ゲートウェイ VPN

次のトピックでは、VPN 展開を管理する方法について説明します。

ゲートウェイ VPN の基本

バーチャル プライベート ネットワーク（VPN）は、インターネットや他のネットワークなどのパブリック ソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。Firepower 管理対象デバイスの仮想ルータ間にセキュア VPN トンネルを確立するように Firepower システムを設定できます。システムは、インターネット プロトコル セキュリティ（IPsec）プロトコル スイートを使用してトンネルを構築します。

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。接続は、2 つのゲートウェイの IP アドレスとホスト名、その背後のサブネット、および相互認証のための 2 つのゲートウェイの共有秘密で構成されます。

VPN エンドポイントは、Internet Key Exchange（IKE）のバージョン 1 またはバージョン 2 のいずれかのプロトコルを使用して相互に認証し、トンネルに対してセキュリティ アソシエーションを作成します。システムは IPsec Authentication Header（AH）プロトコルまたは IPsec Encapsulating Security Payload（ESP）プロトコルのいずれかを使用して、トンネルに入るデータを認証します。ESP プロトコルは、AH と同じ機能を提供する他にデータの暗号化も行います。

展開にアクセス コントロール ポリシーが存在する場合、システムは、VPN トラフィックがアクセス コントロールを通過するまで VPN トラフィックを送信しません。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 を Firepower 用に設定して展開するには、展開先の各管理対象デバイスで VPN ライセンスを有効にしておく必要があります。また、VPN 機能は 7000 および 8000 シリーズ デバイスでのみ使用できます。

IPsec

IPsec プロトコル スイートは、VPN トンネルにおいて、IP パケットが ESP または AH セキュリティ プロトコルでどのようにハッシュ、暗号化、およびカプセル化されるかを定義します。Firepower システムはハッシュ アルゴリズムおよび Security Association（SA）の暗号キーを使用しますが、これは、Internet Key Exchange（IKE）プロトコルによって 2 つのゲートウェイ間で確立されています。

セキュリティ アソシエーション（SA）は 2 つのデバイス間で共有のセキュリティ属性を確立し、VPN エンドポイントがセキュアな通信をサポートできるようにします。SA は、2 つの VPN エンドポイントが、VPN トンネルがどのようにセキュアにされているかを表すパラメータを処理することができます。

システムは、IPsec 接続のネゴシエーションの最初の段階で Internet Security Association and Key Management Protoco（ISAKMP）を使用し、エンドポイントと認証キー交換の間で VPN を確立します。IKE プロトコルは ISAKMP 内にあります。

AH セキュリティ プロトコルは、パケット見出しとデータを保護しますが、暗号化はできません。ESP はパケットを暗号化および保護しますが、最も外側の IP 見出しをセキュアにすることはできません。多くの場合、この保護は必要なく、大半の VPN 展開は、（暗号化の機能により）AH よりも頻繁に ESP を使用します。VPN はトンネル モードのみで動作するため、システムはレイヤ 3 からのパケット全体を暗号化および認証し、ESP プロトコル内で稼動します。トンネル モードの ESP は、後者の暗号化機能だけでなく、データを暗号化します。

IKE

Firepower システムは IKE プロトコルを使用して、トンネルに対して SA をネゴシエートする他に、2 つのゲートウェイを相互に認証します。プロセスは、次の 2 つのフェーズで構成されます。

IKE フェーズ 1 では、Diffie-Hellman キー交換によってセキュアに認証された通信チャネルを確立し、その後の IKE 通信を暗号化するために事前共有キーを生成します。このネゴシエーションにより、双方向の ISAKMP セキュリティ アソシエーションが生じます。ユーザは、事前共有キーを使用して認証を行うことができます。フェーズ 1 はメイン モードで機能します。このフェーズでは、ネゴシエーションの間にすべてのデータを保護しようとしますが、ピアのアイデンティティも保護します。

IKE フェーズ 2 では、IKE ピアが、フェーズ 1 で確立されたセキュアなチャネルを使用して、IPsec の代わりにセキュリティ アソシエーションにネゴシエートします。ネゴシエーションにより、最低 2 つの単方向セキュリティ アソシエーション（一方は着信、他方は発信）が生じます。

