Cisco SD-WAN 設計ガイド

2020 年 9 月

目次

はじめに

エンタープライズ環境は常に進化しています。モバイルおよび Internet-of-Things（IoT）デバイスのトラフィック、SaaS アプリケーション、およびクラウドの採用に対する需要が高まっています。さらに、セキュリティのニーズが高まり、アプリケーションに優先順位付けと最適化が必要になっています。この複雑さが増すにつれて、コストと運用費の削減が求められています。高可用性と拡張性は引き続き重要です。

従来の WAN アーキテクチャは、この進化する状況において大きな課題に直面しています。従来の WAN アーキテクチャでは、一般に複数の MPLS か MPLS とインターネットまたは LTE をアクティブ/バックアップ方式で使用したペアでトランスポートが構成され、ほとんどの場合、インターネットや software-as-a-service（SaaS）のトラフィックはインターネットアクセス用の中央のデータセンターまたは地域のハブにバックホールされます。これらのアーキテクチャには、帯域幅が十分でない、帯域幅のコストが高い、アプリケーションのダウンタイムがある、SaaS のパフォーマンスが低い、運用が複雑である、クラウド接続のワークフローが複雑である、導入やポリシーの変更に時間がかかる、アプリケーションの可視性に制限がある、ネットワークのセキュリティの保護が難しいなどの課題があります。

近年、このような課題に対処するために、ソフトウェア定義型ワイドエリア ネットワーキング（SD-WAN）ソリューションが進化してきました。SD-WAN は、ソフトウェア定義型ネットワーキング（SDN）の広範なテクノロジーの一部です。SDN は、基盤となるネットワーク インフラストラクチャをアプリケーションから切り離して抽象化し一元的に管理するネットワーク管理方法です。データプレーンの転送とコントロールプレーンを切り離すことで、ネットワークのインテリジェンスを集約し、ネットワークの高度な自動化、運用の簡素化、一元化されたプロビジョニング、モニタリング、トラブルシューティングが可能になります。SD-WAN は、このような SDN の原理を WAN に当てはめたものです。

Cisco® SD-WAN ソリューションは、企業でのデジタルおよびクラウド変革を実現する、エンタープライズ向けのオーバーレイ方式 WAN アーキテクチャです。ルーティング、セキュリティ、集中型ポリシー、およびオーケストレーションを大規模なネットワークに完全に統合します。このソリューションは、マルチテナント、クラウド経由のオペレーションを提供し、高度に自動化された、セキュア、スケーラブル、アプリケーション認識型で、優れた分析機能を備えています。Cisco SD-WAN テクノロジーは、一般的な WAN 導入の問題と課題に対応します。次のような利点があります。

- 集中型ネットワークおよびポリシー管理、および運用の簡素化。変更管理と導入の時間を短縮します。
- MPLS と低コストブロードバンドの組み合わせ、またはアクティブ/アクティブ方式のトランスポートの組み合わせ。キャパシティを最適化し、帯域幅コストを削減します。
- データセンター、ブランチ、クラウドに拡張するトランスポートに依存しないオーバーレイ。
- 導入の柔軟性。コントロールプレーンとデータプレーンが分離されているため、コントローラをオンプレミスまたはクラウドに導入できます。Cisco WAN エッジルータの導入は、物理的または仮想的に行うことができ、ネットワーク内の任意の場所に導入できます。
- 堅牢で包括的なセキュリティ。データの強力な暗号化、エンドツーエンドのネットワーク セグメンテーション、ゼロトラスト セキュリティ モデルによるルータおよびコントローラの証明書 ID、コントロールプレーンの保護、アプリケーション ファイアウォール、Cisco Umbrella™ の挿入、ファイアウォール、他のネットワークサービスを含みます。
- パブリッククラウドへのシームレスな接続と、ブランチへの WAN エッジの移動。
- リアルタイムのサービスレベル契約（SLA）を適用するアプリケーション認識型ポリシーに加えて、アプリケーションの可視性と認識。
- SaaS アプリケーションの動的な最適化。ユーザのアプリケーション パフォーマンスが向上します。
- アプリケーションとインフラストラクチャを可視化する豊富な分析。迅速なトラブルシューティングを可能にし、効果的なリソース計画のための予測と分析を支援します。

このマニュアルについて

この設計ガイドでは、Cisco SD-WAN ソリューションの概要について説明します。コントロールプレーン、データプレーン、ルーティング、認証、SD-WAN デバイスのオンボーディングなど、ソリューションのアーキテクチャとコンポーネントについて説明します。SD-WAN コンポーネントの冗長性について説明し、多くの WAN エッジ導入の考慮事項と一般的なシナリオについて説明します。また、NAT、ファイアウォール、およびその他の導入計画の考慮事項にも焦点を当てています。

対象読者は、Cisco SD-WAN ソリューションの理解を深めたい方、特に、組織の Cisco SD-WAN の実装に適した設計を選択するために、仕組みと導入のベストプラクティスを理解する必要があるネットワークアーキテクトを対象としています。

この設計ガイドは、SD-WAN の関連する規範的な導入ガイドのコンパニオンガイドであり、最も一般的な SD-WAN の使用例の導入に関する詳細を提供します。このガイドは、vManage バージョン 19.2.1 以下に基づいています。このガイドのトピックはすべてを網羅しているわけではありません。一部のトピックの下位レベルの技術的な詳細については、関連する規範的な導入ガイドまたは他のホワイトペーパーを参照してください。ドキュメントの一覧については、付録 A を参照してください。

Cisco SD-WAN、vEdge、および IOS XE SDWAN WAN エッジデバイスでは、2 つの主要なプラットフォーム間で機能に違いがあることに注意してください。一部の相違点と制限事項がガイドで指摘されていますが、SD-WAN の導入を計画する前に、https://content.cisco.com/compatibilitymatrix.html のハードウェア/ソフトウェア/機能互換性ツールでサポート情報を確認してください。また、特定のソフトウェアリリースの詳細については、導入する前に、https://www.cisco.com/c/en/us/support/routers/sd-wan/products-release-notes-list.html のソフトウェアリリースノートを参照してください。

使用例

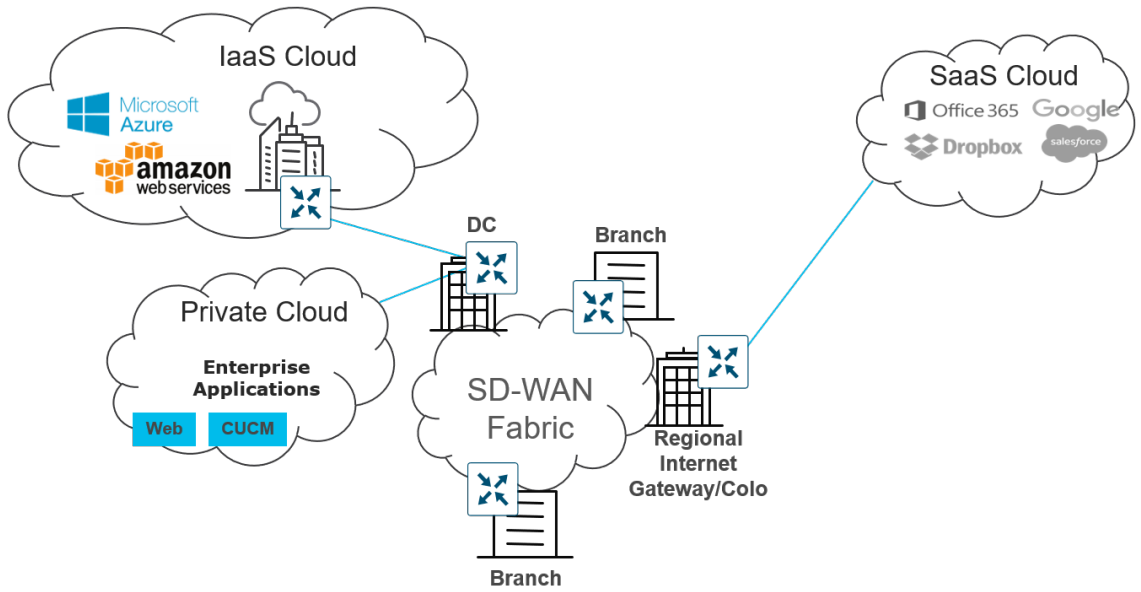
Cisco SD-WAN ソリューションには、主に 4 つの使用例カテゴリがあります。

使用例	説明
自動化されたセキュアな WAN	トランスポート非依存ネットワークを介したリモートオフィス、データセンター、およびパブリック/プライベートクラウド間のセキュアな接続
アプリケーション パフォーマンスの最適化	リモートオフィスのユーザのアプリケーション エクスペリエンスの向上
セキュアなダイレクト インターネット アクセス	インターネットトラフィックをリモートオフィスでローカルにオフロード
マルチクラウド接続	セキュリティサービスを適用できる最適なパスおよび地域のコロケーション/エクスチェンジポイントを介して、クラウド（SaaS および IaaS）アプリケーションとリモートオフィスを接続します。

自動化されたセキュアな WAN

自動化されたセキュアな WAN の使用例では、トランスポート非依存ネットワークを介して、ブランチ、データセンター、コロケーション、パブリックおよびプライベートクラウド間のセキュアな接続を提供することに重点を置いています。また、ユビキタスでスケーラブルなポリシーとテンプレートを使用した合理化されたデバイスの導入、および新規インストール用の自動化されたノータッチプロビジョニングについても説明します。

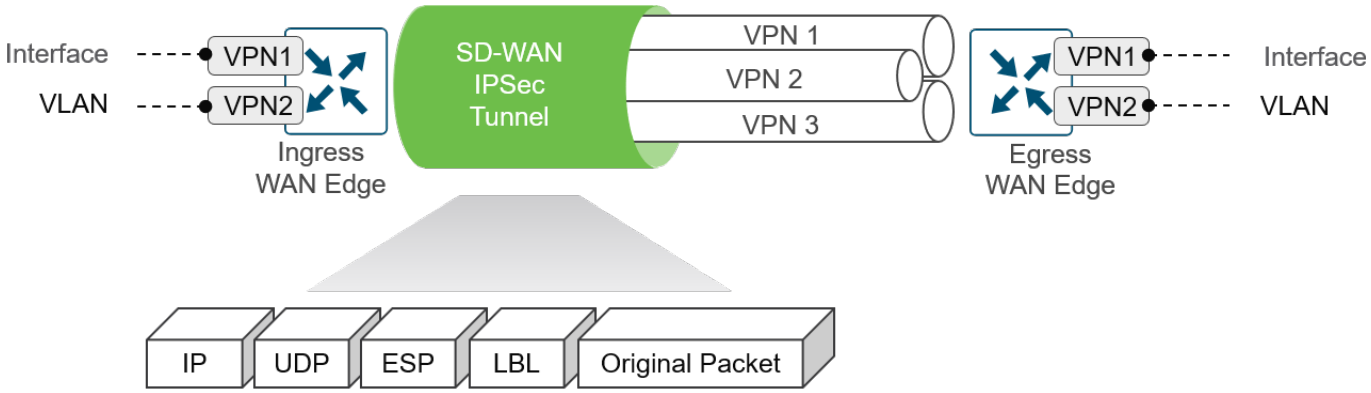
図 1. 自動化されたセキュアな WAN：プライベート/パブリッククラウドおよびその他のサイトへのセキュアな接続を提供



以下は、このカテゴリに関連する使用例のサンプルです。

- 自動ゼロタッチプロビジョニング：ケーブルを使用してトランスポートネットワークに接続し、電源をオンにするだけで、WAN の任意の場所にルータをリモートでプロビジョニングできます。WAN エッジルータは、コントローラを自動的に検出して完全に認証し、準備された設定を自動的にダウンロードしてから、残りの既存ネットワークとの IPsec トンネルを確立します。自動プロビジョニングは、IT コストの削減に役立ちます。
- 帯域幅拡張：使用可能なすべての WAN トランスポートとルーティング機能を活用して、アクティブ/アクティブ方式で使用可能なパスにトラフィックを分散することで、WAN 帯域幅を増やすことができます。トラフィックは、MPLS のような高品質で高価な回線から、わずかなコストで同じ可用性とパフォーマンスを実現できるブロードバンド回線にオフロードできます。アプリケーションの可用性は、パフォーマンスモニタリングと障害に関するプロアクティブな再ルーティングによって最大化されます。
- VPN セグメンテーション：トラフィックの分離は、セキュリティ戦略の鍵となります。ルータに入るトラフィックは、ユーザトラフィックを分離するだけでなく、ルーティングテーブルを分離する VPN に割り当てられます。これにより、ある VPN のユーザは、明示的に設定しない限り、別の VPN にデータを送信できなくなります。トラフィックが WAN を介して送信される場合、ESP ヘッダーの後にラベルが挿入され、リモート宛先に到達したときにユーザのトラフィックが属する VPN を識別します。

図 2. エンドツーエンドのセグメンテーション



- 集中管理：vManage は、Day0、Day1、Day2 運用の一元管理として、一元化された障害、設定、アカウンティング、パフォーマンス、およびセキュリティ管理を提供します。vManage は、ユビキタスポリシーとテンプレートを使用して運用を簡素化し、導入を合理化することで、変更管理と導入の時間を短縮します。

導入の詳細については、次を参照してください。

- 『SD-WAN End-to-End Deployment Guide』
- 『SD-WAN Controller Certificates and Authorized Serial Number File Deployment Guide』
- 『Cisco SD-WAN：WAN Edge Onboarding Deployment Guide』
- 『Cisco SD-WAN：Enabling Firewall and IPS for Compliance』
- 『SD-WAN：Administrator-Triggered Cluster Failover Deployment Guide』

アプリケーション パフォーマンスの最適化

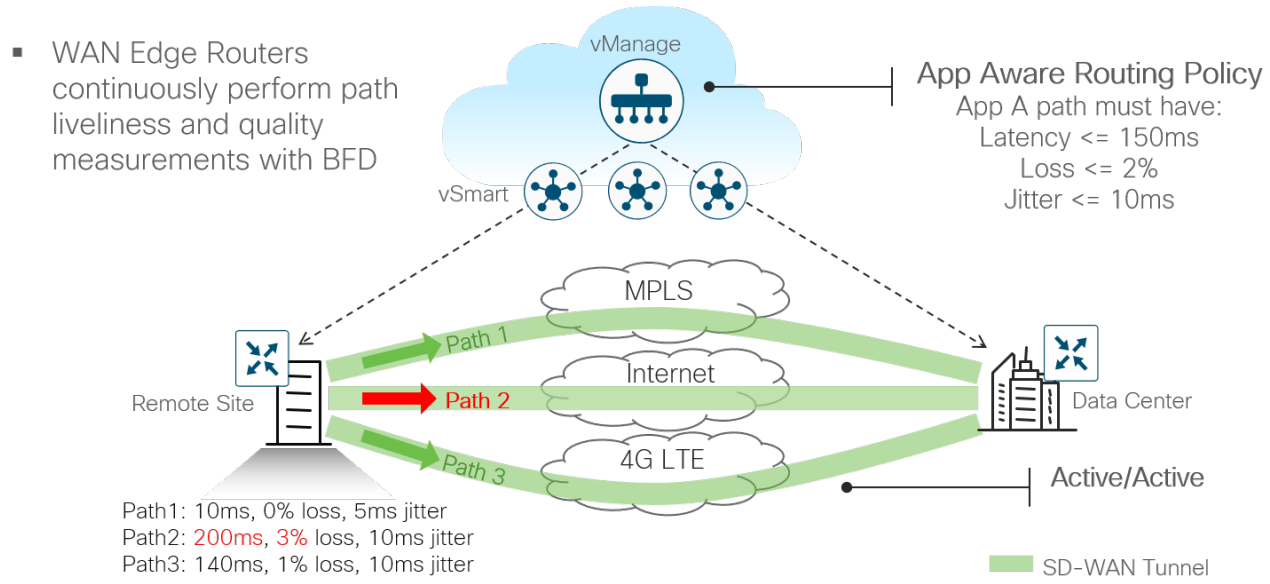
エンドユーザのアプリケーション パフォーマンスに影響を与える可能性のあるさまざまなネットワークの問題があります。これには、パケット損失、輻輳した WAN 回線、遅延が大きい WAN リンク、最適ではない WAN パス選択などがあります。高いユーザ生産性を実現するには、アプリケーション エクスペリエンスを最適化することが重要です。Cisco SD-WAN ソリューションは、損失、ジッター、および遅延を最小限に抑え、WAN の遅延と転送エラーを克服して、アプリケーション パフォーマンスを最適化します。

次の Cisco SD-WAN 機能は、アプリケーション パフォーマンスの最適化に役立ちます。

- アプリケーション認識型ルーティング：アプリケーション認識型ルーティングでは、トラフィック用にカスタマイズされた SLA ポリシーを作成し、BFD プローブによって取得されたリアルタイムのパフォーマンスを測定できます。アプリケーション トラフィックは、そのアプリケーションの SLA をサポートする WAN リンクに転送されます。パフォーマンスが低下している間は、SLA を超えると、トラフィックを他のパスに転送できます。

次の図は、アプリケーション A で、パス 1 と 3 は有効なパスですが、パス 2 は SLA に適合していないため、アプリケーション A のトラフィックを転送するためのパス選択では使用されないことを示しています。

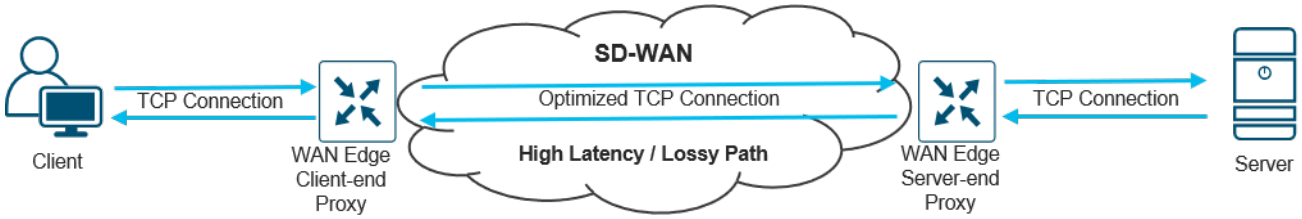
図 3. アプリケーション認識型ルーティング：パフォーマンスベースのパス選択によるトラフィックの保護



- Quality of Service（QoS）：QoS には、WAN ルータインターフェイス上のトラフィックの分類、スケジューリング、キューイング、シェーピング、およびポリシングが含まれます。この機能は、重要なアプリケーションフローの遅延、ジッター、およびパケット損失を最小限に抑えるように設計されています。
- 前方誤り訂正（FEC）とパケット複製：両方の機能はパケット損失の軽減に使用されます。FEC では、送信側 WAN エッジは 4 つのデータパケットごとにパリティパケットを挿入し、受信側 WAN エッジはパリティ値に基づいて失われたパケットを再構築できます。パケット複製では、送信側 WAN エッジは選択された重要なアプリケーションのすべてのパケットを一度に 2 つのトンネル経由で複製し、受信側 WAN エッジは重要なアプリケーションフローを再構築して重複パケットを廃棄します。

- TCP 最適化とセッション永続性：これらの機能は、長距離または高遅延の衛星リンクなどの、高遅延と低スループットに対処できます。TCP 最適化では、WAN エッジルータはクライアントとサーバ間の TCP プロキシとして機能します。セッションの永続性では、TCP の要求と応答のペアごとに新しい接続を作成する代わりに、単一の TCP 接続を使用して複数の要求と応答を送受信します。

図 4. TCP 最適化



導入の詳細については、次を参照してください。

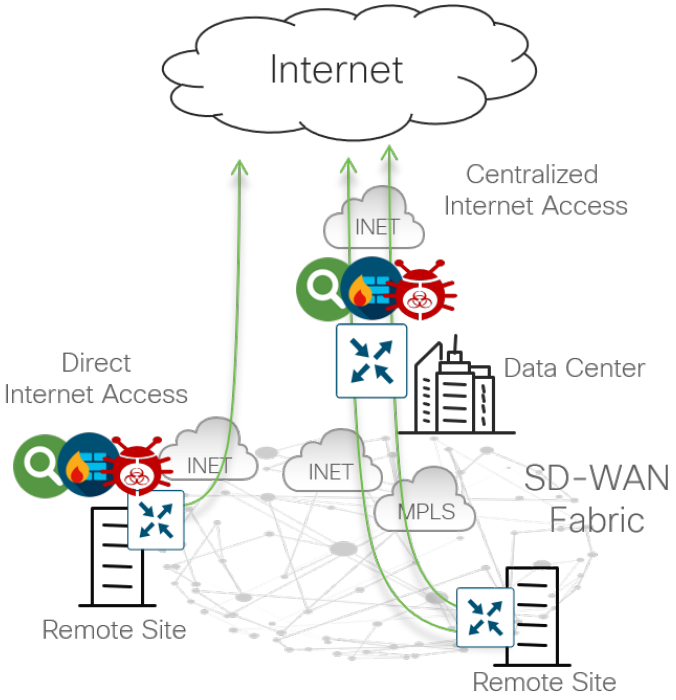
『Cisco SD-WAN：Application-Aware Routing Deployment Guide』

セキュアなダイレクト インターネット アクセス

従来の WAN では、ブランチサイトからのインターネットトラフィックは中央のデータセンターサイトにバックホールされ、そこでリターントラフィックがブランチに送り返される前に、セキュリティスタックによってトラフィックをスクラビングできます。徐々にアプリケーションにクラウドサービスを利用する企業が増加し、より多くのアプリケーションがインターネットベースになるにつれて、インターネットトラフィックの需要は増加していきます。セントラルサイトにトラフィックをバックホールすると、セントラルサイトのセキュリティおよびネットワークデバイスとリンクの帯域幅使用率が増加し、アプリケーション パフォーマンスに影響する遅延が増大します。

ダイレクト インターネット アクセス（DIA）は、VPN からのインターネット宛トラフィック（すべてのトラフィックまたはトラフィックのサブセット）がリモートサイトからローカルに出るようにすることで、これらの問題の解決に役立ちます。

図 5. 集中型インターネットアクセスとダイレクト インターネット アクセス



リモートサイトのトラフィックはインターネットの脅威に対するセキュリティを必要とするため、DIA はセキュリティ上の課題を引き起こす可能性があります。Cisco SD-WAN は、IOS XE SD-WAN デバイスの組み込み SD-WAN セキュリティ機能を利用するか、Cisco Umbrella クラウドであるセキュア インターネット ゲートウェイ（SIG）を利用することで、この問題を解決できます。

IOS XE SD-WAN セキュリティ機能には、エンタープライズ アプリケーション認識型ファイアウォール、侵入検知システム（IDS）/侵入防御システム（IPS）、DNS/Web レイヤセキュリティ、URL フィルタリング、SSL プロキシ、および高度なマルウェア防御（AMP）が含まれます。vEdge ルータは、アプリケーション認識型ファイアウォールをネイティブにサポートします。Cisco Umbrella クラウドは、複数のセキュリティ機能を統合し、クラウドベースのサービスとして提供します。これらの機能には、セキュア Web ゲートウェイ、DNS レイヤセキュリティ、クラウド提供ファイアウォール、クラウド アクセス セキュリティ ブローカ機能、脅威インテリジェンスが含まれます。詳細については、https://umbrella.cisco.com/products/secure-internet-gateway を参照してください。

設計と導入の詳細については、次を参照してください。

『SD-WAN Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices』
『SD-WAN：Enabling Direct Internet Access Deployment Guide』
『SD-WAN：Secure Direct Cloud Access for Cisco IOS-XE SD-WAN Devices Deployment Guide』
『SD_WAN：Secure Direct Internet Access for Cisco IOS-XE SD-WAN Devices Deployment Guide』
『SD-WAN：Secure Guest Access for Cisco IOS-XE SD-WAN Devices Deployment Guide』

マルチクラウド接続

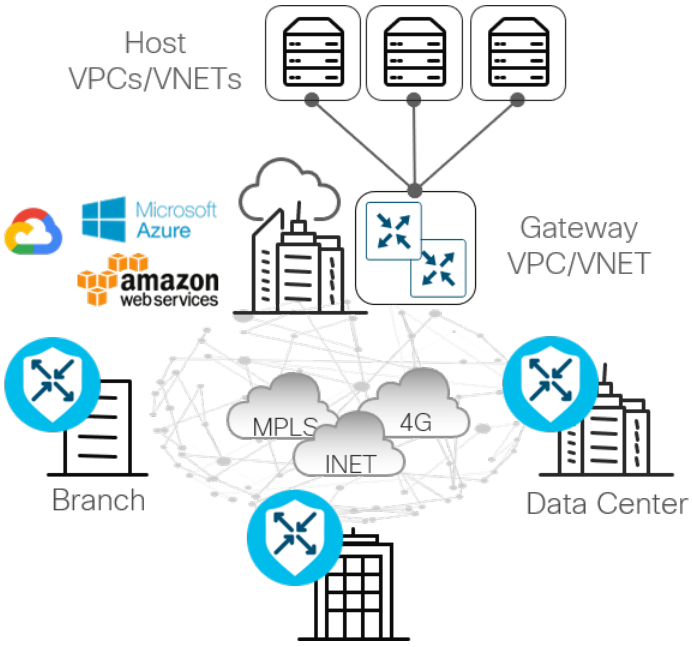
アプリケーションは複数のクラウドに移動し、複数のトランスポートを介して到達可能です。マルチクラウド接続の使用例カテゴリでは、IaaS または SaaS クラウドアプリケーションを最適なパスでリモートサイトに接続する方法と、セキュリティサービスを適用できる地域のコロケーション/交換ポイントを介して接続する方法を扱います。

次の使用例は、このカテゴリに関連付けられています。

- Infrastructure-as-a-Service（IaaS）：IaaS は、インターネット経由でパブリッククラウド（AWS や Azure など）で利用可能なネットワーク、コンピューティング、およびストレージのリソースをオンデマンドでエンドユーザに提供します。従来、ブランチが IaaS リソースに到達するために、パブリック クラウド データ センターへのダイレクトアクセスはありませんでした。これは、通常、データセンターまたはコロケーションサイトを介したアクセスを必要とするためです。さらに、ブランチからパブリッククラウドへの一貫したセグメンテーションまたは QoS ポリシーがない状態で、プライベート クラウド データ センターの IaaS リソースに到達するために MPLS に依存していました。

  Cisco Cloud onRamp for IaaS は、データセンターまたはブランチからパブリッククラウドのワークロードへの接続を自動化する機能です。これは、SD-WAN オーバーレイの一部となる WAN エッジルータインスタンスを自動的にパブリッククラウドに導入し、データセンターまたはブランチにあるルータへのデータプレーン接続を確立します。SD-WAN の全機能をクラウドに拡張し、SD-WAN ファブリックとクラウド全体に共通のポリシーフレームワークを拡張します。Cisco Cloud onRamp for IaaS は、データセンターを通過する必要がある SD-WAN サイトからのトラフィックを排除し、パブリッククラウドでホストされるアプリケーションのパフォーマンスを向上させます。また、中継 VPC/VNET 構成で仮想ルータのペアを導入することで、クラウドでホストされるアプリケーションに高可用性とパスの冗長性を提供します。これはコスト効率も非常に良いものです。

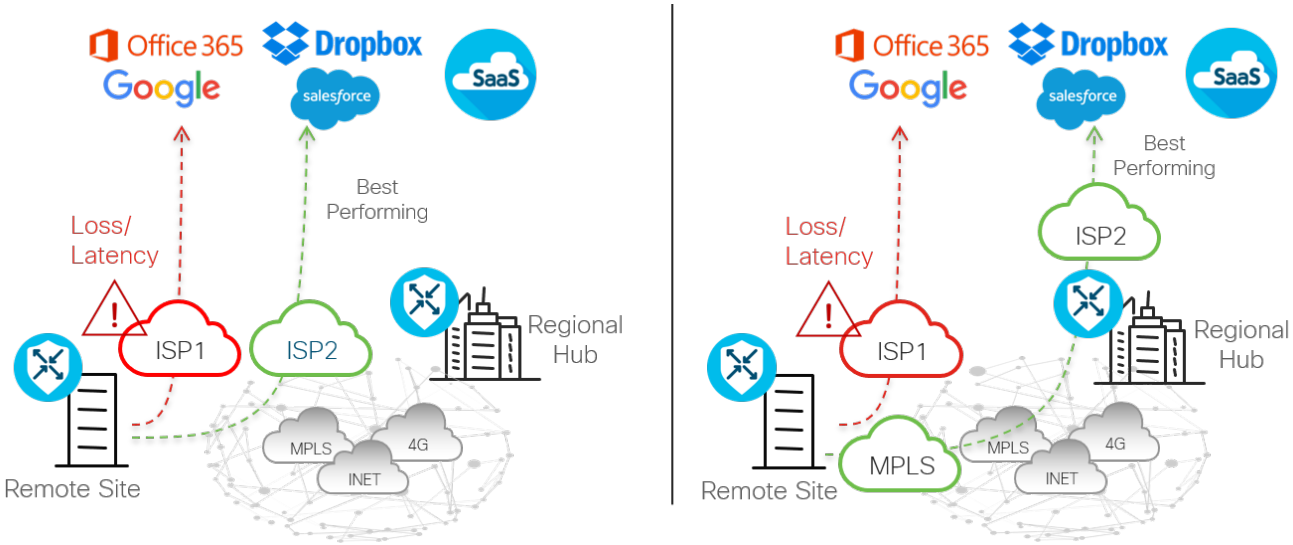
図 6. Cloud onRamp for IaaS：SD-WAN ファブリックをクラウド サービス プロバイダーに安全に拡張



- Software-as-a-Service（SaaS）：従来、ブランチは一元化されたデータセンターを介して SaaS アプリケーション（Salesforce、Box、Office 365 など）にアクセスしてきました。その結果、アプリケーションの遅延が増大し、ユーザエクスペリエンスが予測不能になっていました。SD-WAN の進化に伴い、ダイレクト インターネット アクセスや、地域ゲートウェイまたはコロケーションサイトを介したアクセスなど、SaaS アプリケーションにアクセスするための追加のネットワークパスが可能になりました。ただし、ネットワーク管理者は、リモートサイトから SaaS アプリケーションのパフォーマンスを限定的にしか把握できない、またはまったくできない場合があります。そのため、エンドユーザ エクスペリエンスを最適化するために SaaS アプリケーションにアクセスするネットワークパスを選択することが問題となる可能性があります。また、ネットワークの変更や障害が発生した場合、影響を受けるアプリケーションを代替パスに簡単に移動する方法はありません。

  Cloud onRamp for SaaS を使用すると、インターネットから直接、またはゲートウェイロケーションを介して、SaaS アプリケーションへのアクセスを簡単に設定できます。各 SaaS アプリケーションへの各パスのパフォーマンスを継続的にプローブ、測定、およびモニタし、損失と遅延に基づいて最適なパフォーマンスのパスを選択します。障害が発生した場合、SaaS トラフィックは更新された最適なパスに動的かつインテリジェントに移動されます。

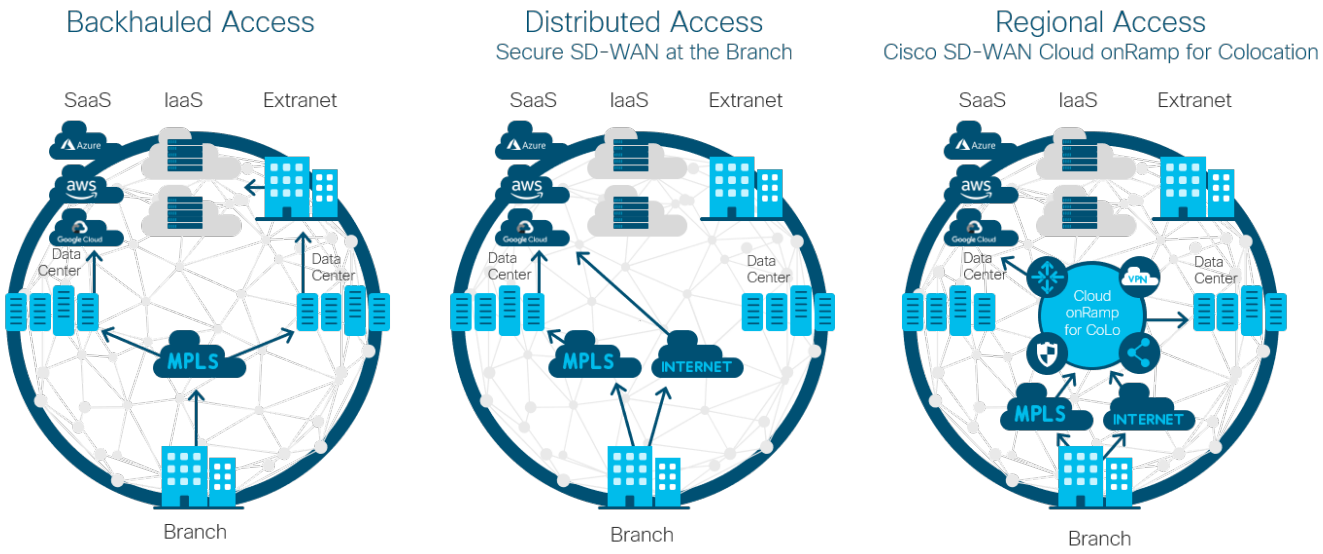
図 7. Cloud onRamp for SaaS：ベストパフォーマンスパスの選択



- 地域型マルチクラウドアクセス：従来の WAN は、セントラルサイトへのトラフィックのバックホールを利用し、そこでのセキュリティデバイスの一元化されたプロビジョニングに依存してトラフィックをスクラブします。これにより、セントラルサイトでの帯域幅要件が増加し、アプリケーションの遅延が増大します。DIA は、ブランチユーザがブランチからインターネットリソースおよび SaaS アプリケーションに直接アクセスできるようにすることで、これらの問題を軽減し、ユーザエクスペリエンスを向上させます。この分散型アプローチは効率的で非常に有益ですが、規制機関や企業のセキュリティポリシーにより、ブランチからのインターネットへのアクセスが禁止されている組織も多くあります。これらの組織では、Cloud onRamp for Colocation を使用することで、ネットワークの戦略的なポイントでコロケーションを利用してネットワークとセキュリティスタックを統合し、遅延を最小限に抑えることにより、問題に対するハイブリッドアプローチが可能になります。

コロケーションセンターは、組織が機器スペースを借りて、さまざまなネットワークおよびクラウド サービス プロバイダーに接続できるパブリックデータセンターです。エンドユーザの近くに戦略的に選択されたコロケーションは、パブリックおよびプライベート クラウド リソースへの高速アクセスを実現し、プライベート データセンターを使用するよりもコスト効率が高くなります。

図 8. 集中型、分散型、地域型のマルチクラウドアクセス



コロケーションでは、複数のネットワーク機能（WAN エッジルータ、プロキシ、ファイアウォール、ロードバランサ、IDS/IPS など）を仮想化できます。これらのサービスは残りの SD-WAN ネットワークにアナウンスされ、必要に応じて制御ポリシーとデータポリシーを使用して、これらのコロケーションリソースを介してトラフィックに影響を与えることができます。

導入の詳細については、次を参照してください。

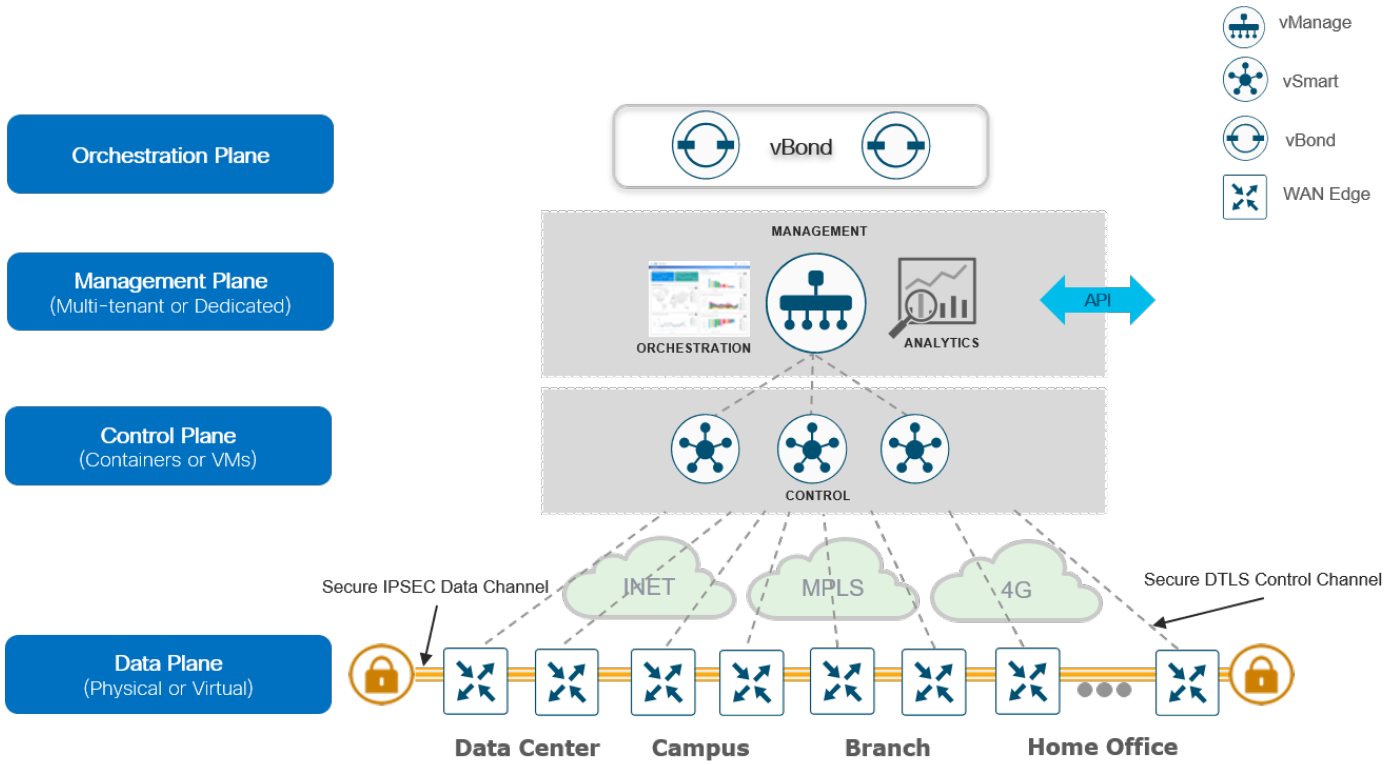
- 『SD-WAN：Enabling Cisco Cloud onRamp for IaaS with AWS Deployment Guide』
- 『SD-WAN：Cloud onRamp for SaaS Deployment Guide』

アーキテクチャとコンポーネント

Cisco SD-WAN ソリューションは、個別のオーケストレーション、管理、コントロール、およびデータの各プレーンで構成されています。

- オーケストレーション プレーンは、SD-WAN オーバーレイへの SD-WAN ルータの自動オンボーディングを支援します。
- 管理プレーンは、中央構成とモニタリングの役割を担います。
- コントロールプレーンは、ネットワークトポロジを構築して維持し、トラフィックが流れる場所を決定します。
- データプレーンは、コントロールプレーンからの決定に基づいてパケットを転送する役割を担います。

図 9. Cisco SD-WAN ソリューションプレーンの概要



コンポーネント

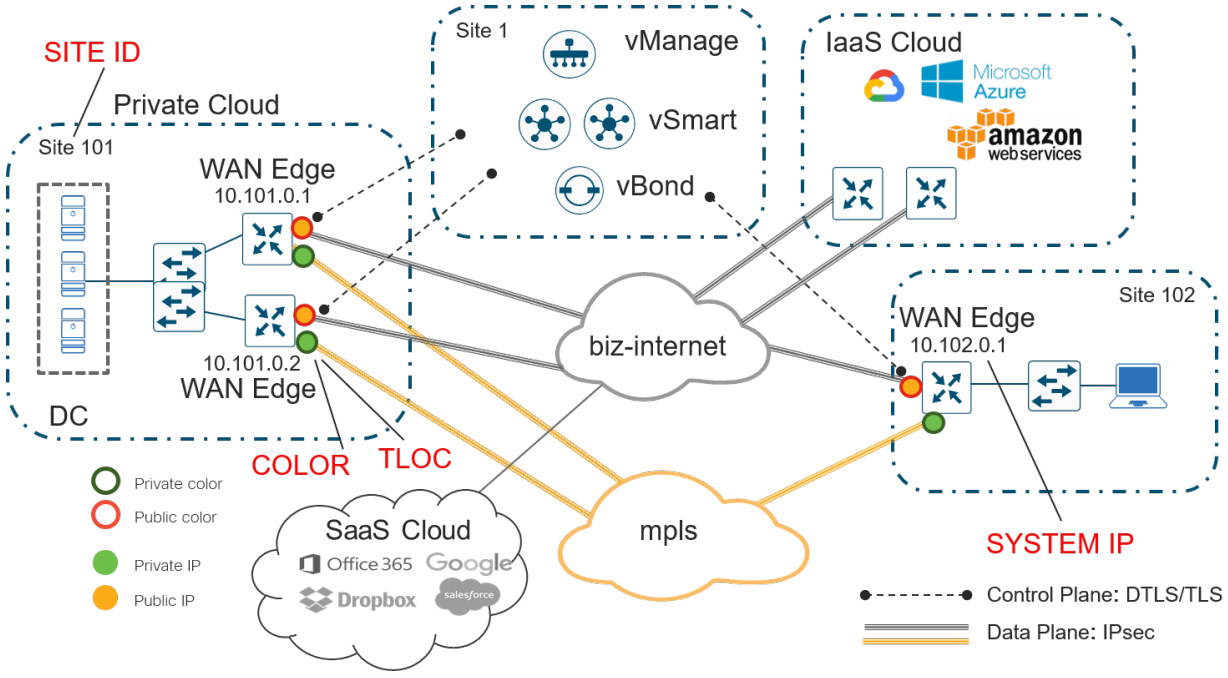
Cisco SD-WAN ソリューションの主要なコンポーネントは、vManage ネットワーク管理システム（管理プレーン）、vSmart コントローラ（コントロールプレーン）、vBond オーケストレータ（オーケストレーション プレーン）、および WAN エッジルータ（データプレーン）で構成されます。

- vManage：この集中型ネットワーク管理システムは、ソフトウェアベースで、アンダーレイおよびオーバーレイネットワーク内のすべての Cisco SD-WAN デバイスと接続されたリンクを容易にモニタ、設定、および維持するための GUI インターフェイスを提供します。Day0、Day1、Day2 運用の一元管理を提供します。

- vSmart コントローラ：このソフトウェアベースのコンポーネントは、SD-WAN ネットワークの集中型コントロールプレーンの役割を担います。このコンポーネントは、各 WAN エッジルータへのセキュアな接続を維持し、Overlay Management Protocol（OMP）を介してルートおよびポリシー情報を配布し、ルートリフレクタとして動作します。また、WAN エッジルータから発信される暗号キー情報を反映することで、WAN エッジルータ間のセキュアなデータプレーン接続を調整し、非常にスケーラブルな IKE レスアーキテクチャを実現します。
- vBond オーケストレータ：このソフトウェアベースのコンポーネントは、WAN エッジデバイスの初期認証を実行し、vSmart、vManage、および WAN エッジ接続を調整します。また、ネットワークアドレス変換（NAT）の背後にあるデバイス間の通信を可能にするための重要な役割も担います。
- WAN エッジルータ：このデバイスは、ハードウェアアプライアンスまたはソフトウェアベースのルータとして使用でき、物理サイトまたはクラウドに配置され、1 つ以上の WAN トランスポートを介してサイト間でセキュアなデータプレーン接続を提供します。トラフィック転送、セキュリティ、暗号化、Quality of Service（QoS）、Border Gateway Protocol（BGP）や Open Shortest Path First（OSPF）などのルーティングプロトコルを担当します。

次の図は、Cisco SD-WAN ソリューションのいくつかの側面を示しています。このサンプルトポロジは、プライベート MPLS トランスポートとパブリック インターネット トランスポートにそれぞれ直接接続された 2 つの WAN エッジサイトを示しています。クラウドベースの SD-WAN コントローラ（2 つの vSmart コントローラ、vBond オーケストレータ、vManage サーバ）は、インターネット トランスポートを介して直接到達できます。さらに、このトポロジには、SaaS および IaaS アプリケーションへのクラウドアクセスも含まれます。

図 10.　　SD-WAN トポロジの例



WAN エッジルータは、vSmart コントローラへの永続的 Datagram Transport Layer Security（DTLS）または Transport Layer Security（TLS）制御接続を形成し、各トランスポートを介して両方の vSmart コントローラに接続します。ルータは、vManage サーバへの永続的な DTLS または TLS 制御接続も形成しますが、トランスポートの 1 つだけを介します。WAN エッジルータは、各トランスポートで IPsec トンネルを使用して他の WAN エッジルータと安全に通信します。Bidirectional Forwarding Detection（BFD）プロトコルはデフォルトで有効になっており、これらの各トンネルで実行され、損失、遅延、ジッター、およびパスの障害を検出します。

サイト ID

サイト ID は、数値 1 ～ 4294967295（2^32-1）を持つ SD-WAN オーバーレイネットワーク内のサイトの一意の識別子であり、アドバタイズされたプレフィックスの送信元の場所を識別します。この ID は、コントローラを含むすべての WAN エッジデバイスで設定する必要があり、同じサイトに存在するすべての WAN エッジデバイスで同じである必要があります。サイトには、データセンター、ブランチオフィス、キャンパスなどがあります。デフォルトでは、同じサイト ID を共有する同じサイト内の WAN エッジルータ間で IPsec トンネルは形成されません。

システム IP

システム IP は、インターフェイスアドレスとは無関係にデバイスを一意に識別する永続的なシステムレベルの IPv4 アドレスです。ルータ ID のように機能するため、アンダーレイでアドバタイズまたは認識される必要はありません。VPN 0 に存在するシステムインターフェイスに割り当てられ、アドバタイズされることはありません。ただし、ベストプラクティスは、このシステム IP アドレスをループバック インターフェイスに割り当て、任意のサービス VPN でアドバタイズすることです。その後、SNMP およびロギングの送信元 IP アドレスとして使用できるため、ネットワークイベントと vManage 情報の関連付けが容易になります。

