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 （1 ページ）
- ネットワーク設計 （5 ページ）

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。

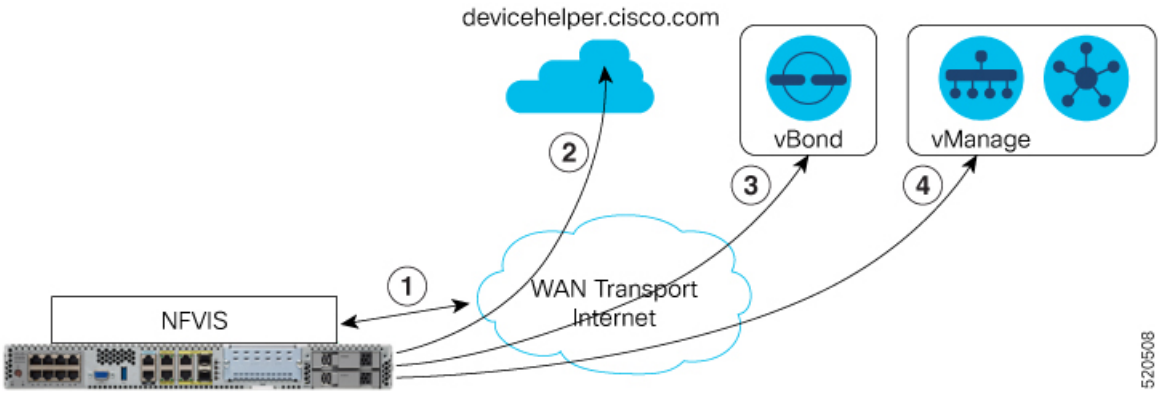
Cisco vBond への PnP リダイレクションの進行状況を表示するには、**show pnp status**コマンドを使用します。

```
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。

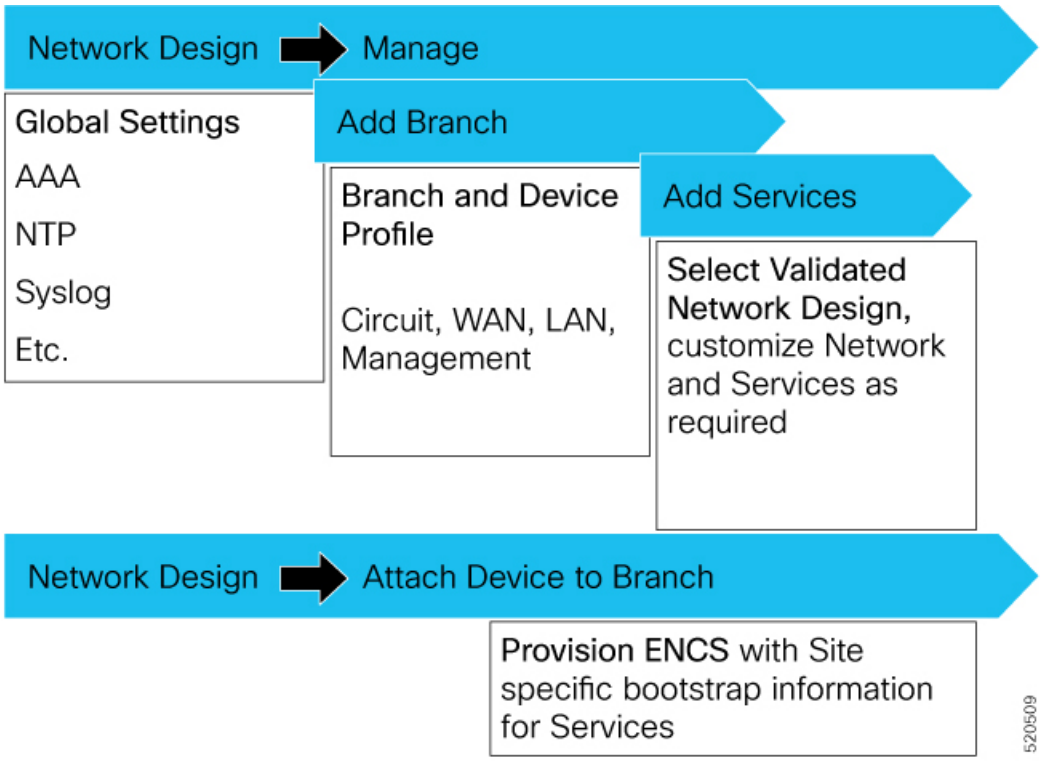
ネットワーク ファイアウォールの要件

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 *1*:

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。

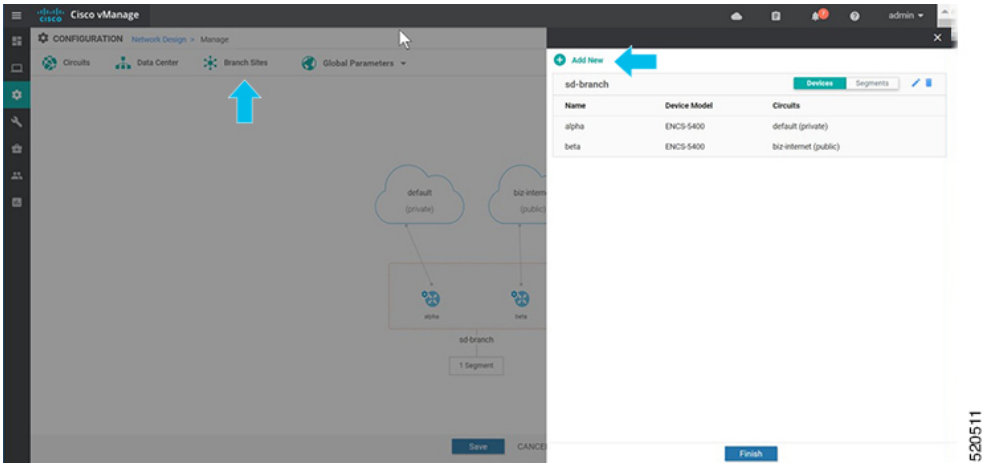
ネットワークトポロジのブランチサイトを設定するには、次の手順を実行します。

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。

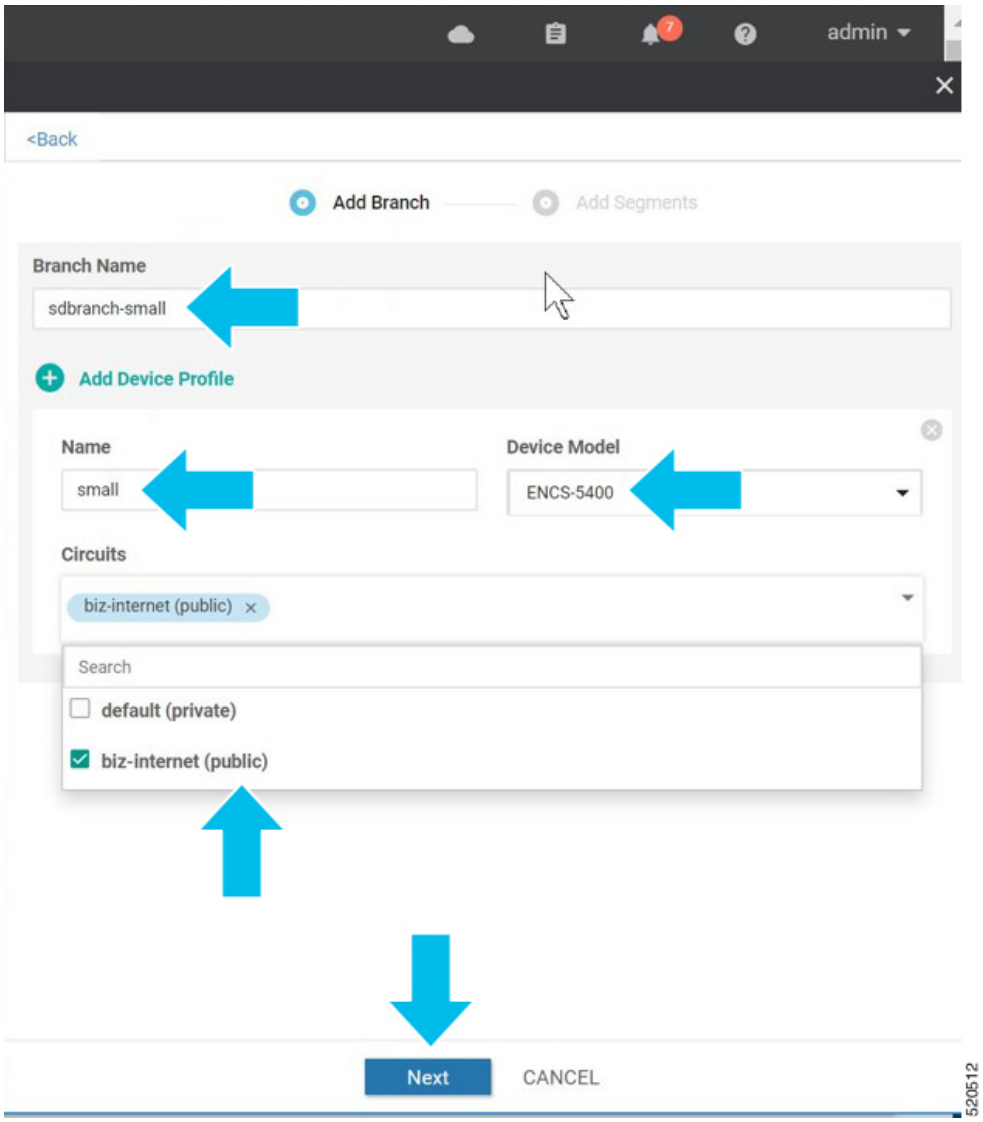
