GRE および DM VPN

総称ルーティング カプセル化（GRE）、および GRE モード設定を含む Dynamic Multipoint（DM; ダイナミック マルチポイント）VPN を設定できます。ハブアンドスポーク トポロジ、ポイントツーポイント トポロジ、および完全メッシュ VPN トポロジに IPsec GRE VPN を設定できます。DMVPN は、ハブアンドスポーク トポロジだけで使用可能です。

この章は次のトピックで構成されています。

[GRE Modes] ページについて

[GRE Modes] ページを使用して、GRE、GRE ダイナミック IP、および DMVPN のポリシーで IPsec トンネリングについてルーティング パラメータおよびトンネル パラメータを定義します。

ポリシーの内容は、アクセスする方法によって異なります。

- （[Site-to-Site VPN Manager] ウィンドウ）GRE VPN または DMVPN を選択する場合は、[GRE Modes] ポリシーには、VPN で使用されるテクノロジーとテクノロジー タイプに関連するプロパティが含まれています。
- （ポリシービュー）[サイト間 VPN（Site-to-Site VPN）] > [GRE モード（GRE Modes）] を選択して、新しいポリシーを作成するか既存のポリシーを選択する場合は、ポリシーには [GRE 方式（GRE Method）] という追加のフィールドがあります。[GRE Method] リストから、ポリシーを定義する VPN テクノロジーとテクノロジー タイプとして [IPsec/GRE]、[GRE Dynamic IP]、[DMVPN]、または [Large Scale DMVPN] を選択する必要があります。このオプションは、ポリシーに表示されるフィールドを制御します。ポリシーの保存後は [GRE Method] を変更できません。

共有される [GRE モード（GRE Modes）] ポリシーを VPN に割り当てる場合は、[GRE 方式（GRE Method）] および VPN のテクノロジーとタイプが一致する必要があります。一致しな

い場合は、ポリシーを選択できません。たとえば、共有される [DMVPN GRE Modes] ポリシーを IPsec/GRE VPN に割り当てることはできません。

次のトピックで、選択した [GRE Methods] に基づいて [GRE Modes] ポリシーについて詳細に説明します。

- [IPsec/GRE] または [GRE Dynamic IP]： GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定 （8 ページ）を参照してください。
- [DMVPN] または [Large Scale DMVPN]： DMVPN の [GRE Modes] の設定 （16 ページ）を参照してください。

（注） IPsec/GRE、GRE ダイナミック IP、または DMVPN のルーティング ポリシーを設定する場合、Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、同じルーティング プロトコルと、[GRE Modes] ポリシーで定義した自律システム（またはプロセス ID）番号を使用して（各メンバー デバイスで）ルータ プラットフォーム ポリシーを作成する必要があります。

関連項目

- GRE について （3 ページ）
- 動的にアドレス指定されるスポークの GRE 設定について （6 ページ）
- DMVPN について （13 ページ）
- IPsec テクノロジーおよびポリシーについて

GRE およびダイナミック GRE VPN

Generic Routing Encapsulation（GRE）を使用して、ハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、完全メッシュ VPN トポロジにおいて Cisco IOS セキュリティ ルータおよび Catalyst 6500/7600 デバイスを使用する VPN を作成できます。

ここでは、次の内容について説明します。

- GRE について （3 ページ）
- IPsec GRE VPN の設定 （7 ページ）
- GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定 （8 ページ）

GRE について

Generic Routing Encapsulation（GRE）は、IP トンネルにさまざまなプロトコル パケット タイプをカプセル化し、IP ネットワーク経由でリモート ポイントのデバイスへの仮想的なポイントツーポイント接続を作成するトンネリング プロトコルです。このテクノロジーでは、GRE によって、IPsec 処理の前に元のパケット全体が標準 IP ヘッダーおよび GRE ヘッダーでカプセル化されます。その後、IPsec では、GRE パケットは通常の IP パケットであると認識されて、IKE のネゴシエーションされたパラメータに従って暗号化サービスおよび認証サービスが実行されます。GRE ではマルチキャスト トラフィックおよびブロードキャスト トラフィックを伝送できるため、仮想 GRE トンネルにルーティング プロトコルを設定できます。ルーティング プロトコルによって接続の切断が検出されると、パケットはバックアップ GRE トンネルに再ルーティングされるため、高い耐障害性が提供されます。

VPN の耐障害性を確保するためには、スポークにおいて、プライマリ ハブとバックアップ ハブへの 2 つの GRE トンネルを設定する必要があります。どちらの GRE トンネルも、IPsec によって保護されます。各トンネルは、独自の IKE Security Association（SA; セキュリティ アソシエーション）および IPsec SA のペアを持っています。関連付けられたルーティング プロトコルによって、フェールオーバー メカニズムが自動化され、仮想リンクの切断が検出されるとバックアップ トンネルに転送されます。

（注） GRE は、ハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、および完全メッシュ VPN トポロジの Cisco IOS セキュリティ ルータと Catalyst 6500/7600 デバイスに設定できます。

ここでは、次の内容について説明します。

GRE を使用した IPsec トンネリングの利点

GRE を使用した IPsec トンネリングの主な利点は次のとおりです。

- GRE では、すべての IPsec ピアが他のすべてのピアのステータスを常に把握できるルーティング プロトコルが使用されます。
- GRE では、IKE キープアライブよりも高い耐障害性が実現されます。
- GRE を使用すると、スポーク間の接続がサポートされます。
- GRE では、マルチキャスト伝送およびブロードキャスト伝送がサポートされます。

（注） GRE では、ダイナミック クリプト トンネルの使用はサポートされていません。

Security Manager における GRE の実装

Security Manager では、GRE 用に追加の Interior Gateway Protocol（IGP）ソリューションが実装されています。IGP とは、ルーティング プロトコル（EIGRP、OSPF、または RIP）によって相互にルーティング更新を受信するデバイスのグループを指しています。各「ルーティンググループ」は、論理番号によって識別されます。一般的なルーティングのために、ネットワーク内のルータのインターフェイスは 1 つの IGP に属しています。Security Manager によって、IPsec および GRE によって保護された通信専用の追加の IGP が追加されます。この追加の IGP が保護された IGP です。既存の IGP（保護されていない IGP）は、暗号化を必要としないトラフィックのルーティングに使用されます。