組織名

組織名は、SD-WAN オーバーレイに割り当てられる名前です。大文字と小文字が区別され、オーバーレイ内のすべての SD-WAN デバイスで設定されている組織名と一致する必要があります。これは、SD-WAN デバイスがオーバーレイネットワークに導入されたときに、証明書認証プロセスで照合するための組織単位（OU）フィールドを定義するために使用されます。

パブリック IP アドレスとプライベート IP アドレス

プライベート IP アドレス

WAN エッジルータでは、プライベート IP アドレスは SD-WAN デバイスのインターフェイスに割り当てられた IP アドレスです。これは、NAT 前のアドレスであり、名前にかかわらず、パブリックアドレス（パブリックにルーティング可能）またはプライベートアドレス（RFC 1918）のいずれかです。

パブリック IP アドレス

vBond オーケストレータによって検出された NAT 後のアドレス。このアドレスは、パブリックアドレス（パブリックにルーティング可能）またはプライベートアドレス（RFC 1918）のいずれかです。NAT がない場合、SD-WAN デバイスのプライベート IP アドレスとパブリック IP アドレスは同じです。

TLOC

TLOC（トランスポートロケーション）は、WAN エッジルータが WAN トランスポートネットワークに接続する接続ポイントです。TLOC は一意に識別され、システム IP アドレス、リンクの色、およびカプセル化（Generic Routing Encapsulation（GRE）または IPsec）で構成される 3 つのタプルで表されます。

色

色属性は、WAN エッジルータまたは vManage および vSmart コントローラに適用され、個々の TLOC の識別に役立ちます。異なる TLOC には異なる色のラベルが割り当てられます。図 10 の SD-WAN トポロジの例では、インターネット トランスポート TLOC に biz-internet と呼ばれるパブリックカラーを使用し、他のトランスポート TLOC には mpls と呼ばれるプライベートカラーを使用します。単一の WAN エッジルータに同じカラーを 2 回使用することはできません。

オーバーレイ マネジメント プロトコル（OMP）

BGP と同様の構造を持つ OMP ルーティングプロトコルは、SD-WAN オーバーレイネットワークを管理します。このプロトコルは vSmart コントローラ間と、vSmart コントローラと WAN エッジルータ間で動作します。ここでは、ルートプレフィックス、ネクストホップルート、暗号キー、ポリシー情報などのコントロールプレーン情報がセキュアな DTLS または TLS 接続を介して交換されます。vSmart コントローラは、BGP ルートリフレクタと同様に機能します。WAN エッジルータからルートを受信し、それらにポリシーを適用して処理し、オーバーレイネットワーク内の他の WAN エッジルータにルートをアドバタイズします。

バーチャル プライベート ネットワーク（VPN）

SD-WAN オーバーレイでは、仮想プライベートネットワーク（VPN）がセグメンテーションを提供します。すでによく知られている仮想ルーティングおよびフォワーディング（VRF）によく似ています。各 VPN は相互に分離されており、それぞれに独自のフォワーディングテーブルがあります。インターフェイスまたはサブインターフェイスは、単一の VPN で明示的に設定され、複数の VPN の一部になることはできません。ラベルは、OMP ルート属性、およびパケットが属する VPN を識別するパケットのカプセル化で使用されます。

VPN 番号は、0 ～ 65535 の値を持つ 4 バイトの整数ですが、複数の VPN が内部使用のために予約されているため、設定できる、または設定する必要がある VPN の最大数は 65527 です。WAN エッジデバイスとコントローラには、デフォルトで 2 つの主要な VPN、VPN 0 と VPN 512 があります。VPN 0 および 512 は、vManage および vSmart コントローラで設定できる唯一の VPN であることに注意してください。vBond オーケストレータでは、さらに多くの VPN を設定できますが、機能し、使用する必要があるのは VPN 0 と VPN 512 だけです。

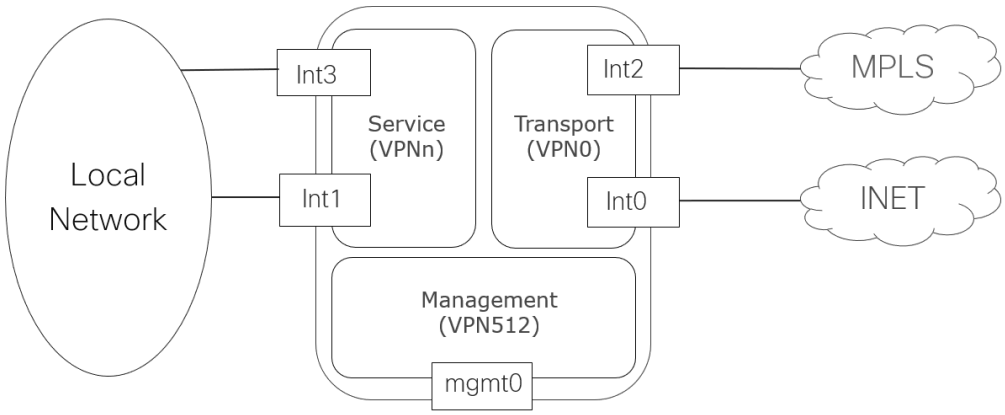
- VPN 0 はトランスポート VPN です。これには、WAN トランスポートに接続するインターフェイスが含まれています。コントローラへのセキュアな DTLS / TLS 接続は、この VPN から開始されます。コントロールプレーンを確立し、IPsec トンネルトラフィックがリモートサイトに到達できるように、適切なネクストホップ情報を取得するために、この VPN 内でスタティックまたはデフォルトルート、あるいはダイナミック ルーティング プロトコルを設定する必要があります。
- VPN 512 は管理 VPN です。Cisco SD-WAN デバイスとの間でアウトオブバンド管理トラフィックを伝送します。この VPN は OMP によって無視され、オーバーレイネットワークで伝送されません。

すでに定義されているデフォルト VPN に加えて、ローカルサイトネットワークに接続し、ユーザデータトラフィックを伝送するインターフェイスを含む 1 つ以上のサービス側 VPN を作成する必要があります。1 ～ 511 の範囲でサービス VPN を選択することをお勧めしますが、デフォルトおよび予約済み VPN と重複しない限り、より大きな値を選択できます。サービス VPN は、OSPF または BGP、Virtual Router Redundancy Protocol（VRRP）、QoS、トラフィックシェーピング、ポリシングなどの機能に対して有効にできます。サイトの vSmart コントローラから受信した OMP ルートをサービス側 VPN ルーティングプロトコルに再配布することで、ユーザトラフィックを IPsec トンネル経由で他のサイトに転送できます。次に、サービス VPN ルートを OMP ルーティングプロトコルにアドバタイズすることで、ローカルサイトからのルートを他のサイトにアドバタイズできます。OMP ルーティングプロトコルは vSmart コントローラに送信され、ネットワーク内の他の WAN エッジルータに再配布されます。

次の図は、WAN エッジルータ上の VPN を示しています。インターフェイス Int0 および Int2 は、トランスポート VPN の一部です。Int1 と Int3 は、サイトのローカルネットワークに接続されたサービス VPN の一部です。mgmt0 ポートは VPN 512 の一部です。

技術的なヒント
任意のインターフェイスをサブインターフェイスにすることもできます。この場合、サブインターフェイスが属するメイン（または親）物理インターフェイスは、VPN 0 で設定する必要があります。また、サブインターフェイスの MTU は、802.1Q タグにより、物理インターフェイスより 4 バイト小さくする必要があります。この要件を満たすには、メインインターフェイスの MTU を 1504 に設定し、サブインターフェイスの MTU をデフォルト（1500）のままにします。

図 11.　　WAN エッジルータ上の VPN



注：上記は、vEdge ルータ上で vManage 設定を介して VPN が直接表示される方法を示しています。設定が vManage から IOS XE SD-WAN ルータにプッシュされると、IOS XE SD-WAN ソフトウェアパーサーで受け入れられる形式に自動的に変換されます。いくつかの違いは次のとおりです。

- VPN キーワードの代わりに VRF 用語が使用されます
- グローバルテーブルは、VPN 0 を表すために使用されます
- VRF Mgmt-intf は管理インターフェイスでデフォルトで有効になっており、VPN 512 を表すために使用されます

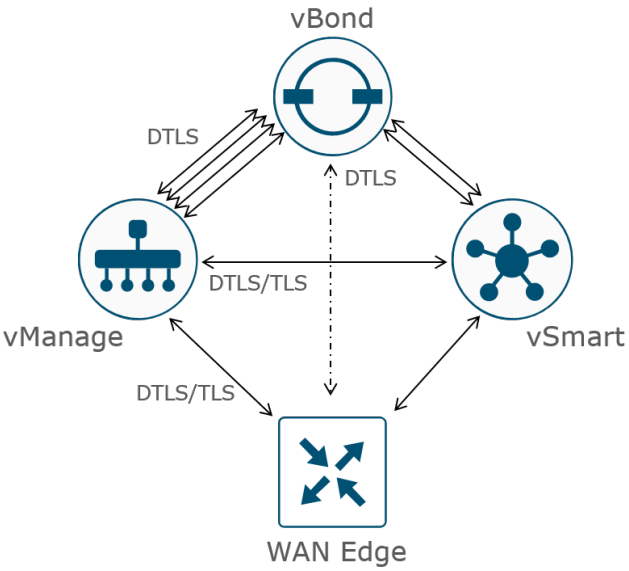
技術的なヒント
IOS XE ルータは VRF 定義の名前を受け入れますが、IOS XE SD-WAN コードでは、VRF 定義は数字のみである必要があります。

コントロールプレーン

制御接続

Cisco SD-WAN vManage および vSmart コントローラは、最初に vBond コントローラに接続して認証し、永続的な DTLS 接続を形成します。その後、相互に永続的な DTLS/TLS 接続を確立して維持します。WAN エッジデバイスも同様の方法でオンボードしますが、vManage と vSmart コントローラとの一時的な vBond 接続をドロップし、DTLS/TLS 接続を維持します。次の図は、これを図で表したものです。

図 12.　　SD-WAN 制御接続



技術的なヒント
vBond への制御接続は常に DTLS です。デフォルトでは、vManage と vSmart への接続も DTLS ですが、これはセキュリティ制御プロトコルの TLS を設定することで、任意のデバイスで変更できます。1 つのデバイスが TLS 用に設定され、別のデバイスが DTLS 用に設定されている場合、2 つのデバイス間の制御接続に TLS が選択されます。TLS は TCP を使用するため推奨されます。TCP は確認応答を使用して信頼性を高めます。TCP も接続指向であるため、ファイアウォールは接続の状態を維持し、明示的にトラフィックを許可することなく、リターントラフィックを許可できます。

注：vManage および vSmart の各コア（最大 8）は、vManage と各 vSmart コントローラ間で単一の接続が維持されている間、各 vBond（単一のコアを持つ）への制御接続を開始して維持します。たとえば、vSmart に 2 つの vCPU がある場合（2 つのコアに変換されます）、vSmart から各 vBond への合計 2 つの制御接続が維持されます（各コアから 1 つ）。vManage に 4 つの vCPU がある場合（4 つのコアに変換されます）、vManage から各 vBond への合計 4 つの制御接続が維持されます（各コアから 1 つ）。各 vSmart から vSmart コントローラ、および vManage から vManage サーバの間に形成される制御接続は 1 つだけです。冗長 vBond オーケストレータ間で制御接続は形成されません。

WAN エッジ制御接続

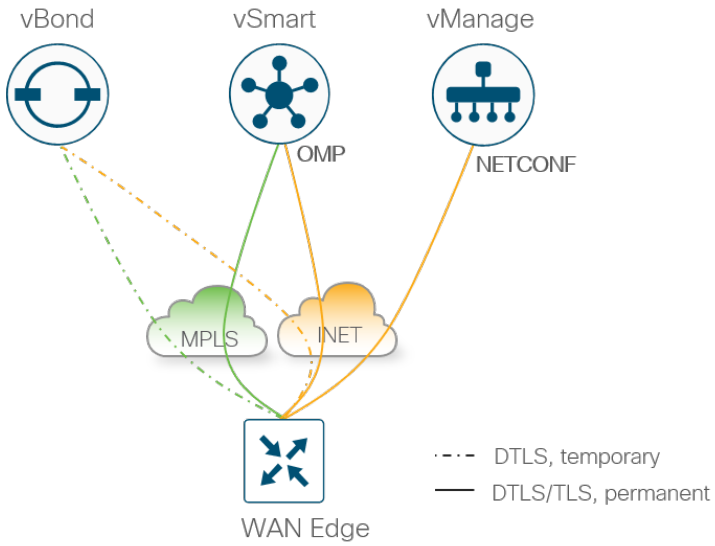
WAN エッジルータは、デフォルトでは、プロビジョニングされたすべてのトランスポートで制御接続を確立しようとします。まず、各トランスポートで vBond オーケストレータとの接続を開始してから、他のコントローラへの接続を試みます。複数の vBond オーケストレータが存在する場合、トランスポートごとに 1 つの vBond 制御接続のみが確立されます。トランスポートは、一度に 1 つずつ試行されます。通常は、最も小さいポート番号に接続されたトランスポートから開始されます。WAN エッジルータは、各トランスポートを介して vSmart コントローラへの永続的な接続を確立し、1 つのトランスポートを介して vManage への単一の永続的な接続を確立します。これは、接続を確立する最初の WAN エッジルータです。その後、vBond 接続が終了します。WAN エッジルータはすべての vSmart コントローラに接続する必要はなく、ネットワークの冗長性の設計と設定に依存します。技術的には、WAN エッジルータがコントロールプレーン情報を受信するには、1 つのトランスポートを介した vSmart コントローラへの単一の接続で十分ですが、冗長性を確保するために、通常は複数のトランスポートを介した追加の vSmart コントローラが設定されます。WAN エッジルータが vManage クラスタに接続する場合、制御接続は 1 つの vManage インスタンスにハッシュされ、すべてのメンバーとの接続を確立する必要はありません。

技術的なヒント
すべての vSmart コントローラ接続が失われた場合、WAN エッジルータは OMP グレースフル リスタート タイマー（デフォルトでは 12 時間）の間、最新のコントロールプレーン情報を使用して動作し続けます。

セキュアな接続が確立されると、vManage が NETCONF を使用して WAN エッジデバイスをプロビジョニングし、vSmart と WAN エッジの間で OMP ピアリングが確立されます。OMP ピアリングはシステム IP を使用して確立され、複数の DTLS/TLS 接続が存在する場合でも、WAN エッジデバイスと vSmart コントローラの間で確立されるピアリングセッションは 1 つだけです。

技術的なヒント
vManage への接続に使用されるトランスポートは 1 つだけであるため、トンネルインターフェイスで **vmanage-connection-preference** パラメータをより高い値に設定することで、トランスポート設定に影響を与えることができます。デフォルト値は 5 です。値 0 は、トンネルを介して vManage への接続が行われないことを示すために使用されます。これは、LTE などの従量制リンクに実装されることがよくあります。

図 13.　　WAN エッジ制御接続



制御接続の概要

次に、コントローラと WAN エッジルータの制御接続の概要を示します。

- 各 vSmart コア（最大 8）と各 vBond オーケストレータ間の永続的な DTLS 接続
- 各 vManage コア（最大 8）と各 vBond オーケストレータ間の永続的な DTLS 接続
- 各 vManage と各 vSmart コントローラ間の永続的な TLS または DTLS 接続
- vSmart コントローラ間の TLS または DTLS 接続のフルメッシュ（各ペア間に 1 つの接続）
- vManage クラスタインスタンス間の TLS または DTLS 接続のフルメッシュ（各ペア間に 1 つの接続）*
- 各 WAN エッジと 1 つの vBond 間の一時的な DTLS 接続（各トランスポートに 1 つの接続）
- 各 WAN エッジと 1 つの vManage インスタンス間の永続的な TLS または DTLS 接続（1 つのトランスポートを介して 1 つの接続のみが選択されます）
- デフォルトでは、各 WAN エッジと 2 つの vSmart コントローラ間の永続的な TLS または DTLS 接続（各トランスポートを介したそれぞれへの接続**）

* vManage クラスタインスタンスの場合、例として統計専用であり、WAN エッジデバイスを処理しない一部のインスタンスは、トンネルインターフェイスなしで設定できるため、これらのインスタンスへの制御接続は構築されません。

** vSmart コントローラの場合、接続数は WAN エッジルータの **max-control-connections** および **max-omp-sessions** の設定によって異なります。

許可リストモデル

すべての WAN エッジデバイスとコントローラは、許可リストモデルを使用して相互に認証します。この場合、デバイスは、接続を確立してネットワークへのアクセスを許可する前に承認される必要があります。

vManage によって配布される 2 つの許可リストがあります。1 つはコントローラ用、もう 1 つは WAN エッジデバイス用です。

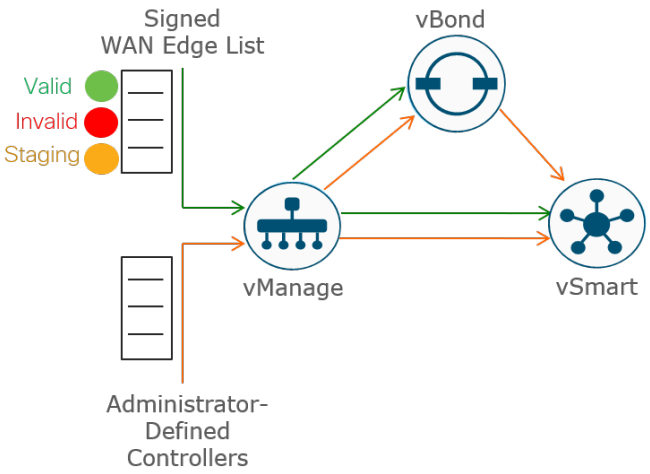
- 許可コントローラリスト：許可コントローラリストは、管理者が vManage ユーザインターフェイスにコントローラを手動で追加した結果です。このリストは、vManage からコントローラに配布され、その後 vBond から vSmart コントローラに配布されます。
- WAN エッジデバイスの許可シリアル番号リスト：WAN エッジデバイスのデジタル署名付き許可シリアル番号リストは、http://software.cisco.com のプラグアンドプレイ接続ポータルから変更および取得できます。リストは、SD-WAN オーバーレイの適切なスマートアカウントとバーチャルアカウントにアクセスできる有効な Cisco CCO アカウントを持つユーザが、vManage から手動で取得するか、自動的に同期できます。ファイルが vManage にアップロードまたは同期されると、vManage によってすべてのコントローラに配布されます。

  WAN エッジの許可シリアル番号リストを使用して、管理者は個々の WAN エッジルータのアイデンティティの信頼性を決定および設定できます。次のオプションがあります。

  - **[Valid]**：ルータは SD-WAN ネットワークで完全に動作することが許可されています。
  - **[Invalid]**：ルータは SD-WAN ネットワークで許可されていないため、コントローラとの制御接続は確立されません。
  - **[Staging]**：ルータはコントローラとの制御接続を認証および形成できますが、OMP は WAN エッジルータにルート、データポリシー、または TLOC を送信しないため、トラフィックは転送されません。この状態では、実稼働 SD-WAN ネットワークへの参加を許可する前に、ルータをプロビジョニングしてテストできます。

WAN エッジの許可シリアル番号リストが vManage にロードまたは同期されると、デバイスを検証するオプションが表示されます。リストをインポートする前にデバイスを検証するチェックボックスをオンにすると、すべてのデバイスがデフォルトで [Valid] になります。検証するチェックボックスをオンにしない場合、すべてのデバイスはデフォルトで [Invalid] になります。ルータがコントローラとの制御接続を形成し、SD-WAN ネットワークに参加する前に、各デバイスを [Valid] に設定する必要があります。

図 14.　　許可コントローラおよび WAN エッジのシリアル番号リスト



ID

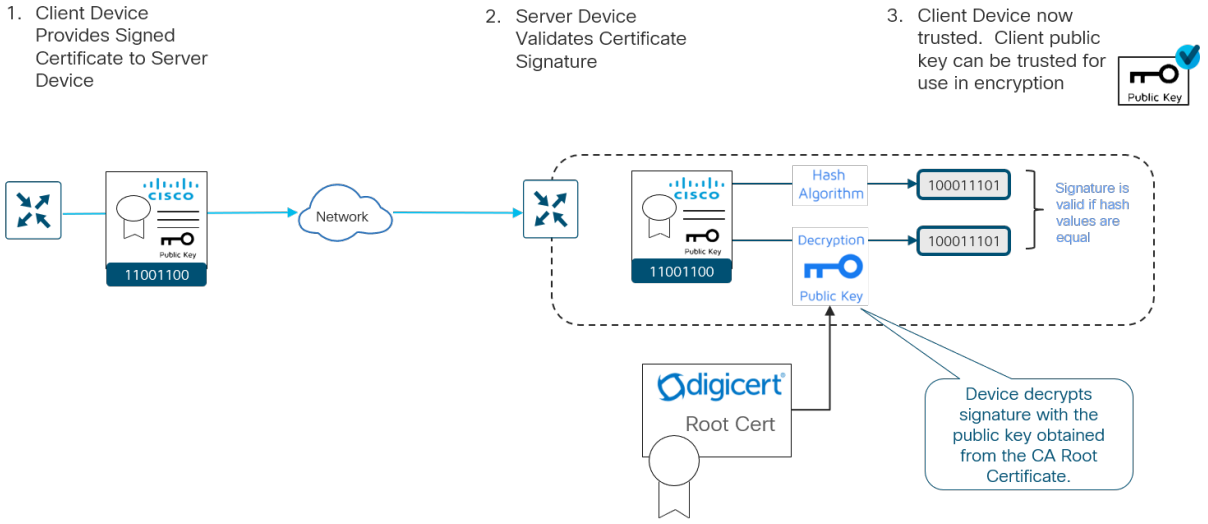
デバイス間の認証には、証明書を介したデバイス ID の検証が含まれます。

デバイス証明書の検証の仕組み：

- クライアントデバイスは、CA 署名付きデバイス証明書をサーバに提示します。
- サーバは、次の方法で証明書の署名を検証します
  1. 証明書データに対してハッシュアルゴリズムを実行して値を取得する
  2. CA ルート証明書から取得した公開キーを使用して証明書の署名を復号し、2 番目の値を取得する

  両方の値が等しい場合、署名は有効です。
- これでクライアントデバイスが信頼され、暗号化で使用するためにクライアント公開キーを信頼できるようになります。

図 15.　　証明書によるデバイス ID の検証



デバイス証明書を検証するには、対応するルート証明書が必要であることに注意してください。

コントローラ ID

コントローラ ID は、Symantec/Digicert またはシスコ署名付き証明書、あるいはエンタープライズ CA 証明書によって提供されます。ネットワーク内の各コントローラには、証明書が署名され、インストールされている必要があります。また、コントローラ証明書をインストールする前に、対応する CA のルート証明書チェーンも各コントローラにインストールする必要があります。同じ CA ルートを使用しないデバイスのデバイス証明書を検証するために、追加のルートチェーンがインストールされます。一部のルート証明書チェーンはプリロードされているか、自動的にインストールされます。また、エンタープライズルート CA などの他のルート証明書チェーンは管理者がインストールする必要があります。

WAN エッジルータ ID

vEdge ハードウェアルータの ID は、Avnet によって署名されたデバイス証明書によって提供され、製造プロセスで生成されて、トラステッド プラットフォーム モジュール（TPM）チップに焼き付けられます。Symantec/Digicert および Cisco ルート証明書は、コントローラの証明書を信頼するためにソフトウェアにプリロードされています。追加のルート証明書は、手動でロードするか、vManage によって自動的に配布するか、ZTP 自動プロビジョニングプロセス中にインストールできます。

IOS XE SD-WAN ハードウェアルータの ID は、ASR 1002-X を除き、安全な固有デバイス ID（SUDI）によって提供されます。これは、ハードウェアで保護されているキーペアに関連付けられた X.509v3 証明書です。Symantec/Digicert および Cisco ルート証明書は、コントローラの証明書を信頼するためにソフトウェアにプリロードされています。追加のルート証明書は、手動でロードするか、vManage NMS によって自動的に配布するか、プラグアンドプレイ（PnP）自動プロビジョニングプロセス中にインストールできます。

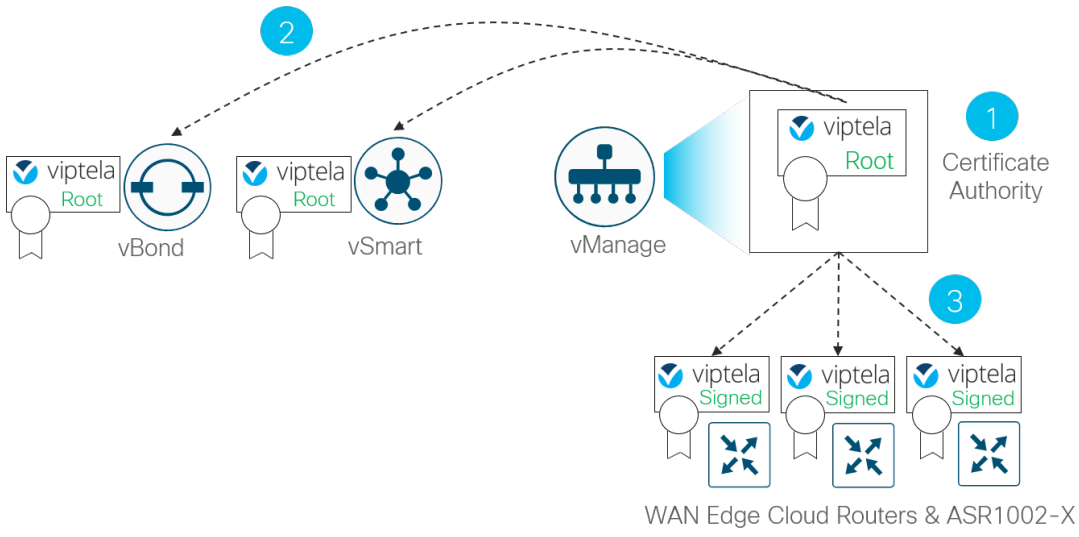
vEdge クラウドルータ、ISRv ルータ、CSR1000v ルータ、および Cisco ASR 1002-X ルータには、デバイス証明書がプリインストールされていません。各デバイスは、vManage によって生成され、一時的な ID を目的としてデバイスの導入時に設定されるワンタイムパスワード（OTP）/トークンを使用します。デバイスが一時的に認証されると、vManage によって永続的なアイデンティティが提供されます。vManage は、これらのデバイスの証明書を生成してインストールするための認証局（CA）として動作できます。

次の図に示します。

1. WAN エッジクラウドルータおよび ASR 1002-X の認証局（CA）として機能する vManage。
2. vManage は、Viptela ルート証明書を vBond と vSmart に配布して、WAN エッジクラウド ID を検証します。
3. WAN エッジルータが OTP 経由で認証されると、vManage CA は Viptela 署名付き証明書を発行し、それ以降は認証に使用されます。

vManage クラスタがある場合、各 vManage はデバイスの証明書に署名し、対応するルート証明書を配布します。

図 16.　　WAN エッジクラウドルータおよび ASR1002-X の vManage ルート CA



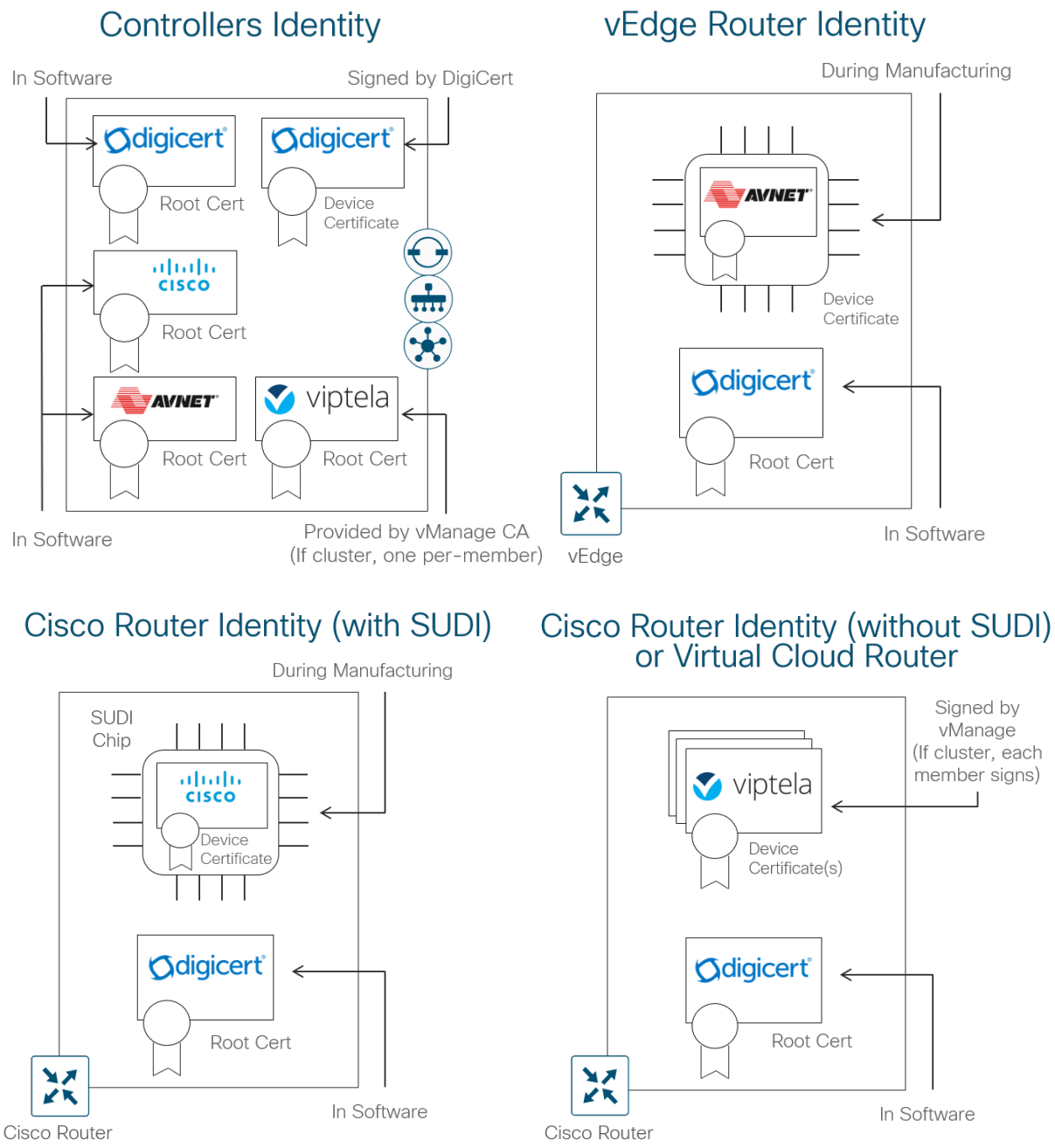
証明書

次に、さまざまな Cisco SD-WAN デバイスの認証用にインストールされたデバイスとルート証明書を示します。この例では、Symantec/Digicert 証明書がコントローラにインストールされます。シスコの証明書またはエンタープライズ CA 証明書を使用することもできます。エンタープライズ CA 証明書を使用するには、エンタープライズ CA ルートチェーンをすべての SD-WAN デバイスにインストールする必要があります。これは手動でインストールするか、ZTP または PnP 経由で WAN エッジデバイスに自動的に配布できます。

次の例では、この認証の例で使用される証明書のみを示しています。Cisco ルート証明書などの追加のルート証明書もインストールされる場合があります。

- コントローラ：Digicert によって署名されたデバイス証明書が、SHA 256 アルゴリズムを使用する独自の ID としてインストールされます。ソフトウェアには、次のルート証明書が存在します。
  - Digicert（旧 Symantec）ルートチェーン：他のコントローラ証明書を信頼するため
  - Avnet ルートチェーン：vEdge ルータ証明書を信頼するため
  - Cisco ルートチェーン：Cisco SUDI ルータ証明書を信頼するため
  - Viptela ルートチェーン（vManage）：SUDI 証明書のない WAN エッジ仮想ルータおよび Cisco ルータを信頼するため
- vEdge ルータ：Avnet によって署名されたデバイス証明書は、SHA 1 アルゴリズムを使用する製造プロセス中にインストールされます。ソフトウェアでは、コントローラ証明書を信頼するために Digicert ルートチェーンが存在します。
- Cisco ルータ（SUDI を使用）：シスコによって署名されたデバイス証明書は、SHA 256 アルゴリズムを使用する製造プロセス中にインストールされます。ソフトウェアでは、コントローラ証明書を信頼するために Digicert ルートチェーンが存在します。
- クラウドルータおよび SUDI を使用しない Cisco ルータ（ASR 1002-X）：vManage によって署名されたデバイス証明書は、SHA 256 アルゴリズムを使用するワンタイムパスワード（OTP）認証の後にインストールされます。ソフトウェアでは、コントローラ証明書を信頼するために Digicert ルートチェーンが存在します。

図 17.　　認証目的で存在する証明書



SD-WAN デバイスの認証/認可

コントローラが相互に認証し、WAN エッジデバイスが認証されると、通常は次のようになります。

1. 証明書ルート認証局（CA）の信頼を検証します。
2. 受信した証明書 OU の組織名をローカルに設定された OU と比較します（WAN エッジハードウェアデバイスに対する認証の場合を除く）
3. 証明書のシリアル番号を vManage から配布された許可シリアル番号リストと比較します（vBond に対する認証の場合を除く）

WAN エッジデバイスがコントローラに認証されると、次のようになります。

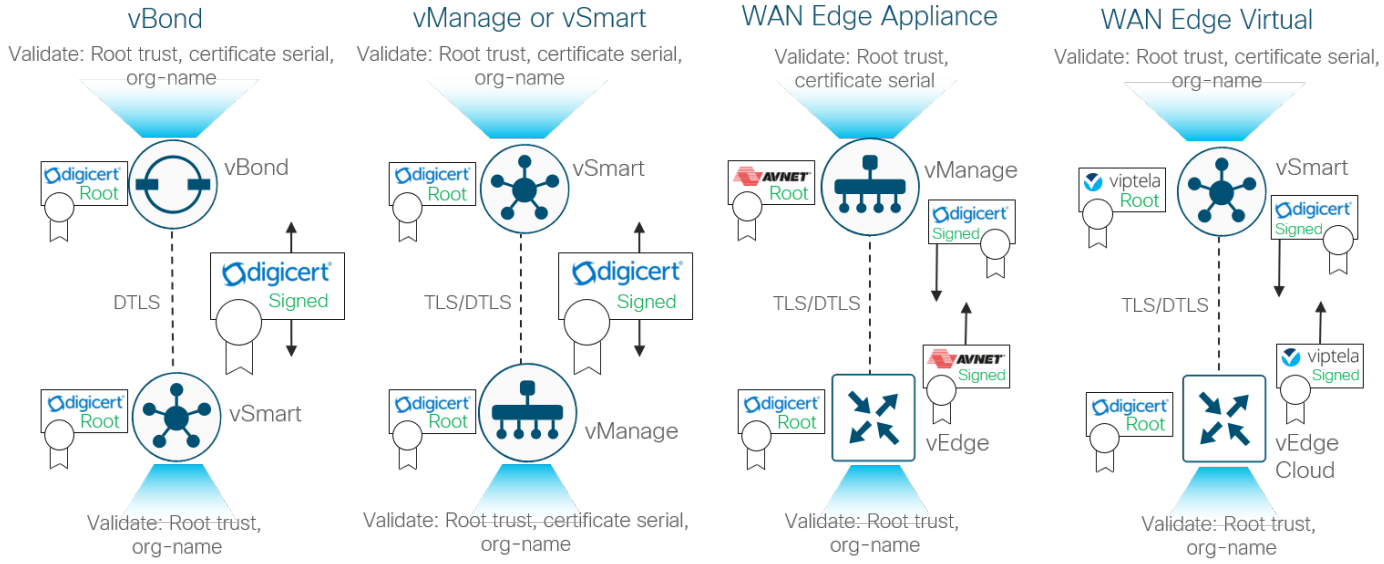
1. 証明書ルート認証局（CA）の信頼を検証します。
2. 受信した証明書 OU の組織名をローカルに設定された OU と比較します。

認証および認可が成功すると、DTLS/TLS 接続が確立されます。

次の図は、Symantec/Digicert またはシスコの証明書を使用して、異なるデバイスが相互に認証する方法を示しています。エンタープライズ CA 証明書も同様に動作します。通常、次のことに注意してください。

- コントローラおよび WAN エッジデバイスはクライアントとして機能し、サーバとして機能する vBond との接続を開始します
- vManage コントローラは、サーバとして機能する vSmart との接続を開始するクライアントとして機能します
- vSmart コントローラは、他の vSmart コントローラとの接続を開始するクライアントとして機能し、パブリック IP アドレスが最も大きいコントローラがサーバとして機能します
- WAN エッジデバイスはクライアントとして機能し、サーバとして機能する vManage および vSmart コントローラとの接続を開始します

図 18.　　SD-WAN デバイスの認証および認可



Cisco SD-WAN ソリューションの証明書の導入については、『Cisco SD-WAN Controller Certificates and Authorized Serial Number File Deployment Guide』（https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/cisco-sd-wan-certificates-deploy-2019sep.pdf）を参照してください

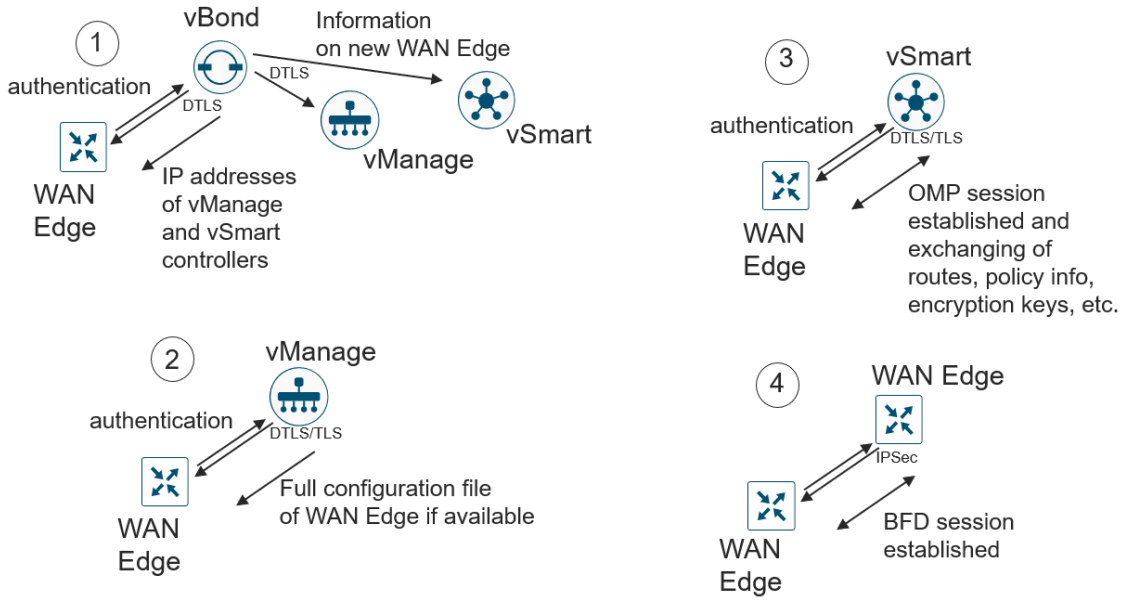
オーケストレーション プレーン

WAN エッジのオーバーレイへの移行

オーバーレイネットワークに参加するには、WAN エッジルータが vManage へのセキュアな接続を確立して設定ファイルを受信できるようにし、vSmart コントローラとのセキュアな接続を確立してオーバーレイネットワークに参加できるようにする必要があります。vManage と vSmart の検出は自動的に行われ、最初に vBond オーケストレータへのセキュアな接続を確立します。

次の図は、WAN エッジルータをオーバーレイに追加するときに発生するイベントのシーケンスを示しています。

図 19.　　WAN エッジのオーバーレイへの移行



1. 最小限のブートストラップ設定または自動プロビジョニング（ZTP または PnP）プロセスによって、WAN エッジルータは最初に、暗号化された DTLS 接続を介して vBond オーケストレータで認証を試みます。認証されると、vBond オーケストレータは、vManage ネットワーク管理システム（NMS）と vSmart コントローラの IP アドレスを WAN エッジルータに送信します。また、vBond オーケストレータは、ドメインに参加する新しい WAN エッジルータを vSmart コントローラと vManage に通知します。
2. WAN エッジルータは、vManage および vSmart コントローラとのセキュアな DTLS または TLS セッションの確立を開始し、vBond オーケストレータとのセッションを切断します。WAN エッジルータが vManage NMS で認証されると、vManage は WAN エッジルータに設定をプッシュします（使用可能な場合）。
3. WAN エッジルータは、各トランスポートリンクを介して vSmart コントローラへの DTLS/TLS 接続を確立しようとします。vSmart コントローラに認証されると、OMP セッションを確立し、プレフィックス、TLOC、サービスルート、暗号キー、およびポリシーを含むルートを学習します。
4. WAN エッジルータは、IPsec を使用して各トランスポートを介してリモート TLOC への BFD セッションを確立しようとします。

WAN エッジルータのオンボーディング

WAN エッジルータをネットワーク上で稼働させる方法は複数あります。1 つの方法は、手動の方法です。手動の方法では、デバイスへのコンソールを確立し、いくつかの設定行を設定できます。または、ゼロタッチプロビジョニング（ZTP）やプラグアンドプレイ（PnP）のような自動プロビジョニング方式を使用します。この場合、WAN エッジルータをネットワークに接続して電源を入れると、自動的にプロビジョニングされます。さらに、ブートストラップ方式を使用するオプションがあります。これは、IOS XE SD-WAN ルータにのみ適用され、ブートフラッシュまたは USB キーを介して設定がロードされ、デバイスを SD-WAN ネットワークに接続できます。自動プロビジョニングの要件が満たされていない場合に使用することができます。仮想クラウドルータのオンボーディングでは、vManage を介してデバイス証明書を永続的に取得する前に、ワンタイムパスワード（OTP）を一時的に認証するよう設定します。手動および自動の方法について、以下に簡単に説明します。オンボーディングデバイスの詳細については、『Cisco SD-WAN：WAN Edge Onboarding Prescriptive Deployment Guide』を参照してください。

手動

手動の設定方法では、最小のネットワーク接続と最小の識別情報を vBond オーケストレータの IP アドレスまたはホスト名とともに設定します。WAN エッジルータは vBond オーケストレータに接続し、そこから他のネットワークコントローラを検出しようとします。WAN エッジルータを正常に起動するために、WAN エッジルータで設定する必要があるものがいくつかあります。

- トランスポートネットワークに接続されたインターフェイスに IP アドレスとゲートウェイアドレスを設定するか、または Dynamic Host Configuration Protocol（DHCP）を設定して、IP アドレスとゲートウェイアドレスを動的に取得します。WAN エッジは、ネットワーク経由で vBond に到達できる必要があります。
- vBond IP アドレスまたはホスト名を設定します。ホスト名を設定する場合は、WAN エッジルータがそのホスト名を解決できる必要があります。これを行うには、VPN 0 で有効な DNS サーバアドレスまたはスタティックホスト名 IP アドレスマッピングを設定します。
- 組織名、システム IP アドレス、およびサイト ID を設定します。必要に応じて、ホスト名を設定します。

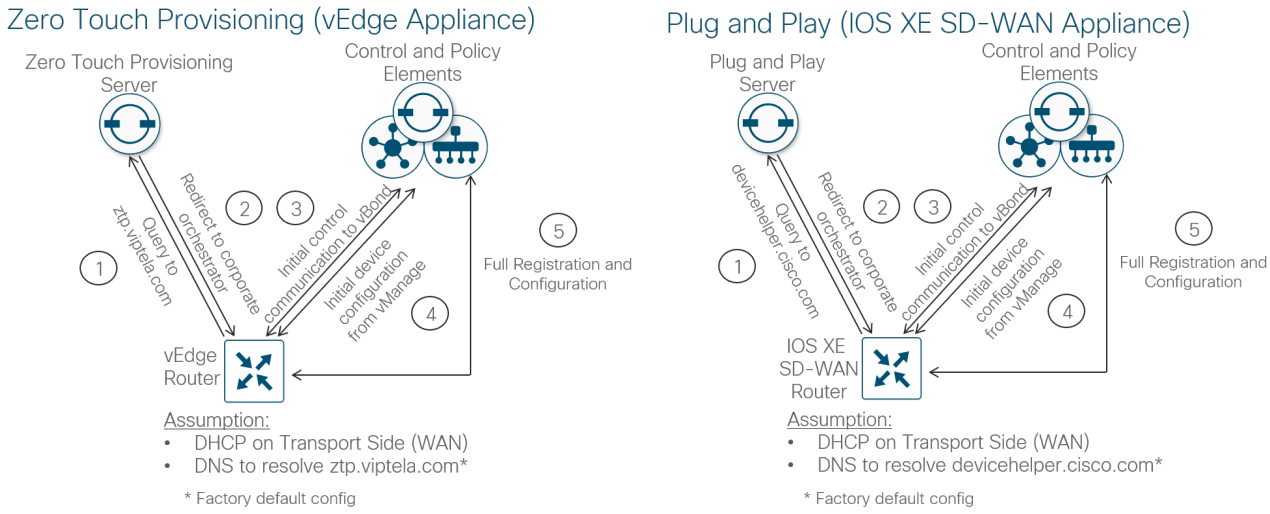
技術的なヒント
上記の要件に加えて、WAN エッジルータには有効な証明書がインストールされている必要がありますが、工場出荷時にはほとんどのハードウェアベースの WAN エッジルータに証明書がすでにインストールされています。また、システムクロックは、証明書認証のために正確な時刻を反映する必要があり、必要に応じて手動または Network Time Protocol（NTP）を使用して設定できますが、新しいデバイスをオンボーディングする際にこれに対処する必要はほとんどありません。

自動デバイスプロビジョニング（ZTP または PnP）

vEdge デバイスの自動デバイスプロビジョニングはゼロタッチプロビジョニング（ZTP）と呼ばれ、IOS XE SD-WAN デバイスの場合はプラグアンドプレイ（PnP）と呼ばれます。プロセスは非常に似ていますが、2 つの異なるサービスが関係しています。

自動プロビジョニング手順は、WAN エッジルータの電源が初めて投入されたときに開始されます。vEdge ルータは、ホスト名が ztp.viptela.com の ZTP サーバへの接続を試み、vBond オーケストレータ情報を取得します。IOS XE SD-WAN ルータの場合、ホスト名 devicehelper.cisco.com を使用して PnP サーバに接続しようとします。vBond オーケストレータ情報が取得されると、その後、vManage および vSmart コントローラに接続して、その完全な設定を取得し、オーバーレイネットワークに参加できます。

