VPN の概要

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介してエンドポイント間の安全なトンネルを確立します。

この章は、Firepower Threat Defense デバイス上のリモート アクセスおよびサイト間 VPN にのみ適用されます。サイト間およびリモート アクセス VPN の構築に使用される Internet Protocol Security（IPsec）、Internet Security Association and Key Management Protocol（ISAKMP、または IKE）および SSL 規格について説明します。

Firepower Management Center でゲートウェイ VPN または Firepower VPN と呼ばれる、7000 および 8000 シリーズ デバイス上のサイト間 VPN については ゲートウェイ VPN で説明しています。

VPN タイプ

Firepower Management Center は次のタイプの VPN 接続をサポートします。

- Firepower Threat Defense デバイス上のリモート アクセス VPN。

  リモート アクセス VPN は、リモート ユーザと会社のプライベート ネットワーク間のセキュアな暗号化接続、またはトンネルです。接続は、社内のプライベート ネットワークのエッジにある、VPN クライアント機能を備えたワークステーションやモバイル デバイスである VPN エンドポイント デバイス、VPN ヘッドエンド デバイス、またはセキュア ゲートウェイで構成されます。

  Firepower Threat Defense デバイスは SSL 経由のリモート アクセス VPN または Firepower Management Center による IPsec IKEv2 をサポートするように設定できます。このデバイスは、この容量でセキュアなゲートウェイとして機能して、リモートユーザを認証し、アクセスを許可し、データを暗号化してネットワークへのセキュアな接続を提供します。

Firepower Management Center によって管理されるその他のタイプのアプライアンスは、リモート アクセス VPN 接続をサポートしていません。

Firepower Threat Defense セキュア ゲートウェイは、AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] の完全なトンネル クライアントをサポートしています。このクライアントは、リモート ユーザにセキュアな SSL IPsec IKEv2 接続を提供するために必要です。接続時にクライアントプラットフォームに展開できるため、このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモートユーザはクライアントを活用できます。これは、エンドポイント デバイスでサポートされている唯一のクライアントです。

- Firepower Threat Defense デバイス上のサイト間 VPN。

  サイト間 VPN は、地理的に異なる場所にあるネットワークを接続します。管理対象デバイス間、および管理対象デバイスと関連するすべての規格に準拠するその他のシスコまたはサードパーティのピアとの間で、サイト間IPsec接続を作成できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコル スイートと IKEv1 または IKEv2 を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。

- 7000 および 8000 シリーズ デバイス上のサイト間 VPN。

  これらのサイト間 VPN は、Firepower Management Center 内でゲートウェイ VPN または Firepower VPN と呼ばれます。このタイプの VPN 接続については、ゲートウェイ VPN を参照してください。

VPN の基本

トンネリングによって、インターネットなどのパブリック TCP/IP ネットワークの使用が可能となり、リモートユーザとプライベート企業ネットワークとの間でセキュアな接続を作成できます。各セキュアな接続がトンネルと呼ばれます。

IPsec ベースの VPN テクノロジーでは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリングを使用して、トンネルを構築し管理します。ISAKMP と IPsec は、次を実現します。

- トンネル パラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。

- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル エンドポイントとして機能します。プライベート ネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信することができます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリック ネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

サイト間 VPN 接続が確立された後、ローカル ゲートウェイの背後にあるホストは、セキュアなVPNトンネルを介してリモート ゲートウェイの背後にあるホストと接続できます。接続は、2つのゲートウェイのIPアドレスとホスト名、それらの背後にあるサブネット、および2つのゲートウェイが互いを認証するために使用する方式で構成されます。

インターネット キー エクスチェンジ（IKE）

インターネット キー エクスチェンジ（IKE）は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション（SA）を自動的に確立するために使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ2で安全に通信できるようになります。フェーズ2のネゴシエーションでは、IKEによってIPsecなどの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE ポリシーは、2 つのピアが、ピア間の IKE ネゴシエーションの安全性を確保するために使用する一連のアルゴリズムです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティ パラメータが後続の IKE ネゴシエーションを保護するかを規定します。 IKE バージョン 1（IKEv1）の場合、IKEポリシーには単一セットのアルゴリズムとモジュラス グループが含まれます。IKEv1とは異なり、IKEv2 ポリシーでは、フェーズ 1 ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラス グループを選択できます。単一の IKE ポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間 VPN の場合は、単一の IKE ポリシーを作成できます。

