ポリシーの概要

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

ポリシーは、オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス 間のデータトラフィックおよびルーティング情報のフローに影響を与えます。

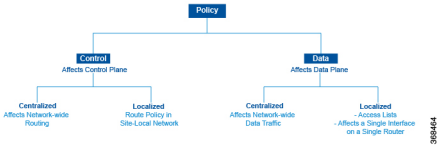
このポリシーは次の内容で構成されます。

- ルーティングポリシー：ネットワークのコントロールプレーンでのルーティング情報のフローに影響します。
- データポリシー：ネットワークのデータプレーンのデータトラフィックのフローに影響します。

企業固有のトラフィック制御要件を実装するには、基本ポリシーを作成し、ポリシー設定インフラストラクチャによってアクティブ化される高度な機能を展開します。

Cisco Catalyst SD-WAN オーバーレイ ネットワーク アーキテクチャがコントロールプレーンをデータプレーンから明確に分離し、一元管理型の機能とローカライズ型の機能の制御を分離しているように、Cisco Catalyst SD-WAN ポリシーも明確に分離されています。ポリシーは、コントロールプレーンまたはデータプレーントラフィックのいずれかに適用され、Cisco SD-WAN コントローラ で一元的に、または Cisco IOS XE Catalyst SD-WAN デバイス でローカルに設定されます。次の図は、制御ポリシーとデータポリシー間、および一元管理型ポリシーとローカルポリシー間の分離を示しています。

図 *1:* ポリシーのアーキテクチャ



制御ポリシーとデータポリシー

制御ポリシーはルーティング プロトコル ポリシーに相当し、データポリシーは一般にアクセス制御リスト（ACL）およびファイアウォールフィルタと呼ばれるものに相当します。

一元管理型ポリシーとローカライズ型ポリシー

Cisco Catalyst SD-WAN ポリシー設計では、一元管理型ポリシーとローカライズ型ポリシーを明確に分離しています。つまり、一元管理型ポリシーは、オーバーレイネットワーク内の一元化された Cisco SD-WAN コントローラでプロビジョニングされ、ローカライズ型ポリシーは、インターネット、MPLS、メトロイーサネットなどのトランスポートネットワークおよびブランチまたはエンタープライズサイト間のネットワークエッジにある、Cisco IOS XE Catalyst SD-WAN デバイス でプロビジョニングされるということです。

一元管理型ポリシー

一元管理型ポリシーとは、Cisco SD-WAN コントローラ 上でプロビジョニングされるポリシーのことであり、Cisco Catalyst SD-WAN オーバーレイネットワーク内の一元化されたコントローラです。一元管理型ポリシーは、次の 2 つのコンポーネントで構成されます。

- 制御ポリシー：トラフィックのオーバーレイネットワーク全体のルーティングに影響
- データポリシー：ネットワーク内の VPN セグメント全体のデータトラフィックフローに影響

一元管理型制御ポリシーは、Cisco SD-WAN コントローラ のルートテーブルに保存され、Cisco IOS XE Catalyst SD-WAN デバイス にアドバタイズされる情報に影響を与えることによって、トラフィックのネットワーク全体のルーティングに適用されます。一元管理型制御ポリシーの効果は、Cisco IOS XE Catalyst SD-WAN デバイス がオーバーレイネットワークのデータトラフィックを宛先に送信する方法に見られます。

（注） 一元管理型制御ポリシーの設定自体は Cisco SD-WAN コントローラ に残り、ローカルデバイスにプッシュされることはありません。

一元管理型データポリシーは、オーバーレイネットワーク内の VPN 全体のデータトラフィックのフローに適用されます。これらのポリシーは、6 タプルの一致（送信元と宛先の IP アドレスとポート、DSCP フィールド、プロトコル）または VPN メンバーシップのいずれかに基づいてアクセスを許可および制限できます。これらのポリシーは、選択した Cisco IOS XE Catalyst SD-WAN デバイス にプッシュされます。

ローカライズ型ポリシー

ローカライズ型ポリシーとは、Cisco IOS XE Catalyst SD-WAN デバイス の CLI または Cisco SD-WAN Manager デバイステンプレートを介してローカルにプロビジョニングされたポリシーを指します。

ローカライズ型制御ポリシーはルートポリシーとも呼ばれ、サイトローカルネットワーク上の（BGP および OSPF）ルーティング動作に影響します。

ローカライズ型データポリシーを使用すると、アクセスリストをプロビジョニングし、デバイス上の特定のインターフェイスに適用できます。簡易アクセスリストは、一元管理型データポリシーと同じように、6 タプルの照合（送信元と宛先の IP アドレスとポート、DSCP フィールド、およびプロトコル）に基づいてアクセスを許可および制限します。また、アクセスリストを使用すると、サービスクラス（CoS）のプロビジョニング、ポリシング、を行うことができ、デバイスのインターフェイスおよびインターフェイスキュー間でデータトラフィックが送受信される方法を制御できます。

Cisco Catalyst SD-WAN ポリシーの設計によって、基本ポリシーと高度なポリシーが区別されます。基本ポリシーは、オーバーレイネットワークを通過する基本的なトラフィックフローに影響を与えたり、決定したりすることができます。ここでは、ネットワークを介してトラフィックがルーティングされるパスの管理、パケットの IP ヘッダーのアドレス、ポート、DSCP フィールドに基づくトラフィックの許可またはブロックなどの標準的なポリシータスクを実行します。また、 Cisco IOS XE Catalyst SD-WAN デバイス のインターフェイスに出入りするデータトラフィックのフローを制御して、サービスクラス、キューイング、、ポリシングなどの機能を有効にすることもできます。

- アプリケーション認識型ルーティング。リアルタイムのネットワークとパスのパフォーマンス特性に基づいて、トラフィックのベストパスを選択します。
- cflowd。トラフィックフローのモニタリング用。

デフォルトでは、中央管理型 Cisco SD-WAN コントローラ またはローカル型 Cisco IOS XE Catalyst SD-WAN デバイス のいずれの Cisco IOS XE Catalyst SD-WAN デバイスにも、いかなるポリシーも設定されていません。ルート情報を配信するコントロール プレーン トラフィックがポリシングされていない場合、下記の通りとなります。

- OMP が Cisco IOS XE Catalyst SD-WAN デバイス 間で伝播するすべてのルート情報は、オーバーレイ ネットワーク ドメイン内のすべての Cisco SD-WAN コントローラ および Cisco IOS XE Catalyst SD-WAN デバイス で共有され、変更されません。
- Cisco IOS XE Catalyst SD-WAN デバイス がローカルサイトネットワーク内で伝播するルート情報に影響を与える BGP または OSPF ルートポリシーは設定されていません。

データプレーントラフィックがポリシングされていない場合、すべてのデータトラフィックは、ローカルの Cisco IOS XE Catalyst SD-WAN デバイス ルートテーブルのエントリのみに基づいて宛先に向けられ、オーバーレイネットワーク内のすべての VPN がデータトラフィックを交換できます。

- ポリシーのアーキテクチャ （4 ページ）
- Cisco Catalyst SD-WAN コントローラ のポリシーコンポーネント （13 ページ）

ポリシーのアーキテクチャ

このトピックでは、オーバーレイネットワーク全体にポリシーを実装するために使用される Cisco Catalyst SD-WAN ポリシーのアーキテクチャについて説明します。これらのポリシーは、Cisco SD-WAN Validator **ポリシー**または**一元管理型ポリシー**と呼ばれています。理由は、こうしたポリシーが Cisco SD-WAN コントローラ で一元的に設定されるからです。Cisco SD-WAN コントローラ ポリシーは、コントロール プレーン トラフィック（オーバーレイ管理プロトコル（OMP）によって伝送され、オーバーレイネットワークのトポロジとステータスを決定するために Cisco SD-WAN コントローラ によって使用されるルーティング更新）とデータプレーントラフィック（オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス 間を行き来するデータトラフィック）の両方のフローに影響を及ぼします。

Cisco Catalyst SD-WAN では、Cisco IOS XE Catalyst SD-WAN デバイス でもルーティングポリシーの作成が可能です。こうしたポリシーは、デバイス上でローカルにルーティングプロトコル（BGP または OSPF）に関連付けられている従来のルーティングポリシーと変わりありません。使用する場合は、従来の感覚で行えます。たとえば、BGP や OSPF を制御して、ルート情報の交換に影響を与えたり、ルート属性を設定したり、パス選択に影響を与えたりする場合と同じ感覚で使用できます。

