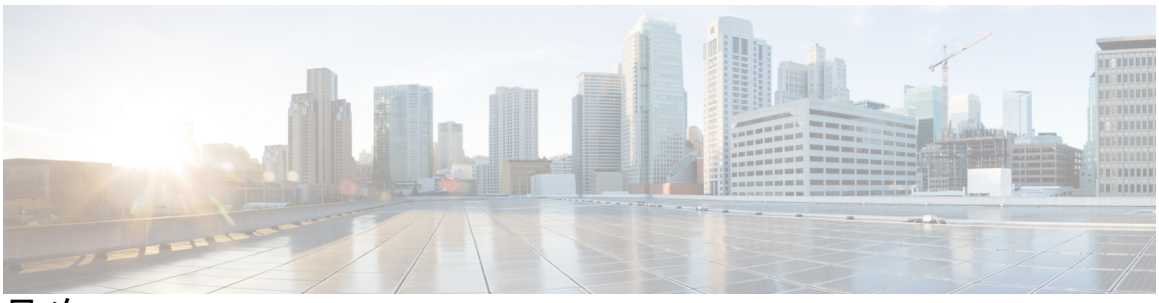
Cisco vManage を使用した Cisco NFVIS SD-Branch の設計と導入

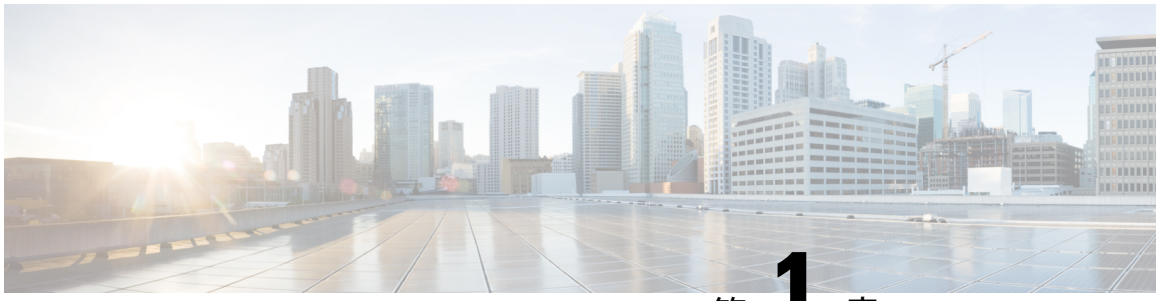
最終更新：2020 年 12 月 18 日

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/



目 次

【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。



第 1 章

Cisco NFVIS の新機能

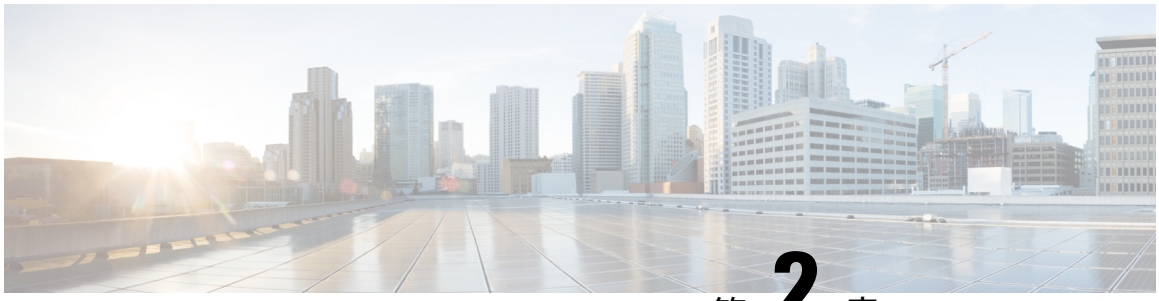
（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

表 *1 : NFVIS 4.6* リリース

機能	リリース情報	説明
デバイスに接続されたプロファイルの N 日目の変更のサポート	NFVIS 4.6 リリース Cisco vManage リリース 20.6.1	この機能を使用すると、デバイスに接続された後でも、ネットワーク設計プロファイルを変更できます。
異なる VNF イメージパッケージのアップロードのサポート	NFVIS 4.6 Cisco vManage リリース 20.6.1	この機能を使用すると、イメージパッケージ、スキャフォールド、およびディスクイメージ用の個別の VNF パッケージをアップロードして、VNF イメージを登録できます。

表 *2 : NFVIS 4.5* リリース

機能	リリース情報	説明
NFVIS およびルータ VM の単一 IP アドレスのサポート	NFVIS 4.5 リリース Cisco vManage リリース 20.5.1	このリリースでは、NFVIS とルータ VM の間で単一のパブリック IP アドレスを使用するためのサポートが SD-Branch ソリューションに拡張されています。
WAN エッジデバイスの開始、停止、および再起動（66 ページ）	NFVIS 4.5 リリース Cisco vManage リリース 20.5.1	このリリースでは、展開された VM の起動、停止、および再起動のサポートが拡張されています。



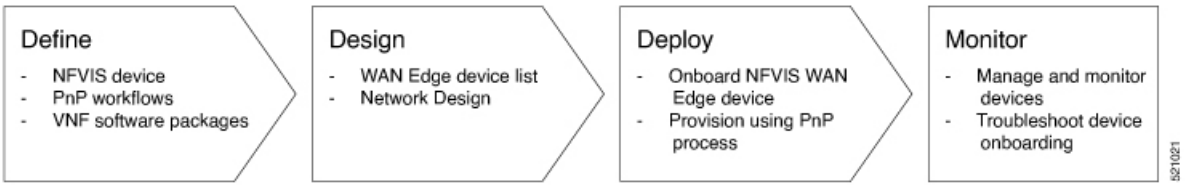
第 2 章

Cisco NFVIS SD-Branch ソリューションの概要

企業およびサービスプロバイダは、専用ハードウェアアプライアンスからのネットワークサービスを仮想化されたオンデマンド アプリケーションに統合しています。これらのアプリケーションは、一元化されたオーケストレーションと管理を備えたブランチ オフィス ソフトウェアで実行されます。ブランチ オフィス ソフトウェアは、ブランチの各機能のハードウェアへの依存を排除し、設定可能なタスクを簡素化し、時間を短縮し、運用と管理を一元化します。これにより、ネットワーク機能仮想化（NFV）サービスをより迅速かつ柔軟に展開できるようになります。

Cisco Software-Defined Branch（SD-Branch）ソリューションは、短時間で展開できるシンプルなハードウェア、ソフトウェア、および仮想化サービスの組み合わせです。Cisco SD-Branch ソリューションでは、シスコが検証した設計テンプレートのリストから選択し、数分でフルサービスブランチを展開できます。

中央集中型のオーケストレーションと WAN ネットワーク管理により、Cisco SD-Branch ソリューションは、初期導入の設定と管理、単一の場所からの IT 環境への新しいサービスの変更と追加を可能にし、個々のブランチオフィスを訪問する時間を削減します。オーケストレーションは、既存の SD-Branch サービス、新しいネットワーク サービス オンボーディング、仮想ネットワーク機能（VNF）パッケージ、ネットワーク サービス ライフサイクル管理、グローバル リソース管理、および SD-Branch インフラストラクチャ リソース要求の検証と承認を 1 つのポイントから管理します。

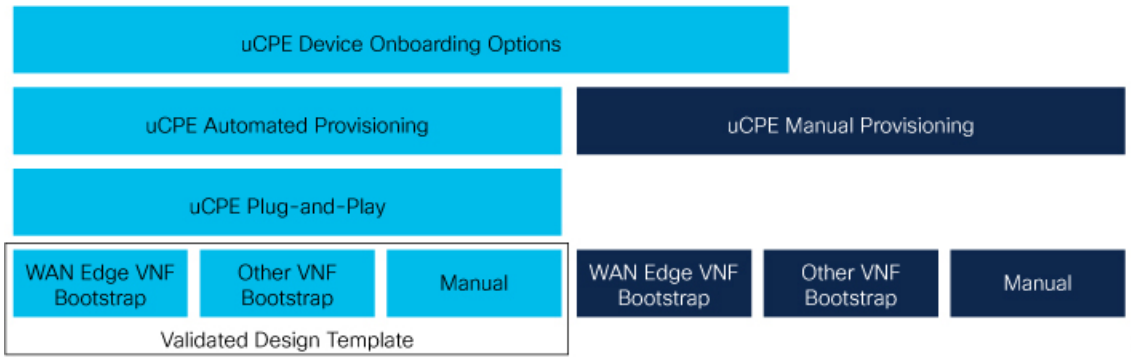


Cisco SD-Branch ソリューションには、次のオーケストレーション機能が含まれています。

- サービスの調整とインスタンス化：オーケストレーション ソフトウェアは、基盤となる Cisco SD-Branch プラットフォームと通信してサービスをインスタンス化し、プラットフォーム上にサービスの仮想インスタンスを作成します。

- サービスチェーン：ルーティング、ファイアウォール、WAN 最適化などのネットワークサービスを仮想チェーンに接続し、ネットワークリソースの使用を最適化しながら、アプリケーションのパフォーマンスを向上させます。
- スケーリングサービス：サービス数が増加した場合に、サービスを提供するのに十分なリソースを管理します。
- サービスモニタリング：プラットフォームとリソースのパフォーマンスを追跡し、適切なサービスを提供できるようにします。

このドキュメントでは、NFVIS SD-Branch ソリューションの設計および導入手順について説明します。また、ブランチ環境での ENCS 5400 uCPE WAN エッジデバイスおよびその他の仮想ネットワークサービスまたはアプリケーションの展開方法についても説明します。



- Cisco SD-Branch ソリューションのコンポーネント （4 ページ）
- 開始する前の主なタスク （6 ページ）

Cisco SD-Branch ソリューションのコンポーネント

Cisco SD ブランチソリューションにはさまざまなコンポーネントがあります。

- **ハードウェアコンポーネント**：
  - **Cisco 5000 エンタープライズ ネットワーク コンピューティング システム**：Cisco 5000 エンタープライズ ネットワーク コンピューティング システム（ENCS）は、Cisco SD-Branch およびエンタープライズ ネットワーク機能の仮想化（ENFV）ソリューション向けに設計されたコンピューティング アプライアンス シリーズです。5000 ENCS は、従来のルータと従来のサーバーの最適な特性を組み合わせたハイブリッドプラットフォームで、インフラストラクチャ フットプリントを小型化しながらも同じ機能を提供します。シスコ サービス統合型仮想ルータ（ISRv）と NFV インフラストラクチャ ソフトウェア（NFVIS）をホスティングレイヤとするこのプラットフォームは、シンプルに展開できる包括的なソリューションを提供します。

    NFVIS 4.2.1、ENCS 5400 デバイス上の Cisco vManage 20.3.1 以降のリリースは、Cisco SD-Branch ソリューションでサポートされます。

- **Cisco Catalyst 8200 シリーズ エッジ ユニバーサル CPE**：Cisco Catalyst 8200 エッジ uCPE は、中小規模の仮想化ブランチ向けに、ルーティング、スイッチング、アプリケーションホスティングをコンパクトな1ラックユニットデバイスに統合した次世代の Cisco エンタープライズ ネットワーク コンピューティング システム 5100 シリーズです。これらのプラットフォームは、Cisco NFVIS ハイパーバイザソフトウェアを搭載した同じハードウェアプラットフォーム上で、仮想化されたネットワーク機能やその他のアプリケーションを仮想マシンとして実行できるように設計されています。

  Catalyst 8200-UCPE Edge シリーズ デバイス上の NFVIS 4.4.1、Cisco vManage 20.4.1 以降のリリースは、Cisco SD-Branch ソリューションでサポートされています。

- **Cisco Network Function Virtualization Infrastructure Software**：Cisco Network Function Virtualization Infrastructure Software（NFVIS）ソフトウェアは、x86 コンピューティング プラットフォーム上で実行されるベース仮想化インフラストラクチャ ソフトウェアとして使用されます。Cisco NFVIS ソフトウェアは、VM ライフサイクル管理、VM サービスチェーン、VM イメージ管理、プラットフォーム管理、デバイスをブートストラップするための PNP、AAA 機能、syslog、および SNMP サーバーを提供します。NFVIS ソフトウェアは、前述のすべての機能にプログラム可能な REST および netconf API を提供します。

- **仮想ネットワーク機能**：シスコの SD ブランチソリューションは、シスコが開発した仮想ネットワーク機能（VNF）をサポートします。次の表に、検証済みの VNF とそのバージョンを示します。

シスコの仮想ネットワーク機能（VNF）	バージョン
Cisco ISRv	17.2.1 16.12.1a 16.11.1b
Cisco ASAv	9.13.1
Cisco vWAAS	6.4.3c-b-42
Cisco vEdge	20.1 19.2.1

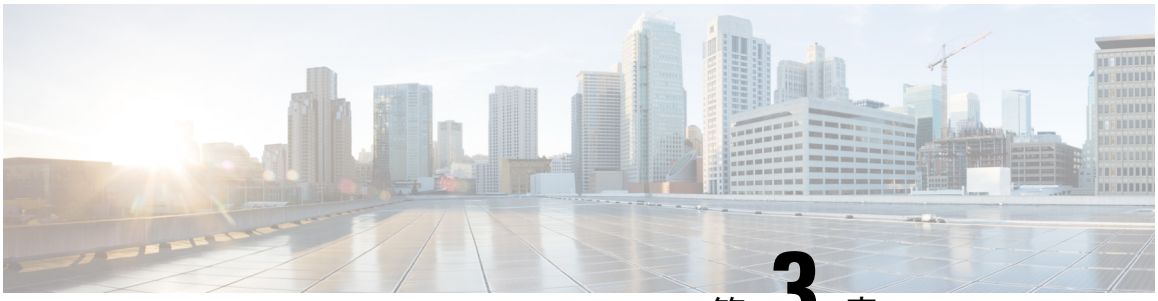
サードパーティ製仮想ネットワーク機能（VNF）	Versions
Fortinet®	v5.4.1、build9317、161003
PaloAlto®	8.1.3
Riverbed®	9
CheckPoint®	77.30
SilverPeak®	7.3.9.0

- **Cisco vManage によるオーケストレーション**：Cisco vManage は、Cisco SD ブランチソリューションのオーケストレーションに使用されます。Cisco vManage および vBond バージョン 20.1.1 以降は、Cisco SD ブランチソリューションでサポートされます。オーケストレータは次の機能を提供します。
  - Cisco vBond：Cisco vBond オーケストレータは、ネットワークアドレス変換（NAT）の背後で実行されている可能性があるネットワーク要素にCisco vManage 情報を提供します。初期認証を実行し、NAT（STUN）サーバー機能のセッショントラバーサルユーティリティを提供するネットワーク要素を許可します。
  - Cisco vManage：Cisco vManage は、SD ブランチソリューションの一元化された設定管理、モニタリング、およびトラブルシューティングを提供する SDN コントローラです。

開始する前の主なタスク

開始する前に、次の前提条件が満たされていることを確認してください。

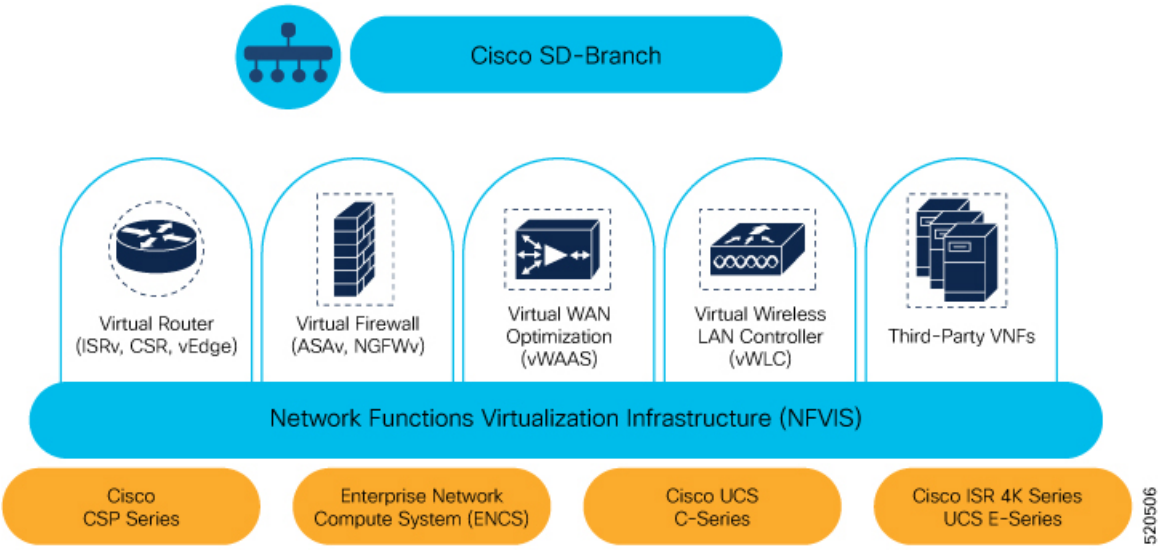
- Cisco vManage、Cisco vBond、Cisco vSmart などの Cisco SD-WAN コントローラは、クラウドまたはオンプレミスで有効な証明書とともにすでに展開されています。
- NFVIS WAN エッジデバイスは、Cisco vBond オーケストレータおよびその他の SD-WAN コントローラに到達可能です。これらのコントローラは、WAN トランスポート全体のパブリック IP アドレスを介して到達可能です。



第 3 章

Cisco NFVIS SD-Branch ソリューションの定義

Cisco SD-Branch ソリューションは、エンタープライズグレードのネットワークおよびアプリケーションサービスを提供するフルスタックソリューションです。設計要件に合わせて、さまざまなコンピューティングプラットフォームから選択できます。サポートされているすべてのプラットフォームには、SD-Branch デバイスのライフサイクル管理用のホスト OS として NFVIS があります。このアーキテクチャでは、Cisco vManage を使用してブランチ ネットワーク コンピューティング デバイスのサービスをゼロタッチでプロビジョニングできます。



（注） NFVIS SD-Branch ソリューションは現在、ENCS 5400 デバイスのみをサポートしています。

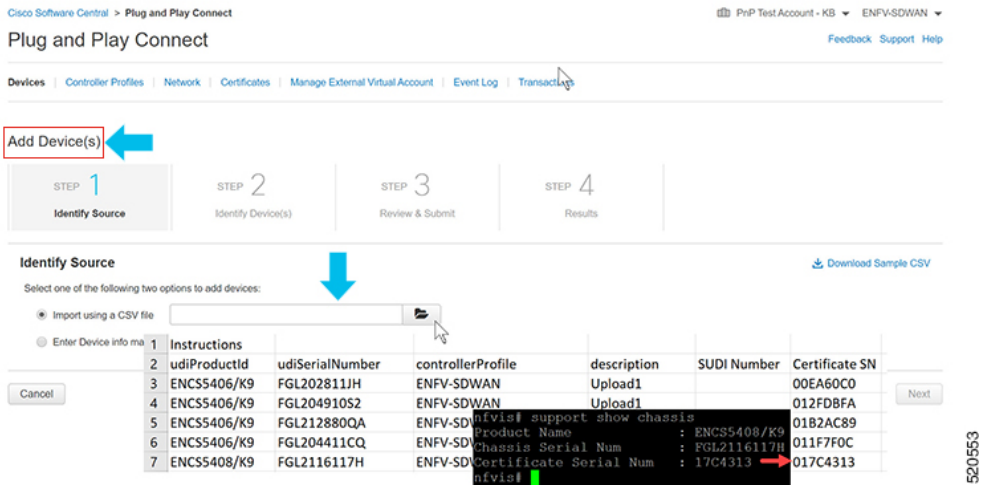
- 承認済みデバイスリストの作成 （8 ページ）
- VNF イメージパッケージの作成 （10 ページ）
- デバイスの検出と展開 （14 ページ）

承認済みデバイスリストの作成

ENCS デバイスのシリアル番号は、お客様固有の Cisco スマートアカウントとバーチャルアカウントにアップロードされます。これは自動化されたプロセスですが、場合によっては、バーチャルアカウントを手動で作成し、ENCS デバイスのシリアル番号をアップロードする必要があります。次の手順は、顧客ロケーションのデバイスを顧客固有のコントローラにリダイレクトする方法を示しています。

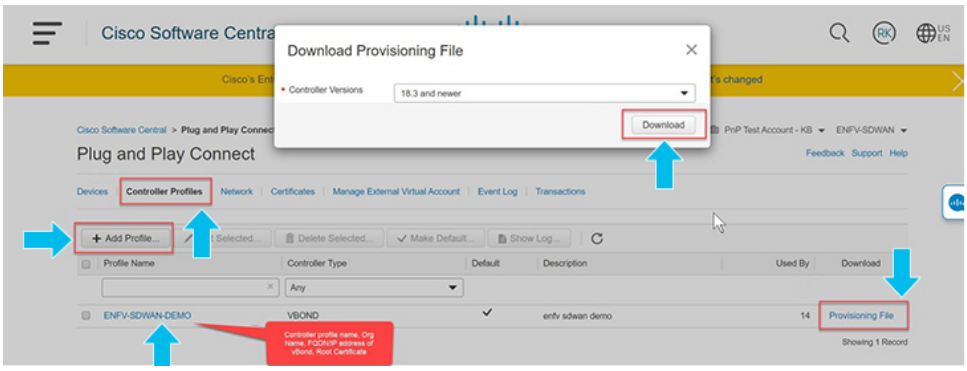
1. バーチャルアカウントにコントローラ情報を追加します。

   - PnP Connect サーバーで [Devices] を選択し、[+ Add Devices] をクリックして、PID、シリアル番号、およびコントローラに関する情報を含むCSV ファイルをアップロードします。Symantec によって発行された証明書をアップロードするか、エンタープライズのルート証明書をアップロードできます。



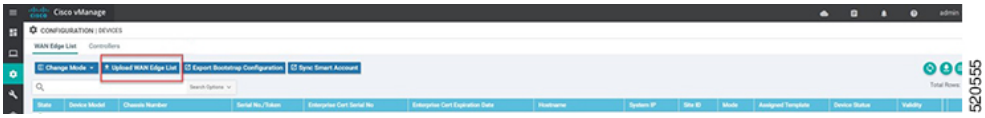
> **注** Cisco vManage 20.4 以降では、ENCS デバイス証明書のシリアル番号が使用できない場合、[SUDI Number] 列にデバイスのシリアル番号を入力することで、デバイスのシリアル番号を使用してデバイスを認証できます。Cisco vManage スマート同期では、デバイスのシリアル番号を使用してデバイスを認証します。

   - [Controller Profiles] を選択し、[+Add Profiles] をクリックします。コントローラに関連する詳細を入力して、プロファイルを作成します。[Provisioning File] を選択してダウンロードします。



2. デバイスリストを Cisco vManage に追加します。

   • 承認済みデバイスリストをバーチャルアカウントから Cisco vManage にアップロードします。



アイデンティティ、トラスト、およびホワイトリスト

NFVIS WAN エッジデバイスの ID は、シャーシ ID と証明書のシリアル番号によって一意に識別されます。WAN エッジデバイスに応じて、次の証明書が提供されます。

- ENCS ハードウェアデバイス証明書は、製造時に取り付けられたオンボード SUDI チップに保存されます。ENCS ハードウェアは Cisco NFVIS ソフトウェアに付属しています。
- Cisco SD-WAN 仮想デバイスには、デバイスにルート証明書が事前にインストールされていません。これらのデバイスでは、ワンタイムパスワード（OTP）が Cisco vManage によって提供され、SD-WAN コントローラでデバイスを認証します。

WAN エッジデバイスの信頼性は、製造時にプリロードされたルートチェーン証明書、手動でロードされたルートチェーン証明書、Cisco vManage によって自動的に配布されたルートチェーン証明書、自動展開プロビジョニングプロセスであるプラグアンドプレイ（PnP）またはゼロタッチプロビジョニング（ZTP）でインストールされたルートチェーン証明書を使用して実現されます。

Cisco SD-Branch ソリューションはホワイトリストモデルを使用します。つまり、SD-Branch オーバーレイネットワークに参加できる NFVIS WAN Edge デバイスは、すべての SD-Branch コントローラで事前に認識されている必要があります。これを行うには、PnP 接続ポータルに WAN エッジデバイスを追加します。追加された WAN エッジデバイスは、PnP ポータル（SD-Branch オーバーレイの組織名に関連付けられている）に含まれる Cisco vBond コントローラプロファイルに接続され、プロビジョニングファイルが作成されます。このファイルは SD-Banch vManage コントローラにインポートされ、デバイスのホワイトリストが残りの SD-Branch コントローラ（vBond）と自動的に共有されます。デバイスのホワイトリストを含

むプロビジョニングファイルは、PnP 接続ポータルから Cisco vManage に REST API を使用してセキュアな SSL 接続を介して直接同期することもできます。

（注） Cisco SD-WAN コンポーネント（Cisco vManage、Cisco vBond、Cisco vSmart コントローラ、WAN エッジデバイスなど）はすべて、同じ SD-Branch オーバーレイネットワークに参加するために同じ組織名で設定する必要があります。

VNF イメージパッケージの作成

表 *3:* 機能の履歴（表）

機能名	リリース情報	説明
異なる VNF イメージパッケージのアップロードのサポート	NFVIS 4.6.1 Cisco vManage リリース 20.6.1	この機能を使用すると、イメージパッケージ、スキャフォールド、およびディスクイメージ用の個別の VNF パッケージをアップロードして、VNF イメージを登録できます。

事前にパッケージ化された Cisco VM イメージ tar.gz のアップロードは、Cisco vManage でサポートされています。また、サポートされている形式（qcow2）でルートディスクイメージを提供することで、VM イメージをパッケージ化することもできます。Linux のコマンドライン NFVIS VM パッケージツール nfvpt.py を使用して qcow2 をパッケージ化するか、Cisco vManage からカスタマイズされた VM イメージを作成します。

（注） 事前にパッケージ化された Cisco VM イメージを [ISRv Software Download] ページからダウンロードし、[Scaffold Files for Third Party VMs Software Download] ページからダウンロードします。https://software.cisco.com/download/home/286308649/type/286327969/release/17.03.01https://software.cisco.com/download/home/286308649/type/286327978/release/4.4.1

ファイアウォールなどの各 VM タイプには、カタログに追加される同じまたは異なるベンダーから Cisco vManage にアップロードされる複数の VM イメージを含めることができます。また、同じ VM のリリースに基づく異なるバージョンをカタログに追加できます。ただし、VM 名が一意であることを確認してください。

Cisco VM イメージ形式は *.tar.gz としてバンドルでき、次のものを含めることができます。

- VM を起動するルートディスクイメージ。
- パッケージ内のファイルリストのチェックサム検証用のパッケージマニフェスト。

- VM メタデータをリストする XML 形式のイメージプロパティファイル。
- （任意）0 日目設定、VM のブートストラップに必要なその他のファイル。
- VM システムプロパティをリストする XML 形式のシステム生成プロパティファイル

VM イメージは、vManage がホストする HTTP サーバーローカルリポジトリまたはリモートサーバーの両方でホストできます。

VM が tar.gz などの NFVIS でサポートされる VM パッケージ形式である場合、Cisco vManage はすべての処理を実行し、VNF プロビジョニング中に変数キーと値を指定できます。

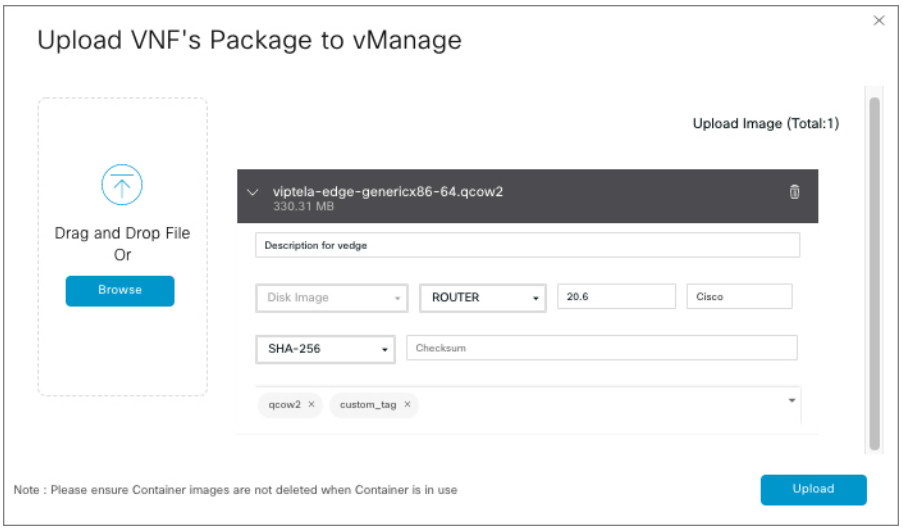
異なるイメージタイプのアップロード

NFVIS リリース 4.6.1 以降、イメージの登録プロセスはイメージプロパティのアップロードプロセスから分離されています。VNF イメージは、サポートされている任意のイメージ形式でアップロードすることで登録できます。サポートされるイメージ形式は次のとおりです。