IKE ポリシーを定義するには、次を指定します。

- 固有の優先順位（1 ～ 65,543、1 が最高の優先順位）。
- データを保護し、プライバシーを確保するための IKE ネゴシエーションの暗号化方式。
- 送信者のIDを保証し、メッセージが伝送中に変更されないように確保するためのハッシュ メッセージ認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれる）。
- IKEv2 の場合、IKEv2 トンネル暗号化に必要なキーの材料とハッシュ操作を派生させるためのアルゴリズムとして使用される個別の擬似乱関数（PRF）。オプションは、ハッシュ アルゴリズムで使用されているものと同じです。

- 暗号化キー判別アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュ キーを派生させます。
- ピアの ID を保証するための認証方式。

（注） 認証には事前共有キーのみが使用されます。

- デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKE ネゴシエーションが開始すると、ネゴシエーションを開始するピアはリモート ピアにすべてのポリシーを送信し、リモート ピアは優先順位順に自身のポリシーとの一致を検索します。ピアが、暗号化、ハッシュ（IKEv2 の場合は整合性と PRF）、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが同じでない場合は、リモート ピア ポリシーの短い方のライフタイムが適用されます。デフォルトでは、Firepower Management Center は、正常なネゴシエーションを確保するために、すべての VPN エンドポイントに対して IKEv1 ポリシーを最低優先順位で展開します。

IPsec

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2 つのピア間のセキュアで論理的な通信パスです。IPSec トンネルを通過するトラフィックは、セキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

IPsec プロポーザル ポリシーは、IPsec トンネルに必要な設定を定義します。IPsec プロポーザルとは、デバイスの VPN インターフェイスに適用される 1 つ以上の暗号マップの集合です。暗号マップには、IPsec 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。これらのコンポーネントには以下のものがあります。

- プロポーザル（またはトランスフォーム セット）とは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせです。IPsec セキュリティ アソシエーション（SA）ネゴシエーション中に、ピアでは、両方のピアに共通するプロポーザルが検索されます。そのようなプロポーザルが検出されると、そのプロポーザルを適用して、その暗号マップのアクセス リストでデータ フローを保護する SA が作成され、VPN でトラフィックが保護されます。IKEv1 と IKEv2 には別個の IPsec プロポーザルがあります。IKEv1 プロポーザル（トランスフォーム セット）では、パラメータごとに 1 つの値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに複数の暗号化アルゴリズムと統合アルゴリズムを設定できます。
- 暗号マップには、IPsec ルール、プロポーザル、リモート ピア、IPsec SA を定義するために必要なその他のパラメータを含む、IPsec セキュリティ アソシエーション（SA）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つの互換暗号マップエントリが必要です。

不明なリモート ピアがローカル ハブとの間の IPsec セキュリティ アソシエーションの開始を試みた場合、ダイナミック暗号マップ ポリシーがサイト間 VPN で使用されます。ハブは、セキュリティ アソシエーション ネゴシエーションを開始できません。ダイナミック暗号ポリシーを使用することによって、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間でIPsecトラフィックを交換できます。実質的には、ダイナミック暗号マップポリシーによって、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 スポークおよび完全メッシュ VPN トポロジでのみ適用されます。ポイントツーポイントまたはフルメッシュ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。ポイントツーポイント トポロジでダイナミック暗号マップ ポリシーをエミュレートするには、2つのデバイスでハブアンドスポーク トポロジを作成します。スポークのダイナミック IP アドレスを指定して、このトポロジでダイナミック暗号マップを有効にします。

VPN パケット フロー

Firepower Threat Defense デバイスでは、デフォルトでは、明示的な許可なしにいずれのトラフィックもアクセス コントロールを通過できません。VPN トンネル トラフィックも、Snort を通過するまでは、エンドポイントにリレーされません。着信トンネルパケットは復号されてから、Snort プロセスへ送信されます。Snort は、暗号化の前に発信パケットを処理します。

