Cisco SD-WAN Cloud onRamp for Colocation ソリューションの利用を開始

Cisco SD-WAN Cloud onRamp for Colocation ソリューション – 展開ワークフロー

このトピックでは、colo デバイスの使用を開始し、Cisco vManage でクラスタを構築する手順の概要を説明します。クラスタを作成して構成したら、クラスタをアクティブ化するために必要な手順を実行できます。サービスグループまたはサービスチェーンを設計し、それらをアクティブ化されたクラスタに接続する方法を理解します。サポートされている Day-N 操作もこのトピックにリストされています。

1. ソリューションの前提条件と要件を満たします。「Cisco SD-WAN Cloud onRamp for Colocation ソリューションの前提条件と要件」を参照してください。
   - CSP デバイス（初期 CSP アクセス用の CIMC のセットアップ）および Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチ（コンソールサーバーのセットアップ）と OOB または管理スイッチの配線を完了します。 すべてのデバイスの電源をオンにします。
   - DHCP サーバーをセットアップして構成します。「コロケーションごとの DHCP サーバーのプロビジョニング （14 ページ）」を参照してください。

2. インストールされている Cisco NFVIS のバージョンを確認し、必要に応じて NFVIS をインストールします。「Cisco CSP での Cisco NFVIS Cloud OnRamp for Colocation のインストール （3 ページ）」を参照してください。
3. クラスタをセットアップまたはプロビジョニングします。クラスタは、CSP デバイスや Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを含むすべての物理デバイスで構成されます。「Cisco SD-WAN Cloud onRamp for Colocation ソリューションの利用を開始 （1 ページ）」を参照してください。
   - CSP デバイスを起動します。「プラグアンドプレイプロセスを使用した CSP デバイスのオンボード （6 ページ）」を参照してください。
   - Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを起動します。「スイッチデバイスの起動 （10 ページ）」を参照してください。
   - クラスタをプロビジョニングして構成します。「クラスタのプロビジョニングと構成」を参照してください。

     クラスタ設定でクラスタを構成します。「クラスタの設定」を参照してください。
4. クラスタをアクティブ化します。『クラスタの作成とアクティブ化』を参照してください。
5. サービスグループまたはサービスチェーンを設計します。『サービスグループの管理』を参照してください。

（注） クラスタを作成する前、またはすべての VM がリポジトリにアップロードされた後にクラスタをアクティブ化する前に、いつでもサービスチェーンを設計し、サービスグループを作成できます。

6. サービスグループとサービスチェーンをクラスタに接続または切り離します。『クラスタ内のサービスグループの接続または切断』を参照してください。

（注） クラスタがアクティブになった後、サービスチェーンをクラスタに接続できます。

7. （オプション）すべての Day-N 操作を実行します。
   - サービスグループを切り離して、サービスチェーンを切り離します。『クラスタ内のサービスグループの接続または切断』を参照してください。
   - クラスタに CSP デバイスを追加および削除します。Cisco vManage を使用した Cloud OnRamp Colocation デバイスの追加および Cisco vManage からの Cloud OnRamp for Colocation デバイスの削除を参照してください。
   - クラスタを非アクティブ化します。『Cisco vManage からのクラスタの削除』を参照してください。

- クラスタを再アクティブ化します。『Cisco vManage からのクラスタの再アクティブ化』を参照してください。
- より多くのサービスグループまたはサービスチェーンを設計します。『サービスグループでのサービスチェーンの作成』を参照してください。

Cisco CSP での Cisco NFVIS Cloud OnRamp for Colocation のインストール

このセクションでは、NFVIS Cloud OnRamp for Colocation を Cisco CSP デバイスにインストールするために実行する必要がある一連のタスクに関する情報を提供します。

CIMC ユーザーインターフェイスのログイン

始める前に

- CIMC にアクセスするための IP アドレスが設定済みであることを確認します。
- ローカルシステムに Adobe Flash Player 10 以降がインストールされていない場合はインストールします。

CIMC の IP アドレスを設定する方法の詳細については、cisco.com の『*Set up CIMC for UCS C-Series Server*』ガイドを参照してください。

CIMC のアップグレードについては、cisco.com の『CIMC Firmware Update Utility』ガイドを参照してください。

ステップ 1 初期セットアップ時に CIMC へのアクセス用に設定した IP アドレスを Web ブラウザに入力します。

ステップ 2 セキュリティ ダイアログボックスが表示された場合は、次の操作を実行します。

a) **オプション**：チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。

b) [Yes] をクリックして証明書を受け入れ、続行します。

ステップ 3 ログイン ウィンドウで、ユーザ名とパスワードを入力します。

未設定のシステムに初めてログインする場合は、ユーザー名に **admin**、パスワードに **password** を使用します。

ステップ 4 [Log In] をクリックします。

[Change Password] ダイアログボックスは、CIMC に初めてログインしたときにのみ表示されます。

ステップ 5 パスワードを適宜変更して保存します。

CIMC のホームページが表示されます。

ステップ 6 [CIMC Server] タブで、[Summary] を選択し、[Launch KVM Console] をクリックします。

[KVM Console] が別ウィンドウで開きます。

ステップ 7 KVM コンソールの [Virtual Media] メニューから、[Activate Virtual Devices] を選択します。

暗号化されていない仮想メディアセッションメッセージが表示されたら、[Accept this session] を選択し、[Apply] をクリックします。仮想デバイスがアクティブになります。

ステップ 8 KVM コンソールの [Virtual Media] メニューから、[Map CD/DVD] を選択します。

ステップ 9 ローカルシステム上のインストールファイル（ISO）を参照して選択します。

ステップ 10 [Map Device] をクリックします。

これで、ISO イメージファイルが CD/DVD にマップされました。

ステップ 11 [CIMC Server] タブから、[BIOS] を選択します。

BIOS のアップグレードの詳細については、cisco.com の「BIOS Upgrade」ガイドを参照してください。

ステップ 12 [BIOS Actions] エリアから、[Configure Boot Order] を選択します。

[Configure Boot Order] ダイアログボックスが表示されます。

ステップ 13 [Device Types] エリアから、[CD/DVD Linux Virtual CD/DVD] を選択し、[Add] をクリックします。

ステップ 14 [HDD] を選択し、[Add] をクリックします。

ステップ 15 [Up] および [Down] オプションを使用して、起動の順序を設定します。[CD/DVD Linux Virtual CD/DVD] 起動順序オプションは、最初の選択肢である必要があります。

ステップ 16 起動順序の設定を完了するには、[Apply] をクリックします。

ステップ 17 CIMC の [Server Summary] ページから [Power Off Server] オプションを選択して、サーバーをリブートします。

