検証済みソリューション：Cisco SD-Access と Cisco SD-WAN の統合

ソリューションの概要　2

ソリューション環境　5

ソリューションの導入例のシナリオ　6

ベストプラクティスと推奨事項　7

改訂：2021 年 5 月 31 日

ソリューションの概要

Cisco Software-Defined Access（SD-Access）アーキテクチャは、従来のキャンパス LAN 設計から進化した Cisco DNA です。SD-Access では、Cisco DNA Center を使用して、キャンパスの有線/ワイヤレスネットワークの設計、プロビジョニング、ポリシー適用、および提供を確実に行うことができます。

Cisco SD-WAN は、単一のファブリックを介して複数のサイトを接続するオーバーレイ WAN アーキテクチャです。Cisco SD-WAN アーキテクチャは、個別のオーケストレーション、管理、コントロール、およびデータの各プレーンで構成されています。vBond コントローラは、SD-WAN オーバーレイへの SD-WAN ルータの自動オンボーディングを提供します。vManage コントローラは、一元的な設定とモニタリングの役割を担います。vSmart コントローラは、SD-WAN ネットワークの中央集中型コントロールプレーンの役割を担います。WAN エッジは、他の WAN エッジとのセキュアなデータプレーン接続を確立します。

Cisco SD-Access と SD-WAN の統合により、Cisco SD-WAN ファブリックを介して複数の Cisco SD-Access サイトを接続できます。SD-Access SD-WAN 統合には次の 2 タイプがあります。この検証済みソリューションは、両方のタイプを対象としています。

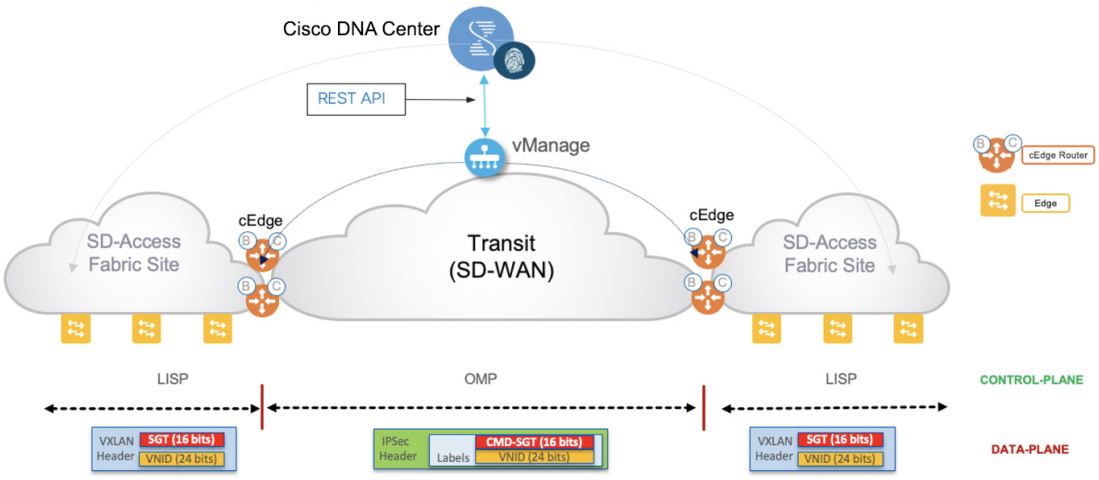
- 1 ボックス統合
- 手動 2 ボックス統合

ソリューション環境には、手動 2 ボックス統合を使用して展開されたメインサイトと、1 ボックス統合および手動 2 ボックス統合ソリューションを使用して展開されたブランチサイトが含まれます。さらに、2 ボックスサイトでは、インライン セキュリティグループタグ（SGT）のタギングと IPv4 マルチキャスト機能が有効化されています。このソリューションでは、1 ボックス統合ソリューションと手動 2 ボックス統合ソリューションの相互運用性を検証しています。

SD-Access SD-WAN 1 ボックス統合

SD-Access SD-WAN 1 ボックス統合は、SD-Access ファブリックへの SD-WAN cEdge の展開、エンドツーエンドのセグメンテーション、および企業全体での一貫性のあるポリシー適用を自動化します。Cisco DNA Center は、vManage と連携し、REST API を介してアンダーレイおよびファブリックの設定指示をプッシュします。 vManage は、これらの指示を受け取り、NETCONF を介して cEdge をプロビジョニングします。cEdge デバイスレベルでは、1 ボックス統合により、SD-WAN ルータと SD-Access ファブリックボーダーの機能が 1 つのボックスに統合されます。

図 *1 : SD-Access SD-WAN 1* ボックス統合アーキテクチャ



SD-Access SD-WAN 1 ボックス統合ソリューションには、次の特性があります。

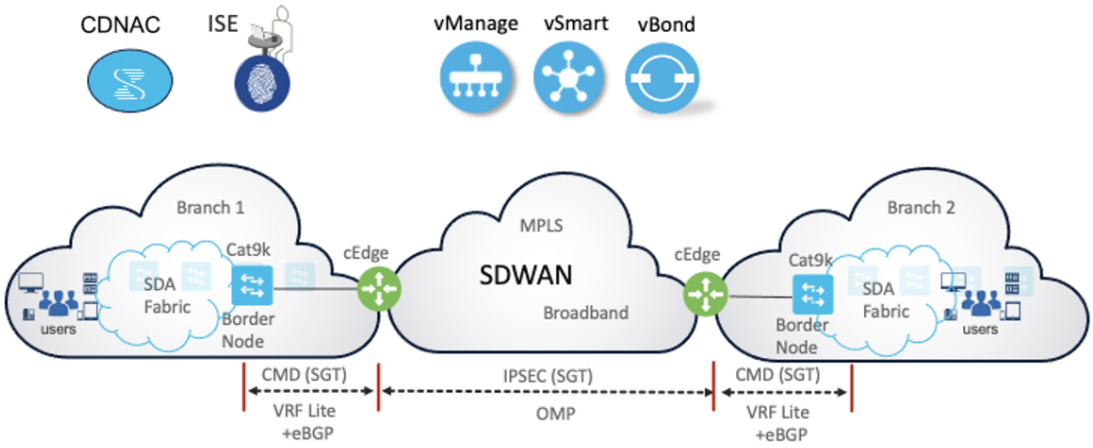
- Cisco DNA Center は REST API を介して設定変更を vManage に伝達します。
- vManage は NETCONF を介して設定変更を cEdge にプッシュします。
- cEdge は SD-WAN ルータとコロケーション ファブリックボーダー（外部ボーダー/場所を問わないボーダー＋コントロールプレーン）の両方として機能します。
- cEdge は VXLAN を終端し、SD-Access ファブリックに参加します。
- cEdge は SD-WAN ファブリックを通過するトラフィックを暗号化します。
- cEdge はコントロールプレーンで OMP-LISP ルートの再配布を実行します。
- cEdge は SD-WAN データプレーンを介して SGT を抽出および転送します。

SD-Access SD-WAN 手動 2 ボックス統合（インライン SGT および IPv4 マルチキャスト対応）

SD-Access SD-WAN 手動 2 ボックス統合では、Cisco DNA Center および vManage は統合されません。SD-Access 仮想ネットワークは、VRF-Lite と eBGP を使用して SD-WAN VPN に手動でマッピングされます。cEdge ルータ上の BGP と OMP 間におけるルートの相互再配布により、2 つの SD-Access サイトの仮想ネットワークが SD-WAN ファブリックを介して通信できるようになります。

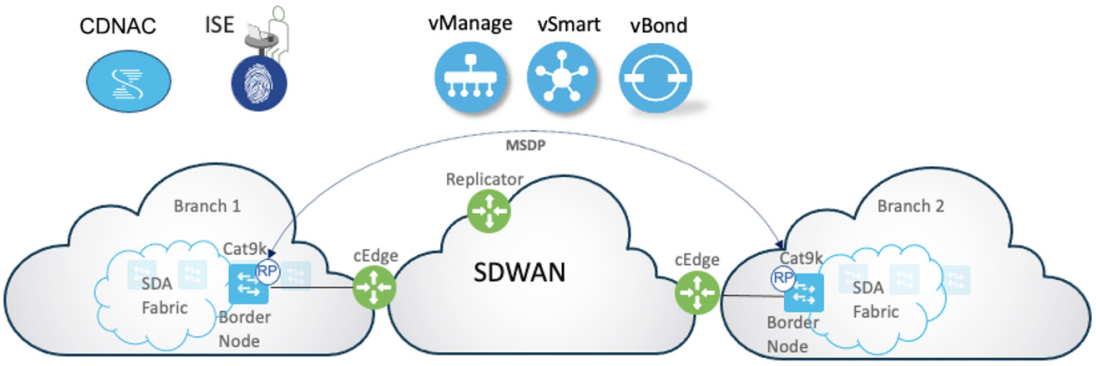
以前は、フレームが SD-WAN ファブリックを通過するときに SGT コンテキストが失われていました。SD-WAN 17.3.1/20.3.1 では、Cisco TrustSec が導入されたため、Cisco Catalyst 9000 スイッチによって生成された SGT を他の SD-WAN ルータに伝播できます。Cisco TrustSec を有効にすると、SGT がエンドツーエンドで維持され、1 ボックスサイトと 2 ボックスサイトの間でドメイン全体にわたり一貫性のあるポリシー適用が可能になります。

