サイト間 VPN

- サイト間 VPN について （1 ページ）
- サイト間 VPN トポロジのタイプ （5 ページ）
- サイト間 VPN の要件と前提条件 （5 ページ）
- サイト間 VPN の管理 （6 ページ）
- ポリシーベースのサイト間 VPN の設定 （7 ページ）
- 仮想トンネル インターフェイスについて （25 ページ）
- 仮想トンネルインターフェイスのガイドラインと制限事項 （29 ページ）
- VTI インターフェイスの追加 （34 ページ）
- ルートベースのサイト間 VPN の作成 （36 ページ）
- バックアップ VTI トンネルを介したトラフィックのルーティング （50 ページ）
- ルートベースのサイト間 VPN のダイナミック VTI の設定 （52 ページ）
- ダイナミック VTI を使用した仮想ルータの設定方法 （52 ページ）
- VTI のルーティングおよび AC ポリシーの設定 （53 ページ）
- 仮想トンネル情報の表示 （57 ページ）
- Umbrella に SASE トンネルを展開する （58 ページ）
- Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 （59 ページ）
- Cisco Umbrella に SASE トンネルを展開する方法 （60 ページ）
- サイト間 VPN のモニタリング （66 ページ）
- サイト間 VPN の履歴 （73 ページ）

サイト間 VPN について

Secure Firewall Threat Defense サイト間 VPN では、次の機能がサポートされています。

- IPsec IKEv1 および IKEv2 プロトコルの両方。
- 証明書および自動または手動の事前共有認証キー。
- IPv4 および IPv6。内部、外部のすべての組み合わせをサポート。
- IPsec IKEv2 サイト間 VPN トポロジにより、セキュリティ認定に準拠するための設定を提供。

- スタティック インターフェイスおよびダイナミック インターフェイス。
- Firewall Management Center と Firewall Threat Defense の両方の HA 環境。
- トンネルがダウンした際の VPN アラート。
- Firewall Threat Defense 統合 CLI により利用可能なトンネル統計。
- ポイントツーポイント エクストラネット VPN およびハブアンドスポーク VPN の IKEv1 および IKEv2 バックアップピア設定。
- 「ハブアンドスポーク」展開でのハブとしてのエクストラネットデバイス。
- 「ポイントツーポイント」展開でのエクストラネットデバイスを使用した管理対象エンドポイントペアリングのダイナミック IP アドレス。
- エンドポイントとしてのエクストラネットデバイスのダイナミック IP アドレス。
- 「ハブアンドスポーク」展開でのエクストラネットとしてハブ。

VPN トポロジ

新しいサイト間VPNトポロジを作成するには、一意の名前を付け、トポロジタイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンと認証方式を選択する必要があります。また、認証方法を決定します。設定したら、Firewall Threat Defense デバイスにトポロジを展開します。Secure Firewall Management Center は、Firewall Threat Defense デバイスのサイト間 VPN のみ設定します。

次の 3 つのタイプのトポロジから選択することができます。トポロジには、VPN トンネルが 1 つ以上含まれています。

- ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。
- ハブ アンド スポーク型の展開は、VPN トンネルのグループを確立し、ハブ エンドポイントをスポーク ノードのグループに接続します。
- フル メッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

IPsec と IKE

Secure Firewall Management Center では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。ポリシーとプロポーザル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。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。

認証

VPN接続の認証には、トポロジ内で事前共有キー、または各デバイスでトラストポイントを設定します。事前共有キーにより、IKE 認証フェーズで使用する秘密鍵を 2 つのピア間で共有できます。トラストポイントには、CA の ID、CA 固有のパラメータ、登録されている単一の ID 証明書とのアソシエーションが含まれています。

エクストラネット デバイス

各トポロジタイプには、Firewall Management Center で管理しないデバイスである、エクストラネットデバイスが含まれる可能性があります。次のようなものがあります。

- Secure Firewall Management Center ではサポートされているが、ユーザーの部門が担当していないシスコデバイス。たとえば、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などです。
- シスコ製以外のデバイス。Secure Firewall Management Center 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。

シスコ以外のデバイス、または Secure Firewall Management Center で管理されていないシスコデバイスをVPNトポロジに「エクストラネット」デバイスとして追加します。また、各リモート デバイスの IP アドレスも指定します。

Secure Firewall Threat Defense サイト間 VPN ガイドラインと制約事項

- ECMP ゾーンインターフェイスは、サイト間 VPN でサポートされます。
- 暗号 ACL または保護されたネットワークのいずれかを使用して、トポロジ内のすべてのノードを設定する必要があります。あるノードでは暗号 ACL を使用し、別のノードでは保護されたネットワークを使用するトポロジを設定することはできません。
- 現在のドメイン内ではないエンドポイント用のエクストラネットピアを使用して、ドメイン間の VPN 接続を設定できます。
- Firewall Management Center バックアップを使用して Firewall Threat Defense VPN をバックアップできます。
- IKEv1 は、CC/UCAPL 準拠のデバイスをサポートしていません。これらのデバイスには IKEv2 を使用することをお勧めします。
- VPN トポロジをドメイン間で移動させることはできません。
- VPNは、「範囲」オプションのあるネットワークオブジェクトをサポートしていません。
- Firewall Threat Defense VPN では、現在、PDF のエクスポートおよびポリシーの比較をサポートしていません。
- Firewall Threat Defense VPN ではトンネル単位またはデバイス単位の編集オプションはありません。トポロジ全体のみ編集できます。

- 暗号 ACL を選択した場合、Firewall Management Center は、トランスポートモードのデバイス インターフェイス アドレスの検証を行いません。
- 自動ミラー ACE 生成はサポートされません。ピアのミラー ACE 生成は、どちらの側でも手動プロセスです。
- 暗号 ACL では、Firewall Management Center はポイントツーポイント VPN のみをサポートし、トンネルヘルスイベントはサポートしません。
- IKE ポート 500/4500 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、サイト間 VPN を同じポートに設定することはできません。
- Firewall Management Center では、トンネルの状態はリアルタイムではなく、5 分間隔でアップロードされます。
- 文字「"」（二重引用符）は事前共有キーの一部として使用できません。事前共有キーで「"」を使用した場合は、文字必ずを変更してください。
- 2 つのデバイスが同じ Firewall Management Center によって管理されているサイト間 VPN 設定では、デバイスをバックアップピアとして設定できません。トポロジ内のピアデバイスの 1 つをエクストラネットデバイスとして設定する必要があります。
- すべての VPN トポロジのすべてのトンネルで一意のローカル IKE アイデンティティを設定します。
- 高可用性を備えたリモートブランチ展開（RBD）において、高可用性ペアを解除する場合は以下を参照してください。
  - ハブアンドスポーク VPN の場合
    - Firewall Threat Defense HAがハブの場合、VPN 設定はアクティブなデバイスで使用可能になり、スタンバイデバイスでは削除されます。
    - Firewall Threat Defense HAがスポークの場合、VPN 設定はアクティブデバイスとスタンバイデバイスで使用可能になります。
  - ポイントツーポイント VPN の場合、エンドポイントに RBD Firewall Threat Defense HA WAN インターフェイスがある場合、VPN 設定はスタンバイデバイスから削除されます。

サイト間 VPN トポロジのタイプ

サイト間 VPN トポロジ	説明	詳細情報
SD-WANトポロジ	SD-WAN ウィザードを使用して、セキュアなブランチネットワークを設定します。このウィザードによって、ハブアンドスポークトポロジを使用したネットワークの VPN およびルーティング設定を簡素化および自動化し、SD-WAN 機能を有効化します。	SD-WAN ウィザードを使用したセキュアなブランチネットワークの展開
ルートベース VPN	仮想トンネルインターフェイス（VTI）を介したルーティングに基づいて、セキュアなネットワーク内のピア間のトラフィックを動的に設定します。	ルートベースのサイト間 VPN の作成 （36 ページ）
ポリシーベース VPN	保護されたネットワークを使用し、静的ポリシーに基づいて、ネットワーク内のピア間のセキュアなトラフィックを設定します。	ポリシーベースのサイト間 VPN の設定 （7 ページ）
SASEトポロジ	Threat Defense デバイスから Umbrella Secure Internet Gateway（SIG）への IPsec IKEv2 トンネルを設定します。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Cisco Umbrella SIG に転送します。	Cisco Umbrella 用の SASE トンネルの設定 （63 ページ）

サイト間 VPN の要件と前提条件

Model support

Firewall Threat Defense

Supported domains

Leaf

User roles

Admin

サポートされるインターフェイス

トポロジタイプ	インターフェイス タイプ

ポリシーベース および SD-WAN	• 物理インターフェイス
	  • 非管理
	  • インターフェイスモードは「ルーテッド」または「なし」のいずれかにする必要があります
	• サブインターフェイス インターフェイス
	• 冗長インターフェイス
	• EtherChannel インターフェイス
	• VLAN インターフェイス

ルートベース	スタティック仮想トンネル インターフェイス

サイト間 VPN の管理

[サイト間VPN（Site-to-Site VPN）]ページには、サイト間VPNトンネルのスナップショットが表示されます。トンネルのステータスを表示し、デバイス、トポロジ、またはトンネルタイプに基づいてトンネルをフィルタ処理できます。このページには、ページごとに 20 のトポロジが一覧表示され、ページ間を移動してトポロジの詳細を表示できます。個々の VPN トポロジをクリックして展開し、エンドポイントの詳細を表示できます。

始める前に

サイト間 VPN の証明書認証の場合は、証明書の説明に従い、トラストポイントを割り当てて デバイスを準備する必要があります。

手順

Devices > **VPN** > **Site to Site** を選択して、Firewall Threat Defense のサイト間 VPN の設定と展開を管理します。

このページには、サイト間 VPN トポロジが一覧表示され、色コードを使用してトンネルのステータスが示されます。

- [アクティブ（Active）]（緑）：アクティブな IPsec トンネルがあります。
- [不明（Unknown）]（オレンジ）：デバイスからトンネル確立イベントをまだ受信していません。
- [ダウン（Down）]（赤）：アクティブな IPsec トンネルがありません。
- [展開保留中（Deployment Pending）]：トポロジはまだデバイスに展開されていません。

次のオプションから選択します。

- [更新（Refresh）]：VPN の更新されたステータスが表示されます。
- [追加（Add）]：新しいポリシーベースまたはルートベースのサイト間 VPN を作成します。
- [編集（Edit）]：既存の VPN トポロジの設定を変更します。

  （注）
  トポロジ タイプは、最初の保存後に編集することはできません。トポロジ タイプを変更するには、トポロジを削除してから新しいものを作成します。

  2 人のユーザーで同じトポロジを同時に編集しないでください。ただし、Web インターフェイスでは同時編集できます。

- [削除（Delete）]：VPN の展開を削除するには、**Delete** ( )をクリックします。
- [デプロイ（Deploy）]：[**Deploy**>**Deploy**] を選択します。（「設定変更の展開」を参照）。

  （注）
  一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

ポリシーベースのサイト間 VPN の設定

手順

ステップ 1 **Devices** > **VPN** > **Site to Site** を選択し、**[追加（Add）]** をクリックしします。
ステップ 2 **[トポロジ名（Topology Name）]** フィールドに、トポロジの名前を入力します。
ステップ 3 **[ポリシーベース VPN（Policy-Based VPN）]** ラジオ ボタンをクリックします。
ステップ 4 VPN トポロジを選択して、**[作成（Create）]**をクリックします。

ステップ 5 IKE ネゴシエーション中に使用する IKE バージョンとして、**[IKEv1]** または **[IKEv2]** チェックボックスをオンにします。

デフォルトは [IKEv2] です。必要に応じて、いずれかまたは両方のオプションを選択します。トポロジ内のデバイスが IKEv2 をサポートしていない場合は、[IKEv1] を選択します。

ポイントツーポイント エクストラネット VPN のバックアップピアも設定できます。詳細については、Firewall Threat Defense VPN エンドポイント オプション （9 ページ）を参照してください。

ステップ 6 必須: トポロジの各ノードの **Add** (+) をクリックして、この VPN 展開のためのエンドポイントを追加します。

Firewall Threat Defense VPN エンドポイント オプション （9 ページ）の説明に従って各エンドポイント フィールドを設定します。

- ポイントツーポイントの場合は、ノード A とノード B を設定します。
- ハブ アンド スポークの場合は、ハブ ノードとスポーク ノードを設定します。
- フル メッシュの場合は、複数のノードを設定します

ステップ 7 （任意）次の説明に従って、この展開のデフォルト以外の IKE オプションを指定しますFirewall Threat Defense VPN IKE オプション （14 ページ）

ステップ 8 （任意） 次の説明に従って、この展開のデフォルト以外の IPsec オプションを指定しますFirewall Threat Defense VPN IPsec オプション （17 ページ）

ステップ 9 （任意） Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （20 ページ）の説明に従って、この展開のデフォルト以外の詳細オプションを指定します。

ステップ 10 [保存（Save）] をクリックします。
エンドポイントが構成に追加されます。

次のタスク

設定変更を展開します設定変更の展開を参照してください。

（注） 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

VPN セッションが稼働しているのに VPN トンネルが非アクティブであるというアラートを受け取った場合は、VPN のトラブルシューティング手順に従って、VPN がアクティブであることを確認します。詳細については、VPN のモニタリングとトラブルシューティングおよびVPN のトラブルシューティングを参照してください。

Firewall Threat Defense VPN エンドポイント オプション

ナビゲーション パス

「ポイントツーポイント トポロジのエンドポイントの設定」の説明に従って、ルートベース VPN のポイントツーポイント トポロジの基本パラメータを設定し、**[エンドポイント（Endpoints）]** タブをクリックします。

フィールド

Device

展開するエンドポイント ノードを選択します。

- この Firewall Management Center で管理する Firewall Threat Defense デバイス。
- この Firewall Threat Defense で管理する Firewall Management Center ハイ アベイラビリティ コンテナ。
- [エクストラネット（Extranet）] デバイス。この Firewall Management Center の管理対象ではない任意のデバイス（シスコまたはサードパーティ）。

デバイス名（Device Name）

エクストラネットデバイスの場合のみ、このデバイスの名前を入力します。シスコでは、管理対象ではないデバイスとして識別できるような名前を付けることを推奨します。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、その管理対象デバイスのインターフェイスを選択します。

「ポイントツーポイント」展開の場合、ダイナミック インターフェイスを使用してエンドポイントを設定することもできます。ダイナミック インターフェイスを使用したエンドポイントはエクストラネットデバイスとのみペアリングできます。管理対象デバイスを持つエンドポイントとはペアリングできません。

[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの追加/編集（Add/Edit device）] > [インターフェイス（Interfaces）] でデバイスのインターフェイスを設定できます。

IP アドレス（IP Address）

- Firewall Management Center の管理対象デバイス**ではない**エクストラネット デバイスを選択した場合は、エンドポイントの IP アドレスを指定します。

  エクストラネット デバイスの場合は、[スタティック（Static）] を選択して IP アドレスを指定するか、または [ダイナミック（Dynamic）] を選択してダイナミック エクストラネット デバイスを許可します。

- エンドポイントとして管理対象デバイスを選択した場合は、ドロップダウンリストから 1 つの IPv4 アドレスまたは複数の IPv6 アドレスを選択します。これらはすでにこの管理対象デバイスのインターフェイスに割り当てられている IP アドレスです。

- トポロジ内のすべてのエンドポイントは、同じ IP アドレッシング方式でなければなりません。IPv4 トンネルは IPv6 トラフィックを伝送でき、逆もまた同様です。保護ネットワークでは、トンネルするトラフィックで使用するアドレッシング方式が定義されます。
- 管理対象デバイスがハイ アベイラビリティ コンテナである場合は、インターフェイスのリストから選択します。

この IP はプライベートです（This IP is Private）

エンドポイントが、ネットワーク アドレス変換（NAT）を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

（注） このオプションは、ピアが同じ Firewall Management Center によって管理されている場合にのみ使用します。ピアがエクストラネットデバイスである場合は、このオプションは使用しません。

パブリック IP アドレス（Public IP address）

[この IP はプライベートです（This IP is Private）] チェックボックスがオンの場合は、ファイアウォールのパブリック IP アドレスを指定します。エンドポイントがレスポンダの場合は、この値を指定します。

接続タイプ（Connection Type）

許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。接続タイプのサポートされる組み合わせは次のとおりです。

表 *1*: 接続タイプのサポートされる組み合わせ

リモート ノード	中央ノード
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

証明書マップ

事前設定された証明書マップオブジェクトを選択するか、**Add**(＋)をクリックして証明書マップオブジェクトを追加します。証明書マップは、VPN 接続で有効になるには受信したクライアント証明書でどのような情報が必要かを定義します。詳細については、「証明書マップオブジェクト」を参照してください。

保護されたネットワーク（Protected Networks）

注意 ハブアンドスポークトポロジ：ダイナミッククリプトマップでトラフィックのドロップを避けるために、両方のエンドポイントで保護されたネットワークに *any* を選択しないでください。

保護されたネットワークが両方のエンドポイントで *any* として設定されている場合、トンネルで機能する暗号 ACL が生成されません。

この VPN エンドポイントによって保護されるネットワークを定義します。このエンドポイントによって保護されるネットワークを定義するサブネット/IP アドレスのリストを選択することで、ネットワークを選択することができます。**Add**(＋)をクリックして、使用可能なネットワークオブジェクトから選択するか、新しいネットワークオブジェクトを追加します。ネットワーク オブジェクトの作成を参照してください。アクセスコントロールリストは、ここで選択されたものから生成されます。

- [サブネット/IPアドレス（ネットワーク）（Subnet/IP Address (Network)）]：VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできません。エンドポイントの保護されたネットワークに IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っている必要があります。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4 については/32 CIDR アドレスを使用し、IPv6 については/128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

（注） Firewall Management Center では、デフォルトで**リバース ルート インジェクションが有効になっています**。

[サブネット/IPアドレス（ネットワーク）（Subnet/IP Address (Network)）] はデフォルトの選択のままにします。

[保護されたネットワーク（Protected Networks）] を [任意（Any）] として選択し、デフォルトのルートトラフィックがドロップされることを確認した場合は、リバース ルート インジェクションを無効にします。[VPN] > [サイト間（Site to Site）] > [VPNの編集（edit a VPN）] > [IPsec] > [リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] を選択します。設定変更を展開して、暗号マップ設定から set reverse-route（リバース ルート インジェクション）を削除し、リバース トンネル トラフィックのドロップを引き起こす NVP でアドバタイズされたリバースルートを削除します。

- [アクセス リスト（拡張）（Access List (Extended)）]：拡張アクセスリストは、GRE トラフィックや OSPF トラフィックなどの、このエンドポイントによって受け入れられるトラフィックのタイプを制御する機能を提供します。トラフィックは、アドレスまたはポートにより制限できます。**Add**(+)をクリックして、アクセス コントロール リスト オブジェクトを追加します。

（注） アクセス コントロール リストは、ポイントツーポイント トポロジでのみサポートされています。

NAT トラバーサルの有効化

ピア Firewall Threat Defense デバイス間に NAT デバイスがある場合に、これらのデバイス間のシームレス コミュニケーションを許可するには、このチェックボックスをオンにします。ハブアンドスポークトポロジの場合、このオプションはスポークでのみ使用できます。エンドポイントに対してこの機能を無効化にするには、このチェックボックスをオフにします。このパラメータは、トポロジ内のエンドポイントに対するピアごとの設定です。

グローバル NAT トラバーサル（NAT-T）設定を表示または設定するには、**[VPNトポロジの追加/編集（Add/Edit VPN Topology）]** ダイアログボックスで次の手順を実行します。

