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、Secure Firewall 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。

VPN タイプ

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

- Firewall 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。

  Secure Firewall Threat Defense デバイスは SSL 経由のリモート アクセス VPN または Firewall 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。Firewall

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。

Secure Firewall Threat Defense セキュア ゲートウェイは、Secure Client 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。

- Firewall 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。

VPN の基本

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモートユーザと企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

IPsec ベースの VPN テクノロジーは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリング標準を使用して、トンネルの構築と管理を行います。ISAKMP と IPsec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション。
- 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。
- トンネル経由のデータ転送の管理。
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理。

VPN内のデバイスは、双方向の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てカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプ

セル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

サイト間 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が、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します。接続は、2 つのゲートウェイの IP アドレスとホスト名、それらの背後のサブネット、2 つのゲートウェイが相互認証に使用する方式で構成されます。

ハブ：1つ以上のリモートブランチデバイスまたはスポークとの間でセキュアなVPN接続を可能にするデバイスです。ハブは、スポーク同士が相互通信するためのゲートウェイとしても機能します。

スポーク：VPNを介してハブに接続し、ハブの背後にある企業リソースにセキュアにアクセスするデバイスです。スポーク同士は、ハブを介して相互に通信します。

Internet Key Exchange（IKE）

インターネット キー交換（IKE）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、およびセキュリティ アソシエーション（SAs）の自動的な確立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 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。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）では、IKEポリシーに、単一のアルゴリズムのセットと係数グループが含まれています。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。IKEv1 と IKEv2 はどちらも、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。

IKE ポリシーを定義するには、次を指定します。

- 一意の優先順位（1 ～ 65,543、1 が最高優先順位）。
- データを保護して、プライバシーを確保するための IKE ネゴシエーション用の暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証するハッシュ 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ます）。

- IKEv2 では、別個の疑似乱数関数（PRF）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していました。オプションは、ハッシュ アルゴリズムに使用されるものと同じです。
- 暗号キー決定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、暗号キーとハッシュ キーを導き出します。
- ピアの ID を保証するための認証方式。
- 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されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。暗号化、ハッシュ（IKEv2 の場合、整合性と PRF）、認証、および Diffie-Hellman 値が同じで、SA ライフタイムが、送信されたポリシーのライフタイム以下の場合に、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、リモート ピア ポリシーから取得した短い方のライフタイムが適用されます。デフォルトでは、Secure Firewall 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。

（注） Firepower Threat Defense（FTD）でのリモートアクセス VPN とサイト間 VPN の両方の同じインターフェイスでは、同時 IKEv2 ダイナミッククリプトマップはサポートされていません。

VPN パケット フロー

Firewall 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 Firewall 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。

IPsec フローのオフロード

IPsec フローのオフロードを使用するように、サポートするデバイスモデルを設定できます。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。

オフロード操作は、特に、入力の事前復号および復号処理と出力の事前暗号化および暗号化処理に関連しています。システムソフトウェアは、セキュリティポリシーを適用するための内部フローを処理します。

IPsec フローのオフロードはデフォルトで有効になっており、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 3100

IPsec フローのオフロードに関する制約事項

次の IPsec フローはオフロードされません。

- IKEv1 トンネル。IKEv2 トンネルのみがオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- ボリュームベースのキー再生成が設定されているフロー。
- 圧縮が設定されているフロー。
- トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
- AH 形式。ESP/NAT-T 形式のみがサポートされます。
- ポストフラグメンテーションが設定されているフロー。
- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。
- ファイアウォールフィルタが有効になっているフロー。
- マルチインスタンス モード。

IPsec フローのオフロードの設定

IPsec フローのオフロードは、この機能をサポートするハードウェア プラットフォームではデフォルトで有効になっています。設定を変更するには、FlexConfig を使用して **flow-offload-ipsec** コマンドを実装します。このコマンドの詳細については、ASA コマンドリファレンスを参照してください。

VPN ライセンス

Secure Firewall 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。

Firewall Management Center は、スマートライセンスサーバーから提供される属性に基づいて、Firewall 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。

評価ライセンスを使用して VPN 構成を作成し、ライセンスを評価版から輸出規制により機能が限定されたスマートライセンスにアップグレードした場合は、暗号化アルゴリズムを確認および更新して暗号化を強化し、VPN が適切に機能するようにしてください。DES ベースの暗号化はサポートされなくなりました。

VPN 接続をセキュアにする方法

通常、VPN トンネルはインターネットなどのパブリック ネットワークを通過するため、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 プロポーザルの使用を適用するために、暗号化とその他のセキュリティ テクニックを定義します。

