サービス挿入

表 *1*:機能の履歴

機能名	リリース情報	説明
ワークフローを使用したサービス挿入	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	この機能を使用すると、**ワークフローライブラリ**からサービスチェーンを作成し、ポリシーのサービスチェーンアクションを設定できます。サービスチェーンは、トラフィックのフローに一連のサービスを挿入し、必要に応じてトラフィックに影響を与えるように設計できます。
信頼できるポスチャと信頼できないポスチャ	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	この機能を使用すると、信頼できるトラフィックがサービスチェーン内の信頼できる高可用性ペアに流れるように設定できます。

サービス挿入に関する情報

サービス挿入は、サービスチェーンとも呼ばれ、Cisco Catalyst SD-WAN オーバーレイファブリック内の特定のデータトラフィックのパスに1つ以上のネットワークサービスまたはセキュリティサービスを配置することを指します。これらのサービスは、トラフィックがルーティングされる一連のサービスであるサービスチェーンで定義されます。トラフィックは、データポリシーに設定したサービスチェーンアクションに従ってルーティングされます。

サービスチェーンは任意のデバイスに配置でき、フルメッシュ、ハブスポーク、Cisco Catalyst SD-WAN マルチリージョン ファブリック（MRF）など、任意のトポロジで使用できます。

Cisco Catalyst SD-WAN サービスチェーンは柔軟性があり、完全に自動化されており、VPN ごとに展開できます。サービスチェーンには、次の主な機能が含まれます。

- サービスチェーンは、オーバーレイ、ローカル入力と出力、VPN間とVPN内、トランジット、ブランチ間、ブランチからインターネット、ブランチからクラウド、およびクラウド間のトラフィックに使用できます。
- チェーン内のすべてのサービスを通過するトラフィックの自動転送
- IPv4、IPv6、デュアルスタック、およびトンネル化のサービス接続メソッド
- 単一サービスのインスタンス間で設定可能な高可用性
- 単一サービスのインスタンス間での組み込みのロードバランシングにより、高可用性ペア間で等コスト マルチパス ルーティング（ECMP）をサポート
- 高度なサービストラッキング
- 複数のユーザー VPN（ユーザートラフィック VPN と異なる場合も同じ場合もあり）間でのサービスチェーン共有
- 制御ポリシー、データポリシー、インターフェイスACL、およびサポートされている一致条件を使用したトラフィック ステアリング メソッド
- フォールバックおよび制限動作
- パスの設定と対称ルーティング
- サービストランスポートとの間のセキュリティサービス
- 信頼できる高可用性ペアと信頼できない高可用性ペアおよびトラフィックマーキング（Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降）
- 有用性に関する定期的なオンデマンド状態通知
- Cisco Catalyst SD-WAN Manager オーケストレーション：ワークフローベースのサービスチェーンとトラフィックポリシーの設定

サービス挿入機能

次の表に、Cisco Catalyst SD-WAN Manager リリース 20.13.1 の前後のリリースにおけるサービスチェーン機能の機能に関する情報を示します。

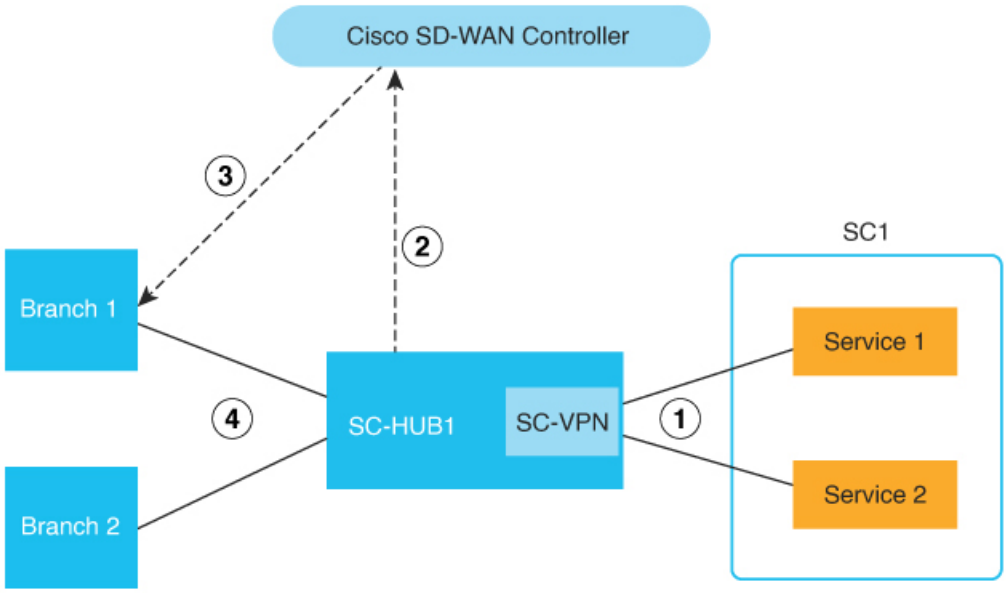
機能	Cisco Catalyst SD-WAN Manager リリース 20.13.1 より前のリリース	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降のリリース
チェーン内の複数のサービス	ネイティブサポートなし	ネイティブサポート
トラフィックステアリング	制御ポリシー	制御ポリシー、データポリシー、インターフェイス ACL
ポリシーバインディング	リモート	リモートおよびローカル
トラフィックのタイプ	IPv4	IPv4、IPv6、デュアルスタック、トンネル
ロードバランシング	サービスエンドポイントとして機能する 4 つの IP アドレス間	すべてのトラフィックタイプのアクティブバックアップペアの 4 つのインスタンス間
高可用性	ロードバランシングによって提供されるとおり	アクティブおよびバックアップペア
トラッキング	サービスインスタンスごとに 1 つの接続	抽象サービスへのすべての接続
設定可能なトラッカープローブ	サポート対象外	すべてのトラッカーは個別に設定可能
バックグラウンドでのトラッキング	サポート対象外	対応
アフィニティ（サービスルートとデータポリシー）	サポート対象外	対応
TLOC 設定	サポート対象	サポート対象
フォールバック、制限	サポート対象外	対応
トンネル接続サービス	サポート対象外	対応
共有サービス VPN	サポート対象外	対応
サービストランスポートとの間	サポート対象外	対応

