ゲートウェイ VPN の使用

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。Cisco 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 FireSIGHT 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。

Cisco の 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 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、インターネット キー エクスチェンジ（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 認証ヘッダー（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 展開を設定および適用するには、該当する対象管理デバイスで 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 シリーズ 3 デバイスでのみ使用できます。

VPN 展開の作成および管理の詳細については、以下の項を参照してください。

IPSec について

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。FireSIGHT システムはハッシュ アルゴリズムおよびセキュリティ アソシエーション（SA）の暗号キーを使用しますが、これは、インターネット キー エクスチェンジ（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 Protocol（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。IKE プロトコルの詳細については、IKE について（10-2 ページ）を参照してください。

AH セキュリティ プロトコルは、パケット ヘッダー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 ヘッダー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 プロトコル内で稼働します。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 について

FireSIGHT システムは、トンネルに対して SA をネゴシエートする他に、IKE プロトコルを使用して 2 つのゲートウェイを相互に手動で認証します。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、より多くの 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 展開について

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、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 展開を設定したら、その展開を管理対象デバイス、または他の 防御センター で管理されているデバイスに適用することができます。

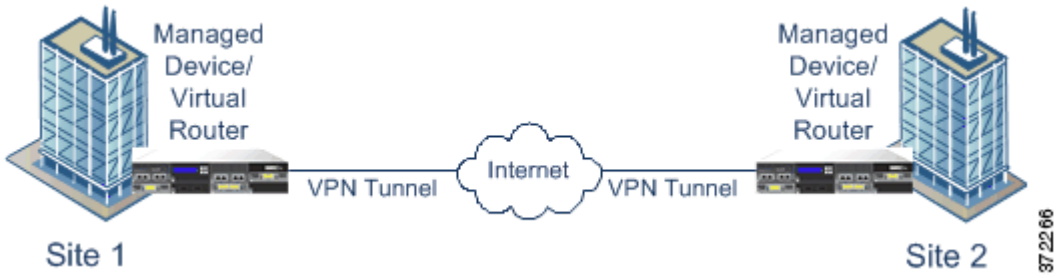
システムでは、3 つのタイプの VPN 展開（ポイントツーポイント、スター、メッシュ）をサポートしています。これらの VPN 展開の詳細については、以下の項を参照してください。

- ポイントツーポイントの VPN 展開について（10-3 ページ）
- スター VPN 展開について（10-3 ページ）
- メッシュ VPN 展開について（10-4 ページ）

ポイントツーポイントの VPN 展開について

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することができます。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。