図 *2 : SD-Access SD-WAN* 手動 *2* ボックス統合（インライン *SGT* 対応）



SD-Access SD-WAN 1 ボックス統合は、IPv4 マルチキャストを現在サポートしていません。したがって、SD-WAN ファブリックを介して複数の SD-Access サイト間で IPv4 マルチキャストを伝送できるようにするには、SD-Access SD-WAN 手動 2 ボックス統合を実装します。SD-WAN での IPv6 マルチキャストは現在サポートされていません。図 3 は、各 SD-Access サイトのファブリックボーダーに設定されたマルチキャスト RP を示しています。サイト固有のマルチキャスト送信元をリモートマルチキャスト RP に伝達するように、両方の SD-Access サイトのマルチキャスト RP 間で MSDP ピアリングが設定されています。

図 *3 : SD-Access SD-WAN* 手動 *2* ボックス統合（*IPv4* マルチキャスト対応）



ハードウェアと仕様

ソリューションは、次の表に示すハードウェアとソフトウェアでテストされています。

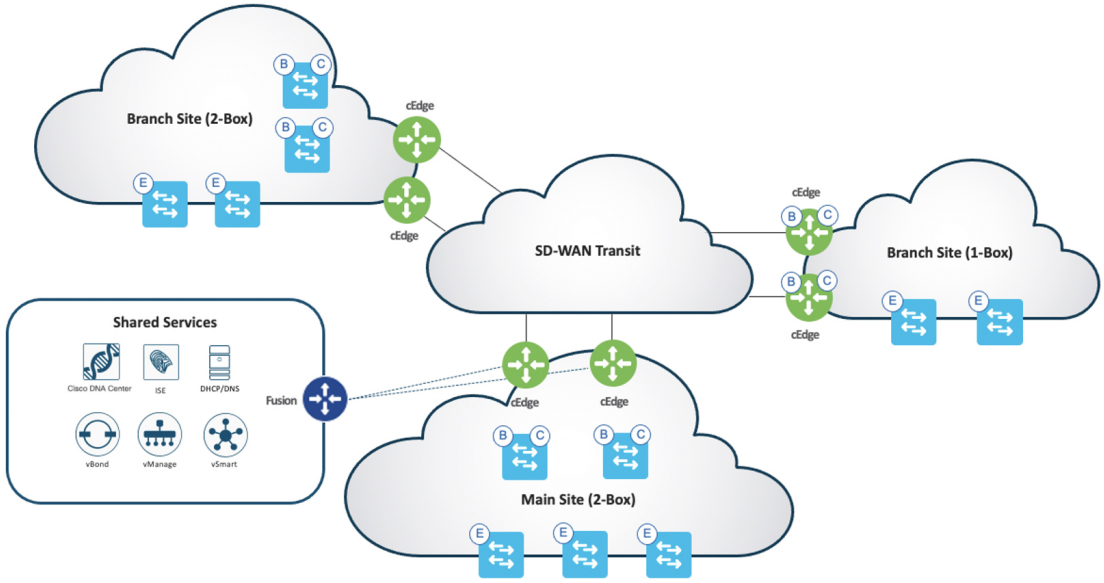
ロール	ハードウェア プラットフォーム	ソフトウェア リリース
Cisco DNA Center コントローラ	DN2-HW-APL	2.1.2.4
Cisco Identity Service Management - RADIUS サーバ	仮想（ISE-VM-K9）プラットフォーム	2.6 パッチ 6
Cisco SD-WAN NMS コントローラ	vManage	20.3.2

ロール	ハードウェア プラットフォーム	ソフトウェア リリース
Cisco SD-WAN エッジ	ASR1002-X ASR1001-HX ISR4K	17.3.2
Cisco SDA ファブリックエッジ	サポートされているすべての Catalyst 9000 エッジ C9300/C9400/C9500	17.3.2

ソリューション環境

トポロジ

図 *4 : SD-Access SD-WAN* 統合のトポロジ



この図は、ソリューション環境の論理トポロジを示しています。

- コントローラによる統合：Cisco DNA Center、Cisco ISE クラスタ、SD-WAN コントローラ（vManage、vBond、vSmart）。
- Cisco DNA Center、Cisco ISE、DHCP/DNS サービス、および SD-WAN コントローラは共有サービスセグメントに存在します。
- Cisco DNA Center は、INFRA_VN 仮想ネットワーク上のアンダーレイ グローバル ルーティング テーブルを使用して、SD-WAN 経由でファブリックデバイスと通信します。INFRA_VN 仮想ネットワークは、ユーザ定義のサービス VPN にマッピングされています。

- フュージョンルータにより、共有サービスセグメントが SD-Access ファブリックに接続されます。フュージョンルータは、INFRA_VN にマッピングされたサービス VPN に対応する cEdge サービスインターフェイスに接続されています。
- メインサイトは、手動 2 ボックス統合ソリューションを使用して展開されています。
- ブランチサイトは、1 ボックス統合または 2 ボックス統合ソリューションを使用して展開されています。
- エンドツーエンドのトラフィックは、メインサイト、ブランチサイト、およびインターネットを通過します。

スケール

ソリューションテストで検証した規模を次の表に示します。ハードウェアキャパシティについては、『Cisco DNA Center Data Sheet』を参照してください。

カテゴリ（Category）	値
ファブリックサイトの数	100
ファブリックサイトあたりの IP プール数	100
SGT	1000
VN	10
エンドポイント	10,000
トラフィックプロファイル（ユニキャスト/マルチキャスト）	アプリケーション TCP/UDP トラフィック IMIX

ソリューションの導入例のシナリオ

SD-Access SD-WAN 統合ソリューションは、次の導入例をサポートします。

- SD-Access SD-WAN 1 ボックス統合
  - 1 ボックスブランチサイトでの LAN 自動化
  - 手動アンダーレイ + OSPF
  - ブランチサイトでのダイレクト インターネット アクセス
  - ブランチサイトでメインサイトを介してデフォルトトラフィックをルーティング
  - ハブアンドスポーク
  - TLOC Extension
- SD-Access SD-WAN 手動 2 ボックス統合
  - インライン SGT

- IPv4 および IPv6 ユニキャスト
- IPv4 マルチキャスト

- SD-WAN を介した SD-Access サイト間のエンドツーエンドのインライン SGT

ベストプラクティスと推奨事項

ここでは、ソリューションの展開に役立つテクニカルノートについて説明します。

SD-Access SD-WAN 1 ボックス統合の設計上の考慮事項

- 1 ボックスの各サイトには、最大 2 つのコロケーション ファブリック ボーダー（外部ボーダーまたは場所を問わないボーダー）を配置できます。
- 内部専用ファブリックボーダーはサポートされていません。
- SDA 中継への cEdge 接続はサポートされていません。
- SD-WAN を介した IPv4 マルチキャストはサポートされていません。
- IP 中継への cEdge 接続がサポートされています。
- アンダーレイは、LAN 自動化または手動アンダーレイを使用して設定できます。

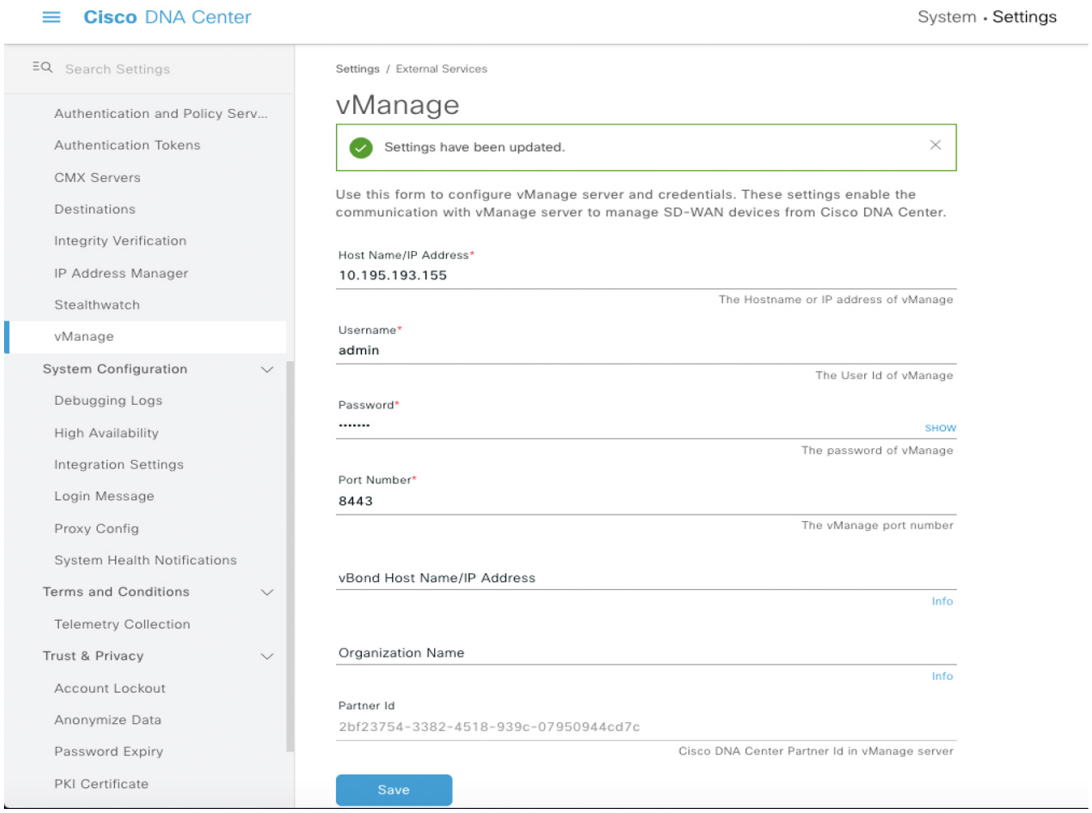
SD-Access SD-WAN 1 ボックス統合の前提条件

- SD-WAN コントローラがインストールされ、有効な証明書を使用して設定されている。
- cEdge が SD-WAN ファブリックにオンボーディングされている。
- Cisco DNA Center がインストールされ、Cisco ISE と統合されている。
- Cisco DNA Center のサイト階層、ログイン情報、仮想ネットワーク、IP プールが設定されている。