機能	Cisco Catalyst SD-WAN Manager リリース 20.13.1 より前のリリース	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降のリリース
信頼できるポスチャと信頼できないポスチャ	サポート対象外	Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降でサポート対象
定期的およびオンデマンドの有用性	サポート対象外	対応
Cisco Catalyst SD-WAN Manager オーケストレーション	機能テンプレートを使用	ワークフローライブラリと設定グループを使用（機能テンプレートはサポート対象外）
展開	オンプレミス	オンプレミス、クラウド、ミドルマイルのコロケーション
サービスインスタンスタイプ	物理	物理または仮想

サービス挿入の主要な概念と実装

次の図は、サービスチェーンの基本概念と、サービスチェーンの作成と実行に関連する一般的な手順を示しています。

図 *1*: サービス挿入の概念と手順



1	サービスの起動： • サービスを起動し、Cisco Catalyst SD-WAN ルータに接続します。 • Cisco Catalyst SD-WAN Manager を使用して目的のサービスを起動します。
2	サービスチェーンの設定とアドバタイジング： • ワークフローライブラリまたは CLI コマンドを使用して、SC1 として表示されるルータのサービスチェーンを設定します。 • 設定グループを使用して SC-HUB1 を設定します。ワークフローライブラリ設定により、入力に基づいて自動生成されたサービスチェーン設定が設定グループのサービス VPN 部分に追加されます。 • SC-HUB はサービスチェーンを Cisco SD-WAN コントローラにアドバタイズします。
3	サービスチェーンポリシー： • トラフィックまたはルートを照合し、サービスチェーンアクションを実行します。 • トラフィックの発信元サイトにサービスチェーンポリシーを適用します。 • Cisco SD-WAN コントローラはサービスチェーンを解決し、ターゲットサイトにアドバタイズします。

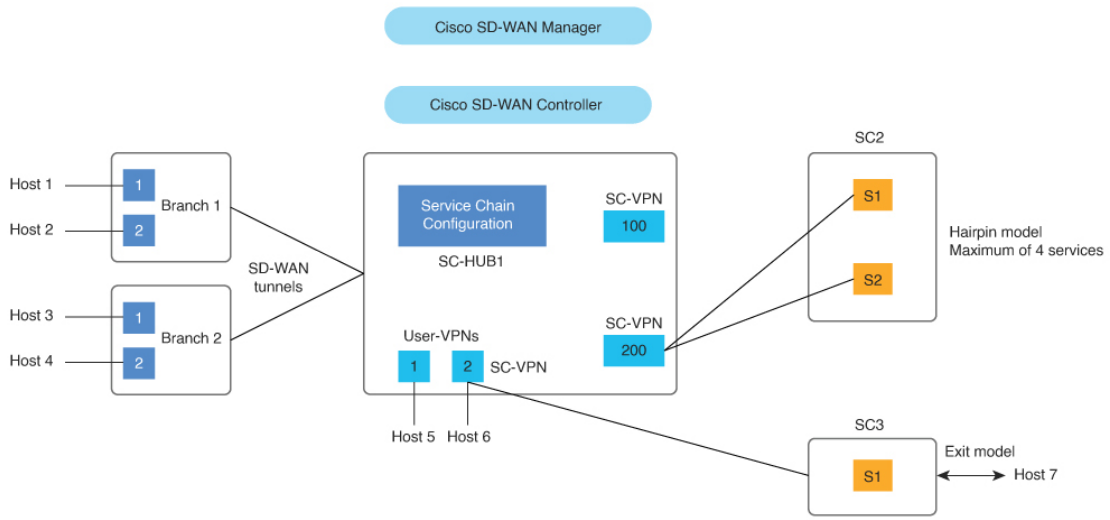
4	トラフィックステアリング： • トラフィックは送信元（B1）からSC-HUBにステアリングされます。 • サービスチェーンの最初のサービスが実行されます。 • 最初のサービスからSC-HUBにトラフィックが戻ります。 • サービスチェーンの 2 番目のサービスが実行されます。 • 2 番目のサービスから SC-HUB にトラフィックが戻ります。 • トラフィックは宛先（B2）に転送されます。