詳細については、ポイントツーポイント VPN 展開の設定（10-6 ページ）を参照してください。

スター VPN 展開について

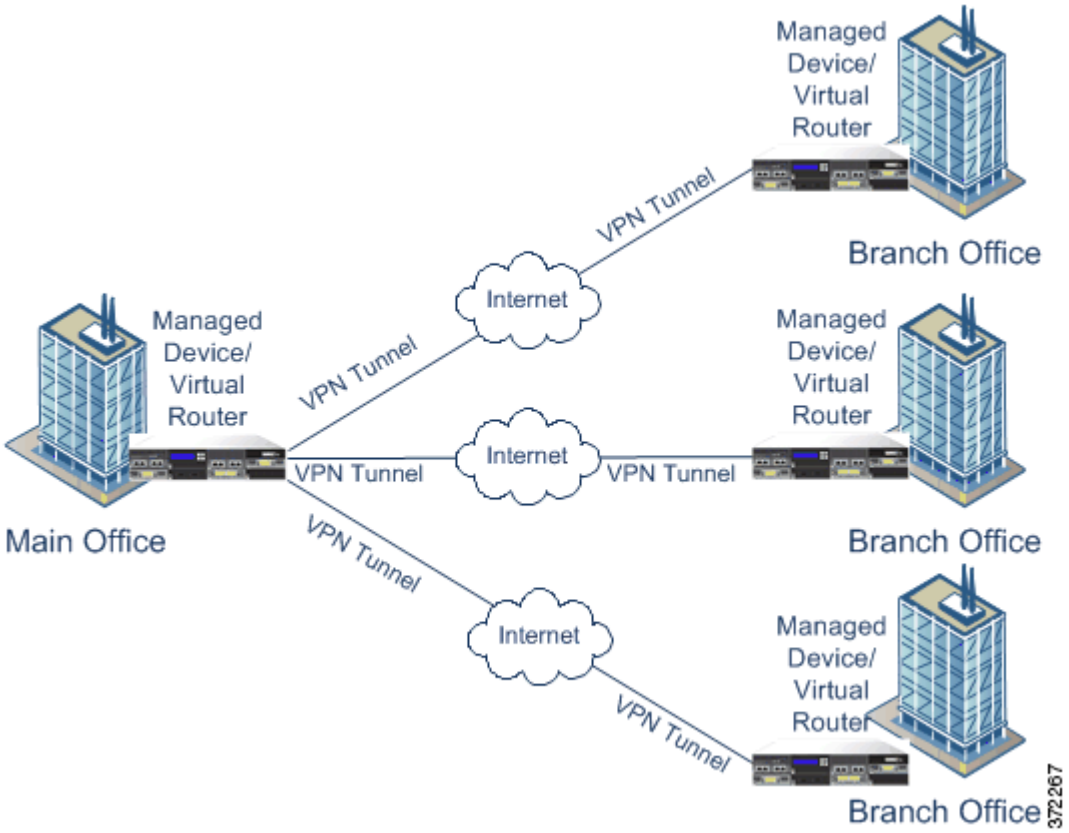
スター VPN 展開では、中央のエンドポイント（ハブ ノード）が、複数のリモート エンドポイント（リーフ ノード）とのセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間のそれぞれの接続は、別の VPN トンネルです。いずれのリーフ ノードの背後にあるホストも、ハブ ノードを介して互いに通信できます。

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社とブランチ オフィスを接続する VPN を表します。スター VPN 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。

一般的なスター型の展開では、ハブ ノードは本社に配置します。リーフ ノードはブランチ オフィスに配置します。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。