- イメージパッケージ：完全なイメージパッケージの .tar.gz ファイル。
- Scaffold：.tar.gz ファイル（メタデータのみで構成）（イメージプロパティおよび第 0 日のコンフィギュレーション ファイル）。
- ディスクイメージ：.qcow2 ディスクイメージ。

イメージタイプをアップロードするには、次の手順を実行します。

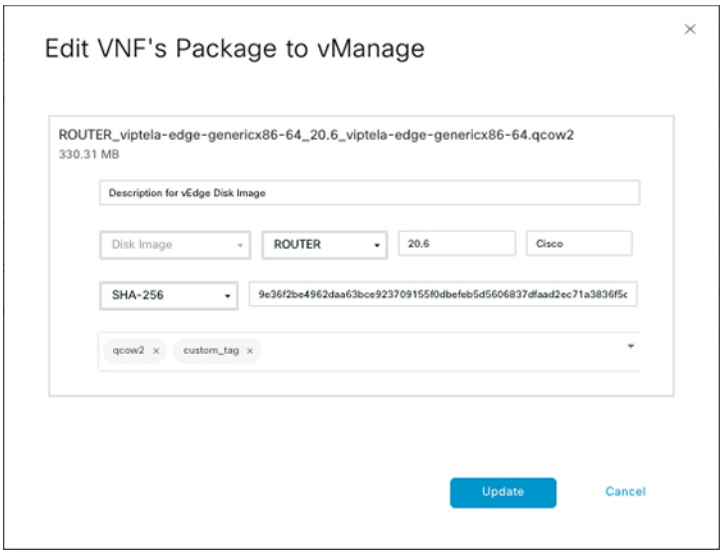
1. [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。
2. [Virtual Images] をクリックします。
3. [Upload Virtual Image] ドロップダウンリストから、[vManage] を選択します。
4. [Upload VNF's Package to vManage] ウィンドウで、tar.gz または qcow2 ファイルをアップロードします。
5. [File Type] ドロップダウンリストから、イメージタイプ（[Image Package]、[Scaffold]、または [Disk Image]）を選択します。
6. （任意）説明とタグを追加して、イメージを識別しやすくします。使用可能なデフォルトタグを使用するか、独自のカスタムタグを作成できます。
7. ディスクイメージをアップロードする場合は、[VNF Type]、[VNF Type]、および [Vendor] の値を選択します。



8. [Upload] をクリックします。

VNF パッケージを編集するには、次の手順を実行します。

1. [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。
2. [Virtual Images] をクリックします。
3. 目的のイメージの [...] をクリックし、[Edit] を選択します。



4. 必要な変更を行った後、[Update] をクリックします。

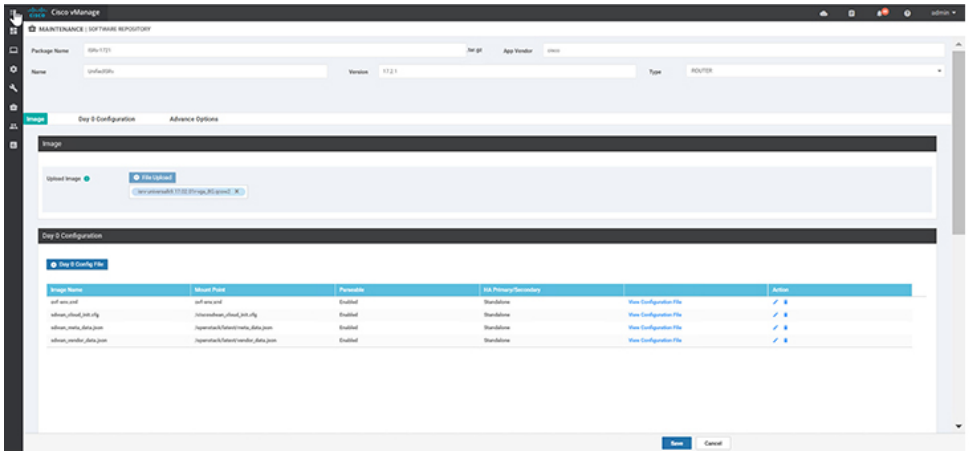
（注） Cisco vManage は Cisco VNF のみを管理しますが、VNF 内の 1 日目 および N 日目の設定は他の VNF ではサポートされません。VM パッケージの形式と内容、および image_properties.xml とマニフェスト（package.mf）のサンプルの詳細については、『NFVIS Configuration Guide』の「VM Image Packaging」[英語] を参照してください。

同じ VM、同じバージョン、Communication Manager（CM）タイプの複数のパッケージをアップロードするには、3つの値（名前、バージョン、VNF タイプ）のいずれかが異なることを確認します。その後、アップロードする VM *.tar.gz を再パッケージ化できます。

次に、ISRv パッケージの作成方法の例を示します。

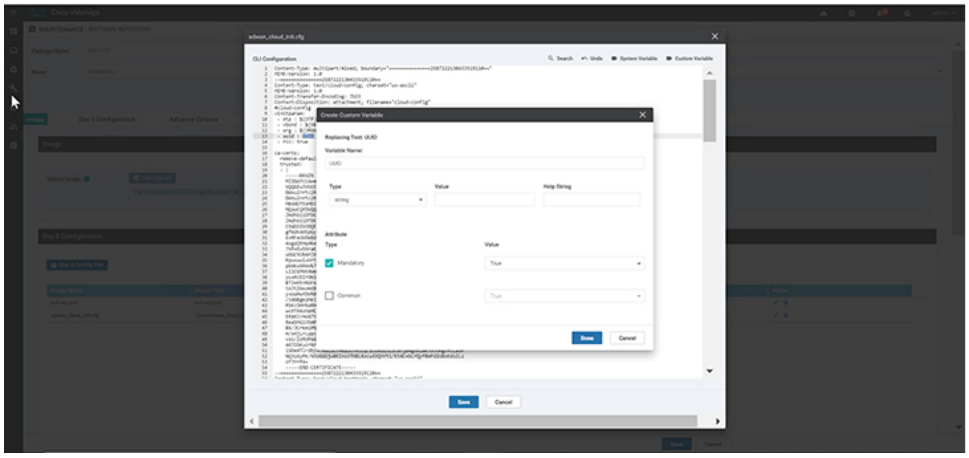
1. ブートストラップ設定のルートディスクイメージをアップロードします。

   イメージの横にある [View Configuration File] をクリックします。



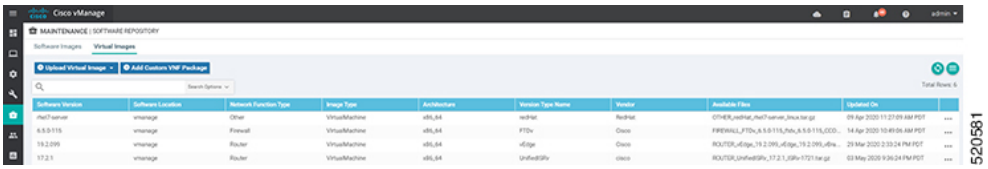
2. 変数を選択し、[Custom Variable] をクリックします。ポップアップウィンドウで、ドロップダウンメニューから変数タイプを選択します。

   [Done] をクリックしてから、 [Save] をクリックします。



3. 必要に応じてイメージプロパティを選択できます。

4. イメージパッケージが作成され、仮想イメージのリストに追加されたことを確認できます。



デバイスの検出と展開

WAN エッジデバイスは、ブートアップ時に Cisco vBond オーケストレータに接続し、セキュアな一時的な DTLS 制御接続を確立します。Cisco vBond 情報は、IP アドレスまたは解決可能なドメイン名 FQDN を使用し、WAN エッジデバイスの CLI を通じて手動で設定できます。または、PnP または ZTP プロセスによって自動的に取得することもできます。

SD-Branch コントローラ（Cisco vBond、Cisco vManage、および Cisco vSmart）と WAN Edge デバイスは、セキュアな制御接続を確立する前に、相互に認証して信頼する必要があります。SD-Branch コントローラが相互に認証し、WAN エッジデバイスが認証されると、次のようになります。

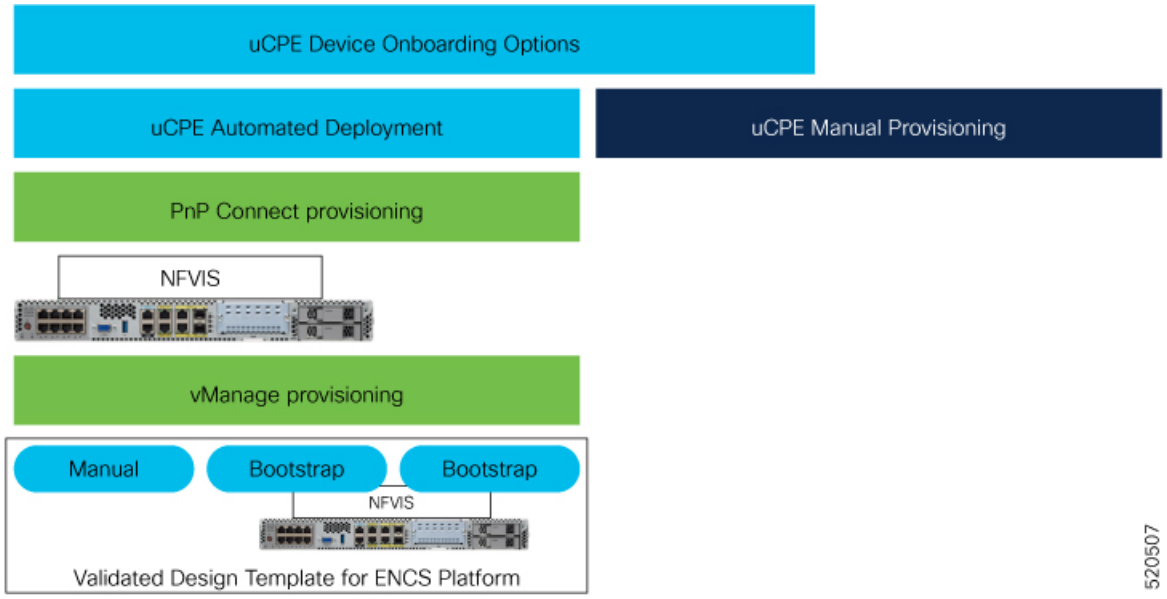
- 証明書ルート CA の信頼ルートの検証
- 受信した証明書の組織単位（OU）の組織名をローカルに設定された OU と比較します。
- 証明書のシリアル番号を承認済みのホワイトリストと比較します。

WAN エッジデバイスがコントローラを認証すると、次のようになります。

- 証明書ルート CA の信頼ルートの検証
- 受信した証明書 OU の組織名をローカルに設定された OU と比較します。

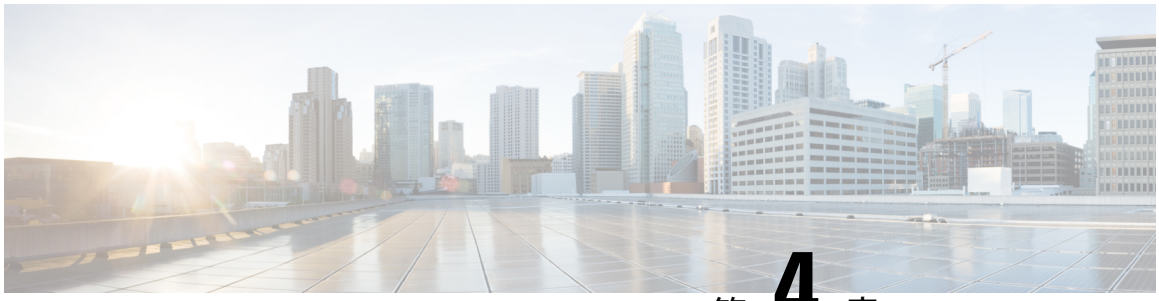
認証に成功すると、vBond オーケストレータはセキュアな一時的な DTLS 制御接続を確立し、Cisco vManage IP アドレスを共有します。この時点で、Cisco vBond オーケストレータは、他の SD ブランチコントローラ（Cisco vManage および Cisco vSmart）に、WAN エッジデバイスからの制御接続要求を予期するよう通知します。ENCS デバイスは、Cisco SD-WAN デバイスとは異なり、vSmart との制御接続を維持しません。

NFVIS WAN エッジデバイスは、Cisco vManage 情報を学習すると、Cisco vManage サーバーへの制御接続を開始します。認証に成功すると、別のセキュアで永続的な DTLS/TLS 接続が確立されます。Cisco vManage は、WAN エッジデバイスに接続されたデバイステンプレートに基づいて、NETCONF プロトコルを使用して設定をプロビジョニングします。



NFVIS WAN エッジデバイスのデフォルトの動作は、次のとおりです。

- オンボーディングプロセス中のみ、1 つの WAN トランスポートを介した Cisco vBond への一時的な DTLS 制御接続を保護します。
- 単一の WAN トランスポートを介した Cisco vManage への永続的な DTLS/TLS 制御接続を保護します。



第 4 章

Cisco NFVIS SD-Branch ソリューションの設計

NFVIS SD-Branch ソリューションは、完全なサービス機能を備えたブランチデバイスのゼロタッチプロビジョニング（ZTP）を提供します。WAN 回線タイプ、ネットワーク IP アドレス、およびトポロジを設定すると、ENCS ネットワーク コンピューティング WAN エッジ プラットフォームをプロビジョニングする際に固有の考慮事項が生じます。

WAN エッジのオンボーディング方法

展開の自動化

展開の自動化により、工場出荷時のデフォルト設定で NFVIS WAN エッジデバイスを SD-WAN ネットワークに安全にオンボーディングおよび展開できます。

自動展開は、ENCS 物理プラットフォームの PnP プロセスを使用して vBond IP アドレスを動的に検出します。

このオンボーディングオプションを使用するための主な要件は次のとおりです。

- NFVIS WAN エッジデバイスは、ダイナミック IP アドレス、デフォルトゲートウェイ、および DNS 情報を提供できる WAN トランスポートに接続する必要があります。

  静的 IP アドレスがある場合は、次の設定例を使用して IP アドレスを設定する必要があります。

```
configure terminal
bridges bridge wan-br
no dhcp
bridges bridge wan-br
no dhcp
system settings wan ip address 1.1.1.1 255.255.255.0
system settings default-gw 1.1.1.2
system settings dns-server 8.8.8.8
```

```
pnp automatic dhcp disable
pnp automatic dns disable
pnp automatic cco enable
commit
```

- NFVIS WAN エッジデバイスは、プラグアンドプレイ接続サーバーの devicehelper.cisco.com を DNS で解決できます。
- Cisco vManage では、デバイスを正常にオンボードするために、デバイス設定を作成して WAN エッジデバイスに接続する必要があります。

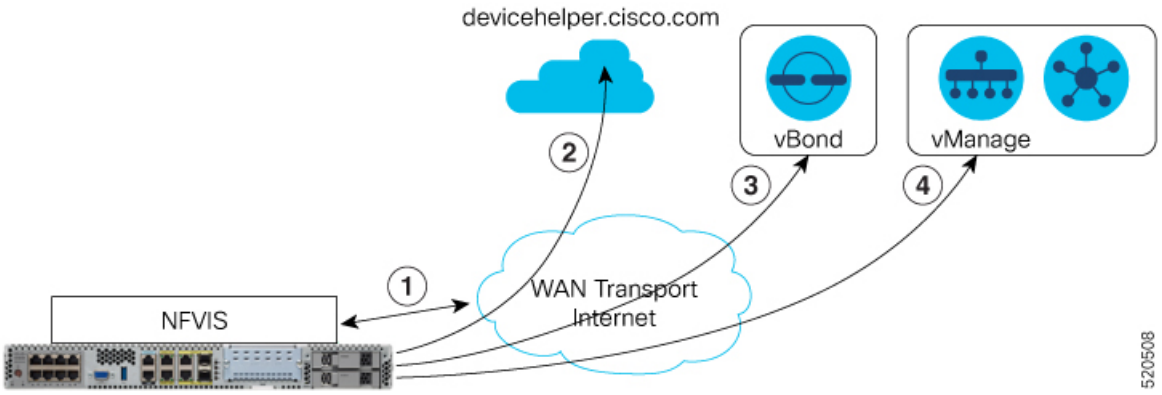
Cisco vBond への PnP リダイレクションの進行状況を表示するには、**show pnp status**コマンドを使用します。

```
Device# show pnp status

pnp status response PnP Agent is not running
server-connection
status: Success
time: 22:22:20 Dec 09
device-info
status: Success
time: 22:09:19 Dec 09
capability
status: Success
time: 22:06:17 Dec 09
redirection
status: Success
time: 22:25:46 Dec 09
certificate-install
status: Success
time: 22:51:26 Dec 09
device-auth
status: Success
time: 22:01:29 Dec 09

pnp status ip-address ""
pnp status ipv6-address ""
pnp status port ""
pnp status transport ""
pnp status cafile ""
pnp status created_by user
pnp status dhcp_opt43 0
pnp status dns_discovery 0
pnp status cco_discovery 0
pnp status dhcp-ipv6 0
pnp status dns-ipv6 0
pnp status cco-ipv6 0
pnp status timeout 0
```

障害が発生した場合は、**pnp action command stop**、**pnp action command start**、または**pnp action command restart**コマンドを使用してプロセスを開始、停止、または再起動できます。

プラグアンドプレイプロセス

デイゼロの自動化されたプラグアンドプレイ（PnP）プロセスは、SD-WAN オーバーレイネットワークに参加するための NFVIS WAN エッジデバイスの検出、インストール、およびプロビジョニングを行うための簡単で安全な手順を提供します。



PnP オンボーディングプロセスの手順は次のとおりです。

1. 起動時に NFVIS WAN エッジデバイスは、WAN トランスポート（通常はインターネット）に接続されているサポート対象デバイスの PnP インターフェイスで、DHCP 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。
2. NFVIS WAN エッジデバイスは、シスコがホストする PnP 接続サーバーに到達しようとします。ルータは devicehelper.cisco.com で PnP サーバーの名前を解決しようとし、HTTPS 接続を使用して組織名などの SD-WAN vBond オーケストレータに関する情報を収集します。

> **注** エンタープライズルート CA 証明書を使用する ENCS 展開の場合、WAN エッジデバイスは、PnP Connect ポータルから vBond および組織名情報とともにルート証明書を受信します。
>
> devicehelper.cisco.com の結果としてエンタープライズルート CA 証明書が予期される場合は、**show certificate root-ca-cert** コマンドを使用して証明書が受信されたことを確認します。

3. WAN エッジデバイスは、シャーシまたはシリアル番号とルート証明書を使用して Cisco vBond オーケストレータで認証します。認証に成功すると、Cisco vBond オーケストレータはデバイスに Cisco vManage を提供します。
4. WAN エッジデバイスは、Cisco vManage とのセキュアな接続を開始および確立し、Cisco vManage から NETCONF を使用して設定をダウンロードし、SD-WAN オーバーレイネットワークに参加します。

ステージング

NFVIS WAN エッジデバイスは、Cisco vManage から制御される証明書ステータスを通じてステージングできます。デバイスの証明書は、展開前にステージング状態にすることができます。ステージング状態の間、WAN エッジデバイスは SD-WAN コントローラとのセキュアな制御接続のみを確立できます。データプレーン接続は作成されません。

ステージングされた状態の WAN エッジデバイスを使用してデバイスを準備できます。これには、ソフトウェアのアップグレードとデバイスの設定が含まれます。その前に、Cisco vManage GUI の証明書のステータスを [Staging] から [Valid] に変更して、SD-WAN オーバーレイネットワークに完全に統合します。

NFVIS WAN エッジ証明書のステータス

Cisco vManage の NFVIS WAN Edge デバイス証明書は、次のいずれかの状態になるように設定できます。

- [Invalid]：この状態では、WAN エッジデバイスは SD-WAN コントローラとオーバーレイネットワークに参加する権限がありません。デバイスは、SD-WAN コンポーネントへのコントロールプレーンまたはデータプレーン接続を形成しません。
- [Staging]：この状態では、WAN エッジデバイスは SD-WAN コントローラ（Cisco vBond、Cisco vManage）のみにセキュアなコントロールプレーン接続を確立します。オーバーレイネットワーク内の他の WAN エッジデバイスとのデータプレーン接続は確立されないことに注意してください。
- [Valid]：この状態では、WAN エッジデバイスは SD-WAN ネットワークに完全にオンボードされています。デバイスは、コントローラとのセキュアなコントロールプレーン接続、および SD-WAN オーバーレイネットワーク内の他のすべての WAN エッジルータとのセキュアなデータプレーン接続を確立します。

ゼロトラストモデル

NFVIS SD-Branch ソリューションは、ゼロトラストモデルです。WAN エッジデバイスの信頼には、WAN デバイスのホワイトリストとルート証明書が含まれます。また、デバイス証明書は、ネットワークで承認されるために [Valid] の状態である必要があります。

WAN エッジデバイスは、すべての SD-WAN コントローラによって認識され、ネットワークに接続する前に承認される必要があります。デバイスの認証は、次の方法で実行できます。

- プラグアンドプレイ接続ポータルでデバイスを追加し、vBond コントローラプロファイルに関連付けます。
- デバイスリストを Cisco vManage に同期するか、プロビジョニングファイルを Cisco vManage に手動でダウンロードしてインポートします。

（注） WAN エッジネットワークデバイスは、スマートアカウントとバーチャルアカウントの詳細を割り当てることで、プラグアンドプレイ接続ポータルの Cisco vBond プロファイルに自動的に追加して関連付けることができます。

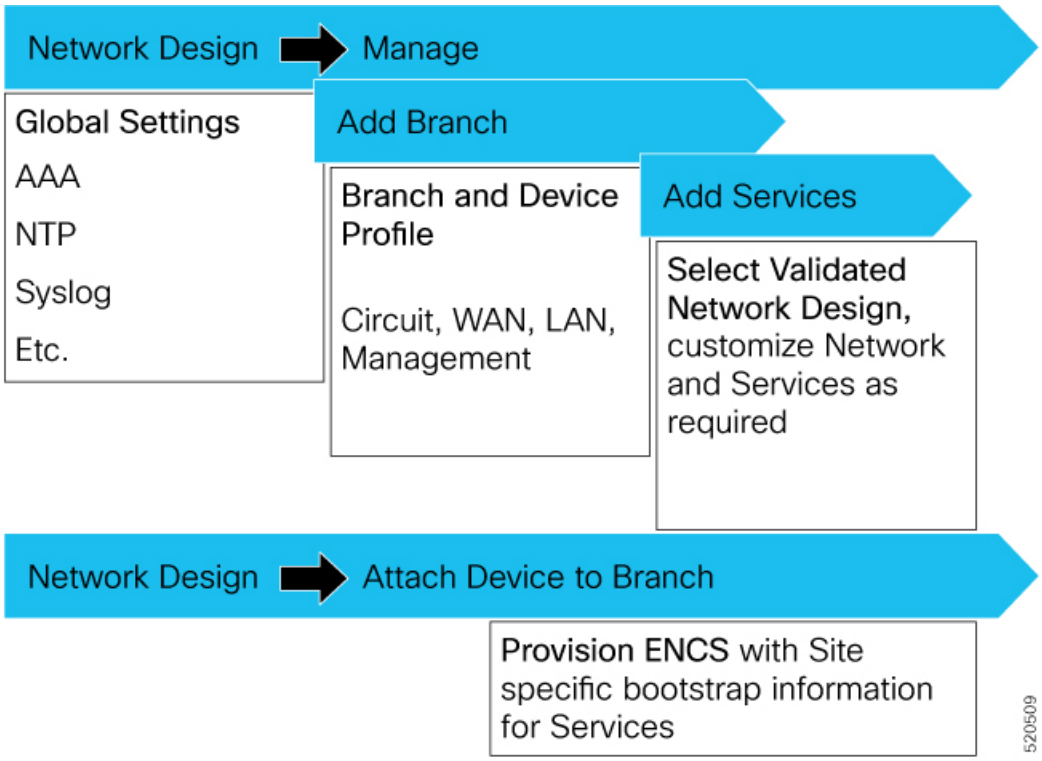
ネットワーク ファイアウォールの要件

ファイアウォールの背後に WAN エッジデバイスを展開するには、SD-WAN コンポーネントが安全に接続を確立できるように、適切なポートが開かれていることを確認します。

- デフォルトでは、すべての SD-WAN コンポーネントは DTLS、UDP ベースポート 12346 を使用して接続を確立しようとします。
- WAN エッジデバイスがデフォルトのベースポートを使用して SD-WAN コントローラとの制御接続を確立できない場合、または複数の WAN エッジデバイスが NAT デバイスの背後に配置されている場合、WAN エッジデバイスは 5 つのベースポートを介してポートホップできます。ポート 12346、12366、12386、12406、12426 でポートホッピングが順番に実行されてから、ポート 12346 に戻ります。WAN エッジデバイスでは、ポートホッピングがデフォルトで有効になっています。
- ポートオフセットは、NAT デバイスの背後に配置された各 WAN エッジデバイスを一意に識別し、同じベースポートを使用しないように設定できます。ポートオフセットは 0 ー 19 の数字で、0 がデフォルトです。ポートオフセットが設定されている場合、デフォルトのベースポートはポートオフセット値で増分され、後続のポートは 20 ずつ増分されます。たとえば、ポートオフセットの値が 1 に設定された展開では、WAN エッジはポート 12347（12346 + 1）との接続を開始し、その後、ポート 12347、12367、12387、12407、12427 でポートホッピングが順番に実行され、ポート 12347 に戻ります。
- WAN エッジデバイスは、同じ基本ポートを使用して、オーバーレイネットワーク内の他の WAN エッジデバイスとのデータプレーン接続（IPsec 接続や BFD セッションなど）を確立します。
- vBond オーケストレータは、DTLS、UDP 送信元ポート 12346 を常に使用して、SDWAN コンポーネントとの制御接続を確立します。デフォルトポートは、設定を変更することで変更できます。

ネットワーク設計

オーバーレイ ネットワーク トポロジを作成および管理するには、Cisco vManage のネットワーク設計機能を使用します。ネットワークトポロジに回線、データセンター、およびブランチサイトを追加し、トポロジ内の要素の LAN、WAN、および管理インターフェイスを設定し、トポロジを確認し、関連タスクを実行できます。ネットワーク設計操作は、データセンターやブランチサイトを含む小規模な導入で特に役立ちます。



ネットワーク設計は、次の主要なワークフローで構成されます。

- ネットワークトポロジの作成：回線、データセンター、およびブランチサイトをこの順序で作成します。ネットワークトポロジには、少なくとも 1 つの回線と 1 つのデータセンターを含める必要があります。
- デバイスプロファイルの設定：LAN、WAN、および管理設定のグローバルパラメータとオプションを設定します。
- デバイスプロファイルの接続：デバイスプロファイルをデバイスに接続します。
- 継続的な管理：ネットワークトポロジに要素を追加し、必要に応じて要素の設定を変更します。

ネットワーク設計要素の設定

ネットワーク設計機能を使用すると、新しいオーバーレイ ネットワーク トポロジを作成し、トポロジ内の既存の要素を変更できます。これらのアクティビティは、Cisco vManage の [Network Design] ページから実行できます。

新しいネットワークトポロジを作成するには、次の手順を示されている順序で実行します。

表 *4*:

手順	説明	参照先
1	回線を追加する。	回線の設定を参照してください。
3	ブランチサイトを追加する 。	ブランチサイトの設定を参照してください。
4	グローバルパラメータを設定する。	グローバルパラメータの設定を参照してください。
5	デバイスプロファイルを設定する。	デバイスプロファイルの設定を参照してください。

ネットワークトポロジには、少なくとも 1 つの回線が含まれている必要があります。ネットワークトポロジを作成した後、その要素を直接変更できます。

回線の設定

各ネットワークトポロジには少なくとも 1 つの回線が必要で、最大 18 の回線を設定できます。NFVIS は、制御接続の確立に 1 つの回線のみを使用できます。設定された回線に障害が発生した場合、代替回線は使用できません。

ネットワークトポロジの回線を設定するには、次の手順を実行します。

1. Cisco vManageメニューで、[Configuration] > [Network Design] を選択します。
2. [Create Network Design]（ネットワークトポロジをまだ作成していない場合に表示）または [Manage Network Design]（ネットワークトポロジを作成した場合に表示）を選択します。
3. [Circuits] を選択します。

   回線を設定するための画面が表示されます。回線が作成されている場合は、この画面に表示されます。回線を削除するには、対応する削除アイコンをクリックします。
4. [Add New] をクリックします。
5. [Private] または [Public] のオプションボタンを選択して、回線がプライベートかパブリックかを示します。
6. [Circuit Color] ドロップダウンリストから、定義済みの色を選択して、回線内の転送ロケーション（TLOC）を一意に識別します。

   選択した色は、トポロジ内の他の回線の TLOC には使用できません。
7. さらに回線を追加するには、ステップ 2 ー 5 を繰り返します。
8. 追加した回線を削除するには、対応する [Delete] アイコンをクリックします。
9. [Finish] をクリックします。
10. ネットワーク設計画面で [Save] をクリックします。

