ダイナミック仮想トンネルインターフェイス（DVTI）を使用したブランチからハブへの通信の簡素化

この章では、ハブアンドスポークトポロジでの DVTI の実践的な応用について詳しく説明します。この使用例では、シナリオ、ネットワークトポロジ、ベストプラクティス、および前提条件について詳しく説明します。また、シームレスな導入のための包括的なエンドツーエンドの手順も提供します。

ハブアンドスポークトポロジでのルートベースの VPN

Cisco Secure Firewall Management Center は、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サポートしています。このインターフェイスを使用して、スタティック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。VTI を使用すると、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングする必要がなくなります。すべてのリモート サブネットを追跡し、暗号マップのアクセス リストに含める必要がなくなります。

VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。VTI ではスタティックまたはダイナミックルートが使用されます。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、ルーティングテーブルに従って転送します。

Management Center は、VTI またはルートベースの VPN を設定するためのデフォルトのサイト間 VPN ウィザードをサポートしています。

ハブアンドスポークトポロジでルートベースの VPN を導入する場合、ダイナミック仮想トンネルインターフェイス（DVTI）はハブで設定され、スタティック仮想トンネルインターフェイス（SVTI）はスポークで設定されます。

ダイナミック VTI では、IPsecインターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPNセッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。

Cisco Secure Firewall Threat Defense は、ルートベース（VTI）VPN のバックアップトンネルの設定をサポートし、リンクの冗長性を提供します。プライマリ VTI（プライマリトンネル）がトラフィックをルーティングできない場合、VPN内のトラフィックはバックアップVTI（セカンダリトンネル）を介してトンネリングされます。

利点

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

1. **設定の簡素化**：VTIは、トンネル自体を表す論理インターフェイスを提供することで、VPN トンネルの設定を簡素化します。これにより、通常は従来の VPN 設定に伴う複雑なクリプトマップまたはアクセスリストの設定が不要になります。
2. **管理の簡素化**：大企業のハブアンドスポーク展開のピア設定を簡単に管理できます。スポークで設定された複数のスタティック VTI に対して、ハブでは 1 つのダイナミック VTI のみが設定されます。
3. **拡張性**：VTI により、簡単に拡張することができます。新しいスポークを追加しても、ハブで追加の VPN 設定を行う必要はありません。設定によっては、NAT およびルーティングの設定の更新が必要になる場合があります。

4. **ダイナミックルーティングのサポート**：VTI は、Open Shortest Path First（OSPF）などのダイナミック ルーティング プロトコルをサポートしているため、VPN エンドポイント間でルーティング情報をダイナミックに交換できます。これにより、リアルタイムのネットワーク状態に基づいた効率的なルーティングの決定が可能になります。
5. **デュアル ISP の冗長性**：SVTI はバックアップ VTI トンネルをサポートしています。
6. **ロードバランシング**：SVTI は ECMP を使用した VPN トラフィックのロードバランシングをサポートしています。

この使用例の対象者

このDVTIハブアンドスポーク設定の対象者には、組織のネットワーク インフラストラクチャの設計と管理を担当するネットワークアーキテクト、IT管理者、およびネットワーク技術者が含まれます。この使用例は、リモートスポークサイトに接続するセキュアなトンネルを備えた集中型ハブを導入することで、ネットワーク接続の最適化、データセキュリティの確保、およびネットワーク管理の合理化を求めるユーザーのために役立ちます。

シナリオ

複数の都市に複数の分散拠点を持つ中規模企業が、これらのブランチを中央の本社と接続するためのセキュアで効率的なネットワーク インフラストラクチャを確立したいと考えています。会社の IT 管理者である Alice が、ネットワークの設定と管理を担当しています。

リスクがあるもの

現在のネットワーク設定では、各分散拠点と中央の本社の間にある複数のポイントツーポイント接続を手動で設定する必要があります。このアプローチは時間がかかり、エラーが発生しやすく、すべての場所でネットワーク設定の一貫性を維持することが困難です。Alice は、設定プロセスを簡素化し、集中管理を提供するソリューションを必要としています。

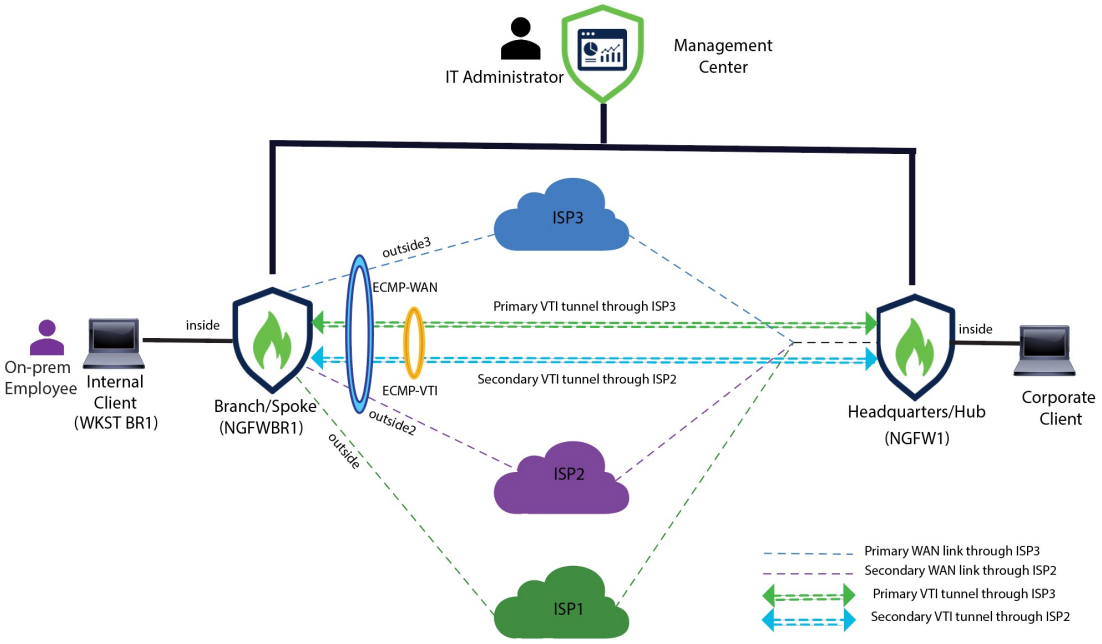
ブランチ（スポーク）と本社（ハブ）の間のルートベース VPN による問題の解決方法

1. 集中型設定：AliceはDVTIハブアンドスポークトポロジを導入し、ハブでの設定と管理を一元化します。これにより、すべての場所でのネットワーク設定が簡素化されます。
2. ダイナミックルーティング：Alice はルーティング情報の交換を自動化するダイナミック ルーティング プロトコル（OSPF など）を設定します。スタティックルートの手動設定が不要になり、ネットワーク管理が簡素化されます。
3. 迅速なプロビジョニング：DVTI により、Alice はスポークルータを設定し、ハブとのセキュアなトンネルを確立することで、新しい分散拠点を迅速にプロビジョニングできます。これにより、プロビジョニングプロセスが簡素化され、ネットワークの拡張性がサポートされます。

DVTIを導入することで、Aliceはネットワーク設定を簡素化し、管理を一元化し、一貫性を確保し、企業のネットワークでの効率的なプロビジョニングと拡張性を実現します。

ネットワーク トポロジ

このハブスポークトポロジでは、Threat Defense デバイスがブランチロケーションに展開されます。次の図では、内部クライアントまたはブランチワークステーションには WKST BR というラベルが付けられ、ブランチ（スポーク）の Threat Defense には NGFWBR1 というラベルが付けられています。本社（ハブ）は NGFW1 としてラベル付けされ、企業のネットワークに接続されています。VPN トンネルは NGFWBR1 と NGFW1 の間に設定されます。リンクの冗長性と VPN トラフィックのロードバランシングのために、ブランチノードのプライマリおよびセカンダリのスタティック VTI インターフェイスで ECMP ゾーンが設定されます。



ベストプラクティス

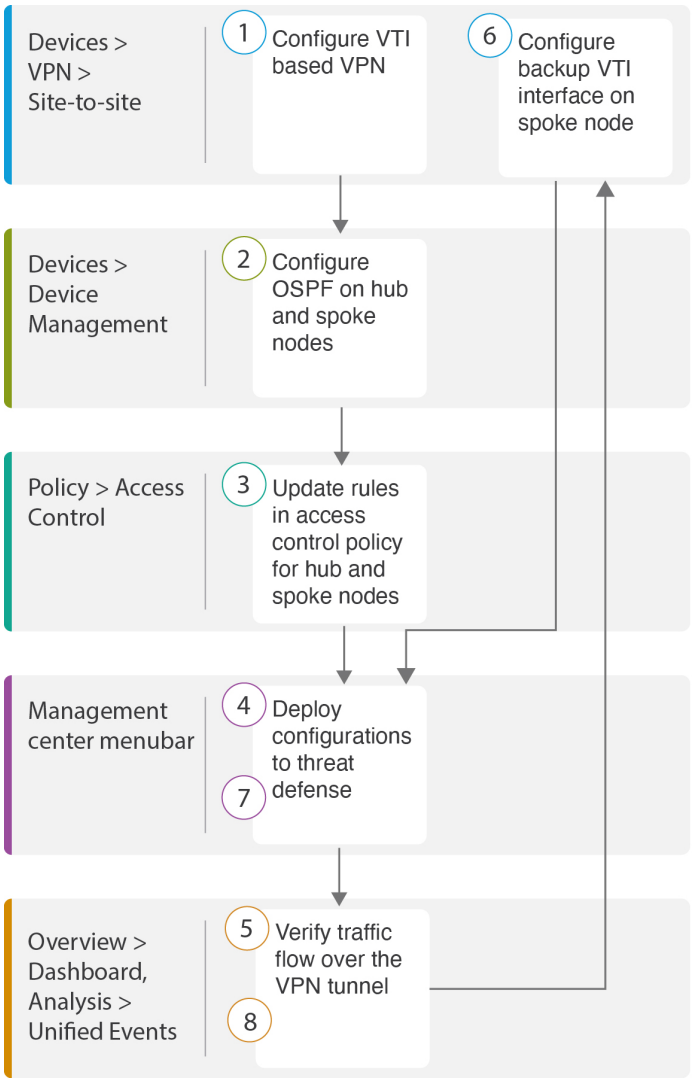
- Cisco Secure Firewall Threat Defense がバージョン 6.7 以降で実行されていることを確認します。
- VTI はルーテッドモードのみでサポートされています。
- ループバック インターフェイスから動的インターフェイスの借用 IP を設定します。
- VTI 経由のトラフィックを制御するために、VTI インターフェイスにアクセスルールを適用していることを確認します。
- VTI トラフィックをロードバランシングするために、SVTI の ECMP ゾーンを設定します。