1. [詳細（Advanced）] タブをクリックします。
2. 左側のナビゲーションウィンドウで、[トンネル（Tunnel）] をクリックします。
3. [NAT設定（NAT Settings）] の [キープアライブ メッセージ トラバーサル（Keepalive Messages Traversal）] は、トポロジ内のすべてのエンドポイントに対して NAT -T を有効にするグローバル設定です。

VPNトラフィックをネットワークアドレス変換から除外する（Exempt VPN traffic from network address translation）

ネットワークアドレス変換（NAT）ルールの対象から VPN トラフィックを除外するには、このチェックボックスをオンにします。

NAT ルールの対象から VPN トラフィックを除外しない場合、トラフィックはドロップされるか、VPN トンネルを介してリモートデバイスにルーティングされません。このオプションを有効にすると、[NATポリシー（NAT policy）] ページ（[デバイス（Device）] > [NAT] > [NAT免除（NAT Exemptions）]）でデバイスの NAT 免除を表示できます。

内部ネットワークに直接接続された内部インターフェイス（Inside interfaces directly connected to the internal network）

保護されたネットワークが存在する内部インターフェイスのセキュリティゾーンまたはインターフェイスグループを指定します。デフォルトでは、内部インターフェイスは any です。

[+] をクリックして、1 つ以上の内部インターフェイスにマッピングできるセキュリティゾーンまたはインターフェイスグループから 1 つ以上のインターフェイスを設定します。セキュリティゾーンまたはインターフェイスグループのインターフェイスタイプがルーテッドであることを確認します。

詳細設定（Advanced Settings）

[ダイナミック リバース ルート インジェクションを有効にする（Enable Dynamic Reverse Route Injection）]：リバース ルート インジェクション（RRI）では、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティングプロセスに、ルートを自動的に組み込むことができます。ダイナミック RRI ルートは IPsec セキュリティ アソシエーション（SA）の確立成功時にのみ作成されます

（注）

- ダイナミック RRI は IKEv2 でのみサポートされ、IKEv1 または IKEv1 + IKEv2 ではサポートされません。
- ダイナミック RRI は、発信のみのピア、フルメッシュトポロジ、およびエクストラネットピアではサポートされていません。
- ポイントツーポイントでは、1 つのピアでのみダイナミック RRI を有効にすることができます。
- ハブとスポークの間では、1 つのエンドポイントでのみダイナミック RRI を有効にすることができます。
- ダイナミック RRI は、ダイナミッククリプトマップと組み合わせることはできません。

[ピアへのローカルIDの送信（Send Local Identity to Peers）]：ローカル ID 情報をピアデバイスに送信するには、このオプションを選択します。リストから次のいずれかの [ローカルID構成（Local Identity Configuration）] を選択し、ローカル ID を設定します。

- [IPアドレス（IP address）]：ID にインターフェイスの IP アドレスを使用します。
- [自動（Auto）]：事前共有キーには IP アドレスを使用し、証明書ベースの接続には証明書 DN を使用します。
- [電子メールID（Email ID）]：ID に使用する電子メール ID を指定します。電子メール ID は最大 127 文字です。
- [ホスト名（Hostname）]：完全修飾ホスト名を使用します。
- [キーID（Key ID）]：ID に使用するキー ID を指定します。キー ID は 65 文字未満にする必要があります。

ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。一意の ID を設定すると、Cisco Umbrella Secure Internet Gateway（SIG）に接続するために、Firewall Threat Defense が NAT の背後に複数の IPsec トンネルを持つことができます。

Cisco Umbrella での一意のトンネル ID の設定については、**Cisco Umbrella SIG ユーザーガイド** [英語] を参照してください。

[VPNフィルタ（VPN Filter）]：リストから拡張アクセスリストを選択するか、[追加（Add）] をクリックして新しい拡張アクセスリストオブジェクトを作成し、サイト間 VPN トラフィックをフィルタリングします。

VPN フィルタはセキュリティを強化し、拡張アクセスリストを使用してサイト間VPNデータをフィルタリングします。VPNフィルタ用に選択された拡張アクセスリストオブジェクトを使用すると、VPN トンネルに入る前に事前暗号化されたトラフィックと、VPN トンネルを出る復号されたトラフィックをフィルタリングできます。**sysopt permit-vpn** オプションを有効にすると、VPN トンネルからのトラフィックのアクセス コントロール ポリシー ルールがバイパスされます。**sysopt permit-vpn** オプションが有効になっている場合、VPN フィルタは、サイト間 VPN トラフィックの識別とフィルタリングに役立ちます。

（注） VPN フィルタは、ポイント ツー ポイント トポロジおよびハブアンドスポークトポロジでのみサポートされます。メッシュトポロジではサポートされていません。

ハブアンドスポークトポロジの場合、特定のトンネルで別の VPN フィルタを有効にする必要がある場合に備えて、スポークエンドポイントでハブ VPN フィルタをオーバーライドすることを選択できます。

スポークのハブ VPN フィルタを無効にするには、[ハブでのVPNフィルタのオーバーライド（Override VPN Filter on the Hub）] オプションを選択します。[リモートVPNフィルタ（Remote VPN Filter）] 拡張アクセスリストオブジェクトを選択するか、上書きするアクセスリストを作成します。

（注） エクストラネットデバイスをスポークとして使用する場合、[ハブでのVPNフィルタのオーバーライド（Override VPN Filter on the Hub）] オプションのみを使用できます。

sysopt permit-VPN の詳細については、Firewall Threat Defense のサイト間 VPN トンネルの詳細オプション （23 ページ）を参照してください。

Firewall Threat Defense VPN IKE オプション

このトポロジに選択した IKE のバージョンの場合は、[IKEv1/IKEv2 設定（IKEv1/IKEv2 Settings）] を指定します。

（注） このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

ナビゲーション パス

「ポイントツーポイント トポロジのエンドポイントの設定」の説明に従って、ルートベース VPN のポイントツーポイント トポロジの基本パラメータを設定し、**[IKE]** タブをクリックします。

フィールド

ポリシー（Policy）

事前定義リストから必要な IKEv1 または IKEv2 ポリシーオブジェクトを選択するか、または使用する新しいポリシーオブジェクトを作成します。複数の IKEv1 および IKEv2 ポリシーを選択できます。IKEv1 と IKEv2 は、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

10、20 などの値は使用しないことを推奨します。リモート アクセス VPN のデフォルト IKEv2 ポリシーにプライオリティ値としてこれらの値を設定している場合があるからです。展開前に、IKE ポリシー（サイト間およびリモート アクセス VPN）のプライオリティ値が競合しないことを確認してください。

詳細については、IKE ポリシーを参照してください。

認証タイプ（Authentication Type）

サイト間 VPN では、事前共有キーと証明書の 2 つの認証方式がサポートされています。2 つの方式の説明については、使用する認証方式の決定を参照してください。

（注） IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式（Authentication Method）] が、IKEv1 の [認証タイプ（Authentication Type）] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

- [事前共有自動キー（Pre-shared Automatic Key）]：Firewall Management Center により、この VPN の事前共有キーが自動的に定義されます。[事前共有キー長（Pre-shared Key Length）] を指定します。キーの文字数は 1 ～ 27 文字です。

  文字 "（二重引用符）は事前共有キーの一部としてサポートされていません。事前共有キーで " を使用した場合は、Secure Firewall Threat Defense 6.30 以降にアップグレードした後に必ず文字を変更してください。

- [事前共有手動キー（Pre-shared Manual Key）]：この VPN の事前共有キーを手動で割り当てます。[キー（Key）] を指定して、[キーの確認（Confirm Key）] に同じキーを再入力します。

  IKEv2 に対してこのオプションを選択すると、[16進数ベースの事前共有キーのみを適用する（Enforce hex-based pre-shared key only）] チェックボックスが表示されるので、必要に応じてオンにします。適用する場合は、キーの有効な 16 数値を、数字 0 ～ 9 または A ～ F を使用して、2 ～ 256 文字の偶数で入力する必要があります。

- [証明書（Certificate）]：VPN 接続の認証方法として証明書を使用する場合、ピアは PKI インフラストラクチャ内の CA サーバーからデジタル証明書を取得し、相互に認証するためにトレードします。

  [証明書（Certificate）]フィールドで、事前設定された証明書登録オブジェクトを選択します。この登録オブジェクトにより、管理対象デバイス上で同じ名前のトラストポイントが生成使用されます。証明書登録オブジェクトが関連付けられ、デバイスにインストールされ、登録プロセスが完了してから、トラストポイントが作成されます。

  トラストポイントとは、CA またはIDペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

  このオプションを選択する前に、次の点に注意してください。

  - トポロジ内のすべてのエンドポイントに証明書登録オブジェクトが登録されていることを確認します。証明書登録オブジェクトには、証明書署名要求（CSR）を作成し、指定された認証局（CA）からアイデンティティ証明書を取得するために必要な CA サーバー情報と登録パラメータが含まれています。証明書登録オブジェクトは、管理対象デバイスを PKI インフラストラクチャに登録し、VPN 接続をサポートするデバイス上にトラストポイント（CA オブジェクト）を作成するために使用されます。証明書登録オブジェクトの作成手順については、証明書の登録オブジェクトの追加を参照してください。エンドポイントにオブジェクトを登録する手順については、次のいずれかを参照してください。
    - 自己署名登録を使用した証明書のインストール
    - EST 登録を使用した証明書のインストール
    - SCEP の登録を使用した証明書のインストール
    - 手動登録を使用した証明書のインストール
    - PKCS12 ファイルを使用した証明書のインストール

  （注） サイト間 VPN トポロジの場合、同じ証明書登録オブジェクトがトポロジ内のすべてのエンドポイントに登録されていることを確認します。詳細については、次の表を参照してください。

  - さまざまなシナリオの登録要件については、次の表を参照してください。一部のシナリオでは、特定のデバイスの証明書登録オブジェクトを上書きする必要があります。オブジェクトの上書き方法については、オブジェクト オーバーライドの管理を参照してください。

証明書の登録タイプ	すべてのエンドポイントのデバイス ID 証明書の CA が同じ		すべてのエンドポイントのデバイス ID 証明書の CA が異なる
	デバイス固有のパラメータが証明書登録オブジェクトで指定されていない	デバイス固有のパラメータが証明書登録オブジェクトで指定されている	
手動	上書きは不要	上書きが必要	上書きが必要
EST	上書きは不要	上書きが必要	上書きが必要
SCEP	上書きは不要	上書きが必要	上書きが必要
PKCS	上書きが必要	上書きが必要	上書きが必要
自己署名	N/A	N/A	N/A

- Secure Firewall Threat Defense VPN 証明書の注意事項と制約事項記載されている VPN 証明書の制限事項を確認。

（注） Windows認証局（CA）を使用する場合、デフォルトのアプリケーションポリシー拡張は**IP セキュリティ IKE 中間**です。このデフォルト設定を使用している場合は、選択したオブジェクトの [PKI証明書登録（PKI Certificate Enrollment）] ダイアログボックスの [キー（Key）] タブにある [詳細設定（Advanced Settings）] セクションで [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] オプションを選択する必要があります。それ以外の場合、エンドポイントでサイト間 VPN 接続を完了できません。

Firewall Threat Defense VPN IPsec オプション

（注） このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

ポイントツーポイント トポロジのエンドポイントの設定の説明に従って、ルートベース VPN のポイントツーポイント トポロジの基本パラメータを設定し、**[IPsec]** タブをクリックします。

クリプト マップ タイプ（Crypto-Map Type）
クリプト マップには、IPsec Security Association（SA; セキュリティ アソシエーション）を設定するために必要なすべてのコンポーネントが組み合わされています。2つのピアが SA

を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップ エントリが必要です。IPsec セキュリティ ネゴシエーションでは、クリプトマップエントリに定義されたプロポーザルを使用して、そのクリプトマップの IPsec ルールによって指定されたデータフローが保護されます。この展開のクリプト マップにスタティックまたはダイナミックを選択します。

- [スタティック（Static）]：スタティック クリプト マップは、ポイントツーポイントまたは完全メッシュ VPN トポロジで使用します。
- [ダイナミック（Dynamic）]：実質的に、ダイナミック暗号マップによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。

  ダイナミック暗号マップ ポリシーは、ハブアンドスポークとポイントツーポイント VPN トポロジの両方に適用されます。これらのポリシーを適用するには、トポロジ内のピアの 1 つにダイナミック IP アドレスを指定し、このトポロジでダイナミック暗号マップが有効になっていることを確認します。フルメッシュ VPN トポロジでは、スタティック暗号マップポリシーのみを適用できます。

IKEv2 モード（IKEv2 Mode）

IPsec IKEv2 の場合のみ、カプセル化モードはトンネルに ESP 暗号化と認証を適用するために指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

- [トンネルモード（Tunnel mode）]：（デフォルト）カプセル化モードがトンネル モードに設定されます。トンネル モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、最終的な送信元アドレスと宛先アドレスが非表示になり、新しい IP パケットでペイロードになります。

  トンネルモードの主な利点は、エンドシステムを変更しなくても IPsec を利用できることです。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。また、トラフィック分析から保護することもできます。トンネルモードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- [転送優先（Transport preferred）]：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転送モードに設定されます。トランスポートモードでは、IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。したがって、管理者は、VPN インターフェイスの IP アドレスと一致する保護されたネットワークを選択する必要があります。

  このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッ

ダーの情報に基づいて実行できるようになります。ただし、レイヤ4ヘッダーが暗号化されるため、パケットの検査が制限されます。

- [転送必須（Transport required）]：カプセル化モードは転送モードのみに設定され、トンネルモードにフォールバックできます。転送モードをサポートしていない1つのエンドポイントがあるせいで、エンドポイントが転送モードを正常にネゴシエートできない場合、VPN 接続は行われません。

プロポーザル（Proposals）

選択した IKEv1 または IKEv2 メソッドのプロポーザルを指定するには、**Edit** ()をクリックします。利用可能な [IKEv1 IPsecプロポーザル（IKEv1 IPsec Proposals）] または [IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposals）] オブジェクトから選択するか、または新しいプロポーザルを作成して選択します。詳細については、「IKEv1 IPsec プロポーザル オブジェクトの設定」および「IKEv2 IPsec プロポーザル オブジェクトの設定」を参照してください。

セキュリティ アソシエーション（SA）の強度適用の有効化（Enable Security Association (SA) Strength Enforcement）

このオプションを有効にすると、子 IPsec SA で使用される暗号化アルゴリズムが、親 IKE SA よりも強くなることはありません（キー内のビット数の観点から）。

リバース ルート インジェクションを有効にする（Enable Reverse Route Injection）

リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

Perfect Forward Secrecy の有効化（Enable Perfect Forward Secrecy）

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイントデバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

係数グループ（Modulus Group）

2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの詳しい説明については、Deciding Which Diffie-Hellman Modulus Group to Useを参照してください。

ライフタイム期間

セキュリティ アソシエーションが期限切れになる前に存続できる秒数。デフォルトは 28,800 秒です。

ライフタイム サイズ

特定のセキュリティ アソシエーションが期限切れになる前にそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。デフォルトは 4,608,000 KB です。無制限のデータは許可されていません。

ESPv3 設定（ESPv3 Settings）

着信 ICMP のエラーメッセージを検証（Validate incoming ICMP error messages）
IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラー メッセージを検証するかどうかを選択します。

「フラグメント禁止」ポリシーを有効にする（Enable 'Do Not Fragment' Policy）
IP ヘッダーに Do-Not-Fragment（DF）ビット セットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。

ポリシー

- [DF ビッドのコピー（Copy DF bit）]：DF ビットを維持します。
- [DF ビッドのクリア（Clear DF bit）]：DF ビットを無視します。
- [DF ビットの設定（Set DF bit）]：DF ビットを設定して使用します。

トラフィック フロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）
トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト（Burst）]、[ペイロードサイズ（Payload Size）]、および [タイムアウト（Timeout）]パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

（注） IPSec セキュリティ アソシエーション（SA）における、ランダムな長さおよび間隔のダミーのトラフィックフローの機密性（TFC）パケットを有効にできます。TFC をイネーブルにするには、IKEv2 IPsec プロポーザルが設定されている必要があります。

TFC パケットを有効にすると、VPN トンネルがアイドル状態になることが防止されます。そのため、TFC パケットを有効にすると、グループポリシーで設定された VPN アイドル タイムアウトが期待どおりに機能しません。

Firewall Threat Defense のサイト間 VPN 展開の詳細オプション

ここでは、サイト間 VPN の展開で指定できる詳細オプションについて説明します。それらの設定は、トポロジ全体、すべてのトンネル、およびすべての管理対象デバイスに適用されます。

Firewall Threat Defense VPN の IKE 詳細オプション

[詳細設定（Advanced）] > [IKE] > [ISAKAMP 設定（ISAKAMP Settings）]

IKE キープアライブ（IKE Keepalive）

IKE キープアライブを有効または無効にします。このオプションを [永続的に有効にする（EnableInfinite）] に設定して、デバイス自体がキープアライブモニタリングを開始しないようにできます。

しきい値（Threshold）
IKEキープアライブの信頼間隔を指定します。この間隔は、キープアライブモニタリングを開始するまでにピアに許可されるアイドル時間（秒）です。最小およびデフォルトの間隔は 10 秒で、最大の間隔は 3,600 秒です。

再試行間隔（Retry Interval）
IKEキープアライブの再試行から再試行までの待機秒数を指定します。デフォルトは 2 秒で、最大値は 10 秒です。

ピアに送信される ID:（Identity Sent to Peers:）
IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。

- [autoOrDN]（デフォルト）：接続タイプによって IKE ネゴシエーションを判別します。事前共有キーの IP アドレスまたは証明書認証の証明書 DN（未サポート）を使用します。
- [IPアドレス（ipAddress）]：ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
- [ホスト名（hostname）]：ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します。この名前は、ホスト名とドメイン名で構成されます。

（注） すべての VPN 接続のこのオプションを有効または無効にします。

ピアIDの確認
IKEトンネルの確立中に、ピアはそのアイデンティティ（IPアドレス、完全修飾ドメイン名（FQDN）、または識別名（DN）のいずれかを提供します。また、証明書も提示します。これらのフィールドをまったく含まない、一部を含む、またはすべてを含むのいずれかです。

IKE ピア アイデンティティの検証がイネーブルの場合、 Firewall Threat Defense はピアのアイデンティティ証明書の対応するフィールドと比較して、情報が一致するかどうかを確認します。情報が一致すると、ピアのアイデンティティが検証され、Firewall Threat Defense はトンネルを確立します。情報が一致していない場合、トンネルは確立されません。

- **[確認しない（Do not check）]**：Firewall Threat Defense はピアのアイデンティティを検証しません。
- **[必須（Required）]**：Firewall Threat Defense はピアのアイデンティティを検証します。
- **[証明書でサポートされている場合（If supported by cert）]**：Firewall Threat Defense はピアが証明書を提供する場合にのみピアのアイデンティティを検証します。

アグレッシブ モードの有効化（Enable Aggressive Mode）
IP アドレスが不明で、デバイスで DNS 解決を使用できない可能性がある場合は、このネゴシエーション方式を選択してキー情報を交換します。ホスト名およびドメイン名に基づいてネゴシエーションが行われます。

トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）
管理者は、SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にすることができます。この通知はデフォルトで無効になっています。

[詳細設定（Advanced）]>[IKE]>[IVEv2 セキュリティ アソシエーション（SA）設定（IVEv2 Security Association (SA) Settings）]

IKE v2 について、オープン SA の数を制限するさらに詳細なセッション制御を使用することができます。デフォルトでは、オープン SA の数に制限はありません。