GRE トンネルを確立するために、Security Manager によって各デバイスに仮想インターフェイスが設定されます。これらの仮想インターフェイスは、GRE トンネルのエンドポイントとなります。それぞれの仮想インターフェイスは固有です。GRE トンネル インターフェイスには、Security Manager によって作成されるインターフェイスから取得された IP アドレス（内部トンネル IP アドレス）が設定されます。GRE トンネルは、各デバイスの物理インターフェイスまたはループバック インターフェイスのいずれかの送信元 IP アドレスおよび宛先 IP アドレスを指しています。GRE 仮想インターフェイスは、内部インターフェイスと同様に保護された IGP に属しています。保護された IGP 内でのルーティング更新は、GRE でカプセル化され、IPsec が適用されます。保護されたインターフェイス宛のフロー（保護された IGP のルーティング更新によって判断されます）は、GRE インターフェイスから送信されます。このフローは、GRE インターフェイスで GRE によってカプセル化されて、クリプト ACL に対して評価されます。クリプト ACL に一致すると、GRE および VPN トンネル経由でルーティングされます。

GRE を正常に設定するための前提条件

ネットワークで GRE を使用する前に、次の前提条件を考慮してください。

- デバイスの内部インターフェイス（デバイスを内部サブネットおよび内部ネットワークに接続するデバイス上の物理インターフェイス）を特定する必要があります。
- GRE をイネーブルにする場合は、常にルーティング プロトコル（IGP と呼ばれています）またはスタティック ルートを選択する必要があります。

Security Manager では、EIGRP、OSPF、RIPv2 というダイナミック ルーティング プロトコル、および GRE スタティック ルートがサポートされています。

- • EIGRP：Enhanced Interior Gateway Routing Protocol を使用すると、自律システム内でルーティング情報を交換でき、大規模な異種ネットワークにおけるルーティングに関連するいくつかのより困難な問題に対処できます。他のプロトコルと比較して、EIGRP にはより優れたコンバージェンス特性が備えられています。また、効率的な運用が可能で、複数の異なるプロトコルの利点を兼ね備えています。詳細については、Cisco IOS ルータにおける EIGRP ルーティングを参照してください。

- OSPF：Open Shortest Path First は、最小コストでのルーティング機能、マルチパス ルーティング機能、およびロード バランシング機能を備えた、階層型リンクステート プロトコルです。

OSPF を使用すると、ルーティング テーブルの変更を取得したホスト、またはネットワークの変更を検出したホストは、その情報をすぐにネットワーク内の他のすべてのホストにマルチキャストするため、すべてのホストが同じルーティング テーブル情報を保持できます。詳細については、Cisco IOS ルータにおける OSPF ルーティングを参照してください。

- RIPv2：Routing Information Protocol は、定期的にルーティング更新メッセージを送信する距離ベクトルプロトコルです。ネットワーク トポロジが変更された場合にもルーティング更新メッセージが送信されます。

RIPv2 を使用すると、（ルータ機能を備えた）ゲートウェイ ホストは、30 秒ごとに最も近いネイバー ホストにルーティング テーブル全体を送信します。そのネイバー ホストからも次のネイバーに情報が渡され、最終的にネットワーク内のすべてのホストに同じルーティング パス情報が渡されます。RIPv2 では、ホップ カウントを使用してネットワーク上の距離が判断されます。ネットワーク内のルータ機能を備えた各ホストは、ルーティング テーブル情報を使用して、指定した宛先へのパケットをルーティングする次のホストを判断します。

RIP は、小規模な同種ネットワークにおいて効率的なソリューションです。RIP では 30 秒ごとにルーティングテーブル全体が送信されるため、より複雑で大規模なネットワークにおいては、ネットワーク上に大量の余剰トラフィックが流れる可能性があります。詳細については、Cisco IOS ルータにおける RIP ルーティングを参照してください。

- スタティック ルート：2 つのデバイス間に固定されて変更されないルートがある場合には、スタティック ルーティング ポリシーを使用して、IPsec によって保護され、堅牢かつ安定した GRE トンネルを提供できます。各デバイスのサブネットでは、対応するトンネル インターフェイスを指すスタティック ルートがデバイスに作成されます。詳細については、Cisco IOS ルータにおけるスタティック ルーティングを参照してください。

- IGP プロセス番号を指定する必要があります。IGP プロセス番号によって、デバイスの内部インターフェイスが属する IGP プロセスが特定されます。GRE の実装時には、これは保護された IGP となります。セキュアな通信を行うために、VPN 内のデバイスの内部インターフェイスでは同じ IGP プロセスを使用する必要があります。IGP プロセス番号は、指定された範囲内である必要があります。デバイスに、この範囲内ではあるが、GRE 設定に指定された IGP プロセス番号とは異なる既存の IGP プロセスがある場合、Security Manager によって既存の IGP プロセスが削除されます。GRE 設定に指定された番号に一致する既存の IGP プロセスがある場合、既存の IGP プロセスに含まれ、指定された内部インターフェイスに一致しないすべてのネットワークは削除されます。

- デバイスの内部インターフェイスが、GRE 設定に指定された IGP プロセス以外の IGP プロセスを使用するように設定されている場合（つまり、インターフェイスが保護されていない IGP に属している場合）は、次の作業を行います。

- スポークの場合：GRE を設定する前に、デバイス CLI を使用して、保護されていない IGP から内部インターフェイスを手動で削除します。
- ハブの場合：ハブの内部インターフェイスが Security Manager のネットワーク アクセス ポイントとして使用されている場合は、展開時に、このインターフェイスが保護された IGP と保護されていない IGP の両方にアドバタイズされます。スポーク ピアで保護された IGP だけが使用されるようにするには、保護されていない IGP に手動で auto-summary コマンドを追加するか、またはその内部インターフェイスの保護されていない IGP を手動で削除します。

- ループバックには、一意でグローバルにルーティング可能でないサブネットを指定する必要があります。このサブネットは、GRE のループバックの実装をサポートするためにだけ使用する必要があります。ループバック インターフェイスは、Security Manager によってだけ作成、維持、および使用されます。他のいかなる目的にも使用できません。
- 保護されていない IGP ではないスタティック ルートを使用する場合は、ハブの内部インターフェイス経由のスタティック ルートをスポークに設定する必要があります。

（注） 上記の設定は、IPsec テクノロジーとして IPsec/GRE が選択されている場合に、[GRE Modes] ページで設定できます。

動的にアドレス指定されるスポークの GRE 設定について

スポークにダイナミック IP アドレスがある場合、（スポーク側で GRE トンネルによって使用される）固定の GRE トンネル ソース アドレスまたは（ハブ側で GRE トンネルによって使用される）送信先アドレスはありません。そのため、Security Manager によってハブおよびスポークに追加のループバック インターフェイスが作成されて、GRE トンネル エンドポイントとして使用されます。Security Manager がループバック インターフェイスの IP アドレスを割り当てることのできるサブネットを指定する必要があります。

