サービス チェーニング

（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。

ネットワーク内のサービス

ファイアウォール、ロードバランサ、侵入検知と防御（IDP）などのサービスは通常、仮想環境内で実行され、物理的に1か所に集中することもあれば、冗長性を確保するために数か所に分散されることもあります。サービスは、内部、クラウドベース、または外部のサブスクリプションの場合があります。ネットワークはこのようなサービスを介して、ネットワーク内の任意の場所からのトラフィックを再ルーティングできなければなりません。

お客様は、キャパシティ、冗長性、または単に最高水準の技術を選択するために、新しいサービスを要求に応じて社内に導入したり、社外にサブスクライブできるようにしたいと考えています。たとえば、ファイアウォールサイトがその容量を超えた場合、新しい場所で新しいファイアウォールサービスを生成できるなどです。この新しいファイアウォールをサポートするには、ポリシーベースで重み付けされた負荷分散を複数のファイアウォールに設定する必要があります。

サービスまたはサービスチェーンを介してトラフィックフローを再ルーティングする理由の一部を以下に示します。

- 安全性の低いネットワーク領域からのトラフィックフローは、改ざんされていないことを確認するために、ファイアウォールなどのサービスを通過するか、サービスチェーンを通過する必要があります。

- 複数のVPNで構成され、それぞれが機能または組織を代表するネットワークの場合、VPN間のトラフィックは、ファイアウォールなどのサービスまたはサービスチェーンを通過する必要があります。たとえばキャンパス内では、部門間のトラフィックはファイアウォールを通過し、部門内のトラフィックは直接ルーティングされる場合があります。
- 特定のトラフィックフローは、ロードバランサなどのサービスを通過する必要があります。

現在、トラフィックフローを再ルーティングする唯一の方法は、ポリシールートを使用して、送信元からサービスノード、サービスノードからその先のシステムにいたるまで、すべてのルーティングノードをプロビジョニングすることです。これは、オペレータが各ノードを手動で設定するか、オペレータに代わって各ノードの設定を実行するプロビジョニングツールを使用して行います。いずれの場合も、このプロセスのプロビジョニング、維持、およびトラブルシューティングは運用上複雑です。

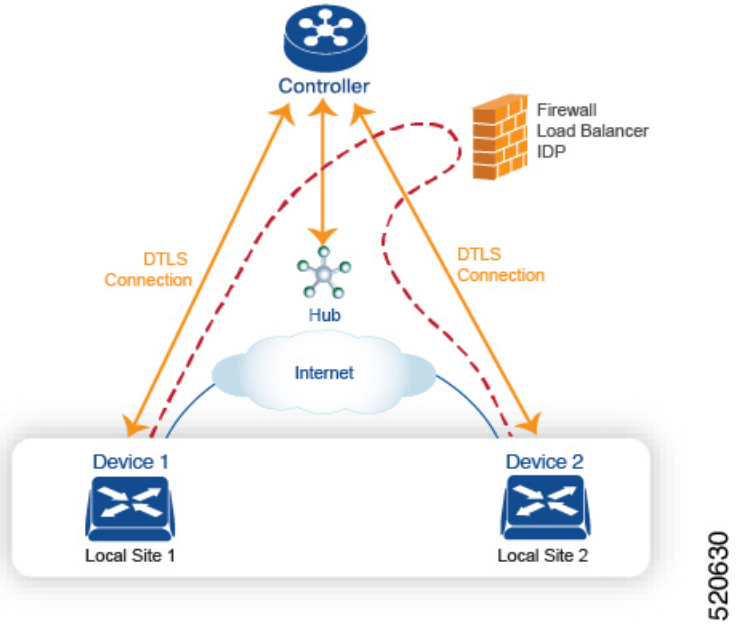
Cisco Catalyst SD-WAN オーバーレイネットワークにおけるサービスのプロビジョニング

Cisco Catalyst SD-WAN ソリューションでは、ネットワークオペレータは、中央コントローラ、つまり Cisco SD-WAN コントローラ から、すべてのサービスチェーンを有効にしてオーケストレーションできます。設定やプロビジョニングはどのデバイスにも必要ありません。

Cisco Catalyst SD-WAN ネットワークにおけるサービスチェーンの一般的なフローは次のとおりです。

- デバイスは、ブランチまたはキャンパスで使用可能なサービス（ファイアウォール、IDS、IDP など）をドメイン内の Cisco SD-WAN コントローラ にアドバタイズします。複数のデバイスが同じサービスをアドバタイズできます。
- また、デバイスは OMP ルートと TLOC を Cisco SD-WAN コントローラ にアドバタイズします。
- サービスを必要とするトラフィックの場合、Cisco SD-WAN コントローラ のポリシーは、OMP ルートのネクストホップをサービス ランディング ポイントに変更します。このようにして、トラフィックはサービスによって最初に処理されてから、最終的な宛先にルーティングされます。

