Cisco Secure Firewall Threat Defense SD-WAN 展開

2025 年 9 月

SD-WAN ウィザードを使用した SD-WAN オーバーレイの展開

Management Center では、新しい SD-WAN ウィザードを使用して、中央の本社（ハブ）とリモートのブランチサイト（スポーク）間の VPN トンネルおよびルーティング設定を簡単に設定できます。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。

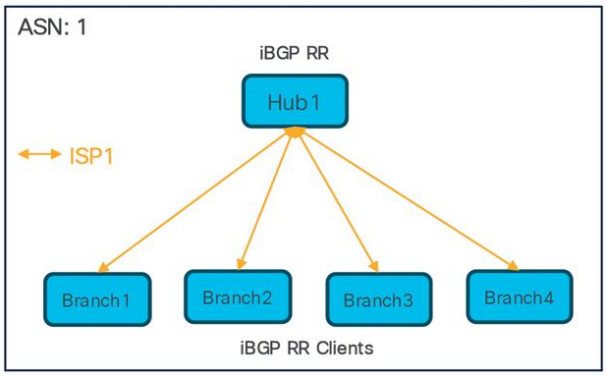
SD-WAN ウィザードを使用する利点

- SD-WAN ネットワークの VPN およびルーティング設定を簡素化および自動化します。
- ルートベースの VPN トンネルを作成し、以下のようなタスクを自動化することで設定プロセスを簡素化します。
  - ブランチのスタティック トンネル インターフェイスを生成する。
  - トンネルインターフェイスに IP アドレスを割り当てる。
  - SD-WAN オーバーレイネットワークの BGP を設定する。これらの設定により、ハブとスポーク間、およびハブを介したスポーク同士のシームレスな接続を確立できます。
- ハブがルートリフレクタとして機能し、以下を実現するため、シームレスなルーティングを提供します。
  - スポーク間を接続する。
  - スポークのアクティブトンネルとバックアップトンネルに基づいて最適なルーティングパスを決定する。
- 必要なユーザー入力を最小限にする。
- 一度に複数のブランチを簡単に追加。
- 簡単なデュアル ISP 設定を提供。
- ネットワークのスケーリングが可能。

SD-WAN ウィザードは、Threat Defense のハブアンドスポークトンネルおよびルーティングの設定を簡素化し自動化しますが、エクストラネットデバイスまたはユーザー定義の仮想ルータがある VPN 展開の場合には、ルートベースまたはポリシーベースの VPN ウィザードを使用します。

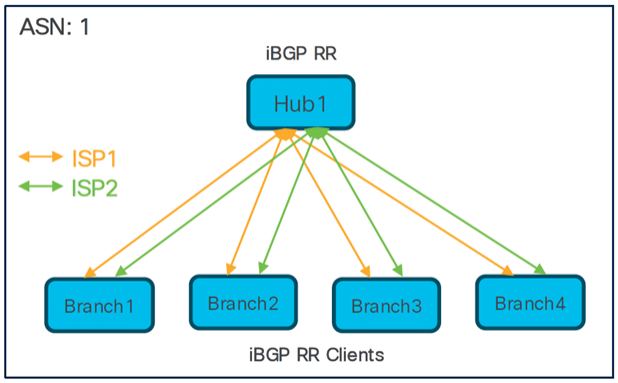
SD-WAN ウィザードの展開モデル

単一ハブと単一 ISP



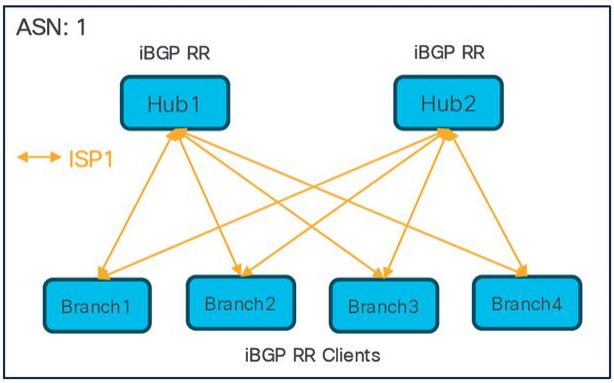
- 1 つの SD-WAN ハブアンドスポークトポロジ
- SD-WAN VPN トンネルの総数：4

単一ハブとデュアル ISP



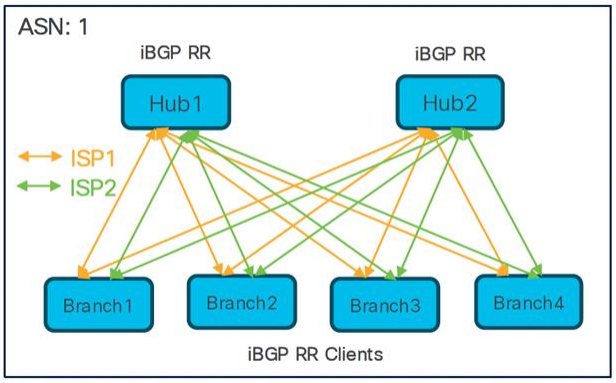
- 2 つの SD-WAN ハブアンドスポークトポロジ
- SD-WAN VPN トンネルの総数：8

デュアルハブと単一 ISP



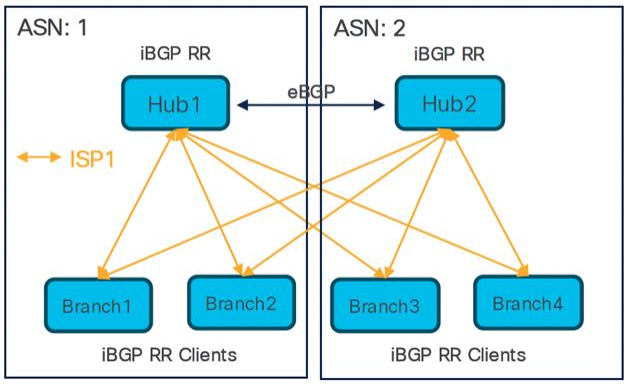
- 単一の SD-WAN ハブアンドスポークトポロジ
- SD-WAN VPN トンネルの総数：8

デュアルハブとデュアル ISP



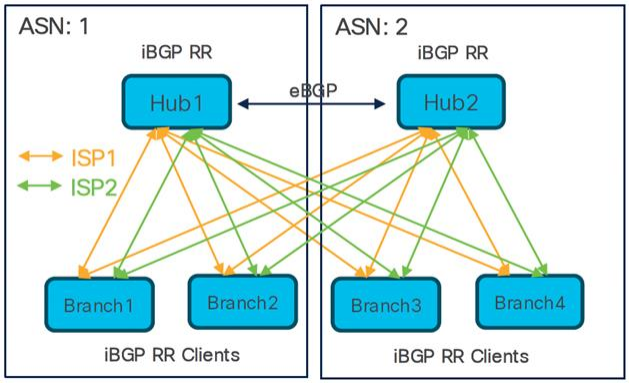
- 2 つの SD-WAN ハブアンドスポークトポロジ
- SD-WAN VPN トンネルの総数：16

異なる地域にあるデュアルハブと単一 ISP



- 2 つの SD-WAN ハブアンドスポークトポロジ
- ハブ間の eBGP ピアリング
- SD-WAN VPN トンネルの総数：8

異なる地域にあるデュアルハブとデュアル ISP



- 4 つの SD-WAN ハブアンドスポークトポロジ
- ハブ間の eBGP ピアリング

SD-WAN VPN トンネルの総数：16

SD-WAN ウィザードを使用したデュアルハブおよびデュアル ISP SD-WAN オーバーレイネットワークの展開

SD-WAN ウィザードの使用に関する前提条件

- Management Center はバージョン 7.6.0 以降である必要があります。
- ハブデバイスはバージョン 7.6.0 以降である必要があります。
- スポークデバイスはバージョン 7.3.0 以降である必要があります。
- Management Center Essentials（旧 Base）ライセンスでは、輸出規制対象機能を許可する必要があります。
- 管理者ユーザーである必要があります。

SD-WAN ウィザードの使用に関するガイドライン

ガイドライン

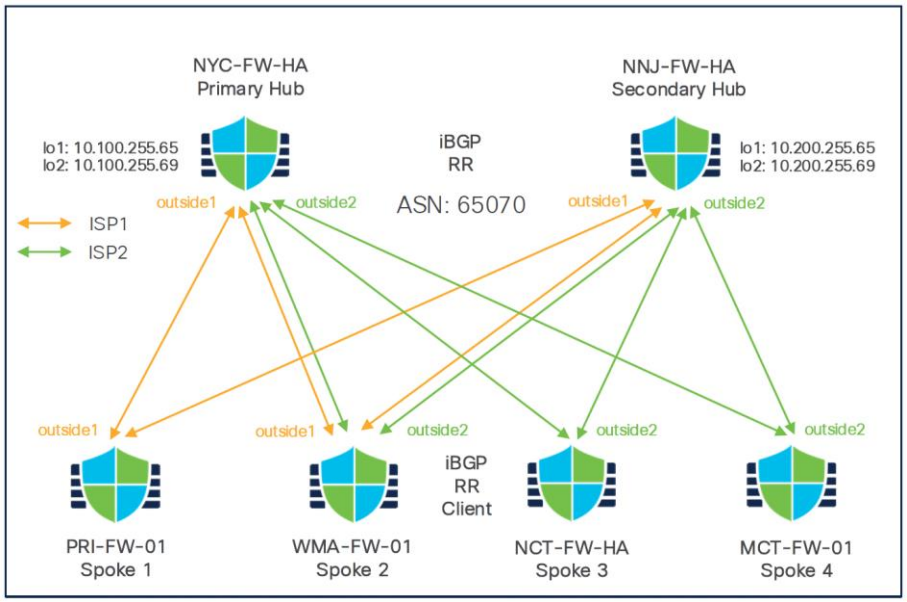
- 2 つのハブの DVTI を設定する場合は、それらの IPsec トンネルモード（IPv4 または IPv6）が同じであることを確認します。
- ハブが個別の保護ネットワークで地理的に分離されている場合は、それらの間でポイントツーポイント ルートベース VPN トポロジを設定して、これらのネットワーク間の直接通信を有効にします（[デバイス（Devices）] > [サイト間（Site-to-site）] > [追加（Add）] > [ルートベースVPN（Route-Based VPN）]）。
- セキュリティゾーンまたはインターフェイスグループを作成する場合は、[インターフェイスタイプ（Interface Type）] に [ルーテッド（Routed）] を選択します。
- スポークセキュリティゾーンを使用して、スポークとの間のトンネルトラフィックを許可するアクセス コントロール ポリシーを設定します。
- デバイスに IPv6 アドレス設定のみがある場合は、IPv4 アドレスを持つループバックまたは物理インターフェイスで BGP ルータ ID を設定する必要があります（[デバイス（Device）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [一般設定（General Settings）] > [BGP]）。
- すべての SD-WAN VPN トポロジのすべてのトンネルに一意のローカル IKE ID を設定します。

