

Ask the Experts

ユースケースの概要と計画：自動化された
セキュアな WAN
(Use Case Overview Planning for Secure Automated WAN)



Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

セッションの対象者



- SD-WAN ソリューションの導入について学習したい
- ユースケース「自動化されたセキュアな WAN」の概要を知りたい

Today's Discussion

01

SD-WANアーキテクチャの概要

02

自動化されたセキュアなWANの概要と計画

03

デモ

Cisco SD-WAN から Cisco Catalyst SD-WAN に 名称の変更

旧名称	新名称
Cisco SD-WAN	Cisco Catalyst SD-WAN
Cisco vManage	Cisco Catalyst SD-WAN Manager
Cisco vBond	Cisco Catalyst SD-WAN Validator
Cisco vSmart	Cisco Catalyst SD-WAN Controller
Cisco vAnalytics	Cisco Catalyst SD-WAN Analytics

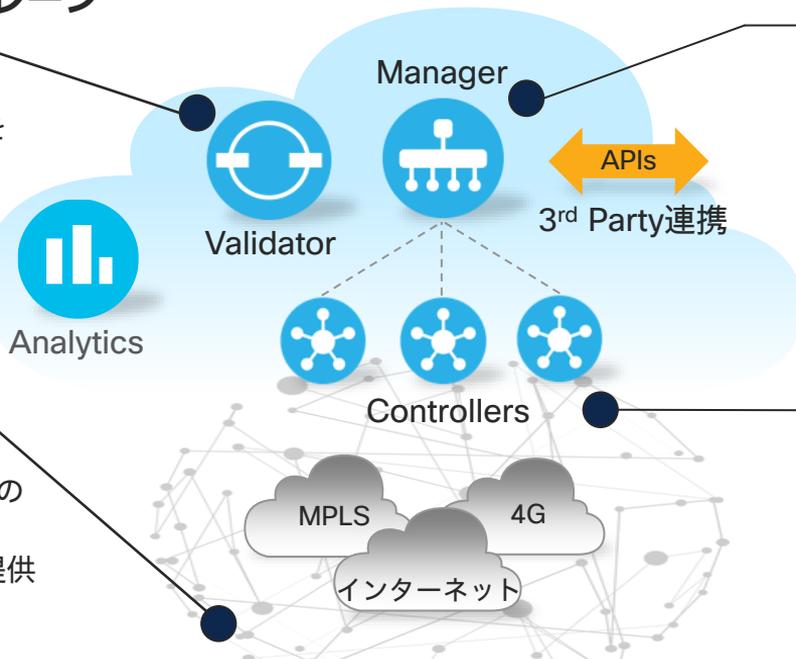
SD-WAN アーキテクチャの概要



Cisco SD-WAN アーキテクチャ

オーケストレーションプレーン

- デバイス認証のポイント
- Manager / Controller の情報を全 WAN Edge へ配信
- NAT トラバーサルを提供



データプレーン

- データ転送
- ゼロタッチプロビジョニングの提供
- 物理/仮想アプライアンスの提供

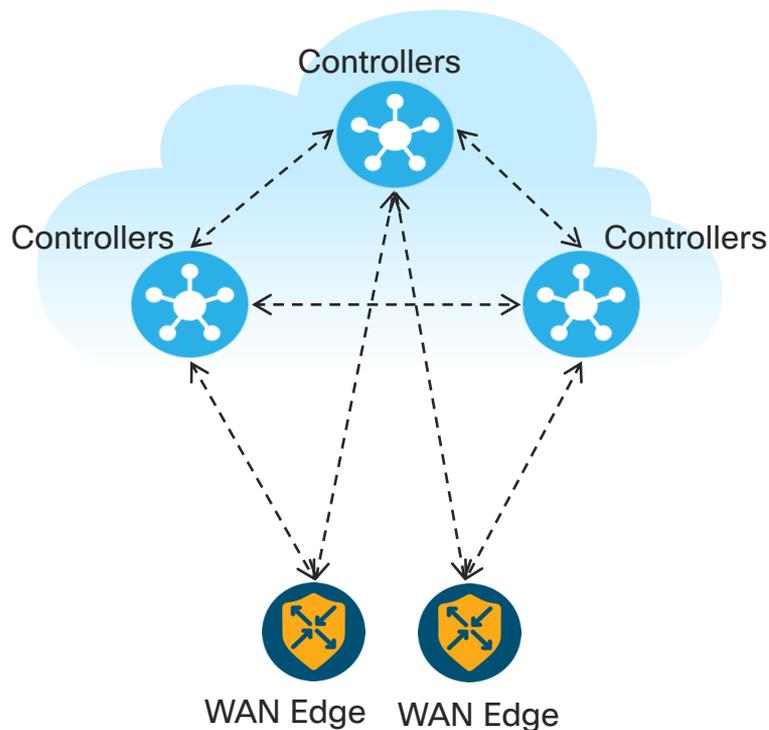
マネジメントプレーン

- 一元化された管理プラットフォーム
- マルチテナントやAPI連携の提供
- トラブルシューティング
- RBAC (Role Based Access Control) によるアクセス制御を提供