次の図は、サービス挿入の主要な要素を示しています。この図で、SC-HUB1はサービスチェーンが接続されているルータです。

ヘアピンモデルでは、トラフィックは SC-HUB1 によってサービスチェーン内のサービスに送信され、サービスはSC-HUB1にトラフィックを返します。SC-HUB1は、トラフィックをサービスチェーン内の次のサービスに転送し、トラフィックがサービスチェーン内の最後のサービスから戻る場合は宛先に転送します。

Exit モデルでは、トラフィックは SC-HUB1 によってサービスチェーン内のサービスに送信され、サービスはトラフィックを宛先に転送します。トラフィックは宛先からサービスに戻り、SC-HUB1 に戻される場合があります。

図 *2:* サービス挿入の主要な要素



サービス挿入の制約事項

- サービスチェーンには、最大4つのサービスタイプを含めることができます。各サービスタイプは、機能によってロードバランシングされる高可用性ペアとして、またはサードパーティのロードバランサの背後で、サービスの複数のインスタンスを持つことができます。
- サービスチェーン内のサービスは、単一の VPN の中に存在する必要があります。
- サービスチェーンでデュアルスタックサービスを使用している場合は、そのサービスチェーンのすべてのサービスにデュアルスタック高可用性ペアが必要です。
- 特定のデバイスインターフェイスは、特定のサービスチェーン内の複数のサービスには使用しないでください。
- 特定のインターフェイスは、各サービスチェーンで同じサービスタイプに使用される場合にのみ、異なるサービスチェーンで使用できます。
- サービスチェーン内のサービスのインターフェイスとトンネルはすべて、サービスチェーンが定義されている VPN の一部である必要があります。
- 特定のインターフェイスに複数のトラッカーを関連付けることはできません。たとえば、エンドポイントトラッカー tracker1 が GigabitEthernet1 に関連付けられている場合、別のトラッカーを GigabitEthernet1 に関連付けることはできません。

サービス挿入の使用例

- 安全性の低いネットワーク領域からのトラフィックが、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を通過する必要がある場合、サービスチェーンを使用できます。
- それぞれが異なる機能または組織を表す複数の VPN で構成されるネットワークでサービスチェーンを使用すると、VPN 間のトラフィックがファイアウォールを通過するようにすることができます。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。
- サービスチェーンを使用すると、PCI DSS（クレジットカードデータ保護基準）などの適合規格を順守できます。PCI DSS では、PCI トラフィックが集中型データセンターまたは地域ハブのファイアウォールを通過する必要があります。

サービス挿入の設定

Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、**ワークフローライブラリ**を使用してサービス挿入を設定できます。**ワークフローライブラリ**から、新しいサービスチェーンを作

成したり、既存のサービスチェーンを変更したりすることができます。サービスチェーンには、最大 4 つのサービスタイプを含めることができます。

ワークフローでは、次のような複数の手順を設定できます。

- サービスチェーンの名前と説明を設定する
- サービスチェーン内のサービスとチェーン内のサービスの順序を指定する
- サービスチェーンをルータに接続するときに使用される、チェーン内のサービスの接続パラメータを指定する
- サービスタイプごとに、VPN を指定し、ロードバランシング、高可用性、トラッキングなどのオプションを設定する

サービスチェーンを作成または変更するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューで **[Workflows]** > **[Workflow Library]** を選択します。
2. [Define and Configure Service Chain] をクリックします。
3. ワークフローのプロンプトに従います。

   タッカーを定義していることを確認します。トラッカーの設定は、ブラックホールを回避するために非常に重要です。トラッカーを定義すると、サービスチェーンがアップ状態であると判断され、使用されます。サービス チェーン ファイアウォールの IP アドレスが ICMP ベースのトラッカーで使用されている場合は、ファイアウォールが適切なインターフェイスで ICMP を許可していることを確認します。

   サービスチェーンがリターントラフィックを Cisco Catalyst SD-WAN ファブリックにルーティングできることを確認します。これを行うには、サービスチェーンと Cisco Catalyst SD-WAN ルータ（サービスチェーンハブ）の間でダイナミック ルーティング プロトコルを使用するか、スタティックルートを使用します。

   サービスチェーンを適切な Cisco Catalyst SD-WAN SC-Hub ルータに接続します。サービスチェーンをブランチルータに接続する必要はありません。