クッキー チャレンジ（Cookie Challenge）
SA 開始パケットの応答としてピア デバイスにクッキー チャレンジを送信するかどうかを指定します。これは、サービス妨害（DoS）攻撃の防止に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキー チャレンジを使用します。次のオプションのいずれか 1 つを選択します。

- カスタム（Custom）
- しない（Never）（デフォルト）
- 常に（Always）

着信クッキー チャレンジのしきい値（Threshold to Challenge Incoming Cookies）
許可されるネゴシエーション中の SA の総数の割合。この設定を指定すると、以降の SA ネゴシエーションに対してクッキー チャレンジがトリガーされます。範囲は 0 ～ 100 % です。

許可されるネゴシエーション中の SA の数（Number of SAs Allowed in Negotiation）
一時点でネゴシエーション中にできる SA の最大数を制限します。クッキー チャレンジと共に使用する場合は、有効なクロス チェックが実行されるようにするため、クッキーチャレンジのしきい値をこの制限値よりも低くしてください。

許可される SA の最大数（Maximum number of SAs Allowed）
許可される IKEv2 接続の数を制限します。デフォルトでは無制限です。

トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）
管理者は、SA で受信された着信パケットがその SA のトラフィックセレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にできます。デフォルトでは、[この通知を送信する（Sending this notification）] は無効になっています。

Firewall Threat Defense VPN の IPsec 詳細オプション

[詳細設定（Advanced）] > [IPsec] > [IPsec 設定（IPsec Settings）]

暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）
このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。

パスの最大伝送ユニットのエージング（Path Maximum Transmission Unit Aging）
オンにすると、パス最大伝送ユニット（PMTU）のエージング、つまり、セキュリティアソシエーション（SA）の PMTU がリセットされるまでの時間が有効になります。

値のリセット間隔（Value Reset Interval）
SA の PMTU 値が元の値にリセットされるまでの時間（分）を入力します。有効範囲は 10 ～ 30 分です。デフォルトは無制限です。

Firewall Threat Defense のサイト間 VPN トンネルの詳細オプション

ナビゲーション パス

[詳細（Advanced）] > [トンネル（Tunnel）]。

トンネル オプション

ハブ アンド スポークおよびフル メッシュ トポロジでのみ使用できます。このセクションはポイントツーポイント構成の場合は表示されません。

- [ハブを介したスポークツースポーク接続を有効にする（Enable Spoke to Spoke Connectivity through Hub）]：デフォルトでは無効になっています。このフィールドを選択すると、スポークの両端にあるデバイスは、ハブ ノードを介して他のデバイスへの接続を拡張できます。

NAT 設定

- [キープアライブ メッセージ トラバーサル（Keepalive Messages Traversal）]：デフォルトで有効です。このパラメータは、トポロジ内のすべてのエンドポイントに対して NAT -T を有効にするグローバル設定です。NAT トラバーサルのキープアライブメッセージを有効にするには、このチェックボックスをオンにします。VPN接続ハブアンドスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブメッセージを転送するために NAT トラバーサルキープアライブを使用します。このデバイスでは、IPsec フローで NAT が実行されます。

  NAT トラバーサルにより、ピア Firewall Threat Defense デバイス間に NAT デバイスがある場合、これらのデバイス間のシームレス コミュニケーションが可能になります。ハブアンドスポークトポロジの場合、このオプションはスポークでのみ使用できます。

  このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される**間隔**（秒）を設定します。値は、5 ～ 3600 秒の範囲で指定します。デフォルトは 20 秒です。VPN ウィザード（[エンドポイントの追加（Add Endpoint）] ダイアログボックスの [NATトラバーサルの有効化（Enable NAT Traversal）] チェックボックス）を使用して追加するときに、トポロジ内のエンドポイントに対してこの機能を無効化にできます。

[Session Settings]

- [VPNアイドルタイムアウトの有効化（Enable VPN Idle Timeout）]：デフォルトで有効になっています。このタイムアウトは、トンネル内でアクティビティがない状態が続いた場

合に、VPN接続が切断されるまでのアイドル時間を指します。デフォルトのタイムアウトは 30 分です。

VPN トラフィックのアクセス制御

[復号されたトラフィック（sysopt permit-vpn）に対するバイパスアクセスコントロールポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：Firewall Threat Defense デフォルトでは、アクセス コントロール ポリシーの検査は復号されたトラフィックに適用されます。ACL検査をバイパスするには、このオプションを有効にします。Firewall Threat Defense では、AAA サーバーからダウンロードされた VPN フィルタ ACL および認証 ACL は引き続き VPN トラフィックに適用されます。

すべての VPN 接続のオプションを有効または無効にします。このオプションを無効にする場合は、トラフィックがアクセス コントロール ポリシーまたはプレフィルタポリシーによって許可されていることを確認してください。

（注） ルートベースの VPN の場合、**sysopt permit-vpn** は機能しません。ルートベースの VPN トラフィックを許可するには、アクセス制御ルールを設定する必要があります。

証明書マップの設定

- [エンドポイントで設定された証明書マップを使用してトンネルを判別する（Use the certificate map configured in the Endpoints to determine the tunnel）]：このオプションを有効にする（オンにする）と、受信した証明書の内容をエンドポイントノードに設定されている証明書マップオブジェクトと照合することによってトンネルが判別されます。
- [証明書のOUフィールドを使用してトンネルを判別する（Use the certificate OU field to determine the tunnel）]：選択した場合、設定されたマッピング（上記のオプション）に基づいてノードが判別されない場合は、受信した証明書のサブジェクト識別名（DN）の組織単位（OU）の値を使用してトンネルを判別することを示します。
- [IKE IDを使用してトンネルを判別する（Use the IKE identity to determine the tunnel）]：選択した場合、OU（上記のオプション）と一致するルールまたは OU から取得されたルールに基づいてノードが判別されない場合は、証明書ベースのIKEセッションが、フェーズ 1 IKE ID の内容に基づいてトンネルにマッピングされることを示します。
- [ピアIPアドレスを使用してトンネルを判別する（Use the peer IP address to determine the tunnel）]：選択した場合、トンネルがOUまたはIKE ID方式と一致するルールまたはその方式から取得されたルールに基づいて判別されない場合は、確立されたピア IP アドレスを使用することを示します。

仮想トンネル インターフェイスについて

Firewall Management Center は、仮想トンネルインターフェイス（VTI）と呼ばれるルーティング可能な論理インターフェイスをサポートします。VTI では、IPsec セッションから物理インターフェイスへのスタティックマッピングは不要です。IPsec トンネルエンドポイントは仮想インターフェイスに関連付けられます。仮想インターフェイスを他のインターフェイスと同様に使用して、スタティックおよびダイナミック ルーティング ポリシーを適用できます。

ポリシーベースの VPN の代わりに、VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。VTI ではスタティックまたはダイナミックルートが使用されます。デバイスは、トンネルインターフェイスとの間のトラフィックを暗号化または復号し、ルーティングテーブルに従って転送します。展開が用意になり、ダイナミック ルーティング プロトコルのルートベースの VPN をサポートする VTI があると、仮想プライベートクラウドの多くの要件も満たせます。Firewall Management Center を使用すると、暗号マップベースの VPN の設定を VTI ベースの VPN に簡単に移行できます

サイト間 VPN ウィザードを使用して、静的またはダイナミック VTI でルートベース VPN を構成できます。トラフィックは、スタティックルート、BGP、OSPFv2/v3、または EIGRP を使用して暗号化されます。

ルーテッド セキュリティ ゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネルを介して復号されたトラフィック制御のアクセス制御ルールを定義できます。

VTI ベースの VPN は、次の間で作成できます。

- 2 つの Firewall Threat Defense デバイス。
- Firewall Threat Defense とパブリッククラウド。
- サービスプロバイダーの冗長性を備えた Firewall Threat Defense と別の Firewall Threat Defense
- VTI インターフェイスが設定されている Firewall Threat Defense およびその他のデバイス
- ポリシーベースの VPN 構成を持つ Firewall Threat Defense およびその他のデバイス

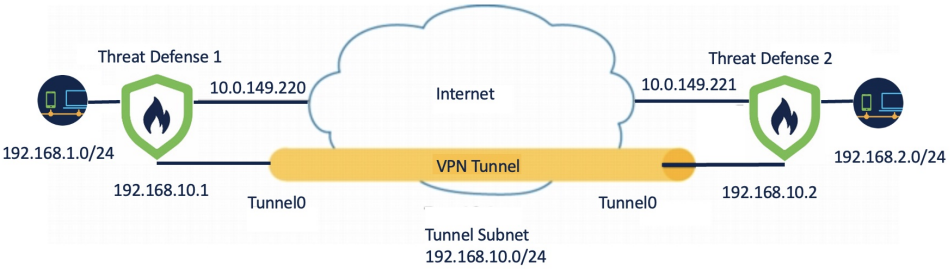
スタティック VTI とダイナミック VTI という 2 つのタイプの VTI インターフェイスが存在します。

詳細については、スタティック VTI （25 ページ） およびDynamic VTI （27 ページ）を参照してください。

スタティック VTI

スタティック VTI は、トンネルインターフェイスを使用して、2 つのサイト間で常時接続のトンネルを作成します。スタティック VTI のトンネル送信元として、物理インターフェイスを定義する必要があります。デバイスごとに最大 1024 の VTI を関連づけることができます。Management Center でスタティック VTI インターフェイスを作成する場合は、VTI インターフェイスの追加 （34 ページ）を参照してください。

以下の図に、スタティック VTI を使用した VPN トポロジを示します。



Threat Defense 1 の場合：

- スタティック VTI の IP アドレス：192.168.10.1
- トンネルの送信元：10.0.149.220
- トンネルの宛先：10.0.149.221

Threat Defense 2 の場合：

- スタティック VTI の IP アドレス：192.168.10.2
- トンネルの送信元：10.0.149.221
- トンネルの宛先：10.0.149.220

利点

- 設定を最小限に抑えて簡素化します。

  クリプト マップ アクセス リストのすべてのリモートサブネットを追跡し、複雑なアクセスリストまたはクリプトマップを設定する必要はありません。

- ルーティング可能なインターフェイスを提供します。

  BGP、EIGRP、OSPFv2/v3 などの IP ルーティングプロトコルと、スタティックルートをサポートします。

- バックアップ VPN トンネルのサポート
- ECMP を使用したロード バランシングをサポートします。
- 仮想ルータをサポートします。
- VPN トラフィックに差別化したアクセス制御を提供します。

  セキュリティゾーンを使用して VTI を設定し、AC ポリシーで使用できます。この設定は以下を可能にします。

  - VPN トラフィックをクリアテキストトラフィックから分類および差別化し、VPN トラフィックを選択的に許可できます。

- 異なる VPN トンネル間の VPN トラフィックに差別化したアクセス制御を提供します。

Dynamic VTI

ダイナミック VTI では、IPsec インターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。

利点

- 設定を最小限に抑えて簡素化します。

  複雑なアクセスリストやクリプトマップを設定する必要はありません。

- 管理を簡素化します。
  - 大規模な企業のハブアンドスポーク展開で、ピア設定を容易に管理できます。
  - スポークごとに 1 つの静的 VTI を設定するのではなく、複数のスポークに 1 つのダイナミック VTI のみを使用します。
- ルーティング可能なインターフェイスを提供します。

  BGP、EIGRP、OSPFv2/v3 などの IP ルーティングプロトコルと、 スタティックルートをサポートします。

- スケーリングの簡素化

  新しいスポークを追加しても、ハブで追加の VPN 設定を行う必要はありません。設定によっては、NAT およびルーティングの設定の更新が必要になる場合があります。

- バックアップ VPN トンネルをサポートします。
- ダイナミックスポークをサポートします。

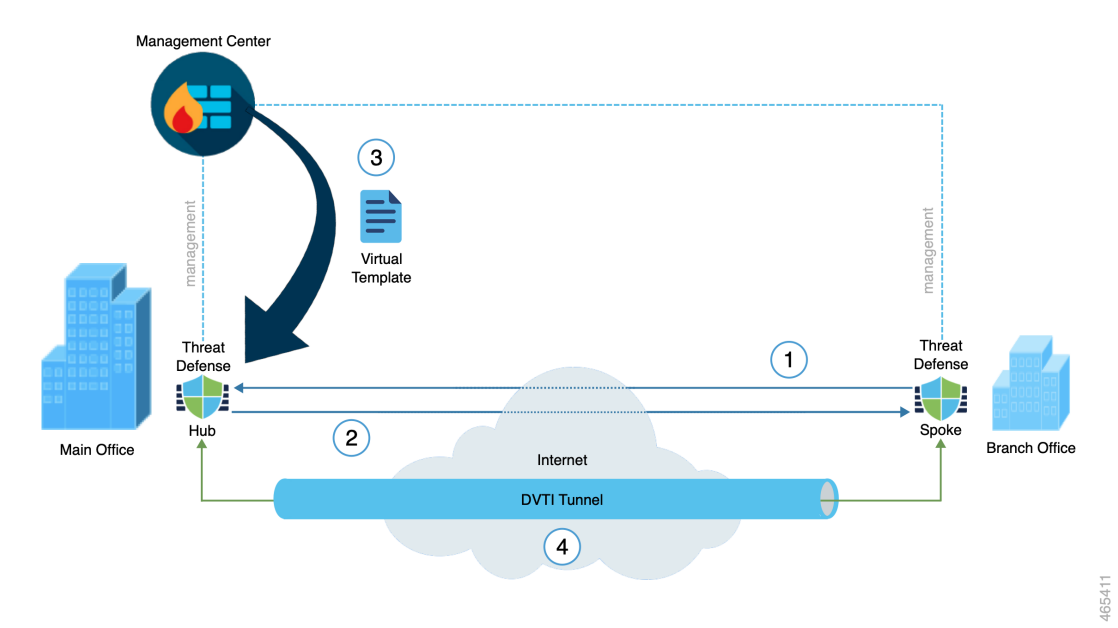
  スポークの DHCP IP アドレス変更のためにハブ設定を更新する必要はありません。

- IP アドレスを節約します。
  - IP のアンナンバード インターフェイス機能を使用して、別の物理インターフェイスまたはループバック インターフェイスから IP アドレスを借用します。
  - ダイナミック VTI に関連付けられているすべての仮想アクセスインターフェイスは、同じ IP アドレスを使用します。
- 仮想ルータをサポートします。
- VPN トラフィックに差別化したアクセス制御を提供します。

セキュリティゾーンを使用して VTI を設定し、AC ポリシーで使用できます。この設定は以下を可能にします。

- VPN トラフィックをクリアテキストトラフィックから分類および差別化し、VPN トラフィックを選択的に許可できます。
- 異なる VPN トンネル間の VPN トラフィックに差別化したアクセス制御を提供します。

Firewall Management Center による VPN セッションのダイナミック VTI トンネルの作成方法



スポークがハブとのトンネル要求を開始する場合

1. スポークが VPN 接続のためにハブとの IKE 交換を開始します。
2. ハブがスポークを認証します。
3. Firewall Management Center がスポークのハブにダイナミック仮想テンプレートを割り当てます。

   仮想テンプレートにより、ハブの仮想アクセスインターフェイスが動的に生成されます。このインターフェイスは、スポークとの VPN セッションに固有です。
4. ハブが仮想アクセスインターフェイスを使用して、スポークとのダイナミック VTI トンネルを確立します。
   1. ハブアンドスポークでは、以下を使用して、トンネルを介してトラフィックが交換されます。
      - IKE 交換を介してスポークによって提案された特定のトラフィック。
      - IPsec 経由の BGP/OSPF/EIRGP プロトコル。

2. VPN セッションが終了すると、トンネルは切断され、ハブは対応する仮想アクセスインターフェイスを削除します。

Firewall Management Center でダイナミック VTI インターフェイスを作成するには、VTI インターフェイスの追加 （34 ページ）を参照してください。

ダイナミック VTI を使用してルートベースのサイト間 VPN を設定するには、ルートベースのサイト間 VPN のダイナミック VTI の設定 （52 ページ）を参照してください。

仮想ルータとダイナミック VTI

仮想ルータを作成し、作成した仮想ルータにダイナミック VTI を関連付けて、ネットワーク内のダイナミック VTI の機能を拡張できます。ダイナミック VTI は、グローバルまたはユーザー定義の仮想ルータに関連付けることができます。ダイナミック VTI は、1 つの仮想ルータにのみ割り当てることができます。

以下と関連付けられた仮想ルータ：

- ダイナミック VTI は、屋内 VRF（IVRF）と呼ばれます。
- トンネル送信元インターフェイスは、Front Door VRF（FVRF）と呼ばれます。

ダイナミック VTI および対応する保護されたネットワークインターフェイスは、同じ仮想ルータの一部である必要があり、借用 IP インターフェイスとダイナミック VTI を同じ仮想ルータにマッピングする必要があります。トンネル送信元インターフェイスは、複数の仮想ルータの一部にできます。

ルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを構成する場合は、ダイナミック VTI を使用した仮想ルータの設定方法 （52 ページ）を参照してください。

構成例の詳細については、ダイナミック VTI を使用したサイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法を参照してください。

仮想トンネルインターフェイスのガイドラインと制限事項

IPv6 のサポート

- VTI は IPv6 をサポートしています。
- トンネル送信元インターフェイスに IPv6 アドレスを使用でき、同じアドレスをトンネルエンドポイントとして使用できます。
- Firewall Management Center は、パブリック IP バージョンを介した VTI IP（または内部ネットワーク IP バージョン）の次の組み合わせをサポートしています。
  - IPv6 over IPv6

- IPv4 over IPv6
- IPv4 over IPv4
- IPv6 over IPv4

- VTI は、トンネルの送信元および宛先として静的および動的 IPv6 アドレスをサポートしています。
- トンネル送信元インターフェイスには IPv6 アドレスを設定でき、トンネルエンド ポイント アドレスを指定できます。このアドレスを指定しない場合、デフォルトでは、Firewall Threat Defense はリスト内の最初の IPv6 グローバルアドレスをトンネルエンドポイントとして使用します。

BGP IPv6 のサポート

VTI は IPv6 BGP をサポートしています。

EIGRP IPv4 のサポート

VTI は IPv4 EIGRP をサポートしています。

OSPFv2 および OSPFv3 IPv6/IPv4 のサポート

VTI は、IPv4 および IPv6 OSPF をサポートしています。

ECMP サポート

- アプリケーション トラフィックのロード バランシングを行うために、ECMP ゾーンでスポークのスタティック VTI を設定します。ECMP ゾーンを設定しない場合、残りのパスは、プライマリパスがダウンしたときにバックアップパスとして機能します。

マルチインスタンスおよびクラスタリング

- VTI は複数のインスタンスでサポートされています。
- VTI はクラスタリングではサポートされていません。

ファイアウォールモード

VTI はルーテッドモードのみでサポートされています。

スタティック VTI の制限事項

- 20 個の一意の IPSec プロファイルのみがサポートされます。
- ルートベースのルーティングでは、VTI を出力インターフェイスとしてのみ設定できます。

ダイナミック VTI の制限事項

- ダイナミック VTI は以下をサポートしていません。
  - ECMP
  - マルチインスタンスの VRF
  - クラスタリング
  - IKEv1
  - QoS
- スポークに動的 IP アドレスがあり、ハブに NAT の背後のダイナミック VTI がある場合、トンネルステータスは不明になります。
- ダイナミックエクストラネットの場合、複数のスポークが接続を確立すると、サイト間監視ダッシュボードに個々のトンネルが表示されません。
- ダイナミックスポークのある NAT の背後にダイナミック VTI を使用してハブを設定すると、VPN モニタリングデータが不正確になります。

