Cloud Network Controller との統合

概要

ご存じのとおり、Nexus Dashboard Orchestrator は、異なる Nexus ダッシュボード ファブリック コントローラ（NDFC）インスタンスによって管理される複数のオンプレミス VXLAN EVPN ファブリック間の EVPN マルチサイト拡張をサポートしています。これには、ボーダー ゲートウェイ（BGW）での EVPN ピアリングのプロビジョニングと、さまざまなオンプレミス NX-OS ベースのネットワーク スイッチにわたるテンプレートを介したオーバーレイ ネットワーク/VRF のプロビジョニングが含まれます。Nexus Dashboard Orchestrator は、オンプレミスとクラウドの統合と、オンプレミスの ACI ファブリックと Cisco Cloud Network Controller（以前の Cisco Cloud APIC）によって管理されるパブリック クラウド ネットワーク間のワークロード接続もサポートしています。

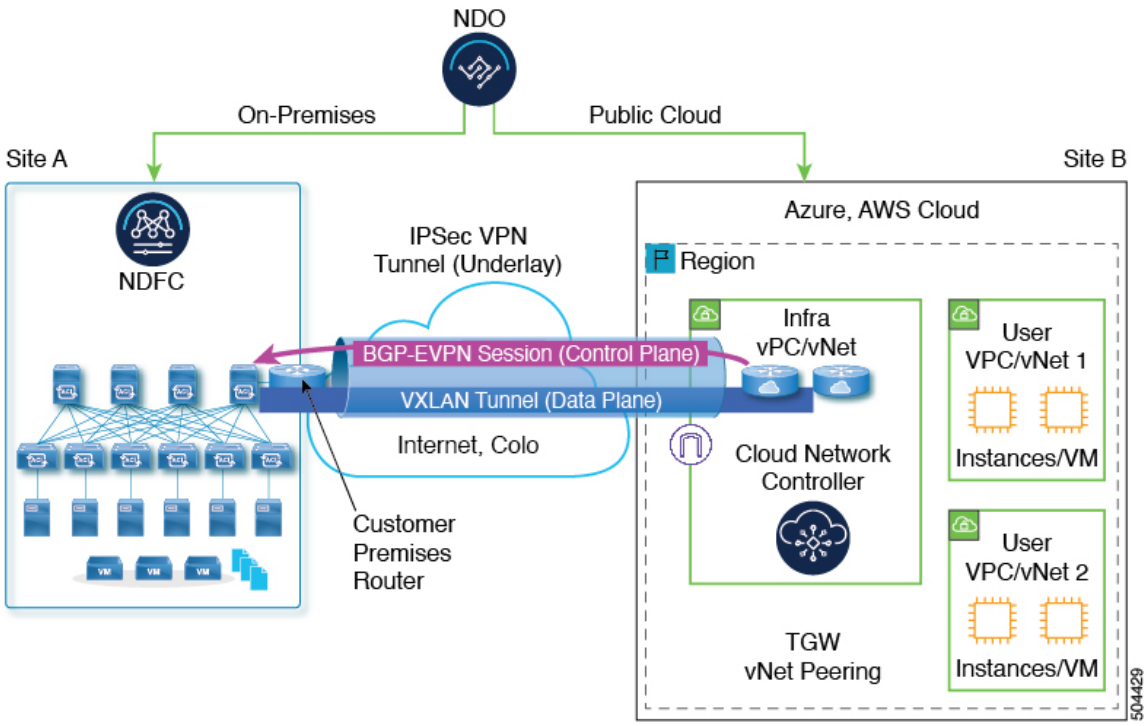
Nexus Dashboard Orchestrator のリリース 4.0(2) は、NDFC によって管理されるオンプレミスの NX-OS ベースのファブリックにパブリック クラウドを統合します。次のセクションでは、NDFC によって管理されるオンプレミスの VXLAN EVPN ベースのデータ センターからのワークロードを構成して、パブリック クラウドで実行され、クラウド ネットワーク コントローラによって管理されるワークロードと通信する方法について詳しく説明します。

（注） Nexus Dashboard Orchestrator のこのリリースは、Amazon Web Services（AWS）および Microsoft Azure のみの NDFC ファブリックとパブリック クラウド間の統合をサポートします。

次の図は、このドキュメント全体で使用されるサンプル トポロジを示しています。これには、NDFC によって管理されるオンプレミス サイト（`SiteA`）、AWS または Azure パブリック クラウド サイト（`SiteB`）、およびインフラストラクチャの Catalyst 8000V が接続されている 2 つのサイト間の安全な接続が含まれます。 VPC/VNET は、オンプレミス サイトとの間で送受信されるすべてのトラフィックのクラウド ゲートウェイとして機能します。

（注） 次の図は、ボーダー ゲートウェイ（BGW）として機能するスパイン スイッチを示しています。ただし、BGW はリーフ スイッチとしても展開できます。

図 *1*: ***NDO***、***NDFC***、およびクラウド ネットワーク コントローラの統合例のトポロジ



サイト間のアンダーレイとオーバーレイの接続を確立するときは、次のアプローチを取ります。

- オンプレミス側では、異なるオンプレミス VXLAN EVPN サイト間のシームレスなレイヤ 2/レイヤ 3 DCI 拡張をすでにサポートしている BGW により、VRF をパブリック クラウドに拡張できます。

  BGW 機能は、一連のリーフ スイッチで有効にすることも、スパイン スイッチ上で同じ場所に配置することもできます。

- Orchestrator は、オンプレミスの BGW とクラウド内の Catalyst 8000V 間のコントロール プレーンに BGP EVPN を使用します。

  VXLAN カプセル化は、オンプレミス サイトとパブリック クラウド間の L3 拡張のデータ プレーンで使用されます。

- オンプレミスのデータセンターからクラウドへの接続がパブリック インターネットを介している場合、安全なチャネルを確立するために IPsec トンネルが作成されます。

  この目的のため、BGW は、ASR 1000 または CSR 1000v または Catalyst 8000V などのオンプレミスの IPsec 対応デバイスに接続されます。このデバイスは基本的に、オンプレミスの BGW からクラウドの Catalyst 8000V へのエンドツーエンド トラフィックが VXLAN over IPsec を使用するように IPsec トンネルを追加します。

  BGW が Direct Connect または Express Route オプションを介してパブリック クラウドに接続されている場合、IPsec の有効化はオプションであることに注意してください。

- アンダーレイの観点から、BGW はオンプレミスの IPsec デバイスと eBGP をピアリングします。オンプレミスの IPsec デバイスは、確立された IPsec トンネルを介して、クラウド内の Catalyst 8000V と eBGP をピアリングします。

  NDFC は NX-OS ベースのデバイスと IOS-XE ベースのデバイスの両方を管理できるため、NDO は BGP EVPN オーバーレイ、eBGP アンダーレイ、および NDFC 経由でオンプレミス側の IPsec トンネル構成をプロビジョニングします。同様に、NDO は、クラウド ネットワーク コントローラを介して、対応するピア関連の構成を Catalyst 8000V にプロビジョニングします。

  IPsec が有効になっている場合、アンダーレイは IPsec デバイスで終了します。それ以外の場合は、オンプレミス サイトの BGW で終了します。

- これは標準ベースのオンプレミス ファブリックであるため、ACI ファブリックで使用される iVXLAN（UDP 宛先ポート `0xBEEF`）の代わりに、オンプレミス VXLAN EVPN データセンターとクラウド Catalyst 8000V ルータの間で標準 VXLAN（UDP 宛先ポート `4789`）を使用することに注意してください。

必要なコンポーネント

ハイブリッド クラウドは、オンプレミス ネットワークとパブリック クラウド ネットワークを相互接続するためのソリューションです。ハイブリッド クラウド ソリューションの主なコンポーネントは次のとおりです。

