-if)# tunnel protection IPsec profile PROF`	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。

ダイナミック IPsec 仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface virtual-template** *number*
6. **tunnel mode** *mode*
7. **tunnel protection IPsec profile** *profile-name* [**shared**]
8. **exit**
9. **crypto isakamp profile** *profile-name*
10. **virtual-template** *template-number*

手順の詳細

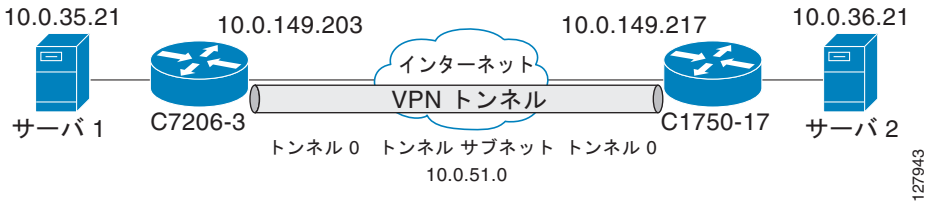
	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto IPsec profile** *profile-name* **例：** `Router(config)# crypto IPsec profile PROF`	2 つの IPsec ルータ間における IPsec 暗号化のために使用される IPsec パラメータを定義します。
ステップ 4	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **例：** `Router(config)# set transform-set tset`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 5	**interface virtual-template** *number* **例：** `Router(config)# interface virtual-template 2`	仮想テンプレート トンネル インターフェイスを定義し、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 6	**tunnel mode ipsec ipv4** **例：** `Router(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 7	**tunnel protection IPsec profile** *profile-name* [**shared**] **例：** `Router(config-if)# tunnel protection IPsec profile PROF`	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 8	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**crypto isakamp profile** *profile-name* **例：** `Router(config)# crypto isakamp profile red`	仮想テンプレート用に使用される ISAKAMP プロファイルを定義します。
ステップ 10	**virtual-template** *template-number* **例：** `Router(config)# virtual-template 1`	ISAKAMP プロファイルに付加された仮想テンプレートを指定します。

IPsec 仮想トンネル インターフェイスの設定例

IPsec を使用したスタティック仮想トンネル インターフェイス：例

次の設定例では、ピア間の認証用に事前共有キーが使用されています。VPN トラフィックは、暗号化のために IPsec VTI に転送されてから、物理インターフェイスに送信されます。サブネット 10 のトンネルでは、IPsec ポリシーに関してパケットがチェックされ、IPsec 暗号化のために Crypto Engine（CE; 暗号エンジン）に渡されます。図 5 に、IPsec VTI の設定を示します。

図 5　　IPsec を使用した VTI



C7206 ルータ設定

```
version 12.3

service timestamps debug datetime
service timestamps log datetime
hostname 7200-3
no aaa new-model
ip subnet-zero
ip cef
controller ISA 6/1
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto IPsec transform-set T1 esp-3des esp-sha-hmac
crypto IPsec profile P1
set transform-set T1
!
```

```
interface Tunnel0
 ip address 10.0.51.203 255.255.255.0
 ip ospf mtu-ignore
 load-interval 30
 tunnel source 10.0.149.203
 tunnel destination 10.0.149.217
 tunnel mode IPsec ipv4
 tunnel protection IPsec profile P1
!
interface Ethernet3/0
 ip address 10.0.149.203 255.255.255.0
 duplex full
!
interface Ethernet3/3
 ip address 10.0.35.203 255.255.255.0
 duplex full
!
ip classless
ip route 10.0.36.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end
```

C1750 ルータ設定

```
version 12.3

hostname c1750-17
no aaa new-model
ip subnet-zero
ip cef
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2

crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto IPsec transform-set T1 esp-3des esp-sha-hmac
crypto IPsec profile P1
set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 ip ospf mtu-ignore
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
interface FastEthernet0/0
 ip address 10.0.149.217 255.255.255.0
 speed 100
 full-duplex
!
interface Ethernet1/0
 ip address 10.0.36.217 255.255.255.0
 load-interval 30
 full-duplex
!


ip classless
ip route 10.0.35.0 255.255.255.0 Tunnel0
```

```
line con 0
line aux 0
line vty 0 4
end
```

