CHAPTER 25

仮想ルーティングおよび転送（VRF）モードでのバーチャル プライベート ネットワーク（VPN）の設定

この章では、Virtual Routing and Forwarding（VRF）モードで IP セキュリティ（IPSec）VPN を設定する方法について説明します。Virtual Routing and Forwarding（VRF）モードは、IPSec VPN SPA によってサポートされる 2 つの VPN 設定モードの 1 つです。もう一方の VPN モードである暗号接続モードの詳細については、第 24 章「暗号接続モードでの VPN の設定」を参照してください。

この章の内容は次のとおりです。

IPSec VPN SPA の IPSec VPN の全般的な情報については、「IPSec および IKE 設定の基本概念の概要」（P.23-4）を参照してください。

（注） この章に記載された手順は、読者がセキュリティ設定の概念（Virtual LAN（VLAN; 仮想 LAN）、Internet Security Association and Key Management Protocol（ISAKMP）ポリシー、事前共有キー、トランスフォーム セット、Access Control List（ACL; アクセス コントロール リスト）、暗号マップなど）についての知識があることを前提としています。これらの機能の設定に関する詳細は、次の Cisco IOS マニュアルを参照してください。

次の URL の『*Cisco IOS Security Configuration Guide*』*Release 12.2*
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

次の URL の『*Cisco IOS Security Command Reference*』*Release 12.2*
http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

この章で使用するコマンドの詳細については、『*Cisco 7600 Series Router Command Reference, 12.2SR*』、関連する Cisco IOS Release 12.2 ソフトウェア コンフィギュレーション ガイド、およびマスター インデックスを参照してください。これらのマニュアルの入手方法については、「関連資料」（P.li）を参照してください。

ヒント IPSec VPN SPA を使用して VPN を正しく設定するために、設定の概要および注意事項にすべて目を通してから設定作業を始めてください。

VRF モードでの VPN の設定

VRF モード（別名 VRF 対応 IPSec）を使用すると、公衆向けのアドレスを 1 つ使用して IPSec トンネルを VPN ルーティングおよび転送（VRF）インスタンスにマッピングできます。

VRF インスタンスは、Provider Edge（PE; プロバイダー エッジ）ルータに接続されたカスタマー サイトの VPN メンバーシップを定義する、VPN 単位のルーティング情報リポジトリです。VRF は IP ルーティング テーブル、派生した Cisco Express Forwarding（CEF）テーブル、フォワーディング テーブルを使用する一連のインターフェイス、およびルーティング テーブルに含まれる情報を制御する一連の規則とルーティング プロトコル パラメータで構成されます。VPN カスタマーごとに、異なるルーティング テーブルおよび CEF テーブルのセットが保持されます。

各 IPSec トンネルには、VRF ドメインが 2 つ対応付けられています。カプセル化された外部パケットは 1 つの VRF ドメイン Front Door VRF（FVRF; 前面扉 VRF）に、保護された内部 IP パケットは別のドメイン Inside VRF（IVRF; 内部 VRF）に属します。つまり、IPSec トンネルのローカル エンドポイントは FVRF に属しますが、内部パケットの送信元アドレスおよび宛先アドレスは IVRF（保護されない（LAN）側）に属します。

（注） 前面扉 VRF（FVRF）がサポートされるのは、Cisco IOS Release 12.2(33)SRA 以降です。

1 つのインターフェイスに IPSec トンネルを 1 つ以上終端できます。これらのすべてのトンネルで FVRF は同じであり、このインターフェイスに設定された VRF に設定されます。これらのトンネルの IVRF は、暗号マップ エントリに適用される ISAKMP プロファイルで定義された VRF に応じて、異なることがあります。

VRF モードでは、特定の VRF に属するパケットが IPSec 処理のために IPSec VPN SPA 経由でルーティングされます。CLI を使用して、IPSec VPN SPA に送信されるように設定されたインターフェイス VLAN に、VRF を対応付けます。VRF ごとにインターフェイス VLAN を作成する必要があります。Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）クラウド経由でインターネットに流れるパケットを内部 VRF から受信すると、インターフェイス VLAN にそのパケットがルーティングされ、IPSec VPN SPA に送信されて IPSec 処理が実行されます。IPSec VPN SPA は、特殊なレイヤ 3 VLAN に入れられるようにパケットを変更し、そのパケットは IPSec VPN SPA から発信されたあと、WAN 側のポートにルーティングされます。

crypto engine slot コマンドが入力されている保護対象ポートからインバウンド方向に流れるパケットは、特殊な ACL から IPSec VPN SPA にリダイレクトされて、パケットの IPSec ヘッダーに含まれる Security Parameter Index（SPI; セキュリティ パラメータ インデックス）に従って処理されます。IPSec VPN SPA で処理することにより、カプセル開放されたパケットが、内部 VRF に対応する適切なインターフェイス VLAN にマッピングされます。このインターフェイス VLAN は特定の VRF に対応付けられているので、パケットはその VRF 内で正しい内部インターフェイスにルーティングされます。

（注） Tunnel Protection（TP; トンネル保護）は、VRF モードでサポートされます。トンネル保護の設定については、「トンネル保護（GRE）を使用した VRF モードでの VPN の設定」（P.25-11）および「トンネル保護を使用した VRF モードの設定例」（P.25-33）を参照してください。

VRF モードを使用して VPN を設定する場合は、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用したトンネル保護（TP）、および Virtual Tunnel Interface（VTI）の追加トンネリング オプションを使用できます。これらのオプションのいずれかを指定すると、VRF（通常の VRF モード）またはグローバル コンテキストでトンネルを終端できます。

ここでは、IPSec VPN SPA に VRF モードで VPN を設定する方法について説明します。

- 「VRF モードでの VPN 設定の概要」（P.25-3）

（注） VRF モードでの VPN 設定の詳細については、次の URL にある Cisco IOS マニュアルを参照してください。
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_aware_ipsec_ps6017_TSD_Products_Configuration_Guide_Chapter.html

VRF モードでの VPN 設定の概要

従来の暗号接続モードでは、VPN を設定するには、暗号マップをインターフェイス VLAN に適用し、そのインターフェイス VLAN に物理ポートを暗号接続していました。IPSec VPN SPA を使用して VRF モードで VPN を設定する場合、インターフェイス VLAN のモデルは残されていますが、**crypto connect vlan** CLI コマンドは使用しません。特定の VRF でインターフェイスにパケットが着信したとき、そのパケットを適正なインターフェイス VLAN に送らなければなりません。特定の VRF の特定のサブネットを宛先とするパケットが、そのインターフェイス VLAN に到達するように、ルートを構築する必要があります。これは、次の設定オプションによって達成できます。

- パケットの宛先 IP アドレスと同じサブネットにあるインターフェイス VLAN 上の IP アドレスを設定します。たとえば、次のようにパケットがサブネット 10.1.1.x に送られる場合、パケットの宛先 IP アドレスは 10.1.1.1 です。

```
int vlan 100
 ip vrf forwarding coke
 ip address 10.1.1.254  255.255.255.0 <-- same subnet as 10.1.1.x that we are trying
to reach.
 crypto map mymap
 crypto engine slot 4/1
```

- 次のようにスタティック ルートを設定します。

```
ip route vrf coke 10.1.1.0 255.255.255.0 vlan 100
```

- ルーティング プロトコルを設定します。リモート ルータがルートをブロードキャストするように、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、Open Shortest Path First（OSPF）、または他のルーティング プロトコルを設定します。

  （注） トンネル保護を使用している場合以外は、ルーティング プロトコルは設定しないでください。

- Reverse Route Injection（RRI; 逆ルート注入）を設定します。RRI を設定すると、リモート側が（リモート アクセスの場合のように）IPSec セッションを開始した時点でルートが確立されます。

VRF モードでは、ルータはインターフェイス VLAN をポイントツーポイント接続と見なします。パケットはインターフェイス VLAN に直接渡されます。VRF ごとに個別のインターフェイス VLAN があります。