サービス挿入を設定した後、必要に応じて次のアクションを実行します。

- データポリシーのサービスチェーンアクションを設定して、サービスチェーンを介してトラフィックをルーティングします。「データポリシーでのサービスチェーンアクションの設定」を参照してください。
- 制御ポリシー、データポリシー、またはインターフェイスアクセス制御リストを使用して、トラフィックをサービスチェーンに転送します。「サービスチェーンへのトラフィックステアリング」を参照してください。
- TLOC 設定またはアフィニティ設定を構成して、サービスチェーンへのトラフィックの優先パスを選択します。「パスの設定」を参照してください。
- 送信トラフィックと受信トラフィックに別々のインターフェイスを設定します。「送信トラフィックと受信トラフィックの別々のインターフェイス」を参照してください。

- 信頼できるトラフィックが信頼できる高可用性ペアに流れるように設定します。「信頼できるトラフィックと信頼できないトラフィックのサービスチェーン」を参照してください。
- サービスチェーンを通過するトラフィックのフォールバックまたは制限動作を設定します。「サービスチェーンを介したトラフィックのフォールバックおよび制限動作の設定」を参照してください。

データポリシーでのサービスチェーンアクションの設定

Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、データポリシーのサービスチェーンアクションを設定することで、サービスチェーンを介してトラフィックをルーティングできます。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Custom Options] をクリックしてから、[Centralized Policy] で [Traffic Policy] をクリックします。
3. [Traffic Data] タブをクリックします。
4. [Add Policy] をクリックし、[Create New] をクリックします。
5. [Sequence Type] をクリックし、[Add Data Policy] ダイアログボックスから [Service Chaining] を選択します。
6. [Actions] タブをクリックします。
7. [Service] をクリックします。
8. 次の表で説明するフィールドを設定します。

表 *2:* サービスチェーンアクションのフィールド

フィールド	説明
Service: Type	サービスチェーンのサービスタイプを選択します。
Service: VPN	サービスチェーンがホストされている VPN。 範囲：0 ～ 65530
Service: TLOC IP	サービスチェーン内のサービスを適用するためのトランスポートロケータ（TLOC）の IP アドレスを入力します。
色	TLOC の色を選択します。
カプセル化	TLOC のカプセル化タイプを選択します。

フィールド	説明
Service: TLOC List	ブランチトラフィックにサービスを適用するために使用する定義済みの TLOC リストを選択します。
Local	サービスチェーンがローカルでホストされている場合は、[Local] チェックボックスをオンにします。 このチェックボックスをオンにしない場合、サービスチェーンはリモートでホストされます。
[Restrict]	サービスチェーンがダウンした場合にパケットがドロップされるようにするには、このオプションをオンにします。[Local] オプションを使用してこのポリシーを設定すると、パケットはローカルでドロップされます。[Remote] オプションを使用してこのポリシーを設定すると、パケットはリモートホストでドロップされます。 このオプションは、デフォルトではオフになっています（トラフィックはルーティングにフォールバックします）。