重要な考慮事項

- SD-WAN ウィザードを使用して、SD-WAN トポロジで最大 2 つのハブを設定できます。
- 各スポークで、トポロジごとに WAN インターフェイスを 1 つだけ使用できます。

  セカンダリ WAN インターフェイスのあるスポークは、最初の WAN インターフェイスにすでに存在する場合、既存の SD-WAN トポロジに追加できません。ただし、デュアル ISP 設定の場合は、2 つ目の SD-WAN トポロジと 2 つ目の WAN インターフェイスを設定できます。
- Cisco Secure Firewall は、最大 1024 の仮想トンネルインターフェイスをサポートします。
- Cisco Secure Firewall は、デバイスあたり最大 500 の BGP ピアをサポートします。
- SD-WAN ウィザードは、以下の機能をサポートしていません。
  - IKEv1
  - VTI はクラスタデバイスでサポートされていないため、クラスタデバイスはハブとスポークではサポートされません。
  - ASA、Cisco IOS、Cisco Viptela、Umbrella、Meraki、またはベンダーデバイスなどのエクストラネット ハブおよびスポーク。

ネットワーク トポロジ



このデュアル ISP トポロジでは、ハブとスポークは単一の地域にあり、AS 番号（ASN）は 65070 です。ハブとスポークは、内部ボーダー ゲートウェイ プロトコル（IBGP）をルーティングプロトコルとして使用して、ルーティング情報を交換します。

このトポロジのハブとスポーク間の VPN トンネルを設定するには、SD-WAN ウィザードを使用して次の 2 つの SD-WAN トポロジを作成する必要があります。

表 1. SD-WANトポロジ 1

パラメータ	値
Primary Hub	NYC
セカンダリハブ	NNJ
スポーク	Branch1（PRI）、Branch2（WMA）
[ASN]	65070
BGP コミュニティ	1000
VPN インターフェイス（スポーク トンネル送信元）	outside1（ISP1）
トンネル数	4

表 2. SD-WANトポロジ 2

パラメータ	値
Primary Hub	NNJ
セカンダリハブ	NYC
スポーク	Branch2（WMA）、Branch3（NCT）、Branch4（MCT）
[ASN]	65070
BGP コミュニティ	1000
VPN インターフェイス（スポークトンネル送信元）	outside2（ISP2）
トンネル数	[6]

注： 各ブランチの outside2 インターフェイスから各ハブに 2 つの SD-WAN VPN トンネルが確立されます。したがって、SD-WAN トポロジ 2 の SD-WAN VPN トンネルの数は 6 です。

このデュアル ISP 展開の VPN トンネルの総数は 10 です。

SD-WAN ウィザードを使用した SD-WAN オーバーレイの設定

次の 2 つの SD-WAN トポロジを設定する必要があります。

- ISP1 のスポークの VPN インターフェイスとして outside1 を使用する SDWAN-Topology1
- ISP2 のスポークの VPN インターフェイスとして outside2 を使用する SDWAN-Topology 2

ステップ 1. [デバイス（Devices）] > [VPN] > [サイト間（Site to Site）] を選択し、[追加（Add）] をクリックします。

ステップ 2. [SD-WANトポロジ（SD-WAN Topology）] オプションボタンをクリックします。

ステップ 3. [トポロジ名（Topology Name）] フィールドに、トポロジの名前として SDWAN-Topology1 と入力します。

ステップ 4. [作成（Create）] をクリックします。

ステップ 5. 次のようにして、ハブを設定します。

i. [ハブの追加（Add Hub）] をクリックします。

ii. [デバイス（Device）] ドロップダウンリストからハブを選択します。この例では、**NYC-FW-HA** を選択します。

iii. [ダイナミック仮想トンネルインターフェイス（DVTI）（Dynamic Virtual Tunnel Interface (DVTI)）] ドロップダウンリストの横にある [+] をクリックして、ハブのダイナミック VTI を追加します。

iv. [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。

- [セキュリティゾーン（Security Zone）] ドロップダウンリストからセキュリティゾーンを選択します。この例では、**tunnel-zone** です。

- [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。この例では、Ethernet1/1 です。
- [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。ループバック インターフェイスがない場合は、[+] をクリックして作成します。この例では、**Loopback1** です。
- [OK] をクリックします。

v. [ハブゲートウェイIPアドレス（Hub Gateway IP Address）] フィールドに、ハブの VPN インターフェイスのパブリック IP アドレス、またはスポークが接続するダイナミック VTI のトンネル送信元を入力します。

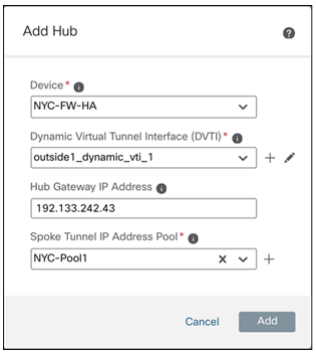
注： インターフェイスに静的 IP アドレスがある場合、このアドレスは自動入力されます。ハブが NAT デバイスの背後にある場合は、NAT 後の IP アドレスを手動で設定する必要があります。

vi. [スポークトンネルIPアドレスプール（Spoke Tunnel IP Address Pool）] ドロップダウンリストから、IP アドレスプールを選択するか、[+] をクリックしてアドレスプールを作成します。

注： 各 IP アドレスプールは一意である必要があるため、[IPプールの追加（Add IP Pool）] ダイアログボックスでアドレスプールを作成する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにしないでください。

スポークを追加すると、ウィザードはスポーク トンネル インターフェイスを自動生成し、この IP アドレスプールからこれらのスポークインターフェイスに IP アドレスを割り当てます。この例では、NYC-Pool1 です。

vii. [追加] をクリックしてハブの設定を保存します。



viii. セカンダリハブを追加するために、手順 5a から手順 5g を繰り返します。この例では、NNJ-FW-HA です。

ステップ 6. スポークを設定します。

a. [スポークの追加（一括追加）（Add Spokes (Bulk Addition)）] をクリックします。

b. [スポークの一括追加（Add Bulk Spokes）] ダイアログボックスで、次のパラメータを設定します。

i. スポークデバイスを [利用可能なデバイス（Available Devices）] リストから選択し、[追加（Add）] をクリックしてデバイスを [選択済みのデバイス（Selected Devices）] に移動します。この例では、**PRI-FW-01** と **WMA-FW-01** を移動します。

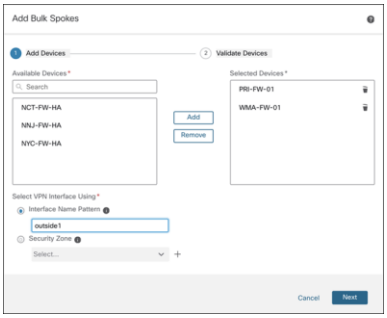
ii. 次のいずれかの方法を使用して、スポークの VPN インターフェイスを選択します。

iii. [インターフェイス名パターン（ Interface Name Pattern ）] のオプションボタンをクリックし、スポークのインターネットまたは WAN インターフェイスの論理名と一致する文字列を指定します（outside*、wan* など）。この例では、ISP1 インターフェイスの文字列は outside1 です。

スポークに同じパターンを持つ複数のインターフェイスがある場合、パターンに一致する最初のインターフェイスがトポロジに選択されます。

または

[セキュリティゾーン （Security Zone）] のオプションボタンをクリックし、ドロップダウンリストからスポークの VPN インターフェイスを含むセキュリティゾーンを選択するか、[+]をクリックしてセキュリティゾーンを作成します。



c. [次へ（Next）] をクリックします。ウィザードは、指定されたパターンのインターフェイスがスポークにあるかどうかを検証します。検証済みのデバイスのみがトポロジに追加されます。

d. [追加（Add）] をクリックし、[次へ（Next）] をクリックします。ウィザードは、各スポークについて、トンネルの接続先 IP アドレスとしてハブのパブリック IP アドレス（[ハブゲートウェイIPアドレス（Hub Gateway IP Address）] で定義）を自動的に選択します。

ステップ 7. SD-WAN トポロジ内のデバイスの**認証設定**を行います。

a. [認証タイプ（Authentication Type）] ドロップダウンリストから、デバイス認証に使用する手動の事前共有キー、自動生成された事前共有キー、または証明書を選択します。