インターフェイス VLAN に暗号マップが適用され、**ip vrf forwarding** コマンドによってその VLAN が特定の VRF に対応付けられている場合、ソフトウェアはポイントツーポイント接続を確立し、そのインターフェイス VLAN に到達するすべてのルートが、Address Resolution Protocol（ARP; アドレス解決プロトコル）を実行しないようにします。VRF 内部での通常のルーティングにより、IPSec VPN

SPA によって処理すべきパケットは、このインターフェイス VLAN に送信されます。インターフェイス VLAN に機能を設定できます。パケットを正しくルーティングするために、インターフェイス VLAN の IP アドレスは、目的の宛先サブネットと同じサブネットに属している必要があります。

内部インターフェイスに **ip vrf forwarding** コマンドを入力すると、このインターフェイスに着信するすべてのパケットが、その VRF 内で正しくルーティングされます。

crypto engine mode vrf コマンドをイネーブルにしてインターフェイスに **crypto engine slot outside** コマンドを入力すると、特殊な ACL がインストールされます。この ACL は、システム IP アドレスに指定された着信 Encapsulating Security Payload（ESP; カプセル化セキュリティ ペイロード）/Authentication Header（AH; 認証ヘッダー）IPSec パケットを、すべて強制的に IPSec VPN SPA の WAN 側ポートに送信します。NAT Traversal（NAT-T）パケットも、この特殊な ACL によって IPSec VPN SPA に送信されます。

（注）　**vrf** *vrf_name* コマンドは、ISAKMP プロファイルのコンテキスト内部から入力する必要があります。このコマンドは、VRF 対応の暗号インフラストラクチャには適用されず、汎用的な暗号化処理だけに適用されます。ISAKMP プロファイルを暗号マップ セットに追加すると、リスト内のすべての暗号マップに対して、その VRF がデフォルトの VRF になります。このデフォルト VRF は、異なる VRF を含む別のポリシー プロファイルを指定することにより、個々の暗号マップで上書きされます。暗号マップ タグにプロファイルを適用しない場合、**ip vrf forwarding** コマンドでインターフェイスを設定していれば、そのインターフェイスから VRF が継承されます。

保護された外部インターフェイスを宛先とする、この VRF コンテキストで受信されたすべてのパケットは、対応するインターフェイス VLAN に送られます。同様に、この VRF に対応付けられたカプセル開放済みの入力パケットは、適切なインターフェイス VLAN に送られ、適切な VRF コンテキストでルーティングされるようになります。

VRF モード設定時の注意事項および制約事項

VRF モードを使用して IPSec VPN SPA の VPN を設定する場合は、次の注意事項および制約事項に従ってください。

（注）　[**no**] **crypto engine mode vrf** コマンドを使用して VRF モードをイネーブルまたはディセーブルにしたら、スーパーバイザ エンジンをリロードする必要があります。さらに、VRF モードに対して MPLS トンネル再循環をイネーブルにする必要があります。つまり、**crypto engine mode vrf** コマンドを入力する前に、**mls mpls tunnel-recir** コマンドを追加する必要があります。

- VRF モードでの VPN の設定手順は、トンネル保護を使用しているかどうかによって異なります。
- IPSec VPN SPA の暗号接続モードを設定する場合と違って、VRF モードでの VPN の設定時には **crypto connect vlan** コマンドは使用しません。
- Cisco IOS Release 12.2(33)SRA 以降のリリースでは、それまでのリリースで使用されていた **crypto engine subslot** コマンドは、**crypto engine slot** コマンド（形式は **crypto engine slot** *slot/subslot* {**inside** | **outside**}）に置き換えられました。**crypto** engine subslot コマンドはサポートされなくなりました。Cisco IOS Release 12.2(33)SRA 以降のリリースでは、**outside** キーワードを使用して **slot** *slot/subslot* 情報を指定する必要はありません。アップグレード時には、余計なメンテナンス時間がかからないように、**crypto engine** コマンドが起動コンフィギュレーション内で変更されていることを確認してください。
- Cisco IOS Release 12.2(33)SRA では、GRE にトンネル保護を設定するときの **ip vrf forwarding** コマンドは必要なくなりました。

- 暗号 ACL は、EQ 演算子だけをサポートします。GT、LT、および NEQ などの他の演算子はサポートされません。
- 次の例のように、暗号 ACL で隣接しないサブネットはサポートされません。

```
deny ip   10.0.5.0   0.255.0.255   10.0.175.0   0.255.0.255
deny ip   10.0.5.0   0.255.0.255   10.0.176.0   0.255.0.255
```

- 暗号 ACL では、ACL カウンタはサポートされません。
- 出力 ACL は、ルート プロセッサによって生成されるパケットには適用されません。入力 ACL は、ルート プロセッサを宛先とするパケットには適用されません。
- ISAKMP プロファイルを作成するとき、**vrf** コマンドの使用にあたっては次の注意事項を参考にしてください。
  - ISAKMP プロファイルを暗号マップとともに使用している場合は、**vrf** コマンドを使用する必要があります。
  - ISAKMP プロファイルをトンネル保護とともに使用している場合は、**vrf** コマンドを使用する必要はありません。
  - ISAKMP プロファイルを Dynamic Multipoint VPN（DMVPN）とともに使用している場合は、**vrf** コマンドを使用しないでください。
- **ip vrf forwarding** コマンドを VLAN に適用している場合、以前その VLAN に割り当てた既存のすべての IP アドレスは削除されます。IP アドレスを VLAN に割り当てるには、**ip vrf forwarding** コマンドの前ではなく後に **ip address** コマンドを入力します。
- Cisco IOS Release 12.2(18) SXE からは、1 つのシャーシで複数の IPSec VPN SPA がサポートされますが、VRF モードでは、複数の IPSec VPN SPA を運用する場合と単一の IPSec VPN SPA を運用する場合とで設定上の違いはありません。複数の IPSec VPN SPA を運用する場合、唯一異なる点は **show crypto vlan** コマンドの出力です。次に例を示します。

```
Interface Tu1 on IPSec Service Module port Gi7/1/1 connected to VRF vrf1
Interface VLAN 2 on IPSec Service Module port Gi7/1/1 connected to VRF vrf2
```

- ACL を入力インターフェイスに適用すると、パケット フローの妨げになります。

（注） VRF モードの設定中は、ACL を適用しないでください。

- IPSec VPN SPA がサポートする外部インターフェイスの数は、システム リソースに応じて異なります。
- VRF モードでは、同じローカル アドレスを共有する暗号マップ インターフェイスは、同じ暗号エンジンにバインドされている必要があります。
- 2 つのトンネルが同じトンネル送信元アドレスを共有する場合、次の 2 つの条件のいずれかを満たす場合に限り、IPSec VPN SPA によってテイクオーバーされます。
  - 両方のトンネルが同じ FVRF を共有する場合。
  - **crypto engine gre vpnblade** コマンドが入力されている場合。
- FVRF は IVRF と同じになるように設定できます。
- VRF モードでは、入力 ACL は暗号エンジンの外部インターフェイスに設定します。これらの ACL を他の設定済み ACL と併用すると、ACL-TCAM が過剰使用になることがあります。TCAM の使用を減らすには、コンフィギュレーションに **mls acl tcam share-global** コマンドを入力して TCAM リソースを共有します。ACL の使用状況を表示するには、**show tcam counts** コマンドを使用します。

VRF モードでサポートされる機能およびサポートされない機能

VRF モードでサポートされる機能およびサポートされない機能については、「IPsec 機能のサポート」（P.23-7）を参照してください。詳細は次のとおりです。

- 以下を使用する、VRF（プロバイダー エッジ（PE））へのリモート アクセス
  - 暗号マップを使用する逆ルート注入（RRI）のみ
  - Proxy Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）（1 つの VRF が専用 AAA にプロキシされる）
- 以下を使用するトンネル保護を適用した、Customer Edge-Provider Edge（CE-PE）暗号化
  - CE 間でのルーティング アップデートの伝播
  - PE と CE の間での Interior Gateway Protocol（IGP）/External BGP（eBGP; 外部 BGP）ルーティング アップデートの伝播

