のサイト間 VPN Firepower Threat Defense

Firepower Threat Defense サイト間 VPN について

Firepower 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 プロトコルの両方をサポート。
- 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 トポロジは、セキュリティ認証に準拠するための構成時の設定を提供します。
- 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。
- Firepower Management Center および FTD 両方の HA 環境をサポート。
- トンネルがダウンした際の VPN アラート。
- FTD 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 の IKEv1 バックアップ ピア設定をサポート。
- 「ハブ アンド スポーク」展開でのハブとしてエクストラネット デバイスをサポート。
- 「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 アドレスをサポート。
- エクストラネットデバイスのダイナミック IP アドレスをエンドポイントとしてサポート。
- 「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をサポート。

VPN トポロジ

新しいサイト間 VPN トポロジを作成するには、少なくとも、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、Firepower Threat Defense デバイスにトポロジを展開します。Firepower Management Center は、FTD 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

Firepower 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、Firepower 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。これには次が含まれます。

- Firepower Management Center ではサポートされているが、ユーザ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。Firepower 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Firepower 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。

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

- 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 ピアを使用してのみ、ドメイン間の VPN 接続が可能です。
- 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。
- 「範囲」オプションのあるネットワーク オブジェクトは、VPN では対応していません。
- Firepower Threat Defense VPN のバックアップは、Firepower Management バックアップを使用した場合のみ行われます。
- Firepower 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には対応していません。
- Firepower 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 が選択されている場合、トランスポート モードのデバイス インターフェイス アドレス検証は実行されません。
- 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して、トポロジを設定することはできません。
- 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 を使用している間はハブ、スポーク、フル メッシュのトポロジはサポートされません。ポイントツーポイント VPN のみがサポートされます。さらに、暗号 ACL では、VPN トポロジのトンネル ヘルス イベントがサポートされません。
- 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。
- Firepower 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、Firepower Threat Defense 6.30 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。

Firepower Threat Defense のサイト間 VPN の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

ステップ 1 VPN の証明書認証の場合は、トラストポイントを割り当てることでデバイスを準備する必要があります。詳細については、Firepower Threat Defense Certificate ベースの認証 を参照してください。

ステップ 2 **[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）]** を選択して、Firepower Threat Defense のサイト間 VPN の設定と展開を管理します。次のオプションから選択します。

- 追加：新しい VPN トポロジを作成するには、**[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]** をクリックして、Firepower Threat Defense サイト間 VPN の設定 （5 ページ） の手順を実行します。

  （注） VPN トポロジは、リーフ ドメインでのみ作成できます。

- 編集：既存の VPN トポロジの設定を変更するには、編集アイコン（）をクリックします。変更は設定とほとんど同じです。前述の手順を実行してください。

  （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 人のユーザが同じトポロジを同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していません。

- 削除：VPN の展開を削除するには、削除アイコン（）をクリックします。
- VPN ステータスの表示：このステータスは Firepower の VPN にのみ適用されます。現時点では、FTD VPN についてはステータスが表示されません。FTD VPN のステータスを確認するには、Firepower Threat Defense の VPN モニタリング を参照してください。
- 展開：[展開（Deploy）] をクリックします（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。

Firepower Threat Defense サイト間 VPN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

ステップ 1 [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）]。次に、[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]、または、リストされている VPN トポロジを編集します。を選択します。

ステップ 2 一意のトポロジ名を入力します。トポロジには、FTD VPN であることとトポロジタイプを示す名前を付けることをお勧めします。

ステップ 3 この VPN のネットワーク トポロジを選択します。

ステップ 4 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] のいずれかを選択します。

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 をサポートしない場合は、[IKEv1] を選択します。

Ikev1 の場合は、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 ピアを設定できます。詳細については、FTD VPN エンドポイント オプション （6 ページ）を参照してください。

ステップ 5 必須: トポロジの各ノードの追加アイコン（  ）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。

FTD VPN エンドポイント オプション （6 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 6 （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 FTD VPN IKE オプション （9 ページ）

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 IPsec オプションを指定します FTD VPN IPsec オプション （11 ページ）

