



Managed SD-WAN
ユーザ設定マニュアル
(コントローラ設定編)
Ver 2.2

目次

1 Managed SD-WAN の事前知識	8
1.1. はじめに	8
1.1.1. 用語集	9
1.1.2. 注意事項	10
1.1.3. Managed SD-WAN の設定に関する主な流れ	11
2 コントローラ接続までの手順/基本操作	13
2.1. 多要素認証	13
2.2. コントローラ認証	14
2.3. コントローラ画面について	14
2.4. CPE 正常性確認方法	15
2.4.1. コントローラとの接続状態確認	15
2.4.2. CPE の接続状態確認	16
3 バックアップ取得方法と戻し方	17
3.1. Device Template/Feature Template のコピー	17
3.2. Policy のコピー	18
3.3. バックアップ取得方法	20
3.4. バックアップ復元方法	21
4 設定手順	25
4.1. パラメータ変更	25
4.1.1. デバイス一覧画面から対象の CPE を選択	26
4.1.2. パラメータの編集画面を表示	26
4.1.3. パラメータの編集	26
4.1.4. 適用するコンフィグの最終確認	27
4.1.5. CPE にパラメータ変更を行ったコンフィグの適用を実施	27
4.2. VPN グループ数の変更	28

4.2.1.	NW 構成例	28
4.2.2.	追加する VPN 用の Feature Template を作成	29
4.2.3.	追加する VPN グループに紐づける SVI の Feature Template を作成.....	30
4.2.4.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	31
4.2.5.	Device Template に追加 VPN グループ用の Feature Template をアタッチ.....	32
4.2.6.	作成した Device Template を CPE にアタッチ	34
4.3.	スタティックルートの設定	37
4.3.1.	NW 構成例	37
4.3.2.	スタティックルート用 Feature Template を作成	38
4.3.3.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	41
4.3.4.	Device Template にスタティックルート用の Feature Template をアタッチ	42
4.3.5.	作成した Device Template を CPE にアタッチ	44
4.4.	DHCP サーバの設定	47
4.4.1.	NW 構成例	47
4.4.2.	DHCP サーバ用 Feature Template を作成	48
4.4.3.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	49
4.4.4.	Device Template に DHCP サーバ用の Feature Template をアタッチ.....	50
4.4.5.	作成した Device Template を CPE にアタッチ	51
4.5.	DHCP リレーの設定	54
4.5.1.	NW 構成例	54
4.5.2.	DHCP リレー用の Feature Template を作成	55
4.5.3.	DHCP リレー用の Device Template を作成	57
4.5.4.	DHCP リレー用の Device Template を作成	58

4.5.5.	DHCP リレー用の Device Template をアタッチ	60
4.6.	DNS リレーの設定.....	63
4.6.1.	NW 構成例.....	63
4.6.2.	DNS リレー用 Feature Template を作成.....	64
4.6.3.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	66
4.6.4.	Device Template に DNS サーバ用の Feature Template をアタッチ	66
4.6.5.	作成した Device Template を CPE にアタッチ	67
4.7.	インターネットブレイクアウト (全てのインターネット通信を対象).....	70
4.7.1.	NW 構成例.....	70
4.7.2.	WAN インターフェース用 Feature Template を作成.....	73
4.7.3.	PPPoE 用 Feature Template を作成.....	76
4.7.4.	インターネットブレイクアウト用コマンド Feature Template を作成	77
4.7.5.	インターネットブレイクアウト用セキュリティポリシーを作成	80
4.7.6.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	87
4.7.7.	Device Template にインターネットブレイクアウト用の Feature Template をア タッチ	88
4.7.8.	作成した Device Template を CPE にアタッチ	89
4.7.9.	インターネットブレイクアウト用通信ポリシーを作成.....	92
4.7.10.	LBO 接続制限設定	102
4.7.11.	ポリシーの有効化.....	109
4.8.	インターネットブレイクアウト (アプリ指定).....	111
4.8.1.	NW 構成例.....	111
4.8.2.	インターネットブレイクアウト(アプリ指定)の留意点.....	114
4.8.3.	インターネットブレイクアウト用通信ポリシーを作成.....	115

4.8.4.	LBO 接続制限設定	128
4.8.5.	ポリシーの有効化	136
4.8.6.	プロキシサーバ利用時の留意点	138
4.8.7.	アプリ指定インターネットブレイクアウトの確認方法	140
4.9.	インターネットブレイクアウト設定の解除方法	142
4.9.1.	①ポリシーにインターネットブレイクアウト以外の設定が入っている場合の解除 方法(detach)	142
4.9.2.	②ポリシーにインターネットブレイクアウトのみが入っている場合の解除方法 (deactivate)	145
4.10.	VLAN の分割	147
4.10.1.	NW 構成例	147
4.10.2.	追加 VLAN 用 Feature Template を作成	148
4.10.3.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	150
4.10.4.	Device Template に追加 VLAN 用の Feature Template をアタッチ	150
4.10.5.	作成した Device Template を CPE にアタッチ	152
4.11.	パブリッククラウドのネットワークセグメント変更/追加する際の設定手順(クラウドゲー トウェイクロスコネクト利用時)	155
4.11.1.	NW 構成例	155
4.11.2.	クラウド NW の変更	156
4.12.	アクセスリスト (ACL) 追加手順	163
4.12.1.	NW 構成例	163
4.12.2.	アクセスリストの作成 (Localized Policy 作成)	164
4.12.3.	NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	167
4.12.4.	SVI Template(Sub-Template)の確認	168
4.12.5.	SVI Template(Sub-Template)のコピーと編集	169

4.12.6. Device Template を編集.....	170
4.12.7. SVI Template (Sub-template) の適用.....	170
4.12.8. アクセスリストの適用.....	171
4.12.9. 作成した Device Template を CPE にアタッチ	171
4.13. タイプ I、タイプ II で NAT セッション数を 10 万に変更する際の設定手順.....	174
4.13.1. セッション変更用の Feature テンプレートの作成.....	174
4.13.2. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備	176
4.13.3. Device Template にセッション変更用の Feature Template をアタッチ	176
4.13.4. 作成した Device Template を CPE にアタッチ	177
5 各種状態の確認方法.....	180
5.1. 全 CPE の状態確認方法	180
5.2. CPE のインターフェース状態確認方法	181
5.3. CPE のログ確認方法	182
5.4. vManage のトラブルシューティング機能(Ping 機能).....	183
5.4.1. トラブルシューティング(Ping)利用方法.....	184
5.4.2. Troubleshooting(Traceroute)利用方法.....	187
5.4.3. (参考) CPE の SSH 接続.....	189
5.4.4. Tools の非推奨事項.....	194
5.5. CPE 故障通知サービス通知先アドレス確認方法	195
5.5.1. 通知先メールアドレスの確認方法	195
5.5.2. 検知したアラームログの確認方法	200
6 禁止事項.....	203
6.1. NTT 東日本デフォルト提供のテンプレート/パラメータに関わる禁止事項.....	203
6.2. NTT 西日本エリアに CPE がある/モバイル接続サービス利用時の禁止事項.....	204
6.3. モバイル接続サービス利用時の禁止事項.....	205

6.4. SSH Terminal 利用のための ID/PW 変更時の禁止事項.....	206
6.5. Device Template の禁止事項.....	207
6.6. Cli Add-On Template の禁止事項	208
6.7. Device Template の禁止事項.....	209
6.8. CPE 初期化に関する禁止事項	209
7 困ったときは?.....	210
7.1. 「Out of Sync」状態の解消方法	210
7.2. テンプレートアタッチ時に DNS アドレスが Invalid となる事象の解消方法.....	213
7.3. SSH 接続時のログイン ID/パスワード不明時の対応.....	216
7.4. FAQ	220
参考資料	221
テンプレートに設定するパラメーター一覧表.....	221
CPE 下部端末の最適な MTU 値について	222

改版履歴

版数	改定日	主な改訂内容	備考
第 1.0 版	2021 年 3 月 25 日	・初版制定	
第 1.1 版	2021 年 4 月 30 日	・DHCP リレー設定手順追加 ・インターネットブレイクアウト設定解除手順追加	
第 1.2 版	2021 年 7 月 20 日	・トラブルシューティング機能（Ping 機能）の利用方法追加	
第 1.3 版	2021 年 7 月 30 日	・CPE 故障通知サービスの確認方法追加	
第 1.4 版	2021 年 10 月 29 日	・ハイエンドタイプ提供に伴う記載変更	
第 1.5 版	2022 年 1 月 19 日	・コントローラアップデートに伴う画像差し替え	
第 1.6 版	2022 年 2 月 9 日	・LBO 接続制限設定手順の追加のため、以下を編集 1.1.3.「Managed SD-WAN の設定に関する主な流れ」 →LBO 接続制限の設定のイメージを追加で記載 4.7.1.「NW 構成例」 →【設定の流れ】に LBO 接続制限の設定のイメージを追加 4.7.9.「インターネットブレイクアウト用通信ポリシーを作成」 →手順 32 を追記	

		4.7.10.「LBO 接続制限設定」 →項目として新規作成 4.8.1.「NW 構成例」 →【設定の流れ】に LBO 接続制限の設定のイメージを追加で記載 4.8.3.「インターネットブレイクアウト用通信ポリシーを作成」 →手順 32 を追記 →手順 33 に(留意事項)を追記 4.8.4.「LBO 接続制限設定」を項目として新規作成	
第 1.7 版	2022 年 3 月 11 日	p.27、p.36、p.54、p.55、p.65、p.74、p.77、p.78、 p.147 記述追記 ⇒※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」に チェック	
第 1.8 版	2022 年 4 月 27 日	CPE 故障通知のアラート名変更	
第 1.9 版	2022 年 6 月 29 日	4.11 章にセキュアインターネット接続サービスとインターネットブレイクアウトを重畳利用する場合、クロスコネクタ接続とインターネットブレイクアウトを重畳利用する場合の注意事項を記載	
第 2.0 版	2023 年 3 月	4.12 章に NAT10 万セッションへの拡大方法記載および表記誤り修正	
第 2.1 版	2023 年 12 月	コントローラアップデートに伴う画像差し替え	
第 2.2 版	2025 年 1 月	4.12 アクセスリスト (ACL) 追加手順を追記	

1

Managed SD-WAN の事前知識

本マニュアルは Managed SD-WAN においてお客様自身でコントローラの設定を行うためのものです。お客様自身の設定作業により、正常に通信が出来なくなった場合、NTT 東日本でサポートできることとして申込時の設定に戻す事となりますのでご注意ください。

お客様による設定後に正常な通信ができなくなった場合、正常な通信ができていた時点へ戻すため、お客様自身で設定をされる前に、**必ずバックアップを保存（3 章参照）** していただきますようお願いいたします。また、**必ず禁止事項をご確認（6 章参照）** いただけますようお願いいたします。以降、Managed SD-WAN の設定に関する事前知識を説明いたします

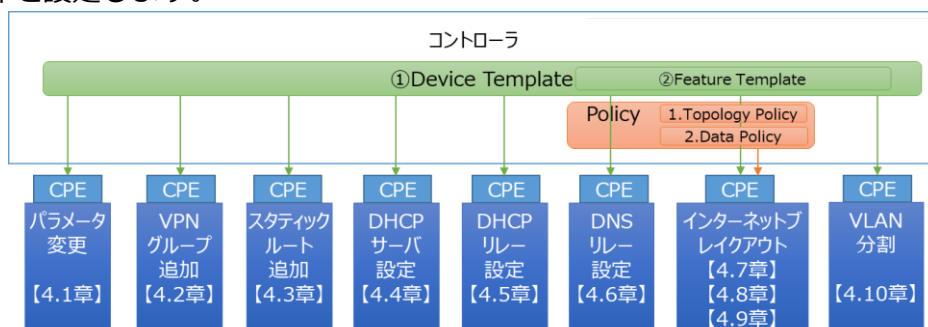
1.1. はじめに

Managed SD-WAN では GUI ベースで設定いただきます。（お客様による CLI ベースでの設定は NTT 東日本によるサポートの範囲外とさせていただきます。）

CPE の設定に必要なテンプレートは①Device Template、②Feature Template の 2 つがあります。①Device Template は CPE の設定を行うためのテンプレートで、機能毎の設定を行う②Feature Template を組み合わせて構成されています。

ポリシーは、条件の設定やアクションの適用先をリストで指定します。

- 1.Topology Policy : CPE 間のトンネルの有無、ルーティングなど、ネットワーク構成に関する条件を設定します。
- 2.Data Policy : ローカルブレイクアウトや優先制御など、条件に合致した通信に対する操作を設定します。



4.11 章 パブリッククラウドのネットワークセグメント変更/追加する際の
設定手順(クラウドゲートウェイクロスコネクト利用時)…【Policy 設定】

4.12 章 タイプ I、タイプ II で NAT セッション数を 10 万に変更する際の
設定手順…【Template 設定】

1.1.1. 用語集


本書で使用する用語の解説を下記にまとめます。

【Managed SD-WAN 全般の用語解説】

用語	解説
コントローラ	CPE への設定や状態管理（ポート閉塞、トラフィック状況など）を遠隔で行うシステム
CPE	お客様宅内に設置するルータ
vCPE	NTT 東日本ビル内に設置する仮想ルータ。NTT 東日本以外のネットワーク（NTT 西日本、モバイル事業者）との接続を行う場合に経由する。
VPN グループ	仮想ルータ(VRF)機能を指します。CPE では最大 4 つまで設定可能となります。

【設定に関する基本用語の解説】

用語	解説
Device Template	<p>コンフィグの雛形です。</p> <p>Device Template を CPE にアタッチすることにより CPE にコンフィグが適用されます。</p> <p>CPE 共通のパラメータは固定(global)で設定しておくことが可能です。</p> <p>CPE 固有のパラメータは変数(device specific)としておき、アタッチ時に入力します。</p>
Feature Template	<p>Device Template を構成するパーツです。</p> <p>複数の Feature Template を組み合わせることで Device Template が完成します。</p> <p>例えば Ethernet 用の Feature Template があり、様々な種類があります。</p>
Policy	トポロジやローカルブレイクアウトなどの WAN 側に関わる通信のルールです。

用語	アイコン	解説
Global		<p>Feature Template に固定で埋め込まれる値となります。</p> <p>CPE 共通のパラメータは Global で設定します。</p>
Device Specific		<p>Feature Template に変数として設定される値となります。</p> <p>各 CPE で固有のパラメータは Device Specific で設定します。</p>
Default		<p>Managed SD-WAN のデフォルトで設定されている値となります。</p> <p>必要に応じて Global/Device Specific に変更します。</p>

1.1.2. 注意事項

- ① 開通時に NTT 東日本よりデフォルトの Device Template、Feature Template および Policy が提供されますので、絶対に削除や設定変更を行わないようお願いいたします。
- ② Device Template/Feature Template/Policy の設定変更をする場合は NTT 東日本より提供するデフォルトのテンプレート/ポリシーをコピーし、コピーしたテンプレート/ポリシー上で設定変更を行うようお願いいたします。

※デフォルトのテンプレート/ポリシーについてはネットワーク初期構築の際に、NTT 東日本のアカウント「sd-wan-order-ml/Provider-sdwan-order-ml(※ Device Template/Feature Template/Policy の一覧の Updated By 列から参照できる)」により作成されたテンプレート/ポリシーが該当します。

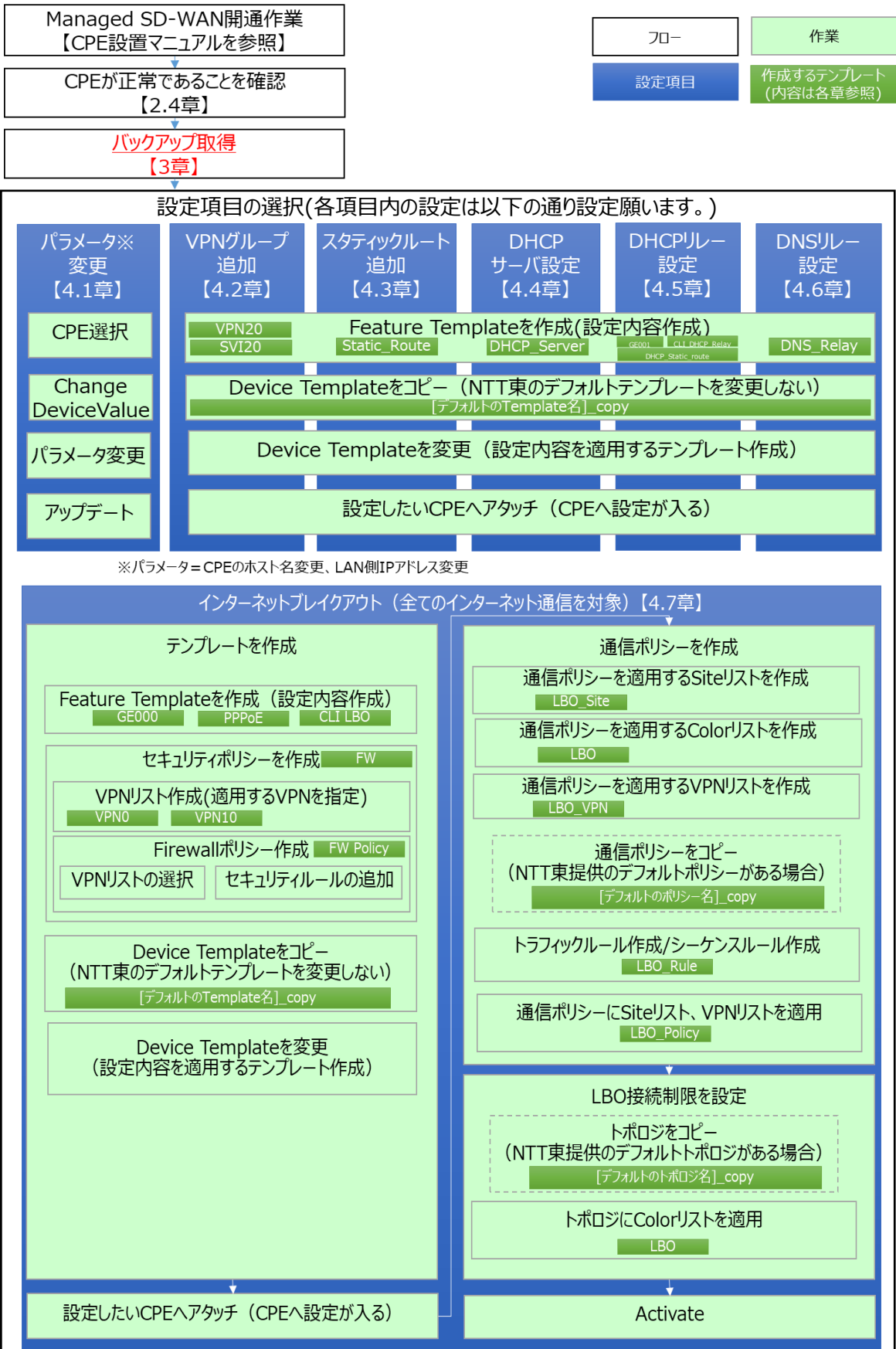
- ③ CPE のパラメータの中には NTT 東日本デフォルトの値から変更すると正常な通信ができなくなるパラメータがございます。Color/Device group/System IP/Site ID の値は絶対に変更しないようお願いいたします。
- ④ NTT 西日本エリアに拠点がある場合もしくはモバイル接続サービスを利用している場合、正常に通信出来なくなる恐れがあるため、お客様でトンネリングプロトコル/VPN グループの追加に関わる設定変更を行わないようお願いいたします。
- ⑤ セキュリティ上、コントローラログイン後にコントローラ無操作状態が 60 分継続すると強制ログアウトします。
- ⑥ 速度低下の原因となるため CPE 下部のお客様端末には最適な MTU 値の設定をお願いいたします。
- ⑦ **コントローラ画面は全て英語表記となります。日本語表記にしたい場合はブラウザの翻訳機能をご利用ください。**

※禁止事項の詳細については 6 章を参照願います。

※最適な MTU 値の詳細は末尾(参考)を参照願います。

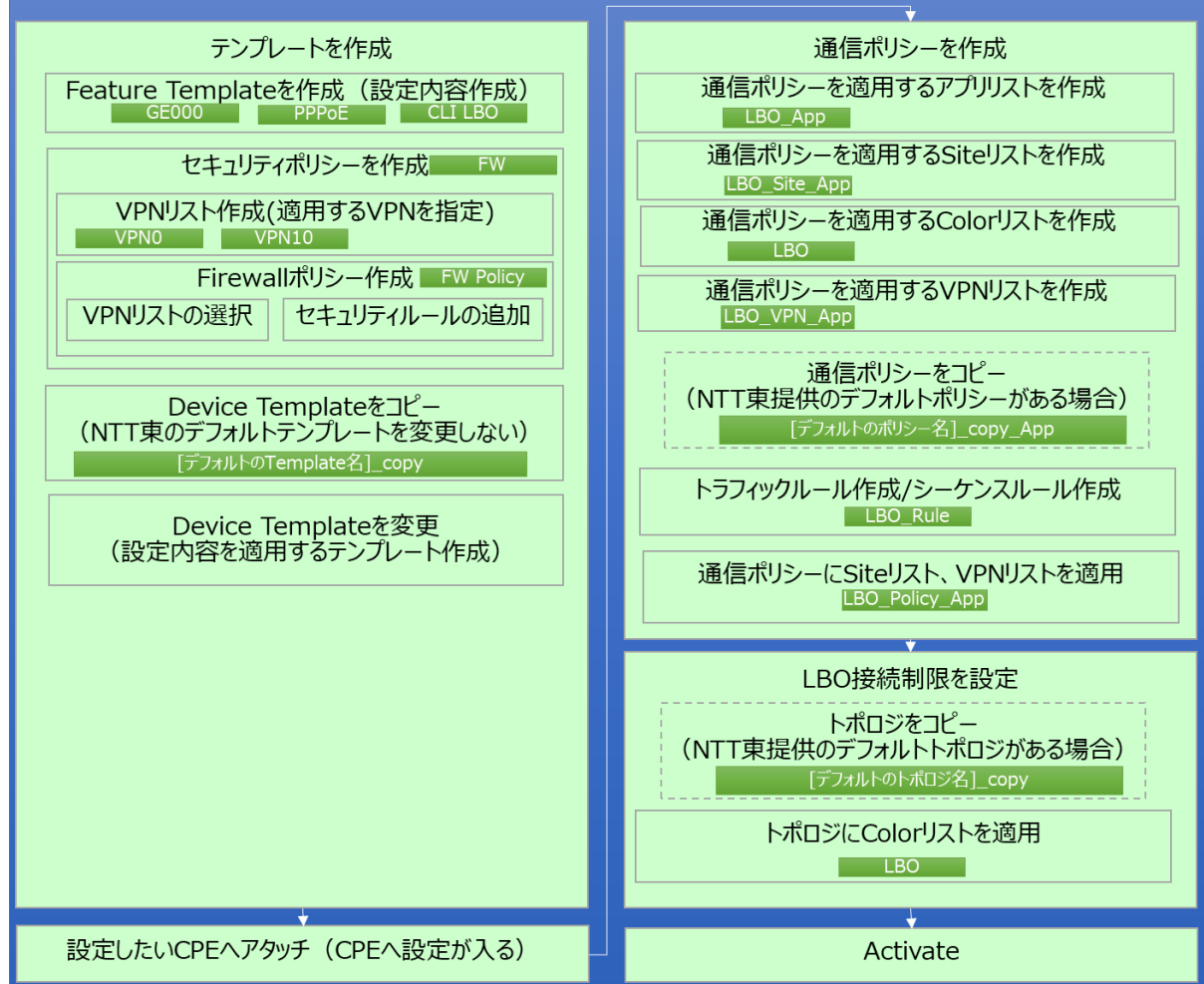
1.1.3. Managed SD-WAN の設定に関する主な流れ

Managed SD-WAN の設定に関する主な流れを説明いたします

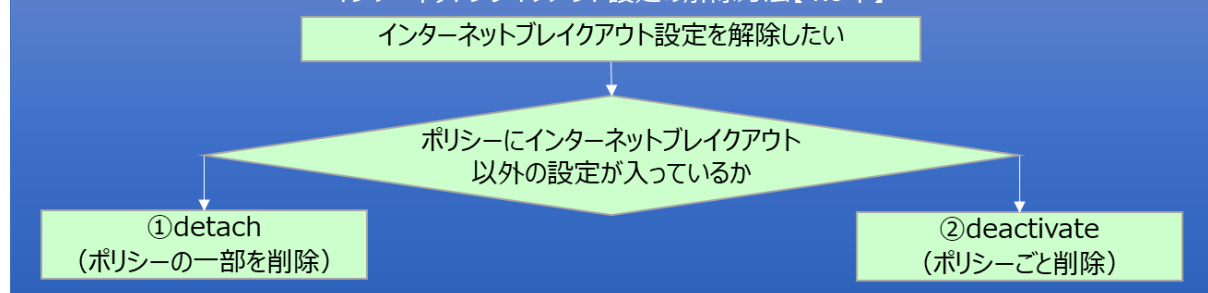


設定項目の選択(各項目内の設定は以下の通り設定願います。)

インターネットブレイクアウト（アプリケーション指定）【4.8章】



インターネットブレイクアウト設定の解除方法【4.9章】



VLAN分割 【4.10章】



4.11 章 パブリッククラウドのネットワークセグメント変更/追加する際の設定手順(クラウドゲートウェイクロスコネクタ利用時)
…【Policy 設定】

4.12 章 タイプ I、タイプ II で NAT セッション数を 10 万に変更する際の設定手順
…【Template 設定】

2

コントローラ接続までの手順/基本操作

本章では、コントローラ接続までの手順/基本操作について解説します。

2.1. 多要素認証

「開通のご案内」に記載してある URL へアクセスし、ユーザー名/パスワードを入力後ワンタイムパスワードを入力

手順1



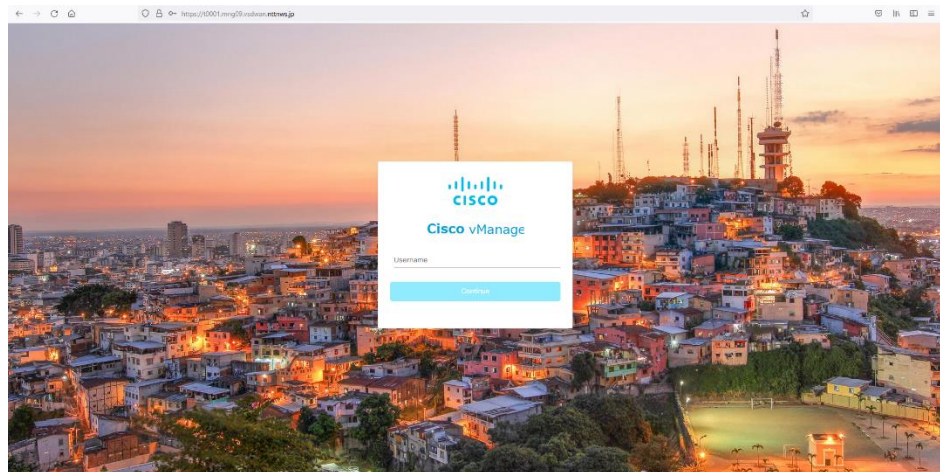
手順2



- ※ 推奨ブラウザは「Google Chrome」、「Mozilla Firefox」となります。
推奨ブラウザ以外では正常にアクセスできない可能性があります。
- ※ユーザー名/パスワードはお客さまから申込書に記載頂いた情報となります。
- ※ワンタイムパスワードはユーザー名/パスワードを入力し、ログインボタンを押した後、申込書に記載頂いたメールアドレス宛に送付されます。
- ※ワンタイムパスワードは「sdwan.ntt-east.net」から送信されますので、ドメイン指定受信を設定している方は受信可能の設定を行ってください。
- ※多要素認証のワンタイムパスワード送付先メールアドレスが「@以降含め 32 文字以上」で設定されている場合、【多要素認証】の入力画面のユーザーID は@以降の入力が不要となります。

2.2. コントローラ認証

コントローラログイン画面にてログイン ID/PW を入力
 ※ログイン ID/PW は申込書に記載頂いた情報となります



2.3. コントローラ画面について

コントローラにログインすると以下のメインダッシュボード画面が表示されます
 ・主な画面表示の意味を紹介します

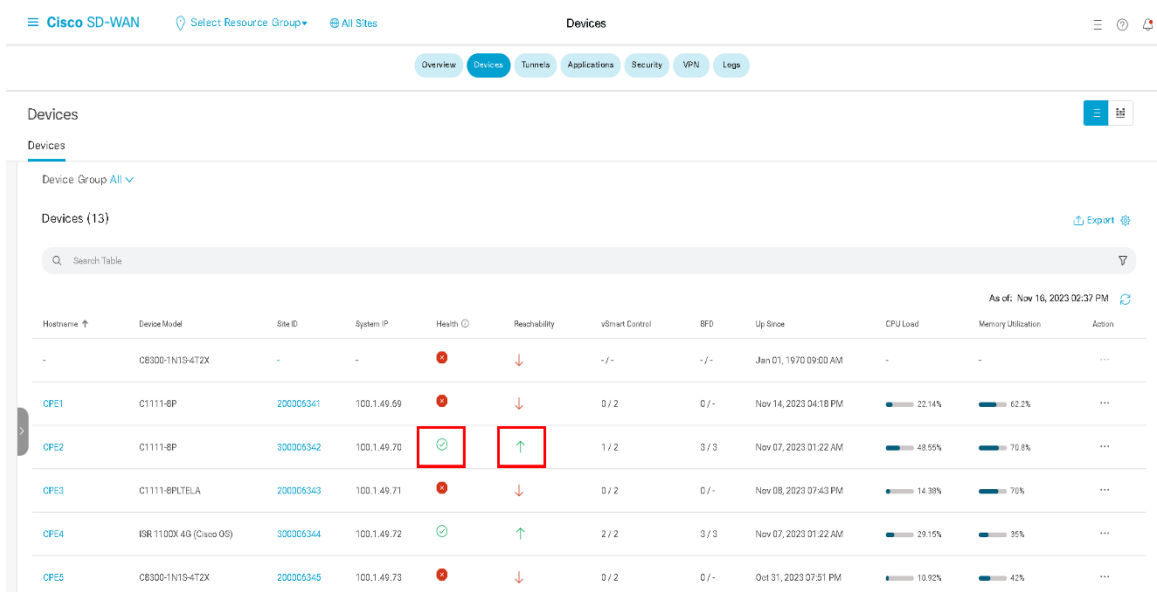


2.4. CPE 正常性確認方法

2.4.1. コントローラとの接続状態確認

左ペイン(左の領域)の「monitor」から「network」を選択し、以下の画面を表示します
確認ポイント

- ・今回接続した CPE の「State」が「緑チェック」、「Reachability」が「緑上矢印」になっていれば正常です



Hostname	Device Model	Site ID	System IP	Health	Reachability	vSmart Control	BFD	Up Since	CPU Load	Memory Utilization	Action
-	CE300-1NTS-4T2X	-	-	●	↓	- / -	- / -	Jan 01, 1970 09:00 AM	-	-	...
CPE1	C1111-8P	200005341	100.1.49.69	●	↓	0 / 2	0 / -	Nov 14, 2023 04:18 PM	22.14%	62.2%	...
CPE2	C1111-8P	300005342	100.1.49.70	●	↑	1 / 2	3 / 3	Nov 07, 2023 01:22 AM	48.55%	70.8%	...
CPE3	C1111-8P-LELA	200005343	100.1.49.71	●	↓	0 / 2	0 / -	Nov 08, 2023 07:43 PM	14.38%	70%	...
CPE4	ISR 1100X 40 (Cisco OS)	300005344	100.1.49.72	●	↑	2 / 2	3 / 3	Nov 07, 2023 01:22 AM	28.15%	95%	...
CPE5	CE300-1NTS-4T2X	200005345	100.1.49.73	●	↓	0 / 2	0 / -	Oct 31, 2023 07:51 PM	10.92%	42%	...

2.4.2. CPE の接続状態確認

左ペイン(左の領域)の Configuration から Devices を選択し、以下の画面を表示します
確認ポイント

- ・今回接続した CPE の「Device Status」が「In Sync」になっていれば正常です
- ※「In Sync」とならない場合は 6.1 章を参照してください

Cisco SD-WAN
Select Resource Group
Devices
WAN Edge List

Search

Change Mode
Upload WAN Edge List
Export Bootstrap Configuration
Sync Smart Account
Add PAYG WAN Edges

Total Rows: 13

Chassis Number	Tags	Hostname	Site ID	Region ID	Mode	Device Status	Assigned Config Group	Assigned Template	Device Model	Draft Mode	Serial No./Token	R
C1111-8P-FGL2605L3Y5	Add Tag	CPE1	200006341	-	vManage	In Sync	-	C1111-8P_Default05...	C1111-8P	Disabled	C28548857670558...	u ...
C1111-8P-FGL2605L3VE	Add Tag	CPE2	300006342	-	vManage	In Sync	-	C1111-8P_Default05...	C1111-8P	Disabled	C15861759337185...	rt ...
C1111-8P-TELTA-FGL2622L2DJ	Add Tag	CPE3	200006343	-	vManage	In Sync	-	C1111-8P-TELTA_Defa...	C1111-8P-TELTA	Disabled	C748784621704746...	u ...
ISR1100X-4G-FGL2643LULB	Add Tag	CPE4	300006344	-	vManage	In Sync	-	ISR1100X-4G_DS-Ita	ISR 1100X 4G (...)	Disabled	C12618489082858...	rt ...
C8300-1N1S-4TZK-FD02630M1GQ	Add Tag	CPE5	200006345	-	vManage	Sync Pending - Devi...	-	C8300-1N1S-4TZK_D...	C8300-1N1S-4...	Disabled	C808358185113671...	u ...
C1111-8P-FGL2252114Y	Add Tag	jaki1	200000001	-	vManage	Out of Sync - Device...	-	C1111-8P_Default05...	C1111-8P	Disabled	C17950F8	rt ...

3

バックアップ取得方法と戻し方

本章では、バックアップの取得方法と戻し方を解説します。

3.1. Device Template/Feature Template のコピー

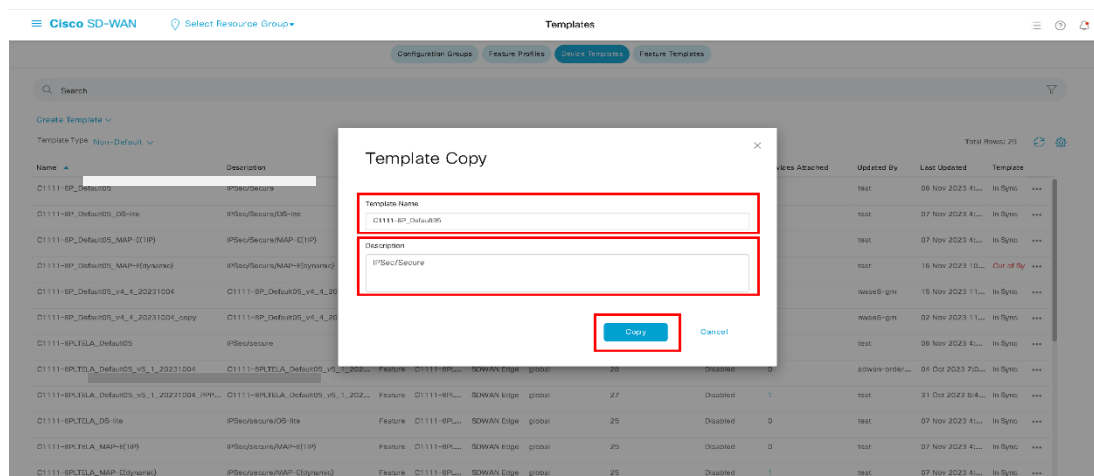
各種設定を行っていただく際に、まず Template のコピーから始めていただきます
 以下は Device Template/Feature Template のコピー手順となります

1. 左ペインの Configuration から「Templates」を選択、そこから更に「Device Templates」のタブに切り替え以下の画面を表示
2. コピーしたい Template の右端にある「…」から「Copy」を選択

The screenshot displays the Cisco SD-WAN management interface. On the left, the 'Configuration' menu is expanded, and 'Templates' is selected. The main panel shows the 'Device Templates' tab. A table lists various templates, including 'C1111-SP_Default05'. A dropdown menu is open for the first row, showing options like 'Edit', 'View', 'Delete', and 'Copy'. The 'Copy' option is highlighted with a red box.

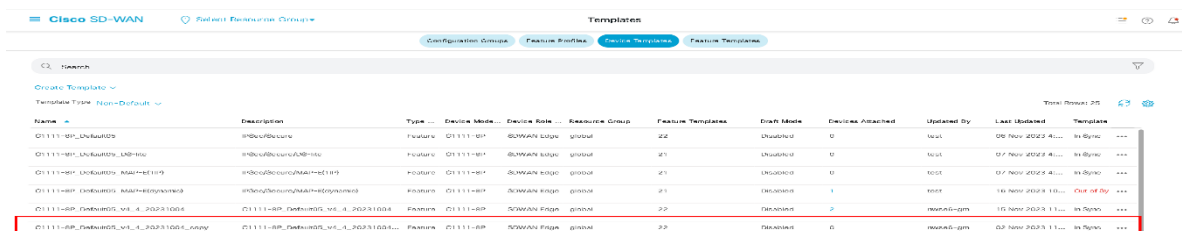
Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Li
C1111-SP_Default05	IPSec/Secure	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	0	test	...
C1111-SP_Default05_DS-ite	IPSec/Secure/DS-ite	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	0	test	...
C1111-SP_Default05_MAP-E(1P)	IPSec/Secure/MAP-E(1P)	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	1	test	...
C1111-SP_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	0	test	...
C1111-SP_Default05_v4_4_20231004	C1111-SP_Default05_v4_4_20231004	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	2	mns66	...
C1111-SP_Default05_v4_4_20231004_copy	C1111-SP_Default05_v4_4_20231004_copy	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	0	mns66-gm	...

- 新しく作成する Template に「Template Name」※および「Description」※を入力し、「Copy」を選択



※Template Name/Descriptionは「[コピー元のテンプレート名+yyyyymmdd]」

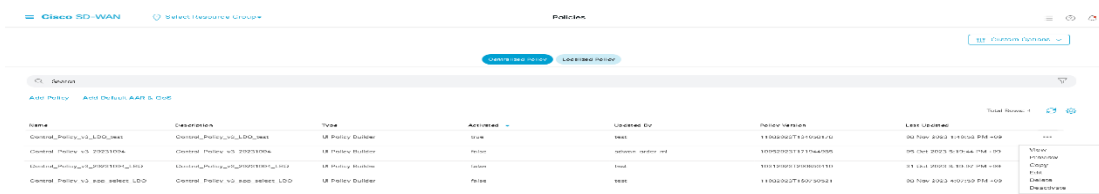
新しい Template が作成されていることを確認



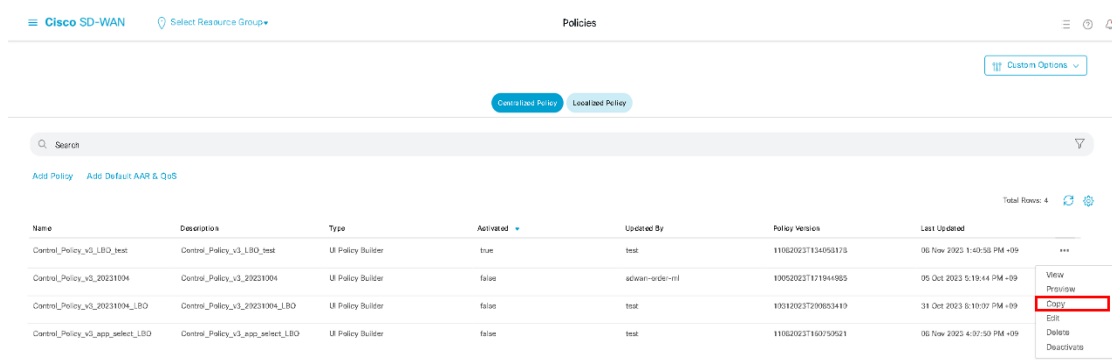
3.2. Policy のコピー

以下は Policy のコピー手順となります。

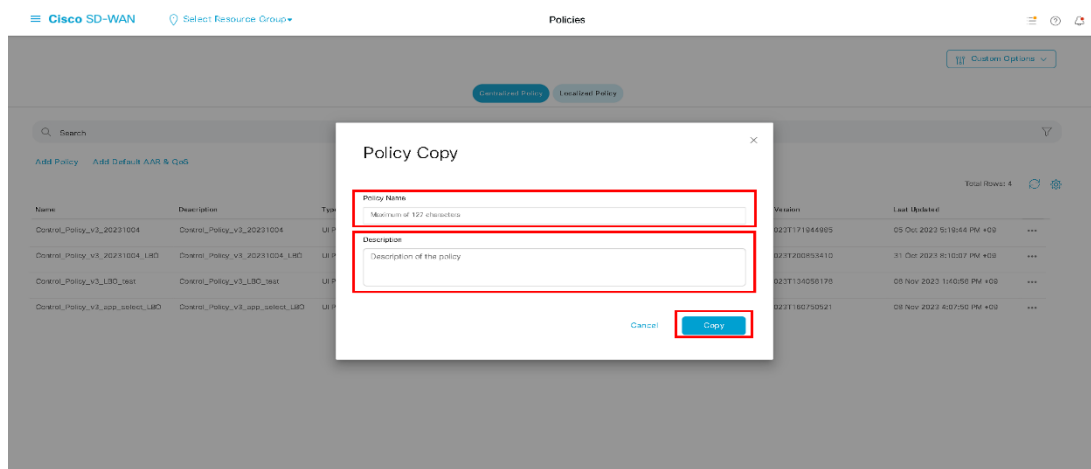
- 左ペイン(左の領域)の Configuration から「Policies」を選択し以下の画面を表示



- コピーしたい Policy の右端にある「…」から「Copy」を選択

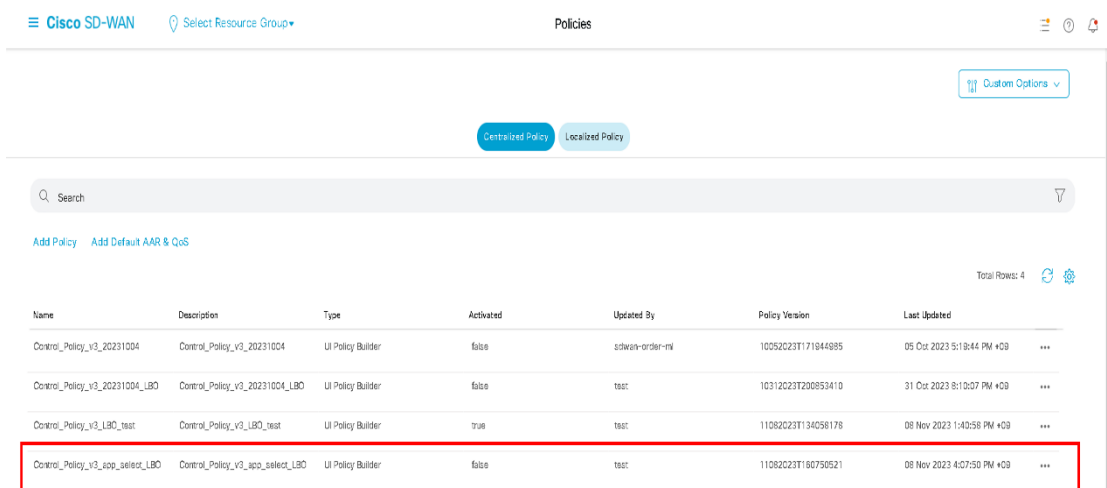


- 新しく作成する Policy に「Policy Name」および「Description」を入力し、「Copy」を選択



※Policy Name/Descriptionは「[コピー元のポリシー名+yyyymmdd]」

- 新しい Policy が作成されていることを確認



Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	sdwan-order-nl	10052023T171944985	05 Oct 2023 5:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	1031023T200853410	31 Oct 2023 8:10:07 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	true	test	11062023T134058178	08 Nov 2023 1:40:58 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	false	test	11062023T180750521	08 Nov 2023 4:07:50 PM +09

3.3. バックアップ取得方法

お客様自身で設定により正常な通信ができなくなった場合、正常な通信ができていた時点の状況に復旧するために、設定を行う前に必ずバックアップを取得願います。以下はデバイステンプレート/パラメータのバックアップ取得方法です

1. 左ペイン(左の領域)の Configuration から「Templates」を選択。

Device Template を「…」から「Copy」を選択し Template Name/Description※を入力し「Copy」を選択。 ※Template Name/Description の名前は「[コピー元のテンプレート名]_copy_yymmdd」

→新しい Template が作成されているか確認

Device Template の「…」から「Export CSV」を選択し、パラメータのバックアップ※を実施。

→作業中の PC の「ダウンロード」フォルダに作成されることを確認

※バックアップファイルの名前は「sdwan_backup_yymmdd」
yymmdd : 2034 年 5 月 16 日の場合 340516

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	La
C1111-8P_Default05	IPSec/Secure	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	test	OK
C1111-8P_Default05_DS-lite	IPSec/Secure/DS-lite	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test	
C1111-8P_Default05_MAP-E(1P)	IPSec/Secure/MAP-E(1P)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	1	test	
C1111-8P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test	
C1111-8P_Default05_v4_4_20231004	C1111-8P_Default05_v4_4_20231004	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	2	mesa	
C1111-8P_Default05_v4_4_20231004_copy	C1111-8P_Default05_v4_4_20231004_c...	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	mesa	

2. 左ペイン(左の領域)の Configuration から「Policies」を選択。Policy を「…」から「Copy」を選択し、ポリシーのバックアップを実施。

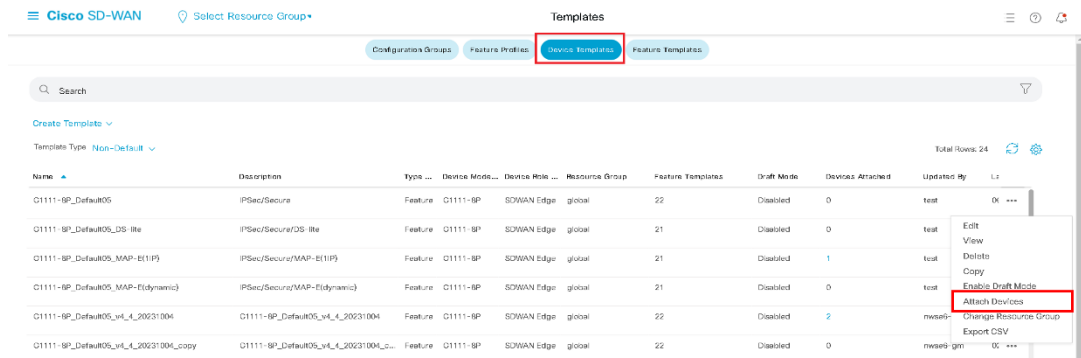
→Policy Name/Description※を入力し「Copy」を選択

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_LBQ_test	Control_Policy_v3_LBQ_test	UI Policy Builder	true	test	110620221134193173	06 Nov 2023 1:40:56 PM +09
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	sdwan-order-m	10092022111944965	05 Dec 2023 1:19:44 PM +09
Control_Policy_v3_20231004_LBQ	Control_Policy_v3_20231004_LBQ	UI Policy Builder	false	test	100920231209050449	31 Dec 2023 8:19:07 PM +09
Control_Policy_v3_jap_select_LBQ	Control_Policy_v3_jap_select_LBQ	UI Policy Builder	false	test	110620221140759521	06 Nov 2023 4:37:59 PM +09

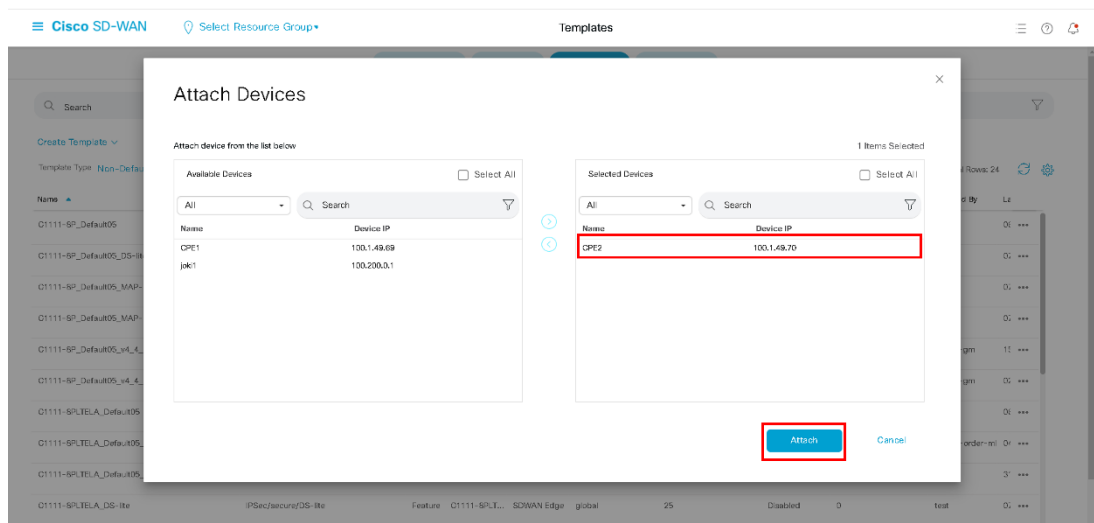
3.4. バックアップ復元方法

以下はデバイステンプレート/パラメータのバックアップデータ復元方法です。

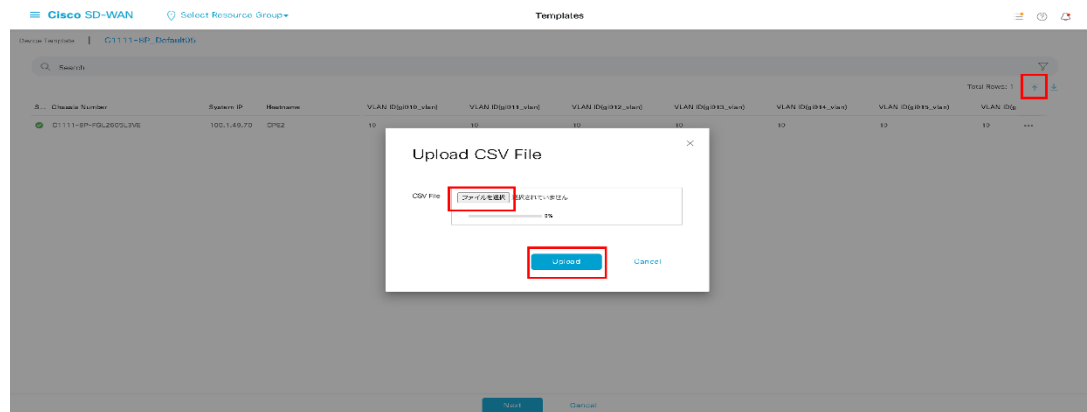
1. 左ペイン(左の領域)の Configuration から「Templates」⇒「Device Templates」を選択。
2.1 章で作成したバックアップテンプレートの「…」から「Attach Devices」を選択。



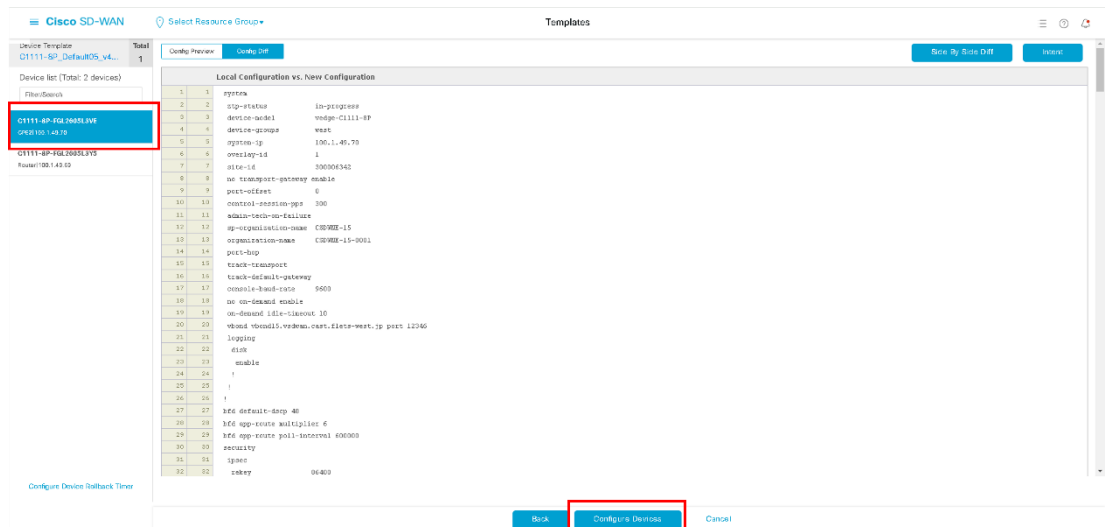
2. 適用したい CPE を選択し, 「→」を選択し右ボックスに移動。
「Attach」を選択。



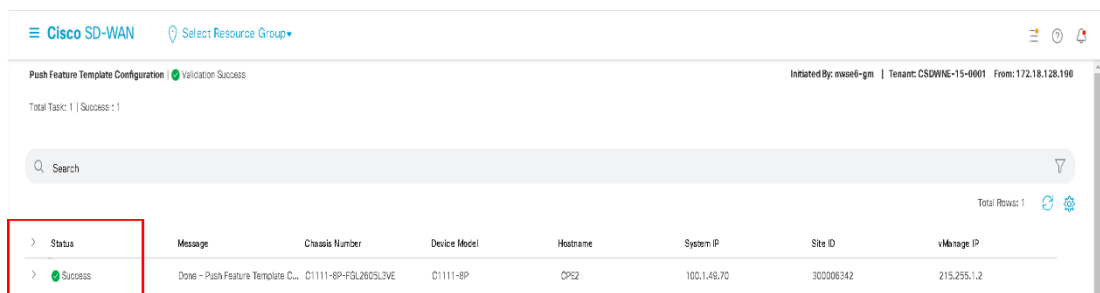
3. 右上の「↑」ボタンを選択。
2.1 章で取得した csv ファイルをアップロード
⇒作業用 PC の「ダウンロードフォルダ」から該当の csv ファイルを選択し「開く」を選択
「Upload」を選択。
元の画面に戻った後に「Next」を選択。



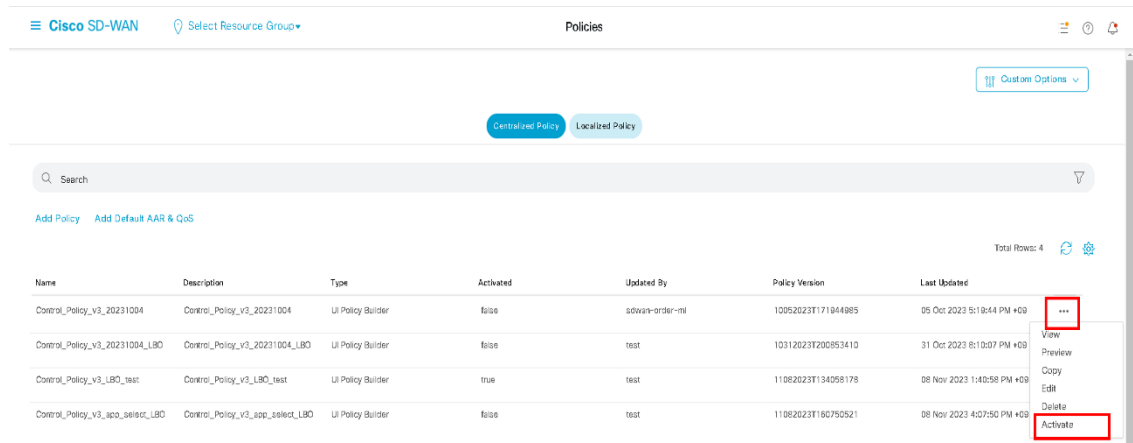
4. 以下の画面で CPE を選択し、コンフィグを出力。
問題なければ「Configure Devices」を選択。



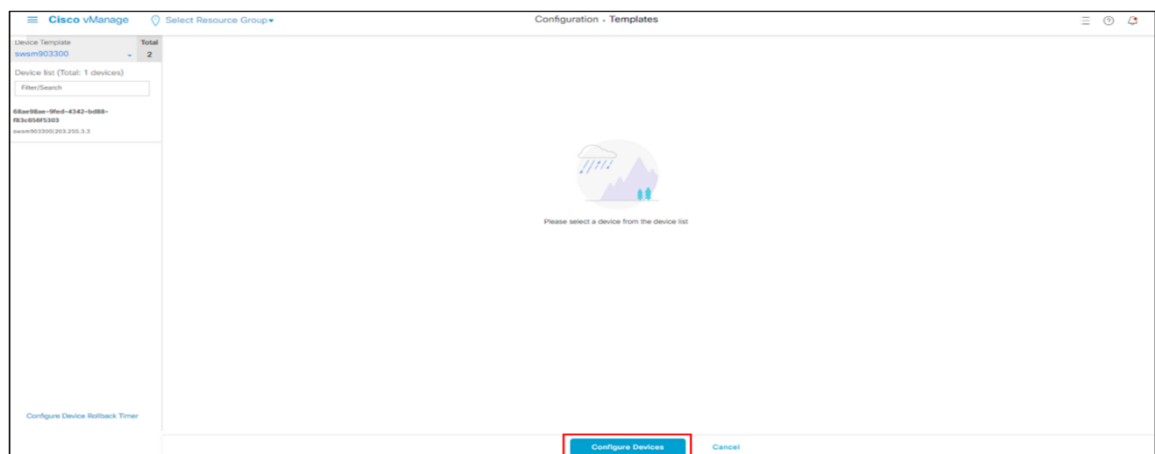
5. Status が success, Message が Done となっていればコンフィグ適用が完了。
⇒Status 変更まで 1 分程度かかります。



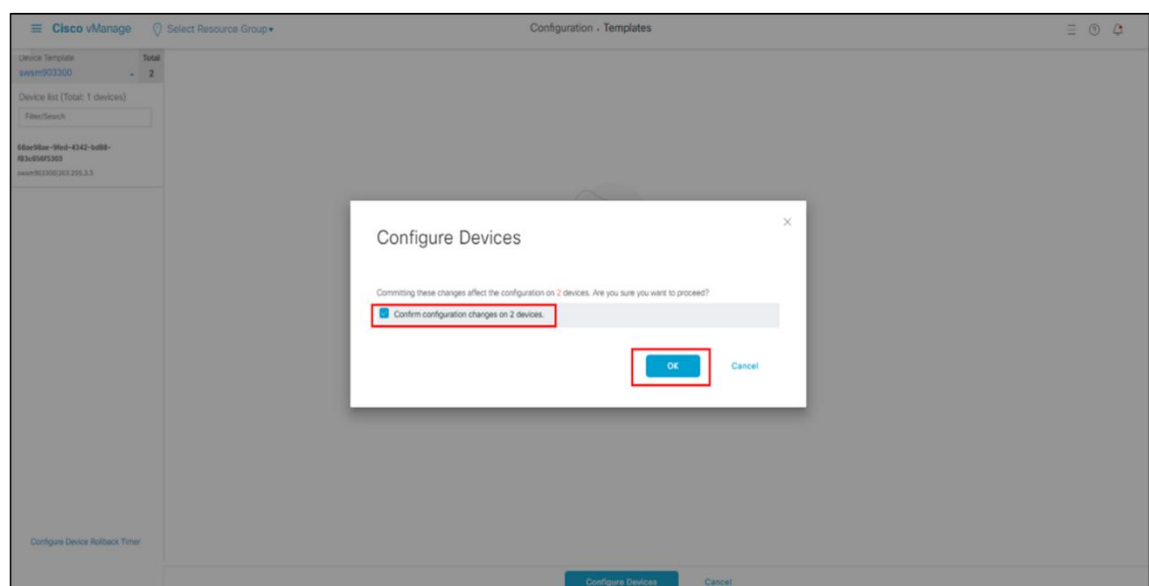
6. 左ペイン(左の領域)の Configuration から「Policy」を選択
 2.1 章で作成したバックアップポリシーの「…」から「Activate」を選択
 ⇒ポップアップ後の画面で「Activate」を選択



7. 下記画面へ遷移するので「Configure Devices」を選択



8. 下記画面へ遷移するので「Confirm Configuration changes on 2 devices」にチェックを入れ、「OK」を選択



9. Status, Message が Success となっていればコンフィグ適用が完了

Cisco SD-WAN Select Resource Group

Total Rows: 2

Status	Message	Hostname	System IP	Site ID	vManage IP
Success	Config status from device: success	swanb15010	215.255.3.1	1000000000	215.255.1.3
Success	Config status from device: success	swanb15030	215.255.3.3	1000000000	215.255.1.3

4

設定手順

本章では、Managed SD-WAN の運用を開始後に、ネットワークの構成変更などによってその設定を追加もしくは変更しなければならない場合の、具体的な操作手順を説明します。各セクションは独立していますので、必要に応じてご参照下さい。

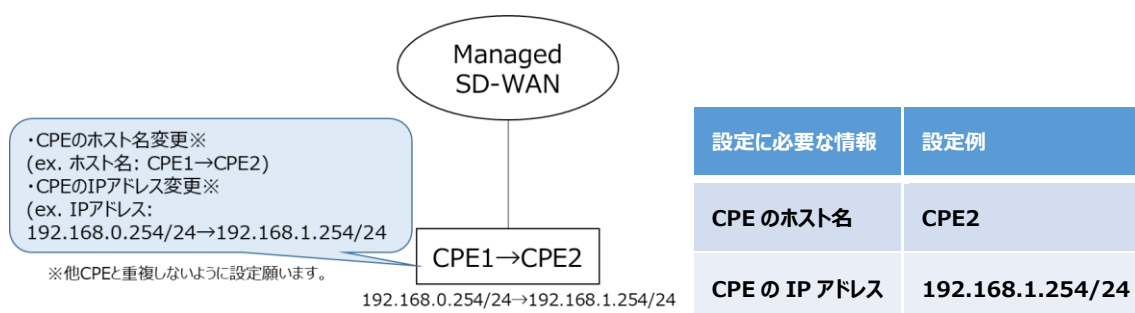
4.1. パラメータ変更

Template 内で Device Specific(CPE 固有)と設定しているパラメータの変更方法を紹介します。

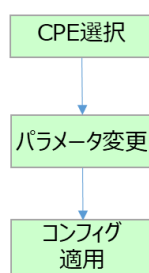
CPE に設定されているパラメータを変更する際に次ページ以降を実施します。

開通時の NTT 東日本デフォルト提供のテンプレートではホスト名/IP アドレスが変更可能なパラメータとなります

お客様にて Device Specific(CPE 毎の変数)の設定を追加している場合、本手順と同様の手順で設定変更可能となります



【設定の流れ】



4.1.1. デバイス一覧画面から対象の CPE を選択

CPE 選択

1. 左ペイン(左の領域)の Configuration から「Devices」を選択し以下の画面を表示
変更したい CPE の右端にある「…」から「Change Device value」を選択

Chassis Number	Tags	Hostname	Site ID	Region ID	Mode	Device Status	Assigned Config Group	Assigned Template	Device Model	Draft Mode	Serial No./Serial	R
C1111-8P-FGL2605.3VE	Add Tag	CPE1	200006361	-	vManage	In Sync	-	C1111-8P_Default05...	C1111-8P	Disabled	028548857678058...	...
C1111-8P-FGL2605.3VE	Add Tag	CPE2	300006362	-	vManage	In Sync	-	C1111-8P_Default05...	C1111-8P	Disabled	0	...
C1111-8P-UTLA-FGL2622.2DU	Add Tag	CPE3	200006363	-	vManage	In Sync	-	C1111-8P-UTLA_Def...	C1111-8P-UTLA	Disabled	0	...
ISR1100X-4G-FGL2643.LULU	Add Tag	CPE4	300006364	-	vManage	In Sync	-	ISR1100X-4G_05-site	ISR1100X 4G (...)	Disabled	0	...
CR300-1N1S-4T2X-FGL2630M1.BQ	Add Tag	CPE5	200006365	-	vManage	Sync Pending - Dev...	-	CR300-1N1S-4T2X_D...	CR300-1N1S-4...	Disabled	0	...

4.1.2. パラメータの編集画面を表示

パラメータ変更

2. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択

S...	Chassis Number	System IP	Hostname	VLAN ID(g0/10_vlan)	VLAN ID(g0/11_vlan)	VLAN ID(g0/12_vlan)	VLAN ID(g0/13_vlan)	VLAN ID(g0/14_vlan)	VLAN ID(g0/15_vlan)	VLAN ID(g...)
...	C1111-8P-FGL2605.3VE	100.1.1.1	CPE2	10	10	10	10	10	10	...

4.1.3. パラメータの編集

パラメータ変更

3. 以下の画面で変更したいパラメータ値を変更後に「Update」を選択し、「Next」を選択 ※開通時の NTT 東日本デフォルト提供のテンプレートで変更可能なパラメータは「IPv4 Address」および「Hostname」になります

<注意>

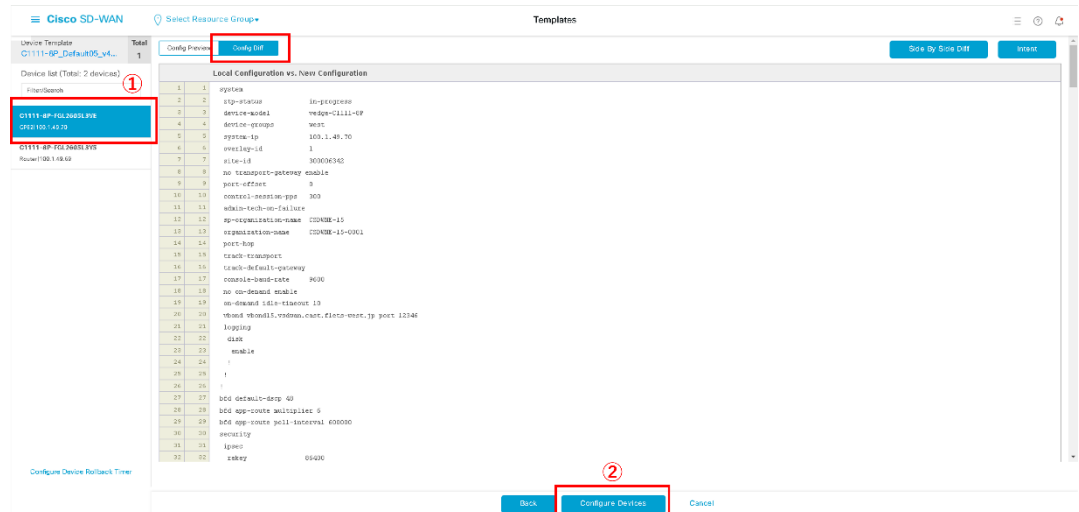
Color, Device group, System IP, Site ID はデフォルト値から変更すると通信ができなくなる恐れがあるため、変更しないようお願いいたします

4.1.4. 適用するコンフィグの最終確認

コンフィグ適用

4. ①以下の画面で該当の CPE を選択、出力されたコンフィグを確認
(「Config Diff」を選択すると差分表示が可能)
- ②内容を確認し、「Configure Devices」を選択

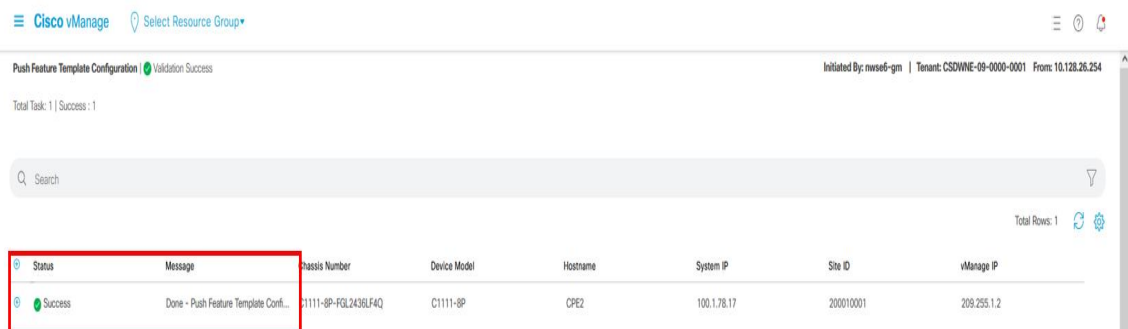
※エラーがでる場合、設定が誤っている可能性があります。エラー内容及び手順を確認願います。



4.1.5. CPE にパラメータ変更を行ったコンフィグの適用

コンフィグ適用

5. Status が success, Message が Done となっていればコンフィグ適用の完了
⇒Status 変更までに 1 分程度かかります。
- ※Status が success とならない場合、エラー内容及び手順を確認し時間を置いてリトライの実施をお願いします



4.2. VPN グループ数の変更

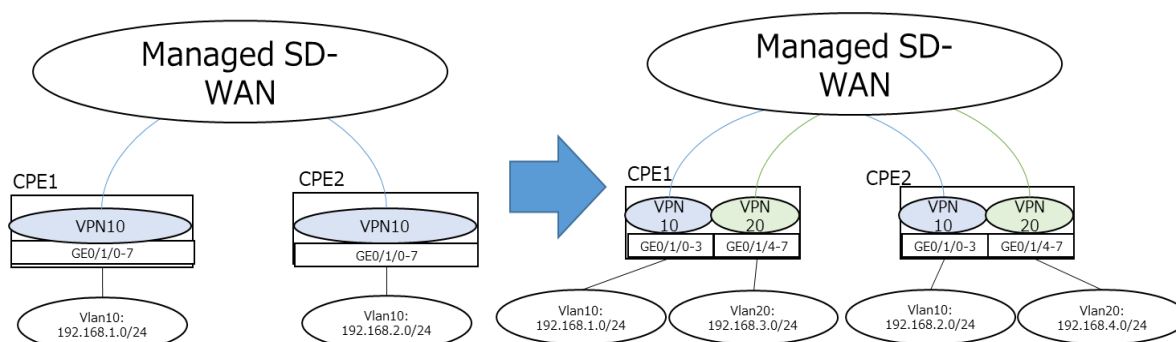
CPE に仮想ルータを設定し、論理的に分かれた NW を設定することが可能です。利用できる VPN グループ数は最大 4 つとなります。

- ・下記の図のように VPN グループを追加したい場合、次ページ以降を実施します

※VPN グループ 10 はデフォルトで設定されています

※VPN10-VPN20 間の通信は不可となります

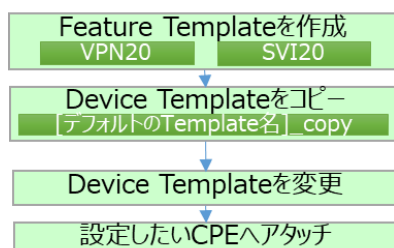
4.2.1. NW 構成例



【Device Template 作成に必要となる Feature Template】

作成する Feature Template	手順	用途
VPN20	1～3	VPN20 の作成
SVI20	4～5	VPN20 に紐づける SVI の作成

【設定の流れ】



4.2.2. 追加する VPN 用の Feature Template を作成

Feature Template を作成

VPN20

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択後に「Add Template」を選択

Name	Description	Type	Device Model	Feature Template	Resource Group	Features Attached	Updated By	Last Modified
ISR1100K-4S_203-22_VPN...	ISR1100K-4S_203-22_VPN...	Cisco VPN	ISR 1100K 4S (Cisco OS)	0	global	1	Provider-swam-order-mi	05 Oct 2023 2:33:18 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	Cisco VPN interface Ethernet	CS300-1N1S-4T2X	1	global	1	Provider-swam-order-mi	05 Oct 2023 1:30:40 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	Cisco VPN interface Ethernet	CS300-1N1S-4T2X	2	global	2	Provider-swam-order-mi	04 Oct 2023 4:12:26 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	Cisco VPN interface Ethernet	CS300-1N1S-4T2X	3	global	3	Provider-swam-order-mi	04 Oct 2023 4:15:37 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	Cisco VPN interface Ethernet	CS300-1N1S-4T2X	4	global	4	Provider-swam-order-mi	04 Oct 2023 4:17:10 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	WAN Edge Cloud Cellular W...	CS300-1N1S-4T2X	5	global	5	Provider-swam-order-mi	05 Oct 2023 1:30:10 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X	1	global	1	Provider-swam-order-mi	05 Oct 2023 1:30:40 PM +...
ISR1100K-4S_203-22_VPN...	ISR1100K-4S_203-22_VPN...	Cisco VPN	ISR 1100K 4S (Cisco OS)	0	global	1	Provider-swam-order-mi	05 Oct 2023 2:33:18 PM +...
CS300-1N1S-4T2X_203-...	CS300-1N1S-4T2X_203-...	Cellular Controller	CS300-1N1S-4T2X	2	global	2	Provider-swam-order-mi	05 Oct 2023 1:30:40 PM +...
ISR1100K-4S_203-22_VPN...	ISR1100K-4S_203-22_VPN...	Cisco VPN	ISR 1100K 4S (Cisco OS)	0	global	1	Provider-swam-order-mi	05 Oct 2023 2:33:18 PM +...
ISR1100K-4S_203-22_VPN...	ISR1100K-4S_203-22_VPN...	Cisco VPN	ISR 1100K 4S (Cisco OS)	1	global	0	Provider-swam-order-mi	05 Oct 2023 2:33:18 PM +...
ISR1100K-4S_203-22_VPN...	ISR1100K-4S_203-22_VPN...	Cisco VPN interface Ethernet	ISR 1100K 4S (Cisco OS)	0	global	1	Provider-swam-order-mi	05 Oct 2023 1:11:02 AM +...

注意

- NTT 西日本エリアに拠点がある場合、もしくはモバイル接続サービスを利用している場合は、正常な通信ができなくなる可能性がありますので、お客様にて VPN グループ変更作業実施しないようお願いいたします
- VPN グループを変更したい場合は NTT 東日本へ設定変更依頼を提出願います（有料工事）

2. Select Devices の「C1111-8P」※にチェックをいれ、「Cisco VPN」を選択
※タイプ II なら「C1111-8PLTELA」にチェック
※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック
※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック

Select Devices

- ☐ C1109-2PLTEV2
- ☐ C1109-4PLTE2P
- ☐ C1109-4PLTE2PW*
- ☐ C1111-4P
- ☐ C1111-4PLTEA
- ☐ C1111-4PLTELA
- ☐ C1111-4PW*
- ☒ C1111-8P
- ☐ C1111-8PLTEA
- ☐ C1111-8PLTEAW*
- ☐ C1111-8PLTELA
- ☐ C1111-8PLTELAJ*
- ☐ C1111-8PW*
- ☐ C1111X-8P
- ☐ C1112-8P
- ☐ C1112-8PLTEA

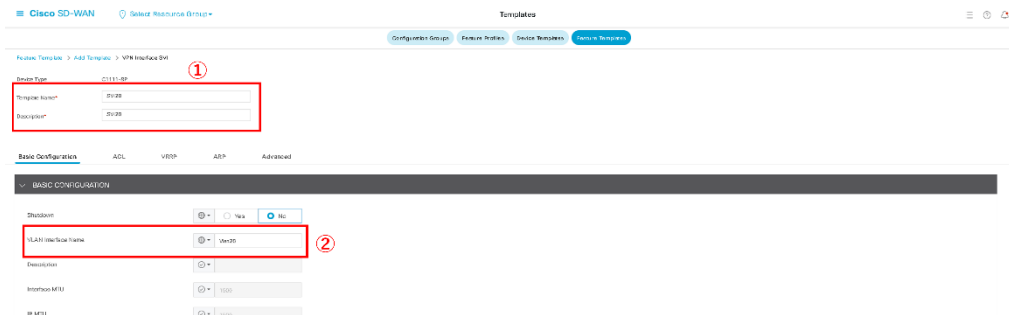
Global Settings

VPN

- Cisco Secure Internet Gateway (SIG) WAN
- Cisco VPN
- Cisco VPN interface Ethernet Management WAN LAN
- Cisco VPN interface GRE WAN
- Cisco VPN interface IPsec WAN
- VPN interface Ethernet PPPoE WAN
- VPN interface Multilink WAN LAN
- VPN interface Ssl Management WAN LAN

OTHER TEMPLATES

3. ① Template Name/Description に「VPN20」を入力（設定内容はお客様任意）
② VPN の値を Global で 20 に変更し、「SAVE」を選択

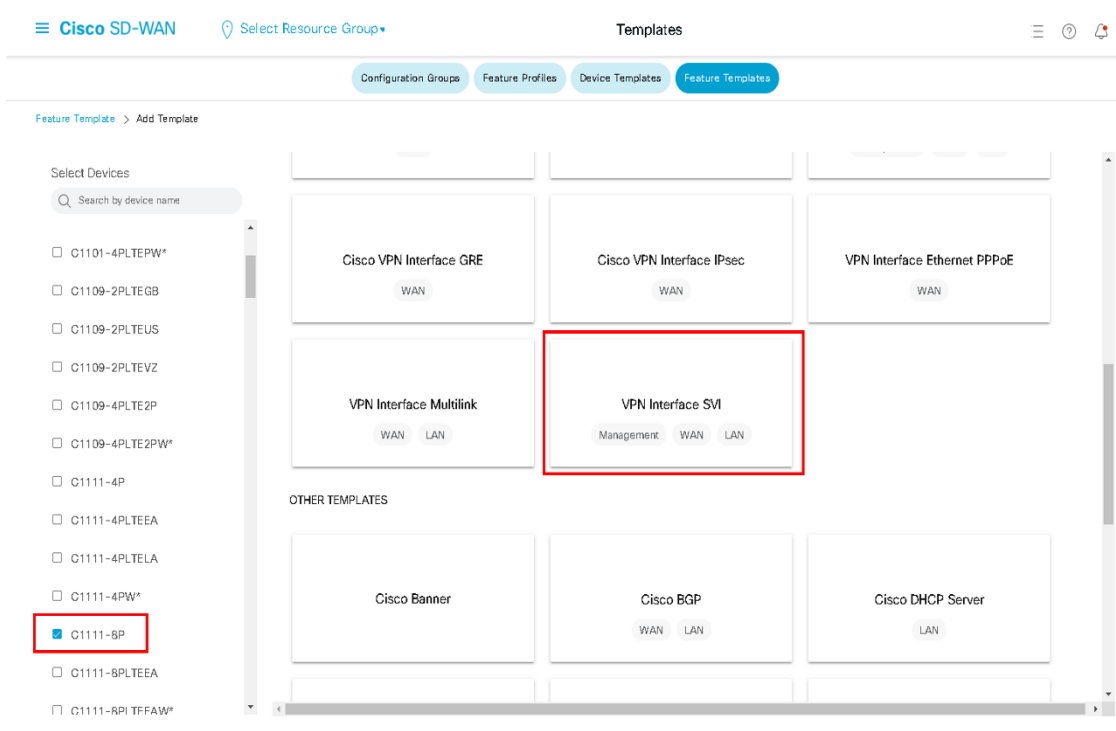


4.2.3. 追加する VPN グループに紐づける SVI の Feature Template を作成

Feature Template を作成

SVI20

4. 手順 1（「Add Template」）を実施後、Select Devices の「C1111-8P」にチェックをいれ、「VPN Interface SVI」を選択



5. ①Template Name/Description に「SVI20」を入力
- ②Shutdown を Global で「no」
- ③VLAN Interface Name を Global で「Vlan20」
- ④IPv4 Address を「device specific」と選択
- ⑤TCP MSS を「1412(GRE の場合)もしくは 1378(IPsec の場合)」に変更
- ⑥最後に「Save」を選択

4.2.4. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

Device Template をコピー

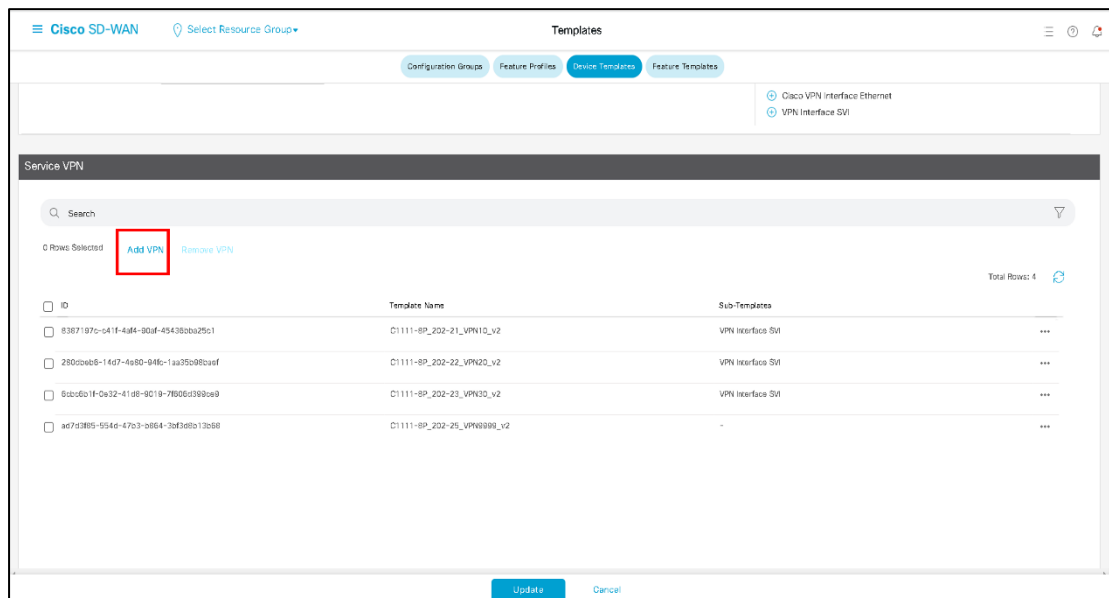
6. 左ペイン(左の領域)の Configuration から「Templates」を選択
- 画面上部のタブから「Devices Templates」を選択
- NTT 東日本デフォルトの Template をコピー※し、コピーした Template の「…」から「Edit」を選択
- ※コピーの手順については、3.1 「Device Template/Feature Template」のコピーを参照ください

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated
C1111-8P_DefaultIOS	IPSec/Secure	Feature	C1111-8P	SD-WAN Edge	global	22	Disabled	0	test	0
C1111-8P_DefaultIOS_DS-File	IPSec/Secure/DS-File	Feature	C1111-8P	SD-WAN Edge	global	21	Disabled	0	test	0
C1111-8P_DefaultIOS_MAP-E(1P)	IPSec/Secure/MAP-E(1P)	Feature	C1111-8P	SD-WAN Edge	global	21	Disabled	1	test	0
C1111-8P_DefaultIOS_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-8P	SD-WAN Edge	global	21	Disabled	0	test	0
C1111-8P_DefaultIOS_v4_4_20231004	C1111-8P_DefaultIOS_v4_4_20231004	Feature	C1111-8P	SD-WAN Edge	global	22	Disabled	2	rwse6	0
C1111-8P_DefaultIOS_v4_4_20231004_copy	C1111-8P_DefaultIOS_v4_4_20231004_copy	Feature	C1111-8P	SD-WAN Edge	global	22	Disabled	0	rwse6-gm	0

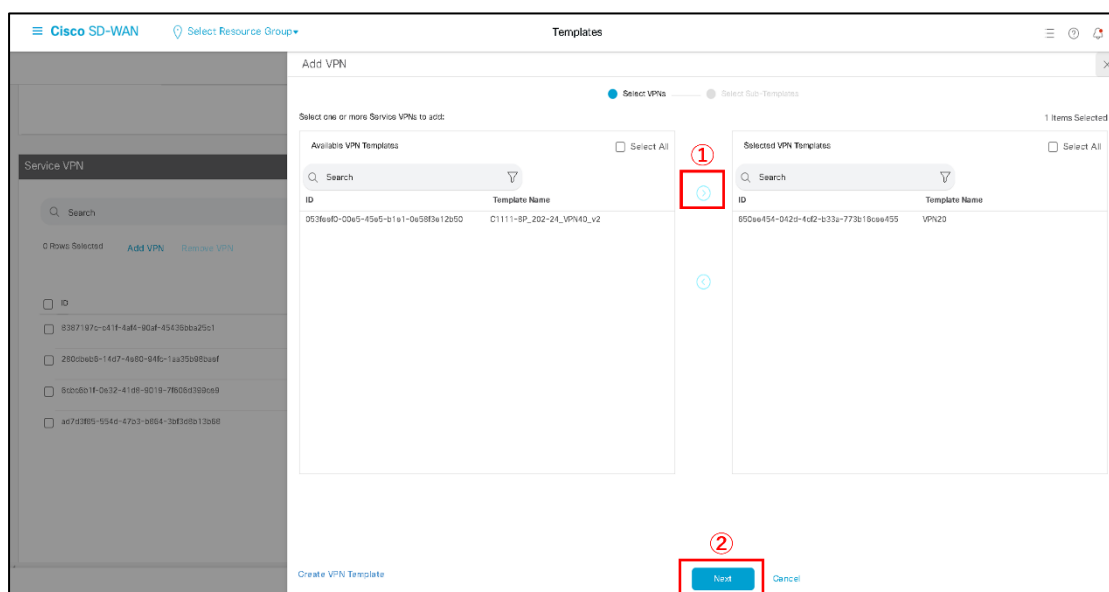
4.2.5. Device Template に追加 VPN グループ用の Feature Template をアタッチ

Device Template を変更

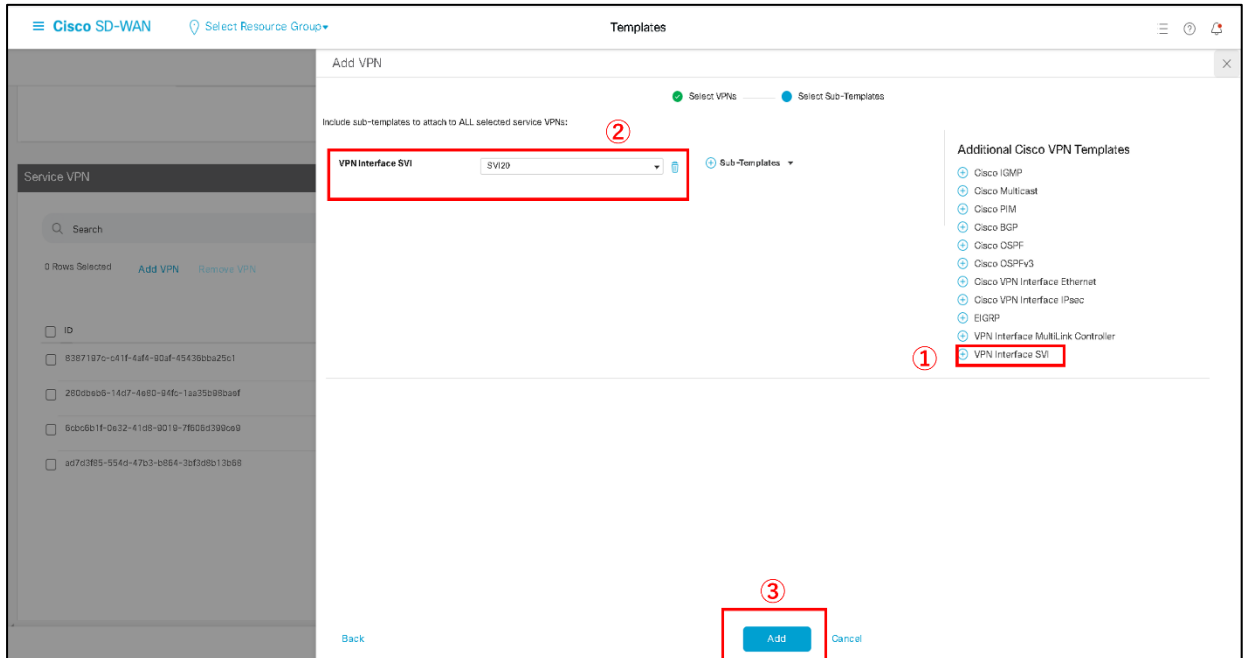
7. Service VPN 欄の「Add VPN」を選択



8. ① 「VPN20」を選択し「→」を選択し右ボックスに移動
- ② 「Next」を選択

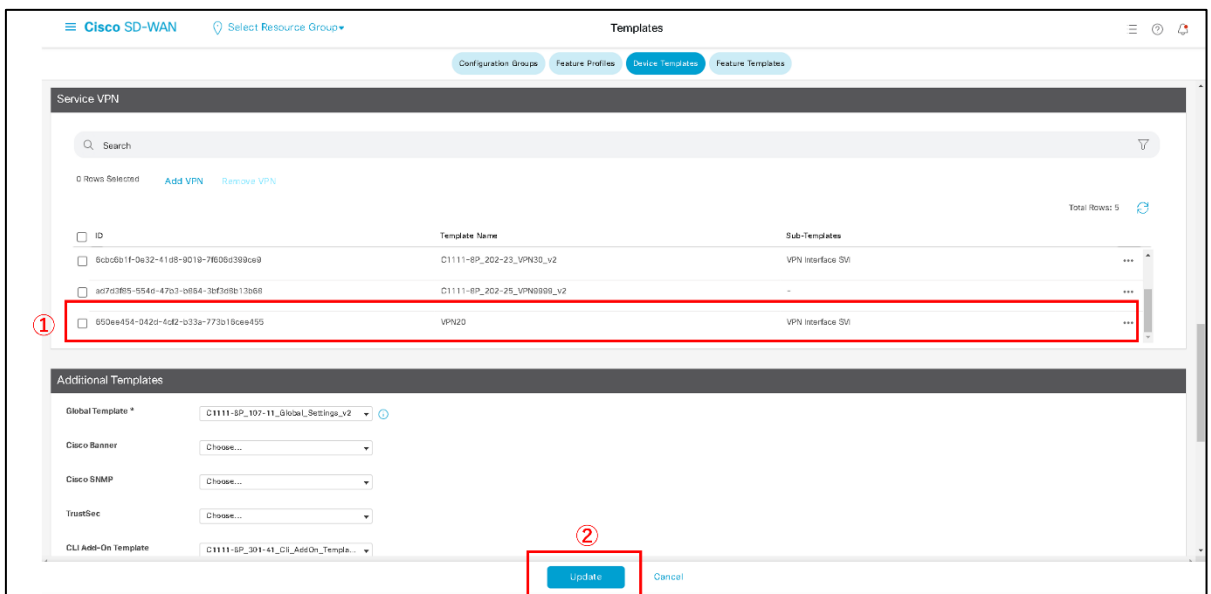


9. ①右側「VPN Interface SVI」を選択
- ②VPN Interface SVI のプルダウンから SVI20 を選択
- ③「Add」を選択



The screenshot shows the 'Add VPN' dialog in the Cisco SD-WAN interface. On the left, there's a 'Service VPN' list. The main area is titled 'Add VPN' and has two tabs: 'Select VPNs' (active) and 'Select Sub-Templates'. Under 'Include sub-templates to attach to ALL selected service VPNs:', there's a dropdown menu labeled 'VPN Interface SVI' with 'SVI20' selected. To the right, under 'Additional Cisco VPN Templates', a list of templates is shown, with 'VPN Interface SVI' highlighted. At the bottom right, the 'Add' button is highlighted.