次の図は、Cisco Catalyst SD-WAN ソリューションでサービスチェーンがどのように機能するかを示しています。図のネットワークでは、中央ハブルータが2つのブランチに接続され、それぞれにデバイスを備えています。標準的なネットワーク設計では、ブランチサイト1からブランチサイト2へのトラフィックはすべてハブルータを通過するような制御ポリシーが実装されています。ハブルータの背後には、ファイアウォールデイバスがあります。ここで、サイト1 からサイト 2 へのすべてのトラフィックを、最初にファイアウォールで処理するとします。サイト1のデバイスからのトラフィックは引き続きハブルータに流れますが、ハブルータはサイト2に直接送信する代わりに、トラフィックをファイアウォールデバイスにリダイレクトします。ファイアウォールが処理を完了すると、クリアされたすべてのトラフィックがハブに返され、このトラフィックはハブからサイト 2 のデバイスに渡されます。



サービスルート SAFI

ハブおよびローカルブランチデバイスは、サービスルートを使用して、ネットワークで使用可能なサービスをドメイン内の Cisco SD-WAN コントローラ にアドバタイズします。このサービスルートは、OMP NLRI のサービスルート後続アドレスファミリ識別子（SAFI）ビットを使用して OMP 経由で送信されます。Cisco SD-WAN コントローラ は RIB でサービスルートを維持し、これらのルートをデバイスには伝播しません。

各サービスルート SAFI には、次の属性があります。

- VPN ID（vpn-id）：サービスが属する VPN を識別します。
- サービス ID（svc-id）：サービスノードによってアドバタイズされているサービスを識別します。Cisco Catalyst SD-WAN ソフトウェアには、次の定義済みサービスがあります。
  - ファイアウォール用の FW（svc-id 1 にマッピング）
  - 侵入検知システム用の IDS（svc-id 2 にマッピング）
  - ID プロバイダー用の IDP（svc-id 3 にマッピング）
  - カスタムサービス用に予約されている netsvc1、netsvc2、netsvc3、netsvc4（それぞれ svc-id 4、5、6、7 にマッピング）
- ラベル：サービスを通過する必要があるトラフィックの場合、Cisco SD-WAN コントローラ はトラフィックをそのサービスに転送するために、OMP ルートのラベルをサービスラベルに置き換えます。
- 発信元 ID（originator-id）：サービスをアドバタイズしているサービスノードの IP アドレス。

- TLOC：サービスを「ホスティング」しているデバイスのトランスポートロケーションアドレス。
- パス ID（path-id）：OMP パスの識別子。

サービスチェーンポリシー

サービスを介してトラフィックをルーティングするには、Cisco SD-WAN コントローラ で制御ポリシーまたはデータポリシーをプロビジョニングします。一致基準が宛先プレフィックスまたはその属性のいずれかに基づいている場合は、制御ポリシーを使用します。一致基準にパケットまたはトラフィックフローの送信元アドレス、送信元ポート、DSCP 値、または宛先ポートが含まれている場合は、データポリシーを使用します。ポリシーは、CLI を使用して直接プロビジョニングすることも、Cisco SD-WAN Manager からプッシュすることもできます。

Cisco SD-WAN コントローラ は、OMP ルート、TLOC ルート、サービスルートをルートテーブルに保持します。指定された OMP ルートは、TLOC とそれに関連付けられたラベルを伝送します。Cisco SD-WAN コントローラ では、TLOC とそれに関連付けられたラベルをサービスのラベルに変更するポリシーを適用できます。

サービスチェーンの正常性の追跡

Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、Cisco Catalyst SD-WAN はネットワークサービスを提供するデバイスを定期的にプローブして、それらが動作しているかどうかをテストします。サービスチェーン内のデバイスの可用性を追跡することは、ポリシーが使用できないサービスデバイスにトラフィックをルーティングする場合に発生し得る null ルートの回避に役立ちます。デフォルトでは、Cisco Catalyst SD-WAN はトラッキング結果をサービスログに書き込みますが、これは無効にすることができます。

制限事項

- トンネルインターフェイスを介したサービス挿入は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。
- ローカルでホストされているサービスチェーンでの制御ポリシーベースのサービスチェーンアクションはサポートされていません。
- 同じデバイス上でのサービスチェーンと AppQoE の設定は、データポリシーまたは制御ポリシーベースのアクションに関係なくサポートされていません。

