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。

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 Flow Offload

You can configure supporting device models to use IPsec flow offload. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the

field-programmable gate array (FPGA) in the device, which should improve device performance. On the Secure Firewall 1200 series, IPsec connections are offloaded to the Marvell Cryptographic Accelerator (CPT) to improve device performance.

Offloaded operations specifically relate to the pre-decryption and decryption processing on ingress, and the pre-encryption and encryption processing on egress. The system software handles the inner flow to apply your security policies.

IPsec flow offload is enabled by default, and applies to the following device types:

- Secure Firewall 1200
- Secure Firewall 3100
- Secure Firewall 4200

IPsec flow offload is also used when the device's VTI loopback interface is enabled.

Limitations for IPsec Flow Offload

The following IPsec flows are not offloaded:

- IKEv1 tunnels. Only IKEv2 tunnels will be offloaded. IKEv2 supports stronger ciphers.
- Flows that have volume-based rekeying configured.
- Flows that have compression configured.
- Transport mode flows. Only tunnel mode flows will be offloaded.
- AH format. Only ESP/NAT-T format will be supported.
- Flows that have post-fragmentation configured.
- Flows that have anti-replay window size other than 64bit and anti-replay is not disabled.
- Flows that have firewall filter enabled.
- Mult-instance mode.

Configure IPsec Flow Offload

IPsec flow offload is enabled by default on hardware platforms that support the feature. To change the configuration, use FlexConfig to implement the **flow-offload-ipsec** command. See the ASA command reference for detailed information about the command.

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。

How Secure Should a VPN Connection Be?

Because a VPN tunnel typically traverses a public network, most likely the Internet, you need to encrypt the connection to protect the traffic. You define the encryption and other security techniques to apply using IKE polices and IPsec proposals.

If your device license allows you to apply strong encryption, there is a wide range of encryption and hash algorithms, and Diffie-Hellman groups, from which to choose. However, as a general rule, the stronger the encryption that you apply to the tunnel, the worse the system performance. Find a balance between security and performance that provides sufficient protection without compromising efficiency.

We cannot provide specific guidance on which options to choose. If you operate within a larger corporation or other organization, there might already be defined standards that you need to meet. If not, take the time to research the options.

The following topics explain the available options.

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。

Deciding Which Encryption Algorithm to Use

When deciding which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN.

For IKEv2, you can configure multiple encryption algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

For IPsec proposals, the algorithm is used by the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-.

If your device license qualifies for strong encryption, you can choose from the following encryption algorithms. If you are not qualified for strong encryption, you can select DES only.

（注） If you are qualified for strong encryption, before upgrading from the evaluation license to a smart license, check and update your encryption algorithms for stronger encryption so that the VPN configuration works properly. Choose AES-based algorithms. DES is not supported if you are registered using an account that supports strong encryption. After registration, you cannot deploy changes until you remove all uses of DES.

- AES-GCM—(IKEv2 only.) Advanced Encryption Standard in Galois/Counter Mode is a block cipher mode of operation providing confidentiality and data-origin authentication, and provides greater security than AES. AES-GCM offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance. GCM is a mode of AES that is required to support NSA Suite B. NSA Suite B is a set of cryptographic algorithms that devices must support to meet federal standards for cryptographic strength. .
- AES—Advanced Encryption Standard is a symmetric cipher algorithm that provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance.
- DES—Data Encryption Standard, which encrypts using 56-bit keys, is a symmetric secret-key block algorithm. If your license account does not meet the requirements for export controls, this is your only option.
- Null, ESP-Null—A null encryption algorithm provides authentication without encryption. This method is not secure; use at your own discretion.

Deciding Which Hash Algorithms to Use

In IKE policies, the hash algorithm creates a message digest, which is used to ensure message integrity. In IKEv2, the hash algorithm is separated into two options, one for the integrity algorithm, and one for the pseudo-random function (PRF).

In IPsec proposals, the hash algorithm is used by the Encapsulating Security Protocol (ESP) for authentication. In IKEv2 IPsec Proposals, this is called the integrity hash. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-, and there is also an -HMAC suffix (which stands for “hash method authentication code”).

For IKEv2, you can configure multiple hash algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

You can choose from the following hash algorithms.

- SHA (Secure Hash Algorithm)—Standard SHA (SHA1) produces a 160-bit digest.

  The following SHA-2 options, which are even more secure, are available for IKEv2 configurations. Choose one of these if you want to implement the NSA Suite B cryptography specification.

