Cisco SD-WAN ソリューション

Cisco SD-WAN ソリューション

Cisco SD-WAN ソリューションの必要性

従来のネットワーキングテクノロジーは、ますます高価で複雑になってきており、現代のマルチサイト企業のニーズに合わせて拡張することができません。Cisco SD-WAN ソリューションは、実績のあるネットワーキングの要素に基づいており、エンタープライズネットワークの運用コストを削減する洗練されたソフトウェアベースのソリューションを提供し、複数の場所と地域にまたがって分散した大規模で複雑なネットワークのプロビジョニングと管理を簡素化する簡単なツールを提供します。Cisco SD-WAN ソリューションには、ネットワークとそのデータトラフィックの安全性とプライバシーを確保する固有の認証およびセキュリティプロセスが組み込まれています。

Cisco SD-WAN ソリューションは、古いハードウェアベースのモデルから、安全なソフトウェアベースの仮想 IP ファブリックにネットワークが進化したことを表しています。オーバーレイネットワークとも呼ばれる Cisco SD-WAN ファブリックは、パブリックインターネット、MPLS、ブロードバンドなどの標準ネットワークトランスポートサービス上で実行されるソフトウェアオーバーレイを形成します。オーバーレイネットワークは、次世代のソフトウェアサービスもサポートしているため、クラウドネットワーキングへの移行が促進されます。

従来のネットワーク設計における課題

ネットワーク設計に対する従来のアプローチでは、次の4つの根本的原因により、現代のニーズに合わせて拡張できません。

- コスト：従来のネットワークはルータやスイッチなどの高価なハードウェア上で動作し、時間のかかる設定とメンテナンスが必要です。さらに、これらのネットワークでは、ネッ

Cisco SD-WAN ソリューション

トワークを保護してセグメント化するために、高価なトランスポート接続またはキャリア回線が必要です。

- 複雑性：従来のネットワークは古いモデルの分散型コントロールプレーンで動作します。つまり、ネットワーク内のすべてのノードにルーティングとセキュリティルールを設定する必要があります。リモートサイトの管理、変更管理、およびネットワークのメンテナンスは、ロジスティクス上の主要な課題となっています。
- 設置に長い時間がかかる：専用のキャリア回線で動作する従来のネットワークでは、新しい回線の設置がキャリアに依存しており、数ヵ月かかる場合があります。これにより、新しいブランチの立ち上げが大幅に遅れる可能性があります。
- 制御：キャリア回線で動作する従来のネットワークは、ネットワーク設計から設定、監視に至るまで、ISP に対する制御を犠牲にしています。ISP から変更を要求すると、余分な時間がかかり、通信エラーが発生しやすくなります。

次のような現代の要件に直面すると、従来のネットワークのコストと複雑性はさらに高まります。

- 徹底したエンドツーエンドのセキュリティ
- 個別のトランスポート ネットワーク
- 複数のデータセンターでホストされる高帯域幅のクラウドアプリケーション
- モバイルエンドユーザーの人数の継続的な増加
- 流体トポロジ経由の Any-to-Any 接続
- 特定のビジネスに固有のニーズ

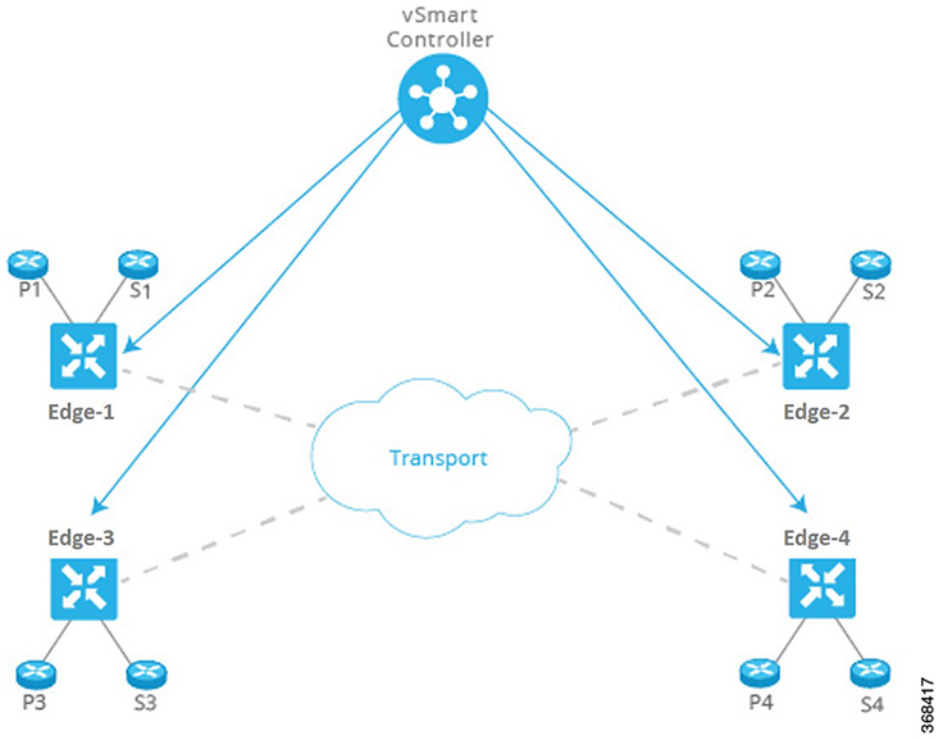
Cisco SD-WAN ソリューション

Cisco SD-WAN ソリューションは、ソフトウェア定義型 WAN（SD-WAN）です。すべての SD-WAN と同様に、1990 年代と 2000 年代にインターネットの拡張を可能にしたものと同じルーティング原則に基づいています。Cisco SD-WAN が他の SD-WAN と異なる点は、WAN を新世代のエンタープライズネットワークに合わせて再解釈し、データプレーンをコントロールプレーンから分離し、それまでは専用ハードウェアを必要としていたルーティングの多くを仮想化したことです。

仮想化されたネットワークは、物理ルータまたは仮想デバイスのいずれであっても、費用対効果の高いハードウェアのオーバーレイとして動作します。Cisco vSmart コントローラと呼ばれる集中型コントローラは、Cisco SD-WAN ファブリックのコントロールプレーンを監視し、Cisco SD-WAN オーバーレイネットワーク全体のプロビジョニング、メンテナンス、セキュリティを効率的に管理します。Cisco vBond オーケストレーション と呼ばれる別のデバイスは、Cisco SD-WAN オーバーレイネットワークに参加するときに、他のすべての Cisco vEdge デバイスs を自動的に認証します。

Cisco SD-WAN ソリューション

図 *1 : Cisco SD-WAN* ソリューションのコンポーネント



この分業により、ネットワークレイヤーはそれぞれが最も得意とすることに集中できます。コントロールプレーンはオーバーレイネットワークを介したトラフィックのルーティングルールを管理し、データプレーンは実際のデータパケットをネットワークデバイスに渡します。コントロールプレーンとデータプレーンは、柔軟で堅牢なファブリックの縦糸と横糸となり、ニーズとスケジュールに従って、既存の回路に織り込むことができます。

Cisco vManage は、オーバーレイネットワーク内のすべてのデバイスのネットワークパフォーマンスを集中監視ステーションから監視するための、シンプルでありながら強力なグラフィカルダッシュボードのセットを提供します。また、Cisco vManage では、ソフトウェアのインストール、アップグレード、プロビジョニングも一元化され、単一のデバイスでも複数のデバイスでも一括で処理できます。

Cisco SD-WAN はクラウドネットワーキングのニーズに最適です。Cisco SD-WAN 仮想 IP ファブリックは、クラウドネットワーキングを合理化および最適化するソフトウェアサービスをサポートし、個々のクラウドアプリケーションのオーバーレイネットワークの機能を最大限に活用できるようにします。

（注）

- Cisco SD-WAN コントローラは専用のカスタムスタックです。オープンソースの Linux コンポーネントが使用されていますが、当社のカスタム オペレーティング システム スタックは、使用されているオープンソースの Linux コンポーネントとは類似していません。Linux コンポーネントは、それらが使用されるカスタム オペレーティング システム スタックと同じ強化要件の対象ではありません。
- Cisco SD-WAN コントローラではルートアクセスが無効になっており、ユーザースペースからアクセスできません。
- 当社はFedRAMP、FIPS、CCなどのコンプライアンス基準と要件を満たしています。このコンプライアンスは、当社のオペレーティングシステムのセキュリティ検証の証拠であると見なされます。
- 当社はこちらで概説されている安全な開発ライフサイクルに準拠しています。
- また、Cisco Product Security Incident Response Team（PSIRT）によって実行される明確に定義されたプロセスに従って、CVEなどの新しいエクスプロイトや攻撃に対処しています。
- Cisco SD-WAN コントローラのプラットフォームのセキュリティについて引き続き懸念がある場合は、サードパーティを通じて、独立したペネトレーションテストを実施することをお勧めします。