VPN 展開

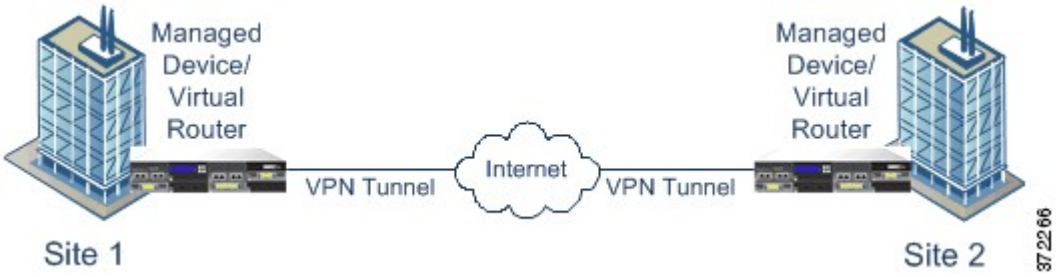
VPN 展開は、VPN に含まれているエンドポイントおよびネットワークを指定し、またそれらが相互にどのように接続しているかを指定します。VPN 展開を Firepower Management Center に設定すると、次に管理対象デバイス、または別の Firepower Management Center によって管理されているデバイスにその VPN 展開を導入できます。

システムでは、ポイントツーポイント、スター、およびメッシュという 3 つのタイプの VPN 展開がサポートされています。

ポイントツーポイントの VPN 展開

ポイントツーポイントの VPN 展開では、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できます。この設定の各デバイスは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なポイントツーポイントの VPN 展開を示しています。



スター VPN 導入

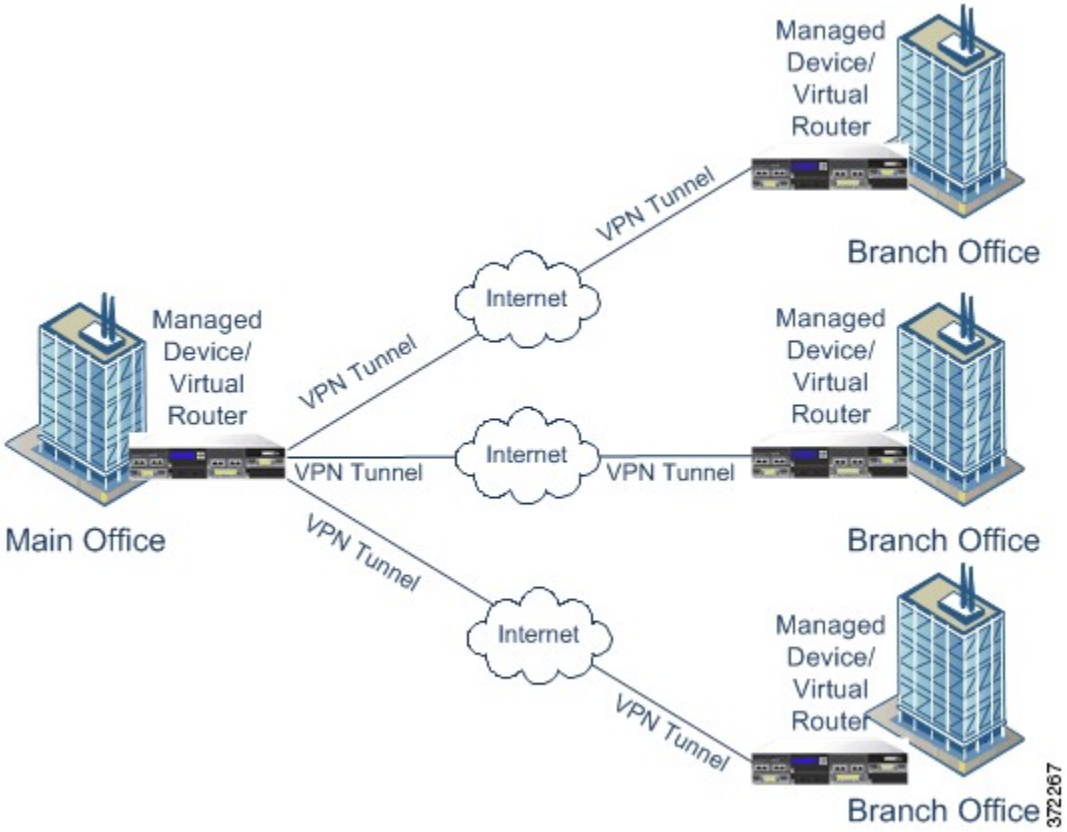
スター VPN 導入では、中央のエンドポイント（ハブ ノード）が、複数のリモート エンドポイント（リーフ ノード）とのセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間のそれぞれの接続は、別の VPN トンネルです。いずれかのリーフ ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