ステップ 18 サーバーがダウンしたら、CIMC で [Power On Server] オプションを選択します。

サーバーがリブートすると、KVM コンソールによって、仮想 CD/DVD ドライブから Cisco Enterprise NFVIS が自動的にインストールされます。インストールが完了するまで 30 分～ 1 時間ほどかかることがあります。

ステップ 19 インストールが完了すると、システムはハードドライブから自動的にリブートします。リブート後、コマンドプロンプトが「localhost」から「nfvis」に変わったら、システムにログインします。

システムがコマンドプロンプトを自動的に変更するまでしばらく待ちます。自動的に変更されない場合は、Enter キーを押して、コマンドプロンプトを「localhost」から「nfvis」に手動で変更します。ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123#** を使用します。

（注） 初めてログインすると、デフォルトのパスワードを変更するように求められます。アプリケーションを続行するには、画面の指示に従って強力なパスワードを設定する必要があります。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。デフォルトのパスワードがリセットされていない場合、API は 401 未承認エラーを返します。

ステップ 20 システム API を使用するか、Cisco Enterprise NFVIS ポータルからシステム情報を表示して、インストールを確認できます。

（注） RAID 構成が 4.8 TB RAID-10 であることを確認します。CIMC を介して RAID を構成するには、cisco.com の『Cisco UCS Servers RAID Guide』を参照してください。

仮想デバイスのアクティブ化

仮想デバイスをアクティブ化するには、KVM コンソールを起動する必要があります。

始める前に

Java 1.6.0_14 以降のバージョンがローカルシステムにインストールされていることを確認します。

ステップ 1 所定の場所からローカルシステムに Cisco Enterprise NFVIS イメージをダウンロードします。

ステップ 2 CIMC から、[Server] タブを選択し、[Launch KVM Console] をクリックします。

（注） JNLP ファイルがシステムにダウンロードされます。セッションタイムアウトを回避するには、ダウンロードした直後にファイルを開く必要があります。

ステップ 3 名前を変更した .jnlp ファイルを開きます。Cisco Virtual KVM Console をダウンロードするように求められたら、[Yes] をクリックします。すべてのセキュリティ警告を無視して、起動を続行します。

KVM コンソールが表示されます。

ステップ 4 KVM コンソールの [Virtual Media] メニューから、[Activate Virtual Devices] を選択します。

暗号化されていない仮想メディア セッション メッセージが表示されたら、[Accept this session] を選択し、[Apply] をクリックします。仮想デバイスがアクティブになります。

NFVIS Cloud OnRamp for Colocation イメージのマッピング

ステップ 1 KVM コンソールの [Virtual Media] メニューから、[Map CD/DVD...] を選択します。.

ステップ 2 ローカルシステム上のインストールファイル（ISO）を参照して選択します。

ステップ 3 [Map Device] をクリックします。
これで、ISO イメージファイルが CD/DVD にマップされました。

ステップ 4 KVM コンソールから、電源の再投入（ウォームリブート）とシステムのインストールプロセスが開始され、NFVIS がインストールされます。

Cisco Cloud サービス プラットフォーム デバイスの起動

表 *1:* 機能の履歴

機能名	リリース情報	Description
USB ドライブを使用した Day-0 構成での CSP デバイスのオンボーディング	Cisco SD-WAN リリース 20.4.1	この機能により、Day-0 構成ファイルを USB ドライブにロードすることにより、CSP デバイスをオンボードできます。インターネットにアクセスして Plug-and-Play Connect サーバーに到達できない場合は、このオンボーディングオプションを使用します。

Cisco Cloud Services Platform（CSP）デバイスを起動するには、次のオプションを使用できます。

- 自動展開：Day-0 構成時に、工場出荷時の設定で CSP デバイスを Cisco SD-WAN ネットワークに安全にオンボードして展開します。この展開では、Cisco CSP デバイスのプラグアンドプレイ（PnP）プロセスを使用して Cisco vBond オーケストレーション の IP アドレスを動的に検出します。
- ブートストラップ展開：構成ファイルを CSP デバイスと共有する必要があります。構成ファイルを作成して起動可能 USB にコピーするか、構成ファイルを USB に追加することができます。起動可能 USB が接続されていて、起動時にデバイスで使用できます。

プラグアンドプレイプロセスを使用した CSP デバイスのオンボード

このトピックでは、PnP プロセスを使用して Cisco CSP デバイスの起動を自動化する方法について説明します。

始める前に

- 所定のトポロジに従って CSP デバイスを接続し、電源をオンにします。
- プラグアンドプレイ（PnP）対応インターフェイスを WAN トランスポート（通常はインターネット）に接続します。

Cisco CSP デバイスの電源を入れます。次のプロセスが発生します。

ステップ 1 デバイスが起動すると、デバイスのサポートされている PnP インターフェイス上の DHCP プロセスを介して、IP アドレス、デフォルトゲートウェイ、および DNS 情報を取得します。

ステップ 2 デバイスは、Cisco Cloud でホストされている PnP Connect サーバーに接続し、そのシャーシまたはシリアル番号を PnP サーバーと共有して認証を受けます。

ステップ 3 認証後、PnP Connect ポータルは Cisco vBond オーケストレーション、組織名、およびルート証明書に関する情報をデバイスに提供します。

エンタープライズルート CA 証明書を使用する展開の場合、Cisco vBond オーケストレーション の IP アドレスまたは DNS、組織名、およびエンタープライズルート CA 証明書に関する情報は、HTTPS プロトコルを使用して PnP Connect ポータルからデバイスにダウンロードされます。デバイスはこの情報を使用して、Cisco vBond オーケストレーション との制御接続を開始します。

PnP 接続ポータルを介して、PnP インターフェイスでデバイスの可用性と Cisco vBond オーケストレーション との関連付けを表示できます。

ステップ 4 デバイスが PnP 経由で Cisco vBond オーケストレーション にリダイレクトされると、PnP 接続ポータルに [Redirect Successful] ステータスが表示されます。

ステップ 5 Cisco vBond オーケストレーション での認証後、デバイスには Cisco vManage と Cisco vSmart コントローラ情報が提供され、登録してセキュアな接続を確立します。

ステップ 6 デバイスは、Cisco vManage サーバーとのセキュアな制御接続を確立しようとします。

ステップ 7 Cisco vBond オーケストレーション での認証後、Cisco vManage サーバーはデバイスのシステム IP でデバイスに応答し、共有システム IP 情報を使用してデバイスを再認証します。

