Cisco SD-WAN

クラウド スケール アーキテクチャ

Cisco SD-WAN

クラウド スケール アーキテクチャ

はじめに

作成者

本書は、カリフォルニア州サンノゼにあるシスコ本社で 1 週間にわたって実施された集中セッションにおいて、テクニカル マーケティング、プロダクト マネジメント、セールス、カスタマー エクスペリエンス、エンジニアリング、マーケティングの諸チームが取り組んだコラボレーションの成果物です。

- テクニカル マーケティング エンジニア、Aaron Rohyans
- テクニカル ソリューション アーキテクト、Ali Shaikh
- テクニカル マーケティング エンジニア、Chandra Balaji Rajaram
- テクニカル マーケティング マネージャ、David Klebanov
- テクニカル マーケティング エンジニア、Deepesh Kumar
- テクニカル マーケティング エンジニア、Gina Cornett
- テクニカル マーケティング エンジニア、Hasham Malik
- マーケティング マネージャ、Kiran Ghodgaonkar
- プロダクト マネージャ、Madhavan Arunachalam
- テクニカル マーケティング エンジニア、Nikolai Pitaev
- プロダクト マネージャ、Travis Carlson
- シニア テクニカル リーダー、Zaheer Aziz

謝辞

本書の作成に際し、シスコ エンタープライズ ネットワーキング事業部の支援に対し深く感謝します。

また、拡張チーム メンバーの Sehjung Hah、Rohan Grover、Sukruth Srikantha、Misbah Rehman 諸氏にも、この取り組みへのサポートに対し、感謝の意を表します。Christina Munoz 氏の卓越したリソース調整と多大なる貢献に対し、感謝の意を表します。あわせて、Book Sprints（*www.booksprints.net*）チームにも心より感謝申し上げます。

- Faith Bosworth（ファシリテータ）
- Henrik van Leeuwen および Lennart Wolfert（イラストレータ）
- Agathe Baëz（書籍プロデューサ）
- Raewyn Whyte、Susan Tearne（校正）

対象者

2017 年に、シスコは、SD-WAN のリーダーとして広く認識されていた Viptela® を買収しました。本書は、ワイド エリア ネットワークの日常的な運用に携わり、Viptela を搭載した Cisco SD-WAN をすでに導入している、または評価している情報技術の専門家を対象としています。

本書では、ワイド エリア ネットワークの設計とアーキテクチャに関与するネットワーク エンジニア、マネージャ、またはアーキテクトに、Viptela を搭載した Cisco SD-WAN の多くの機能と、ワイド エリア ネットワークの導入および管理中に発生する可能性がある一般的なユース ケースについて概説します。

本書は、設計または導入ガイドとして作成されているものではありません。Cisco SD-WAN の詳細情報については、付録の「*関連資料*」のセクションを参照してください。

本書の構成

本書では、ワイド エリア ネットワークを含む一般的なビジネス上の問題を解決するために、ユース ケースに基づくアプローチを採用しています。Cisco SD-WAN アーキテクチャについて説明し、ビジネス ニーズに対応するユース ケースと、Cisco SD-WAN がそれらをどのように解決するかについて説明します。また、実際のお客様の導入環境でのユース ケースを示す例と導入事例によって補完します。各章には主な要点と参照が追加されており、詳細を調べることができます。

概要

なぜ SD-WAN なのか

企業はデジタル変革を採り入れ、テクノロジーを迅速に導入して、生産性の向上、コストの削減、カスタマー エクスペリエンスの変革を実現しています。

ワイド エリア ネットワーク（WAN）の従来の役割は、ブランチまたはキャンパスのユーザをデータセンター内のサーバでホストされているアプリケーションに接続することでした。専用の MPLS 回線を使用して、セキュリティと信頼性の高い接続を確保しました。これは、アプリケーションがデータセンターからクラウドに移行しているデジタル世界ではもはや機能しません。また、それらのアプリケーションを利用するユーザは多様なデバイスを使用して、ますますモバイル化されています。

複数のクラウドにわたって Software as a Service（SaaS）や Infrastructure as a Service（IaaS）を導入する企業が増えているため、IT 部門はビジネスクリティカルなアプリケーションにとって満足のいくエクスペリエンスを提供することに苦労しています。従来の WAN ネットワークは、クラウド接続を提供するためにデータセンター インフラストラクチャに大きく依存していますが、これにより、遅延が増大し、データセンター負荷が大きくなり、単一障害点が発生するという非効率性が生じています。帯域幅の要求が急増しているため、ネットワークキャパシティに大きな負荷がかかり、組織はプライベート WAN 回線を継続的にアップグレードすることを余儀なくされています。ある組織はインターネット回線に注意を向けています。一般のインターネット回線は通常、はるかに低価格で非常に高いキャパシティを提供します。しかし、組織はビジネスクリティカルな接続の実行可能な手段としてインターネットを運用化することに苦慮していて、非効率的なアクティブ/スタンバイ アプローチを用いています。

企業をインターネットに晒すことにより、インターネット アクセスがデータセンターで保護されていたときには経験しなかった脅威とコンプライアンスの問題が発生する可能性があります。従業員からパートナー、請負業者、ベンダー、ゲストまで、さまざまなレベルのアクセス範囲のワークフォースがアプリケーションにアクセスする場合、企業の重要な資産を保護することは非常に困難です。WAN でブロードバンドを有効にすると、セキュリティ要件はさらに深刻になり、ユーザ エクスペリエンス、セキュリティ、複雑性のバランスを取る点での IT の課題が生じます。

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。従来のネットワーキング ソリューションでは同一プラットフォーム上にデータプレーン、コントロール プレーンおよびマネジメント プレーンが統合されていることと比較すると、SDN はコントロール プレーンおよびマネジメント プレーンからフォワーディング プレーンを分離し、ネットワーク インテリジェンスの一元化を可能にします。これにより、ネットワークの自動化、運用やプロビジョニング、モニタリング、トラブルシューティングのさらなる簡素化が可能になります。SD-WAN は、このような SDN の原理を WAN に当てはめたものです。

そこで、なぜ SD-WAN なのかという問題が残ります。SDN の原理は WAN の課題をどのように解決するのでしょうか。この質問に答えるために、車での旅行を例として考えましょう。GPS が普及する前は、インディアナポリスからダラスへ車で旅行する場合、最適なルートを特定するためにロードマップが使用されていました。ルートに沿って移動中に事故や遅延が発生した場合、ドライバは限定的な情報に基づいて代替ルートを見つけることを余儀なくされました。

WAN ルータはかつてこのように運用されていました。各ルータは、トラフィックを転送する方法について、その周囲の世界の限定されたビューに基づいて、独自の自律的な意思決定を行います。多くの場合、これらの決定はダウンストリームの中断を認識していませんでした。今日、GPS が車の旅行を変革したのと同様に、SD-WAN は WAN アーキテクチャを変革しています。SD-WAN を使用することで、エッジ ルータは、トラフィックを転送する方法と場所に関して、「上空からの俯瞰」に頼ることができるようになりました。GPS は人が道路の建設、事故、運行の遅延、非効率なルートを回避するのに役立つのに対し、SD-WAN はブランチ ルータがネットワーク内の損失、遅延、ジッターを回避するのに役立ちます。

Cisco SD-WAN とは

ベネフィット

SD-WAN が 5 年以上前に初めて市場に投入されたとき、価値提案は次の 4 つの重要な要件に基づいていました。

- アイドル状態のバックアップ リンクのアクティベーションとダイナミック ロードバランシングにより、帯域幅を拡大
- ブランチでダイレクト インターネット アクセスを実行できるようにすることで、クラウド アクセスの高速化を実現
- クラウドベースのものも一元管理することで、運用コストと管理コストを削減
- MPLS の代替として安価なインターネットまたは LTE 接続を使用することで、WAN コストを削減

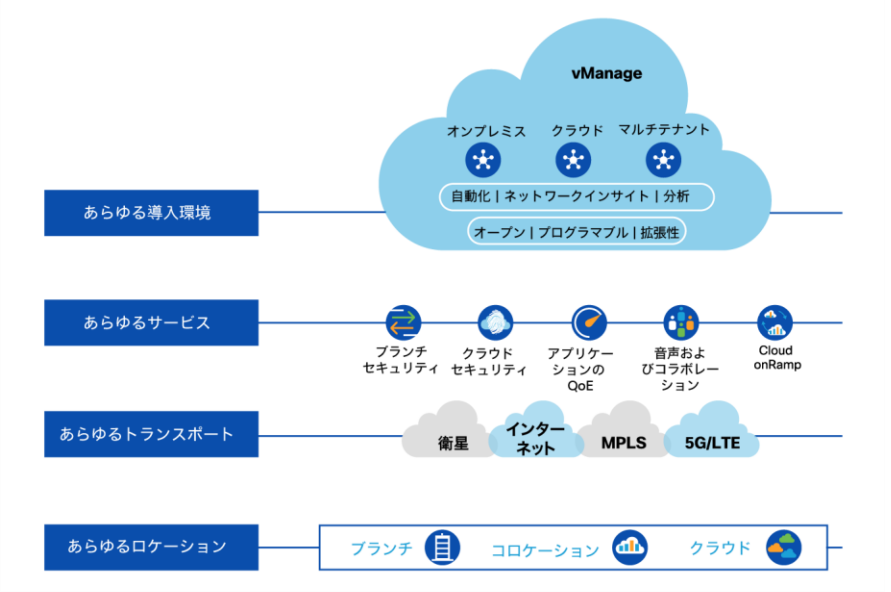
デジタル ビジネスは進化し、今日のオフィス環境、従業員が働くロケーションはますます分散しています。また、データセンターからマルチクラウド環境に移行することで、それらの従業員が使用するアプリケーションもまた分散化が進みつつあります。これらが組み合わさり、クラウド アプリケーションにアクセスするユーザ、デバイス、ロケーションの数が増えていくことで、IT における複雑さは圧倒的なものになります。これらの課題に対処するには、IT 部門は以前の SD-WAN ソリューションが提供する基本的な機能を超えた、より高度な WAN のユース ケースを検討する必要があります。

Cisco SD-WAN は、次の 3 つの主要な領域を通じて、今日のワイド エリア ネットワークの複雑なニーズを満たすように設計された、クラウドスケール アーキテクチャです。

- ビジネス アプリケーション戦略の進化に伴って、予測可能なアプリケーション エクスペリエンスを実現する高度なアプリケーション最適化

- オンプレミスでもクラウドでも、適切な場所に適切なセキュリティを導入できる柔軟性を提供する、マルチレイヤ セキュリティ
- ユーザからアプリケーションへのエンドツーエンドのポリシーを数千拠点で実現する、エンタープライズ規模でのシンプルさ

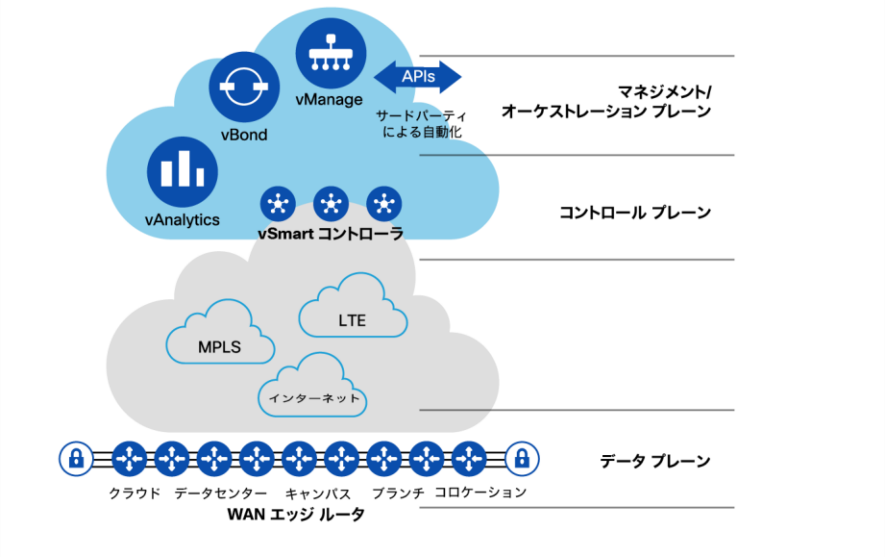
図　Cisco SD-WAN クラウドスケール アーキテクチャ



コンポーネントとアーキテクチャ

Cisco SD-WAN ソリューションは、ソフトウェア定義型ネットワーキング（SDN）の原理を WAN に拡張する、クラウド提供型のワイド エリア ネットワーク（WAN）オーバーレイ アーキテクチャです。このソリューションは、データ、コントロール、マネジメント、オーケストレーションの 4 つのプレーンに分割されます。

図　　WAN に SDN の原理を適用する



Cisco SD-WAN ソリューションは、アーキテクチャ上の各プレーンを担う 4 つの主要コンポーネントで構成されてます。

Cisco vManage

マネジメントプレーンにおいては、Cisco vManage が本ソリューションにおけるユーザ インターフェイス部分を担います。ネットワーク管理者および運用担当者は、設定、プロビジョニング、トラブルシューティング、およびモニタリングの各アクティビティをここで実行します。vManage には、シングルテナント ダッシュボードとマルチテナント ダッシュボードがあり、顧客企業やサービス プロバイダーのさまざまな導入環境に対応します。

Cisco vBond

Cisco vBond はオーケストレーション プレーンを担います。vBond コントローラは、ゼロタッチ プロビジョニング のプロセスと、最初の認証、コントロール/マネジメント情報の配信、およびネットワーク アドレス変換 (NAT) トラバーサルの円滑化を主に担当します。ルータが未設定の状態で初めて起動すると、vBond がそのルータを SD-WAN ファブリックにオンボーディングします。ネットワークの構造を理解し、その情報を他のコンポーネント間で共有することは、vBond の役割です。

Cisco vSmart

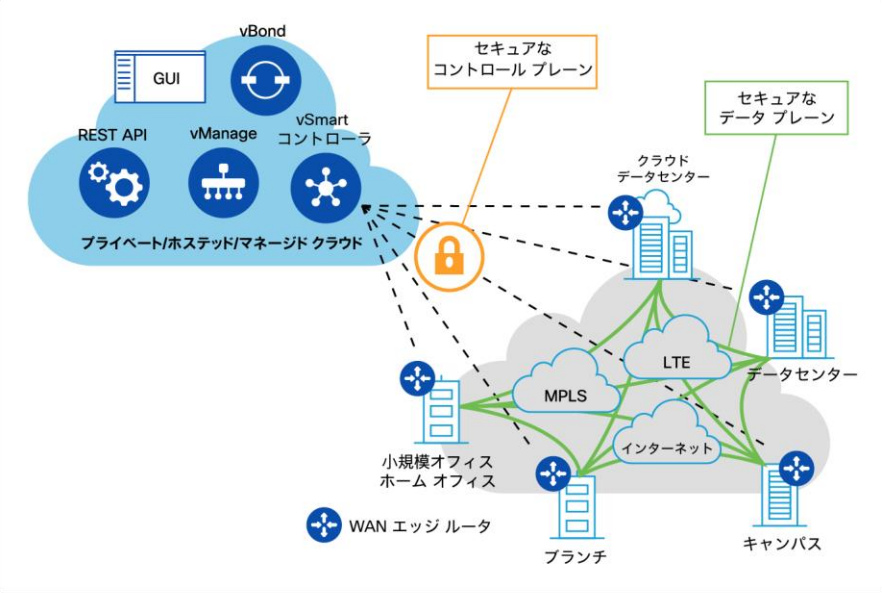
Cisco vSmart は、本ソリューションの「ブレイン」となる部分であり、コントロールプレーンに相当します。vSmart は、vManage で作成されたポリシーの一元的な適用を担当するコンポーネントです。ブランチ拠点が接続されると、それらのルーティング情報は vSmart コントローラと交換され、他のブランチ拠点間では直接交換されません。ポリシーを適用することで、ルーティング情報が影響を受け、他のロケーションと共有されます。それにより、個々のブランチが相互に通信する方法が決定されます。vSmart コントローラは、ブランチ拠点からオーバーレイ マネジメント プロトコル (OMP) 経由でルートを受信すると、これらのルートに対して vManage で作成されたポリシーを呼び出し、トラフィックが SD-WAN ファブリックを通過する方法を制御します。

Cisco WAN エッジ ルータ

Cisco WAN エッジ ルータは、ネットワーク ファブリックの確立とトラフィックの転送を担当します。Cisco WAN エッジ ルータにはハードウェア アプライアンスおよび仮想アプライアンスがあり、各拠点の接続性やスループット、および機能要件に応じて複数のモデルから選択します。

これらすべてのコンポーネントが組み合わされて、Cisco SD-WAN ファブリックが形成されます。次の図に、各コンポーネントの関係を表します。

図　Cisco SD-WAN ファブリック コンポーネント



WAN エッジ ルータは相互に IPSecトンネルを張り、SD-WAN オーバーレイを構成します。さらに、WAN エッジ ルータとコントローラ間では、コントロール チャネルが確立されます。このコントロール チャネルを通じて、各WAN エッジ ルータは、設定、プロビジョニング、およびルーティング情報を受信します。データ プレーン トラフィックがコントローラ側に転送されないことに注意してください。

オーバーレイ マネジメント プロトコル（OMP）

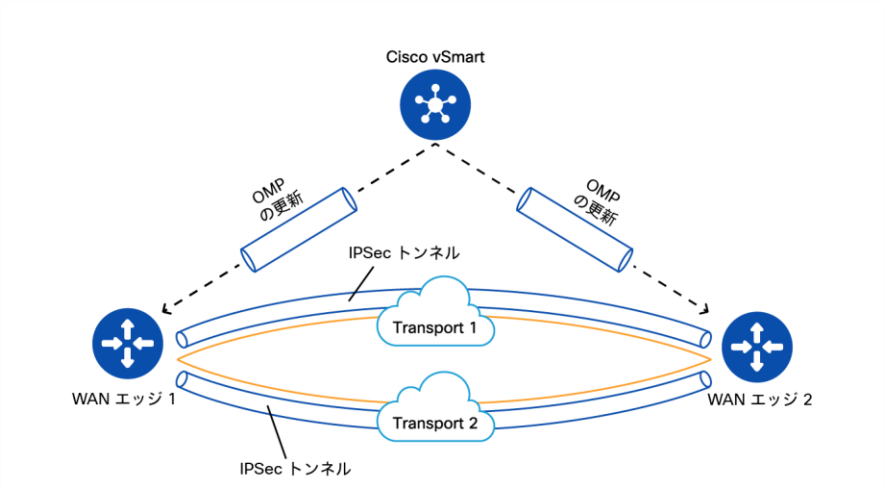
Cisco SD-WAN は、OMP を用いてオーバーレイ ネットワークを管理します。OMP は vSmart コントローラと WAN エッジ ルータ間で動作するプロトコルです。ここでは、ルート プレフィックス、ネクストホップ ルート、暗号キー、ポリシー情報などのコントロール プレーン情報がセキュアな接続を介して交換されます。ポリシーが定義されていない場合、OMP のデフォルト動作ではオーバーレイ ネットワークはフル メッシュ トポロジとなります。そうすると、各 WAN エッジ ルータは他の WAN エッジ ルータに直接接続できます。OMP は、次の 3 つのタイプのルートをアドバタイズします。

1. OMP ルート：ローカル サイトで学習されるサービス サイドのプレフィックス（Connected、Static、OSPF、BGP）です。プレフィックスは OMP に再配布され、オーバーレイ上を伝送されます。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、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ーされます。

2. TLOC ルート：トランスポート ネットワークに接続する WAN エッジ ルータ上の論理的なトンネル エンドポイントです。TLOC ルートは、システム IP アドレス、リンクのカラー（color）、カプセル化の 3 つのタプルによって一意に識別され、表されます。

3. サービス ルート：WAN エッジの拠点 LAN 側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 チェイニングに使用できます。またこのサービス ルートには VPN 情報も含まれています。VPN ラベルはサービス ルートを用いて送信され、どの VPN がどのリモート サイトに属するのかを vSmart コントローラに通知します。サービス チェイニングの詳細については、本書の「*コロケーションの利用*」の章を参照してください。

図　OMP



Bi-directional Forwarding Detection（BFD）

WAN エッジ ルータは、BFD メカニズムを用いて、トランスポート リンクのパフォーマンスをプローブし測定します。また、BFD プローブの結果に基づいて最適なパフォーマンスのパスを決定し、すべてのトランスポート リンクの遅延、ジッター、損失に関する情報を提供します。

高可用性と冗長性

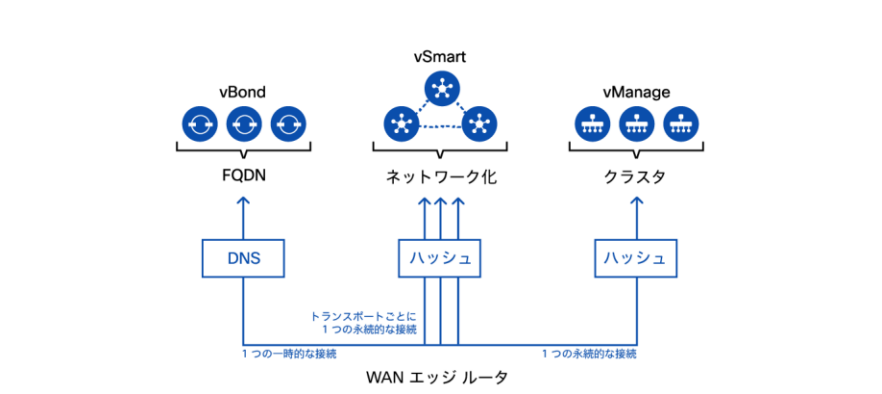
Cisco SD-WAN ソリューションは、アプリケーションの可用性とパフォーマンスを最大化することを念頭に設計されています。高可用性とは、ネットワーク サービスが障害に対して十分な復元力を備えていることを意味します。Cisco SD-WAN における高可用性は、次の 3 つの中核的な要素を組み合わせて実現しています。

- **デバイスの冗長性**：これは、デバイスを冗長してインストールしプロビジョニングすること、およびハードウェア内でコンポーネントを冗長化することからなります。これらのデバイスは、アクティブ/アクティブで動作するセキュアなコントロール プレーンによって接続されます。
- **堅牢なネットワーク設計**：複数のプロトコル（VRRP、BGP、OSPF など）と、LAN と WAN の両方のセグメントへの冗長物理接続をサポートします。
- **ソフトウェア メカニズム**：ソフトウェア メカニズムにより、直接的および間接的な障害から迅速にリカバリできます。復元力のあるコントロール プレーンを提供するために、本ソリューションではネットワーク内のすべての WAN エッジ ルータのステータスを定期的にモニタし、ルータがネットワークに参加したり離れたりする際に、トポロジの変更に合わせて自動的に調整します。データ プレーンの復元力を実現するために、Cisco SD-WAN ソフトウェアは、WAN エッジ ルータ間のセキュアな IPsec トンネル上で動作する標準プロトコル メカニズム（具体的には BFD）を実装します。

コントロール プレーンの冗長性

オーケストレーション レベルの冗長性は、異なる vBond コントローラに紐づく複数の IP アドレスに対して 1 つの DNS 名 (FQDN) が付けられることによって実現されます。コントロール プレーンの冗長性は、複数の vSmart コントローラで実装されています。1 つの WAN エッジ ルータが 1 つのハッシュを作成し、これを用いてデフォルトで 2 つの冗長 vSmart コントローラに接続します。ネットワーク管理システムの冗長性は、複数の vManage インスタンスを使用してクラスタを構築することで実現できます。

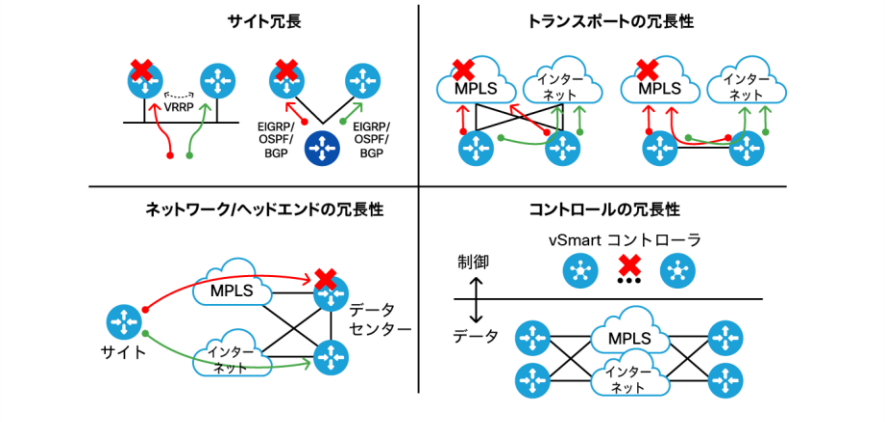
図　　コントロール プレーンの冗長性



データ プレーンの冗長性

データ プレーンの冗長性は、複数のレベルで実現されます。これはサイトの冗長性から始まりますが、この場合は LAN 側のクライアントが Virtual Router Redundancy Protocol（VRRP）や、BGP、OSPF、EIGRP などのルーティング プロトコルを確実に使用できることを確認します。TLOC Extension などの機能は、2 つの冗長 WAN エッジ ルータ間のクロス リンクを使用することにより、トランスポートの冗長性を構築するのに役立ちます。ネットワーク レベルの冗長性は、複数のデータセンターを地理的に分散させ冗長する場合に実装されます。

図　　データ プレーンの冗長性



すべてを統合する

上述のアーキテクチャを備えた Cisco SD-WAN オーバーレイを導入するための、簡易的な導入ワークフローは次のとおりです。

1. SD-WAN オーバーレイに参加する WAN エッジ ルータの設定テンプレートを作成します。

2. WAN エッジ ルータが設置され、電源がオンになり、ケーブル接続されると、ゼロタッチ プロビジョニングのプロセスが開始されます。これらの WAN エッジ ルータは、接続された回線を使用して、シスコがホストするプラグアンドプレイ サービスに接続します。このホステッド サービスは、WAN エッジ ルータを vBond にリダイレクトしてデバイスを認証し、vManage からテンプレート設定を受信できるようにします。

3. WAN エッジ ルータが設定されると、vSmart へのチャネルが構築されます。

4 コントロール プレーンの接続が確立されると、WAN エッジ ルータは vSmart コントローラとの OMP ピアリングをセットアップします。このピアリングにより、WAN エッジ ルータは、他のすべてのサイトに関するルーティング情報と、リモート ブランチへの IPSec 接続を行うための情報を学習できます。

5 IPSec トンネルを確立し、SD-WAN オーバーレイが形成されると、WAN エッジ ルータはポリシーに基づいて相互の BFD 隣接関係を形成するプロセスを開始します。

プラットフォーム

Cisco SD-WAN ソリューションに対応したプラットフォームは一般的に WAN エッジ ルータと呼ばれ、さまざまなフォーム ファクタのモデルがあります。WAN エッジ ルータは、ブランチ、キャンパス、データセンター、パブリック クラウド、またはプライベート クラウド（コロケーション施設など）での使用に対応しています。どの導入環境を選択するかにかかわらず、すべての WAN エッジ ルータは SD-WAN オーバーレイ ファブリックの一部として、vManage を通じて管理されます。Cisco SD-WAN に対応したプラットフォームには、次の 2 つのタイプがあります。

1. ハードウェア プラットフォーム

- Viptela OS を実行する Cisco vEdge（旧 Viptela vEdge）ルータ
- IOS® XE SD-WAN ソフトウェアを実行するサービス統合型ルータCisco ISR 1000 シリーズおよび 4000 シリーズ
- IOS XE SD-WAN ソフトウェアを実行するアグリゲーション サービス ルータ Cisco ASR 1000 シリーズ

2. 仮想プラットフォーム

- IOS XE SD-WAN ソフトウェアを実行するクラウド サービス ルータ Cisco CSR 1000v
- Viptela OS を実行する vEdge Cloud ルータ

仮想プラットフォームは、Cisco x86 コンピューティング プラットフォーム（Enterprise Network Computing System（ENCS）5000 シリーズ、Unified Computing System®（UCS）、Cloud Service Platform（CSP）5000 シリーズなど）に導入できます。仮想プラットフォームは、KVM や VMware ESXi などのハイパーバイザを使用して、任意の x86 デバイスで実行することも可能です。

図　ハードウェア プラットフォームと導入ケース

クラウド

Cisco SD-WAN は、データセンター（DC）、ハブ、ブランチなどの任意のサイトからネットワークをクラウドに拡張し、クラウド内のアプリケーションにシームレスに接続する方法を提供します。

Cloud onRamp for Software as a Service（SaaS）を使用すると、使用可能な最適パスを選択することにより、Salesforce や Office 365 などの特定の SaaS ベースのアプリケーションへの接続の最適化を図ることができます。パスの選択は、使用可能なすべてのパスから取得されたパフォーマンスの測定値に基づいています。パスのパフォーマンスが低下した場合、トラフィックはより最適なパスに動的に移動されます。詳細については、「SaaS の最適化」のセクションを参照してください。

Cisco SD-WAN ソリューションでは、パブリック クラウド上のワークロードとブランチや DC からの接続を非常に簡易に構築することが可能です。Cloud onRamp for Infrastructure as a Service（IaaS）を使用すると、vManage の操作のみで仮想 WAN エッジ ルータ インスタンスをクラウド上に自動構築することができ、ホステッド サービスを SD-WAN オーバーレイの一部として提供できます。詳細については、「*パブリック クラウドへの SD-WAN の拡張*」のセクションを参照してください。

Cloud onRamp for Colocation ソリューションを使用することにより、アプリケーション トラフィックをコロケーション施設に集約して宛先に送信することができ、サービスとクラウド アクセスを地域ごとに集約することができます。Cloud onRamp for IaaS と Cloud onRamp for SaaS を使用して、コロケーション施設から IaaS および SaaS へのトラフィックを最適化することもできます。詳細については、「コロケーションの利用」のセクションを参照してください。

本書では、クラウドベースの SD-WAN のシナリオとユース ケースを個々の章で包括的に扱っています。

セキュリティ

Cisco SD-WAN アーキテクチャは、コントロール プレーン、データ プレーン、およびマネジメント プレーンの運用に対して強力なセキュリティを提供します。これについては、「コンプライアンス要件を満たす」の章で詳しく説明されています。

SD-WAN ブランチ、つまり、別のデバイスやソリューションに依存せずにセキュアなダイレクト インターネット アクセス（DIA）を実現するために、WAN エッジ ルータには強力な脅威防御メカニズムが組み込まれています。これにより、インターネットの脅威に対しブランチ ネットワークのユーザ トラフィックが確実に保護され、アプリケーションのパフォーマンスも向上し、最適なパスとしての DIA を安全に使用することが可能になります。

次に、WAN エッジ ルータで利用可能な脅威防御機能を示します。

- ステートフル アプリケーション ファイアウォール
- 侵入防御 & 侵入検知（IPS/IDS）
- URL フィルタリング
- Cisco Advanced Malware Protection（AMP）および ThreatGRID®
- Cisco Umbrella® DNS
- クラウド内のインターネット ゲートウェイを保護するためのトンネリング（サードパーティ）

脅威防御機能とその使用方法の詳細については、「*セキュアなダイレクト インターネット アクセス*」の章を参照してください。

アプリケーション エクスペリエンス

Cisco SD-WAN ソリューションは、エンド ユーザのアプリケーション エクスペリエンスを向上させるために複数の手法を提供します。それは次のようなものです。

- Quality of Service（QoS）：アプリケーション トラフィックの優先順位付けを行います。
- 前方誤り訂正（Forward Error Correction, FEC）およびパケット複製（Packet Duplication）機能：修復の損失が不十分な品質の回線で発生します。
- アプリケーション アウェア ルーティング：重要なビジネス アプリケーション向けに SLA とダイナミック ルーティングを提供します。
- TCP 最適化：TCP データ トラフィックの処理を微調整して、ラウンドトリップ遅延を低減し、スループットを向上させます。
- Cloud onRamp for SaaS：アプリケーションのパフォーマンスを測定し、動的に最適なパスを選択することで、SaaS アプリケーションのパフォーマンスを最適化します。

アプリケーション エクスペリエンスの最適化の詳細については、「アプリケーション エクスペリエンスの改善」の章を参照してください。そのソリューションの詳細については、「SaaS の最適化」の章を参照してください。

管理と運用

Cisco SD-WAN ソリューションの主な利点は、管理の自動化と運用の簡素化です。Cisco vManage は、Cisco SD-WAN ソリューションの管理、モニタリング、トラブルシューティングのすべての側面に関する一括管理を提供します。Cisco vManage により、管理者は新しいサイトのプロビジョニング、ポリシーの導入、アプリケーションの可視性とパフォーマンスに関する深い知見の活用、デバイスのヘルス チェック、ソフトウェア アップグレードの実行などを行うことができます。Cisco vManage は、異なるアクセス権限を割り当てることで職務を分離するために、ロールベースのアクセス コントロール (RBAC) を採用しています。

Cisco vManage は、Cisco SD-WAN ソリューション全体を運用できる、REST API の豊富なセットを公開しています。これらの API は、ユーザ定義の自動化や、他のオーケストレーション システムやツールへの統合にも使用できます。

Cisco vAnalytics は、ネットワークの健全性と可用性、アプリケーションのパフォーマンスと異常、およびネットワークとアプリケーションの使用率の予測に関する詳細情報を提供する SaaS ベースの追加サービスを提供し、キャパシティ プランニングに役立てることができます。

Cisco SD-WAN はマルチテナント機能をサポートし、柔軟な分割運用を可能にします。マルチテナント機能を使用して、パートナーおよびサービス プロバイダーは Cisco SD-WAN をサービスの形態でお客様に提供することもできます。

SD-WAN ソリューションの管理と運用の詳細については、「運用のシンプル化」、「Cisco SD-WAN API」、および「SD-WAN マネージド サービス」のセクションを参照してください。

アプリケーション
エクスペリエンスの改善

ビジネス ニーズ

ネットワークはアプリケーション トラフィックを伝送するために構築されていますが、最適なアプリケーション エクスペリエンスを提供することは、ユーザの生産性を向上させる上で最も重要な側面の 1 つです。最適なアプリケーション エクスペリエンスを提供するには、何が必要でしょうか。この回答は、ネットワークに存在する一連の条件と動作によって異なります。これは解決すべき多次元の問題であり、そうするには多くのことを考える必要があります。

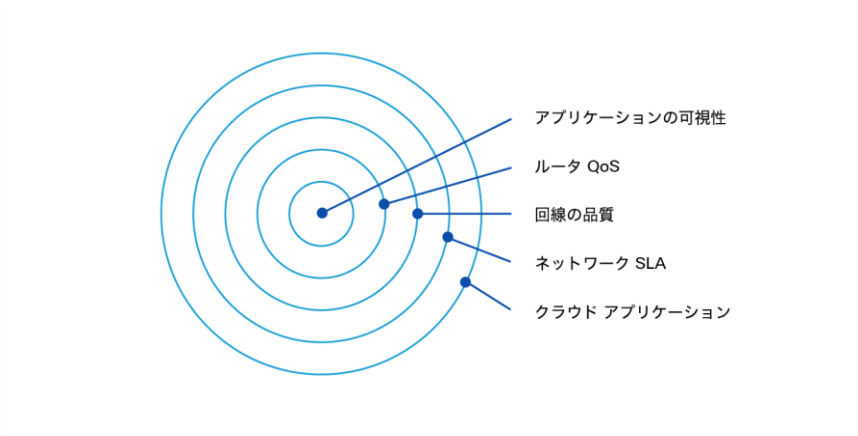
SD-WAN ソリューションは、アプリケーションの品質の問題が発生しにくくなる方法で採用する必要がありますが、発生した場合には、ネットワークは自動化された修復によって対応し、悪影響を最小化または排除する必要があります。