- **Easy Fabric**：ボーダー ゲートウェイ（BGW）を含む NDFC 管理のオンプレミス VXLAN ベースのファブリック。

  このファブリックはスタンドアロンにすることも、他のオンプレミス サイトからパブリック クラウドへの接続を提供する POP サイトとして機能させることもできます。

- **外部ファブリック**：オンプレミスの Easy Fabric をパブリック クラウドに相互接続するための IPN デバイス（ASR 1000、CSR 1000v、または Catalyst 8000V など）を含む NDFC 管理ファブリック。

この場合、オンプレミスの Easy Fabric サイトの BGW は、外部ファブリックの IPN デバイスに接続されます。

- **パブリック クラウド**：クラウドネットワーク コントローラによって管理され、CSR 1000v または Catalyst 8000V を含むパブリック クラウド サイト。

  オンプレミスとパブリック クラウド間のレイヤ 3 到達可能性は、パブリック クラウドと外部ファブリックの CSR 1000v または Catalyst 8000V を介してプロビジョニングされます。

ワークフロー

このドキュメントの他のセクションでは、必要な構成について詳しく説明しています。簡単に言えば、次のワークフローを実行します。

- Nexus Dashboard Orchestrator のホストに使用される Nexus ダッシュボード クラスターを展開します。

（注） NDO サービスと NDFC サービスには、個別の Nexus ダッシュボード クラスタを使用する必要があります。

- Cisco Nexus Dashboard Orchestrator をインストール。
- NDFC サイトとクラウド ネットワーク コントローラ サイトをオンボードします。
- NDO を使用してサイトのインフラ接続を構成し、オンプレミス サイトとクラウド サイト間の接続を確立します。
- 既存の NDFC 構成をインポートします。

サポートされる使用例

VRF ストレッチング

このユース ケースでは、NDFC サイトから AWS または Azure のパブリック サイトへの VRF のレイヤ 3 拡張を構成できます。これは、NDFC サイトのボーダー ゲートウェイ（BGW）のルート ターゲット （RT）と、クラウド ネットワーク コントローラ側の CSR 1000v または Catalyst 8000V をプログラミングすることによって行われます。これにより、これらのサイトのワークロード間でトラフィックが流れるようになります。

このユースケースを展開するには、次の手順を実行します。

1. 単一のテンプレートで VRF を定義し、そのテンプレートを両方のサイトに関連付けます。
2. NDFC のサイトローカル VRF プロパティを設定します。
3. クラウドのサイトローカル VRF プロパティを設定します。

4. 設定を展開します。

VRF リーク（共有サービス）

これは、オンプレミスのACIファブリックで以前サポートされていた機能です。これにより、オンプレミス サイトに VRF（vrf1）、クラウド サイトに別の VRF（vrf2）を設定し、それらの VRF のワークロードが相互に通信できるようにします。この場合、オンプレミスの VRF は、ストレッチまたはサイトローカルのいずれかにすることができます。

このユースケースを展開するには、次のことができます。

1. dcnm-default-tn テナントに関連付けられた template1 に vrf1 を定義します。
2. template1 をオンプレミスおよびクラウド サイト、またはオンプレミス サイトのみに関連付けます。
3. dcnm-default-tn テナントに関連付けられた template2 に vrf2 を定義します。

   このテンプレートをクラウド サイトにも関連付けますが、dcnm-default-tn と別のクラウド テナントとの間のルート リークはサポートされないことに注意してください。
4. template2 をクラウド サイトのみに関連付けます。
5. 2 つの VRF 間のルート リークを構成します。
6. 設定を展開します。

サポートされるトポロジ

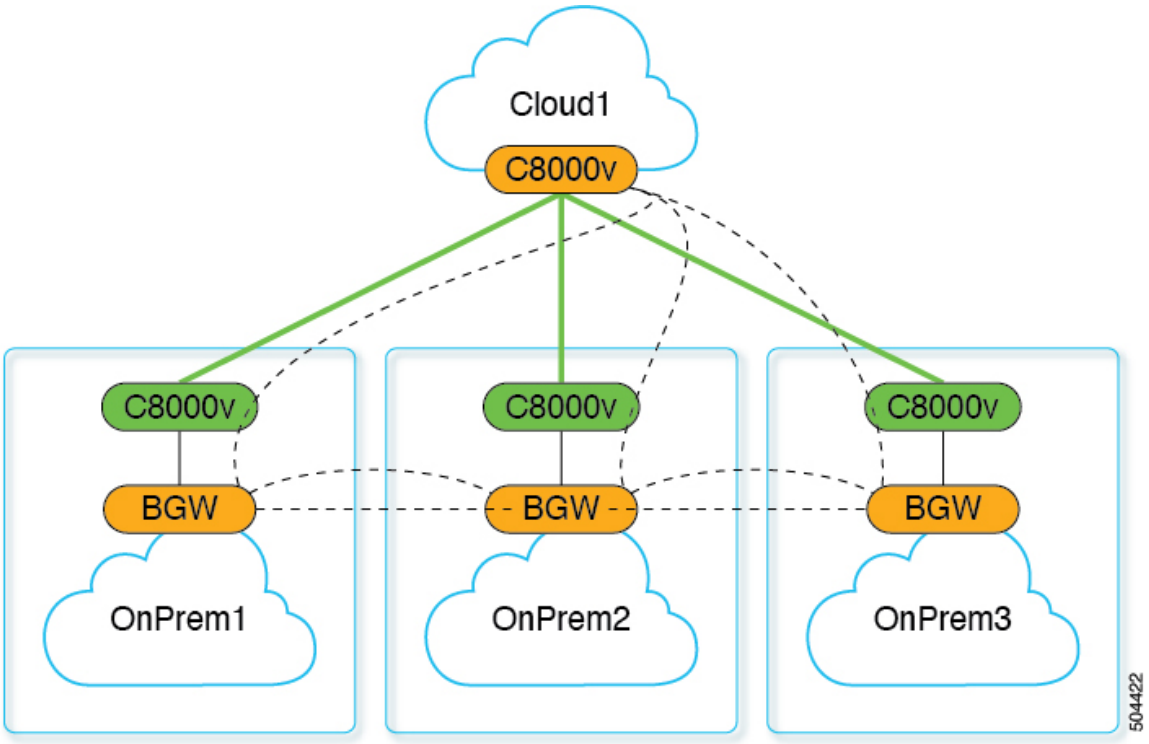
NDFCファブリックとクラウドサイト間のサイト間接続を展開する場合、次の全体的なトポロジがサポートされます。