コントロールプレーン

- WAN Edge のコントロールプレーン分離
- ルート情報やトラフィック制御ポリシーを全 WAN Edge に配布
- オーバレイネットワークの制御

OMP

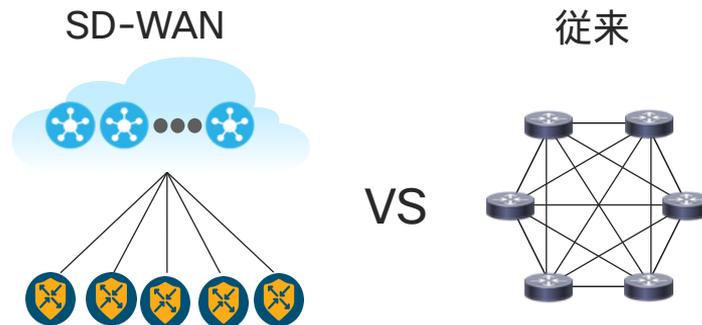


<-----> OMP

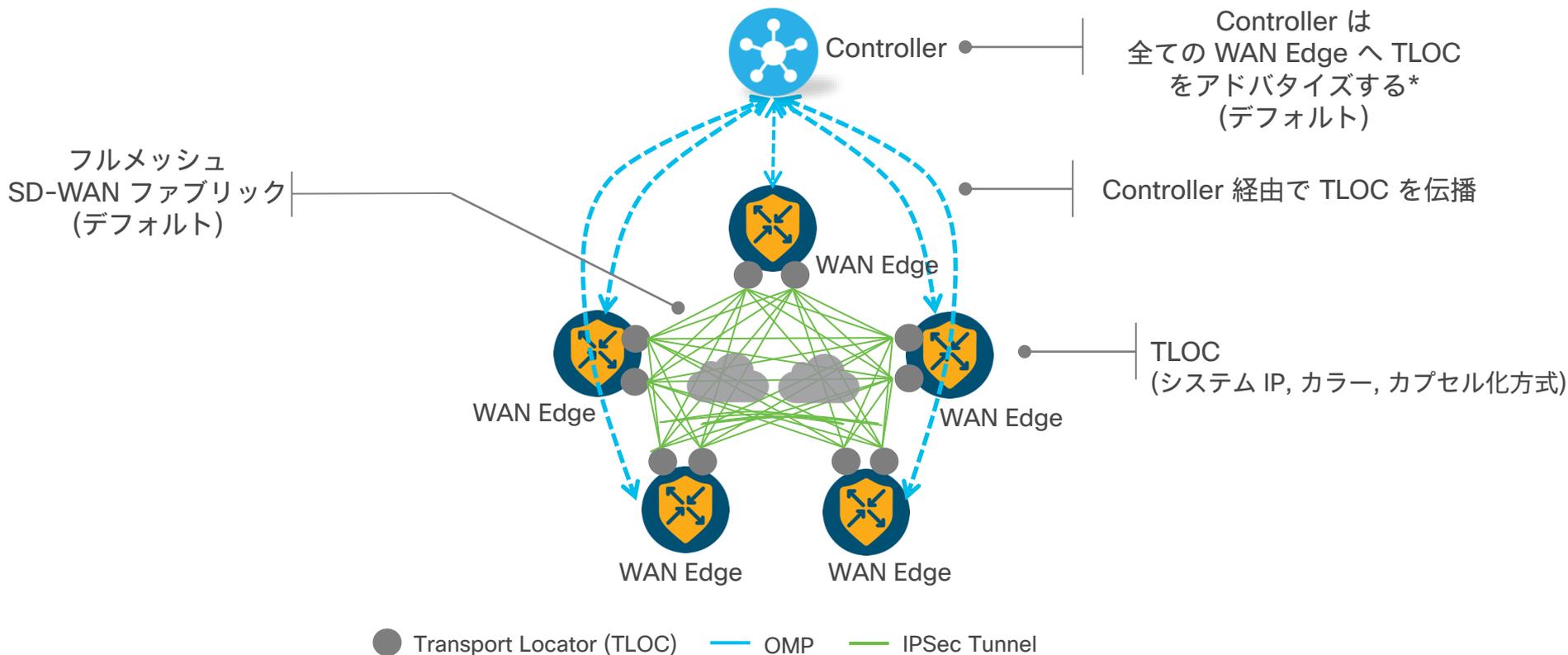
※ WAN EdgeはすべてのControllerに接続する必要はありません

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

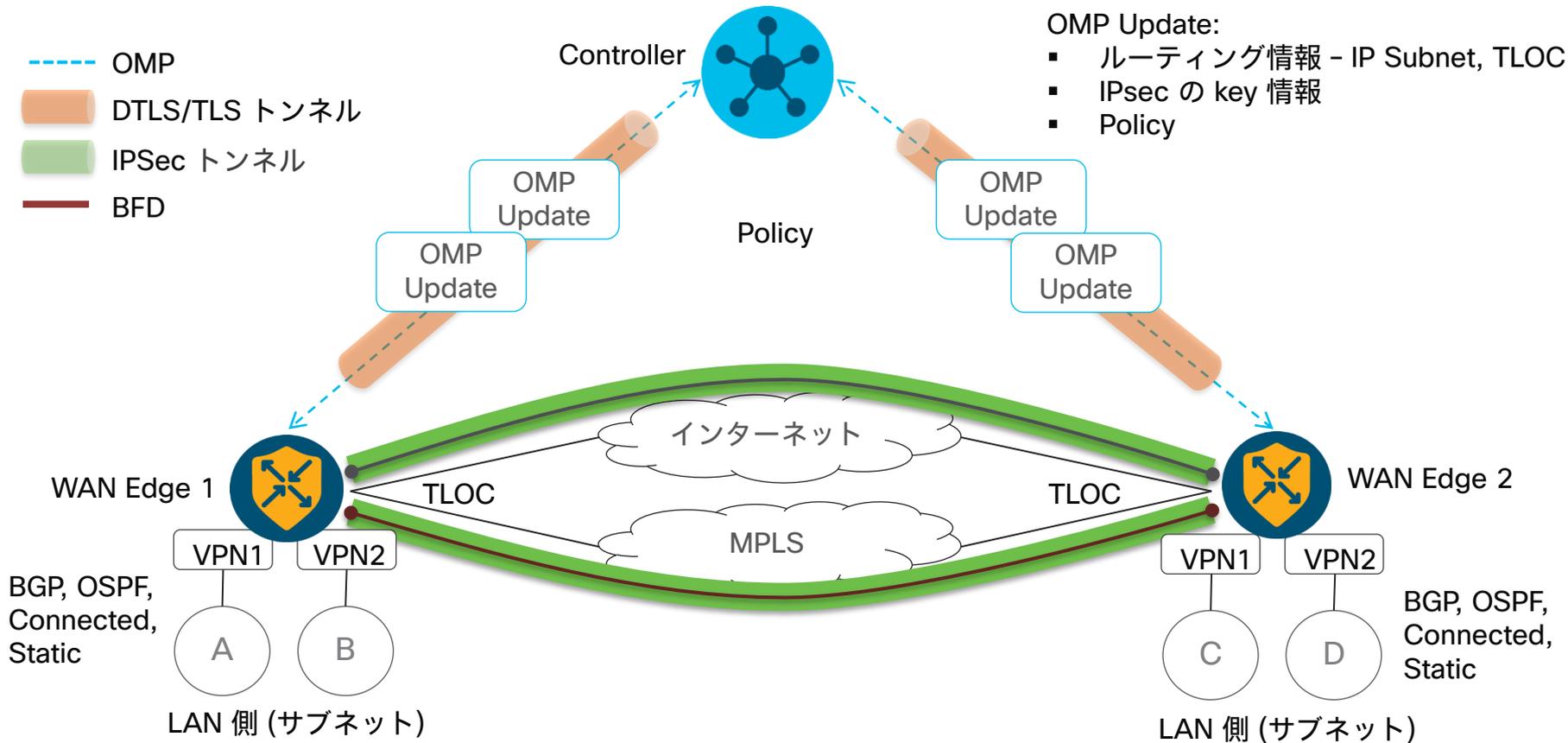
- Overlay Management Protocol (OMP)
- WAN エッジルーターと Controller および Controller 間でやりとり
 - TLS/DTLS コネクション内
- コントロールプレーンのポリシーを WAN Edge へ伝播
- ネットワークの複雑性を低減しスケールを向上



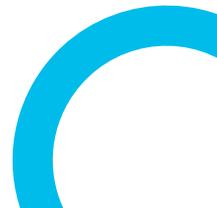
セキュアコントロールプレーン : Transport Locator (TLOC)



Cisco SD-WAN Fabricトラフィック流れ



自動化された セキュアなWANの 概要と計画



SD-WAN 導入ワークフロー

Step 1

ネットワーク計画



Step 2

Cisco SD-WAN
コントローラの展開



Step 3

WANエッジリストの
アップロード
Manager SAを接続



Step 4

テンプレートの作成



Step 5

ローカライズされた
ポリシーの設定および
デバイステンプレート



Step 6

集中型ポリシーの設定



Step 7

デバイスへ適用



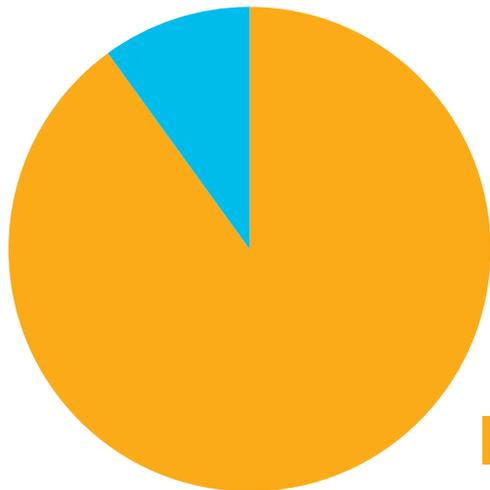
Step 8

デプロイとモニタリング



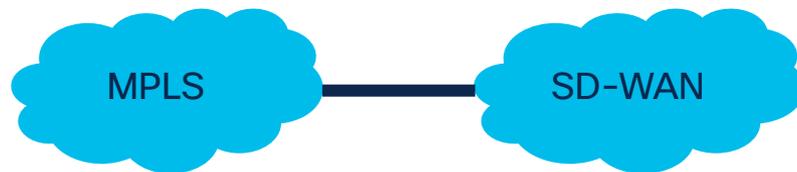
ネットワーク計画・準備が重要

SD-WAN 導入時における
必要な時間と労力



- 準備：既存ネットワーク
- 導入と移行：SD-WAN ルーター

移行中は既存ネットワークと
SD-WAN が共存する



Cisco DNA SD-WAN ライセンス

Cisco DNA Essentials

接続/管理

- ・ クラウドまたはオンプレミスの管理
- ・ 柔軟なトポロジ
 - ・ ハブアンドスポーク
 - ・ フルメッシュ/部分メッシュ
- ・ アプリケーションおよび SLA ベースのポリシー
- ・ ダイナミック ルーティング (BGP、OSPF)
- ・ VNF ライフサイクル管理

セキュリティ

- ・ Talos を使用した IPS とアプリケーション制御を備えたエンタープライズ ファイアウォール
- ・ Cisco Umbrella DNS モニタリング (可視性のみ)

SD-WAN サービス

- ・ FEC と パケット重複による基本的なパス最適化
- ・ TCP 最適化

Cisco DNA Advantage

クラウド/分析

- ・ Cloud OnRamp for IaaS と Cloud OnRamp for SaaS
- ・ 自動化されたサービス ステッチング
- ・ 暗号化トラフィック分析
- ・ vAnalytics

セキュリティ

- ・ セグメンテーション (VPN 無制限)
- ・ Cisco AMP および SSL プロキシ
- ・ URL フィルタリング
- ・ Cisco Umbrella アプリケーションの検出

クロスドメインのイノベーション

- ・ Integrated Border for Campus (SD-Access)
- ・ アプリケーション SLA のための ACI との統合

サービス

- ・ Web キャッシング、DRE (SSL プロキシを含む)
- ・ 音声モジュールと SRST の統合
- ・ マルチキャスト

Cisco DNA Essentials

Cisco DNA Premier

セキュリティ

Cisco Umbrella SIG Essentials

トランザクション

- ・ 5 ~ 250 Mbps = 1 Mbps あたり 1 ライセンス
- ・ 500 Mbps = 375 ライセンス
- ・ 1 Gbps = 500 ライセンス
- ・ 2.5、5、10 Gbps = 750 ライセンス