トンネル保護を使用しない VRF モードでの VPN の設定

暗号マップを使用し、トンネル保護を使用しないで VRF モードで VPN を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# mls mpls tunnel-recir`	トンネル MPLS 再循環をイネーブルにします。
ステップ 2	`Router(config)# crypto engine mode vrf`	IPSec VPN SPA で VRF モードをイネーブルにします。 （注）　**crypto engine mode vrf** コマンドを使用して VRF モードをイネーブルまたはディセーブルにしたら、スーパーバイザ エンジンをリロードする必要があります。
ステップ 3	`Router(config)# ip vrf` *vrf-name*	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 4	`Router(config-vrf)# rd` *route-distinguisher*	VRF のルーティング テーブルおよびフォワーディング テーブルを作成します。 • *route-distinguisher*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。
ステップ 5	`Router(config-vrf)# route-target export` *route-target-ext-community*	指定した VRF のエクスポート ルート ターゲット拡張コミュニティのリストを作成します。 • *route-target-ext-community*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。ステップ 4 で指定した *route-distinguisher* 値を入力します。

	コマンド	説明
ステップ 6	`Router(config-vrf)# route-target import route-target-ext-community`	指定した VRF のインポート ルート ターゲット拡張コミュニティのリストを作成します。 • *route-target-ext-community*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。ステップ 4 で指定した *route-distinguisher* 値を入力します。
ステップ 7	`Router(config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 8	`Router(config)# crypto keyring keyring-name [vrf fvrf-name]`	Internet Key Exchange（IKE; インターネット キー エクスチェンジ）認証時に使用する暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。 • *keyring-name*：暗号キーリングの名前。 • *fvrf-name*：（任意）キーリングの参照先となる前面扉仮想ルーティングおよび転送（FVRF）名。fvrf-name は、仮想ルーティングおよび転送（VRF）設定中に定義された FVRF 名と一致する必要があります。
ステップ 9	`Router(config-keyring)# pre-shared-key {address address [mask] | hostname hostname} key key`	IKE 認証に使用する事前共有キーを定義します。 • *address* [*mask*]：リモート ピアの IP アドレスまたはサブネットおよびマスク • *hostname*：ピアの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名） • *key*：秘密鍵を指定します。
ステップ 10	`Router(config-keyring)# exit`	キーリング コンフィギュレーション モードを終了します。
ステップ 11	`Router(config)# crypto ipsec transform-set transform-set-name transform1[transform2[transform3]]`	トランスフォーム セット（セキュリティ プロトコルとアルゴリズムの可能な組み合わせ）を定義し、暗号トランスフォーム コンフィギュレーション モードを開始します。 • *transform-set-name*：トランスフォーム セットの名前。 • *transform1*[*transform2*[*transform3*]]：IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。指定できる値については、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 12	`Router(config-crypto-trans)# exit`	暗号トランスフォーム コンフィギュレーション モードを終了します。

	コマンド	説明
ステップ 13	`Router(config)# crypto isakmp policy priority`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。 • *priority*：IKE ポリシーを指定し、このポリシーにプライオリティを割り当てます。1 ～ 10,000 の整数を使用します。プライオリティは 1 が最高、10,000 が最低です。
ステップ 14	`Router(config-isakmp)# authentication pre-share`	IKE ポリシーを使用する認証方式を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。
ステップ 15	`Router(config-isakmp)# lifetime seconds`	IKE Security Association（SA; セキュリティ アソシエーション）のライフタイムを指定します。 • *seconds*：各 SA が期限切れになるまでの秒数。60 ～ 86,400 の整数を使用します。デフォルトは 86,400 秒（1 日）です。
ステップ 16	`Router(config-isakmp)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了します。
ステップ 17	`Router(config)# crypto isakmp profile profile-name`	ISAKMP プロファイルを定義し、ISAKMP プロファイル コンフィギュレーション モードを開始します。 • *profile-name*：ユーザ プロファイルの名前。
ステップ 18	`Router(config-isa-prof)# vrf ivrf`	IPSec トンネルがマッピングされる VRF を定義します。 • *ivrf*：IPSec トンネルにマッピングする VRF の名前。ステップ 3 で指定した値と同じ値を入力します。
ステップ 19	`Router(config-isa-prof)# keyring keyring-name`	ISAKMP プロファイル内にキーリングを設定します。 • *keyring-name*：キーリング名。この名前は、グローバル コンフィギュレーションで定義したキーリング名と同じである必要があります。ステップ 8 で指定した値を入力します。
ステップ 20	`Router(config-isa-prof)# match identity address address [mask] [vrf]`	ピアからのアイデンティティを ISAKMP プロファイルと照合します。 • *address* [*mask*]：リモート ピアの IP アドレスまたはサブネットおよびマスク • [*vrf*]：（任意）この引数が必要になるのは、前面扉 VRF（FVRF）を設定する場合だけです。この引数は、アドレスが FVRF インスタンスであることを指定します。
ステップ 21	`Router(config-isa-prof)# exit`	ISAKMP プロファイル コンフィギュレーション モードを終了します。

	コマンド	説明
ステップ 22	`Router(config)# access list access-list-number {deny | permit} ip host source host destination`	拡張 IP アクセス リストを定義します。 • *access-list-number*：アクセス リストの番号。100 ～ 199 または 2,000 ～ 2,699 の範囲の 10 進数です。 • {**deny** | **permit**}：条件が満たされた場合にアクセスを拒否または許可します。 • *source*：パケットの送信元ホストの番号。 • *destination*：パケットの宛先ホストの番号。
ステップ 23	`Router(config)# crypto map map-name seq-number ipsec-isakmp`	暗号マップ エントリを作成または修正し、暗号マップ コンフィギュレーション モードを開始します。 • *map-name*：暗号マップ セットの識別名。 • *seq-number*：暗号マップ エントリに割り当てるシーケンス番号。値が小さいほどプライオリティが高くなります。 • **ipsec-isakmp**：IKE を使用して IPSec セキュリティ アソシエーションを確立することを表します。
ステップ 24	`Router(config-crypto-map)# set peer {hostname | ip-address}`	暗号マップ エントリで IPSec ピアを指定します。 • {*hostname* | *ip-address*}：—IPSec ピアのホスト名または IP アドレス。ステップ 20 で指定した値を入力します。
ステップ 25	`Router(config-crypto-map)# set transform-set transform-set-name`	暗号マップ エントリとともに使用するトランスフォーム セットを指定します。 • *transform-set-name*：トランスフォーム セットの名前。ステップ 11 で指定した値を入力します。
ステップ 26	`Router(config-crypto-map)# set isakmp-profile profile-name`	ISAKMP プロファイル名を設定します。 • *profile-name*：ISAKMP プロファイルの名前。ステップ 17 で入力した値を入力します。
ステップ 27	`Router(config-crypto-map)# match address [access-list-id | name]`	暗号マップ エントリに対応する拡張アクセス リストを指定します。 • *access-list-id*：拡張アクセス リストを名前または番号で指定します。ステップ 22 で指定した値を入力します。 • *name*：（任意）名前付きの暗号化アクセス リストを識別します。この名前は、照合中の名前付き暗号化アクセス リストの name 引数と一致する必要があります。
ステップ 28	`Router(config-crypto-map)# exit`	暗号マップ コンフィギュレーション モードを終了します。

	コマンド	説明
ステップ 29	`Router(config)# crypto map map-name local-address interface-id`	IPSec トラフィックを識別するために暗号マップが使用するインターフェイスを指定し、名前を付けます。 • *map-name*：暗号マップ セットの識別名。ステップ 23 で指定した値を入力します。 • **local address** *interface-id*：ルータのローカル アドレスを持つインターフェイスの名前 **（注）** ローカル アドレスは FVRF に属している必要があります。 **（注）** VRF モードでは、VPN 機能は最大 1024 のローカル アドレスをサポートします。これはシャーシ内での限度です（VPN モジュール単位ではなく）。
ステップ 30	`Router(config)# interface fastethernet slot/port`	ファスト イーサネット インターフェイスを設定し、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 31	`Router(config-if)# ip vrf forwarding vrf-name`	インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name*：VRF に割り当てられた名前。ステップ 3 で指定した値を入力します。
ステップ 32	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 33	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 34	`Router(config-if)# interface gigabitethernet slot/subslot/port`	ギガビット イーサネット インターフェイスを設定します。ステップ 29 で指定した *interface-id* の値と一致させます。
ステップ 35	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 36	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 37	`Router(config-if)# crypto engine slot slot/subslot outside`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot/subslot*：slot は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 38	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 39	`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。

