SD-WAN の機能

この章では、Management Center でサポートされている SD-WAN 機能について説明します。

SD-WAN の機能

ソフトウェア定義型 WAN（SD-WAN）ソリューションは、従来の WAN ルータに代わるものであり、WAN トランスポートテクノロジーに依存しません。SD-WAN は、複数の WAN 接続で動的なポリシーベースのアプリケーションパス選択を提供し、WAN最適化やファイアウォールなどの追加サービスに向けてサービスチェーンをサポートします。

組織が複数のブランチロケーションに業務を拡大するにつれて、セキュアで合理化された接続を確保することが最優先されるようになります。セキュアなブランチ ネットワーク インフラストラクチャを展開するには、複雑な設定が必要です。これには時間がかかり、適切に処理しないと設定エラーが発生しやすくなります。ただし、組織は、Cisco Secure Firewall Management Center（Management Center）と Cisco Secure Firewall Threat Defense（Threat Defense）デバイスを活用して、簡素化された安全なブランチ展開を実現することで、これらの課題を克服できます。

このガイドでは、堅牢なファイアウォール ソリューションを使用した、セキュアなブランチ展開の簡素化の概念について説明します。セキュアなファイアウォールをブランチ ネットワーク アーキテクチャの基本コンポーネントとして統合することで、組織は展開プロセスを簡素化しながら、強力なセキュリティベースラインを確立することができます。このアプローチにより、組織は統合されたセキュリティポリシーを適用し、トラフィックルーティングを最適化し、復元力のある接続を確保することができます。

Cisco Secure Firewall でサポートされている SD-WAN 機能の一部は以下のとおりです。

- **シンプルな管理**：
  - SD-WAN ウィザード

- SASE：Cisco Umbrella 自動トンネルの展開
- ダイナミック VTI（DVTI）ハブスポークトポロジの簡素化

- **アプリケーション認識**：
  - パブリッククラウドおよびゲストユーザーのダイレクト インターネット アクセス（DIA）
  - 一致基準としてアプリケーションを使用したポリシーベースルーティング（PBR）
  - Cisco Umbrella のためのローカルトンネル ID のサポート

- **使用可能帯域幅の増加**：
  - 複数の ISP と VTI にまたがるロードバランシングのための ECMP のサポート
  - PBR を使用したアプリケーションベースのロードバランシング

- **ネットワークのダウンタイムがほぼゼロの高可用性**：
  - デュアル ISP 設定
  - アプリケーションベースのインターフェイス モニタリングに基づく最適なパス選択

- **セキュアで柔軟な接続**：
  - 本社（ハブ）とブランチ（スポーク）の間のルートベース（VTI）VPN トンネル
  - VTI を介した IPv4 および IPv6 BGP、IPv4 および IPv6 OSPF、IPv4 EIGRP
  - スタティックまたはダイナミック IP を持つスポークをサポートする DVTI ハブ

機能

以下の表に、一般的に使用される SD-WAN 機能の一部を示します

機能	リリース 15.4 で	詳細情報
SD-WAN ウィザード	リリース 7.6	SD-WAN ウィザードを使用したセキュアなブランチネットワークの展開 （4 ページ）
Cisco SD-WAN サマリーダッシュボードを使用したアプリケーション モニタリング	リリース 7.4.1	Cisco SD-WAN サマリーダッシュボード
Cisco SD-WAN サマリーダッシュボード	リリース 7.4	Cisco SD-WAN サマリーダッシュボード

機能	リリース 15.4 で	詳細情報
ユーザーアイデンティティと SGT を使用したポリシーベースのルーティング	リリース 7.4	ポリシーベースルーティング
HTTP パスのモニタリングを使用したポリシーベースのルーティング。	リリース 7.4	ポリシーベースルーティング
VTI のループバック インターフェイス サポート	リリース 7.3	ループバック インターフェイスについて
サイト間 VPN を使用したダイナミック VTI（DVTI）のサポート	リリース 7.3	Dynamic VTI
Cisco Umbrella 自動トンネル	リリース 7.3	Umbrella に SASE トンネルを展開する
VTI の IPv4 および IPv6 BGP、IPv4 および IPv6 OSPF、IPv4 EIGRP のサポート	リリース 7.3	BGP Open Shortest Path First（OSPF） EIGRP
ハブアンドスポークトポロジを使用したルートベースのサイト間 VPN	リリース 7.2	ルートベースのサイト間 VPN の作成
パスのモニタリングによるポリシーベースのルーティング	リリース 7.2	ポリシーベースルーティング
サイト間 VPN 監視ダッシュボード	リリース 7.1	サイト間 VPN のモニタリング
ダイレクト インターネット アクセス/ポリシーベースルーティング	リリース 7.1	ポリシーベースルーティング
WAN インターフェイスを使用した Equal-Cost-Multi-Path（ECMP）ゾーン	リリース 7.1	ECMP
VTI インターフェイスを使用した ECMP ゾーン	リリース 7.1	ECMP

機能	リリース 15.4 で	詳細情報
ルートベースのサイト間VPN向けバックアップ用 VTI	リリース 7.0	バックアップ VTI トンネルを介したトラフィックのルーティング
サイト間 VPN を使用したスタティック VTI（SVTI）のサポート	リリース 6.7	スタティック VTI