この手順ではデフォルト設定を使用して、次の手順に進むことができます。設定は必要に応じて後で編集できます。この例では、デバイス認証に**事前共有手動キー**を使用します。

- **[事前共有手動キー（Pre-shared Manual Key）]**：VPN 接続用の事前共有キーを指定します。
- **[事前共有自動キー（Pre-shared Automatic Key）]**：（デフォルト値）ウィザードにより、この VPN 接続の事前共有キーが自動的に定義されます。[事前共有キー長（Pre-shared Key Length）] フィールドでキーの長さを指定します。指定できる範囲は 1 ～ 127 です。
- **[証明書（Certificate）]**：認証方法として証明書を使用する場合、ピアは PKI インフラストラクチャ内の CA サーバーからデジタル証明書を取得し、相互に認証するために使用します。

b. [トランスフォームセット（Transform Sets）] ドロップダウンリストから 1 つ以上のアルゴリズムを選択するか、デフォルト値を使用します。

c. [IKEv2ポリシー（IKEv2 Policies）] ドロップダウンリストから 1 つ以上のアルゴリズムを選択するか、デフォルト値を使用します。

d. [次へ（Next）] をクリックします。

ステップ 8. SD-WAN 設定を行います。

この手順には、スポーク トンネル インターフェイスの自動生成と、オーバーレイネットワークの BGP 設定が含まれます。

a. [スポーク トンネル インターフェイス セキュリティ ゾーン（Spoke Tunnel Interface Security Zone）] ドロップダウンリストからセキュリティゾーンを選択するか、[+] をクリックしてセキュリティゾーンを作成します。このセキュリティゾーンには、ウィザードにより、スポークの自動生成されたスタティック仮想トンネルインターフェイス（SVTI）が自動的に追加されます。この例では、セキュリティゾーンは **tunnel-zone** です。

b. [VPNオーバーレイトポロジでBGPを有効化（Enable BGP on the VPN Overlay Topology）] チェックボックスをオンにして、オーバーレイ トンネル インターフェイス間のネイバー設定や、ハブとスポークの直接接続された LAN インターフェイスからの基本ルートの再配布などの BGP 設定を自動化します。

c. [自律システム番号（Autonomous System Number ）] フィールドに、自律システム（AS）番号を入力します。この例の AS 番号は **65070** です。

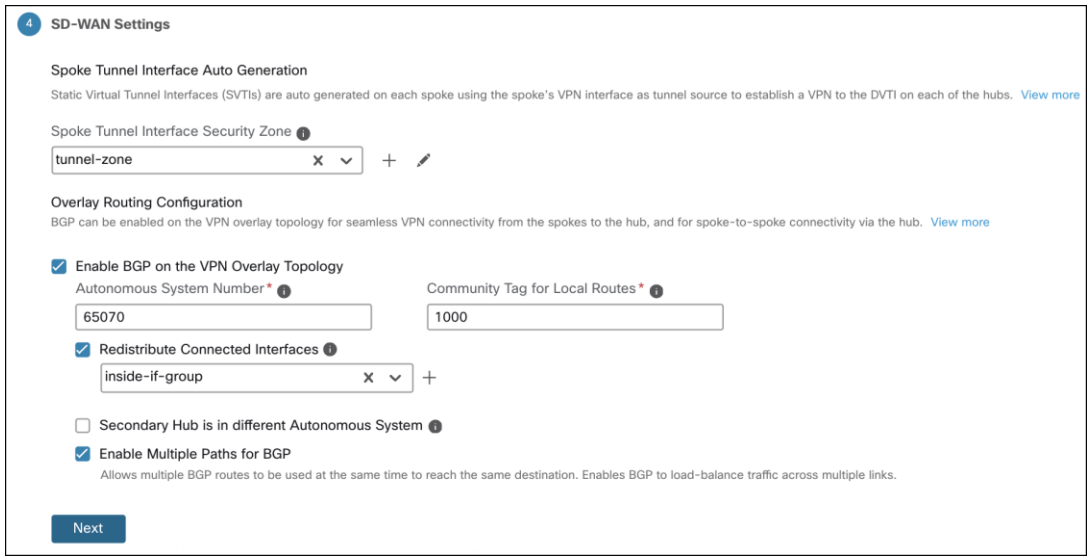
d. [ローカルルートのコミュニティタグ（Community Tag for Local Routes ）] フィールドに、接続されたローカルルートと再配布されたローカルルートにタグを付けるための BGP コミュニティ属性を入力します。

この属性は、簡単なルートのフィルタリングを有効にします。このコミュニティ文字列については、セカンダリ SD-WAN VPN トポロジにも同じコミュニティ文字列を使用する必要があることに注意してください。この例では、コミュニティ文字列は 1000 です。

e. [接続インターフェイスの再配布（Redistribute Connected Interfaces）] チェックボックスをオンにして、ドロップダウンリストからインターフェイスグループを選択するか、[+] をクリックして、オーバーレイトポロジでの BGP ルート再配布用に接続された内部または LAN インターフェイスを持つインターフェイスグループを作成します。この例では、インターフェイスグループは inside-if-group です。

f. [BGPのマルチパスの有効化（Enable Multiple Paths for BGP）] チェックボックスをオンにして、同じ宛先に到達するために複数の BGP ルートを同時に使用できるようにします。このオプションによって、BGPが複数のリンク間でトラフィックをロードバランシングできます。

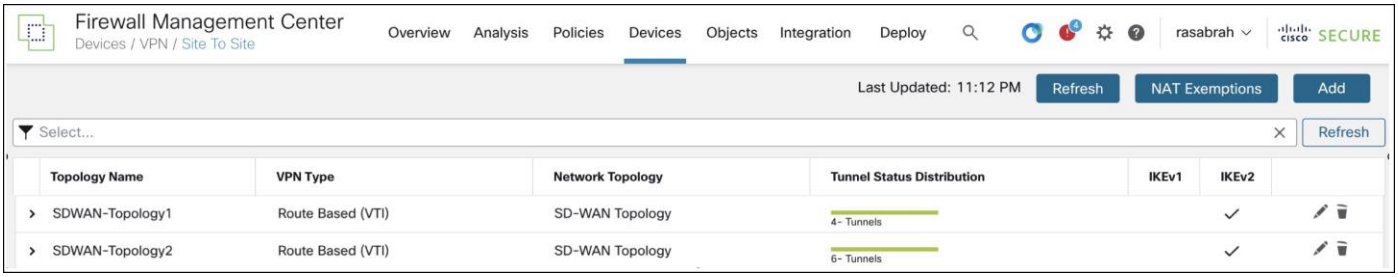
g. [次へ（Next）] をクリックします。



h. [完了（Finish）] をクリックして、SD-WAN トポロジを保存および検証します。

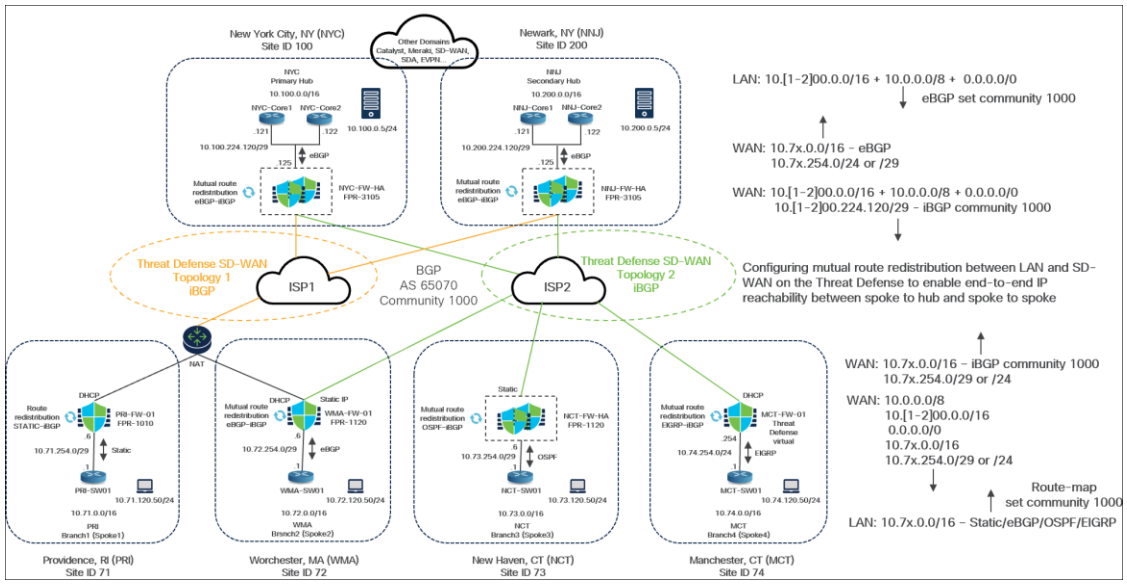
ステップ 9. 手順 1 から手順 8 を繰り返して、ISP2 の VPN インターフェイス（outside2）を使用して SDWAN-Topology2 を設定します。

[サイト間VPN概要（Site-to-Site VPN Summary）] ページ（[デバイス（Devices）] > [サイト間 VPN（Site To Site VPN）]）で、トポロジを表示できます。すべてのデバイスに設定を展開すると、このページですべてのトンネルのステータスを確認できます。



SD-WAN ネットワークのオーバーレイルーティングを設定します。

SD-WAN ウィザードは直接接続されたインターフェイスを自動的に再配布しますが、エンドツーエンドのサイト間通信では、特に Threat Defense デバイスの背後に他のルータや内部ネットワークが存在する場合に、追加のルート再配布が必要になります。