一元管理型制御ポリシーのアーキテクチャ

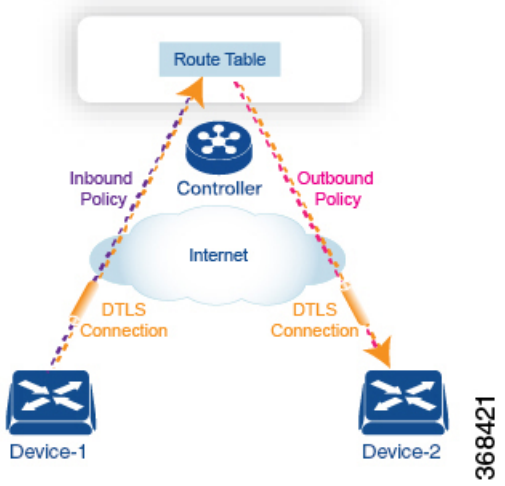
Cisco IOS XE Catalyst SD-WAN ネットワークアーキテクチャでは、一元管理型制御ポリシーは、実質的にネットワークのルーティングエンジンである Cisco SD-WAN コントローラ によって処理されます。Cisco SD-WAN コントローラ は、ネットワーク全体のルートで一元化されたマネージャであり、これらのルートのプライマリルートテーブルを管理します。Cisco SD-WAN コントローラ は、ドメイン内の Cisco IOS XE Catalyst SD-WAN デバイス によってアドバタイズされたルート情報に基づいてルートテーブルを作成し、これらのルートを使用してネットワークトポロジを検出し、ネットワークの宛先へのベストパスを決定します。Cisco SD-WAN コントローラは、そのルートテーブルからドメイン内のデバイスにルート情報を配布し、デバイスはこれらのルートを使用して、ネットワークを介してデータトラフィックを転送します。このアーキテクチャの結果、ネットワーク全体のルーティングの決定とルーティングポリシーは、ネットワーク内のデバイスによってホップごとに実装されるのではなく、中央機関によって調整されます。

一元管理型制御ポリシーを使用すると、Cisco SD-WAN コントローラ によってアドバタイズされるネットワークルートに影響を与えることができます。このタイプのポリシーは、Cisco SD-WAN コントローラ で一元的にプロビジョニングされ、Cisco SD-WAN コントローラ がプライマリルートテーブルに保存するルート情報と、デバイスに配布するルート情報の両方に影響します。

一元管理型制御ポリシーは、Cisco SD-WAN コントローラ でのみプロビジョニングおよび適用されます。制御ポリシーの設定自体は、オーバーレイネットワーク内のデバイスにプッシュされることはありません。オーバーレイ管理プロトコル（OMP）を使用してデバイスにプッシュされるのは、制御ポリシーの結果です。デバイスはこのポリシーをローカルルートテーブルにインストールし、データトラフィックの転送に使用します。この設計は、ネットワーク管理者が設計したポリシーを使用して、ネットワーク全体のルート配布が常に一元的に管理されることを意味します。これらのポリシーは、一元管理型の Cisco SD-WAN コントローラ によって常に実装され、Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークでルーティングの決定を調整します。

ネットワークドメイン内では、すべての Cisco SD-WAN コントローラ のネットワークトポロジマップを同期する必要があります。これをサポートするには、ドメイン内のすべての Cisco SD-WAN コントローラ で同一のポリシーを設定する必要があります。

図 *2:* 一元管理型制御ポリシー



ルート情報を含むすべての一元管理型制御プレーントラフィックは、デバイスとそのドメイン内の Cisco SD-WAN コントローラ 間のセキュアで永続的な DTLS 接続内で実行される OMP ピアリングセッションによって伝送されます。OMP ピアリングセッションのエンドポイントは、デバイスのシステム ID によって識別され、ピアリングセッションは、デバイスが配置されているサイトを識別するサイト ID を伝送します。DTLS 接続とその上で実行されている OMP セッションは、2 つのピアが動作している限りアクティブなままです。

制御ポリシーは、Cisco SD-WAN コントローラ がデバイスから受信するルートアドバタイズメントに対するインバウンドと、デバイスに送信するアドバタイズメントに対するアウトバウンドの両方に適用できます。インバウンド制御ポリシーは、Cisco SD-WAN コントローラ のローカル ルーティング データベースにインストールされるルートとルート情報、およびこの情報をそのままインストールするか変更するかを制御します。アウトバウンド制御ポリシーは、ルートがルーティングデータベースから取得された後、Cisco SD-WAN コントローラ がアドバタイズする前に適用され、ルート情報がそのままアドバタイズされるか、変更されるかに影響します。

ルート タイプ

Cisco SD-WAN コントローラ は、OMP によって伝送される Cisco IOS XE Catalyst SD-WAN 固有のルートである OMP ルートからネットワークトポロジを学習します。OMP ルートには次の 3 つのタイプがあります。

- Cisco IOS XE Catalyst SD-WAN OMP ルート：このルートは、デバイスがローカルネットワーク上で実行されているルーティングプロトコルから学習したプレフィックス情報を伝送します。情報には、BGP および OSPF から学習したルート、直接ルート、接続ルート、および静的ルートが含まれます。OMP は、OMP ルート SAFI（後続のアドレスファミリ識別子）を使用して OMP ルートを Cisco SD-WAN コントローラ にアドバタイズします。これらのルートは、一般に単に OMP ルートと呼ばれます。
- TLOC ルート：このルートは、デバイスが WAN またはトランスポートネットワークに接続する物理ポイントであるトランスポートロケーションに関連付けられたプロパティを伝送します。TLOC を識別するプロパティには、WAN インターフェイスの IP アドレスと、特定のトラフィックフローを識別する色が含まれます。OMP は TLOC SAFI を使用して TLOC ルートをアドバタイズします。
- サービスルート：これらのルートは、デバイスが接続されているローカルサイトネットワークで使用可能なネットワークサービス（ファイアウォールや IDP など）を識別します。OMP は、サービス SAFI を使用してこれらのルートをアドバタイズします。

これら 3 種類のルートの違いは、 Cisco SD-WAN コントローラ または Cisco IOS XE Catalyst SD-WAN デバイスの CLI にログインしているときに、さまざまな **show sdwan omp** 操作コマンドを使用して表示できます。 **show sdwan omp routes** コマンドは情報をプレフィックスでソートして表示し、**show sdwan omp services** コマンドはルート情報をサービスでソートして表示し、**show sdwan omp tlocs** コマンドはルート情報を TLOC でソートします。

一元管理型制御ポリシーを使用しない場合のデフォルト動作

デフォルトでは、一元管理型制御ポリシーは Cisco SD-WAN コントローラ でプロビジョニングされません。これにより、ドメイン内で次のルートアドバタイズメントおよび再配布動作は次のようになります。

- すべての Cisco IOS XE Catalyst SD-WAN デバイス は、サイトローカルネットワークから学習したすべてのルート関連プレフィックスを Cisco SD-WAN コントローラ に再配布します。このルート情報は、デバイスと Cisco SD-WAN コントローラ 間の DTLS 接続を介して送信される OMP ルートアドバタイズメントによって伝送されます。ドメインに複数の Cisco SD-WAN コントローラ が含まれている場合、デバイスはすべての OMP ルートアドバタイズメントをすべてのコントローラに送信します。
- すべてのデバイスは、OMP を使用して、すべての TLOC ルートをドメイン内の Cisco SD-WAN コントローラ またはコントローラに送信します。
- すべてのデバイスは、デバイスが配置されたローカルサイトで使用可能なネットワークサービス（ファイアウォールや IDP など）をアドバタイズするために、すべてのサービスルートを送信します。これらも OMP によって伝送されます。

- Cisco SD-WAN コントローラ は、ドメイン内のすべてのデバイスから受信したすべての OMP、TLOC、およびサービスルートを受け入れ、ルートテーブルにその情報を保存します。Cisco SD-WAN コントローラ は、どの OMP ルート、TLOC、およびサービスがどの VPN に属しているかを追跡します。Cisco SD-WAN コントローラ は、すべてのルートを使用してネットワークのトポロジマップを作成し、オーバーレイネットワークを通過するデータトラフィックのルーティングパスを決定します。
- Cisco SD-WAN コントローラ は、特定の VPN 内の OMP、TLOC、およびサービスルートから学習したすべての情報を、同じ VPN 内のすべてのデバイスに再配布します。
- デバイスは、ルート更新を定期的に Cisco SD-WAN コントローラ に送信します。
- Cisco SD-WAN コントローラ はルーティングパスを再計算し、ルートテーブルを更新し、新規および変更されたルーティング情報をすべてのデバイスにアドバタイズします。

一元管理型制御ポリシーを使用した場合の動作の違い

すべてのルート情報をドメイン内のすべての Cisco IOS XE Catalyst SD-WAN デバイス に再配布しない場合、または Cisco Catalyst SD-WAN コントローラ のルートテーブルに保存されているルート情報や Cisco Catalyst SD-WAN コントローラ によってアドバタイズされるルート情報を変更する場合は、一元管理型制御ポリシーを設計してプロビジョニングします。制御ポリシーをアクティブ化するには、インバウンドまたはアウトバウンド方向のオーバーレイネットワーク内の特定のサイトにそのポリシーを適用します。その際、方向は Cisco Catalyst SD-WAN コントローラを基点として考えます。一元管理型制御ポリシーのすべてのプロビジョニングは、Cisco Catalyst SD-WAN コントローラ で実行されます。

インバウンド方向に一元管理型制御ポリシーを適用すると、Cisco IOS XE Catalyst SD-WAN デバイス によってアドバタイズされているルートは Cisco Catalyst SD-WAN コントローラ のルートテーブルに配置される前にフィルタリングまたは変更されます。プロセスにおける最初のステップとして、ルートは受け入れられるか拒否されます。受け入れられたルートは、受信したルート、または制御ポリシーによって変更されたルートとして、Cisco Catalyst SD-WAN コントローラ のルートテーブルにインストールされます。制御ポリシーによって拒否されたルートは、通知なしに破棄されます。