- サービス チェーニングの設定 （4 ページ）
- サービスチェーン設定例 （7 ページ）
- サービスチェーンのモニター （15 ページ）

サービス チェーニングの設定

Cisco Catalyst SD-WAN によって管理されるデバイスのサービスチェーンを設定するワークフローを次に示します。

1. サービスデバイスは、特定の VRF を介してアクセスされます。サービスデバイスの VRF に対応する VPN テンプレートで、サービスチェーンを設定し、サービスタイプとデバイスアドレスを指定します。デフォルトでは、トラッキング機能によって各サービスデバイスステータスの更新がサービスログに追加されます。VPNテンプレートでこれを無効にできます。
2. Cisco Catalyst SD-WAN によって管理されるデバイスのデバイステンプレートに VPN テンプレートをアタッチします。
3. デバイステンプレートをデバイスに適用します。

Cisco SD-WAN Manager を使用したサービスチェーンの設定

デバイスのサービスチェーンを設定します。

1. Cisco SD-WAN Manager で VPN テンプレートを作成します。
2. [サービス（Services）] をクリックします。
3. [サービス（Service）] セクションで [新規サービス（New Service）] をクリックし、以下を設定します。
   - **サービスタイプ（Service Type）**：サービスデバイスが提供するサービスのタイプを選択します。
   - **IPアドレス（IP Address）**：IP アドレスは唯一の有効なオプションです。
   - **IPv4アドレス（IPv4 Address）**：デバイスのアドレスを 1 ～ 4 つ入力します。
   - **トラッキング（Tracking）**：サービスデバイスの定期的な正常性アップデートをシステムログに記録するかどうかを決定します。デフォルトは On です。

（注） サービスの最大数は 8 です。

4. [Add]をクリックします。設定されたサービスの表にサービスが表示されます。

Cisco IOS XE Catalyst SD-WAN デバイス における CLI での同等コマンド

次の表に、CLI によるサービスチェーンの設定が Cisco SD-WAN Manager の設定とどのように対応するかを示します。CLI 設定は、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco vEdge デバイス で異なります。次の CLI の例は、Cisco IOS XE Catalyst SD-WAN デバイス の場合です。

CLI（Cisco IOS XE Catalyst SD-WAN デバイス）	Cisco SD-WAN Manager
`service firewall vrf 10`	Cisco SD-WAN Manager で、特定の VRF（この例では VRF 10）の VPN テンプレートにサービス挿入を設定します。 ドロップダウンリストから、サービスタイプを選択します（この例では firewall）。
`no track-enable` （注）　デフォルト：enabled	VPN テンプレートの [サービス（サービス）] にサービスを追加する場合は、[トラッキング（Tracking）] で [オン（On）] または [オフ（Off）] を選択します。
`ipv4 address 10.0.2.1 10.0.2.2`	VRF テンプレートの [サービス（Service）] で、特定のサービスを提供するサービスデバイスの IP アドレスを 1 つ以上入力します。

CLI の例

```
sdwan
  service firewall vrf 10
  ipv4 address 10.0.2.1 10.0.2.2
commit
```

Cisco vEdge デバイス における CLI での同等コマンド

次の表に、CLI によるサービスチェーンの設定が Cisco SD-WAN Manager の設定とどのように対応するかを示します。CLI 設定は、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco vEdge デバイス で異なります。次の CLI の例は、Cisco vEdge デバイス の場合です。

CLI（Cisco vEdge デバイス）	Cisco SD-WAN Manager
`vpn 10`	Cisco SD-WAN Manager で、VPN テンプレートにサービス挿入を設定します（この例では VPN 10）。 ドロップダウンリストから、サービスタイプを選択します（この例では firewall）。
`service FW address 10.0.2.1`	ドロップダウンリストから、サービスタイプを選択します（この例では firewall）。サービスデバイスのアドレスを 1 つ以上指定します。
`no track-enable` （注）　デフォルト：enabled	VPN テンプレートの [サービス（サービス）] にサービスを追加する場合は、[トラッキング（Tracking）] で [オン（On）] または [オフ（Off）] を選択します。

CLI の例

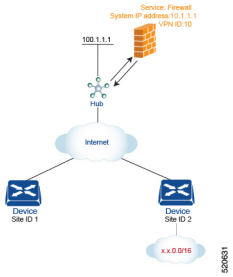
```
vpn 10
  service FW address 10.0.2.1
commit
```

サービスチェーン設定例

サービスチェーン制御ポリシーは、トラフィックが宛先に配信される前に、ネットワーク内のさまざまな場所に配置できるサービス側デバイスにデータトラフィックを転送するものです。サービスチェーンを機能させるには、Cisco SD-WAN コントローラ で一元管理型制御ポリシーを設定し、そのデバイスと同じサイトに配置されたデバイス上でサービスデバイス自体を設定します。サービスが Cisco SD-WAN コントローラ にアドバタイズされるようにするには、サービス側デバイスの IP アドレスをローカルで解決する必要があります。

