Firepower Threat Defense VPNの導入

Firepower Threat Defense サイト間 VPN について

Firepower Threat Defense サイト間 VPN では、次の機能がサポートされています。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 自動または手動の事前共有認証キー。
- IPv4 および IPv6。内部、外部のすべての組み合わせをサポート。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- Firepower Management Center および Firepower Threat Defense 両方の HA 環境をサポート。
- トンネルがダウンした際の VPN アラート。
- Firepower Threat Defense 統合 CLI により利用可能なトンネル統計。

VPN トポロジ

新しいサイト間 VPN トポロジを作成するには、少なくとも、一意の名前を付け、トポロジ タイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンを選択する必要があります。また、事前共有キーを指定します。設定したら、Firepower Threat Defense デバイスにトポロジを展開します。Firepower Management Center は、Firepower Threat Defense デバイスのサイト間 VPN のみ設定します。

次の 3 つのタイプのトポロジから選択することができます。トポロジには、VPN トンネルが 1 つ以上含まれています。

- 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。

- ハブ アンド スポーク型の展開は、VPN トンネルのグループを確立し、ハブ エンドポイントをスポーク ノードのグループに接続します。
- フル 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。

IPsec と IKE

Firepower Management Center では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよびIPsecプロポーザルに基づいて設定されます。ポリシーとプロポーザルはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

認証

VPN 認証の事前共有キーを定義します。トポロジ内のすべての VPN ノードに使用するデフォルト キーを手動で指定するか、Firepower Management Center に自動的に生成させることが可能です。

エクストラネット デバイス

各トポロジ タイプには、Firepower Management Center で管理しないデバイスである、エクストラネット デバイスが含まれる可能性があります。これには次が含まれます。

- Firepower Management Center ではサポートされているが、ユーザの部門が担当していないシスコ デバイス。たとえば、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続などです。
- シスコ製以外のデバイス。Firepower Management Center を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。

シスコ以外のデバイス、またはFirepower Management Centerで管理されていないシスコ デバイスを VPN トポロジに「その他の」デバイスとして追加します。また、各リモート デバイスの IP アドレスも指定します。

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。

Firepower Threat Defense サイト間 VPN ガイドラインと制約事項

- PKI 証明書には対応していません。認証にあたっては、事前共有キーにのみ対応しています。
- 現在のドメイン内ではないエンドポイント用のエクストラネット ピアを使用してのみ、ドメイン間の VPN 接続が可能です。
- VPN トポロジをドメイン間で移動させることはできません。
- 「範囲」オプションのあるネットワーク オブジェクトは、VPN では対応していません。
- Firepower Threat Defense VPN のバックアップは、Firepower Management バックアップを使用した場合のみ行われます。
- Firepower Threat Defense VPN では、現在、PDF のエクスポートおよびポリシーの比較には対応していません。
- Firepower Threat Defense VPN ではトンネル単位またはデバイス単位の編集オプションはありません。トポロジ全体のみ編集できます。
- クラスタ化環境では、Firepower Threat Defense VPN には対応していません。
- Firepower Management Center では、トンネルの状態はリアルタイムではなく、5 分間隔でアップロードされます。
- トンネル モードにのみ対応し、トランスポート モードには対応していません。IPsec トンネル モードは、新しい IP パケットのペイロードになる元の IP データグラム全体を暗号化します。トンネル モードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPsec が実装される標準の方法です。