仮想 IP ファブリック

従来のエンタープライズ ネットワークの複雑さは、次の 3 つの主な原因に起因します。

- データトラフィックを交換するエンティティと、それらのエンティティを結合するトランスポートネットワークの間に明確な区別はありません。つまり、ネットワークのサービス側にあるホスト、デバイス、サーバー間、およびネットワークのトランスポート側にあるルータ間の相互接続は明確に区別されていません。
- ポリシーと制御の判断は、エンタープライズネットワーク全体のすべてのホップに組み込まれています。
- セキュリティは時間のかかる手動の作業であり、ネットワーク内のすべてのノードで、または集中型セキュリティサーバーを使用してセキュリティサーバーを管理することによって、セキュリティ管理を実装する必要があります。

Cisco SD-WAN は、実績のあるネットワーク要素を革新的な方法で使用して、安全な仮想 IP ファブリックを構築します。ネットワーク要素には次のものが含まれます。

- ルーティングおよびルーティングアドバタイズメントを使用して、ネットワーク全体のトラフィックフローを確立および維持します。
- レイヤ 3 セグメンテーション（仮想ルーティングおよび転送（VRF）と呼ばれることもある）はトラフィックのさまざまなフローを分離します。これは、企業内のさまざまなお客様やビジネス組織のトラフィックを分離するのに役立ちます。

- プロトコルエンティティのペア間の双方向接続を設定および維持するためのピア ツーピアの概念
- 認証および暗号化
- ルーティングとデータトラフィックのポリシー

Cisco SD-WAN 仮想 IP ファブリックでは、5 つの簡単なステップで、複雑な従来のネットワークが管理しやすいスケーラブルなネットワークに変換されます。

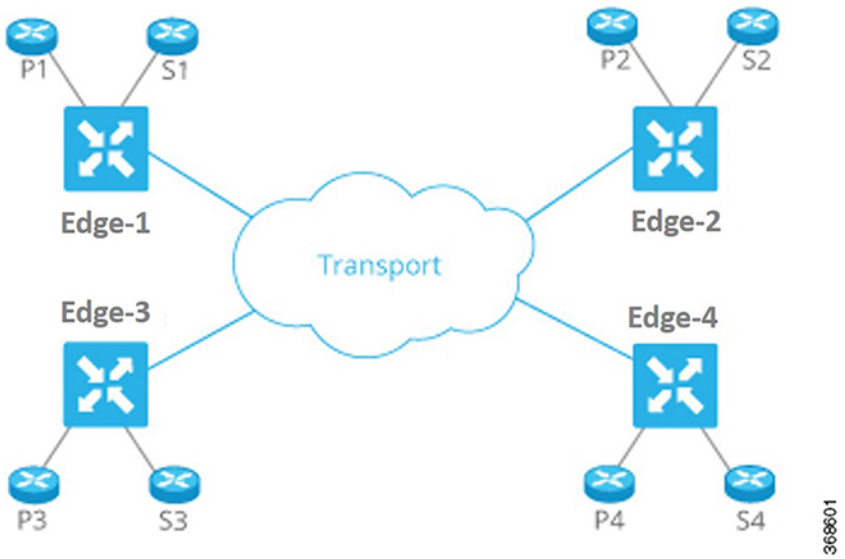
- ステップ 1：ネットワークのサービス側からトランスポートを分離する
- ステップ 2：ルーティング インテリジェンスを一元化し、セグメンテーションを有効にする
- ステップ 3：ネットワークを自動的に保護する
- ステップ 4：一元化されたポリシーを通じて到達可能性に影響を与える
- ステップ 5：オーケストレーションとプロビジョニングを簡素化する

ステップ 1：ネットワークのサービス側からトランスポートを分離する

トランスポートネットワークの役割は、トランスポートルータ間でパケットを運ぶことです。トランスポートネットワークは、次のホップまたは宛先ルータに到達するために通過するルートのみ認識している必要があります。非トランスポートルータ（ローカル サービス ネットワーク内のトランスポートルータの背後にあるルータ）のプレフィックスを認識する必要はありません。

ネットワークトランスポートをネットワークのサービス側から分離することにより、ネットワーク管理者は、ユーザー間またはホスト間の通信とは無関係に、ルータ間通信に影響を与えることができます。

図 *2:* サービスネットワークから分離された転送ネットワーク



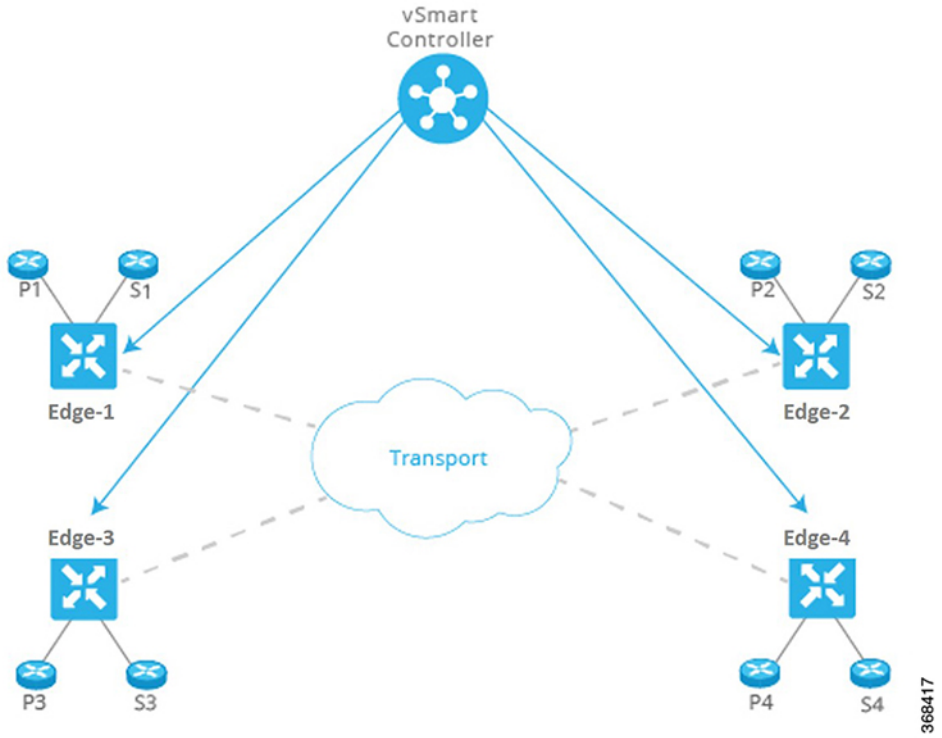
このアプローチには多くの利点があります。

- ネットワーク管理者は、SLA とコストに基づいてトランスポート回線を選択できます。
- ルーティングシステムは、最適なルーティング、ロードバランシング、およびポリシーベースのルーティングのために、属性をトランスポートリンクに割り当てることができます。

ステップ 2：ルーティング インテリジェンスを一元化し、セグメンテーションを有効にする

ネットワークのエッジにあるすべてのルータには、ルーティング用の 2 つの側があります。1 つはトランスポートネットワーク向けで、もう 1 つはネットワークのサービス側です。すべてのルータ間で Any-to-Any 通信を行うには、すべてのルータがすべてのプレフィックスを学習する必要があります。伝統的に、ルータは、フルメッシュ IGP/BGP を使用するか、オーバーレイトンネルでルーティングを有効にすることで、プレフィックスを学習します（MPLS または GRE を介した BGP または IGP など）。BGP にルートリフレクタを使用するなど、さまざまな手法により、フルメッシュルーティング隣接関係に関連する拡張性の問題を軽減または排除できます。

図 *3*: 集中型コントローラによるルーティング インテリジェンスの集中化



Cisco SD-WAN ファブリックは、ルーティング インテリジェンスを一元化することにより、ルートリフレクタモデルに基づいて構築されます。基本的に、ルータのサービス側から学習したプレフィックスはすべて中央のコントローラにアドバタイズされてから、ネットワークのコントロールプレーンを介して他のルータに情報が反映されます。コントローラはデータトラフィックを一切処理しません。データトラフィックはコントロールプレーン通信にのみ関係します。

このアプローチには多くの利点があります。

- 集中型コントローラは、コントロールプレーンの処理に安価なサーバーや市販のサーバーを使用できます。
- ルータには既成のシリコンを使用できるため、規模の経済によるコストメリットを得られます。
- ネットワークのトランスポート側でのフルメッシュルーティングに関連する拡張性の問題が解消されます。
- ネットワーク管理者は、複雑なシグナリングプロトコルを使用せずに、複数のセグメントを作成できます。たとえば、この図では、すべての Px プレフィックスを 1 つの VPN の一部にし、すべての Sx プレフィックスを別の VPN の一部にできます。

（注） 集中型コントローラは、ルータのルーティングにのみ「影響」を与えます。コントローラは、ネットワークを通過するすべてのフローに参加したり、サービス側のルーティングに参加したりしません。この設計により、ルータはローカルインテリジェンス（ローカルサイトの決定を迅速に行うのに十分なインテリジェンス）を得ることができます。