スター型の展開は一般的に、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店と支店を接続する VPN を表します。スター VPN 導入は、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。

一般的なスター型の導入では、ハブ ノードは本社に配置します。リーフ ノードは支社に配置します。トラフィックの大部分は、これらのリーフ ノードから開始されます。各ノードは、VPN 対応の管理対象デバイスであることが必要です。

スター型の導入は、IKE バージョン 2 のみをサポートします。

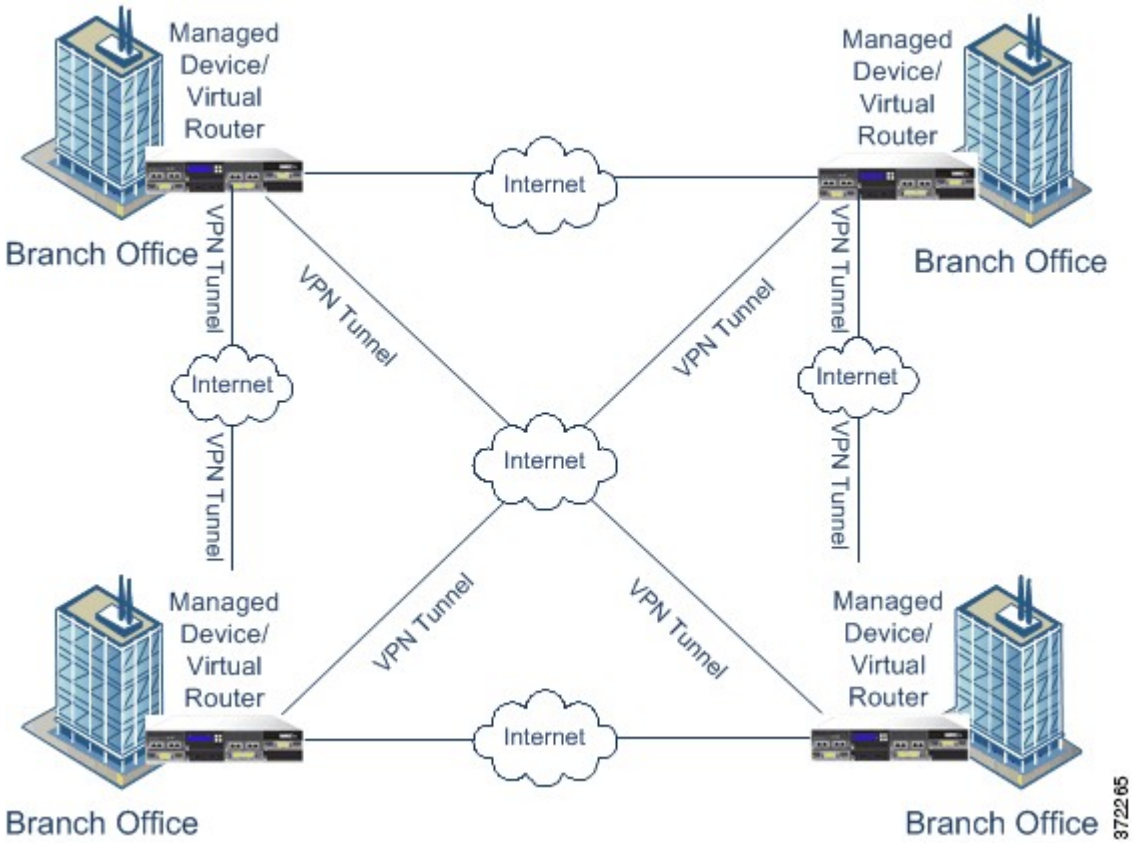
次の図は、一般的なスター VPN 導入を示しています。



メッシュ VPN 展開

メッシュ VPN 展開では、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。メッシュ型の展開では 1 つの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が相互に通信できるように、冗長性を備えています。このタイプの展開は、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。各エンドポイントは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なメッシュ VPN 展開を示しています。



VPN 展開の管理

[VPN] ページ（**[Devices]** > **[VPN]** > **[Site to Site]**）で、現行のすべての VPN 展開を、展開に含まれている名前およびエンドポイントごとに表示することができます。このページ内のオプションを使用して、VPN展開のステータスを表示する、新しい展開を作成する、管理対象デバイスに展開する、展開を修正または削除する、といった操作を実行することができます。

デバイスを Firepower Management Center に登録すると、登録中に、展開済みの VPN が Firepower Management Center と同期されることに注意してください。

関連トピック

VPN 展開の管理 （12 ページ）

VPN 展開オプション

新しい VPN 展開を作成する場合には、最小限の処理として、一意の名前と展開のタイプを指定し、事前共有キーを指定する必要があります。次の 3 つのタイプの展開から選択することができ、それぞれの展開には VPN トンネルが含まれています。

- 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。

- スター型の展開は VPN トンネルのグループを確立し、ハブ エンドポイントをリーフ エンドポイントのグループに接続します。
- 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。

VPN 展開でエンドポイントとして使用できるのは、Cisco の管理対象デバイスのみです。サードパーティ製のエンドポイントはサポートされません。

VPN 認証に対して事前共有キーを定義する必要があります。展開内で生成したすべての VPN 接続で使用するデフォルトのキーを指定できます。ポイントツーポイント型の展開では、各エンドポイントのペアに事前共有キーを指定できます。

