IKEv2 ロード バランサの設定

IKEv2 ロードバランサ機能は、FlexVPN ゲートウェイのクラスタを有効にするためのサポートを提供し、FlexVPN ゲートウェイ間で受信インターネット キー エクスチェンジ バージョン 2（IKEv2）の接続要求を配信します。この機能は、システムおよび暗号の負荷率に基づいて最も負荷の小さい FlexVPN ゲートウェイに受信 FlexVPN または AnyConnect クライアントの要求をリダイレクトします。

IKEv2 ロード バランサの前提条件

- サーバー側の設定として、Hot Standby Router Protocol（HSRP）および FlexVPN サーバー（IKEv2 プロファイル）が設定されていること。
- クライアント側の設定として、FlexVPN クライアントが設定されていること。

IKEv2 ロード バランサに関する情報

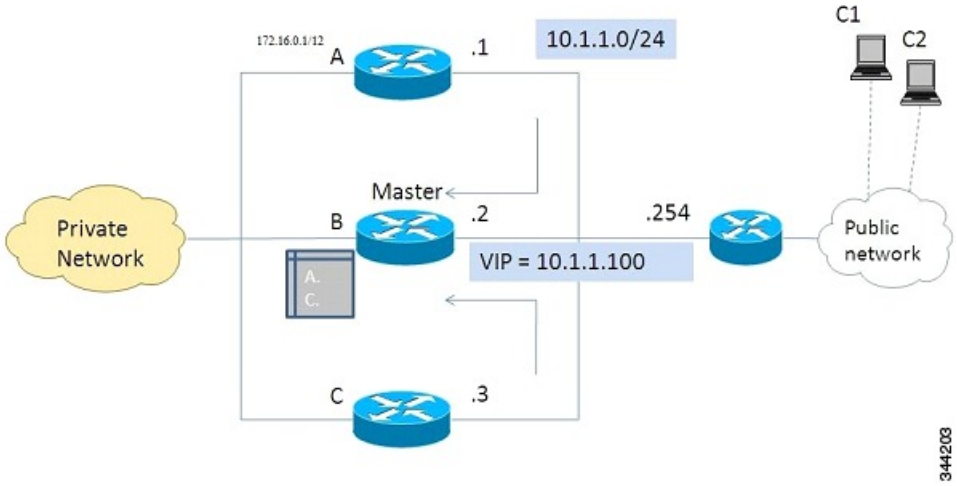
IKEv2 ロード バランサの概要

IKEv2 ロード バランサ サポート機能は、リモート アクセス クライアントからの要求を、Hot Standby Router Protocol（HSRP）グループまたはクラスタ内の最低負荷ゲートウェイ（LLG）にリダイレクトすることで、クラスタロードバランシング（CLB）ソリューションを提供します。HSRP クラスタは、LAN またはエンタープライズ ネットワーク内のゲートウェイまたは FlexVPN サーバーのグループです。CLB ソリューションは、要求の HSRP クラスタ内 LLG へ

のリダイレクトにより、RFC 5685 で定義されたインターネット キー エクスチェンジ バージョン 2（IKEv2）リダイレクト メカニズムと連携します。

次の図は、IKEv2 クラスタのロード バランシング ソリューションの仕組みを示します。

図 *1 : IKEv2* クラスタのロード バランシング ソリューション



1. アクティブ HSRP ゲートウェイは、HSRP グループの「プライマリ」として選択され、グループの仮想 IP アドレス（VIP）の所有権を取得します。プライマリはクラスタ内にゲートウェイのリストを保持して、各ゲートウェイの負荷を追跡し、FlexVPN クライアントの要求を LLG にリダイレクトします。
2. 残りのゲートウェイは「従属」と呼ばれ、負荷の更新をプライマリに定期的に送信します。
3. IKEv2 クライアントが HSRP VIP に接続すると、要求はまずプライマリに到達し、クラスタ内の LLG に順番にリダイレクトされます。

