サイト間 VPN の管理：基本

バーチャルプライベートネットワーク（VPN）は、インターネットなどのセキュアでないネットワーク経由で相互にプライベート データを安全に送信する、複数のリモート ピアで構成されています。サイト間 VPN は、トンネルを使用してデータ パケットを通常の IP パケット内でカプセル化し、IP ベースのネットワーク経由で転送するものです。その際、暗号化を使用してプライバシーを確保し、認証を使用してデータの整合性を確保します。

Cisco Security Manager では、サイト間 VPN は、VPN トポロジに割り当てられた IPsec ポリシーに基づいて実装されています。IPsec ポリシーとはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。Security Manager は、IPsec ポリシーを、VPN トポロジ内のデバイスに展開可能な CLI コマンドに変換します。IPsec テクノロジーのタイプによっては、VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

Site-to-Site VPN Manager では、Cisco IOS セキュリティ ルータ、PIX ファイアウォール、Catalyst VPN サービス モジュール、および Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）ファイアウォール デバイスにサイト間 VPN トポロジおよびポリシーが定義されて設定されます。

ヒント ASA の資料では、サイト間 VPN は LAN-to-LAN VPN と呼ばれています。これらの用語は同義語であり、この資料では「サイト間 VPN」を使用します。

Site-to-Site VPN Manager にアクセスするには、**[管理（Manage）] > [サイト間VPN（Site-to-Site VPNs）]** を選択するか、またはツールバーの [Site-to-Site VPN Manager] ボタンをクリックします。

また、ポリシー ビューでの共有ポリシーの設定や、デバイス ビューでのトポロジの表示および設定も可能です。ポリシー ビューでは、IPsec ポリシーを VPN トポロジに割り当てることができます。

この章は次のトピックで構成されています。

- VPN トポロジについて （2 ページ）
- IPsec テクノロジーおよびポリシーについて （6 ページ）

• サイト間 VPN トポロジおよびポリシーへのアクセス （25 ページ）
• サイト間 VPN ディスカバリ （28 ページ）
• VPN トポロジの作成または編集 （38 ページ）
• エクストラネット VPN の作成または編集 （90 ページ）
• VPN トポロジの削除 （95 ページ）

VPN トポロジについて

VPN トポロジでは、その VPN に属するピアとネットワーク、およびそれらの間の接続方法が指定されます。VPN トポロジを作成したあと、割り当てられた IPsec テクノロジーに応じて、VPN トポロジに適用可能なポリシーが設定に使用できるようになります。

Security Manager では、ハブアンドスポーク、ポイントツーポイント、完全メッシュという 3 種類の主要なトポロジがサポートされており、これらを使用してサイト間 VPN を作成できます。すべてのポリシーをすべての VPN トポロジに適用できるわけではありません。適用できるポリシーは、VPN トポロジに割り当てられた IPsec テクノロジーに応じて異なります。また、VPN に割り当てられる IPsec テクノロジーは、トポロジタイプに応じて異なります。たとえば、DMVPN および Easy VPN テクノロジーは、ハブアンドスポーク トポロジにだけ適用できます。

詳細については、IPsec テクノロジーおよびポリシーについて （6 ページ）を参照してください。

ここでは、次の内容について説明します。

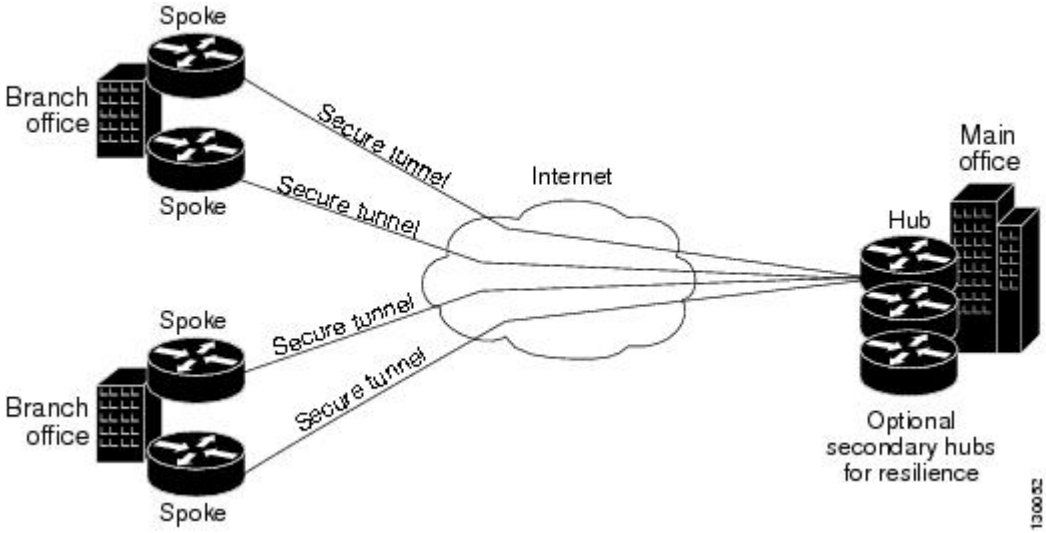
• ハブアンドスポーク VPN トポロジ （2 ページ）
• ポイントツーポイント VPN トポロジ （4 ページ）
• 完全メッシュ VPN トポロジ （4 ページ）
• 暗黙的にサポートされるトポロジ （6 ページ）

ハブアンドスポーク VPN トポロジ

ハブアンドスポーク VPN トポロジでは、複数のリモート デバイス（スポーク）が 1 つの中央のデバイス（ハブ）と安全に通信します。ハブと個別の各スポークとの間には、保護されたトンネルが個別に設定されます。

次の図に、一般的なハブアンドスポーク VPN トポロジを示します。

図 *1*：ハブアンドスポーク *VPN* トポロジ



通常、このトポロジは、サードパーティネットワークまたはインターネットへの永続的な接続を使用して、企業のメインオフィスとブランチオフィスを接続するイントラネット VPN を表しています。ハブアンドスポーク トポロジの VPN を使用することによって、どのような場所でリモートの業務を行うか、またはその規模や数に関係なく、すべての従業員が企業ネットワークに完全にアクセスできます。

ハブは、一般的には企業のメインオフィスに配置されます。スポークデバイスは、一般的には企業のブランチオフィスに配置されます。ハブアンドスポーク トポロジでは、ほとんどのトラフィックはスポーク サイトにあるホストによって開始されますが、一部のトラフィックは、セントラル サイト側で開始されてスポークに送られる場合もあります。

ハブアンドスポーク設定において何らかの理由でハブが利用できなくなると、IPsec フェールオーバーによって、すべてのスポークが使用するフェールオーバー（バックアップ）ハブにトンネル接続がシームレスに転送されます。1 台のプライマリ ハブに対して、複数のフェールオーバー ハブを設定できます。

ハブアンドスポーク VPN トポロジでは、GET VPN 以外のすべての IPsec テクノロジー タイプを割り当てることができます。

関連項目

- IPsec テクノロジーおよびポリシーについて　（6 ページ）
- 暗黙的にサポートされるトポロジ　（6 ページ）
- IKE および IPsec ポリシーの設定

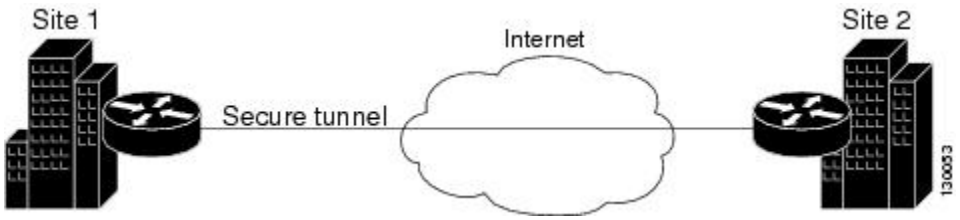
ポイントツーポイント VPN トポロジ

ポイントツーポイント VPN トポロジでは、2 つのデバイスが相互に直接通信します。ハブアンドスポーク設定の場合のような IPsec フェールオーバーのオプションはありません。ポイントツーポイント VPN トポロジを確立するためには、ピア デバイスとして 2 つのエンドポイントを指定します。これら 2 つのデバイスのどちらからでも接続を開始できるため、IPsec テクノロジー タイプとして通常の IPsec または IPsec/GRE のみを割り当てることができます。

Security Manager では、エクストラネットと呼ばれる、通常の IPsec ポイントツーポイント VPN の特殊タイプを設定できます。エクストラネット VPN は、管理対象ネットワーク内のデバイスと管理対象外デバイスの間の接続です。管理対象外デバイスは、サービスプロバイダーのネットワーク内のルータ、シスコ製以外のデバイス、または単に別のグループで管理される、ご使用のネットワーク内のデバイス（つまり、Security Manager インベントリには現れないデバイス）などです。

次の図に、一般的なポイントツーポイント VPN トポロジを示します。

図 *2:* ポイントツーポイントの *VPN* トポロジ



関連項目

- IPsec テクノロジーおよびポリシーについて （6 ページ）
- 暗黙的にサポートされるトポロジ （6 ページ）
- VPN トポロジの作成または編集 （38 ページ）
- エクストラネット VPN の作成または編集 （90 ページ）
- IKE および IPsec ポリシーの設定

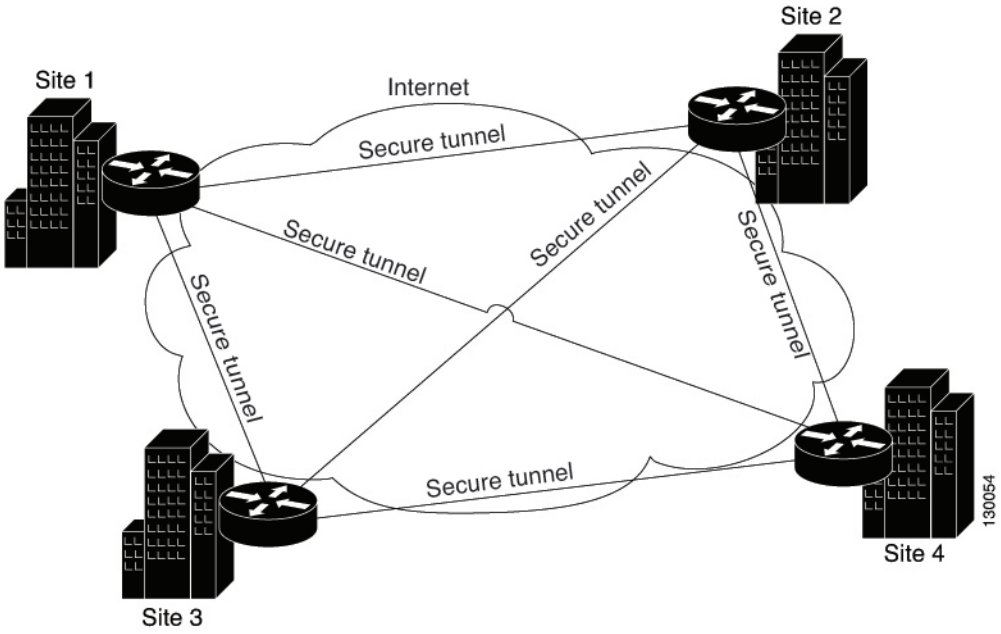
完全メッシュ VPN トポロジ

完全メッシュ トポロジは、すべてのピアが相互に通信する必要があるような複雑なネットワークに適しています。このトポロジ タイプでは、ネットワーク内のすべてのデバイスが固有の IPsec トンネルを経由して他のすべてのデバイスと通信します。すべてのデバイスが相互に直接のピア関係を持っているため、VPN ゲートウェイ デバイスでボトルネックが発生せず、デバイスにおける暗号化および復号化のオーバーヘッドを低減できます。

完全メッシュ VPN トポロジには、通常の IPsec、IPsec/GRE、および GET VPN テクノロジーだけを割り当てることができます。

次の図に、一般的な完全メッシュ VPN トポロジを示します。

図 *3:* フル メッシュ *VPN* トポロジ



完全メッシュ ネットワークは信頼性が高く、冗長性を備えています。GRE テクノロジーが割り当てられている場合は、1 つのデバイス（またはノード）が動作できなくなっても、他のすべてのデバイスは引き続き、直接または1つ以上の中間ノード経由で、相互に通信できます。通常の IPsec では、1 つのデバイスが動作できなくなった場合、保護対象のネットワークを指定するクリプト アクセス コントロール リスト（ACL）が 2 つのピアごとに作成されます。

GET VPN は、グループ トラスト モデルに基づいています。このモデルでは、グループ メンバーはキー サーバに登録されます。キー サーバは、Group Domain of Interpretation（GDOI）プロトコルを使用して、セキュリティ ポリシー、およびグループ メンバー間のトラフィックを暗号化するためのキーを配布します。プライマリ キー サーバと、プライマリ サーバとポリシーを同期するセカンダリ キー サーバを設定できるため、プライマリ キー サーバが利用できなくなった場合にはセカンダリ キー サーバが処理を引き継ぐことができます。

（注） 完全メッシュ トポロジ内のノード数が増加すると、スケーラビリティが問題となる可能性があります。つまり、デバイスが適度な CPU 使用率でサポートできるトンネル数が、制限要因となる可能性があります。

関連項目

- IPsec テクノロジーおよびポリシーについて （6 ページ）
- 暗黙的にサポートされるトポロジ （6 ページ）
- VPN トポロジの作成または編集 （38 ページ）

- IKE および IPsec ポリシーの設定

暗黙的にサポートされるトポロジ

3つの主要なVPNトポロジに加えて、これらのトポロジを組み合わせた他のより複雑なトポロジを作成することもできます。具体的には以下のとおりです。

- 部分メッシュ：このネットワークでは、一部のデバイスはフル メッシュ トポロジに編成され、その他のデバイスは、フルメッシュ構成のデバイスのうちのいくつかとのハブアンドスポーク接続またはポイントツーポイント接続を形成します。部分メッシュには、フル メッシュ トポロジほどの冗長性はありませんが、導入コストがより低くなります。部分メッシュ トポロジは、通常、完全メッシュ構成のバックボーンに接続する境界ネットワークで使用されます。
- 階層型ハブアンドスポーク：このネットワークでは、あるデバイスが、1 つ以上のトポロジでハブとして動作し、他のトポロジではスパイクとして動作できます。スポーク グループからそれらの直近のハブへのトラフィックが許可されます。
- 結合ハブアンドスポーク：接続して 1 つのポイントツーポイント トンネルを形成する、2 つのトポロジ（ハブアンドスポーク、ポイントツーポイント、またはフル メッシュ）の組み合わせです。たとえば、2 つのハブアンドスポーク トポロジから構成され、それぞれのハブがポイントツーポイント トポロジのピア デバイスとして動作する結合ハブアンドスポーク トポロジを作成できます。

関連項目

- VPN トポロジの作成または編集 （38 ページ）
- ハブアンドスポーク VPN トポロジ （2 ページ）
- ポイントツーポイント VPN トポロジ （4 ページ）
- 完全メッシュ VPN トポロジ （4 ページ）

IPsec テクノロジーおよびポリシーについて

Security Manager には、サイト間 VPN トポロジのデバイスに設定できる 7 種類の IPsec テクノロジーが用意されています。それらは、通常の IPsec、IPsec/GRE、GRE ダイナミック IP、標準 DMVPN、大規模 DMVPN、Easy VPN、および GET VPN です。割り当てられたテクノロジーに応じて、VPN に対して設定できるポリシーが決まります。

VPN トポロジの作成時に VPN トポロジに IPsec テクノロジーを割り当てることができます。VPN トポロジに IPsec テクノロジーを割り当てたあとは、テクノロジーを変更できません。変更する場合は、いったん VPN トポロジを削除してから新たなトポロジを作成する必要があります。 VPN トポロジの名前および IPsec テクノロジーの定義 （42 ページ）を参照してください。

ここでは、IPsec テクノロジーおよびサイト間 VPN ポリシーのいくつかの基本的な概念について説明します。

- サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （7 ページ）
- サイト間 VPN ポリシーの概要 （10 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （14 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （16 ページ）
- VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）
- デバイスのオーバーライドを使用した VPN ポリシーのカスタマイズ （20 ページ）
- VRF 対応 IPsec について （20 ページ）

サイト間 VPN の必須ポリシーおよびオプションのポリシーについて

一部のサイト間 VPN ポリシーは必須です。つまり、VPN トポロジを作成したり、ポリシー編集時に変更内容を保存したりする場合には、これらのポリシーを設定する必要があります。ほとんどの必須ポリシーには定義済みのデフォルトが用意されています。このデフォルトを使用して VPN トポロジを定義することもできますが、通常はこれらのポリシーを編集して、ご使用のネットワークに適した設定にする必要があります。

オプションのポリシーは、それらのポリシーによって定義されるサービスを必要とする場合にだけ設定する必要があり、デフォルトは用意されていません。

ヒント　必要な設定を指定した共有ポリシーを作成し、VPN 作成時にこれらの共有ポリシーを選択することによって、独自の必須ポリシーのデフォルトを設定できます。共有ポリシーを Create VPN ウィザードのデフォルトとすることもできます。ただし、これらのデフォルト ポリシーはエクストラネット VPN の作成時には適用されません。エクストラネット VPN を使用する場合、常に通常のウィザード フローの一部として必須ポリシーの設定値を設定する必要があります。さらに、IKEv2 認証のデフォルト ポリシーは作成できません。詳細については、 VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）を参照してください。

一部の必須ポリシーは、特定の条件の下でだけ必須となります。たとえば、IKEv1 Preshared Key ポリシーは、デフォルトの（必須）IKEv1 プロポーザルで事前共有キー認証を使用する場合にだけ必須となります。選択された IKE 認証方式が証明書（RSA の署名）である場合は、IKEv1 Public Key Infrastructure ポリシーが必須となります（使用する認証方式の決定を参照）。トポロジで IKEv2 ネゴシエーションを許可する場合、IKEv2 Authentication ポリシーは必須です。

次の表に、サイト間VPNトポロジ内のデバイスに割り当て可能な各定義済みテクノロジーの、必須ポリシーおよびオプションのポリシーを示します。

表 *1*：サイト間 *VPN IPsec* テクノロジーおよびポリシー

テクノロジー	必須ポリシー	オプションのポリシー
通常の IPsec サイト間 VPN の IPsec プロポーザルについてを参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 を許可する場合、IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • IKEv2 を許可する場合、IKEv2 Authentication	• VPN Global Settings
IPsec/Generic Routing Encapsulation（GRE） GRE についてを参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード	• VPN Global Settings
GRE ダイナミック IP 動的にアドレス指定されるスポークの GRE 設定についてを参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード	• VPN Global Settings
ダイナミック マルチポイント VPN（DMVPN） DMVPN についてを参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード	• VPN Global Settings
大規模 DMVPN 大規模 DMVPN の設定を参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード • Server Load Balance	• VPN Global Settings

テクノロジー	必須ポリシー	オプションのポリシー
Easy VPN Easy VPN についてを参照してください。	• IKE Proposal • Easy VPN IPsec Proposal • Client Connection Characteristics • いずれかのサーバが IOS または PIX 6.3 デバイスである場合、User Group • いずれかのサーバが ASA または PIX 7.0+デバイスである場合、Connection Profiles	• IKEv1 Public Key Infrastructure（証明書を使用している場合は必須） • VPN Global Settings
GET VPN Group Encrypted Transport（GET）VPN についてを参照してください。	• Group Encryption • IKE Proposal for GET VPN • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか	• Global Settings for GET VPN
通常の IPSec VTI トンネルインターフェイスの設定を参照してください。	• IKE Proposal • ピア（Peers） • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • IKEv2 認証 • IPsec プロファイルとのトンネルインターフェイス	

関連項目

- VPN トポロジの作成または編集 （38 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （14 ページ）
- VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）
- IKE および IPsec ポリシーの設定
- ポリシーについて

サイト間 VPN ポリシーの概要

サイト間 VPN ポリシーにアクセスするには、[管理（Manage）] > [サイト間VPN（Site-To-Site VPNs）] を選択するか、ツールバーの [Site-To-Site VPN Manager] ボタンをクリックして、[サイト間VPN（Site-To-Site VPN）] ウィンドウのポリシーセレクタで必要なポリシーを選択します。また、デバイス ビューまたはポリシー ビューからサイト間 VPN ポリシーにアクセスすることもできます。詳細については、サイト間 VPN トポロジおよびポリシーへのアクセス （25 ページ）を参照してください。

バージョン 4.21 以降、Cisco Security Manager は、IKEv2 のサイト間 VPN の複数ピアクリプトマップをサポートしています。ただし、複数ピアクリプトマップはFlexConfig を介してのみ設定できます。

（注） 複数ピアクリプトマップを設定し、VPN トポロジを展開して検出すると、シーケンス内の次のクリプトマップは生成されません。その後の展開では、単一ピアクリプトマップが無効になり、複数ピアクリプトマップが生成されます。

次に、すべてのサイト間 VPN ポリシーの要約を示します。このなかには、共有ポリシーとして作成できないポリシーもあります。一部のポリシーは、リモート アクセスとサイト間 VPN の両方で使用されるため、リモート アクセス VPN を説明するセクションに記載されていることに注意してください。ただし、これらのポリシーは、それぞれのタイプの VPN 用に別の設定する必要があります。

- Client Connection Characteristics。Easy VPN のクライアント接続特性の設定を参照してください。
- Connection Profiles。Easy VPN のクライアント接続特性の設定を参照してください。
- Easy VPN IPsec Proposal。[Connection Profiles] ページを参照してください。
- GRE Modes。[GRE Modes] ページについてを参照してください。
- Group Encryption Policy。 GET VPN ピアの定義 （82 ページ）を参照してください。
- Group Members。GET VPN グループ メンバーの設定を参照してください。
- IKE Proposal。IKE プロポーザルの設定を参照してください。
- IKE Proposal for GET VPN。GET VPN の IKE プロポーザルの設定を参照してください。
- IKEv2 Authentication。[IKEv2 Proposal] ポリシー オブジェクトの設定を参照してください。
- IPsec Proposal。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
- Key Servers。GET VPN キー サーバの設定を参照してください。
- セグメント分割 エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。
- IKEv1 Preshared Key。IKEv1 事前共有キー ポリシーの設定を参照してください。

- IKEv1 Public Key Infrastructure。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。
- Server Load Balance。大規模 DMVPN でのサーバ ロード バランシングの設定を参照してください。
- User Group Policy。Easy VPN における User Group ポリシーの設定を参照してください。
- VPN Global Settings。VPN グローバル設定を参照してください。
- Global Settings for GET VPN。GET VPN のグローバル設定 を参照してください。

IKEv2 のサイト間 VPN での複数ピアクリプトマップの設定

バージョン 4.21 以降、Cisco Security Manager は、IKEv2 のサイト間 VPN の複数ピアクリプトマップをサポートしています。ただし、複数ピアクリプトマップは FlexConfig を介してのみ設定できます。P2P、ハブアンドスポーク、またはフルメッシュトポロジの複数ピアクリプトマップを作成できます。

この手順では、P2P、ハブアンドスポーク、およびフルメッシュトポロジのサイト間 VPN で複数ピアクリプトマップを設定する方法について説明します。サイト間 VPN トポロジおよびポリシーの詳細については、サイト間 VPN トポロジおよびポリシーへのアクセス （25 ページ）を参照してください。

ステップ 1 目的の VPN トポロジ（P2P、ハブアンドスポーク、またはフルメッシュ）を展開します。

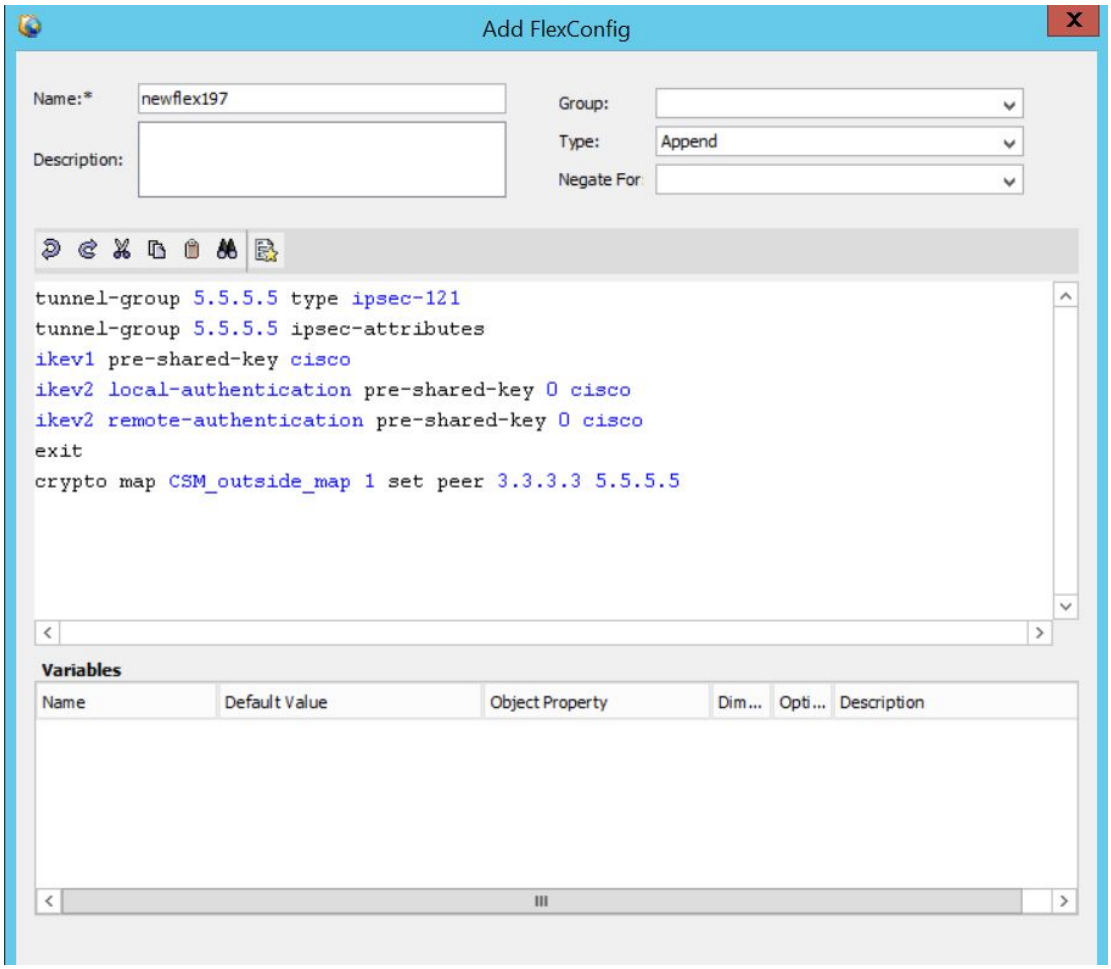
注：ハブアンドスポークトポロジを使用する場合は、ハブピアの**接続タイプ**が**双方向**に設定されていることを確認してください。

ステップ 2 [ツール（Tools）] > [Security Manager の管理（Security Manager Admin）] > [展開（Deployment）] で、[新規または変更済みの FlexConfig のみを展開する（Deploy only new or modified Flexconfigs）] チェックボックスをオフにします。

ステップ 3 [FlexConfig の追加（Add FlexConfig）] をクリックし、[タイプ（Type）] で [付加（Append）] を選択して、複数ピア CLI と対応するトンネルグループ CLI を入力します。