ビジネスクリティカルなアプリケーションに最適のエクスペリエンスを提供するには、ネットワーク上のアプリケーションを理解し、適切にコントロールする必要があります。アプリケーションの QoE に影響を与える問題には、次のようなものがあります。

- 低品質の回線でのデータ損失。
- 音声またはその他のビジネスクリティカルなアプリケーションに影響を与える回線上の過度の遅延またはジッター。
- データセンターに集約されたクラウド トラフィックのバックホーリング(Backhauling)による遅延。
- 低帯域幅リンクでの、ビジネス クリティカルなトラフィックに対する不適切な優先順位付け。

Cisco SD-WAN ソリューションは、アプリケーションの QoE を最適化する多様な機能を提供することで、これらの問題に対応できます。

図　アプリケーションの QoE を最適化するためのツール

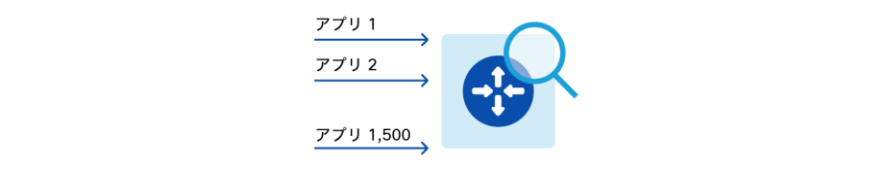


アプリケーションの可視性

アプリケーションがクラウドに移行し、ソーシャル メディアやストリーミング サービスの利用が増加するにつれて、エンタープライズ ネットワークではビジネスとエンターテイメントの両方の Web トラフィックの量が増えています。多くの場合、Office 365 や Cisco Webex® などのクラウド アプリケーションを含むビジネス アプリケーションは、エンターテイメント用の Web トラフィックで使用されるのと同じ HTTP および HTTPS プロトコルを使用します。

アプリケーションのパフォーマンスを最適化し、アプリケーションごとのネットワーク使用ポリシーを定義するには、管理者がネットワーク上で流れるさまざまなタイプのアプリケーションを詳細に可視化する必要があります。

図　ディープ パケット インスペクションの可視化



Cisco WAN エッジ ルータ上に統合されたディープ パケット インスペクション（DPI）エンジンは、さまざまなテクノロジーを活用して、1,500 を超えるアプリケーションを認識します。対象となるアプリケーションには、音声およびビデオ、電子メール、ファイル共有、ゲーム、ピアツーピア（P2P）、クラウドベース アプリケーションなどがあります。アプリケーションが分類されると、ポリシーを設定してビジネスクリティカルなアプリケーションに優先順位を付け、SLA メトリックを使用して WAN パスを選択できます。

QoS

WAN エッジ ルータは、アプリケーション トラフィックに対するルーティングを適用することで、最適なアプリケーション エクスペリエンスを実現するという、きわめて大きな役割を担います。WAN エッジ ルータに適用される 3 つの主要な動作は次のとおりです。

- アプリケーション トラフィックの優先順位付け
- サービス プロバイダーのサービス クラスへのアプリケーション トラフィックのマッピング
- 過剰なアプリケーション トラフィックのフラグメンテーションの回避

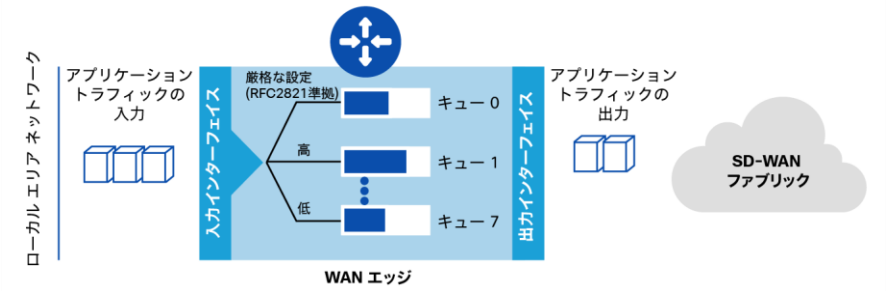
アプリケーション トラフィックの優先順位付け

アプリケーションの状況は多岐にわたり、すべてのアプリケーションが同じように作成されるわけではありません。多くの帯域幅を必要とするアプリケーションもあれば、遅延（レイテンシ）に対する要件が非常に厳しいアプリケーションもあります。また、損失に敏感なものもあれば、ジッターがあるとパフォーマンスが大きく低下するものもあります。アプリケーション トラフィックが WAN エッジ ルータを通過する際は、通常、ネットワーク リソースがほとんど競合しない高帯域幅のローカル エリア ネットワークから、時には「全ビット数がカウントされる」ような低帯域幅のワイド エリア ネットワークを通過することになります。今日、大容量ブロードバンド回線が広く行き渡り、状況が劇的に改善されたとは言え、ワイド エリア ネットワークのリソースの競合は依然として問題になっています。

ワイド エリア ネットワークの輻輳が発生した場合、WAN エッジ ルータは QoS を採用することで、低クラスのトラフィックよりもビジネスクリティカルなトラフィックを優先します。これを実現するために、キューイングが使用されます。重み付きラウンドロビン (Weighted

Round Robin）スケジューリングでは、さまざまなアプリケーションが帯域幅を公平に共有します。一方、厳格なプライオリティ キューイング（strict priority queuing）では、時間的な制約のあるアプリケーションのジッターと遅延を最小限に抑えることができます。また、WAN エッジ ルータは、キャリアが提供する回線容量に対応するために、トラフィック シェーピングやトラフィック ポリシングなどのメカニズムを使用することもできます。Cisco vManage は、QoS ポリシーを設定するためのインターフェイスを提供するとともに、その動作をモニタリングします。

図　QoS



サービス プロバイダーのサービス クラスへのアプリケーション トラフィックのマッピング

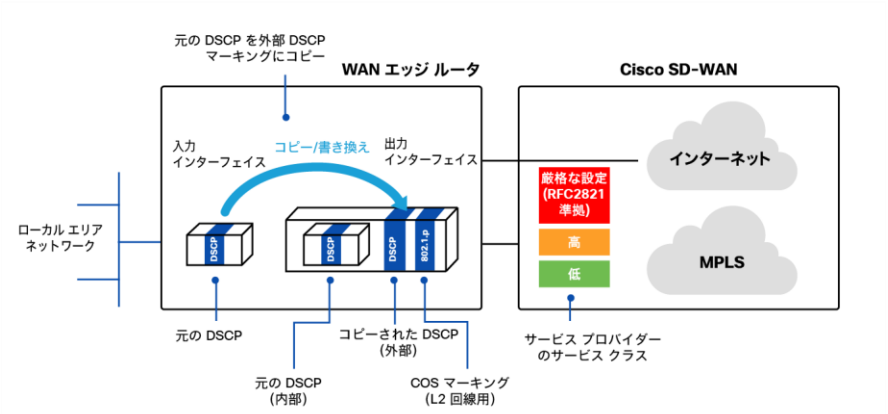
Cisco SD-WAN は、トランスポートに依存することなく、WAN エッジ ルータに展開されたすべての回線を利用します。これらの回線を通じて、SD-WAN サイト間の実際のアプリケーション トラフィックが伝送されます。プライベート回線を利用する場合、サービス プロバイダーはアプリケーション トラフィックを優先付けするために、ネットワークのコアを通過す

る際に特定のサービス クラスを付与することがあります。サービス プロバイダーのサービス クラスに対するアプリケーション トラフィックのマッピングは、通常、レイヤ 3 回線の場合は DSCP マーキングで照合し、レイヤ 2 回線の場合は COS マーキングで照合することによって行われます。DSCP マーキングと COS マーキングのどちらも、データグラムのヘッダー内に存在します。

Cisco SD-WAN ソリューションは、IPsec や GRE などのトンネリング テクノロジーを活用して、アプリケーション トラフィックをワイド エリア ネットワーク回線経由で送信される前にカプセル化します。このカプセル化により、追加の IP ヘッダーがパケットに付加されます。その結果、元の IP ヘッダーは「隠蔽」され、サービス プロバイダーはトラフィックの優先順位を適用できなくなります。ただし、Cisco SD-WAN ソリューションは、内部のカプセル化された IP ヘッダーから新しく追加した外部 IP ヘッダーに元の DSCP マーキングをコピーすることにより、サービス プロバイダーのサービス クラスの優先順位付けと連携して機能します。レイヤ 2 回線の場合、ソリューションは出力フレームに COS マーキングを適用することもできます。

一部のサービス プロバイダーは、企業で使用されるクラスの数と比較して少ない数のクラスを提供します。Cisco SD-WAN ソリューションでは、元の DSCP 値を外部ヘッダーの別の DSCP 値に書き換えて、サービス プロバイダーがサポートするクラスに一致させることができます。

図　アプリケーション トラフィックをサービス プロバイダーの
サービス クラスにマッピングする



サービス プロバイダーがサービス クラスを維持できるようにすると、プライベート トランスポートで適切なアプリケーション エクスペリエンスを保証するのに非常に役立ちます。インターネット回線は通常、いかなるタイプの QoS 保証も提供しません。そこで、これらの回線を介してルーティングされるトラフィックには、最適なアプリケーション エクスペリエンスを保証する他の方法が必要です。

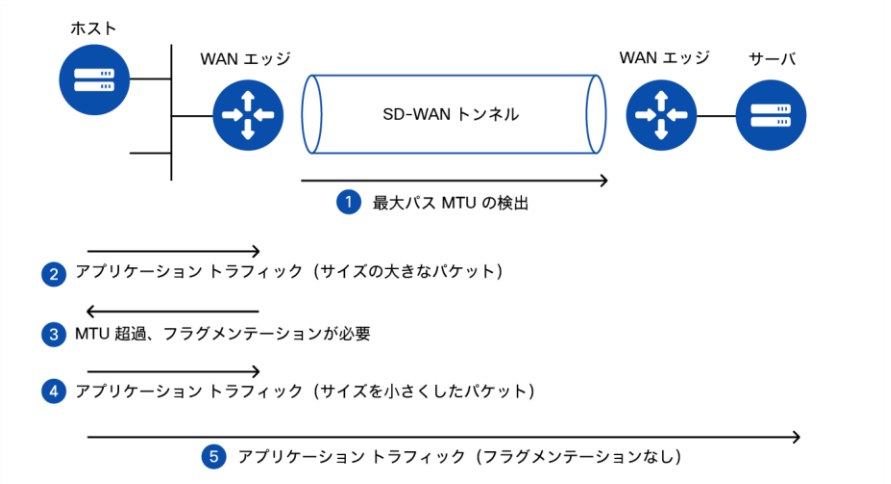
アプリケーション トラフィックのフラグメンテーションの回避

ネットワーク回線とルータ インターフェイスは、それらを介して送信されるデータグラムの最大伝送ユニット（MTU）サイズを定義します（バイト単位）。MTU サイズを超える IP パケットは、送信前にセグメントに分割される必要があります。ネットワーク上で通信するアプリケーション ホストは、IP ヘッダー内に「フラグメント化しない」（do-not-fragment, DF）フラグを設定することでフラグメンテーションを禁止できます。パス MTU ディスカバリ（PMTUD）のプロセスでは、フラグメンテーションが発生する前に、ホストがトランジット ネットワーク上で MTU を検出できるようにするために、DF マーキングを使用することもできます。フラグメンテーションおよび、さらに重要なフラグメントのリアセンブルは、

本来はアプリケーション トラフィックの処理に利用されるべき処理能力を大幅に消費する可能性があるので、これは効率面で非常に重要な要素と言えます。

Cisco SD-WAN は、IP カプセル化を利用して SD-WAN サイト間のトラフィックを送信するため、ファブリック全体で利用可能な MTU 全体を削減する追加のヘッダーが導入されています。インターネット回線の使用が増加することで、異なるサービス プロバイダー間の相互接続ポイントでの MTU 削減という悪影響が生じる可能性が高くなります。最適なアプリケーション エクスペリエンスを維持するために、Cisco SD-WAN ファブリックは、すべての SD-WAN トンネルでパス MTU をプロアクティブに検出します。また、ファブリック経由で利用可能な MTU を通知することで、ホスト パスの MTU 検出プロセスと相互運用します。

図　　パス MTU 検出プロセス



回線の品質

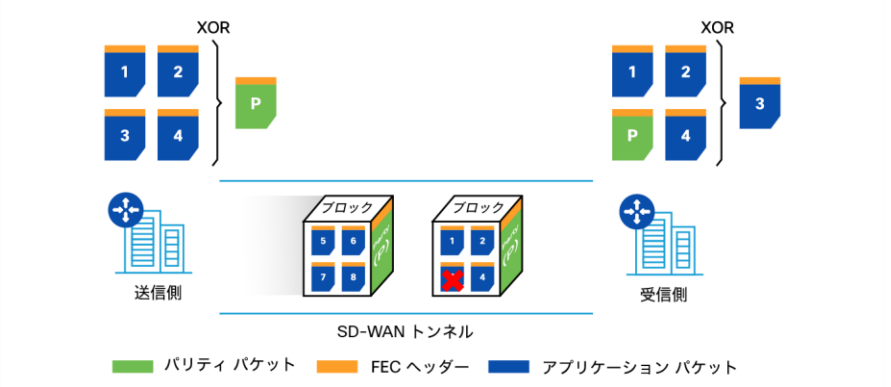
SD-WAN を使用することで、重要なアプリケーション トラフィックにインターネット回線を利用できます。現在のインターネットは高帯域幅を提供していますが、MPLS などのプレミアム WAN 回線と比較すると、その信頼性は依然として十分ではありません。そのため、アプリケーションによっては、偶発的なパケット損失が問題となることがあります。Cisco SD-WAN は、パフォーマンスを損なうことなく、アプリケーションがパケット損失に対処できるようにする、回線修復機能を提供します。

インターネット回線経由の重要なアプリケーション トラフィック

Cisco SD-WAN の前方誤り訂正（Forward Error Correction, FEC）機能を使用して、重要なトラフィックが信頼性の低い WAN リンク全体でうまく機能することを保証できます。FEC は、4 つのパケットの事前定義されたグループごとに、「パリティ」パケットを付加して送信することで、リンク上で失われたパケットを回復するメカニズムです。受信側の WAN エッジ ルータは、受信したパリティ パケットを使用し、XOR 計算を実行することで、グループから失われたパケットを回復できます。これにより、アプリケーション データを再送信することなく、アプリケーションのパフォーマンスを維持できます。

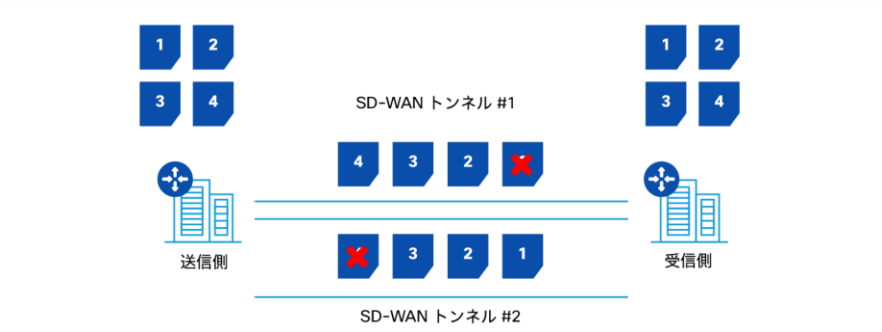
次の図は FEC を表しており、WAN リンクでアプリケーション パケット番号 3 が失われたことを示しています。

図　前方誤り訂正（Forward Error Correction, FEC）機能



FEC に加えて、Cisco SD-WAN のパケット複製（Packet Duplication）機能を使用して、複数のリンク間で同じアプリケーション フローを送信し、アプリケーションの信頼性を向上させることができます。特定の回線でフローの一部のパケットが失われた場合、受信側の WAN エッジ ルータは他の回線からの複製パケットを使用して、そのトラフィック フローの失われたパケットを回復します。

図　　パケット複製（Packet Duplication）機能



パケットの複製は、アプリケーションの可用性を大幅に向上させますが、帯域幅の消費が増加するという犠牲を伴うことに注意してください。そのため、慎重に使用する必要があります。

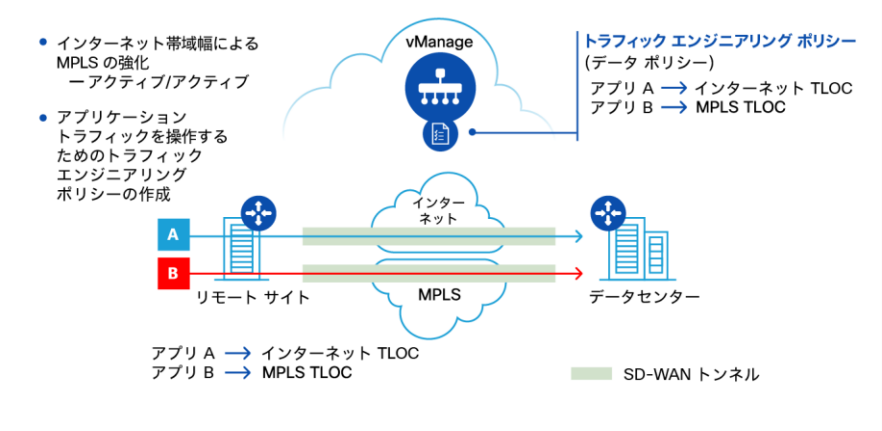
SLA への適合

すべてのお客様は、ネットワーク全体で重要なアプリケーションの SLA 要件を満たすことが急務となっています。SLA の要件は、遅延、損失、およびジッターのしきい値で構成されます。お客様は、TCP 最適化、Wide Area Application Services（WAAS）、帯域幅の増強、アプリケーション アウェア ルーティング ポリシーの使用などの最適化手法を使用して、これらの要件を満たすことができます。

すべての帯域幅の活用

使用可能なすべての帯域幅を使用することで、お客様は、MPLS などの高品質回線から一般インターネット回線にトラフィックをオフロードして、アプリケーションに対して同じ SLA を実現できます。理論的には、複数のインターネット回線が 1 つのプレミアム回線として同等もしくはそれ以上の可用性とパフォーマンスを、わずかなコストで実現することができます。Cisco SD-WAN は、使用可能なすべてのトランスポート帯域幅を選択できる柔軟性を備えており、この同等レベルの可用性とパフォーマンスをアプリケーションに拡張します。Cisco SD-WAN ポリシーを使用して、特定のトラフィックが適切な回線にマッピングされることを保証できます。たとえば、音声は MPLS 回線に、Web ブラウジングはインターネット回線に送信されます。

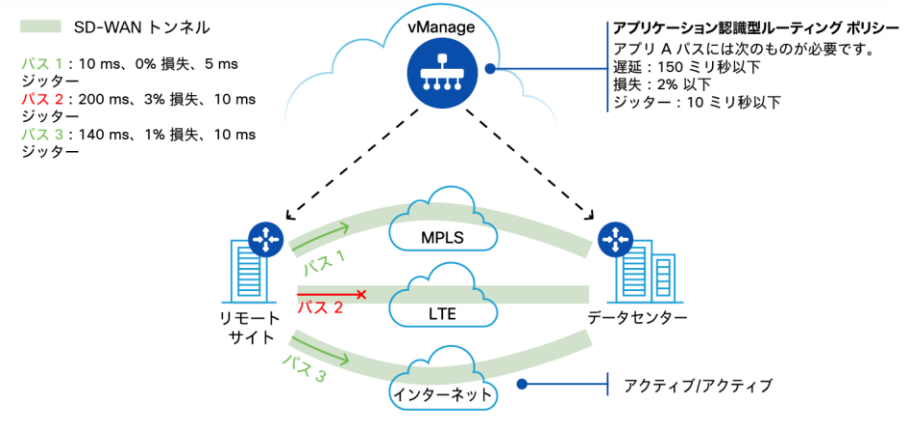
図　　帯域幅の増強



Cisco SD-WAN を使用したアプリケーションベースのルーティング

SLA ベースのポリシーを使用して、重要なアプリケーション向けに最適なパスを選択するほか、それらの SLA が満たされていない場合にはパスを動的に切り替えることができます。Cisco SD-WAN ソリューションでは、これらのポリシーは、アプリケーション アウェア ルーティングと呼ばれる機能の一部になっています。アプリケーション認識型のルーティング ポリシーは、重要なアプリケーションに対して厳格な SLA が定義され、パスが SLA を満たしている場合に特定のパスが選択されるように設定できるという方法で定義できます。たとえば、MPLS が設定された SLA を満たしている場合は、音声トラフィック用の MPLS トランスポートが選択されます。もう 1 つのオプションは、準拠している任意のパスを介してトラフィックを送信できるような SLA を定義することです。次の図では、パス 1 と 3 のみがアプリケーション A の SLA を満たしているため、アプリケーション A のフローは、リモート サイトからデータセンターに到達するためにパス 1 または 3 を選択します。

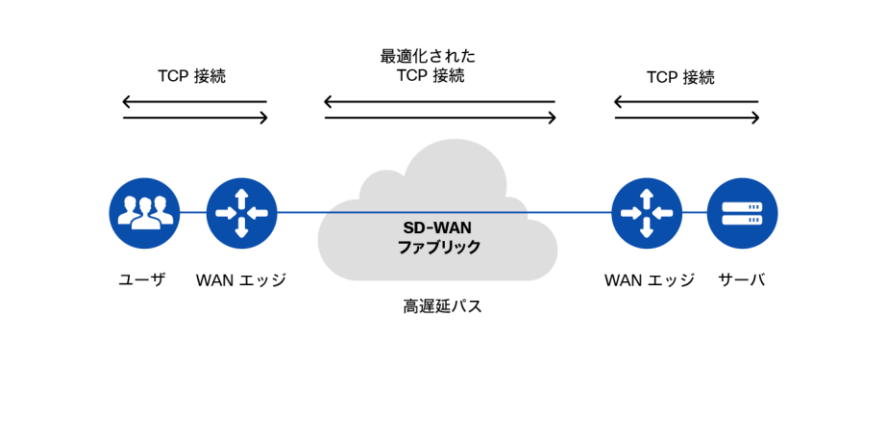
図　アプリケーション アウェア ルーティング



TCP 最適化

Cisco SD-WAN の TCP 最適化機能は、スループットを最大化し、より優れた QoE を実現するために、TCP 選択的確認応答（Selective Acknowledgement, SACK）を使用して、不必要な再送信と TCP の初期ウィンドウ サイズが大きくなるのを防止します。

図　TCP 最適化機能


TCP 接続
最適化された
TCP 接続
TCP 接続
SD-WAN
ファブリック
ユーザ
WAN エッジ
WAN エッジ
サーバ
高遅延パス

クラウド アプリケーションのパフォーマンス

Cisco SD-WAN は、SaaS アプリケーションを可視化し、リアルタイムの転送を実行できるようにする Cloud onRamp 機能を提供します。さらに、Cloud onRamp は、クラウドベースのアプリケーション エクスペリエンスを向上させるために、IaaS クラウド サービス プロバイダーとのシームレスな統合も実現します。

SaaS アプリケーション エクスペリエンスの改善

Microsoft や Salesforce などのエンタープライズ ソフトウェア プロバイダーは、Software as a Service (SaaS) を介してインターネット経由で多数のアプリケーションを提供します。遅延とパケット損失はこれらのアプリケーションのパフォーマンスに影響を及ぼしますが、レガシー ネットワークでは、ネットワーク管理者はエンド ユーザと SaaS アプリケーション間のネットワーク特性をほとんど把握できません。レガシー ネットワークでパスの品質が損なわれた場合、アプリケーション トラフィックを手動で代替パスに移すプロセスは、複雑で時間がかかり、エラーが発生しやすくなります。

Cloud onRamp for SaaS 機能は、Cisco SD-WAN オーバーレイ ネットワークで SaaS アプリケーションのパフォーマンスを最適化することで、これらの問題に対応します。Cloud onRamp for SaaS は、センター集約型のダッシュボード上で個々のクラウド 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。これは、ネットワーク パフォーマンスの変化にリアルタイムで応答し、クラウド アプリケーション トラフィックを使用可能な最適なパスにインテリジェントに再ルーティングします。詳細については、本書の「SaaS の最適化」の章を参照してください。

コロケーションの利用

Cloud onRamp for Colocation 機能は、冗長パスを提供するために、SaaS アプリケーション用のゲートウェイとして使用できます。理想的には、Cisco Cloud onRamp for Colocation は、SaaS プロバイダーのリソースに直接接続するコロケーションに配置されます。コロケーションによる SaaS プロバイダーのクラウドへの高速トランスポートを活用するには、ユーザ トラフィックを最も近いコロケーションに迅速かつ効率的に転送することが重要です。Cloud onRamp for SaaS 機能と組み合わせることで、損失と遅延を測定するために、アプリケーション プローブも各コロケーション施設を介して送信されます。理論的には、コロケーションはプロバイダーのクラウドへの損失と待ち時間が最適になるため、アプリケーションに到達するためのプライマリ パスとして選択できます。コロケーション内で損失または遅延が発生した場合、次の 2 つのいずれかを選択することになります。ひとつは、「次善の」パフォーマンスを提供できるコロケーションにトラフィックを転送するもの、もうひとつの選択肢は、ローカルに接続されたインターネット回線を使用するというものです。

Cisco Cloud onRamp for Colocation 機能の詳細については、本書の「コロケーションの利用」の章を参照してください。

IaaS アプリケーション エクスペリエンスの改善

Cloud onRamp for IaaS は、Cisco SD-WAN オーバーレイ ネットワークのファブリックをパブリック クラウド インスタンスに拡張して、ブランチ ルータがパブリック クラウド アプリケーション プロバイダーに直接接続できるようにします。この接続を提供するための物理データセンターが不要となり、Cloud onRamp for IaaS は IaaS アプリケーションのパフォーマンスを向上させます。Cloud onRamp for IaaS 機能は、AWS 仮想プライベート クラウド (VPC) および Azure 仮想ネットワーク（VNET）と連動して動作します。

この機能の詳細については、本書の「パブリック クラウドへの SD-WAN の拡張」の章を参照してください。

導入事例

米国最大手銀行の 1 つは、1,100 か所以上の拠点を設け、約 2,500 台の現金自動預払機（ATM）を設置していますが、次の主要な目標を達成するために、1,400 か所の拠点向けの SD-WAN ソリューションを探していました。

- セルフサービス キオスク、エキスパートとのライブ ビデオ会議、新しいリテール バンキング アプリケーションなどのアプリケーションのカスタマー エクスペリエンスを向上させる。
- コンプライアンスとセキュリティに関連するオーバーヘッドを削減する。
- リアルタイムのデータを金融テクノロジー パートナーと共有する。
- 支店と ATM の運用を簡素化する。
- API 主導型にする。

選択したソリューションは、Cisco SD-WAN で構築されたマネージド サービスで、サービスの提供と QoE を大幅に改善しました。トランスポートとしてインターネットと MPLS を並用することで、リモート ロケーションにより高い帯域幅容量を提供するのに必要な時間が大幅に短縮され、60 日からわずか数日になりました。MPLS、インターネット、および LTE 回線経由でのダイナミックな SLA ベースのトラフィック ルーティングにより、アプリケーションのパフォーマンスが向上しました。パフォーマンスの高いネットワークは、データ損失の防止とバックアップにも役立ちました。ブランチでビデオと Wi-Fi を有効にすることに加えて、このネットワーク基盤は、銀行がアジャイル開発に移行し、より柔軟な Web サービス アーキテクチャを使用し、金融テクノロジー パートナーと安全に接続できるように支援しました。Cisco vManage が主導する一元化されたソフトウェア アップデートを使用して、ネットワークを迅速に更新しました。

主な要点

アプリケーションのパフォーマンスは、ビジネスの継続性とユーザ エクスペリエンスにとって重要です。ネットワーク パフォーマンスの低下と不適切な設計は、アプリケーションのパフォーマンスに悪影響を及ぼす可能性があります。Cisco SD-WAN には、アプリケーション エクスペリエンスを大幅に向上させる多くの機能があります。今まで説明したそれぞれの機能を個別に、または組み合わせて有効にすることにより、重要なアプリケーション トラフィックが高品質を維持することを保証できます。

Cisco SD-WAN ソリューションが提供する事柄は次のとおりです。

- アプリケーションの優先順位付けや、重要なアプリケーションに必要な SLA に基づく最適化されたパスの選択などの QoS。
- 重要なトラフィックの回線修復により、品質の低い回線を通過するトラフィックのエンドユーザ エクスペリエンスを向上させる。
- クラウド SaaS および IaaS プロバイダーとの統合により、最適なアプリケーション エクスペリエンスを実現する。

その他の参考資料

- Cisco SD-WAN Cloud onRamp for SaaS：*http://cs.co/onramp*
- シスコ検証済みデザイン（CVD）：Cloud onRamp for SaaS Deployment Guide（Cloud onRamp for SaaS 導入ガイド）：*http://cs.co/onramp-saas-cvd*

セキュアなダイレクト インターネット アクセス

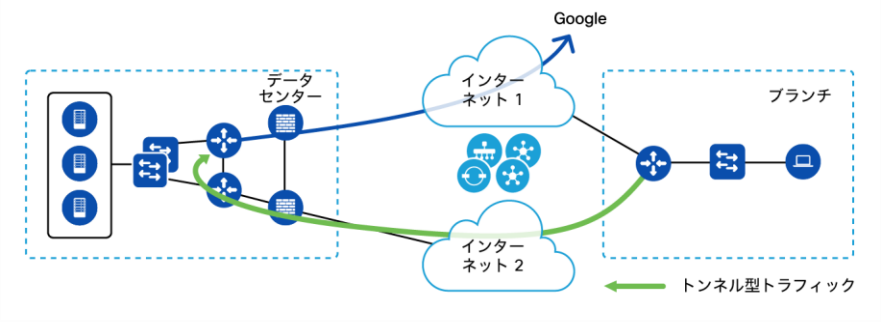
ビジネス ニーズ

従来のワイドエリア ネットワーキングでは、拠点などのブランチ サイトからのインターネット トラフィックが、データセンターや地域のハブ サイトなどの中心となるロケーションに送信されます。これにより、インターネットから返されたトラフィックが、ブランチに返送される前にセキュリティ機器によってスクラビング処理されます。このような従来の方法では、あらゆるロケーションにセキュリティ機器を導入することとなり、膨大なコストがかかります。

インターネット トラフィックの帯域が増加するにつれて、SaaS（例：Office 365、Box）や IaaS などのクラウド サービスを利用する企業が増えています。さらに、インターネットベースのアプリケーションが増加し、在宅勤務を行うビジネス従業員が増え、Internet of Things（IoT）デバイスも同様に多くの帯域を利用しています。

インターネット アクセス用のトラフィックを、データセンターに集中させると、帯域幅使用率が増加してしまいます。これは、インターネットにアクセスする前にトラフィックをデータセンターにトンネリングする必要があるためです。これにより、ブランチから中央への帯域幅を大きく消費してしまう可能性があります。データセンターのセキュリティ機器とネットワーク デバイスは、ブランチからの受信帯域幅に対応する必要があります。また、アプリケーション利用については遅延が増大するため、パフォーマンスの低下に繋がります。

図　データセンターを介したインターネット トラフィックのバックホーリング

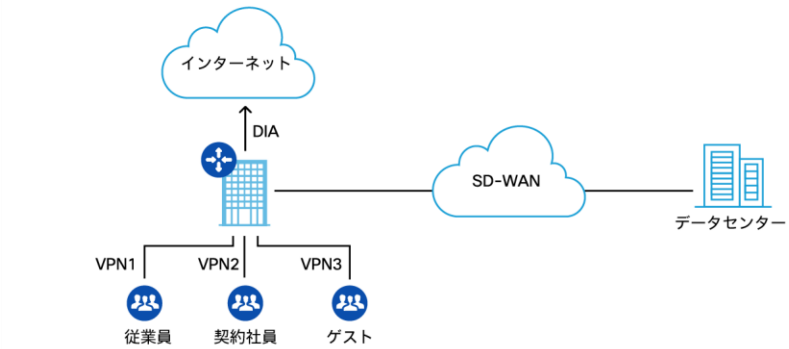


ダイレクト インターネット アクセス：DIA

ダイレクト インターネット アクセスは、データセンターなどのセントラル サイトへのバックホーリング トラフィックの遅延を解消することで、拠点ユーザのインターネット エクスペリエンスを向上させます。データセンターでは回線帯域幅の消費が減少するため、WAN コストも削減されます。

Cisco SD-WAN DIA ソリューションは、安全かつ実装が非常に容易です。DIA は特定のアプリケーション用に設定されており、ビジネスクリティカルなアプリケーションをプレミアム WAN 経由で利用します。たとえば、インターネット閲覧や SaaS アプリケーションでは DIA を有効にすることができますが、ビジネスクリティカルなアプリケーションや、音声などの遅延に影響されやすいアプリケーションはプライベート WAN 回線にとどまることができます。Cisco SD-WAN ソリューションには、ユーザをセグメント化する機能があります。セグメンテーションは、従業員とゲストを分離しておくのに役立ちます。Cisco SD-WAN では、DIA を VPN セグメント用に設定できるため、VPN セグメントごとにインターネット アクセスを制御できます。

図　ブランチからのさまざまな VPN セグメント用の DIA



ユーザとブランチ ネットワークは、Cisco SD-WAN セキュリティ機能を実装することで、インターネット脅威からから保護することができます。セキュリティ機能には、アプリケーション認識型ファイアウォール、侵入検知・防御、URL フィルタリング、高度なマルウェア防御、DNS セキュリティが含まれます。これらのセキュリティ機能は、WAN エッジ ルータ自体に導入することも、統合されたサードパーティのセキュリティ サービスとして導入することもできます。

セキュリティ ポリシー

Cisco SD-WAN を使用すると、ゲスト ユーザや従業員はインターネットに直接アクセスできるようになり、次のことが可能となります。

- アプリケーション エクスペリエンスの改善
- プレミアム WAN 接続からのインターネット トラフィックのオフロード
- アプリケーション認識型ファイアウォール、URL フィルタリング、IPS/IDS、高度なマルウェア防御（AMP）、DNS セキュリティなどのセキュリティ機能を実装することで、あらゆるロケーションでセキュリティ機能を強化することが可能となり、セキュリティアプライアンスを新たに立てる必要が無くなります。

ゲスト アクセス

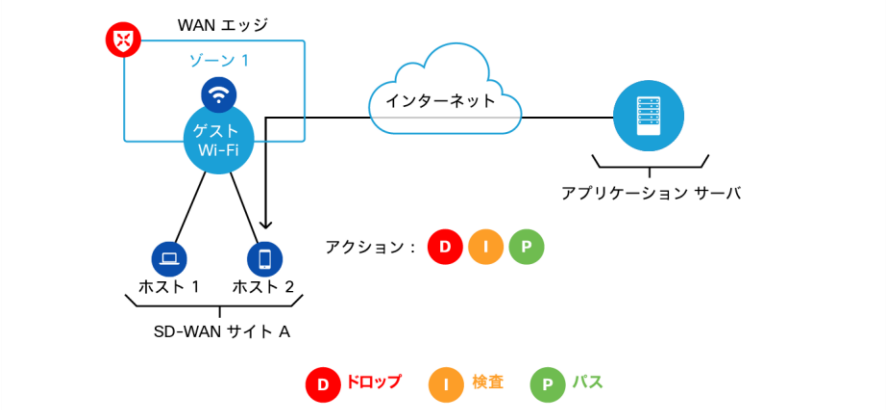
ゲスト アクセスの場合、セキュリティは WAN エッジ ルータで直接有効にすることも、クラウド セキュリティ プロバイダーを介して DIA トラフィックをルーティングすることで有効にすることができます。

