BGP-EVPN インターサイト接続を構成

インフラの設定: 一般設定

ここでは、すべてのサイトの一般的なインフラ設定を構成する方法について説明します。

（注） 次の設定には、すべてのサイトに適用されるものと、特定のタイプのサイト（Cloud Network Controller サイトなど）に必要なものとがあります。各サイト固有のサイト ローカル設定に進む前に、インフラ一般設定で必要なすべての設定を完了していることを確認します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、**[全般設定（General Settings）]**を選択します。

ステップ 5 **[コントロール プレーン設定（Control Plane Configuration）]** を指定します。

a) **[コントロール プレーン設定（Control Plane Configuration）]** タブを選択します。

b) **[BGP ピアリング タイプ（Bgp Peering Type）]** を選択します。

- `full-mesh`：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。

  `full-mesh` 構成では、Nexus Dashboard Orchestrator は ACI 管理ファブリックのスパイン スイッチと NDFC 管理ファブリックのボーダー ゲートウェイを使用します。

- `[route-reflector]`：route-reflector オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロール プレーン ノードを指定できます。ルート リフレクタ ノー

ドを使用すると、NDO によって管理されるすべてのサイト間で MP-BGP EVPN フル メッシュ隣接関係が作成されなくなります。

ACIファブリックの場合、`[route-reflector]` オプションは、同じ BGP ASN の一部であるファブリックに対してのみ有効です。

c) **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]** フィールドに、キープアライブ間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

d) **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

e) **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

f) **[グレースフル ヘルパー (Graceful Helper)]** オプションをオンにするかどうかを選択します。

g) **[AS 上限（Maximum AS Limit）]**を入力します。

デフォルト値を維持することを推奨します。

h) **[ピア間のBGP TTL（BGP TTL Between Peers）]** を入力します。

デフォルト値を維持することを推奨します。

i) **[OSPF エリア ID (OSPF Area ID)]** を入力します。

Cloud Network Controller サイトがない場合、このフィールドは UI に表示されません。

これは、オンプレミス IPN ピアリングのためにクラウド サイトで使用される OSPF エリア ID です。

j) (オプション) CloudSec 暗号化の **[IANA 割り当てポート（IANA Assigned Port）]**を有効にします。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

（注） IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、[IANA 予約 UDP ポート（IANA Reserve UDP Port）] オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

CloudSec を構成するための詳細情報と手順については、*『ACI ファブリック用のNexus Dashboard Orchestrator 構成ガイド（Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics）』*の「CloudSec 暗号化」の章を参照してください。

ステップ 6 **[IPN デバイス情報]** を入力します。

オンプレミスとクラウドサイト間のサイト間接続を設定する予定がない場合は、この手順をスキップできます。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウドCSRへの接続を確立するオンプレミスIPNデバイスを選択する必要があります。これらのIPNデバイスは、オンプレミスのサイト設定画面で使用可能になる前に、ここで定義する必要があります。

a) **[オンプレミス IPSec デバイス（On Premises IPSec Devices）]** タブを選択します。
b) **[+オンプレミス IPSec デバイスを追加（+Add On-Premises IPSec Device）]** をクリックします。
c) デバイスが**[管理対象外（Unmanaged）]**か**[管理対象（Managed）]**かを選択し、デバイス情報を提供します。

これは、デバイスがNDFCによって直接管理されるかどうかを定義します。

- **[管理対象（Managed）]** IPNデバイスにはシンプルにデバイスの**[名前（Name）]** と **[IP アドレス（IP Address）]** を入力してください。

  指定したIPアドレスは、IPNデバイスの管理IPアドレスではなく、クラウドCSRからのトンネル ピア アドレスとして使用されます。

- **[管理対象（Managed）]** IPNデバイスには、デバイスが入っているNDFC **[サイト（Site）]** を選択し、そのサイトの **[デバイス（Device）]** を選択します。

  次に、インターネットに接続しているデバイスの**[インターフェイス（Interface）]**を選択し、インターネットに接続しているゲートウェイのIPアドレスである**[ネクスト ホップ（Next Hop）]** IPアドレスを指定します。

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
e) 追加するIPNデバイスについて、この手順を繰り返します。

ステップ 7 **[外部 デバイス（External Devices）]** 情報を入力します。

Cloud Network Controllerサイトがない場合、このタブはUIに表示されません。

Multi-Site ドメインに Cloud Network Controller サイトがない場合、またはクラウド サイトとブランチ ルータまたはその他の外部デバイス間の接続を設定する予定がない場合は、この手順をスキップできます。

次の手順では、クラウドサイトからの接続を設定するブランチルータまたは外部デバイスに関する情報を指定する方法について説明します。

a) **[外部デバイス（External Devices）]** タブを選択します。

このタブは、Multi-Site ドメインに少なくとも 1 つのクラウドサイトがある場合にのみ使用できます。

b) **[外部デバイスの追加（Add External Device）]** をクリックします。

[外部デバイスの追加（Add External Device）] ダイアログが開きます。

c) デバイスの **[名前（Name）]**、**[IP アドレス（IP Address）]**、および **[BGP 自律システム番号（BGP Autonomous System Number）]** を入力します。

