CHAPTER 31

IPSec VPN SPA を使用した重複ハードウェアおよび IPSec フェールオーバーの設定

この章では、Cisco 7600 シリーズ ルータ上の IPSec VPN SPA を使用して重複ハードウェアおよび IPSec フェールオーバーを設定する方法について説明します。具体的な内容は次のとおりです。

システム イメージおよびコンフィギュレーション ファイルの管理については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』Release 12.2 および『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。

Cisco IOS の IPSec 暗号化処理およびポリシーについての詳細は、『*Cisco IOS Security Configuration Guide, Release 12.2*』および『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

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*』を参照してください。また、関連する Cisco IOS Release 12.2 ソフトウェア コマンド リファレンスおよびマスター インデックスも参照してください。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。

重複ハードウェア構成および IPSec フェールオーバーの概要

重要な VPN 通信のために、冗長 VPN ハードウェアを導入し、ハードウェア障害が発生したときのためにフェールオーバーを設定できます。ここでは、IPSec VPN SPA を使用した IP セキュリティ フェールオーバーの設定に関する情報を説明します。

シャーシに搭載した複数の IPSec VPN SPA の設定

1 つのシャーシには、暗号接続モードの場合は最大 10 個の IPSec VPN SPA を搭載できます。ただし、いずれのインターフェイス VLAN に対しても、IP セキュリティ サービスを実行できる IPSec VPN SPA は 1 つだけです。

シャーシに搭載した複数の IPSec VPN SPA の設定に関する注意事項

1 つのシャーシに搭載した複数の IPSec VPN SPA を設定する場合は、次の注意事項に従ってください。

- **no switchport** コマンドに続いて **switchport** コマンドを入力すると、すべての VLAN が再度トランク ポートに追加されます（この状況は、最初にルーテッド ポートに切り替え、そのあとスイッチ ポートに戻した場合に該当します）。トランク ポートの設定についての詳細は、「トランク ポートの設定」（P.24-14）を参照してください。
- IPSec VPN SPA を 1 つだけ搭載する場合と同じように、各 IPSec VPN SPA の内部ポートおよび外部ポートを適切に設定する必要があります。インターフェイス VLAN を追加できるのは、1 つの IPSec VPN SPA の内部ポートだけです。複数の IPSec VPN SPA の内部ポートに、同じインターフェイス VLAN を追加しないでください。

  IPSec VPN SPA の内部ポートへインターフェイス VLAN を割り当てることによって、特定のインターフェイス VLAN に IPSec サービスを提供する IPSec VPN SPA を決定できます。

  （注）　IPSec VPN SPA の内部トランク ポートにインターフェイス VLAN を追加する場合、個別に指定する必要はありません。**crypto engine slot** コマンドで、同じ結果が得られます。

  （注）　1 つのインターフェイス VLAN に対する IPSec 処理の実行は、1 つの IPSec VPN SPA でしかサポートされません。

- Security Association（SA）ベースのロード バランシングはサポートされません。
- 同じ暗号マップを複数のインターフェイスに割り当てる場合、**crypto map local address** コマンドを使用し、すべてのインターフェイスを同じ暗号エンジンに割り当てる必要があります。

シャーシでの複数の IPSec VPN SPA 設定例は、「シャーシに搭載した複数の IPSec VPN SPA の設定例」（P.31-24）を参照してください。

HSRP を使用するステートレス フェールオーバーについて

IPSec フェールオーバー（VPN ハイ アベイラビリティ）機能により、アクティブ ルータに障害が発生した場合にプライマリ（アクティブ）ルータのタスクを自動的にテイクオーバーするセカンダリ（スタンバイ）ルータを配置できます。IPSec ステートレス フェールオーバーまたは IPSec ステートフル フェールオーバーは、Hot Standby Routing Protocol（HSRP）と Reverse Route Injection（RRI）との組み合わせで動作するよう、設計されています。

HSRP はステートレス モードまたはステートフル モードのアクティブおよびスタンバイ ルータ間で使用しされます。HSRP はルータ インターフェイスの状態を追跡し、プライマリ デバイスとセカンダリ デバイスとの間のフェールオーバー メカニズムを提供します。HSRP グループは 1 つの仮想 IP アドレスを暗号ピア アドレスとして共有し、フェールオーバー後にリモート暗号ピアで再設定を行わなくてもよいようにします。設定された HSRP タイマーによって、スタンバイ ルータがテイクオーバーするのにかかる時間が決定されます。

RRI ではネゴシエートされた IPSec SA から取得した情報を使用して、これらの SA で識別されたネットワークへのスタティック ルートを作成します。HSRP および IPSec フェールオーバー中、RRI によりダイナミック ルーティング情報の更新を行うことができます。

IPSec ステートレス フェールオーバーでは、HSRP グループの仮想 IP アドレスがスタンバイ ルータに転送されますが、IPSec または ISAKMP SA ステート情報はスタンバイ ルータに転送されません。リモート暗号ピアは、Dead Peer Detection（DPD）またはキープアライブ メカニズムを使用して障害を検出します。リモート暗号ピアは HSRP グループ アドレスでスタンバイ ルータと通信し、トラフィックの伝送をレジュームする前に、ドロップされた ISAKMP SA および IPSec SA と再ネゴシエーションします。

一緒に使用すると、HSRP および RRI は、信頼性のあるネットワーク設定を VPN に提供し、リモートピアでの設定の複雑さを軽減します。

HSRP 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/ipapp/configuration/guide/ipapp_hsrp_ps6922_TSD_Products_Configuration_Guide_Chapter.html

HSRP および SSP を使用するステートフル フェールオーバーについて

（注）　Cisco IOS Release 12.2(33)SRA 以降では、HSRP と SSP を使用した IPSec ステートフル フェールオーバーをサポートしなくなりました。Release 12.2SXF ではこの機能がサポートされています。

IPSec ステートフル フェールオーバーにより、ルータは予定内または予定外の停止後に IPSec パケットの処理および転送を継続できます。フェールオーバー処理はユーザおよびリモート IPSec ピアに対して透過的に行われます。

IPSec ステートレス フェールオーバーと同様、IPSec ステートフル フェールオーバーは HSRP および RRI を使用するように設計されていますが、IPSec ステートフル フェールオーバーは SSP も使用します。HSRP および IPSec フェールオーバー中、SSP はアクティブおよびスタンバイ ルータ間で IPSec および ISAKMP SA ステート情報を転送し、ルータのフェールオーバー後に既存の VPN 接続が維持されるようにします。

IPSec ステートフル フェールオーバーの設定時の注意事項および制約事項

IPSec ステートフル フェールオーバーを設定する場合は、次の注意事項および制約事項に従ってください。

- IPSec VPN SPA で IPSec ステートフル フェールオーバーを設定するときは、すべての IPSec VPN SPA の設定が適用されることに注意してください。暗号マップをインターフェイス VLAN に適用する必要があります。
- IPSec ステートフル フェールオーバーを 2 つのシャーシの IPSec VPN SPA で設定するとき、両方のシャーシのハードウェア コンフィギュレーションがまったく同じ状態になっている必要があることに注意します。たとえば、1 つのシャーシでスロット 2 にある IPSec VPN SPA がインターフェイス VLAN 100 の保護に使用されていて、スロット 3 にある IPSec VPN SPA が VLAN 101 の保護に使用されている場合、2 番めのシャーシでも同一のコンフィギュレーションが反映されている必要があります。2 番めのシャーシのスロット 3 にある IPSec VPN SPA がインターフェイス VLAN 100 の保護に使用されている場合が、設定ミスの例です。
- 存在しない、または適切でない設定の HSRP スタンバイ グループを State Synchronization Protocol（SSP）の設定に追加しないでください。このアクションを行うと、コンフィギュレーションが修正されるまでハイ アベイラビリティ機能がディセーブルになります。
- HSRP タイマーの推奨値は、hello タイマーで 1 秒、ホールド タイマーで 3 秒です。これらの値であれば、一時的なネットワーク輻輳または CPU の高負荷によって引き起こされる、望ましくないフェールオーバーを防ぐことができます。