図 20.　　WAN Edge アプライアンスの自動デバイスプロビジョニング



自動デバイスプロビジョニングには、いくつかの要件があります。

- ハードウェア vEdge アプライアンスでは、特定のポートのみがデフォルトで DHCP クライアント インターフェイスとして事前設定されており、ZTP に使用できます。次の表に、ZTP が機能するためにネットワークに接続する必要があるポートの概要を示します。IOS XE SD-WAN デバイスでは、管理インターフェイス（GigabitEthernet0）を除くすべてのルーテッド ギガビット イーサネット インターフェイスで PnP がサポートされます。

表 1.　vEdge ZTP インターフェイス

vEdge モデル	インターフェイス
vEdge 5000	ge0/0（スロット 0 のネットワークモジュール用）
vEdge 2000	ge2/0
vEdge 1000、ISR1100-4G/8G	ge0/0
vEdge 100b/m	ge0/4
vEdge 100wm	ge0/4、cellular0
ISR1100-4GLTE	ge0/4、cellular0

- WAN エッジルータは、DHCP を介して IP アドレスを取得するか、自動 IP（vEdge のみ）を使用して IP アドレスを検出できる必要があります。
- ネットワーク内の WAN エッジルータのゲートウェイルータは、パブリック DNS サーバに到達可能で、vEdge デバイスの場合は ztp.viptela.com、IOS XE SD-WAN デバイスの場合は devicehelper.cisco.com に到達できる必要があります。ZTP サーバはオンプレミスで展開できますが、PnP サーバにはインターネットアクセスが必要です。

- SD-WAN デバイスを https://software.cisco.com の PnP ポータルに正しく入力し、vBond ホスト名または IP アドレス情報を定義するコントローラプロファイルに関連付ける必要があります。
- vManage には、WAN エッジデバイスに接続された WAN エッジルータのデバイス設定テンプレートが必要です。プロセスを機能させるには、このデバイステンプレートにシステム IP とサイト ID を含める必要があります。これがないと、ZTP または PnP プロセスは成功しません。

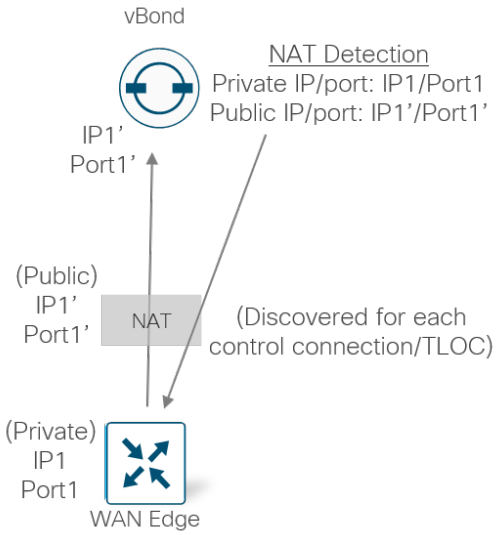
データプレーン

このセクションでは、Cisco SD-WAN データプレーンがどのように確立されるかを確認し、その実現に役立つコンポーネントに焦点を当てます。

NAT トラバーサルファシリテータとしての vBond

コントローラまたは SD-WAN ルータは、知らないうちに NAT デバイスの背後にある可能性があります。SD-WAN ネットワークでコントロールプレーンとデータプレーンの接続を正常に確立するには、ネットワークの外部から接続する IP アドレス/ポートを把握することが重要です。vBond は重要な役割を果たし、Session Traversal Utilities for NAT（STUN）サーバとして機能します。これにより、他のコントローラと SD-WAN ルータは、自身のマッピング/変換された IP アドレスとポート番号を検出できます。SD-WAN デバイスは TLOC とともにこの情報をアドバタイズするため、他の SD-WAN デバイスは接続を成功させるための情報を保持します。

図 21.　　vBond が NAT トラバーサルを促進

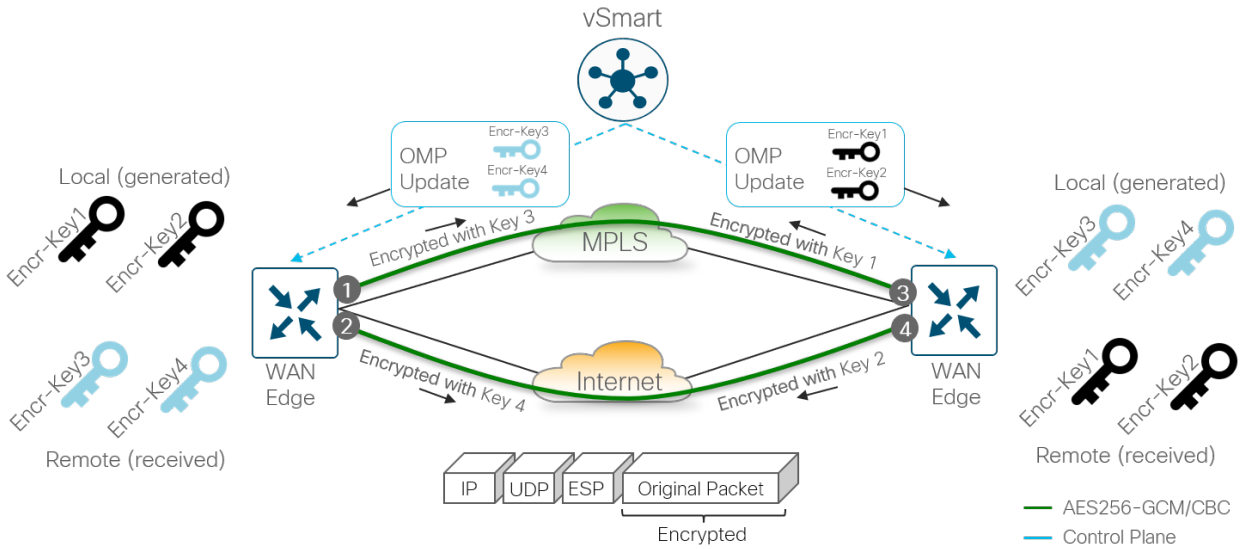


データプレーンのプライバシーと暗号化

WAN エッジルータは、データを暗号化および復号化する暗号キーを使用して、IPsec を使用してルータ間で交換されるデータトラフィックを保護します。従来の IPsec 環境では、ピア間のキー交換を容易にするためにインターネット キー エクスチェンジ（IKE）が使用されます。これにより、ペアごとのキーが作成され、各デバイスがフルメッシュ環境で n^2 個のキー交換と（n-1）個の異なるキーを管理する必要があります。Cisco SD-WAN ネットワークでより効率的なスケーリングを実現するために、WAN エッジルータとコントローラ間で ID がすでに確立されているため、IKE は実装されていません。DTLS または TLS を使用してすでに認証、暗号化、および改ざんされているコントロールプレーンは、AES-256 対称キーの通信に使用されます。各 WAN エッジルータは TLOC ごとに 1 つの AES キーを生成し、この情報を OMP ルートパケットで vSmart コントローラに送信します。その後、このパケットはすべての WAN エッジルータに配布されます。

各キーのライフタイムはデフォルトで 24 時間です。12 時間ごとに新しいキーが生成され、vSmart コントローラに送信されてから、他の WAN エッジルータに配布されます。つまり、常に 2 つのキーが存在します。WAN エッジルータが新しく生成されたキーを使用するように切り替わる間、最後の既知のキーはさらに 12 時間保持され、トラフィックはいずれかのキーを使用して受け入れられます。vSmart コントローラへの OMP セッションが失われた場合、WAN エッジルータは、保持している最後の情報（設定、ポリシー、ルート、および IPsec キー）を最大 12 時間（OMP グレースフル リスタート タイマーの長さ）使用し続けます。OMP の停止がいつ発生するかを知る方法がないため、2 つのキーにより、12 時間の OMP グレースフル リスタート タイマーをサポートできます。

図 22.　　データプレーン暗号キー



技術的なヒント
ペアワイズキーは、19.2 vEdge および 16.12.1b IOS XE SD-WAN コード以降でも設定できます。ペアワイズキーは引き続き AES256 対称暗号化アルゴリズムを使用しますが、SD-WAN ルータがオーバーレイ内の他のすべての SD-WAN ルータと同じ TLOC キーを共有する代わりに、この方法ではパスを共有する各 SD-WAN ルータと一意の TLOC キーを共有します。

データプレーントラフィックの暗号化では、Encapsulating Security Payload（ESP）の修正バージョンを使用してデータパケットペイロードを保護します。暗号化アルゴリズムは AES-256 GCM ですが、必要に応じて AES-256 CBC にフォールバックできます（マルチキャストトラフィックの場合）。データの整合性と信頼性を検証する認証アルゴリズムは設定可能であり、vSmart コントローラと交換される TLOC プロパティに含まれます。デフォルトでは、AH-SHA1 HMAC と ESP HMAC-SHA1 の両方が設定されます。複数の認証タイプが設定されている場合は、2 つのポイント間の最も強力な方式（AH-SHA1 HMAC）が選択されます。

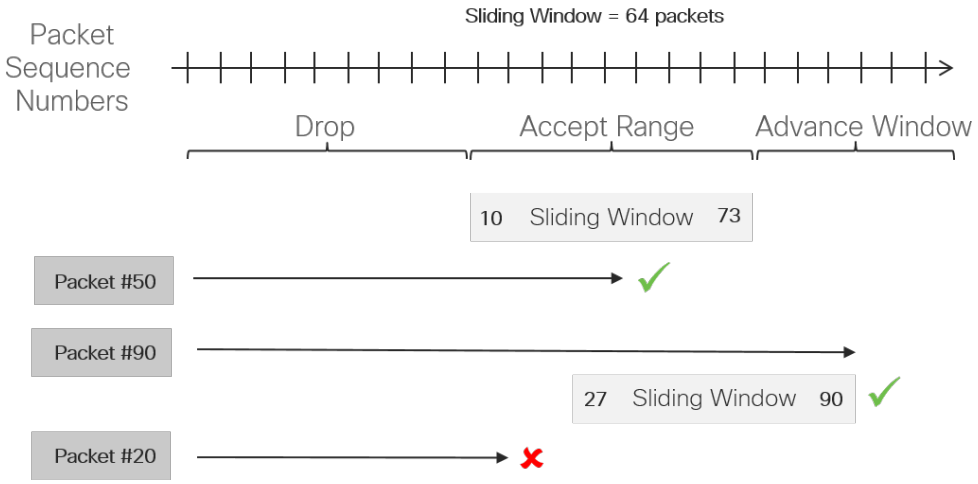
アンチリプレイ

アンチリプレイ保護により、IPsec パケットは攻撃者によるパケットの挿入または変更から保護されます。送信者は連続して増加するシーケンス番号を IPsec パケットに割り当てます。パケットは常に順序どおりに到着するとは限らないため、接続先はこれらのシーケンス番号をチェックし、受け入れるシーケンス番号のスライディングウィンドウを維持します。重複するシーケンス番号を持つパケットはドロップされます。スライディングウィンドウの左側に到着したパケットは古いと見なされ、接続先はそれらをドロップします。スライディングウィンドウの右側に到着したパケットの場合、パケットが検証され、最大値を持つパケットシーケンス番号にスライディングウィンドウが進められます。

アンチリプレイは無効化できません。デフォルトでは、スライディングウィンドウは 512 パケットに設定されています。これは 2 の累乗である必要があり、**replay-window** コマンドを使用して 64 ～ 4096 の範囲で設定できます。大量の優先順位の高いトラフィックと組み合わせた QoS などの特定のネットワークシナリオでは、512 パケットは十分な大きさのウィンドウサイズではない可能性があるため、アンチリプレイは非常に多くの正当なパケットをドロップする可能性があります。このウィンドウサイズは最大 4096 に設定することをお勧めします。

以下の図にアンチリプレイ機能を示します。スライディングウィンドウ内のシーケンス番号が付いた到着したパケットは受け入れられ、ウィンドウの右側に到着したパケットは受け入れられてスライディングウィンドウが進み、スライディングウィンドウの左側に到着したパケットは廃棄されます。

図 23.　　アンチリプレイ



複数のシーケンス番号スペース（マルチ SNS）

暗号化後に発生する QoS キューイングにより、非優先パケットがキューに入れられて遅延し、リプレイウィンドウが失われる可能性があるため、アンチリプレイドロップが発生する可能性があります。アンチリプレイウィンドウを最大化することが役立つ場合もありますが、すべての状況で問題を解決できるわけではありません。

SD-WAN は、IOS XE SD-WAN ルータに実装された複数のシーケンス番号スペース（マルチ SNS）でこれを軽減します。マルチ SNS は、セキュリティ アソシエーションごとに複数の一意のシーケンス番号スペースを維持します。スペースは、出力キューイングスキームと一致するため、特定のキュー内のすべてのパケットが同じシーケンス番号スペースからシーケンス番号を受信します。これにより、同じシーケンス番号スペース内のパケットが同じキューを通過するため、出力 QoS によってパケットの順序が変更される可能性がなくなります。

マルチ SNS は、QoS が設定されているかどうかに関係なく、SD-WAN オーバーレイトンネルに対して常に有効です。デフォルトでは、BFD トラフィック用（キュー 0）とデータトラフィック用（キュー 2）の 2 つのスペースが使用されます。QoS が設定されると、定義されたクラスごとに一意のシーケンス番号スペースが自動的に作成されます (IOS XE SD-WAN ルータでは最大 8 つ）。各 QoS クラスには、ESP/AH ヘッダーの 32 ビット SPI フィールドにエンコードされた SNS グループがあります。

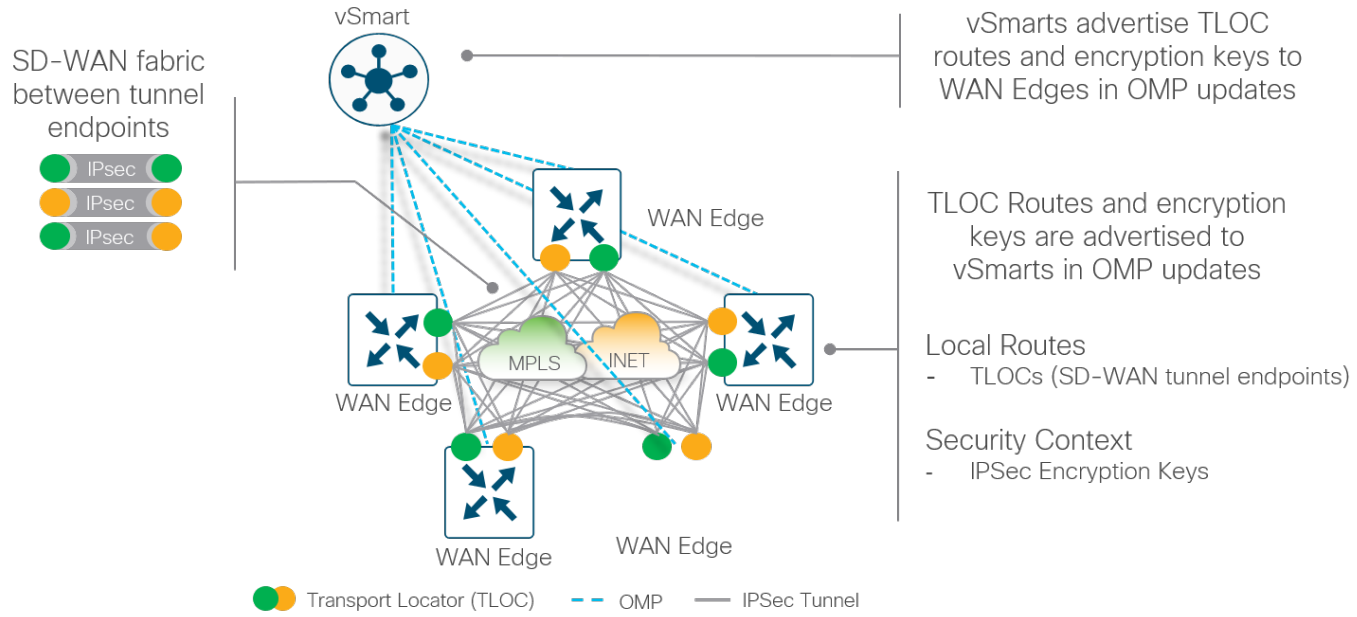
IPsec トンネルの両側で同じ数のクラスが設定された QoS を持つことが重要です。そうしないと、アンチリプレイがパケットを無差別にドロップする可能性があります。

データプレーンセキュリティおよびその他のセキュリティトピックの詳細については、https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html を参照してください。

トランスポートロケータ（TLOC）

トランスポートロケータ（TLOC）は、WAN エッジルータが WAN トランスポートネットワークに接続する接続ポイントです。TLOC は一意に識別され、システム IP アドレス、カラー、およびカプセル化（Generic Routing Encapsulation（GRE）または IPsec）で構成される 3 つのタプルで表されます。TLOC ルートは、OMP を介して vSmart にアドバタイズされます。これには、各 TLOC に関連付けられたプライベートおよびパブリック IP アドレスとポート番号、およびカラーと暗号キーを含む多数の属性が含まれます。これらの TLOC ルートとその属性は、他の WAN エッジルータに配布されます。これで、TLOC 属性と暗号キー情報が判明したため、WAN エッジルータは他の WAN エッジルータと IPsec を使用して BFD セッションの形成を試みることができます。

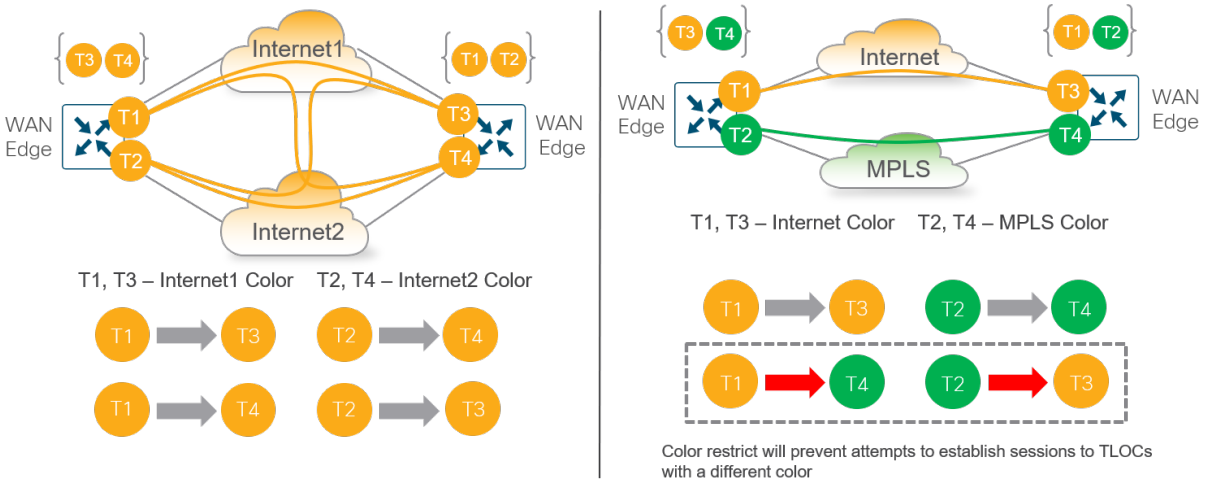
図 24.　　データプレーンの確立



デフォルトでは、WAN エッジルータは、異なるカラーでマークされた他のトランスポートに属する TLOC を含む、各 WAN トランスポートを介してすべての TLOC への接続を試みます。これは、異なる場所に異なるインターネットトランスポートがある場合（たとえば、相互に直接通信する必要がある場合）に役立ちます。この動作を防ぐために、トンネルのカラーとともに指定できる **restrict** キーワードがあります。これにより、異なるカラーの TLOC への BFD セッションを確立しようとする試みが防止されます。これは一般に、プライベートトランスポートで、パブリックトランスポートとのセッションの形成を防ぐために使用されます。

次の図は、restrict キーワードが BFD セッションの確立にどのように影響するかを示しています。左の図では、すべての TLOC が相互にセッションを確立できるように、restrict キーワードが使用されていません。右の図では、restrict キーワードが MPLS カラーで使用されているため、MPLS TLOC は他の MPLS TLOC とのセッションのみを形成できます。

図 25.　　restrict キーワードの使用



カラー

カラーは、WAN エッジデバイスで終端する個々の WAN トランスポートを識別するために使用される抽象概念です。カラーは静的に定義されたキーワードであり（自由形式のラベルではありません）、個々のトランスポートをパブリックまたはプライベートとして識別するため、重要です。メトロイーサネット、mpls、および private1、private2、private3、private4、private5、private6 のカラーは、プライベートカラーと見なされます。これらは、プライベートネットワーク、またはトランスポート IP エンドポイントの NAT アドレッシングがない場所で使用されることを目的としています。パブリックカラーは、3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、public-internet、red、silver です。これらは、パブリックネットワーク、またはトランスポート IP エンドポイントのパブリック IP アドレッシングをネイティブまたは NAT 経由で使用する場所で使用されることを目的としています。コントロールプレーンまたはデータプレーンを介して通信する場合、カラーによってプライベート IP アドレスまたはパブリック IP アドレスの使用が決まります。

技術的なヒント
WAN エッジルータでは、すべての TLOC がプライベート IP アドレスとパブリック IP アドレスのペアに関連付けられます。 プライベート IP アドレスは、SD-WAN デバイスのインターフェイスに割り当てられた IP アドレスです。これは、NAT 前のアドレスであり、名前にかかわらず、パブリックにルーティング可能なアドレスまたはプライベート（RFC 1918）のいずれかです。 パブリック IP アドレスは、vBond オーケストレータによって検出された NAT 後のアドレスです。このアドレスは、パブリックにルーティング可能なアドレスまたはプライベート（RFC 1918）アドレスのいずれかです。NAT がない場合、SD-WAN デバイスのプライベート IP アドレスとパブリック IP アドレスは同じです。

プライベートカラーとパブリックカラー間の通信

SD-WAN デバイスが vBond オーケストレータと通信して認証を行うと、vBond オーケストレータは交換中に SD-WAN デバイスのピアプライベート IP アドレス/ポート番号とピアパブリックアドレス/ポート番号の両方の設定を学習します。NAT が関係する場合、プライベート IP アドレスはインターフェイスに割り当てられたネイティブ IP アドレスを参照し、パブリック IP アドレスは NAT 後の IP アドレスを参照します。

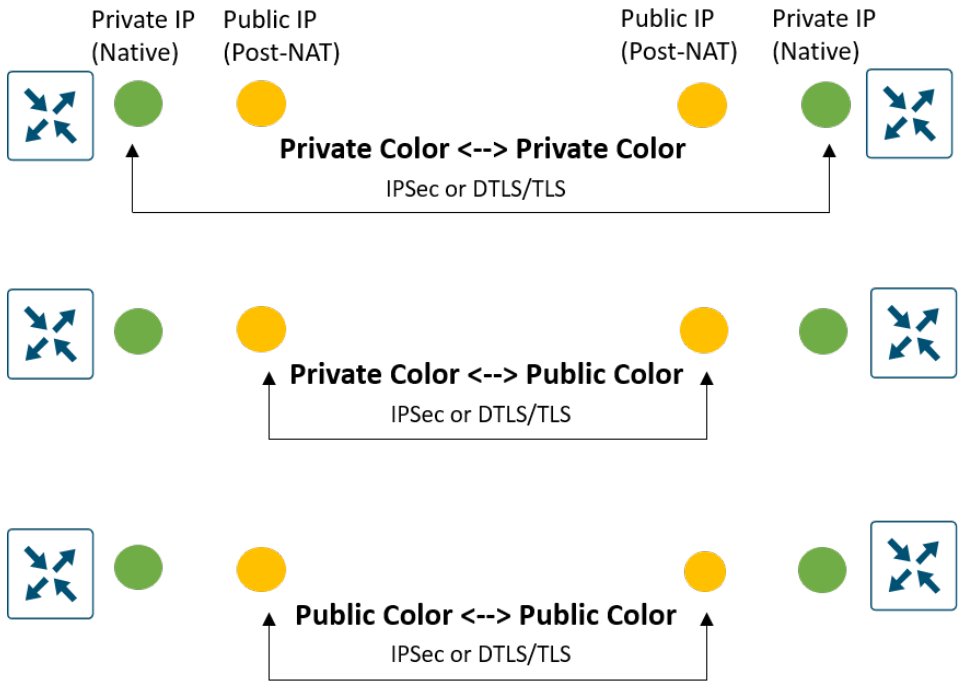
2 つの SD-WAN デバイスがプライベートカラーのインターフェイスを使用して相互に通信しようとすると、両側がリモートデバイスのプライベート IP アドレスに接続しようとします。一方または両側がパブリックカラーを使用している場合、各側はリモートデバイスのパブリック IP アドレスへの接続を試みます。

技術的なヒント
サイト ID が同じで、カラーがパブリックの場合は、代わりにプライベート IP アドレスが通信に使用されることに注意してください。これは、たとえば、同じサイトのオンプレミスにある vManage または vSmart と、または同じファイアウォールの背後にあるオンプレミスコントローラ間で通信しようとする WAN エッジルータで発生します。

次の図は、一般的な動作を示しています。これらのルールは以下に適用されます。

- 他の WAN エッジルータへの IPsec を使用する WAN エッジルータ
- WAN エッジルータと vManage および vSmart コントローラ間の DTLS/TLS 接続
- vManage コントローラと vSmart コントローラ間の DTLS/TLS 接続

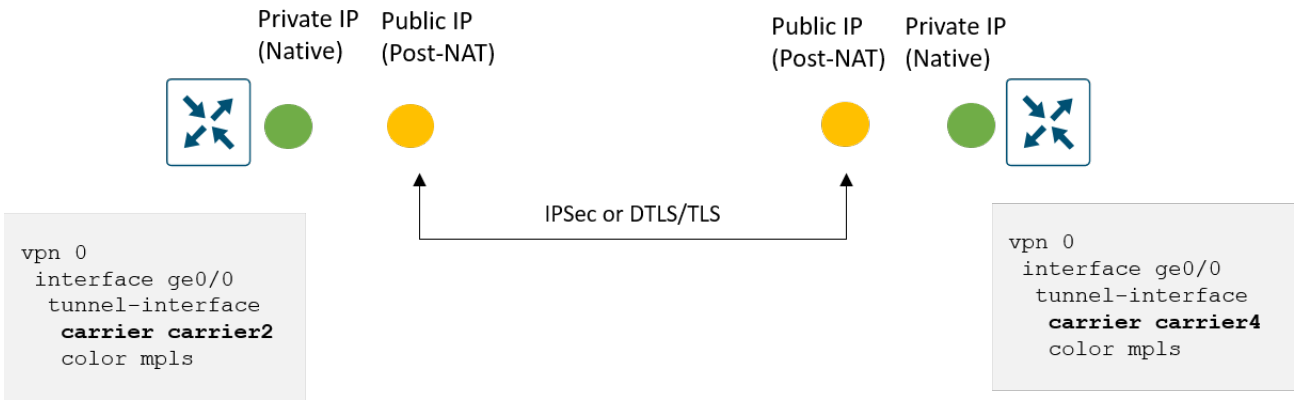
図 26.　　プライベートカラーとパブリックカラー間の通信



キャリア設定

プライベートカラーを使用していて他のプライベートカラーと通信するために NAT が必要な場合は、構成内のキャリア設定によってプライベート IP アドレスかパブリック IP アドレスのどちらを使用するかが決定されます。この設定を使用して、1 つまたは両方が NAT を使用している場合は、2 つのプライベートカラーがセッションを確立します。キャリア設定がインターフェイス間で同じ場合、プライベート IP アドレスがインターフェイス間で使用され、キャリア設定が異なる場合は、パブリック IP アドレスが使用されます。次の図にこれを示します。

図 27.　　キャリア設定

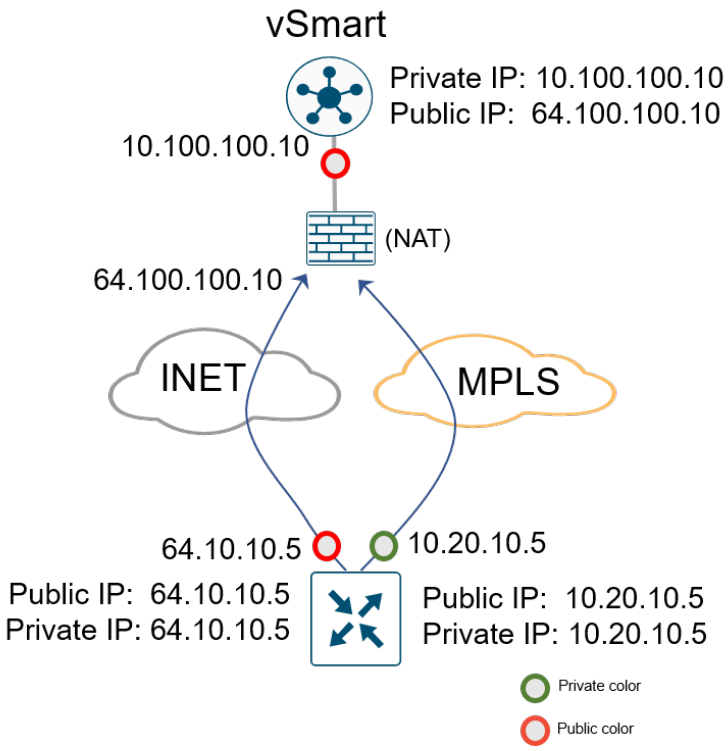


パブリック IP アドレスとプライベート IP アドレスの例

次の例は、カラーのあるパブリック IP アドレスとプライベート IP アドレスをネットワークで使用する方法を示しています。次の図は、プライベート（RFC 1918）IP アドレスでアドレス指定された vSmart コントローラ インターフェイスを示していますが、ファイアウォールはそのアドレスを、WAN エッジルータが到達するために使用するパブリックにルーティング可能な IP アドレスに変換します。また、RFC 1918 IP アドレスが設定された MPLS インターフェイスと、パブリックにルーティング可能な IP アドレスが設定されたインターネット インターフェイスを備えた WAN エッジルータも示しています。WAN エッジルータのプライベート IP アドレスを変換する NAT がないため、パブリック IP アドレスとプライベート IP アドレスはどちらの場合も同じです。

vSmart のトランスポートカラーはパブリックカラーに設定され、WAN エッジでは、インターネット側がパブリックカラーに設定され、MPLS 側がプライベートカラーに設定されます。WAN エッジルータは、vSmart インターフェイス上のパブリックカラーにより、リモートパブリック IP アドレス（64.100.100.10）を宛先として使用して、どちらかのトランスポートの vSmart に到達します。

図 28.　　SD-WAN デバイスのパブリック IP アドレスとプライベート IP アドレス



双方向フォワーディング検出（BFD）

Cisco WAN エッジルータでは、BFD はピア間で自動的に開始され、無効化できません。IPsec トンネルにカプセル化されたトポロジ内のすべての WAN エッジルータ間およびすべてのトランスポート間で動作します。BFD はエコーモードで動作します。つまり、WAN エッジルータによって BFD パケットが送信されると、受信側の WAN エッジルータはそれらを処理せずに返します。その目的はパスの活性度を検出することであり、損失、遅延、ジッターなどのアプリケーション認識型ルーティングの品質測定も実行できます。BFD は、停電と電圧低下の両方のシナリオを検出するために使用されます。

トンネルの活性度

IPsec トンネルが稼働しているかどうかを検出するために、BFD hello パケットは、すべてのトンネルインターフェイスで、デフォルトで 1000 ミリ秒（1 秒）ごとに送信されます。デフォルトの BFD 乗数は 7 です。これは、7 つの連続した hello が失われたら、トンネルがダウンしたと宣言されることを意味します。BFD hello の間隔と乗数は、カラーごとに設定できます。

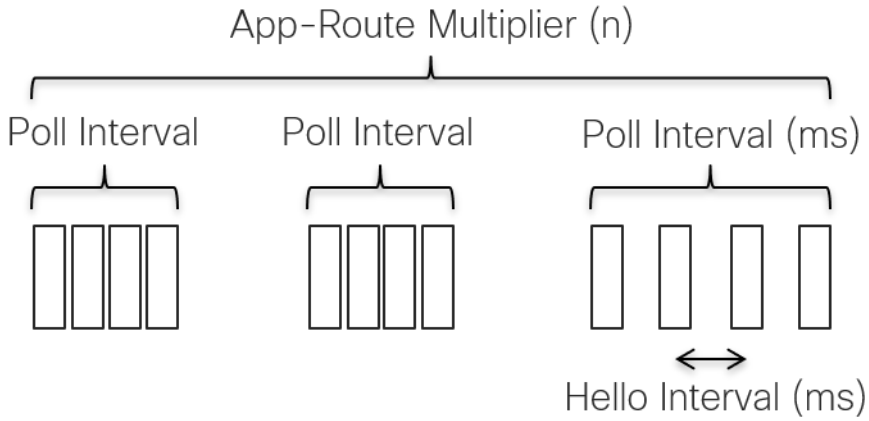
BFD パケットは、CS6 または IP Precedence 6 に相当する DSCP 48 でマークされます。パケットは、回線上で送信される前に低遅延高プライオリティ QoS キュー（LLQ）に配置されますが、LLQ ポリサーの対象にはなりません。めったに必要ではありませんが、WAN インターフェイスで出力 ACL を使用して DSCP 値を変更できます。

パス品質

BFD は、停電状態の検出だけでなく、損失、遅延、ジッターなどのさまざまなパス特性の測定にも使用されます。これらの測定値は、アプリケーション認識型ルーティングポリシーで定義された設定済みのしきい値と比較されます。また、ビジネスクリティカルなアプリケーションに最適な品質を提供するために、結果に基づいてダイナミックパスを決定できます。

測定のために、WAN エッジルータはすべての BFD hello パケットのパケット損失、遅延、およびジッター情報を収集します。この情報は、poll-interval 時間（デフォルトでは 10 分）にわたって収集され、各統計の平均がこの poll-interval 時間にわたって計算されます。次に、SLA 基準に対してレビューする必要がある poll-interval の平均の数を指定するために、乗数が使用されます。デフォルトでは、乗数は 6 であるため、損失、遅延、およびジッターの 6 x 10 分の poll-interval の平均がレビューされ、SLA しきい値と比較されてから、しきい値を超えているかどうかの決定が行われます。計算はローリングします。つまり、7 番目のポーリング間隔で、最新の情報に対応するために最も古いポーリングデータが廃棄され、最新のデータを使用して SLA 基準と比較されます。

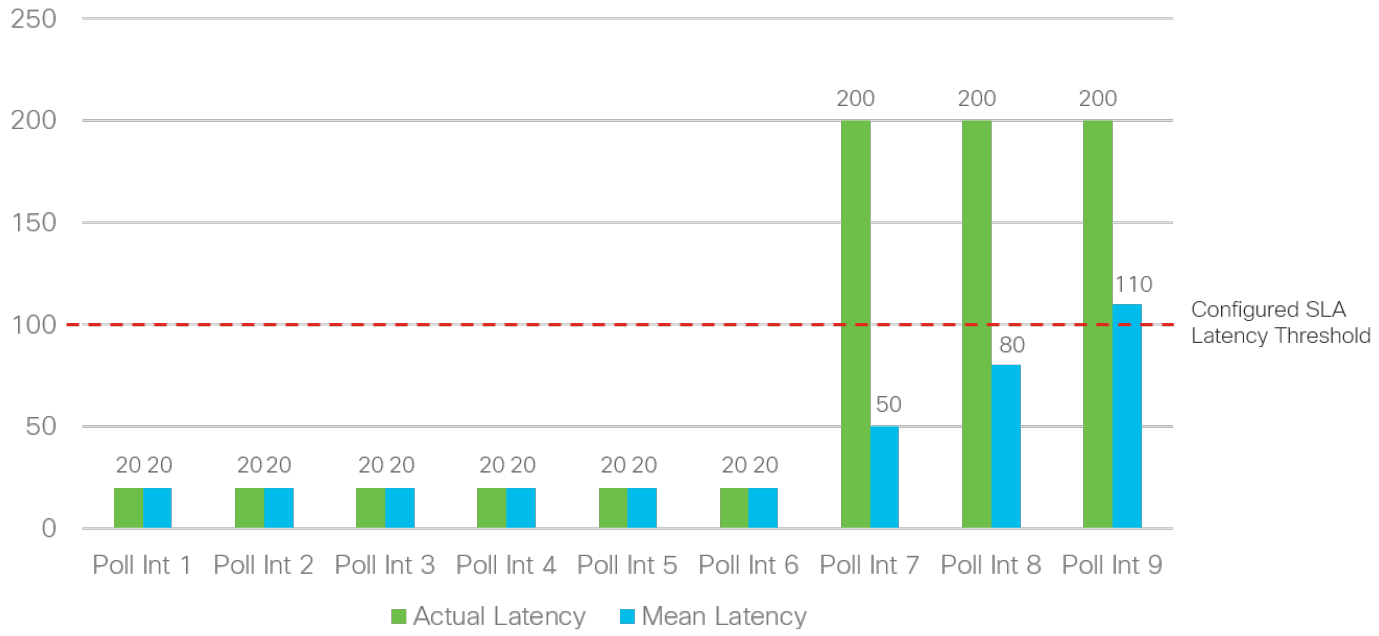
図 29.　　パス品質の検出



統計平均は設定された SLA 基準との比較に使用されるため、コンバージェンスがどの程度迅速に行われるかは、パラメータがしきい値からどれだけ離れているかによって異なります。デフォルト設定を使用した場合の最適なケースは、1 回のポーリング間隔（10 分）の完了後にしきい値を超えた状態が発生し、最悪のケースは、6 回のポーリング間隔（60 分）の完了後に発生します。しきい値を超えた状態が発生すると、トラフィックはより最適なパスに移動されます。

次の図に、遅延が突然増加したときにしきい値を超えた状態が認識された例を示します。poll-interval 7 の開始時に遅延が 20 ミリ秒から 200 ミリ秒に急増すると、6 ポーリング間隔にわたる遅延の平均が設定された SLA しきい値の 100 ミリ秒を超えるまでに 3 ポーリング間隔の計算が必要になります。

図 30.　　アプリケーション ルート ポリシーの平均遅延計算



アプリケーションルートの poll-interval 値を調整することもできますが、設定が低すぎると、損失、遅延、およびジッターの値によって誤検出が発生し、トラフィックが不安定になる可能性があるため、注意が必要です。平均計算のためには、ポーリング間隔ごとに十分な数の BFD hello が存在することが重要です。そうしないと、1 つの BFD hello が失われたときに、誤って大きな損失率が集計される場合があります。また、これらのタイマーを小さくすると、WAN エッジルータの全体的な規模とパフォーマンスに影響する可能性があります。

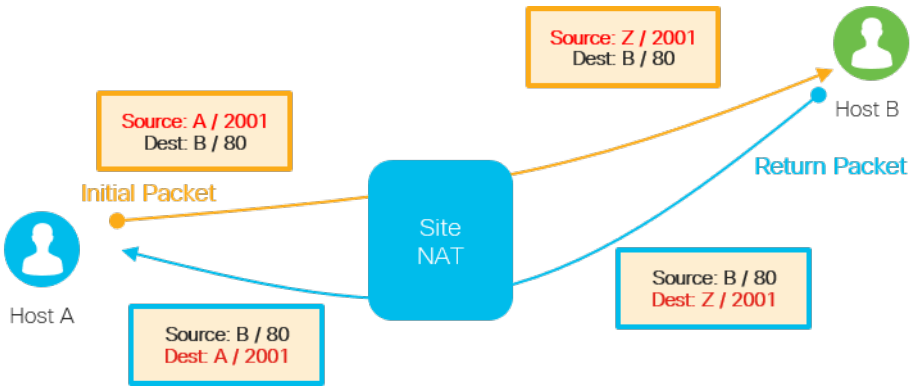
1 秒の hello の場合、展開する必要がある最も低いアプリケーションルートの poll-interval は 120 秒です。間隔が 6 の場合、2 分間のベストケースと 12 分間のワーストケースの後で、しきい値を超えたことが宣言され、トラフィックが現在のパスから移動されます。さらにタイマーを調整する場合は、十分にテストして慎重に使用する必要があります。

NAT

ブランチサイトで使用される NAT タイプは、サイトが接続を形成して相互に直接通信できるかどうかに影響する可能性があるため、SD-WAN 設計では慎重に考慮する必要があります。

すべての NAT タイプで、IP ネットワークパケットの送信元 IP アドレス、送信元ポート、宛先 IP、および宛先ポートのマッピングを作成できます。次の一般的な例では、送信元 NAT を使用して、パケットの送信元プライベート（RFC 1918）IP アドレス A をパブリックにルーティング可能な送信元 IP アドレス Z に変更し、ホストがインターネットベースのサーバ（ホスト B）に接続できるようにします。応答パケットがインターネットから返されると、宛先 IP アドレス Z は元の IP アドレス A にマッピングされ、発信元ホストに配信されます。

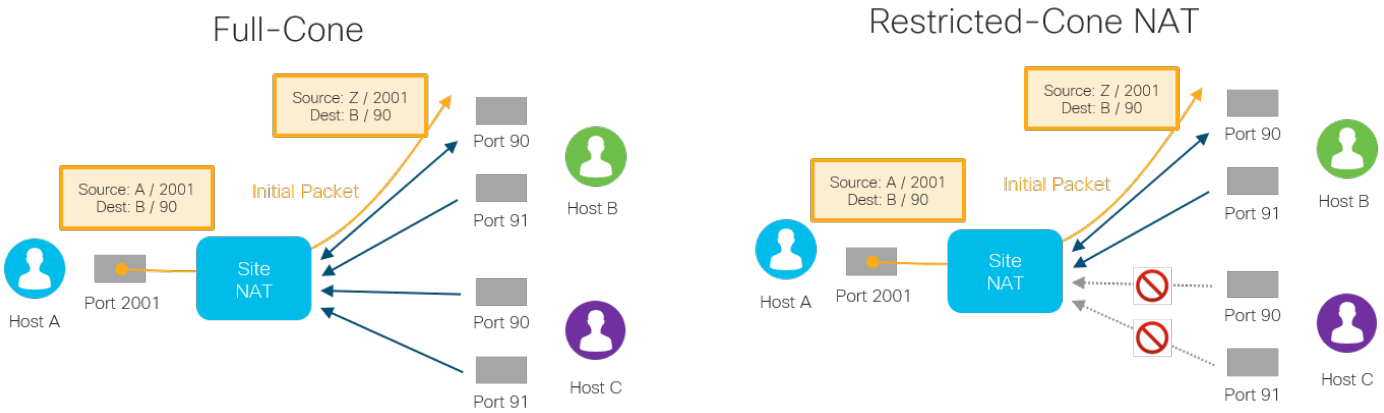
図 31.　　送信元 NAT の例



考慮すべき動作が異なる 4 種類の NAT があります。

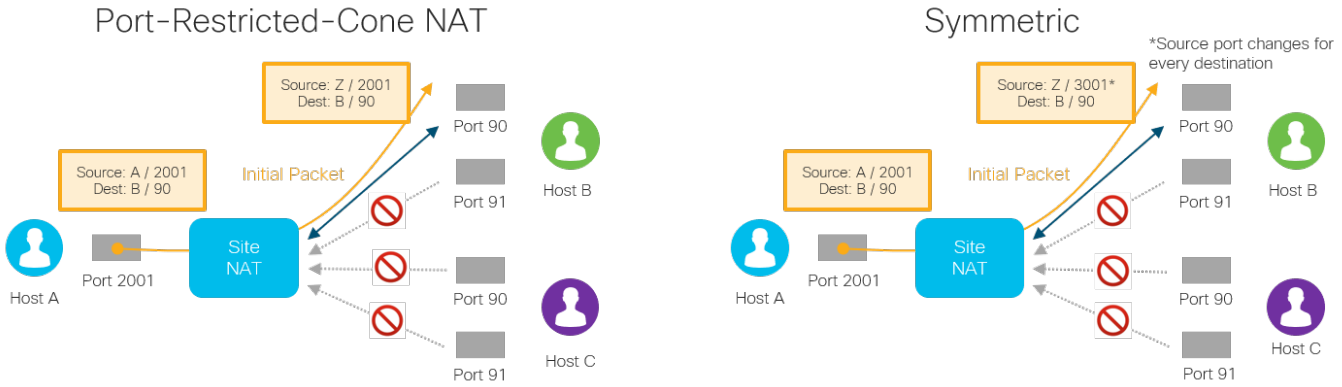
- Full-Cone NAT：この NAT タイプは 1 対 1 の NAT とも呼ばれ、最も制限の少ない NAT タイプです。これにより、1 つのローカル IP アドレスとポートが 1 つのパブリック IP アドレスとポートにマッピングされます。NAT 変換が発生するか、または静的な 1 対 1 の NAT がローカル IP アドレスおよびポートに設定されると、任意のポートをソースとする外部ホストは、マッピングされた NAT IP アドレスおよびポートを介してローカルホストにデータを送信できます。
- Restricted-Cone NAT：この NAT は Full-Cone NAT に似ていますが、より制限的です。内部ホスト A が外部ホスト B にパケットを送信し、ローカル IP アドレスとポートの NAT 変換が行われると、マッピングされた NAT IP アドレスとポートを介してローカルホスト A にデータを送信できるのは外部ホスト B（任意のポートをソースとする）だけです。

図 32.　　NAT タイプの図：Full-Cone および Restricted-Cone NAT



- Port-Restricted-Cone NAT：この NAT は Restricted-Cone NAT に似ていますが、制限にポート番号が含まれます。内部ホスト A が外部ホスト B とポート番号 X にパケットを送信し、ローカル IP アドレスとポートの NAT 変換が行われると、マッピングされた NAT IP アドレスとポートを介してローカルホスト A にデータを送信できるのは外部ホスト B（ポート X のみをソースとする）だけです。
- 対称 NAT：これは最も制限の厳しい NAT であり、Port-Restricted-Cone NAT と似ています。マッピングされた NAT IP アドレスとポートを介してローカルホスト A にデータを送信できるのは外部ホスト B（ポート X のみをソースとする）だけです。対称 NAT は、ホスト A が異なる宛先と通信するたびに一意の送信元ポートが使用される点で異なります。対称 NAT は、STUN サーバが学習する IP アドレス/ポートマッピングが別のホストへの異なるマッピングであるため、STUN サーバで問題を引き起こす可能性があります。