サービスチェーンへのトラフィックステアリング

制御ポリシー、データポリシー、またはインターフェイスアクセス制御リストを使用して、トラフィックをサービスチェーンに転送できます。

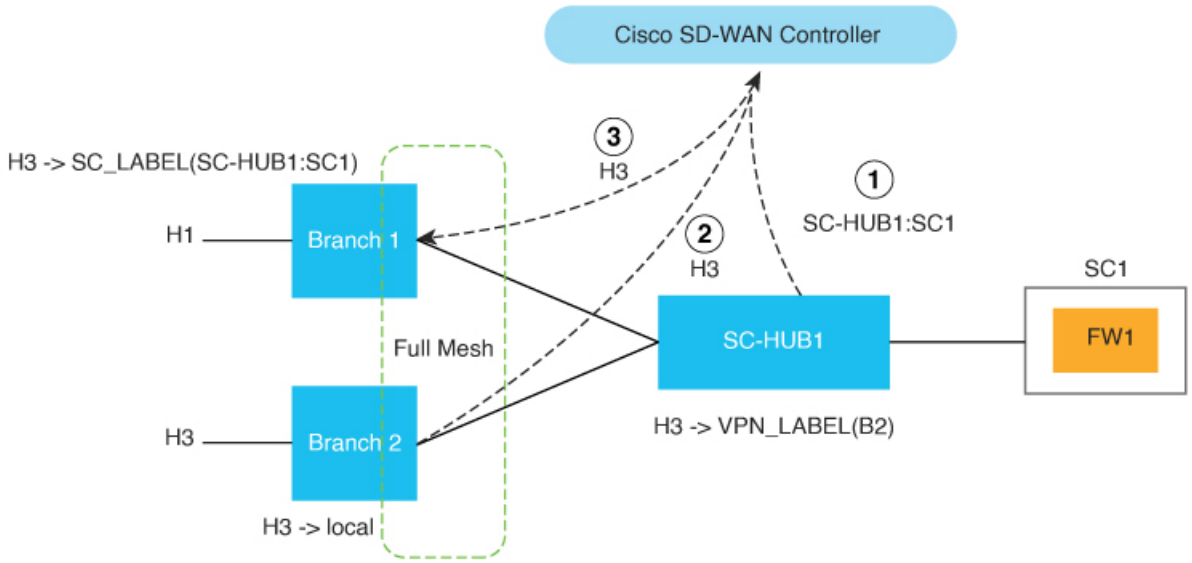
制御ポリシーを使用したトラフィックステアリング

制御ポリシーを使用してシスコのオーバーレイ管理ルート（vRoute とも呼ばれる）を変更して、トラフィックを元の宛先ではなくサービスチェーンに転送できます。

次の図は、制御ポリシーを使用してトラフィックをサービスチェーンに転送する例を示しています。

この例では、ポリシーにより、H1（ホスト 1）と H3（ホスト 3）の間を流れるトラフィックにサービスチェーン 1（SC1）が適用されます。このポリシーは、H1 および H3 トラフィックルートのネクストホップとして SC1 を設定します。ポリシーが有効になる前は、トラフィックは B2（ブランチ 2）から B1（ブランチ 1）に流れます。ポリシーが有効になると、トラフィックは B2 から SC-HUB1:SC1、それから B1 に流れます。

図 *3*: 制御ポリシーを使用したトラフィックステアリング



1	SC-HUB1 は SC1 ルートをアドバタイズします。
2	B2 は H3 ルートを Cisco SD-WAN コントローラにアドバタイズします。
3	制御ポリシーにより、H3 ルートのネクストホップが SC1 にオーバーライドされ、Cisco SD-WAN コントローラは H3 ルートを B1 にアドバタイズします。

設定例：

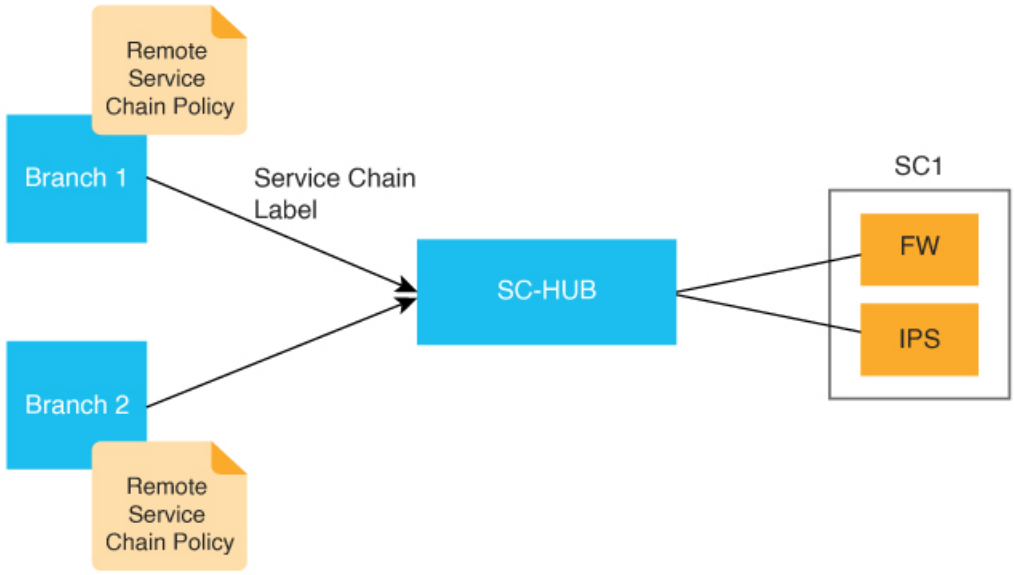
```
Control-policy name
    sequence number
        match route
        action accept
   set service-chain sc_name [tloc|tloc-list name] [vpn vpn]
apply-policy site-list site_list control-policy name out
```

データポリシーを使用したトラフィックステアリング

データポリシーを使用してトラフィックを照合し、転送時に送信元 VPN のコンテキストで動作することができます。

次の図は、データポリシーを使用してリモートブランチでサービスチェーンインテントを指定する例を示しています。

図 *4:* リモートブランチでトラフィック サービス チェーン インテントが指定されたトラフィックステアリング



次に、リモートデバイスでトラフィックインテントが指定されている場合の、データポリシーを使用したトラフィックステアリングの設定例を示します。この例では、次のようになります。

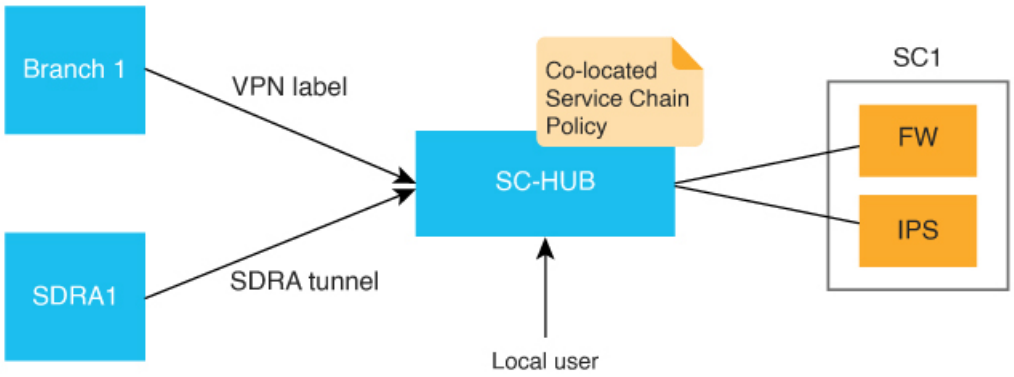
- **match criteria** では、送信元と宛先の IP アドレスの組み合わせに一致するアプリケーションを指定します。
- **restrict|fallback** では、制限またはフォールバックを設定します。
- **tloc|tloc-list** *list* では、TLOC ランキングを使用してトラフィック パスの優先順位を指定します。