マルチドメイン展開では、ドメイン間で VPN 展開を構成できます。つまり、異なるドメインに属するデバイスにエンドポイントを割り当てることができます。このような場合は、関連する子孫ドメインで先祖の展開を表示できますが、変更することはできません。ドリルダウンして展開の詳細を表示すると、現在のドメインに属するデバイスの情報のみが表示されます。

ポイントツーポイント VPN 展開オプション

ポイントツーポイント VPN 展開を設定する場合は、エンドポイント ペアのグループを定義し、各ペアの 2 つのノード間に VPN を作成します。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

ポイントツーポイント型の展開を設定するには、[PTP] をクリックします。

事前共有キー（Pre-Shared Key）

認証に対して一意の事前共有キーを定義します。各エンドポイント ペアに対して事前共有キーを指定しない場合は、システムで展開内のすべての VPN に対してこのキーが使用されます。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

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、指定した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッドインターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

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ないことに注意してください。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（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。

[内部 IP（Internal IP）]

エンドポイントが、ネットワーク アドレス変換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（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

[実装キーを使用する（Use Deployment Key）]

展開に対して定義されている事前共有キーを使用する場合は、チェックボックスをオンにします。このエンドポイント ペアに対して VPN 認証の事前共有キーを指定するには、チェックボックスをオフにします。

事前共有キー（Pre-Shared Key）

[実装キーを使用する（Use Deployment Key）] チェックボックスをオフにした場合は、このフィールドに事前共有キーを指定します。

関連トピック

ポイントツーポイント VPN 展開の設定 （13 ページ）

スター VPN の展開オプション

スター VPN 展開を設定する場合は、1 つのハブ ノード エンドポイント、およびリーフ ノード エンドポイントのグループを定義します。展開を設定するには、ハブ ノード エンドポイントと、少なくとも 1 つのリーフ ノード エンドポイントを定義する必要があります。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