10. ①VPN が追加されたことを確認
 - ②「Update」を選択
- ※VPN グループを 3 つ以上作る場合は手順 1~9 の値を変えて繰り返してください



The screenshot shows the 'Service VPN' table in the Cisco SD-WAN interface. The table has columns for 'ID', 'Template Name', and 'Sub-Templates'. The row for 'VPN20' is highlighted. Below the table, there's an 'Additional Templates' section with various dropdown menus. At the bottom right, the 'Update' button is highlighted.

ID	Template Name	Sub-Templates
6c8c0b1f-0a32-41d8-9019-7f606d389ca9	C1111-SP_202-23_VPN30_v2	VPN Interface SVI
ad7d3f65-554d-47b3-b864-3ef36b13b68	C1111-SP_202-25_VPN0000_v2	-
850ea454-042d-4d2d-b33a-773b18caa495	VPN20	VPN Interface SVI

4.2.6. 作成した Device Template を CPE にアタッチ

設定したい CPE へアタッチ

11. 新たに作成した Device Template の「…」から「Attach devices」を選択

The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' tab selected. A table lists various device templates. The context menu for the first template is open, and the 'Attach Devices' option is highlighted.

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Li
C1111-6P_Default05	IPSec/Secure	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	0	test	0: ...
C1111-6P_Default05_DS-Itle	IPSec/Secure/DS-Itle	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	0	test	0: ...
C1111-6P_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	1	test	0: ...
C1111-6P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	0	test	0: ...
C1111-6P_Default05_v4_4_20231004	C1111-6P_Default05_v4_4_20231004	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	2	mwse0	0: ...
C1111-6P_Default05_v4_4_20231004_copy	C1111-6P_Default05_v4_4_20231004_c...	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	0	mwse0	0: ...

12. ①適用したい CPE を選択し,「→」を選択し右ボックスに移動

②「Attach」を選択

The screenshot shows the 'Attach Devices' dialog box. It has two panes: 'Available Devices' and 'Selected Devices'. The 'Available Devices' pane shows a list of devices. The 'Selected Devices' pane shows the selected device 'CPE2' with IP '100.1.49.70'. The 'Attach' button is highlighted.

Name	Device IP
CPE1	100.1.49.69
jok1	100.200.0.1

Name	Device IP
CPE2	100.1.49.70

13. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択

S...	Chassis Number	System IP	Hostname	VLAN ID(gi010_vlan)	VLAN ID(gi011_vlan)	VLAN ID(gi012_vlan)	VLAN ID(gi013_vlan)	VLAN ID(gi014_vlan)	VLAN ID(gi015_vlan)	VLAN ID(gi016_vlan)	VLAN ID(gi017_v
①	C1111-8P-FGL2436LFAQ	100.1.78.17	CPE2	10	10	10	10	20	20	20	20

14. ①各 IF に所属する VPN を設定

(下記画面は GE0/1/0-3 を 10, GE0/1/4-7 を 20 に設定した場合)

②VPN20 に設定する IP アドレスを入力

③「Update」を選択し、「Next」を選択

注: Color, Device group, System IP, Site ID はデフォルト値から変更すると通信ができなくなる恐れがあるため、変更しないようお願いいたします

Update Device Template

① Variable List (Hover over each field for more information)

VLAN ID(gi010_vlan)	10
VLAN ID(gi011_vlan)	10
VLAN ID(gi012_vlan)	10
VLAN ID(gi013_vlan)	10
VLAN ID(gi014_vlan)	20
VLAN ID(gi015_vlan)	20
VLAN ID(gi016_vlan)	20
VLAN ID(gi017_vlan)	20
dns_primary_ipv6	2404:1a6:7b1:a::3
dns_secondary_ipv6	2404:1a6:7b1:b::3
IPv4 Address(vi40_ipv4_address)	10.40.1.254/24
IPv4 Address(vi00_ipv4_address)	10.30.1.254/24
② IPv4 Address(vi05_ipv4_address)	10.20.1.254/24
IPv4 Address(vi10_ipv4_address)	192.168.2.254/24
Color(gi000_color)	private1
Hostname(system_host_name)	CPE2
Device Groups(system_device_groups)	east
System IP(system_system_ip)	100.1.78.17
Site ID(system_site_id)	200010001

③ Update Cancel

③ Next Cancel

15. ①以下の画面で CPE を選択し、コンフィグを出力

(Config Diff を選択すると差分表示が可能です)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を確認願います

16. Status が success, Message が Done となっていればコンフィグ適用が完了

※Status 変更までに 1 分程度かかります

※Status が success とならない場合、エラー内容及び手順を確認し時間をおいてリトライの実施をお願いします

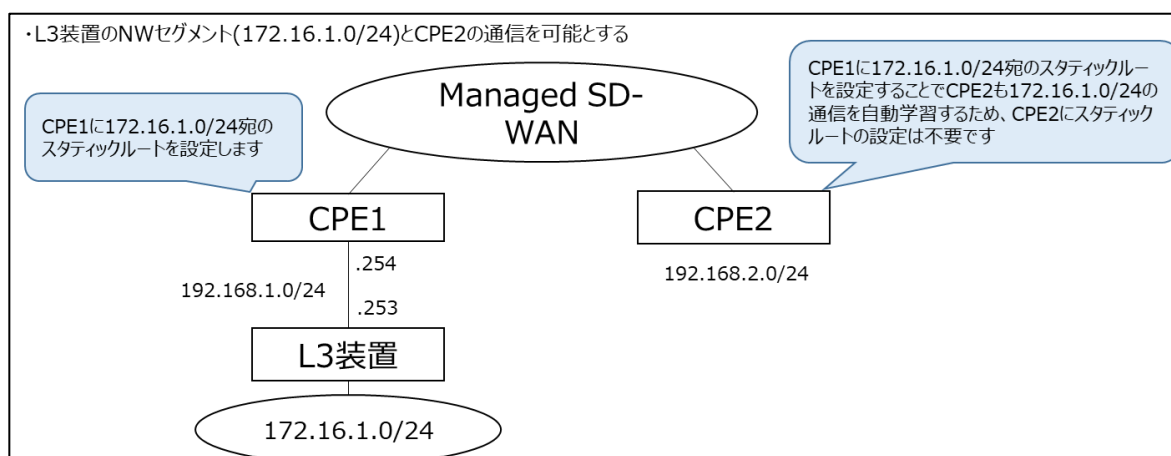
Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template Conf...	C1111-8P-FGL2436LF4Q	C1111-8P	CPE2	100.1.78.17	200010001	209.255.1.2

4.3. スタティックルートの設定

スタティックルートの設定手順を紹介します。

CPE 下部に L3 装置等があり、別 NW セグメントと通信が必要な場合に次ページ以降の手順を実施します。

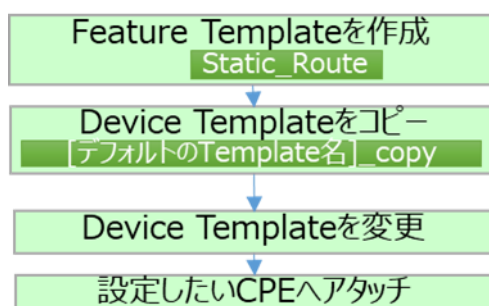
4.3.1. NW 構成例



【Device Template 作成に必要な Feature Template】

作成するFeature Template	手順	用途
static_route	1～7	スタティックルート設定用

【設定の流れ】



4.3.2. スタティックルート用 Feature Template を作成

Feature Template を作成

Static_Route

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature Templates」を選択
「Add Template」を選択

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
ISR1100X-4G_202-22_VPN...	ISR1100X-4G_202-22_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:23:19 PM
CS300-1N1S-4T2X_203-7...	CS300-1N1S-4T2X_203-7...	Cisco VPN Interface Ethernet	CS300-1N1S-4T2X	1	global	1	Provider-sdwan-order-mi	05 Oct 2023 1:30:50 PM
CS300-1N1S-4T2X_203-5...	CS300-1N1S-4T2X_203-5...	Cisco VPN Interface Ethernet	CS300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:13:26 PM
CS300-1N1S-4T2X_203-5...	CS300-1N1S-4T2X_203-5...	Cisco VPN Interface Ethernet	CS300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:15:37 PM
CS300-1N1S-4T2X_203-5...	CS300-1N1S-4T2X_203-5...	Cisco VPN Interface Ethernet	CS300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:17:19 PM
CS300-1N1S-4T2X_206-1...	CS300-1N1S-4T2X_206-1...	WAN Edge cEdge Cellular In...	CS300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	05 Oct 2023 1:38:10 PM
CS300-1N1S-4T2X_301-4...	CS300-1N1S-4T2X_301-4...	CLI Template	CS300-1N1S-4T2X	1	global	1	Provider-sdwan-order-mi	05 Oct 2023 1:33:04 PM
ISR1100X-4G_202-11_VPN...	ISR1100X-4G_202-11_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:24:51 PM
CS300-1N1S-4T2X_303-1...	CS300-1N1S-4T2X_303-1...	Cellular Controller	CS300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	05 Oct 2023 1:39:41 PM
ISR1100X-4G_202-23_VPN...	ISR1100X-4G_202-23_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:25:44 PM
ISR1100X-4G_202-25_VPN...	ISR1100X-4G_202-25_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	1	global	0	Provider-sdwan-order-mi	05 Oct 2023 2:26:12 PM
ISR1100X-4G_203-51_VF...	ISR1100X-4G_203-51_VF...	Cisco VPN Interface Ethernet	ISR 1100X 4G (Cisco OS)	5	global	1	Provider-sdwan-order-mi	05 Oct 2023 11:10:26 AM

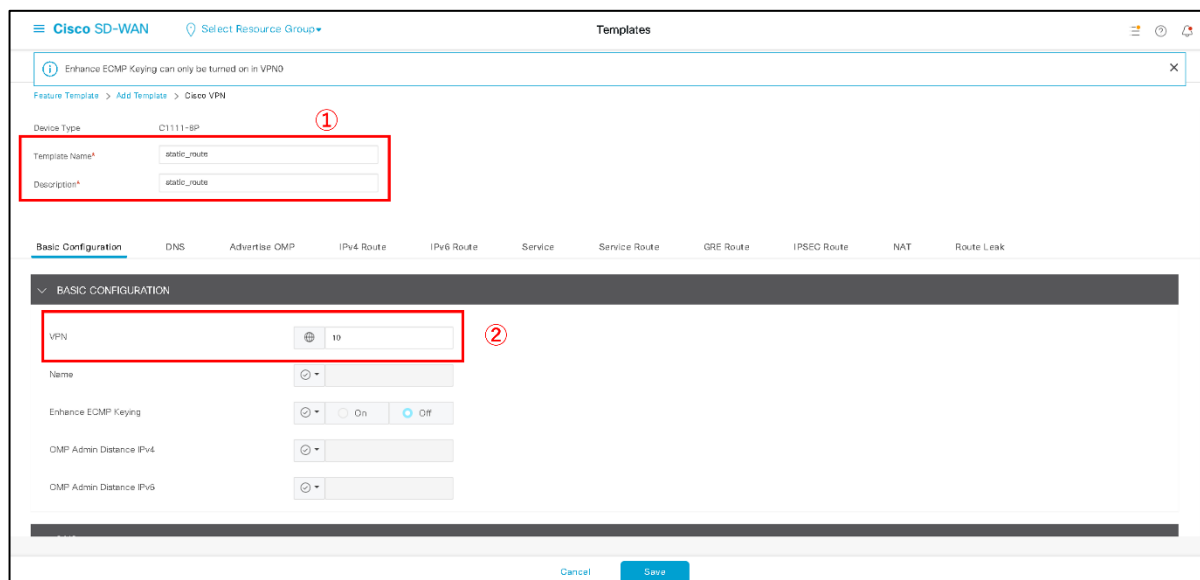
機種名は「C1111-8P」にチェックをいれ、「Cisco VPN」を選択

※タイプⅡの CPE へ設定する場合は「C1111-8PLTELA」にチェック

※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック

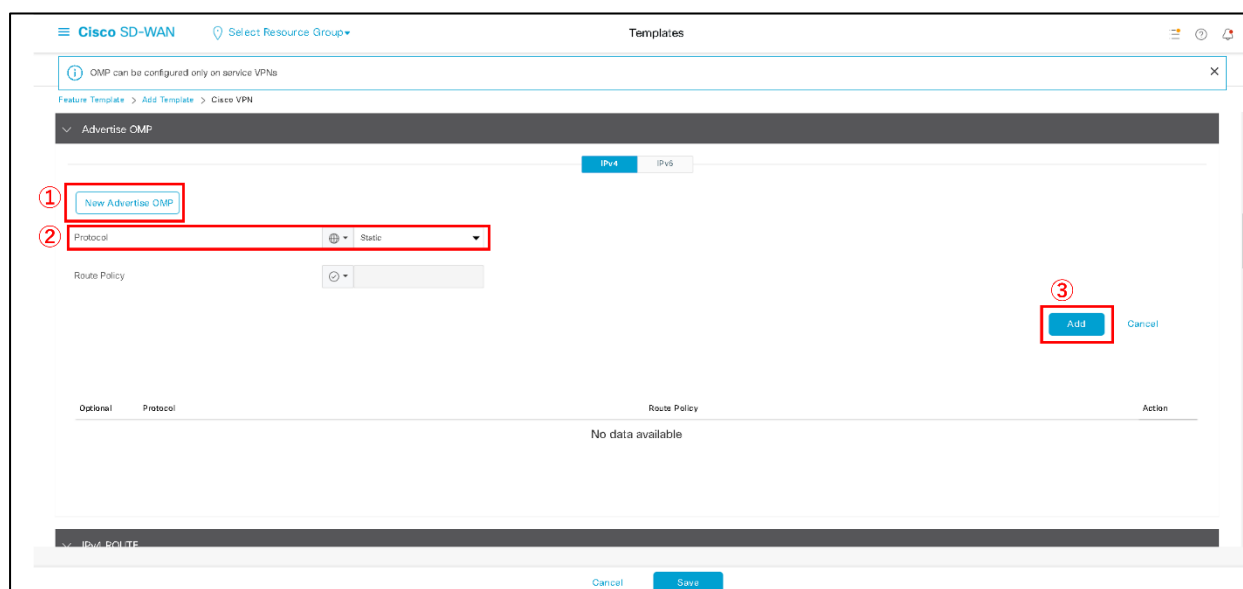
※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック

2. ① Template Name/Description に「static_route」を入力
 ② VPN の値を Global で 10 に変更 ※static route を追加したい VPN 番号を記載



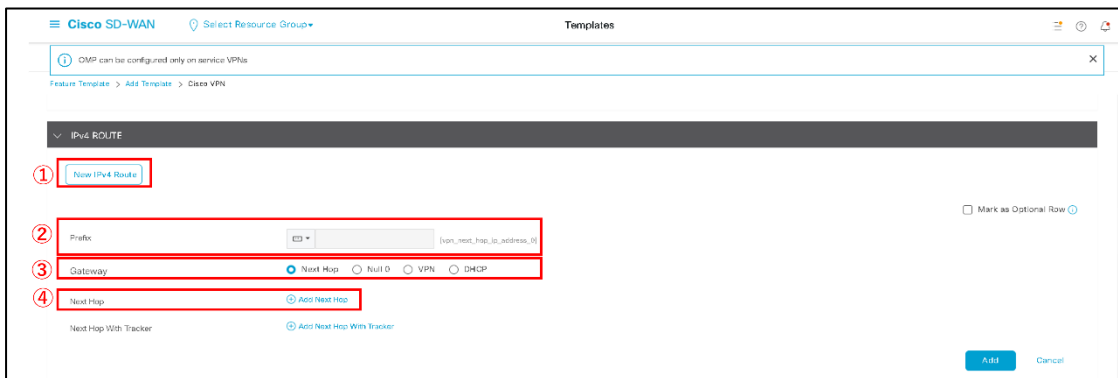
The screenshot shows the 'Cisco SD-WAN' interface for configuring a 'static_route' template. The 'Template Name' and 'Description' fields are both set to 'static_route'. The 'VPN' dropdown menu is set to '10'. The 'Basic Configuration' tab is active, and the 'Save' button is visible at the bottom right.

3. ① 「New Advertise OMP」を選択
 ② Protocol について Global で「Static」を選択
 ③ 「Add」を選択

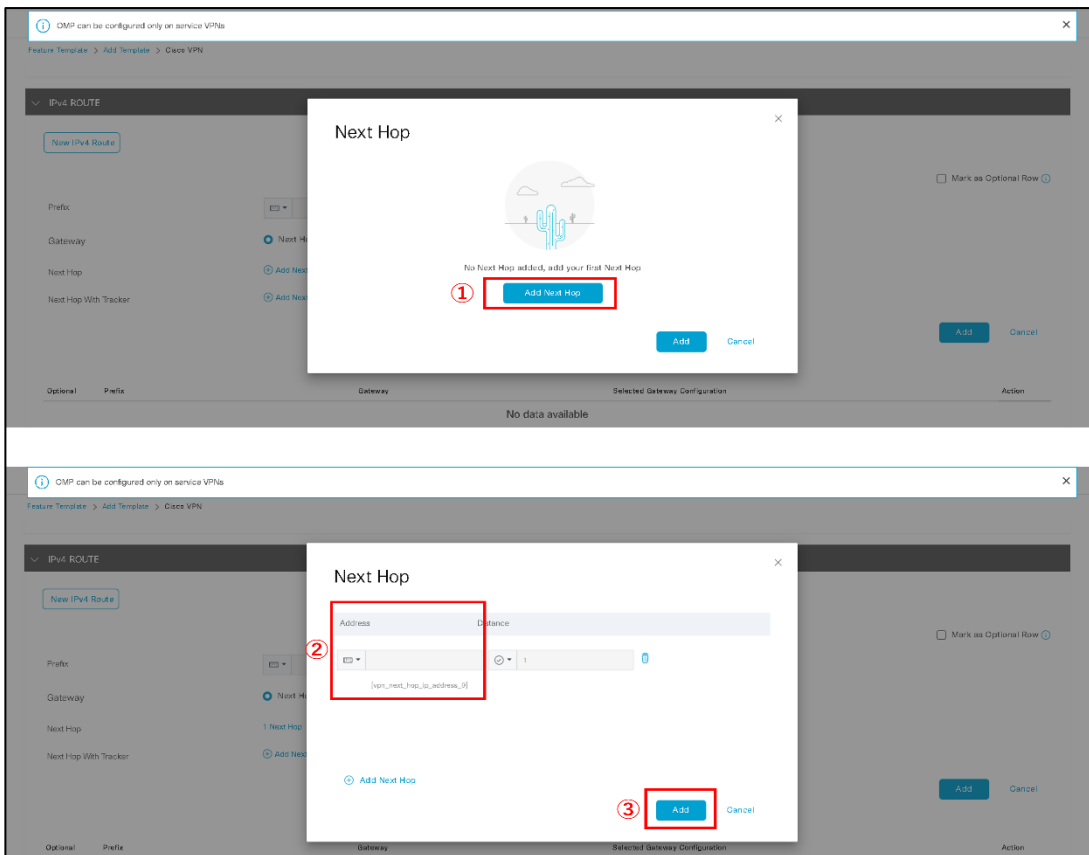


The screenshot shows the 'Cisco SD-WAN' interface for configuring 'Advertise OMP'. The 'New Advertise OMP' button is highlighted with a red box and labeled ①. The 'Protocol' dropdown menu is set to 'Static' and is highlighted with a red box and labeled ②. The 'Add' button is highlighted with a red box and labeled ③. The 'Save' button is visible at the bottom right.

4. ①「New IPv4 Route」を選択
- ②Prefix は「Device Specific」を選択し、変数名を入力する(※Sample では変数名は **vpn_next_hop_ip_addrss_0** としております。)
- ③Gateway は「Next hop」を選択
- ④「Add Next Hop」を選択



5. ①下記画面が表示されるので、「Add Next Hop」を選択
- ②Address は「Device Specific」
- ③「Add」を選択



※スタティックルートを複数設定する場合、4,5 の手順を参照し、変数名を変えて繰り返してください(例えば 4 に記載の変数名の末尾を変え **vpn_next_hop_ip_addrss_1** など)

【注意】vCPE では 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 を設定します。プライベートアドレスへの通信のためにデフォルトルート(0.0.0.0/0)等を設定するとプライベートアドレス向け通信はロングストマッチで vCPE 側にルーティングされて想定通りの通信ができないため、集約ルートを設定したい場合は 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 より長いサブネットマスク(例：10.0.0.0/9、10.128.0.0/9 等)でのルーティング設定が必要です。

6. ①下記画面が表示されるので、「Add」を選択
- ②最後に、「Save」を選択

4.3.3. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

Device Template をコピー

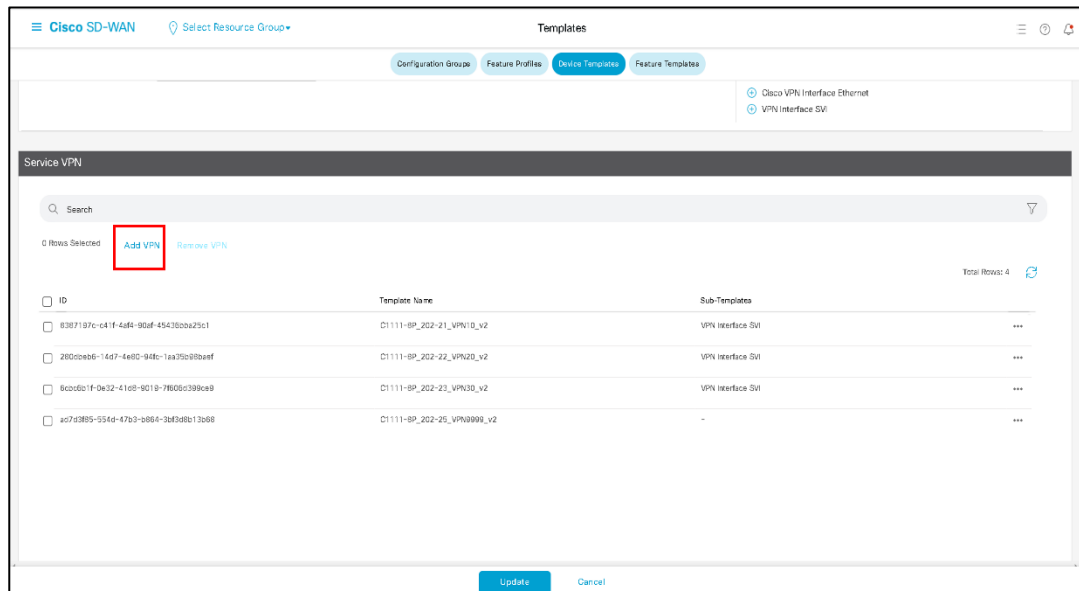
7. 左ペイン(左の領域)の Configuration から「Templates」を選択
- 画面上部のタブから「Device Templates」を選択
- NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Li
C1111-8P_Default05	IPSec/Secure	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	test	0
C1111-8P_Default05_DS-lite	IPSec/Secure/DS-lite	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test	0
C1111-8P_Default05_MAP-E(1P)	IPSec/Secure/MAP-E(1P)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	1	test	0
C1111-8P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test	0
C1111-8P_Default05_v4_4_20231004	C1111-8P_Default05_v4_4_20231004	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	2	rwse6-	0
C1111-8P_Default05_v4_4_20231004_copy	C1111-8P_Default05_v4_4_20231004_copy	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	rwse6-gre	0

4.3.4. Device Template にスタティックルート用の Feature Template をアタッチ

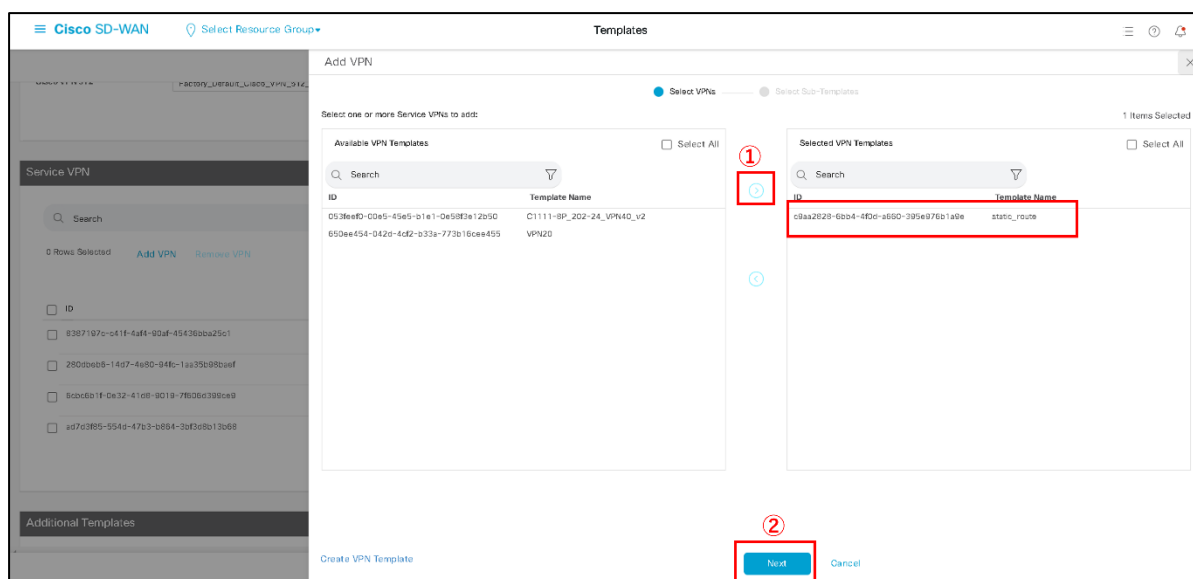
Device Template を変更

8. Service VPN 欄の「Add VPN」を選択

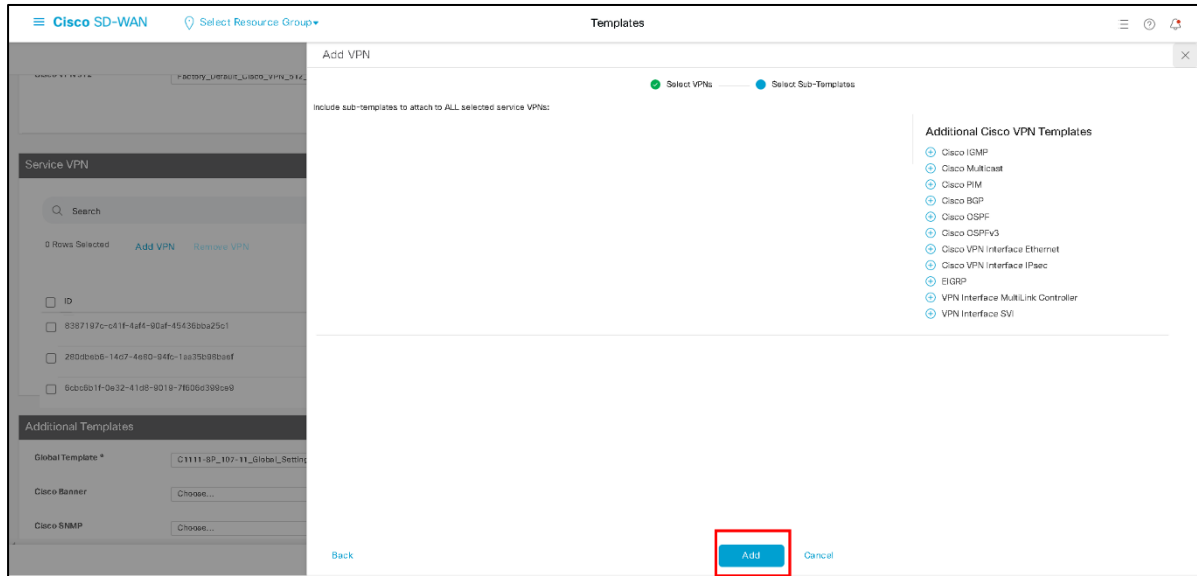


9. ①「static route」を選択し「→」を選択し右ボックスに移動

②「Next」を選択



10. 「Add」を選択



Add VPN

Select VPNs | Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

Service VPN

Search

0 Rows Selected | [Add VPN](#) | [Remove VPN](#)

ID
6387197c-c41f-4af4-90af-45438ba25c1
280cbab6-14c7-4e80-94fc-1aa35b98baef
6c0c0b1f-0e32-41d8-9d19-7f50ed398ce9

Additional Templates

Global Template * | C1111-8P_107-11_Global_Settings

Cisco Banner | Choose...

Cisco SNMP | Choose...

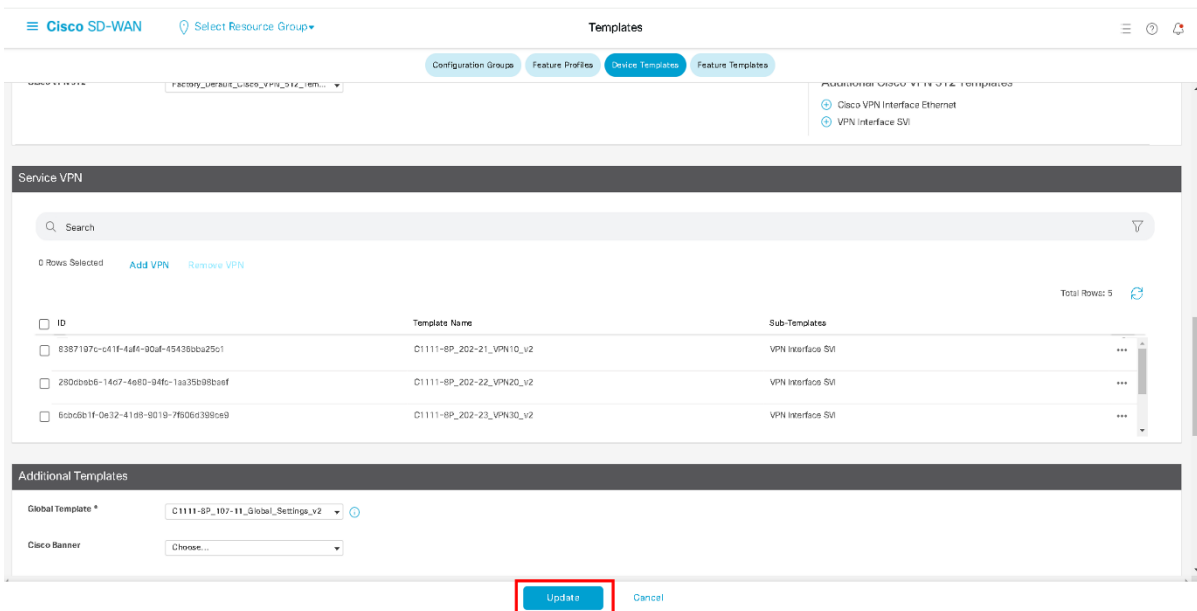
[Back](#) | [Add](#) | [Cancel](#)

Additional Cisco VPN Templates

- Cisco IGMP
- Cisco Multicast
- Cisco PIM
- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco VPN Interface Ethernet
- Cisco VPN Interface IPsec
- BLRP
- VPN Interface MultiLink Controller
- VPN Interface SVI

11. ①VPN が追加されことを確認

②「Update」を選択



Templates

Configuration Groups | Feature Profiles | **Device Templates** | Feature Templates

Service VPN

Search

0 Rows Selected | [Add VPN](#) | [Remove VPN](#)

ID	Template Name	Sub-Templates
6387197c-c41f-4af4-90af-45438ba25c1	C1111-8P_202-21_VPN10_v2	VPN Interface SVI
280cbab6-14c7-4e80-94fc-1aa35b98baef	C1111-8P_202-22_VPN20_v2	VPN Interface SVI
6c0c0b1f-0e32-41d8-9d19-7f50ed398ce9	C1111-8P_202-23_VPN30_v2	VPN Interface SVI

Total Rows: 5

Additional Templates

Global Template * | C1111-8P_107-11_Global_Settings_v2

Cisco Banner | Choose...

[Update](#) | [Cancel](#)

4.3.5. 作成した Device Template を CPE にアタッチ

設定したい CPE へアタッチ

12. 新たに作成した Template の「…」から「Attach Devices」を選択

Table with 10 columns: Name, Description, Type, Device Mode, Device Role, Resource Group, Feature Templates, Draft Mode, Devices Attached, Updated By. The table lists several templates, including C1111-BP_Default05 and C1111-BP_Default05_DS-lite. A context menu is open for the first row, showing options like Edit, View, Delete, Copy, Enable Draft Mode, Attach Devices (highlighted), Change Resource Group, and Export CSV.

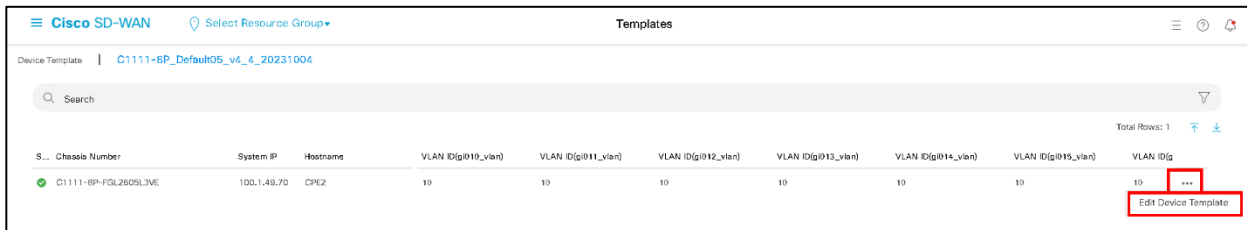
13. ①適用したい CPE を選択し、「→」を選択し右ボックスに移動

②「Attach」を選択

The 'Attach Devices' dialog box is shown. It has two main sections: 'Available Devices' and 'Selected Devices'. In the 'Available Devices' section, a table lists devices with columns 'Name' and 'Device IP'. 'CPE2' with IP '100.149.70' is selected. A red box highlights the right arrow button between the two sections. In the 'Selected Devices' section, 'CPE2' is now listed. A red box highlights the 'Attach' button at the bottom right of the dialog.

14. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択

※Status が success とならない場合、エラー内容及び手順を確認し時間を置いてリトライの実施をお願いします



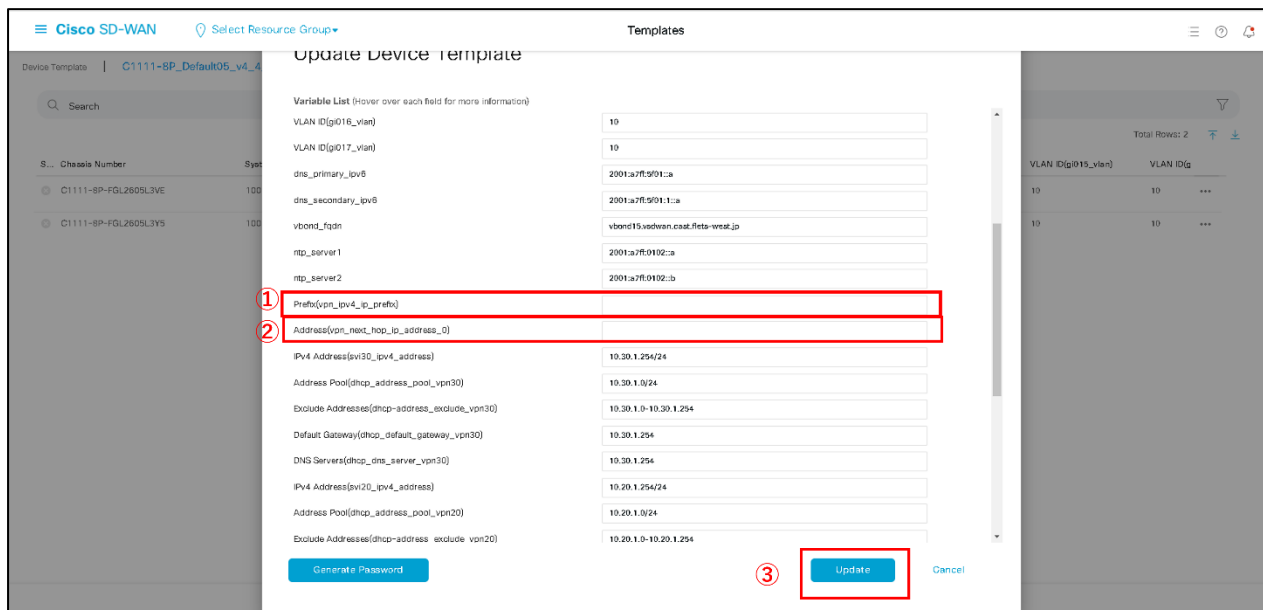
S...	Chassis Number	System IP	Hostname	VLAN ID(g010_vlan)	VLAN ID(g011_vlan)	VLAN ID(g012_vlan)	VLAN ID(g013_vlan)	VLAN ID(g014_vlan)	VLAN ID(g015_vlan)	VLAN IDg
●	C1111-8P-FGL2605L3VE	100.1.48.70	CPE2	10	10	10	10	10	10	10 ... Edit Device Template

15. ①宛先 NW を入力(ex. 172.16.1.0/24)

②ネクストホップを入力(ex. 192.168.1.253)

③「Update」を選択し、「Next」を選択

注: Color, Device group, System IP, Site ID はデフォルト値から変更すると通信ができなくなる恐れがあるため、変更しないようお願いいたします



Update Device Template

Variable List (Hover over each field for more information)

VLAN ID(g016_vlan)	10
VLAN ID(g017_vlan)	10
dns_primary_ipv6	2001:a7f:901::a
dns_secondary_ipv6	2001:a7f:901::a
vbond_fqdn	vbond15.sdwan.cust.flets-wrest.jp
ntp_server1	2001:a7f:9012::a
ntp_server2	2001:a7f:9012::b
① Prefix(vpn_ipv4_ip_prefix)	
② Address(vpn_next_hop_ip_address_0)	
IPv4 Address(vpn30_ipv4_address)	10.30.1.254/24
Address Pool(dhcp_address_pool_vpn30)	10.30.1.0/24
Exclude Addresses(dhcp-address_exclude_vpn30)	10.30.1.0-10.30.1.254
Default Gateway(dhcp_default_gateway_vpn30)	10.30.1.254
DNS Servers(dhcp_dns_server_vpn30)	10.30.1.254
IPv4 Address(vpn20_ipv4_address)	10.30.1.254/24
Address Pool(dhcp_address_pool_vpn20)	10.20.1.0/24
Exclude Addresses(dhcp-address_exclude_vpn20)	10.20.1.0-10.20.1.254

Generate Password

③ Update Cancel

16. ①以下の画面で CPE を選択し、コンフィグを出力

(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を確認願います

The screenshot shows the Cisco SD-WAN configuration interface. On the left, a list of device templates is shown, with 'C1111-8P-FGL2605L3VE' selected. The main area displays a 'Local Configuration vs. New Configuration' diff view. At the bottom, the 'Configure Devices' button is highlighted with a red box and a circled '2'.

17. Status が success, Message が Done となっていればコンフィグ適用が完了

※Status が success とならない場合、エラー内容及び手順を確認し時間をおいてリトライの実施をお願いします

The screenshot shows the 'Push Feature Template Configuration' status page. The 'Status' column shows 'Success' and the 'Message' column shows 'Done - Push Feature Template C...'. The 'Chassis Number' column shows 'C1111-8P-FGL2605L3VE'. The 'Device Model' column shows 'C1111-8P'. The 'Hostname' column shows 'CPE2'. The 'System IP' column shows '100.1.49.70'. The 'Site ID' column shows '300006342'. The 'vManage IP' column shows '215.255.1.2'.

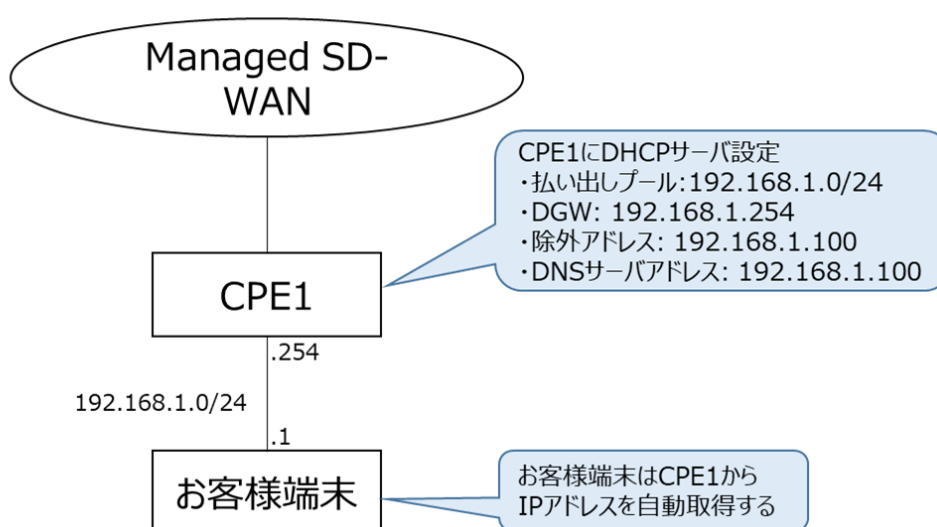
4.4. DHCP サーバの設定

DHCP サーバの設定方法を紹介します。

CPE の下部端末に自動で IP アドレスを払い出したい場合、次ページ以降の手順を実施します。

4.4.1. NW 構成例

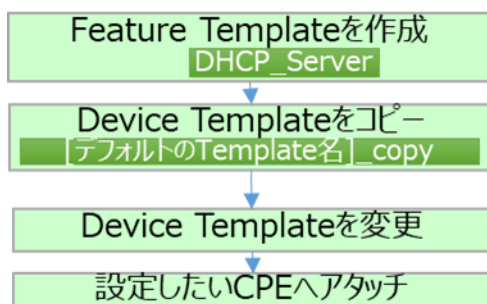
- ・CPE1の下部端末にCPE1から自動的にIPアドレスを払い出す



【Device Template 作成に必要となる Feature Template】

作成する Feature Template	手順	用途
DHCP_Server	1～3	DHCP サーバ設定用

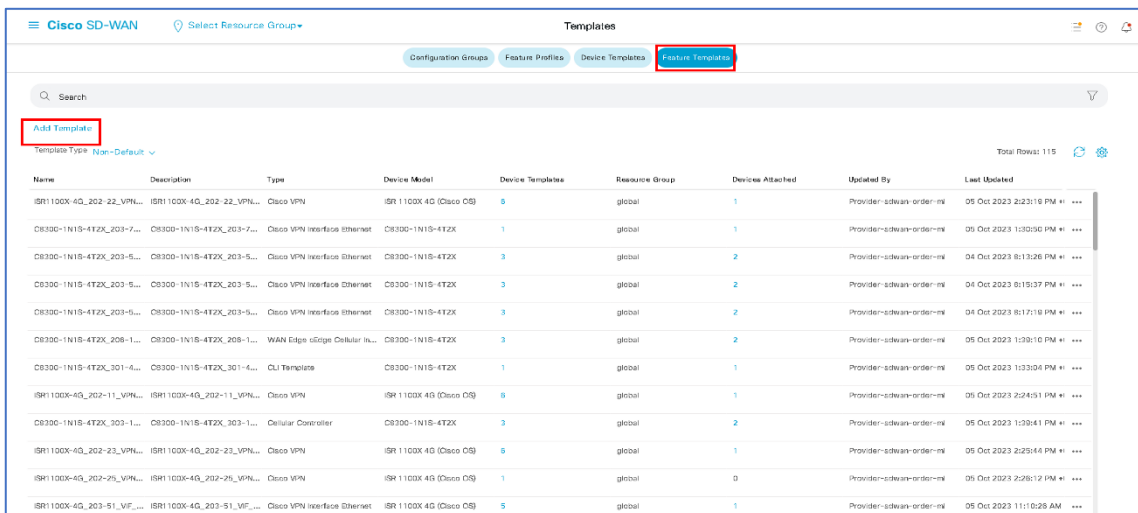
【設定の流れ】



4.4.2. DHCP サーバ用 Feature Template を作成

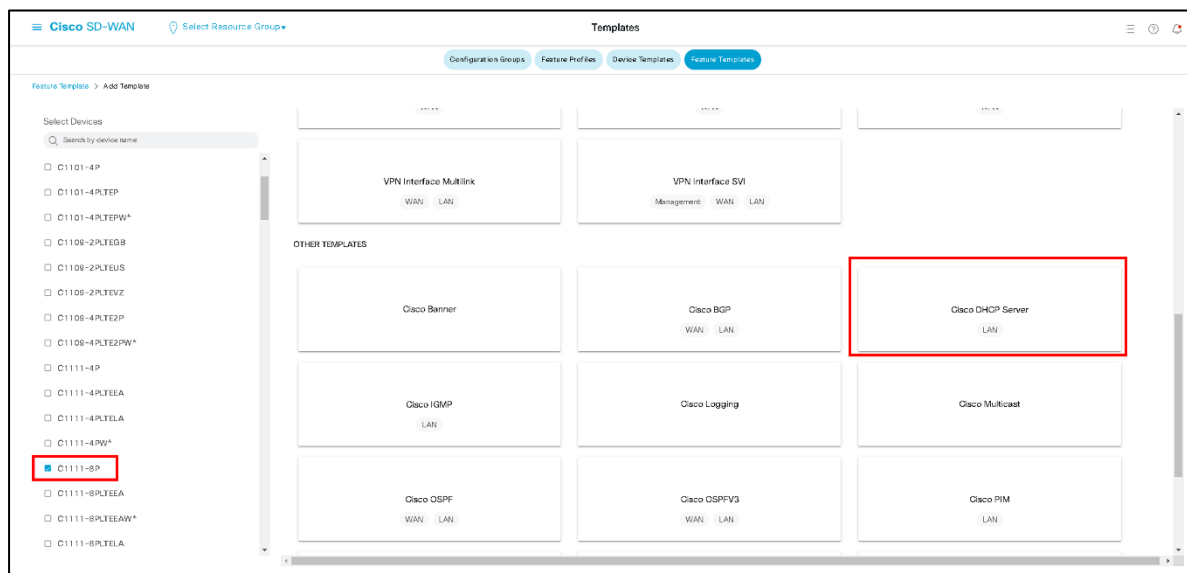
Feature Template を作成
DHCP_Server

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature Templates」を選択
「Add Template」を選択



Name	Description	Type	Device Model	Device Template	Resource Group	Device Attached	Updated By	Last Updated
ISR1100X-4G_202-22_VPN...	ISR1100X-4G_202-22_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	5	global	1	Provider-sdwan-order-m	05 Oct 2023 2:23:16 PM
CS300-1N1S-4TZK_203-7...	CS300-1N1S-4TZK_203-7...	Cisco VPN Interface Ethernet	CS300-1N1S-4TZK	1	global	1	Provider-sdwan-order-m	05 Oct 2023 1:30:50 PM
CS300-1N1S-4TZK_203-5...	CS300-1N1S-4TZK_203-5...	Cisco VPN Interface Ethernet	CS300-1N1S-4TZK	3	global	2	Provider-sdwan-order-m	04 Oct 2023 8:13:06 PM
CS300-1N1S-4TZK_203-5...	CS300-1N1S-4TZK_203-5...	Cisco VPN Interface Ethernet	CS300-1N1S-4TZK	3	global	2	Provider-sdwan-order-m	04 Oct 2023 8:15:37 PM
CS300-1N1S-4TZK_203-5...	CS300-1N1S-4TZK_203-5...	Cisco VPN Interface Ethernet	CS300-1N1S-4TZK	3	global	2	Provider-sdwan-order-m	04 Oct 2023 8:17:18 PM
CS300-1N1S-4TZK_208-1...	CS300-1N1S-4TZK_208-1...	WAN Edge cEdge Cellular In...	CS300-1N1S-4TZK	3	global	2	Provider-sdwan-order-m	05 Oct 2023 1:30:16 PM
CS300-1N1S-4TZK_301-4...	CS300-1N1S-4TZK_301-4...	CU Template	CS300-1N1S-4TZK	1	global	1	Provider-sdwan-order-m	05 Oct 2023 1:33:04 PM
ISR1100X-4G_202-11_VPN...	ISR1100X-4G_202-11_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-m	05 Oct 2023 2:23:16 PM
CS300-1N1S-4TZK_303-1...	CS300-1N1S-4TZK_303-1...	Cellular Controller	CS300-1N1S-4TZK	3	global	2	Provider-sdwan-order-m	05 Oct 2023 1:30:41 PM
ISR1100X-4G_202-23_VPN...	ISR1100X-4G_202-23_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-m	05 Oct 2023 2:23:16 PM
ISR1100X-4G_202-25_VPN...	ISR1100X-4G_202-25_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	1	global	0	Provider-sdwan-order-m	05 Oct 2023 2:28:12 PM
ISR1100X-4G_203-51_VF...	ISR1100X-4G_203-51_VF...	Cisco VPN Interface Ethernet	ISR1100X 4G (Cisco OS)	5	global	1	Provider-sdwan-order-m	05 Oct 2023 11:02:28 AM

2. 機種名は「C1111-8P」にチェックをいれ、「Cisco DHCP Sever」を選択
※タイプ II の CPE へ設定する場合は「C1111-8PLTELA」にチェック



3. ①Template Name/Description に「DHCP_Server」入力
 - ②Address Pool/Exclude Address を「Device specific」と選択
 - ③Default Gateway/DNS server を「Device specific」と選択
- ※DNS サーバを払い出さない場合は DNS server の設定は不要(Device specific を選択しない)
- ④「Save」を選択

4.4.3. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

Device Template をコピー

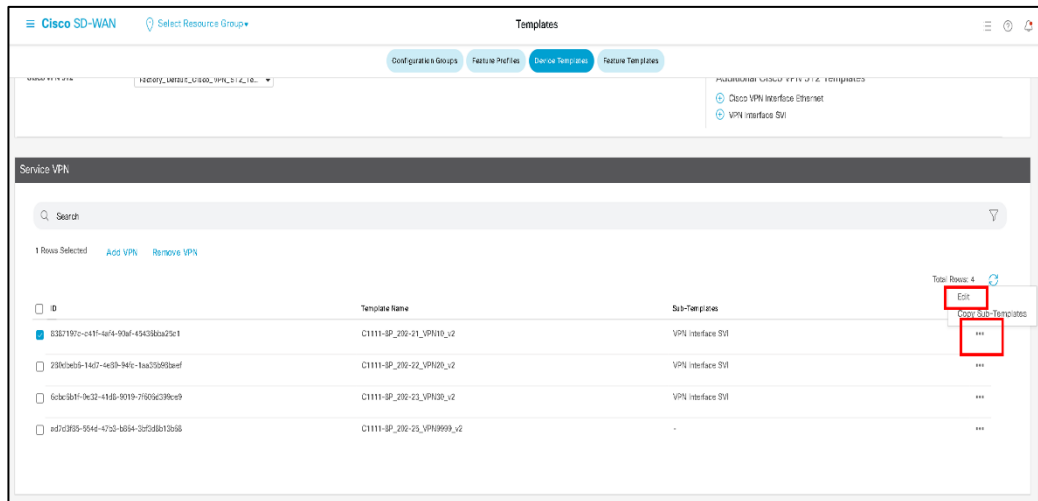
4. 左ペイン(左の領域)の Configuration から「Templates」を選択
 - 画面上部のタブから「Device Templates」を選択
 - NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択
- ※Template のコピーの手順は P10 を参照

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Actions
C1111-BP_Default05	IPSec/Secure	Feature	C1111-BP	SOWAN Edge	global	22	Disabled	0	test	...
C1111-BP_Default05_DS-1ite	IPSec/Secure/DS-1ite	Feature	C1111-BP	SOWAN Edge	global	21	Disabled	0	test	...
C1111-BP_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-BP	SOWAN Edge	global	21	Disabled	1	test	...
C1111-BP_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-BP	SOWAN Edge	global	21	Disabled	0	test	...
C1111-BP_Default05_v4_4_20231004	C1111-BP_Default05_v4_4_20231004	Feature	C1111-BP	SOWAN Edge	global	22	Disabled	2	nws66-	...
C1111-BP_Default05_v4_4_20231004_copy	C1111-BP_Default05_v4_4_20231004_copy	Feature	C1111-BP	SOWAN Edge	global	22	Disabled	0	nws66-gm	...

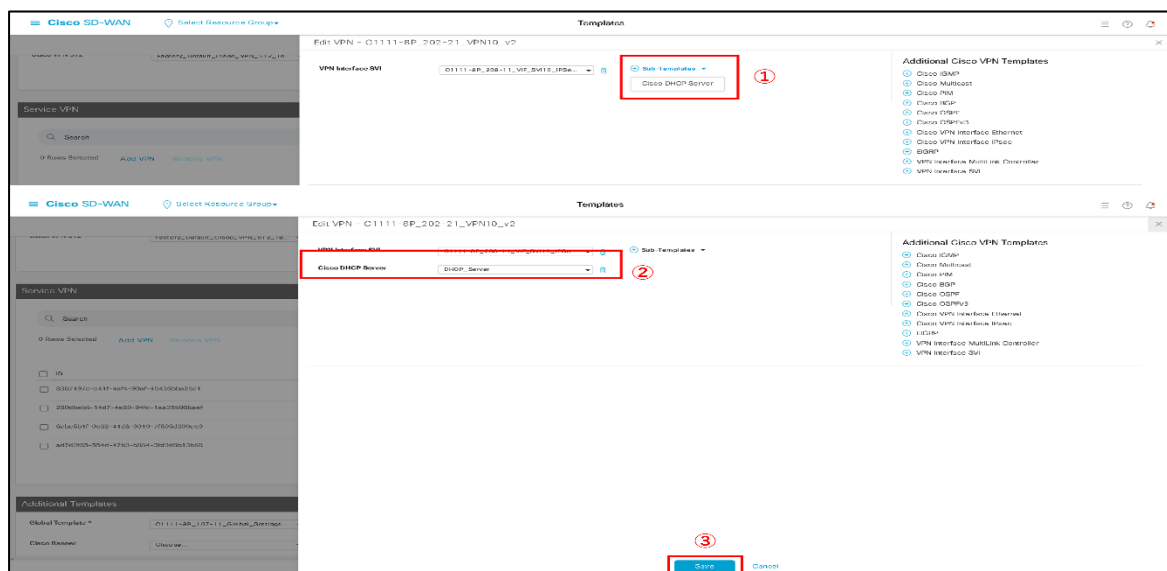
4.4.4. Device Template に DHCP サーバ用の Feature Template をアタッチ

Device Template を変更

5. Service VPN 欄の「…」から「Edit」を選択



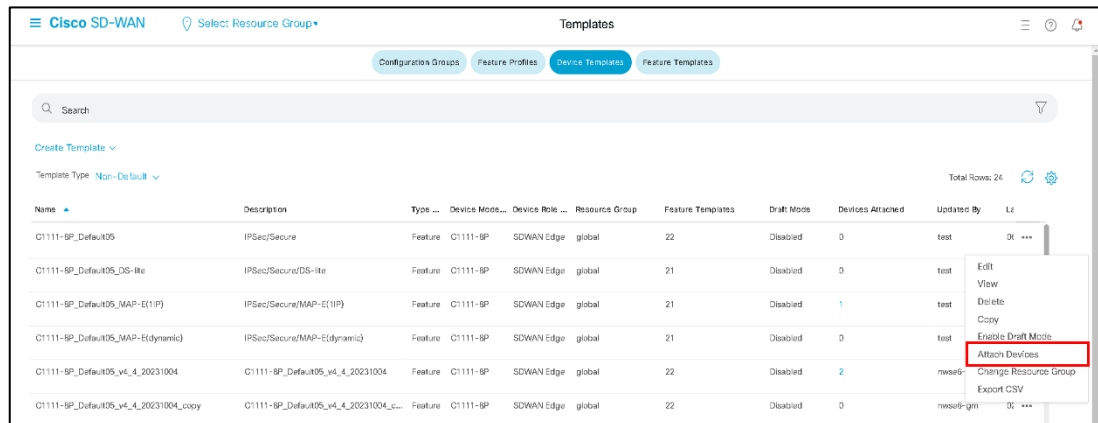
6. ①Sub Template から「Cisco DHCP Server」を選択
- ②「DHCP_Server」を選択し、「Save」を選択
- ③元の画面で「Update」を選択



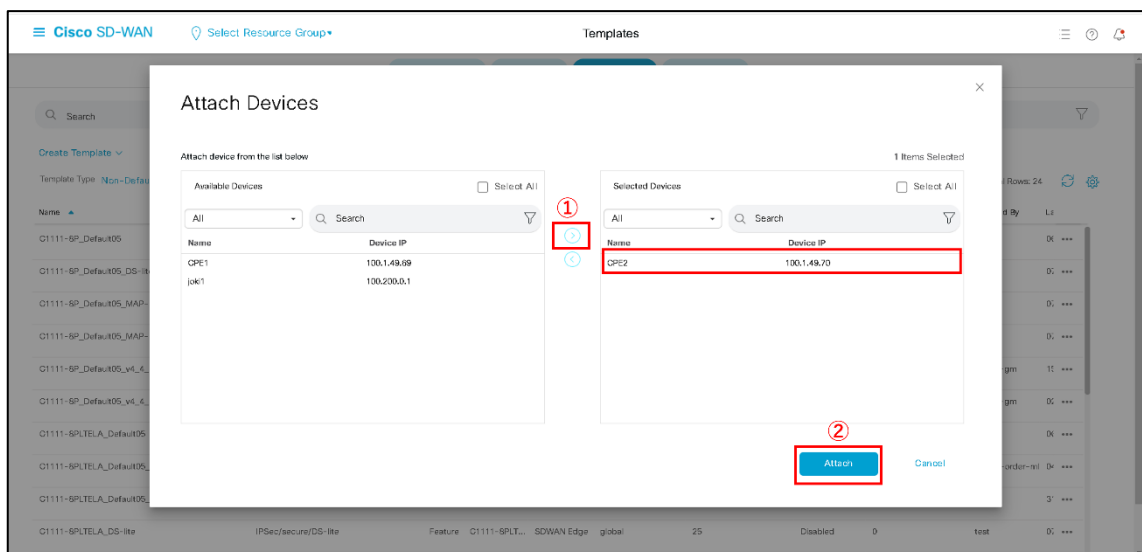
4.4.5. 作成した Device Template を CPE にアタッチ

設定したい CPE へアタッチ

7. 新たに作成したテンプレートの「…」から「Attach Devices」を選択



8. ①適用したい CPE を選択し, 「→」を選択し右ボックスに移動 ②「Attach」を選択



9. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択

Cisco SD-WAN

Select Resource Group

Templates

Device Template

C1111-8P_Default05_v4_4_20231004

Q Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	VLAN ID(gi010_vlan)	VLAN ID(gi011_vlan)	VLAN ID(gi012_vlan)	VLAN ID(gi013_vlan)	VLAN ID(gi014_vlan)	VLAN ID(gi015_vlan)	VLAN ID(gi016_vlan)
✓	C1111-8P-FGL2605L3VE	100.1.48.70	CPE2	10	10	10	10	10	10	10

...

Edit Device Template

10. ① Address Pool/Exclude Address/Default Gateway/DNS server の値を入力

②「Update」を選択し、「Next」を選択

注:Color, Device group, System IP, Site ID はデフォルト値から変更すると通信ができなくなる恐れがあるため、変更しないようお願いいたします

Select Resource Group

Update Device Template

Device Template | C1111-SP-DefaultIOS_v4_2023

Search

System IP

193.1.49.2

OS: Cisco IOS

193.1.49.2

OS: Cisco IOS

193.1.49.2

Variable List (Hover over each field for more information)

Address Pool(address_pool_vpn30)

Exclude Addresses(dhcp_exclude_vpn30)

Default Gateway(dhcp_default_gateway_vpn30)

DNS Servers(dhcp_dns_server_vpn30)

IPv4 Address(es)(v10_ip4_address)

Address Pool(address_pool_vpn30)

Exclude Addresses(dhcp_exclude_vpn30)

Default Gateway(dhcp_default_gateway_vpn30)

DNS Servers(dhcp_dns_server_vpn30)

IPv4 Address(es)(v10_ip4_address)

Address Pool(address_pool_vpn30)

Exclude Addresses(dhcp_exclude_vpn30)

Default Gateway(dhcp_default_gateway_vpn30)

DNS Servers(dhcp_dns_server_vpn30)

Order(g0/0/0_order)

Hostname(system_hostname)

Device Group(system_device_group)

System IP(system_ip)

Site ID(system_site_id)

193.1.10/24

193.1.10-193.1.254

193.1.10/24

193.1.100

193.1.100

193.1.200

193.1.10/24

193.1.100

193.1.254

193.1.200

green

CPU2

vnet

193.1.49.70

30003042

Generate Password

Update

Cancel

入力例

Address Pool(払い出しIPアドレス用プール):192.168.1.0/24

Exclude Addresses(払い出し除外アドレス):192.168.1.100

Default Gateway(デフォルトゲートウェイ):192.168.1.254

DNS Server(DNSサーバ設定) : 192.168.1.200

11. ①以下の画面で CPE を選択し、コンフィグを出力(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を再確認して下さい

12. Status が success, Message が Done となっていればコンフィグ適用が完了

※Status 変更までに 1 分程度かかります

※Status が success とならない場合、エラー内容及び手順を確認し時間をおいてリトライの実施をお願いします

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template C...	C1111-8P-FGL2605L3VE	C1111-8P	CPE2	100.1.49.70	300006342	215.255.1.2

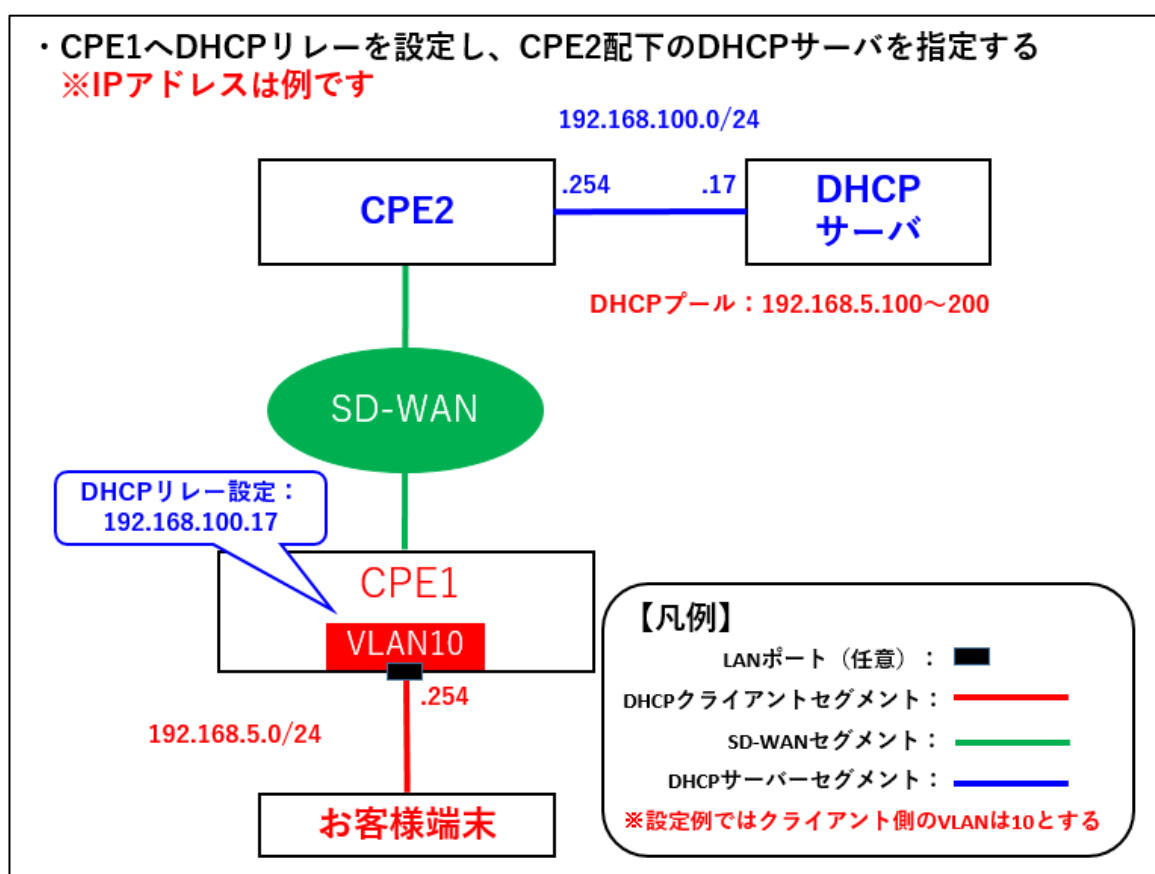
4.5. DHCP リレーの設定

DHCP リレーの設定方法について紹介します

CPE へ DHCP リレーの設定をする場合、次ページ以降の手順を実施します

※正常性はお客様端末にて IP アドレスの払い出し状況を確認願います。

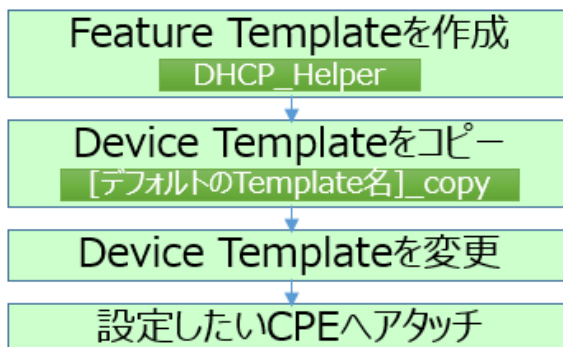
4.5.1. NW 構成例



【Device Template 作成に必要な Feature Template】

作成する Feature Template	手順	用途
DHCP_Helper	1-3	DHCP リレー用 Helper 設定

【設定の流れ】



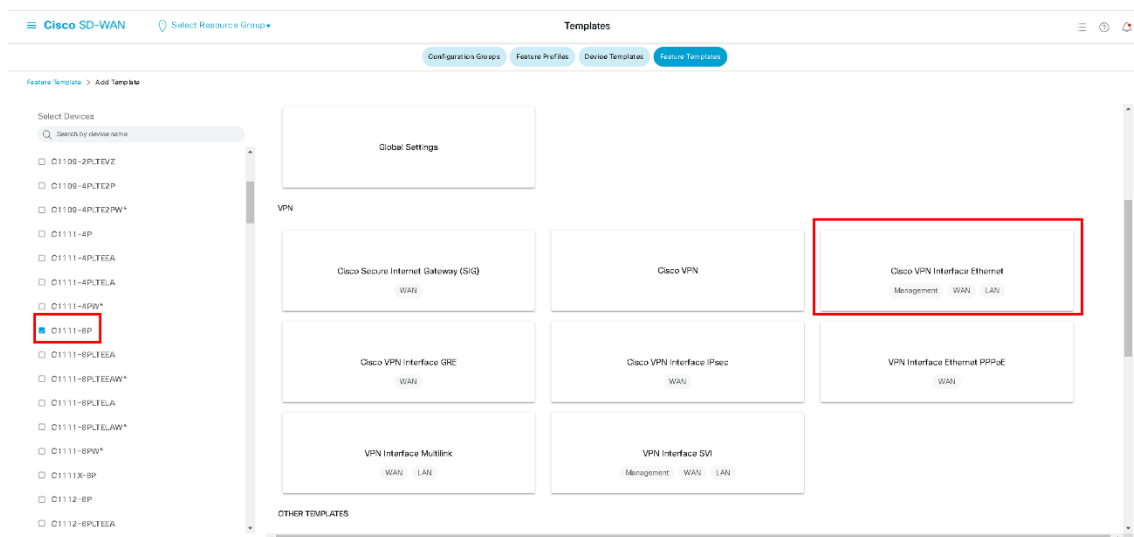
4.5.2. DHCP リレー用の Feature Template を作成

Feature Template を作成
DHCP_Helper

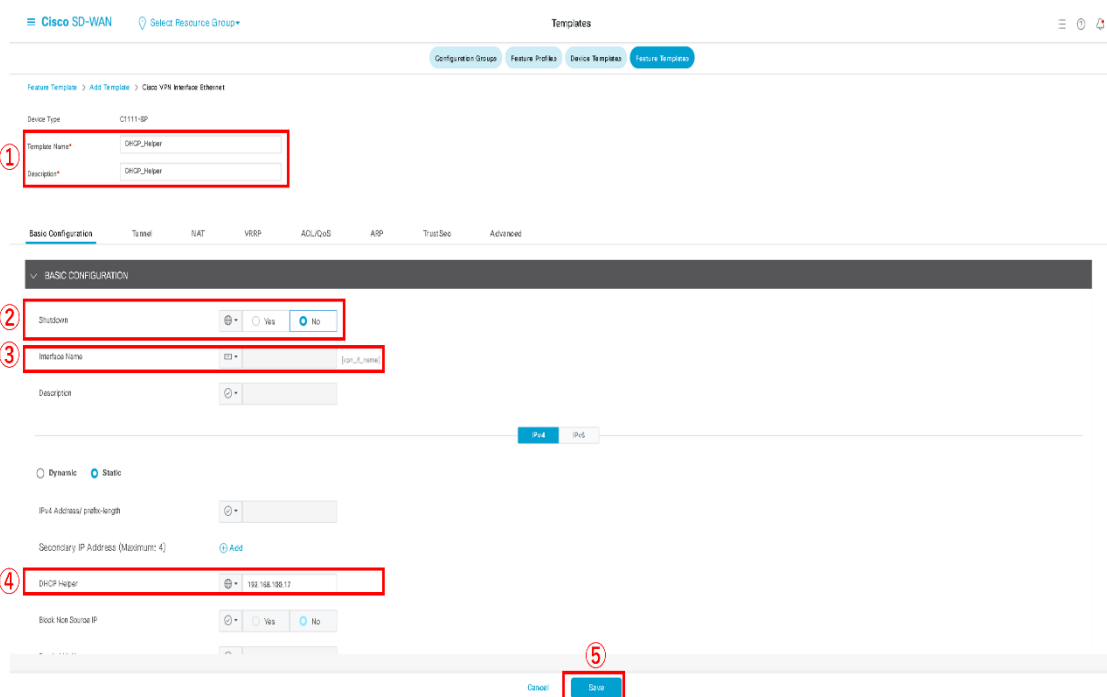
1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択
「Add Template」を選択

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
ISR1100X-45_202-22_VPN...	ISR1100X-45_202-22_VPN...	Cisco VPN	ISR1100X-45 (Cisco OS)	6	global	1	Provider-sdwan-order-mi	03 Oct 2023 2:23:19 PM +...
CS330-1N15-4T2X_203-7...	CS330-1N15-4T2X_203-7...	Cisco VPN interface Ethernet	CS330-1N15-4T2X	1	global	1	Provider-sdwan-order-mi	03 Oct 2023 1:50:50 PM +...
CS330-1N15-4T2X_203-5...	CS330-1N15-4T2X_203-5...	Cisco VPN interface Ethernet	CS330-1N15-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:13:26 PM +...
CS330-1N15-4T2X_203-5...	CS330-1N15-4T2X_203-5...	Cisco VPN interface Ethernet	CS330-1N15-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:15:27 PM +...
CS330-1N15-4T2X_203-5...	CS330-1N15-4T2X_203-5...	Cisco VPN interface Ethernet	CS330-1N15-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:17:19 PM +...
CS330-1N15-4T2X_203-1...	CS330-1N15-4T2X_203-1...	WAN Edge edge Cellular R...	CS330-1N15-4T2X	3	global	2	Provider-sdwan-order-mi	03 Oct 2023 1:36:10 PM +...
CS330-1N15-4T2X_201-4...	CS330-1N15-4T2X_201-4...	CU Template	CS330-1N15-4T2X	1	global	1	Provider-sdwan-order-mi	03 Oct 2023 1:33:04 PM +...
ISR1100X-45_202-11_VPN...	ISR1100X-45_202-11_VPN...	Cisco VPN	ISR1100X-45 (Cisco OS)	6	global	1	Provider-sdwan-order-mi	03 Oct 2023 2:24:51 PM +...
CS330-1N15-4T2X_203-1...	CS330-1N15-4T2X_203-1...	Cisco VPN	CS330-1N15-4T2X	3	global	2	Provider-sdwan-order-mi	03 Oct 2023 1:38:41 PM +...
ISR1100X-45_202-21_VPN...	ISR1100X-45_202-21_VPN...	Cisco VPN	ISR1100X-45 (Cisco OS)	6	global	1	Provider-sdwan-order-mi	03 Oct 2023 2:25:44 PM +...
ISR1100X-45_202-25_VPN...	ISR1100X-45_202-25_VPN...	Cisco VPN	ISR1100X-45 (Cisco OS)	1	global	0	Provider-sdwan-order-mi	03 Oct 2023 3:26:12 PM +...
ISR1100X-45_201-51_VF...	ISR1100X-45_201-51_VF...	Cisco VPN interface Ethernet	ISR1100X-45 (Cisco OS)	5	global	1	Provider-sdwan-order-mi	03 Oct 2023 1:11:02:26 AM +...

2. 機種名は「C1111-8P」にチェックをいれ、「Cisco VPN Interface Ethernet」を選択
 - ※タイプⅡの CPE へ設定する場合は「C1111-8PLTELA」にチェック
 - ※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック
 - ※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック



3. ①Template Template Name/Description へ「DHCP_Helper」を入力
 - ② shutdown へ Global で「No」を選択
 - ③ Interface Name を「device specific」と選択
 - ④ DHCP Helper を Global で DHCP サーバーのアドレスを入力（例として 192.168.100.17 を入力）
 - ⑤ Save をクリック

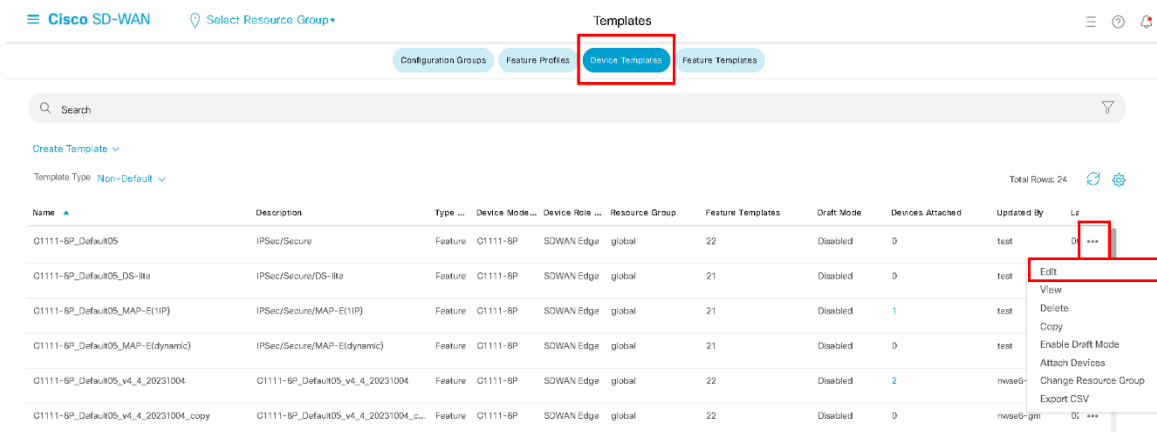


4.5.3. DHCP リレー用の Device Template を作成

Device Template を作成

[デフォルトの Template 名]_copy

4. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Device」を選択
NTT 東日本デフォルトの Template をコピー※し、コピーした Template の「…」から「Edit」を選択
※Template のコピーの手順は 3.1 章を参照



Search

Create Template ▾

Template Type Non-Default ▾

Total Rows: 24

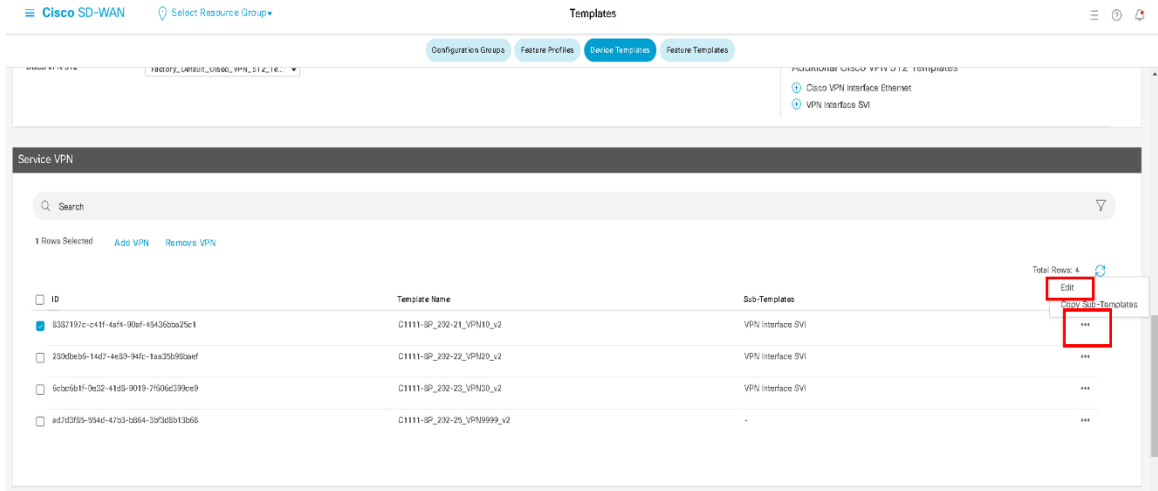
Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	...
C1111-6P_Default05	IPSec/Secure	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	0	test	0
C1111-6P_Default05_DS-lite	IPSec/Secure/DS-lite	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	0	test	...
C1111-6P_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	1	test	...
C1111-6P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-6P	SDWAN Edge	global	21	Disabled	0	test	...
C1111-6P_Default05_v4_4_20231004	C1111-6P_Default05_v4_4_20231004	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	2	mwise	...
C1111-6P_Default05_v4_4_20231004_copy	C1111-6P_Default05_v4_4_20231004_copy	Feature	C1111-6P	SDWAN Edge	global	22	Disabled	0	mwise-gm	...

Edit
View
Delete
Copy
Enable Draft Mode
Attach Devices
Change Resource Group
Export CSV

4.5.4. DHCP リレー用の Device Template を作成

Device Template を変更

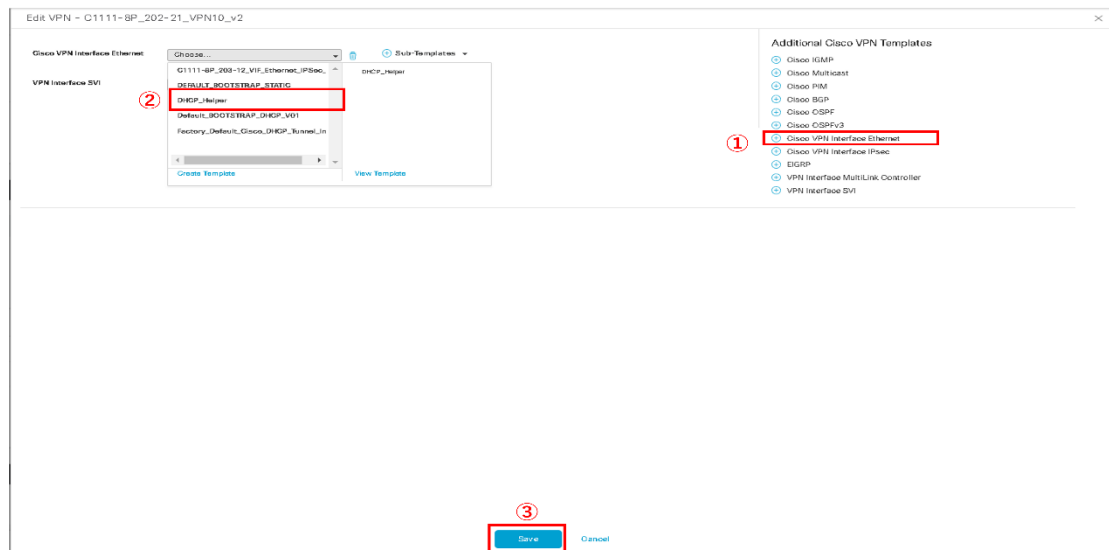
5. 「Service VPN」 から VPN10 を選択して、「…」⇒「Edit」を選択する。



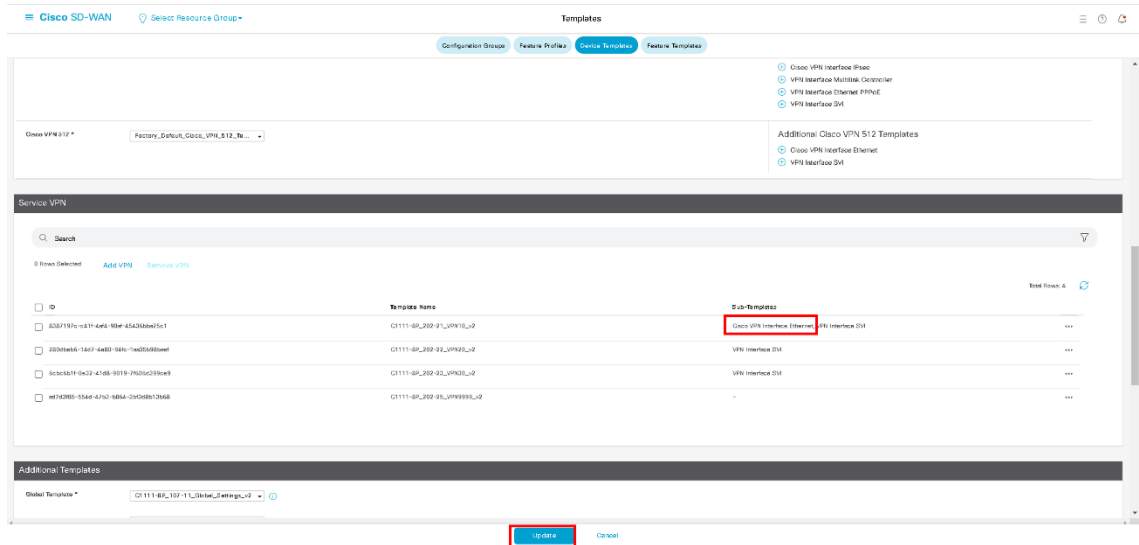
6. ①右側「VPN Interface Ethernet」を選択

②手順 3~で設定した VPN Interface Ethernet のテンプレートをプルダウンから選択

③「Save」を選択



7. VPN10 の Sub-Template の欄に「VPN Interface Ethernet」が追加されたことを確認してから画面下部の「Update」を選択



The screenshot shows the 'Cisco SD-WAN' interface for configuring templates. The 'Service VPN' section contains a table with the following data:

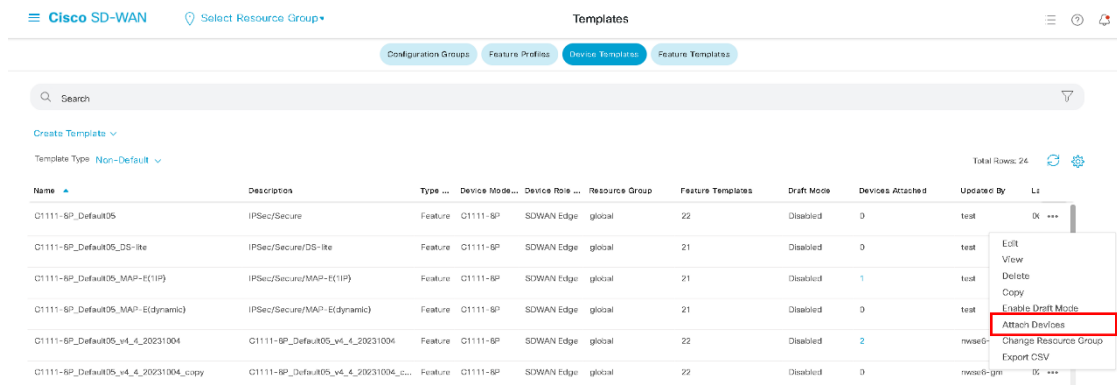
Template Name	Sub-Templates
C1111-8P_202-0_LVPN10_L2	Cisco VPN Interface Ethernet, VPN Interface D11
C1111-8P_202-02_VPN02_L2	VPN Interface D11
C1111-8P_202-02_VPN02_L2	VPN Interface D11
C1111-8P_202-02_VPN02_L2	-

At the bottom of the page, the 'Update' button is highlighted with a red box.