SD-WAN ウィザードを使用したセキュアなブランチネットワークの展開

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。

ハブとスポークとは

ハブ：1つ以上のリモートブランチデバイスまたはスポークとの間でセキュアなVPN接続を可能にするデバイスです。ハブは、スポーク同士が相互通信するためのゲートウェイとしても機能します。

スポーク：VPNを介してハブに接続し、ハブの背後にある企業リソースにセキュアにアクセスするリモートブランチ上のデバイスです。スポーク同士は、ハブを介して相互に通信します。

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 ウィザードの使用に関するガイドラインと制限事項

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。
- デュアルハブ SD-WAN トポロジでは、ハブを異なる地理的場所に配置し、その背後に異なる保護されたネットワークを配置できます。これらのネットワーク間の直接通信を確立するには、以下を設定してください。
  - 2 つのハブ間のポイントツーポイント ルートベース VPN トポロジ（[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）]）。
  - ハブ間のダイナミック ルーティング プロトコル（[デバイス（Device）] > [デバイス管理（Device Management）] > [ルーティング（Routing）]）。
- スポークの IP アドレスプールを設定する場合は、以下のことを確認してください。
  - [オーバーライドを許可（Allow Overrides）] チェックボックスをオフにする必要があります。
  - 複数のプールを使用している場合は、プールの IP アドレスが重複しないようにする必要があります。
  - IP アドレスは、スポーク上のどのインターフェイスとも重複してはなりません。
- 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。
- アプリケーション トラフィックのロード バランシングを行うために、ECMP ゾーンでスポークのスタティック VTI を設定します。ECMP ゾーンを設定しない場合、残りのパスは、プライマリパスがダウンしたときにバックアップパスとして機能します。ECMP ゾー

ンの物理インターフェイスではなく、スポークのスタティック VTI を設定する必要があることに注意してください。この設定は、SD-WAN ウィザードの一部ではありません。

- スポークのデュアル ISP を使用する SD-WAN トポロジでは、スポークのトンネルアイデンティティとトンネル送信元は一意である必要があります。
- スポークが複数の SD-WAN トポロジの一部である場合は、各 SD-WAN トポロジで同じローカルコミュニティ タグと学習したルート コミュニティ タグを使用していることを確認してください。ローカル コミュニティ タグと学習済みルート コミュニティ タグは互いに異なっている必要があることに注意してください。
- 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 アイデンティティを設定します。
- SD-WAN トポロジのスポークが同じ保護対象ネットワークに属していないことを確認します。

制限事項

- 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。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。詳細については、「SD-WAN ウィザードを使用したデュアル ISP 展開の構成例 （13 ページ）」を参照してください。
- SD-WAN ウィザードは、以下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。

SD-WAN ウィザードの使用に関する前提条件

- Firewall 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。

  Firewall Management Center でこの機能を確認するには、**[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]** の順に選択します。
- 管理者ユーザー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。
- Firewall Threat Defense デバイスには、インターネットでルーティング可能なパブリック IP アドレスが必要です。IP アドレスは、静的またはダイナミックのいずれかです。
- Firewall Threat Defense デバイスのインターフェイスに、適切な論理名とIPアドレスを割り当てます。たとえば、LANに接続されたインターフェイスには*inside*を使用し、インターネットまたは WAN に接続されたインターフェイスには *outside* を使用します。
- 証明書ベースの認証を使用している場合は、ハブとスポークに証明書を登録する必要があります。
- ルーティング、NAT、AC ポリシーを設定して、デバイス間のアンダーレイ接続を確保します。

SD-WAN ウィザードを使用した SD-WAN トポロジの設定

SD-WAN ウィザードを使用すると、中央の本社とリモートのブランチサイト間の VPN トンネルを簡単に設定できます。

始める前に

必ずSD-WAN ウィザードの使用に関する前提条件 （6 ページ）およびSD-WAN ウィザードの使用に関するガイドラインと制限事項 （5 ページ）を確認してください。

手順

ステップ 1 **Devices** > **VPN** > **Site to Site** を選択し、**[追加（Add）]** をクリックします。

ステップ 2 [トポロジ名（Topology Name）] フィールドに、SD-WAN VPN トポロジの名前を入力します。

ステップ 3 [SD-WANトポロジ（SD-WAN Topology）]ボタンをクリックして、[作成（Create] をクリックします。

ステップ 4 ハブを設定します。

a) [ハブの追加（Add Hub）] をクリックします。

b) [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。

c) [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、ハブのダイナミック 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にデフォルト設定が入力されます。ただし、[トンネル送信元（Tunnel Source）] と [IPアドレスの借用（Borrow IP Address）] を設定する必要があります。詳細については、Hub のダイナミック仮想トンネルインターフェイスの追加 （12 ページ）を参照してください。

d) [OK] をクリックします。

e) [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。

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。

f) [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。

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。

g) [追加] をクリックしてハブの設定を保存します。
h) （任意）セカンダリハブを追加するには、ステップ 4a ～ 4f を繰り返します。
i) [次へ（Next）] をクリックします。

ステップ 5 スポークを設定します。

[スポークの追加（Add Spoke）] をクリックして単一のスポークデバイスを追加するか、[スポークの追加（一括追加）（Add Spokes (Bulk Addition)）] をクリックしてトポロジに複数のスポークを追加します。