（注） **set attribute trust-posture** は、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降で使用できます。

```
policy
 data-policy name
  vpn-list name
   sequence 100
    match criteria
    action accept
     set service-chain sc_name vpn vpn {restrict|fallback} [tloc|tloc-list list]
set attribute trust-posture {trusted | untrusted}
apply-policy site-list remote-sites data-policy name from-service
```

次の図は、データポリシーを使用して、サービスチェーンが接続されているデバイスでサービスチェーンインテントをローカルに指定する例を示しています。

図 *5:* ローカルデバイスでトラフィック サービス チェーン インテントが指定されたトラフィックステアリング



次に、ローカルデバイスでのサービスチェーンインテントの設定例を示します。この例で、**local** は、トラフィックをサービスチェーンにローカルに送信する必要があることを示します。

```
set service-chain SC1 [vpn vpn] local [restrict|fallback]
apply-policy site-list SC-HUB-sites data-policy policy {from-service|from
tunnel}|from-tunnel}
```

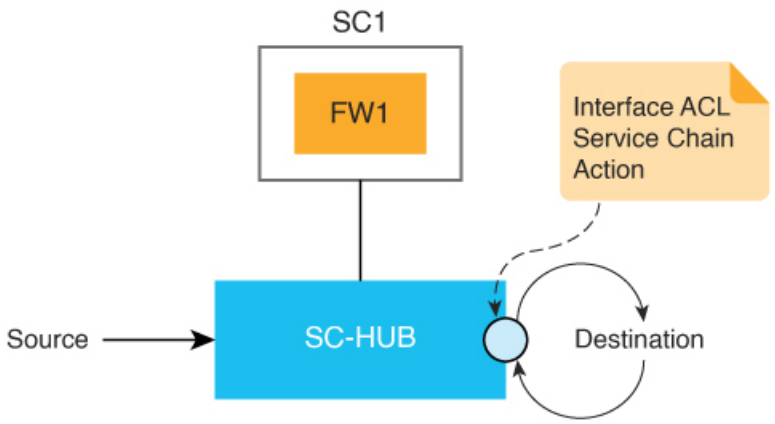
インターフェイスアクセス制御リストを使用したトラフィックステアリング

インターフェイスアクセス制御リスト（ACL）を使用して、指定したインターフェイスで着信または発信するトラフィックをサービスチェーン化できます。状況によっては、以前のルーティングルックアップまたはデータポリシーからトラフィック転送の決定を行う必要がある場合があります。

このアプローチは、インターフェイスからのすべてのトラフィックをサービスチェーン経由で送信する必要がある場合に役立ちます。

次の図は、ACL を使用して、サービスチェーンを介してトラフィックを転送する例を示しています。

図 *6 : ACL* を使用したトラフィックステアリング



次に、ACL を使用したトラフィックステアリングの設定例を示します。

```
access-list list
  sequence number
    match criteria
    action accept
     set service-chain SC1 [vpn vpn] {restrict|fallback}
interface interface
 access-list list {in|out}
```

Path Preference

TLOC 設定またはアフィニティ設定を使用して、サービスチェーンへのトラフィックの優先パスを選択できます。

これを行うには、特定の TLOC 経由でのみトラフィックを転送するか、特定の TLOC を他の TLOC よりも優先するように TLOC リストを設定します。TLOC リストは、データポリシーまたは制御ポリシーのサービスチェーンアクションの一部として **tloc-list** で指定できます。

アフィニティ設定を構成するには、ブランチサイトで **affinity-group preference** を使用してブランチのアフィニティを設定し、サービスチェーンハブで **affinity-group** を使用して VPN のアフィニティを設定します。データポリシー **set service chain** アクションは、デフォルトでアフィニティに準拠しています。