エンタープライズ アグリーメント(EA)

- ・ Tier 0 : Premier では使用できません
- ・ Tier 1 : 25 ライセンス
- ・ Tier 2 : 250 ライセンス
- ・ Tier 3 : 750 ライセンス
- ・ 追加の Cisco Umbrella SIG Essentials ライセンスは別途購入できます。

Cisco Threat Grid

- ・ 顧客アカウントごとに 1 日あたり 200 ファイルの権限を提供
- ・ サンドボックス化のために Threat Grid クラウドに送信されるファイル。オンプレミスの Threat Grid は Premier では使用できません
- ・ すべての顧客サイトにわたるグローバルな権限付与
- ・ 追加の Cisco Threat Grid ライセンスは別途購入できます。

Cisco DNA Advantage

Cisco DNA Essentials

コントローラの実装方式



★ 推奨

Cisco による実装

お客様による実装



クラウドホスト型

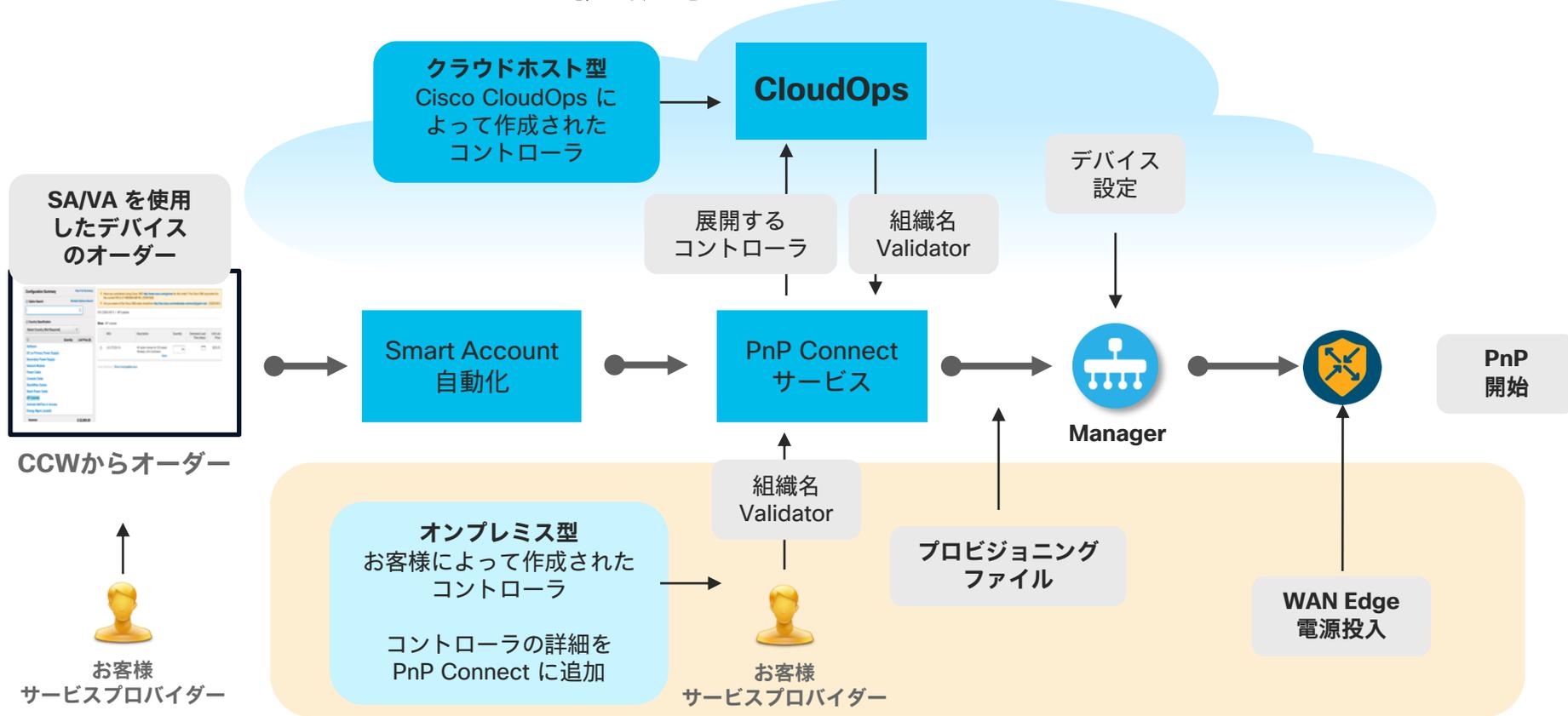
AWS、Azure



オンプレミス型

KVM、ESXi

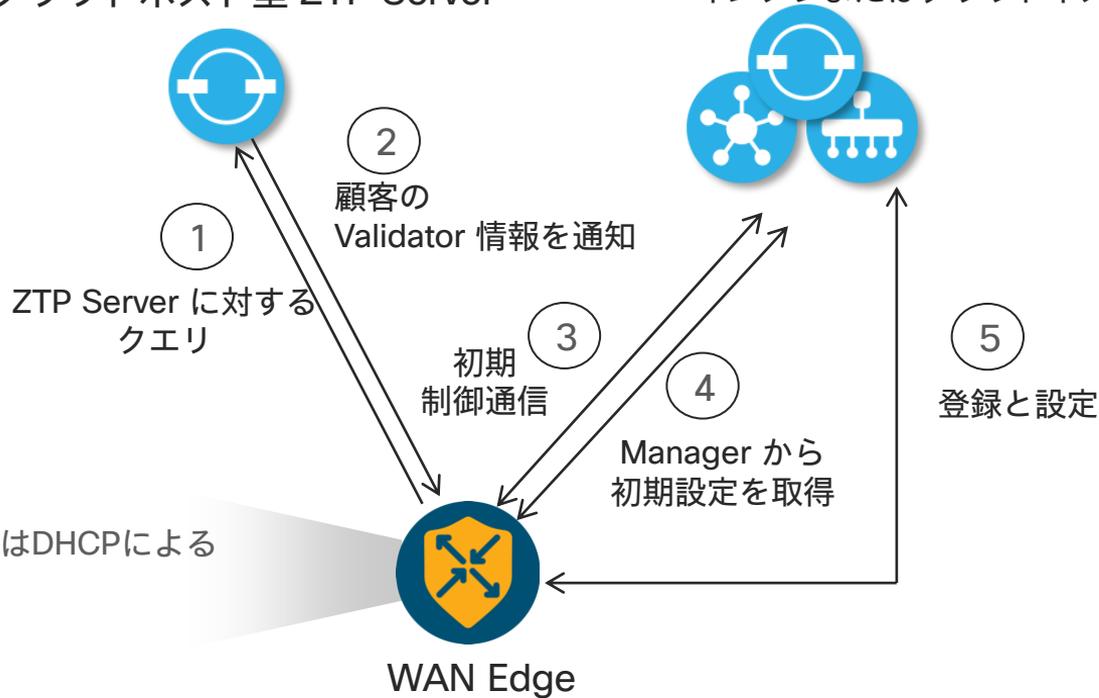
PnP Connect を使用したデバイスの追加



ゼロタッチプロビジョニング

PnP コネクトポータル
Cisco クラウドホスト型 ZTP Server

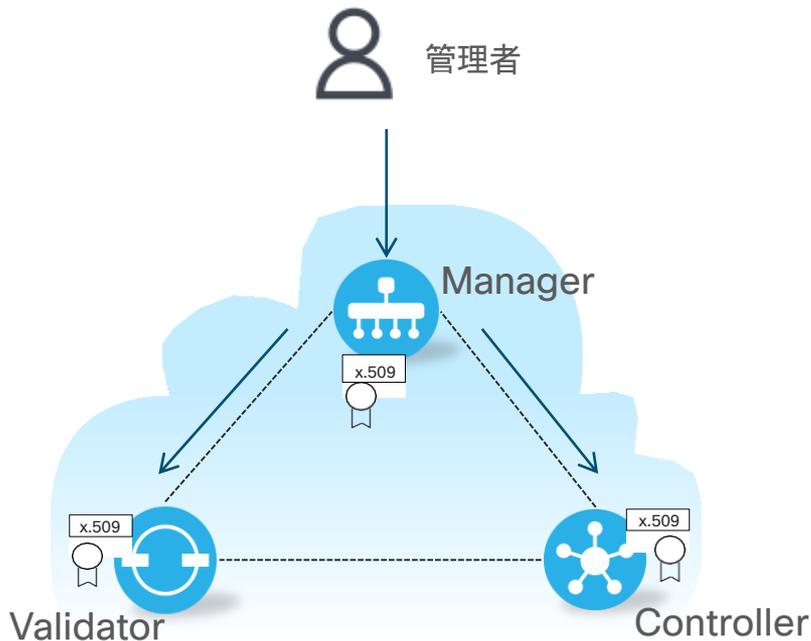
お客様 コントローラ
(Validator / Manager / Controller)
オンプレまたはクラウドホスト型