図 33.　　NAT タイプの図：Port-Restricted-Cone および対称 NAT



NAT の推奨事項

WAN エッジルータではいくつかのタイプの NAT がサポートされていますが、フルメッシュトラフィックが必要な場合は、パスにファイアウォールが存在しても、WAN エッジトンネルの少なくとも一方の側で、常に 2 番目の WAN エッジへのインバウンド接続を確実に開始できるように注意してください。ブランチで実行されている NAT タイプ（restricted-cone、port-restricted cone、または対称 NAT）に関係なく、データセンターまたはハブサイトで full-cone または 1 対 1 の NAT を設定することを推奨します。ブランチは、IPsec を使用して少なくとも問題なくハブサイトにトラフィックを送信できます。対称 NAT を実行するファイアウォールを持つ 2 つのサイトでは、トンネル接続の形成に問題があります。これは、この NAT が両側の送信元ポートをランダムなポート番号に変換し、トラフィックを外部から開始できないためです。あるサイトで設定された対称 NAT には、他のサイトとの間に直接 IPsec トンネルを確立するために、他のサイトに full-cone NAT または NAT なしの場合はパブリック IP が必要です。直接接続できないサイトは、データセンターまたは他の中央サイトを介して相互に到達できるように設定する必要があります。

次の表に、さまざまな NAT タイプの組み合わせと、対応する IPsec トンネルステータスを示します。

図 34.　　2 つの SD-WAN サイト間の NAT タイプの組み合わせ

WAN Edge A	WAN Edge B	IPSec Tunnel Status	
Public IP (No NAT)	Public IP (No NAT)	●	★
Full Cone	Full Cone	●	★
Full Cone	Port/Address Restricted	●	
Port/Address Restricted	Port/Address Restricted	●	
Public	Symmetric	●	
Full Cone	Symmetric	●	★
Symmetric	Port/Address Restricted	●	
Symmetric	Symmetric	●	★

● Direct IPSec Tunnel　● No Direct IPSec Tunnel (traffic traverses hub)　★ Mostly Encountered

技術的なヒント

NAT の背後にある GRE カプセル化トンネルでは、1 対 1 の NAT のみがサポートされます。GRE パケットには L4 ヘッダーがないため、ポートオーバーロードを使用する NAT はどのタイプもサポートされません。

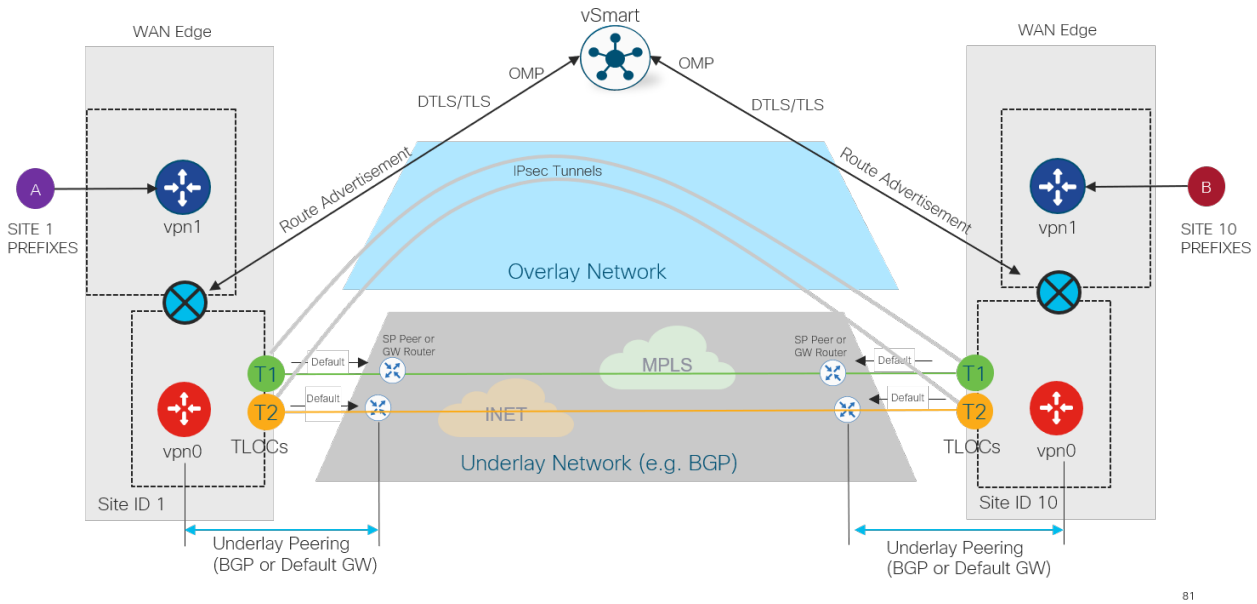
SD-WAN ルーティング

アンダーレイとオーバーレイルーティング

Cisco SD-WAN ネットワークは、アンダーレイネットワークとオーバーレイネットワークの 2 つの部分に分かれています。アンダーレイネットワークは、ルータやスイッチなどのネットワークデバイスを接続し、従来のルーティングメカニズムを使用してデバイス間でトラフィックをルーティングする物理ネットワーク インフラストラクチャです。SD-WAN ネットワークでは、通常、これは WAN エッジルータからトランスポートネットワークへの接続、およびトランスポートネットワーク自体で構成されます。アンダーレイネットワークに接続するネットワークポートは、VPN 0（トランスポート VPN）の一部です。トランスポートネットワークのサービス プロバイダー ゲートウェイへの接続を取得するには、通常、静的デフォルトゲートウェイを設定する（最も一般的）か、BGP や OSPF などのダイナミック ルーティング プロトコルを設定します。アンダーレイネットワークのルーティングプロセスは VPN 0 に限定され、その主な目的は、IPsec トンネルを構築してオーバーレイネットワークを形成できるように、他の WAN エッジルータ上の TLOC への到達可能性を確保することです。

アンダーレイネットワークを使用してサイト間を通過する IPsec トンネルは、SD-WAN オーバーレイネットワークの形成に役立ちます。オーバーレイ管理プロトコル（OMP）は、BGP に似た TCP ベースのプロトコルで、オーバーレイネットワークのルーティングを提供します。このプロトコルは、セキュアな DTLS または TLS 接続を介してコントロールプレーン情報が交換される vSmart コントローラと WAN エッジルータ間で実行されます。vSmart コントローラは、ルートリフレクタのように機能します。WAN エッジルータからルートを受信し、それらにポリシーを適用して処理し、オーバーレイネットワーク内の他の WAN エッジルータにルートをアドバタイズします。

図 35.　　アンダーレイとオーバーレイルーティング



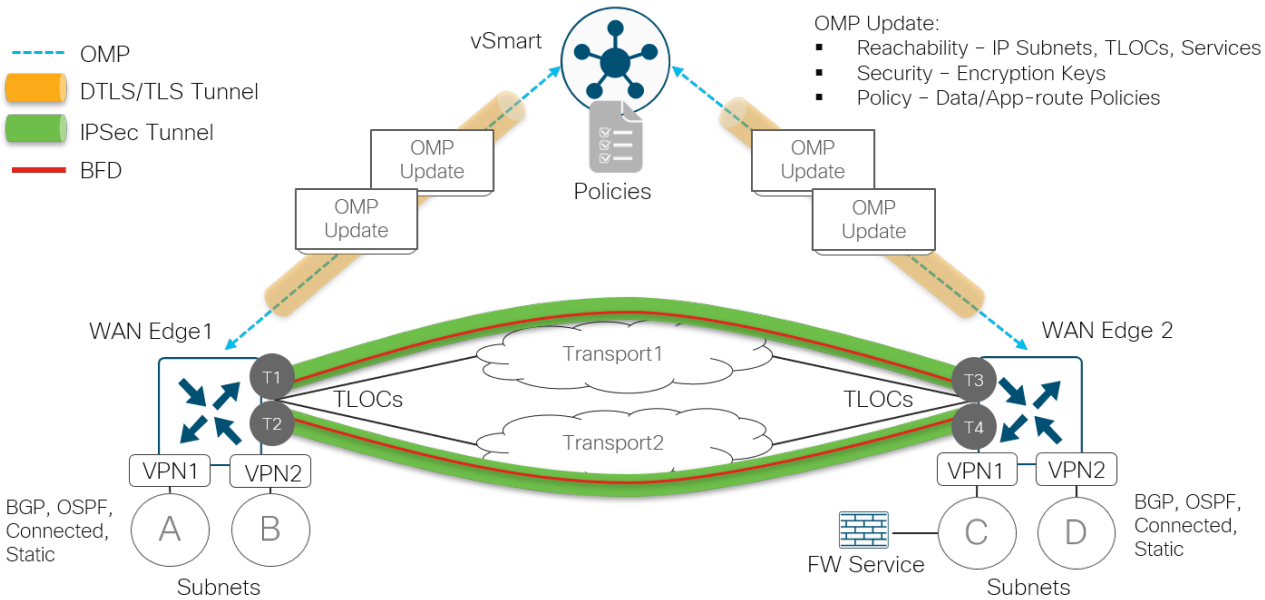
OMP の概要

OMP は WAN エッジルータと vSmart コントローラの間で実行し、vSmart コントローラ同士の間のフルメッシュとしても実行します。DTLS/TLS 制御接続が形成されると、OMP は自動的に有効になります。OMP ピアリングはシステム IP を使用して確立され、複数の DTLS/TLS 接続が存在する場合でも、WAN エッジデバイスと vSmart コントローラの間で 確立されるピアリングセッションは 1 つだけです。OMP は、ルートプレフィックス、ネクストホップルート、暗号キー、およびポリシー情報を交換します。

OMP は、WAN ルータから vSmart コントローラへの 3 種類のルートをアドバタイズします。

- OMP ルート（vRoute）は、WAN エッジルータのローカルサイトまたはサービス側から学習されるプレフィックスです。プレフィックスは、スタティックルートまたは接続ルートとして、または OSPF、BGP、EIGRP プロトコル内から発信され、OMP に再配布されるため、オーバーレイ全体で伝送されます。OMP ルートは、ルートの BGP ネクストホップ IP アドレスに類似したトランスポートロケーション（TLOC）情報や、オリジン、オリジンメトリック、発信元、プリファレンス、サイト ID、タグ、VPN などのその他の属性をアドバタイズします。OMP ルートは、それが向かう先の TLOC がアクティブな場合にのみ、フォワーディングテーブルにエントリされます。
- TLOC ルートは、WAN トランスポートに接続された TLOC を、TLOC のプライベート IP アドレスとパブリック IP アドレス、キャリア、プリファレンス、サイト ID、タグ、重み付け、暗号キー情報などの追加の属性とともにアドバタイズします。
- サービスルートは WAN エッジのローカルサイトネットワークに接続されているサービス（ファイアウォール、IPS、アプリケーション最適化など）を表し、他の拠点でのサービス挿入に使用できます。さらに、これらのルートには、発信元のシステム IP、TLOC、および VPN-ID が含まれます。VPN ラベルは、この更新タイプで送信され、リモートサイトで処理される VPN を vSmart コントローラに通知します。

図 36.　　OMP 操作



デフォルトでは、OMP は、等コストパスの場合に最適なルートのみをアドバタイズします。vSmart コントローラで **send-backup-paths** OMP パラメータを有効にすることをお勧めします。これにより、OMP は、特定のプレフィックスの最適なパスではない追加の有効なパスをアドバタイズします。これにより、コンバージェンスが向上するだけでなく、WAN エッジルータが TLOC の可用性に基づいて最適なパスを決定できるようになります。

さらに、OMP は、特定のプレフィックスに対して 4 つの等コストパスだけをアドバタイズします。この制限は、それぞれが 2 つの異なるトランスポートに接続されたデュアル WAN エッジルータを使用するサイトでは簡単に到達できるため、設計によっては不十分な場合があります。vSmart コントローラの **send-path-limit** OMP パラメータ、または**プレフィックスごとにアドバタイズされるパスの数**を最大 16 に設定することを推奨します。**send-path-limit** パラメータには、最適パスとバックアップパスの両方が含まれます。WAN エッジルータはデフォルトで 4 つの等コストパスのみをインストールすることに注意してください。この値を大きくする場合は、WAN エッジルータの **ecmp-limit** OMP パラメータを使用して変更します。

デフォルトでは、接続ルート、スタティックルート、および OSPF（エリア内およびエリア間）ルートタイプは、サービス側 VPN から OMP に自動的に配布されます。他のすべてのルートタイプ（OSPF 外部ルートを含む）は、明示的に設定する必要があります。OMP ルートには、vEdge ルータの場合は 250、IOS XE SD-WAN ルータの場合は 251 の管理距離が割り当てられるため、ローカルサイトのルートが優先されます。

OMP ルーティングおよびパス選択の詳細については、「Unicast Overlay Routing Overview」を参照してください。

グレースフルリスタート

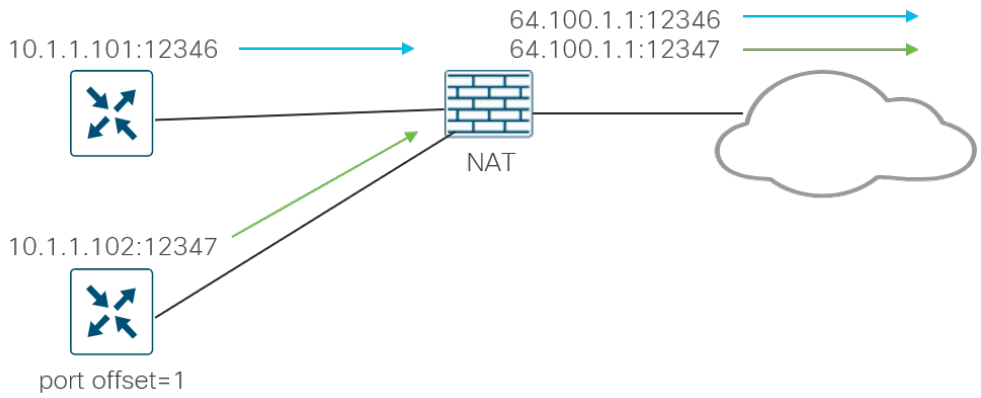
OMP ピアが使用できなくなった場合、OMP グレースフルリスタートにより、他の OMP ピアは一時的に動作を継続できます。WAN エッジルータが vSmart コントローラへの接続を失った場合、ルータは最後に確認された正常なルーティング情報を使用してトラフィックの転送を続行できます。デフォルトの OMP グレースフルリスタート値は 12 時間で、最大 604,800 秒（7 日間に相当）に設定できます。IPsec キー再生成タイマーはデフォルトで 24 時間に設定されており、両方のタイマーを設定できますが、IPsec キー再生成タイマーは OMP グレースフル リスタートタイマーの値の 2 倍以上にする必要があります。これは、vSmart コントローラが IPsec キーを WAN エッジルータに配布し、vSmart コントローラへの接続が失われた場合、グレースフルリスタート時間内に IPsec キー再生成が発生すると、トラフィックが失われるためです。

ファイアウォールポートの考慮事項

WAN エッジルータとコントローラ間（およびコントローラ間）のセキュアなセッションは、デフォルトでは DTLS（User Datagram Protocol（UDP）ベース）です。デフォルトのベース送信元ポートは 12346 です。WAN エッジは、最初のポートでの接続試行が失敗した場合、デバイスが相互に接続を確立しようとするときに、異なる送信元ポートを試行するポートホッピングを使用できます。WAN エッジはポートを 20 ずつ増やし、ポート 12366、12386、12406、および 12426 を試行してから 12346 に戻ります。ポートホッピングは、WAN エッジルータではデフォルトで設定されますが、グローバルに、またはトンネルインターフェイスごとに無効にできます。ブランチでポートホッピングを実行することをお勧めしますが、ポートホッピングが発生すると接続が中断される可能性があるため、データセンター、地域ハブ、または集約トラフィックが存在する場所の SD-WAN ルータではこの機能を無効にします。デフォルトでは、ポートホッピングはコントローラで無効になっているため、無効のままにしておく必要があります。複数のコアを持つ vManage および vSmart コントローラの制御接続には、コアごとに異なるベースポートがあります。

同じ NAT デバイスの背後にあり、パブリック IP アドレスを共有する WAN エッジルータの場合、各 WAN エッジが同じポート番号を使用して同じコントローラに接続しようとすることは望ましくありません。NAT またはポートホッピングにより、両方のデバイスが一意の送信元ポートを使用できる場合がありますが、代わりにベースポート番号 12346 にオフセットを設定して、WAN エッジルータ間でポートの試行を一意（およびさらに確定的）にすることができます。ポートオフセットが 1 の場合、WAN エッジはベースポート 12347 を使用し、ポート 12367、12387、12407、および 12427 でポートホップを使用します。ポートオフセットは明示的に設定する必要があり、デフォルトではポートオフセットは 0 です。

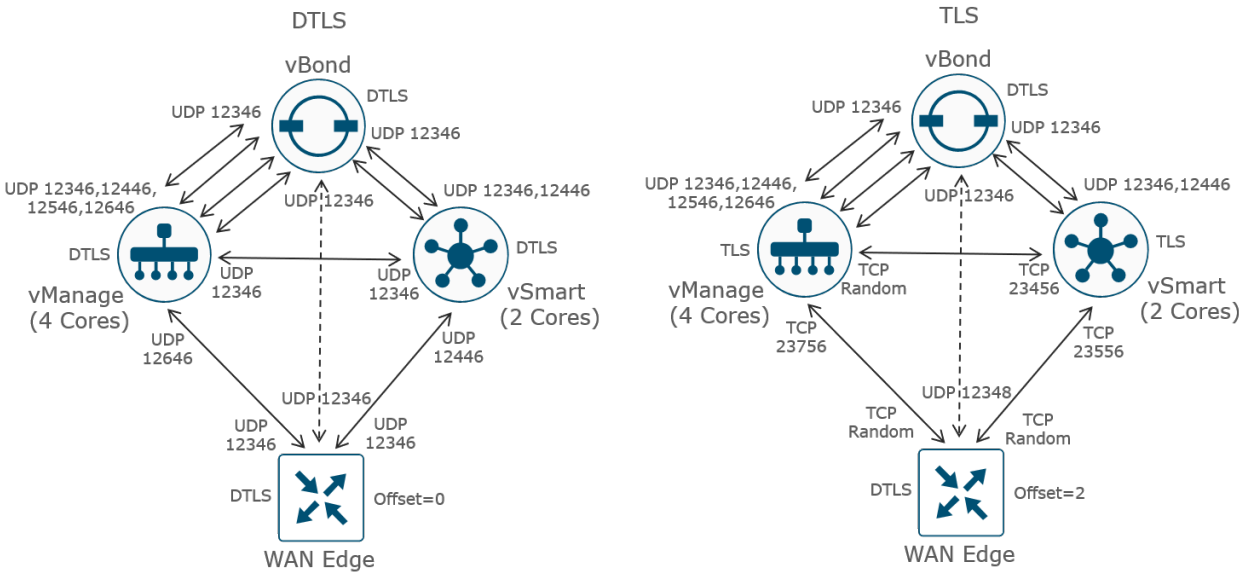
図 37.　　WAN エッジポートオフセット



または、UDP ベースではなく TCP ベースの vManage および vSmart コントローラに TLS を使用して接続できます。ただし、vBond コントローラ接続は常に DTLS を使用します。TCP ポートはランダムなポート番号から WAN エッジで発信され、複数のコアを持つコントローラへの制御接続には、DTLS の場合と同様に、コアごとに異なるベースポートがあります。

DTLS および TLS 制御接続の例を次の図に示します。vManage および vSmart 上のすべてのコアは vBond への永続的な接続を行い、WAN エッジルータは DTLS のみを使用して vBond への一時的な接続を行うことに注意してください。WAN エッジルータは、1 つの vManage および vSmart コアにのみ接続します。vManage および WAN エッジルータは、vSmart コントローラに接続するときにクライアントとして機能するため、TLS を使用する場合、送信元ポートはランダムな TCP ポート（1024 超）です。TLS の例の WAN エッジルータはオフセット 2 で設定されているため、vBond に接続するときに DTLS 送信元ポートのオフセットを使用します。

図 38.　　制御接続の DTLS および TLS ポートの例



WAN エッジルータから別の WAN エッジルータへの IPsec トンネルカプセル化では、DTLS で定義されたポートと同様の UDP が使用されます。

ネットワーク内のすべてのファイアウォールで、WAN エッジルータとコントローラ間、およびコントローラ間の通信が許可されていることを確認します。リターントラフィックも許可するように設定されていることを確認します。次の表に、コントロールプレーンとデータプレーンのトラフィックに使用されるポートの概要を示します。

表 2.　SD-WAN デバイス接続用の DTLS、TLS、および IPsec ポート

送信元デバイス	送信元ポート	接続先デバイス	宛先ポート
vManage/vSmart（DTLS）	Core1 = UDP 12346 Core2 = UDP 12446 Core3 = UDP 12546 Core4 = UDP 12646 Core5 = UDP 12746 Core6 = UDP 12846 Core7 = UDP 12946 Core8 = UDP 13046	vBond	UDP 12346
vManage（DTLS）	UDP 12346	vSmart	UDP 12346
vManage（DTLS）	UDP 12346	vManage	UDP 12346
vSmart（DTLS）	UDP 12346	vSmart	UDP 12346

送信元デバイス	送信元ポート	接続先デバイス	宛先ポート
WAN エッジ（DTLS）	UDP 12346+n、12366+n、12386+n、12406+n、および 12426+n。ここで、n は 0 ～ 19 で、設定されたオフセットを表します	vBond	UDP 12346
WAN エッジ（DTLS）	UDP 12346+n、12366+n、12386+n、12406+n、および 12426+n。ここで、n は 0 ～ 19 で、設定されたオフセットを表します	vManage/vSmart	Core1 = UDP 12346 Core2 = UDP 12446 Core3 = UDP 12546 Core4 = UDP 12646 Core5 = UDP 12746 Core6 = UDP 12846 Core7 = UDP 12946 Core8 = UDP 13046
vManage（TLS）	TCP ランダムポート番号（1024 超）	vSmart	TCP 23456
vManage（TLS）	TCP ランダムポート番号（1024 超）	vManage	TCP 23456
vSmart（TLS）	TCP ランダムポート番号（1024 超）	vSmart	TCP 23456
WAN エッジ（TLS）	TCP ランダムポート番号（1024 超）	vManage/vSmart	Core1 = TCP 23456 Core2 = TCP 23556 Core3 = TCP 23656 Core4 = TCP 23756 Core5 = TCP 23856 Core6 = TCP 23956 Core7 = TCP 24056 Core8 = TCP 24156
WAN エッジ（IPsec）	UDP 12346+n、12366+n、12386+n、12406+n、および 12426+n。ここで、n は 0 ～ 19 で、設定されたオフセットを表します	WAN エッジ	UDP 12346+n、12366+n、12386+n、12406+n、および 12426+n。ここで、n は 0 ～ 19 で、設定されたオフセットを表します

VPN 0 トランスポートの追加ポート

トランスポート インターフェイスの VPN 0 では、ほとんどすべての通信が DTLS/TLS または IPsec を介して行われますが、他にも考慮すべきポートがいくつかあります。

ネットワーク設定プロトコル（NETCONF）

NETCONF プロトコルは、ネットワークデバイスを管理および設定するメカニズムを定義します。vManage は、主に DTLS/TLS を介した SD-WAN デバイスとの通信に NETCONF を使用しますが、DTLS/TLS 接続が形成される前に NETCONF がネイティブに使用される状況がいくつかあります。

- コントローラ（vManage、vBond、または vSmart）が vManage に追加されると、vManage インスタンスは NETCONF を使用してそこから情報を取得し、デバイスとして GUI に追加できるようになります。これは、最初にコントローラを vManage に追加する場合、または vManage インスタンスをクラスタに追加するか、追加の vSmart または vBond コントローラを追加することによって、水平方向に段階的に拡張する場合です。
- コントローラがリロードまたはクラッシュした場合、暗号化された DTLS/TLS セッションが再形成される前に、そのコントローラは NETCONF を使用して vManage と通信します。
- NETCONF は、DTLS/TLS 接続が形成される前に vManage GUI を介してコントローラから証明書署名要求を生成するときに、vManage からも使用されます。

NETCONF は、AES-256-GCM を使用して暗号化された SSH であり、TCP 宛先ポート 830 を使用します。

セキュアシェル（SSH）

SSH は、セキュアでないネットワーク上でセキュアな暗号化チャネルを提供します。通常は、リモートマシンにログインしてコマンドを実行するために使用されますが、すべての SD-WAN デバイスとの間でファイル転送（SFTP）およびセキュアコピー（SCP）にも使用できます。コントローラ間で DTLS/TLS 接続がまだ形成されていない場合、vManage は SCP を使用して署名付き証明書をコントローラ上にインストールします。SSH は TCP 宛先ポート 22 を使用します。

Network Time Protocol（NTP）

NTP は、ネットワークデバイス間のクロック同期に使用されるプロトコルです。NTP サーバが使用されており、VPN 0 WAN トランスポートを介してネイティブにアクセスできる場合は、NTP がファイアウォールを通過できることを確認します。NTP は UDP ポート 123 を使用します。

ドメインネームシステム（DNS）

DNS は、ホスト名を解決するために DNS サーバを使用しており、サーバが VPN 0 トランスポートを介してネイティブに到達可能である場合に必要になることがあります。vBond または NTP サーバ名を解決するために DNS が必要になる場合があります。DNS は UDP ポート 53 を使用します。

Hypertext Transfer Protocol Secure（HTTPS）（vManage）

HTTPS は、vManage への管理者ユーザまたはオペレータのセキュアなアクセスを提供し、VPN 0 インターフェイスを介してアクセスできます。vManage は、TCP ポート 443 または 8443 を使用してアクセスできます。

vManage は、HTTPS（TCP ポート 443）を使用して、証明書サービスやプラグアンドプレイポータルなどの複数のサービスに到達します。Symantec/Digicert 証明書の場合、宛先ホストは certmanager.blu.websecurity.symauth.net で、Cisco PKI 証明書の場合は、宛先は cloudso.cisco.com で、その後に apx.cisco.com が続きます。WAN エッジルータの許可シリアル番号リストを自動的にダウンロードするために Cisco プラグアンドプレイポータルに同期する場合、vManage は宛先 cloudso.cisco.com に続いて apx.cisco.com を使用して HTTPS に到達する必要があります。

トンネルインターフェイスで許可されるプロトコル

VPN 0 トランスポート インターフェイスにはトンネルが設定されているため、コントロールおよびデータプレーンのトラフィックを暗号化し、ネイティブトラフィックを制限できます。DTLS または TLS 以外に、次のネイティブプロトコルがデフォルトでインターフェイスを介して許可されます。

DHCP

DNS

ICMP

HTTPS

技術的なヒント

SD-WAN デバイスの VPN 0 内のトランスポート インターフェイス下のトンネルで、必要な追加プロトコルも許可されていることを確認します。vManage GUI を使用して、VPN インターフェイス機能テンプレートのトンネルインターフェイスでプロトコルを有効または無効にできます。CLI では、コマンドは tunnel-interface の下の **allow-service *[protocol]*** です。すべての SD-WAN デバイスで **ntp** および **dns** を有効にし、コントローラで **netconf** を有効にする必要がある場合があります。証明書をインストールする目的でコントローラを導入する場合は、コントローラで **ssh** を有効にすることを検討してください。また、ネットワーク内のすべてのファイアウォールがこの通信を許可していることを確認します。

可能であれば、トランスポート インターフェイスで **ssh** を無効にします。vManage からの SSH は暗号化され、オーバーレイを通過するため、vManage 制御接続を確立できる場合は、インターフェイスでネイティブ SSH を許可する必要はありません。SSH が許可され、誰かが SSH セッションを試行し、不正なログインを 5 回連続して入力した場合、ユーザには 15 分の厳密なロックアウト期間が適用されます。その時間内にログインを試行すると、タイマーがリセットされ、無期限のロックアウト状態が発生する可能性があります。セカンダリユーザ名とパスワードを **netadmin** 権限で設定することも推奨されます。

これらの追加ポートの概要は次のとおりです。

表 3. SD-WAN デバイス通信用の追加 VPN 0 プロトコルの概要

サービス	プロトコル/ポート	方向
NETCONF	TCP 830	bidirectional
SSH	TCP 22	bidirectional
NTP	UDP 123	outgoing
DNS	UDP 53	outgoing
HTTPS	TCP 443/8443	bidirectional

コントローラ管理用のポート

SD-WAN デバイスの VPN 512 インターフェイスでは、追加の管理プロトコルを使用できます。これらの概要は次のとおりです。

表 4. SD-WAN デバイスの管理プロトコルの概要

サービス	プロトコル/ポート	方向
NETCONF	TCP 830	bidirectional
SSH	TCP 22	incoming
SNMP クエリ	UDP 161	incoming
RADIUS	UDP 1812	outgoing
SNMP トラップ	UDP 162	outgoing
Syslog	UDP 514	outgoing
TACACS	TCP 49	outgoing
HTTPS（vManage）	TCP 443、8443、80	incoming

vManage クラスタリングおよびディザスタリカバリ用のポート

vManage クラスタの場合、コントローラのクラスタインターフェイスで次のポートを使用できます。クラスタメンバー間に存在するファイアウォール内で正しいポートが開かれていることを確認します。

表 5. vManage クラスタリングに必要なポートの概要

vManage サービス	プロトコル/ポート	方向
アプリケーションサーバ	TCP 80、443、7600、8080、8443、57600	bidirectional
設定データベース	TCP 6362-6372、7687、7474、5000、6000、7000	bidirectional
調整サーバ	TCP 2181、3888	bidirectional
メッセージバス	TCP 9092	bidirectional
統計データベース	TCP 9200、9300	bidirectional
デバイス設定のトラッキング（NCS および NETCONF）	TCP 830	bidirectional

ディザスタリカバリが設定されている場合は、プライマリクラスタとスタンバイクラスタ間のデータセンターのアウトオブバンド インターフェイスで次のポートが開かれていることを確認します。

表 6. vManage ディザスタリカバリに必要なポートの概要

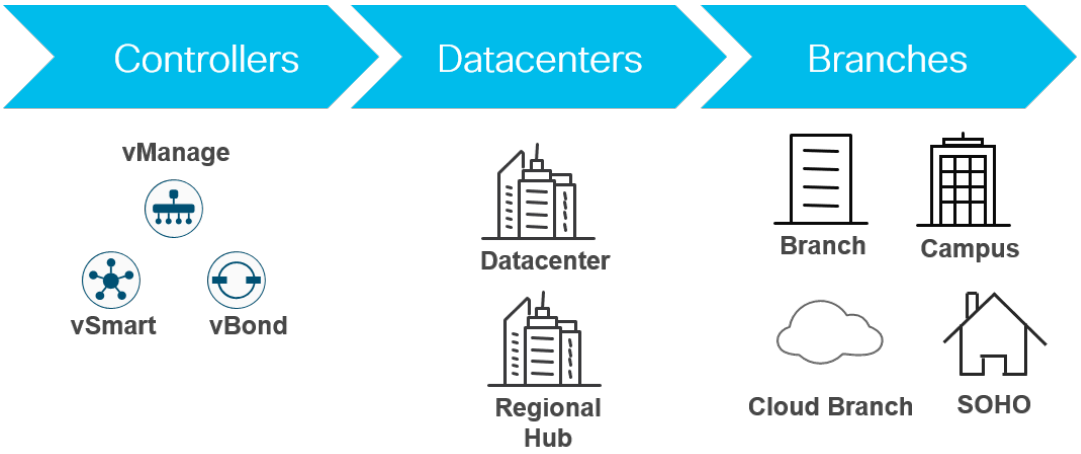
vManage サービス	プロトコル/ポート	方向
ディザスタリカバリ	TCP 443、830、18600、18500、18501、18301、18302、18300	bidirectional

コントローラの導入

概要

SD-WAN の導入では、まずコントローラを導入して設定し、次にメインハブまたはデータセンターのサイト、最後にリモートサイトの順に設定します。各サイトが導入されると、最初にコントロールプレーンが確立され、その後自動的にデータプレーンが確立されます。サイトを SD-WAN に移行する際には、SD-WAN サイトと非 SD-WAN サイト間のルーティングにハブサイトを使用することをお勧めします。

図 39.　　SD-WAN 導入シーケンス



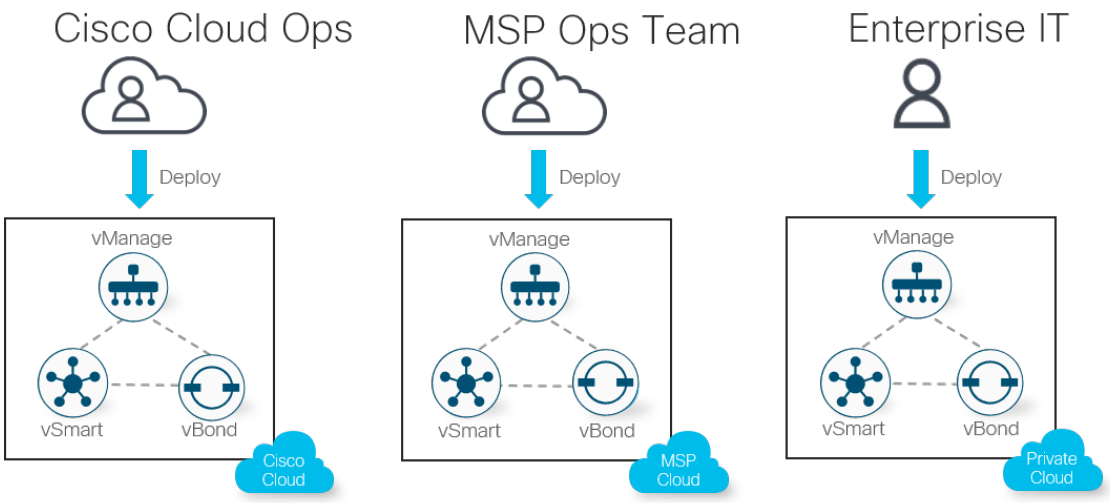
コントローラ導入オプション

お客様は、複数の柔軟なコントローラ導入オプションを利用できます。コントローラは次のように導入できます。

- シスコがホストするクラウド内。これは推奨モデルであり、コントローラは AWS または Azure に導入できます。単一または複数のゾーンを導入に使用できます。ほとんどのお客様は、導入が容易で拡張性に優れているため、シスコのクラウドホスト型コントローラを選択します。シスコは、証明書を使用してコントローラをプロビジョニングし、規模と冗長性の要件を満たします。シスコは、バックアップ/スナップショットとディザスタリカバリを担当します。お客様には、vManage へのアクセス権が付与され、デバイスの設定テンプレートと制御およびデータポリシーが作成されます。
- マネージド サービス プロバイダー（MSP）またはパートナーがホストするクラウド内。これはプライベートクラウドでホストされるか、パブリッククラウドでホストされ、AWS または Azure に導入されます。通常、MSP またはパートナーは、コントローラのプロビジョニングと、バックアップおよびディザスタリカバリを担当します。
- 組織が所有するプライベートクラウドまたはデータセンターでのオンプレミス。通常、お客様は、コントローラのプロビジョニングと、バックアップおよびディザスタリカバリを担当します。金融機関や政府機関などの一部のお客様は、主にセキュリティおよびコンプライアンスの理由により、オンプレミス導入を選択する場合があります。

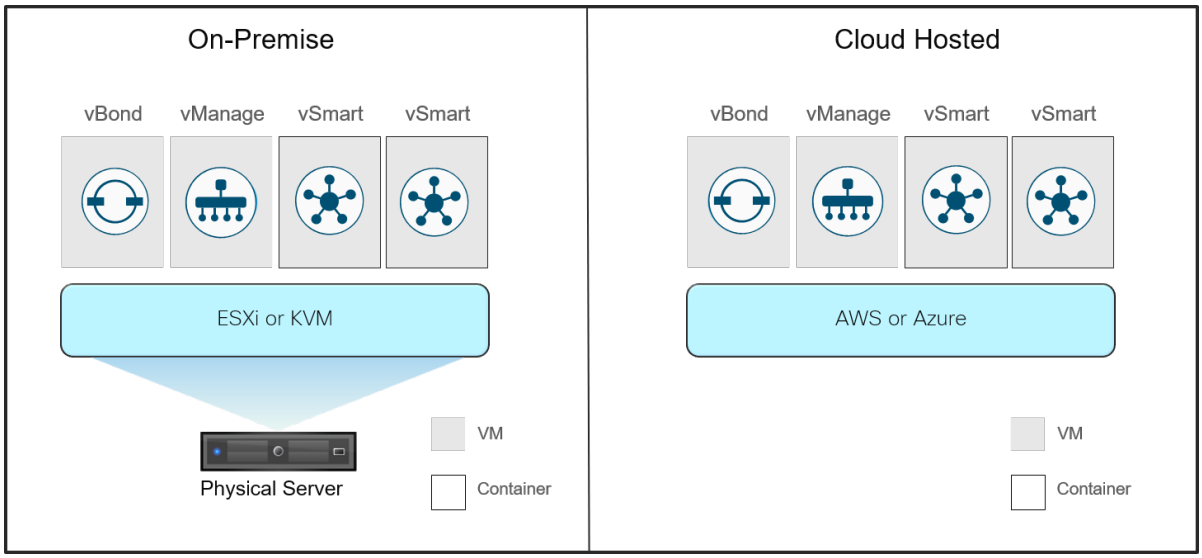
MSP には、これらの導入のいずれかを持つお客様が存在し、各タイプの導入で異なるレベルのサービスと管理オプションを提供する場合があることに注意してください。

図 40.　　柔軟なコントローラ導入オプション



クラウドホスト型の導入では、コントローラを Amazon Web Services（AWS）または Microsoft Azure に導入できます。オンプレミス型または SP ホスト型の導入では、コントローラは ESXi または KVM のデータセンターに導入されます。仮想マシン（VM）またはコンテナのいずれかを導入できます。

図 41.　　コントローラ導入オプション



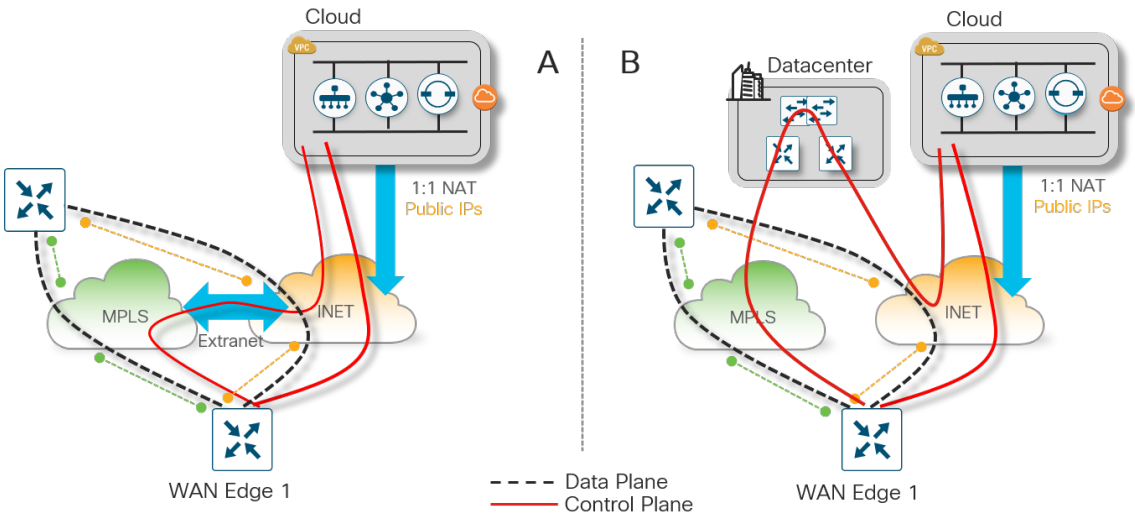
シスコのクラウドホスト型導入（推奨）

Cisco SD-WAN コントローラのクラウドホスト型導入は、シスコがオーケストレーションし、導入と拡張が容易で高可用性であるため、推奨される導入モードです。コントローラに接続するには、インターネットへの到達可能性が必要です。欠点は、2 番目のトランスポートを介してインターネットに到達できない場合、制御接続の冗長性がないことです。

次の図は、クラウドホスト型の導入例です。コントローラはパブリッククラウドでホストされ、インターネット トランスポート経由で到達可能です。WAN エッジルータは、すべてのトランスポートを介してコントローラへの制御接続を確立しようとします。3 種類の一般的なシナリオがあります。

- 導入 A では、インターネット トランスポートは MPLS トランスポートからエクストラネットまたは直接接続を介して到達可能であるため、WAN エッジ 1 は両方のトランスポートからコントローラに直接接続できます。このため、MPLS クラウドは、ネットワークに応じて、コントローラのパブリックにルーティング可能な IP アドレス、またはデフォルトルートをアドバタイズします。
- 導入 B では、MPLS トランスポートにエクストラネット接続がなく、代わりに、両方のトランスポートに接続されている地域のハブまたはデータセンターサイトを経由してルーティングされることでインターネットに到達できます。このために、データセンターサイトは、ネットワークに応じて、コントローラのパブリックにルーティング可能な IP アドレス、またはデフォルトルートをアドバタイズします。

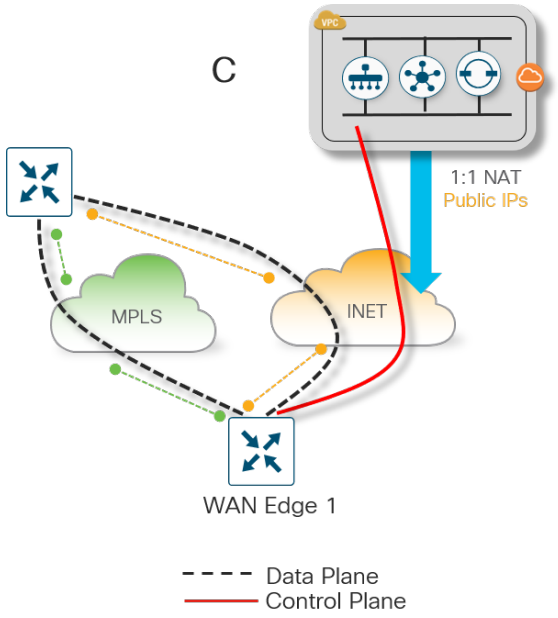
図 42.　　クラウドホスト型の導入制御およびデータプレーン確立オプション A および B



- 導入 C では、インターネット トランスポートは MPLS トランスポートから到達できないため、WAN エッジ 1 はインターネット トランスポートからのみコントローラに接続できます。TLOC 情報は引き続きインターネット トランスポートから OMP 経由で受信されるため、WAN エッジ 1 は MPLS トランスポートを介してデータプレーン IPsec 接続を確立できます。インターネット トランスポートに障害が発生した場合のコントロールプレーンの冗長性はありません。

技術的なヒント
導入 C では、MPLS トンネルインターフェイスで **max-control-connections 0** を使用する必要があります。これにより、TLOC に制御接続がないことが WAN エッジルータに通知されます。MPLS TLOC はインターネット側の制御接続を介してアドバタイズされますが、データプレーン接続は MPLS トランスポートを介して他の WAN エッジルータと引き続き形成できます。

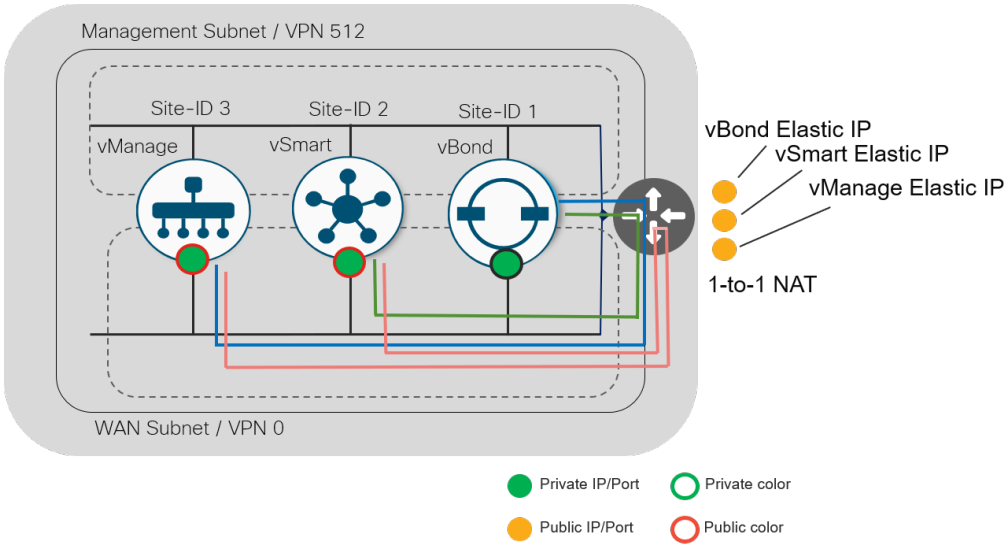
図 43.　　クラウドホスト型の導入制御およびデータプレーン確立オプション C



クラウドホスト型導入コントローラの通信

クラウドホスト型環境では、コントローラは仮想ゲートウェイの背後に配置されます。各コントローラはプライベート IP アドレスでアドレス指定され、仮想ゲートウェイは、各プライベート コントローラ アドレスを個別のパブリックにルーティング可能な IP アドレスに変換して 1 対 1 の NAT を適用し、インターネット経由で到達可能にします。

図 44.　　クラウドホスト型導入：コントローラ通信



vManage および vSmart コントローラは、トンネルインターフェイスでパブリックカラーを使用します。これにより、常にパブリック IP アドレスを使用して WAN エッジデバイスと通信します。vBond インターフェイスにはカラーの概念はありません。

vSmart および vManage には、vBond のパブリック IP アドレスを指す vBond 設定があります。いずれかのコントローラが vBond と通信しようとすると、トラフィックはゲートウェイを通過し、ゲートウェイは vSmart および vManage のプライベート IP に 1 対 1 の送信元 NAT を適用します。次に、vBond は NAT が実行されたパブリック IP アドレスを使用して vSmart および vManage と通信するため、リターントラフィックもゲートウェイを通過する必要があります。vBond がパブリックアドレスを介して vSmart および vManage と通信することは、vBond がこれらの IP アドレスを学習し、オーバーレイに接続する WAN エッジデバイスにそれらのパブリック IP アドレスを渡すことができるための要件です。