    行った更新を保存しない場合は、[Cancel] をクリックします。

ブランチサイトの設定

ブランチサイトの設定では、ブランチサイトに名前を割り当て、デバイスプロファイルとセグメントを追加します。各ネットワークトポロジには、少なくとも1つのブランチサイトが必要です。

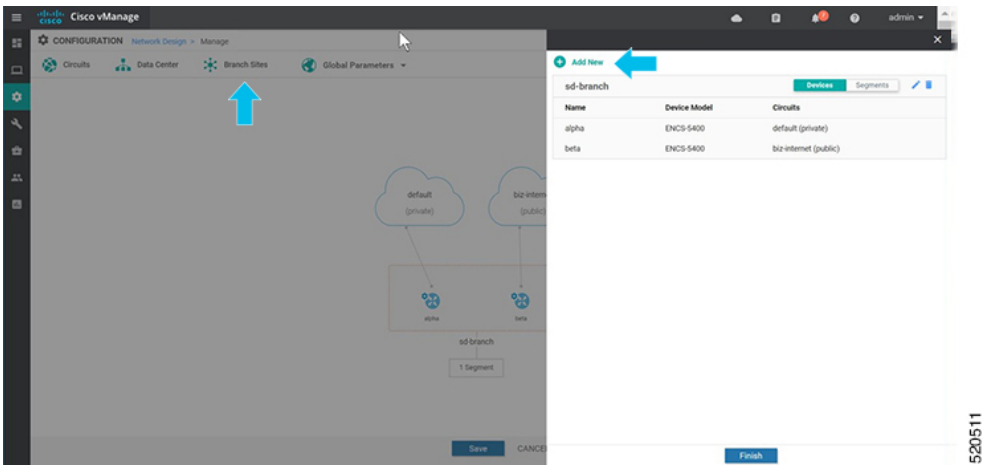
ネットワークトポロジのブランチサイトを設定するには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Network Design] を選択します。
2. [Create Network Design]（ネットワークトポロジをまだ作成していない場合に表示）または [Manage Network Design]（ネットワークトポロジを作成した場合に表示）を選択します。

   [Branch Sites] をクリックします。回線を 1 つも追加していない場合、このオプションはグレー表示されます。

   [Configure Branch Sites] ページが表示されます。ブランチサイトがすでに作成されている場合は、このページにリストされます。

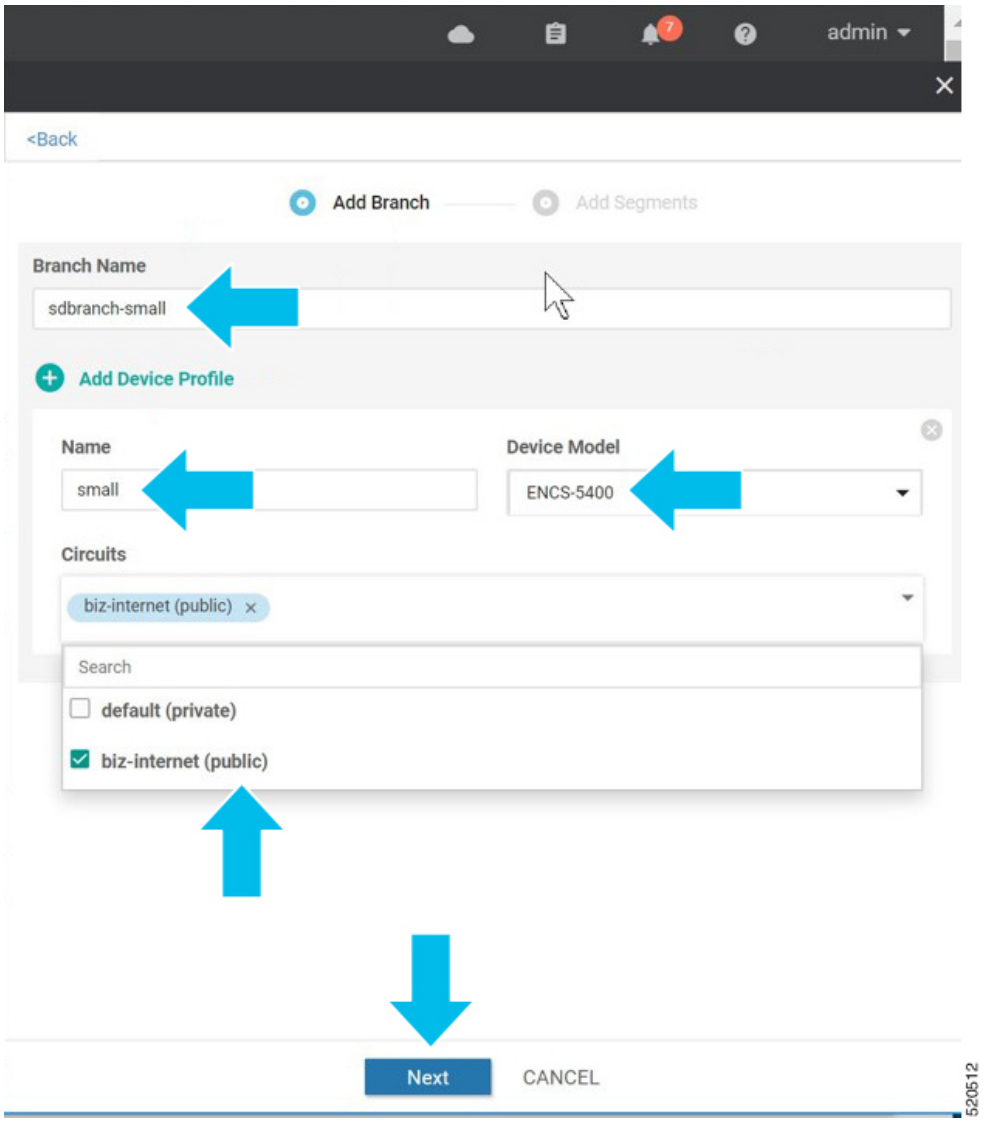
   ブランチサイトを追加するには、[Add new] をクリックします。



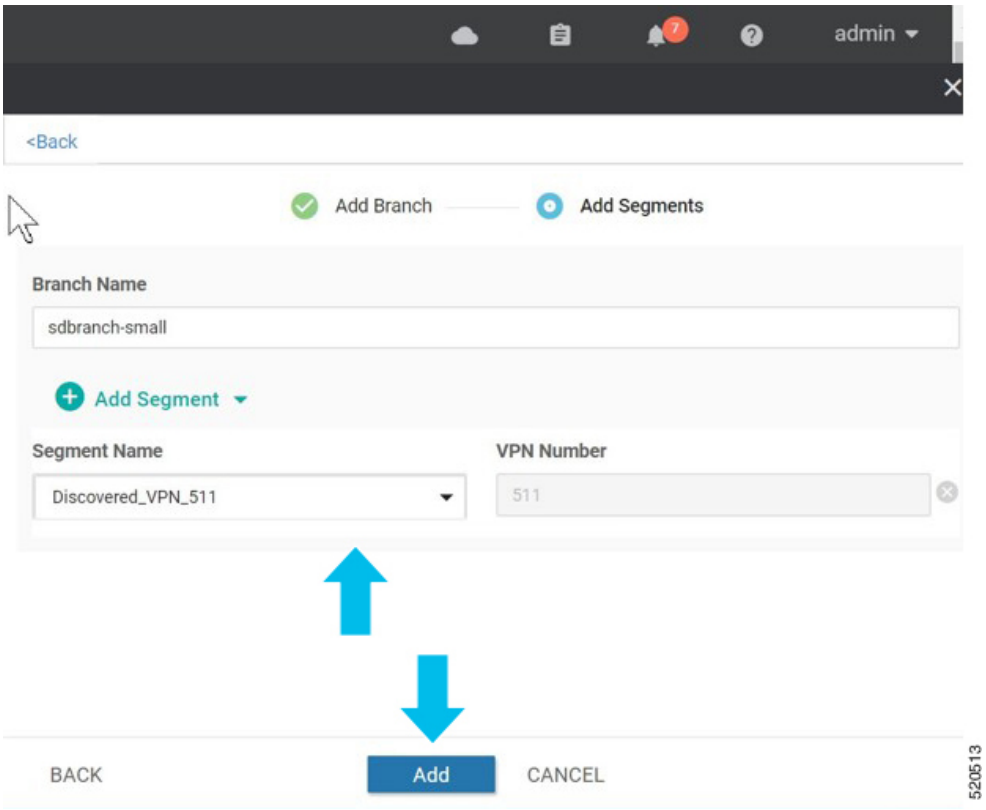
3. ブランチを追加するには、次の手順を実行します。
   1. [Branch Name] にブランチサイトの一意の名前を入力します。この名前は、トポロジ内の他のデータセンター、ブランチサイト、またはデバイスプロファイルには使用できません。名前には、文字、数字、アンダースコア、ハイフンを使用できますが、スペースや特殊文字は使用できません。
   2. 新しいデバイスプロファイルを追加するには、[Add Device Profile] をクリックします。

      各ブランチサイトには、少なくとも 1 つのデバイスプロファイルが必要です。デバイスプロファイルは、ブランチサイト内の特定のデバイスタイプに関連付けられ、それらのデバイスタイプにプッシュされる設定を提供します。
   3. [Name] にデバイスの名前を入力します。
   4. [Device Model] ドロップダウンリストから、デバイスプロファイルに関連づけるデバイスタイプを選択します。

5. [Circuits] を選択して、作成した回線のリストを表示し、デバイスプロファイルを関連付ける各回線の横にあるチェックボックスをオンにします。
6. [Next] をクリックします。

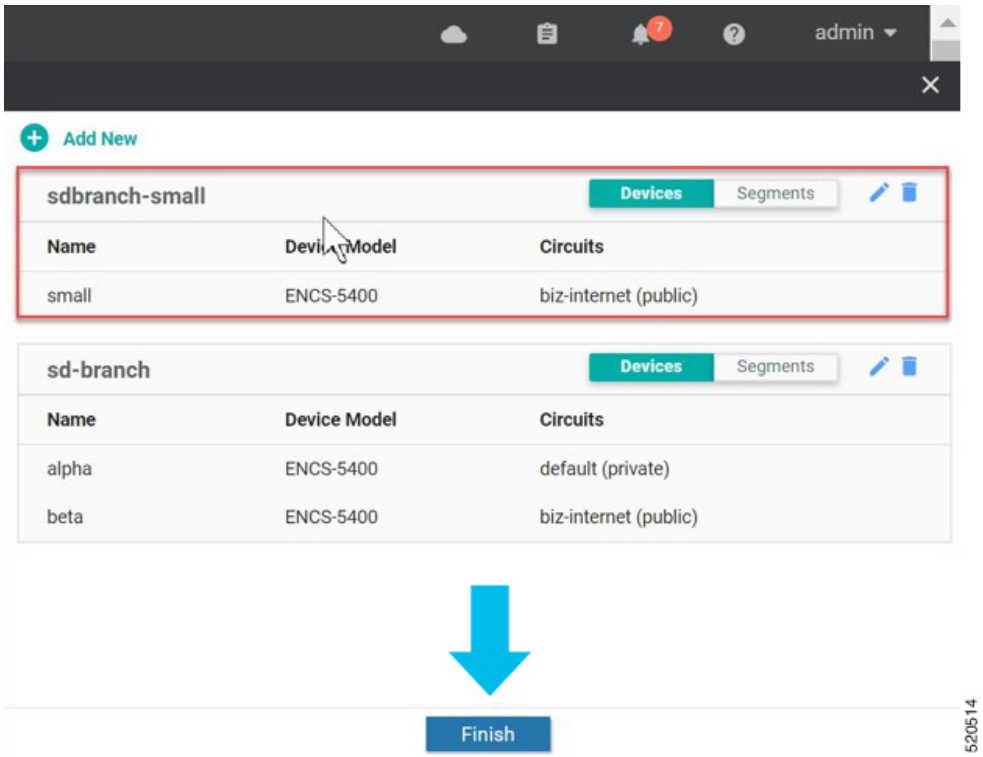


4. セグメントは、ブランチサイト内のすべてのデバイスプロファイルに関連付けられているサービス側VPNです。各ブランチサイトには、少なくとも1つのセグメントが必要です。複数のブランチサイトで同じセグメントを使用できます。1 つ以上のセグメントを追加するには、次の手順を実行します。
   1. [Add Segment] をクリックします。ドロップダウンリストからセグメントを選択します。VPN 番号には、セグメントに設定された VPN ID が自動的に入力されます。
   2. [Add] をクリックします。

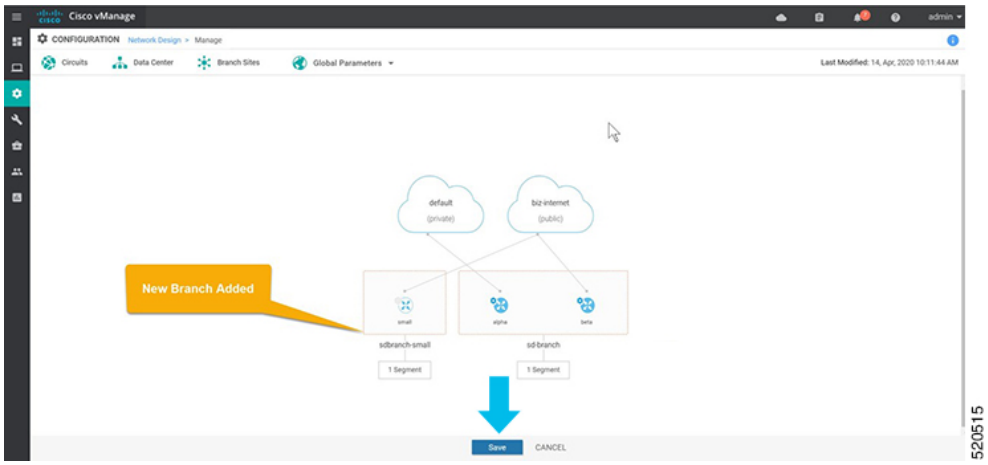


ブランチサイトのリストが表示されます。

5. [Finish] をクリックします。



6. [Network Design] ページで [Save] をクリックします。



グローバルパラメータの設定

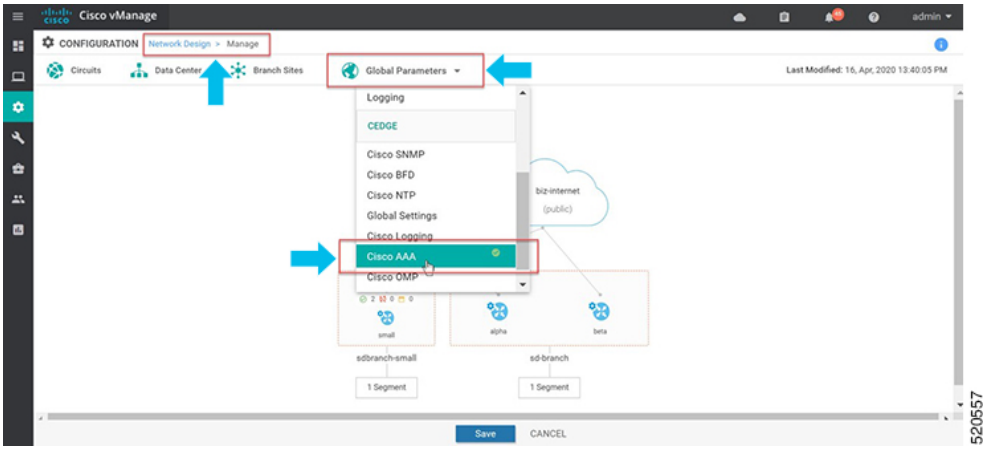
グローバルパラメータは、ネットワークトポロジ内のすべてのデバイスプロファイルで使用される設定です。グローバルパラメータを設定しない場合は、工場出荷時のデフォルト設定がデバイスプロファイルに使用されます。

SD-Branch は現在、NTP、AAA、およびロギングパラメータのみをサポートしています。

グローバルパラメータの設定：

1. [Cisco vManage] メニューから、[Configuration]、[Network Design] の順に選択します。
2. [Create Network Design]（ネットワークトポロジをまだ作成していない場合に表示）または [Manage Network Design]（ネットワークトポロジを作成した場合に表示）を選択します。

   [Global Parameters] を選択し、ドロップダウンリストから目的のテンプレートを選択します。

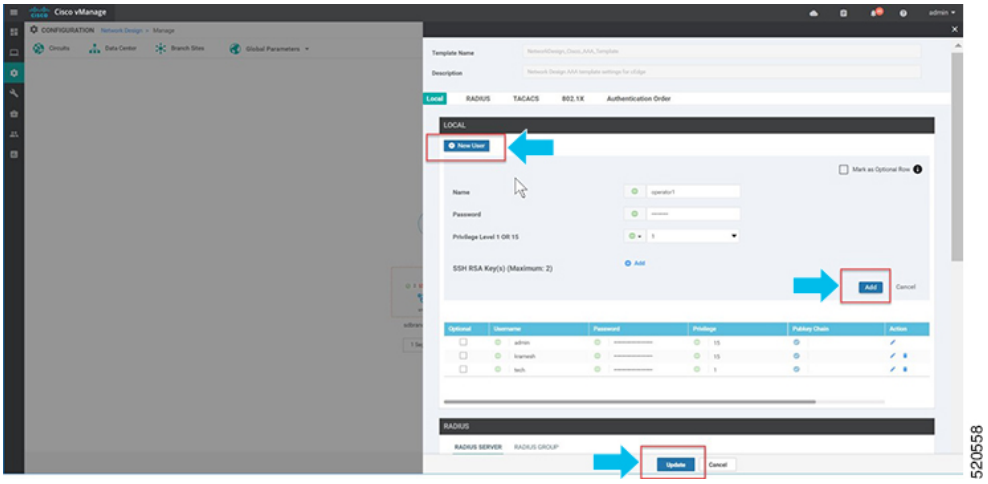


3. テンプレートの設定

   テンプレートの名前と説明は自動的に入力されます。変更はできません。テンプレートはネットワーク全体のすべてのデバイスに使用されるため、デバイスタイプを選択することはできません。

   新しいユーザーを追加するには、[+ New User] を選択し、詳細を入力します。[Add] をクリックします。

   [Update] をクリックし、設定を完了します。



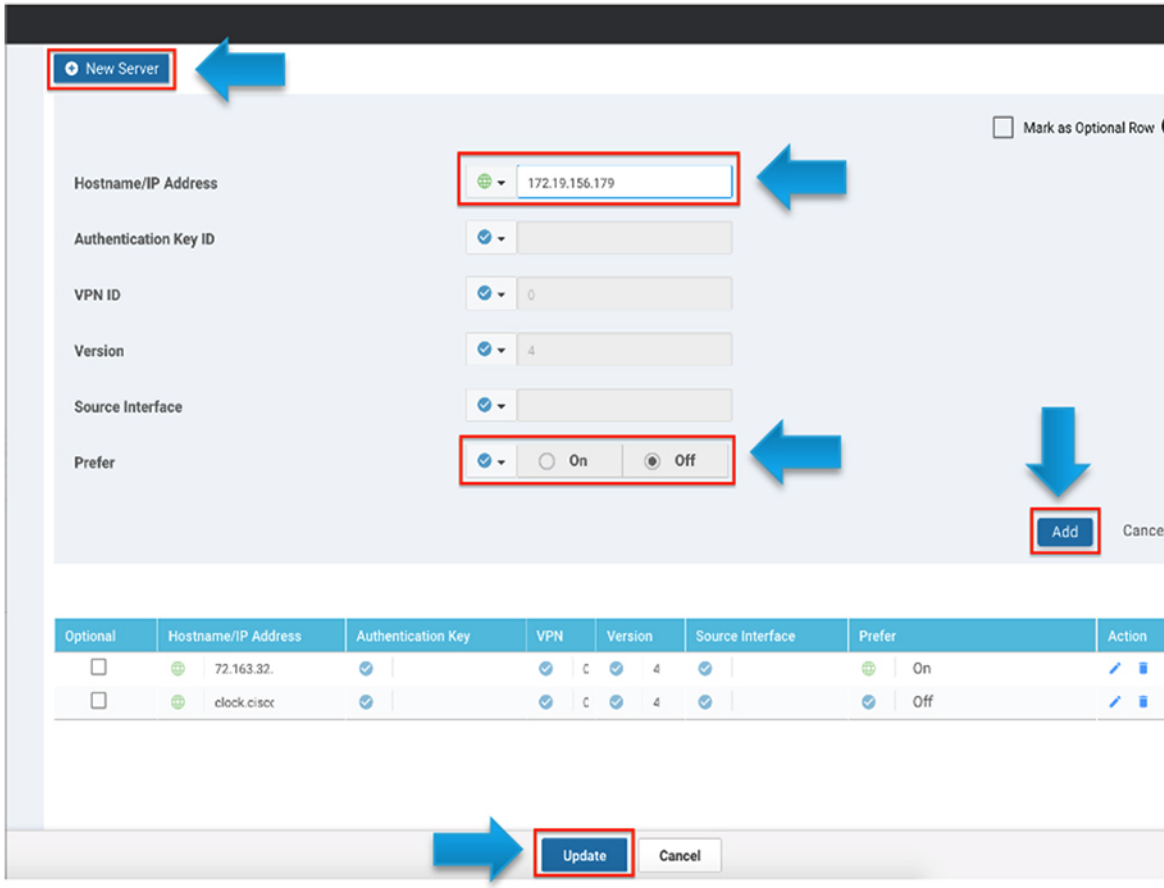
Cisco vManage 20.1 および 20.3 リリースは、ローカルユーザーの AAA グローバルパラメータのみをサポートします。TACACS および RADIUS 設定は、デバイスのアドオン CLI 機能の設定を使用して更新できます。

4. NTP サーバーを追加します。

   新しいサーバーを追加するには、[+ New Server] を選択し、[Hostname/IP Address] を入力します。

5. [Prefer] オプションを選択し、[Add] をクリックします。

   [Update] をクリックし、設定を完了します。

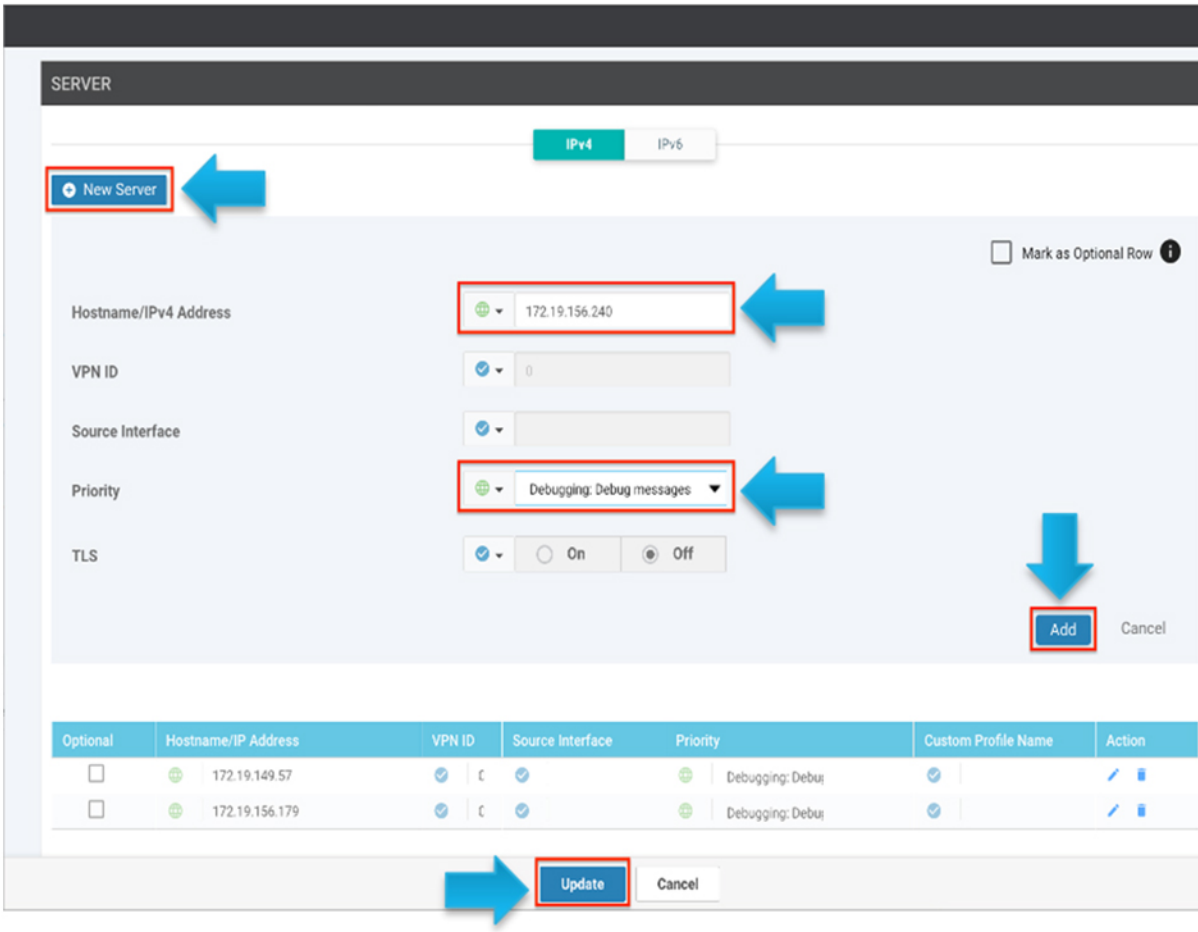


   [Authentication Key ID]、[VLAN ID]、[Version]、[Source Interface] は、NFVIS プラットフォームには適用されません。NFVIS プラットフォームは、1 つの優先 NTP サーバーと 1 つのバックアップ NTP サーバーのみをサポートします。

6. ロギングサーバーを追加します。

   新しいサーバーを追加するには、[+ New Server] を選択し、[Hostname/IP Address] を入力します。[Priority] オプションを選択し、[Add] をクリックします。

   [Update] をクリックし、設定を完了します。



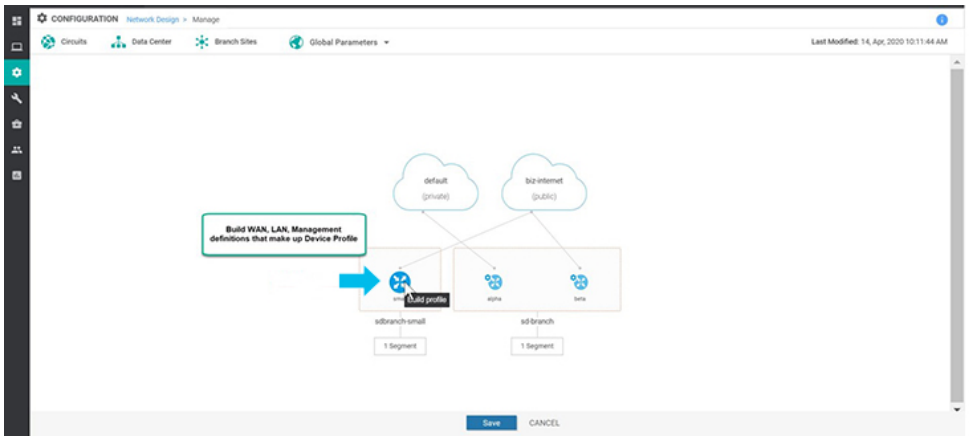
[VPN ID]、[Source Interface] は、NFVIS プラットフォームには適用されません。サポートされるロギングサーバーの最大数は 4 です。[Priority] が同じ設定を使用していることを確認します。NFVIS プラットフォームは、グローバル設定として 1 つのプライオリティまたはロギング重大度のみをサポートします。