スタティックおよびダイナミック VTI の設定時の一般的な注意事項

- サイト間 VPN でダイナミッククリプトマップとダイナミック VTI を使用する場合は、ダイナミック VTI トンネルのみが起動します。この動作は、クリプトマップとダイナミック VTI の両方がデフォルトのトンネルグループを使用しようとするために発生します。

  次のいずれかを実行することを推奨します。
  - サイト間 VPN をダイナミック VTI に移行します。
  - 独自のトンネルグループを持つ静的クリプトマップを使用します。
- VTI は IPsec モードのみで設定可能です。
- Management Center では、ダイナミック VTI はハブアンドスポークトポロジのみをサポートします。
- ダイナミック VTI は、バージョン 7.3 以降の Threat Defense デバイスのみをサポートしています。
- ルートベースのハブアンドスポークトポロジには、1 つのハブだけを設定することをお勧めします。一組のスポークに対して複数のハブを持ち、1 つのハブをバックアップハブとして使用するトポロジを設定するには、単一のハブと同じ一組のスポークを持つ複数のトポロジを設定します。詳細については、ルートベースの VPN での複数ハブの設定 （45 ページ）を参照してください。
- トンネルインターフェイスを使用するトラフィックには、静的、BGP、EIGRP IPv4、OSPFv2/v3 ルートを使用できます。

- ダイナミックルーティングを使用したHA構成では、これらのトンネルはアクティブなIPアドレスを使用して作成されるため、スタンバイデバイスはVTIトンネルを介して既知のサブネットにアクセスできません。
- デバイスには最大 1024 のスタティックおよびダイナミック VTI を設定できます。VTI 数を計算する際は、次の点を考慮してください。
  - nameifサブインターフェイスを含めて、デバイスに設定できるVTIの総数を導き出します。
  - ポートチャネルのメンバーインターフェイスにnameifを設定することはできません。したがって、トンネル数は実際のメイン ポートチャネル インターフェイスの数だけ減少し、そのメンバーインターフェイスの数は減少しません。
  - プラットフォームでの VTI の数は、そのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、Firepower 1120 は 512 個の VLAN をサポートしているため、トンネル数は512から設定された物理インターフェイスの数を引いた数になります。
- 高可用性設定でデバイスに 400 個を超える VTI を設定する場合は、Firewall Threat Defense HA のユニットの保留時間として 45 秒を設定する必要があります。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。
- ダイナミックVTIの場合、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。トンネル送信元インターフェイスを指定しない場合、仮想アクセスインターフェイスは、Threat Defense が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。
- スタティック VTI は IKE のバージョン v1 および v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- ダイナミック VTI は IKE のバージョン v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- スタティックおよびダイナミックVTIの場合は、借用IPインターフェイスをVTIインターフェイスのトンネルソース IP アドレスとして使用しないでください。
- スタティックまたはダイナミックVTIインターフェイスを使用してルートベースのサイト間 VPN を設定する際に、 BGP を使用している場合は、TTL ホップの値が 2 以上であることを確認してください。
- NAT を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- IKE および IPsec のセキュリティ アソシエーションには、トンネル内のデータ トラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。
- トンネルグループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。

- LAN-to-LAN トンネルグループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブモードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。
- 暗号マップに設定されるピアアドレスと VTI のトンネル宛先が異なる場合、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- デフォルトでは、VTI を経由して送信されるすべてのトラフィックは暗号化されます。
- VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセスルールを適用することができます。
- VTI インターフェイスを ECMP ゾーンに関連付け、ECMP スタティックルートを設定して、次のことを実現できます。
  - ロードバランシング（アクティブ-アクティブ VTI）：任意の並列 VTI トンネルを介して接続を送ることができます。
  - シームレスな接続移行：VTI トンネルが到達不能になると、フローは同じゾーンで設定されている別の VTI インターフェイスにシームレスに移行されます。
  - 非対称ルーティング：ある VTI インターフェイスを介したトラフィックフローを転送し、別の VTI インターフェイスを介したリバーストラフィックフローを設定します。

  ECMP の設定については、等コストスタティックルートの設定を参照してください。
- ルートベースの VPN の場合、復号されたトラフィックのバイパス アクセス コントロール ポリシー（**sysopt connection permit-vpn**）は機能しません。ルートベースの VPN トラフィックを許可するには、アクセス制御ルールを設定する必要があります。

バックアップ VTI の注意事項と制約事項

- トンネルフェールオーバー全体のフローの復元力はサポートされていません。たとえば、トンネルフェールオーバー後にクリアテキストの TCP 接続が失われ、フェールオーバー中に行われた FTP 転送を再開始する必要があります。
- バックアップ VTI では、証明書認証はサポートされていません。

ダイナミック VTI と仮想ルータに関する注意事項

- ダイナミック VTI および対応する保護されたネットワーク インターフェイスは、同じ仮想ルータの一部である必要があります。
- 借用 IP インターフェイスとダイナミック VTI を同じ仮想ルータにマッピングする必要があります。
- ユーザー定義の仮想ルータは、BGPv4/v6 および OSPFv2 ルーティングプロトコルのみをサポートします。
- トンネル送信元インターフェイスは、ダイナミック VTI に関連付けられているものとは異なるユーザー定義の仮想ルータにある可能性があります。

関連トピック

ループバック インターフェイスのガイドラインと制限事項
ルートベースのサイト間 VPN の作成 （36 ページ）

VTI インターフェイスの追加

ルートベースのサイト間VPNを設定するには、VTIトンネルの両方のノードでデバイスにVTIインターフェイスを作成する必要があります。

トンネルタイプを「ダイナミック」として指定し、関連パラメータを設定すると、Firewall Management Centerはダイナミック仮想テンプレートを生成します。仮想テンプレートは、VPNセッションごとに固有の仮想アクセスインターフェイスを動的に生成します。

始める前に

スタティックおよびダイナミック VTI VPN トンネルの冗長性のためにループバック インターフェイスを設定します。詳細については、ループバック インターフェイスの設定を参照してください。

Cisco Secure Firewall 1200、Secure Firewall 3100 または Secure Firewall 4200 デバイスの場合、IPsec フローオフロードは、デバイスの VTI ループバック インターフェイスが有効になっている場合にも使用されます。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 VTI インターフェイスを作成するデバイスの横にある**編集**アイコンをクリックします。

ステップ 3 [インターフェイスの追加（Add Interfaces）] > [仮想トンネルインターフェイス（Virtual Tunnel Interface）] を選択します。

ステップ 4 [トンネルタイプ（Tunnel Type）] として [スタティック（Static）] または [ダイナミック（Dynamic）] を選択します。

ステップ 5 インターフェイスの名前と説明を入力します。デフォルトでは、インターフェイスはイネーブルになっています。

28 文字以下の名前を指定してください。

ステップ 6 （任意）[セキュリティゾーン（Security Zone）] ドロップダウンメニューからセキュリティゾーンを選択して、そのゾーンにスタティック VTI インターフェイスまたはダイナミック VTI インターフェイスを追加します。

セキュリティゾーンに基づいてトラフィック検査を実行する場合は、VTIをセキュリティゾーンに追加し、アクセスコントロール（AC）ルールを設定します。トンネルを介したVPNトラフィックを許可するには、このセキュリティゾーンをソースゾーンとして使用するACルールを追加する必要があります。

ステップ 7 **[優先順位（Priority）]** フィールドに、複数の VTI 間でトラフィックのロードバランシングを行うための優先順位を入力します。

指定できる範囲は 0 ～ 65535 です。最も小さい番号が最も高い優先順位になります。このオプションは、ダイナミック VTI には適用されません。

ステップ 8 トンネルタイプに応じて、次のいずれかを実行します。

- ダイナミック VTI の場合は、[テンプレートID（Template ID）] フィールドに 1 ～ 10413 の範囲で一意の ID を入力します。
- スタティック VTI の場合は、[トンネル ID（Tunnel ID）] フィールドに 1 ～ 10413 の範囲で一意のトンネル ID を入力します。

ステップ 9 （ダイナミック VTI の場合は任意）[トンネル送信元（Tunnel Source）] ドロップダウンリストからトンネル送信元インターフェイスを選択します。

VPN トンネルは、このインターフェイス（物理インターフェイスまたはループバック インターフェイス）で終端します。ドロップダウンリストからインターフェイスの IP アドレスを選択します。IPSec トンネルモードに関係なく IP アドレスを選択できます。IPv6 アドレスが複数ある場合は、トンネルエンドポイントとして使用するアドレスを選択します。

ステップ 10 [IPSecトンネルモード（IPSec Tunnel Mode）] で、[IPv4] または [IPv6] オプションボタンをクリックして、IPSec トンネルを通過するトラフィックのタイプを指定します。

ステップ 11 [IPアドレス（IP Address）] で、次の手順を実行します。

- [IPの設定（Configure IP）]：スタティック VTI インターフェイスの IPv4 アドレスまたは IPv6 アドレスを入力します。ダイナミック VTI インターフェイスの IP アドレスは設定できません。ダイナミック VTI インターフェイスについては、[IP の借用（Borrow IP）] フィールドを使用します。
- [IPの借用（IP アンナンバード）（Borrow IP (IP unnumbered)）]：ドロップダウンリストから物理インターフェイスまたはループバック インターフェイスを選択します。VTI インターフェイスはこの IP アドレスを継承します。

  トンネル送信元 IP アドレスとは異なる IP アドレスを使用していることを確認してください。このオプションは、スタティック VTI インターフェイスまたはダイナミック VTI インターフェイスに使用できます。

  Add ＋ をクリックしてループバック インターフェイスを設定します。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバックインターフェイスに割り当てられたIPアドレスを使用してすべてのインターフェイスにアクセスできます。

ステップ 12 [OK] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

ルートベースのサイト間 VPN の作成

次の 2 つのトポロジに対してルートベースのサイト間 VPN を設定できます。

- [ポイントツーポイント（Point to Point）]：トンネルの両方のノードで VTI を設定し、ウィザードを使用して VPN を設定します。
- [ハブおよびスポーク（Hub and Spoke）]：ハブとスポークで VTI を設定します。ハブをダイナミック VTI で設定し、スポークを静的 VTI で設定します。

エクストラネットデバイスをハブとして設定し、管理対象デバイスをスポークとして設定することができます。複数のハブとスポークを設定でき、バックアップのハブとスポークも設定できます。

- エクストラネットのハブとスポークの場合、複数の IP をバックアップとして設定できます。
- 管理対象スポークの場合、プライマリ VTI インターフェイスとともにバックアップのスタティック VTI インターフェイスを設定できます。

VTI の詳細については、仮想トンネル インターフェイスについて （25 ページ）を参照してください

（注） VTI へのすべての言及は、明記されていないかぎり、スタティック VTI とダイナミック VTI を表します。

手順

ステップ 1 **Devices** > **VPN** > **Site to Site** を選択し、**[追加（Add）]** をクリックしします。

ステップ 2 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 3 [ルートベース（VTI）（Route Based (VTI)）] を選択し、次のいずれかを実行します。

- ネットワークトポロジとして [ポイントツーポイント（Point to Point）] を選択します。ルートベースの「ポイントツーポイント」トポロジのエンドポイントを設定するには、ポイントツーポイント トポロジのエンドポイントの設定 （37 ページ）を参照してください。
- ネットワークトポロジとして [ハブアンドスポーク（Hub and Spoke）] を選択します。ルートベースの「ハブアンドスポーク」トポロジのエンドポイントを設定するには、ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）を参照してください。

ステップ 4 [作成（Create）] をクリックします。

ステップ 5 （任意） Firewall Threat Defense VPN IKE オプション （14 ページ）の説明に従って、展開の [IKE] オプションを指定します。

ステップ 6 （任意） Firewall Threat Defense VPN IPsec オプション （17 ページ）の説明に従って、展開の [IPsec] オプションを指定します。

ステップ 7 （任意） Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （20 ページ）の説明に従って、展開の [詳細（Advanced）] オプションを指定します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

両方のデバイスで VTI インターフェイスと VTI トンネルを設定したら、次のものを設定する必要があります。

- VTI トンネルを介してデバイス間で VTI トラフィックをルーティングするルーティングポリシー。詳細については、VTI のルーティングおよび AC ポリシーの設定 （53 ページ）を参照してください。
- 暗号化されたトラフィックを許可するアクセスコントロールルール。[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

ポイントツーポイント トポロジのエンドポイントの設定

ポイントツーポイント トポロジ ノードのルートベースのサイト間 VPN のエンドポイントを設定するには、次のパラメータを設定します。

始める前に

ルートベースのサイト間 VPN の作成 （36 ページ）の説明に従って、ルートベース VPN のポイントツーポイント トポロジの基本パラメータを設定し、[エンドポイント（Endpoints）] タブをクリックします。

手順

ステップ 1 [ノードA（Node A）] の [デバイス（Device）] ドロップダウンメニューで、VTI トンネルの最初のエンドポイントとして使用する登録済みデバイス（Firewall Threat Defense）またはエクストラネットの名前を選択します。

エクストラネットピアの場合は、次のパラメータを指定します。

1. デバイスの名前を指定します。
2. [エンドポイントのIPアドレス（Endpoint IP address）] フィールドに、プライマリ IP アドレスを入力します。バックアップ VTI を設定している場合は、カンマを追加して、バックアップ IP アドレスを指定します。
3. [OK] をクリックします。

エクストラネットハブに対する前述のパラメータを設定後、[IKE] タブでエクストラネットの事前共有キーを指定します。

（注）
AWS VPC には、デフォルトのポリシーとして **AES-GCM-NULL-SHA-LATEST** があります。リモートピアが AWS VPC に接続する場合は、[ポリシー（Policy）] ドロップダウンリストから [AES-GCM-NULL-SHA-LATEST] を選択して、AWS のデフォルト値を変更せずに VPN 接続を確立します。

ステップ 2 登録済みデバイスの場合、[仮想トンネルインターフェイス（Virtual Tunnel Interface）] ドロップダウンリストからノード A の VTI インターフェイスを指定できます。

選択したトンネルインターフェイスはノード A の送信元インターフェイスであり、ノード B のトンネルの宛先です。

ノード A に新しいインターフェイスを作成する場合は、Add ＋アイコンをクリックして、VTI インターフェイスの追加 （34 ページ） の説明に従ってフィールドを設定します。

既存の VTI の設定を編集する場合は、[仮想トンネルインターフェイス（Virtual Tunnel Interface）] ドロップダウンフィールドで VTI を選択し、[VTIの編集（Edit VTI）] をクリックします。

ステップ 3 ノード A デバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェックボックスをオンにします。[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドに、トンネル送信元のパブリック IP アドレスを入力します。

ステップ 4 [ピアへのローカルIDの送信（Send Local Identity to Peers）]：ローカル ID 情報をピアデバイスに送信するには、このオプションを選択します。リストから次のいずれかの [ローカルID構成（Local Identity Configuration）] を選択し、ローカル ID を設定します。

- [IPアドレス（IP address）]：ID にインターフェイスの IP アドレスを使用します。
- [自動（Auto）]：事前共有キーにはIPアドレスを使用し、証明書ベースの接続には証明書 DN を使用します。
- [電子メールID（Email ID）]：ID に使用する電子メール ID を指定します。電子メール ID は最大 127 文字です。
- [ホスト名（Hostname）]：完全修飾ホスト名を使用します。
- [キーID（Key ID）]：ID に使用するキー ID を指定します。キー ID は 65 文字未満にする必要があります。

ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。一意の ID を指定すると、Cisco Umbrella Secure Internet Gateway（SIG）に接続するために、Firewall Threat Defense が NAT の背後に複数の IPsec トンネルを持つことができます。

Cisco Umbrella での一意のトンネル ID の設定については、**Cisco Umbrella SIG ユーザーガイド** [英語] を参照してください。

ステップ 5 （任意）[バックアップVTIの追加（Add Backup VTI）] をクリックして、追加の VTI をバックアップ インターフェイスとして指定し、パラメータを設定します。

（注）
トポロジの両方のピアで、バックアップVTIに対して同じトンネル送信元が設定されていないことを確認します。デバイスに、同じトンネル送信元とトンネル宛先を持つ2つのVTIは設定できないため、一意のトンネル送信元とトンネル宛先の組み合わせを設定します。

仮想トンネルインターフェイスはバックアップVTIで指定されますが、どちらのトンネルがプライマリまたはバックアップとして使用されるかは、ルーティング設定によって決まります。

ステップ 6 [追加の設定（Additional Configuration）] で、次の手順を実行します。

- [ルーティングポリシー（Routing Policy）] をクリックします。Firewall Management Center で**[デバイス（Devices）]** > **[ルーティング（Routing）]** ページが表示されます。

  VPN トラフィックのスタティックルーティング、BGP、OSPF v2/v3、または EIGRP ルーティングを設定できます。

- VPN トラフィックを許可するには、[ACポリシー（AC Policy）] をクリックします。Firewall Management Center でデバイスのアクセス コントロール ポリシー ページが表示されます。VTI のセキュリティゾーンを指定する、許可/ブロックルールの追加に進みます。バックアップ VTI を設定している場合は、プライマリ VTI と同じセキュリティゾーンへのバックアップトンネルが含まれていることを確認します。AC ポリシーページのバックアップ VTI に特定の設定は必要ありません。

ステップ 7 [詳細設定（Advance Settings）] を展開して、デバイスの追加構成を設定します。詳細については、ルートベース VPN のポイントツーポイント トポロジの詳細設定 （40 ページ）を参照してください。

ステップ 8 ノード B に対して上記の手順を繰り返します。

ステップ 9 [OK] をクリックします。

次のタスク

- （任意）Firewall Threat Defense VPN IKE オプション （14 ページ）の説明に従って、展開の [IKE] オプションを指定します。
- （任意）Firewall Threat Defense VPN IPsec オプション （17 ページ）の説明に従って、展開の [IPsec] オプションを指定します。
- （任意）Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （20 ページ）の説明に従って、展開の [詳細（Advanced）] オプションを指定します。
- [保存（Save）] をクリックします。
- トラフィックを VTI にルーティングするには、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、Threat Defense デバイスを編集して、[ルーティング（Routing）] タブをクリックします。

VPN トラフィックのルーティングには、スタティックルートを設定したり、BGP、OSPF v2/v3、または EIGRP を使用したりできます。

- VPN トラフィックを許可するには、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。 。VTI のセキュリティゾーンを指定するルールを追加します。バックアップ VTI の場合は、プライマリ VTI と同じセキュリティゾーンにバックアップ VTI が含まれていることを確認します。

ルートベース VPN のポイントツーポイント トポロジの詳細設定

ルートベース VPN のポイントツーポイント トポロジに対して、次の詳細な設定を設定します。

始める前に

ポイントツーポイント トポロジのエンドポイントの設定 （37 ページ）の説明に従って、ルートベースの VPN でポイントツーポイント トポロジの基本パラメータを設定し、[詳細設定（Advance Settings）] を展開します。

手順

ステップ 1 [ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにして、VTI IP アドレスをピアデバイスに送信します。

ステップ 2 [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、スポークおよびピアからの着信 IKEv2 ルートを許可します。

ステップ 3 [接続タイプ（Connection Type）] ドロップダウンリストから、次のいずれかを選択します。

[応答のみ （Answer Only）] : デバイスは、ピアデバイスが接続を開始したときにのみ応答でき、接続は開始できません。

[双方向（Bidirectional）] : デバイスは接続を開始または応答できます。これがデフォルトのオプションです。

ハブアンドスポークトポロジのエンドポイントの設定

ダイナミック VTI を使用して、ハブアンドスポークトポロジ専用のルートベースのサイト間 VPN を作成できます。ハブはダイナミック VTI のみを使用でき、スポークはスタティック VTI インターフェイスのみを使用できます。エクストラネットデバイスをハブとして構成することもできます。