スター型の展開は、IKE バージョン 2 のみをサポートしていることに注意してください。

次の図は、一般的なスター VPN 展開を示しています。

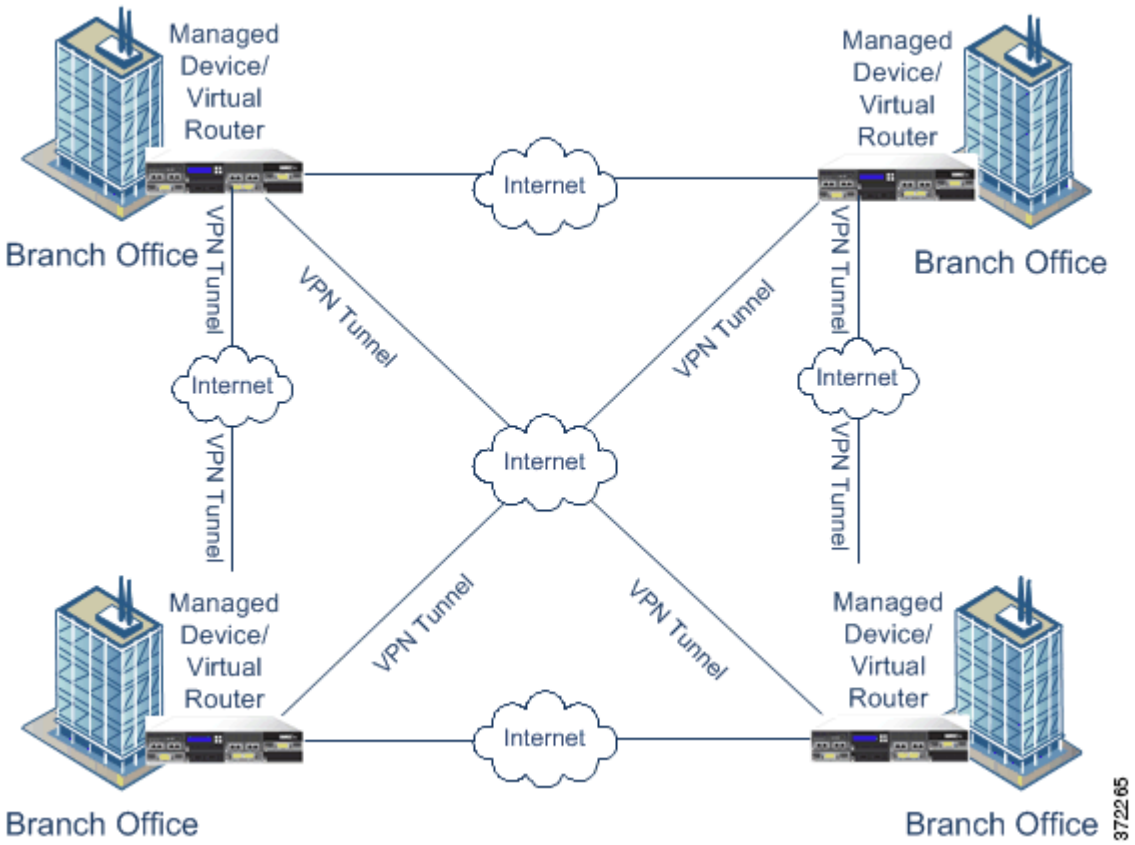


詳細については、スター VPN 展開の設定（10-9 ページ）を参照してください。

メッシュ VPN 展開について

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。



詳細については、メッシュ VPN 展開の設定（10-12 ページ）を参照してください。

VPN 展開の管理

ライセンス：VPN

サポートされるデバイス：シリーズ 3

[VPN] ページ（[デバイス（Devices）] > [VPN]）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。このページでのオプションで、VPN 展開のステータスを表示する、新しい展開を作成する、展開を適用する、展開を編集または削除する、といったことができます。

注意　デバイスを 防御センターに登録するときにデフォルトのアクセス コントロール ポリシーを選択した場合は、デフォルトのアクセス コントロール ルールがすべてのトラフィックをブロックします。デバイス上で VPN 展開を設定すると、展開は失敗します。

デバイスを防御センターに登録すると、適用した VPN 展開は、登録中は防御センターと同期することに注意してください。

以下の表で、[VPN] ページで展開を管理するために実行できる操作について説明します。

表 10-1　VPN 展開の管理操作

目的	操作
新しい VPN 展開を作成する	[追加(Add)] をクリックします。詳細については、VPN 展開の設定(10-6 ページ)を参照してください。
既存の VPN 展開の設定を変更する	編集アイコン( )をクリックします。詳細については、VPN 展開の設定(10-6 ページ)を参照してください。
既存の VPN 展開のステータスを表示する	ステータス アイコンをクリックします。詳細については、VPN 展開のステータスの表示(10-16 ページ)を参照してください。
VPN 展開を、展開内で対象とするすべてのデバイスに適用する	適用アイコン( )をクリックします。詳細については、VPN 展開の適用(10-15 ページ)を参照してください。
VPN 展開を削除する	削除アイコン( )をクリックして [はい(Yes)] をクリックします。展開を削除しない場合は [いいえ(No)] をクリックします。

VPN 展開の設定

ライセンス: VPN

サポートされるデバイス: シリーズ 3

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ます。それぞれの展開には、VPN トンネルのグループが含まれています。