デバイスプロファイルの設定

デバイスプロファイルをルータに接続する前に、データセンターまたはブランチサイトの各ルータにデバイスプロファイルを設定する必要があります。

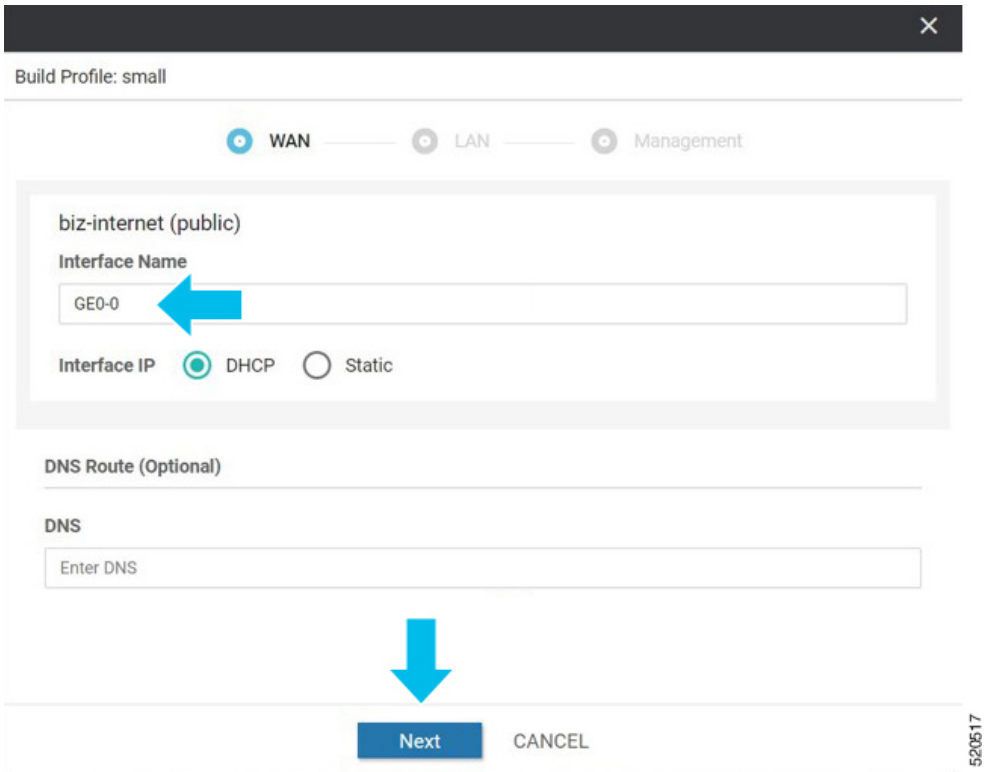
ネットワークトポロジでルータのデバイスプロファイルを設定するには、次の手順を実行します。

1. [Cisco vManage] メニューから、[Configuration]、[Network Design] の順に選択します。
2. ネットワーク図が [Network Design] ページに表示されます。デバイスのイメージ表示の上にマウスを移動して、[Build profile] を選択します。



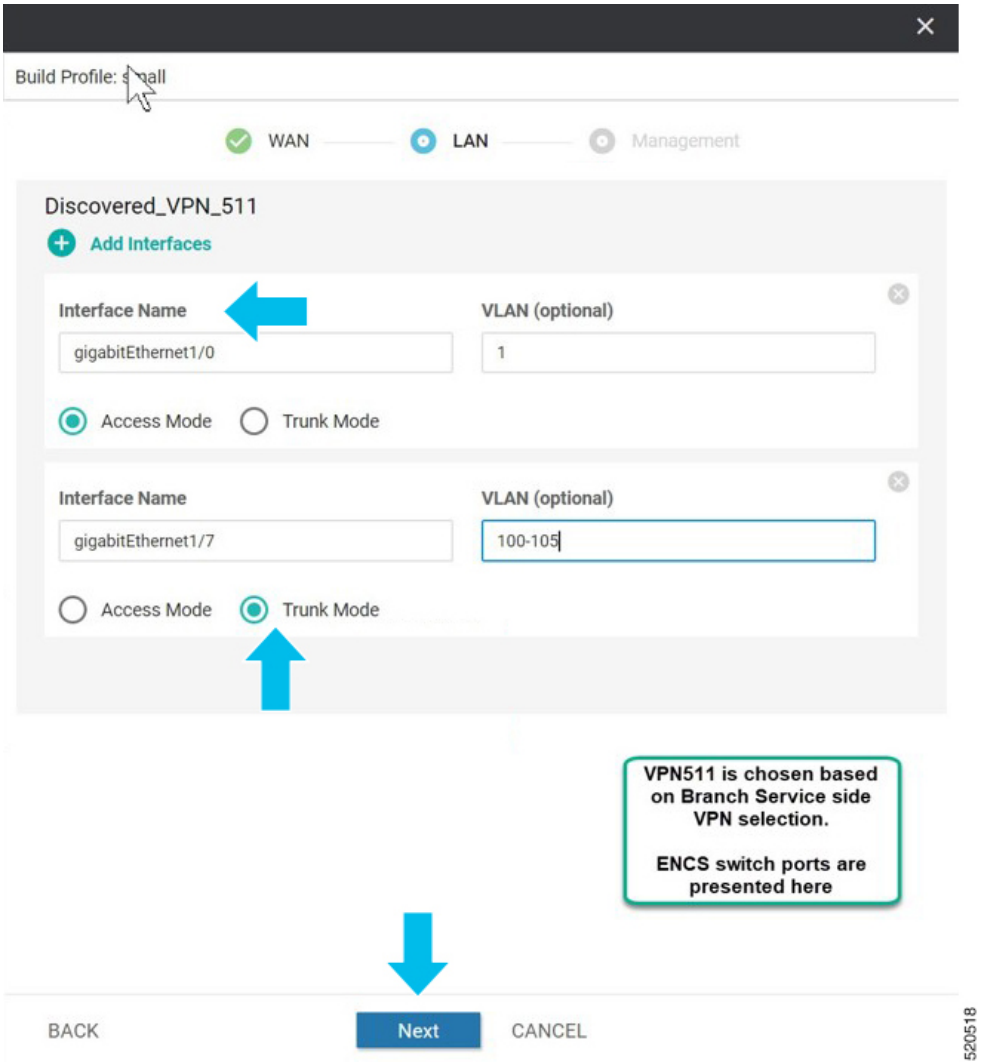
3. デバイスプロファイルを作成するには、プロファイルの WAN インターフェイスの詳細を入力します。

   - [Interface Name] に、このルータに関連付けられている回線に関連付ける TLOC インターフェイスの名前を入力します。
   - [DHCP] または [Static] のいずれかのオプションボタンを選択します。
   - （任意）プライマリ DNS サーバーの IP アドレスを [DNS Server] フィールドに入力します。
   - [Next] をクリックします。

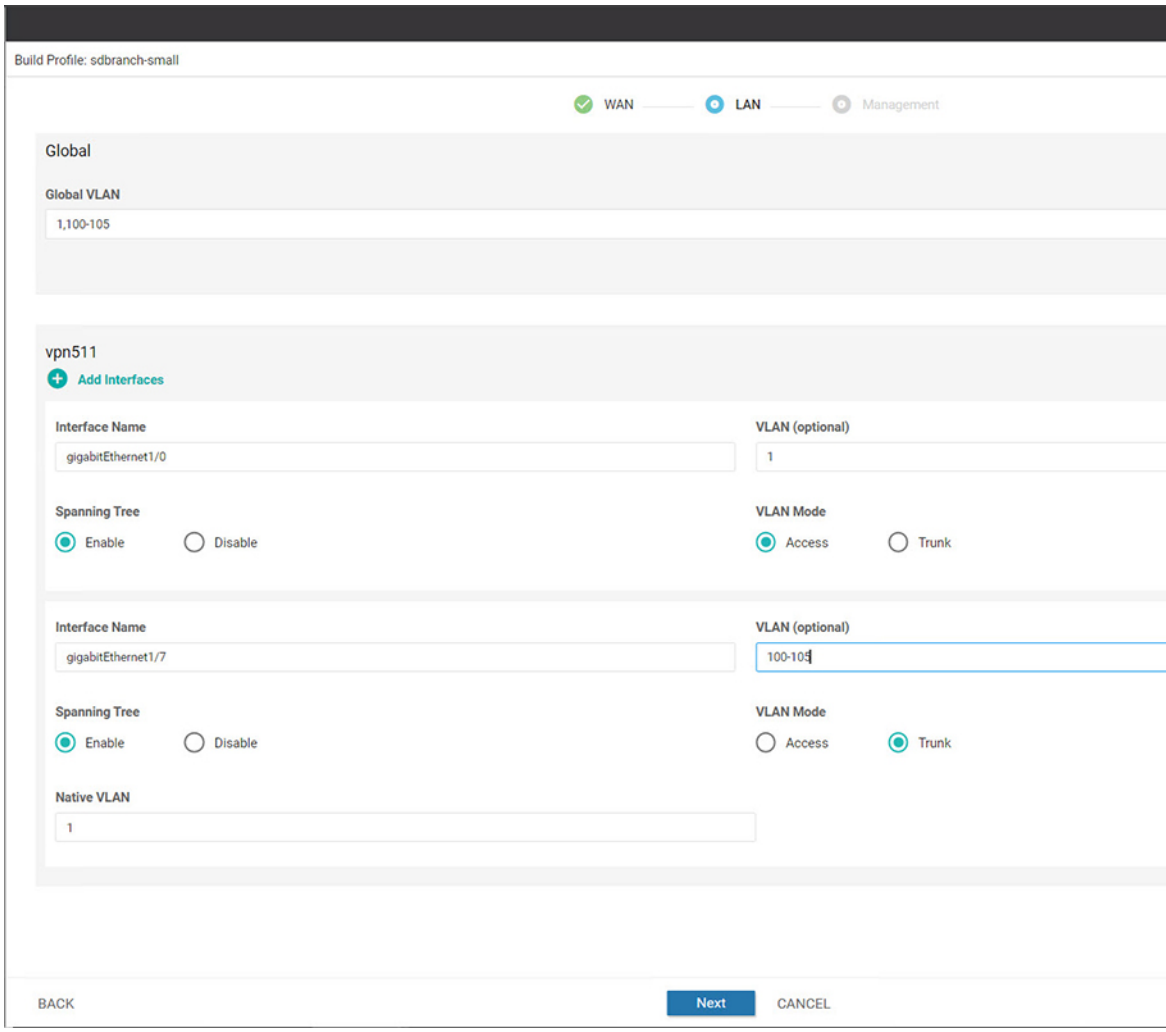


4. プロファイルの LAN インターフェイスの詳細を入力します。
   - [Interface Name] に LAN 側インターフェイスの名前を入力して、セグメントに関連付けます。
   - （任意）展開に必要な場合は、VLAN にサブインターフェイスを入力します。
   - [Access Mode] または [Trunk Mode] オプションボタンのいずれかを選択します。
   - [Next] をクリックします。

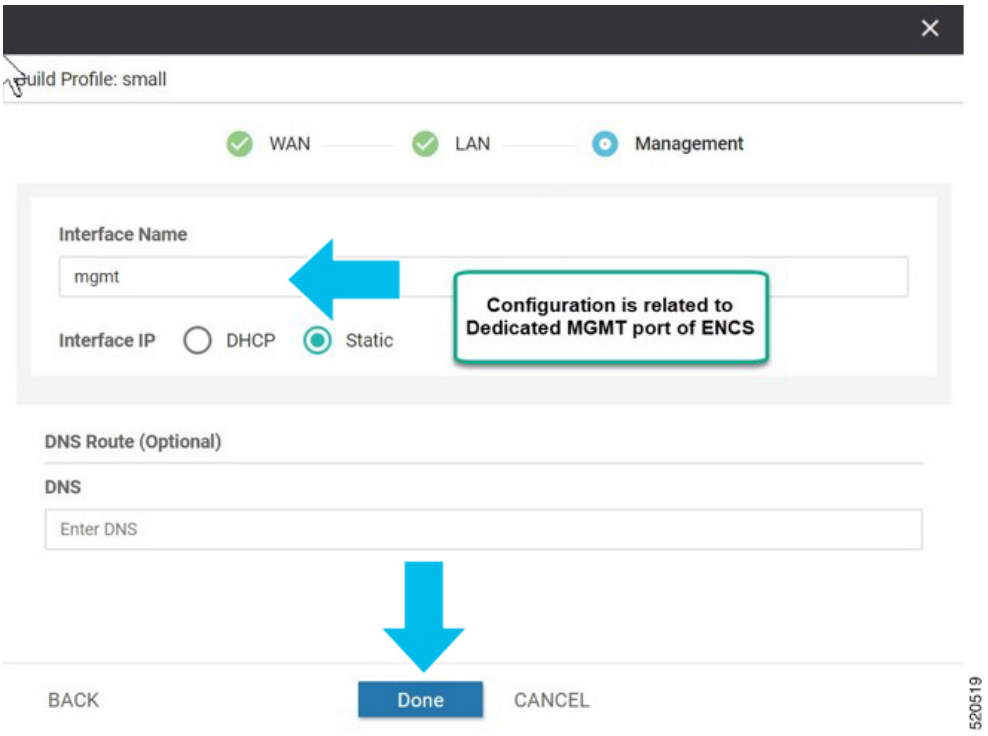
グローバル VLAN は、アドオン CLI テンプレートを使用して定義する必要があります。グローバル VLAN は、ENCS スイッチポートで使用されるすべての VLAN の集合です。



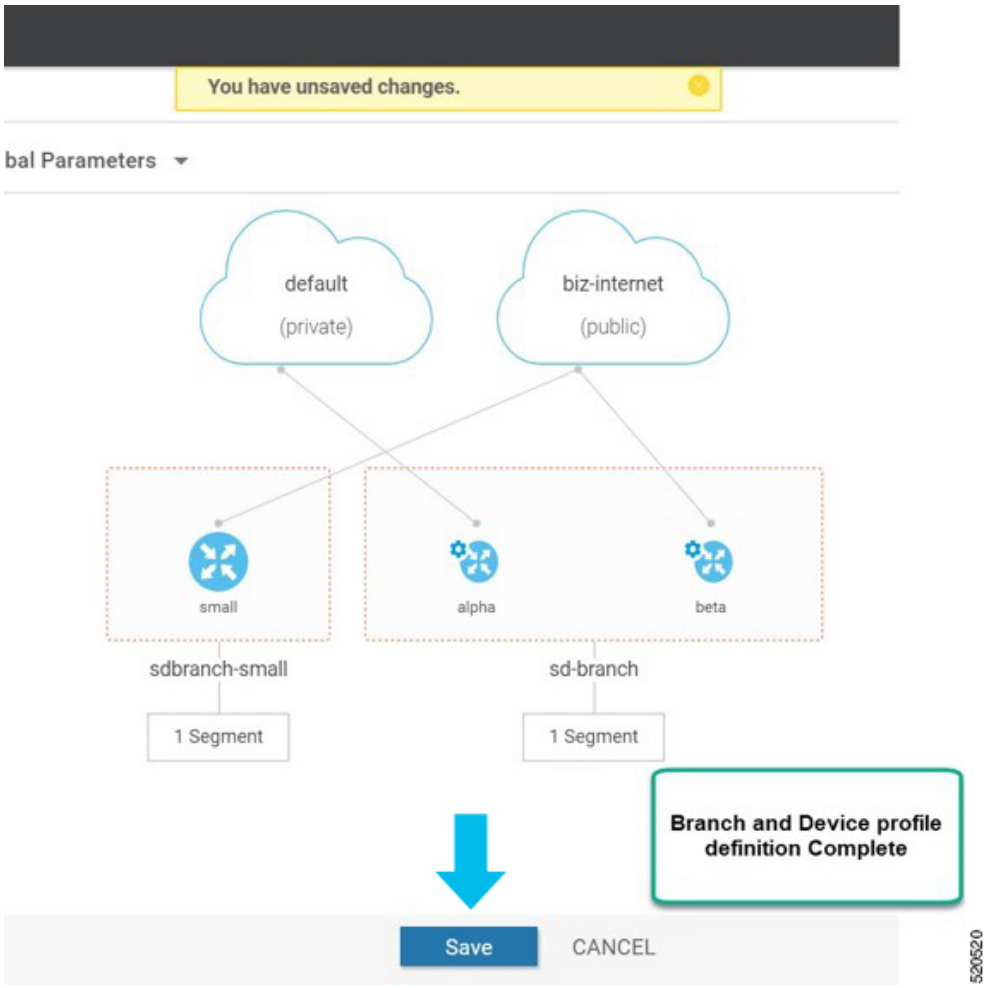
NFVIS 4.4 リリース以降、Cisco vManage から追加の LAN インターフェイスの詳細を設定できます。



5. プロファイルの管理インターフェイスの詳細を入力します。
   - [Interface Name] に管理インターフェイスの名前を入力して、デバイスに関連付けます。
   - [DHCP] または [Static] のいずれかのオプションボタンを選択します。
   - [Done] をクリックします。



6. ネットワーク設計画面で [Save] をクリックします。



ENCS デバイスプロファイルと追加サービス

ENCS 5400 デバイスの場合は、デバイスプロファイルとアドオンサービスの両方を設定する必要があります。デバイスプロファイルを設定したら、ENCS ブランチ設計でのサービスの追加に進みます。

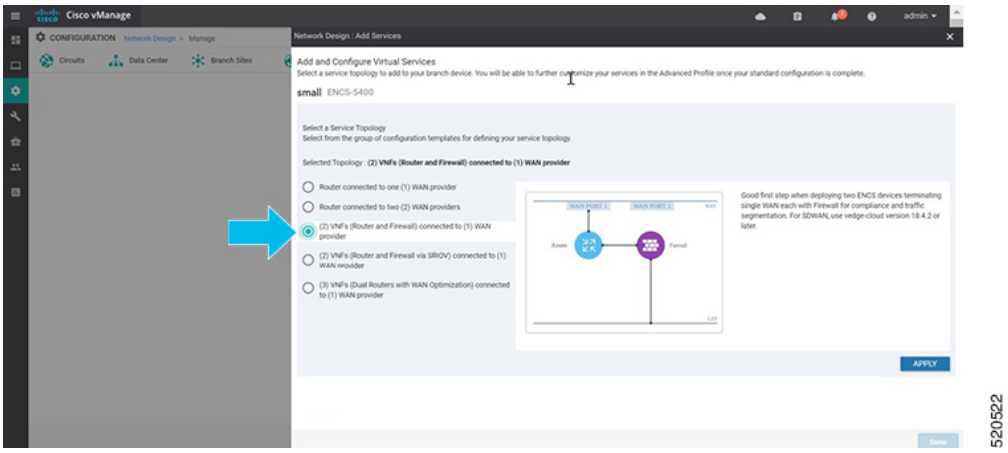
サービス、仮想ネットワーク、および関連する仮想スイッチまたはブリッジ用の VNF イメージパッケージは、ENCS ネットワーク設計の一部です。仮想 NIC（VNIC）は VNF サービスの一部であり、VNIC の順序は、異なるサービスを通過するトラフィックフローが意図した順序で連続するように正しく設定する必要があります。ユーザーエクスペリエンスを簡素化するために、シスコが設計した一連の規範的な検証済み設計を選択し、ネットワーク設計を完成させることができます。必要に応じて、ネットワークトポロジをカスタマイズして、サービスまたはネットワークを削除および変更することもできます。

次の例では、SD-WAN ルータと Cisco NGFW ベースのネットワークトポロジが作成されます。この手順は、シスコが検証した他のネットワーク設計テンプレートに適用できます。

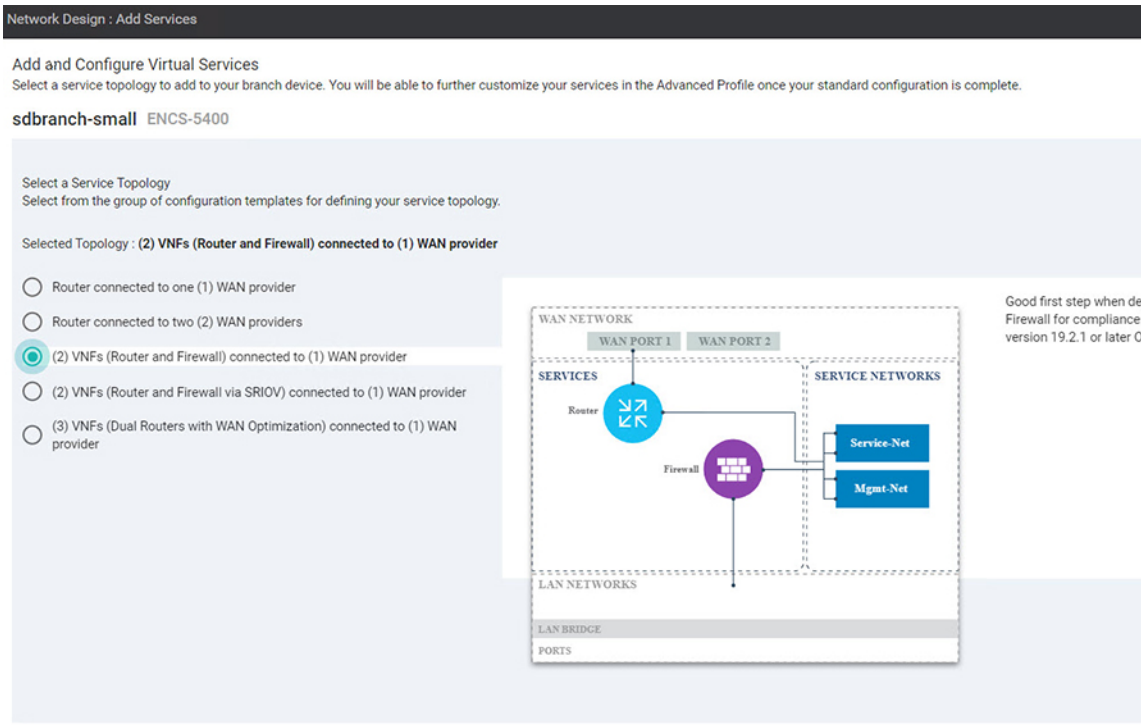
サイトグループのサービスを追加し、ネットワークトポロジテンプレートを作成するには、次の手順を実行します。

1. [Cisco vManage] メニューから、**[Configuration]** > **[Network Design]** を選択します。
2. ネットワーク図が [Network Design] ページに表示されます。ブランチデバイスのイメージ表示の上にマウスを移動し、[Add services] を選択します。

3. [Add services] ページで、使用可能な設定テンプレートのリストからサービストポロジを選択します。[Apply] をクリックします。



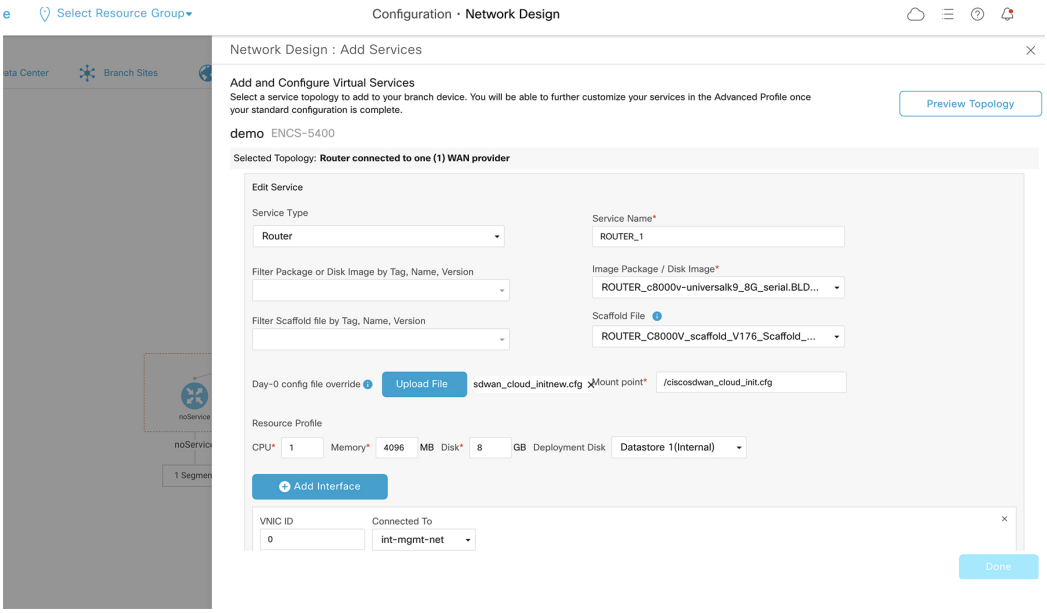
NFVIS 4.4 リリース以降、リストされているテンプレートのトポロジのグラフィカルビューを使用できます。



4. NFVIS 4.6.1 リリース以降、イメージの登録時に tar.gz ファイルまたは qcow2 ファイルのいずれかをアップロードできます。また、イメージを識別するためのキーワードでイメージにタグを付けることができます。scaffold ファイルをアップロードすることもできます。

   （任意）scaffold または tar.gz ファイルの設定、またはパッケージまたはスキャフォールドファイルの既存の第0日のコンフィギュレーションを上書きする第0日のコンフィギュレーション ファイルをアップロードするには、次の手順を実行します。

   - 変数は、「{{“”}}」で表されます。例：**{{SAMPLE_VARIABLE}}**
   - パスワードは「$${“ and “}」で表されます。例：**$${SAMPLE_PASSWORD}**
   - 無視される変数は、「${“ and “}」で表されます。例：**${NICID_0}**

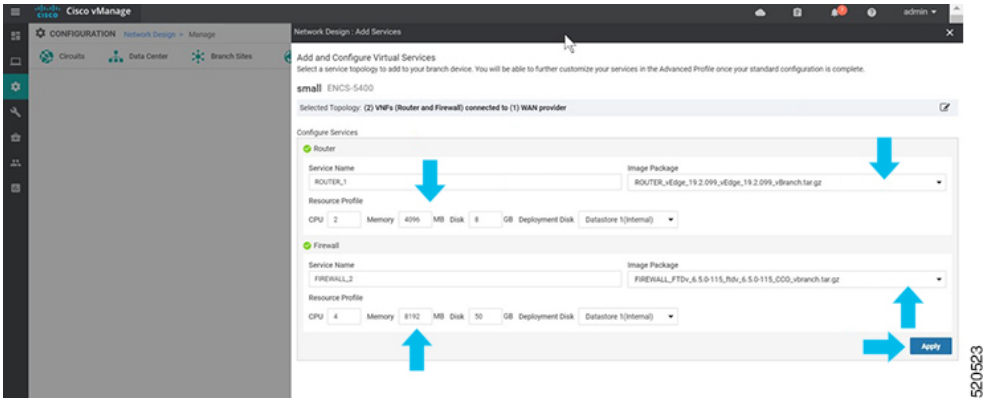


5. 仮想サービスを追加して設定するには、仮想サービスの詳細を入力します。

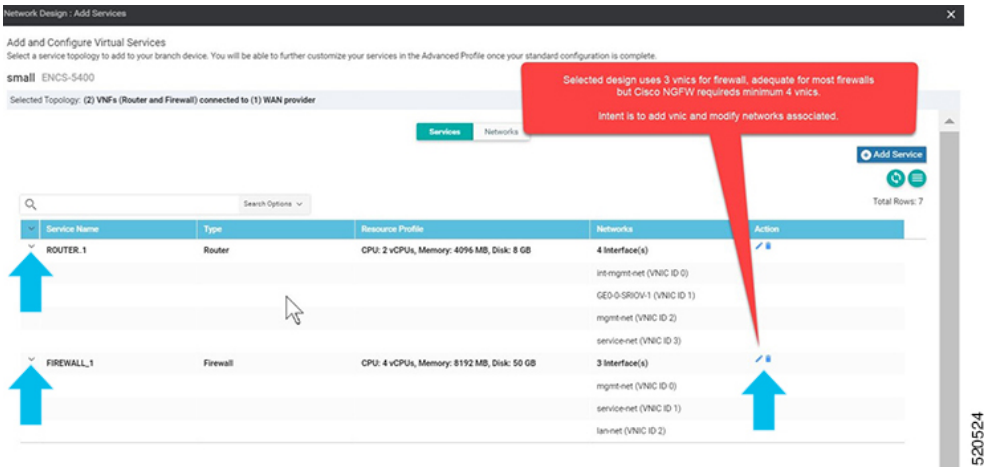
- ドロップダウンリストから [Image Package] を選択し、リソースプロファイルの詳細を入力します。

> **注** リモートサイトにデバイスを展開する場合は、ローカルシステムでイメージを使用できるかどうかを確認し、WAN 経由のイメージダウンロードをスキップします。詳細については、以下を参照してください。 WAN 帯域幅が低いサイトでの ENCS5400 の展開 （79 ページ）