  これらのタイマー値は、高負荷で実行していたり、多数の HSRP があったりする場合、上方修正できます。一時的な障害および負荷に関連するシステムの安定性は、必要に応じてタイマー値を上げることで確実に影響を受けます。hello タイマー値は、ホールド タイマー値のおよそ 1/3 です。
- デバイスがハイ アベイラビリティ ペアとして関与する前に、起動、初期化、および同期化を完了できるようにするには、HSRP 「遅延」タイマーを使用します。アクティブ/スタンバイ フラッピングを避けるには「最小」遅延を 30 秒以上に設定し、「リロード」遅延は最小遅延より大きい値に設定します。遅延タイマーを使用して、さまざまなハードウェアの特定の設定の複雑性およびサイズを反映できます。遅延タイマーは、プラットフォームごとに異なる傾向があります。
- シーケンス番号は、SA ごとに 20 秒の最小間隔で、アクティブからスタンバイに更新されます。
- **standby preempt** コマンドが必要で、**priority** オプションまたは **delay** オプションで、設定する必要があります。
- HSRP および IPSec フェールオーバー中に、ダイナミック ルーティング情報の更新を行うには、**reverse-route** コマンドを使用して RRI 機能をイネーブルにします。
- HSRP および IPSec ステートフル フェールオーバーの両方をイネーブルにしたあと、すべてのプロセスが正常に実行されていることを確認するには、**show ssp** コマンド、**show standby** コマンド、**show crypto ipsec** コマンド、および **show crypto isakmp** コマンドを使用します。
- 次の機能は、IPSec ステートフル フェールオーバーではサポートされません。
  - **standby use-bia** コマンド：ルータの Media Access Control（MAC; メディア アクセス制御）アドレスには、常に仮想 HSRP MAC アドレスを使用してください。
  - Easy VPN クライアントまたは IKE キープアライブ：IPSec ステートフル フェールオーバーは、DPD 使用時にはピアとともに使用できます。
  - DMVPN またはトンネル保護。
  - セキュリティ保護された WAN ポート（IPSec over FlexWAN または SIP モジュール ポート アダプタなど）：この制約事項は、HSRP の制限によるものです。

IPSec フェールオーバーの設定

次に、暗号接続モードおよび VRF モードでの IPSec ステートレスおよびステートフル フェールオーバーの設定方法について説明します。

暗号接続モードで HSRP を使用した IP ステートレス フェールオーバーの設定

HSRP および SSP を使用して IP ステートフル フェールオーバーを設定するには、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)# **crypto isakmp policy** *priority* ... Router(config-isakmp) # **exit**	ISAKMP 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。 ISAKMP ポリシーの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。
ステップ 2	Router(config)# **crypto isakmp key** *keystring* **address** *peer-address*	事前共有認証キーを設定します。 • *keystring*：事前共有キー。 • *peer-address*：リモート ピアの IP アドレス。 事前共有キーの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。
ステップ 3	Router(config)# **crypto ipsec transform-set** *transform-set-name transform1*[*transform2*[*transform3*]] ... Router(config-crypto-tran)# **exit**	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。 許容される *transformx* 値、およびトランスフォーム セットの設定についての詳細は、『*Cisco IOS Security Command Reference*』を参照してください。

	コマンド	説明
ステップ 4	`Router(config)# access-list access-list-number {deny | permit} ip source source-wildcard destination destination-wildcard`	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。 • **ip** *source*：パケットの送信元ホストのアドレス。 • *source-wildcard*：送信元アドレスに適用されるワイルドカード ビット。 • *destination*：パケットの宛先ホストのアドレス。 • *destination-wildcard*：宛先アドレスに適用されるワイルドカード ビット。 アクセス リストの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。

ステップ 5	`Router(config)# crypto dynamic-map dynamic-map-name seq-number ipsec-isakmp`
	`...`
	`Router(config-crypto-map)# exit`
		ダイナミック暗号マップ テンプレート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。
		• *dynamic-map-name*：ダイナミック暗号マップ テンプレートの識別名。
		• *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 SA を確立することを表します。
		暗号マップの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。

ステップ 6	`Router(config)# crypto map map-name seq-number ipsec-isakmp dynamic dynamic-map-name`	暗号マップ エントリを作成し、ダイナミック暗号マップ テンプレートにバインドします。 • *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 SA を確立することを表します。 • *dynamic-map-name*：ダイナミック暗号マップ テンプレートの識別名。
ステップ 7	`Router(config-if)# interface gigabitethernet slot/subslot/port`	LAN 側ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンド	説明
ステップ 8	`Router(config-if)# ip address address mask`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 9	`Router(config-if)# standby [group-number] ip ip-address`	HSRP をイネーブルにします。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。デフォルト値は 0 です。グループ番号の範囲は、HSRP バージョン 1 では 0 ～ 255、HSRP バージョン 2 では 0 ～ 4,095 です。 • *ip-address*：（任意）スタンバイ ルータ インターフェイスの IP アドレス。
ステップ 10	`Router(config-if)# standby [group-number] timers [msec] hellotime [msec] holdtime`	他のルータによってアクティブ ルータのダウンが宣言されるまでの、hello パケットの間隔およびホールド タイムを設定します。 • *group-number*：（任意）タイマーを適用するグループ番号。 • **msec**：（任意）インターバルをミリ秒単位で指定します。ミリ秒単位のタイマーを使用すると、より迅速なフェールオーバーが可能になります。 • *hellotime*：hello インターバル（秒）。1 ～ 254 の整数を使用します。デフォルトは 3 秒です。**msec** オプションを指定する場合、*hellotime* はミリ秒単位で、15 ～ 999 の整数を使用します。 • *holdtime*：アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒）。x ～ 255 の整数を使用します。デフォルトは 10 秒です。**msec** オプションを指定する場合、*holdtime* はミリ秒単位で指定し、y ～ 3,000 の整数を使用します。

	コマンド	説明
ステップ 11	`Router(config-if)# standby [group-number] [priority priority] preempt [delay [minimum | sync] seconds]`	アクティブ ルータの選択に使用されるスタンバイ プライオリティを設定します。 • *group-number*：（任意）プライオリティを適用するグループ番号。 • *priority*：（任意）プライオリティ値は 1 ～ 255 の範囲で、1 が最低、255 が最高のプライオリティを表します。プライオリティが指定されていると、ローカル ルータのプライオリティが現在のアクティブ ルータより高い場合には、そのローカル ルータがアクティブ ルータとなるように要求が出されます。 • **delay**：ホット スタンバイ ルータがプリエンプション処理を行ってアクティブ ルータになるまでのプリエンプション遅延を指定します。 • **minimum**：（任意）最小の遅延時間（秒）を指定します。 • **sync**：（任意）IP 冗長クライアントの最大の同期化時間（秒）を指定します。 • *seconds*：（任意）ローカル ルータが最後に再起動されてからの最少秒数を指定し、その間はアクティブ ルータのテイクオーバーを延期させます。範囲は 0 ～ 3,600 秒（1 時間）で、デフォルトは 0 秒（遅延なし）です。
ステップ 12	`Router(config-if)# standby [group-number] track type number [interface-priority]`	インターフェイスが他のインターフェイスを追跡し、いずれかの他のインターフェイスがダウンした場合に、デバイスのホット スタンバイ プライオリティを下げるように設定します。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。 • *type*：追跡するインターフェイス タイプ（インターフェイス番号と組み合わせて使用）。 • *number*：追跡するインターフェイス番号（インターフェイス タイプと組み合わせて使用）。 • *interface-priority*：（任意）インターフェイスがダウンした場合（または再度アップになった場合）に、ルータのホット スタンバイ プライオリティの減算値（または加算値）を指定します。範囲は 0 ～ 255 です。デフォルトは 10 です。
ステップ 13	`Router(config-if)# standby [group-number] name`	インターフェイスのスタンバイ グループ名を設定します。 • *group-number*：（任意）名前を適用するグループ番号。 • *name*：HSRP スタンバイ グループの名前。