VPN トンネルのエンドポイント ノードごとに保護されたネットワークを識別するアクセス制御は、どのトラフィックが Firepower Threat Defense デバイスをパス スルーしてエンドポイントに到達できるかを決定します。リモート アクセス VPN トラフィックでは、グループ ポリシー フィルタまたはアクセス制御ルールを、VPN トラフィック フローを許可するように設定する必要があります。

さらに、システムは、トンネルがダウンしている場合は、トンネル トラフィックをパブリックなソースに送信しません。

VPN ライセンス

Firepower Threat Defense VPN を有効にするための特別なライセンスはありません。デフォルトで利用可能です。

Firepower Management Center は、スマート ライセンス サーバから提供される属性に基づいて、Firepower Threat Defense デバイスで強力な暗号の使用を許可するかブロックするかを決定します。

これは、Cisco Smart License Manager に登録するときにデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。

VPN 接続の安全性を確保する方法

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーサルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、トンネルに適用する暗号化が強力なほど、システム パフォーマンスは低下します。効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、使用可能なオプションについて説明します。

セキュリティ証明書要件の遵守

多数の VPN 設定には、さまざまなセキュリティ認証規格に準拠するためのオプションがあります。認定要件と使用可能なオプションを確認して、VPN 構成を計画します。コンプライアンスに関連する追加のシステム情報については、セキュリティ認定準拠 を参照してください。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルに使用する暗号化アルゴリズムを決定する際、選択肢は VPN のデバイスでサポートされるアルゴリズムに限られます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティ プロトコル（ESP）によってアルゴリズムが使用されます。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の前に ESP というプレフィックスが付けられます。

デバイス ライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

- AES-GCM—（IKEv2 のみ）Galois/カウンタ モードの Advanced Encryption Standard は、機密性、データの発信元の認証を提供する操作のブロック暗号モードであり、AES よりも優れたセキュリティを提供します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCM は NSA Suite B をサポートするために必要となる AES モードです。NSA Suite B は、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。.
- AES-GMAC—（IKEv2 IPsec プロポーザルのみ）。Advanced Encryption Standard のガロアメッセージ認証コード（GMAC）は、データ発信元認証だけを行う操作のブロック暗号モードです。これは AES-GCM の一種であり、データを暗号化せずにデータ認証が行えます。AES-GMAC には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。
- AES（Advanced Encryption Standard）は DES よりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算的には 3DES よりも効率的です。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- 3DES（トリプル DES）：56 ビット キーを使用して暗号化を 3 回行います。異なるキーを使用してデータの各ブロックを 3 回処理するため、DES よりも安全です。ただし、使用するシステム リソースが多くなり、DES よりも速度が遅くなります。
- DES（データ暗号化標準）：56 ビット キーを使用して暗号化する対称秘密鍵ブロック アルゴリズムです。3DES よりも高速であり、使用するシステム リソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステム リソースや速度が重要である場合には、DES を選択します。
- Null：ヌル暗号化アルゴリズムは暗号化なしで認証します。通常はテスト目的にのみ使用されます。

使用するハッシュ アルゴリズムの決定

IKE ポリシーでは、ハッシュ アルゴリズムがメッセージ ダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数（PRF）に使用されます。

IPsec プロポーザルでは、ハッシュ アルゴリズムは Encapsulating Security Protocol（ESP）による認証に使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名の接頭辞が「ESP-」となり、「-HMAC」（Hash Method Authentication Code）という接尾辞も使用されます。

IKEv2 では、複数のハッシュ アルゴリズムを設定できます。各設定が、安全性の高い順に順序付けられ、ピアとのネゴシエーションにはこの順序が使用されます。IKEv1 では、1 つのオプションしか選択できません。

選択可能なハッシュ アルゴリズムは、次のとおりです。

- SHA (Secure Hash Algorithm)：160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。

  Standard SHA（SHA1）は 160 ビットのダイジェストを生成します。

  IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現することができます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。

  - SHA256：256 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA384：384 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA512：512 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。