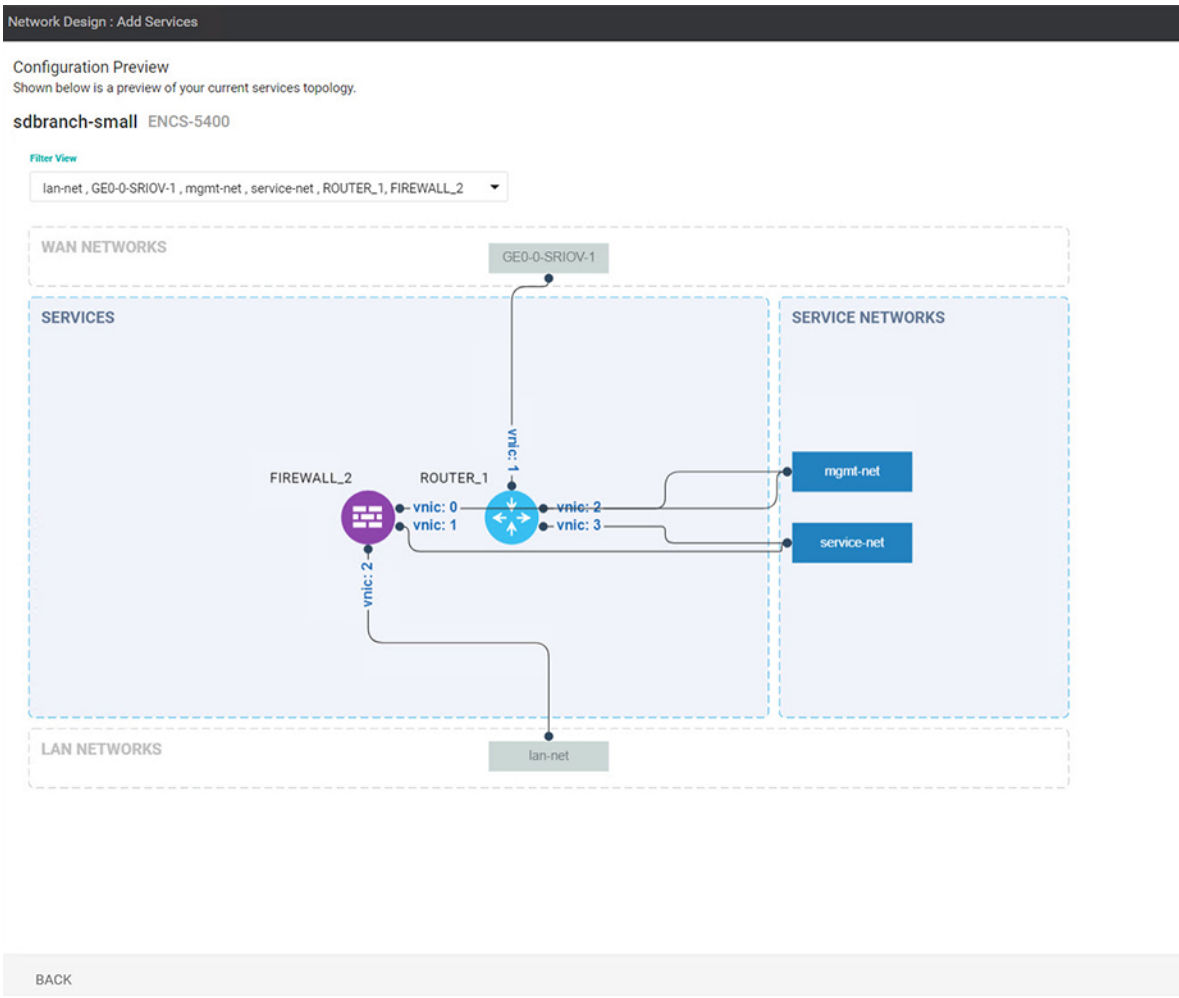
- [Apply] をクリックします。



6. 前の手順で追加したサービスのリストがこのページに表示されます。各デバイスに関連付けられたネットワークを追加または変更できます。



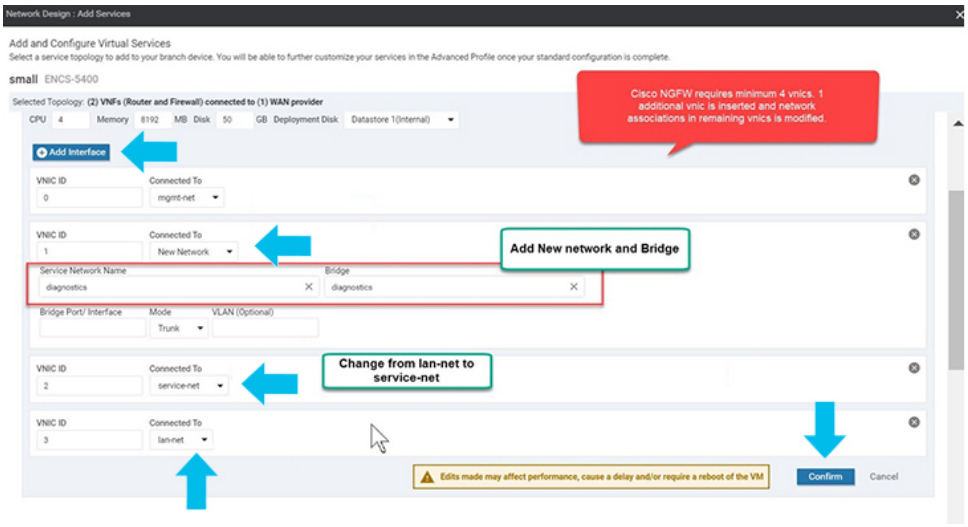
NFVIS 4.4 以降では、[Preview Topology] をクリックして、追加されたサービスのトポロジを関連ネットワークとともに表示できます。ドロップダウンメニューを使用して [Filter View] を選択し、必要なサービスだけを表示できます。



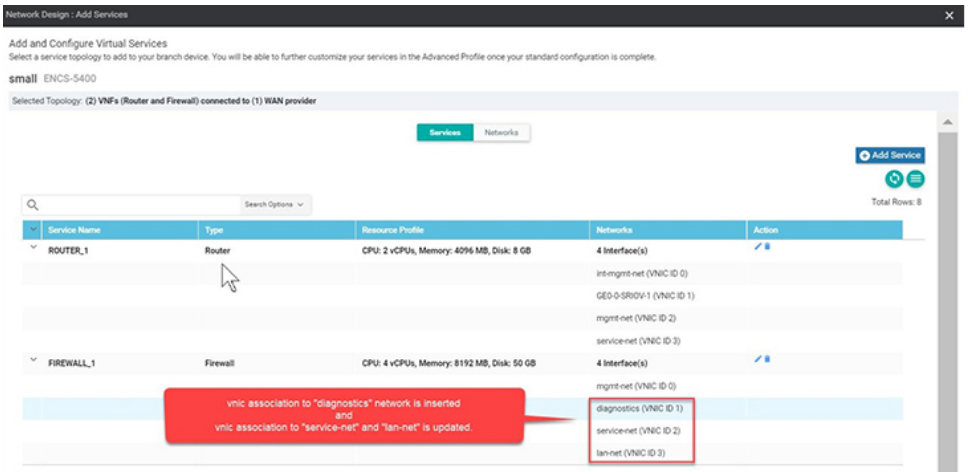
7. [+ Add Interface] をクリックして新しいネットワークを追加します。新しいネットワークに関連付けられたネットワークの詳細を入力します。

   既存のインターフェイスに関連する詳細を変更します。

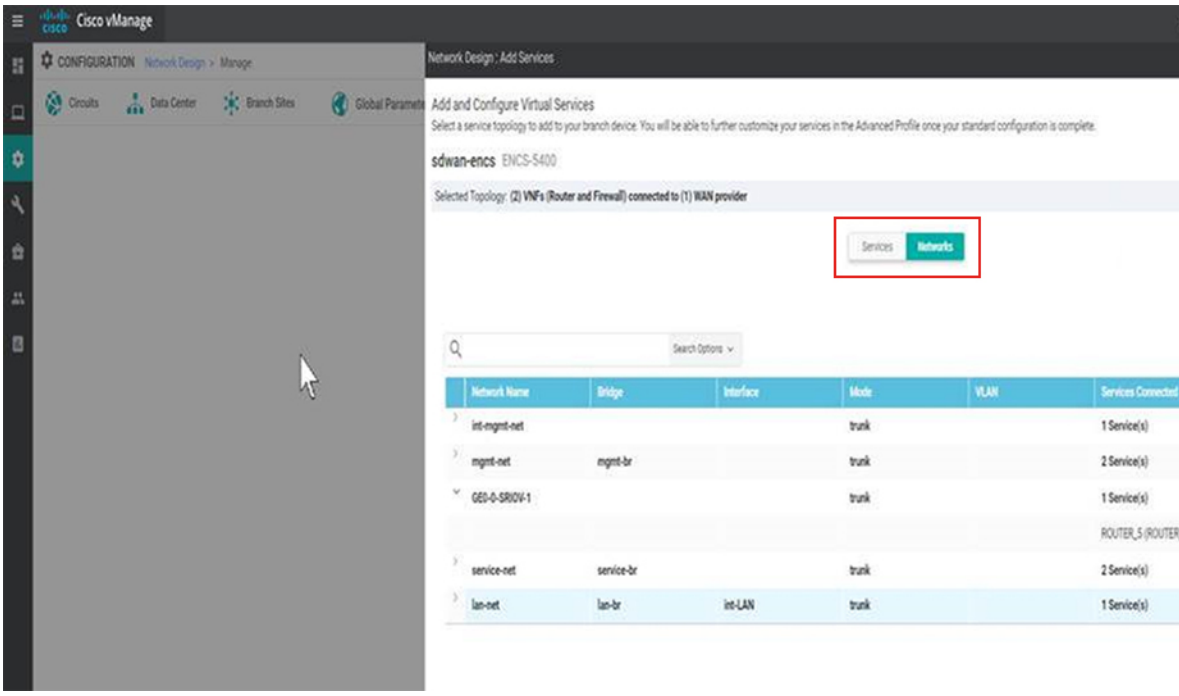
   [Confirm] をクリックします。



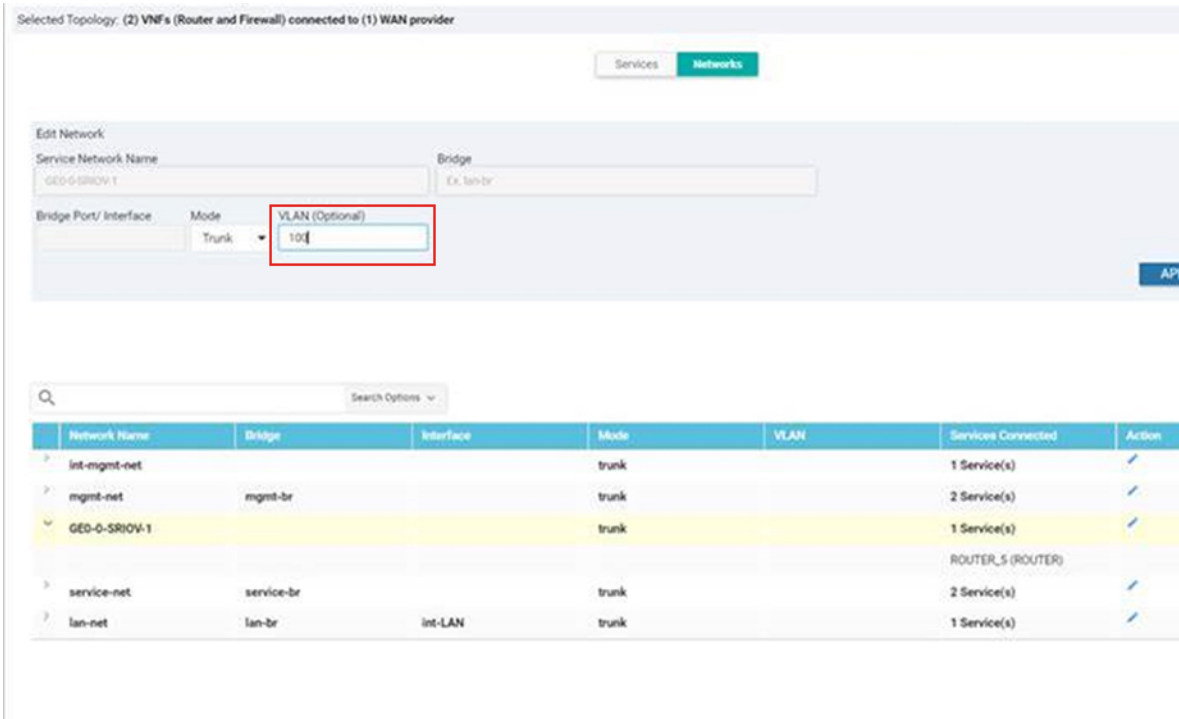
8. [Services]ページで、新しいインターフェイスと変更されたインターフェイスを確認できます。



9. SRIOV ネットワークの VLAN を定義するには、[Networks] を選択します。表示されたネットワークのリストで、ネットワークを追加または変更できます。



10. WAN 側のネットワークでは、デフォルトでトランクモードのすべての VLAN が許可されます。ISRv で Dot1q を設定した場合、VLAN はネットワークを通過します。



(注) NFVIS 4.2.1 を使用するネットワークで VLAN が設定されている場合、VNF 展開の失敗の要因となる既知の競合状態の欠陥があります。この問題を解決するには、Cisco vManage 20.4.1 以降とともに NFVIS 4.4.1 にアップグレードします。

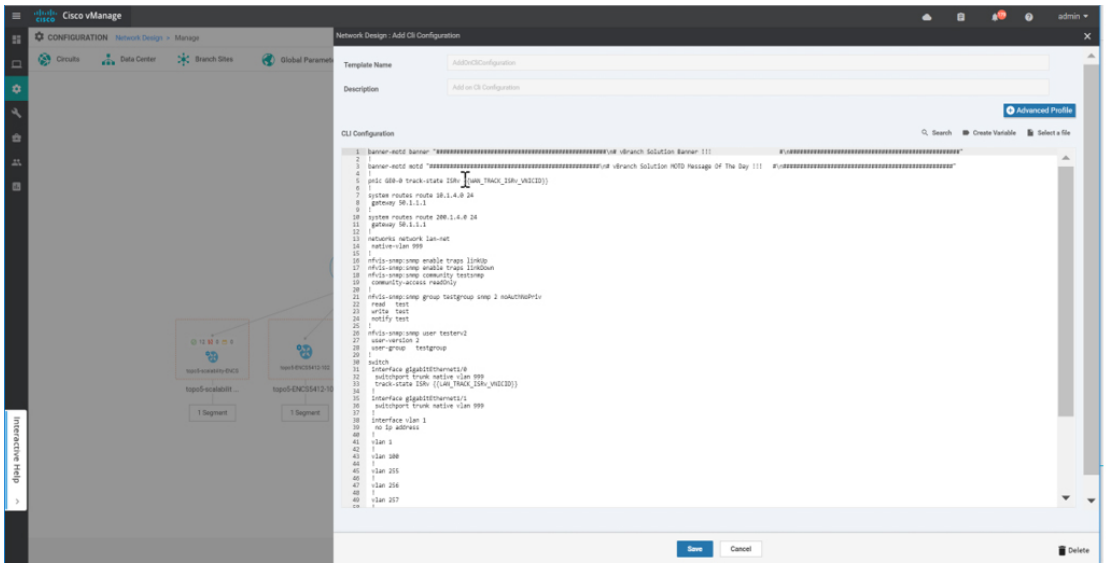
CLI アドオン機能テンプレート

CLI アドオン機能テンプレートを使用して、特定の CLI 設定をデバイスに接続できます。CLI アドオン機能テンプレートは、ネットワーク設計と組み合わせて使用する必要があります。この機能は、ネットワーク設計でネイティブにサポートされていない設定にのみ使用することを推奨します。

CLI アドオン機能テンプレートを作成するには、次の手順を実行します。

1. [Cisco vManage] メニューから、[Configuration]、[Network Design] の順に選択します。
2. [Create Network Design]（ネットワークトポロジをまだ作成していない場合に表示）または [Manage Network Design]（ネットワークトポロジを作成した場合に表示）をクリックします。

   ブランチデバイスのイメージ表示の上にマウスを移動し、[Add CLI Configuration] を選択します。



このセクションでは、NFVIS の次の機能でサポートされるアドオン CLI 設定を示します。詳細については、『Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide』[英語] を参照してください。

起動時間	`vm_lifecycle tenants tenant admin`
	`deployments deployment deployment-ROUTER_1`
	`  vm_group deployment-ROUTER_1`
	`   bootup_time        600`

ポート トラッキング	`pnic GE0-0 track-state ROUTER_1 1`

ACL	`system settings ip-receive-acl 0.0.0.0/0`
	`service  [ scpd ]`
	`action   accept`
	`priority 0`
	`!`
	`system settings ip-receive-acl 10.31.40.24/32`
	`service  [ scpd ]`
	`action   accept`
	`priority 5`
	`!`

スタティック ルート	`system routes route 102.0.0.0 24` `gateway 192.168.0.2`

TACACS+	`aaa authentication tacacs`
	`tacacs-server host 172.19.156.179`
	`key                      7`
	`encrypted-shared-secret cisco123`
	`admin-priv              15`
	`oper-priv               14`
	`!`

バナー	`banner-motd banner "Banner for vBranch"`
本日のメッセージ（MOTD）	`banner-motd motd "MOTD for vBranch"`

SNMP	nfvis-snmp:snmp enable traps linkUp nfvis-snmp:snmp enable traps linkDown nfvis-snmp:snmp community testsnmp community-access readOnly ! nfvis-snmp:snmp group snmpgroupv1 snmp 1 noAuthNoPriv read test write test notify test ! nfvis-snmp:snmp group snmpgroupv2 snmp 2 noAuthNoPriv read test write test notify test ! nfvis-snmp:snmp group snmpgroupv3 snmp 3 authPriv read test write test notify test ! nfvis-snmp:snmp user testerv1 user-version 1 user-group snmpgroupv1 ! nfvis-snmp:snmp user testerv2 user-version 2 user-group snmpgroupv2 ! nfvis-snmp:snmp user testerv3 user-version 3 user-group snmpgroupv3 auth-protocol sha passphrase cisco123 priv-protocol aes passphrase cisco123 ! nfvis-snmp:snmp host SNMP-SERVER-57 host-port 161 host-ip-address 172.19.149.57 host-version 3 host-security-level authPriv host-user-name testerv3 ! nfvis-snmp:snmp host SNMP-SERVER-179 host-port 161 host-ip-address 172.19.156.179 host-version 1 host-security-level noAuthNoPriv host-user-name testerv1 ! nfvis-snmp:snmp host SNMP-SERVER-229 host-port 161 host-ip-address 172.25.221.229 host-version 2 host-security-level noAuthNoPriv host-user-name testerv2 !
デフォルトゲートウェイ	system settings default-gw 172.25.217.1

ENCS スイッチの個々の VLAN CLI の代わりに VLAN 範囲を設定します。VLAN 範囲の値はパラメータ化でき、サイト固有の VLAN 範囲のバリエーションを設定するのに役立ちます。 （注） このコマンドは、NFVIS 4.4 以降のバージョンでのみサポートされます。	`switch vlan-range 1,100,200,300-305`

ENCS スイッチの設定：グローバル VLAN、アクセス VLAN、トランク VLAN、ネイティブVLAN、スパニングツリープロトコル、ポートチャネル、トラックステート、速度、デュプレックス、および QoS	

	switch interface gigabitEthernet1/0 track-state ISRv 3 ! interface gigabitEthernet1/1 speed 100 duplex full ! interface gigabitEthernet1/2 channel-group 1 mode auto ! interface gigabitEthernet1/3 channel-group 1 mode auto ! interface gigabitEthernet1/4 speed 100 switchport mode access switchport access vlan 100 ! interface gigabitEthernet1/5 spanning-tree disable ! interface gigabitEthernet1/6 speed 1000 duplex full switchport mode trunk switchport trunk native vlan 101 no switchport trunk allowed switchport trunk allowed vlan vlan-range 8,113-114,130 ! interface gigabitEthernet1/7 qos cos 3 switchport mode trunk switchport trunk native vlan 999 no switchport trunk allowed switchport trunk allowed vlan vlan-range 255-257,999 ! interface port-channel1 spanning-tree mst 1 cost 200000000 spanning-tree mst 2 cost 200000000 switchport mode trunk no switchport trunk allowed switchport trunk allowed vlan vlan-range 100,126-128 ! vlan 1 ! vlan 8 ! vlan 100 ! vlan 101 ! vlan 113 ! vlan 114 ! vlan 126 ! vlan 127

	! vlan 128 ! vlan 130 ! vlan 255 ! vlan 256 ! vlan 257 ! vlan 996 ! vlan 997 ! vlan 998 ! vlan 999 ! qos port ports-trusted qos trust cos-dscp spanning-tree mode mst spanning-tree mst 2 priority 61440 spanning-tree mst configuration name mst_LAN instance 1 vlan 996-998 instance 2 vlan 100,126-128 ! !
NFVIS とルータ VM 間の単一 IP アドレスの共有	single-ip-mode vm-name deployment-name-of-ROUTER

NFVIS とルータ VM 間の単一 IP アドレスの共有

表 *5*：機能の履歴

機能名	リリース情報	説明
NFVIS およびルータ VM の単一 IP アドレスのサポート	NFVIS 4.5 Cisco vManage リリース 20.5.1 以降	このリリースでは、NFVIS とルータ VM の間で単一のパブリック IP アドレスを使用するためのサポートが SD-Branch ソリューションに拡張されています。

単一 IP アドレス共有の概要

通常、仮想ブランチ展開では、各ブランチサイトに 2 つのパブリック IP アドレスが必要です。1 つは NFVIS 用で、もう 1 つはルータ VM 用です。単一の IP アドレスの共有がサポートされているため、ブランチサイトに割り当てられた単一のパブリック IP アドレスを、NFVIS と NFVIS に導入されたルータ VM の間で共有できます。この機能は、必要なパブリック IP アドレスの数を 1 つに制限し、ルータが障害状態であってもブランチサイトに到達できるようにします。

この機能を設定するには、Cisco vManage の CLI アドオン機能テンプレートを使用します。

単一 IP アドレス共有の仕組み

- ブランチサイトの NFVIS にはパブリック IP アドレスが割り当てられています。必要な単一 IP アドレス設定は、Cisco vManage のアドオン CLI 機能テンプレートを使用して設定されます。
- Cisco vManage はこの設定を NFVIS にプッシュします。NFVIS は、展開されているルータ VM に WAN IP アドレスを解放します。
- 展開された VM は NFVIS のゲートウェイとして機能します。
- NFVIS は、展開された VM を介して NFVIS インターネットゲートウェイに定期的に ping を実行し、NFVIS と Cisco vManage の接続を確認します。NFVIS がインターネットゲートウェイに接続できない場合、次の処理が行われます。
  1. NFVIS に展開されたルータ VM をシャットダウンします。
  2. VM に割り当てられた IP アドレスを再要求します。
  3. Cisco vManage との制御接続の再確立を試みます。

サポート対象の VM

NFVIS とルータ VM 間の単一 IP アドレスの共有は、次のルータ VM でのみサポートされます。

- Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V）
- シスコサービス統合型仮想ルータ（ISRv）
- Cisco vEdge クラウドルータ

単一 IP アドレス共有の設定

ステップ 1：ルータ VM を設定する

次の例は、ルータ VM に含める必要がある SDWAN NAT DIA 設定を示しています。この例では、GigabitEthernet1 は NFVIS の int-mgmt-net を介して接続された MGMT インターフェイスです。GigabitEthernet2 は、NFVIS の GE0-0 を介して接続された VPN 0 WAN インターフェイスです。

```
vrf definition 500
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!

interface Gigabitethernet1
 vrf forwarding 500

interface Gigabitethernet2
 ip nat outside
```

```
ip nat route vrf 500 0.0.0.0 0.0.0.0 global
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
!
```

（注） VRF 500 は 1 つの例であり、0 および 512 以外の任意の許可された SDWAN VPN 番号（0 ー 65527 の範囲）に変更できます。

（注） エンドツーエンドの設定例については、「付録」 を参照してください。

ステップ 2：**単一 IP アドレス共有の設定**

NFVIS とルータ VM の間で単一の IP アドレス共有を有効にするために、CLI アドオン機能テンプレートに含める必要がある設定例を次に示します。この例では、deployment-ROUTER_1.deployment-ROUTER_1 はルータ VM の展開名です。

```
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
```

（注） エンドツーエンドの設定例については、「付録」 の章を参照してください。

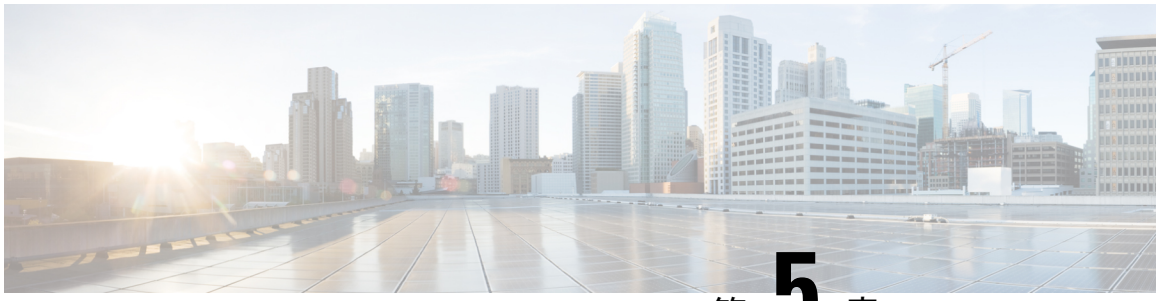
単一 IP アドレス共有の確認

次に、単一 IP モードのステータスを確認するために使用する**show single-ip-mode** コマンドの出力例を示します。

```
Device# show single-ip-mode
single-ip-mode state active
single-ip-mode state-details "VM alive"
```

次に、Cisco NFVIS と Cisco vManage の制御接続を確認するために使用する**show control connections**コマンドの出力例を示します。

```
Device# show control connections
                                PEER                                                 PEER
                  CONTROLLER
PEER    PEER PEER             SITE       DOMAIN PEER
PRIV  PEER                                    PUB
                  GROUP
TYPE    PROT SYSTEM IP        ID         ID     PRIVATE IP        PORT  PUBLIC IP
PORT  LOCAL COLOR     PROXY STATE UPTIME      ID
------------------------------------------------------------------------------------------
vmanage dtls 10.10.10.29     101        0      172.19.156.234    12846 172.19.156.234
12846       bronze    No    up     0:01:41:22  0
```



第 5 章

Cisco NFVIS SD-Branch ソリューションの導入

導入のセクションでは、NFVIS WAN エッジデバイスを導入する上での前提条件について説明し、その後さまざまなオンボーディングオプションやオンボーディング検証について説明します。

NFVIS WAN エッジオンボーディングの前提条件

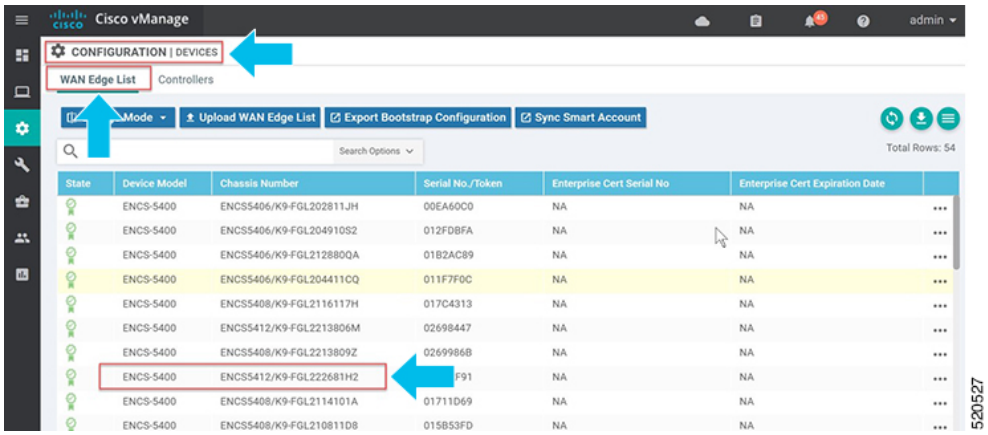
WAN Edge のオンボーディングプロセスを開始する前に、次の前提条件が満たされていることを確認してください。

- NFVIS WAN エッジデバイスは、Cisco vBond オーケストレータおよび Cisco vManage に到達可能です。
- 承認された WAN エッジデバイスのホワイトリストは、WAN エッジデバイスを追加し、PnP ポータルで vBond コントローラプロファイルに関連付けることによって、すべての SD-WAN コントローラにアップロードされます。ホワイトリスト プロビジョニング ファイルは、PnP ポータルからダウンロードして Cisco vManage にアップロードしたり、[Sync Smart] オプションを使用して Cisco vManage に同期したりできます。Cisco vManage は、後でこのホワイトリストを追加のコントローラに配布します。

注　仮想環境に展開されたソフトウェア WAN エッジデバイスには、シャーシまたはシリアル番号がありません。このようなデバイスの場合、ソフトウェアデバイスが PnP ポータルに追加されると、PnP サーバーは一意のシリアル番号を生成します。

- WAN エッジデバイスは、証明書の状態が [Valid] または [Staging] である必要があります。

  Cisco vManage で、[Configuration]、[Devices]、[WAN Edge List] の順に移動し、WAN Edge デバイスを特定します。[Validity] 列で、デバイスが [Valid] または [Staging] 状態になっていることを確認します。



> **注** [Staging] 状態の WAN エッジデバイスは、SD-WAN コントローラとの制御接続のみを確立します。データプレーン接続は、WANエッジデバイス間では確立されません。デバイスを完全にオンボードするには、デバイスの状態を [Staging] から [Valid] に移行する必要があります。Cisco vManageで、[Configuration]、[Certificates]、[WAN Edge List] の順に選択して、WAN Edge デバイスを選択し、[Validity] 列で状態を [Valid]に変更して、[Send to Controllers] をクリックします。