このトピックでは、サービスチェーン設定の例を示します。

サービスを介したサイト間トラフィックのルーティング



簡単な例として、サービスを介して1つのサイトから別のサイトに移動するデータトラフィックのルーティングについて説明します。この例では、サイト1のデバイスからサイト2のデバイスに移動するすべてのトラフィックを、ハブ（システム IP アドレスは 100.1.1.1）の背後にあるファイアウォールサービスを介してルーティングします。簡単にするために、すべてのデバイスが同じ VPN 内にあることにします。

このシナリオの場合、次のように設定します。

- ハブルータで、ファイアウォールデバイスの IP アドレスを設定します。
- Cisco SD-WAN コントローラ で、ファイアウォールサービスを介してサイト 1 からサイト 2 に向かうトラフィックをリダイレクトする制御ポリシーを設定します。
- Cisco SD-WAN コントローラ で、サイト 1 に制御ポリシーを適用します。

設定手順を以下に示します。

1. ハブルータで、ファイアウォールデバイスの IP アドレスを指定して、ファイアウォールサービスをプロビジョニングします。この設定では、ハブルータの OMP が Cisco SD-WAN コントローラに1つのサービスルートをアドバタイズします。サービスルートには、ハブルータの TLOC や、サービスタイプをファイアウォールとして識別する svc-id-1 のサービスラベルなど、ファイアウォールの場所を識別する多数のプロパティが含まれています。（前述のように、ルートをアドバタイズする前に、デバイスでファイアウォールの IP アドレスがローカルで解決できるようにしておきます）。

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
```

2. Cisco SD-WAN コントローラ で、ファイアウォールを介してサイト 1 からサイト 2 に移動するデータトラフィックをリダイレクトする制御ポリシーを設定します。次に、Cisco SD-WAN コントローラ で、このポリシーをサイト 1 に適用します。

```
policy
  lists
    site-list firewall-sites
      site-id 1
  control-policy firewall-service
    sequence 10
      match route
        site-id 2
      action accept
        set service FW vpn 10
    default-action accept
apply-policy
  site-list firewall-sites control-policy firewall-service out
```

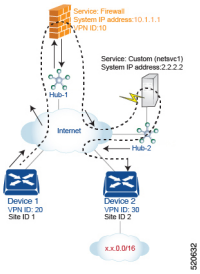
このポリシー設定によって次のことが行われます。

- **apply-policy** コマンドで参照され、このポリシーが適用されるすべてのサイトを列挙する **firewall-sites** というサイトリストを作成する。後でこのポリシーを拡張して、他のサイトからサイト 2 に向かうすべてのトラフィックも最初にこのファイアウォールを通過するようにする場合は、追加のサイト ID を **firewall-sites** サイトリストに追加するだけです。設定の **control-policy firewall-service** 部分を変更する必要はありません。
- **firewall-service** という名前の制御ポリシーを定義する。このポリシーには、1 つのシーケンス要素と次の条件が備わっています。
  - サイト 2 宛てのルートを照合する。
  - マッチした場合は、ルートを受け入れ、VPN 10 にあるハブルータによって提供されるファイアウォールサービスにリダイレクトする。
  - マッチしないすべてのトラフィックを受け入れる。つまり、サイト 2 宛てではないすべてのトラフィックを受け入れる。
- **firewall-list** にリストされているサイト、つまりサイト 1 にポリシーを適用する。Cisco SD-WAN Validator は、アウトバウンド方向、つまりサイト 1 に再配布するルートにポリシーを適用します。これらのルートでは次の変更が起こります。
  - TLOC が、サイト 2 の TLOC からハブ 1 ルータの TLOC に変更される。これは、Cisco SD-WAN コントローラ がハブルータから受信したサービスルートを通じて学習した TLOC です。サイト 2 宛てのトラフィックがハブルータに送信される TLOC の変更が起こったからである。
  - ラベルが svc-id-1（ファイアウォールサービスを識別するもの）に変更される。このラベルにより、ハブルータはトラフィックをファイアウォールデバイスに転送する。

ハブルータはトラフィックを受信すると、ファイアウォールのシステム IP アドレス、10.1.1.1 に転送します。トラフィック処理を完了させたファイアウォールは、トラフィッ

クをハブルータに戻し、このルータがそのトラフィックを最終的な宛先であるサイト 2 に転送します。

ノードごとに1つのサービスを使用するサービスチェーンを介したVPN間トラフィックのルーティング



サービスチェーンを使用すると、トラフィックは宛先に到達する前に2つ以上のサービスを通過できます。ここでは、3 番目の VPN にあるサービスを介して、ある VPN から別の VPN にトラフィックをルーティングする例を紹介します。サービスは、それぞれ異なるハブルータの背後にあります。具体的には、VPN 20 のデバイス 1 からデバイス 2 の VPN 30 のプレフィックス x.x.0.0/16 宛てのすべてのトラフィックが、まずハブ 1 の背後にあるファイアウォールを通過し、次にハブ 2 の背後にあるカスタムサービス netsvc1 を通過してから最終的な宛先に送信されるようにするとします。

このポリシーを機能させる必須条件を以下に示します。

- VPN 10、VPN 20、および VPN 30 は、必ずインターネットなどのエクストラネットで接続する。
- VPN 10 は、必ず VPN 20 および VPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 20 は、 必ず VPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 30 は、必ず VPN 20 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。

このシナリオの場合、次の 4 つの設定を行います。

- ハブ 1 ルータでファイアウォールデバイスの IP アドレスを設定します。
- ハブ 2 ルータでカスタムのサービス側デバイスの IP アドレスを設定します。
- Cisco SD-WAN コントローラ で、ファイアウォールデバイスを介してサイト 1 からサイト 2 に向かうトラフィックをリダイレクトする制御ポリシーを設定します。
- Cisco SD-WAN コントローラ で、トラフィックをカスタムのサービス側デバイスにリダイレクトする 2 番目の制御ポリシーを設定します。

設定手順を以下に示します。

1. ハブ 1 でファイアウォールサービスを設定します。この設定では、ハブ 1 ルータの OMP が Cisco SD-WAN コントローラ にサービスルートをアドバタイズします。サービスルートには、ハブルータの TLOC や、サービスタイプをファイアウォールとして識別する svc-id-1 のサービスラベルなど、ファイアウォールの場所を識別する多数のプロパティが含まれています。

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
```