前提条件

- Device Manager を使用した Threat Defense の初期設定の完了
- デバイスへのライセンスの割り当て
- インターネットアクセスのルートの追加。「スタティックルートの追加」を参照してください
- 脅威に対する防御のための NAT の設定
- 基本的なアクセス コントロール ポリシーの作成

ルートベース VPN（ハブアンドスポークトポロジ）を設定するためのエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center でハブスポークトポロジのルートベース VPN を設定するためのワークフローを示しています。



ステップ	説明
1	VTI ベースの VPN を設定します。参照先 • ルートベースのサイト間 VPN の作成 （7 ページ） • ハブノードのエンドポイントの設定 （8 ページ） • スポークノードのエンドポイントの設定 （10 ページ）
2	ハブノードとスポークノードで OSPF を設定します。参照先 • ハブノードでの OSPF の設定 （12 ページ） • スポークノードでの OSPF の設定 （14 ページ）

ステップ	説明
3	ハブノードとスポークノードのアクセス コントロール ポリシーのルールを更新します。アクセス コントロール ポリシーの設定 （16 ページ）を参照してください。
4	設定を Threat Defense に展開します。設定の展開 （19 ページ）を参照してください。
5	VPN トンネルを介したトラフィックフローを確認します。VPN トンネルを介したトラフィックフローの確認 （19 ページ）を参照してください。
6	スポークノードでバックアップ VTI を設定します。スポークノードでのバックアップ VTI インターフェイスの設定 （23 ページ）を参照してください。
7	設定を Threat Defense に展開します。設定の展開 （19 ページ）を参照してください。
8	セカンダリトンネルを介したトラフィックフローを確認します。プライマリトンネルとセカンダリトンネルの確認 （26 ページ） を参照してください。

ルートベースのサイト間 VPN の作成

2 つのノード間にルートベースのサイト間 VPN を設定できます。VTI ベースの VPN を設定するには、トンネルの両方のノードに仮想トンネルインターフェイスが必要です。

管理対象スポークの場合、プライマリ VTIインターフェイスとともにバックアップのスタティック VTI インターフェイスを設定できます。

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

ステップ 2 [トポロジ名（Topology Name）] フィールドに名前として **Corporate-VPN** と入力します。

ステップ 3 トポロジタイプとして [ルートベース（VTI）（Route Based (VTI)）] を選択します。

ステップ 4 ハブノードのエンドポイントを設定します。ハブノードのエンドポイントの設定 （8 ページ）を参照してください。

ステップ 5 スポークノードのエンドポイントを設定します。スポークノードのエンドポイントの設定 （10 ページ）を参照してください。

ステップ 6 [IKE]、[IPsec]、および [詳細設定（Advanced）] タブでは、デフォルト設定が使用されます。

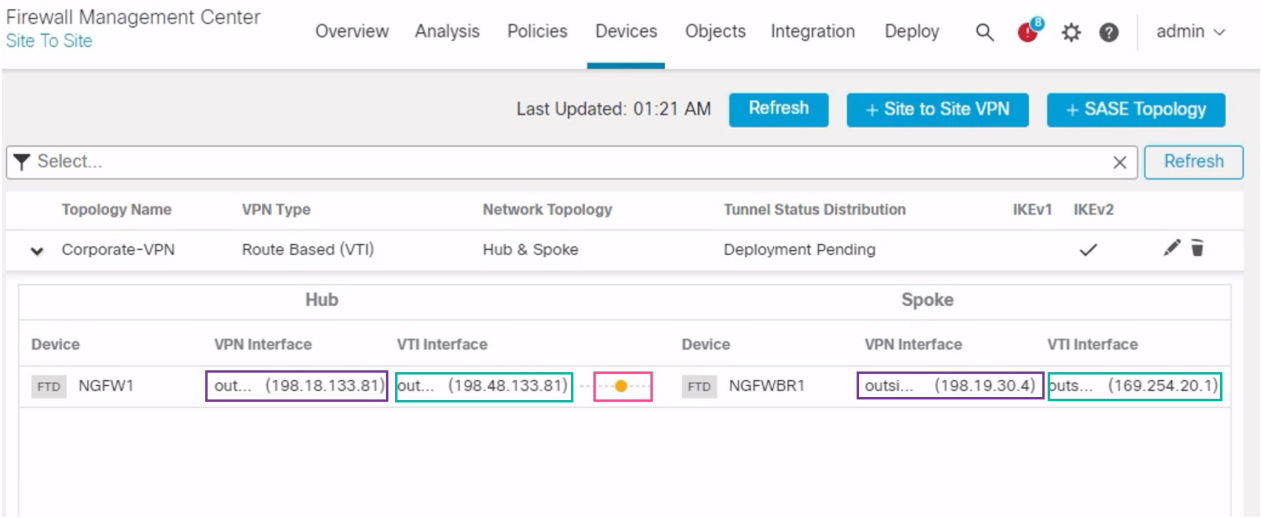
ステップ 7 [保存（Save）] をクリックします。

Corporate-VPN トポロジが正常に作成されます。

ステップ 8 [デバイス（Devices）]>[サイト間VPN（Site-to-site VPN）]に移動すると、[サイト間VPN（Site-to-site VPN）]の一覧ページで VPN トポロジを表示できます。

（注） 作成した VPN トポロジが表示されない場合は、[更新（Refresh）] をクリックします。

ステップ 9 [Corporate-VPN] ノードを展開して、トポロジ内のすべてのトンネルを表示します。**NGFW1** ハブと **NGFWBR1** スポークが、物理ソースと VTI インターフェイスの詳細とともに表示されます。設定がまだ展開されていないため、[導入保留中（Deployment Pending）]と表示され、トンネルのステータスがオレンジで表示されます。



次のタスク

両方のデバイスで VTI インターフェイスと VTI トンネルを設定したら、次のものを設定する必要があります。

- VTI トンネルを介してデバイス間で VTI トラフィックをルーティングするルーティングプロトコル。ハブノードでの OSPF の設定 （12 ページ）およびスポークノードでの OSPF の設定 （14 ページ）を参照してください。
- 暗号化されたトラフィックを許可するアクセスコントロールルール。アクセスコントロール ポリシーの設定 （16 ページ） を参照してください。

ハブノードのエンドポイントの設定

トンネルタイプを「ダイナミック」として指定し、関連パラメータを設定すると、Management Center はダイナミック仮想テンプレートを生成します。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。

ステップ 1 [ハブノード（Hub Nodes）] セクションで、[+] 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が表示されます。

ステップ 2 [デバイス（Device）] ドロップダウンリストからハブとして [NGFW1] を選択します。

（注） ソフトウェアバージョン 7.3 以降で実行されているデバイスである必要があります。

ステップ 3 [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 [+] をクリックして新しいダイナミック VTI を追加します。

[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が表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] には [ダイナミック（Dynamic）] が自動的に入力されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ dynamic_vti +<*tunnel ID*> として自動入力されます。たとえば、**outside_dynamic_vti_1** となります。
- [有効（Enabled）] チェックボックスはデフォルトでオンになります。
- [セキュリティゾーン（Security Zone）]：このインターフェイスのセキュリティゾーンを定義するには、ドロップダウンリストから [新規…（New…）] を選択します。[新規セキュリティゾーン（New Security Zone）] ダイアログボックスで名前として **Tunnel_Zone** と入力し、[OK] をクリックします。このトンネルインターフェイスのセキュリティゾーンとして [Tunnel_Zone] を選択します。
- [テンプレートID（Template ID）] には、DVTI インターフェイスの一意の ID が自動入力されます。
- [トンネルの送信元（Tunnel Source）] は、DVTI の送信元である物理インターフェイスであり、デフォルトで自動入力されます。この使用例では、DVTI の明示的なトンネルの送信元を設定しません。ドロップダウンリストから [インターフェイスの選択（Select Interface）] を選択して、選択をクリアします。
- [IPsecトンネルモード（IPsec Tunnel Mode）] は、デフォルトでは IPv4 に設定されます。
- DVTI はテンプレート インターフェイスであるため、[IPアドレス（IP address）] をスタティック IP アドレスにすることはできません。ループバック インターフェイスから動的インターフェイスの借用 IP を設定することをお勧めします。ループバック インターフェイスを追加するには、[IPの借用（IPアンナンバード）（Borrow IP (IP unnumbered)）] ドロップダウンリストの横にある [+] をクリックします。[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、次の手順を実行します。

  1. [全般（General）] タブで、[名前（Name）] を **HUB_Tunnel_IP**、[ループバックID（Loopback ID）] を **1** として入力します。
  2. [IPv4] タブで、IP アドレスを **198.48.133.81/32** として入力します。
  3. [OK] をクリックして、ループバック インターフェイスを保存します。

  [IPの借用（Borrow IP）] は [ループバック1（HUB_Tunnel_IP）（Loopback 1(HUB_Tunnel_IP)）] に設定されます。

[OK] をクリックして、DVTI を保存します。VTI が正常に作成されたことを確認するメッセージが表示されます。[OK] をクリック

[ダイナミック仮想トンネルインターフェイス（Dynamic Virtual Tunnel Interface）] は [outside_dynamic_vti_1（198.48.133.81）（outside_dynamic_vti_1(198.48.133.81)）] に設定されます。

ステップ 4 [トンネルの送信元（Tunnel Source）] ドロップダウンリストから [GigabitEthernet 0/0（outside）（GigabitEthernet 0/0 (outside)）] を選択します。外部インターフェイスの IP アドレス（**198.18.133.81**）が次のフィールドに自動入力されます。