- WAN エッジデバイスは NFVIS ソフトウェアを実行している必要があります。

PnP プロセスを使用した NFVIS WAN エッジデバイスの導入準備の前提条件

PnP プロセスを使用した NFVIS WAN エッジデバイスのオンボーディングについて、次の前提条件が満たされていることを確認してください。

- 工場出荷時の ENCS NFVIS デバイスは、FQDNのdevicehelper.cisco.com を解決し、Cisco クラウドホスト型のプラグアンドプレイ接続サーバーに到達して、vBond コントローラ情報、組織名、およびエンタープライズルート CA 証明書を取得できる必要があります（エンタープライズルート CA 証明書）。

- ブートストラップオプションを使用してオンボーディングする前に、WAN エッジを工場出荷時のデフォルト設定にする必要があります。

（注） ENCS NFVIS デバイスは、必要に応じてデバイスで CLI コマンドを使用して工場出荷時のデフォルトに設定できます**factory-default-reset all**。

- http://software.cisco.com の Cisco PnP Connect サーバーには、ENCS NFVIS WAN Edge が追加され、vBond コントローラプロファイルに関連付けられたデバイスが必要です。

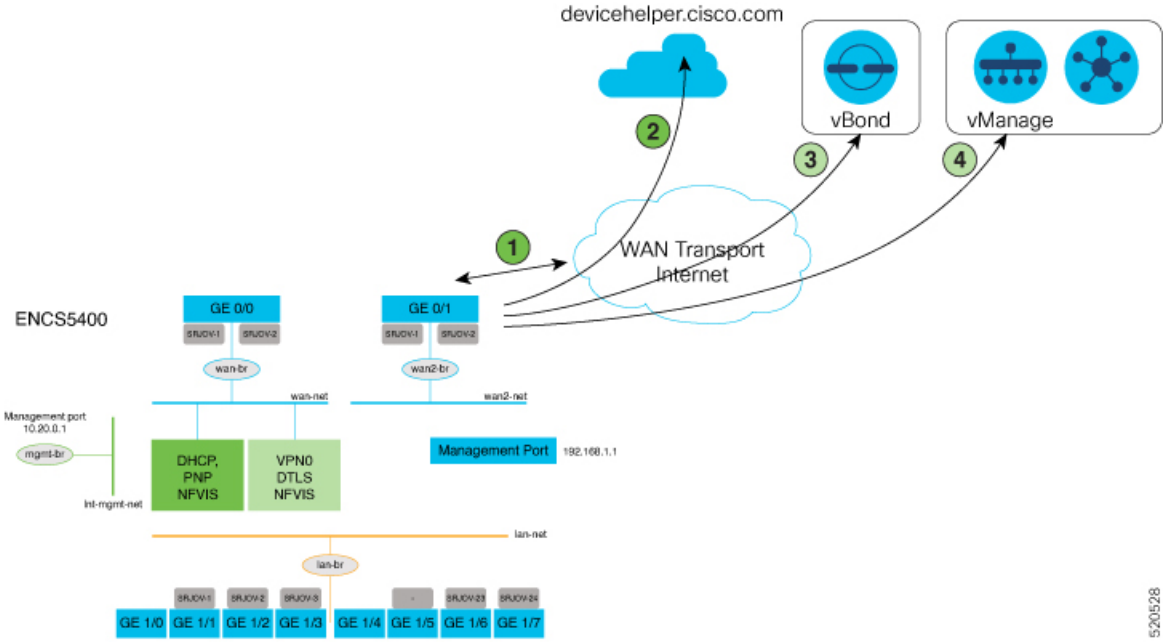
  [Cisco Software Central] > [Network Plug and Play] > [Plug and Play Connect] > [Devices] に移動し、関連付けられた [Controller] プロファイルでデバイスが使用可能であることを確認します。

プラグアンドプレイプロセスを使用した NFVIS デバイスのオンボーディング

NFVIS WAN エッジは、最初に PnP プロセスによって SD-WAN オーバーレイネットワークにオンボードされます。

（注） 出荷時のデフォルトの NFVIS WAN エッジデバイスには、PnP でサポートされるインターフェイスが事前に設定されています。デバイスは IP アドレスを動的に取得し、SD-WAN コントローラに自身を登録します。

1. PnP 対応インターフェイスをインターネット WAN トランスポートに接続します。



上の図に含まれる手順を以下で詳しく説明します。

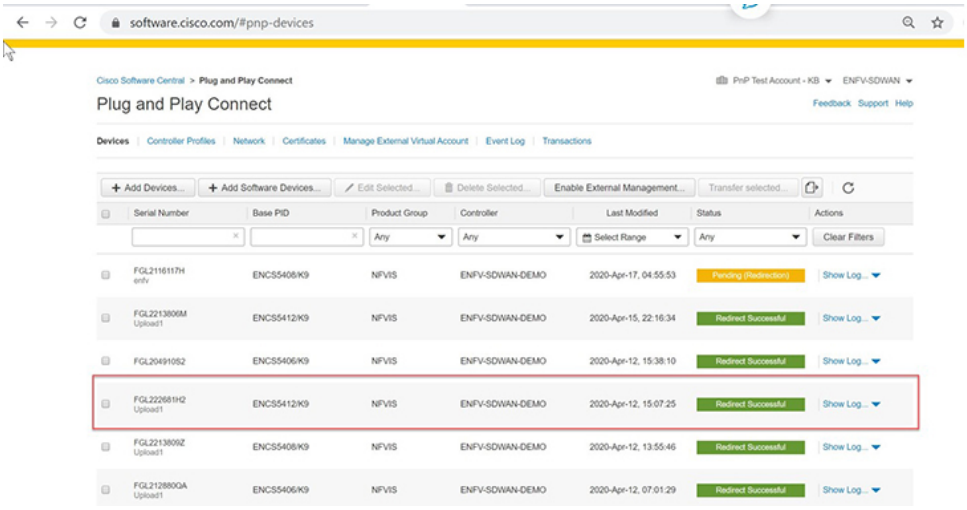
1. ENCS デバイスの電源を入れ、WAN インターフェイスを GE0-0 に接続します。
2. ENCS は devicehelper.cisco.com に接続します。ENCS は、PnP Connect サーバーからルート証明書を取得します。
3. ENCS は vBond にリダイレクトされます。PnP Connect サーバーは、ENCS デバイスの状態を [Pending] から [Redirected] に変更します。
4. ENCS は、このステップで Cisco vManage に自動的に登録されます。

2. GE0/0 ポートを WAN に接続し、ENCS デバイスの電源をオンにします。
   - ブートアップ後、デバイスはアップストリーム WAN 転送デバイスから 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 情報を動的に取得します。
   - WAN エッジデバイスは、devicehelper.cisco.com を ZTP サーバーに接続するための DNS 要求を行います。
   - WAN エッジデバイスは、シスコクラウドでホストされている PnP Connect サーバーに到達し、サーバーで認証するためにシャーシとシリアル番号を提示します。
   - 認証後、PnP Connect ポータルは vBond オーケストレータ、組織名、およびルート証明書に関する情報を提供します。

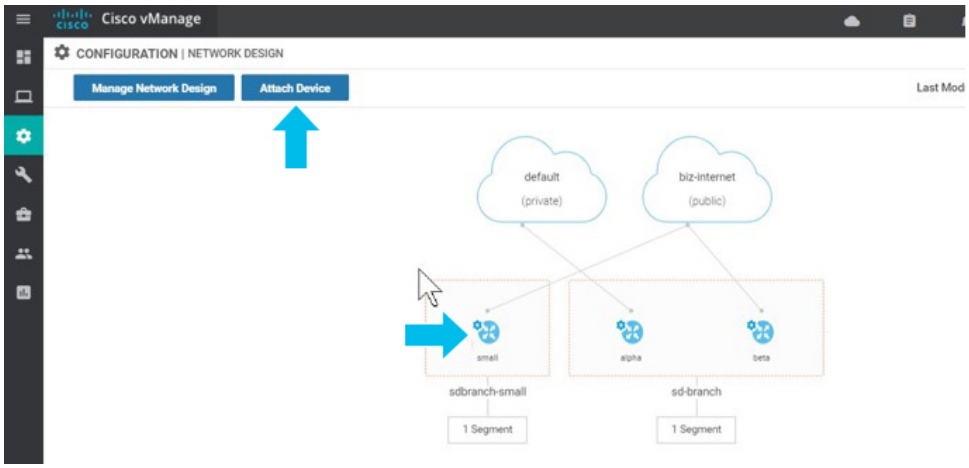
(注) エンタープライズルート CA 証明書を使用する展開の場合、デバイスは、HTTPS プロトコルを使用して、エンタープライズルート CA 証明書を vBond IP アドレスまたは DNS および組織名とともにダウンロードします。この情報は、vEdge コントローラとの制御接続を開始するために WAN エッジデバイスによって使用されます。

- この段階で PnP ポータルは、WAN エッジデバイスが PnP 経由で vBond コントローラにリダイレクトされた場合に、[Redirect Successful] ステータスを示します。

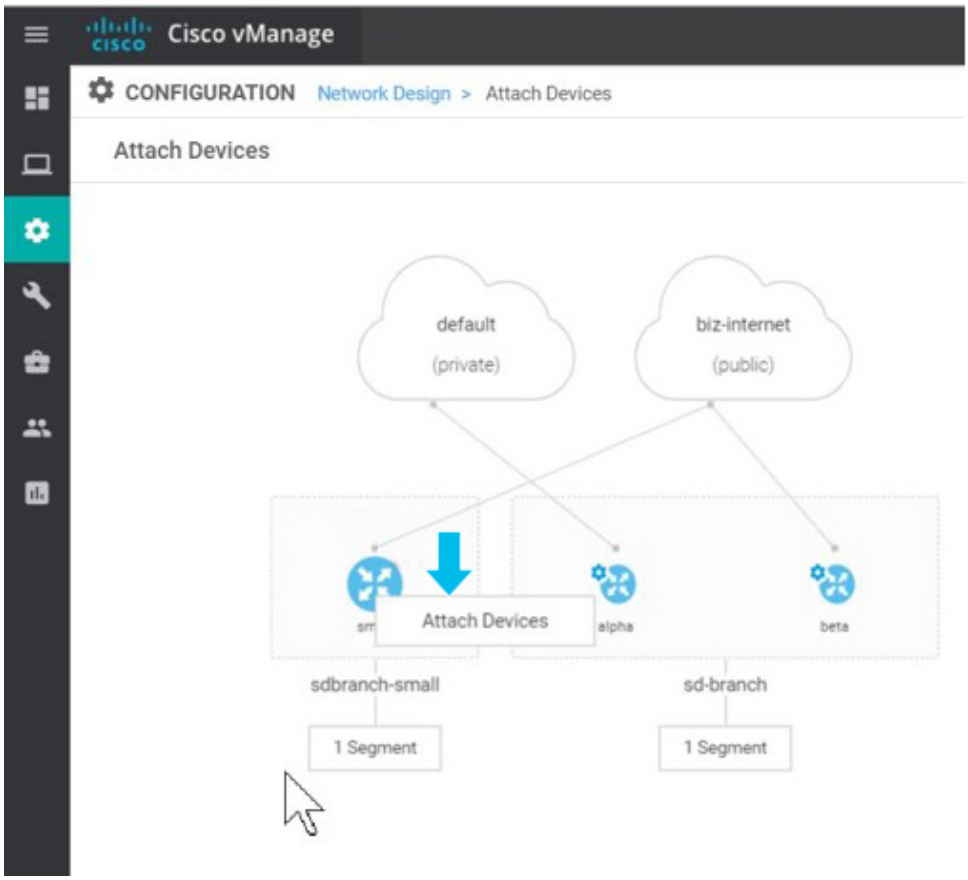
  次に、正常にリダイレクトされる ENCS 5412 の例を示します。



3. vBond オーケストレータによる認証後、Cisco vManage 情報は、NFVIS WAN エッジデバイスで登録され、セキュアな接続を確立します。
   - デバイスは、Cisco vManage とのセキュアな制御接続を確立しようとします。デバイスには設定がなく、システムの IP アドレスとして 0.0.0.0 を使用して Cisco vManage との初期制御接続を確立します。
   - デバイスプロファイルを WAN エッジデバイスに接続すると、Cisco vManage を介してデバイスを制御および設定できるようになります。デバイスを接続するには、次の手順を実行します。
     - [Cisco vManage] メニューから、**[Configuration]** > **[Network Design]** を選択します。
     - [Attach Devices] をクリックし、ネットワークトポロジ上のデバイスを選択します。

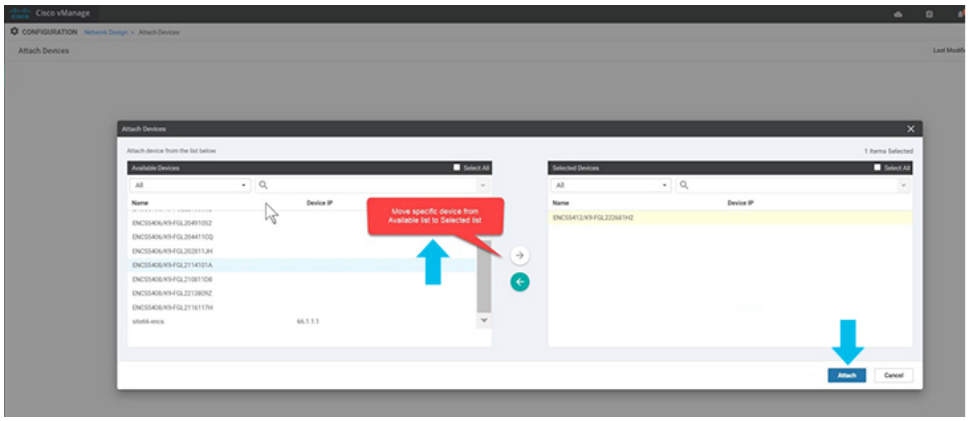


- [Attach Devices] をクリックします。



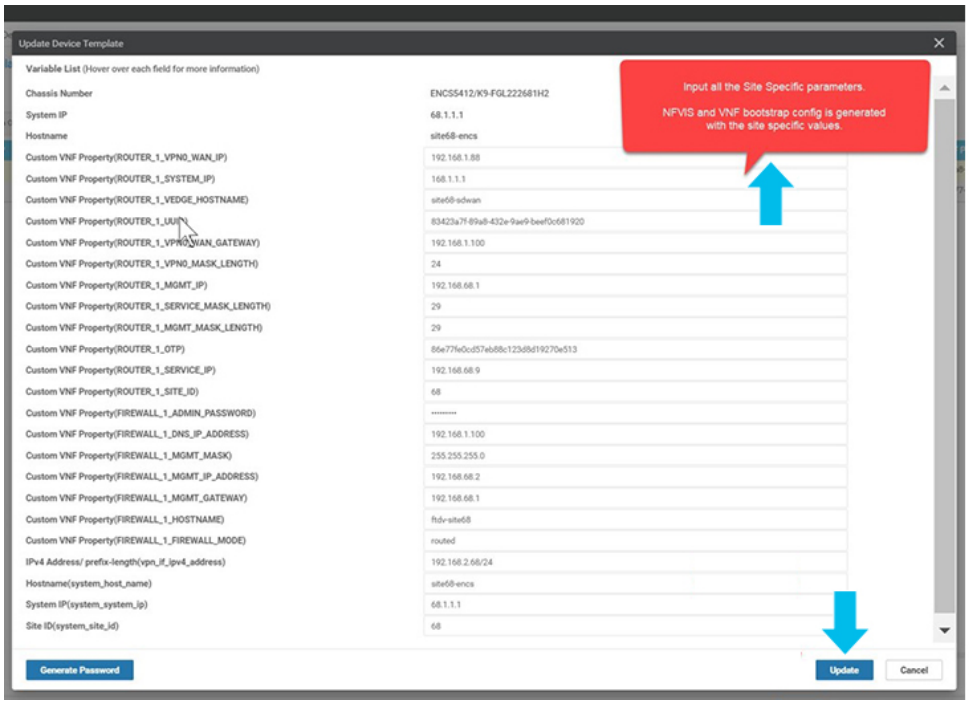
- 使用可能なデバイスのリストがポップアップウィンドウに表示されます。使用可能なリストから特定のデバイスを選択し、矢印を使って選択したリストに移動します。

  [Attach] をクリックします。



- 選択したデバイスは、[Edit Device Template] を使用して変更できます。

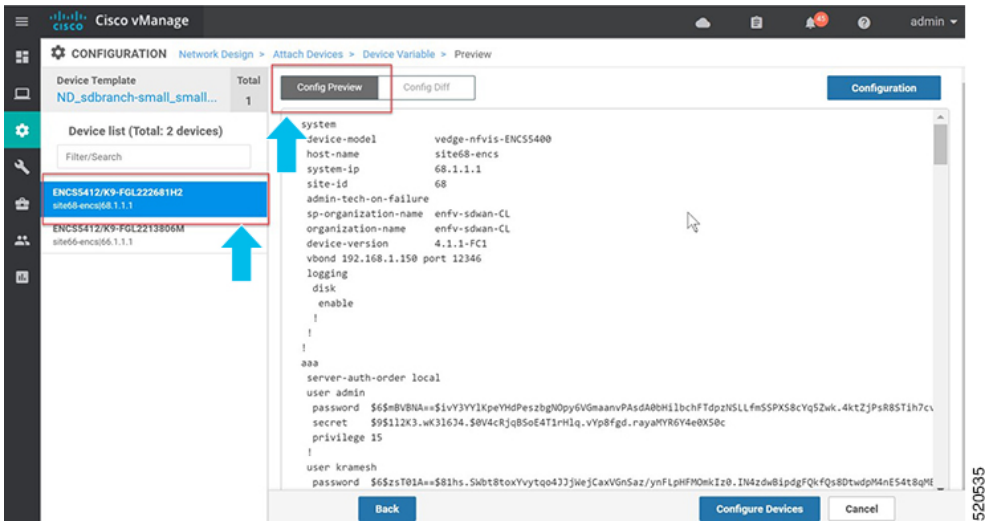
- すべてのサイト固有のパラメータを更新し、[Update] をクリックします。



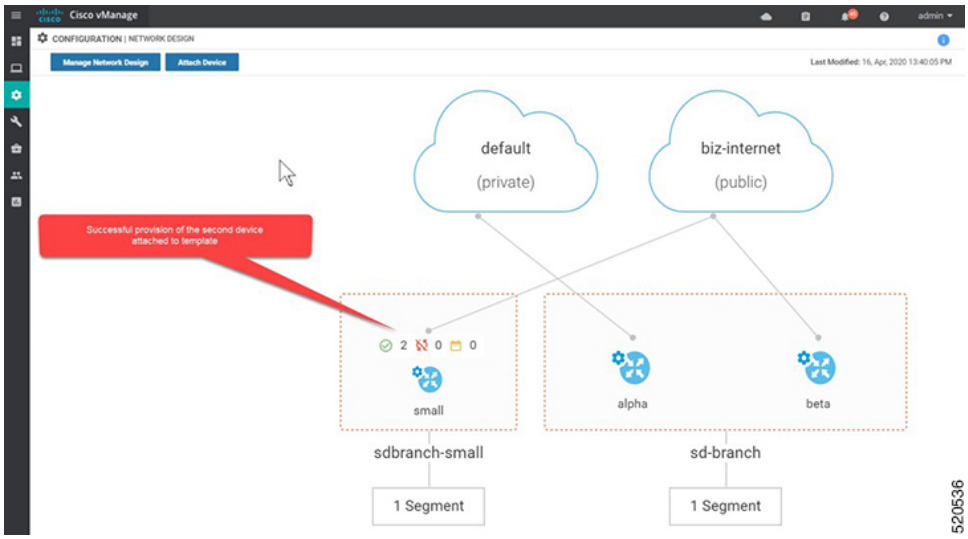
- デバイスの名前をクリックし、[config preview] を選択します。選択したデバイスに関連付けられている設定をプレビューできます。

  新しい CLI アドオン機能テンプレートを含むデバイステンプレートをここにアタッチすると、設定がマージされ、ここに表示されます。

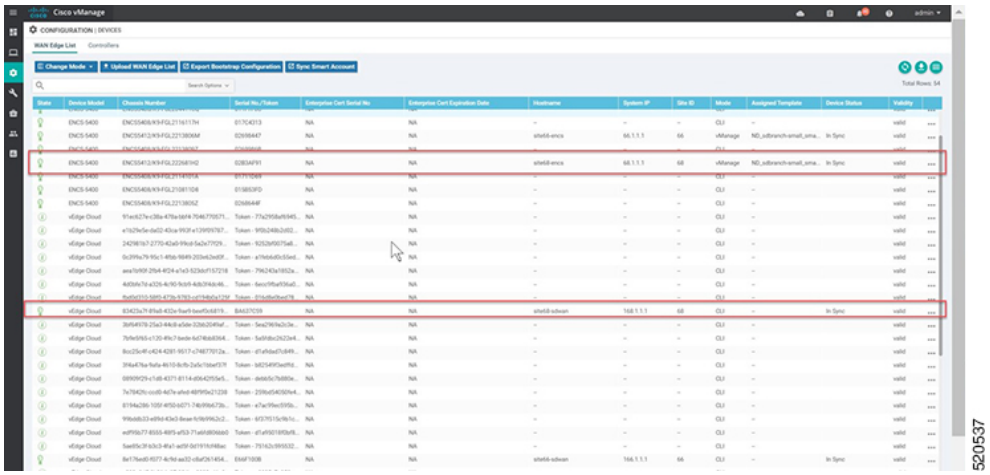
[Configure Devices] をクリックして、設定をデバイスにプッシュします。



- デバイスを設定すると、2 番目のデバイスがトポロジに正常にプロビジョニングされたことが [Network Design] 画面に表示されます。コンフィギュレーションの更新が選択したデバイスにプッシュされます。

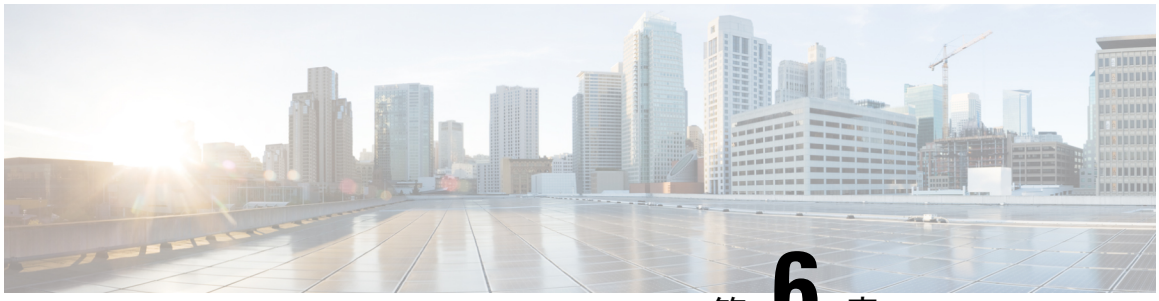


- [WAN Edge List] で接続デバイスの**有効性**を確認できます。



- 認証および**接続デバイス**のプロビジョニングフローの後、Cisco vManage はデバイスのシステム IP アドレスで NFVIS に応答し、共有システム IP アドレスを使用してデバイスで強制的に再認証します。

- 次に、WAN エッジデバイスは、設定されたシステム IP アドレスを使用してすべての SD-WAN コントローラ（Cisco vBond、Cisco vManage コントローラ）への制御接続を再開し、SD-WAN オーバーレイネットワークに参加します。



第 6 章

Cisco NFVIS SD-Branch ソリューションの操作

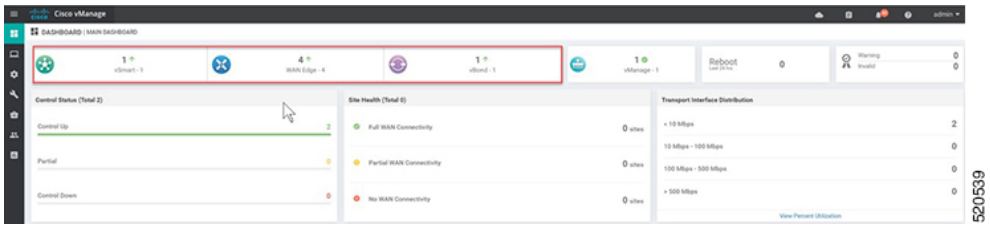
Cisco vManage を使用して、WAN エッジデバイスをモニタ、トラブルシューティング、および管理できます。ここでは、一般的なトラブルシューティングとモニタリングの手順について説明します。

Cisco vManage を使用した SD-WAN コンポーネントのステータスの監視と管理

Cisco vManage ダッシュボード画面を使用して、SD-WAN オーバーレイネットワークの全体的な状態をモニタします。

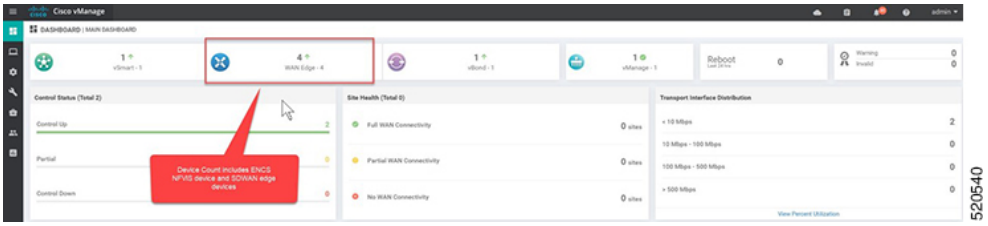
デバイスペインによる SD-WAN コンポーネントの監視

1. Cisco vManage メインダッシュボードで、ダッシュボード画面の上部にある [Device Pane] を表示します。このペインには、Cisco vManage からオーバーレイネットワークの vSmart コントローラ、vEdge ルータ、および vBond オーケストレータへのすべての制御接続が表示されます。ペインには、ネットワーク内の Cisco vManage のステータスも表示されます。すべての SD-WAN コンポーネントの接続が確立されていることを確認します。

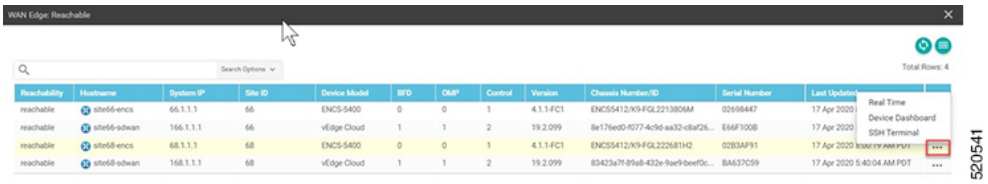


デバイスペインによる WAN エッジデバイスの詳細と統計情報の表示

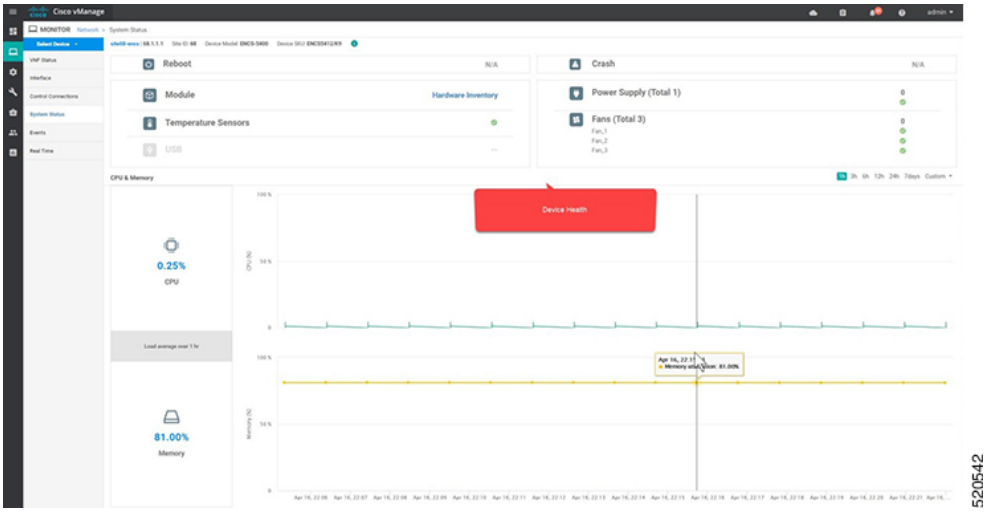
1. Cisco vManage メインダッシュボードで、デバイス統計情報を表示するには、番号または WAN エッジの上にある上下の矢印（4）をクリックして、各接続の詳細情報を含むテーブルを表示します。



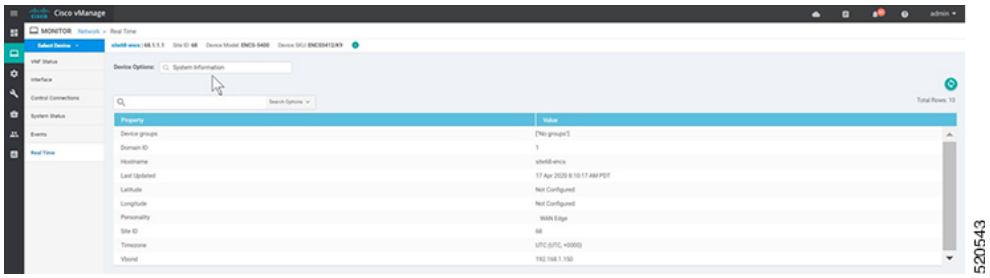
2. テーブルには、[System IP]、[Site ID]、[Device Model]、[Software Version] などが表示されます。デバイス固有の詳細については、各行の末尾にある [...] をクリックしてください。ここから、[Device Dashboard]、[Real Time data]、または [SSH Terminal] にアクセスできます。