ステップ 8 Cisco SD-WAN オーバーレイネットワークに参加するために、デバイスは、設定された `system-ip` IP アドレスを使用して、すべての SD-WAN コントローラへの制御接続を再開します。

USB ブートストラッププロセスを使用した CSP デバイスのオンボード

自動検出オプションを使用できない場合は、この展開オプションを使用して、構成なしで出荷される工場出荷時のデバイスを構成します。

次の場合に、この展開オプションをお勧めします。

- デバイスが、動的IPアドレスを提供できないプライベート WAN トランスポート（MPLS）に接続されている。
- プラグアンドプレイ接続サーバーにアクセスするためのインターネットアクセスが利用できない。

考慮すべき点

- USB ドライブには、ファイル名のデバイスのシリアル番号で識別される複数の Day-0 構成ファイルを含めることができます。この命名規則により、複数のデバイスのブートストラップに同じ USB ドライブを使用できます。
- 構成ファイルに含まれるサポートされている Day-0 構成は次のとおりです。
  - デバイスの静的 IP 構成
  - Cisco vBond オーケストレーション IP アドレスとポート構成

- DNS サーバーとドメイン名構成

- ブートストラップ構成は、USB キーにアップロードして、インストールサイトのデバイスに挿入できます。

始める前に

- デバイスは、構成が追加されていない工場出荷時のデフォルト状態である必要があります。
- デバイスには、Cisco NFVIS の新しいイメージをインストールする必要があります。
- USB ドライブは、ドライブを認識して自動マウントするために仮想ファイルアロケーション テーブル（VFAT）でフォーマットされている必要があります。USB ドライブをラップトップまたはデスクトップに挿入してフォーマットします。
- デバイスは Cisco vBond オーケストレーション に到達できる必要があります。

ステップ 1 USB ドライブのルートフォルダに構成ファイルを作成します。

構成ファイル名が *nfvis_config_SERIAL.xml* であることを確認します。ここで、

SERIAL は、CSP デバイスのシリアル番号を表します。

次に例を示します。

nfvis_config_ WZP232903K6.xml

ステップ 2 以下を構成ファイルにコピーします。

```
<config xmlns="http://tail-f.com/ns/config/1.0">
       <vm_lifecycle xmlns="http://www.cisco.com/nfvis/vm_lifecycle">
  <networks>
  <network>
    <name>int-mgmt-net</name>
    <subnet>
      <name>int-mgmt-net-subnet</name>
      <address>192.168.30.6</address>
      <netmask>255.255.255.0</netmask>
      <gateway>192.168.30.1</gateway>
    </subnet>
  </network>
  </networks>
       </vm_lifecycle>

<system xmlns="http://viptela.com/system">
        <organization-name>vIPtela Inc Regression</organization-name>
        <sp-organization-name>vIPtela Inc Regression</sp-organization-name>
       <vbond>
          <remote>172.23.191.87</remote>
          <port>12346</port>
        </vbond>
      </system>

<vpn xmlns="http://viptela.com/vpn">.
        <vpn-instance>
          <vpn-id>0</vpn-id>
```

```
<interface>
  <if-name>colo-mgmt</if-name>
  <tunnel-interface>
    <encapsulation>
      <encap>ipsec</encap>
    </encapsulation>
  </tunnel-interface>
  <shutdown>false</shutdown>
</interface>
</vpn-instance>
</vpn>
</config>
```

（注） デバイスの上記の静的 IP 構成を構成ファイルにコピーすることが必須です。デバイスの静的 IP 構成は、次の Day-0 構成で表されます。

```
<address></address>, <netmask></netmask>, and <gateway></gateway>
```

ステップ 3 USB ドライブを Cisco CSP デバイスに挿入し、デバイスの電源を入れます。

デバイスが起動すると、デバイスはブート可能な USB ドライブで構成ファイルを検索します。ファイルが見つかると、デバイスは PnP プロセスを一時停止し、ブートストラップ構成ファイルをロードします。

ステップ 4 USB ドライブを取り外します。

（注） 構成の適用後に USB ドライブをアンマウントしてデバイスをリブートしないと、USB ドライブの構成は再適用されません。CSP デバイスが出荷時データリセット（FDR）状態ではないか、元のシステム状態に復元されていません。

ステップ 5 CSP デバイスにアクセスするには、ステップ 2 で指定した静的 IP アドレス（192.168.30.6 など）に SSH で接続します。

ステップ 6 最初のログイン時にシステムから変更を求めるプロンプトが表示されたら、デフォルトのパスワードを変更します。

画面の指示に従って、強力なパスワードを設定してください。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。

次のタスク

デバイスのオンボーディングプロセスを確認するには、オンボードデバイスの確認とデバイスのアクティブ化 （9 ページ）に進みます。

オンボードデバイスの確認とデバイスのアクティブ化

ステップ 1 URL HTTPS: //vManage-ip-address/ を使用して、管理者ログイン情報で Cisco vManage にログインします。

ステップ 2 **[Configuration]** > **[Devices]**をクリックします。

デバイスのリストから、トークンという単語を含むシリアル番号を持つ CSP デバイスは、まだオンボードされていません。これらのデバイスを SD-WAN コントローラで認証するために、Cisco vManage はワンタ

イムパスワード（OTP）を提供します。OTP は、SD-WAN コントローラの承認済みデバイスリストに CSP デバイスを追加した後に Cisco vManage によって自動生成されます。

ステップ 3 [Valid] 列で、一覧表示されているすべての CSP デバイスのインストール済み証明書の有効性を確認します。証明書のインストールの失敗を参照してください。また、ルート CA がインストールされているかどうかを確認します。CSP が Cisco vManage との接続を確立していないを参照してください。

（注） エンタープライズルート CA 証明書を使用するデバイスオンボーディングの場合、CSP デバイスは、PnP Connect ポータルからルート証明書と、Cisco vBond オーケストレーション および組織名情報を受け取ります。

ステップ 4 CSP デバイスをアクティブ化し、シャーシ番号とシリアル番号（ワンタイムパスワード）を CSP デバイスに関連付けるには、CSP デバイスの CLI で次のコマンドを使用します。

request activate chassis-number *chassis-number* **token** *token-number*

request device コマンドの詳細については、「request device」を参照してください。

例：

request activate chassis-number *CSP-5444-serial-number* **token** *70d43cfbd0b3b426da63dba2dd4f4c49*

ステップ 5 残りの CSP デバイスを起動するには、CSP デバイスごとにステップ 1 ～ 4 を繰り返します。

スイッチデバイスの起動

このセクションでは、Day-0 構成を通じて Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスを起動する方法について説明します。