指定したIPアドレスは、デバイスの管理IPアドレスではなく、Cloud Network Controller の CSR からのトンネル ピア アドレスとして使用されます。接続は、IPSec を使用してパブリック インターネット経由で確立されます。

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。

e) 追加する IPN デバイスについて、この手順を繰り返します。

すべての外部デバイスを追加したら、次の手順を完了して、IPSec トンネル サブネット プールにこれらのトンネルに割り当てられる内部 IP アドレスを指定します。

ステップ 8 **[IPSecトンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 情報を入力します。

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール**：クラウド サイトの CSR と他のサイト（クラウドまたはオンプレミス）間の接続に使用されます。

  これらは、Nexus Dashboard Orchestrator によって管理される大規模なグローバル サブネット プールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

  1 つ以上のクラウド サイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネット プールを提供する必要があります。

- **サイト固有のサブネット プール**：クラウド サイトの CSR と外部デバイス間の接続に使用されます。

  これらのサブネットは、外部接続 IPsec トンネルが特定の範囲内にあることが必要な場合に定義できます。たとえば、外部ルータに IP アドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを NDO およびクラウド サイトの IPsec トンネルで引き続き使用する場合です。これらのサブネットは Orchestrator によって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

  名前付きサブネット プールを指定しない場合でも、クラウド サイトの CSR と外部デバイス間の接続を設定すると、外部サブネット プールが IP 割り当てに使用されます。.

（注） 両方のサブネット プールの最小マスク長は `/24` です。

1 つ以上の**外部サブネット プール**を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。
b) **[外部サブネット プール（External Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   このサブネットは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用に Cloud Network Controller で以前に設定した、オンプレミス接続に使用されるクラウド ルータの IPsec トンネル インターフェイスとループバックに対処するために使用されます。

   サブネットは、他のオンプレミス TEP プールと重複してはならず、`0.xxx` または `0.0.xx`で 始まってはならず、`/16` と `/24` の間のネットワーク マスク（`30.29.0.0/16` など）が必要です。

c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。

b) **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

[名前付きサブネットプールの追加（Add Named Subnet Pool）] ダイアログが開きます。

c) サブネットの **[名前（Name）]** を入力します。

後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。

d) **[+ IP アドレスの追加 (+ Add IP Address)]** をクリックして、1 つ以上のサブネット プールを追加します。

サブネットには `/16` と `/24` の間のネットワークが必要で、`0.x.x.x` または `0.0.x.x` で始めることはできません。たとえば、`30.29.0.0/16` のようにします。

e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。

f) **[保存（Save）]** をクリックして、名前付きサブネット プールを保存します。

g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

次のタスク

全般的なインフラ設定を構成した後も、管理するサイトのタイプ（ACI、Cloud Network Controller、またはNDFC）に基づいて、サイト固有の設定に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。

クラウド サイト接続性情報の更新

CSRやリージョンの追加や削除などのインフラストラクチャの変更には、Multi-Site ファブリック接続サイトの更新が必要です。このセクションでは、各サイトのコントローラから直接最新の接続性情報を取得する方法を説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]** を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。

ステップ 5 メインウィンドウで **[更新 (Refresh)]** ボタンをクリックして、新規または変更されたCSRおよびリージョンを検出します。

ステップ 6 最後に、**[はい (Yes)]** をクリックして確認し、接続情報をロードします。

これにより、新規または削除された CSR およびリージョンが検出されます。

ステップ 7 **[導入 (Deploy)]** をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。

クラウドサイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ設定を展開して、そのクラウドサイトへのアンダーレイ接続がある他のサイトが更新された設定を取得する必要があります。

インフラの構成：Google クラウド サイトの設定

ここでは、Cloud Network Controller サイト固有のインフラ設定を構成する方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のクラウド サイトを選択します。

ステップ 5 **[サイト間接続（Inter-Site Connectivity）]** 情報を入力します。

a) 右側の ***[<Site> 設定 (Settings)]*** ペインで、**[サイト間接続 (Inter-Site Connectivity)]** タブを選択します。

b) **[マルチサイト（Multi-Site）]** ノブを有効にします。

これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

オーバーレイ構成は、次の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされないことに注意してください。

ステップ 6 サイト固有の **[サイト間接続 (Inter-Site Connectivity)]** 情報を入力します。

a) **[コントラクトベースのルーティング（Contract Based Routing）]** オプションを有効にする。

b) クラウド サイトの右側のプロパティ サイドバーで、**[サイトの追加（Add Site）]** をクリックします。

[サイトの追加（Add Site）] ウィンドウが表示されます。

c) [サイトへの接続（Connected to Site）] で、[サイトの選択（Select a Site）] をクリックし、構成しているサイト（たとえば、Site1）からの接続を確立するサイト（たとえば、Site2）を選択します。