前提:

- トランスポート側 (WAN) はDHCPによるIPアドレス取得
- DNSによる名前解決 (devicehelper.cisco.com)

ホワイトリスト



- ネットワーク管理者は、Manager GUI でコントローラを追加

Controller Type	Hostname	System IP	Site ID
vManage	vManage	10.10.10.10	10
vSmart	vSmart-2	22.22.22.22	20
vSmart	vSmart-1	12.12.12.12	10
vBond	vBond-2	21.21.21.21	-
vBond	vBond-1	11.11.11.11	-

- Manager はコントローラリストをすべてのコントローラに配布
- 証明書による認証

ホワイトリストと Identity Trust

WAN Edge List
(ホワイトリスト)

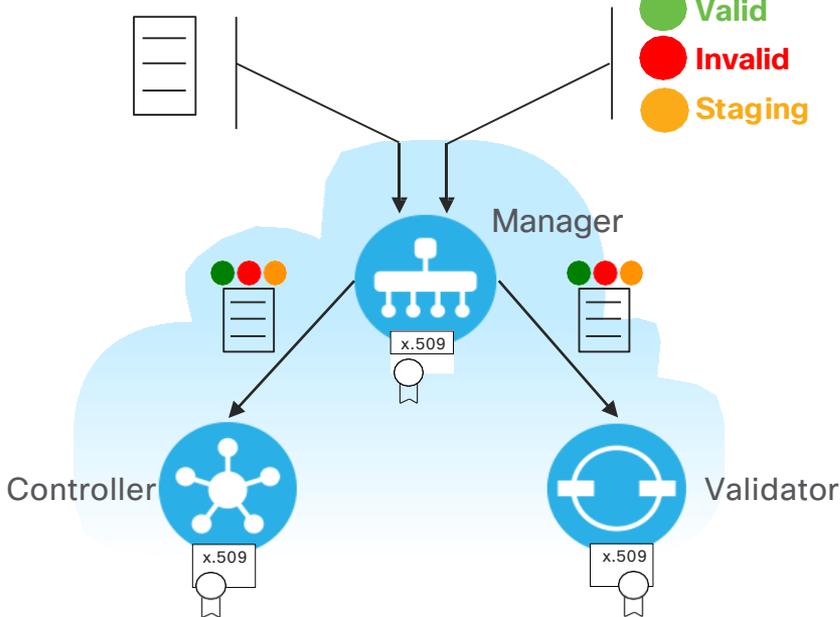
Identity
Trust



- 管理者が Manager GUI へ WAN Edge List をアップロード
 - WAN Edge List のアップロード/同期
 - PnP Connect (software.cisco.com) からダウンロードも可能

Chassis Number	Serial No./Token	Hostname	Site ID
C8300-1N1S-6T-FLM2530112W	0804171629128427	BR1-C8K-1	300
C8300-1N1S-6T-FLM2530112X	0719770445380142	BR1-C8K-2	300
IR1101-K9-FCW23100HTF	0397	BR3-IR1101	500
IR1833-K9-FCW2506PJ84	0878749413292576	BR4-IR1833	600

- Identity Trust (Valid, Invalid, Staging)
- WAN Edge List と Identity Trust は Manager によって Controller および Validator へ配布



WAN エッジへの設定

WAN Edge List Controllers

ISR4431/K9-FOC22469720 Search

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

Chassis Number	Tags	Hostname	Site ID	Region ID	Mode	Device Status
ISR4431/K9-FOC22469720	Add Tag	SJC04-ISR4K-01	900	-	vManage	In Sync