デバイスライセンスで強力な暗号化の適用が可能な場合は、さまざまな暗号化アルゴリズム、ハッシュ アルゴリズム、Diffie-Hellman グループから選択することができます。ただし、一般的なルールとして、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。効率を犠牲にすることなく十分な保護を提供するようにセキュリティとパフォーマンスのバランスを取る必要があります。

オプションの選択肢に関する特定のガイダンスを示すことはできませんが、大規模な企業や組織で運用する場合は、すでに標準が定義されていることがあります。そうでない場合は、時間をかけてオプションを検討してください。

ここでは、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。

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 プロポーザルで使用する暗号化アルゴリズムを決定する場合は、選択肢が VPN 内のデバイスによってサポートされているアルゴリズムに限られます。

IKEv2 の場合は、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の順に並べ、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 の場合は、1 つのオプションしか選択できません。

IPsec プロポーザルの場合、このアルゴリズムはカプセル化セキュリティ プロトコル（ESP）で使用されます。これは、認証サービス、暗号化サービス、アンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の先頭に ESP- が付けられます。

デバイスライセンスが強力な暗号化に対応している場合は、次の暗号化アルゴリズムの中から選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

（注） 強力な暗号化の対象である場合、評価ライセンスをスマートライセンスにアップグレードする前に、暗号化アルゴリズムを確認および更新して暗号化を強化し、VPN設定が適切に機能するようにしてください。AESベースのアルゴリズムを選択します。強力な暗号化をサポートするアカウントを使用して登録されている場合、DES はサポートされません。登録後は、DES の使用対象をすべて削除するまで変更を展開できません。

- AES-GCM—（IKEv2 のみ）ガロア/カウンタ モードの Advanced Encryption Standard は、機密性とデータ発信元認証を提供するブロック暗号モードの操作であり、AES より優れたセキュリティを実現します。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な AES のモードです。NSA Suite B は暗号強度に関する連邦規格を満たすためにデバイスがサポートすべき暗号化アルゴリズムのセットです。。
- AES：Advanced Encryption Standard は、DES よりも優れたセキュリティを提供し、3DES よりも効率的に計算する対称暗号アルゴリズムです。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。
- DES：56 ビットのキーを使用して暗号化するデータ暗号化規格（Data Encryption Standard）は、対称秘密キー ブロック アルゴリズムです。ライセンスアカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。
- NULL、ESP-NULL：使用しないでください。NULL 暗号化アルゴリズムは、暗号化を使用しない認証を提供します。通常はテスト目的にのみ使用されます。ただし、仮想および Firepower 2100 を含む多くのプラットフォームではまったく動作しません。

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（整合性アルゴリズム用に 1 つと Pseudo-Random Function（PRF; 疑似乱数関数）用に 1 つ）に分かれています。

IPsec プロポーザルでは、ハッシュ アルゴリズムが、認証用のカプセル化セキュリティ プロトコル（ESP）で用されます。IKEv2 IPsec プロポーザルでは、これが整合性ハッシュと呼ばれています。IKEv1 IPsec プロポーザルでは、アルゴリズム名の先頭に ESP- が付けられ、末尾に -HMAC（「ハッシュ法認証コード」を意味する）が付けられます。

IKEv2 の場合は、複数のハッシュ 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の順に並べ、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 の場合は、1 つのオプションしか選択できません。

次のハッシュ アルゴリズムから選択できます。

- [SHA (Secure Hash Algorithm)]：標準の SHA（SHA1）は、160 ビットのダイジェストを生成します。

  よりセキュアな次の SHA-2 オプションを IKEv2 設定に使用できます。NSA Suite B 暗号化仕様を実装する場合は、次のいずれかを選択します。

  - SHA256：256 ビットのダイジェストでセキュア 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でセキュア 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でセキュア ハッシュ アルゴリズム SHA 2 を指定します。

- ヌルまたはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）。ヌル ハッシュ アルゴリズムは、通常、テスト目的にのみ使用されます。しかし、暗号化オプションとしていずれかの AES-GCM 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。ヌル以外のオプションを選択した場合でも、これらの暗号化標準で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 セキュリティ アソシエーション（SA）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 暗号化を選択した場合は、AES に必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH）グループ 5 以上を使用する必要があります。IKEv1 ポリシーは、以下に示すすべてのグループをサポートしているわけではありません。

NSA Suite B 暗号化仕様を実装するには、IKEv2 を使用し、楕円曲線 Diffie-Hellman（ECDH）オプション（19、20、または21）のいずれかを選択します。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の順に並べ、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 の場合は、1 つのオプションしか選択できません。