アウトバウンド方向に制御ポリシーを適用すると、Cisco Catalyst SD-WAN コントローラによって Cisco IOS XE Catalyst SD-WAN デバイス に再配布されるルートがフィルタリングまたは変更されます。アウトバウンド方向のポリシーでは最初のステップとして、ルートは受け入れられるか拒否されます。受け入れられたルートの場合、一元管理型制御ポリシーを通じた、Cisco Catalyst SD-WAN コントローラ による配布前のルート変更が可能です。アウトバウンド方向のポリシーによって拒否されたルートはアドバタイズされません。

VPN メンバーシップポリシー

一元管理型データポリシーのもう 1 つのタイプは、VPN メンバーシップポリシーです。これは、Cisco IOS XE Catalyst SD-WAN デバイス が特定の VPN に参加できるかどうかを制御するポリシーです。VPN メンバーシップポリシーは、デバイスのどの VPN のルートであれば受信を許可し、どの VPN のルートなら受信を許可しないかを定義します。

VPN メンバーシップポリシーは一元管理できますが、それは、影響がパケットのヘッダーに対してのみで、Cisco IOS XE Catalyst SD-WAN デバイス がトラフィックの送信に使用するインターフェイスの選択には影響しないからです。一元管理をしていないと、VPN メンバーシップポリシーにより、ある特定の VPN のルートをデバイスが受信できない場合に、Cisco Catalyst SD-WAN コントローラ からそのドライバに対し、そうしたルートの転送が決して行われないということが起こります。

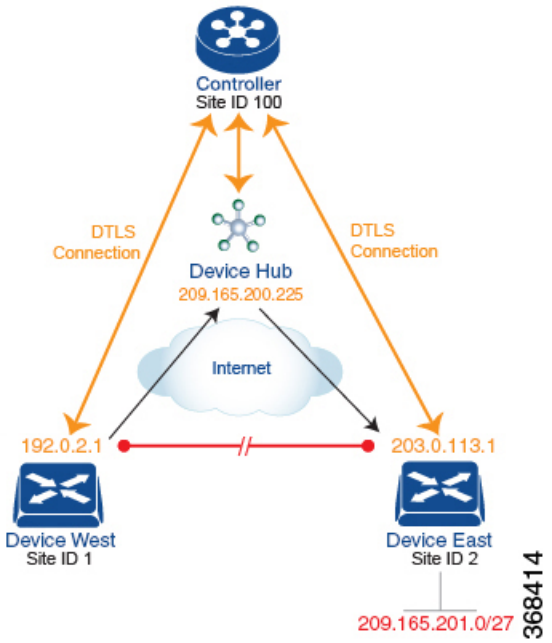
一元管理型制御ポリシーを使用したトラフィックフローの変更例

このセクションでは、一元管理型制御ポリシーを使用して、オーバーレイ ネットワークを通過するデータ トラフィックのフローを変更する方法について基本的な例をいくつか示します。

任意のトポロジの作成

2 つの Cisco IOS XE Catalyst SD-WAN デバイス の間でデータトラフィックが交換されるとき、制御ポリシーをプロビジョニングしていない場合、2 つのデバイスはそれらの間に IPsec トンネルを確立し、データトラフィックは1つのデバイスから次のデバイスに直接流れます。デバイスが2台のみのネットワーク、またはデバイスの数が少ないネットワークでは、通常、デバイスの各ペア間の接続の確立が問題になることはありません。ただし、このようなソリューションは拡張できません。数百または数千のブランチを持つネットワークでは、IPsec トンネルのフルメッシュを確立すると、各デバイスの CPU リソースに負担がかかります。

図 *3:* 任意のトポロジ



このオーバーヘッドを最小限に抑える方法の1つは、ハブアンドスポークタイプのトポロジを作成することです。この場合、デバイスの1つがハブサイトとして機能し、すべてのスポークまたはブランチデバイスからデータトラフィックを受信し、トラフィックを適切な宛先にリダイレクトします。この例では、このようなハブアンドスポークトポロジを作成する方法の1つ

を示します。これは、宛先に関連付けられたTLOCのアドレスを変更する制御ポリシーを作成することです。

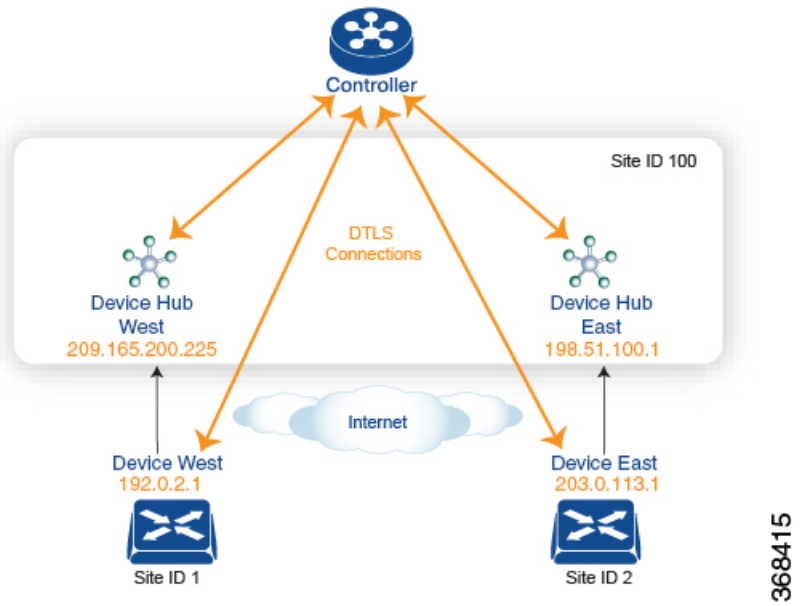
下図は、このようなポリシーがどのように機能するかを示しています。このトポロジには、West と East の 2 つのブランチロケーションがあります。制御ポリシーがプロビジョニングされていない場合、これらの2つのデバイスは、デバイス間にIPsecトンネルを作成することで、データトラフィックを直接交換します（赤線で表示）。ここで、West デバイスのルートテーブルには、宛先 TLOC が 203.0.113.1、色が gold（タプル {192.0.2.1, gold}）の East デバイスへのルートが含まれ、East デバイスのルートテーブルには、宛先 TLOC が {203.0.113.1, gold} である West ブランチへのルートが存在します。

ここで、ハブアンドスポークタイプのトポロジを設定するには、制御ポリシーをプロビジョニングして、West および East デバイスがもう一方のデバイス宛てのすべてのデータパケットをハブデバイスに送信するようにします。（制御ポリシーは常に一元管理型であるため、Cisco Catalyst SD-WAN コントローラ でプロビジョニングすることに注意してください）。West デバイスでは、ポリシーは単に宛先 TLOC を {203.0.113.1, gold} からハブデバイスの TLOC である {209.165.200.225, gold} に変更し、East デバイスでは、ポリシーは宛先 TLOC を {192.0.2.1, gold} からハブの TLOC である {209.165.200.225, gold} に変更します。ネットワークの West 側と East 側にデータトラフィックを交換する他のブランチサイトがある場合は、これら2つの同じ制御ポリシーを適用して、すべてのデータトラフィックをハブを介してリダイレクトすることができます。

トラフィック エンジニアリングの設定

制御ポリシーを使用すると、トラフィックエンジニアリングを設計およびプロビジョニングできます。単純なケースとして、ハブデバイスとして機能する2つのデバイスがあるとします。Cisco IOS XE Catalyst SD-WAN デバイス ブランチ宛てのデータトラフィックが常にいずれかのハブデバイスを通過するようにするには、目的のハブデバイスを優先するように TLOC プリファレンス値を設定します。

図 *4:* トラフィック エンジニアリング トポロジ

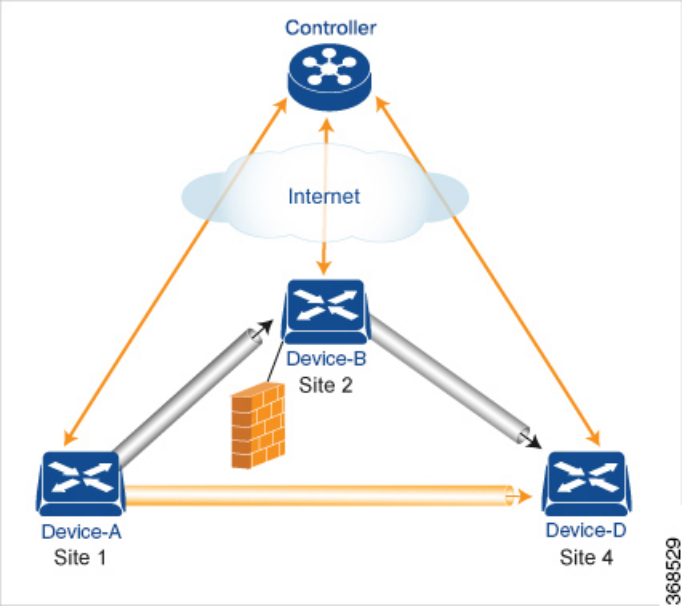


図は、サイト ID 100 に 2 つのハブデバイスがあることを示しています。1 つはネットワークの西側にサービスを提供し、もう 1 つは東側にサービスを提供します。デバイス西ブランチからのデータトラフィックはデバイス西側ハブで処理する必要があり、同様に、デバイス東ブランチからのデータトラフィックはデバイス東側ハブを通過する必要があります。