ステップ 3：ネットワークとリンクを自動的に保護する

Cisco SD-WAN ファブリックは、トランスポート側のリンクを識別し、サイト間のトラフィックを自動的に暗号化します。関連付けられた暗号化キーは、集中型コントローラとのセキュアなセッションを介して交換されます。コントローラとのセキュアなセッションは、RSA と証明書インフラストラクチャを使用して自動的に設定されます。

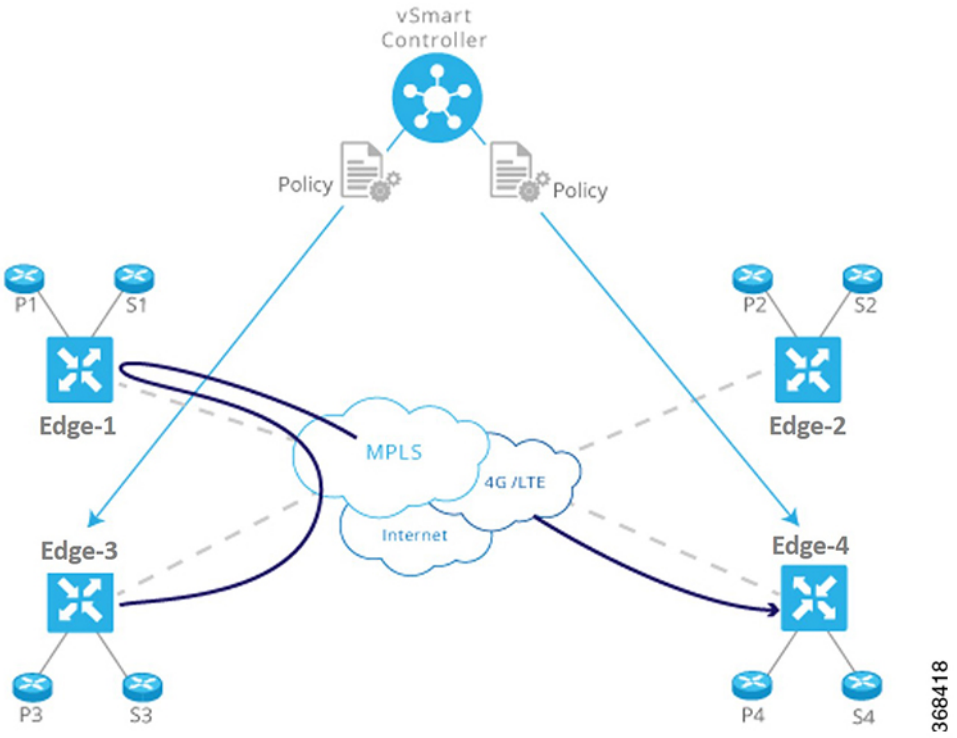
このアプローチには多くの利点があります。

- Cisco SD-WAN ファブリック自体が、ネットワークに参加しているすべてのデバイスを認証します。これは、インフラストラクチャを保護するための重要なステップです。
- ファブリックは、トランスポートリンクに関連する暗号化キーを自動的に交換するため、多数のペアワイズキーを設定する必要がなくなります。
- ファブリックにより、ネットワークはトランスポート側からの攻撃を受けにくくなります。

ステップ 4：一元化されたポリシーを通じて到達可能性に影響を与える

集中型コントローラに設定されたポリシーは、ルータ間でプレフィックスがアドバタイズされる方法に大きく影響します。たとえば、この図のルータ P3 と P4 間のすべてのトラフィックがルータ vEdge-1 で U ターンする必要がある場合、ネットワーク管理者は集中型コントローラに単純なルートポリシーを適用できます。その後、コントローラが影響を受けるエッジルータにポリシーを渡します。ネットワーク管理者は、ルータごとにポリシーをプロビジョニングする必要はありません。

図 *4*：集中型コントローラで設定されたポリシー



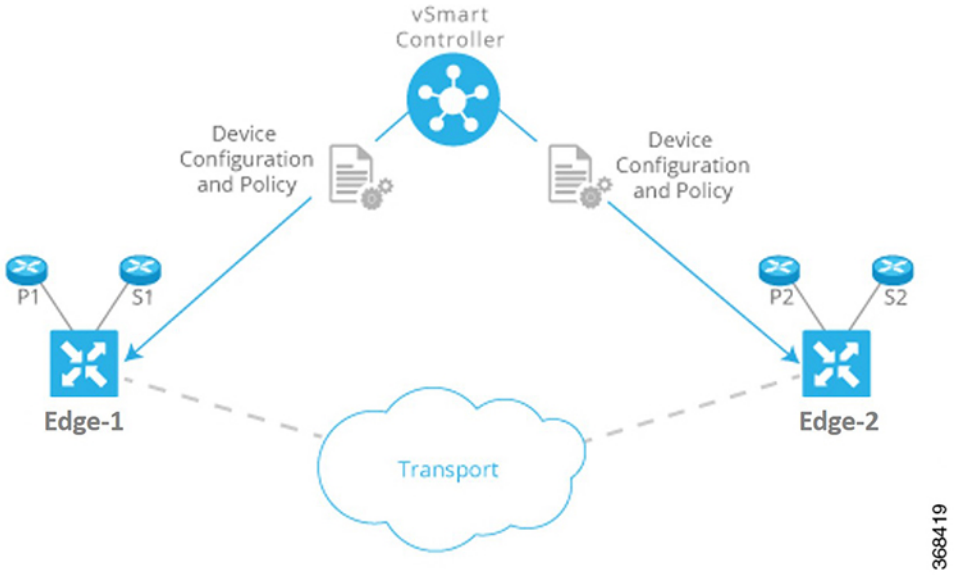
このアプローチには多くの利点があります。

- コントローラは、アクセス制御、つまり、VPN内で相互に通信できるプレフィックスに集中的に影響を与えます。
- コントローラは、SLAまたはその他の属性に基づいてトランスポートリンクの選択に影響を与えることにより、ユーザーエクスペリエンスを最適化します。ネットワーク管理者は、トランスポートリンクに色（ゴールドやブロンズなど）を付け、アプリケーションがその色を適切なトランスポートリンクにマッピングするようにできます。
- ネットワーク管理者は、一元化されたポイントからビジネスロジックをマッピングできます。
- ネットワークは、リスクの高い国からのトラフィックをすべて中間地点を経由してルーティングするなど、計画的または予期しない状況に迅速に対応できます。
- ネットワークは、ファイアウォール、IDP、IDS などのサービスを一元化できます。ネットワーク管理者は、これらのサービスをすべてのブランチやキャンパスのネットワーク全体に分散させる代わりに、機能を一元化して、規模の効率性を達成し、プロビジョニングのタッチポイント数を最小限に抑えることができます。

ステップ 5：プロビジョニングと管理を簡素化する

従来のネットワークデバイスは、CLI を介して手動でプロビジョニングおよび監視されます。ネットワーク管理者は、ステータス情報を取得して読み取るために、構成を 1 行ずつ入力し、個々のデバイスで一度に 1 つずつ操作コマンドを入力する必要があります。この方法は、ネットワークのプロビジョニングとトラブルシューティングの際にエラーが発生しやすく、時間がかかります。また、デバイスが遠隔地にある場合や管理ポートにアクセスできない場合は、深刻な問題が発生する可能性があります。

図 *5 : Cisco SD-WAN* によるネットワークの簡素化されたプロビジョニングと管理



Cisco SD-WAN は、Cisco vManage を介して、プロビジョニングと管理を一元化して大幅に簡素化します。Cisco vManage は、オーバーレイネットワーク内のすべての Cisco vEdge デバイスとリンクを監視、設定、および維持できる使いやすいグラフィカルダッシュボードを提供します。たとえば、GUI ダッシュボードには、サービスのプロビジョニングを容易にするさまざまな構成のテンプレートビューが用意されているため、すべての一般的な要素（AAA サーバーや企業固有のサーバーなど）を 1 回のクリックで複数のデバイスに 1 か所からプッシュできます。

このアプローチには多くの利点があります。

- ネットワーク管理者は、個々のデバイスを一度に 1 つずつ処理する断片的なアプローチとは対照的に、ネットワーク全体を効率的かつ簡単にプロビジョニングおよび管理できます。
- ネットワーク管理者は、 1 か所からネットワークの可視性（ネットワーク全体の VPN 統計の表示など）を改善できます。
- トラブルシューティングタスクは簡素化され、視覚的に表示されます。ネットワーク管理者は、個々のデバイスから長い構成や出力を読み取る必要がありません。

Cisco SD-WAN のコンポーネント (Components)