  - SHA256—Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
  - SHA384—Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
  - SHA512—Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

- Null or None (NULL, ESP-NONE)—(IPsec Proposals only.) A null Hash Algorithm; this is typically used for testing purposes only. However, you should choose the null integrity algorithm if you select one of the AES-GCM options as the encryption algorithm. Even if you choose a non-null option, the integrity hash is ignored for these encryption standards.

Deciding Which Diffie-Hellman Modulus Group to Use

You can use the following Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has a different size modulus. A larger modulus provides higher security, but requires more processing time. You must have a matching modulus group on both peers.

If you select AES encryption, to support the large key sizes required by AES, you should use Diffie-Hellman (DH) Group 5 or higher. IKEv1 policies do not support all of the groups listed below.

To implement the NSA Suite B cryptography specification, use IKEv2 and select one of the elliptic curve Diffie-Hellman (ECDH) options: 19, 20, or 21. Elliptic curve options and groups that use 2048-bit modulus are less exposed to attacks such as Logjam.

For IKEv2, you can configure multiple groups. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

- 14—Diffie-Hellman Group 14: 2048-bit modular exponential (MODP) group. Considered good protection for 192-bit keys.
- 15—Diffie-Hellman Group 15: 3072-bit MODP group.
- 16—Diffie-Hellman Group 16: 4096-bit MODP group.
- 19—Diffie-Hellman Group 19: National Institute of Standards and Technology (NIST) 256-bit elliptic curve modulo a prime (ECP) group.
- 20—Diffie-Hellman Group 20: NIST 384-bit ECP group.
- 21—Diffie-Hellman Group 21: NIST 521-bit ECP group.
- 31—Diffie-Hellman Group 31: Curve25519 256-bit EC Group.

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。

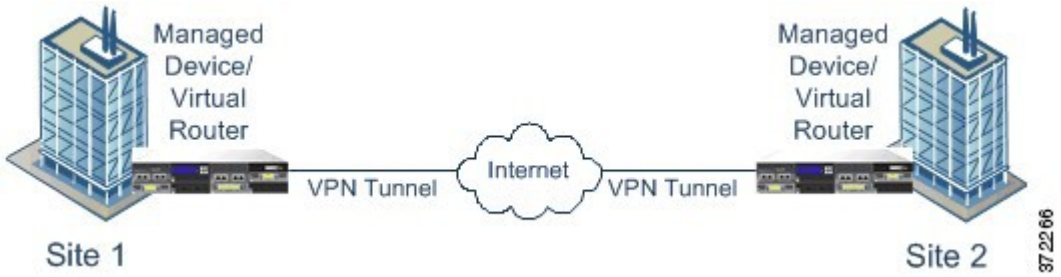
- フル メッシュのトポロジは、エンドポイントのセットの間で VPN トンネルのグループを確立します。