4.5.5. DHCP リレー用の Device Template をアタッチ

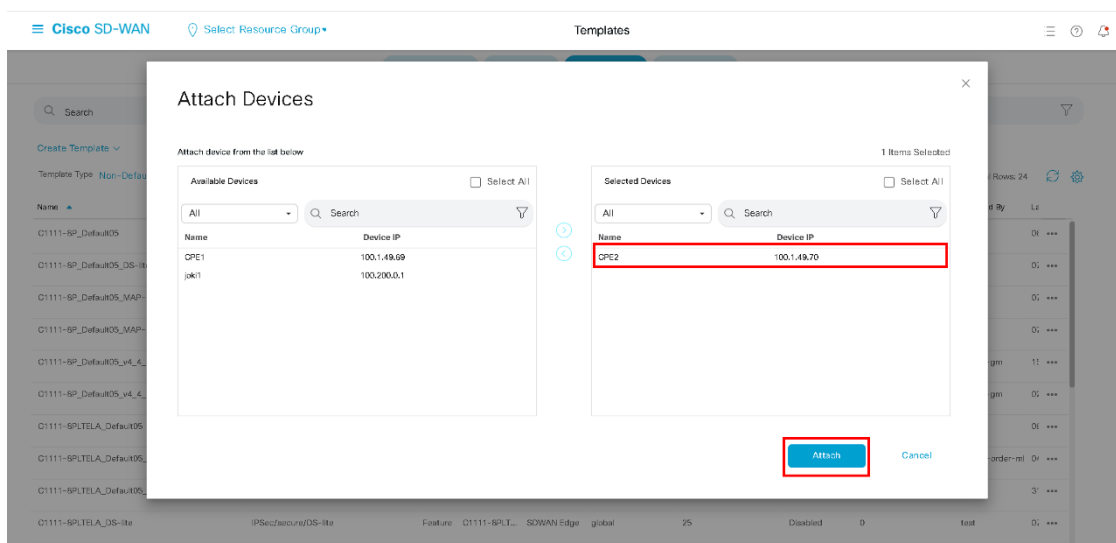
設定したい CPE へアタッチ

8. 新たに作成したテンプレートの「…」から「Attach Devices」を選択



9. ①適用したい CPE を選択し, 「→」を選択し右ボックスに移動

②「Attach」を選択



10. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択



Configuration > Templates

Device Template | C1111-8P_Default05_20220304_noPPoE_DHCP_copy

Search

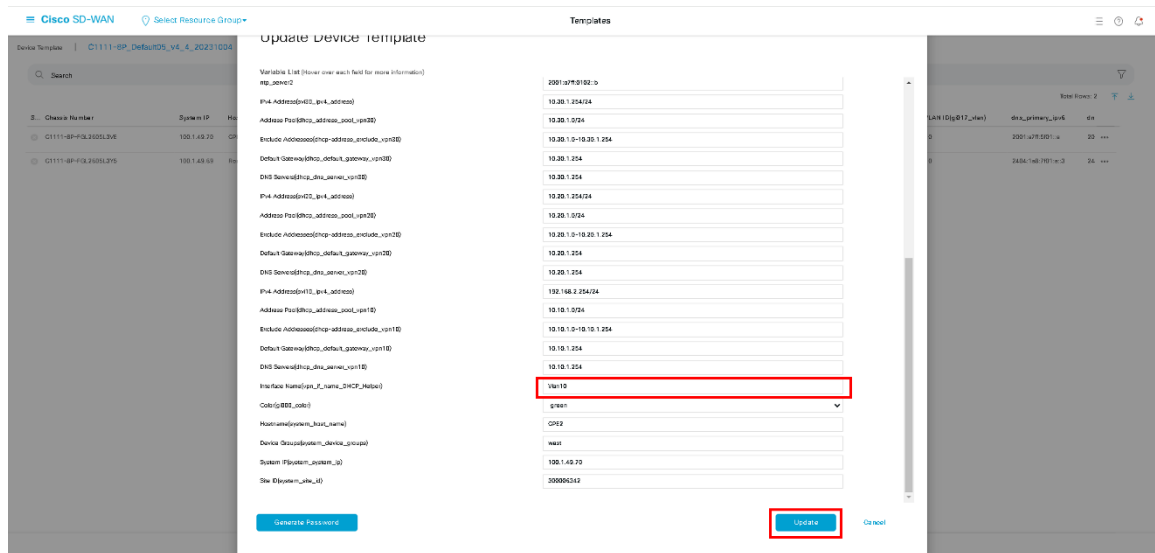
Total Rows: 1

S...	Chassis Number	System IP	Hostname	VLAN ID(gp010_vlan)	VLAN ID(gp011_vlan)	VLAN ID(gp012_vlan)	VLAN ID(gp013_vlan)	VLAN ID(gp014_vlan)	VLAN ID(gp015_vlan)	VLAN ID(g
✓	C1111-8P-FGL2436LGI	100.1.5.54	bjkai1	10	10	20	20	30	30	40

Edit Device Template

11. ①Interface Name(vpn_if_name_DHCP_Helper)に「Vlan10」を入力

②Update を選択



Update Device Template

Variable List (hover over each field for more information)

ipsec2

IPsec Address(gp010_ipsec)

Address Pool(gp010_ipsec_pool)

Exclude Address(gp010_ipsec_pool_excl)

Default Gateway(gp010_ipsec_gateway)

DNS Server(gp010_ipsec_dns_server)

IPsec Address(gp011_ipsec)

Address Pool(gp011_ipsec_pool)

Exclude Address(gp011_ipsec_pool_excl)

Default Gateway(gp011_ipsec_gateway)

DNS Server(gp011_ipsec_dns_server)

IPsec Address(gp012_ipsec)

Address Pool(gp012_ipsec_pool)

Exclude Address(gp012_ipsec_pool_excl)

Default Gateway(gp012_ipsec_gateway)

DNS Server(gp012_ipsec_dns_server)

IPsec Address(gp013_ipsec)

Address Pool(gp013_ipsec_pool)

Exclude Address(gp013_ipsec_pool_excl)

Default Gateway(gp013_ipsec_gateway)

DNS Server(gp013_ipsec_dns_server)

IPsec Address(gp014_ipsec)

Address Pool(gp014_ipsec_pool)

Exclude Address(gp014_ipsec_pool_excl)

Default Gateway(gp014_ipsec_gateway)

DNS Server(gp014_ipsec_dns_server)

Interface Name(vpn_if_name_DHCP_Helper)

Code(gp010_code)

Hostname(system_hostname)

Device Group(system_device_group)

System IP(system_ip)

Site ID(system_site_id)

Generate Password

Update Cancel

12. ①以下の画面で CPE を選択し、コンフィグを出力(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を確認願います

13. Status が success, Message が Done となっていればコンフィグ適用が完了

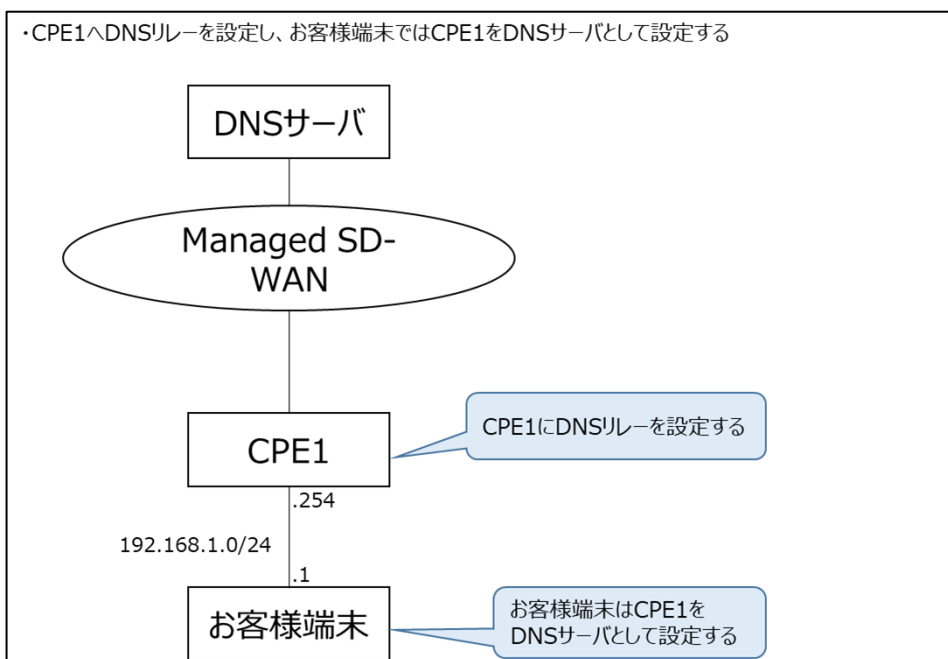
※Status が success とならない場合、エラー内容及び手順を確認し時間を置いてリトライの実施をお願いします

4.6. DNS リレーの設定

DNS リレーの設定方法を紹介します。

CPE へ DNS リレー場合、次ページ以降の手順を実施します。

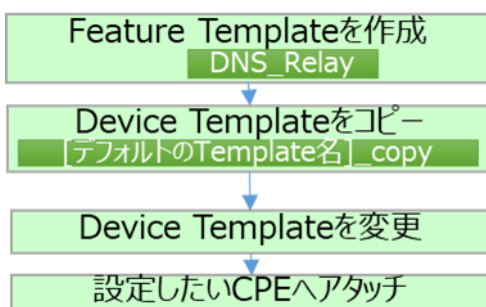
4.6.1. NW 構成例



【Device Template 作成に必要な Feature Template】

作成する Feature Template	手順	用途
DNS_Relay	1～3	DNS リレー設定用

【設定の流れ】



4.6.2. DNS リレー用 Feature Template を作成

Feature Template を作成

DNS relay

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択
「Add Template」を選択

Cisco SD-WAN
Select Resource Group

Templates

Configuration Groups
Feature Profiles
Device Templates
Resource Templates

Search

Add Template

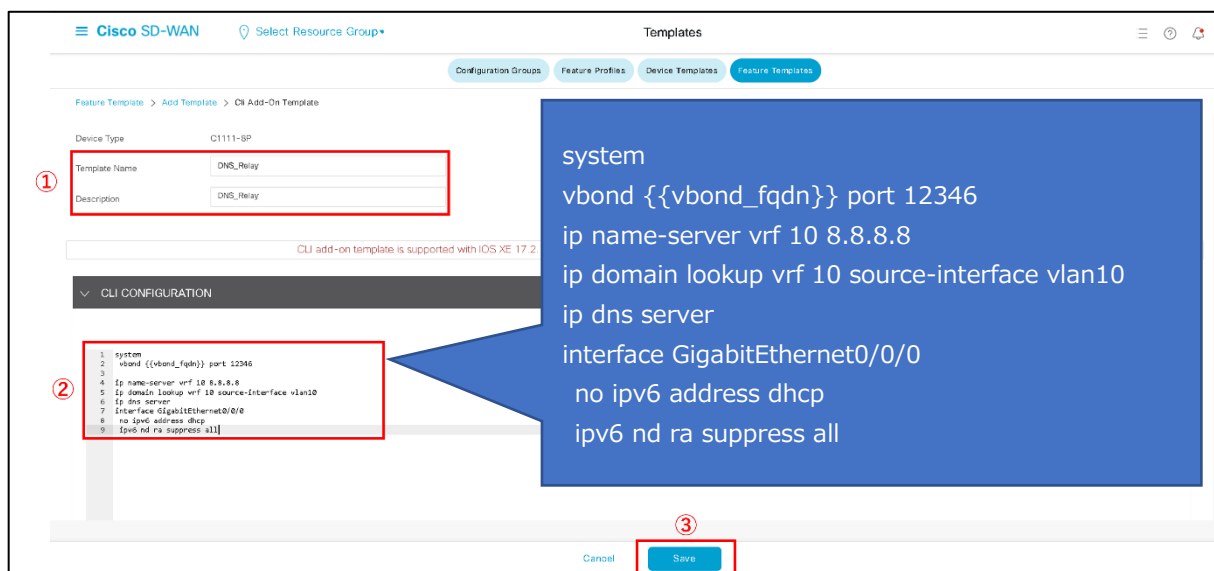
Template Type: Non-Default
Total Rows: 115

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
ISR1100X-6S_202-22_VPN...	ISR1100X-6S_202-22_VPN...	Cisco VPN	ISR1100X-6S (Cisco OS)	6	global	1	Provider-swdev-order-mf	05 Oct 2023 2:23:18 PM +...
CR300-1N1S-4TX2_203-7...	CR300-1N1S-4TX2_203-7...	Cisco VPN Interface Ethernet	CR300-1N1S-4TX2	1	global	1	Provider-swdev-order-mf	05 Oct 2023 1:30:50 PM +...
CR300-1N1S-4TX2_203-5...	CR300-1N1S-4TX2_203-5...	Cisco VPN Interface Ethernet	CR300-1N1S-4TX2	3	global	2	Provider-swdev-order-mf	04 Oct 2023 8:13:26 PM +...
CR300-1N1S-4TX2_203-5...	CR300-1N1S-4TX2_203-5...	Cisco VPN Interface Ethernet	CR300-1N1S-4TX2	3	global	2	Provider-swdev-order-mf	04 Oct 2023 8:15:07 PM +...
CR300-1N1S-4TX2_203-5...	CR300-1N1S-4TX2_203-5...	Cisco VPN Interface Ethernet	CR300-1N1S-4TX2	3	global	2	Provider-swdev-order-mf	04 Oct 2023 8:17:18 PM +...
CR300-1N1S-4TX2_208-1...	CR300-1N1S-4TX2_208-1...	WAN Edge sd-WAN Cellular In...	CR300-1N1S-4TX2	3	global	2	Provider-swdev-order-mf	05 Oct 2023 1:38:10 PM +...
CR300-1N1S-4TX2_301-4...	CR300-1N1S-4TX2_301-4...	CLI Template	CR300-1N1S-4TX2	1	global	1	Provider-swdev-order-mf	05 Oct 2023 1:33:04 PM +...
ISR1100X-6S_202-11_VPN...	ISR1100X-6S_202-11_VPN...	Cisco VPN	ISR1100X-6S (Cisco OS)	6	global	1	Provider-swdev-order-mf	05 Oct 2023 2:44:51 PM +...
CR300-1N1S-4TX2_303-1...	CR300-1N1S-4TX2_303-1...	Cellular Controller	CR300-1N1S-4TX2	3	global	2	Provider-swdev-order-mf	05 Oct 2023 1:38:41 PM +...
ISR1100X-6S_202-23_VPN...	ISR1100X-6S_202-23_VPN...	Cisco VPN	ISR1100X-6S (Cisco OS)	6	global	1	Provider-swdev-order-mf	05 Oct 2023 2:23:44 PM +...
ISR1100X-6S_202-25_VPN...	ISR1100X-6S_202-25_VPN...	Cisco VPN	ISR1100X-6S (Cisco OS)	6	global	0	Provider-swdev-order-mf	05 Oct 2023 2:28:12 PM +...
ISR1100X-6S_203-51_VIF...	ISR1100X-6S_203-51_VIF...	Cisco VPN Interface Ethernet	ISR1100X-6S (Cisco OS)	5	global	1	Provider-swdev-order-mf	05 Oct 2023 1:15:26 AM +...

- 機種名に「C1111-8P」にチェックを入れ、「Cli Add-On Template」を選択
※タイプⅡの CPE へ設定する場合は「C1111-8PLTELA」にチェック
※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック
※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック
※NTT 東日本デフォルト提供の Cli Add-On Template がある場合は、デフォルト提供の Cli Add-On Template をコピーしてください

The screenshot shows the Cisco SD-WAN Templates page. The left sidebar contains a 'Select Devices' section with a search bar and a list of devices. The '01111-BP' device is highlighted with a red box. The main area displays 'OTHER TEMPLATES' in a grid. The '01-Add-On Template' is highlighted with a red box. The top navigation bar includes 'Cisco SD-WAN', 'Select Resource Group', and tabs for 'Configuration Groups', 'Feature Profiles', 'Device Templates', and 'Feature Resources'.

3. ①Template Name/Description に「DNS_Relay」入力
 - ②以下のように 6 行を入力
 - ③「Save」を選択
- ※DNS のアドレスは適宜変更してください



①

Template Name: DNS_Relay

Description: DNS_Relay

CLI CONFIGURATION

②

```

1 system
2 vbond {{vbond_fqdn}} port 12346
3
4 ip name-server vrf 10 8.8.8.8
5 ip domain lookup vrf 10 source-interface vlan10
6 ip dns server
7 interface GigabitEthernet0/0/0
8 no ipv6 address dhcp
9 ipv6 nd ra suppress all

```

③

Save

14. ※既存のコンフィグの中でも特に以下の設定は外さないようにお願いします。正常な通信ができなくなり、CPE 交換が必要となる可能性があります。

```

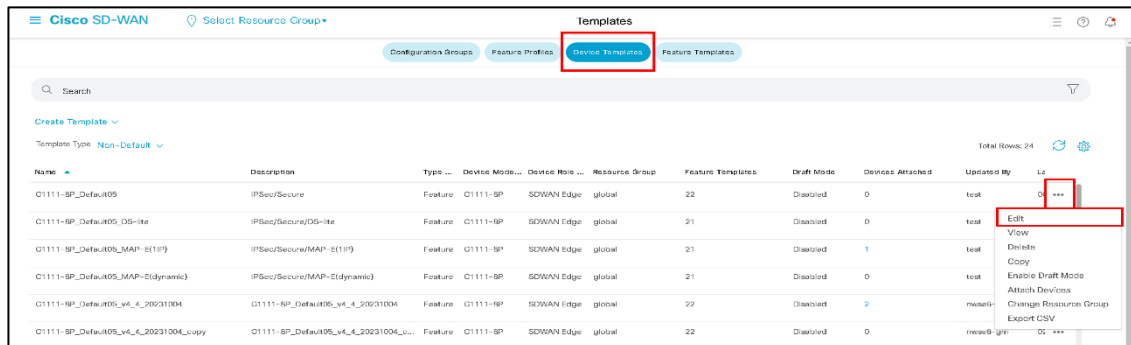
system
vbond {{vbond_fqdn}} port 12346
no ipv6 address dhcp
ipv6 nd ra suppress all

```

4.6.3. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

Device Template をコピー

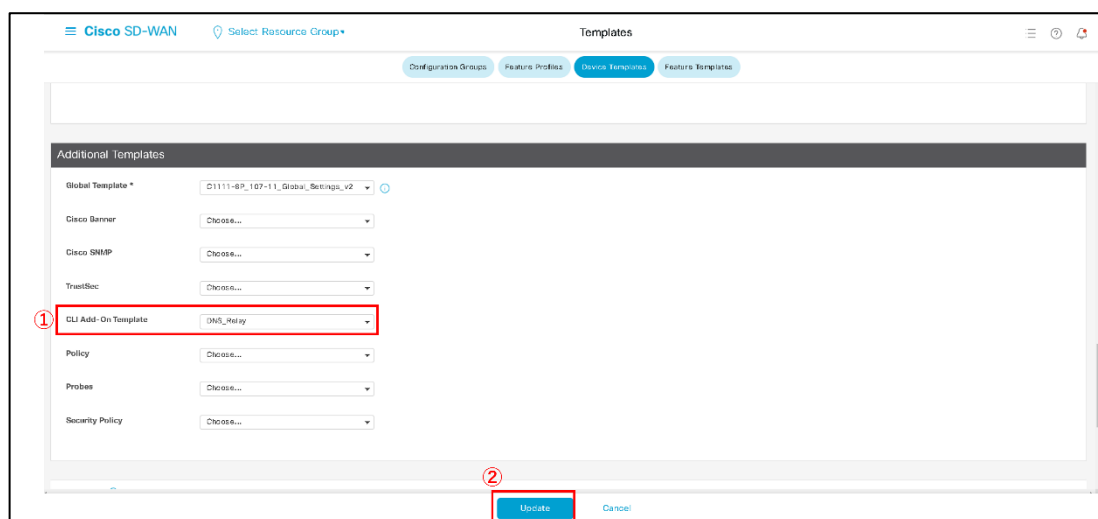
- 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Device Templates」を選択
NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択
※Template のコピーの手順は P10 を参照



4.6.4. Device Template に DNS サーバ用の Feature Template をアタッチ

Device Template を変更

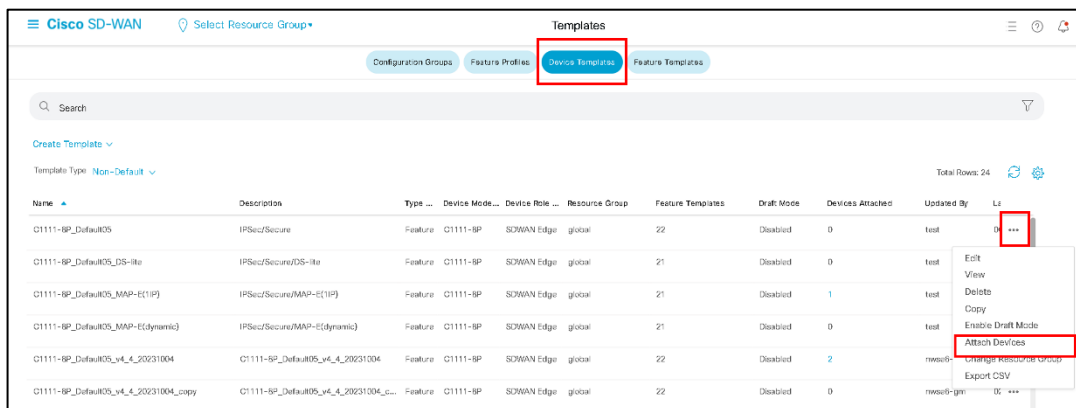
- ①Additional Templates 欄の CLI Add-On Templates を手順 1~3 で作成した「DNS Relay」へ変更
②「Update」を選択



4.6.5. 作成した Device Template を CPE にアタッチ

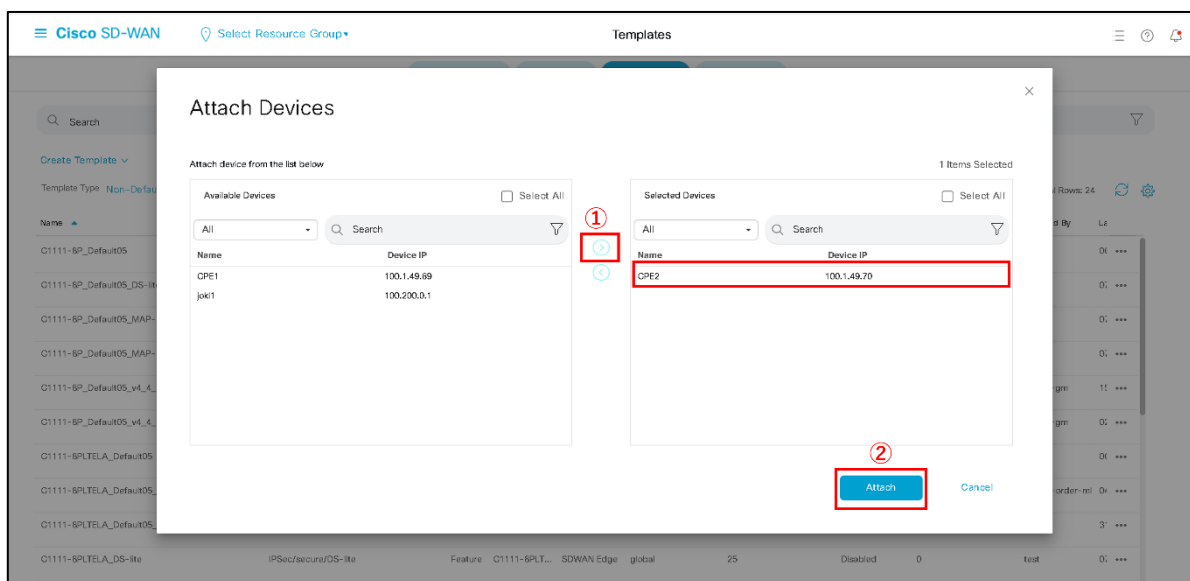
設定したい CPE へアタッチ

6. 新たに作成したテンプレートの「…」から「Attach Devices」を選択



7. ①適用したい CPE を選択し、「→」を選択し右ボックスに移動

②「Attach」を選択



8. 「Next」を選択

The screenshot shows the Cisco vManage Configuration Templates page. The page title is "Configuration - Templates". Below the title, there is a search bar and a table with columns: S. Chassis Number, System IP, Hostname, VLAN ID(g016_vlan), VLAN ID(g011_vlan), VLAN ID(g012_vlan), VLAN ID(g013_vlan), VLAN ID(g014_vlan), VLAN ID(g015_vlan), and VLAN ID(g017_v). The table contains one row with the following data: S. Chassis Number: C1111-8P-FGL2436LFAQ, System IP: 100.1.78.17, Hostname: CPE2, VLAN ID(g016_vlan): 10, VLAN ID(g011_vlan): 10, VLAN ID(g012_vlan): 10, VLAN ID(g013_vlan): 10, VLAN ID(g014_vlan): 20, VLAN ID(g015_vlan): 20, and VLAN ID(g017_v): 20. At the bottom right, there is a "Next" button highlighted with a red box and a "Cancel" button.

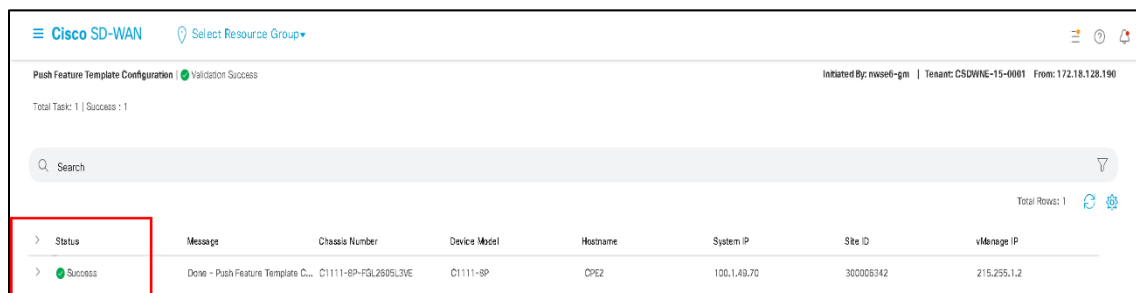
9. ①以下の画面で CPE を選択し、コンフィグを出力(Config Diff を選択すると差分表示が可能)
 - ②内容を確認し、「Configure Devices」を選択
- ※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を再確認して下さい

The screenshot shows the Cisco SD-WAN Templates page. The page title is "Templates". Below the title, there is a search bar and a table with columns: S. Chassis Number, System IP, Hostname, and various VLAN IDs. The table contains one row with the following data: S. Chassis Number: C1111-8P-FGL2436LFAQ, System IP: 100.1.78.17, Hostname: CPE2, VLAN ID(g016_vlan): 10, VLAN ID(g011_vlan): 10, VLAN ID(g012_vlan): 10, VLAN ID(g013_vlan): 10, VLAN ID(g014_vlan): 20, VLAN ID(g015_vlan): 20, and VLAN ID(g017_v): 20. At the bottom right, there is a "Next" button highlighted with a red box and a "Cancel" button.

10. Status が success, Message が Done となっていればコンフィグ適用が完了

※Status 変更までに 1 分程度かかります

※Status が success とならない場合、エラー内容及び手順を確認し時間を置いてリトライの実施をお願いします

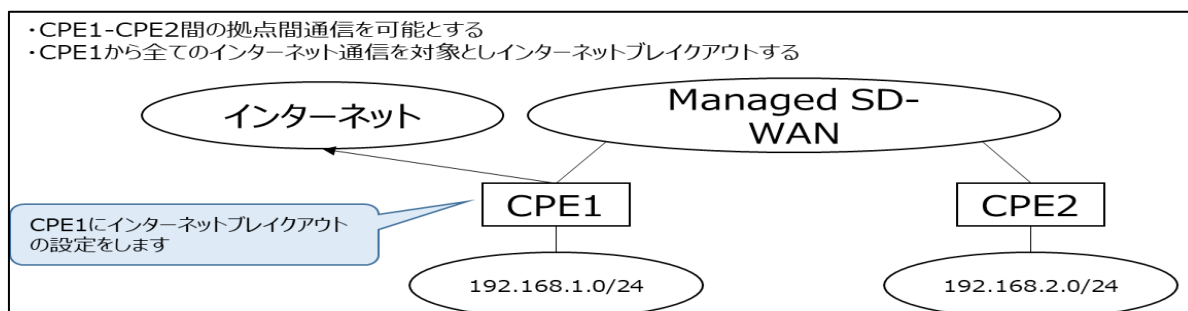


Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template C...	C1111-8P-FGL260SL3VE	C1111-8P	CPE2	100.1.49.70	300006342	215.255.1.2

4.7. インターネットブレイクアウト (全てのインターネット通信を対象)

拠点 CPE から全てのインターネット通信を対象とする場合のインターネットブレイクアウト設定について紹介します。

4.7.1. NW 構成例



【Device Template 作成に必要な Feature Template の作成】

作成する Feature Template	手順	用途
GE000	1～2	WAN インターフェース設定用
PPPoE	3～4	PPPoE 設定用
CLI_LBO	5～6	コマンド設定用
FW	7～21	セキュリティ設定用

【Device Template のコピー】

-	手順	用途
-	22	Device テンプレートのバックアップ

【Device Template への Feature Template の適用】

作成する Feature Template	手順	用途
GE000	23	WAN インターフェース設定用
PPPoE	23	PPPoE 設定用
CLI_LBO	23	コマンド設定用
FW	23	セキュリティ設定用

【Device Template への Feature Template の適用】

作成する Feature Template	手順	用途
GE000	24-30	WAN インターフェース設定用

【ポリシー作成に必要なとなる情報】

作成するポリシー	必要となる情報	手順	用途
LBO_Site	Site ID	31	ブレイクアウトさせる CPE の指定 ※5.1 章を参考に確認
LBO	Color	32	ブレイクアウト通信同士のトンネル接続を防ぐための Color の指定
LBO_VPN	VPN 番号	33	ブレイクアウトさせる VPN の指定 ※ VPN グループ数 1 の場合:10 VPN グループ数 1 の場合:10,20,30,40
LBO_Rule	CPE の NW アドレス	34~43	拠点間通信用ルール
LBO_Policy	LBO_Site LBO_VPN LBO_Rule	44~45	ポリシー設定用

【デフォルトトポロジのコピーと LBO 接続制限トポロジの新規作成】

コピーしたトポロジ	手順	用途
Topology_East_v3_copy	46-48	トポロジのバックアップと新規作成

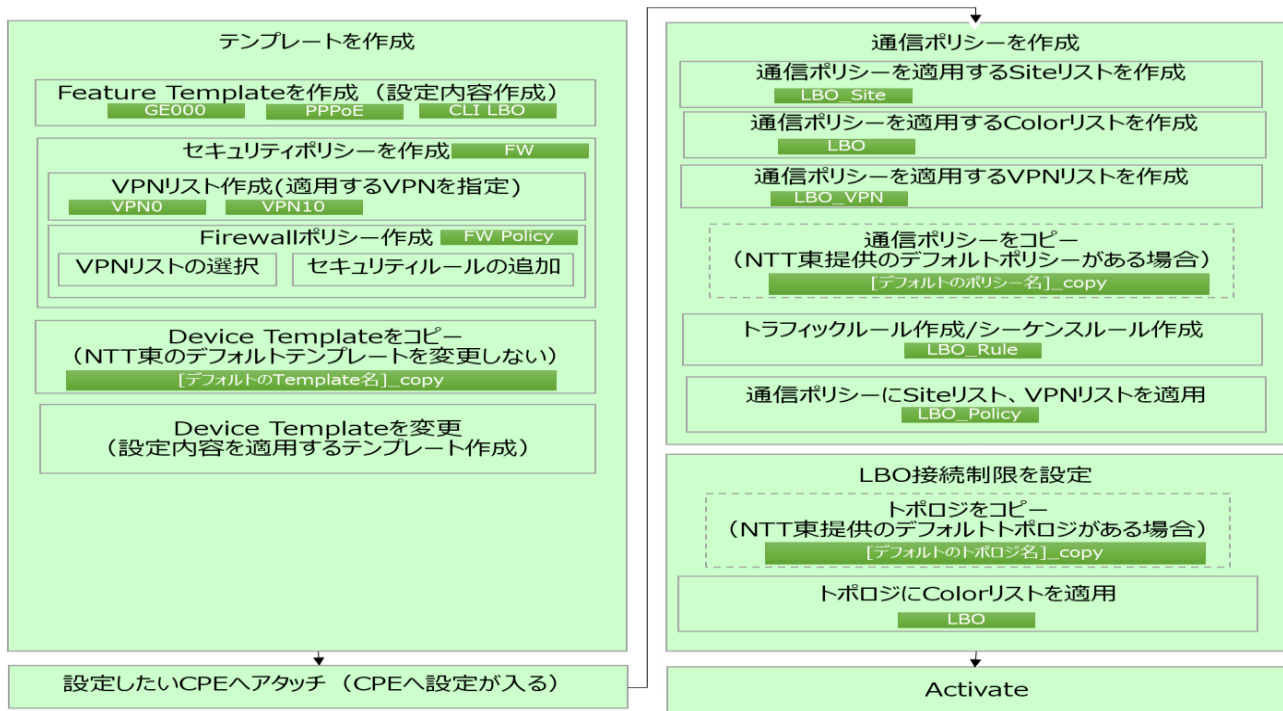
【LBO 接続制限トポロジへの Color-List の適用】

適用する Color-List	手順	用途
LBO	49-51	LBO の接続制限

【ポリシーへ LBO 接続制限トポロジの適用】

適用するトポロジ	手順	用途
Topology_East_v3_copy	52-57	LBO 接続制限

【設定の流れ】



注意: PPPoE のテンプレートをアタッチすると、デタッチできなくなります
PPPoE のデタッチ方法は別途提示予定となります

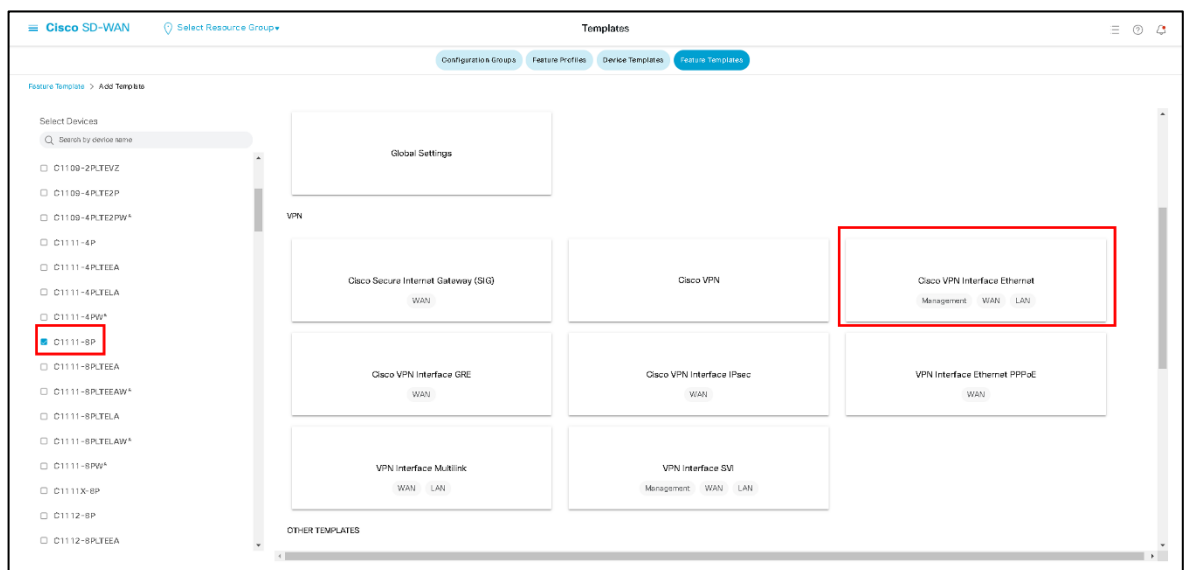
4.7.2. WAN インターフェース用 Feature Template を作成

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択
「Add Template」を選択

Feature Template を作成
GE000

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
ISR1100X-4G_202-22_VPN...	ISR1100X-4G_202-22_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	03 Oct 2023 2:23:18 PM
C8300-1N1S-4T2X_203-7...	C8300-1N1S-4T2X_203-7...	Cisco VPN Interface Ethernet	C8300-1N1S-4T2X	1	global	1	Provider-sdwan-order-mi	05 Oct 2023 1:30:59 PM
C8300-1N1S-4T2X_203-5...	C8300-1N1S-4T2X_203-5...	Cisco VPN Interface Ethernet	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:13:28 PM
C8300-1N1S-4T2X_203-5...	C8300-1N1S-4T2X_203-5...	Cisco VPN Interface Ethernet	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:15:37 PM
C8300-1N1S-4T2X_203-5...	C8300-1N1S-4T2X_203-5...	Cisco VPN Interface Ethernet	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:17:19 PM
C8300-1N1S-4T2X_206-1...	C8300-1N1S-4T2X_206-1...	WAN Edge (Edge Cellular in...	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	05 Oct 2023 1:38:10 PM
C8300-1N1S-4T2X_301-4...	C8300-1N1S-4T2X_301-4...	CLI Templates	C8300-1N1S-4T2X	1	global	1	Provider-sdwan-order-mi	03 Oct 2023 1:33:04 PM
ISR1100X-4G_202-11_VPN...	ISR1100X-4G_202-11_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:24:51 PM
C8300-1N1S-4T2X_303-1...	C8300-1N1S-4T2X_303-1...	Cellular Controller	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-mi	05 Oct 2023 1:38:41 PM
ISR1100X-4G_202-23_VPN...	ISR1100X-4G_202-23_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	03 Oct 2023 2:25:14 PM
ISR1100X-4G_202-25_VPN...	ISR1100X-4G_202-25_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	1	global	0	Provider-sdwan-order-mi	05 Oct 2023 2:26:12 PM
ISR1100X-4G_203-51_VF...	ISR1100X-4G_203-51_VF...	Cisco VPN Interface Ethernet	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 1:10:26 AM

2. 機種名は「C1111-8P」にチェックを入れ、「Cisco VPN Interface Ethernet」を選択



※タイプ II の CPE へ設定する場合は「C1111-8PLTELA」にチェック

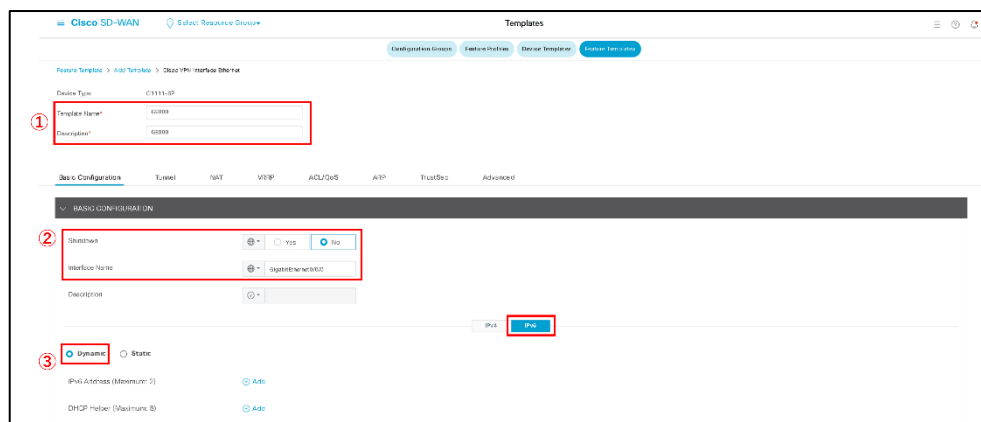
※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック

※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック

(トンネリングプロトコルが GRE の場合)

- ①Template Name/Description に「GE000」を入力
 - ②Shutdown を Global で「No」、Interface Name を Global で「GigabitEthernet0/0/0」を入力(プルダウンから「GigabitEthernet0/」を選択後「0/0」を手入力し欄外をクリック)
 - ③IPv6 を「Dynamic」と入力
 - ④Tunnel Interface を Global で「On」と入力
 - ⑤Color を Global で「public-internet」と入力
 - ⑥Maximum Control Connections を Global で「0」と入力
 - ⑦vManage Connection Preference を Global で「1」と入力
 - ⑧GRE を Global で「On」と入力
 - ⑨GRE Preference を Global で「100」と入力
 - ⑩IPsec を Global で「Off」と入力
- 最後に「Save」を選択

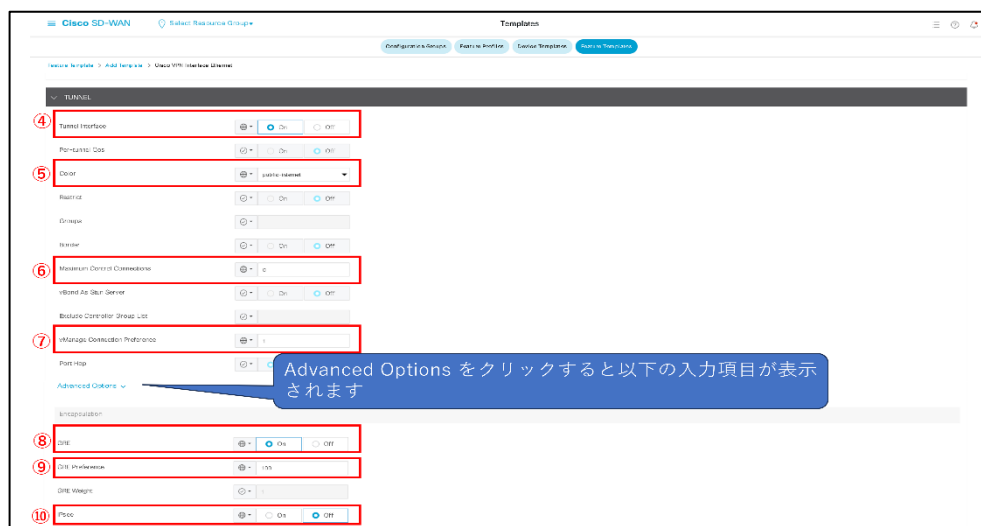
※IPv6 の「Dynamic」設定は「Static」にしないでください。必ず「Dynamic」になっていることを確認願います。正常な通信ができなくなり、CPE 交換が必要となる可能性があります。



① Template Name: GE000, Description: GE000

② Shutdown: No, Interface Name: GigabitEthernet0/0/0

③ IPv6: Dynamic



④ Tunnel Interface: On

⑤ Color: public-internet

⑥ Maximum Control Connections: 0

⑦ vManage Connection Preference: 1

⑧ GRE: On

⑨ GRE Preference: 100

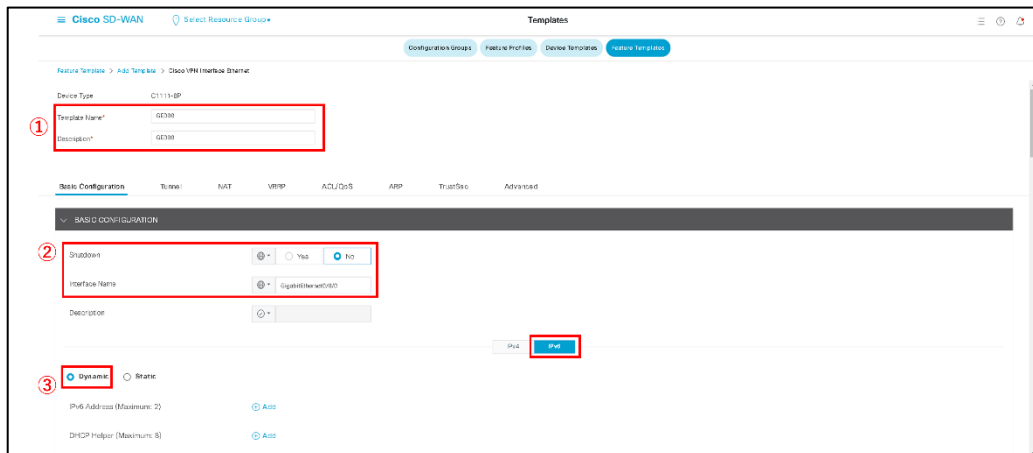
⑩ IPsec: Off

Advanced Options をクリックすると以下の入力項目が表示されます

(トンネリングプロトコルが IPsec の場合)

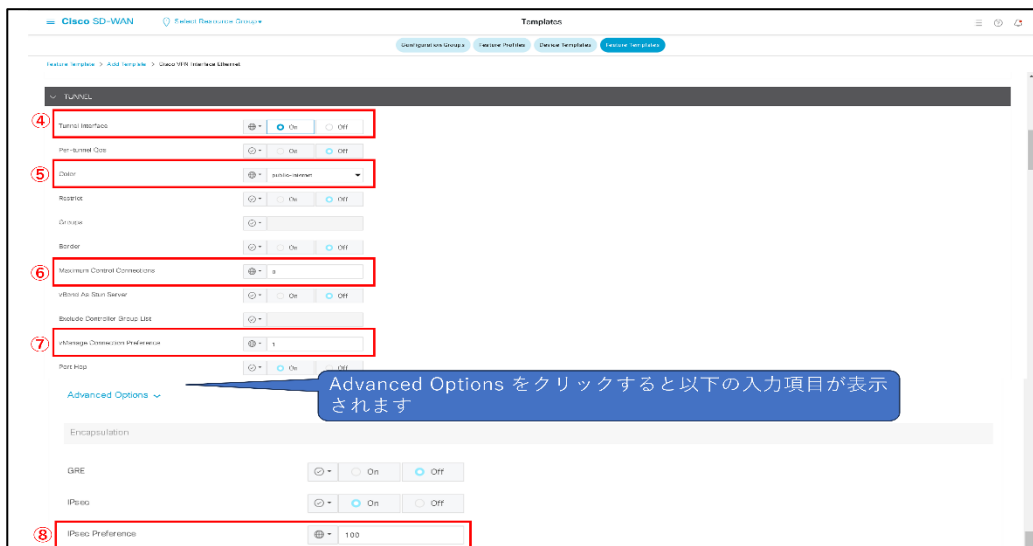
- ① Template Name/Description に「GE000」を入力
 - ② Shutdown を Global で「No」、Interface Name を Global で「GigabitEthernet0/0/0」を入力(プルダウンから「GigabitEthernet0/」を選択後「0/0」を手入力し欄外をクリック)
 - ③ IPv6 を「Dynamic」と入力
 - ④ Tunnel Interface を Global で「On」と入力
 - ⑤ Color を Global で「public-internet」と入力
 - ⑥ Maximum Control Connections を Global で「0」と入力
 - ⑦ vManage Connection Preference を Global で「1」と入力
 - ⑧ IPsec Preference を Global で「100」と入力
- 最後に「Save」を選択

※IPv6 の「Dynamic」設定は「Static」にしないでください。必ず「Dynamic」になっていることを確認願います。正常な通信ができなくなり、CPE 交換が必要となる可能性があります。



The screenshot shows the 'Basic Configuration' tab of the Cisco SD-WAN Templates page. The following fields are highlighted with red boxes and numbered:

- ① Template Name and Description: Both are set to 'GE000'.
- ② Shutdown: Set to 'No'.
- Interface Name: Set to 'GigabitEthernet0/0/0'.
- ③ Dynamic: The 'Dynamic' radio button is selected for IPv6.



The screenshot shows the 'Tunnel' tab of the Cisco SD-WAN Templates page. The following fields are highlighted with red boxes and numbered:

- ④ Tunnel Interface: Set to 'On'.
- ⑤ Color: Set to 'public-internet'.
- ⑥ Maximum Control Connections: Set to '0'.
- ⑦ vManage Connection Preference: Set to '1'.
- ⑧ IPsec Preference: Set to '100'.

A blue callout box points to the 'Advanced Options' section, stating: "Advanced Options をクリックすると以下の入力項目が表示されます"

4.7.3. PPPoE 用 Feature Template を作成

Feature Template を作成 PPPoE

3. 左ペイン(左の領域)の Configuration から「Templates」を選択後、画面上部のタブから「Feature」を選択

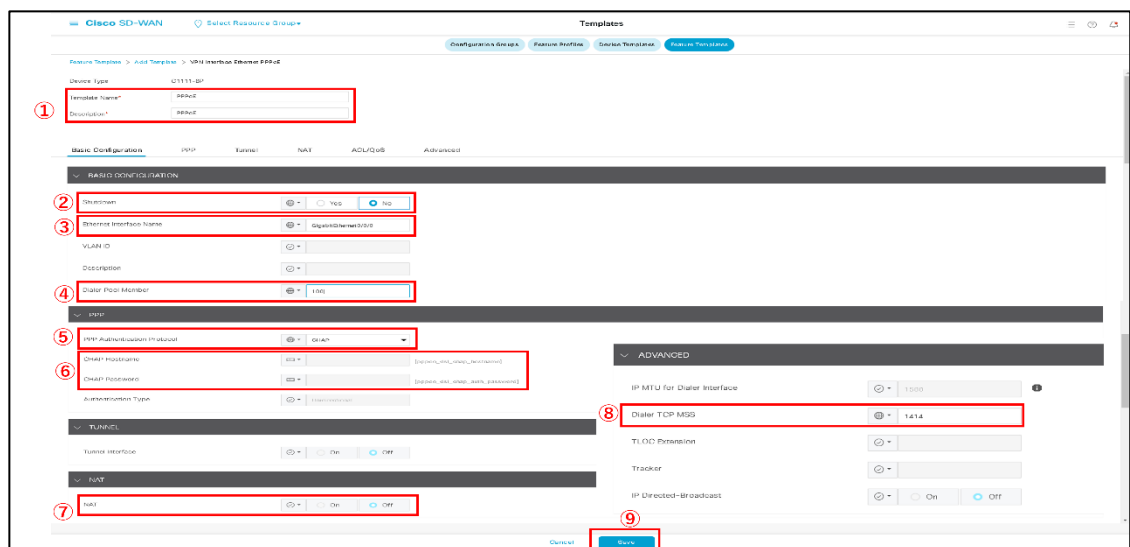
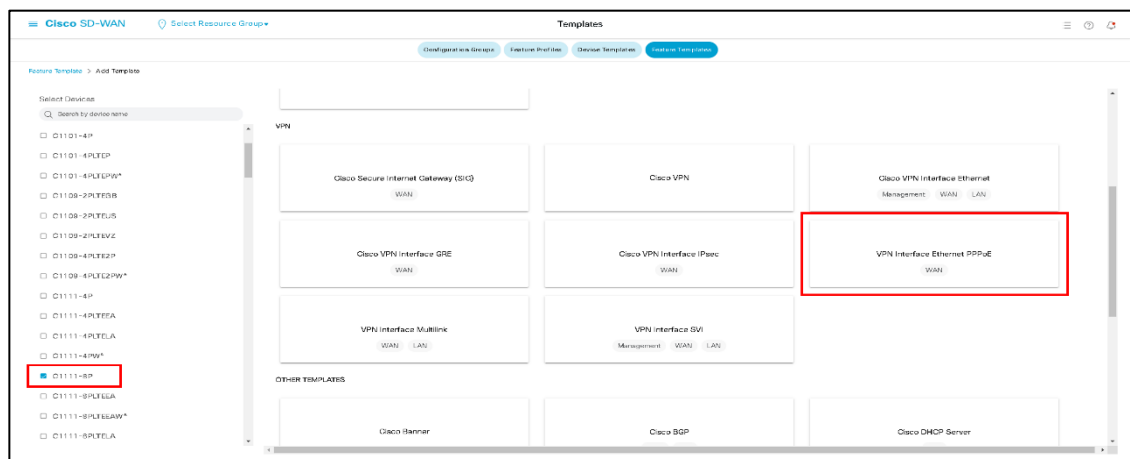
「Add Template」を選択

機種名は「C1111-8P」にチェックを入れ、「VPN Interface Ethernet PPPoE」を選択

※タイプⅡの CPE へ設定する場合は「C1111-8PLTELA」にチェック

※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック

※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック



4. ①Template Name/Description に「PPPoE」を入力
- ②Shutdown を Global で「No」と入力
- ③Ethernet Interface Name を Global で「GigabitEthernet0/0/0(手入力)」と入力
- ④Dialer Pool Member を Global で「100」と入力
- ⑤PPP Authentication Protocol を Global で「CHAP」と入力
- ⑥CHAP Hostname/CHAP Password を「Device Specific」と入力
- ⑦NAT を Global で「On」と入力
- ⑧TCP MSS を Global で「1414」と入力
- ⑨「Save」を選択

4.7.4. インターネットブレイクアウト用コマンド Feature Template を作成

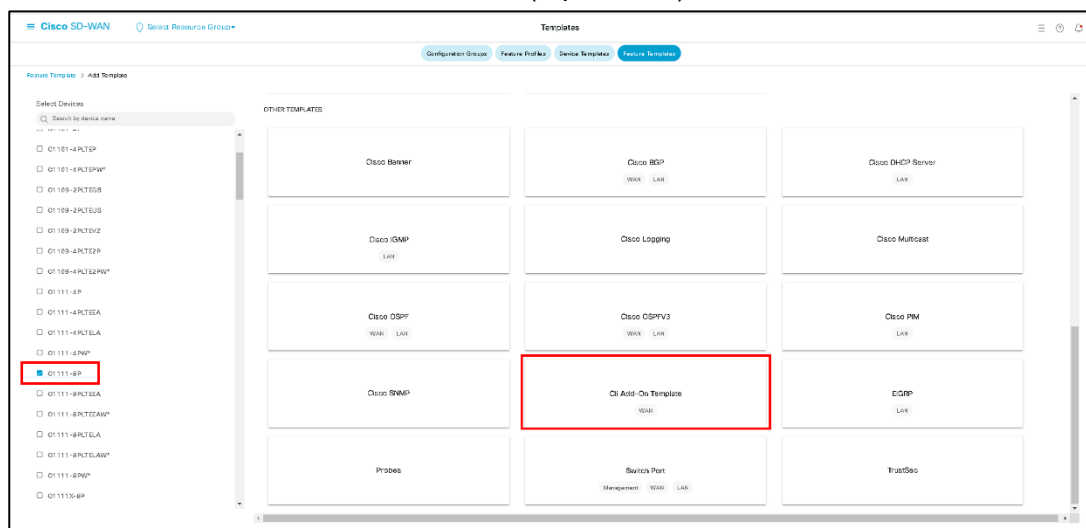
5. 手順 1 に則り Feature Template を新規作成

機種名は「C1111-8P」にチェックを入れ、「CLI Add-On Template」を選択

※タイプ II の CPE へ設定する場合は「C1111-8PLTELA」にチェック

※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック

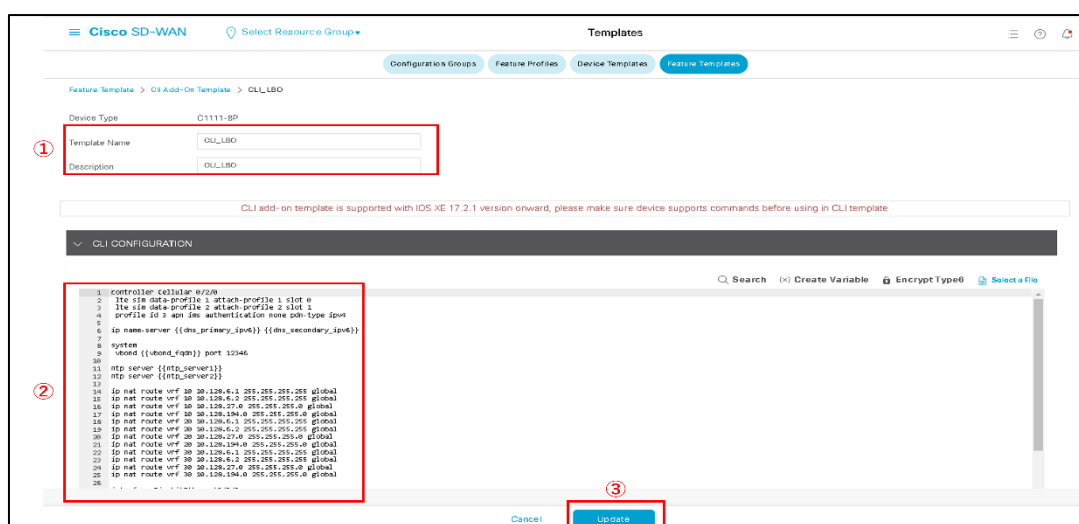
※ミドルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック



6. ①Template Template Name/Description へ「CLI_LBO」を入力

②CLI CONFIGURATION に以下を入力

③「Save」を選択



【GRE の場合のコマンド】

```
system
vbond {{vbond_fqdn}} port 12346
ip name-server {{dns_primary_ipv6}} {{dns_secondary_ipv6}}
interface Tunnel1
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/0/0
  no ipv6 redirects
  tunnel source GigabitEthernet0/0/0
  tunnel mode sdwan
exit

interface Dialer100
  ip mtu 1454
  ip tcp adjust-mss 1414
exit

interface GigabitEthernet0/0/0
  no ipv6 address dhcp
  ipv6 nd ra suppress all
  no ip nat outside
exit

sdwan
interface GigabitEthernet0/0/0
  tunnel-interface
  encapsulation gre preference 100 weight 1
  no border
  color {{gi000_color}} restrict
  no last-resort-circuit
  no low-bandwidth-link
  max-control-connections 2
  no vbond-as-stun-server
  vmanage-connection-preference 8
  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
```

※以下の設定は外さないようにお願いします。正常な通信ができなくなり、CPE 交換が必要となる可能性があります。

```
system
vbond {{vbond_fqdn}} port 12346
no ipv6 address dhcp
ipv6 nd ra suppress all
```

【IPsec の場合のコマンド】

```
system
vbond {{vbond_fqdn}} port 12346
ip name-server {{dns_primary_ipv6}} {{dns_secondary_ipv6}}
interface Tunnel1
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/0/0
  no ipv6 redirects
  tunnel source GigabitEthernet0/0/0
  tunnel mode sdwan
exit

interface Dialer100
  ip mtu 1454
  ip tcp adjust-mss 1414
exit

interface GigabitEthernet0/0/0
  no ipv6 address dhcp
  ipv6 nd ra suppress all
  no ip nat outside
exit

sdwan
interface GigabitEthernet0/0/0
  tunnel-interface
  encapsulation ipsec preference 100 weight 1
  no border
  color {{gi000_color}} restrict
  no last-resort-circuit
  no low-bandwidth-link
  max-control-connections 2
  no vbond-as-stun-server
  vmanage-connection-preference 8
  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
```

※以下の設定は外さないようにお願いします。正常な通信ができなくなり、CPE 交換が必要となる可能性があります。

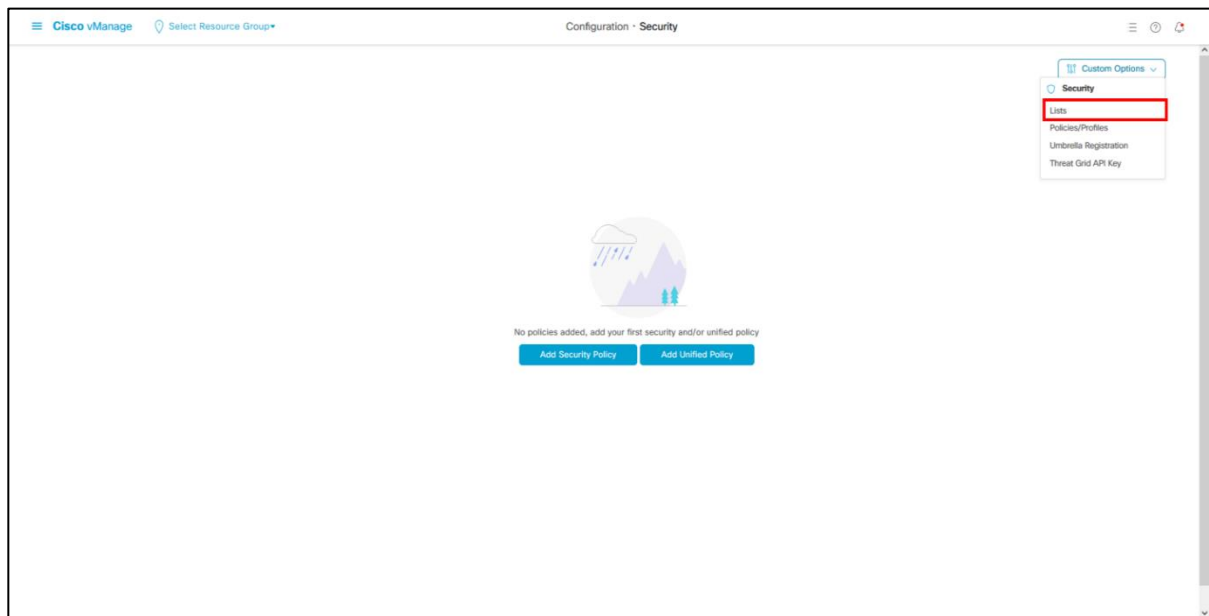
```
system
vbond {{vbond_fqdn}} port 12346
no ipv6 address dhcp
ipv6 nd ra suppress all
```

4.7.5. インターネットブレイクアウト用セキュリティポリシーを作成

セキュリティポリシーを作成

FW

7. 左ペイン(左の領域)の Configuration から「Security」を選択
画面上部の「Custom Options」から「Lists」を選択



8. 左側メニューの「Zones」を選択し、「New Zone List」を選択



9. ①Zone List Name へ「VPN0」を入力
- ②Add VPN に「0」を入力
- ③「Add」を選択



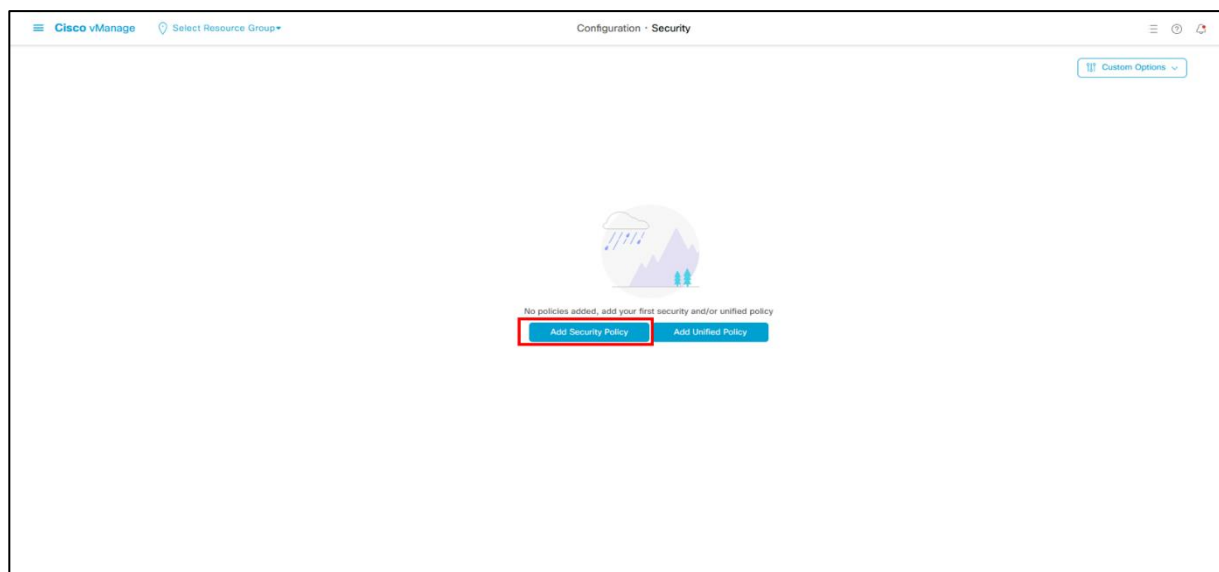
10. ①「New Zone List」を選択
- ②Zone List Name へ「VPN10」を入力
- ③Add VPN に「10」を入力
- ※VPN を追加している場合は追加した VPN 番号も入力
- ※セキュアインターネット、もしくはクロスコネクトを申し込みしている場合は、VPN 番号 9999 も固定で入力

(Ex. VPN20 を追加した場合: 「10,20」と入力、
VPN20 を追加+セキュアインターネット
or クロスコネクト申込の場合: 「10,20,9999」と入力。)

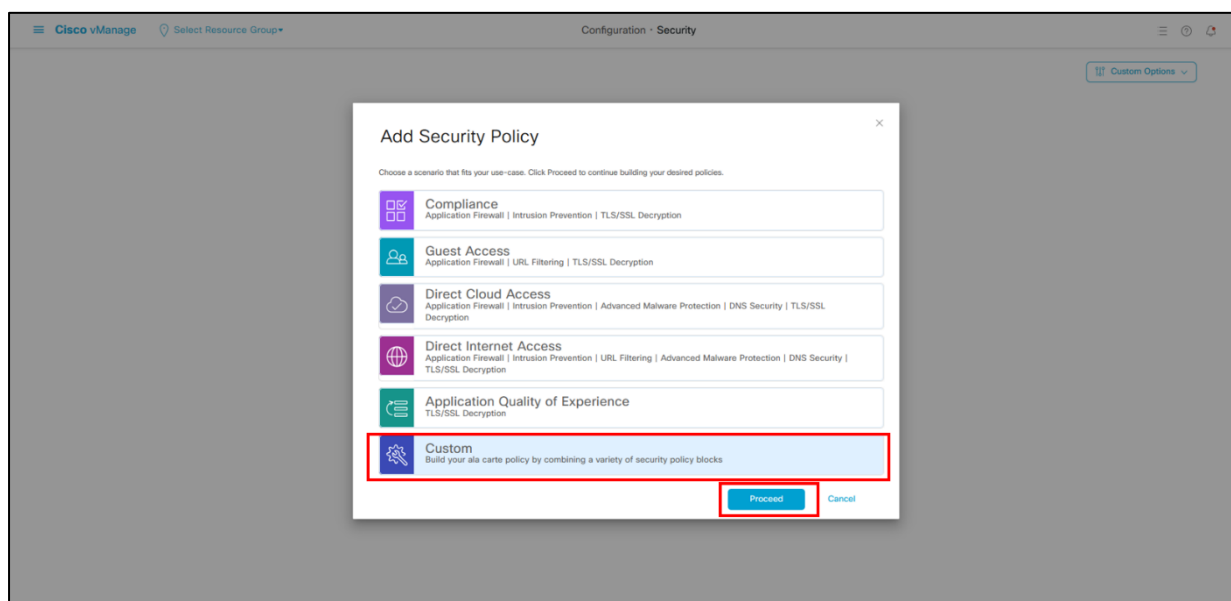
- ④「Add」を選択



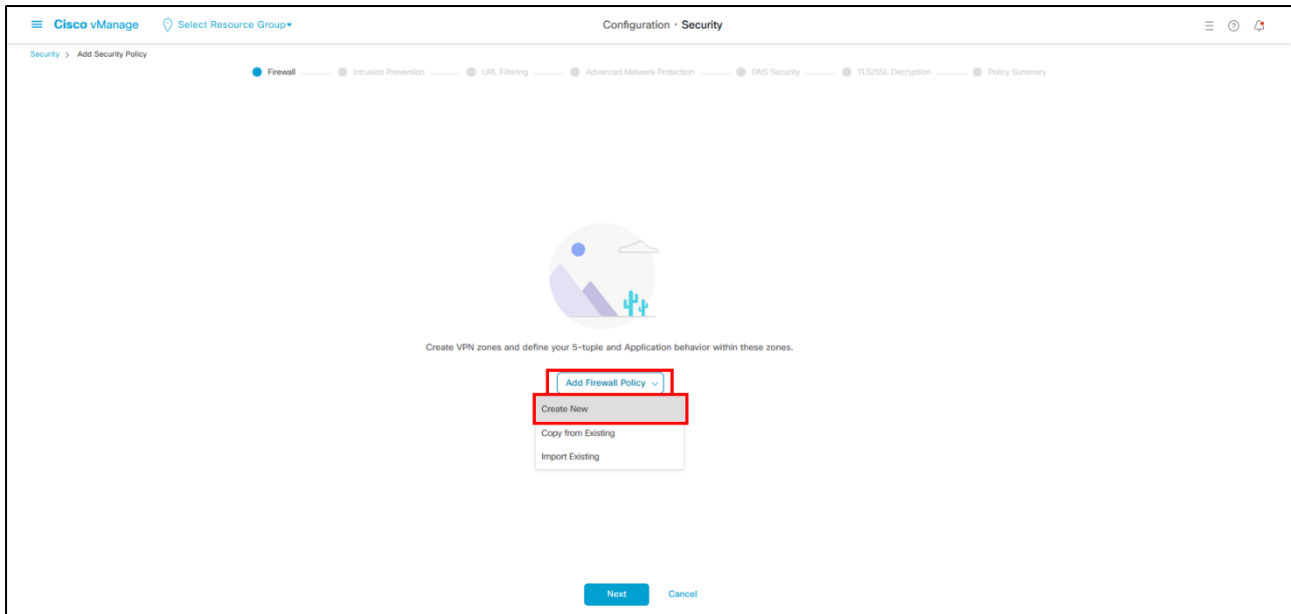
11. 左ペイン(左の領域)の Configuration から「Security」を選択
「Add Security Policy」を選択



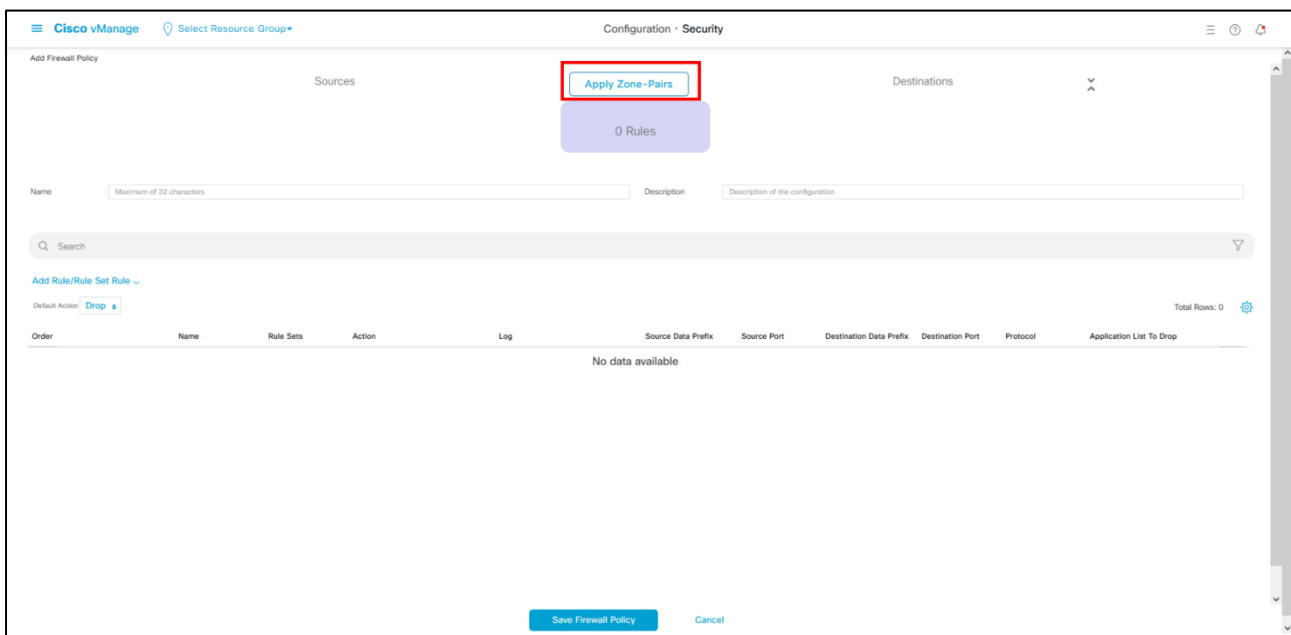
12. 「Custom」を選択し、「Proceed」を選択



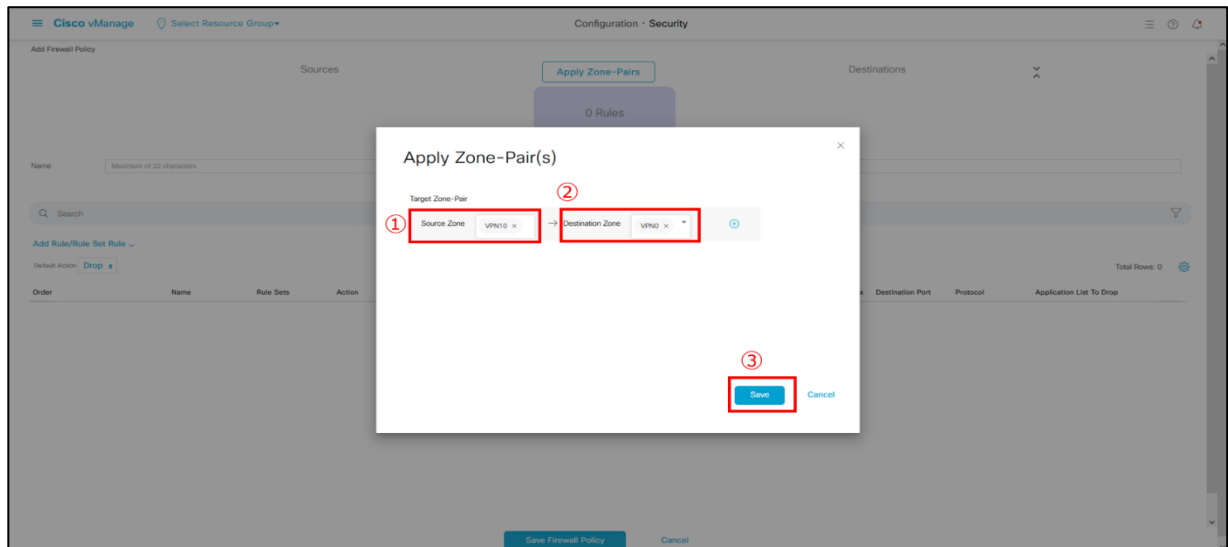
13. 「Add Firewall Policy」を選択し、「Create New」を選択



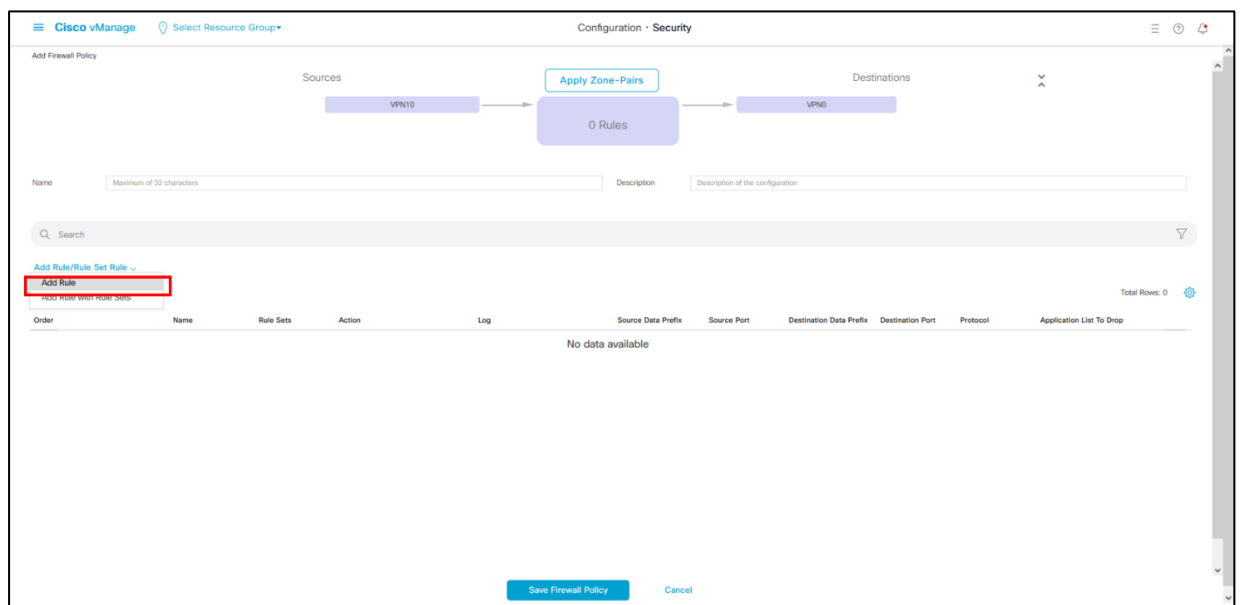
14. 「Apply Zone-Pairs」を選択



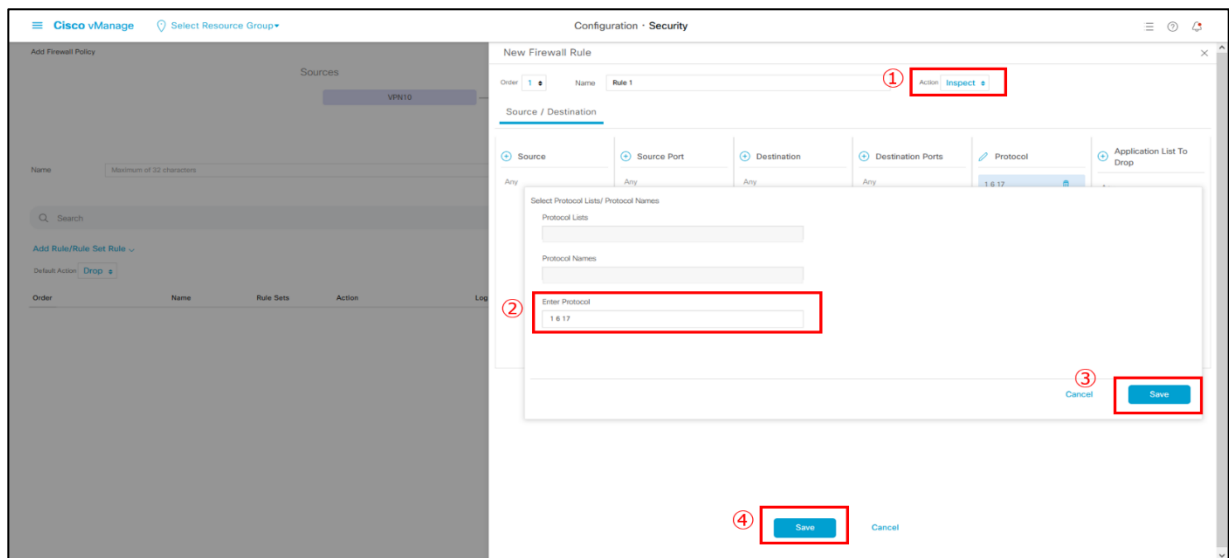
15. ① 「Source Zone」 に「VPN10」 を選択
- ② 「Destination Zone」 に「VPN0」 を選択
- ③ 「Save」 を選択



16. 「Add Rule」 を選択



17. ①Action を「Inspect」に変更
- ②「Protocol」を選択し、「Enter Protocol」に「1 6 17」を入力
※1,6,17の間は半角スペース
- ③「Save」を選択
- ④「Save」を選択

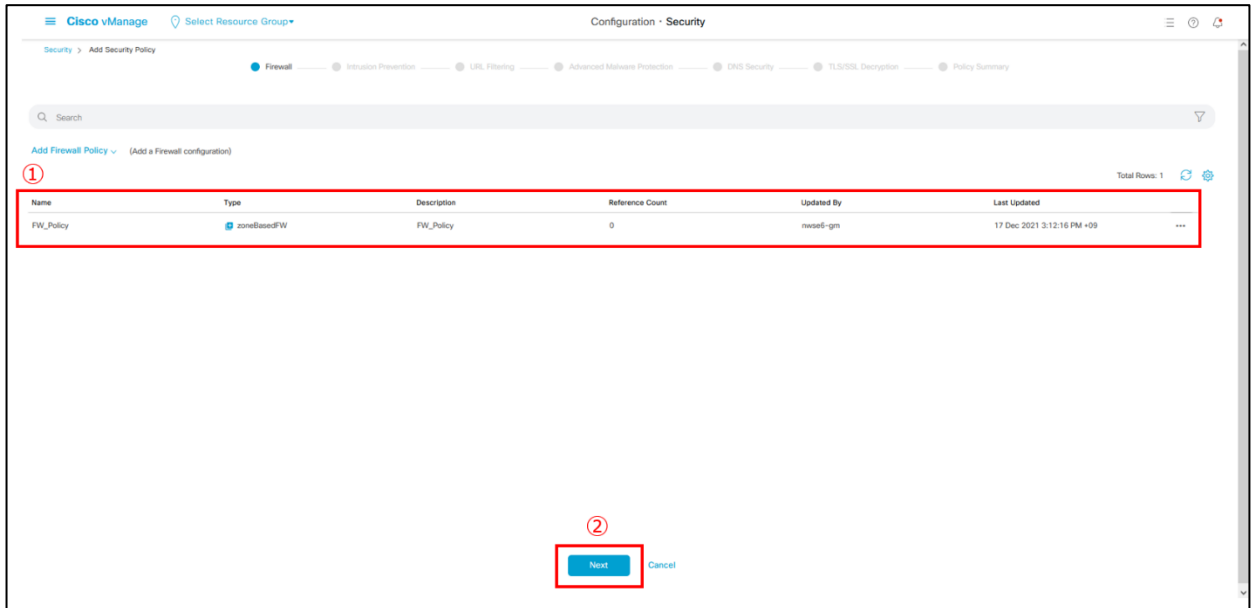


18. ①Name および Description に「FW_Policy」を入力
- ②「Save Firewall Policy」を選択



19. ①設定したポリシーがあることを確認

②「Next」を選択



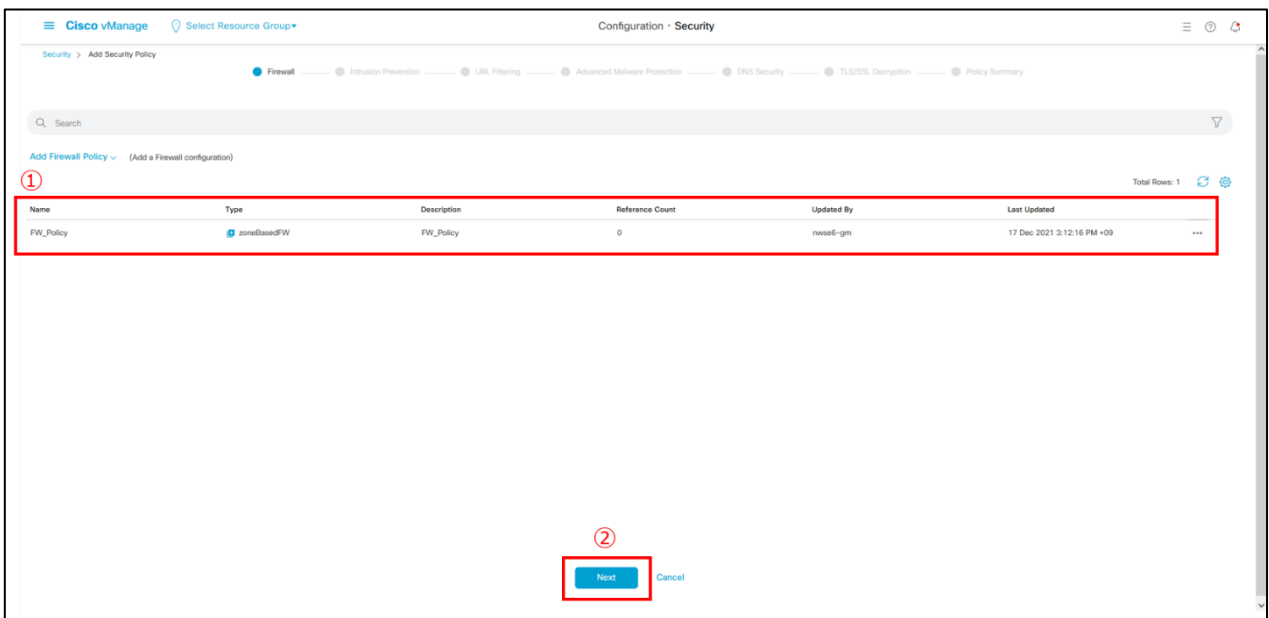
The screenshot shows the Cisco vManage interface for configuring security policies. The breadcrumb trail is "Configuration > Security". The "Add Firewall Policy" section is active, showing a table with one row. A red box highlights the table row, and a red circle with the number 1 is next to it. At the bottom, a red box highlights the "Next" button, with a red circle and the number 2 next to it.

Name	Type	Description	Reference Count	Updated By	Last Updated
FW_Policy	zoneBasedFW	FW_Policy	0	nwse6-gm	17 Dec 2021 3:12:16 PM +09

Next Cancel

20. ①設定したポリシーがあることを確認

②「Next」を選択(手順 21 の画面まで Next を 6 回選択し続ける)



This screenshot is identical to the one in step 19, showing the same table and "Next" button. It is included to illustrate the next step in the process.