ステップ 4 図 4 : 複数ピア固有 CLI およびトンネルグループ CLIに示すように、複数ピアサポート固有 CLI を入力します。

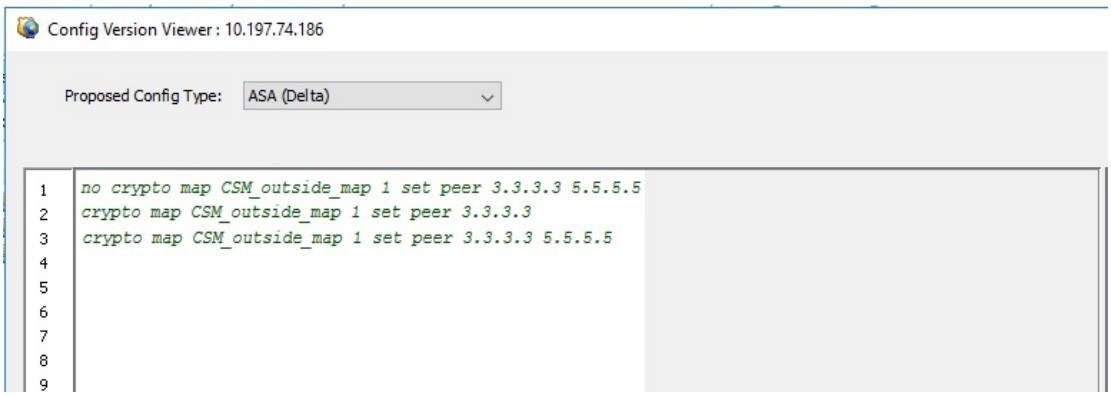
図 *4*：複数ピア固有 *CLI* およびトンネルグループ *CLI*



ステップ 5 設定のプレビューを行い、新しい設定を展開して、[ポリシー（Policy）]>[VPN ポリシーの検出（Discover VPN Policies）] により、複数ピアクリプトマップを設定した VPN トポロジを再検出します。

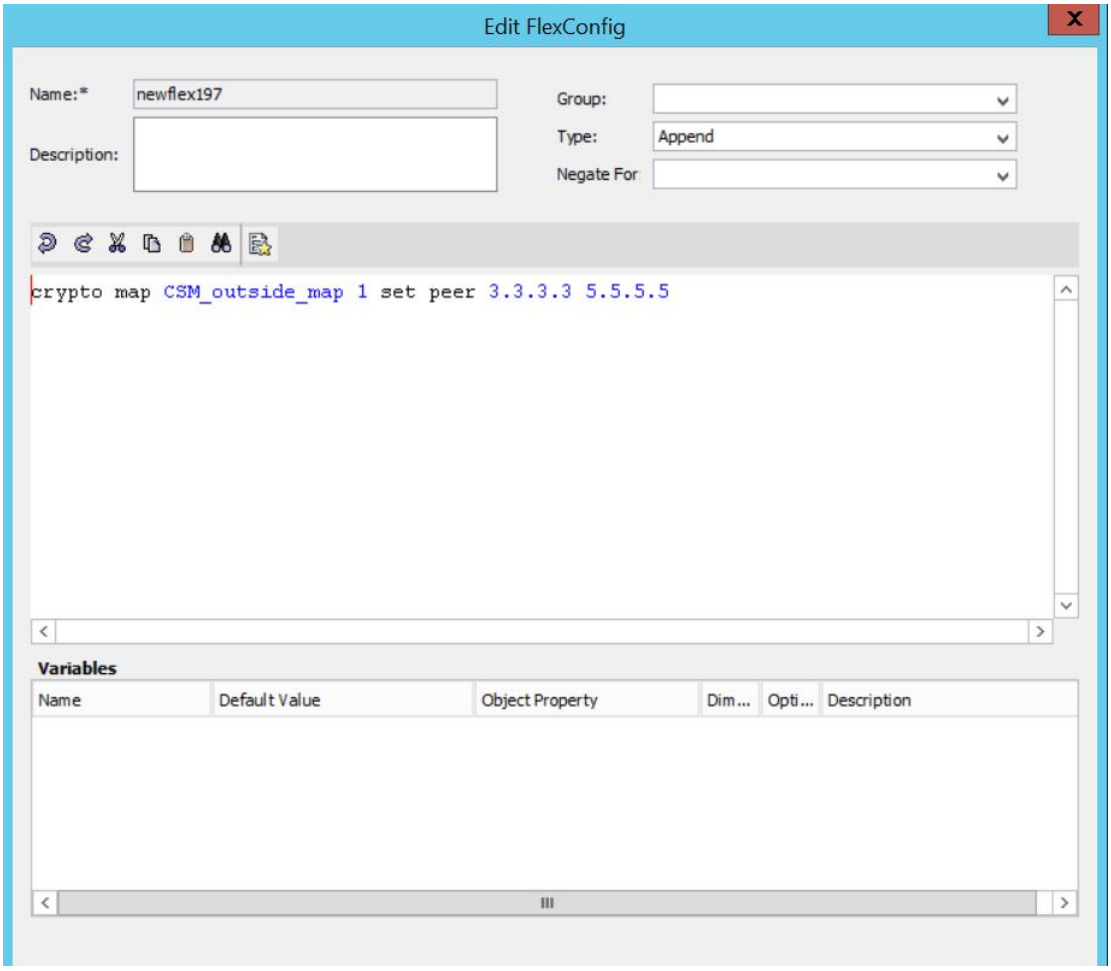
ステップ 6 VPN トポロジを再検出すると、複数ピアクリプトマップ CLI が無効になり、新しい展開が行われるたびに、追加されます。次の図を参照して、CLI がどのように無効になるのかを確認してください。

図 *5* : *CLI* の無効化



ステップ 7 次の図に示すように、FlexConfig でトンネルグループ CLI が削除され、複数ピア CLI のみが保持されていることを確認します。

図 *6* : 複数ピア固有 *CLI*



各 IPsec テクノロジーでサポートされるデバイスについて

各 IPsec テクノロジーでは、異なるデバイスがトポロジのメンバーとしてサポートされます。次の表に、基本的なデバイスのサポートについて示します。これらの要件は、VPN のデバイスを選択する場合に適用されます。場合によっては、デバイス リストは、サポートされているデバイスだけを表示するようフィルタリングされています。また、デバイスは、1 つのロール（スポークなど）としてはサポートされているが、他のロールとしてはサポートされていないことがあります。このような場合は、誤ったデバイス タイプを選択する可能性がありますが、変更内容を保存できないようになっています（メッセージが表示され、具体的な問題の説明が示されます）。

（注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービス ルータ、組み込みサービス ルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。

ヒント デバイスモデルによっては、VPN 設定をサポートしていない NO-VPN バージョンがあります。したがって、あるタイプの VPN で 3845 モデルがサポートされていても、3845 NOVPN モデルはサポートされません。さらに、Cisco Catalyst 6500 シリーズ ASA サービスモジュール（ソフトウェアリリース 8.5(x) を実行）は、どのタイプの VPN もサポートしていません。

表 *2*：各 *IPsec* テクノロジーでサポートされるデバイス

テクノロジー	サポートされるプラットフォーム
通常の IPsec IKE および IPsec ポリシーの設定を参照してください。	通常の IPsec ポリシーは、Cisco IOS セキュリティ ルータ（アグリゲーション サービス ルータ（ASR）を含む）、PIX ファイアウォール、および ASA 5500 シリーズ デバイスで設定できます。エクストラネット VPN の場合を除き、Catalyst VPN サービス モジュールもサポートされます。 IKEv2 は、ASA リリース 8.4(x) でのみサポートされます。トポロジを IKEv2 のみに制限する場合、すべてのデバイスが IKEv2 をサポートする必要があります。IKEv1 と IKEv2 の両方を許可する場合、IKEv2 をサポートしないデバイスは自動的に IKEv1 を使用します。
IPsec/GRE（Generic Routing Encapsulation）。 GRE について を参照してください。	GRE ポリシーは、Cisco IOS セキュリティ ルータ（ASR を含む）および Catalyst 6500/7600 デバイスに設定できます。

テクノロジー	サポートされるプラットフォーム
GRE ダイナミック IP。 動的にアドレス指定されるスポークの GRE 設定についてを参照してください。	GRE ダイナミック IP は、Cisco IOS セキュリティ ルータ（ASR を含む）および Catalyst 6500/7600 デバイスに設定できます。
Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）、大規模 DMVPN。 ダイナミック マルチポイント VPN（DMVPN）および大規模 DMVPN の設定を参照してください。	DMVPN 設定は、Cisco IOS 12.3T 以降のデバイス、および Cisco IOS XE ソフトウェア 2.x 以降（Security Manager では 12.2(33)XNA+ と呼ばれる）を実行している ASR でサポートされます。大規模 DMVPN 設定は、IPsec ターミネータとして Catalyst 6500/7600 デバイスもサポートします。 スポーク間で DMVPN フェーズ 3 接続を使用するには、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。
Easy VPN。 Easy VPN を参照してください。	Easy VPN サーバーは、Cisco IOS セキュリティルータ（ASR を含む）、Catalyst 6500/7600（サポートされる VPN サービスモジュールまたはポートアダプタを使用）、PIX ファイアウォール、または ASA 5500 シリーズ デバイスです。 Easy VPN クライアントは、PIX 6.3 を実行する PIX 501、506、506E Firewall、Cisco 800 ～ 3900 シリーズ ルータ、および OS バージョン 7.2 以降を実行する ASA 5505 デバイスでサポートされます。
GET VPN。 Group Encrypted Transport（GET）VPN を参照してください。	キー サーバは、次のデバイスに設定できます。 • Cisco IOS ソフトウェア Release 12.4(15)T 以降を実行する Cisco 1800、2800、3800 シリーズ ISR、Cisco 7200 シリーズ ルータ、および Cisco 7301 ルータ • Release 15.0 以降を実行する Cisco 1900、2900、3900 シリーズ ISR グループ メンバーは、Cisco 1800、1900、2800、2900、3800、3900 シリーズ ISR、Cisco 7200 シリーズ ルータ、および Cisco 7301 ルータに設定できます。必要最小限のソフトウェア リリース要件は同じです。展開された GET VPN の IPsec SA の数が非常に少ない場合（1 ～ 3 の場合）は、Cisco 871 ISR もグループ メンバーとして使用できます。さらに、Cisco IOS XE ソフトウェア リリース 2.3（12.2(33)XNC）以降を使用する Cisco ASR ルータもグループ メンバーとして設定できます。

（注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェア サポートは提供されません。

関連項目

- VPN トポロジの作成または編集 （38 ページ）
- サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （7 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （16 ページ）
- VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）
- VPN トポロジについて （2 ページ）
- IKE および IPsec ポリシーの設定
- ポリシーについて

管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み

VPN には、Security Manager で管理できないデバイスや、Security Manager では管理しないデバイスが含まれることがあります。次のようなものがあります。

- Security Manager ではサポートされているが、ユーザの組織が担当していないシスコ デバイス。たとえば、VPN に、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続が含まれている場合があります。
- シスコ製以外のデバイス。Security Manager を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。

これらの種類のデバイスを処理する方法は 2 つあります。

- 接続が通常の IPsec ポイントツーポイント接続である場合、エクストラネット VPN の作成または編集 （90 ページ）で説明されているように、エクストラネット VPN として接続を設定できます。
- その他のタイプの接続の場合、これらのデバイスを「管理対象外」デバイスとして Cisco Security Manager インベントリに含めることができます。これらのデバイスは、VPN トポロジ内でエンドポイントとして機能できますが、Security Manager でデバイスから設定を検出したり、デバイスに設定を展開したりすることはできません。

エクストラネット VPN オプションが機能しない場合、管理対象外デバイスを VPN トポロジに追加する前に以下を実行する必要があります。

- 手動定義によるデバイスの追加の手順に従って、デバイスインベントリに管理対象外デバイスとして手動でデバイスを追加します。次の項目を選択する必要があります。
  - VPN でサポートされているテクノロジーという観点から、追加するデバイスに対応するシスコ デバイス タイプを選択します。デバイス タイプによって、デバイスを追加できる VPN トポロジのタイプが決まります。たとえば、GRE や DMVPN では、1800 シリーズや 2800 シリーズなどのサービス統合型ルータを選択できます。Easy VPN では、必要に応じて ASA デバイスや PIX デバイスも選択できます。
  - [Cisco Security Managerで管理（Manage in Cisco Security Manager）] オプションの選択を解除します。デフォルトではすべての新規デバイスが管理対象デバイスとなるため、この操作は重要です。デバイスの追加時にこの操作を行わなかった場合、後で [デバイスのプロパティ（Device Properties）] の [全般（General）] タブ（デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択）でこのオプションの選択を解除できます。
- デバイスのインターフェイス ポリシーを使用して、管理対象デバイスが指す外部 VPN インターフェイスを定義します。デバイスは管理対象外であるため、このポリシーに定義した内容はデバイスに設定されることはありません。単に、Security Manager の外部でデバイスに設定した内容を示すための定義です。

関連項目

- 各 IPsec テクノロジーでサポートされるデバイスについて （14 ページ）
- VPN トポロジのデバイスの選択 （44 ページ）
- VPN トポロジの作成または編集 （38 ページ）

VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定

Security Manager では、ほとんどの必須 VPN ポリシーに対してポリシーの「出荷時のデフォルト」設定が用意されています。これらのデフォルトは汎用的な内容になっており、ご使用のネットワークに対して適切でない可能性がありますが、デフォルトを使用することによって、必要な共有ポリシーが設定されていない場合に、毎回入力し直すことなく VPN を作成できるという利点があります。このため、必須ポリシーには、独自のデフォルト VPN ポリシーを作成する必要があります。また、特定のオプションのポリシーに対してデフォルトを作成することもできます。

新しいデフォルトを設定する前に、設定する予定の VPN のタイプを検討し、デフォルトを作成できるポリシーのタイプを確認します。[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [VPNポリシーのデフォルト（VPN Policy Defaults）] を選択します。目的の IPsec テクノロジーのタブを選択して、どのようなポリシーを利用できるかを確認します。ポリシーに出荷時のデフォルトが割り当てられている場合、またはオプションがドロップダウン リストから選択可能な場合、そのポリシーは必須で

す。その他のポリシーはオプションです。リモート アクセス VPN およびサイト間のエンドポイント設定用のデフォルトポリシーを作成することもできます。選択したポリシーの横にある [コンテンツの表示（View Content）] ボタンをクリックして、ポリシー定義を確認します。

次の手順では、VPN ポリシーのデフォルトを作成する方法および使用する方法について説明します。

ヒント

- VPN デフォルト ポリシーを設定すると、共有ポリシーを選択することになります。IPsec テクノロジーに従い、ポリシーごとに設定できるデフォルトは 1 つだけですが、ユーザは VPN の設定時にさまざまな共有ポリシーを選択できます。したがって、ユーザが選択できる複数の共有ポリシーを設定し、そのうち最も一般的に使用されるポリシーをデフォルトポリシーとして設定できます。VPN 設定時にユーザがどのようにさまざまなポリシーを選択できるかの詳細については、新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て （84 ページ）を参照してください。
- IKEv2 Authentication ポリシーは IKEv2 ネゴシエーションを許可するトポロジの場合は必須ポリシーですが、IKEv2 Authentication の出荷時のデフォルト設定は存在せず、IKEv2 Authentication 共有ポリシーを作成できません。したがって、トポロジで IKEv2 を許可する場合は必ず、トポロジが有効になる前に IKEv2 Authentication ポリシーを手動で設定する必要があります。
- 証明書認証を使用するように IKE Proposal ポリシーを設定する場合、IKEv1 に対して Public Key Infrastructure ポリシーが必須です。ただし、このポリシーに対する出荷時のデフォルト設定は存在しないため、IKEv1 で証明書認証を使用する場合は、デフォルトの Public Key Infrastructure ポリシーを作成することを考慮してください。
- 共有ポリシーを変更すると、そのポリシーを使用しているすべての VPN に影響があることに注意してください。このため、共有ポリシーは、すべての VPN に必要な全社的変更を導入する場合に便利です。ただし、VPN を作成したあと、ユーザは共有ポリシーからローカル ポリシーに切り替えることができます。この場合は、VPN トポロジに対して個別に設定を変更する必要があります。共有ポリシーの詳細については、ポリシー ビューにおける共有ポリシーの管理を参照してください。
- これらのデフォルト ポリシーは、エクストラネット VPN の作成時には適用されません。エクストラネット VPN を使用する場合、通常のウィザード フローの一部として必須ポリシーの設定値を必ず設定する必要があります。

ステップ 1 デフォルト ポリシーを作成します。すべてのデフォルト ポリシーは、共有ポリシーです。

a) ポリシービュー（[表示（View）]>[ポリシービュー（Policy View）] を選択）で、デフォルトを設定するポリシーを選択します。ポリシーは、[サイト間VPN（Site-to-Site VPN）] フォルダまたは [リモートアクセスVPN（Remote Access VPN）] フォルダにあります。

b) [共有ポリシー（shared policy）] セレクタの下部にある [ポリシーの作成（+） （Create a Policy(+)）] ボタンをクリックし、ポリシーの名前を入力して、[OK] をクリックします。

c) 必要な設定を行います。選択したポリシーで利用可能な設定についての情報を参照するには、ツールバーの [ヘルプ（?） （Help(?)）] ボタンをクリックします。

d) このプロセスを繰り返して、デフォルト ポリシーを定義する各ポリシーに対して少なくとも 1 つの共有ポリシーを作成します。

ステップ 2 必要に応じて、VPN エンドポイントのデフォルトを作成します。これらのデフォルトは、VPN 接続に使用されるインターフェイス名（GigabitEthernet0/1 など）を識別する、インターフェイス ロール オブジェクトです。内部および外部 VPN インターフェイスには、それぞれ別個のロールを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、Policy Object Managerを開きます。

b) コンテンツテーブルから [インターフェイスロール（Interface Roles）] を選択します。

c) [新規オブジェクト（+）（New Object(+)）] ボタンをクリックし、ネットワーク内の内部または外部 VPN インターフェイスで最も一般的に使用されるインターフェイスを識別するインターフェイス名のパターンを入力して、[OK] をクリックします。

インターフェイス ロール、およびそれらの設定時に使用するワイルドカードの詳細については、インターフェイス ロール オブジェクトについておよびインターフェイス ロール オブジェクトの作成を参照してください。

ステップ 3 ポリシーおよびポリシー オブジェクトをデータベースに送信します。すべての検証エラーを解決する必要があります。

- Workflow 以外のモードで、[ファイル（File）] > [送信（Submit）] を選択します。
- アクティビティ承認者のいない Workflow モードの場合は、[アクティビティ（Activities）] > [承認アクティビティ（Approve Activity）] を選択します。
- アクティビティ承認者のいる Workflow モードの場合は、[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）] を選択します。アクティビティが承認されるまでは、ポリシーおよびオブジェクトをデフォルトとして選択できません。

ステップ 4 新しく設定したポリシーおよびポリシー オブジェクトを VPN ポリシーのデフォルトとして選択します。

a) [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [VPNポリシーのデフォルト（VPN Policy Defaults）] を選択します（[VPN Policy Defaults] ページを参照）。

b) 適切なタブを選択して、デフォルトを設定した必須またはオプションのポリシーそれぞれのドロップダウン リストから、設定したポリシーを選択します。

[S2S Endpoints] タブで、適切なインターフェイス ロール オブジェクトを選択します。

c) [保存（Save）] をクリックして、デフォルトを保存します。

次回ユーザが Create VPN ウィザードを実行すると、選択したデフォルトがウィザードのデフォルトとして使用されます。ユーザは、他の任意の共有ポリシーまたはインターフェイス ロールを選択して、デフォルトを上書きできます。

デバイスのオーバーライドを使用した VPN ポリシーのカスタマイズ

多くの VPN ポリシーでは、設定で Security Manager ポリシー オブジェクトが使用されます。ポリシー オブジェクトとは、再利用可能な設定を作成できるコンテナを指します。

VPN ポリシーは VPN トポロジ内のすべてのデバイスに適用されるため、VPN トポロジ内の特定のデバイスのポリシーで使用されるポリシー オブジェクトを変更する必要がある場合があります。場合によっては、トポロジ内のすべてのデバイスを変更する必要があることもあります。このような変更は、ポリシー オブジェクトに対するデバイス レベルのオーバーライドを使用して行います。

たとえば、PKI ポリシーを定義する場合は、PKI 登録オブジェクトを選択する必要があります。VPN のハブでスポークとは異なる CA サーバが使用されている場合は、デバイス レベルのオーバーライドを使用して、ハブで使用されている CA サーバを指定する必要があります。PKI ポリシーでは単一の PKI 登録オブジェクトが参照されますが、ハブの場合、定義するデバイス レベルのオーバーライドに基づいて、このオブジェクトで表される実際の CA サーバが異なるものとなります。

ポリシー オブジェクトのオーバーライドをイネーブルにするには、ポリシー オブジェクト定義で [デバイスごとのオーバーライドを許可（Allow Override per Device）] オプションを選択する必要があります。その後、デバイス レベルのオーバーライドを作成できます。デバイス レベルでの VPN ポリシー オブジェクトのオーバーライドの詳細については、次の項を参照してください。

- 個々のデバイスのポリシー オブジェクト オーバーライドについて
- ポリシー オブジェクトの上書きの許可
- 単一デバイスのオブジェクト オーバーライドの作成または編集
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集

VRF 対応 IPsec について

ピアツーピア VPN を展開する場合、ルーティング テーブルの分離、および重複したアドレスの使用が障害となります。アドレスの重複は、通常、お客様のネットワークのプライベート IP アドレスを使用することが原因で起こります。この問題は、マルチプロトコル ラベル スイッチング（MPLS）VPN への IPsec トンネルのマッピングを導入する VRF 対応 IPsec 機能を使用することで解決できます。

VRF 対応 IPsec 機能を使用することによって、単一のパブリック向けアドレスを使用して、IPsec トンネルを Virtual Routing and Forwarding（VRF）インスタンスにマッピングできます。VRF インスタンスでは、プロバイダー エッジ（PE）ルータに接続されたカスタマー サイトの VPN メンバーシップが定義されます。VRF は、IP ルーティング テーブル、派生シスコ エクスプレス フォワーディング（CEF）テーブル、転送テーブルを使用するインターフェイスのセット、ルーティング テーブルに含まれる情報を制御するルールおよびルーティング プロトコル パラメータのセットで構成されています。ルーティング テーブルおよび CEF テーブルのセットは、MPLS/VPN ネットワーク全体で VPN カスタマーごとに保持されます。

各 VPN は、ルータに独自のルーティング テーブルおよび転送テーブルを持っているため、VPN に属するすべての顧客またはサイトは、そのテーブルに含まれているルートのセットにだけアクセスできます。すべての PE ルータには、VPN ごとに数多くのルーティング テーブルと、プロバイダー ネットワーク内の他のルータに到達するのに使用できる 1 つのグローバル ルーティング テーブルが保持されています。事実上、数多くの仮想ルータが単一の物理ルータに作成されます。MPLS コアから他の PE ルータへのルート全体にわたり、ルート識別子（RD）などの一意の VPN 識別子を追加することによって、このルーティングの分離は維持されます。

（注） VRF 対応 IPsec は、リモート アクセス VPN のデバイスにも設定できます。詳細については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス）を参照してください。

Security Manager では、ハブアンドスポーク VPN トポロジに VRF 対応 IPsec を設定できます。この場合、すべての機能を提供する単一のデバイスを使用することも（「1 ボックス」ソリューション）、それぞれが機能の一部を提供する複数のデバイスを使用することもできます（「2 ボックス」ソリューション）。1 つのデバイスですべての機能を提供するソリューションは、システムに過負荷がかかり、パフォーマンスに悪影響がある可能性があります。一方、2 ボックス ソリューションで機能を分離すると、各機能のスケーラビリティを高めることができます。

ここでは、次の内容について説明します。

- VRF 対応 IPsec 1 ボックス ソリューション （21 ページ）
- VRF 対応 IPsec 2 ボックス ソリューション （22 ページ）
- Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化 （24 ページ）

VRF 対応 IPsec の設定の詳細については、 VRF 対応 IPsec の設定 （66 ページ）を参照してください。

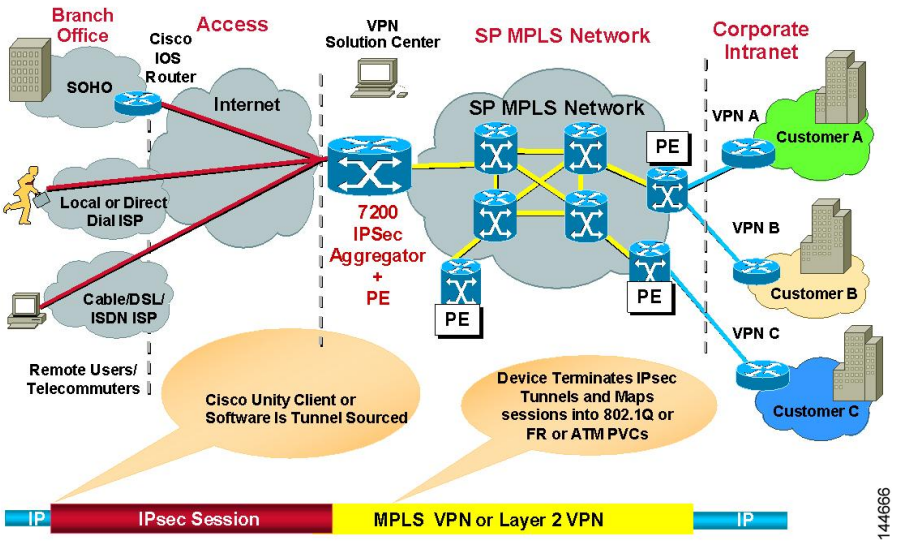
VRF 対応 IPsec 1 ボックス ソリューション

1 ボックス ソリューションでは、IPsec トンネルの終端が Cisco IOS ルータとなり、このルータがプロバイダー エッジ（PE）デバイスとして機能します。PE デバイスは、これらのトンネルを適切な MPLS/VPN ネットワークにマッピングし、カスタマー エッジ（CE）デバイスとの間で IPsec 暗号化および復号化を実行することによって IPsec Aggregator として機能します。

（注） PE デバイスと MPLS クラウドとの間のルーティングの設定は、Cisco IP Solution Center によって行われます。『Cisco IP Solution Center MPLS VPN User Guide』を参照してください。

次の図に、1 ボックス ソリューションのトポロジを示します。

図 *7: VRF* 対応 *IPsec 1* ボックス ソリューション



関連項目

- VRF 対応 IPsec について （20 ページ）
- VRF 対応 IPsec の設定 （66 ページ）
- エンドポイントおよび保護対象ネットワークの定義 （46 ページ）