	コマンド	説明
ステップ 40	`Router(config)# interface vlan-id`	VLAN インターフェイスを設定し、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。 • *vlan-id* : VLAN の識別子
ステップ 41	`Router(config-if)# ip vrf forwarding vrf-name`	インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name* : VRF に割り当てられた名前。ステップ 3 で指定した値を入力します。
ステップ 42	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* : IP アドレス。 • *mask* : サブネット マスク。
ステップ 43	`Router(config-if)# crypto map map-name`	事前に定義した暗号マップ セットをインターフェイスに適用します。 • *map-name* : 暗号マップ セットの識別名。ステップ 23 で指定した値を入力します。
ステップ 44	`Router(config-if)# crypto engine slot slot/subslot inside`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot/subslot* : slot は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 45	`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 46	`Router(config)# ip route vrf vrf-name prefix mask interface-number`	VRF のスタティック ルートを確立します。 • *vrf-name* : スタティック ルートに対応する VRF の名前。ステップ 3 で指定した値を入力します。 • *prefix* : 宛先の IP ルート プレフィクス（ドット区切り 10 進フォーマット） • *mask* : 宛先のプレフィクス マスク（ドット区切り 10 進フォーマット） • *interface-number* : 使用するネットワーク インターフェイスの識別番号。ステップ 40 で指定した *vlan-id* 値を入力します。
ステップ 47	`Router(config)# end`	特権 EXEC モードに戻ります。

VRF 対応 IPSec に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_aware_ipsec_ps6017_TSD_Products_Configuration_Guide_Chapter.html

設定例は、「VRF モードの基本的な設定例」（P.25-23）を参照してください。

トンネル保護（GRE）を使用した VRF モードでの VPN の設定

ここでは、トンネル保護（TP）を使用して、VRF モードで VPN を設定する方法について説明します。トンネル保護は VRF モードでの GRE トンネリングです。

IPSec を設定する際には、インターフェイスに暗号マップを適用して IPSec をイネーブルにします。トンネル保護を使用すると、インターフェイスに暗号マップまたは ACL を適用する必要はありません。トンネル インターフェイスに直接、暗号ポリシーが適用されます。インターフェイスでルーティングされるすべてのトラフィックは GRE でカプセル化され、それから IPSec を使用して暗号化されます。トンネル保護機能は、Point-to-Point（p2p; ポイントツーポイント）GRE に適用できます。

トンネル保護を使用した VRF モード設定時の注意事項および制約事項

IPSec VPN SPA でトンネル保護を設定する場合は、次の注意事項および制約事項に従ってください。

- IPSec VPN SPA が GRE トンネルを占有する妨げになるオプション（シーケンス番号、トンネル キーなど）は設定しないでください。
- GRE トンネルのキープアライブ機能は設定しないでください。
- GRE トンネル インターフェイスに適用する際、**ip tcp adjust-mss** コマンドは無視されます。代わりに、コマンドを入力 LAN インターフェイスに適用します （CSCsl27876）。
- VRF モードでの GRE トラフィックの保護に、暗号マップを使用しないでください。
- 暗号マップ インターフェイスとトンネル保護インターフェイス（VTI または GRE/TP）が同じ外部インターフェイスを共有する場合、両者は同じローカル送信元アドレスを共有できません。
- 暗号化後のフラグメンテーションを避けるため、トンネル IP MTU を、入力インターフェイス MTU から GRE と IPSec の負荷を差し引いた値と同等以下に設定します。出力インターフェイス MTU は、すべてのアクティブな暗号外部インターフェイスの最小 MTU である必要があります。

トンネル保護を使用して VRF モードで VPN を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# mls mpls tunnel-recir`	トンネル MPLS 再循環をイネーブルにします。
ステップ 2	`Router(config)# crypto engine mode vrf`	IPSec VPN SPA で VRF モードをイネーブルにします。 （注）　**crypto engine mode vrf** コマンドを使用して VRF モードをイネーブルまたはディセーブルにしたら、スーパーバイザ エンジンをリロードする必要があります。
ステップ 3	`Router(config)# ip vrf` *vrf-name*	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 4	`Router(config-vrf)# rd` *route-distinguisher*	VRF のルーティング テーブルおよびフォワーディング テーブルを作成します。 • *route-distinguisher*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。

	コマンド	説明
ステップ 5	`Router(config-vrf)# route-target export route-target-ext-community`	指定した VRF のエクスポート ルート ターゲット拡張コミュニティのリストを作成します。 • *route-target-ext-community*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。ステップ 4 で指定した *route-distinguisher* 値を入力します。
ステップ 6	`Router(config-vrf)# route-target import route-target-ext-community`	指定した VRF のインポート ルート ターゲット拡張コミュニティのリストを作成します。 • *route-target-ext-community*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。ステップ 4 で指定した *route-distinguisher* 値を入力します。
ステップ 7	`Router(config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 8	`Router(config)# crypto keyring keyring-name [vrf fvrf-name]`	IKE 認証時に使用する暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。 • *keyring-name*：暗号キーリングの名前。 • *fvrf-name*：（任意）キーリングの参照先となる前面扉仮想ルーティングおよび転送（FVRF）名。*fvrf-name* は、仮想ルーティングおよび転送（VRF）設定中に定義された FVRF 名と一致する必要があります。
ステップ 9	`Router(config-keyring)# pre-shared-key {address address [mask] | hostname hostname} key key`	IKE 認証に使用する事前共有キーを定義します。 • *address* [*mask*]：リモート ピアの IP アドレスまたはサブネットおよびマスク • *hostname*：ピアの完全修飾ドメイン名 • *key*：秘密鍵を指定します。
ステップ 10	`Router(config-keyring)# exit`	キーリング コンフィギュレーション モードを終了します。
ステップ 11	`Router(config)# crypto ipsec transform-set transform-set-name transform1[transform2[transform3]]`	トランスフォーム セット（セキュリティ プロトコルとアルゴリズムの可能な組み合わせ）を定義し、暗号トランスフォーム コンフィギュレーション モードを開始します。 • *transform-set-name*：トランスフォーム セットの名前。 • *transform1*[*transform2*[*transform3*]]：IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。指定できる値については、『*Cisco IOS Security Command Reference*』を参照してください。

	コマンド	説明
ステップ 12	`Router(config-crypto-trans)# exit`	暗号トランスフォーム コンフィギュレーション モードを終了します。
ステップ 13	`Router(config)# crypto isakmp policy priority`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。 • *priority*：IKE ポリシーを指定し、このポリシーにプライオリティを割り当てます。1 ～ 10,000 の整数を使用します。プライオリティは 1 が最高、10,000 が最低です。
ステップ 14	`Router(config-isakmp)# authentication pre-share`	IKE ポリシーを使用する認証方式を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。
ステップ 15	`Router(config-isakmp)# lifetime seconds`	IKE SA のライフタイムを指定します。 • *seconds*：各 SA が期限切れになるまでの秒数。60 ～ 86,400 の整数を使用します。デフォルトは 86,400 秒（1 日）です。
ステップ 16	`Router(config-isakmp)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了します。
ステップ 17	`Router(config)# crypto isakmp profile profile-name`	ISAKMP プロファイルを定義し、ISAKMP プロファイル コンフィギュレーション モードを開始します。 • *profile-name*：ユーザ プロファイルの名前。
ステップ 18	`Router(config-isa-prof)# keyring keyring-name`	ISAKMP プロファイル内にキーリングを設定します。 • *keyring-name*：キーリング名。この名前は、グローバル コンフィギュレーションで定義したキーリング名と同じである必要があります。ステップ 8 で指定した値を入力します。
ステップ 19	`Router(config-isa-prof)# match identity address address [mask]`	ピアからのアイデンティティを ISAKMP プロファイルと照合します。 • *address* [*mask*]：リモート ピアの IP アドレスまたはサブネットおよびマスク
ステップ 20	`Router(config-isa-prof)# exit`	ISAKMP プロファイル コンフィギュレーション モードを終了します。
ステップ 21	`Router(config)# access list access-list-number {deny | permit} ip host source host destination`	拡張 IP アクセス リストを定義します。 • *access-list-number*：アクセス リストの番号。100 ～ 199 または 2,000 ～ 2,699 の範囲の 10 進数です。 • {**deny** | **permit**}：条件が満たされた場合にアクセスを拒否または許可します。 • *source*：パケットの送信元ホストの番号。 • *destination*：パケットの宛先ホストの番号。
ステップ 22	`Router(config)# crypto ipsec profile profile-name`	IPSec プロファイルを定義し、IPSec プロファイル コンフィギュレーション モードを開始します。 • *profile-name*：ユーザ プロファイルの名前。