SD-Access SD-WAN 1 ボックス統合のワークフロー

手順

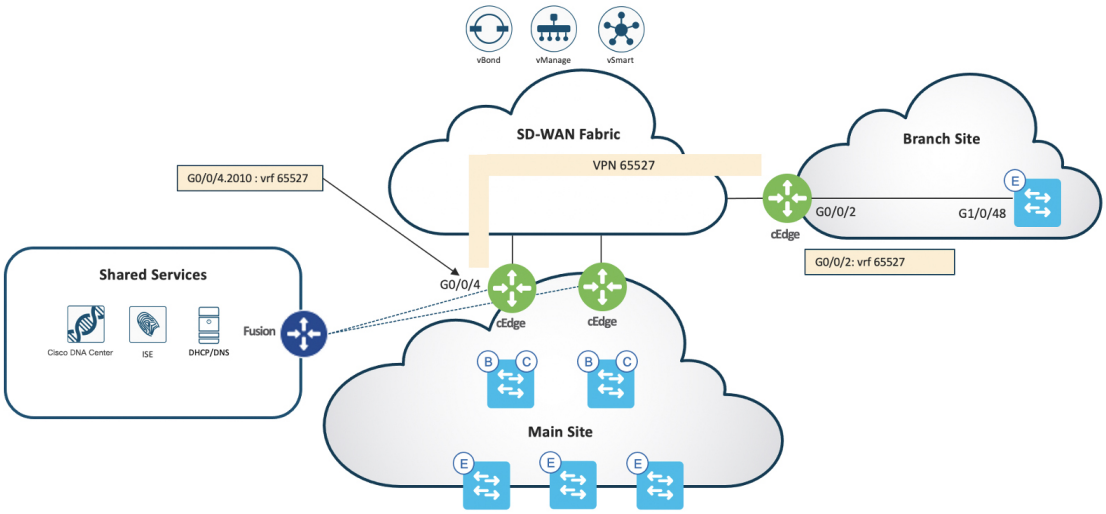
ステップ 1　Cisco DNA Center の [vManage] 設定ページから、vManage への接続および信頼を確立します。



ステップ 2 SD-WAN ファブリックを介した Cisco DNA Center と SD-Access ファブリックデバイスとの間のアンダーレイの到達可能性を実現するために、サービス VPN を設定します。

次の図では、アンダーレイトラフィック用にメインサイトの cEdge とリモートブランチの cEdge との間で VPN 65527 が設定されています。VPN 65527 は、Cisco DNA Center で INFRA_VN にマッピングされるユーザ定義の VPN です。メインサイトの cEdge は、フュージョンルータに接続された VPN 65527 のサービス側インターフェイスを使用して設定されています。これにより、Cisco DNA Center が存在する共有サービスネットワークとリモート SDA ファブリックデバイスとの間に SD-WAN を介したパスが確立されます。メインサイトの cEdge には、サービス側インターフェイスを介した Cisco DNA Center への IP 到達可能性があります。ブランチの cEdge には、サービス VPN 65527 を介した Cisco DNA Center への IP 到達可能性があります。

図 *5*：アンダーレイのサービス *VPN*



ステップ 3　cEdge デバイステンプレートでユーザトラフィック用のサービス VPN を設定します。

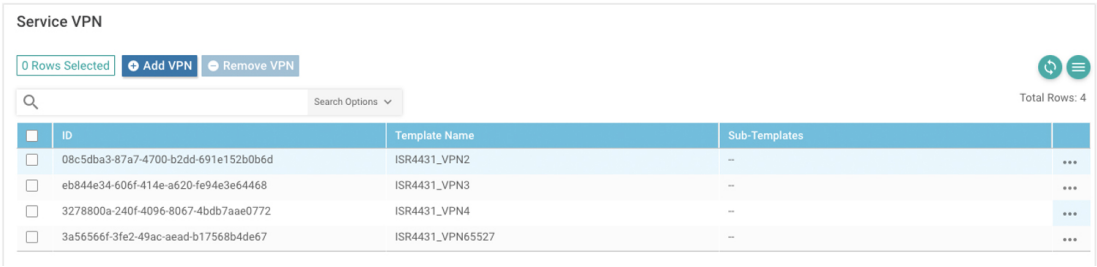
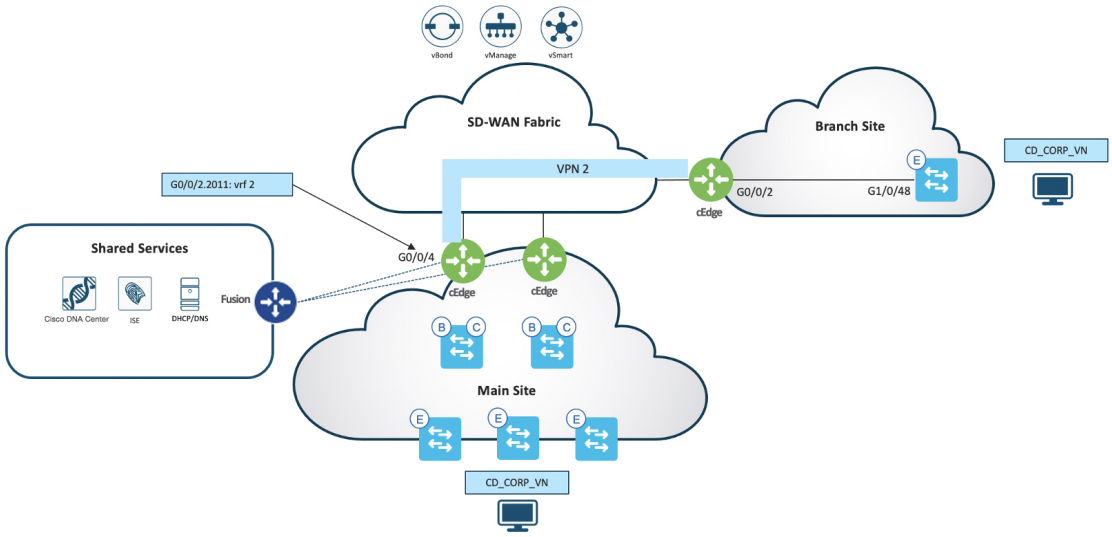
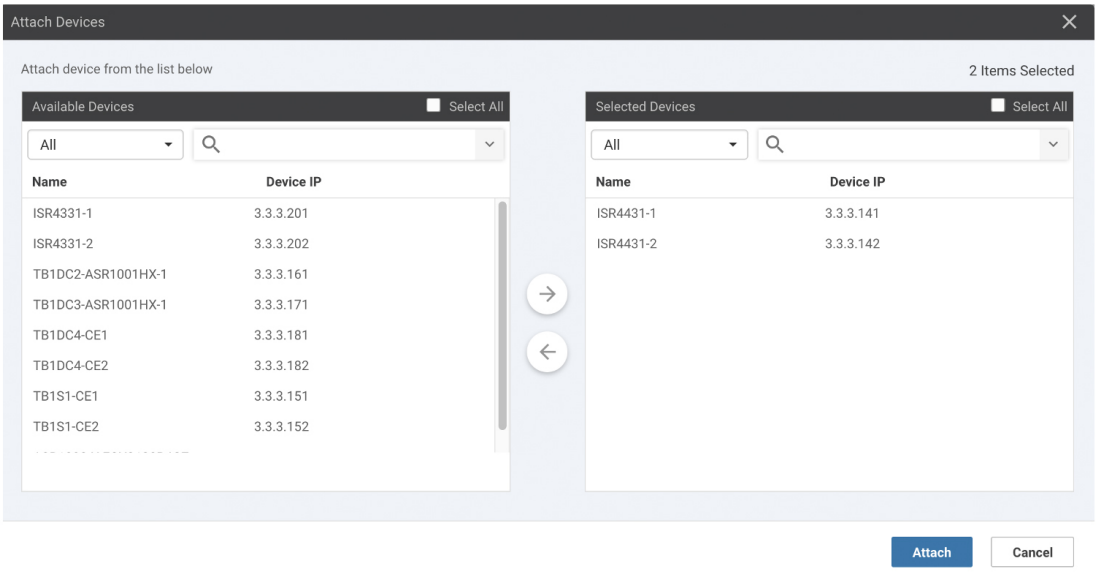