（注） GRE ダイナミック IP は、ハブアンドスポーク VPN トポロジの Cisco IOS ルータおよび Catalyst 6500/7600 デバイスにだけ設定できます。

Security Manager は、Cisco Configuration Engine を使用して、動的にアドレス指定されるデバイスからデバイスの IP アドレスやその他の情報を取得します。ダイナミック IP アドレスを持つデバイスは定期的に Configuration Engine マネージャに接続して、デバイス設定ファイルをアップグレードし、デバイス情報およびステータス情報を渡します。

詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除を参照してください。

（注） GRE ダイナミック IP 設定は、IPsec テクノロジーとして GRE ダイナミック IP が選択されている場合に、[GRE Modes] ページで設定できます。

関連項目

- GRE について （3 ページ）
- DMVPN の [GRE Modes] の設定 （16 ページ）

IPsec GRE VPN の設定

IPsec Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）VPN を設定するには、エクストラネット VPN の作成または編集の説明に従って [Create VPN] ウィザードを使用します。説明されている手順を使用して、VPN のメンバーシップ、またはそのポリシーの一部を編集することもできます。動的にアドレス指定されたスポークを使用してハブアンドスポーク VPN を作成する場合は、 動的にアドレス指定されるスポークの GRE 設定について （6 ページ）も参照してください。

他のポリシーや設定を変更する必要がある場合は、[Site-to-Site Manager] ページで次のようにポリシーを開きます。

- ISAKMP および IPSec 設定の場合は、[VPNグローバル設定（VPN Global Settings）] を選択します。VPN グローバル設定を参照してください。
- IKE プロポーザルポリシーの場合は、[IKEプロポーザル（IKE Proposal）] を選択します。IKE プロポーザルの設定を参照してください。
- IPSec プロポーザルの場合は、[IPsecプロポーザル（IPsec Proposal）] を選択します。サイト間 VPN での IPsec プロポーザルの設定を参照してください。
- 事前共有キーポリシーの場合は、[IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。IKEv1 事前共有キー ポリシーの設定を参照してください。
- 公開キー（PKI）ポリシーの場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] を選択します。サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定を参照してください。
- 総称ルーティングカプセル化の設定では、[GREモード（GRE Modes）] を選択します。DMVPN の [GRE Modes] の設定 （16 ページ） を参照してください。

関連項目

- IKE について
- GRE について （3 ページ）
- GRE を正常に設定するための前提条件 （4 ページ）

• GRE を使用した IPsec トンネリングの利点 （3 ページ）

GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定

[GRE Modes] ポリシーを使用して、GRE または GRE ダイナミック IP VPN で IPsec トンネリングのルーティング パラメータおよびトンネル パラメータを定義します。

[GRE Modes] ポリシーを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ）[IPsec/GRE] または [GREダイナミックIP（GRE Dynamic IP）] トポロジを選択して、ポリシーリストから [GREモード（GRE Modes）] を選択します。
- （ポリシービュー）[サイト間VPN（Site-to-Site VPN）] > [GREモード（GRE Modes）] を選択して、新しいポリシーを作成するか、既存のポリシーを選択します。その後、[GRE メソッド（GRE Method）] リストから [IPsec/GRE] または [ダイナミックGRE（Dynamic GRE）] のいずれかを選択します。

次の表に、GRE または GRE ダイナミック IP に IPsec トンネリングを設定するための [GRE Modes] ページの要素を示します。

（注） GRE ルーティング ポリシーを設定する場合、Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、同じルーティング プロトコルと、[GRE Modes] ポリシーで定義した自律システム（またはプロセス ID）番号を使用して（各メンバー デバイスで）ルータ プラットフォーム ポリシーを作成する必要があります。

表 *1: GRE* または *GRE* ダイナミック *IP VPN* の *[GRE Modes]* ページ

要素	説明
[Routing Parameters] タブ	
ルーティング プロトコル（Routing Protocol）	GRE または GRE ダイナミック IP に使用する、必要なダイナミック ルーティング プロトコル（EIGRP、OSPF、または RIPv2）、あるいはスタティック ルートを選択します。 デフォルトのルーティング プロトコルは EIGRP です。 これらのプロトコルの設定の詳細については、GRE を正常に設定するための前提条件 （4 ページ）を参照してください。

要素	説明
AS 番号（AS Number） （EIGRP だけ）	EIGRP パケットが属する自律システム（AS）領域の識別に使用する数値。範囲は 1 ～ 65535 です。デフォルトは 110 です。 自律システム（AS）は、共通のルーティング ストラテジを共有するネットワークのコレクションです。AS は、連続したネットワークおよび接続ホストのグループであるいくつかの領域に分割できます。複数のインターフェイスがあるルータは、複数の領域に参加できます。AS ID は、パケットが属する領域を識別します。すべての EIGRP パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ AS 番号が必要です。
Hello 間隔（Hello Interval） （EIGRP だけ）	インターフェイスで送信される hello パケットの間隔を 1 ～ 65535 秒の間で指定します。デフォルトは 5 秒です。
保留時間（Hold Time） （EIGRP だけ）	ルータが接続を無効化する前に hello メッセージの受信を待機する秒数。範囲は 1 ～ 65535 です。デフォルトのホールド時間は 15 秒（hello の間隔の 3 倍）です。
遅延 （EIGRP だけ）	プライマリ ルート インターフェイスのスループット遅延（マイクロ秒単位）。トンネル遅延時間の範囲は 1 ～ 16777215 です。デフォルトは 1000 です。
Failover Delay （EIGRP だけ）	フェールオーバー ルート インターフェイスのスループット遅延（マイクロ秒単位）。トンネル遅延時間の範囲は 1 ～ 16777215 です。デフォルト値は 1500 です。
帯域幅 （EIGRP だけ）	プライマリ ルート インターフェイスで EIGRP パケットに使用可能な帯域幅の量。プライマリ ルートが他のルートよりも優先されるように値を入力する必要があります。 1 ～ 10000000 kb の値を入力できます。デフォルトは 1000 kb です。 （注） デフォルトでは、インターフェイスでパケットを送信する場合のコストは帯域幅に基づいて計算されます。帯域幅が広いほど、コストは低くなります。
Failover Bandwidth （EIGRP だけ）	フェールオーバー ルート インターフェイスで EIGRP パケットに使用可能な帯域幅の量。 1 ～ 10000000 kb の値を入力します。デフォルトは 1000 kb です。