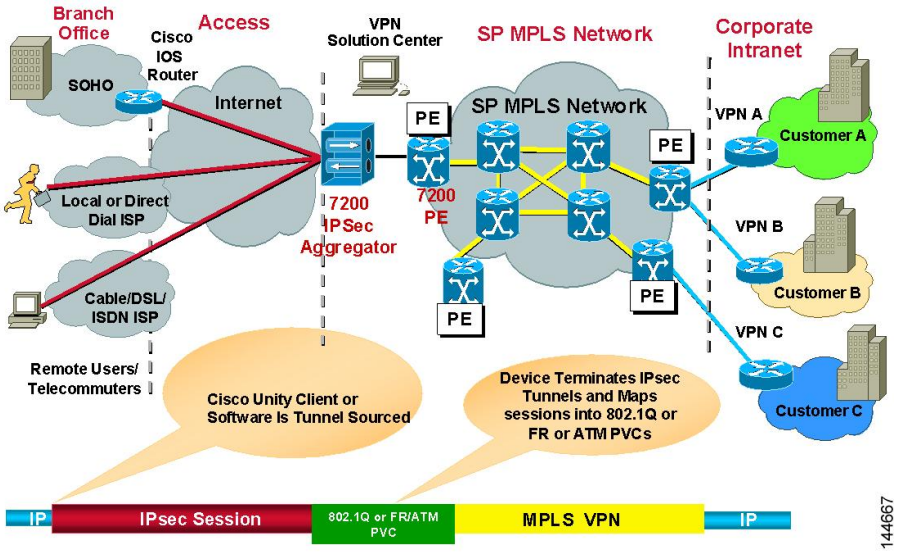
VRF 対応 IPsec 2 ボックス ソリューション

2 ボックス ソリューションでは、PE デバイスは MPLS マッピングだけを行います。CE との間の IPsec 暗号化および復号化は、別の IPsec Aggregator によって行われます。

（注） Security Manager は、PE デバイスへのルーティングも含め、IPsec Aggregator を完全に管理します。PE デバイスは、Cisco IP Solution Center によって完全に管理されます。これには、PE デバイスと MPLS クラウドとの間のルーティングや、PE から IPsec Aggregator へのルーティングが含まれます。詳細については、『Cisco IP Solution Center MPLS VPN User Guide』を参照してください。

次の図に、2 ボックス ソリューションのトポロジを示します。

図 *8 : VRF* 対応 *IPsec 2* ボックス ソリューション



2 ボックス ソリューションを使用して、次のように VPN トポロジのデバイスに VRF 対応 IPsec を設定します。

1. IPsec Aggregator と PE デバイスとの間の接続を設定します。

ハブアンドスポーク VPN トポロジを作成して、それに IPsec テクノロジーを割り当てます。このトポロジでは、ハブは IPsec Aggregator です。スポークは、Cisco IOS ルータ、PIX ファイアウォール、Catalyst VPN サービス モジュール、または Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスです。IPsec Aggregator は、セキュリティ ルータまたは Catalyst VPN サービス モジュールです。次に、ハブに VRF パラメータ（VRF 名および一意のルート識別子）を定義します。

（注） VRF 対応 IPsec では、Cisco IOS ルータおよび Catalyst VPN サービス モジュールへの IPsec、GRE、または Easy VPN テクノロジーの設定がサポートされています。DMVPN は、Cisco IOS ルータでだけサポートされています。

1. IPsec Aggregator と PE デバイスとの間の VRF 転送インターフェイス（または Catalyst VPN サービス モジュールの VLAN）を指定します。
2. IPsec Aggregator と PE との間で使用するルーティング プロトコルおよび自律システム（AS）番号を定義します。使用可能なルーティング プロトコルには、BGP、EIGRP、OSPF、RIPv2、スタティック ルートがあります。

IPsec Aggregator と PE との間に定義されたルーティング プロトコルが、保護された IGP で使用されるルーティング プロトコルと異なる場合、ルーティングはこのルーティング プロトコルと AS 番号を使用して保護された IGP に再配布されます。ルーティングは、保護された IGP から PE にも再配布されます。

（注） ルーティングの再配布は、選択されたテクノロジーが IPsec/GRE または DMVPN の場合にだけ関連します。

関連項目

- VRF 対応 IPsec について （20 ページ）
- VRF 対応 IPsec の設定 （66 ページ）
- エンドポイントおよび保護対象ネットワークの定義 （46 ページ）

Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチをサポートしますが、Cisco Catalyst スイッチはサポートが終了しているため、拡張機能はサポートされません。

既存のサイト間 VPN の Catalyst スイッチおよび 7600 ハブで Virtual Routing and Forwarding（VRF）モードを変更すると、展開に失敗します。たとえば、最初に Create VPN ウィザードで VRF を設定して展開したあと、Peers ポリシーに戻って [Enable VRF Settings] チェックボックスの選択を解除すると、展開に失敗します（この設定は、[エンドポイントの編集（Edit Endpoints）] ダイアログボックスの [VRF対応IPSec（VRF Aware IPSec）] タブにあります。 VRF 対応 IPsec の設定 （66 ページ）を参照してください）。最初に設定されていない VPN で VRF を有効にしようとすると、同様に展開が失敗します。

Catalyst 6500/7600 では、VPN の動作中には VRF モードを変更できません。この制限は、Catalyst 6500/7600 ハブに対してだけ適用されます。他のデバイス タイプには適用されません。

この制限は、VRF 設定自体に加えられる変更には適用されません。たとえば、VPN トポロジに VRF が設定されている場合、Peers ポリシーに戻って VRF 名やルート識別子を変更することができます。

VPN の VRF モードを変更する必要がある場合に、Catalyst 6500/7600 デバイスをハブとして使用しているときは、次の手順を実行します。

関連項目

- VRF 対応 IPsec について （20 ページ）
- VRF 対応 IPsec 1 ボックス ソリューション （21 ページ）
- VRF 対応 IPsec 2 ボックス ソリューション （22 ページ）

ステップ 1 Security Manager から VPN トポロジを削除します。

ステップ 2 変更を展開します。

ステップ 3 Catalyst 6500/7600 デバイスをリロード（再起動）します。

ステップ 4 Security Manager でデバイスを右クリックして、[デバイスでポリシーを検出（Discover Policies on Device）] を選択します。完全なポリシー再検出を実行します。

ステップ 5 Create VPN ウィザードを開いて、VPN トポロジを再定義します。これで、異なる VRF モードを選択できるようになりました。VRF 対応 IPsec の設定 （66 ページ）および VPN トポロジの作成または編集 （38 ページ）を参照してください。

サイト間 VPN トポロジおよびポリシーへのアクセス

次の方法を使用して、サイト間 VPN トポロジおよびポリシーへのアクセスおよび設定を行うことができます。

- Site-to-Site VPN Manager：VPN トポロジを設定するための主要なツールです。Security Manager で設定されているすべてのサイト間 VPN のリストを表示して、それらの設定やポリシー（デバイス メンバーシップを含む）を編集できます。このツールの使用方法の詳細については、[Site-to-Site VPN Manager] ウィンドウ （26 ページ）を参照してください。
- デバイス ビューの [サイト間VPN（Site-to-Site VPN）] ポリシー：デバイス ビューでデバイスを選択するときに、ポリシー セレクタで [サイト間VPN（Site-to-Site VPN）] ポリシーを選択して、デバイスが参加しているすべてのサイト間 VPN のリストを表示し、それらのトポロジを編集できます。新しい VPN を作成したり、VPN を選択して Site-to-Site VPN Manager を開き、選択した VPN のポリシーを編集したりすることもできます。このデバイス ビューのポリシーは、実質的には Site-to-Site VPN Manager へのショートカットです。このポリシーの使用方法の詳細については、デバイス ビューにおける VPN トポロジの設定 （27 ページ）を参照してください。
- ポリシー ビューの [サイト間VPN（Site-to-Site VPN）] フォルダ：ポリシー ビューは、共有ポリシーを作成するために使用されます。多くのサイト間 VPN ポリシーは、共有可能です。したがって、Site-to-Site VPN Manager でトポロジを設定するときに、複数の VPN トポロジに割り当てることができる共有ポリシーを設定できます。VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）に説明したように、共有ポリシーを Create VPN ウィザードのデフォルトとして設定できます。

[Site-to-Site VPN Manager] ウィンドウでも、デバイス ビューのローカル ポリシーから作成する場合と同様に共有ポリシーを作成できますが、[Site-to-Site VPN Manager] ウィンドウにおいては、共有に関するすべてのコマンドは右クリックして表示されるコンテキスト メニューからだけ利用できます（共有可能ポリシーを右クリックします）。

ポリシー ビューにおける共有ポリシー作成の詳細については、ポリシー ビューにおける共有ポリシーの管理を参照してください。

[Site-to-Site VPN Manager] ウィンドウ

Site-to-Site VPN Manager には、Security Manager で設定されたすべてのサイト間 VPN が表示されます。ウィンドウの左上ペインにある VPN セレクタには、既存の VPN トポロジがすべて表示されます（VPN トポロジについて （2 ページ）を参照）。アイコンは、VPN のタイプ（ハブアンドスポーク、ポイントツーポイント、または完全メッシュ）を示します。トポロジを表示または編集するには、トポロジを選択します。これにより、左下ペインのポリシーセレクタにそのポリシーがロードされます。ポリシーを選択すると、その定義が右側のペインに表示されます。

Site-to-Site VPN Manager を開くには、ツールバーの [Site-To-Site VPN Manager] ボタンをクリックするか、**[管理（Manage）] > [サイト間VPN（Site-To-Site VPNs）]** を選択します。

[Site-to-Site VPN Manager] ウィンドウを使用して、次のことを行うことができます。

- VPN トポロジを作成、編集、および削除します。
  - VPN トポロジを作成するには、VPN セレクタの上にある [VPN トポロジの作成（Create VPN Topology）]（+）ボタンをクリックし、表示されるオプションから、作成するトポロジのタイプを選択します。これにより、Create VPN ウィザードまたは Create Extranet VPN ウィザードが開きます。詳細については、VPN トポロジの作成または編集 （38 ページ）またはエクストラネット VPN の作成または編集 （90 ページ）を参照してください。
  - VPN トポロジを編集するには、トポロジを選択して [VPN トポロジの編集（Edit VPN Topology）]（鉛筆）ボタンをクリックするか、トポロジを右クリックして [編集（Edit）] を選択します。これにより、[Edit VPN] ダイアログボックスまたは [Edit Extranet VPN] ダイアログボックスが開きます。このダイアログボックスには、Create VPN ウィザードと同様のページのほとんどがタブ形式のレイアウトで表示されます。
  - VPN トポロジを削除するには、トポロジを選択して [VPN トポロジの削除（Delete VPN Topology）]（ゴミ箱）アイコンをクリックするか、トポロジを右クリックして [削除（Delete）] を選択します。削除の確認が求められます。VPN トポロジの削除 （95 ページ）を参照してください。
- 各 VPN トポロジについての詳細情報を表示します。トポロジを選択して、[VPN Summary] ポリシーを選択します。[VPN トポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）] （85 ページ）を参照してください。
- VPN トポロジに定義されたエンドポイントを表示および設定します。エンドポイントは、VPN トポロジ編集時に [エンドポイント（Endpoints）] タブで確認するか、または [ピア（Peers）] ポリシーを選択して確認します。GET VPN トポロジの場合、[ピア（Peers）] ポリシーはありません。代わりに、[キーサーバー（Key Servers）] ポリシーと [グループメンバー（Group Members）] ポリシーを使用して、エンドポイントを表示および設定します。エクストラネット VPN の場合、エンドポイントは VPN 編集時の [Device Selection] タブ、または [Peers] ポリシーにも表示されます。

- VPN トポロジに割り当てられたポリシーの表示と編集、共有ポリシーの割り当て、または既存のポリシーからの共有ポリシーの作成を行います。個別のポリシーの詳細については、サイト間 VPN ポリシーの概要 （10 ページ）を参照してください。

Site-to-Site VPN Manager から共有ポリシーを設定する場合のオプションおよび方法は、デバイス ビューから設定する場合と同じです。これについては、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用およびポリシー バナーの使用の項で説明しています。ポリシーの共有、割り当て、割り当て解除、割り当ての編集、および名前の変更を行うことができますが、VPN ポリシーの継承はできません。これらのタスクを実行するには、VPN トポロジを選択し、目的のポリシーを右クリックして、必要なコマンドを選択します。

ポリシー ビューを使用して共有 VPN ポリシーを設定することもできます。

デバイス ビューにおける VPN トポロジの設定

デバイスが属するサイト間 VPN トポロジがある場合は、デバイス ビューの Site-to-Site VPN ポリシーを使用して、サイト間 VPN トポロジを表示および編集できます。VPN ポリシーを編集したり、デバイスがトポロジに参加するかどうかを変更したりできます。また、新しい VPN トポロジを作成することもできます。

このポリシーは、実質的には Site-to-Site VPN Manager へのアクセス ポイントです（サイト間 VPN ディスカバリ （28 ページ）を参照）。

このポリシーを開くには、デバイスビューで目的のデバイスを選択して、ポリシーセレクタから [サイト間VPN（Site-to-Site VPN）] を選択します。

VPN トポロジテーブルには、このデバイスが属するすべてのサイト間 VPN が表示されます。VPN のタイプ、その名前、IPsec テクノロジー、説明などの情報が表示されます。バージョン 4.9 以降、Security Manager は VPN トポロジの最後に変更されたチケットの情報も表示します。チケット管理システムを使用して作成または編集された VPN トポロジには、このページで利用可能な最後に変更されたチケットの ID 情報があります。また、最後に変更されたチケットの ID で VPN トポロジをフィルタリングすることもできます。

- VPN を追加するには、[VPNトポロジの作成（Create VPN Topology）] ボタンをクリックするか、またはテーブルを右クリックして [VPNトポロジの作成（Create VPN Topology）] を選択し、表示されるオプションから作成するトポロジのタイプを選択します。これにより、Create VPN ウィザードまたは Create Extranet VPN ウィザードが開きます。詳細については、VPN トポロジの作成または編集 （38 ページ）またはエクストラネット VPN の作成または編集 （90 ページ）を参照してください。
- VPN を編集するには、VPN を選択して [VPNトポロジの編集（Edit VPN Topology）] ボタンをクリックするか、VPN を右クリックして [VPNトポロジの編集（Edit VPN Topology）] を選択するか、または単にエントリをダブルクリックします。これにより、[Edit VPN] ダイアログボックスまたは [Edit Extranet VPN] ダイアログボックスが開きます。このダイアログボックスは、Create VPN ウィザードのタブ形式バージョンです（VPN トポロジの作成または編集 （38 ページ）またはエクストラネット VPN の作成または編集 （90 ページ）を参照）。

- VPN のポリシーを編集するには、VPN を選択して、[VPNポリシーの編集（Edit VPN Policies）] ボタンをクリックします。VPN トポロジについての情報が表示された [Site-to-Site VPN] ウィンドウが開きます。ポリシー セレクタから目的のポリシーを選択して、編集します。
- VPN を削除するには、VPN を選択して [VPNトポロジの削除（Delete VPN Topology）] ボタンをクリックするか、または VPN を右クリックして [VPNトポロジの削除（Delete VPN Topology）] を選択します。削除の確認が求められます。詳細については、VPN トポロジの削除 （95 ページ）を参照してください。

サイト間 VPN ディスカバリ

すでにネットワークに展開されている VPN トポロジを検出して、それらを Security Manager を使用して管理できます。VPN 設定が Security Manager に取り込まれて、サイト間 VPN ポリシーとして表示されます。

エクストラネット VPN の場合を除き、すでに Security Manager によって管理されている既存の VPN トポロジの設定を再検出することもできます。サイト間 VPN の再検出の詳細については、サイト間 VPN の再検出 （37 ページ）を参照してください。

（注） また、すでにネットワークに展開されているリモート アクセス VPN のデバイスの設定も検出できます。リモート アクセス VPN ポリシーの検出を参照してください。

次の各項では、サイト間 VPN ディスカバリについて説明します。

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ （28 ページ）
- VPN ディスカバリの前提条件 （30 ページ）
- VPN ディスカバリ ルール （30 ページ）
- サイト間 VPN の検出 （33 ページ）
- 検出された、複数のスポーク定義を持つ VPN の定義または修復 （35 ページ）
- サイト間 VPN の再検出 （37 ページ）

VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ

ここでは、Security Manager で検出できるテクノロジーとトポロジ、および Security Manager によってプロビジョニングされるが検出できない VPN 機能について説明します。

VPN ディスカバリでサポートされるテクノロジー

- IPsec（ASA デバイスの LAN-to-LAN 設定を含む）
- IPsec + GRE
- IPsec + GRE ダイナミック IP
- DMVPN
- Easy VPN
- GET VPN

VPN ディスカバリでサポートされるトポロジ

- ポイントツーポイント
- ハブアンドスポーク
- 完全メッシュ
- エクストラネット VPN（管理対象外デバイスに対するポイントツーポイント）

Security Manager によってプロビジョニングされるが VPN ディスカバリではサポートされていない VPN 機能

- IPsec ターミネータを使用した大規模 DMVPN（高集中ハブ）
- VRF 対応 IPSec
- ダイヤル バックアップ
- Easy VPN の IPsec および ISAKMP プロファイル
- ハイ アベイラビリティ Easy VPN

Security Manager を使用してこれらのタイプのポリシーを定義および展開すると、検出されなかったデバイス設定がポリシーによって上書きされます。したがって、Security Manager で既存の設定を管理する場合には、既存の設定と可能なかぎり一致するようにポリシーを定義する必要があります（[Tool（ツール）]>[設定のプレビュー（Preview Configuration）] を使用して、展開する前に結果を調べます）。VPN のプロビジョニングメカニズムでは、（既存の設定の内容が Cisco Security Manager で設定されたポリシーに一致するという前提で）可能なかぎり既存の設定の内容が利用されますが、CLI コマンドで使用される命名規則は維持されません。

関連項目

- VPN ディスカバリの前提条件　（30 ページ）
- VPN ディスカバリ ルール　（30 ページ）
- サイト間 VPN の検出　（33 ページ）

VPN ディスカバリの前提条件

正常に VPN を検出するためには、次の前提条件を満たしている必要があります。

- エクストラネット VPN の場合を除き、VPN に参加するすべてのデバイスを Security Manager インベントリに追加する必要があります。
- Security Manager で、VPN に関するいくつかの基本的な情報を指定する必要があります。VPN ディスカバリ ウィザードでは、次の情報の入力を求められます。
  - VPN トポロジ（ハブアンドスポーク、ポイントツーポイント、完全メッシュ、エクストラネット）。
  - VPN テクノロジー（通常の IPsec、IPsec/GRE、GRE ダイナミック IP、DMVPN、Easy VPN、GET VPN）。
  - VPN 内のデバイスおよびそのロール（ハブまたはスポーク）。エクストラネット VPN の場合、管理対象デバイスのみを指定します。
  - VPN 設定のソース。VPN は、ライブネットワークから直接検出することも、Security Manager の Configuration Archive から検出することもできます。
- VPN の各デバイスでは、物理インターフェイスにクリプト マップが関連付けられている必要があります。このルールは、エクストラネット VPN 内のリモート（管理対象外）デバイスには適用されません。
- VPN トポロジ内のルーティング プロトコルとして OSPF を使用する場合は、VPN 内のすべてのデバイスで同じ OSPF プロセス番号を使用する必要があります。
- Easy VPN トポロジ内の各 PIX 6.3 または ASA 5505 クライアント デバイスに vpnclient 設定が必要です。

関連項目

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ（28 ページ）
- VPN ディスカバリ ルール （30 ページ）
- サイト間 VPN の検出 （33 ページ）

VPN ディスカバリ ルール

次の表に、Security Manager が VPN 設定を変換および検出する場合のルール、およびデバイスの設定が Security Manager によってサポートされている設定と一致しない場合の処理方法について示します。

ヒント　エクストラネット VPN 検出には単一デバイス（管理対象デバイス）の分析が含まれるため、これらのルールのほとんどはエクストラネット VPN 検出には適用されません。VPN 内のデバイス間の値の整合性を含むルールはすべて適用されません。

表 *3 : VPN* ディスカバリ ルール

条件	VPN ディスカバリの処理
Security Manager が、ライブ デバイス検出のために VPN 内のデバイスに接続できない	• デバイスが VPN 内の唯一のハブまたはスポークである場合、検出は失敗します。 • VPN 内に他のハブやスポークがある場合、検出は進行しますが、利用できないデバイスは検出されません。 • エクストラネット VPN の場合を除き、デバイスがポイントツーポイントトポロジのピアである場合、検出は失敗します。エクストラネット VPN の場合、管理対象デバイスにのみ接続し、接続できないと検出は失敗します。 • デバイスが完全メッシュ トポロジのピアであり、利用できないデバイスを含めてトポロジ内にデバイスが 2 つしかない場合、検出は失敗します。3 つ以上のデバイスがある場合、検出は進行しますが、利用できないデバイスは検出されません。
VPN が ASA 上の LAN-to-LAN VPN である	ASA の資料では、「サイト間」の同義語として「LAN-to-LAN」が使用されています。LAN-to-LAN VPN 設定では、ASA はトンネルグループを使用します。トンネルグループをリモートアクセス VPN 設定で使用すると、Security Manager は接続プロファイルとして検出します。 LAN-to-LAN（L2L）トンネル グループを使用する ASA でサイト間 VPN を検出する場合、Security Manager はサイト間 VPN トポロジを作成し、L2L トンネル グループはユーザに対して接続プロファイルとして表示されません。代わりに、VPN トポロジのプロパティを編集すると、展開中に、Security Manager が設定を適切な L2L トンネル グループのコマンドに変換します。

条件	VPN ディスカバリの処理
VPN 内のデバイス全体において、VPN 設定のポリシーまたは値に不整合がある	• ハブとスポークの値が異なる場合は、ハブの値が優先されます。 • いくつかのポリシーまたは値の候補から単に 1 つのポリシーや値を選択するだけで済み、機能的な問題が発生しない場合には、Security Manager によってすべてのデバイスに共通するポリシーまたは値が 1 つ選択されます。たとえば、デバイスには複数の IKE ポリシーを設定できますが、VPN では単一の IKE ポリシーだけを選択できます。 • 1 つの値を選択すると機能的な問題が発生する場合は、ポリシーに対して値が検出されず、展開時に確認メッセージが表示されます。 • 数値が異なる場合は、検出中にメッセージが表示され、小さい方の値が検出されます。たとえば、IPsec ポリシーにおいては、最小の SA ライフタイム値が検出されます。 • 上記いずれも実行できない場合、VPN ディスカバリは失敗します。
事前共有キー設定で、ピアのセットごとに異なるキーが存在する	Preshared Key ポリシーは検出されないため、検出完了後に設定する必要があります。Security Manager では、すべてのデバイスで事前共有キーの値が同じ場合にだけ Preshared Key ポリシーが検出されます。
デバイスに複数のクリプト マップ候補が存在する	VPN ディスカバリで選択されたすべてまたは大部分のデバイスに関連付けられているクリプト マップが使用されます。
スポークに、ハブに関連付けられたクリプト マップがない	VPN ディスカバリは進行しますが、スポークは検出されず、エラー メッセージが表示されます。
デバイスに、選択されたトランスフォーム セット値がない	VPN ディスカバリは進行しますが、デバイスは VPN トポロジから削除されることがあります。
デバイスに、選択された IKE プロポーザルがない	VPN ディスカバリは進行しますが、デバイスは VPN トポロジから削除されることがあります。
デバイスで DVTI がサポートされているが、DVTI またはクリプト マップが設定されていない	VPN ディスカバリは失敗します。

条件	VPN ディスカバリの処理
サーバで DVTI がサポートされているが、DVTI 設定に IP アドレスが設定されていない	VPN ディスカバリは進行しますが、警告が表示されます。
クライアントで DVTI がサポートされていない	ハブに DVTI が設定されている場合は、警告やエラーは表示されずに検出が進行します。
ハブアンドスポーク トポロジで、スポークがハブと同じ VPNSPA/VSPA スロットを使用していない（Catalyst 6500/7600）	VPN ディスカバリは失敗します。
キー サーバとグループ メンバーの同一のセットが複数の GET VPN に参加している	Security Manager では、トポロジのうち 1 つだけが検出されます。
User Group ポリシーで、IP アドレスではなくホスト名を使用してバックアップ サーバが設定されている	VPN ポリシー検出は失敗し、次のエラーが表示されます。 Policy Discovery Failed: com.cisco.nm.vms.discovery.DiscoveryException: Internal Error 正常に検出を行うには、ホスト名ではなく IP アドレスを使用して、デバイスの User Group ポリシーのバックアップ サーバを再設定する必要があります。

関連項目

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ（28 ページ）
- VPN ディスカバリの前提条件 （30 ページ）
- サイト間 VPN の検出 （33 ページ）
- サイト間 VPN の再検出 （37 ページ）

サイト間 VPN の検出

ここでは、すでにネットワークで稼働しているが、Security Manager には定義されていないサイト間 VPN を検出する方法について説明します。

関連項目

- サイト間 VPN の検出 （33 ページ）
- ポリシーの検出

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ（28 ページ）
- VPN ディスカバリの前提条件 （30 ページ）
- VPN ディスカバリ ルール （30 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （14 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （16 ページ）

ステップ 1 デバイスビューで、**[ポリシー（Policy）] > [VPNポリシーの検出（Discover VPN Polices）]** を選択して、[VPNポリシーの検出（Discover VPN Polices）] ウィザードの [名前とテクノロジー（Name and Technology）] ページを開きます。

ステップ 2 次の情報を指定します。

- [VPN名（VPN Name）]：検出する VPN の名前です。

エクストラネット VPN を検出する場合は名前を指定できません。代わりに、Security Manager がデバイス上に定義されているすべてのエクストラネットを検出し、各エクストラネットに対して、VPN 名はローカル IP アドレスとリモート IP アドレスがハイフンでつながれたものになります。たとえば、ローカルアドレスが 10.100.10.1、リモートアドレスが 10.100.11.1 である場合、エクストラネット VPN の名前は **10.100.10.1-10.100.11.1** と指定されます。

- [説明（Description）]：（任意）VPN の説明。エクストラネット VPN 検出に説明を追加することはできません。
- [トポロジ（Topology）]：検出する VPN のタイプ（[ハブアンドスポーク（Hub and Spoke）]、[ポイントツーポイント（Point to Point）]、[フルメッシュ（Full Mesh）]、または [エクストラネット（Extranet）]）です。
- [IPsecテクノロジー（IPsec Technology）]：VPN に割り当てられている IPsec テクノロジー（通常の IPsec、IPsec/GRE、GRE ダイナミック IP（サブテクノロジー）、DMVPN、Easy VPN、GET VPN、または通常の IPSEC VTI）です。選択するトポロジに応じて、このリストで利用可能な内容が変わります。

IPsec/GRE を選択した場合は、[標準（Standard）]（IPsec/GRE 用）または [ダイナミックIPを使用したスポーク（Spokes with Dynamic IP）]（GRE ダイナミック IP の設定用）のいずれかのタイプも指定する必要があります。

（注） ハブアンドスポークトポロジ、およびポイントツーポイントトポロジに適用可能なトンネルベースのルーティングには、通常の IPSEC VTI を選択できます。

- [検出元（Discover From）]：VPN は、ネットワークから直接検出することも、設定アーカイブから再検出することもできます。
  - [Network]：Security Manager は、すべてのライブ デバイスに接続してデバイス設定を取得します。エクストラネット VPN 検出の場合、Security Manager はユーザが指定する単一の管理対象デバイスに接続します。

- [Config Archive]：ライブ デバイスではなく設定ファイルに展開する場合は、Configuration Archive からの検出を推奨します。[Configuration Archive] 内のデバイス設定の最新バージョンがすべてのデバイスに使用されます。

ステップ 3 [次へ（Next）] をクリックして、[VPNポリシーの検出（Discover VPN Policies）] ウィザードの [デバイス選択（Device Selection）] ページを開きます。