ステップ 5 [詳細設定（Advanced Settings）] を展開して、デフォルト設定を表示します。

ステップ 6 [OK] をクリック

NGFW1 がハブノードとして正常に設定されました。

スポークノードのエンドポイントの設定

ステップ 1 [スポークノード（Spoke Nodes）] セクションで、[+] 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が表示されます。

ステップ 2 [デバイス（Device）] ドロップダウンリストからハブとして [NGFWBR1] を選択します。

（注） ソフトウェアバージョン 7.3 以降で実行されているデバイスである必要があります。

ステップ 3 [スタティック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 [+] をクリックして新しいスタティック VTI を追加します。

[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が表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] には [スタティック（Static）] が自動的に入力されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*> として自動入力されます。たとえば、**outside_static_vti_1** となります。
- [有効（Enabled）] チェックボックスはデフォルトでオンになります。
- [セキュリティゾーン（Security Zone）] ドロップダウンリストから [Tunnel_Zone] を選択します。
- [トンネルID（Tunnel ID）] には、1 の値が自動入力されます。
- [トンネルの送信元（Tunnel Source）] ドロップダウンリストから [GigabitEthernet0/4（outside3）（GigabitEthernet0/4 (outside3)）] を選択します。その横にあるドロップダウンリストから、outside3 インターフェイスの IP アドレスとして [198.19.30.4] を選択します。
- [IPsecトンネルモード（IPsec Tunnel Mode）] は、デフォルトでは IPv4 に設定されます。

- [IPアドレス（IP address）] は、スタティック IP アドレスまたは借用 IP のいずれかです。ループバック インターフェイスから静的インターフェイスの借用 IP を設定することをお勧めします。ループバック インターフェイスを追加するには、[IPの借用（IPアンナンバード）（Borrow IP (IP unnumbered)）] ドロップダウンリストの横にある [+] をクリックします。[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、次の手順を実行します。

  1. [全般（General）] タブで、[名前（Name）] を **Spoke_Tunnel_IP**、[ループバックID（Loopback ID）] を **1** として入力します。
  2. [IPv4] タブで、IP アドレスを **169.254.20.1/32** として入力します。
  3. [OK] をクリックして、ループバック インターフェイスを保存します。

  [IPの借用（Borrow IP）] は [ループバック1（Spoke_Tunnel_IP）（Loopback 1(Spoke_Tunnel_IP)）] に設定されます。

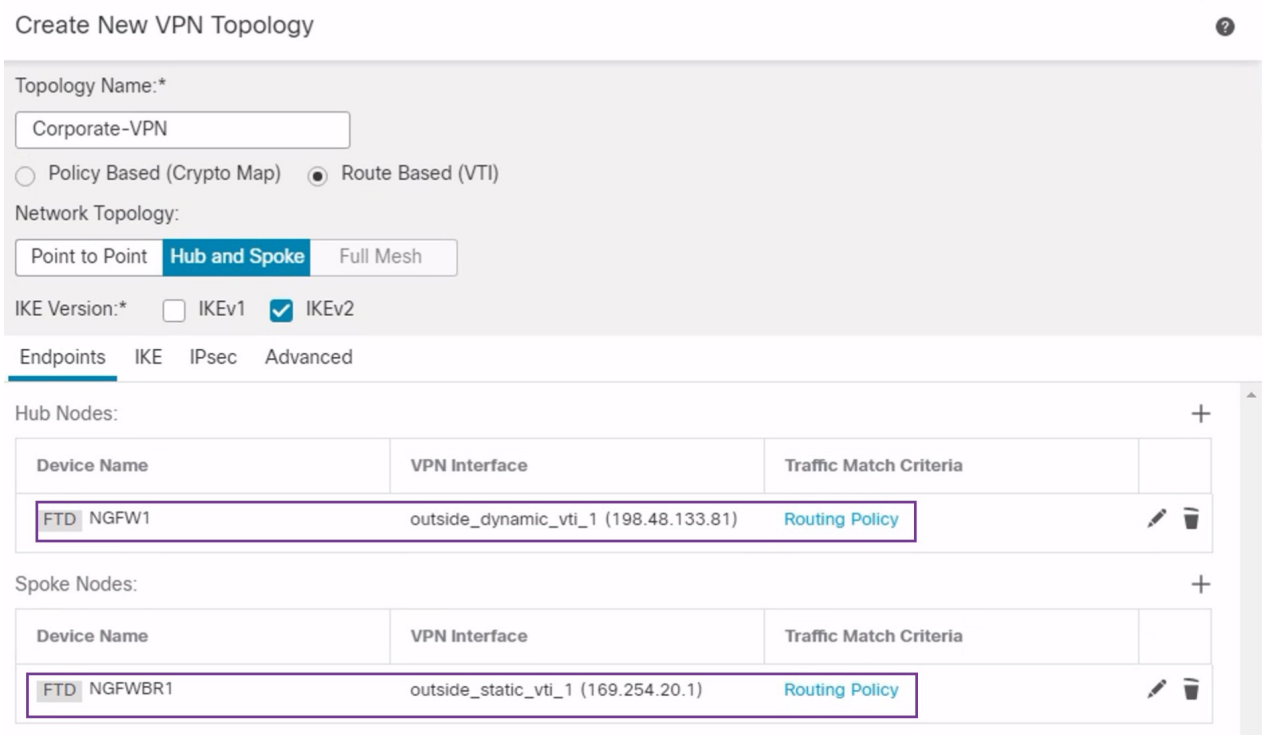
[OK] をクリックして、SVTI を保存します。VTI が正常に作成されたことを確認するメッセージが表示されます。[OK] をクリック

スタティック仮想トンネルインターフェイスが [outside_static_vti_1（169.254.20.1）（outside_static_vti_1(169.254.20.1)）] に設定されます。

ステップ 4 [詳細設定（Advanced Settings）] を展開して、デフォルト設定を表示します。両方のチェックボックスをオンにする必要があります。

ステップ 5 [OK] をクリック

NGFWBR1 がスポークノードとして正常に設定されました。



ハブノードでの OSPF の設定

OSPF は、VPN トンネルを介してトラフィックを送信できるように、ハブとスポークのデバイス間で設定されます。参考までに、スタティックルーティングはアンダーレイであり、その上にスポークからハブへのトンネルが確立され、OSPF はオーバーレイと見なされます。

ステップ 1 ハブノードを編集するには、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、NGFW1 ノードの [編集（Edit）]（✎） アイコンをクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブで、以前に作成された、DVTI インターフェイスの IP アドレスとして機能する **Loopback1** インターフェイスを確認します。

ステップ 3 [Routing] をクリックします。

ステップ 4 左側のパネルで [OSPF] をクリックします。

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。[Add Interface] ダイアログボックスが表示されます。次のフィールドを変更します。

- [インターフェイス（Interface）]：ドロップダウンリストから DVTI インターフェイスの [outside_dynamic_vti_1] を選択します。

- [ポイントツーポイント（Point-to-point）]：この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。

  残りのフィールドではデフォルト値を使用します。

- [OK] をクリック

[インターフェイス（Interface）] タブに **outside_dynamic_vti_1** の行が追加されます。

ステップ 8 [エリア（Area）] タブをクリックします。

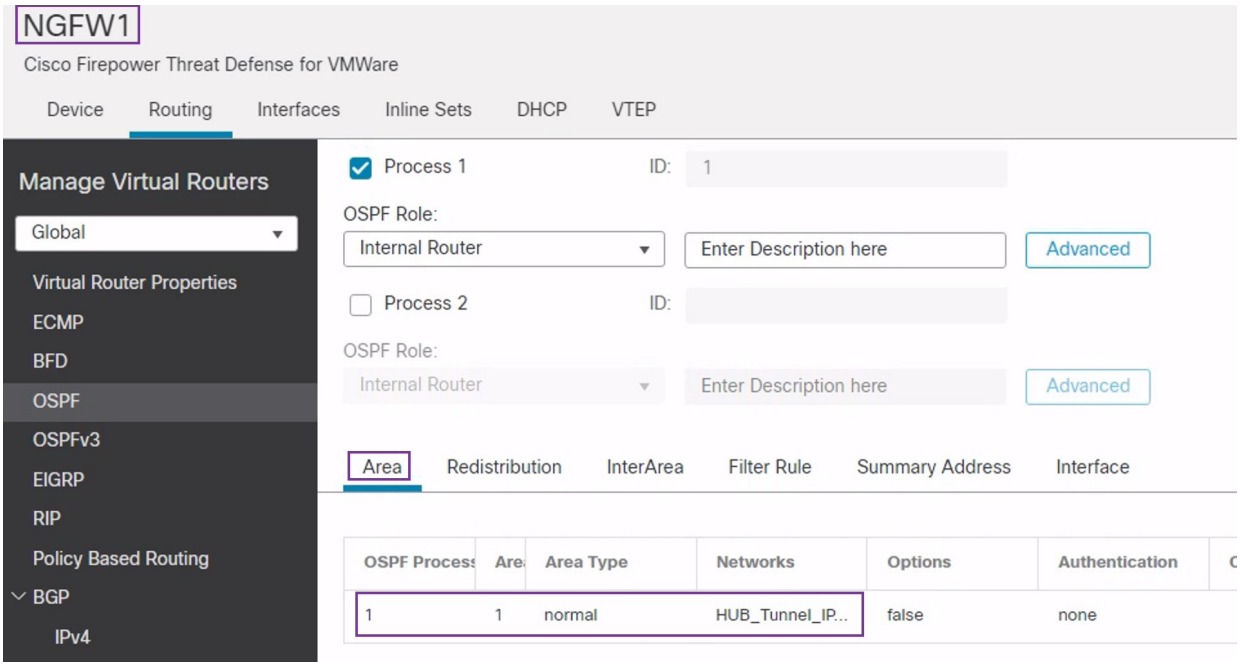
ステップ 9 [追加（Add）] をクリックします。[エリアの追加（Add Area）] ダイアログボックスが表示されます。次のフィールドを変更します。

- [OSPFプロセス（OSPF Process）]：プロセス ID として 1 を選択します。
- [エリアID（Area ID）]：値が 1 であることを確認します。