- [スポークの追加（Add Spoke）] をクリックします。[スポークの追加（Add Spoke）] ダイアログボックスで、次のパラメータを設定します。

  1. [デバイス（Device）] ドロップダウンリストからスポークを選択します。
  2. [VPNインターフェイス（VPN Interface）] ドロップダウンリストから、WAN 側またはインターネット側の物理インターフェイスを選択して、ハブとの VPN 接続を確立します。
  3. [ローカルトンネル（IKE）アイデンティティ（Local Tunnel (IKE) Identity）] チェックボックスをオンにして、このデバイスからリモートピアへの VPN トンネルの一意で設定可能なアイデンティティを有効にします。デフォルトで、このオプションは有効になっています。
  4. [アイデンティティタイプ（Identity Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。
     - [キー識別子（Key ID）]：（デフォルト値）この値は、*<sd-wan topologyname>_<device_IP_address>* で自動入力されます（例：sdwantopo1_192.168.0.200）。任意のキー識別子を指定することもできます。
     - [電子メール識別子（Email ID）]：最大 127 文字の電子メール識別子を指定します。
     - [IPアドレス（IP Address）]：スポークの VPN インターフェイスの IP アドレス。

- [自動（Auto）]：事前共有キー認証の場合はスポークの VPN インターフェイスの IP アドレス、証明書ベースの認証の場合は証明書の識別名（DN）。
- [ホスト名（Hostname）]：スポークの完全修飾ホスト名。

5. [保存（Save）] をクリックして、スポークの設定を保存します。

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

1. 1 台以上のデバイスを [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。
2. 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。
   - [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）。

     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。
   - [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。
3. [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。
4. [追加（Add）] をクリックします。
5. [次へ（Next）] をクリックします。

スポークごとに、ウィザードはトンネルの送信元 IP アドレスとしてハブの DVTI を自動的に選択します。

（注）
ハブのトンネル送信元 IP アドレスが IPv6 アドレスの場合、ウィザードはスポークの選択済みインターフェイスの最初の IPv6 アドレスを自動的に選択します。スポークのトンネル送信元の IPv6 アドレス を編集するには、スポークの横の編集アイコンをクリックし、[IPアドレス（IP Address）] ドロップダウンリストから IPv6 アドレスを選択して [保存（Save）] をクリックします。

ステップ 6 SD-WAN トポロジ内のデバイスの認証設定を構成します。

a) [認証タイプ（Authentication Type）]：デバイス認証では、手動の事前共有キー、自動生成された事前共有キー、または証明書を使用できます。

- [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します。
d) [次へ（Next）] をクリックします。

ステップ 7 SD-WAN 設定を構成します。

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、ウィザードがスポークの自動生成された静的仮想トンネルインターフェイス（SVTI）を自動的に追加するセキュリティ ゾーンを作成します。
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。

   AS 番号は、単一のルーティングポリシーを持つネットワークの一意の番号です。BGP は AS 番号を使用してネットワークを識別します。スポークの BGP ネイバー設定は、対応するハブの AS 番号に基づいて生成されます。範囲は 0 ～ 65536 です。

   - すべてのハブとスポークが同じリージョン内にある場合、デフォルトで **64512** が AS 番号となります。
   - プライマリハブとセカンダリハブのリージョンが異なる場合、プライマリハブとスポークの AS 番号は **64512** に設定され、セカンダリハブには異なる AS 番号が設定されます。

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。

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。

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。

このオプションを有効にすると、BGP マルチパスはスポークに対してのみ有効になります。

g) （任意）[セカンダリハブが別の自律システムにある（Secondary Hub is in Different Autonomous System）] チェックボックスをオンにします。このチェックボックスは、このトポロジにセカンダリハブがある場合にのみ表示されます。

h) [自立システム番号（Autonomous System Number）] フィールドに、セカンダリハブの AS 番号を入力します。

i) [学習ルートのコミュニティタグ（Community Tag for Learned Routes ）] フィールドに、BGP コミュニティ属性を入力して、VPN トンネルを介して他の SD-WAN ピアから学習したルートにタグを付けます。この属性は、セカンダリハブが別の AS 番号を持つ場合の eBGP 設定にのみ必要です。このフィールドは、SD-WAN トポロジで 2 つのハブを設定した場合にのみ表示されます。

j) [次へ（Next）] をクリックします。

ステップ 8 [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。

[サイト間VPN（Site-to-site VPN）] 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。

次のタスク

- 自動生成されたスポーク SVTI とその IP アドレスの表示：スポーク設定の横にある編集アイコンをクリックし、[生成されたトンネルインターフェイスの表示（View Generated Tunnel Interfaces）] をクリックします。
- スポーク SVTI で ECMP を有効にすることを推奨します。**[デバイス（Device）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [ECMP]** を選択します。
- ハブとスポークに設定を展開します。[展開（Deploy）] を選択します。デバイスを選択して、[展開（Deploy）] をクリックします。
- SD-WAN トポロジトンネルのステータスを確認します。詳細については、「SD-WAN トポロジのトンネルステータスの確認 （18 ページ）」を参照してください。
- スポークのトンネル インターフェイス セキュリティゾーンの ACL を設定します。[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