このトラフィックフローを設計するには、2 つの制御ポリシーをプロビジョニングします。1 つはデバイス西側デバイスが配置されているサイト ID 1 用、もう 1 つはサイト ID 2 用です。サイト ID 1 の制御ポリシーは、デバイス東宛てのトラフィックの TLOC を {209.165.200.225, gold} に変更し、サイト ID 2 の制御ポリシーは、サイト ID 1 宛てのトラフィックの TLOC を {198.51.100.1 gold} に変更します。このトラフィック エンジニアリング ポリシーのもう 1 つの作用は、2 つのハブデバイスを通過するトラフィックのロードバランシングです。

このようなトラフィック エンジニアリング ポリシーでは、送信元デバイスから宛先デバイスへのルートがローカルルートテーブルにインストールされ、送信元デバイスと宛先デバイス間のパスが使用可能かどうかに関係なく、トラフィックが宛先に送信されます。最終的な宛先へのパスのエンドツーエンド トラッキングを有効にすると、Cisco Catalyst SD-WAN コントローラは送信元から宛先へのパスをモニターし、そのパスが使用できない場合に送信元デバイスに通知できます。そこで送信元デバイスは、ルートテーブルからそのパスを変更または削除できるのです。

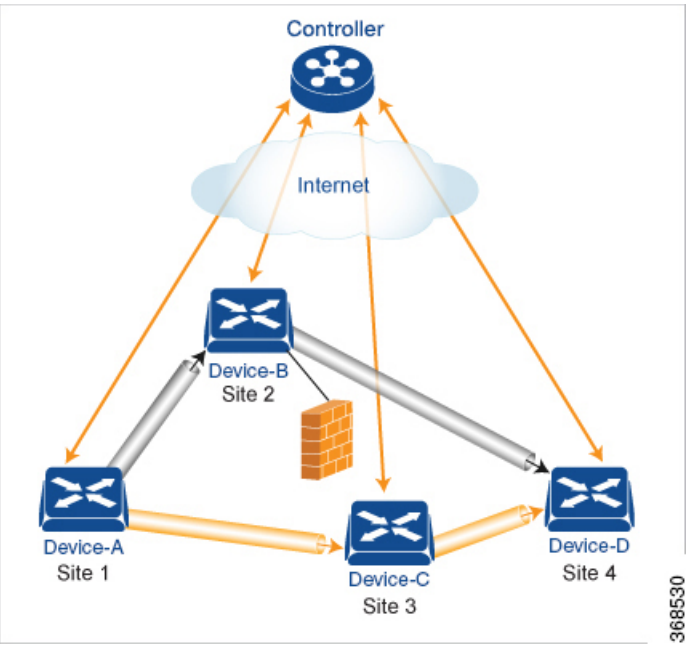
図 *5:* トラフィック エンジニアリング *2*



トラフィック エンジニアリング 2 の図は、エンドツーエンド パス トラッキングを表しています。デバイス A からデバイス D 宛てのトラフィックが最初に中間デバイスであるデバイス B に送信されることを示しているのですが、それは、この中間デバイスがファイアウォールなどのサービスを担っているからでしょう。（サイト 1 のデバイス A に適用される一元管理型制御ポリシーを使用して、このトラフィック エンジニアリングを設定します）。次に、最終的な宛先への直接パスを持つデバイス B がトラフィックをデバイス D に転送します。したがって、この例では、デバイス A とデバイス D の間のエンドツーエンドパスは 2 つのトンネルで構成されます。1 つはデバイス A とデバイス B の間、もう 1 つはデバイス B とデバイス D の間です。Cisco Catalyst SD-WAN コントローラ はこのエンドツーエンドパスを追跡し、デバイス B とデバイス D の間のパスの一部が使用できなくなった場合にデバイス A に通知します。

エンドツーエンド パス トラッキングの一部として、中間デバイスを使用した、送信元から最終的な宛先へのトラフィック転送方法は指定できるようになっています。デフォルトの方法は厳密な転送です。この場合、デバイス B にデバイス D への直接パスがあるかどうか、またはデバイス B とデバイス D 間のトンネルが稼働しているかどうかに関わらず、トラフィックは常にデバイス A からデバイス B に送信されます。柔軟な方法としては、一部またはすべてのトラフィックをデバイス A からデバイス D に直接転送するというのもあります。また、1 番目の中間デバイスが到達不能な場合の冗長パスを設けるために 2 番目の中間デバイスを設定し、ECMP 方式を使用して 2 つのデバイス間のトラフィックを転送するということもできます。トラフィック エンジニアリング 3 の図では、冗長中間デバイスとして Device-C を追加しています。

図 *6:* トラフィック エンジニアリング *3*



Cisco Catalyst SD-WAN コントローラ で設定する一元管理型制御ポリシーは、OMP ルートおよび OMP TLOC の情報に基づくルーティングポリシーに影響を及ぼします。

複数の Cisco Catalyst SD-WAN コントローラ があるドメインでは、オーバーレイネットワーク内のルーティングを安定させて予測可能な状態のままにしておくために、すべてのコントローラに同じ一元管理型制御ポリシーを設定しておく必要があります。

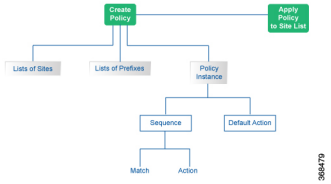
プレフィックスと IP ヘッダーに基づく一元管理型ポリシーの構成

送信元プレフィックスと宛先プレフィックス、および IP パケット内のヘッダーに基づく一元管理型データポリシーは、一連の番号付きの（順番に並んだ）マッチ/アクションペアのシーケンスで構成されます。これらのペアは、シーケンス番号の昇順で評価されます。パケットがマッチ条件のいずれかに一致すると、関連するアクションが実行され、そのパケットに対するポリシー評価が停止します。ポリシーの対象となる項目に対して必要なアクションが実行されるよう、ポリシーを設計する際はこの点に留意するようにしてください。

パケットがポリシー設定のどのシーケンスのパラメータにも一致しない場合、そのパケットはデフォルトではドロップされて廃棄されます。

構成コンポーネント

次の図は、一元管理型データポリシーの構成コンポーネントを示しています。



Cisco Catalyst SD-WAN コントローラ のポリシーコンポーネント

オーバーレイネットワーク全体のポリシーを実装する Cisco SD-WAN コントローラ ポリシーは、Cisco Catalyst SD-WAN 制御コンポーネント に実装されます。Cisco SD-WAN コントローラ は一元化されたデバイスであるため、Cisco SD-WAN コントローラ ポリシーを一元的に管理および維持でき、オーバーレイネットワーク全体でポリシー適用に関する一貫性を確保できます。

Cisco SD-WAN コントローラ ポリシーの実装は、Cisco Catalyst SD-WAN 制御コンポーネントでポリシー全体を設定することで行われます。Cisco SD-WAN コントローラ ポリシー設定は、次の 3 つの構成要素で実現されます。

- リスト：ポリシーの適用または照合のターゲットを定義します。
- ポリシー定義：制御と転送の側面を制御します。ポリシーには、次のようなさまざまなタイプがあります。
  - app-route-policy（アプリケーション認識型ルーティング用）
  - cflowd-template（cflowd フローモニタリング用）
  - control-policy（ルーティングおよびコントロールプレーン情報用）
  - data-policy（データトラフィック用）
  - vpn-membership-policy（トラフィックの範囲を特定の VPN に制限するため）
- ポリシーの適用：ポリシーの適用対象を制御します。ポリシーの適用はサイトに基づき、サイトリストと呼ばれる特定のリストによって定義されます。

これら 3 つの構成要素を組み合わせて Cisco SD-WAN コントローラ のポリシーを作成します。次の表に示すように、ポリシーとは具体的に、1 つ以上のリスト、1 つのポリシー定義、および少なくとも 1 つのポリシー適用の組み合わせです。

表 *1 : Cisco SD-WAN* コントローラ のポリシーの *3* つの構成要素

一覧（Lists）		ポリシーの定義		ポリシー アプリケーション
`data-prefix-list`：データポリシーで使用するプレフィックスのリスト `prefix-list`：他のポリシーで使用するプレフィックスのリスト `site-list`：policy と apply-policy で使用する site-id:s のリスト `tloc-list`：ポリシーで使用する tloc:s のリスト `vpn-list`：ポリシーで使用する vpn:s のリスト	+	`app-route-policy`：アプリケーション認識型ルーティングの `sla-classes` とともに使用 `cflowd-template`：Cisco IOS XE Catalyst SD-WAN デバイスで `cflowd` エージェントを設定 `control-policy`：OMP ルーティング制御を制御 `data-policy`：VPN 全体のポリシーベースルーティングを提供 `vpn-membership-policy`：ノード全体の VPN メンバーシップを制御	+	`apply-policy`：`site-list` とともに使用して、ポリシーが適用される先を決定
=				
Cisco SD-WAN コントローラ で設定され、Cisco SD-WAN コントローラ または Cisco IOS XE Catalyst SD-WAN デバイス のいずれかで適用されるポリシー定義を完了します。				