2. ハブ 2 でカスタムサービス netsvc1 を設定します。この設定では、ハブ 2 ルータの OMP が vSmart コントローラにサービスルートをアドバタイズします。サービスルートには、ハブ 2 の TLOC と、カスタムサービスを識別する svc-id-4 のサービスラベルが含まれています。

```
sdwan
service netsvc1 vrf 10
  ipv4 address 2.2.2.2
```

3. サービスチェーンの 1 番目のサービス（ファイアウォール）用に Cisco SD-WAN コントローラ で制御ポリシーを作成し、デバイス 1 ルータの場所であるサイト 1 に適用します。

```
policy
  lists
    site-list firewall-custom-service-sites
      site-id 1
  control-policy firewall-service
    sequence 10
      match route
        vpn 30
        site-id 2
      action accept
        set service FW
    default-action accept
apply-policy
  site-list firewall-custom-service-sites control-policy firewall-service out
```

このポリシー設定によって次のことが行われます。

- **apply-policy** コマンドで参照され、このポリシーが適用されるすべてのサイトを列挙する **firewall-custom-service-sites** というサイトリストを作成する。
- 1 つのシーケンス要素と次の条件を備えた **firewall-service** という名前の制御ポリシーを定義する。
  - VPN 30 とサイト 2 の両方を宛先とするルートを照合する。
  - マッチした場合は、ルートを受け入れ、ファイアウォールサービスへリダイレクトする。
  - マッチしない場合は、トラフィックを受け入れる。
- **firewall-custom-service-sites** サイトリスト、つまりサイト 1 内のサイトにポリシーを適用する。Cisco vSmart コントローラは、アウトバウンド方向、つまりサイト 1 に再配布するルートにポリシーを適用します。これらのルートでは次の変更が起こります。
  - TLOC が、サイト 2 の TLOC からハブ 1 ルータに変更される。これは、Cisco SD-WAN コントローラ がハブから受信したサービスルートを通じて学習した

TLOC です。サイト 2 宛てのトラフィックがハブ 1 ルータに送信される TLOC の変更が起こったからだ。

- ラベルが svc-id-1（ファイアウォールサービスを識別するもの）に変更される。このラベルにより、ハブ 1 ルータはトラフィックをファイアウォールデバイスに転送する。

ハブ 1 ルータはトラフィックを受信すると、ファイアウォールのシステム IP アドレス、10.1.1.1 に転送します。トラフィックの処理を完了させたファイアウォールは、トラフィックをハブ 1 ルータに返します。ハブ 1 ルータは、次の手順で定義されたポリシーにより、トラフィックをハブ 2 ルータに転送します。

4. サービスチェーン内の 2 番目のサービス（カスタムサービス）用に Cisco SD-WAN コントローラ で制御ポリシーを作成し、ハブ 1 ルータのサイトに適用します。

```
policy
  site-list custom-service
    site-id 3
  control-policy netsvc1-service
    sequence 10
      match route
        vpn 30
        site-id 2
      action accept
        set service netsvc1
    default-action accept
apply-policy
  site-list custom-service control-policy netsvc1-service out
```