	コマンド	説明
ステップ 23	`Router(config-ipsec-profile)# set transform-set transform-set-name`	暗号マップ エントリとともに使用するトランスフォーム セットを指定します。 • *transform-set-name*：トランスフォーム セットの名前。ステップ 11 で指定した値を入力します。
ステップ 24	`Router(config-ipsec-profile)# set isakmp-profile profile-name`	ISAKMP プロファイル名を設定します。 • *profile-name*：ISAKMP プロファイルの名前。ステップ 17 で入力した値を入力します。
ステップ 25	`Router(config-ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーション モードを終了します。
ステップ 26	`Router(config)# interface tunnel-number`	トンネル インターフェイスを設定し、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。 • *tunnel-number*：トンネル インターフェイスに割り当てられた名前
ステップ 27	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name*：VRF に割り当てられた名前。ステップ 3 で指定した値を入力します。
ステップ 28	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 29	`Router(config-if)# tunnel source ip-address`	トンネル インターフェイスの送信元アドレスを設定します。 • *ip-address*：トンネル内のパケットの送信元アドレスとして使用する IP アドレス。
ステップ 30	`Router(config-if)# tunnel vrf vrf-name`	（任意）特定のトンネル宛先、インターフェイス、またはサブインターフェイスに VPN ルーティングおよび転送（VRF）インスタンスを関連付けます。この手順が必要になるのは、前面扉 VRF（FVRF）を設定する場合だけです。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 31	`Router(config-if)# tunnel destination ip-address`	トンネル インターフェイスの宛先アドレスを設定します。 • *ip-address*：トンネル内のパケットの宛先アドレスとして使用する IP アドレス
ステップ 32	`Router(config-if)# tunnel protection ipsec crypto-policy-name`	トンネル インターフェイスを IPSec プロファイルに対応付けます。 • *crypto-policy-name*：ステップ 22 で指定した値
ステップ 33	`Router(config-if)# crypto engine slot slot/subslot inside`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot/subslot*：slot は IPSec VPN SPA が搭載されたスロットを入力します。

	コマンド	説明
ステップ 34	`Router(config-if)# interface fastethernet slot/subslot`	ファスト イーサネット インターフェイスを設定します。
ステップ 35	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 36	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 37	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 38	`Router(config-if)# interface type slot/subslot/port`	物理出力インターフェイスを設定します。
ステップ 39	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 40	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address*：IP アドレス。ステップ 29 で指定した値を入力します。 • *mask*：サブネット マスク。
ステップ 41	`Router(config-if)# crypto engine slot slot/subslot outside`	インターフェイスに暗号エンジンを割り当てます。 • *slot/subslot*：slot は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 42	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 43	`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。

設定例は、「トンネル保護を使用した VRF モードの設定例」（P.25-33）を参照してください。

IPSec Virtual Tunnel Interface（VTI）の設定

IPSec Virtual Tunnel Interface（VTI）は、IPSec トンネルを終端するためのルーティング可能なインターフェイス タイプを提供します。この VTI を使用すると、リモート アクセスを保護する必要がある場合に設定プロセスが大幅に簡素化され、GRE トンネルや暗号マップを IPSec と併用する代わりの簡単な方法になります。また、IPSec VTI により、ネットワーク管理およびロード バランシングも簡単に実行できるようになります。

（注）　IPSec VTI は、Cisco IOS Release 12.2(33)SRA 以降のリリースでサポートされており、暗号接続モードではサポートされません。

IPSec VTI のルーティングおよびトラフィック暗号化に関する次の詳細事項に留意してください。

- トンネル インターフェイス上でルーティング プロトコルをイネーブルにして、仮想トンネルでルーティング情報を伝搬できます。ルータは Virtual Tunnel Interface を介してネイバー関係を確立できます。標準ベース IPSec インストールとの相互運用性を実現するには、IP ANY ANY プロキシを使用します。スタティック IPSec インターフェイスは、IP ANY ANY プロキシとネゴシエーションして、これを受け入れます。
- IPSec VTI はネイティブ IPSec トンネリングをサポートし、物理インターフェイスのほとんどのプロパティを公開します。
- IPSec VTI の場合、トンネル内で暗号化が発生します。トラフィックはトンネル インターフェイスに転送されるときに、暗号化されます。トラフィック転送は IP ルーティング テーブルで処理されます。ダイナミックまたはスタティック IP ルーティングを使用すると、トラフィックを Virtual Tunnel Interface にルーティングできます。IP ルーティングを使用してトラフィックを暗号化すると、ネイティブ IPSec 設定において暗号マップと ACL を併用する必要がなくなるため、IPSec VPN の設定が簡素化されます。IPSec VTI を使用すると、Network Address Translation（NAT; ネットワーク アドレス変換）、ACL、および Quality Of Service（QoS）を個別に適用したり、これらをクリア テキスト、暗号化テキスト、あるいは両方に適用することができます。暗号マップを使用した場合は、強制暗号化機能を簡単に指定できません。

IPSec Virtual Tunnel Interface の設定時の注意事項および制約事項

IPSec VTI を設定する場合は、次の注意事項および制約事項に従ってください。

- VTI トンネルは、VRF（通常の VRF モード）またはグローバル コンテキストで終端できます（トンネル インターフェイスで **ip vrf forwarding** コマンドは使用しません）。
- サポートされているのは、スタティック VTI だけです。
- サポートされているのは、strict IP ANY ANY プロキシだけです。
- IPSec トランスフォーム セットを設定する必要があるのは、トンネル モードの場合だけです。
- IKE セキュリティ アソシエーション（SA）は Virtual Tunnel Interface にバインドされます。そのため、同じ IKE SA を暗号マップに使用できません。
- **mls mpls tunnel-recir** コマンドを VTI コンフィギュレーションに適用している場合、1 つの予約 VLAN が各トンネルに割り当てられます。その結果、VTI トンネル数は最大制限値の 1000 になります。
- さまざまな方法で IPSec を実装できる GRE トンネルと異なり、IPSec Virtual Tunnel Interface は IP ユニキャストに限定されます。
- VTI を介したマルチキャストは、ルーティング プロトコル アップデートなどのコントロール プレーン トラフィックを除いて、サポートされません。

IPSec スタティック トンネルの設定

スタティック IPSec Virtual Tunnel Interface を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# mls mpls tunnel-recir`	トンネル MPLS 再循環をイネーブルにします。
ステップ 2	`Router(config)# crypto engine mode vrf`	IPSec VPN SPA で VRF モードをイネーブルにします。 （注）　**crypto engine mode vrf** コマンドを使用して VRF モードをイネーブルまたはディセーブルにしたら、スーパーバイザ エンジンをリロードする必要があります。
ステップ 3	`Router(config)# ip vrf vrf-name`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 4	`Router(config-vrf)# rd route-distinguisher`	VRF のルーティング テーブルおよびフォワーディング テーブルを作成します。 • *route-distinguisher*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。
ステップ 5	`Router(config-vrf)# route-target export route-target-ext-community`	指定した VRF のエクスポート ルート ターゲット拡張コミュニティのリストを作成します。 • *route-target-ext-community*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。ステップ 4 で指定した *route-distinguisher* 値を入力します。
ステップ 6	`Router(config-vrf)# route-target import route-target-ext-community`	指定した VRF のインポート ルート ターゲット拡張コミュニティのリストを作成します。 • *route-target-ext-community*：Autonomous System Number（ASN）と任意の番号（101:3 など）または IP アドレスと任意の番号（192.168.122.15:1 など）を指定します。ステップ 4 で指定した *route-distinguisher* 値を入力します。
ステップ 7	`Router(config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。