始める前に

スイッチデバイスを起動する前に、次の点に注意してください。

- Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスには、Network-Advantage と Cisco DNA-Advantage の両方のライセンスがあります。スイッチデバイスで使用可能なライセンスを確認するには、次のコマンドを使用します。

  ```
  Device# show license status
  ```

  ライセンス使用情報については、**show license usage** コマンドを参照してください。

- PNP リダイレクトセットアップまたはスイッチデバイスで設定されている手動 PNP プロファイルのいずれかが必要です。PNP リダイレクトセットアップの場合、スイッチ SN と Cisco Colo Manager IP アドレスを PNP に追加し、devicehelper.cisco.com のエントリをネットワークの OOB ルータに追加します（DHCP サーバーが OOB ルータ上にある場合）。次に例を示します。

  ```
  #conf t
  #ip host devicehelper.cisco.com <OOB router of the network>
  ```

- 両方のスイッチが SVL モード構成に従って接続されていることを確認します。

ステップ 1 以前に使用したことがある場合は、スイッチ構成をクリーニングします。

a) SVL スタックモードに必要なスイッチの番号を付け直します。

（注） SVL モード中はスイッチに触れないようにしてください。また、Enter キーやスペースキーを押すなどの操作を実行しないでください。これにより、スイッチで SVL が完了する可能性があります。

show switch コマンドを使用して、スイッチ番号とスイッチスタックにプロビジョニングされたスイッチが存在するかどうかを特定します。スイッチ番号が 2 の場合は、**switch 2 renumber 1** コマンドを使用し、次に構成を消去します。

b) スイッチのスタートアップ構成を消去して初期状態に戻すには、**write erase** コマンドを使用します。

c) 新しい構成でスイッチをリロードするには、特権 EXEC モードで次のコマンドを使用し、変更された構成を保存しないために **no** を入力します。

```
switch(config)#reload
```

（注） 構成を保存する必要はありません。

d) スイッチスタックのリロードが完了したら、セカンダリスイッチデバイスで手順 b および c を実行します。このアクションにより、セカンダリスイッチデバイスが 2 回リロードされます。

ステップ 2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチの起動後、ローカル DHCP サーバーから IP アドレスを取得し、PNP 検出を開始します。

ステップ 3 オプション 43 を使用する DHCP サーバーにより、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチは Cisco Colo Manager の PNP サーバーに到達できます。

Cisco Colo Manager の IP アドレスは、Cisco vManage 上のクラスタの PNP サーバーの IP アドレスです。オプション 43 の DHCP サーバーが常にポート 9191 を指すようにします。

例：

次に、スイッチのローカル PNP サーバーの例を示します。

```
ip dhcp pool Cat9k
network 10.114.11.39 255.255.255.0
dns-server 172.31.232.182
default-router 172.31.232.182
option 43 ascii "5A;B2;K4;I10.114.11.40;J9191”
```

ここで、10.114.11.40 はローカル PNP サーバーまたは Cisco Colo Manager の IP アドレスです。

オプション 43 を使用する DHCP サーバーをポート 9191 に設定した後の出力は次のとおりです。

```
ip dhcp excluded-address 172.31.232.182 172.31.232.185
ip dhcp excluded-address 172.31.233.182
ip dhcp excluded-address 172.31.232.254
ip dhcp excluded-address 172.31.23.10 172.31.23.49
ip dhcp excluded-address 172.31.23.52 172.31.23.100
ip dhcp excluded-address 172.31.23.252
ip dhcp excluded-address 172.31.23.253
ip dhcp excluded-address 172.31.23.230 172.31.23.250
!
```

ステップ 4 スイッチが Cisco Colo Manager の PNP サーバーに到達すると、Day-0 構成がプッシュされます。Day-0 構成のプッシュは、クラスタが Cisco vManage でアクティブ化されている場合に発生します。クラスタがアクティブ化されていない場合、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチは Cisco Colo Manager の PNP サーバーに 1 分ごとに到達し、バックオフモードのままになります。

スイッチデバイスが起動すると、スイッチデバイス上の SSH 接続と NETCONF セッションが有効になり、Cisco Colo Manager が Day-N 構成をプッシュし、継続的なスイッチ管理が続行されます。

例

規範的接続のアップリンクポート 36 および 37 について

規範的接続の場合、ポート 36（入力 VLAN ハンドオフ）および 37（出力 VLAN ハンドオフ）はアップリンクポート用に予約されています。

（注） 1/0/36、1/0/37 および 2/0/36、2/0/37 スイッチポートは「アクティブ」モードで構成されます。ユーザーがポートチャネルを使用しておらず、ポート 36 および 37 に接続していない場合、ポート 36 または 37 の Cisco Catalyst 9500-40X に接続されている OOB スイッチポートを「パッシブ」モードとして構成する必要があります。

次に例を示します。

- **interface Port-channel1 switchport trunk allowed VLAN 100-106**

```
example VLANs
 switchport mode trunk
!
```

- **interface TenGigabitEthernet1/0/1**

```
port connected to cat9k 1/0/36 or 1/0/37
 switchport mode trunk
 channel-group 1 mode passive
 spanning-tree portfast
!
```

- **interface TenGigabitEthernet1/0/2**

```
interface TenGigabitEthernet1/0/2
 switchport mode trunk
 channel-group 1 mode passive
 spanning-tree portfast
!
```

次のタスク

別のスイッチを起動するには、次のスイッチに対して、前述のすべての手順を順番に繰り返します。

Cisco Colo Manager の起動

このセクションでは、Cisco Colo Manager の起動方法について説明します。Cisco Colo Manager は、クラスタ内の Catalyst 9K スイッチの PNP エージェントとして機能します。Catalyst 9K スイッチへの Day-0 構成のプッシュを処理し、Cisco vManage から Catalyst 9K に構成をリレーします。

（注） クラスタのアクティブ化プロセス中に、Cisco Colo Manager が自動的に起動します。

ステップ 1 Cloud onRamp for Colocation 内のすべての CSP デバイスは、Cisco vManage との DTLS トンネルを確立します。

ステップ 2 Cisco vManage は、NETCONF アクション API を送信して、その CSP デバイスで Cisco Colo Manager を起動することにより、1 つの CSP デバイスを選択します。

ステップ 3 Cisco Colo Manager は、起動時は「Starting」状態です。Cisco Colo Manager は、正常性チェックのステータスに応じて、「Healthy」または「Unhealthy」状態に移行できます。

