Cisco Secure Firewall Management Center を使用したポリシーベース VPN からルートベース VPN への移行

改訂：2025 年 2 月 26 日

Cisco Secure Firewall Management Center を使用したポリシーベース VPN からルートベース VPN への移行

はじめに

このドキュメントでは、Cisco Secure Firewall Management Center の VPN ウィザードを使用して、ポリシーベース VPN をルートベース VPN に移行する方法について説明します。

ポリシーベース VPN に依存している組織は、ネットワーク インフラストラクチャの管理と拡張の面で大きな課題に直面しています。ポリシーベース VPN では、複雑なアクセスリストと正確な順序付けが必要であるため、設定エラーが発生しやすく、特にネットワークが拡大するにつれて管理が困難になります。また、ダイナミック ルーティング プロトコルもサポートされていません。新しいスポークを追加する場合、ハブで追加の VPN 設定更新を行う必要があります。これらの欠点は、管理上の負担を増加させるだけでなく、ネットワークの拡張性と柔軟性を制限し、効率を低下させ、エラーの発生率を高ます。

仮想トンネルインターフェイス（VTI）を使用してルートベースの VPN に移行することで、設定と管理が簡素化され、ネットワークの信頼性、拡張性、および管理性が向上し、増大するビジネスニーズに対応できます。

ルートベース VPNについて

ルートベース VPN は、ピア間で VPN トンネルを確立するために、仮想トンネルインターフェイス（VTI）と呼ばれるルーティング可能な論理インターフェイスを使用します。仮想インターフェイスを他のインターフェイスと同様に使用して、静的およびダイナミック ルーティング ポリシーを適用できます。ルーテッドセキュリティ ゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネル上の復号されたトラフィックに対するアクセス制御ルールを定義できます。Threat Defense デバイスは、トンネルインターフェイスとの間のトラフィックを暗号化または復号し、ルーティングポリシーに従って転送します。サイト間 VPN ウィザードを使用して、静的 VTI（SVTI）またはダイナミック VTI（DVTI）でルートベース VPN を構成できます。

ルートベース VPN の利点

ハブアンドスポークトポロジでルートベースの VPN を使用する利点は次のとおりです。

- **セットアップの合理化**：VTI は、従来のクリプトマップとアクセスリストの複雑さを排除して、VPN 設定へのシンプルなアプローチを実現します。
- **管理の簡素化**：VTI を使用することで、大企業のハブとスポーク展開のピア設定の管理を簡素化できます。ハブ上で単一のダイナミック VTI を設定することで、静的 VTI を使用して複数のスポークをサポートできます。
- **適応型ルーティング**：VTI は、BGP、EIGRP、OSPF などのダイナミック ルーティング プロトコルに対応し、ネットワークの状態の変化に応じた VPN エンドポイント間のルートの自動更新を容易にします。
- **デュアル ISP の冗長性**：VTI はセカンダリ バックアップ トンネルの作成を可能にし、接続の信頼性を高めます。

- **ロードバランシング**：VTI により、ECMP ルーティングを介して VPN トラフィックを均等に配分できます。

ポリシーベース VPN からルートベース VPN への移行に関する推奨事項

Management Center を使用してポリシーベース VPN からルートベース VPN への移行を開始する前に、以下の手順を実行する必要があります。

- ネットワーク要件に応じて、ルートベース VPN のルーティングプロトコルを選択します。
- スポークの静的 VTI インターフェイスの IP アドレスを選択します。

  複数のスポークがある場合は、VTI インターフェイスにサブネットを割り当てることを推奨します。

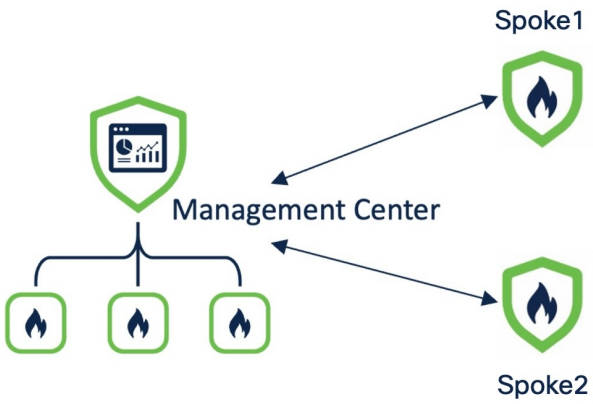
  スポークの静的 VTI IP アドレスを設定する場合は、以下の推奨事項に注意してください。

  - 169.254.xx/16 の範囲の IP アドレスを使用します。
  - Threat Defense デバイス用に予約されている IP アドレスの範囲（169.254.1.x/24）は使用しないでください。
  - 静的VTIを使用するポイントツーポイントトンネルには、ネットマスクを/30にしたIPアドレス（169.254.2.1/30など）を使用します。

ユースケース 1：ピアツーピアのポリシーベース VPN をピアツーピアのルートベース VPN に移行する

シナリオ

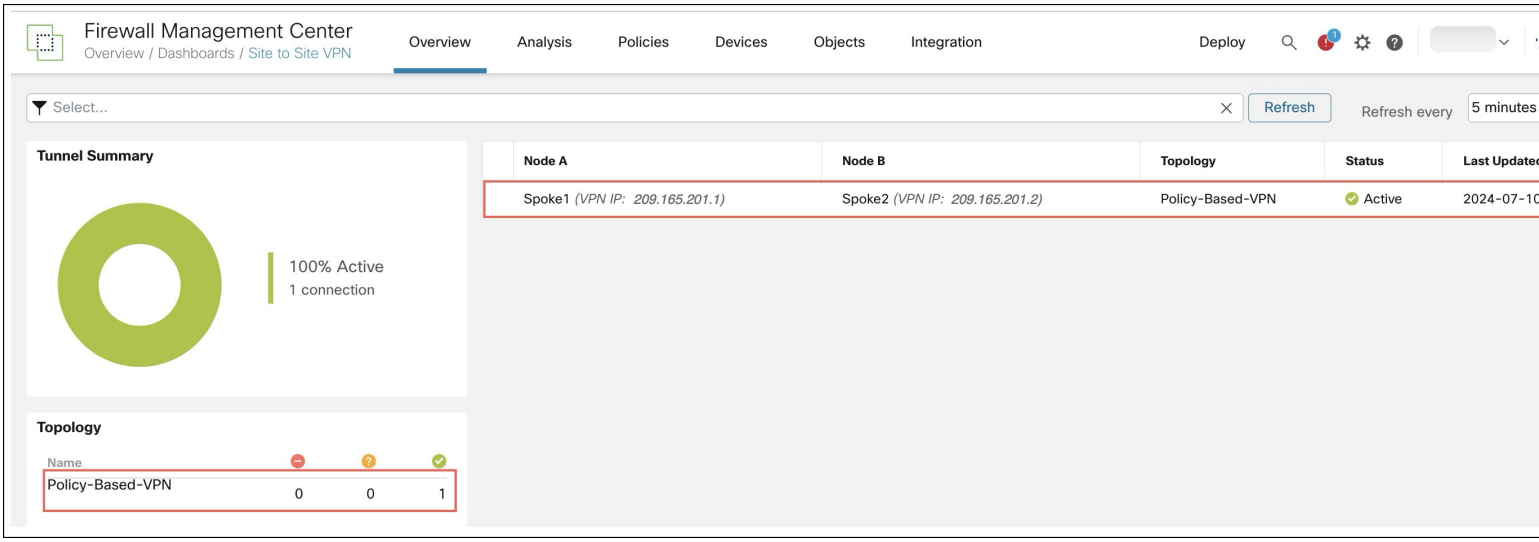
ある中規模企業が、現在、ポリシーベース VPN を使用して 2 台の Threat Defense デバイスでネットワークを運用しているとする。これらのデバイスは、Management Center バージョン 7.4.1 によって管理されています。拡張性の向上やネットワーク管理の簡素化など、ルートベース VPN の利点を認識したネットワーク管理者は、ルートベース VPN への移行を計画しています。この移行を促進するために、管理者は Management Center の VPN ウィザードを使用します。このウィザードは、設定プロセスを合理化し、シームレスな移行を可能にするように設計されています。この移行の目的は、ネットワークの堅牢性と柔軟性を強化し、組織の成長と増大する接続のニーズをサポートすることです。



ポリシーベース VPN トポロジには、以下のパラメータがあります。

Threat Defense デバイス	**保護されたネットワーク（Protected Network）**	**VPN Interface**
Spoke1	198.51.100.16/28	209.165.201.1
スポーク 2	198.51.100.32/28	209.165.201.2

VPN トンネルの詳細を表示するには、[概要（Overview）]>[ダッシュボード（Dashboards）]>[サイト間VPN（Site-to-site VPN）] の順に選択します。