	コマンド	説明
ステップ 8	`Router(config)# crypto keyring keyring-name [vrf fvrf-name]`	IKE 認証時に使用する暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。 • *keyring-name*：暗号キーリングの名前。 • *fvrf-name*：（任意）キーリングの参照先となる前面扉仮想ルーティングおよび転送（FVRF）名。*fvrf-name* は、仮想ルーティングおよび転送（VRF）設定中に定義された FVRF 名と一致する必要があります。
ステップ 9	`Router(config-keyring)# pre-shared-key {address address [mask] | hostname hostname} key key`	IKE 認証に使用する事前共有キーを定義します。 • *address* [*mask*]：リモート ピアの IP アドレスまたはサブネットおよびマスク • *hostname*：ピアの完全修飾ドメイン名 • *key*：秘密鍵を指定します。
ステップ 10	`Router(config-keyring)# exit`	キーリング コンフィギュレーション モードを終了します。
ステップ 11	`Router(config)# crypto ipsec transform-set transform-set-name transform1[transform2[transform3]]`	トランスフォーム セット（セキュリティ プロトコルとアルゴリズムの可能な組み合わせ）を定義し、暗号トランスフォーム コンフィギュレーション モードを開始します。 • *transform-set-name*：トランスフォーム セットの名前。 • *transform1*[*transform2*[*transform3*]]：IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。指定できる値については、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 12	`Router(config-crypto-trans)# exit`	暗号トランスフォーム コンフィギュレーション モードを終了します。
ステップ 13	`Router(config)# crypto isakmp policy priority`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。 • *priority*：IKE ポリシーを指定し、このポリシーにプライオリティを割り当てます。1 ～ 10,000 の整数を使用します。プライオリティは 1 が最高、10,000 が最低です。
ステップ 14	`Router(config-isakmp)# authentication pre-share`	IKE ポリシーを使用する認証方式を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。
ステップ 15	`Router(config-isakmp)# lifetime seconds`	IKE SA のライフタイムを指定します。 • *seconds*：各 SA が期限切れになるまでの秒数。60 ～ 86,400 の整数を使用します。デフォルトは 86,400 秒（1 日）です。
ステップ 16	`Router(config-isakmp)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了します。

	コマンド	説明
ステップ 17	`Router(config)# crypto ipsec profile profile-name`	IPSec プロファイルを定義し、IPSec プロファイル コンフィギュレーション モードを開始します。IPSec プロファイルは、2 つの IPSec ルータ間での IPSec 暗号化に使用される IP セキュリティ（IPSec）パラメータを定義します。 • *profile-name*：ユーザ プロファイルの名前。
ステップ 18	`Router(config-ipsec-profile)# set transform-set transform-set-name [transform-set-name2 ...transform-set-name6]`	暗号マップ エントリとともに使用するトランスフォーム セットを指定します。 • *transform-set-name*：トランスフォーム セットの名前。
ステップ 19	`Router(config)# interface type slot/[subslot]/port`	インターフェイス タイプを設定します。 • *type*：設定するインターフェイスのタイプ。 • *slot*/[*subslot*]/*port*：設定するスロット、サブスロット（省略可能）、およびポートの番号。
ステップ 20	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 21	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 22	`Router(config-if)# tunnel mode ipsec ipv4`	トンネル モードを IPSec として、トランスポートを IPv4 として定義します。
ステップ 23	`Router(config-if)# tunnel source ip-address`	トンネル インターフェイスの送信元アドレスを設定します。 • *ip-address*：トンネル内のパケットの送信元アドレスとして使用する IP アドレス。
ステップ 24	`Router(config-if)# tunnel destination ip-address`	トンネル インターフェイスの宛先アドレスを設定します。 • *ip-address*：トンネル内のパケットの宛先アドレスとして使用する IP アドレス
ステップ 25	`Router(config-if)# tunnel vrf vrf-name`	（任意）特定のトンネル宛先に VPN ルーティングおよび転送インスタンス（VRF）を関連付けます。この手順が必要になるのは、前面扉 VRF（FVRF）を設定する場合だけです。 • *vrf-name*：VRF に割り当てられた名前。
ステップ 26	`Router(config-if)# tunnel protection ipsec profile name`	トンネル インターフェイスを IPSec プロファイルに対応付けます。 • *name*：IPSec プロファイルの名前。この値は、ステップ 1 で **crypto ipsec profile** コマンドで指定した値と同じである必要があります。

	コマンド	説明
ステップ 27	`Router(config-if)# crypto engine slot slot/subslot inside`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot/subslot* : slot は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 28	`Router(config-if)# interface type slot/subslot/port`	物理出力インターフェイスを設定します。
ステップ 29	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name* : VRF に割り当てられた名前。
ステップ 30	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* : IP アドレス。ステップ 23 で指定した値を入力します。 • *mask* : サブネット マスク。
ステップ 31	`Router(config-if)# crypto engine outside`	インターフェイスに暗号エンジンを割り当てます。
ステップ 32	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 33	`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。

IPSec Virtual Tunnel Interface の設定の確認

IPSec Virtual Tunnel Interface の設定が正しく機能していることを確認するには、**show interfaces tunnel**、**show crypto session**、および **show ip route** コマンドを使用します。

show interfaces tunnel コマンドはトンネル インターフェイス情報、**show crypto session** コマンドはアクティブな暗号セッションのステータス情報、**show ip route** コマンドはルーティング テーブルの現在の状態を表示します。

次の出力では、Tunnel 0 およびライン プロトコルが「up」状態です。ライン プロトコルが「down」状態の場合、セッションは非アクティブです。

```
Router1# show interfaces 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

Router1# 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

Router1# 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
```

IPSec Virtual Tunnel Interface の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtIPSctm.html

IPSec Virtual Tunnel Interface の設定例については、「IPSec Virtual Tunnel Interfaces の設定例」（P.25-36）を参照してください。

グローバル コンテキストでの VTI の設定

Cisco IOS Release 12.2(33)SRA 以降のリリースでは、VRF を設定しなくても IPSec VTI を設定できます。VRF モードは **crypto engine mode vrf** コマンドを使用してグローバルに設定する必要がありますが、VRF ではなくグローバル コンテキストでトンネルを終端できます。

グローバル コンテキストでの VTI の設定手順は、**ip vrf forwarding** *vrf-name* コマンドおよび **tunnel vrf** *vrf-name* コマンドが必要ないことを除き、「IPSec スタティック トンネルの設定」（P.25-18）の IPSec VTI の手順と類似しています。

グローバル コンテキストでの IPSec VTI の設定例は、「IPSec Virtual Tunnel Interfaces の設定例」（P.25-36）を参照してください。

設定例

ここでは、VRF モードの設定例を示します。

- 「VRF モードの基本的な設定例」（P.25-23）
- 「Easy VPN を使用した VRF モードでのリモート アクセスの設定例」（P.25-26）

- 「VRF モード PE の設定例」（P.25-29）
- 「VRF モード カスタマー エッジ（CE）の設定例」（P.25-31）
- 「トンネル保護を使用した VRF モードの設定例」（P.25-33）
- 「VRF モードでの IP マルチキャストの設定例」（P.25-34）
- 「IPSec Virtual Tunnel Interfaces の設定例」（P.25-36）

（注）　**ip vrf forwarding** コマンドを VLAN に適用している場合、以前その VLAN に割り当てた既存のすべての IP アドレスは削除されます。IP アドレスを VLAN に割り当てるには、**ip vrf forwarding** コマンドの前ではなく後に **ip address** コマンドを入力します。