要素	説明
Process Number （OSPF だけ）	Security Manager が GRE の設定時に追加する保護された IGP の識別に使用されるルーティング プロセス ID 番号。 範囲は 1 ～ 65535 です。デフォルトは 110 です。 Security Manager によって、IPsec および GRE によって保護された通信専用の追加の Interior Gateway Protocol（IGP）が追加されます。IGP とは、ルーティング プロトコルによって相互にルーティング更新を受信するデバイスのグループを指しています。各「ルーティンググループ」は、プロセス番号によって識別されます。 詳細については、GRE について （3 ページ）を参照してください。
Hub Network Area ID （OSPF だけ）	トンネルサブネットを含めて、ハブの保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を指定できます。デフォルトは 0 です。
Spoke Protected Network Area ID （OSPF だけ）	トンネル サブネットを含め、リモート保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を指定できます。デフォルトは 1 です。
認証 （OSPF または RIPv2 だけ）	OSPF または RIPv2 認証キーを指定する文字列。文字列は最大 8 文字の長さにすることができます。
コスト（Cost） （OSPF または RIPv2 だけ）	プライマリ ルート インターフェイスでのパケットの送信コスト。 選択したプロトコルが OSPF の場合は、1 ～ 65535 の範囲の値を入力します。デフォルトは 100 です。 選択したプロトコルが RIPv2 の場合は、1 ～ 15 の範囲の値を入力します。デフォルトは 1 です。
Failover Cost （OSPF または RIPv2 だけ）	セカンダリ（フェールオーバー）ルート インターフェイスでのパケットの送信コスト。 OSPF では 1 ～ 65535 の値（デフォルトは 125）を、RIPv2 では 1 ～ 15 の値（デフォルトは 2）を入力できます。
Filter Dynamic Updates on Spokes	選択されている場合、スポークにおけるすべてのダイナミック ルーティング更新をフィルタリングする再配布リストの作成がイネーブルになります。これにより、スポーク デバイスは他の IP アドレスではなく固有の保護サブネットだけをアドバタイズ（ハブ デバイスで読み込み）するよう強制されます。
[Tunnel Parameters] タブ	

要素	説明
Tunnel IP	GRE または GRE ダイナミック IP トンネル インターフェイスの IP アドレスを指定する必要なオプションを選択します。 • [物理インターフェイスを使用（Use Physical Interface）]：選択されている場合、保護ネットワークから取得されたトンネルのプライベート IP アドレスが使用されます。 • [サブネットを使用（Use Subnet）]：選択されている場合、IP 範囲から取得されたトンネルIPアドレスが使用されます。これがデフォルトです。 [Subnet] フィールドに、一意のサブネット マスクを含むプライベート IP アドレスを入力します（デフォルトは 1.1.1.0/24 です）。 ダイヤル バックアップ インターフェイスも設定する場合は、用意された [Dial Backup Subnet] フィールドにそのサブネットを入力します（デフォルトは 1.1.2.0/24 です）。 （注） ほとんどの場合、サブネットを使用して GRE トンネル インターフェイスの IP アドレスを指定すると、Security Manager によって、トンネルの IP アドレスに使用されるループバック インターフェイスがデバイスに作成されます。Security Manager によって設定が検出された VPN トポロジにデバイスが属しており、デバイスの GRE トンネルに直接 IP アドレスを設定する場合は、Security Manager によってその設定が維持されて、デバイスにループバック インターフェイスは作成されません。ただし、VPN トポロジ内のハブには常にループバックが設定されます。複数のハブがあるハブアンドスポーク VPN トポロジでは、スポークにもループバック インターフェイスが設定されます。 • [ループバックインターフェイスを使用（Use Loopback Interface）]：選択されている場合、既存のループバック インターフェイスから取得されたトンネルIPアドレスが使用されます。[ロール（Role）] フィールドに、ループバック インターフェイス名を定義するインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、新しいオブジェクトを作成します。 （注） 新しい GRE トンネルまたはループバック インターフェイスを [Router Interfaces] ページに表示するには、VPN をデバイスに正常に展開したあとでデバイス インベントリの詳細を再検出する必要があります。

要素	説明
Configure Unique Tunnel Source for each Tunnel	イネーブルになっている場合、VPN の各 GRE トンネル インターフェイスに一意のトンネル ソースが割り当てられます。[トンネルソースのIP範囲（Tunnel Source IP Range）] フィールドに、トンネルソースとして使用するサブネット IP を入力します。 （注） イネーブルになっている場合、この機能は、VPN 内のすべての GRE トンネル インターフェイスに設定されます。1 つのインターフェイスに特定のトンネル ソースを割り当てる場合は、Peers ポリシーを使用して、目的のデバイスにエンドポイントを設定します。エンドポイントおよび保護対象ネットワークの定義を参照してください。
Tunnel Source IP Range （GRE ダイナミック IP だけ）	一意のサブネット マスクを含む、GRE のループバックをサポートするプライベート IP アドレス。GRE トンネル インターフェイスの IP アドレス（内部トンネル IP アドレス）は、Security Manager がループバック専用に作成するループバック インターフェイスから取得されます。 スポークにダイナミック IP アドレスがある場合、（スポーク側で GRE トンネルによって使用される）固定の GRE トンネル ソース アドレスまたは（ハブ側で GRE トンネルによって使用される）送信先アドレスはありません。そのため、Security Manager によってハブおよびスポークに追加のループバック インターフェイスが作成されて、GRE トンネル エンドポイントとして使用されます。Security Manager がループバック インターフェイスの IP アドレスを割り当てることのできるサブネットを指定する必要があります。
Enable IP Multicast	選択されている場合は、GRE トンネル間でマルチキャスト送信をイネーブルにします。IP マルチキャストは、最小限のネットワーク帯域幅を使用して、送信元または受信側に負荷をかけることなく複数の受信側にアプリケーション ソース トラフィックを配信します。
ランデブー ポイント	[Enable IP Multicast] チェックボックスをオンにした場合にだけ使用可能です。 必要に応じて、マルチキャスト送信のランデブー ポイント（RP）として機能するインターフェイスの IP アドレスを入力できます。送信元は RP にトラフィックを送信します。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。