Name	Type	Description	Reference Count	Updated By	Last Updated
FW_Policy	zoneBasedFW	FW_Policy	0	nwse6-gm	17 Dec 2021 3:12:16 PM +09

Next Cancel

21. ①Security Policy Name および Security Policy Description は「FW」を入力
②「Save Policy」を選択

4.7.6. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

Device Template をコピー

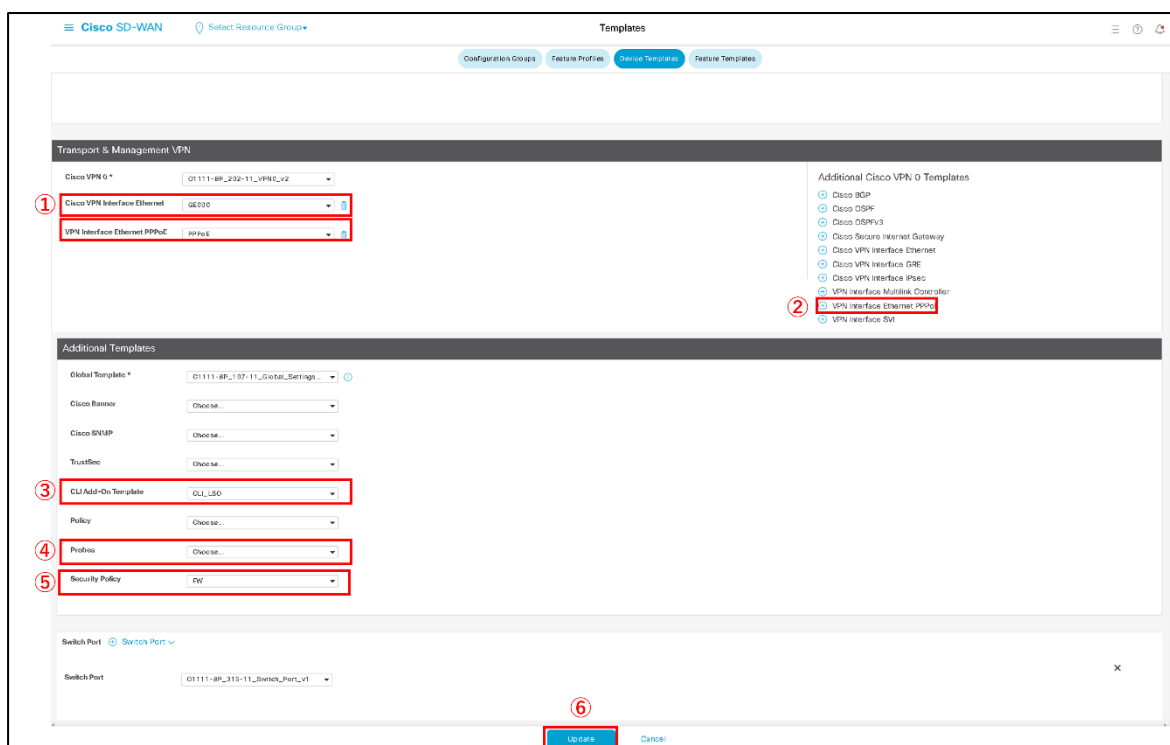
22. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Devices」を選択
NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	...
C1111-BP_Default05	IPSec/Secure	Feature	C1111-BP	SDWAN Edge	global	22	Disabled	0	test	...
C1111-BP_Default05_DS-lite	IPSec/Secure/DS-lite	Feature	C1111-BP	SDWAN Edge	global	21	Disabled	0	test	Edit
C1111-BP_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-BP	SDWAN Edge	global	21	Disabled	1	test	View
C1111-BP_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-BP	SDWAN Edge	global	21	Disabled	0	test	Delete
C1111-BP_Default05_v4_4_20231004	C1111-BP_Default05_v4_4_20231004	Feature	C1111-BP	SDWAN Edge	global	22	Disabled	2	nws66	Copy
C1111-BP_Default05_v4_4_20231004_copy	C1111-BP_Default05_v4_4_20231004_c...	Feature	C1111-BP	SDWAN Edge	global	22	Disabled	0	nws66-gm	Enable Draft Mode

4.7.7. Device Template にインターネットブレイクアウト用の Feature Template をアタッチ

Device Template を変更

23. ①Cisco VPN Interface Ethernet に「GE000」を選択
- ②「VPN Interface Ethernet PPPoE」を選択
- ③VPN Interface Ethernet PPPoE に「PPPoE」を選択
- ④CLI Add-On Template に「CLI_LBO」を選択
- ⑤Security Policy に「FW」を選択
- ⑥「Update」を選択



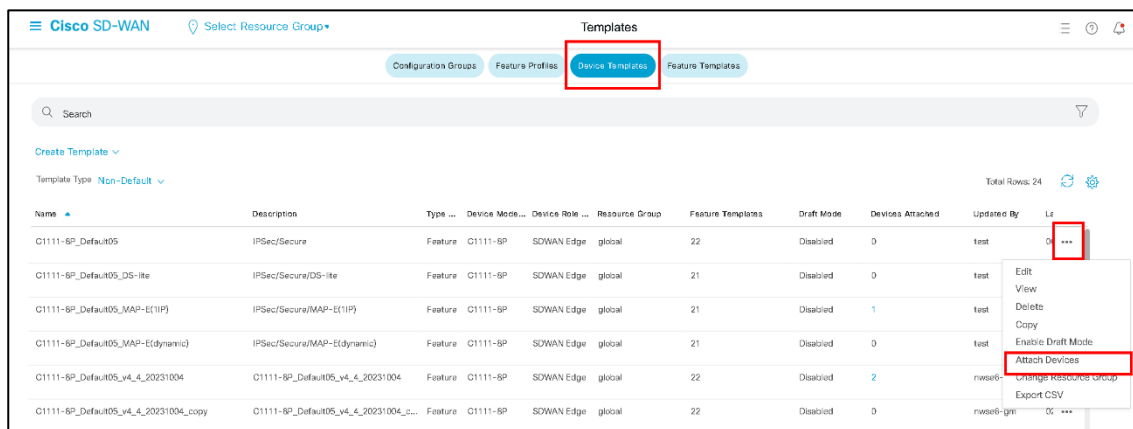
The screenshot shows the 'Templates' configuration page in the Cisco SD-WAN interface. The page is divided into several sections:

- Transport & Management VPN:** Contains dropdowns for 'Cisco VPN 0' (set to '0111-IP_232-11_VPN0_v2') and 'VPN Interface Ethernet PPPoE' (set to 'PPPoE').
- Additional Cisco VPN 0 Templates:** A list of templates on the right side, including 'Cisco BGP', 'Cisco OSPF', 'Cisco OSPFv3', 'Cisco Secure Internet Gateway', 'Cisco VPN Interface Ethernet', 'Cisco VPN Interface GRE', 'Cisco VPN Interface IPsec', 'VPN Interface Multilink Controller', 'VPN Interface Ethernet PPPoE' (highlighted with a red box and number 2), and 'VPN Interface SVI'.
- Additional Templates:** Contains dropdowns for 'Global Template' (set to '0111-IP_107-11_Global_Settings...'), 'Cisco Banner', 'Cisco SNMP', 'TrustSec', 'CLI Add-On Template' (set to 'CLI_LBO' and highlighted with a red box and number 3), 'Policy' (set to 'FW' and highlighted with a red box and number 4), 'Provision' (set to 'FW' and highlighted with a red box and number 5), and 'Security Policy' (set to 'FW' and highlighted with a red box and number 5).
- Switch Port:** A dropdown for 'Switch Port' (set to '0111-IP_315-11_Switch_Port_v1').
- Buttons:** At the bottom, there are 'Update' and 'Cancel' buttons. The 'Update' button is highlighted with a red box and number 6.

4.7.8. 作成した Device Template を CPE にアタッチ

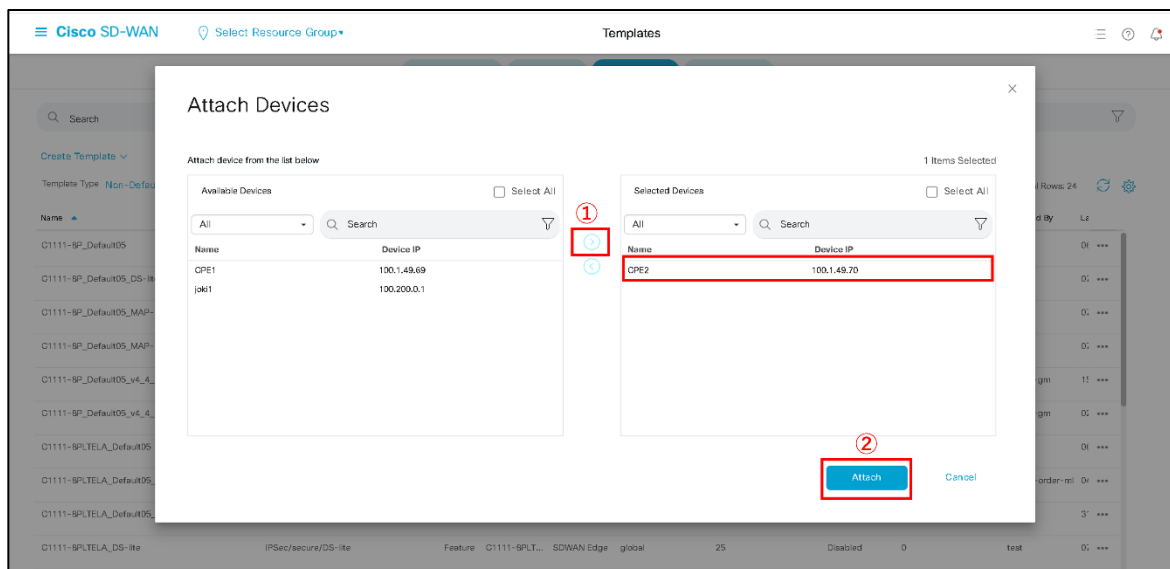
設定したい CPE へアタッチ

24. 手順 1~23 で作成した Template の「…」から「Attach devices」を選択



25. ①適用したい CPE を選択し、「→」を選択し右ボックスに移動

②「Attach」を選択



26. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択

Cisco SD-WAN

Select Resource Group

Templates

Device Template

C1111-8P_Default05_v4_4_20231004

Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	VLAN ID(gi010_vlan)	VLAN ID(gi011_vlan)	VLAN ID(gi012_vlan)	VLAN ID(gi013_vlan)	VLAN ID(gi014_vlan)	VLAN ID(gi015_vlan)	VLAN ID(gi016_vlan)
	C1111-8P-FGL2605L3VE	100.1.49.70	CPE2	10	10	10	10	10	10	10

...

Edit Device Template

27. ①dns_primary_ipv6/dns_secondary_ipv6 に「2404:1a8:7f01:a::3/2404:1a8:7f01:b::3」を入力

※西日本エリア拠点の場合は「2001:a7ff:5f01::a/2001:a7ff:5f01:1::a」を入力

②gi000 color に「private1」 (東日本エリア拠点の場合)を入力

※西日本エリア拠点の場合は「green」を入力

③CHAP Hostname および CHAP Password の値を入力

④「Update」を選択し、「Next」を選択

The screenshot displays the 'Update Device Template' page in the Cisco SD-WAN configuration tool. On the left, a sidebar shows a list of device templates, with 'C1111-SP-FGL2609L-DVE' selected. The main area is titled 'Update Device Template' and contains a 'Variable List' on the left and a table of values on the right. The variables and their values are as follows:

Variable List	Value
vsnr_tagout_v4_vary	10
VLAN ID(g015_vlan)	10
VLAN ID(g016_vlan)	10
VLAN ID(g017_vlan)	10
dns_primary_ipv6	2001:a7f:0101::a
dns_secondary_ipv6	2001:a7f:0101::a
vbond_fqdn	vbond15.vbondwan.cisco.net:8443-west.jp
ntp_server1	2001:a7f:0102::a
ntp_server2	2001:a7f:0102::a
gig00_color	primary1
IPv4 Address(vn30_ipv4_address)	10.30.1.254/24
IPv4 Address(vn20_ipv4_address)	10.20.1.254/24
IPv4 Address(vn10_ipv4_address)	192.168.2.254/24
CHAP Hostname(pppoe_sdl_chap_hostname)	asa@vsnr.net.jp
CHAP Password(pppoe_sdl_chap_auth_password)	--
Hostname(system_host_name)	OPE2
Device Group(system_device_group)	west
System IP(system_system_ip)	100.1.49.70
Site ID(system_site_id)	300006342

Four items are highlighted with red boxes and numbered 1 through 4:

- ntp_server1
- ntp_server2
- gig00_color
- CHAP Password(pppoe_sdl_chap_auth_password)

At the bottom right, there is a 'Generate Password' button, a '4' icon, and a 'Generate' button highlighted with a red box. A 'Cancel' button is also visible.

注: Color, Device group, System IP, Site ID はデフォルト値から変更すると通信ができなくなる恐れがあるため、変更しないようお願いいたします

28. ①以下の画面で CPE を選択し、コンフィグを出力(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を確認願います

29. Status が success, Message が Done となっていればコンフィグ適用が完了

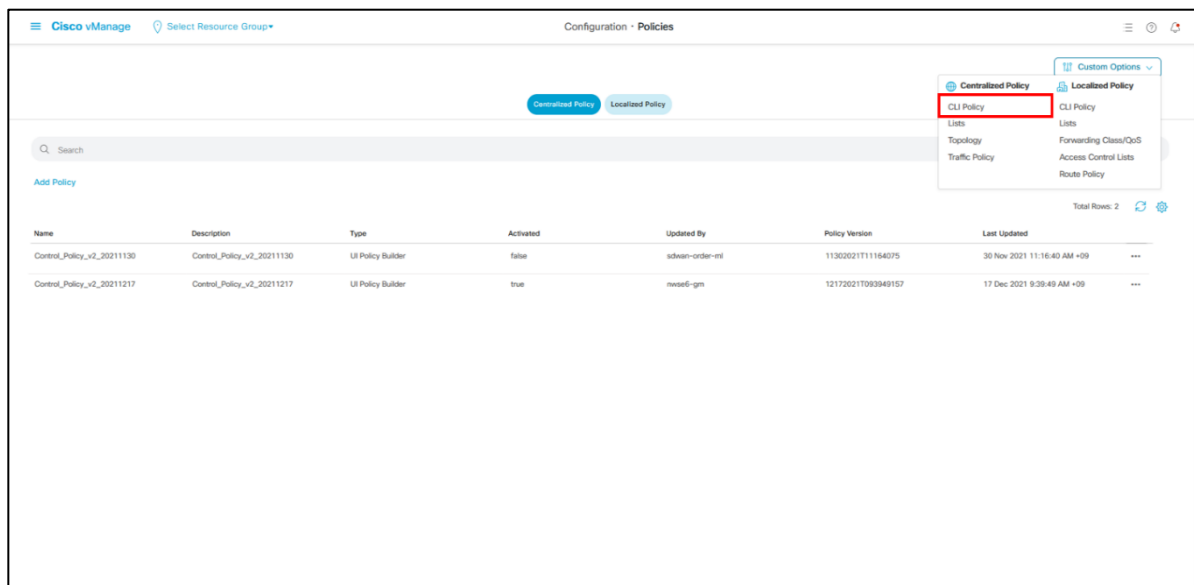
※Status が success とならない場合、エラー内容及び手順を確認し時間を置いてリトライの実施をお願いします

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template C...	C1111-8P-FGL2605L3VE	C1111-8P	CPE2	100.1.48.70	300006342	215.255.1.2

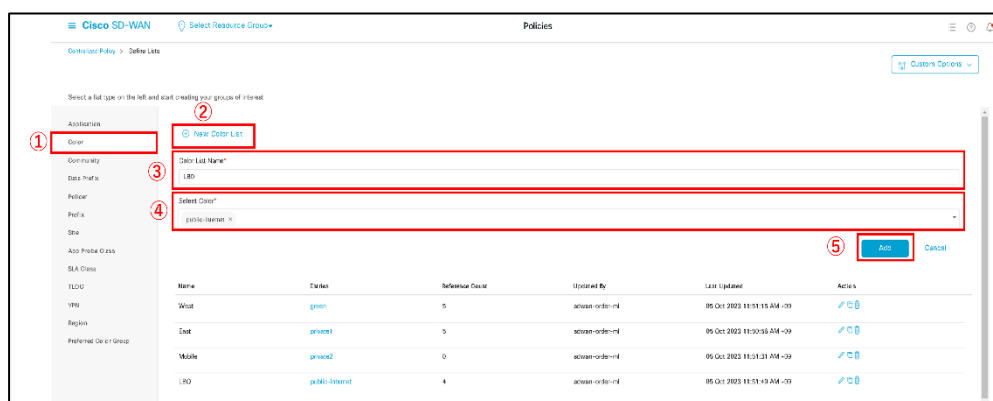
4.7.9. インターネットブレイクアウト用通信ポリシーを作成

通信ポリシー作成

30. 左ペイン(左の領域)の Configuration から「Policies」を選択
画面上部の「Custom Options」から「Lists」を選択



31. ①「Color」を選択
②「New Color List」を選択
③Color List Name は「LBO」を入力
④Select Color は「public-internet」を設定
⑤「Add」を選択



32. ①「Site」を選択
 - ②「New Site List」を選択
 - ③Site List Name は「LBO_Site」を入力
 - ④Add Site はインターネットブレイクアウトする CPE の Site ID※を設定
(複数設定する場合は、で区切る)
 - ⑤「Add」を選択
- ※Site ID の確認方法は 5.1 章を参照；

Name	Entries	Reference Count	Updated By	Last Updated	Action
Site_vCPE	10000000-19999999	15	sdwan-order-nl	05 Oct 2023 11:53:31 AM +09	Edit Delete
Site_vCPE_Act	110000000-119999999	5	sdwan-order-nl	05 Oct 2023 11:53:47 AM +09	Edit Delete
Site_vCPE_Stat	120000000-129999999	5	sdwan-order-nl	05 Oct 2023 11:54:01 AM +09	Edit Delete
Site_East	200000000-299999999	7	sdwan-order-nl	05 Oct 2023 11:54:13 AM +09	Edit Delete
Site_East_Mesh	200000000-299999999	4	sdwan-order-nl	05 Oct 2023 11:54:37 AM +09	Edit Delete
Site_East_Center	220000000-229999999	6	sdwan-order-nl	05 Oct 2023 11:54:52 AM +09	Edit Delete
Site_East_Spoke	210000000-219999999	4	sdwan-order-nl	05 Oct 2023 11:55:05 AM +09	Edit Delete

33. ①「VPN」を選択
 - ②「New VPN List」を選択
 - ③VPN List Name は「LBO_VPN」を設定
 - ④Add VPN はインターネットブレイクアウトする VPN 番号を設定
(複数設定する場合は「,」で区切る※)
 - ⑤「Add」を選択
- ※VPN 番号は基本的に 10 を設定、VPN を追加している場合は追加した VPN 番号を必要に応じて設定

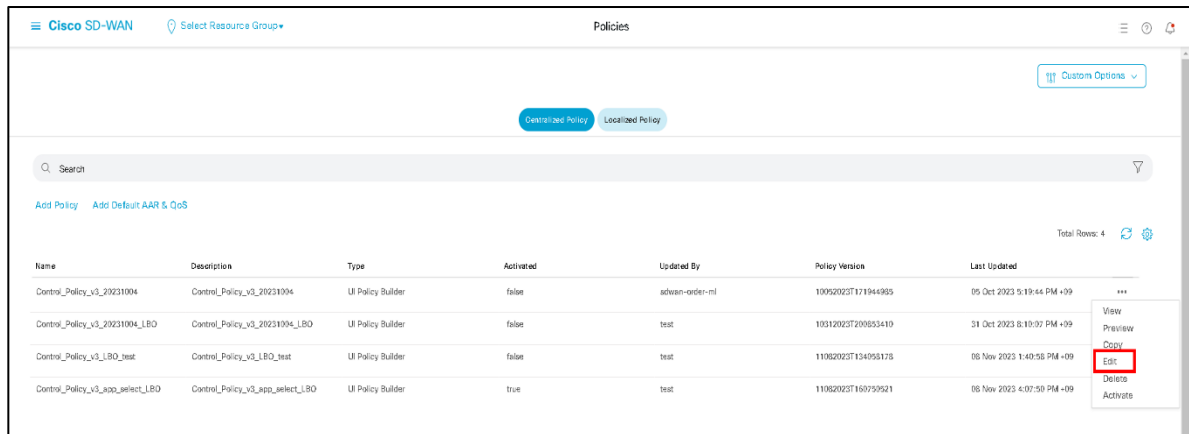
Name	Entries	Reference Count	Updated By	Last Updated	Action
all_VPN_List	10, 20, 30, 40, 9999	6	sdwan-order-nl	05 Oct 2023 4:52:23 PM +09	Edit Delete
Local_VPN	512	6	sdwan-order-nl	05 Oct 2023 4:52:49 PM +09	Edit Delete

34. (NTT 東日本提供のデフォルトポリシーが表示される場合)

左ペイン(左の領域)の Configuration から「Policies」を選択

「…」 から NTT 東日本デフォルトポリシーをコピー

コピーしたポリシーの「…」 から「Edit」を選択

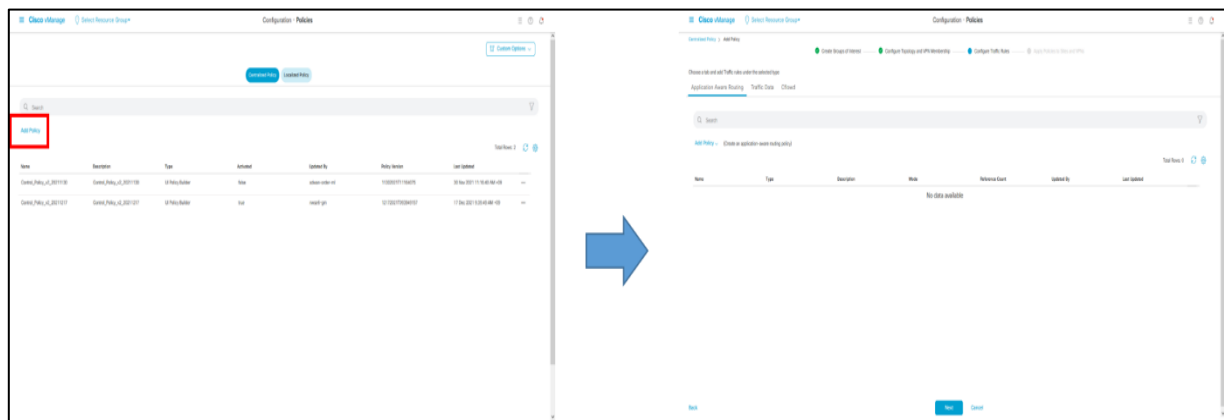


34. (NTT 東日本提供のデフォルトポリシーが表示されない場合)

左ペイン(左の領域)の Configuration から「Policies」を選択

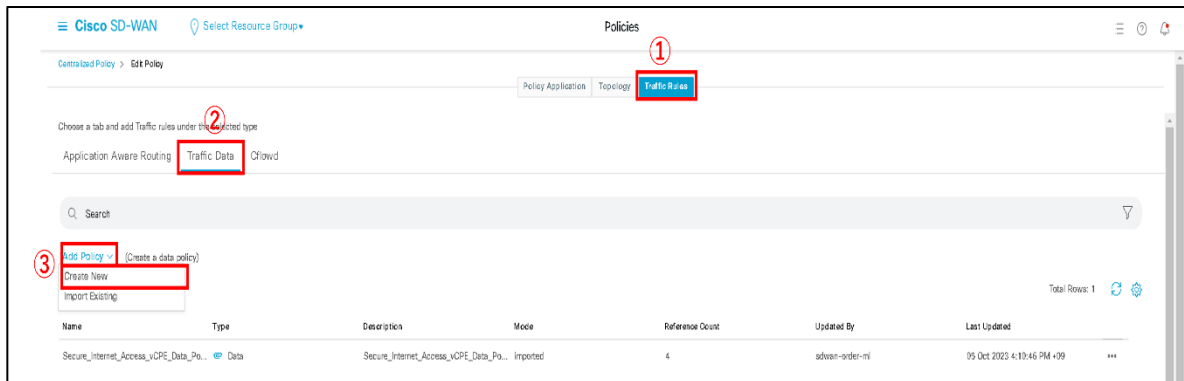
「Add Policy」を選択

右の画面が表示されるまで何もせず「Next」を選択



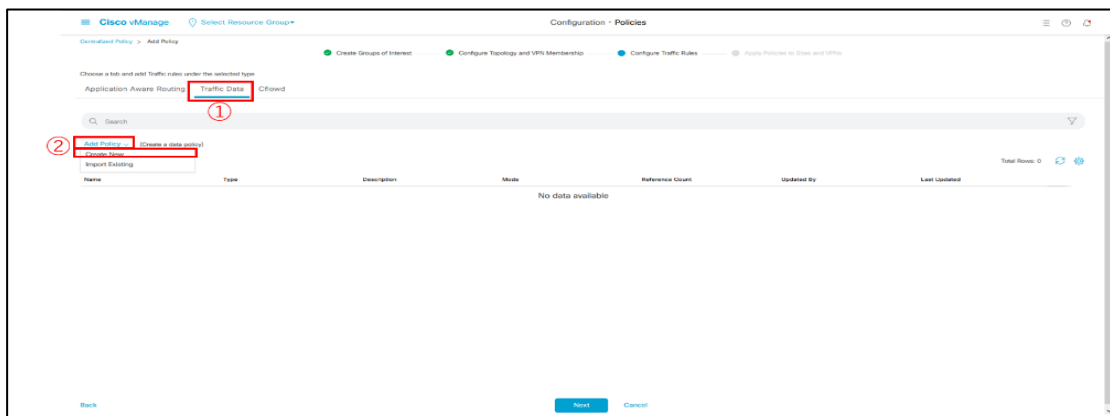
35. (NTT 東日本提供のデフォルトポリシーが表示される場合)

- ①画面上部の「Traffic Rules」を選択
- ②画面中部の「Traffic Data」を選択
- ③Add Policy から「Create New」を選択

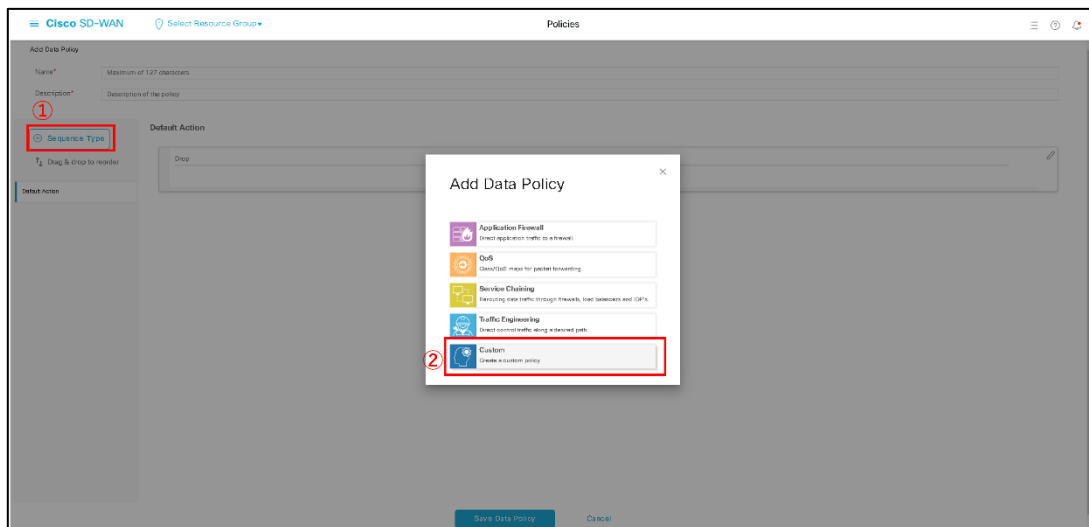


35. (NTT 東日本提供のデフォルトポリシーが表示されない場合)

- ①画面中部の「Traffic Data」を選択
- ②Add Policy から「Create New」を選択



36. ① 「Sequence type」を選択
 ② 「Custom」を選択

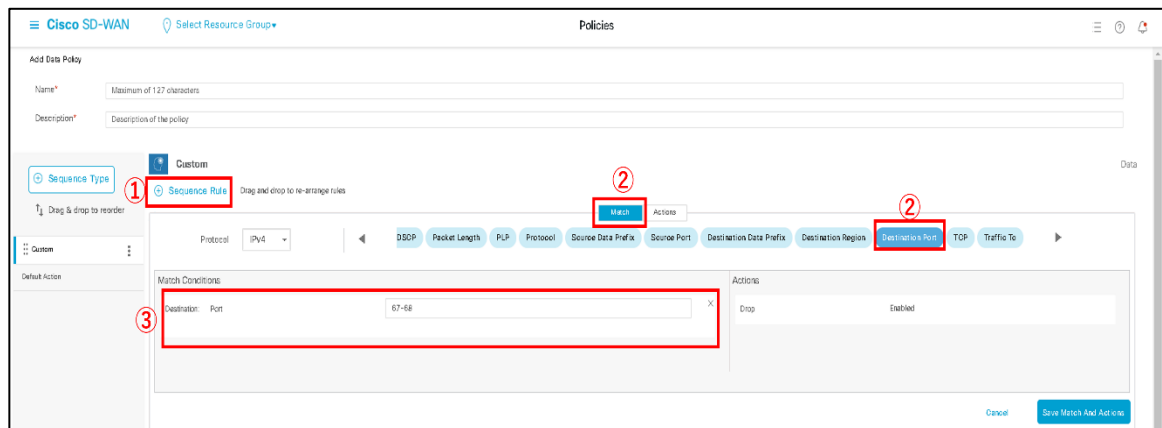


37. ①「Sequence Rule」を選択

②Match タブから「Destination Port」を選択

③Destination Port に「67-68」を設定

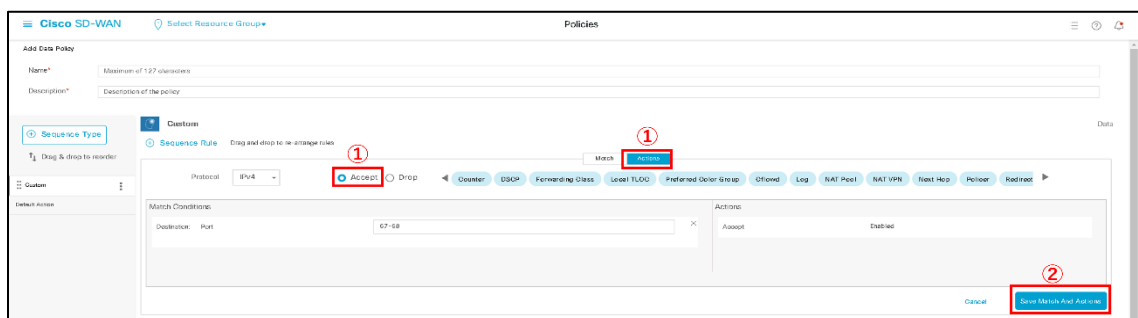
※手順 37-38 は CPE でインターネットブレイクアウトと DHCP サーバの機能を併用する場合に必要な手順となります、CPE で DHCP サーバを利用しない場合は省略して頂いて問題ありません



38. ①Actions タブを選択し「Accept」にチェックを入れる

②「Save Match And Action」を選択

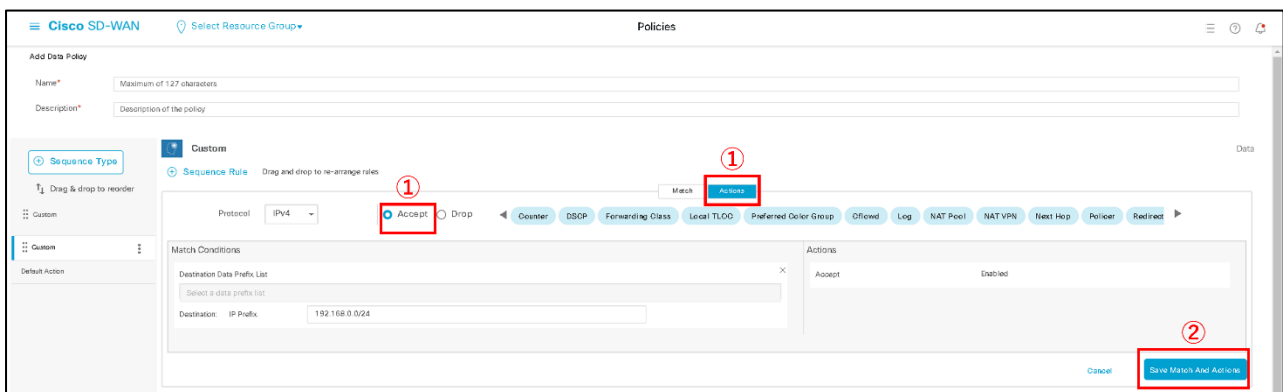
※手順 37-38 は CPE でインターネットブレイクアウトと DHCP サーバの機能を併用する場合に必要な手順となります、CPE で DHCP サーバを利用しない場合は省略して頂いて問題ありません



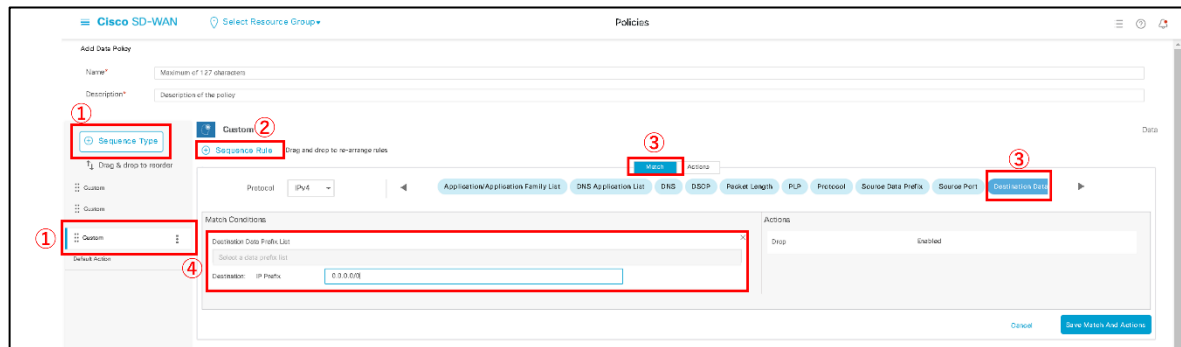
39. ①「Sequence Type」から「Custom」を選択
- ②「Sequence Rule」を選択
- ③Match タブから「Destination Data Prefix」を選択
- ④Destination IP Prefix に全 CPE のセグメントを集約したセグメントを設定
(Ex. 193.168.1.0/24,193.168.2.0/24,193.168.3.0/24 の3拠点の場合は 193.168.0.0/16 と記載)



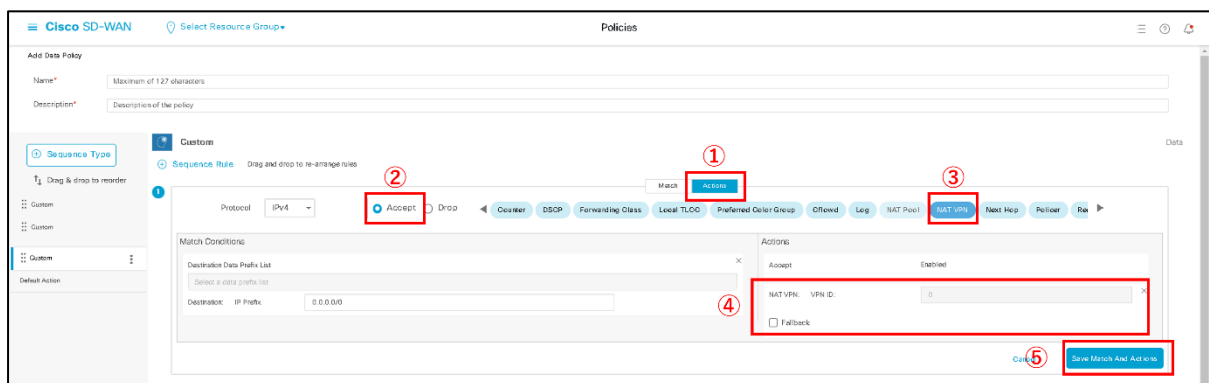
40. ①Actions タブを選択し「Accept」をチェック
- ②「Save Match And Action」を選択



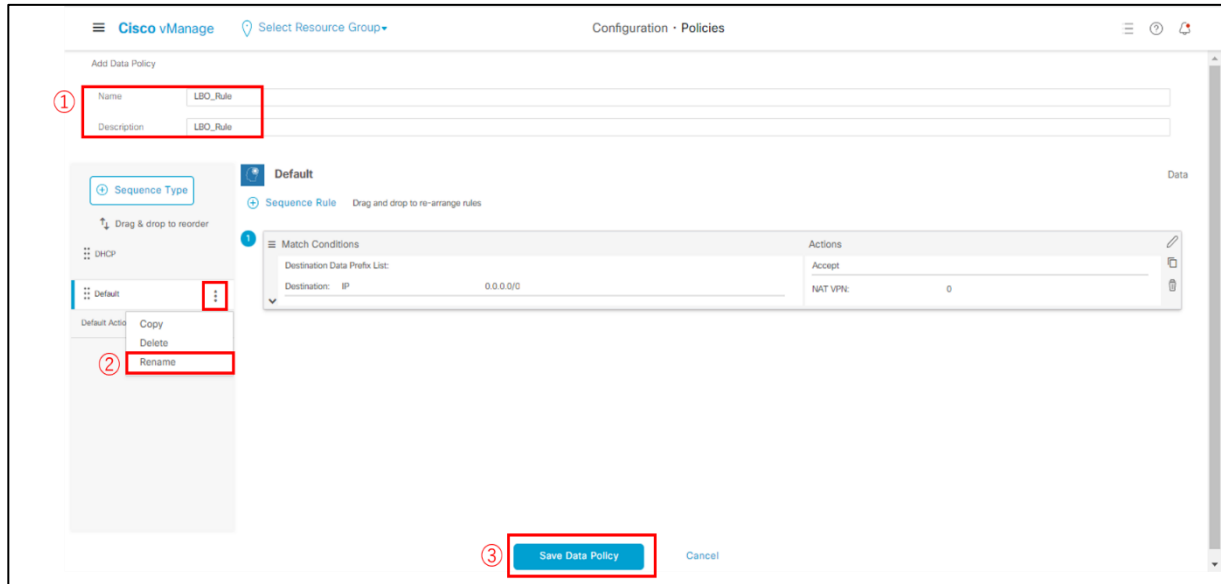
41. ①「Sequence Type」から「Custom」を選択
- ②「Sequence Rule」を選択
- ③Match タブから「Destination Data Prefix」を選択
- ④Destination IP Prefix に 0.0.0.0/0 を設定



42. ①Actions タブを選択
- ② Protocol は「IPv4」、「Accept」をチェック
- ③「NAT VPN」を選択
- ④NAT VPN ID が「0」になっていることを確認
- ⑤「Save Match And Action」を選択



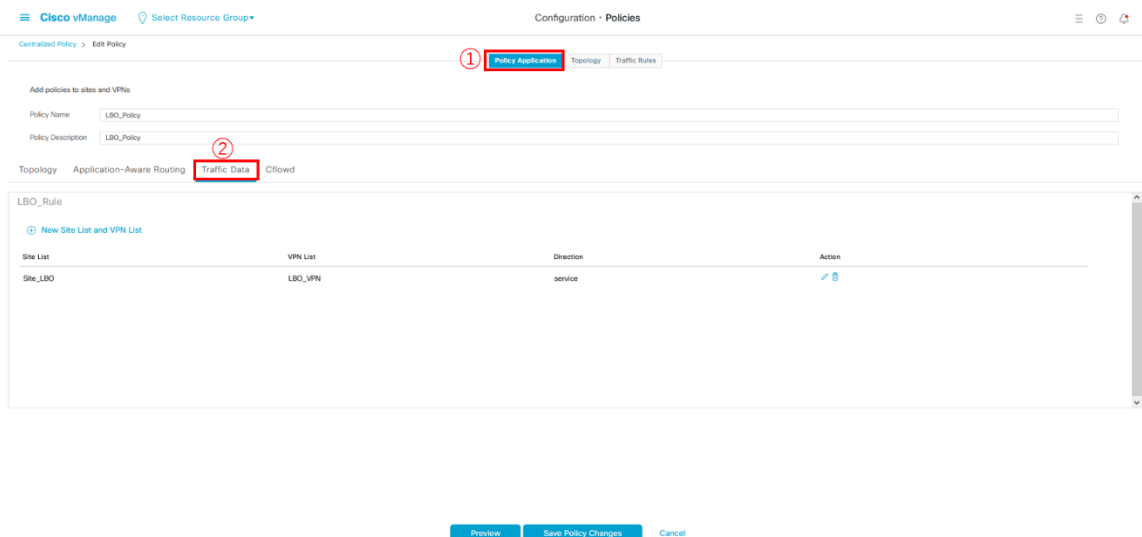
43. ①Name および Description は「LBO_Rule」を入力
- ②手順 37-42 で作成したルール の Name を「…」から Rename を選択し、37-38 は「DHCP」,39-42 は「Default」にリネーム
- ※同じ名前のルールが二つあるとエラーになります
- ③「Save Data Policy」を選択



The screenshot shows the 'Add Data Policy' configuration page in Cisco vManage. The 'Name' and 'Description' fields are both set to 'LBO_Rule'. On the left, the 'Default' policy is selected, and the 'Rename' option is highlighted. At the bottom, the 'Save Data Policy' button is highlighted.

44. (NTT 東日本提供のデフォルトポリシーが表示される場合)

- ①画面上部のタブから「Policy Application」を選択
- ②画面中部のタブから「Traffic Data」を選択

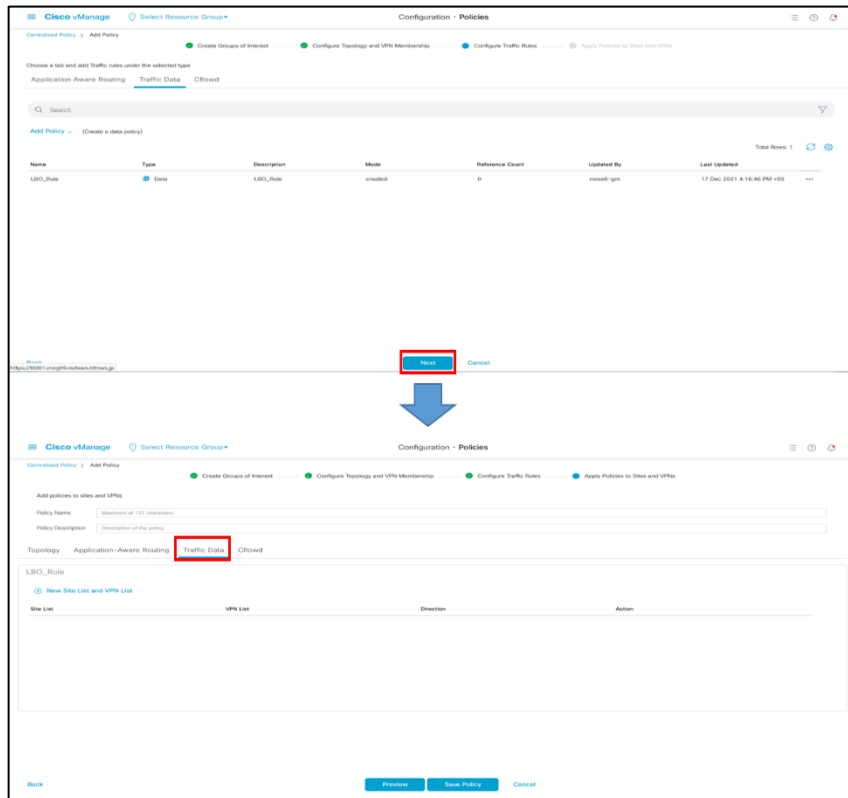


The screenshot shows the 'Policy Application' configuration page in Cisco vManage. The 'Policy Application' tab is selected, and the 'Traffic Data' sub-tab is selected. The 'Policy Name' is 'LBO_Policy' and the 'Policy Description' is 'LBO_Policy'. The 'Traffic Data' table shows a single entry for 'Site_LBO' with 'LBO_VPN' as the VPN List and 'service' as the Direction.

44. (NTT 東日本提供のデフォルトポリシーが表示されない場合)

上画面で「Next」を選択

下画面に遷移するので、中部のタブから「Traffic Data」を選択



45. ①Policy Name および Policy Description は「LBO_Policy」を入力
 - ②「New Site List and VPN List」を選択
 - ③Select Site List に「LBO_Site」を設定
 - ④Select VPN List に「LBO_VPN」を設定
 - ⑤「Add」を選択
 - ⑥「Save Policy」※を選択
- ※既にポリシーがある場合には「Save Policy Changes」

4.7.10. LBO 接続制限設定

LBO接続制限を設定

※ 本項目は 2 台以上の CPE にてローカルブレイクアウトを設定し、さらに NTT 東日本提供のデフォルトトポロジが作成されている場合に必要手順となります。デフォルトトポロジが作成されていない場合の手順については次版以降の記載となります。

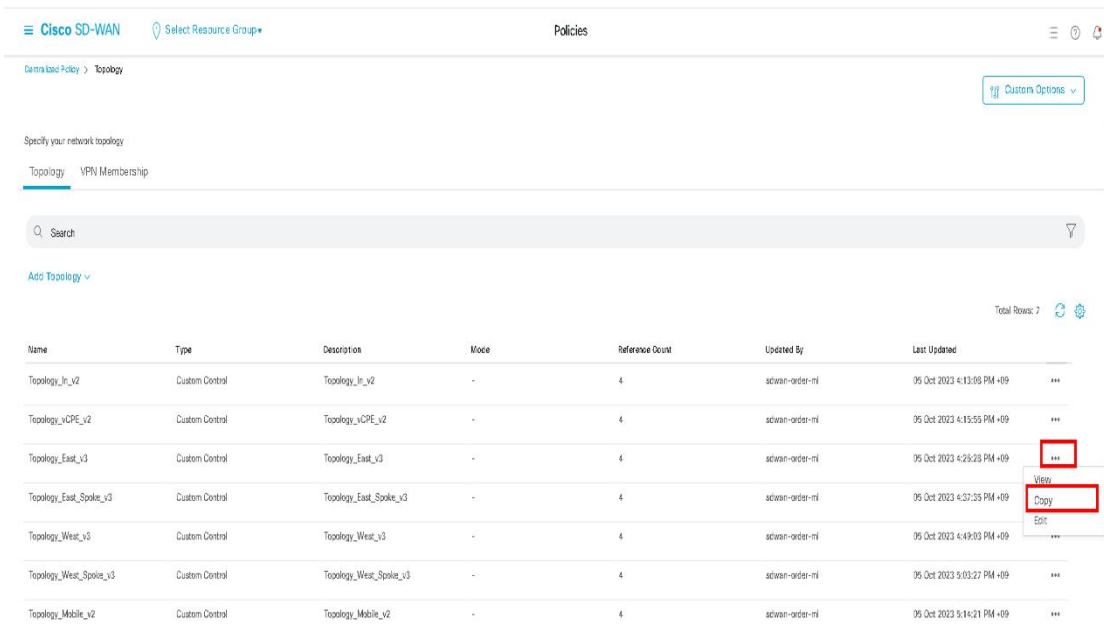
46. 左ペイン(左の領域)の Configuration から「Policies」を選択
画面上部の「Custom Options」から「Topology」を選択

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	adwan-order-ml	10952023T171944955	05 Oct 2023 3:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10312023T20053410	31 Oct 2023 3:10:07 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11062023T134056178	08 Nov 2023 1:40:56 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11062023T160750521	08 Nov 2023 4:07:50 PM +09

47. NTT 東日本デフォルトの Topology の「…」から「copy」を選択

※Topology_East,Topology_West から始まるトポロジ名が NTT 東日本提供のデフォルトトポロジになります。

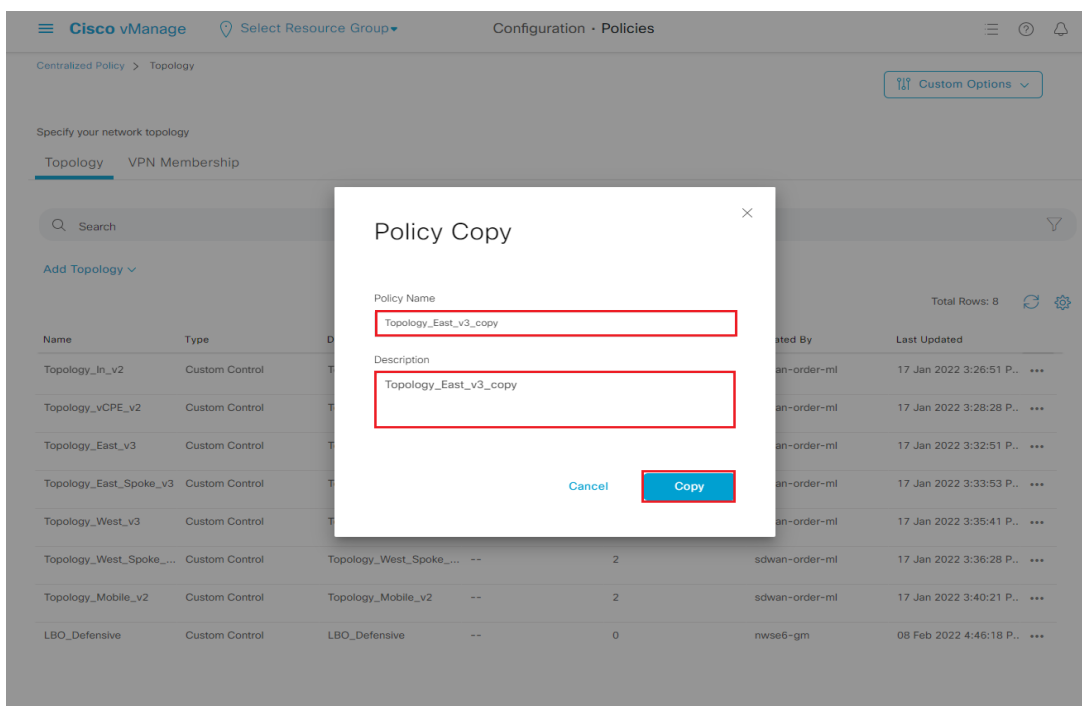
複数設定されていければ、移行の設定もその分だけ必要となります。



Name	Type	Description	Mode	Reference Count	Updated By	Last Updated	
Topology_In_v2	Custom Control	Topology_In_v2	-	4	sdwan-order-mi	05 Oct 2023 4:13:09 PM +09	...
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	-	4	sdwan-order-mi	05 Oct 2023 4:15:55 PM +09	...
Topology_East_v3	Custom Control	Topology_East_v3	-	4	sdwan-order-mi	05 Oct 2023 4:26:23 PM +09	...
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	-	4	sdwan-order-mi	05 Oct 2023 4:27:35 PM +09	...
Topology_West_v3	Custom Control	Topology_West_v3	-	4	sdwan-order-mi	05 Oct 2023 4:49:02 PM +09	...
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	-	4	sdwan-order-mi	05 Oct 2023 5:03:27 PM +09	...
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	-	4	sdwan-order-mi	05 Oct 2023 5:14:21 PM +09	...

48. 「Policy Name」と「Description」に任意の名前と説明を入力する

※例ではどちらも「Topology_East_v3_copy」となります



Policy Name

Description

Cancel Copy

49. コピーした Topology の右枠の「…」から「Edit」を選択

Cisco vManage Select Resource Group Configuration · Policies

Centralized Policy > Topology

Specify your network topology

Topology VPN Membership

Search

Add Topology

Total Rows: 7

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated	
Topology_In_v2	Custom Control	Topology_In_v2	--	2	sdwan-order-ml	17 Jan 2022 3:26:51 PM	...
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	--	2	sdwan-order-ml	17 Jan 2022 3:28:28 PM	...
Topology_East_v3	Custom Control	Topology_East_v3	--	2	sdwan-order-ml	17 Jan 2022 3:32:51 PM	...
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	--	2	sdwan-order-ml	17 Jan 2022 3:36:28 PM	...
Topology_West_v3	Custom Control	Topology_West_v3	--	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM	...
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	--	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM	...
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	--	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM	...

View
Copy
Edit

50. 左枠の「TLOC」を選択し、「Sequence Rule」を選択

Cisco vManage Select Resource Group Configuration · Policies

Centralized Policy > Topology > Edit Custom Control Policy

Name Topology_East_v3

Description Topology_East_v3

Sequence Type

Drag & drop to reorder

TLOC

Sequence Rule Drag and drop to re-arrange rules

Match Conditions

Site List: Site_vCPE

Site ID:

Actions

Accept

Match Conditions

Site List: Site_East

Site ID:

Actions

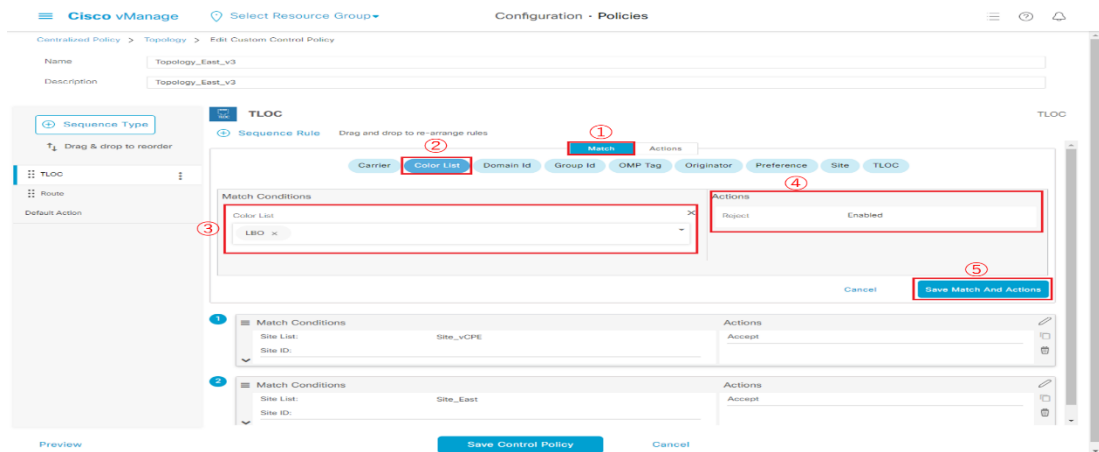
Accept

Preview

Save Control Policy

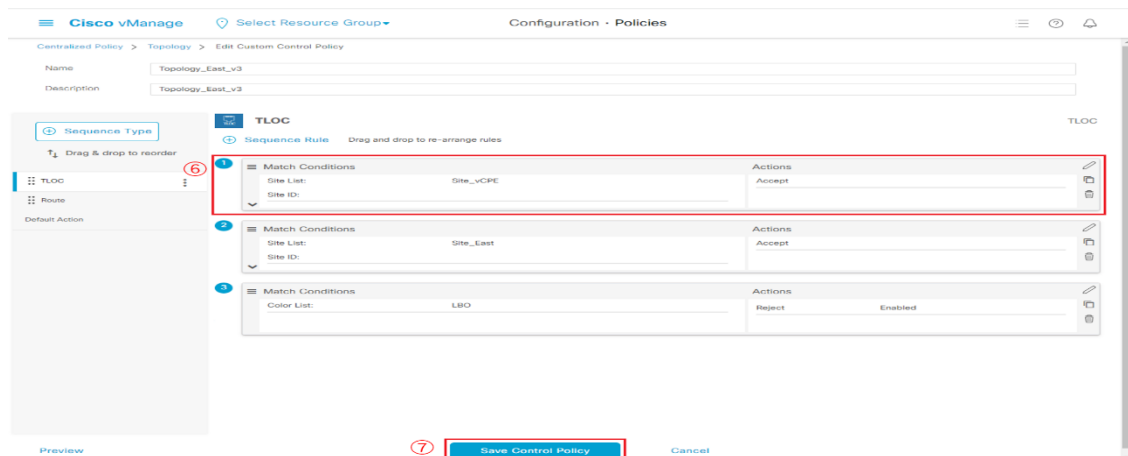
Cancel

51. ①「Match」タブを選択
- ②「Color List」タブを選択
- ③手順 32 にて作成した「LBO」の Color List を選択
- ④「Actions」にて、Reject が「Enabled」であることを確認する。
- ※デフォルトでは Enabled のため、設定の変更は不要です
- ⑤「Save Match And Actions」を選択



The screenshot shows the 'Configuration - Policies' page in Cisco vManage. The 'Match' tab is selected for a TLOC policy. The 'Color List' dropdown is set to 'LBO'. The 'Actions' section shows 'Reject' is 'Enabled'. The 'Save Match And Actions' button is highlighted with a red box and a circled 5.

- ⑥投入した設定を一番上の Sequence にドラッグ&ドロップ
- ⑦「Save Control Policy」を選択



The screenshot shows the 'Configuration - Policies' page in Cisco vManage. The 'Match' tab is selected for a TLOC policy. The 'Color List' dropdown is set to 'LBO'. The 'Actions' section shows 'Reject' is 'Enabled'. The 'Save Control Policy' button is highlighted with a red box and a circled 7.

52. 左ペイン(左の領域)の Configuration から「Policies」を選択
 手順 45 にて作成済みの Policy の右枠の「…」から「Edit」を選択

Configuration - Policies

Custom Options

Centralized Policy Localized Policy

Search

Add Policy

Total Rows: 2

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_2022...	Control_Policy_v3_2022...	UI Policy Builder	true	sdwan-order-ml	01172022T154353140	17 Jan 2022 3:43:53 PM ...
Control_Policy_v3_2022...	Control_Policy_v3_2022...	UI Policy Builder	false	nwse6-gm	02012022T114439372	10 Feb 2022 11:09:44 P ...

View
 Preview
 Copy
 Edit
 Delete
 Activate

53. ①「Topology」タブを選択
 ②手順 51 で作成したトポロジのコピー元の「…」から「Detach」を選択

Configuration - Policies

Centralized Policy > Edit Policy

Policy Application Topology Traffic Rules

Specify your network topology

Topology VPN Membership

Search

Add Topology

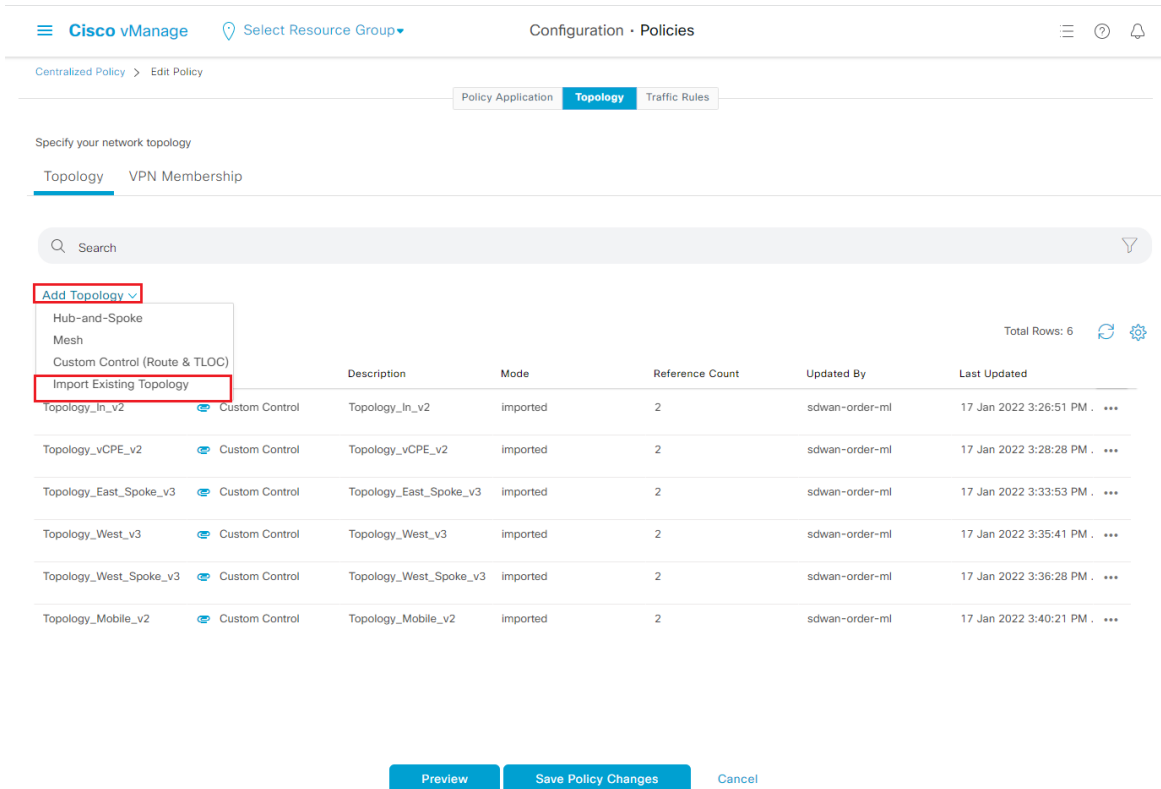
Total Rows: 7

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	Topology_In_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:46:13 PM ...
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:46:13 PM ...
Topology_East_v3	Custom Control	Topology_East_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:32:51 PM ...
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:33:53 PM ...
Topology_West_v3	Custom Control	Topology_West_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:35:41 PM ...
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:36:28 PM ...
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM ...

View
 Copy
 Detach

Preview Save Policy Changes Cancel

54. 「Add Topology」 → 「Import Existing Topology」を選択



Specify your network topology

Topology VPN Membership

Search

Add Topology ▾

- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)
- Import Existing Topology

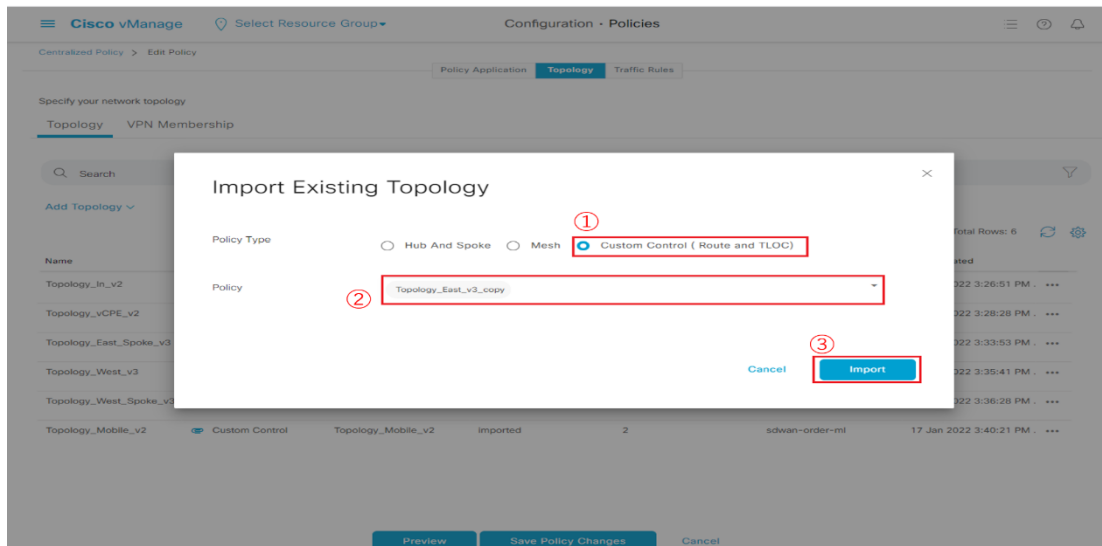
Name	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	imported	2	sdwan-order-ml	17 Jan 2022 3:26:51 PM
Topology_vCPE_v2	Custom Control	imported	2	sdwan-order-ml	17 Jan 2022 3:28:28 PM
Topology_East_Spoke_v3	Custom Control	imported	2	sdwan-order-ml	17 Jan 2022 3:33:53 PM
Topology_West_v3	Custom Control	imported	2	sdwan-order-ml	17 Jan 2022 3:35:41 PM
Topology_West_Spoke_v3	Custom Control	imported	2	sdwan-order-ml	17 Jan 2022 3:36:28 PM
Topology_Mobile_v2	Custom Control	imported	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM

Preview Save Policy Changes Cancel

55. ① 「Custom Control(Route and TLOC)」を選択

②手順 51 で作成したトポロジを選択

③ 「Import」を選択



Import Existing Topology

Policy Type

☐ Hub And Spoke ☐ Mesh ☒ Custom Control (Route and TLOC)

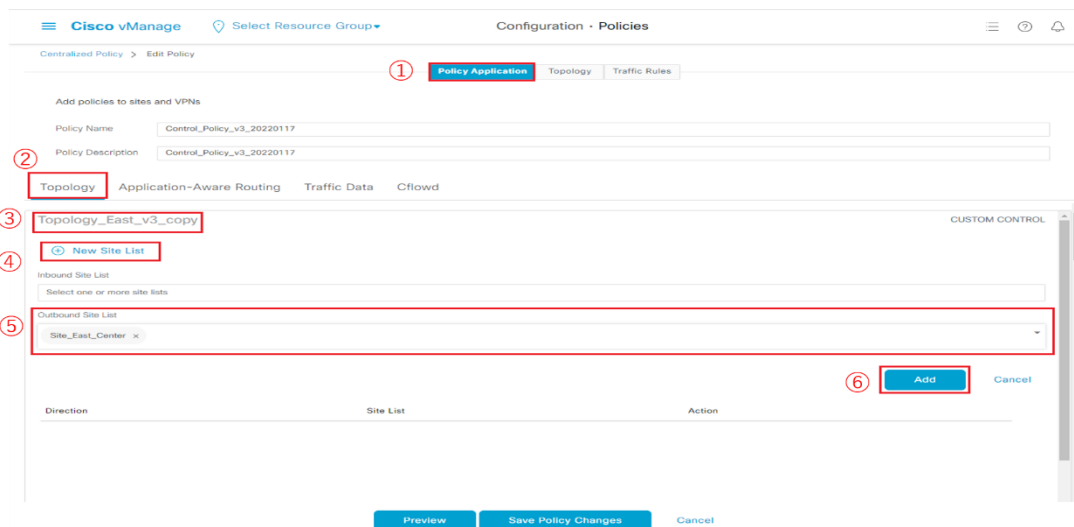
Policy

Topology_East_v3_copy

Cancel Import

Preview Save Policy Changes Cancel

56. ①「Policy Application」タブを選択
 ②「Topology」タブを選択
 ③手順 55 で Import したトポロジの欄を選択
 ④「New Site List」を選択
 ⑤Outbound Site List に 各トポロジに対応した SiteList を入力
 ※各トポロジに対応した SiteList は以下の通りです
 Topology_East:Site_East_Center
 Topology_West:Site_West_Center
 ⑥「Add」を選択



① Policy Application

② Topology

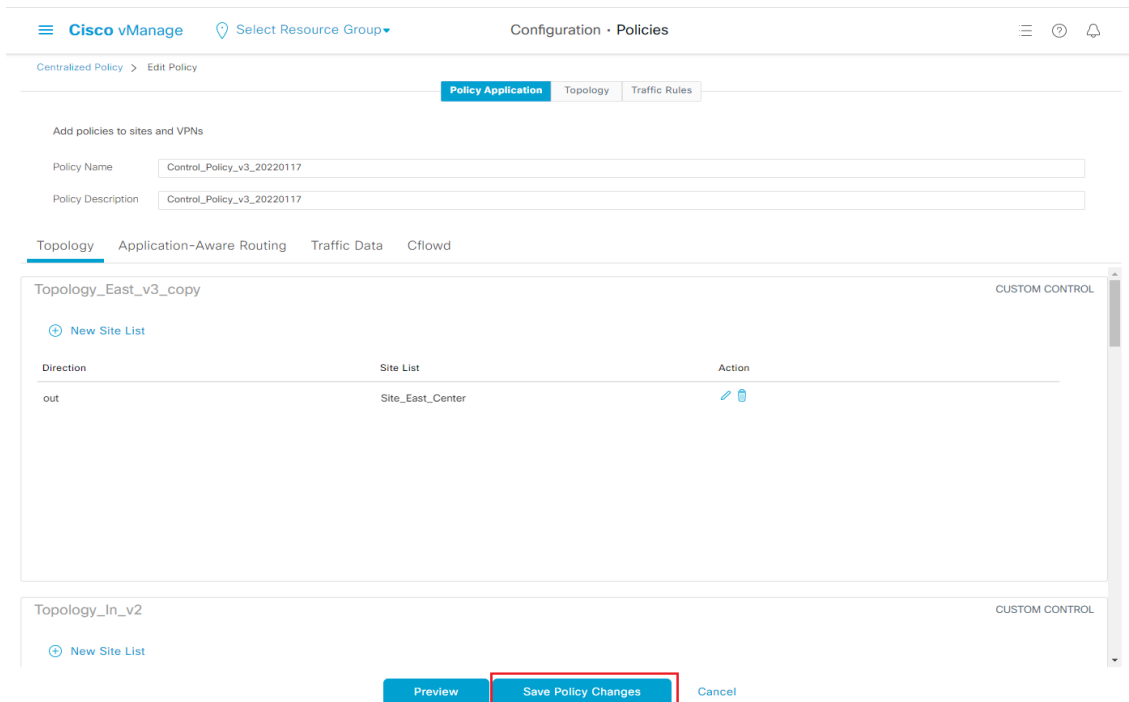
③ Topology_East_v3_copy

④ New Site List

⑤ Site_East_Center



⑥ Add

57. 「Save Policy Changes」を選択



Policy Application

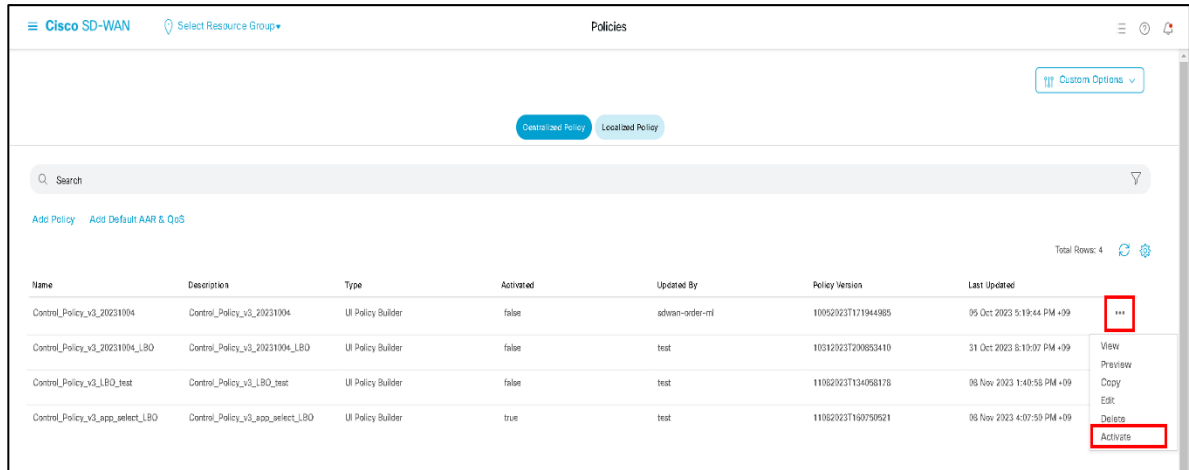
Topology_East_v3_copy

Direction	Site List	Action
out	Site_East_Center	 

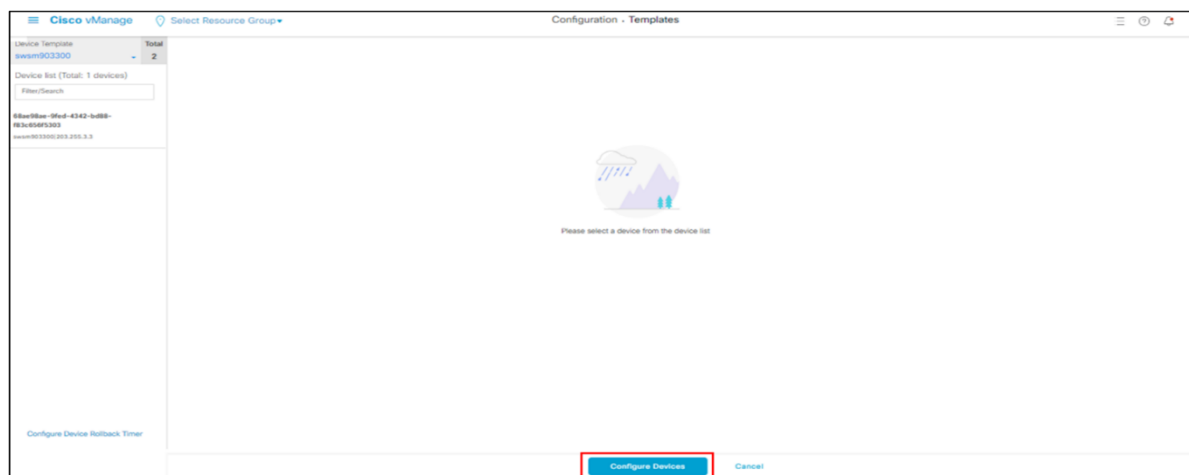
Save Policy Changes

4.7.11. ポリシーの有効化

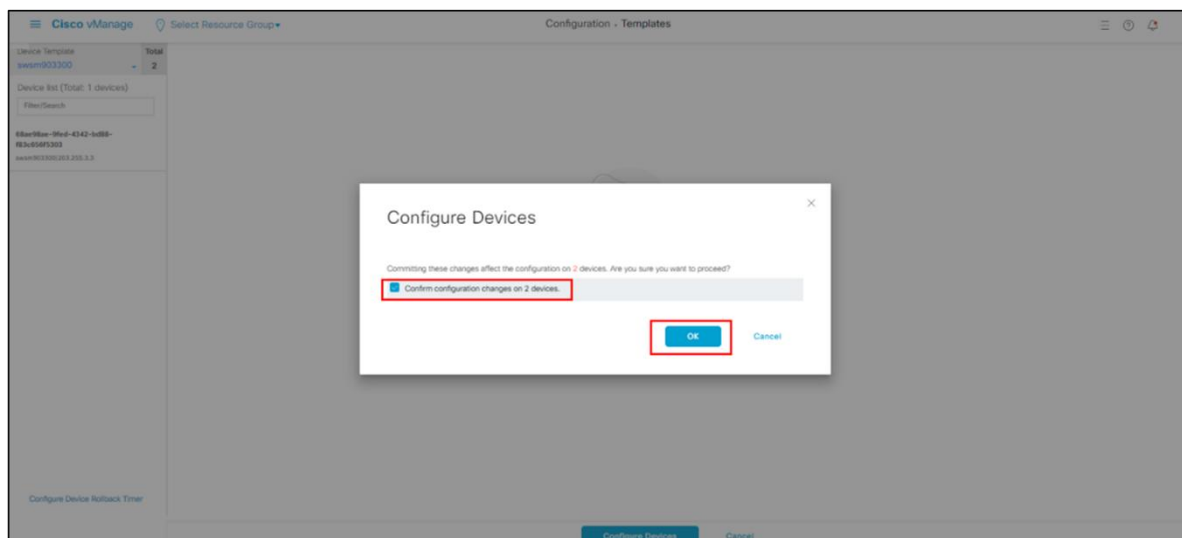
58. 手順 57 までで作成したポリシーの「…」から「Activate」を選択
⇒選択後のポップアップ画面で「Activate」を選択



59. 下記画面へ遷移するので「Configure Devices」を選択



60. 下記画面へ遷移するので「Confirm Configuration changes on 2 devices」にチェックを入れ、「OK」を選択



61. Status が success, Message が Done となっていればコンフィグ適用が完了
⇒Status 変更までに 1 分程度かかります

Cisco SD-WAN Select Resource Group

Push vSmart Policy | Validation Success Initiated By: nvsad-gm | Tenant: CSDWNE-15-0001 From: 172.18.128.190

Total Task: 2 | Success: 2

Search

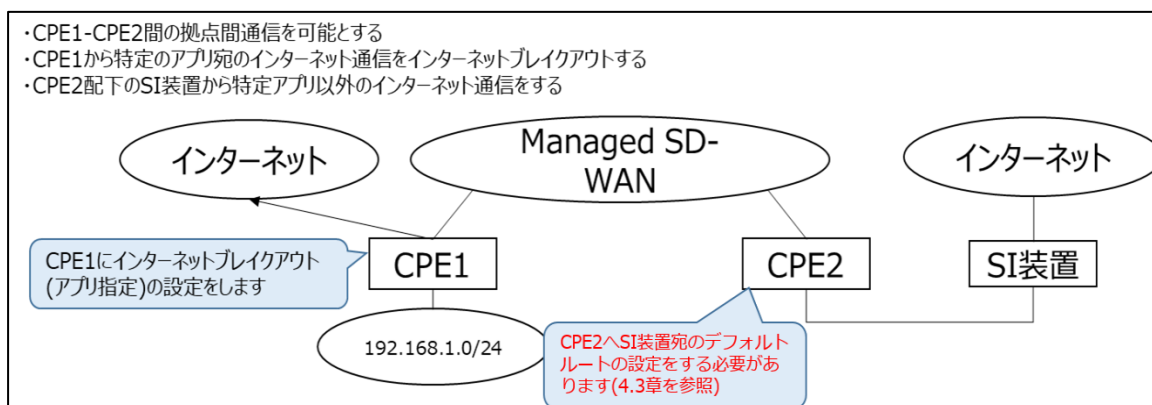
Total Rows: 2

Status	Message	Hostname	System IP	Site ID	vManage IP
Success	Config status from device: success	swsm615010	215.255.3.1	1000000000	215.255.1.1
Success	Config status from device: success	swsm615020	215.255.3.3	1000000000	215.255.1.1

4.8. インターネットブレイクアウト (アプリ指定)

指定した通信を対象とするインターネットブレイクアウト設定について紹介します。

4.8.1. NW 構成例



【Device Template 作成に必要な Feature Template】

作成する Feature Template	手順	用途
GE000	1～2	WAN インターフェース設定用
PPPoE	3～4	PPPoE 設定用
CLI_LBO	5～6	コマンド設定用
FW	7～21	セキュリティ設定用

【ポリシー作成時に必要な List 及び Topology】

作成する List	必要となる情報	手順	用途
LBO	Color	31	ブレイクアウト通信同士のトンネル接続を防ぐための Color の指定
LBO_App	ブレイクアウトさせたいアプリ	32~33	アプリケーション指定のため
LBO_Site_App	Site ID	34	ブレイクアウトさせる CPE の指定 ※5.1 章を参考に確認
LBO_VPN_App	VPN 番号	35	ブレイクアウトさせる VPN の指定 VPN グループ数 1 の場合:10 VPN グループ数 1 の場合:10,20,30,40
LBO_Rule_App	-	36~42	拠点間通信用ルール
LBO_Policy_App	LBO_Site_App LBO_VPN_App LBO_Rule	43~44	ポリシー設定用

【デフォルトトポロジのコピーと LBO 接続制限トポロジの新規作成】

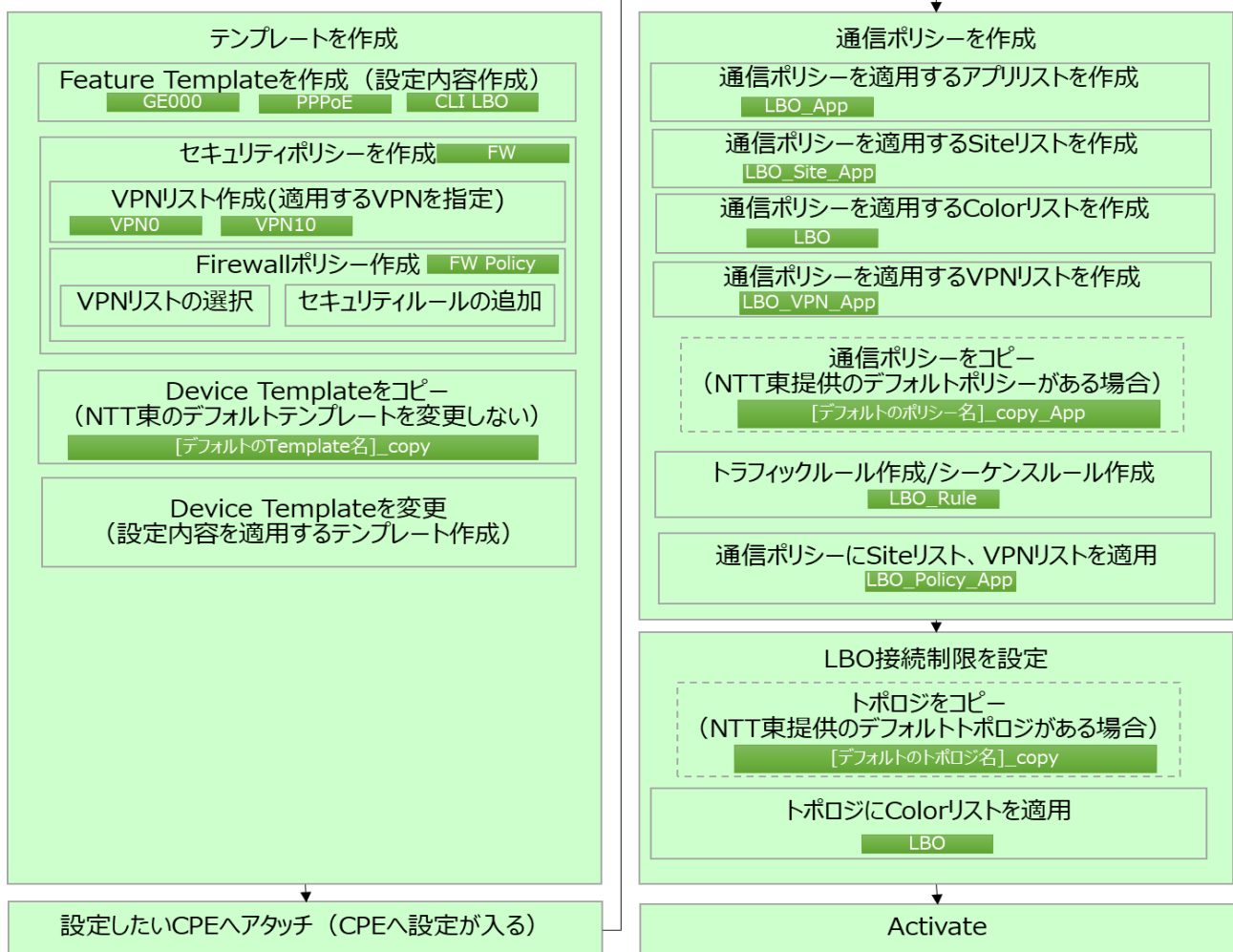
コピーしたトポロジ	手順	用途
Topology_East_v3_copy	45-47	トポロジのバックアップと新規作成

【LBO 接続制限トポロジへの Color-List の適用】

適用する Color-List	手順	用途
LBO	48-50	LBO の接続制限

【ポリシーへ LBO 接続制限トポロジの適用】

適用するトポロジ	手順	用途
Topology_East_v3_copy	51-56	LBO 接続制限

【設定の流れ】


4.8.2. インターネットブレイクアウト(アプリ指定)の留意点

インターネットブレイクアウト（アプリケーション指定）をご利用の際は、アプリケーション通信の識別ができず通信不可となる可能性があるため以下を留意ください。

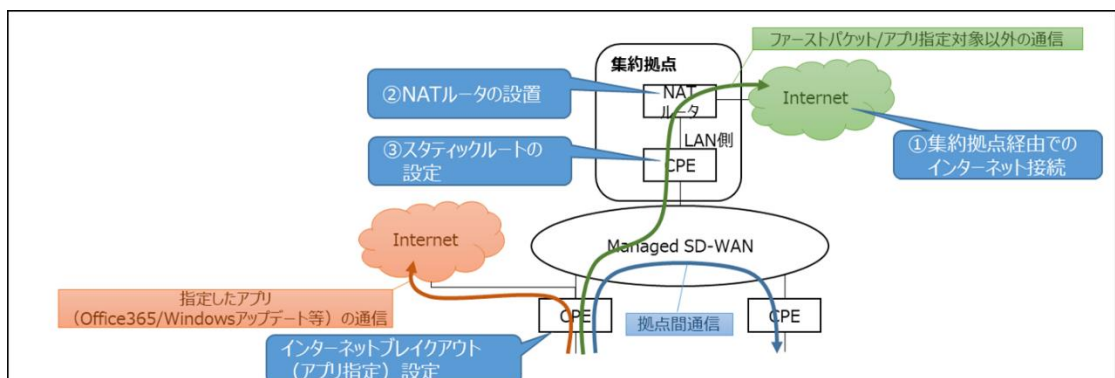
- ①CPE でのインターネットブレイクアウト接続の他に集約拠点(センタ等)からインターネットへの接続が可能であることが必要です。
- ②CPE では LAN 側への NAT 機能がないことから、集約拠点からインターネットへの接続の際は CPE の他に NAT ルータが必要です。
- ③集約拠点からインターネットへ接続するためのスタティックルートはお客様にて設定が必要です。

【補足】

- I. 指定したアプリケーションを識別するための CPE の仕組みとして、シグネチャ（アプリケーション識別のためのデータ）がありますが本サービスがセキュアな完全閉域サービスのため、Cisco 社から提供されるシグネチャが閉域内に配信されず自動的に更新されません。そのため CPE のファイル更新の際にアップデートされます。CPE のファイル更新タイミングは現在検討中です。シグネチャ識別対象外のアプリケーションは CPE でブレイクアウトせず、集約拠点経由でのインターネット接続で通信します。
- II. ファーストパケットは、アプリケーションを識別するために必要な情報がデータに含まれない可能性があり、シグネチャで識別できない場合があります。そのため、ファーストパケットは別のインターネットの経路で通信する必要があります。
- III. I、II を回避するためには、アクセス先サーバの IP アドレス指定によるインターネットブレイクアウト設定が必要です。また、当該の IP アドレスは変更の可能性があるため、RSS 等で自動的に IP アドレス変更情報を受信できる仕組みを構築することをお勧めします。

(参考)

<https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/microsoft-365-ip-web-service?view=o365-worldwide>