（注） 次のすべての図で：

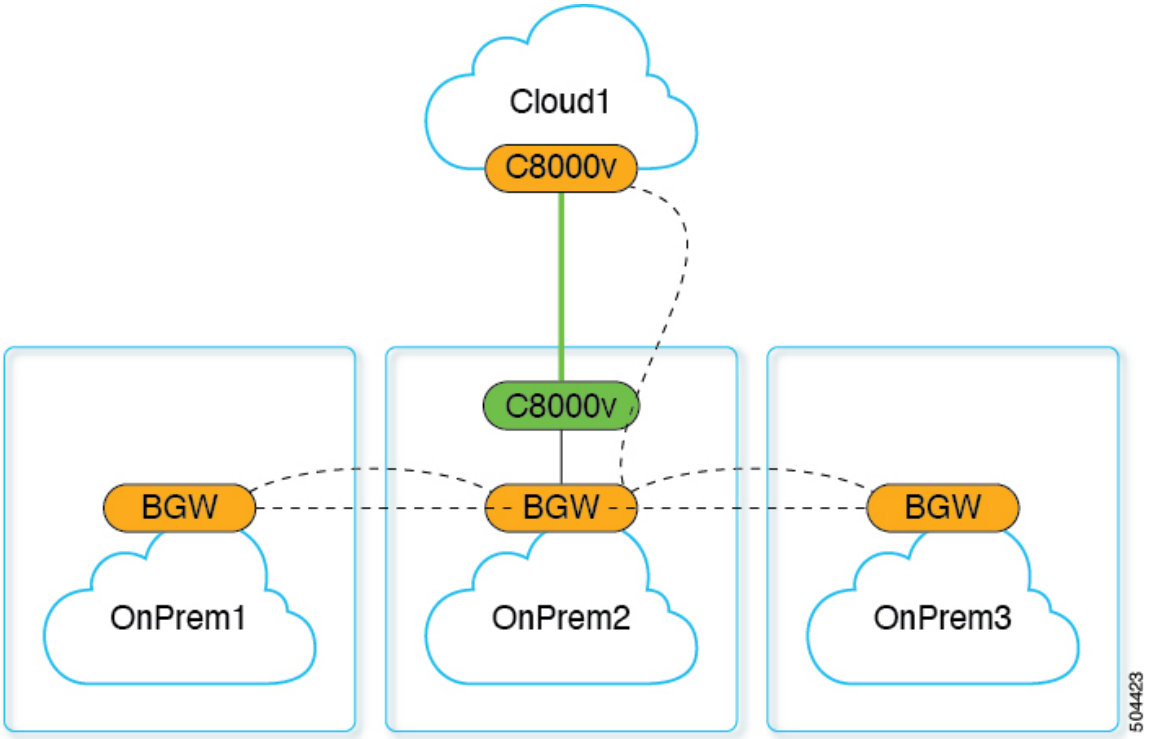
- 緑の実線は IPsec トンネルを表します。
- 点線は、BGP-EVPN オーバーレイ ピアリングを表します。
- クラウド サイトの C8KV は CSR を表しています。CSR 1000v または Catalyst 8000V の可能性があります。
- オンプレミス サイトの C8KV は IPN デバイスで、ASR 1000、CSR 1000v、または Catalyst 8000V の可能性があります。

  NDFC の観点からは、これらはすべて管理対象の IOS-XE デバイスです。

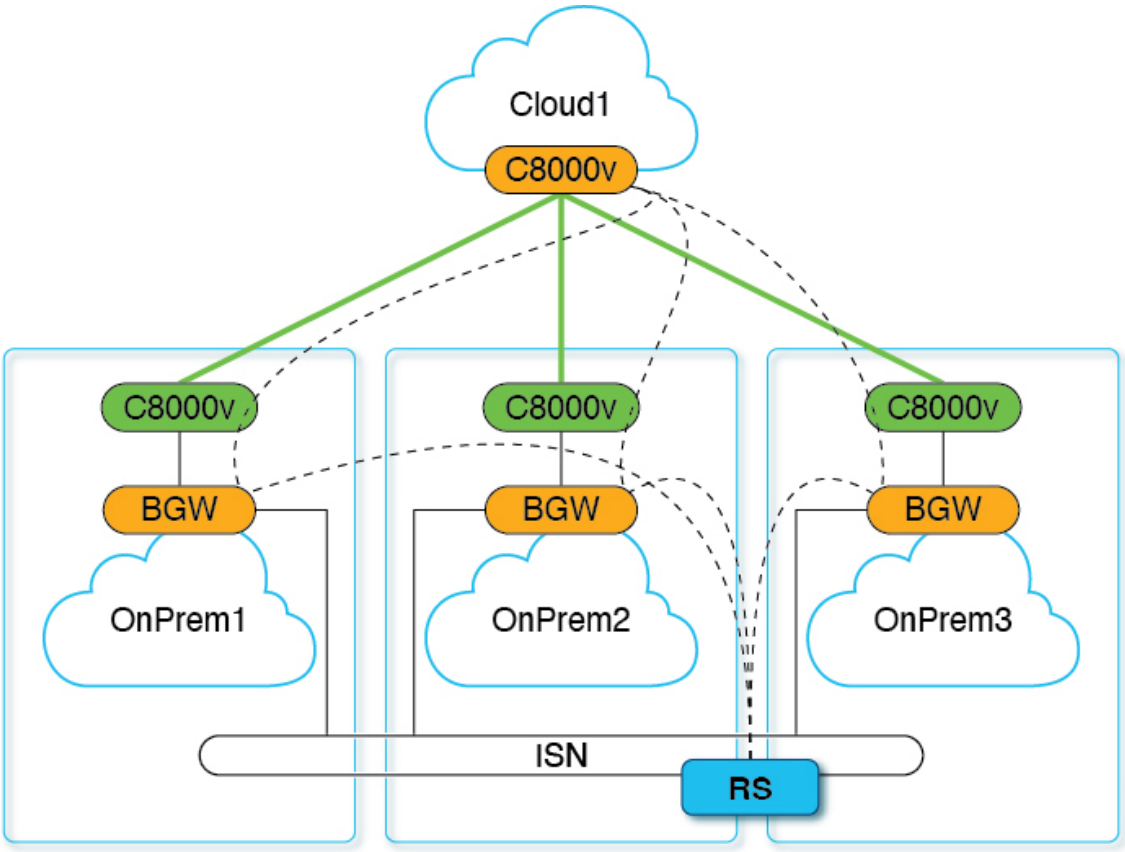
- オンプレミス サイトと、クラウド サイト両方の分散型フルメッシュ接続：



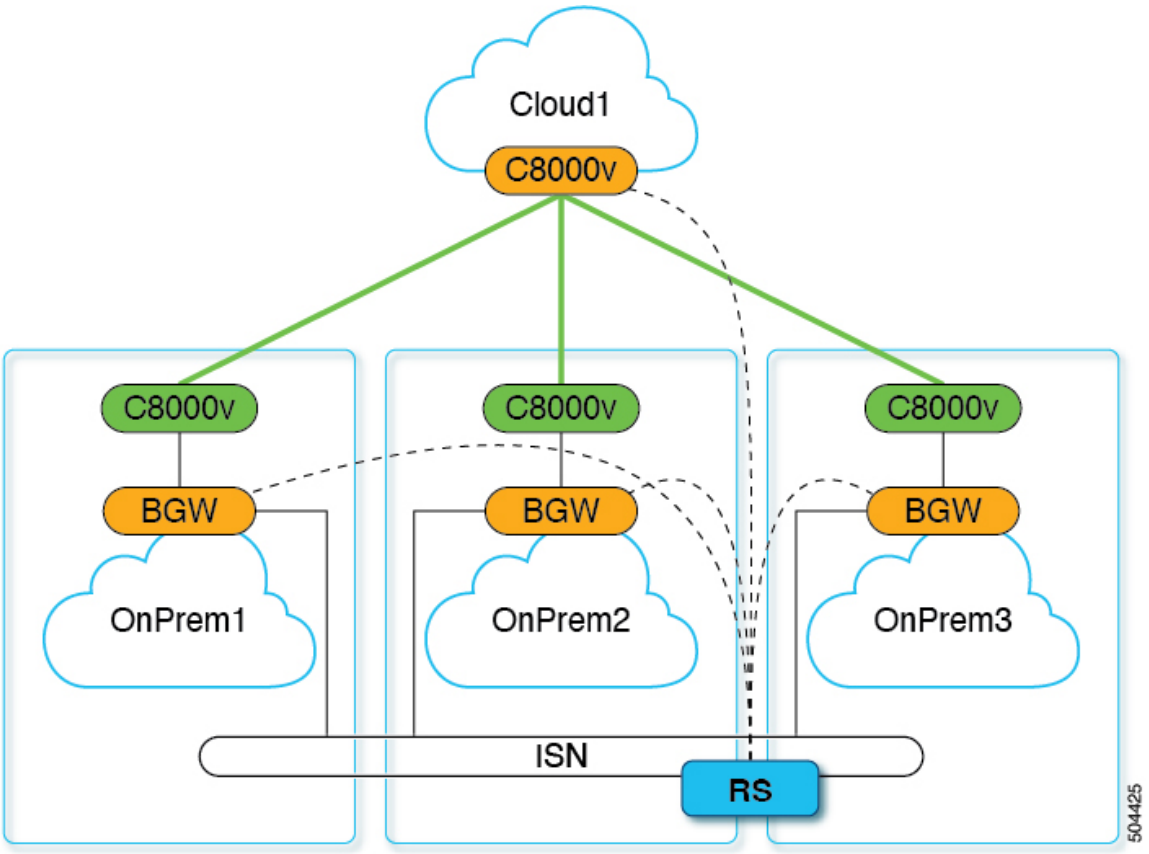
- オンプレミス サイトと、クラウド サイトに接続されている単一のオンプレミス サイトとの分散型フルメッシュ接続：