ゲスト DIA トラフィックの重要な優先事項は次のとおりです。

- 特定のサイトやインターネット アクセスの制限
- マルウェアや悪意のあるコンテンツからのゲスト ネットワークの保護
- ゲストの帯域幅使用率の制限

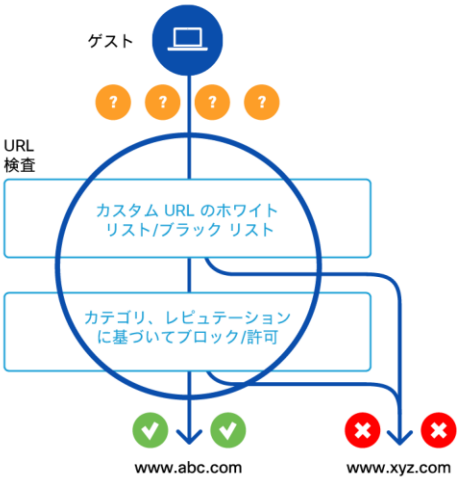
アプリケーション認識型ファイアウォールを WAN エッジ ルータで有効にすることで、ゲスト デバイスからインターネットへのトラフィックを検査することができます。次の図では、インターネット経由のホストとアプリケーション サーバ間のトラフィックが WAN エッジ ルータによって検査されていることを現しています。

図　ゲスト ゾーンからの DIA トラフィックに対するアプリケーション認識型ファイアウォール



URL フィルタリングは、ゲスト トラフィックがインターネット上の特定サイトへのアクセスするのを制限するために、WAN エッジ ルータで動作します。次の図で、ゲスト ユーザは「www.abc.com」へのアクセスは許可されていますが、「www.xyz.com」へのアクセスは拒否されています。

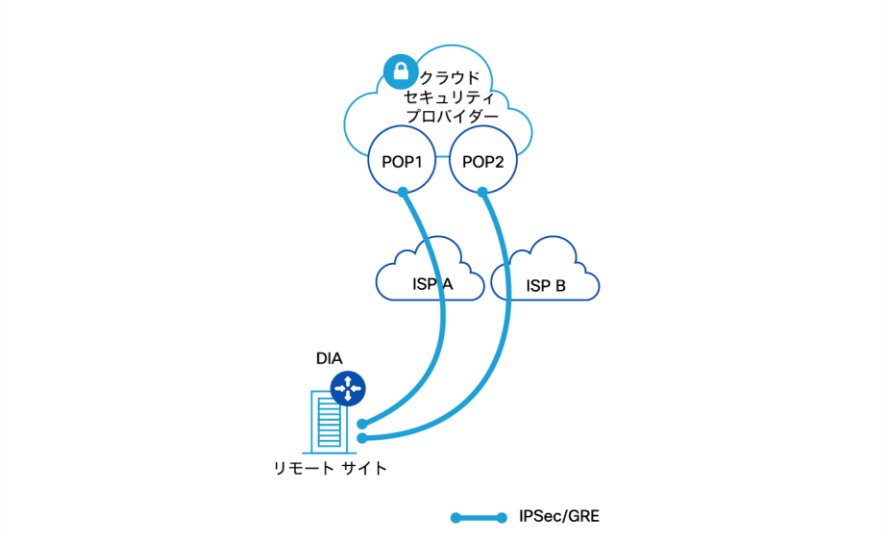
図　ゲスト ゾーンからの DIA トラフィックの URL フィルタリング



クラウド セキュリティ プロバイダーを介したゲスト アクセス

SD-WAN セキュリティをブランチ ルータで有効にする代わりに、お客様はインターネット宛てのトラフィックをクラウド セキュリティ プロバイダーにルーティングするように選択することもできます。ゲスト セグメントから送信されたトラフィックは、ポイントツーポイント（IPSec または GRE）トンネルを介してクラウド セキュリティ プロバイダーにリダイレクトされます。この場合、クラウド セキュリティ プロバイダーは DIA トラフィックに必要なセキュリティ フィルタリングを提供します。

図　クラウド セキュリティ プロバイダーを介したゲスト DIA トラフィック



従業員のインターネット アクセス コントロール

ゲスト アクセスと同様に、SD-WAN セキュリティを有効にすることで、従業員のトラフィックは、制限されます。

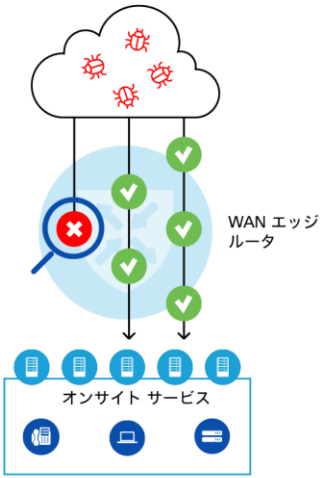
従業員のトラフィックの重要な優先事項は次のとおりです。

- 特定のインターネット サイトへのアクセスの制限
- マルウェアや悪意のあるコンテンツのダウンロードの検出/防止

WAN エッジ ルータは、アプリケーション認識型ファイアウォールや URL フィルタリングとともに、IPS/IDS や AMP などの高度なセキュリティ機能を有効にすることで、従業員が悪意のあるコンテンツをインターネットからダウンロードしないようにすることができます。

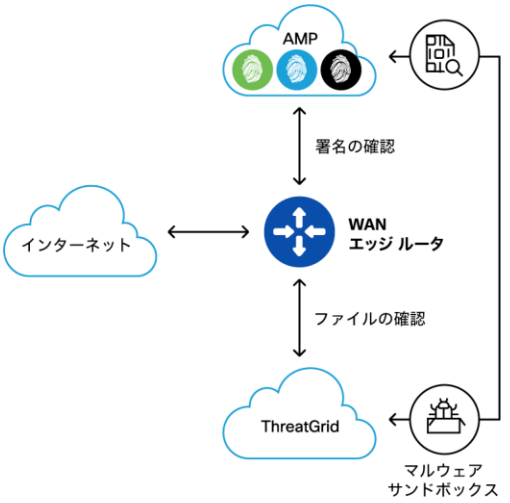
次の図では、WAN エッジ ルータが IPS で有効になっていて、インターネットから悪意のあるパケットが従業員のセグメントに侵入するのを防いでいます。

図　インターネットの脅威から保護するために有効になっている IPS/IDS



AMP 機能を利用することで、WAN エッジ ルータは、ファイル レピュテーションをチェックし、従業員がインターネットから悪意のあるファイルをダウンロードすることを防止可能となります。ファイル レピュテーションが不明で、サンドボックスを必要とする場合には、WAN エッジ ルータはバックグラウンドで Cisco 脅威インテリジェンス（Talos & CTI: Cognitive Threat Intelligence）と通信し、未知のマルウェアの解析を行います。IPS/IDS および AMP 機能は、必要に応じてゲスト アクセスの通信にも適用することができます。

図　ファイル レピュテーションおよび分析

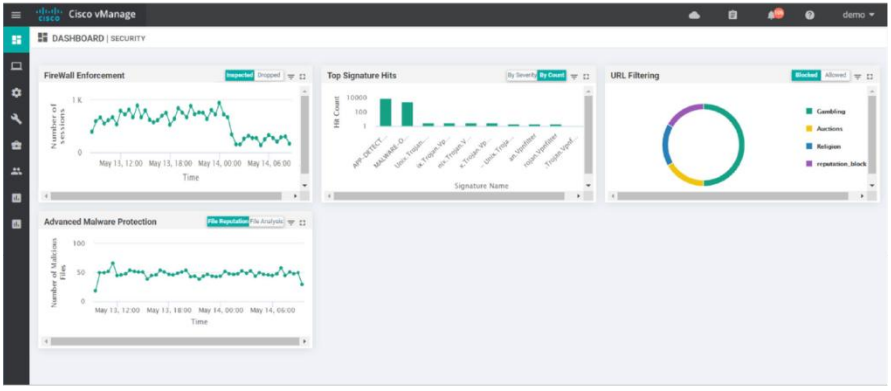


セキュリティ モニタリング

Cisco vManage ダッシュボードを使用して、DIA トラフィックのさまざまな要素をモニタできます。個々のデバイスでは、インターフェイス帯域幅、アプリケーションの使用状況、リアルタイム フロー情報、NAT 変換などの要素をモニタできます。セキュリティ ダッシュボードには、DIA トラフィックに対して有効なセキュリティのさまざまな側面が表示されます。

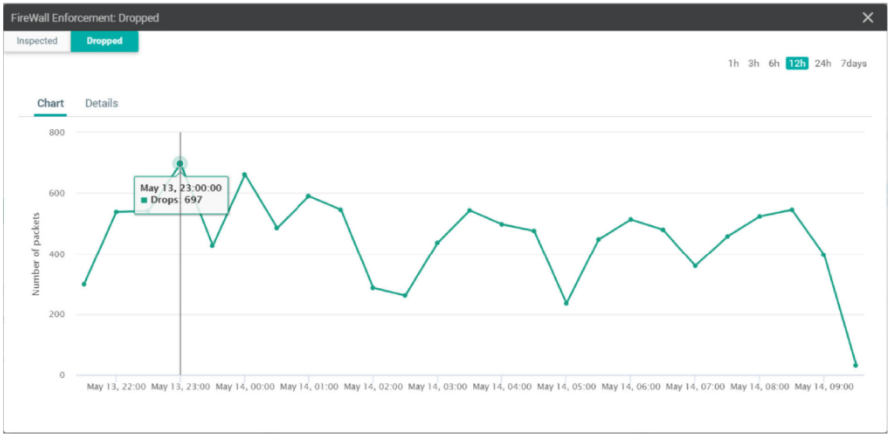
次のセキュリティ ダッシュボードのスクリーンショットは、ファイアウォールの適用アクティビティ、IPS/IDS データ、URL フィルタリングの結果、および高度なマルウェア防御の数が表示されています。各グラフをドリルダウンすると、詳細情報が表示されます。

図　SD-WAN セキュリティ ダッシュボード



ファイアウォール適用グラフの詳細を開くと、時間の経過とともに実行された検査とドロップ数が表示されます。

図　時間の経過に伴うファイアウォール適用のドロップの数



さらに、任意の WAN エッジ ルータについて [モニタ（Monitor）] > [ネットワーク（Network）] > [デバイス（Device）] > [リアルタイム（Real Time）] を表示することで、vManage を介して特定のセッション情報を取得できます。他のセキュリティ機能についても同様の情報を得ることが可能です。

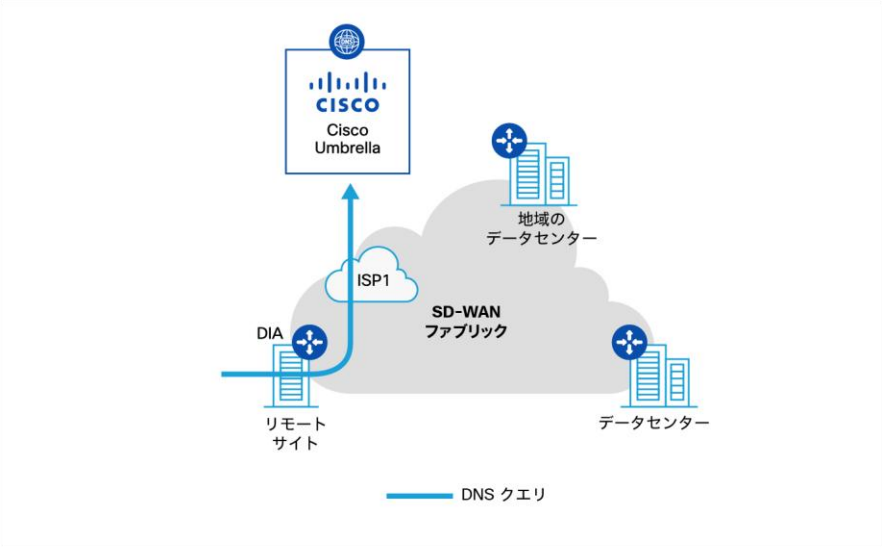
導入事例

1,000 を超える拠点を持つ大規模なファッション小売業者は、すべての拠点で帯域幅を拡大し、コストの高いプライベート MPLS 回線への依存を軽減させ、来店客のインターネット アクセスを向上させることを求めていました。

Cisco SD-WAN の導入の一環として、このお客様はデュアル インターネット回線を備えた WAN エッジ ルータ デバイスを採用しました。また、これらのサイトは、DNS ベースの Web フィルタリングを実行するために、Cisco Umbrella と連携しています。この導入モデルは、非常に望ましい成果を導き出しており、モニタリング、統合セキュリティ、帯域幅の向上、パフォーマンスの向上、および著しいコスト メリットをもたらしました。

同社は現在、小規模な拠点にはインターネット回線のみを使用し、大規模で重要な拠点には MPLS とインターネット回線を併用しています。複数のインターネット回線を使用することで、ネットワークの信頼性が向上します。ある回線に障害が発生した場合には、別回線に簡単にロールオーバーすることができます。また、DIA を有効にすると、すべてのゲスト トラフィックがインターネットに直接接続します。これにより、環境をリスクにさらすことなくエンドユーザ エクスペリエンスを大幅に向上させ、セキュリティ ポリシーが環境に確実に実装されるようになります。

図　DIA トラフィック用に Cisco Umbrella を使用した DNS ベースの Web フィルタリング



主な要点

従来のワイド エリア ネットワークでは、拠点や店舗などのブランチ サイトからのインターネット トラフィックは、データセンターや地域のハブ サイトなどの中央のロケーションに送信されていました。これにより、インターネットからの戻りのトラフィックが、ブランチに返送される前にセキュリティ機器によってスクラビング処理されます。これにより、あらゆるロケーションにセキュリティ機器を導入することとなり、膨大なコストを必要としていました。

- Cisco SD-WAN は、統合セキュリティにより、ブランチでダイレクト インターネット アクセスをよりセキュアにすることが可能です。
- このアプローチにより、組み込みのセキュリティ機能を使用して、ブランチ サイトからのインターネット トラフィックのフローを一元管理できます。
- これは、インターネットにおける脅威からネットワークを保護し、より優れたアプリケーション エクスペリエンスを実現するのに役立ちます。

その他の参考資料

ダイレクト インターネット アクセスの設定：*http://cs.co/config_local_internet_exit*

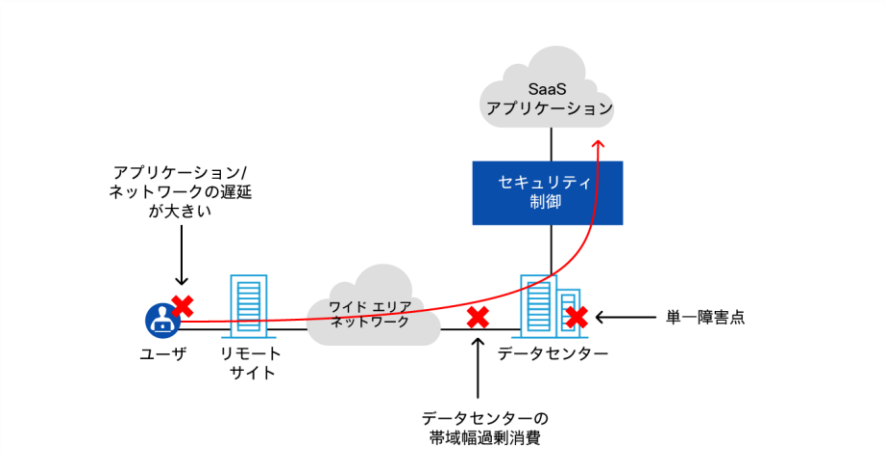
SaaS の最適化

ビジネス ニーズ

エンタープライズ データセンターでホストされている従来のビジネス アプリケーションは、クラウド ベースへと進化を遂げ、Software as a Service（SaaS）として提供されています。SaaS アプリケーションへのアクセスは、インターネット へのアクセス方法によって異なります。適切に設計されたインターネットの出口ポイントは、SaaS アプリケーションを使用する際に最適なユーザ エクスペリエンスを確保するうえで重要な役割を果たしています。残念ながら、既存のワイド エリア ネットワークの大部分は、クラウドを念頭に置いて構築されていませんでした。インターネット宛てのトラフィックは、多くの場合、エンタープライズ データセンターを経由して、そうでなければバックホールまたはヘアピンとして知られている方法で送信されます。この一元化されたインターネット アクセス方法は、従来はデータセンターからのみ提供されていたインターネット宛てのトラフィックに対してセキュリティ制御を提供する必要があるために推進されました。クラウド アクセス用のデータセンターを使用すると、次のような重要な非効率性が生じます。

- アプリケーションとネットワークの遅延が大きい
- データセンターの帯域幅過剰消費
- 単一障害点

図　データセンターを介した従来の一元化されたインターネット アクセス



SaaS アプリケーションへのアクセスやセキュリティ制御がクラウド アクセス用のデータセンターに依存しない、異なるクラウド戦略を採用する必要があります。

Cloud onRamp for SaaS

Software as a Service（SaaS）アプリケーションの使用は、過去 10 年間で増加しています。Cisco SD-WAN ソリューションは、これらのアプリケーションの使用時に最適なユーザ エクスペリエンスを実現するためのネットワーク インテリジェンスを提供します。Cisco SD-WAN ソリューションでは、これを Cloud onRamp for SaaS と呼びます。

最適な SaaS アプリケーション エクスペリエンスを提供するには、最適なパフォーマンスのインターネット出口ポイントへのパスを特定して設計するという課題に対処することが不可欠です。Cisco SD-WAN Cloud onRamp for SaaS は、すべてのサイトに対して次のことを行うことで、これを実現します。

- サイトを特定する
- SaaS アプリケーションを検出する
- SaaS アプリケーションのパフォーマンスを判別する
- 最適なパフォーマンスのパスに沿って SaaS アプリケーション トラフィックをルーティングする
- Quality of Experience（vQoE）スコアについてレポートする

Cloud onRamp for SaaS は、地域のコロケーション施設を統合して SaaS アプリケーション アクセスを多様化することもできます。これは、リモート サイトの 1 つ以上のダイレクト クラウド アクセス ポイントと、コロケーション施設の地域のクラウド アクセス ポイントを選択することで行われます。

サイトを特定する

Cloud onRamp for SaaS ソリューションに参加することを選択したサイトは、次のいずれかの機能を持つものとして指定されています。

- DIA サイト：ローカル ユーザ向けのダイレクト クラウド アクセスが可能なサイト。
- ゲートウェイ サイト：ゲートウェイとして機能するクラウド アクセスが可能なサイト。DIA サイトは、ダイレクト クラウド アクセス全体でパフォーマンスが低下した場合に、ゲートウェイ サイトを使用して、SaaS アプリケーション トラフィックをルーティングできます。
- クライアント サイト：ダイレクト クラウド アクセスができないサイト。これらは、最適な SaaS アプリケーション ルーティングを実行するためにゲートウェイ サイトのみ使用します。

コロケーション センターは、SaaS アクセスを提供するためのゲートウェイ サイトとして使用でき、さまざまな通信、ネットワーク、およびクラウド サービス プロバイダーと直接接続できる柔軟性を提供しながら、コストを削減します。Cloud onRamp for Colocation ソリューションは、Cisco vManage でオーケストレーションを行い、コロケーション施設内のクラスタに導入される、さまざまな VNF サービス チェーンを作成できます。Cloud onRamp for Colocation の詳細については、本書の「*コロケーションの利用*」の章を参照してください。

SaaS アプリケーションを検出する

Cloud onRamp for SaaS は、いくつかの一般的な SaaS アプリケーションに最適なエクスペリエンスを提供します。多くの一般的な SaaS アプリケーションは、地理的に異なるロケーションに分散したクラウド サービス プロバイダーのデータセンターでホストされ、より高い可用性とエンド クライアントへのプロキシミティを実現します。Microsoft Office 365 は、そのようなアプリケーションの 1 つです。Cisco SD-WAN ソリューションは、Office 365 サービスのロケーション（IP アドレス）をプロアクティブに検出するために、WAN エッジ ルー

タからの DNS 解決を利用します。DNS 解決は定期的に繰り返されて、Office 365 サービスの IP アドレスの変更に対応します。この章全体の例として Office 365 が使用されていますが、同じ方法が、他のサポートされている SaaS アプリケーションにも使用されます。

SaaS アプリケーションのパフォーマンスを判断する

Cloud onRamp for SaaS に参加している WAN エッジ ルータは、Office 365 サービスの検出された IP アドレスの Hyper Text Transfer Protocol Secure（HTTPS）要求を使用して、品質調査を継続的に実行します。これらの品質調査は、エンド クライアント アプリケーションの要求を詳細にシミュレートします。これにより、WAN エッジ ルータはエンド ユーザが経験したアプリケーション品質を検出できます。

SaaS アプリケーションのパフォーマンスを判断するプロセスは、すべてのダイレクト クラウド アクセス パス全体にわたる DIA サイトと、地域の SaaS ゲートウェイ サイトで実施されます。WAN エッジ ルータは、HTTPS 品質調査によって検出された損失および遅延特性に基づいて、SaaS アプリケーションに対する最適なパフォーマンスのパスを決定します。ゲートウェイ サイトを使用して SaaS アプリケーションにアクセスするリモート サイトでは、リモート サイトから SaaS アプリケーションへのゲートウェイを介してパス全体のパフォーマンスを測定することで、最適なパフォーマンスのパスが計算されます。

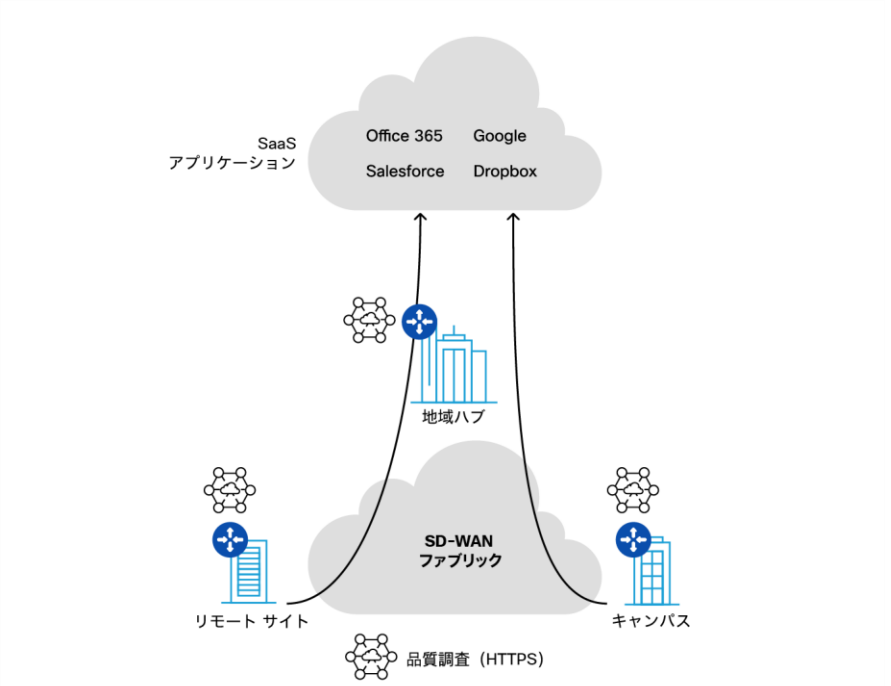
最適な実パフォーマンスのパスに沿って SaaS アプリケーション トラフィックをルーティングする

WAN エッジ ルータは、組み込みのアプリケーション認識機能（ディープ パケット インスペクション（DPI）とも呼ばれる）を利用して、アプリケーションを検出します。DPI エンジンは、1000 を超えるアプリケーションとアプリケーションのサブカテゴリを特定して分類することができます。たとえば、Microsoft のアプリケーション セットには、Exchange、Sharepoint、OneDrive、Skype などが含まれています。

アプリケーションの検出後、WAN エッジ ルータは、その SaaS アプリケーション トラフィックを最適なアプリケーションQoE であるパスへルーティングします。このパスは、ローカル サイトのダイレクト インターネット アクセス回線のいずれか、または SD-WAN ファブリック全体の地域の SaaS ゲートウェイを経由することができます。

品質調査のプロセスは継続的であり、パフォーマンス特性の変化が発生した場合、リモート サイトの WAN エッジ ルータは、選択された SaaS アプリケーションについて高品質のエクスペリエンスを維持するために適切なルーティングの決定を下すことができます。

図 Cloud onRamp for SaaS アプリケーション



Quality of Experience（vQoE）スコアについてレポートする

SaaS アプリケーションを使用する場合のユーザ エクスペリエンスの品質は、1 ~ 10 の範囲で vQoE スコアとして数値化されます。最高は 10 で、最低は 1 です。vQoE スコアは、HTTPS 品質調査によって検出された損失と遅延特性を考慮に入れます。Cloud onRamp for SaaS ソリューションで有効になっているすべての SaaS アプリケーション出口ポイントについて、品質スコアが計算されます。

設計上の考慮事項

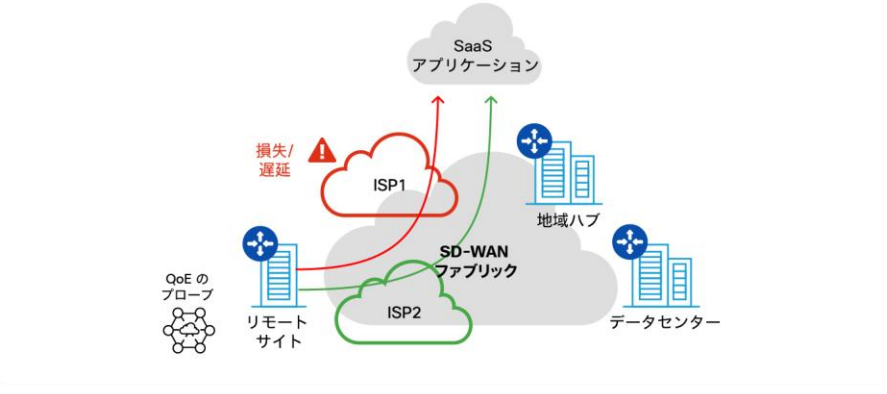
Cloud onRamp for SaaS で使用できる設計の選択肢は 3 つあります。

- ダイレクト クラウド アクセス
- ゲートウェイ クラウド アクセス
- クラウド セキュリティが適用されているダイレクト クラウド アクセス

ダイレクト クラウド アクセス

この場合、Cloud onRamp for SaaS は、リモート サイトで 1 つ以上のダイレクト インターネット アクセス回線を使用します。Cloud onRamp for SaaS は、選択した SaaS アプリケーションに最高のエクスペリエンス品質を提供する回線を動的に選択します。

図　ダイレクト インターネット アクセスを使用する Cloud onRamp for SaaS

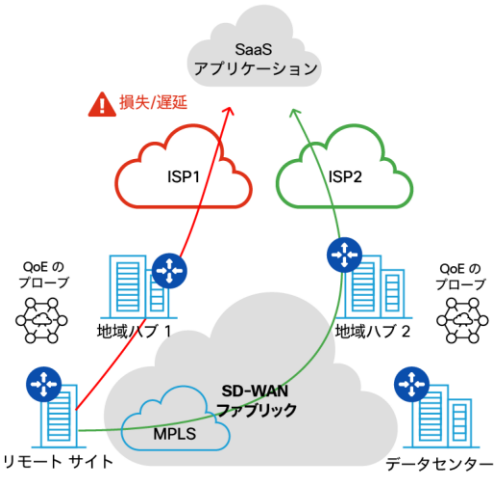


WAN エッジ ルータは、Cloud onRamp for SaaS 向けに設定されたすべてのダイレクト インターネット アクセス回線を介して品質調査を継続的に送信することで、アプリケーションの QoE の変化を検出します。複数のダイレクト インターネット アクセス回線がある場合、WAN エッジ ルータは、最適なアプリケーション QoE スコアを提供する回線に SaaS アプリケーション トラフィックをルーティングします。リモート サイトでのダイレクト インターネット アクセスは、統合された SD-WAN セキュリティ機能によって保護できます。Cloud onRamp for SaaS とリモート ロケーションの SD-WAN セキュリティ制御はどちらも Cisco vManage によって管理されます。

ゲートウェイ クラウド アクセス

ゲートウェイ クラウド アクセスの場合、インターネット アクセスが行われるサイトを、他のサイトの SaaS アプリケーションに到達するためのゲートウェイとして指定できます。ゲートウェイ サイトには、地域のハブ、データセンター、大規模なブランチ、コロケーションなどが含まれます。また、ゲートウェイ サイトをパブリック クラウドに含めることもできます。ゲートウェイは、それらのロケーションの帯域幅、パフォーマンス、およびセキュリティ機能に基づいて選択できます。リモート サイトは、SaaS ゲートウェイ サイトに対する Cloud onRamp for SaaS クライアント サイトとして設定されます。Cloud onRamp は、クライアント サイトからゲートウェイ経由で SaaS アプリケーションまでのパフォーマンスを測定し、トラフィックが最適なパフォーマンスのパスを選択するようにします。

図　地域のゲートウェイを経由する Cloud onRamp for SaaS

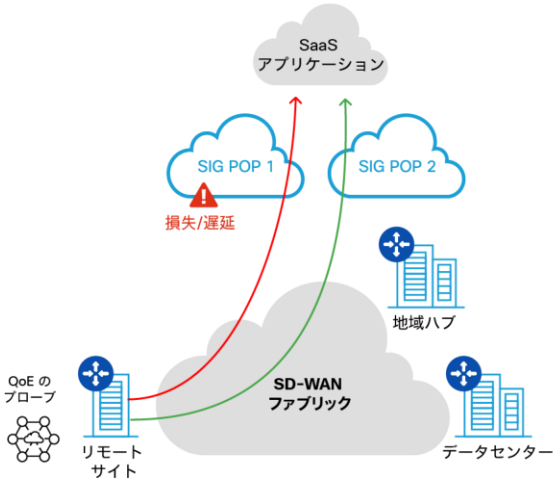


クラウド セキュリティ プロバイダーを介したダイレクト クラウド アクセス

セキュア インターネット ゲートウェイ (SIG) またはクラウド アクセス セキュリティ ブローカ（CASB）は、SaaS アプリケーション トラフィックのセキュリティ ポリシーを適用するためのアプローチです。このモデルは、ブランチやコロケーション施設ではなく、クラウドでセキュリティ制御を利用します。

Cloud onRamp for SaaS は、リモート サイトから 1 つ以上のクラウド セキュリティ エンフォースメント ポイントを介して、最適なアプリケーション エクスペリエンスをパスに提供します。

図　クラウド セキュリティ プロバイダーを介した Cloud onRamp for SaaS



導入事例

この導入事例では、シスコ IT による SaaS の導入に関する SD-WAN の取り組みについて説明します。シスコ IT は、92 ヵ国にまたがるシスコの世界的なネットワーク内のすべての IT サービスを担当しています。ネットワークは、複数のトポロジにわたって 400 を超えるオフィスを接続し、地域のハブに転送して、接続している従業員とパートナーの俊敏なモバイル ワークフォースにビジネスクリティカルなサービスを提供します。

多くのお客様のケースと同様に、シスコのアプリケーションの状況は、データセンター アプリケーションから SaaS モデルで提供されるアプリケーションに移行しています。リモート サイトでプロビジョニングされたダイレクト インターネット アクセス（DIA）回線を介してインターネット トラフィックをオフロードすると、シスコのデータセンターでホストされているアプリケーションのワイド エリア ネットワーク帯域幅を有効活用して、大きなメリットが得られました。シスコ IT は、Cloud onRamp for SaaS を評価して導入し、何百ものリモート ロケーションで 7 万人を超えるユーザが使用している最も重要な SaaS アプリケーション、Salesforce、Box、および Office 365 のエクスペリエンスを最適化しました。

Cloud onRamp for SaaS により、シスコ IT は、SaaS アプリケーションを最適なアプリケーション パフォーマンス特性に基づくダイレクト インターネット アクセス回線に移行することで、エリア ネットワークのキャパシティをカスタマイズできました。QoE スコアでは、ユーザ アプリケーション エクスペリエンスに関する洞察が得られました。Cloud onRamp for SaaS により、シスコ IT は、複数のダイレクト インターネット アクセス回線を同時に使用して、複数の SaaS アプリケーションに動的でインテリジェントにサービスを提供することができました。また、複数の DIA 回線は、SaaS アプリケーションにもある程度の高可用性を提供しました。

最後に、シスコ IT は、DIA 回線全体でセキュリティ制御をすることで、最適なアプリケーション エクスペリエンスと強固なセキュリティ体制との微妙なバランスを取ることができました。

詳細については、Cisco Live ブレークアウト セッション、BRKCOC-1236（*http://cs.co/on-demand-library* [英語]）を参照してください。

主な要点

アプリケーションの状況は変化しており、従来のアプリケーションの利用は、クラウドから提供された SaaS アプリケーションに置き換わっています。この移行は、クラウドを念頭に置いて設置されていない、既存のワイド エリア ネットワーク設計に挑戦を投げかけています。Cisco SD-WAN は、SaaS アプリケーションを最適化する、クラウド対応の使いやすいアーキテクチャを装備しています。Cloud onRamp for SaaS は、SaaS アプリケーションを導入する組織にとって重要な要素です。

Cloud onRamp for SaaS は以下を実現します。

- 使用可能なすべてのトランスポートでプローブ機構を利用することで、SaaS アプリケーションの最適なパス使用率を実現
- 損失と遅延によって損なわれるエンドユーザ エクスペリエンスを向上
- 優れたアプリケーション パフォーマンスを実現

その他の参考資料

- Cisco SD-WAN Cloud onRamp for SaaS：*https://cs.co/onramp*
- シスコ検証済みデザイン（CVD）：Cloud onRamp for SaaS Deployment Guide（Cloud onRamp for SaaS 導入ガイド）：*http://cs.co/onramp-saas-cvd*
- Microsoft Office 365 用の Cisco SD-WAN Cloud onRamp：*http://cs.co/onramp-o365*

パブリック クラウドへの SD-WAN の拡張

ビジネス ニーズ

Infrastructure as a Service（IaaS）は、インターネット経由でエンタープライズ アプリケーションをホストして提供するために使用できる、基本的なコンピューティング リソースのセットです。これには、ストレージ、コンピューティング、ネットワーキングの各コンポーネントが含まれます。IaaS により、オンプレミスの物理データセンター インフラストラクチャは、コンピューティング リソースが Amazon Web Services（AWS）や Microsoft Azure などのパブリック クラウド プロバイダーによってホストされている仮想環境にオフプレミスで移行されます。IaaS により、企業の IT 部門は、いつ、どのように、どのコンピューティング リソースを使用するかを選択し、需要の変化に応じて迅速にスケールアップまたはスケールダウンすることができます。その結果、市場投入までの時間が大幅に短縮されます。

各クラウド プロバイダーは接続に異なるコンサンプション モデルを使用しているため、エンタープライズ ネットワークをクラウド プロバイダー インフラストラクチャに接続することは IT 部門にとって困難です。IT マネージャは、エンタープライズ ネットワークをパブリック クラウドに拡張するための、シームレスで自動化された方法を模索しています。また、企業の IT 部門は、マルチクラウドと物理データセンターおよびブランチ間の単一のオーバーレイ接続も探しています。