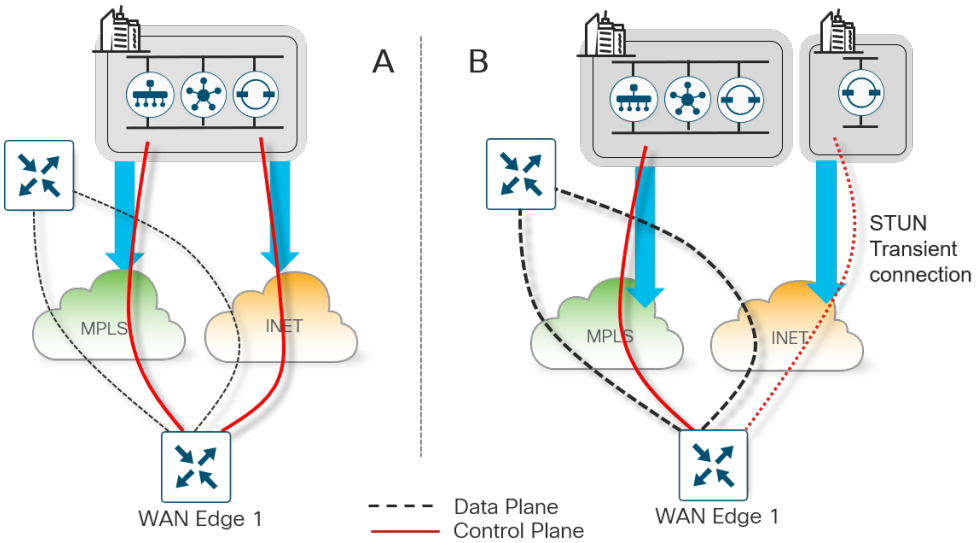
vManage と vSmart は、NAT が実行されたパブリック IP アドレスを介して相互に通信します。これは、パブリックカラー設定とサイト ID 設定が異なるためです。サイト ID が等しければ、プライベート IP アドレスを介して通信し、その通信のゲートウェイをバイパスします。

オンプレミスコントローラの導入

このタイプのコントローラの導入では、コントローラはデータセンターまたはプライベートクラウドにオンプレミスで導入されます。通常、企業の IT 組織はコントローラのプロビジョニングとバックアップとディザスタリカバリを担当します。金融機関や政府機関などの一部のお客様は、主にセキュリティ コンプライアンスの理由により、オンプレミス導入を選択する場合があります。

次の図は、オンプレミス導入の 2 つの例です。導入 A では、WAN エッジ 1 は両方のトランスポートからデータセンターのコントローラに接続できます。導入 B では、コントローラはプライベート MPLS を介してのみ到達可能です。追加の vBond がインターネットに導入され、インターネットにアクセスできる WAN エッジデバイスの STUN サーバとして機能し、それらをプライベートコントローラの IP アドレスにリダイレクトします。TLOC 情報は引き続き MPLS トランスポートから OMP 経由で受信されるため、WAN エッジ 1 はインターネット トランスポートを介してデータプレーン IPsec 接続を確立できます。

図 45.　　オンプレミスの導入制御とデータプレーンの確立



オンプレミスの導入では、NAT、パブリック IP、および/またはプライベート IP を使用してコントローラを配置する方法が複数あります。オンプレミスの導入の一般的なオプションは次のとおりです。

- 制御接続は、パブリックにルーティング可能な IP アドレスを使用して、インターネット トランスポートと MPLS トランスポートの両方を介して確立されます。パブリックにルーティング可能な IP アドレスは、コントローラに直接割り当てることも、1 対 1 の NAT を使用して割り当てることもできます。
- 制御接続は、プライベート（RFC 1918）IP アドレスを使用して MPLS トランスポートを介して確立され、パブリックにルーティング可能な IP アドレスを使用してインターネットを介して確立されます。vBond は、いずれかのトランスポートからアクセス可能な、パブリックにルーティング可能な IP アドレスを使用できます。または、MPLS トランスポートを介して、プライベート RFC 1918 IP アドレス経由でアクセスできます。

コントローラの冗長性および高可用性

コントローラの冗長性は、コントローラのタイプに応じてさまざまな方法で実現されます。

vBond オーケストレータ

vBond オーケストレータの冗長性は、複数の vBond コントローラを起動し、単一の完全修飾ドメイン名（FQDN）を使用して vBond コントローラを参照することで実現されます。FQDN は、WAN エッジルータか、vSmart または vManage コントローラの **system vbond** コンフィギュレーション コマンドで使用されます。適切な冗長性を維持するために、クラウドから管理する場合はさまざまな地域で、またはオンプレミスで導入する場合はさまざまな地理的場所/データセンターで、vBond オーケストレータを使用することをお勧めします。これにより、SD-WAN デバイスがネットワークに参加しようとしているときに、少なくとも 1 つの vBond が常に使用可能になります。

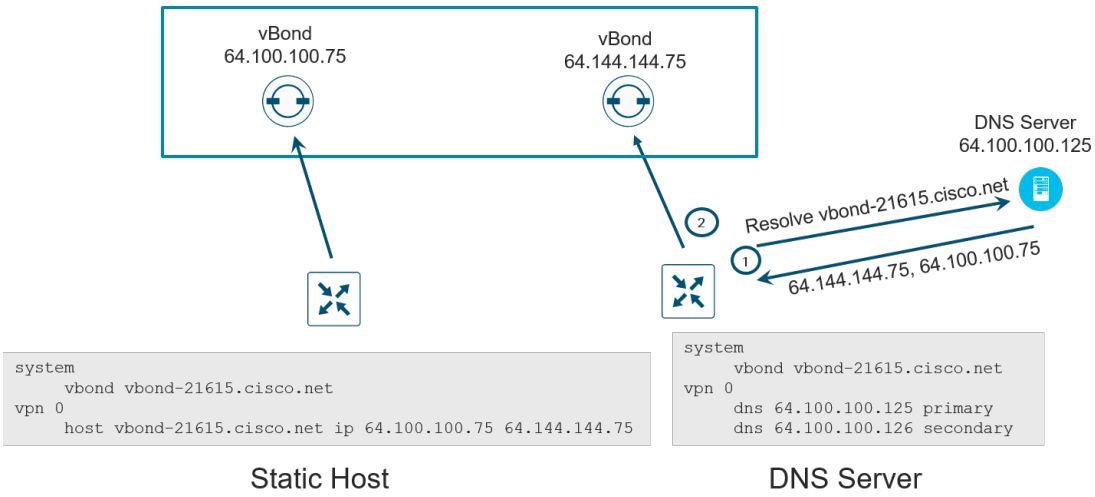
ドメインネームサーバ（DNS）では、複数の IP アドレスが vBond の FQDN に関連付けられます。通常、すべての vBond IP アドレスは DNS クエリアに戻され、各 IP アドレスは接続が成功するまで連続して試行されます。DNS リストへの開始点インデックスは、ハッシュ関数によって決定されます。DNS サーバが使用できない場合は、代替手段としてスタティック ホスト ステートメントを WAN エッジで設定できます。

ネットワークに存在する vBond オーケストレータが 1 つだけの場合でも、vBond にはドメイン名を使用することをお勧めします。これにより、オーケストレータを追加してもネットワークで設定を変更する必要がなくなります。

各 vBond は、vManage および vSmart コントローラの各コアへの永続的な接続を確立することに注意してください。これにより、vBond がネットワークに参加している WAN エッジルータに使用できないコントローラの IP アドレスを提供しないようにすることができます。vBond オーケストレータ自体またはそれらの間で維持される状態の間には、コントローラ接続はありません。

次の図は、スタティック ホスト ステートメントまたは DNS サーバを使用した WAN エッジルータからの vBond 冗長性を示しています。WAN エッジルータは、IP アドレスを学習し、vManage および vSmart コントローラに対して認証を行う前に、まず各トランスポートを介して vBond オーケストレータに接続する必要があります。

図 46.　　vBond オーケストレータの冗長性



vSmart コントローラ

vSmart コントローラの場合、アクティブ/アクティブ方式で動作するコントローラを追加することで冗長性が実現されます。適切な冗長性を維持するために、クラウドから管理する場合はさまざまな地域で、またはオンプレミスで導入する場合はさまざまな地理的場所/データセンターで、vSmart コントローラを使用することをお勧めします。

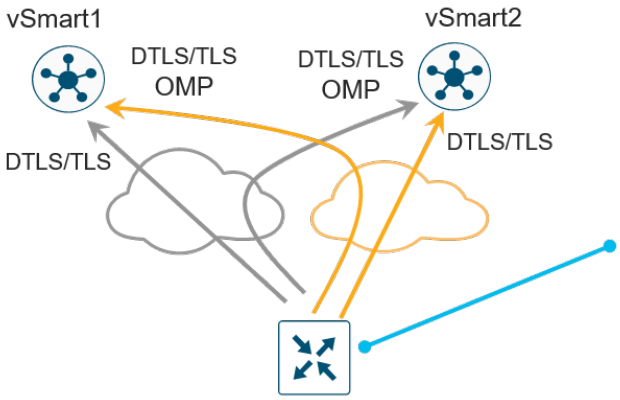
デフォルトでは、WAN エッジルータは、各トランスポートを介して 2 つの vSmart コントローラに接続します。vSmart コントローラの 1 つに障害が発生した場合、他の vSmart コントローラがネットワークのコントロールプレーンの処理をシームレスに引き継ぎます。1 つの vSmart コントローラが存在し、ドメイン内で動作している限り、ネットワークは中断することなく動作を継続できます。vSmart コントローラは、相互にフルメッシュの DTLS/TLS 接続を維持し、その上で OMP セッションのフルメッシュが形成されます。OMP セッションでは、ルート、TLOC、ポリシー、サービス、および暗号キーを交換することで、vSmart コントローラの同期が維持されます。

技術的なヒント
すべての WAN エッジルータは、接続先の vSmart コントローラに関係なく、ネットワークの同一ビューを表示する必要があるため、すべての制御ポリシーが各 vSmart コントローラで同一であることが非常に重要です。すべての vSmart コントローラが vManage によって管理されている場合、vManage はすべての vSmart コントローラに集中型ポリシーを適用するため、その制御ポリシーは同一になります。

VPN 0 の各インターフェイストンネルで **max-control-connections** コマンドを使用して、各 TLOC を介して WAN ルータが vSmart コントローラと確立する vSmart 接続の数を制御できます。デフォルトの設定は 2 です。さらに、システム設定の下に **max-mp-sessions** コマンドがあり、これも調整できます。このデフォルトの設定も 2 です。同じ vSmart コントローラに対して行われる接続の数は、同じ OMP セッションの一部と見なされることに注意してください。WAN エッジの **max-control-connections** で許容される数を超える vSmart コントローラがネットワークにある場合、WAN エッジルータの制御接続は vSmart コントローラのサブセットにハッシュされます。

次の図では、WAN エッジは各トランスポートを介して 2 つの DTLS または TLS 制御接続を確立します（各 vSmart コントローラに対して 1 つ）。OMP はこの接続を介して動作します。各 TLOC からの接続は **max-control-connections** コマンド（2）によって制限され、合計 OMP セッションは **max-mp-sessions** コマンド（2）によって制限されます。

図 47.　　vSmart コントローラの冗長性




```
system
     max-omp-sessions 2
vpn 0
     interface ge0/2
       tunnel-interface
         max-control-connections 2

     interface ge0/4
       tunnel-interface
         max-control-connections 2
```

vSmart コントローラのアフィニティ

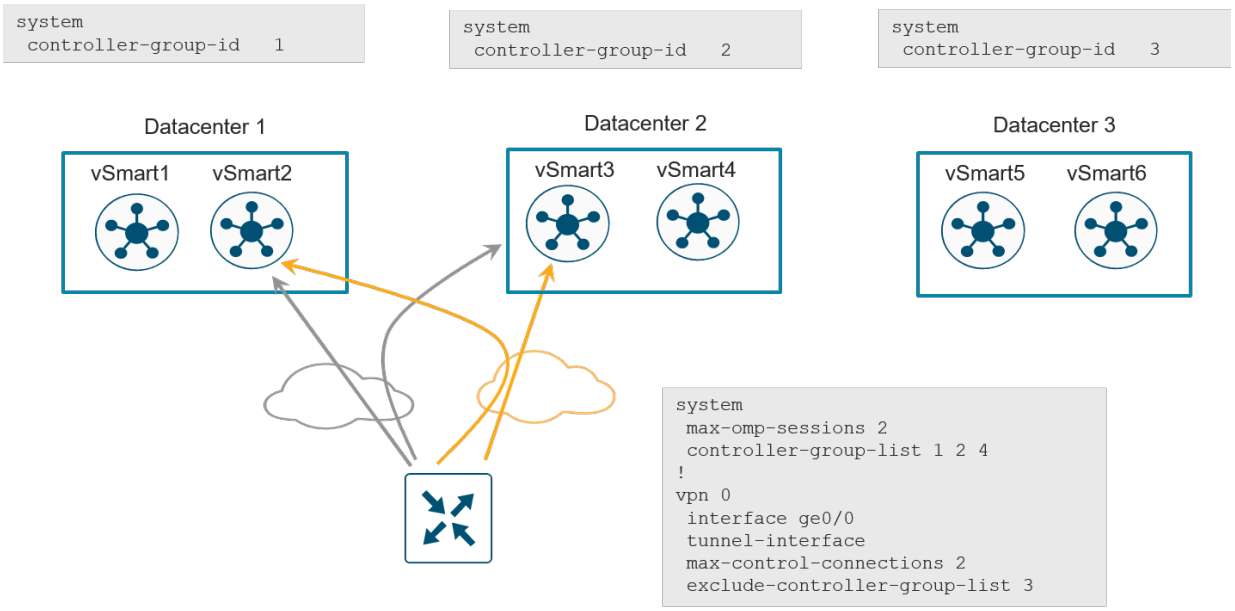
ネットワークが拡大し、より多くの vSmart コントローラがネットワークに追加され、グローバルに分散された場合、アフィニティを使用して、拡張を管理し、WAN エッジルータが接続する vSmart コントローラを選択できます。これは、WAN エッジデバイスを同じ地域のコントローラに接続する場合に重要であり、冗長性のために適切な vSmart コントローラに接続するのに役立ちます。たとえば、West データセンターに 2 つの vSmart コントローラがあり、East データセンターに 2 つの vSmart コントローラがあり、WAN エッジルータを 2 つの vSmart コントローラに接続する場合、1 つの WAN Edge ルータを West データセンターの両方の vSmart コントローラに接続したくはありません。適切な冗長性を確保するには、West データセンターの vSmart への接続を 1 つ、East データセンターの vSmart への接続を 1 つにする必要があります。

コントローラグループを使用してアフィニティを実現できます。各 vSmart コントローラは、コントローラグループに割り当てられます。コントローラグループ内では、WAN エッジルータは vSmart コントローラに接続します。その vSmart が使用できなくなると、WAN エッジは同じコントローラグループ内の別の vSmart コントローラへの接続を試みます。

vSmart コントローラへの接続数を最小限に抑えながら、適切なレベルの冗長性を維持することをお勧めします。デフォルトでは、各 TLOC の **max-control-connections** は 2 で、**max-omp-sessions** は 2 です。そのため、WAN エッジデバイスは、最大で 2 つの異なる vSmart コントローラとの接続を確立します。vSmart コントローラはコントローラグループ ID を使用して設定され、WAN エッジルータは接続先のグループ ID の優先順位に従ってコントローラグループリストを使用して設定されます。

次の図に、地域に応じた導入でのアフィニティの使用例を示します。この図は、3 つのデータセンターを示しています。vSmart コントローラは、データセンター 1 の controller-group-id 1、データセンター 2 の controller-group-id 2、データセンター 3 の controller-group-id 3 の一部です。各 DC は異なる地域にあります。

図 48.　　vSmart アフィニティの例



WAN エッジルータでは次の設定が行われます。

- **max-omp-sessions** 2：WAN エッジデバイスは、最大 2 つの異なる vSmart コントローラを接続できます（2 つのデバイス間で形成される DTLS/TLS セッションの数に関係なく、vSmart ごとに 1 つの OMP セッションが確立されます）。
- **max-control-connections** 2：WAN エッジデバイスは、TLOC ごとに 2 つの vSmart コントローラに接続できます。
- **controller-group-list** 1 2 4：WAN エッジルータが属するコントロールグループを優先順に示します。ルータは、同じコントローラグループ内のコントローラに接続できます。WAN エッジルータは、コントローラの現在の状態と WAN エッジ設定セッションの制限に基づいて、明示的に除外されていないすべてのコントローラグループに接続しようとします。この例では、ルータは最初にグループ 1 の vSmart コントローラに接続し、次に各トランスポートのグループ 2 に接続しようとします。
- **exclude-controller-group-list** 3：controller-group-id 3 に接続しないことを示します。

controller-group-id 1 の vSmart コントローラが使用できなくなると、WAN エッジルータは controller-group-id 1 の別の vSmart コントローラに接続しようとします。controller-group-id 1 と 2 の両方が使用できない場合、WAN エッジルータは controller-group-id 3 を除く controller-group-list（4）内の別の使用可能なグループ、または exclude-controller-group-id コマンドで定義した別のグループに接続しようとします。controller-group-list に他のコントローラグループがリストされていない場合、ルータはオーバーレイへの接続を失います。

各コントローラグループの vSmart コントローラの数は同じにすることをお勧めします。各 vSmart コントローラは、ネットワーク全体で同じハードウェアリソース機能を持つ必要があります。

vManage ネットワーク管理システム（NMS）

vManage は、スタンドアロンとクラスタリングの 2 つの基本的な方法で導入できます。プライマリクラスタ内のすべての vManage インスタンスはアクティブモードで動作します。vManage クラスタの目的は拡張性です。単一の vManage 障害に対する冗長性レベルは提供しますが、クラスタレベルの障害に対する保護は行いません。クラスタメンバー間のデータベース レプリケーションには 4 ミリ秒以下の遅延が必要なため、地理的な場所をまたいだクラスタリングは推奨されません。したがって、クラスタのメンバーは同じサイトに存在する必要があります。冗長性は、スタンバイモードのバックアップ vManage またはバックアップ vManage クラスタで実現されます。

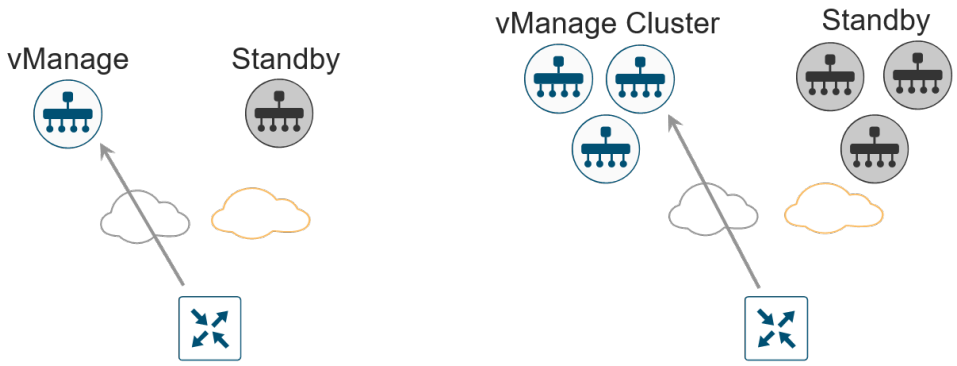
原則として、WAN エッジルータの数が 2000 以下の場合は、アクティブモードの vManage をプライマリとして、スタンバイモードの vManage をバックアップとして導入します。冗長性を実現するために、これらを 2 つの異なる地理的な場所に導入することを推奨します。

WAN エッジルータの数が 2000 を超える場合は、アクティブモードの vManage クラスタをプライマリとして、およびスタンバイモードの vManage クラスタをバックアップとして導入します。クラスタには、少なくとも 3 つの vManage インスタンスが必要であり、それぞれがアクティブで独立して実行されます。冗長性を実現するために、各クラスタを 2 つの異なる地理的な場所に導入することを推奨します。

技術的なヒント
ネットワークによっては、アプリケーションの可視性と統計情報が vManage で CPU を集中的に使用する可能性があるため、単一の vManage でサポートされる WAN エッジルータの数が減少します。

WAN エッジルータは、いずれかのトランスポートを介して vManage に接続します。WAN エッジのトンネルインターフェイスの **vmanage-connection-preference *<number>*** コマンドで、使用するトランスポートを制御できます。vManage への接続に使用する特定のトンネルインターフェイスを優先するには、より高いプリファレンス値を使用します。vManage 接続には最高の帯域幅のリンクを使用し、可能な場合はセルラーインターフェイスを使用しないようにします。ゼロの値は、トンネルインターフェイスが vManage に接続しないことを示します。少なくとも 1 つのトンネルインターフェイスにゼロ以外の値を設定する必要があります。

図 49.　　vManage の冗長性



シスコがホストするクラウド導入では、スタンバイ vManage インスタンスは導入されないことに注意してください。Cisco Cloud Ops は、vManage バックアップとディザスタリカバリを処理します。

vManage クラスタリング

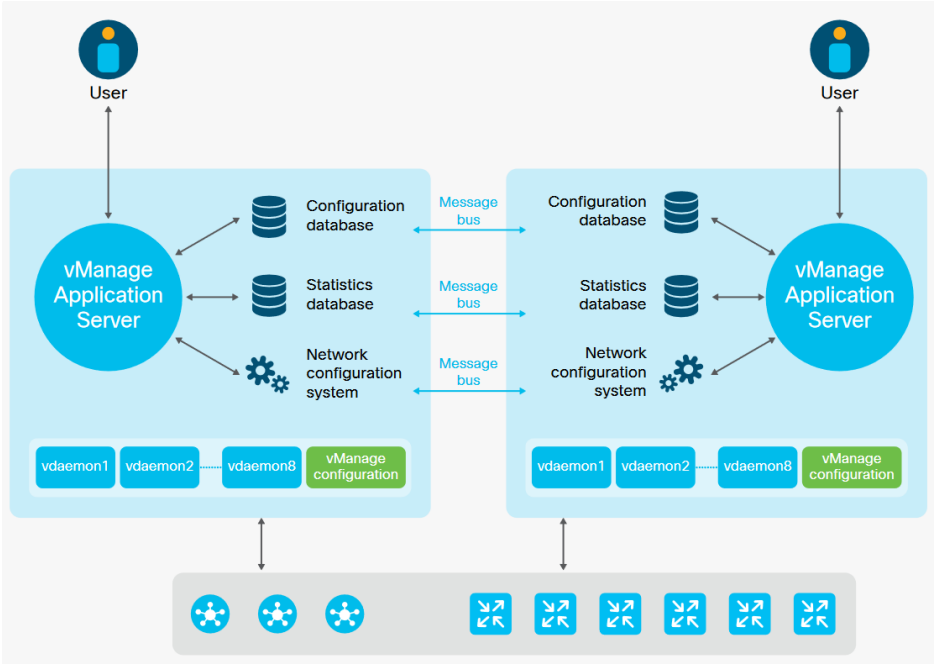
vManage クラスタは、さまざまな NMS サービスの負荷を分散し、vManage サービスに高可用性と拡張性を提供します。vManage は、少なくとも 3 つの vManage サーバインスタンスで構成され、それぞれがアクティブで独立して実行されます。vManage サーバと WAN ルータ間の制御接続もロードバランシングされます。制御接続（各 vManage インスタンスから各 vSmart へ、各 vManage インスタンスから他の各 vManage インスタンスへ、および各 vManage インスタンスコアから各 vBond へ）は完全にメッシュ化されています。

vManage クラスタは、クラスタが動作している間は単一の vManage サーバの障害を許容するように設計する必要がありますが、高可用性を確保するためには、vManage クラスタが存在するサイトに対するクラスタ障害または接続障害の場合に、スタンバイクラスタが導入されている必要があります。

vManage サーバは、いくつかの主要なサービスを実行します。次の内容で構成されています。

- アプリケーションサーバ：管理者セッションの Web サーバ（GUI）です。ユーザはステータスとネットワークイベントを表示でき、証明書、ソフトウェア、デバイスの再起動、および vManage クラスタ設定を管理できます。
- 統計データベース：オーバーレイネットワーク内のすべての SD-WAN デバイスからの統計データ、監査ログ、アラーム、およびイベントが保存されます。
- 設定データベース：デバイスインベントリ、ポリシー、証明書、および SD-WAN デバイスの設定と状態が保存されます。
- メッセージングサーバ：このサービスは、クラスタ内の vManage デバイス間でメッセージを渡し、データを共有し、動作を調整します。vManage デバイスは、それらの間でメッセージバスを介して情報を共有します。これは、特にクラスタ内のデバイスと通信するための VPN 0 の個別のインターフェイスです。
- ネットワーク設定システム：このシステムは、SD-WAN デバイスに設定をプッシュし、SD-WAN デバイスから設定を取得します。

図 50.　　vManage クラスタコンポーネント



vManage クラスタを導入する際には、次の点に注意してください。

- クラスタリングのために、VPN 0（トランスポート）および VPN 512（管理）に使用されるインターフェイスに加えて、3 番目のインターフェイスが必要です。このインターフェイスは、クラスタ内の vManage サーバ間の通信および同期に使用されます。このインターフェイスは 1 Gbps 以上で、遅延は 4 ms 以下である必要があります。10 Gbps インターフェイスが推奨されます。
- ESXi では、インターフェイスに VMXNET3 アダプタを使用することをお勧めします。VMXNET3 は 10 Gbps の速度をサポートします。VMXNET3 NIC を使用可能にするには、ESXi 5.0 以降（VM バージョン 8）の互換性設定で、[Edit Settings] > [VM Options] > [General Options] で、VMXNET3 をサポートするゲスト OS バージョン（**Ubuntu Linux（64 ビット）**または **Red Hat Linux 5（64 ビット）**以降など）を選択します。
- 設定および統計情報サービスは、少なくとも 3 つの vManage デバイスで実行する必要があります。各サービスは奇数のデバイスで実行する必要があります。これは、書き込み操作中のデータの整合性を確保するために、vManage デバイスのクォーラム（単純な過半数）が実行中で同期している必要があるためです。クラスタ内に 4 つの vManage デバイスがある場合、これらのサービスが奇数のデバイスで実行されるように、vManage サーバの 1 つで統計および設定データベースサービスを無効にします。
- クラスタを変更すると、サービスの再起動とクラスタの再同期が必要になる場合があります。クラスタ設定の変更は、メンテナンス期間中に行う必要があります。

その他のベストプラクティスのガイダンスと vManage クラスタの設定およびトラブルシューティングに関する情報については、https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-741440.pdf を参照してください。

ディザスタリカバリ

vBond および vSmart コントローラはステートレスです。仮想マシンのスナップショットは、メンテナンスまたは設定変更の前に作成できます。CLI モードで実行している場合は、設定をコピーして保存できます。また、vManage で機能テンプレートまたは CLI テンプレートが設定されている場合（vManage から集中型ポリシーを作成して適用する場合は vSmart に必要）、それらの設定は vManage スナップショットおよびデータベースとともに保存されます。ディザスタリカバリのシナリオでは、スナップショットを復元したり、デバイスを再導入したり、vManage から設定テンプレートをプッシュしたりできます。

vManage は唯一のステートフル SD-WAN コントローラであり、そのバックアップはアクティブモードで導入できません。vManage サーバの場合、スナップショットを作成し、データベースを定期的にバックアップする必要があります。

さまざまなディザスタリカバリ方式を使用できます。一般的なディザスタリカバリのシナリオでは、アクティブ vManage または vManage クラスタは、少なくとも 1 つのアクティブな vSmart コントローラと vBond オーケストレータとともに、1 つのデータセンターサイトに存在します。2 番目のデータセンターでは、スタンバイ（非アクティブ）vManage または vManage クラスタは、少なくとも 1 つのアクティブな vSmart コントローラと vBond オーケストレータとともに導入されます。アクティブ vManage または vManage クラスタでは、各 vManage インスタンスが両方のデータセンターの vSmart コントローラと vBond オーケストレータへの制御接続を確立します。スタンバイ vManage または vManage クラスタがアクティブになると、両方のデータセンターで vSmart コントローラと vBond オーケストレータへの制御接続が確立されます。

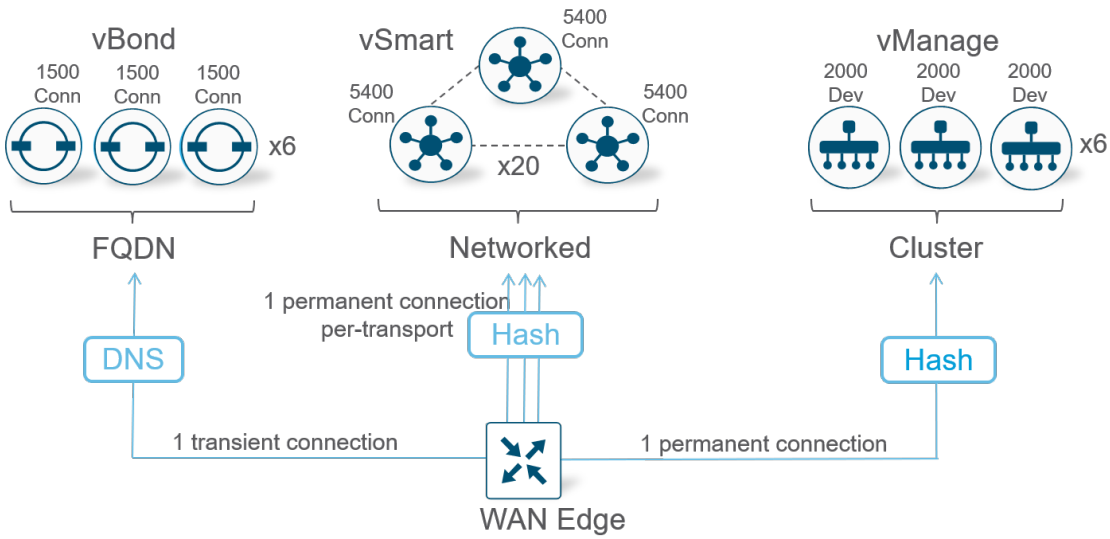
次のディザスタリカバリ方式を使用できます。

- 手動（vManage スタンドアロンまたはクラスタ）：バックアップ vManage サーバまたは vManage クラスタは、コールドスタンバイ状態でシャットダウンされたままになります。アクティブデータベースの定期的なバックアップが作成され、プライマリ vManage または vManage クラスタがダウンすると、スタンバイ vManage または vManage クラスタが手動で起動され、バックアップデータベースが復元されます。
- システムトリガー フェールオーバー（vManage クラスタ）：vManage コードの 19.2 バージョンから、システムトリガー ディザスタリカバリ スイッチオーバー オプションを設定できます。データは、プライマリとセカンダリの vManage クラスタ間で自動的に複製されます。アービトレータ vManage はクラスタをモニタし、必要なフェールオーバーを実行します。アービトレータは、アクティブクラスタとスタンバイクラスタの両方をモニタするために 3 番目のデータセンターに配置することも、スタンバイクラスタと同じサイトに配置することもできます。vManage クラスタとアービトレータは、サイト間の DCI を介して拡張される vManage クラスタリンクを介して通信します。
- 管理者がトリガーするフェールオーバー（vManage クラスタ）（推奨）：これは、システムがトリガーする DR フェールオーバー方式に似ていて、データはプライマリとセカンダリの vManage クラスタ間で自動的に複製されますが、セカンダリクラスタへのスイッチオーバーを手動で実行する必要があります。アービトレータ vManage は必要ありません。これは、vManage コードのバージョン 19.2 以降でサポートされています。これは、推奨されるディザスタリカバリ方式です。

コントローラのスケーリング

- vBond オーケストレータ：vBond オーケストレータは、各アクティブ vManage コア（最大 8）と各 vSmart コア（最大 8）との永続的な接続を維持します。WAN エッジルータは最初は vBond に接続しますが、vManage および vSmart コントローラへの永続的な接続が確立されると、その接続は一時的なものになります。各 vBond オーケストレータは 1500 の接続をサポートし、1 つの Cisco SD-WAN ドメインで最大 6 つの vBond オーケストレータがテストされています。2000 台 の WAN エッジデバイスごとに 1 つの vBond を見積もります。vBond への WAN エッジ接続は一時的なものであるため、スケーリング要件を簡素化するために vBond をオーバーサブスクライブできます。十分な冗長性を確保するために、vBond オーケストレータが追加されていることを確認します。
- vSmart コントローラ：vSmart コントローラは、各アクティブ vManage サーバと他のすべての vSmart コントローラへの永続的な接続を維持し、各 vSmart コントローラコア（最大 8）は、各 vBond オーケストレータとの永続的な接続を維持します。WAN エッジルータは、デフォルトで各トランスポートを介して 2 つの vSmart コントローラに永続的に接続します。各 vSmart コントローラは、コントローラあたり 5400 の接続をサポートし、最大 20 台のコントローラが高可用性環境でテストされています。各コントローラは、最大 2700 の OMP セッションと 256K のルートもサポートします。2000 台の WAN エッジデバイスごとに 1 つの vSmart コントローラを見積もります。多くの導入では、冗長性のために 2 つの vSmart コントローラで十分ですが、大規模な導入では、追加のコントローラを導入し、アフィニティ機能を使用して WAN エッジルータに制御接続を分散できます。
- vManage サーバ：vManage コントローラは、各 vSmart コントローラと他のすべてのアクティブ vManage サーバへの永続的な接続を維持し、各 vManage コントローラコア（最大 8）は、各 vBond オーケストレータとの永続的な接続を維持します。原則として、各 vManage サーバは約 2000 台のデバイスをサポートし、単一クラスタで最大 6 台のサーバがテストされています。十分な冗長性を確保するため、バックアップ vManage または vManage クラスタが追加されていることを確認します。vManage がサポートできるデバイスの数は、生成される統計情報やフローの数など、さまざまな要因によって大きく異なる可能性があるため、ネットワークの需要に応じて vManage インスタンスを追加する必要がある場合があります。

図 51.　　コントローラの高可用性と拡張性



次の表に、WAN エッジルータデバイスの数に対し最低限必要なコントローラの数に関する一般的なガイドラインを示しますが、すべての状況に適用されるわけではありません。ほとんどのネットワークでは、コントローラごとに 2000 台のデバイスが適切な経験則であることが表に示されていますが、ネットワークのパフォーマンス要求によっては、追加のコントローラが必要になる場合があります。

vBond および vSmart の場合は、冗長性のために 1 ～ 2 台のデバイスを追加する必要があります。デバイスの数と場所は、コントローラの全体的な設計によって異なります。vManage の場合、通常は単一の vManage で最大 2000 台のデバイスをサポートできますが、それ以上のデバイスではクラスタが必要です。クラスタの場合のテーブル内の数値は、1 つの vManage がクラスタ内で失敗しても、クラスタ内で必要な数の WAN エッジルータをサポートできるように、vManage を追加します。WAN エッジデバイスは、vSmart コントローラおよび vManage への永続的な接続を試みる前に、一時的な接続にのみ vBond を使用するため、vBond がオーバーサブスクライブされる可能性があることに注意してください。

表 7. WAN エッジデバイスをサポートするために必要なコントローラの数

WAN エッジの数	vBond の数	vSmart の数	vManage の数（アクティブ）
2000 以下	1	1	1
4000 以下	2	2	3
6000 以下	3	3	4*
8000 以下	4	4	5
<=10000	5	5	6

* 偶数の vManage インスタンスがあるクラスタでは、少なくとも 1 つの vManage インスタンスの設定および統計情報サービスをオフにしてください。これらのサービスには書き込み操作にクォーラム（過半数）が必要です。設定および統計情報サービスは、単一クラスタ内の 3 つ以上の vManage インスタンスで実行する必要があります。

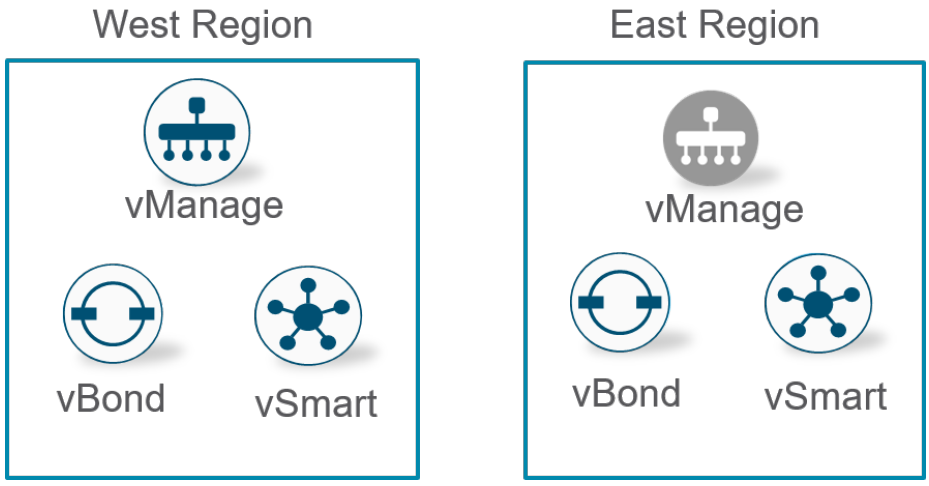
技術的なヒント
コントローラの導入設計では、特に 4 つ以上の vManage インスタンスのクラスタリングが必要な場合は、導入前に設計を検証するためにシスコセールスに連絡することをお勧めします。vManage でサポートされる実際のデバイス数は、統計情報と DPI の要件によって異なるため、この場合は設計の検証も役立ちます。

コントローラの導入例

コントローラは、いくつかの異なる方法で導入できます。次に、一定数の WAN エッジデバイスに対する地域およびグローバルコントローラの導入例をいくつか示します。設計の計画時に、単一のデバイス障害が発生した場合や、到達できない地域にデータセンター全体が存在する場合に、残りのコントローラがネットワークの残りの部分を処理できる必要があることを確認します。1 つの vSmart は、最大 5400 の接続と 2700 の OMP セッションをサポートできます。vSmart アフィニティを使用して設計する場合は、グループが処理できる接続の数に注意してください。また、障害が発生したときに WAN エッジルータにサービスを提供することを設計で想定している場合は、別のアフィニティグループに障害が発生した場合に、必要な数の接続を処理できる容量があることを確認してください。また、WAN エッジルータは、障害シナリオでトラフィック/ルーティングの中断を防ぐために 1 つの vSmart 接続のみが必要で、vBond ルータは、新しい導入、デバイスのリロード、インターフェイスのリセットなどによってネットワークに参加または再参加するときに WAN エッジルータでのみ必要であることに注意してください。

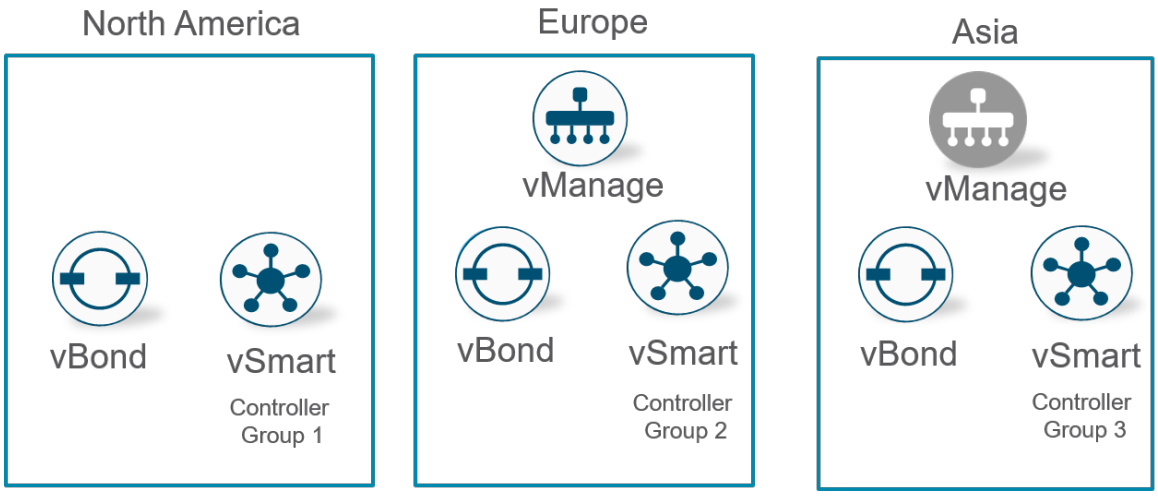
1. 最小限のコントローラ設計（2000 台以下のデバイス）。次に、デバイスが 2000 台以下のネットワークの例を示します。
    - この地域の例では、この設計には 1 つのアクティブ vManage と 1 つのスタンバイ vManage、2 つの vBond オーケストレータ、および 2 つの異なる地域に分割された 2 つの vSmart コントローラが含まれています。

図 52.　　地域コントローラの導入例



- この例では、コントローラは世界中のさまざまな地理的地域に集中しています。この設計には、3 つの vBond、3 つの vSmart、および 1 つのアクティブ vManage と 1 つのスタンバイ vManage が含まれます。vSmart アフィニティは、WAN エッジデバイスが地理的に最も近い 2 つのエリア（北米とヨーロッパ、またはヨーロッパとアジアなど）の vSmart に接続するために使用されます。

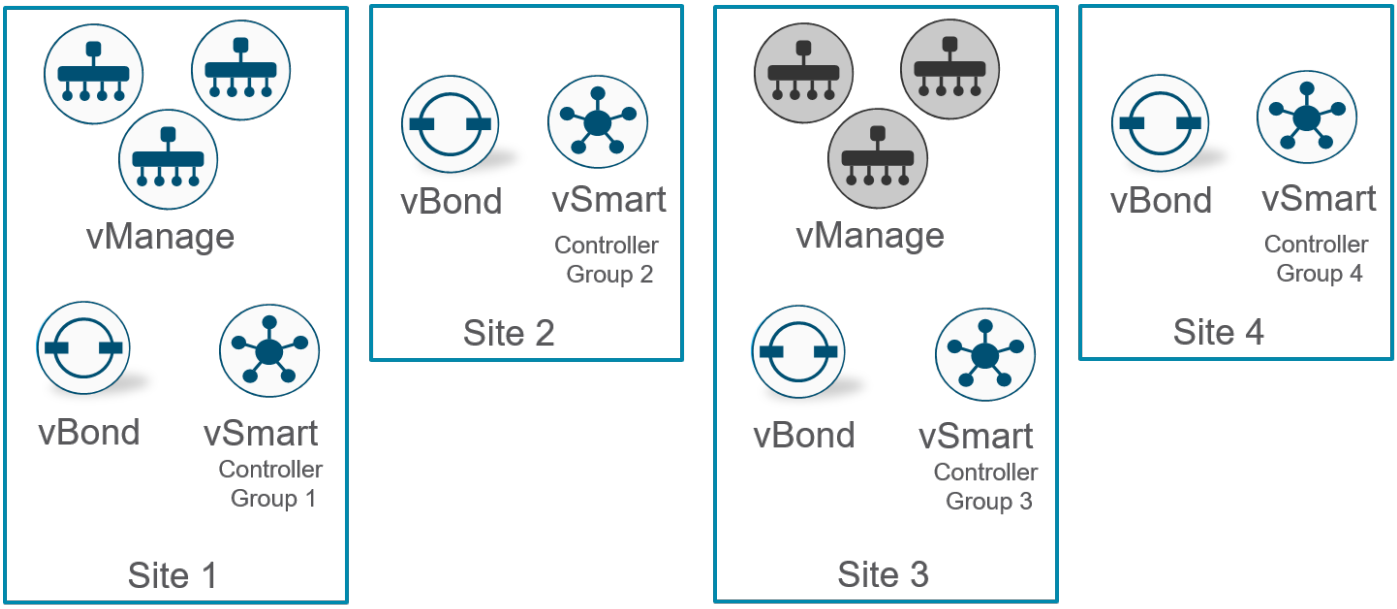
図 53.　　グローバルコントローラの導入例



2. 小規模なコントローラ設計（4000 台以下のデバイス）。設計にはさまざまな方法がありますが、4000 台のデバイスをサポートするコントローラの導入例を次に示します。

   この例では、1 つのアクティブ vManage クラスタと 1 つのスタンバイ vManage クラスタが含まれ、それぞれに 3 つの vManage インスタンスがあります。クラスタ内の 1 つの vManage を無効にできますが、残りのクラスタが WAN エッジデバイスをサポートできます。また、地域内またはグローバルで複数のサイトに分割された 4 つの vBond オーケストレータ、4 つの vSmart コントローラも含まれます。vSmart アフィニティを使用して、WAN エッジデバイスが地理的に近い 2 つのエリアの vSmart コントローラに接続できるようにします。

図 54.　　小規模コントローラの導入例



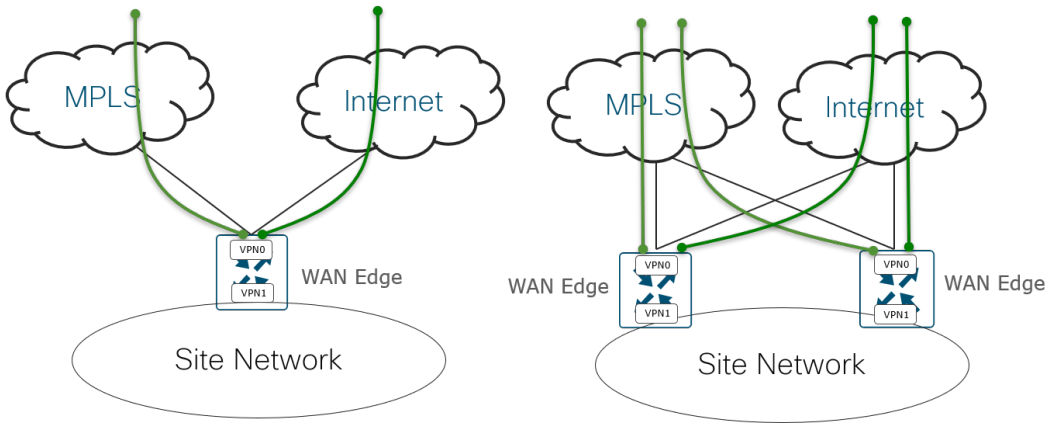
WAN エッジ導入

WAN エッジルータは、リモートサイト、キャンパス、およびデータセンターに導入され、SD-WAN オーバーレイネットワークを介してサイトとの間でデータトラフィックをルーティングします。