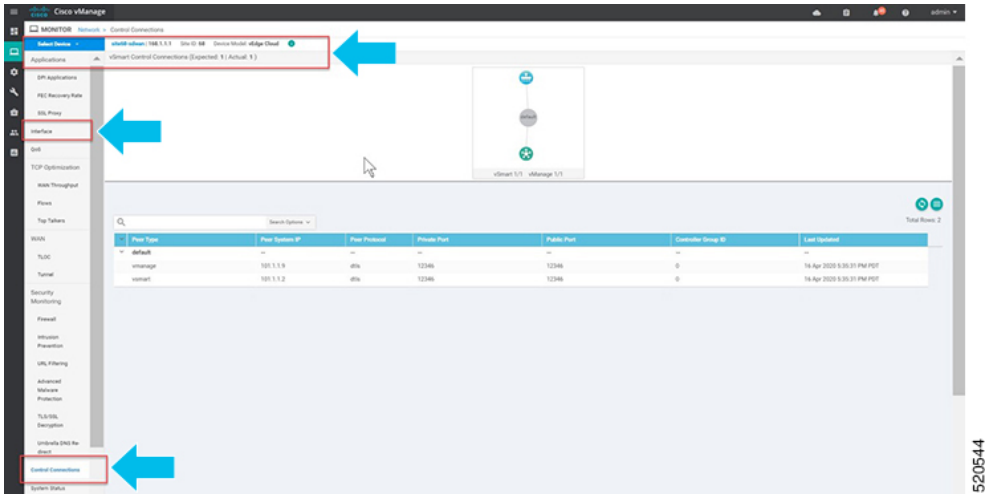
[Device Dashboard] には、デバイスの [System Status]、デバイスの [Module Hardware Inventory] 情報、[CPU & Memory] のリアルタイム統計情報が表示されます。



[Real Time] には、[Site ID]、[Vbond]、[Hostname]、[Latitude]、[Longitude] など、デバイスの基本的なシステム情報が表示されます。

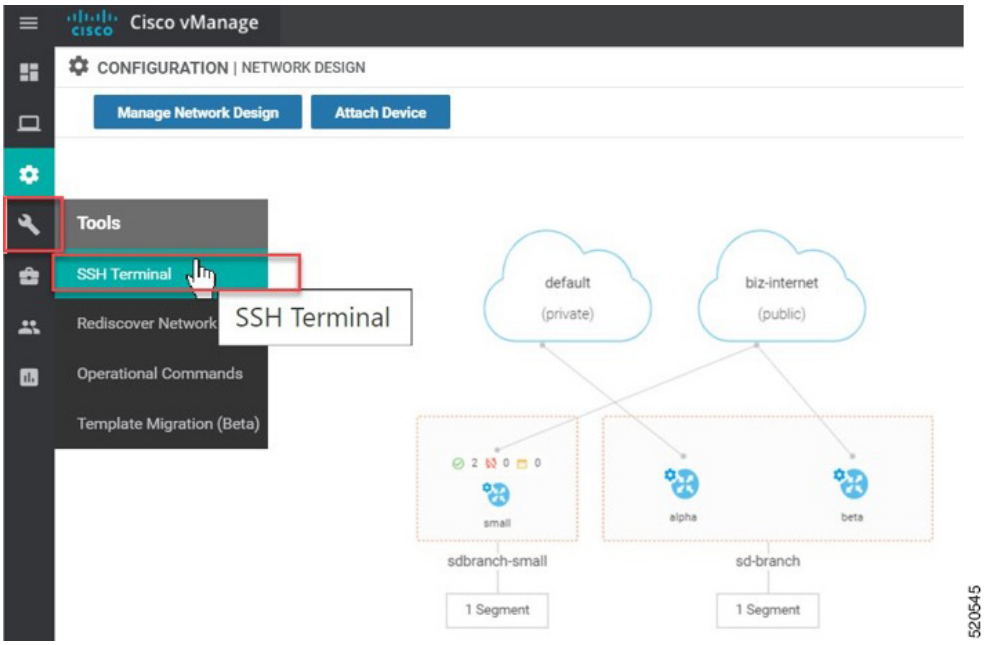


3. WAN エッジデバイスのインターフェイスを介した [Control Connections] などの追加情報は、Cisco vManage から表示できます。[Cisco vManage] メニューから**[Monitor]** > **[Network]** を選択し、リストからデバイスを選択して、左側のパネルからデバイス情報を探します。



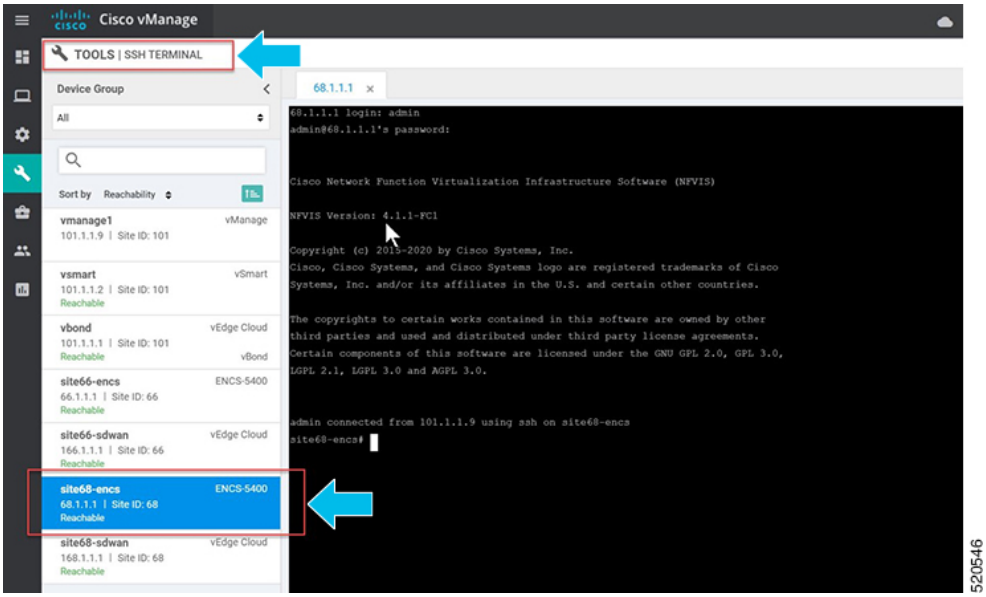
CLI コマンドを使用した Cisco vManage SSH サーバーダッシュボードによる WAN エッジデバイスの監視

1. [Cisco vManage] メニューから、**[Tools]** > **[SSH Terminal]**を選択します。



2. [Device Group] から WAN エッジを選択します。

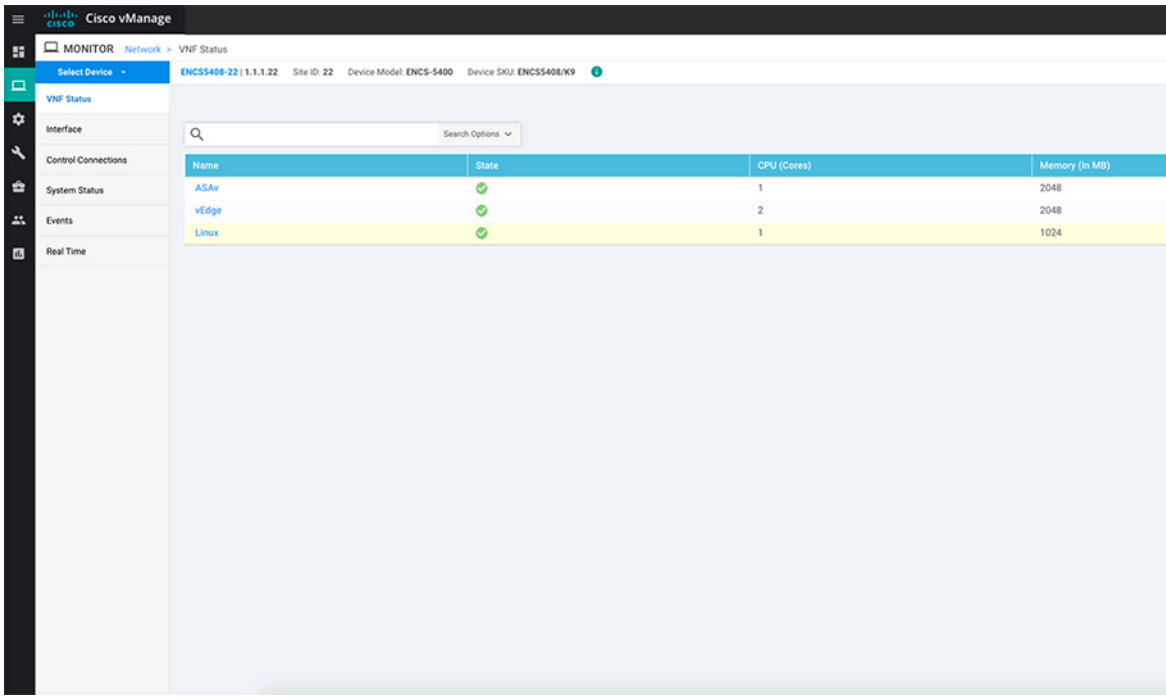
   WAN エッジデバイスが SD-WAN コントローラとのセキュアな制御接続を確立したかどうかを確認するには、**show control connections** コマンドを入力します。



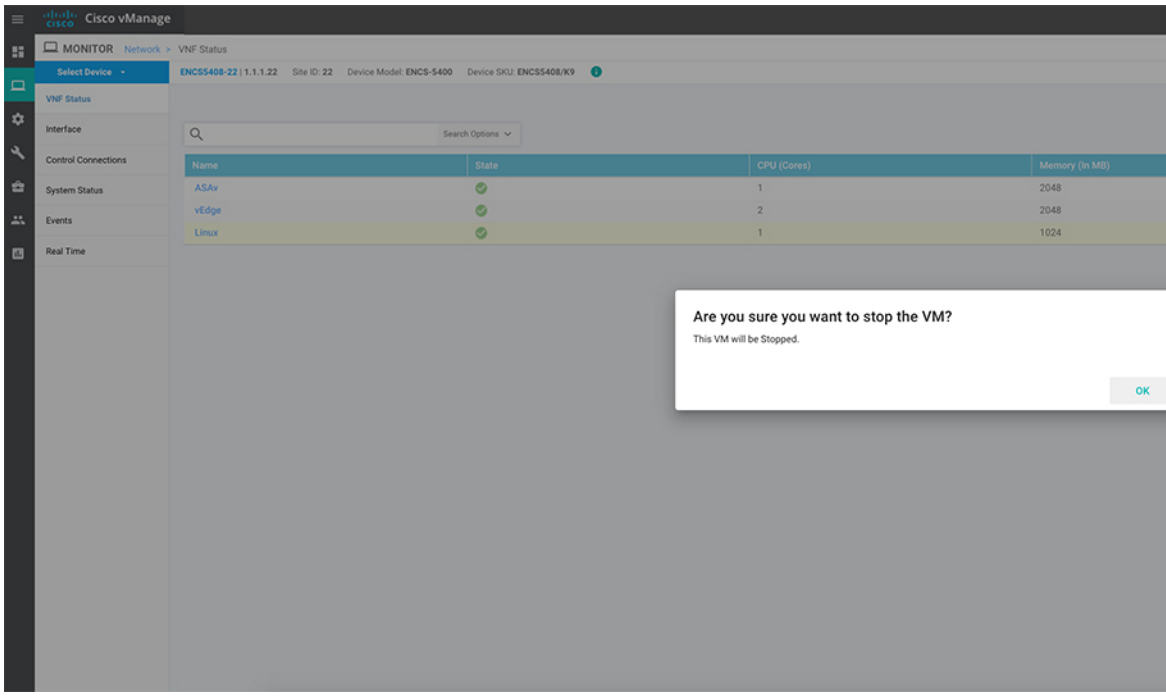
WAN エッジデバイスの開始、停止、および再起動

1. [Cisco vManage] メニューから、[Monitor]、[Network] の順に選択します。
2. WAN エッジデバイスを選択します。

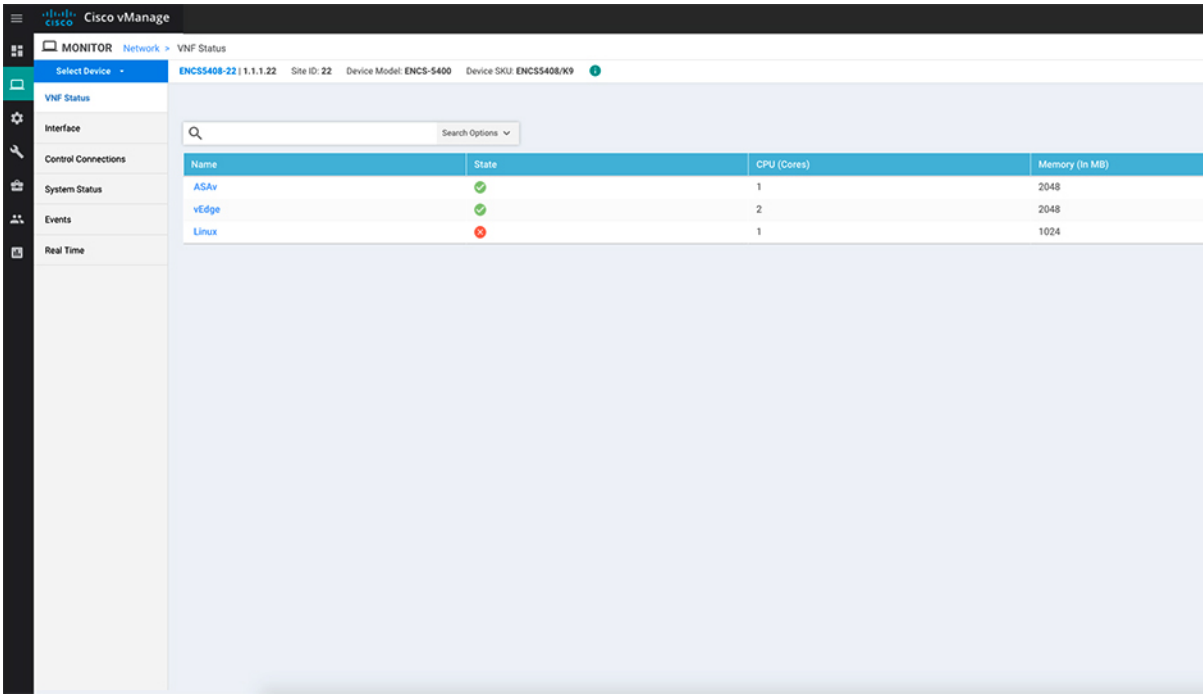
3. デバイスに展開された VM のリストが画面に表示されます。VM の横にある [...] をクリックして、デバイスを起動、停止、または再起動します。



次の例は、VM の停止方法と VM のステータスの変化を示しています。



注 VM のステータスを表示するには、Cisco vManage メニューから**[Tools]** > **[Discover Network]**を選択します。[Device] を選択し、[Rediscover] をクリックして最新のステータスを同期します。



vmAction vmName Linux actionType STOP/START/REBOOTコマンドを使用して VM を起動、停止、または再起動することもできます。VM のステータスを表示するには、**show system:system deployments**または**show vm_lifecycle deployments all**コマンドを使用します。

```
Device# vmAction vmName Linux actionType STOP

Device# show system:system deployments
NAME   ID  STATE
--------------------
ASAv   1   running
vEdge  2   running
Linux  -   shut
```

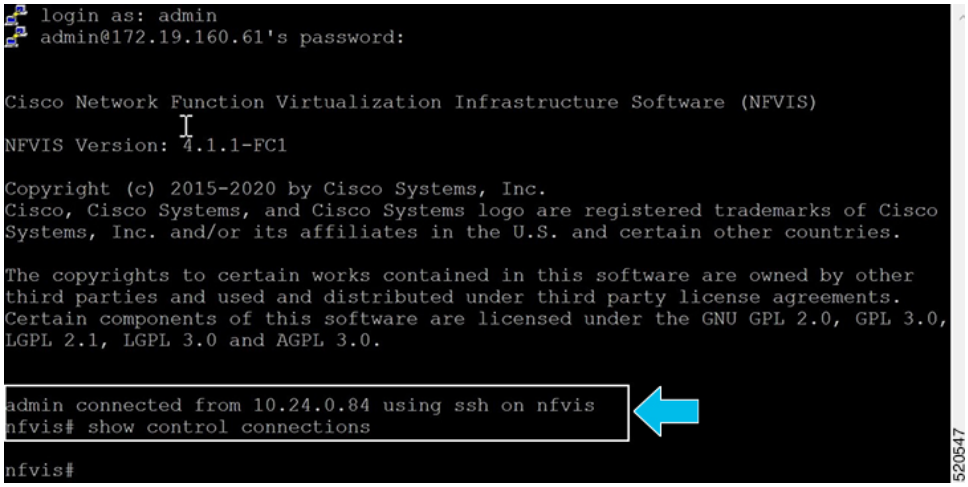
デバイスオンボーディングのトラブルシューティング

ここでは、一般的なトラブルシューティング手順について説明します。

オンボーディングの問題の診断

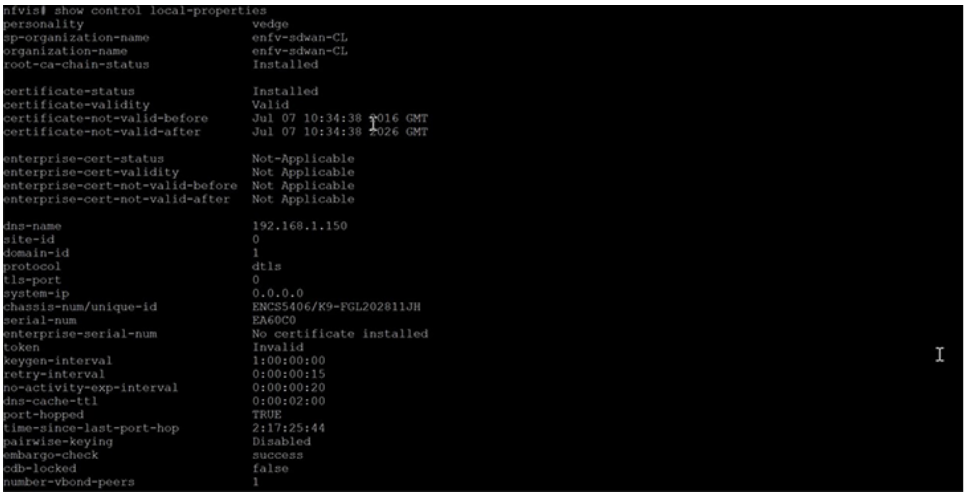
ここでは、WAN エッジデバイスのオンボーディングプロセス中に発生する可能性のある最も一般的な問題と、問題を解決するための推奨される解決方法について説明します。

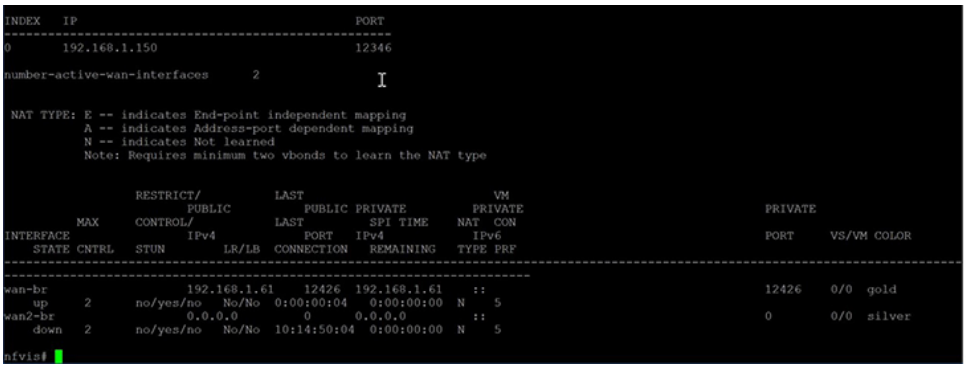
1. WAN エッジデバイスが SD-WAN コントローラとのセキュアな制御接続を確立したことを確認するには、**show control connections**コマンドを入力します。



2. WANエッジデバイスの認証に使用されるデバイスプロパティを確認するには、**show control local-properties**コマンドを入力します。

出力で、次のことを確認します。

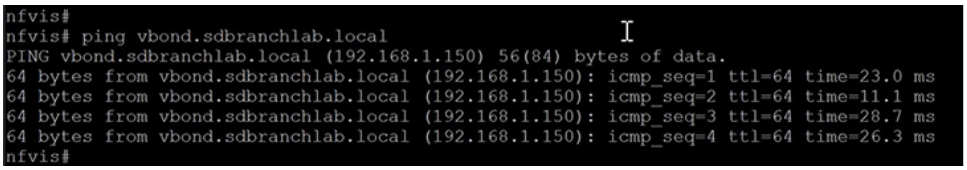




- システムパラメータは、organization-name と site-id を含むように設定されている
- certificate-status および root-ca-chain-status がインストールされている
- certificate-validity が有効になっている
- dns-name が vBond IP アドレス/DNS を指している
- system-ip が設定されており、chassis-num/unique-id および serial-num/token がデバイスで使用可能

上記のパラメータは、接続を確立する前に SD-WAN コントローラと相互認証するために WAN エッジデバイスで使用できる必要があります。

3. WAN エッジデバイスから vBond コントローラの到達可能性を確認するには、次の手順を実行します。



4. WAN エッジデバイスが SD-WAN コントローラとの接続を確立できない場合は、**show control connections-history** コマンドを入力して失敗の理由を表示します。[LOCAL ERROR] および [REMOTE ERROR] 列を表示して、エラーの詳細を収集します。

以下に、WAN Edge デバイスが SD-WAN コントローラとの制御接続を確立できない理由の一部を示します。

CRTVERFL：エラー状態は、WAN デバイスと SD-WAN コントローラ間のルート CA 証明書の不一致が原因で、WAN エッジデバイスの認証が失敗したことを示します。vEdge デバイスでは show certificate root-ca-cert を使用し、IOS-XE SD-WAN デバイスでは show sdwan certificate root-ca-cert を使用して、同じ証明書が WAN Edge デバイスと SD-WAN コントローラにインストールされていることを確認します。

CTorgNMMIS：エラー状態は、SD-WAN コントローラで設定された組織名と比較して、組織名が一致しないために WAN エッジデバイスの認証が失敗したことを示します。vEdge デバイスで show sdwan control local-properties を使用し、IOS-XE SD-WAN デバイスで show sdwan control local-properties を使用して、すべての SD-WAN コンポーネントが SD-WAN 環境全体で同じ組織名で設定されていることを確認します。

NOZTPEN：エラー状態は、オンボーディング vEdge デバイスが ZTP サーバー上の承認済みホワイトリストデバイスの一部ではないことを示します。オンプレミス ZTP サーバーで show ztp entry を使用して、デバイスのホワイトリストを確認します。

NOVMCFG：エラーステータスは、WAN エッジデバイスが Cisco vManage のデバイステンプレートにアタッチされていないことを示します。このステータスは、自動展開オプション（PnP または ZTP プロセス）を使用してデバイスをオンボーディングするときに表示されます。

VB_TMO、VM_TMO、VP_TMO、VS_TMO：このエラーは、WAN エッジデバイスが SD-WAN コントローラに到達できないことを示します。

5. WAN エッジデバイスの制御接続を確認するには、次の show コマンドを使用します。

   - **show control connections**
   - **show control connections-history**
   - **show control connections-info**
   - **show control local-properties**
   - **show control statistics**
   - **show control summary**

- **show control valid-vmanage-id**

ルート CA 証明書が WAN エッジデバイスで不明になっている

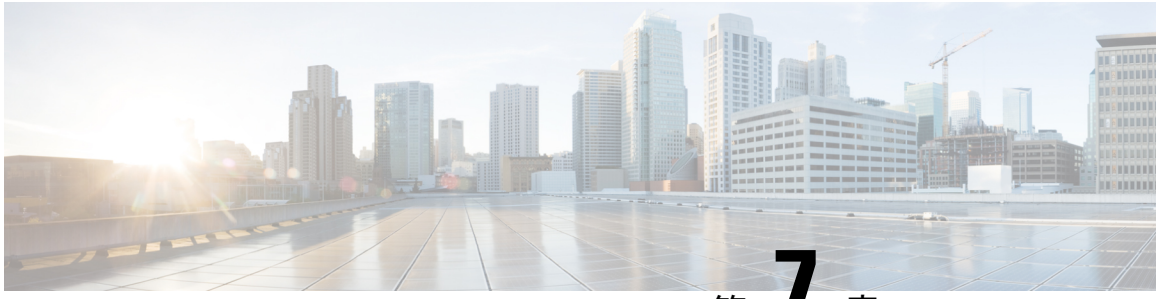
オンボーディングプラットフォームのルートCAチェーン証明書がない場合、デバイス認証は失敗します。デバイス認証の失敗では、SD-WAN コントローラへの制御接続を確立できません。次の手順は、デバイスコンポーネントにルートCA証明書をインストールする方法を示しています。

デバイスにログインし、**show control local-properties**コマンドから root-ca-chain ステータスを表示します。次の例は、root-ca-chain-status が **Not-Installed** 状態であることを示す出力例です。

```
show control local-properties
personality                     vedge
sp-organization-name            ENB-Solutions -21615
organization-name               ENB-Solutions -21615
root-ca-chain-status            Not-Installed
```

次に、NFVIS にルート証明書をアップロードする方法の例を示します。

```
nfvis# request root-cert-chain install scp://admin@10.28.13.168
Uploading root-ca-cert-chain via VPN 0
Enter directory of root CA certificate file : /ws/admin-sjc/
Enter root CA certificate file name (default: root-ca.crt) : TPMRootChain.pem
Copying ... admin@10.28.13.168:/ws/admin-sjc//TPMRootChain.pem via VPN 0
Warning: Permanently added '10.28.13.168' (ECDSA) to the list of known hosts.

WARNING!!!
READ THIS BEFORE ATTEMPTING TO LOGON

This System is for the use of authorized users only. Individuals
using this computer without authority, or in excess of their
authority, are subject to having all of their activities on this
system monitored and recorded by system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement
officials.

Cisco Acceptable Use Policy:
http://wwwin.cisco.com/c/cec/organizations/security-trust/infosec/policies.html

admin@10.28.13.168's password:
TPMRootChain.pem 100% 7651 1.8MB/s 00:00
Updating the root certificate chain..
Successfully installed the root certificate chain
nfvis#
```



第 7 章

デバイスに接続されたプロファイルの N 日目の変更のサポート

表 *6*:

機能名	リリース情報	説明
デバイスに接続されたプロファイルの N 日目の変更のサポート	NFVIS 4.6.1 Cisco vManage リリース 20.6.1	この機能を使用すると、デバイスに接続された後でも、ネットワーク設計プロファイルを変更できます。

N 日目のネットワーク設計の変更に関する制限事項

- デュアル WAN からシングル WAN への更新はサポートされていません。
- デュアル WAN を機能させるには、NFVIS 制御接続を両方の WAN（wan-br および wan2-br）を介して確立する必要があります。
- SRIOV および OVS インターフェイスはスワップできません。これは、インターフェイスの MAC アドレスが変更されるためです。
- 物理ポートはデフォルトのマッピングから削除できません。
- 1 つの物理ポートのみを 1 つの OVS-bridge に割り当てることができます。
- MACアドレスを変更するネットワークマッピングスワップは許可されません。たとえば、VNIC タイプを virtio から SRIOV に変更すると、MAC アドレスが変更されるため、許可されません。
- フレーバーでは、CPU とメモリの値のみを更新できます。フレーバーは、Cisco vManage を使用して更新することをお勧めします。

- 最初に DPDK の有効化コマンドのみを N 日目の設定変更に適用し、それが成功して VM が稼働している場合は、フレーバー設定の更新を適用することをお勧めします。これは、DPDK を有効にするには VM を再起動する必要がありますが、VM の起動時に VM フレーバーを更新できないためです。したがって、設定変更を有効にする DPDK を残りの設定変更から分離することを推奨します。