図 6 は、CD_CORP_VN と VPN 2 の間のマッピングを示しています。トラフィックが SD-WAN を経由して SD-Access サイト間を移動する際に、VPN 間のマッピングを使用して、エンドツーエンドのセグメンテーションが適用されます。

図 *6* : ユーザ *VN* のサービス *VPN*

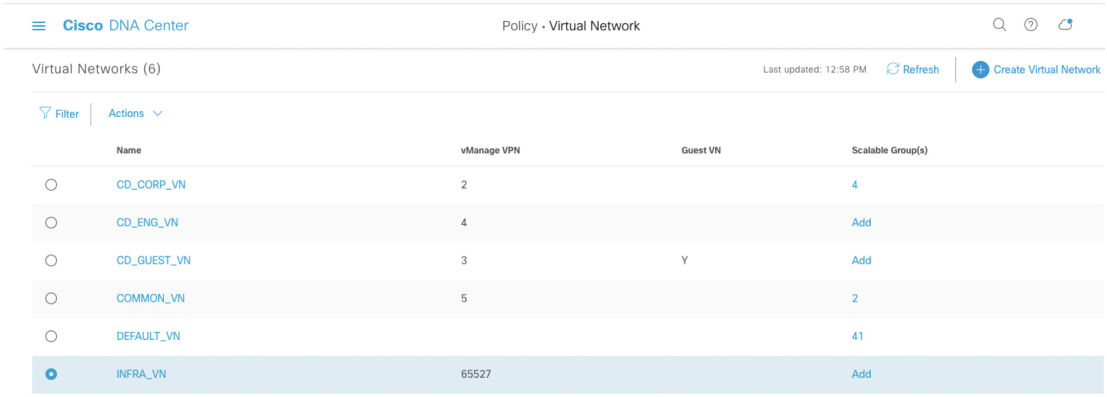


ステップ 4　**[vManage Administration]** > **[Integration Management]** で cEdge デバイスを Cisco DNA Center パートナー統合に接続します。

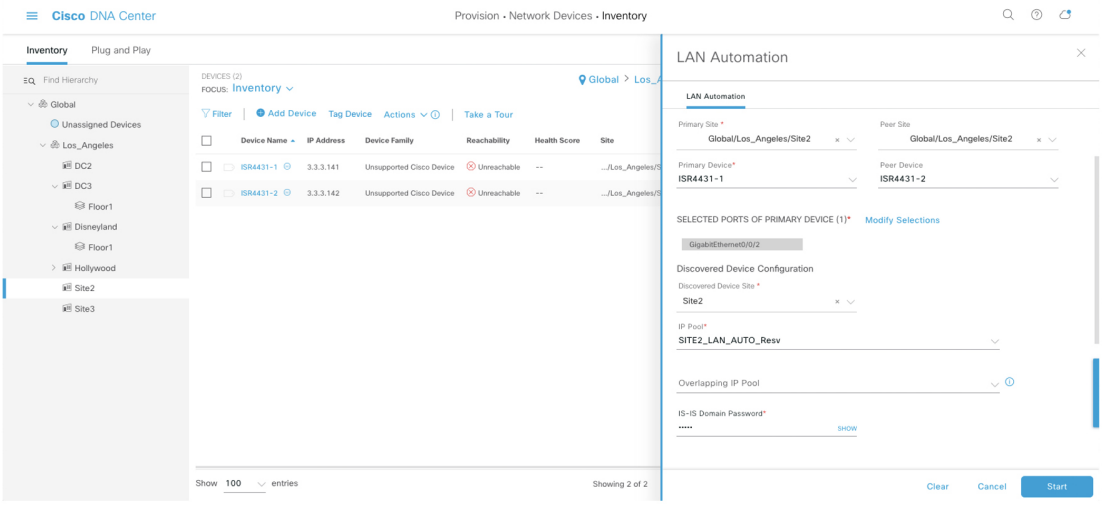


ステップ 5　Cisco DNA Center で cEdge デバイスをサイトに割り当てます。

ステップ 6　**[Cisco DNA Center]** > **[Policy]** > **[Virtual Network]** ページで、SD-Access 仮想ネットワークを SD-WAN VPN にマッピングします。



ステップ 7 cEdge をシードとして LAN 自動化を実行し、リモートファブリックエッジにアンダーレイをプロビジョニングします。



ステップ 8 Cisco DNA Center でデバイスをプロビジョニングします。

ステップ 9 Cisco DNA Center で cEdge デバイスを [External-Only] または [Anywhere Borders + Control Plane] としてファブリックに追加します。

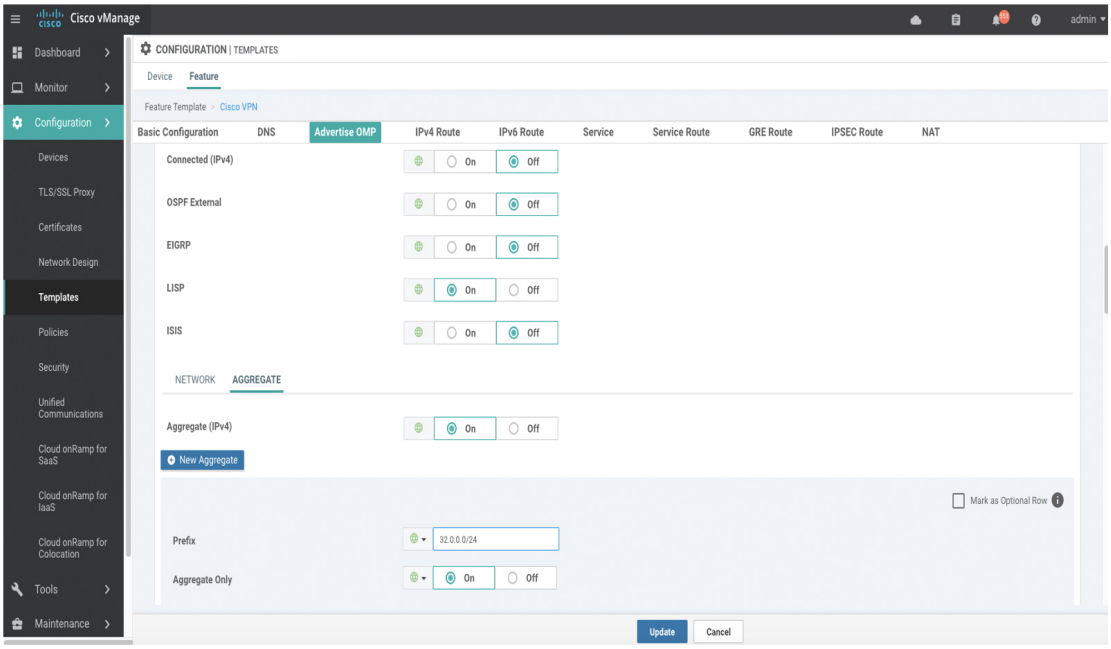
ステップ 10 Cisco DNA Center でファブリックエッジデバイスをファブリックに追加します。

ステップ 11 Cisco DNA Center で SD-Access ホストのオンボーディングを設定します。

SD-Access SD-WAN 1 ボックス統合：ネットワークのトラブルシューティング

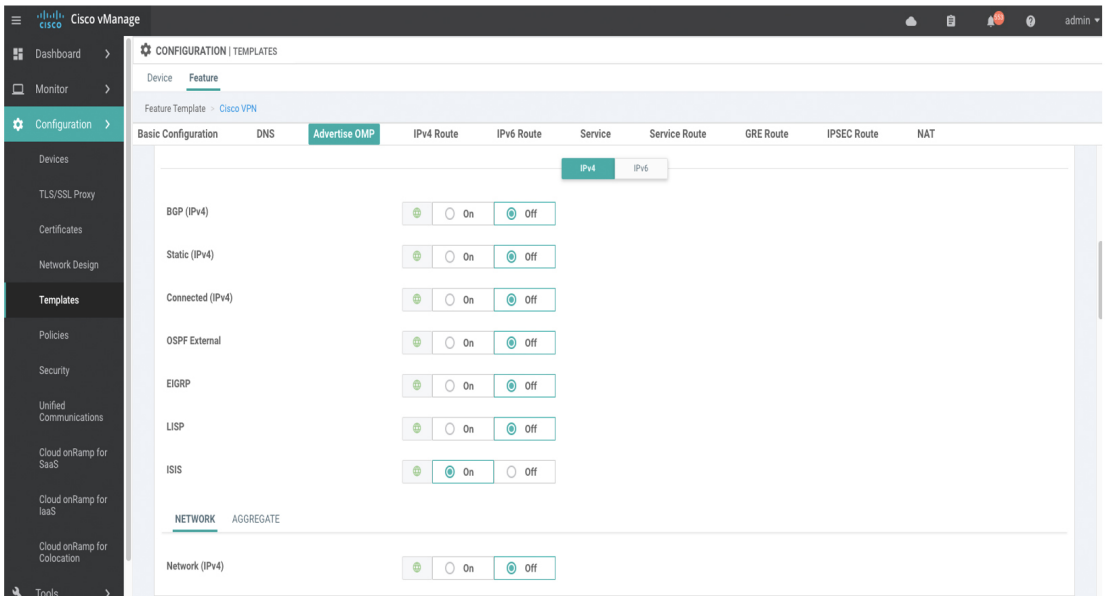
1. **問題**：複数のサイトにまたがる SD-Access 仮想ネットワーク間に到達可能性がない。