トンネルの詳細を表示するには、Threat Defense デバイスで **show crypto ikev2 sa** と **show crypto ipsec sa** コマンドを使用します。

```
> show crypto ipsec sa
interface: outside
    Crypto map tag: CSM_outside_map, seq num: 1, local addr: 209.165.201.1

      access-list CSM_IPSEC_ACL_1 extended permit ip 198.51.100.16 255.255.255.240 198.51.100.32 255.255.255.240
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (198.51.100.16/255.255.255.240/0/0)
      remote ident (addr/mask/prot/port): (198.51.100.32/255.255.255.240/0/0)
      current_peer: 209.165.201.2


      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1/500    remote crypto endpt.: 209.165.201.2/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 460FEE39
      current inbound spi : A258BF8E

    inbound esp sas:
      spi: 0xA258BF8E (2723725198)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 14, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (4055040/27945)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x460FEE39 (1175449145)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 14, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (3916799/27945)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                 Remote                                fvrf/ivrf     Status
30504265  209.165.201.1/500                     209.165.201.2/500                     Global/Global      READY
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/876 sec
Child sa: local selector  198.51.100.16/0 - 198.51.100.31/65535
          remote selector 198.51.100.32/0 - 198.51.100.47/65535
          ESP spi in/out: 0xa258bf8e/0x460fee39
```

ピアツーピアのポリシーベース VPN のルートベース VPN への移行

ピアツーピアのポリシーベース VPN からルートベース VPN に移行するには以下の手順を実行します。

ステップ	タスク	詳細情報
1	VPN ウィザードを使用して、ピアツーピアのルートベース VPN を設定します。	ピアツーピアのルートベース VPN の設定 （6 ページ）
2	ルーティングプロトコルを設定します。	ルーティングプロトコルの設定 （7 ページ）
3	ポリシーベース VPN を削除します。	-
4	デバイスに設定を展開します。	-
5	VPN トンネルのステータスと設定を確認します。	VPN トンネルのステータスと設定を確認します。 （9 ページ）

ピアツーピアのルートベース VPN の設定

手順

ステップ 1 [デバイス（Devices）] > [サイト間（Site To Site）] を選択します。

ステップ 2 [+サイト間VPN（+ Site To Site VPN）] をクリックします。

ステップ 3 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 4 [ルートベース（VTI）（Route Based (VTI)）] オプションボタンをクリックします。

ステップ 5 ネットワークトポロジとして [ポイントツーポイント（Point to Point）] を選択します。

ステップ 6 [IKEv1] または [IKEv2] チェックボックスをオンにして、IKE ネゴシエーション中に使用する IKE バージョンを選択します。

ステップ 7 [エンドポイント（Endpoints）] タブをクリックします。

ステップ 8 [ノードA（Node A）] について、次のパラメータを設定します。

a) [デバイス（Device）] ドロップダウンリストから [Spoke1] を選択します。

b) [+] をクリックして、静的 VTI を作成します。

[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスにデフォルト設定が入力されます。ただし、以下のパラメータを設定する必要があります。

1. [トンネル送信元（Tunnel Source）] ドロップダウンリストから、静的 VTI の送信元である物理インターフェイスを選択します。隣のドロップダウンリストからこのインターフェイスの IP アドレスを選択します。
2. [IPの設定（Configure IP）] フィールドに、スタティック VTI の IP アドレスを入力します。

   この例では、静的 VTI IP アドレスは 169.254.2.1/30 です。
3. [OK] をクリックします。

ステップ 9 [ノードB（Node B）] について、次のパラメータを設定します。

a) [デバイス（Device）] ドロップダウンリストから [Spoke2] を選択します。

b) [+] をクリックして、静的 VTI を作成します。

静的 VTI パラメータを設定するには、手順 8bi ～ 8biii を繰り返します。この例では、静的 VTI IP アドレスは 169.254.2.2/30 です。

ステップ 10 [保存（Save）] をクリックします。

ルーティングプロトコルの設定

ルートベース VPN の場合は、BGP、OSPF、 EIGRP などのルーティングプロトコルを設定する必要があります。ダイナミック VTI はスタティックルートをサポートしていません。この例では、ルーティングプロトコルとして BGP を使用します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 Spoke1 の横にある編集アイコンをクリックします。

ステップ 3 [ルーティング（Routing）] タブをクリックします。

ステップ 4 左側のペインで、[一般設定（General Settings）] > [BGP] を選択します。

ステップ 5 [BGPの有効化（Enable BGP）] チェックボックスをオンにします。

ステップ 6 [AS番号（AS Number）] フィールドにデバイスの AS 番号を入力します。

ステップ 7 他のフィールドは任意です。要件に応じて設定してください。

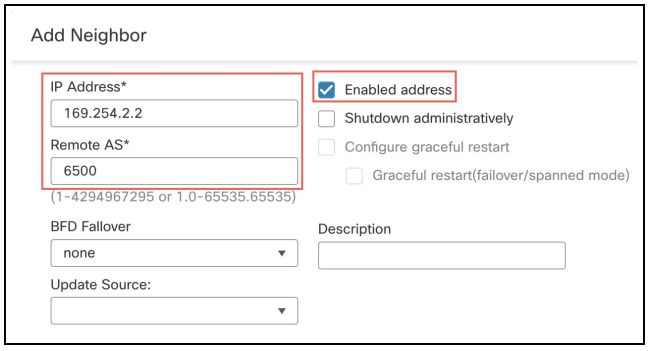
ステップ 8 [保存（Save）] をクリックします。

ステップ 9 左側のペインで、[BGP] > [IPv4] を選択します。

ステップ 10 [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。

ステップ 11 [ネイバー（Neighbor）] ダイアログボックスで、[+追加（+Add）] をクリックします。

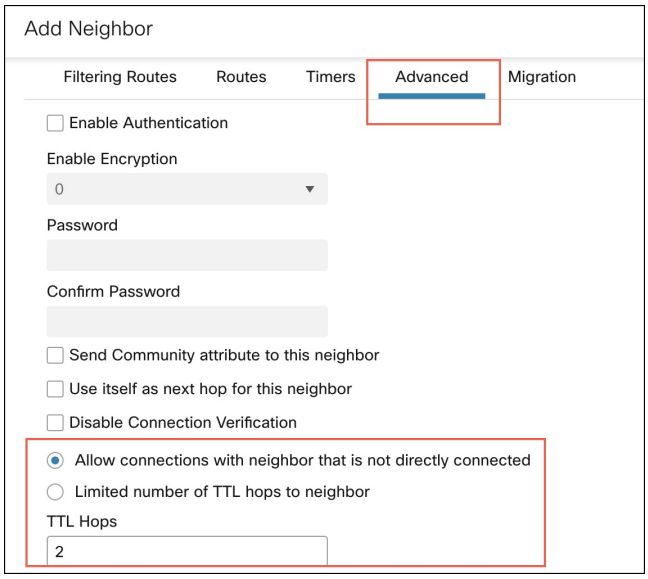
[ネイバーの追加（Add Neighbor）] ダイアログボックスで、以下のパラメータを設定します。



a) [IPアドレス（IP Address）] フィールドで、BGP ピアの IP アドレスを入力します。

この例では、スポーク 2 の VTI IP アドレス（169.254.2.2）です。

b) [リモートAS（Remote AS）] フィールドに AS 番号を入力します。
c) [有効なアドレス（Enabled address）] チェックボックスをオンにします。
d) 他のフィールドは任意です。要件に応じて設定してください。
e) （任意）デバイスが異なるリージョンにある場合、外部ボーダー ゲートウェイ プロトコル（eBGP）を使用してルーティング情報を交換するため、マルチホップパラメータを設定する必要があります。



1. [詳細（Advanced）] タブをクリックします。
2. [直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）] オプションボタンを選択します。
3. [TTLホップ（TTL Hops）] フィールドに、値として 2 を入力します。
4. 他のフィールドは任意です。要件に応じて設定してください。

f) [OK] をクリックします。

ステップ 12 [ネットワーク（Networks）] タブをクリックし、[追加（Add）] をクリックして、ネットワークをピアにアドバタイズします。

[ネットワークの追加（Add Networks）] ダイアログボックスで、以下のパラメータを設定します。

a) [ネットワーク（Network）] ドロップダウンリストから、デバイスの保護されたネットワークを選択します。

この例の Spoke1 では、保護されたネットワーク 198.51.100.16/28 です。

b) （任意）[ルートマップ（Route Map）] ドロップダウンリストから、アドバタイズされるネットワークをフィルタ処理するために検証する必要のあるルートマップを選択します。デフォルトでは、すべてのネットワークが再配布されます。
c) [OK] をクリックします。