  残りのフィールドではデフォルト値を使用します。

- [使用可能なネットワーク（Available Network）]：トンネルを介してアドバタイズされるネットワークを追加するために、次の手順を実行します。
  - 新しいネットワークオブジェクトを追加するには、＋をクリックします。次の詳細を入力します。
    - [名前（Name）]：名前として **HUB_Tunnel_IP** と入力します。
    - [ネットワーク（Network）]：[ホスト（Host）] オプションを選択し、ホスト IP として **198.48.133.81** と入力します。
    - [保存（Save）] をクリックします。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **HUB** と入力します。新しく追加されたネットワークオブジェクト（**HUB_Tunnel_IP**）が表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **Corporate** と入力します。**Corporate_LAN** ネットワークオブジェクトが表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
- [OK] をクリック

[エリア（Area）] タブに行が追加されます。



ステップ 10 [保存（Save）] をクリックして、ハブノードの OSPF 設定を保存します。

スポークノードでの OSPF の設定

ステップ 1 スポークノードを編集するには、[デバイス（Devices）]>[デバイス管理（Device Management）] を選択し、NGFWBR1 ノードの [編集（Edit）]（✎） アイコンをクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブで、次の手順を実行します。

- スポーク設定で以前に作成された **Tunnel1** インターフェイスの詳細を確認します。
- 以前に作成された、Tunnel1 の IP アドレスとして機能する **Loopback1** インターフェイスの詳細を確認します。

ステップ 3 [Routing] をクリックします。

ステップ 4 左側のパネルで [OSPF] をクリックします。

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 [エリア（Area）] タブをクリックします。

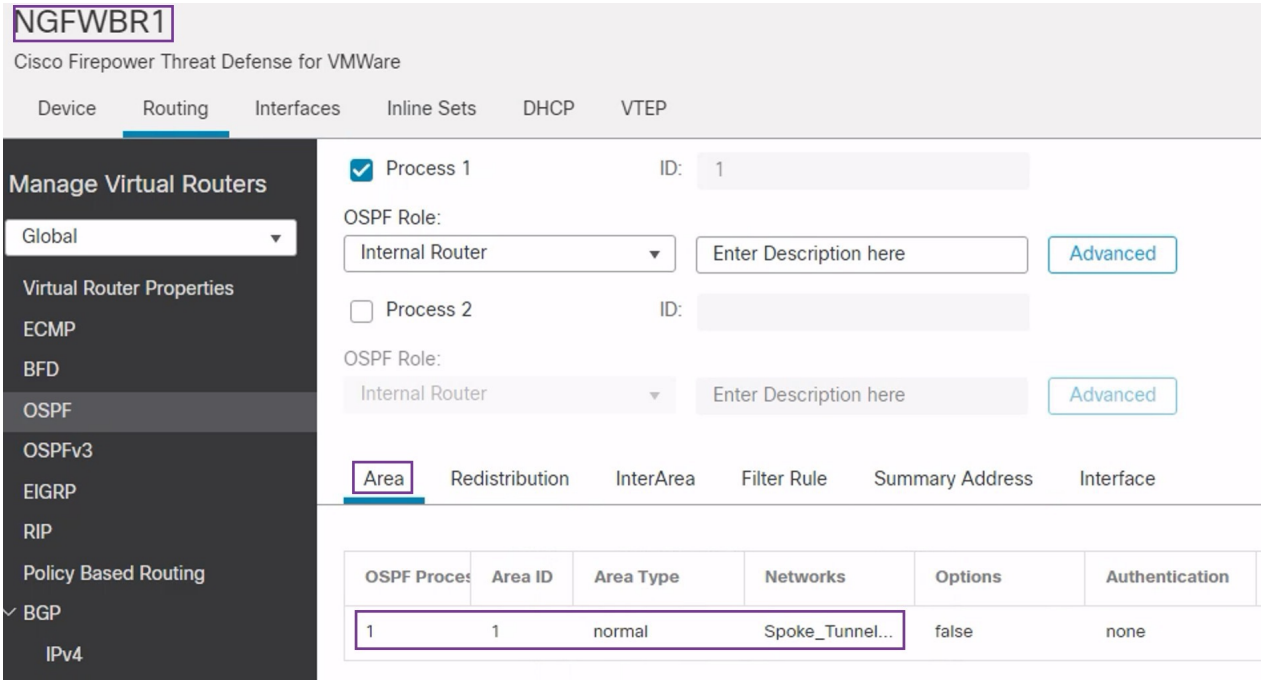
ステップ 7 [追加（Add）] をクリックします。[エリアの追加（Add Area）] ダイアログボックスが表示されます。次のフィールドを変更します。

- [OSPFプロセス（OSPF Process）]：プロセス ID として 1 を選択します。
- [エリアID（Area ID）]：値が 1 であることを確認します。

残りのフィールドではデフォルト値を使用します。

- [使用可能なネットワーク（Available Network）]：トンネルを介してアドバタイズされるネットワークを追加するために、次の手順を実行します。
  - 新しいネットワークオブジェクトを追加するには、＋をクリックします。次の詳細を入力します。
    - [名前（Name）]：名前として **Spoke_Tunnel_IP** と入力します。
    - [ネットワーク（Network）]：[ホスト（Host）] オプションを選択し、ホスト IP として **169.254.20.1** と入力します。
    - [保存（Save）] をクリックします。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **Spoke** と入力します。新しく追加されたネットワークオブジェクト（**Spoke_Tunnel_IP**）が表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **Branch** と入力します。**Branch_LAN** ネットワークオブジェクトが表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
- [OK] をクリック

[エリア（Area）] タブに行が追加されます。



ステップ 8 [保存（Save）] をクリックして、スポークノードの OSPF 設定を保存します。

アクセス コントロール ポリシーの設定

続行する前に、**NGFW1** ノードと **NGFWBR1** ノードの VTI インターフェイスが、**Tunnel_Zone** というラベルの付いた新しいゾーンに関連付けられていることを確認します。

[ポリシー（Policies）]>[アクセス制御（Access Control）] に移動して、アクセス コントロール ポリシーを確認します。トンネルとの間の VPN トラフィックを許可するには、ハブとスポークの両方で次のアクセス コントロール ポリシーを更新する必要があります。

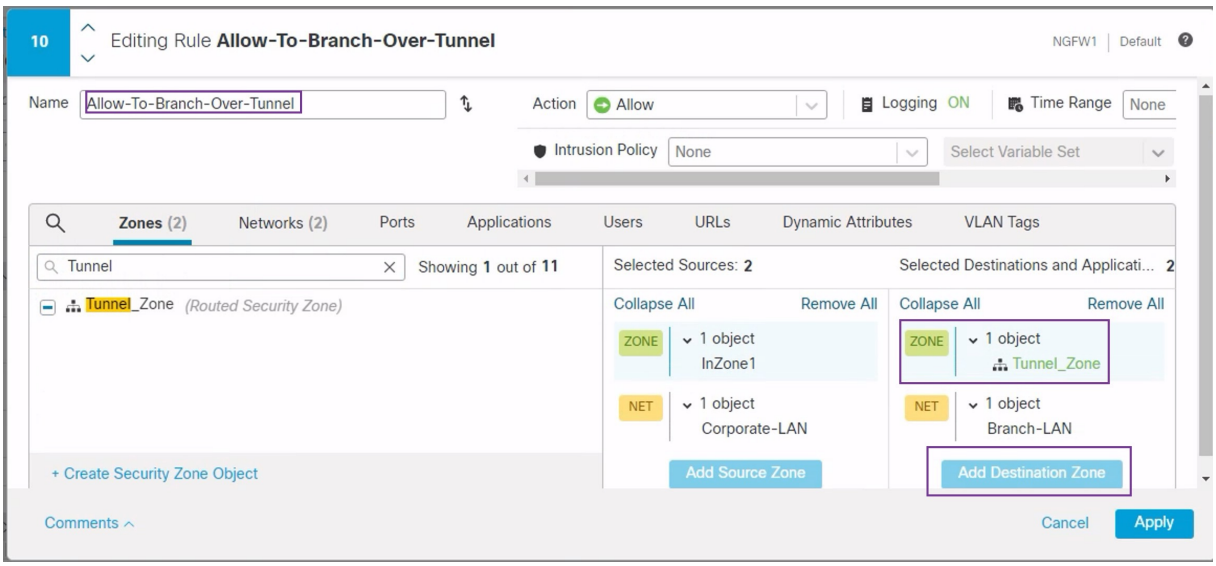
- **NGFW1**：ハブノード（NGFW1）のアクセス コントロール ポリシー
- **ブランチのアクセスコントロール**：スポークノード（NGFWBR1）のアクセス コントロール ポリシー

ステップ 1 ハブノード（NGFW1）の AC ポリシーを編集するには、[編集（Edit）]（✎）アイコンをクリックします。

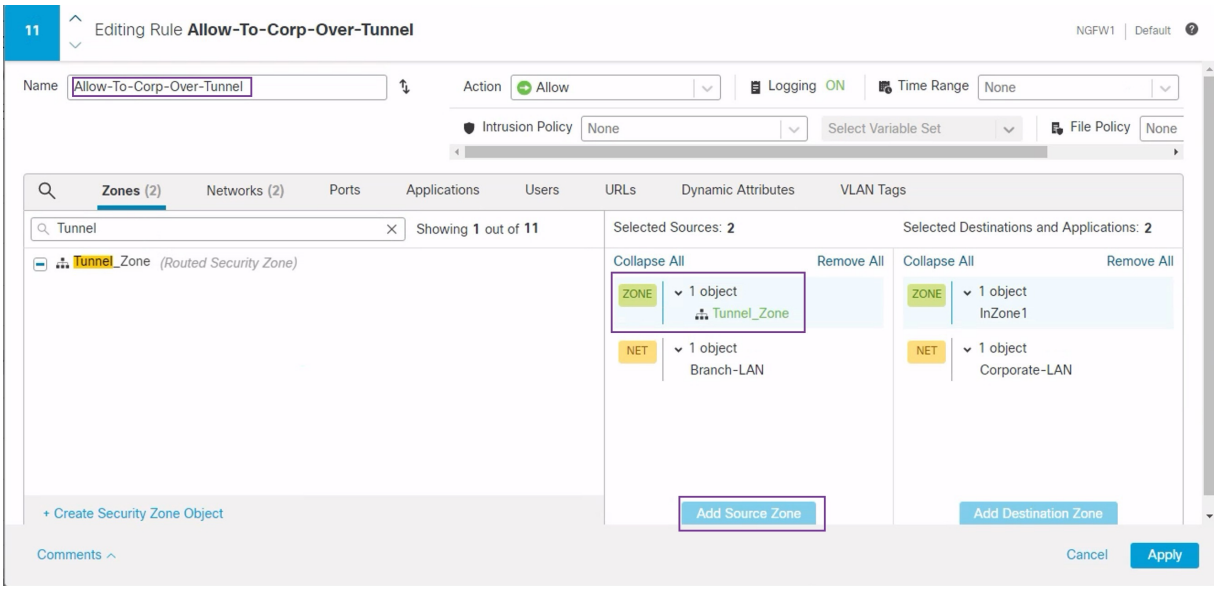
この使用例で変更する必要がある既存のルールは次のとおりです。

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. **Allow-To-Branch-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
2. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[宛先ゾーンを追加（Add Destination Zone）] をクリックします。