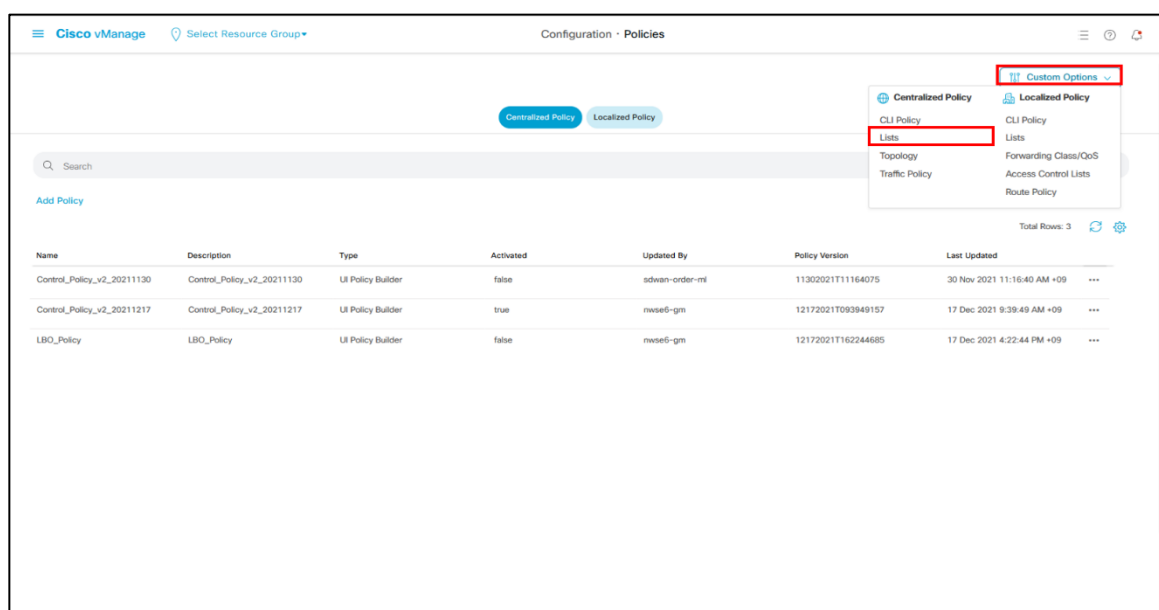
4.8.3. インターネットブレイクアウト用通信ポリシーを作成

通信ポリシー作成

手順 29 までは 4.7 章と共通になります。(4.7 章を参照願います)

30. 左ペイン(左の領域)の Configuration から「Policies」を選択

・画面上部の「Custom Options」から「Lists」を選択



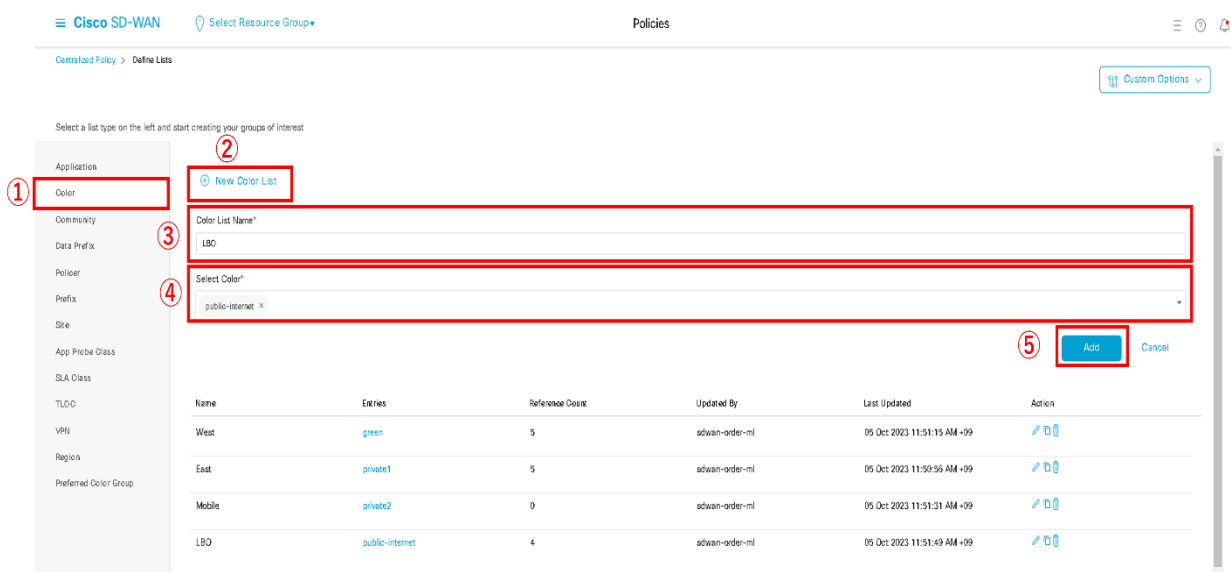
31. ①「Color」を選択

②「New Color List」を選択

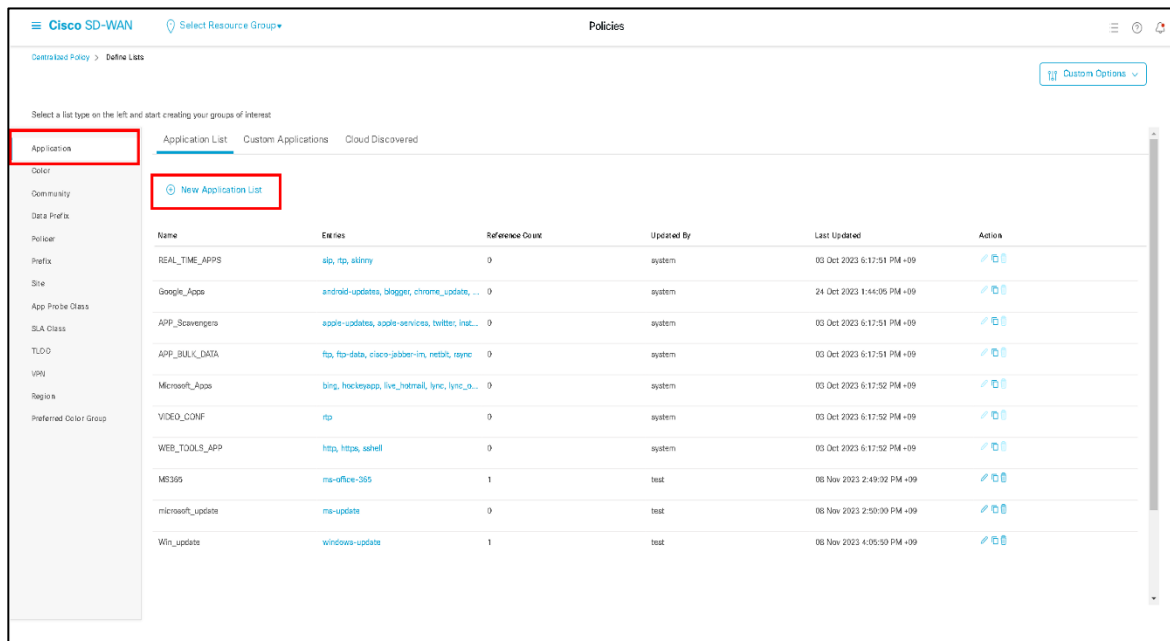
③Color List Name は「LBO」を設定

④Select Color は「public-internet」を設定

⑤「Add」を選択



32. 画面左列の「Application」を選択 「New Application List」を選択



Controlled Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application List Custom Applications Cloud Discovered

New Application List

Name	Entries	Reference Count	Updated By	Last Updated	Action
REAL_TIME_APPS	slp, rtp, skinny	0	system	03 Oct 2023 6:17:51 PM +09	Edit Delete
Google_Apps	android-updates, blogger, chrome_update, ...	0	system	24 Oct 2023 1:44:05 PM +09	Edit Delete
APP_Scavengers	apple-updates, apple-services, twitter, inst...	0	system	03 Oct 2023 6:17:51 PM +09	Edit Delete
APP_BULK_DATA	ftp, ftp-data, cisco-jabber-im, netbit, ryme	0	system	03 Oct 2023 6:17:51 PM +09	Edit Delete
Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, lync_o...	0	system	03 Oct 2023 6:17:52 PM +09	Edit Delete
VIDEO_CONF	rtp	0	system	03 Oct 2023 6:17:52 PM +09	Edit Delete
WEB_TOOLS_APP	http, https, sshell	0	system	03 Oct 2023 6:17:52 PM +09	Edit Delete
MS365	ms-office-365	1	test	08 Nov 2023 2:49:02 PM +09	Edit Delete
microsoft_update	ms-update	0	test	08 Nov 2023 2:50:00 PM +09	Edit Delete
Win_update	windows-update	1	test	08 Nov 2023 4:05:30 PM +09	Edit Delete

33. ①Application List Name に「LBO_App」を入力
- ②Applications の欄を選択し、ブレイクアウトさせたいアプリを入力
- ③Add を選択

(参考手順) 参考として MS 系通信のアプリリストの作成方法を以下に記載します

- ① デフォルトで存在する NTT_Microsoft_Apps をコピー

- ② List Name ヘリストの名前を記載し、「Copy」を選択

③ Application List が追加されたことを確認し、Edit(ペンマーク)をクリック

Application	Application List		Custom Applications	Cloud Discovered		
Color	New Application List					
Community						
Data Profile						
Policy						
Site						
App Profile Class						
SUA Class						
ECG						
VPN						
	Name	Entries	Reference Count	Updated By	Last Updated	Action
	REAL_TIME_APPS	http, https, skype	0	system	28 Nov 2021 9:35:43 AM +09	
	Google_Apps	android, updates, blogger, chrome, google, g...	0	system	28 Nov 2021 9:35:43 AM +09	
	APP_Servers	apple, updates, apple-services, twitter, instag...	0	system	28 Nov 2021 9:35:43 AM +09	
	APP_SUA_SUA	ftp, ftp-data, cloud-pdms-vpn, netbios, ntpc...	0	system	28 Nov 2021 9:35:43 AM +09	
	Microsoft_Apps	http, hockeapoo, live, hotmail, lync, lync, onli...	0	system	28 Nov 2021 9:35:43 AM +09	
	VIDEO_C2RM	rtsp	0	system	28 Nov 2021 9:35:43 AM +09	
	WEB_TORUS_APP	http, https, webal	0	system	28 Nov 2021 9:35:43 AM +09	
	NTT_Microsoft_Apps	http, hockeapoo, live, hotmail, lync, lync, onli...	0	system-order-nd	28 Nov 2021 10:47:53 AM +09	
	NTT_Microsoft_Update	updates	0	system-order-nd	28 Nov 2021 10:47:53 AM +09	
	USD_Apps	updates	0	rebuild-gn	17 Dec 2021 4:24:48 PM +09	
	NTT_Microsoft_Apps_copy	http, hockeapoo, live, hotmail, lync, lync, onli...	0	rebuild-gn	17 Dec 2021 4:47:48 PM +09	

Edit

Edit

④ 空白をクリックし、「Windows Update」を追加し、「Save」を選択

Application List

Application List Name

NTT_Microsoft_Apps_copy

☒ Application
 ☐ Application Family

Select Application

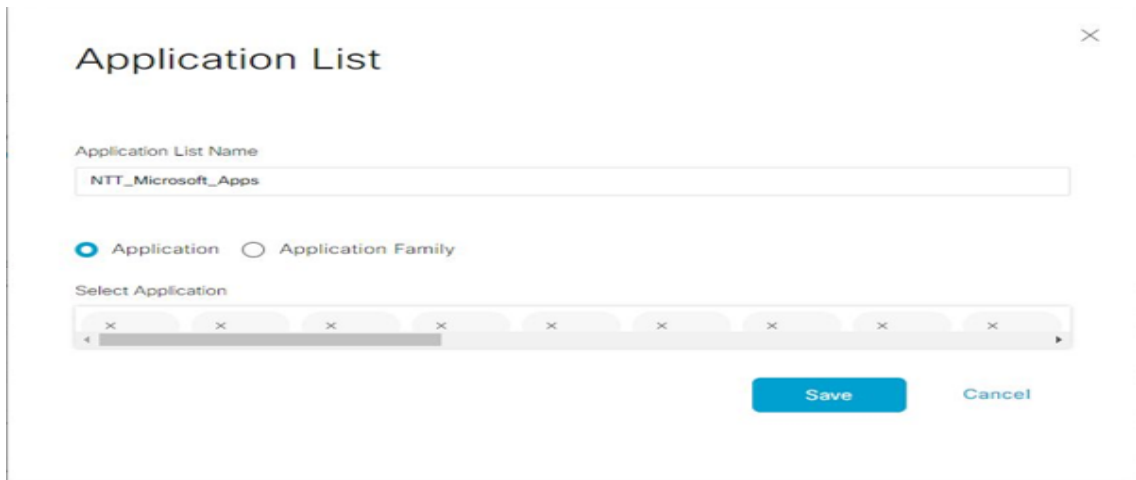
Bing hockeapoo (not supported) live hotmail (not supported) lync (not supported) lync onli

Applicationの間の隙間をクリック

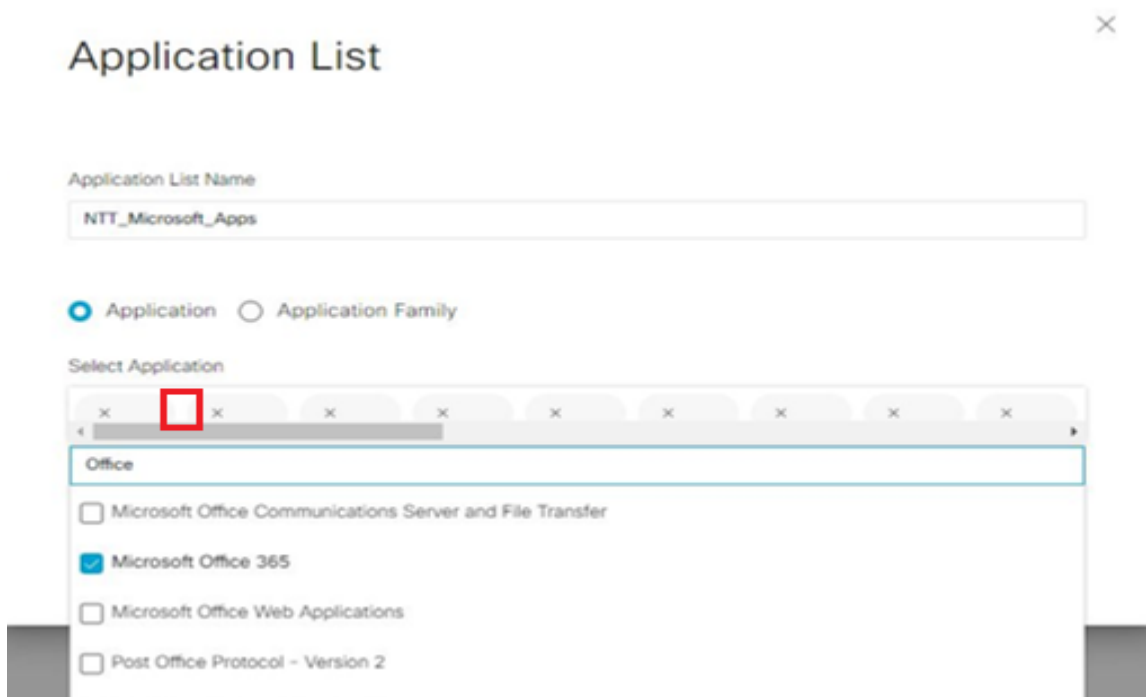
Save Cancel

☒ Windows Live Messenger File Transfer
 ☒ Microsoft Windows Azure
 ☐ Microsoft Windows Store
 ☒ Windows Update

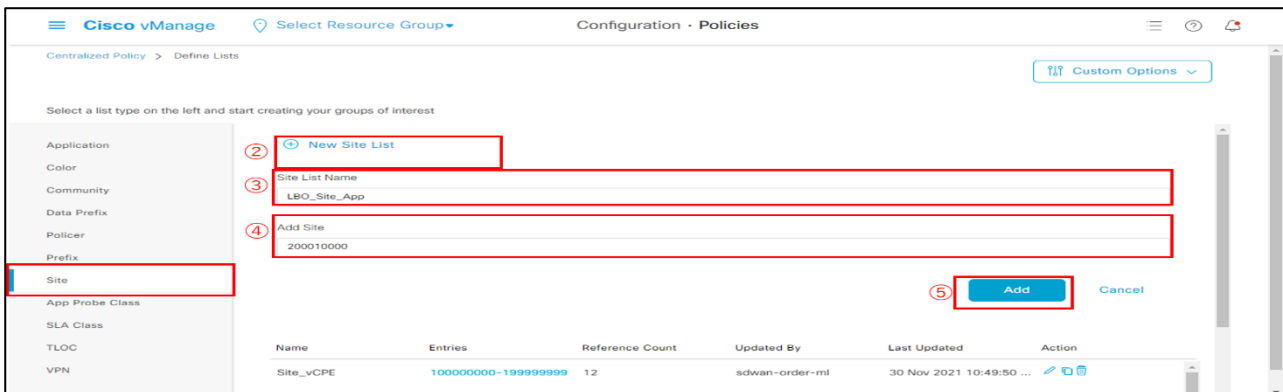
(留意事項) 環境によっては Application List 表示が見えない事象が発生する可能性がありますので、以下に発生した際の例を記載します。



この事象が発生した際でも、間の空欄(※赤枠に囲まれた部分が目安です)を以下のようをクリックすることで、有効化されている Application は確認が可能です。



34. ①「Site」を選択
 ②「New Site List」を選択
 ③Site List Name は「LBO_Site_App」を入力
 ④Add Site はインターネットブレイクアウトする CPE の Site ID※を設定
 (複数設定する場合は、で区切る)
 ⑤「Add」を選択
 ※Site ID の確認方法は 5.1 章を参照



Configuration - Policies

Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

② New Site List


③ Site List Name
LBO_Site_App

④ Add Site
200010000

⑤ Add Cancel

Name	Entries	Reference Count	Updated By	Last Updated	Action
Site_vCPE	100000000-199999999	12	sdwan-order-mi	30 Nov 2021 10:49:50 ...	

35. ①左メニューから「VPN」を選択
 ②「New VPN List」を選択
 ③VPN List Name へ「LBO_VPN_App」を入力
 ④Add VPN はインターネットブレイクアウトする VPN 番号を設定
 (複数設定する場合は「,」で区切る※)
 ⑤「Add」を選択
 ※VPN 番号は基本的に 10 を設定、VPN を追加している場合は追加した VPN 番号を必要に応じて設定



Configuration - Policies

Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

② New VPN List

③ VPN List Name
LBO_VPN_App

④ Add VPN
10

⑤ Add Cancel

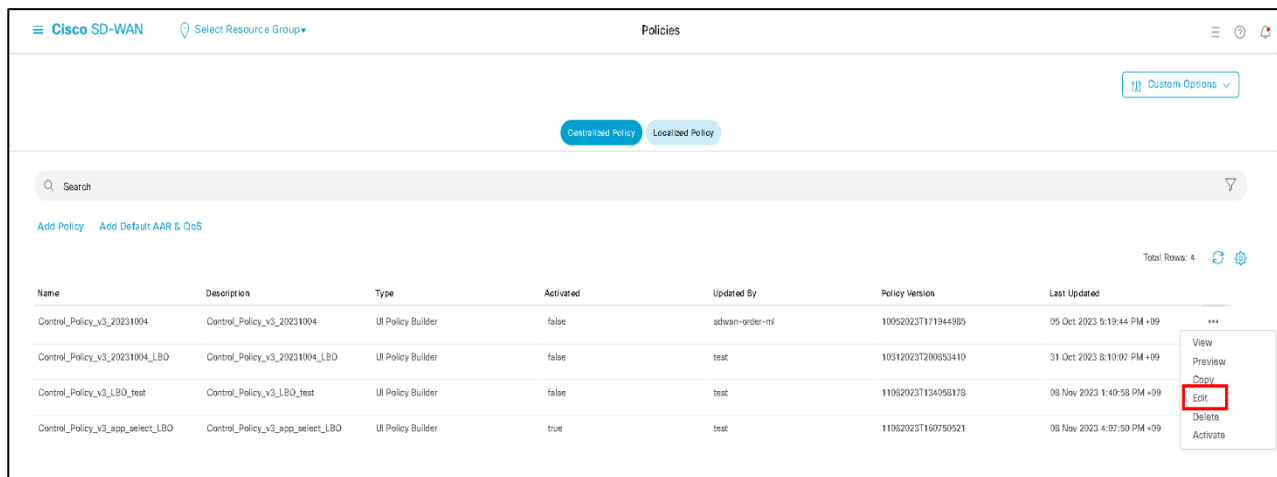
Name	Entries	Reference Count	Updated By	Last Updated	Action
all_VPN_List	10, 20, 30, 40, 9999	6	sdwan-order-mi	30 Nov 2021 10:55:42 ...	

36. (NTT 東日本提供のデフォルトポリシーが表示される場合)

左ペイン(左の領域)の Configuration から「Policies」を選択

「…」から NTT 東日本デフォルトポリシーをコピー

コピーしたポリシーの「…」から「Edit」を選択

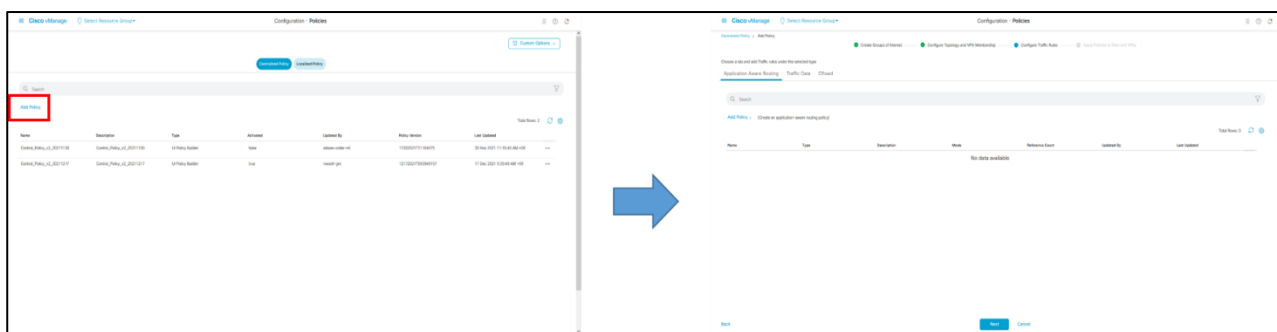


36. (NTT 東日本提供のデフォルトポリシーが表示されない場合)

左ペイン(左の領域)の Configuration から「Policies」を選択

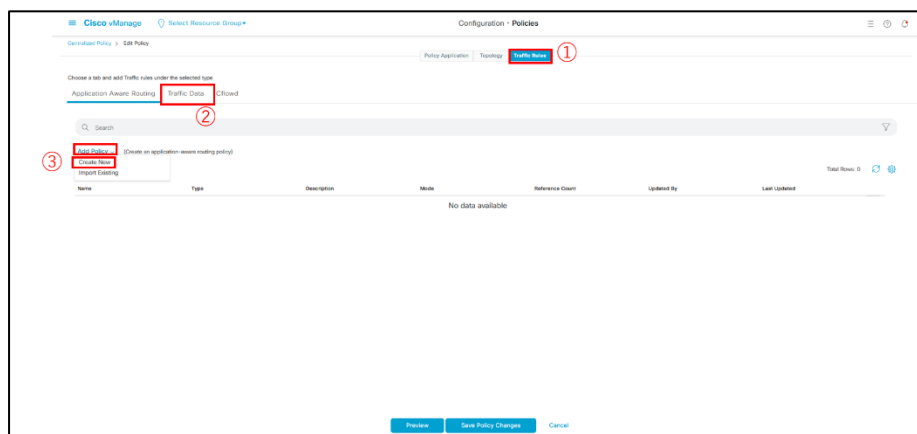
「Add Policy」を選択

右の画面が表示されるまで何もせず「Next」を選択(2回)



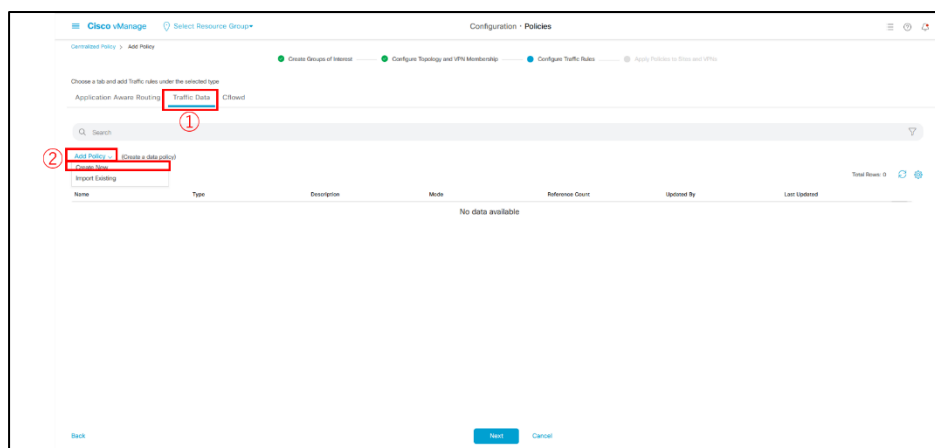
37. (NTT 東日本提供のデフォルトポリシーが表示される場合)

- ①画面上部の「Traffic Rules」を選択
- ②画面中部の「Traffic Data」を選択
- ③Add Policy から「Create New」を選択

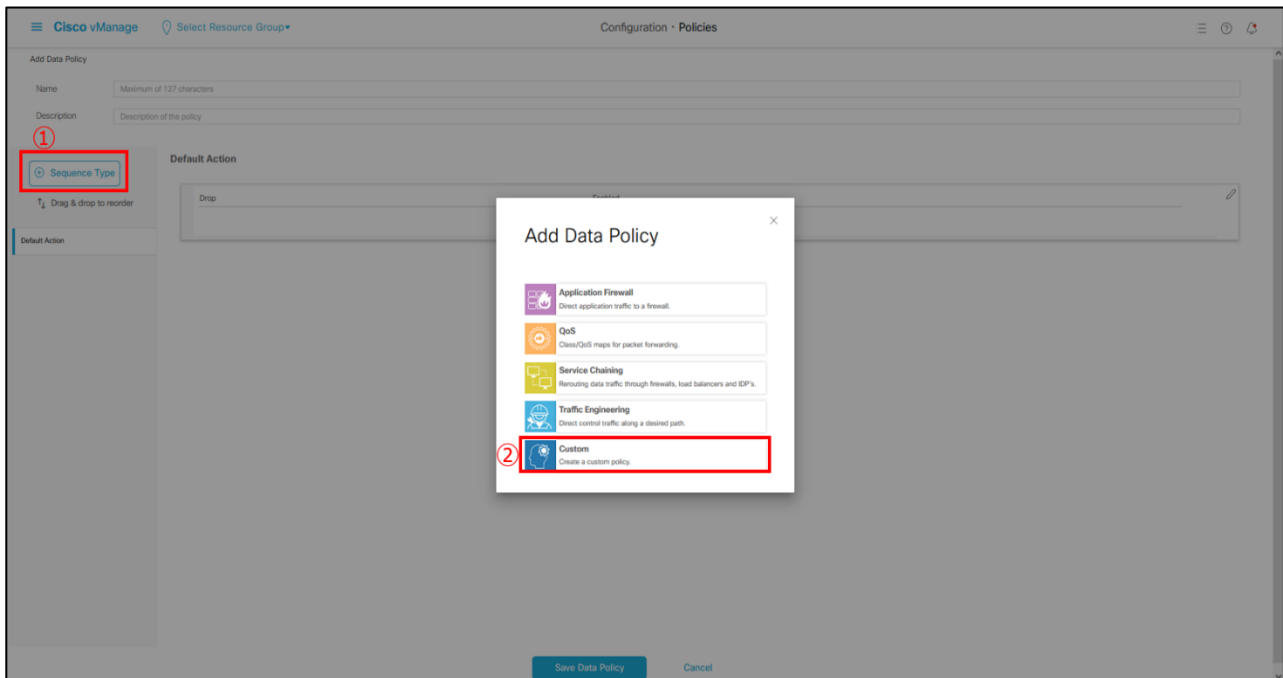


37. (NTT 東日本提供のデフォルトポリシーが表示されない場合)

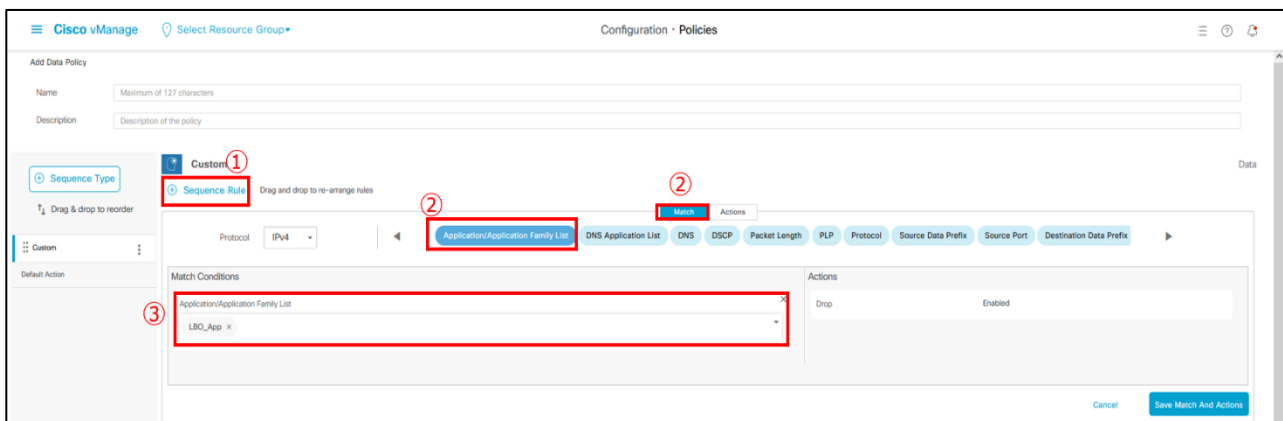
- ①画面中部の「Traffic Data」を選択
- ②Add Policy から「Create New」を選択



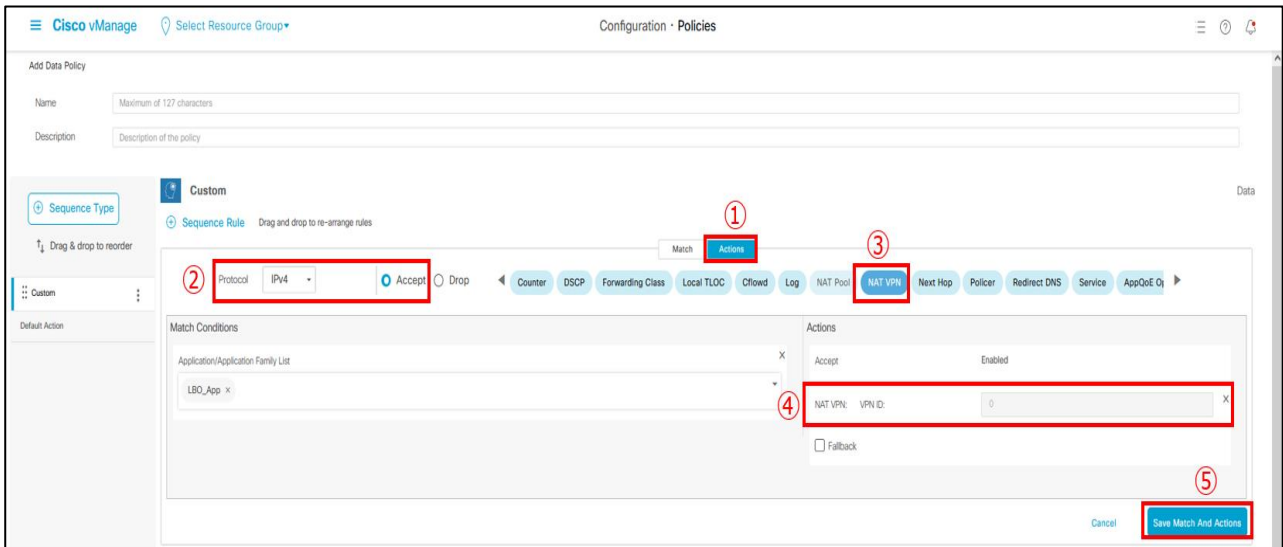
38. ① 「Sequence type」を選択
 ② 「Custom」を選択



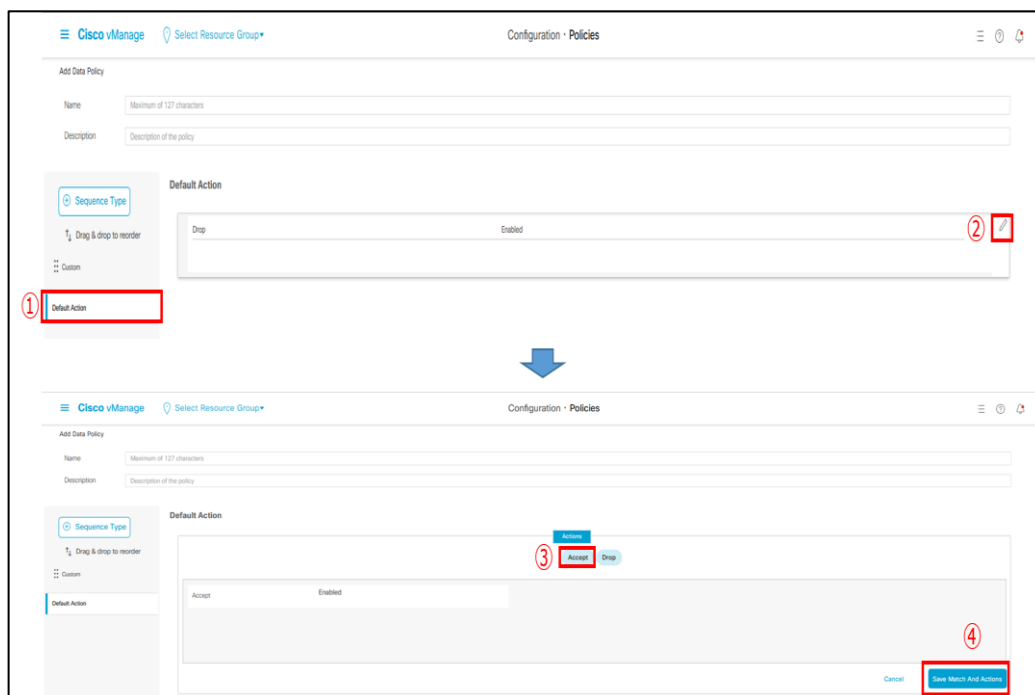
39. ① 「Sequence Rule」を選択
 ② Match タブから「Application/Application Family List」を選択
 ③ 「LBO_App」を入力



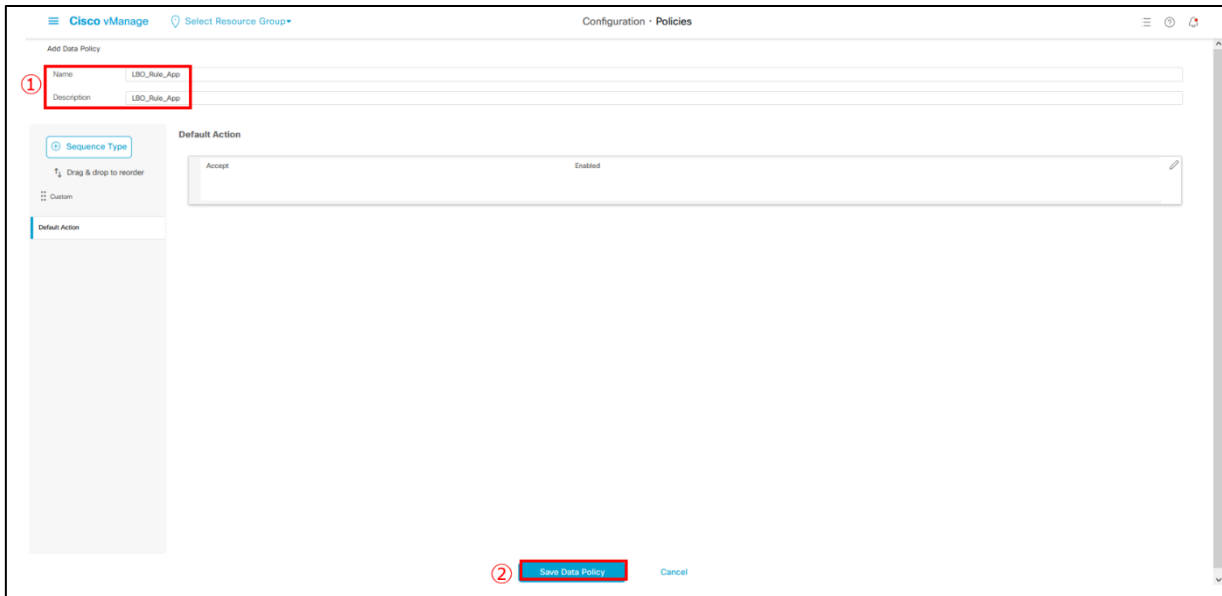
40. ①「Actions」タブを選択
- ②Protocol は「IPv4」、「Accept」を選択
- ③「NAT VPN」を選択
- ④NAT VPN ID が「0」になっていることを確認
- ⑤「Save Match And Action」を選択



41. ①Default Action をクリック
- ②ペンマークを選択して編集画面を開く
- ③Accept をクリック
- ④「Save Match And Action」を選択



42. ①Name および Description は「LBO_Rule_App」を入力
 ②「Save Data Policy」を選択



Configuration - Policies

Add Data Policy

① Name: LBO_Rule_App
 Description: LBO_Rule_App

Sequence Type
 Drag & drop to reorder
 Custom

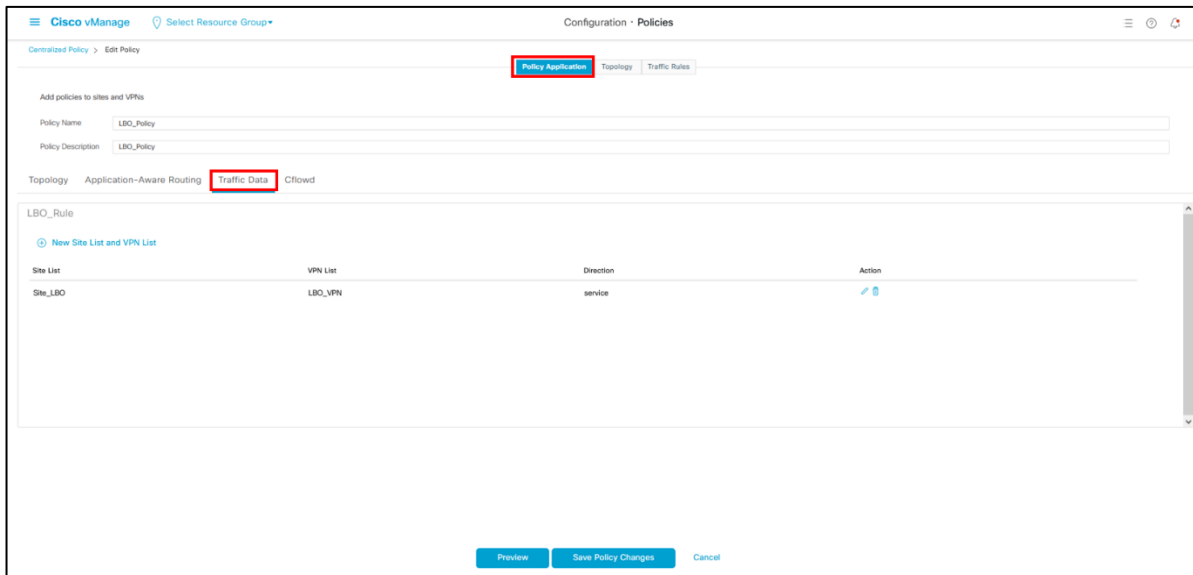
Default Action
 Accept Enabled

② Save Data Policy Cancel

43. (NTT 東日本提供のデフォルトポリシーが表示される場合)

画面上部のタブから「Policy Application」を選択

画面中部のタブから「Traffic Data」を選択



Configuration - Policies

Centralized Policy > Edit Policy

Policy Application Topology Traffic Rules

Add policies to sites and VPNs

Policy Name: LBO_Policy
 Policy Description: LBO_Policy

Topology Application-Aware Routing Traffic Data Cflowd

LBO_Rule

New Site List and VPN List

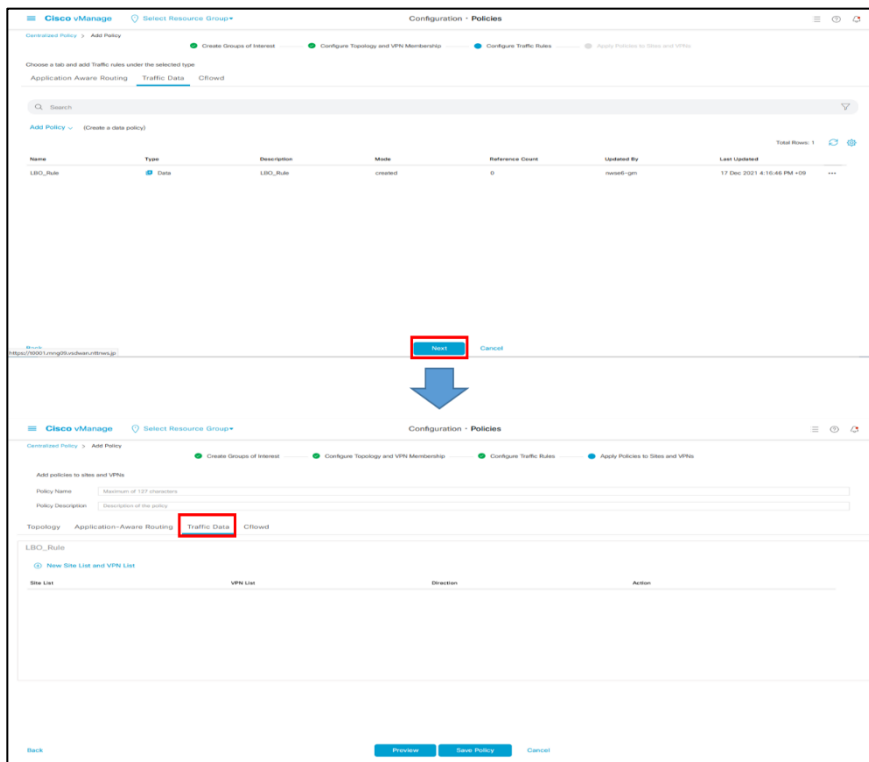
Site List	VPN List	Direction	Action
Site_LBO	LBO_VPN	service	

Preview Save Policy Changes Cancel

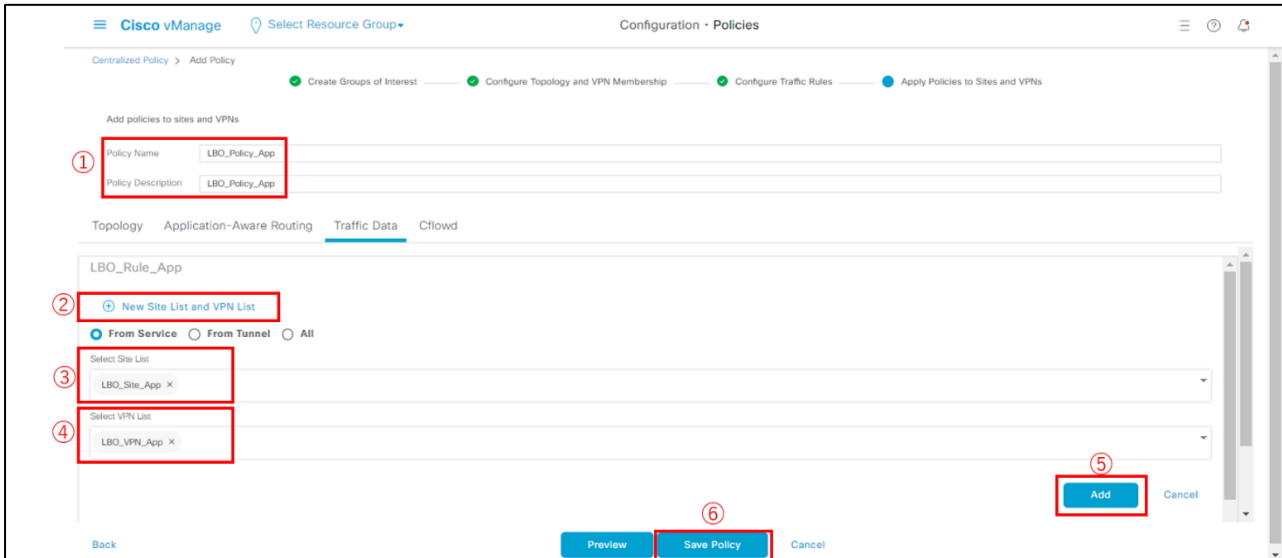
43. (NTT 東日本提供のデフォルトポリシーが表示されない場合)

上画面で「Next」を選択

下画面に遷移するので、中部のタブから「Traffic Data」を選択



44. ①Policy Name および Policy Description は「LBO_Policy_App」を入力
 ②「New Site List and VPN List」を選択
 ③Select Site List に「LBO_Site_App」を設定
 ④Select VPN List に「LBO_VPN_App」を設定
 ⑤「Add」を選択
 ⑥「Save Policy」※を選択
 ※既にポリシーがある場合には「Save Policy Changes」



The screenshot shows the Cisco vManage Configuration - Policies page. The page is titled "Configuration - Policies" and has a breadcrumb "Centralized Policy > Add Policy". The page is divided into four steps: "Create Groups of Interest", "Configure Topology and VPN Membership", "Configure Traffic Rules", and "Apply Policies to Sites and VPNs". The "Add Policy" form is shown with the following fields:

- Policy Name: LBO_Policy_App
- Policy Description: LBO_Policy_App

Below the form, there are tabs for "Topology", "Application-Aware Routing", "Traffic Data", and "Cflowd". The "Traffic Data" tab is selected. Under the "Traffic Data" tab, there is a section for "LBO_Rule_App" with a "New Site List and VPN List" button. Below this, there are radio buttons for "From Service" (selected), "From Tunnel", and "All". There are two dropdown menus: "Select Site List" with "LBO_Site_App" selected, and "Select VPN List" with "LBO_VPN_App" selected. At the bottom right, there is an "Add" button and a "Cancel" button. At the bottom center, there are "Preview", "Save Policy", and "Cancel" buttons.

4.8.4. LBO 接続制限設定

LBO接続制限を設定

※本項目は2台以上のCPEにてローカルブレイクアウトを設定し、さらにNTT東日本提供のデフォルトトポロジが作成されている場合の手順となります。デフォルトトポロジが作成されていない場合の手順については次版以降の記載となります。

45. 左ペイン(左の領域)の Configuration から「Policies」を選択
画面上部の「Custom Options」から「Topology」を選択

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	sdwan-order-ni	10052023T171944935	05 Oct 2023 5:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10312023T230653410	31 Oct 2023 3:10:57 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11062023T134056173	06 Nov 2023 1:40:56 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11062023T160759521	06 Nov 2023 4:07:59 PM +09

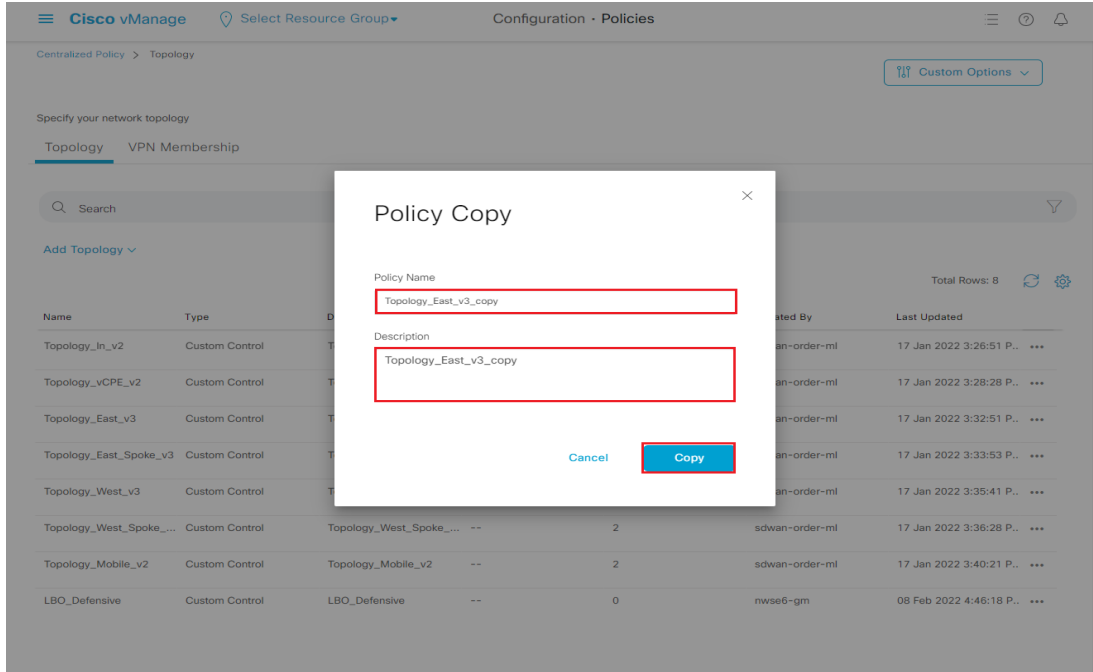
46. NTT 東日本デフォルトの Topology の「…」から「copy」を選択

※Topology_East,Topology_West から始まるトポロジ名が NTT 東日本提供のデフォルトトポロジになります。

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	Topology_In_v2	-	4	sdwan-order-ni	05 Oct 2023 4:13:09 PM +09
Topology_v_CPE_v2	Custom Control	Topology_v_CPE_v2	-	4	sdwan-order-ni	05 Oct 2023 4:15:55 PM +09
Topology_East_v3	Custom Control	Topology_East_v3	-	4	sdwan-order-ni	05 Oct 2023 4:25:23 PM +09
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	-	4	sdwan-order-ni	05 Oct 2023 4:37:35 PM +09
Topology_West_v3	Custom Control	Topology_West_v3	-	4	sdwan-order-ni	05 Oct 2023 4:49:03 PM +09
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	-	4	sdwan-order-ni	05 Oct 2023 5:03:27 PM +09
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	-	4	sdwan-order-ni	05 Oct 2023 5:14:21 PM +09

47. 「Policy Name」と「Description」に任意の名前と説明を入力する

※例ではどちらも「Topology_East_v3_copy」となります



Policy Copy

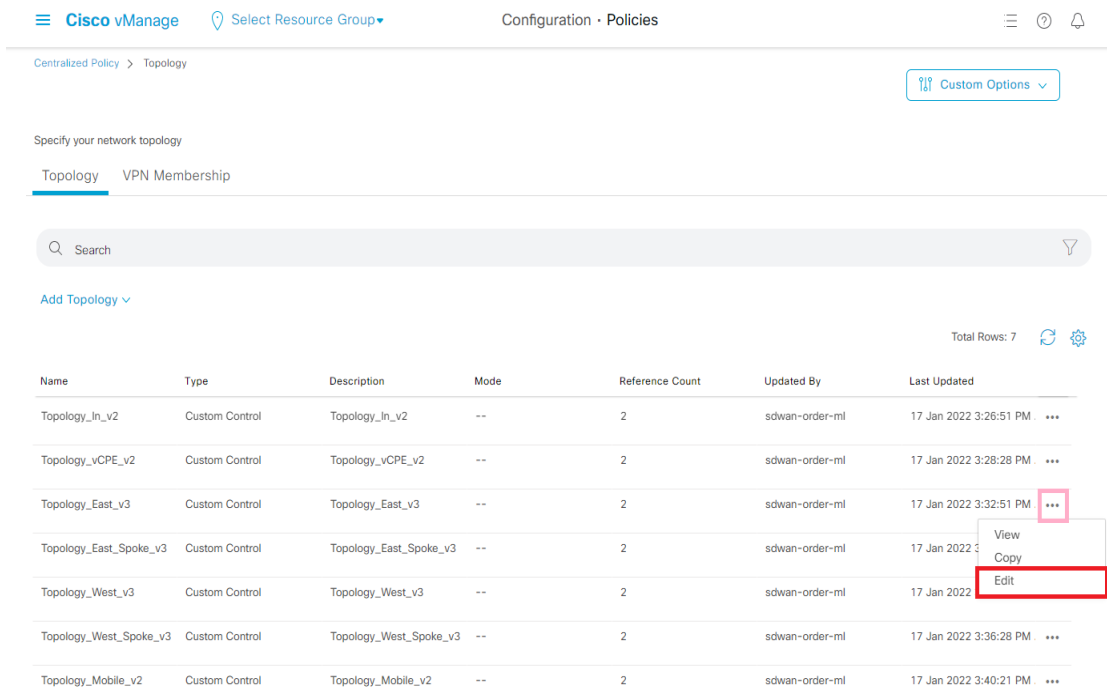
Policy Name
Topology_East_v3_copy

Description
Topology_East_v3_copy

Cancel Copy

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	Topology_In_v2	--	2	sdwan-order-ml	17 Jan 2022 3:26:51 P..
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	--	2	sdwan-order-ml	17 Jan 2022 3:28:28 P..
Topology_East_v3	Custom Control	Topology_East_v3	--	2	sdwan-order-ml	17 Jan 2022 3:32:51 P..
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	--	2	sdwan-order-ml	17 Jan 2022 3:33:53 P..
Topology_West_v3	Custom Control	Topology_West_v3	--	2	sdwan-order-ml	17 Jan 2022 3:35:41 P..
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	--	2	sdwan-order-ml	17 Jan 2022 3:36:28 P..
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	--	2	sdwan-order-ml	17 Jan 2022 3:40:21 P..
LBO_Defensive	Custom Control	LBO_Defensive	--	0	nwse6-gm	08 Feb 2022 4:46:18 P..

48. コピーした Topology の右枠の「…」から「Edit」を選択



Configuration · Policies

Centralized Policy > Topology

Specify your network topology

Topology VPN Membership

Search

Add Topology

Total Rows: 7

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	Topology_In_v2	--	2	sdwan-order-ml	17 Jan 2022 3:26:51 PM
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	--	2	sdwan-order-ml	17 Jan 2022 3:28:28 PM
Topology_East_v3	Custom Control	Topology_East_v3	--	2	sdwan-order-ml	17 Jan 2022 3:32:51 PM
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	--	2	sdwan-order-ml	17 Jan 2022 3:33:53 PM
Topology_West_v3	Custom Control	Topology_West_v3	--	2	sdwan-order-ml	17 Jan 2022 3:35:41 PM
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	--	2	sdwan-order-ml	17 Jan 2022 3:36:28 PM
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	--	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM

View
Copy
Edit

49. 左枠の「TLOC」を選択し、「Sequence Rule」を選択

Cisco vManage Select Resource Group Configuration · Policies

Centralized Policy > Topology > Edit Custom Control Policy

Name Topology_East_v3

Description Topology_East_v3

Sequence Type

Drag & drop to reorder

TLOC

Route

Default Action

TLOC

Sequence Rule Drag and drop to re-arrange rules

- Match Conditions

Site List: Site_vCPE

Site ID:

Actions

Accept
- Match Conditions

Site List: Site_East

Site ID:

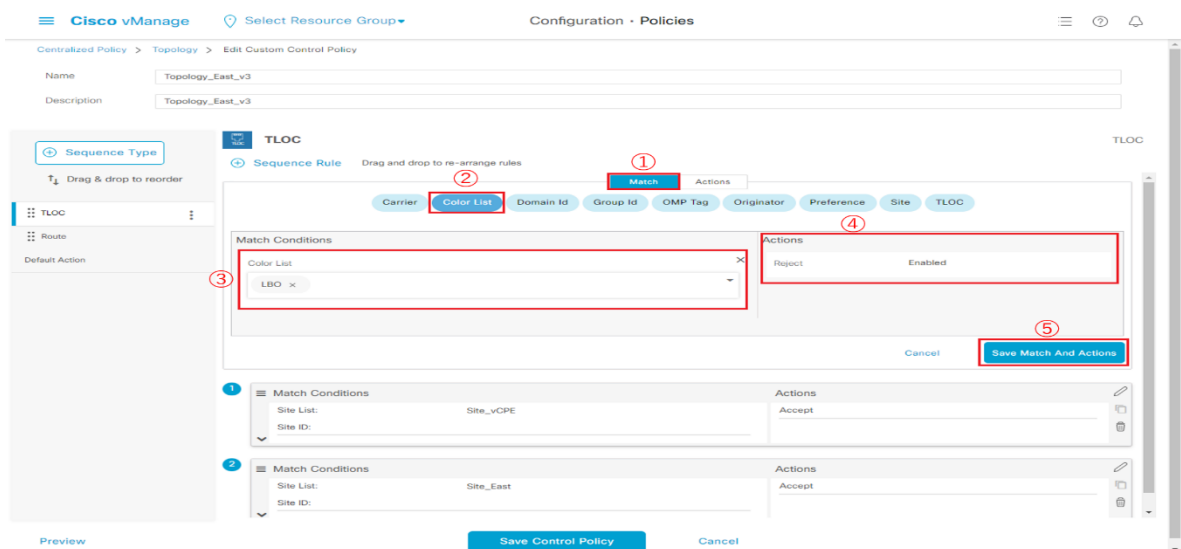
Actions

Accept

Preview

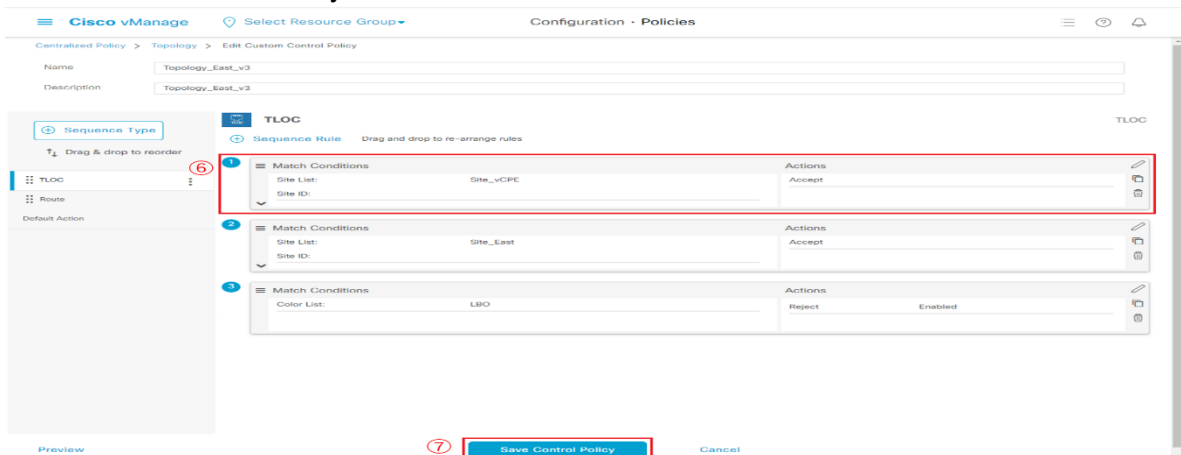
Save Control Policy Cancel

50. ①「Match」タブを選択
- ②「Color List」タブを選択
- ③手順 31 にて作成した「LBO」の Color List を選択
- ④「Actions」にて、Reject が「Enabled」であることを確認する。
- ※デフォルトでは Enabled のため、設定の変更は不要です
- ⑤「Save Match And Actions」を選択



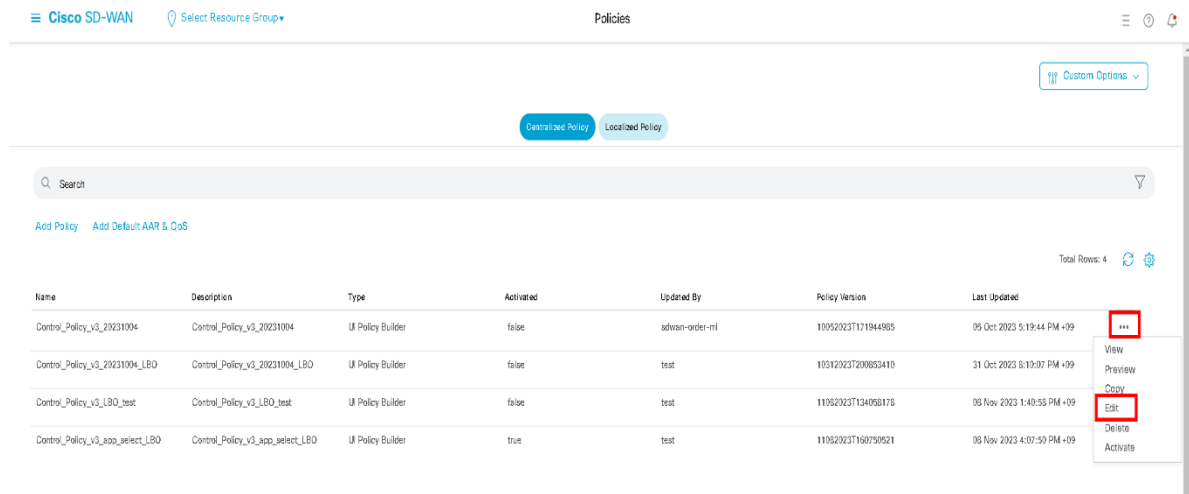
The screenshot shows the 'Configuration - Policies' page in Cisco vManage. The 'Match' tab is selected. Under 'Sequence Rule', the 'Color List' dropdown is set to 'LBO'. The 'Actions' section shows 'Reject' is 'Enabled'. The 'Save Match And Actions' button is highlighted with a red box and a circled 5.

- ⑥投入した設定を一番上の Sequence にドラッグ&ドロップ
- ⑦「Save Control Policy」を選択



The screenshot shows the 'Configuration - Policies' page in Cisco vManage. The 'LBO' rule is now at the top of the sequence. The 'Save Control Policy' button is highlighted with a red box and a circled 7.

51. 左ペイン(左の領域)の Configuration から「Policies」を選択
 手順 44 にて作成済みの Policy の右枠の「…」から「Edit」を選択



Custom Options

Centralized Policy Localized Policy

Search

Add Policy Add Default AAR & QoS

Total Rows: 4

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	sdwan-order-ml	11052023T171944585	05 Oct 2023 5:19:44 PM +09	...
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	110312023T200852410	31 Oct 2023 8:19:07 PM +09	
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11032023T134058176	06 Nov 2023 1:40:58 PM +09	
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11032023T160750521	06 Nov 2023 4:07:50 PM +09	

- View
- Preview
- Copy
- Edit**
- Delete
- Activate

52. ① 「Topology」タブを選択

②手順 50 で作成したトポロジのコピー元の「…」から「Detach」を選択

Configuration · Policies

Centralized Policy > Edit Policy

Policy Application **Topology** Traffic Rules

Specify your network topology

Topology VPN Membership

Search

Add Topology

Total Rows: 7

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	Topology_In_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:36:51 PM ...
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:36:51 PM ...
Topology_East_v3	Custom Control	Topology_East_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:32:51 PM ...
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:33:53 PM ...
Topology_West_v3	Custom Control	Topology_West_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:35:41 PM ...
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:36:28 PM ...
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM ...

Preview Save Policy Changes Cancel

53. 「Add Topology」→「Import Existing Topology」を選択

Configuration · Policies

Centralized Policy > Edit Policy

Policy Application **Topology** Traffic Rules

Specify your network topology

Topology VPN Membership

Search

Add Topology

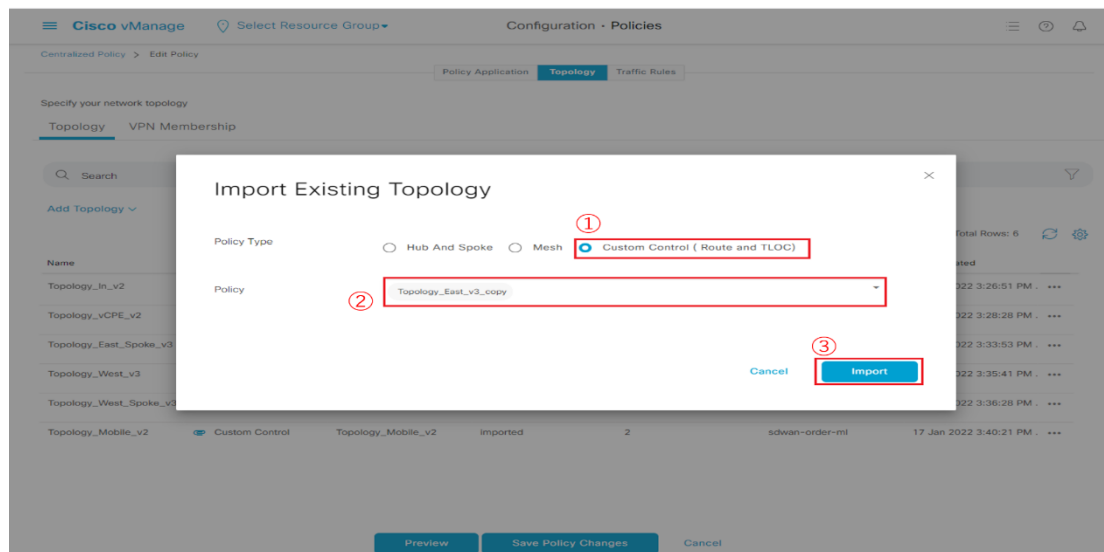
- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)
- Import Existing Topology

Total Rows: 6

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
Topology_In_v2	Custom Control	Topology_In_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:26:51 PM ...
Topology_vCPE_v2	Custom Control	Topology_vCPE_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:28:28 PM ...
Topology_East_Spoke_v3	Custom Control	Topology_East_Spoke_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:33:53 PM ...
Topology_West_v3	Custom Control	Topology_West_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:35:41 PM ...
Topology_West_Spoke_v3	Custom Control	Topology_West_Spoke_v3	imported	2	sdwan-order-ml	17 Jan 2022 3:36:28 PM ...
Topology_Mobile_v2	Custom Control	Topology_Mobile_v2	imported	2	sdwan-order-ml	17 Jan 2022 3:40:21 PM ...

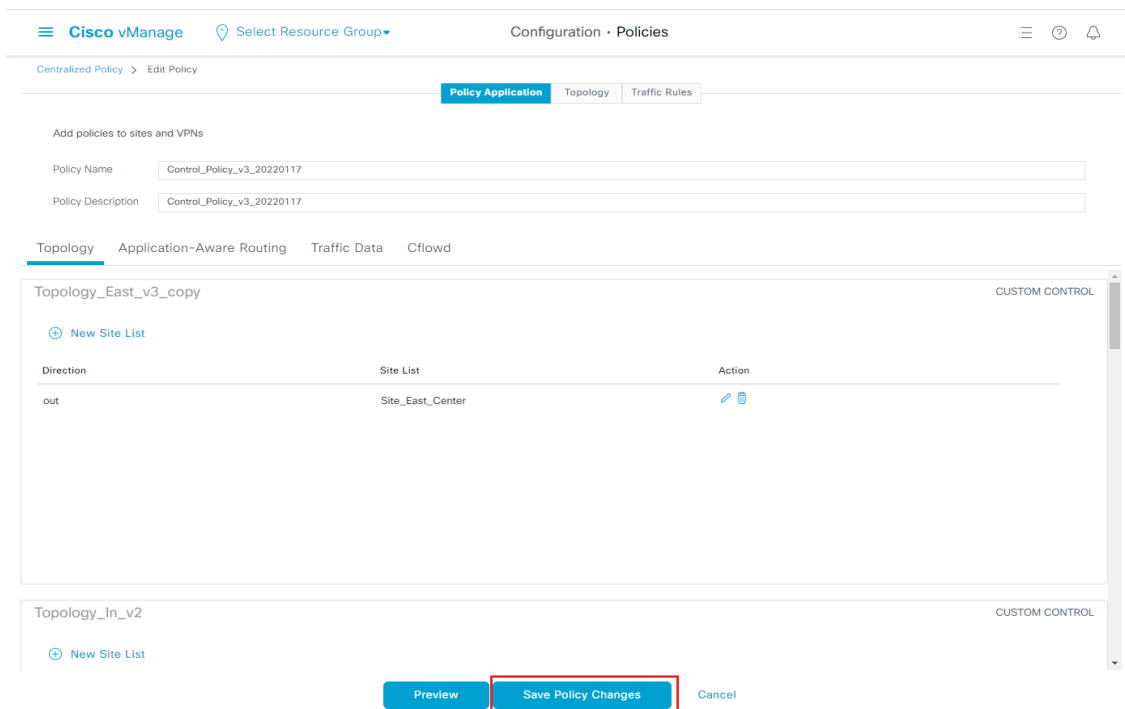
Preview Save Policy Changes Cancel

54. ①「Custom Control(Route and TLOC)」を選択
 ②手順 50 で作成したトポロジを選択
 ③「Import」を選択



55. ① 「Policy Application」 タブを選択
- ② 「Topology」 タブを選択
- ③ 手順 54 で Import したトポロジの欄を選択
- ④ 「New Site List」 を選択
- ⑤ Outbound Site List に 各トポロジに対応した SiteList を入力
※各トポロジに対応した SiteList は以下の通りです
Topology_East:Site_East_Center
Topology_West:Site_West_Center
- ⑥ 「Add」 を選択

56. 「Save Policy Changes」 を選択



Centralized Policy > Edit Policy



Policy Name: Control_Policy_v3_20220117

Policy Description: Control_Policy_v3_20220117

Topology Application-Aware Routing Traffic Data Cflowd

Topology_East_v3_copy

Direction Site List Action

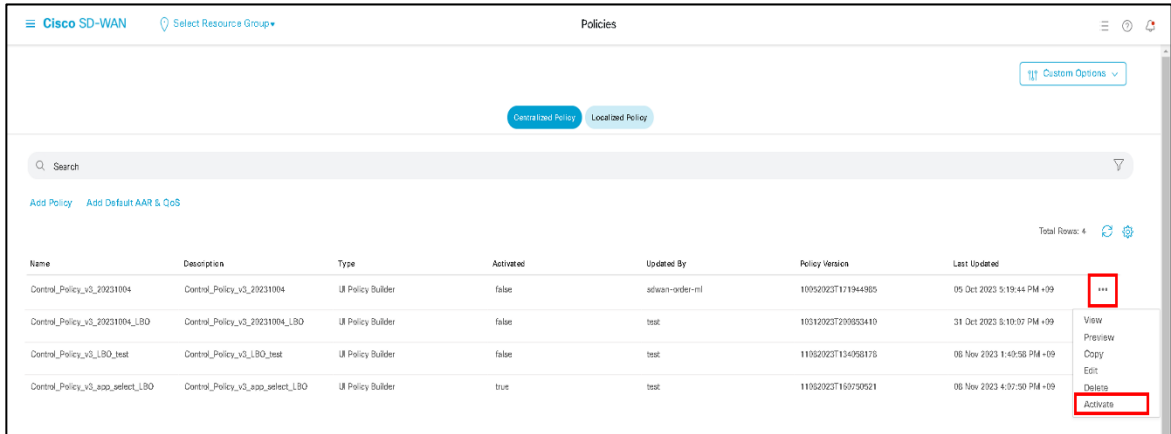
out	Site_East_Center	 
-----	------------------	---

Topology_In_v2

Preview Save Policy Changes Cancel

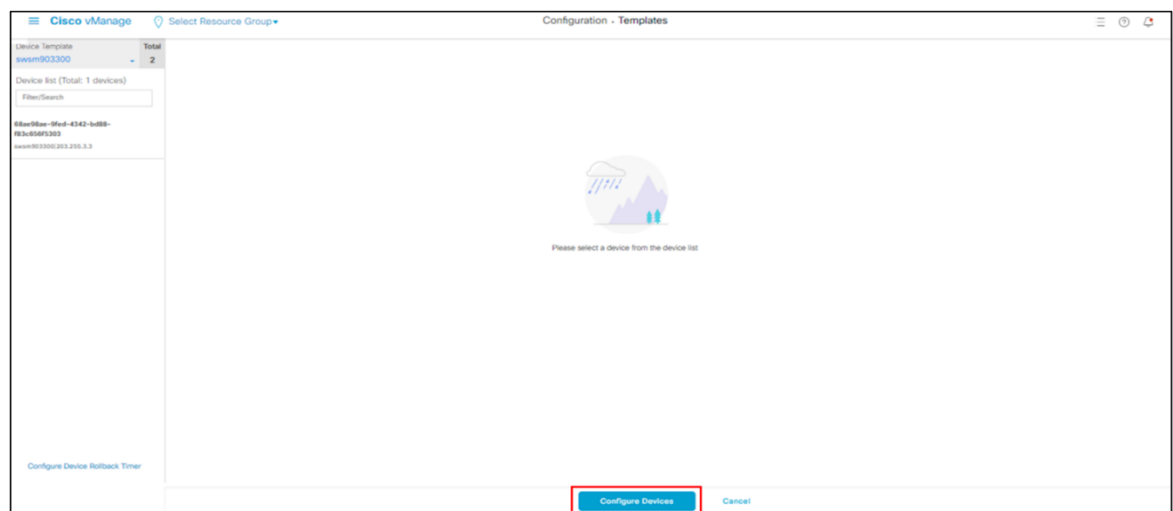
4.8.5. ポリシーの有効化

57. 手順 56 までで作成したポリシーの「…」から「Activate」を選択
⇒選択後のポップアップ画面で「Activate」を選択

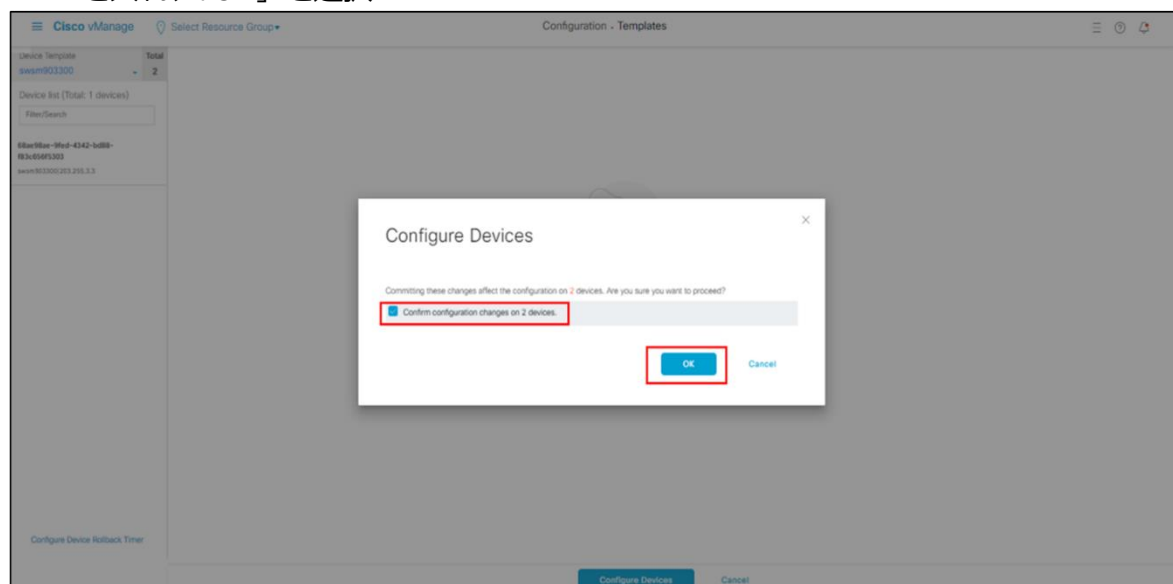


Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	adwan-order-nl	110520237171944905	05 Oct 2023 3:19:44 PM +09	...
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10312023720953410	31 Oct 2023 3:10:07 PM +09	View Preview Copy Edit Delete Activate
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	110520237134056176	06 Nov 2023 1:49:56 PM +09	
Control_Policy_v3_sso_select_LBO	Control_Policy_v3_sso_select_LBO	UI Policy Builder	true	test	110520237150750521	06 Nov 2023 4:57:50 PM +09	

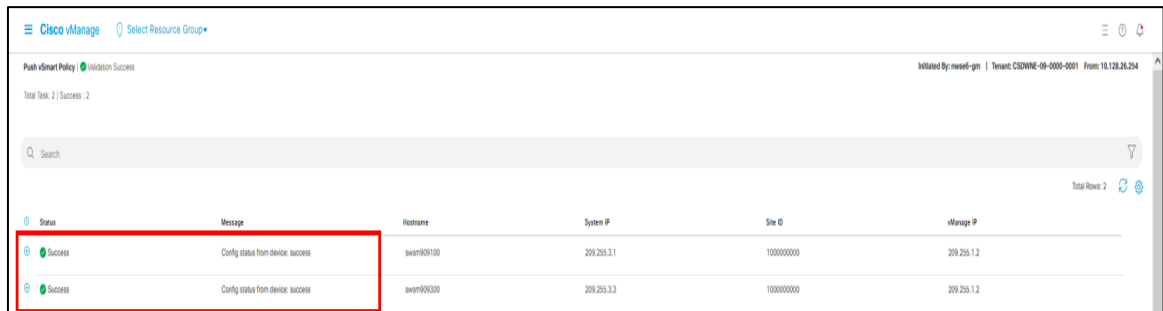
58. 下記画面へ遷移するので「Configure Devices」を選択



59. 下記画面へ遷移するので「Confirm Configuration changes on 2 devices」にチェックを入れ、「OK」を選択



60. Status が success, Message が Done となっていればコンフィグ適用が完了
⇒Status 変更までに 1 分程度かかります



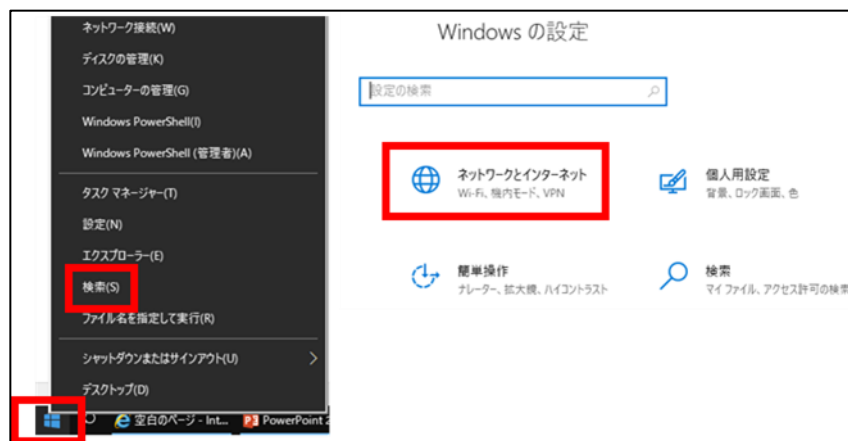
The screenshot shows the Cisco vManage interface with a table displaying the status of configuration pushes. The table has columns for Status, Message, Hostname, System IP, Size ID, and vManage IP. Two rows are shown, both with a status of 'Success' and a message of 'Config status from device: success'. The first row is for device 'swan900100' and the second for 'swan900300'. A red box highlights the first two rows.

Status	Message	Hostname	System IP	Size ID	vManage IP
Success	Config status from device: success	swan900100	209.255.3.1	1000000000	209.255.1.2
Success	Config status from device: success	swan900300	209.255.3.3	1000000000	209.255.1.2

4.8.6. プロキシサーバ利用時の留意点

アプリ指定でインターネットブレイクアウトを利用し、インターネット向けの社内プロキシがある場合には端末にプロキシ除外設定が必要となります。

1. [スタート]メニューを右クリックし、[設定]をクリックし、[ネットワークとインターネット]を選択



2. [プロキシ]をクリックし、インターネットブレイクアウト対象の URL を設定し、保存

設定

ホーム

設定の検索

ネットワークとインターネット

状態

イーサネット


ダイヤルアップ

VPN

プロキシ

状態

ネットワークの状態



インターネットに接続されています

制限付きのデータ通信プランをお使いの場合は、このネットワークを従量制課金接続に設定するか、またはその他のプロバイダを変更できます。

[接続プロバイダの変更](#)

[利用できるネットワークの表示](#)

手動プロキシ セットアップ

イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。

プロキシ サーバーを使う

☒ オン

アドレス

ポート

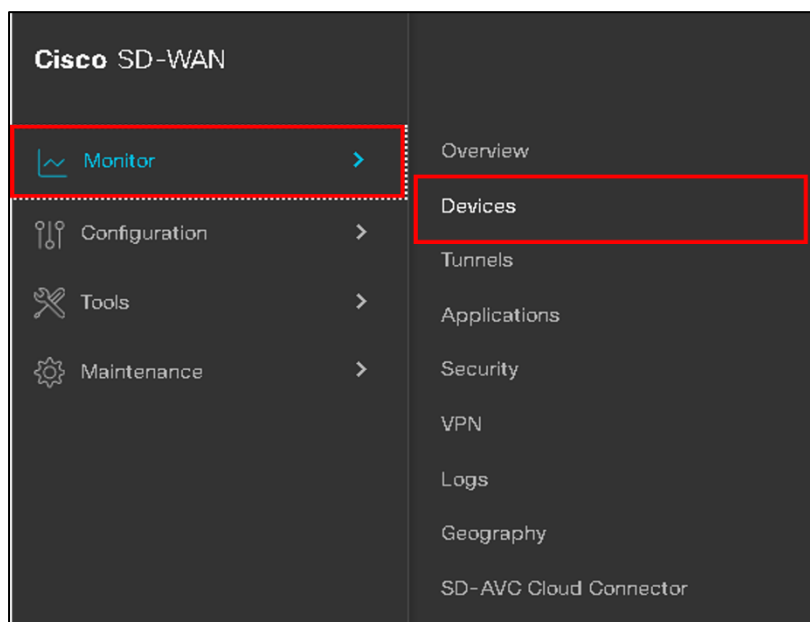
次のエントリで始まるアドレス以外にプロキシ サーバーを使います。エントリを区切るにはセミコロン (;) を使います。

☐ ローカル (イントラネット) のアドレスにはプロキシ サーバーを使わない

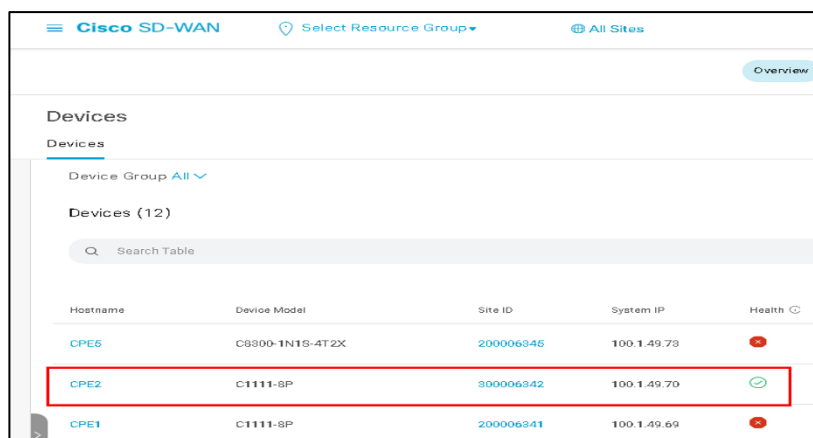
4.8.7. アプリ指定インターネットブレイクアウトの確認方法

アプリ指定のインターネットブレイクアウトのトラフィックを確認する手順は以下の通りです。

1. 左ペイン(左の領域)から Monitor→Devices を選択



2. 確認したい CPE を選択



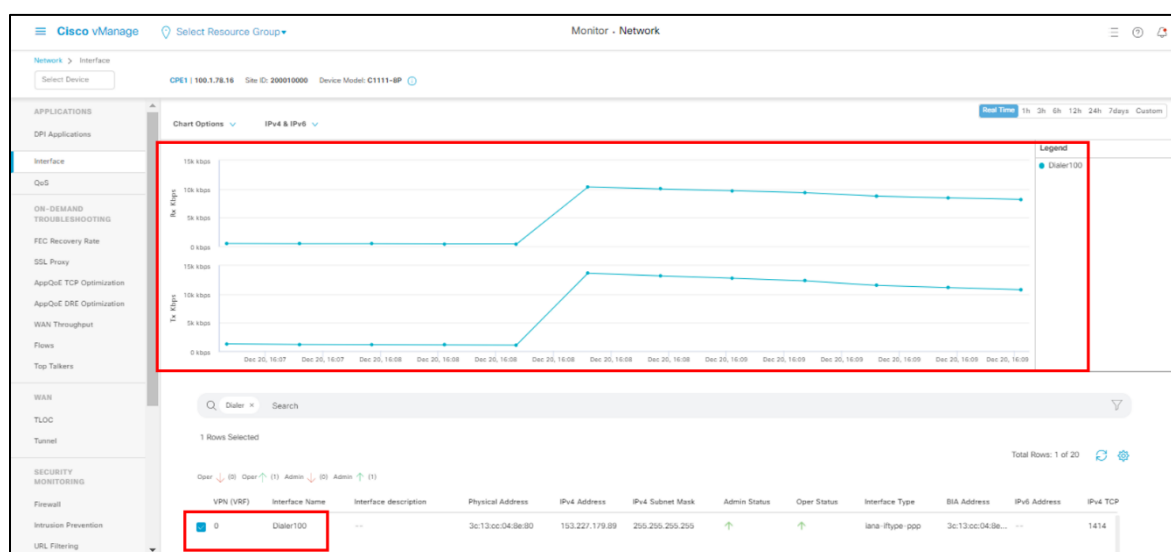
The screenshot shows the 'Devices' page in the Cisco SD-WAN interface. A table lists 12 devices. The row for 'CPE2' is highlighted with a red box. The table has the following columns: Hostname, Device Model, Site ID, System IP, and Health.