IPsec スタティック仮想トンネル インターフェイスの結果の確認：例

ここでは、設定が正しく動作しているか確認するうえで利用可能な情報を示します。この表示では、Tunnel 0 が「up」で、回線プロトコルが「up」になっています。回線プロトコルが「down」の場合、セッションは非アクティブです。

C7206 ステータスの確認

```
Router# show interface tunnel 0

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport IPsec/IP, key disabled, sequencing disabled
Tunnel TTL 255

Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

Router# show crypto session

Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4, origin: crypto map

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

VRF 認識スタティック仮想トンネル インターフェイス：例

VRF をスタティック VTI の例に追加するには、次の例で示すように、**ipvrf** コマンドおよび **ip vrf forwarding** コマンドを設定に含めます。

C7206 ルータ設定

```
hostname c7206
.
.
ip vrf sample-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
.
interface Tunnel0
 ip vrf forwarding sample-vti1
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
.
.
!
end
```

QoS を使用したスタティック仮想トンネル インターフェイス：例

トンネル インターフェイスの下に **service-policy** 文を指定することによって、QoS ポリシーをトンネル エンドポイントに適用できます。次に、トンネル インターフェイス外のポリシング トラフィックの例を示します。

C7206 ルータ設定

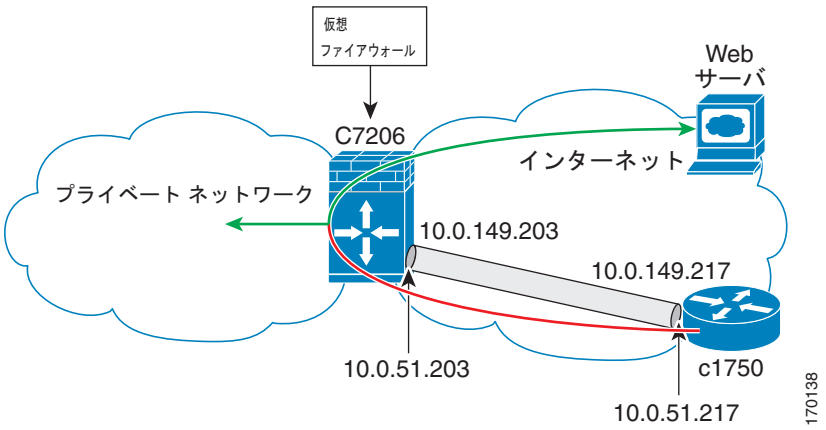
```
hostname c7206
.
.
class-map match-all VTI
 match any
!
policy-map VTI
  class VTI
  police cir 2000000
    conform-action transmit
    exceed-action drop
!
.
.
```

```
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
 service-policy output VTI
!
.
.
!
end
```

仮想ファイアウォールを使用したスタティック仮想トンネル インターフェイス：例

仮想ファイアウォールを SVTI トンネルに適用することによって、スポークからのトラフィックを、ハブを通過させてインターネットに送信できます。図 6 に、企業ファイアウォールによって本質的に保護されているスポークを使用した SVTI を示します。

図 6　　仮想ファイアウォールを使用したスタティック VTI



SVTI の基本設定は、仮想ファイアウォール定義を含むように変更されています。

C7206 ルータ設定

```
hostname c7206
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
```

```
 ip access-group 100 in
 ip nat outside
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 ip nat inside
 ip inspect IOSFW1 in
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny   esp any any
access-list 110 deny   udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny   udp any eq non500-isakmp any
!
end
```

ダイナミック仮想トンネル インターフェイス Easy VPN サーバ：例

次に、DVTI Easy VPN サーバを使用する例を示します。このサーバは、IPsec リモート アクセス アグリゲータになります。クライアントを、Cisco VPN クライアントが実行されるホーム ユーザにしたり、Easy VPN クライアントとして設定された Cisco IOS ルータにしたりできます。

C7206 ルータ設定