ハブ アンド スポーク トポロジ ノードのルートベースのサイト間 VPN のエンドポイントを設定するには、次のパラメータを設定します。

始める前に

ルートベースのサイト間 VPN の作成 （36 ページ）の説明に従って、ルートベース VPN のハブアンドスポークトポロジの基本パラメータを設定し、[エンドポイント（Endpoints）] タブをクリックします。

手順

ステップ 1 [ハブノード（Hub Nodes）]の下で、次の手順を実行します。

a) Add ＋ をクリックして、**[エンドポイントの追加（Add Endpoint）]** ダイアログボックスでハブ ノードを設定します。

b) [デバイス（Device）] ドロップダウンリストからハブを選択します。

エクストラネットハブの場合は、次のパラメータを指定します。

1. デバイスの名前を入力します。
2. プライマリ IP アドレスを入力します。バックアップ VTI を設定している場合は、カンマを追加して、バックアップ IP アドレスを指定します。
3. [OK] をクリックします。

エクストラネットハブに対する前述のパラメータを設定後、[IKE] タブでエクストラネットの事前共有キーを指定します。

（注）
AWS VPC には、デフォルトのポリシーとして **AES-GCM-NULL-SHA-LATEST** があります。リモートピアが AWS VPC に接続する場合は、[ポリシー（Policy）] ドロップダウンリストから [AES-GCM-NULL-SHA-LATEST] を選択して、AWS のデフォルト値を変更せずに VPN 接続を確立します。

c) [ダイナミック仮想トンネルインターフェイス（Dynamic Virtual Tunnel Interface）] ドロップダウンリストからダイナミック VTI を選択します。

ダイナミック VTI にはトンネルソースの設定が必須です。これは、Management Center ではスポークのトンネル宛先を決定するためにこの情報を必要になるためです。

Add ＋ をクリックして、新しいダイナミック VTI を追加します。ループバック インターフェイスから動的インターフェイスの借用 IP を設定することをお勧めします。

既存のダイナミック VTI を編集する場合は、インターフェイスを選択して、[VTIの編集（Edit VTI）] をクリックします。

d) （オプション）エンドポイントデバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェック ボックスをオンにして、[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドでトンネル送信元の IP アドレスを設定します。

e) [ルーティングポリシー（Routing Policy）] をクリックして、ハブのルーティングポリシーを設定します。

f) [ACポリシー（AC Policy）] をクリックして、アクセス コントロール ポリシーを設定します。

g) [詳細設定（Advance Settings）] を展開して、ハブの追加構成を設定します。詳細については、ルートベースの VPN のハブアンドスポークに対する詳細設定 （44 ページ）を参照してください。

h) [OK] をクリックします。

ステップ 2 [スポークノード（Spoke Nodes）] の下で、次の手順を実行します。

a) Add ＋ をクリックして、**[エンドポイントの追加（Add Endpoint）]** ダイアログボックスでスポークを設定します。

b) [デバイス（Device）] ドロップダウンリストからスポークを選択します。

エクストラネットスポークの場合は、次のパラメータを指定します。

1. デバイスの名前を入力します。
2. [エンドポイントIPアドレス（Endpoint IP Address）] で、次のいずれかを選択します。
   - [静的（Static）]：デバイスの IP アドレスと、必要に応じてバックアップ IP アドレスを入力します。
   - [動的（Dynamic）]：エクストラネットスポークの IP アドレスを動的に割り当てるには、このオプションを選択します。
3. [OK] をクリックします。

c) [スタティック仮想トンネルインターフェイス（Static Virtual Tunnel Interface）] ドロップダウンリストからスタティック VTI を選択します。

Add ＋ をクリックして、新しいスタティック VTI を追加します。スタティック VTI のトンネル IP は自動入力されます。この IP アドレスがスポークに対して一意であることを確認してください。

既存のスタティック VTI を編集する場合は、インターフェイスを選択して、[VTIの編集（Edit VTI）] をクリックします。

d) （オプション）エンドポイントデバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェックボックスをオンにします。Management Center では、スポークにトンネル宛先 IP アドレスを設定するために、トンネルの送信元インターフェイスアドレスが必要です。[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドに、トンネル送信元のパブリック IP アドレスを入力します。

e) （オプション）[ピアへのローカルIDの送信（Send Local Identity to Peers）]：ローカル ID 情報をピアデバイスに送信するには、このチェックボックスをオンにします。[ローカルID設定（Local Identity Configuration）] ドロップダウンリストから次のいずれかのパラメータを選択し、ローカル ID を設定します。

- [IPアドレス（IP address）]：ID にインターフェイスの IP アドレスを使用します。

- [自動（Auto）]：事前共有キーには IP アドレスを使用し、証明書ベースの接続には証明書 DN を使用します。
- [電子メールID（Email ID）]：ID に使用する電子メール ID を指定します。電子メール ID は最大 127 文字です。
- [ホスト名（Hostname）]：完全修飾ホスト名を使用します。
- [キーID（Key ID）]：ID に使用するキー ID を指定します。キー ID は 65 文字未満にする必要があります。

ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。一意の ID を設定すると、Cisco Umbrella Secure Internet Gateway（SIG）に接続するために、Firewall Threat Defense が NAT の背後に複数の IPsec トンネルを持つことができます。

Cisco Umbrella での一意のトンネル ID の設定については、*Cisco Umbrella SIG* ユーザーガイド [英語] を参照してください。

f) （オプション）[バックアップVTIの追加（Add Backup VTI）] をクリックして、追加の VTI インターフェイスをバックアップ インターフェイスとして指定します。

（注）
トポロジの両方のピアで、同じトンネル送信元にバックアップ VTI が設定されていないことを確認します。たとえば、ピア A で 1 つのトンネル送信元インターフェイス（10.10.10.1/30 など）を使用して 2 つの VTI（プライマリとバックアップ）が設定されている場合は、ピア B でも 1 つのトンネル送信元 IP（20.20.20.1/30 など）を使用して 2 つの VTI を設定することはできません。

仮想トンネルインターフェイスはバックアップ VTI で指定されますが、どちらのトンネルがプライマリまたはバックアップとして使用されるかは、ルーティング設定によって決まります。

g) [ルーティングポリシー（Routing Policy）] をクリックして、スポークのルーティングポリシーを設定します。

h) [ACポリシー（AC Policy）] をクリックして、アクセス コントロール ポリシーを設定します。

i) [詳細設定（Advance Settings）] を展開して、スポークの追加構成を設定します。詳細については、ルートベースの VPN のハブアンドスポークに対する詳細設定 （44 ページ）を参照してください。

j) [OK] をクリックします。

次のタスク

- （任意）Firewall Threat Defense VPN IKE オプション （14 ページ）の説明に従って、展開の [IKE] オプションを指定します。

- （任意）Firewall Threat Defense VPN IPsec オプション （17 ページ）の説明に従って、展開の [IPsec] オプションを指定します。
- （任意）Firewall Threat Defense のサイト間 VPN 展開の詳細オプション （20 ページ）の説明に従って、展開の [詳細（Advanced）] オプションを指定します。
- [保存（Save）] をクリックします。

ルートベースの VPN のハブアンドスポークに対する詳細設定

ルートベースの VPN のハブアンドスポークに対して、次の詳細設定を構成します。

始める前に

ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）の説明に従って、ルートベースの VPN でハブアンドスポークの基本パラメータを設定し、[詳細設定（Advance Settings）] を展開します。

手順

ステップ 1 [ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにして、VTI IP アドレスをピアデバイスに送信します。

ハブの場合、ルーティングプロトコルとして BGP を使用する場合は、このチェックボックスをオンにする必要があります。この構成により、ループバック IP アドレスが BGP ルーティングテーブルで共有されます。

スポークの場合、このオプションはデフォルトで有効になっています。

ステップ 2 [保護されたネットワーク（Protected Networks）] を追加して、VPN エンドポイントによって保護されるネットワークを定義します。Add＋をクリックして、保護されたネットワークを選択します。

ハブの場合、ハブの背後にある保護されたネットワークを設定します。この情報とスポークの保護されたネットワークにより、スポークアクセスリストが生成されます。

ダイナミック VTI を使用したハブの仮想アクセスインターフェイスのスタティックルートは作成できません。これらのインターフェイスは、トンネルの確立および終了時にハブで動的に作成および削除されます。

スポークの場合、スポークの保護されたネットワークを設定します。

スポークのスタティックルーティングを有効にするには、トポロジのエンドポイントを設定後、[IPsec] タブをクリックし、[リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] チェックボックスをオンにします。

BGP、OSPF、または EIGRP を使用する場合、このオプションは不要です。

ステップ 3 [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、スポークおよびピアからの着信 IKEv2 ルートを許可します。

ハブの場合：IKE交換中、ハブは動的に作成された仮想アクセスインターフェイスをスポークにアドバタイズし、スポークはその VTI IP アドレスをハブにアドバタイズします。

スポークの場合：このオプションはデフォルトで有効になっています。

ステップ 4 [接続タイプ（Connection Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

[応答のみ （Answer Only）]：デバイスは、ピアデバイスが接続を開始したときにのみ応答でき、接続は開始できません。

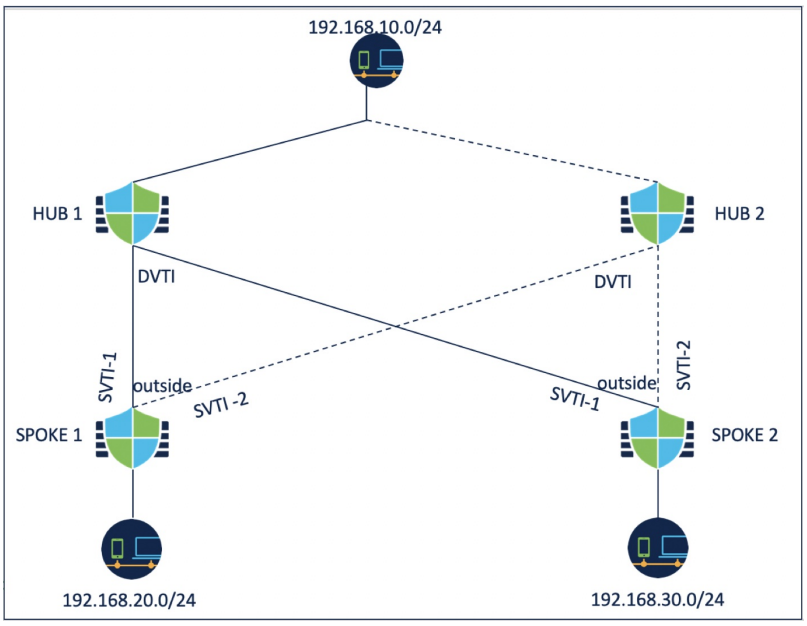
[双方向（Bidirectional）]：デバイスは接続を開始または応答できます。これがデフォルトのオプションです。

ルートベースの VPN での複数ハブの設定

一組のスポークに対して複数のハブを使用するトポロジを設定できます。1 つのハブをバックアップハブとした場合、単独のハブと同じ一組のスポークを持つ複数のトポロジを設定できます。

次の例では、2 つのハブが同じ一組のスポークに接続されています。ハブ 1 はプライマリハブで、ハブ 2 はセカンダリハブです。Firewall Management Center でこのネットワークを設定するには、ルートベースのハブ アンド スポーク トポロジを 2 つ設定する必要があります。

- トポロジ 1：ハブ 1 がスポーク 1 とスポーク 2 に接続されている。
- トポロジ 2：ハブ 2 がスポーク 1 とスポーク 2 に接続されている。



トポロジ 1 を設定するには、次の手順を実行します。

手順

ステップ 1 **Devices** > **VPN** > **Site to Site** を選択し、**[追加（Add）]** をクリックしします。

ステップ 2 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 3 [ルートベース（VTI）（Route Based (VTI)）] を選択し、次のいずれかを実行します。

- ネットワークトポロジとして [ポイントツーポイント（Point to Point）] を選択します。ルートベースの「ポイントツーポイント」トポロジのエンドポイントを設定するには、ポイントツーポイント トポロジのエンドポイントの設定 （37 ページ）を参照してください。
- ネットワークトポロジとして [ハブアンドスポーク（Hub and Spoke）] を選択します。ルートベースの「ハブアンドスポーク」トポロジのエンドポイントを設定するには、ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）を参照してください。

ステップ 4 [作成（Create）] をクリックします。

ステップ 5 IKE バージョンを設定します。

ステップ 6 [エンドポイント（Endpoints）] タブをクリックします。

ステップ 7 [ハブノード（Hub Nodes）]の下で、次の手順を実行します。

a) Add ＋ をクリックしてハブを追加します。

b) [デバイス（Device）] ドロップダウンリストからハブ 1 を選択します。

c) **[ダイナミック仮想トンネル インターフェイス（Dynamic Virtual Tunnel Interface）]** ドロップダウンリストからダイナミック VTI を設定するか、Add ＋ をクリックして新しいダイナミック VTI を追加します。

ループバック インターフェイスから動的インターフェイスの借用 IP を設定することをお勧めします。

d) （オプション）エンドポイントデバイスが NAT デバイスの背後にある場合は、[トンネル送信元IPはプライベートです（Tunnel Source IP is Private）] チェック ボックスをオンにして、[トンネル送信元のパブリックIPアドレス（Tunnel Source Public IP Address）] フィールドでトンネル送信元の IP アドレスを設定します。

e) [ルーティングポリシー（Routing Policy）] をクリックして、ハブのルーティングポリシーを設定します。BGP を使用して動的ルーティングを設定できます。

f) [詳細設定（Advance Settings）] を展開します。ハブの次の詳細設定を構成して、動的ルーティングを使わない場合に使用できる IKEv2 ルーティングを有効にすることができます。

- （オプション）[ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにします。
- ハブの [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、スポークからのルートを許可し、ルーティングテーブルを更新します。
- [接続タイプ（Connection Type）] ではドロップダウンリストから [双方向（Bidirectional）] を選択します。

g) [OK] をクリックします。

ステップ 8 [スポークノード（Spoke Nodes）] の下で、次の手順を実行します。

a) Add ＋ をクリックしてスポークを追加します。

b) [デバイス（Device）] ドロップダウンリストからスポーク 1 を選択します。

c) **[スタティック仮想トンネル インターフェイス（Static Virtual Tunnel Interface）]** ドロップダウンリストからスポークのスタティック VTI として SVTI-1 を選択するか、Add ＋ をクリックして新しいスタティック VTI を追加します。

SVTI-1 のトンネル送信元として外部インターフェイスを選択します。SVTI-1 のトンネル IP は自動入力されます。この IP アドレスが、両方のトポロジのピア間でスポーク 1 に対して一意であることを確認してください。

d) [詳細設定（Advance Settings）] を展開します。動的ルーティングを使用しない場合は、これらの設定を行って、スポークの IKEv2 ルーティングを有効にすることができます。

- [ピアに仮想トンネルインターフェイスIPを送信（Send Virtual Tunnel Interface IP to the peers）] チェックボックスをオンにして、VTI IP アドレスをピアデバイスに送信します。
- [ピアからの着信IKEv2ルートを許可する（Allow incoming IKEv2 routes from the peers）] チェックボックスをオンにして、ピアからの着信 IKEv2 ルートを許可します。
- [接続タイプ（Connection Type）] ではドロップダウンリストから [双方向（Bidirectional）] を選択します。

e) [OK] をクリックします。

f) 手順 5a ～ 5e を繰り返して、スポーク 2 を追加します。SVTI-1 をスポーク 2 のスタティック VTI として設定します。

ステップ 9 必要に応じて IKE および IPSec パラメータを設定するか、デフォルト値を使用します。

次のタスク

1. ハブ 2、スポーク 1、およびスポーク 2 を使用してトポロジ 2 を設定します。

   SVTI-2 をスポーク 1 のスタティック VTI として設定し、SVTI-2 をスポーク 2 のスタティック VTI として設定します（上の図を参照）。SVTI-2 のトンネル送信元は同じ外部インターフェイスとしてください。

2. スポークごとに、ルーティングポリシーを設定します。詳細については、ルートベース VPN での複数ハブのルーティングの設定 （48 ページ）を参照してください。

3. 設定とトンネルのステータスを確認します。詳細については、「ルートベースの VPN での複数ハブ構成の確認 （49 ページ）」を参照してください。

ルートベース VPN での複数ハブのルーティングの設定

次の手順では、ハブとスポークでダイナミックルーティングを設定し、スポークでポリシーベースルーティングを設定する方法について説明します。

始める前に

ルートベースの VPN での複数ハブの設定 （45 ページ）で説明されているように、トポロジ 1 とトポロジ 2 を設定します。

手順

ステップ 1 BGP を使用してハブのダイナミックルーティングを設定します。

a) [デバイス（Device）]>[デバイス管理（Device Management）]>[ルーティング（Routing）] を選択します。
b) 左側のペインで、[一般設定（General Settings）] > [BGP] を選択します。
c) [BGPの有効化（Enable BGP）] チェックボックスをオンにして、**AS 番号**を入力します。

要件に応じて他のフィールドを設定できます。

d) [保存（Save）] をクリックします。
e) 左側のペインで、[BGP] > [IPv4] を選択します。
f) [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。
g) [ネイバー（Neighbor）] タブをクリックし、[追加（Add）] をクリックして、パラメータを設定します。

1. [IPアドレス（IP Address）]：スポーク 1 のトンネルインターフェイス IP アドレスを入力します。
2. [リモートAS（Remote AS）]：スポーク 1 の AS 番号。
3. [アドレスの有効化（Enabled Address）] チェックボックスをオンにします。
4. [OK] をクリックします。

上記の手順を繰り返して、スポーク 2 をネイバーとして追加します。

h) [保存（Save）] をクリックします。
i) [ネットワーク（Networks）] タブをクリックし、[追加（Add）] をクリックして、ハブの背後にあるネットワークをピアにアドバタイズします。

ステップ 2 BGP を使用して、スポークのダイナミックルーティングを設定します。

スポークの BGP 設定は、次の相違点を除いてハブの BGP 設定と似ています。

- ハブ 1 とハブ 2 を両方のスポークのネイバーとして設定し、ハブのトンネルインターフェイス IP アドレスを使用します。
- ネットワークを設定するときは、各スポークの背後にあるネットワークを使用します。

ステップ 3 スポークでポリシーベースルーティングを設定します。

a) 左側のペインで、[ポリシーベースルーティング（Policy Based Routing）] を選択し、[追加（Add）] をクリックします。

b) ドロップダウンリストから [入力インターフェイス（Ingress Interface）] を選択します。

c) [追加（Add）] をクリックして、一致 ACL を設定します。

たとえば、スポーク 1 の場合、送信元ネットワークは 192.168.20.0/24 で、宛先ネットワークは 192.168.10.0/24 です。

d) [宛先（Send to）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

e) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [順序（Order）] を選択します。

f) 出力インターフェイスとして SVTI-1 インターフェイスと SVTI-2 インターフェイスを選択します。

g) [保存（Save）] をクリックします。

ハブをロードバランシングペアとして使用する場合は、ECMP を設定する必要があります。

ステップ 4 ハブとスポークに設定を展開します。

次のタスク

設定とトンネルのステータスを確認します。詳細については、「ルートベースの VPN での複数ハブ構成の確認 （49 ページ）」を参照してください。

ルートベースの VPN での複数ハブ構成の確認

複数ハブ構成とトンネルのステータスを確認するには、次の手順を実行します。

- 展開後、ダッシュボードでトンネルステータスを確認します。
- サイト間監視ダッシュボードからパケットトレーサを使用して、トラフィックの選択されたパス（ハブ 1 またはハブ 2）を確認します。
- エンドポイントごとに次の show コマンドを使用して、構成を確認します。
  - **show run route-map**
  - **show run access-list**
  - **show route-map**
  - **show route**