- 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。

Cisco の 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。

各タイプの VPN 展開の作成の詳細については、次の項を参照してください。

- ポイントツーポイント VPN 展開の設定(10-6 ページ)
- スター VPN 展開の設定(10-9 ページ)
- メッシュ VPN 展開の設定(10-12 ページ)

ポイントツーポイント VPN 展開の設定

ライセンス: VPN

サポートされるデバイス: シリーズ 3

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。詳細については、ポイントツーポイントの VPN 展開について(10-3 ページ)を参照してください。

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）]
展開に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ことを指定するには、[PTP] をクリックします。

事前共有キー（Pre-shared Key）
認証のための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 スタックやクラスタなどの管理対象デバイスを選択できます。使用している防御センターで管理されていない Cisco 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、選択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、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 クラスタの場合は、SFRP の 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防御センターで管理されて**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無効になります。

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）] を選択した場合は、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。

公共 IKE ポート（Public IKE Port）

[内部 IP（Internal IP）] を選択した場合は、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。

展開キーの使用（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）

[展開キーの使用（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。

ヒント　既存のポイントツーポイント型の展開を編集するには、展開の隣にある編集アイコン（ ）をクリックします。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。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。

ポイントツーポイント VPN 展開を設定する方法

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。

[VPN] ページが表示されます。

手順 2　[追加（Add）] をクリックします。

[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウが表示されます。

手順 3　展開に一意の [名前（Name）] を指定します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

手順 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。

手順 5　展開に一意の [事前共有キー（Pre-shared Key）] を指定します。

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

[新しいエンドポイント ペアの追加（Add New Endpoint Pair）] ポップアップ ウィンドウが表示されます。

手順 7　この項で説明したとおりに、VPN 展開を設定します。

手順 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。

[ネットワークを追加（Add Network）] ポップアップ ウィンドウが表示されます。

手順 9　保護されたネットワークの CIDR ブロックを入力します。

手順 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。

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

手順 12　[保存（Save）] をクリックします。

エンドポイントのペアが展開に追加され、[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウがもう一度表示されます。

手順 13　[保存（Save）] をクリックして展開の設定を終了すると、[VPN] ページがもう一度表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

スター VPN 展開の設定

ライセンス：VPN

サポートされるデバイス：シリーズ 3

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。詳細については、スター VPN 展開について（10-3 ページ）を参照してください。

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）]
展開に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ことを指定するには、[スター（Star）] をクリックします。

事前共有キー（Pre-shared Key）
認証のための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 スタックやクラスタなどの管理対象デバイスを選択できます。使用している防御センターで管理されていない Cisco 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、選択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、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 クラスタの場合は、SFRP の 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防御センターで管理されて**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無効になります。

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）] を選択した場合は、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。

公共 IKE ポート（Public IKE Port）

[内部 IP（Internal IP）] を選択した場合は、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。

ヒント　既存のスター型の展開を編集するには、展開の隣にある編集アイコン（）をクリックします。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。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。

スター型の展開を設定する方法

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。

[VPN] ページが表示されます。

手順 2　[追加（Add）] をクリックします。

[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウが表示されます。

手順 3　展開に一意の [名前（Name）] を指定します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

手順 4　[タイプ（Type）] を指定して [スター（Star）] をクリックします。

手順 5　展開に一意の [事前共有キー（Pre-shared Key）] を指定します。

手順 6　[ハブ ノード（Hub Node）] の隣の追加アイコン（  ）クリックします。

[ハブ ノードの追加（Add Hub Node）] ポップアップ ウィンドウが表示されます。

手順 7　この項で説明したとおりに、VPN 展開を設定します。

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

[ネットワークを追加（Add Network）] ポップアップ ウィンドウが表示されます。

手順 9　保護されたネットワークの IP アドレスを入力します。

手順 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。

手順 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、[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウがもう一度表示されます。

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

[リーフ ノードの追加（Add Leaf Node）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 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、[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウがもう一度表示されます。

手順 15　[保存（Save）] をクリックして展開の設定を終了すると、[VPN] ページがもう一度表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