   ブランチサイトを追加するには、[Add new] をクリックします。



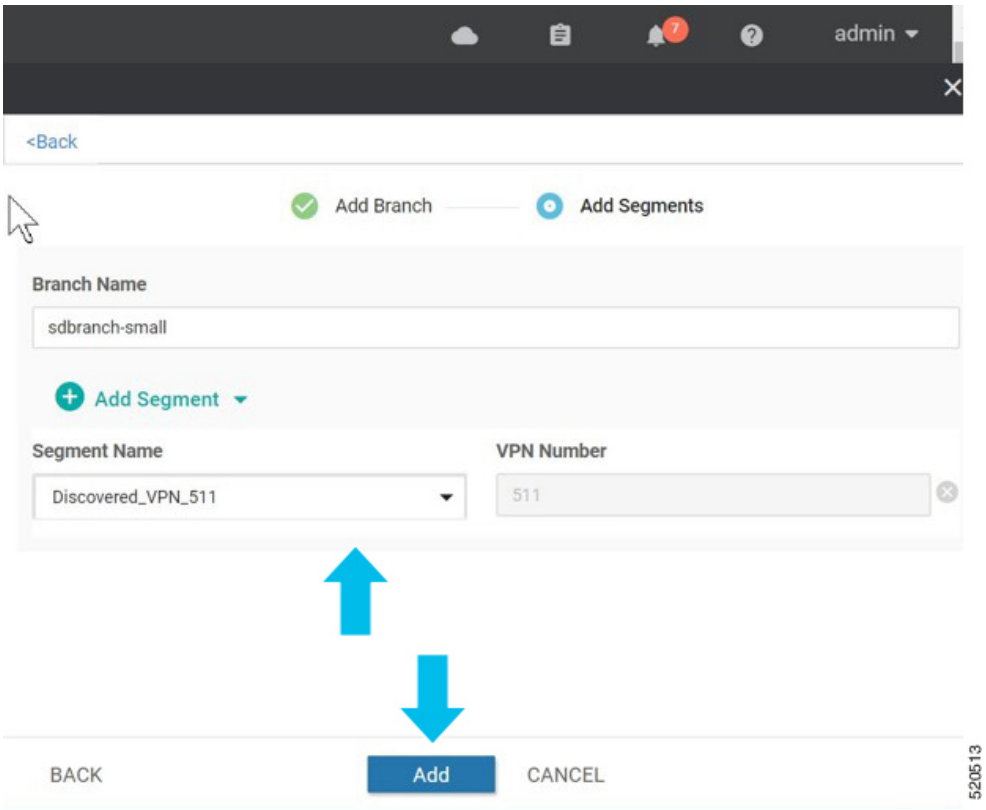
3. ブランチを追加するには、次の手順を実行します。
   1. [Branch Name] にブランチサイトの一意の名前を入力します。この名前は、トポロジ内の他のデータセンター、ブランチサイト、またはデバイスプロファイルには使用できません。名前には、文字、数字、アンダースコア、ハイフンを使用できますが、スペースや特殊文字は使用できません。
   2. 新しいデバイスプロファイルを追加するには、[Add Device Profile] をクリックします。

      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。

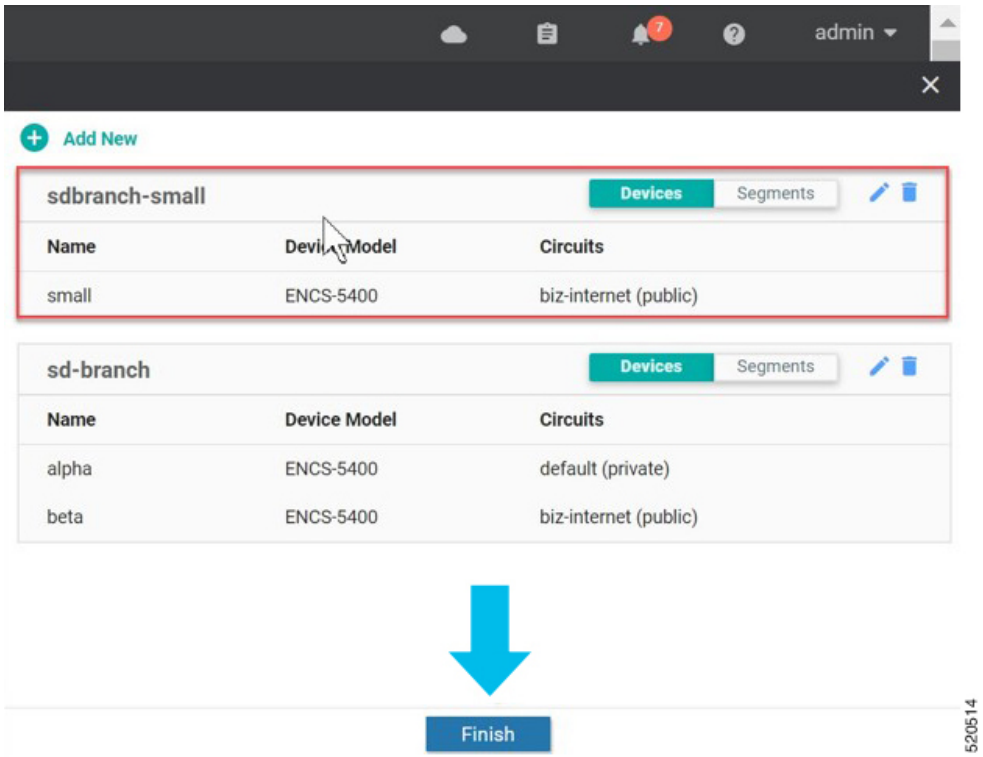


4. セグメントは、ブランチサイト内のすべてのデバイスプロファイルに関連付けられているサービス側VPNです。各ブランチサイトには、少なくとも1つのセグメントが必要です。複数のブランチサイトで同じセグメントを使用できます。1 つ以上のセグメントを追加するには、次の手順を実行します。
   1. [Add Segment] をクリックします。ドロップダウンリストからセグメントを選択します。VPN 番号には、セグメントに設定された VPN ID が自動的に入力されます。