次のコマンドを設定すると、データポリシーでのアフィニティの考慮を無効にすることができます。

data-policy-ignore-affinity-metric

TLOC 設定とアフィニティ設定の両方が設定されている場合、アフィニティ設定が最初に評価され、次に TLOC 設定が評価されます。

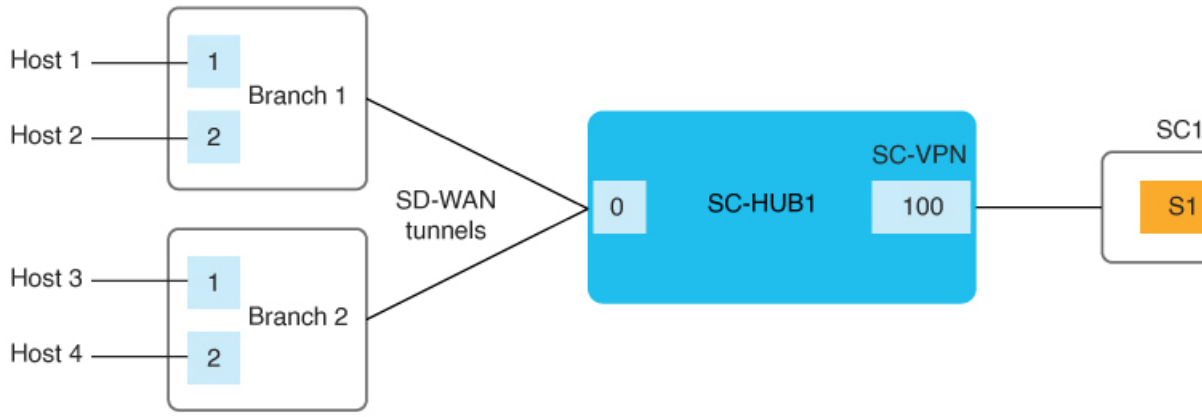
ユーザー VPN 間でのサービスチェーンの共有

サービスチェーン VPN は複数のユーザー VPN 間で共有でき、VPN 間のトラフィックは任意の VPN でサービスチェーン化できます。サービスチェーンの共有には、追加の設定は必要ありません。送信元と宛先の VPN が異なる場合は、送信元と宛先の VPN 間でルートリークが必要です。

次の図は、ユーザー VPN 間でのサービスチェーンの共有を示しています。この図では次のようになっています。

- VPN100 に接続されている SC1（サービスチェーン 1）は、VPN1（H1）および VPN2（H4）のトラフィックで自動的に共有できます。
- VPN1（H1）と VPN2（H4）間のトラフィックは、VPN1 または VPN2 あるいは共有サービスチェーン（VPN100）でサービスチェーン化できます。

図 *7: VPN* 間のサービスチェーン共有

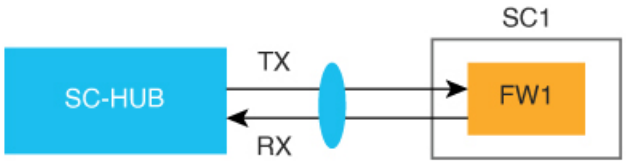


送信トラフィックと受信トラフィックの別々のインターフェイス

service コマンドを使用すると、サービスチェーンを介する送信トラフィックと受信トラフィックに別々のインターフェイスを設定できます。この場合、送信トラフィックと受信トラフィックは個別にトラッキングされます。詳細については、「service」を参照してください。

このアプローチを次の図に示します。

図 *8*: 送信トラフィックと受信トラフィックの別々のインターフェイス



信頼できるトラフィックと信頼できないトラフィックのサービスチェーン

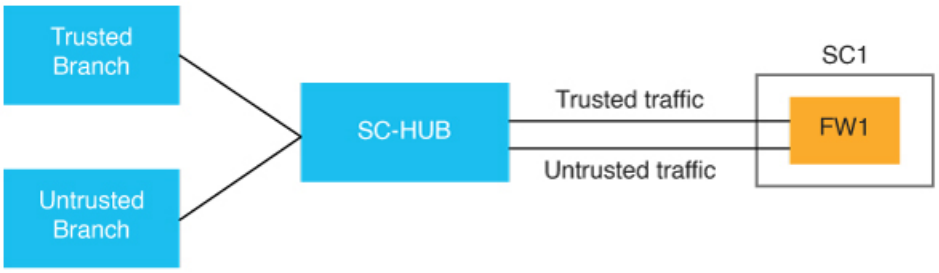
サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

信頼できるトラフィックが信頼できる高可用性ペアに流れるように設定できます。この場合、信頼できないトラフィックは信頼できない高可用性ペアに流れます。

データポリシーで **set attribute trust-posture untrusted action** を使用して、パケットを信頼できる（trusted）または信頼できない（untrusted）としてマークします。パケットのデフォルトの trust-posture は trusted です。

次の図は、信頼できるトラフィックと信頼できないトラフィックのフローを示しています。

図 *9*: 信頼できるトラフィックと信頼できないトラフィック



設定例：

```
service-chain SC1
    service netsvc1
        sequence 10
        service-transport-ha-pair 1
            attribute trust-posture {trusted|untrusted}
```

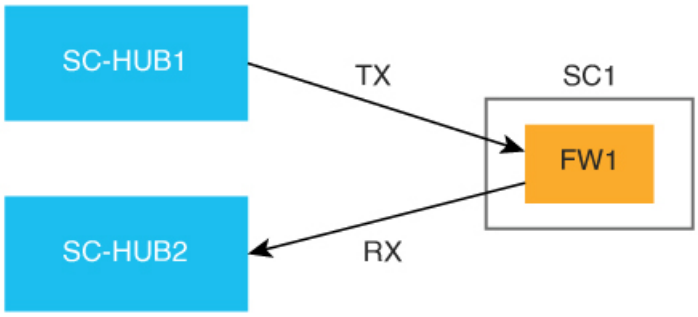
2 つのルータ間のサービスチェーン

サービスチェーンにトラフィックを送信しているルータが、サービスチェーンからトラフィックを受信しているルータと異なる場合は、それぞれのデバイスで同じサービスチェーンを設定