次のタスク

スイッチの構成後、Colo Manager が起動すると、両方のスイッチが Colo Manager に到達します。Cisco Colo Manager の PNP リストをチェックして、両方のスイッチデバイスがホームにコールしたことを確認してください。『スイッチデバイスが PNP または Cisco Colo Manager にコールホームしていない』を参照してください。

（注） アクティベーションを続行するには、両方のスイッチがホームにコールする必要があります。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションのプロビジョニングと構成

Cisco SD-WAN Cloud onRamp for Colocation PID を注文するには、Cisco Commerce Workspace（CCW）で Cisco SD-WAN Cloud onRamp for Colocation を選択します。

注文時に、スマートアカウント名、バーチャルアカウント名などの顧客固有の注文の詳細を指定する必要があります。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションをプロビジョニングして構成するには、次の手順を実行します。

1. Cloud Service Platform（CSP）デバイスおよび Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチが、所定の接続またはフレキシブルな接続に従ってケーブル接続され、電源がオンになっていることを確認します。
2. スマートアカウントは、顧客固有のデバイス注文の詳細を PNP Connect および vOrchestrator と同期します。

コロケーションごとの DHCP サーバーのプロビジョニング

スイッチ、VNF、CSP デバイスなどの物理デバイスの IP アドレスを管理するには、コロケーションごとに DHCP サーバーを構成する必要があります。Cisco Colo Manager の IP アドレスは、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C の DHCP オプション 43 で、Cisco Colo Manager に到達するように設定できます。

Cisco vManage は、コロケーションの Cisco Colo Manager IP アドレスを修正して割り当てます。これは、Day-0 構成を通じてすべての VNF の IP アドレスを管理および割り当てます。

（注） 物理（CSP デバイス、スイッチ）と仮想アプライアンス（Cisco Colo Manager、VNF）の両方のサブネットは同じである必要があります。

コロケーションに適切なサブネットを選択し、コロケーション内の CSP デバイスとスイッチの数に応じて IP アドレスのプールを制限できます。Cisco vManage は、Cisco vManage インターフェイスの VNF 管理 IP プールに入力された最初の IP アドレスを選択し、（スイッチ PNP サーバー IP）Cisco Colo Manager IP アドレスとして構成します。管理プールの 2 番目と 3 番目の IP アドレスは、スイッチ管理 IP アドレスに使用されます。スイッチの PNP の DHCP サーバーで別の IP アドレスが構成されている場合は、[Switch PNP Server IP] フィールドを編集して、代替の IP アドレスを指定できます。Cisco vManage プールの残りの IP アドレスは、コロケーション内の残りの VNF に割り当てられます。

（注） 各コロケーションに DNS サーバーを設定してください。

規範的接続のためのデバイスポート接続の詳細とサービスチェーン

Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開では、CSP システムに接続された Cisco Catalyst 9500-40X スイッチがサービスチェーンを実行します。VM が SR-IOV をサポートしている場合、Cisco Catalyst 9500-40X スイッチはサービスチェーンを実行しますが、SR-IOV をサポートしていない VM は、オープン仮想スイッチ（OVS）によってサービスチェーンを実行します。

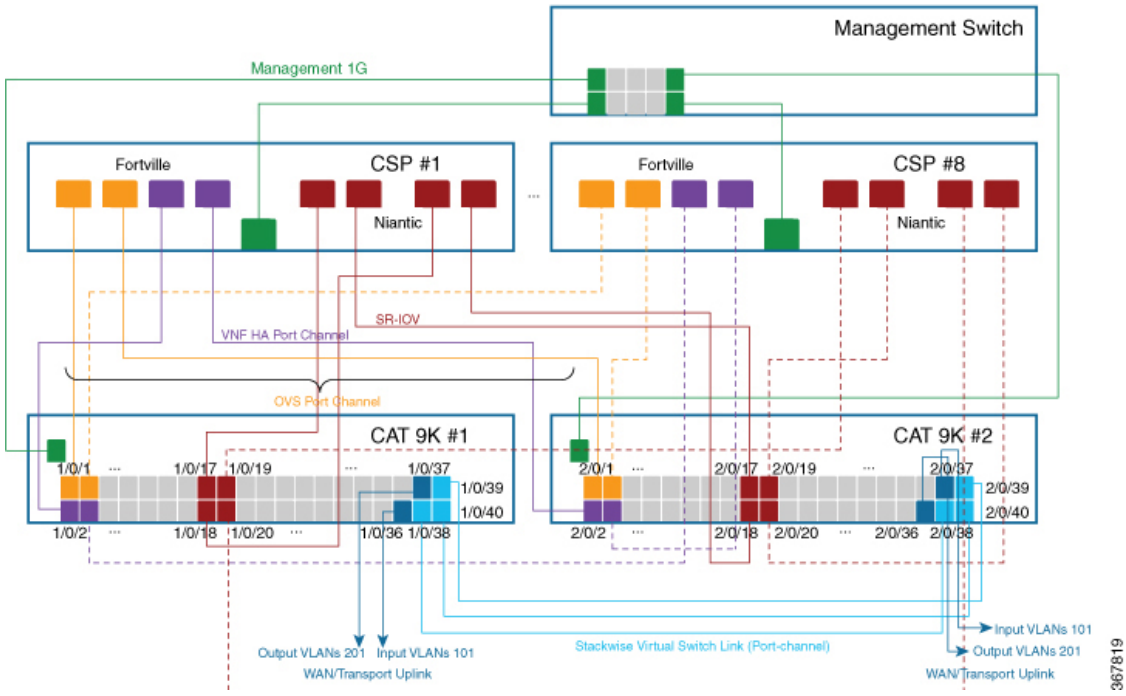
仮想スイッチベースのサービスチェーンは、高可用性トラフィックと制御トラフィックに使用されます。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションには、Cisco Catalyst 9500-40X スイッチからの VLAN ベースの L2 サービスチェーンが使用されます。このサービスチェーンでは、サービスチェーン内の VM の各仮想 NIC インターフェイスが、CSP 仮想スイッチ上の同じアクセス VLAN 上に構成されます。スイッチは、vNIC インターフェイスに出入りするパケットの VLAN タグをプッシュします。VNF は、サービスチェーンの次のサービスを認識しないままにすることができます。同じ CSP でホストされている VNF 間、またはクラスタ内の異なる CSP デバイス間でトラフィックを転送するには、一致する VLAN を持つ物理スイッチを構成します。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションの展開では、ユニキャストトラフィック用の CSP デバイスに接続されているスイッチポートで deja-vu チェックが無効になっています。