   サービス VPN テンプレートの OMP で **LISP をアドバタイズする**オプションが選択されていることを確認します。OMP で /32 ホストプレフィックスをアドバタイズしないように、ローカル SD-Access ネットワークに対してネットワーク集約を設定する必要があることに注意してください。



2. **問題**：Cisco DNA Center からリモート ファブリック デバイスへのアンダーレイの到達可能性がない。

   INFRA_VN にマッピングされた VPN の OMP に内部ゲートウェイプロトコル（OSPF/ISIS/EIGRP）がアドバタイズされていることを確認します。

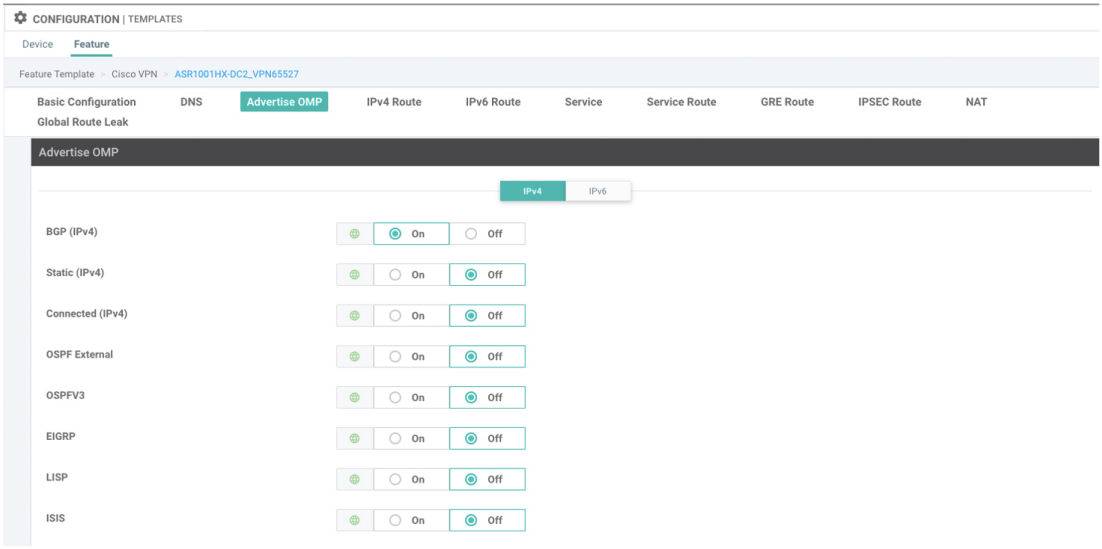


SD-Access SD-WAN 手動 2 ボックス統合のワークフロー

手順

ステップ 1 cEdge のアンダーレイおよびユーザトラフィック用のサービス VPN を設定します。

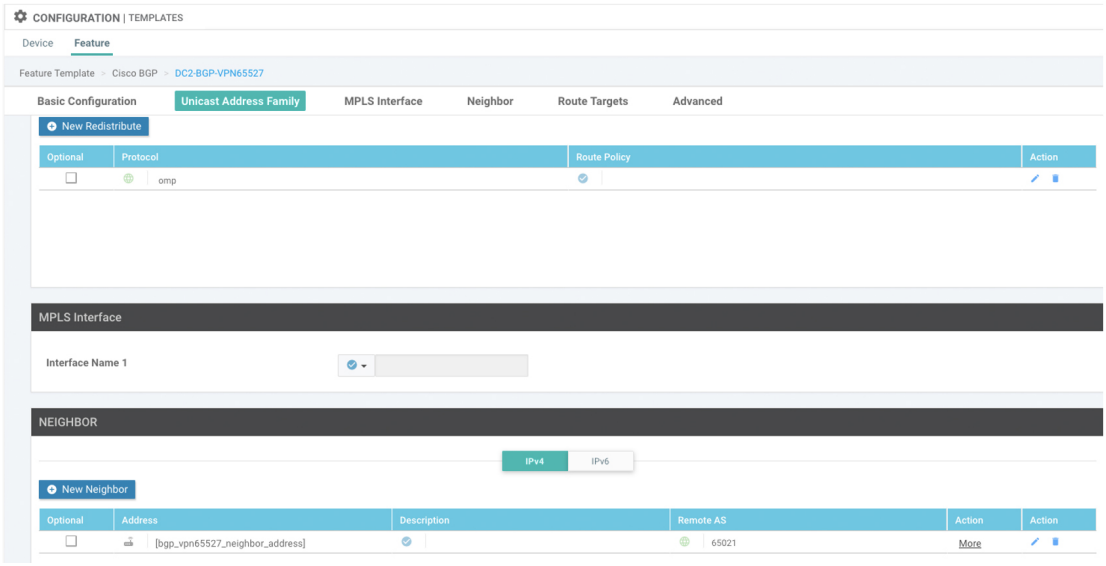
VPN テンプレートで、BGP を OMP にアドバタイズします。



ステップ 2 cEdge のアンダーレイトラフィック用のサービス VPN サブインターフェイス、およびファブリックボーダーの対応するグローバル SVI インターフェイスを設定します。

ステップ 3 cEdge のサービスインターフェイス（vrf65527）とファブリックボーダーのグローバル SVI インターフェイスとの間で eBGP を設定します。

a) BGP テンプレートで、cEdge の BGP に OMP を再配布します。



b) ファブリックボーダーで BGP/IGP の再配布を手動で設定します。

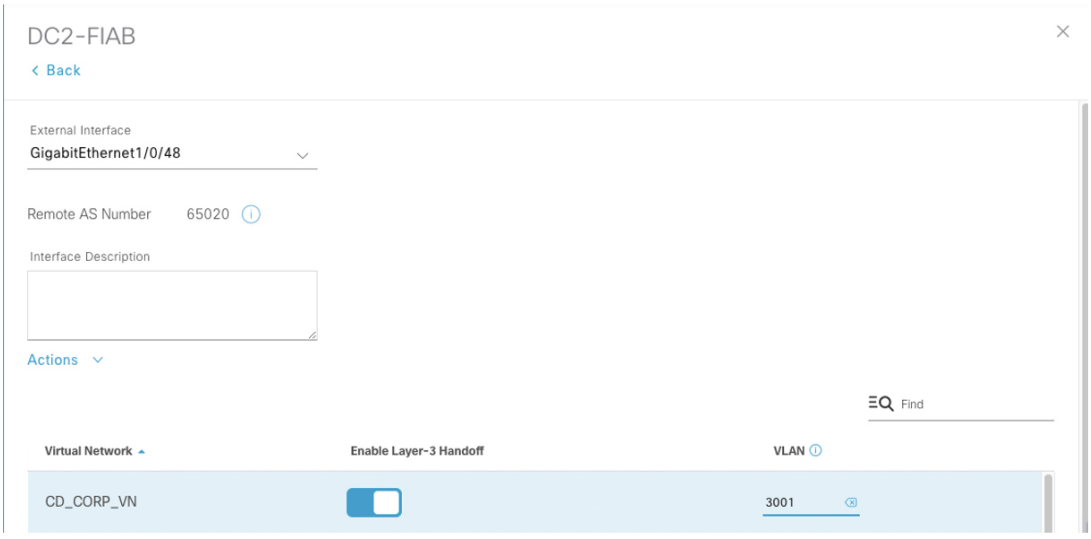
ステップ 4 Cisco DNA Center への IP 到達可能性が確立された後、Cisco DNA Center でファブリックデバイスを検出します。

ステップ 5 デバイスをサイトに追加し、Cisco DNA Center でプロビジョニングします。

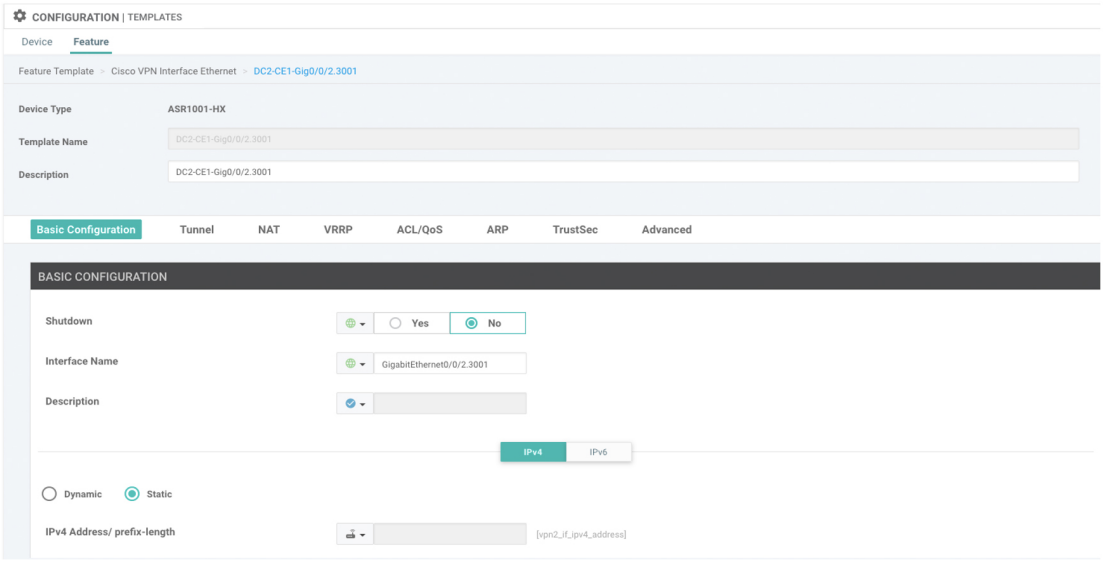
ステップ 6 Cisco DNA Center でデバイスをファブリックボーダーとして追加します。