サイトに WAN エッジルータを導入する場合は、トラフィックスループットとサポートされるトンネル数などに応じてプラットフォームを選択し、適切なサイズにする必要があります。冗長性を確保するために、2 番目の WAN エッジルータを追加することをお勧めします。導入時には、適切な冗長性を確保するために、WAN エッジルータは通常、すべてのトランスポートに接続されます。

次の図は、単一のルータサイトとデュアルルータサイトを示しており、各 WAN エッジルータは両方のトランスポートに接続しています。

図 55.　　単一およびデュアル WAN エッジルータサイト



IPsec カプセル化トンネルは、他の WAN エッジルータのロケーションへのデータトラフィックを暗号化し、BFD セッションもこれらのトンネル上で形成されます。サービス VPN から発信されるユーザトラフィックは、トンネルに転送されます。トランスポートまたはトランスポートへのリンクがダウンし、WAN エッジルータがその状態を検出すると、BFD がタイムアウトし、両側のトンネルがダウンします。残りのトランスポートまたはトランスポートリンクは、トラフィックに使用できます。デュアルルータサイトでは、ルータの 1 つに障害が発生すると、両方のトランスポートへの接続が残っている残りのルータがサイトのルーティングを引き継ぎます。

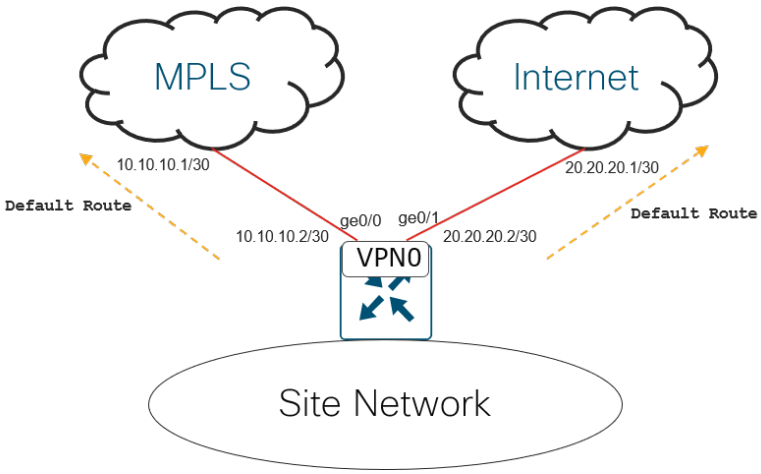
トランスポート側

アンダーレイ

アンダーレイには、トランスポート VPN（VPN 0）と各トランスポートへの接続が含まれます。簡単にするために、ダイナミックルーティングではなく、可能な限り VPN 0 でスタティックルーティングを使用することを推奨しますが、ループバックまたは TLOC Extension インターフェイスをアドバタイズするには、VPN 0 でのダイナミックルーティングが必要になる場合があります。また、レガシーネットワークに接続するためにアンダーレイルーティングを実行する必要がある特定のサイトでも必要になることがあります。いずれにしても、アンダーレイネットワークとオーバーレイネットワークを可能な限り混在させないように注意する必要があります。

通常、VPN 0 でのルーティングに必要なのは、各トランスポートのネクストホップ IP アドレスを指定するデフォルトルートだけです。その目的は、他の WAN エッジルータへの IPsec カプセル化データトンネルを構築し、SD-WAN コントローラへのコントロールプレーン DTLS/TLS トンネルを構築することです。VPN 0 内に複数のデフォルトルートが存在する可能性があります。これは、選択されるルートがトンネルの送信元 IP アドレスに依存するためです。トンネルの送信元 IP アドレスは、デフォルトルートのネクストホップ IP アドレスと同じサブネット内にある必要があります。

図 56.　　アンダーレイルーティング



接続の選択

アンダーレイを確立するために必要なのは、WAN エッジルータからトランスポート サービス プロバイダーへの IP 接続だけです。トランスポート サービス プロバイダーは、トンネルサブネットルート情報をリモート SD-WAN サイトに伝播します。トランスポートへの接続は複数の方法で行うことができますが、可能な限りトランスポートの近くに配置することをお勧めします。

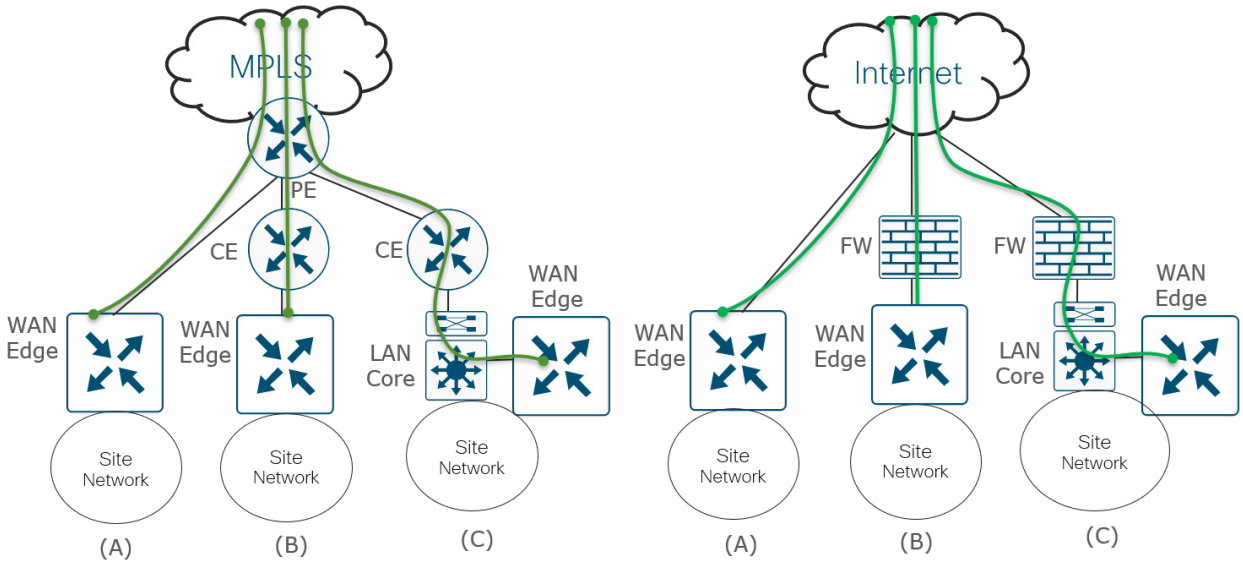
一般的な接続の選択肢は次のとおりです。

- (A) MPLS では、WAN エッジルータはカスタマーエッジ（CE）ルータを完全に置き換えることができるため、WAN エッジルータから MPLS トランスポートのプロバイダーエッジ（PE）ルータに直接接続できます。インターネット トランスポートの場合、WAN エッジルータはファイアウォールなしでインターネット トランスポートに直接接続されます。この接続タイプは、ブランチサイトでよく見られます。
- (B) MPLS では、MPLS トランスポートに接続する CE ルータの背後に WAN エッジルータを配置できます。これは、次のような理由で CE ルータを所定の場所に保持する必要がある場合に使用されます。
  - CE ルータは、SRST/音声や DLSW など、SD-WAN ルータでサポートされていない機能を有効にしてネットワーク接続またはネットワークサービスを提供します。
  - CE ルータは、SD-WAN の導入時に移行されない SD-WAN サイトに直接アクセスします。
  - 中断を最小限に抑えてサイトに SD-WAN を導入するために、CE ルータはそのままにしておく必要があります。

インターネット トランスポートの場合、企業のセキュリティポリシーで要求されている場合は、WAN エッジルータをファイアウォールの背後に配置できます。この接続タイプは、データセンターサイトでよく見られます。

- (C) MPLS およびインターネット トランスポートの両方で、CE またはファイアウォールが必要であるが、SD-WAN ルータの CE またはファイアウォールに直接接続できない場合、WAN エッジルータをトランスポート接続の LAN スイッチに直接接続できます。

図 57.　　MPLS およびインターネット WAN エッジ接続



SD-WAN ルータおよびファイアウォール

SD-WAN ルータは、ファイアウォールの背後に配置する必要はありませんが、セキュリティポリシーで規定されている場合は可能です。通常、ブランチの WAN ルータはトランスポートに直接接続し、別のファイアウォール アプライアンスの背後には配置しません。WAN エッジルータのトランスポート物理インターフェイスにトンネルが設定されている場合、WAN エッジルータの物理インターフェイスはデフォルトで限られた数のプロトコルのみに制限されます。デフォルトでは、DTLS/TLS および IPsec パケットに加えて、DHCP、DNS、ICMP、および HTTPS ネイティブパケットがインターフェイスに許可されます。アンダーレイルーティングの SSH、NTP、STUN、NETCONF、OSPF および BGP ネイティブパケットはデフォルトでオフになっています。不要なものはすべて無効にし、インターフェイスで許可するネイティブプロトコルを最小限に抑えることを推奨します。さらに、WAN エッジルータは、WAN エッジの許可シリアル番号リストに含まれ、許可されているデバイスによってのみ、証明書認証によって SD-WAN オーバーレイに許可された他の WAN エッジルータとだけ、IPsec 接続を形成できます。

ファイアウォールが WAN エッジルータの前に配置されている場合、ファイアウォールは WAN エッジルータデータプレーン接続の AES 256 ビット暗号化 IPsec パケットと、WAN エッジコントロールプレーン接続の DTLS/TLS 暗号化パケットを認識するため、ほとんどのトラフィックをファイアウォールで検査できません。ただし、ファイアウォールを使用する場合は、ファイアウォールの必要なポートを開くことで、SD-WAN ルータの IPsec および DTLS/TLS 接続に対応する必要があります。NAT を適用する必要がある場合は、特にデータセンターサイトで 1 対 1 の NAT を使用することを推奨します。他の NAT タイプはブランチで使用できますが、対称 NAT は他のサイトとのデータプレーン接続の問題を引き起こす可能性があるため、導入する際には注意が必要です。

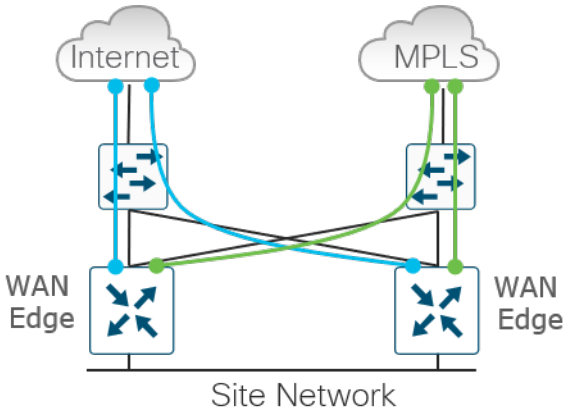
直接インターネットトラフィックおよび PCI コンプライアンスの使用例では、IOS XE SD-WAN ルータは、アプリケーション ファイアウォール、IPS/IDS、マルウェア保護、および URL フィルタリングを含む独自のネイティブの完全なセキュリティスタックをサポートします。このセキュリティスタックのサポートにより、追加のセキュリティハードウェアをリモートサイトに導入してサポートする必要がなくなります。vEdge ルータは、独自のゾーンベースファイアウォールをサポートします。どちらのルータタイプも、クラウドベースのセキュリティのためのセキュア インターネット ゲートウェイ（SIG）として Cisco Umbrella と統合できます。IOS XE SD-WAN セキュリティ機能の詳細については、『Cisco SD-WAN Security Design guide』（近日提供予定）を参照してください。

TLOC Extension

WAN エッジルータを各トランスポートに直接接続できず、1 つのトランスポートに接続できる WAN エッジルータが 1 つだけである場合があります。

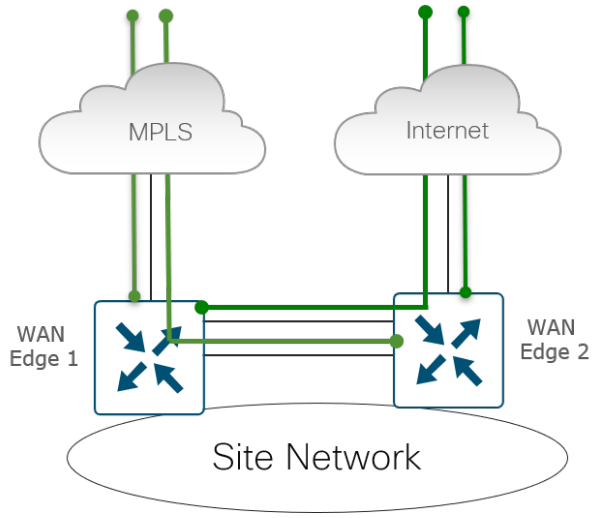
または、スイッチを各トランスポートに接続し、SD-WAN ルータを接続されたスイッチを介して各トランスポートに接続することもできます。これは、ソリューションのコストが増加し、別のデバイスの管理が必要になるため、通常はブランチでは推奨されません。

図 58.　　すべてのトランスポートオプションに接続するための L2 スイッチフロントエンド



TLOC Extension により、各 WAN エッジルータは、隣接する WAN エッジルータ上の TLOC Extension インターフェイスを介して反対のトランスポートにアクセスできます。次の図では、WAN エッジ 1 が MPLS トランスポートに直接接続し、WAN エッジ 2 の TLOC Extension インターフェイスを使用して INET トランスポートに接続しています。次に、WAN エッジ 2 は INET トランスポートに直接接続し、WAN エッジ 1 の TLOC Extension インターフェイスを使用して MPLS トランスポートに接続します。TLOC Extension インターフェイスからトランスポートへの接続は透過的です。図の WAN エッジ 1 ルータには、トンネルが設定された 2 つの物理インターフェイス（MPLS へのトンネルとインターネットへのトンネル）があり、インターネットへのトンネルが別の SD-WAN ルータを通過することを認識していません。

図 59.　　TLOC Extension

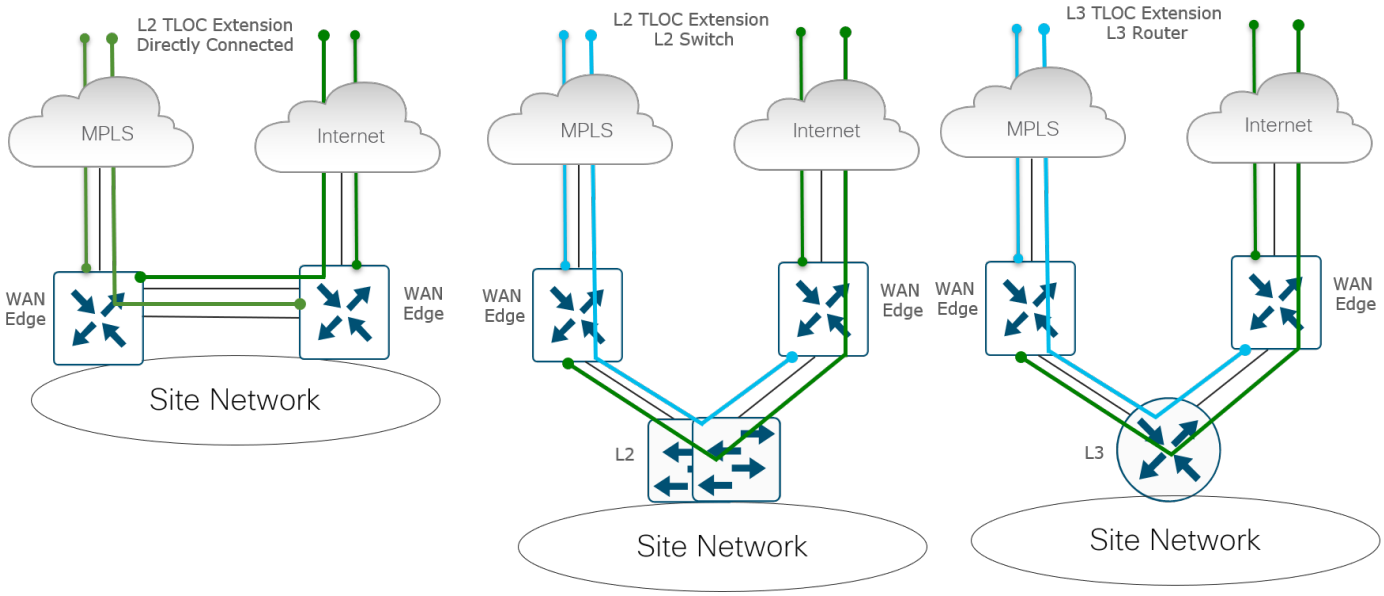


TLOC Extension タイプ

SD-WAN ルータの TLOC Extension は、複数の方法で接続できます。SD-WAN ルータは、直接接続することも、L2 スイッチを介して接続することも、L3 スイッチ/ルータを介して接続することもできます。L2 TLOC Extension は、相互に L2 隣接する 2 つのルータ間の TLOC Extension を表し、リンクは同じサブネット内にあります。L3 TLOC Extension は、リンクが異なるサブネットにある L3 スイッチまたはルータによって分離された 2 つのルータ間の TLOC Extension を記述します。L3 TLOC Extension は、GRE トンネルを使用して実装されます。TLOC Extension は、個別の物理インターフェイスまたはサブインターフェイスにすることができます（帯域幅が許容される場合）。

次に、異なる L2 および L3 TLOC Extension の導入を示します。

図 60.　　L2 と L3 TLOC Extension の導入



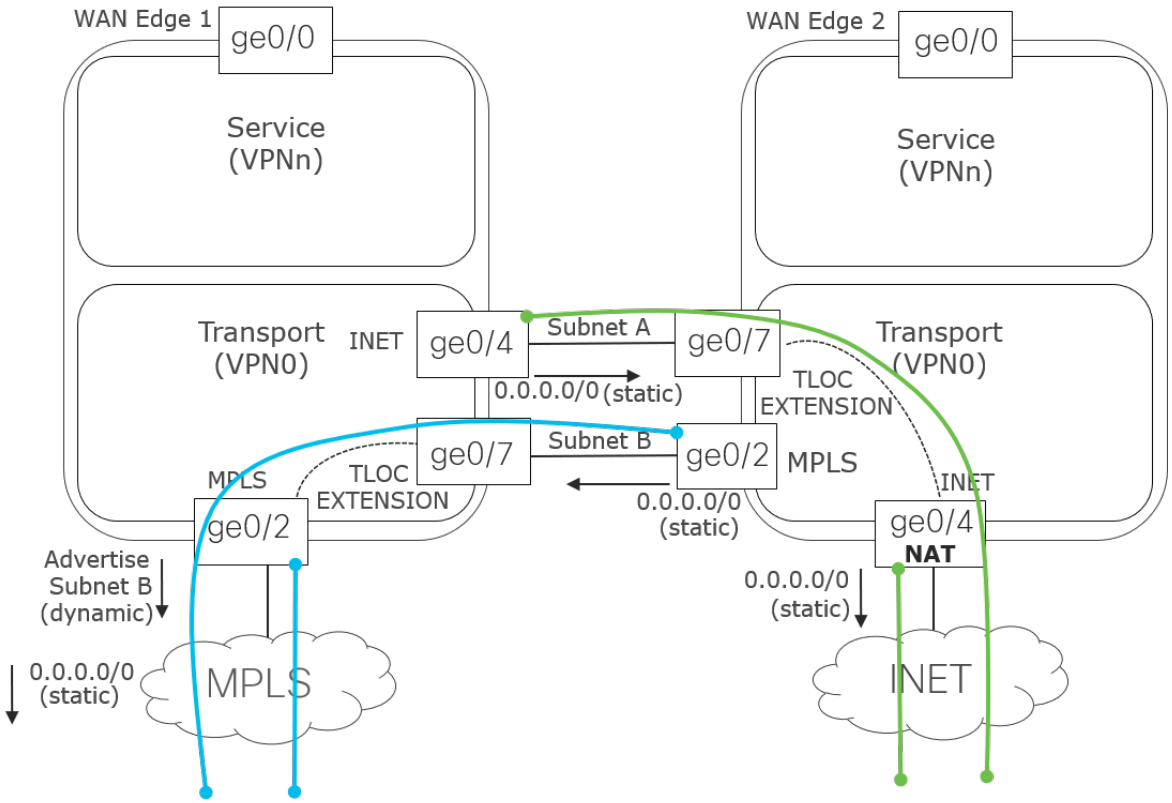
TLOC Extension の使用にはいくつかの制限があります。

- TLOC および TLOC Extension インターフェイスは、L3 ルーテッドインターフェイスでのみサポートされます。L2 スイッチポート/SVI は WAN/トンネルインターフェイスとして使用できず、サービス側でのみ使用できます。LTE は、WAN エッジルータ間の TLOC Extension インターフェイスとしても使用できません。
- L3 TLOC Extension は、IOS XE SD-WAN ルータでのみサポートされます。vEdge ルータではサポートされません。
- TLOC Extension は、ループバック トンネル インターフェイスにバインドされたトランスポート インターフェイスでは機能しません。

TLOC Extension ルーティング

TLOC Extension インターフェイスを設定する場合は、VPN 0 で設定し、IP アドレスを割り当て、バインド先の WAN インターフェイスを指定します。次の図では、WAN エッジ 1 の TLOC Extension インターフェイスは ge0/7 で、ge0/2 を介して MPLS トランスポートにバインドされています。WAN エッジ 2 の TLOC Extension は ge0/7 で、ge0/4 を介して INET トランスポートにバインドされています。

図 61.　　TLOC Extension



コントローラの到達可能性が発生し、IPsec トンネルおよび BFD セッションが TLOC Extension インターフェイスを介して他のサイトと起動するためには、ルーティングに関するいくつかの考慮事項が必要です。スタティック デフォルト ルートは、各 WAN エッジルータのアンダーレイ（トランスポート VPN 0）で設定し、ネクストホップとしてサービスプロバイダールータを指定する必要があります。

INET トランスポートに到達するには、WAN エッジ 1 の INET インターフェイス（ge0/4）に、WAN エッジ 2 の ge0/7 IP アドレスを指すデフォルトルートを設定する必要があります。サブネット A がプライベートアドレス空間にある場合は、WAN エッジ 2 の ge0/4 トランスポート インターフェイス上で NAT を設定して、TLOC Extension を介してインターネットから WAN エッジ 1 にトラフィックをルーティングできるようにします。

MPLS トランスポートに到達するには、WAN エッジ 2 の MPLS インターフェイスに、WAN エッジ 1 の ge0/7 IP アドレスを指すデフォルトルートを設定する必要があります。トラフィックを TLOC Extension インターフェイスにルーティングできるようにするには、ルーティングプロトコル（通常は BGP または OSPF）を WAN エッジ 1 のトランスポート VPN（VPN 0）で実行し、MPLS プロバイダーが WAN エッジ 1 を介してサブネット B へのルートを持つようにサブネット B をアドバタイズします。通常、スタティック デフォルト ルートはコントロールプレーンと IPsec トンネルの確立のためにトランスポート VPN で使用されるため、ルートマップはインバウンドにも適用され、サービスプロバイダーからのすべての着信ダイナミックルートが拒否されます。ルーティングプロトコルの代わりに、MPLS PE ルータは WAN エッジ 1 を介してサブネット B へのスタティックルートを実装できます。これは、サービス プロバイダー ネットワークを通じて再配布できます。スタティックルートは、多数のサイトがある場合にダイナミック ルーティング プロトコルを使用する場合ほど管理や拡張ができないため、推奨されません。

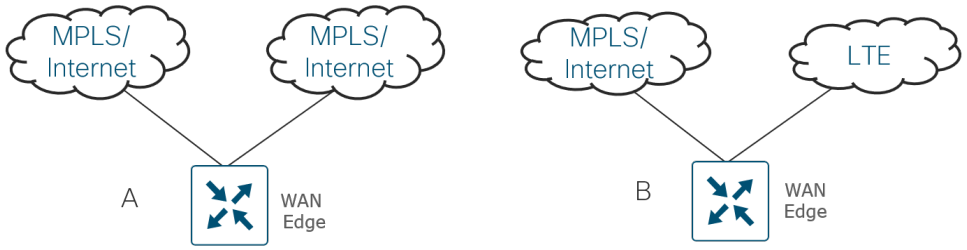
トランスポートの選択肢

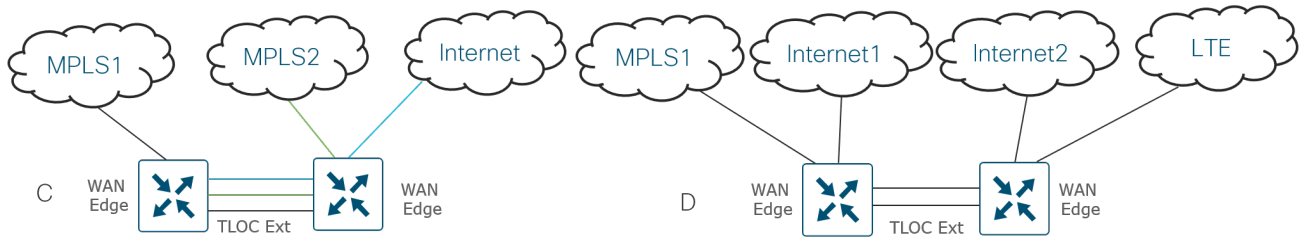
使用できるトランスポートには、さまざまな選択肢と組み合わせがあります。トランスポートはアクティブ/アクティブ状態で導入され、その使用方法は非常に柔軟です。非常に一般的なトランスポートの組み合わせは、MPLS とインターネットです。MPLS はビジネスクリティカルなトラフィックに使用でき、インターネットはバルクトラフィックやその他のデータに使用できます。一方のトランスポートがダウンすると、もう一方のトランスポートを使用して、サイトとの間でトラフィックをルーティングできます。インターネットはほとんどの場所で信頼性が高く、ほとんどのアプリケーションの SLA を満たすことができるため、多くの場合、サイトは代わりに 2 つのインターネット トランスポートを導入します。

LTE はトランスポートの選択肢として頻繁に使用され、アクティブモードで導入でき、または他のすべてのトランスポートが使用できなくなるまでアクティブにならない、最後の手段の回線として導入できます。

次に、さまざまなトランスポートオプションの簡単な例を示します。図 C は個別の物理インターフェイスの TLOC Extension を示し、図 D は 2 つの物理インターフェイスでサブインターフェイスを使用する複数の TLOC Extension を示します。

図 62.　　複数の SD-WAN トランスポートの選択肢



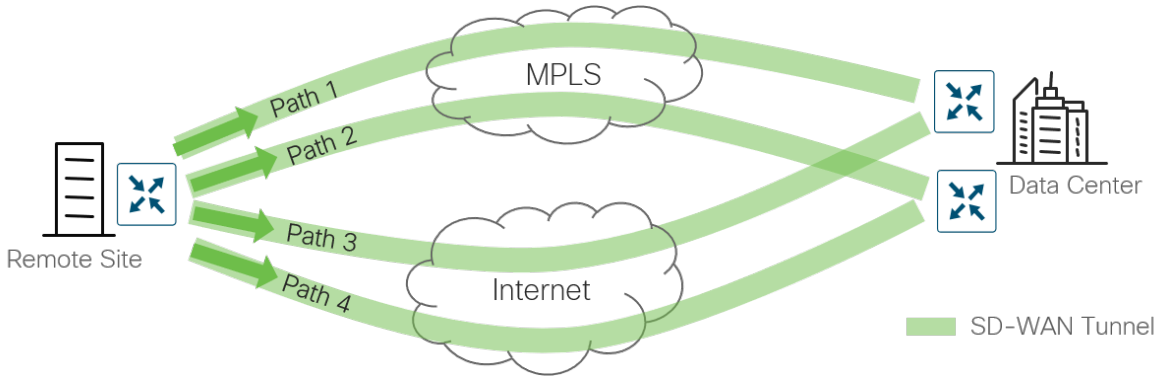


技術的なヒント
同時転送の数には制限があることに注意してください。1 つの WAN エッジルータでは、最大 8 つのトンネルインターフェイスを設定できます。これは 8 つの TLOC に相当します。

トンネルの等コストマルチパス（ECMP）

2 つの SD-WAN サイト間では、デフォルトで 1 つの SD-WAN ルータから各トランスポートを経由してリモートサイトの各 SD-WAN ルータにトンネルが構築されます。これにより、同じサイトへの複数の等コストマルチパストンネルが発生する可能性があり、トラフィックは、IP ヘッダーのキーフィールドのハッシュを使用してどのパスを取るかを決定して、これらのパスのいずれかを通過して宛先に到達します。

図 63.　　等コストマルチパストンネル



vEdge ルータのデフォルトでは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、および DSCP 値の組み合わせがハッシュキーとして使用され、選択する等コストパスが決定されます。[Enhance ECMP Keying] オプションを vManage GUI（または CLI の **ecmp-hash-key layer4**）から選択して、ハッシュキーの計算に L4 送信元および宛先ポート情報を含めることができます。トンネル間のトラフィック分散に影響を与えるために、サービス VPN で設定変更が行われます。アンダーレイルーティングとダイレクト インターネット アクセスのトラフィック分散に影響を与えるために、トランスポート VPN（VPN 0）で設定変更が行われます。

IOS XE SD-WAN ルータの場合、パスを選択するためのハッシュは、送信元と宛先の IP アドレス、および送信元と宛先のポート番号に基づいて行われます。他にオプションはありません。

TLOC プリファレンス

デフォルトでは、WAN エッジルータ上のすべての TLOC には、値 0 の同じプリファレンスが割り当てられます。すべての TLOC は OMP にアドバタイズされ、ルータは ECMP を使用してトンネル間でトラフィックを分散します。トンネルには、0 ～ 4294967295（2^32 – 1）の任意の値のプリファレンスを割り当てることができます。トラフィックはアウトバウンド方向とインバウンド方向の両方で影響を受け、リモート TLOC のプリファレンス値にも依存します。

重量

weight パラメータを使用すると、重み付けされたトンネルを介してトラフィックを送信できます。この値が大きいほど、別のトンネルよりも多くのトラフィックがトンネルに送信されます。重みは、TLOC の帯域幅が異なり、リンク上で ECMP を実行できない場合によく使用されます。重みは 1 ～ 255 の範囲で設定でき、デフォルト値は 1 です。トラフィック分散では、リモート TLOC の重みとローカル TLOC の重みが考慮されます。

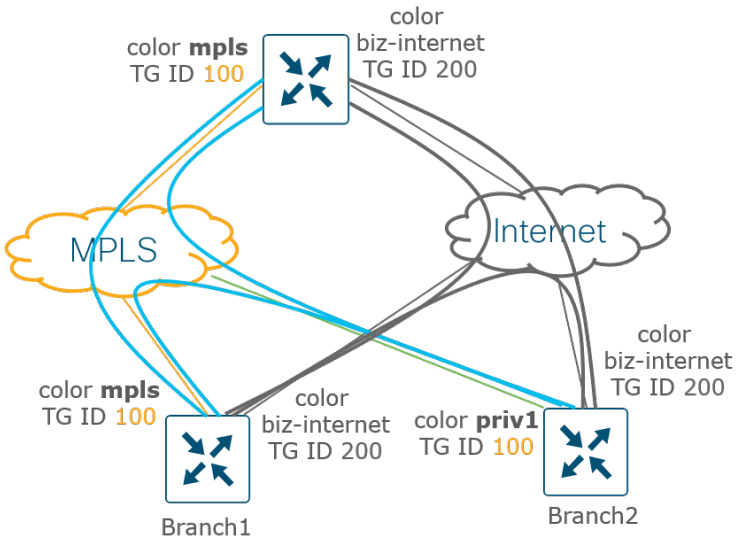
トンネルグループ

デフォルトでは、WAN エッジルータはカラーに関係なく、他のすべての TLOC へのトンネルを構築しようとします。トンネルの下でカラーを指定して restrict オプションを使用すると、トンネルは同じカラーの TLOC へのトンネルの構築のみに制限されます。トンネルグループ機能はこの機能に似ていますが、トンネルグループ ID がトンネルの下で割り当てられると、同じトンネルグループ ID を持つ TLOC のみがカラーに関係なく相互にトンネルを形成できるため、柔軟性が向上します。任意のトンネルグループ ID を持つ TLOC は、トンネルグループ ID が割り当てられていない TLOC を持つトンネルも形成します。restrict オプションは、この機能と組み合わせて使用できます。使用すると、インターフェイスで定義されたトンネルグループ ID と restrict オプションを持つインターフェイスは、同じトンネルグループ ID とカラーを持つ他のインターフェイスとだけトンネルを形成します。

トンネルグループを使用するいくつかの使用例を次に示します。

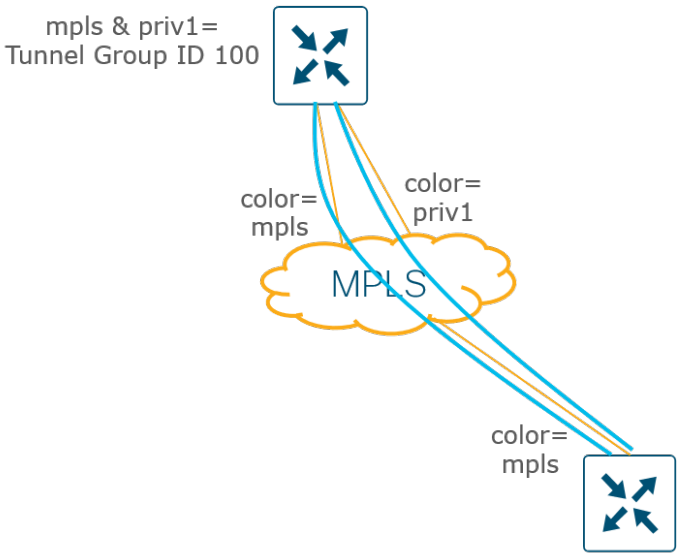
- 次の図は、他の 2 つのブランチとは異なるプライベートカラーを使用するブランチを示しています。トンネルグループを使用すると、すべてのプライベートトランスポートがトンネル接続を確立できますが、パブリックトランスポートには異なるトンネルグループ ID が割り当てられるため、すべてをパブリックトランスポートから分離できます。restrict オプションは有効になっていません。

図 64.　　トンネルグループの使用例：同じトンネルグループ内の複数のプライベートカラー（restrict オプションなし）



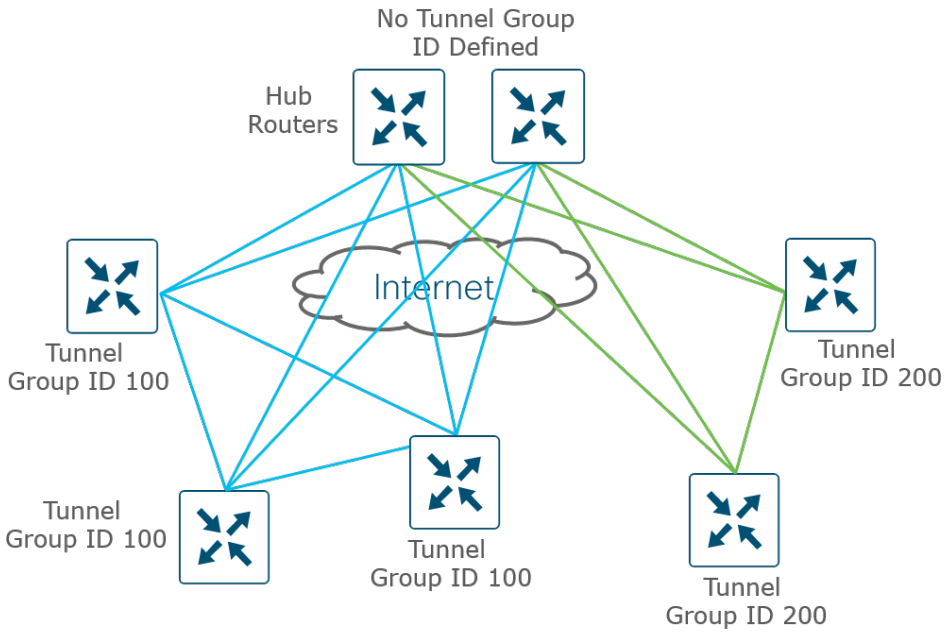
次の使用例では、WAN エッジルータに同じトランスポートへの 2 つの接続があります。WAN エッジルータでは、1 つのカラーを複数のインターフェイスで使用することはできないため、各インターフェイスに異なるカラーを割り当てる必要があります。この場合、トンネルグループを使用して、両方のインターフェイスが同じブランチにトンネルを構築し、WAN エッジルータからのトラフィックが ECMP を使用して両方のインターフェイス間でトラフィックをロードシェアリングできるようにします。

図 65.　　トンネルグループの使用例：同じトランスポートへのトラフィックのスケーリング



トンネルグループは、サイトまたは地域内でメッシュトンネルのグループ化を作成するためにも使用できます。次の例では、2 つの会社が統合され、2 つの集中型ハブルータを介してのみ相互に通信しています。各企業 WAN エッジルータは、同じ企業 WAN エッジルータとフルメッシュで通信します。各 WAN エッジブランチルータは、トンネルグループ ID 100 または 200 に割り当てられます。ハブルータのトンネルインターフェイスにはトンネルグループ ID が定義されていないため、これらの TLOC は他のすべてのトンネルグループ ID とトンネルを形成します（restrict オプションがない場合）。

図 66.　　トンネルグループの使用例：メッシュトンネルのグループ化

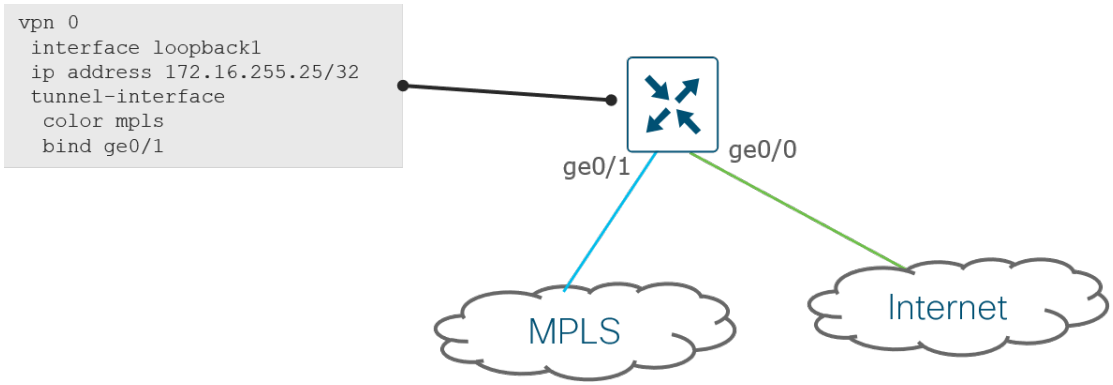


ループバック インターフェイス トンネル

物理インターフェイスをトンネルインターフェイスとして使用できない場合があり、代わりにトンネルインターフェイスを使用してループバック インターフェイスを設定する必要があります。いずれの場合も、WAN エッジルータが他の WAN エッジルータへのデータプレーン接続と SD-WAN コントローラとのコントロールプレーン接続を確立できるように、ループバック インターフェイスに到達できる必要があります。MPLS トランスポートの場合、これは通常、ループバックがダイナミック ルーティング プロトコル（通常は BGP）を介してアドバタイズされることを意味します。インターネット トランスポートでは、通常、NAT が有効になっているため、ループバック インターフェイスの IP アドレスはルーティング可能です。次に、ループバック トンネル インターフェイスの使用例を示します。

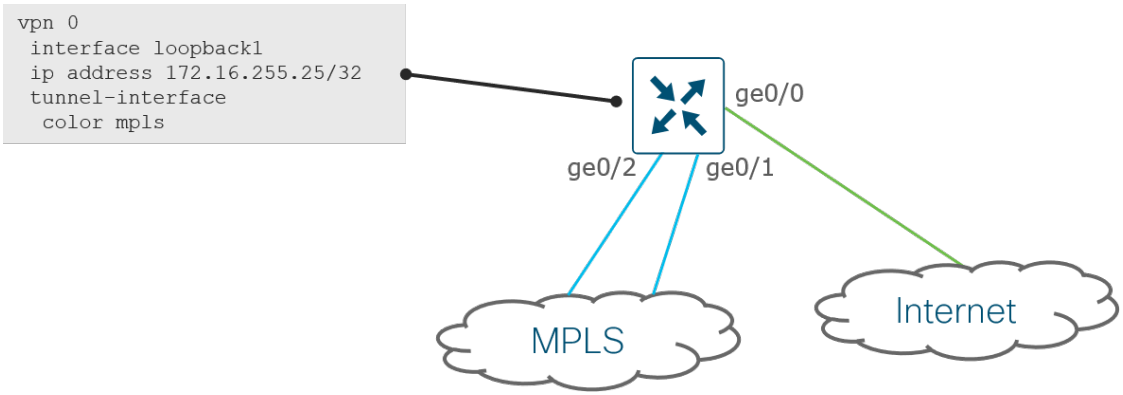
- MPLS サービスプロバイダーの IP アドレス空間がフィルタリングされている場合、またはアドレスがサービスプロバイダーによってアドバタイズされていない場合は、アドレス空間をトンネルエンドポイントとして使用できません。代わりにループバック インターフェイスを使用してトンネルを送信元とし、トンネルを物理インターフェイスにバインドできます。

図 67.　　ループバック インターフェイス トンネルの使用例：トンネルエンドポイントにプロバイダー IP スペースを使用できない



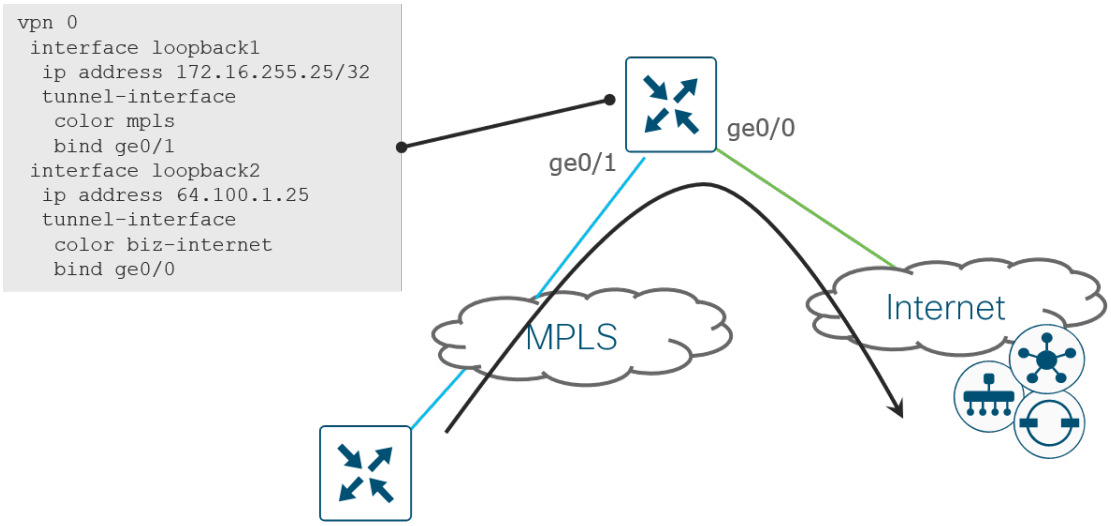
- 同じトランスポートに複数のインターフェイスが接続されている場合（たとえば、帯域幅を増やすため）、特定のカラーを WAN エッジルータの複数のインターフェイスに割り当てることはできないため、各トランスポートで異なるカラーを使用する必要があります。または、トンネルをループバック インターフェイスに設定し、ECMP を使用して物理インターフェイスからトランスポートネットワークにトラフィックをルーティングすることもできます。

図 68.　　ループバック インターフェイス トンネルの使用例：同じトランスポートへのトラフィックのスケーリング



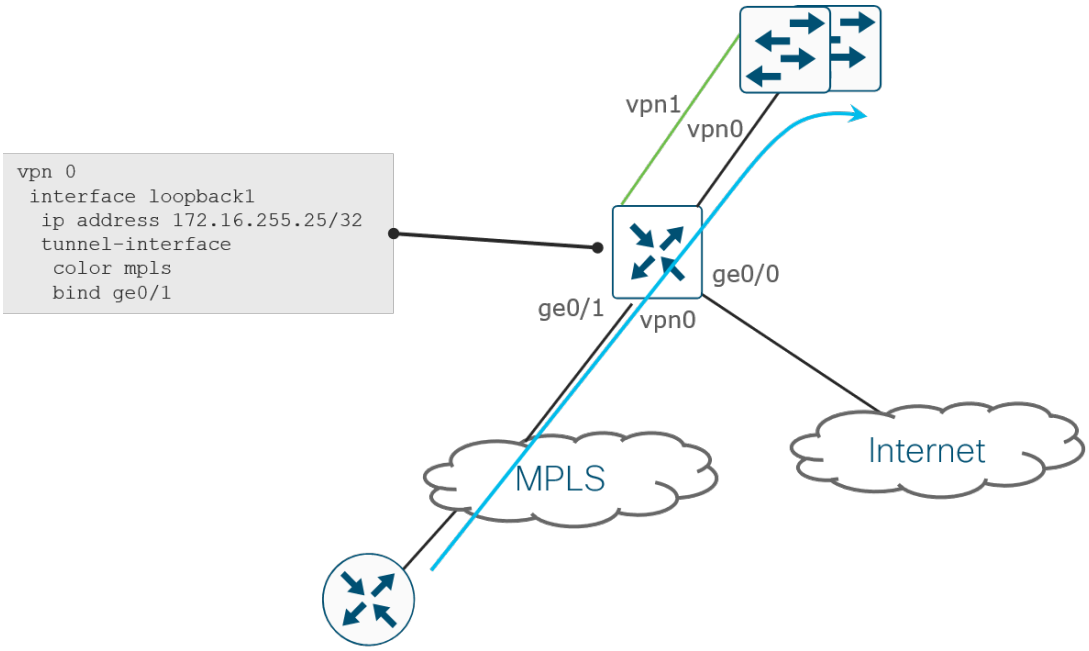
- WAN エッジルータがインラインで導入され、VPN 0 の 1 つのインターフェイスから VPN 0 の別のインターフェイスにトラフィックをルーティングする必要がある場合、これはループバック インターフェイスでトンネル設定を使用する別の使用例です。トンネルインターフェイスを物理インターフェイスから削除する必要があるのは、トンネルがそこで適用されると、強化されたインターフェイスになり、特定のトラフィックの送受信のみを許可し、ルーティングされるトラフィックに応じて接続が切断される可能性があるためです。次に、いくつかの例を示します。
  - インライン DC WAN エッジの導入では、MPLS から着信する制御トラフィックがインターネット上のクラウドベースのコントローラに到達する必要がある場合があります。VPN 0 の MPLS とインターネット間でトラフィックをルーティングできます。この場合、トンネル設定を MPLS およびインターネット物理インターフェイスから削除し、2 つの個別のループバック インターフェイスに配置する必要があります。