ステップ 4 VPN に参加しているデバイス、およびそれらのデバイスの VPN 内でのトポロジタイプに応じたロール（ハブ、スポーク、ピア 1、ピア 2、ローカル デバイス、キー サーバ、グループ メンバー、または単に完全メッシュ VPN で選択されるデバイス）を選択します。Easy VPN トポロジの場合は、サーバがハブ、クライアントがスポークになります。

ハブアンドスポーク VPN に 2 つ以上の IPsec ターミネータがある場合は、上向きおよび下向き矢印ボタンを使用して、プライマリ ハブがリストの先頭にくるようにします。IPsec ターミネータが 1 つだけの場合は、同じ IPsec ターミネータにいくつのハブが接続されているかに関係なく、1 つのハブをプライマリ ハブとして指定できません。

VPN のデバイスの選択の詳細については、VPN トポロジのデバイスの選択 （44 ページ）を参照してください。

ステップ 5 [終了（Finish）] をクリックしてウィザードを閉じ、検出プロセスを開始します。[Discovery Status] ウィンドウが開き、検出のステータスが表示されます。また、各デバイスの検出が成功したか、または失敗したかが示されます（ポリシー検出タスクのステータスの表示を参照）。問題の原因を示すためにエラーまたは警告メッセージが提供されます。問題の原因は、VPN に固有またはデバイスに固有の可能性があります。

エクストラネット検出の場合を除き、検出プロセスが正常に完了し、[Discovery Status] ダイアログボックスを閉じると、[Site-to-Site VPN Manager] ウィンドウが開き、検出された VPN の概要情報が表示されます。エクストラネット検出の場合、検出されたエクストラネット VPN のリストを参照するには、Site-to-Site VPN Manager を手動で開くか、またはデバイス ビューで Site-to-Site VPN ポリシーを選択する必要があります。

ステップ 6 VPN ポリシーが必要な内容となっていることを確認します。必要に応じて、ポリシーを編集します。

ヒント エクストラネット VPN を検出する場合、選択されたデバイスに定義されているすべてのエクストラネット VPN が検出されます。Security Manager で管理しないエクストラネット VPN は削除してください。

検出された、複数のスポーク定義を持つ VPN の定義または修復

各スポークに異なる定義が含まれる VPN を検出した場合（たとえば Easy VPN スポークのクライアント モードが異なる場合）、Security Manager では検出中に定義が変更されて、すべてのスポークに対して統一された定義が作成されます。Security Manager では、VPN トポロジに 1 セットのスポーク定義だけを含むことができるため、このような動作になります。

元の定義を維持する場合、または異なる定義を持つスポークで構成された新しい VPN を作成する場合は、次のいずれかの方法を実行します。

- Security Manager に複数の VPN トポロジを定義し、各トポロジには、一致するスポーク定義を含むスポークを設定します。
- 特殊な定義を含むFlexConfigポリシーを定義して、次の手順で説明するように、この定義を必要とするスポークにポリシーを割り当てます。

関連項目

- 新しい共有ポリシーの作成
- FlexConfig ポリシー オブジェクトの作成
- ポリシー ビューにおけるポリシー割り当ての変更
- サイト間 VPN ディスカバリ （28 ページ）
- サイト間 VPN の検出 （33 ページ）
- VPN ディスカバリ ルール （30 ページ）

ステップ 1 ポリシー ビューで、共有 FlexConfig ポリシーを作成します。

a) **[表示（View）] > [ポリシービュー（Policy View）]** を選択します。
b) ポリシータイプセレクタで [FlexConfigs] を右クリックして、[新しいFlexConfigポリシー（New FlexConfigs Policy）] を選択します。
c) ポリシーの名前を入力し、[OK] をクリックします。

ステップ 2 FlexConfig オブジェクトを作成および選択して、FlexConfig ポリシーを定義します。

a) ポリシービューの作業領域にある [詳細（Details）] タブで [追加（Add）] ボタンをクリックします。
b) FlexConfigs セレクタで、ウィンドウの左下隅にある [作成（Create）] ボタンをクリックして、[Add FlexConfig]/[Edit FlexConfig] ダイアログボックスを開きます。
c) 必要なクライアント定義を含む追加の FlexConfig オブジェクトを定義します。たとえば、Easy VPN スポークでクライアント モードを定義するには、次のコマンドを入力します。

```
crypto ipsec client ezvpn CSM_EASY_VPN_CLIENT_1
mode client
exit
```

d) FlexConfigオブジェクトを作成したあと、セレクタを使用してこのオブジェクトをFlexConfigポリシーに追加します。

ステップ 3 ポリシー ビューの作業領域にある [割り当て（Assignments）] タブを使用して、このポリシーを割り当てるスポークを選択し、[保存（Save）] をクリックします。

ステップ 4 ポリシーを展開します。

サイト間 VPN の再検出

ポリシーの変更をアプリケーションで再作成する必要がないように、すでに Security Manager で管理されている既存の VPN トポロジの設定を再検出できます。

Security Manager が VPN 設定を変換および検出する場合と同じルールが再検出にも適用されます。ただし、再検出は、VPN トポロジに参加するデバイスに対してだけ実行できます。また、IPsec テクノロジーやトポロジ タイプは変更できません。VPN インターフェイスや保護対象ネットワークなどのデバイス固有のポリシー、およびハブに設定される任意のハイ アベイラビリティ（HA）ポリシーの設定だけを再検出できます。IKE プロポーザルや PKI 登録などの VPN グローバル ポリシーは再検出できません。さらに、次のトポロジは再検出できません。

- ダイナミック VTI を使用する Easy VPN トポロジ
- エクストラネット VPN

ここでは、すでに Security Manager に存在するサイト間 VPN トポロジの設定を再検出する方法について説明します。

関連項目

- サイト間 VPN の検出　（33 ページ）
- ポリシーの検出
- VPN ディスカバリの前提条件　（30 ページ）
- VPN ディスカバリ ルール　（30 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて　（14 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み　（16 ページ）

ステップ 1 [Site-to-Site VPN Manager] ウィンドウで、設定を再検出する VPN トポロジを右クリックして、[ピアの再検出（Rediscover Peers）] を選択します。これにより、Rediscover VPN Policies ウィザードの [Name and Technology] ページが開きます。

このページには、トポロジのタイプ、および VPN で使用される IPsec テクノロジーが表示されますが、これらは変更できません。

ステップ 2 次の情報を指定します。

- [VPN検出名（VPN Discovery Name）]：VPN 再検出ジョブの名前です。
- [説明（Description）]：（任意）VPN の説明。
- [検出元（Discover From）]：VPN は、ネットワークから直接再検出することも、設定アーカイブから再検出することもできます。
  - [Network]：Security Manager は、すべてのライブ デバイスに接続してデバイス設定を取得します。

- [Config Archive]：ライブ デバイスではなく設定ファイルに展開する場合は、Configuration Archive からの再検出を推奨します。[Configuration Archive] 内のデバイス設定の最新バージョンがすべてのデバイスに使用されます。

ステップ 3 [次へ（Next）] をクリックして、[VPNポリシーの再検出（Rediscover VPN Policies）] ウィザードの [デバイス選択（Device Selection）] ページを開きます。

ステップ 4 ピア レベルのポリシーを再検出する必要があるデバイス、およびそれらのデバイスの VPN 内でのトポロジ タイプに応じたロール（ハブ、スポーク、ピア 1、ピア 2、キー サーバ、グループ メンバー、または単に完全メッシュ VPN で選択されるデバイス）を選択します。Easy VPN トポロジの場合は、サーバがハブ、クライアントがスポークになります。

ハブアンドスポーク VPN に 2 つ以上の IPsec ターミネータがある場合は、上向きおよび下向き矢印ボタンを使用して、プライマリ ハブがリストの先頭にくるようにします。IPsec ターミネータが 1 つだけの場合は、同じ IPsec ターミネータにいくつのハブが接続されているかに関係なく、1 つのハブをプライマリ ハブとして指定できません。

VPN のデバイスの選択の詳細については、VPN トポロジのデバイスの選択 （44 ページ）を参照してください。

ステップ 5 [終了（Finish）] をクリックしてウィザードを閉じ、再検出プロセスを開始します。[Discovery Status] ウィンドウが開き、再検出のステータスが表示されます。また、各デバイスの再検出が成功したか、または失敗したかが示されます（ポリシー検出タスクのステータスの表示を参照）。問題の原因を示すためにエラーまたは警告メッセージが提供されます。問題の原因は、VPN に固有またはデバイスに固有の可能性があります。

再検出プロセスが正常に完了し、[Discovery Status] ダイアログボックスを閉じると、[Site-to-Site VPN Manager] ウィンドウが開き、再検出された VPN の概要情報が表示されます。

VPN トポロジの作成または編集

Security Manager では、サイト間 VPN を作成するための 3 つの基本的なトポロジ タイプがサポートされています。Create VPN ウィザードを使用して、複数のデバイス タイプにまたがる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、または完全メッシュ VPN トポロジを作成できます。これらのトポロジの詳細については、VPN トポロジについて （2 ページ）を参照してください。

ヒント エクストラネット ポイントツーポイント VPN を作成する場合は、このトピックではなく、エクストラネット VPN の作成または編集 （90 ページ）を参照してください。

VPN トポロジを作成する場合は、サイト間 VPN を構成するデバイスおよびネットワークを指定します。デバイス、デバイスのロール（ハブ、スポーク、ピア、キー サーバ、グループ メンバーなど）、VPN トンネルの送信元エンドポイントおよび宛先エンドポイントとなる VPN インターフェイス、トンネルによって保護される保護対象ネットワークを定義します。VPN ト

ポロジを作成する場合は、トポロジに対して、定義済みのポリシーのセットが関連付けられた IPsec テクノロジー（通常の IPsec、IPsec/GRE、GRE ダイナミック IP、DMVPN、大規模 DMVPN、Easy VPN、GET VPN など）を割り当てます。サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （7 ページ）を参照してください。

（注） Create VPN ウィザードを完了すると、Security Manager によって必須ポリシーに対してデフォルトが指定されるため、すぐにトポロジを展開可能になります。ただし、Security Managerのデフォルトを使用する場合は、ご使用のネットワークでその設定が適切に動作することを確認する必要があります。詳細については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）を参照してください。

VPN トポロジを編集する場合、[Edit VPN] ダイアログボックスには（[VPN defaults] ページを除いて）Create VPN ウィザードと同じページが含まれていますが、ウィザード形式ではなく、タブ形式でページがレイアウトされています。GET VPN トポロジだけは例外であり、トポロジの名前と説明だけを編集できます（トポロジの属性を変更するには、GET VPN ポリシーを編集する必要があります。GET VPN の設定を参照してください）。ダイアログボックスの任意のタブで [OK] をクリックすると、すべてのタブの定義が保存されます。すべてのトポロジにおいて、当初 [VPN defaults] ページに表示された必須ポリシーおよびオプションのポリシーを直接編集する必要があります。

VPN トポロジを編集することによって、トポロジのデバイス構造の変更（デバイスの追加または削除）、デバイスに定義された VPN インターフェイスおよび保護対象ネットワークの変更、または VPN に割り当てられているポリシーの変更を行うことができます。たとえば、組織において新規サイトを頻繁にオープンする場合、既存のハブアンドスポーク VPN にスポークを追加して、新しいスポークに VPN のすべてのポリシーを適用する必要があります。また、1 つのハブだけを持つ VPN にセカンダリ ハブを追加して、耐障害性を高めることもできます。VPN トポロジの編集時に、トポロジに割り当てられたポリシーを変更する必要がある場合もあります。たとえば、IKE アルゴリズムをより安全なアルゴリズムに変更したり、VPN の DES 暗号化アルゴリズムを変更してより安全にしたりします。

ヒント トポロジを作成したあとは、VPN で使用されているテクノロジーを変更することはできません。テクノロジーを変更する場合は、古い VPN を削除してから、必要なテクノロジーを使用する新しい VPN を作成します。

Create VPN ウィザードを開始する、または既存の VPN トポロジを編集するには、次の手順を実行します。

- Create VPN ウィザードを開くには、[Site-to-Site VPN Manager] ウィンドウ （26 ページ）または [サイト間VPNポリシー（Site-to-Site VPN Policy）] ページ（デバイスビュー）で、[新規VPNトポロジの作成（Create VPN Topology）]（+）ボタンをクリックして、作成する VPN トポロジのタイプを表示されるオプション（[ハブアンドスポーク（Hub and Spoke）]、[ポイントツーポイント（Point to Point）]、または [フルメッシュ（Full Mesh）]）から選択します。[Back] ボタンと [Next] ボタンを使用してページを移動します。終了したら、[Finish] をクリックして、トポロジを作成します。

- [VPNの編集（Edit VPN）] ダイアログボックスを開くには、[Site-to-Site VPN Manager] ウィンドウまたは[サイト間VPNポリシー（Site-to-Site VPN Policy）]ページ（デバイスビュー）で VPN トポロジを選択し、[PNトポロジの編集（Edit VPN Topology）]（鉛筆）ボタンをクリックします。

表示されるページまたはタブ、およびその順序は、作成する VPN トポロジのタイプに応じて異なります。それらについて、次の表に示します。

表 *4 : Create VPN/Edit VPN* ウィザードのページ

ページ	ハブアンドスポーク VPN	ポイントツーポイント VPN	完全メッシュ VPN
[Name and Technology] ページ。 VPN トポロジの名前および IPsec テクノロジーの定義 （42 ページ）を参照してください。	ステップ 1	ステップ 1	ステップ 1
[Device Selection] ページ。 VPN トポロジのデバイスの選択 （44 ページ）を参照してください。	ステップ 2	ステップ 2	ステップ 2
[Endpoints] ページ。 エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。 このページから、いくつかの高度な設定を作成することもできます。詳細については、表のあとにある説明を参照してください。	ステップ 3	ステップ 3	手順 3（通常の IPsec、IPsec GRE だけ）
[High Availability] ページ。 VPN トポロジにおけるハイ アベイラビリティの設定 （71 ページ）を参照してください	ステップ 4：	—	—
[GET VPN Group Encryption Policy] ページ。 GET VPN グループ暗号化の定義 （74 ページ）を参照してください。	—	—	手順 3（GET VPN だけ）
[GET VPN Peers] ページ。 GET VPN ピアの定義 （82 ページ）を参照してください。	—	—	手順 4（GET VPN だけ）

ページ	ハブアンドスポーク VPN	ポイントツーポイント VPN	完全メッシュ VPN
[VPN Defaults] ページ。 新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て （84 ページ）を参照してください。	ステップ 5	ステップ 4	手順 4（GET VPN では手順 5）
[Synchronize Keys] ダイアログボックス。GET VPN で Create VPN ウィザードを完了するときに、キーを同期するかどうかを尋ねられます。[はい（Yes）] をクリックすると、プロセスが開始されます。 RSA キーの生成と同期を参照してください。	—	—	手順 6（GET VPN だけ）

VPN トポロジの作成中または作成後、エンドポイント編集時に、次の高度な設定を作成することもできます。

- ハブアンドスポーク トポロジでの、ハブにおける VRF 対応 IPsec（VRF 対応 IPsec の設定（66 ページ）を参照）
- 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、または完全メッシュ VPN トポロジでの、Catalyst 6500/7600 における VPNSM または VPNSPA/VSPA（VPNSM または VPN SPA/VSPA エンドポイントの設定 （58 ページ）を参照）
- 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、または完全メッシュ VPN トポロジでの、VPN サービス モジュールまたは VPN SPA が設定された Catalyst 6500/7600 デバイスにおけるファイアウォール サービス モジュール（VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 （64 ページ）を参照）

（注） マップ ビューでは、VPN トポロジをそのすべての要素とともに視覚的に表現できます。詳細については、マップ ビューにおける VPN トポロジの作成を参照してください。

関連項目

- デバイス ビューにおける VPN トポロジの設定 （27 ページ）
- IPsec テクノロジーおよびポリシーについて （6 ページ）
- ウィザードの使用

VPN トポロジの名前および IPsec テクノロジーの定義

（注） このトピックは、エクストラネット VPN には適用されません。エクストラネット VPN の名前の設定については、エクストラネット VPN の作成または編集 （90 ページ）を参照してください。

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [Name and Technology] ページ（またはタブ）を使用して、VPN トポロジの名前と説明を定義します。新しいトポロジを作成するときには、トポロジに割り当てる IPsec テクノロジーを選択する必要があります。ただし、既存のトポロジを編集するときにテクノロジーを変更することはできません。

Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開く方法については、VPN トポロジの作成または編集 （38 ページ）を参照してください。

（注） 既存の VPN を編集する場合、割り当てられている IPsec テクノロジーおよびタイプが表示されますが、変更はできません。テクノロジーまたはタイプを変更するには、トポロジを削除してから新しいトポロジを作成する必要があります。

次の表に、名前およびテクノロジーを定義する場合に設定可能なオプションを示します。

表 5 : [Name and Technology] ページ

要素	説明
名前	VPN トポロジを識別する一意の名前です。
説明	VPN トポロジについての情報です。
IPsec Technology	VPN トポロジで使用される IPsec テクノロジーです。 • 通常の IPsec • IPsec/GRE • DMVPN（ハブアンドスポーク VPN だけ） • Easy VPN（ハブアンドスポーク VPN だけ） • GET VPN（完全メッシュ VPN だけ） • 通常の IPSec VTI

要素	説明
タイプ（Type）	選択された IPsec テクノロジーが IPsec/GRE またはハブアンドスポークトポロジにおける DMVPN の場合、テクノロジータイプフィールドが表示されます。 • [IPsec/GRE]：[標準（Standard）]（IPsec/GRE）または [ダイナミック IP を使用したスポーク（Spokes with Dynamic IP）]（GRE ダイナミック IP）を選択します。詳細については、動的にアドレス指定されるスポークの GRE 設定についてを参照してください。 • [DMVPN]：[標準（Standard）]（通常の DMVPN）または [IPsec ターミネータを使用した大規模型（Large Scale with IPsec Terminator）]（大規模 DMVPN）を選択します。詳細については、大規模 DMVPN の設定を参照してください。
IKE バージョン	IKE ネゴシエーションで許可するインターネット キー エクスチェンジ（IKE）バージョン。 通常の IPsec VTI トポロジを設定する場合、バージョン 1（[IKEv1]）またはバージョン 2（[IKEv2]）を許可できます。 通常の IPsec トポロジを設定する場合、バージョン 1（[IKEv1]）、バージョン 2（[IKEv2]）、または [IKEv1 と IKEv2（IKEv1 & IKEv2）] の両方を許可できます。 [IKEv1 と IKEv2（IKEv1 & IKEv2）] を選択すると、IKEv2 をサポートしないデバイスでは自動的に IKEv1 が使用されます。ただし、IKEv2 のみを選択する場合は、IKEv2 をサポートしていないデバイスを選択しないようにする必要があります（ウィザードは無効な選択を阻止しません）。間違ったオプションを選択した場合、VPN の作成後に IKE Proposal ポリシーと IPsec Proposal ポリシーを編集してサポートされる IKE バージョンを変更できます。 IKE について、および各バージョンの相違点については、IKE および IPsec 設定の概要を参照してください。IKEv2 をサポートするデバイスについては、各 IPsec テクノロジーでサポートされるデバイスについて （14 ページ）を参照してください。 **ヒント** Create VPN ウィザード使用時に IKEv2 を許可するオプションを選択すると、ウィザードは有効なトポロジを作成しません。ウィザードの完了後、IKEv2 Authentication ポリシーを手動で設定して、設定を完了する必要があります。

関連項目

- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （16 ページ）

VPN トポロジのデバイスの選択

（注） このトピックは、エクストラネット VPN には適用されません。エクストラネット VPN でのデバイスの選択については、エクストラネット VPN の作成または編集 （90 ページ）を参照してください。

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [Device Selection] ページ（またはタブ）を使用して、VPN トポロジに組み込むデバイスを選択します。このページの内容は、作成または編集する VPN トポロジがハブアンドスポーク、大規模 DMVPN、ポイントツーポイント、または完全メッシュのいずれであるかに応じて異なります。また、このページを使用して GET VPN のメンバーシップを編集することはできません（既存の GET VPN について作業する場合は、GET VPN グループ メンバーの設定およびGET VPN キー サーバの設定を参照してください）。

Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開く方法については、VPN トポロジの作成または編集 （38 ページ）を参照してください。

ほとんどの場合、[使用可能なデバイス（Available Devices）] リストには、選択した VPN トポロジタイプで使用できるデバイス、IPsec テクノロジータイプをサポートするデバイス、および表示する権限があるデバイスだけが表示されます。また、利用可能なデバイスは、選択した IPsec テクノロジーによっても異なります。たとえば、IPsec テクノロジーが IPsec/GRE、GRE ダイナミック IP、または DMVPN の場合、PIX ファイアウォールと ASA デバイスは表示されません。リストはトポロジでサポートする IKE バージョンを考慮するようには調整されません。ただし、通常の IPsec VTI トポロジ設定の場合、IKEv1 が選択されていると、ASA 9.7.1 以降のシングル コンテキスト デバイスが表示されます。IKEv2 の場合は、ASA 9.8.1 以降のシングル コンテキスト デバイスが表示されます。詳細については、各 IPsec テクノロジーでサポートされるデバイスについて （14 ページ）に説明されている、サポートされるプラットフォームを参照してください。

ヒント デバイスを選択する場合、デバイス グループを選択して、そのグループ内のすべての選択可能なデバイスを選択することができます。

次のリストに、トポロジのタイプに応じてデバイスを追加または削除する方法を示します。

- **通常の IPsec または IPsec/GRE テクノロジーを使用する完全メッシュ VPN トポロジでデバイスを選択するには、**[使用可能なデバイス（Available Devices）] リストでデバイスを選択して、[>>] をクリックします。
- **GET VPN テクノロジーを使用する完全メッシュ VPN トポロジでデバイスを選択するには、次の手順を実行します。**
  - キーサーバーとして定義するデバイスを選択して、[キーサーバー（Key Servers）] フィールドの横にある [>>] をクリックします。

複数のキーサーバーがある場合は、**上向き**および**下向き**の矢印ボタンを使用して、プライマリ キーサーバーを先頭に配置します。グループ メンバーは、リストの最初のキー サーバに登録されます。最初のキー サーバに到達できない場合は、2 番め以降のキー サーバに順番に登録が試みられます。

- グループメンバーとして定義するデバイスを選択して、[グループメンバー（Group Members）] フィールドの横にある [>>] をクリックします。
- **ハブアンドスポーク VPN トポロジでデバイスを選択するには、次の手順を実行します。**
  - ハブとして定義するデバイス（または Easy VPN 設定でサーバーとして定義するデバイス）を選択して、[ハブ（Hubs）] リストの横にある [>>] をクリックします。

複数のハブがある場合は、ハブ リストをプライオリティ順に並べて、プライマリ ハブを先頭に配置します。順序を変更するには、ハブを選択し、**上向き**および**下向き**の矢印ボタンをクリックして、デバイスを適切な順序に並べ替えます。

（注） プライマリ ハブは、2 つ以上の IPsec ターミネータがある場合にだけ選択する必要があります。IPsec ターミネータが 1 つだけの場合は、同じ IPsec ターミネータにいくつのハブが接続されているかに関係なく、1 つのハブをプライマリ ハブとして指定できません。

- スポークとして定義するデバイス（または Easy VPN 設定でクライアントとして定義するデバイス）を選択して、[スポーク（Spokes）] リストの横にある [>>] をクリックします。
- **IPsec ターミネータを使用した大規模 DMVPN** トポロジを設定する場合は、大規模 DMVPN 設定で **IPsec ターミネータ**となる Catalyst 6500/7600 デバイスを選択する必要もあります。2 つ以上の IPsec ターミネータを選択する場合は、**上向き**および**下向き**の矢印ボタンを使用して、プライオリティ順に並べ替えます。詳細については、大規模 DMVPN の設定を参照してください。
- **ポイントツーポイント VPN トポロジでデバイスを選択するには、次の手順を実行します。**
  - [デバイス（Devices）] リストから、**ピア 1** とするデバイスを選択して、[>>] をクリックします。
  - **ピア 2** とする別のデバイスを選択して、[>>] をクリックします。
- **（任意のトポロジまたはテクノロジーの組み合わせにおいて）デバイスを削除するには、**選択されたデバイスのいずれかのリストでデバイスを選択し、[<<] をクリックして、そのデバイスを [使用可能なデバイス（Available Devices）] リストに戻します。

既存の VPN トポロジを編集している場合は、VPN トポロジからデバイスを削除することはできますが、その結果として無効な VPN 設定となる場合には、変更内容を保存できません。デバイスを削除する場合、次の点に注意する必要があります。

- デバイスがハブアンドスポーク VPN トポロジにおける唯一のハブである場合、そのデバイスは削除できません。他のハブに置き換える必要があります。

- デバイスがポイントツーポイント VPN トポロジにおける 2 つのデバイスのいずれかである場合、そのデバイスは削除できません。他のハブに置き換える必要があります。
- 複数のハブ デバイスがある VPN トポロジでは、ハブを削除すると、そのハブを使用するトンネルが削除されます。
- VPN トポロジのすべてのスポークではなく一部のスポークが削除されると、ハブ側の crypto ステートメントが変更されて、削除内容が反映されます。
- GET VPN には、少なくとも 1 つのキー サーバと 1 つのグループ メンバーが必要です。

関連項目

- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （16 ページ）

エンドポイントおよび保護対象ネットワークの定義

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [Endpoints] ページを使用して、VPN トポロジ内のデバイスを表示し、それらの VPN 特性および機能を定義または編集します。主に、VPN トポロジ内のデバイスの外部または内部 VPN インターフェイス、および保護対象ネットワークを定義します。VPN インターフェイスは、データを暗号化するインターフェイスです。保護対象ネットワークは、暗号化されるネットワークです。

[Endpoints] ページは、次のいずれかの方法で開きます。

- Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開きます。手順については、 VPN トポロジの作成または編集 （38 ページ）を参照してください。
- Site-to-Site VPN Manager で目的の VPN トポロジを選択して（GET VPN トポロジを除く）、[ピア（Peers）] ポリシーを選択します。

ヒント：

- この設定は、GET VPN 以外のすべての IPsec テクノロジー タイプに適用されます。VPN 作成時に GET VPN エンドポイントを設定する方法については、 GET VPN ピアの定義 （82 ページ）を参照してください。既存の GET VPN では、Key Servers ポリシーおよび Group Members ポリシーを使用してエンドポイントを設定します。GET VPN キー サーバの設定およびGET VPN グループ メンバーの設定を参照してください。
- このページに表示されるデバイスは、[Device Selection] ページで選択します（VPN トポロジのデバイスの選択 （44 ページ）を参照）。このリストは、Peers ポリシーの編集時にだけ変更できます。この場合、デバイスを選択し、[削除（Delete）]（ゴミ箱）ボタンをクリックして、デバイスを削除します。デバイスを追加するには、VPN トポロジ自体を編集する必要があります。
- Peers ポリシーを使用してエクストラネット VPN のエンドポイントを編集することはできますが、代わりに、[Edit Extranet VPN] ダイアログボックスで VPN トポロジを編集するこ

とによりエンドポイントを編集してください。Create Extranet VPN ウィザードには [Endpoints] ページは表示されません。

テーブルには、VPN における各デバイスのロール（ハブ、スポーク、ピア、または IPsec ターミネータ）、デバイス名、および VPN インターフェイスと保護対象ネットワークが表示されます。当初、VPN インターフェイスと保護対象ネットワークは、外部および内部インターフェイスに対して、Security Manager の管理設定で定義されたデフォルトのインターフェイス ロールに設定されています（[VPN Policy Defaults] ページを参照）。エンドポイント設定には、このテーブルに表示されない設定が含まれている場合もありますが、必須の設定は VPN インターフェイスと保護対象ネットワークだけです。