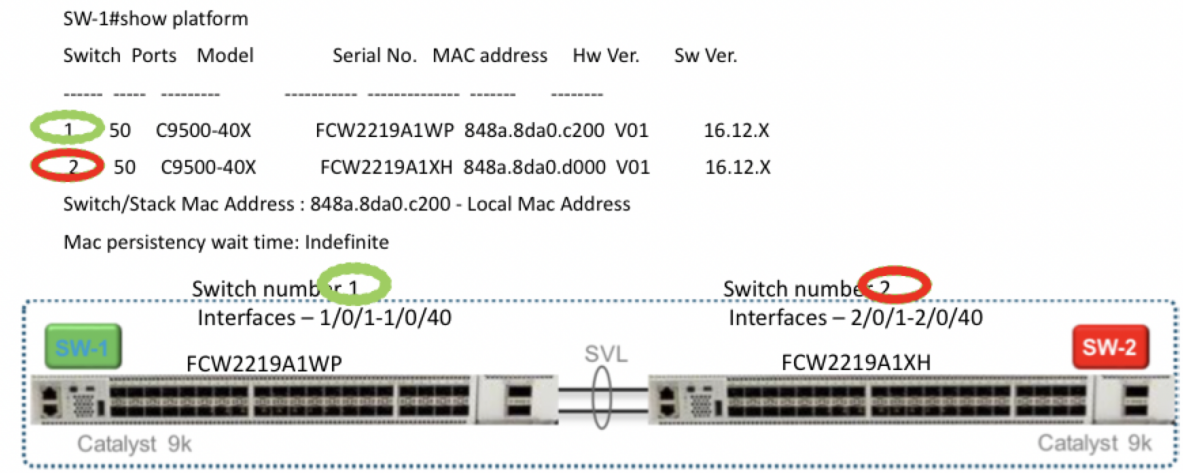
次のトポロジは、CSP ポートから Cisco Catalyst 9500-40X スイッチおよび OOB スイッチへの接続を示しています。

図 *1 : OVS*、*VEPA* 対応スイッチポートによるサービスチェーン接続



スイッチのインターフェイスの場所は次のとおりです。

（注） インターフェイスの場所は、クラスタが正常にアクティブ化された後、スイッチが SVL モードになると適用されます。



次のポートは VEPA が無効になっていて、ポートチャネルで構成されています。

- 1/0/1 ～ 1/0/16
- 2/0/1 ～ 2/0/16

次のポートは VEPA が有効になっていて、ポートチャネル構成は無効になっています。

- 1/0/17 ～ 1/0/32
- 2/0/17 ～ 2/0/32

（注） VEPA ポートは、SRIOV インターフェイスにのみ適用されます。

次のポートは、WAN 接続ポートです。

- 1/0/36、2/0/36：ポート 1/0/36 を接続して、ブランチ/VPN 接続からの外部トラフィックを受信します（OOB スイッチ経由）。
- 1/0/37、2/0/37：ポート 1/0/37 を接続して、サービス チェーン トラフィックを、OOB スイッチ上のプロバイダーネットワークにマッピングされている特定の VLAN に転送します。

ポートは次のように接続できます。

- データポート：ポート 1/0/1 ～ 1/0/35 を CSP デバイスに接続します。スイッチ全体で冗長性と HA を実現するには、2 つのポートを 1 つの CSP に接続し、他の 2 つのポートを次の CSP に接続します。たとえば、ポート 1/0/1 と 2/0/1 はデータに使用され、HA はそれぞれ最初の CSP、CSP #1 に接続できます。次に、1/0/2 および 2/0/2 は、次の CSP、CSP #2 などに接続される別のポートチャネルです。したがって、OVS ポートは 8 つの CSP デバイスすべてを使用します。

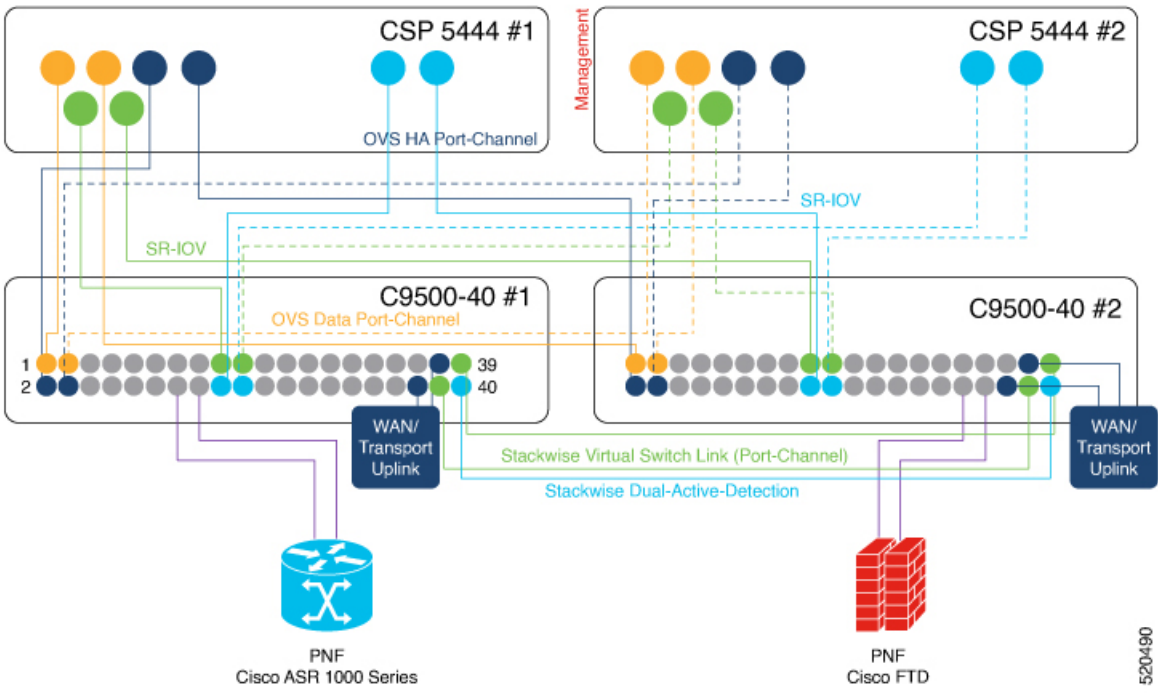
- WAN 接続ポート：構成された VLAN のポート 1/0/36 を接続して、外部トラフィックを受信します（入力 VLAN ハンドオフ）。ポート 1/0/37 を接続して、サービス チェーン トラフィックをプロバイダーネットワークにマッピングされている特定の VLAN に転送します（出力 VLAN ハンドオフ）。外部入力または出力 VLAN トラフィックは、ブランチまたは VPN 接続から来ることができ、プロバイダーネットワークは、OOB スイッチを介して Cloud OnRamp for Colocation で終端します。クラスタに構成された各サービスチェーンと、各サービスチェーンに構成された入力または出力 VLAN の場合、ポート 36 および 37 の構成は、サービスチェーンの展開中に発生します。