Cisco SD-WAN の主要コンポーネント

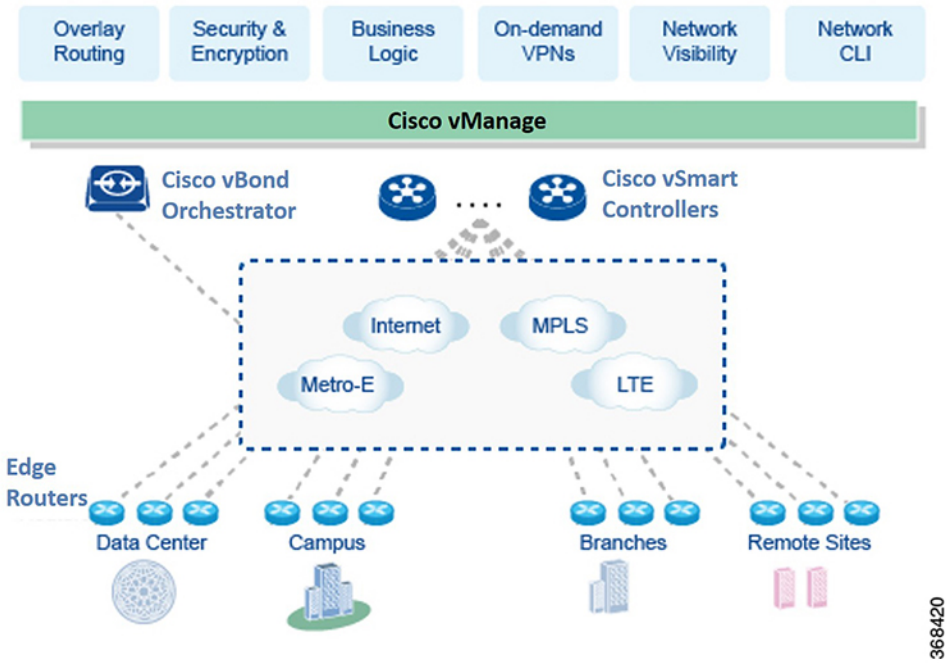
Cisco SD-WAN のセキュアな仮想 IP ファブリックは、次の 4 つの基本的なコンポーネントで構成されています。

- **Cisco vManage**：Cisco vManage は、シンプルなグラフィカルダッシュボードからオーバーレイネットワーク全体の設定と管理を可能にする中央集中型のネットワーク管理システムです。
- **Cisco vSmart コントローラ**：Cisco vSmart コントローラ は Cisco SD-WAN ソリューションの中心的な要素であり、ネットワーク全体のデータ トラフィックの流れを制御します。Cisco vSmart コントローラ は Cisco vBond オーケストレーション と連携して、Cisco vEdge デバイスがネットワークに参加するときに認証し、エッジルータ間の接続を調整します。
- **Cisco vBond オーケストレーション**：Cisco vBond オーケストレーション は、エッジルータと Cisco vSmart コントローラ の間の接続を自動的に調整します。任意のエッジルータまたは Cisco vSmart コントローラ コントローラが NAT の背後にある場合、Cisco vBond オーケストレーション は最初の NAT トラバーサル オーケストレータとしても機能します。
- **Cisco IOS XE SD-WAN および Cisco vEdge デバイス**：エッジルータはサイトの境界（リモートオフィス、ブランチ、キャンパス、データセンターなど）に配置され、サイト間の接続を提供します。これらは、ハードウェアデバイスまたは仮想マシンとして実行されるソフトウェア（クラウドルータ）のいずれかです。エッジルータは、データトラフィックの送信を処理します。

これら 4 つのコンポーネントのうち、エッジルータは Cisco SD-WAN ハードウェアデバイスまたは仮想マシンとして実行されるソフトウェアであり、残りの 3 つのコンポーネントはソフトウェアのみのコンポーネントです。クラウドルータ、Cisco vManage および Cisco vSmart コントローラ ソフトウェアはサーバー上で実行され、Cisco vBond オーケストレーション ソフトウェアはエッジルータ上でプロセス（デーモン）として実行されます。

下の図は、Cisco SD-WAN のコンポーネントを示しています。以下のセクションでは、各コンポーネントについて詳しく説明します。

図 *6 : Cisco SD-WAN* のコンポーネント



Cisco vManage

Cisco vManage は集中ネットワーク管理システムです。Cisco vManage ダッシュボードは、ネットワークへの視覚的なウィンドウを提供し、Cisco エッジネットワークデバイスを設定および管理できます。Cisco vManage ソフトウェアは、ネットワーク内のサーバー上で実行されます。このサーバーは通常、データセンターなどの一元化された場所にあります。Cisco vManage ソフトウェアは、Cisco vSmart コントローラ ソフトウェアと同じ物理サーバー上で実行できます。

Cisco vManage を使用すると、証明書のクレデンシャルを保存したり、すべての Cisco エッジネットワーク コンポーネントの設定を作成および保存したりできます。これらのコンポーネントがネットワークでオンラインになると、Cisco vManage から証明書と設定を要求します。Cisco vManage がこれらの要求を受信すると、証明書と設定を Cisco エッジネットワーク デバイスにプッシュします。

クラウドルータの場合、Cisco vManage は証明書に署名してブートストラップ設定を生成することもでき、デバイスをデコミッションすることもできます。

Cisco vSmart Controller

Cisco vSmart コントローラは、Cisco SD-WAN オーバーレイネットワークのコントロールプレーンを監視し、Cisco SD-WAN ファブリックを形成する接続を確立、調整、および維持します。

Cisco vSmart コントローラ の主要なコンポーネントは次のとおりです。

- コントロールプレーン接続：それぞれの Cisco vSmart コントローラ がオーバーレイネットワーク内の各エッジルータとのコントロールプレーン接続を確立および維持します（複数

の Cisco vSmart コントローラ があるネットワークでは、ロードバランシングのために、単一の Cisco vSmart コントローラ がエッジルータのサブセットのみに接続している場合があります）。DTLS トンネルとして実行される各接続は、デバイス認証が成功した後に確立され、Cisco vSmart コントローラ とエッジルータの間で暗号化されたペイロードを伝送します。このペイロードは、Cisco vSmart コントローラ がネットワークトポロジを決定し、ネットワークの宛先への最適なルートを計算し、このルート情報をエッジルータに配布するために必要なルート情報で構成されます。Cisco vSmart コントローラ とエッジルータ間の DTLS 接続は、永続的な接続です。Cisco vSmart コントローラ には、サービス側でエッジルータが接続されているデバイスとの直接のピアリング関係はありません。

- OMP（オーバーレイ管理プロトコル）：OMP プロトコルは、Cisco SD-WAN オーバーレイネットワークを管理する BGP に似たルーティングプロトコルです。OMP は DTLS コントロールプレーン接続内で実行され、オーバーレイネットワークの確立と維持に必要なルート、ネクストホップ、キー、およびポリシー情報を伝送します。OMP は Cisco vSmart コントローラ とエッジルータの間で実行され、コントロールプレーン情報のみを伝送します。Cisco vSmart コントローラ はルートを処理し、これらのルートから学習した到達可能性情報をオーバーレイネットワーク内の他のエッジルータにアドバタイズします。
- 認証：Cisco vSmart コントローラ には、オンラインになったすべての新しいエッジルータを認証できるクレデンシャルが事前にインストールされています。これらのクレデンシャルにより、認証されたデバイスのみがネットワークにアクセスできるようになります。
- キーリフレクションとキー再生成：Cisco vSmart コントローラ は、エッジルータからデータプレーンキーを受信し、データプレーンのトラフィックを送信する必要がある他の関連するエッジルータにそれらを反映します。
- ポリシーエンジン：Cisco vSmart コントローラ は、ルーティング情報、アクセス制御、セグメンテーション、エクストラネット、およびサービスチェイニングを操作するための豊富なインバウンド/アウトバウンドポリシー構成を提供します。
- Netconf と CLI：Netconf は、Cisco vSmart コントローラ をプロビジョニングするために Cisco vManage によって使用される標準ベースのプロトコルです。さらに、各 Cisco vSmart コントローラ がローカル CLI アクセスと AAA を提供します。

Cisco vSmart コントローラ は、エッジルータおよび Cisco SD-WAN オーバーレイネットワーク内の他の Cisco vSmart コントローラ から学習した OMP ルートと呼ばれるルート情報を格納する、集中型ルートテーブルを維持します。Cisco vSmart コントローラ は、設定されたポリシーに基づいて、このルート情報をネットワーク内の Cisco エッジネットワークデバイスと共有して、相互に通信できるようにします。

Cisco vSmart コントローラ は、ESXi または VMware ハイパーバイザソフトウェアで設定されたサーバー上で仮想マシンとして実行されるソフトウェアです。vSmart ソフトウェアイメージは、Cisco SD-WAN Web サイトからダウンロード可能な署名付きイメージです。すべての vSmart ソフトウェアイメージには、単一の Root of Trust（信頼の基点）となる Cisco SD-WAN 公開証明書が埋め込まれています。

Cisco vSmart コントローラ の初回起動時に、コントローラと Cisco vBond オーケストレーション の IP アドレスなどの最小限の設定情報を入力します。Cisco vSmart コントローラ は、この情報と信頼の基点のパブリック証明書を使用して、ネットワーク上で自身を認証し、Cisco

vBond オーケストレーション との DTLS 制御接続を確立し、ドメインに存在する場合は完全な設定を Cisco vManage から受信してアクティブ化します（または、設定ファイルを手動でダウンロードするか、コンソール接続を介して Cisco vSmart コントローラ で直接設定を作成できます）。これで、Cisco vSmart コントローラ でもドメイン内のエッジルータからの接続を受け入れる準備ができました。