ダイナミック マルチポイント VPN（DMVPN）

Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）とは、Generic Routing Encapsulation（GRE）トンネル、IP Security（IPsec; IP セキュリティ）暗号化、および Next Hop Resolution Protocol（NHRP）ルーティングを組み合わせることによって、大規模および小規模

な IPsec VPN におけるスケーラビリティを向上できるハブアンドスポーク VPN テクノロジーです。

ここでは、次の内容について説明します。

DMVPN について

Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）では、Generic Routing Encapsulation（GRE）トンネル、IP Security（IPsec; IP セキュリティ）暗号化、および Next Hop Resolution Protocol（NHRP）ルーティングを組み合わせることによって、大規模および小規模な IPsec VPN におけるスケーラビリティを向上できます（大規模 DMVPN の詳細については、大規模 DMVPN の設定 （21 ページ）を参照してください）。

Security Manager では、EIGRP、OSPF、RIPv2 というダイナミック ルーティング プロトコル、および GRE スタティック ルートを使用する DMVPN がサポートされています。On-Demand Routing（ODR; オンデマンド ルーティング）もサポートされています。ODR は、ルーティング プロトコルではありません。ハブアンドスポーク VPN トポロジにおいて、スポーク ルータがハブ以外の他のルータに接続していない場合に使用できます。ダイナミック プロトコルを実行しているネットワーク環境では、ODR は適していません。

DMVPN は、ハブアンドスポーク VPN トポロジにおいて、Cisco IOS ソフトウェア リリース 12.3T デバイス以降を実行するデバイス、または Cisco IOS XE ソフトウェア 2.x 以降（Security Manager では 12.2(33)XNA+ と呼ばれています）を実行する ASR だけで使用できます。DMVPN は、Catalyst VPN サービス モジュール デバイス、またはハイ アベイラビリティ（HA）グループではサポートされていません。デバイスで DMVPN がサポートされていない場合は、GRE ダイナミック IP を使用して、動的にアドレス指定されるスポークに GRE を設定します。動的にアドレス指定されるスポークの GRE 設定について （6 ページ）を参照してください。

次のトピックでは、DMVPN の概要について説明します。

Cisco.com の次のマニュアルには、DMVPN の詳細が記載されています。

- 『*Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications*』：DMVPN テクノロジーおよびこのテクノロジーを使用する場所と理由が説明されています。このデータ シートでは、DMVPN とともに使用されるテクノロジー、およびこれらのテクノロジーによって得られる利点について説明します。

- 『*Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3*』：フェーズ 2 およびフェーズ 3 のスポーク間接続の違いが説明されています。スポーク間接続の作成は、DMVPN での設定オプションです。フェーズ 3 では、ショートカット スイッチングという拡張機能を使用して、ネットワークのパフォーマンスとスケーラビリティを向上できます。
- 追加のホワイトペーパーとプレゼンテーションは、http://www.cisco.com/en/US/products/ps6658/prod_literature.html で入手できます。

DMVPN トポロジでのスポーク間接続のイネーブル化

DMVPN を使用して、従来のハブアンドスポーク接続が、スポーク間に動的に作成された直接の IPsec トンネルによって補われる完全メッシュ VPN を実質的に作成できます。直接のスポーク間トンネルでは、リモート サイト間のトラフィックは、ハブを通過する必要はありません。これによって、追加の遅延がなくなり、WAN 帯域幅を節約できます。スポーク間機能は、シングルハブまたはマルチハブ環境でサポートされます。マルチハブ展開では、スポーク間の復元力と冗長性が向上します。

80:20 トラフィック ルールを使用して、基本のハブアンドスポーク トポロジを使用するか、直接のスポーク間接続を許可するかを判別できます。

- スポークからの 80 % 以上のトラフィックをハブ ネットワーク自体に転送する場合は、ハブアンドスポーク モデルを展開します。
- 20 % を超えるトラフィックが他のスポーク用である場合は、スポーク間モデルを検討します。

IP マルチキャスト トラフィックが大量にあるネットワークでは、通常ハブアンドスポーク モデルが推奨されます。

DMVPN の [GRE Modes] ポリシーを設定する場合は、これらの直接接続を作成するためにスポークを許可することを選択できます。これらの接続に使用する DMVPN フェーズを選択する必要があります。

- [フェーズ2（Phase 2）]：スポーク間接続はリージョナルハブを通過し、ハブからスポークへのルーティングプロトコル更新はサマライズされません。
- [フェーズ3（Phase 3）]（デフォルト）：スポークは、相互の直接接続を作成でき、ハブからスポークへのルーティング更新はサマライズされます。このオプションを使用すると、スケーラビリティが最大になり、遅延が低減されます。デバイスは IOS ソフトウェア リリース 12.4(6)T 以降を実行している必要があります。ASR は IOS XE ソフトウェア リリース 2.4（12.2(33)XND と呼ばれる）以降を実行している必要があります。Security Manager は、それより低い OS バージョンが実行されているデバイスではフェーズ 2 設定を自動的に作成します。

[GRE Modes] ポリシーの設定に関する詳細については、DMVPN の [GRE Modes] の設定 （16 ページ）を参照してください。

関連項目

- DMVPN について （13 ページ）
- 『*Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications*』
- 『*Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3*』

DMVPN を使用した GRE の利点

DMVPN を使用した GRE には、次の利点があります。

- **ハブにおける GRE 設定の簡素化**

GRE では、ハブにおいて、接続された各スポークに対してトンネルが設定されます。GRE と DMVPN を使用すると、すべての接続されたスポークに対してトンネルが 1 つだけ設定されます。

- **動的にアドレス指定されるスポークのサポート**

GRE を使用する場合、ハブ ルータを設定するときに、スポーク ルータの物理インターフェイス IP アドレスを GRE トンネルの宛先アドレスとして設定する必要があります。DMVPN を使用すると、スポーク ルータに動的な外部インターフェイス IP アドレスを設定できます。また、外部インターフェイス IP アドレスが変更された場合でも設定をデバイスに再展開する必要がなく、設定が堅固になります。スポークがオンラインになると、スポークの物理インターフェイス IP アドレスが含まれた登録パケットをハブに対して送信します。

- **直接のスポーク間通信用のダイナミック トンネルの作成**

NHRP では、スポーク ルータは、VPN ネットワーク内のルータの外部インターフェイス IP アドレスを動的に学習できます。NHRP を使用すると、ハブにすべてのスポーク（クライアント）のパブリック インターフェイス アドレスの NHRP データベースが保持されます。各スポークは、起動時にハブに対してスポークの実際のアドレスを登録します。