スター型の展開を設定するには、[スター（Star）] をクリックします。

事前共有キー（Pre-Shared Key）

認証に対して一意の事前共有キーを定義します。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

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する場合は、選択した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッドインターフェイスに割り当てられている IP アドレスを選択します。

- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。

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ないことに注意してください。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（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。

[内部 IP（Internal IP）]

エンドポイントが、ネットワーク アドレス変換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（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

関連トピック

スター VPN 展開の設定 （14 ページ）

メッシュ VPN 展開オプション

メッシュ VPN 展開を設定する場合は、VPN のグループを定義して、特定のエンドポイントセットに任意の 2 つのポイントをリンクさせます。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

メッシュ型の展開を設定するには、[メッシュ（Mesh）] をクリックします。

事前共有キー（Pre-Shared Key）

認証に対して一意の事前共有キーを定義します。

Device

展開のエンドポイントとして、デバイススタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

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、指定したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

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、指定した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- 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、選択したルーテッドインターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

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ないことに注意してください。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（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。

[内部 IP（Internal IP）]

エンドポイントが、ネットワークアドレス変換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（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

関連トピック

メッシュ VPN 展開の設定 （15 ページ）

VPN 展開の詳細オプション

VPN の展開には、展開の VPN で共有できる共通設定がいくつか含まれています。各 VPN では、デフォルトの設定を使用するか、またはそのデフォルトの設定を上書きすることができます。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

次に、展開で指定できる詳細オプションについて説明します。

許可されるその他のアルゴリズム（Other Algorithm Allowed）

このチェックボックスをオンにすると、[アルゴリズム（Algorithm）] リストに含まれていないがリモートピアによって提案されるアルゴリズムについて、自動ネゴシエーションが有効になります。

アルゴリズム（SNMP (v3) Auth. Alrorithm）

展開でデータのセキュリティを確保するため、フェーズ 1 とフェーズ 2 のアルゴリズムの提案を指定します。両方のフェーズに対して、**[暗号（Cipher）]**、**[ハッシュ（Hash）]**、および [Diffie-Hellman (**DH**)]グループ認証メッセージを選択します。

IKE ライフタイム（IKE Life Time）

IKE SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 15 分、最大 30 日を指定できます。

IKE v2

システムで IKE バージョン 2 を使用する場合は、このチェックボックスをオンにします。このバージョンでは、スター型の展開と複数の保護ネットワークがサポートされます。

ライフタイム（Life Time）

SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 5 分、最大 24 時間を指定できます。

ライフ パケット数（Life Packets）

有効期限までに IPsec SA を介して伝送できるパケット数を指定します。0 ～ 18446744073709551615 の整数を使用できます。

ライフ バイト（Life Bytes）

有効期限までに IPsec SA を介して伝送できるバイト数を指定します。0 ～ 18446744073709551615 の整数を使用できます。

AH

保護対象のデータに対して認証ヘッダー セキュリティ プロトコルを使用するように指定する場合は、このチェックボックスをオンにします。暗号化サービス ペイロード（ESP）プロトコルを使用する場合は、このチェックボックスをオフにします。

関連トピック

高度な VPN 展開を設定する方法 （16 ページ）

VPN 展開の管理

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

⚠

注意 7000 または 8000 シリーズ デバイス上の VPN を追加または削除して、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は Snort® の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 VPN の展開を管理します。

- 追加：新しい VPN の展開を作成するには、**[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックして、展開タイプに応じて次の手順を実行します。
  - メッシュ VPN 展開の設定 （15 ページ）

- ポイントツーポイント VPN 展開の設定 （13 ページ）
- スター VPN 展開の設定 （14 ページ）

- 編集：既存の VPN 展開の設定を変更するには、編集アイコン（）をクリックします。VPN 展開の編集 （17 ページ）を参照してください。
- 削除：VPN 展開を削除するには、削除アイコン（）をクリックします。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 を参照）。
- VPN ステータスの表示：既存の VPN 展開のステータスを表示するには、ステータス アイコンをクリックします。VPN ステータスの表示 （18 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ

ポイントツーポイント VPN 展開の設定

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。

（注） 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、仮想ルータのセットアップを参照してください。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 **[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [タイプ（Type）] として [PTP] が選択されていることを確認します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ノード ペア（Node Pairs）] の隣の追加アイコン（）をクリックします。

ステップ 7 ポイントツーポイント VPN 展開オプション （6 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [ノード A（Node A）] の下の [保護されたネットワーク（Protected Networks）] の隣にある追加アイコン（  ）をクリックします。

ステップ 9 保護されたネットワークの CIDR ブロックを入力します。

ステップ 10 [OK] をクリックします。

ステップ 11 [ノード B（Node B）] に対して手順 8 ～ 10 を繰り返します。

ステップ 12 [保存（Save）] をクリックします。
エンドポイント ペアが展開に追加されます。

ステップ 13 [保存（Save）] をクリックして、展開の設定を終了します。

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。

スター VPN 展開の設定

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。

（注） 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、仮想ルータのセットアップを参照してください。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 **[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [スター（Star）] をクリックしてタイプを指定します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ハブ ノード（Hub Node）] の隣の編集アイコン（  ）をクリックします。

ステップ 7 スター VPN の展開オプション （8 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [保護されたネットワーク（Protected Networks）] の隣の追加アイコン（）をクリックします。

ステップ 9 保護されたネットワークの IP アドレスを入力します。

ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。ハブ ノードが展開に追加されます。

ステップ 12 [リーフ ノード（Leaf Nodes）] の隣の追加アイコン（）をクリックします。

ステップ 13 リーフ ノードを完了するには、手順 7 ～ 10 を繰り返します。これにより、ハブ ノードと同じオプションが設定されます。

ステップ 14 [保存（Save）] をクリックします。
リーフ ノードが展開に追加されます。

ステップ 15 [保存（Save）] をクリックして、展開の設定を終了します。

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。

メッシュ VPN 展開の設定

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。

（注） 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、仮想ルータのセットアップを参照してください。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 **[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [メッシュ（Mesh）] をクリックして [タイプ（Type）] を指定します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ノード（Nodes）] の隣の追加アイコン（  ）をクリックします。

ステップ 7 メッシュ VPN 展開オプション （9 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [保護されたネットワーク（Protected Networks）] の隣の追加アイコン（  ）をクリックします。

ステップ 9 保護されたネットワークの CIDR ブロックを入力します。

ステップ 10 [OK] をクリックします。
保護されたネットワークが追加されます。

ステップ 11 [保存（Save）] をクリックします。
展開にエンドポイントが追加されます。

ステップ 12 エンドポイントをさらに追加するには、ステップ 6 ～ 11 を繰り返します。

ステップ 13 [保存（Save）] をクリックして展開を完了します。

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。

高度な VPN 展開を設定する方法

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン展開では、現在のドメインで作成された VPN 展開が表示されます。これは編集できます。また、エンドポイントデバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 VPN 展開の詳細オプション （11 ページ）の説明に従って、詳細設定を行います。

ステップ 5 [アルゴリズム（Algorithms）] の隣の追加アイコン（  ）をクリックします。

ステップ 6 両方のフェーズに対して、[暗号（Cipher）]、[ハッシュ（Hash）]、および [Diffie-Hellman]（[DH]）グループ認証のメッセージを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

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。

VPN 展開の編集

注意 2 人のユーザが同じ展開について同時に編集**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ないことに注意してください。

マルチドメイン展開では、現在のドメインで作成された VPN 展開が表示されます。これは編集できます。また、エンドポイントデバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 必要な設定を変更します。

- [詳細設定（Advanced）] の設定。高度な VPN 展開を設定する方法 （16 ページ）を参照してください。
- メッシュ展開の設定。メッシュ VPN 展開の設定 （15 ページ）を参照してください。
- ポイントツーポイント型の展開の設定。ポイントツーポイント VPN 展開の設定 （13 ページ）を参照してください。
- スター型の展開の設定。スター VPN 展開の設定 （14 ページ）を参照してください。