バックアップ VTI トンネルを介したトラフィックのルーティング

Secure Firewall Threat Defense は、ルートベース（VTI）VPN のバックアップトンネルの構成をサポートします。プライマリ VTI がトラフィックをルーティングできない場合、VPN 内のトラフィックはバックアップ VTI を介してトンネリングされます。

次のシナリオでバックアップ VTI トンネルを展開できます。

- 両方のピアにサービスプロバイダーの冗長性バックアップがある。

  この場合、2 つの物理インターフェイスがあり、ピアの 2 つの VTI のトンネルソースとして機能します。

- 一方のピアにのみ、サービスプロバイダーの冗長性バックアップがある。

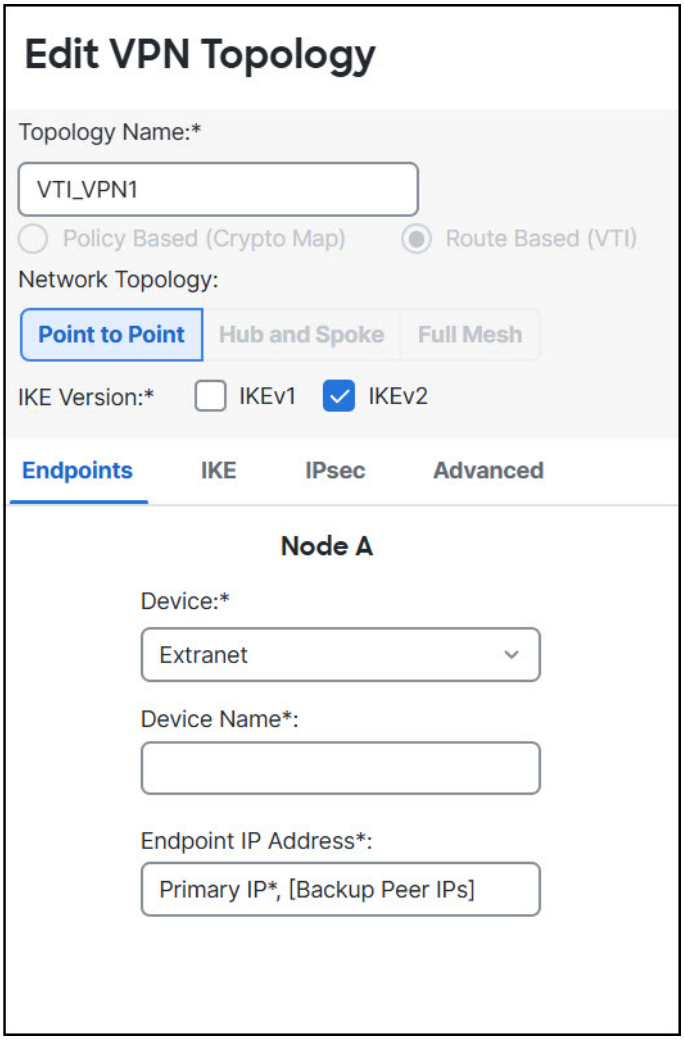
  この場合、ピアの一方の側だけにインターフェイスバックアップがあり、もう一方の端にはトンネル ソース インターフェイスが 1 つだけあります。

手順	操作手順	詳細
1	注意事項と制限事項を確認します。	仮想トンネルインターフェイスのガイドラインと制限事項 （29 ページ）
2	VTIインターフェイスを作成します。	VTI インターフェイスの追加 （34 ページ）
3	[新しいVPNトポロジの作成（Create New VPN Topology）] ウィザードの [エンドポイントの追加（Add Endpoint）] ダイアログボックスで、[バックアップVTIの追加（Add Backup VTI）] をクリックして、各ピアのそれぞれのバックアップ インターフェイスを構成します。	• ポイントツーポイント トポロジのエンドポイントの設定 （37 ページ） • ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）
4	ルーティングポリシーを設定します。	• [デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、Threat Defense デバイスを編集します。 • [ルーティング（Routing）] をクリックします。
5	アクセス コントロール ポリシーを設定します。	• [ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

バックアップ VTI トンネルを構成するためのガイドライン

- エクストラネットピアの場合、バックアップ インターフェイスのトンネルソース IP アドレスを指定し、管理対象ピアでトンネルの宛先 IP を構成できます。

  [新規VPNトポロジの作成（Create New VPN Topology）] ウィザードの [エンドポイントIPアドレス（Endpoint IP Address）] フィールドで、バックアップピアの IP アドレスを指定できます。



- バックアップインターフェイスを設定した後、ルーティングトラフィックのルーティングポリシーとアクセス コントロール ポリシーを設定します。

  プライマリ VTI とバックアップ VTI は常に使用可能ですが、トラフィックはルーティングポリシーで設定されたトンネルのみを通過します。詳細については、VTI のルーティングおよび AC ポリシーの設定 （53 ページ）を参照してください。

- バックアップ VTI を設定している場合は、プライマリ VTI と同じセキュリティゾーンへのバックアップトンネルが含まれていることを確認します。AC ポリシーページのバックアップ VTI に特定の設定は必要ありません。

- バックアップトンネルにスタティックルートを設定する場合は、バックアップトンネルを介したトラフィックフローのフェールオーバーを処理するために、異なるメトリックでスタティックルートを設定します。

ルートベースのサイト間 VPN のダイナミック VTI の設定

Management Center でルートベースのサイト間 VPN のダイナミック VTI を設定するには、次の手順を実行します。

手順	操作手順	詳細情報
1	ハブにダイナミック VTI インターフェイスを作成します。	VTI インターフェイスの追加 （34 ページ）
2	スポークにスタティック VTI インターフェイスを作成します。	VTI インターフェイスの追加 （34 ページ）
3	ルートベースのサイト間 VPN を作成します。	ルートベースのサイト間 VPN の作成 （36 ページ）
4	ルーティングポリシーとアクセス コントロール ポリシーを設定します。	ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）

ダイナミック VTI を使用した仮想ルータの設定方法

管理センターのルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを設定するには、次の手順を実行します。

手順	操作手順	詳細情報
1	ハブのダイナミック VTI インターフェイスとスポークのダイナミック VTI を使用する、ルートベースのサイト間 VPN を作成します。	ルートベースのサイト間 VPN の作成 （36 ページ）
2	仮想ルータを作成します。	仮想ルータの作成
3	インターフェイスを仮想ルータに割り当てます。	仮想ルータの設定
4	ハブとスポークのルーティングポリシーを設定します。	ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）
5	ハブとスポークのアクセス コントロール ポリシーを設定します。	ハブアンドスポークトポロジのエンドポイントの設定 （40 ページ）

VTI のルーティングおよび AC ポリシーの設定

両方のデバイスで VTI インターフェイスと VTI トンネルを設定したら、次のものを設定する必要があります。

- VTI トンネルを介してデバイス間で VTI トラフィックをルーティングするルーティングポリシー。
- 暗号化されたトラフィックを許可するアクセスコントロールルール。

VTI のルーティング設定

VTI インターフェイスの場合、スタティックルートまたはルーティングプロトコル（BGP、EIGRP、OSPF/OSPFv3 など）を設定できます。

1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、Firewall Threat Defense デバイスを編集します。
2. [ルーティング（Routing）] をクリックします。
3. スタティックルート、または BGP、EIGRP、OSPF/OSPFv3 を設定します。

ルーティング	パラメータ	詳細情報
Static Route	• [インターフェイス（Interface）]：VTI インターフェイスを選択します。バックアップトンネルの場合は、バックアップ VTI インターフェイスを選択します。 • [選択したネットワーク（Selected Network）]：リモートピアの保護されたネットワーク。 • [ゲートウェイ（Gateway）]：リモートピアのトンネルインターフェイスの IP アドレス。バックアップトンネルの場合は、リモートピアのバックアップトンネルインターフェイスの IP アドレスを選択します。 • [メトリック（Metrick）]：バックアップトンネルの場合は、異なるメトリックを設定して、バックアップトンネルを介したトラフィックフローのフェールオーバーを処理します。	スタティック ルートの追加

ルーティング	パラメータ	詳細情報

BGP	• [一般設定（General Settings）] > [BGP] で、BGP を有効にし、ローカルデバイスの AS 番号を指定して、ルータ ID を追加します（[手動（Manual）] を選択した場合）。
	• [BGP] で、IPv4/IPv6 を有効にして、[ネイバー（Neighbor）] タブでネイバーを設定します。
	  • [IPアドレス（IP Address）]：リモートピアの VTI インターフェイス IP アドレス。バックアップトンネルの場合は、リモートピアのバックアップ VTI インターフェイスの IP アドレスを使用したネイバーを追加します。
	  • [リモートAS（Remote AS）]：リモートピアの AS 番号。
	• [再配布（Redistribution）] タブをクリックし、[ソースプロトコル（Source Protocol）] を [接続済み（Connected）] として選択し、接続済みルートの再配布を有効にします。
		BGP の設定

ルーティング	パラメータ	詳細情報
EIGRP	• EIGRP を有効にし、ローカルデバイスの AS 番号を指定して、EIGRP ルーティングプロセスに参加するネットワークまたはホストを選択します。 • [ネイバー（Neighbors）] タブをクリックし、EIGRP プロセスの静的ネイバーを定義します。 • VTI インターフェイスからサマリーアドレスをアドバタイズするには、[サマリーアドバイス（Summary Address）] タブで、[インターフェイス（Interface）] ドロップダウンから VTI インターフェイスを選択します。[ネットワーク（Network）] ドロップダウンから、要約するネットワークを選択します。 • [インターフェイス（Interface）] タブをクリックして、VTI インターフェイスのインターフェイス固有 EIGRP ルーティングプロパティを設定します。 インターフェイスで EIGRP スプリットホライズンを有効にするには、[スプリットホライズン（Split Horizon）] チェックボックスをオンにします。EIGRP hello パケットでデバイスによってアドバタイズされる [ホールド時間（Hold Time）] を設定することもできます。	EIGRP の設定

ルーティング	パラメータ	詳細情報
OSPF	• [プロセス 1（Process 1）] チェックボックスをオンにして、OSPF ロールを選択します。 • [インターフェイス（Interface）] タブをクリックし、VTI インターフェイスを選択します。	OSPFv2 の設定
OSPFv3	• [プロセス1（Process 1）] チェックボックスと [プロセス1の有効化（Enable Process 1）] チェックボックスをオンにして、OSPFv3 ロールを選択します。 • [インターフェイス（Interface）] タブをクリックし、VTI インターフェイスを選択します。	OSPFv3 の設定

AC ポリシールール

デバイスのアクセス コントロール ポリシーにアクセスコントロールルールを追加して、次の設定を使用して VTI トンネル間の暗号化されたトラフィックを許可します。

1. 許可アクションを使用してルールを作成します。
2. ローカルデバイスの VTI セキュリティゾーンを送信元ゾーンとして選択し、リモートピアの VTI セキュリティゾーンを宛先ゾーンとして選択します。
3. リモートピアの VTI セキュリティゾーンを送信元ゾーンとして選択し、ローカルデバイスの VTI セキュリティゾーンを宛先ゾーンとして選択します。

アクセス制御ルールの設定の詳細については、アクセス コントロール ルールの作成および編集を参照してください。

仮想トンネル情報の表示

デバイス上のルートベース VPN のダイナミックおよびスタティック VTI の詳細を表示できます。すべての VPN トポロジについて、各ダイナミック VTI に関連付けられている、動的に生成されたすべての仮想アクセスインターフェイスの詳細を表示することもできます。

始める前に

- スタティック VTI の場合：Firewall Threat Defense バージョン 7.0 以降
- ダイナミック VTI の場合：Firewall Threat Defense バージョン 7.3 以降

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 [仮想トンネル（Virtual Tunnels）] タブをクリックします。

VTI ごとに、名前、IP アドレス、IPsec モード、トンネル送信元インターフェイスの詳細、トポロジ、リモート ピア IP などの詳細を表示できます。また、各インターフェイスでパスモニタリングが有効になっているかどうかを確認することもできます。

Umbrella に SASE トンネルを展開する

Cisco Umbrella は、シスコのクラウドベース Secure Internet Gateway（SIG）プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Cisco Umbrella は、セキュア Web ゲートウェイ、DNS レイヤセキュリティ、およびクラウド アクセス セキュリティ ブローカ（CASB）機能を統合して、システムを脅威から保護します。

Management Center を使用すると、Threat Defense デバイスから Cisco Umbrella への IPsec IKEv2 トンネルを展開できます。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Cisco Umbrella SIG に転送します。このソリューションは、セキュリティの中央管理を実現するため、ネットワーク管理者は各ブランチのセキュリティ設定を個別に管理する必要がありません。

Threat Defense デバイスから Cisco Umbrella トンネルを直接設定して展開するには、シンプルなウィザードを使用して SASE トポロジを作成します。SASE トポロジは、次のものをサポートする新しいタイプのサイト間 VPN トポロジです。

- 静的 VTI ベースのサイト間 VPN。
- Cisco Umbrella がハブであり、管理対象の Threat Defense デバイスがスポークである、ハブアンドスポークトポロジ。
- 事前共有キーベースの認証。
- HA モードで展開された Firewall Threat Defense。
- マルチインスタンス：マルチインスタンス展開では、1 つの Cisco Umbrella アカウントのみを統合できます。

高可用性のために、Threat Defense デバイスからの 2 つのトンネルを設定し、2 つ目のトンネルをバックアップトンネルとして使用することができます。必ず、トンネルごとに異なるローカルトンネル ID を設定してください。

設定を容易にするために、Management Center はデフォルトの IPsec および IKEv2 ポリシーを設定します。

デフォルトの IKEv2 ポリシー設定：

- 整合性アルゴリズム：NULL
- 暗号化アルゴリズム：AES-GCM-256
- PRF アルゴリズム：SHA-256
- DH グループ：19、20

デフォルトの IKEv2 IPSec ポリシー設定：

- ESP ハッシュ：SHA-256
- ESP 暗号化：AES-GCM-256

関連トピック

Cisco Umbrella に SASE トンネルを展開する方法 （60 ページ）

Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項

SASE トポロジでは以下の内容がサポートされます。

- PSK ベースの認証のみ
- IKEv2
- ハイ アベイラビリティ

一般的な設定時の注意事項

- Firewall Management Center は、Cisco Umbrella で直接作成されたトンネルや、他のアプリケーションによって作成されたトンネルを検出しません。
- Firewall Management Center によって管理されるデバイスのみを SASE トポロジのエンドポイントとして追加できます。エクストラネットデバイスは追加できません。

  高可用性ペアの場合、HA ペアの名前がエンドポイントリストに表示されます。
- Firewall Management Center からトンネルを削除し、そのトンネルを Cisco Umbrella から削除できない場合は、Cisco Umbrella にログインして手動でトンネルを削除する必要があります。

- Cisco Umbrella への展開が進行中の場合、SASE トポロジは編集または削除できません。トンネルの展開ステータスは、以下で確認できます。
  - ウィザードの [Cisco Umbrella設定（Cisco Umbrella Configuration）] ダイアログボックス
  - [展開（Deployments）] タブと [タスク（Tasks）] タブの [通知（Notifications）] ページ
  - サイト間 VPN 監視ダッシュボード
- ウィザードで [Threat Defenseノードに構成を展開する（Deploy configuration on threat defense nodes）] チェックボックスをオンにすると、トンネルが Cisco Umbrella に展開された後にのみ、Cisco Umbrella SASE トポロジ構成が Firewall Threat Defense に展開されます。

  Firewall Management Center で Firewall Threat Defense に Cisco Umbrella 設定を展開するには、ローカルトンネル ID が必要です。Firewall Management Center で Cisco Umbrella にトンネルが展開された後にのみ、Cisco Umbrella によって完全なトンネル ID（<*prefix*>@<*umbrella generated ID*>-umbrella.com）が生成されます。
- Firewall Management Center では、バージョン 7.3 より前でエクストラネットハブとして作成された Cisco Umbrella データセンターのトポロジは SASE トポロジとして認識されません。バージョン 7.3 で新しい SASE トポロジを作成し、既存のトポロジを削除する必要があります。
- Firewall Threat Defense HA スイッチオーバー後、SASE トポロジはサイト間監視/VPN サマリーダッシュボードには表示されません。**vpn-sessiondb logoff index** コマンドを使用してトンネルを停止し、パケットトレーサを使用してトンネルを起動することを推奨します。

制限事項

SASE トポロジでは以下の内容はサポートされていません。

- クラスタ
- 証明書ベースの認証
- IKEv1

Cisco Umbrella に SASE トンネルを展開する方法

このセクションでは、Firewall Management Center を使用して Firewall Threat Defense デバイスから Cisco Umbrella に SASE トンネルを展開する手順について説明します。

手順	操作手順	詳細
1	注意事項と制限事項を確認します。	Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 （59 ページ）

手順	操作手順	詳細
2	前提条件を満たしていることを確認します。	Cisco Umbrella SASE トンネルを設定するための前提条件 （61 ページ）
3	Cisco Umbrella 接続設定を行います。	• [Cisco Umbrellaの接続設定（Cisco Umbrella Connection Setting）] の設定 • Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング （62 ページ）
4	Cisco Umbrella で SASE トンネルを設定します。	Cisco Umbrella 用の SASE トンネルの設定 （63 ページ）
5	SASE トンネルのステータスを表示します。	SASE トンネルステータスの表示 （65 ページ）

Cisco Umbrella SASE トンネルを設定するための前提条件

- Cisco Umbrella Secure Internet Gateway（SIG）Essentials サブスクリプションが必要です。
- Firewall Management Center から Cisco Umbrella にトンネルを展開するには、輸出規制機能を使用してスマート ライセンス アカウントを有効にする必要があります。このライセンスが有効になっていない場合は、SASE トポロジのみを作成できます。Cisco Umbrella にはトンネルを展開できません。
- https://umbrella.cisco.com で Cisco Umbrella のアカウントを確立し、http://login.umbrella.com で Cisco Umbrella にログインして、Cisco Umbrella への接続を確立するために必要な情報を取得する必要があります。
- Cisco Umbrella を Firewall Management Center に登録し、Cisco Umbrella の接続設定で管理キーと管理シークレットを設定する必要があります。Management Center で、Cisco Umbrella クラウドからデータセンターの詳細を取得するには、管理キーと管理シークレットが必要です。Cisco Umbrella の接続設定で、[組織ID（Organization ID）]、[ネットワークデバイスキー（Network Device Key）]、[ネットワークデバイスシークレット（Network Device Secret）]、および[レガシーネットワークデバイストークン（Legacy Network Device Token）] も設定する必要があります。[

  詳細については、以下を参照してください。

  - Cisco Umbrella の接続設定の設定
  - Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング （62 ページ）