3. [適用（Apply）] をクリックして、ルールを保存します。
4. **Allow-To-Corp-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
5. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[送信元ゾーンを追加（Add Source Zone）] をクリックします。



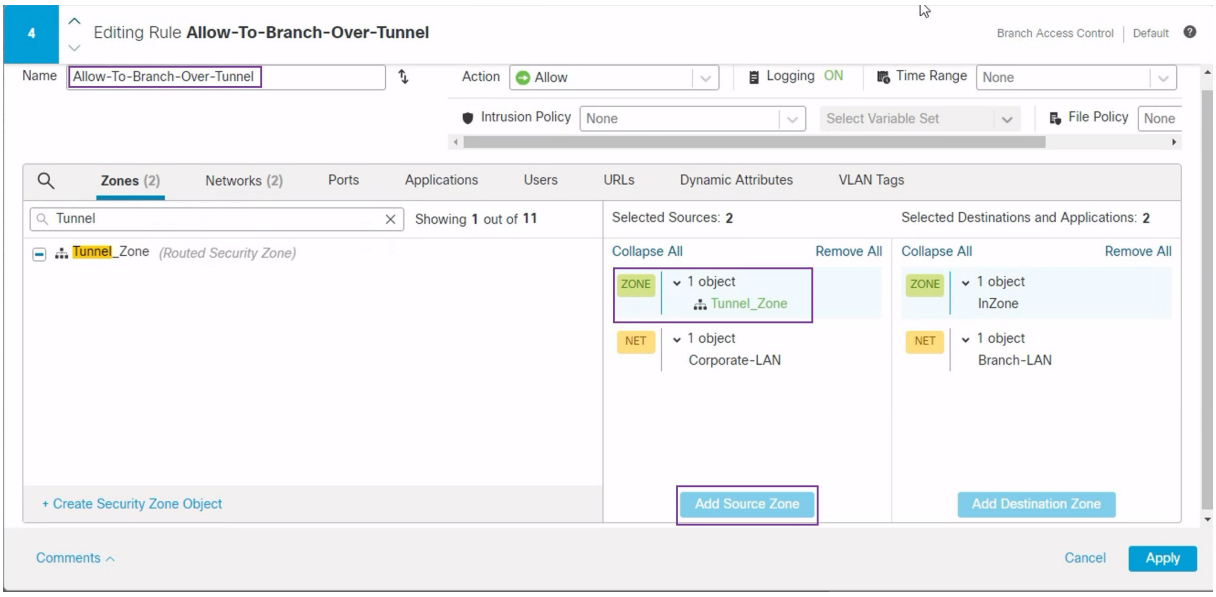
6. [適用（Apply）] をクリックして、ルールを保存します。
7. NGFW1 で更新されたルールを確認します。
8. [保存（Save）] をクリックして、AC ポリシーを保存します。
9. [アクセスコントロールポリシー管理に戻る（Return to Access Control Policy Management）] をクリックして、ポリシーページに戻ります。

ステップ 2 スポークノード（NGFWBR1）の AC ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。

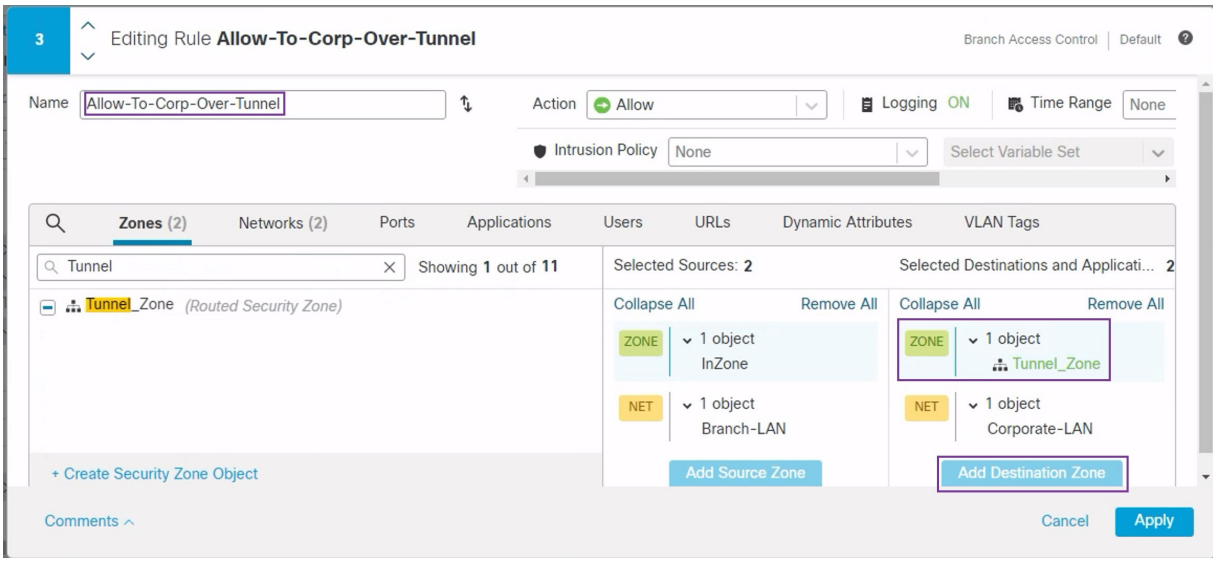
この例で編集する必要があるルールは次のとおりです。

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. **Allow-To-Branch-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
2. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[送信元ゾーンを追加（Add Source Zone）] をクリックします。



3. [適用（Apply）] をクリックして、ルールを保存します。
4. **Allow-To-Corp-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
5. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[宛先ゾーンを追加（Add Destination Zone）] をクリックします。



6. [適用（Apply）] をクリックして、ルールを保存します。
7. NGFWBR1 で更新されたルールを確認します。

8. [保存（Save）] をクリックして、AC ポリシーを保存します。

設定の展開

すべての設定が完了したら、管理対象デバイスに設定を展開します。

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックします。展開準備が完了しているデバイスのリストが表示されます。

ステップ 2 設定の変更を展開する NGFWBR1 と NGFW1 の横にあるチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。[展開（Deploy）] ダイアログボックスで展開が [完了（Completed）] とマークされるまで待ちます。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] リンクをクリックします。

次の選択肢があります。

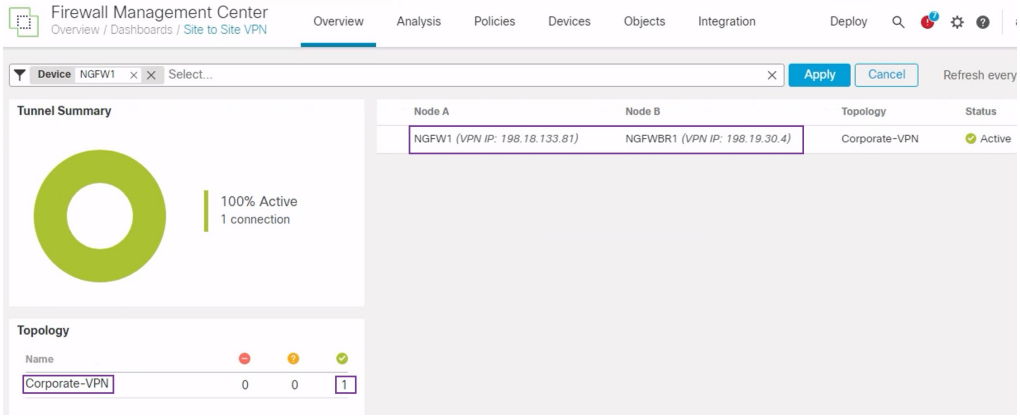
- [展開の続行（Proceed with Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

VPN トンネルを介したトラフィックフローの確認

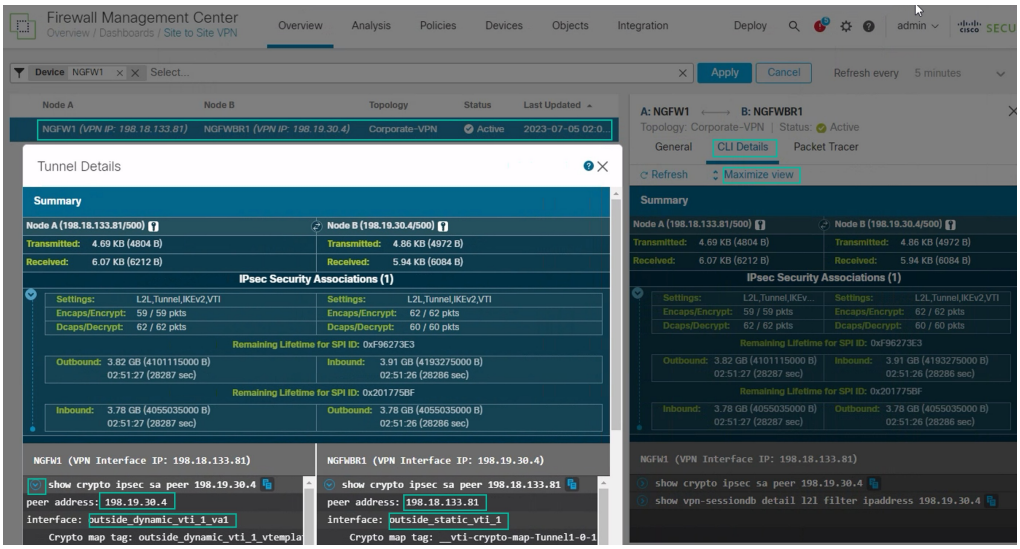
VPN トンネルに対して次の確認を行います。

- **[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 トンネルが稼働していて緑であることを確認するために、[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site-to-site VPN）] を選択します。