   2. [Add] をクリックします。

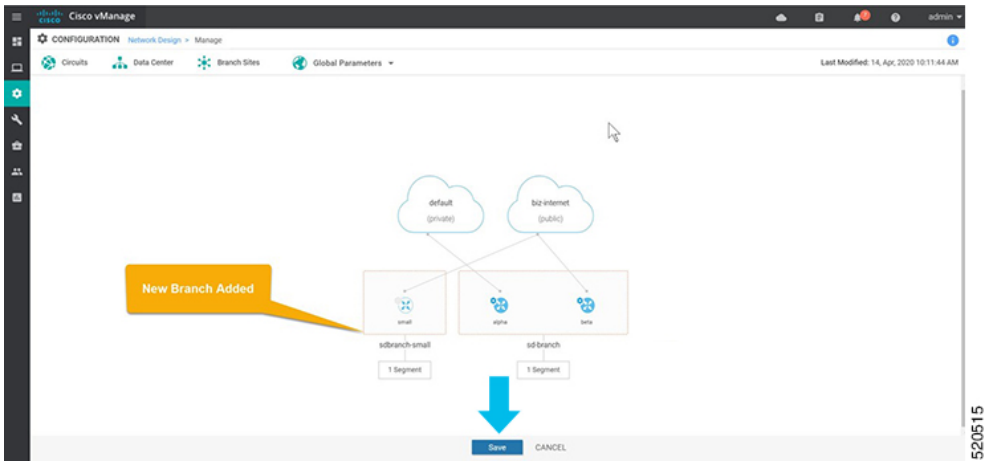


ブランチサイトのリストが表示されます。

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

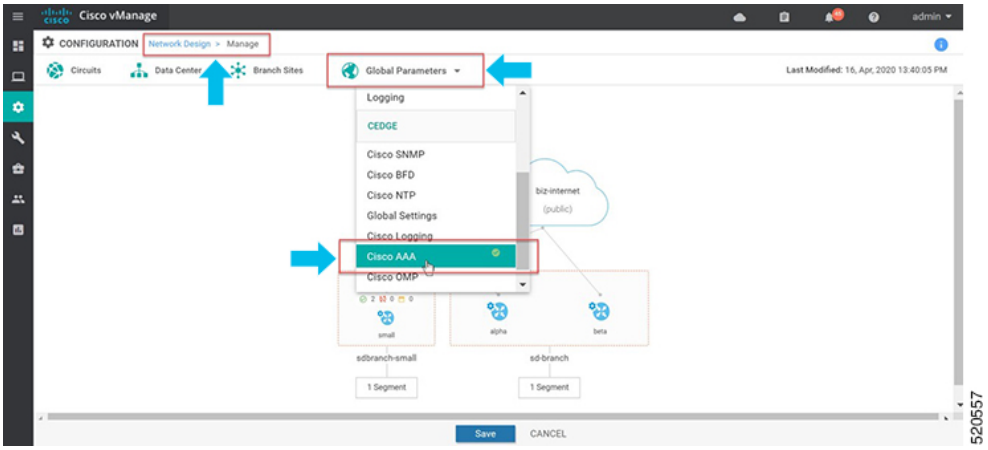
グローバルパラメータは、ネットワークトポロジ内のすべてのデバイスプロファイルで使用される設定です。グローバルパラメータを設定しない場合は、工場出荷時のデフォルト設定がデバイスプロファイルに使用されます。

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。

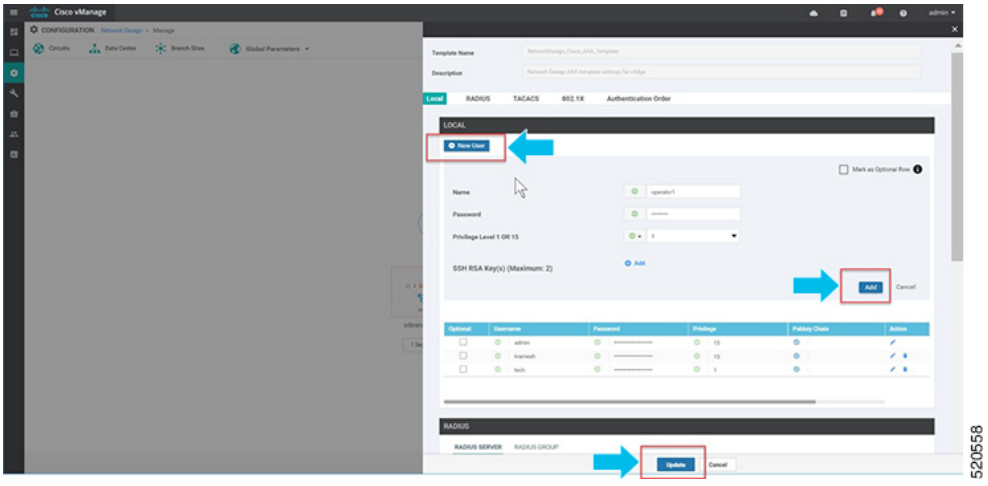


3. テンプレートの設定

   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。



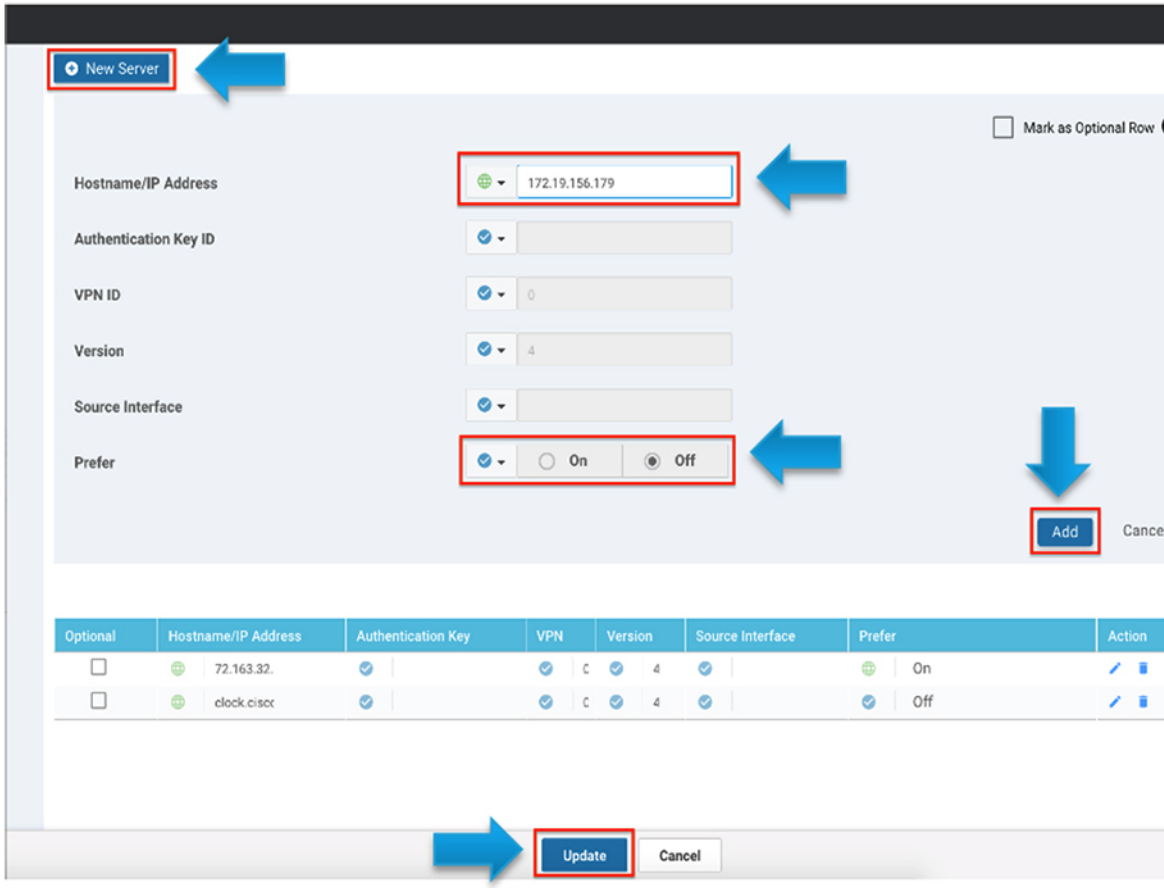
Cisco vManage 20.1 および 20.3 リリースは、ローカルユーザーの AAA グローバルパラメータのみをサポートします。TACACS および RADIUS 設定は、デバイスのアドオン CLI 機能の設定を使用して更新できます。