```
hostname c7206
!
aaa new-model
aaa authentication login local_list local
aaa authorization network local_list local
aaa session-id common
!
ip subnet-zero
ip cef
!
username cisco password 0 cisco123
!
controller ISA 1/1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group group1
 key cisco123
```

```
 pool group1pool
 save-password
!
crypto isakmp profile vpn1-ra
   match identity group group1
   client authentication list local_list
   isakmp authorization list local_list
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set VTI-TS esp-3des esp-sha-hmac
!
crypto ipsec profile test-vti1
 set transform-set VTI-TS
!
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
!
interface GigabitEthernet0/2
 description Internal Network
 ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/1
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
!
ip local pool group1pool 192.168.1.1 192.168.1.4
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
end
```

ダイナミック仮想トンネル インターフェイス Easy VPN サーバの結果の確認：例

次に、DVTI が、Easy VPN サーバ用に設定されている例を示します。

```
Router# show running-config interface Virtual-Access2

Building configuration...

Current configuration : 250 bytes
!
interface Virtual-Access2
 ip unnumbered GigabitEthernet0/1
 ip virtual-reassembly
 tunnel source 172.18.143.246
 tunnel destination 172.18.143.208
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
 no tunnel protection ipsec initiate
end

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.2.1.10 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, GigabitEthernet0/1
     192.168.1.0/32 is subnetted, 1 subnets
S       192.168.1.1 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/24 is subnetted, 1 subnets
C       10.2.1.0 is directly connected, GigabitEthernet0/2
S*   0.0.0.0/0 [1/0] via 172.18.143.1
```

ダイナミック仮想トンネル インターフェイス Easy VPN クライアント：例

次に、ルータを Easy VPN クライアントとして設定する場合の例を示します。この例では、接続する PC から実行できる Easy VPN クライアントと、基本的に同じ考えが使用されています。実際、Easy VPN サーバの設定は、ソフトウェア クライアントまたは Cisco IOS クライアント用に動作します。

```
hostname c1841
!
no aaa new-model
!
ip cef
!
username cisco password 0 cisco123
!
crypto ipsec client ezvpn CLIENT
 connect manual
 group group1 key cisco123
 mode client
 peer 172.18.143.246
 virtual-interface 1
 username cisco password cisco123
 xauth userid mode local
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 description Internet Connection
 ip address 172.18.143.208 255.255.255.0
 crypto ipsec client ezvpn CLIENT
!
interface FastEthernet0/1
 ip address 10.1.1.252 255.255.255.0
 crypto ipsec client ezvpn CLIENT inside
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
!
ip route 0.0.0.0 0.0.0.0 172.18.143.1 254
!
end
```

クライアント定義は、さまざまな方法で設定できます。**connect** コマンドで、モードを自動かマニュアルに指定できます。接続モードをマニュアルに設定した場合。ユーザが IPsec トンネルを手動で開始する必要があります。

mode コマンドにも注意してください。モードは、クライアント、ネットワーク拡張、またはネットワーク拡張プラスにできます。この例は、クライアント モードを示しています。つまり、クライアントに対してサーバからのプライベート アドレスが与えられます。ネットワーク拡張モードは、クライ

アントがサーバに対して、その接続プライベート サブネットを指定する点で、クライアント モードとは異なります。モードによって、両端のルーティング テーブルが若干異なります。指定したモードにかかわらず、IPSec トンネルの基本動作は同じです。

ダイナミック仮想トンネル インターフェイス Easy VPN クライアントの結果の確認：例

次の各例では、DVTI のステータスを表示するための各種方法を示します。

```
Router# show running-config interface Virtual-Access2

Building configuration...

Current configuration : 148 bytes
!
interface Virtual-Access2
 ip unnumbered Loopback1
 tunnel source FastEthernet0/0
 tunnel destination 172.18.143.246
 tunnel mode ipsec ipv4
end

Router# show running-config interface Loopback1

Building configuration...