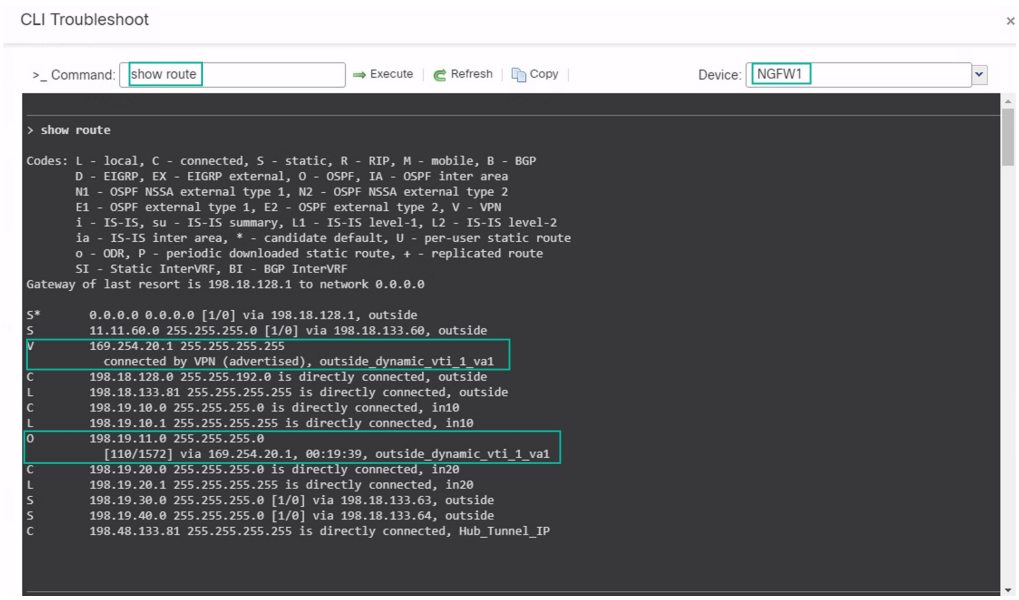
2. NGFW1 にカーソルを合わせます。[すべての情報を表示（View Full Information）] アイコンが NGFW1 の横に表示されます。
3. [すべての情報を表示（View Full Information）] アイコンをクリックします。トンネルの詳細と追加のアクションを含むサイドペインが表示されます。
4. サイドペインの [CLIの詳細（CLI Details）] タブをクリックします。
5. [ビューの最大化（Maximize View）] をクリックして、IPSec セキュリティ アソシエーションの詳細を含む、最大化されたダイアログボックスを表示します。
6. ダイアログボックスの下部にある show コマンドの CLI を展開すると、デバイスの VTI インターフェイスを表示できます。



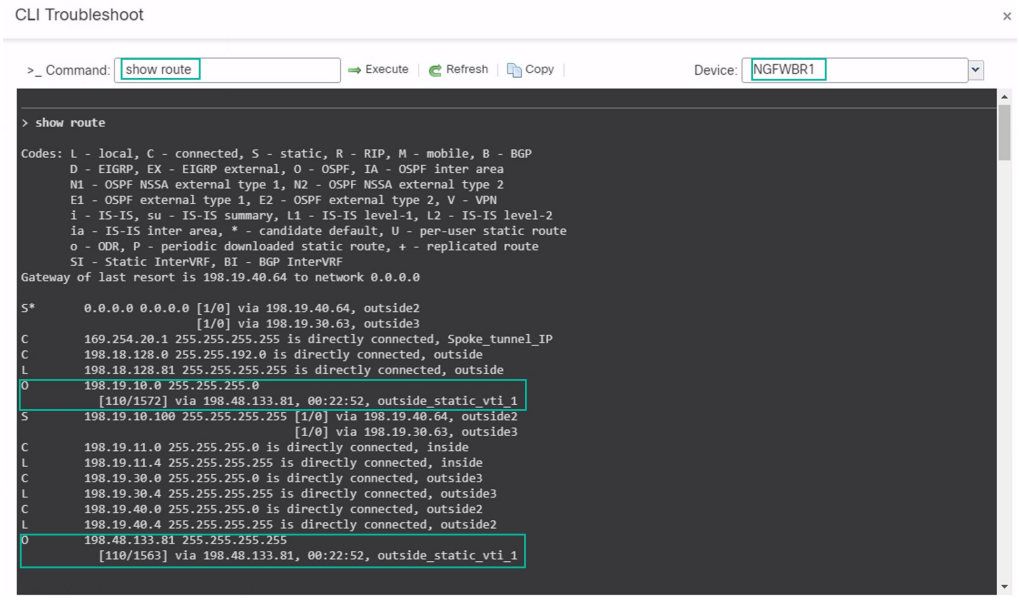
7. [閉じる（Close）] をクリックして [トンネルの詳細（Tunnel Details）] ウィンドウを終了します。

- **ハブノードとブランチノードでのルーティングの確認**：OSPF ルートが **NGFW1** および **NGFWBR1** ノードで正しく学習されていることを確認するために、次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. NGFW1 を編集するために、[編集（Edit）]（✎） 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] ボタンをクリックします。[CLIのトラブルシュート（CLI Troubleshoot）] ウィンドウが表示されます
5. [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。
6. NGFW1 ノードでルートを確認し、次の図に示すように、スポークの VTI IP（169.254.20.1）の VPN ルートと Branch_LAN（198.19.11.0/24）の OSPF 学習ルートを確認します。

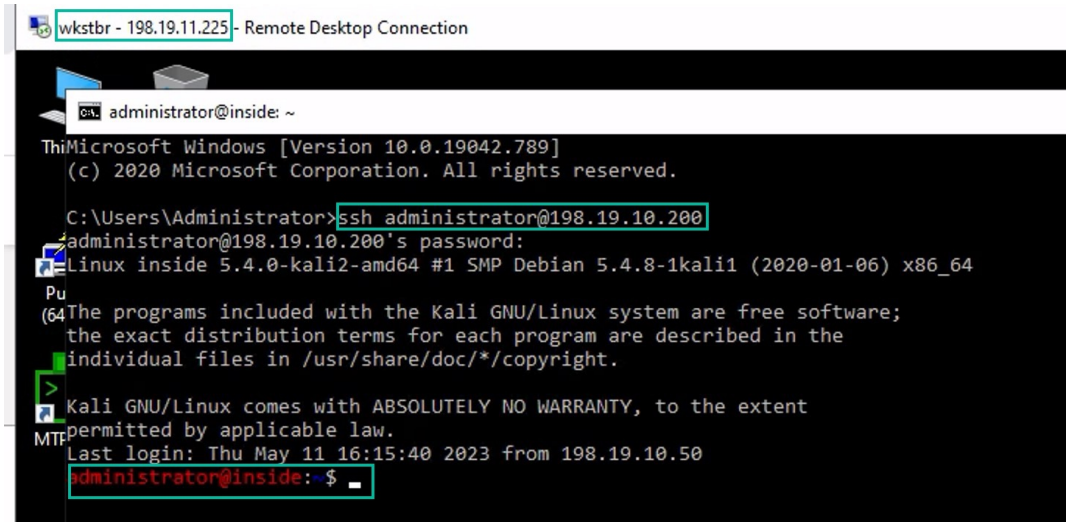


7. NGFWBR1 ノードに対してステップ 2 ～ 5 を繰り返します。
8. NGFWBR1 ノードでルートを確認します。次の図に示すように、ハブの VTI IP（198.48.133.81）および Corporate_LAN（198.19.10.0/24）の学習された OSPF ルートを確認します。



- スポークノードとハブノードの背後にある保護されたネットワーク間のトラフィックの確認

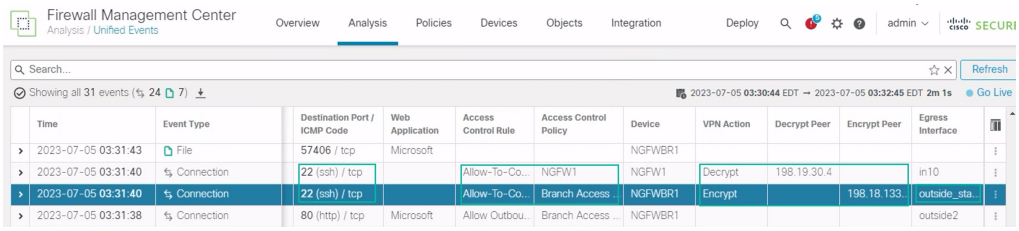
  WKST BR ワークステーション（198.19.11.225）にログインし、NGFW1 の背後にあるホスト（198.19.10.200）に SSH 接続します。ホストに正常に SSH 接続できることを確認します。



- 統合イベントを使用したブランチノードとスポークノードの間の接続の確認

  1. [分析（Analysis）] > [統合イベント（Unified Events）] を選択します。
  2. 列ピッカーを使用して、[VPNアクション（VPN Action）]、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、および [出力インターフェイス（Egress Interface）] の列を追加します。

3. 次の図に示すように、新しい列と、[宛先ポート/ICMPコード（Destination Port/ICMP Code）]、[アクセスコントロールルール（Access Control Rule）]、[アクセスコントロールポリシー（Access Control Policy）]、および[デバイス（Device）]の列を並べ替えてサイズ変更します。



4. **WKST BR** から**企業ホスト**への SSH 接続に関連するイベントを表示するには、[宛先ポート/ICMPコード（Destination Port/ICMP Code）]列で[22（ssh/tcp）（22 (ssh/tcp)）]の行を選択します。上の図に示すように、**outside_static_vti_1** インターフェイスを介した **NGFWBR1** での [暗号化（Encrypt）] アクションの後に、**NGFW1** での [復号（Decrypt）] アクションが続くことに注意してください。