この例のトポロジには、次のパラメータが指定されています。

ハブサイト

- ニューヨーク市、NYC：プライマリハブとして指定。HA ペアで NYC-FW-HA FPR-3105 ファイアウォールを使用します。
  - コアスイッチと Threat Defense デバイス（NYC-FW-HA）間で eBGP ピアリングを使用します
- ニューアーク、NY（NNJ）
  - セカンダリハブとして指定。HA ペアでも NNJ-FW-HA FPR-3105 ファイアウォールを使用します。
- 両方のハブで、さまざまな内部ドメインを相互接続するために、レイヤ 2/レイヤ 3 のコア スイッチ（「NYC Core 1 および Core 2」）のペアが利用されます。
- DNS サーバー 10.100.0.5/24 および 10.200.0.5/24 は、これらのサイトでテストを目的として使用できます。

スポークサイト：4 つのブランチオフィスがあり、LAN のルーティング設定はそれぞれ異なります。

- プロビデンス、RI（PRI）：
  - PRI-SW01 への LAN 接続のための Threat Defense（PRI-FW-01）でのスタティックルーティング。
  - スタティックルートと iBGP の間に設定されたルート再配布。
- ウースター、MA（WMA）：
  - Threat Defense（WMA-FW-01）と（WMA-SW01）LAN スイッチ間の eBGP ピアリング
  - eBGP と iBGP の間に設定された相互ルート再配布。
- ニューヘブン、CT（NCT）：
  - Theat Defense（NCT-FW-HA）とレイヤ 2/レイヤ 3（NCT-SW01）LAN スイッチ間の OSPF ピアリング

- OSPF と iBGP の間に設定された相互ルート再配布。

- マンチェスター、CT（MCT）：
  - Theat Defense（MCT-FW-01）からとレイヤ 2/レイヤ 3（MCT-SW01）LAN スイッチ間の EIGPR ピアリング
  - EIGRP と iBGP の間に設定された相互ルート再配布。

注： ルート再配布の制御には、ルートマップを使用することを強く推奨します。これは、ルーティングループを防止するのに役立ちます。

ハブ側（ニューヨーク市）ルートアドバタイズメント（eBGP）

この例では、新しい都市ハブについて、次の 3 つのプライマリルートが eBGP を介してアドバタイズされます。

- 10.100.0.0/16
- 10.0.0.0/8 の要約または集約されたルート

コアは、1000 の BGP コミュニティを使用してこれらのルートをアドバタイズするように設定されます。BGP コミュニティが正しく設定されていない場合、これらのルートはオーバーレイに再配布されません。これらのルートには、1000 の BGP コミュニティが設定されています。

WAN から LAN へのルート再配布（ハブ）

ハブサイトの Threat Defense デバイスには、SD-WAN オーバーレイ（WAN）から LAN 側に戻るルートのアドバタイズを制御するためのルートマップが設定されています。

- このルートマップは特に、10.7x.x.x/16 ネットワークのアドバタイズを制御します。この場合、「x」はブランチの場所に対応します（たとえば、PRI の場合は 71、WMA の場合は 72、NCT の場合は 73、MCT の場合は 74）。
- 特定の WAN インターフェイスルート、10.7x.254.0/24 または /29 のみがアドバタイズされます。なぜなら、これらが、直接接続されているインターフェイスを表しているためであり、ハブがルートを正しく配置するために必要です。
- これらの特定ルートがアドバタイズされない場合、ブランチからアドバタイズされた集約ルートは配置されません。これにより再帰ルーティングのルックアップが容易になり、正しいネクストホップ情報がルーティングテーブルに正しく入力されるようになります。

SD-WAN オーバーレイへの Threat Defense アドバタイズ

- ハブの Threat Defense デバイスは、1000 の iBGP コミュニティで直接接続されたセグメント（10.100.224.120/29、10.200.224.120/29）をアドバタイズします。
- すでに BGP コミュニティ設定（たとえば、1000）が設定されている LAN 側から（eBGP 再配布を使用して）受信したルートも、オーバーレイにアドバタイズされます。

受信側（ハブ）ルートの承認

- 受信側（ハブ）では、BGP コミュニティが 1000 に設定されているルートのみを受け入れるように Threat Defense デバイス上でルートマップが設定されます。

ルート再配布の必要性

LAN 側ネットワーク（たとえば、PRI、WMA、NCT、MCT などのブランチまたはスポークサイトや、ハブサイト NYC、NNJ の背後）は、Threat Defense デバイスに直接接続されていません。したがって、相互に直接通信することはできません。

代わりに、これらの LAN ネットワークは、Threat Defense デバイスの背後にある別のレイヤ 2/レイヤ 3 スイッチまたはルータに設定された他のルーティングプロトコルまたはスタティックルートを介して接続されます。

- PRI はスタティックルートを使用します
- WMA は eBGP を使用します
- NCT は OSPF を使用します
- MCT は EIGRP を使用します

ハブサイト（NYC、NNJ）の背後には、eBGP を使用して内部ネットワークをアドバタイズするコアスイッチまたはルータもあります。

あるブランチのデバイスが別のブランチまたはハブのデバイスと通信する場合、関連するすべての LAN 側ルートは、BGP を実行している SD-WAN BGP オーバーレイにアドバタイズする必要があり、オーバーレイ BGP ルートは LAN ルーティングドメインにアドバタイズする必要があります。

SD-WAN ウィザードは、オーバーレイに BGP を自動的に設定し、直接接続された（内部または LAN に接続した）インターフェイスを再配布することにより展開を簡素化しますが、LAN 側ネットワークが Threat Defense デバイスに直接接続されておらず、他のルーティングプロトコルまたはスタティックルートに依存しているような環境では、多くの場合、十分ではありません。このような場合は、LAN 側のルーティングプロトコル（スタティック、eBGP、OSPF、EIGRP など）と SD-WAN BGP オーバーレイとの間に相互ルート再配布を手動で設定し、スポークサイトとハブサイト間でエンドツーエンドの完全な IP 到達可能性を確保する必要があります。

ハブの **BGP** ピアリングの表示

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

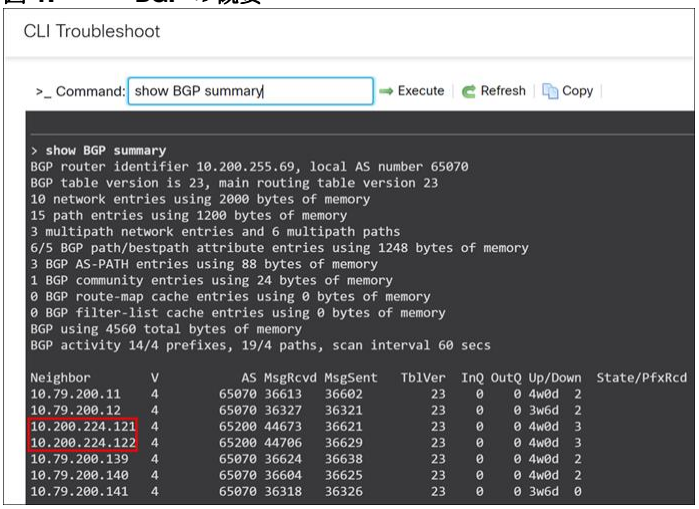
ステップ 2. デバイスリストページから **NNJ-FW-HA** をクリックします。

ステップ 3. [サマリー（Summary）] タブをクリックします。

ステップ 4. [全般（Genera）] エリアで、[CLI] をクリックし、次のコマンドを実行して、LAN ネイバーにアドバタイズされたルートを表示します。

```
> show bgp summary
```

図 1.　　BGP の概要



強調表示されている IP アドレスは、ハブにある Threat Defense デバイスとそれぞれの LAN 側コアスイッチとの間で確立された 2 つの eBGP ピアリングです。

ネイバーにアドバタイズされたルートの表示

Threat Defense が特定の eBGP ネイバーにアドバタイズしている BGP ルートを表示するには、次の手順を実行します。

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

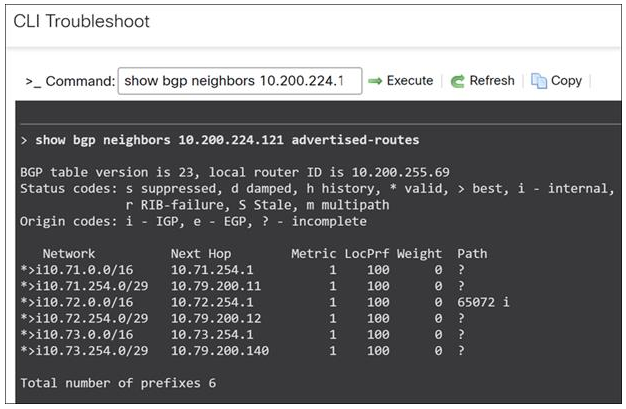
ステップ 2. デバイスリストページから **NNJ-FW-HA** をクリックします。

ステップ 3. [サマリー（Summary）] タブをクリックします。

ステップ 4. [全般（General）] エリアで、[CLI] をクリックし、次のコマンドを実行します。

```
> show bgp neighbors 10.200.224.121 advertised-routes
```