CLB ソリューションのコンポーネントは次のとおりです。

- HSRP
- CLB プライマリ
- CLB 従属
- CLB 通信
- IKEv2 リダイレクト メカニズム

Hot Standby Router Protocol

Hot Standby Router Protocol（HSRP）は、プライマリ HSRP またはアクティブルータ（AR）を選択するために使用されます。専用デバイスを選択する HSRP では、グループ内の 1 つのデバイスに VIP を設定する必要があります。このアドレスは、グループ内の他デバイスによって学習されます。プライマリに割り当てられた IP アドレスは、グループの VIP として使用されま

す。HSRP アクティブルータ（「プライマリ CLB」とも呼ばれる）は IKEv2 要求を受信し、クラスタの LLG にこれらの要求をリダイレクトします。リダイレクトが IKEv2 プロトコル レベルで実行されると、以下を実行できるようになります。

- FlexVPN クライアントからのすべての要求は、VIP が FlexVPN クライアントで設定されると、プライマリ HSRP で受信される。FlexVPN クライアントが知る必要があるのは HSRP クラスタの VIP のみであるため、FlexVPN クライアントの設定は最小化される。
- プライマリ CLB はプライマリ HSRP と同じゲートウェイで実行されるため、すべての従属 CLB の負荷情報が維持される。プライマリ CLB では、要求の効率的なリダイレクトが可能なため、複数のリダイレクトやループを防ぐことができる。

プライマリ CLB

プライマリ CLB は、プライマリ HSRP またはアクティブルータ（AR）上で動作します。プライマリは、従属 CLB から更新を受信し、その負荷条件に基づいてそれらをソートし、負荷が最小のゲートウェイ（LLG）を計算します。プライマリは、LLG の IP アドレスを IKEv2（FlexVPN サーバー上）に送信します。IP アドレスは、LLG との IKEv2 セッションを開始した発信側（FlexVPN クライアント）に送信されます。プライマリは受信する IKEv2 クライアント接続を LLG にリダイレクトします。詳細については、IKEv2 リダイレクト メカニズム （4 ページ）を参照してください。

（注） 「CLB ノード」は、プライマリ CLB と従属 CLB を指定する必要がある場所で使用します。

従属 CLB

従属 CLB は、アクティブルータ（AR）上を除いた、HSRP グループ内のすべてのデバイスで動作します。従属は、サーバーに負荷更新を定期的に送信します。従属 CLB は、プライマリ CLB に情報を提供する、フル機能の IKEv2 ゲートウェイです。更新以外にも、従属 CLB は活動管理のメッセージをプライマリ CLB に送信します。

CLB 負荷管理メカニズム

CLB 負荷管理メカニズムは、プライマリ CLB と従属 CLB 間で動作する、TCP ベースのプロトコルです。CLB 負荷管理メカニズムは、プライマリ CLB に従属 CLB の負荷について情報を提供します。この情報に基づいて、プライマリ CLB は、新しく受信する各 IKEv2 接続のセッションを処理する LLG を選択します。

IKEv2 ロード バランサの利点

- IKEv2 ロード バランサ サポート機能は、設定が簡単でコスト効率に優れています。
- FlexVPN クライアントは、クラスタ内のすべてのゲートウェイの IP アドレスを知る必要はありません。クライアントが知っておく必要があるのは、クラスタの仮想 IP アドレスのみです。

• すべての暗号化セッションは、クラスタ内のノードにリダイレクトされます。

IKEv2 リダイレクト メカニズム

IKEv2 リダイレクト メカニズムによって、VPN ゲートウェイは負荷条件およびメンテナンス要件に基づいて FlexVPN クライアント要求を別の VPN ゲートウェイにリダイレクトできます。

IKEv2 リダイレクト メカニズムは、セキュリティ アソシエーション（SA）の初期化（IKE_SA_INIT）と SA 認証（IKE_AUTH）で実行されます。