リモート サイトを選択すると、[サイトの追加（Add Site）] ウィンドウが更新され、両方向の接続が反映されます：[サイト1（Site1）] > [サイト2（Site2）] および [サイト2（Site2）] > [サイト1（Site1）]。

d) [サイト1（Site1）] > [サイト2（Site2）] エリアで、[接続タイプ（Connection Type）] ドロップダウンから、サイト間の接続のタイプを選択します。

次のオプションを使用できます。

- `[パブリックインターネット (Public Internet)]`：2 つのサイト間の接続は、インターネットを介して確立されます。

  このタイプは、任意の 2 つのクラウド サイト間、またはクラウド サイトとオンプレミス サイト間でサポートされます。

- [プライベート接続 (Private Connection)]：2 つのサイト間のプライベート接続を使用して接続が確立されます。

  このタイプは、クラウド サイトとオンプレミス サイトの間でサポートされます。

- [クラウド バックボーン (Cloud Backbone)]：クラウドバックボーンを使用して接続が確立されます。

  このタイプは、Azure-to-Azure、AWS-to-AWS、GCP-to-GCP など同じタイプの 2 つのクラウド サイト間でサポートされます。

複数のタイプのサイト（オンプレミス、AWS、AzureとGCP）がある場合、サイトの異なるペアは異なる接続タイプを使用できます。

e) これら 2 つのサイト間の接続に使用する [プロトコル（Protocol）] を選択します。

このユース ケースでは、**BGP-EVPN** を使用します。オプションで **IPSec** を有効にして、使用するインターネット キー エクスチェンジ（IKE）プロトコルのバージョン（構成に応じて IKEv1（[バージョン 1 (Version 1)]）または IKEv2（[バージョン 1 (Version 1)]））を選択できます。

- パブリック インターネット接続の場合、IPsec は常に有効です。
- クラウド バックボーン接続の場合、IPsec は常に無効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

代わりに [BGP-IPv4] 接続を使用する場合は、構成しているクラウドサイトからのルート リーク構成に使用される外部 VRF を提供する必要があります。

[サイト1（Site1）] > [サイト2（Site2）] の接続情報が提供された後、[サイト2（Site2）] > [サイト1（Site1）] 領域は、反対方向の接続情報を反映します。

f) **[保存 (Save)]** をクリックして、設定を保存します。

Site1 から Site2 への接続情報を保存すると、Site2 から Site1 へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、右側のサイドバーにある **[サイト間接続（Inter-site Connectivity）]** 情報を選択することで確認できます。

g) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

Site1 から Site2 へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、Site1 から Site3 へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

ステップ 7 **[外部接続 (External Connectivity)]** 情報を入力します。

NDOによって管理されていない外部サイトまたはデバイスへの接続を設定する予定がない場合は、この手順をスキップできます。

外部接続の使用例の詳細な説明は、『Nexus Dashboard Orchestrator を使用したクラウド CSR からの外部接続の構成』ドキュメントで入手できます。

a) 右側の ***[<Site> 設定 (Settings)]*** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。
b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

c) **[VRF]** ドロップダウンから、外部接続に使用する VRF を選択します。

これは、クラウド ルートをリークするために使用される VRF です。**[リージョン (Regions)]** セクションには、この設定を適用する CSR を含むクラウド リージョンが表示されます。

d) **[外部デバイス (External Devices)]** セクションの **[名前 (Name)]** ドロップダウンから、外部デバイスを選択します。

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]** > **[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、インフラの設定: 一般設定 （1 ページ）の説明に従ってすでに定義されている必要があります。

e) **[トンネル IKE バージョン (Tunnel IKE Version)]** ドロップダウンから、クラウド サイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。

f) （任意）**[トンネル サブネット プール (Tunnel Subnet Pool)]** ドロップダウンから、名前付きサブネット プールのいずれかを選択します。

名前付きサブネット プールは、クラウド サイトの CSR と外部デバイス間の IPSec トンネルに IP アドレスを割り当てるために使用されます。ここで**名前付き**サブネット プールを指定しない場合、**外部**サブネット プールが IP 割り当てに使用されます。

外部デバイス接続用の専用サブネット プールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されており、それらのサブネットを NDO およびクラウド サイトのIPSecトンネルに引き続き使用する場合に役立ちます。

この接続に特定のサブネット プールを提供する場合は、インフラの設定: 一般設定 （1 ページ）の説明に従って作成済みである必要があります。

g) （オプション）**[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタム キーを入力します。

h) 必要に応じて、同じ外部接続（同じ VRF ）に対して追加する外部デバイスについて、前のサブステップを繰り返します。

i) 必要に応じて、追加の外部接続（異なる VRF ）に対してこの手順を繰り返します。

CSR と外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。

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。