します。サービスチェーンには1つのサービスのみを含めることができ、VPN内トラフィック専用です。

このアプローチを次の図に示します。

図 *10*：*2* つのルータ間のサービスチェーン



サービスチェーンを介したトラフィックのフォールバックおよび制限動作の設定

サービスチェーンを通過するトラフィックのフォールバックまたは制限動作を設定できます。

set service-chain アクションで **fallback** が設定されていると、サービスチェーンがダウンした場合、またはポリシーで指定されたTLOCが使用できない場合、トラフィックはルーティングにフォールバックします。

set service-chain アクションで **restrict** が設定されていると、サービスチェーンがダウンした場合、またはポリシーで指定されたTLOCが使用できない場合、パケットはドロップされます。制限動作は、ファイアウォールなどのセキュリティサービスに適しています。

フォールバックおよび制限は、一元管理型データポリシー（リモートまたはコロケーション）およびインターフェイス ACL で指定できます。

（注） 出力 ACL を使用してトラフィックをサービスチェーンに転送する場合、制限動作が設定されていても、すべてのパケットは宛先に送信されます。これは、サービスチェーンの状態が検出される前に転送の決定が行われるためです。

サービスチェーン内のサービスをルータに接続するためのインターフェイス

サービスチェーン内のサービスは、サービスチェーン VPN または SC-VPN と呼ばれる単一の VPN の中に存在する必要があります。

サービスチェーン内のサービスは、IPv4、IPv6、デュアルスタック、またはトンネルインターフェイスの任意の組み合わせを介して Cisco Catalyst SD-WAN ルータに接続できます。

次の図は、サービスチェーン内のサービスをルータに接続するためのインターフェイスを示しています。

図 *11* : サービスのルータへの接続

1	IPv4 接続
2	IPv6 接続
3	デュアルスタック接続
4	トンネル接続

Software Defined Cloud Interconnect Bring Your Own Service を使用したサービスチェーン

Software Defined Cloud Interconnect（SDCI）は、Megaport や Equinix などのネットワーク サービス プロバイダーを介して、ブランチサイトとクラウド間の接続を確立します。SDCI Bring Your Own Service（BYOS）機能は、ミドルマイルネットワークに展開されている Cisco Catalyst 8000v Edge ソフトウェア（Catalyst 8000v）SDCI ゲートウェイにサービスチェーンを接続することで、サービス検査のための一元化された場所を確立します。BYOS を使用すると、外部サービスと SDCI インフラストラクチャのシームレスな統合が実現します。一元管理型データポリシーとも呼ばれる同じ場所に配置されたデータポリシーは、選択的なデータトラフィック検査のために、ミドルマイルネットワーク内のこれらのゲートウェイに適用されます。

このコンテキストでは、ブランチサイトがファーストマイルを表し、サービスプロバイダーがミドルマイルとして機能して、クラウドがラストマイルとして機能します。

SDCI の BYOS サービス検査では、次の状況でサービスチェーンを使用できます。

- C8000v SDCI ゲートウェイを使用して、ミドルマイルプロバイダーを介してブランチサイトをクラウドワークロードに接続する。

- Catalyst 8000v SDCI ゲートウェイを使用して、ミドルマイルプロバイダーを介してブランチサイトをインターコネクトする。
- Catalyst 8000v SDCI ゲートウェイを使用してミドルマイルプロバイダーによるインタークラウド トラフィック接続を促進する。

CLI テンプレートを使用したサービス挿入の設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

ここでは、サービス挿入の CLI 設定の例を示します。

1. サービスチェーンを作成します。

   service-chain *chain-number*
2. サービスチェーンの説明を設定します。

   service-chain-description *description*
3. サービスチェーン内のサービスを指定し、関連オプションを設定します。

   service *service-type service-parameters*
4. （オプション、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降）サービスチェーン内のサービスの信頼ポスチャを設定します。

   service *service-type* **service-transport-ha-pair** *value* **attribute trust-posture** {**trusted** | **untrusted**}
5. （オプション）すべての Cisco Catalyst SD-WAN Bidirectional Forwarding（BFD）セッションがダウンするように設定します。

   service-chain-affect-bfd
6. サービスチェーン内のすべてのサービスをホストする VPN の名前を指定します。

   service-chain-vrf *vrf*
7. （オプション、デフォルトで有効）サービスチェーン内のサービスのエンドポイントトラッキングを有効にします。

   track-enable
8. （オプション、デフォルトで有効）サービスチェーンを有効にすることにより、デバイスでアクティブにします。

   service-chain-enable

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。