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。

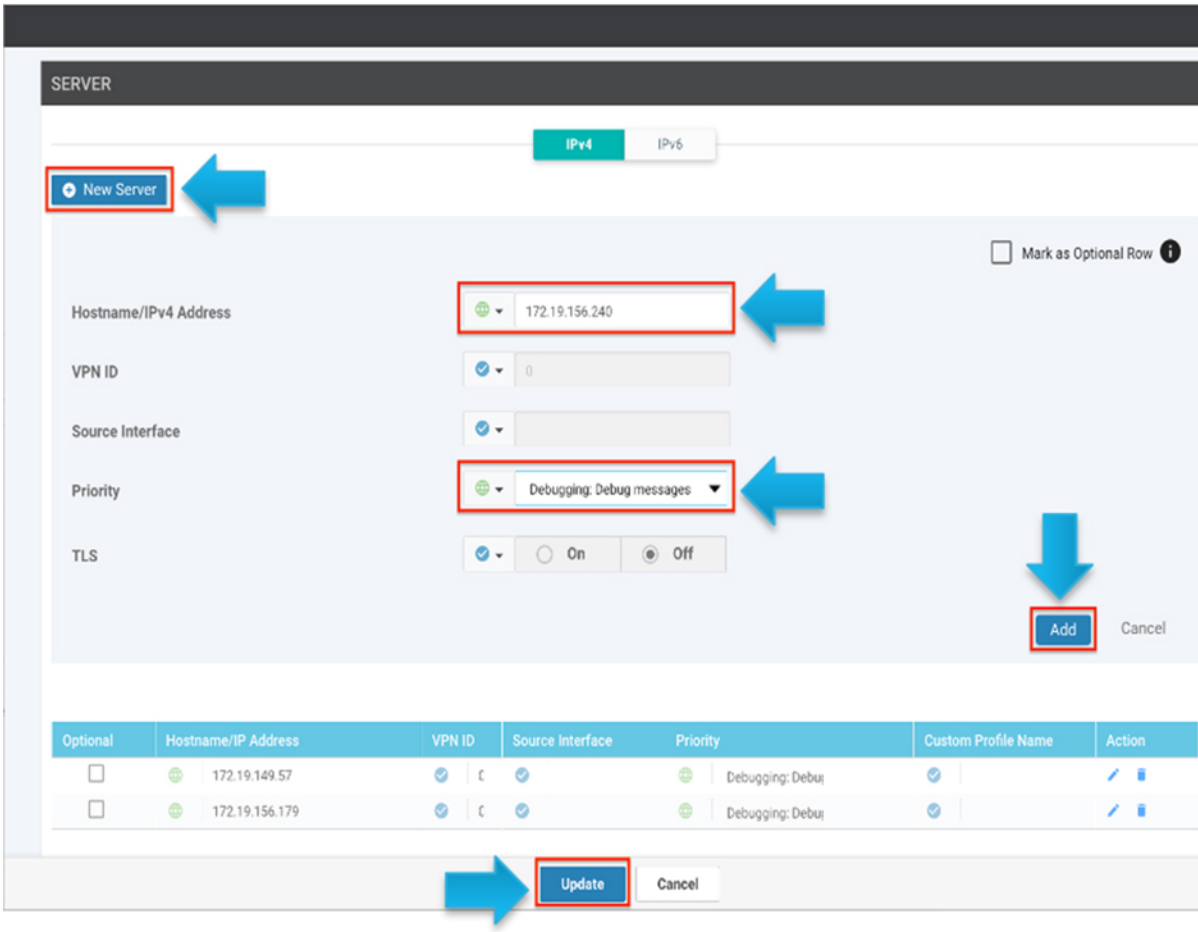


   [Authentication Key ID]、[VLAN ID]、[Version]、[Source Interface] は、NFVIS プラットフォームには適用されません。NFVIS プラットフォームは、1 つの優先 NTP サーバーと 1 つのバックアップ NTP サーバーのみをサポートします。

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。



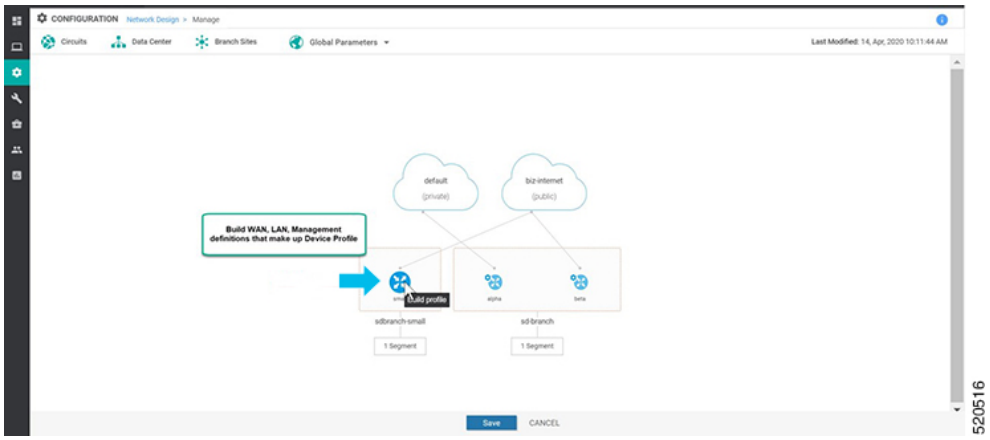
[VPN ID]、[Source Interface] は、NFVIS プラットフォームには適用されません。サポートされるロギングサーバーの最大数は 4 です。[Priority] が同じ設定を使用していることを確認します。NFVIS プラットフォームは、グローバル設定として 1 つのプライオリティまたはロギング重大度のみをサポートします。

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。

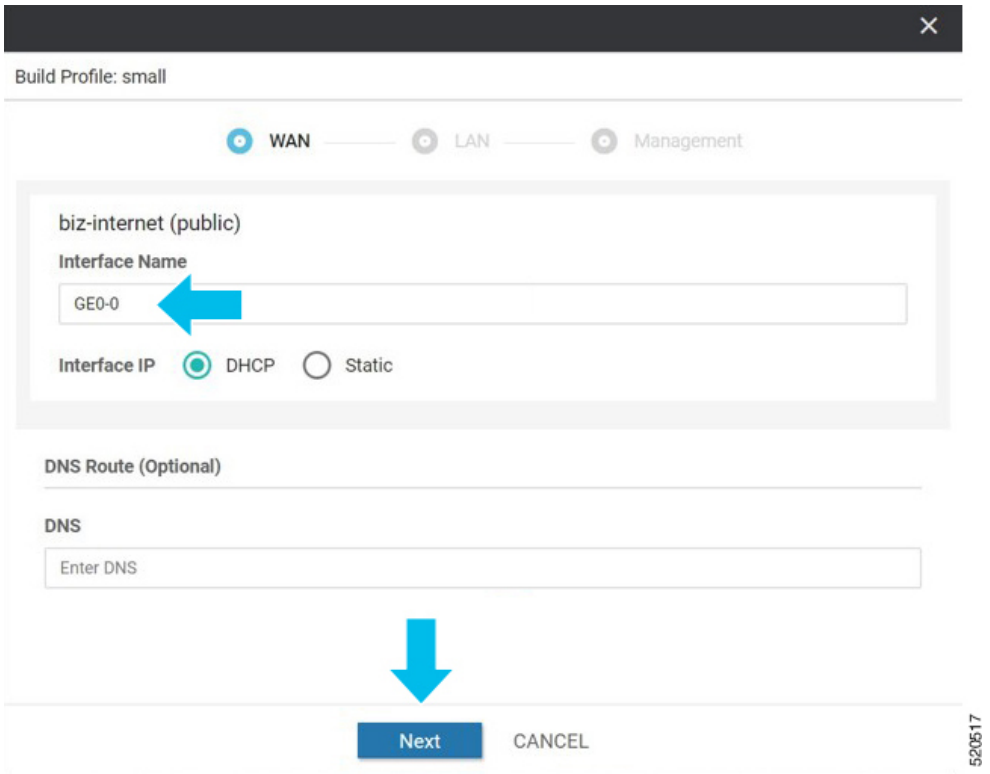