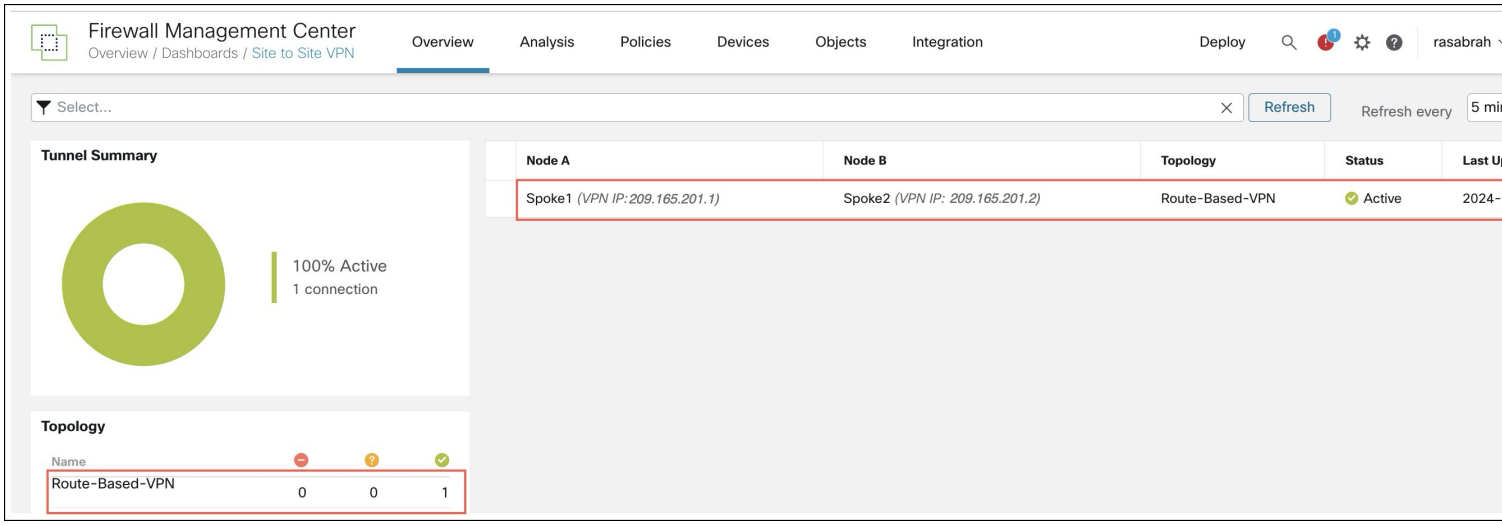
ステップ 13　[保存（Save）] をクリックします。

ステップ 14　ピア（Spoke2）で BGP を設定するには、ステップ 1 ～ 13 を繰り返します。

ステップ 15　両方のデバイスに設定を展開します。

VPN トンネルのステータスと設定を確認します。

VPN トンネルの詳細を表示するには、[概要（Overview）]>[ダッシュボード（Dashboards）]>[サイト間VPN（Site-to-site VPN）] の順に選択します。



トンネルの詳細を表示するには、デバイスで **show crypto ipsec sa** と **show crypto ikev2 sa** コマンドを使用します。

```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 209.165.201.1

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 209.165.201.2


      #pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
      #pkts decaps: 31, #pkts decrypt: 31, #pkts verify: 31
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 24, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1/500    , remote crypto endpt.: 209.165.201.2/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: EDA26B0F
      current inbound spi : BBAE8073

    inbound esp sas:
      spi: 0xBBAE8073 (3148775539)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 6, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055037/24765)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0xFFFFFFFF
    outbound esp sas:
      spi: 0xEDA26B0F (3986844431)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 6, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (3916798/24765)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remot
 13394065  209.165.201.1/500                                    209.16
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign:
      Life/Active Time: 86400/2485 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xbbae8073/0xeda26b0f
```

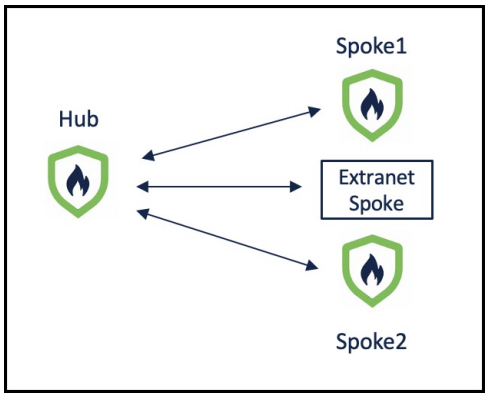
Threat Defense デバイスでのルーティング設定の確認

ハブとスポークの BGP、OSPF、または EIGRP ルートを確認するには、デバイスで **show route** コマンドを使用します。**show bgp**、**show eigrp**、または **show ospf** コマンドを使用することもできます。

ユースケース 2：ハブとスポークのポリシーベース VPN をルートベース VPN に移行する

シナリオ

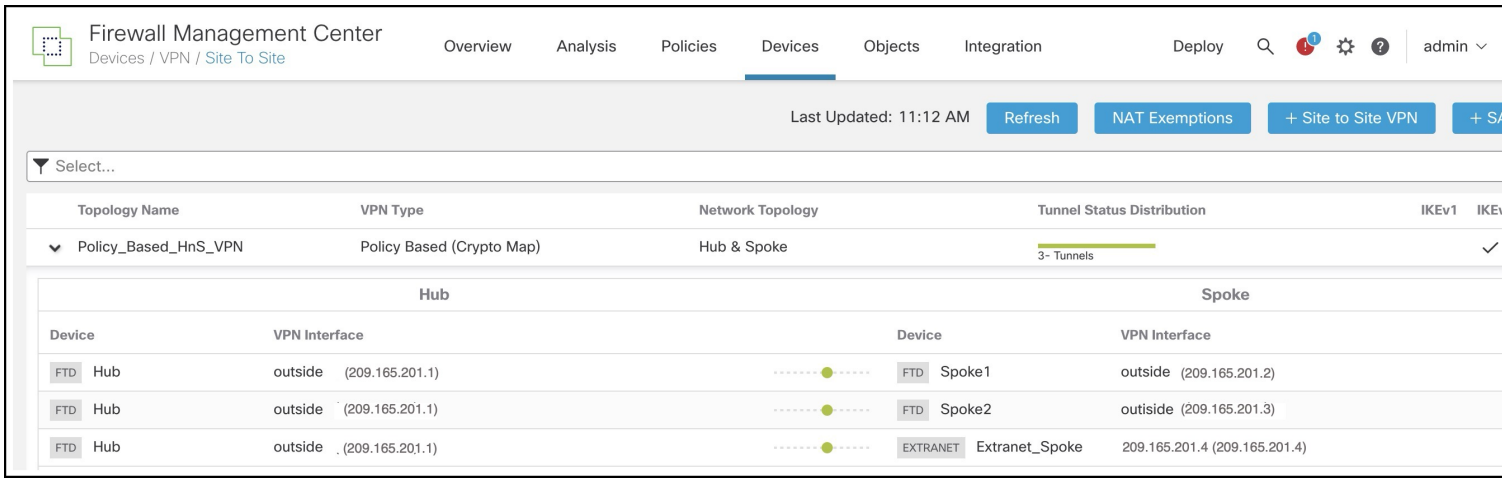
現在、ある中規模企業には、3 つの Threat Defense デバイス（1 つのハブと 2 つのスポーク）と 1 つのエクストラネットデバイスで構成されるハブ アンド スポークネットワークがあります。これらのデバイスは、Management Center バージョン 7.4.1 によって管理されるポリシーベース VPN を使用して接続されています。ルートベース VPN の利点と、ネットワークを簡単に拡張できる特徴を考慮して、ネットワーク管理者は、Management Center の VPN ウィザードを使用してこのネットワークをルートベース VPN に移行することを計画しています。



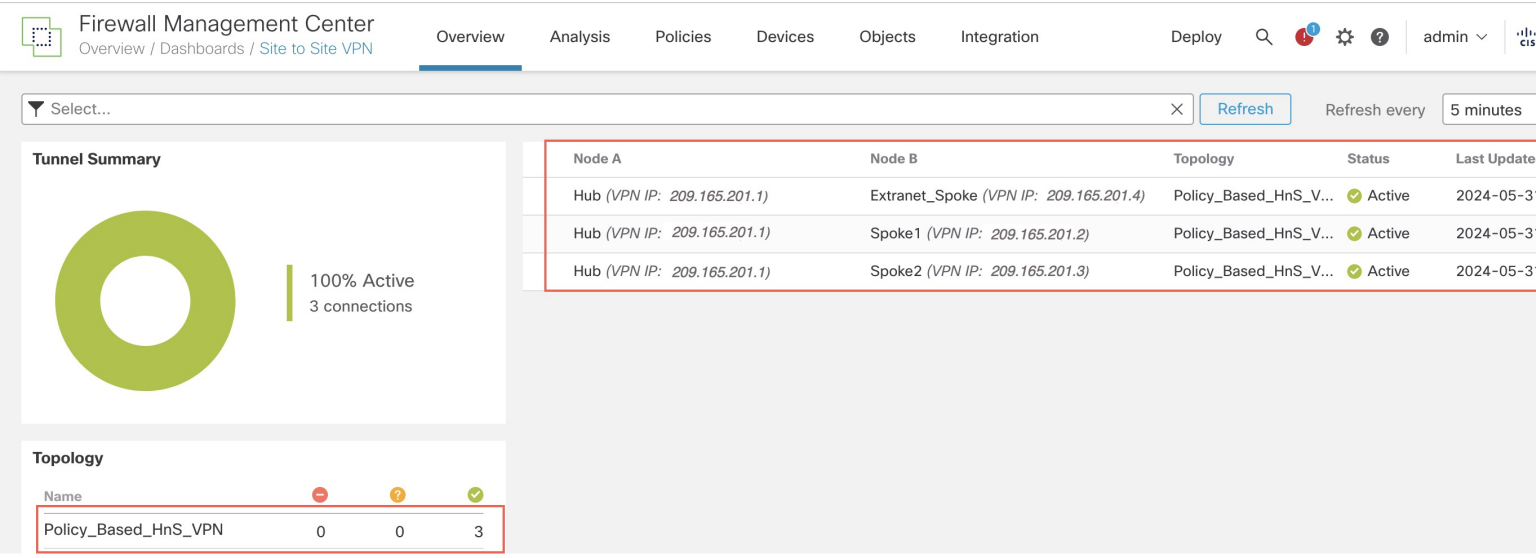
ポリシーベース VPN には以下のパラメータがあります。

デバイス	保護されたネットワーク（Protected Network）	VPN Interface
ハブ	198.51.100.16/28	209.165.201.1
Spoke1	198.51.100.32/28	209.165.201.2
Spoke2	198.51.100.64/28	209.165.201.3
エクストラネットスポーク	209.165.200.225/27	209.165.201.4