エンタープライズ IaaS と Cisco SD-WAN を統合する主な理由は次のとおりです。

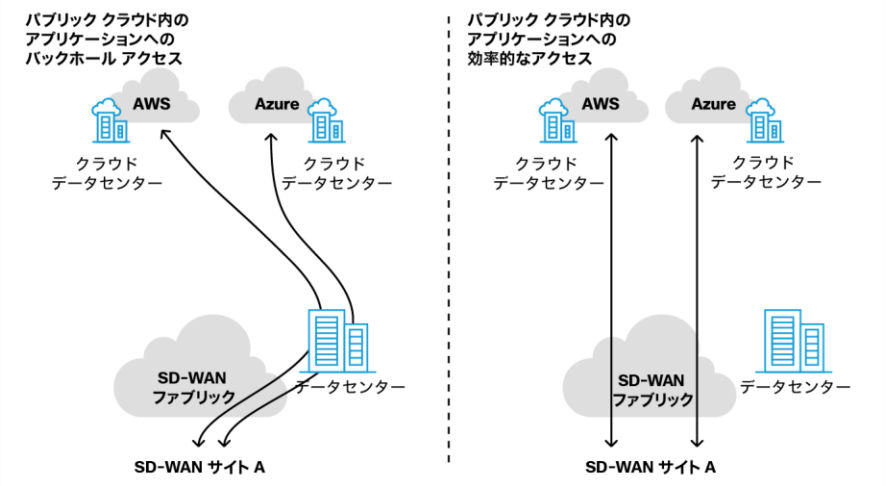
- クラウドで SD-WAN のすべての機能を使用する。
- SD-WAN と複数のクラウドで共通のポリシー フレームワークを適用する。
- Cisco vManage を介してクラウドおよび物理ルータを管理する。
- 最適なインフラストラクチャ セキュリティを確保する。

Cloud onRamp for IaaS

Cisco SD-WAN ソリューションは、ブランチまたはデータセンター（DC）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のに役立ちます。この機能を使用すると、仮想 WAN エッジ ルータのインスタンスは、パブリック クラウドの特定の地域で Cisco vManage を介して自動的に起動されます。これらの仮想インスタンスは、SD-WAN オーバーレイの一部となり、ブランチまたはデータセンターにある WAN エッジ ルータへのデータ プレーン接続を確立します。その結果、クラウド、物理ブランチ、およびデータセンターのワークロード間でエンドツーエンドの接続が確立されます。

Cloud onRamp for IaaS は、SD-WAN ファブリックをパブリック クラウドにシームレスに拡張します。また、データセンターを通過する SD-WAN サイトからのトラフィックを排除することで、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。さらに、Cloud onRamp for IaaS は、仮想ルータの冗長化により、パブリック クラウドでホストされるアプリケーションにパスの復元力と高可用性を提供します。

図　Cloud onRamp for IaaS を使用したパブリック クラウドでの効率的なアプリケーション アクセス



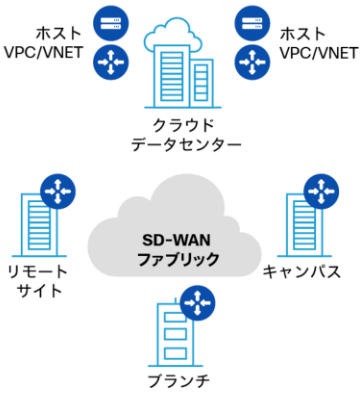
設計上の考慮事項

Amazon Web Services（AWS）と Microsoft Azure は、世界中のお客様が使用する最も一般的な IaaS サービスのうちの 2 つです。Cisco SD-WAN ソリューションにより、SD-WAN ファブリック インテリジェンスを AWS 環境および Microsoft Azure IaaS 環境に拡張できます。これを実現するには 2 つのアプローチがあります。

- クラウド ゲートウェイ：仮想 WAN エッジ ルータは、各仮想ネットワークに手動で導入されます。
- Cloud onRamp for IaaS：仮想 WAN エッジ ルータのペアは、仮想集約ルータとして機能する中継ハブに導入されます。

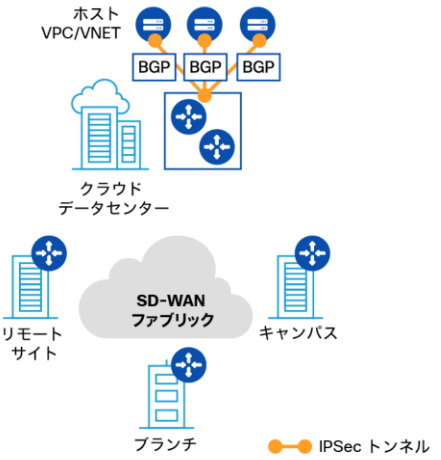
最初のアプローチは、各 AWS 仮想プライベート クラウド（VPC）または Microsoft Azure VNET で仮想 WAN エッジ ルータをインスタンス化することです。この場合、コンピューティング リソースは WAN エッジ ルータ インスタンスに直接接続されます。この方法は非常にシンプルですが、既存の（または新しい）VPC または VNET ごとに WAN エッジ ルータ インスタンスを導入する必要があります。この仮想ルータは、他の物理ルータと同じ方法で、vManage を介してシームレスに管理されます。これは、AWS と Azure Marketplace の両方で、Bring-Your-Own-License（BYOL）インスタンスとして使用できます。

図　クラウド ゲートウェイ



2 番目のアプローチは、Cloud onRamp for IaaS と呼ばれます。Cloud onRamp for IaaS では、中継 VPC/VNET（ゲートウェイとも呼ばれます）をフロントエンドのすべてのホスト VPC/VNET に対して利用できます。ゲートウェイ VPC/VNET は、冗長な WAN エッジ ルータのペアをホストします。標準の IKE ベースの IPSec 接続は、ゲートウェイ VPC/VNET とすべての参加ホスト VPC/VNET 間で確立されます。BGP ルーティング プロトコルは、ホスト VPC/VNET への SD-WAN ファブリック ルートの相互アドバタイズメントのために、これらの IPSec トンネルを経由して実行されます。その逆も同様です。このアプローチでは、ゲートウェイ VPC/VNET が SD-WAN ファブリックへのエントリ ポイントとなり、マルチパス、セキュリティ、セグメンテーション、および QoS が提供されます。また、マルチパスは、AWS Direct Connect または Azure Express Route とインターネット接続を利用することで有効にすることもできます。

図　Cloud onRamp for IaaS

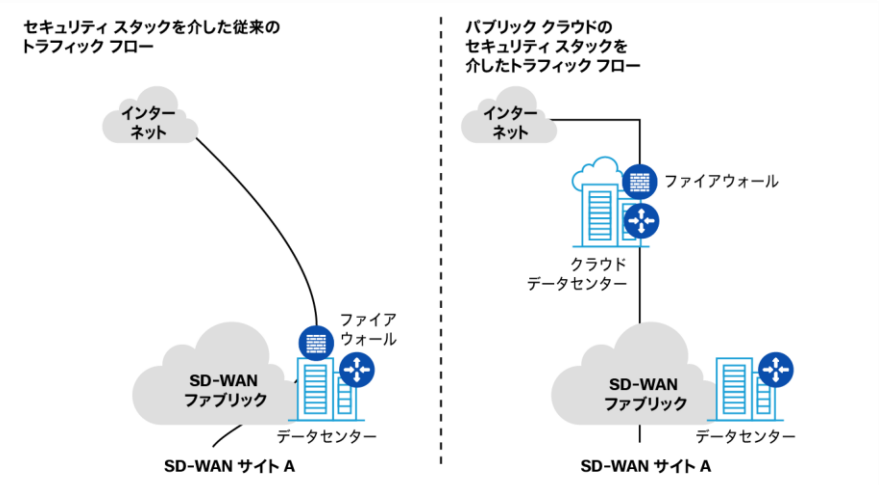


Cloud onRamp for IaaS は、SD-WAN をパブリック クラウドに拡張するために使用できます。また、パブリック クラウドでカスタム セキュリティ スタックを構築するために使用することもできます。

パブリック クラウドでのカスタム セキュリティ スタックの構築

Cisco SD-WAN のお客様は、パブリック クラウド内に独自のセキュリティ スタック（たとえば、ベンダー A からのファイアウォール、ベンダー B からの IPS など）を、VPC または VNET でホストされている仮想ネットワーク機能（VNF）として構築して使用できます。さらに、セキュリティ分析をさらに必要とするインターネット宛てのトラフィックは、SD-WAN ファブリックを介してクラウドで実行されているセキュリティ スタックに送信できます。トラフィックがクラウド WAN エッジに到達すると、セキュリティ スタックを介してフィルタリングされ、インターネットに送信されます。

図　Cloud onRamp for IaaS を使用したクラウド セキュリティ スタック



導入事例

ディストリビュータは、食品および飲料業界において重要な役割を果たし、製造業者とそれぞれの小売店、レストラン、およびフード サービスの顧客の仲介役を務めています。Fortune 500 の全国的な食品流通業者は、単一障害点に対して脆弱になることなく、すべてのリモート ロケーションをクラウドに接続しようとしていました。この要件を実現するには、クラウドベースのアプリケーションの増加に対応するために帯域幅を増やす必要がありました。また、ビジネスのペースが加速し続けているため、オンプレミスのデータセンターから AWS に移行して、柔軟性と俊敏性を向上させることが求められていました。

Cisco SD-WAN および Cloud onRamp for IaaS を使用することで、お客様は WAN にマルチクラウド アプローチを採用することができました。お客様は、AWS マーケットプレイスを通じて vEdge クラウドの仮想インスタンスを起動することで、ネットワーク（ブランチからクラウドへ）をシームレスに拡張し、Cisco vManage を介してすべてのエンドポイントを管理することができました。SD-WAN ファブリックを AWS クラウドに拡張することで、お客様はクラウド内のアプリケーションをネットワークの他の部分と接続できました。

主な利点は、セキュリティ ポリシーの一元管理、導入の容易さによる俊敏性の向上、アプリケーションを顧客に迅速に提供できることなどです。最も重要なことですが、クラウドに迅速に拡張できるということは、ビジネスが資本計画の面で俊敏性を高めることができることを意味します。

主な要点

各クラウド プロバイダーは接続に異なるコンサンプション モデルを使用しているため、エンタープライズ ネットワークをクラウド プロバイダー インフラストラクチャに接続することは IT 部門にとって困難です。IT マネージャは、マルチクラウドと物理データセンターおよびブランチ間の単一のオーバーレイ接続を使用して、エンタープライズ ネットワークをクラウドに拡張するためのシームレスで自動化された方法を模索しています。

Cisco Cloud onRamp for IaaS は以下を実現します。

- パブリック クラウドへの導入を簡素化。
- WAN を複数のパブリック クラウドにシームレスに拡張。
- 自動化により、新規または既存のパブリック クラウドのオンボードに要する時間を短縮。
- パブリック クラウドに移行することで、オンプレミスのセキュリティ設備を縮小し、セキュア ゲートウェイへの最適なパスを提供。
- ブランチ サイトからの暗号化されたダイレクト アクセスを提供して、IT 部門に SD-WAN の導入に対する最大限の選択肢と制御を提供。

その他の参考資料

- IaaS 向けの Cisco SD-WAN Cloud onRamp の設定の概要
  http://cs.co/confgure_onRamp_iaas [英語]

- シスコ検証済みデザイン：Enabling Cisco Cloud onRamp for IaaS with AWS（Cisco Cloud onRamp for IaaS を AWS とともに有効にする）
  http://cs.co/onramp-iaas-cvd

- Configuring Cisco SD-WAN Cloud onRamp for IaaS with AWS（Cisco SD-WAN Cloud onRamp for IaaS を AWS とともに設定する）
  http://cs.co/confgure_onRamp_AWS [英語]

- Cisco SD-WAN Cloud onRamp for IaaS を Azure とともに設定する
  http://cs.co/confgure_onRamp_Azure [英語]

コロケーションの利用

ビジネス ニーズ

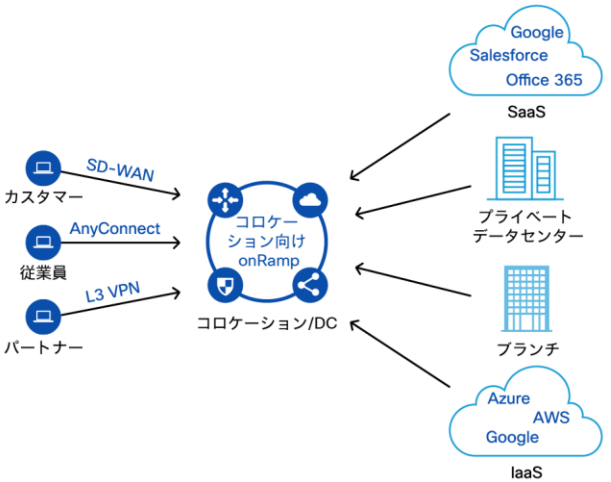
トラフィックの最適化を実現する従来の方法(ロード バランシング、セキュリティ ポリシー、WAN 最適化など) は、データセンターに代表されるような「集約ポイント」に設置された、ファイアウォール、侵入検知/防御センサー、URL フィルタリング、プロキシ等のセンター一元管理型に依存していました。SaaS アプリケーションとインターネット アクセスの場合、このアプローチを使用すると、リモート サイトからメイン データセンターにユーザ トラフィックがバックホーリングされ、アプリケーションの遅延が増加し、全体的なユーザ エクスペリエンスに悪影響を及ぼしました。データセンターでホストされているアプリケーションの場合、このアプローチを使用すると、データセンターの帯域幅リソースが浪費される可能性がありました。さらに、このアーキテクチャ手法では、ウイルス アウトブレイク、マルウェアのエクスプロイト、および内部的に生じる DoS（サービス拒否）攻撃などの、セキュリティ インシデントの効果的な緩和にも課題をもたらしました。

今日では、SD-WAN の時代に移行すると、本書ですでに説明したように、ダイレクト インターネット アクセスの使用による分散型アクセス モデルへのアーキテクチャの移行により、この問題は悪化しています。現在、ブランチとユーザは、上記で強調した集約ポイントをバイパスして、SaaS アプリケーションとインターネット リソースに自由に直接アクセスすることができます。これはポイント A からポイント B にデータを移動する方法として、はるかに効率的ですが、規制機関によってブランチから直接インターネットにアクセスすることが禁止されている IT チームにとっては課題である可能性があります。では、どうすれば一元化されたアーキテクチャのメリットと分散アーキテクチャの効率性を得られるでしょうか。Cloud onRamp for Colocation は、組織がこの問題に対してハイブリッド アプローチを採用できるようにします。それは、戦略的な集約ポイント（コロケーション）を利用し、それによって遅延を最小化し、ネットワーク スタックを統合することで可能になります。

Cloud onRamp for Colocation

コロケーション センターでは、セキュアなパブリック データセンターで機器、帯域幅、またはスペースをレンタルすることができます。これらの施設には柔軟性があり、プライベート データセンターに直接接続するためにかかるコストのほんの一部で、さまざまな通信、ネットワーク、クラウド サービス プロバイダーと直接接続することが可能です。コロケーション センターを利用する最大のメリットの1つは、地理的範囲です。コロケーション施設は、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提供するだけでなく、センターの地理的なプレゼンスにより、エンド ユーザに近接する施設（または複数の施設）を戦略的に選択することができます。したがって、Cisco SD-WAN と組み合わせることで、エンド ユーザ トラフィックは最も近いコロケーションに転送されます。ここで、トラフィックが最適化され、さらに保護され、高速なバックボーンを介してその目的の宛先に転送されます。

図　Cloud onRamp for Colocation



仕組み

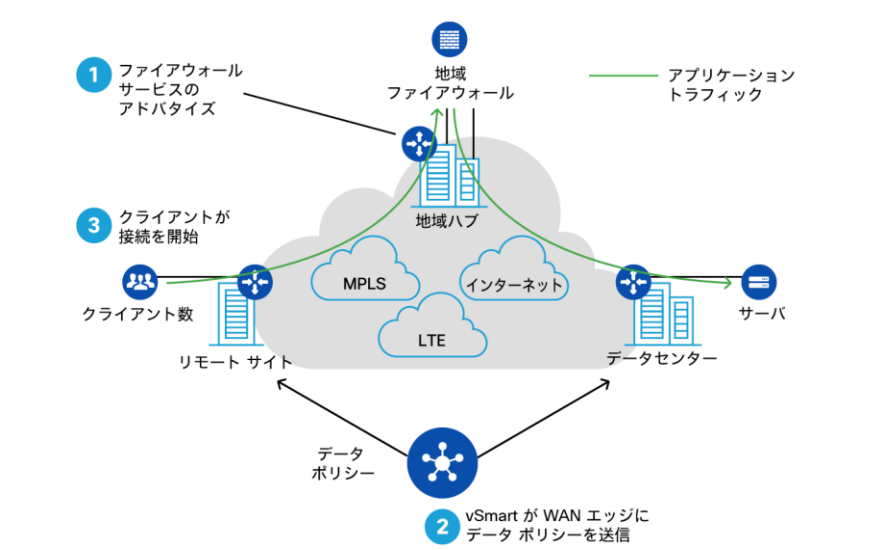
サービス挿入ポリシーとインテリジェント ルーティングを利用することで、Cisco SD-WAN は目的のトラフィックを必要な場所に導くことができます。このコア機能が、地域化されたサービス チェイニングの概念を生み出しました。ネットワーク全体の戦略的なポイントに最適化/セキュリティ ネットワークの要素を配置することで（つまりコロケーション）、地域のサービス チェイニングでは、運用、コスト、アプリケーションの QoE、およびセキュリティ インシデントを効率的に緩和する機能の適正なバランスを取ります。

SD-WAN サービス チェイニングは WAN エッジ ルータによって実行されます。これを「仮想化ブランチの構築」の章に記載されている VNF サービス チェイニングと混同しないようにしてください。ブランチ ルータは、Cisco vManage 内で作成された SD-WAN ポリシーに基づいて、トラフィックを特定し、ペイロードを分析し、コロケーション施設の適切なネットワーク機能を介してトラフィックを操作します。この機能は、インターネット宛先や仮想アプライアンスに限定されないことに注意する必要があります。実際に、サイト間のセキュリティと最適化を提供することを求めている組織は、サービス チェイニングを利用することもできます。

ネットワーク機能（WAN エッジ ルータ、ロードバランサ、IDS/IPS、ファイアウォール、プロキシなど）は、通常、Cisco ENCS やクラウド サービス プラットフォームなどのコンピューティング プラットフォーム内で仮想化/ホストされます。これらの仮想（および場合によっては物理）ネットワーク機能は、VLAN スティッチングまたは物理ケーブル配線によって、WAN エッジ ルータに直接接続できます。これらのアプライアンスは接続されると、OMP を介して SD-WAN ファブリックの他の部分にアナウンスされます。次に、制御およびデータ ポリシーを使用して、これらのアナウンスに基づいて、接続されたリソースを介してトラフィックを制御します。

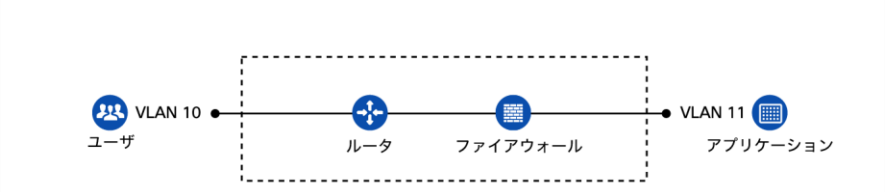
次の図は、データ ポリシーを利用して、ファイアウォールをユーザの中継パスに挿入する方法を示しています。ここでは、Cloud onRamp for Colocation ソリューションが地域のハブ サイトに存在し、ファイアウォール サービスをアナウンスしています。

図　Cloud onRamp for Colocation サービス チェイニング



次の例は、シンプルなルータとファイアウォール サービス チェーンを示しています。

図　サービス チェーンの例



SaaS 向けのサービス チェイニング

これらのアプリケーションはインターネット経由でしかアクセスできないため、SaaS トラフィックはネットワーク アーキテクチャに対して固有の課題をもたらします。分散型インターネット アクセスは、ブランチ ロケーションからダイレクト アクセスできるようにすることで、この問題を解決しました。ただし、組織は SaaS 用のセキュリティ レイヤを追加する必要がある場合があります。Cisco SD-WAN は Cloud onRamp for Colocation と連携して、この要件に対応しています。

Cloud onRamp for Colocation を使用することで、管理者はネットワーク サービスを SaaS 宛のトラフィック パスに挿入することもできます。たとえば、管理者は、データ損失防止センサーを、Dropbox などのファイル共有サービス宛てのトラフィックの中継パスに挿入することができます。ここでは、サービス チェイニング ポリシーを利用することで、管理者は任意の数のネットワーク サービスを使用してこのトラフィックを制御し、これらのサービスが物理アプライアンスであるか、仮想サービスであるかにかかわらず、組織のセキュリティ ポリシーを満たすことができます。

IaaS 向けのサービス チェイニング

IaaS 宛てのトラフィックの中継パス内でネットワーク機能をプロビジョニングすることが望ましい場合があります。対象のトラフィックはネットワーク機能に送信され、そこで処理され、IaaS プロバイダーに転送されます。組織が必要とするセキュリティ レイヤが追加されている場合があります。サービス チェイニングを利用して、Cloud onRamp for Colocation を介してこのトラフィックを保護することができます。

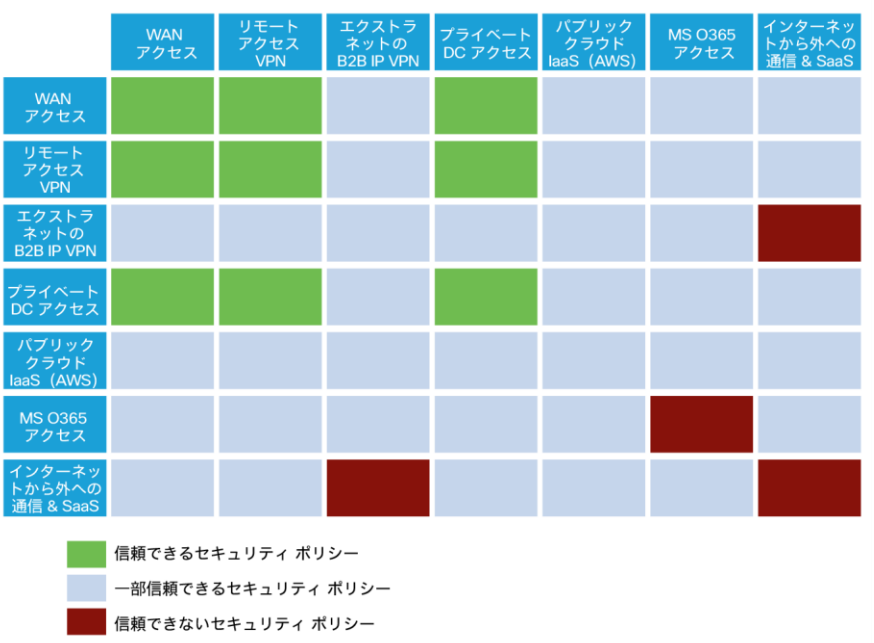
サービス チェイニング設計のベスト プラクティス

Cloud onRamp for Colocation に関する戦略の追求に関心がある場合は、サービス チェーンの設計時に次の段階を検討してください。

- 仮想ネットワーク機能（VNF）を特定する
- トラフィック パターンを特定する
- サービス チェーンを設計する

例として、一般的な顧客ネットワークの分析から、次の接続パターンが出現する場合があります。

図　サービス チェーンの設計



この情報に基づいて、要件を満たすために必要な VNF（または物理アプライアンス）で実行できるのと同様にして、SD-WAN サービス チェイニング ポリシーを導き出すことができます。上の表には、連携動作できないグループ（赤）、連携動作はできるが特定のコントロールがあるグループ（グレー）、および直接連携動作できるグループ（緑）が示されています。たとえば、組織の従業員から送信されるトラフィックのサービス チェーンを作成する場合、そのようなトラフィックのソースは信頼できると見なされるため、ファイアウォールが少なくて済む場合があります。

また、VNF とその配置を選択する際には、次のことを考慮する必要があります。

- コンピューティングのニーズ
- 高可用性（HA）
- ポート チャネリング

最後に、必要なコンピューティングのニーズを評価します。デフォルトでは、Cloud onRamp for Colocation クラスタは、ほとんどのアプリケーションに高スループットと十分なコンピューティング機能を提供します。個々のクラスタは、要件を満たすために拡張できます。

導入事例

多くの組織が統合を求めていて、場合によっては、コスト削減のためにプライベート データセンターを廃止しています。そのようなケースとして、ヨーロッパのあるお客様は、すべてのプライベート データセンターのワークロードをクラウドに移行しようとしていました。それには、トラフィックに対するセキュリティと最適化のポリシーを維持するための効果的な方法が必要でした。これはすでに地域のデータセンターによって提供されていますが、新しいモデルでは地域のコロケーション施設を使用する必要がありました。このお客様は、Cisco Cloud onRamp for Colocation を利用しました。そして、SD-WAN サービス チェイニングを利用してこれらのネットワーク要素を介してトラフィックを制御することで、セキュリティと最適化のインフラストラクチャを仮想化できました。トラフィックは最寄りのコロケーション施設にリダイレクトされ、検査/最適化が行われてから、目的の宛先に向けて高速バックボーンに配置されるため、ブランチ ユーザにとって遅延が最小限になります。

このお客様は、Cloud onRamp for Colocation 機能を利用することで、次のようなメリットを実現できました。

- WAN の俊敏性の向上：WAN サービス チェーンは、動的なビジネス ニーズを満たすために、オンデマンドで導入および廃止できます。
- 遅延の低減：コロケーション施設のバックボーンを利用することで、このお客様はクラウド アプリケーションとの間の遅延を低減することができました。
- 一貫性のあるセキュリティ：Cloud onRamp for Colocation に先立って、このお客様は、ネットワーク内の複数のポイント（データセンター、ブランチ、クラウド サービス プロバイダー）にセキュリティ ポリシーを実装する必要がありました。ただし、このソリューションを利用することで、すべてのブランチ、コロケーション施設、およびクラウド サービス プロバイダー全体にわたり、vManage GUI を使用してセキュリティ ポリシーを一貫して導入できました。

主な要点

企業はマルチクラウド戦略を採用しているため、ユーザ エクスペリエンス、セキュリティ、回線コストの削減、柔軟性の確保のためにトラフィック パターンの最適化を検討する必要があります。マルチクラウド ソリューションの成功は、新しいクラウド エッジ機能に依存しています。クラウド エッジでは、すべてのコンシューマ ネットワークがキャリアに依存しない施設で終了し、最適化ポリシーを一元的に適用することができます。

ここで登場するのが Cisco Cloud onRamp for Colocation です。Cisco Cloud onRamp for Colocation は、ネットワーク エッジを仮想化してコロケーション センターに拡張する機能を提供します。つまり、お客様をクラウドに拡張するのではなく、クラウドをお客様の元に持ち込みます。このソリューションは、企業に対して仮想化、自動化、オーケストレーションを実現します。また、必要に応じてスケールアップおよびスケールダウンできる俊敏性を提供するため、将来の要件や規模に合わせてインフラストラクチャを設計する必要がなくなります。

Cisco Cloud onRamp for Colocation は以下を実現します。

- ロケーションに関係なく、クラウドをブランチに拡張し、ユーザ/デバイス/モノとアプリケーション リソース間の責任分界点として機能。
- 規範的で、ターンキー方式の、柔軟なアーキテクチャであり、カスタマイゼーションよりもシンプルさを検討しているお客様に最適。
- vManage を通じて、SD-WAN と WAN サービス チェーン オーケストレーションのための一元管理 GUI を提供。
- ゼロタッチ導入モデルを提供。
- シスコとサードパーティの両方のデバイスを含むサービス チェイニング モデルをサポート（独自の VNF をカスタマイズするオプション付き）。

その他の参考資料

Cisco SD-WAN Cloud onRamp for Colocation がクラウド戦略の開発にどのように役立つのかを調べるには、次のリソースを参照してください。

- ソリューション ガイド：*http://cs.co/cor-for-colo*
- FAQ：http://cs.co/cor-faq

仮想化ブランチの構築

ビジネス ニーズ

企業やサービス プロバイダーは、ブランチで急増する物理アプライアンスから仮想化インフラストラクチャに移行することにより、運用を合理化し、機器障害を排除しようと試みています。

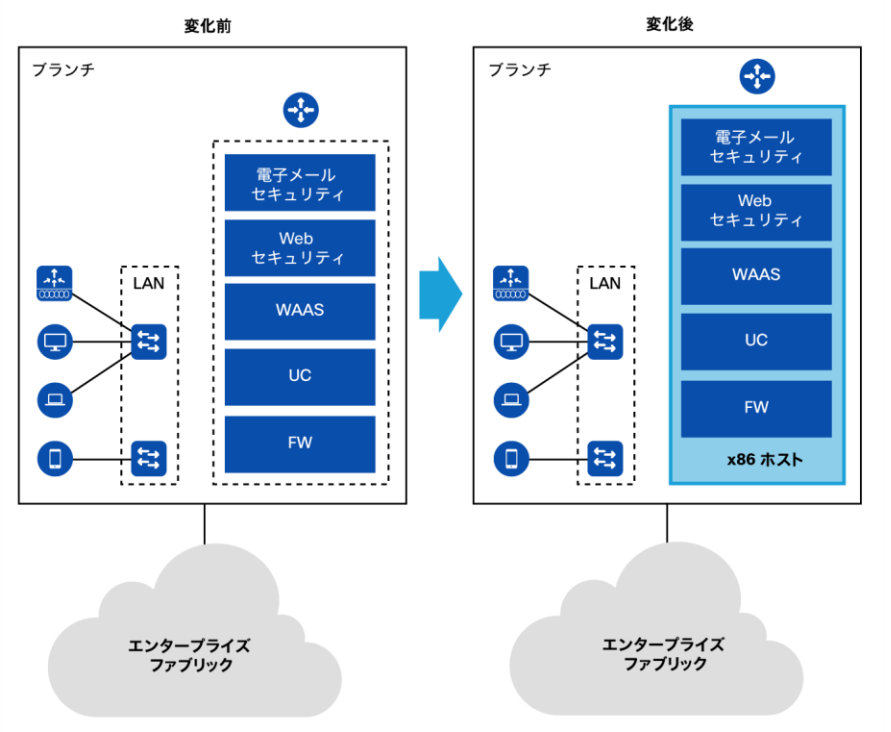
様々なネットワーク機能をブランチ拠点に配備する「マルチサービス ブランチ」を構築するには、それぞれのサービス機能に対応した物理アプライアンス製品を複数、導入することになります。また、それぞれのサービス機能の特性に応じたトポロジを設計する必要もあります。このようなアプライアンス製品として、ルータ、ファイアウォール、WAN 最適化製品などがあります。そして、新機能の追加や既存機能の接続形態の変更など、そのソリューション構成の中で何かを変更するには、多大な労力が必要です。この変更は、追加のケーブル配線からルーティング プロトコルの再設定など幅広い領域に及ぶ可能性があり、リスク、追加のテスト、および展開時間の延長をもたらします。これらすべては生産性に影響を与える可能性があります。

運用の非効率性により、重大な遅延が生じ、ビジネスが中断されるだけでなく、多額のコストが発生する可能性もあります。またさらに、派遣された IT 担当者の派遣に要するコストや、さらに高価な物理アプライアンスのコストもかさむことになります。

ネットワーク機能の仮想化

ネットワーク機能仮想化（NFV）は、マルチサービス環境を構築するための基本要素です。NFV は、ネットワーク サービスを提供する手段として、それを専用ハードウェアではなく、x86 コンピューティング プラットフォームで稼働する仮想化ソフトウェアとして提供します。NFV とソフトウェア定義型ネットワーキング（SDN）を混同してしまうこともしばしば起こります。

図　マルチサービス ブランチの進化



NFV ソリューションは、ネットワーク運用を簡素化して新しいサービスを迅速に提供することで、ビジネス目標の達成に役立ちます。NFV により、ユーザはサービスを実行するコストを削減し、新たな収益もつなげる手段が得られます。NFV を使用することで、汎用ハードウェアでの機能の実行、オーケストレーションによるサービス提供の自動化、容易な拡張が可能になります。

次の表は、設備投資（CAPEX）に関する既知の利点の要約を示しています。

図　仮想化の既知の利点 - CAPEX

動機	説明
標準の x86 ベース サーバの導入	・ルータ/アプライアンスよりも安価と考えられるサーバ ・ブランチ、DC、PoP にすでに導入されているサーバ
ベスト オブ ブリードの導入	・ネットワーク機能の分離により、ベスト オブ ブリードのサービスを実現する ・ベンダーによる囲い込みの廃止 ・ソフトウェア ベンダー間のオープン性と競争を促進する ・競争による CAPEX の削減
スケール メリットによるコスト削減	・DC に大規模なサーバ ファームを導入することで、リソース使用率が向上する
パフォーマンス アップグレードの簡素化	・ハードウェアのアップグレードなしにソフトウェアをアップグレードすることにより、パフォーマンスを向上させる

次の表は、運用コスト（OPEX）に関する同様の要約を示しています。

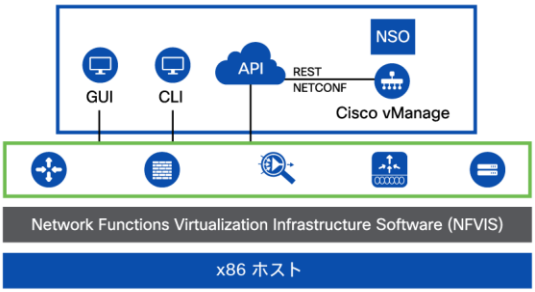
図　仮想化の既知の利点 - OPEX

動機	
ブランチへの担当者派遣の回数の削減	・サービスの変更/アップグレードをソフトウェアで行う ・サービス向けのアプライアンスをオンサイトで交換する必要がなくなる
ネットワーク運用の自動化	・仮想化では自動化と柔軟性に重点が置かれ、これが管理の縮小につながる
VNF ベースの柔軟な運用	・ソフトウェアを個別にアップグレード可能 ・VNF は、ブランチ、DC、または PoP に柔軟に配置できる
組織の境界の排除/縮小	・IT 運用とネットワーク運用の連携

NFV の構成要素

シスコ NFV インフラストラクチャ ソフトウェア（NFVIS）は、導入オプションを自由に選択できる柔軟性を備えています。NFVIS では、ネットワーク サービスを基盤となるハードウェアから切り離して仮想化および抽象化することによって、仮想ネットワーク機能（VNF）を独立して管理したり、動的にプロビジョニングしたりすることが可能になります。NFVIS は、vEdge Cloud、サービス統合型仮想ルータ（ISRv）、仮想 WAN 最適化（vWAAS）、仮想 ASA（ASAv）、仮想ワイヤレス LAN コントローラ（vWLAN）、次世代仮想ファイアウォール（FTDv）などの Cisco VNF をサポートしています。また、NFVIS は、多数のサードパーティ ネットワーク サービスの実行にも対応しています。