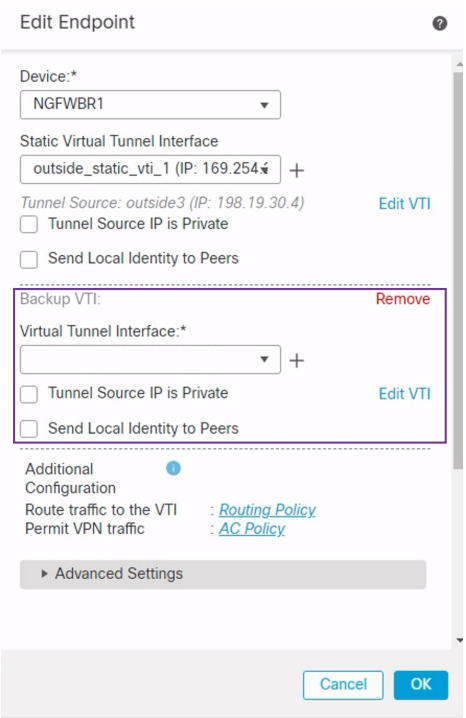
スポークノードでのバックアップ VTI インターフェイスの設定

Cisco Secure Firewall Threat Defense は、ルートベース（VTI）VPN のバックアップトンネルの設定をサポートします。プライマリ VTI がトラフィックをルーティングできない場合、VPN 内のトラフィックはバックアップ VTI を介してトンネリングされます。

ステップ 1 [デバイス（Devices）] > [サイト間VPN（Site-to-site VPN）] を選択し、設定された企業 VPN の VPN トポロジを表示し、[編集（Edit）]（✎）アイコンをクリックします。[VPNトポロジの編集（Edit VPN Topology）] ウィンドウが表示されます。

ステップ 2 [スポークノード（Spoke Nodes）] セクションで、**NGFWBR1** ノードの [編集（Edit）]（✎）アイコンをクリックします。[エンドポイントの編集（Edit Endpoint）] ダイアログボックスが表示されます。

ステップ 3 [バックアップVTIの追加（Add Backup VTI）] リンクをクリックして、セカンダリ VTI トンネルを追加します。このリンクをクリックすると、[バックアップVTI（Backup VTI）] セクションが表示されます。



ステップ 4 [仮想トンネルインターフェイス（Virtual Tunnel Interface）] ドロップダウンリストの横にある [+] をクリックして新しい VTI を追加します。

[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が表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] には [スタティック（Static）] が自動的に入力されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*> として自動入力されます。たとえば、**outside_static_vti_2** となります。
- [有効（Enabled）] チェックボックスはデフォルトでオンになります。
- [セキュリティゾーン（Security Zone）] ドロップダウンリストから [Tunnel_Zone] を選択します。
- [トンネルID（Tunnel ID）] には、2 の値が自動入力されます。
- [トンネルの送信元（Tunnel Source）] ドロップダウンリストから [GigabitEthernet0/3（outside2）（GigabitEthernet0/3 (outside2)）] を選択します。その横にあるドロップダウンリストから、outside3 インターフェイスの IP アドレスとして [198.19.40.4] を選択します。
- [IPsecトンネルモード（IPsec Tunnel Mode）] は、デフォルトでは IPv4 に設定されます。
- [IPアドレス（IP address）] は、スタティック IP アドレスまたは借用 IP のいずれかです。ループバック インターフェイスから静的インターフェイスの借用 IP を設定することをお勧めします。ループバック インターフェイスを追加するには、ドロップダウンリストから [ループバック1（Spoke_Tunnel_IP）（Loopback 1(Spoke_Tunnel_IP)）] を選択します。

[OK] をクリックして、VTI を保存します。VTI が正常に作成されたことを確認するメッセージが表示されます。[OK] をクリック

バックアップ VTI インターフェイスが [outside_static_vti_2（169.254.20.1）（outside_static_vti_2(169.254.20.1)）] に設定されます。

ステップ 5 [OK] をクリックして、スポーク設定を保存します。

ステップ 6 [保存（Save）] をクリックして、VPN トポロジを保存します。

プライマリおよびセカンダリ VTI インターフェイスの ECMP ゾーンの設定

リンクの冗長性と VPN トラフィックのロードバランシングのために、ブランチノードのプライマリおよびセカンダリのスタティック VTI インターフェイスで ECMP ゾーンを設定します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

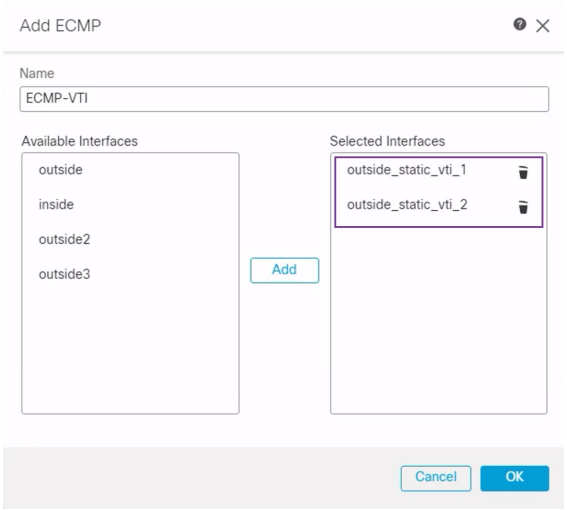
ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ECMP] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ECMPの追加（Add ECMP）] ボックスで、ECMP ゾーンの名前に **ECMP-VTI** と入力します。

ステップ 6 インターフェイスを関連付けるには、[使用可能なインターフェイス（Available Interfaces）] ボックスで [outside_static_vti_1] と [outside_static_vti_2] のインターフェイスを選択し、[追加（Add）] をクリックします。



ステップ 7 [OK] をクリック

[ECMP] ページに、新しく作成された ECMP ゾーンが表示されます。

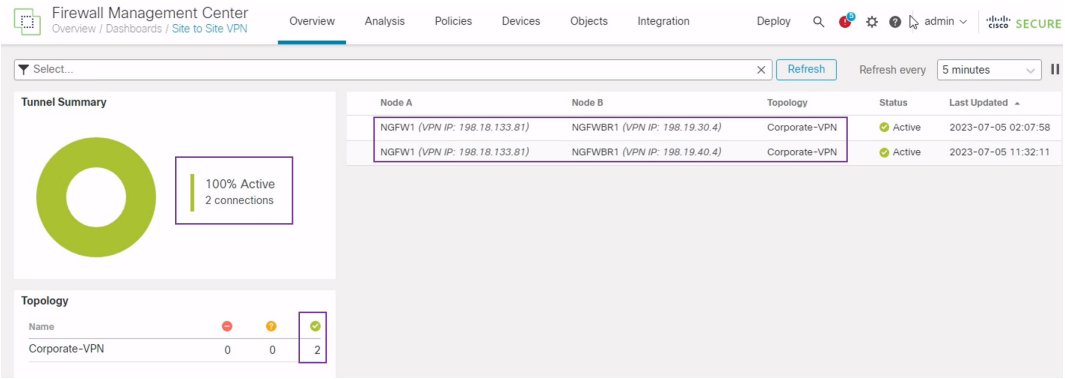
ステップ 8 [保存（Save）] をクリックします。

プライマリトンネルとセカンダリトンネルの確認

ブランチノードとハブノードの間のプライマリ VTI トンネルとセカンダリ VTI トンネルの両方が設定され、稼働していて、アクティブであることを確認します。

- **[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**

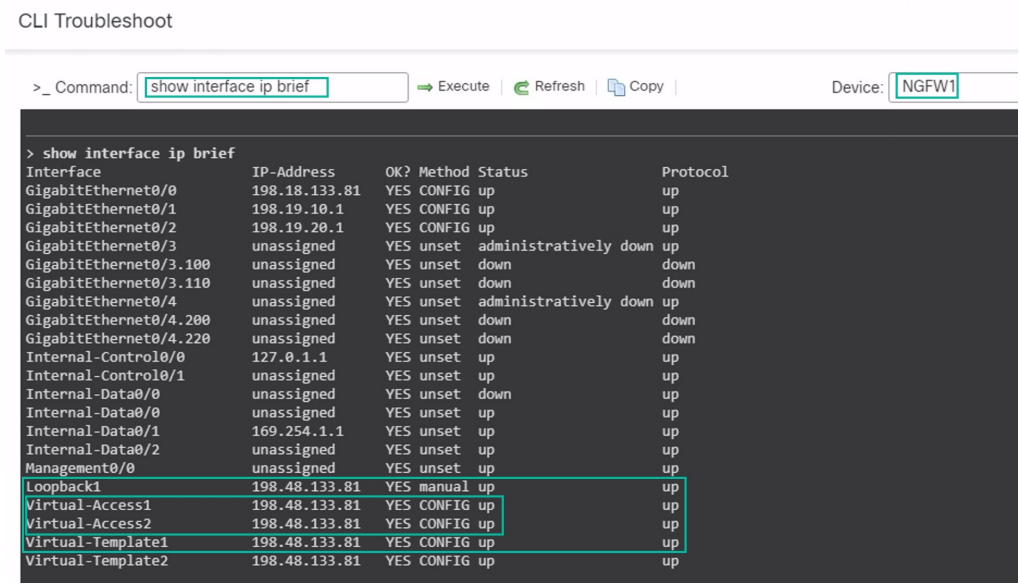
  VPN トンネルが稼働していて緑であることを確認するために、[概要（Overview）]>[ダッシュボード（Dashboards）]>[サイト間VPN（Site-to-site VPN）] を選択します。