- ハブで BGP マルチパスを有効にすることを推奨します。ハブで BGP マルチパスを有効にするには、次の手順を実行します。
  1. **[デバイス（Device）] > [デバイス管理（Device Management）] > [ルーティング（Routing）]** を選択します。
  2. **[全般設定（General Settings）]** で **[BGP]** をクリックします。
  3. **[BGP の有効化（Enable BGP）]** チェック ボックスをオンにして、BGP を有効にします。
  4. **[AS番号（AS Number）]** フィールドに、SD-WAN トポロジで設定した AS 番号を入力します。
  5. [保存（Save）] をクリックします。
  6. 左側のペインで、**[BGP] > [IPv4] または [IPv6]** を選択し、 **[全般（General）**] タブをクリックします。
  7. **[多重パスでパケットを転送（Forward Packets over Multiple Paths）]** セクションで、編集アイコンをクリックします。
  8. **[パス数（Number of Paths）]** と **[IBGP パス数（IBGP number of paths）]**の値を設定します。これらの値は 8 に設定することを推奨します。

- SD-WAN ウィザードを使用した設定例について詳しくは、SD-WAN ウィザードを使用したデュアル ISP 展開の構成例 （13 ページ） を参照してください。
- WAN インターフェイスのアプリケーション パフォーマンス メトリックに基づいて、各スポークでアプリケーション認識型ルーティングのための PBR ポリシーを設定します。詳細は、「ダイレクト インターネット アクセス（DIA）を使用したブランチからインターネットへのアプリケーション トラフィックのルーティング」を参照してください。

Hub のダイナミック仮想トンネルインターフェイスの追加

SD-WAN ウィザードでは、ハブごとに DVTI を設定する必要があります。DVTI は仮想テンプレートを使用して、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。

始める前に

SD-WAN ウィザードで、[ハブの追加（Add Hub）] をクリックし、[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。

手順

ステップ 1 [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、ハブの DVTI 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。

1. [トンネルタイプ（Tunnel Type）] = [ダイナミック（Dynamic）]。
2. [名前（Name）] : <*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。
3. [有効（Enabled）] チェックボックス：デフォルトでオンになっています。
4. [テンプレートID（Template ID）] : DVTI の一意の ID。
5. [トンネルの送信元（Tunnel Source）] : 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。
6. [IPsecトンネルモード（IPsec Tunnel Mode）] : デフォルトでは IPv4 です。

ステップ 2 [セキュリティゾーン（Security Zone）] ドロップダウンリストから、ダイナミック VTI のセキュリティゾーンを選択します。

ステップ 3 [IPの借用（Borrow IP）] : ドロップダウンリストから物理インターフェイスまたは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 インターフェイスはこの IP アドレスを継承します。

トンネル送信元 IP アドレスとは異なる IP アドレスを使用していることを確認してください。ループバック IP アドレスを使用することを推奨します。

ステップ 4 [OK] をクリックして、ダイナミック VTI を保存します。

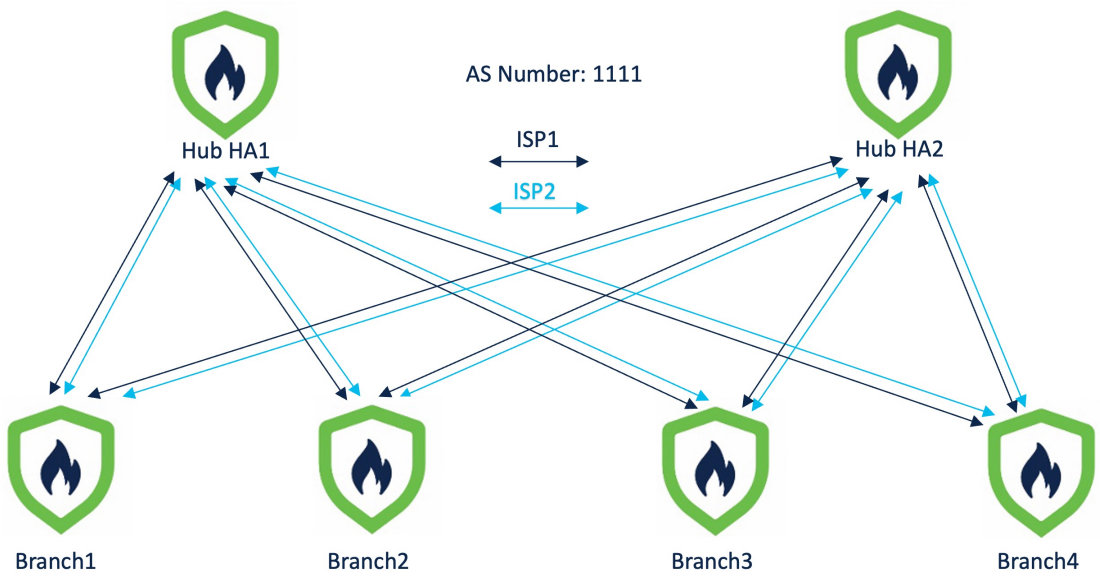
SD-WAN ウィザードを使用したデュアル ISP 展開の構成例

デュアル ISP 展開：同じリージョンの 2 つのハブと 4 つのスポーク

以下のデュアルISPトポロジでは、ハブとスポークは単一のリージョンにあり、AS番号は1111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。