- デバイスのエンドポイント設定を変更するには、デバイスを選択して、テーブルの下にある [行の編集（Edit Row）] ボタンをクリックします。一度に複数のデバイスを選択して編集することもできますが、その場合、それらのデバイスのロールは同じである必要があります。複数のデバイスを選択する場合は、Catalyst 6500/7600 デバイスまたは VPN サービス モジュールを含めることはできません。エンドポイントの編集は [Edit Endpoints] ダイアログボックスで実行しますが、その内容は選択したデバイス タイプおよび IPsec テクノロジーに応じて異なります。

[Edit Endpoints] ダイアログボックスで設定できるオプションの詳細については、次の項を参照してください。

- - [VPNインターフェイス（VPN Interface）] タブ：VPN インターフェイスを設定し、その他の必要なインターフェイス設定を行います（VPN インターフェイス エンドポイントの設定 （49 ページ）を参照）。ダイヤル バックアップも設定できる場合があります（ダイヤル バックアップの詳細については、ダイヤル バックアップの設定 （54 ページ）を参照してください）。

Catalyst 6500/7600 デバイスでは、[VPN Interface] タブに、デバイス（大規模 DMVPN における IPsec ターミネータの場合もあります）に VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA ブレードを設定できる設定が表示されます。これについては、VPNSM または VPN SPA/VSPA エンドポイントの設定 （58 ページ）を参照してください。

トンネルベースの VPN を設定する場合は、[VPNインターフェイス（VPN Interface）] タブのみが表示されます。[選択（Select）] ボタンを使用して、トンネルインターフェイスを選択します。

Easy VPN は、ASA の起動時に最高および最低のセキュリティレベルのインターフェイスを判別することによって機能します。VPN クライアントは、同じ最高セキュリティレベルの複数のインターフェイスを拒否します。BVI で、Easy VPN によって同じ最高セキュリティ レベルの複数のインターフェイスがあることが特定されると、VPN クライアントが無効になります。この問題を解決するために、ASA 9.9(2) 以降のすべての ASA 5506、5508、および 5512 [x/h/w] デバイスに vpnclient secure interface CLI が導入されました。そのため、Cisco Security Manager で CLI をサポートするために、バージョン 4.17 以降、新しいコンポーネント「VPN クライアント インターフェイス」がタイプ（Easy VPN）のハブアンドスポークトポロジに導入されました。

- • [エクストラネットデバイスの詳細（Extranet Device Details）]：エクストラネット VPN 内のリモート（管理対象外）デバイスのエンドポイント設定値を設定します。このタブは、Peers ポリシーの場合にのみ表示されます。このタブで情報を編集する代わりに、VPN トポロジを編集して設定を変更する方法を推奨します。詳細については、エクストラネット VPN の作成または編集 （90 ページ）を参照してください。

  • [ハブインターフェイス（Hub Interface）] タブ：選択されたデバイスが大規模 DMVPN におけるハブである場合、IPsec ターミネータに接続されたインターフェイスを指定します。大規模 DMVPN の設定を参照してください。

  • [保護対象ネットワーク（Protected Networks）] タブ：暗号化されるネットワークを定義します（エンドポイントの保護対象ネットワークの特定 （62 ページ）を参照）。保護対象ネットワークは、インターフェイスロール、ネットワーク/ホストオブジェクト、または通常の IPsec の場合は ACL ポリシーオブジェクトです。

  • [FWSM] タブ：Firewall Services Module（FWSM）と、Catalyst 6500/7600 デバイスにすでに設定されている IPsec VPN サービスモジュール（VPNSM）または VPNSPA/VSPA との間を接続できるようにするための設定を定義します。この設定は、ハブがこれらのモジュールがインストールされた Catalyst 6500/7600 デバイスであるハブアンドスポーク トポロジでだけ可能です。詳細については、VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 （64 ページ）を参照してください。

  • [VRF対応IPsec（VRF Aware IPsec）] タブ：ハブアンドスポーク VPN トポロジにおいて、ハブ（IPsec アグリゲータ）に VRF-Aware IPsec ポリシーを設定します。詳細については、VRF 対応 IPsec の設定 （66 ページ）および VRF 対応 IPsec について （20 ページ）を参照してください。

  • [クリプトマップ（Crypto Map）] タブ：各ピアのクリプトマップ名とクリプト ACL 名を手動で設定します。これは、バージョン 4.7 以降の Security Manager でサポートされます。クリプトマップとクリプト ACL は、通常の IPSec テクノロジーでサポートされています。したがって、この設定は、通常の IPSec テクノロジーを使用するトポロジにのみ適用できます。詳細については、クリプトマップの設定 （69 ページ）を参照してください。

- 各デバイスのインターフェイスロールに関連付けられている実際のインターフェイスを表示するには、テーブルの下にある [表示（Show）] リストの [一致するインターフェイス（Matching Interfaces）] を選択します。一致するインターフェイスがない場合は、「一致なし（No Match）」と表示されます。デフォルトでは、インターフェイス ロール ポリシーオブジェクト名が表示されます。有効な VPN を作成するには、これらのロールがデバイスに定義されている実際のインターフェイスに一致する必要があります。

関連項目

- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

VPN インターフェイス エンドポイントの設定

[Edit Endpoints] ダイアログボックスの [VPN Interface] タブを使用して、[Endpoints] テーブルのデバイスに定義された VPN インターフェイスを編集します。ルータ デバイスのプライマリ VPN インターフェイスを定義する場合は、プライマリ ルート VPN インターフェイスの接続リンクが利用できなくなった場合にフォールバック リンクとして使用するバックアップ インターフェイスも設定できます。バックアップ インターフェイスは、ポイントツーポイント トポロジまたは完全メッシュ トポロジにある Cisco IOS セキュリティ ルータ、ハブアンドスポーク トポロジのスポークとなっている Cisco IOS セキュリティ ルータ、または Easy VPN トポロジのリモート クライアントとなっている Cisco IOS セキュリティ ルータで設定できます。詳細については、ダイヤル バックアップの設定 （54 ページ）を参照してください。

ヒント

- デバイスが大規模 DMVPN のハブである場合、このタブは [ハブインターフェイス（Hub Interface）] と呼ばれます。[IPsecターミネータに接続されたハブインターフェイス（Hub Interface Toward the IPsec Terminator）] フィールドで、IPsec ターミネータに接続されているインターフェイスを指定します。インターフェイスまたはインターフェイスロール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します。詳細については、大規模 DMVPN の設定を参照してください。
- デバイスが Catalyst 6500/7600 デバイスの場合、[VPN Interface] タブでは、デバイスの VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA ブレードを設定できます。Catalyst 6500/7600 デバイスの場合に [VPN Interface] タブに表示される要素の詳細については、VPNSM または VPN SPA/VSPA エンドポイントの設定 （58 ページ）を参照してください。次の表では、デバイスが Catalyst 6500/7600 デバイスではない場合について示します。

ナビゲーション パス

[VPNの作成（Create VPN）] ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページ、あるいは [VPNピア（VPN Peers）] ポリシーでデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [VPNインターフェイス（VPN Interfaces）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義（46 ページ）を参照してください。

フィールド リファレンス

表 *6 : [Edit Endpoints]* ダイアログボックスの *[VPN Interface]* タブ

要素	説明
Enable the VPN Interface Changes on All Selected Peers	[Endpoints] ページで編集用に複数のデバイスを選択した場合に使用可能です。 選択されている場合は、[VPN interface] タブで行った変更内容が、選択したすべてのデバイスに適用されます。
VPN Interface	選択したデバイスに定義された VPN インターフェイスです。インターフェイスを識別するインターフェイス ロール ポリシー オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか、新しいインターフェイス ロール オブジェクトを作成します。（インターフェイス ロール オブジェクトの作成 を参照。） （注） デバイスでクリプトマップを手動で設定する場合は、ピアインターフェイスの名前ではなく IP アドレスを指定する必要があります。 デバイスが ASA 5505 バージョン 7.2(1) 以降である場合は、異なるセキュリティ レベルを持つ 2 つのインターフェイスを定義する必要があります。詳細については、デバイスインターフェイス、ハードウェア ポート、ブリッジ グループの管理を参照してください。
VPN クライアントインターフェイス	選択したデバイスに定義された VPN クライアント インターフェイスです。[選択（Select）] をクリックして、リストから選択します。Cisco Security Manager 4.17 から、Easy VPN のクライアント インターフェイスを指定できます。これは以下に適用されます。 • ASA 5506 デバイス以降 • BVI インターフェイスまたはその他の物理インターフェイス（BVI メンバーインターフェイス以外） • ハブ アンド スポーク トポロジのデバイス
VPN クライアントのセキュアインターフェイス	4.17 以降、Cisco Security Manager は ASA 9.9(2) の BVI に対する EzVPN 機能の対応をサポートします。このフィールドでは、保護されたインターフェースを定義できます。トンネル確立のために保護されたネットワークとして機能するインターフェースを選択します。この機能は、次の場合にのみ適用されます。 • EasyVPN トポロジ • スポークインターフェイス • ASA 9.9.2 デバイス以降

要素	説明
接続タイプ	選択したデバイスが ASA または PIX 7.0+ デバイスであり、かつ選択したテクノロジーが通常の IPsec の場合にだけ、ハブアンドスポーク VPN トポロジで使用できます。 SA ネゴシエーション中にハブまたはスポークが使用する接続のタイプを選択します。 • [応答のみ（Answer Only）]：ハブが、SA ネゴシエーションへの応答だけを行い、SA ネゴシエーションを開始しないように設定します。これは、ハブの場合のデフォルトです。 • [発信のみ（Originate Only）]：デバイスが、SA ネゴシエーションの開始だけを行い、SA ネゴシエーションには応答しないように設定します。これは、スポークの場合のデフォルトです。 • [双方向（Bidirectional）]：ハブまたはスポークが、SA ネゴシエーションの開始および SA ネゴシエーションへの応答の両方を行うように設定します。

要素	説明
Local Peer IPSec Termination	選択したテクノロジーが Easy VPN の場合は使用できません。 ローカル ルータの VPN インターフェイスの IP アドレスを指定します。次のいずれかのオプションを選択できます。 • [トンネル送信元のIPアドレス（Tunnel Source IP Address）]：トンネル送信元の IP アドレスを使用します。 • [VPNインターフェイスのIPアドレス（VPN Interface IP Address）]：選択した VPN インターフェイスに設定された IP アドレスを使用します。インターフェイス ロールに一致できるのは、1 つの VPN インターフェイスだけです。このオプションは、GRE Modes ポリシーで [各トンネルに一意のトンネル送信元を設定（Configure Unique Tunnel Source for each Tunnel）] を選択した場合にだけ使用できます。 （注） バージョン 4.9 以降、Security Manager では IPv6 アドレスを選択できます。この機能は、IPv6 アドレスを持つインターフェイスでサポートされており、ASA ソフトウェア バージョン 9.0 以降を実行しているデバイスに適用されます。また、IPv6 アドレスのオプションは、Regular IPSec テクノロジでのみ使用できます。 • [IPアドレス（IP Address）]：ローカルルータの VPN インターフェイスの IP アドレスを明示的に指定します。このオプションは、デバイスが NAT 境界の背後にあり、NAT IP アドレスを指定する場合に使用します。バージョン 4.9 以降、Security Manager では IPv6 アドレスを指定できます。 （注） VPN インターフェイスとしてトンネル ソースを選択した場合は、VPN インターフェイスに IP アドレスが動的に割り当てられている可能性があります。 • [別の既存のインターフェイスのIPアドレスをローカルアドレスとして使用（IP Address of Another Existing Interface to be Used as Local Address）]（IPsec テクノロジーが DMVPN の場合は使用不可）：任意のインターフェイスに設定された IP アドレスをローカルアドレスとして使用します（VPN インターフェイスにかぎりません）。提供されたフィールドにインターフェイスを入力します。 [選択（Select）] をクリックして、必要なインターフェイスを選択できます。すべての使用可能な定義済みのインターフェイス ロールが示されたダイアログボックスが表示されます。このダイアログボックスでは、インターフェイス ロール オブジェクトを作成できます。

要素	説明
トンネルの送信元	IPsec/GRE または DMVPN でだけ使用可能です。 **[GREモード（GRE Modes）] > [トンネルパラメータ（Tunnel Parameters）]** タブで、トンネルインターフェイスごとに一意のトンネルソースを使用する設定を有効にしている場合、[トンネルインターフェイスごとに一意のトンネルソースをオーバーライド（Override Unique Tunnel Source per Tunnel Interface）] チェックボックスが使用可能になります。このオプションを選択して、選択したデバイスに別のトンネル ソースを指定します。 スポーク側の GRE または DMVPN トンネルで使用するトンネル ソース アドレスを指定します。次のいずれかのオプションを選択できます。 • [VPNインターフェイス（VPN Interface）]：トンネルソースアドレスとして、VPN インターフェイスを使用します。 • [インターフェイス（Interface）]：任意のインターフェイスをトンネルソースアドレスとして使用します。VPN インターフェイスにかぎりません。インターフェイス名を入力します。または、[選択（Select）] をクリックして、インターフェイスを識別するインターフェイスロールを選択します（選択ダイアログボックスからロールを作成することもできます）。
Dial Backup Settings	
Enable Backup	選択したデバイスが、ポイントツーポイント トポロジまたは完全メッシュ トポロジにある IOS ルータ、ハブアンドスポーク トポロジのスポークとなっている IOS ルータ、または Easy VPN トポロジのリモート クライアントとなっている IOS ルータの場合に使用できます。 プライマリ ルート VPN インターフェイスの接続リンクが利用できなくなった場合にフォールバック リンクとして使用するバックアップ インターフェイスを設定するかどうかを指定します。 **ヒント** バックアップインターフェイスを設定する前に、まずデバイスでダイヤラインターフェイスを設定する必要があります。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイスを参照してください。
ダイヤラ インターフェイス	ダイヤラ インターフェイスがアクティブになったときに、セカンダリ ルート トラフィックが送信される論理インターフェイスです。シリアルインターフェイス、非同期インターフェイス、または BRI インターフェイスを選択できます。 インターフェイスまたはインターフェイス 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します。

要素	説明
Primary Next Hop IP Address	選択されたテクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合にだけ使用できます。 プライマリ インターフェイスがアクティブな場合に接続する IP アドレスです。これは、ネクスト ホップ IP アドレスと呼ばれています。 ネクスト ホップ IP アドレスを指定しない場合、Security Manager は、VPN インターフェイス名を使用してスタティック ルートを設定します。VPN インターフェイスはポイントツーポイントである必要があります。それ以外の場合は、展開に失敗します。 [選択（Select）] をクリックして、必要な IP アドレスを選択できます。ネットワーク/ホストセレクタが開き、そこで IP アドレスの割り当て元のネットワークを選択できます。
Tracking IP Address	プライマリ VPN インターフェイス接続からの接続を維持する必要がある宛先デバイスの IP アドレスです。Service Assurance Agent では、プライマリ ルートを経由してこのデバイスに対して ping を実行し、接続性を追跡します。このデバイスへの接続が失われた場合にバックアップ接続がトリガーされます。 IP アドレスを指定しない場合は、ハブアンドスポークまたは Easy VPN トポロジでプライマリ ハブ VPN インターフェイスが使用されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ピア VPN インターフェイスが使用されます。 [選択（Select）] をクリックして、必要な IP アドレスを選択できます。ネットワーク/ホストセレクタが開き、そこで IP アドレスの割り当て元のネットワークを選択できます。
[Advanced] ボタン	選択したテクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合に使用できます。 [Dial Backup Settings] ダイアログボックス （56 ページ）を使用して、追加のオプションの設定を行うには、このボタンをクリックします。

ダイヤル バックアップの設定

ダイヤルバックアップを使用すると、プライマリ リンクが利用できなくなった場合に備えて、直接のプライマリ接続に対するフォールバック リンクを提供できます。ダイヤル バックアップは、ポイントツーポイント、エクストラネット、または完全メッシュ VPN トポロジに参加している Cisco IOS セキュリティ ルータ、あるいはハブアンドスポーク トポロジのスポークとなっている Cisco IOS セキュリティ ルータで設定できます。Easy VPN トポロジにおいて IOS バージョン 12.3(14)T+ を実行するリモート クライアント ルータでも設定できます。

ダイヤル バックアップ機能は、次の 2 つのスタティック ルートが存在するという前提に基づいて実装されています。

- プライマリ ゲートウェイ経由の、最も高いプライオリティを持つプライマリ ルート

- セカンダリ ゲートウェイ経由の、低いプライオリティを持ち、プライマリ ゲートウェイがダウンしたときにだけルーティング テーブルに表示されるセカンダリ ルート

Security Manager によって、スポークに論理ダイヤラ インターフェイスが設定されます。このダイヤラインターフェイスは、物理的なバックアップインターフェイスに関連付けられます。プライマリ ルートがダウンすると、ダイヤラ インターフェイスがアクティブになり、トラフィックはこのバックアップ インターフェイス経由でセカンダリ ルートにリダイレクトされます。スポークとハブとの間のトラフィックが暗号化されるように、Security Manager によってダイヤラ インターフェイスに対してクリプト マップが適用されます。このクリプト マップは、VPN インターフェイス（プライマリ ルート インターフェイス）のクリプト マップと同一のものです。Easy VPN では、バックアップ設定は、ダイヤラ インターフェイスに追加されます。

IOS バージョンによっては、Response Time Reporter（RTR）または Service Level Agreement（SLA; サービス レベル契約）IOS テクノロジーを使用して、プライマリ ルートでのネットワークのパフォーマンス低下が検出されます。割り当てられている IPsec テクノロジーが DMVPN である場合は、Dialer Watch-List（DWL）が使用されます。

ISDN Basic Rate Interface（BRI; 基本インターフェイス）およびアナログ モデム インターフェイスを他のプライマリ インターフェイスに対するバックアップ インターフェイスとして設定できます。この場合、ISDN またはアナログ モデム接続は、プライマリ インターフェイスがダウンした場合に確立されます。プライマリ インターフェイスおよびその接続がダウンすると、ISDN またはアナログ モデム インターフェイスからすぐにダイヤルアウトが実行されて、ネットワーク サービスが停止しないように接続が確立されます。

はじめる前に

- Cisco IOS ルータでダイヤラ インターフェイスを設定します。このためには、物理 BRI および非同期インターフェイス間の関係、およびダイヤルバックアップを設定する場合に使用する仮想ダイヤラインターフェイスを定義する必要があります。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイスを参照してください。
- プライマリ ルートが機能していることを確認します。
- エクストラネット VPN の場合、ローカル（管理対象）デバイスのみにダイヤルバックアップを設定できます。

ステップ 1 ほとんどの VPN トポロジの場合、サイト間 VPN の作成時または編集時にダイヤル バックアップを設定します。既存 VPN トポロジの Peers ポリシーを編集することもできます。エクストラネット VPN の場合、Peers ポリシーを介してのみダイヤル バックアップを設定できます。

次のいずれかを実行します。

- Create VPN ウィザードで、[Endpoints] ページに進みます（VPN トポロジの作成または編集 （38 ページ）およびエンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照）。
- [VPN の編集（Edit VPN）] ダイアログボックスで、[エンドポイント（Endpoints）] タブをクリックします（VPN トポロジの作成または編集 （38 ページ）およびエンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照）。

- エクストラネット VPN の場合、またはその他の VPN トポロジを編集する場合、[Peers] ポリシーを選択します。エンドポイント編集の一般情報については、エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。

ステップ 2 ダイヤルバックアップを設定するルータを選択して、[編集（Edit）]（鉛筆）ボタンをクリックします。同じダイヤラ設定を行うルータが複数ある場合は、それらを選択して、同時に編集できます。

これにより、[Edit Endpoints] ダイアログボックスが開きます。[VPN インターフェイス（VPN Interface）] タブが選択されていない場合は、このタブを選択します。

ステップ 3 [VPN Interface] タブで、ダイヤル バックアップに関する次のオプションを設定します。新しい VPN を作成している場合は、VPN インターフェイスなどの他の設定も行う必要があります。これらのオプションの詳細については、VPN インターフェイス エンドポイントの設定 （49 ページ）を参照してください。

- [バックアップの有効化（Enable Backup）]：このオプションを選択します。
- [ダイヤラインターフェイス（Dialer Interface）]：論理ダイヤラインターフェイスがアクティブになったときに、セカンダリ ルート トラフィックが送信される物理インターフェイスを指定します。
- [プライマリネクストホップ IP アドレス（Primary Next Hop IP Address）]：選択した IPsec テクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合、ネクストホップ IP アドレスを入力します。ネクスト ホップ IP アドレスを入力しない場合、Security Manager は、インターフェイス名を使用してスタティック ルートを設定します。
- [追跡 IP アドレス（Tracking IP Address）]：プライマリ VPN インターフェイス接続からの接続を維持する必要がある宛先デバイスの IP アドレスを指定します。これは、接続性を追跡するために、プライマリ ルートを経由して ping が実行されるデバイスです。このデバイスへの接続が失われた場合にバックアップ接続がトリガーされます。

IP アドレスを指定しない場合は、ハブアンドスポークまたは Easy VPN トポロジでプライマリ ハブ VPN インターフェイスが使用されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ピア VPN インターフェイスが使用されます。

ステップ 4 選択した IPsec テクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合は、[詳細設定（Advanced）] をクリックして、[ダイヤルバックアップ設定（Dial Backup Settings）] ダイアログボックスで追加の（任意の）設定を行います。これらの設定については、[Dial Backup Settings] ダイアログボックス （56 ページ）で説明します。[OK] をクリックして変更を保存します。

ステップ 5 [エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [OK] をクリックします。

[Dial Backup Settings] ダイアログボックス

[Dial Backup Settings] ダイアログボックスを使用して、サイト間 VPN にダイヤル バックアップ ポリシーを設定するためのオプションの設定を定義します。これらの設定は、通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN テクノロジーにおいて使用できます。

ダイヤル バックアップの必須の設定は、[Edit Endpoints] ダイアログボックスの [VPN Interface] タブで行います。VPN インターフェイス エンドポイントの設定 （49 ページ）を参照してください。

（注） ダイヤラ インターフェイスを設定しないと、ダイヤル バックアップは正常に動作しません。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイスを参照してください。

ナビゲーション パス

[ダイヤルバックアップ設定（Dial Backup Settings）] ダイアログボックスを開くには、ダイヤルバックアップを有効にして、[エンドポイントの編集（Edit Endpoints）] ダイアログボックスの [VPNインターフェイス（VPN Interface）] タブにある [詳細設定（Advanced）] をクリックします。[Edit Endpoints] ダイアログボックスを開く方法については、エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。

関連項目

- ダイヤル バックアップの設定 （54 ページ）
- Easy VPN について

フィールド リファレンス

表 *7 : [Dial Backup Settings]* ダイアログボックス

要素	説明
Next Hop Forwarding Backup Next Hop IP Address	必要に応じて、ISDN BRI またはアナログ モデム バックアップ インターフェイスのネクスト ホップ IP アドレス（バックアップ インターフェイスがアクティブになったときに接続する IP アドレス）を入力します。IP アドレス、またはネットワーク/ホスト オブジェクトの名前を入力できます。または、[Select] をクリックして、IP アドレスを指定するネットワーク/オブジェクトを選択します。 ネクスト ホップ IP アドレスを入力しない場合、Security Manager は、インターフェイス名を使用してスタティック ルートを設定します。
Tracking Object Settings	
タイムアウト（Timeout）	Service Assurance Agent の動作において、宛先デバイスからの応答を受信するまで待機するミリ秒単位の時間です。デフォルトは 5000 ms です。
周波数（Frequency）	プライマリ ルートのパフォーマンスの低下を検出するために Response Time Reporter（RTR）を使用する頻度です。デフォルトは 60 秒ごとです。

要素	説明
[しきい値（Threshold）]	RTR 動作において、対応イベントを生成し、履歴情報を保存する、ミリ秒単位の上昇しきい値です。デフォルトは 5000 ms です。

VPNSM または VPN SPA/VSPA エンドポイントの設定

[Endpoints] テーブルで編集用に Catalyst 6500/7600 デバイスを選択した場合、[Edit Endpoints] ダイアログボックスの [VPN Interface] タブで、デバイスに Cisco VPN Services Module（VPNSM; VPN サービス モジュール）、Cisco VPN Shared Port Adapter（VPN SPA; VPN 共有ポート アダプタ）、および Cisco VPN Service Port Adapter（VSPA; VPN サービス ポート アダプタ）を設定できます。同時に複数の Catalyst 6500/7600 デバイスを選択できます。変更内容は、選択したすべてのデバイスに適用されます。

Security Manager によって管理されたポイントツーポイントまたは完全メッシュ VPN トポロジ内のデバイス、またはハブアンドスポーク VPN トポロジ内のハブやスポークをデバイスとして選択できます（Easy VPN では、スポークをデバイスとして選択することはできません）。これらの設定は、選択したデバイスが大規模 DMVPN における IPsec ターミネータである場合にも設定する必要がありますが、次に示すすべての設定が使用できるわけではありません。大規模 DMVPN の設定を参照してください。

一般的な注意点

- Catalyst 6500/7600 デバイスには、3 ～ 13 のシャーシ スロットが備えられています。ブレードの設計上、スロットあたり 1 つの VPNSM または 2 つの VPNSPA/VSPA をインストールできます。VPNSPA/VSPA の位置は、スロット番号とサブスロット番号で識別されます。Security Manager は、この情報をインベントリに保存して、VPN トポロジを管理できるようにします。
- シャーシ内のハイ アベイラビリティを設定する場合は、同じデバイスで VPNSM ブレードと VPNSPA/VSPA ブレードをプライマリ ブレードおよびフェールオーバー ブレードとして使用することはできません。
- リモート アクセス VPN では、各 IPsec プロポーザルに対して 1 つのフェールオーバー装置だけを設定できます。[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックスを参照してください。
- Catalyst 6500/7600 に Firewall Services Module（FWSM; ファイアウォール サービス モジュール）がある場合は、これらのモジュールと連携して動作するように設定できます。詳細については、VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 （64 ページ）を参照してください。
- デバイスで VRF 対応 IPsec とともに VPNSM または VPNSPA/VSPA を設定する場合、そのデバイスは、VRF 対応 IPsec が設定されていない別の VPN トポロジに属することができません。詳細については、VRF 対応 IPsec の設定 （66 ページ）を参照してください。

- Catalyst 6500/7600 デバイスに内部 VLAN を作成するか、または既存のポートや VLAN 設定を編集します。デバイスに VRF 対応 IPsec が設定されている場合は、転送 VLAN を作成する必要があります。

VPNSM に関する注意点

- Security Manager では、Catalyst 6500/7600 デバイスにおける複数の VPNSM の設定がサポートされていますが、VPN トポロジあたり 1 つ（シャーシ内のハイ アベイラビリティを設定する場合は 2 つ）のモジュールだけを設定できます。
- VPNSM を設定する場合、親の Catalyst 6500/7600 デバイスで Cisco IOS ソフトウェア Release 12.2(18)SXD1 以降が実行されている必要があります。
- VPNSM 設定では、レイヤ 3 VLAN だけを使用できます。