ポリシーベース VPN は、[サイト間VPNの概要（Site-to-Site VPN Summary）] ページで確認できます。



ポリシーベース VPN の詳細は、[サイト間VPNダッシュボード（Site-to-Site VPN Dashboard）] で確認できます。



VPN トンネルの詳細を表示するには、デバイスで **show crypto ikev2 sa** と **show crypto ipsec sa** コマンドを使用します。

```
> show crypto ipsec sa
interface: outside
    Crypto map tag: CSM_outside_map, seq num: 5, local addr: 209.165.201.1

      access-list CSM_IPSEC_ACL_1 extended permit ip 198.51.100.16 255.255.255.224 198.51.100.32 255.255.255.224
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (198.51.100.16/255.255.255.224/0/0)
      remote ident (addr/mask/prot/port): (198.51.100.32/255.255.255.224/0/0)
      current_peer: 209.165.201.2


      #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 2, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1/500   remote crypto endpt.: 209.165.201.2/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: C470054C
      current inbound spi : 307C5CE9

    inbound esp sas:
      spi: 0x307C5CE9 (813456617)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 74, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (4285440/28168)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0xC470054C (3295675724)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 74, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (4147199/28168)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001

    Crypto map tag: CSM_outside_map, seq num: 4, local addr: 209.165.201.1

      access-list CSM_IPSEC_ACL_2 extended permit ip  198.51.100.16 255.255.255.224 198.51.100.64 255.255.255.224
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (198.51.100.16/255.255.255.224/0/0)
      remote ident (addr/mask/prot/port): (198.51.100.64/255.255.255.224/0/0)
      current_peer: 209.165.201.3


      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1      remote crypto endpt.: 209.165.201.3
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 29E5932E
      current inbound spi : FE2CD7DC
```

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:17, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  fvrf/ivrf     Status
169182659 209.165.201.1                           209.165.201.2/500                                     READY
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/131 sec
Child sa: local selector    198.51.100.16 - 198.51.100.31
          remote selector   198.51.100.32 - 198.51.100.47
          ESP spi in/out: 0x307c5ce9/0xc470054c

IKEv2 SAs:

Session-id:18, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  fvrf/ivrf     Status
171392979 209.165.201.1/500                       209.165.201.3/500                                     READY
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/115 sec
Child sa: local selector     198.51.100.16 - 198.51.100.31
          remote selector    198.51.100.64 - 198.51.100.79
          ESP spi in/out: 0xfe2cd7dc/0x29e5932e
```

ハブとスポークのポリシーベース VPN のルートベース VPN への移行

前提条件

エクストラネットデバイスの場合：

- サードパーティの展開で、エクストラネットデバイスに必要な設定を行う必要があります。
- エクストラネットでルートベースの VPN を使用する場合は、エクストラネットデバイスが以下をサポートしている必要があります。
  - スタティック VTI
  - BGP、OSPF、または EIGRP（ルーティングプロトコルとして）。ダイナミック VTI はスタティックルートをサポートしていません。
- エクストラネットでポリシーベースの VPN を使用する場合、ダイナミック VTI ハブはポリシーベースの VPN をサポートし、エクストラネットとのトンネルを形成できます。

手順

ハブとスポークのポリシーベース VPN をルートベース VPN に移行するには、以下の手順を実行します。

ステップ	タスク	詳細情報
1	ハブとスポークでループバック インターフェイスを設定します。 このループバック インターフェイスは、両方のデバイスで VPN トンネル ネットワークをエミュレートします。	ハブとスポークでのループバック インターフェイスの設定 （15 ページ）
2	VPN ウィザードを使用して、ハブとスポークのルートベース VPN を設定します。	ハブとスポークのルートベース VPN の設定 （16 ページ）

ステップ	タスク	詳細情報
3	ルーティングプロトコルを設定します。ルーティングプロトコルとして BGP、EIGRP、または OSPF を使用できます。	• ハブとスポークでの BGP の設定（19 ページ） • ハブとスポークでの EIGRP の設定（18 ページ） • ハブとスポークでの OSPF の設定（21 ページ）
3	ポリシーベース VPN を削除します。	-
4	デバイスに設定を展開します。	-
5	VPN トンネルのステータスと設定を確認します。	ルートベース VPN のトンネルのステータスと設定の確認 （23 ページ）

ハブとスポークでのループバック インターフェイスの設定

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 デバイスの横にある編集アイコンをクリックします。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 [インターフェイスの追加（Add Interfaces）] ドロップダウンリストから、[ループバック インターフェイス（Loopback Interface）] を選択します。

[ループバック インターフェイスの追加（Add Loopback Interface）] ダイアログボックスで、次のパラメータを設定します。

a) [名前（Name）] フィールドに、ループバック インターフェイスの名前を入力します。
b) [有効（Enabled）] チェックボックスをオンにします。
c) [ループバックID（Loopback ID）] フィールドに、1 ～ 1024 の ID を入力します。
d) [IPv4] タブまたは [IPv6] タブをクリックします。
e) [IPアドレス（IP Address）] フィールドに、ループバック インターフェイスの IP アドレスを入力します。
f) [OK] をクリックします。

ステップ 5 他の 2 台の Threat Defense デバイスでループバック インターフェイスを設定するには、ステップ 1 ～ 4 を繰り返します。

この例では、デバイスの VPN トンネルネットワークをエミュレートするループバック インターフェイスは Tunnel_Loopback と呼ばれます。

以下の表に、この例で使用するデバイスのループバック インターフェイスを示します。

デバイス	保護されたネットワーク（Protected Network）	Tunnel_Loopback インターフェイス	VPN Interface
ハブ	198.51.100.16/28	192.0.2.1/24	209.165.201.1
Spoke1	198.51.100.32/28	192.0.2.2/24	209.165.201.2
Spoke2	198.51.100.64/28	192.0.2.3/24	209.165.201.3
エクストラネットスポーク	209.165.200.225/27	192.0.2.4/24	209.165.201.4

ループバック インターフェイスについては、以下の点に注意してください。

- ルーティングプロトコルとして BGP を使用する場合：/32 マスクを使用すると、ピア IP アドレスを手動で定義する場合に IP アドレスを節約できます。
- OSPF または EIGRP をルーティングプロトコルとして使用する場合、OSPF または EIGRP のネイバーシップがデフォルトで確立されるためには、ピアデバイスが同じサブネット内にある必要があります。/32 マスクを使用する場合は、ピア IP アドレスを手動で定義できます。

ハブとスポークのルートベース VPN の設定

手順

ステップ 1 [デバイス（Devices）] > [サイト間（Site To Site）] を選択します。

ステップ 2 [+サイト間VPN（+ Site To Site VPN）] をクリックします。

ステップ 3 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 4 [ルートベース（VTI）（Route Based (VTI)）] オプションボタンをクリックします。

ステップ 5 ネットワークトポロジとして [ハブアンドスポーク（Hub and Spoke）] を選択します。