	コマンド	説明
ステップ 14	`Router(config-if)# interface vlan vlan_ID`	指定した暗号インターフェイス VLAN のインターフェイス コンフィギュレーション モードを開始します。
ステップ 15	`Router(config-if)# ip address address mask`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。 • *address* : IP アドレス。 • *mask* : サブネット マスク。
ステップ 16	`Router(config-if)# standby [group-number] ip ip-address`	HSRP をイネーブルにします。 • *group-number* :（任意）HSRP をアクティブにするインターフェイスのグループ番号。デフォルト値は 0 です。グループ番号の範囲は、HSRP バージョン 1 では 0 ～ 255、HSRP バージョン 2 では 0 ～ 4,095 です。 • *ip-address* :（任意）HSRP スタンバイ グループの仮想 IP アドレス。
ステップ 17	`Router(config-if)# standby [group-number] timers [msec] hellotime [msec] holdtime`	他のルータによってアクティブ ルータのダウンが宣言されるまでの、hello パケットの間隔およびホールド タイムを設定します。 • *group-number* :（任意）タイマーを適用するグループ番号。 • **msec** :（任意）インターバルをミリ秒単位で指定します。ミリ秒単位のタイマーを使用すると、より迅速なフェールオーバーが可能になります。 • *hellotime* : hello インターバル（秒）。1 ～ 254 の整数を使用します。デフォルトは 3 秒です。**msec** オプションを指定する場合、*hellotime* はミリ秒単位で、15 ～ 999 の整数を使用します。 • *holdtime* : アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒）。x ～ 255 の整数を使用します。デフォルトは 10 秒です。**msec** オプションを指定する場合、*holdtime* はミリ秒単位で指定し、y ～ 3,000 の整数を使用します。

	コマンド	説明
ステップ 18	`Router(config-if)# standby [group-number] [priority priority] preempt [delay [minimum | sync] seconds]`	アクティブ ルータの選択に使用されるスタンバイ プライオリティを設定します。 • *group-number*：（任意）プライオリティを適用するグループ番号。 • *priority*：（任意）プライオリティ値は 1 ～ 255 の範囲で、1 が最低、255 が最高のプライオリティを表します。プライオリティが指定されていると、ローカル ルータのプライオリティが現在のアクティブ ルータより高い場合には、そのローカル ルータがアクティブ ルータとなるように要求が出されます。 • **delay**：（任意）ホット スタンバイ ルータがプリエンプション処理を行ってアクティブ ルータになるまでのプリエンプション遅延を指定します。 • **minimum**：（任意）最小の遅延時間（秒）を指定します。 • **sync**：（任意）IP 冗長クライアントの最大の同期化時間（秒）を指定します。 • *seconds*：（任意）ローカル ルータが最後に再起動されてからの最少秒数を指定し、その間はアクティブ ルータのテイクオーバーを延期させます。範囲は 0 ～ 3,600 秒（1 時間）で、デフォルトは 0 秒（遅延なし）です。
ステップ 19	`Router(config-if)# standby [group-number] track type number [interface-priority]`	インターフェイスが他のインターフェイスを追跡し、いずれかの他のインターフェイスがダウンした場合に、デバイスのホット スタンバイ プライオリティを下げるように設定します。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。 • *type*：追跡するインターフェイス タイプ（インターフェイス番号と組み合わせて使用）。 • *number*：追跡するインターフェイス番号（インターフェイス タイプと組み合わせて使用）。 • *interface-priority*：（任意）インターフェイスがダウンした場合（または再度アップになった場合）に、ルータのホット スタンバイ プライオリティの減算値（または加算値）を指定します。範囲は 0 ～ 255 です。デフォルトは 10 です。
ステップ 20	`Router(config-if)# standby [group-number] name`	インターフェイスのスタンバイ グループ名を設定します。 • *group-number*：（任意）名前を適用するグループ番号。 • *name*：スタンバイ ルータの名前。

	コマンド	説明
ステップ 21	`Router(config-if)# crypto map map-name redundancy name`	バックアップ IPSec ピアを定義します。スタンバイ グループにある両方のルータは、冗長スタンバイ名で定義され、同じ仮想 IP アドレスを共有します。 • *map_name*：暗号マップ セットの名前。 • *name*：HSRP スタンバイ グループの名前。
ステップ 22	`Router(config-if)# crypto engine slot slot`	内部インターフェイス VLAN に暗号エンジンを割り当てます。 • *slot*：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 23	`Router(config-if)# interface gigabitethernet slot/subslot/port`	外部ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 24	`Router(config-if)# crypto connect vlan vlan_ID`	外部アクセス ポートを内部インターフェイス VLAN に接続し、暗号接続モードを開始します。 • *vlan_ID*：インターフェイス VLAN の識別子。

HSRP による IPSec ステートレス フェールオーバーの設定例は、「暗号接続モードで HSRP を使用した IPSec ステートレス フェールオーバーの設定例」（P.31-27）を参照してください。

暗号接続モードで HSRP と SSP を使用した IP ステートフル フェールオーバーの設定

HSRP を使用した IPSec ステートフル フェールオーバーの設定は、HSRP および SSP 関連コマンドを使用した IPSec ステートレス フェールオーバーの設定と非常によく似ています。

HSRP および SSP を使用して IP ステートフル フェールオーバーを設定するには、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)# ssp group group`	ハイ アベイラビリティ（HA）情報を通信し、SSP コンフィギュレーション モードを開始するために使用されるチャネルを示します。 • *group*：1 ～ 100 の間の整数。
ステップ 2	`Router(config-ssp)# redundancy name`	HSRP グループを特定します。 • *name*：有効な IP 冗長性グループ名。
ステップ 3	`Router(config-ssp)# remote ipaddr`	HA 送信を受け取るピアを特定します。 • *ipaddr*：スタンバイ ルータの IP アドレス。

	コマンド	説明
ステップ 4	Router(config)# **crypto isakmp policy** *priority* ... Router(config-isakmp) # **exit**	ISAKMP 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。 ISAKMP ポリシーの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。
ステップ 5	Router(config)# **crypto isakmp key** *keystring* **address** *peer-address*	事前共有認証キーを設定します。 • *keystring*：事前共有キー。 • *peer-address*：リモート ピアの IP アドレス。 事前共有キーの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。
ステップ 6	Router(config)# **crypto isakmp ssp** *id*	ID で説明される SSP チャネルで転送される ISAKMP ステートをイネーブルにします。この機能がディセーブルになっている場合、スタンバイ ルータのその ID にバインドされたすべての休止 SA エントリが削除され、新しいステート エントリが追加されることはありません。 • *id*：SA エントリの転送に使用するチャネル。
ステップ 7	Router(config)# **crypto ipsec transform-set** *transform-set-name transform1*[*transform2*[*transform3*]] ... Router(config-crypto-tran)# **exit**	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。 許容される *transformx* 値、およびトランスフォーム セットの設定についての詳細は、『*Cisco IOS Security Command Reference*』を参照してください。