Current configuration : 65 bytes
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.255
end

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.18.143.1 to network 0.0.0.0

     10.0.0.0/32 is subnetted, 1 subnets
C       10.1.1.1 is directly connected, Loopback0
     172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, FastEthernet0/0
     192.168.1.0/32 is subnetted, 1 subnets
C       192.168.1.1 is directly connected, Loopback1
S*   0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access2

Router# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 6

Tunnel name : CLIENT
Inside interface list: FastEthernet0/1
Outside interface: Virtual-Access2 (bound to FastEthernet0/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.1.1
Mask: 255.255.255.255
```

```
Save Password: Allowed
Current EzVPN Peer: 172.18.143.246
```

ダイナミック VTI を使用した VRF 認識 IPsec：例

この例では、DVTI を利用するための VRF 認識 IPsec の設定方法を示します。

```
hostname c7206
.
.
ip vrf test-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
.
interface Virtual-Template1 type tunnel
 ip vrf forwarding test-vti1
 ip unnumbered Loopback0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
!
.
.
end
```

仮想ファイアウォールを使用したダイナミック仮想トンネル インターフェイス：例

DVTI Easy VPN サーバは、仮想ファイアウォールの背後に設定できます。Behind-the-firewall 設定を使用すれば、ユーザはネットワークに入れますが、ネットワーク ファイアウォールは不正アクセスから保護されます。仮想ファイアウォールでは、Context-Based Access Control（CBAC; コンテキストベースのアクセス制御）と、インターネット インターフェイスおよび仮想テンプレートに対して適用される NAT が使用されます。

```
hostname c7206
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
 ip access-group 100 in
 ip nat outside
!
```

```
interface GigabitEthernet0/2
 description Internal Network
 ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nat inside
 ip inspect IOSFW1 in
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny   esp any any
access-list 110 deny   udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny   udp any eq non500-isakmp any
!
end
```

QoS を使用したダイナミック仮想トンネル インターフェイス：例

サービス ポリシーを仮想テンプレートに適用することによって、QoS を DVTI トンネルに追加できます。仮想アクセス インターフェイスを作成するためにテンプレートがコピーされると、サービス ポリシーがそこで適用されます。次に、QoS が追加された DVTI 基本設定をの例を示します。

```
hostname c7206
.
.
class-map match-all VTI
 match any
!
policy-map VTI
  class VTI
  police cir 2000000
    conform-action transmit
    exceed-action drop
!
.
.
interface Virtual-Template1 type tunnel
 ip vrf forwarding test-vti1
 ip unnumbered Loopback0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
 service-policy output VTI
!
.
.
```

```
!
end
```

その他の参考資料

関連資料

内容	参照先
IPsec、セキュリティ問題	「*Configuring Security for VPNs with IPsec*」
QoS、設定	『*Cisco IOS Quality of Service Solutions Configuration Guide*』（Cisco.com）
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
VPN 設定	• 「*Cisco Easy VPN Remote*」 • 「*Easy VPN Server*」

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*The Internet Key Exchange (IKE)*』

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

IPsec 仮想トンネル インターフェイスの機能情報

表 1 は、この機能のリリース履歴です。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 1　IPsec 仮想トンネル インターフェイスの機能情報

機能名	リリース	機能設定情報
スタティック IPsec VTI	12.3(7)T 12.3(14)T 12.2(33)SRA 12.2(33)SXH	IPsec VTI（VTI）では、IPsec トンネルを終了するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。IPsec VTI によって、リモート リンクを保護するための IPsec の設定が簡素化され、マルチキャストがサポートされ、さらには、ネットワーク管理およびロード バランシングが簡単に実現できるようになります。
ダイナミック IPsec VTI	12.3(7)T 12.3(14)T	ダイナミック VTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。ダイナミック VTI によって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーを RADIUS サーバ上で設定できます。グループごとまたはユーザごとの定義を、Xauth User または Unity グループを使用して作成するか、証明書から取得できます。ダイナミック VTI は、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。IPsec ダイナミック VTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）と組み合せて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。ダイナミック VTI によって、VRF 認識 IPsec の導入が簡単になります。VRF は、インターフェイス上で設定されます。 次のコマンドが導入または変更されました。**crypto isakmp profile**、**interface virtual-template**、**show vtemplate**、**tunnel mode**、**virtual-template**