ステップ 6 [IKEv1] または [IKEv2] チェックボックスをオンにして、IKE ネゴシエーション中に使用する IKE バージョンを選択します。

ステップ 7 [エンドポイント（Endpoints）] タブをクリックします。

ステップ 8 [ハブノード（Hub Node）] について、次のパラメータを設定します。

[エンドポイントの追加（Add Endpoint）] ダイアログボックスで、次のパラメータを設定します。

a) [デバイス（Device）] ドロップダウンリストから [ハブ（Hub）] を選択します。

b) [ダイナミック仮想トンネルインターフェイス（Dynamic Virtual Tunnel Interface）] ドロップダウンリストの横にある [+] をクリックします。

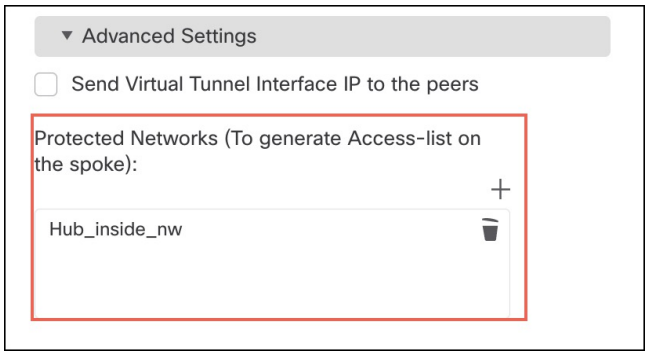
[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスにデフォルト設定が入力されます。ただし、次のパラメータを設定する必要があります。

1. [トンネル送信元（Tunnel Source）] ドロップダウンリストから、ダイナミック VTI の送信元である物理インターフェイスを選択します。隣のドロップダウンリストからこのインターフェイスの IP アドレスを選択します。
2. [借用IP（Borrow IP）] ドロップダウンリストから、ループバック インターフェイスを選択します。ダイナミック VTI はこの IP アドレスを継承します。

   この例では、借用 IP は Tunnel_Loopback インターフェイス（192.0.2.1/24）です。
3. [OK] をクリックします。

c) （任意）ハブの保護されたネットワークを VTI 設定に追加する場合は、以下の手順を実行します。

1. [詳細設定（Advance Settings）] を展開します。
2. [保護されたネットワーク（Protected Networks）] の横にある [+] をクリックします。
3. [ネットワークオブジェクト（Network Objects）] ダイアログボックスで、[使用可能なネットワーク（Available Networks）] リストからハブの保護されたネットワークを選択します。
4. [追加（Add）] をクリックして、[選択したネットワーク（Selected Networks）] に移動します。
5. [OK] をクリックします。



d) [OK] をクリックします。

ステップ 9 [スポークノード（Spoke Notdes）] の場合は、[+] をクリックしてスポークを設定します。

[エンドポイントの追加（Add Endpoint）] ダイアログボックスで、次のパラメータを設定します。

a) [デバイス（Device）] ドロップダウンリストから [スポーク1（Spoke1）] を選択します。
b) [静的仮想トンネルインターフェイス（Static Virtual Tunnel Interface）] ドロップダウンリストの横にある [+] をクリックします。

   [仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスにデフォルト設定が入力されます。ただし、次のパラメータを設定する必要があります。

1. [トンネル送信元（Tunnel Source）] ドロップダウンリストから、静的 VTI の送信元である物理インターフェイスを選択します。 隣のドロップダウンリストからこのインターフェイスの IP アドレスを選択します。

2. [借用IP（Borrow IP）] ドロップダウンリストから、ループバック インターフェイスを選択します。静的 VTI はこの IP アドレスを継承します。

   この例では、Spoke1 の 借用 IP は Tunnel_Loopback インターフェイス（192.0.2.2/24）です。

3. [OK] をクリックします。

c) （任意）スポークの保護されたネットワークを VTI 設定に追加する場合は、手順 8c を繰り返します。

d) [OK] をクリックします。

ステップ 10 手順 9 を繰り返して、Spoke2 を設定します。

ステップ 11 エクストラネットデバイスを設定するには、[スポークノード（Spoke Nodes）] の横にある [+] をクリックします。

[エンドポイントの追加（Add Endpoint）] ダイアログボックスで、次のパラメータを設定します。

a) [デバイス（Devices）] ドロップダウンリストから、[エクストラネット（Extranet）] を選択します。

b) [デバイス名（Device Name）] フィールドにデバイス名を入力します。

c) [エンドポイントIPアドレス（Endpoint IP Address）] で、[静的（Static）] または [動的（Dynamic）] オプションボタンクリックます。

d) デバイスの IP アドレスを入力します。

e) [OK] をクリックします。

ハブとスポークでの EIGRP の設定

ルーティングプロトコルとして EIGRP を選択した場合は、以下の手順を実行します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 ハブの横にある編集アイコンをクリックします。

ステップ 3 [ルーティング（Routing）] タブをクリックします。

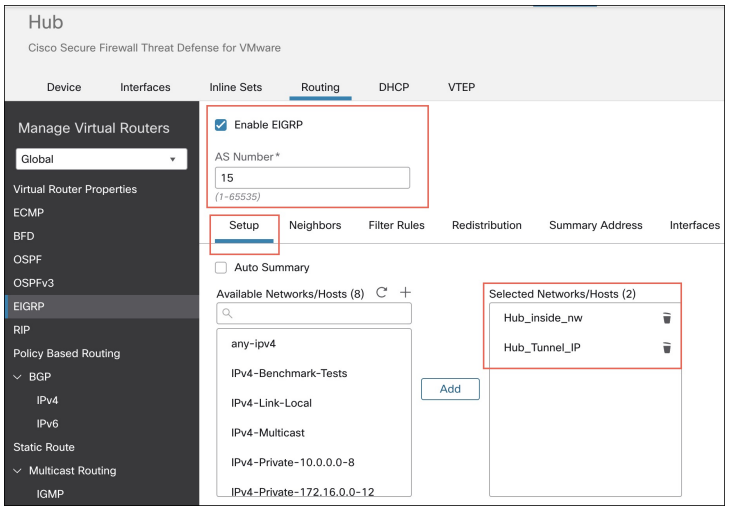
ステップ 4 左側のペインで、[EIGRP] を選択します。

ステップ 5 [EIGRPルーティングの有効化（Enable EIGRP routing）] チェックボックスをオンにします。

ステップ 6 [AS番号（AS Number）] フィールドにデバイスの AS 番号を入力します。

ステップ 7 [設定（Setup）] タブをクリックします。

ステップ 8 [使用可能なネットワーク/ホスト（Available Networks/Hosts）] リストから、デバイスの保護されたネットワークと VPN トンネルネットワークを選択します。これらのネットワークのネットワークオブジェクトがない場合は、[+追加（+ Add）] をクリックして作成します。



ステップ 9　他のフィールドは任意です。要件に応じて設定してください。

ステップ 10　[保存（Save）] をクリックします。

ステップ 11　Spoke1 および Spoke2 で EIGRP を設定するには、ステップ 1 ～ 10 を繰り返します。

ステップ 12　すべてのデバイスに設定を展開します。

ハブとスポークでの BGP の設定