ネットワークトポロジでルータのデバイスプロファイルを設定するには、次の手順を実行します。

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。



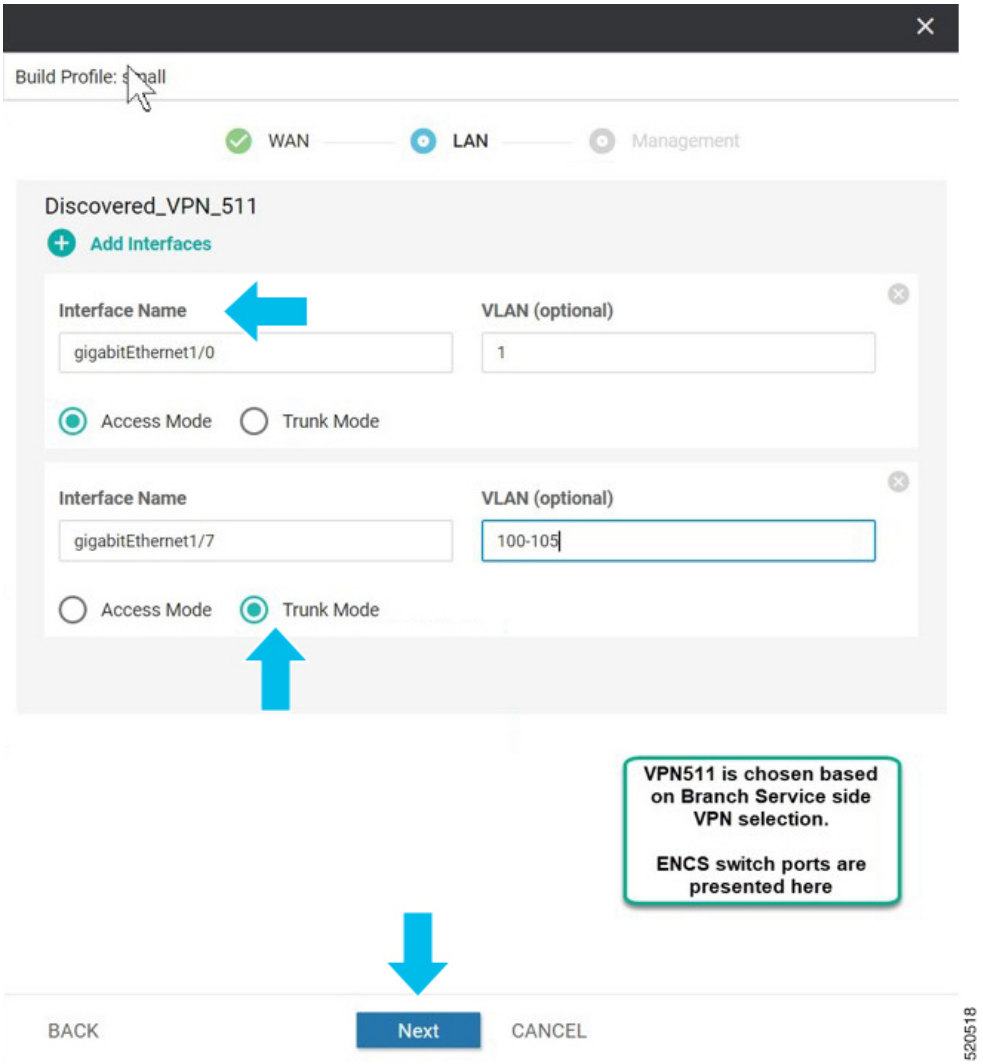
3. デバイスプロファイルを作成するには、プロファイルの WAN インターフェイスの詳細を入力します。

   - [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。

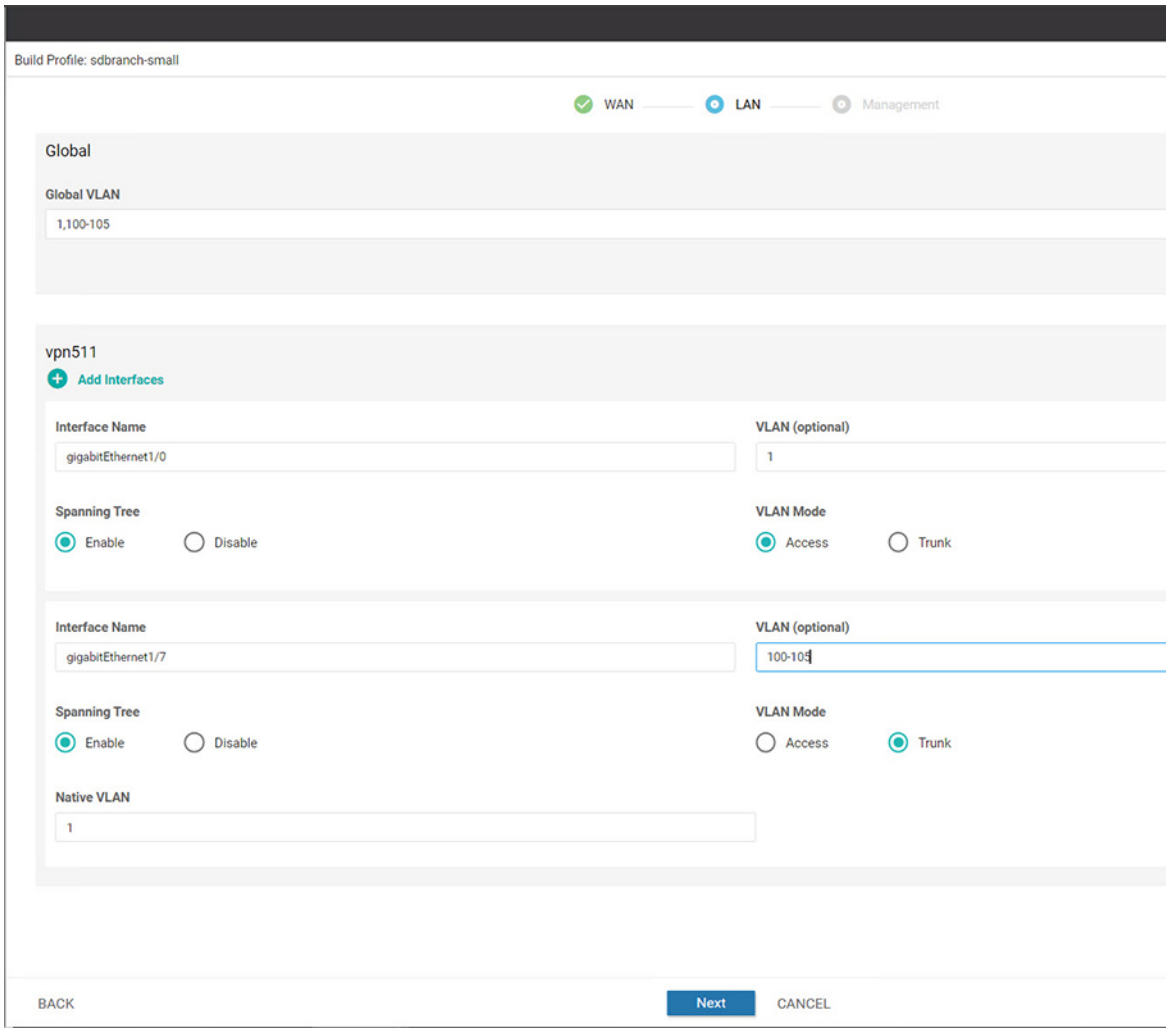


4. プロファイルの LAN インターフェイスの詳細を入力します。
   - [Interface Name] に LAN 側インターフェイスの名前を入力して、セグメントに関連付けます。
   - （任意）展開に必要な場合は、VLAN にサブインターフェイスを入力します。
   - [Access Mode] または [Trunk Mode] オプションボタンのいずれかを選択します。
   - [Next] をクリックします。

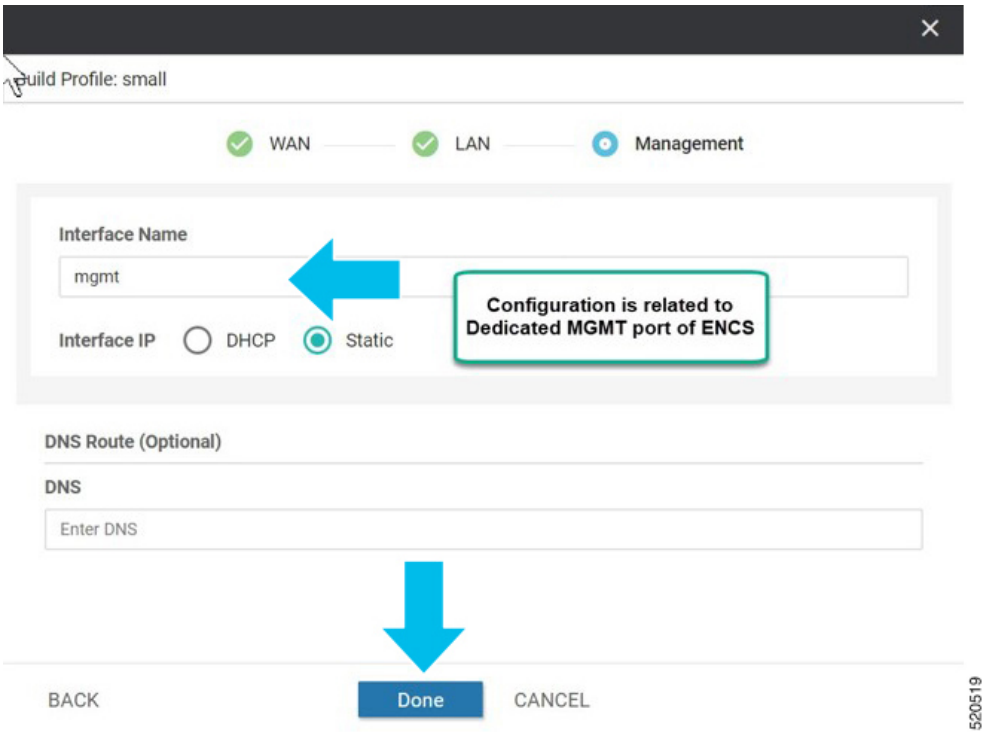
グローバル VLAN は、アドオン CLI テンプレートを使用して定義する必要があります。グローバル VLAN は、ENCS スイッチポートで使用されるすべての VLAN の集合です。