冗長性と高可用性を提供するために、一般的なオーバーレイネットワークには、各ドメインに複数の Cisco vSmart コントローラ が含まれています。ドメインには最大 20 の Cisco vSmart コントローラ を含めることができます。OMP ネットワークルートの同期を維持するには、すべての Cisco vSmart コントローラ でポリシーと OMP の設定を同じにする必要があります。ただし、インターフェイスの場所とアドレス、システム ID、ホスト名など、デバイス固有の情報の設定は異なっていても構いません。冗長な Cisco vSmart コントローラ を持つネットワークでは、Cisco vBond オーケストレーション は Cisco vSmart コントローラ にお互いについての情報を伝え、ドメイン内のどのエッジルータからの制御接続を受け入れる必要があるかをそれぞれの Cisco vSmart コントローラ に伝えます（ロードバランシングを提供するために、同じドメイン内の異なるエッジルータは、異なる Cisco vSmart コントローラ に接続します）。1 つの Cisco vSmart コントローラ が使用できなくなった場合、他のコントローラがオーバーレイネットワークの機能を自動的かつ即座に維持します。

Cisco vBond Orchestrator

Cisco vBond オーケストレーション は、Cisco vSmart コントローラ とエッジルータの初期起動を自動的に調整し、Cisco vSmart コントローラ とエッジルータ間の接続を容易にします。立ち上げプロセス中に、Cisco vBond オーケストレーション はオーバーレイネットワークへの参加を希望するデバイスを認証および検証します。この自動オーケストレーション プロセスにより、面倒でエラーが発生しやすい手動での起動を行う必要がなくなります。

Cisco vBond オーケストレーション は、パブリックアドレス空間にある唯一の Cisco vEdge デバイス です。この設計により、Cisco vBond オーケストレーション は Cisco vSmart コントローラ および NAT デバイスの背後にあるエッジルータと通信でき、Cisco vBond オーケストレーション はこれらの Cisco vEdge デバイス の NAT トラバーサルの問題を解決できます。

Cisco vBond オーケストレーション の主要なコンポーネントは次のとおりです。

- コントロールプレーン接続：それぞれの Cisco vBond オーケストレーション に、ドメイン内のそれぞれの Cisco vSmart コントローラ との DTLS トンネル形式の永続的なコントロールプレーン接続があります。さらに、Cisco vBond オーケストレーション は DTLS 接続を使用して、エッジルータがオンラインになったときにそれらと通信し、ルータを認証し、ルータがネットワークに参加できるようにします。エッジルータの基本認証は、証明書と RSA 暗号化を使用して行われます。
- NAT トラバーサル：Cisco vBond オーケストレーション は、エッジルータと Cisco vSmart コントローラ の一方または両方が NAT デバイスの背後にある場合に、それらの間の最初のオーケストレーションを促進します。このオーケストレーションを促進するために、標準のピアツーピア技術が使用されます。
- ロードバランシング：Cisco vSmart コントローラ が複数あるドメインでは、ルータがオンラインになると、Cisco vBond オーケストレーション は Cisco vSmart コントローラ を介してエッジルータのロードバランシングを自動的に実行します。

Cisco vBond オーケストレーションは、オーバーレイネットワーク内の Cisco vSmart コントローラ とエッジルータを認証し、それらの間の接続を調整するソフトウェアモジュールです。ネットワーク内のすべての Cisco vEdge デバイス が接続できるように、パブリック IP アドレスが必要です（パブリックアドレスが必要な Cisco vEdge デバイス はこれだけです）。

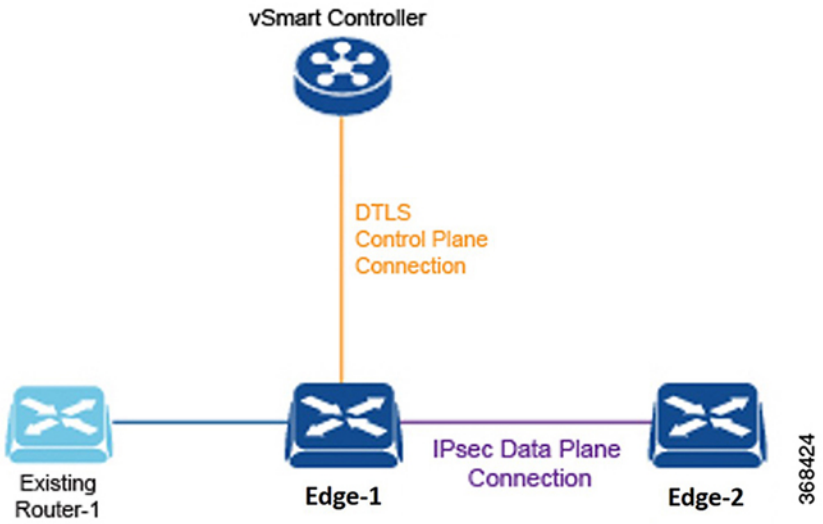
Cisco vBond オーケストレーション は、Cisco vSmart コントローラ とエッジルータ間の初期制御接続のオーケストレーションを行います。Cisco vSmart コントローラ およびエッジルータへの DTLS トンネルを作成して、コントロールプレーン接続を要求している各ノードを認証します。この認証動作により、有効な顧客ノードのみが Cisco SD-WAN オーバーレイネットワークに参加できることが保証されます。Cisco vSmart コントローラ との DTLS 接続は永続的であるため、エッジルータがネットワークに参加すると vBond コントローラは Cisco vSmart コントローラ に通知できます。エッジルータとの DTLS 接続は一時的なものであるため、Cisco vBond オーケストレーション がエッジルータを Cisco vSmart コントローラ と一致させた後は、Cisco vBond オーケストレーション とエッジルータが相互に通信する必要はなくなります。Cisco vBond オーケストレーションは、コントロールプレーン接続に必要な情報のみを共有し、適切なエッジルータと Cisco vSmart コントローラ に対して、相互に安全な接続を開始するように指示します。Cisco vBond オーケストレーション では状態は保持されません。

Cisco vBond オーケストレーション に冗長性を提供するために、ネットワークに複数の vBond エンティティを作成し、すべてのエッジルータをそれらの Cisco vBond オーケストレーション に向けることができます。それぞれの Cisco vBond オーケストレーション は、ネットワーク内のそれぞれの Cisco vSmart コントローラ と永続的な DTLS 接続を維持します。1 つの Cisco vBond オーケストレーションが使用できなくなった場合、他のネットワークは自動的および即座にオーバーレイネットワークの機能を維持できます。複数の Cisco vSmart コントローラ があるドメインでは、Cisco vBond オーケストレーション はエッジルータと Cisco vSmart コントローラ のいずれかをペアにして、ロードバランシングを提供します。

Cisco IOS XE SD-WAN および Cisco vEdge デバイス

エッジルータは、ハードウェアデバイスであるかソフトウェアデバイスであるかにかかわらず、ネットワークを介して送信されるデータトラフィックを処理します。エッジルータを既存のネットワークに配置すると、標準ルータとして表示されます。

図 7: 既存のネットワークに配置されたエッジルータ



これを説明するため、ここに示す図では、標準のイーサネットインターフェイスによって接続されたエッジルータと既存のルータを示しています。これら 2 つのルータは互いにレイヤ 3 エンドポイントのように見え、2 つのデバイス間でルーティングが必要な場合は、インターフェイス上で OSPF または BGP を有効にすることができます。このインターフェイスでは、VLAN タギング、QoS、ACL、ルートポリシーなどの標準ルータ機能も使用できます。

エッジルータのコンポーネントは次のとおりです。

- DTLS コントロールプレーン接続：各エッジルータには、通信する各 Cisco vSmart コントローラ に対して 1 つの永続的な DTLS 接続があります。この永続的な 接続は、デバイス認証が成功した後に確立され、エッジルータと Cisco vSmart コントローラ の間で暗号化されたペイロードを伝送します。このペイロードは、Cisco vSmart コントローラ がネットワークトポロジを決定し、ネットワークの宛先への最適なルートを計算し、このルート情報をエッジルータに配布するために必要なルート情報で構成されます。
- OMP（オーバーレイ管理プロトコル）：Cisco vSmart コントローラ で説明したように、OMP は DTLS 接続内で実行され、オーバーレイネットワークを確立および維持するために必要なルート、ネクストホップ、キー、およびポリシー情報を伝送します。OMP はエッジルータと Cisco vSmart コントローラ の間で実行され、制御情報のみを伝送します。
- プロトコル：エッジルータは、OSPF、BGP、VRRP、BFD などの標準プロトコルをサポートしています。
- ルーティング情報ベース（RIB）：各エッジルータには、直接インターフェイスルート、静的ルート、および BGP および OSPF を介して学習した動的ルートが自動的に入力される複数のルートテーブルがあります。ルートポリシーは、どのルートが RIB に保存されるかに影響を与える可能性があります。
- 転送情報ベース（FIB）：これは、エッジルータの CPU がパケットを転送するために使用する RIB の抽出バージョンです。