Hostname	Device Model	Site ID	System IP	Health
CPE5	C6300-1N1S-4T2X	200006346	100.1.49.73	🔴
CPE2	C1111-8P	300006342	100.1.49.70	🟢
CPE1	C1111-8P	200006341	100.1.49.69	🔴

3. Interface を選択



4. Interface Name の Dialer にチェックを入れ、グラフにてトラフィックが流れていることを確認

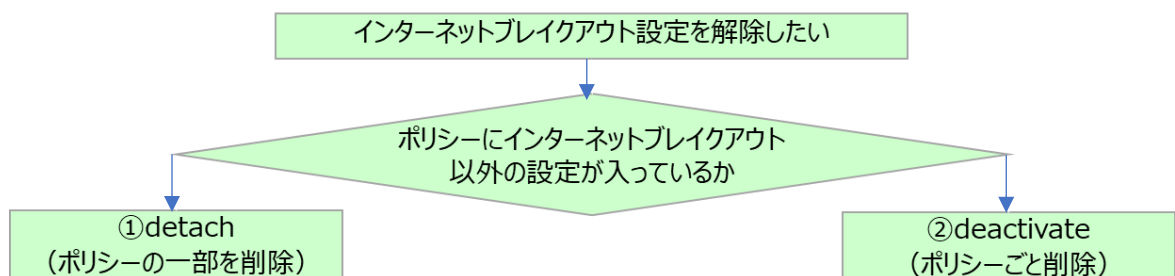


4.9. インターネットブレイクアウト設定の解除方法

インターネットブレイクアウト設定を解除したい場合、以降の手順を実施します。全拠点のインターネットブレイクアウト設定を解除します。ポリシーにインターネットブレイクアウト以外の設定が入っている場合は「①detach」、インターネットブレイクアウトのみの場合は「②deactivate」を実施します。

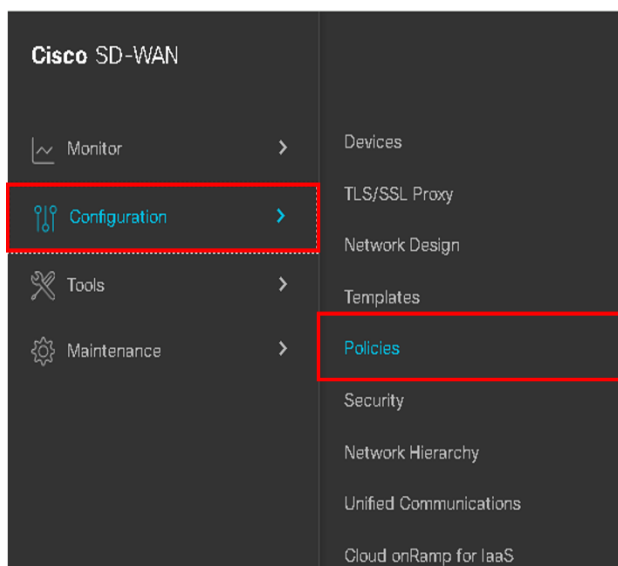
※PPPoEのテンプレートの削除はできませんが、インターネットブレイクアウトの設定解除が可能です。

※設定解除後の確認は4.8.2章の4の手順にて、Dialerにチェックを入れ、グラフにてトラフィックが流れていないことを確認願います。



4.9.1. ①ポリシーにインターネットブレイクアウト以外の設定が入っている場合の解除方法(detach)

1. 左ペイン(左の領域から Configuration→Policies を選択



2. 解除したいポリシー→Edit を選択

Name	Resource Group	Type	Associated By	Associated To	Policy Version	Last Updated	Actions
Control_Policy_v3_20231004	Control_Policy_v3_20231004	LR Policy Builder	Admin	admin-center-01	3/20/2023 12:12:14 PM +09:00	03 Oct 2023 10:10:45 PM +09	Edit
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	LR Policy Builder	Admin	test	3/20/2023 12:08:52 PM +09:00	31 Oct 2023 10:10:45 PM +09	Edit
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	LR Policy Builder	Admin	test	3/20/2023 12:08:52 PM +09:00	03 Oct 2023 10:10:45 PM +09	Edit
Control_Policy_v3_LBO_admin-01	Control_Policy_v3_LBO_admin-01	LR Policy Builder	Admin	test	3/20/2023 12:08:52 PM +09:00	03 Oct 2023 10:10:45 PM +09	Edit

3. Policy Application の Traffic Rules に既に設定が入っていることを確認する

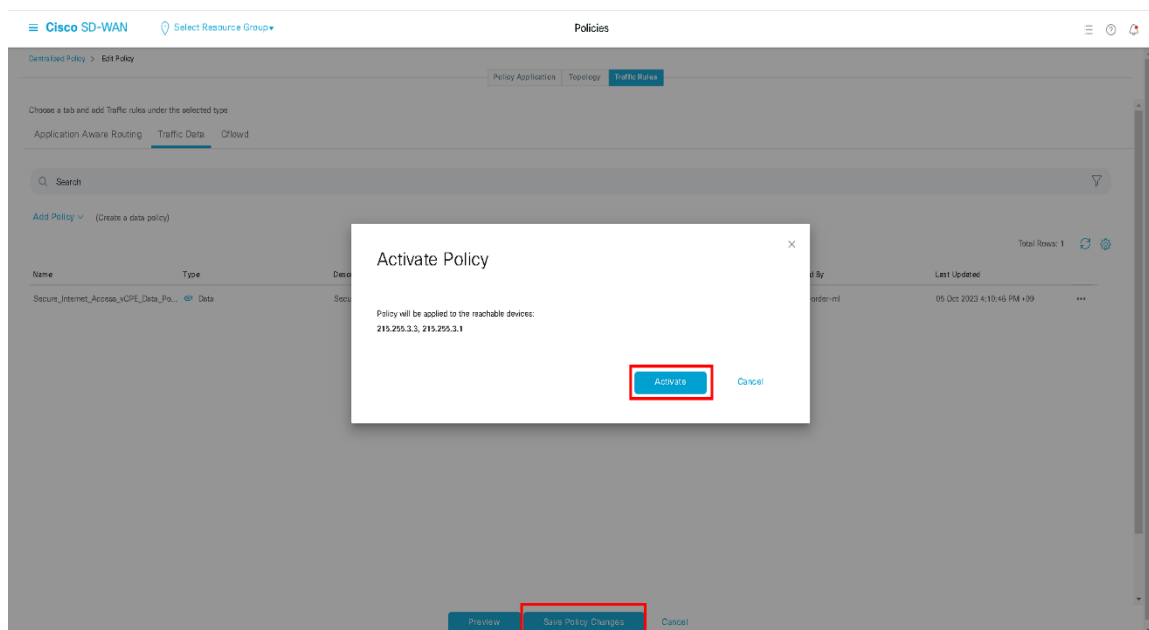
Name	Type	Description	Mode	Reference Count	Updated By	Last Updated	Actions
LBO_PPPoE	Data	LBO_PPPoE	Imported	2	test	31 Oct 2023 7:44:23 PM +09	View Copy Detach
Secure_Internet_Access_vCPE_Data_Po...	Data	Secure_Internet_Access_vCPE_Data_Po...	Imported	4	sdwan-order-ml	05 Oct 2023 4:10:45 PM +09	View Copy Detach

(※設定が入っていない場合はdeactivateの手順を実施します)

4. Traffic Rules→解除したいポリシー→Detach を選択する

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated	Actions
LBO_PPPoE	Data	LBO_PPPoE	Imported	2	test	31 Oct 2023 7:44:23 PM +09	View Copy Detach
Secure_Internet_Access_vCPE_Data_Po...	Data	Secure_Internet_Access_vCPE_Data_Po...	Imported	4	sdwan-order-ml	05 Oct 2023 4:10:45 PM +09	View Copy Detach

5. Activate→Save Policy Changes を選択する



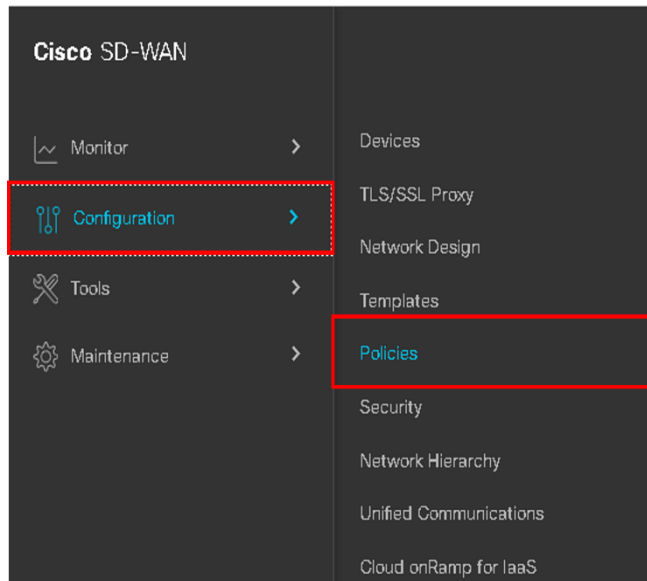
6. Status が success, Message が Done となっていればコンフィグ適用が完了 ⇒Status 変更までに 1 分程度かかります

Cisco SD-WAN Select Resource Group					
Status	Message	Hostname	System IP	Site ID	vManage IP
Success	Config status from device: success	swam815010	215.255.3.1	1000000000	215.255.1.3
Success	Config status from device: success	swam815030	215.255.3.3	1000000000	215.255.1.3

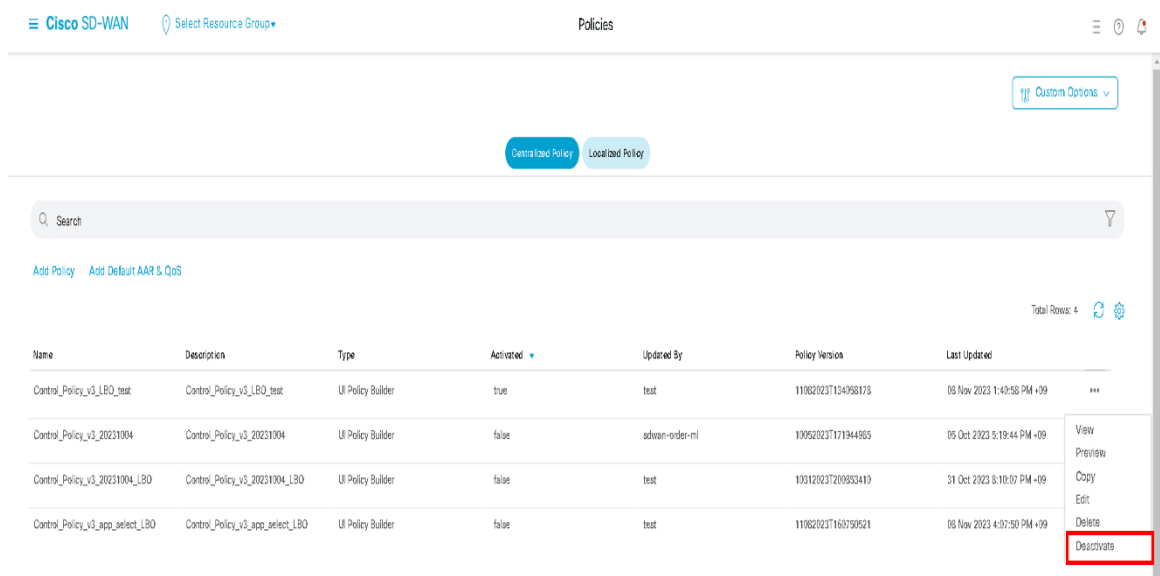
4.9.2. ②ポリシーにインターネットブレイクアウトのみが入っている場合の解除方法(deactivate)

※①ブレイクアウト設定の解除方法(detach)の手順 3 で、設定が無かったことを前提とする手順です)

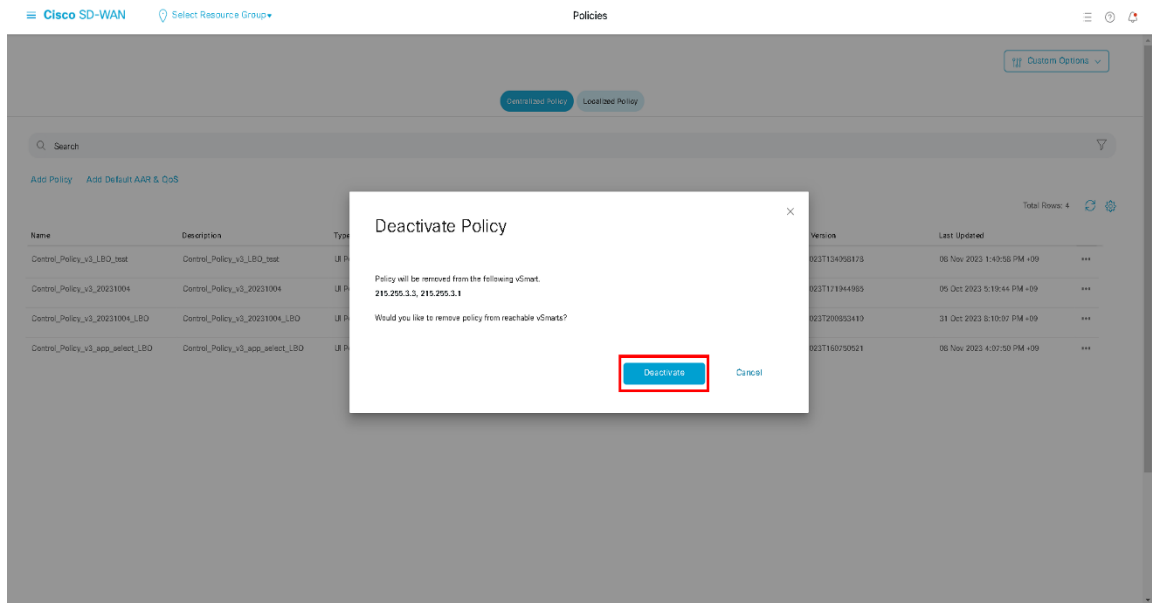
1. 左ペイン(左の領域から Configuration→Policies を選択



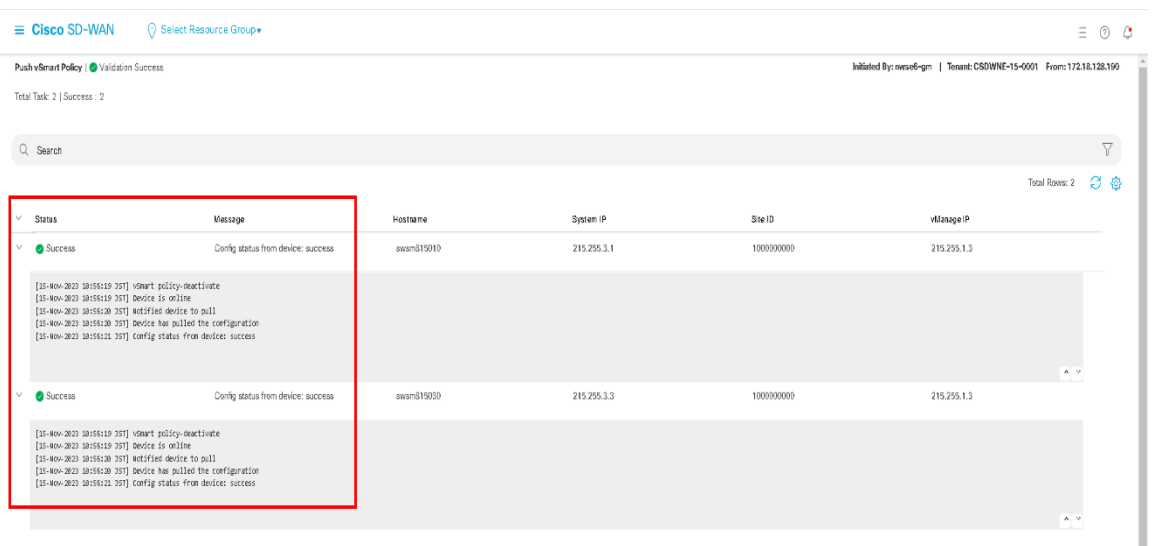
2. 解除したいポリシー→Deactivate を選択する



3. Deactivate を選択する



4. Status が success, Message が Done となっていればコンフィグ適用が完了 ⇒Status 変更までに 1 分程度かかります

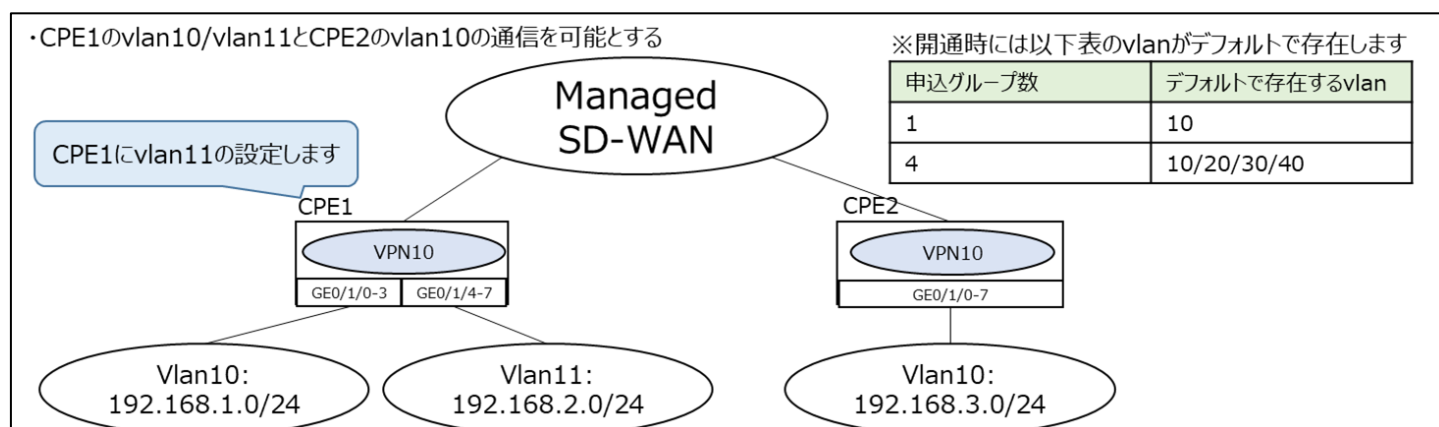


4.10. VLAN の分割

CPE に複数の VLAN を設定して複数 NW セグメントを設定したい場合、次ページ以降の手順を実施します

(※4.10 VLAN 分割は同一 VPN グループでセグメント分けをするための手順となります。アクセスリスト等で VLAN 間通信を不可とする手順は次版以降で記載します。)

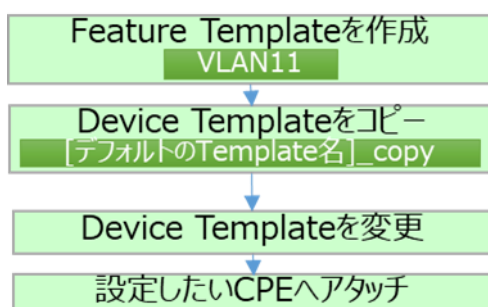
4.10.1. NW 構成例



【Device Template 作成に必要な Feature Template】

作成する Feature Template	手順	用途
VLAN11	1～3	VLAN 追加用 SVI

【設定の流れ】



4.10.2. 追加 VLAN 用 Feature Template を作成

Feature Template を作成
VALN11

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択後に「Add Template」を選択

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
ISR1100X-4G_202-22_VPN...	ISR1100X-4G_202-22_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	0	global	1	Provider-sdwan-order-nl	05 Oct 2023 22:51:19 PM
C8300-1N1S-4T2X_203-7...	C8300-1N1S-4T2X_203-7...	Cisco VPN interface Ethernet	C8300-1N1S-4T2X	1	global	1	Provider-sdwan-order-nl	05 Oct 2023 13:05:50 PM
C8300-1N1S-4T2X_203-5...	C8300-1N1S-4T2X_203-5...	Cisco VPN interface Ethernet	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-nl	04 Oct 2023 8:13:26 PM
C8300-1N1S-4T2X_203-5...	C8300-1N1S-4T2X_203-5...	Cisco VPN interface Ethernet	C8300-1N1S-4T2X	2	global	2	Provider-sdwan-order-nl	04 Oct 2023 8:15:37 PM
C8300-1N1S-4T2X_203-5...	C8300-1N1S-4T2X_203-5...	Cisco VPN interface Ethernet	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-nl	04 Oct 2023 8:17:19 PM
C8300-1N1S-4T2X_203-1...	C8300-1N1S-4T2X_203-1...	WAN large edge Cellular n...	C8300-1N1S-4T2X	2	global	2	Provider-sdwan-order-nl	05 Oct 2023 13:06:10 PM
C8300-1N1S-4T2X_303-1...	C8300-1N1S-4T2X_303-1...	CU Template	C8300-1N1S-4T2X	1	global	1	Provider-sdwan-order-nl	05 Oct 2023 13:35:04 PM
ISR1100X-4G_202-11_VPN...	ISR1100X-4G_202-11_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	0	global	1	Provider-sdwan-order-nl	05 Oct 2023 22:43:51 PM
C8300-1N1S-4T2X_303-1...	C8300-1N1S-4T2X_303-1...	Cellular Controller	C8300-1N1S-4T2X	3	global	2	Provider-sdwan-order-nl	05 Oct 2023 13:38:41 PM
ISR1100X-4G_202-23_VPN...	ISR1100X-4G_202-23_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	0	global	1	Provider-sdwan-order-nl	05 Oct 2023 22:54:44 PM
ISR1100X-4G_202-25_VPN...	ISR1100X-4G_202-25_VPN...	Cisco VPN	ISR1100X 4G (Cisco OS)	1	global	0	Provider-sdwan-order-nl	05 Oct 2023 22:56:12 PM
ISR1100X-4G_203-51_VF...	ISR1100X-4G_203-51_VF...	Cisco VPN interface Ethernet	ISR1100X 4G (Cisco OS)	0	global	1	Provider-sdwan-order-nl	05 Oct 2023 11:10:26 AM

2. Select Devices の「C1111-8P」にチェックをいれ、「VPN Interface SVI」を選択
※タイプ II の CPE へ設定する場合は「C1111-8PLTELA」にチェック
※ハイエンドタイプなら「C8300-1N1S-4T2X」にチェック
※モデルタイプなら「ISR 1100X 4G (Viptela OS)」にチェック

Select Devices

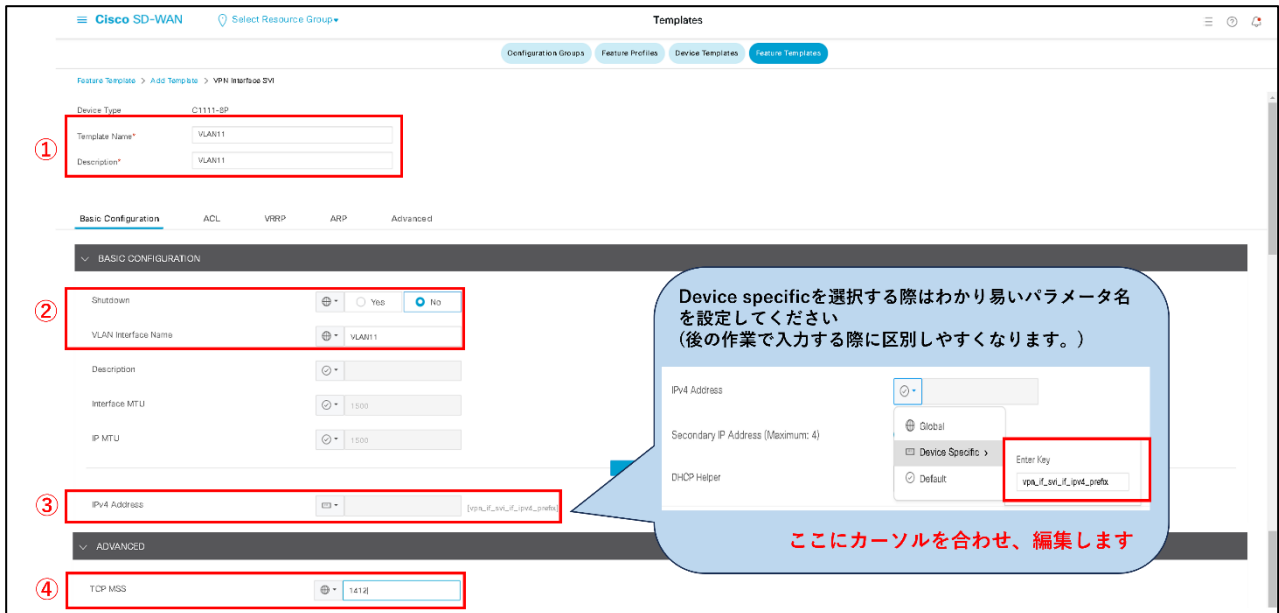
Search by device name

- ☐ C1101-4PLTEPW*
- ☐ C1109-2PLTEGB
- ☐ C1109-2PLTEUS
- ☐ C1109-2PLTEVZ
- ☐ C1109-4PLTE2P
- ☐ C1109-4PLTE2PW*
- ☐ C1111-4P
- ☐ C1111-4PLTEEA
- ☐ C1111-4PLTELA
- ☐ C1111-4PW*
- ☒ C1111-8P
- ☐ C1111-8PLTEEA
- ☐ C1111-RPI TFFAW*

OTHER TEMPLATES

- Cisco VPN Interface GRE (WAN)
- Cisco VPN Interface IPsec (WAN)
- VPN Interface Ethernet PPPoE (WAN)
- VPN Interface Multilink (WAN, LAN)
- VPN Interface SVI (Management, WAN, LAN)
- Cisco Banner
- Cisco BGP (WAN, LAN)
- Cisco DHCP Server (LAN)

3. ①Template Name/Description へ「VLAN11」を入力
- ②Shutdown を Global で「no」, VLAN Interface Name を Global で「Vlan11」と入力
- ③IPv4 Address を「device specific」と選択
- ④TCP MSS を「1412(GRE の場合)もしくは 1378(IPsec の場合)」に変更
- 最後に「Save」を選択



① Template Name/Description へ「VLAN11」を入力

② Shutdown を Global で「no」, VLAN Interface Name を Global で「Vlan11」と入力

③ IPv4 Address を「device specific」と選択

④ TCP MSS を「1412(GRE の場合)もしくは 1378(IPsec の場合)」に変更

最後に「Save」を選択

Device specificを選択する際はわかり易いパラメータ名を設定してください
(後の作業で入力する際に区別しやすくなります。)

ここにカーソルを合わせ、編集します

4.10.3. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

Device Template をコピー

- 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Devices」を選択
NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	sdwan-order-mf	10052023T171944985	05 Oct 2023 5:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10242023T200653410	31 Oct 2023 8:10:07 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11062023T134058176	06 Nov 2023 1:40:58 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11062023T150750521	06 Nov 2023 4:07:50 PM +09

4.10.4. Device Template に追加 VLAN 用の Template を作成

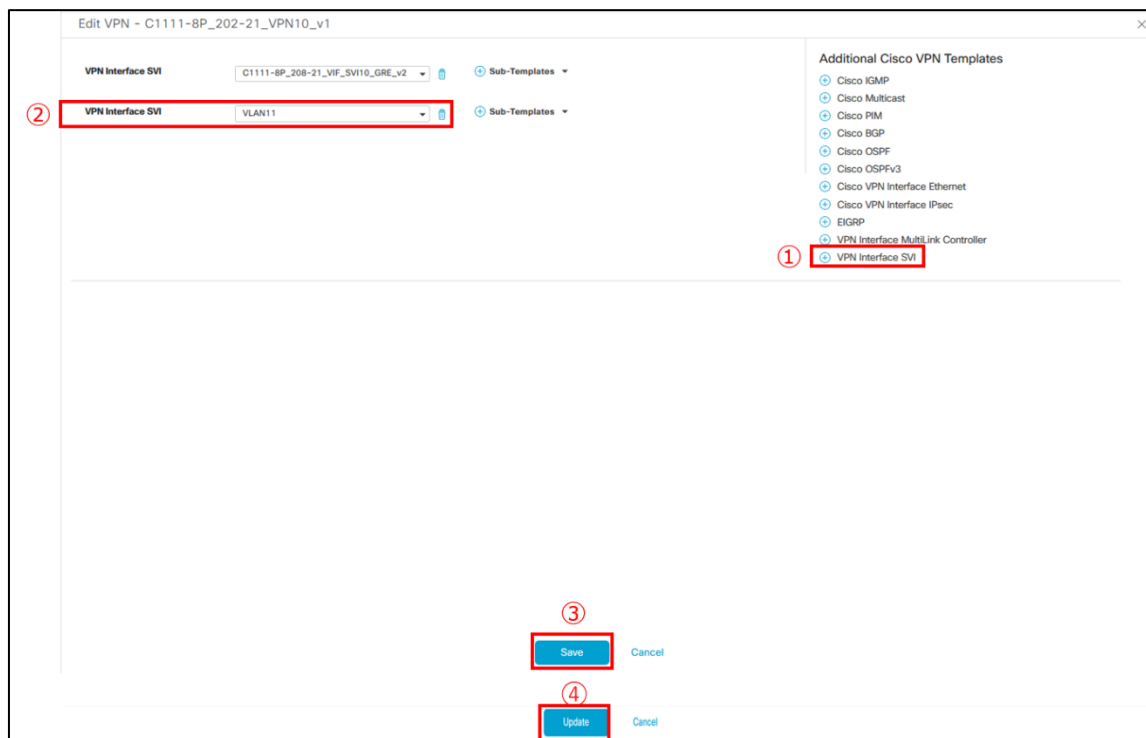
Device Template を変更

- Service VPN 欄の「…」から「Edit」を選択
※VPN が複数ある場合は、vlan を追加したい対象の VPN を選択

VPNが複数設定されている場合、左枠の欄にチェックを入れ、どのVPNにVLANを追加するか選択する

Template Name	Sub-Templates
C1111-6P_202-01_VPN10_v2	VPN Interface SVI
C1111-6P_202-02_VPN20_v2	VPN Interface SVI
C1111-6P_202-03_VPN30_v2	VPN Interface SVI

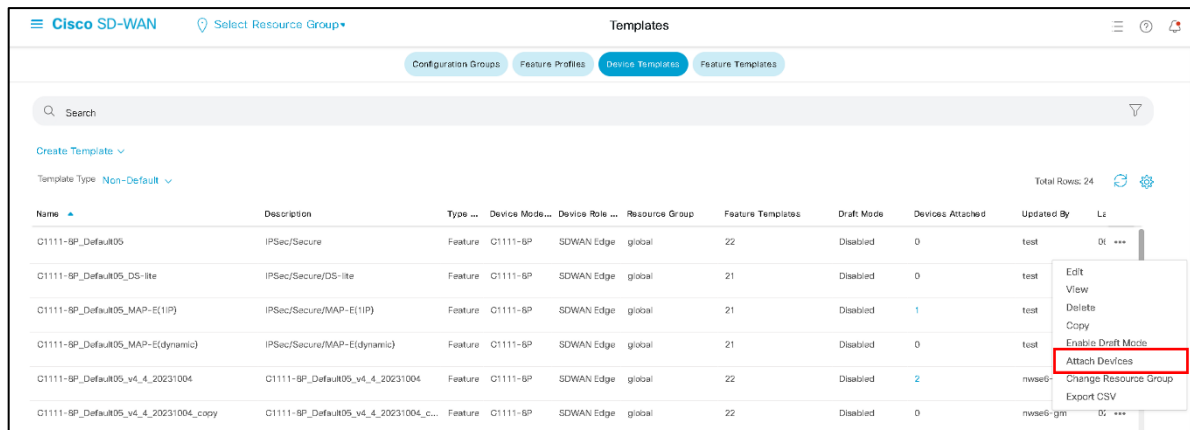
6. ①画面右の「+VPN Interface SVI」を選択
- ②VPN Interface SVI の欄が追加されるので、「VLAN11」を選択
- ③「Save」を選択
- ④「Update」を選択



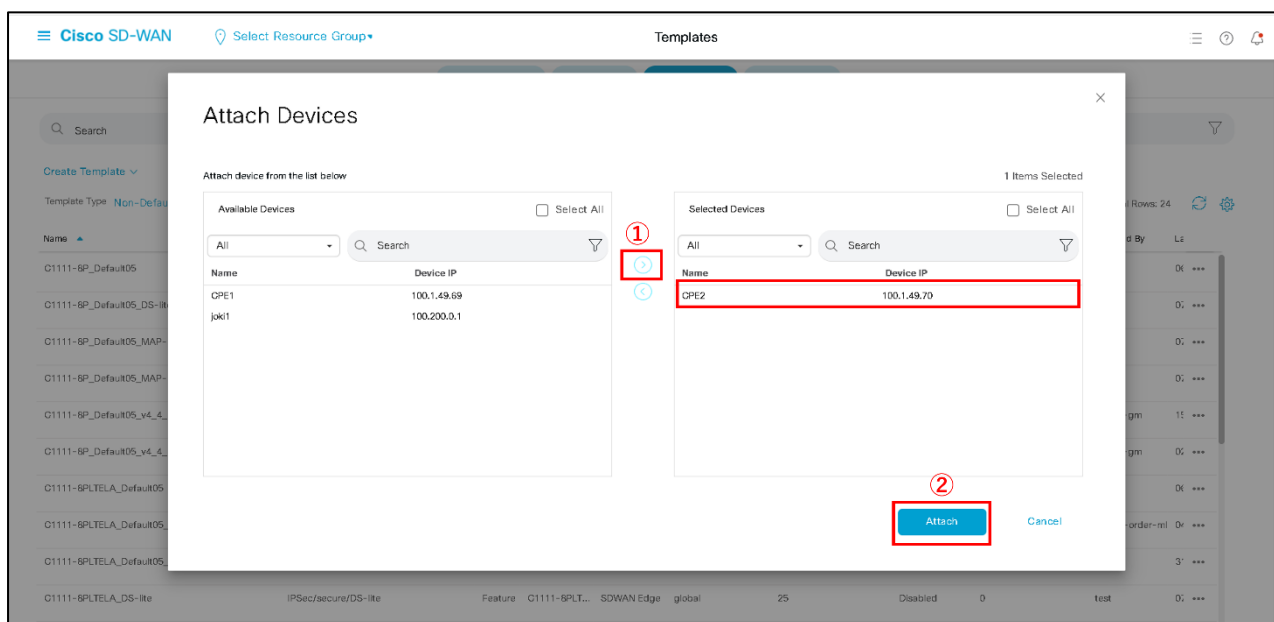
4.10.5. 作成した Device Template を CPE にアタッチ

設定したい CPE へアタッチ

7. 新たに作成した Template の「…」から「Attach devices」を選択



8. ①適用したい CPE を選択し、「→」を選択し右ボックスに移動 ②「Attach」を選択



9. 変更したい CPE の右端にある「…」から「Edit Device Template」を選択

S...	Chassis Number	System IP	Hostname	VLAN ID(gi010_vlan)	VLAN ID(gi011_vlan)	VLAN ID(gi012_vlan)	VLAN ID(gi013_vlan)	VLAN ID(gi014_vlan)	VLAN ID(gi015_vlan)	VLAN ID(gi016_vlan)	VLAN ID(gi017_vlan)	...
✓	C1111-8P-FGL260SLIVE	100.1.49.70	CPE2	10	10	10	10	10	10	10	10	...

10. ①IF に割り当てる VLAN の値を入力(ex. Gi010-013: 10, Gi014-017: 11 を入力)

②追加した vlan の IP アドレスを入力(ex. 192.168.1.254/24)

③「Update」を選択し、「Next」を選択

※Color, Device group, System IP, Site ID はデフォルト値から変更すると通信ができなくなる恐れがあるため、変更しないようお願いいたします

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	C1111-8P-FGL260SLIVE
System IP	100.1.49.70
Hostname	CPE2
VLAN ID(gi010_vlan)	10
VLAN ID(gi011_vlan)	10
VLAN ID(gi012_vlan)	10
VLAN ID(gi013_vlan)	10
VLAN ID(gi014_vlan)	11
VLAN ID(gi015_vlan)	11
VLAN ID(gi016_vlan)	11
VLAN ID(gi017_vlan)	11
dns_primary_ipv6	2001:a7f:5f01::a
dns_secondary_ipv6	2001:a7f:5f01:1::a
vbond_fqdn	vbond15.vsdwan.cast.flets-west.jp
ntp_server1	2001:a7f:0102::a
ntp_server2	2001:a7f:0102::b
IPv4 Address(svi30_ipv4_address)	10.30.1.254/24
Address Pool(dhcp_address_pool_vpn30)	10.30.1.0/24

Generate Password

Update

11. ①以下の画面で CPE を選択し、コンフィグを出力(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を確認願います

The screenshot shows the Cisco SD-WAN configuration interface. On the left, a list of devices is shown, with 'C1111-8P-FGL260SL3VE' selected. The main area displays the 'Local Configuration vs. New Configuration' for the selected device. At the bottom, the 'Configure Devices' button is highlighted with a red box and a red circle.

12. Status が success, Message が Done となっていればコンフィグ適用が完了

※Status が success とならない場合、エラー内容及び手順を確認し時間をおいてリトライの実施をお願いします

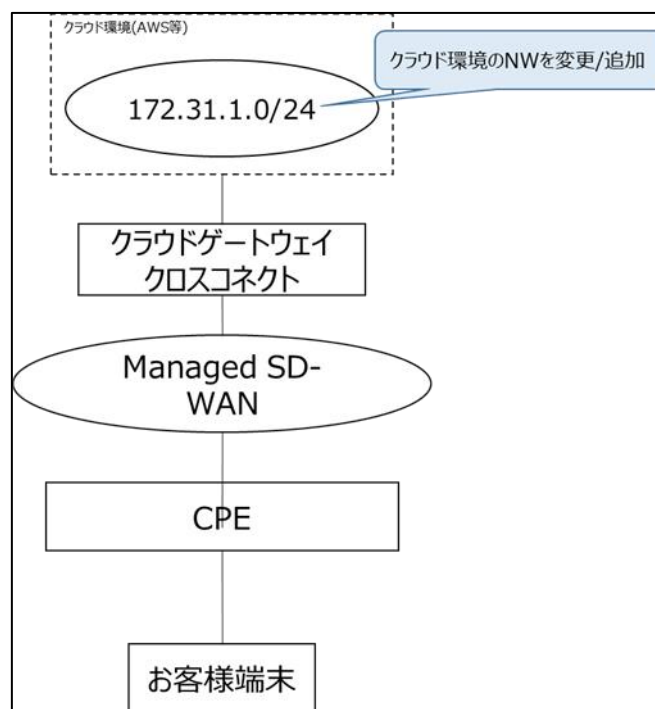
The screenshot shows the Cisco SD-WAN configuration interface. The 'Status' tab is highlighted with a red box and a red circle. The table below shows the status of the configuration push.

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Templates C...	C1111-8P-FGL260SL3VE	C1111-8P	CPE2	100.1.48.70	300006342	215.255.1.2

4.11. パブリッククラウドのネットワークセグメント変更/追加する際の設定手順(クラウドゲートウェイクロスコネクト利用時)

クラウドゲートウェイクロスコネクト利用時にパブリッククラウド(AWS 等)の NW を変更/追加したい場合、次ページ以降の手順を実施します。

4.11.1. NW 構成例



4.11.2. クラウド NW の変更

1. 左ペイン(左の領域)の Configuration から「Policies」を選択
画面右上の「Custom Options」から「Centralized Policy」の「Lists」を選択

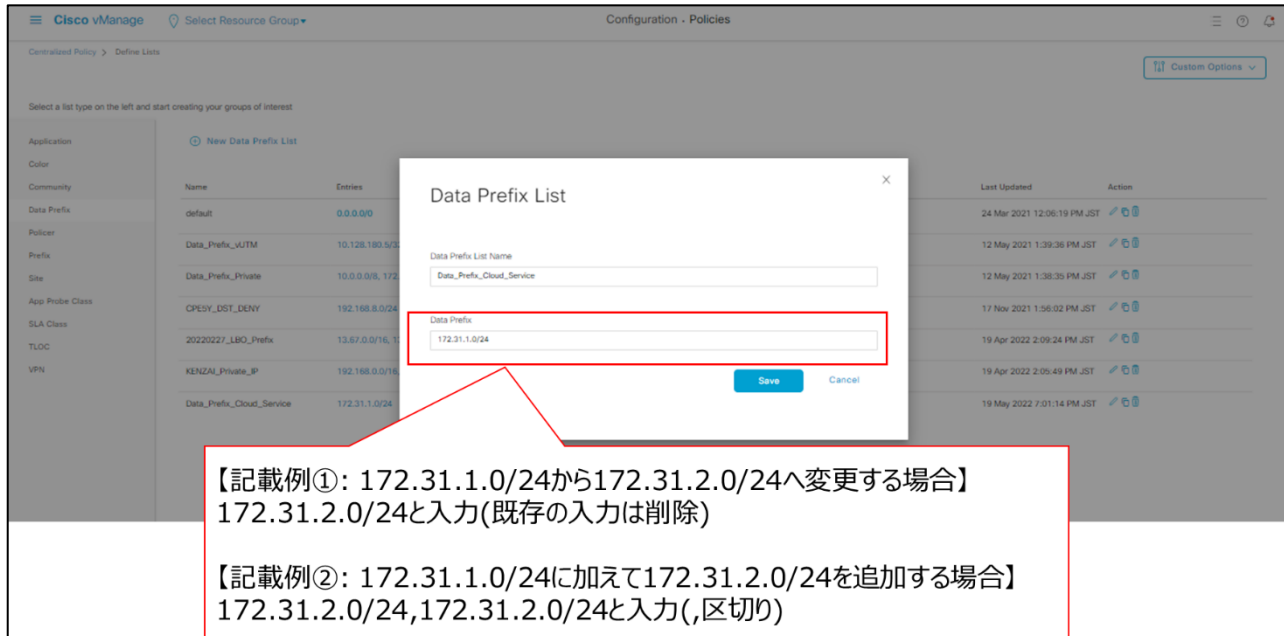
Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	sdwan-order-mi	10052023T171944385	05 Oct 2023 5:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10312023T20053410	31 Oct 2023 8:10:07 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11082023T134058175	08 Nov 2023 1:40:58 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11082023T160750521	08 Nov 2023 4:07:50 PM +09

2. 左ペイン(左の領域)から「Data Prefix」を選択
「Data_Prefix_Cloud_Service」の「ペンマーク」を選択

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
default	0.0.0.0/0	IPv4	0	admin	24 Mar 2021 12:06:19 PM JST	
Data_Prefix_vUTM	10.128.180.5/32	IPv4	1	sdwan-order-mi	12 May 2021 1:39:36 PM JST	
Data_Prefix_Private	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	IPv4	1	sdwan-order-mi	12 May 2021 1:38:35 PM JST	
CPESy_DST_DENY	192.168.8.0/24	IPv4	2	nws66-gm	17 Nov 2021 1:56:02 PM JST	
20220227_LBO_Prefix	13.67.0.0/16, 13.69.0.0/16, 13.76.0.0/16, 13...	IPv4	0	nws66-gm	19 Apr 2022 2:09:24 PM JST	
KENZAI_Private_IP	192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12, 1...	IPv4	1	nws66-gm	19 Apr 2022 2:05:49 PM JST	
Data_Prefix_Cloud_Service	172.31.1.0/24	IPv4	1	sdwan-order-mi	12 May 2022 5:44:03 PM JST	

3. 「Data Prefix」の値を変更します

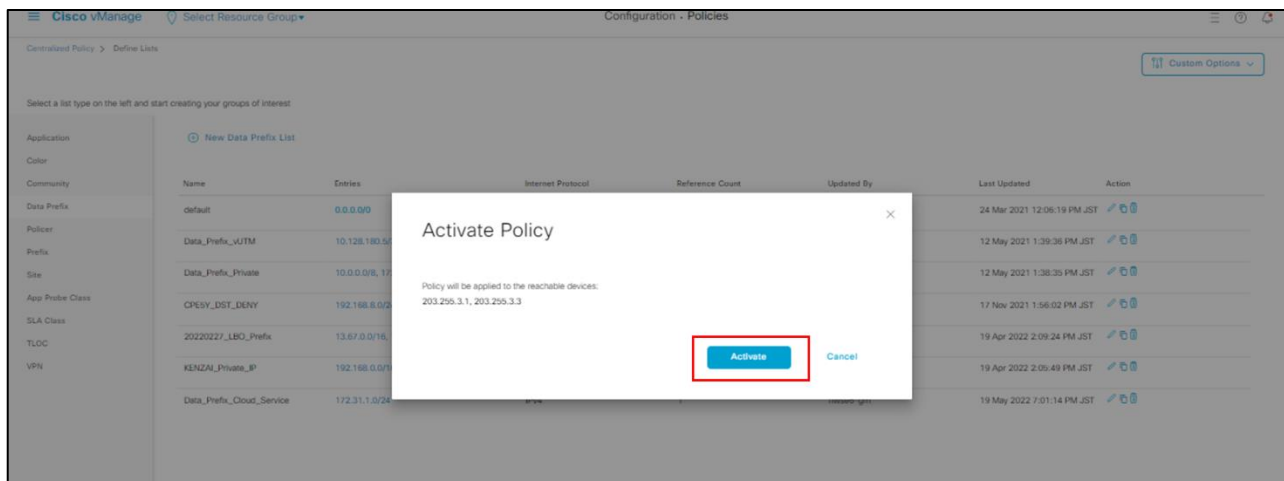
※NWを追加する場合は「,」区切りで複数記載



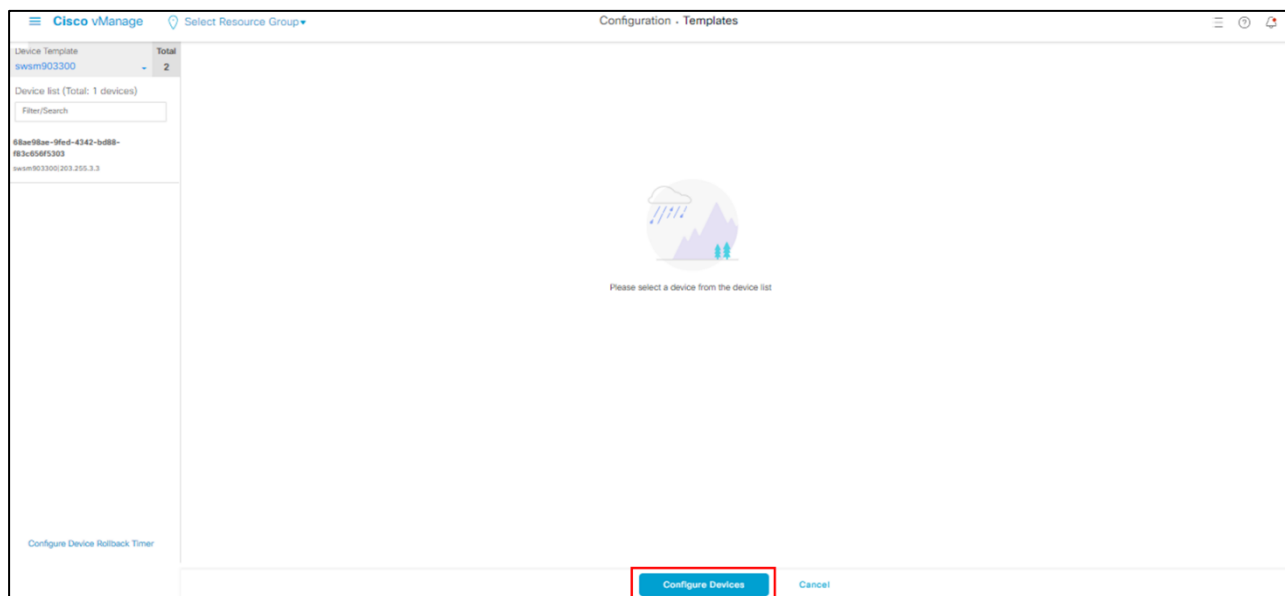
【記載例①: 172.31.1.0/24から172.31.2.0/24へ変更する場合】
172.31.2.0/24と入力(既存の入力は削除)

【記載例②: 172.31.1.0/24に加えて172.31.2.0/24を追加する場合】
172.31.2.0/24,172.31.2.0/24と入力(,区切り)

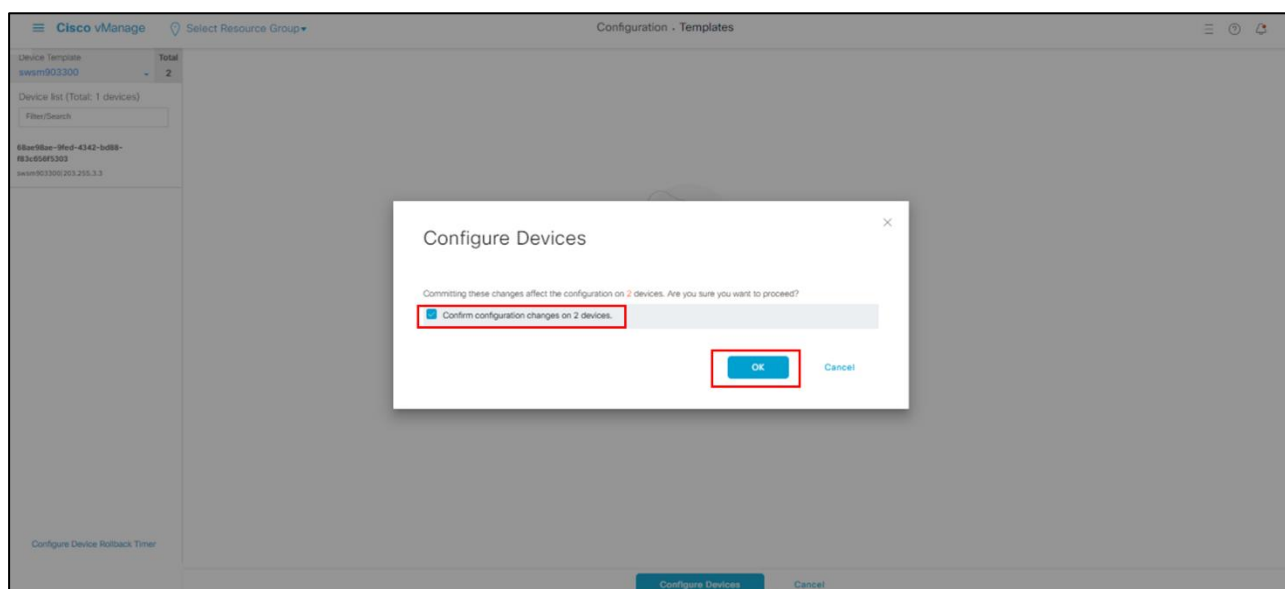
4. 下記画面へ遷移するので「Activate」を選択



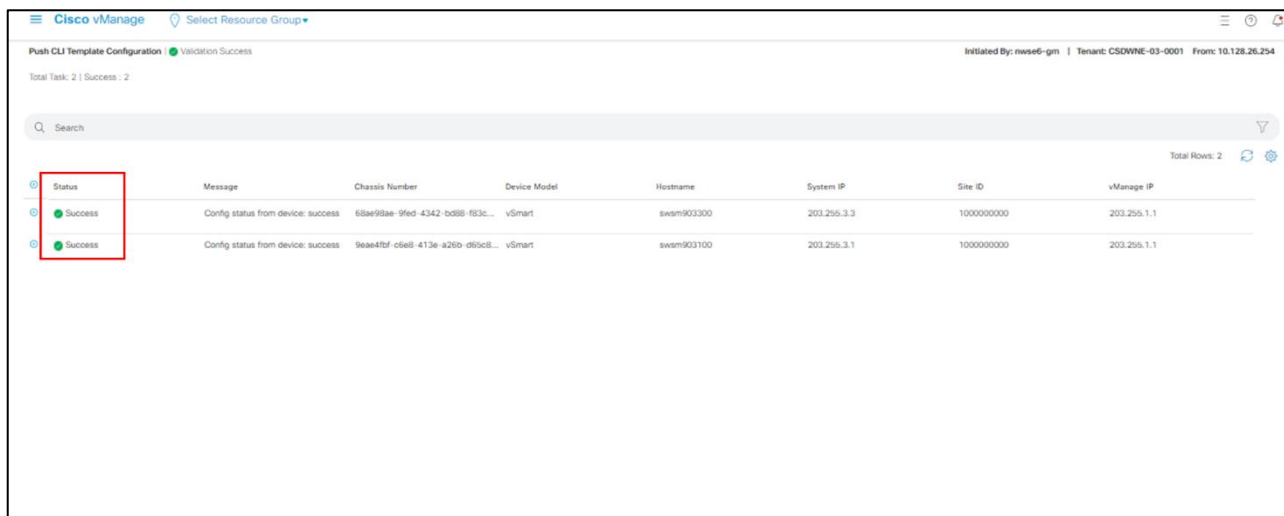
5. 下記画面へ遷移するので「Configure Devices」を選択



6. 下記画面へ遷移するので「Confirm Configuration changes on 2 devices」にチェックを入れ、「OK」を選択



7. Status が「success」になったら完了です



Push CLI Template Configuration Validation Success

Initiated By: nese6-gm | Tenant: CSDWNE-03-0001 | From: 10.128.26.254

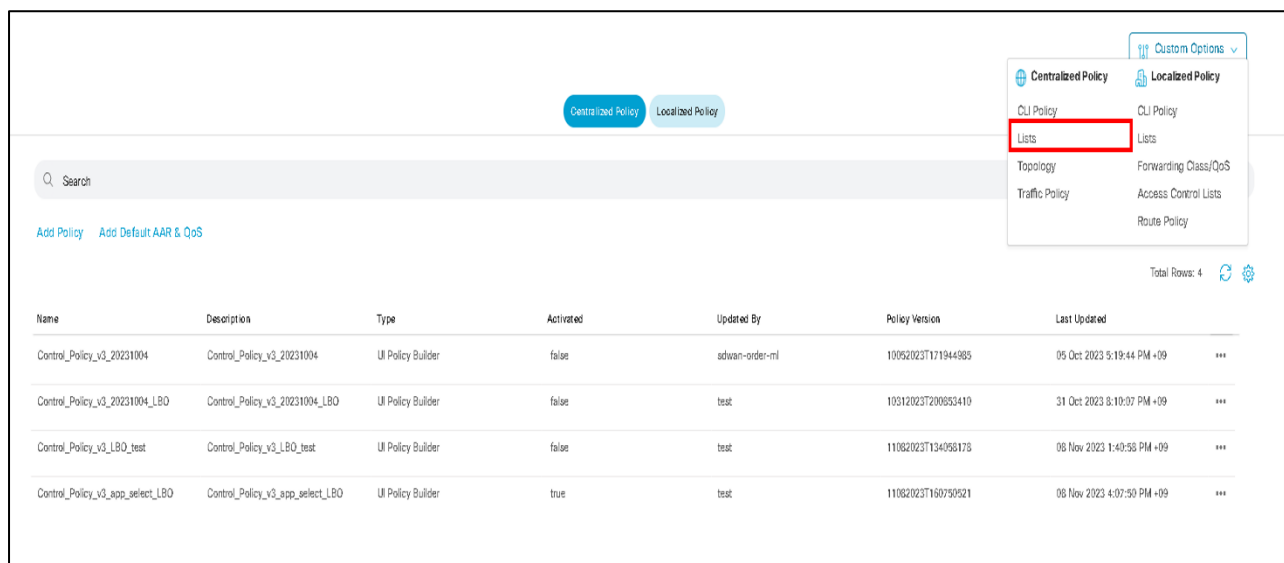
Total Task: 2 | Success: 2

Search

Total Rows: 2

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Config status from device: success	68ae98ae-9fed-4342-bd88-f83c...	vSmart	swm903300	203.256.3.3	1000000000	203.256.1.1
Success	Config status from device: success	9eae47bf-c6e8-413e-a26b-d85c8...	vSmart	swm903100	203.256.3.1	1000000000	203.256.1.1

8. 左ペイン(左の領域)の Configuration から「Policies」を選択 画面右上の「Custom Options」から「Centralized Policy」の「Lists」を選択



Centralized Policy Localized Policy

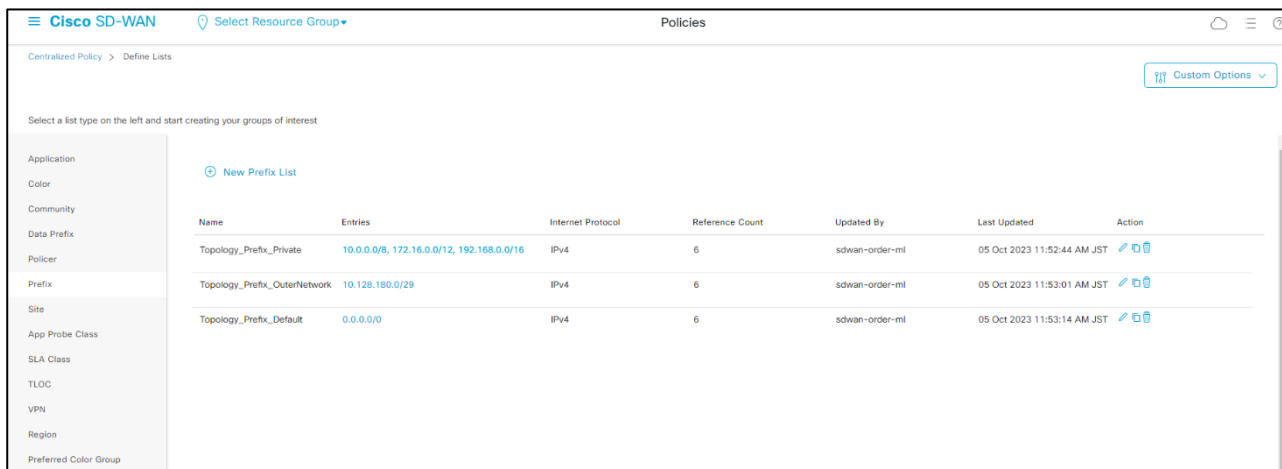
Search

Add Policy Add Default AAR & QoS

Total Rows: 4

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	adwan-order-ml	10052023T171944985	09 Oct 2023 5:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10312023T20053410	31 Oct 2023 8:10:07 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11082023T134056178	08 Nov 2023 1:40:56 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11082023T160750521	08 Nov 2023 4:07:50 PM +09

9. 左ペイン(左の領域)から「Prefix」を選択
「Topology_Prefix_OuterNetwork」の「ペンマーク」を選択



Centralized Policy > Define Lists

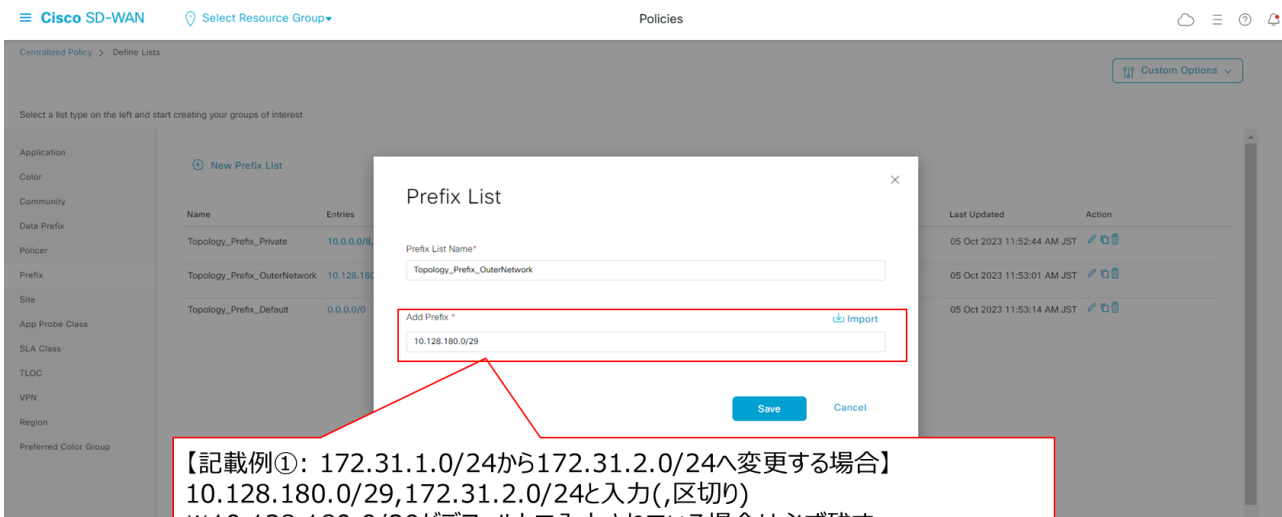
Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN
Region
Preferred Color Group

[New Prefix List](#)

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
Topology_Prefix_Private	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	IPv4	6	sdwan-order-mil	05 Oct 2023 11:52:44 AM JST	Edit Delete
Topology_Prefix_OuterNetwork	10.128.180.0/29	IPv4	6	sdwan-order-mil	05 Oct 2023 11:53:01 AM JST	Edit Delete
Topology_Prefix_Default	0.0.0.0/0	IPv4	6	sdwan-order-mil	05 Oct 2023 11:53:14 AM JST	Edit Delete

10. 「Add Prefix」の値を変更します
※NWを追加する場合は「,」区切りで複数記載



Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN
Region
Preferred Color Group

[New Prefix List](#)

Name	Entries
Topology_Prefix_Private	10.0.0.0/8
Topology_Prefix_OuterNetwork	10.128.180.0/29
Topology_Prefix_Default	0.0.0.0/0

Prefix List

Prefix List Name*

Topology_Prefix_OuterNetwork

Add Prefix *

10.128.180.0/29

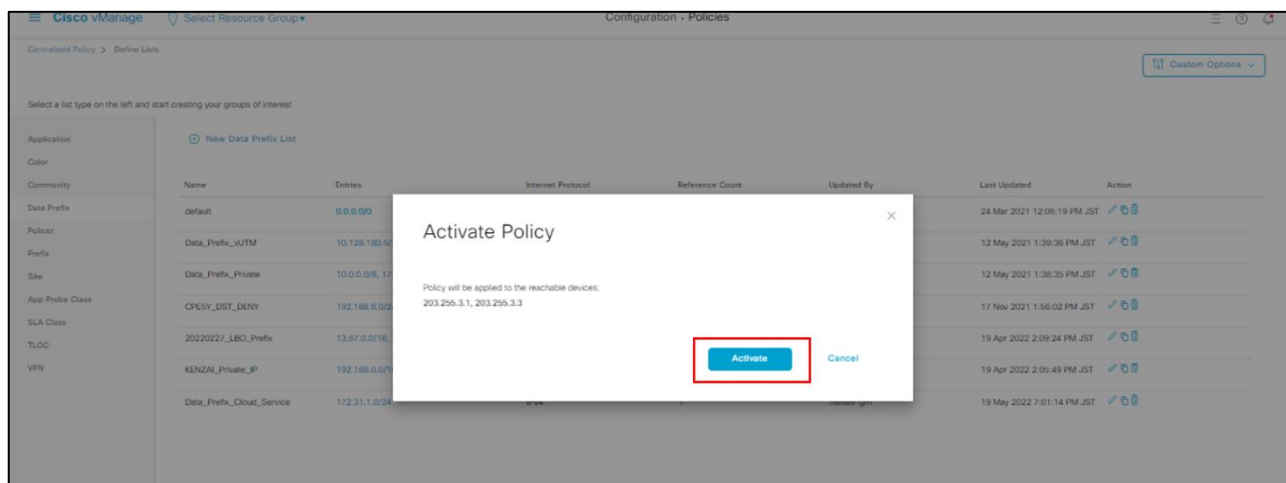
[Import](#)

[Save](#) [Cancel](#)

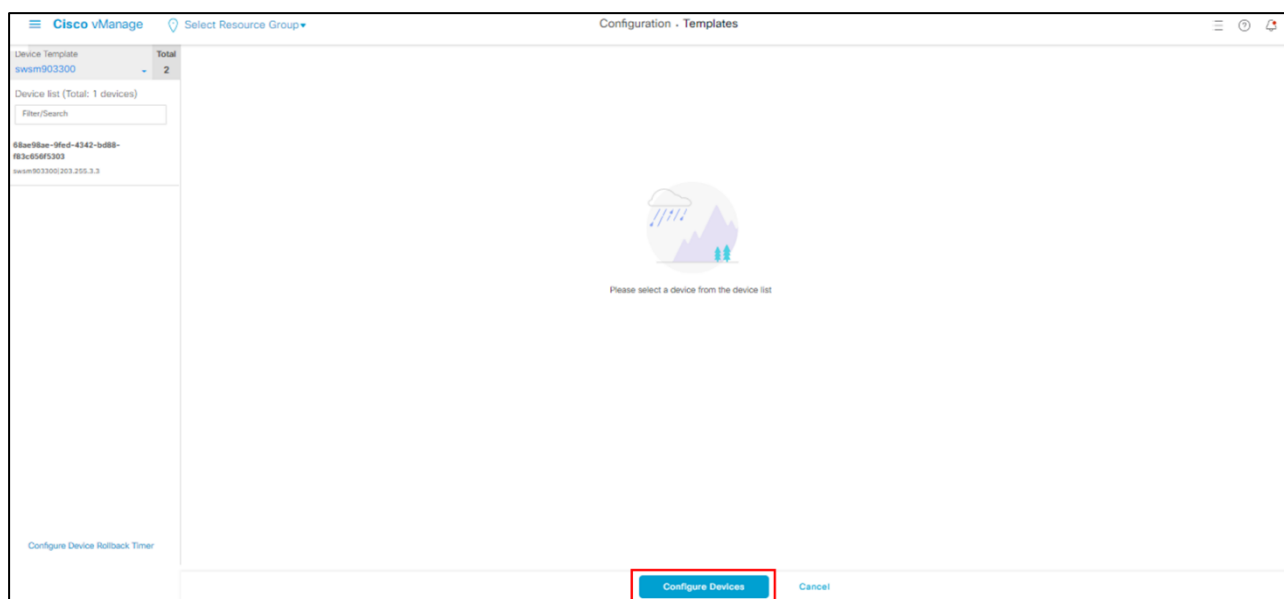
【記載例①: 172.31.1.0/24から172.31.2.0/24へ変更する場合】
10.128.180.0/29, 172.31.2.0/24と入力(区切り)
※10.128.180.0/29がデフォルトで入力されている場合は必ず残す
※172.31.1.0/24を172.31.2.0/24へ変更

【記載例②: 172.31.1.0/24に加えて172.31.2.0/24を追加する場合】
10.128.180.0/29, 172.31.1.0/24, 172.31.2.0/24と入力(区切り)
※10.128.180.0/29がデフォルトで入力されている場合は必ず残す

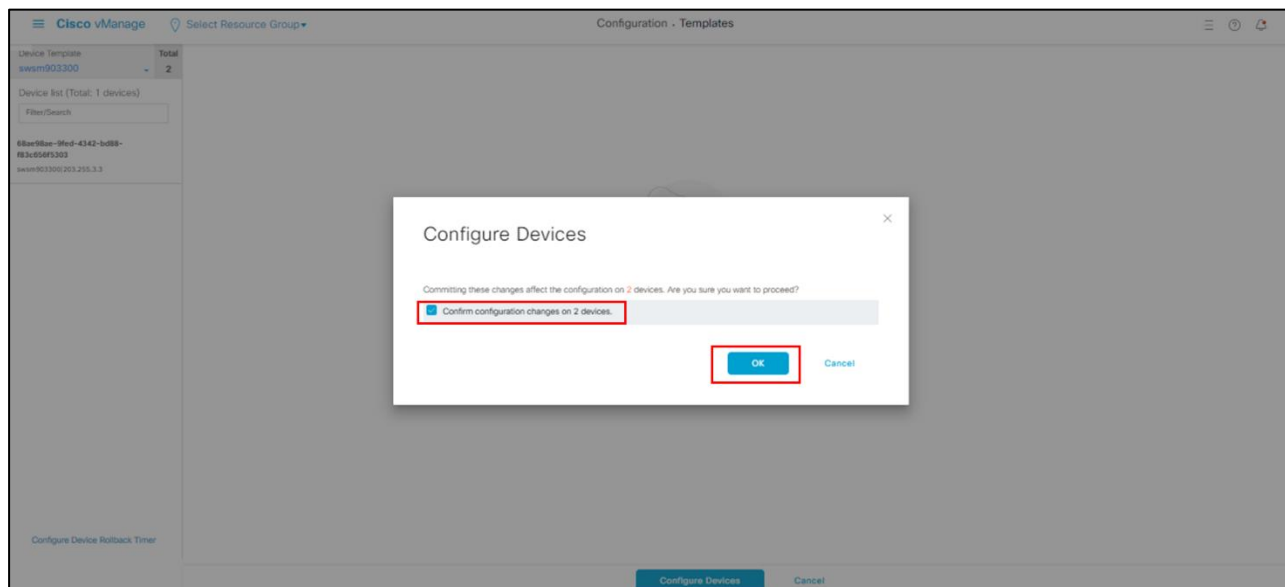
11. 下記画面へ遷移するので「Activate」を選択



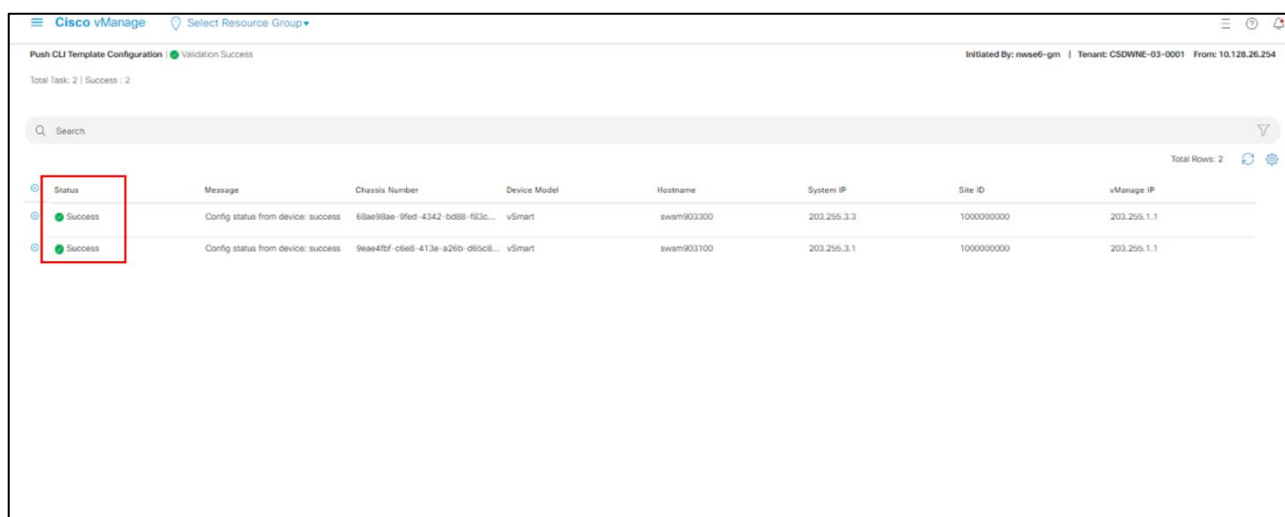
12. 下記画面へ遷移するので「Configure Devices」を選択



13. 下記画面へ遷移するので「Confirm Configuration changes on 2 devices」にチェックを入れ、「OK」を選択



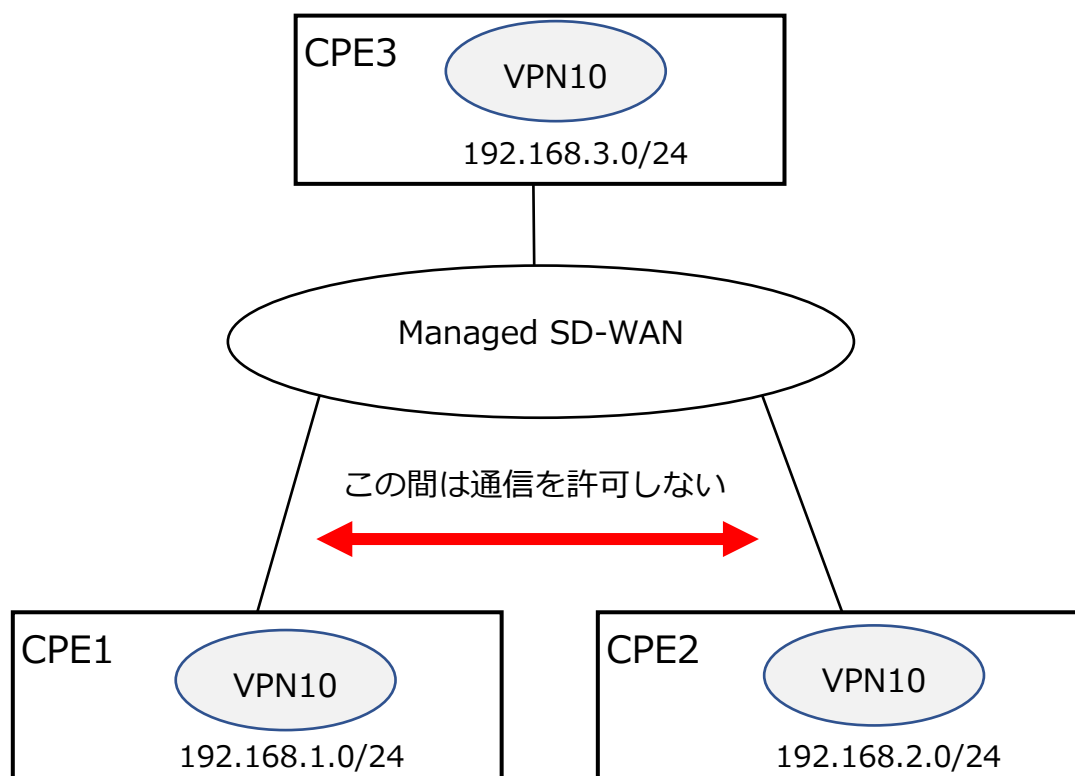
14. Status が「success」になったら完了です



4.12. アクセスリスト（ACL）追加手順

4.12.1. NW 構成例

CPE1、2 は CPE3 と通信させ、CPE1 と CPE2 の通信は不可とする



【Device Template 作成に必要な Localized Policy 作成】

作成する Localized Policy	手順	用途
ACL_yyyymmdd	1～5	アクセスリスト

【Device Template のコピー】

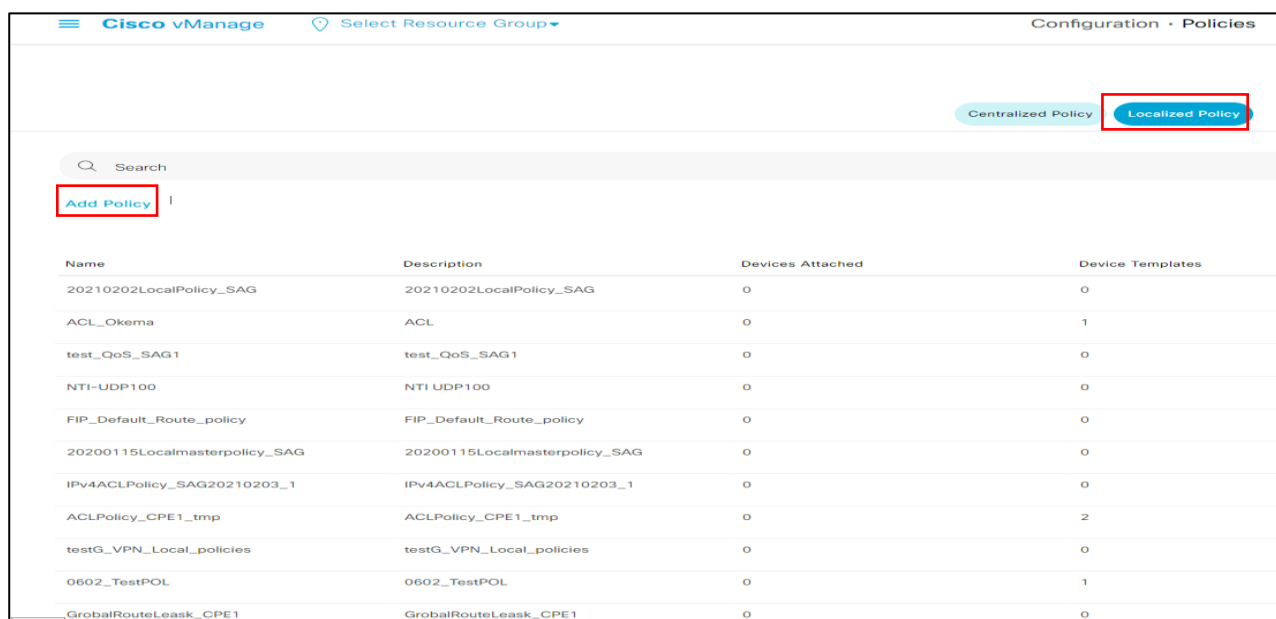
-	手順	用途
-	6	Device テンプレートのバックアップ

【Sub-template のコピー】

-	手順	用途
-	8	Device テンプレートのバックアップ

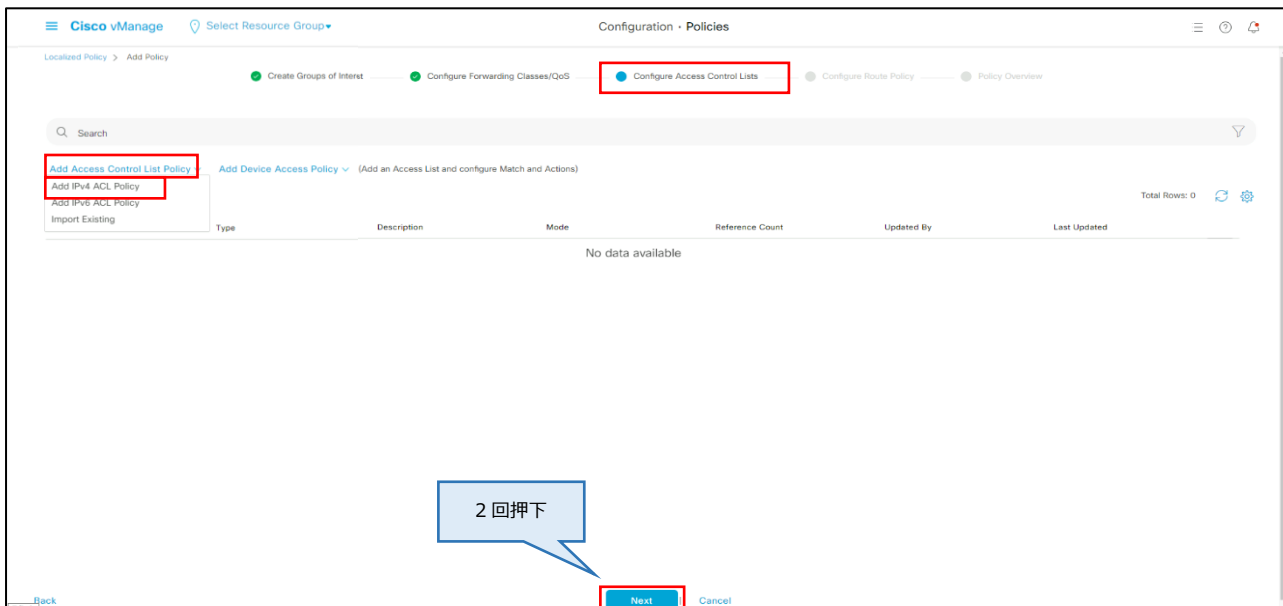
4.12.2. アクセスリストの作成（Localized Policy 作成）

1. 左ペイン(左の領域)の Configuration から「Policies」を選択
画面上部のタブから「Localized Policy」を選択後に「Add Policy」を選択

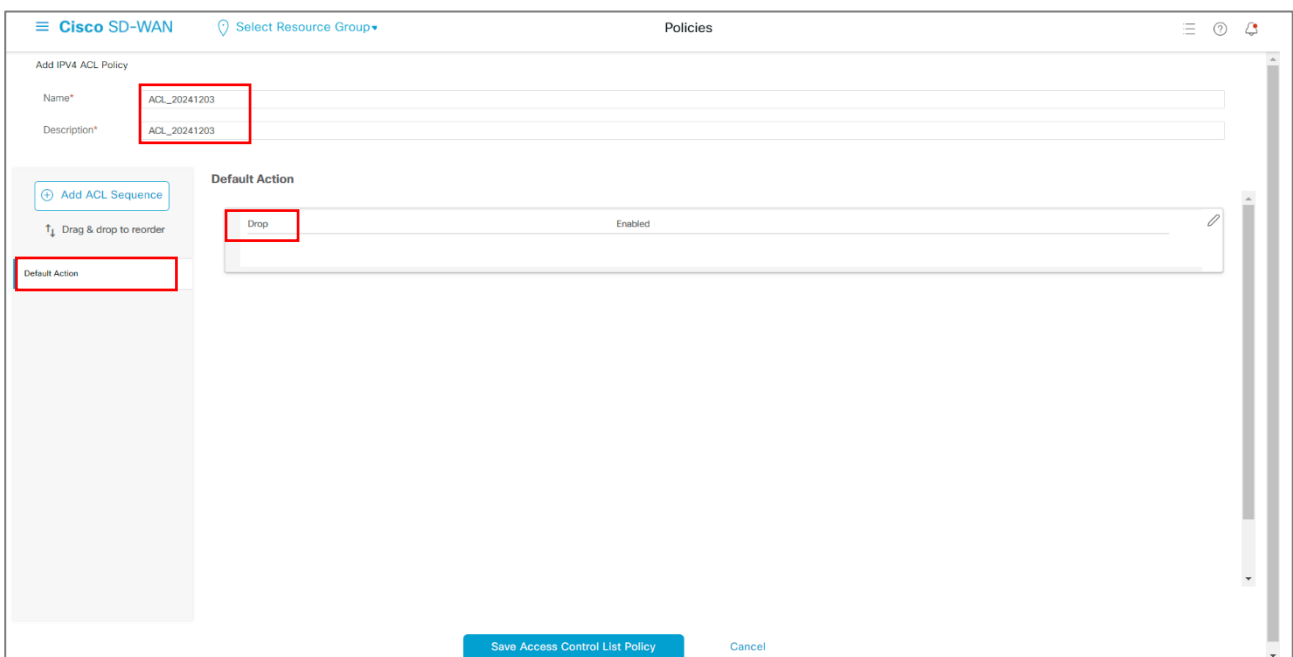


Name	Description	Devices Attached	Device Templates
20210202LocalPolicy_SAG	20210202LocalPolicy_SAG	0	0
ACL_Okema	ACL	0	1
test_QoS_SAG1	test_QoS_SAG1	0	0
NTI-UDP100	NTI UDP100	0	0
FIP_Default_Route_policy	FIP_Default_Route_policy	0	0
20200115Localmasterpolicy_SAG	20200115Localmasterpolicy_SAG	0	0
IPv4ACLPolicy_SAG20210203_1	IPv4ACLPolicy_SAG20210203_1	0	0
ACLPolicy_CPE1_tmp	ACLPolicy_CPE1_tmp	0	2
testG_VPN_Local_policies	testG_VPN_Local_policies	0	0
0602_TestPOL	0602_TestPOL	0	1
GrobalRouteLeask_CPE1	GrobalRouteLeask_CPE1	0	0

2. 上部の進捗状況が「Configure Access Control Lists」になるまで画面下部「Next」を押下(2回)、「Add Access Control List Policy」から「Add IPv4 ACL Policy」を選択

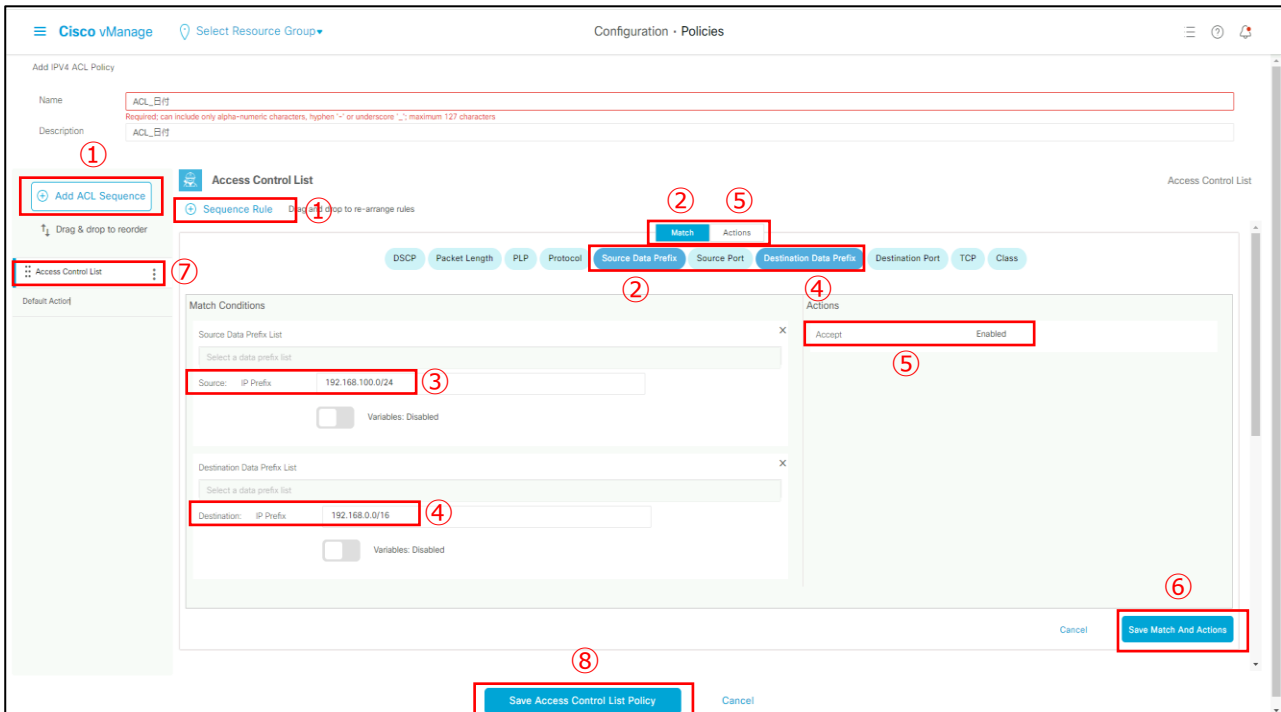


3. ACL Policy の name/description に「ACL_yyyymmdd」を入力
※yyyymmdd は作業日
Default Action が「Drop」になっている事を確認。



4. ※以下は必要な ACL に応じて繰り返す

- ①「Add ACL Sequence」を押して「Sequence Rule」を選択
- ②マッチ条件を設定(中央「Match」タブから設定するボタンを選択し、「Match Conditions」を編集する)
- ③送信元を設定:「Source Data Prefix」を選んで、「IP Prefix」にアドレス入力
※NW 例から 192.168.1.0/24
- ④宛先を設定:「Destination Data Prefix」を選んで、「IP Prefix」にアドレス入力
※NW 例から 192.168.3.0/24
- ⑤中央「Action」タブを選択し、「Actions」を編集して、「Accept」を選択
- ⑥右下から「Save match and actions」で保存
- ⑦追加した Sequence Rule が複数の場合は…から Rename を選択して名前を変更
※Access Control List1、Access Control List2、Access Control List3 など
- ⑧「Save Access Control Policy」を押下して保存



The screenshot displays the Cisco vManage interface for configuring an IPv4 ACL Policy. The page is titled "Configuration - Policies" and "Add IPv4 ACL Policy".

- 1**: The "Add ACL Sequence" button is highlighted in the left sidebar.
- 2**: The "Sequence Rule" button is highlighted in the "Access Control List" section.
- 3**: The "Source" field under "Source Data Prefix List" is highlighted, showing the value "192.168.100.0/24".
- 4**: The "Destination" field under "Destination Data Prefix List" is highlighted, showing the value "192.168.0.0/16".
- 5**: The "Match" tab is selected, and the "Accept" action is chosen under the "Actions" section.
- 6**: The "Save Match And Actions" button is highlighted at the bottom right.
- 7**: The "Access Control List" dropdown menu is highlighted on the left.
- 8**: The "Save Access Control List Policy" button is highlighted at the bottom center.