IKEv2 初期交換中のリダイレクト（SA 初期化）

FlexVPN クライアントまたは AnyConnect クライアントは、最初の IKE_SA_INIT 要求に REDIRECT_SUPPORTED 通知メッセージを含めることで、インターネット キー エクスチェンジバージョン 2（IKEv2）リダイレクト メカニズムのサポートを示します。**crypto ikev2 redirect client** コマンドを使用して、クライアントのリダイレクト メカニズムを有効にします。**crypto ikev2 redirect gateway init** コマンドを使用して、ゲートウェイの IKE_SA_INIT でのリダイレクトを有効にします。

IKEv2 要求を別の新しいゲートウェイにリダイレクトするには、IKE_SA_INIT 要求を受信するゲートウェイが、暗号ロードバランサ（CLB）モジュールのサポートによって、新しいゲートウェイ（この場合は LLG）の IP アドレスまたは完全修飾ドメイン名（FQDN）を選択します。このゲートウェイは、REDIRECT 通知メッセージを含む IKE_SA_INIT 応答で応答します。通知には、IKE_SA_INIT 要求内のペイロードからの新しいゲートウェイやナンス値などの情報が含まれます。IKE_SA_INIT 応答を受信したクライアントは、IKE_SA_INIT 要求で送信されたナンス値とリダイレクト通知で指定されたゲートウェイ情報を検証し、リダイレクト通知が設定のとおりかどうかを確認します。

（注） ナンス値が一致しない場合、クライアントはその応答を破棄して別の応答を待って、発信側のサービス妨害（DoS）攻撃を防ぎます。IKE_SA_INIT 応答内に攻撃者が不正なリダイレクト ペイロードが挿入すると、DoS 攻撃が発生する場合があります。

新しいゲートウェイとの IKE_SA_INIT 交換では、クライアント メッセージに REDIRECTED_FROM 通知ペイロードが含まれます。REDIRECTED_FROM 通知ペイロードは、クライアントにリダイレクトされる送信元 VPN ゲートウェイの IP アドレスで構成されています。IKEv2 交換は、送信元ゲートウェイでの処理と同じように処理されます。

（注） 新しいゲートウェイもクライアントの目的を果たせない場合、クライアントは新しいゲートウェイによって再度リダイレクトされることがあります。クライアントでは、リダイレクト後の新しいゲートウェイとの IKE_SA_INIT 交換に、REDIRECT_SUPPORTED ペイロードは再度含まれません。新しいゲートウェイとの IKE_SA_INIT 交換内に REDIRECTED_FROM 通知ペイロードが存在することは、クライアントが IKEv2 リダイレクト メカニズムをサポートすることを、新しいゲートウェイに示します。

IKE_AUTH 交換中のリダイレクト（SA 認証）

詳細なセキュリティ分析によって、IKE_AUTH 中のリダイレクトは IKE_INIT 中のリダイレクトと比較してより安全でも危険でもないことが示されました。ただし、パフォーマンスと拡張性の理由により、シスコは IKE_INIT 中のリダイレクトを推奨します。**crypto ikev2 redirect gateway auth** コマンドを使用して、ゲートウェイのリダイレクト メカニズムを有効にします。**redirect gateway auth** コマンドを使用して、選択した IKEv2 プロファイル認証時のリダイレクトを有効にします。

この方法では、クライアント認証ペイロードは、リダイレクト通知ペイロードを送信する前に検証されます。また、クライアントでも、リダイレクト通知に従って動作する前に、ゲートウェイ認証ペイロードが検証されます。任所ペイロードが交換され、正常に検証されると、IKEv2 セキュリティ アソシエーション（SA）が正常に検証され、要求のリダイレクトを決定する INITIAL_CONTACT が処理されます。リダイレクトが有効な場合、ゲートウェイでは IKE SA が作成され、リダイレクト通知で IKE_AUTH 応答が送信されます。