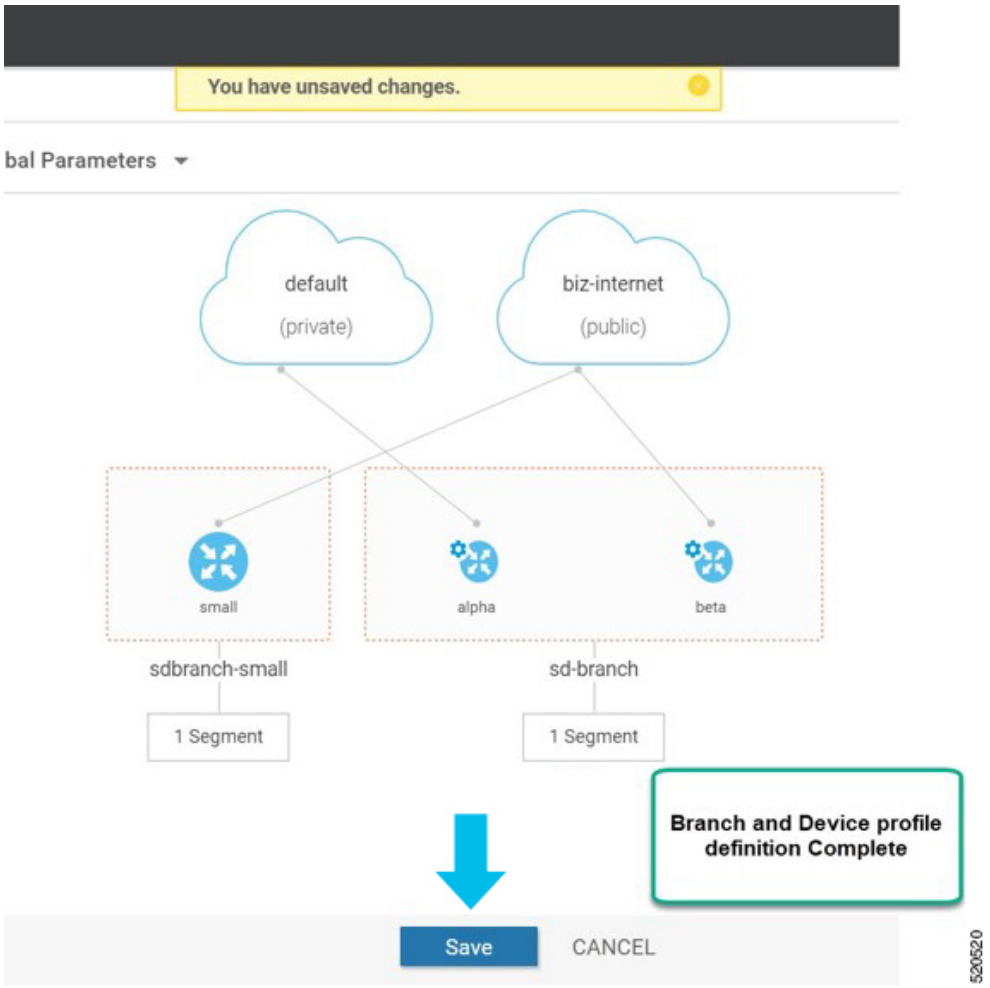
NFVIS 4.4 リリース以降、Cisco vManage から追加の LAN インターフェイスの詳細を設定できます。



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。

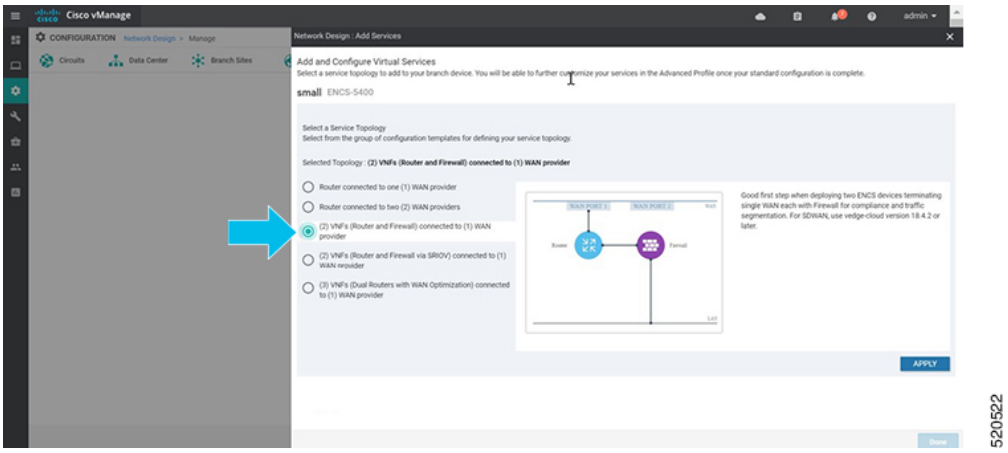
サービス、仮想ネットワーク、および関連する仮想スイッチまたはブリッジ用の VNF イメージパッケージは、ENCS ネットワーク設計の一部です。仮想 NIC（VNIC）は VNF サービスの一部であり、VNIC の順序は、異なるサービスを通過するトラフィックフローが意図した順序で連続するように正しく設定する必要があります。ユーザーエクスペリエンスを簡素化するために、シスコが設計した一連の規範的な検証済み設計を選択し、ネットワーク設計を完成させることができます。必要に応じて、ネットワークトポロジをカスタマイズして、サービスまたはネットワークを削除および変更することもできます。

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。

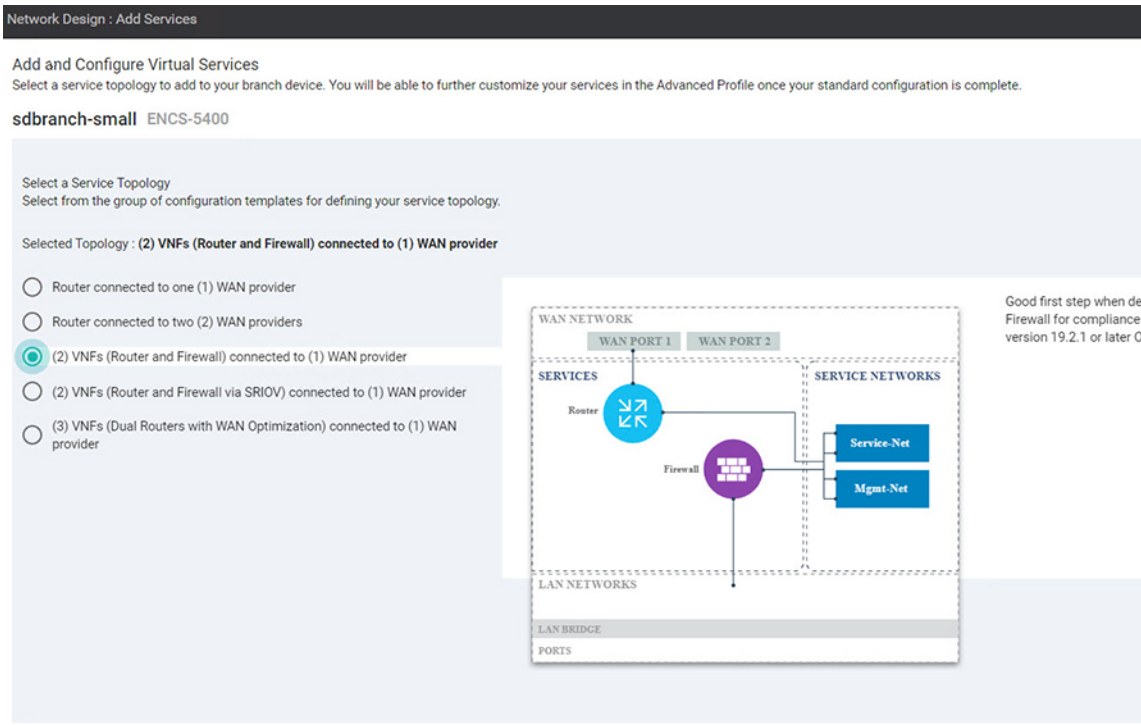
サイトグループのサービスを追加し、ネットワークトポロジテンプレートを作成するには、次の手順を実行します。