一覧（Lists）

リストとは、関連する項目をまとめて参照できるよう、グループ化する方法です。リストに含める項目の例に、プレフィックス、TLOC、VPN、オーバーレイ ネットワーク サイトなどがあります。Cisco SD-WAN コントローラ のポリシーでは、ポリシー定義の作成時と適用時の 2 か所でリストを呼び出します。関連項目の定義をポリシーの定義から分離するということは、リストの項目を追加または削除できる際、変更を 1 か所でのみ行えるということです。ポリシー定義を使用して変更する必要はありません。したがって、ネットワークに 10 個のサイトを追加し、それらに既存のポリシーを適用する場合は、サイト識別子をサイトリストに追加するだけで適用できます。また、ルールが適用されるプレフィックスや VPN などを手動で変更することなく、ポリシー規則を変更することもできます。

表 *2 :* リストのタイプ

リストのタイプ	使用方法
data-prefix-list	data-policy で使用され、トラフィック照合用にプレフィックスおよび上位層ポートを個別にまたはまとめて定義します。

リストのタイプ	使用方法
prefix-list	control-policy で使用され、RIB エントリに一致するプレフィックスを定義します。
site-list	control-policy では送信元サイトを照合するために、apply-policy ではポリシー適用のためのサイトを定義するために使用されます。
tloc-list	control-policy で使用され、RIB エントリに一致する TLOC を定義し、再定義された TLOC を vRoutes に適用します。
vpn-list	control-policy では RIB エントリに一致するプレフィックスを定義するために、data-policy と app-route-policy ではポリシー適用のための VPN を定義するために使われます。

次の設定は、Cisco SD-WAN コントローラ ポリシーリストのタイプを示しています。

```
policy
    lists
     data-prefix-list app1
      ip-prefix 209.165.200.225/27 port 100
    !
    prefix-list pfx1
     ip-prefix 209.165.200.225/27
    !
    site-list site1
     site-id 100
    !
    tloc-list site1-tloc
     tloc 209.165.200.225 color mpls
    vpn-list vpn1
     vpn1
    !
   !
```

ポリシーの定義

ポリシーの定義では、ポリシー規則を作成します。マッチ条件（制御ポリシーのルート関連プロパティおよびデータポリシーのデータ関連フィールド）と一致したときに実行するアクションを指定します。ポリシーにはマッチ/アクションのペアが含まれ、このペアには番号が付けられ、順番に検査されます。一致が発生するとアクションが実行され、そのルートまたはパケットのポリシー分析が終了します。ポリシー定義のタイプによっては、特定の VPN にのみ適用されます。

表 *3:* ポリシー タイプ

ポリシータイプ	使用方法
policy-type	**control-policy**、**data-policy**、または **vpn-menbership** でポリシーのタイプを指定できます。各タイプには、特定のシンタックスと、特定のマッチ条件および設定可能なアクションのセットがあります。
vpn-list	ポリシーを適用できる VPN をリストするために data-policy および app-route-policy で使用します。
sequence	ポリシーの各シーケンシャルステップをシーケンス番号で定義します。
match	特定のポリシーシーケンスで一致するエンティティを決定します。
アクション	直前の match ステートメントに対応するアクションを決定します。
default-action	ポリシーのどのシーケンスでも一致しないエンティティに対して実行するアクションです。デフォルトでは、アクションは拒否に設定されています。

次の設定は、Cisco SD-WAN コントローラ ポリシー定義のコンポーネントを示しています。これらの項目は、ポリシーの設計時に使用すべき論理的な順序でリストされています。また、設定に項目を追加する順序に関係なく、設定ではこの順序で項目が表示されます。

```
policy
    policy-type name
     vpn-list vpn-list
     sequence number
       match
        <route | tloc vpn | other>
    !
    action <accept reject drop>
     set attribute value
    !
    default-action <reject accept>
    !
   !
  !
```

ポリシー アプリケーション

設定コンポーネントは次のとおりです。

コンポーネント	使用方法
site-list	指定されたポリシーが適用されるサイトを決定します。方向（**in | out**）は、control-policy にのみ適用されます。
policy-type	ポリシータイプは**control-policy**、**data-policy**、または**vpn-membership** で、名前はセクションの site-list で指定されたサイトに適用される設定済みのポリシーを参照します。

ポリシー定義を有効にするには、オーバーレイネットワーク内のサイトに関連付けます。

```
apply-policy
 site-list name
  control-policy name <inout>
 !
 site-list name
  data-policy name
  vpn-membership name
  !
 !
```

ポリシーの例

リスト、ポリシー定義、ポリシー適用で構成される完全なポリシーです。次の例では、2 つのリスト（site-list と tloc-list）を作成します。1 つのポリシー（制御ポリシー）を定義し、そのポリシーを site-list に適用します。この図では、ノード設定で表示される項目がリストされています。通常の設定プロセスでは、最初にリストを作成し（使用するすべてのものをグループ化）、次にポリシー自体を定義し（実行することを定義）、最後にポリシーを適用します（設定したポリシーが適用されるサイトを指定）。

```
apply-policy
 site-list site1  ---------→ Apply the defined policy towards the sites in site-list
  control-policy prefer_local out
  !
policy
 lists
 site-list site1
  site-id 100
 tloc-list prefer_site1 ----→ Define the lists required for apply-policy and for use
within the policy
  tloc 192.0.2.1 color mols encap ipsec preference 400
 control-policy prefer_local
  sequence 10
   match route
    site-list sitele ------->Lists previously defined used within policy
  !
   action accept
    set
     tloc-list prefer_site
    !
   !
  !
```

ポリシーで使用される TLOC 属性

トランスポートロケーション（TLOC）は、オーバーレイネットワーク内の特定のインターフェイスを定義します。各 TLOC は、Cisco IOS XE Catalyst SD-WAN デバイス 間の OMP 更新で交換される一連の属性で構成されます。各 TLOC は、IP アドレス、色、およびカプセル化の 3 タプルによって一意に識別されます。他の属性を TLOC に関連付けることができます。

次にリスト表示した TLOC 属性は、Cisco SD-WAN コントローラ のポリシーで照合または設定できます。

表 *4:*

TLOC 属性	機能	アプリケーションポイント 設定元	アプリケーションポイント 変更元
アドレス（IP アドレス）	インターフェイスが配置されている送信元デバイスのシステム IP アドレスです。	送信元デバイスの設定	control-policy data-policy
キャリア	キャリアタイプの識別子。主に、トランスポートがパブリックかプライベートかを示します。	送信元デバイスの設定	control-policy
色	TLOC タイプの識別子です。	送信元デバイスの設定	control-policy data-policy
ドメイン ID	オーバーレイ ネットワーク ドメインの識別子です。	送信元デバイスの設定	control-policy
カプセル化	トンネルのカプセル化（IPsec または GRE のいずれか）です。	送信元デバイスの設定	control-policy data-policy
発信元（Originator）	発信元ノードのシステム IP アドレスです。	任意の発信者の設定	control-policy
[優先順位（Preference）]	OMP path-selection の設定。値が大きいほど、優先パスが高くなります。	送信元デバイスの設定	control-policy
サイト ID	特定のサイトの ID。サイトには、複数のノードまたは TLOC を設定できます。	送信元デバイスの設定	control-policy
Tag	任意による TLOC 識別子です。	送信元デバイスの設定	control-policy

ポリシーで使用される Cisco Catalyst SD-WAN ルート属性

Cisco Catalyst SD-WAN ルートは、オーバーレイネットワークのルートを定義したものです。標準 IP ルートに似ていますが、TLOC 属性と VPN 属性があります。OMP アップデート時には、Cisco IOS XE Catalyst SD-WAN デバイス で ルート交換が行われます。

次にリスト表示したルート属性は、Cisco SD-WAN コントローラ ポリシーで照合または設定できます。

表 *5:*

ルート属性	機能	アプリケーションポイント 設定元	アプリケーションポイント 変更元
Origin	ルートの送信元（BGP、OSPF、接続、静的のいずれか）。	送信元デバイス	control-policy
発信元（Originator）	ルートを伝送するアップデートの送信元。	発信元	control-policy
[優先順位（Preference）]	OMP path-selection の設定。値が大きいほど、優先パスが高くなります。	送信元デバイスまたはポリシーの設定	control-policy
サービス	ルートに関連付けられているアドバタイズされたサービス。	送信元デバイスの設定	control-policy
サイト ID	特定のサイトの識別子。サイトには、複数のノードまたは TLOC を設定できます。	送信元デバイスの設定	control-policy
Tag	任意による識別。	送信元デバイスの設定	control-policy
TLOC	ルートのネクストホップとして使用される TLOC。	送信元デバイスまたはポリシーの設定	control-policy data-policy
[VPN]	ルートが属する VPN。	送信元デバイスまたはポリシーの設定	control-policy data-policy