- Netconf と CLI：Netconf は、Cisco vManage がエッジルータのプロビジョニングのために使用する標準ベースのプロトコルです。さらに、各エッジルータはローカル CLI アクセスと AAA を提供します。
- キー管理：エッジルータは、標準の IPsec プロトコルを使用して、他のエッジルータとの安全な通信に使用される対称キーを生成します。
- データプレーン：エッジルータは、IP 転送、IPsec、BFD、QoS、ACL、ミラーリング、ポリシーベースの転送など、データプレーン機能の豊富なセットを提供します。

エッジルータには、ルーティング、高可用性（HA）、インターフェイス、ARP 管理、ACL などに関するサイトローカルの決定を行うためのローカルインテリジェンスがあります。Cisco vSmart コントローラとの OMP セッションは、エッジルータの RIB に影響を与え、オーバーレイネットワークの構築に必要なサイトローカルでないルートと到達可能性情報を提供します。

ハードウェアエッジルータには、ルータの秘密キーと公開キー、および署名付き証明書を含む安全な暗号プロセッサであるトラステッドボード ID チップが含まれています。このすべての情報がデバイス認証に使用されます。エッジルータの初回起動時に、エッジルータと Cisco vBond オーケストレーションの IP アドレスなどの最小限の設定情報を入力します。エッジルータは、この情報とトラステッドボード ID チップの情報を使用して、ネットワーク上で自身を認証し、ドメイン内の Cisco vSmart コントローラとの DTLS 接続を確立し、ドメインに存在する場合は完全な設定を Cisco vManage から受信してアクティブ化します。それ以外の場合は、設定ファイルを手動でダウンロードするか、コンソール接続を介してエッジルータ上で直接設定を作成できます。

Cisco SD-WAN ソリューション

クラウドネットワーキングを合理化および最適化するために、Cisco SD-WAN はセキュアな仮想 IP ファブリック上で実行される次世代のソフトウェアサービスを提供します。

- **Cloud onRamp for SaaS**：Cloud onRamp for SaaS は、サービスとしてのソフトウェア（SaaS）クラウドアプリケーションのパフォーマンスを最適化します。個々のアプリケーションのパフォーマンスを明確に可視化し、それぞれに最適なパスを自動的に選択します。Cloud onRamp は、アプリケーションごとにカスタマイズされた式を使用して、損失と遅延に関するメトリックを計算します。
- [Cisco vAnalytics]：Cisco vAnalytics は、ソリューションの一部として Cisco SD-WAN によってホストされる SaaS サービスです。オーバーレイネットワーク全体のパフォーマンスを経時的にグラフィカルに表示し、特定の時間における単一のキャリア、トンネル、またはアプリケーションの特性にドリルダウンできます。
- **Cisco SD-WAN セルフサービスポータル**：Cisco SD-WAN セルフサービスポータル は、Cisco SD-WAN に適したクラウドインフラストラクチャ自動化ツールであり、パブリッククラウドプロバイダーで Cisco SD-WAN コントローラをプロビジョニング、モニター、および保守するための迅速な方法を提供します。

Cloud onRamp for SaaS

企業は、Microsoft Office365、Salesforce、Dropbox などのビジネスクリティカルな SaaS アプリケーションを採用しています。企業は、次の 3 つの主要な方法を使用して、ユーザーに SaaS アプリケーションへの接続を提供します。

• 支社からのダイレクト インターネット アクセス（DIA）。

• 地域施設のゲートウェイを介したインターネットアクセス。

• キャリア ニュートラル ファシリティ（CNF）のゲートウェイを介したクラウドエクスチェンジまたは直接接続。

遅延とパケット損失は、アプリケーションのパフォーマンスとエンド ユーザー エクスペリエンスに直接影響しますが、多くの場合、ネットワーク管理者は、エンドユーザーと SaaS アプリケーション間のネットワークのパフォーマンス特性を限定的に認識できる、またはまったく認識できません。パスの障害が発生し、アプリケーションのパフォーマンスが低下した場合、トラフィックをプライマリパスから代替パスに移行するには、通常、ネットワーク管理者が、複雑で時間がかかり、エラーが発生しやすい一連の手順を手作業で実行する必要があります。

Cisco SD-WAN Cloud onRamp for SaaS は、ネットワークのパフォーマンス特性の可視性と継続的な監視を提供します。最適なユーザーエクスペリエンスを実現するために、エンドユーザーと SaaS アプリケーションの間で最高のパフォーマンスを発揮するパスを選択することで、リアルタイムの意思決定を行います。劣化したネットワークパスのアプリケーショントラフィックをインテリジェントに再ルーティングして、ネットワークパフォーマンスの変化に自動的に対応します。

Cloud onRamp for SaaS は、DIA、地域施設を介したインターネットアクセス、CNF を介したアクセスなど、クラウドベースの SaaS アプリケーションのすべてのアクセス方法をサポートします。

Cloud onRamp for SaaS は、エンタープライズ クラウド アプリケーションの Viptela Quality of Experience（vQoE）と呼ばれるアプリケーションのパフォーマンス値を計算します。vQoE 値は、アプリケーションごとにカスタマイズされた式を使用して、損失と遅延を比較検討します。たとえば、電子メールアプリケーションはビデオアプリケーションよりも遅延の許容度が高く、ビデオアプリケーションは電子メールよりも損失の許容度が高くなります。vQoE 値の範囲は 0 から 10 で、0 が最低品質、10 が最高品質です。

マウスを数回クリックするだけで Cisco vManage で Cloud onRamp for SaaS を有効にできます。その後 Cisco vManage の Cloud onRamp ダッシュボードにアクセスして、個々のアプリケーションのパフォーマンスを継続的に可視化します。

Cisco vAnalytics

Cisco vAnalytics は、アプリケーションとネットワークのパフォーマンスの経時的な可視性を提供します。Cisco vAnalytics は、ソリューションの一部として Cisco SD-WAN によってホストされる SaaS サービスです。オーバーレイネットワーク全体をグラフィカルに表示し、ドリルダウンして特定の時間における単一のキャリア、トンネル、またはアプリケーションの特性を表示できます。

Cisco vAnalytics ダッシュボードでネットワークの概要をインタラクティブに確認し、そこからさらに詳しい情報を確認することができます。このダッシュボードにはデフォルトで過去 24 時間に集計された情報が表示されます。ドリルダウンすると、表示するデータセットごとに異なる期間を選択できます。ダッシュボードには、アプリケーションのパフォーマンス、WAN サイトの使用状況、およびキャリアの使用状況に関するデータが表示されます。

Cisco vAnalytics プラットフォームは、個々のアプリケーション用にカスタマイズされた QoE 値により、アプリケーションのパフォーマンスを計算します。この値の範囲は 0 から 10 で、0 が最低のパフォーマンス、10 が最高のパフォーマンスです。Cisco vAnalytics は、遅延、損失、およびジッターに基づいて QoE を計算し、アプリケーションごとに計算をカスタマイズします。

Cisco vAnalytics は長期間にわたってデータを保存し、過去の傾向情報を表示し、将来の計画に使用できる洞察を提供します。

次の構成が可能です。

- アプリケーションの可視性：
  - パフォーマンスが最高および最低のアプリケーション：パフォーマンスが最高および最低のアプリケーションを表示し、サイトレベルで詳細にドリルダウンします。
  - 最も帯域幅を消費するアプリケーション：最も帯域幅を消費するアプリケーションを表示し、サイトとユーザーにドリルダウンします。
- ネットワークの可視性：
  - ネットワークの可用性と回線の可用性：ネットワークの可用性を表示し、ネットワークと回線の可用性を関連付けます。
  - トンネルのパフォーマンス：さまざまな SD-WAN トンネルでの損失、遅延、ジッターなどの主要なパフォーマンス インジケーターを表示します。
  - キャリアの使用状況ビュー：プロバイダーとそのネットワーク特性を表示します。

Cisco SD-WAN セルフサービスポータル

Cisco SD-WAN セルフサービスポータル は、Cisco SD-WAN に適したクラウドインフラストラクチャ自動化ツールであり、パブリック クラウド プロバイダーで Cisco SD-WAN コントローラをプロビジョニング、モニター、および保守するための迅速な方法を提供します。

Cisco SD-WAN セルフサービスポータル を使用して、次のコントローラをプロビジョニングできます：

- Cisco vManage
- Cisco vBond オーケストレーション
- Cisco vSmart コントローラ

（注） Cisco vManage リリース 20.9.1 以降、Cisco SD-WAN セルフサービスポータル へのリンクが Cisco SD-WANメニューから追加されます。Cisco SD-WAN メニューから [SD-WAN Portal] をクリックして、Cisco SD-WAN コントローラのプロビジョニング、監視、および保守のために Cisco SD-WAN セルフサービスポータル にアクセスします。

Cisco SD-WANセルフサービスポータルの詳細については、*Cisco SD-WAN*セルフサービスポータル コンフィギュレーション ガイドを参照してください。