VPNSPA/VSPA に関する注意点

- この設定は、大規模 DMVPN 設定で IPsec ターミネータを設定する場合にも適用されます。詳細については、大規模 DMVPN の設定を参照してください。
- VPN SPA では、すべてのキー サイズ（128、192、および 256 ビット）の AES 暗号化アルゴリズム、および DES 暗号化アルゴリズムと 3DES 暗号化アルゴリズムがサポートされています。詳細については、使用する暗号化アルゴリズムの決定を参照してください。

VRF モードでは、**crypto engine slot** *slot/subslot* {**inside** | **outside**} コマンドは内部および外部 VPN インターフェイスに展開されます。

- Catalyst 6500/7600 デバイスで、Cisco IOS ソフトウェア Release 12.2(18)SXE2 以降を実行している必要があります。
- 暗号接続代替モード（このモードでは、暗号化されたトラフィックが VPNSM/VPN SPA で受信された場合はパススルーされ、クリアテキストのトラフィックは迂回されます）を使用する予定の場合、Catalyst 6500 デバイスでは Cisco IOS ソフトウェア バージョン 12.2(33)SXH 以降が、7600 ルータでは 12.2(33)SRA 以降が実行されている必要があります。
- 複数のハブが参加する DMVPN トポロジで 1 つのハブに VPN SPA ブレードが設定されている場合は、スポークであるかハブであるかにかかわらず、いずれのデバイスにもトンネルキーを設定しないでください。このようなトポロジに参加するデバイスでは、キーなしでのトンネルをサポートするために Cisco IOS ソフトウェア バージョン 12.3T 以降が実行されている必要があります。

ナビゲーション パス

Create VPN ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページ、あるいは [VPNピア（VPN Peers）] ポリシーで Catalyst 6500/7600 デバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックス

で[FWSM] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。

フィールド リファレンス

表 *8 : [*エンドポイントの編集（*Edit Endpoints*）*]* ダイアログボックス、*[VPN*インタフェース（*VPN Interface*）*]* タブの *[VPNSM/VPN SPA/VSPA*設定（*VPNSM/VPN SPA/VSPA Settings*）*]*

要素	説明
Enable the VPN Interface Changes on All Selected Peers	（注） [Endpoints] ページで、編集用に複数の Catalyst 6500/7600 デバイスを選択した場合に使用できます。 選択されている場合は、[VPN interface] タブで行った変更内容が、選択したすべてのデバイスに適用されます。
VPNSM/VPN SPA/VSPA Settings	• [暗号接続代替の使用（Use Crypto Connect Alternate）]：選択されている場合、Catalyst 6500/7600 上の VPNSM/VPN SPA に入った暗号化されたトラフィックだけがパススルーされます。クリアテキストのトラフィックは、アダプタを通過しません（迂回されます）。このオプションを使用するには、Catalyst 6500 ではバージョン 12.2(33)SXH 以降が、7600 ルータでは 12.2(33)SRA 以降が実行されている必要があります。 このモードは、大規模な VPN トポロジをサポートする必要がある企業のお客様（金融機関など）や、暗号化されたチャネル上で大量のデータを送信する必要がある企業のお客様（インターネット上でのリモートディザスタリカバリやバックアップなど）にとって、暗号接続モードの代替選択肢として推奨されます。 • [内部VLAN（Inside VLAN）]：サービスモジュールまたはアダプタへの内部インターフェイスとして機能する VLAN です。また、VPN トンネルのハブ エンドポイントでもあります（デバイスに VRF 対応 IPsec が設定されていない場合）。VLAN またはインターフェイス 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します。 • [スロットとサブスロット（Slot and Subslot）]：VPNSM または VPNSPA/VSPA のスロット位置を指定する番号です。VPNSPA/VSPA を設定する場合は、サブスロット番号も必要です。 • [外部VLAN/外部ポート（Outside VLAN/External port）]：内部 VLAN に接続する外部ポートまたはVLAN です。VLAN またはインターフェイス 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します。内部 VLAN に選択したものとは異なるインターフェイスまたはインターフェイス ロールを選択する必要があります。 （注） VRF 対応 IPsec がデバイスに設定されている場合は、外部ポートまたは VLAN に IP アドレスが必要です。

要素	説明
トンネルの送信元	（注） 選択されたテクノロジーが IPsec/GRE または DMVPN の場合は、ハブに対してだけ使用できます。 スポーク側の GRE または DMVPN トンネルで使用するトンネル ソース アドレスを指定します。次のいずれかのオプションを選択できます。 • [トンネルインターフェイスごとに一意のトンネルソースをオーバーライド（Override Unique Tunnel Source per Tunnel Interface）]：[GREモード（GRE Modes）] > [トンネルパラメータ（Tunnel Parameters）] タブで、トンネルインターフェイスごとに一意のトンネルソースを使用する設定を有効にしている場合、このオプションが選択可能になります。このオプションを選択して、選択したデバイスに別のトンネル ソースを指定します。 • [外部VLAN/外部ポート（CCA/VRFが有効な場合）（Outside VLAN/External Port (When CCA/VRF is Enabled)）]：[暗号接続代替の使用（Use Crypto Connect Alternate）] チェックボックスがオンになっている場合、このオプションボタンが使用可能になります。選択されている場合、外部 VLAN または外部ポートがトンネル ソースとして指定されます。 • [内部VLAN（Inside VLAN）]：選択されている場合、内部 VLAN に設定されているインターフェイスがトンネルソースとして使用されます。 • [インタフェース（Interface）]：任意のインターフェイス（VPN インターフェイスとは限らない）をトンネルソースアドレスとして使用するには、インターフェイス名を入力するか、または [選択（Select）] をクリックしてインターフェイスを識別するインターフェイスロールを選択します。選択リストから新しいロールを作成することもできます。
Local Peer IPSec Termination	ローカル ルータに、VPN インターフェイスの IPsec 終端ポイントを定義します。 • [内部VLAN（Inside VLAN）]：内部 VLAN として設定されているインターフェイスを使用します。 • [IPアドレス（IP Address）]：ローカルルータの VPN インターフェイスの IP アドレスを使用します。IP アドレスを入力します。 （注） VPNインターフェイスとしてトンネル ソースを選択した場合は、VPN インターフェイスに IP アドレスが動的に割り当てられている可能性があります。

要素	説明
Enable Failover Blade	シャーシ内のハイ アベイラビリティを確保するために、フェールオーバー VPNSM または VPNSPA/VSPA ブレードを設定するかどうかを指定します。 （注） 同じデバイスで VPNSM ブレードと VPNSPA/VSPA ブレードをプライマリ ブレードおよびフェールオーバー ブレードとして使用することはできません。 次のように、フェールオーバー ブレードを指定します。 • [スロット（Slot）]：VPNSM ブレードまたは VPNSPA/VSPA ブレードの位置を特定するスロット番号です。 • [サブスロット（Subslot）]：VPNSPA/VSPA を設定する場合は、フェールオーバー VPN SPA ブレードがインストールされているサブスロットの番号（0 または 1）を選択します。 （注） VPNSM を設定している場合は、ブランク オプションを選択します。

エンドポイントの保護対象ネットワークの特定

[Edit Endpoints] ダイアログボックスの [Protected Networks] タブを使用して、[Endpoints] テーブルのデバイスに定義された保護対象ネットワークを編集します（エンドポイントおよび保護対象ネットワークの定義 （46 ページ） を参照。）

保護対象ネットワークは、命名パターンがデバイスの内部 VPN インターフェイスと一致するインターフェイス ロールとして指定することも、1 つ以上のネットワークやホストの IP アドレス、インターフェイス、その他のネットワーク オブジェクトを含むネットワーク/ホスト グループ オブジェクトとして指定することも、（割り当てられているテクノロジーが通常の IPsec の場合には）アクセス コントロール リスト オブジェクトとして指定することもできます。

- 同時に複数のデバイスを編集している場合は、[選択したすべてのピアで保護されたネットワークの変更を有効にする（Enable the Protected Networks Changes on All Selected Peers）] を選択して、[保護されたネットワーク（Protected Networks）] タブで行ったすべての変更内容を選択されたすべてのデバイスに適用します。
- 保護されたネットワークを追加するには、[使用可能な保護されたネットワーク（Available Protected Networks）] リストからネットワークを選択し、[>>] をクリックして、[選択済みの保護されたネットワーク（Selected Protected Networks）] リストに移動します。インターフェイス ロール オブジェクト、（[Protected Networks] フォルダに表示された）ネットワーク/ホスト グループ オブジェクト、またはアクセス コントロール リスト オブジェクトの任意の組み合わせを使用して、デバイスの保護対象ネットワークを定義できます（ACL オブジェクトは、割り当てられたテクノロジーが通常の IPsec の場合にだけ使用できます）。

バージョン 4.9 以降、Security Manager では IPv6 アドレスがサポートされます。

- [保護されたネットワーク（Protected Networks）] フォルダでは、IPv6 オブジェクトがサポートされるようになりました。

- [アクセスコントロールリスト（Access Control Lists）] フォルダでは、拡張および統合 ACL がサポートされるようになりました。
- インターフェイスロールの場合、IPv6 が有効なインターフェイスを選択して [>>] をクリックすると、設定されているすべての IPv6 アドレスのリストを含むポップアップウィンドウが表示されます。リストからアドレスを選択し、[OK] をクリックして、そのアドレスを [選択済みの保護されたネットワーク（Selected Protected Networks）] リストに移動できます。アドレスを編集するには、[選択済みの保護されたネットワーク（Selected Protected Networks）] リストでアドレスを選択し、[選択の編集（Edit Selection）] リンクをクリックします。
- エクストラネット VPN の場合、リモートバックアップピアでは IPv6 アドレスがサポートされます。

（注） 割り当てられているテクノロジーが通常の IPsec であるハブアンドスポーク VPN トポロジで ACL オブジェクトを使用してスポークで保護対象ネットワークが定義されている場合、Security Manager によってハブ上のスポークの ACL オブジェクトが、一致するクリプトマップエントリにミラーリングされます。

クリプトマップエントリを指定しない場合、展開時に Security Manager は、ハブデバイスのクリプト ACL 名を、スポーク デバイスの ACL オブジェクト名に「_1」を付加して生成します。たとえば、スポークの ACL オブジェクト名が「spokeACL」である場合、Security Manager はハブデバイスのクリプト ACL 名を「spokeACL_1」として生成します。同じ ACL オブジェクト名を持つ複数のスポークデバイスが存在する場合、Security Manager はハブ デバイスのクリプト ACL 名を「ACLobjectName_spokeDisplayName_1」として生成します。

ここで、「ACLobjectName」はトポロジ内のすべてのスポークデバイスの ACL オブジェクト名であり、「spokeDisplayName」はスポークごとに異なるスポークデバイスの表示名です。

Cisco Security Manager は、次のいずれかを実行すると、トポロジタイプに関係なく、ASA デバイスの新しい ACL を作成します。

- 保護されたネットワークにエントリを追加する。
- 既存のハブアンドスポークトポロジの [VPNグローバル設定（VPN Global Setting）] > [全般設定（General Settings）] タブで、[スポーク間接続を有効にする（Enable Spoke to spoke connectivity）] チェックボックスをオンにする。
- 既存のハブアンドスポークトポロジに新しいピアを（スポークとして）追加する。

即座に生成されるこの新しい ACL は、VPN トラフィックを混乱させる可能性があります。したがって、保護されたネットワークで ACL 構成要素を使用して直接変更を行うことをお勧めします。

- 選択済みの保護されたネットワークを削除するには、ネットワークを選択して、[<<] ボタンをクリックします。

- オブジェクトの順序が問題となる場合は、上向き矢印ボタンと下向き矢印ボタンを使用して、必要に応じて選択されたオブジェクトのリスト内でオブジェクトのプライオリティの順序を調整できます。順序が問題とならない場合には、これらのボタンは使用できません。
- 保護されたネットワークを定義するために必要なオブジェクトがリストに表示されていない場合は、[作成（Create）]（+）ボタンをクリックしてオブジェクトを追加します。この場合、追加するオブジェクトのタイプを選択するように求められます。既存のオブジェクトを選択し、[編集（Edit）]（鉛筆）ボタンをクリックして、既存のオブジェクトの定義を変更することもできます。 詳細は、次のトピックを参照してください。
  - インターフェイス ロール オブジェクトについて、インターフェイス ロール オブジェクトの作成
  - ネットワーク/ホストオブジェクトについて、ネットワーク/ホストオブジェクトの作成
  - アクセス コントロール リスト オブジェクトの作成

ナビゲーション パス

VPNの作成（Create VPN）ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページ、あるいは [ピア（Peers）] ポリシーでデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [保護されたネットワーク（Protected Networks）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義（46 ページ）を参照してください。

VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定

（注） 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、FWSM はサポートが終了しているため、FWSM の拡張機能はサポートされません。

Security Manager では、Catalyst 6500/7600 デバイスに、IPsec VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA とともに Firewall Services Module（FWSM; ファイアウォールサービスモジュール）を設定できます。この機能を使用すると、VPNSM または VPN SPA/VSPA で内部ネットワークに対してセキュアなアクセスを提供するとともに、FWSM で信頼できないクライアントに対してファイアウォール ポリシーを適用できます。

FWSM と、Catalyst 6500/7600 デバイスにすでに設定されている VPNSM または VPNSPA/VSPA との間の接続を可能にする設定を定義するには、[Edit Endpoints] ダイアログボックスの [FWSM] タブを使用します。[FWSM] タブは、ハブアンドスポーク VPN トポロジにおいて、選択されたハブが Catalyst 6500/7600 デバイスの場合にだけ使用できます。

ヒント

- FWSM 設定を定義する前に、FWSM をホストする Catalyst 6500/7600 デバイスを Security Manager インベントリに追加して、FWSM とそのポリシーおよびセキュリティ コンテキストを検出する必要があります。ネットワークからのデバイスの追加およびセキュリティ コンテキストの管理を参照してください。
- Catalyst 6500/7600 デバイスで内部インターフェイスがまだ作成されていない場合は、内部インターフェイスを作成する必要があります（VLAN の作成または編集を参照）。その後、FWSM 内部インターフェイス（VLAN）を適切なセキュリティ コンテキストに割り当てるか、または FWSM ブレードに直接割り当てます。
- また、IPsec VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA に関連する設定を [VPN Interfaces] タブで行う必要があります。詳細については、VPNSM または VPN SPA/VSPA エンドポイントの設定 （58 ページ）を参照してください。

ナビゲーション パス

VPNの作成（Create VPN） ウィザードの [エンドポイント（Endpoints）] ページ、または [VPN の編集（Edit VPN）] ダイアログボックス、または [VPN ピア（VPN Peers）] ポリシーで、FWSM を搭載した Catalyst 6500/7600 デバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [FWSM] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。

フィールド リファレンス

表 9 : [Edit Endpoints] ダイアログボックスの [FWSM] タブ

要素	説明
Enable FWSM Settings	Catalyst 6500/7600 デバイスで、Firewall Services Module（FWSM; ファイアウォール サービス モジュール）と VPN Services Module（VPNSM; VPN サービス モジュール）または VPN SPA との間に接続を設定するかどうかを指定します。
FWSM Inside VLAN	Firewall Services Module（FWSM; ファイアウォール サービス モジュール）への内部インターフェイスとして機能する VLAN です。インターフェイスまたはインターフェイス ロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか新しいインターフェイス ロール オブジェクトを作成します。
FWSM Blade	使用可能なブレードのリストから、選択した FWSM 内部 VLAN インターフェイスが接続されているブレード番号を選択します。

要素	説明
セキュリティコンテキスト	FWSM 内部 VLAN がセキュリティ コンテキストの一部である場合（つまり、FWSM がマルチ コンテキスト モードで実行されている場合）、このフィールドにセキュリティ コンテキスト名を指定します。名前では、大文字と小文字が区別されます。

VRF 対応 IPsec の設定

[Edit Endpoints] ダイアログボックスの [VRF-Aware IPsec] タブを使用して、ハブアンドスポーク VPN トポロジ内のハブに VRF-Aware IPsec ポリシーを設定します。VRF 対応 IPsec は、1 ボックス ソリューションまたは 2 ボックス ソリューションとして設定できます。VRF 対応 IPsec の詳細については、VRF 対応 IPsec について （20 ページ）を参照してください。

ヒント

- VRF 対応 IPsec は、ハブアンドスポーク VPN トポロジのハブにだけ設定できます。
- 2 つのハブがある VPN トポロジでは、両方のデバイスに VRF 対応 IPsec を設定する必要があります。
- VRF 対応 IPsec が設定されていない他の VPN トポロジに属するデバイスに対して VRF 対応 IPsec を設定することはできません。
- ハイ アベイラビリティが設定されているハブに対して VRF 対応 IPsec を設定することはできません。VPN トポロジにおけるハイ アベイラビリティの設定 （71 ページ）を参照してください。
- IPsec Aggregator が、既存の事前共有キー（keyring）コマンドと同じ **keyring** CLI コマンドを使用して設定されており、他のコマンドによって参照されていない場合には、展開に失敗する場合があります。この場合、Security Manager では VRF keyring CLI が使用されず、異なる名前でキーリングが生成されるため、展開に失敗します。設定を展開する前に、事前共有キー keyring コマンドを CLI から手動で削除する必要があります。

ナビゲーション パス

[VPNの作成（Create VPN）] ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページで、ハブアンドスポーク トポロジ内の VRF 対応 IPsec 設定をサポートするデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [VRF対応IPsec（VRF-Aware IPsec）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （46 ページ）およびVPN トポロジの作成または編集 （38 ページ）を参照してください。

フィールド リファレンス

表 *10 : [Edit Endpoints]* ダイアログボックスの *[VRF Aware IPsec]* タブ

要素	説明
Enable the VRF Settings Changes on All Selected Peers	[Endpoints] ページで編集用に複数のデバイスを選択した場合に使用できます。 選択されている場合、[VRF Settings] タブで行ったすべての変更内容が、選択したすべてのデバイスに適用されます。
Enable VRF Settings	デバイスで VRF の設定をイネーブルにするかどうかを指定します。 （注） このチェックボックスの選択を解除することによって、VPN トポロジに定義された VRF 設定を削除できます。ただし、Catalyst 6500/7600 デバイスに VRF 対応 IPsec が設定されている場合、VRF 設定をディセーブルにするには追加の手順が必要となります。 Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化 （24 ページ）を参照してください。
VRF Solution	設定する VRF ソリューションのタイプを指定します。 • [1-Box]（IPsec Aggregator + MPLS PE）：1 ボックス ソリューションでは、1 つのデバイスが、パケットへの MPLS タギング、およびカスタマーエッジ（CE）デバイスとの間での IPsec 暗号化と復号化を行うプロバイダーエッジ（PE）ルータとして機能します。詳細については、 VRF 対応 IPsec 2 ボックス ソリューション （22 ページ）を参照してください。 • [2-Box]（IPsec Aggregator だけ）：2 ボックス ソリューションでは、PE デバイスは MPLS タギングだけを行います。CE との間の IPsec 暗号化および復号化は、IPsec Aggregator によって行われます。詳細については、 VRF 対応 IPsec 2 ボックス ソリューション （22 ページ）を参照してください。
[VRF名（VRF Name）]	IPsec Aggregator の VRF ルーティング テーブルの名前。VRF 名では、大文字と小文字が区別されます。

要素	説明
ルート識別子	IPsec Aggregator の VRF ルーティング テーブルの固有識別情報。この一意のルート識別子によって、MPLS コアおよび他の PE ルータにまたがる各 VPN のルーティングの分離が維持されます。 識別情報は次のいずれかの形式です。 • IP アドレス:X（X は 0 ～ 2147483647 の数値） • N:X（N は 0 ～ 65535 の数値、X は 0 ～ 2147483647 の数値） （注） VRF 設定をデバイスに展開したあとは RD 識別子を上書きできません。展開後に RD 識別子を変更するには、デバイス CLI を使用して手動で削除してから、再度展開する必要があります。
Interface Towards Provider Edge （2 ボックス ソリューションのみ）	IPsec Aggregator 上の、PE デバイスに向けた VRF 転送インターフェイス。IPsec Aggregator（ハブ）が Catalyst VPN サービス モジュールの場合は、VLAN を指定する必要があります。 インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか、新しいインターフェイス ロール オブジェクトを作成します。
ルーティング プロトコル（Routing Protocol） （2 ボックス ソリューションのみ）	IPsec Aggregator と PE との間で使用するルーティング プロトコル。オプションは、[BGP]、[EIGRP]、[OSPF]、[RIPv2]、または [Static route] です。デフォルトは BGP です。 保護された IGP で使用されるルーティング プロトコルが、IPsec Aggregator と PE との間で使用されるルーティング プロトコルと異なる場合は、保護された IGP へのルーティングの再配布に使用するルーティング プロトコルを選択します。 プロトコルの詳細については、ルータの管理を参照してください。 （注） 1 ボックス ソリューションでは、ルーティング プロトコルおよび AS 番号は指定する必要がないため、これらのフィールドは使用できません。1 ボックス ソリューションでは、BGP プロトコルだけがサポートされています。

要素	説明
AS 番号（AS Number） （2 ボックス ソリューション、BGP または EIGRP ルーティングだけ）	IPsec Aggregator と PE との間の自律システム（AS）領域の識別に使用する番号。AS 番号は、1 ～ 65535 の範囲である必要があります。 保護された IGP で使用されるルーティング プロトコルが、IPsec Aggregator と PE との間で使用されるルーティング プロトコルと異なる場合は、IPsec Aggregator および PE からルーティングが再配布される保護された IGP を識別するために使用する AS 番号を入力します。この設定は、IPsec/GRE または DMVPN が適用されている場合にだけ関連があります。
Process Number （2 ボックス ソリューション、OSPF ルーティングのみ）	OSPF ルーティングを使用している場合に、保護された IGP を識別するために使用するルーティング プロセス ID 番号。 範囲は 1 ～ 65535 です。
OSPF Area ID （2 ボックス ソリューション、OSPF ルーティングのみ）	パケットが属する領域の ID 番号。0 ～ 4294967295 の範囲の任意の番号を入力できます。 （注） すべての OSPF 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領域 ID 番号が必要です。
Next Hop IP Address （2 ボックス ソリューション、スタティック ルーティングだけ）	スタティック ルーティングを使用している場合の、IPsec Aggregator に接続されているプロバイダーエッジ（PE）またはインターフェイスの IP アドレス。
Redistribute Static Route （2 ボックス ソリューション、スタティック ルーティング以外だけ）	IPsec Aggregator に設定されたルーティング プロトコルで、スタティック ルートを PE デバイスにアドバタイズするかどうかを指定します。

クリプトマップの設定

バージョン 4.7 以降、Cisco Security Manager では、VPN トポロジ内の各ピアデバイスのクリプトマップ名とクリプト ACL 名を手動で設定できます。この機能は、通常の IPsec トポロジでのみサポートされています。

[エンドポイントの編集（Edit Endpoints）] ダイアログボックスの [クリプトマップ（Crypto Map）] タブを使用して、ピアに設定されているクリプトマップ名とクリプト ACL 名とともにピアデバイスを一覧表示します。リストでピアデバイスを選択し、[編集（Edit）]（鉛筆）ボタンをクリックすると、[クリプトマップエントリの編集（Edit Crypto Map Entry）] ダイアログボックスが開きます。

（注） トポロジがダイナミッククリプトマップをサポートしている場合、[編集（Edit）] ボタンをクリックすると開くダイアログボックスで、ダイナミッククリプトマップ名を入力できます。

ナビゲーション パス

Create VPN ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページでデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [クリプトマップ（Crypto Map）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （46 ページ）を参照してください。

フィールド リファレンス

表 *11 : [*エンドポイントの編集（*Edit Endpoints***）*]* ダイアログボックス、*[*クリプトマップ（***Crypto Map***）*]* タブ**

要素	デフォルト値（Default Value）
暗号マップ名（Crypto Map Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager はデバイスのクリプトマップ名を使用するか、または新しいクリプトマップ名を生成します。VPN インターフェイスにクリプトマップがすでに存在する場合、Cisco Security Manager は同じ名前を再利用します。
クリプトマップシーケンス（Crypto Map Sequence）	Cisco Security Manager は、管理対象ネットワークでデバイスを検出すると、このフィールドにデバイスのシーケンス番号を表示します。この値は編集できません。 新しい VPN トポロジを追加する場合、Cisco Security Manager は [シーケンス番号（Sequence Number）] フィールドに # の値を入力します。この値は編集できません。
クリプトACL名（Crypto ACL Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager は新しいクリプト ACL 名を生成します。
ダイナミッククリプトマップ名（Dynamic Crypto Map Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager はデバイスのクリプトマップ名を使用するか、または新しいクリプトマップ名を生成します。

- インターフェイスに適用できるクリプトマップは 1 つだけです。
- デバイスの複数のインターフェイスに同じクリプトマップ名を割り当てることはできません。

- デバイスの同じインターフェイスに異なるクリプトマップ名を割り当てることはできません。

[クリプトマップエントリの編集（Edit Crypto Map Entry）] ダイアログボックス

フィールド リファレンス

表 *12 : [クリプトマップエントリの編集（Edit Crypto Map Entry）] ダイアログボックス*

要素	デフォルト値（Default Value）
クリプトACL名（Crypto ACL Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager は新しいクリプト ACL 名を生成します。
クリプトマップシーケンス（Crypto Map Sequence）	Cisco Security Manager は、管理対象ネットワークでデバイスを検出すると、このフィールドにデバイスのシーケンス番号を表示します。この値は編集できません。 新しい VPN トポロジを追加する場合、Cisco Security Manager は [シーケンス番号（Sequence Number）] フィールドに # の値を入力します。この値は編集できません。
暗号モード（Crypto Mode）	ASA デバイスバージョン 9.6(2) 以降向けの Cisco Security Manager バージョン 4.12 以降では、次の暗号モードからオプションを選択できます。 • [トンネル（Tunnel）] : デフォルト値。カプセル化モードがトンネルモードになります。 • [トランスポート（Transport）] : ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きのトランスポートモードになります。 • [トランスポート必須（Transport-Require）] : カプセル化モードはトランスポート必須モードのみになります。 （注） トランスポートおよびトランスポート必須モードは、IKEv2 でのみサポートされます。

VPN トポロジにおけるハイ アベイラビリティの設定

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [High Availability] ページを使用して、ハブのグループをハイ アベイラビリティ（HA）グループとして定義します。ハイ アベイラビリティを設定するかどうかはオプションです。

Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開く方法については、VPN トポロジの作成または編集 （38 ページ）を参照してください。

LAN 上で IP を実行する Cisco IOS ルータまたは Catalyst 6500/7600 デバイスにハイ アベイラビリティ（HA）ポリシーを設定すると、自動デバイス バックアップ機能を使用できます。ハイ アベイラビリティは、通常の IPsec または Easy VPN テクノロジーを使用するハブアンドスポーク VPN トポロジで設定できます。

Security Manager では、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブ デバイスで構成された HA グループによって HA がサポートされます。仮想 IP アドレスを共有することによって、HA グループのハブは、外観上は、LAN 上のホストに対して単一の仮想デバイスまたはデフォルト ゲートウェイになります。HA グループの 1 つのハブが常にアクティブになって仮想 IP アドレスを独占的に使用し、同時に他のハブはスタンバイ ハブになります。グループ内のハブは、アクティブ デバイスおよびスタンバイ デバイスから hello パケットが着信するのを待ちます。アクティブ デバイスが何らかの理由で使用できなくなると、スタンバイ ハブが仮想 IP アドレスの所有権を取得して、ハブの機能を引き継ぎます。この移行は、LAN 上のホストおよびピア デバイスに対してシームレスかつ透過的に実行されます。