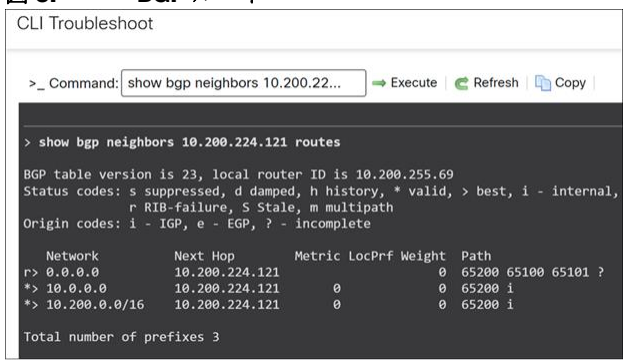
図 2. BGP ネイバー



ステップ 5. Threat Defense デバイスが LAN 側から受信したルートを表示するには、次の手順を実行します。

```
> show bgp neighbors 10.200.224.121 routes
```

図 3. BGP ルート



LAN 側（コアスイッチ）は、デフォルトルート（0.0.0.0/0）、サマリールート 10.0.0.0、および場所がニュージャージーの場合には 10.200.0.0/16 といった特定のルートを含むルートをアドバタイズします。

NNJ-FW-HA（ハブ）：SD-WAN オーバーレイ用の BGP の設定

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. デバイスリストページから **NNJ-FW-HA** 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。

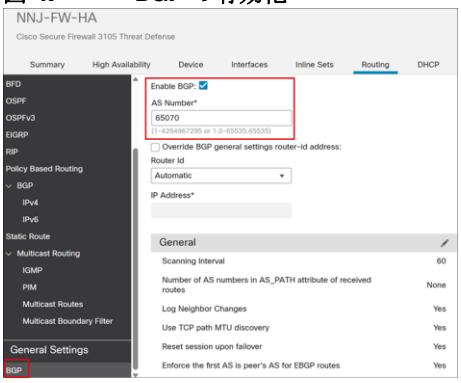
ステップ 4. [一般設定（General Settings）] で [BGP] をクリックします。

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て、BGP ルーティングプロセスを有効にします。

ステップ 6.　[AS 番号（AS Number）] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。

この例では、プライベート AS 番号 **65070** が SD-WAN オーバーレイに使用されます。

図 4.　BGP の有効化



ステップ 7.　[BGP] > [IPv4] を選択します。

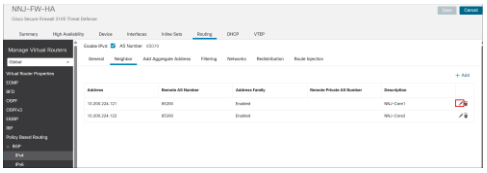
ステップ 8.　[BGP の有効化（Enable BGP）] チェックボックスをオンにして、BGP ルーティングプロセスを有効にします。

ステップ 9.　[Neighbor] クリックします。

ステップ 10.　[追加（Add）] をクリックして、BGP ネイバーとネイバーの設定を**定義します**。

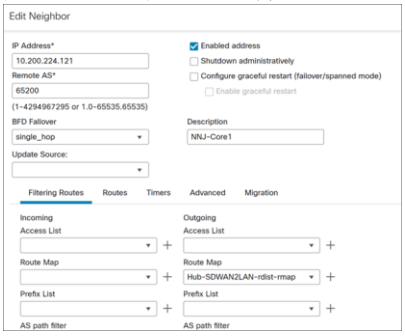
この例では、2 つのネイバー、10.200.224.121（NNJ-Core1）と 10.200.224.122（NNJ-Core2）が設定されています。これは、コアスイッチを表します。

図 5.　ネイバーの設定



ステップ 11.　設定の詳細を表示するには、既存のネイバーの横にある [編集（Edit）] アイコンをクリックします。

図 6.　ネイバーの詳細



ルートマップを使用して、インバウンドとアウトバウンドの両方向でルートの再配布を管理できます。この例では、特に BGP の場合、アウトバウンドルートマップ（SD-WAN から LAN へ）を使用し、インバウンドルートマップ（LAN から SD-WAN へ）は使用しません。

ハブ用の **IPv4** プレフィックスリストの設定

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. **[プレフィックスリスト（Prefix List）] > [IPv4プレフィックスリスト（IPv4 Prefix List）]** を選択します。

ステップ 3. [IPv4プレフィックスリストの追加（Add IPv4 Prefix List）] をクリックします。

ステップ 4. [名前（Name）] フィールドに、**All-branch-inside-networks** と入力します。

ステップ 5. [追加（Add）] をクリックします。

[プレフィックス リスト エントリの追加（Add Prefix List Entry）] ダイアログボックスが表示されます。次の設定を行えます。

- **アクション**：許可
- **シーケンス番号**：10
- **IP アドレス**：10.64.0.0/12。IP アドレスは、スポーク側ネットワークの要約された範囲、具体的には PRI（71）、WMA（72）、NCT（73）、MCT（74）を表します。これにより、最小マスク長 /16、最大マスク長 /29 などの定義済みサブネットマスク条件に基づいてルートを照合できます。
- **プレフィックスの長さの最小値**：16
- **プレフィックスの長さの最大値**：29

ステップ 6. [追加（Add）] をクリックします。

ステップ 7. [保存（Save）] をクリックします。

ハブのコミュニティリストの作成

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. [コミュニティリスト（Community List）] を展開し、[コミュニティ（Community）] をクリックします。

ステップ 3. [コミュニティ リストの追加（Add Community List）] をクリックします。

ステップ 4. **[名前（Name）]** フィールドに、名前を入力します。この例では、**SDWAN-BGP-community** を使用します。

ステップ 5. [追加（Add）] をクリックします。

[コミュニティリストエントリの追加（Add Community List Entry）] ダイアログボックス。

ステップ 6. [標準（Standard）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

ステップ 7. [アクション（Action）] ドロップダウンリストから [許可（Allow）] オプションを選択して、再配布アクセスを指定します。

ステップ 8. [コミュニティ（Communities）] フィールドで、コミュニティ番号を指定します。この例では、**1000** と入力します。

ステップ 9. [追加（Add）] をクリックします。

ステップ 10. [保存（Save）] をクリックします。

ハブのルートマップオブジェクトの追加

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. [ルートマップ（Route Map）] をクリックします。

ステップ 3. [ルート マップの追加（Add Route Map）] をクリックします。

ステップ 4. [名前（Name）] フィールドに、**Hub-SDWAN2LAN-rdist-rmap** と入力します。

ステップ 5. [追加（Add）] をクリックします。

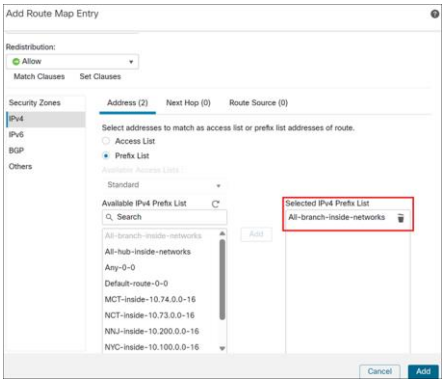
ステップ 6. [シーケンス番号（Sequence No.）] フィールドに数値を入力します。この例では、**10** と入力します。

ステップ 7. [再配布（Redistribution）] ドロップダウンリストから、再配布アクセスを示す [許可（Allow）] **アクション**を選択します。

ステップ 8. [IPv4] をクリックします。

i. [アドレス（Address）] タブをクリックします。

ii. ドロップダウンリストから [プレフィックスリスト（Prefix list）] を選択し、照合に使用する**プレフィックス リスト** オブジェクトを入力または選択します。この例では、**All-branch-inside-networks** を選択します。



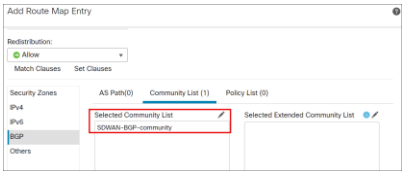
iii. [追加（Add）] をクリックします。

ステップ 9. [BGP] をクリックします。

ステップ 10. [コミュニティリスト（Community List）] タブをクリックします。

ステップ 11. [編集（edit）] をクリックし、SDWAN-BGP-community コミュニティリストを選択します。

ステップ 12. [OK] をクリックします。



ステップ 13. [追加（Add）] をクリックします。

ステップ 14. [保存（Save）] をクリックします。

PRI ブランチ（スポーク 1）：スタティックおよび iBGP 相互ルート再配布の設定

PRI ブランチ（スポーク 1）は、LAN 側でスタティックルーティングを使用するように設定されています。

PRI（スポーク）の IPv4 プレフィックスリストの設定

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. [プレフィックスリスト（Prefix List）] > [IPv4プレフィックスリスト（IPv4 Prefix List）] を選択します。

ステップ 3.　[IPv4プレフィックスリストの追加（Add IPv4 Prefix List）] をクリックします。

ステップ 4.　[名前（Name）] フィールドに、**PRI-inside-10.71.0.0-16** と入力します。

ステップ 5.　[追加（Add）] をクリックします。

[プレフィックス リスト エントリの追加（Add Prefix List Entry）] ダイアログボックスが表示されます。次の設定を行えます。

- **アクション**：許可
- **シーケンス番号**：10
- **IP アドレス**：10.64.0.0/16

ステップ 6.　[追加（Add）] をクリックします。

ステップ 7.　[保存（Save）] をクリックします。

PRI（スポーク）のルートマップオブジェクトの追加

ステップ 1.　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2.　[ルートマップ（Route Map）] をクリックします。