- ルート サーバー（RS）を備えたオンプレミス サイトと、クラウド サイトに接続されているすべてのオンプレミス サイトとのフルメッシュ接続：



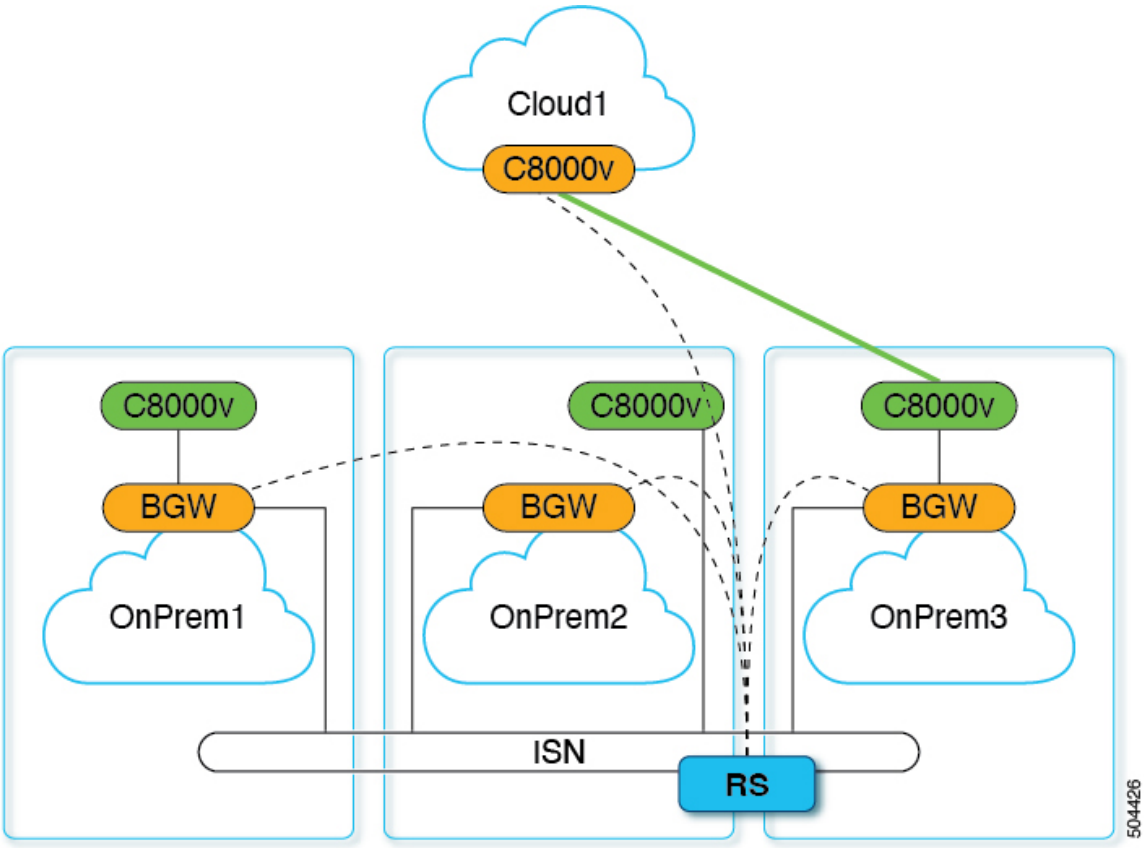
- RS を備えたオンプレミス サイトと、RS を介してクラウド サイトに接続されているすべてのオンプレミス サイトとのフルメッシュ接続：



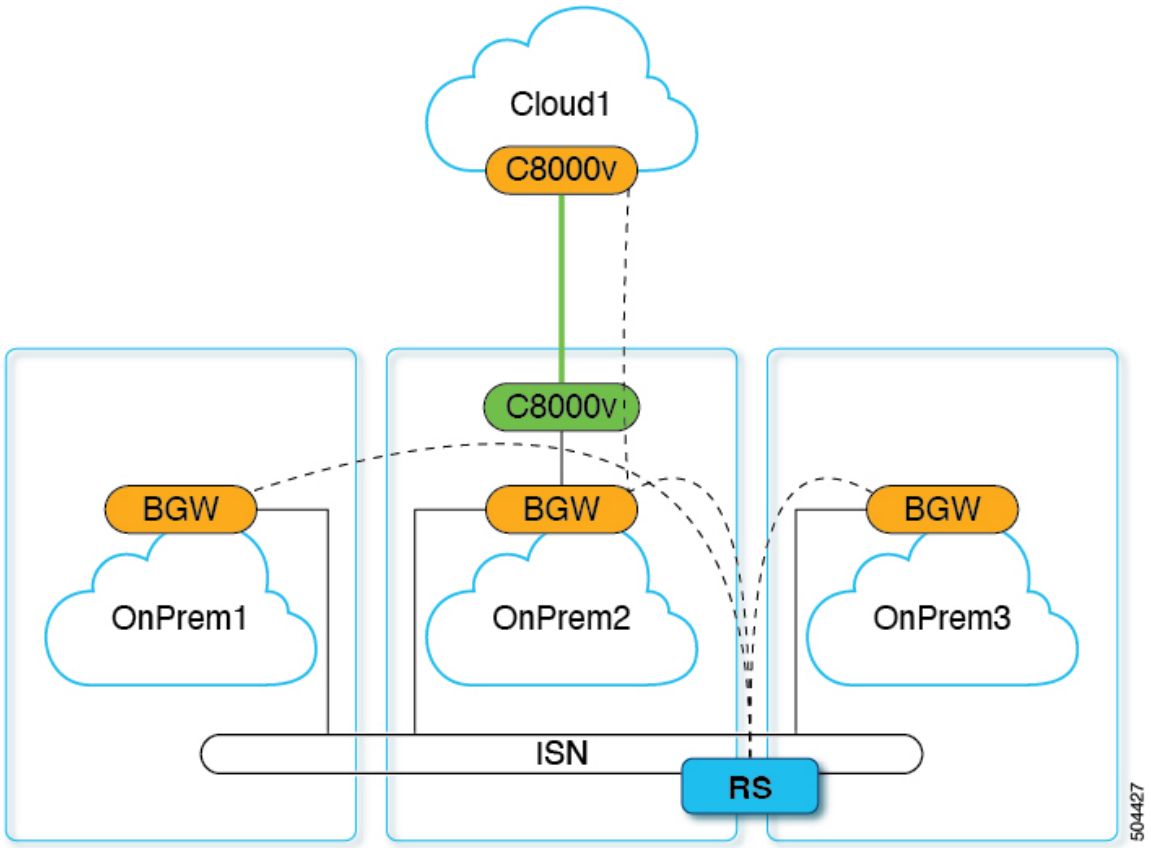
サポートされていないトポロジ

以下のトポロジは**サポートされていません**。

- RS を備えたオンプレミス サイトと、すべてのクラウド サイトの共有 CSR とのフル メッシュ接続：



- RS を備えたオンプレミス サイトと、クラウド サイトに接続された単一のオンプレミス サイトとのフル メッシュ接続：



前提条件とガイドライン

このユースケースを構成する前に、以下を完了しておく必要があります。

- このユースケースに必要なすべてのソフトウェアのサポートされているバージョンがデプロイまたはアップグレードされている：
  - Nexus Dashboard リリース 2.2(2) 以降と、Nexus Dashboard ファブリック コントローラ リリース 12.1(1p)