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。



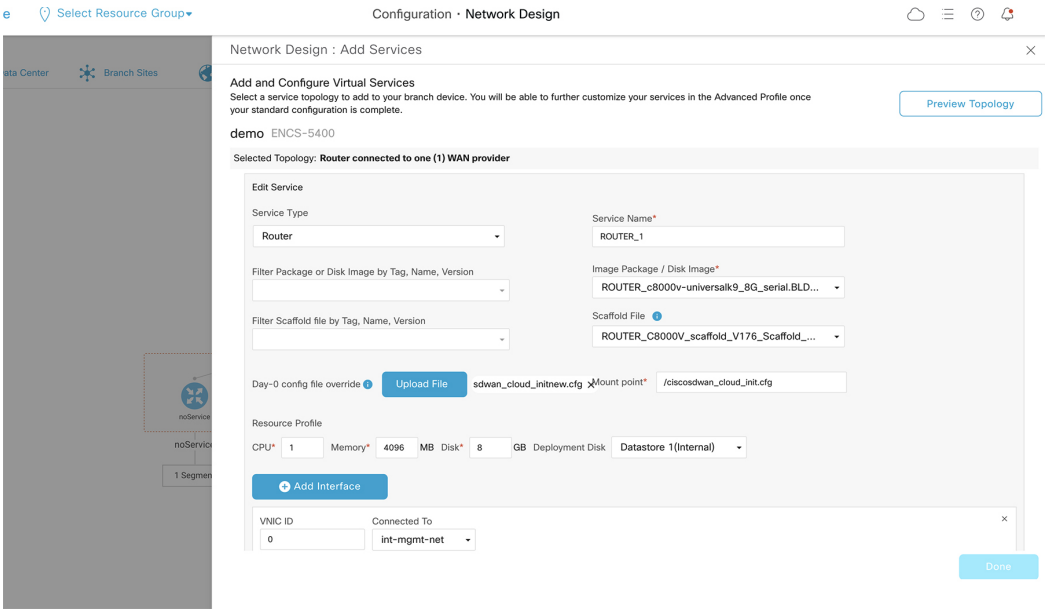
NFVIS 4.4 リリース以降、リストされているテンプレートのトポロジのグラフィカルビューを使用できます。



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}**

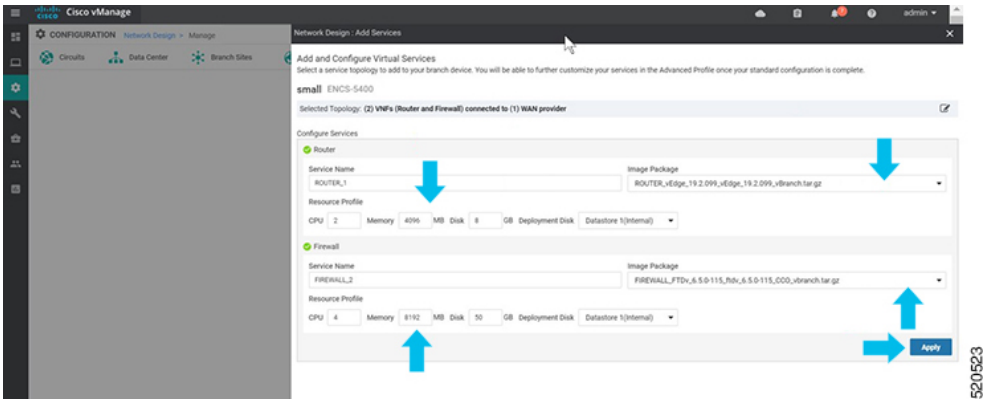


5. 仮想サービスを追加して設定するには、仮想サービスの詳細を入力します。

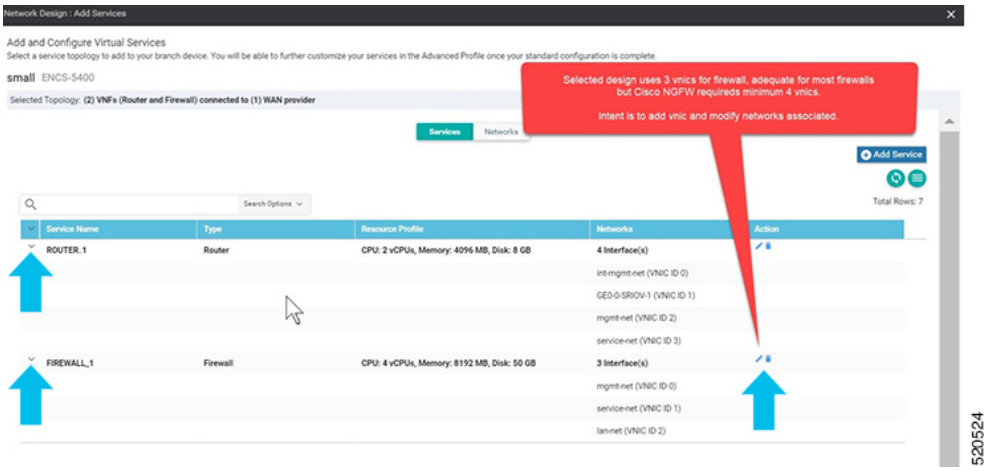
   - ドロップダウンリストから [Image Package] を選択し、リソースプロファイルの詳細を入力します。

   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

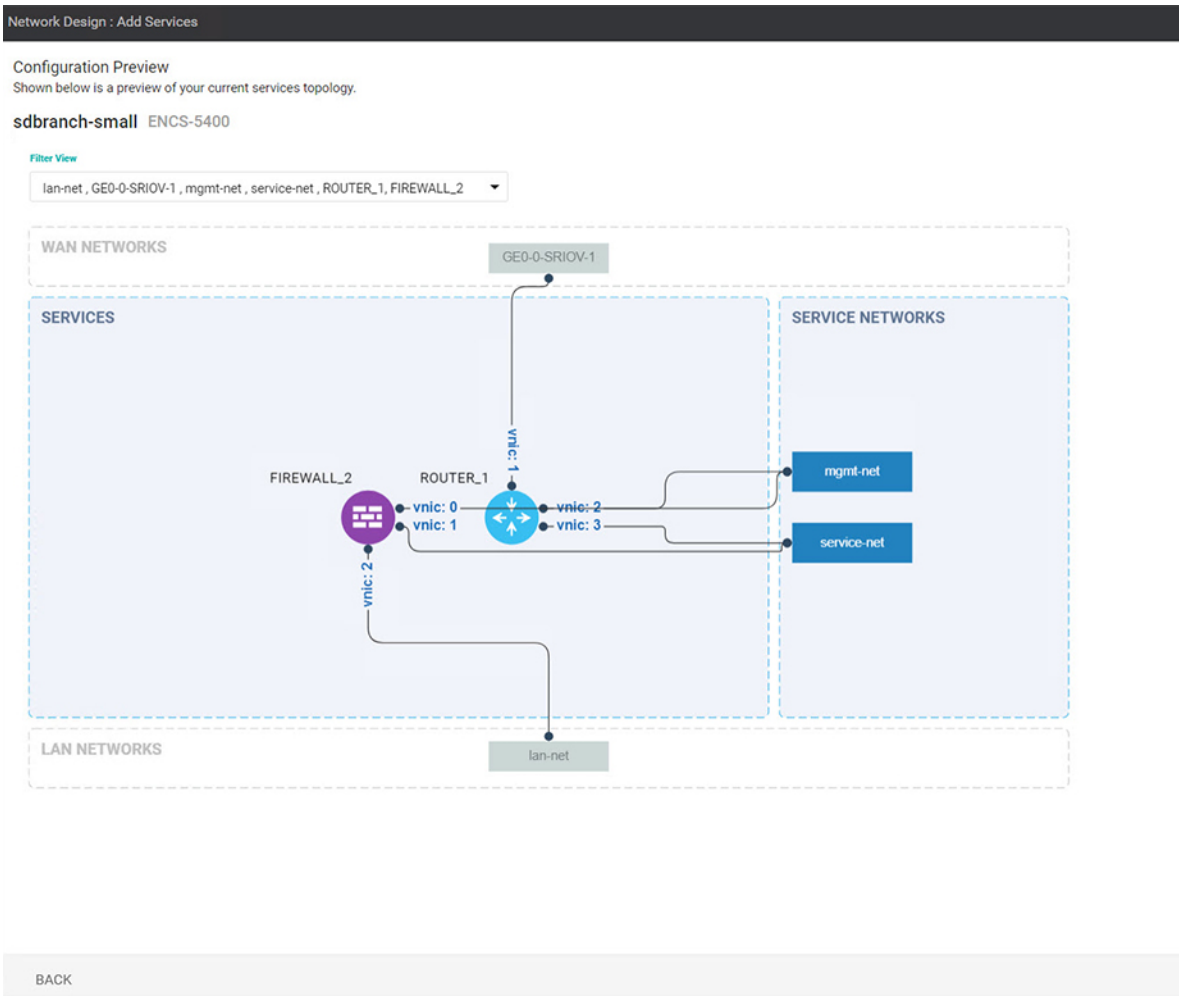
   - [Apply] をクリックします。



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。



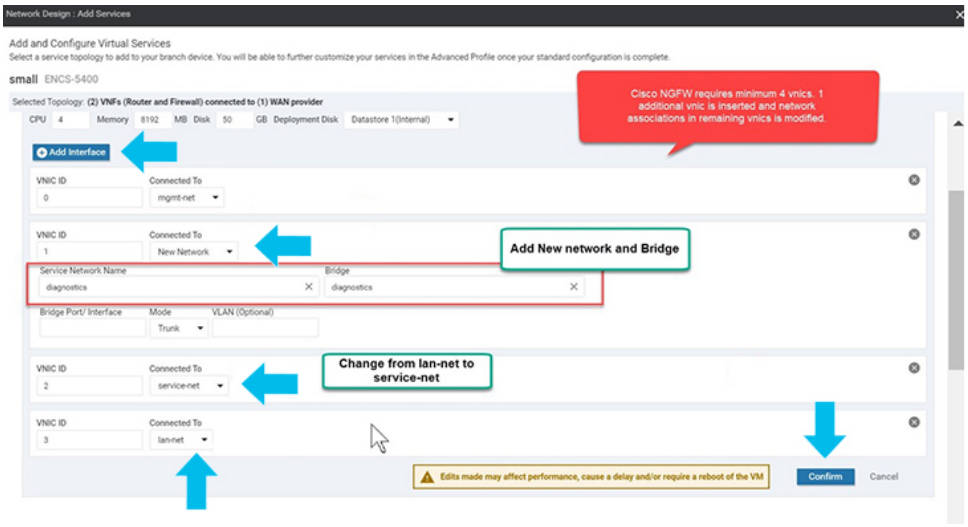