- ハブ HA1 とハブ HA2 は、本社のハブ脅威防御デバイスです。
- Branch1、Branch2、Branch3、Branch4 は、ブランチのスポーク型脅威防御デバイスです。
- ISP1 は、ISP1 への各スポークの VPN インターフェイスです。
- ISP2 は、各スポークの ISP2 へのVPN インターフェイスです。

図 *1*：同じリージョン内に *2* つのハブと *4* つのスポークがあるデュアル *ISP* トポロジ



このトポロジを設定するには、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。

SD-WAN トポロジ 1

パラメータ	値
Primary Hub	ハブ HA1
セカンダリハブ	ハブ HA2
スポーク	Branch1、Branch2、Branch3、Branch4
AS 番号（AS Number）	1111
VPNインターフェイス（スポークトンネルソース）	ISP1
トンネル数	8

SD-WAN トポロジ 1 のトンネルの総数は 8 です。

SD-WAN トポロジ 2

パラメータ	値
Primary Hub	ハブ HA1
セカンダリハブ	ハブ HA2

パラメータ	値
スポーク	Branch1、Branch2、Branch3、Branch4
AS 番号（AS Number）	1111
VPNインターフェイス（スポークトンネルソース）	ISP2
トンネル数	8

SD-WAN トポロジ 2 のトンネルの総数は 8 です。

このデュアル ISP 展開の VPN トンネルの総数は 16 です。

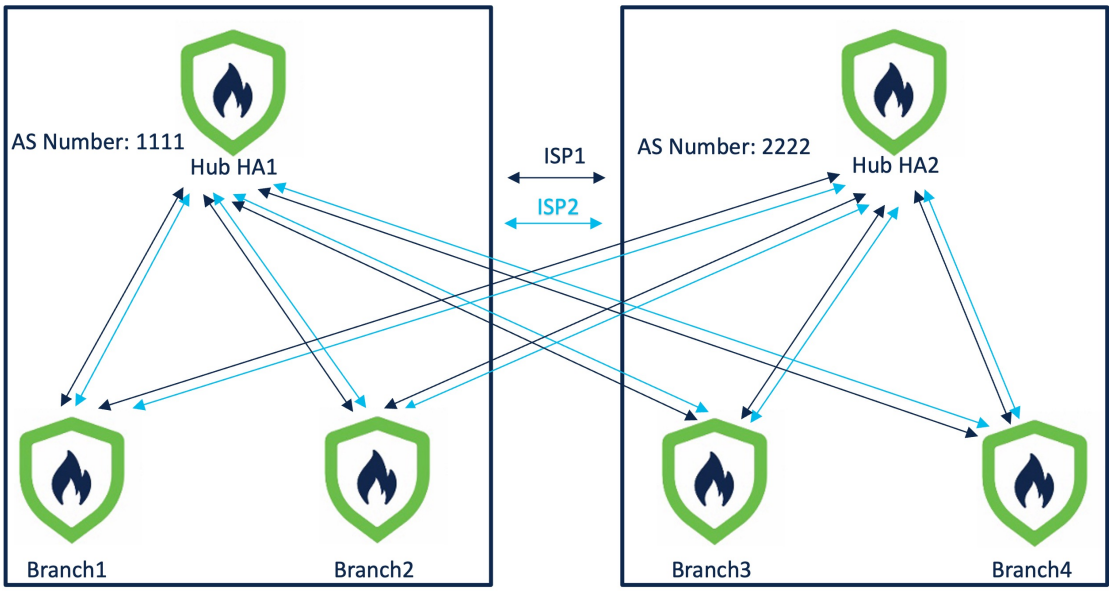
（注） ハブが地理的に異なる場所にあり、その背後に異なる保護されたネットワークがある場合、これらのネットワーク間の直接通信を確保するには、ルートベースの VPN ウィザードを使用して 2 つのハブ間にポイントツーポイント ルートベース VPN トポロジを設定します。

デュアル ISP 展開：異なるリージョンの 2 つのハブと 4 つのスポーク

以下のデュアル ISP トポロジでは、ハブは異なるリージョンにあり、それぞれに 2 つの直接接続されたスポークがあります。ハブと直接接続されたスポークは、ルーティングプロトコルとして内部ボーダー ゲートウェイ プロトコル（iBGP）を使用し、ハブは外部ボーダー 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します。

- ハブ HA1 とハブ HA2 は、本社のハブ脅威防御デバイスです。
- Branch1、Branch2、Branch3、Branch4 は、ブランチのスポーク型脅威防御デバイスです。
- HQ1、Branch1、Branch2 は、AS 番号が 1111 の単一リージョンにあります。
- HQ2、Branch3、Branch4 は、AS 番号が 2222 の単一リージョンにあります。
- ISP1 は、ISP1 への各スポークの VPN インターフェイスです。
- ISP2 は、各スポークの ISP2 へのVPN インターフェイスです。

図 *2*：異なるリージョンに *2* つのハブと *4* つのスポークがあるデュアル *ISP* トポロジ



このトポロジを設定するには、SD-WAN ウィザードを使用して次の 4 つの SD-WAN トポロジを作成する必要があります。

SD-WAN トポロジ 1

パラメータ	値
Primary Hub	ハブ HA1
セカンダリハブ	ハブ HA2
スポーク	Branch1、Branch2
AS 番号（AS Number）	1111
セカンダリ AS 番号	2222
VPNインターフェイス（スポークトンネルソース）	ISP1