ヒント　展開を最初に保存した後で、展開のタイプを編集することはできません。展開のタイプを変更するには、展開を削除してから新しい展開を作成する必要があります。

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。

VPN 展開のステータス

VPN 展開を設定した後で、設定した VPN トンネルのステータスを表示できます。VPN ページには、各 VPN 展開の展開後に、その展開のステータス アイコンが表示されます。

- （  ）アイコンは、すべての VPN エンドポイントが稼動していることを表します。
- （  ）アイコンは、すべての VPN エンドポイントが停止していることを表します。
- （  ）アイコンは、稼働しているエンドポイントと停止しているエンドポイントがあることを表します。

ステータスアイコンをクリックして、展開のステータス、および展開内のエンドポイントに関する基本情報（エンドポイント名やIPアドレスなど）を表示することができます。VPN ステータスは、毎分、または（エンドポイントが停止した、または稼動したなど）ステータスの変更が生じた場合に更新されます。

関連トピック

VPN ステータスの表示 （18 ページ）

VPN ステータスの表示

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。
ステップ 2 ステータスを表示する展開の隣にある、VPN ステータス アイコンをクリックします。
ステップ 3 [OK] をクリックします。

VPN の統計およびログ

VPN 展開を設定した後で、設定した VPN トンネルを通過するデータの統計を表示することができます。また、各エンドポイントについて最新の VPN システムと IKE ログを表示することができます。

システムには、次の統計情報が表示されます。

エンドポイント（Endpoint）

VPN エンドポイントとして指定されたルーテッド インターフェイスおよび IP アドレスへのデバイス パス。

ステータス

VPN 接続の状態（稼働または停止のどちらか）。

プロトコル

暗号化で使用されるプロトコル（ESP または AH）。

受信パケット数（Packets received）

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのパケット数。

転送パケット数（Packets Forwarded）

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのパケット数。

受信バイト数（Bytes Received）

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのバイト数。

転送バイト数（Bytes Forwarded）

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのバイト数。

作成時刻（Time Created）

VPN 接続が作成された日時。

最後に使用された時刻（Time Last Used）

ユーザが最後に VPN 接続を開始した時間。

NAT トラバーサル（NAT Traversal）

[はい（Yes）] が表示されている場合、ネットワーク アドレス変換を備えたデバイスの背後に少なくとも 1 つの VPN エンドポイントが存在します。

IKE 状態（IKE State）

IKE SA の状態（接続、確立、削除、または廃棄）。

IKE イベント（IKE Event）

IKE SA イベント（再認証、またはキー再生成）。

IKE イベント時間（IKE Event Time）

次のイベントが発生する時間（秒）。

IKE アルゴリズム（IKE Algorithm）

VPN 展開で使用されている IKE アルゴリズム。

IPSec 状態（IPSec State）

IPSec SA の状態（インストール中、インストール済み、更新中、キー再生成、削除、および廃棄）。

IPSec イベント（IPSec Event）

IPSec SA イベントがキーを再生成するタイミングの通知。

IPSec イベント時間（IPSec Event Time）

次のイベントが発生するまでの時間（秒）。

IPSec アルゴリズム（IPSec Algorithm）

VPN 展開で使用されている IPSec アルゴリズム。

関連トピック

VPN 統計情報およびログの表示 （20 ページ）

VPN 統計情報およびログの表示

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	サポートされるドメイン	アクセス（Access）
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成さ

れた VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

手順

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 統計情報を表示する展開の隣にある、VPN ステータス アイコンをクリックします。

ステップ 3 統計情報の表示アイコン（  ）をクリックします。

ステップ 4 オプションで、[更新（Refresh）] をクリックして、VPN の統計情報を更新することもできます。

ステップ 5 オプションで、[最新のログの表示（View Recent Log）] をクリックして、各エンドポイントの最新のデータ ログを表示することもできます。ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスおよびスタック デバイスのログを表示するには、アクティブ/プライマリ、またはバックアップ/セカンダリのいずれかのデバイスへのリンクをクリックします。