- [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 は処理時間が短いため、全体的なパフォーマンスが SHA より高速ですが、SHA より強度は低いと考えられています。
- NULL またはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）NULL ハッシュ アルゴリズム。通常はテスト目的のみに使用されます。しかし、暗号化オプションとしていずれかの AES-GCM/GMAC オプションを選択した場合は、NULL 整合性アルゴリズムを選択する必要があります。NULL 以外のオプションを選択した場合、これらの暗号化標準に対しては、整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec Security Association（SA：セキュリティ アソシエーション）キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。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。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択する場合は、AES で必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH：デフィーヘルマン）グループ 5 以降を使用する必要があります。IKEv1 ポリシーではグループ 1、2、5 のみ許可されます。

NSA Suite-B の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman（ECDH）オプション：19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

- 1：Diffie-Hellman グループ 1（768 ビット係数）。

- 2：Diffie-Hellman グループ 2（1024 ビット係数）。
- 5：Diffie-Hellman グループ 5（1536 ビット係数）。128 ビットのキーでは十分な保護レベルです。
- 14：Diffie-Hellman グループ 14（2048 ビット係数）。192 ビットのキーでは十分な保護レベルです。
- 19：Diffie-Hellman グループ 19（256 ビット楕円曲線）。
- 20：Diffie-Hellman グループ 20（384 ビット楕円曲線）。
- 21：Diffie-Hellman グループ 21（521 ビット楕円曲線）。
- 24：Diffie-Hellman グループ 24（2048 ビット係数および 256 素数位数サブグループ）。

使用する認証方式の決定

事前共有キーとデジタル証明書は、VPN で使用可能な認証方法です。

サイト間、IKEv1 および IKEv2 VPN 接続では、両方のオプションを使用できます。

SSL および IPsec IKEv2 のみを使用するリモート アクセスでは、デジタル証明書認証だけがサポートされます。

事前共有キーを使用すると、秘密鍵を 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていない場合は、IKE SA を確立できません。

デジタル証明書は IKE キー管理メッセージの署名や暗号化に RSA キー ペアを使用します。証明書によって、2 つのピア間の通信の否認防止を実施します。つまり、実際に通信が行われたことを証明できます。この認証方式を使用する場合、ピアが証明機関（CA）からデジタル証明書を取得できるように Public Key Infrastructure（PKI）を定義する必要があります。CA は参加するネットワーク デバイスの証明書要求を管理し、証明書の発行を行うことで、すべての参加デバイスの Centralized Key Management を行っています。

事前共有キーの拡張性は高くありませんが、CA を使用することによって IPsec ネットワークの管理性や拡張性が高まります。CA を使用する場合は、すべての暗号化デバイス間でキーを設定する必要がありません。代わりに、参加する各デバイスは CA に登録され、CA に対して証明書を要求します。自身の証明書と CA の公開キーを持つ各デバイスは、その CA のドメイン内にある他のすべてのデバイスを認証できます。

事前共有キー

事前共有キーにより、秘密キーを 2 つのピアの間で共有できます。このキーは、認証フェーズで IKE が使用します。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていなければ、IKE SA を確立できません。

事前共有キーを設定するには、手動または自動生成されたキーを使用するかどうかを選択し、IKEv1/IKEv2 オプションでキーを指定します。これにより、設定の展開時に、トポロジ内のすべてのデバイス上に共有キーが設定されます。

PKI インフラストラクチャとデジタル証明書

公開キー インフラストラクチャ

PKI では、参加ネットワーク デバイスのキーを一元管理できます。PKI は、一般にデジタル証明書 と呼ばれる公開キー証明書 を生成、検証、失効することで公開キー暗号化 をサポートするポリシー、プロシージャ、権限の定義済みセットです。

公開キー暗号化では、接続の各エンドポイントが公開キーと秘密キーの両方からなるキー ペアを保持します。キー ペアは、VPN エンドポイントがメッセージに署名して暗号化するために使用します。これらのキーは相互に補完し合い、一方のキーで暗号化されたものはもう一方のキーでしか復号できません。この仕組みにより、接続で送受信されるデータを保護します。