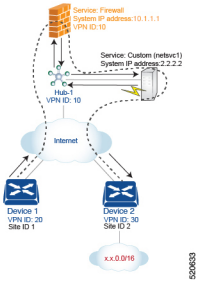
このポリシー設定によって次のことが行われます。

- **apply-policy** コマンドで参照され、このポリシーが適用されるすべてのサイトを列挙する **custom-service** というサイトリストを作成する。
- 1 つのシーケンス要素と次の条件を備えた **netsvc1-service** という名前の制御ポリシーを定義する。
  - VPN 30 とサイト 2 の両方を宛先とするルートを照合する。
  - マッチした場合は、ルートを受け入れ、カスタムサービスへリダイレクトする。
  - マッチしない場合は、トラフィックを受け入れる。
- **custom-service** リスト、つまりサイト 3 内のサイトにポリシーを適用する。Cisco vSmart コントローラは、アウトバウンド方向、つまりサイト 3 に再配布するルートにポリシーを適用します。これらのルートでは次の変更が起こります。
  - TLOC が、サイト 2 の TLOC からハブ 2 ルータの TLOC に変更される。これは、Cisco SD-WAN コントローラ がハブ 2 ルータから受信したサービスルートを通じて学習した TLOC です。サイト 2 宛てのトラフィックがハブ 2 ルータに送信される TLOC の変更が起こったからです。

- ラベルが svc-id-4（ファイアウォールサービスを識別するもの）に変更される。このラベルにより、ハブ 2 は、カスタムサービスをホストしているデバイスにトラフィックを転送します。

ハブ 2 ルータはトラフィックを受信すると、カスタムサービスをホストしているデバイスのシステム IP アドレス、2.2.2.2 に転送します。トラフィックは処理された後、ハブ 2 ルータに戻され、最終的な宛先であるサイト 2 に転送されます。

ノードごとに複数のサービスがあるサービスチェーンを介した VPN 間トラフィックのルーティング



サービスチェーンに同じノードに接続されているサービスが複数ある場合、つまり両方のサービスが同じデバイスの背後にある場合は、制御ポリシーとデータポリシーを組み合わせて目的のサービスチェーンを作成します。この例は、前のセクションの例に似ていますが、単一のハブルータの背後にファイアウォールとカスタムサービス（netsvc-1）がある点が異なります。ここでは、VPN 20 の デバイス 1 から VPN 30 のデバイス 2 のプレフィックス x.x.0.0/16 宛てのすべてのデータトラフィックが、最初にハブ 1 のファイアウォールを通過し、その後同じハブ 1 にあるカスタムサービス netsvc1 を通過してから最終的な宛先に送信されるようにするとします。

このポリシーを機能させる必須条件を以下に示します。

- VPN 10、VPN 20、および VPN 30 は、必ずインターネットなどのエクストラネットで接続する。
- VPN 10 は、必ず VPN 20 および VPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 20 は、 必ず VPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 30 は、必ず VPN 20 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。

このシナリオの場合、次のように設定します。

- ハブルータで、ファイアウォールとカスタムサービスを設定します。
- Cisco SD-WAN コントローラ で、ファイアウォールを介してサイト 1 からサイト 2 に向かうデータトラフィックをリダイレクトする制御ポリシーを設定します。

- Cisco SD-WAN コントローラ で、データトラフィックをカスタムサービスにリダイレクトするデータポリシーを設定します。

設定手順を以下に示します。

1. ハブルータで、ファイアウォールとカスタムサービスを設定します。

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
service netsvc1 vrf 10
  ipv4 address 2.2.2.2
```

この設定では、ハブルータの OMP が 2 つのサービスルートを Cisco SD-WAN コントローラにアドバタイズします。1つはファイアウォール用、もう1つはカスタムサービス netsvc1 用です。どちらのサービスルートにも、ハブ 1 ルータの TLOC と、サービスのタイプを識別するサービスラベルが含まれています。ファイアウォールサービスの場合のサービスラベルは svc-id-1 で、カスタムサービスの場合は svc-id-4 となります。

2. Cisco SD-WAN コントローラ で、VPN 30（サイト 2）宛てのトラフィックをハブ 1（サイト 3）に接続されているファイアウォールサービスに再ルーティングするように制御ポリシーコントローラを設定し、このポリシーを次のようにサイト 1 に適用します。

```
policy
  lists
    site-list device-1
      site-id 1
  control-policy firewall-service
    sequence 10
      match route
        vpn 30
      action accept
        set service FW
apply-policy
  site-list device-1 control-policy firewall-service out
```

3. Cisco SD-WAN コントローラ で、ファイアウォールデバイスから受信したデータトラフィックをカスタムサービス netsvc1 にリダイレクトまたはチェーンするデータポリシーを設定します。次に、このポリシーをハブ 1 に適用します。このデータポリシーは、ネットワーク x.x.0.0/16 の宛先に向かうパケットを IP アドレス 2.2.2.2 というカスタムサービスをホストしているデバイスのシステム IP アドレスにルーティングするためのものです。