ルーティングプロトコルとして BGP を選択した場合は、以下の手順を使用します。

手順

ステップ 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2　ハブの横にある編集アイコンをクリックします。

ステップ 3　[ルーティング（Routing）] タブをクリックします。

ステップ 4　左側のペインで、[一般設定（General Settings）] > [BGP] を選択します。

ステップ 5　[BGPの有効化（Enable BGP）] チェックボックスをオンにします。

ステップ 6　[AS番号（AS Number）] フィールドにデバイスの AS 番号を入力します。

ステップ 7　他のフィールドは任意です。要件に応じて設定してください。

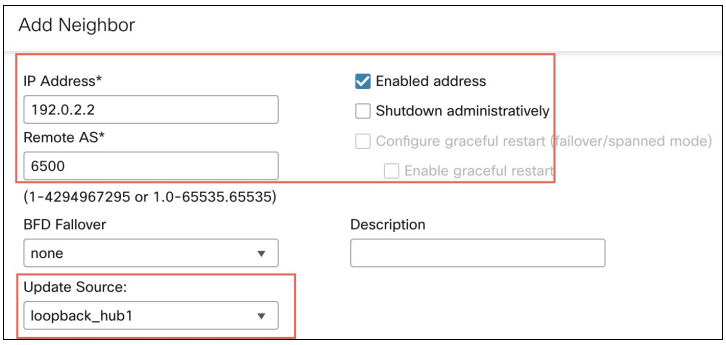
ステップ 8　[保存（Save）] をクリックします。

ステップ 9　左側のペインで、[BGP] > [IPv4] を選択します。

ステップ 10　[IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。

ステップ 11　[ネイバー（Neighbor）] タブをクリックし、[+追加（+Add）] をクリックします。

[ネイバーの追加（Add Neighbor）] ダイアログボックスで、以下のパラメータを設定します。



a) [IPアドレス（IP Address）] フィールドで、BGP ピアの IP アドレスを入力します。

この例では、Spoke1 の VTI IP アドレス（192.0.2.2/24）です。

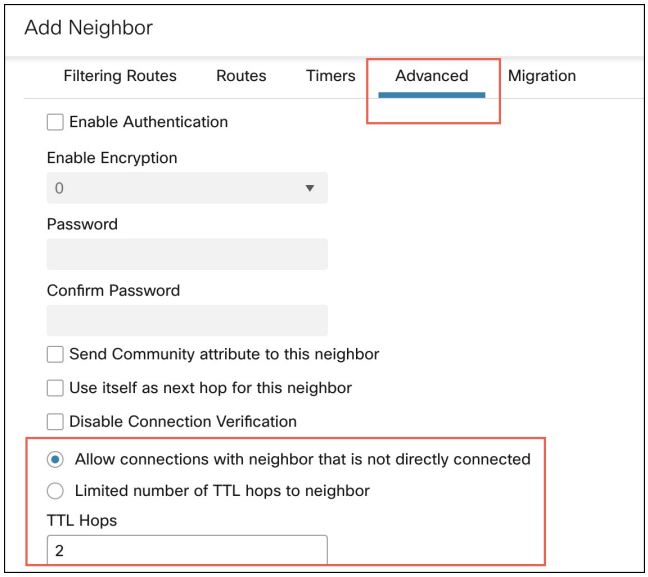
b) [リモートAS（Remote AS）] フィールドに AS 番号を入力します。

c) [有効なアドレス（Enabled address）] チェックボックスをオンにします。

d) [更新の送信元（Update Source）] ドロップダウンリストからループバック インターフェイスを選択します。

e) 他のフィールドは任意です。要件に応じて設定してください。

f) （任意）デバイスが異なるリージョンにある場合、外部ボーダー ゲートウェイ プロトコル（eBGP）を使用してルーティング情報を交換するため、マルチホップパラメータを設定する必要があります。



1. [詳細（Advanced）] タブをクリックします。
2. [直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）] オプションボタンを選択します。
3. [TTLホップ（TTL Hops）] フィールドに、値として 2 を入力します。
4. 他のフィールドは任意です。要件に応じて設定してください。

g) [OK] をクリックします。

ステップ 12 Spoke2 をネイバーとして追加には、ステップ 11 を繰り返します。

ステップ 13 [Networks] タブをクリックします。

ステップ 14 [+追加（+ Add）] をクリックして、ネットワークをピアにアドバタイズします。

[ネットワークの追加（Add Networks）] ダイアログボックスで、以下のパラメータを設定します。

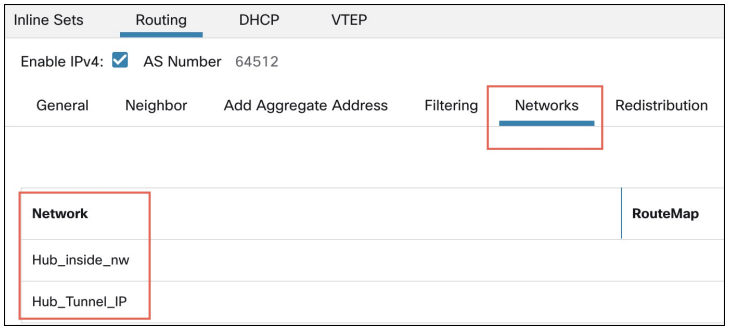
a) **[ネットワーク（Network）]** ドロップダウンリストから、デバイスの保護されたネットワークを選択します。

この例のハブでは、保護されたネットワーク 198.51.100.16/28 です。

b) （任意）[ルートマップ（Route Map）] ドロップダウンリストから、アドバタイズされるネットワークをフィルタ処理するために検証する必要のあるルートマップを選択します。デフォルトでは、すべてのネットワークが再配布されます。

c) [OK] をクリックします。

ステップ 15 トンネルを介してアドバタイズされる VPN トンネルネットワークを追加には、ステップ 14 を繰り返します。



ステップ 16 [保存（Save）] をクリックします。

ステップ 17 ピア（Spoke1 および Spoke2）で BGP を設定するには、ステップ 1 ～ 16 を繰り返します。

ステップ 18 両方のデバイスに設定を展開します。

ハブとスポークでの OSPF の設定

ルーティングプロトコルとして OSPF を選択した場合は、以下の手順を使用します。

手順

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 ハブの横にある編集アイコンをクリックします。

ステップ 3 [ルーティング（Routing）] タブをクリックします。

ステップ 4 左側のペインで、[OSPF] を選択します。

ステップ 5 [プロセス1（Process 1）] チェックボックスをオンにして、OSPF インスタンスを有効にします。

ステップ 6 [インターフェイス（Interface）] タブをクリックします。

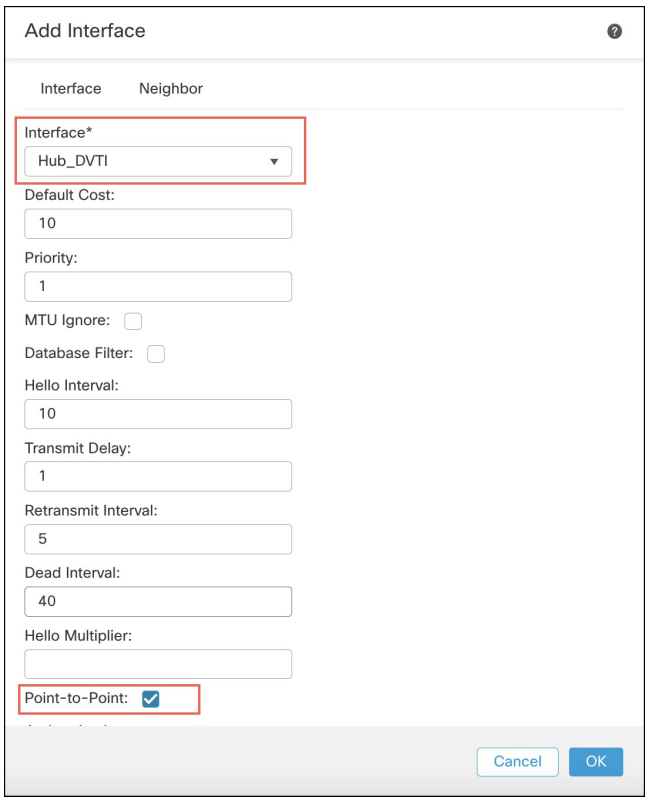
ステップ 7 [追加（Add）] をクリックします。

[インターフェイスの追加（Add Interface）] ダイアログボックスで、次のパラメータを設定します。

a) [インターフェイス（Interface）] ドロップダウンリストから、デバイスのダイナミック VTI インターフェイスを選択します。

b) [ポイントツーポイント（Point-to-point）] チェックボックスをオンにして、VPN トンネル経由で OSPF ルートを送信します。

c) 残りのフィールドではデフォルト値を使用します。



d) [OK] をクリックします。

ステップ 8 [エリア（Area）] タブをクリックします。

ステップ 9 [追加（Add）] をクリックします。

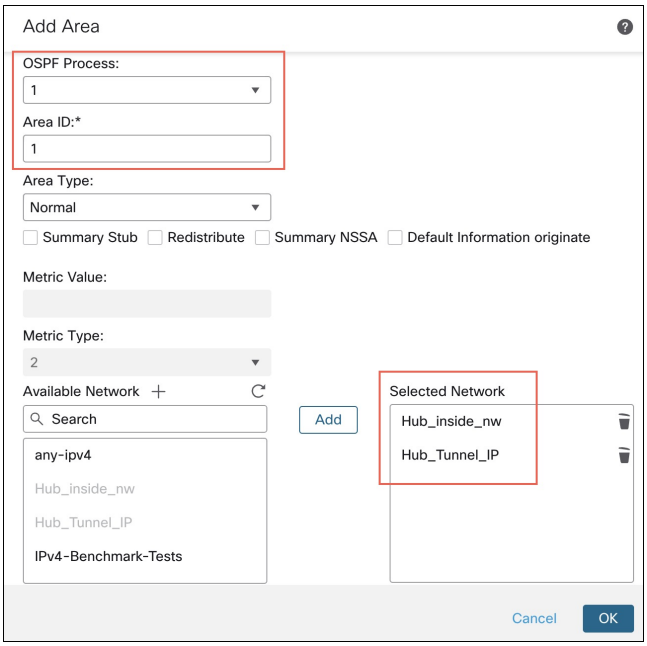
[エリアの追加（Add Area）] ダイアログボックスで、以下のパラメータを設定します。

a) [OSPFプロセス（OSPF Process）] ドロップダウンリストから [1] を選択します。

b) [エリアID（Area ID）] フィールドに [1] を入力します。

c) 残りのフィールドではデフォルト値を使用します。

d) [使用可能なネットワーク（Available Network）] リストから、デバイスの保護されたネットワークと VPN トンネルネットワークを選択します。これらのネットワークのネットワークオブジェクトがない場合は、[+] をクリックして作成します。