  ポート 36 または 37 が OOB スイッチに接続されていて、ポートチャネルを使用していない場合は、すべての VLAN ハンドオフが、入力または出力 VLAN ハンドオフに対応して設定されていることを確認します。たとえば、ポート 36 が接続されている場合、サービスチェーンの入力 VLAN ハンドオフですべての VLAN ハンドオフを構成します。ポート 37 が接続されている場合、サービスチェーンの出力 VLAN ハンドオフですべての VLAN ハンドオフを構成します。

- Stackwise Virtual Switch Link（SVL）構成でポート 1/0/38 ～ 1/0/40 を接続します。

次のケーブル接続イメージは、物理ネットワーク機能が Cisco Catalyst 9500-40X スイッチにどのように接続されているかを示しています。

図 *2 : PNF* ケーブル接続イメージ



次の表に、PNF で使用できるポートを示します。

表 *2 : Cisco Catalyst 9500-40X* スイッチ上の *PNF* のポート

CSP デバイスの数	PNF の数	最初のスイッチの PNF に使用可能なスイッチポート	2 番目のスイッチの PNF に使用可能なスイッチポート
7	1	1/0/15 ～ 1/0/16、 1/0/31 ～ 1/0/32	2/0/15 ～ 2/0/16、 2/0/31 ～ 2/0/32
6	2	1/0/13 ～ 1/0/16、 1/0/29 ～ 1/0/32	2/0/13 ～ 2/0/16、 2/0/29 ～ 2/0/32
4	4	1/0/11 ～ 1/0/16、 1/0/27 ～ 1/0/32	2/0/11 ～ 2/0/16、 2/0/27 ～ 2/0/32

CSP デバイスを削除してポートを入れ替えるには、次の手順を実行します。

1. 8 つすべての CSP デバイスがスイッチに接続されていて、PNF デバイスをスイッチに接続する場合は、次の手順を実行します。
    1. Cisco vManage の RMA ワークフローを使用して、クラスタから 8 番目の CSP（スイッチの右端のデータポートに接続されている CSP）を非アクティブ化または削除します。
    2. Cisco Catalyst 9500-40X スイッチの CSP 物理接続を切断します。
    3. 切断された CSP の代わりに PNF デバイスを接続します。
2. 追加のポートを PNF で使用できるようにするために、最初の 7 つの CSP デバイスのいずれかを削除する必要がある場合は、次の手順を実行します。
    1. 1 に記載されている手順を実行します。
    2. 8 番目の CSP である右端の接続された CSP を、削除された CSP によって使用可能になるポートに移動します。

       たとえば、1 番目の CSP が削除されている場合は、8 番目の CSP を 1 番目の CSP の位置に移動し、8 番目の CSP の代わりに PNF を接続します。

Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開の最初のフェーズでは、フルチェーン VNF 構成がサポートされます。フルチェーン構成では、プロデューサチェーンとコンシューマチェーンのすべての VNF は、単一のサービスチェーンの一部です。VNF は、異なるタイプのプロデューサとコンシューマ間で共有されません。サービスチェーンの個別のインスタンスは、コンシューマタイプとプロデューサタイプの各組み合わせをサポートします。フルチェーン構成の場合、チェーン内のすべての VNF は L2 サービスチェーンです。

Cisco vManage は、Cisco SD-WAN Cloud onRamp for Colocation ソリューションのサービスチェーン構成を管理します。Cisco vManage は、コロケーション用に提供された VLAN プールから個々の VM VNIC に VLAN を割り当て、適切な VLAN でスイッチを構成します。VNF は、サー

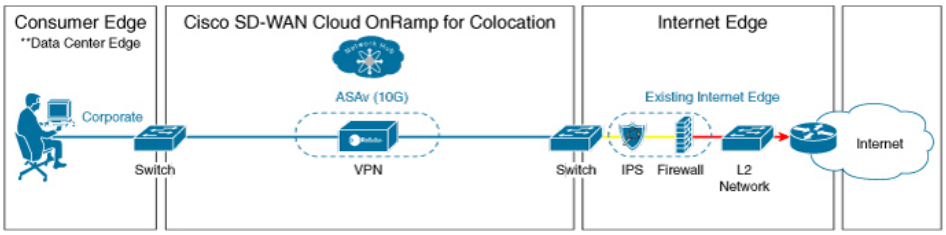
ビスチェーンを認識しないままにすることができます。Day-0 VNF 構成とは別に、Cisco vManage はサービスチェーンの一部である個々の VNF を構成しません。。

検証済みサービスチェーン

Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開で、Cisco vManage からクラスタ内に展開できる 4 つの検証済みサービスチェーンを次に示します。すべての検証済みサービスチェーンについて、各 VM は HA またはスタンドアロンモードでインスタンス化できます。

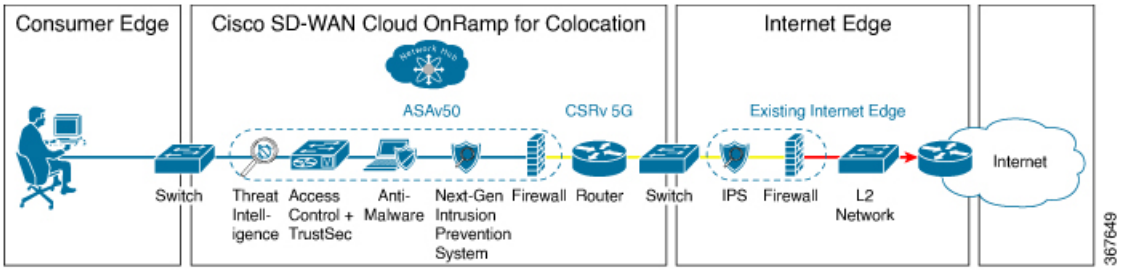
- 従業員のリモート VPN アクセス：このサービスチェーンには、L3 VPN HA または L3 VPN 非 HA モードのファイアウォールがあります。ファイアウォール VNF は、ASAv、パロアルト ネットワークス ファイアウォール、Firepower_Threat_Defense_Virtual（FTDv）にすることができます。ここでは、ASAv はルーテッドモードであり、VPN 接続に対する Day-0 構成のサポート、コンシューマチェーン上の BGP、および VLAN はありません。