（注） 既存の NDFC インストールをこのリリースにアップグレードすることはサポートされていないため、新しい NDFC インスタンスをデプロイする必要があります。

NDFC 12.1(1p) リリースの提供対象は限られています。詳細については、シスコの担当者にお問い合わせください。

  - Nexus Dashboard リリース 2.1(2d) 以降と、Nexus Dashboard Orchestrator リリース 4.0(2)

（注） ファブリック コントローラとオーケストレータ サービスは、別々の Nexus ダッシュボード クラスタにデプロイする必要があります。

詳細については、*Cisco Nexus Dashboard Deployment Guide* および *Cisco Nexus Dashboard Orchestrator Deployment Guide* を参照してください。

- AWS または Azure パブリック クラウドのクラウド ネットワーク コントローラー リリース 25.0(5) 以降。

（注） このユース ケースは、AWS または Azure クラウド サイトでのみサポートされています。

詳細については、*Cisco Cloud Network Controller for AWS Installation Guide* または *Cisco Cloud Network Controller for Azure Installation Guide* を参照してください。

- Nexus Dashboard Orchestrator サービスをホストしている Nexus Dashboardクラスタで、NDFC とクラウド ファブリックをオンボーディングします。

  これには、Nexus Dashboard にサイトを追加し、Nexus Dashboard Orchestrator で管理できるようにすることが含まれます（*Cisco Nexus Dashboard Orchestrator 導入ガイド*を参照）。

上記の要件に加えて、このユース ケースには次の制限があります。

- このリリースでは、オンプレミス サイトとクラウド サイト間の VRF のストレッチがサポートされています。
- VRF 間のルート リークを設定する場合、「Leak All」オプションはサポートされません。
- クラウド サイトへのインターネット ルートのエクスポートはサポートされていません。

  その結果、インターネット接続が NDFC サイトで構成されていて、NDFC とクラウド サイトの間でサイト間接続が確立されている場合、クラウド EPG はインターネットに到達できません。

インフラの設定：Orchestrator 一般設定

このセクションでは、Nexus Dashboard Orchestrator によって搭載および管理される NDFC 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。

このセクションでは、複数の UI タブにわたっていくつかの設定を構成します。

- **[コントロール プレーンの構成（Control Plane Configuration）]** タブには、オンプレミス サイト間のマルチサイト VXLAN 構成の設定情報が含まれています。

- **[IPN デバイス（IPN Devices）]** タブには、オンプレミスの IPN デバイス（ASR 1000、CSR 1000v、Catalyst 8000V など）に関する設定情報が含まれています。これらは、オンプレミス サイトの BGW とクラウド CSR 1000v または Catalyst 8000V 間の安全な接続を提供します。
- **[外部デバイス（External Devices）]** タブは、このハイブリッド クラウドのユース ケースでは使用されません。
- **[IPsec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** タブでは、IPsec トンネルに使用されるサブネット プールを定義できます。
- **[NDFC 設定（NDFC Settings）]** タブには、VNI、マルチサイト ループバック IP、エニーキャスト ゲートウェイ、およびオンプレミス VXLAN 接続のその他の設定が含まれています。

ステップ 1 Orchestrator の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 2 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 3 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 4 **[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。
- `route-server`：route-server 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。ルートサーバー ノードは、従来の BGP ルート リフレクタと同様の機能を実行しますが、EBGP（iBGP）セッションでは使用しません。ルートサーバー ノードを使用すると、NDO によって管理されるすべての VXLAN EVPN 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。

c) **[BGP ピアリングタイプ（BGP Peering Type）]** を `route-server` に設定する場合は、**[+ルート サーバーを追加（+ Add Route Server）]** をクリックして、1 台以上のルート サーバーを追加します。

[ルート サーバーの追加（Add Route Server）] ウィンドウが開きます。

- **[サイト（Site）]** ドロップダウンから、ルート サーバーに接続するサイトを選択します。
- **[ASN]** フィールドには、サイトのASNが自動的に入力されます。
- **[コア ルータ デバイス（Core Router Device）]** ドロップダウンから、接続するルート サーバーを選択します。
- **[インターフェイス（Interface）]** ドロップダウンから、コア ルータ デバイスのインターフェイスを選択します。

ルート サーバーは最大 4 台まで追加できます。複数のルート サーバーを追加すると、すべてのサイトがすべてのルート サーバーに対して MP-BGP EVPN 隣接関係を確立します。

d) **[キープアライブ間隔（秒）（Keepalive Interval（Seconds））]**、**[ホールド間隔（秒）Hold Interval（Seconds）]**、**[ステール間隔（秒）（Stale Interval（Seconds））]**、**[グレースフル ヘルパー（Graceful Helper）]**、**[最大 AS 限界（Maximum AS Limit）]**、および **[ピア間の BGP TTL（BGP TTL Between Peers）]** フィールドは、Cisco ACI ファブリックにのみ関連するため、デフォルト値のままにします。

e) 設定は eBGP ピアリングには適用されないため、**[OSPF エリア ID（OSPF Area ID）]** をスキップします。

f) 設定は Cisco ACI ファブリックのみに適用されるため、**[IANA 割り当てポート（IANA Assigned Port）]** をスキップします。

ステップ 5 **[IPN デバイス情報]** を入力します。

IPN（IP ネットワーク）デバイスは、オンプレミスまたはクラウドサイト（あるいはその両方）の間のネットワーク インフラストラクチャを提供します。これにより、VXLAN EVPN コントロールおよびデータ プレーン接続を確立できます。

オンプレミスとクラウド サイト間接続でプライベート接続を使用し、IPsec を有効化しない場合は、この手順をスキップできます。パブリック インターネット経由の接続では、IPsec が常に有効になっており、この手順で情報を提供する必要があります。

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 6 **[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。

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 と外部またはオンプレミス 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、外部またはオンプレミスデバイスに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。

  サイト固有のサブネット 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、外部またはオンプレミスのサブネット 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 で構成した、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。

   [サイト固有サブネットプールの追加（Add Site-Specific 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、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。

インフラの構成: NDFC インフラ サイト固有の設定

ここでは、オンプレミス サイトに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 **[サイト接続（Site Connectivity）]** ページの左サイドバーの、**[サイト（Sites）]** の下で、特定の NDFC サイトを選択します。

ステップ 2 右側の **<*Site*> [設定 (Settings)]**サイドバーで、**[マルチサイト（Multi-Site）]** 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、以下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 3 **[マルチサイト VIP（Multi-Site VIP）]** を指定します。

このアドレスは、サイト間の L2 BUM および L3 マルチキャスト トラフィックのために使用されます。この IP アドレスは、同じファブリックの一部であるすべてのボーダーゲートウェイスイッチに導入されます。

（注） 設定するサイトが NDFC マルチサイトドメイン（MDS）の一部である場合、このフィールドには NDFC からインポートされた情報が事前に入力されます。この場合、値を変更してインフラ設定を再展開すると、MDS の一部であるサイト間のトラフィックに影響します。

ステップ 4 **[IPN デバイス IPsec IP（IPN Devices IPsec IP）]** 情報を追加します。

複数のサイトがあり、それらの各サイトが異なる IPsec デバイス セットに接続している場合は、ここでその情報を定義できます。前のセクションで説明したように、最初にすべての IPN デバイスを **[一般設定（General Settings）]** タブで指定する必要があることに注意してください。

a) 右側のプロパティ サイドバーの **[サイト間接続（Inter-Site Connectivity）]** タブで、**[+ IPN デバイスの追加（+Add IPN Divice）]** をクリックします。
b) **[名前（Name）]** ドロップダウンから、前に追加した IPN デバイスのいずれかを選択します。
c) チェックマーク アイコンをクリックして保存します。