	コマンド	説明
ステップ 8	`Router(config)# crypto map name ha replay-interval inbound inbound-interval outbound outbound-interval`	（任意）アクティブ スイッチがスタンバイ スイッチに対し、アンチリプレイ シーケンス番号を更新する間隔を指定します。 • *name*：コンフィギュレーションで説明される暗号マップのタグ名。 • *inbound-interval*：アクティブ スイッチが着信パケットのパケット シーケンス アップデートを送信する間隔。範囲は 0 ～ 10000（パケット）で、デフォルトは 1000 です。 • *outbound-interval*：アクティブ スイッチが送信パケットのパケット シーケンス アップデートを送信する間隔。範囲は 1 ～ 10（単位は 100 万パケット）で、デフォルトは 1 です。
ステップ 9	`Router(config)# access-list access-list-number {deny | permit} ip source source-wildcard destination destination-wildcard`	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アドレス。 • *source-wildcard*：送信元アドレスに適用されるワイルドカード ビット。 • *destination*：パケットの宛先ホストのアドレス。 • *destination-wildcard*：宛先アドレスに適用されるワイルドカード ビット。 アクセス リストの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。

ステップ 10	`Router(config)# crypto dynamic-map dynamic-map-name seq-number ipsec-isakmp`
	`...`
	`Router(config-crypto-map)# exit`
		ダイナミック暗号マップ テンプレート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。
		• *dynamic-map-name*：ダイナミック暗号マップ テンプレートの識別名。
		• *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 SA を確立することを表します。
		暗号マップの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。

	コマンド	説明
ステップ 11	`Router(config)# crypto map map-name seq-number ipsec-isakmp dynamic dynamic-map-name`	暗号マップ エントリを作成し、ダイナミック暗号マップ テンプレートにバインドします。 • *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 SA を確立することを表します。 • *dynamic-map-name*：ダイナミック暗号マップ テンプレートの識別名。
ステップ 12	`Router(config-if)# interface gigabitethernet slot/subslot/port`	LAN 側ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 13	`Router(config-if)# ip address address mask`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 14	`Router(config-if)# standby [group-number] ip ip-address`	HSRP をイネーブルにします。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。デフォルト値は 0 です。グループ番号の範囲は、HSRP バージョン 1 では 0 ～ 255、HSRP バージョン 2 では 0 ～ 4,095 です。 • *ip-address*：（任意）HSRP スタンバイ グループの仮想 IP アドレス。
ステップ 15	`Router(config-if)# standby [group-number] timers [msec] hellotime [msec] holdtime`	他のルータによってアクティブ ルータのダウンが宣言されるまでの、hello パケットの間隔およびホールド タイムを設定します。 • *group-number*：（任意）タイマーを適用するグループ番号。 • **msec**：（任意）インターバルをミリ秒単位で指定します。ミリ秒単位のタイマーを使用すると、より迅速なフェールオーバーが可能になります。 • *hellotime*：hello インターバル（秒）。1 ～ 254 の整数を使用します。デフォルトは 3 秒です。**msec** オプションを指定する場合、*hellotime* はミリ秒単位で、15 ～ 999 の整数を使用します。 • *holdtime*：アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒）。x ～ 255 の整数を使用します。デフォルトは 10 秒です。**msec** オプションを指定する場合、*holdtime* はミリ秒単位で指定し、y ～ 3,000 の整数を使用します。

	コマンド	説明
ステップ 16	`Router(config-if)# standby [group-number] [priority priority] preempt [delay [minimum | sync] seconds]`	アクティブ ルータの選択に使用されるスタンバイ プライオリティを設定します。 • *group-number*：（任意）プライオリティを適用するグループ番号。 • *priority*：（任意）プライオリティ値は 1 ～ 255 の範囲で、1 が最低、255 が最高のプライオリティを表します。プライオリティが指定されていると、ローカル ルータのプライオリティが現在のアクティブ ルータより高い場合には、そのローカル ルータがアクティブ ルータとなるように要求が出されます。 • **delay**：（任意）ホット スタンバイ ルータがプリエンプション処理を行ってアクティブ ルータになるまでのプリエンプション遅延を指定します。 • **minimum**：（任意）最小の遅延時間（秒）を指定します。 • **sync**：（任意）IP 冗長クライアントの最大の同期化時間（秒）を指定します。 • *seconds*：（任意）ローカル ルータが最後に再起動されてからの最少秒数を指定し、その間はアクティブ ルータのテイクオーバーを延期させます。範囲は 0 ～ 3,600 秒（1 時間）で、デフォルトは 0 秒（遅延なし）です。
ステップ 17	`Router(config-if)# standby [group-number] track type number [interface-priority]`	インターフェイスが他のインターフェイスを追跡し、いずれかの他のインターフェイスがダウンした場合に、デバイスのホット スタンバイ プライオリティを下げるように設定します。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。 • *type*：追跡するインターフェイス タイプ（インターフェイス番号と組み合わせて使用）。 • *number*：追跡するインターフェイス番号（インターフェイス タイプと組み合わせて使用）。 • *interface-priority*：（任意）インターフェイスがダウンした場合（または再度アップになった場合）に、ルータのホット スタンバイ プライオリティの減算値（または加算値）を指定します。範囲は 0 ～ 255 です。デフォルトは 10 です。
ステップ 18	`Router(config-if)# standby [group-number] name`	インターフェイスのスタンバイ グループ名を設定します。 • *group-number*：（任意）名前を適用するグループ番号。 • *name*：HSRP スタンバイ グループの名前。

	コマンド	説明
ステップ 19	`Router(config-if)# interface vlan vlan_ID`	指定した暗号インターフェイス VLAN のインターフェイス コンフィギュレーション モードを開始します。
ステップ 20	`Router(config-if)# ip address address mask`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。 • *address*：IP アドレス。 • *mask*：サブネット マスク。
ステップ 21	`Router(config-if)# standby [group-number] ip ip-address`	HSRP をイネーブルにします。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。デフォルト値は 0 です。グループ番号の範囲は、HSRP バージョン 1 では 0 ～ 255、HSRP バージョン 2 では 0 ～ 4,095 です。 • *ip-address*：（任意）HSRP スタンバイ グループの仮想 IP アドレス。
ステップ 22	`Router(config-if)# standby [group-number] timers [msec] hellotime [msec] holdtime`	他のルータによってアクティブ ルータのダウンが宣言されるまでの、hello パケットの間隔およびホールド タイムを設定します。 • *group-number*：（任意）タイマーを適用するグループ番号。 • **msec**：（任意）インターバルをミリ秒単位で指定します。ミリ秒単位のタイマーを使用すると、より迅速なフェールオーバーが可能になります。 • *hellotime*：hello インターバル（秒）。1 ～ 254 の整数を使用します。デフォルトは 3 秒です。**msec** オプションを指定する場合、*hellotime* はミリ秒単位で、15 ～ 999 の整数を使用します。 • *holdtime*：アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒）。x ～ 255 の整数を使用します。デフォルトは 10 秒です。**msec** オプションを指定する場合、*holdtime* はミリ秒単位で指定し、y ～ 3,000 の整数を使用します。