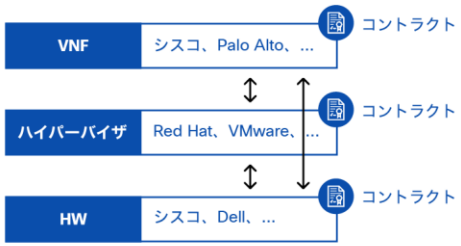
図　NFVIS アーキテクチャ



マルチサービス仮想環境でのサポート

マルチサービス仮想化ブランチでは、ハードウェア アプライアンス、ハイパーバイザ、および個々の VNF に異なるベンダーが存在する場合があります。これにより、導入の管理とサポートに関する課題が生じます。NFVIS と仮想 Cisco WAN エッジ ルータを使用して ENCS を利用する場合、シスコはそのソリューション構成全体をサポートします。また、シスコの NFVIS 認定プロセスでは、互換性のあるサードパーティの VNF をシスコが導入してサポートすることもできます。

図　1 つのソリューションによってサポートを簡素化



1 つのソリューション：VNF + NFVIS + ENCS + Cisco SD-WAN

サービス チェイニング

ここではまず、分かりやすくするために、サービス チェイニングに関連する用語をいくつか定義します。

トラフィック ステアリングは、ネットワークを介して送信されるデータの動作を動的に分析して制御することで、ネットワークのパフォーマンスを最適化する方法です。

*サービス挿入は、ネットワーク サービスのラベルを使用して、特定のデバイスを流れる、目的のアプリケーション トラフィックを、ステアリングするという概念です。*これにより、リモート サイトまたはデータセンターのいずれかでネットワークを再設計する必要なく、ネットワーク パスを変更できます。

VNF *サービス チェイニングは、x86 コンピューティング プラットフォームのトラフィック フローの順序です。*これは、ユニバーサル CPE、またはシスコの仮想化プラットフォーム（エンタープライズ ネットワーク コンピューティング システム（ENCS）、クラウド サービス プラット フォーム（CSP）など）に複数の VNF を実装する場合に特に重要です。

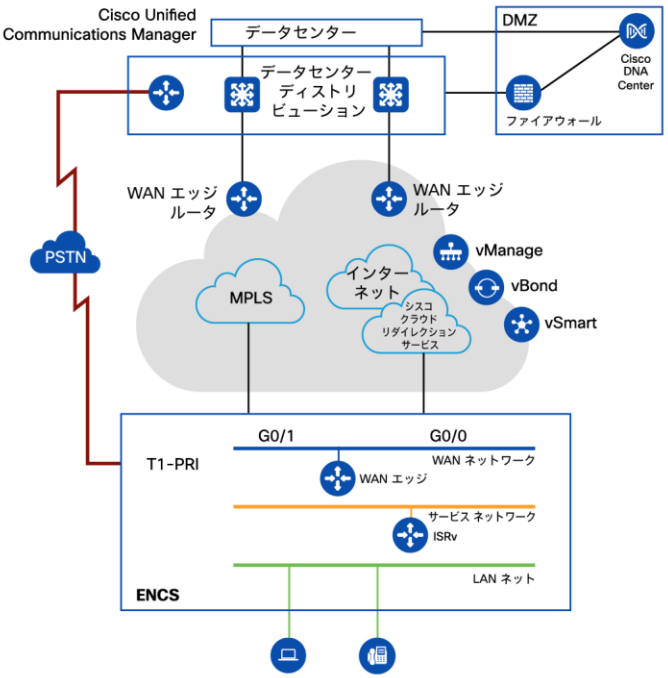
SD-WAN *サービス チェイニングにより、管理者は、ポリシーに基づいて、ネットワーク サービスをユーザの中継パスに挿入可能です。*1 つのアプリケーションの中継パスを操作することも、リモート サイトのトラフィック フロー全体を変更することもできます。ブランチ WAN エッジ ルータで受信されたトラフィックは、Cisco vManage でのプロビジョニングに従い、適切なサービス チェーンを介して転送されます。

導入事例

この導入事例では、2 つの仮想ネットワーク機能を備えたシンプルなソフトウェア定義型ブランチの展開に、Cisco vEdge Cloud と Cisco ISRv の展開が必要でした。Cisco DNA Center が、これらの VNF を、シスコ エンタープライズ ネットワーク コンピューティング システム（ENCS）5412 プラットフォームに実装するオーケストレータとして使用されています。また、Cisco vManage が、SD-WAN のオーケストレータとして使用されています。ENCS アプライアンスは、シスコ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しています。このシナリオでは、ENCS は x86 プラットフォームであり、NFVIS は NFV を実行しているハイパーバイザです。Cisco DNA Center により、VNF が x86 プラットフォームに実装されます。その後、WAN エッジ ルータが vManage に登録され、SD-WAN ファブリックに参加します。

この事例の目的は、この 2 つの仮想ルータをサービス ネットワーク（VNF サービス チェイニング）によって接続することで、ISRv の音声機能と、vEdge Cloud の SD-WAN 機能を組み合わせることです。こうして、1 つの物理デバイス、つまり、SD-WAN と複数の LAN サービスを可能にする 2 つの仮想ルータを備えた ENCS のみを稼働させることで、ラック スペースと運用コスト（OPEX）を節減できます。

図　　ISRv および WAN エッジの VNF による ENCS の展開



ルータの設定や使用されるソフトウェアのバージョンなどの詳細については、次を参照してください。*http://cs.co/nfvis-case-study*

主な要点

技術が進歩し、コスト削減を求めている企業では、ユーザ エクスペリエンス、セキュリティ、柔軟性を向上させるために、トラフィック パターンの最適化を検討する必要があります。ENCS、NFVIS、サービス チェイニングを結び付けた Cisco SD-WAN では、次の機能によって最適化を行えます。

- ネットワーク エッジの仮想化
- vManage による、SD-WAN と WAN サービス チェーン オーケストレーションの簡素化
- シスコとサードパーティ製の両方の VNF をサポート
- 総所有コストの低減
- 必要に応じて、専用アプライアンスのケーブル、ラック、スタックを不要にすることで、スケール アップまたはダウンを実行

その他の参考資料

- ENCS 5400 プラットフォームの詳細については、次のデータ シートを参照してください。
  https://www.cisco.com/c/ja_jp/products/collateral/routers/5400-enterprise-network-compute-system/datasheet-c78-738512.html
- Cisco ENFV のホームページを参照してください。
  https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/enterprise-network-functions-virtualization-nfv/index.html

コンプライアンス要件を満たす

ビジネス ニーズ

新しいビジネス目標が掲げられ、情報セキュリティの脅威が増大するなど、世界が変化する中、デジタル テクノロジー業界では、コンプライアンスを徹底するための厳しい標準が採用されています。法的および規制の枠組みで構成されている標準もあれば、準拠できない場合の厳しい罰則を設けている標準もあります。技術が進歩し、技術に依存するビジネスが増加するにつれ、コンプライアンス要件がさらに複雑になっています。また、増大するコンプライアンス要件を満たし、ビジネスにおけるリスク要因の低減と脅威からの保護を行う必要があるため、ネットワーク オーナー、アーキテクト、管理者、コンシューマに対する圧力がますます高まっています。

Cisco SD-WAN ソリューションにより、コンプライアンスに関する適切な対策を講じることができます。さらに、データを保護し、ユーザから最大限の信頼と信用を得られます。

コントロール プレーンのセキュリティ

Cisco SD-WAN ファブリックのコントロール プレーンでは、ゼロ トラスト セキュリティ モデルが採用されており、ネットワークに接続しようとするファブリックの要素すべてに対して、認証と許可が確実に行われます。このモデルでは、デジタル証明書の使用を基に、ファブリックの各要素のアイデンティティが確立されます。この証明書によって、WAN エッジ ルータとコントローラ間に、Transport Layer Security または Datagram Transport Layer Security（TLS/DTLS）のセキュアなコントロール チャネルが確立します。セキュアなコントロール チャネルの確立後、これらのチャネルを使用して、OMP（Overlay Management Protocol）と NETCONF というプロトコルが実行されます。これにより、コントローラが、設定とネットワーキングの情報を、暗号化されたセキュアなチャネル内に伝達できます。OMP プロトコルは、データ プレーンで使用される暗号化キーを伝達する役割を果たします。

証明書

Cisco SD-WAN では、システムで事前共有キーを使用しません。このソリューションの要素すべてに、信頼できる認証局（CA）によって発行された一意のデバイス証明書が必要です。また、ソリューション内で証明書をさまざまに利用できるように、各 SD-WAN コンポーネントには、複数のベンダーのルート証明書がプリロードされています。

- Avnet
- DigiCert/Symantec
- シスコ

証明書の署名には、DigiCert とシスコの CA ではなく、お客様独自のエンタープライズ CA を選択して、ご利用いただくことも可能です。

SD-WAN コントローラでは、ルート CA によってコントローラに発行された証明書に基づいて、証明書署名要求（CSR）を生成する必要があります。シスコが発行する証明書の大部分

で、コントローラに DigiCert またはシスコの証明書が使用されます。こうした証明書は、コントローラが他のデバイスと通信するために使用されます。

各物理 WAN エッジ ルータには、一意のデバイス証明書が個別にプリロードされています。WAN エッジ ルータの製造時に証明書が発行されます。この証明書は、WAN エッジ ルータの最初の認証および許可プロセス中にコントローラに提示され、ソリューションにおける各ソフトウェア要素のアイデンティティを一意に保証します。

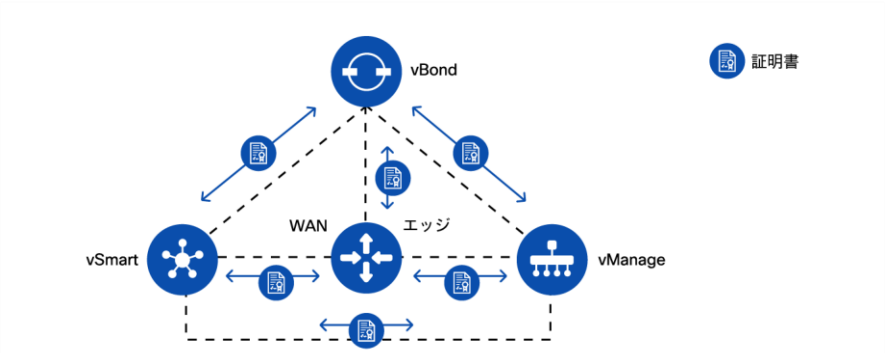
仮想ルータの場合、ルータごとに CSR を生成し、そのルータの有効性を保証する証明書を取得する必要があります。仮想ルータは、自身に発行された 1 回限りのライセンス トークンを Cisco vManage に提示します。vManage はライセンス トークンを検証し、ルータの CSR を生成します。CSR によって、信頼できるルート CA から、そのデバイスに証明書が発行されます。

このような環境を管理制御できるように、SD-WAN ソリューションでは、ホワイトリスト モデルを活用します。これにより、管理者が証明書を環境内で無効にしたり、有効な証明書によってデバイスを拒否したりできます。また、セキュリティ ポリシーの決定どおりに新しい証明書を生成できます。証明書アクティビティのプロセスを簡素化するために、このソリューションでは API を利用可能です。すべてのアクティビティで監査証跡が取得されます。

TLS/DTLS

各 SD-WAN コンポーネントに発行された証明書は、双方向通信を確立する相互認証プロセスに使用されます。各コントローラは、他のコントローラすべてに DTLS または TLS 1.2 接続を確立します。これにより、すべての SD-WAN コントローラが同期できるようになります。ルータがコントローラへの通信を試行した際に、DTLS または TLS 1.2 接続も確立します。その後、こうしたセキュアなトンネルによって、セキュアなデータ プレーンの確立に使用されるルーティング プロトコル、OMP、および隣接関係が確立されます。SD-WAN のコントロール プレーンで使用するハッシュ アルゴリズムでは、SHA256 を活用します。また、このコントロール トンネルに使用する暗号化アルゴリズムには、より高いセキュリティの要件を満たすために AES-256-GCM が採用されています。Cisco SD-WAN ソリューションでは、RFC6347 および RFC5246 で公開されている標準に従って DTLS と TLS を使用します。

図　証明書ベースの認証



OMP と NETCONF

すべてのルータが、すべてのルーティング、ネットワーク ポリシー、暗号化に関する情報のやり取りに OMP を使用して、SD-WAN コントローラと通信します。SD-WAN デバイスは、NETCONF を使用して管理レイヤと通信し、DTLS または TLS のトンネル内で、設定とテレメトリを行います。このトンネルにより、ルーティングの更新情報と暗号化キーが安全な方法で配布されます。

OMP プロトコルにより、コントロール プレーンの利便性が大幅に高まります。OMP は、セキュアな DTLS/TLS トンネル上に確立された、スケーラブルで可用性の高いプロトコルです。このプロトコルにより、デバイスと SD-WAN コントローラ間のすべてのルーティング情報が伝送されます。また、サイト間のキー交換にインターネット キー エクスチェンジ(IKE)プロトコルを使用しなくても済みます。OMP は、N2 の隣接関係を不要にするカスタム プロトコルを確立するとともに、一意の暗号化キー情報を効率的に伝達します。これにより、Cisco SD-WAN 環境では、数十から数千を超えるサイトをつなぐ、きわめて大規模なネットワークを 1 つのオーバーレイで構築可能です。

キー交換

各 WAN エッジ ルータは、そのデータ プレーンの WAN リンクごとに対称暗号化キーとハッシュ キーを生成します。WAN エッジ ルータは、セキュアなオフパス チャネル（OMP チャネル）を使用して、暗号化キーとハッシュ キーを交換し、ルータ間で IPSec セキュリティ アソシエーション（SA）を確立します。こうした暗号化キー/ハッシュ キーは vSmart コントローラに保存/キャッシュされません。vSmart コントローラは、暗号化キーとハッシュ キーをリモート デバイスに反映するリフレクタとしてのみ機能し、リモート デバイス間で IPSec SA を確立できます。WAN エッジのデバイスツーデバイス通信は、AES-256-GCM による IPSec SA を使用して一意に暗号化されます。

データ プレーンのセキュリティ

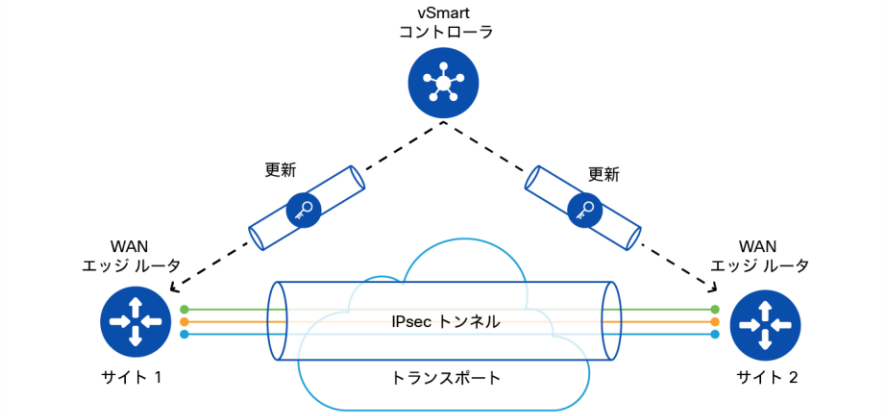
データ プレーン（フォワーディング プレーンとも呼ばれる）は、SD-WAN ソリューションの一部であり、これによって、WAN ネットワーク全体にユーザ トラフィックが伝送されます。ほとんどの SD-WAN ソリューションで、データ プレーンのセキュリティはルータ間での暗号化によって確保されると最も一般的に認識されていますが、それだけでは不十分です。規制機関の多くが、コンプライアンスを目的として、暗号化の他に、トラフィック分離とファイアウォールの両方を求めています。たとえば、Payment Card Industry（PCI）のコンプライアンスでは、万一悪意のあるユーザが意図していないトラフィックを傍受した場合に、それを読み取れないようにすることを義務付けています。同様に、悪意のあるユーザが、PCI 準拠のネットワークにある許可されていないセグメントにアクセスした場合、そのセグメントからアクセスできる宛先が制限されなければなりません。Cisco WAN エッジ ルータは、コンプライアンス確保の取り組みを支援するいくつかの機能を備えています。

暗号化

Cisco SD-WAN ソリューションでは、256 ビットのキー長を使用する、最高レベルの暗号化が可能な Advanced Encryption Standard（AES）を採用しています。Cisco SD-WAN の AES には、Galois/Counter Mode（GCM）と暗号ブロック連鎖（CBC）の 2 つの動作モードがあります。優先モードは GCM ですが、必要に応じて CBC モードをインスタンス化することもできます（マルチキャスト トラフィックの場合など）。

前に説明したキー交換方式に基づいて、次の図に示すように、WAN エッジ ルータ間にセキュアなデータ プレーン通信チャネルが確立されます。

図　セキュアなデータ プレーン通信



従来の IPSec フレームワークでは、インターネット キー交換（IKE）と呼ばれるプロセスを使用する WAN エッジ ルータによって暗号化キーが生成されます。Cisco SD-WAN アーキテクチャ独自のメリットの 1 つは、こうしたキーがコントロール プレーン インフラストラクチャ経由で配布される方法にあります。IKE のプロセスをなくすことで、Cisco WAN エッジ ルータは、コンピューティング リソースをさらに節約し、より高い拡張性を実現します。

ただし、場合によっては、組織外部のサードパーティ ベンダーやビジネス パートナーにデータを送信するときなど、SD-WAN ファブリック外部でのデータ プレーン トラフィックに暗号化が必要になることがあります。こうした状況では、ベンダーまたはビジネス パートナーは、発信側の企業と同じコントロール インフラストラクチャを共有していないため、同じキー配布の方法を使用できません。このため、Cisco WAN エッジ ルータでは、インターネット キー交換（IKE）と呼ばれる従来のキー配布アプローチを採る IPSec トンネルの作成/終了も行えます。IKE は、近年進歩し、安全性が向上しています。IKE バージョン 1 は、デフォルトであり、広く使用されていますが、IKE バージョン 2 よりも推奨されません。それでも、WAN エッジ ルータは両方のバージョンをサポートし、最大限の互換性を提供します。WAN エッ

ジ ルータで IKE ベースの IPSec トンネルを有効にすると、IKE フェーズ 1 の交換において、デフォルトで次のプロパティが有効になります。

- 認証：SHA1-HMAC
- 暗号化：AES-256
- Diffie-Hellman グループ：1、14、15 または 16（デフォルト）
- キー再生成ライフタイム：30 秒から最大 14 日（デフォルトは 4 時間）
- モード：Main（デフォルト）または Aggressive

フェーズ 1 でセキュア チャネルが確立すると、WAN エッジ ルータは、キー生成プロセスを開始し、データを暗号化してリモート エンドポイントに送信します。これを、フェーズ 2 と呼びます。SD-WAN ファブリックと同様に、従来の IPSec VPN では、データ送信用の暗号化アルゴリズムに AES を使用しますが、このパラメータは設定可能です。ただし、動作モードとして使用できるのは CBC 変数のみであることに注意してください。WAN エッジ ルータは、次に示すフェーズ 2 のパラメータを使用して設定できます（デバイス固有の IPSec サポートについては CCO のドキュメントを参照してください）。

- 認証：SHA1-HMAC または SHA2-HMAC
- 暗号化：AES-128 または AES-256

セグメンテーション

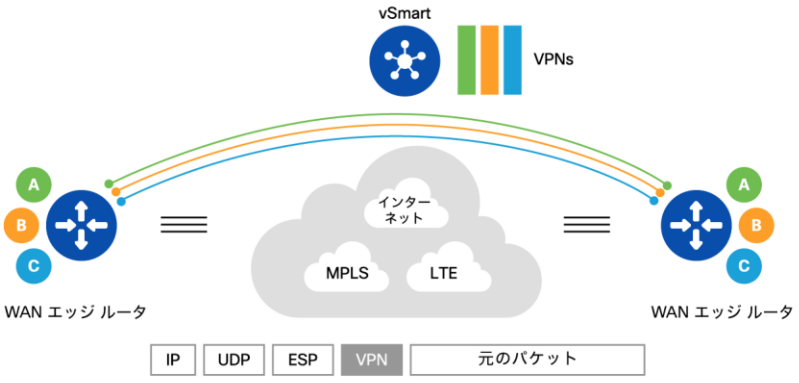
暗号化と同様に、いずれのコンプライアンス戦略でも、トラフィックの分離は重要な要素になります。その理由は、セグメンテーションに基づいてファイアウォール ポリシーを設計する際に、本質的なメリットと運用上のメリットの両方を得られることにあります。Cisco SD-

WAN ソリューションのセグメンテーションは、コントロール プレーンで開始されますが、適用されるのは、データ プレーン内です。ルータで受信されたトラフィックは、VPN に割り当てられます。各 VPN には、数値が割り当てられます（0 ~ 512 の数値。0 と 512 はシステムで使用するために予約されています）。その後、各ルータが、OMP を介してこれらの VPN 値をコントロール プレーンにアドバタイズします。この VPN の割り当てにより、ユーザ トラフィックだけでなく、ルーティング テーブルも分離されます。そのため、デフォルトでは、ある VPN を使用するユーザは、トラフィックを許可する明示的な設定がなければ、他の VPN にデータを送信できません。

ユーザが WAN 経由でデータを送信すると、WAN エッジ ルータはユーザの VPN（ラベル形式を採ります）をトラフィックに追加します。このラベルは、ESP ヘッダーのすぐ後に配置され、ユーザのトラフィックがリモート接続先に到着したときに、そのトラフィックが属する VPN の識別に使用されます。

リモート ルータは、暗号化されたデータのカプセル化を解除した際に、このラベルを使用して、トラフィックの配信先となる VPN を決定します。

図　エンドツーエンドのセグメンテーション



ファイアウォール

データ プレーンのコンプライアンス戦略における最後の要素の 1 つは、適切に設定したファイアウォールです。ファイアウォールによって、許可された宛先のみにユーザ トラフィックが送信され、セキュリティ インシデントが発生した際の監査が可能になります。WAN エッジ ルータは、こうした対応を支援するステートフル ファイアウォールを備えています。

ファイアウォール ポリシーはゾーン経由で適用されます。各ゾーンは、SD-WAN ネットワーク内の 1 つ以上のインターフェイス/ネットワークで構成される VPN です。送信元ゾーンを定義することで、データ トラフィックの送信元となる VPN を特定します。同様に、宛先ゾーンを定義して、トラフィックの送信先となる VPN を特定します。

ファイアウォール ポリシーは、一致とアクションがペアになった一連の番号付きシーケンスで構成されています。これにより、最下位から最上位のシーケンス番号順に評価が行われます。データ パケットが特定の条件に一致すると、関連付けられた 1 つまたは複数のアクションが実行され、そのパケットに対するポリシーの評価が終了します。ファイアウォール ポリシーでは、一致基準として破棄する対象の定義に、送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル、およびアプリケーションのすべてまたはいずれかを使用できます。また、アクションには検査、パス、または破棄のいずれかを指定可能です。

マネジメント プレーンのセキュリティ

Cisco SD-WAN ソリューションでは、vManage ネットワーク管理システム（NMS）によって、マネジメント プレーンを実現しています。vManage は、シンプルなダッシュボード、または Cisco SD-WAN の API を使用して、SD-WAN ネットワークの設定、監視、管理を行えるシステムです。Cisco SD-WAN では、設定やポリシーに対して、誰がアクセス、読み取り、変更を行えるのかを制御することで、管理コンプライアンスを可能にします。これを行うには、ロールベースのアクセス（RBAC）と、アクセス コントロール リスト（ACL）を使用した、送信元 IP アドレスのホワイトリストを定義します。

ロールベース アクセス コントロール

RBAC は、ユーザ権限に基づくアクセス権限の制御に使用され、認証、許可、およびアカウンティング（AAA）アーキテクチャに相当します。vManage でローカルに定義することも、SAML SSO、RADIUS、TACACS プロトコルを使用して、お客様の既存の AAA ソリューションと統合することもできます。

ユーザは通常、異なる権限を割り当てたユーザ グループにグループ化され、環境内でタスクを実行します。

- 「basic」グループには、インターフェイスとシステム情報を表示する権限が付与されています。
- 「operator」グループには、情報を表示する権限のみ付与されています。
- 「netadmin」は、すべての操作を実行できます。「admin」ユーザは、このカテゴリに分類されます。

事前定義された上記のユーザ グループとは別に、お客様は、新しいカスタム ユーザ グループを作成し、各グループに、読み取り/書き込み権限のセットを選択することもできます。

初期設定では、vManage にローカル認証が設定されます。お客様は、SAML SSO/RADIUS/TACACS を介して統合し、多要素認証（MFA）を有効にすることができます。

vManage へのアクセスの制御

ネットワーク管理者は、ホワイトリストのアクセス コントロール リスト（ACL）を作成して、許可した IP サブネットのみ vManage にアクセスするように制限できます。これにより、vManage にアクセスできる、ネットワーク内のデバイスを制御する方法として、RBAC の他に別のセキュリティ レイヤが追加されます。

たとえば、vManage にアクセスできる送信元 IP サブネットを 172.2.0.0/16 のみにする場合、172.2.0.0/16 を許可するシンプルな ACL を定義することで、そのように制限できます。これで、許可していないユーザ、または侵害されたデバイスが 172.2.0.0/16 以外から vManage にアクセスすることを防ぎます。

プラットフォーム コンプライアンス

Cisco SD-WAN ソリューションは、セキュアなプラットフォームに構築されます。プラットフォームのコンプライアンス要件では、以下の側面が重視されます。

- ハードウェアのコンプライアンス
- ソフトウェアのコンプライアンス
- ソリューションのコンプライアンス

このセクションでは、これらのトピックを取り上げます。まず、安全で信頼できる方法による個々のハードウェア コンポーネントの構成について、その後、ソフトウェア開発プロセス、および SD-WAN ソリューションのコンプライアンスについて説明します。

ハードウェアのコンプライアンス

トラステッド プラットフォーム モジュール（TPM、ISO/IEC 11889 とも呼ばれます）は、セキュアな暗号化プロセッサの国際標準であり、統合された暗号化キーによってハードウェアを保護するために設計された専用のマイクロコントローラです。WAN エッジ ルータは、TPM チップ内の証明書/RSA キーを使用して自身を認証し、SD-WAN ネットワークに参加します。各 TPM チップには、一意の秘密 RSA キーが製造時に組み込まれているため、ルータに保存されているキーを変更できないことが保証されています。

Cisco vEdge ルータ

Cisco vEdge ルータは 5 段階のプロセスを経て製造されます。これには、デバイスの TPM ハードウェアにデジタル証明書を組み込むプロセスも含まれます。

1. vEdge ルータで、秘密キーと公開キーを生成する。
2. 証明書署名要求を生成する。

3 Avnet が証明書に署名する（25 年間有効）。

4 証明書を vEdge ルータの軽量な TPM チップにロードする。

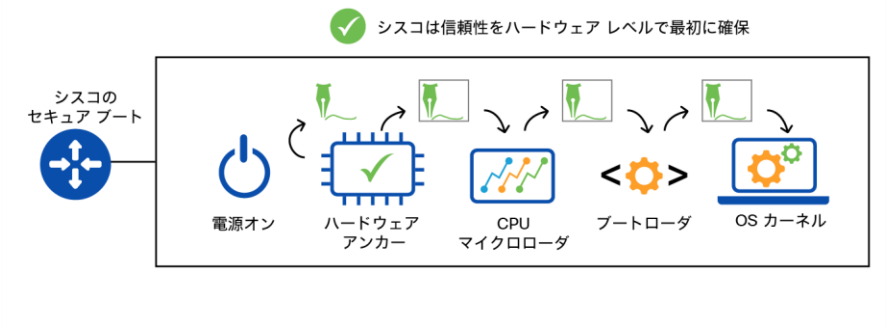
5 Cisco vEdge ルータが、DigiCert ルート証明書のルート CA 信頼チェーンと、シスコの CA ルート証明書が組み込まれた状態で出荷される。これらが、コントローラとリモート WAN エッジ ルータの認証に使用される。

Cisco IOS XE WAN エッジ ルータ

Cisco IOS XE ベースの WAN エッジ ルータは、セキュアな固有デバイス識別子（SUDI）を使用する信頼できるシステムです。

- SUDI は、関連付けられたキーペアを使用する X.509v3 証明書です。キーペアは、ハードウェア内で保護されています。
- Cisco IOS XE ベースの WAN エッジ ルータは「信頼できるシステム」です。つまり、期待どおりの検証可能な方法で稼働します。
- 信頼性の高い主要な技術に、イメージ署名、セキュア ブート、ランタイム防御、Cisco Trust Anchor モジュール（TAm）などがあります。これらが、偽造ハードウェアとソフトウェア変更を防止します。具体的には、セキュアで暗号化された通信のほか、プラグアンドプレイ (PnP) とゼロタッチ プロビジョニング (ZTP) を可能にします。
- シスコのセキュア ブートにより、シスコのハードウェア プラットフォームで実行されるコードが本物で、改ざんされていないことを確認できます。
- ハードウェアアンカーの信頼ルートと、デジタル署名されたソフトウェア イメージを使用する、シスコのハードウェアアンカー セキュア ブートによって、信頼チェーンが確立されます。これにより、システムが安全に起動し、各ステップでソフトウェアの完全性が検証されます。

図　　シスコ セキュア ブート プロセス



仮想化ネットワーク機能における信頼性の確保

SD-WAN の仮想ネットワーク機能 (VNF) は、アプライアンスのハードウェアが、ハードウェアアンカーのセキュア ブートを適用する TAm などの適切な組み込みのセキュリティ機能を備えている限り信頼できます。ルーティング アプライアンスが、セキュアなデータセンターに配置されていても、リモート サイトでゼロタッチ運用によってインストールされていても、またはクラウド コロケーション ファシリティで稼働していても、シスコのハードウェアは、エンドツーエンドのセキュリティと信頼性を備えた VNF をサポートします。

ルーティングやセキュリティなどのクリティカルな仮想化機能の実行に適したハードウェアを選択する場合、ハードウェア エコシステム全体を最適化して、SLA をサポートするために必要なパフォーマンス レベルと、アプリケーションに期待される Quality of Experience（QoE）を達成することが重要です。高速ギガビット ルーティングと、暗号化トラフィックのリアルタイム分析に関して言えば、パフォーマンスは処理能力以上の意味を持ちます。複雑なルーティング機能用のカスタム ASIC を設計し、フィールドでの更新をサポートする Field Programmable Devices（FPD）を採用することで、シスコは、ネットワーク ワークロード、セキュリティ分析、リモート オーケストレーション向けに、ハードウェアを微調整しています。

ソフトウェア イメージの署名

イメージ署名では、2 段階のプロセスを経て、特定のコード ブロックに一意のデジタル署名を作成します。まず、チェックサムに似たハッシュ アルゴリズムを使用して、コード ブロックのハッシュ値を計算します。その後、ハッシュをシスコの秘密キーで暗号化してデジタル署名を作成し、それを追加したイメージを提供します。起動中に、署名付きイメージをチェックして、そのソフトウェアが改ざんされていないことを確認します。

デジタル署名付きシスコ ソフトウェアでは、システムで実行するソフトウェアが、改ざんされておらず、その提供元が信頼できることを確認できます。それにより、Cisco IOS デバイスにおけるセキュリティ ポスチャが強化されます。管理者は、SHA512 または MD5 チェックサムの確認により、バイナリ ファイルの信頼性と完全性を検証できます。

データ保持

記録管理と記録保持ポリシー

シスコは、国固有のビジネス、法律、またはグローバルな規制上の義務に基づいて保持期間を定義する、エンタープライズ記録保持スケジュール（ERRS）を維持しています。ERRS では、企業全体の記録管理を標準化し、ライフサイクル全体でのデータ保持を支援します。ライフサイクルの終了時には、保持要件、および記録が保存されているメディアに基づく情報廃棄ポリシーに従って、記録が、適時、効率的に安全な方法で廃棄されます。

個人情報

個人データを処理するユーザは、次の方法で、ソリューションのユーザ インターフェイスにサインインすることができます。

- シスコ以外のシングル サインオン（RADIUS または TACACS）。この場合、個人データは、ユーザが指定したサードパーティ SSO 事業者により処理されます。
- シスコ シングル サインオン（SmartAccount）。この場合、個人データは、シスコ スマート アカウント サービスによって処理されます。

シスコがホストする SD-WAN コントロール インフラストラクチャ内に保存されているデータはすべて、暗号化されたディスクによって保護されます。

Cisco SD-WAN で使用するユーザ名とパスワード

ユーザ名とパスワードは、シスコがホストする、お客様の SD-WAN アカウントで保持されます。IP アドレスと、その他の一意の識別子は、サインオン プロセス中に、Cisco SD-WAN によってキャプチャされません。

お客様は、アカウント設定によって個人データを削除することができます。シスコは、お客様がアクティブな Cisco SD-WAN サブスクリプションを保有している間、お客様に代わって、そうした削除を行うことはできません。ただし、お客様の Cisco SD-WAN サブスクリプションが期限切れになった、または終了した 60 日後に、シスコは、お客様保有の個人データを含む、SD-WAN コントロール インフラストラクチャ全体を自動的に削除します。

データ分類ポリシー

シスコには、データの分類、ラベリング、保護の要件を定める、正式なポリシー、関連する標準、ガイドラインがあります。これに含まれる、一般的なガイドラインと意思決定ツリーは、データの分類に役立ちます。また、個人に、データ アクセスとデータ利用に対する正当なビジネス目的（把握が必要な目的）があるかどうかの判断を容易にします。

グローバルの状況

本書では、地域と国固有の規制要件、またはコンプライアンスに関する考慮事項すべてを網羅してはいません。本書では、次の地域/国を含む世界中で、Cisco SD-WAN ソリューションが成功裏に導入されたことを紹介します。

- 北米
- ヨーロッパ
- 中国
- ロシア

Cisco SD-WAN では、汎用のクラウド サービスを活用しています。お客様の環境に適した地域固有のデータセンター（オーストラリア、ブラジル、ドイツ、インド、アイルランド、日本、シンガポール、米国）を選択できます。

シスコは、複数の司法管轄区域にまたがる合法的なデータの使用を可能にするための複数の輸出入制度に準拠しています。特に、次の制度が挙げられます。

- シスコ社内ルールへの適合
- EU-米国間のプライバシー シールド フレームワーク
- スイス-米国間のプライバシー シールド フレームワーク
- APEC クロスボーダー プライバシー ルール
- EU 標準契約条項

主な要点

新しいビジネス目標が掲げられ、情報セキュリティの脅威が増大するなど、世界が変化する中、デジタル業界では、コンプライアンスを徹底するための厳しい標準が採用されています。また、増大するコンプライアンス要件を満たし、ビジネスにおけるリスク要因の低減と脅威からの保護を行う必要があるため、ネットワーク オーナー、アーキテクト、管理者、コンシューマに対する圧力がますます高まっています。

- Cisco SD-WAN ソリューションでは、ソリューションのコンポーネントごとに対策を立てるという包括的な方法で、コンプライアンスに取り組んでいます。
- コントロール、データ、マネジメント プレーンといった各 SD-WAN 技術のコンポーネントを、革新的な手法、業界標準、最高レベルの暗号化アルゴリズムを組み合わせて強化しています。
- SD-WAN ソリューションは世界中で導入され、行政機関と規制機関のさまざまなコンプライアンス要件を満たしています。

その他の参考資料

プライバシー データ シート：*http://cs.co/SD-WAN-privacy-datasheet*

Cisco SD-WAN への移行

ビジネス ニーズ

企業は、新しいソリューションや、収益を生むサービスにシームレスに移行することを求められています。市場投入までの時間の短縮、リスクの軽減、既存のサービスやアプリケーションへの影響を最小限に抑えることは、いずれも、お客様の移行戦略における要因と言えます。WAN への移行それぞれが、特定の環境固有のものであっても、Cisco SD-WAN なら、上記の要件を妥協せず、シームレスに移行を完了できます。

