Catalyst SD-WANトラッカーの使いやすさとユースケースの理解

内容

はじめに

このドキュメントでは、Catalyst SD-WANエンタープライズオーバーレイネットワーク、トラッカーの使いやすさ、およびユースケースについて説明します。

背景説明

Catalyst SD-WANエンタープライズオーバーレイネットワークは、通常、外部の多様なワークロード、アプリケーション、およびサービスと相互に作用し、クラウド、データセンター/ハブ、またはリモートブランチに配置されます。SD-WANコントロールプレーンは、スケーラブルな方法でオーバーレイ上でこれらのサービスに向けてルートをアドバタイズする役割を担います。重要なアプリケーションやサービスが特定のパスで到達不能になる状況では、ネットワークオペレータは通常、これらのイベントを検出し、ユーザトラフィックをより適切なパスにリダイレクトして、無期限のトラフィックのブラックホール化を防ぐ必要があります。これらのタイプのネットワーク障害を検出して修正するために、Catalyst SD-WANコントロールプレーンはトラッカーを利用して外部サービスの状態を監視し、必要に応じてルーティングを変更します。

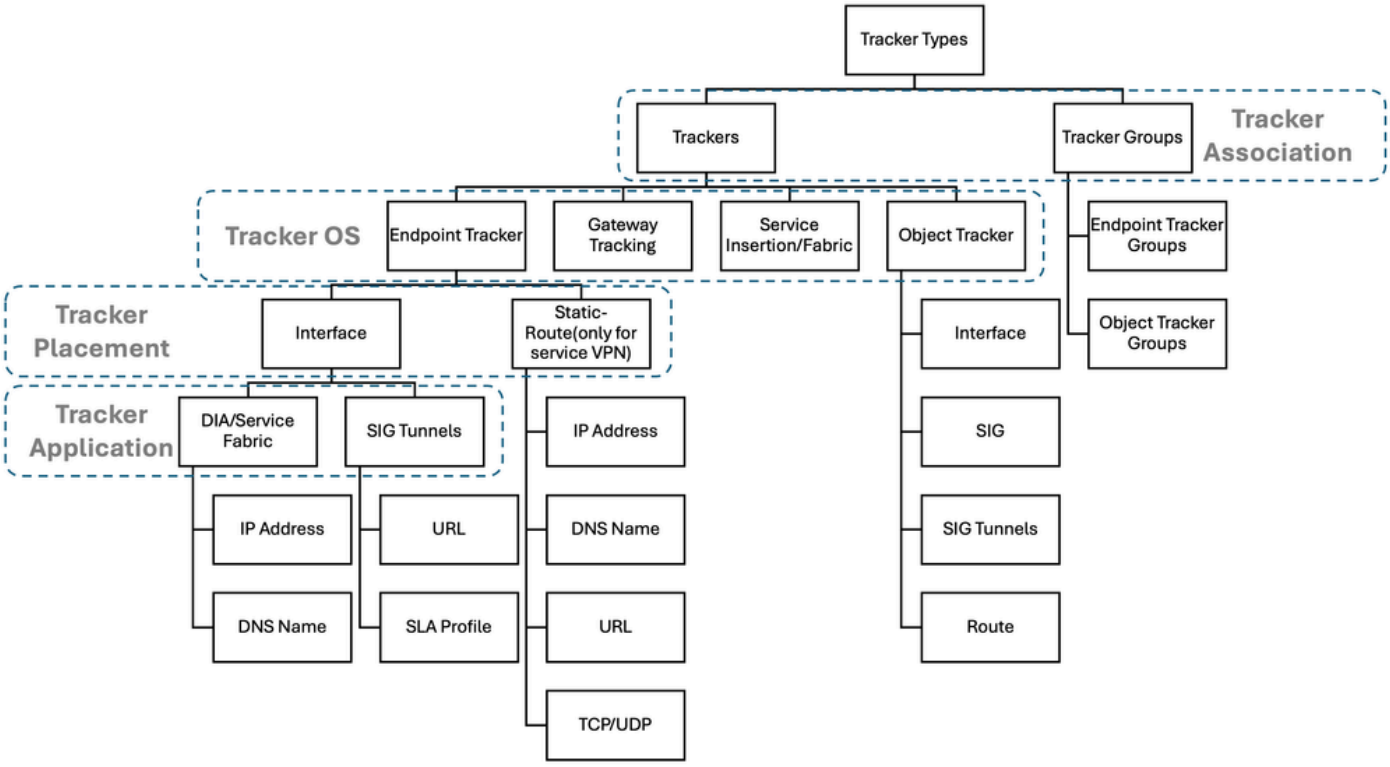
トラッカーは、特定のエンドポイントに向けてプローブパケットを送信し、対象モジュールにエンドポイントの到達可能性ステータスの変更（アップまたはダウン）を通知するコントロールプレーンの到達可能性検出メカニズムです。トラッカーは、ネイティブのCisco IOS-XE® IP SLA機能のスケーラブルでハイレベルな抽象化として設計されており、さまざまなプローブ（HTTP、ICMP、DNSなど）を形成できます。 トラッカーがクライアントモジュールにステータスの変更を通知すると、そのモジュールは、ルートまたはルートのセットのインストールまたはアンインストールなど、トラフィックのブラックホールを防ぐために適切なアクションを実行できます。 SD-WANとSD-Routingソリューションの両方におけるトラッカーの現在のアプリケーションには、DIA(Direct Internet Access)トラッカー、SIG(Secure Internet Gateway)トラッカー、サービストラッカー、スタティックルートトラッカー、トラッカーグループなどが含まれますが、これらに限定されません。