5. ①ACL を入れて保存したら Next を 2 回さらに押下
下記の図の様に Policy の名前等を入れる画面になるので、
②name/description に「Policy_ACL_yyyymmdd」入力
③「Save Policy」を押下
※Localized Policy 一覧の画面に作成した ACL の Policy が追加されます

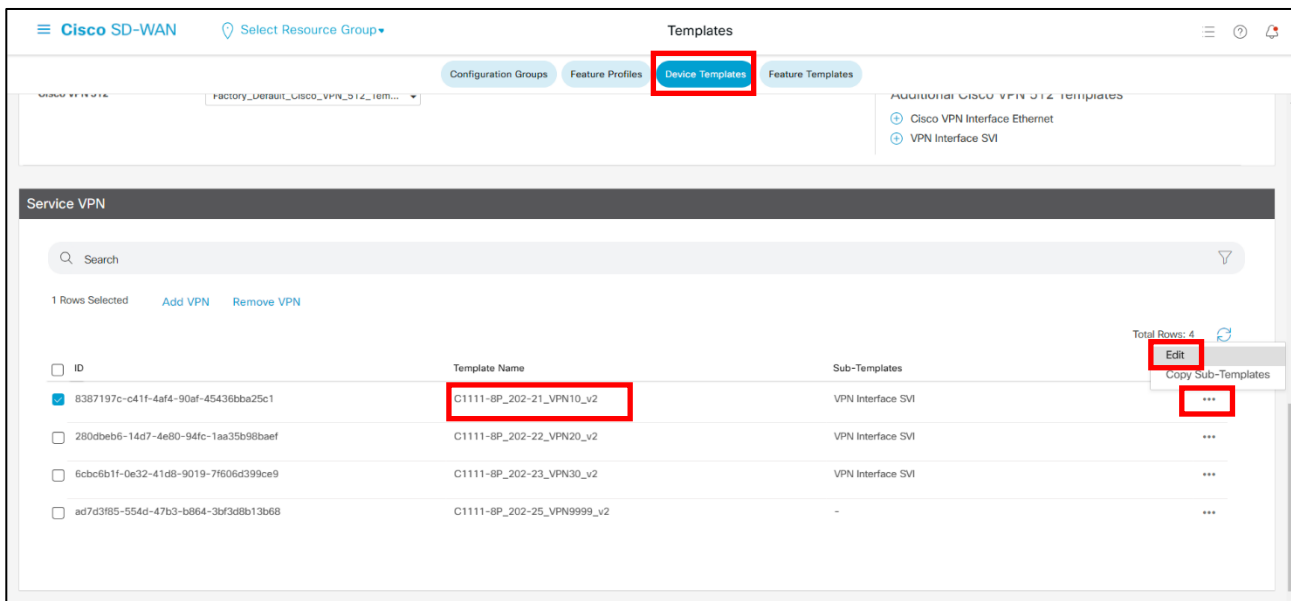
4.12.3. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

6. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Devices」を選択
NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Control_Policy_v3_20231004	Control_Policy_v3_20231004	UI Policy Builder	false	advan-order-mi	10052023T171944985	05 Oct 2023 5:19:44 PM +09
Control_Policy_v3_20231004_LBO	Control_Policy_v3_20231004_LBO	UI Policy Builder	false	test	10052023T200653410	31 Oct 2023 9:10:07 PM +09
Control_Policy_v3_LBO_test	Control_Policy_v3_LBO_test	UI Policy Builder	false	test	11062023T134055176	06 Nov 2023 1:40:55 PM +09
Control_Policy_v3_app_select_LBO	Control_Policy_v3_app_select_LBO	UI Policy Builder	true	test	11062023T160759521	06 Nov 2023 4:07:50 PM +09

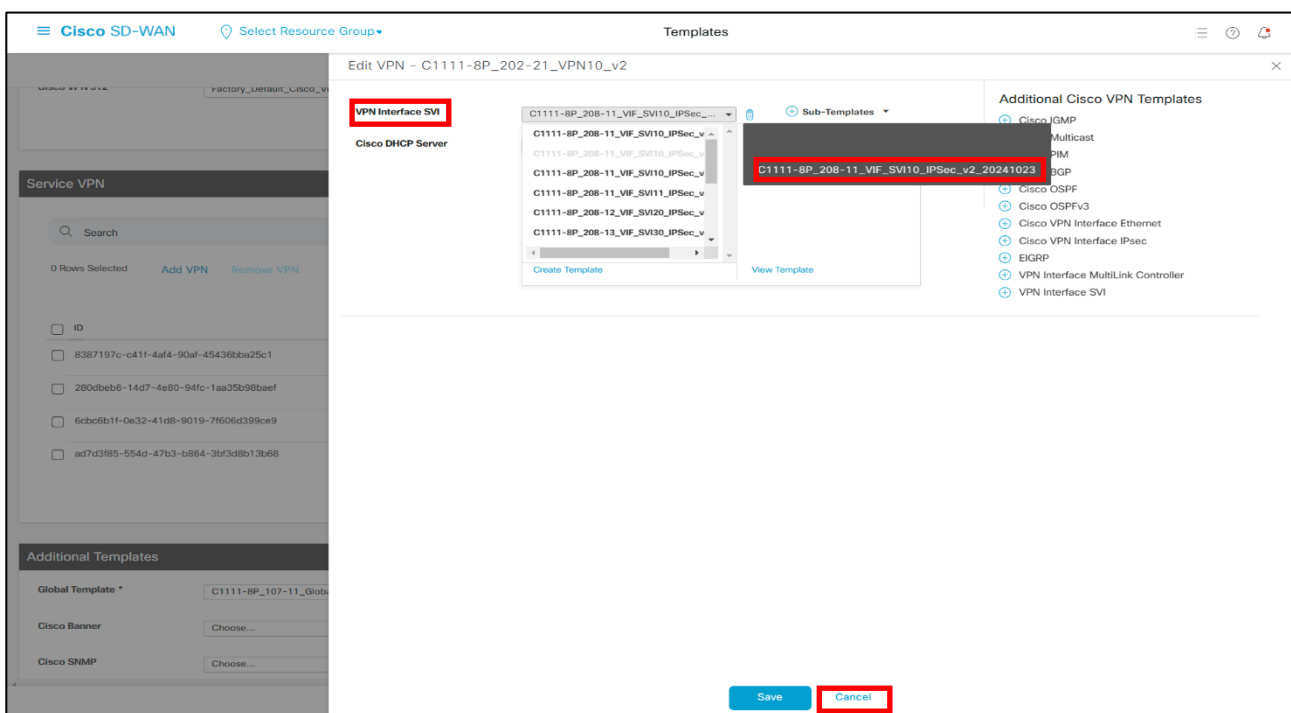
4.12.4. SVI Template(Sub-Template)の確認

- 「Service VPN」→VPN10 の「…」から Edit→「VPN Interface SVI」の Feature Template 名を確認してメモする。そのあと「Cancel」を 2 回押下
※今回は VPN10 を使用



The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' section. The 'Device Templates' tab is active. A table lists VPN templates. The first row is selected, and the 'Edit' button is highlighted.

ID	Template Name	Sub-Templates
8387197c-c41f-4af4-90af-45436ba25c1	C1111-8P_202-21_VPN10_v2	VPN Interface SVI
280dbeb6-14d7-4e80-94fc-1aa35b98baef	C1111-8P_202-22_VPN20_v2	VPN Interface SVI
6c6cb6b1f-0e32-41d8-9019-7f606d399ce9	C1111-8P_202-23_VPN30_v2	VPN Interface SVI
ad7d3f85-554d-47b3-b864-3bf3d8b13b68	C1111-8P_202-25_VPN9999_v2	-



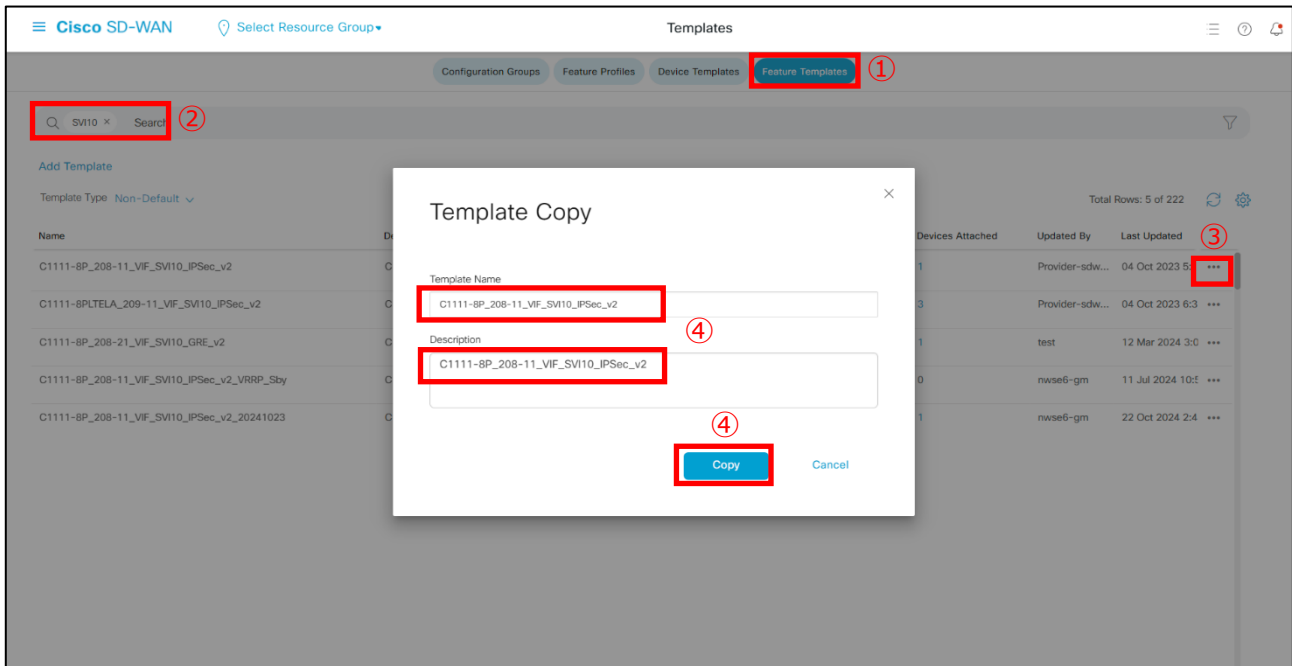
The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' section. The 'Edit VPN' dialog is open, showing the 'VPN Interface SVI' template. The 'Cancel' button is highlighted.

Additional Cisco VPN Templates:

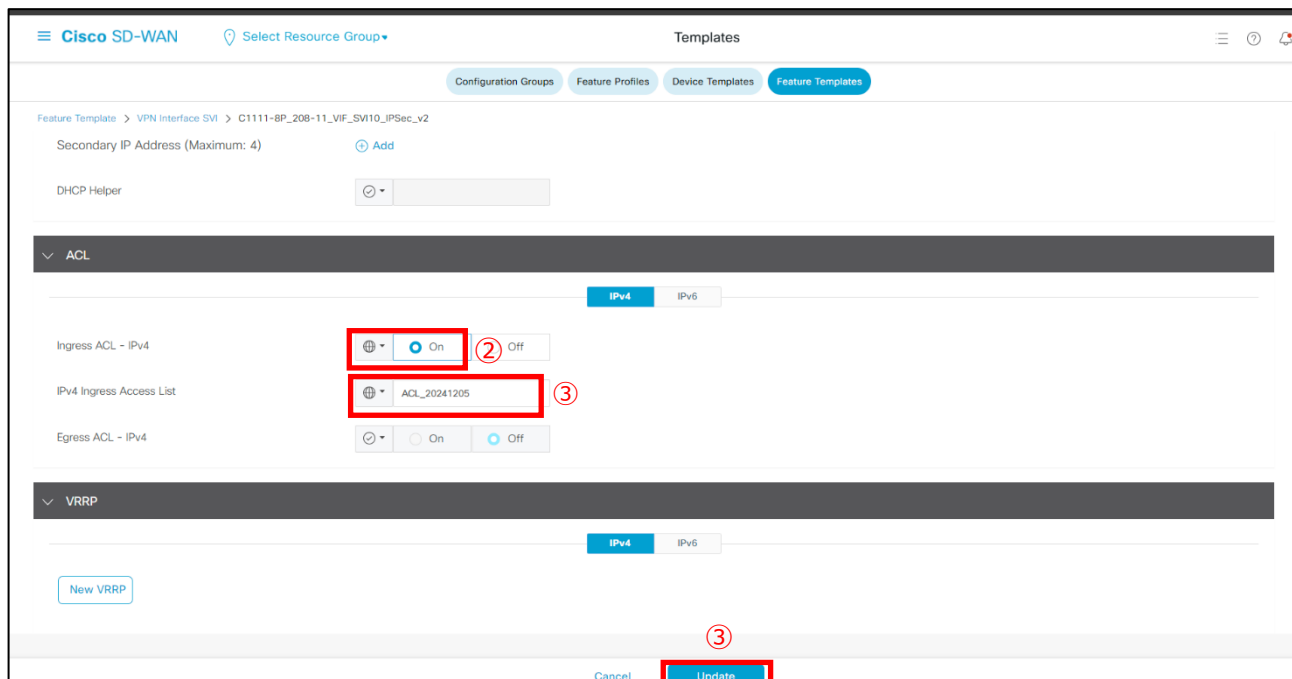
- Cisco IGMP
- Multicast
- PIM
- BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco VPN Interface Ethernet
- Cisco VPN Interface IPsec
- EIGRP
- VPN Interface MultiLink Controller
- VPN Interface SVI

4.12.5. SVI Template(Sub-Template)のコピーと編集

8. ①「Configuration」→「Template」→画面上部のタブを「Feature Template」を選択
- ② 手順7でメモした「VPN Interface SVI」名を検索する
- ③「…」からCopyを選択
- ④name/descriptionに「既存名前+_yyyymmdd」を記載し、Copyを押下

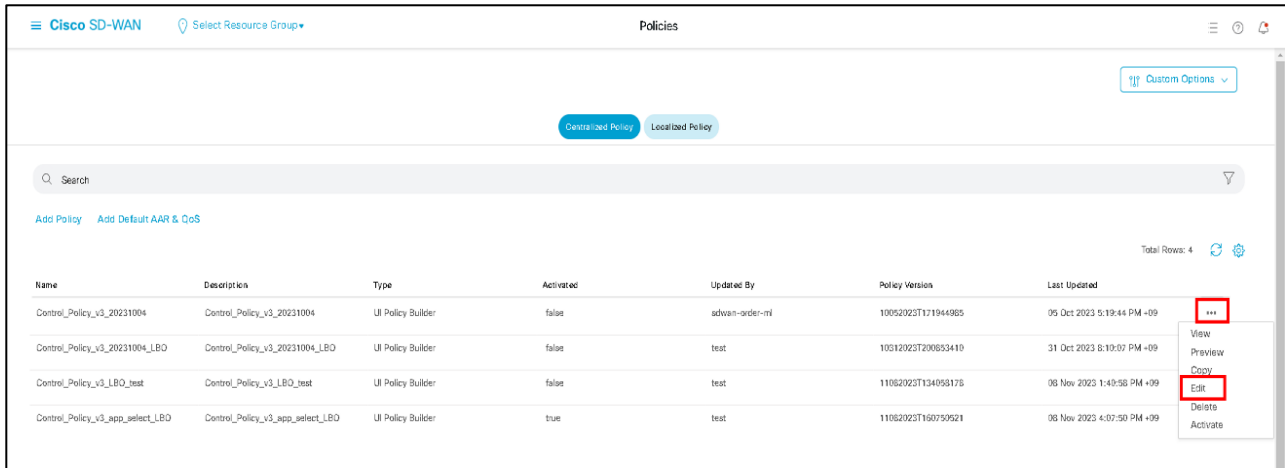


9. ①コピーした「VPN Interface SVI」の「…」から「Edit」を選択
- ②「ACL」タブに移動し「Ingress ACL - IPv4」を「Global」で「On」を選択
- ③「IPv4 Ingress Access List」を「Global」を選択したら
手順3で作成した「ACL_yyyymmdd」の名前を記入し、「Update」を押下



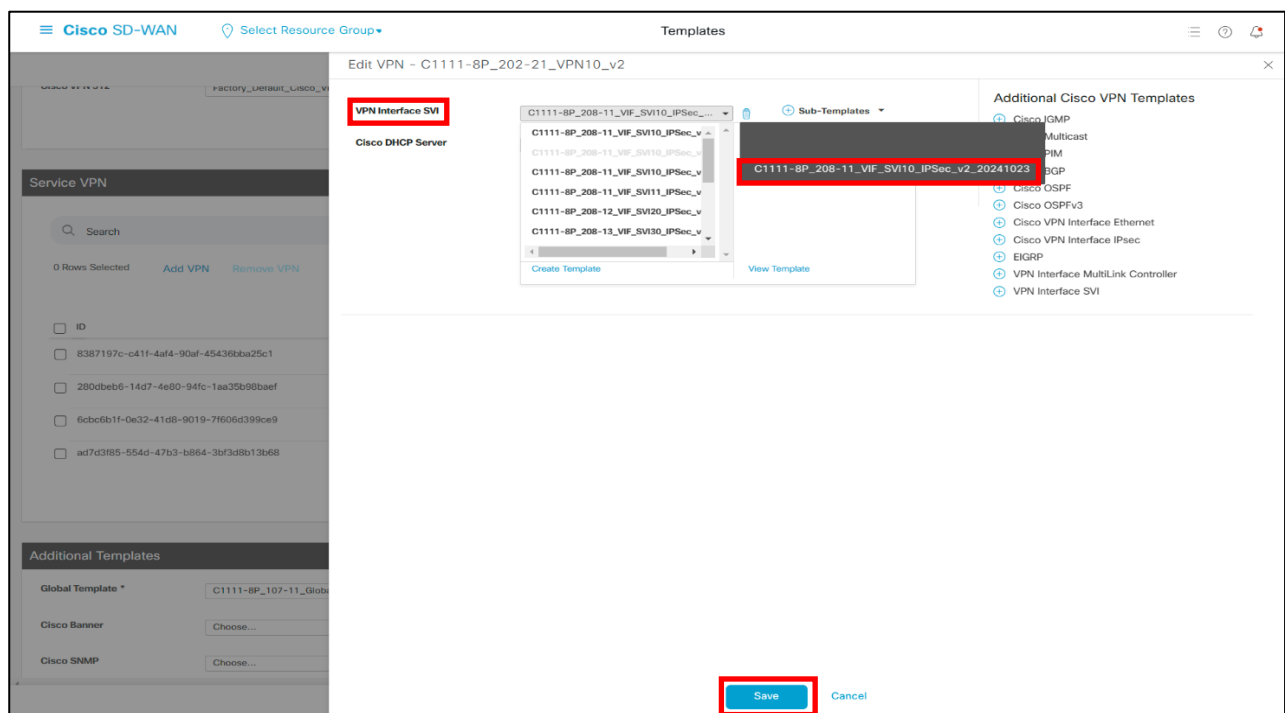
4.12.6. Device Template を編集

10. 手順 6 でコピーした Device Template の「…」から「Edit」を選択



4.12.7. SVI Template (Sub-template) の適用

11. 「Service VPN」→VPN10 の「…」から Edit→「VPN Interface SVI」の Feature Template を手順 8 で作成した SVI Template に変更して「Save」を押下



4.12.8. アクセスリストの適用

- 「Additional Template」→「Policy」のプルダウンから手順 5 で作成したポリシーを選択して「Update」を押下

The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' tab selected. Under 'Additional Templates', the 'Policy' dropdown menu is open, displaying a list of policies. The policy 'Policy_ACL_20241212_CPE1' is highlighted. The 'Update' button at the bottom is also highlighted.

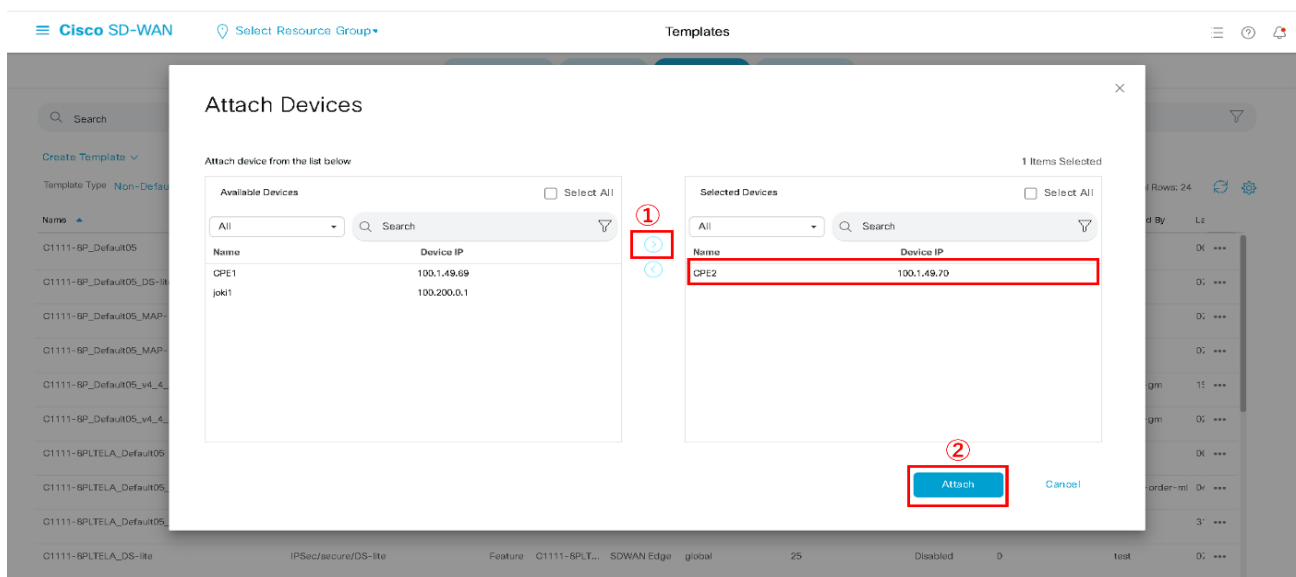
4.12.9. 作成した Device Template を CPE にアタッチ

- 新たに作成したテンプレートの「…」から「Attach Devices」を選択

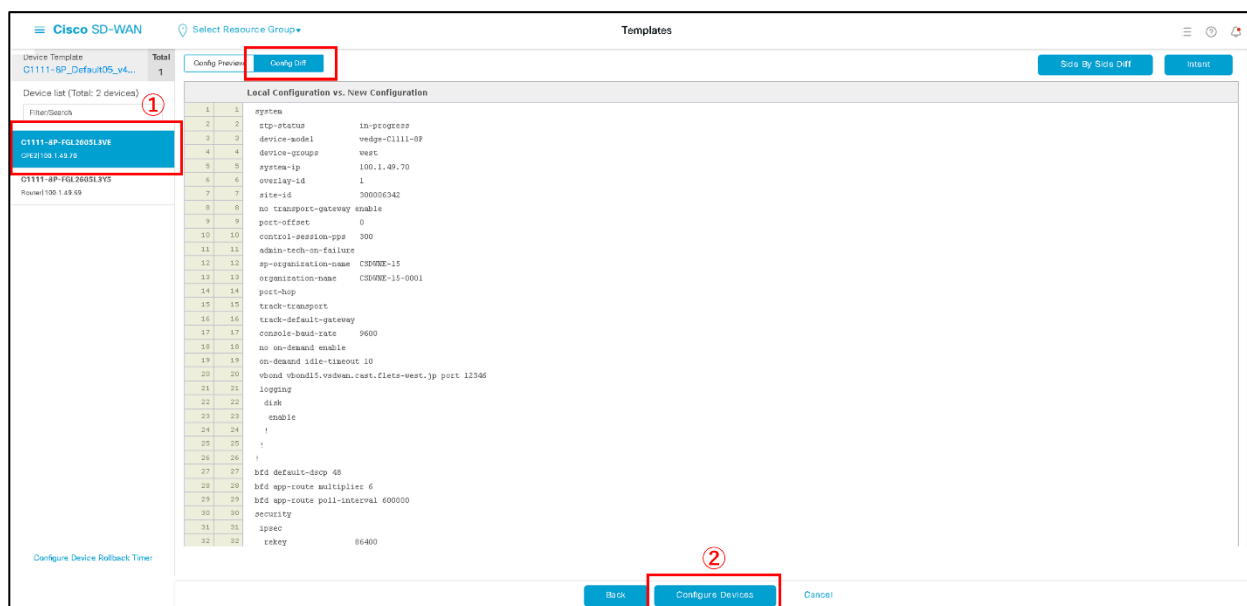
The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' tab selected. A table lists various templates. The 'C1111-8P_Default05_v4_4_20231004' template is selected, and a context menu is open, showing the 'Attach Devices' option highlighted.

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	...
C1111-8P_Default05	IPSec/Secure	Feature	C1111-8P	SD-WAN Edge	global	22	Disabled	0	test	OK
C1111-8P_Default05_D35-88a	IPSec/Secure/D35-88a	Feature	C1111-8P	SD-WAN Edge	global	21	Disabled	0	test	Edit, View, Delete, Copy, Enable Draft Mode, Attach Devices, Change Resource Group, Export CSV
C1111-8P_Default05_MAP-E(1P)	IPSec/Secure/MAP-E(1P)	Feature	C1111-8P	SD-WAN Edge	global	21	Disabled	1	test	
C1111-8P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-8P	SD-WAN Edge	global	21	Disabled	0	test	
C1111-8P_Default05_v4_4_20231004	C1111-8P_Default05_v4_4_20231004	Feature	C1111-8P	SD-WAN Edge	global	22	Disabled	2	nwaso	
C1111-8P_Default05_v4_4_20231004_copy	C1111-8P_Default05_v4_4_20231004	Feature	C1111-8P	SD-WAN Edge	global	22	Disabled	0	nwaso@gn	OK

14. ①適用したい CPE を選択し、「→」を選択し右ボックスに移動
- ②「Attach」を選択



15. ①以下の画面で CPE を選択し、コンフィグを出力
(Config Diff を選択すると差分表示が可能)
 - ②内容を確認し、「Configure Devices」を選択
- ※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を確認願います



16. Status が success, Message が Done となっていればコンフィグ適用が完了
 ※Status が success とならない場合、エラー内容及び手順を確認し時間を置いてリトライの実施をお願いします

Cisco SD-WAN

Select Resource Group

Push Feature Template Configuration

Validation Success

Initiated By: nase6-gm

Tenant: CSDWNE-15-0001

From: 172.18.128.190

Total Task: 1 | Success : 1

Search

Total Rows: 1

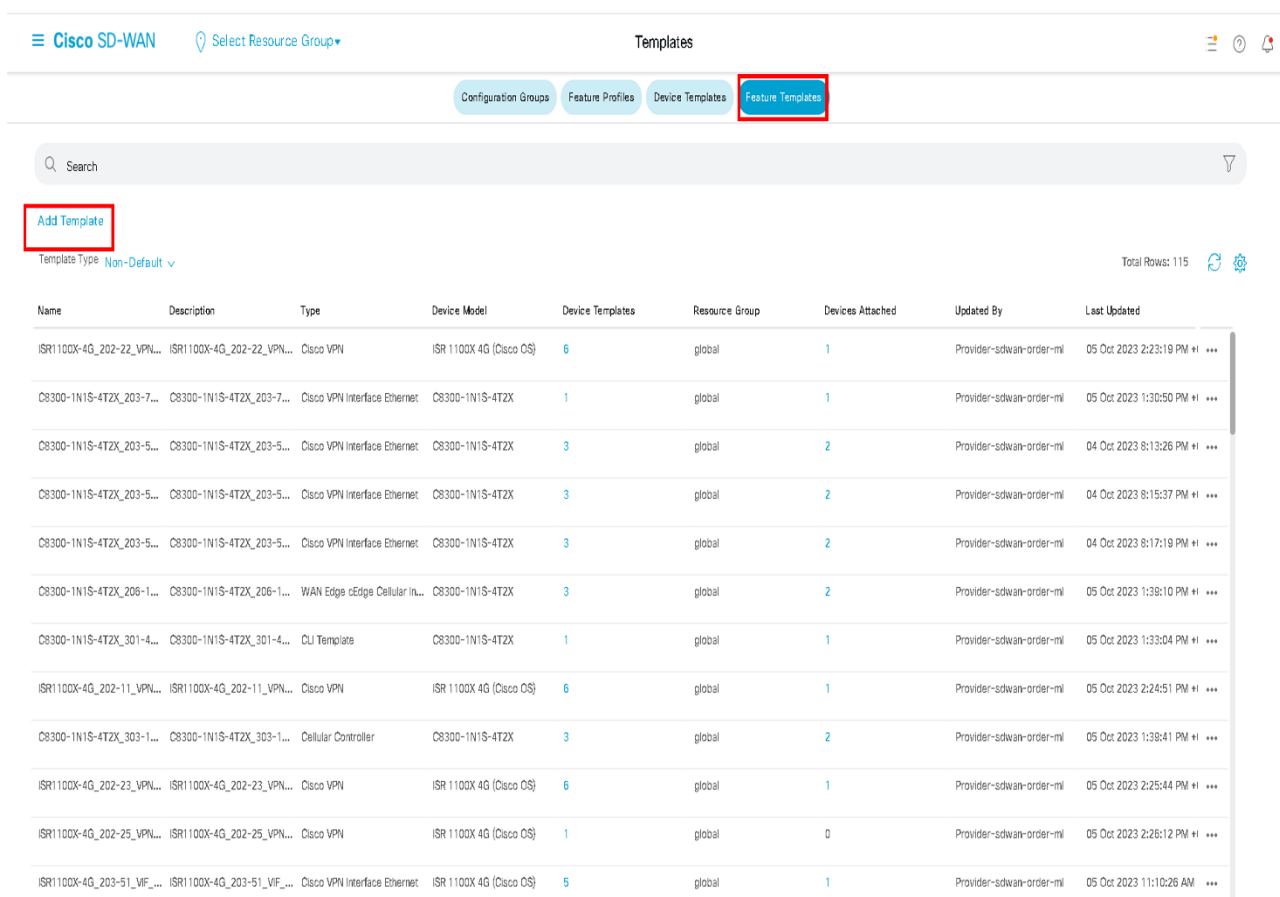
>	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
>	Success	Done - Push Feature Template C...	C1111-8P-FGL2605L3VE	C1111-8P	CPE2	100.149.70	300006342	215.255.1.2

4.13. タイプ I、タイプ II で NAT セッション数を 10 万に変更する際の設定手順

タイプ I、タイプ II は開通時の NAT セッション数が 16,000 となっています。10 万セッションまで拡大が必要な場合、次ページ以降の手順を実施します。

4.13.1. セッション変更用の Feature テンプレートの作成

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択
「Add Template」を選択



Search

Add Template

Template Type: Non-Default

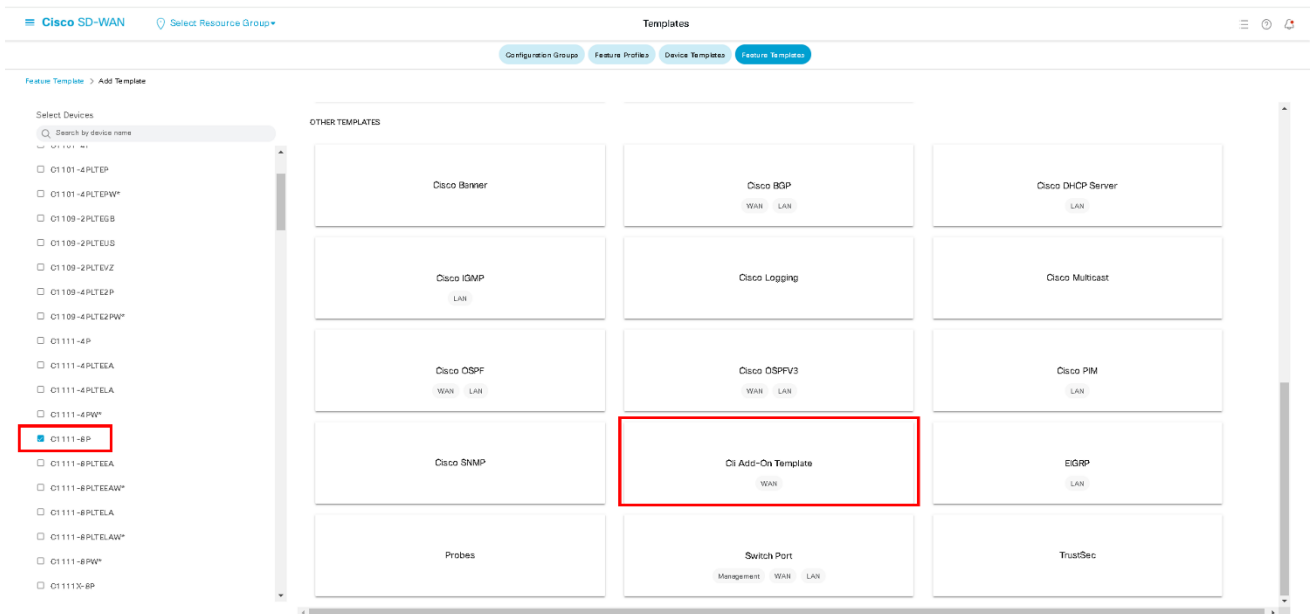
Total Rows: 115

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
ISR1100X-4G_202-22_VPN...	ISR1100X-4G_202-22_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:23:19 PM +
C8300-1N1S-4TZK_203-7...	C8300-1N1S-4TZK_203-7...	Cisco VPN Interface Ethernet	C8300-1N1S-4TZK	1	global	1	Provider-sdwan-order-mi	05 Oct 2023 1:30:50 PM +
C8300-1N1S-4TZK_203-5...	C8300-1N1S-4TZK_203-5...	Cisco VPN Interface Ethernet	C8300-1N1S-4TZK	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:13:26 PM +
C8300-1N1S-4TZK_203-5...	C8300-1N1S-4TZK_203-5...	Cisco VPN Interface Ethernet	C8300-1N1S-4TZK	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:15:37 PM +
C8300-1N1S-4TZK_203-5...	C8300-1N1S-4TZK_203-5...	Cisco VPN Interface Ethernet	C8300-1N1S-4TZK	3	global	2	Provider-sdwan-order-mi	04 Oct 2023 8:17:19 PM +
C8300-1N1S-4TZK_206-1...	C8300-1N1S-4TZK_206-1...	WAN Edge cEdge Cellular In...	C8300-1N1S-4TZK	3	global	2	Provider-sdwan-order-mi	05 Oct 2023 1:39:10 PM +
C8300-1N1S-4TZK_301-4...	C8300-1N1S-4TZK_301-4...	CU Template	C8300-1N1S-4TZK	1	global	1	Provider-sdwan-order-mi	05 Oct 2023 1:33:04 PM +
ISR1100X-4G_202-11_VPN...	ISR1100X-4G_202-11_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:24:51 PM +
C8300-1N1S-4TZK_303-1...	C8300-1N1S-4TZK_303-1...	Cellular Controller	C8300-1N1S-4TZK	3	global	2	Provider-sdwan-order-mi	05 Oct 2023 1:39:41 PM +
ISR1100X-4G_202-23_VPN...	ISR1100X-4G_202-23_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	6	global	1	Provider-sdwan-order-mi	05 Oct 2023 2:25:44 PM +
ISR1100X-4G_202-25_VPN...	ISR1100X-4G_202-25_VPN...	Cisco VPN	ISR 1100X 4G (Cisco OS)	1	global	0	Provider-sdwan-order-mi	05 Oct 2023 2:26:12 PM +
ISR1100X-4G_203-51_VF...	ISR1100X-4G_203-51_VF...	Cisco VPN Interface Ethernet	ISR 1100X 4G (Cisco OS)	5	global	1	Provider-sdwan-order-mi	05 Oct 2023 11:10:26 AM

2. 機種名に「C1111-8P」にチェックを入れ、「Cli Add-On Template」を選択

※タイプⅡのCPEへ設定する場合は「C1111-8PLTELA」にチェック

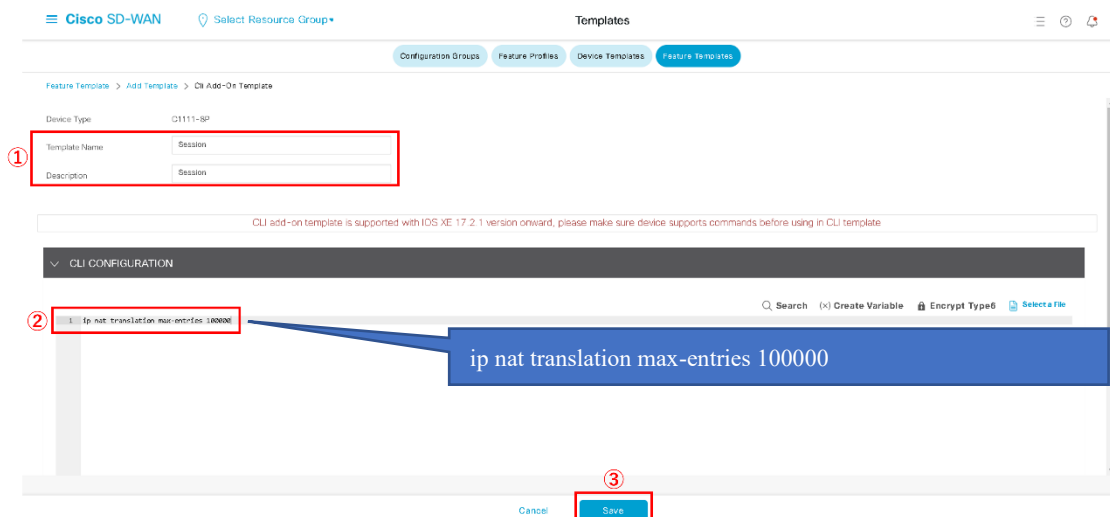
※開通時に既にNTT東日本で作成したCli Add-On Templateがある場合は、そのCli Add-On Templateをコピーしてください。Templateのコピーの手順は3.1. Device Template/Feature Templateのコピーを参照してください。



3. ①Template Name/Description に「Session」を入力

②以下のように1行を入力

③「Save」を選択

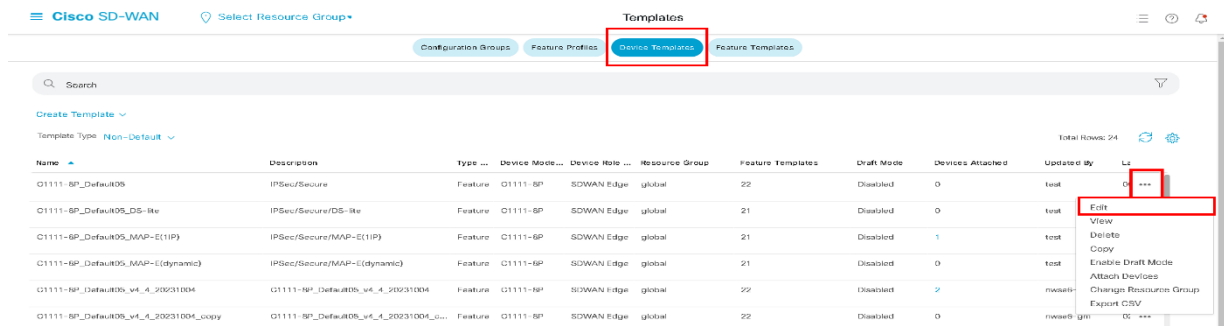


※既存のコンフィグの中でも特に以下の設定は外さないようにお願いします。正常な通信ができなくなり、CPE 交換が必要となる可能性があります。

```
system
vbond {{vbond_fqdn}} port 12346
no ipv6 address dhcp
ipv6 nd ra suppress all
```

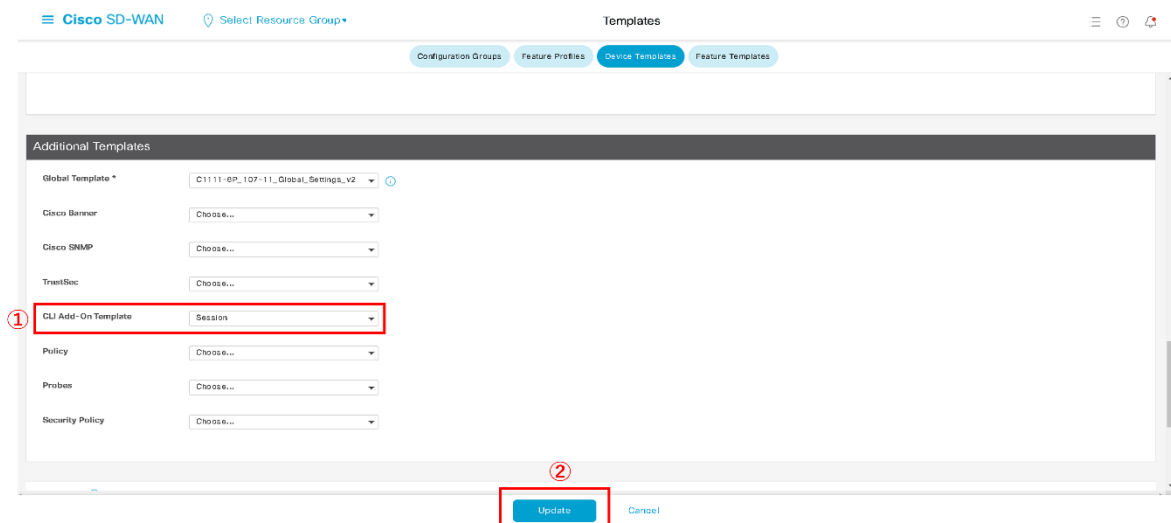
4.13.2. NTT 東日本デフォルト Template をコピーして設定変更をする用途の新しい Device Template を準備

- 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Device」を選択
NTT 東日本デフォルトの Template をコピーし、コピーした Template の「…」から「Edit」を選択
※Template のコピーの手順は 3.1. Device Template/Feature Template のコピーを参照してください。



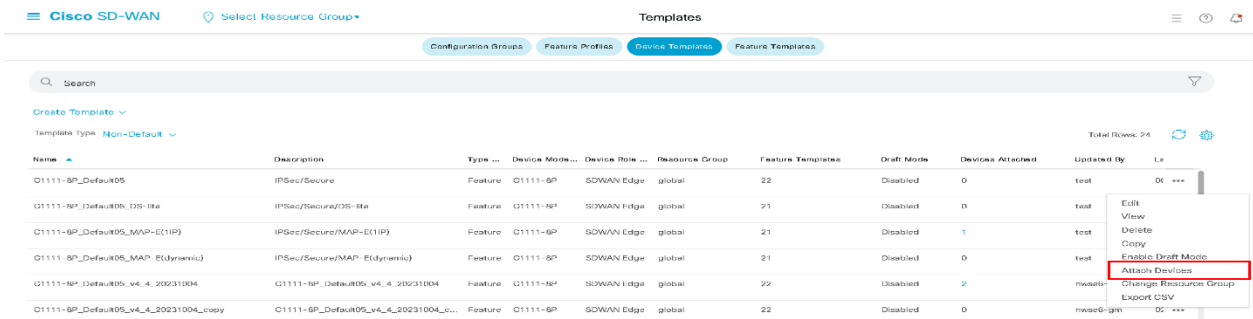
4.13.3. Device Template にセッション変更用の Feature Template をアタッチ

- ①Additional Templates 欄の CLI Add-On Templates を手順 1~4 で作成した「Session」へ変更
②「Update」を選択



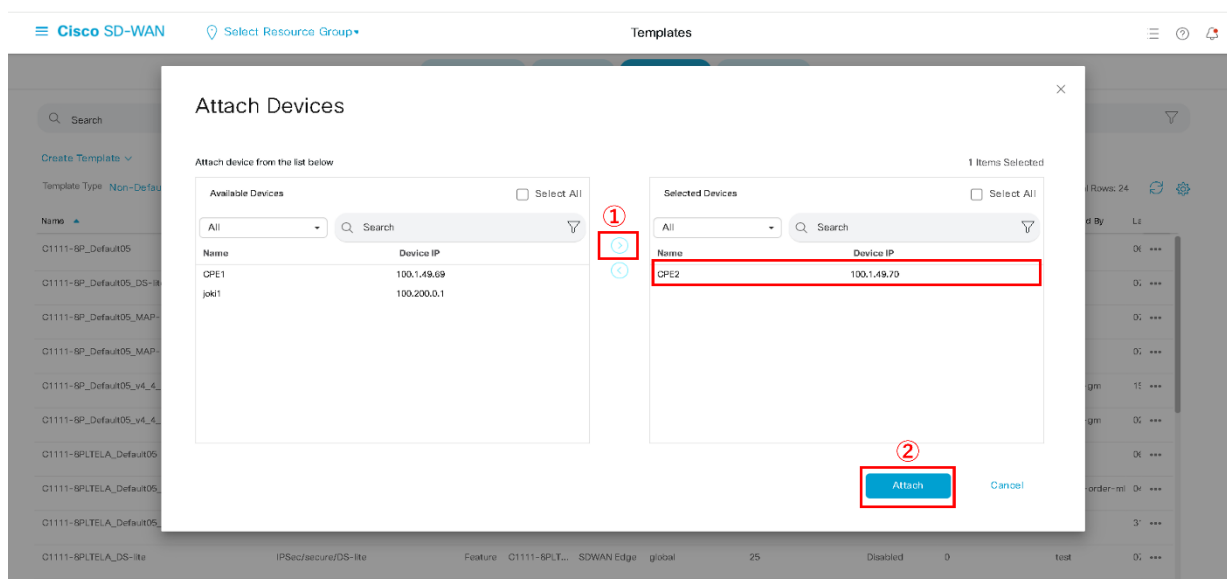
4.13.4. 作成した Device Template を CPE にアタッチ

6. 新たに作成したテンプレートの「…」から「Attach Devices」を選択



7. ①適用したい CPE を選択し, 「→」を選択し右ボックスに移動

②「Attach」を選択



8. 「Next」を選択

The screenshot shows the Cisco vManage Configuration - Templates page. The page title is 'Configuration - Templates'. Below the title, there is a search bar and a table of device templates. The table has columns for S. Chassis Number, System IP, Hostname, and several VLAN ID columns. The first row is selected, and the 'Next' button is highlighted with a red box.

S. Chassis Number	System IP	Hostname	VLAN ID(g010_vlan)	VLAN ID(g011_vlan)	VLAN ID(g012_vlan)	VLAN ID(g013_vlan)	VLAN ID(g014_vlan)	VLAN ID(g015_vlan)	VLAN ID(g016_vlan)	VLAN ID(g017_v
C1111-SP-FGL2K36LFAQ	100.1.78.17	CPE2	10	10	10	10	20	20	20	20

9. ①以下の画面で CPE を選択し、コンフィグを出力(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります、エラー内容及び手順を再確認して下さい

The screenshot shows the Cisco vManage Configuration - Templates page. The 'Device list (Total: 1 devices)' section is expanded, showing a list of devices. The first device, 'C1111-SP-FGL2K36LFAQ', is selected and highlighted with a red box. The 'Local Configuration vs. New Configuration' dialog is open, showing a list of configuration items. The 'Configure Devices' button is highlighted with a red box.

Line	Configuration
1	system
2	ntp-status
3	device-model
4	device-group
5	system-ip
6	overlay-id
7	site-id
8	port-offset
9	control-session-gps
10	admin-tech-on-failure
11	sp-organization-name
12	organization-name
13	port-bgp
14	track-transport
15	track-default-gateway
16	console-band-rate
17	no co-demand enable
18	co-demand life-timeout
19	vbond vbond09.vbond.ottawa.jp port 12346
20	logging
21	disk
22	enable
23	!
24	!
25	!
26	bfd app-route multiplier 6
27	bfd app-route poll-interval 600000
28	asocing
29	ipsec
30	rekey
31	replay-window
32	authentication-type sha1-hmac ah-sha1-hmac

10. Status が success, Message が Done となっていればコンフィグ適用が完了

※Status 変更までに 1 分程度かかります

※Status が success とならない場合、エラー内容及び手順を確認し時間をおいてリトライの実施をお願いします

Cisco vManage Select Resource Group

Push Feature Template Configuration Validation Success Initiated By: nmesef-gm | Tenant: CSDWNE-09-0000-0001 From: 10.128.26.254

Total Task: 1 | Success: 1

Search

Total Rows: 1

Status	Message	chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template Conf...	1111-8P-FGL2436LF4Q	C1111-8P	CPE2	100.1.78.17	200010001	209.255.1.2

5

各種状態の確認方法

本章では、CPE の各種状態の確認方法を解説します。

5.1. 全 CPE の状態確認方法

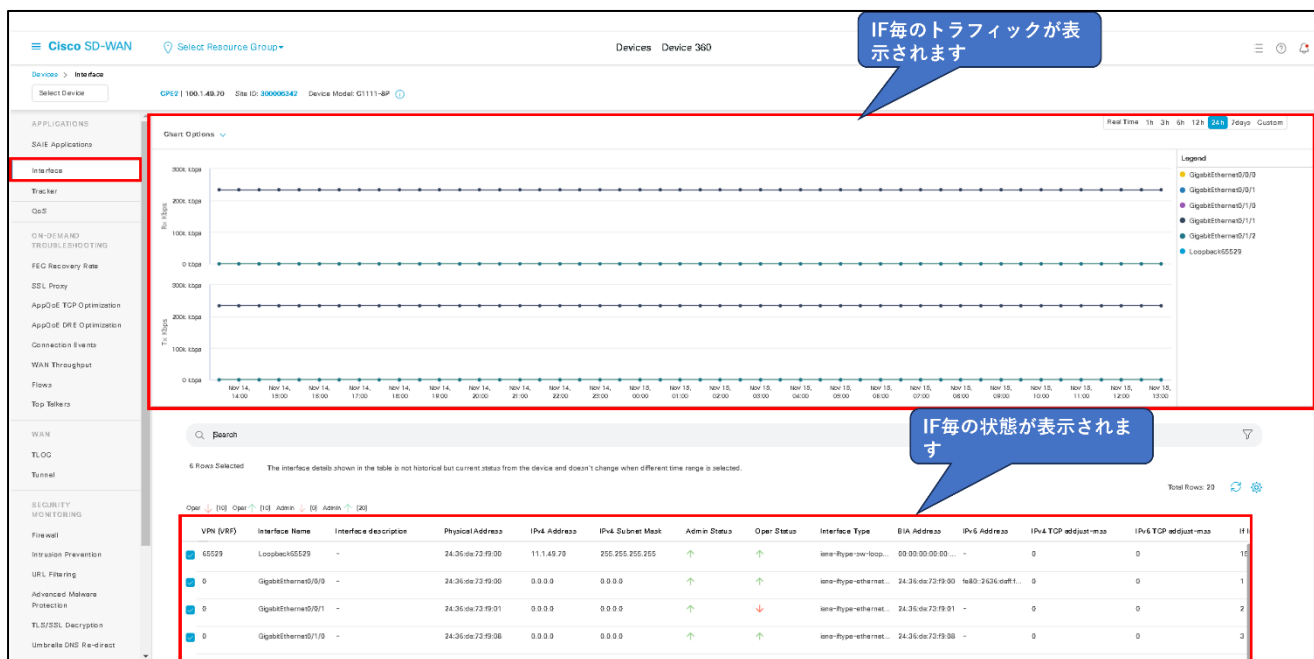
1. 左ペイン(左の領域)の Monitor から Network を選択
2. 全 CPE の情報が表示される
3. ホスト名を選択すると CPE の詳細な情報を確認することが可能

The screenshot shows the 'Devices' page in the Cisco SD-WAN interface. A table lists 12 devices. Three callouts highlight specific columns: 'Hostname' (labeled 'ホスト名を確認できます'), 'Site ID' (labeled 'CPEのSite-IDを確認できます'), and 'Reachability' (labeled 'CPEのUP/DOWNの状態を確認できます').

Hostname	Device Model	Site ID	System IP	Health	Reachability	vSmart Control	BFD	Up Since	CPU Load	Memory Utilization	Action
CPE1	CT1111-BP	200000541	100.1.49.69	●	↓	0 / 2	0 / -	Nov 14, 2023 04:18 PM	22.14%	62.2%	...
CPE2	CT1111-BP	300000342	100.1.49.70	●	↑	1 / 2	3 / 3	Nov 07, 2023 01:22 AM	49.56%	75.9%	...
CPE3	CT1111-BP/LELA	200000343	100.1.49.71	●	↓	0 / 2	0 / -	Nov 08, 2023 07:43 PM	14.58%	70%	...
CPE4	ISR 1100X 49 (Cisco OS)	300000344	100.1.49.72	●	↑	2 / 2	3 / 3	Nov 07, 2023 01:22 AM	27.64%	85%	...
CPE5	C8300-1N12-4T2X	200000345	100.1.49.73	●	↓	0 / 2	0 / -	Oct 31, 2023 07:51 PM	10.92%	42%	...
Router	ISR 1100X 49 (Cisco OS)	200000004	100.200.0.4	●	↑	2 / 2	0 / 0	Nov 15, 2023 11:51 AM	32.35%	35%	...

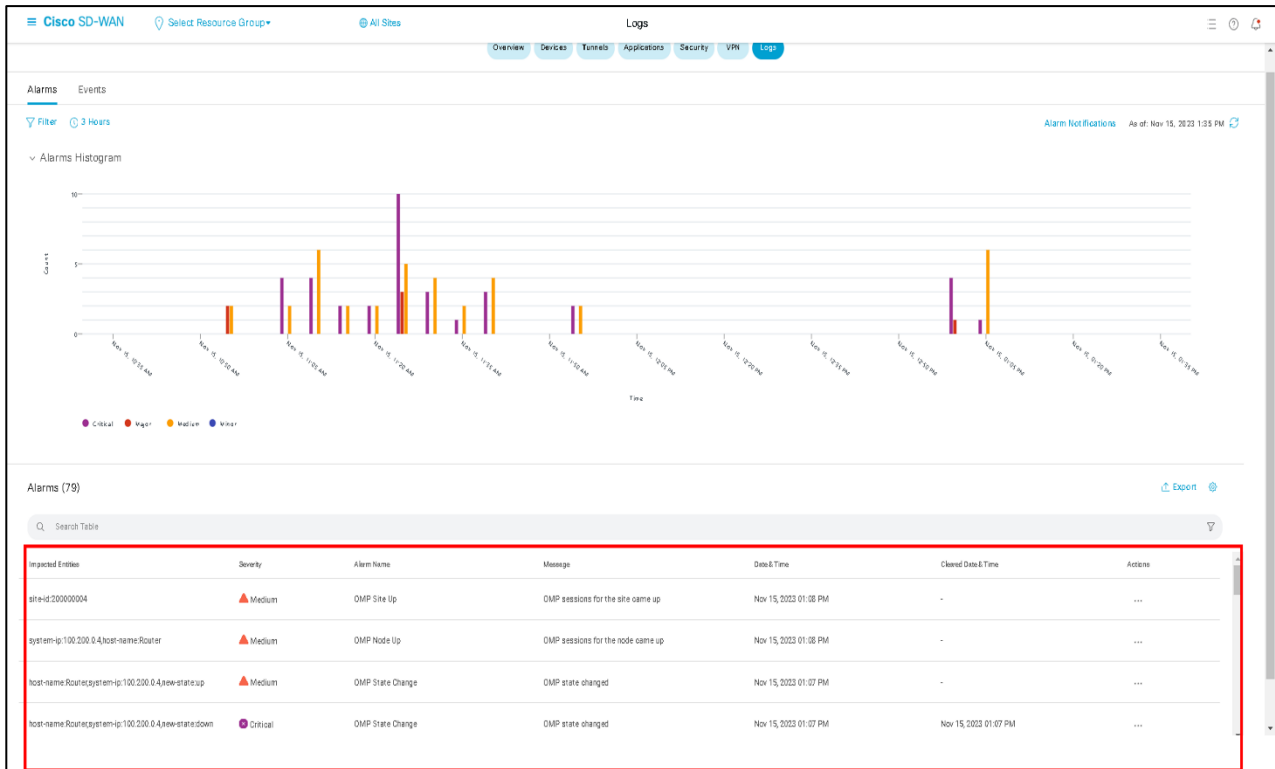
5.2. CPE のインターフェース状態確認方法

1. 左ペイン(左の領域)の Monitor から Network を選択
2. 詳細を確認したい CPE のホスト名を選択
3. 左メニューから Interface を選択



5.3. CPE のログ確認方法

1. 左ペイン(左の領域)の Monitor から Logs を選択
2. アラームの発生状況を表示

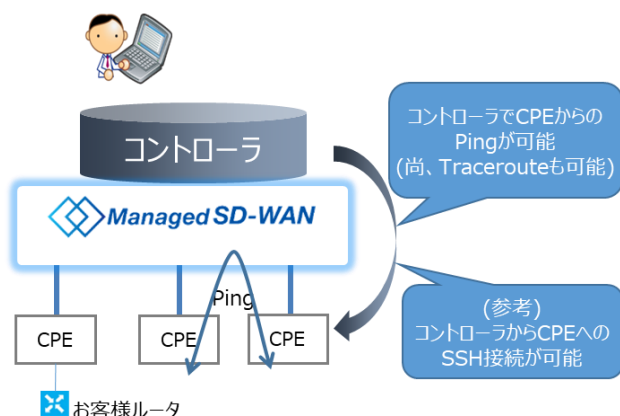


5.4. vManage のトラブルシューティング機能(Ping 機能)

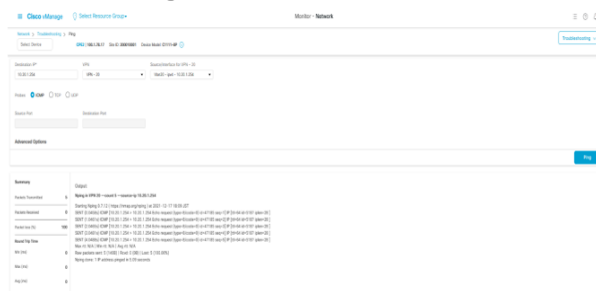
■お客様ご自身で遠隔で通信確認が可能となるようコントローラからのトラブルシューティング機能（Ping 機能）を提供します。

コントローラからの Ping 機能等を提供します。尚、CPE への SSH 接続も可能ですが、留意事項がありますので必ずご確認ください。また Speed Test はご利用いただけません。

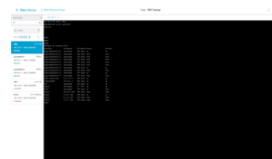
■ サービス概要図



コントローラからPing試験時の画面イメージ



(参考) vManageからSSH接続時の画面イメージ

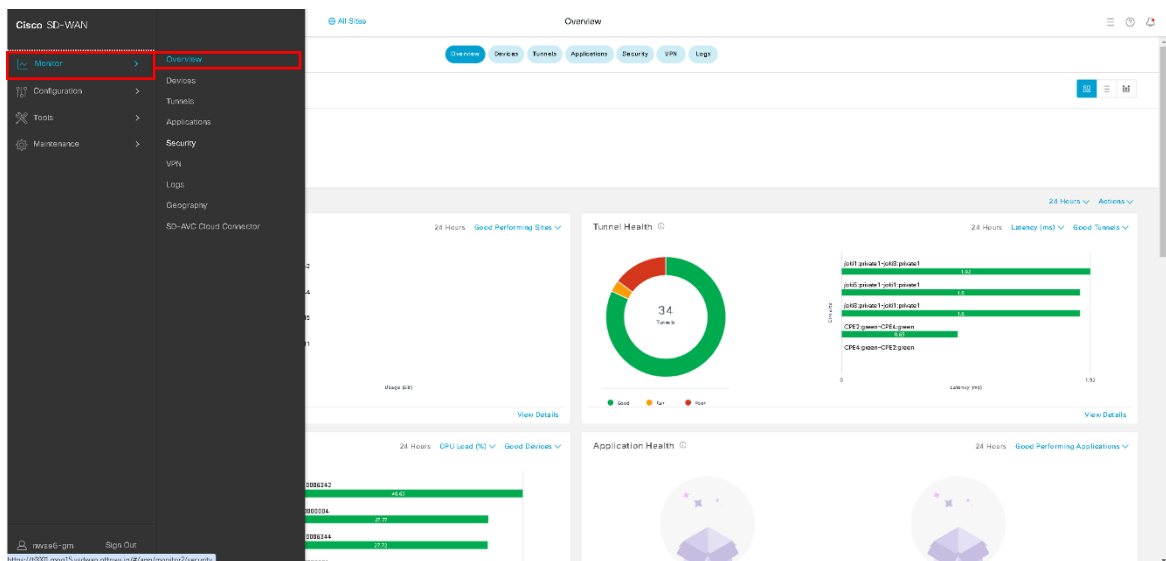


■ SSH 接続ご利用の際の留意事項

- ・ SSH 接続でもでもお客様にて通信の確認ができます。
- ・ 初期 Username/Password は申込書へ記載します。
- ・ Username「admin」の編集は禁止です。もし間違えて削除、変更した場合は、ユーザ設定マニュアル（コントローラ設定編）7.3 章に基づき設定の戻しが必要となります。設定を戻した場合は、CPE の設定自体も元に戻ります。
- ・ コマンドリファレンスのカテゴリ「非推奨」のコマンド記載がありますので参照下さい。

5.4.1. トラブルシューティング(Ping)利用方法

1. 左ペイン(左の領域)の Monitor から Overview を選択



2. Ping/Trace Route 実施対象の CPE を選択

Cisco SD-WAN Select Resource Group All Sites Devices

Overview **Devices** Tunnels Applications Security VPN Logs

Devices

Device Group All

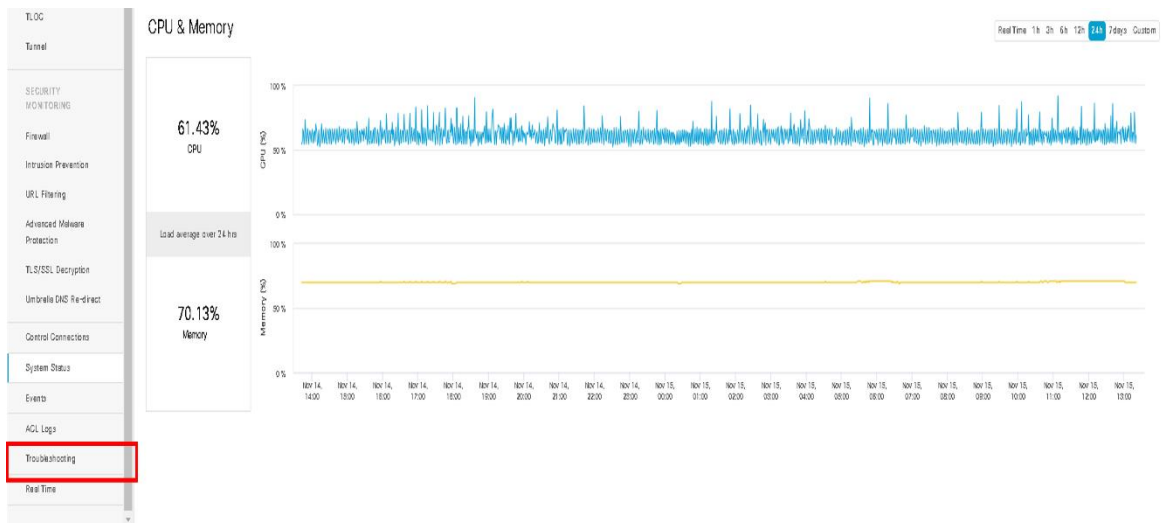
Devices (12) Export

Search Table

As of: Nov 15, 2023 01:49 PM

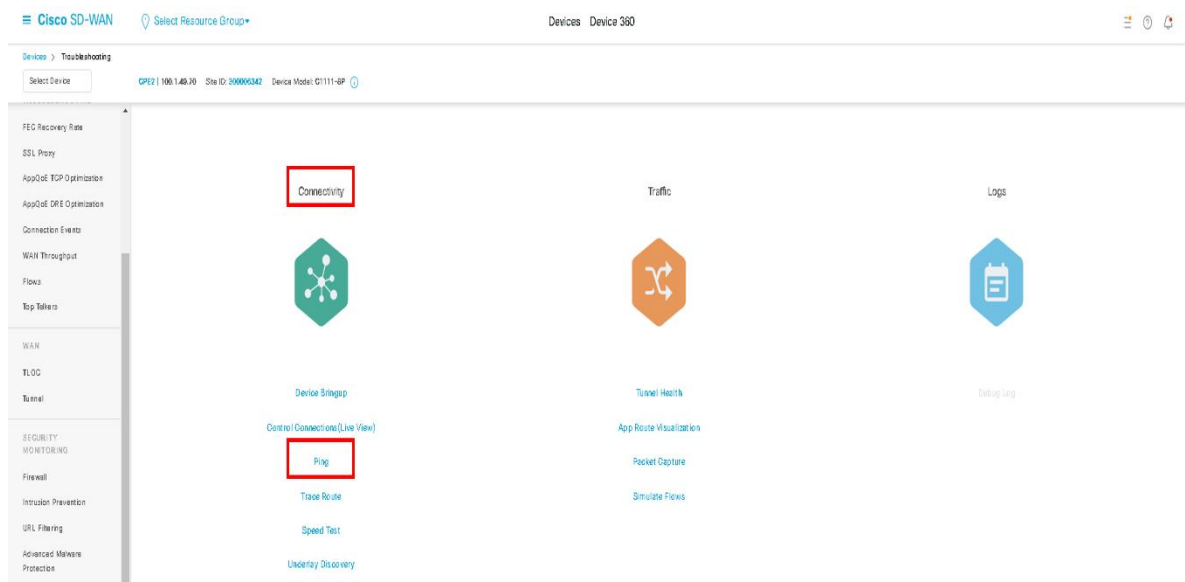
Hostname	Device Model	Site ID	System IP	Health	Reachability	vSmart Control	BFD	Up Since	CPU Load	Memory Utilization	Action
CPE1	C1111-IP	300015342	100.1.49.70	Good	Up	1 / 2	3 / 3	Nov 07, 2023 01:22 AM	49.55%	79.7%	...
CPE4	ISR 1100C 46 (Cisco IOS)	300015344	100.1.49.72	Good	Up	2 / 2	3 / 3	Nov 07, 2023 01:22 AM	28.57%	35%	...

3. Monitor 項目の最下部へスクロールし、Troubleshooting を選択

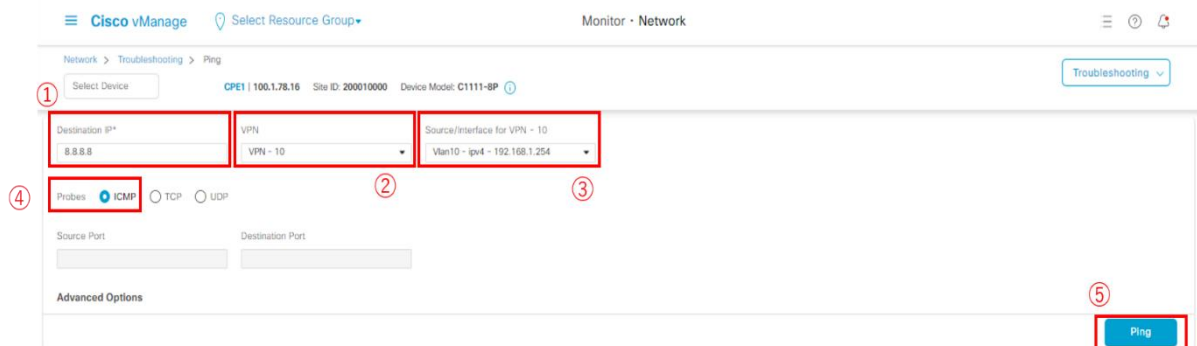


4. Connectivity の Ping を選択

(※Troubleshooting 画面を表示すると「No data available from device」が表示されますが表示上の仕様であり通信影響はございません。)

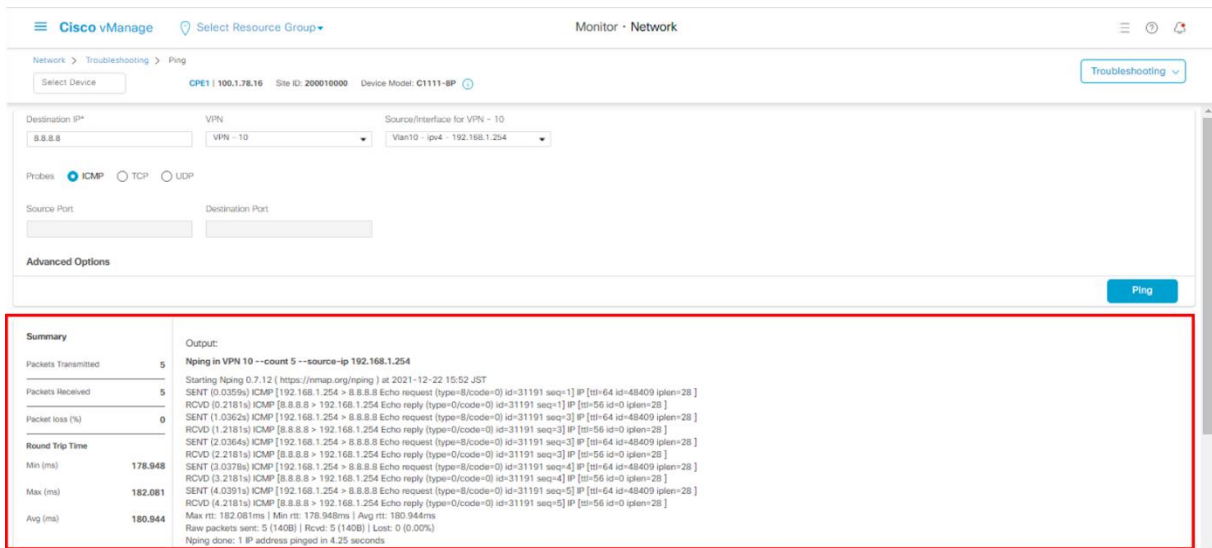


5. ①「Destination IP」を入力
- ②「VPN」を選択
- ③「Source/Interface」を選択（※②で選択した VPN にて利用できる Source/Interface が選択できます）
- ④「Probes」にて「ICMP」を選択
- ⑤「Ping」を押下



The screenshot shows the Cisco vManage interface for configuring a Ping test. The interface includes a header with 'Cisco vManage' and 'Monitor - Network'. Below the header, there's a 'Select Device' dropdown set to 'CPE1 | 100.1.78.16'. The main configuration area has three input fields: 'Destination IP*' (8.8.8.8), 'VPN' (VPN - 10), and 'Source/Interface for VPN - 10' (Vlan10 - ip4 - 192.168.1.254). Below these, there are radio buttons for 'Probes': ICMP (selected), TCP, and UDP. There are also input fields for 'Source Port' and 'Destination Port'. At the bottom right, there is a 'Ping' button. Red circles and boxes highlight the steps: ① Destination IP, ② VPN, ③ Source/Interface, ④ ICMP, and ⑤ Ping button.

6. Ping の結果が表示される

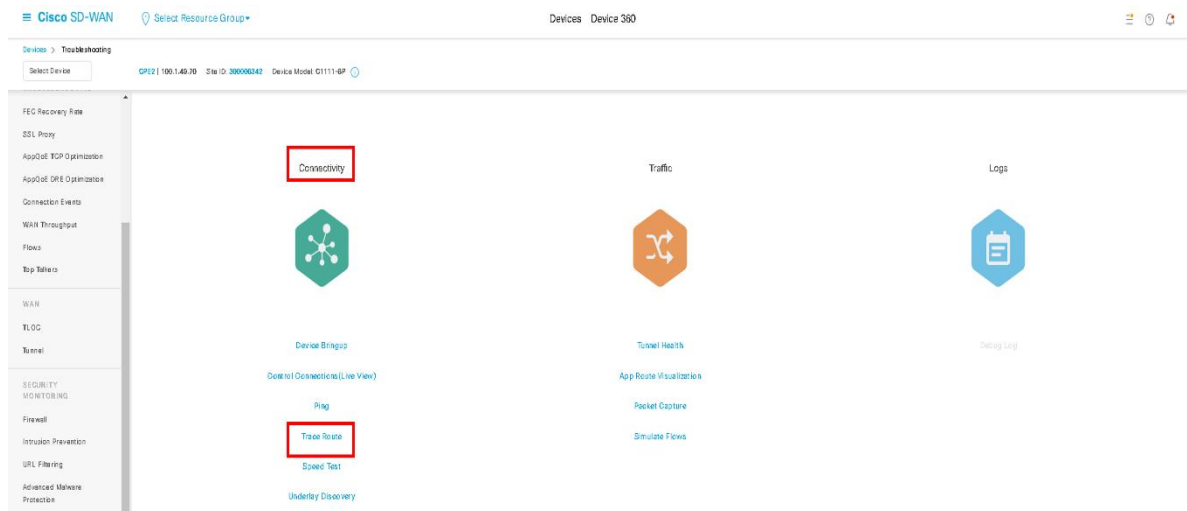


The screenshot shows the Cisco vManage interface displaying the results of a Ping test. The interface includes a header with 'Cisco vManage' and 'Monitor - Network'. Below the header, there's a 'Select Device' dropdown set to 'CPE1 | 100.1.78.16'. The main configuration area is the same as in the previous screenshot. Below the configuration area, there is a 'Summary' section and an 'Output' section. The 'Summary' section shows: Packets Transmitted: 5, Packets Received: 5, Packet loss (%): 0, Round Trip Time: Min (ms): 178.948, Max (ms): 182.081, Avg (ms): 180.944. The 'Output' section shows the command 'Nping in VPN 10 --count 5 --source-ip 192.168.1.254' and the results of the ping test, including the start time, the command used, and the results of the ping test (5 successful pings, 0% loss).

5.4.2. Troubleshooting(Traceroute)利用方法

1. Connectivity の Trace Route を選択

(※TroubleShooting 画面を表示すると「No data available from device」が表示されることは仕様です)

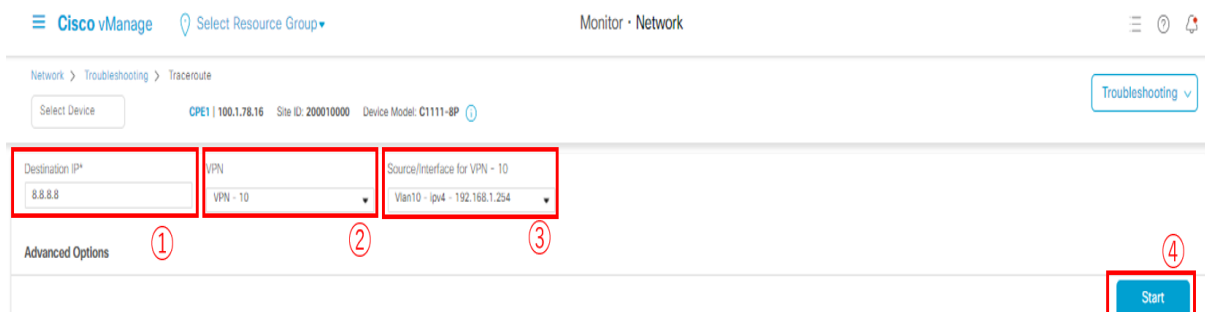


2. ①Destination IP を入力

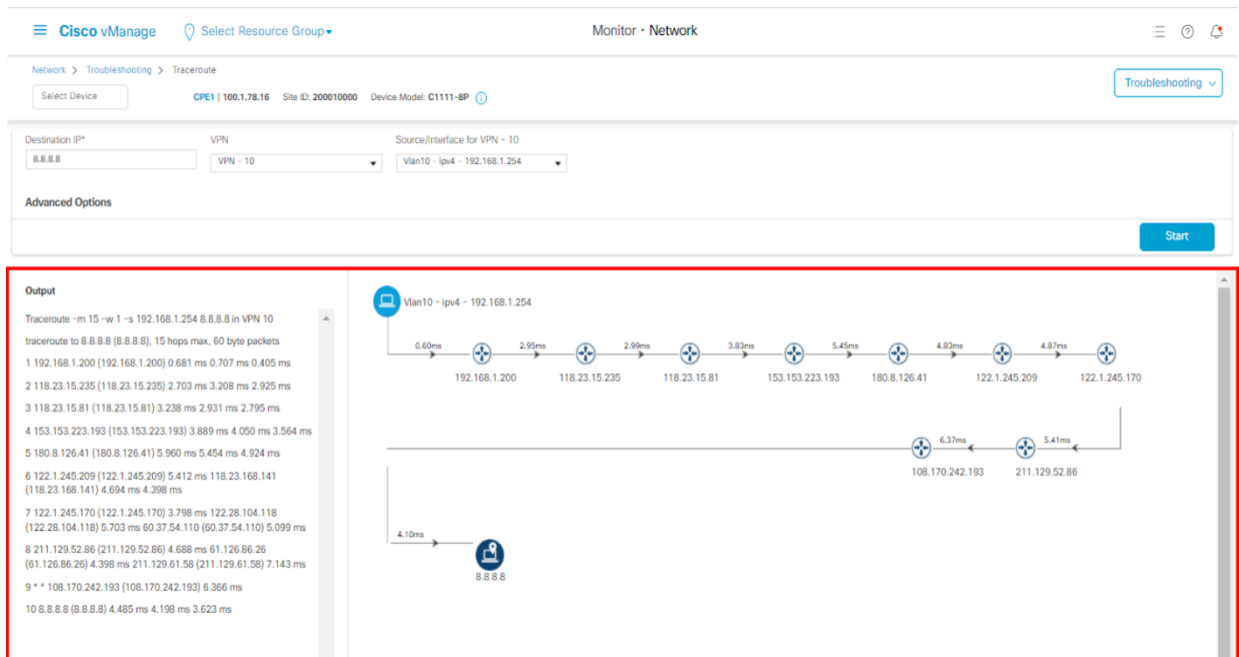
②VPN を選択

③Source/Interface を選択 (※②で選択した VPN にて利用できる Source/Interface が選択できます)

④Start を選択し、Trace Route を実施



3. Trace Route の結果が表示



The screenshot shows the Cisco vManage interface for the 'Monitor - Network' section, specifically the 'Traceroute' tool. The configuration is as follows:

- Destination IP:** 8.8.8.8
- VPN:** VPN - 10
- Source/Interface for VPN - 10:** Vlan10 - ipv4 - 192.168.1.254

The **Output** section displays the traceroute results in two formats: a text-based table and a visual hop diagram.