（注）　次に、Cisco IOS Release 12.2(33)SRA のレベルでコマンドを使用する例を示します。

Cisco IOS Release 12.2(33)SRA 以降のリリースでは、それまでのリリースで使用されていた **crypto engine subslot** コマンドは、**crypto engine slot** コマンド（形式は **crypto engine slot** *slot/subslot* {**inside** | **outside**}）に置き換えられました。**crypto** engine subslot コマンドはサポートされなくなりました。アップグレード時には、余計なメンテナンス時間がかからないように、このコマンドが起動コンフィギュレーション内で変更されていることを確認してください。

VRF モードの基本的な設定例

次に、VRF モードを使用した IPSec VPN SPA の基本的な設定例を示します。

ルータ 1 の設定

```
hostname router-1
!
ip vrf ivrf
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto engine mode vrf
!
vlan 2,3
!
crypto keyring key0
  pre-shared-key address 11.0.0.2 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
!
crypto isakmp profile prof1
   vrf ivrf
   keyring key0
   match identity address 11.0.0.2 255.255.255.255
!
!
crypto ipsec transform-set proposal1  esp-3des esp-sha-hmac
!
crypto map testtag local-address Vlan3
```

```
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.2
 set transform-set proposal1
 set isakmp-profile prof1
 match address 101
!
interface GigabitEthernet1/1
 !switch inside port
 ip vrf forwarding ivrf
 ip address 12.0.0.1 255.255.255.0
!
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 3
 switchport mode access
!
interface GigabitEthernet4/0/1
 !IPSec VPN SPA inside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 !IPSec VPN SPA outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip vrf forwarding ivrf
 ip address 13.0.0.252 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0 inside
!
interface Vlan3
 ip address 11.0.0.1 255.255.255.0
 crypto engine slot 4/0 outside
!
access-list 101 permit ip host 12.0.0.2 host 13.0.0.2
```

ルータ 2 の設定

```
hostname router-2
!
ip vrf ivrf
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto engine mode vrf
```

```
!
vlan 2,3
!
crypto keyring key0
  pre-shared-key address 11.0.0.1 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
!
crypto isakmp profile prof1
   vrf ivrf
   keyring key0
   match identity address 11.0.0.1 255.255.255.255
!
!
crypto ipsec transform-set proposal1  esp-3des esp-sha-hmac
!
crypto map testtag local-address Vlan3
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set proposal1
 set isakmp-profile prof1
 match address 101
!
interface GigabitEthernet1/1
 !switch inside port
 ip vrf forwarding ivrf
 ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 switchport
 switchport access vlan 3
 switchport mode access
!
interface GigabitEthernet4/0/1
 !IPSec VPN SPA inside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 !IPSec VPN SPA outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip vrf forwarding ivrf
 ip address 12.0.0.252 255.255.255.0
 crypto map testtag
 crypto engine slot 4/0 inside
```

```
!
interface Vlan3
 ip address 11.0.0.2 255.255.255.0
 crypto engine slot 4/0 outside
!
access-list 101 permit ip host 13.0.0.2 host 12.0.0.2
```

Easy VPN を使用した VRF モードでのリモート アクセスの設定例

次に、Easy VPN を使用したリモート アクセスに関する VRF モードの設定例を示します（最初に RADIUS 認証を使用し、次にローカル認証を使用）。

RADIUS 認証の使用

```
aaa group server radius acs-vrf1
 server-private 192.1.1.251 auth-port 1812 acct-port 1813 key allegro
 ip vrf forwarding vrf1
!
aaa authentication login test_list group acs-vrf1
aaa authorization network test_list group acs-vrf1
aaa accounting network test_list start-stop group acs-vrf1
!
ip vrf ivrf
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2

crypto isakmp client configuration group test
 key world
 pool pool1
!
crypto isakmp profile test_pro
   vrf ivrf
   match identity group test
   client authentication list test_list
   isakmp authorization list test_list
   client configuration address respond
   accounting test_list
crypto ipsec transform-set t3 esp-3des esp-sha-hmac
!
crypto dynamic-map remote 1
 set transform-set t3
 set isakmp-profile test_pro
 reverse-route
!
!
crypto map map-ra local-address GigabitEthernet2/1
crypto map map-ra 10 ipsec-isakmp dynamic remote
!
interface GigabitEthernet2/1
  mtu 9216
 ip address 120.0.0.254 255.255.255.0
 ip flow ingress
```

```
 logging event link-status
 mls qos trust ip-precedence
 crypto engine slot 1/0 outside
!
interface GigabitEthernet1/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos trust ip-precedence
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet1/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos trust ip-precedence
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!

interface Vlan100
 ip vrf forwarding vrf1
 ip address 120.0.0.100 255.255.255.0
 no mop enabled
 crypto map map-ra
 crypto engine slot 1/0 inside

ip local pool pool1 100.0.1.1 100.0.5.250
```

ローカル認証の使用

```
username t1 password 0 cisco
aaa new-model
!
aaa authentication login test_list local
aaa authorization network test_list local
!
aaa session-id common
!
ip vrf ivrf
 rd 1:2
 route-target export 1:2
 route-target import 1:2


!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group test
 key world
 pool pool1
crypto isakmp profile test_pro
```

```
   vrf ivrf
   match identity group test
   client authentication list test_list
   isakmp authorization list test_list
   client configuration address respond
   accounting test_list
crypto ipsec transform-set t3 esp-3des esp-sha-hmac
!
crypto dynamic-map remote 10
 set transform-set t3
 set isakmp-profile test_pro
 reverse-route

!
!
crypto map map-ra local-address GigabitEthernet2/1
crypto map map-ra 11 ipsec-isakmp dynamic remote
!
!

!
interface GigabitEthernet2/1
  mtu 9216
 ip address 120.0.0.254 255.255.255.0
 ip flow ingress
 logging event link-status
 mls qos trust ip-precedence
 crypto engine slot 1/0 outside
!
!
interface GigabitEthernet1/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos trust ip-precedence
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet1/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos trust ip-precedence
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan100
 ip vrf forwarding ivrf
 ip address 120.0.0.100 255.255.255.0
 ip flow ingress
 crypto map map-ra
 crypto engine slot 1/0 inside
!
!
ip local pool pool1 100.0.1.1 100.0.5.250
```

VRF モード PE の設定例

次に、プロバイダー エッジ（PE）に関する VRF モードの設定例を示します。

```
!
version 12.2
!
hostname EXAMPLE-PE
!
no aaa new-model
ip subnet-zero
!
ip vrf vrf1
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto engine mode vrf
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
crypto keyring key0
  pre-shared-key address 11.0.0.1 key mykey
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 lifetime 500
crypto isakmp profile prof1
   vrf vrf1
   keyring key0
   self-identity user-fqdn a@example.com
   match identity address 11.0.0.1 255.255.255.255
!
crypto ipsec transform-set proposal1 ah-sha-hmac esp-3des esp-sha-hmac
!
crypto map testtag local-address Vlan3
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set security-association lifetime seconds 1000
 set transform-set proposal1
 set pfs group2
 set isakmp-profile prof1
 match address 101
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
```

```
 switchport
 switchport access vlan 3
 switchport mode access
 no ip address
!
interface GigabitEthernet1/14
 ip vrf forwarding vrf1
 ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet6/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet7/1
 no ip address
 shutdown
!
interface GigabitEthernet7/2
 ip address 17.1.5.4 255.255.0.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip vrf forwarding vrf1
 ip address 12.0.0.252 255.255.255.0
 crypto map testtag
 crypto engine subslot 6/0
!
interface Vlan3
 ip address 11.0.0.2 255.255.255.0
 crypto engine subslot 6/0
!
ip classless
ip route 223.255.254.0 255.255.255.0 17.1.0.1
!
no ip http server
!
access-list 101 permit ip host 13.0.0.2 host 12.0.0.2
!
control-plane
!
dial-peer cor custom
!
```

```
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
end
```