図 69.　ループバック インターフェイス トンネルの使用例：MPLS エッジルータはインターネット上のコントローラにアクセスする必要がある



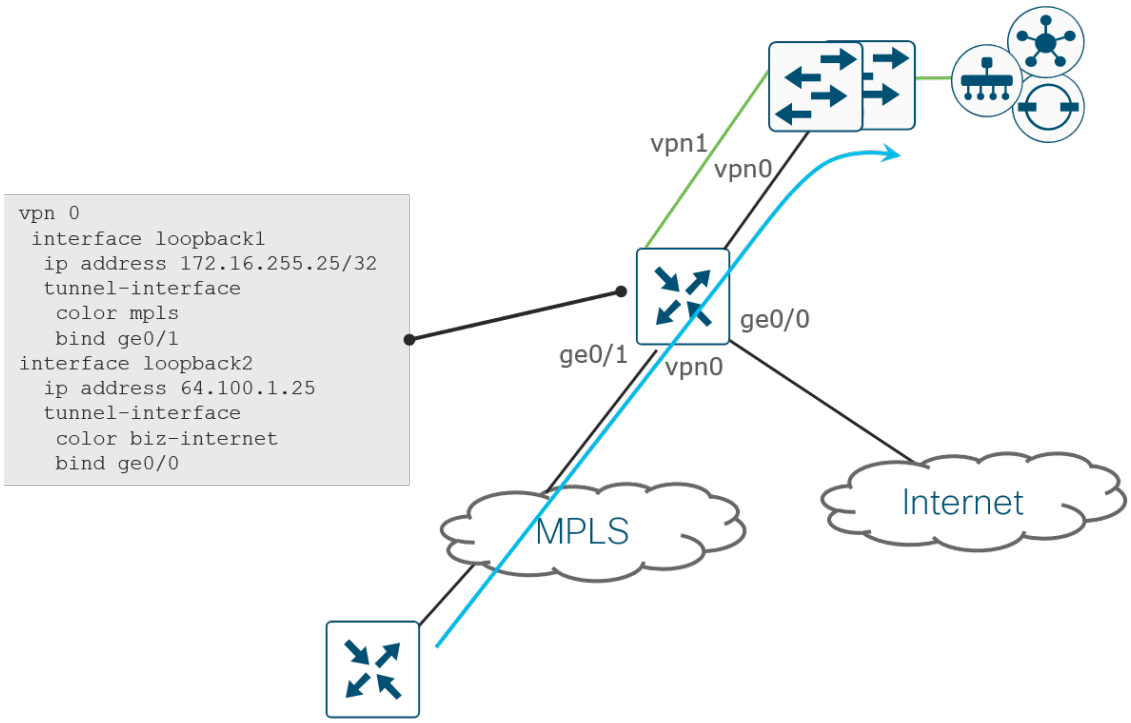
- レガシー MPLS トラフィックは、DC WAN エッジルータを介してサービス VPN にアクセスする必要があります。VPN 0 の追加の物理インターフェイスはサービス側への接続に使用され、トンネルは着信トラフィック用に WAN エッジルータの MPLS 物理インターフェイスから削除され、代わりにループバック インターフェイスに移動されます。

図 70.　ループバック インターフェイス トンネルの使用例：MPLS レガシールータは DC サービス VPN にアクセスする必要がある



SD-WAN デバイスは、DC でのインライン WAN エッジの導入を介してオンプレミスコントローラにアクセスする必要があります。前の使用例と同様に、VPN 0 の追加の物理インターフェイスはサービス側に接続するために使用され、トンネルは WAN エッジルータの両方のトランスポート物理インターフェイスから削除され、代わりにループバック インターフェイスに移動されます。この導入では、DC WAN エッジが制御接続を確立できるように、ループバック インターフェイスとオンプレミスコントローラ間の接続も必要です。

図 71.　　ループバック インターフェイス トンネルの使用例：SD-WAN ルータはオンプレミスコントローラに到達する必要がある



サービス側

トンネルは各トランスポート上に構築されます。ローカルサイトのプレフィックスは、関連する TLOC またはネクストホップとともに、OMP に再配布されます。接続ルートとスタティックルートはデフォルトで再配布されることに注意してください。プレフィックスは、OMP 経由で他のサイトからも受信され、ローカルサイトのルーティングプロトコル（存在する場合）に再配布できます。その後、サービス VPN のユーザトラフィックをオーバーレイトンネルに転送できます。

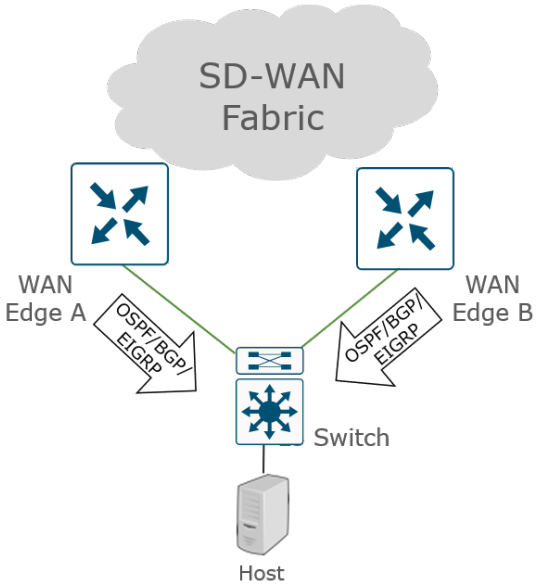
デュアルルータサイトの場合、サービス側 VPN の冗長性は、ルーティング（レイヤ 3）または VRRP（レイヤ 2）で実現できます。

レイヤ 3 の冗長性

ホストから 1 ホップ以上離れているルータの場合、サイトの冗長性のためにルーティングプロトコルを使用できます。WAN エッジルータは、アクティブ/アクティブモードで動作し、WAN エッジルータと LAN スイッチ/ルータ間で OSPF、BGP、または EIGRP（IOS XE SD-WAN ルータ用）を実行します。LAN スイッチからは、リモートサイトのプレフィックスは SD-WAN ファブリックへの等コストパスとして表示されます。ルーティングプロトコルは、トラフィックのプライマリとして 1 つの WAN エッジを優先するように変更できます。サイトからプレフィックスを送信するには、ルーティングプロトコルが OMP に再配布され、サイトにプレフィックスをインポートするには、OMP がルーティングプロトコルに再配布される必要があります。

技術的なヒント
ルートが OMP に再配布される際には、ルートメトリックも OMP 属性として含まれます。OMP メトリックは SD-WAN ファブリック全体のルートプリファレンスに影響しますが、トラフィックフローに影響を与える推奨方法は、TLOC プリファレンスまたは OMP ルートプリファレンスを設定することです。

図 72.　　レイヤ 3 ブランチの冗長性



技術的なヒント
すべてのサービス側ルーティングプロトコルでは、OMP をサービス側ルーティングプロトコルに再配布するときにルートマップを適用してルートを照合し、パラメータを設定し、ルートをフィルタリングできますが、OMP にルートをアドバタイズするときにはルートマップを適用できません。

BGP

ルーティングプロトコルとしての BGP は、CE ルータまたはサービスプロバイダーとピアリングするアンダーレイ、およびローカルサイトのルータとピアリングするサービス側のオーバーレイの両方でサポートされます。デフォルトでは、BGP は OMP に再配布されず、OMP から BGP へのルートも再配布されないため、両方向の再配布を明示的に設定する必要があります。

SD-WAN で特に使用されるループ防止方法がいくつかあります。

- Site of Origin（SoO）拡張コミュニティが使用され、形式は 0:<site ID> です。目的は、OMP が同じサイトから発信されたサイトに BGP ルートを再配布しないようにすることです（そのサイト ID とローカルに設定されたサイト ID を比較することによる）。
- デフォルトでは、BGP が OMP に再配布されるときに AS-Path 情報は含まれません。ループ防止のために AS-Path 情報を含めるには、**propagate-aspath** コマンドを使用します。
- オーバーレイとアンダーレイの両方のルーティングに BGP を使用するネットワークでは、AS 番号を OMP 自体に割り当て、BGP ルーティングアップデートの AS パスに含めることができます。OMP では、このコマンドは **overlay-as** *<AS-number>* です。

BGP ルートが OMP に再配布されると、**propagate-aspath** コマンドが有効になっている場合は、AS パス情報とともに、元のプロトコル（eBGP など）とメトリック（MED）が OMP に再配布されます。OMP で伝送されるメトリックは、サイトのどの WAN エッジルータが SD-WAN ファブリックを介してリモートサイトから優先されるかを左右します。最も低い値のメトリックが優先されます。

サービス側では、as-path、local-preference、metric（MED）、community、および weight が BGP ルートに設定できるパラメータです。

OSPF

ルーティングプロトコル OSPF は、CE ルータまたはサービスプロバイダーとピアリングするアンダーレイ、およびローカルサイトのルータとピアリングするサービス側のオーバーレイの両方でサポートされます。デフォルトでは、エリア間およびエリア内の OSFP ルートだけが OMP にアドバタイズされます。外部 OSPF ルートの OMP への再配布、および OMP ルートの OSPF への再配布は明示的に設定する必要があります。

ループ防止のために、ルートは外部 OSPF ルートとして OMP から OSPF に再配布され、DN ビットが設定されます。これにより、他のルータがルートを再配布できなくなります。OMP から OSPF への再配布されたルートを受信する SD-WAN ルータでは、DN ビットが設定された OSPF ルートが受信され、vEdge ルータでは 251、IOS XE SD-WAN ルータでは 252 のアドミニストレーティブ ディスタンス（AD）が割り当てられます（AD は、OMP ルート上の AD よりも 1 つ多くなります）。OMP が表示されなくなった場合は、再配布されたルートをルーティングテーブルにインストールできます。

プロバイダーエッジ（PE）ルータは、DN ビットが設定された VRF に OSPF ルートをインストールしません。ネットワーク分散/コア内の Cisco ルータまたはスイッチが VRF 用に設定されている場合（セグメンテーションの実装時によく見られます）、デバイスは同様のチェックを使用し、PE ルータと同様に動作します。DN ビットが設定されている場合、VRF に OSPF ルートをインストールしません。この問題を回避するには、受信側ルータの OSPF VRF 設定で **capability vrf-lite** コマンドを設定します。この設定では、ルータは設定された DN ビットを無視し、ルートを OSPF に再配布するときに DN ビットを設定しません。

OSPF ルートが OMP に再配布されると、元のプロトコルとメトリック（コスト）が OMP に再配布されます。OMP で伝送されるメトリックは、サイトのどの WAN エッジルータが SD-WAN ファブリックを介してリモートサイトから優先されるかを左右します。最も低い値のメトリックが優先されます。

コンバージェンスイベントの影響を最小限に抑えるために、可能な限りインターフェイスを OSPF ネットワーク ポイントツーポイントとして設定することをお勧めします。

EIGRP

ルーティングプロトコル Enhanced Interior Gateway Routing Protocol（EIGRP）は、vManage バージョン 19.1 以降の Cisco IOS XE SD-WAN デバイスでのみサポートされ、ローカルサイトのルータとピアリングするサービス側でのみサポートされます。デフォルトでは、EIGRP は OMP に再配布されず、OMP から EIGRP へのルートも再配布されないため、両方向の再配布を明示的に設定する必要があります。

ループを防止するために、OMP ルートが EIGRP に再配布されると、プレフィックスは、トポロジテーブルで「OMP-Agent」を意味する 17 という外部プロトコル ID 属性でタグ付けされます。ルーティング情報ベース（RIB）を更新すると、プレフィックスは「SDWAN-Down」ビットセットでタグ付けされ、アドミニストレーティブ ディスタンスが 252 に設定されます。再配布されたルートのアドミニストレーティブ ディスタンスは OMP よりも高いため、ルートは vSmart コントローラに再配布されません。

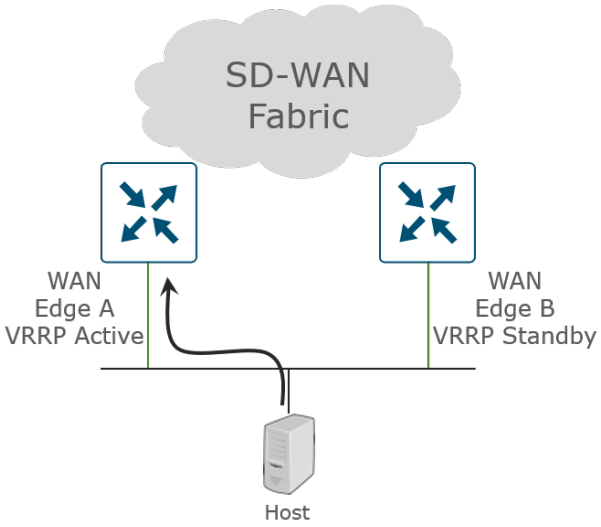
EIGRP ルートが OMP に再配布されると、元のプロトコルとメトリック（帯域幅と遅延の組み合わせ）が OMP に再配布されます。OMP で伝送されるメトリックは、サイトのどの WAN エッジルータが SD-WAN ファブリックを介してリモートサイトから優先されるかを左右します。最も低い値のメトリックが優先されます。

技術的なヒント
19.x vManage バージョンでは、vManage GUI を使用して EIGRP メトリックをインターフェイスに対して調整することはできません。EIGRP メトリックを変更するには、delay パラメータを変更するのがベストプラクティスです。このパラメータは、必要に応じて CLI で調整できます。 また、vManage コードのバージョン 19.x では、EIGRP テンプレートは ISR4461 ルータ用に作成できません。ただし、EIGRP は CLI を使用して設定できます。

レイヤ 2 の冗長性

ホストに隣接するレイヤ 2 のルータの場合、Virtual Router Redundancy Protocol（VRRP）がサイトの冗長性に使用され、ホストのデフォルトゲートウェイとして機能します。1 つのデバイスがアクティブで、もう 1 つのデバイスがスタンバイです。アクティブ VRRP ルータは、仮想 MAC アドレス 00:00:5E：00:01:XX で仮想 IP アドレスの ARP 要求に応答します。XX は VRRP グループ ID を表します。スタンバイ VRRP ルータが引き継ぐと、Gratuitous ARP が送信され、新しいルータの仮想 MAC アドレスでスイッチ MAC テーブルまたはホスト ARP テーブルが更新されます。

図 73.　　L2 ブランチの冗長性



VRRP の場合、プライオリティを 1 ～ 254（100 がデフォルト）に設定でき、プライオリティが最も高いピアがプライマリまたはアクティブな VRRP ピアとして選択されます。プライオリティが同じ場合、LAN IP アドレスが小さい方のルータがプライマリに選択されます。サイトからのトラフィック転送が確定的であるように、アクティブピアを選択して設定することをお勧めします。プリエンプションは自動的に有効になります。つまり、最初に選択または設定されたプライマリが使用できなくなり、その後使用可能になると、アクティブピアとして引き継ぎます。

VRRP プライマリは、デフォルトでアドバタイズメントを毎秒送信します。このタイマーは設定可能です。バックアップ VRRP ルータが 3 つの連続したアドバタイズメントを失うと、プライマリがダウンしていると見なされ、新しいプライマリが選択されます。

WAN が特定の WAN エッジルータに到達不能になった場合、そのルータが VRRP アクティブルータとしての役割を放棄するようにします。これには主に 2 つのオプションがあります。

- OMP での追跡：この場合、vSmart ルータへの OMP セッションがモニタされ、セッションが失われると、新しい VRRP プライマリが選択されます。VRRP プライマリが選択される前に、OMP ホールドタイマーが期限切れになる必要があることに注意してください。デフォルトのホールドタイマーは 60 秒で、調整できます。キープアライブは、この OMP ホールドタイマー値の 1/3 ごとに送信され、3 つが欠落すると、OMP セッションはダウンしていると見なされます。
- プレフィックスリストの追跡：この場合、1 つ以上のプレフィックスがリストで追跡されます。リスト内のすべてのプレフィックスがルーティングテーブルから失われると、OMP ホールドタイマーの期限切れを待たずに VRRP フェールオーバーが発生します。コンバージェンスは OMP でのトラッキングよりも迅速に行われるため、プレフィックスリストでのトラッキングが推奨されます。

技術的なヒント
OMP またはプレフィックスリストを追跡する場合、OMP がダウンしたり、ルーティングテーブルからプレフィックスが消えたりすると、VRRP は非アクティブになります。これが両方の WAN エッジルータで同時に発生すると、デフォルトゲートウェイが両方のルータで非アクティブになります。WAN が失われた場合でも、サイトでローカルスイッチングが必要な場合は、この状態を回避するために、プライマリ VRRP ルータだけにトラッキングを実装できます。

データセンター

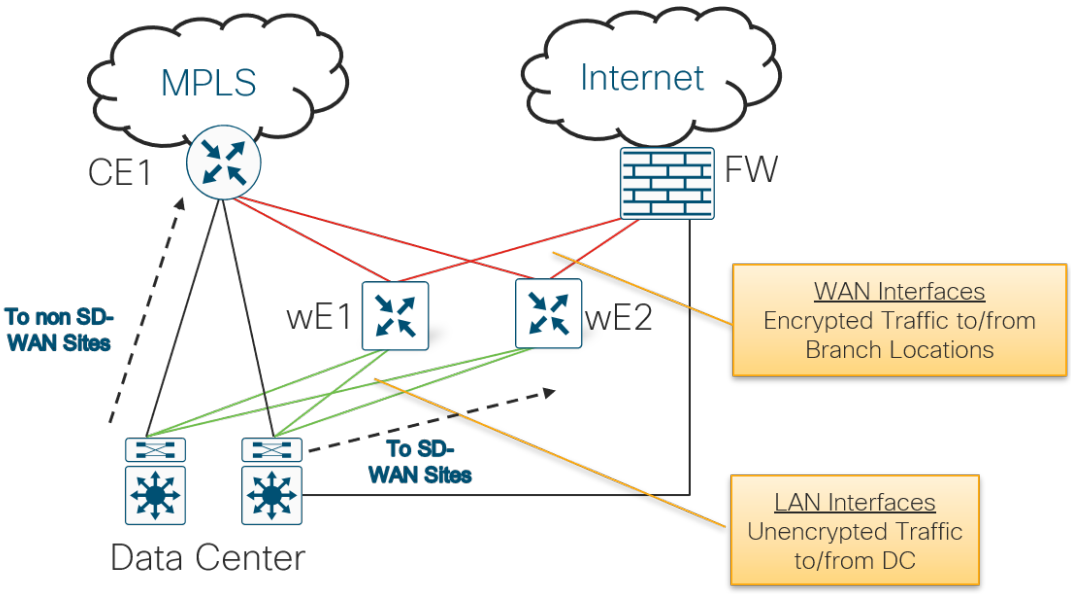
SD-WAN エッジ導入は、データセンターで開始する必要があります。導入時には、非 SD-WAN サイトのデータセンターとの間の通常のトラフィックフローに影響を与えないことが重要です。そのため、SD-WAN 導入の開始時に CE ルータを SD-WAN ルータで即座に置き換えることは一般的ではありません。可能な場合は、移行中に、データセンターを SD-WAN および非 SD-WAN トラフィックの中継として使用することを推奨します。詳細については、『Cisco SD-WAN Migration Guide』を参照してください。

WAN エッジルータをデータセンターサイトにインライン配置しないことを推奨します。導入時にトラフィックを中断したり、WAN エッジルータをすべての SD-WAN および非 SD-WAN トラフィックにとってのボトルネックにしたくない場合、SD-WAN トラフィックには WAN エッジを使用します。非 SD-WAN トラフィックは CE に入り、コアにルーティングできます。可能な場合は、VPN 0 インターフェイスを MPLS の CE ルータおよびインターネットのファイアウォールに接続することをお勧めします。WAN エッジで、可能であれば各 WAN の両方のトランスポートに接続します。TLOC Extension は、データセンターでは一般的に使用されません。リンクまたはデバイスの障害によって、トラフィックに大きな影響を与えたくはありません。

LAN 側で、CE ルータが接続する同じスイッチにインターフェイスを接続します（コアまたは WAN サービスブロック）。すでに存在する場合は、LAN で BGP（iBGP よりも eBGP を優先）を使用することを推奨します。それ以外で、LAN 側にすでに存在する場合は、SD-WAN ルータは OSPF または EIGRP と統合できます（IOS XE SD-WAN ルータの場合）。必ずしもコアを再配布ポイントにする必要はないため、複雑さを軽減するようにしてください。必要に応じて CE ルーティングと統合します。

IPsec トンネルは、異なるサイト ID を持つロケーション間で自動的に構築されることに注意してください。2 つのデータセンター間に DCI がある場合は、DCI を使用してサイト間でトラフィックを転送し、IPsec トンネルをトランスポート間で形成しないようにします（ルーティングループを回避するため）。集中型ポリシーを変更することで、サイト間でトンネルが形成されないようにすることができます。データセンター間の DCI リンクで SD-WAN を実行することは推奨されません。

図 74.　　データセンターの導入



ブランチ

ブランチの設計では、設計をシンプルにすることが重要です。可能な場合は LAN コアと統合し、必要な場合にのみ CE と統合します。音声サービスまたは特定の接続タイプの CE を保持する必要がある場合があります。可能な限り、CE ルータを交換することを推奨します。

ハブ/データセンターサイトでのみアンダーレイおよびオーバーレイルーティングを組み込み、可能な場合はブランチサイトで回避することを推奨します。ブランチサイトでは、サイトを SD-WAN に完全に変換することを推奨します。ブランチにアンダーレイルーティングを組み込むことで、非 SD-WAN サイトとの直接通信が可能になり、複雑さが増し、ルーティングループが発生し、適切に実装されていなければブランチがトラフィックの中継サイトになる可能性があります。音声には、人間の耳で検出できるまでに 300 ミリ秒のトリップ遅延バジェットがあります。これは、ほとんどの場合、移行中に問題にはなりません。

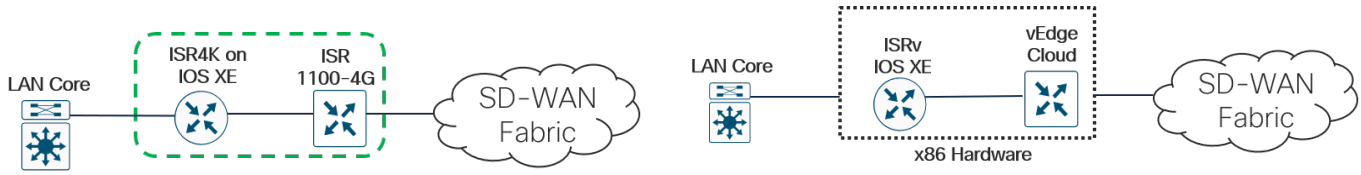
SD-WAN サービスポイントの導入

IOS XE SD-WAN または vEdge ルータを使用した純粋な SD-WAN 導入では、まだ完全にサポートされていない機能や接続が必要なブランチがあります。IOS XE ルータと WAN エッジ SD-WAN ルータを組み合わせて導入することで、その間に必要な機能をカバーできます。

LAN 側の要件

ブランチの LAN 側では、IOS XE ルータ（ISR4k など）でサポートできる WAN エッジルータではサポートされない要件がある場合があります。これには、音声サポート、WAN 最適化、サービスルートトラッキング、セキュリティ、EEM が含まれます。IOS XE コードの ISR 4k ルータは、追加の要件を満たすために SD-WAN ルータの LAN 側に導入できます。IOS XE ルータと WAN エッジルータのこの組み合わせは、ENCS プラットフォームなどの単一の物理デバイスで仮想化することもできます。

図 75.　　ハードウェアおよび仮想化された SD-WAN LAN 側サービスポイントの導入



WAN 側の要件

LAN 側の要件と同様に、IOS XE ルータでサポートできる WAN エッジルータではサポートされないブランチの WAN 側の要件がある場合があります。これには、ATM、フレームリレー、EEM、クラウド SIG への ECMP ルーティングが含まれます。IOS XE コードの ISR 4k ルータは、追加の要件を満たすために SD-WAN ルータの WAN 側に導入できます。

図 76.　　ハードウェア SD-WAN の WAN 側サービスポイントの導入

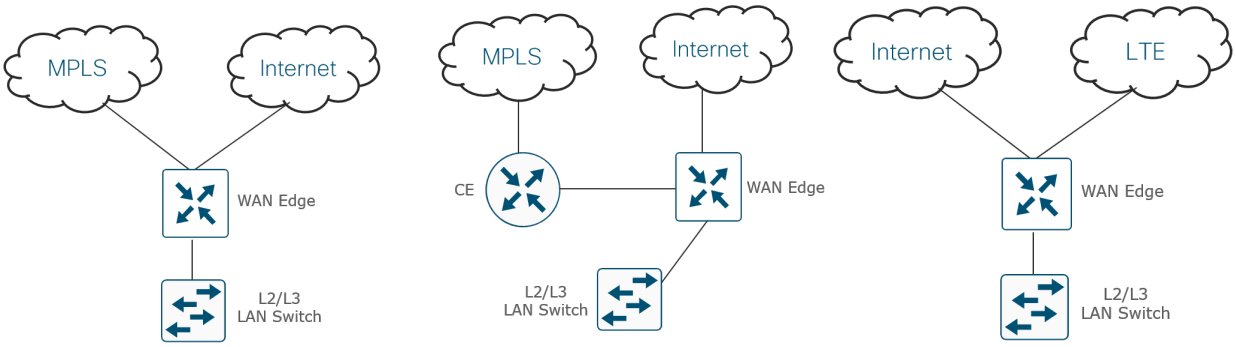
一般的なブランチ導入

次に、一般的なブランチ導入を示します。これは詳細なリストではありません。

単一の WAN エッジ

次の導入は、ブランチサイトに導入された単一の WAN エッジルータを示しています。すべてが少なくとも 2 つのトランスポートに接続され、中央の導入は MPLS トランスポートに到達するために CE ルータを介して接続されます。スイッチは、レイヤ 2 またはレイヤ 3 スイッチとして設定できます。

図 77.　　単一の WAN エッジブランチの導入例

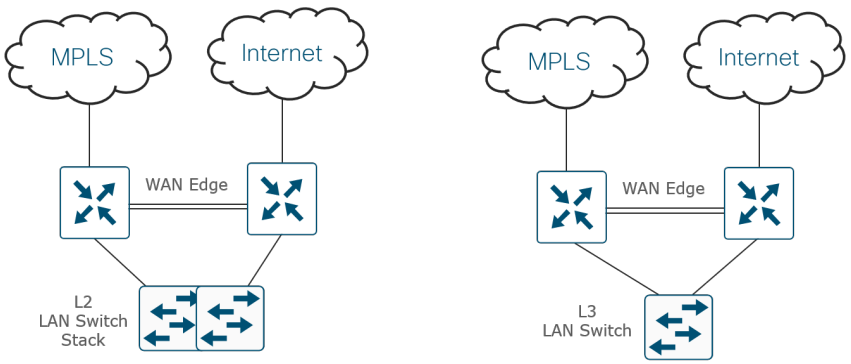


デュアル WAN エッジ

次の導入は、ブランチサイトに導入されたデュアル WAN エッジルータを示しています。各 WAN Edge ルータは 1 つのトランスポートに接続し、WAN Edge ルータは TLOC Extension リンクに直接接続されます。L2 スイッチスタック展開では、各 WAN エッジルータがスタック内の 1 つのスイッチに接続されます。WAN エッジルータは、ポートチャネルまたはスパニングツリープロトコルをサポートしません。各 WAN エッジルータがスイッチスタックにデュアル接続されている場合は、WAN エッジルータにブリッジインターフェイスを実装する必要があります。これにより、設定の複雑さが増すので、推奨しません。

L3 スイッチの導入では、ルーティングプロトコル（OSPF、BGP、または IOS XE SD-WAN ルータの EIGRP）がスイッチと WAN エッジルータ間で実行されます。

図 78.　　デュアル WAN エッジブランチの導入例



アプリケーションの可視性

アプリケーションの可視性は、SD-WAN の主要コンポーネントであり、いくつかの使用例の実現要因です。アプリケーションの可視性により、データトラフィックを詳細に検査および分析でき、ステートフル インスペクションや動作および統計分析などの高度な手法を使用して、プロトコルおよびアプリケーションを学習および分類できます。その後、モニタリング、セキュリティポリシー、Cloud onRamp for SaaS、アプリケーション認識型ルーティングポリシー、Quality of Service（QoS）などのさまざまな機能でアプリケーション分類を使用できます。Cloud onRamp for SaaS など、一部の機能ではアプリケーションの可視性が必要ですが、その他の機能では、ポリシーでアプリケーションマッチングを使用することはオプションです。

vEdge および IOS XE SD-WAN ルータは現在、異なる分類エンジンを使用しています。vEdge ルータは Qosmos 分類エンジンを使用してディープ パケット インスペクション（DPI）を使用し、IOS XE SD-WAN ルータは NBAR2 を使用します。両方のプラットフォームの相互運用性はサポートされていますが、アプリケーションの分類にわずかな違いがあるため、作成されるポリシーに影響がある可能性があります。

SD-AVC

SD-AVC は、可視性とポリシー設定のためのアプリケーション認識も実装しますが、集中型ネットワークサービスとして動作します。厳密にローカライズされた情報である DPI または NBAR2 のみを実行するのとは対照的に、SD-AVC はネットワーク内の複数のデバイスからアプリケーションデータを集約し、ネットワークノード間でアプリケーションの状態を同期できます。SD-AVC は、バージョン 18.4 以降の vManage でコンテナとして実行されます。SD-AVC は、現時点では、16.10.1 バージョンのコードから Linux コンテナを仮想サービスとして使用する IOS XE SD-WAN ルータでのみサポートされています。

アプリケーションの可視性のためのトラフィックの対称性

ローカライズされたアプリケーションの可視性機能（DPI および NBAR2）がほとんどのアプリケーション トラフィックを分類できるようにするには、WAN エッジルータがネットワークトラフィックを両方向で認識することが重要です。ポリシーが有効になっていないデュアル WAN エッジサイトでは、各トランスポート上および各 WAN エッジルータへの等コストパスが存在し、IP ヘッダーのフィールドに応じてネットワークトラフィックがハッシュされます。トラフィックが LAN から WAN、WAN から LAN の両方向で常に同じ WAN エッジルータに転送されることはほとんどありません。対称トラフィックを維持するために、デュアル WAN エッジルータサイトでトラフィックが 1 つの WAN エッジを別の WAN エッジよりも優先するようにルーティングを設定することを推奨します。

SD-AVC は集中型ネットワークサービスであり、アプリケーションの状態はネットワークノード間で同期されるため、トラフィックの対称性は必要ありません。

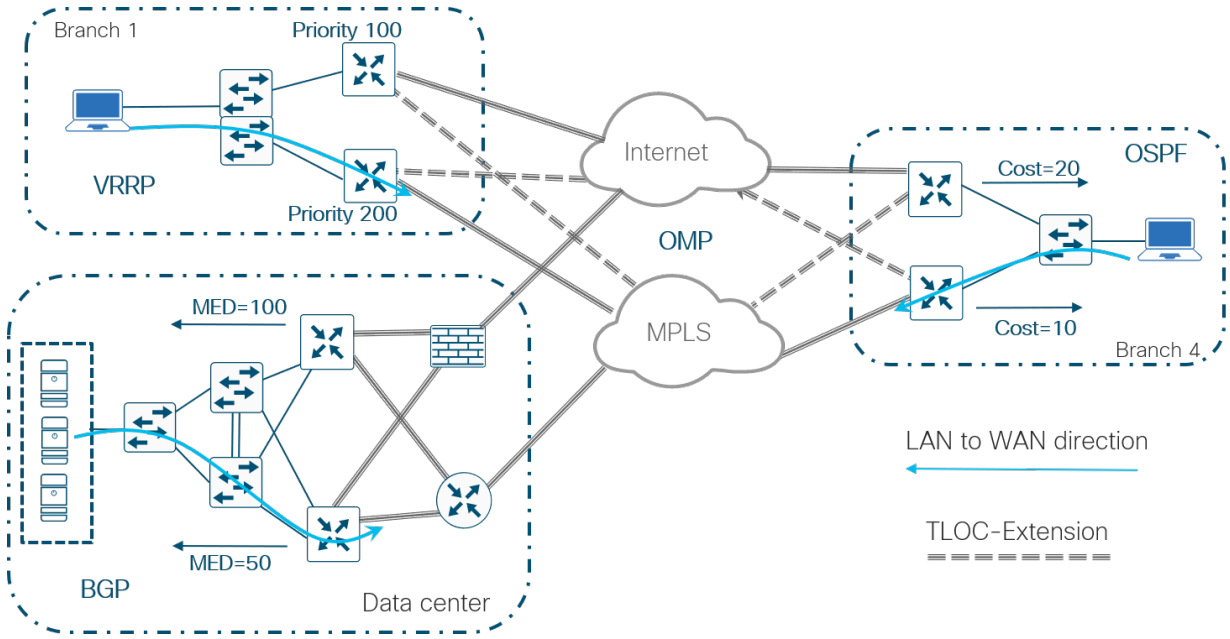
対称性を確保するために、トラフィックは、LAN から WAN、WAN から LAN の両方向で 1 つのルータを優先する必要があります。これを行うには、いくつかの方法があります。

LAN から WAN 方向のトラフィックに影響を与えるには、次の手順を実行します。

- VRRP の場合は、VRRP プライオリティを使用して、1 つの WAN エッジルータを優先します。最高のプライオリティ値を持つルータが優先されます。
- OSPF の場合は、隣接スイッチ/ルータ自体のインターフェイスで設定されたコストメトリックを使用するか、OMP から OSPF に再配布されたルートのメトリックを変更する WAN エッジルータのルートポリシーを使用して設定します。最も低いコストを持つリンクが優先されるパスです。

- EIGRP の場合は、隣接スイッチ/ルータのインターフェイスで設定された遅延メトリックを使用します。
- BGP の場合は、ルートポリシーを使用し、OMP から BGP に再配布されるルートに AS パスプリペンドまたは Multi-Exit 識別子（MED）を設定します。

図 79.　　LAN から WAN 方向のトラフィックへの影響

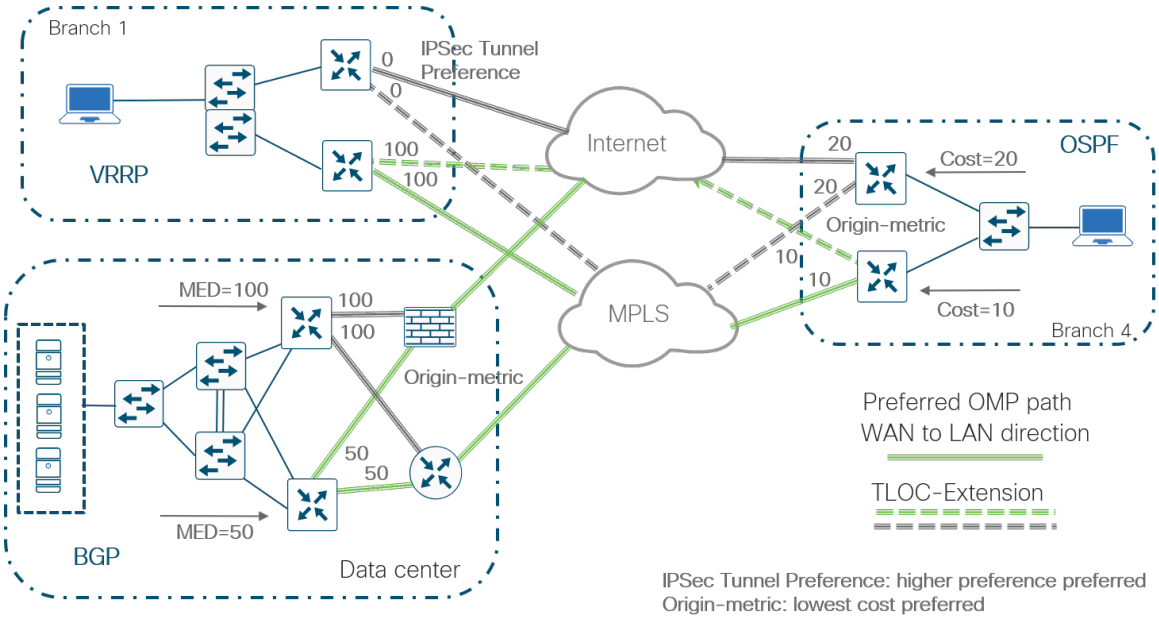


オーバーレイを介して WAN から LAN 方向のトラフィックに影響を与えるには、OMP 属性（OMP ルートプリファレンスを含む）を制御するか、トンネルインターフェイスで TLOC プリファレンスを設定します。BGP または OSPF が OMP に再配布されると、BGP の MED 設定と OSPF のコストは自動的に OMP 発信元メトリックに変換され、最適ルートを選択するための意思決定に使用されます。OMP メトリックを使用して SD-WAN オーバーレイ上のトラフィックに影響を与えることができますが、OMP ルートプリファレンスと TLOC プリファレンスを使用してトラフィックに影響を与えることが一般的です。

WAN から LAN 方向のトラフィックに影響を与える一般的な方法：

- BGP の場合、ルートポリシーを使用し、LAN BGP ネイバーから着信するルートに MED（メトリック）を設定します
- OSPF の場合、WAN エッジ ルータ インターフェイス コストを使用して、LAN インターフェイスに着信するルートのメトリックを設定します
- VRRP ルータを含むすべての WAN エッジルータの場合、TLOC プリファレンスを使用して、WAN オーバーレイを介して優先 WAN エッジを制御します

図 80.　　WAN から LAN 方向のトラフィックへの影響



WAN エッジのスケール

特定のサイトの WAN エッジルータのタイプを適切にサイジングすることが重要です。適切なサイジングを行うには、スループット制限、アクティブなスタティックトンネルの持続数、VPN セグメント、およびデバイスが処理できるルートの数を理解することが重要です。

IPsec Tunnels

デフォルトでは、集中型ポリシーおよび制限設定がない場合、WAN エッジルータは、カラーに関係なく、すべての WAN エッジルータのリモート TLOC と IPsec トンネルを形成しようとします。ネットワークの規模によっては、リモートサイトのルータのタイプと、それぞれがサポートできるトンネルの数が原因で、これは望ましくない場合があります。ブランチサイトでトンネルの数を制限する 1 つの方法は、ハブサイトの WAN エッジルータが必要なトンネルスケールに対応できるように、集中型制御ポリシーまたはトンネルグループを使用してハブアンドスポークトポロジまたは部分メッシュトポロジを設定することです。

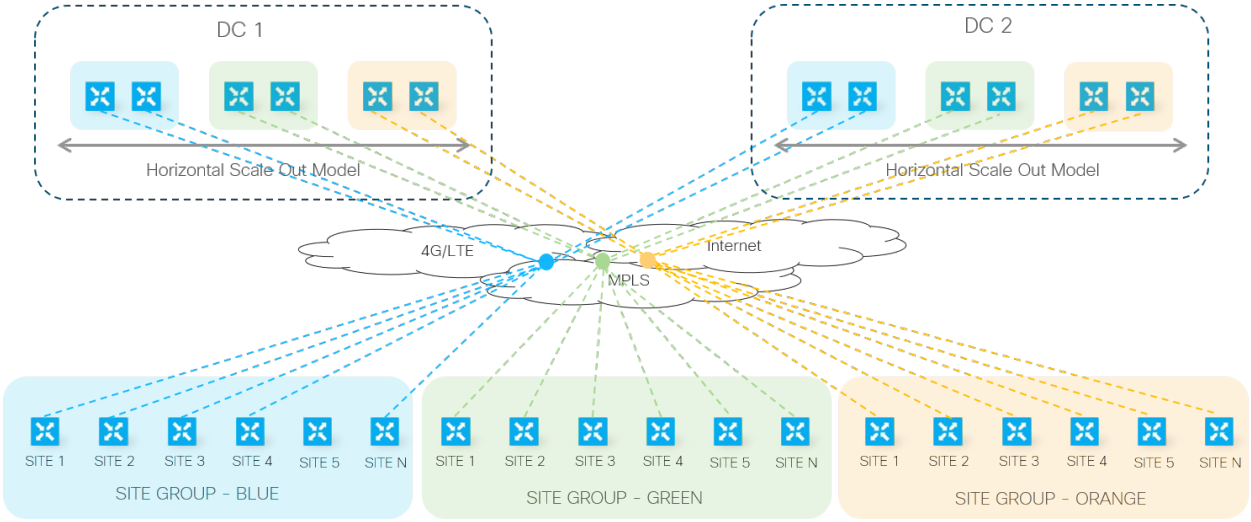
水平方向への拡張

サイトで必要なスループットまたは IPsec トンネルが、単一のルータでサポートできる数を超える場合があります。このような場合、WAN エッジルータは水平方向に拡張できます。これらのネットワーク用に設計する場合、vSmart コントローラでは、プレフィックスの等コストパスの数は 16 に制限され、デフォルトは 4 に設定されることに注意してください。

リモートサイトのグループ化

次の図は、ヘッドエンドルータでより多くのトンネルとスループットに対応するためのデータセンターの水平方向への拡張の例を示しています。すべてのリモートサイトは、異なるサイトグループに分割されます。各データセンターでは、サイトグループごとに、1 つのプライマリと 1 つのセカンダリの WAN エッジルータのペアが導入されます。トンネルは、集中型制御ポリシーを使用して、データセンタールータのペアとそれぞれのサイトグループ間で制限されます。トンネルグループは、さまざまなヘッドエンドルータへのサイトグループを作成するための大規模な設計でも使用できます。

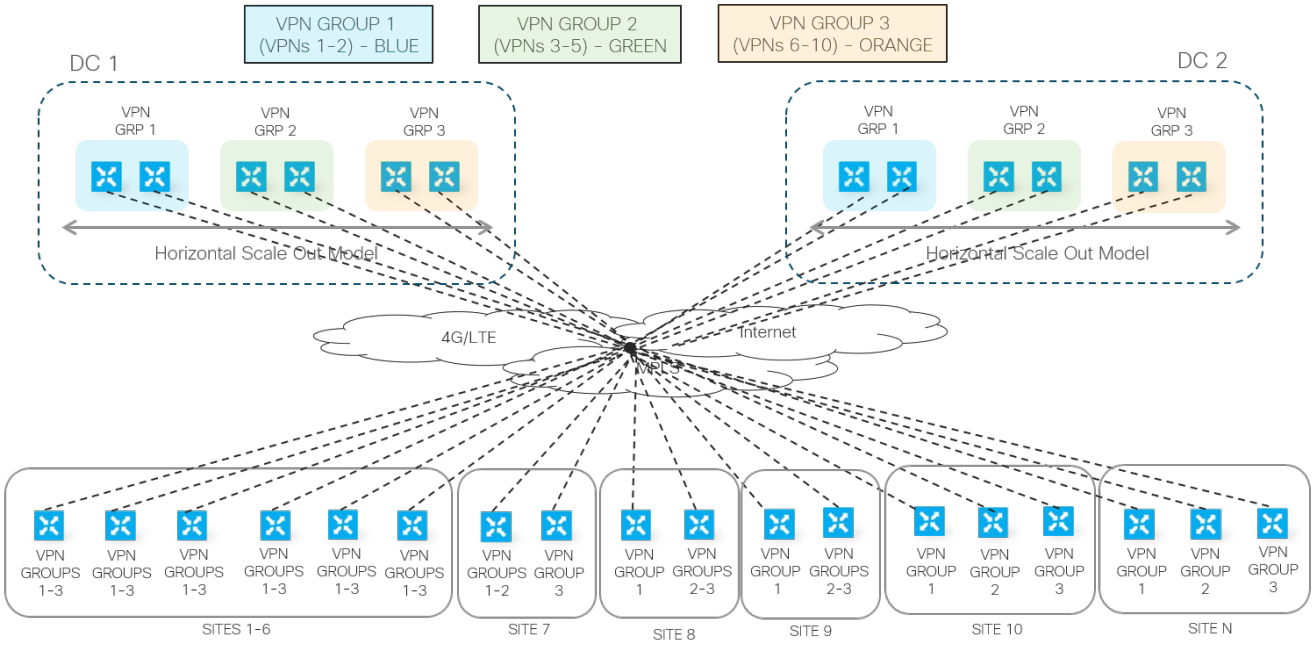
図 81.　　WAN エッジルータの水平方向への拡張例：サイトのグループ化



VPN のグループ化

水平方向への拡張を実現するもう 1 つの方法は、ルータ間で VPN を分散することによって、WAN エッジルータ間でトラフィックを分割することです。これにより、ヘッドエンドサイトに加えて、より多くの帯域幅を必要とするブランチで拡張できます。次の図に、この例を示します。VPN の 3 つのグループが作成されます。各データセンターでは、VPN の異なるセットごとに、1 つのプライマリと 1 つのセカンダリの WAN エッジルータのペアが導入されます。任意の数のブランチルータを VPN 間で分割できます。リモートサイトルータは、すべてのヘッドエンドルータへ完全なトンネル接続を行うことができます。また、サービス対象の VPN に応じて、集中型制御ポリシーを使用してフィルタリングすることもできます。