ステップ 3.　[ルート マップの追加（Add Route Map）] をクリックします。

ステップ 4.　[名前（Name）] フィールドに、**Static2iBGP-rdist-rmap** と入力します。

ステップ 5.　[追加（Add）] をクリックします。

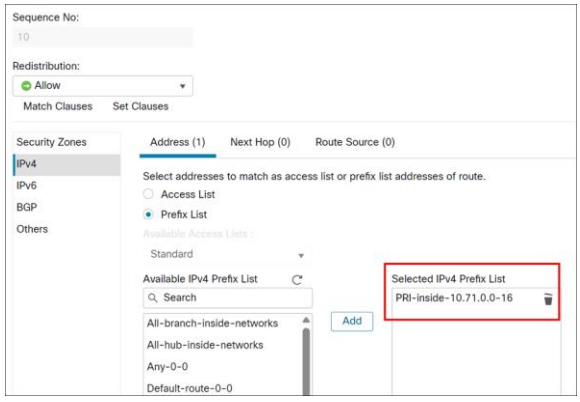
ステップ 6.　[シーケンス番号（Sequence No.）] フィールドに数値を入力します。この例では、**10** と入力します。

ステップ 7.　[再配布（Redistribution）] ドロップダウンリストから、再配布アクセスを示す [許可（Allow）] アクションを選択します。

ステップ 8.　[IPv4] をクリックします。

ステップ 9.　[アドレス（Address）] タブをクリックします。

ステップ 10.　ドロップダウンリストから [プレフィクスリスト（Prefix List）] を選択し、照合に使用するプレフィックス リスト オブジェクトを入力または選択します。この例では、**PRI-inside-10.71.0.0-16** を選択します。



ステップ 11.　[追加（Add）] をクリックします。

ステップ 12.　[保存（Save）] をクリックします。

スポークのスタティックルート再配布の設定（PRI-FW-01）

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

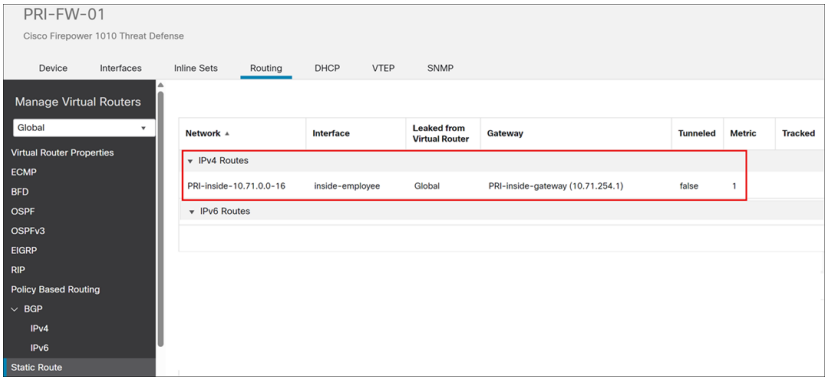
ステップ 2.　デバイスリストページから **PRI-FW-01** をクリックします。

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.　[Static Route] をクリックします。

ファイアウォールからのスタティックルートが LAN 側へと戻ります。

図 7.　PRI-FW-01 でのスタティックルートの設定



スタティックルートは BGP に再配布される必要があります。

ステップ 5.　[一般設定（General Settings）] で [BGP] をクリックします。

ステップ 6.　[BGP の有効化（Enable BGP）] チェックボックスをオンにして、BGP ルーティングプロセスを有効にします。

ステップ 7.　[AS番号（AS Number）] フィールドに、自律システム番号を入力し、[保存（Save）] をクリックします。

この例の AS 番号は **65070** です。

ステップ 8.　[BGP] > [IPv4] を選択します。

ステップ 9.　[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 10.　[再配布（Redistribution）] タブをクリックします。再配布設定により、別のルーティング ドメインから BGP にルートを再配布する条件を定義できます。

ステップ 11.　[追加（Add）] をクリックします。

ステップ 12.　[再配布の追加（Add Redistribution）] ダイアログボックスで、以下のパラメータを設定します。

i.　[送信元プロトコル（Source Protocol）] ドロップダウンリストで、BGP ドメインにルートを再配布する元となるプロトコルを選択します。この例では、[スタティック（Static）] を選択します。

ii.　[メトリック（Metric）] フィールドに、再配布されるルートのメトリックを入力します。この例の値は **1** です。

iii.　[ルートマップ（Route Map）] ドロップダウンリストで、再配布するネットワークをフィルタリングするために調べる必要のあるルートマップを選択します。この値を指定しない場合、すべてのネットワークが再配布されます。**Static2iBGP-rdist-map** が選択されています。これにより、必要なルートのみがアドバタイズされ、SD-WAN オーバーレイ内の適切なルーティング機能のために正しいコミュニティでタグ付けされます。

iv.　[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。

WMA ブランチ（スポーク 2）：eBGP および iBGP 相互ルート再配布の設定

WMA は eBGP を使用するため、LAN 側（eBGP）と SD-WAN オーバーレイ（iBGP）間のルート再配布を手動で設定する必要はありません。Threat Defense デバイスは、eBGP と iBGP 間のルートを自動的に再配布します。これにより、eBGP を使用したブランチの設定プロセスが簡素化されます。

NCT ブランチ（スポーク 3）：OSPF および iBGP 相互ルート再配布の設定

NCT（スポーク）の IPv4 プレフィックスリストの設定

ステップ 1.　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2.　**[プレフィックスリスト（Prefix List）] > [IPv4プレフィックスリスト（IPv4 Prefix List）]** を選択します。

ステップ 3.　[IPv4プレフィックスリストの追加（Add IPv4 Prefix List）] をクリックします。

ステップ 4.　[名前（Name）] フィールドに、**NCT-inside-10.73.0.0-16** と入力します。

ステップ 5.　[追加（Add）] をクリックします。

[プレフィックス リスト エントリの追加（Add Prefix List Entry）] ダイアログボックスが表示されます。次の設定を行えます。

- **アクション**：許可
- **シーケンス番号**：10
- **IPアドレス**：10.73.0.0/16

ステップ 6.　[追加（Add）] をクリックします。

ステップ 7.　[保存（Save）] をクリックします。

NCT（スポーク）のルートマップオブジェクトの追加

OSPF から iBGP へのルートマップを設定します。

ステップ 1.　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2.　[ルートマップ（Route Map）] をクリックします。

ステップ 3.　[ルート マップの追加（Add Route Map）] をクリックします。

ステップ 4.　[名前（Name）] フィールドに、**OSPF2iBGP-rdist-rmap** と入力します。

ステップ 5.　[追加（Add）] をクリックします。

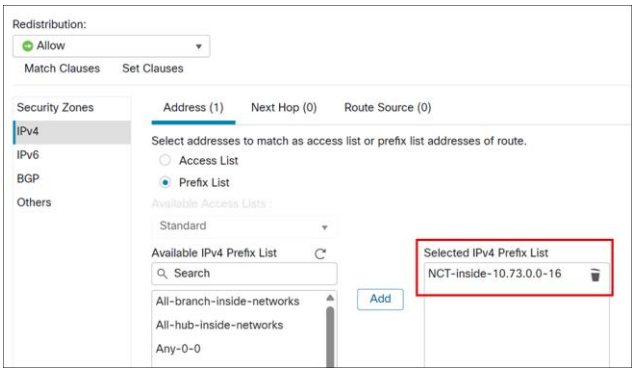
ステップ 6.　[シーケンス番号（Sequence No.）] フィールドに数値を入力します。この例では、**10** と入力します。

ステップ 7.　[再配布（Redistribution）] ドロップダウンリストから、再配布アクセスを示す [許可（Allow）] アクションを選択します。

ステップ 8.　[IPv4] をクリックします。

i.　[アドレス（Address）] タブをクリックします。

ii.　ドロップダウンリストから [プレフィックスリスト（Prefix List）] を選択し、照合に使用するプレフィックス リスト オブジェクトを入力または選択します。この例では、**NCT-inside-10.73.0.0-16** を選択します。



iii. [追加（Add）] をクリックします。

ステップ 9. [保存（Save）] をクリックします。

NCT（スポーク）のルートマップオブジェクトの追加

SD-WAN からブランチの LAN 側へのルートマップを設定します。

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. [ルートマップ（Route Map）] をクリックします。

ステップ 3. [ルート マップの追加（Add Route Map）] をクリックします。

ステップ 4. [名前（Name）] フィールドに、**Branch-SDWAN2LAN-rdist-map** と入力します。

ステップ 5. [追加（Add）] をクリックします。

ステップ 6. [シーケンス番号（Sequence No.）] フィールドに数値を入力します。この例では、**10** と入力します。

ステップ 7. [再配布（Redistribution）] ドロップダウンリストから、再配布アクセスを示す [許可（Allow）] アクションを選択します。

ステップ 8. [追加（Add）] をクリックします。

ステップ 9. [保存（Save）] をクリックします。

スポークの OSPF および iBGP 相互ルート再配布の設定（NCT-FW-HA）

トポロジ内のスポークサイトである NCT の設定では、LAN 側の OSPF ルーティングが SD-WAN オーバーレイの BGP ルーティングと統合され、ネットワーク全体のエンドツーエンドの IP 到達可能性が確保されます。

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. デバイスリストページから **NCT-FW-HA** 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. [一般設定（General Settings）] で [BGP] をクリックします。

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て、BGP ルーティングプロセスを有効にします。

ステップ 6. [AS番号（AS Number）] フィールドに、自律システム番号を入力し、[保存（Save）] をクリックします。この例の AS 番号は **65070** です。