e) [OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

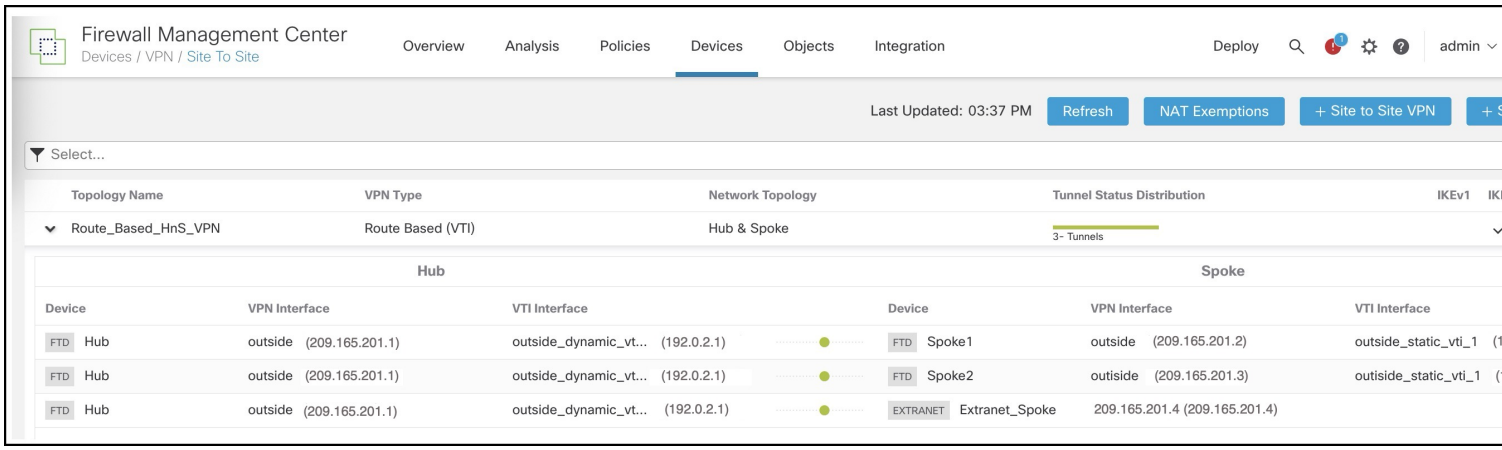
ステップ 11 Spoke1 および Spoke2 で OSPF を設定するには、手順 1 ～ 10 を繰り返します。

ステップ 12 すべてのデバイスに設定を展開します。

ルートベース VPN のトンネルのステータスと設定の確認

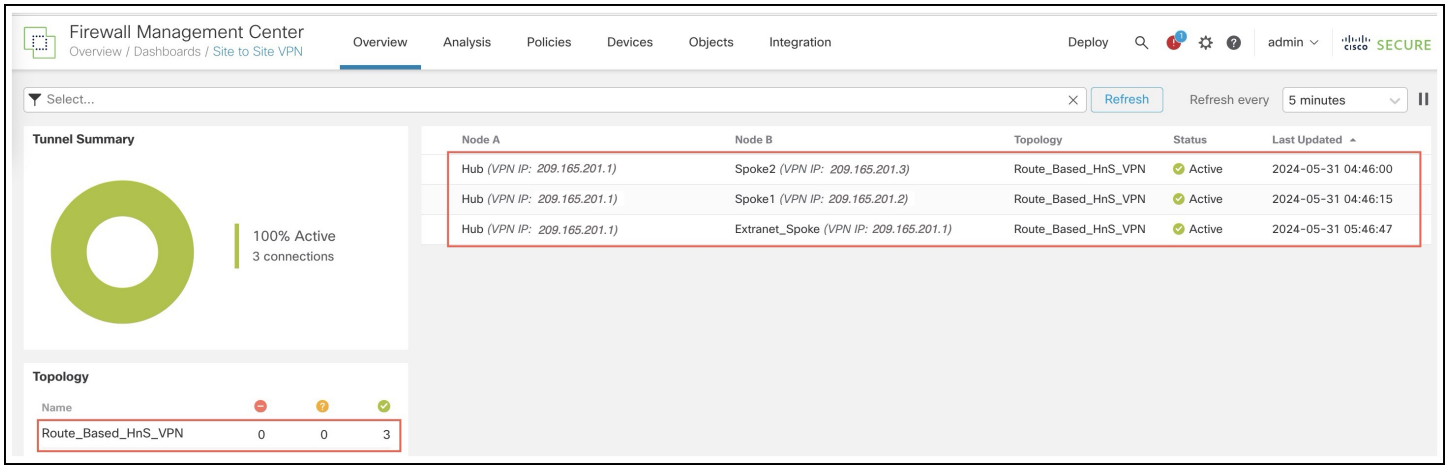
[サイト間VPN概要（Site-to-Site VPN Summary）] ページでのトンネルステータスの確認

VPN トンネルのステータスを確認するには、[デバイス（Device）] > [VPN] > [サイト間（Site To Site）] の順に選択します。



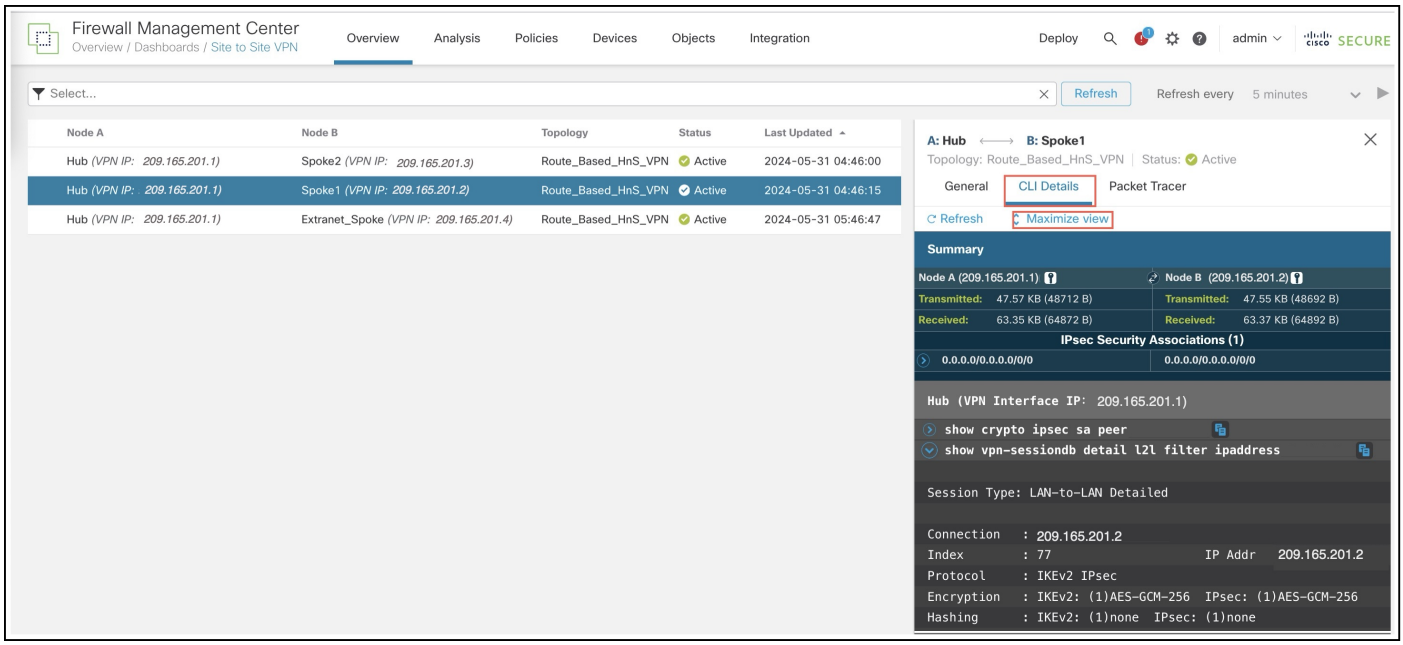
[サイト間VPN（Site-to-site VPN）] ダッシュボードでのトンネルステータスの確認

1. VPN トンネルの詳細を表示するには、[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site-to-site VPN）] の順に選択します。



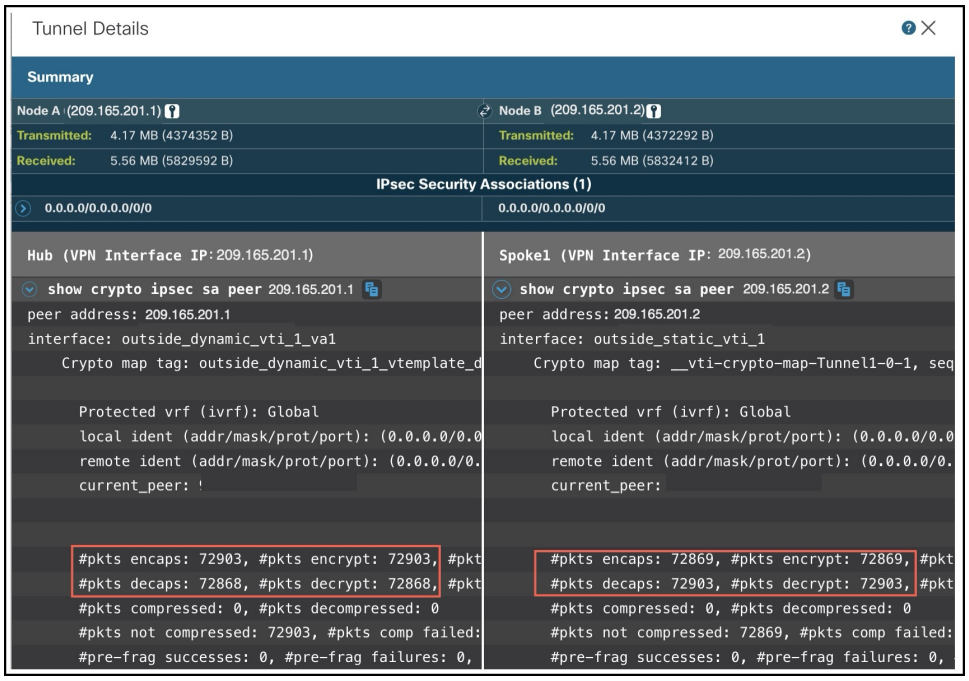
2. 各トンネルで、トポロジの上にカーソルを置き、[表示（View）] アイコン をクリックしてトンネルに関する詳細情報を表示します。

3. [CLIの詳細（CLI Details）] タブをクリックします。

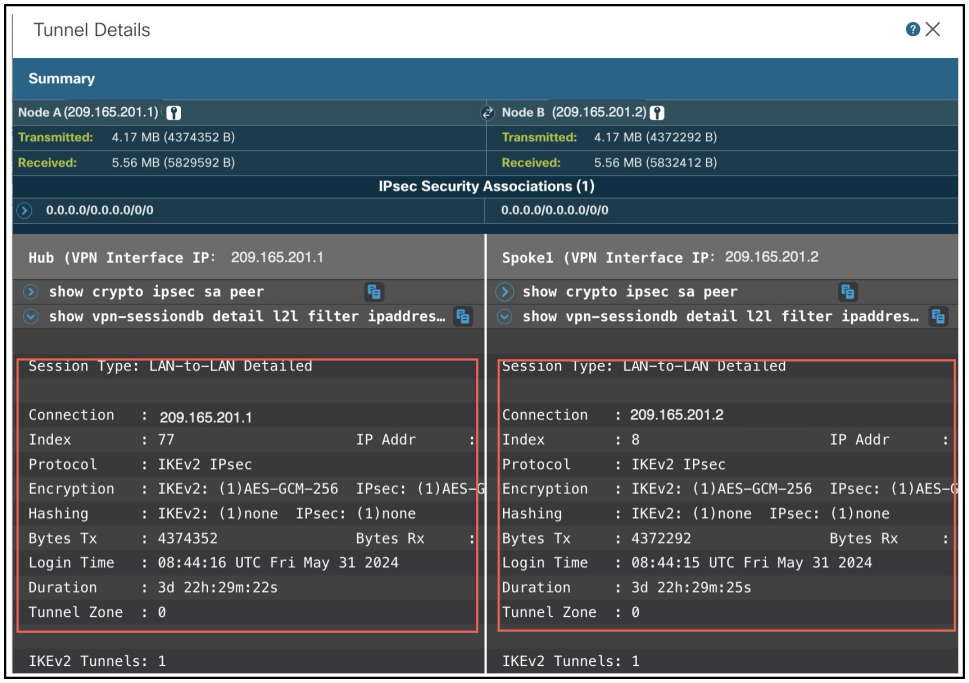


4. [ビューの最大化（Maximize View）] をクリックします。以下のコマンドの出力を表示できます。

   • **show crypto sa peer**：トンネルを介して送信されたパケットの数を表示します。



- **show vpn-sessiondb detail l2lfilter ipaddress**：VPN 接続のより詳細なデータを表示します。



Threat Defense デバイスでのルーティング設定の確認

ハブとスポークの BGP、OSPF、または EIGRP ルートを確認するには、Management Center または デバイスの CLI を使用して、デバイスで **show route** コマンドを使用します。**show bgp**、**show ospf**、または **show eigrp** コマンドを使用することもできます。

1. Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
2. デバイスの横にある編集アイコンをクリックします。
3. [デバイス（Device）] タブをクリックします。
4. [全般（General）] カードの [CLI] をクリックします。

   [CLI トラブルシュート（CLI Troubleshoot）] ウィンドウで、[コマンド（Command）] フィールドに **show route** と入力し、[実行（Execute）] をクリックします。

Threat Defense デバイスの仮装トンネルインターフェイスの表示

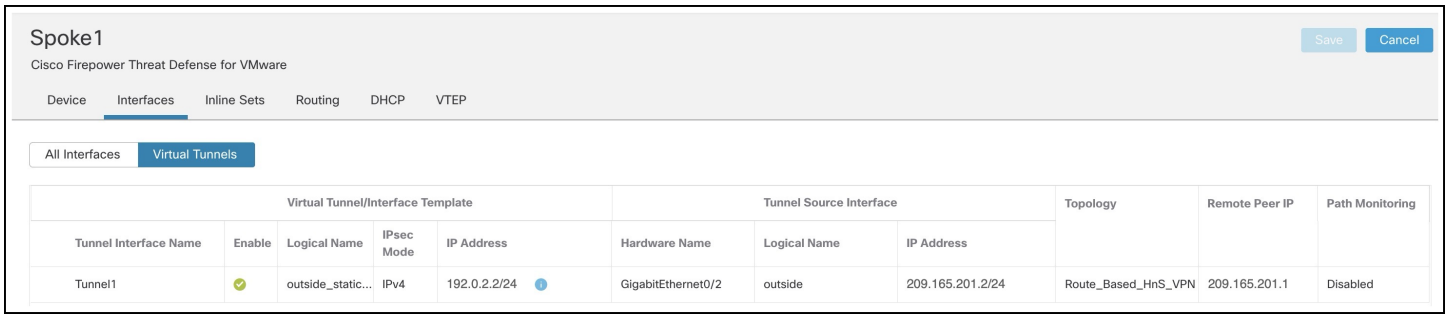
ハブのダイナミック VTI とスポークの静的 VTI を表示するには、以下の手順を実行します。

1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
2. デバイスの横にある編集アイコンをクリックします。
3. [インターフェイス（Interfaces）] タブをクリックします。
4. [仮想トンネル（Virtual Tunnels）] タブをクリックします。

VTI ごとに、名前、IP アドレス、IPsec モード、トンネル送信元インターフェイスの詳細、トポロジ、リモート ピア IP などの詳細を表示できます。

ハブのダイナミック VTI と、動的に作成されたリモート対応アクセスインターフェイスを次の図に示します。

Spoke1 で作成された静的 VTI を次の図に示します。



ルートベースの VPN トンネルのトラブルシューティング

展開後に、次の CLI コマンドとツールを使用して、Threat Defense デバイスのルートベースの VPN トンネルに関連する問題をデバッグします。

CLI とデバッグコマンド

コマンド	説明
ping	ピアの外部 IP アドレスに ping を実行して、デバイス間の接続を確認します。
show vpnsession db	現在の VPN セッションに関する概要情報を表示します。
debug crypto condition peer <peer-IP>	特定のピアの条件付きデバッグを有効にする
debug vti 255	仮想トンネルインターフェイス情報をデバッグする

パケットトレーサ

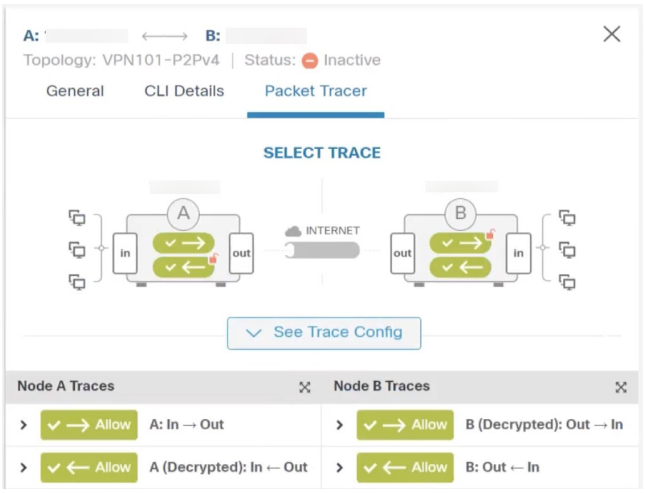
パケットトレーサツールを使用すると、送信元および宛先のアドレスとプロトコルの特性によってパケットをモデル化することにより、ポリシー設定をテストできます。設定の確認に加えて、このツールを使用して、パケットがアクセスを拒否されるなどの予期せぬ動作をデバッグできます。

Threat Defense デバイスでパケットトレーサを使用するには、[デバイス（Devices）]、[パケットトレーサ（Packet Tracer）] の順に選択します。このツールを使用するには、管理者またはメンテナンスユーザーである必要があります。

[サイト間VPNダッシュボード（Site to Site VPN Dashboard）] のパケットトレーサを使用して、2 台の Threat Defense デバイス間の VPN トンネルをトラブルシュートすることもできます。

1. [概要（Overview）] > [ダッシュボード（Dashboards）] の順に選択します。
2. 各トンネルで、トポロジの上にカーソルを置き、[表示（View）] アイコンをクリックしてトンネルに関する詳細情報を表示します。
3. [パケット トレーサ（Packet Tracer）] タブをクリックします。
4. パラメータを設定します。
5. [今すぐトレース（Trace Now）] をクリックします。

6. トレースが完了したら、各モジュールの結果を含むトレースの出力を表示できます。



【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。