```
policy
  lists
    site-list device-2
      site-id 2
    site-list Hub-1
      site-id 3
    prefix-list svc-chain
      ip-prefix x.x.0.0/16
    vpn-list vpn-10
      vpn 10
  data-policy netsvc1-policy
    vpn-list vpn-10
      sequence 1
        match
          ip-destination x.x.0.0/16
        action accept
          set next-hop 2.2.2.2
```

```
    apply-policy
      site-list Hub-1 data-policy netsvc1-policy from-service
```

サービスチェーンを使用したアクティブシナリオまたはバックアップシナリオ

set service アクションを使用して、サービスチェーン用にアクティブまたはバックアップ制御ポリシーを設定する場合に、使用可能なパスの合計数（アクティブパスとスタンバイパスの合計）が設定された **send-path-limit** を超えるようなら、ルートへの直接的な基本設定はしないでください。基本設定を行う場合は、**set tloc-list** アクションと **set service** アクションを併用するようにしてください。そうしないと、アクティブパスのみ、またはバックアップパスのみが特定のスポークルータにアドバタイズされることがあります。

たとえば、Cisco SD-WAN コントローラ OMP テーブルには、8 つのアクティブパスとバックアップパスがあります。ベストパスの計算に基づいて、パスは次の順序でソートされます。

backup1、backup2、backup3、backup4、active1、active2、active3、active4

send-path-limit 4 が設定されている場合、1 番目のポリシーを適用すると、4 つのバックアップパスのみが送信されます。2 番目のポリシーを適用すると、2 つのアクティブパスと 2 つのバックアップパスが送信されます。

send-path-limit がアクティブパスとバックアップパスの合計数よりも小さい場合に障害が発生しやすいポリシーの例を以下に示します。

```
control-policy SET_SERVICE_ACTIVE-BACKUP
  sequence 10
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_PRIMARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     preference 200
     service FW vpn 10
    !
   !
  !
  sequence 20
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_SECONDARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     preference 100
     service FW vpn 10
    !
   !
  !
  default-action accept
!
!
```

ポリシー同じですが、推奨事項に従って修正した例を以下に示します。

```
policy
lists
```

```
  tloc-list HUBS_PRIMARY_INTERNET_TLOCS
   tloc 10.0.0.0 color biz-internet encap ipsec preference 200
   tloc 10.0.0.1 color biz-internet encap ipsec preference 200
  !
  tloc-list HUBS_SECONDARY_INTERNET_TLOCS
   tloc 10.255.255.254 color biz-internet encap ipsec preference 100
   tloc 10.255.255.255 color biz-internet encap ipsec preference 100
  !
!
control-policy SET_SERVICE_ACTIVE-BACKUP_FIXED
  sequence 10
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_PRIMARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     service FW vpn 10 tloc-list HUBS_PRIMARY_INTERNET_TLOCS
    !
   !
  !
  sequence 20
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_SECONDARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     service FW vpn 10 tloc-list HUBS_SECONDARY_INTERNET_TLOCS
    !
   !
  !
  default-action accept
!
!
```

サービスチェーンのモニター

ハブアンドスポークデバイスで、サービスチェーンのさまざまな側面をモニタリングできます。

（注） サービスデバイスをサービスチェーンの一部として動作するように設定することを、サービスの挿入と呼びます。

- ハブデバイスで、設定されたサービスを表示します。
  - Cisco SD-WAN Manager のメニューから、次の手順を実行します。

    [リアルタイムモニタリング（Real Time monitoring）] ページで、設定されたサービスを表示します（[モニター（Monitor）] > [デバイス（Devices）] > [ハブデバイス（hub-device）] > [リアルタイム（Real Time）]）。[デバイスオプション（Device Options）] で、[OMPサービス（OMP Services）] を選択します。

Cisco vManage リリース 20.6.x 以前：[リアルタイムモニタリング（Real Time monitoring）] ページで、設定されたサービスを表示します（[モニター（Monitor）] > [ネットワーク（Network）] > [ハブデバイス（hub-device）] > [リアルタイム（Real Time）]）。[デバイスオプション（Device Options）] で、[OMPサービス（OMP Services）] を選択します。

- スポークデバイスで、サービスチェーンパスの詳細を表示します。
  - **Cisco SD-WAN Manager を使用**：

    [トレースルート（Traceroute）] ページでサービスチェーンパスを表示します（[モニター（Monitor）] > [デバイス（Devices）] > [スポークデバイス（spoke-device）] > [トラブルシューティング（Troubleshooting）]>[接続（Connectivity）]>[トレースルート（Trace Route）]）。目的のパスの宛先 IP、VPN、および送信元インターフェイスを入力します。

    Cisco vManage リリース 20.6.x 以前：[トレースルート（Traceroute）] ページでサービスチェーンパスを表示します（[モニター（Monitor）] > [ネットワーク（Network）] > [スポークデバイス（spoke-device）] > [トラブルシューティング（Troubleshooting）] >[接続（Connectivity）]>[トレースルート（Trace Route）]）。目的のパスの宛先 IP、VPN、および送信元インターフェイスを入力します。

  - **CLI を使用**：

    traceroute コマンドを使用します。詳細については、『Cisco Catalyst SD-WAN Command Reference』を参照してください。

例：2 つのスポークデバイス間のサービスチェーンパスを表示する

次の例は、Cisco SD-WAN Manager または CLI を使用して、2 つのスポーク間にサービスチェーンを追加する前と後に、スポーク間のパスを表示する方法を示しています。

わかりやすくするために、この例では、2 つのスポークデバイス、ハブデバイス、およびファイアウォールサービスを提供するサービスデバイスのシナリオを示し、ファイアウォール サービス チェーンを設定する方法を示します。

シナリオの各デバイスの詳細は次のとおりです。

デバイス	Address
ハブ、インターフェイス ge0/4 経由	10.20.24.15
スポーク 1	10.0.3.1
スポーク 2	10.0.4.1
サービスデバイス（ファイアウォールサービス）	10.20.24.17

3 つのデバイスの設定：