- Firewall Threat Defense から Cisco Umbrella データセンターに到達できることを確認します。

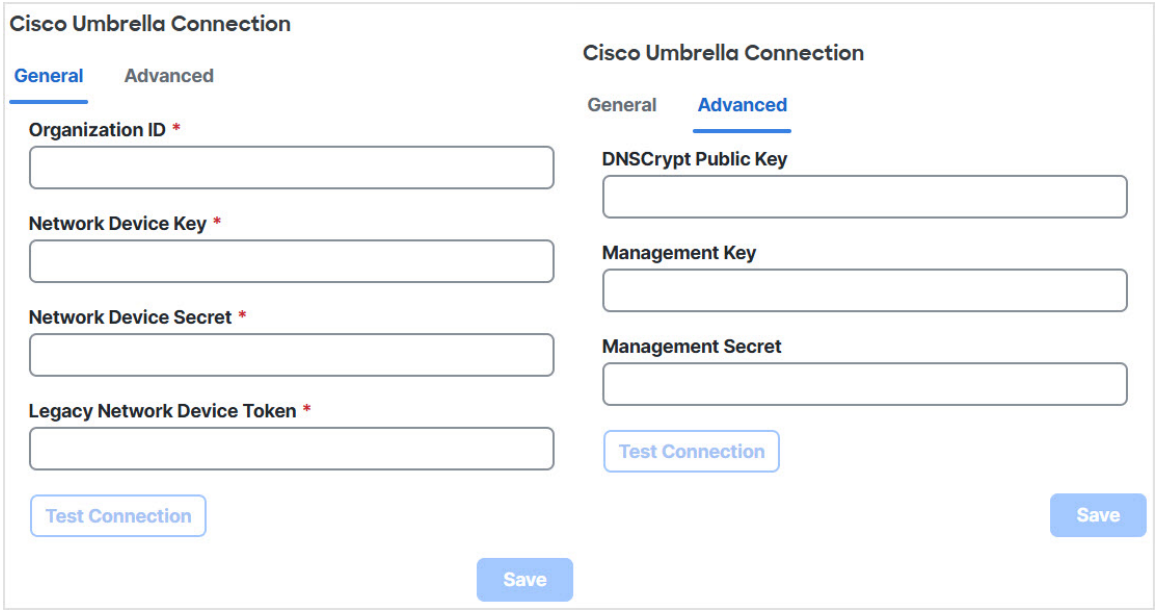
- Cisco Umbrella と Firewall Threat Defense バージョン 7.1.0 以降の間にのみトンネルを展開できます。

Management Center の Umbrella パラメータと Cisco Umbrella の API キーのマッピング

Firewall Management Center を使用して Cisco Umbrella を登録し、Firewall Management Center で Umbrella パラメータを設定するには、次の手順を実行する必要があります。

1. Cisco Umbrella にログインします。
2. [管理（Admin）]>[APIキー（API Keys）]>[レガシーキー（Legacy Keys）] を選択します。
3. 必要な API キーを生成してコピーします。
4. Firewall Management Center で API キーを使用して Cisco Umbrella 接続パラメータを設定します。

次の図は、Firewall Management Center の [Cisco Umbrella接続（Cisco Umbrella Connection）] で設定する必要があるパラメータを示しています。DNSCrypt 公開キーはオプションのパラメータです。



次の図は、Cisco Umbrella を Firewall Management Center に登録するために使用する必要がある Cisco Umbrella API キーを示しています。

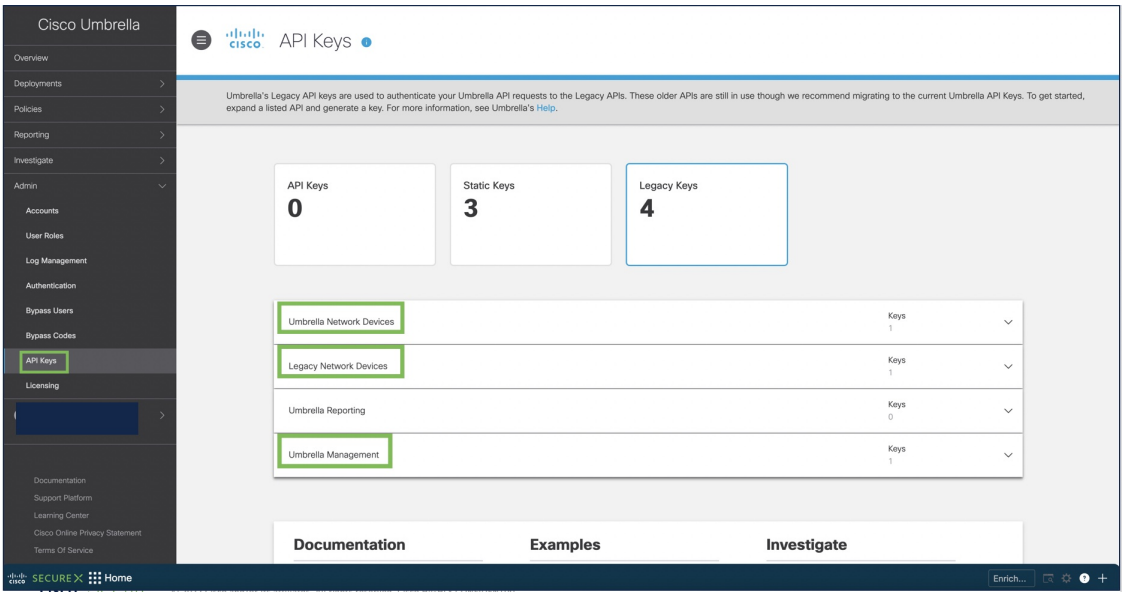


表 *2 : Firewall Management Center* の *Umbrella* パラメータと *Cisco Umbrella* の *API* キーのマッピング

Management Center のパラメータ	Cisco Umbrella の API キー
ネットワークデバイスキー ネットワーク デバイス シークレット	Umbrella ネットワークデバイス
レガシー ネットワーク デバイス トークン	レガシー ネットワーク デバイス
管理キー Management Secret	Umbrella 管理

Cisco Umbrella 用の SASE トンネルの設定

始める前に

Cisco Umbrella SASE トンネルを設定するための前提条件 （61 ページ） および Cisco Umbrella での SASE トンネルの設定に関するガイドラインと制限事項 （59 ページ） の前提条件とガイドラインを確認してください。

手順

ステップ 1 **Devices** > **VPN** > **Site to Site** を選択し、**[追加（Add）]** をクリックしします。

ステップ 2 **[トポロジ名（Topology Name）]** フィールドに、トポロジの名前を入力します。

ステップ 3 **[SASEトポロジ（SASE Topology）]** ボタンをクリックして、**[作成（Create）]** をクリックします。

ステップ 4 [事前共有キー（Pre-shared Key）]：このキーは、Umbrella PSK 要件に従って自動生成されます。単一トポロジの場合、事前共有キーはすべての Threat Defense スポークと Cisco Umbrella で共通です。

デバイスと Cisco Umbrella はこの秘密鍵を共有し、IKEv2 はそれを認証に使用します。このキーを構成する場合は、長さが 16 ～ 64 文字で、少なくとも 1 つの大文字、1 つの小文字、1 つの数字を使用する必要があります。特殊文字は使用できません。各トポロジには、一意の事前共有キーが必要です。トポロジに複数のトンネルがある場合、すべてのトンネルの事前共有キーは同じです。

ステップ 5 [Cisco Umbrellaデータセンター（Umbrella Data center）] ドロップダウンリストからデータセンターを選択します（Firewall Threat Defense からの Cisco Umbrella DC への到達可能性を確保するために、Firewall Threat Defense でルーティングを設定します）。

ステップ 6 [追加（Add）] をクリックして、Firewall Threat Defense ノードを追加します。

a) [デバイス（Device）] ドロップダウンリストから Firewall Threat Defense を選択します。

Firewall Management Center によって管理されているデバイスのみがリストに表示されます。高可用性ペアの場合、HA ペアの名前がエンドポイントリストに表示されます。

b) [VPNインターフェイス（VPN Interface）] ドロップダウンリストからスタティック VTI インターフェイスを選択します。

新しいスタティック VTI インターフェイスを作成するには、Add＋をクリックします。[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスが表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] は static です。
- [名前（Name）] は <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*> です。たとえば、outside_static_vti_2 です。
- [トンネルID（Tunnel ID）] には、一意の ID が自動的に入力されます。
- [トンネル ソース インターフェイス（Tunnel Source Interface）] には、「outside」プレフィックスを持つインターフェイスが自動的に入力されます。
- IPsec トンネルモードは IPv4 です。
- IP アドレスは、169.254.xx/30 プライベート IP アドレスの範囲内です。

c) [ローカルトンネルID（Local Tunnel ID）] フィールドに、ローカルトンネル ID のプレフィックスを入力します。

プレフィックスは 8 文字以上で、100 文字を上限とします。管理センターで Cisco Umbrella にトンネルが展開された後、Cisco Umbrella によって完全なトンネル ID（<*prefix*>@<*umbrella generated ID*>-umbrella.com）が生成されます。次に、管理センターは完全なトンネル ID を取得して更新し、Threat Defense デバイスに展開します。各トンネルには、一意のローカルトンネル ID があります。

d) [保存（Save）] をクリックして、エンドポイントデバイスをトポロジに追加します。

SASE トポロジには複数のエンドポイントを追加できます。

ステップ 7 [次へ（Next）] をクリックして、Cisco Umbrella SASE トンネル設定の概要を確認します。

- [エンドポイント（Endpoints）]ペイン：設定されたエンドポイントの概要を表示します。
- [暗号化設定（Encryption Settings）] ペイン：トポロジのデフォルトの IKEv2 ポリシーと IKEv2 IPsec トランスフォームセットを表示します。

ステップ 8 [Threat Defenseノードに構成を展開する（Deploy configuration on threat defense nodes）] チェック ボックスをオンにすると、Threat Defense へのネットワークトンネルの展開がトリガーされます。この展開は、トンネルが Cisco Umbrella に展開された後に行われます。Threat Defense の展開には、ローカルトンネル ID が必要です。

ステップ 9 [保存（Save）] をクリックします。

このアクションは、次のように動作します。

1. トポロジを管理センターに保存します。
2. Cisco Umbrella へのネットワークトンネルの展開をトリガーします。
3. オプションが有効になっている場合、Threat Defense デバイスへのネットワークトンネルの展開をトリガーします。このアクションでは、デバイスでの最後の展開以降に更新されたすべての構成とポリシー（非 VPN ポリシーを含む）がコミットされて展開されます。
4. [Cisco Umbrella設定（Cisco Umbrella Configuration）] ウィンドウを開き、Cisco Umbrella でのトンネル展開のステータスを表示します。詳細については、SASE トンネルステータスの表示 （65 ページ）を参照してください。

次のタスク

SASE トンネルを通過するように意図された対象のトラフィックについては、特定の一致基準を使用して PBR ポリシーを設定し、VTI インターフェイスを介してトラフィックを送信します。

SASE トポロジのエンドポイントごとに PBR ポリシーを設定してください。

SASE トンネルステータスの表示

手順

ステップ 1 **Devices** > **VPN** > **Site to Site** を選択し、**[追加（Add）]** をクリックしします。

ステップ 2 **[トポロジ名（Topology Name）]** フィールドに、トポロジの名前を入力します。

ステップ 3 **[SASEトポロジ（SASE Topology）]** ボタンをクリックして、**[作成（Create）]** をクリックします。

ステップ 4 一意の **[事前共有キー（Pre-shared Key）]** を入力して、データセンターを選択し、デバイスを追加して、**[次へ（Next）]** をクリックします。

ステップ 5 Cisco Umbrella SASE トンネル設定の概要を表示し、[保存（Save）] をクリックします。[Cisco Umbrella設定（Cisco Umbrella Configuration）] ウィンドウが表示されます。

トンネル展開の名前、データセンター、データセンターの IP アドレス、開始時刻、終了時刻などのトポロジの詳細を確認できます。

Cisco Umbrella でトンネルの展開ステータスを確認できます。さまざまなトンネル展開ステータスは次のとおりです。

- 保留中：Management Center が構成を Cisco Umbrella にプッシュしていません。
- 成功：Management Center が Cisco Umbrella にトンネルを正常に設定しました。
- 進行中：Management Center が Cisco Umbrella にトンネルを展開しています。
- 失敗：Management Center が Cisco Umbrella でトンネルを設定できませんでした。

ステータスが保留中または失敗として表示される場合は、トランスクリプトを使用してトンネル作成のトラブルシューティングを行います。**[トランスクリプト（ transcript）]** ボタンをクリックして、API、リクエスト ペイロード、Cisco Umbrella から受信したレスポンスなど、トランスクリプトの詳細を表示します。

ステップ 6 [Cisco Umbrellaダッシュボード（Umbrella Dashboard）] をクリックして、Cisco Umbrella のネットワークトンネルを表示します。

ステップ 7 次の場所で Cisco Umbrella トンネルの展開ステータスを確認します。

- [展開（Deployments）] タブと [タスク（Tasks）] タブの [通知（Notifications）] ページ。
- **サイト間** VPN 監視ダッシュボード（**[概要（Overview）]>[ダッシュボード（Dashboards）]>[サイト間 VPN（Site to Site VPN）]**）。

  ダッシュボードには、Cisco Umbrella SASE トポロジを含むサイト間 VPN トポロジの概要が表示されます。ピアデバイス間のトンネルと各トンネルのステータスを確認できます。CLI コマンドとパケットトレーサを使用して、トンネルの展開に関する問題をトラブルシューティングすることもできます。

サイト間 VPN のモニタリング

Secure Firewall Management Center は、サイト間 VPN トンネルのステータスを判断するために、サイト間VPNトンネル（SASEトポロジトンネルを含む）のスナップショットを提供します。ピアデバイス間のトンネルのリストと、各トンネルのステータス（[アクティブ（Active）]、[非アクティブ（Inactive）]、または[アクティブデータなし（No Active Data）]）を表示できます。トポロジ、デバイス、およびステータスでテーブル内のデータをフィルタ処理できます。監視ダッシュボードのテーブルにはライブデータが表示され、指定した間隔でデータが更新されるように設定できます。このテーブルは、暗号マップベースの VPN のピアツーピア、ハブアンドスポーク、およびフルメッシュトポロジを示しています。トンネル情報には、ルートベースの VPN または仮想トンネルインターフェイス（VTI）のデータも含まれます。

このデータを使用して、次のことができます。

- 問題のある VPN トンネルを特定し、トラブルシューティングを行います。
- サイト間 VPN ピアデバイス間の接続を確認します。
- VPN トンネルの正常性を監視して、サイト間の中断のない VPN 接続を提供します。

暗号マップベースのサイト間 VPN の設定については、ポリシーベースのサイト間 VPN の設定（7 ページ）を参照してください。

VTI の詳細については、仮想トンネル インターフェイスについて （25 ページ）を参照してください。

Firewall Threat Defenseの VPN モニタリングおよびトラブルシューティングについては、VPN のモニタリングとトラブルシューティングを参照してください。

注意事項と制約事項

- テーブルには、展開されているサイト間（SASE トポロジを含む）VPN のリストが表示されます。作成されていても展開されていないトンネルは表示されません。
- テーブルには、ポリシーベースの VPN およびバックアップ VTI のバックアップトンネルに関する情報は表示されません。
- クラスタ展開の場合、テーブルには、ディレクタの変更はリアルタイムデータでは表示されません。VPN が展開されたときに存在していたディレクタ情報のみが表示されます。ディレクタ変更は、変更後にトンネル AM が再展開された後にのみテーブルに反映されます。

サイト間 VPN 監視ダッシュボード

[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site to Site VPN）] を選択してサイト間監視ダッシュボードを開きます。

サイト間 VPN 監視ダッシュボードには、サイト間 VPN トンネルの次のウィジェットが表示されます。

- **トンネルステータス（Tunnel Status）**：Firewall Management Centerを使用して設定されたサイト間 VPN（Umbrella 用の SASE トンネルを含む）のトンネルステータスのリストが示されるテーブル。
- **トンネル要約（Tunnel Summary）**：トンネルステータスが集計されたドーナツグラフ。
- **トポロジ（Topology）**：トポロジ別に要約されたトンネルステータス。

VPN トンネルのステータス

サイト間監視ダッシュボードには、次の状態にある VPN トンネルのリストが表示されます。

- **非アクティブ（Inactive）**：すべての IPSec トンネルがダウンしている場合、ポリシーベース（暗号マップベース）の VPN トンネルは非アクティブです。トンネルで設定または接

続に関する問題が発生した場合、VTI および SASE トポロジ VPN トンネルはダウンします。

- **アクティブ（Active）**：Firewall Management Center では、ポリシーベースのサイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよび IPsec プロポーザルに基づいて設定されます。展開後に Firewall Management Center がトンネルを通過する対象トラフィックを識別すると、ポリシーベースの VPN トンネルはアクティブ状態になります。IKE トンネルは、少なくとも 1 つの IPsec トンネルが稼働状態になった場合にのみ稼働状態になります。

  ルートベースの VPN（VTI）および SASE トポロジの VPN トンネルでは、対象トラフィックがアクティブ状態である必要はありません。それらは、エラーなしで設定および展開されると、アクティブ状態になります。

- **アクティブデータなし（No Active Data）**：ポリシーベースのトンネルおよび SASE トポロジ VPN トンネルは、トンネルを通過するトラフィックフローが初めて発生するまで、アクティブデータなし状態のままになります。アクティブデータなし状態では、展開済みでエラーのあるポリシーベースおよびルートベース VPN のリストも表示されます。

Firewall Management Centerでのトンネルステータスに関する重要な注意事項

- Firewall Management Centerでの VPN ステータスはイベントベースです。Firewall Management Centerはステータスの更新を開始しません。そのため、ダッシュボードとFirewall Threat Defenseでトンネルステータスが一致しない場合があります。正しいステータスは、[トンネルステータス（Tunnel Status）] ウィジェットの [CLIの詳細（CLI Details）] タブで表示できます。
- Firewall Threat Defenseがセカンダリ Firewall Threat Defenseにスイッチオーバーすると、Firewall Management CenterとFirewall Threat Defenseで VPN トンネルのステータスに一致が発生します。デバイスがプライマリデバイスに戻ると、正しいトンネルステータスが表示されます。
- Firewall Management Centerは、デバイスの再起動後、7.3 より前のFirewall Threat Defenseデバイスのトンネルステータスを更新しません。**vpn-sessiondb logoff index** コマンドを使用してトンネルを停止し、パケットトレーサを使用してトンネルを起動することを推奨します。

Tunnel Status

このテーブルには、Firewall Management Centerを使用して設定されたサイト間 VPN（SASE トポロジ VPN を含む）のリストが示されます。トポロジにマウスのカーソルを合わせて **View** (👁) をクリックすると、トポロジに関する次の詳細情報が表示されます。

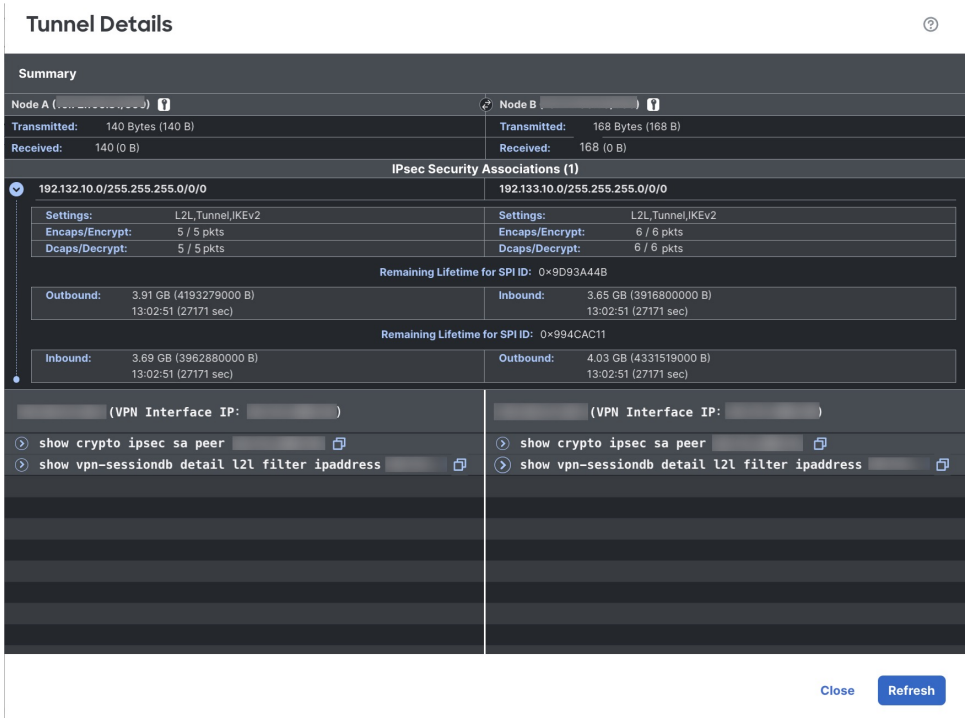
- [全般（General）]：IP アドレスやインターフェイス名など、ノードに関する詳細情報が表示されます。
- [CLIの詳細（CLI Details）]：次のコマンドの CLI 出力が表示されます。
  - **show crypto ipsec sa peer** <*node A/B_ip_address*>：ノード A とノード B の間に構築された IPSec SA が表示されます。