メッシュ VPN 展開の設定

ライセンス：VPN

サポートされるデバイス：シリーズ 3

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。詳細については、メッシュ VPN 展開について（10-4 ページ）を参照してください。

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）]

展開に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ことを指定するには、[メッシュ（Mesh）] をクリックします。

事前共有キー（Pre-shared Key）

認証のための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 スタックやクラスタなどの管理対象デバイスを選択できます。使用している防御センターで管理されていない Cisco 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、選択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、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 クラスタの場合は、SFRP の 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防御センターで管理されて**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無効になります。

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）] を選択した場合は、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。

公共 IKE ポート（Public IKE Port）

[内部 IP（Internal IP）] を選択した場合は、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。

ヒント　既存のメッシュ型の展開を編集するには、展開の隣にある編集アイコン（ ）をクリックします。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。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。

メッシュ VPN 展開を設定する方法

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。

[VPN] ページが表示されます。

手順 2　[追加（Add）] をクリックします。

[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウが表示されます。

手順 3　展開に一意の [名前（Name）] を指定します。

スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。

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

手順 5　展開に一意の [事前共有キー（Pre-shared Key）] を指定します。

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

[エンドポイントの追加（Add Endpoint）] ポップアップ ウィンドウが表示されます。

手順 7　この項で説明したとおりに、VPN 展開を設定します。

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

[ネットワークを追加（Add Network）] ポップアップ ウィンドウが表示されます。

手順 9　保護されたネットワークの CIDR ブロックを入力します。

手順 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。

手順 11　[保存（Save）] をクリックします。

エンドポイントが展開に追加され、[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウがもう一度表示されます。

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

手順 13　[保存（Save）] をクリックして展開の設定を終了すると、[VPN] ページがもう一度表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

高度な VPN 展開を設定する方法

ライセンス：VPN

サポートされるデバイス：シリーズ 3

VPN の展開には、展開内の VPN で共有できる一般的な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、展開で指定できる高度なオプションについて示します。

使用できるその他のアルゴリズム（Other Algorithm Allowed）

[アルゴリズム（Algorithm）] リストに記載されていないものの、リモート ピアがサードパーティ デバイスの場合にリモート ピアで提案されているアルゴリズムに対して自動ネゴシエーションを有効にするには、このチェックボックスをオンにします。

アルゴリズム（SNMP (v3) Auth. Alrorithm）

展開内でデータをセキュアにするための、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]）グループ認証のメッセージを選択します。

IKE ライフ タイム（IKE Life Time）

IKE SA の最大の再ネゴシエーション間隔に対して数値を指定し、時間単位を選択します。最低 15 分、最大 30 日まで指定できます。

IKE v2

システムで IKE バージョン 2 を指定する場合は、このチェックボックスを選択します。このバージョンでは、スター型の展開と保護された複数のネットワークをサポートしています。

ライフタイム（Life Time）

SA の最大の再ネゴシエーション間隔に対して数値を指定し、時間単位を選択します。最低 5 分、最大 24 時間まで指定できます。

ライフ パケット（Life Packets）

有効期間が終了する前に、IPsec SA を介して送信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）

有効期間が終了する前に、IPsec SA を介して送信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

システムで、保護される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ことを指定するには、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。各プロトコルを使用する場合のガイダンスについては、IPSec について（10-1 ページ）を参照してください。

高度な VPN 展開を設定する方法

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。

[VPN] ページが表示されます。

手順 2　[追加（Add）] をクリックします。

[新しい VPN 展開の作成（Create New VPN Deployment）] ポップアップ ウィンドウが表示されます。

手順 3　[Advanced] タブをクリックします。

手順 4　この項で説明したとおりに、詳細設定を行います。

手順 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。

[IKE アルゴリズムの提案の追加（Add IKE Algorithm Proposal）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 7　[OK] をクリックします。