VRF モード カスタマー エッジ（CE）の設定例

次に、Customer Edge（CE; カスタマー エッジ）に関する VRF モードの設定例を示します。

```
!
version 12.2
!
hostname EXAMPLE-CE
!
no aaa new-model
ip subnet-zero
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
!
power redundancy-mode combined
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 lifetime 500
crypto isakmp key mykey address 11.0.0.2
!
crypto ipsec transform-set proposal1 ah-sha-hmac esp-3des esp-sha-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.2
 set security-association lifetime seconds 1000
 set transform-set proposal1
 set pfs group2
 match address 101
!
interface GigabitEthernet1/1
 ip address 12.0.0.1 255.255.255.0
 load-interval 30
 no keepalive
!
interface GigabitEthernet1/2
 switchport
 switchport access vlan 3
 switchport mode access
 no ip address
!
interface GigabitEthernet5/2
 ip address 17.1.5.3 255.255.0.0
 media-type rj45
```

```
!
interface GigabitEthernet6/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 11.0.0.1 255.255.255.0
 no mop enabled
 crypto map testtag
 crypto engine subslot 6/0
!
interface Vlan3
 no ip address
 crypto connect vlan 2
!
ip classless
ip route 13.0.0.0 255.0.0.0 11.0.0.2
ip route 223.255.254.0 255.255.255.0 17.1.0.1
!
no ip http server
```

```
!
access-list 101 permit ip host 12.0.0.2 host 13.0.0.2
!
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
end
```

トンネル保護を使用した VRF モードの設定例

次に、トンネル保護を使用した VRF モードの設定例を示します。

```
ip vrf coke
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto keyring key1
 pre-shared-key address 100.1.1.1 key happy-eddie
!
crypto isakmp policy 1
 authentication pre-share

crypto isakmp profile prof1
 keyring key1
 match identity address 100.1.1.1 255.255.255.255
!
crypto ipsec transform-set TR esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile tp
 set transform-set TR
 set isakmp-profile prof1
!
!
crypto engine mode vrf
!
interface Tunnel1
 ip vrf forwarding coke
 ip address 10.1.1.254 255.255.255.0
 tunnel source 172.1.1.1
 tunnel destination 100.1.1.1
 tunnel protection ipsec profile tp
 crypto engine slot 4/0 inside
!
interface GigabitEthernet4/0/1
 !IPSec VPN SPA inside port
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
```

```
!
interface GigabitEthernet4/0/2
 !IPSec VPN SPA outside port
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1
 ip address 172.1.1.1 255.255.255.0
 crypto engine slot 4/0 outside
!
interface FastEthernet7/13
 ip vrf forwarding coke
 ip address 13.1.1.2 255.255.255.0
!
ip route 100.1.1.1 255.255.255.255 Tunnel1
```

VRF モードでの IP マルチキャストの設定例

（注）　Cisco 7600 SSC-400 に IPSec VPN SPA が 2 つあり、コンフィギュレーションに **hw-module slot** *X* **subslot** *Y* **only** が含まれている場合、1 つはシャットダウンされます。この場合、サブスロット Y の IPSec VPN SPA がアクティブで、もう一方のサブスロットの IPSec VPN SPA がディセーブルになります。

次の例は、GRE トンネルを介して IP マルチキャストを設定する方法を示しています。

```
hostname router-1
!
ip vrf ivrf
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
!
!
ip multicast-routing vrf ivrf
!
crypto engine mode vrf
!
!
hw-module slot 4 subslot 0 only
!
crypto keyring key1
  pre-shared-key address 11.0.0.0 255.0.0.0 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp profile isa_prof
   keyring key1
   match identity address 11.0.0.0 255.0.0.0
```

```
!
crypto ipsec transform-set proposal esp-3des
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set proposal
 set isakmp-profile isa_prof
!
!
!
interface Tunnel1
 ip vrf forwarding ivrf
 ip address 20.1.1.1 255.255.255.0
 ip mtu 9216
 ip hold-time eigrp 1 3600
 ip pim sparse-mode
 tunnel source 1.0.1.1
 tunnel destination 11.1.1.1
 tunnel protection ipsec profile vpnprof
 crypto engine slot 4/0 inside
!
interface Loopback1
 ip address 1.0.1.1 255.255.255.0
!
interface GigabitEthernet1/1
 mtu 9216
 ip vrf forwarding ivrf
 ip address 50.1.1.1 255.0.0.0
 ip pim sparse-mode
!
interface GigabitEthernet1/2
 mtu 9216
 ip address 9.1.1.1 255.255.255.0
 crypto engine slot 4/0 outside
!
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
router eigrp 1
 !
 address-family ipv4 vrf ivrf
  autonomous-system 1
  network 20.1.1.0 0.0.0.255
  network 50.1.1.0 0.0.0.255
  no auto-summary
  no eigrp log-neighbor-changes
```

```
 exit-address-family
!
router ospf 1
 log-adjacency-changes
 network 1.0.0.0 0.255.255.255 area 0
 network 9.0.0.0 0.255.255.255 area 0
!
ip pim vrf ivrf rp-address 50.1.1.1
!
```

IPSec Virtual Tunnel Interfaces の設定例

次に、VTI を使用した VRF モードの設定例を示します。

- 「IPSec Virtual Tunnel Interface FVRF の設定例」（P.25-36）
- 「グローバル コンテキストでの IPSec Virtual Tunnel Interface の設定例」（P.25-38）

IPSec Virtual Tunnel Interface FVRF の設定例

次に、FVRF VTI コンフィギュレーションの設定例を示します。

```
hostname router-1
!
!
ip vrf fvrf
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf ivrf
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto engine mode vrf
!
crypto keyring key1 vrf fvrf
  pre-shared-key address 11.1.1.1 key cisco47
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
!
crypto isakmp profile isa_prof
   keyring key1
   match identity address 11.1.1.1 255.255.255.255 fvrf

crypto ipsec transform-set proposal esp-3des esp-sha-hmac
!
!
crypto ipsec profile vpnprof
 set transform-set proposal
 set isakmp-profile isa_prof
!
!
!
!
!
```

```
interface Tunnel1
 ip vrf forwarding ivrf
 ip address 20.1.1.1 255.255.255.0
 ip pim sparse-mode
 ip ospf network broadcast
 ip ospf priority 2
 tunnel source 1.0.0.1
 tunnel destination 11.1.1.1
 tunnel mode ipsec ipv4
 tunnel vrf fvrf
 tunnel protection ipsec profile vpnprof
 crypto engine slot 4/0 inside
!
interface Loopback1
 ip vrf forwarding fvrf
 ip address 1.0.0.1 255.255.255.0
!
interface GigabitEthernet1/1
 !switch inside port
 ip vrf forwarding ivrf
 ip address 50.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
 ip vrf forwarding fvrf
 ip address 9.1.1.1 255.255.255.0
 crypto engine slot 4/0 outside
!
interface GigabitEthernet4/0/1
 !IPSec VPN SPA inside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 !IPSec VPN SPA outside port
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
router ospf 1 vrf ivrf
 log-adjacency-changes
 network 20.1.1.0 0.0.0.255 area 0
 network 21.1.1.0 0.0.0.255 area 0
 network 50.0.0.0 0.0.0.255 area 0
!
ip classless
ip route vrf fvrf 11.1.1.0 255.255.255.0 9.1.1.254
```

グローバル コンテキストでの IPSec Virtual Tunnel Interface の設定例

次に、グローバル コンテキストでの IPSec VTI の設定例を示します。

```
!
crypto engine mode vrf
!
crypto keyring key1
  pre-shared-key address 14.0.0.2 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share

!
crypto isakmp profile prof1
   keyring key1
   match identity address 14.0.0.2 255.255.255.255
!
crypto ipsec transform-set t-set1 esp-3des esp-sha-hmac
!
crypto ipsec profile prof1
 set transform-set t-set1
 set isakmp-profile prof1
!
!
interface Tunnel1
 ip address 122.0.0.2 255.255.255.0
 tunnel source 15.0.0.2
 tunnel destination 14.0.0.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof1
 crypto engine slot 2/0 inside
!
interface Loopback2
 ip address 15.0.0.2 255.255.255.0
!

interface GigabitEthernet1/3
 ip address 172.2.1.1 255.255.255.0
 crypto engine slot 2/0 outside
!
interface GigabitEthernet2/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet2/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
```

```
!
ip route 14.0.0.0 255.0.0.0 172.2.1.2
ip route 172.0.0.0 255.0.0.0 172.2.1.2
```