Cisco Catalyst SD-WAN Controller ポリシー処理と適用の設計

Cisco SD-WAN コントローラ ポリシーがどのように処理および適用されるかを理解することで、ポリシーを適切に設計し、オーバーレイネットワーク全体でポリシーを実装する方法を評価できます。

ポリシーは次のように処理されます。

- ポリシー定義は、番号付きで番号順に並んだ一連のマッチ/アクションペアで構成されます。各ポリシー内では、ペアリングは、最小の番号から始まり、番号順に処理されます。
- 一致があった場合、一致したエンティティはシーケンスの設定されたアクションの対象になり、その後継続的な処理の対象にはなりません。
- シーケンスで一致しないエンティティは、ポリシーのデフォルトアクションの対象になります。デフォルトでは、このアクションは拒否されます。

Cisco SD-WAN コントローラ ポリシーはサイトリストごとに適用されるため、次のようになります。

- サイトリストにポリシーを適用する場合は、各タイプのポリシーを 1 つだけ適用できます。たとえば、1 つの制御ポリシーと 1 つのデータポリシー、または 1 つの制御ポリシーを入力し、1 つの制御ポリシーを出力することができます。2 つのデータポリシーまたは 2 つのアウトバウンド制御ポリシーを設定することはできません。
- サイトリストは多数のサイトをグループ化したものであるため、1 つのサイトを複数のサイトリストに含める場合は注意が必要です。サイトリストにさまざまなサイト識別子が含まれている場合は、重複がないことを確認します。同じサイトが 2 つのサイトリストに属し、同じタイプのポリシーが両方のサイトリストに適用されている場合、ポリシーの動作は予測できず、致命的となる可能性があります。
- 制御ポリシーは単方向であり、Cisco SD-WAN コントローラ へのインバウンドまたはアウトバウンドのいずれかに適用されます。両方向で制御ポリシーが必要な場合は、2 つの制御ポリシーを設定します。
- データポリシーは双方向であり、Cisco IOS XE Catalyst SD-WAN デバイス のサービス側から受信したトラフィック、トンネル側から受信したトラフィック、またはこれらすべての組み合わせに適用できます。
- VPN メンバーシップポリシーは、Cisco SD-WAN コントローラ からの発信トラフィックに常に適用されます。
- 制御ポリシーは Cisco SD-WAN コントローラ に残り、コントローラが送受信するルートに影響します。

- データポリシーは、サイトリスト内の Cisco IOS XE Catalyst SD-WAN デバイス に送信されます。ポリシーは OMP 更新で送信され、デバイスが送受信するデータトラフィックに影響します。
- オーバーレイネットワーク内のいずれかのノードがルーティングを決定する場合、使用可能なすべてのルーティング情報を使用します。オーバーレイネットワークで、ルーティング情報を Cisco IOS XE Catalyst SD-WAN デバイス ノードに配布するのは Cisco Catalyst SD-WAN コントローラ です。
- 複数の Cisco Catalyst SD-WAN コントローラ があるネットワーク展開では、各コントローラが独立して動作し、ルーティング情報を他の Cisco SD-WAN コントローラ およびオーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス に伝達します。したがって、Cisco SD-WAN コントローラ ポリシーがオーバーレイネットワークで目的の効果を持つようにするには、Cisco SD-WAN コントローラ のそれぞれに同じポリシーを設定し、同じように適用する必要があります。どのポリシーでも、同じポリシーを設定し、すべての Cisco SD-WAN コントローラ に同じように適用する必要があります。

（注） ポリシーを展開すると、展開ステータスはポリシーのタイムアウト制限である 30 分間のみ更新されます。タイムアウト期間が経過すると、展開タスクのステータスはモニタリングされません。行数が多く、より大きなポリシーを展開し、それが 30 分以上かかる場合、タスクのステータスはモニタリングされません。

Cisco Cisco Catalyst SD-WAN Controller によるポリシーの運用

大まかに説明すると、制御ポリシーとは、ルーティング情報という、Cisco IOS XE Catalyst SD-WAN ネットワークで OMP アップデートの際に伝送される情報をもとに操作を行うポリシーです。データポリシーはデータトラフィックに影響を及ぼすものであり、VPN メンバーシップは VPN ルーティングテーブルの配布を制御するものです。

基本的な Cisco SD-WAN コントローラ ポリシーは次のとおりです。

- 制御ポリシー
- データポリシー
- VPN メンバーシップ

制御ポリシー

制御ポリシーは標準的なルーティングポリシーに類似し、オーバーレイネットワークのコントロールプレーンのルートおよびルーティング情報に作用します。Cisco SD-WAN コントローラでプロビジョニングされる一元管理型制御ポリシーは、オーバーレイネットワークを介した

ルーティングパスを決定または影響を与えるネットワーク全体のルーティング決定をカスタマイズするための Cisco Catalyst SD-WAN の技術です。Cisco IOS XE Catalyst SD-WAN デバイスでプロビジョニングされるローカル制御ポリシーを使用すると、サイトローカルブランチまたはエンタープライズ ネットワークで BGP および OSPF によって行われるルーティングの決定をカスタマイズできます。

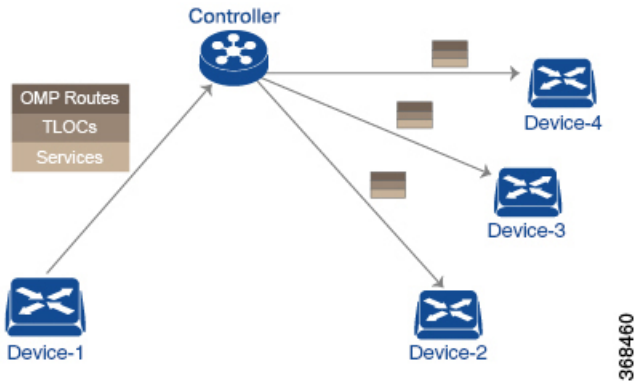
一元管理型制御ポリシーの基礎となるルーティング情報は、Cisco IOS XE Catalyst SD-WAN ルートアドバタイズメントで伝送され、Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間の DTLS または TLS 制御接続で送信されます。一元管理型制御ポリシーによって、Cisco SD-WAN コントローラ の一元管理型ルートテーブルに配置されるルートおよびルート情報、およびオーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスにアドバタイズされるルートおよびルート情報が決定されます。基本的な一元管理型制御ポリシーはトラフィック エンジニアリングを確立し、トラフィックがネットワークを通過するパスを設定します。高度な制御ポリシーは、オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス がファイアウォールやロードバランサなどのネットワークサービスを共有できるようにする、多数の機能をサポートしています。

一元管理型制御ポリシーは、Cisco SD-WAN コントローラ によってオーバーレイネットワーク全体に配信される OMP ルートに影響します。Cisco SD-WAN コントローラ は、Cisco SD-WAN コントローラ とデバイス間の DTLS または TLS 接続内の OMP セッションを介して Cisco IOS XE Catalyst SD-WAN デバイス によってアドバタイズされた OMP ルートから、オーバーレイネットワーク トポロジを学習します。

3 つのタイプの OMP ルートは、Cisco SD-WAN コントローラ がネットワークトポロジを決定するために使用する情報を伝送します。

- Cisco Catalyst SD-WAN OMP ルートは IP ルートアドバタイズメントに類似しており、デバイスがローカルサイトから学習したルーティング情報と、ローカル ルーティング プロトコル（BGP および OSPF）を Cisco SD-WAN コントローラ にアドバタイズします。これらのルートは、OMP ルートまたはルートとも呼ばれます。
- TLOC ルートは、トランスポートネットワークに接続するインターフェイスの IP アドレス、トラフィックフローを識別するリンクの色、カプセル化タイプなど、オーバーレイネットワーク固有のロケータプロパティを伝送します。（TLOC（トランスポートロケーション）は、Cisco IOS XE Catalyst SD-WAN デバイス がトランスポートネットワークに接続する物理的なロケーションを意味します。IP アドレス、リンクの色、カプセル化によって主に識別されますが、他にも多くのプロパティが TLOC に関連付けられます）。
- サービスルートは、ローカルサイトの VPN メンバーが使用できるファイアウォールなどのネットワークサービスをアドバタイズします。

図 7: 制御ポリシーのトポロジ



デフォルトでは、一元管理型制御ポリシーはプロビジョニングされません。ポリシーがまったく適用されていないネットワークでは、すべての OMP ルートがそのまま Cisco SD-WAN コントローラ のルートテーブルに配置され、Cisco SD-WAN コントローラ はすべての OMP ルートをそのまま、ネットワークドメイン内の同一 VPN 内のあらゆるデバイスにアドバタイズします。

一元管理型制御ポリシーをプロビジョニングすることで、Cisco SD-WAN コントローラ のルートテーブルに配置される OMP ルート、デバイスにアドバタイズされるルート情報、および OMP ルートの変更をルートテーブルへの配置前またはアドバタイズ前にするかどうかに影響を与えることができます。