組織のビジネス目標がどのようなものになるかを把握することが重要になりますが、それについては、Cisco SD-WAN への移行を進めながら検討できます。次に例を示します。

- トラフィックの優先順位付けとトランスポートの選択
- WAN のコスト削減と帯域幅の増強
- セグメンテーション
- セキュアなダイレクト インターネット アクセス
- ゲスト アクセス

移行計画

SD-WAN への移行はネットワーク アーキテクチャの変更を伴うため、計画の立て方が非常に重要です。

移行前に、ネットワークの現在のアーキテクチャを理解する必要があります。現在のハードウェアとソフトウェア、トランスポート、アプリケーション、トラフィック フローを特定します。SD-WAN ネットワークを適切に設計するには、現在の帯域幅要件のベースラインを定義し、将来の成長を示すことが重要です。

Cisco SD-WAN ソリューションの効果的な移行と導入を計画する際に考慮すべき事項を以下に示します。

コントローラの考慮事項

クラウドホスト型やオンプレミスといった導入モデルを選択する必要があります。サイジング、拡張性、冗長性は、準備フェーズにおいて、非常に重要な意味を持ちます。一般的な検討事項を以下に示します。

- Cisco vManage、Cisco vBond、および Cisco vSmart コントローラの数量
- コントローラの配置先
- Cisco vManage クラスタ化の必要性

SD-WAN コントローラは、地理的に冗長なデータセンター、またはクラウドのリージョンに展開されます。このように分散展開することで、コントロール プレーンとマネジメント プレーン インフラストラクチャの可用性と復元力を高めています。適切なコントローラ設計により、数十から数千のロケーションに拡張可能なネットワークを展開できます。

データセンター設計の考慮事項

WAN エッジ ルータを導入する場合、インターネットおよびプライベート回線が、データセンターのロケーションでヘッドエンド ルータにどのように接続されるかを、その計画によって示す必要があります。

パスの対称性を維持し、ループを確実に回避するために重要なのは、データセンターのルーティング プロトコルへの統合です。Cisco SD-WAN では、インテリジェントな制御によって、BGP、OSPF、EIGRP をベースとするデータセンター環境に統合できます。データセンターの移行では、SD-WAN のオーバーレイとすべてのアンダーレイ ネットワーク間におけるルーティング ポリシーを策定し、SD-WAN サイトと 非 SD-WAN サイト間でどのようにトラフィックが処理されるかを示すことが重要です。

地域/ブランチ設計の考慮事項

シンプルとは言え、ブランチ ネットワークの設計は、SD-WAN で利用可能なさまざまなオプションを実装するのに、最も適しています。たとえば、プライベートまたはインターネットベースの回線を追加する機会を得られます。LTE をバックアップ回線として統合する絶好の機会でもあります。LTE の統合では設計上、使用可能な帯域幅の有効利用とともに、従量制課金回線での不要な使用防止を検討することになります。WAN の変更に加えて、可用性の高いサイトを構築し、ブランチに新しいサービスを導入することも、設計上の主な考慮事項です。

ポリシーの考慮事項

SD-WAN の技術により、さまざまなサイト間で任意のトポロジを作成できます。そのネットワーク トポロジでは、アプリケーションの動作を定義する必要があります。また、既存のビジネスクリティカルなアプリケーションとそれに関連する QoS 設定を明確に把握することも重要です。そうすることで、アプリケーション パスを SD-WAN ファブリック全体で最適化する SLA を定義できます。

セグメンテーションなどのセキュリティ機能を追加することで、さまざまな基幹業務を分離し、セグメントごとにカスタム ポリシーを作成できます。一般的な利用例として、ダイレクト インターネット アクセスを実装し、必要なセキュリティ ポリシーを有効にすることが挙げられます。これにより、セキュリティ リスク放置箇所の拡大を伴わずにカスタマー エクスペリエンスが向上します。

クラウドの考慮事項

SD-WAN の技術では、ネットワークをクラウドに拡張できます。その場合、IaaS にアクセスするためのルーティングに関する検討事項、関係する地域のほか、SD-WAN ファブリックに Microsoft ExpressRoute や AWS Direct Connect などのプライベート クラウド接続モデルを採用する必要があるかどうかを把握することが重要です。SaaS のエンドポイント、特に Office 365 とそれを構成するアプリケーション スイートがある場合、最適化が必要な SaaS アプリケーションと、アプリケーションに求められる帯域幅の量を特定しなければなりません。そうすることで、理想的なアプリケーション エクスペリエンスを提供するポリシーを設定した SD-WAN 環境を構築できます。

管理と運用に関する考慮事項

RADIUS、TACACS、または SSO の要件は、移行に大きく影響する可能性があります。また、既存のモニタリング ツールとワークフローを明確に表して、設計に組み込めるようにする必要があります。Cisco SD-WAN ソリューションは、API、SNMP v2c/v3、Syslog、NETCONF、および NetFlow によるモニタリングをサポートしています。つまり、このソリューションを、移行の一環として、既存のインフラストラクチャに統合できます。

その他の考慮事項

Cisco SD-WAN には、その他にも多くの機能があり、そうした機能を導入するには、独自の計画が必要です。たとえば、IPv6 とマルチキャスト トラフィックは、一部の環境で使用される独自のシナリオです。SD-WAN を IPv6 機能の導入手段にすることは、多くの場合、重要な考慮事項です。また、SD-WAN ネットワークでマルチキャスト機能を維持または拡張する

には、プロトコルの実行環境、マルチキャスト ストリームの送信者と受信者、およびそれらをサポートする帯域幅の要件を把握する必要があります。

その他の前提条件

移行ステップを開始する前に、次の要因も考慮していることを確認します。

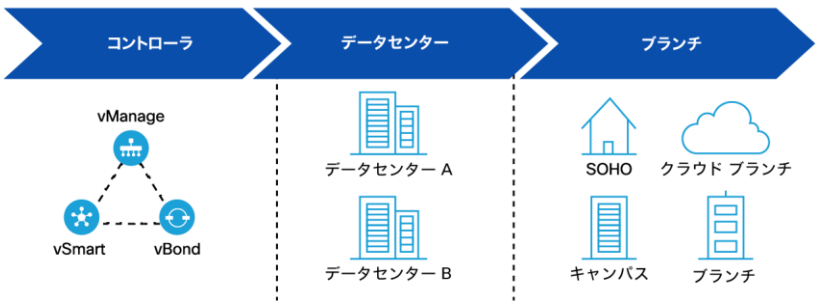
- ファイアウォール ポート：Cisco WAN エッジ ルータとコントローラ間には、DTLS 接続と TLS（オプション）接続が必要です。これらの接続を確立できるように、ファイアウォール ポートを適切に開いていることを確認します。
- ハードウェア サポートの要件を確認します。必要に応じて、既存の IOS XE ASR/ISR ルータに IOS XE SD-WAN ソフトウェアをインストールします。
- http://software.cisco.com にある PnP Connect ポータルを活用して、WAN エッジ ルータがスマート アカウントとバーチャル アカウントに関連付けられていることを確認します。PnP Connect ポータルから取得したデバイス許可ファイルは、Cisco vManage に手動でインポートできます。または、Cisco vManage を PnP Connect サービスと自動的に同期させることができます。

詳細については「その他の参考資料」セクションを参照してください。

移行戦略

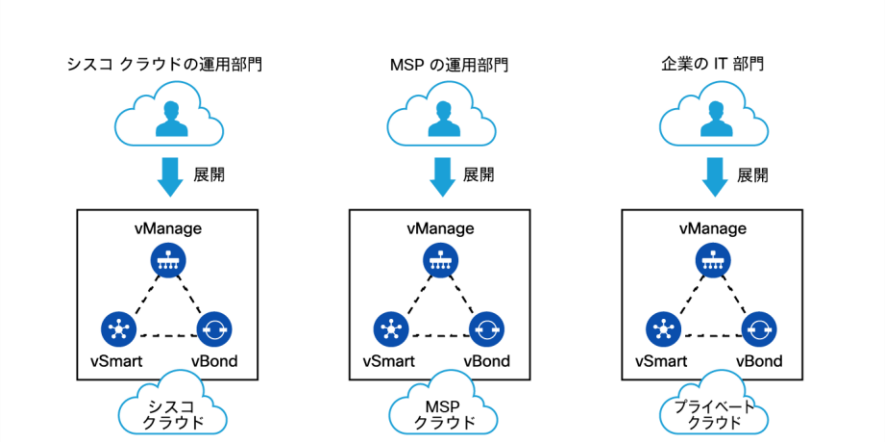
SD-WAN への移行では、次の図に示すように、まず SD-WAN コントローラの展開、次にデータセンターでの SD-WAN の展開、最後にブランチでの SD-WAN の展開を行います。

図　SD-WAN の移行順序



Cisco SD-WAN コントローラは、シスコがホストするクラウド、MSP/パートナーがホストするクラウド、または組織が管理するデータセンター内オンプレミスのいずれかに展開できます。導入モデルは、組織における選択、またはマネージド サービス契約によって異なります。

図　Cisco SD-WAN コントローラの導入モデル



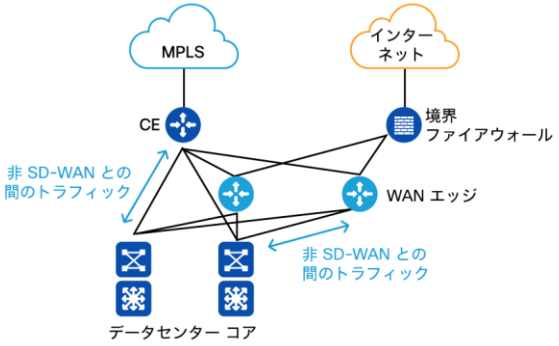
いずれのコントローラ導入モデルでも、同等の SD-WAN 機能を得られます。

データセンターの移行

通常、データセンターが、SD-WAN に移行する最初のサイトとして選択され、最初の SD-WAN ファブリックの入り口が確立されます。最も一般的な移行シナリオでは、データセンターが中継ハブとして機能し、SD-WAN と非 SD-WAN サイト間のトラフィックをルーティングします。また、データセンターでホストされているアプリケーションとサービスへのアクセスを引き続き可能にします。

WAN エッジ ルータは、SD-WAN ファブリックのヘッドエンドとして機能します。通常、MPLS カスタマー エッジ（CE）ルータの「背後」に展開され、DMZ を介して、データセンター境界のファイアウォールを経由し、インターネットに接続されています。これにより、WAN エッジ ルータは、リモート サイトに接続する SD-WAN ファブリックを、すべてのトランスポートで確立できます。また、データセンターのコア レイヤ/ディストリビューション レイヤに接続されています。

図　Cisco SD-WAN のデータセンター トポロジ

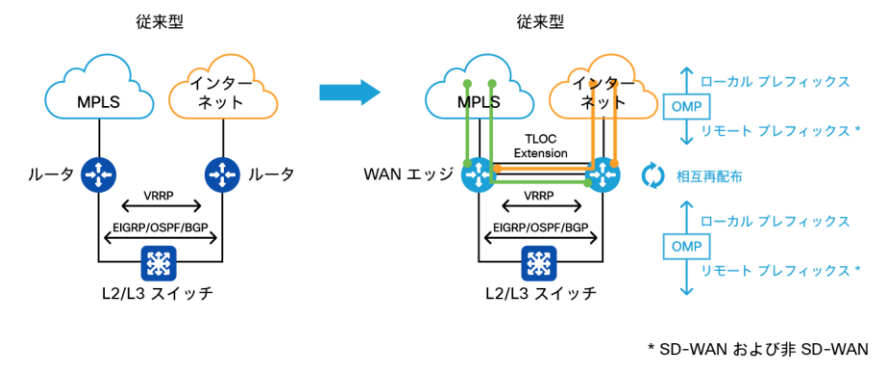


ブランチの移行

ブランチ サイトでは、WAN 回線の種類と数、および高可用性の設計要件に応じて、異なるトポロジを設定できます。

単一のルータを使用するサイトの場合、ルータを IOS XE SD-WAN ソフトウェアにアップグレードして、サイトを SD-WAN に転換することができます。2 台のルータを使用するサイトの場合、両方のルータを IOS XE SD-WAN ソフトウェアにアップグレードして、サイトを SD-WAN に転換可能です。または、段階的なアプローチを採り、ルータを 1 つずつアップグレードしても構いません。この場合、ソフトウェア アップグレードの間、ユーザ トラフィックを、移行していないルータに移動する必要があります。両方のルータでアップグレードが完了したら、高可用性を設定して、アクティブ/アクティブ方式で動作させることができます。

図　2 台のルータを使用する SD-WAN ブランチへの移行

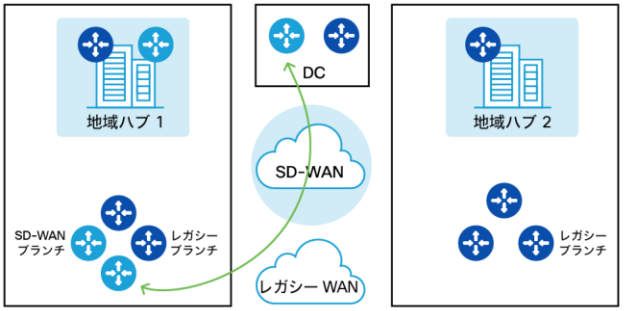


詳細については、この章の「その他の参考資料」セクションに記載のリンクを参照してください。

トラフィック フロー

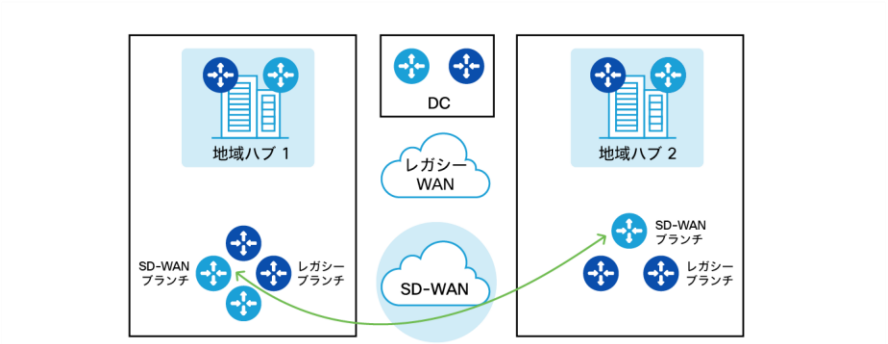
このセクションでは、SD-WAN への移行中に、地域間で設定される、トラフィック フローのさまざまなシナリオについて説明します。SD-WAN と非 SD-WAN 間の通信は、移行期間全体で、そのまま継続します。移行済み、および移行されていないブランチ間の通信は、地域のハブ、またはデータセンターを介して行われます。

図　ブランチとデータセンターのトラフィック フロー（SD-WAN 経由）



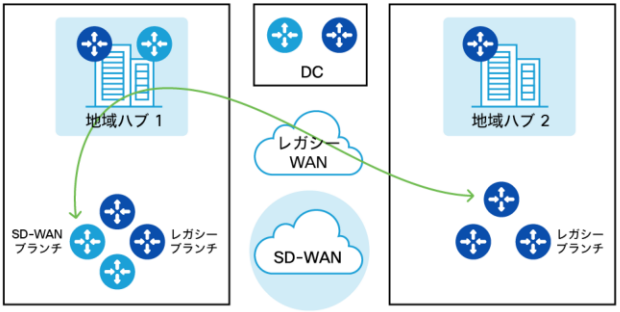
SD-WAN に移行したブランチは、SD-WAN ファブリックを介して、そのままの状態で相互通信します。こうした通信は、地域内でも地域間でも発生します。

図　移行済みブランチのトラフィック フロー（SD-WAN 経由）



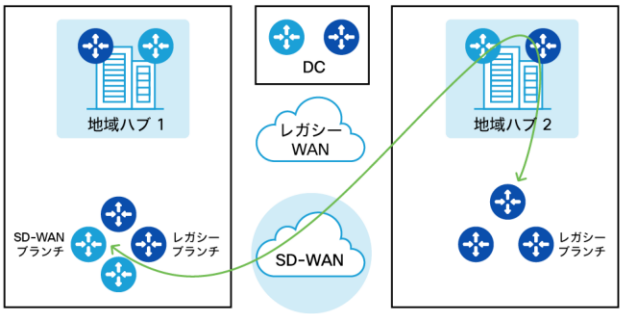
SD-WAN に移行したブランチは、ローカルの地域ハブ、およびレガシー WAN を介してトラフィックを送信することで、異なる地域の移行していないレガシー ブランチと通信します。

図　移行済みブランチとレガシー ブランチのトラフィック フロー（レガシー WAN 経由）



SD-WAN に移行したブランチは、SD-WAN ファブリック経由でリモートの地域ハブを介してトラフィックを送信することで、異なる地域の移行していないレガシー ブランチと通信します。

図　異なる地域における、移行済みブランチとレガシー ブランチの
トラフィック フロー（SD-WAN 経由）



導入事例

Recreational Equipment, Inc（REI）は、屋外レクリエーションに特化した米国の小売店です。REI は、36 の州で 154 店舗を運営し、スポーツ用品、キャンプ用品、旅行用品、衣料品を小売りしていて、安定性、使いやすさ、プロトコルの標準化とともに、小売店の可視化と報告を実現するために、Cisco SD-WAN ソリューションに移行しました。約 6 ヵ月で、自社のネットワーク インフラストラクチャを Cisco SD-WAN に成功裏に移行できました。

Cisco SD-WAN ソリューションをインストールする移行体験が、そのソリューションの柔軟性を証明するとともに、新しい店舗を簡単に展開する手段を REI にもたらしました。また、きわめて優れた設計計画であることも明らかになりました。いずれの技術とも同様に、問題にぶつかりましたが、チームはそれを迅速に解決し、ビジネス運営のリスクをすべて軽減できました。

SD-WAN を何千もの顧客向けに展開してきたシスコの知識と経験から利点を得られるように、REI はシスコに、あらゆる移行領域に関する広範なトレーニングを依頼しました。

詳細については、次を参照してください。*http://cs.co/rei-sdwan-migration* [英語]

主な要点

新しいアーキテクチャに移行する際には、既存のサービスやアプリケーション提供への影響を最小限に抑えることが重要です。移行計画が入念に行われていれば、SD-WAN への移行はシームレスに進みます。移行計画には、コントローラ、管理、データセンター、ブランチ、ポリシー、クラウドなどの多くの要因が含まれます。移行戦略では、その出発点にかかわらず、最初にコントローラ、その後データセンター、ブランチ サイトの順に、展開を進める必要があります。通常、移行完了まで SD-WAN サイトと非 SD-WAN サイト間でシームレスな通信が行われるように、データセンターを設定します。

その他の参考資料

- SD-WAN 移行ガイド *http://cs.co/sdwan-migration*
- Cisco IOS XE ルータのソフトウェアのインストールとアップグレード *http://cs.co/ios-xe-sdwan-install-upgrade*
- Cisco Live セッション：次世代 SD-WAN への移行 BRKCRS-2111 *http://cs.co/on-demand-library* [英語]
- シスコ検証済みデザイン：SD-WAN エンドツーエンド導入ガイド *http://cs.co/cvd-sdwan-deploy*

運用のシンプル化

ビジネス ニーズ

ネットワーク運用の一環として、組織はシンプルかつ効果的な方法で管理、モニタ、トラブルシューティングを行う必要があります。今日の組織の多くは、さまざまなツールを使用して、ネットワーク インフラストラクチャを運用しています。多くの場合、ツールは、ルータの設定、ルータ ヘルスのモニタリング、WAN 回線使用率のモニタリング、アラートとイベントの収集など、特定の運用ニーズのみに対応しています。個々のツールが急増すると、収集されたデータを相互に関連付ける際に重大な運用上の課題が生じます。

Cisco SD-WAN では、Cisco vManage を通じて、環境の管理、モニタ、トラブルシューティングを行えます。vManage は、管理、モニタリング、トラブルシューティングのすべてのタスクに対応できるグラフィカル ユーザ インターフェイスです。ノースバウンド REST API、または SNMP/Syslog/NetFlow のエクスポートを活用することで、既存のツールとのインターフェイスとしても簡単に利用可能です。

モニタリングとアラート

Cisco vManage は、モニタリング、アラート、監査の機能を備えています。

モニタリング ダッシュボード

Cisco vManage には 3 つのダッシュボードがあります。

1 メイン ダッシュボード：ネットワークのステータスと健全性に関する情報を表示します。

2 セキュリティ ダッシュボード：ネットワークで有効になっているセキュリティ機能のステータスを表示します。

3 VPN ダッシュボード：ネットワーク内の VPN セグメントに関する情報を表示します。

図 Cisco vManage メイン ダッシュボード

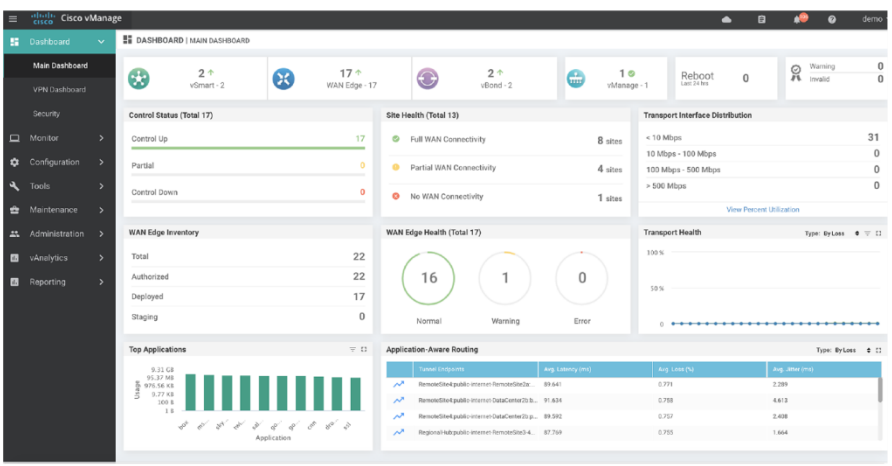


図　Cisco vManage セキュリティ ダッシュボード

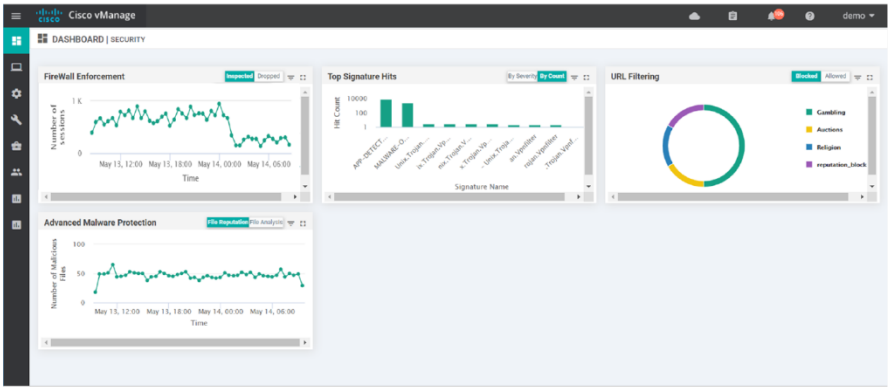
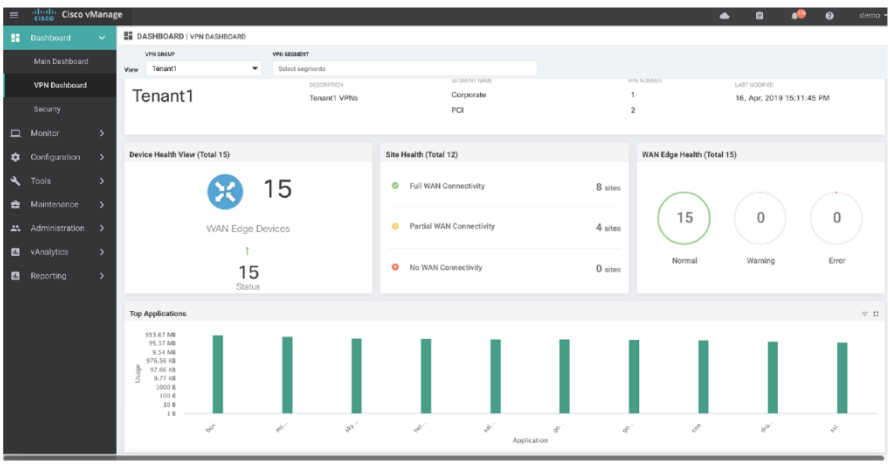


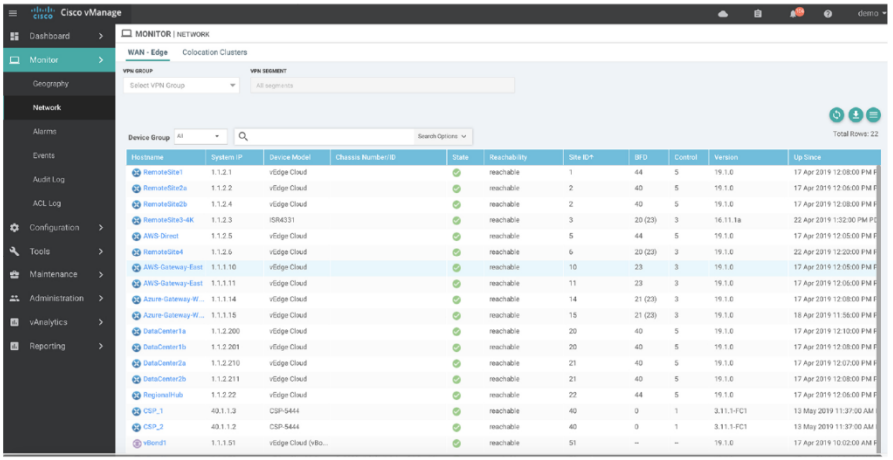
図　Cisco vManage VPN ダッシュボード



デバイスレベルのモニタリング

お客様は、[モニタ（Monitor）] タブのオプションを使用して、ネットワークを構成するすべての WAN エッジ ルータを確認できます。

図　　WAN エッジ デバイス リスト

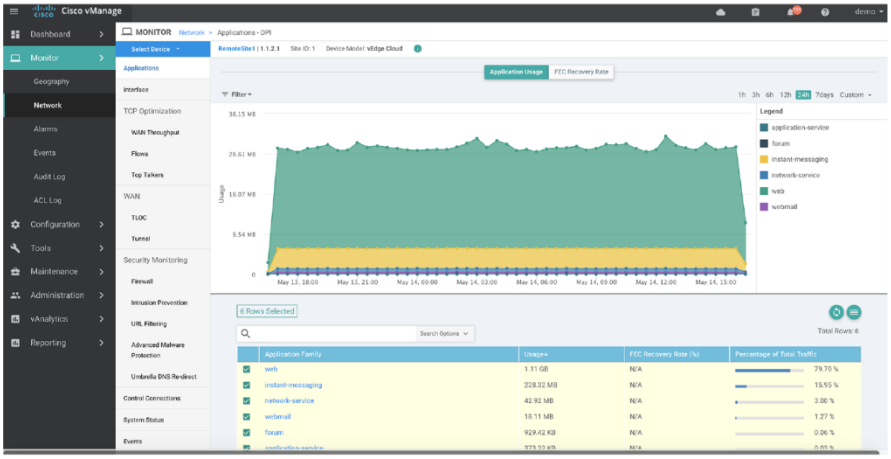


管理者は、個々の WAN エッジ ルータを選択して詳細情報を表示できます。

アプリケーション

アプリケーションの可視化により、選択した WAN エッジ ルータでトラフィックが処理されているアプリケーションをすべて表示できます。これらのアプリケーションは、WAN エッジ ルータ自体のソフトウェアに常駐するアプリケーション認識エンジンによって検出されます。アプリケーションは、識別しやすくするために、アプリケーション ファミリとして整理されており、アプリケーション ファミリごとに、消費帯域幅のパーセンテージを表示することも可能です。また、ネットワーク オペレータは、ドリルダウンをして、個々のアプリケーション、および関連するホスト情報を確認できます。

図　　アプリケーション認識のビュー

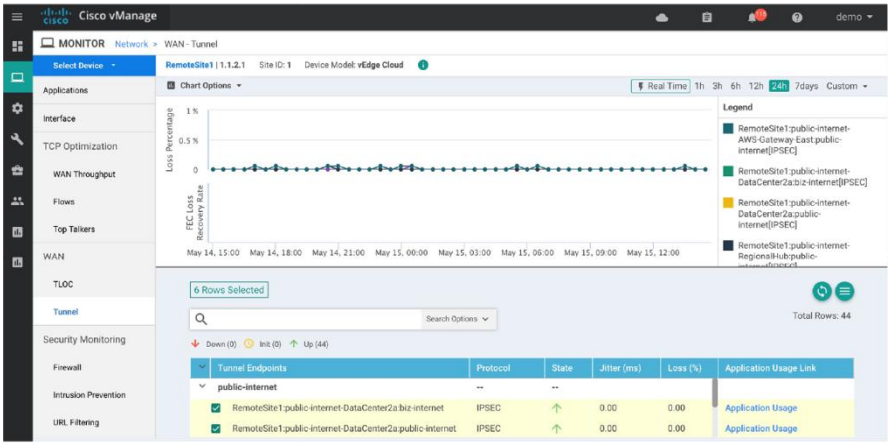


アプリケーション ビューでは、タイムフレームに、1 時間 ~ 7 日の期間を選択できます。カスタム タイムフレームを選択すると、それよりも長い期間のビューを利用可能です。履歴アプリケーションの可視性データ全体は、vAnalytics プラットフォームで収集および維持されます。

トンネル パフォーマンスのモニタリング

SD-WAN トンネルのパフォーマンス ビューには、すべての SD-WAN トンネルの損失、遅延、およびジッターのパフォーマンス特性が表示されます。また、設定されている場合には、FEC（前方誤り訂正機能）などによるリンク修復も表示されます。

図　vManage に表示されるトンネル パフォーマンス

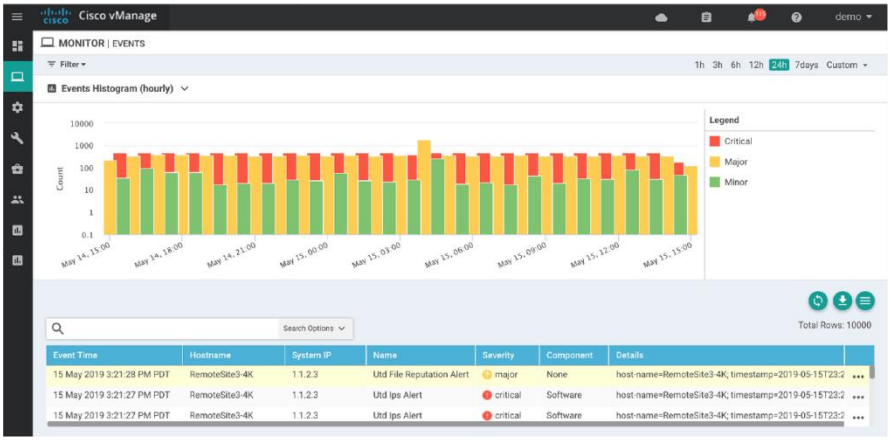


SD-WAN トンネルのパフォーマンスは、リアルタイムで表示されます。これにより、管理者は、アプリケーションに生じた品質の問題を特定して、トラブルシューティングを行えます。

イベントとアラート

Cisco vManage は、SD-WAN ファブリックから送信されるすべてのイベントの中央リポジトリ (貯蔵庫) として機能します。イベントは、重大度に基づいて、クリティカル、メジャー、またはマイナーに分類されます。vManage は、イベントを相互に関連付けた後、それらのイベントに基づいてアラームを送出します。管理者は、アラームの重大度に応じて、電子メールで通知を受けることもできます。

図　vManage に表示されるトンネル パフォーマンス



モニタリング ツール

SD-WAN エッジ ルータでは、SNMP がサポートされており、フロー データを外部のフロー コレクタにエクスポート可能です。また、Syslog メッセージを外部のロギング サーバに送信できるため、セキュリティ インシデント/イベント管理（SIEM）ツールといった外部のモニタリング ツールとの統合も可能です。

API

Cisco vManage では REST API を利用できます。この API は、SD-WAN ソリューションであらゆる側面から、管理、モニタリング、トラブルシューティングを行えるプログラマチック インターフェイスです。セキュアで認証済みの HTTPS 接続を使用して、Cisco vManage Web サーバ経由で REST API にアクセスできます。このトピックの詳細については、本書の「Cisco SD-WAN API」の章を参照してください。

テンプレートとポリシー

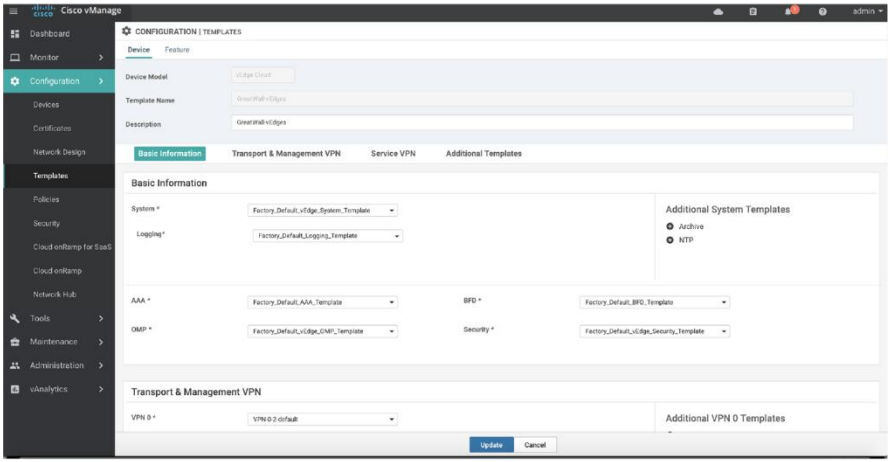
WAN エッジ ルータと SD-WAN コントローラは、vManage のテンプレートを使用して設定します。vManage テンプレートは、複数の WAN エッジ ルータに、同時に接続できます。設定テンプレートを変更すると、その変更内容は、接続されているすべての WAN エッジ ルータに自動的に伝達されます。

設定テンプレートには、フィーチャー テンプレートとデバイス テンプレートの 2 種類があります。

フィーチャー テンプレート：ルータの設定に含まれる各コンポーネント、たとえば、セグメンテーション、インターフェイス、システム、ルーティング、ロギング、RADIUS や TACACS によるデバイス アクセスなどの構成に役立ちます。