署名と暗号化の両方に使用される汎用 RSA または ECDSA キー ペアを生成するか、署名用と暗号化用に別々のキー ペアを生成します。署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。SSL は署名用ではなく暗号化用にキーを使用しますが、IKEは暗号化ではなく署名にキーを使用します。キーを用途別に分けることで、キーの公開頻度が最小化されます。

デジタル証明書

デジタル証明書を VPN 接続の認方式として使用する場合、ピアはデジタル証明書を認証局（CA）から取得するように設定されます。CAは、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。

CA サーバは公開 CA 証明書要求を管理し、参加ネットワーク デバイスに公開キー インフラストラクチャ（PKI）の一部として証明書を発行します。このアクティビティは、証明書の登録と呼ばれます。これらのデジタル証明書は、アイデンティティ証明書とも呼ばれています。デジタル証明書の内容は以下のとおりです。

- 認証のための所有者のデジタル識別（名前、シリアル番号、会社、部署、IP アドレスなど）。
- 証明書所有者に対して暗号化データを送受信するために必要な公開キー。
- CA のセキュアなデジタル署名。

また、証明書によって、2 つのピア間の通信の否認が防止されます。つまり、実際に通信が行われたことを証明できます。

証明書の登録

PKIを使用すると、すべての暗号化デバイス間で事前に共有するキーを設定する必要がなくなるため、VPNをもっと容易に管理できるようになり、スケーラビリティが高まります。代わりに、参加する各デバイスを CA サーバに個別に登録します。CA サーバは、アイデンティティを検証し、デバイスのアイデンティティ証明書を作成することを明示的に信任されています。登録が完了すると、参加する各ピアは、もう一方の参加するピアにアイデンティティ証明書を送信し、証明書に含まれる公開キーでそのアイデンティティを検証して、暗号化セッションを

確立できるようにします。Firepower Threat Defense デバイスの登録の詳細については、証明書の登録オブジェクトを参照してください。

認証局証明書

ピアの証明書を検証するには、参加デバイスのそれぞれが CA の証明書をサーバから取得する必要があります。CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。この証明書に含まれる CA の公開キーを使用して、CA のデジタル署名および受信したピアの証明書の内容を復号して検証します。CA 証明書は次の方法で取得可能です。

- Simple Certificate Enrollment Protocol（SCEP）を使用して、CA サーバから CA の証明書を取得します。
- 別の参加デバイスから CA の証明書を手動でコピーします。

トラストポイント

登録が完了すると、管理対象デバイス上にトラストポイントが作成されます。トラストポイントは、CA および関連する証明書を表すオブジェクトです。トラストポイントには、CA の ID、CA 固有のパラメータ、単一の登録済みアイデンティティ証明書とのアソシエーションが含まれています。

PKCS#12 ファイル

PKCS#12（PFX）ファイルとは、サーバ証明書、中間証明書、秘密キーのすべてを暗号化して保持するファイルです。このタイプのファイルをデバイスに直接インポートして、トラストポイントを作成できます。

失効チェック

さらに CA は、ネットワークに参加しなくなったピアの証明書を無効にすることもできます。失効した証明書は、オンライン証明書ステータス プロトコル（OCSP）サーバによって管理されるか、LDAP サーバに格納されている証明書失効リスト（CRL）に含まれます。ピアは、別のピアからの証明書を受け入れる前に、これらを検査できます。

VPN トポロジ オプション

新しい VPN トポロジを作成するには、最低でも、固有の名前をつけ、トポロジの型を特定し、IKE バージョンを選択する必要があります。それぞれが VPN トンネル グループを含む 3 つの型のトポロジから選択できます。

- ポイントツーポイント（PTP）トポロジでは、2 つのエンドポイント間に VPN トンネルを確立します。
- ハブおよびスポーク トポロジは、ハブ エンドポイントをスポーク エンドポイントのグループに接続する VPN トンネル グループを確立します。