ステップ 7 Cisco DNA Center で SD-Access ファブリックボーダーのレイヤ 3 ハンドオフを設定します。

SVI VLAN 番号は、Cisco DNA Center によって動的に割り当てることも、手動で割り当てることもできます。これらの VLAN 番号は、対応する cEdge サブインターフェイスの dot1q の番号と一致する必要があります。



ステップ 8 cEdge の対応するサブインターフェイスを設定します。



ステップ 9 ファブリックボーダーと cEdge とでレイヤ 3 インターフェイスの IP MTU を一致させます。

cEdge

```
interface GigabitEthernet0/0/2.3001
 encapsulation dot1Q 3001
 vrf forwarding 2
 ip address 124.1.32.1 255.255.255.0
 no ip redirects
 ip mtu 1496
```

SD-Access ファブリックボーダー

```
interface Vlan3001
 vrf forwarding CD_CORP_VN
 ip address 124.1.32.2 255.255.255.0
 ip mtu 1496
```

ステップ 10 各 VRF/VPN でファブリックボーダーと cEdge の間の eBGP を有効にします。

ステップ 11 BGP ルートを OMP にアドバタイズし（VPN テンプレート）、OMP ルートを cEdge の BGP に再配布します（BGP テンプレート）。

SD-Access と SD-WAN の手動 2 ボックス統合（インライン SGT 対応）の注意事項

- **cts manual** で TrustSec を有効にすると、一時的にインターフェイスでフラッピングが発生します。ベストプラクティスとして、まず SD-WAN ルータで TrustSec を設定してください。次に Cisco Catalyst スイッチで TrustSec を有効にしてください。
- ベストプラクティスとして、cEdge の物理インターフェイスとサブインターフェイスの両方で **cts manual** を設定してください。

ファブリックボーダーと cEdge 間のインライン SGT の有効化

次の設定例は、ファブリックボーダーと cEdge の間でインライン SGT を有効にする方法を示しています。

SD-Access ファブリックボーダー

```
interface GigabitEthernet1/0/48
 description To cEdge
 switchport mode trunk
 cts manual
  policy static sgt 2 trusted
```

cEdge

```
interface GigabitEthernet0/0/3
 description To Fabric Border
 no ip address
 ip mtu 1500
 negotiation auto
 cdp enable
 cts manual

interface GigabitEthernet0/0/3.3002
 encapsulation dot1Q 3002
 vrf forwarding 2
 ip address 124.1.34.1 255.255.255.0
 no ip redirects
 ip mtu 1496
 ip pim sparse-mode
 cts manual
  policy static sgt 2 trusted
```

SD-Access と SD-WAN の手動 2 ボックス統合（IPv4 マルチキャスト対応）：設計上の考慮事項と注意事項

- エニーキャスト RP は cEdge では現在サポートされていません。推奨される方法は、SD-Access ファブリックボーダーなどの非 cEdge デバイスにマルチキャスト RP を展開することです。
- SD-Access マルチキャストは、ネイティブマルチキャスト モードまたはヘッドエンド レプリケーション モードで展開できます。
- SD-Access ネイティブマルチキャストは、アンダーレイの Source Specific Multicast（SSM; 送信元特定マルチキャスト）に依存します。SD-Access ネイティブマルチキャスト モードを使用する場合は、ファブリック ノードと中間ノードのアンダーレイで SSM 設定が設定されていることを確認してください。

ファブリックボーダーのネイティブマルチキャスト アンダーレイの設定例

```
!Enable multicast and ip pim ssm globally

ip multicast-routing
ip pim ssm default

!Enable ip pim sparse-mode on Loopback0 and L3 interfaces

interface Loopback0
 ip pim sparse-mode

!Enable ip pim sparse-mode on all uplinks to cEdges and on iBGP links
```

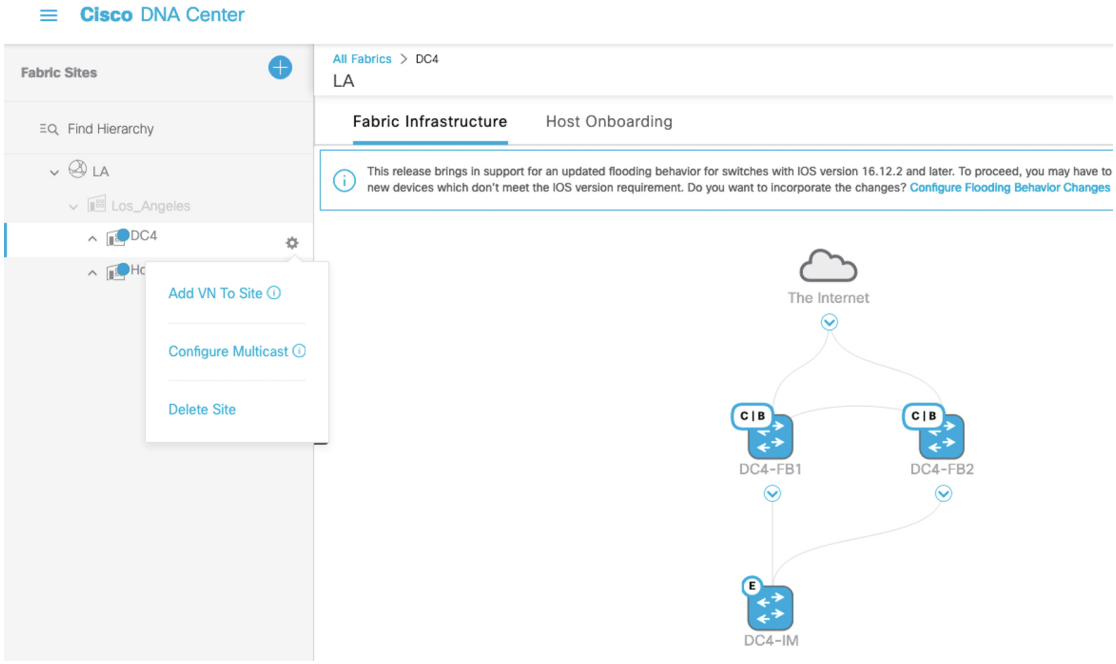
```
interface vlan 3012
 ip pim sparse-mode

!Enable ip pim sparse mode downlinks to Intermediate Nodes/Fabric Edge Nodes

interface GigabitEthernet1/0/x
 ip pim sparse-mode
```

SD-Access SD-WAN IPv4 マルチキャストのワークフロー

手順

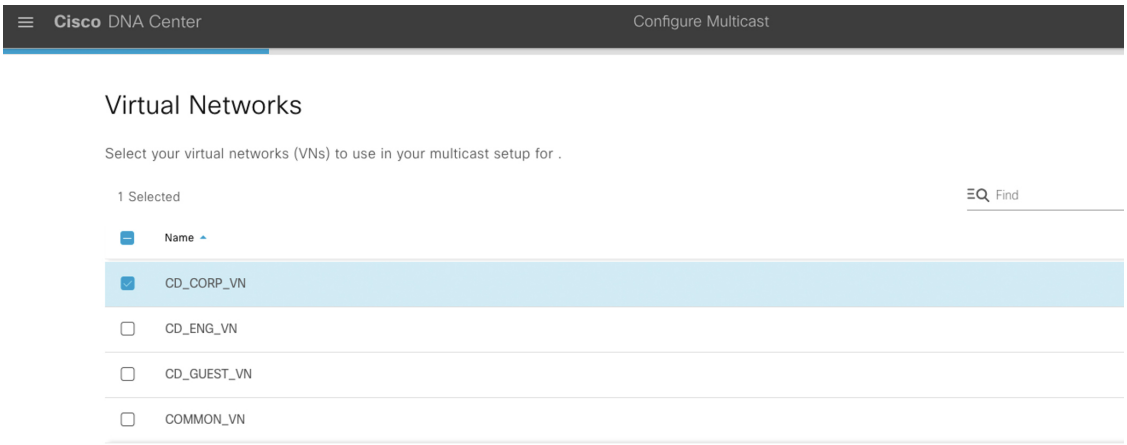
ステップ 1 ファブリックボーダーをマルチキャスト RP として、仮想ネットワークで SD-Access マルチキャストを有効にします。