サービス障害に対して復元力のある可用性の高いネットワークを構築するには、トラッカー構成/モデルの各タイプを使用するタイミングを理解することが重要です。この記事の目的は、トラッカーの各タイプが使用される場所と方法を説明することです。ここでは、各種トラッカー、各トラッカーの主な使用例、および各ソリューションを実装するための基本設定ワークフローについて説明します。 最後に、Cisco IOS-XE®のトラッカーに関する一般的な注意事項について説明します。

この記事では、さまざまなユースケースに対処するエンドポイントトラッカー（SD-WANおよびSD-Routing固有）とオブジェクトトラッカー（ネイティブIOS-XE）の違いを示します。

トラッカーのタイプ

この表は、Cisco Catalyst SD-WANソリューションで使用可能なすべてのタイプのトラッカーの概要を示しています。



上の表から、トラッカーを分類できる4つの領域があります。それは、トラッカーの関連付け、トラッカーのOS、トラッカーの配置、およびトラッカーアプリケーションです。次のセクションでは、各分類について説明します。

1. トラッカーの関連付け：この分類は、トラッカーが単一トラッカーかトラッカーグループかを記述します。Cisco Catalyst SD-WANでは、1つのグループ内で複数のトラッカーの使用がサポートされます（現時点で2つまで）。トラッカーグループの全体的なステータスは、ブール演算のANDまたはOR演算子によって決定されます。たとえば、endpoint-trackerグループやobject trackerグループなどがあります。
2. トラッカーOS：この分類は、トラッカーがサポートされているCisco IOS-XE®オペレーティングシステムまたはモードを記述します。Cisco Catalyst IOS XEルータは、次の2つの動作モードをサポートします。