- Running Configuration
- Local Configuration
- Delete WAN Edge
- Generate Bootstrap Configuration**
- Change Device Values
- Template Log
- Device Bring Up

```
#cloud-boothook
system
personality          vedge
device-model        vedge-ISR-4321
host-name            WanEdge
system-ip           10.255.255.121
site-id             21
organization-name   ""CLEUR 2019 BRKRST - 2559""
console-baud-rate   9600
vbond 10.0.0.23 port 12346
!
!
!
interface GigabitEthernet0/0/0
 no shutdown
 ip address 192.168.10.10 255.255.255.0
 exit
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

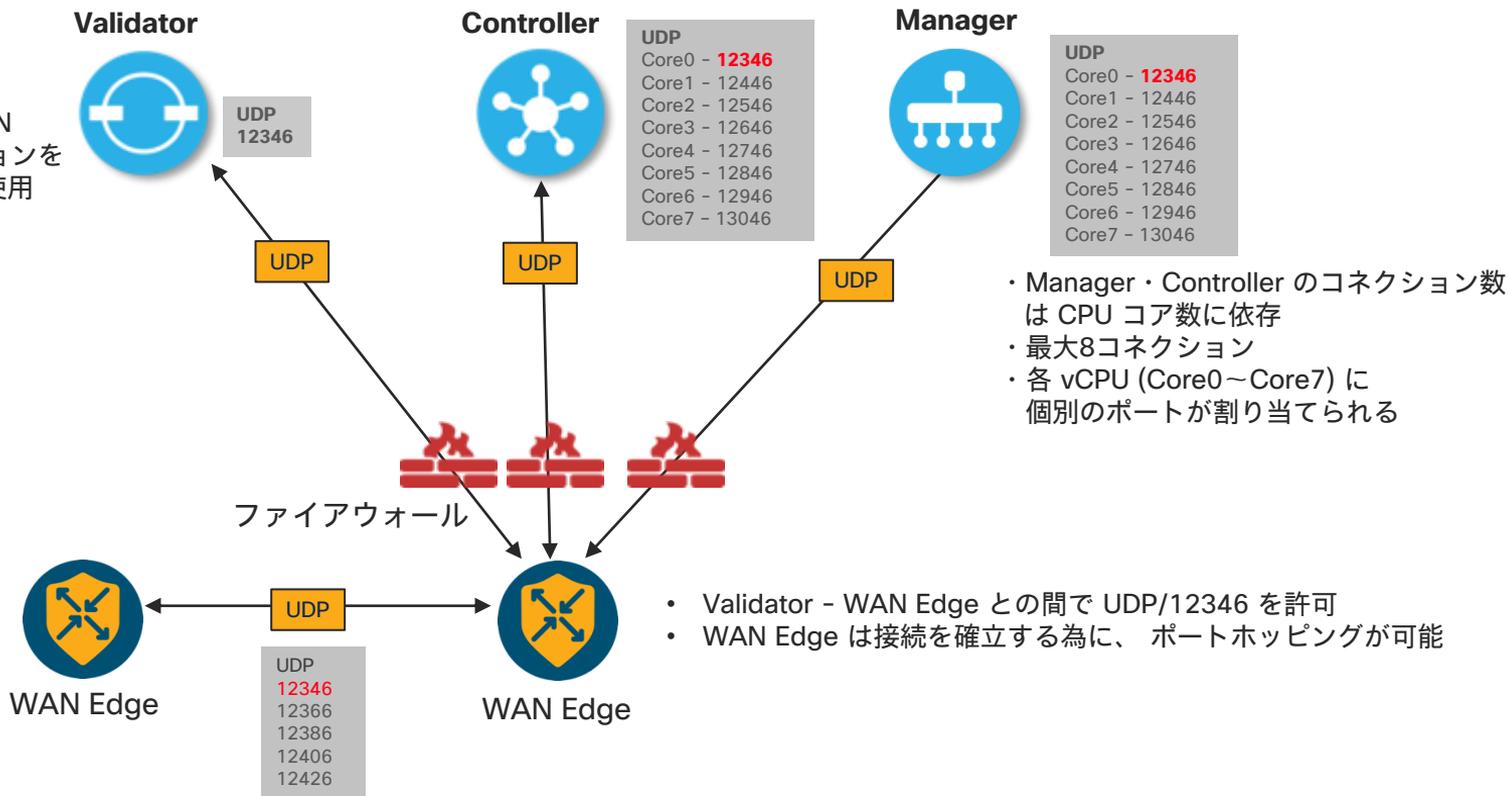


- Cisco Manager を使用して設定ファイルを生成
- 設定ファイルをブート可能な USB ドライブにコピー
- USB ドライブをデバイスに接続、または設定をデバイスのブートフラッシュにコピー
- デバイスを起動
- 起動時にルータは bootflash: または usbflash: でファイル名 ciscoSD-WAN.cfg を検索

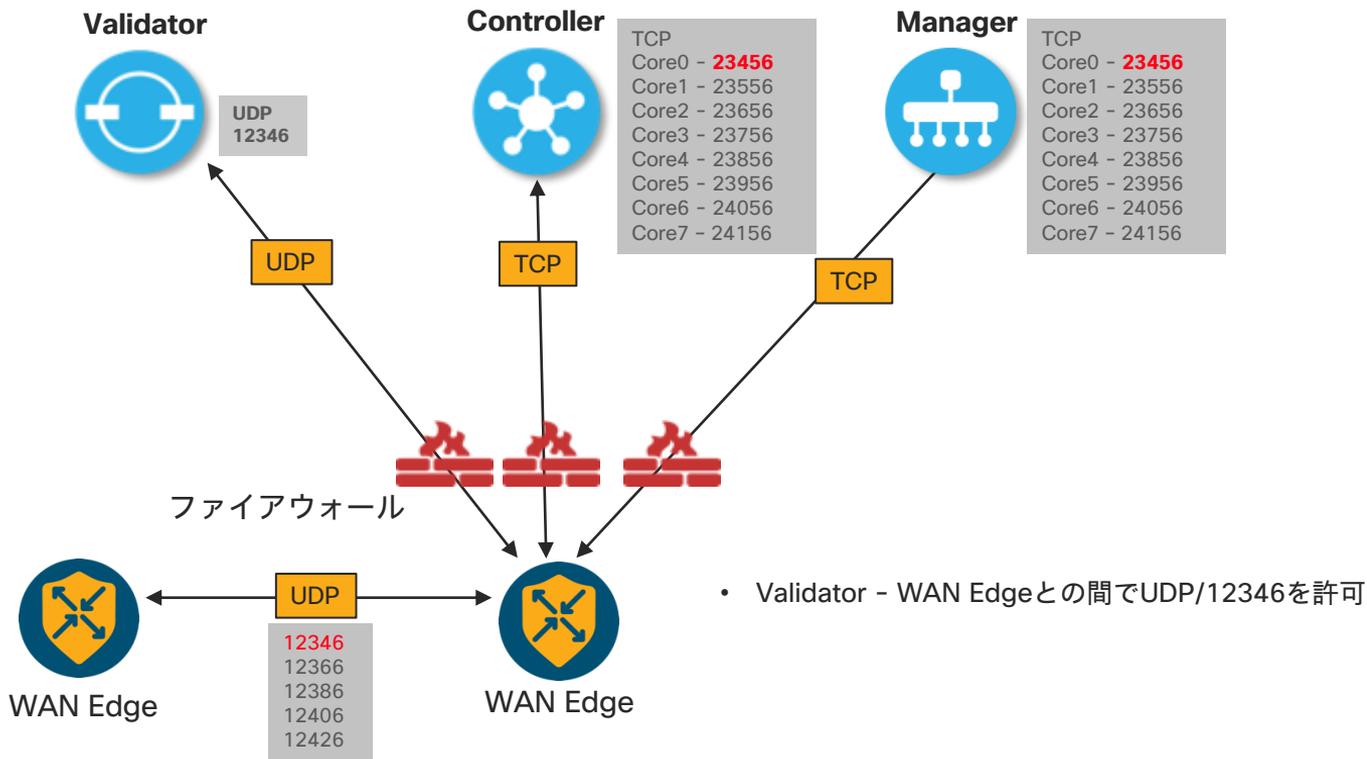


ファイアウォールポート : DTLS

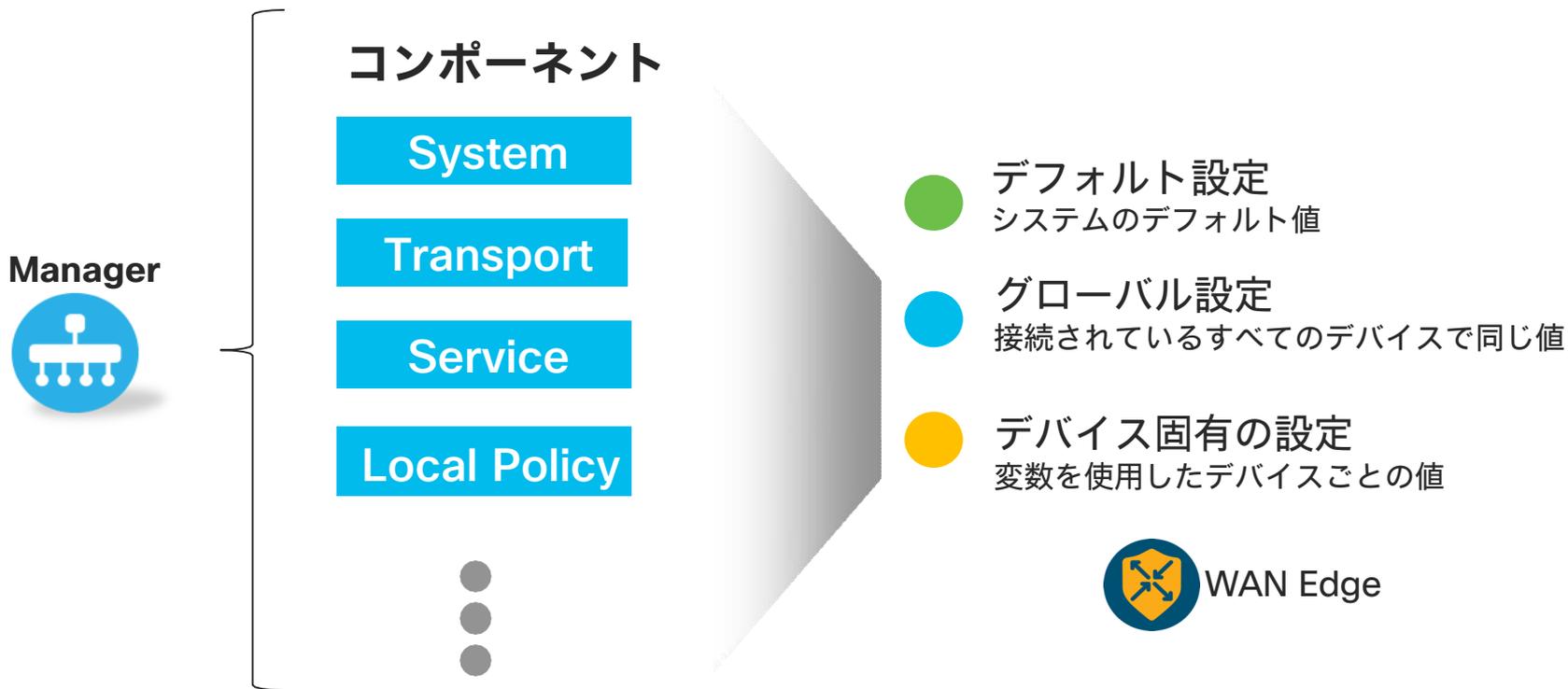
- Validator は複数のコアをサポートしない
- Validator は他の SD-WAN デバイスと制御コネクションを確立する際に、DTLS を使用する
- UDP ポートは12346



ファイアウォールポート : TLS



テンプレートによる SD-WAN デバイス設定



デバイステンプレートによる一元化されたデバイス設定

Cisco SD-WAN Configuration · Templates

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

Device Model* C8300-1N1S-6T

Device Role* SDWAN Edge

Template Name* C8K_BranchType1Template

Description* Branch Type 1 Template for C8K Routers

Basic Information Transport & Management VPN Service V...