- 14：Diffie-Hellman グループ 14（2048 ビット Modular Exponential（MODP）グループ）。192 ビットのキーでは十分な保護レベルです。
- 15：Diffie-Hellman グループ 15（3072 ビット MODP グループ）。
- 16：Diffie-Hellman グループ 16（4096 ビット MODP グループ）。

- 19：Diffie-Hellman グループ 19（国立標準技術研究所（NIST）256 ビット楕円曲線モジュロプライム（ECP）グループ）。
- 20：Diffie-Hellman グループ 20（NIST 384 ビット ECP グループ）。
- 21：Diffie-Hellman グループ 21（NIST 521 ビット ECP グループ）。
- 31：Diffie-Hellman グループ 31（Curve25519 256 ビット EC 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、証明書を発行することで、すべての参加デバイスの Centralized Key Management を行います。

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

事前共有キーを使用すると、2 つのピア間で秘密キーを共有できます。IKE は、このキーを認証フェーズで使用します。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い場合は、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、ECDSA、またはEDDSAキーペアを生成するか、署名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。

デジタル証明書またはアイデンティティ証明書

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 サーバーに個別に登録します。CA サーバーは、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。Firewall 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）または Enrollment over Secure Transport（EST）を使用して、CA サーバーから 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、サーバー証明書、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。

削除または廃止されたハッシュアルゴリズム、暗号化アルゴリズム、および Diffie-Hellman モジュラスグループ

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 および IKEv2 では廃止されました。
- 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引き続きサポートされます。

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。

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。

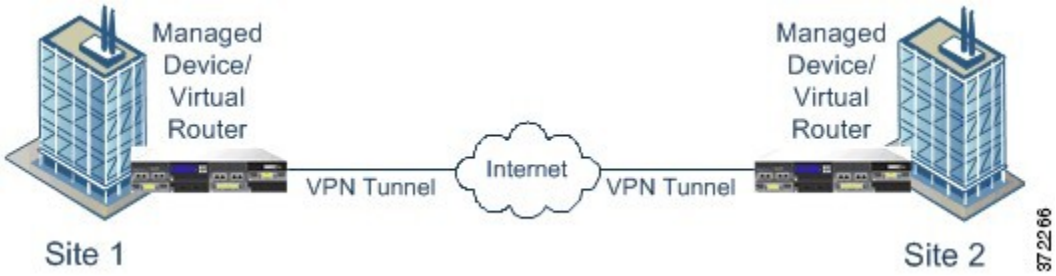
- ポイントツーポイント（PTP）トポロジでは、2 つのエンドポイント間に VPN トンネルを確立します。
- ハブおよびスポーク トポロジは、ハブ エンドポイントをスポーク エンドポイントのグループに接続する VPN トンネル グループを確立します。
- フル メッシュのトポロジは、エンドポイントのセットの間で VPN トンネルのグループを確立します。

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、Secure Firewall 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。