ステップ 7. [BGP] > [IPv4] を選択します。

i. [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。

ii. [再配布（Redistribution）] タブをクリックします。再配布設定により、別のルーティング ドメインから BGP にルートを再配布する条件を定義できます。

iii. [追加（Add）] をクリックします。

iv. [再配布の追加（Add Redistribution）] ダイアログボックスで、以下のパラメータを設定します。

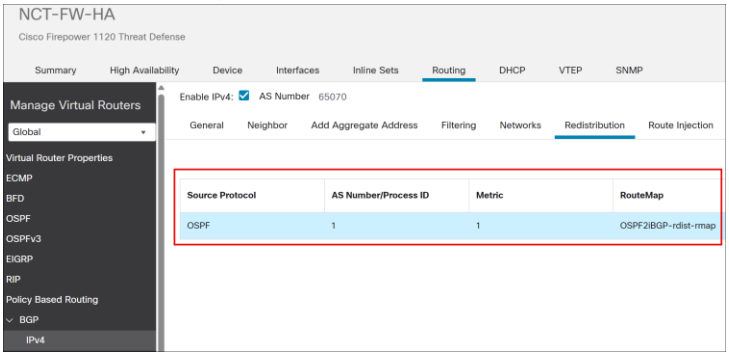
v. [送信元プロトコル（Source Protocol）] ドロップダウンリストで、BGP ドメインにルートを再配布する元となるプロトコルを選択します。この例では、**OSPF** を選択します。

vi. [メトリック（Metric）] フィールドに、再配布されるルートのメトリックを入力します。この例の値は **1** です。

vii. [ルートマップ（Route Map）] ドロップダウンリストで、再配布するネットワークをフィルタリングするために調べる必要のあるルートマップを選択します。この値を指定しない場合、すべてのネットワークが再配布されます。**OSPF2iBGP-rdist-map** が選択されています。これにより、必要なルートのみがアドバタイズされ、SD-WAN オーバーレイ内の適切なルーティング機能のために正しいコミュニティでタグ付けされます。

viii. [OK] をクリックします。

図 8.　　ルーティングの設定



ステップ 8. [保存（Save）] をクリックします。

ステップ 9. [OSPF] をクリックします。

ステップ 10. BGP を介して（SD-WAN オーバーレイから）学習したルートを、NCT デバイスの LAN 側の OSPF ドメインに再配布しています。

ステップ 11. [Redistribution] をクリックします。

ステップ 12. [追加（Add）] をクリックします。

ステップ 13. [再配布の追加（Add Redistribution）] ダイアログボックスで、以下のパラメータを設定します。

i. [OSPFプロセス（OSPF Process）] ドロップダウンリストから、プロセス ID に 1 を選択します。仮想ルーティングを使用するデバイスの場合、このドロップダウンリストに選択した仮想ルータ用に生成された一意のプロセス ID が表示されます。

ii. [ルートタイプ（Route Type）] ドロップダウンリストから、[BGP] を選択します。これにより、BGP ルーティングプロセスからルートが再配布されます。

iii. [AS番号（AS Number）] フィールドに AS 番号を入力します。

iv. （オプション）[サブネットを使用（Use Subnets）] チェックボックスをオンにします。

v. [サブネットを使用（Use Subnets）] チェックボックスをオンにします。

vi. [メトリック値（Metric Value）] : 再配布するルートのメトリック値。この例の値は、**1** です。

vii. [メトリックタイプ（Metric Type）] フィールドでは、OSPF の場合、メトリックタイプ 1 および 2 によって、外部ルート（他のルーティングプロトコルから再配布されたもの）が OSPF ドメイン内でアドバタイズされる方法が決まります。タイプ 1 メトリックでは、自律システム境界ルータ（ASBR）に到達するための内部 OSPF コストが外部コストに追加され、より正確なエンドツーエンドのパスコストが提供されます。タイプ 2 メトリックでは、ASBR への内部コストは無視され、外部コストのみが使用されます。この例では、メトリックタイプ **1** を選択しています。

viii. [ルートマップ（RouteMap）] ドロップダウンリストで、ルートマップを入力または選択します。これは、送信元ルーティングプロトコルから現在のルーティングプロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。**Branch-SDWAN2LAN-rdist-map** を選択します。

ix. [OK] をクリックします。

ステップ 14. [保存（Save）] をクリックします。

MCT ブランチ（スポーク 4）：EIGRP および iBGP 相互再配布の設定

MCT（スポーク）のルートマップオブジェクトの追加

SD-WAN からブランチの LAN 側へのルートマップを設定します。

ステップ 1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. [ルートマップ（Route Map）] をクリックします。

ステップ 3. [ルート マップの追加（Add Route Map）] をクリックします。

ステップ 4. [名前（Name）] フィールドに、**EIGRP2iBGP-rdist-rmap** と入力します。

ステップ 5. [追加（Add）] をクリックします。

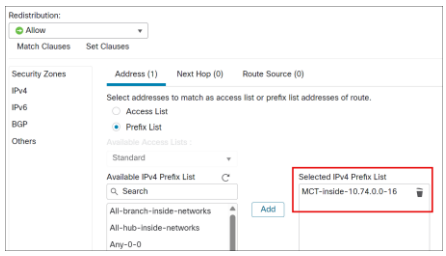
ステップ 6. [シーケンス番号（Sequence No.）] フィールドに数値を入力します。この例では、**10** と入力します。

ステップ 7. [再配布（Redistribution）] ドロップダウンリストから、再配布アクセスを示す [許可（Allow）] アクションを選択します。

ステップ 8. [IPv4] をクリックします。

i. [アドレス（Address）] タブをクリックします。

ii. ドロップダウンリストから [プレフィックスリスト（Prefix List）] を選択し、照合に使用するプレフィックス リスト オブジェクトを入力または選択します。この例では、**MCT-inside-10.74.0.0-16** を選択します。



iii. [追加（Add）] をクリックします。

ステップ 9. [保存（Save）] をクリックします。

スポークの **EIGRP** および **iBGP** 相互ルート再配布の設定（**MCT-FW-01**）

トポロジ内のスポークサイトである MCT ブランチ（スポーク 4）の設定では、LAN 側の EIGRP ルーティングが SD-WAN オーバーレイの iBGP ルーティングと統合され、ネットワーク全体のエンドツーエンドの IP 到達可能性が確保されます。

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. デバイスリストページから **MCT-FW-01** 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. [一般設定（General Settings）] で [BGP] をクリックします。

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て、**BGP** ルーティングプロセスを有効にします。

ステップ 6. [AS番号（AS Number）] フィールドに、自律システム番号を入力し、[保存（Save）] をクリックします。

この例では、**65070** です。

ステップ 7. [保存（Save）] をクリックします。

ステップ 8. [BGP] > [IPv4] を選択します。

ステップ 9. [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 10. [再配布（Redistribution）] タブをクリックします。再配布設定により、別のルーティング ドメインから BGP にルートを再配布する条件を定義できます。

ステップ 11. [追加（Add）] をクリックして、[再配布の追加（Add Redistribution）] ダイアログを更新します。

i. [送信元プロトコル（Source Protocol）] ドロップダウンリストで、BGP ドメインにルートを再配布する元となるプロトコルを選択します。この例では、**EIGRP** を選択します。

ii. [AS番号（AS Number）] フィールドに AS 番号を入力します。ここでの **AS 番号**は EIGRP AS 番号（BGP ではありません）を指し、設定された EIGRP AS 番号と一致する必要があります。この例では、EIGRP AS 番号は **74** です。

iii. [メトリックタイプ（Metric Type）] フィールドに、再配布されるルートのメトリックを入力します。この例の値は **1** です。

iv. [ルートマップ（RouteMap）] ドロップダウンリストから、再配布するネットワークをフィルタリングするために調べる必要のあるルートマップを選択します。この値を指定しない場合、すべてのネットワークが再配布されます。EIGRP2iBGP-rdist-map が選択されています。これにより、必要なルートのみがアドバタイズされ、SD-WAN オーバーレイ内の適切なルーティング機能のために正しいコミュニティでタグ付けされます。

v. [OK] をクリックします。

ステップ 12. [保存（Save）] をクリックします。

ステップ 13. [EIGRP] をクリックします。BGP を介して（SD-WAN オーバーレイから）学習したルートを、MCT デバイスの LAN 側の EIGRP ドメインに再配布しています。

i. [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。

ii. [AS番号（AS Number）] フィールドに、**74** を指定します。

iii. [使用可能なネットワーク（Available Networks）] リストから、**MCT-inside-if-subnet** ネットワークを選択します。（ネットワークオブジェクトを作成し、値 10.74.254.0/24 を割り当てます）。

iv. [Redistribution] をクリックします。

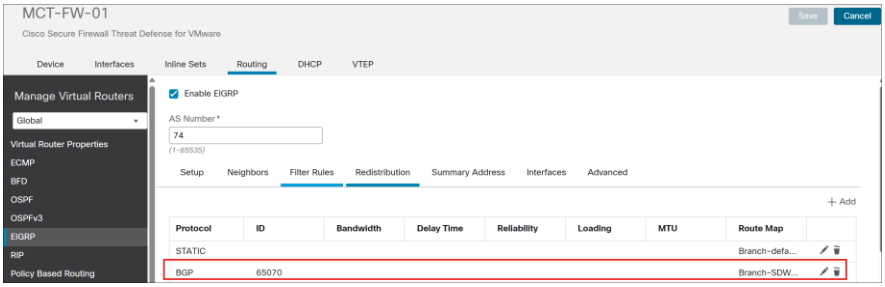
v. [再配布の追加（Add Redistribution）] ダイアログボックスの [プロトコル（Protocol）] ドロップダウンから、ルートが再配布される送信元プロトコルとして [BGP] を選択します。

vi. [プロセスID（Process ID）] フィールドに、プロセス ID **65070** を入力します。

vii. [ルートマップ（RouteMap）] ドロップダウンリストで、ルートマップを入力または選択します。この例では、ルートマップとして **Branch-SDWAN2LAN-rdist-rmap** を選択します。

viii. [OK] をクリックします。

図 9.　再配布の追加



ステップ 14.　[保存（Save）] をクリックします。

デバイスに設定を導入

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。

ステップ 2.　設定の変更をすべてのデバイスに展開する場合は、[すべて展開（Deploy All）] をオンにします。

NNJ-FW-HA（ハブ）のルーティングテーブルの確認

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

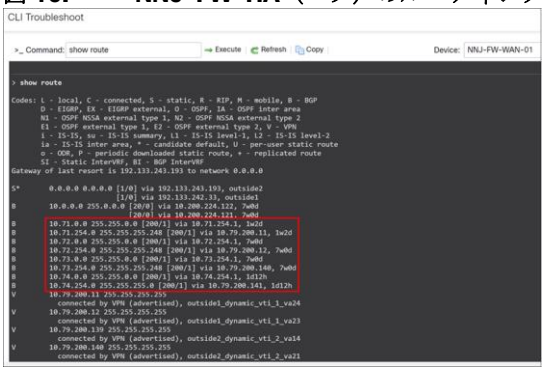
ステップ 2.　デバイスリストページから **NNJ-FW-HA** をクリックします。