Basic Information

Cisco System* C8K_All-System-Template

Cisco Logging* C8K_Factory_Default_Logging_Template

Cisco AAA Factory_Default_AAA_CISCO_Template

Cisco BFD* C8K_All-BFDTemplate

Name	Description	Type	Device Model	Device Role	Feature Templates	Devices Attached
C8K_BranchType1Template	Branch Type 1 ...	Feature	C8300-1N1S-6T	SDWAN Edge	22	2
vSmartConfigurationTemplate	Config templat...	CLI	vSmart		0	0
BranchType2Template-cEdge	Branch Type 2 ...	Feature	C1111-8PLTEEA	SDWAN Edge	21	0
VSMART-device-template	vSmart device t...	Feature	vSmart		8	2

WAN Edge



Cisco SD-WAN ポリシーアーキテクチャ

集中型ポリシー

トポロジー & VPN メンバーシップ:
コントロールポリシー
VPN メンバーシップポリシー

トラフィックルール:
AAR ポリシー
データポリシー
(トラフィックデータ)
Cflowd

ローカライズされたポリシー

ローカル ポリシー:
ローカルコントロールポリシー
(ルーティングポリシー)
ローカルデータポリシー
(QoS, ACL など)

ポリシー 設定



Netconf



OMP



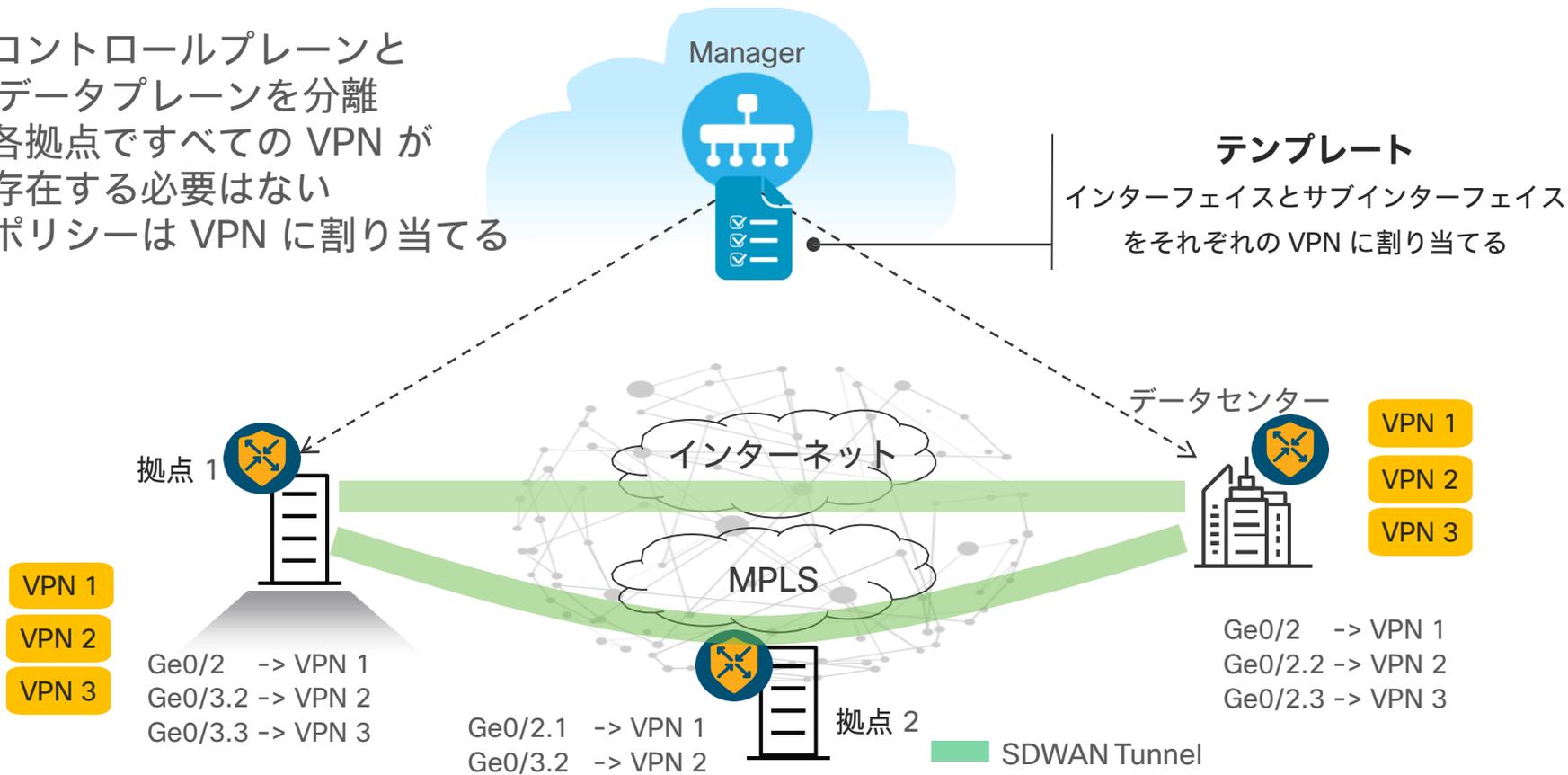
デバイス
テンプレート

Netconf

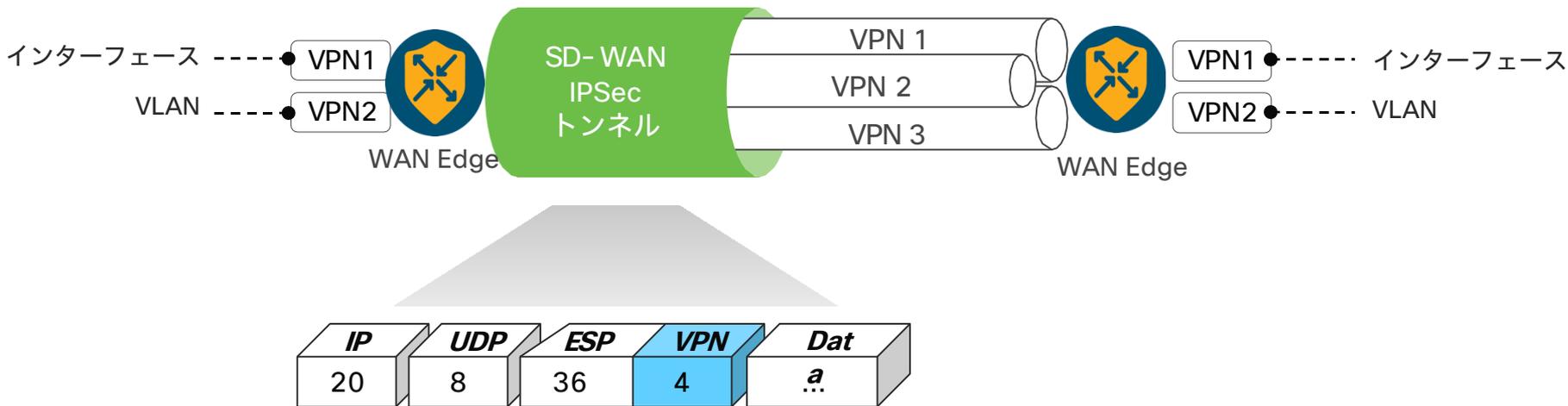


VPN セグメンテーション

- コントロールプレーンとデータプレーンを分離
- 各拠点ですべての VPN が存在する必要はない
- ポリシーは VPN に割り当てる

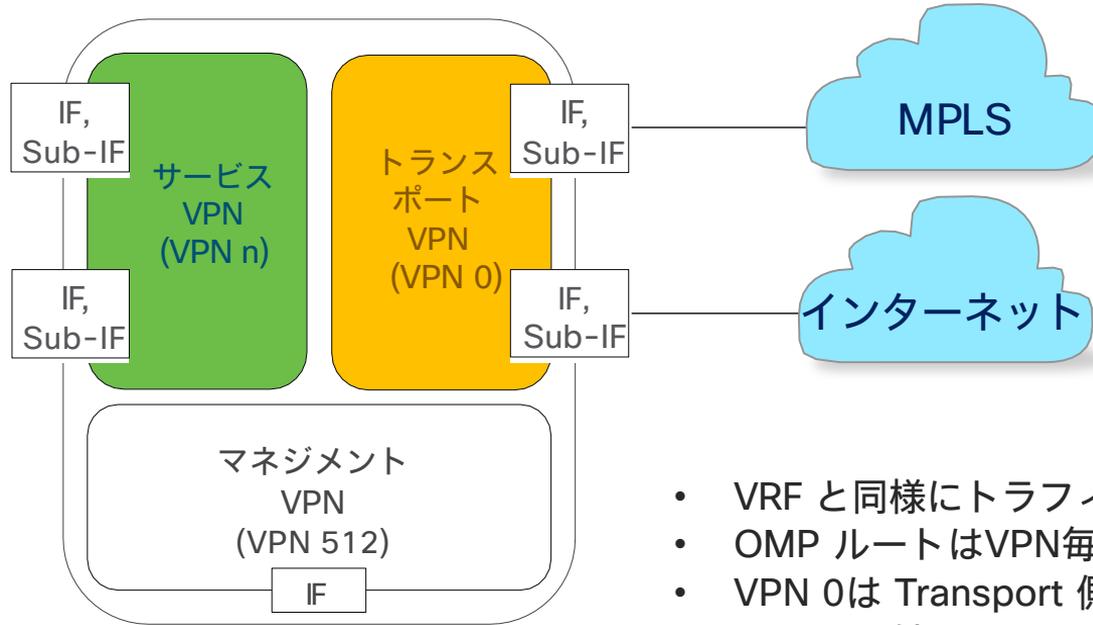


VPN セグメンテーション



- アンダーレイ回線に依存しないファブリック
- WAN エッジに VPN ごとにルーティングテーブルが作成される
- ラベルは VPN を識別するために使用される (rfc 4023)
- インターフェイス および サブインターフェイス (802.1Q タグ) と VPN をマッピング

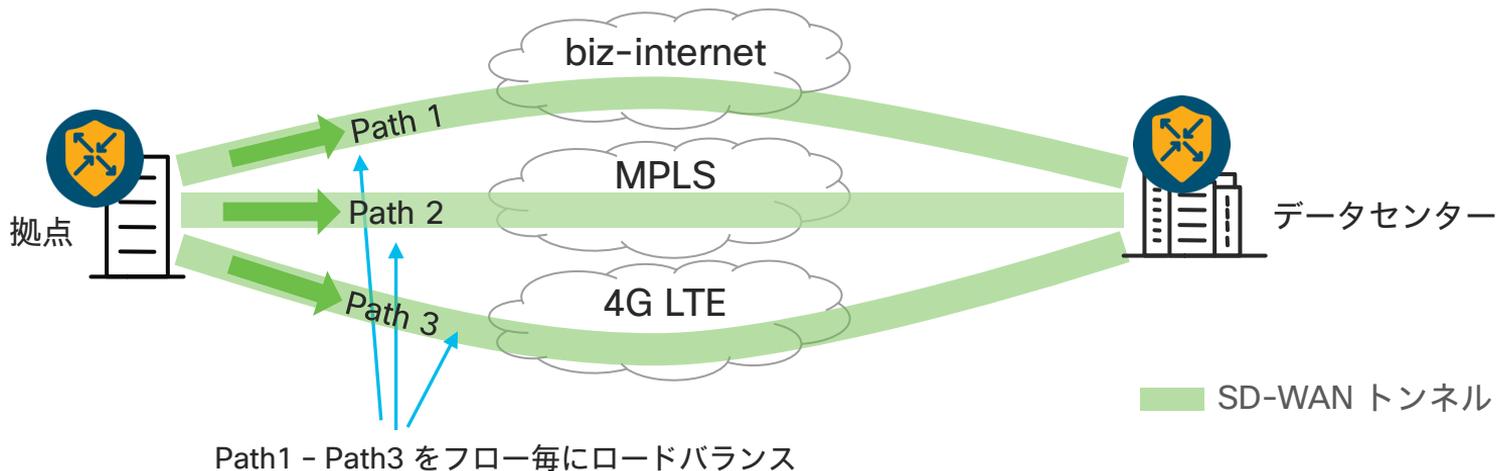
SDWAN VPN とセキュリティゾーン



- VRF と同様にトラフィックやルーティングテーブルを分離
- OMP ルートはVPN毎に処理される
- VPN 0は Transport 側 (WAN 側) に割り当てられる