この方法では、子 SA は作成されません。IKE_AUTH には、子 SA に関連するペイロードは含まれません。IKE_AUTH 応答を受信すると、クライアントは、ゲートウェイ認証ペイロードを検証し、削除通知を送信してそのゲートウェイがある IKEv2 SA を削除します。クライアントは、リダイレクト通知ペイロードに従って動作し、新しいゲートウェイとの接続を確立します。クライアントは、削除通知の確認応答を待たずに、新しいゲートウェイとの接続を確立します。IKE_AUTH 交換で Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）認証が呼び出される場合、ゲートウェイでは、リダイレクトペイロードの送信を最初と最後の IKE_AUTH 応答のどちらで送信するかを選択します。リダイレクトごとに認証情報を指定する必要がないため、EAP 認証は最初の IKE_AUTH 応答に含まれます。

互換性および相互運用性

IKEv2 リダイレクト メカニズムは、RFC 5685 に基づいています。ゲートウェイ（IKEv2 応答側）は、標準を実装するクライアント（IKEv2 発信側）と互換性があります。同様に、クライアント（発信者）の実装では、標準を実装しているサードパーティ製サーバー（応答側）との互換性が必要です。負荷管理メカニズムは Cisco 独自のもので、Cisco IOS デバイスでのみサポートされます。

リダイレクト ループ処理

クライアント要求は、正しくない設定またはサービス妨害（DoS）攻撃を理由として、順番に複数回リダイレクトできます。場合によっては、クライアントを他のゲートウェイにリダイレ

クトする複数のゲートウェイによってクライアントがループに入り、その結果クライアントへのサービスが拒否されることがあります。これを防ぐには、**max-redirects** *number* キーワード/引数ペアを指定して **crypto ikev2 redirect client** コマンドを使用し、特定の IKEv2 セキュリティ アソシエーション（SA）設定について特定数を超えるリダイレクトを受け入れないようにクライアントを設定します。

IKEv2 クラスタの再接続

IKEv2 クラスタの再接続機能によって、Cisco AnyConnect クライアントはクラスタ内のサーバーに再接続できます。**crypto ikev2 reconnect key** は、クライアントにプッシュされた不明瞭なデータを暗号化するためにサーバーに導入されています。障害を検出すると、クライアントは、認証クレデンシャルの入力を再度要求せずに新規または既存のサーバーと再接続します。

キー インデックス値は 2 つのみ（1 および 2）です。いずれかの時点で、これを使用して設定されたキーの 1 つがアクティブになります。IOS サーバーで再接続キーの CLI を使用して再接続キーが設定されている場合、Cisco IOS サーバーは再接続データを復号できます。これは、キーがバックアップ キーのみの場合にも当てはまります。

この機能は、**authentication** コマンドで IKEv2 プロファイルの認証方式として **anyconnect-eap** キーワードを指定した場合にはサポートされません。

（注） この機能は、Cisco AnyConnect サーバーとして動作するように設定された Cisco IOS デバイスで使用できます。この機能をサポートする AnyConnect クライアント ソフトウェア バージョンは、4.2 以降のリリースです。この機能は、新規導入にのみ適用できます。Cisco IOS サーバーでこの機能が有効になると、以前のリリースの Cisco AnyConnect クライアントはサポートされなくなります。

IKEv2 ロード バランサの設定方法

サーバー クラスタの設定

ロード バランシングに対する HSRP グループの設定

このタスクを実行して、単一の Hot Standby Router Protocol（HSRP）グループをクラスタ用に設定します。

Hot Standby Router Protocol（HSRP）は、プライマリ HSRP またはアクティブルータ（AR）を選択するために使用されます。専用デバイスを選択する HSRP では、グループ内の 1 つのデバイスに VIP を設定する必要があります。このアドレスは、グループ内の他デバイスによって学習されます。プライマリに割り当てられた IP アドレスは、グループの VIP として使用されます。HSRP アクティブルータ（「プライマリ CLB」とも呼ばれる）は IKEv2 要求を受信し、ク

ラスタの LLG にこれらの要求をリダイレクトします。リダイレクトが IKEv2 プロトコル レベルで実行されると、以下を実行できるようになります。

- FlexVPN クライアントからのすべての要求は、VIP が FlexVPN クライアントで設定されると、プライマリ HSRP で受信される。FlexVPN クライアントが知る必要があるのは HSRP クラスタの VIP のみであるため、FlexVPN クライアントの設定は最小化される。
- プライマリ CLB はプライマリ HSRP と同じゲートウェイで実行されるため、すべての従属 CLB の負荷情報が維持される。プライマリ CLB では、要求の効率的なリダイレクトが可能なため、複数のリダイレクトやループを防ぐことができる。