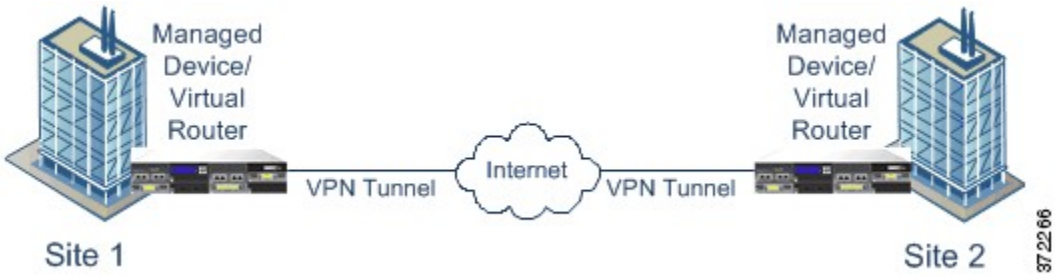
- フル メッシュのトポロジは、エンドポイントのセットの間で VPN トンネルのグループを確立します。

VPN認証の事前共有キーを手動または自動で定義します。デフォルトのキーはありません。自動を選択すると、Firepower Management Center は事前共有キーを生成して、そのキーをトポロジ内のすべてのノードに割り当てます。

ポイントツーポイントの VPN トポロジ

ポイントツーポイントのVPNトポロジでは、2つのエンドポイントが相互に直接通信します。2つのエンドポイントをピアデバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。

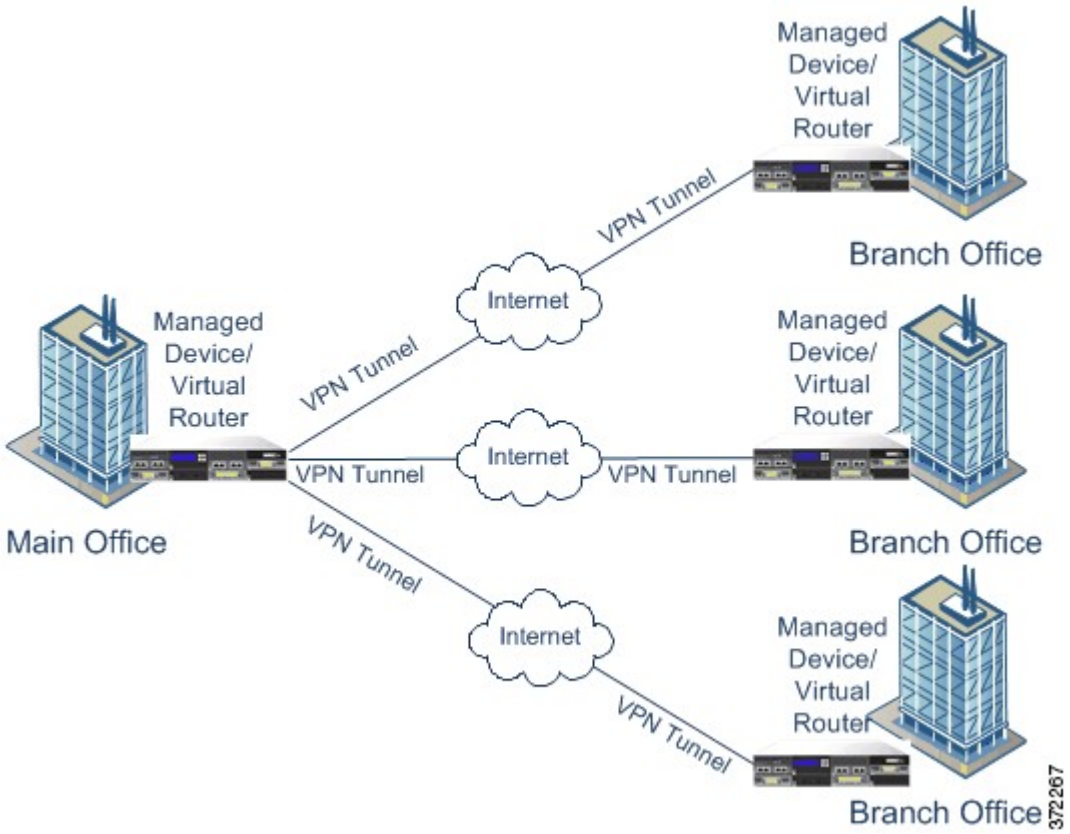


ハブ アンド スポーク VPN トポロジ

ハブ アンド スポーク VPN トポロジでは、中央のエンドポイント（ハブ ノード）が複数のエンドポイント（スポーク ノード）と接続します。ハブ ノードと個々のスポーク エンドポイント間のそれぞれの接続は、別の VPN トンネルです。いずれかのスポーク ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