- VPN 512は Management 用に割り当てられる

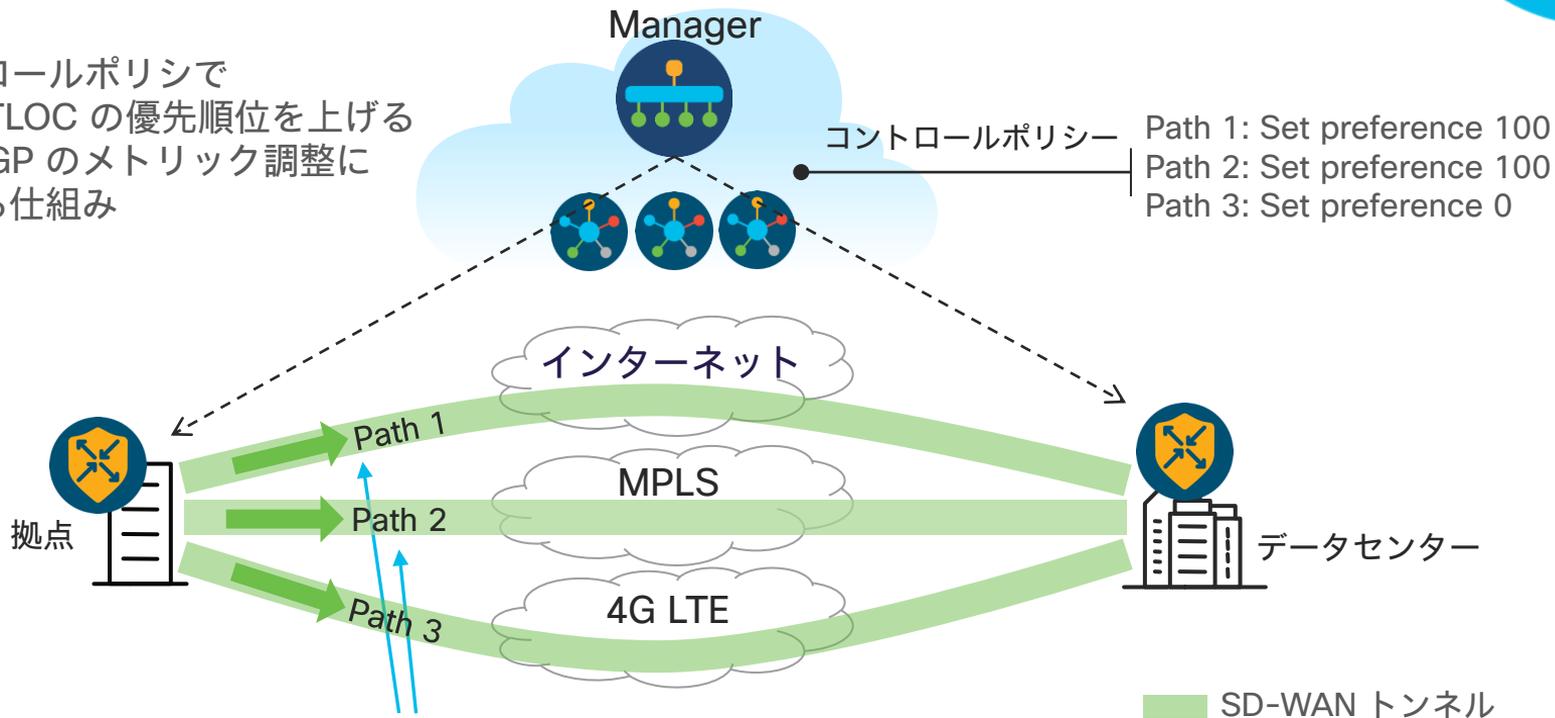
帯域の増強 (等コストロードバランス)

- プリファレンス(重み付け) で特定サイトのトラフィックを制御可能
- 4G LTE をバックアップとして指定可能



帯域の増強 (WAN回線の優先順位)

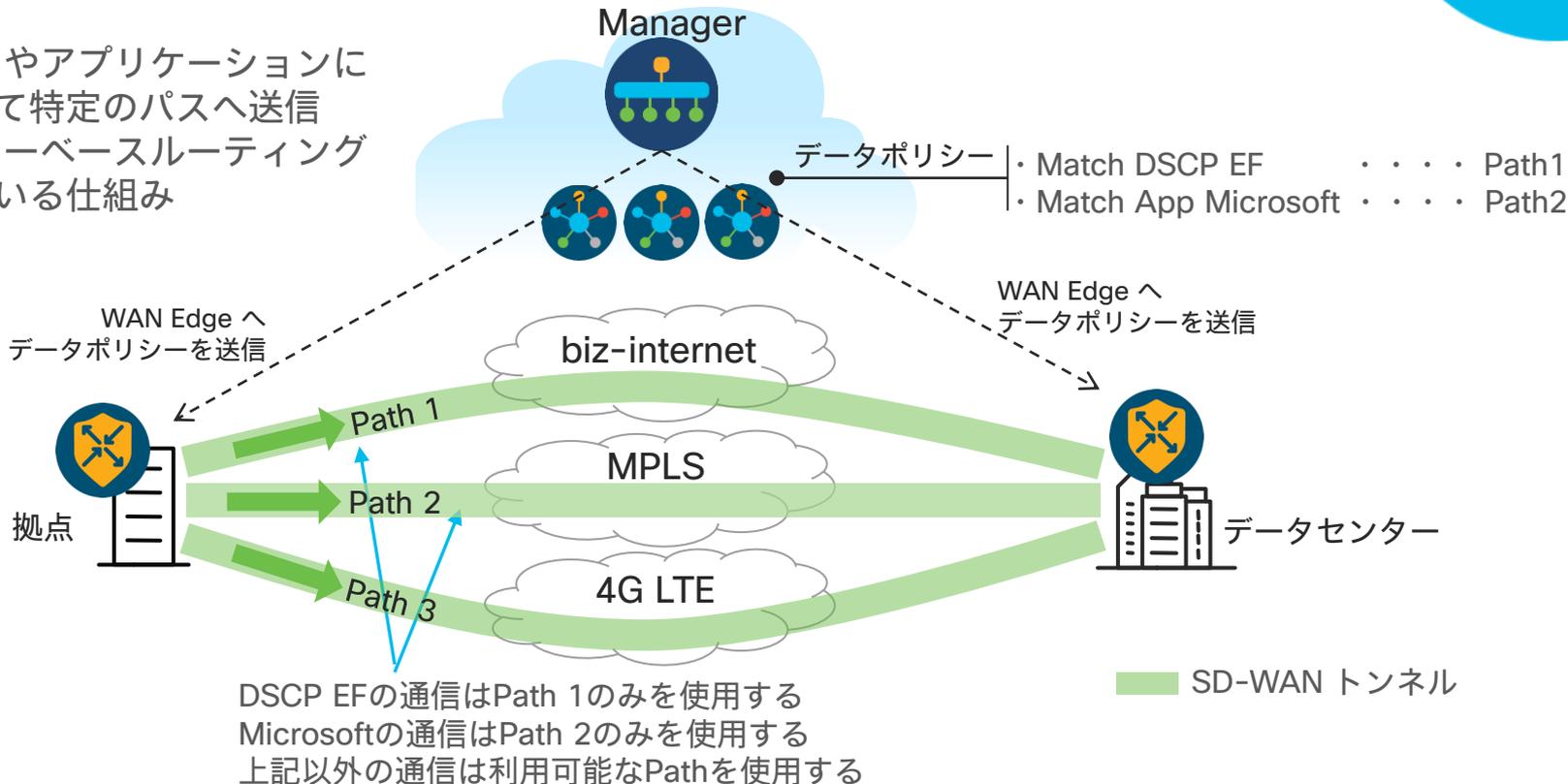
- コントロールポリシーで特定の TLOC の優先順位を上げる
- IGP / BGP のメトリック調整に似ている仕組み



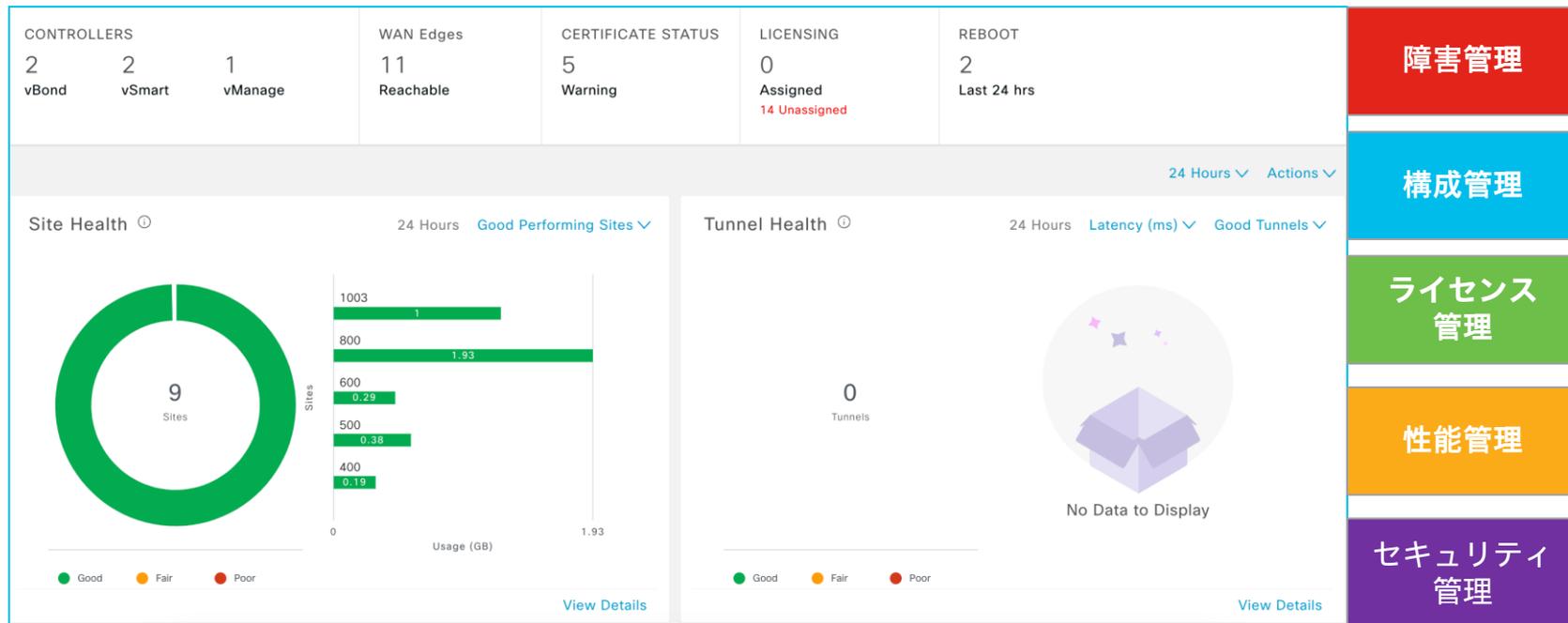
Path 1 - Path 2 の間でロードバランス
Path 3 はバックアップとして動作

帯域の増強 (アプリケーションパスの制御)

- ・ DSCP やアプリケーションに基づいて特定のパスへ送信
- ・ ポリシーベースルーティングに似ている仕組み



集中管理 一元化されたManager NMS





デモ

キーポイント



- 01 ネットワークの計画
- 02 ZTP
- 03 VPN セグメンテーション
- 04 帯域の増強

関連資料

これらのリソースを使用する

- [Cisco SD-WAN End-To-End Deployment Guide](#)
- [Cisco SD-WAN Design Guides Library](#)
- [SD-WAN SD-WAN DevNet APIs](#)

Cisco SD-WAN コミュニティを活用：

<https://cs.co/sdwan-community>



Accelerators (1社様向けセッション)

お客様に応じて 1 対 1 のガイダンスや
ツールを提供し価値の最大化を促進

- 1:1 でのコーチングセッション形式
- 特定トピックであれば柔軟なメニューを提供
(お客様の環境確認、製品機能説明がメイン)
- スコープは固定

Cisco エキスパート ↔ お客様/パートナー様



1 対 1 のコーチングセッション

1 - 2 時間程度の
セッション



カスタマイズ

決められたトピック
柔軟な内容

Webex / オンライン
(要相談)

詳細については japan-atx@cisco.comまでお問い合わせください。

Accelerators サンプル

Cisco Catalyst Center を使った
ヒューマンエラーの発見と是正

コンプライアンス サマリー

場所: >> プロビジョニング>インベントリ
デバイスを選択 > View Device Details
左のメニューから
コンプライアンス サマリー

- Start-up vs Running Config
- ソフトウェアイメージ
- EoX
- セキュリティアドバイザリ
- ネットワークプロファイル

スタートアップ構成と実行構成

コンプライアンスの概要

コンプライアンスチェックをトリガーするイベントは構成変更ではありません。 コンプライアンスチェックの結果