（注） このタスクでは、ロードバランシングのため、HSRP グループの設定に必要な最小限のコマンドを説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** *group-name*
7. **exit**
8. 手順 3 ～ 7 を繰り返して、別のクラスタに HSRP グループを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス タイプを設定し、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 4	**ip address** *ip-address mask* [**secondary**] 例：	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 10.0.0.1 255.255.255.0`	
ステップ 5	**standby** [*group-number*] **priority** *priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP 優先度を設定します。
ステップ 6	**standby** *group-name* 例： `Device(config-if)# standby group1`	HSRP スタンバイ グループの名前を指定します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	手順 3 ～ 7 を繰り返して、別のクラスタに HSRP グループを設定します。	—

負荷管理メカニズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 cluster**
4. **holdtime** *milliseconds*
5. **master** { **overload-limit** *percent* | **weight** { **crypto-load** *weight-number* | **system-load** *weight-number*}}
6. **port** *port-number*
7. **slave** { **hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*}
8. **standby-group** *group-name*
9. **shutdown**
10. **exit**
11. **crypto ikev2 reconnect key** *key index* **active** *name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 cluster** 例： `Device(config)# crypto ikev2 cluster`	IKEv2 クラスタ ポリシーを定義し、IKEv2 クラスタ コンフィギュレーション モードを開始します。
ステップ 4	**holdtime** *milliseconds* 例： `Device(config-ikev2-cluster)# holdtime 10000`	（オプション）ピアからのメッセージを受信する時間をミリ秒単位で指定します。 • 設定された時間内にメッセージを受信しない場合、ピアは「死んでいる」と宣言されます。
ステップ 5	**master** { **overload-limit** *percent* | **weight** { **crypto-load** *weight-number* | **system-load** *weight-number*}} 例： `Device(config-ikev2-cluster)# master weight crypto-load 10`	HSRP クラスタのプライマリの設定を指定します。 • **overload-limit** *percent*：クラスタのしきい値負荷。デバイスがビジーなことを判断し、要求へのリダイレクトを無視するための負荷制限。 • **weight**：負荷属性の重みを指定します。範囲：0 ～ 100。デフォルトは 100 です。 • **crypto-load** *weight-number*：IKE と IPSec のセキュリティ アソシエーション（SA）の負荷。 • **system-load** *weight-number*：システムとメモリの負荷。
ステップ 6	**port** *port-number* 例： `Device(config-ikev2-cluster)# port 2000`	（任意）クラスタプライマリのリッスンポートを指定します。
ステップ 7	**slave** { **hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*} 例： `Device(config-ikev2-cluster)# slave max-session 90`	HSRP グループの従属ゲートウェイ設定を指定します。 • **hello** *milliseconds*：ミリ秒単位の従属ゲートウェイの Hello インターバル。 • **max-session** *number*：従属上で許可される SA の最大数。このキーワードは必須であり、スキップできません。 • **priority** *number*：従属の優先順位。