```
Hub
====
vm5# show running-config  vpn 1
vpn 1
 name ospf_and_bgp_configs
 service FW
  address 10.20.24.17
 exit
 router
  ospf
   router-id 10.100.0.1
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
   area 0
    interface ge0/4
    exit
   exit
  !
 !
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
 !
 interface ge0/5
  ip address 10.30.24.15/24
  no shutdown
 !
!


Spoke 1
=======
vpn 1
 name ospf_and_bgp_configs
 interface ge0/1
  ip address 10.0.3.1/24
  no shutdown
 !
!


Spoke2
======
vpn 1
 interface ge0/1
  ip address 10.0.4.1/24
  no shutdown
 !
!
```

1. **サービス挿入なし**：

   この時点ではサービス挿入ポリシーは設定されていないため、スポーク 1 で **traceroute** を実行してスポーク 2（10.0.4.1）へのパスの詳細を表示すると、スポーク 2 への単純なパスが表示されます。

   → スポーク 2（10.0.4.1）

   ```
   vm4# traceroute vpn 1 10.0.4.1
   Traceroute  10.0.4.1 in VPN 1
   traceroute to 10.0.4.1 (10.0.4.1), 30 hops max, 60 byte packets
    1  10.0.4.1 (10.0.4.1)  7.447 ms  8.097 ms  8.127 ms
   ```

同様に、Cisco SD-WAN Manager で [トレースルート（Traceroute）] ページを表示すると、スポーク 1 からスポーク 2 への単純なパスが表示されます。

2. **サービス挿入あり**：

次の Cisco SD-WAN コントローラ のポリシーは、前述のファイアウォール サービス デバイスを使用して、ファイアウォールサービスのサービス挿入を設定します。

```
vm9# show running-config policy
policy
 lists
  site-list firewall-sites
   site-id 400
  !
 !
 control-policy firewall-services
  sequence 10
   match route
    site-id 600
   !
   action accept
    set
     service FW vpn 1
    !
   !
  !
  default-action accept
 !
!
vm9# show running-config apply-policy
apply-policy
 site-list firewall-sites
  control-policy firewall-services out
 !
!
```

サービス挿入を設定した後、スポーク 1（10.0.3.1）で **traceroute** を実行してスポーク 2（10.0.4.1）へのパスの詳細を表示すると、次のパスが表示されます。

→ ハブ（10.20.24.15） → ファイアウォール サービス デバイス（10.20.24.17） → ハブ（10.20.24.15） → スポーク 2（10.0.4.1）

```
Traceroute -m 15 -w 1 -s 10.0.3.1 10.0.4.1 in VPN 1
traceroute to 10.0.4.1 (10.0.4.1), 15 hops max, 60 byte packets
1 10.20.24.15 (10.20.24.15) 2.187 ms 2.175 ms 2.240 ms
2 10.20.24.17 (10.20.24.17) 2.244 ms 2.868 ms 2.873 ms
3 10.20.24.15 (10.20.24.15) 2.959 ms 4.910 ms 4.996 ms
4 10.0.4.1 (10.0.4.1) 5.045 ms 5.213 ms 5.247 ms
```

同様に、Cisco SD-WAN Manager で [トレースルート（Traceroute）] ページを表示すると、ハブおよびファイアウォール サービス デバイスを経由するスポーク 1 からスポーク 2 へのパスの各手順が表示されます。

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。