名前	ステータス	最後のチェック日時	最後の失敗日時
スタートアップ構成と実行構成	失敗	2024.09.03 04:00:00	2024.09.03 04:00:00
ソフトウェアイメージ	成功	2024.09.03 04:00:00	2024.09.03 04:00:00
EoX	成功	2024.09.03 04:00:00	2024.09.03 04:00:00

- デバイスの start-up configuration と running configuration が同期しているか確認
- 変更が発生してから 5 分以内にチェックされる

カスタマーサクセス ぽーたる のご紹介

カスタマーサクセス ぽーたる

<https://community.cisco.com/t5/-/ta-p/4791205>



新着情報や ATX、ユーザ会情報、
ラーニングマップ、Upgrade方法
など掲載

The screenshot shows the Customer Success Portal interface. At the top, there is a navigation bar with the Cisco logo and the text "Customer Success Moderator Beginner". Below this is a main header with the title "Customer Success Portal" and the subtitle "シスコ製品の使いこなしまでの近道". A button labeled "詳細はコチラ" is visible. The main content area features a list of featured items:

- 特集
- 今月~来月のATX
- Success Tracks情報
- ATX情報
- Success Community紹介
- 技術・ベストプラクティス ドキュメント

Below the list, there is a paragraph of text: "Cisco Customer Successでは、Customer Successが提供するATXの情報やテクノロジーTips、設計、運用のベストプラクティスに関する記事を投稿しています。以下に各サイトを纏めていますので、ぜひ活用ください。"

The "特集" (Featured) section includes a bullet point: "ウェビナー「CX Cloud と Customer Success その魅力の紹介」を開催しました。録画や資料はコチラ". Below this is an image showing three people sitting on a couch in a modern office setting, engaged in a discussion. The Cisco logo is visible in the top left corner of the image.



Cisco

Customer Experience