	コマンド	説明
ステップ 23	`Router(config-if)# standby [group-number] [priority priority] preempt [delay [minimum | sync] seconds]`	アクティブ ルータの選択に使用されるスタンバイ プライオリティを設定します。 • *group-number*：（任意）プライオリティを適用するグループ番号。 • *priority*：（任意）プライオリティ値は 1 ～ 255 の範囲で、1 が最低、255 が最高のプライオリティを表します。プライオリティが指定されていると、ローカル ルータのプライオリティが現在のアクティブ ルータより高い場合には、そのローカル ルータがアクティブ ルータとなるように要求が出されます。 • **delay**：（任意）ホット スタンバイ ルータがプリエンプション処理を行ってアクティブ ルータになるまでのプリエンプション遅延を指定します。 • **minimum**：（任意）最小の遅延時間（秒）を指定します。 • **sync**：（任意）IP 冗長クライアントの最大の同期化時間（秒）を指定します。 • *seconds*：（任意）ローカル ルータが最後に再起動されてからの最少秒数を指定し、その間はアクティブ ルータのテイクオーバーを延期させます。範囲は 0 ～ 3,600 秒（1 時間）で、デフォルトは 0 秒（遅延なし）です。
ステップ 24	`Router(config-if)# standby [group-number] track type number [interface-priority]`	インターフェイスが他のインターフェイスを追跡し、いずれかの他のインターフェイスがダウンした場合に、デバイスのホット スタンバイ プライオリティを下げるように設定します。 • *group-number*：（任意）HSRP をアクティブにするインターフェイスのグループ番号。 • *type*：追跡するインターフェイス タイプ（インターフェイス番号と組み合わせて使用）。 • *number*：追跡するインターフェイス番号（インターフェイス タイプと組み合わせて使用）。 • *interface-priority*：（任意）インターフェイスがダウンした場合（または再度アップになった場合）に、ルータのホット スタンバイ プライオリティの減算値（または加算値）を指定します。範囲は 0 ～ 255 です。デフォルトは 10 です。
ステップ 25	`Router(config-if)# standby [group-number] name`	インターフェイスのスタンバイ グループ名を設定します。 • *group-number*：（任意）名前を適用するグループ番号。 • *name*：HSRP スタンバイ グループの名前。

	コマンド	説明
ステップ 26	`Router(config-if)# crypto map map-name ssp id`	ID で説明される SSP チャネルで転送される IPSec ステート情報をイネーブルにします。この機能がディセーブルになっている場合、そのインターフェイスにバインドされたすべてのスタンバイ エントリが削除されます。
ステップ 27	`Router(config-if)# crypto engine slot slot`	内部インターフェイス VLAN に暗号エンジンを割り当てます。 • *slot* : 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 gigabitethernet slot/subslot/port`	外部ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 29	`Router(config-if)# crypto connect vlan vlan_ID`	外部アクセス ポートを内部インターフェイス VLAN に接続し、暗号接続モードを開始します。 • *vlan_ID* : インターフェイス VLAN の識別子。

HSRP および SSP を使用した IPSec ステートフル フェールオーバーの設定例は、「暗号接続モードで HSRP と SSP を使用した IPSec ステートフル フェールオーバーの設定」（P.31-29）を参照してください。

VRF モードでの IPSec ステートレスおよびステートフル フェールオーバーの設定

（注）　Cisco IOS Release 12.2(33)SRA では、IPSec ステートフル フェールオーバーをサポートしなくなりました。Release 12.2SXF ではこの機能がサポートされています。

VRF モードでのシャーシ間フェールオーバーは、非 VRF（暗号接続）モードとの場合とは異なって設定されます。VRF モードでは、HSRP 設定は物理インターフェイスに適用されますが、暗号マップはインターフェイス VLAN に追加されます。非 VRF モードでは、HSRP 設定と暗号マップの両方が同じインターフェイスに適用されます。RRI ではアクティブおよびスタンバイ ルータ VRF ルーティング テーブルから動的にルートを挿入および削除します。

VRF モードでのステートレス フェールオーバーの設定例は、「VRF モードで HSRP を使用した IPSec ステートレス フェールオーバーの設定例」（P.31-33）を参照してください。

VRF モードでのステートフル フェールオーバーの設定例は、「VRF モードで HSRP を使用した IPSec ステートフル フェールオーバーの設定例」（P.31-34）を参照してください。

HSRP コンフィギュレーションの確認

IPSec ステートフル フェールオーバー HSRP の設定を確認するには、**show crypto isakmp ha standby** コマンド、**show crypto ipsec ha** コマンド、**show crypto ipsec sa** コマンド、および **show crypto ipsec sa standby** コマンドを入力します。

ISAKMP スタンバイ SA またはアクティブ SA を表示するには、**show crypto isakmp ha standby** コマンドを入力します。

```
Router# show crypto isakmp ha standby
```

```
dst             src             state       I-Cookie           R-Cookie

172.16.31.100   20.3.113.1      QM_IDLE     796885F3 62C3295E  FFAFBACD EED41AFF

172.16.31.100   20.2.148.1      QM_IDLE     5B78D70F 3D80ED01  FFA03C6D 09FC50BE

172.16.31.100   20.4.124.1      QM_IDLE     B077D0A1 0C8EB3A0  FF5B152C D233A1E0

172.16.31.100   20.3.88.1       QM_IDLE     55A9F85E 48CC14DE  FF20F9AE DE37B913

172.16.31.100   20.1.95.1       QM_IDLE     3881DE75 3CF384AE  FF192CAB 795019AB
```

IPSec HA Manager ステートを表示するには、**show crypto ipsec ha** コマンドを入力します。

```
Router# show crypto ipsec ha

Interface              VIP              SAs     IPSec Ha State

GigabitEthernet5/0/1   172.16.31.100    1800    Active since 13:00:16 EDT Tue Oct 1 2002
```

IPSec SA の HA ステータス（スタンバイまたはアクティブ）を表示するには、**show crypto ipsec sa** コマンドを入力します。

```
Router# show crypto ipsec sa

interface: GigabitEthernet5/0/1
   Crypto map tag: mymap, local addr. 172.168.3.100

    local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
    current_peer: 172.168.3.1
    PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
    path mtu 1500, media mtu 1500
    current outbound spi: 132ED6AB

    inbound esp sas:
    spi: 0xD8C8635F(3637011295)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    IV size: 8 bytes
    replay detection support: Y
    HA Status: STANDBY

  inbound ah sas:
    spi: 0xAAF10A60(2867923552)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

  inbound pcp sas:
```

```
  outbound esp sas:
    spi: 0x132ED6AB(321836715)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    IV size: 8 bytes
    replay detection support: Y
    HA Status: STANDBY

  outbound ah sas:
    spi: 0x1951D78(26549624)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
    ssa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

  outbound pcp sas:
```

スタンバイ SA を表示するには、**show crypto ipsec sa standby** コマンドを入力します。

```
Router# show crypto ipsec sa standby

interface: GigabitEthernet5/0/1
    Crypto map tag: mymap, local addr. 172.168.3.100

    local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
    current_peer: 172.168.3.1
    PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
    path mtu 1500, media mtu 1500
    current outbound spi: 132ED6AB

    inbound esp sas:
    spi: 0xD8C8635F(3637011295)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    IV size: 8 bytes
    replay detection support: Y
    HA Status: STANDBY

    inbound ah sas:
    spi: 0xAAF10A60(2867923552)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

    inbound pcp sas:

    outbound esp sas:
```

```
    spi: 0x132ED6AB(321836715)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    IV size: 8 bytes
    replay detection support: Y
    HA Status: STANDBY

    outbound ah sas:
    spi: 0x1951D78(26549624)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4499/59957)
    replay detection support: Y
    HA Status: STANDBY

    outbound pcp sas:
```

SSP 情報の表示

IPSec ステートフル フェールオーバー SSP の設定を確認するには、**show ssp client** コマンド、**show ssp packet** コマンド、**show ssp peers** コマンド、および **show ssp redundancy** コマンドを使用します。

SSP クライアント情報を表示するには、**show ssp client** コマンドを入力します。

```
Router# show ssp client

SSP Client Information

    DOI   Client Name                       Version   Running Ver

      1   IPSec HA Manager                   1.0       1.0

      2   IKE HA Manager                     1.0       1.0
```

SSP パケット情報を表示するには、**show ssp packet** コマンドを入力します。

```
Router# show ssp packet

SSP packet Information

    Socket creation time: 01:01:06

    Local port: 3249      Server port: 3249

    Packets Sent = 38559, Bytes Sent = 2285020

    Packets Received = 910, Bytes Received = 61472
```