Cisco IOS XE Catalyst SD-WAN デバイス は、Cisco SD-WAN コントローラ から学習したすべてのルート情報をそのままローカルルートテーブルに配置して、データトラフィックの転送時に使用します。Cisco SD-WAN コントローラ の役割はネットワーク内の一元化されたルーティングシステムであるため、Cisco IOS XE Catalyst SD-WAN デバイス は、Cisco SD-WAN コントローラ から学習した OMP ルート情報を変更することはできません。

Cisco SD-WAN コントローラ はデバイスから OMP ルートアドバタイズメントを定期的に受信し、オーバーレイネットワークを介してルーティングパスを再計算および更新した後、新しいルーティング情報をデバイスにアドバタイズします。

Cisco SD-WAN コントローラ でプロビジョニングした一元管理型制御ポリシーは Cisco SD-WAN コントローラに残り、デバイスにダウンロードされることはありません。ただし、一元管理型制御ポリシーの結果としてのルーティングの決定は、ルートアドバタイズメントの形でデバイスに渡されるため、制御ポリシーの影響は、デバイスがデータトラフィックを宛先に転送する方法に反映されます。

デバイス上でローカルにプロビジョニングされるローカライズ型制御ポリシーは、ルートポリシーと呼ばれます。このポリシーは、通常のドライバで設定するルーティングポリシーに似ており、サイトとローカル間ネットワークでの BGP および OSPF ルーティング動作を変更できるようにします。一元管理型制御ポリシーはオーバーレイネットワーク全体のルーティング動作に影響しますが、ルートポリシーはローカルブランチのルーティングにのみ適用されます。

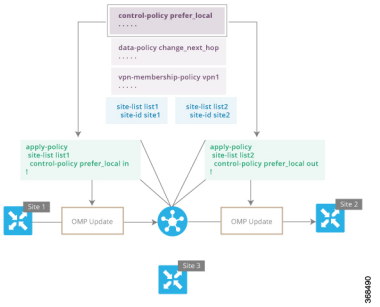
Cisco IOS XE Catalyst SD-WAN デバイスは OMP アップデートを定期的に交換し、オーバーレイネットワークに関するルーティング情報を伝送します。これらのアップデートには、ルート属性とトランスポートロケーション（TLOC）属性の 2 つが含まれます。

Cisco SD-WAN コントローラは、OMP アップデートによるこれらの属性からオーバーレイネットワークのトポロジとステータスを判断し、オーバーレイネットワークに関するルーティング情報をルートテーブルにインストールします。次に、コントローラは OMP アップデートを送信することで、ネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス にオーバーレイトポロジをアドバタイズします。

制御ポリシーは、OMP アップデートに含まれるルート属性と TLOC 属性を調べて、ポリシーに一致する属性を変更できます。制御ポリシーによる変更は、インバウンドまたはアウトバウンドのいずれかの方向に適用されます。

この図は、Cisco SD-WAN コントローラ に設定された **prefer_local** という制御ポリシーを、サイト 1（site-list list1 経由）とサイト 2（site-list list2 経由）に適用したものです。

図 *8*: 制御ポリシーのトポロジ




```
Device# apply-policy
site-list list1
control-policy prefer_local in
!
```

左上の矢印は、ポリシーがサイト 1、具体的にはサイト 1 のエントリを含む **site-list list1** に適用されていることを示しています。コマンド **control-policy prefer_local** は、Cisco IOS XE Catalyst SD-WAN デバイス から Cisco SD-WAN コントローラに入ってくる OMP アップデートにポリシーを適用するために使用されます。これは、コントローラからはインバウンドにあたります。**in** キーワードは、**inbound** ポリシーを示します。そのため、サイト 1 のデバイスが Cisco SD-WAN コントローラ に送信するすべての OMP アップデートにおいて、「prefer_local」制御ポリシーは、アップデートが Cisco SD-WAN コントローラ のルートテーブルに到達する前に適用されます。OMP アップデートのルートまたは TLOC 属性がポリシーと一致する場合、Cisco SD-WAN コントローラ が OMP アップデート情報をルートテーブルにインストールする前に、ポリシーアクションの結果としての変更が発生します。

Cisco SD-WAN コントローラ のルートテーブルは、オーバーレイネットワークのトポロジを決定するために使用されます。次に、Cisco SD-WAN コントローラ はこのトポロジ情報を OMP アップデートを介してネットワーク内のすべてのデバイスに配信します。ポリシーをインバウンド方向に適用すると、Cisco SD-WAN コントローラ で使用可能な情報に影響を与えるためです。これはネットワークトポロジとネットワークの到達可能性を決定し、ルート属性と TLOC 属性をコントローラのルートテーブルに配置する前に変更します。

```
apply-policy
site-list list2
control-policy prefer_local out
!
```

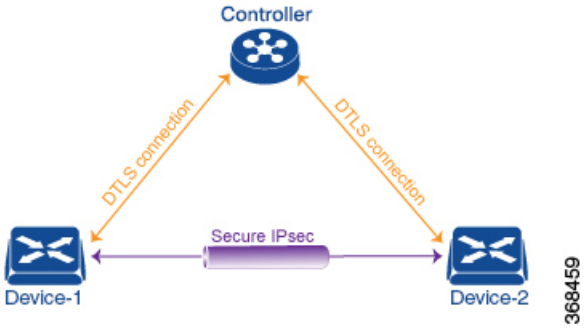
上の図の右側では、**control-policy prefer_local out** コマンドにより「prefer_local」ポリシーがサイト 2 に適用されています。コマンドの **out** キーワードは、**outbound policy** を示します。これは、Cisco SD-WAN コントローラ がサイト 2 のデバイスに送信する OMP アップデートにポリシーが適用されることを意味します。ポリシーに起因する変更は、Cisco SD-WAN コントローラ のルートテーブルからの情報が OMP アップデートに配置された後、デバイスがアップデートを受信する前に発生します。方向はここでも、Cisco SD-WAN コントローラ の観点からはアウトバウンドであることに注意してください。

Cisco SD-WAN コントローラ 上の一元化されたルートテーブルに影響し、オーバーレイネットワーク内のすべてのデバイスにアドバタイズされるルート属性に広く影響するインバウンドポリシーとは対照的です。アウトバウンド方向に適用される制御ポリシーは、サイトリストに含まれる個々のデバイス上のルートテーブルにのみ影響します。

同じ制御ポリシー（**prefer_local** ポリシー）が、インバウンドとアウトバウンドの両方の OMP アップデートに適用されます。ただし、同じポリシーをインバウンドとアウトバウンドに適用した場合の影響は異なります。図に示す使用方法は、Cisco IOS XE Catalyst SD-WAN 制御ポリシー設計のアーキテクチャと構成の柔軟性を示しています。

データポリシー

データポリシーは、パケットの IP ヘッダー内のフィールド、またはトラフィックが送受信されるルータインターフェイスのいずれかに基づいて、ネットワークを通過するデータトラフィックのフローに影響を与えます。データトラフィックは、隣接する図に紫色で示されている Cisco IOS XE Catalyst SD-WAN デバイス 間の IPsec 接続を介して移動します。

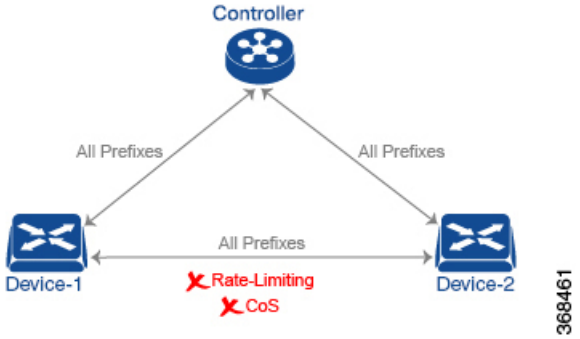


この Cisco IOS XE Catalyst SD-WAN アーキテクチャでは、次の 2 種類のデータポリシーを実装します。

- パケットの IP ヘッダー（5 タプルと呼ばれる）の送信元アドレスと宛先アドレス、ポート、およびDSCP フィールドに基づいて、そしてネットワーク セグメンテーションと VPN メンバーシップを基に、データトラフィックのフローを制御する一元管理型データポリシー。こうしたタイプのデータポリシーは、Cisco SD-WAN コントローラ で一元的にプロビジョニングされ、ネットワーク全体のトラフィックフローに影響を与えます。

- Cisco IOS XE Catalyst SD-WAN デバイス 上のインターフェイスおよびインターフェイスキューに出入りするデータトラフィックのフローを制御するローカライズ型データポリシー。このタイプのデータポリシーは、アクセスリストを使用してローカルにプロビジョニングされます。トラフィックを分類し、異なるクラスを異なるキューにマッピングできます。また、トラフィックをミラーリングし、データトラフィックの送受信レートをポリシングすることもできます。

デフォルトでは、一元管理型データポリシーはプロビジョニングされません。そのため、VPN 内のすべてのプレフィックスは、その VPN 内のどこからでも到達可能になります。一元管理型データポリシーをプロビジョニングすると、送信元と宛先間のアクセスを制御する 6 タプルフィルタを適用できます。