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。

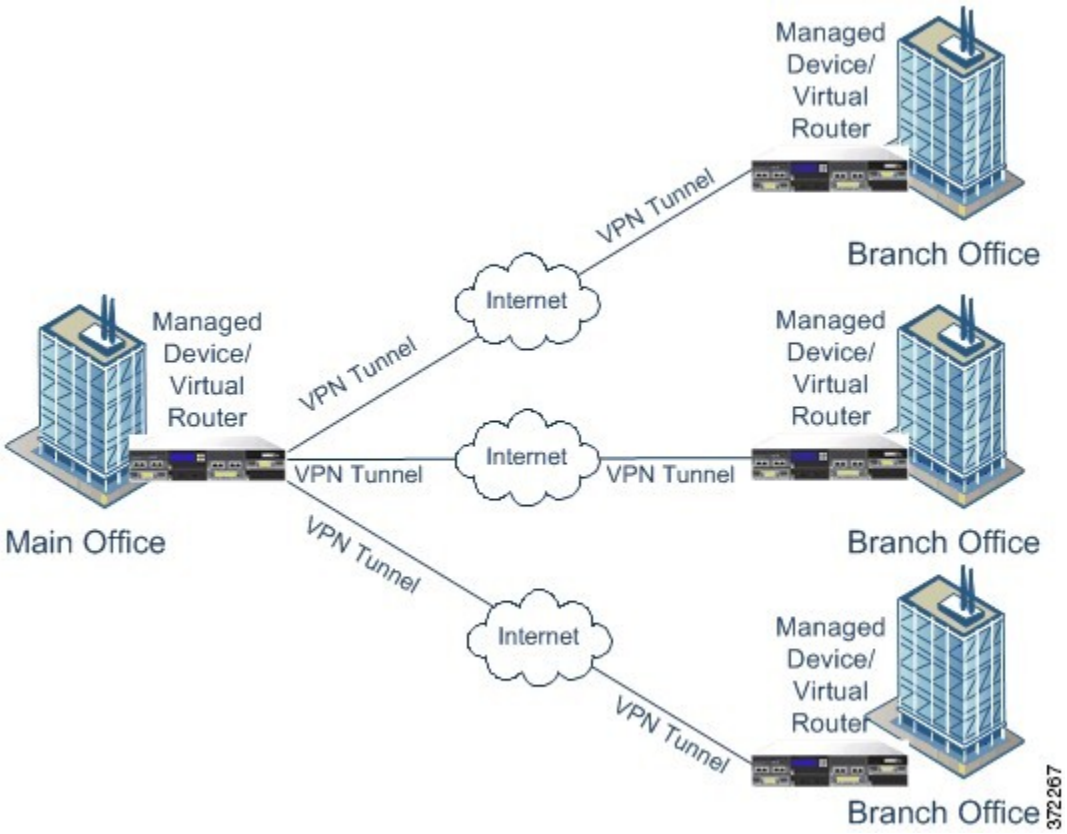


ハブ アンド スポーク VPN トポロジ

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。

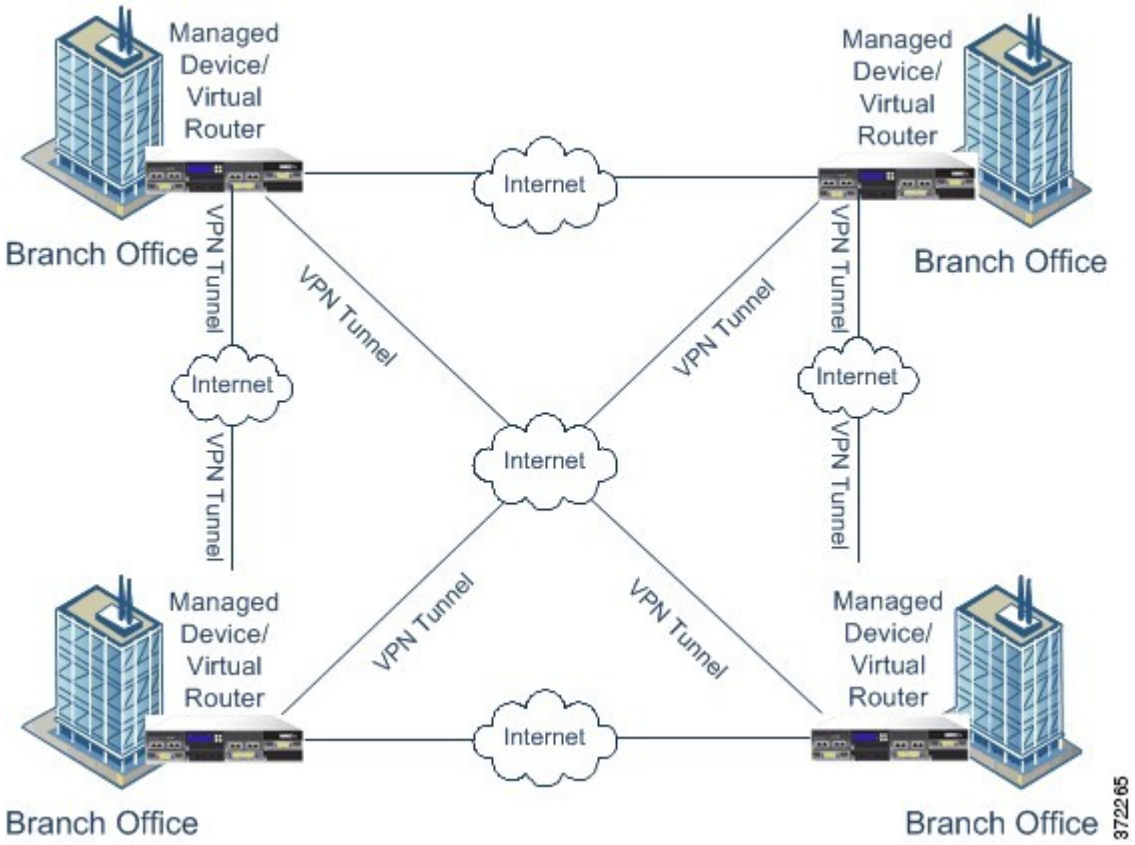
次の図は、一般的なハブ アンド スポーク VPN トポロジを示しています。



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。