ステップ 3.　[デバイス（Device）] タブをクリックします。

ステップ 4.　[全般（General）] エリアで、[CLI] をクリックし、次の手順を実行します。

```
> show route
```

図 10.　NNJ-FW-HA（ハブ）のルーティング情報



個々のサブネット 10.71.0.0、10.72.0.0、10.73.0.0、10.74.0.0 は、それぞれ PRI、WMA、NCT、MCT のリモートブランチに対応します。

MCT-FW-01 デバイスのルーティングテーブルの確認

完全なエンドツーエンドの到達可能性を表示するには、次のようにして、MCT スポークデバイスのルーティングテーブルを調べます。

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

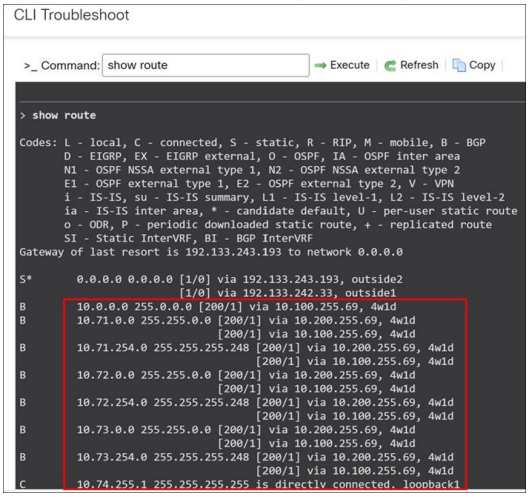
ステップ 2.　デバイスリストページから **MCT-FW-01** をクリックします。

ステップ 3.　[デバイス（Device）] タブをクリックします。

ステップ 4.　[全般（General）] エリアで、[CLI] をクリックし、次の手順を実行します。

```
> show route
```

図 11.　MCT-FW-01（スポーク）のルーティング情報

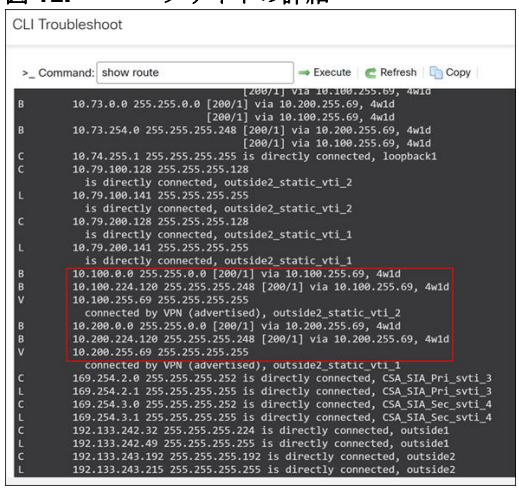


ここで、10.0.0.0 255.0.0.0 は、ハブサイト（ニューヨーク市およびニュージャージー）の LAN 側からアドバタイズされた集約ルートを表しています。

個々のサブネット 10.71.0.0、10.72.0.0、10.73.0.0 は、それぞれ PRI、WMA、NCT のリモートブランチに対応します。

下にスクロールして、ハブサイトからの LAN サブネットの詳細を表示します。

図 12.　　ハブサイトの詳細



ハブサイトからの特定の LAN サブネットは、ニューヨーク（NYC）の場合は 10.100.0.0/16、ニュージャージー（NNJ）の場合は 10.200.0.0/16 です。

完全なルーティングテーブルは、ネットワーク全体でエンドツーエンドの到達可能性を実現するために不可欠です。この広範囲に及ぶルーティング情報により、スポークとハブ間だけでなく、スポークサイト間直接でのシームレスな通信が可能になります。

NCT-FW-HA デバイスのルーティングテーブルの確認

ステップ 1.　完全なエンドツーエンドの到達可能性を表示するには、次のようにして、MCT スポークデバイスのルーティングテーブルを調べます。

ステップ 2.　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

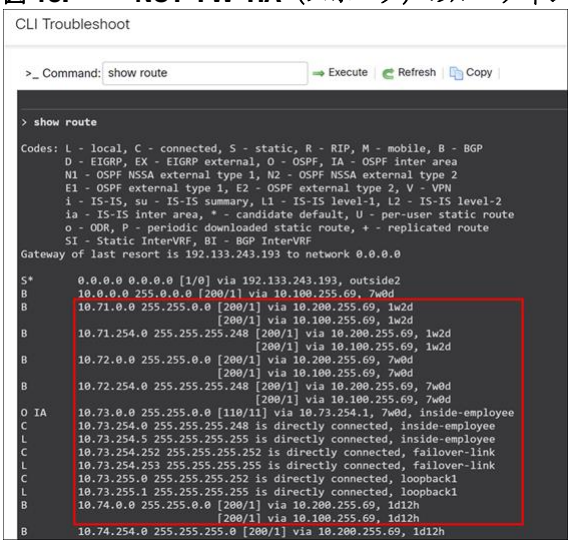
ステップ 3.　デバイスリストページから **NCT-FW-HA** をクリックします。

ステップ 4.　[デバイス（Device）] タブをクリックします。

ステップ 5.　[全般（General）] エリアで、[CLI] をクリックし、次の手順を実行します。

```
> show route
```

図 13.　　NCT-FW-HA（スポーク）のルーティング情報



PRI-FW-01 デバイスのルーティングテーブルの確認

完全なエンドツーエンドの到達可能性を表示するには、次のようにして、MCT スポークデバイスのルーティングテーブルを調べます。

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

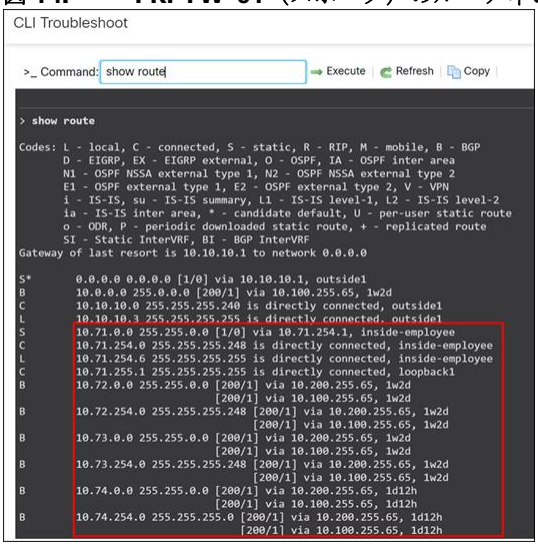
ステップ 2.　デバイスリストページから **PRI-FW-01** をクリックします。

ステップ 3.　[デバイス（Device）] タブをクリックします。

ステップ 4.　[全般（General）] エリアで、[CLI] をクリックし、次の手順を実行します。

```
> show route
```

図 14.　　PRI-FW-01（スポーク）のルーティング情報



WMA-FW-01 デバイスのルーティングテーブルの確認

完全なエンドツーエンドの到達可能性を表示するには、次のようにして、MCT スポークデバイスのルーティングテーブルを調べます。

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

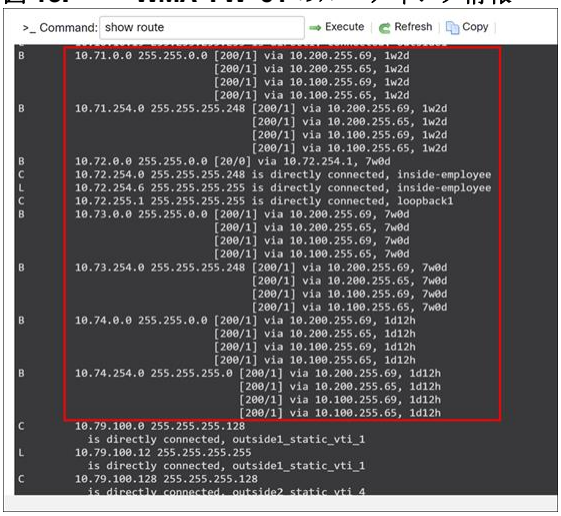
ステップ 2.　デバイスリストページから **WMA-FW-01** をクリックします。

ステップ 3.　[デバイス（Device）] タブをクリックします。

ステップ 4.　[全般（General）] エリアで、[CLI] をクリックし、次の手順を実行します。

```
> show route
```

図 15.　WMA-FW-01 のルーティング情報



SD-WAN 設計およびその他のユースケースの詳細については、『Cisco Secure Firewall Threat Defense SD-WAN 設計および展開ガイド』を参照してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

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。