SSP ピア情報を表示するには、**show ssp peers** コマンドを入力します。

```
Router# show ssp peers

SSP Peer Information

    IP Address      Connection State   Local Interface

    40.0.0.1        Connected          FastEthernet0/1
```

冗長性情報を表示するには、**show ssp redundancy** コマンドを入力します。

```
Router# show ssp redundancy

SSP Redundancy Information

  Device has been ACTIVE for 02:55:34

    Virtual IP      Redundancy Name             Interface

    172.16.31.100   KNIGHTSOFNI                 GigabitEthernet5/0/1GigabitEthernet0/0
```

Cisco IOS の IPSec ステートフル フェールオーバーのサポート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/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html

IPSec ステートフル フェールオーバーの設定例は、「暗号接続モードで HSRP と SSP を使用した IPSec ステートフル フェールオーバーの設定」（P.31-29）を参照してください。

BFG によるシャーシ内 IPSec ステートフル フェールオーバーの設定

ここでは、BFG を使用してシャーシ内で IPSec ステートフル フェールオーバーを設定する方法について説明します。

1 つのシャーシに 1 つまたは複数の IPSec VPN SPA のペアが搭載されている場合、各ペアを BFG として設定できます。2 つのモジュールを同一 SSC 内に配置する必要はありません。BFG 内では、IPSec VPN SPA はもう一方の IPSec VPN SPA のバックアップとしての役割を果たします。BFG はアクティブ / アクティブ構成またはアクティブ / スタンバイ構成です。

各 IPSec トンネルには、アクティブな IPSec VPN SPA が 1 つだけ対応付けられています。BFG では、もう一方の IPSec VPN SPA は、IPSec トンネルのバックアップとして動作します。IKE SA または IPSec トンネルごとに、それぞれ 1 つのアクティブ IPSec VPN SPA とそのバックアップがあります。たとえば、2 つの IPSec VPN SPA で 1,000 のトンネルをサポートするシステムでは、500 のトンネルを一方の SPA で、残り 500 のトンネルをもう一方の SPA でアクティブにできます。障害が発生した場合に、双方がもう一方の処理をテイクオーバーできるように、両方の SPA では相互にデータの複製が行われます。

BFG による IPSec ステートフル フェールオーバー設定時の注意事項および制約事項

BFG を使用して IPSec ステートフル フェールオーバーを設定する場合は、次の注意事項および制約事項に従ってください。

- BFG を構成する一方の IPSec VPN SPA の取り付けまたは取り外しを行っても、もう一方の IPSec VPN SPA 上でトンネルが中断されることはありません。
- フェールオーバー時のオーバーサブスクリプションを回避するため、BFG はアクティブ / スタンバイ構成で展開することをお勧めします。
- BFG をアクティブ / アクティブ構成で配置する場合、フェールオーバー時のオーバーサブスクリプションを回避するため、各 IPSec VPN SPA の使用率を 50% を超えないように制限することをお勧めします。

- Cisco IOS Release 12.2(33)SXH 以前のリリースでは、ステートフル BFG フェールオーバー中に、IPsec 統計情報がわずかに中断されることがありますが、フェールオーバー前近くの値にレジュームします。
- Cisco IOS Release 12.2(33)SXI 以降のリリースでは、ステートフル BFG フェールオーバー中に、IPsec 統計情報がリセットされ、ゼロからレジュームします。

IPSec ステートフル フェールオーバーでの BFG の設定

BFG を使用して IPSec ステートフル フェールオーバーを設定するには、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)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-red)# linecard-group` *group-number* `feature-card`	BFG のラインカード グループ ID を識別し、冗長ラインカード コンフィギュレーション モードを開始します。 • *group-number* : BFG の グループ ID を指定します。
ステップ 3	`Router(config-r-lc)# subslot` *slot/subslot*	グループに最初の SPA を追加します。 • *slot* : SSC が搭載されたシャーシ スロット番号を指定します。 • *subslot* : SPA が搭載されている SSC のセカンダリ スロット番号を指定します。
ステップ 4	`Router(config-r-lc)# subslot` *slot/subslot*	グループに 2 番めの SPA を追加します。

BFG による IPSec ステートフル フェールオーバーの設定例は、「BFG を使用した IPSec ステートフル フェールオーバーの設定例」（P.31-38）を参照してください。

BFG による IPSec ステートフル フェールオーバー設定の確認

BFG による IPSec ステートフル フェールオーバー設定を確認するには、**show redundancy linecard-group** コマンドおよび **show crypto ace redundancy** コマンドを入力します。

BFG のコンポーネントを表示するには、**show redundancy linecard group** コマンドを入力します。

```
Router# show redundancy linecard-group 1

Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Sublot:0
Slot:5 Sublot:0
```

BFG に関する情報を表示するには、**show crypto ace redundancy** コマンドを入力します。

```
Router# show crypto ace redundancy

---------------------------------------
LC Redundancy Group ID             :1
Pending Configuration Transactions:0
Current State                      :OPERATIONAL
```

```
Number of blades in the group     :2
Slots
-------------------------------------
Slot:3 subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running
```

設定例

ここでは、次の設定例を示します。

- 「シャーシに搭載した複数の IPSec VPN SPA の設定例」（P.31-24）
- 「暗号接続モードで HSRP を使用した IPSec ステートレス フェールオーバーの設定例」（P.31-27）
- 「暗号接続モードで HSRP と SSP を使用した IPSec ステートフル フェールオーバーの設定」（P.31-29）
- 「VRF モードで HSRP を使用した IPSec ステートレス フェールオーバーの設定例」（P.31-33）
- 「VRF モードで HSRP を使用した IPSec ステートフル フェールオーバーの設定例」（P.31-34）
- 「BFG を使用した IPSec ステートフル フェールオーバーの設定例」（P.31-38）

（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。

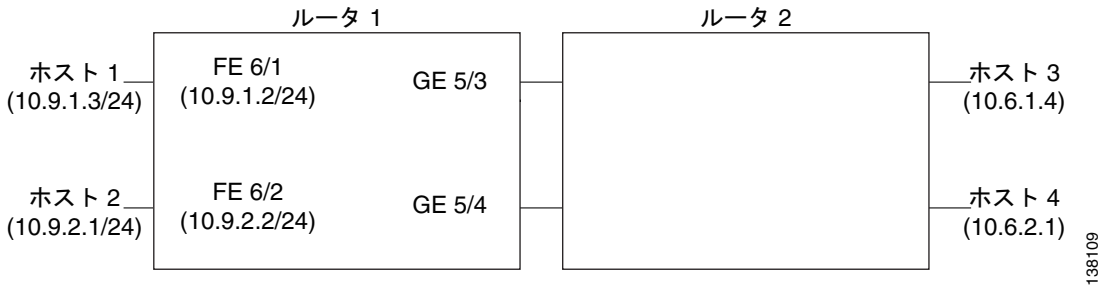
Cisco IOS Release 12.2(33)SRA では、それまでのリリースで使用されていた **crypto engine subslot** コマンドは、**crypto engine slot** コマンド（形式は **crypto engine slot** *slot* {**inside** | **outside**}）に置き換えられました。**crypto engine subslot** コマンドはサポートされなくなりました。アップグレード時には、余計なメンテナンス時間がかからないように、このコマンドが起動コンフィギュレーション内で変更されていることを確認してください。

シャーシに搭載した複数の IPSec VPN SPA の設定例

ここでは、1 つのシャーシに搭載した複数の IPSec VPN SPA の設定例を示します（図 31-1 を参照）。これらの例での注意点は次のとおりです。

- IPSec VPN SPA は、ルータ 1 のスロット 2、サブスロット 0 と、スロット 3、サブスロット 0 に搭載されています。
- この設定例では、注釈の前に 3 つの感嘆符（!!!）を使用しています。