N 日目のネットワーク設計の変更に関する情報

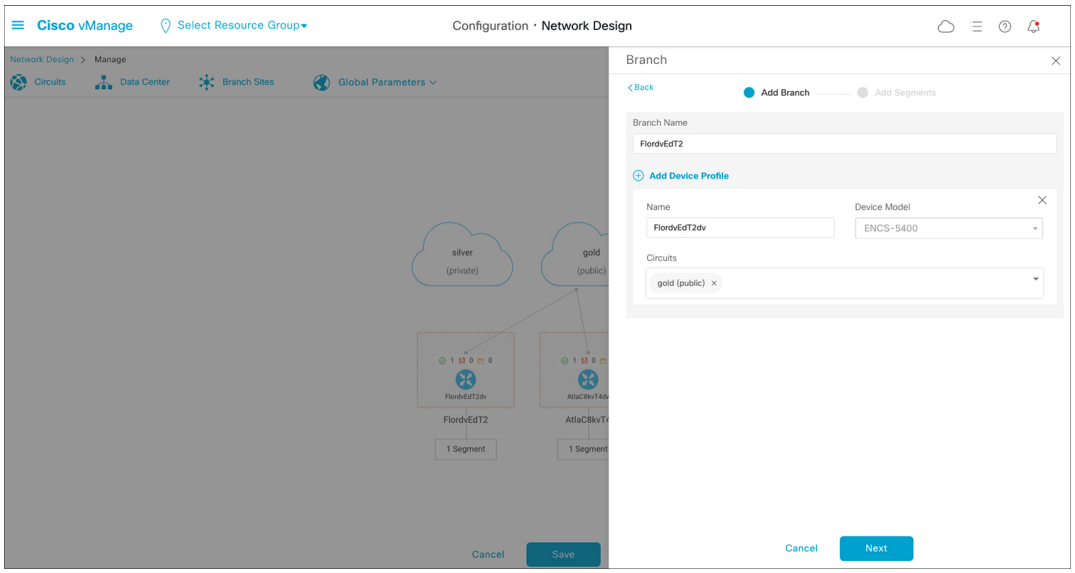
この機能を使用すると、1 つ以上のデバイスに接続された後でも、ネットワーク設計プロファイルを変更できます。グローバルパラメータの変更、サービスとネットワークの設定の編集、および WAN と LAN の設定の変更を行うことができます。CLI 設定を変更することもできます。

ネットワークプロファイルの N 日目の変更の設定

デバイス名とブランチ名の変更

ネットワークに接続されているデバイスの名前を変更するには、次の手順を実行します。

1. [Cisco vManage] メニューから、**[Configuration]** > **[Network Design]** を選択します。
2. [Manage Network Design] をクリックします。
3. [Branch Sites] をクリックします。
4. 編集するデバイスを検索し、編集記号をクリックします。
5. ブランチ名を変更する場合は、[Branch Name] フィールドに名前を入力します。



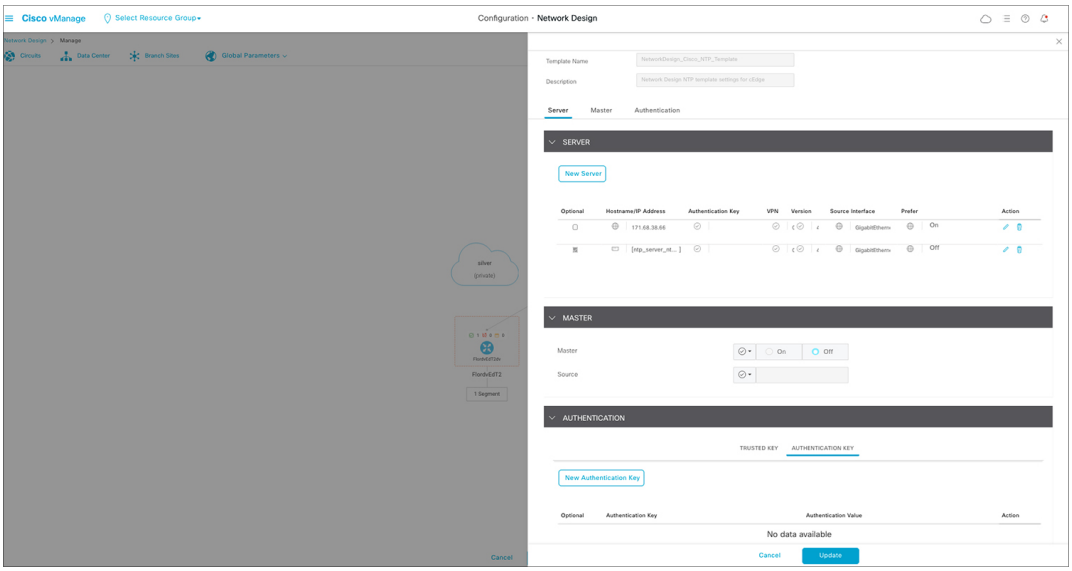
6. [Next] をクリックします。
7. セグメント名が選択されていない場合は、[Segment Name] ドロップダウンリストをクリックし、セグメント名を選択します。
8. [Add] をクリックし、[Finish] をクリックします。
9. [Save] をクリックします。表示されるダイアログボックスで [Proceed] をクリックします。

グローバルパラメータの変更

グローバルパラメータの変更は、ネットワーク内のすべてのデバイスにグローバルに影響します。NFVIS 4.6 リリース以降、ネットワークに接続されているデバイスでもグローバルパラメータを変更できます。

N 日目にグローバルパラメータを変更するには、次の手順を実行します。

1. [Cisco vManage] メニューから、**[Configuration]** > **[Network Design]** を選択します。
2. [Manage Network Design] をクリックします。
3. [Global Parameters] をクリックします。
4. [Selected Device] ドロップダウンリストから、変更するスタックを選択します。これらのパラメータ（Cisco NTP、Cisco AAA、Cisco Logging）に対して N 日目の変更を行うことができます。
5. 新しいサーバーをプロファイルに追加するには、[New Server] をクリックし、新しい認証キーを追加するには、[New Authentication Key] をクリックします。既存のサーバーおよび認証キーパラメータを変更できます。
6. **Master** および **Source** のパラメータを修正することもできます。



7. [Update] をクリックします。

（注） NFVIS デバイスの変更を設定するには、cEdge パラメータを使用します。

デバイスプロファイルの変更

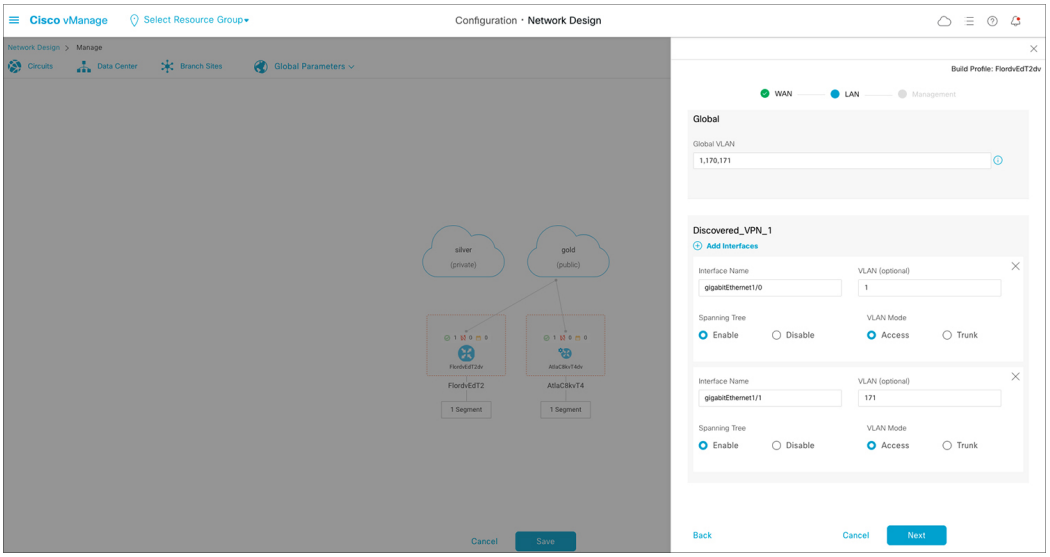
デバイスプロファイルを N 日目に変更するには、次の手順を実行します。

1. [Cisco vManage] メニューから、**[Configuration]** > **[Network Design]** を選択します。
2. [Manage Network Design] をクリックします。
3. N 日目の変更を行うデバイスをクリックします。
4. [Edit Profile] を選択します。
5. パラメータを変更するには、編集記号をクリックします。
6. WAN で、インターフェイス IP を [DHCP] または [Static] に設定します。

注 インターフェイス IP を静的として選択する場合は、CLI アドオン機能テンプレートを使用して IP デフォルトゲートウェイを設定する必要があります。

7. [Next] をクリックします。
8. [LAN] で、[Global VLAN] の値を入力します。
9. 新しいインターフェイスを追加するには、[Add Interface] をクリックします。

10. 新しいインターフェイスのスパニングツリープロトコル、VLAN（VLAN ID）、およびVLAN モードの設定を変更するには、それぞれスパニングツリー、VLAN（オプション）、およびVLANモードのフィールドを使用します。既存のインターフェイスに対してこれらの変更を行うこともできます。



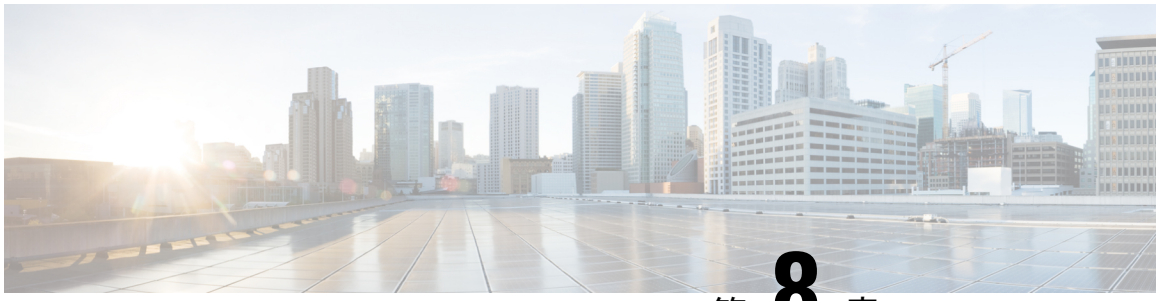
11. [Next] をクリックします。

12. [Management] で、WAN プロファイルでの選択に基づいて、インターフェイス IP を [DHCP] または [Static] に設定できます。WAN プロファイルでインターフェイス IP を [DHCP] に設定する場合は、管理プロファイルで [Static] を選択する必要があります。逆も同様です。

注 インターフェイス名は、どのプロファイルでも変更しないでください。デフォルトのインターフェイス名は次のとおりです。

- WAN プロファイル：GE0-0 または GE0-1
- LAN プロファイルの場合：gigabitEthernet1/0 ～ gigabitEthernet1/7
- 管理プロファイルの場合：mgmt

13. [Done] をクリックします。



第 8 章

付録

WAN 帯域幅が低いサイトでの ENCS5400 の展開

VNF イメージは、プロビジョニング時に Cisco vManage から ENCS 5400 デバイスにダウンロードされます。低帯域幅の WAN アップリンクでは、イメージのダウンロードに時間がかかることがあります。この場合、ENCS 5400 デバイスのローカルリポジトリで大きなイメージファイルを使用可能にするオプションがあり、デバイスはプロビジョニング中にローカルイメージを使用するように指示されます。

次の手順は、イメージ ENCS 5400 を作成してアップロードする方法を示しています。

1. Cisco vManage イメージリポジトリにイメージパッケージをアップロードします。

   次に例を示します。

   vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz

2. SCP は VNF イメージを ENCS 5400 にコピーします。Cisco vManage はパッケージのダウンロードをスキップします。SCP でパッケージの名前を変更し、同じパッケージを Cisco vManage にアップロードしたことを確認します。

   ```
   <username>@<SCP_SERVER_IP>:/<package_name>
   intdatastore:<vnf_typ>_<name>_<version>_<package_name>
   ```

   例：

   ```
   scp admin@172.19.156.240:/vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz

   intdatastore:/ROUTER_vEdge_20.3.904-9_vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz
   ```

   パッケージ内の image_properties.xml ファイルの情報に基づいて、元のパッケージ名の前に <vnf_typ>_<name>_<version>_ プレフィックスを追加します。

   ```
   <image_properties>
   ```

```
        <vnf_type>ROUTER</vnf_type>
        <name>vEdge</name>
        <version>20.3.904-9</version>
……
……
.…..
</image_properties>
```

3. **show system:system file-list**コマンドを使用して、イメージが正常にコピーされたことを確認します。

その後、残りのネットワーク設計テンプレートワークフローに進み、Cisco vManage は VNF のダウンロード手順をスキップします。ネットワーク設計テンプレートで正しいパッケージを選択していることを確認します。

NFVIS とルータ VM 間の単一 IP アドレスの共有

このトピックでは、NFVIS とルータ VM の間で単一 IP アドレス共有機能を設定するためのエンドツーエンドの設定例を示します。

ステップ 1：第 0 日の HTTP ホストの設定

次の例は、HTTP サーバーを設定して、Cisco Catalyst 8000V と Cisco vEdge デバイスの第 0 日のコンフィギュレーション ファイルをホストする方法を示しています。

例：Cisco Catalyst 8000Vの第 0 日のコンフィギュレーション ファイルをホストする

```
Content-Type: multipart/mixed; boundary="==========2587222130433519110=="
MIME-Version: 1.0
--==========2587222130433519110==
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config"
#cloud-config
vinitparam:
 - otp : ${EX_OTP}
 - vbond : ${EX_VBOND}
 - org : ${EX_ORGNAME}
 - uuid : ${EX_UUID}

--==========2587222130433519110==
Content-Type: text/cloud-boothook; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
 filename="config-default.txt"
#cloud-boothook
system
   host-name             ${EX_HOSTNAME}
   system-ip             ${EX_SYSTEM_IP}
   overlay-id            1
   site-id               ${EX_SITE_ID}
   port-offset           0
   control-session-pps   300
   admin-tech-on-failure
   sp-organization-name  "${EX_ORGNAME}"
```

```
 organization-name     "${EX_ORGNAME}"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     115200
 vbond ${EX_VBOND} port 12346
 logging
  disk
   enable
  !
 !
!
bfd app-route multiplier 6
bfd app-route poll-interval 600000
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
 ca-tp-label          PROXY-SIGNING-CA
 settings expired-certificate  drop
 settings untrusted-certificate drop
 settings unknown-status       drop
 settings unsupported-protocol-versions drop
 settings unsupported-cipher-suites drop
 settings failure-mode         close
 settings minimum-tls-ver      TLSv1
!
no tcpproxy enable
!
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color default
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
  exit
 exit
 appqoe
  no tcpopt enable
 !
 omp
  no shutdown
```

```
    send-path-limit  4
    ecmp-limit       4
    graceful-restart
    no as-dot-notation
    timers
     holdtime               60
     advertisement-interval 1
     graceful-restart-timer 43200
     eor-timer              300
    exit
    address-family ipv4
     advertise connected
     advertise static
    !
    address-family ipv6
     advertise connected
     advertise static
    !
   !
  !
  security
   ipsec
    rekey               86400
    replay-window       512
    authentication-type sha1-hmac ah-sha1-hmac
   !
  !
  no service pad
  service tcp-keepalives-in
  service tcp-keepalives-out
  no service tcp-small-servers
  no service udp-small-servers
  username admin privilege 15 secret 0 admin
  vrf definition Mgmt-intf
   description Transport VPN
   rd          1:512
   address-family ipv4
    route-target export 1:512
    route-target import 1:512
    exit-address-family
   !
   address-family ipv6
    exit-address-family
   !
  !
vrf definition 500
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
 !
!
vrf definition ${EX_DATA_VPN_NUMBER}
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition ${EX_MGMT_VPN_NUMBER}
 !
 address-family ipv4
```

```
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
hostname ${EX_HOSTNAME}
username ${EX_SSH_USERNAME} privilege 15 secret 0 ${EX_SSH_PASSWORD}
enable password ${EX_ENABLE_PASSWORD}
!
ip name-server ${EX_DNS_IP}
!
  ip arp proxy disable
  no ip finger
  no ip rcmd rcp-enable
  no ip rcmd rsh-enable
  no ip dhcp use class
  ip multicast route-limit 2147483647
  ip bootp server
  no ip source-route
  no ip http server
  no ip http secure-server
  no ip http ctc authentication
  no ip igmp ssm-map query dns
  interface GigabitEthernet1
   vrf forwarding 500
   description MGMT
   no shutdown
   arp timeout 1200
   ip address ${NICID_0_IP_ADDRESS} ${NICID_0_NETMASK}
   ip redirects
   ip mtu    1500
   mtu         1500
   negotiation auto
  exit
  interface GigabitEthernet2
   description Transport
   no shutdown
   arp timeout 1200
   ip address ${EX_VPN0_WAN_IP_ADDRESS} ${EX_VPN0_WAN_NETMASK}
   ip nat outside
   ip redirects
   ip mtu    1500
   mtu         1500
   negotiation auto
  exit
interface GigabitEthernet3
 vrf forwarding ${EX_MGMT_VPN_NUMBER}
 ip address ${EX_MGMT_IP_ADDRESS} ${EX_MGMT_NETMASK}
 no shutdown
 exit
!
interface GigabitEthernet4
 vrf forwarding ${EX_DATA_VPN_NUMBER}
 ip address ${EX_LAN_IP_ADDRESS} ${EX_LAN_NETMASK}
 no shutdown
 exit
!
  interface Tunnel2
   no shutdown
   ip unnumbered GigabitEthernet2
   no ip redirects
   ipv6 unnumbered GigabitEthernet2
   no ipv6 redirects
   tunnel source GigabitEthernet2
```

```
   tunnel mode sdwan
  exit
  clock timezone UTC 0 0
  logging persistent size 104857600 filesize 10485760
  logging buffered 512000
  no logging rate-limit
  logging persistent
  aaa authentication login default local
  aaa authorization exec default local
  aaa session-id common
  no crypto ikev2 diagnose error
  no crypto isakmp diagnose error
  snmp-server ifindex persist
  line con 0
   login authentication default
   speed    115200
   stopbits 1
  !
  line vty 0 4
   transport input ssh
  !
  line vty 5 80
   transport input ssh
  !
  lldp run
  nat64 translation timeout tcp 60
  nat64 translation timeout udp 1
 !
!
ip route 0.0.0.0 0.0.0.0 ${EX_VPN0_WAN_GATEWAY}
!
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat route vrf 500 0.0.0.0 0.0.0.0 global
!

--================2587222130433519110==
```

例：バージョン 20.5 の Cisco vEdge デバイスの第 0 日のコンフィギュレーション ファイルをホストする

```
#cloud-config
write_files:
- path: /etc/viptela/otp
  content: "${OTP}"
- path: /etc/viptela/uuid
  content: "${UUID}"
- path: /etc/default/personality
  content: "vedge"
- path: /etc/default/inited
  content: "1"
- path: /etc/viptela/cdb_init_done
  content: "1"
- path: /etc/viptela/vdaemon_gen_id
  content: "0"
- path: /etc/confd/init/cloud-init.xml
  content: |
    <config xmlns="http://tail-f.com/ns/config/1.0">
      <omp xmlns="http://viptela.com/omp">
        <advertise>
          <protocol>ospf</protocol>
          <route>external</route>
        </advertise>
        <advertise>
          <protocol>connected</protocol>
```

```
  </advertise>
  <advertise>
    <protocol>static</protocol>
  </advertise>
</omp>
<security xmlns="http://viptela.com/security">
  <ipsec>
    <authentication-type>ah-sha1-hmac</authentication-type>
    <authentication-type>sha1-hmac</authentication-type>
  </ipsec>
</security>
<system xmlns="http://viptela.com/system">
  <personality>vedge</personality>
  <rootcert-installed>true</rootcert-installed>
  <host-name>${HOSTNAME}</host-name>
  <system-ip>${SYSTEM_IP}</system-ip>
  <site-id>${SITE_ID}</site-id>
  <organization-name>${ORGNAME}</organization-name>
  <vbond>
    <remote>${VBOND}</remote>
  </vbond>
  <aaa>
    <auth-order>local</auth-order>
    <auth-order>radius</auth-order>
    <auth-order>tacacs</auth-order>
    <usergroup>
      <name>basic</name>
      <task>
        <mode>system</mode>
        <permission>read</permission>
        <permission>write</permission>
      </task>
      <task>
        <mode>interface</mode>
        <permission>read</permission>
        <permission>write</permission>
      </task>
    </usergroup>
    <usergroup>
      <name>netadmin</name>
    </usergroup>
    <usergroup>
      <name>operator</name>
      <task>
        <mode>system</mode>
        <permission>read</permission>
      </task>
      <task>
        <mode>interface</mode>
        <permission>read</permission>
      </task>
      <task>
        <mode>policy</mode>
        <permission>read</permission>
      </task>
      <task>
        <mode>routing</mode>
        <permission>read</permission>
      </task>
      <task>
        <mode>security</mode>
        <permission>read</permission>
      </task>
    </usergroup>
```

```
            <user>
              <name>admin</name>
<password>$6$siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdkorYYTLrL6syiG6qnLABInrE96HJiKF6QRq1</password>
            </user>
          </aaa>
        </system>
        <vpn xmlns="http://viptela.com/vpn">
          <vpn-instance>
            <vpn-id>0</vpn-id>
            <dns>
              <dns-addr>${DNS_IP}</dns-addr>
            </dns>
            <interface>
              <if-name>ge0/0</if-name>
              <ip>
                <dhcp-client>true</dhcp-client>
              </ip>
              <nat/>
              <tunnel-interface>
                <encapsulation>
                  <encap>ipsec</encap>
                </encapsulation>
                <allow-service>
                  <all>true</all>
                </allow-service>
              </tunnel-interface>
              <shutdown>false</shutdown>
            </interface>
            <interface>
              <if-name>ge0/3</if-name>
              <ip>
                <address>${NICID_4_IP_ADDRESS}/${NICID_4_CIDR_PREFIX}</address>
              </ip>
              <shutdown>false</shutdown>
            </interface>
          </vpn-instance>
          <vpn-instance>
            <vpn-id>${DATA_VPN_NUMBER}</vpn-id>
            <interface>
              <if-name>ge0/2</if-name>
              <ip>
                <address>${SERVICE_IP}/${SERVICE_MASK_LENGTH}</address>
              </ip>
              <shutdown>false</shutdown>
            </interface>
          </vpn-instance>
          <vpn-instance>
            <vpn-id>${MANAGEMENT_VPN_NUMBER}</vpn-id>
            <interface>
              <if-name>ge0/1</if-name>
              <ip>
                <address>${MGMT_IP}/${MGMT_MASK_LENGTH}</address>
              </ip>
              <shutdown>false</shutdown>
            </interface>
          </vpn-instance>
          <vpn-instance>
            <vpn-id>512</vpn-id>
            <interface>
              <if-name>eth0</if-name>
              <shutdown>false</shutdown>
            </interface>
```

```
        </vpn-instance>
      </vpn>
    </config>
```

ステップ 2：単一 IP アドレス共有の設定

この例では、Cisco vManage の CLI アドオン機能テンプレートを使用して、NFVIS とルータ VM 間の単一 IP アドレス共有を設定する方法を示します。

CLI アドオン機能テンプレートを使用したCisco Catalyst 8000Vの設定例

この例では、NFVIS は VPN 0 の int-mgmt-net-br インターフェイスを使用して、Cisco vManage との制御接続を確立します。この設定には、第 0 日のコンフィギュレーションの VM ライフサイクル設定も含まれます。NFVIS は、設定に含まれている HTTP サーバーからこの情報を取得します。

```
vm_lifecycle tenants tenant admin
 description      "Built-in Admin Tenant"
 managed_resource true
 vim_mapping      true
 deployments deployment deployment-ROUTER_1
  vm_group deployment-ROUTER_1
   image
ROUTER_C8000V_V175-Serial_C8Kv_175_LATEST_20201115_122120-serial_vBranch_Ubaid_Sdwan3.tar.gz

   flavor             ROUTER_1
   vim_vm_name        ROUTER_1
   bootup_time        900
   recovery_wait_time 5
   recovery_policy action_on_recovery REBOOT_ONLY
   !
   config_data configuration ciscosdwan_cloud_init.cfg
    file "http://172.25.221.219/config/UBAID_SDWAN_CLOUD_INITnew.cfg"
    variable EX_UUID
     val [ {{EX_UUID}} ]
    !
    variable EX_OTP
     val [ {{EX_OTP}} ]
    !
    variable EX_ORGNAME
     val [ "{{EX_ORGNAME}}" ]
    !
    variable EX_VBOND
     val [ {{EX_VBOND}} ]
    !
    variable EX_SYSTEM_IP
     val [ {{EX_SYSTEM_IP}} ]
    !
    variable EX_SITE_ID
     val [ {{EX_SITE_ID}} ]
    !
    variable EX_VPN0_WAN_GATEWAY
     val [ {{EX_VPN0_WAN_GATEWAY}} ]
    !
    variable EX_VPN0_WAN_IP_ADDRESS
     val [ {{EX_VPN0_WAN_IP_ADDRESS}} ]
    !
    variable EX_VPN0_WAN_NETMASK
     val [ {{EX_VPN0_WAN_NETMASK}} ]
    !
    variable EX_DNS_IP
     val [ {{EX_DNS_IP}} ]
```

```
    !
    variable EX_SSH_USERNAME
     val [ {{EX_SSH_USERNAME}} ]
    !
    variable EX_SSH_PASSWORD
     val [ "{{EX_SSH_PASSWORD}}" ]
    !
    variable EX_ENABLE_PASSWORD
     val [ "{{EX_ENABLE_PASSWORD}}" ]
    !
    variable EX_HOSTNAME
     val [ {{EX_HOSTNAME}} ]
    !
    variable EX_LAN_IP_ADDRESS
     val [ {{EX_LAN_IP_ADDRESS}} ]
    !
    variable EX_LAN_NETMASK
     val [ {{EX_LAN_NETMASK}} ]
    !
    variable EX_MGMT_IP_ADDRESS
     val [ {{EX_MGMT_IP_ADDRESS}} ]
    !
    variable EX_MGMT_NETMASK
     val [ {{EX_MGMT_NETMASK}} ]
    !
    variable EX_DATA_VPN_NUMBER
     val [ {{EX_DATA_VPN_NUMBER}} ]
    !
    variable EX_MGMT_VPN_NUMBER
     val [ {{EX_MGMT_VPN_NUMBER}} ]
    !
   !
  !
 !
!
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
!
vpn 0
interface int-mgmt-net-br
  no shutdown
  tunnel-interface
   color bronze
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
!
```

CLI アドオン機能テンプレートを使用した Cisco vEdge クラウドルータの設定例

この例では、NFVIS は VPN 0 の int-mgmt-net-br インターフェイスを使用して、Cisco vManage との制御接続を確立します。この設定には、第 0 日のコンフィギュレーションの VM ライフサイクル設定も含まれます。NFVIS は、設定に含まれている HTTP サーバーからこの情報を取得します。

```
vm_lifecycle tenants tenant admin
 description      "Built-in Admin Tenant"
 managed_resource true
 vim_mapping      true
 deployments deployment deployment-ROUTER_1
  vm_group deployment-ROUTER_1
   bootup_time        600
   recovery_wait_time 5
   recovery_policy action_on_recovery REBOOT_ONLY
   !
   kpi_data kpi VM_ALIVE
     metric_collector type ICMPPing
     metric_collector nicid 4
     !

   config_data configuration /openstack/latest/user_data
    file "http://172.25.221.219/config/20.5-vedge-single-ip-dhcp.cfg"
    variable EX_UUID
     val [ {{EX_UUID}} ]
    !
    variable EX_OTP
     val [ {{EX_OTP}} ]
    !
    variable EX_ORGNAME
     val [ "{{EX_ORGNAME}}" ]
    !
    variable EX_VBOND
     val [ {{EX_VBOND}} ]
    !
    variable EX_SYSTEM_IP
     val [ {{EX_SYSTEM_IP}} ]
    !
    variable EX_SITE_ID
     val [ {{EX_SITE_ID}} ]
    !
    variable EX_DNS_IP
     val [ {{EX_DNS_IP}} ]
    !
    variable EX_SSH_USERNAME
     val [ {{EX_SSH_USERNAME}} ]
    !
    variable EX_SSH_PASSWORD
     val [ "{{EX_SSH_PASSWORD}}" ]
    !
    variable EX_ENABLE_PASSWORD
     val [ "{{EX_ENABLE_PASSWORD}}" ]
    !
    variable EX_HOSTNAME
     val [ {{EX_HOSTNAME}} ]
    !
    variable EX_SERVICE_IP
     val [ {{EX_SERVICE_IP}} ]
    !
    variable EX_SERVICE_MASK_LENGTH
     val [ {{EX_SERVICE_MASK_LENGTH}} ]
    !
    variable EX_MGMT_IP
     val [ {{EX_MGMT_IP}} ]
    !
    variable EX_MGMT_MASK_LENGTH
     val [ {{EX_MGMT_MASK_LENGTH}} ]
    !
    variable EX_DATA_VPN_NUMBER
     val [ {{EX_DATA_VPN_NUMBER}} ]
```

```
    !
    variable EX_MANAGEMENT_VPN_NUMBER
     val [ {{EX_MANAGEMENT_VPN_NUMBER}} ]
    !
   !
  !
 !
!
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
!
vpn 0
interface int-mgmt-net-br
  no shutdown
  tunnel-interface
   color bronze
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
!
```