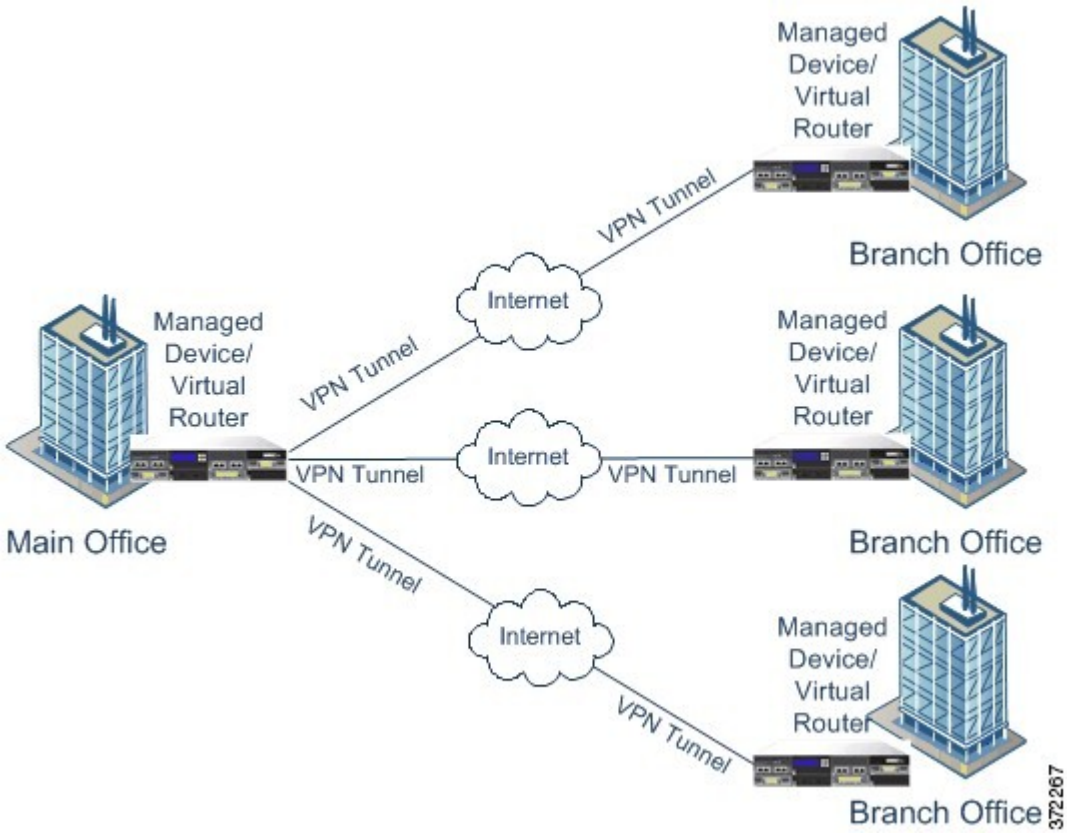


ハブ アンド スポーク VPN トポロジ

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。

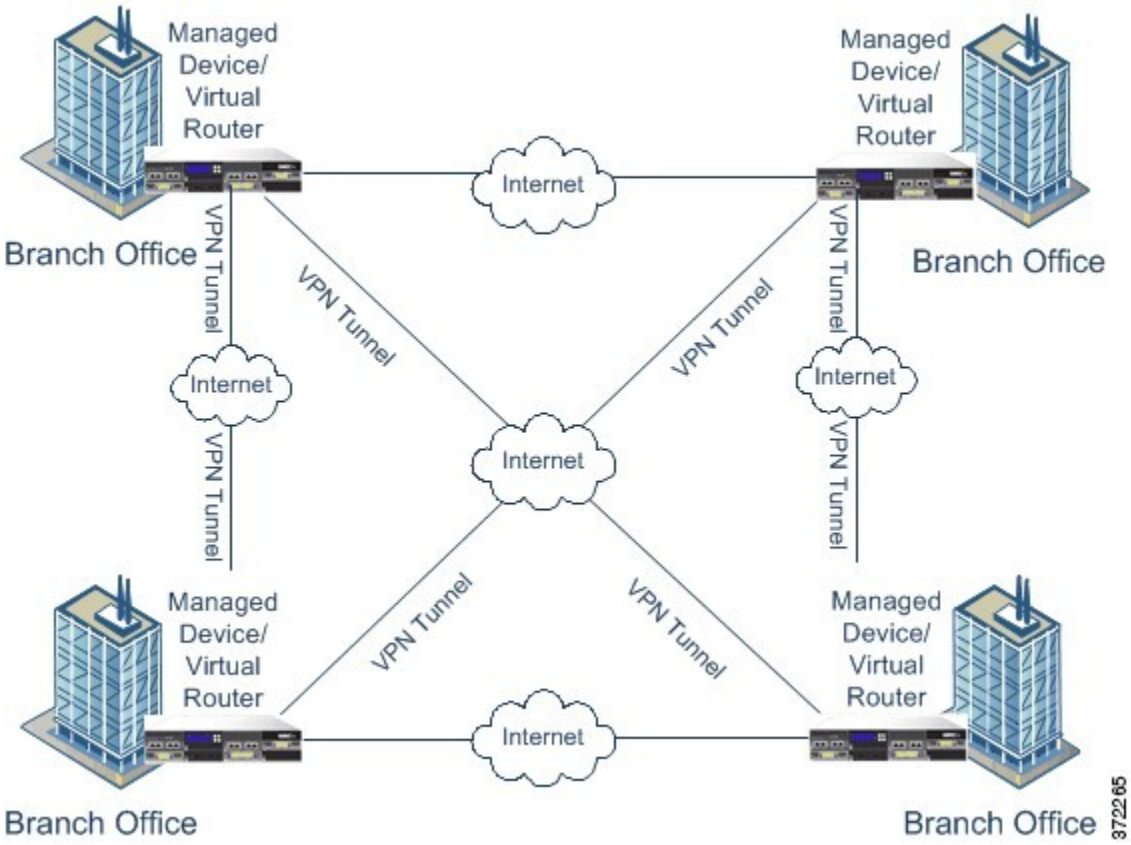
次の図は、一般的なハブ アンド スポーク VPN トポロジを示しています。



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。

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。