SD-WAN トポロジ 1 のトンネルの数は 4 です。

SD-WAN トポロジ 2

パラメータ	値
Primary Hub	ハブ HA1
セカンダリハブ	ハブ HA2

パラメータ	値
スポーク	Branch1、Branch2
AS 番号（AS Number）	1111
セカンダリ AS 番号	2222
VPNインターフェイス（スポークトンネルソース）	ISP2

SD-WAN トポロジ 2 のトンネルの数は 4 です。

SD-WAN トポロジ 3

パラメータ	値
Primary Hub	ハブ HA2
セカンダリハブ	ハブ HA1
スポーク	Branch3、Branch4
AS 番号（AS Number）	2222
セカンダリ AS 番号	1111
VPNインターフェイス（スポークトンネルソース）	ISP1

SD-WAN トポロジ 3 のトンネルの数は 4 です。

SD-WAN トポロジ 4

パラメータ	値
Primary Hub	ハブ HA2
セカンダリハブ	ハブ HA1
スポーク	Branch3、Branch4
AS 番号（AS Number）	2222
セカンダリ AS 番号	1111
VPNインターフェイス（スポークトンネルソース）	ISP2

SD-WAN トポロジ 4 のトンネルの数は 4 です。

このデュアル ISP 展開の VPN トンネルの総数は 16 です。

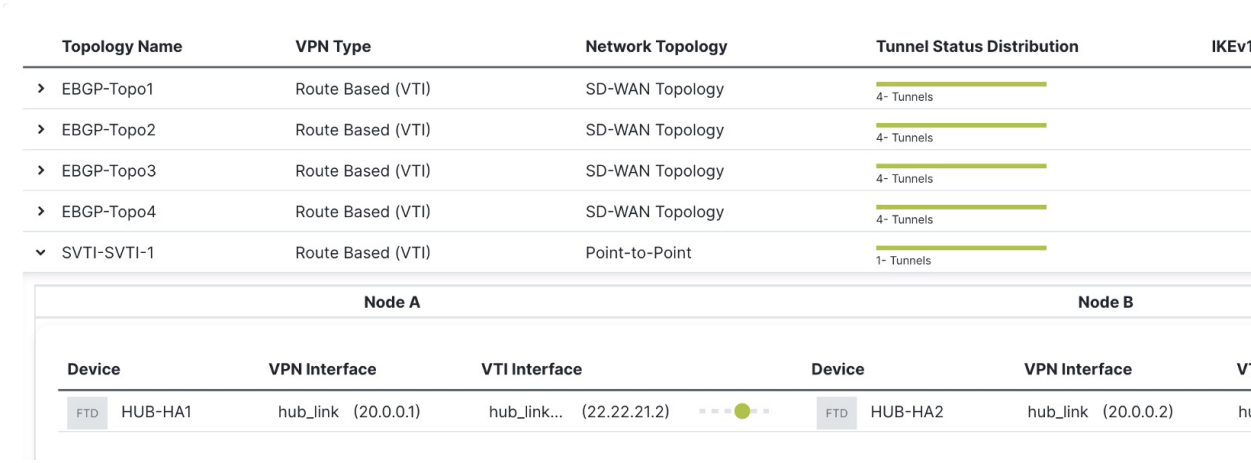
（注） ハブが地理的に異なる場所にあり、その背後に異なる保護されたネットワークがある場合、これらのネットワーク間の直接通信を確保するには、ルートベースの VPN ウィザードを使用して 2 つのハブ間にポイントツーポイント ルートベース VPN トポロジを設定します。

SD-WAN トポロジのトンネルステータスの確認

[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

SD-WAN トポロジの VPN トンネルが稼働しているかどうかを確認するには、[デバイス（Device）] > [VPN] > [サイト間（Site-to-Site）] の順に選択します。

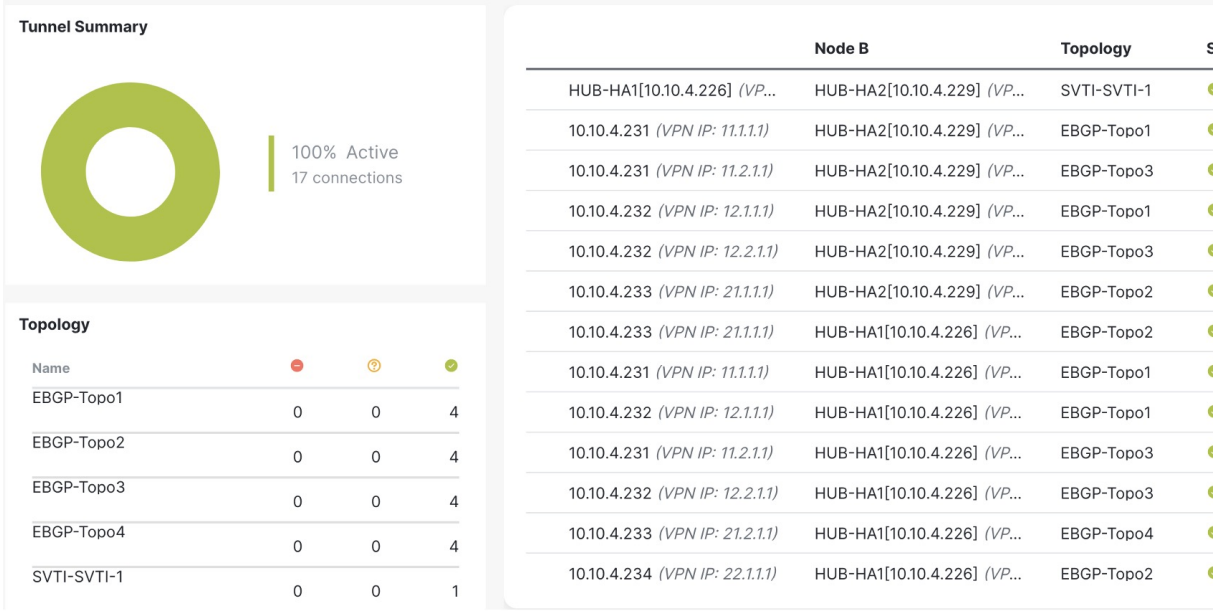
次に、2 つのハブと 4 つのスポークが異なるリージョンに配置され、デュアル ISP に接続された 5 つの SD-WAN トポロジを示します。