一元管理型制御ポリシーと同様に、一元管理型データポリシーを Cisco SD-WAN コントローラにプロビジョニングすると、その設定は Cisco SD-WAN コントローラ に残ります。データポリシーの効果は、Cisco IOS XE Catalyst SD-WAN デバイス によるデータトラフィックを宛先に転送する方法に反映されます。ただし、制御ポリシーとは異なり、一元管理型データポリシーは読み取り専用でデバイスにプッシュされます。これらはルータの構成ファイルには追加されませんが、ルータの CLI から表示できます。

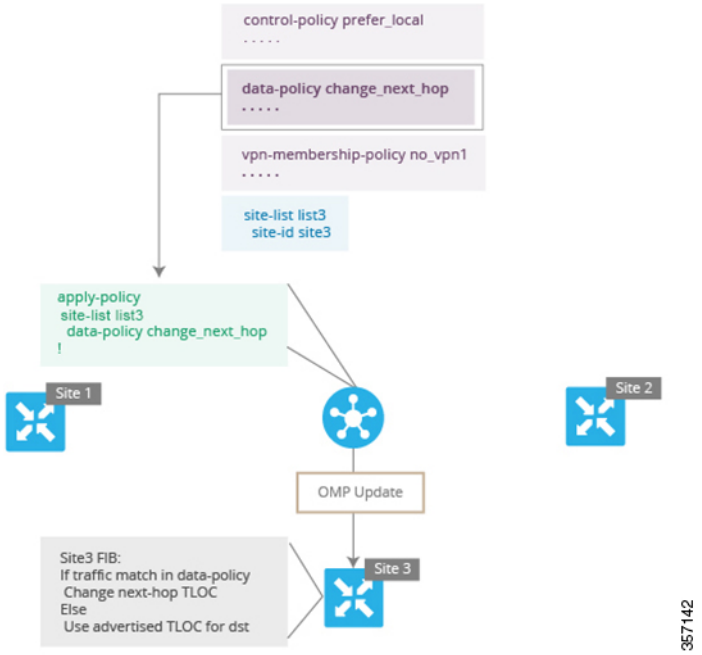
Cisco IOS XE Catalyst SD-WAN デバイス にアクセスリストがプロビジョニングされていない場合、すべてのデータトラフィックは、インターフェイスのキューの 1 つを使用して、ラインレートで同じ重要度でもって送信されます。アクセスリストを使用すると、サービスクラスをプロビジョニングできます。これにより、データトラフィックを重要度で分類して、複数のインターフェイスキューに展開させ、さまざまなクラスのトラフィックの送信レートを制御できるようになります。ポリシングもプロビジョニングできます。

データポリシーは、送信元と宛先のアドレスとポート、プロトコル、DSCP 値を参照してデータパケットのヘッダー内のフィールドを調査します。マッチするパケットについては、さまざまな方法でネクストホップを変更するか、パケットにポリサーを適用します。データポリシーが Cisco SD-WAN コントローラ で設定および適用されると、ポリシーが適用されるサイトリスト内の Cisco IOS XE Catalyst SD-WAN デバイス に OMP アップデートで送信されます。データトラフィックを送受信するときに、マッチ操作とその結果に伴うアクションがデバイス上で実行されます。

データポリシートポロジの図では、「change_next_hop」という名前のデータポリシーが、サイト 3 を含むサイトのリストに適用されます。Cisco SD-WAN コントローラ がサイト 3 のデバイスに送信する OMP 更新には、このポリシー定義が含まれています。デバイスは、ポリシーに

マッチするデータトラフィックを送受信すると、ネクストホップを指定されたTLOCに変更します。マッチしないトラフィックは、元のネクストホップ TLOC に転送されます。

図 *9*: データポリシートポロジ



データポリシーの **apply-policy** コマンドで、デバイスから見た方向を指定します。図の「all」方向では、トンネルインターフェイスを通過するインバウンドおよびアウトバウンドデータトラフィックに対し、ポリシーが適用されます。**data-policy change_next_hop from-tunnel** コマンドを使用してポリシーのスパンをインバウンドトラフィックのみに制限したり、**data-policy change_next_hop from-service** コマンドを使用してアウトバウンドトラフィックのみに制限したりできます。

VPN メンバーシップポリシーの運用

VPN メンバーシップポリシーは、その名前が示すように、特定の Cisco IOS XE Catalyst SD-WAN デバイス に配布される VPN ルートテーブルに影響します。 VPN メンバーシップポリシーのないオーバーレイネットワークでは、Cisco Catalyst SD-WAN コントローラ はすべての VPN のルートをすべてのデバイスにプッシュします。ビジネス使用モデルで特定の VPN への特定のデバイスの参加を制限する場合は、VPN メンバーシップポリシーを使用してこの制限を適用します。

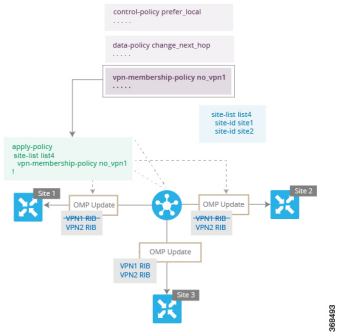
下図のVPN メンバーシップトポロジは、VPN メンバーシップポリシーの仕組みを示しています。このトポロジには、3 つの Cisco IOS XE Catalyst SD-WAN デバイス があります。

- サイト 1 および 2 の Cisco IOS XE Catalyst SD-WAN デバイス は、VPN 2 のみにサービスを提供します。

- サイト 3 の Cisco IOS XE Catalyst SD-WAN デバイス は、VPN 1 と VPN 2 の両方にサービスを提供します。

この図では、サイト 3 のデバイスは Cisco SD-WAN コントローラ からすべてのルート更新を受信します。これは、これらの更新が VPN 1 と VPN 2 の両方に対するものであるためです。ただし、他の Cisco IOS XE Catalyst SD-WAN デバイス は VPN 2 のみにサービスを提供するため、これらに送信されたルート更新をフィルタリングし、VPN 1 に関連付けられているルートを削除して、VPN 2 に適用されるルートのみを送信できます。

図 *10 : VPN* メンバーシップトポロジ

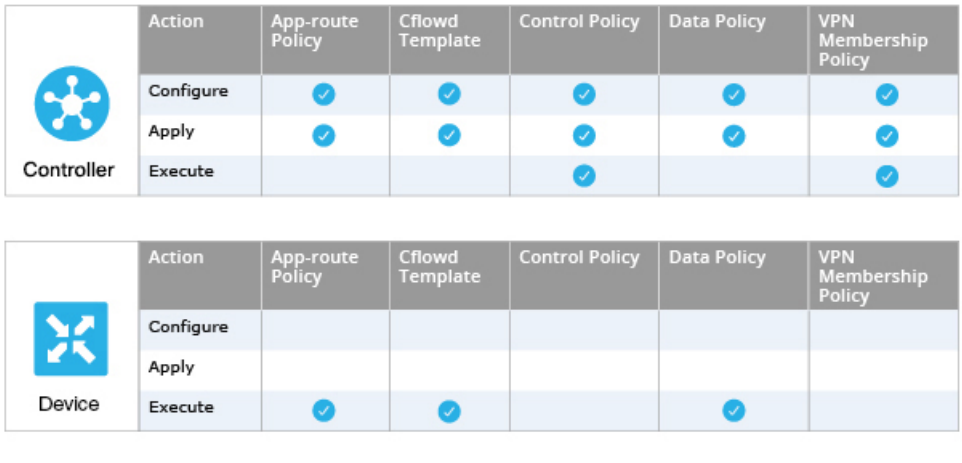


ここでは、VPN メンバーシップポリシーを適用するときに方向が設定されていないことに注意してください。Cisco SD-WAN コントローラ は、Cisco IOS XE Catalyst SD-WAN デバイス の外部に送信する OMP 更新に常にこのタイプのポリシーを適用します。

Cisco SD-WAN コントローラ ポリシーの設定と実行

すべての Cisco SD-WAN コントローラ ポリシーの設定は、ポリシーの定義とリストの組み合わせを使用して、Cisco IOS XE Catalyst SD-WAN デバイス に対して行われます。すべての Cisco SD-WAN コントローラ ポリシーの適用も、apply-policy とリストを組み合わせて、Cisco IOS XE Catalyst SD-WAN デバイス に対して行われます。ただし、次の図に示すように、実際の Cisco SD-WAN コントローラ ポリシーが実行される場所はポリシーのタイプによって異なります。

図 *11 : Cisco SD-WAN* コントローラ ポリシー



制御ポリシーと VPN メンバーシップポリシーの場合、ポリシー設定全体は Cisco SD-WAN コントローラに残り、ポリシーにマッチするルートまたはVPNの結果として実行されるアクションは Cisco SD-WAN コントローラ で実行されます。

他の 3 つのポリシータイプ（アプリケーション認識型ルーティング、cflowdテンプレート、およびデータポリシー）の場合、ポリシーは OMP 更新で Cisco IOS XE Catalyst SD-WAN デバイス に送信され、ポリシーの結果として実行されるアクションはデバイスで実行されます。

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