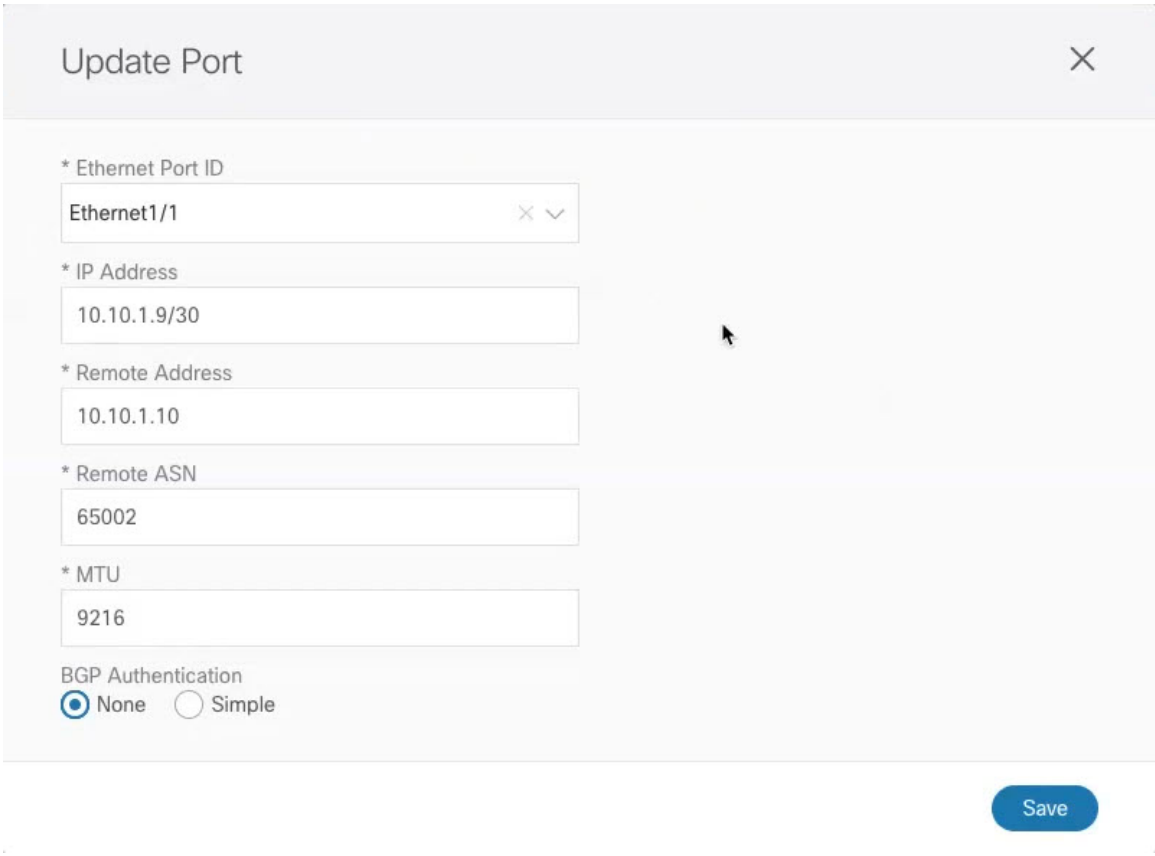
ステップ 5 **<fabric-name>** タイル内で、ボーダーゲートウェイを選択します。

ステップ 6 右側**<*border-gateway*>**サイドバーを設定し、**BGP-EVPN ROUTER-ID** と **BGW PIP** を指定します。

vPCドメインの一部であるボーダーゲートウェイの場合は、**VPC VIP** も指定する必要があります。

ステップ 7 **[ポートの追加 (Add Port)]** をクリックして、IPN に接続するポートを設定します。

（注） このリリースでは、NDFC からのポート設定のインポートはサポートされていません。設定するサイトがすでに NDFC マルチサイトドメイン（MDS）の一部である場合は、NDFC ですでに設定されている値と同じ値を使用する必要があります。



このボーダーゲートウェイをコアスイッチまたは別のボーダーゲートウェイに接続するポートの展開に固有の次の情報を入力します。

- **[イーサネット ポート ID (Ethernet Port ID)]** ドロップダウンから、IPNに接続するポートを選択します。
- **[IP アドレス (IP Address)]** フィールドに、IP アドレスとネットマスクを入力します。

- **[リモート アドレス (Remote Address)]** フィールドに、ポートが接続されているリモート デバイスの IP アドレスを入力します。
- **[リモート ASN (Remote ASN)]** フィールドに、リモート サイトのIDを入力します。
- **[MTU]** フィールドに、サーバーの MTU を入力します。

  スパイン ポートの MTU は、IPN 側の MTU と一致させる必要があります。

  [継承 (inherit)] を指定することも、576 ～ 9000 の値を指定することもできます。
- **BGP認証**の場合は、[なし (None)] または [シンプル (Simple (MD5))] を選択できます。

  [シンプル (Simple)]を選択した場合は、**認証キー**も指定する必要があります。

インフラの構成：パブリック クラウドサイトの設定とサイト間接続

このセクションでは、クラウド サイトのサイト固有のインフラ設定を構成し、クラウド サイトとオンプレミスの NDFC ファブリック間の接続を確立する方法について説明します。

ステップ 1 **[サイト接続（Site Connectivity）]** ページの左サイドバーの、**[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 2 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、**[マルチサイト（Multi-Site）]** 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、以下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 3 このサイトから他のサイトへの **[サイト間接続（Inter-Site Connectivity）]** を構成します

a) 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。

b) **[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、確立する接続の接続先サイトを選択します。

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）]。

c) [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。

（注） 複数のタイプのサイト（オンプレミス、AWS、Azure）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。

d) **[プロトコル（Protocol）]** で、[BGP-EVPN] を選択し、追加の詳細を指定します。

このユース ケースでは、オンプレミスの NDFC ファブリックとクラウド サイトの間で BGP-EVPN 接続を確立する方法について説明します。

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を選択します。構成に応じて IKEv1（バージョン 1）または IKEv2（バージョン 2）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。
- 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。

また、**[ハブ サイト（Hub Site）]** オプションを有効にすることもできます。これは、2 つのクラウド サイト間の EVPN ピアリングが、ルート サーバー モデルなどの中間のオンプレミス VXLAN EVPN サイトを経由することを示します。

e) **[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。

f) 他のクラウド サイトへ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。

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。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。インフラ設定の展開 （19 ページ）の説明に従って、設定を展開する必要があります。

インフラ設定の展開

ここでは、各 NDFC 管理対象サイトにインフラ設定を展開する方法について説明します。

インフラ構成を展開すると、IPsec デバイスの構成、オンプレミス サイトに対してローカルのオーバーレイ ピアリング、およびサイト間接続を構成したクラウド サイトとオンプレミス サイト間のオーバーレイ ピアリングがプッシュされます。

ステップ 1 メインペインの右上で、**[展開（Deploy）]**そして**[IPN デバイス構成ファイルの展開とダウンロード（Deploy & Download External Device Config files）]** クリックします。

[IPN デバイス構成ファイルの展開とダウンロード（Deploy & Download IPN Device Config files）] は、オンプレミスの NDFC 管理対象サイトと Cloud Network Controller サイトの両方に構成をプッシュし、サイト間のエンドツーエンド インターコネクトを有効にします。

さらに、IPN デバイスを非管理対象として構成していた場合、このオプションは、IPN デバイスからクラウド サイトの C8000V への接続を可能にするための構成情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

ステップ 2 確認ウィンドウで **[はい (Yes)]** をクリックします。

[展開が開始されました。個々のサイトの展開ステータスメッセージについては、左側のメニューを参照してください (Deployment started, refer to left menu for individual site deployment status)] というメッセージにより、インフラ構成の展開が開始されたことが示されます。左側のペインのサイト名の横に表示されるアイコンで、各サイトの進行状況を確認できます。