Text-based Output:

```
Traceroute -m 15 -w 1 -s 192.168.1.254 8.8.8.8 in VPN 10
traceroute to 8.8.8.8 (8.8.8.8), 15 hops max, 60 byte packets
 1 192.168.1.200 (192.168.1.200) 0.681 ms 0.707 ms 0.405 ms
 2 118.23.15.235 (118.23.15.235) 2.703 ms 3.208 ms 2.925 ms
 3 118.23.15.81 (118.23.15.81) 3.238 ms 2.931 ms 2.795 ms
 4 153.153.223.193 (153.153.223.193) 3.889 ms 4.050 ms 3.564 ms
 5 180.8.126.41 (180.8.126.41) 5.960 ms 5.454 ms 4.924 ms
 6 122.1.245.209 (122.1.245.209) 5.412 ms 118.23.168.141 (118.23.168.141) 4.694 ms 4.398 ms
 7 122.1.245.170 (122.1.245.170) 3.798 ms 122.28.104.118 (122.28.104.118) 5.703 ms 60.37.54.110 (60.37.54.110) 5.099 ms
 8 211.129.52.86 (211.129.52.86) 4.688 ms 61.126.86.26 (61.126.86.26) 4.398 ms 211.129.61.58 (211.129.61.58) 7.143 ms
 9 * * 108.170.242.193 (108.170.242.193) 6.366 ms
10 8.8.8.8 (8.8.8.8) 4.485 ms 4.198 ms 3.623 ms
```

Visual Hop Diagram:

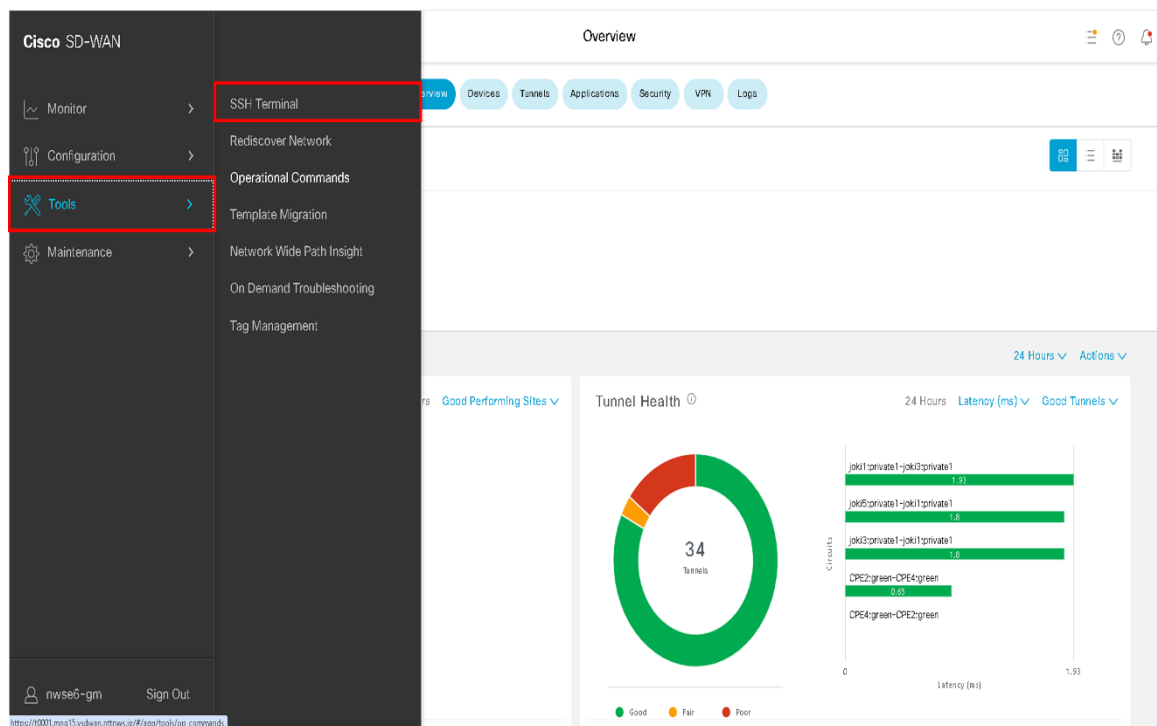
The diagram illustrates the path from the source 'Vlan10 - ipv4 - 192.168.1.254' to the destination '8.8.8.8'. It shows 10 hops with the following IP addresses and round-trip times (ms):

- Hop 1: 192.168.1.200 (0.68ms)
- Hop 2: 118.23.15.235 (2.95ms)
- Hop 3: 118.23.15.81 (2.99ms)
- Hop 4: 153.153.223.193 (3.83ms)
- Hop 5: 180.8.126.41 (5.45ms)
- Hop 6: 122.1.245.209 (4.87ms)
- Hop 7: 122.1.245.170 (4.87ms)
- Hop 8: 211.129.52.86 (5.41ms)
- Hop 9: 108.170.242.193 (6.37ms)
- Hop 10: 8.8.8.8 (4.10ms)

※1hop目のIPアドレスに2で入力したDestination IP アドレスが表示される場合があります。

5.4.3. (参考) CPE の SSH 接続

1. 左ペイン(左の領域)の Tools から SSH Terminal を選択

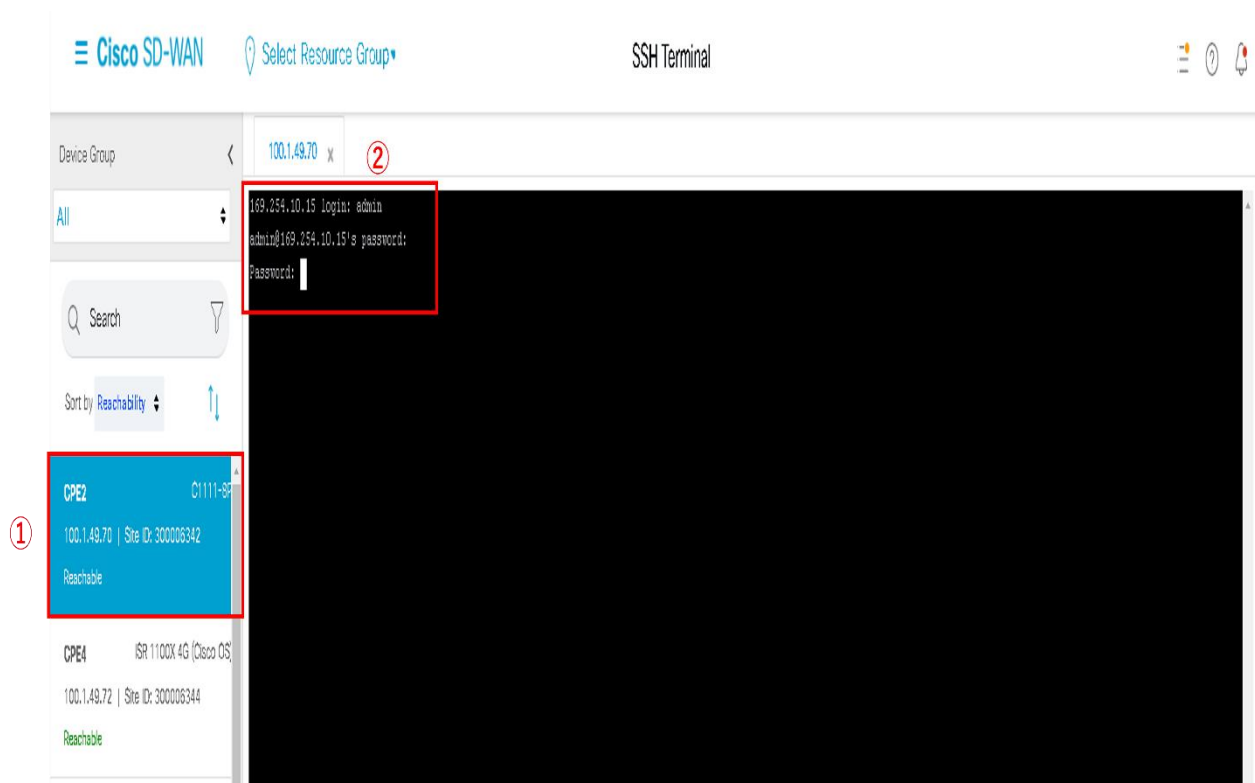


2. ①確認したいCPEを選択

②「login:」にアカウント名を入力し、「password:」および「Password」にパスワード名を入力

※初期の login/password については、「申込書」を参照ください。

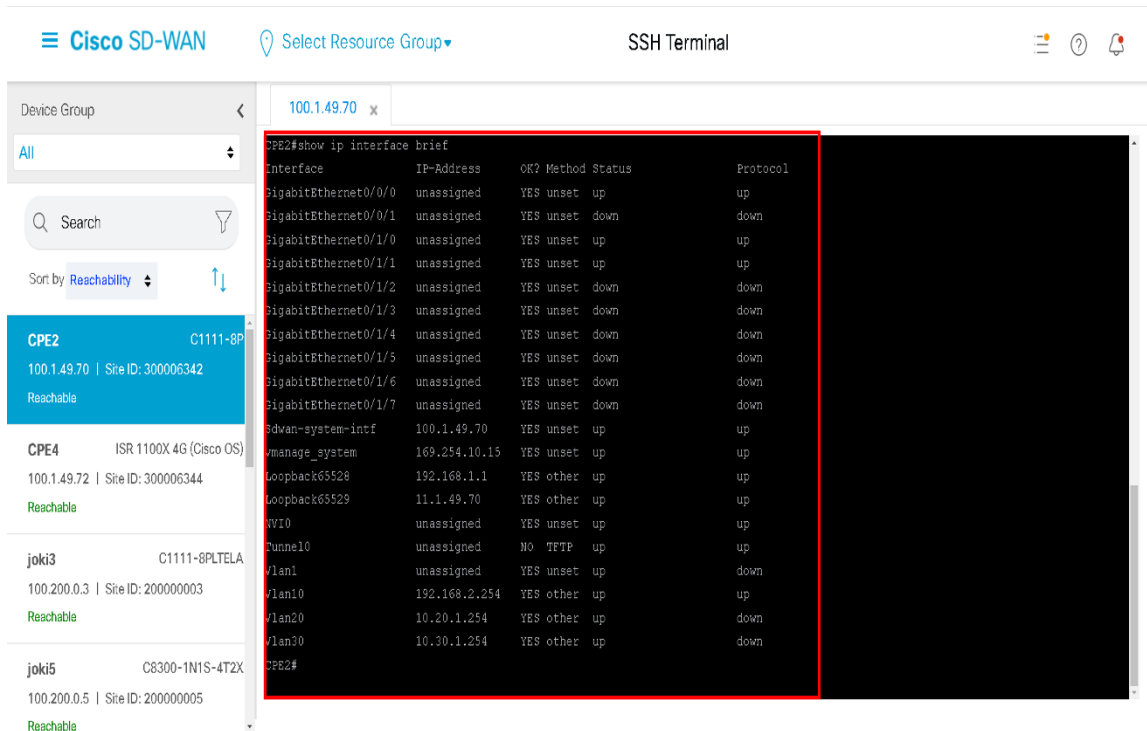
※コマンドの詳細は同梱のコマンドリファレンスを参照ください。



(参考) CPE のインターフェース状態確認方法(SSH)

(※SSH 接続していることを前提とした手順です)

「show ip interface brief」をターミナル上に入力



The screenshot shows the Cisco SD-WAN management interface. On the left, a sidebar lists device groups: CPE2 (100.1.49.70), CPE4 (100.1.49.72), joki3 (100.200.0.3), and joki5 (100.200.0.5). The main area is titled 'SSH Terminal' and shows the command prompt 'CPE2#show ip interface brief'. The output is a table with columns: interface, IP-Address, OK?, Method, Status, and Protocol.

interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0/1	unassigned	YES	unset	down	down
GigabitEthernet0/1/0	unassigned	YES	unset	up	up
GigabitEthernet0/1/1	unassigned	YES	unset	up	up
GigabitEthernet0/1/2	unassigned	YES	unset	down	down
GigabitEthernet0/1/3	unassigned	YES	unset	down	down
GigabitEthernet0/1/4	unassigned	YES	unset	down	down
GigabitEthernet0/1/5	unassigned	YES	unset	down	down
GigabitEthernet0/1/6	unassigned	YES	unset	down	down
GigabitEthernet0/1/7	unassigned	YES	unset	down	down
sdwan-system-intf	100.1.49.70	YES	unset	up	up
manage_system	169.254.10.15	YES	unset	up	up
Loopback65528	192.168.1.1	YES	other	up	up
Loopback65529	11.1.49.70	YES	other	up	up
VV10	unassigned	YES	unset	up	up
Tunnel10	unassigned	NO	TFTP	up	up
vlan1	unassigned	YES	unset	up	down
vlan10	192.168.2.254	YES	other	up	up
vlan20	10.20.1.254	YES	other	up	down
vlan30	10.30.1.254	YES	other	up	down

(参考) CPE のルーティング情報の確認方法(SSH)

「show ip route vrf 10」をターミナル上に入力(※手順例では vrf の値は 10 とします)

Cisco SD-WAN
Select Resource Group
SSH Terminal

Device Group
100.1.49.70
All
Search
Sort by Reachability

CPE2
C1111-8P
100.1.49.70 | Site ID: 300006342
Reachable

CPE4
ISR 1100X 4G (Cisco OS)
100.1.49.72 | Site ID: 300006344
Reachable

Jok3
C1111-8P1TELA
100.200.0.3 | Site ID: 200000003
Reachable

Jok5
C8300-1N1S-4T2X
100.200.0.5 | Site ID: 200000005
Reachable

swve15000111
C8000v
215.110.1.1 | Site ID: 110150001
Reachable

```

CPE2#show ip route vrf 10

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - CMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - OER, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from Pfr
       & - replicated local route overrides by connected

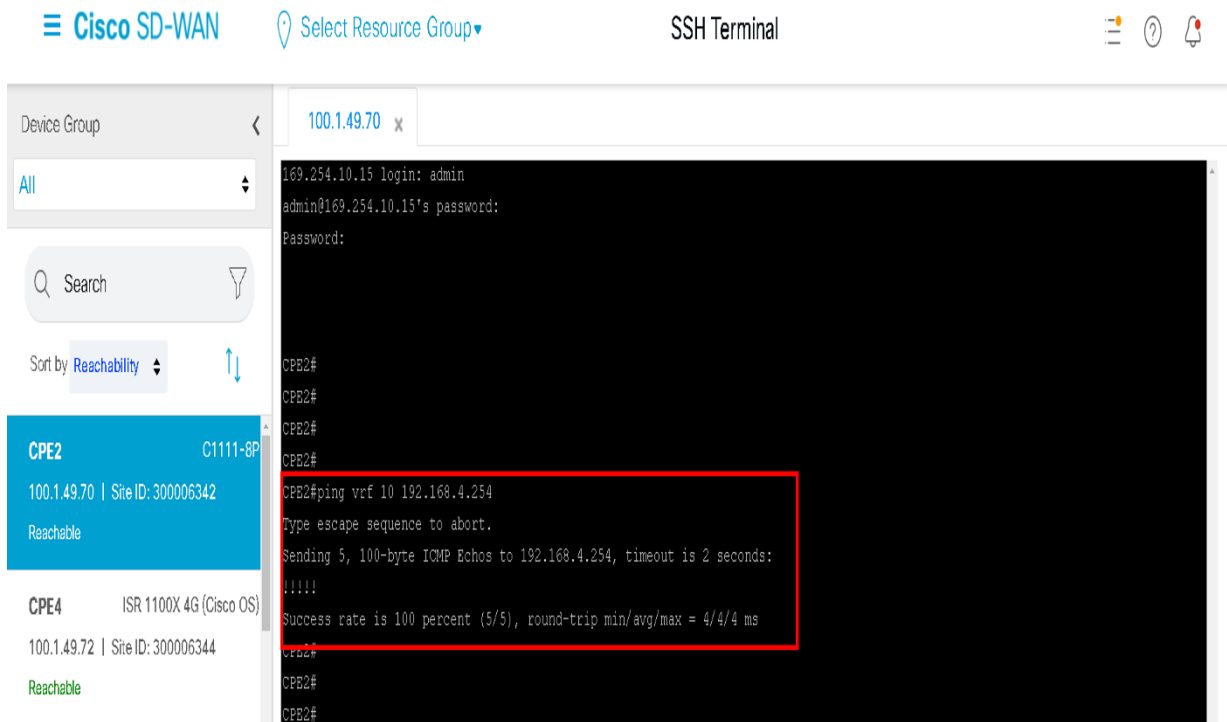
Gateway of last resort is not set

R      10.0.0.0/8 [251/0] via 215.110.1.1, 02:58:42, Sdwan-system-intf
R      172.16.0.0/12 [251/0] via 215.110.1.1, 02:58:42, Sdwan-system-intf
R      192.168.0.0/16 [251/0] via 215.110.1.1, 02:58:42, Sdwan-system-intf
R      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, Vlan10
L      192.168.2.254/32 is directly connected, Vlan10
R      192.168.4.0/24 [251/0] via 100.1.49.72, 5d20h, Sdwan-system-intf
CPE2#

```

(参考) CPE の ping 確認方法(SSH)

「ping vrf 10 [宛先アドレス]」をターミナル上に入力(※手順例では vrf の値は 10 とします)



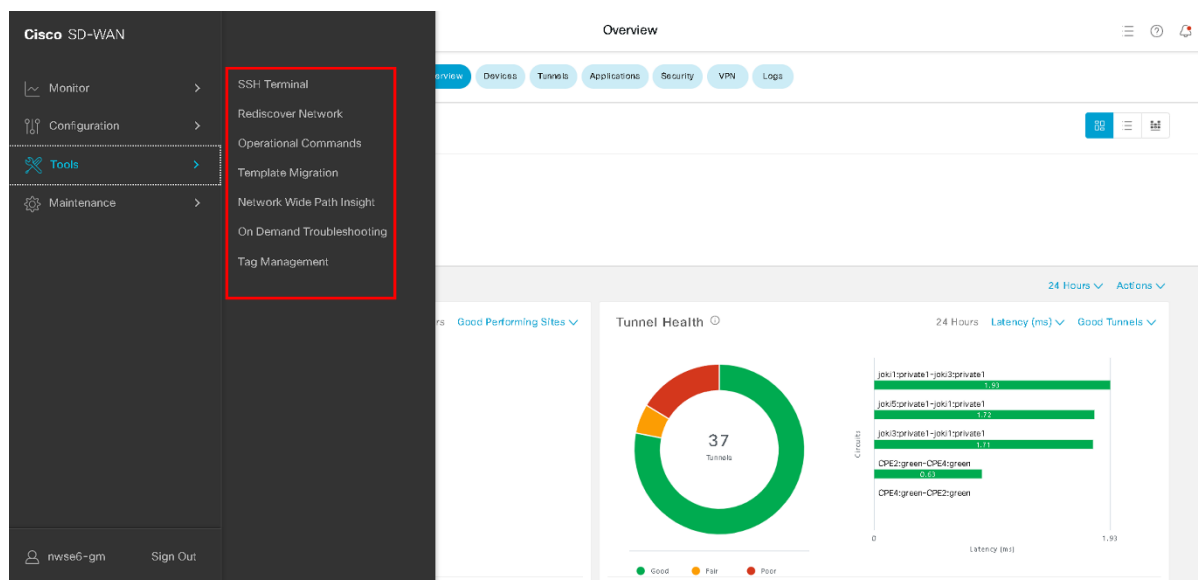
The screenshot displays the Cisco SD-WAN management console. On the left, a sidebar shows the 'Device Group' dropdown set to 'All', a search bar, and a 'Sort by' menu set to 'Reachability'. Below this, a list of devices is shown, with 'CPE2' (C1111-8P) highlighted in blue. The main area is titled 'SSH Terminal' and shows a terminal session for IP 100.149.70. The terminal output shows a successful login as 'admin' and a ping command being executed: 'CPE2#ping vrf 10 192.168.4.254'. The ping results show a success rate of 100 percent (5/5) with a round-trip time of 4/4/4 ms. The terminal text is as follows:

```
169.254.10.15 login: admin
admin@169.254.10.15's password:
Password:

CPE2#
CPE2#
CPE2#
CPE2#
CPE2#ping vrf 10 192.168.4.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.254, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
CPE2#
CPE2#
CPE2#
```

5.4.4. Tools の非推奨事項

Tools の SSH Terminal 以外の機能（Rediscover Network/Operational Commands/Template Migration）はお客様ご利用上不要ですので、使用は推奨されません。



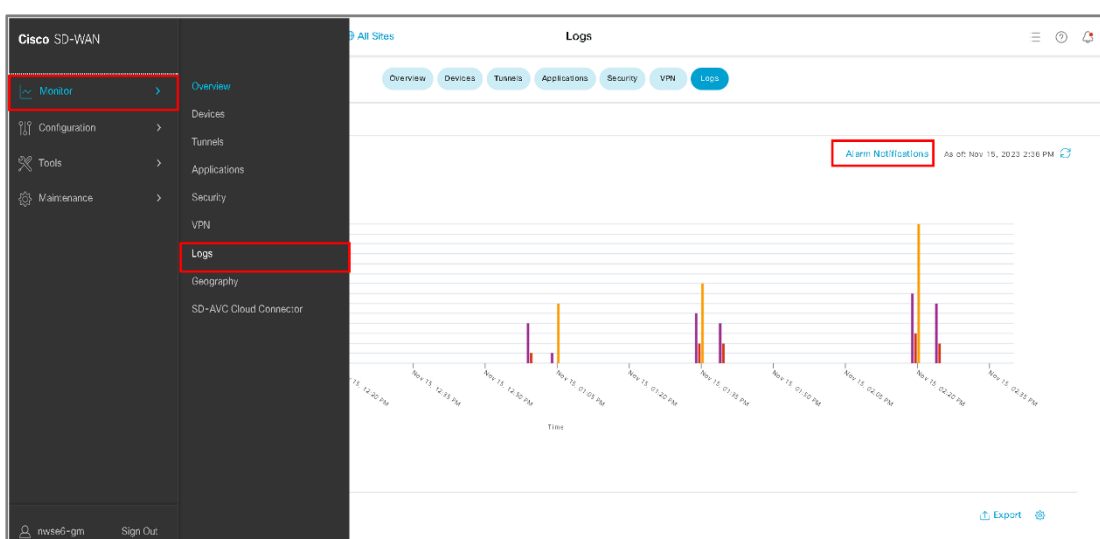
5.5. CPE 故障通知サービス通知先アドレス確認方法

Managed SD-WAN のオプションサービスである CPE 故障通知サービスにおける通知先アドレスの確認したい場合、以降の手順を実施します。

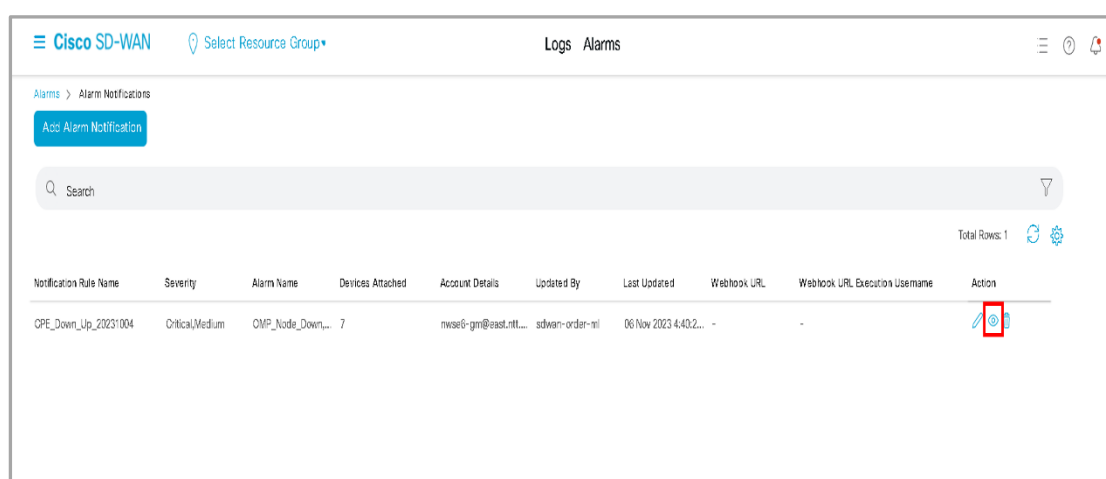
※CPE 故障時メール通知は別途契約が必要です。


5.5.1. 通知先メールアドレスの確認方法

1. 左ペイン(左の領域)の「monitor」>「Logs」を選択し「Alarm Notifications」をクリック

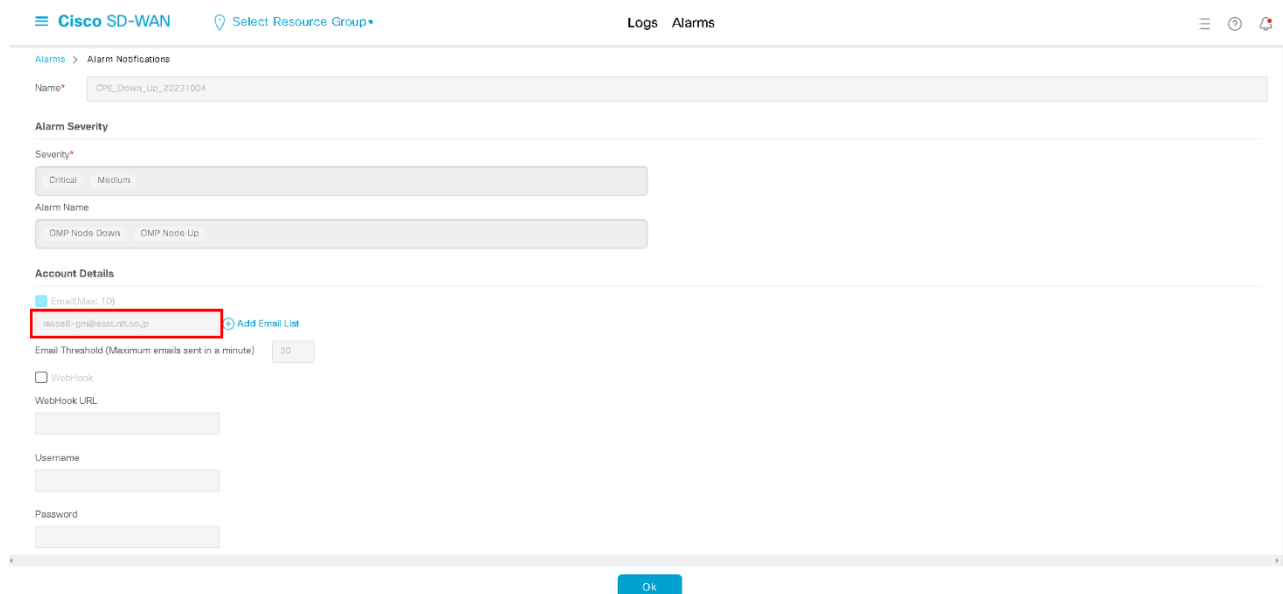


2. 作成されている項目の参照マークを選択



Notification Rule Name	Severity	Alarm Name	Devices Attached	Account Details	Updated By	Last Updated	Webhook URL	Webhook URL Execution Username	Action
CPE_Down_Up_20231004	Critical/Medium	CMP_Node_Down...	7	mwse6-grn@east.ntt...	sdwan-order-mi	06 Nov 2023 4:40:2...	-	-	

- 「Notification Configuration」画面にて「Account Details」の「Emails」をクリックします。



Cisco SD-WAN Select Resource Group Logs Alarms

Alarms > Alarm Notifications

Name* CPE_Down_Up_20231004

Alarm Severity

Severity* Critical Medium

Alarm Name OMP Node Down OMP Node Up

Account Details

Email (Max: 10)

nwse6-mi@east.ntt.co.jp Add Email List

Email Threshold (Maximum emails sent in a minute) 30

☐ Webhook

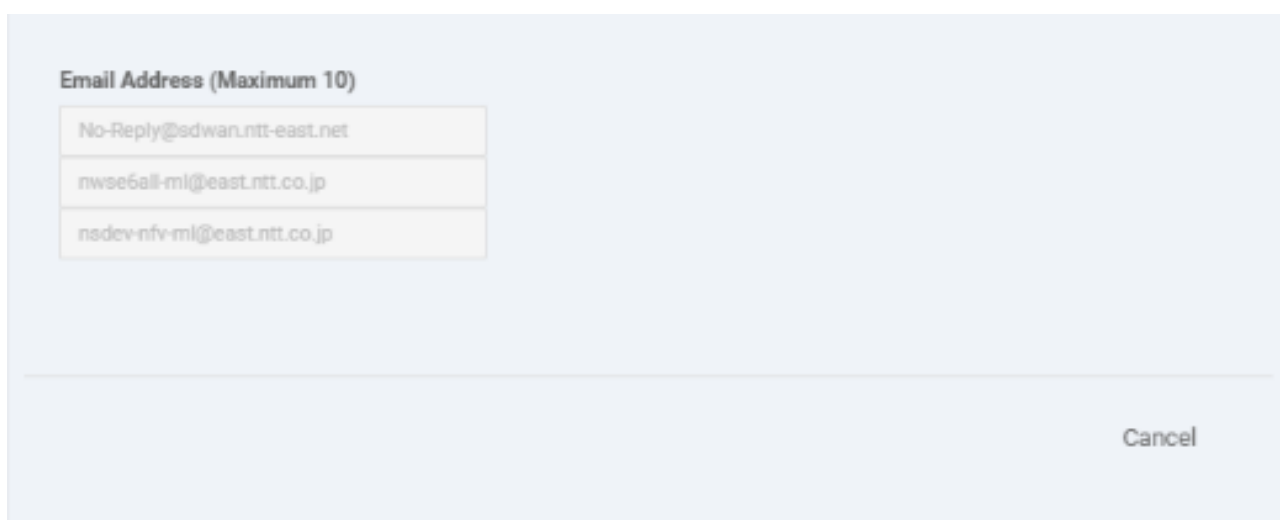
Webhook URL

Username

Password

Ok

- Email List を確認いただきます。



Email Address (Maximum 10)

No-Reply@sdwan.ntt-east.net

nwse6-mi@east.ntt.co.jp

nsdev-nfv-mi@east.ntt.co.jp

Cancel

(留意事項)

※CPE 故障通知サービスは CPE をコントローラから死活監視し、通信不可/復旧の状態の変化を検知した際にお客さまへメール通知するサービスです。通知受領後、お客さまにて速やかに切り分け・故障申告してください。

※通知先メールアドレスは NTT 東日本にて初期設定で最大 10 個設定します。メールアドレスに誤りがないか開通時にお客さま自身でコントローラにアクセスしご確認くださいませようお願いします。

※テストメールは送付されません。通知確認をされたい場合はお客様にて CPE の疑似的な故障発生（CPE の WAN 側ケーブル抜去や再起動等）にてご確認くださいませようお願いします。

※CPE 故障通知サービスでは故障内容により通知しない場合があります。モバイル接続の不具合等におけるコントローラとの通信断時等お客さまがご契約の回線の故障すべて遅滞なく通知することを保証するものではありません。

※CPE 故障通知サービスでお客さまに送られるメール文内の返信用アドレスへは返信することができません。

※CPE 故障通知サービスををご利用にあたって、利用開始希望日までに弊社にてメールアドレス等の設定を実施しますので、利用開始日前にメールが通知される場合があります。

※メールアドレスは最大 10 個まで設定可能です。メールアドレスの変更、追加、削除をご希望の場合は別途設定費用が必要となります。

通知アラームの設定について

NTT 東日本にて設定する通知アラームは以下になります。

No	Severity	Alarm Name	解説
①	Critical	OMP Node Down	該当のCPE とコントローラが通信できなくなったことを示すアラーム
②	Medium	OMP Node Up	該当のCPE とコントローラが通信できるようになったことを示すアラーム

【OMP Node Down】（実際の通知メール）

Subject: [NETWORK EVENT] Critical OMP_Node_Down
Date: Wed, 09 Jun 2021 13:35:19 +0900 (JST)
From: cpe-alarm@sdwan.ntt-east.net
Reply-To: No-Reply@sdwan.ntt-east.net
To: *****@*****
*** This is an automatically generated email, please do not reply ***
An event with following details happened in your network: Severity: Critical
Event: OMP Node Down
Devices: [201.100.7.1]
Hostnames: [swve01000701]
Site id: xxxxxxxxxxxxxx
Message: OMP session for the node are down
Occurred on: Wed Jun 09 13:35:16 JST 2021

※参考：日本語訳

件名： [通信に関する事象] 重要 該当の CPE との通信が切断されました。
日時： 送信日時
送信元アドレス： cpe-alarm@sdwan.ntt-east.net
返信先アドレス： No-Reply@sdwan.ntt-east.net
送信先アドレス： お客さまがご指定のメールアドレス
自動送信アドレスのため、返事しないでください
以下のイベントがあなたのネットワーク上で発生しています：重要度：重大
事象： 該当の CPE との通信が切断されました。
端末： CPE 識別子
CPE ホスト名： CPE に設定される機器の名称（申込書に記載の内容が表示されます）
サイト番号: xxxxxxxxxxxxxx
メッセージ: OMP セッションが切れました

【OMP Site UP】（実際の通知メール）

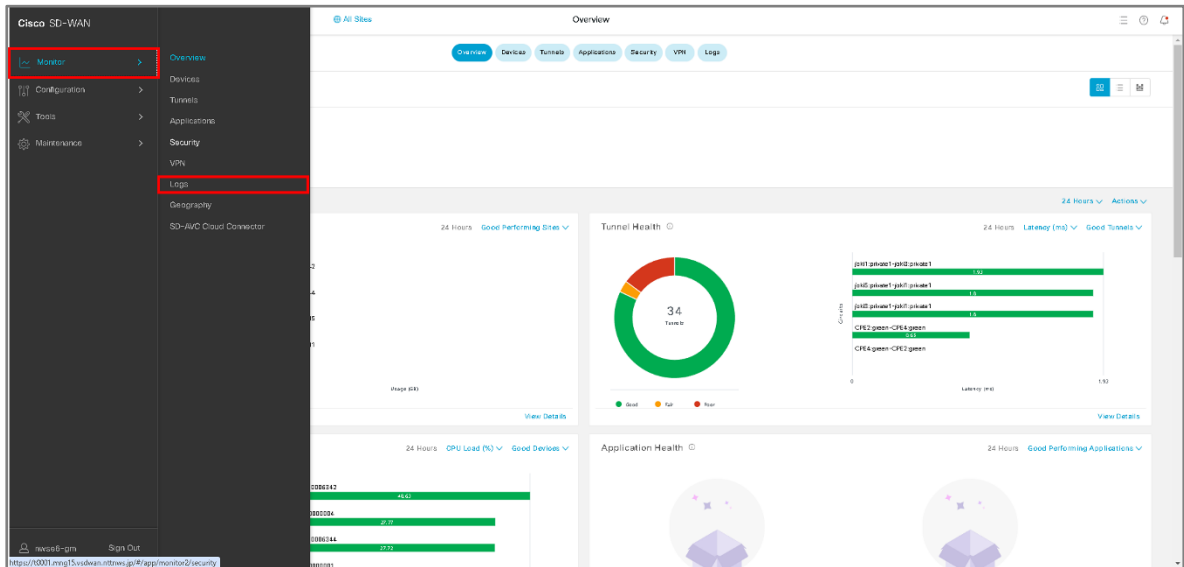
Subject: [NETWORK EVENT] Critical OMP_Node_Up
Date: Wed, 09 Jun 2021 13:35:19 +0900 (JST)
From: cpe-alarm@sdwan.ntt-east.net
Reply-To: No-Reply@sdwan.ntt-east.net
To: *****@*****
*** This is an automatically generated email, please do not reply ***
An event with following details happened in your network: Severity: Medium
Event: OMP Node Up
Devices: [201.100.7.1]
Hostnames: [swve01000701]
Site id: xxxxxxxxxxxxxx
Message: OMP session for the node came up
Occurred on: Wed Jun 09 13:35:16 JST 2021

※日本語訳

件名: [通信に関する事象] 重要 該当の CPE との通信が接続されました。
日時: 送信日
送信元アドレス: cpe-alarm@sdwan.ntt-east.net
返信先アドレス: No-Reply@sdwan.ntt-east.net
送信先アドレス: お客さまがご指定のメールアドレス
****自動送信アドレスのため、返信しないでください****
以下のイベントがあなたのネットワーク上で発生しています: 重要度: 普通
事象: 該当の CPE との通信が接続されました。
端末: CPE 識別子

5.5.2. 検知したアラームログの確認方法

1. 左ペイン(左の領域)の「Monitor」>「Logs」を選択

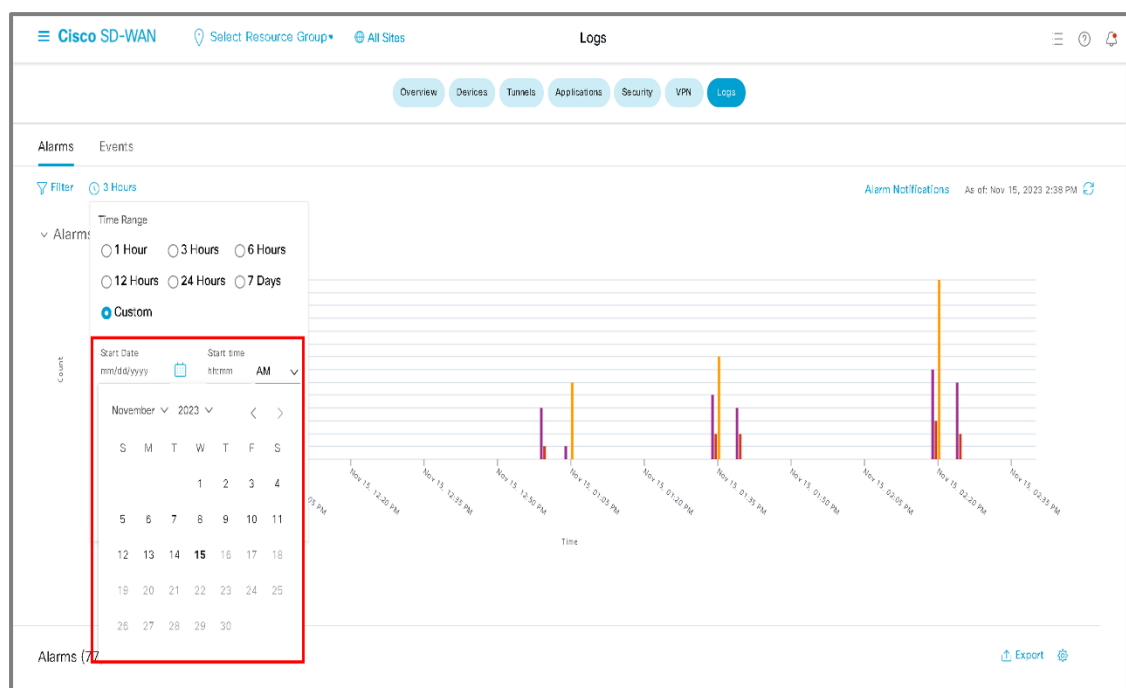


2. 必要に応じて、確認したい期間を指定したい場合

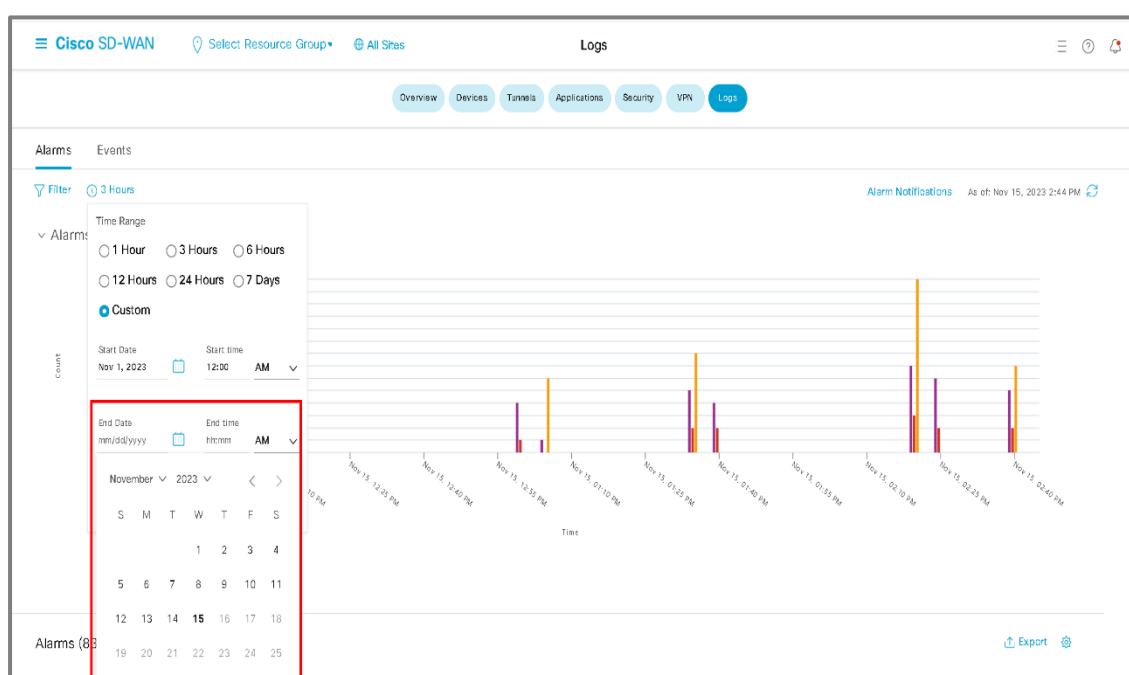
画面左上にて「3hours」⇒「Custom」を選択



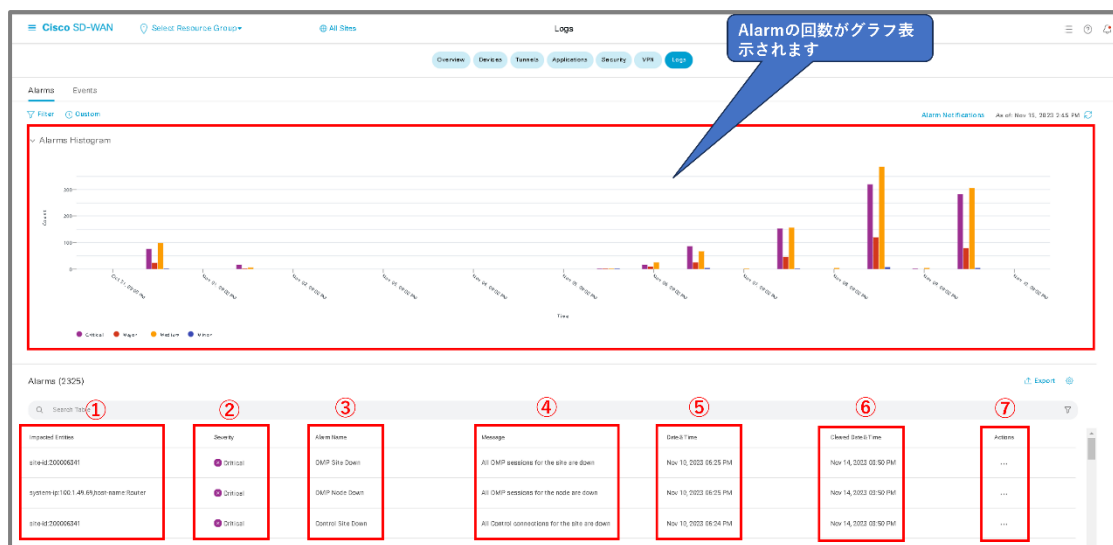
3. [Start date time]で確認したい期間の開始の日付、時刻を指定



4. [End date time]で確認したい期間の終わりの日付、時刻を指定



5.発生アラームを確認することができます。



項番	項目名	解説
1	Impacted Entities	アラームが発生した装置やインタフェースの情報が表示されます。表示内容はアラーム種別により異なります。
2	Severity	重要度が表示されます。
3	Alarm Name	発生したアラームの種別が表示されます。
4	Message	発生したアラームの説明が表示されます
5	Date & Time	アラームの発生時刻が表示されます。
6	Cleared Date & Time	そのアラームの事象が解消された時刻が表示されます。(表示の有無はアラームによります)
7	Actions	Action が表示されます。

6

禁止事項

本章では、Managed SD-WAN サービスの禁止事項を解説します。

6.1. NTT 東日本デフォルト提供のテンプレート/パラメータに関わる禁止事項

- 開通時に NTT 東日本よりデフォルトの Device Template/Feature Template/Policy が提供されますが、削除や設定変更を行うと正常に通信できなくなる恐れがあるため、絶対に行わないようご注意ください
- Device Template/Feature Template/Policy の設定変更をする場合はデフォルト提供のテンプレートをコピーし、コピーしたテンプレート上で設定変更を行うようお願いいたします(3.3 章/3.4 章を参照してください)
- CPE のパラメータの中には NTT 東日本デフォルトの値から変更すると正常な通信ができなくなるパラメータがございます、**Color/Device group/System IP, Site ID の設定は絶対に変更しないようご注意ください**

6.2. NTT西日本エリアにCPEがある/モバイル接続サービス/セキュアインターネット接続サービス/無線LAN おまかせサービス接続 OP/クラウドゲートウェイクロスコネクト利用時の禁止事項

- NTT 西日本エリアに CPE がある場合、もしくはモバイル接続サービス/セキュアインターネット接続サービス/無線LAN おまかせサービス接続 OP/クラウドゲートウェイクロスコネクト利用時は「swvexxxxxxxx」というホスト名の装置がデフォルトで存在しますが、この装置の設定変更を行うと正常な通信ができなくなる恐れがありますので、絶対に設定変更しないようご注意ください
- トンネリングプロトコルの変更/VPN グループの追加に関わる設定変更を行うと正常な通信ができなくなる恐れがありますので、絶対に上記設定変更しないようご注意ください

The screenshot shows the Cisco SD-WAN 'Devices' page. A table lists 12 devices. Two devices are highlighted with a red box:

Hostname	Device Model	Site ID	System IP	Health	Reachability	vSmart Control	BFD	Up time	CPU Load	Memory Utilization	Action
swve15000112	C8000v	120150001	215.110.1.2	▲	↑	6 / 6	4 / 6	Oct 25, 2023 11:00 AM	4.88%	79%	...
swve15000111	C8000v	110150001	215.110.1.1	▲	↑	6 / 6	4 / 6	Oct 25, 2023 10:33 AM	4.96%	79%	...

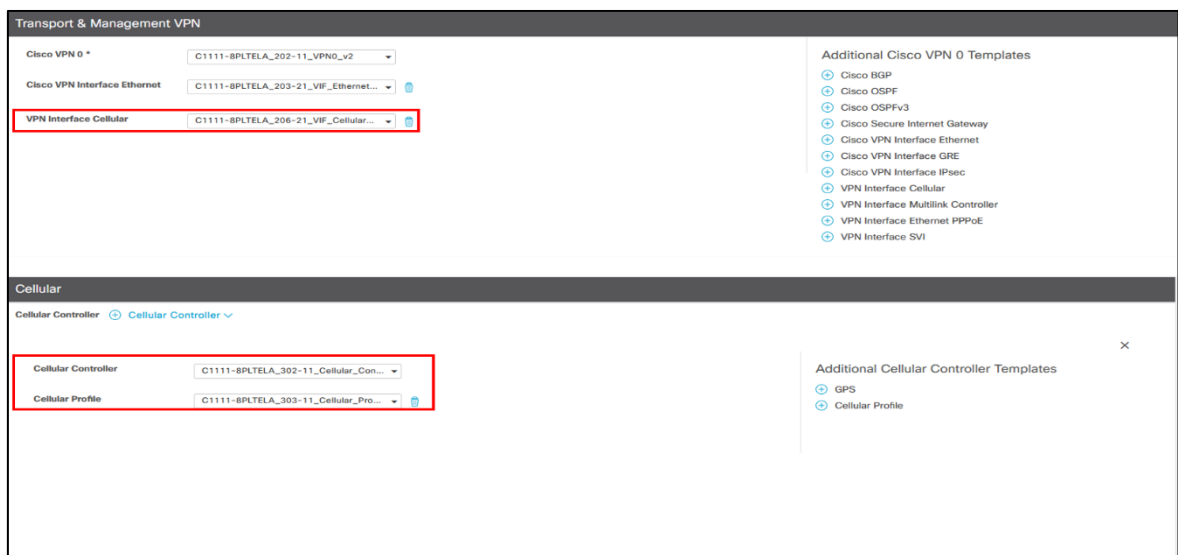
設定変更不可装置

- vCPE には 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 のルーティングが設定されます。プライベートアドレスへの通信のために CPE ヘデフォルトルート(0.0.0.0/0)等を設定するとプライベートアドレス向け通信はロングストマッチで vCPE 側にルーティングされて想定通りの通信ができないため、集約ルートを設定したい場合は 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 より長いサブネットマスク(例: 10.0.0.0/9、10.128.0.0/9 等)でのルーティング設定が必要です。

6.3. モバイル接続サービス利用時の禁止事項

- モバイル接続サービス利用時は、「C1111-8PLTELA_206-11_VIF_Cellular_***」、「C1111-8PLTELA_302-11_Cellular_Controller」、「C1111-8PLTELA_303-11_Cellular_Profile」の3種類の Feature Template が提供されますので、この3種類の Feature Template の設定変更及び Device Template から外さないでください。

※正常な通信ができなくなる恐れがあります。



The screenshot displays the configuration interface for Managed SD-WAN, divided into two main sections: "Transport & Management VPN" and "Cellular".

Transport & Management VPN Section:

- Cisco VPN 0 *:** A dropdown menu showing "C1111-8PLTELA_202-11_VPN0_v2".
- Cisco VPN Interface Ethernet:** A dropdown menu showing "C1111-8PLTELA_203-21_VIF_Ethernet...".
- VPN Interface Cellular:** A dropdown menu showing "C1111-8PLTELA_206-21_VIF_Cellular..." (highlighted with a red box).
- Additional Cisco VPN 0 Templates:** A list of templates including Cisco BGP, Cisco OSPF, Cisco OSPFv3, Cisco Secure Internet Gateway, Cisco VPN Interface Ethernet, Cisco VPN Interface GRE, Cisco VPN Interface IPsec, VPN Interface Cellular, VPN Interface Multilink Controller, VPN Interface Ethernet PPPoE, and VPN Interface SVI.

Cellular Section:

- Cellular Controller:** A dropdown menu showing "C1111-8PLTELA_302-11_Cellular_Con..." (highlighted with a red box).
- Cellular Profile:** A dropdown menu showing "C1111-8PLTELA_303-11_Cellular_Pro..." (highlighted with a red box).
- Additional Cellular Controller Templates:** A list of templates including GPS and Cellular Profile.

6.4. SSH Terminal 利用のための ID/PW 変更時の禁止事項

- 5.4.4 章の「(参考) CPE ログインパスワードの変更」で実施する ID/PW 変更時に行う Cisco AAA 編集時は絶対に Username「admin」の編集はしないでください。

NTT 東日本によるサポート対応ができなくなります。もし、変更された場合はお客様にてお申込時の状態に戻していただきます。

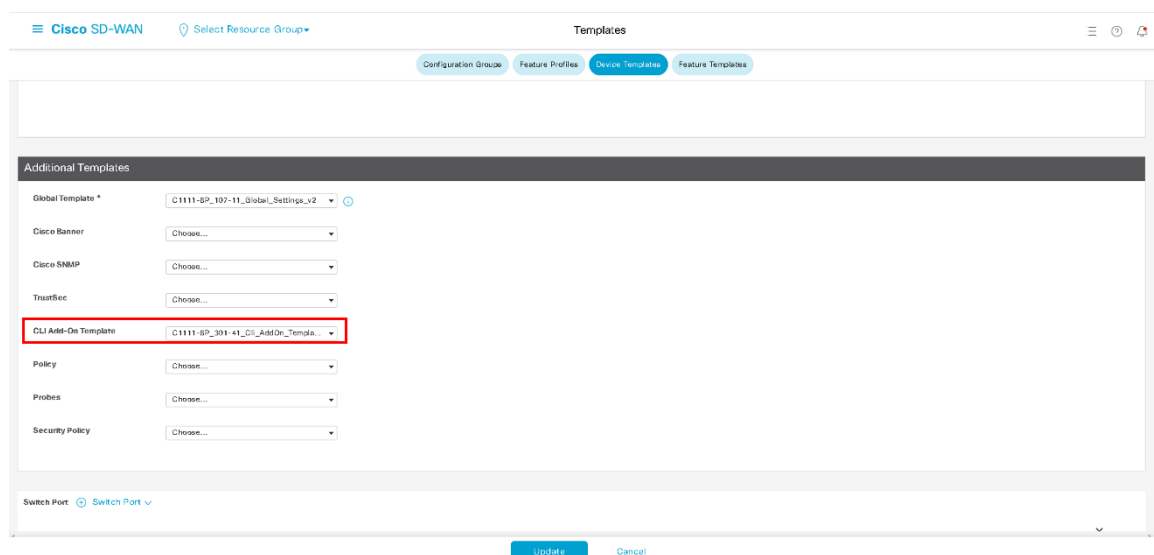
The screenshot shows the Cisco SD-WAN configuration interface. The breadcrumb trail is: Feature Template > Cisco AAA > C1111-SP_101-11_AAA_v2. The page title is 'Templates'. The navigation tabs are: Configuration Groups, Feature Profiles, Device Templates, and Feature Templates (selected). The left sidebar shows the configuration tree: LOCAL, RADIUS, TACACS, ACCOUNTING, AUTHORIZATION, 802.1X, and Authentication and Authorization Order. The 'LOCAL' section is expanded, showing a 'New User' button and a table of users. The table has columns: Optional, Username, Password, Privilege, Pubkey Chain, and Action. The 'admin' user is highlighted with a red box.

Optional	Username	Password	Privilege	Pubkey Chain	Action
<input type="checkbox"/>	admin	•••••	15		Edit
<input type="checkbox"/>	user	•••••	15		Edit Delete

6.5. Device Template の禁止事項

- Device テンプレートから「Cli Add-On Template」の設定は削除しないでください。必ず「Cli Add-On Template」が入っていることを確認願います。

※正常な通信ができなくなり、CPE 交換が必要となる可能性があります。



The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' tab selected. Under the 'Additional Templates' section, the 'CLI Add-On Template' is highlighted with a red box. The value for this template is 'C1111-SP-991-41_CLI_AddOn_Template...'. Other templates listed include Global Template, Cisco Banner, Cisco SNMP, TrustSec, Policy, Probes, and Security Policy, each with a 'Choose...' button.

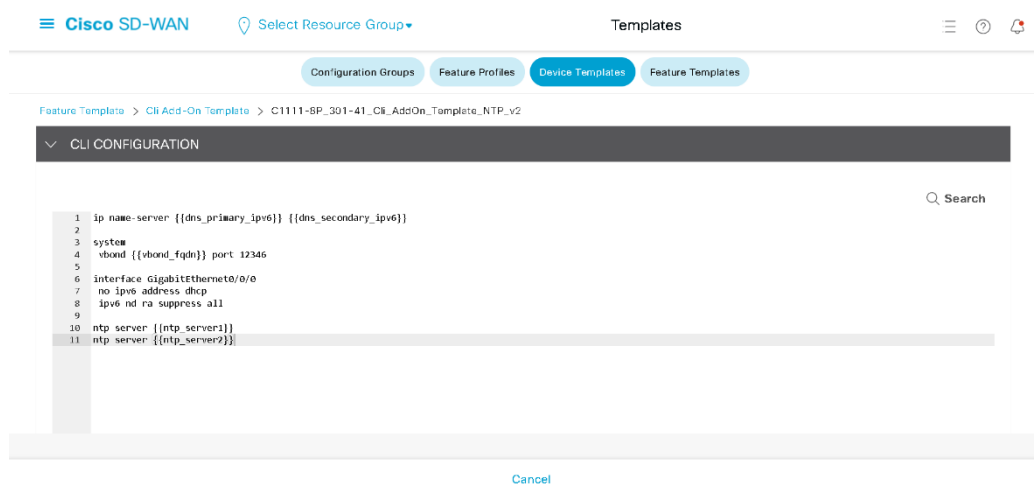
6.6. Cli Add-On Template の禁止事項

- Feature テンプレート「Cli Add-On Template」の以下の設定は変更・削除しないでください。また、設定前に以下の設定が必ず入っていることを確認願います。

※正常な通信ができなくなり、CPE 交換が必要となる可能性があります。

※別の設定行の追記は可能です

```
system
vbond {{vbond_fqdn}} port 12346
no ipv6 address dhcp
ipv6 nd ra suppress all
```



6.7. Device Template の禁止事項

- Feature テンプレート「Cisco VPN Interface Ethernet」の IPv6 の「Dynamic」設定は「Static」にしないでください。必ず「Dynamic」になっていることを確認願います。

※正常な通信ができなくなり、CPE 交換が必要となる可能性があります。

The screenshot shows the Cisco SD-WAN configuration interface. The breadcrumb navigation is: Feature Template > Cisco VPN Interface Ethernet > C1111-SP_203-12_VF_Ethernet_IPSec_NTP_v2. The 'Device Type' is C1111-SP. The 'Template Name' and 'Description' are both C1111-SP_203-12_VF_Ethernet_IPSec_NTP_v2. The 'Basic Configuration' tab is active, showing the 'BASIC CONFIGURATION' section. Under 'Shutdown', the 'No' radio button is selected. The 'Interface Name' is GigabitEthernet0/0/0. The 'Description' field is empty. At the bottom, the 'IPv6' tab is selected, and the 'Dynamic' radio button is selected, which is highlighted with a red box. The 'Static' radio button is also visible.

6.8. CPE 初期化に関する禁止事項

- テンプレートの設定により通信に異常が発生した場合、故障受付窓口に申告をいただくことで開通時の設定に戻すことが可能ですので、ユーザでの CPE 初期化の実施はしないでください。
※CPE が unreachable 状態の場合、CPE 交換となります

7

困ったときは?

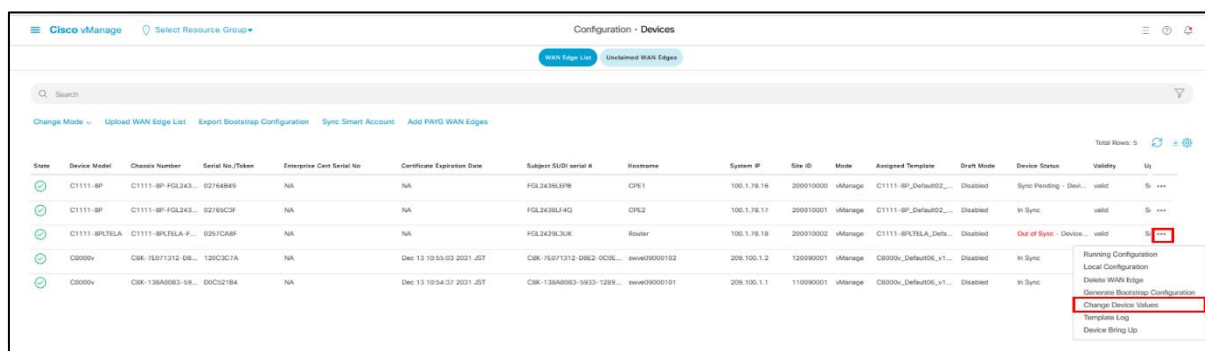
本章では、トラブル時の対処方法について解説します。

7.1. 「Out of Sync」状態の解消方法

開通時などに Device status が Out of Sync になる場合がありますので、

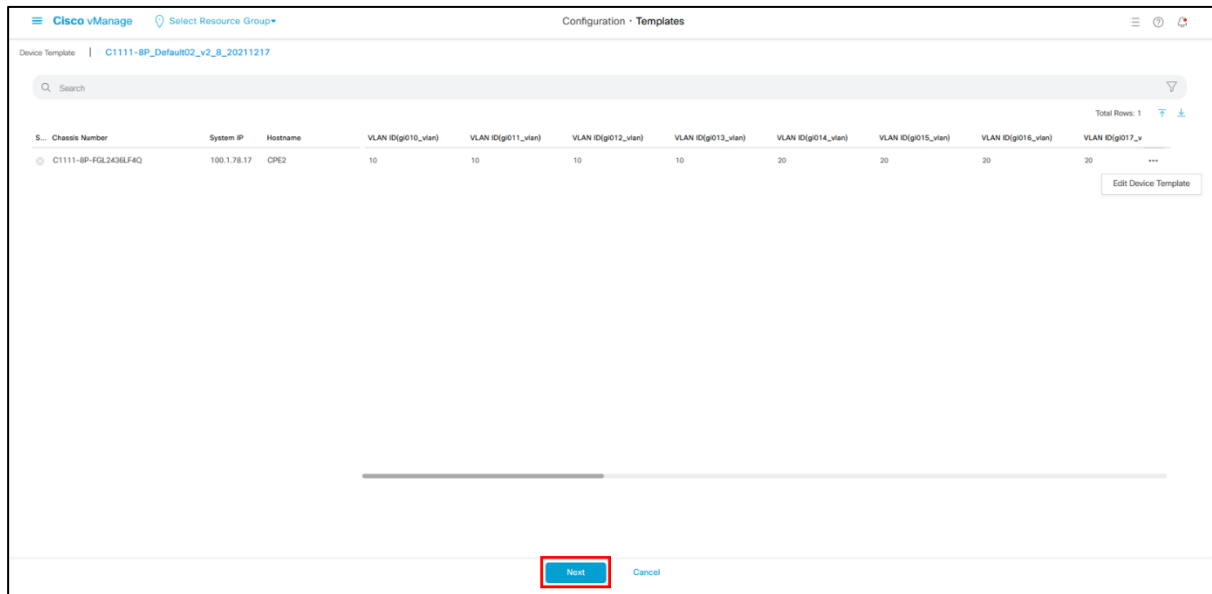
Out of Sync の解消方法を紹介します

1. 左ペイン(左の領域)の Configuration から「Device」を選択
Out of Sync となっている CPE の「…」から「Change device value」を選択

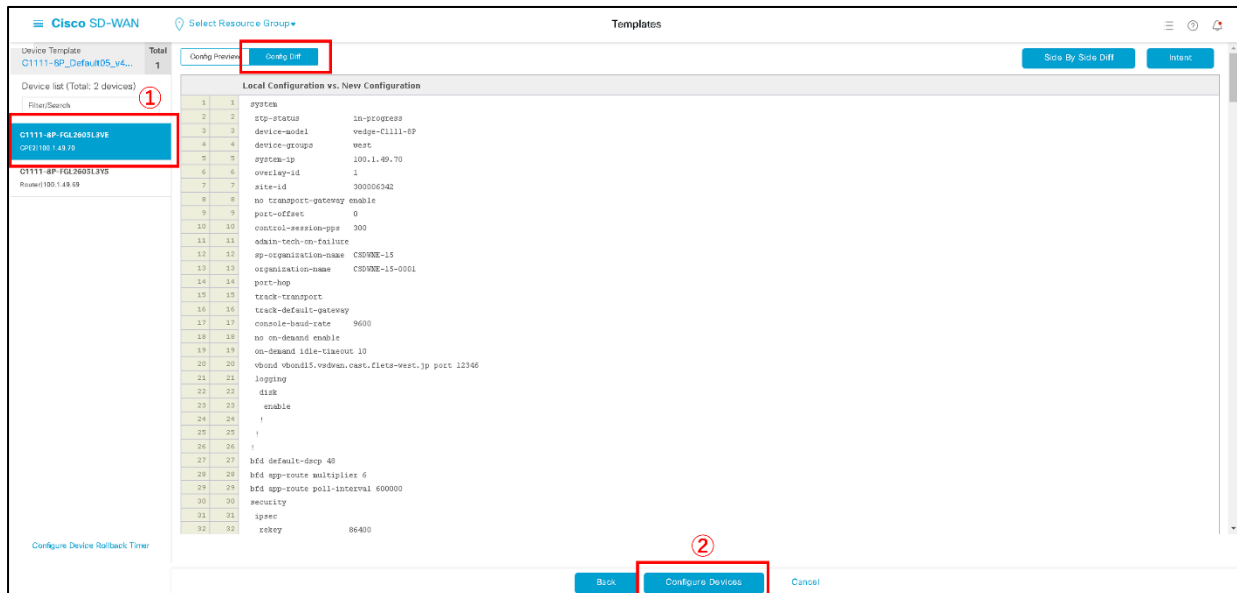


State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No.	Certificate Expiration Date	Subject SUDI serial #	Role/Name	System IP	Site ID	Mode	Assigned Template	Drift Mode	Device Status	Validity	UI
✓	CT1111-SP	CT1111-SP-FGL243...	02764849	NA	NA	FGL243SLF4Q	CPE1	100.1.78.16	200010000	Manage	CT1111-SP_Default02...	Disabled	Sync Pending - Dev...	valid	Si ...
✓	CT1111-SP	CT1111-SP-FGL243...	02769C3F	NA	NA	FGL243SLF4Q	CPE2	100.1.78.17	200010001	Manage	CT1111-SP_Default02...	Disabled	In Sync	valid	Si ...
✓	CT1111-SP/TELA	CT1111-SP/TELA F...	0257C8F8	NA	NA	FGL243SLF4Q	Router	100.1.78.18	200010002	Manage	CT1111-SP/TELA_Delta...	Disabled	Out of Sync - Device...	valid	Si ...
✓	CB000v	CBK-75271212 DB...	120C3C7A	NA	Dec 13 10:55:03 2031 JST	CBK-75271212 DB2 - CDR...	www09000102	208.100.1.2	120990001	Manage	CB000v_Default00_v1...	Disabled	In Sync		
✓	CB000v	CBK-138A8083-59...	D0C321E4	NA	Dec 13 10:54:27 2031 JST	CBK-138A8083-5953-1289...	www09000101	208.100.1.1	110990001	Manage	CB000v_Default00_v1...	Disabled	In Sync		

2. 「Next」を選択



3. 以下の画面で CPE を選択し、コンフィグを出力 「Configure Devices」を選択



4. Status が success, Message が Done となっていればコンフィグ適用が完了

⇒ 「Out of Sync」 が解消されたことを確認

Cisco SD-WAN
Select Resource Group

Push Feature Template Configuration
Validation Success
Initiated By: nusse6-gm | Tenant: CSDWNE-15-0001 | From: 172.18.128.190

Total Task: 1 | Success: 1

Search

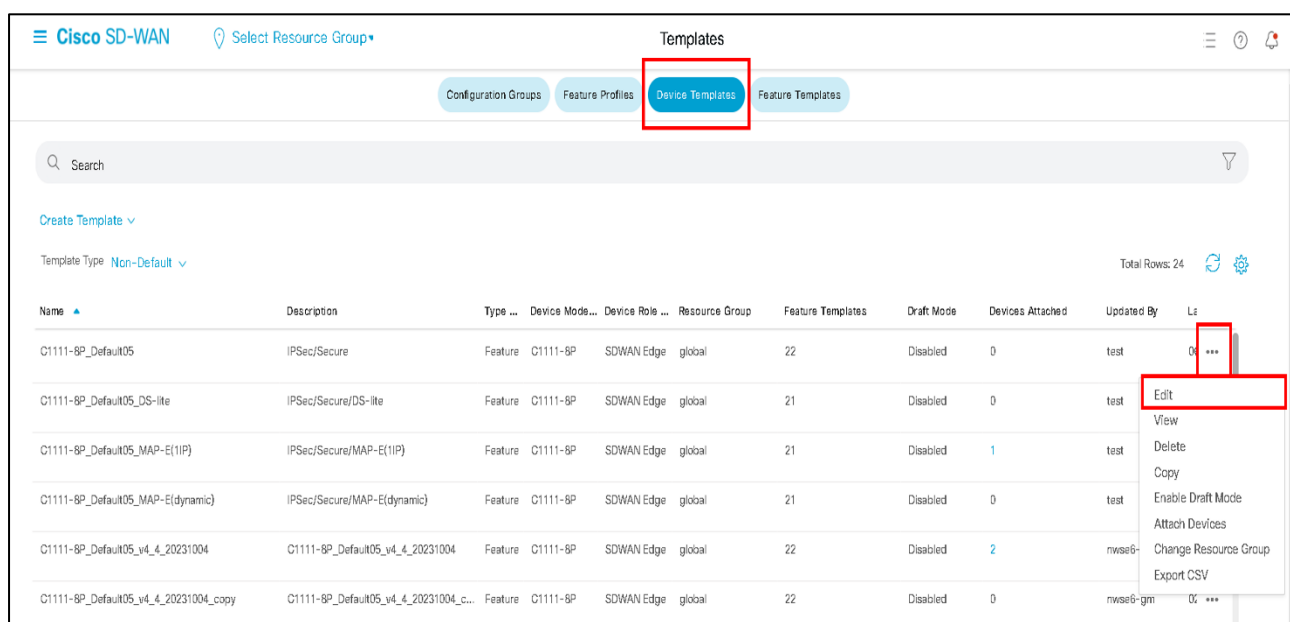
Total Rows: 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template C...	C1111-8P-FGL2605L3NE	C1111-8P	CPE2	100.148.70	300006342	215.255.1.2

7.2. テンプレートアタッチ時に DNS アドレスが Invalid となる事象の解消方法

DNS_Address が Invalid となりデバイステンプレートをアタッチできない事象が発生する場合の解消方法を紹介します

1. 左ペイン(左の領域)の Configuration から「Templates」を選択
画面上部のタブから「Feature」を選択
「C11111-8P_202-11_VPN0」の右の...から Edit を選択

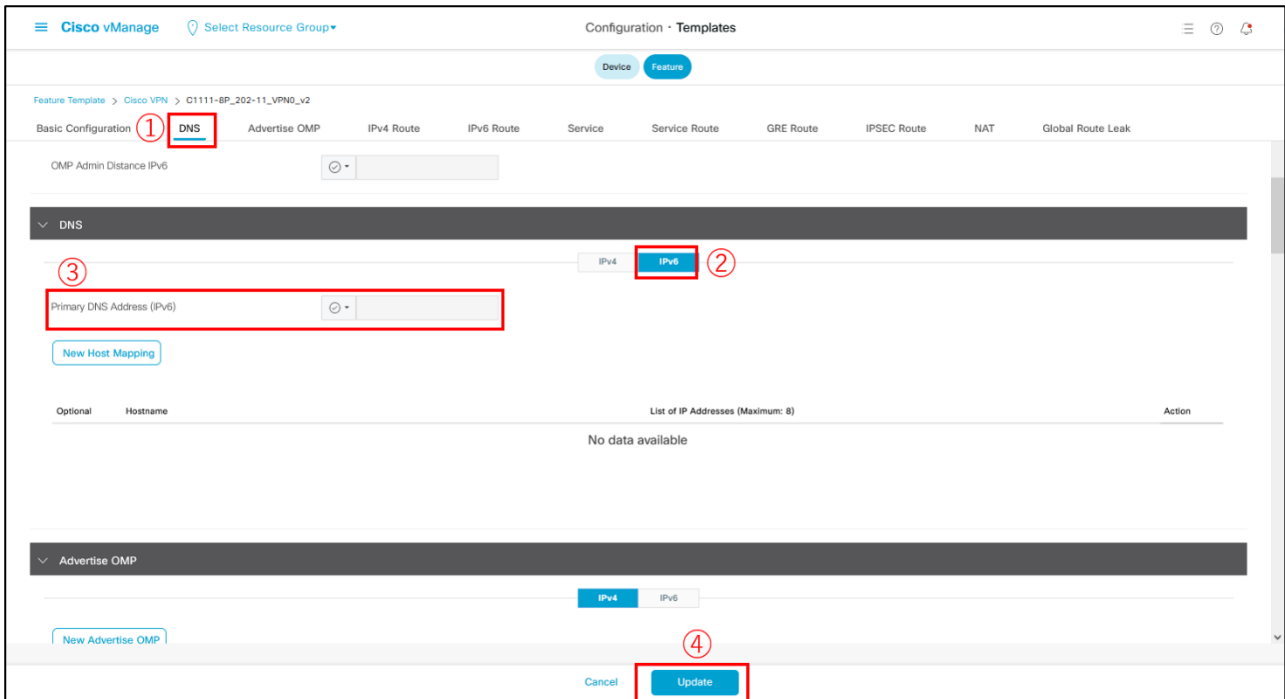


The screenshot shows the Cisco SD-WAN interface with the 'Templates' section active. The 'Device Templates' tab is selected. A table displays the following data:

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Modified	Actions
C1111-8P_Default05	IPSec/Secure	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	test	0%	...
C1111-8P_Default05_DS-lite	IPSec/Secure/DS-lite	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test		...
C1111-8P_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	1	test		...
C1111-8P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test		...
C1111-8P_Default05_v4_4_20231004	C1111-8P_Default05_v4_4_20231004	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	2	nwsa6-		...
C1111-8P_Default05_v4_4_20231004_copy	C1111-8P_Default05_v4_4_20231004_c...	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	nwsa6-gm	0%	...

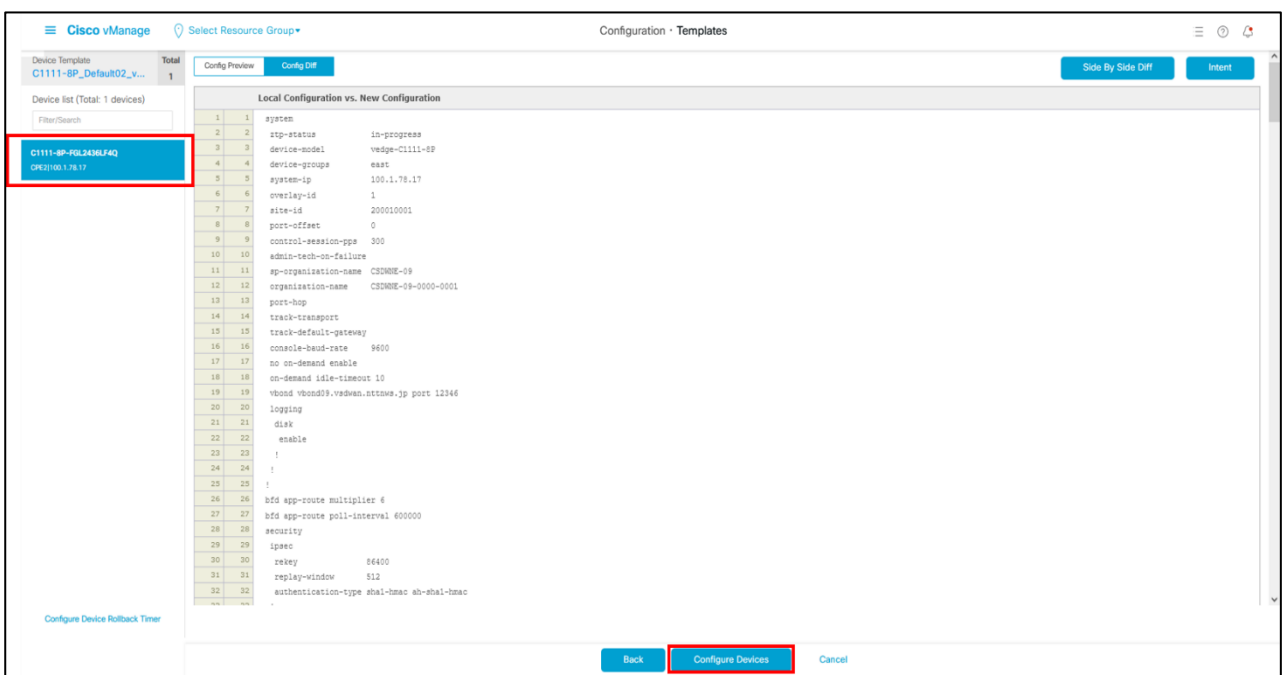
The context menu for the first row shows the following options: Edit, View, Delete, Copy, Enable Draft Mode, Attach Devices, Change Resource Group, and Export CSV.

2. ①DNS タブを選択
- ②IPv6 タブを選択
- ③Primary DNS Address(IPv6)の箇所のルータマークのアイコンをクリックし、Default を選択
- ⇒Secondary DNS Address が消えたことを確認
- ④Update を選択



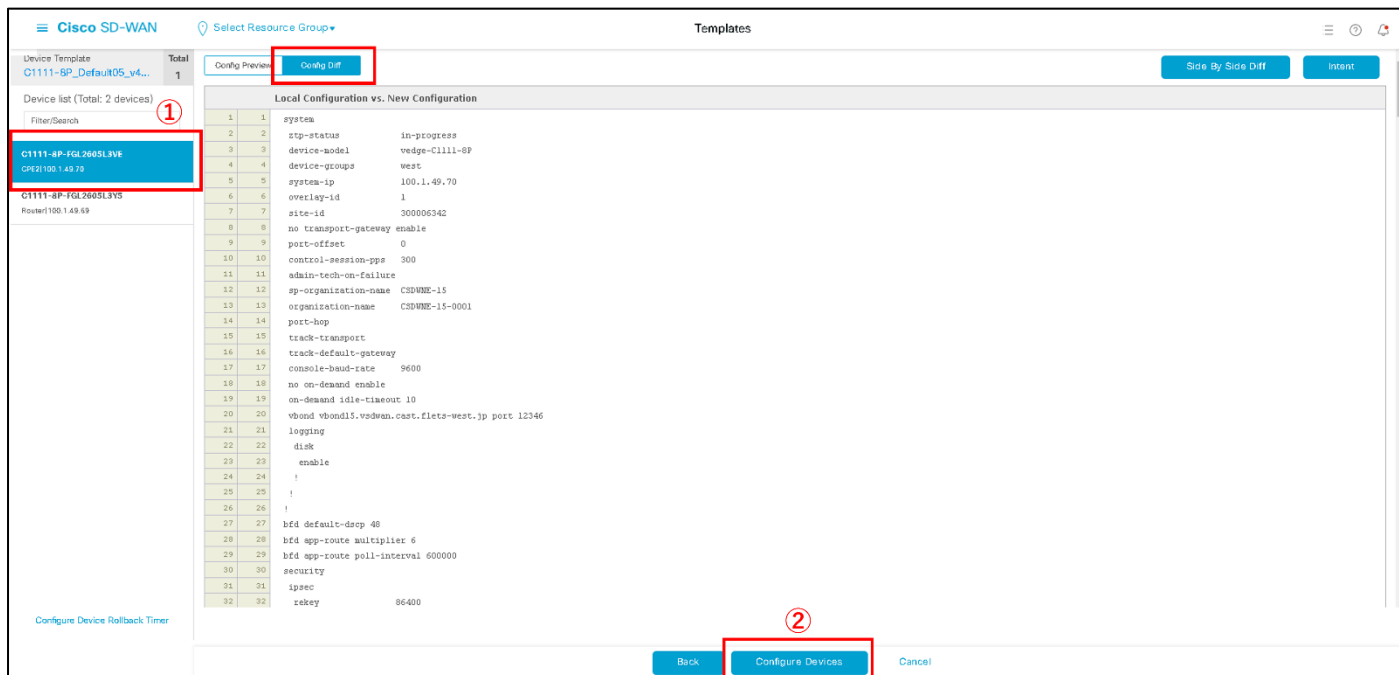
The screenshot shows the Cisco vManage Configuration - Templates page. The 'DNS' tab is selected (①). Under the 'DNS' section, the 'IPv6' tab is selected (②). The 'Primary DNS Address (IPv6)' field is highlighted with a red box (③). At the bottom, the 'Update' button is highlighted with a red box (④).

3. 以下の画面に遷移するので、「Next」を選択



The screenshot shows the Cisco vManage Configuration - Templates page. The 'Configure Devices' button is highlighted with a red box. The 'Device List' on the left shows the selected device template 'C1111-8P-FGL3436/F4Q'.

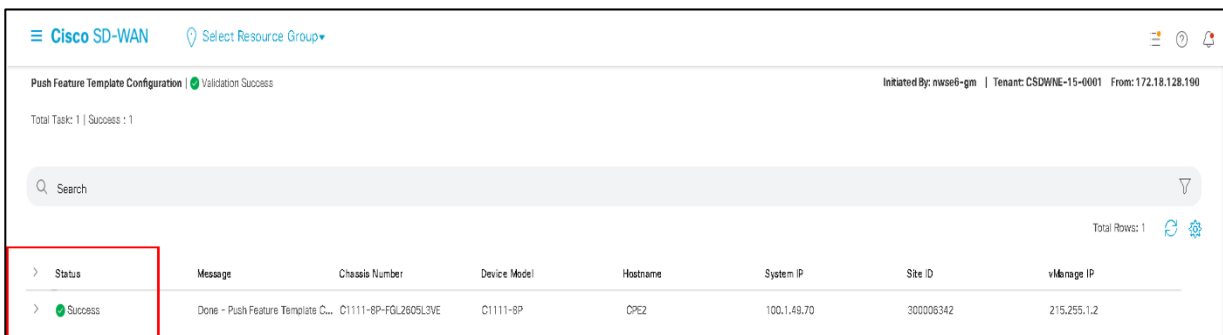
4. 「Configure Devices」を選択



The screenshot shows the Cisco SD-WAN configuration interface. On the left, a list of device templates is shown, with 'C1111-8P-FGL2605L3VE' highlighted. In the center, a table displays the 'Local Configuration vs. New Configuration' for the selected device. At the bottom, the 'Configure Devices' button is highlighted with a red box and a circled '2'.

Line	Config	Value
1	system	
2	stp-status	in-progress
3	device-model	vedge-C1111-8P
4	device-groups	west
5	system-ip	100.1.49.70
6	overlay-id	1
7	site-id	300006342
8	no transport-gateway	enable
9	port-offset	0
10	control-session-pps	300
11	admin-tech-on-failure	
12	sp-organization-name	CSDWNE-15
13	organization-name	CSDWNE-15-0001
14	port-hop	
15	track-transport	
16	track-default-gateway	
17	console-band-rate	9600
18	no on-demand	enable
19	on-demand idle-timeout	10
20	vbond vbond15.vodwan.cast.flets-west.jp port	12346
21	logging	
22	disk	
23	enable	
24	!	
25	!	
26	!	
27	bfd default-dscp	40
28	bfd app-route multiplier	6
29	bfd app-route poll-interval	600000
30	security	
31	ipsec	
32	rekey	86400

5. Status が success, Message が Done となっていればコンフィグ適用が完了
⇒以降テンプレートアタッチ時にエラーが発生しなくなります



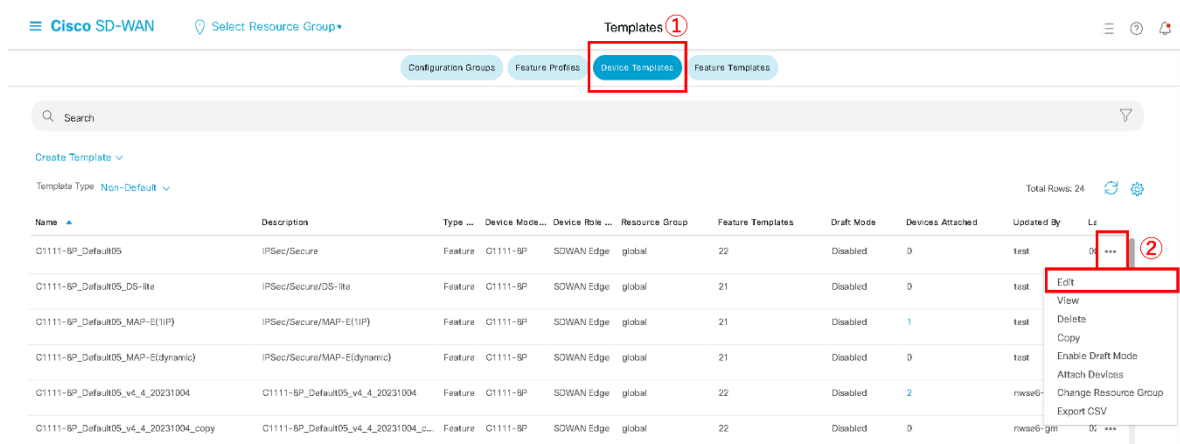
The screenshot shows the 'Push Feature Template Configuration' status page. The status is 'Success' and the message is 'Done - Push Feature Template C...'. The table below shows the configuration details for the device.

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template C...	C1111-8P-FGL2605L3VE	C1111-8P	CPE2	100.1.49.70	300006342	215.255.1.2

7.3. SSH 接続時のログイン ID/パスワード不明時の対応

SSH 接続時のログイン ID/パスワード不明時の対応は、CPE ログインパスワードを出時に戻していただきたいため、対象の CPE のみ AAA 設定を出荷時に戻す方法について紹介します

- ① 左ペイン(左の領域)の Configuration から「Templates」を選択し、画面上部のタブから「Device Templates」を選択
- ② 対象の CPE に適用している Template の「…」から「Edit」を選択



The screenshot shows the Cisco SD-WAN configuration interface. The 'Templates' tab is selected, and the 'Device Templates' sub-tab is active. A table lists several templates. The first template, 'C1111-SP_Default05', is highlighted. A dropdown menu is open for this template, showing the 'Edit' option, which is circled in red and labeled with a red '2'.

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	...
C1111-SP_Default05	IPSec/Secure	Feature	C1111-SP	SDWAN Edge	global	22	Disabled	0	test	...
C1111-SP_Default05_DS-Ita	IPSec/Secure/DS-Ita	Feature	C1111-SP	SDWAN Edge	global	21	Disabled	0	test	...
C1111-SP_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-SP	SDWAN Edge	global	21	Disabled	1	test	...
C1111-SP_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-SP	SDWAN Edge	global	21	Disabled	0	test	...
C1111-SP_Default05_v4_4_20231004	C1111-SP_Default05_v4_4_20231004	Feature	C1111-SP	SDWAN Edge	global	22	Disabled	2	mxwse6-	...
C1111-SP_Default05_v4_4_20231004_copy	C1111-SP_Default05_v4_4_20231004_copy	Feature	C1111-SP	SDWAN Edge	global	22	Disabled	0	mxwse6-gm	...

①Basic Information 欄の Cisco AAA をデフォルト「C1111-8P_101-11_AAA_v2」へ変更

②「Update」を選択

The screenshot shows the 'Cisco SD-WAN' interface with the 'Templates' section. Under the 'Basic Information' tab, the 'Cisco AAA' dropdown menu is set to 'C1111-8P_101-11_AAA_v2'. The 'Update' button at the bottom right of the form is highlighted with a red box and a circled '2'.

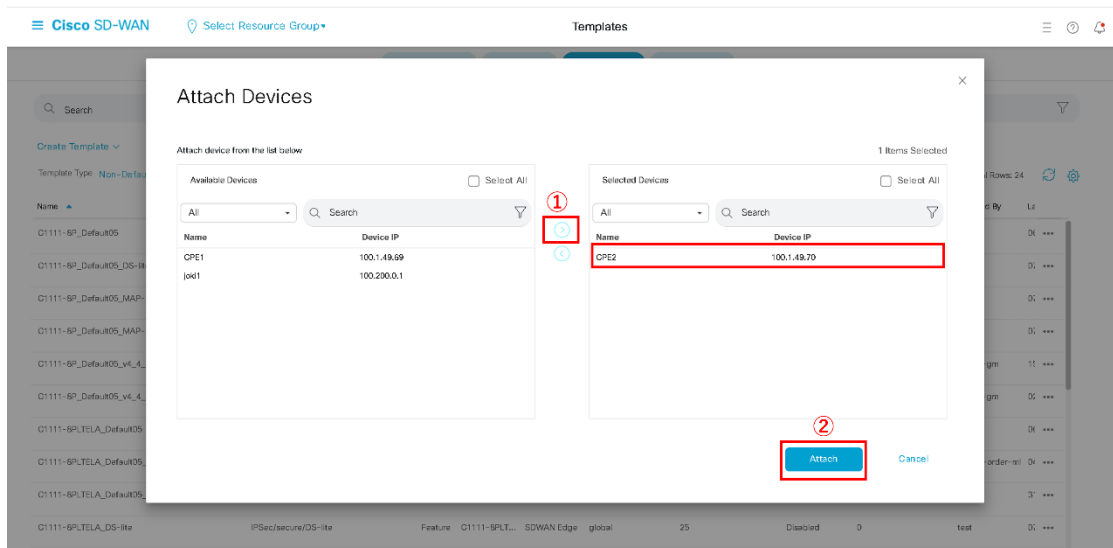
1. デフォルトテンプレートの「…」から「Attach Devices」を選択

The screenshot shows a list of templates. The first template, 'C1111-8P_Default05', has a context menu open with the 'Attach Devices' option highlighted. The table below lists the templates:

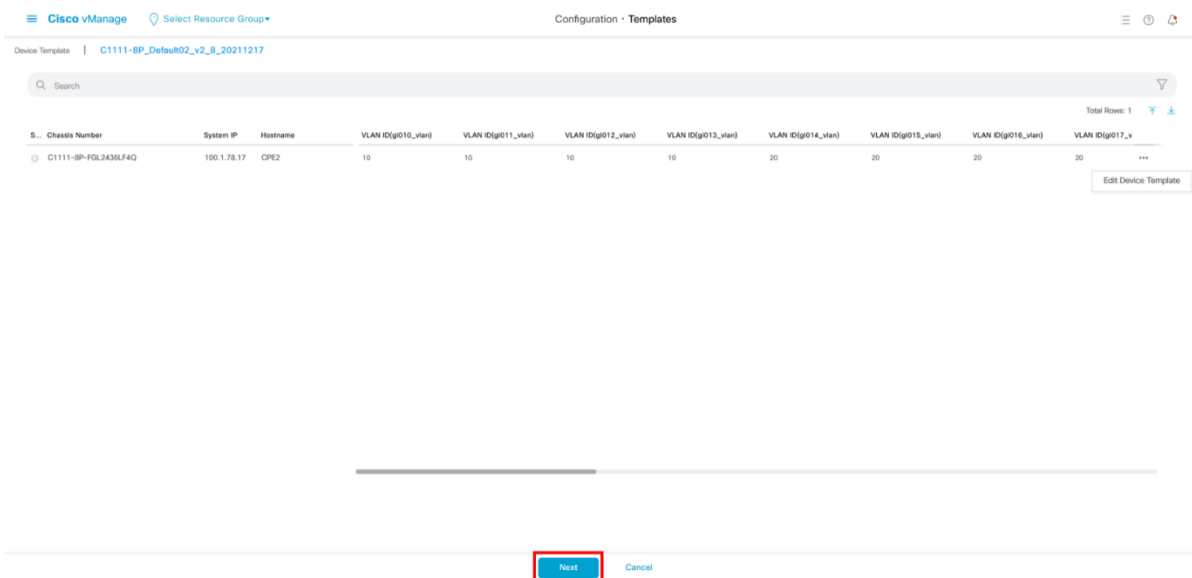
Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Li
C1111-8P_Default05	IPSec/Secure	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	test	OK
C1111-8P_Default05_DS-lite	IPSec/Secure/DS-lite	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test	
C1111-8P_Default05_MAP-E(1IP)	IPSec/Secure/MAP-E(1IP)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	1	test	
C1111-8P_Default05_MAP-E(dynamic)	IPSec/Secure/MAP-E(dynamic)	Feature	C1111-8P	SDWAN Edge	global	21	Disabled	0	test	
C1111-8P_Default05_v4_4_20231004	C1111-8P_Default05_v4_4_20231004	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	2	mwae6-	
C1111-8P_Default05_v4_4_20231004_copy	C1111-8P_Default05_v4_4_20231004_c...	Feature	C1111-8P	SDWAN Edge	global	22	Disabled	0	mwae6-jm	OK

4. ①適用したい CPE を選択し,「→」を選択し右ボックスに移動

②「Attach」を選択



5. 「Next」を選択



6. ①以下の画面で CPE を選択しコンフィグを出力(Config Diff を選択すると差分表示が可能)

②内容を確認し、「Configure Devices」を選択

※エラーがでる場合、設定が誤っている可能性があります。エラー内容及び手順を確認します。

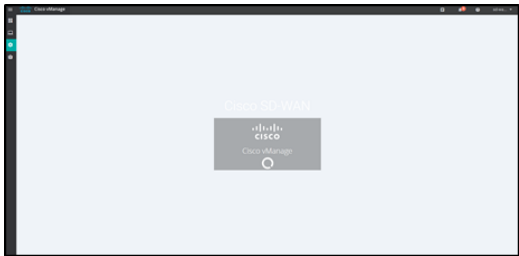
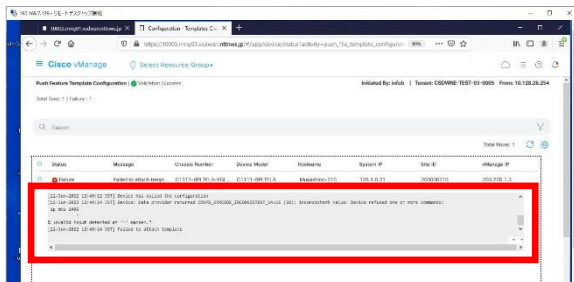
7. Status が success, Message が Done となっていればコンフィグ適用が完了⇒Status 変更まで 1 分程度かかります

※Status が success とならない場合、エラー内容及び手順を確認し時間をおいてリトライの実施をお願いします

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template C...	C1111-8P-FGL2605L3VE	C1111-8P	CPE2	100.1.49.70	300006342	215.255.1.2

7.4. FAQ

その他の困りごとについては下記の FAQ を参考ください

困りごと	対処方法
設定を誤ってしまい、元に戻したい	バックアップからの復元を願います。
設定を誤ってしまい、コントローラ上で CPE が Unreachable になってしまった	重要説明事項に記載してある Managed SD-WAN 故障受付へ連絡願います。
通信速度が遅い	端末などに最適な MTU 値が設定されているか確認願います
CPE が正常に起動しない	電源ボタンを押しなおして CPE の再起動を実施してください。それでも CPE が正常に起動しない場合は Managed SD-WAN 故障受付へご連絡願います。
コントローラが以下のような画面になり固まった	ブラウザを更新して、コントローラへ再ログインを願います
	
<p>コントローラが以下のような画面になり、MTU の値により、テンプレートのアタッチに失敗のメッセージが出力された</p> 	<p>本マニュアルの「3.6 インターネットブレイクアウト 全てのインターネット通信を対象」の手順 7 を参照し、interface Dialer100 の MTU 値を確認し「ip mtu 1454」に設定してください。</p>

参考資料

テンプレートに設定するパラメーター一覧表

【VPN/VLAN】

Feature Template		VPN グループ数			
		1	2	3	4
Cisco VPN	VPN	10	20	30	40
VPN Interface SVI	Vlan	10	20	30	40

【MTU/MSS 値】

Feature Template		GRE		IPsec	
		タイプ I	タイプ II	タイプ I	タイプ II
VPN Interface SVI	MTU 値	1500byte	1500byte	1500byte	1500byte
	MSS 値	1412byte	1360byte	1378byte	1326byte
VPN Interface Ethernet PPPoE	MTU 値	1454byte	1454byte	1454byte	1454byte
	MSS 値	1414byte	1414byte	1414byte	1414byte

CPE 下部端末の最適な MTU 値について

CPE 下部に設置する端末の最適な MTU 値は以下となります

最適な MTU 値を設定しないと CPE でフラグメントが発生しスループット低下の要因となるため、最適な MTU 値を CPE 下部装置へ設定願います。

トンネリング プロトコル	グループ内にモバイル接続サービスを利用している CPE がある場合	グループ内にモバイル接続サービスを利用している CPE がない場合
GRE	1400byte	1452byte
IPsec	1366byte	1418byte