IKE アルゴリズムの提案が追加されます。

手順 8　[保存（Save）] をクリックします。

変更が保存され、[VPN] ページが表示されます。

内容を反映させるには、展開を適用する必要があることに注意してください。VPN 展開の適用（10-15 ページ）を参照してください。

VPN 展開の適用

ライセンス：VPN

サポートされるデバイス：シリーズ 3

VPN 展開に対して設定または変更した後は、1 つ以上のデバイスに展開を適用して、展開に指定した設定を実装する必要があります。

注意　シリーズ 3 デバイスの VPN を追加または削除すると、変更を適用したときに一時的にトラフィックのインスペクションが中断され、Snort プロセスが再起動されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

VPN 展開を適用する方法

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。

[VPN] ページが表示されます。

手順 2　適用する VPN 展開の隣の適用アイコン（）をクリックします。

手順 3　プロンプトが表示されたら、[はい（Yes）] をクリックします。

VPN 展開が適用されます。

ヒント　オプションで、[VPN 展開の適用（Apply VPN deployment）] ダイアログボックスから [変更の表示（View Changes）] をクリックします。新しいブラウザ ウィンドウに [VPN 比較ビュー（VPN Comparison View）] ページが表示されます。詳細については、VPN 展開の比較ビューの使用（10-19 ページ）を参照してください。

手順 4　[OK] をクリックします。

[VPN] ページに戻ります。

VPN 展開のステータスの表示

ライセンス：VPN

サポートされるデバイス：シリーズ 3

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、適用されたそれぞれの VPN 展開に対するステータス 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働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（エンドポイントの停止、稼働など）ステータスの変更が生じた場合に更新されます。

VPN のステータスを表示する方法

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。

[VPN] ページが表示されます。

手順 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。

[VPN ステータス（VPN Status）] ポップアップ ウィンドウが表示されます。

手順 3　[OK] をクリックして [VPN] ページに戻ります。

VPN の統計およびログの表示

ライセンス: VPN

サポートされるデバイス: シリーズ 3

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 イベント時刻（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。

VPN の統計情報を表示する方法
アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [VPN] を選択します。
[VPN] ページが表示されます。

手順 2　VPN の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。
[VPN ステータス（VPN Status）] ポップアップ ウィンドウが表示されます。

手順 3　統計情報の表示アイコン（  ）をクリックします。
[VPN 統計（VPN Statistics）] ポップアップ ウィンドウが表示されます。

手順 4　[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。

手順 5　[最近のログの表示(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。

クラスタ化されたデバイスおよびスタック構成の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選択します。

VPN 展開の比較ビューの使用

ライセンス: VPN

サポートされるデバイス: シリーズ 3

VPN 展開の比較ビューを使用して、展開を適用する前に、展開に対して行った変更を表示することができます。レポートでは、現在の展開と提案された展開の違いがすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

比較ビューには 2 つの展開が左右に分かれて表示され、比較ビューの両側のタイトル バーには、それぞれの展開が名前で識別されて示されます。展開名とともに、最後に変更した時間と、最後に変更したユーザが表示されます。

2 つの展開の相違は、次のように強調されます。

- 青は、2 つの展開において強調された設定が異なっていることを表し、相違点は赤で示されています。
- 緑は、強調された設定が一方展開に存在し、他方の設定にはないことを表します。

次の表に、実行できる操作を記載します。

表 10-2　VPN 展開の比較ビューの操作

目的	操作
変更に個別にナビゲートする	タイトル バーの上にある [前へ(Previous)] または [次へ(Next)] をクリックします。 左側と右側の間にある二重矢印アイコン( )が移動し、表示している違いを示す [差異(Difference)] 番号が変わります。
展開の比較レポートを生成する	[比較レポート(Comparison Report)] をクリックします。 展開の比較レポートでは、2 つのポリシー間の違いのみが示された PDF ドキュメントが作成されます。