図 31-1　シャーシに搭載した複数の IPSec VPN SPA の設定例




```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key mykey address 10.8.1.1
crypto isakmp key mykey address 10.13.1.1
!
crypto ipsec transform-set xform1 ah-md5-hmac esp-des esp-sha-hmac
crypto ipsec transform-set xform2 esp-3des esp-sha-hmac
!
!!! crypto map applied to VLAN 12, which is
!!! assigned to "inside" port of IPSec VPN SPA in slot 3
crypto map cmap2 10 ipsec-isakmp
 set peer 10.8.1.1
 set transform-set xform1
 match address 102
!
!!! crypto map applied to VLAN 20, which is
!!! assigned to "inside" port of IPSec VPN SPA in slot 2/0
crypto map cmap3 10 ipsec-isakmp
 set peer 10.13.1.1
 set transform-set xform2
 match address 103
!
!!! "port" VLAN, crypto connected to VLAN 12 by IPSec VPN SPA on slot 3/0
interface Vlan11
 no ip address
 crypto connect vlan 12
!
!!! "interface" VLAN, assigned to IPSec VPN SPA on slot 3/0
interface Vlan12
 ip address 10.8.1.2 255.255.0.0
 crypto map cmap2
 crypto engine slot 3/0
!
!!! "port" VLAN, crypto connected to VLAN 20 by IPSec VPN SPA on slot 2/0
interface Vlan19
 no ip address
 crypto connect vlan 20
!
!!! "interface" VLAN, assigned to IPSec VPN SPA on slot 2/0
interface Vlan20
 ip address 10.13.1.2 255.255.0.0
 crypto map cmap3
 crypto engine slot 2/0
!
!!! connected to Host 1
interface FastEthernet6/1
```

```
 ip address 10.9.1.2 255.255.255.0
!
!!! connected to Host 2
interface FastEthernet6/2
 ip address 10.9.2.2 255.255.255.0
!
!!! connected to Router 2
interface GigabitEthernet5/3
 switchport
 switchport mode access
 switchport access vlan 11
!
!!! connected to Router 2
interface GigabitEthernet5/4
 switchport
 switchport mode access
 switchport access vlan 19
!
interface GigabitEthernet2/0/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 12,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet2/0/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 11,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet3/0/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet3/0/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 19,1002-1005
 switchport mode trunk
 cdp enable
!
ip classless
!
!!! packets from Host 1 to Host 3 are routed from FastEthernet6/1
!!! to VLAN 12, encrypted with crypto map cmap2
!!! using IPSec VPN SPA in slot 3/0, and forwarded to peer 10.8.1.1
!!! through GigabitEthernet5/3
ip route 10.6.1.4 255.255.255.255 10.8.1.1
!
!!! packets from Host 2 to Host 4 are routed from FastEthernet6/2
!!! to VLAN 20, encrypted with crypto map cmap3
```

```
!!! using IPSec VPN SPA in slot 2/0, and forwarded to peer 10.13.1.1
!!! through GigabitEthernet5/4
ip route 10.6.2.1 255.255.255.255 10.13.1.1
!
!!! ACL matching traffic between Host 1 and Host 3
access-list 102 permit ip host 10.9.1.3 host 10.6.1.4
!
!!! ACL matching traffic between Host 2 and Host 4
access-list 103 permit ip host 10.9.2.1 host 10.6.2.1
```

暗号接続モードで HSRP を使用した IPSec ステートレス フェールオーバーの設定例

ここでは、次の HSRP を使用する IPSec ステートレス フェールオーバーの設定例を示します。

- 「アクティブ シャーシでの IPSec ステートレス フェールオーバーの設定例」（P.31-27）
- 「リモート ルータでの IPSec ステートレス フェールオーバーの設定例」（P.31-28）

アクティブ シャーシでの IPSec ステートレス フェールオーバーの設定例

以下に、HSRP を使用して IPSec ステートレス フェールオーバーを設定したアクティブ シャーシの設定例を示します。

```
hostname router-1
!
vlan 2-1001
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set PYTHON esp-3des
!
crypto dynamic-map dynamap_1 20
 set transform-set PYTHON
 reverse-route
!
!
crypto map MONTY 1 ipsec-isakmp dynamic dynamap_1
!
interface GigabitEthernet1/3
 switchport
 switchport access vlan 502
 switchport mode access
!
interface GigabitEthernet1/4
 ip address 50.0.0.3 255.0.0.0
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 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 502
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 172.1.1.3 255.255.255.0
 standby ip 172.1.1.100
 standby preempt
 standby name KNIGHTSOFNI
 standby track GigabitEthernet1/3
 standby track GigabitEthernet1/4
 no mop enabled
 crypto map MONTY redundancy KNIGHTSOFNI
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
ip route 10.0.0.0 255.0.0.0 172.1.1.4
ip route 20.0.0.0 255.0.0.0 172.1.1.4
ip route 50.0.0.0 255.0.0.0 50.0.0.13
ip route 50.0.1.1 255.255.255.255 50.0.0.13
ip route 50.0.2.1 255.255.255.255 50.0.0.13
ip route 50.0.3.1 255.255.255.255 50.0.0.13
ip route 50.0.4.1 255.255.255.255 50.0.0.13
ip route 50.0.5.1 255.255.255.255 50.0.0.13
```

リモート ルータでの IPSec ステートレス フェールオーバーの設定例

以下に、HSRP を使用する IPSec ステートレス フェールオーバーを設定したリモート ルータの設定例を示します。

```
hostname router-remote
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 172.1.1.100
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto map test_1 local-address Vlan2
crypto map test_1 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
 match address test_1
```

```
!
interface GigabitEthernet1/1
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
!
interface GigabitEthernet4/0/1
 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
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 20.0.1.1 255.255.255.0
 crypto map test_1
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip route 50.0.1.0 255.255.255.0 20.0.1.2
ip route 172.1.1.0 255.255.255.0 20.0.1.2
!
ip access-list extended test_1
 permit ip host 10.0.1.1 host 50.0.1.1
```

暗号接続モードで HSRP と SSP を使用した IPSec ステートフル フェールオーバーの設定

（注） Cisco IOS Release 12.2(33)SRA 以降では、HSRP と SSP を使用した IPSec ステートフル フェールオーバーをサポートしなくなりました。Release 12.2SXF ではこの機能がサポートされています。

（注）　この設定例では、SSP トラフィックが保護されていません。SSP トラフィックを保護するには、新しい暗号マップを定義し、「ssp」タグを付けないで SSP インターフェイスに接続します。この暗号マップの ACL は、リモート IP アドレスおよび SSP グループで定義された TCP ポートから取得できます。

次に、HSRP および SSP を使用する IPSec ステートフル フェールオーバーの設定例を示します。

```
hostname router-1
!
ssp group 100
 remote 50.0.0.6
 redundancy PUBLIC
 redundancy PRIVATE
!
vlan 502
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 0.0.0.0 0.0.0.0
crypto isakmp ssp 100
!
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto dynamic-map ha_dynamic 10
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
!
!
crypto map ha_dynamic 10 ipsec-isakmp dynamic ha_dynamic
!
!
!
interface GigabitEthernet1/1
 no ip address
 crypto connect vlan 502
!
interface GigabitEthernet1/2
 ip address 50.0.0.5 255.255.255.0
 load-interval 30
 no keepalive
 standby delay minimum 30 reload 60
 standby 2 ip 50.0.0.100
 standby 2 preempt
 standby 2 name PRIVATE
 standby 2 track GigabitEthernet1/1
 standby 2 track Vlan502
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 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
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan502
 ip address 172.1.1.5 255.255.255.0
 no mop enabled
 standby delay minimum 30 reload 60
 standby 1 ip 172.1.1.100
 standby 1 preempt
 standby 1 name PUBLIC
 standby 1 track GigabitEthernet1/1
 standby 1 track GigabitEthernet1/2
 crypto map ha_dynamic ssp 100
 crypto engine slot 4/0
!
ip route 10.0.0.0 255.0.0.0 172.1.1.4
ip route 20.0.0.0 255.0.0.0 172.1.1.4
ip route 50.0.0.0 255.0.0.0 50.0.0.13
```