Cisco SD-WAN との連携

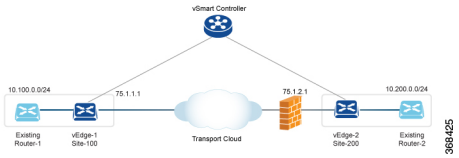
CiscovEdgeデバイスを使用した基本的なオーバーレイネットワークの構築

2 つの vEdge ルータと 1 つの Cisco vSmart コントローラ を含む単純なネットワーク設計を使用して、正常に機能するオーバーレイネットワークを Cisco vEdge コンポーネントから形成する方法を説明します。このトポロジでは、Cisco vBond オーケストレーション ソフトウェアが一方のvEdgeルータで有効になっています。単純なネットワークを理解できたら、より複雑なトポロジの設計と構築を開始できます。

単純なネットワークトポロジ

次の図に、単純なトポロジを示します。ここには、Site-100 と Site-200 の 2 つのサイトがあります。vEdge-1 は Site-100 のエッジデバイスであり、vEdge-2 は Site-200 のエッジデバイスです。各ローカルサイトで、vEdgeルータは標準のイーサネットインターフェイスを介して既存の従来型ルータに接続します。vEdge-2 は、ファイアウォール機能も備えたNATデバイスを介してトランスポートネットワークに接続されます。

図 *8:* 単純なネットワークトポロジ



この設計の目的は、プライベートネットワークを作成して、レイヤ 3 の観点から Router-1 と Router-2 を相互に隣接させ、これらの各ルータに接続されているホストがプライベートネットワークを介して通信できるようにすることです。

基本的なネットワークの構築

次の手順により、上記のトポロジに示されている単純なオーバーレイネットワークを作成できます。

- 手順 1：初期起動および基本構成を実行します。
- 手順 2：ホストまたはサービス側のインターフェイスとルーティングを有効にします。
- 手順 3：OMP を介したオーバーレイルーティングを有効にします。
- 手順 4：IPsec データプレーンの自動セットアップを確認します。
- 手順 5：ポリシーを適用します。

これらの手順について、もう少し詳しく説明します。

手順 1：初期起動および基本構成の実行

ネットワーク管理者の観点では、Cisco vEdge ネットワークコンポーネントの初期起動は、各ネットワークコンポーネントの構成を作成し、いくつかの重要な認証関連ファイルが適切に配置されていることを確認することを含む、簡単で単純なプロセスです。ユーザーの観点では、起動は、vEdge ルータの電源を入れ、ケーブルを差し込んでルータをネットワークに接続するだけです。起動の残りの部分は、ゼロタッチ プロビジョニング プロセスによって自動的に実行されます。

ネットワーク管理者は、初期起動の一部として次のタスクを実行します。

1. ネットワーク内のいずれかの vEdge ルータで Cisco vBond オーケストレーション 機能を設定します。この例では、これは vEdge-1 です。
2. 必要に応じて、トップレベルの Cisco vBond オーケストレーション を ZTP サーバーとして機能するように設定します。この状況では、DNS サーバーがエンタープライズ ネットワークに存在する必要があります。
3. DHCP サーバーがエンタープライズ ネットワークに存在することを確認します。
4. 署名付き証明書を Cisco vManage にインストールし、その証明書を Cisco vManage Orchestrator にダウンロードします。
5. Cisco vManage に vEdge ルータ認定シリアル番号ファイルをインストールし、それを Cisco vSmart コントローラ にダウンロードします。
6. Cisco vManage CLI から、オーバーレイネットワークの各 Cisco vSmart コントローラ および vEdge ルータの構成を作成します。
    1. 従来型ルータのルータ ID アドレスに似たシステム IP アドレスを設定します。この、デバイス上のどのインターフェイスにも依存しないアドレスにより、Cisco vEdge デバイスが識別されます。システム IP アドレスは、事前に割り当てられる必要があり、各 vEdge ルータと Cisco vSmart コントローラ の全体にわたって一意である必要があります。これらのアドレスは、ネットワーク経由でルーティング可能である必要はありません。
    2. オーバーレイネットワーク内のさまざまなサイトのサイト ID を設定します。この例では、vEdge-1 が Site-100、vEdge-2 が Site-200 にあります。Cisco vSmart コントローラ は、一つのサイトに併置することも、独自のサイトに配置することもできます。

3. ドメイン ID を設定します。これは、クラスタを作成するためのオプションの手順です。この例では、ドメイン ID を 1 として設定します。
4. vBond サーバーと Cisco vSmart コントローラ の IP アドレスまたは DNS 名を設定します。
5. vEdge-1 および vEdge-2 で WAN インターフェイスを設定します。VPN 0 は、WAN トランスポート インターフェイス用に予約された VPN です。IP アドレスは DHCP 経由で自動的に取得できます。また、デフォルトゲートウェイと DNS を明示的に設定することもできます。
6. デフォルトでは、WAN インターフェイスで DTLS と IPsec が有効になっています。
7. 設定を保存します。

Cisco vSmart コントローラ はネットワークに参加すると Cisco vBond オーケストレーション によって認証され、vEdge ルータはネットワークに参加すると Cisco vBond オーケストレーション と Cisco vSmart コントローラ の両方によって認証されます。その後、これらのデバイスが Cisco vManage に接続し、構成をダウンロードします。

vEdge-1 の構成例：

```
system
  host-name vEdge-1
  system-ip 1.0.0.1
  domain-id 1
  site-id   100
  vbond 75.1.1.1  local
!
vpn 0
  interface ge 0/0
    ip address 75.1.1.1/24
    tunnel-interface
      color default
    no shutdown
  ip route 0.0.0.0/0 75.1.1.254
!
```

この記事の残りのセクションでは、vEdge ルータおよび Cisco vSmart コントローラ で他の一般的な機能を設定する方法について説明します。通常、Cisco vManage で作成する構成において、すべての機能を一度に設定します。この構成は、オーバーレイネットワークに参加するときにデバイスにダウンロードされます。ただし、各種機能を詳しく説明するために、この記事では構成のさまざまな部分を個別に説明します。

手順 2：ホストまたはサービス側のインターフェイスとルーティングの有効化

Cisco vManage から、サービス側のインターフェイスと通常のルーティングを設定することもできます。

1. 既存の従来型ルータに向けて vEdge-1 のインターフェイスを設定します。IP アドレスを割り当て、そのインターフェイスをデフォルト以外の VPN に配置します。この例では、これは VPN 1 です。vEdge-2 で同じ手順を実行します。
2. 既存のルータに向けて vEdge ルータで OSPF または BGP を設定します。

3. コミットします。

ローカルサイトで標準の IP 到達可能性、ルート、およびネクストホップを確認するには、標準の **ping**、**traceroute**、およびさまざまな **show** コマンドを Cisco vManage で、またはデバイスの CLI から（デバイスに直接接続している場合）使用します。

ホストまたはサービス側の VPN の構成例：

```
vpn 1
  router
    ospf
      redistribute omp
      area 0
        interface ge 0/1
        exit
      exit
    !
  !
  interface ge 0/1
    ip address 10.1.2.12/24
    no shutdown
!
```

手順 3：OMP を介したオーバーレイルーティングの有効化

すべてのサイトローカルルートは、vEdgeルータに入力されます。これらのルートは他のvEdgeルータに配布されます。これは、Cisco vSmart コントローラ によって、OMP を介して実行されます。

1. BGP を使用しているか OSPF 外部 LSA がある場合は、OMP による BGP ルートの再配布を許可します。
2. OMP ルートを BGP または OSPF に再アドバタイズします。
3. コミットします。

OMP を介したオーバーレイルーティングの構成例：

```
omp
  advertise ospf external
!
```

この時点で、vEdge-1 は Site-200 からプレフィックスについて学習でき、vEdge-2 は Site-100 からプレフィックスについて学習できます。すべてのプレフィックスが VPN 1 の一部であるため、Site-100 と Site-200 のホストは相互に到達可能です。Cisco SD-WAN オーバーレイネットワークの観点では、vEdge-1 が、アドレス 10.100.0.0/24 とデフォルトの TLOC カラーで構成される vRoute（この例では {75.1.1.1, default } と記述）を Cisco vSmart コントローラ にアドバタイズするため、この到達可能性が実現されます。つづいて、Cisco vSmart コントローラ がこの vRoute を vEdge-2 にアドバタイズします。同じプロセスが vEdge-2 でプレフィックス 10.200.0.0/24 によって発生します。

手順 4：IPsec データプレーンの自動セットアップの確認

vEdge ルータのすべての TLOC について、vEdge ルータが暗号化用の対称キーをアドバタイズします。Cisco vSmart コントローラ は、このキーを自動的に反映し、対称キーを使用して TLOC

をアドバタイズします。その結果、双方向のIPsec SAがセットアップされ（つまり、各方向に異なるキーが存在します）、データトラフィックは自動的にこの IPsec トンネルの使用を開始します。トンネルが稼働状態になると、そのトンネルで BFD が自動的に開始されます。これは、トランスポートネットワークで障害が発生した場合にデータプレーンの高速コンバージェンスを確保するために行われます。