ハブアンドスポーク トポロジは一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本社とブランチ オフィスを接続する VPN を表します。これらの展開は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。一般的に、ハブ ノードは本社に配置します。スポーク ノードはブランチ オフィスに配置し、大半のトラフィックはここから開始されます。

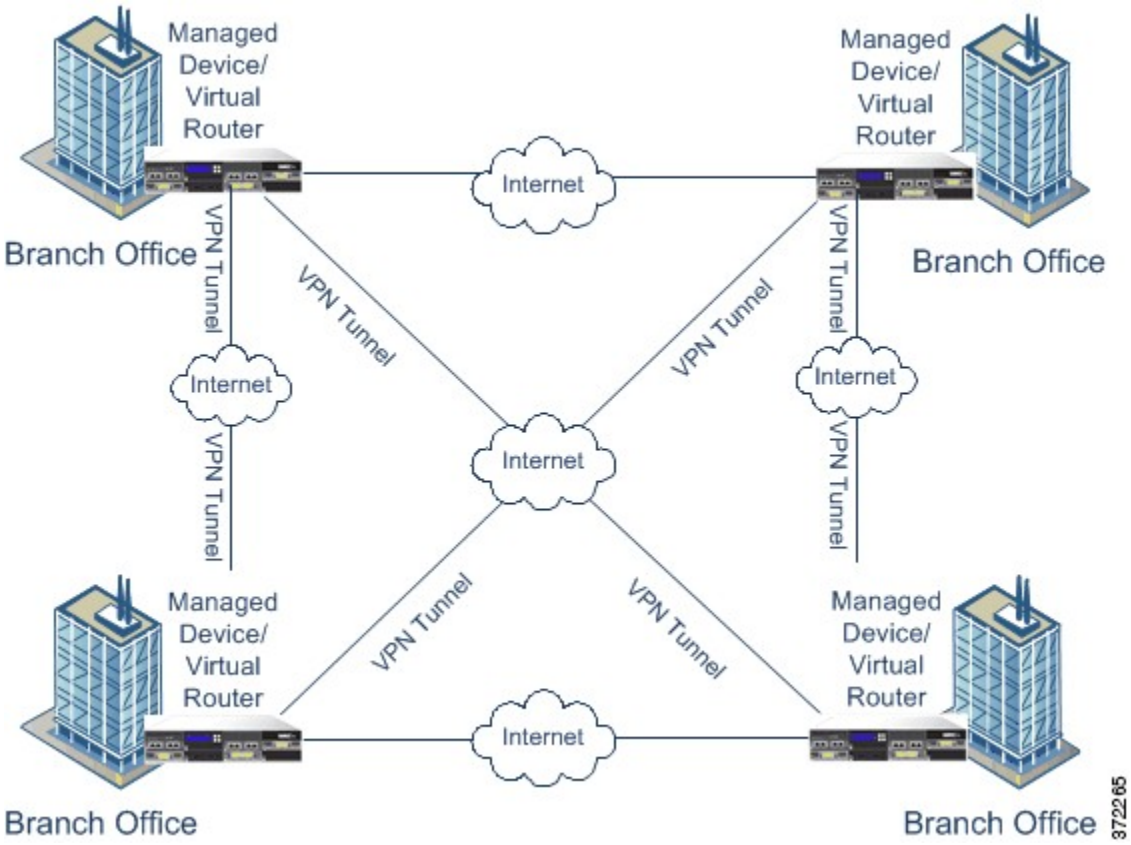
次の図は、一般的なハブ アンド スポーク VPN トポロジを示しています。



フル メッシュ VPN トポロジ

フル メッシュ VPN トポロジでは、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。このトポロジにより、あるエンドポイントで障害が発生しても、残りのエンドポイントの相互通信は維持されるように冗長性が提供されます。これは、一般的に分散したブランチ オフィスが配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。

次の図は、一般的なフル メッシュ VPN トポロジを示しています。



暗黙的トポロジ

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

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