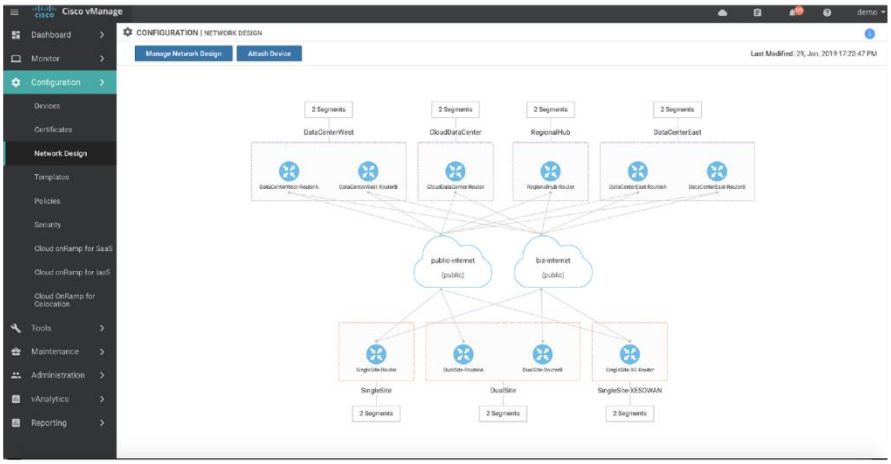
デバイス テンプレート：フィーチャー テンプレートで構成されており、ルータ設定全体のフレームワークを提供します。柔軟に使用できるため、高度にカスタマイズしたルータ設定が可能です。効率を考慮した設計により、最小限の作業で数千のデバイスを設定できます。テンプレートを更新すると、その更新内容は、ただちに WAN エッジ ルータに伝達されます。設定エラーがある場合、テンプレートの設定は以前の状態にロールバックされます。このロールバックの動作によって、人的ミスからシステムを保護できます。

図　サンプルのデバイス テンプレート



WAN エッジ ルータを設定するもう 1 つの方法は、Cisco vManage の [設定（Configuration）] メニューにある [ネットワーク設計（Network Design）] 機能を使用することです。[ネットワーク設計（Network Design）] を利用すると、指示に従うだけのウィザードを活用して、ネットワーク構成を簡単に設計できます。また、vManage に、サイト設定のトポロジを視覚的に表示可能です。[ネットワーク設計（Network Design）] ウィザードでは、テンプレートが自動的に作成されます。これにより、WAN エッジ ルータの展開に着手できます。

図　ネットワーク設計



ポリシー

SD-WAN のポリシーを使用して、SD-WAN ファブリック内で、WAN エッジ ルータ間におけるデータ トラフィックのフローを制御します。ポリシーには複数の種類があります。

- トポロジを制御するポリシー
- トラフィック フローを制御するポリシー
- サイトのローカルで特定の意味を持つポリシー

トポロジ ポリシー

一元化されたコントロール ポリシーが、OMP 内にあるルーティングとトランスポート ロケータ（TLOC）の情報に基づいて機能します。これにより、ルーティングの決定をカスタマイズ可能です。こうしたポリシーを、トラフィック エンジニアリング、パスの優先度、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、パーシャル メッシュなど）の設定に使用できます。

トラフィック フロー ポリシー

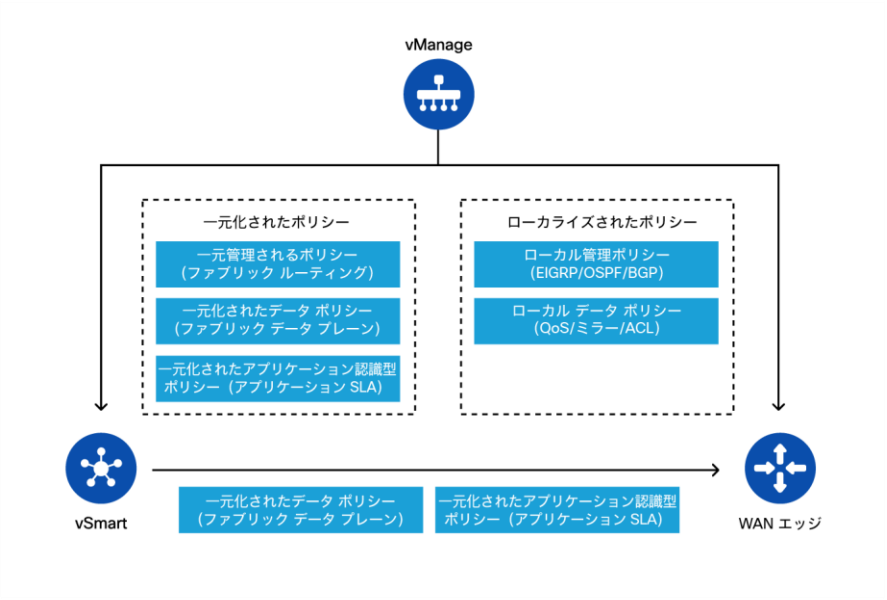
データ トラフィック ポリシーでは、アプリケーション署名、IP ヘッダーのフィールド、またはトラフィックが発生している VPN セグメントに基づいて、ネットワークを通過するトラフィック フローを制御します。一元化されたデータ ポリシーを使用して、アプリケーション ファイアウォール、サービス チェイニング、トラフィック エンジニアリング、Quality of Service（QoS）を設定できます。こうしたポリシーの例として、アプリケーションとトラフィック ステアリング向けの SLA に適用されるアプリケーション アウェア ルーティングのほか、パケット重複のような AppQoE 機能の適用が挙げられます。

ローカルで重要なポリシー

ローカライズしたポリシーを使用して、特定のサイトのトラフィックを処理できます。たとえば、アクセス コントロール リスト（ACL）、Quality of Service（QoS）、および OSPF、BGP、または EIGRP のルート マップが、そうしたポリシーに該当します。

ポリシーは、vManage の [設定（Configuration）] メニューの [ポリシー（Policy）] ウィザードを使用して管理者が定義します。一元化されたポリシーが vManage によって vSmart コントローラに適用され、ローカライズされたポリシーが vManage から WAN エッジ ルータに直接適用されます。

図　Cisco SD-WAN のポリシー フレームワーク



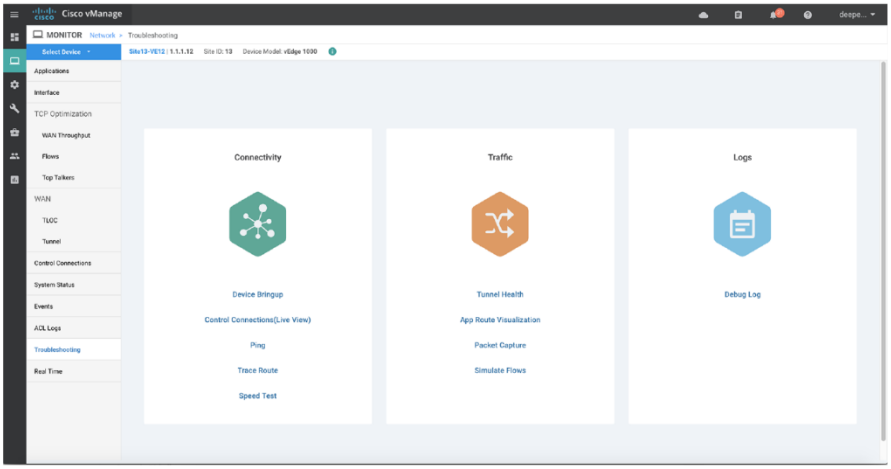
トラブルシューティング

Cisco vManage では、グラフィカル ユーザ インターフェイスを使用して、SD-WAN ソリューションが持つさまざまな側面のトラブルシューティングを実施できます。

- 基本的なトラブルシューティング：Ping や Traceroute など
- 中程度のトラブルシューティング：アプリケーション ルートの可視化やフローのシミュレートなど
- 高度なトラブルシューティング：パケット キャプチャやデバッグ ロギングなど

トラブルシューティングのセクションは、vManage の [モニタ（Monitor）] > [ネットワーク（Network）] > [トラブルシューティング（Troubleshooting）] にあります。

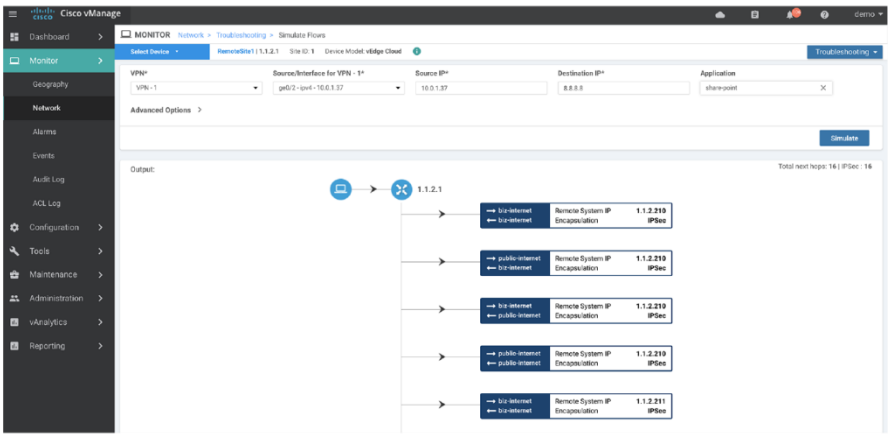
図　Cisco vManage のトラブルシューティング



Cisco vManage では、グラフィカル ユーザ インターフェイス (GUI) から、WAN エッジ ルータごとの [トラブルシューティング（Troubleshooting）] サブメニューに移動して、さまざ

まなトラブルシューティング機能を行えます。トラブルシューティング ツールでは、vManage GUI のコマンドを実行し、WAN エッジ ルータに、タスクの実施と、その結果報告を指示します。このため、ルータにログインして、こうしたタスクを手動で行わずに済みます。以下に、SharePoint アプリケーションに向かうトラフィックのシンプルな [フローのシミュレート（Simulate Flows）] の例を示します。このツールは、WAN エッジ ルータが、DPI によって SharePoint アプリケーションを照合することで、このフローをどのようにリアルタイムに処理するかをシミュレートします。また、設定済みポリシーをすべて通過した後に、このルータの転送エンジンが、外部へのトランスポートをどのように選択するかを表示します。

図　Cisco vManage による、トラブルシューティング フローのシミュレート



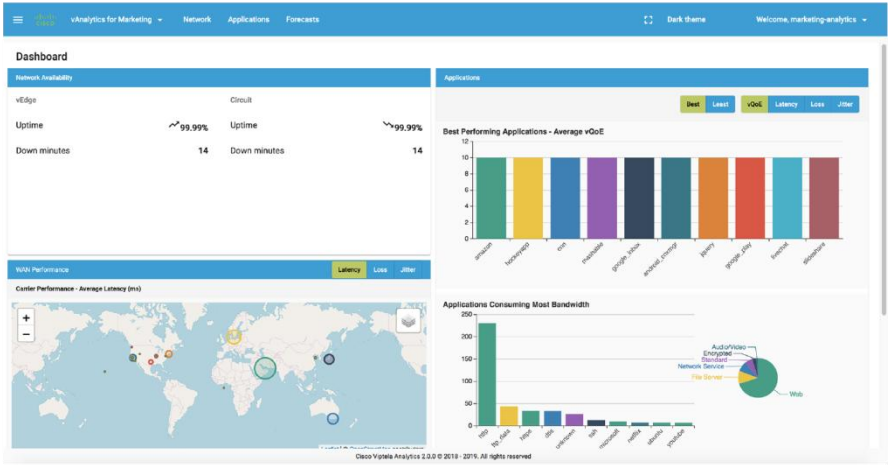
ルータでデバッグを有効にして、vManage の [トラブルシューティング (Troubleshooting)] メニューに表示することもできます。こうしたデバイスで、詳細なトラブルシューティングを行うと、ログ ファイルが vManage ダッシュボードに直接ストリーミングされます。

図　vManage デバッグ ログ

分析

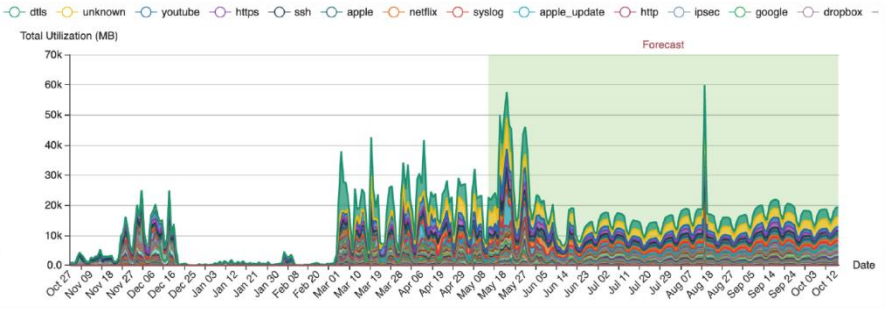
Cisco vAnalytics プラットフォームは、シスコが提供する、Software as a Service（SaaS）製品です。これにより、Cisco SD-WAN ファブリック全体のパフォーマンスと可用性の推移をグラフィカルに表示できます。また、ファブリックを通過するアプリケーションのパフォーマンスも可視化できます。さらに、vAnalytics は、ある時点の、個々のキャリア、トンネル、アプリケーションが持つ特性を、きわめて詳細なレベルで表示可能です。vAnalytics を使用することで、企業は、帯域幅の使用率や、アプリケーションのパフォーマンスを簡単に特定するとともに、履歴のトレンドとの差分で異常を検出できます。

図　Cisco vAnalytics ダッシュボード



Cisco vAnalytics は、機械学習と人工知能の技術を活用し、回線とアプリケーションが将来どのように使用されるかを示す分析情報を提供します。これが、企業のインテリジェントなキャパシティ プランニングを後押しします。

図　　Cisco vAnalytics による予測



導入事例

Cisco SD-WAN ソリューションの vManage を使用すると、数多くの差し迫った問題を解決できます。独自の問題解決に vManage の機能を活用しているお客様のシナリオを、3 つご紹介します。

- ネットワーク設計の簡素化と合理化を検討する小売業者
- 大規模なモニタリングに、API ゲートウェイを使用する金融サービス機関
- アプリケーションのトラブルシューティングに運用ツールキットを活用する医療機関

小売業者の例

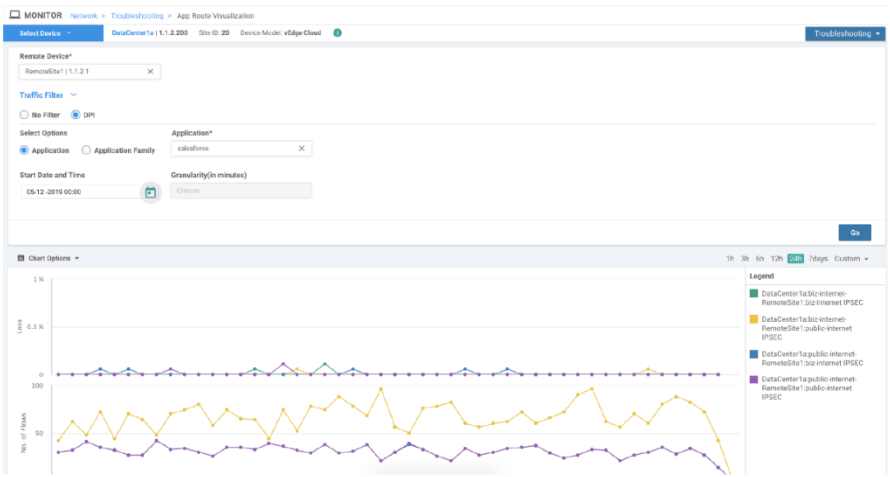
Cisco SD-WAN ソリューションは豊富な機能を備えていますが、そのシンプルさの活用を好まれるお客様もいらっしゃいます。この例では、大規模な小売業者が、vManage テンプレートの構成を使用して、リモート ブランチの展開を簡素化できました。この組織は、変数を使用する単一のテンプレートを設定することで、vManage への API コールを活用し、デバイス固有の属性を指定できました。さらに、複数のデータセンターとリモート サイトをそれぞれのハブに配置した設計フレームワークを確立できました。

財務サービス機関の例

ある大規模な金融サービス機関が、社内で SD-WAN 環境の展開を進めていて、vManage システムのテレメトリ データが貴重なものであることに気が付きました。このテレメトリ データには、選択されるパスに基づいて、サイトの各アプリケーションで発生した損失、遅延、ジッターの情報が含まれていました。このデータが、クライアントからアプリケーションの遅延が報告された際に、問題のトラブルシューティングを行うためだけでなく、回線の動作の推移を観察するためにも使用されました。ネットワーク オペレータは、このデータを抽出し、環境内の別のツールから収集したその他のデータとともに処理する必要があると判断しました。

vManage の一括 API を使用することで、すべての属性に関するデータ セットを、サイトですべて抽出して、それらを、その他のネットワーク データに相互に関連付けることができました。サイトごとにデータを抽出するような手間はかけず、vManage に、大規模なデータ セットを取得させたのです。これにより、損失、遅延、ジッター、アプリケーションの使用状況の推移を示す情報と、SLA 違反のデータを入手できました。

図　アプリケーション ルートの可視化



このお客様は、今では、こうしたレポートを利用して、回線状態の概要を示したり、影響を受けたアプリケーションを報告したりしています。基盤となるトランスポートの問題を調査する際に、インターネット サービス プロバイダーとプロアクティブに連携できるようになったのです。

医療機関の例

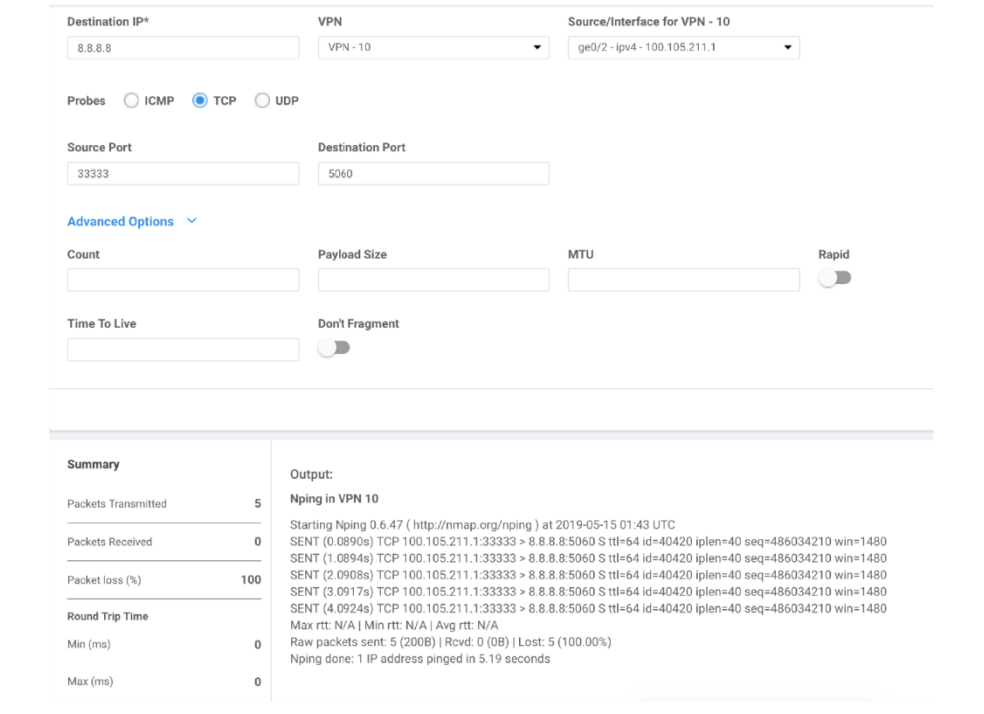
SD-WAN ソリューションでとりわけ必要とされる機能は、ネットワークの状況にリアルタイムに対応できる非常に広範なツールです。この点について例を挙げると、ある医療機関のお客様が、問題の発生時に Cisco SD-WAN のツールを組み合わせて使用して、社内のエスカ

レーション リソース、サービス プロバイダー、Cisco TAC に問題解決を依頼しました。問題が発生した際に、お客様は、以下を実施できました。

- 特定のトラフィック フローに関するパス情報を取得
- 原因とされるパスでの損失、遅延、ジッターをリアルタイムで観察
- 該当のトラフィックで、必要なパケット キャプチャを実行

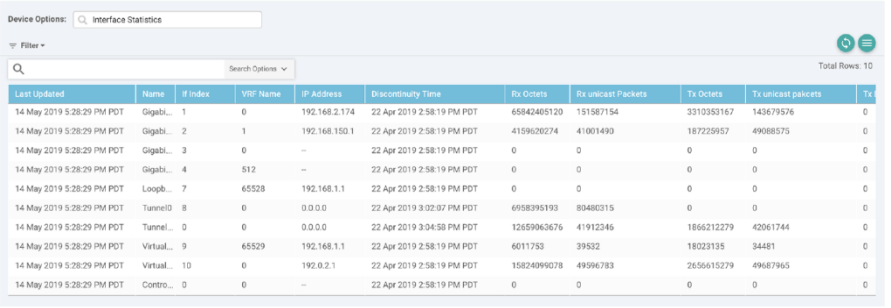
具体的には、その調査結果を検証して、ユーザの特定のアプリケーションによって起こりうる動作を観察できました。以下の図では、アプリケーションによって選択されたパスを調査しています。アプリケーション ルートの仮想化ツールと Ping ツールの使用方法に注目してください。

図　vManage トラブルシューティング ツール



さらに、このお客様は、組み込みのデバイス モニタリング機能を利用して、インターフェイスの統計情報を調査し、WAN エッジ ルータがトラフィックを適切に、配信、処理、転送していることを確認できました。

図　インターフェイスの統計情報



主な要点

ネットワーク運用の一環として、組織はシンプルかつ効果的な方法で管理、モニタ、トラブルシューティングを行う必要があります。そうすることで、現在と将来のビジネス ニーズを満たすネットワーク インフラストラクチャを実現できます。ネットワーク インフラストラクチャでは、問題の発生時に、影響を受けたサービスをただちに復旧できる機能を利用できなければなりません。

- Cisco SD-WAN なら、管理と運用を簡素化して、ネットワークで、最大限の俊敏性を確保できます。
- Cisco vManage では、GUI 主導のシンプルなメニューを使用して、0 日目、1 日目、2 日目のタスクや課題に対応できます。
- ログ収集とフロー収集を行うその他のエンタープライズ ツールと、API を介して統合可能です。

その他の参考資料

シスコ ラーニングのオプション『Cisco SD-WAN Operation and Deployment (ENSDW) v1.0（Cisco SD-WAN の運用と展開（ENSDW）v1.0）』：
http://cs.co/SD-WAN-Operation-Training

Cisco SD-WAN API

ビジネス ニーズ

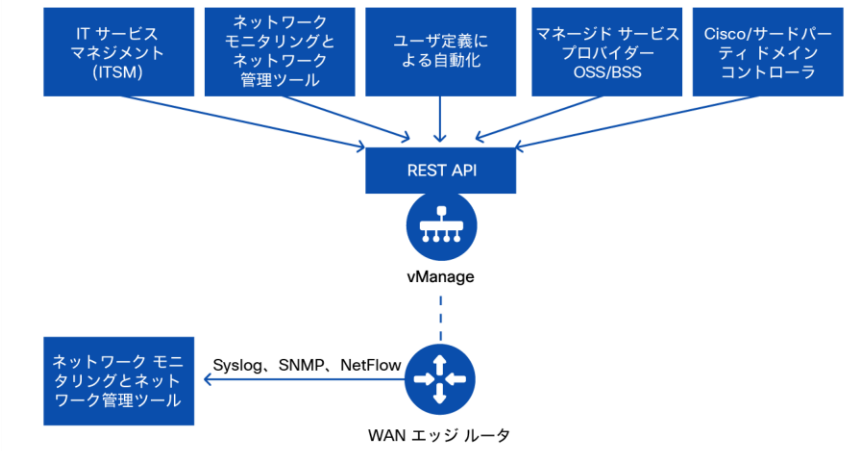
API を使用すると、IT 部門は、既存の運用環境を Cisco SD-WAN とシームレスに統合できます。同時に、新しい機能を提供する優れた柔軟性を得られます。たとえば、企業の IT サービス マネジメント（ITSM）ツールを使用して、WAN で問題が発生した際にトラブル チケットの起票を自動化できます。その一方で、ネットワーク モニタリング ツールによって、WAN のデータと、それ以外のネットワーク データを集約可能です。これにより、システムの状態を、より包括的に把握できるため、問題を迅速に特定してトラブルシューティングを行えます。サービス プロバイダーも、API を通じて、運用システムと課金システムに統合し、顧客のネットワークと利用状況をモニタするとともに、多数のノードに対して変更をオーケストレーションできます。

ツールの統合

Cisco vManage の REST API を使用して Cisco SD-WAN と統合できるツールには、5 つの異なるカテゴリがあります。こうしたツールを Cisco SD-WAN と統合すると、可視性、柔軟性、制御、カスタマイゼーションをそれぞれレベルアップして、独自のビジネス ニーズに応えられます。Cisco SD-WAN と統合可能なツールの 5 つのカテゴリは次のとおりです。

- IT サービス マネジメント（ITSM）
- マネージド サービス プロバイダー向けの運用サポート システムと課金サポート システム（OSS および BSS）ツール
- ネットワーク モニタリングとネットワーク管理ツール
- ユーザ定義の自動化
- シスコまたはサードパーティのドメイン コントローラ

図　Cisco vManage REST API インターフェイス



ITSM

Cisco SD-WAN と ITSM システムの統合により、問題の迅速な特定、重要な情報の収集にかかる時間の短縮、サポート チームの運用の簡素化を実現できるほか、早急な復旧によってダウンタイムを削減可能です。ITSM の利点は次のとおりです。

- ネットワークの状態に基づいて ITSM システムのチケットを自動的に起票できるため、ネットワークの重大な問題を迅速に特定して修復できます。たとえば、WAN エッジ ルータまたは WAN 回線がダウンした場合、常にチケットを自動的に起票するワークフローを作成できます。

- ネットワーク データから抽出した重要な情報を ITSM システムのチケットに直接追加することで、問題の迅速な特定とトラブルシューティングに必要な情報を運用チームに提供できます。
- 修復の自動化により、IT 担当者の明示的な指示を必要とせずに、ネットワークにアクションを直接適用できます。

マネージド サービス プロバイダー向けの OSS/BSS ツール

Cisco vManage で公開さていれる REST API を活用することで、MSP は、Cisco SD-WAN の導入と、自社の運用および課金サポート システム（OSS/BSS）とを完全に統合できます。こうした統合の主な例を次に示します。

- サービスのオーケストレーション : MSP ホスト型 SD-WAN コントローラの展開を自動化して、新規顧客を、オンボーディング、または、既存の MSP ホスト型 SD-WAN コントローラにテナントとしてオンボーディングします。
- セルフサービス ポータル : お客様が新しいサービスを登録したり、既存のサービスの条件を変更したりできます。たとえば、新しい回線の調達と構成、既存の回線の帯域幅拡大、既存のルーティング プラットフォームにおける SD-WAN セキュリティ機能の実装、ネットワーク セグメンテーションの展開などが可能です。
- Cisco vManage で収集した、サービスの利用状況データを活用し、REST API 経由で MSP の課金システムにフィードします。

ネットワーク/セキュリティのモニタリング ツールと管理ツール

最新のネットワーク/セキュリティのモニタリングおよび管理ツールの多くで、vManage REST API を使用できます。これにより、運用状態についての情報を、ネットワーク全体できわめ

て詳細に抽出できるとともに、個々のデバイスレベルで必要な、データの収集と分析の必要性を削減できます。ネットワーク デバイスで直接利用可能な Syslog、SNMP、NetFlow の機能に主に依存する従来のモニタリングおよび管理ツールも、引き続き使用できます。どちらかを選択するのではなく、両方のアプローチを採ることができます。とりわけ、従来のネットワーキングから SD-WAN への移行時にその両方が選択されます。次のように、ネットワーク/セキュリティ向けモニタリングおよび管理ツールを統合可能です。

- セキュリティ情報とイベント管理（SIEM）：セキュリティ リスクと進行中のインシデントに関する分析情報を得られます。また、自動または手動の修復アクションによってそれらを軽減できます。Cisco vManage API を使用することで、ネットワーク全体で、セキュリティ ポリシーの適用とインシデント管理が可能になります。

- アプリケーション/ネットワークのパフォーマンス：アプリケーションとネットワークのパフォーマンスに特化した詳細な情報を得られます。多くの場合、スイッチ、ルータ、アクセスポイントなどの複数の要素でデータが分析されます。vManage API を使用すると、ネットワークとアプリケーションのパフォーマンス テレメトリを統合して表示可能です。これを利用および統合することにより、エンドツーエンドでパフォーマンスを簡単に可視化できます。

- ネットワーク モニタリング：ネットワークの可用性と使用率のベースラインをモニタリングできます。vManage API によってネットワーク全体のデータを利用可能にすることで、個々のデバイスレベルでの調査が不要になります。

- ネットワーク デバイスで生成されるイベント通知の収集、およびイベント通知への対応を行えます（多くの場合、Syslog メッセージまたは SNMP トラップによって生成）。

- メンテナンス アクティビティの計画とスケジューリング：変更管理の効率的なライフサイクルを実現します。必要に応じてロールバックも容易に行えます。これにより、運用の一貫性と透明性が向上し、インフラストラクチャで行われた変更アクティビティを、エグゼクティブ管理で常に認識できます。vManage API を使用することで、すべての運用アクティビティ向けにインターフェイスを一元化し、インフラストラクチャの変更に必要なタスクを大幅に簡素化できます。

ユーザ定義の自動化

vManage グラフィカル ユーザ インターフェイス（GUI）は、一元化された管理システムとして利用でき、Cisco SD-WAN ソリューションの運用に必要なさまざまな機能を備えています。また、vManage REST API によって、あらゆるユーザ定義のタスクで、自動化の可能性が広がります。多くのユーザが、こうした API を活用し、SD-WAN 環境の管理、モニタリング、設定、トラブルシューティングを実行する自動化シーケンスを、特定のニーズに基づいてカスタマイズしています。API を使用して特定の vManage タスクを自動化する場合、Python スクリプトを作成することが少なくありません。より高度なユース ケースには、Ansible プレイブック、または Chef と Puppet のクックブックを活用できます。vManage API のユース ケースを次に示します。

- アプリケーションに関する SLA のビジネス要件に基づく、時間ベースのポリシー自動化。
- カスタマイズした、vManage のポリシー設定に基づく、トポロジ マップや、ネットワーク トポロジ図のカスタマイズ。
- モバイル WAN エッジ ルータのロケーションに基づいて、ファブリック ルーティングの動作を制御するロケーションベースのポリシー。

シスコ/サードパーティのドメイン コントローラ

Cisco vManage の REST API を活用して、マネジメント プレーンで複数のドメイン コントローラを統合すると、管理、モニタリング、設定、トラブルシューティングで、単一のエンドツーエンドの運用エクスペリエンスを得られます。たとえば、vManage の API を Cisco DNA Center と Cisco APIC コントローラで活用することで、キャンパスとデータセンターを Cisco SD-WAN ソリューションに統合できます。こうした統合によって、エンドツーエンドポリシーの共通化が進み、ユーザとアプリケーションの間から、ブランチとクラウドの間、クラウド間まで、インフラストラクチャ全体にわたり望ましい動作を適用できます。

vManage の REST API が持つオープンな性質により、Cisco SD-WAN ファブリックと、サードパーティのドメイン コントローラを簡単に統合できます。これらが、コントロール プレーンとマネジメント プレーンの要素となり、環境内にシスコ以外のインフラストラクチャがある場合、その運用を可能にします。多くの場合、これらは独自の管理ツールによって管理されるサードパーティのサービス ノードです。

マルチドメイン統合の詳細については「マルチドメイン」の章を参照してください。

vManage API のライブラリ

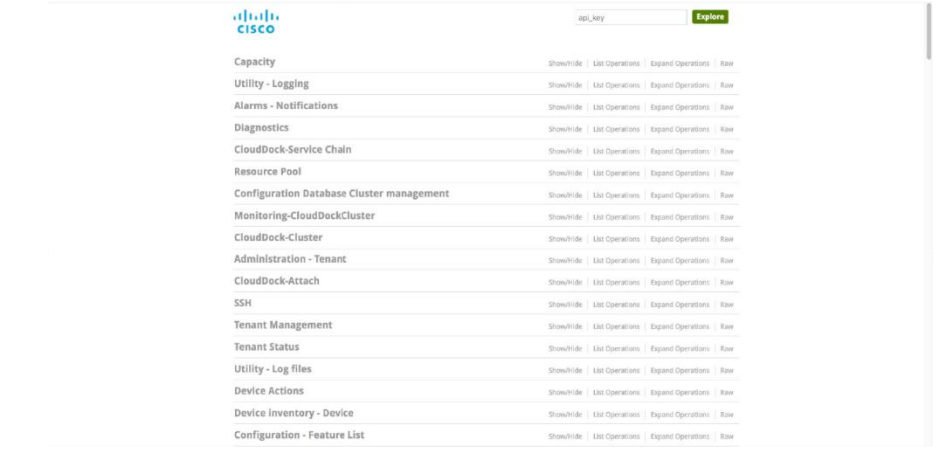
Cisco vManage の REST API は、ネットワーク内にある SD-WAN エッジ ルータの制御、設定、モニタリングに使用できます。これらの API には、vManage Web サーバを通じてアクセスできます。また、API は、次の主要なカテゴリにグループ化されています。

管理者	ユーザとユーザ グループの管理、監査ログの表示、およびローカル vManage サーバの管理。
証明書の管理	証明書とセキュリティ キーの管理。
設定	機能とデバイスを設定するテンプレートの作成、既存のテンプレートからの設定取得、および vManage クラスタの作成と設定。
デバイス インベントリ	シリアル番号やシステム ステータスなどのデバイス インベントリ情報の収集。
モニタリング	オーバーレイ ネットワーク内の運用デバイスに関するステータス、統計情報、およびその他の情報の表示。
リアルタイム モニタリング	統計とトラフィックのリアルタイムな情報の取得、表示、および管理。
トラブルシューティングツール	ポリシーの効果の判断、ソフトウェアの更新、ソフトウェア バージョン情報の取得に必要な、デバイスのトラブルシューティング。

さらに、次の URL を使用して Web ブラウザから、個別のダッシュボードにアクセスできます。ここで、ユーザは、API ライブラリを確認して、使用する特定の API をテストできます。

https://<vManage IP アドレス>:<ポート>/apidocs

図　Cisco vManage API ライブラリ ダッシュボード



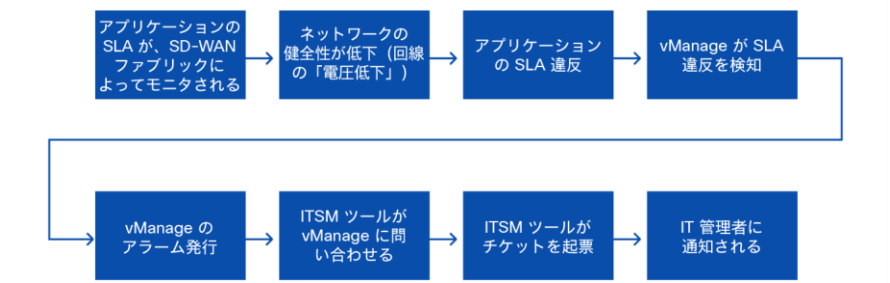
API ダッシュボードから、API コールをテストして、その使用の検証と、結果の確認を行えます。

導入事例

Cisco SD-WAN のプログラマチック API により、Cisco vManage と IT サービス マネジメント（ITSM）ツールをシンプルに統合できます。この導入事例の例では、ITSM ツールを使用して、サービス要求の生成と追跡を行うことを決定した金融機関をご紹介します。

Cisco vManage は、SD-WAN ファブリック全体の健全性と可用性を継続的にモニタします。障害、または最適とは言えない状況が発生した場合、vManage はそれらをイベントとアラームとしてマークします。その後、ITSM ツールが、REST API を介して、マークされた対象を定期的に問い合わせます。ITSM ツールは、サービス要求を作成し、vManage から抽出されたデータを追加します。IT 管理者は、そのデータを使用して、問題の調査とトラブルシューティングを進めます。