図 *3*: 従業員リモート *VPN* アクセスサービスチェーン



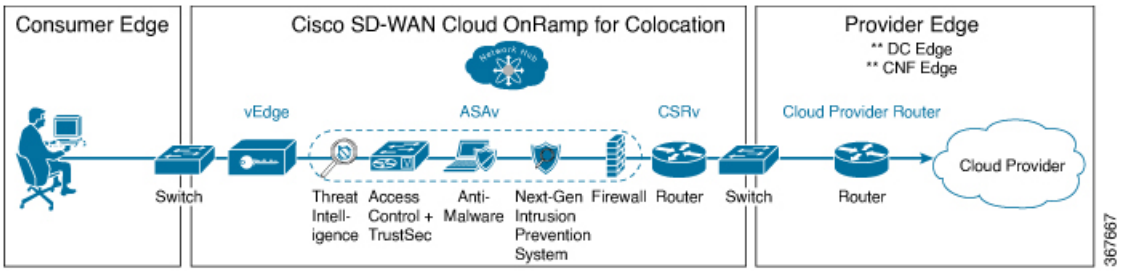
- インターネットエッジ（アウトバウンドインターネット、e コマース、SaaS） - このサービスチェーンでは、ファイアウォールの後にルータが続きます。ファイアウォールモードは、L3-VLAN HA および L3-VLAN 非 HA にすることができます。ルータは、L3 HA モードおよび L3 非 HA モードにすることができます。ここで、ASAv は常にルーテッドモードです。1 つの VLAN ハンドオフが必要であり、インバウンド サブインターフェイスは最大 4 つまで可能です。終端は、最大 4 つのサブインターフェイスがあるルーテッドモードまたはトランクモードにすることができます。ハイパーバイザのタグ付き VLAN と、VLAN のタグ付けを行うために VNF のどちらかを選択できます。VNF の VLAN タグ付けでは、最小 1 つの VLAN、最大 4 つの VLAN に終端できます。ハイパーバイザのタグ付き VLAN では、すべての VLAN が同じインバウンド VNF インターフェイスでタグ付けされます。

図 *4*: インターネット エッジ サービス チェーン



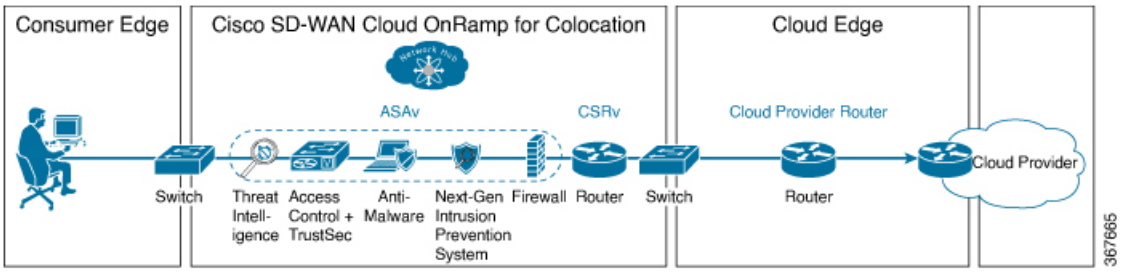
- SD-WAN アクセス：このサービスチェーンでは、vEdge の後にファイアウォールが続き、その後にルータが続きます。ファイアウォールモードは、L2 HA、L2 非 HA、L3 HA、および L3 非 HA にすることができます。ルータは、L3 HA モードおよび L3 非 HA モードにすることができます。

図 *5 : SD-WAN* アクセスサービスチェーン



- クラウドエッジ（パブリッククラウドアクセス）：このサービスチェーンでは、ファイアウォールの後にルータが続き、ファイアウォールはルーテッドモードです。ファイアウォールモードは、L3 HA および L3 非 HA にすることができます。ルータは、L3 HA モードおよび L3 非 HA モードにすることができます。このサービスチェーンは、ファイアウォールモードが L3 のインターネットエッジ（アウトバウンド インターネット、e コマース、SaaS）です。

図 *6 :* クラウドエッジ（パブリッククラウドアクセス）サービスチェーン



Cisco vManage を介して検証済みのサービスチェーンを選択する方法については、サービスグループでのサービスチェーンの作成のトピックを参照してください。

検証済み VM パッケージ

VM パッケージは、ユースケースごとに作成されます。これらのパッケージには、サポートされているユースケースごとに推奨される Day-0 構成が含まれています。すべてのユーザーは、必要なカスタム Day-0 構成を持ち込み、要件に従って VM をパッケージ化できます。検証済みパッケージでは、さまざまな Day-0 構成が単一の VM パッケージにバンドルされています。たとえば、VM がファイアウォール VM である場合、サービスチェーンの途中にある場合は、トランスペアレントモードまたはルーテッドモードで使用できます。VM がサービスチェーンの最初または最後の VM である場合、ブランチまたはプロバイダーへの終端トンネルになるか、ルーティングされたトラフィックになるか、複数のブランチまたはプロバイダーを終端することができます。各ユースケースは、展開時またはサービスチェーンのプロビジョニング中に

ユーザーが選択できるように、イメージメタデータの特別なタグとして設定されます。VM がサービスチェーンの中心にある場合、Cisco vManage はそれらのセグメントの IP アドレスと VLAN を自動化できます。VM がブランチまたはプロバイダーに終端している場合、ユーザーは IP アドレス、ピアアドレス、自律システム番号などを構成する必要があります。

カスタマイズされたサービスチェーン

サービスチェーンは、パケットが通過するサービス機能と関連するエンドポイントグループの名前付きリストです。サービスチェーンをカスタマイズし、サービス チェーン テンプレートを作成できます。サービス チェーン テンプレートは、入力トラフィックをクラウドに接続する目的でサービスを提供する VM のチェーンです。サービス チェーン テンプレートには、検証済みの VM を含む事前定義されたサービスチェーンを含めることができます。

カスタマイズされたサービスチェーンの最初の VNF と最後の VNF は、ルータ（またはファイアウォール）にすることができます。SD-WAN の場合、最初の VM はオーケストレーションされた vEdge です。非 SD-WAN の場合、最初の VM は、オーケストレーションされないゲートウェイルータとしてモデル化できます。

サービス チェーン テンプレートを選択し、1 つ以上の VM を挿入して 1 つ以上の VM を削除することでテンプレートを変更できます。サービスチェーン内の各 VM について、VM カタログから取得された VM イメージを選択できます。たとえば、サービスチェーンの最初の VM がルータである場合、Cisco 1000v を選択するか、VM リポジトリから選択するか、サードパーティルータを選択できます。

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。