[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

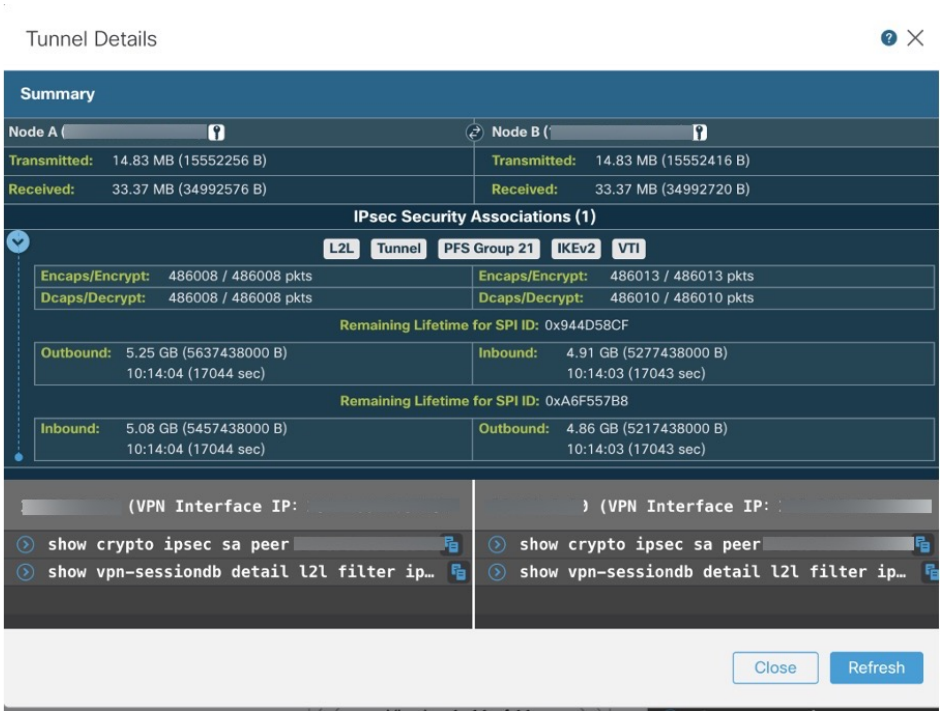
SD-WAN VPN トンネルの詳細を表示するには、[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site-to-site VPN）] の順に選択します。

次に、2 つのハブと 4 つのスポークが異なるリージョンに配置され、デュアル ISP に接続された SD-WAN トポロジの VPN トンネルを示します。



各 VPN トンネルの詳細を表示するには、以下の手順を実行します。

1. トンネルにカーソルを合わせます。
2. [すべての情報を表示（View Full Information）] アイコン（👁）をクリックします。トンネルの詳細とその他のアクションを含むペインが表示されます。
3. IPsec セキュリティ アソシエーションの show コマンドと詳細を表示するには、サイド ペインの [CLIの詳細（CLI Details）] タブをクリックします。