図　REST API を介した、サービス要求の生成と追跡



この金融機関は、Cisco vManage のプログラム可能な API を活用し、検出された特定の条件に従って、IT 管理者が修復アクションを行うことも許可しました。たとえば、IT 管理者は、ルータのインターフェイスをリセットして、障害が発生した WAN 回線の接続を復旧できま

す。その際には、ITSM 管理インターフェイスでスクリプトを直接実行し起動した REST API コールを活用します。この金融機関はさらに、ITSM ツールによって、IT 管理者の明示的な指示なしに、修復アクションを自動実行できるようにしました。こうしたアクションを取ることで、サービスの問題解決に必要な時間が大幅に短縮されました。

ITSM ツールと vManage API の統合により、この組織では、IT 部門が社内で提供するサービス レベルを大幅に改善するとともに、サービス全体の復旧にかかる時間を削減できました。

主な要点

Cisco SD-WAN では、vManage でさまざまな API セットを利用可能です。こうした API により、IT ツールとプロセスを、ワイド エリア ネットワーク（WAN）の日常的な運用と管理に簡単に統合できます。API の利用により、グラフィカル ユーザ インターフェイス（GUI）の操作に依存せずに Cisco SD-WAN ソリューションの自動化を推進できる柔軟性を得られます。マネージド サービス プロバイダーとパートナーは、API を使用して、Cisco SD-WAN に自社の課金ツールと運用ツールを統合するとともに、カスタマイズしたサービスを顧客に提供できます。

その他の参考資料

SD-WAN の自動化とオーケストレーションに API を活用する方法の詳細については、次のリソースを参照してください。

- Cisco DevNet：*https://cs.co/sdwan-devnet* [英語]
- vManage REST API ライブラリ：*https://cs.co/sdwan-apis* [英語]

マルチドメイン

ビジネス ニーズ

私たちの働き方は変化しています。ユーザは移動中も常にネットワークに接続しています。同時に、IoT の拡大によってネットワークに接続されるデバイスやモノが増加しています。こうしたデバイスはクラウドで管理され、そのデータもクラウドに保存されます。アプリケーションそのものも移動可能になり、データセンターからクラウドへと移行が進んでいます。多くの場合、その行き先は、1 つのクラウドではなく、マルチクラウド環境です。こうした中での IT の課題は、ユーザの場所や、アプリケーションのホスト先がどこであっても、ネットワークやデバイスにかかわらず、すべてのユーザをすべてのアプリケーションに安全に接続させることです。ネットワーク ドメインには、データセンター、キャンパス、ブランチ、外部のクラウド プロバイダーが存在します。絶えず変化するネットワーク環境で不可欠なセキュリティを、エンドツーエンドで確保する必要があります。こうした異なるドメインの統合により、ワークロードを環境全体に分散できる柔軟な IT を実現するとともに、ユーザやデバイスに対する信頼性の高いセキュアなアクセスを維持できます。

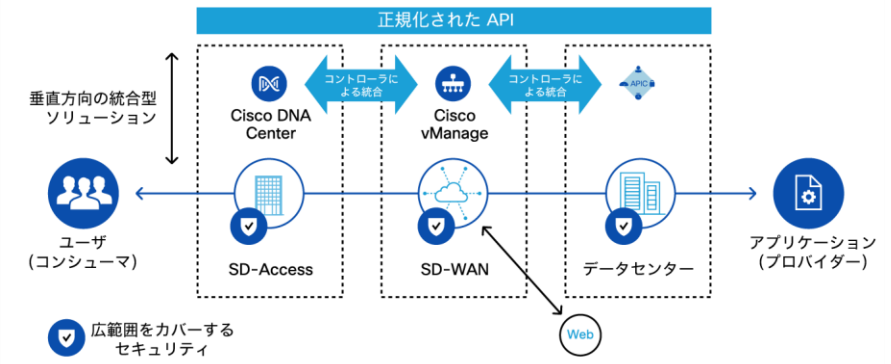
マルチドメイン アーキテクチャ

シスコは、お客様の多様なネットワーキング ドメインの統合を支援するアーキテクチャを構築しています。Cisco SD-WAN を使用すると、マルチドメインの統合により、次のユース ケースを実現できます。

- エンドツーエンドのセグメンテーション
- 統合されたクロスドメイン ポリシー
- アクセス ネットワークを複数のクラウドに接続

Cisco SD-Access、Cisco SD-WAN、および Cisco ACI を統合した、マルチドメイン統合により、エンドツーエンドのエクスペリエンスを得られます。各ドメインを独自のドメイン マネージャによって管理し、API を使用してクロスドメイン インテントを分散します。このアプローチでは、キャンパス、WAN、およびデータセンター向けにベスト オブ ブリードのソリューションを実現できる一方で、各ドメイン固有の利点を維持可能です。

図　マルチドメイン アーキテクチャ

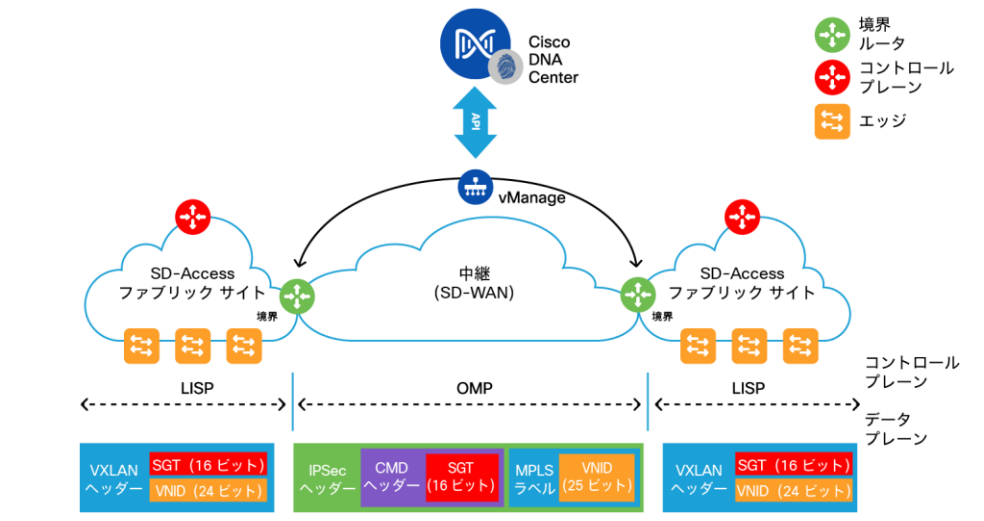


SD-WAN と SD-Access

Cisco Software-Defined Access（SD-Access）では、アクセス レイヤからクラウドに至る範囲で、単一のネットワーク ファブリックを定義します。ポリシーベースの自動化を、ネットワーク内のセキュリティと可視性を損なうことなく、ユーザ、デバイス、およびあらゆるアプリケーションに設定できます。

SD-WAN と SD-Access の統合では、拡張可能グループ タグ（SGT）でアクセス メタデータ情報を伝達する必要があります。SGT は、IPSec パケットでカプセル化され、WAN 経由で送信されます。受信側 SD-Access サイトの境界ルータがトラフィックのカプセル化を解除するため、それを受信側で使用できるようになります。次の図は、統合された SD-WAN によって中継するマルチサイト SD-Access を示しています。

図　　統合された SD-WAN、および SD-Access

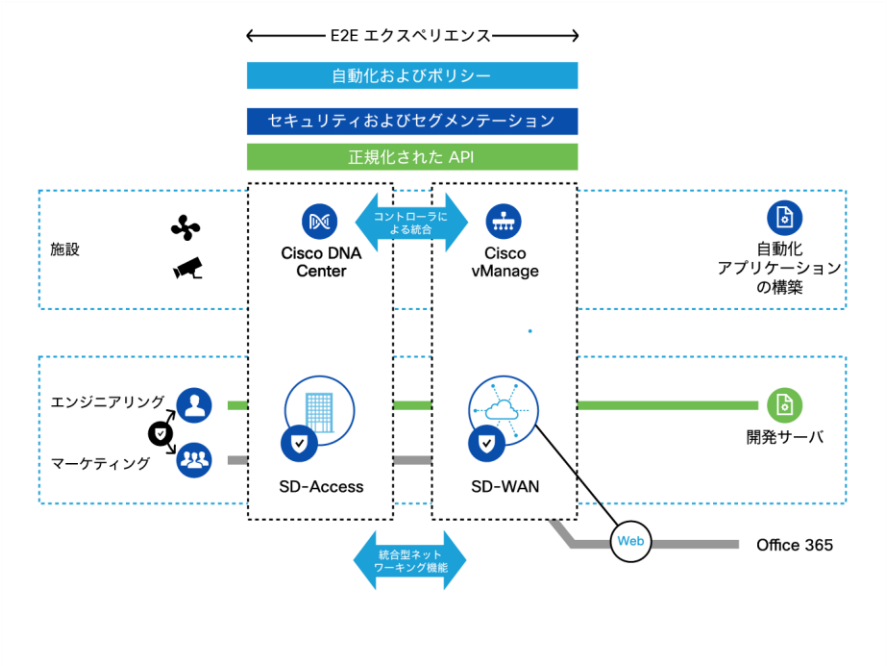


この統合により、エンドツーエンドのセキュアな接続が実現します。SD-Access のアイデンティティ サービスは、ユーザ/モノを特定し、トラスト（信頼）ベースのセキュリティ レイヤを提供するうえで重要です。SD-Access のセグメンテーション (マクロ/マイクロ) によって、マルウェアが水平方向に拡散するのを防ぎ、脅威を前提としたセキュリティ モデルの最初のレイヤを確立できます。また、SD-WAN の統合により、SD-Access のセグメンテーションをサイト間でシームレスに拡張可能です。Cisco DNA Center と Cisco vManage の間では、セグメンテーション ポリシーの統一が自動的に行われます。

SD-Access の境界ルータには、WAN エッジと、SD-Access の終端という 2 つの機能があります。WAN エッジの機能は vManage によって制御され、SD-Access の機能は Cisco DNA Center によって制御されます。

マネジメント プレーンは、API によって統合されます。このソリューションは、可視性とアシュアランス情報をドメイン全体で統合し、包括的なエクスペリエンスを実現します。境界ルータのテレメトリはすべて、SD-Access と SD-WAN コントローラ間の API 接続を介して Cisco DNA Center に送信されます。次の図は、このエンドツーエンド アーキテクチャを示しています。

図　SD-WAN および SD-Access の統合管理

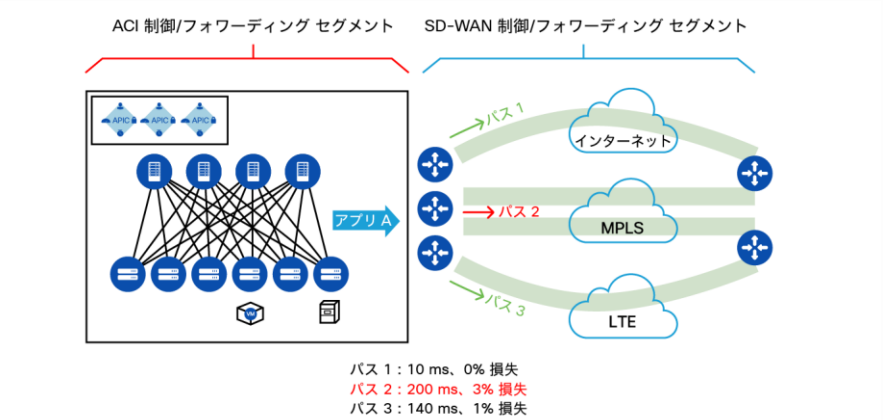


SD-WAN と Cisco ACI

Cisco Application Centric Infrastructure（ACI）では、アプリケーションの要件によって、データセンターの環境内のネットワークを定義できます。

リモート サイトから、データセンター内のアプリケーションに WAN 経由で接続する場合、SLA が意識されず、遅延の影響も受けやすくなります。接続に信頼性がなければ、アプリケーションのユーザ エクスペリエンスが低下します。SD-WAN と ACI を統合して、ACI のポリシーを SD-WAN ファブリックに自動的に伝達することで、そうした問題を解決できます。これを行うには、Cisco vManage と Cisco Application Policy Infrastructure Controller（APIC）の間で REST API を使用して、ワークフローを自動化します。

図　SD-WAN と ACI の統合



データセンターからブランチへの接続を強化するには、ユーザ定義のポリシーによって、特定のアプリケーション トラフィックの SLA を設定します。Cisco vManage で API を使用して、特定のアプリケーションの SLA ポリシーを APIC から適用し、WAN エッジ ルータにプッシュします。ポリシーが適用されると、トラフィックは最適なパスを通過します。

この統合で今後強化される機能は次のとおりです。

- パブリック クラウドから、データセンター内の ACI ファブリックに接続する
- SD-WAN を介したマルチ ACI データセンター接続
- ブランチ内の ACI リモートリーフ接続

主な要点

ネットワーク ドメインには、データセンター、キャンパス、ブランチ、外部のクラウド プロバイダーが存在します。絶えず変化するネットワーク環境で不可欠なセキュリティを、エンドツーエンドで確保する必要があります。こうした異なるドメインにより、ワークロードを環境全体に分散できる柔軟な IT を実現するとともに、ユーザやデバイスに対する信頼性の高いセキュアなアクセスを維持できます。

- Cisco SD-Access、Cisco SD-WAN、および Cisco ACI の統合により、一貫性のあるエンドツーエンドのエクスペリエンスを得られます。
- 各ドメインを独自のドメイン マネージャによって管理し、API を使用してクロスドメイン インテントを分散します。
- マルチドメインにより、キャンパス、WAN、およびデータセンター向けにベスト オブ ブリードのソリューションを実現できる一方で、各ドメイン固有の利点を維持可能です。

その他の参考資料

- SD-Access の詳細については、次のリンクから「Cisco SD-Access（Software-Defined Access）」のマニュアルを参照してください。*http://cs.co/9001Ec6nD*
- Cisco SD-WAN と Cisco ACI の統合の詳細については次を参照してください。*http://cs.co/aci-sdwan*

SD-WAN のマネージド サービス

ビジネス ニーズ

企業は、自社の WAN を従来の MPLS から進化させようとしています。Cisco SD-WAN では、サービス プロバイダーとパートナーの両方が、新たな収益源を得られます。SD-WAN の機能を超えるマネージド サービスである、セキュリティとアプリケーションの最適化は、付加価値サービスの例と言えます。お客様は、この新しいアーキテクチャへの移行を支援してくれるサービス プロバイダーを求めています。シスコのパートナーも、SD-WAN によって、マネージド サービス市場に参入したり、既存のマネージド サービスをコア ビジネスを超えて拡大したりする機会を得られます。

サービス オーケストレーション

Cisco SD-WAN への移行に着手するパートナーとサービス プロバイダーには、顧客のオンボーディング、自動プロビジョニング、管理、モニタリングに関するニーズを満たすツールと機能が求められます。エンド カスタマー側での運用を可能にするには、以下を考慮して、効果的な SD-WAN の実践方法を確立する必要があります。

- 展開前のデバイスのステージングと証明書の管理
- 新しい回線の開通、および回線の移行/追加/変更の支援
- デイゼロ（展開前）とデイワン（展開時）における構成の開発と展開
- エンドツーエンドで実施する SD-WAN ソリューションのテスト
- イベントのロギングやアラートの収集といったデイツー（展開後）の運用（例：サービス チケットの起票）
- Cisco vManage、または WAN エッジ ルータの CLI で利用可能なトラブルシューティング ツールによる問題の修復
- ソフトウェア アップデート
- レポートのカスタマイズ

パートナーとサービス プロバイダーは、Cisco SD-WAN のサービスを提供する際に、オーケストレーションの方法に関連していくつかの選択肢を利用できます。その選択肢とは、Cisco vManage のみ、Cisco vManage と Cisco Network Services Orchestrator（NSO）、または Cisco vManage と Cisco Managed Services Accelerator（MSX）です。パートナーとサービス プロバイダーは、こうした選択肢を評価して、顧客のニーズとともに、どれがそのニーズを最も満たすかを把握する必要があります。これらのどのオプションでも、既存の OSS/BSS ツールをさまざまなレベルで統合可能です。

Cisco vManage のみ

このモデルでは、単一またはマルチテナントの運用に Cisco vManage を活用します。Cisco vManage グラフィカル ユーザ インターフェイス（GUI）機能のフルセットを利用することも、Cisco vManage の API でプロビジョニングと運用をプログラミングすることもできます。このモデルを利用するパートナーとサービス プロバイダーは、Cisco vManage で公開されているさまざまな REST API を通じて、マネージド SD-WAN サービスを、自社で選択したオーケストレーション ツールや、OSS/BSS システムに統合できます（REST API の詳細については「Cisco SD-WAN API」の章を参照してください）。

Cisco vManage および Cisco NSO

このモデルでは、Cisco NSO を活用します。Cisco NSO は、自動化、およびワークフロー構成を行える、高度にカスタマイズ可能なプラットフォームを提供します。Cisco NSO とその SD-WAN 機能パックは、Cisco vManage でネイティブに利用可能なあらゆる機能に基づいています。これにより、SD-WAN インフラストラクチャのプロビジョニングを、新たな方法で実施したり、あらゆる面で大幅に簡素化したりできます。Cisco NSO により、パートナーとサービス プロバイダーは、リソース向けサービス（RFS）のレイヤで、これまでにない俊敏性と柔軟性を得られます。

Cisco vManage および Cisco MSX

このモデルでは、Cisco MSX を活用します。Cisco MSX により、完全なオーケストレーションと管理プラットフォームを利用でき、マネージド サービス スタックの構築、展開、保守にかかる運用コストを削減可能です。このソリューションでは、マネージド サービスの展開方法が、手動による最新のネットワーク デバイスの設定から、ソフトウェアの抽象化によるサービス定義に移行されます。プロバイダーは、このアプローチのサービス モデルを使用して、クラウドベースのサービスの作成とカスタマイズを自動化することで、サービス目的を達成できます。その結果、どのお客様に対しても、Cisco SD-WAN のサービス提供までの時間を大幅に短縮可能です。

マルチテナント機能

マネージド サービス プロバイダー（MSP）とシスコのパートナーは、エンド カスタマー向けのサービスとして Cisco SD-WAN を提供します。複数の顧客向けに SD-WAN の展開を実施している MSP は、SD-WAN コントローラに関する特定の要件があります。Cisco SD-WAN の大規模な展開も、小規模な展開も行えるように、このソリューションでは、MSP 向けに、プロビジョニング、管理、モニタリングの簡素化を目的とした選択肢を設けています。これにより、コストも最小限に抑えられます。

顧客向けに SD-WAN のサービスを作成する場合、MSP は、顧客ごとに独自のコントローラ セットを展開することも、マルチテナント コントローラ機能を活用して、多数の顧客をサポートすることもできます。SD-WAN コントローラには 4 つの展開モデルが想定され、MSP は自社の SD-WAN サービスに合わせてそれらを選択可能です。

名前	単一またはマルチテナント	システム管理者	ロケーション
クラウドホスト型	単一のテナント	シスコ	Cisco Cloud
クラウドホスト型	マルチテナント	シスコ	Cisco Cloud
MSP ホスト型	単一のテナント	MSP	MSP クラウド
MSP ホスト型	マルチテナント	MSP	MSP クラウド

Cisco SD-WAN では、さまざまな物理および仮想の WAN エッジ ルータがサポートされており、それらを、SD-WAN の機能に活用できます。MSP は、顧客のニーズに応じて、そうした中から WAN エッジ ルータを選択します。このため、多くの場合、物理および仮想の WAN エッジ ルータを組み合わせて活用します。

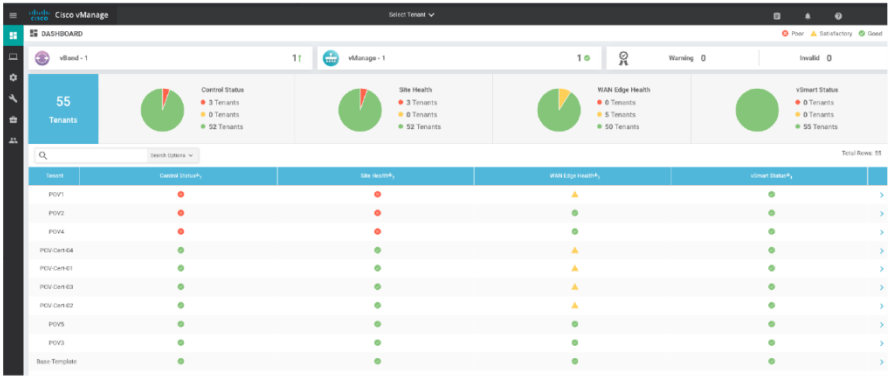
テナント モデル

顧客向けのサービスを作成する場合、MSP にはいくつかの方法でテナントを定義し、きめ細かい制御を行う選択肢があります。

- オーバーレイのテナント単位 : 共有のコントローラ インフラストラクチャ、および各顧客専用の WAN エッジ ルータ
- VPN のテナント単位 : 共有のコントローラと WAN エッジ ルータ、および各顧客専用の VPN セグメント

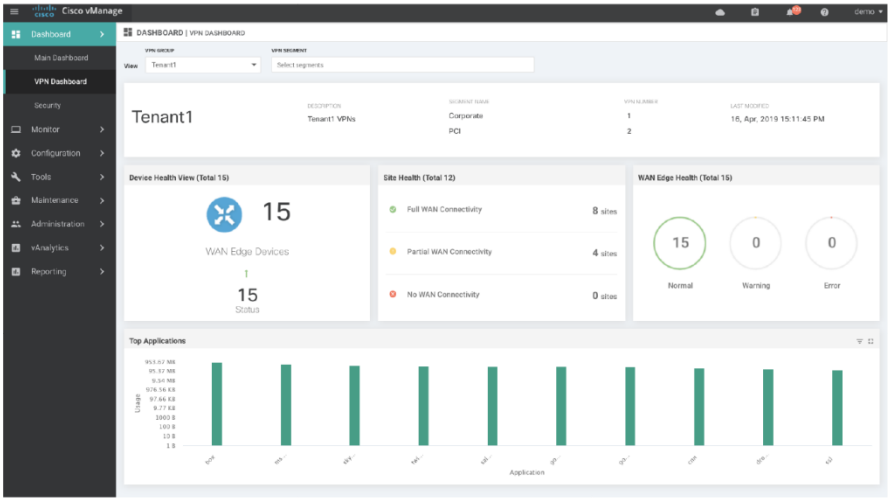
MSP は、共通の SD-WAN vManage インフラストラクチャを使用して、完全に分離されたテナントを環境内に作成することもできます。この導入モデルの WAN エッジ ルータは、環境内のその他のテナントから分離され、特定の顧客専用に使用されます。

図　vManage マルチテナント ダッシュボード



共通の WAN エッジ ルータを使用して VPN セグメンテーション技術を活用し、複数の顧客をサポートする場合、MSP は、VPN ごとにテナントを作成できます。この場合、特定の VPN 1 つ、または VPN のセットを特定の顧客に割り当てて、MSP 独自の設定とモニタリング ダッシュボード環境を使用できます。

図　Cisco vManage の VPN テナント



ロールベースのアクセスにより、MSP は、顧客がマルチテナント環境の一部を自分専用に使用してモニタと操作を行えるサービスを提供できます。

導入事例

Cisco SD-WAN により、ネットワークを自動化するとともに、設定を簡素化できます。これは、いずれの MSP にとっても重要な利点です。この導入事例では、MSP が、世界規模の輸送ロジスティクス企業で、SD-WAN の展開にかかる時間をどのように削減したかを示しています。

ある顧客が、国際拠点全体で SD-WAN を活用する、新しい施設の段階的な展開を計画しました。ビジネスと技術の目標を達成しようと、MSP に連絡を取り、リモート サイトの展開を進める支援を求めました。これまで、新しいリモート ロケーションの立ち上げには非常に時間がかかっていました。リモート サイトで、MPLS の WAN 接続を可能にするには、平均 96 日が必要でした。Cisco SD-WAN により、MSP は、ビジネスグレードのインターネット リンクと LTE を活用して、リモート サイトを 10 時間で展開できました。また、短時間での展開に加えて、顧客が日常的に行う SD-WAN の運用を簡素化し、新しいアプリケーションの展開に注力できるようにしました。アプリケーションの可視性、一元化されたネットワーク管理、ダッシュボードベースのリアルタイム分析が、さらに顧客の自信につながりました。

MSP は、この多国籍企業に Cisco SD-WAN を導入する際に、Cisco Managed Services Accelerator（MSX）を活用しました。これにより、ネットワーク サービスを一元的にプロビジョニングして、シスコ エンタープライズ ネットワーク コンピューティング システム（ENCS）プラットフォームで仮想 WAN エッジ ルータをオーケストレーションしました。こうして、完全に管理された、マルチサービスのブランチを実現できました。

主な要点

企業は、WAN 戦略の策定を進めていて、その多くが、マネージド サービス プロバイダーやパートナーに支援と解決策を求めています。サービスを提供する組織は、こうした動きを活用して、既存のサービスを拡大したり、新たな収益源を見出したりすることができます。同時に、次のような価値を提供できます。Cisco SD-WAN には、MSP とパートナーが、そうした取り組みで成功を得るために必要なツールが用意されています。

- SD-WAN によって、サービス プロバイダーとパートナーの両方が、新しい収益源を得られます。
- マネージド サービス プロバイダーは、単一のテナントまたはマルチテナント モードで、顧客向けに SD-WAN を導入できます。
- Cisco SD-WAN は、SD-WAN サービスをオーケストレーションする方法として、MSP にいくつかの選択肢を用意しています（vManage、Network Services Orchestrator、Cisco Managed Services Accelerator）。

その他の参考資料

次のリソースでは、SD-WAN をマネージド サービスとしてお客様に提供する際に、Cisco SD-WAN がどのように役立つかをご確認いただけます。

- Cisco MSX：*https://www.cisco.com/c/ja_jp/products/cloud-systems-management/managed-services-accelerator/index.html*
- Cisco vManage：*https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/sd-wan/solution-overview.html*
- Cisco NSO：*https://www.cisco.com/c/ja_jp/solutions/service-provider/solutions-cloud-providers/network-services-orchestrator-solutions.html*

付録

カスタマー リファレンス

これは、本書を発行したときのカスタマー リファレンスの例です。
次のリンクから、最新のカスタマー リファレンスをご覧ください。
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/sd-wan/index.html

「シスコのおかげで、モバイル決済、生体認証、インテリジェンス アプリケーション、ビッグデータなどのテクノロジーの活用、小売業のビッグデータの構築で自信がつきました...」
Xingbianli 社 IT ディレクタ Wang Mengzhe 氏

「当社では、Cisco SD-WAN を利用することで、MPLS コストを 25% 削減しながら帯域幅を 3,075% 拡大できました。」
National Instruments 社グローバル ネットワーク チーム マネージャ Luis Castillo 氏

「Agilent では Viptela SD-WAN をグローバルに導入したおかげで、ビジネス要件の変化に IT チームが迅速に対応できるようになりました。新機能のターンアラウンド タイムが 80 % 以上改善され、アプリケーションの信頼性とユーザ エクスペリエンスが大幅に向上しました。」
Agilent Technologies 社 グローバル ネットワーク アーキテクト Pascal Heger 氏

「Cisco ISR 4000 ルータ上の SD-WAN によって、信頼できる堅牢なプラットフォームが構築されます。それにより、ソフトウェアのアップグレードがシンプルになり、セキュリティとパフォーマンス上のメリットがすぐに得られます。」
Altice Portugal 社 Rui Pereira 氏

「シスコの SD-WAN 製品を活用する Verizon の仮想ネットワーク サービスは数万の顧客ロケーションに導入されており、IT の複雑さを軽減してコストを管理すると共に、デジタル変革を可能にして企業のクラウドへの移行を促進しています」
Verizon 社上級副社長 Shawn Hakl 氏

「最適な Office 365 のパフォーマンスは、ローカル インターネット ブレイクアウトを可能にすることで実現されます。つまり、重要な Office 365 シナリオでは、ユーザはブランチ内から直接 Microsoft のグローバル ネットワークに接続します。シスコの SD-WAN など現在の SD-WAN ソリューションでは、お客様によるこのような構成の実装、複数の DIA リンクのサポート、最善のリンクの動的な選択が簡単になるため、Office 365 のユーザ エクスペリエンスが改善されます。」

Microsoft 社パートナー アーキテクト Konstantin Ryvkin 氏

「ISR ルータに実装された Cisco SD-WAN によって信頼性の高い基盤が構築され、SD-WAN の統合が速やかに進み、管理がシンプルになるほか、重要なクラウドベースのビジネス アプリケーションへのリアルタイム アクセスが向上します。」

米国の金融機関

「シスコの SD-WAN の高度なセキュリティでは、さまざまなクラウド環境がある中でお客様のネットワーク全体をすぐに要塞化できます。これは、統合セキュリティ、ソフトウェア定義型 WAN、クラウド サービスのすべてを単一のポリシー コントローラで管理するエンタープライズ アーキテクチャの採用に向けた重要なステップになります。」

World Wide Technology 社プラクティス マネージャ Bill Thompson 氏

「単一の統合ソリューションとして提供される Cisco SD-WAN の新しいセキュリティ機能によって、WAN エッジをインターネットに安全に接続できるようになりました。」

Datacom 社ネットワーク ソリューション アーキテクト Hussein Omar 氏

「お客様はよりセキュアな接続を求めていますが、たいていは複数のクラウド環境をご利用です。そのため CDW では SD-WAN 向けのシスコの新しい統合セキュリティ機能を他との差別化を図れる重要な機能と位置付けています」

CDW テクニカルアーキテクト Will Kerr 氏

「Cisco SD-WAN により、ネットワーク管理者としての業務が非常に楽になりました。新しい設定とポリシーの変更をネットワーク全体に展開するためには、以前なら多数あるデバイスを 1 つ 1 つ作業しなければならず、非常に時間がかかっていましたが、現在は数分で完了します。」

Reece Group ネットワーク管理者 Peter Castle 氏

関連資料

Cisco SD-WAN の詳細については、以下のサイトを参照してください。

- Cisco SD-WAN 製品のメイン ページ：*http://www.cisco.com/jp/go/sdwan*
- Cisco コミュニティ - SD-WAN：*https://cs.co/sdwan-community* [英語]
- ブランチ、WAN、インターネット エッジのためのデザイン ゾーン：*https://www.cisco.com/c/ja_jp/solutions/design-zone/networking-design-guides/branch-wan-edge.html*
- Cisco SD-WAN 製品に関する資料：*http://cs.co/sdwan-docs* [英語]
- シスコ検証済みデザイン SD-WAN 設計ガイド：*http://cs.co/sdwan-design* [英語]
- Software Licensing for SD-WAN and Routing（SD-WAN およびルーティングのソフトウェア ライセンス）：*http://cs.co/one-wan-subscription* [英語]

略語

AAA：Authentication, Authorization, and Accounting

ACI：Application Centric Infrastructure

ACL：Access Control List

AES：Advanced Encryption Standard

AMP：Advanced Malware Protection

API：Application Programming Interface

APIC：Application Policy Infrastructure Controller

ASA：Adaptive Security Appliance

ASIC：Application-Specific Integrated Circuit（特定用途集積回路）

ASR：Aggregation Services Routers

AWS：Amazon Web Services

BFD：Bidirectional Forwarding Detection

BGP：Border Gateway Protocol

BSS：Business Support System

BYOL：Bring Your Own License

CA：Certificate Authority（証明局）

CBC：Cipher Blocker Chaining（暗号ブロック連鎖）

CE：Customer Edge

COS：Class of Service

CSP：Cloud Services Platform

Cisco CSR：Cloud Services Router

CSR：Certificate Signing Request（証明書署名要求）

CSV：Comma Separated Values（カンマ区切り値）

DIA：Direct Internet Access

DMZ：Demilitarized Zone（緩衝地帯）

DNA：Digital Network Architecture

DNS：Domain Name Services

DPI：Deep Packet Inspection

DSCP：Differentiated Services Code Point

DTLS：Datagram Transport Layer Security

EIGRP：Enhanced Interior Gateway Routing Protocol

ENCS：Enterprise Network Compute System

ERRS：Enterprise Records Retention Schedule

ESP：Encapsulating Security Payload

FEC：Forward Error Correction（前方誤り訂正）

FPD：Field Programmable Device

FQDN：Fully Qualified Domain Name

FTD：Firepower Threat Defense

GCM：Galois/Counter Mode

GRE：Generic Routing Encapsulation

GUI：Graphical User Interface

HTTP：Hypertext Transfer Protocol

HTTPS：Hyper Text Transfer Protocol Secure

IaaS：Infrastructure as a Service

IDS：Intrusion Detection System（侵入検知システム）

IKE：Internet Key Exchange

IoT：Internet of Things

IPFIX：Internet Protocol Flow Information Export

IPS：Intrusion Prevention System（侵入防御システム）

IPSEC：Internet Protocol Security

ISR：Integrated Service Router

IT：Infrastructure Technology

ITSM：Infrastructure Technology Service Management

KVM：Kernel-based Virtual Machine

LTE：Long Term Evolution

MFA：Multi-Factor Authentication（多要素認証）

MPLS：Multiprotocol Label Switching

MSP：Managed Service Provider

MSX：Managed Services Accelerator

MTU：Maximum Transmission Unit（最大伝送ユニット）

NAT：Network Address Translation（ネットワーク アドレス変換）

NETCONF：Network Configuration Protocol

NSO：Network Service Orchestrator

OMP：Overlay Management Protocol

OPEX：Operating Expenses（運用コスト）

OSPF：Open Shortest Path First

OSS：Operational Support System（運用サポート システム）

PCI：Payment Card Industry
（決済カード業界）

PnP：Plug and Play

QoS：Quality of Service（サービス品質）

QoE：Quality of Experience

RADIUS：Remote Authentication Dial-In User Service

RBAC：Role Based Access Control

REST：Representational State Transfer

RSA：Rivest-Shamir-Adleman

SA：Security Association

SaaS：Software as a Service

SAML：Security Assertion Markup Language

SDA：Software-Defined Access

SDN：Software-Defined Network

SGT：Scalable Group Tag

SHA：Secure Hash Algorithm

SIEM：Security Information and Event Management

SLA：Service-Level Agreement

SD-WAN：Software-Defined Wide Area Network

SNMP：Simple Network Management Protocol

SSO：Single Sign On

SUDI：Secure Unique Device Identifier

TAC：Technical Assistance Center

TACACS：Terminal Access Controller Access Control System

TAM：Trust Anchor Module

TCP：Transmission Control Protocol

TLOC：Transport Location

TLS：Transport Layer Security

TPM：Trusted Platform Module

UCS：Unified Computing System

URL：Uniform Resource Locator

VPN：Virtual Private Network

VPC：Virtual Private Cloud
（仮想プライベート クラウド）

VNF：Virtual Network Function
（仮想ネットワーク機能）

VNET：Virtual Network
（仮想ネットワーク）

vQoE：Viptela Quality of Experience

VRRP：Virtual Router Redundancy Protocol

ZTP：Zero-Touch Provisioning

Aaron Rohyans
Ali Shaikh
Chandra Balaji Rajaram
David Klebanov
Deepesh Kumar
Gina Cornett
Hasham Malik
Kiran Ghodgaonkar
Madhavan Arunachalam
Nikolai Pitaev
Travis Carlson
Zaheer Aziz