ステップ 8 （任意） FTD のサイト間 VPN 展開の詳細オプション （14 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 9 [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。

FTD VPN エンドポイント オプション

ナビゲーション パス

> [サイト間（Site To Site）]。その後、[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]、またはリストされている VPN トポロジを編集します。[エンドポイント（Endpoint）] タブを開きます。

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 FTD で管理する Firepower Management Center デバイス。
- この FTD で管理する Firepower 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 Firepower 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 Address

- Firepower 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。

ポイントツーポイント トポロジーと IKEv1 のみを選択した場合は、プライマリ IP アドレスとバックアップ ピアの IP アドレスをカンマで区切って入力することでバックアップ ピアを設定できます。

- 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このインターフェイスに割り当てられているアドレスです）。
- 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。

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

事前構成された証明書マップ オブジェクトを選択するか、受信したクライアント証明書に必要な情報が VPN 接続に有効であることを定義する証明書マップ オブジェクトを追加アイコン（  ）をクリックして追加します。詳細については、「FTD 証明書のマップ オブジェクトについて」を参照してください。

保護されたネットワーク（Protected Networks）

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、ネットワークにマークを付けることができます。追加アイコン（  ）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 リストが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。エンドポイントについて保護されたネットワークのリストに 1 つ以上の 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（つまり、IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。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） [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、[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）] でリバース ルート インジェクションを無効にします。設定変更を展開します。これによって暗号マップから set reverse-route（リバース ルート インジェクション）が削除され、リバース トンネル トラフィックをドロップするようにする NVP でアドバタイズされたリバース ルートが削除されます。

- [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。[追加（Add）] アイコン（  ）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。

FTD 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

> [サイト間（Site To Site）]。その後、[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]、またはリストされている VPN トポロジを編集します。[IKE] タブを開きます。

フィールド

ポリシー

事前定義済みの 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。詳細については、FTD 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）]：管理センターが、この VPN に使用される事前共有キーを自動的に定義します。[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、Firepower 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 に使用される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）] に再入力して確認します。

  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は、管理対象デバイス上で同じ名前のトラストポイントを生成するために使用されます。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 ID 証明書を取得するために必要な CA サーバ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
    - 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（Manual）]	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（Self-signed）	N/A	N/A	N/A

- Firepower 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）] タブの [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、エンドポイントはサイト間 VPN 接続を完了できません。

FTD 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。

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。クリプト マップ エントリに定義されたプロポーザルは、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 フローを保護するための IPsec セキュリティ

ネゴシエーションで使用されます。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。ダイナミック暗号マップ 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 クリプト 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 モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。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。転送モードでは 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。transport 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することはできません。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、（）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、使用する Diffie-Hellman 係数グループの決定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。

FTD のサイト間 VPN 展開の詳細オプション

ここでは、S2S 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。

FTD 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。または、[永続的に有効にする（EnableInfinite）] に設定して、デバイスがキープアライブ モニタリングを開始することがないように指定します。

しきい値（Threshold）
IKE キープアライブの信頼間隔を指定します。これは、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。最小値およびデフォルトは 10 秒で、最大値は 3600 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。
- 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。

アグレッシブ モードの有効化（Enable Aggressive Mode）

ハブアンドスポーク VPN トポロジでのみ使用できます。IP アドレスが不明であり、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。

[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、SA の数は制限されません。

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することができます。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。

FTD 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 デバイスの動作を妨げ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、PMTU（パス最大伝送ユニット）のエージング、つまり、SA（セキュリティ アソシエーション）の PMTU リセット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（セキュリティ アソシエーション）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。

FTD 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

[サイト間（Site To Site）]、その後 [VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）] を選択するか、またはリストされている VPN トポロジを編集します。[詳細設定（Advanced）] タブを開き、ナビゲーション ウィンドウで [トンネル（Tunnel）] を選択します。

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では表示されません。

- [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）] : NAT キープアライブ メッセージ トラバーサルを有効にするかどうかを指定します。VPN 接続ハブと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 を実行します。

  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 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)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。復号されたトラフィック オプションに対してバイパス アクセス コントロールポリシーを有効にすると、ACLインスペクションがバイパスされますが、AAA サーバからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

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。