a) サイトレベルでマルチキャストを設定します。

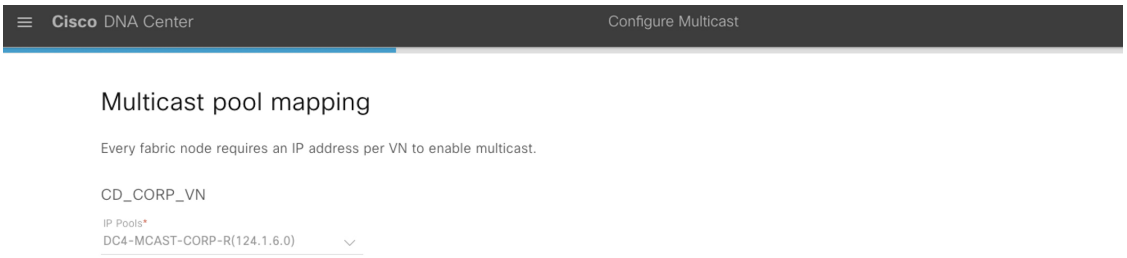


b) [Native multicast] または [Head-end replication] オプションボタンをクリックします。

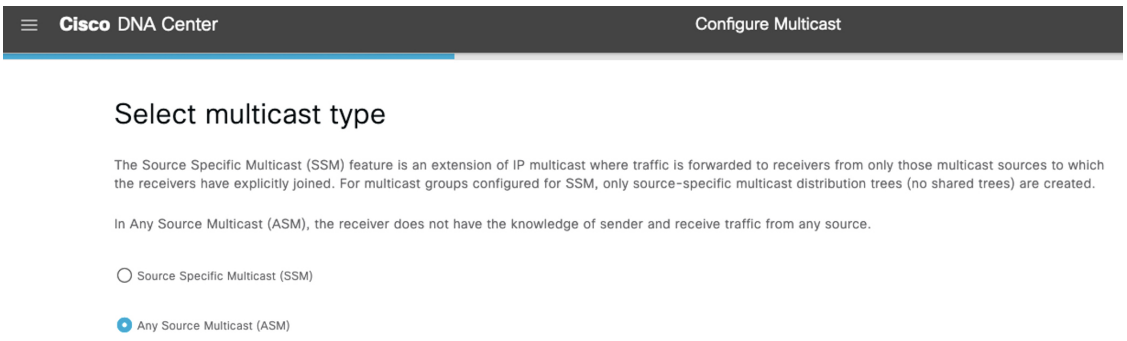
c) サイトのマルチキャスト設定で使用する仮想ネットワーク（VN）を選択します。



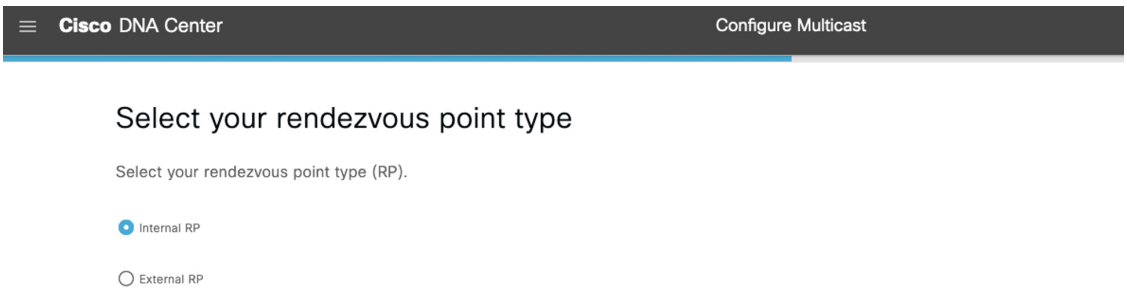
d) マルチキャストを有効にするために、各 VN のファブリックノードに IP アドレスを割り当てる IP プールを選択します。



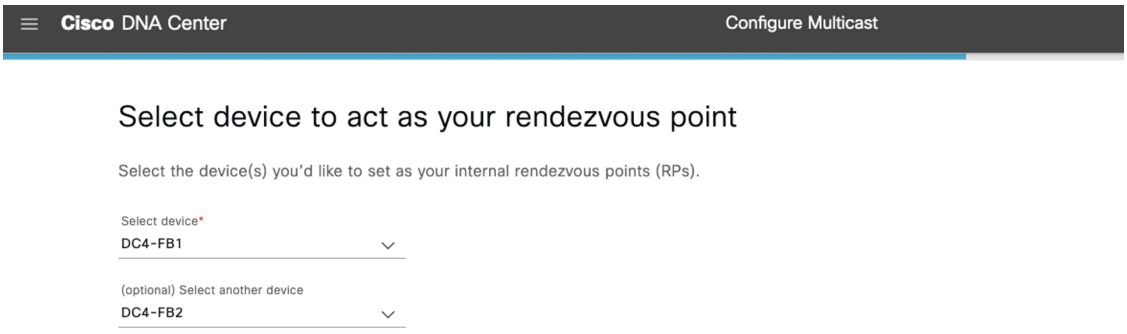
e) [Any Source Multicast (ASM)] オプションボタンをクリックします。