NFVIS 4.4 以降では、[Preview Topology] をクリックして、追加されたサービスのトポロジを関連ネットワークとともに表示できます。ドロップダウンメニューを使用して [Filter View] を選択し、必要なサービスだけを表示できます。



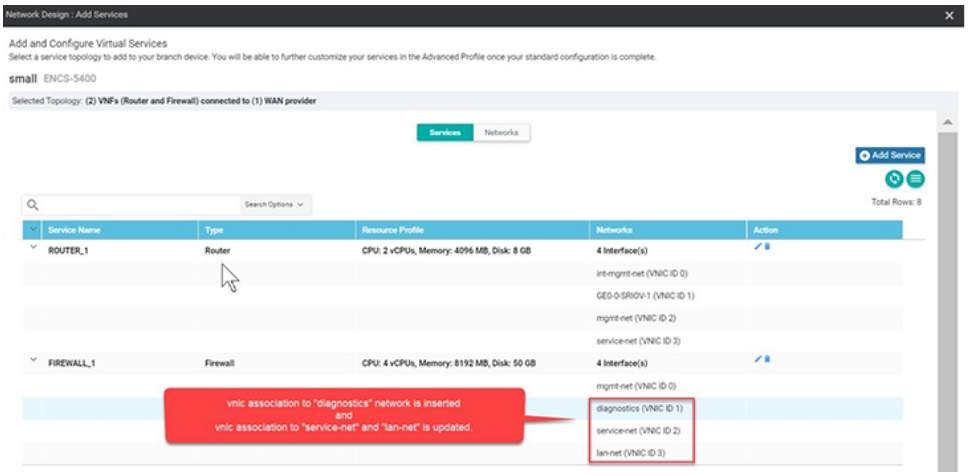
7. [+ Add Interface] をクリックして新しいネットワークを追加します。新しいネットワークに関連付けられたネットワークの詳細を入力します。

   既存のインターフェイスに関連する詳細を変更します。

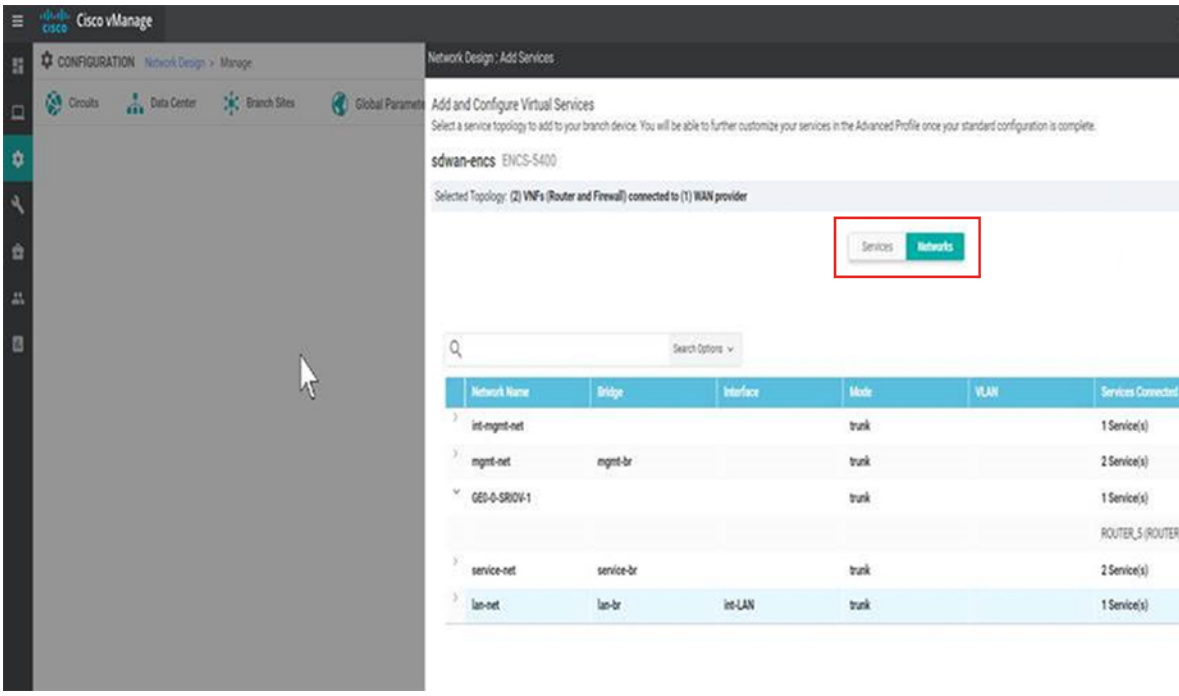
   [Confirm] をクリックします。



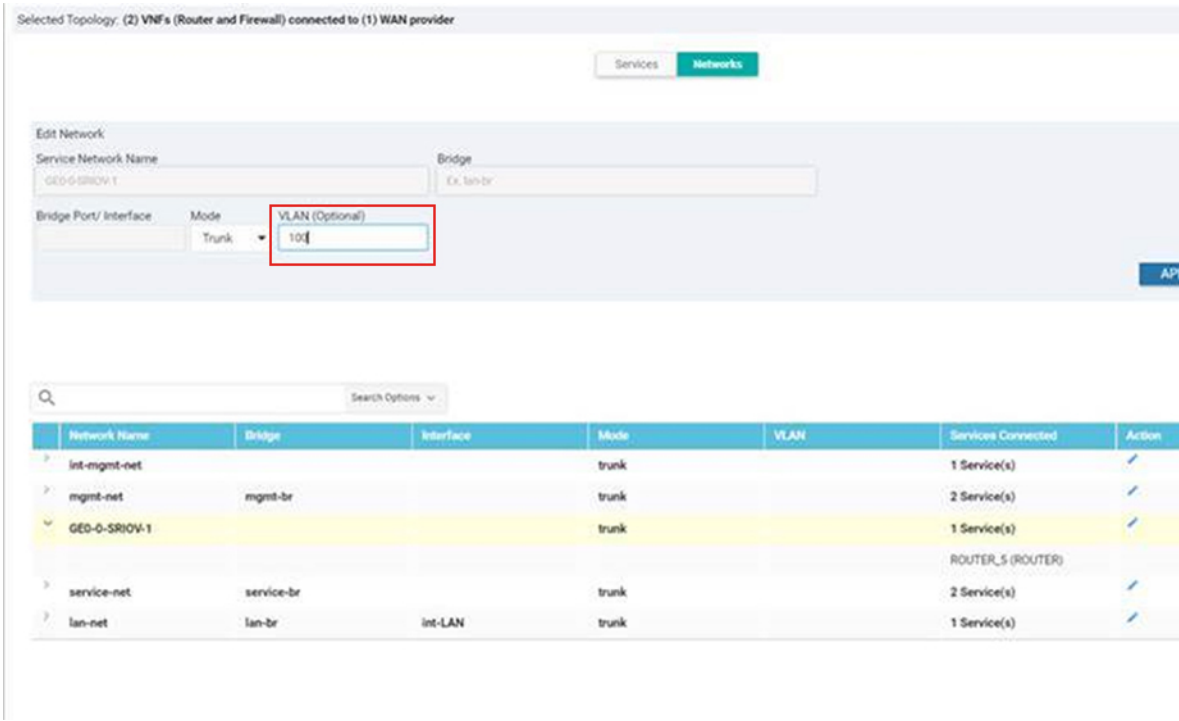
8. [Services]ページで、新しいインターフェイスと変更されたインターフェイスを確認できます。



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。

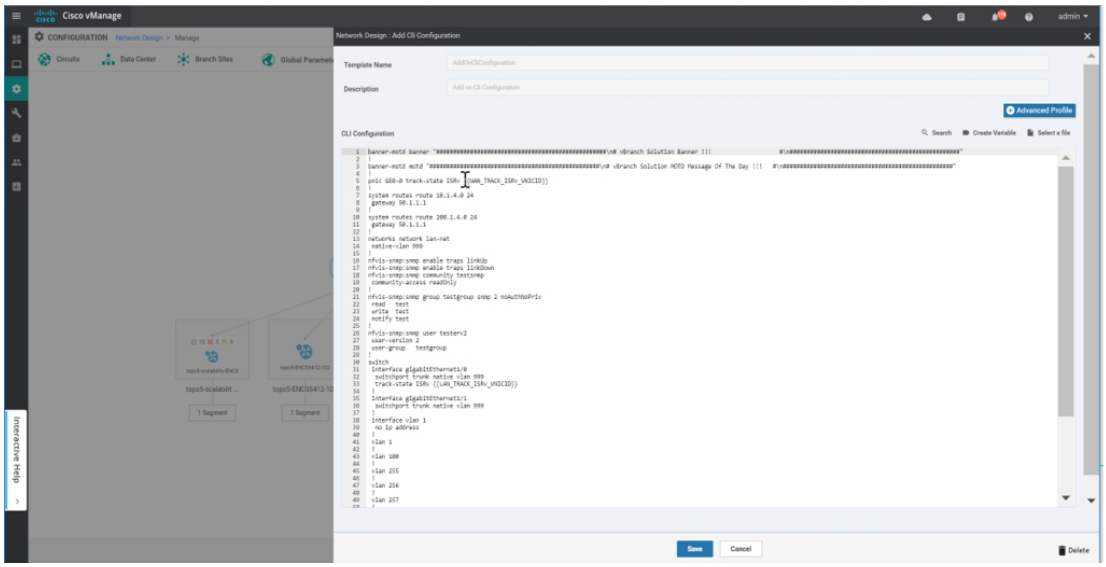
CLI アドオン機能テンプレート

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 *2*：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
```