スポークは、他のスポークにパケットを送信する必要がある場合、NHRP を使用して、宛先スポークの必要な宛先アドレスを動的に決定できます。ハブは、送信元スポークの要求を処理する NHRP サーバとして動作します。これにより、ハブ ルータを経由せずにスポーク ルータ間で直接の IPsec および GRE トンネルを動的に作成でき、それによりハブにおいて複数回暗号化と復号化を繰り返すことによる遅延を低減できます。

DMVPN の設定

ハブアンドスポーク ダイナミック マルチポイント VPN を設定するには、VPN トポロジの作成または編集の説明に従って [Create VPN] ウィザードを使用します。説明されている手順を使用して、VPN のメンバーシップ、またはそのポリシーの一部を編集することもできます。大規模 DMVPN を作成する場合は、 大規模 DMVPN の設定 （21 ページ）も参照してください。

他のポリシーや設定を変更する必要がある場合は、[Site-to-Site Manager] ページで次のようにポリシーを開きます。

- ISAKMP および IPSec 設定の場合は、[VPNグローバル設定（VPN Global Settings）] を選択します。VPN グローバル設定を参照してください。
- IKE プロポーザルポリシーの場合は、[IKEプロポーザル（IKE Proposal）] を選択します。IKE プロポーザルの設定を参照してください。
- IPSec プロポーザルの場合は、[IPsecプロポーザル（IPsec Proposal）] を選択します。サイト間 VPN での IPsec プロポーザルの設定を参照してください。
- 事前共有キーポリシーの場合は、[IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。IKEv1 事前共有キー ポリシーの設定を参照してください。
- 公開キー（PKI）ポリシーの場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] を選択します。サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定を参照してください。
- スポーク間のフェーズ 2 または 3 接続の選択を含め、Generic Routing Encapsulation の設定では、[GREモード（GRE Modes）] を選択します。 DMVPN の [GRE Modes] の設定 （16 ページ）を参照してください。
- 大規模 DMVPN とともに使用するサーバー ロードバランシング ポリシーでは、[サーバーロードバランシング（Server Load Balance）] を選択します。 大規模 DMVPN でのサーバ ロード バランシングの設定 （22 ページ） を参照してください。

関連項目

- IKE について
- DMVPN について （13 ページ）
- DMVPN トポロジでのスポーク間接続のイネーブル化 （14 ページ）
- DMVPN を使用した GRE の利点 （15 ページ）

DMVPN の [GRE Modes] の設定

[GRE Modes] ポリシーを使用して、DMVPN で IPsec トンネリングのルーティング パラメータおよびトンネル パラメータを定義します。

[GRE Modes] ポリシーを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ）[DMVPN] または [大規模DMVPN（Large Scale DMVPN）] トポロジを選択して、ポリシーリストから [GREモード（GRE Modes）] を選択します。
- （ポリシービュー）[サイト間VPN（Site-to-Site VPN）] > [GREモード（GRE Modes）] を選択して、新しいポリシーを作成するか、既存のポリシーを選択します。その後、[GRE メソッド（GRE Method）] リストから [DMVPN] または [大規模DMVPN（Large Scale DMVPN）] のいずれかを選択します。

次の表に、DMVPN を設定するための [GRE Modes] ページの要素を示します。

（注） DMVPN ルーティング ポリシーを設定する場合、Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、同じルーティング プロトコルと、[GRE Modes] ポリシーで定義した自律システム（またはプロセス ID）番号を使用して（各メンバー デバイスで）ルータ プラットフォーム ポリシーを作成する必要があります。

表 2 : [DMVPN] の [GRE Modes] ページ

要素	説明
[Routing Parameters] タブ	
ルーティング プロトコル（Routing Protocol）	DMVPN トンネルで使用する、必要なダイナミック ルーティング プロトコルまたはスタティック ルートを選択します。 オプションには、EIGRP、OSPF、RIPv2 というダイナミック ルーティング プロトコル、および GRE スタティック ルートがあります。On-Demand Routing（ODR; オンデマンド ルーティング）もサポートされています。オンデマンド ルーティングは、ルーティング プロトコルではありません。ハブアンドスポーク VPN トポロジにおいて、スポーク ルータがハブ以外の他のルータに接続していない場合に使用できます。ダイナミック プロトコルを実行しているネットワーク環境では、オンデマンド ルーティングは適していません。 詳細については、GRE について （3 ページ）を参照してください。
AS 番号（AS Number） （EIGRP だけ）	EIGRP パケットが属する自律システム（AS）領域の識別に使用する数値。範囲は 1 ～ 65535 です。デフォルトは 110 です。 自律システム（AS）は、共通のルーティング ストラテジを共有するネットワークのコレクションです。AS は、連続したネットワークおよび接続ホストのグループであるいくつかの領域に分割できます。複数のインターフェイスがあるルータは、複数の領域に参加できます。AS ID は、パケットが属する領域を識別します。すべての EIGRP パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ AS 番号が必要です。
Hello 間隔（Hello Interval） （EIGRP だけ）	インターフェイスで送信される hello パケットの間隔を 1 ～ 65535 秒の間で指定します。デフォルトは 5 秒です。
保留時間（Hold Time） （EIGRP だけ）	ルータが接続を無効化する前に hello メッセージの受信を待機する秒数。範囲は 1 ～ 65535 です。デフォルトのホールド時間は 15 秒（hello の間隔の 3 倍）です。

要素	説明
遅延 （EIGRP だけ）	プライマリ ルート インターフェイスのスループット遅延（マイクロ秒単位）。トンネル遅延時間の範囲は 1 ～ 16777215 です。デフォルトは 1000 です。
Bandwidth （EIGRP だけ）	プライマリ ルート インターフェイスの帯域幅（キロビット単位）。帯域幅の範囲は 1 ～ 10000000 です。デフォルトは 1000 です。
Bandwidth （EIGRP だけ）	プライマリ ルート インターフェイスで EIGRP パケットに使用可能な帯域幅の量。プライマリ ルートが他のルートよりも優先されるように値を入力する必要があります。 1 ～ 10000000 kb の値を入力できます。デフォルトは 1000 kb です。 （注） デフォルトでは、インターフェイスでパケットを送信する場合のコストは帯域幅に基づいて計算されます。帯域幅が広いほど、コストは低くなります。
Process Number （OSPF だけ）	Security Manager が DMVPN の設定時に追加する保護された IGP の識別に使用されるルーティング プロセス ID 番号。 いずれのプロトコルにおいても、有効な範囲は 1 ～ 65535 です。デフォルトは 110 です。
Hub Network Area ID （OSPF だけ）	トンネルサブネットを含めて、ハブの保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を入力できます。デフォルトは 0 です。
Spoke Protected Network Area ID （OSPF だけ）	トンネル サブネットを含め、リモート保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を入力できます。デフォルトは 1 です。
認証キー（Authentication Key） （OSPF と RIPv2）	OSPF または RIPv2 認証キーを指定する文字列。文字列は最大 8 文字の長さにすることができます。
コスト（Cost） （OSPF と RIPv2）	プライマリ ルート インターフェイスでのパケットの送信コスト。 選択したプロトコルが OSPF の場合は、1 ～ 65535 の範囲の値を入力します。デフォルトは 100 です。 選択したプロトコルが RIPv2 の場合は、1 ～ 15 の範囲の値を入力します。デフォルトは 1 です。