クラウド テナント情報の提供

ここでは、クラウド テナント情報を追加する方法について説明します。

始める前に

- Nexus Dashboard Orchestrator でクラウド サイトをオンボーディングし、管理する必要があります。

ステップ 1 Orchestrator' の左型のナビゲーションメニューから、**[アプリケーション管理（Application Management）]>>[テナント（Tenants）]** を選択します。

ステップ 2 情報を提供するテナントをクリックするか、**[テナントの追加（Add Tenant）]** をクリックして新しいテナントを追加します。

ステップ 3 クラウド サイトのテナント情報を提供します。

a) **[関連サイト（Associated Sites）]** 領域で、このテナントを関連付けるクラウド サイトを選択します。
b) サイト名の横にある **[編集（Edit）]** アイコンをクリックして、情報を編集します。
c) （任意）**[セキュリティ ドメイン（Security Domains）]** ドロップダウン リストから、セキュリティ ドメインを選択します。

セキュリティドメイン（例では `SecDom1`）を使用すると、両方のグループのユーザーに同じ特権が割り当てられている場合であっても、別のセキュリティドメイン（例では `SecDom2`）のユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、`SecDom1` のセキュリティ ドメインのテナント管理者は、`SecDom2` で構成されたポリシー、プロファイル、またはユーザーを表示できません。

d) テナントのクラウド アカウント情報を提供します。

クラウド テナントとそれらに必要なクラウド アカウント情報の詳細については、クラウド プロバイダーおよびリリースに対応したクラウド ネットワーク コントローラ ユーザー ガイドの「Cisco クラウド ネットワーク コントローラ コンポーネントの構成」の章を参照してください。

e) マルチサイト ドメインに統合する追加のクラウド サイトについて、この手順を繰り返します。

スキーマとテンプレートの作成

このセクションでは、オンプレミス サイトとクラウド サイトのワークロード間ネットワーク接続を可能にする構成を定義するための、スキーマとテンプレートを作成する方法について説明します。

始める前に

- オンプレミスの NDFC ファブリックとクラウド サイト間のサイト インフラおよびサイト間接続を構成しておく必要があります。

ステップ 1 スキーマを新規作成します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。
b) [スキーマ (Schema)] ページで、**[スキーマの追加 (Add Schema)]** をクリックします。
c) スキーマ作成ダイアログで、スキーマの **[名前 (Name)]** と説明（オプション）を入力します。
d) **[追加（Add）]** をクリックして、スキーマの概要ページに移動します。

デフォルトでは、新しいスキーマは空であるため、次の手順に従って 1 つ以上のテンプレートを追加する必要があります。

ステップ 2 テンプレートを作成します。

a) スキーマの概要ページで、**[新しいテンプレートの追加（Add New Template）]** をクリックします。

b) **[テンプレート タイプの選択 (Select a Template type)]** ウィンドウで、テンプレート タイプとして **[NDFC]** を選択します。
c) **[追加 (Add)]** をクリックしてテンプレートを追加します。

ステップ 3 テンプレートの名前とテナントを指定します。

a) 右側のサイドバーで、テンプレートの **[表示名（ Display Name）]** を入力します。
b) **[テナントの選択（Select a Tenant）]** ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

ステップ 4 スキーマビューの右上隅で、**[保存 (Save)]** をクリックしてスキーマとテンプレートを保存します。

ステップ 5 テンプレートをサイトと関連付けます。

a) メイン ペインの **[表示（View）]** ドロップダウンから、テンプレートを選択します。
b) **[アクション（Actions）]** メニューから、**[サイトの関連付け（Site Association）]** を選択します。
c) テンプレートを関連付けるオンプレミスおよびクラウド サイトを選択します。

テンプレートをオンプレミス サイトとクラウド サイトの両方に関連付けると、テンプレートで定義されているすべてのオブジェクトがそれらのサイト間に「ストレッチ」されます。オンプレミス サイトとクラウド サイトにまたがるネットワークのストレッチはサポートされていないため、ネットワークを含むテンプレートをオンプレミス サイトとクラウド サイトに同時に割り当てないでください。

ステップ 6 スキーマビューの右上隅で、**[保存 (Save)]** をクリックしてスキーマとテンプレートを保存します。

NDFC サイトから VRF とネットワークをインポートする

このセクションでは、既存の NDFC ファブリックから VRF とネットワークをインポートする方法について説明します。

（注） グリーンフィールド構成を定義する場合は、このセクションをスキップして、VRF とネットワークの作成 （22 ページ） の説明に従って新しい VRF とネットワークを作成します。

始める前に

- 前のセクションで説明したように、テンプレートを既存のファブリックに関連付ける必要があります。

ステップ 1 メインペインで **[インポート (Import)]** ボタンをクリックし、インポート元の **[サイト (Site)]** を選択します。

インポートできるのは一度に 1 つのファブリックからなので、ファブリックごとにこれらの手順を繰り返します。

ステップ 2 開いた **[<*site-name*>からのインポート（Import from <site-name>）]** ウィンドウから 1 つまたは複数の VRF またはネットワーク（あるいはその両方）を選択します。

a) インポート画面で、既存のオブジェクトのすべてまたは一部を選択できます。

（注） Nexus Dashboard Orchestrator にインポートするオブジェクトの名前は、すべてのサイトにわたって一意にする必要があります。重複する名前を持つ別のオブジェクトをインポートすると、スキーマ検証エラーとなり、インポートに失敗します。同じ名前のオブジェクトをインポートする必要がある場合は、先に名前を変更してください。

b) 選択したオブジェクトに関連するすべてのオブジェクトもインポートする場合は、**[関係を含める（Include Relations）]** オプションをオンにします。

たとえば、インポートするネットワークを選択した場合、このオプションはそのネットワークに関連付けられた VRF を自動的にインポートします。

c) **[インポート (Import)]** をクリックしてオブジェクトをインポートします。

ステップ 3 このステップを繰り返して、ほかのファブリックから追加の構成をインポートします。

インポートしたサイトの下でテンプレートを選択した場合、そのサイトからインポートされたかのように、スイッチとポート構成がネットワークにすでに作成されています。ただし、同じネットワークが存在する別のファブリックでテンプレートを選択した場合、スイッチ構成は空になります。

インポートしたネットワークのインターフェイス構成を取得するには、他のファブリックから同じネットワークを再度インポートする必要があります。

VRF とネットワークの作成

このセクションでは、既存の NDFC ファブリックから VRF とネットワークを作成する方法について説明します。

（注） NDFC ファブリックから既存の VRF とネットワークをインポートする場合は、このセクションをスキップして、代わりに NDFC サイトから VRF とネットワークをインポートする （21 ページ） で説明されている手順に従ってください。

始める前に

- 前のセクションで説明したように、テンプレートを既存のファブリックに関連付ける必要があります。

ステップ 1 VRF を作成するためのスキーマとコントラクトを選択します。

ステップ 2 VRF を作成します。

a) スキーマ編集ビューで、**[オブジェクトの作成 (Create Object)]** > **[VRF]**を選択します。

b) 右側ペインで、VRF の **[表示名 (Display Name)]** を入力します。

c) （任意）**[VRF ID]** を指定します。

VRF の VNI を指定することも、フィールドを空のままにしておくこともできます。VNI は、インフラの設定：Orchestrator 一般設定 （11 ページ）で指定した範囲から NDO によって自動的に割り当てられます。

d) **[VRF プロファイル (VRF Profile)]** ドロップダウンから、VRF プロファイルを選択します。

`Default_VRF_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能な VRF プロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

e) **[VRF 拡張プロファイル (VRF Extension Profile)]** ドロップダウンから、拡張プロファイルを選択します。

`Default_VRF_Extension_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能な VRF 拡張プロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

f) **[ループバックルーティングタグ (Loopback Routing Tag)]** を指定します。

VLAN が複数のサブネットに関連付けられている場合、このタグは各サブネットの IP プレフィックスに関連付けられます。

g) **[直接ルート マップの再配布 (Redistribute Direct Route Map)]** を指定します。

VRF でルートを再配布するためのルート マップ名を指定します。

h) (オプション) **[RT 自動生成の無効化（Disable RT Auto-Generate）]** をオンにして、ルート ターゲットの自動生成を無効にします。