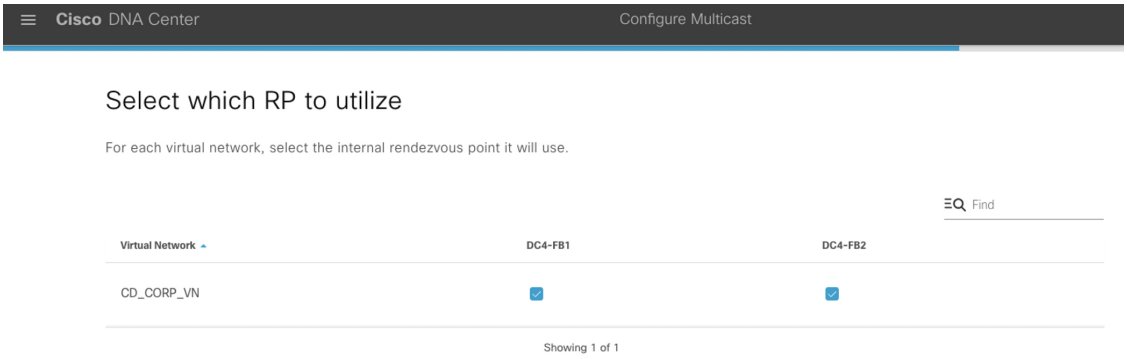
f) [Internal RP] オプションボタンをクリックします。



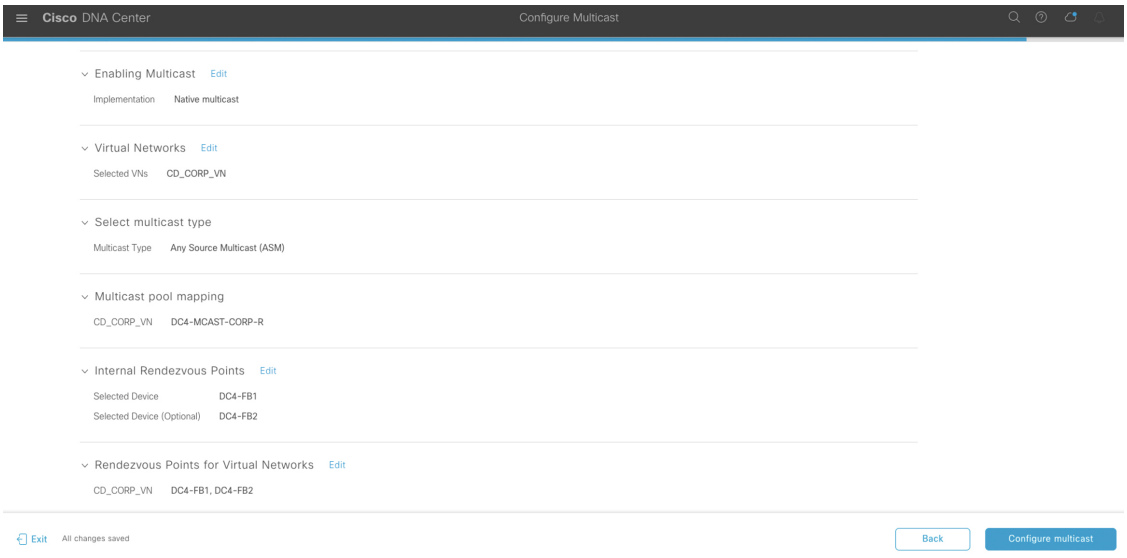
g) 内部 RP として設定するファブリックボーダーを選択します。



h) 各 VN の内部 RP を選択します。

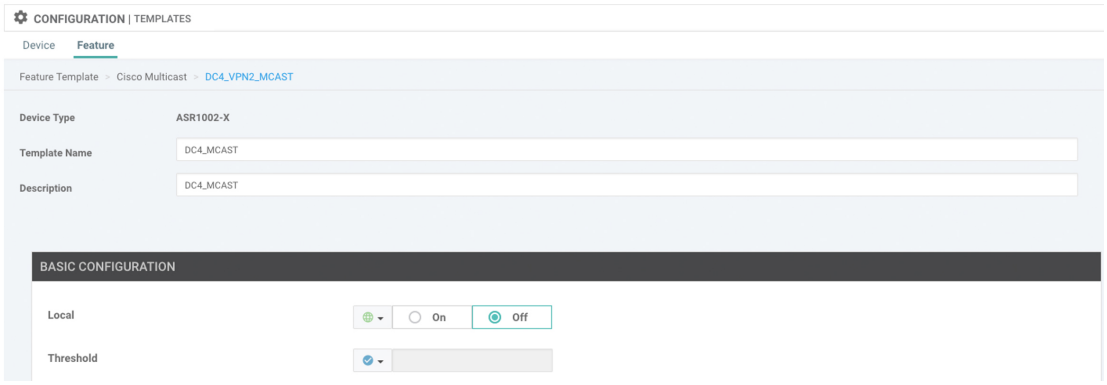


i) マルチキャスト設定の概要を確認し、[Configure multicast to deploy] をクリックします。

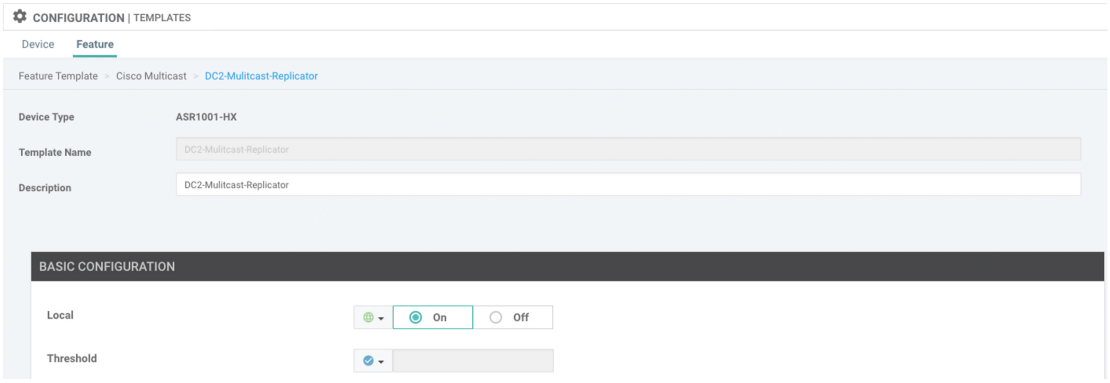


ステップ 2 サービス VPN で SD-WAN マルチキャストを有効にします。

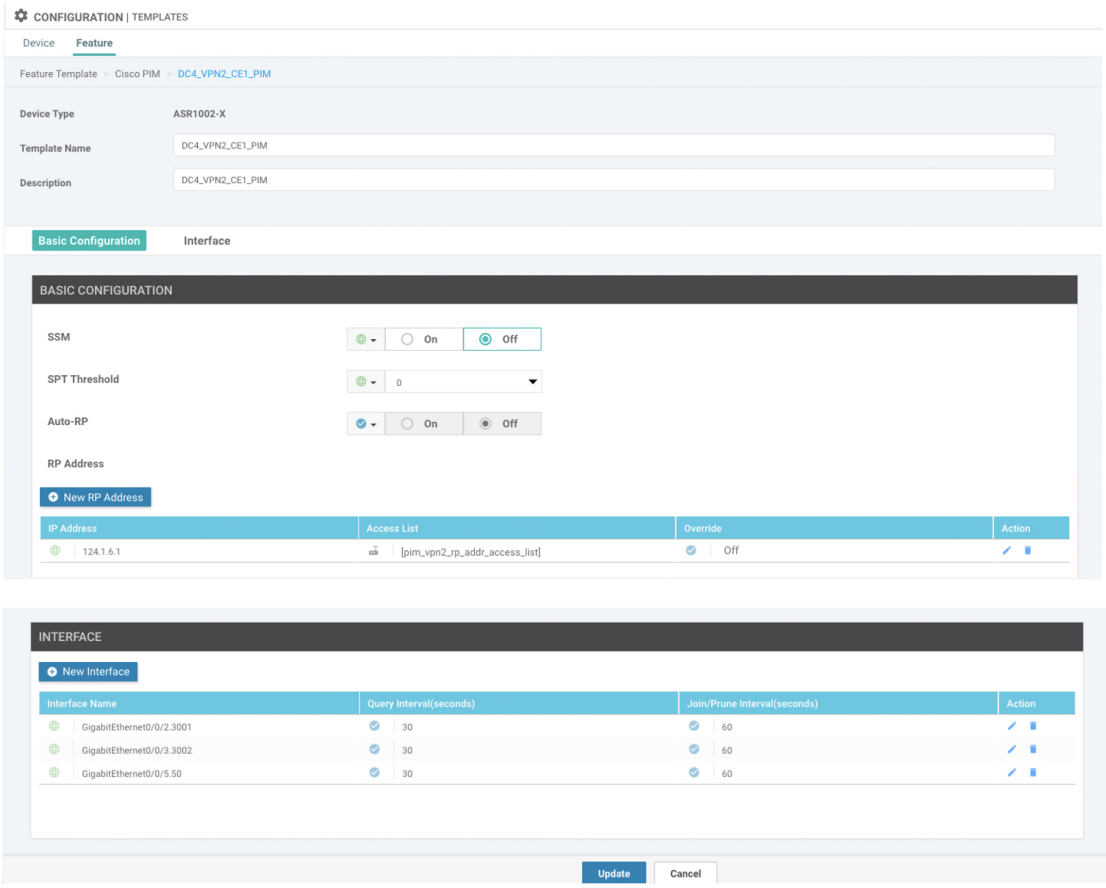
a) サービス VPN マルチキャストテンプレートを設定します。



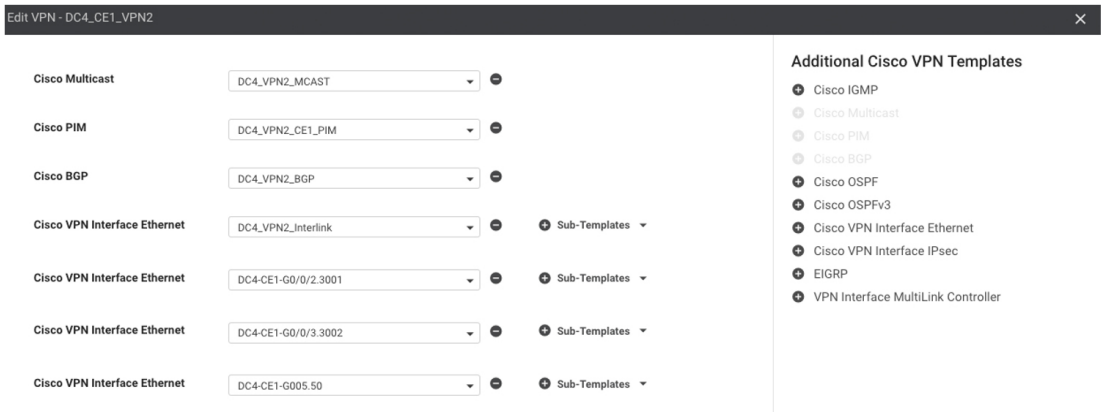
b) マルチキャストレプリケータでサービス VPN マルチキャストテンプレートを設定します。



ステップ 3 サービス VPN PIM テンプレートを設定します。cEdge のスタティック RP は、ローカルサイトのファブリックボーダーのエニーキャスト RP IP アドレスを指します。



デバイステンプレートの VPN セクションでマルチキャストと PIM を有効にします。



ステップ 4 ファブリックボーダーと cEdge の間の VRF-Lite インターフェイスで PIM を手動で設定します。

ステップ 5 サイト固有のマルチキャスト送信元をリモートマルチキャスト RP に伝達するように、クロスサイト MSDP ピアリングを手動で設定します。

Cisco DNA Center は、SD-Access マルチキャストが有効になっている同じサイトのファブリックボーダーで MSDP 設定をプロビジョニングします。次の例は、2 つの SD-Access サイトのファブリックボーダー間でフルメッシュ MSDP 接続を確立するために必要な手動の VRF 単位の設定を示しています。

クロスサイト MSDP ピアリングの手動設定の例

サイト 1 のファブリックボーダー

[S1-FB1]

```
ip msdp vrf CD_CORP_VN peer 124.1.6.5 connect-source Loopback 4601
ip msdp vrf CD_CORP_VN peer 124.1.6.6 connect-source Loopback 4601
```

[S1-FB2]

```
ip msdp vrf CD_CORP_VN peer 124.1.6.5 connect-source Loopback 4601
ip msdp vrf CD_CORP_VN peer 124.1.6.6 connect-source Loopback 4601
```

DC4 のファブリックボーダー

[DC4-FB1]

```
ip msdp vrf CD_CORP_VN peer 31.1.6.6 connect-source Loopback4601
ip msdp vrf CD_CORP_VN peer 31.1.6.7 connect-source Loopback4601
```

[DC4-FB2]

```
ip msdp vrf CD_CORP_VN peer 31.1.6.6 connect-source Loopback4601
ip msdp vrf CD_CORP_VN peer 31.1.6.7 connect-source Loopback4601
```

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/