要素	説明
Allow Direct Spoke to Spoke Connectivity	ハブを経由せずにスポーク間で直接通信を可能にするかどうか。使用する DMVPN フェーズを選択します。これにより、スポークが行うことができる接続のタイプが決定されます。 • [フェーズ2（Phase 2）]：スポーク間接続はリージョナルハブを通過し、ハブからスポークへのルーティングプロトコル更新はサマライズされません。 • [フェーズ3（Phase 3）]（デフォルト）：スポークは、相互の直接接続を作成でき、ハブからスポークへのルーティング更新はサマライズされます。このオプションを使用すると、スケーラビリティが最大になり、遅延が低減されます。デバイスは IOS ソフトウェアリリース 12.4(6)T 以降を実行している必要があります。ASR は IOS XE ソフトウェアリリース 2.4（12.2(33)XND と呼ばれる）以降を実行している必要があります。Security Manager は、それより低い OS バージョンが実行されているデバイスではフェーズ 2 設定を自動的に作成します。 フェーズ 2 と 3 の違いの詳細については、Cisco.com の『Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3』を参照してください。 （注） 直接のスポーク間通信を使用する場合は、事前共有キー ネゴシエーションで [Main Mode Address] オプションを使用する必要があります。詳細については、サイト間 VPN での IKEv1 事前共有キー ポリシーについてを参照してください。
Filter Dynamic Updates On Spokes	DMVPN トンネルでオンデマンドルーティングまたはスタティック ルートを使用している場合には使用できません。 選択されている場合、スポークにおけるすべてのダイナミック ルーティング更新（EIGRP、OSPF、および RIPv2）をフィルタリングする再配布リストの作成がイネーブルになります。これにより、スポーク デバイスは他の IP アドレスではなく固有の保護サブネットだけをアドバタイズ（ハブ デバイスで読み込み）するよう強制されます。
[Tunnel Parameters] タブ	
Tunnel IP Range	一意のサブネット マスクを含む、内部トンネル インターフェイスの IP アドレスの IP アドレス範囲。このフィールドは、10.1.1.0/24 などのサブネットを定義します。 （注） トンネルインターフェイスの IP アドレスがデバイスにすでに存在すること、およびその IP アドレスがトンネルの IP サブネットのフィールドに一致することが Security Manager によって検出された場合は、そのインターフェイスが GRE トンネルとして使用されます。

要素	説明
Dial Backup Tunnel IP Range	ダイヤル バックアップ インターフェイスを設定する場合は、一意のサブネット マスクを含む、その内部トンネル インターフェイスの IP アドレス範囲を入力します。このフィールドはサブネットを定義します。
Server Load Balance	選択されている場合、複数のハブを使用する設定においてハブとして機能している Cisco IOS ルータでのロードバランシングの設定がイネーブルとなります。 サーバ ロード バランシングを使用すると、作業負荷を分散することによって、複数のハブを使用する設定においてパフォーマンスが最適化されます。この設定では、複数の DMVPN サーバ ハブが同じトンネル IP および送信元 IP アドレスを共有し、VPN トポロジのスパイクによって単一のデバイスのように認識されます。
Enable IP Multicast	選択されている場合は、GRE トンネル間でマルチキャスト送信をイネーブルにします。 IP マルチキャストは、最小限のネットワーク帯域幅を使用して、送信元または受信側に負荷をかけることなく複数の受信側にアプリケーション ソース トラフィックを配信します。
ランデブー ポイント	[Enable IP Multicast] チェックボックスをオンにした場合にだけ使用可能です。 必要に応じて、マルチキャスト送信のランデブー ポイント（RP）として機能するインターフェイスの IP アドレスを入力できます。送信元は RP にトラフィックを送信します。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。
トンネル キー（Tunnel Key）	トンネル キーを示す番号。デフォルトは 1 です。 トンネル キーは、multipoint GRE（mGRE; マルチポイント GRE）トンネル Non Broadcast Multiple Access（NBMA; 非ブロードキャスト マルチアクセス）ネットワークごとに異なります。同じ NBMA ネットワーク内のすべての mGRE インターフェイスでは同じトンネル キーの値を使用する必要があります。同じルータに 2 つの mGRE インターフェイスがある場合、これらのインターフェイスでは異なるトンネル キーの値を使用する必要があります。 （注） 新規に作成したトンネル インターフェイスを、VPN のメンバーであるルータの [Router Interfaces] ページに表示するには、VPN をデバイスに正常に展開したあとでデバイス インベントリの詳細を再検出する必要があります。
NHRP Parameters	

要素	説明
ネットワーク ID（Network ID）	1 つの論理 Non-Broadcast Multi-Access（NBMA; 非ブロードキャスト マルチアクセス）ネットワーク内のすべての Next Hop Resolution Protocol（NHRP）ステーションには、同じネットワーク ID を設定する必要があります。1 ～ 4294967295 の範囲の、グローバルに一意な 32 ビットのネットワーク ID を入力します。
保留時間	正規の NHRP 応答に指定されている情報をルータで保持する時間（秒数）。ホールド時間を経過すると、キャッシュされた IP から NBMA へのアドレス マッピング エントリは廃棄されます。 デフォルトは 300 秒です。
認証	送信元および宛先 NHRP ステーション間で相互に通信できるかどうかを制御する認証文字列。NHRP を使用している同じネットワーク内のすべてのルータが同じ認証文字列を共有する必要があります。文字列は最大 8 文字の長さにすることができます。