IPsec データプレーンのセットアップは自動的に実行されます。コンフィギュレーションは必要ありません。複数の show コマンドを使用して、SA と、IPsec トンネルの状態を確認できます。

手順 5：ポリシーの適用

オプションの手順として、Cisco vSmart コントローラ でコントロールプレーンポリシーとデータプレーンポリシーを作成し、それらをvEdgeルータにプッシュすることができます。たとえば、ネットワーク管理者が { vEdge-2, prefix 10.200.0.0/24 } 宛てのトラフィックを vEdge-3 などの別のサイトに転送するポリシーを適用する場合は、Cisco vSmart コントローラ でコントロール プレーン ポリシーを作成し、それぞれの vEdge ルータにプッシュすることができます。構成自体ではなくポリシーの結果が vEdge ルータにプッシュされます。

ポリシーの構成例：

```
policy
  lists
    site-list site-100
      site-id 100
    !
    prefix-list my-prefixes
      ip-prefix 10.200.0.0/24
    !
  control-policy TE-thru-vedge3
    sequence 10
      match route
        prefix-list my-prefixes
      !
      action accept
        set
          tloc 1.0.0.3 color default
        !
      !
      default action accept
    !
apply-policy
  site-list site-100
    control-policy TE-thru-vedge3 out
  !
!
```

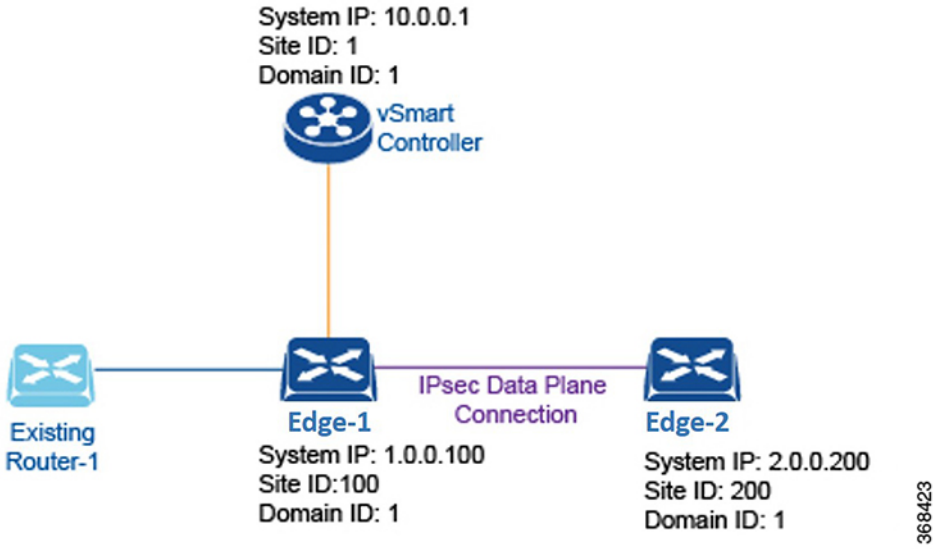
Advanced Options

基本的なルーティング、セキュリティ、およびポリシーを確認したので、ネットワークへの他のさまざまな要素の追加を開始できます。[Software] カテゴリを調べて、高可用性、コンバージェンス、BFD、QoS、ACL、セグメンテーション、高度なポリシーなどの要素を追加することをお勧めします。

Cisco SD-WAN に関する用語

次の図は、Cisco SD-WAN オーバーレイネットワークの説明に使用される用語をまとめたものです。

図 *9 : Cisco SD-WAN* オーバーレイネットワークで使用される用語



ドメイン ID

ドメインは、Cisco vSmart コントローラ の制御範囲を区切る、エッジルータと Cisco vSmart コントローラ の論理グループです。各ドメインは、ドメイン ID と呼ばれる一意の整数によって識別されます。現時点では、Cisco SD-WAN オーバーレイネットワークで設定できるドメインは 1 つだけです。

ドメイン内では、エッジルータは、独自のドメイン内の Cisco vSmart コントローラ にのみ接続できます。Cisco vBond オーケストレーション は、どの Cisco vSmart コントローラ がどのドメインにあるのかを認識しているため、新しいエッジルータが起動したときに、Cisco vBond オーケストレーション はそれらのルータを適切なドメインの Cisco vSmart コントローラ に向けることができます。ただし、Cisco vBond オーケストレーション はドメインのメンバーにはなりません。

ドメイン内では、Cisco vSmart コントローラ とエッジルータの間にルーティング情報の完全な同期があり、ルート集約および要約の範囲が存在します。組織は、ネットワークをドメインに分割して、必要なビジネス目的に合致させることができます。たとえば、ドメインを大きな地理的領域またはデータセンターに対応させ、各データセンターとそれが担当する分散拠点が単一のドメインに含まれるようにすることができます。

OMP ルート

Cisco vSmart コントローラ およびエッジルータでは、OMP はローカルサイトから学習したルートとサービスを、対応するトランスポートロケーションマッピング（「トランスポートロケー

ション」（TLOC）と呼ばれる）とともにピアにアドバタイズします。これらのルートは、標準の IP ルートと区別するために「OMP ルート」と呼ばれます。Cisco vSmart コントローラは、この OMP ルートを介して、ネットワークトポロジと使用可能なサービスを学習します。

Cisco SD-WAN コントロール プレーン アーキテクチャは、次の 3 種類の OMP ルートを使用します。

- OMP ルート：OMP 編成のトランスポートネットワークを使用するエンドポイント間の到達可能性を確立するプレフィックス。OMP ルートは、中央データセンターのサービス、ブランチオフィスのサービス、またはオーバーレイネットワークの任意の場所にあるホストやその他のエンドポイントの集合を表すことができます。OMP ルートは、機能転送のために TLOC を必要とし、TLOC に解決されます。BGP と比較すると、OMP ルートは、いずれかの BGP AFI/SAFI フィールドで伝送されるプレフィックスと同等です。
- TLOC：OMP ルートを物理ロケーションに関連付ける識別子。TLOC は、基盤となるネットワークから認識できる OMP ルーティングドメインの唯一のエンティティであり、基盤となるネットワークのルーティングを介して到達できる必要があります。TLOC は、物理ネットワークのルーティングテーブル内のエントリを介して直接到達できるか、または NAT デバイスの外部に存在するプレフィックスによって表され、ルーティングテーブルに含まれている必要があります。BGP と比較すると、TLOC は OMP ルートのネクストホップとして機能します。
- サービスルート：OMP ルートをネットワーク内のサービスに関連付ける識別子であり、ネットワーク内のサービスの場所を指定します。サービスには、ファイアウォール、侵入検知システム（IDP）、およびロードバランサが含まれます。

サイト ID

サイトは、分散拠点、データセンター、キャンパスなど、Cisco SD-WAN オーバーレイネットワーク内にある特定の物理的な場所です。各サイトは、サイト ID と呼ばれる一意の整数によって識別されます。サイトの各 Cisco vEdge デバイスは、同じサイト ID で識別されます。そのため、データセンター内では、すべての Cisco vSmart コントローラおよびエッジルータが同じサイト ID で設定されます。通常、分散拠点またはローカルサイトには単一のエッジルータがありますが、冗長性のために 2 つ目のルータが存在する場合は、両方のルータが同じサイト ID で設定されます。

システム IP アドレス

各エッジルータおよび Cisco vSmart コントローラ にはシステム IP アドレスが割り当てられ、インターフェイスアドレスとは独立して物理システムが識別されます。このアドレスは、通常のルータのルータ ID に似ています。システム IP アドレスは、エッジルータと Cisco vSmart コントローラ の永続的なネットワーク オーバーレイ アドレスを提供し、必要に応じて、Cisco vEdge デバイスの到達可能性に影響を与えることなく、物理インターフェイスの番号付けを変更することを可能にします。システム IP アドレスは、IPv4 アドレスと同様に、ドットで区切られた 4 つの部分からなる 10 進表記で記述します。

TLOC

TLOC（トランスポートロケーション）は、エッジルータが WAN トランスポートネットワークまたは NAT ゲートウェイに接続する物理インターフェイスを識別します。TLOC はいくつかのプロパティで識別されますが、主要なものは {IP-address, color} タプルとして記述できる IP アドレス/カラーペアです。このタプルでは、IP アドレスはシステム IP アドレスであり、カラーは VPN または VPN 内のトラフィックフローを識別する固定のテキスト文字列です。OMP は TLOC ルートを使用して TLOC をアドバタイズします。

その他の情報

Cisco SD-WAN オーバーレイネットワークの要素の説明については、「Components of the Cisco SD-WAN Solution」を参照してください。Cisco SD-WAN ソフトウェアおよびハードウェアを使用してオーバーレイネットワークを構築する方法については、「Constructing a Basic Network Using Cisco SD-WAN Components」を参照してください。オーバーレイネットワークのコンポーネントの機能例については、「Validated Examples」を参照してください。

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。