HA グループを使用する場合は、次の点に注意します。

- ハイ アベイラビリティは、通常の IPsec または Easy VPN テクノロジーを使用するハブアンドスポーク VPN トポロジ内のハブに対してだけ設定できます。
- ハイ アベイラビリティは、Cisco IOS ルータまたは Catalyst 6500/7600 デバイスにだけ設定できます。ただし、HA グループには、Cisco IOS ルータと Catalyst 6500/7600 デバイスの両方を含むことはできません。
- ステートフル フェールオーバーを設定する場合、HA グループには 2 つのハブだけを含むことができます。これらのハブは、Cisco IOS ルータである必要があります。Catalyst 6500/7600 デバイスは使用できません。
- VRF 対応 IPsec が設定されたハブにはハイ アベイラビリティを設定できません。VRF 対応 IPsec について （20 ページ）を参照してください。
- HA グループには GRE を設定できません。
- HA グループ内のデバイスは、複数のハブアンドスポーク トポロジに属することができます。
- サイト間 VPN で HA が設定されたハブとして設定されているデバイスは、同じ外部インターフェイスを使用して、異なるサイト間 VPN で HA が設定されたハブとして設定できません。同様に、このようなデバイスは、同じ外部インターフェイスを使用して、HA が設定されたリモート アクセス VPN サーバとして設定できません。
- すべてのピアにおいて、同じ自動生成された事前共有キーを認証に使用する必要があります。Preshared Key ポリシーを設定するときにこのオプションの使用を指定していない場合、このオプションは、ハイ アベイラビリティの設定中に上書きされます。詳細については、IKEv1 事前共有キー ポリシーの設定を参照してください。
- 設定の生成中に、HA グループ内のすべてのハブは同じコマンドを受信します。コマンドは、HA グループ全体に対して展開する必要があります。グループ内の個別のハブに対して展開することはできません。

次の表に、ハイ アベイラビリティ設定用のオプションを示します。

表 *13 : [High Availability]* ページ

要素	説明
有効化（Enable）	ハブのグループに対してハイ アベイラビリティ設定をイネーブルにするかどうかを指定します。すでにハイ アベイラビリティを設定している場合は、このオプションの選択を解除することによって、設定を削除できます。
Inside Virtual IP	HA グループ内のハブによって共有され、HA グループの内部インターフェイスを表す IP アドレス。仮想 IP アドレスは、HA グループ内のハブの内部インターフェイスと同じサブネットである必要がありますが、これらのインターフェイスのいずれかと同じ IP アドレスにすることはできません。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
Inside Mask	内部仮想 IP アドレスのサブネット マスク。
VPN Virtual IP	HA グループ内のハブによって共有され、HA グループの VPN インターフェイスを表す IP アドレス。この IP アドレスは、VPN トンネルのハブ エンドポイントとして機能します。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
VPN Mask	VPN 仮想 IP アドレスのサブネット マスク。
Hello 間隔（Hello Interval）	ステータスと優先度を示すためにハブがグループ内の別のハブにエコー hello メッセージを送信する秒単位の間隔（1 ～ 254）。デフォルトは 5 秒です。
保留時間（Hold Time）	ハブがダウンしていると結論付ける前に、スタンバイ ハブがアクティブなハブから hello メッセージの受信を待機する秒単位の期間（2 ～ 255）。デフォルトは 15 秒です。
Standby Group Number (Inside)	HA グループ内のハブの内部仮想 IP サブネットと一致する内部ハブ インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 1 です。
Standby Group Number (Outside)	HA グループ内のハブの外部仮想 IP サブネットと一致する外部ハブ インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 2 です。 （注） 外部スタンバイ グループの番号と内部スタンバイ グループの番号は異なっている必要があります。

要素	説明
Enable Stateful Failover	ステートフル フェールオーバーをイネーブルにし、ステートフル スイッチオーバー（SSO）を使用して HA グループ内の HSRP デバイス間で状態情報が共有されるようにするかどうかを指定します。デバイスで障害が発生した場合、共有されている状態情報により、スタンバイデバイスは、トンネルの再確立またはセキュリティアソシエーションの再ネゴシエートを行わずに、IPsec セッションを維持できます。 ステートフル フェールオーバーは、Cisco IOS ルータである 2 つのハブを含む HA グループでだけ設定できます。このチェックボックスは、HA グループに 3 つ以上のハブが含まれる場合にディセーブルになります。 Easy VPN トポロジでは、ステートフル フェールオーバーを常に設定する必要があるため、このチェックボックスは選択されてディセーブルになります。 **ヒントTips:** • 通常の IPsec トポロジの場合に選択解除すると、HA グループにステートレス フェールオーバーが設定されます。ステートレス フェールオーバーは、HA グループに 3 つ以上のハブが含まれる場合にも設定されます。ステートレス フェールオーバーは、Cisco IOS ルータまたは Catalyst 6500/7600 デバイスに設定できます。 • ステートレス フェールオーバーは、IKE 認証方式が RSA の署名である場合には使用できません。 • Cisco IOS バージョン 12.3(14)T 以降が実行されているデバイスでだけ、ステートフル フェールオーバーと PKI を同時に設定できます。

関連項目

- ハブアンドスポーク VPN トポロジ （2 ページ）
- Easy VPN について

GET VPN グループ暗号化の定義

[GET VPN Group Encryption] ページを使用して、GET VPN トポロジのグループ設定およびセキュリティ アソシエーションを定義します。

このページの内容は、Create VPN ウィザードを使用しているか、または Group Encryption ポリシーを編集しているかに応じて異なります。ウィザードのページはタブ形式ではありませんが、ポリシーはタブ形式で表示されます。ウィザードのページには追加のフィールドが用意されており、セキュリティ アソシエーションを設定できます。

[GET VPN Group Encryption] ページを開くには、次の手順を実行します。

- 新しい GET VPN を作成する場合は、Create VPN ウィザードを使用します。ウィザードの開始方法の詳細については、VPN トポロジの作成または編集 （38 ページ）を参照してください。
- （[Site-to-Site VPN Manager] ウィンドウ （26 ページ））既存の GET VPN トポロジを選択して、ポリシーセレクタで [グループ暗号化ポリシー（Group Encryption Policy）] を選択します。
- （ポリシービュー）**[サイト間VPN（Site-to-Site VPN）]>[グループ暗号化ポリシー（Group Encryption Policy）]** を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

次の表に、GET VPN グループ暗号化設定を定義する場合に設定可能なオプションを示します。

表 14 : [GET VPN Group Encryption Policy] ページ

要素	説明
[Group Settings] タブ	
グループ名（Group Name）	Group Domain of Interpretation（GDOI）グループの名前。この名前は、VPN 名と同じです。
Group Identity	グループを識別するために使用されるパラメータ。すべてのキーサーバおよびグループ メンバーは、このパラメータを使用してグループを識別します。 ID には、番号（3333 など）または任意の IP アドレス（キーの再生成に使用するマルチキャスト アドレスなど）を使用できます。
受信のみ	イネーブルに設定すると、グループ メンバーによってトラフィックが復号化されて、クリア テキストで転送されます。この機能は、VPN のテストに役立ちます。通常の運用においては、このオプションを選択しないでください。詳細については、パッシブ モードを使用した GET VPN への移行を参照してください。

要素	説明
セキュリティ ポリシー （Create VPN ウィザードだけ）	セキュリティ ポリシーとして使用される ACL ポリシー オブジェクト。このオブジェクトの内容の詳細な説明とグループ メンバー セキュリティ ポリシーとの関連については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについてを参照してください。 このフィールドは、Create VPN ウィザードを使用している場合にだけ表示されます。Group Encryption ポリシーでは、[Security Associations] タブでセキュリティ ポリシーを設定します（後述の説明を参照）。 （注） キーの配布方法としてマルチキャストを使用している場合は、ACL ポリシー オブジェクトにマルチキャスト アドレスの拒否ルール（ACE）が含まれている必要があります。こうすると、マルチキャストを使用して送信されるキーの再生成パケットは、TEK によって暗号化されなくなります。このステートメントにより、グループ メンバーは、マルチキャスト プロトコルを使用して送信されたキーの再生成パケットを受信できます。
認証タイプ（Authorization Type）	グループで使用する認可メカニズムのタイプを [None]、[Certificates]、または [Preshared Key] から選択します。[Certificates] または [Preshared Key] を選択すると、権限のあるグループ メンバーだけがキー サーバに登録できるようになり、セキュリティが強化されます。キー サーバが複数の GDOI グループで使用される場合には、このような追加のセキュリティが必要となります。 [証明書（Certificates）] を選択した場合は、証明書フィルタのリストを作成する必要があります（識別名属性または完全修飾ドメイン名属性の組み合わせを使用）。このフィルタは、キー サーバに配置されて、GDOI グループに参加する権限がグループ メンバーにあるかどうかを確認するために使用される属性や値を指定します。証明書フィルタの名前を入力し、[行の追加（Add Row）]（+）ボタンをクリックして、[Add Certificate Filter] ダイアログボックス （79 ページ）に入力します。 （注） 証明書認可を設定するには、GET VPN の Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーも設定する必要があります。使用する PKI 登録オブジェクトには、必要に応じて、同じ識別名が定義されているか、またはデバイスの完全修飾ドメイン名が含まれている必要があります。 [事前共有キー（Preshared Key）] を選択した場合は、権限のあるグループ メンバーを特定するための ACL ポリシー オブジェクトも選択します。許可ルールを使用して、グループ メンバーのホストまたはネットワーク アドレスを特定します。

要素	説明
Key Distribution	各グループ メンバーにキーを配布するために使用する転送方法（[unicast] または [multicast]）。どちらを使用するかを決定するのに役立つ情報については、キーの再生成転送メカニズムの選択を参照してください。 [unicast] を選択した場合、キーサーバーは登録されている各グループメンバーに対してキーの再生成メッセージを送信し、確認応答を待機します。[multicast] を選択した場合、キー サーバはキーの再生成メッセージをすべてのグループ メンバーに一度に送信し、確認応答は待機しません。キーの再生成メッセージは、このポリシーに設定された再送信間隔経過後に再送信されます。 [multicast] を選択した場合、キーサーバーとして使用されているルータでマルチキャストがイネーブルになっていることを確認します。また、次のオプションを設定します。 • [グループIPアドレス（Group IP Address）]：キー配布に使用されるマルチキャストグループの IP アドレスです。 • [グループメンバーでStatic IGMP Joinsを使用（Use Static IGMP Joins on Group Members）]：このオプションを選択すると、静的な Source Specific Multicast（SSM）マッピングがイネーブルとなり、グループメンバーに対してマルチキャストトラフィックの送信元が通知されます。GET VPN の場合、グループ メンバーには、キー サーバのアドレスが通知されます。
RSA Key Label	さまざまなメッセージの暗号化に使用される、RSA キーのラベル。このキーは、デバイスにすでに存在している場合もありますが、使用されていない新しいラベルを指定することもできます。 新しい VPN を作成している場合、[VPNの作成（Create VPN）] ウィザードの最後にキーサーバー間でこのキーを同期するかどうかを尋ねられます。[はい（Yes）] をクリックすると、キーが存在していない場合には Security Manager によってキーが生成されます。既存の GET VPN でこの値を変更した場合は、Key Servers ポリシーからキーを同期する必要があります。このキーの用途、およびキーの生成と同期のプロセスの詳細については、RSA キーの生成と同期を参照してください。

要素	説明
Lifetime (KEK)	Key Encryption Key（KEK; キー暗号化キー）が有効な秒数。このキーは、キーの再生成メッセージの暗号化に使用されます。このライフタイムが終了する前に、キーサーバからグループにキーの再生成メッセージが送信されます。このメッセージには、新しい KEK 暗号化キーとトランスフォーム、および新しい TEK 暗号化キーとトランスフォームが含まれています。 KEK ライフタイム値は、TEK ライフタイム値よりも大きい必要があります（KEK ライフタイム値は、TEK ライフタイム値の少なくとも 3 倍以上にすることが推奨されます）。通常は、デフォルト値である 86,400 秒が適しています。TEK ライフタイム値は、セキュリティ アソシエーションごとに設定します（[Add New Security Association]/[Edit Security Association] ダイアログボックス （80 ページ）を参照）。
暗号化アルゴリズム（Encryption Algorithm）	キー サーバからグループ メンバーへのキーの再生成メッセージを暗号化するために使用されるアルゴリズム。
Retransmits	1 つ以上のグループ メンバーがキーの再生成メッセージを受信しない場合にメッセージを送信できる回数。
インターバル	再試行間隔を表す秒数。
[Security Associations] タブ	
[Security Associations] テーブル	[Security Associations] テーブルを使用して、VPN のセキュリティ アソシエーションを定義します。テーブルのカラムには、エントリの設定の概要が表示されます。これらについては、[Add New Security Association]/[Edit Security Association] ダイアログボックス （80 ページ）で説明します。新しい VPN を作成する場合は、このタブではなく [Security Policy] フィールド（上記の説明を参照）を使用します。このタブは、ウィザードには表示されません。 セキュリティ アソシエーションを設定するには、次の手順を実行します。 • テーブルにエントリを追加するには、[追加（Add）] ボタンをクリックして、[新しいセキュリティアソシエーションの追加（Add New Security Association）] ダイアログボックスに入力します。 • エントリを選択し、[編集（Edit）] ボタンをクリックして、既存のエントリを編集します。 • エントリを選択し、[削除（Delete）]ボタンをクリックして削除します。

関連項目

- GET VPN 登録プロセスについて

- Group Encrypted Transport（GET）VPN について
- GET VPN の設定

[Add Certificate Filter] ダイアログボックス

[Add Certificate Filter] ダイアログボックスを使用して、GET VPN の Group Encryption ポリシー用の証明書フィルタを定義します。このフィルタは、キーサーバに配置されて、グループに参加する権限がグループメンバーにあるかどうかを確認するために使用される属性や値を指定します。

次のフィルタ タイプのいずれかを選択します。

- [dn]：（識別名。）[サブジェクト（Subject）] フィールドに、名前=値のペアのリストをカンマで区切って指定します。 たとえば、OU=Cisco, C=US のように指定します。Public Key Infrastructure ポリシーを設定する場合は、選択する PKI 登録オブジェクトの [Certificate Subject Name] タブで同じ値が定義されている必要があります（[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブを参照）。識別名を使用すると、1 つのフィルタで複数のデバイスに一致させることができます。
- [fqdn]：（完全修飾ドメイン名。）[ドメイン名（Domain Name）] フィールドに、単一のデバイスの完全修飾ドメイン名（router1.example.com など）を指定します。公開鍵インフラストラクチャ ポリシーを設定する場合は、選択する PKI 登録オブジェクトで [デバイスの FQDNを含める（Include Device's FQDN）] オプションが選択されている必要があります。各デバイスは一意の名前を持つため、FQDN フィルタは単一のデバイスにだけ一致します。

ヒント　証明書認可を設定するには、GET VPN の Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーも設定する必要があります。PKI ポリシーは、VPN のすべてのデバイスに設定します。

ナビゲーション パス

[GET VPNグループ暗号化（GET VPN Group Encryption）] ページの [グループ設定（Group Settings）] タブで、認可タイプとして [証明書（Certificates）] を選択し、[認可フィルタ（Authorization Filter）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、フィルタを選択して [行の編集（Edit Row）] ボタンをクリックします。[Group Encryption] ページを開く方法については、GET VPN グループ暗号化の定義 （74 ページ）を参照してください。

関連項目

- GET VPN 登録プロセスについて
- Group Encrypted Transport（GET）VPN について
- GET VPN の設定

[Add New Security Association]/[Edit Security Association] ダイアログボックス

[Add New Security Association]/[Edit Security Association] ダイアログボックスを使用して、選択した GET VPN トポロジで使用される IPsec プロファイル（名前とトランスフォーム セットだけ）およびセキュリティ ポリシーを定義します。

ナビゲーション パス

[新しいセキュリティアソシエーションの追加（Add New Security Association）] ダイアログボックスを開くには、[GET VPNグループ暗号化（GET VPN Group Encryption）] ページの [セキュリティアソシエーション（Security Associations）] タブで、[行の追加（Add Row）]（+）ボタンをクリックするか、または既存のアソシエーションを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。[Group Encryption] ページを開く方法については、GET VPN グループ暗号化の定義 （74 ページ）を参照してください。

関連項目

- GET VPN 登録プロセスについて
- Group Encrypted Transport（GET）VPN について
- GET VPN の設定

フィールド リファレンス

表 *15 : [Add New Security Association]* ダイアログボックス

要素	説明
ID	プロファイルのシーケンス番号。この番号によって、セキュリティアソシエーションの相対的なプライオリティが定義されます（1 が最も高いプライオリティです）。複数のセキュリティ アソシエーションがある場合、それぞれの ACL がこの番号で表された順序で連結（およびマージ）され、グループ メンバーは、連結された ACL を単一の ACL として処理します。 デフォルトの番号のままにするか、または新しい番号を入力します。
IPSec Profile Name	IPsec プロファイルの名前。
トランスフォーム セット（Transform Sets）	IPsecプロファイルに定義されたトランスフォームセットポリシーオブジェクト（セキュリティ プロトコル、アルゴリズム、およびその他の設定）。複数のエントリがある場合は、カンマで区切って、プライオリティ順に並べます。[選択（Select）] をクリックして定義済みのトランスフォームセットのリストから選択するか、または新しいトランスフォームセットを作成します。

要素	説明
セキュリティ ポリシー	セキュリティ アソシエーションに対して定義されているアクセス コントロール リスト ポリシー オブジェクト。[選択（Select）] をクリックして定義済みの ACL オブジェクトのリストから選択するか、または新しい ACL オブジェクトを作成します。このオブジェクトの内容の詳細な説明とグループ メンバー セキュリティ ポリシーとの関連については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについてを参照してください。 （注） キーの配布方法としてマルチキャストを使用している場合は、ACL ポリシー オブジェクトにマルチキャスト アドレスの拒否ルール（ACE）が含まれている必要があります。こうすると、マルチキャストを使用して送信されるキーの再生成パケットは、TEK によって暗号化されなくなります。このステートメントにより、グループ メンバーは、マルチキャスト プロトコルを使用して送信されたキーの再生成パケットを受信できます。
Enable Anti-Replay	盗聴者がデータ ストリームにパケットを挿入できないようにするアンチリプレイ機能をイネーブルにするかどうかを指定します。アンチリプレイは、トラフィック カウンタまたは時間に基づいて設定できます。 • [カウンタウィンドウサイズ（Counter Window Size）]：これがデフォルトですが、推奨されません。カウンタ ベースのアンチリプレイは、グループ メンバーが 2 つの場合（実質的にポイントツーポイント VPN の場合）にだけ役立ちます。ウィンドウ サイズを選択します。 • [時間ウィンドウサイズ（Time Window Size）]：これが推奨される方法ですが、グループメンバーが 3 つ以上必要です。Synchronous Anti-Replay（SAR;同期アンチリプレイ）クロックの間隔を表す秒数を入力します。1 ～ 100 の範囲の値を入力します。デフォルト値は 100 です。時間ベースのアンチリプレイの詳細については、時間ベースのアンチリプレイについてを参照してください。 （注） カウンタ ベースのアンチリプレイにおいて、パケット レートが高い状態で暗号化を行う場合は、KEK ライフタイムまたは TEK ライフタイムをあまり長くしないでください。数時間でシーケンス番号が折り返す可能性があるためです。たとえば、パケット レートが 100 キロパケット/秒の場合、シーケンス番号が折り返す前に SA が使用されるように、ライフタイムを 11.93 時間未満に設定する必要があります。

要素	説明
Enable IPSec Lifetime	Global Settings for GET VPN ポリシーで設定されるグローバル設定を上書きする IPsec セキュリティ アソシエーション ライフタイムを設定するかどうかを指定します（GET VPN のグローバル設定を参照）。このライフタイム値によって、キーの再生成が必要となるまでに、どの程度の時間 Traffic Encryption Key（TEK; トラフィック暗号化キー）を使用できるかが制御されます。 グループ メンバー間のトラフィック量（KB 単位）、秒数、またはその両方に基づいて値を設定します。いずれかの値に達するとキーが失効します。次の推奨事項を考慮してください。 • ライフタイムは、Key Encryption Key（KEK; キー暗号化キー）に使用されるライフタイムよりも大幅に短く（3 分の 1 程度に）する必要があります（ GET VPN グループ暗号化の定義 （74 ページ）を参照）。 • トラフィック量が多い場合にはキーの再生成が頻繁に発生し、データが消失する危険性があるため、時間に基づくライフタイムを推奨します。 • グローバル設定を上書きしない場合は、フィールドを空白のままにします。

GET VPN ピアの定義

Create VPN ウィザードの [GET VPN Peers] ページを使用して、GET VPN トポロジ内のキー サーバおよびグループ メンバーのピア プロパティを設定します。トポロジを作成したあとは、[キー サーバー（Key Servers）] ポリシーおよび [グループメンバー（Group Members）] ポリシーを使用して、これらの設定を変更します。ポリシーは、キー サーバとグループ メンバーのテーブルが異なるポリシーに分割されている点を除いて、ウィザードのページと同じです。

ヒント　キーサーバーおよびグループメンバーのリストには、ウィザードの [デバイスの選択（Device Selection）] ページで選択したデバイスが含まれます（VPN トポロジのデバイスの選択 （44 ページ）を参照）。ただし、[追加（Add）]（+）ボタンおよび [削除（Delete）]（ゴミ箱）ボタンを使用して、このページのデバイスを追加または削除できます。

キー サーバとグループ メンバーのリストを確認して、デフォルト設定がご使用の VPN に適しているかどうかを判断します。各テーブルの下にある [表示（Show）] フィールドで [一致するインターフェイス（Matching Interfaces）] を選択して、デフォルトのインターフェイス ロールによって選択される実際のインターフェイスを表示できます。GET VPN 設定を有効にするには、インターフェイス ロールがデバイスの実際のインターフェイスに解決される必要があります。

はじめる前に

ここでは、新しい VPN を作成するときに GET VPN のピアを定義する方法、および GET VPN のピア設定について説明します。Create VPN ウィザードを開く方法については、VPN トポロジの作成または編集 （38 ページ）を参照してください。

関連項目

- 登録の失敗時にも保護するためのフェールクローズの設定
- パッシブ モードを使用した GET VPN への移行
- GET VPN キー サーバの設定
- GET VPN グループ メンバーの設定

ステップ 1 デフォルト設定が適切でない場合は、キー サーバを設定します。

変更する各キーサーバーを選択し、テーブルの下にある [編集（Edit）]（鉛筆）ボタンをクリックして、少なくとも次の項目を設定します。使用可能なすべての設定については、[Edit Key Server] ダイアログボックスを参照してください。

- [アイデンティティインターフェイス（Identity Interface）]：グループメンバーがキーサーバーを識別し、キーサーバーに登録するために使用するインターフェイスを選択します。デフォルトは、キーサーバに定義されているすべてのループバック インターフェイスを識別するループバック インターフェイス ロールです。
- [プライオリティ（Priority）]：1 ～ 100 の範囲のプライオリティ値を入力することによって、キーサーバーのロールをプライマリまたはセカンダリとして定義します。最も高いプライオリティを持つキーサーバがプライマリ キー サーバとなります。2 つ以上のキー サーバに同じプライオリティ値が割り当てられている場合は、最も大きい IP アドレスを持つデバイスが使用されます。デフォルトのプライオリティは、最初のキー サーバに対しては 100、2 番めのキー サーバに対しては 95 などになります。

（注） ネットワークがパーティション化されている場合は、複数のプライマリ キー サーバが存在することがあります。

ステップ 2 テーブル内でキー サーバを上方または下方に移動して、グループ メンバーがキー サーバに登録する場合に使用する順序を指定します。グループ メンバーは、リストの最初のキー サーバに登録されます。最初のキー サーバに到達できない場合は、2 番め以降のキー サーバに順番に登録が試みられます。この順序は、どのキー サーバがプライマリ キー サーバであるかを判断するために使用される全体的なキー サーバのプライオリティを定義するものではないことに注意してください。

ステップ 3 デフォルト設定が適切でない場合は、グループ メンバーを設定します。

変更する各グループメンバーを選択し、テーブルの下にある [編集（Edit）]（鉛筆）ボタンをクリックして、少なくとも次の項目を設定します。

- [GET対応インターフェイス（GET-Enabled Interface）]：プロバイダーエッジ（PE）への VPN 対応外部インターフェイスです。このインターフェイスで発信または終了するトラフィックは、暗号化または復号化が適宜評価されます。複数のインターフェイスに解決されるインターフェイス ロール オブジェクトを選択することによって、複数のインターフェイスを設定できます。[選択（Select）]をクリックして、インターフェイス ロール オブジェクトを選択するか、新しいオブジェクトを作成します。

- [ローカルアドレスとして使用するインターフェイス（Interface To Be Used As Local Address）]：キーサーバーがキーの再生成情報などのデータを送信する場合にグループメンバーを識別するために使用する IP アドレスを持つインターフェイス。GET が 1 つのインターフェイスでだけイネーブルになっている場合は、ローカル アドレスとして使用するインターフェイスを指定する必要はありません。GET が複数のインターフェイスでイネーブルになっている場合は、ローカル アドレスとして使用するインターフェイスを指定する必要があります。インターフェイスまたはインターフェイスロールの名前を入力します。または [選択（Select）] をクリックしてインターフェイスロールを選択します。

他の使用可能な設定については、[Edit Group Member] ダイアログボックスを参照してください。

新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て

Create VPN ウィザードの [VPN Defaults] ページを使用して、作成する VPN トポロジに割り当てられる共有サイト間 VPN ポリシーを表示および選択します。このページには、選択した IPsec テクノロジーに応じて、VPN トポロジに割り当てることができるすべての使用可能な必須およびオプションのポリシーが表示されます（詳細については、サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （7 ページ）を参照してください。）

Create VPN ウィザードを開く方法については、VPN トポロジの作成または編集 （38 ページ）を参照してください。トポロジを作成したあとは、これらのポリシーを直接編集できます。

各ポリシー タイプにおいて、VPN トポロジに割り当てる共有 VPN ポリシーを選択します。共有ポリシーだけを選択できます。次のヒントに従って選択します。

- このページに表示される初期デフォルトは、Security Manager Administration の[VPN Policy Defaults]ページで設定します。必須ポリシーに対して特定のデフォルトが設定されていない場合は、出荷時のポリシーが選択されます。デフォルトポリシーの設定の詳細については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （17 ページ）を参照してください。
- リストされる共有ポリシーは、データベースにコミットされた共有ポリシーのみです。たとえば、Create VPN ウィザードを使用する前に新規共有 IPsec Proposal ポリシーを作成したが、そのポリシーを事前に送信しない（および、必要に応じて承認した）場合、その新規ポリシーはリストに表示されません。新規ポリシーを使用する必要がある場合は、VPN を作成する前にそのポリシーを必ず送信してください。
- ポリシーが必須の場合は、必ず選択を行う必要があります。共有ポリシーがない場合は、出荷時のポリシーだけを選択できます。トポロジを作成したあと、いつでもポリシーを編集できます。

（注） 現在他のユーザによってロックされている共有ポリシーの選択を試みた場合は、ロックに関する問題が存在することを示す警告メッセージが表示されます。ロックを回避するには、別のポリシーを選択するか、またはロックが解除されるまで VPN トポロジの作成をキャンセルします。詳細については、ポリシーのロックについてを参照してください。