- **show vpn-sessiondb l2l filter ipaddress** <*node A/B_ip_address*>：VPN セッションに関する情報が表示されます。

エクストラネットデバイスの場合、コマンド出力は表示されません。

上記のコマンド出力で得られる IKE および IPsec セッションに関する重要な詳細情報が、要約され、ユーザーフレンドリな形式で表示されます。両方のノードの詳細情報を一度に表示できます。ノード名の横にあるアイコンは、認証タイプ（事前共有キーまたはクライアント証明書）を示します。詳細情報には、次に示すように、トンネルごとの IKE 統計と、IPSec SA 統計が含まれます。

図 *1 : [*トンネルステータス（*Tunnel Status***）*] > [*（表示）*View] > [CLI* 詳細（***CLI Details***）*]***

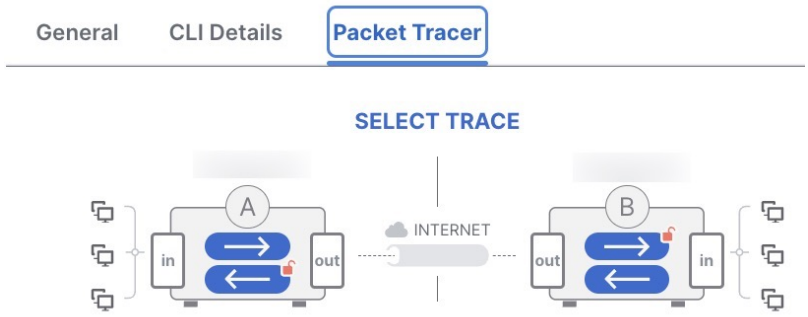


- [パケットトレーサ（Packet Tracer）]：パケットトレーサを使用して、脅威防御 VPN トンネルのトラブルシューティングを行います。

Packet Tracer

パケットトレーサを使用すると、2 つの Threat Defense デバイス間の VPN トンネルのトラブルシューティングを行うことができます。デバイス A とデバイス B の間の VPN 接続が稼働状態かどうかをチェックできます。このツールは、パケットをデバイスに挿入し、入力ポートから出力ポートへのパケットフローを追跡できます。このツールは、保護されるネットワークとともにデバイスの入力インターフェイスを設定した後、トラフィックをシミュレートします。パケットトレーサでは、フローおよびルーティングルックアップ、ACL、プロトコルインスペクション、NAT、QoS などのモジュールに照らしてパケットが評価されます。

図 *2 : Packet Tracer*



このツールは、デバイスごとに、暗号化トレースと復号トレースを実行します（パケットは復号された VPN トラフィックとして扱われます）。デバイスの入力ポートと出力ポートの間で 4つの異なるトレースを実行できます。個別の暗号化オプションおよび復号オプションをクリックして、トレースを有効または無効にします。

トレースを実行すると、ツールは、次の順序で、トレースを順番に実行します。

1. A の暗号化トレース。
2. B の復号トレース。
3. B の暗号化トレース。
4. A の復号トレース。

トレースが完了したら、各モジュールの結果を含むトレースの出力を表示できます。

（注） ルートベース（VTI ベース）の VPN の復号トレースは実行できません。

パケットトレーサを実行するには、次の手順に従います。

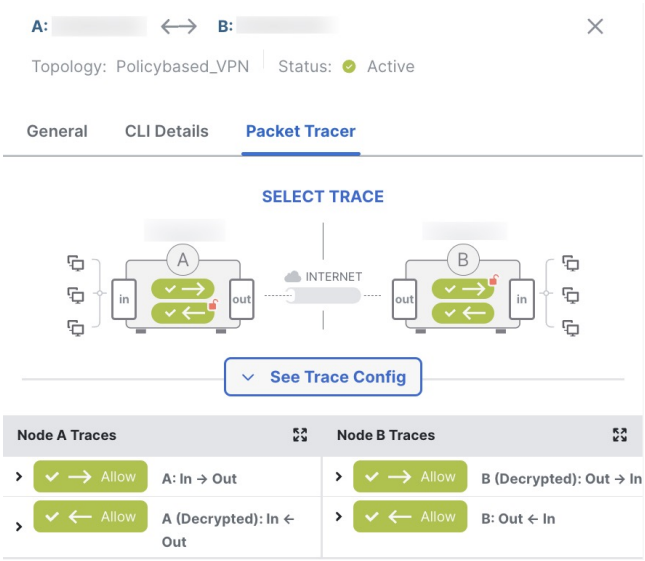
1. [詳細設定を表示する（See Detailed Config）] をクリックして、VPN インターフェイス名、VPN インターフェイスの IP アドレス、VTI インターフェイス名、および VTI インターフェイスの IP アドレスを表示します。
2. （任意）[プロトコル（Protocol）] ドロップダウンリストからプロトコルを選択します。[ICMP/8/0]、[TCP]、または [UDP] を選択できます。

   [ICMP/8/0] がデフォルトのオプションです。[ICMP/8/0] を選択する場合は、8 がエコー要求の ICMP タイプを示し、0 が ICMP コードを示します。[TCP] または [UDP] を選択する場合は、[宛先ポート（Destination Port）] ドロップダウンリストから宛先ポートを選択します。指定できる範囲は 0 ～ 65535 です。
3. [入力インターフェイス（Ingress Interface）] ドロップダウンリストから、パケットをトレースする両方のデバイスの入力インターフェイスを選択します。

4. [保護されたネットワークのIPアドレス（Protected Network IP Address）] フィールドに、入力インターフェイスと同じサブネットからの IP アドレスを入力します。
5. [今すぐトレース（Trace Now）] をクリックします。

   トレースを開始すると、モジュールごとにトレースが成功したかどうかを表示できます。トンネルがダウンしている場合、パスは赤色で表示されます。トンネルが稼働状態の場合、パスは緑色で表示されます。トンネルがダウンしている場合は、[再トレース（Re-trace）] をクリックしてツールを再実行します。暗号マップベースの VPN の場合、対象トラフィックがなく、トンネルが非アクティブのときは、最初のトレースが赤色になる可能性があります。[再トレース（Re-trace）] をクリックしてトレースを再実行してください。

図 *3*：トレースが成功した後のパケットトレーサ



エクストラネットノード：1つのノードをエクストラネットとして使用してVPNトンネルのパケットトレースを開始できます。エクストラネットノードの場合、入力インターフェイスを選択することはできません。パケットトレースの残りの手順は同じです。エクストラネット側でトレースを実行することはできません。

たとえば、ノード A が管理された脅威防御であり、ノード B がエクストラネットである場合は、次の手順に従います。

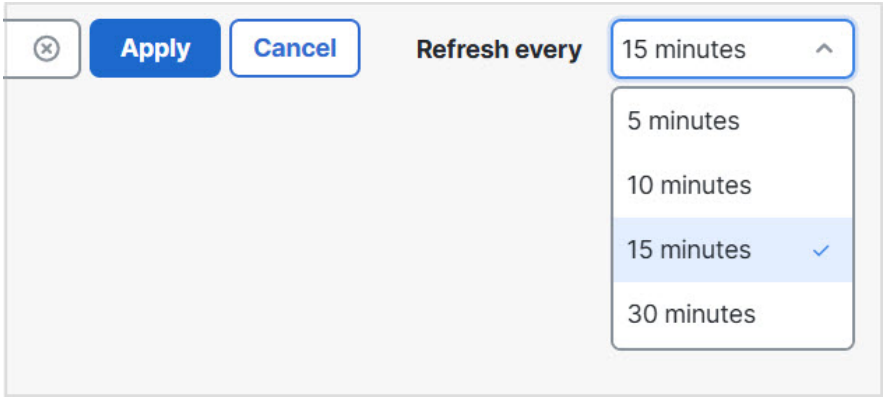
- ノード A の入力インターフェースを設定します。
- ノード A とノード B の保護されたネットワークを設定します。
- [今すぐトレース（Trace Now）] をクリックします。トレースは、ノード B ではなく、ノード A について表示されます。

自動データ更新

テーブル内のサイト間 VPN データは定期的に更新されます。VPN モニタリングデータの更新間隔を特定の間隔で設定するか、自動データ更新をオフにすることができます。

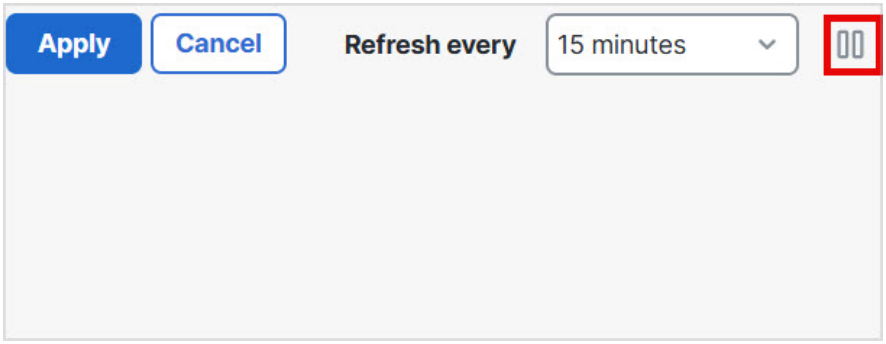
更新間隔のドロップダウンをクリックして、テーブル内のデータの更新に使用する間隔を選択します。

図 *4*: トンネルデータの更新



[一時停止（Pause）]をクリックすると、必要なだけ自動データ更新を停止できます。同じボタンをクリックすると、トンネルデータの更新を再開できます。

図 *5*: 定期的なデータ更新の一時停止



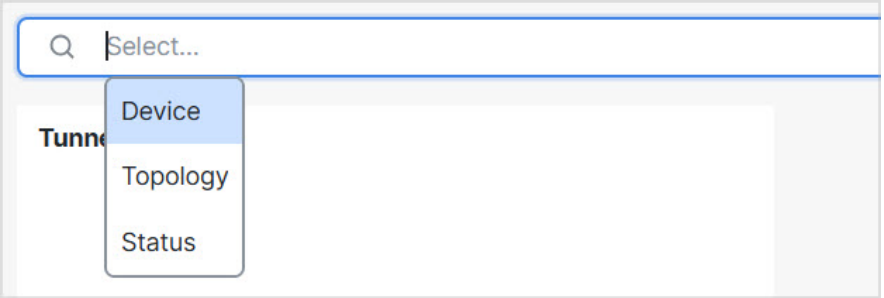
サイト間 VPN モニタリングデータのフィルタ処理およびソート

VPN モニタリングテーブルのデータを、トポロジ、デバイス、およびステータスでフィルタ処理して表示できます。

たとえば、特定のトポロジでダウン状態にあるトンネルを表示できます。

フィルタ処理ボックス内をクリックしてフィルタ条件を選択し、フィルタ処理する値を指定します。

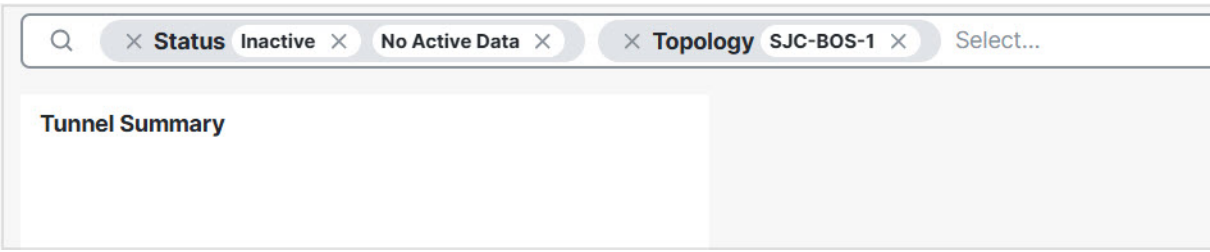
図 *6:* トンネルデータのフィルタ処理



複数のフィルタ処理基準により、要件に基づいてデータを表示できます。

たとえば、稼働状態とダウン状態のトンネルのみを表示し、不明状態のトンネルを無視するように選択できます。

図 *7:* 例：トンネルデータのフィルタ処理



データのソート：列ごとにデータをソートするには、列の見出しをクリックします。

関連トピック

サイト間 VPN について （1 ページ）
仮想トンネル インターフェイスについて （25 ページ）

サイト間 VPN の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
仮想トンネル情報の表示	7.4.1	任意	デバイス上のルートベース VPN のダイナミックおよびスタティック VTI の詳細を表示できます。すべての VPN トポロジについて、ダイナミック VTI に関連付けられているすべての仮想アクセスインターフェイスの詳細も表示できます。 新規/変更された画面：**[デバイス（Device）]** > **[デバイス管理（Device Management）]** > **[デバイスの編集（Edit a device）]** > **[インターフェイス（Interfaces）]** の順に選択し、**[仮想トンネル（Virtual Tunnels）]** タブをクリックします。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
IPSec フローのオフロード	7.4	いずれか	IPSec フローのオフロードは、Secure Firewall 3100 および Secure Firewall 4200 デバイスの VTI ループバック インターフェイスで自動的に有効になります。
Umbrella SASE トポロジ	7.3	任意（Any）	Umbrella SASE トポロジを設定し、Threat Defense デバイスと Umbrella の間に IPsec IKEv2 トンネルを展開できます。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Umbrella Secure Internet Gateway（SIG）に転送します。
ダイナミック仮想トンネルインターフェイスのサポート	7.3	任意（Any）	ダイナミック VTI を作成し、それを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できます。
VTI の EIGRP IPv4 サポート	7.3	任意（Any）	スタティックおよびダイナミック VTI インターフェイスは、EIGRP IPv4 ルーティングプロトコルをサポートしています。
VTI の OSPFv2/v3 IPv4/v6 サポート	7.3	任意（Any）	スタティックおよびダイナミック VTI インターフェイスは、OSPFv2/v3 IPv4/v6 ルーティングプロトコルをサポートしています。
サイト間 VPN 監視ダッシュボードのパケットトレーサ	7.3	任意（Any）	サイト間 VPN モニタリングダッシュボードのパケットトレーサツールを使用して、Threat Defense VPN トンネルのトラブルシューティングを行います。 新規/変更された画面： **[概要（Overview）] > [ダッシュボード（Dashboards）] > [拠点間 VPN（Site to Site VPN）]**
リモートアクセス VPN ダッシュボード	7.3	任意（Any）	リモートアクセス VPN ダッシュボードを使用して、デバイス上のアクティブなリモートアクセス VPN セッションからのリアルタイムデータをモニターします。 新規/変更された画面： **[概要（Overview）] > [ダッシュボード（Dashboards）] > [拠点間VPN（Site to Site VPN）][リモート アクセス VPN（Remote Access VPN）]**
IPSec フローのオフロード	7.2	任意（Any）	Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティアソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブルゲートアレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
サイト間 VPN フィルタ	7.1	任意（Any）	アクセス コントロール ポリシーを使用してサイト間 VPN トラフィックを制御できます。
ローカルトンネル ID のサポート	7.1	任意（Any）	サイト間 VPN の各エンドポイントについて、ピアと共有する一意のトンネル ID を設定できます。
複数の IKE ポリシーのサポート	7.1	任意（Any）	エンドポイントごとに複数の IKEv1 および IKEv2 ポリシーオブジェクトを追加できます。
サイト間 VPN 監視ダッシュボード	7.1	任意（Any）	サイト間 VPN 監視ダッシュボードを使用して、サイト間 VPN トンネルのステータスを表示および監視します。
ルートベースのサイト間 VPN 向けバックアップ用仮想トンネルインターフェイス（VTI）。	7.0	任意（Any）	仮想トンネルインターフェイスを使用するサイト間 VPN を設定する場合、トンネルのバックアップ VTI を選択できます。バックアップ VTI を指定すると復元力が得られるため、プライマリ接続がダウンした場合でもバックアップ接続は継続して機能します。たとえば、プライマリ VTI をあるサービスプロバイダーのエンドポイントに接続し、バックアップ VTI を別のサービスプロバイダーのエンドポイントに接続できます。 ポイントツーポイント接続の VPN タイプとして [ルートベース（Route-Based）] を選択することで、サイト間 VPN ウィザードにバックアップ VTI を追加できます。
VTI の数をインターフェイスあたり 100 からデバイスあたり 1024 に強化	7.0	任意（Any）	VTI の最大数のサポートが、物理インターフェイスあたり 100 からデバイスあたり 1024 VTI に拡張されました。
IPv6 のサポート	7.0	任意（Any）	IPv6 アドレスが指定された VTI を設定できます。トンネルの送信元および接続先としてサポートされるのは、静的 IPv6 アドレスだけですが、VTI では IPv6 BGP はサポートされていません。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
弱い暗号の削除と廃止	6.7	いずれか	安全性の低い暗号のサポートが削除されました。VPN が正しく機能するように、Firewall Threat Defense 6.70 にアップグレードする前に、サポートされる DH および暗号化アルゴリズムに VPN 設定を更新することを推奨します。 Firewall Threat Defense 6.70 でサポートされているものと一致するように IKE プロポーザルと IPSec ポリシーを更新してから、設定の変更を展開します。 次の安全性の低い暗号は、Firewall Threat Defense 6.70 以降では削除または廃止されました。 • **Diffie-Hellman グループ 5** は IKEv1 では廃止され、IKEv2 では削除されました • Diffie-Hellman グループ 2 および 24 は削除されました。 • **暗号化アルゴリズム**：3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256 は削除されました。 （注） **DES** は、評価モードで、または強力な暗号化の輸出規制を満たさないユーザーのためにサポートされます。 **NULL** は IKEv2 ポリシーでは削除されますが、IKEv1 と IKEv2 両方の IPsec トランスフォームセットでサポートされます。
動的 RRI サポート	6.7	いずれか	ダイナミック リバース ルート インジェクションは、IKEv2 ベースの静的暗号マップでサポートされます。
サイト間 VPN のバックアップピア	6.6	任意（Any）	Firewall Management Center を使用して、サイト間 VPN 接続にバックアップピアを追加できます。たとえば、2 つの ISP がある場合は、最初の ISP への接続が使用できなくなった場合に、バックアップ ISP にフェールオーバーするように VPN 接続を設定できます。 新規/変更されたページ： **[デバイス（Devices）] > [VPN] > [サイト間（Site to Site）]**。ポイントツーポイントまたはハブアンドスポークの FTD VPN トポロジを追加または編集してエンドポイントを追加する場合、[IPアドレス（IP Address）] フィールドでカンマ区切りのバックアップピアがサポートされます。

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。