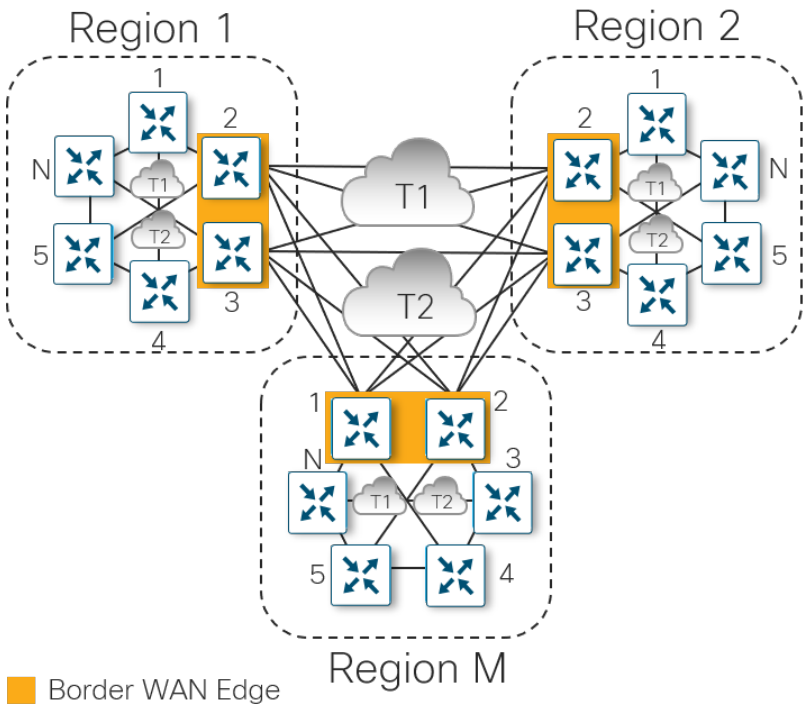
図 82.　　WAN エッジルータの水平方向への拡張例：VPN のグループ化



複数地域の導入

大規模な WAN エッジ導入では、WAN エッジルータが地域内でグループ化されることがよくあります。地域内では、WAN エッジルータは完全にメッシュ化されるか、ハブアンドスポークトポロジで設定されます。ハブアンドスポークトポロジは、トンネルがハブルータに対してのみ構築されるため、トンネル容量を節約できます。ボーダー WAN エッジルータは、地域内のハブルータとして機能し、他の地域内の他のボーダールータに接続します。地域内の TLOC は地域間のネットワークでは許可されません。ある地域の WAN エッジルータが別の地域の別の WAN エッジルータにトラフィックを送信するには、トラフィックがハブルータを通過する必要があります。

図 83.　　大規模な WAN エッジ導入：地域メッシュ



管理プレーン

vManage は、単一のダッシュボードからエンドツーエンドで SD-WAN ネットワークを管理できる Cisco SD-WAN 集中型 GUI です。

ソフトウェア

コントローラおよび WAN エッジルータのソフトウェアバージョンを選択する場合は、すべてのコードバージョンに互換性があることを確認してください。vManage コードバージョンに使用するものによって、さまざまなコントローラおよび WAN エッジルータでサポートされるバージョンが決まります。コードバージョンの互換性のリストについては、https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/compatibility-matrix.html の Cisco SD-WAN ハードウェア互換性マトリックスを参照してください。互換性があるものとしてコードバージョンがリストされている場合でも、vManage の最新バージョンでサポートされている特定の機能は、対応する互換性のあるコントローラまたは WAN エッジルータのソフトウェアバージョンではサポートされない場合があります。サポートされていない機能を vManage からそれらのデバイスにプッシュすると、エラーが発生することがあります。

新しいコードバージョンにアップグレードする前に、リリースノートを確認してください。リリースノートには、IOS XE SD-WAN デバイスの新機能、未解決のバグ、および ROMmon 要件が記載されています。
https://www.cisco.com/c/en/us/support/routers/sd-wan/products-release-notes-list.html

アップグレード

特定のコードバージョンに移行する場合は、最初に vManage、次にコントローラ（vBond、vSmart）、最後に WAN エッジルータでコードをアップグレードすることが重要です。WAN エッジルータをターゲットのコードバージョンに移行する前に、vManage とコントローラが適切なコードバージョンであることを確認します。また、アップグレードを進める前に、コントローラと WAN エッジルータの両方でコードの互換性を確認してください。WAN エッジルータは、必要に応じて、オンライン、ZTP または PnP プロセスの最後に、あるいは導入前に手動で一度アップグレードできます。

必要なコードバージョンがソフトウェアリポジトリにロードされた後、ソフトウェアのアップグレードには、アップグレードとアクティブ化の 2 つの部分があります。アップグレードするとコードバージョンが WAN エッジデバイスにインストールされ、それをアクティブ化するとデバイスが再起動し、新しいコードバージョンの実行が開始されます。これらの手順は、個別に実行することも、アップグレードの直後にアクティブ化を実行することもできます。

技術的なヒント
ベストプラクティスとして、非実稼働時に SD-WAN デバイスにソフトウェアをインストールすることを強く推奨します。これは、任意のサイトのトランスポートの帯域幅によっては実稼働トラフィックのパフォーマンスに影響を与える可能性があるためです。 アップグレードした後に、vManage を下位のメジャーリリースにダウングレードすることはできません。たとえば、18.3.x リリースを実行している場合、18.2.x 以下のバージョンにダウングレードすることはできません。vManage サーバに下位のコードバージョンをインストールできる場合はありますが、それをアクティブ化することはできません。アップグレードする前に VM スナップショットを作成して、必要に応じて下位のコードバージョンで復元できるようにします。

次に、ソフトウェアをアップグレードする際のベストプラクティスを示します。すべての手順を正確に実行する必要はありませんが、ダウンタイムを軽減するための計画を立て、予期しない状況が発生した場合にバックアウトするための計画を立てることが重要です。

1. （必須）最初に vManage をアップグレードしてアクティブ化します。
2. （強く推奨）vBond オーケストレータの半分をアップグレードしてアクティブ化し、他の半分をアップグレードしてアクティブにする前にオーケストレータを一定時間（たとえば 24 時間）安定した状態で実行します。vBond オーケストレータは、vManage サーバの後、vSmart コントローラの前に更新する必要があります。
3. （強く推奨）vSmart コントローラの半分をアップグレードしてアクティブ化し、他の半分をアップグレードしてアクティブにする前にコントローラを一定時間（たとえば 24 時間）安定した状態で実行します。vSmart コントローラは、vBond オーケストレータの後、WAN エッジルータの前に更新する必要があります。
4. WAN エッジルータをさまざまなアップグレードグループに分割します。システムテンプレートの [device groups] フィールドでタグを使用してグループを識別できます。1 つまたは複数のテストサイトをターゲットにし、それらの WAN エッジルータを最初のアップグレードグループに含めます。デュアル WAN エッジサイトでは、各ルータを別のアップグレードグループに含め、両方を同時にアップグレードしません。アップグレードグループ内のすべての WAN エッジルータは並行して（最大 32 の WAN エッジルータ）アップグレードできますが、WAN エッジルータへの同時ファイル転送を処理できる vManage またはリモートファイルサーバの機能を考慮してください。
5. 最初のアップグレードグループをアップグレードしてアクティブ化し、コードを事前に指定した時間安定した状態で実行させてから、事前に指定した時間内に追加のアップグレードグループのアップグレードおよびアクティブ化に進みます。vManage を使用してアップグレードする場合は、vManage またはリモート vManage に直接ロードされたコードイメージを使用してアップグレードできます。また、リモートファイルサーバ上にあるコードイメージを使用してアップグレードすることもできます。

技術的なヒント
vEdge コード 18.2.0 には、イメージのダウングレード機能を制限するセキュリティ拡張機能が実装されています。リリース 18.2.0 以降を実行している vEdge ルータにソフトウェア バージョン リリース 17.2 以前をインストールすることはできません。ただし、すでにインストールされている古いイメージはアクティブ化できます。 vEdge ルータにリリース 18.3 をインストールしてアクティブ化すると、1 週間後に、すべてのリリース 18.1 以前がルータから削除され、再インストールできなくなります。リリース 18.4 では、18.1 以前のすべてのリリースは 20 分後に削除され、再インストールできなくなります。

設定テンプレート

設定とポリシーは、データセンターとブランチ間またはブランチ間のトラフィックフローを可能にする WAN エッジルータおよび vSmart コントローラに適用されます。管理者は、WAN エッジデバイスのコンソールまたはセキュアシェル（SSH）を使用してコマンドライン インターフェイス（CLI）を介して、または vManage GUI を介してリモートで、設定とポリシーを有効にできます。

vManage GUI を使用してネットワーク上で WAN エッジデバイスまたはコントローラを設定するには、管理者がデバイステンプレートを 1 つまたは複数の WAN エッジルータに適用します。これらのテンプレートは、CLI ベースまたは機能ベースで作成できます。CLI ベースのテンプレートを作成することはできますが、機能ベースのテンプレートをお勧めします。モジュールベースで拡張性が高く、エラーが発生しにくいからです。各デバイステンプレートは、インターフェイス設定、トンネル設定、およびローカルルーティング動作を記述する複数の機能テンプレートで構成されます。

技術的なヒント
vManage 集中型ポリシーをネットワークに適用するには、vSmart コントローラを vManage で管理する必要があります。これを実現するには、CLI または機能ベースのデバイステンプレートをアタッチします。

テンプレートは非常に柔軟であり、テンプレートを組み合わせるための多くのアプローチがあります。テンプレート内の変数の数を増やすと、機能テンプレートの数が減り、変数の数を減らすと、機能テンプレートの数が増えます。たとえば、変数またはグローバル値として NAT を有効にすることができます。1 つのインターフェイス機能テンプレートを作成し、変数を使用して NAT を有効または無効にすることを選択できます。または、NAT を無効にしたものと NAT を有効にしたものの 2 つの異なる機能テンプレートを作成し、デバイステンプレートにより、使用するのに最も適切な機能テンプレートを選択できます。いずれの場合も、GUI で各機能とデバイステンプレートの詳細な説明を追加し、各テンプレートと変数が非常に明確になるように、非常にわかりやすい変数名を作成する必要があります。

設定テンプレートを設計するときは、運用が日常的にどのようにテンプレートと連携するかを考えると役立ちます。新しい機能テンプレートを作成してそれを使用する（または同じ機能テンプレートを使用して他のデバイスに割り込む）必要なく、トラブルシューティングのためにインターフェイスを移動できるように、インターフェイス名に変数を使用すると便利です。また、インターフェイスやルーティングプロトコルの状態の変数を作成すると、変数を変更するだけでインターフェイスや BGP ネイバーを無効にできるなど、トラブルシューティングの理由で役立つ場合があります。

技術的なヒント
vManage バージョン 20.1 以降、機能テンプレートは vEdge と IOS XE SD-WAN デバイス間で共有できなくなりました。共有されている機能テンプレートの場合、vManage 20.1 にアップグレードできますが、共有機能テンプレートを変更または編集することはできません。共有機能テンプレートのコピーを作成し、IOS XE SD-WAN デバイスをこれらの新しい機能テンプレートを参照するデバイステンプレートに移行する必要があります。この機能テンプレートの移行を支援するスクリプトを使用できます。詳細については、https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/c-template-migration.pdf を参照してください。

デバイステンプレート

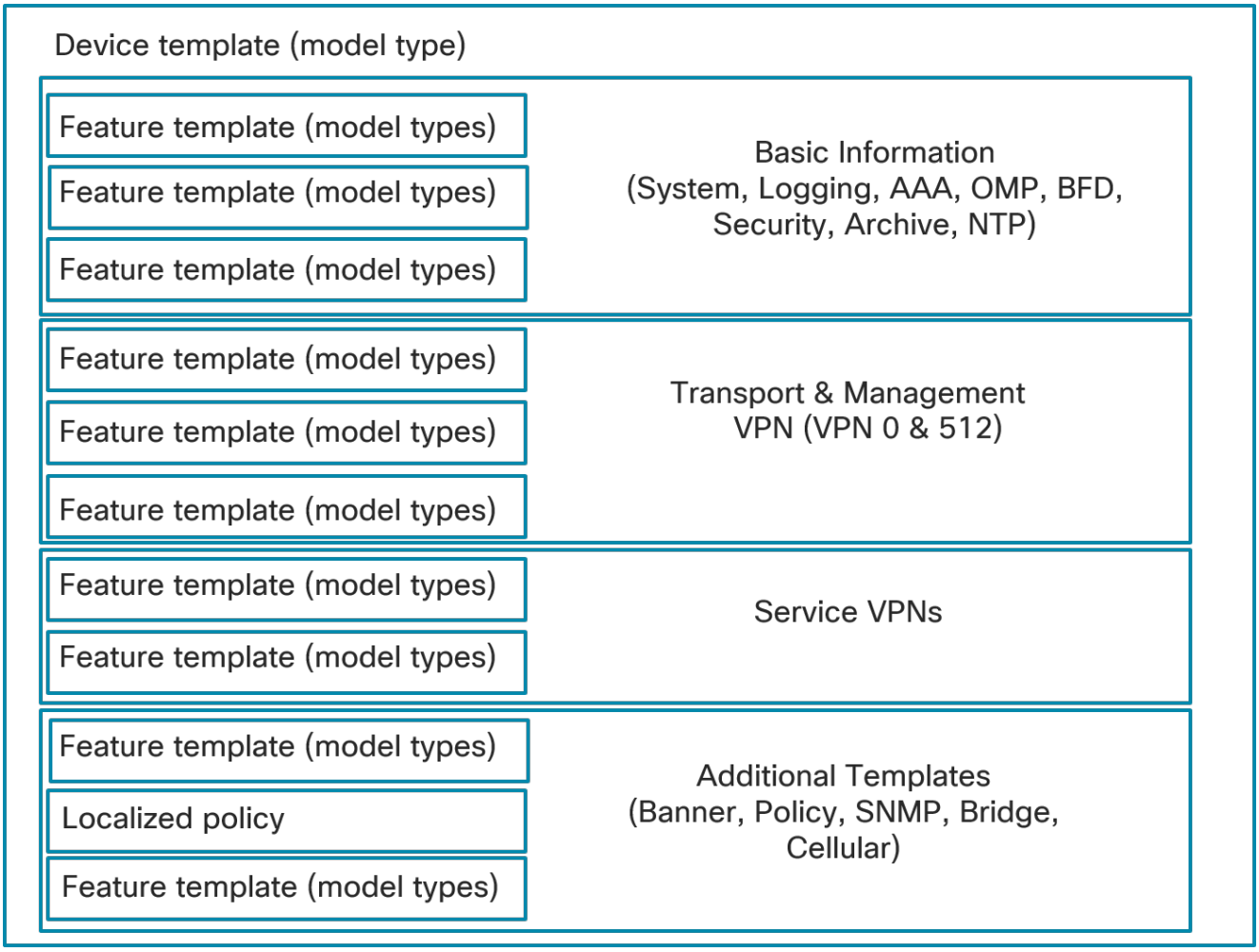
デバイステンプレートは、1 つの WAN エッジモデルタイプに固有ですが、ネットワーク内での場所と機能のために、同じモデルタイプの複数のデバイステンプレートを作成する必要がある場合があります。各デバイステンプレートは、デバイスの設定全体を構成する一連の機能テンプレートを参照します。デバイステンプレート設定を WAN エッジモデル間で共有することはできませんが、機能テンプレートは複数のモデルタイプにまたがることができ、異なるデバイステンプレートで使用できます。

次の図に、デバイステンプレートのコンポーネントを示します。デバイステンプレートは、次のセクションにグループ化された機能テンプレートで構成されます。

- 基本情報：このセクションには、システム、ロギング、AAA、OMP、BFD、セキュリティ、および NTP 機能テンプレートが含まれます。
- トランスポートおよび管理 VPN：このセクションには、VPN 0（アンダーレイ）および VPN 512（アウトオブバンド管理）の設定に使用されるテンプレートが含まれています。これには、BGP、OSPF、VPN インターフェイス、VPN インターフェイスセルラー、VPN インターフェイス GRE、および VPN インターフェイス PPP 機能テンプレートが含まれます。
- サービス VPN：このセクションには、サービス VPN の設定に使用されるテンプレートが含まれています。これには、BGP、IGMP、マルチキャスト、OSPF、EIGRP、PIM、VPN インターフェイス、VPN インターフェイスブリッジ、VPN インターフェイス GRE、VPN インターフェイス IPsec、VPN インターフェイス NAT プール、および DHCP サーバ機能テンプレートが含まれます。
- セルラー：このセクションには、セルラーまたは T1/E1 コントローラの設定に使用されるテンプレートが含まれています。
- 追加のテンプレート：このセクションには、バナー、Simple Network Management Protocol（SNMP）、ブリッジ、ローカライズされたポリシー、およびセキュリティ ポリシー テンプレートが含まれています。

技術的なヒント
各デバイステンプレートでサポートされる機能テンプレートは、SD-WAN プラットフォームによって異なります。

図 84.　　デバイステンプレート



機能テンプレート

次に、いくつかの異なる機能テンプレートの簡単な説明と、それぞれが設定できる情報のサブセットを示します。

- システム：サイト ID、システム IP、タイムゾーン、ホスト名、デバイスグループ、GPS 座標、ポートホッピング、ポートオフセットなどの基本的なシステム情報を設定します。
- ロギング：ディスクおよび/またはリモートロギングサーバへのロギングを設定します。
- AAA：認証方式と順序を指定し、異なる読み取り/書き込み権限を持つローカルユーザグループを含む、RADIUS、TACAC、またはローカル認証を設定します。
- BFD：BFD アプリケーションルート乗数とポーリング間隔を指定し、各トランスポートの hello および BFD 乗数を指定します。
- OMP：グレースフル リスタート タイマーとアドバタイズメントタイマー、ホールドタイマーを変更します。アドバタイズされるパスの数を変更します。AS オーバーレイ番号を設定します。OMP にアドバタイズされるローカルプロトコルを選択します。WAN エッジルータにインストールされている等コストパスの数を変更します。
- セキュリティ：IPsec のキー再生成時間、アンチリプレイウィンドウ、および認証タイプを変更します。

- アーカイブ（オプション）：指定した期間内に完全な実行コンフィギュレーションをファイルサーバにアーカイブします。
- NTP（オプション）：必要に応じて NTP サーバと認証を設定します。
- VPN：ECMP ハッシュを変更し、DNS サーバを追加し、VPN から OMP にプロトコル（BGP、スタティック、接続、OSPF 外部）をアドバタイズし、IPv4 または v6 スタティックルート、サービスルート、および GRE ルートを追加します。
- BGP（オプション）：AS 番号、ルータ ID、距離、最大パス、ネイバー、BGP へのプロトコルの再配布、ホールド時間、およびキープアライブタイマーを設定します。
- OSPF（オプション）：ルータ ID、距離、エリア、OSPF インターフェイス、参照帯域幅、デフォルト情報発信元、メトリック、メトリックタイプ、および SPF タイマーを設定します。
- VPN インターフェイス設定：インターフェイス名、インターフェイスのステータス、スタティックまたはダイナミック IPv4 および v6 アドレッシング、DHCP ヘルパー、NAT、VRRP、シェーピング、QoS、IPv4 および 6 の入力/出力アクセスコントロールリスト（ACL）、ポリシング、スタティック Address Resolution Protocol（ARP）、802.1x、デュプレックス、MAC アドレス、IP 最大伝送ユニット（MTU）、伝送制御プロトコルの最大セグメントサイズ（TCP MSS）、TLOC Extension などを設定します。トランスポート VPN の場合は、トンネル、トランスポートカラー、インターフェイスに許可されるプロトコル、カプセル化、プリファレンス、重み付けなどを設定します。
- VPN インターフェイスブリッジ（オプション）：IPv4 アドレス、DHCP ヘルパー、ACL、VRRP、MTU、TCP MSS などのブリッジインターフェイスのレイヤ 3 特性を設定します。
- DHCP サーバ（オプション）：DHCP サーバの特性（アドレスプール、リース時間、スタティックリース、ドメイン名、デフォルトゲートウェイ、DNS サーバ、TFTP サーバなど）を設定します。
- バナー（オプション）：ログインバナーまたは Message-of-The-Day バナーを設定します。
- ポリシー（オプション）：ローカライズされたポリシーをアタッチします。
- SNMP（オプション）：SNMP デバイスの名前と場所、SNMP バージョン、ビュー、コミュニティ、トラップグループなどの SNMP パラメータを設定します。
- ブリッジ（オプション）：VLAN ID、MAC アドレスエージング、最大 MAC アドレス、ブリッジの物理インターフェイスなど、ブリッジのレイヤ 2 特性を定義します。

BGP、OSPF、または EIGRP などのルーティング プロトコル テンプレートと VPN インターフェイス テンプレートは、VPN で設定されます。DHCP サーバ機能テンプレートは、VPN インターフェイスで設定されます。

パラメータの設定

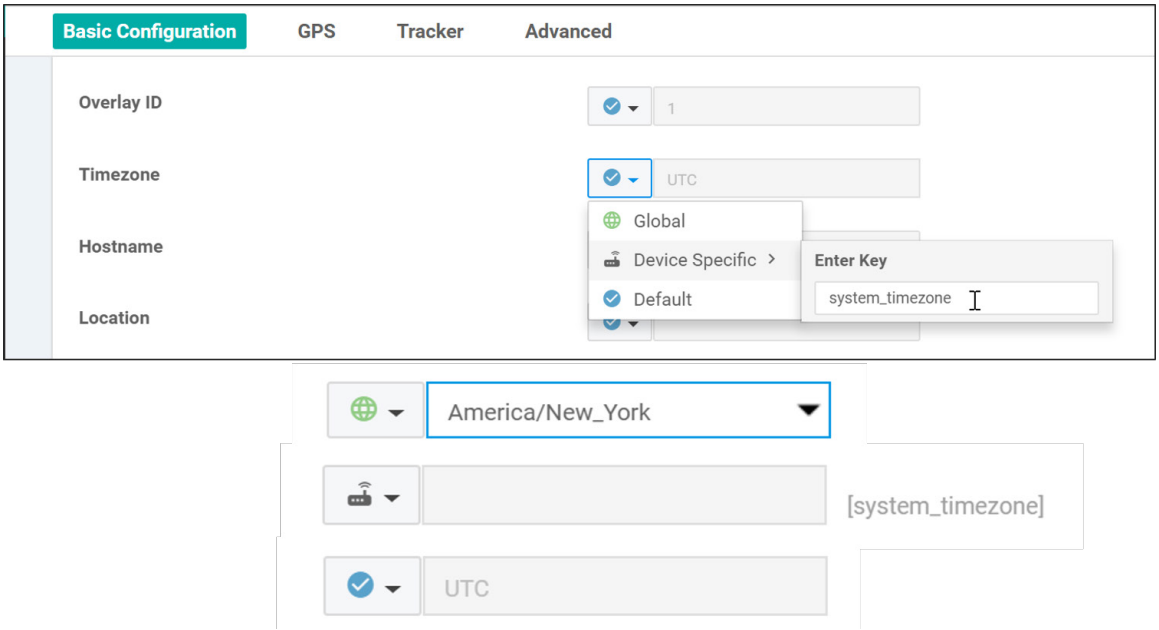
テンプレートは固有の設定を持つ複数の WAN エッジデバイスに適用できるため、管理者は vManage を使用してデバイステンプレートと機能テンプレートを設定し、必要に応じて変数を指定します。

機能テンプレート内のパラメータの値を設定する場合は、多くの場合、3 つの異なるタイプの値を示すドロップダウンボックスがあります。

- グローバル：グローバル値を指定する場合は、テキストボックスに値を入力するか、ラジオボタンから選択肢を選択するか、ドロップダウンボックスから値を選択して、目的の値を指定します。選択した値は、機能テンプレートが適用されるすべてのデバイスに適用されます。
- デバイス固有：デバイス固有の値を指定すると、変数名が作成されます。この変数の値は、デバイステンプレートが適用されるときに定義されます。
- デフォルト：デフォルト値を指定すると、機能テンプレートが適用されるすべてのデバイスにデフォルト値が適用されます。特定の値がある場合は、テキストボックスにグレースケールで表示されます。

次の図では、**タイムゾーン**がグローバル値、デバイス固有の値、またはデフォルト値として示されています。デバイス固有の値を指定する場合は、変数名を入力します。

図 85.　　機能テンプレートのパラメータ値のタイプ



技術的なヒント
各機能テンプレート内では、2 つの異なるパラメータ値に同じ変数名を使用できますが、これらは 2 つの異なる変数のように扱われます。デバイステンプレートをデバイスに適用するときに入力する必要がある値が明確になるように、説明的で一意の変数名が重要です。異なるテンプレートで同じ名前の変数も異なる変数であり、テンプレート間で共有することはできません。

オプション設定

18.2 vManage コードバージョンから、多くの個々の機能テンプレート設定をオプションとしてマークできるようになりました。これにより、個別の機能テンプレートをすべて定義するのではなく、わずかに設定が違う複数のルータに単一の機能テンプレートを使用できます。たとえば、あるサイトでスタティックルートを使用し、別のサイトでは使用しない場合、VPN テンプレートでスタティックルートをオプションにして、スタティックルートを含む 1 つのテンプレートとスタティックルートのない別のテンプレートを作成する代わりに、両方のルータで同じテンプレートを使用できます。

デバイステンプレートの導入

機能テンプレートが設定されると、各設定カテゴリ（システム、AAA、BFD、VPN、VPN インターフェイスなど）で目的の機能テンプレートを参照して、デバイステンプレートの設定が完了します。デバイステンプレートを設定すると、特定の WAN エッジデバイスに接続できます。接続したら、設定を導入する前に、テンプレートを適用する各 WAN エッジのテンプレートの変数の値を入力する必要があります。vManage GUI から直接値を入力するか、アップロード可能な .csv ファイルに値を入力します。.csv ファイル方式を使用すると、多数の WAN エッジルータを迅速かつ簡単に導入できます。vManage は、データベース内のターゲット WAN エッジデバイスの設定を変更してから、設定全体をネットワーク上の目的の WAN エッジルータにプッシュします。

機能テンプレートまたはデバイステンプレートを更新すると、それらのテンプレートに接続されているデバイスがある場合、アプリケーションはすぐに実行されます。設定がプッシュされ、誤った値形式や存在しないループバック インターフェイスへの参照などのエラーが発生した場合、テンプレート設定は編集前の状態にロールバックされます。

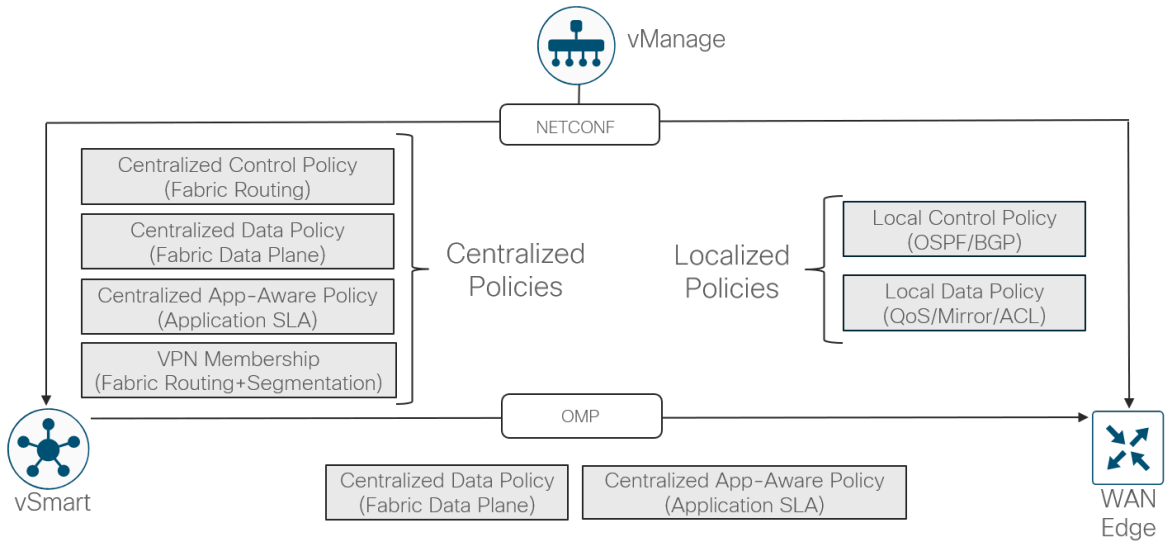
ポリシー

ポリシーは、Cisco SD-WAN ソリューションの重要な部分であり、オーバーレイネットワーク内の WAN エッジルータ間のデータトラフィックのフローに影響を与えるために使用されます。ポリシーは、コントロールプレーンまたはデータプレーンのいずれかのトラフィックに適用され、vSmart コントローラに一元的に（集中型ポリシー）、または WAN エッジルータにローカルに（ローカライズされたポリシー）に設定されます。

集中型制御ポリシーは、ルーティングと TLOC の情報に基づいて機能します。これにより、ルーティングの判断をカスタマイズし、オーバーレイネットワークを介したルーティングパスを決定できます。これらのポリシーは、トラフィック エンジニアリング、パスアフィニティ、サービス挿入、さまざまな種類の VPN トポロジ（フルメッシュ、ハブアンドスポーク、地域メッシュなど）の設定に使用できます。別の集中型制御ポリシーは、アプリケーション認識型ルーティングであり、さまざまなトラフィックタイプのリアルタイムのパスパフォーマンス特性に基づいて最適なパスを選択します。ローカライズされた制御ポリシーを使用すると、特に OSPF または BGP ルートマップとプレフィックスリストを使用して、ローカルサイトのルーティングポリシーに影響を与えることができます。

データポリシーは、IP パケットヘッダーと VPN メンバーシップのフィールドに基づいて、ネットワークを通過するデータトラフィックのフローに影響を及ぼします。集中型データポリシーは、アプリケーション ファイアウォール、サービスチェーン、トラフィック エンジニアリング、quality of service（QoS）、および Cflowd の設定に使用できます。ローカライズされたデータポリシーを使用すると、特定のサイトでのデータトラフィックの処理方法（ACL、QoS、ミラーリング、ポリシングなど）を設定できます。一部の集中型データポリシーは、アプリケーションルートポリシーまたは QoS 分類ポリシーの場合と同様に、WAN エッジ自体の処理に影響を与えることがあります。そのような場合でも、設定は vSmart コントローラに直接ダウンロードされますが、WAN エッジルータに伝達する必要があるポリシー情報はすべて OMP を介して伝達されます。

図 86.　　集中型およびローカライズされたポリシー



ローカライズされたポリシーの設定

ローカライズされたポリシーを設定および適用するには、次の 3 つの手順があります。

vManage GUI で、[Configuration] > [Policies] でローカライズされたポリシーを作成し、[Localized Policy] タブを選択します。リリース 18.2 より前では、ポリシーは CLI ポリシーとして追加されます。リリース 18.2 から、ポリシーの作成を支援するポリシー設定ウィザードが作成されました。

デバイステンプレートで、[Policy] の横にある [Additional Templates] セクションで、ローカライズされたポリシーの名前を参照します。

機能テンプレート内のルートポリシーやプレフィックスリストなどのポリシーコンポーネントを参照します。

デバイステンプレートを作成し、すでにルートポリシーまたはプレフィックスリスト、あるいは別のローカライズされたポリシーコンポーネントが設定されている機能テンプレートを参照する場合、デバイステンプレートを作成または更新する前に、デバイステンプレートで参照されているポリシー名が必要です。デバイスが既存のデバイステンプレートにすでに接続されている場合は、そのデバイステンプレートに関連付けられている機能テンプレート内のローカライズされたポリシー要素を参照する前に、まずはローカライズされたポリシーをデバイステンプレートに接続する必要があります。

WAN エッジデバイスに適用できるローカライズされたポリシーは 1 つだけです。このポリシー内で、制御ポリシーコンポーネントとデータ ポリシー コンポーネントの両方を作成します。プレフィックスリスト、ルートポリシー、as-path リスト、コミュニティリスト、QoS クラスマップ、qos マップポリシー、ミラーポリシーおよびポリシングポリシー、書き換えルールポリシー、およびアクセスリストはすべて、この 1 つのローカライズされたポリシーに含まれます。

集中型ポリシーの設定

vManage GUI で集中型ポリシーを設定する場合、次の 3 つの主要コンポーネントがあります。

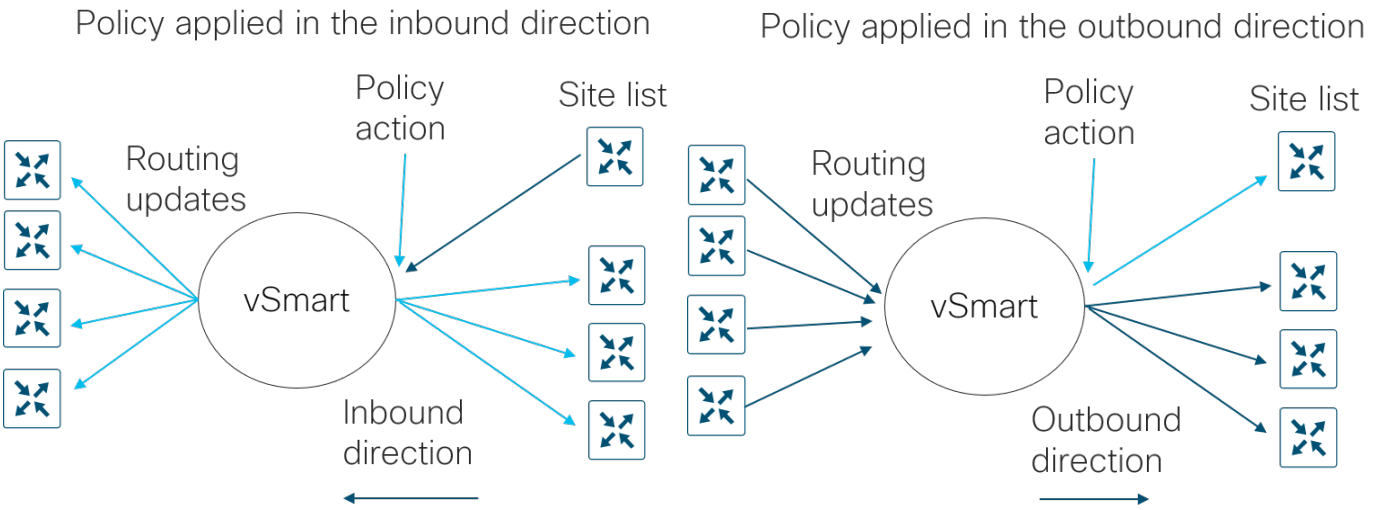
- リスト：リストは、関連する項目をグループ化してグループとして参照できるようにするために使用されます。これらは、ポリシーの適用時に使用されるか、ポリシー定義内の照合またはアクションで使用されます。アプリケーション、カラー、データプレフィックス、ポリサー、プレフィックス、サイト、SLA クラス、TLOC、および VPN のリストを作成できます。データプレフィックスはデータプレフィックスを定義するためにデータポリシーで使用され、プレフィックスはルートプレフィックスで照合するために制御ポリシーで使用されます。
- ポリシー定義：ポリシー定義は、制御と転送の側面を制御します。ポリシー定義内で、ポリシールールを作成し、順番に検査される一連の match-action ペアを指定します。ポリシー定義には、アプリケーションルートポリシー、cflowd テンプレート、制御ポリシー、データポリシー、および vpn メンバーシップポリシーがあります。
- ポリシーの適用：ポリシーはサイトリストに適用されます。

ポリシー定義にはいくつかの異なるタイプがあります。

- アプリケーションルート ポリシー：損失、遅延、ジッターなどのパス特性を追跡するアプリケーション認証型ルーティングポリシーを作成できます。トラフィックはさまざまな SLA カテゴリ（損失、遅延、およびジッター）に分類され、トラフィックは SLA カテゴリを満たす能力に応じて異なるパスに送信されます。
- Cflowd テンプレート：cflowd を有効にし、サンプリングされたネットワークデータフローをコレクタに送信します。
- 制御ポリシー：コントロール プレーン トラフィックで動作し、ネットワーク内のルーティングパスに影響します。
- データポリシー：IP パケットヘッダーのフィールドに基づいて、データトラフィックのフローに影響を及ぼします。
- VPN メンバーシップポリシー：WAN エッジルータでの VPN への参加とそのルートテーブルの数を制限できます。

制御ポリシーは、ルーティング情報内のルートと TLOC 属性を調べ、ポリシーに一致する属性を変更します。このポリシーは単方向で、着信方向または発信方向のサイトリストに適用できます。方向は、vSmart コントローラから見たものです。着信方向のサイトリストに適用されるポリシーは、サイトリストのサイトからのルートにポリシーが適用され、vSmart コントローラの受信側にアクションが適用されることを意味します。発信方向のサイトリストに適用されるポリシーは、サイトリストのサイトに向かうルートにポリシーが適用され、vSmart コントローラの送信側にアクションが適用されることを意味します。

図 87.　　集中型ポリシーの適用



アプリケーションルート ポリシーでは方向は設定されません。このポリシーは、OMP 経由で WAN エッジルータに送信され、LAN から WAN への方向にトラフィックが移動するときに WAN エッジに適用されます。cFlowd および VPN ポリシーでも方向は設定されません。ただし、データポリシーは WAN エッジの視点から見ると方向性があります。これは、from-service、from-tunnel、または all のいずれかで適用できます。

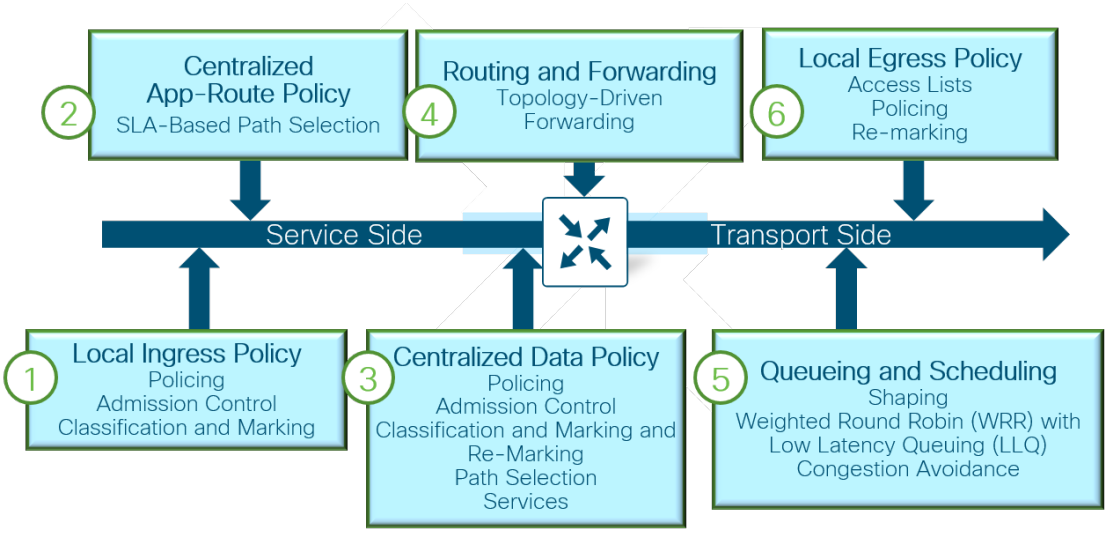
vManage GUI 内で複数の集中型ポリシーを作成できますが、vSmart コントローラで一度にアクティブにできるのは 1 つだけです。集中型ポリシー内では、集中型ポリシーを構成する複数の異なるポリシー定義（アプリケーションルート、cflowd、制御、データ、vpn メンバーシップポリシーなど）を作成できます。特定のサイトリストでは、各タイプのポリシーのいずれかに制限されますが、各方向（着信と発信）に異なる制御ポリシーを設定できます。ポリシー定義を適用する目的でサイト ID リストを作成する場合は、異なるリストのサイト ID と重複させないでください。

動作順序

次に、WAN エッジルータでサービス VPN からトランスポート VPN を通過するパケットの動作順序を示します。

1. ローカルポリシー/設定：QoS 分類、ポリサー、およびマーキングを含む
2. 集中型アプリケーション認識型ルーティングポリシー
3. 集中型データポリシー：QoS 分類、ポリサー、マーキング、およびパス選択を含む
4. ルーティング/転送
5. スケジューリングとキューイング
6. ローカル ポリシー シェーピングおよび ACL：シェーピング、再マーキング、およびポリサーを含む

図 88.　　WAN エッジルータでの動作のポリシー順序



順序付けから、集中型データポリシーがローカルデータポリシー設定のアクションを上書きする可能性があります。また、集中型データポリシーが、アプリケーション認識型ルーティングポリシーの一部として選択されたものとは異なるパス選択に影響を与える可能性もあります。ネットワークのポリシーを定義する際には、この情報に留意してください。

展開のプランニング

設定、日常の運用、およびメンテナンスを容易にするために、SD-WAN の導入を慎重に計画することが重要です。次に、いくつかの考慮事項を示します。

ポート番号付け

ネットワーク全体で一貫したポート番号スキームを使用することを推奨します。一貫性によって、容易な設定とトラブルシューティングをサポートします。

また、WAN エッジルータの工場出荷時のデフォルト設定では、VPN 0 の特定のポートが DHCP 用に指定されているため、WAN エッジは自動的に DHCP アドレスを取得し、DNS を解決し、ZTP または PnP サーバと通信できます。したがって、ZTP または PnP を使用する場合は、このポートをネットワーク内の最も適切な場所に接続して、DHCP サーバと DNS サーバに到達できることを確認してください。

システム IP

システム IP は、インターフェイスアドレスとは無関係にデバイスを一意に識別する永続的なシステムレベルの IPv4 アドレスです。ルータ ID のように機能するため、アンダーレイでアドバタイズまたは認識される必要はありません。ただし、ベストプラクティスは、このシステム IP アドレスをサービス VPN にアドバタイズし、SNMP およびロギングの送信元 IP アドレスとして使用することです。これにより、ネットワークイベントと vManage 情報の関連付けが容易になります。WAN エッジルータをコントローラで認証し、オーバーレイネットワークに導入するには、システム IP アドレスを設定する必要があります。

サイトを認識しやすくするために、システム IP アドレスの論理スキームを使用することをお勧めします。

サイト ID

サイト ID は、数値 1 ～ 4294967295 を持つ SD-WAN オーバーレイネットワーク内のサイトの一意の識別子です。この ID は、同じサイトに存在するすべての WAN エッジデバイスで同じである必要があります。サイトには、データセンター、ブランチオフィス、キャンパスなどがあります。WAN エッジルータをコントローラで認証し、オーバーレイネットワークに導入するには、サイト ID を設定する必要があります。デフォルトでは、同じサイト内の WAN エッジルータ間で IPsec トンネルは形成されません。

サイト ID スキームは、ポリシーの適用を容易にするため、慎重に選択する必要があります。ポリシーを適用すると、サイト ID のリストまたは範囲にポリシーが適用されます（例：100,200-299）。ワイルドカードはサポートされません。

サイト ID スキームを編成する方法はいくつかありますが、次の表に、6 桁を使用するスキームの例を示します。

表 8. Cisco SD-WAN サイト ID スキーム

目	表記	例
1	国/大陸	1 = 北米、2 = ヨーロッパ、3 = アジア太平洋地域
2	リージョン	1 = 米国西部、2 = 米国東部、3 = カナダ西部、4 = カナダ東部
3	サイトタイプ	0 = ハブロケーション、1 = タイプ 1 サイト、2 = タイプ 2 サイト、3 = タイプ 3 サイト、4 = タイプ 4 サイト、5 = 将来の使用
4-6	ストア、サイト、ブランチ番号、またはその他の ID 指定子	001、002、003 など

地域別のグループ化は、集中型インターネットアクセスや、他の国や地域のハブへの接続のために、地域のデータセンターを別の地域より優先する場合に役立ちます。

サイトタイプは、ポリシーの適用を容易にするために、適用されるポリシーのタイプに従って作成する必要があります。新しいサイトが作成されると、ポリシーの一致範囲に該当するサイト ID を作成するだけで、ポリシーが自動的に適用されます。タイプに応じてブランチをグループ化する方法の例を次に示します。

- 中央に配置されたファイアウォールまたは中央に配置された別のサービスを使用するブランチ。
- ダイレクト インターネット アクセスを使用するブランチ。
- 低い帯域幅のサイトと高い帯域幅のサイト。サイトごとに異なるトポロジが必要な場合があるためです。高帯域幅のサイトではフルメッシュトポロジを使用するのに対し、低帯域幅のサイトではハブアンドスポークトポロジを使用して帯域幅を節約できます。
- さまざまな SLA およびトランスポート要件。たとえば、重要なトラフィック、音声、およびビデオに MPLS を使用し、他のすべてはインターネット回線を通過する、またはサイトによっては、音声のみに MPLS を使用し、他のすべてはインターネット回線を通過するかもしれません。

もちろん、重複するタイプを持つことができますが、目的は設定の観点からポリシーを適用しやすくするカテゴリに分けることです。サイト ID を割り当てる前に、必要な要件とポリシーを検討することが役立ちます。

デバイスグループ

デバイスグループは、WAN エッジデバイスに割り当てられるラベルで、vManage GUI を使用してモニタリングやアップグレードを行う際に、共通のデバイスを編成およびグループ化するのに役立ちます。デバイスグループを使用すると、デバイスリストをフィルタリングして、デバイスの管理を容易にすることができます。WAN エッジデバイスは、1 つ以上のデバイスグループに属することができます。タイプ、場所、または機能に応じて SD-WAN デバイスを編成することも、アップグレード手順中にさまざまなアップグレードグループに入れることもできます。

付録 A：参照ドキュメント

- 『Cisco EN Validated Design and Deployment Guides』：https://cs.co/en-cvds
- SD-WAN コミュニティ
- Cisco.com SD-WAN ページ
- 『Cisco SD-WAN Cloud Scale Architecture E-book』
- Cisco SD-WAN リリースノート
- 『Cisco SD-WAN Configuration Guides』
- 『Cisco SD-WAN Migration Guide』
- 『Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices』
- 規範的な導入ガイド：
  - 『SD-WAN：Secure Direct Cloud Access for Cisco IOS-XE SD-WAN Devices Deployment Guide』
  - 『SD_WAN：Secure Direct Internet Access for Cisco IOS-XE SD-WAN Devices Deployment Guide』
  - 『SD-WAN：Secure Guest Access for Cisco IOS-XE SD-WAN Devices Deployment Guide』
  - 『Cisco SD-WAN：Application-Aware Routing Deployment Guide』
  - 『Cisco SD-WAN：WAN Edge Onboarding Deployment Guide』
  - 『Cisco SD-WAN：Enabling Firewall and IPS for Compliance』
  - 『SD-WAN Controller Certificates and Authorized Serial Number File Deployment Guide』
  - 『SD-WAN End-to-End Deployment Guide』
  - 『SD-WAN：Enabling Direct Internet Access Deployment Guide』
  - 『SD-WAN：Enabling Cisco Cloud onramp for IaaS with AWS Deployment Guide』
  - 『SD-WAN：Cloud onramp for SaaS Deployment Guide』
  - 『SD-WAN Administrator-Triggered Cluster Failover Deployment Guide』

フィードバック

このガイドおよび関連ガイドに関するコメントおよび提案については、https://cs.co/en-cvds のシスココミュニティのディスカッションに参加してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。