- ポリシーがオプションであり、共有ポリシーがない場合は、何も選択できません。そのポリシーによって提供される機能が必要な場合は、トポロジ作成終了後に設定します。
- 読み取り専用ダイアログボックスでポリシーの内容を表示するには、ポリシーを選択して、ポリシーリストの横にある [コンテンツを表示（View Contents）] ボタンをクリックします。
- IKEv2 のみをサポートするトポロジを作成している場合でも、Create VPN ウィザードは、選択内容に従って IKEv1 Preshared Key ポリシーまたは IKEv1 Public Key Infrastructure ポリシーのいずれかを作成します。IKEv2 Authentication ポリシーに対するデフォルト設定はありません。IKEv2 をサポートすることを選択する場合は常に、VPN を作成したあとで IKEv2 Authentication ポリシーを手動で編集し、少なくともグローバル IKEv2 設定を定義する必要があります。ピア固有の IKEv2 オーバーライドを作成することもできます。IKEv2 のみをサポートする場合、ウィザードによって作成された IKEv1 固有のポリシーを割り当て解除できます。

完了したら、[終了（Finish）] をクリックして、新しい VPN トポロジを作成します。新しい VPN トポロジが [Site-to-Site VPN] ウィンドウの VPN セレクタに表示され、[VPN Summary] ページが表示されます。[VPN トポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）] （85 ページ） を参照してください。

[VPN トポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）]

[VPN Summary] ページを使用して、選択した VPN トポロジの設定の概要を表示します。概要には、VPN トポロジのタイプ、トポロジ内のデバイス、割り当てられたテクノロジー、およびトポロジに設定されている特定のポリシーについての情報が含まれます。概要ページは、VPN トポロジ作成後に自動的に表示されます。エクストラネット VPN を作成する場合、Create Extranet VPN ウィザードの最後のステップとしても表示されます。

VPN トポロジの [VPN Summary] ページを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （26 ページ））VPN トポロジを選択して、[ポリシー（Policies）] リストから [VPNサマリー（VPN Summary）] を選択します。
- （デバイスビュー）VPN に参加するデバイスを選択して、[ポリシー（Policies）] リストから [サイト間VPN（Site-to-Site VPN）] ポリシーを選択します。VPN トポロジを選択して、[VPNポリシーの編集（Edit VPN Policies）] ボタンをクリックします。これにより、そのトポロジが選択された状態で [Site-to-Site VPN Manager] ウィンドウが表示されます。このウィンドウで、[ポリシー（Policies）] リストから [VPNサマリー（VPN Summary）] を選択できます。

次の表に、このページに表示される情報を示します。

（注） 標準 VPN の概要は、エクストラネット VPN の概要とは大きく異なります。このテーブルは 2 つに分かれていて、上半分では標準 VPN の概要が説明されており、下半分ではエクストラネット VPN の概要が説明されています。

表 *16 : [VPN Summary]* ページ

要素	説明
標準 VPN の概要情報	
名前	VPN トポロジの名前。
テクノロジー	VPN トポロジに割り当てられた IPsec テクノロジー。 IPsec テクノロジーおよびポリシーについて （6 ページ）を参照してください。
タイプ（Type）	VPN トポロジ タイプ（[Hub-and-Spoke]、[Point-to-Point]、または [Full Mesh]）。
説明	VPN トポロジの説明。
IPsec Terminator	VPN トポロジが大規模 DMVPN の場合に使用可能です。 大規模 DMVPN のハブ間で GRE トラフィックを負荷分散するために使用される IPsec ターミネータの名前。
Primary Hub	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク トポロジにおけるプライマリ ハブの名前。
Failover Hubs	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク トポロジに設定されたすべてのセカンダリ バックアップ ハブの名前。
Number of Spokes	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク トポロジに含まれるスポークの数。
ピア 1	VPN トポロジ タイプがポイントツーポイントの場合に使用可能です。 ポイントツーポイント VPN トポロジにおいてピア 1 として定義されるデバイスの名前。
ピア 2	VPN トポロジ タイプがポイントツーポイントの場合に使用可能です。 ポイントツーポイント VPN トポロジにおいてピア 2 として定義されるデバイスの名前。
Number of Peers	VPN トポロジ タイプが完全メッシュの場合に使用可能です。 完全メッシュ VPN トポロジに含まれているデバイスの数。

要素	説明
IKE Proposal	VPN トポロジに設定されている IKEv1 プロポーザルのセキュリティ パラメータ。IKE プロポーザルの設定を参照してください。 （注） IKEv2 プロポーザルは概要に表示されません。
Dynamic VTI	Easy VPN トポロジで使用可能です。 Easy VPN トポロジにおいて、デバイスにダイナミック仮想テンプレート インターフェイスが設定されているかどうかが表示されます。Easy VPN に対するダイナミック VTI の設定を参照してください。
トランスフォーム セット（Transform Sets）	VPN トンネル内のトラフィックを保護するために使用される認証および暗号化アルゴリズムを指定する IPsec IKEv1 トランスフォーム セット。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。 （注） IPsec IKEv2 トランスフォーム セットは概要に表示されません。
事前共有キー（Preshared Key）	選択したテクノロジーが Easy VPN の場合は使用できません。 IKEv1 Preshared Key ポリシーで使用する共有キーがユーザ定義であるか、または自動生成されたものであるかを指定します。IKEv1 事前共有キー ポリシーの設定を参照してください。 （注） IKEv2 事前共有キー設定は概要に表示されません。
公開キー インフラストラクチャ	VPN トポロジに IKEv1 Public Key Infrastructure ポリシーが設定されている場合に、Certificate Authority（CA; 認証局）サーバを指定します。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。 （注） IKEv2 PKI 設定は概要に表示されません。
ルーティング プロトコル（Routing Protocol）	選択したテクノロジーが IPsec/GRE、GRE ダイナミック IP、または DMVPN の場合にだけ使用可能です。 GRE、GRE ダイナミック IP、または DMVPN ルーティング ポリシーを設定するための、保護された IGP で使用されるルーティング プロトコルおよび自律システム（またはプロセス ID）番号です。 （注） 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、このルーティング プロトコルおよび自律システム（またはプロセス ID）番号を使用して、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。 [GRE Modes] ページについてを参照してください。

要素	説明
Tunnel Subnet IP	選択したテクノロジーが IPsec/GRE、GRE ダイナミック IP、または DMVPN の場合にだけ使用可能です。 トンネル サブネットが定義されている場合に、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 IP アドレスが表示されます。 [GRE Modes] ページについてを参照してください。
ユーザー グループ	Easy VPN トポロジで使用可能です。 Easy VPN トポロジ内のデバイスに User Group ポリシーが設定されている場合に、ポリシーの詳細が表示されます。Easy VPN における User Group ポリシーの設定を参照してください。
PIX7.0/ASA Tunnel Group	Easy VPN トポロジで使用可能です。 Easy VPN トポロジ内の PIX ファイアウォール バージョン 7.0+ または ASA アプライアンスに Connection Profile ポリシーが設定されている場合に、ポリシーの詳細が表示されます。
ハイ アベイラビリティ	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク VPN トポロジ内のデバイスに High Availability ポリシーが設定されている場合に、ポリシーの詳細が表示されます。VPN トポロジにおけるハイ アベイラビリティの設定 （71 ページ）を参照してください。
VRF 対応 IPSec	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク VPN トポロジ内のハブに VRF-Aware IPsec ポリシーが設定されている場合に、VRF ソリューションのタイプ（1 ボックスまたは 2 ボックス）および VRF ポリシーの名前が表示されます。 VRF 対応 IPsec の設定 （66 ページ）を参照してください。
エクストラネット VPN の概要情報	
[IKE Phase 1 Proposal] セクション	エクストラネットに対して割り当てられる IKE Proposal ポリシー オブジェクト内に定義される、IKE フェーズ 1 プロポーザルのパラメータ。設定値については、次のトピックを参照してください。 • [IKEv1 Proposal] ポリシー オブジェクトの設定 • [IKEv2 Proposal] ポリシー オブジェクトの設定

要素	説明
[IKE Phase 2 Proposal] セクション	IKE フェーズ 2 プロポーザルのパラメータ。これらのパラメータのほとんどは、エクストラネットに対して割り当てられる IPsec トランスフォーム セット ポリシー オブジェクトで設定されます。説明については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。 Lifetime 属性パラメータは VPN Global Settings ポリシーで定義されます。VPN グローバル設定を参照してください。Perfect Forward Secrecy パラメータは IPsec Proposal ポリシーで定義されます。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。
[Authentication] セクション	接続の認証に使用される証明書を定義する事前共有キーまたは PKI 登録ポリシー オブジェクトの名前。 事前共有キーを使用している場合、[キーの表示/非表示（Show/Hide Key）] ボタンをクリックして、キーの表示とマスクを切り替えることができます。概要の印刷または PDF の生成を行う場合、キーはここでの選択内容に応じて表示または非表示になります。
ローカル（Local）	エクストラネット VPN のローカル（管理対象）エンドにあるデバイス。表示名、VPN インターフェイスの名前と IP アドレス、および保護対象ネットワークが含まれます。
リモート（Remote）	エクストラネット VPN のリモート（管理対象外）エンドにあるデバイス。デバイス名、VPN インターフェイスの IP アドレス、および保護対象ネットワークが含まれます。
[Print] ボタン	概要を印刷するには、このボタンをクリックします。事前共有キーは、ページに現在表示されている内容に基づいて、表示または非表示になります。 概要を印刷するには、Adobe Acrobat Reader がインストールされている必要があります。Security Manager は、概要の PDF を生成してから、Acrobat の印刷機能を使用して印刷します。
[Generate PDF] ボタン	概要の PDF を作成するには、このボタンをクリックします。事前共有キーは、ページに現在表示されている内容に基づいて、表示または非表示になります。PDF の保存先のファイル名と場所のプロンプトが表示されます。

関連項目

- IKE プロポーザルの設定
- サイト間 VPN での IPsec プロポーザルの設定
- IKEv1 事前共有キー ポリシーの設定

- 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
- GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定
- DMVPN の [GRE Modes] の設定
- 大規模 DMVPN の設定
- Easy VPN での IPsec プロポーザルの設定
- Easy VPN における User Group ポリシーの設定
- Easy VPN における Connection Profile ポリシーの設定
- エクストラネット VPN の作成または編集 （90 ページ）

エクストラネット VPN の作成または編集

Security Manager は、Security Manager で管理しているデバイスと管理対象外のデバイスの間に通常の IPsec ポイントツーポイント VPN を作成するための簡単な方式を提供します。このタイプの VPN は、エクストラネットと呼ばれます。

通常、エクストラネットは、ご使用のネットワークとパートナーまたはサービスプロバイダーのネットワークの間のサイト間 VPN 接続です。ただし、ユーザーの組織のネットワーク内の VPN 接続であっても、異なるグループにより管理されているデバイス間の VPN 接続、またはシスコ デバイスとシスコ製以外の（Security Manager では管理できない）デバイスの間の VPN 接続の場合もあります。

このタイプのポイントツーポイント VPN トポロジを作成するには、Create Extranet VPN ウィザードを使用します。エクストラネット VPN の作成には、デバイス、VPN トンネルのソースエンドポイントおよび宛先エンドポイントである VPN インターフェイス、およびトンネルで保護される保護対象ネットワークの指定が含まれます。セキュアな接続の完了のために必要な IKE プロポーザル、IPsec プロポーザル、および事前共有キーまたは証明書も指定します。

エクストラネット VPN トポロジを編集する場合、[Edit Extranet VPN] ダイアログボックスには（[IKE Proposal] ページを除いて）Create Extranet VPN ウィザードと同じページが含まれていますが、ウィザード形式ではなく、タブ形式でページがレイアウトされています。ダイアログボックスの任意のタブで [OK] をクリックすると、すべてのタブの定義が保存されます。IKE プロポーザル、IPsec プロポーザル、事前共有キー、および公開キー インフラストラクチャ証明書について、直接ポリシーを編集する必要があります。

ヒント

- VPN デフォルト ポリシーはエクストラネット VPN には適用されません。[Security Manager Administration] の [VPN Defaults] ページで定義された設定は無視されます。エクストラネット VPN 設定で使用する共有ポリシーがある場合は、Create Extranet VPN ウィザードで作成したあとで VPN に割り当てることができます。共有ポリシーを割り当てると、ウィザードで作成されたポリシーと置き換えられます。

- エクストラネット VPN を作成するときに事前定義 IKE プロポーザルまたは IPsec トランスフォーム セット ポリシー オブジェクトを選択することはできません。使用する既存オブジェクトがある場合は、VPN の作成後に関連ポリシーを編集し、オブジェクトを選択できます。その後、必要に応じて、Create Extranet VPN ウィザードで作成されたオブジェクトを削除できます。
- エクストラネット VPN の作成後、そのエクストラネット VPN を、VPN の両方のエンドを Security Manager で管理する標準ポイントツーポイント VPN に変換することはできません。代わりに、VPN を削除してから再作成する必要があります。
- エクストラネット VPN 接続は、通常の IPsec ポイントツーポイント接続に対してのみ設定できます。たとえば、サービスプロバイダーのネットワーク内に存在する GET VPN キーサーバーをこの方式を使用して識別することはできません。その他のすべてのタイプのエクストラネット接続を設定するには、管理対象外デバイスまたは非シスコデバイスの VPN への組み込み （16 ページ）の説明に従って、Security Manager インベントリにダミーの管理対象外デバイスを追加する必要があります。

関連項目

- VPN トポロジについて （2 ページ）
- デバイス ビューにおける VPN トポロジの設定 （27 ページ）
- IPsec テクノロジーおよびポリシーについて （6 ページ）
- ウィザードの使用

ステップ 1 次のいずれかを実行します。

- 新規エクストラネット VPN を作成するには、[Site-to-Site VPN Manager] ウィンドウ （26 ページ）または [サイト間 VPN ポリシー（Site-to-Site VPN Policy）] ページ（デバイスビュー）で、[VPN トポロジの作成（Create VPN Topology）]（+）ボタンをクリックし、[エクストラネット VPN（Extranet VPN）] を選択します。Create Extranet VPN ウィザードが開始され、[Name and Technology] ページが表示されます。
- 既存のエクストラネット VPN を編集するには、[Site-to-Site VPN Manager] ウィンドウまたは [サイト間 VPN ポリシー（Site-to-Site VPN Policy）] ページ（デバイスビュー）で VPN トポロジを選択し、[VPN トポロジの編集（Edit VPN Topology）]（鉛筆）ボタンをクリックします。[Device Selection] タブに対して [Edit Extranet VPN] ダイアログボックスが開きます。

ステップ 2 [Name and Technology] ページまたはタブで、以下を設定します。名前のみが必須です。

- [名前（Name）]：VPN トポロジを識別する一意の名前。
- [説明（Description）]：最大 1024 文字の VPN の説明。
- [作成日（Creation Date）]：VPN が作成された日付。VPN を作成するときは、今日の日付がデフォルトです。ただし、編集ボックスの横のカレンダー アイコンをクリックして、希望する日付を選択できます。

- [チケット番号（Ticket Number）]：チケットシステムを使用していて、実行するアクションが追跡されている要件に関連する場合は、このフィールドに番号を入力します。Security Manager はこの番号を使用しません。内部追跡目的専用です。
- [最終変更者（Last Modified By）]：最後に VPN の設定を変更したユーザーの名前、ユーザー ID、電子メールアドレス、またはその他のインジケータ。Security Manager はこのフィールドを使用しません。内部追跡目的専用です。

ウィザードで、[次へ（Next）] をクリックします。[エクストラネット VPN の編集（Edit Extranet VPN）] ダイアログボックスで、[デバイスの選択（Device Selection）] タブをクリックします。

ステップ 3 [Device Selection] ページまたはタブで、接続の各エンドのデバイス、インターフェイス、および保護対象ネットワークを設定します。

- [ローカル（Local）]：これは、管理対象ネットワーク内のデバイスです。デバイスは、Security Manager インベントリ内にある必要があります。次のプロパティをすべて設定します。
  - [デバイス（Device）]：デバイスの表示名を入力するか、または [選択（Select）] をクリックしてインベントリ内のデバイスをリストから選択します。ASA 5500 シリーズデバイス、PIX ファイアウォール、または Cisco IOS ルータ（ASR を含む）を選択できます。
  - [VPN トンネルインターフェイス（VPN Tunnel Interface）]：VPN 接続の外部インターフェイスを識別するインターフェイスまたはインターフェイスロールの名前。[選択（Select）] をクリックして、既存のインターフェイスまたはインターフェイスロールを選択するか、または新規インターフェイスロールを作成します。

インターフェイスまたはロールを選択するときに、一致するインターフェイスの IP アドレスが [IP アドレス（IP Address）] フィールドの横あるドロップダウンリストにリストされます。バージョン 4.9 以降、Security Manager はエクストラネット VPN の IPv6 アドレスをサポートします。IPv4 アドレスと IPv6 アドレスのリストを表示できます。デフォルトでは IPv4 アドレスが表示されます。アドレスが表示されない場合、Security Manager は IP アドレスを判別できませんでした。設定またはオブジェクト選択内容を確認してください。

- [保護されたネットワーク（Protected Networks）]：デバイスがこの VPN に対して保護しているネットワーク。[選択（Select）] をクリックして [保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを表示します。このダイアログボックスでは、インターフェイス名、インターフェイス ロール オブジェクト、ネットワーク/ホストグループオブジェクト、または ACL オブジェクトを使用して、保護されたネットワークを指定できます。[保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを使用して、新しいネットワーク/ホストグループまたは ACL オブジェクトを定義することもできます。

（注） エンドポイントおよび保護対象ネットワークの定義 （46 ページ）の説明に従って、ローカル デバイス エンドポイント設定を編集することもできます。設定はこれらに似ていますが、インターフェイス ロール オブジェクトを定義する機能が追加されています。

- [クリプトマップ名（Crypto Map name）]：デバイスのクリプトマップ名を手動で入力できます。デフォルト値はありません。値を入力しない場合、Cisco Security Manager はデバイスのクリプト

マップ名を使用するか、新しいクリプトマップ名を生成します。VPN インターフェイスにクリプトマップがすでに存在する場合、Cisco Security Manager は同じ名前を再利用します。

- [クリプト ACL 名（Crypto ACL name）]：デバイスのクリプト ACL 名を手動で入力できます。デフォルト値はありません。値を入力しない場合、Cisco Security Manager は新しいクリプト ACL 名を生成します。
- [クリプトマップシーケンス（Crypto Map Sequence）]：Cisco Security Manager は、管理対象ネットワークでデバイスを検出すると、このフィールドにデバイスのシーケンス番号を表示します。この値は編集できません。新しい VPN トポロジを追加する場合、Cisco Security Manager は [シーケンス番号（Sequence Number）] フィールドに # の値を入力します。この値は編集できません。

詳細については、以下を参照してください。 クリプトマップの設定 （69 ページ）

- [クリプトモード（Crypto Mode）]：ASA デバイスバージョン 9.6(2) 以降向けの Cisco Security Manager バージョン 4.12 以降では、次のクリプトモードからオプションを選択できます。
  - [トンネル（Tunnel）]：デフォルト値。カプセル化モードがトンネルモードになります。
  - [トランスポート（Transport）]：ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きのクリプトモードになります。
  - [トランスポート必須（Transport-Require）]：カプセル化モードはトランスポートモードのみになります。トランスポートモードは IKEv2 でのみサポートされています。
- [リモート（Remote）]：これは、Security Manager では管理しないデバイスです。次のプロパティをすべて設定します。
  - [名前（Name）]：デバイスの名前。Security Manager インベントリで使用される表示名に対応しています。
  - [IP アドレス（IP Address）]：デバイスの VPN インターフェイスの IP アドレス。スペースを区切り文字として使用して、最大 10 個の IP アドレスを入力できます。バージョン 4.9 以降、Security Manager は IPv4 アドレスに加えて IPv6 アドレスをサポートします。

（注） バージョン 4.8 以降、Security Manager では、同じエクストラネット VPN 構成に複数のピア IP アドレスを設定できます。これにより、最初のデバイスが VPN サービスに使用できない場合に、リスト内の次のピアデバイスがフェールオーバーとして機能できます。このバックアップピアサポートは、Cisco 適応型セキュリティアプライアンス（ASA）デバイスおよび Cisco IOS ルータで利用できます。

- [保護されたネットワーク（Protected Networks）]：デバイスがこの VPN に対して保護しているネットワーク。[選択（Select）] をクリックして [保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを表示します。このダイアログボックスでは、ネットワーク/ホストグループオブジェクトまたは ACL オブジェクトを使用して、保護されたネットワークを指定できます。[保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを使用して、新しいネットワーク/ホストグループまたは ACL オブジェクトを定義することもできます。

（注） エンドポイントおよび保護対象ネットワークの定義 （46 ページ）の説明に従って、リモート デバイス エンドポイント設定を編集することもできます。ただし、設定値はこれらの設定値と同じであり、インターフェイス名またはインターフェイス ロール オブジェクトを使用して保護対象ネットワークを指定することはできません。

ウィザードで、[次へ（Next）] をクリックします。[Edit VPN] ダイアログボックスで終了します。残りの特性を編集するには、IKE Proposal、IPsec Proposal、IKEv1 Preshared Key、IKEv1 Public Key Infrastructure、IKEv2 Authentication、および VPN Global Settings の各ポリシーを編集して、次のステップで説明されている設定を変更する必要があります。

ステップ 4 Create Extranet VPN ウィザードの [IKE Proposal] ページで、IKE プロポーザル、IPsec プロポーザル、および事前共有キーまたは証明書のいずれかを定義します。

- [IKEv1] または [IKEv2] を選択します。リリース 8.4(1) を実行している ASA 5500 シリーズ デバイスでのみ IKEv2 を使用できます。

エクストラネット VPN を作成したあとで IKE バージョンを変更する場合は、これらのポリシーをすべて編集して以前の設定を割り当て解除または置換し、目的のバージョン（IKE Proposal、IPsec Proposal、IKEv1 Preshared Key、IKEv1 Public Key Infrastructure、IKEv2 Authentication、VPN Global Settings）のオプションを設定する必要があります。IKEv1 と IKEv2 の違いについては、IKE バージョン 1 と 2 の比較を参照してください。

- IKE フェーズ 1 プロポーザルのパラメータを設定します。これらのパラメータは、*ExtranetName*_**ikeBB** という名前の IKE プロポーザル ポリシー オブジェクトの作成に使用されます。パラメータの説明については、[IKEv1 Proposal] ポリシー オブジェクトの設定または[IKEv2 Proposal] ポリシー オブジェクトの設定を参照してください。

VPN を作成したあとでこれらの値を編集する場合は、そのオブジェクトを編集する必要があります。オブジェクトは Policy Object Manager で編集できます。または、VPN の IKE Proposal ポリシーを使用して直接編集できます。

（注） **DH Group** 属性（Diffie-Hellman 係数グループの場合）は、その他のポリシーやポリシーオブジェクトでは **Modulus Group** と呼ばれます。

- IKE フェーズ 2（IPsec）プロポーザルのパラメータを設定します。これらのパラメータのほとんどは、*ExtranetName*_**transformSet** という名前の IPsec トランスフォーム セット ポリシー オブジェクトの作成に使用されます。パラメータの説明については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。AH Hash Algorithm 設定はローカル デバイスがルータである場合にのみ使用できることに注意してください。

VPN を作成したあとでこれらの値を編集する場合は、そのオブジェクトを編集する必要があります。オブジェクトは Policy Object Manager で編集できます。または、VPN の IPsec Proposal ポリシーを使用して直接編集できます。

次の設定は、IPsec トランスフォーム セット オブジェクトには含まれません。

- - [Perfect Forward Secrecy、DH Group の有効化（Enable Perfect Forward Secrecy, DH Group）]：それぞれの暗号化された交換に対して固有のセッションキーを使用するかどうか。固有のセッションキーにより、攻撃者がトンネルの両方のエンドで使用される事前共有キーまたは秘密キーを知っている場合でも、その攻撃者がキャプチャされた交換を復号化できなくなります。このオプションを

選択する場合は、キーの導出に使用する Diffie-Hellman（DH）係数グループも選択します。係数グループの詳細については、使用する Diffie-Hellman 係数グループの決定を参照してください。

VPN を作成したあとでこのオプションを変更するには、IPsec Proposal ポリシーを編集します。

- • [ライフタイム（Lifetime）]：セキュリティアソシエーションの期限切れまでの存在秒数。デフォルトは 3,600 秒（1 時間）です。

VPN を作成したあとでこのオプションを変更するには、VPN Global Settings ポリシーを編集します。

- 認証に [事前共有キー（Preshared Key）] を選択する場合は、リモートホストとの接続の認証に使用するキーを入力します。

VPN を作成したあとでキーを編集するには、ご使用の IKE バージョンに応じて IKEv1 Preshared Key ポリシーまたは IKEv2 Authentication ポリシーのいずれかを編集する必要があります。これらのポリシーではキーはマスクされていますが、[VPN Summary] ポリシーを選択し、事前共有キーの横にある [Show Key] ボタンをクリックすることにより、キーを表示できます。

- [証明書（Certificate）] を選択する場合は、証明書名を定義する PKI 登録オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合は、[<新規追加>（<Add New>）] を選択して [PKI の追加（Add PKI）] セレクタを開きます。そこで、新規 PKI 登録オブジェクトの追加、または既存の PKI 登録オブジェクトの編集を行うことができます。PKI 登録オブジェクトの詳細については、[PKI Enrollment] ダイアログボックスを参照してください。

VPN を作成したあとで証明書設定を編集するには、Policy Object Manager でオブジェクトを編集します。または、ご使用の IKE バージョンに応じて、IKEv1 Public Key Infrastructure ポリシーまたは IKEv2 Authentication ポリシーのいずれかを使用して直接編集します。

ウィザードで、[次へ（Next）] をクリックします。

ステップ 5 （Create Extranet VPN ウィザードのみ）[サマリー（Summary）] ページで、設定が正しいことを確認し、[完了（Finish）] をクリックします。

Security Manager は、トポロジおよび必要なポリシー オブジェクトを作成し、Site-to-Site VPN Manager の VPN のリストに VPN を追加します。

ステップ 6 ダイヤルバックアップを設定する場合は、[ピア（Peers）]ポリシーを選択し、ダイヤルバックアップの設定 （54 ページ）の説明に従います。

VPN トポロジの削除

VPN トポロジを削除すると、サイト間 VPN に割り当てられているデバイスとネットワークから、ピア間の IPsec トンネルおよび VPN トポロジに関連付けられたすべての設定が削除されます。設定を展開するまでは、ネットワークから実際の VPN は削除されません。

ステップ 1 次のいずれかを実行します。

- [管理（Manage）] > [サイト間 VPN（Site-To-Site VPNs）] を選択して、[Site-to-Site VPN Manager] ウィンドウ （26 ページ）を開きます。
- デバイスビューで、削除する VPN に参加しているデバイスを選択して、ポリシーセレクタから [サイト間 VPN（Site to Site VPN）] ポリシーを選択します（デバイス ビューにおける VPN トポロジの設定（27 ページ）を参照）。

ステップ 2 削除する VPN トポロジを選択して、[VPN トポロジの削除（Delete VPN Topology）]（ゴミ箱）ボタンをクリックします。削除の確認が求められます。

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。