次に、HSRP および SSP を使用する IPSec ステートフル フェールオーバー用に設定されているリモート ピア ルータの設定例を示します。

```
hostname router-remote
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 172.1.1.100
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto map test_1 local-address Vlan2
crypto map test_1 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
 match address test_1
!
crypto map test_2 local-address Vlan3
crypto map test_2 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set pfs group2
 match address test_2
!
interface GigabitEthernet1/1
```

```
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 no ip address
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-3,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 20.0.1.1 255.255.255.0
 crypto map test_1
 crypto engine slot 4/0
!
interface Vlan3
 ip address 20.0.2.1 255.255.255.0
 crypto map test_2
 crypto engine slot 4/0

interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Vlan503
 no ip address
 crypto connect vlan 3
!
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip route 50.0.1.0 255.255.255.0 20.0.1.2
ip route 50.0.2.0 255.255.255.0 20.0.2.2
ip route 172.1.1.0 255.255.255.0 20.0.1.2
!
ip access-list extended test_1
 permit ip host 10.0.1.1 host 50.0.1.1
ip access-list extended test_2
 permit ip host 10.0.2.1 host 50.0.2.1
```

VRF モードで HSRP を使用した IPSec ステートレス フェールオーバーの設定例

以下に、HSRP シャーシ間ステートレス フェールオーバー（暗号マップあり）を使用した VRF モードの設定例を示します。

```
!
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 key1
  pre-shared-key address 14.0.1.1 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp keepalive 10
crypto isakmp profile ivrf
   vrf ivrf
   keyring key1
   match identity address 14.0.1.1 255.255.255.255
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
!
crypto map map_vrf_1 local-address Vlan3
crypto map map_vrf_1 10 ipsec-isakmp
 set peer 14.0.1.1
 set transform-set ts
 set isakmp-profile ivrf
 match address acl_1
!
interface GigabitEthernet1/1
 !switch inside port
 ip address 13.254.254.1 255.255.255.0
!
interface GigabitEthernet1/1.1
 encapsulation dot1Q 2000
 ip vrf forwarding ivrf
 ip address 13.254.254.1 255.0.0.0
!
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 Vlan3
 ip address 15.0.0.2 255.255.255.0
 standby delay minimum 0 reload 0
 standby 1 ip 15.0.0.100
 standby 1 timers msec 100 1
 standby 1 priority 105
 standby 1 preempt
 standby 1 name std-hsrp
 standby 1 track GigabitEthernet1/2
 crypto engine slot 4/0 outside
!
interface Vlan2
 ip vrf forwarding ivrf
 ip address 15.0.0.252 255.255.255.0
 crypto map map_vrf_1 redundancy std-hsrp
 crypto engine slot 4/0 inside

!
ip classless
ip route 12.0.0.0 255.0.0.0 15.0.0.1
ip route 13.0.0.0 255.0.0.0 13.254.254.2
ip route 14.0.0.0 255.0.0.0 15.0.0.1
ip route 223.255.254.0 255.255.255.0 17.1.0.1
ip route vrf ivrf 12.0.0.1 255.255.255.255 15.0.0.1
!
ip access-list extended acl_1
 permit ip host 13.0.0.1 host 12.0.0.1
!
!
arp vrf ivrf 13.0.0.1 0000.0000.2222 ARPA
```

VRF モードで HSRP を使用した IPSec ステートフル フェールオーバーの設定例

（注）　Cisco IOS Release 12.2(33)SRA 以降では、HSRP を使用した IPSec ステートフル フェールオーバーをサポートしなくなりました。Release 12.2SXF ではこの機能がサポートされています。

以下に、HSRP シャーシ間ステートフル フェールオーバーを使用した VRF モードの設定例を示します。

```
hostname router-1
```

```
!
ip vrf vrf1
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ssp group 100
 remote 172.1.1.60
 redundancy PUBLIC
 redundancy PRIVATE
!
crypto engine mode vrf
!
vlan 2-1001
!
crypto keyring key1
  pre-shared-key address 0.0.0.0 0.0.0.0 key 12345
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp ssp 100
!
crypto isakmp profile prof1
   vrf vrf1
   keyring key1
   match identity address 0.0.0.0
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto dynamic-map ha_dynamic 10
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 set isakmp-profile prof1
 reverse-route
!
!
crypto map ha_dynamic local-address GigabitEthernet1/3
crypto map ha_dynamic 10 ipsec-isakmp dynamic ha_dynamic
!
!
!
interface GigabitEthernet1/2
 no ip address
!
interface GigabitEthernet1/2.1
 encapsulation dot1Q 2500
 ip vrf forwarding vrf1
 ip address 50.0.0.5 255.0.0.0
 standby delay minimum 30 reload 90
 standby 2 ip 50.0.0.100
 standby 2 preempt
 standby 2 name PRIVATE
 standby 2 track GigabitEthernet1/3
 standby 2 track Vlan100
!
interface GigabitEthernet1/3
 ip address 172.1.1.50 255.255.255.0
 standby delay minimum 30 reload 90
 standby 1 ip 172.1.1.100
 standby 1 preempt
```

```
 standby 1 name PUBLIC
 standby 1 track GigabitEthernet1/2
 standby 1 track Vlan100
 crypto engine slot 2/0
!
interface GigabitEthernet2/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 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
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan100
 ip vrf forwarding vrf1
 ip address 172.1.1.6 255.255.255.0
 crypto map ha_dynamic ssp 100
 crypto engine slot 2/0
!
!
ip route 10.0.0.0 255.0.0.0 172.1.1.4
ip route 20.0.0.0 255.0.0.0 172.1.1.4
ip route vrf vrf1 50.0.1.1 255.255.255.255 50.0.0.13
!
```

次に、VRF モードの IPSec ステートフル フェールオーバー用に設定されているリモート ピア ルータの設定例を示します。

```
hostname router-remote
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 172.1.1.100
!
!
crypto ipsec transform-set ha_transform esp-3des
!
crypto map test_1 local-address Vlan2
crypto map test_1 10 ipsec-isakmp
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 match address test_1
!
crypto map test_2 local-address Vlan3
crypto map test_2 10 ipsec-isakmp
```

```
 set peer 172.1.1.100
 set security-association lifetime seconds 86400
 set transform-set ha_transform
 match address test_2
!
interface GigabitEthernet1/1
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 no ip address
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-3,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,503,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!

interface Vlan2
 ip address 20.0.1.1 255.255.255.0
 crypto map test_1
 crypto engine slot 4/0
!
interface Vlan3
 ip address 20.0.2.1 255.255.255.0
 crypto map test_2
 crypto engine slot 4/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Vlan503
 no ip address
 crypto connect vlan 3
!
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip route 50.0.1.0 255.255.255.0 20.0.1.2
ip route 50.0.2.0 255.255.255.0 20.0.2.2
ip route 172.1.1.0 255.255.255.0 20.0.1.2
!
ip access-list extended test_1
 permit ip host 10.0.1.1 host 50.0.1.1
ip access-list extended test_2
```

```
permit ip host 10.0.2.1 host 50.0.2.1
```

BFG を使用した IPSec ステートフル フェールオーバーの設定例

以下に BFG を使用した IPSec ステートフル フェールオーバーの設定例を示します。

```
Router(config)# redundancy
Router(config-red)# line-card-group 1 feature-card
Router(config-r-lc)# subslot 3/1
Router(config-r-lc)# subslot 5/1
```