大規模 DMVPN の設定

数千のスポークで構成される可能性がある大規模な展開について DMVPN を設定できます。大規模 DMVPN トポロジでは、Server Load Balance（SLB; サーバ ロード バランス）デバイスとも呼ばれる IPsec ターミネータがスポークとハブとの間に設置されます。ハブは、IPsec ターミネータに直接接続されている必要があり、ハブと IPsec ターミネータとの間にはその他のデバイスは設置できません。

IPsec ターミネータ（Catalyst 6500/7600 デバイス）では暗号化および復号化が実行され、ハブでは Next Hop Resolution Protocol（NHRP）および multipoint Generic Routing Encapsulation（mGRE; マルチポイント GRE）に関連するすべてのタスクが処理されます。IPsec ターミネータは、ハブへの GRE トラフィックのロード バランスを特化して行うように設定されます。また、IPsec ターミネータには、任意のプロキシを経由する任意のスポークを受け入れるようにダイナミック クリプトが設定されます。スポークでトンネル保護を使用する場合、これらのプロキシは、GRE トラフィックに一致するように自動的に設定されます。スポークには、1 つの GRE トンネルが設定されます。同じ IPsec ターミネータに接続するすべてのハブは、同じトンネル IP アドレスを使用し、トンネル ソースは IPsec ターミネータの仮想 IP アドレスとなります。

Security Manager では、VPN トポロジの作成または編集の説明に従って、新規ハブアンドスポーク VPN トポロジの作成中に大規模 DMVPN を設定します。既存の標準の DMVPN は編集できず、大規模 DMVPN に変換できません。大規模 DMVPN を作成する場合は、次の点に注意してください。

- VPN のテクノロジーを定義する場合は、テクノロジーとして [DMVPN]、タイプとして [IPsecターミネータを使用した大規模型（Large Scale with IPsec Terminator）] を選択します。手順については、VPN トポロジの名前および IPsec テクノロジーの定義を参照してください。

- VPN のデバイスを選択する場合は、必要な IPsec ターミネータ（Catalyst 6500/7600 デバイス）、ハブ、およびすべてのスポークを選択します。手順については、VPN トポロジのデバイスの選択を参照してください。

IPsec ターミネータとハブは直接接続されている必要があります。

- エンドポイントを設定する場合は、エンドポイントおよび保護対象ネットワークの定義の説明に従って、[Edit Endpoints] ダイアログボックスで次の項目を設定します。
  - [Hub Interface] タブで、各ハブ デバイスに対して、IPsec ターミネータに接続するインターフェイスを選択します。それぞれのハブは、1 つの IPsec ターミネータにだけ接続できます。また、保護されたネットワークを識別します。大規模 DMVPN 内の各ハブは自身と保護されたネットワークを識別する必要があります。
  - 大規模 DMVPN 内の IPsec ターミネータごとに、VPN 外部インターフェイス、暗号化エンジン スロット、および内部 VLAN を指定します。IPsec ターミネータでは、保護対象ネットワークは設定されません。

大規模 DMVPN トポロジの作成後、[Server Load Balance] ポリシーが、必要なすべてのパラメータを使用して IPsec ターミネータで設定されます。パラメータは、必要に応じて編集できます。最初に、すべてのハブに VPN 接続の同じプライオリティと番号が指定されます。[Server Load Balance] ポリシーの設定については、大規模 DMVPN でのサーバ ロード バランシングの設定（22 ページ）を参照してください。

（注） 大規模 DMVPN では、VRF 対応 IPsec は設定できません。

関連項目

- DMVPN について （13 ページ）
- DMVPN の設定 （15 ページ）

大規模 DMVPN でのサーバ ロード バランシングの設定

[Server Load Balance] ページを使用して、大規模 DMVPN 内の IPsec ターミネータに設定される Server Load Balance ポリシーを表示または編集します。サーバ ロード バランシングを使用すると、ハブのグループ間で作業負荷を共有することによって、複数のハブアンドスポーク VPN トポロジにおけるパフォーマンスが最適化されます。大規模 DMVPN 設定では、IPsec ターミネータはトラフィックのロードバランシングを実行します。詳細については、大規模 DMVPN の設定 （21 ページ）を参照してください。

Weighted Round Robin（WRR; 重み付けラウンドロビン）スケジューリング アルゴリズムを使用して、出力送信キューに割り当てられる帯域幅が制御されます。重み付けは、インターフェイスの各送信キューで使用される帯域幅の量に基づいて行われます。容量の大きいキューからのパケットは、容量の小さいキューからのパケットよりも高い頻度で送信されます。

[サーバーロードバランス（Server Load Balance）] ポリシーを開くには、[Site-to-Site VPN Manager] ウィンドウで既存の大規模 DMVPN トポロジを選択して、[ポリシー（Policies）] リストから [サーバーロードバランス（Server Load Balance）] を選択します。

表には、VPN 内のハブ、同じ IPsec ターミネータに接続されているその他のハブに対するハブの相対的な重量、ハブで許可されるアクティブな接続の最大数が表示されます。重量または最大接続を変更するには、ハブを選択して、表の真下にある [Edit]（鉛筆）ボタンをクリックして、[Edit Load Balancing Parameters] ダイアログボックス （23 ページ）を開きます。

関連項目

- 大規模 DMVPN の設定 （21 ページ）
- テーブルのフィルタリング

[Edit Load Balancing Parameters] ダイアログボックス

大規模 DMVPN において IPsec ターミネータに接続されているハブに設定されたサーバ ロード バランス パラメータを変更するには、[Edit Load Balancing Parameters] ダイアログボックスを使用します。

ナビゲーション パス

[Server Load Balance] ポリシーで、ハブを選択して、表の下にある **[Edit]（鉛筆）**ボタンをクリックします。[Server Load Balance] ポリシーを開く方法については、大規模 DMVPN でのサーバ ロード バランシングの設定 （22 ページ）を参照してください。

関連項目

- 大規模 DMVPN の設定 （21 ページ）

フィールド リファレンス

表 3 : [Edit Load Balancing Parameters] ダイアログボックス

要素	説明
重量	Weighted Round Robin（WRR; 重み付けラウンドロビン）スケジューリング アルゴリズムに基づいて、IPsec ターミネータに接続されている他のハブに対する、ハブの相対的な容量。 1 ～ 255 の値を入力できます。デフォルトは 1 です。
最大接続数（Max Connections）	ハブから IPsec ターミネータに対して許可されるアクティブな接続の最大数。 1 ～ 65535 の値を入力できます。デフォルトは 500 です。

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。