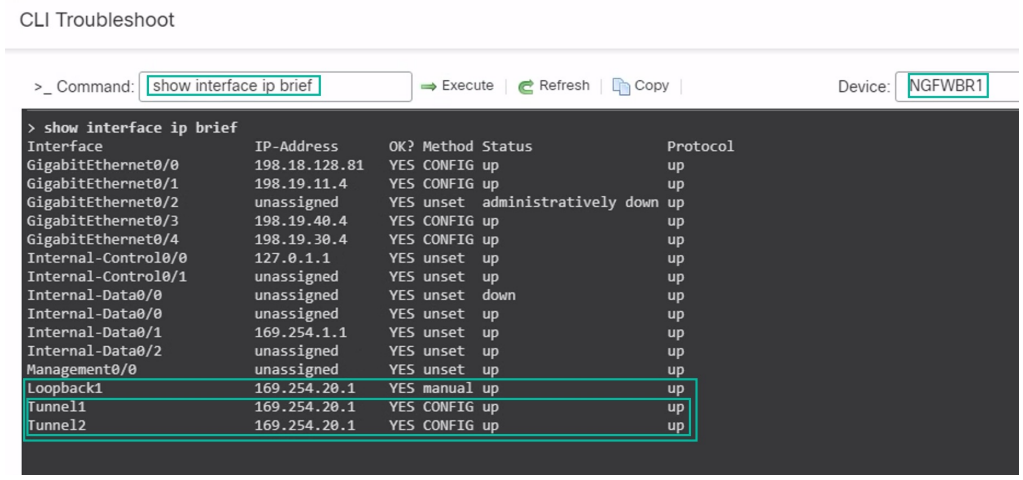
- **ハブノードとブランチノードでのルーティングの確認**

  1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
  2. NGFW1 を編集するために、[編集（Edit）] 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] ボタンをクリックします。[CLIのトラブルシュート（CLI Troubleshoot）] ウィンドウが表示されます
  5. [コマンド（Command）] フィールドに **show interface ip brief** と入力し、[実行（Execute）] をクリックして、ハブの DVTI から作成されたダイナミック仮想アクセスインターフェイスを表示します。

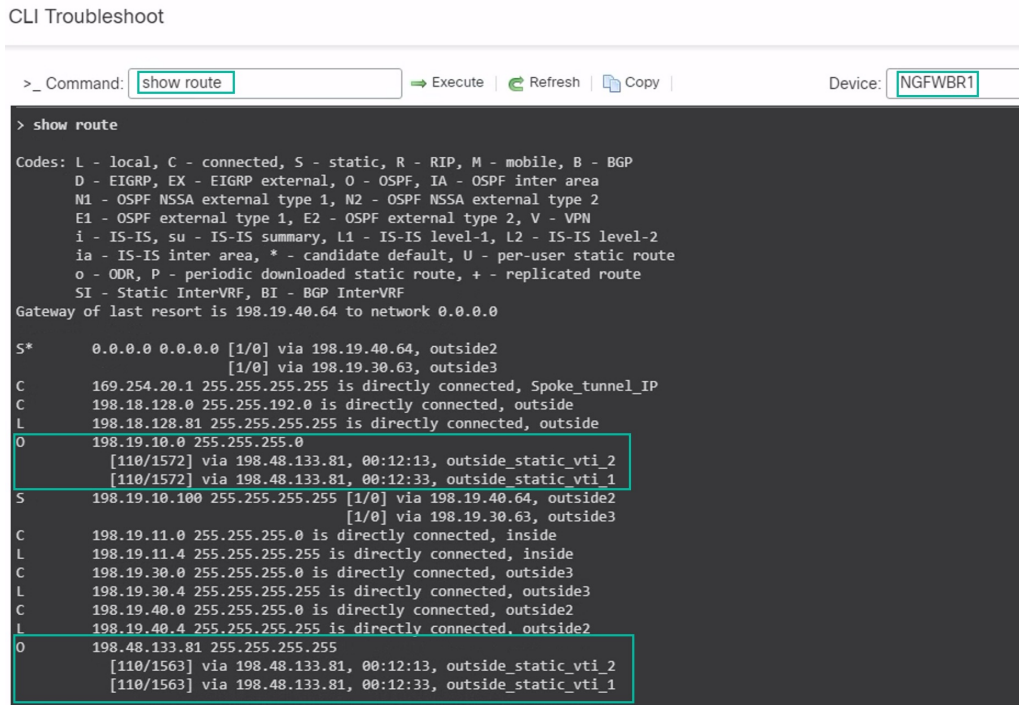
（注） **NGFWBR1** がセカンダリ VTI 接続を介して NGFW1 に接続するときに、同じ DVTI から Virtual-Access2 インターフェイスが生成されます。



6. NGFWBR1 ノードに対してステップ 2 ～ 5 を繰り返して、次の図に示すように、スタティック VTI インターフェイスの **Tunnel1** および **Tunnel2** を表示します。



7. [コマンド（Command）] フィールドに **show route** と入力し、[実行（Execute）] をクリックして、セカンダリ VTI トンネルの追加後のルートを表示します。



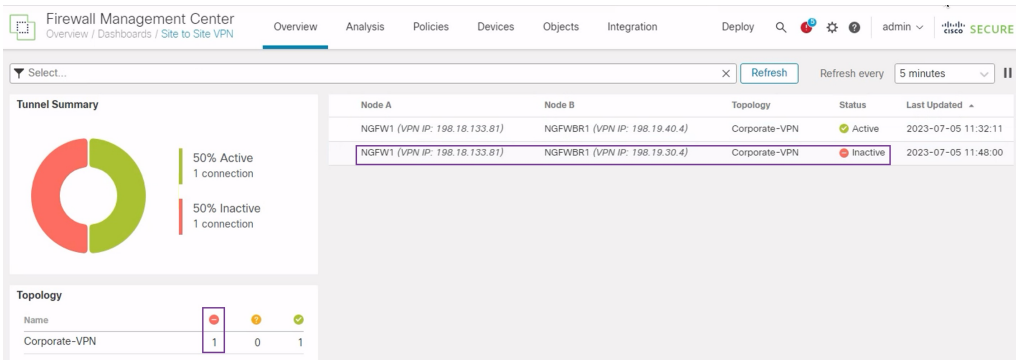
- プライマリ（**outside_static_vti_1**）とセカンダリ（**outside_static_vti_2**）の両方のVTI で、OSPF を介して **Corporate_LAN**（198.19.10.0/24）が学習されていることに注意してください。
- プライマリ VTI とセカンダリ VTI の両方で、OSPF を介して DVTI トンネル IP（198.48.133.81）も学習されていることに注意してください。

- **プライマリトンネルがダウンした場合のセカンダリトンネルへのフェールオーバーの確認**

1. この例では、セカンダリトンネルへのフェールオーバーを検証するために、アップストリームデバイスのアクセス制御リストを通じて、または、Management Center から Threat Defense の outside3 インターフェイスをシャットダウンして、outside3 インターフェイスから送信されてインターネットに向かうアウトバウンドトラフィックを制限することで、パケット損失を引き起こすことができます。

（注） インターフェイスをシャットダウンするとネットワークに影響が出る可能性があるため、実稼働ネットワークで試してはなりません。

2. [サイト間VPN（Site-to-site VPN）] ダッシュボードでは、次の図に示すように、プライマリトンネルがダウンしています。



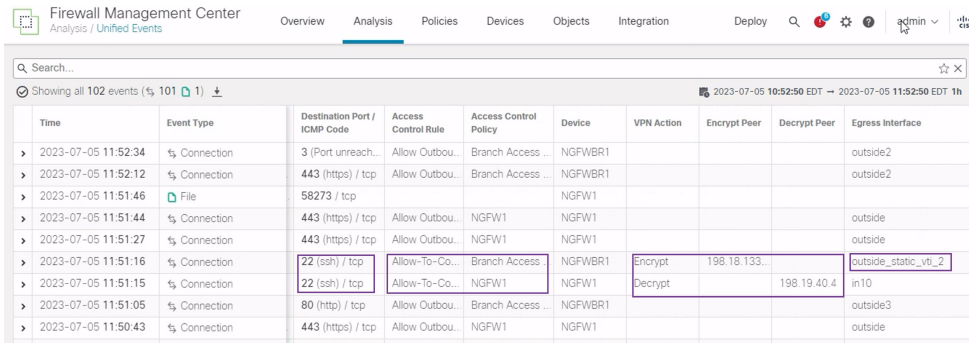
3. ブランチからハブへのトラフィックを開始します。WKST BR ワークステーションにログインし、NGFW1 の背後にあるホストに SSH 接続します。ホストに正常に SSH 接続できることを確認します。

4. 統合イベントビューアを使用して、トラフィックの出力パスを確認します。

   1. [分析（Analysis）] > [統合イベント（Unified Events）] を選択します。

   2. 列ピッカーを使用して、[VPNアクション（VPN Action）]、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、および [出力インターフェイス（Egress Interface）] の列を追加します。

   3. 次の図に示すように、新しい列と、[宛先ポート/ICMPコード（Destination Port/ICMP Code）]、[アクセスコントロールルール（Access Control Rule）]、[アクセスコントロールポリシー（Access Control Policy）]、および [デバイス（Device）] の列を並べ替えてサイズ変更します。



SSH の **NGFWBR1** での出力インターフェイス（ポート 22）がセカンダリインターフェイス（**outside_static_vti_2**）として表示されるようになったことに注意してください。

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 を使用して、Cisco Secure Firewall Threat Defense でのルートベースの VPN トンネルに関連する問題をデバッグします。

（注） 実稼働環境の Threat Defense デバイスで debug コマンドを実行する場合は、注意して進めてください。デバイスでさまざまなデバッグレベルを設定できるため、詳細な出力が行われる可能性があります。

操作	CLI コマンド
特定のピアの条件付きデバッグを有効にする	**debug crypto condition peer <peer-IP>**
仮想トンネルインターフェイス情報をデバッグする	**debug vti 255**
IKEv2 プロトコル関連のトランザクションをデバッグする	**debug crypto ikev2 protocol 255**
IKEv2プラットフォーム関連のトランザクションをデバッグする	**debug crypto ikev2 platform 255**
一般的なIKE関連のトランザクションをデバッグする	**debug crypto ike-common 255**
IPSec関連のトランザクションをデバッグする	**debug crypto ipsec 255**

関連リソース

リソース（Resource）	URL
Cisco Secure Firewall Threat Defense リリースノート	https://www.cisco.com/go/firewall-release-notes
すべての新機能と廃止された機能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com の Cisco Secure Firewall	http://www.cisco.com/go/firewall
Cisco.com のマニュアル	http://www.cisco.com/go/firewall-docs
YouTube 上の Cisco Secure Firewall	https://www.youtube.com/cisco-netsec
Cisco Secure Firewall Essentials	https://secure.cisco.com/secure-firewall

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。