	コマンドまたはアクション	目的
		• **update** *milliseconds*：従属ゲートウェイ用の更新メッセージ間の、ミリ秒単位のインターバル。
ステップ 8	**standby-group** *group-name* 例： `Device(config-ikev2-cluster)# standby-group group1`	従属が含まれている HSRP グループを定義します。 • *group-name*：グループ名は *group-name* 引数から派生します。これは、**standby name** コマンドで指定されます。
ステップ 9	**shutdown** 例： `Device(config-ikev2-cluster)# shutdown`	（オプション）IKEv2 クラスタ ポリシーを無効にします。
ステップ 10	**exit** 例： `Device(config-ikev2-cluster)# exit`	IKEv2 クラスタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ikev2 reconnect key** *key index* **active** *name* 例： `Device(config)# crypto ikev2 reconnect key 1 active test123`	セッション再接続の IKEv2 不透明型データ サポートを有効にします。 （注） IKEv2 クラスタの再接続機能は、**ikev2 reconnect key active** *name key-string* に **active** キーワードが含まれている場合にのみ、暗号化に対して有効になります。クラスタの再接続機能を有効にするには、**active** キーワードは必須です。**active** キーワードを指定せずに **ikev2 reconnect key** *key-name key-string* コマンドを使用すると、ヘッドエンドでは復号化のみが可能になります。
ステップ 12	**end** 例： `Device(config-ikev2-cluster)# end`	IKEv2 クラスタ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サーバーでの IKEv2 リダイレクト メカニズムの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 redirect gateway init**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 redirect gateway init** 例： `Device(config)# crypto ikev2 redirect gateway init`	SA 開始中に、ゲートウェイで IKEv2 リダイレクト メカニズムを有効にします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クライアントでの IKEv2 リダイレクト メカニズムの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 redirect client** [**max-redirects** *number*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 redirect client** [**max-redirects** *number*] 例： `Device(config)# crypto ikev2 redirect client max-redirects 15`	FlexVPN クライアントで IKEv2 リダイレクト メカニズムを有効にします。 • **max-redirects** *number*：（オプション）リダイレクト ループ検出に対して、FlexVPN クライアン

	コマンドまたはアクション	目的
		トで設定できるリダイレクトの最大数を指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 ロード バランサの設定例

例：ロード バランシングに対する HSRP グループの設定

次の例では、プライオリティ 110 で Hot Standby Router Protocol（HSRP）グループのアクティブ ルータとして設定された RouterA を示します。デフォルトのプライオリティ レベルは 100 です。この HSRP グループには、group1 のグループ名が割り当てられます。グループ名は、クラスタ ポリシーに記載されています。

```
Device(config)# hostname RouterA
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby group1
Device(config-if)# end
```

例：負荷管理メカニズムの設定

次の例は、IKEv2 で負荷管理メカニズムを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# holdtime 10000
Device(config-ikev2-cluster)# master crypto-load 10
Device(config-ikev2-cluster)# port 2000
Device(config-ikev2-cluster)# slave priority 90
Device(config-ikev2-cluster)# standby-group group1
Device(config-ikev2-cluster)# shutdown
Device(config-ikev2-cluster)# end
```

例：リダイレクト メカニズムの設定

次の例は、クライアント上およびゲートウェイでの開始中にリダイレクト メカニズムを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 redirect client
Device(config)# crypto ikev2 redirect gateway init
Device(config)# end
```

例：クラスタ再接続キーの設定

次の例は、サーバーで再接続キーを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 reconnect key 1 active key
Device(config)# crypto ikev2 reconnect key 2 test
Device(config)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
HSRP コンフィギュレーション	『*Configuring HSRP*』
HSRP コマンド	『Cisco IOS First Hop Redundancy Protocols Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 5685	*Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 ロード バランサの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IKEv2* ロード バランサの機能情報

機能名	リリース	機能情報
AnyConnect のクラスタ再接続との IKEv2 高速コンバージェンス		AnyConnect のクラスタ再接続との IKEv2 高速コンバージェンス機能では、Cisco AnyConnect クライアントはクラスタ内の任意のサーバーと再接続できます。 次のコマンドが導入または変更されました： **crypto ikev2 reconnect key**

機能名	リリース	機能情報
IKEv2 ロード バランサのサポート		IKEv2 ロード バランサ サポート機能は、要求を最低負荷ゲートウェイにリダイレクトすることで、FlexVPN クライアントから受信する IKEv2 要求を、IKEv2 FlexVPN サーバー間またはゲートウェイ間で分散します。 次のコマンドが導入または変更されました。 **crypto ikev2 cluster, crypto ikev2 redirect, holdtime, primary (IKEv2), port (IKEv2), redirect gateway, subordinate (IKEv2), standby-group, show crypto ikev2 cluster, show crypto ikev2 sa.**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。