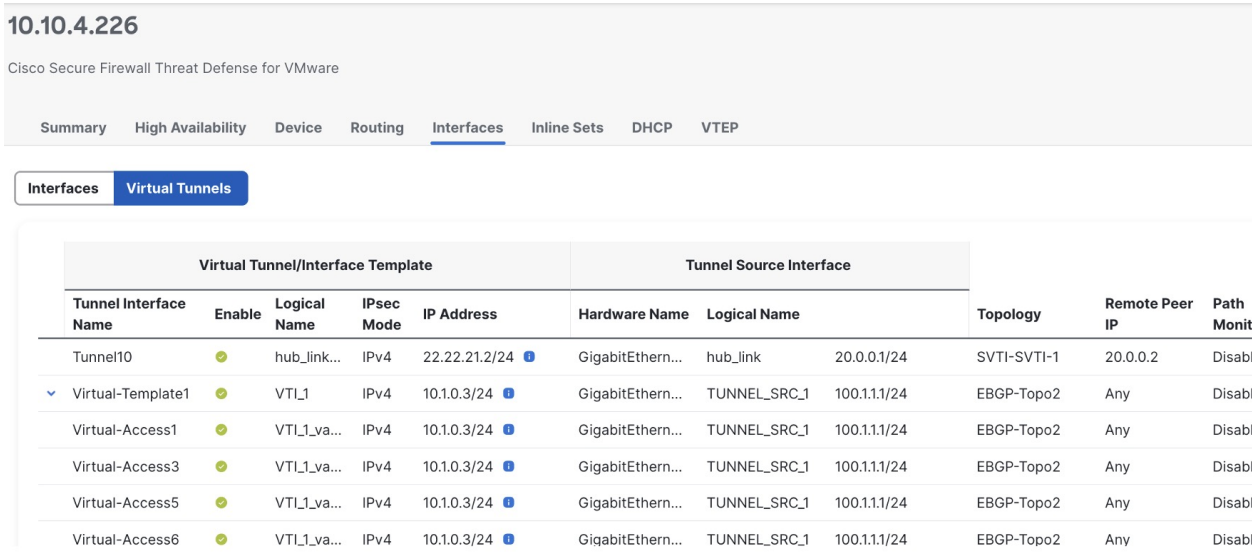
デバイスの仮想トンネルインターフェイスの表示

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。

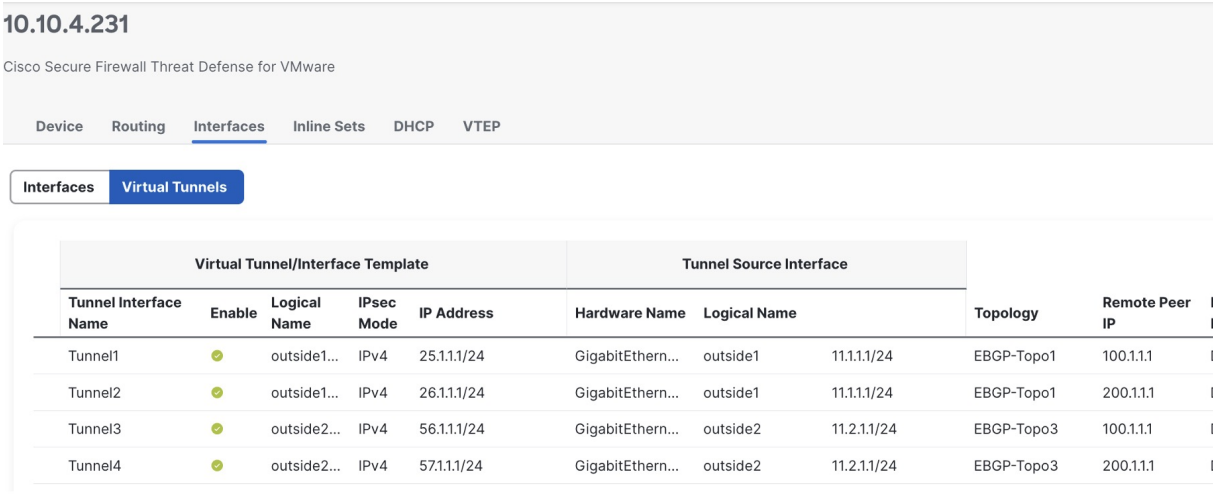
1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
2. ハブまたはスポークデバイスの編集アイコンをクリックします。
3. [インターフェイス（Interface）] タブをクリックします。
4. [仮想トンネル（Virtual Tunnels）] タブをクリックします。

   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。

次の図は、ハブの DVTI によってダイナミックに作成された仮想アクセスインターフェイスの例を示しています。



次の図は、SD-WAN ウィザードによってスポークに作成された静的トンネル仮想インターフェイス（SVTI）の例を示しています。



Virtual Tunnel/Interface Template					Tunnel Source Interface				
Tunnel Interface Name	Enable	Logical Name	IPsec Mode	IP Address	Hardware Name	Logical Name		Topology	Remote Peer IP
Tunnel1	✓	outside1...	IPv4	25.1.1.1/24	GigabitEthern...	outside1	11.1.1.1/24	EBGP-Topo1	100.1.1.1
Tunnel2	✓	outside1...	IPv4	26.1.1.1/24	GigabitEthern...	outside1	11.1.1.1/24	EBGP-Topo1	200.1.1.1
Tunnel3	✓	outside2...	IPv4	56.1.1.1/24	GigabitEthern...	outside2	11.2.1.1/24	EBGP-Topo3	100.1.1.1
Tunnel4	✓	outside2...	IPv4	57.1.1.1/24	GigabitEthern...	outside2	11.2.1.1/24	EBGP-Topo3	200.1.1.1

SD-WAN ウィザードは、ハブの IP アドレスプールからこれらのトンネルインターフェイスに IP アドレスを割り当てます。

ハブとブランチでのルーティングの確認

SD-WAN トポロジのハブとスポークの BGP 構成を確認するには、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. ハブまたはスポークデバイスの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）] フィールドに次のコマンドを入力し、[実行（Execute）] をクリックします。
   - **show route**
   - **show bgp summary**

SD-WAN 機能のユースケース

- 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
- ダイレクト インターネット アクセス（DIA）を使用したブランチからインターネットへのアプリケーション トラフィックのルーティング
- Cisco Umbrella 自動トンネルを使用したセキュアなインターネットトラフィック

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。