デフォルトで、このオプションがオフになっているときは、ルート ターゲット（RT）がスイッチにより生成され、既存の自動生成されたものに加えて、カスタム RT を生成するように選択できます。このオプションを有効にすると、RT の自動生成が無効になり、カスタム RT のみを使用できます。

i) （オプション）カスタム ルート ターゲットを指定します。

カスタム RT を指定するために、次のフィールドに 1 つ以上の値を入力します。

- **インポート（Import）**：VPN ルート インポート
- **エクスポート（Export）**：VPN ルートのエクスポート用
- **EVPN のインポート（Import EVPN）**：EVPN ルートのインポート用
- **EVPN のエクスポート（Export EVPN）**：EVPN ルートのエクスポート用

有効な値を入力する必要があります（例: `12.2.3.4:2200`）。値を入力すると、UI がその値を検証し、フォーマットが正しくなると、`Create "<value>"` ドロップダウンのオプションが表示されます。

合計で最大 10 個のカスタム ルート ターゲット値を指定できます。

ステップ 3 VRF のサイトローカル プロパティを設定します。

VRF が展開されているすべてのサイトに適用されるネットワークの一般プロパティに加えて、この VRF のサイト固有のプロパティをサイトごとに個別に設定できます。

a) **[テンプレート プロパティ（Template Properties）]** ドロップダウンから、このテンプレートが関連付けられているサイトを選択します。
b) メイン ペインで、ネットワークを選択します。
c) 右側の **[プロパティ (Properties)]** サイドバーで、サイト固有の設定を指定します。

次のサイトローカル プロパティを設定できます。

- **[テナント ルーテッド マルチキャスト (Tenant Routed Multicast)]** をオンにする： テナント ルーテッドマルチキャスト（TRM）は、BGP ベースの EVPN コントロールプレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

  TRMを有効にする場合は、**[RPアドレス (RP Address)]** と **[オーバーレイ マルチキャスト グループ (Overlay Multicast Group)]** も指定する必要があります。

- ランデブーポイント（RP）がファブリックの外部にある場合は、**[RP 外部 (RP External)]** を有効にします。

- **[スタティック リーフの追加 (Add Static Leaf)]** をクリックして、VRF を設定する 1 つ以上のリーフ スイッチを選択します。

  開いた **[スタティック リーフの追加 (Add Static Leaf)]** ウィンドウで、リーフノードを選択します。必要に応じて、VRF の VLAN ID を指定することもできます。

ステップ 4 ネットワークを作成します。

（注） VRF は、NDFC サイトとクラウド ネットワーク コントローラ サイトの両方に関連付けられて拡張されたテンプレートで作成できますが、ネットワークは NDFC サイトにのみ展開できるため、NDFC サイトのみに関連付けられた別のテンプレートで作成する必要があります。

a) テンプレート ビューに戻り、**[オブジェクトの作成（Create Object）]** > **[ネットワーク（Network）]** を選択します。
b) 右側の **[表示名 (Display Name)]** ペインで、ネットワークの名前を入力します。
c) （オプション）**[ネットワーク ID (Network ID)]** を入力します。

ネットワーク ID を指定するか、フィールドを空のままにしておくと、スキーマを保存するときに ID が NDO によって自動的に割り当てられます。

d) これが**[レイヤ 2 専用 (Layer2 Only)]** ネットワークであるかどうかを選択します。
e) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、ネットワーク用の VRF を選択します。

このオプションは、**[レイヤ 2 専用 (Layer2 Only)]** を有効にした場合は使用できません。

f) **[ネットワーク プロファイル (Network Profile)]** ドロップダウンから、ネットワーク プロファイルを選択します。

`Default_Network_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能なネットワークプロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

g) **[ネットワーク拡張プロファイル (Network Extension Profile)]** ドロップダウンから、ネットワーク プロファイルを選択します。

`Default_Network_Extension_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能なネットワーク拡張プロファイルを選択します。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

h) （オプション）ネットワークの **[VLAN ID]** を指定します

i) （オプション）**[VLAN 名 (VLAN Name)]** を指定します。

j) 1 つ以上の**[サブネット (Subnets)]** を追加します。

このオプションは、**[レイヤ 2 専用 (Layer2 Only)]** を有効にした場合は使用できません。

1. **[+ サブネットの追加 (+ Add Subnet)]** をクリックします。

   [**サブネットの追加 (Add Subnet)**] ウィンドウが開きます。

2. **[+ ゲートウェイ IP の追加 (+ Add Gateway IP)]** をクリックし、サブネットの **[ゲートウェイ IP (Gateway IP)]** アドレスを入力します。

   最大 4 つのゲートウェイ IP を設定できます。

3. 追加する最初のゲートウェイに対して `[プライマリ (Primary)]` を選択します。

4. ゲートウェイ情報を保存するには、チェックマークをクリックします。

5. 追加のゲートウェイを提供するには、前のサブステップを繰り返します。

6. **[追加 (Add)]** をクリックして、サブネットの追加を終了します。

k) **[ARP の抑制 (Suppress ARP)]** を行うかどうかを選択します。

l) このネットワークの **[MTU]** を指定します。

m) **[ルーティング タグ (Rounting Tag)]** を指定します。

ステップ 5 ネットワークのサイトローカル プロパティを設定します。

ネットワークが展開されているすべてのサイトに適用されるネットワークの一般的なプロパティに加えて、このネットワークのサイト固有のプロパティをサイトごとに個別に設定できます。

a) **[サイト (SITES)]** の下の左側のサイドバーで、VRFが定義されているテンプレートを選択します。

b) メインペインで、[VRF] を選択します。

c) 右側の **[プロパティ (Properties)]** サイドバーで、サイト固有の設定を指定します。

次のサイトローカル プロパティを設定できます。

- **[テナント ルーテッド マルチキャスト (Tenant Routed Multicast)]** をオンにする： テナント ルーテッドマルチキャスト（TRM）は、BGPベースのEVPNコントロールプレーンを使用するVXLANファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同

じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

- **[L3ゲートウェイボーダーの有効化 (Enable L3 Gateway Border)]** をオンにして、ボーダー ゲートウェイでレイヤ 3 SVIを有効にし、デュアルアタッチド ホストを接続できるようにします。
- **[DHCP ループバック ID (DHCP Loopback ID)]** を入力します。

  値は `0` ー `1023` の範囲にする必要があります。
- **[+ DHCP サーバーの追加 (+ Add DHCP Server)]** をクリックして、1 つ以上の DHCP リレー サーバーを追加します。

  開いた **[DHCP サーバーの追加 (Add DHCP Server)]** ウィンドウで、DHCP リレーの IP アドレスと所属する VRF を入力します。
- **[+ スタティック ポートの追加 (+ Add Static Port)]** をクリックして、ネットワークの VLAN を接続する 1 つ以上のポートを追加します。

  開いている **[静的ポートの追加（Add Static Port）]** ウィンドウで、ポートを含むリーフ スイッチを選択します。必要に応じて、VLAN ID も指定できます。最後に、**[ポートの追加（Add Port）]** をクリックして、ネットワークの 1 つ以上のポートを指定します。

  異なるリーフ スイッチから複数のスタティック ポートを追加する場合は、リーフ スイッチごとにこのプロセスを繰り返す必要があります。

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。