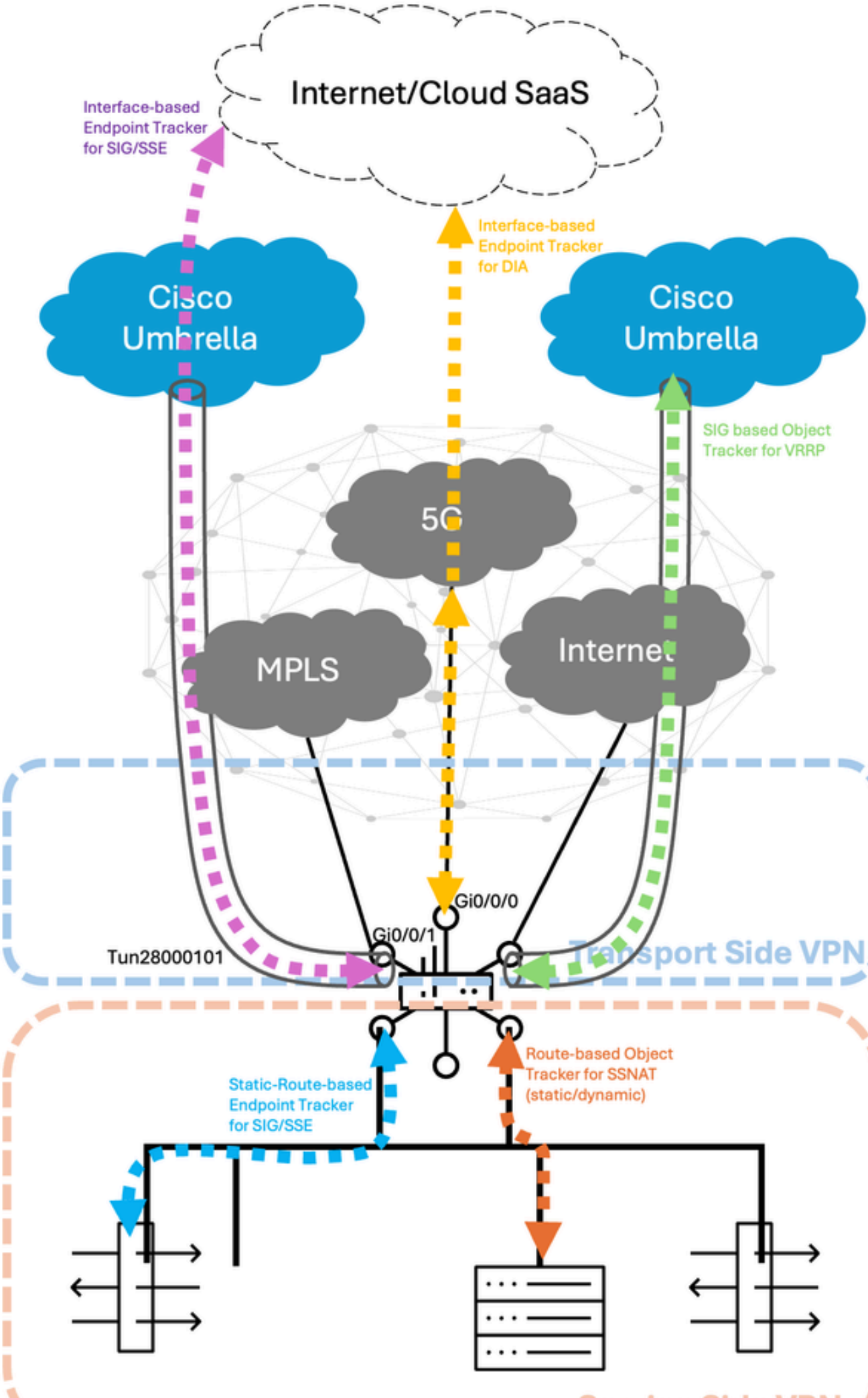
- 自律モードおよび
- コントローラモード。

エンドポイントトラッカーおよびゲートウェイトラッキング機能は、いずれもコントローラモード(SD-WAN)の使用を目的としていますが、オブジェクトトラッカーは自律モード（SDルーティング）の使用を目的としています。

3.トラッカー配置：この分類は、トラッカーが構成される場所を記述します。現在、Cisco Catalyst SD-WANでは、インターフェイス、スタティックルート、またはサービスへのトラッカーの適用がサポートされています。

4.トラッカーアプリケーション：この分類は、Cisco Catalyst SD-WANでサポートされる使用例と機能の概要を説明します。トラッカーには多数のアプリケーション領域がありますが、そのうちのいくつかは、Direct Internet Access(DIA)、Secure Internet Gateway(SIG)、Secure Service Edge(SSE)、サービス側VPNトラッキングなどがあります。

次に、Cisco Catalyst SD-WANエッジ（cEdgeまたはvEdgeとも呼ばれます）での複数の使用例に対する、サービス/トランスポートVPNを通過するトラッカープローブのトラフィックを視覚的に示します。


Internet/Cloud SaaS
Interface-based Endpoint Tracker for SIG/SSE
Interface-based Endpoint Tracker for DIA
Cisco Umbrella
Cisco Umbrella
SIG based Object Tracker for VRRP
5G
MPLS
Internet
Gi0/0/0
Gi0/0/1
Tun28000101
Transport Side VPN
Route-based Object Tracker for SSNAT (static/dynamic)
Static-Route-based Endpoint Tracker for SIG/SSE

Configuration > Templates > Feature Templates > System template > Advanced section > Gateway Tracking（デフォルト：オン）

Service Insertion 1.0とService Fabric 2.0のトラッキング

Service Insertion 1.0 Trackingは20.3/17.3リリースで導入され、サービスアドレス（またはフォワーディングアドレス）が到達可能または使用可能であることを確認するための機能です。この情報は、エッジがコントロール/データポリシーからネクストホップ情報を動的に追加または取り消すのに役立ちます。Service Insertion 1.0の設定では、サービスアドレスに対するトラッカー（トラッキングアドレス）がデフォルトで有効になっています。これに基づいて、フォワーディングアドレスとサービスアドレスは1.0で同じです。サービストラッカーがサービスで自動的に設定されていても、これらのトラッカーを無効にするには、no track-enableコマンドを使用するか、または設定グループ/レガシー設定のトラッカーノブを無効にします。Service Insertion 1.0のサービスに関連するトラッカーでは、これらのみが2つの可能な操作（イネーブル/ディセーブル）であるため、これ以上調整できるパラメータ（しきい値、乗数、間隔など）はありません。 ここで使用されるプローブのタイプは、ICMPエコー要求パケットです。

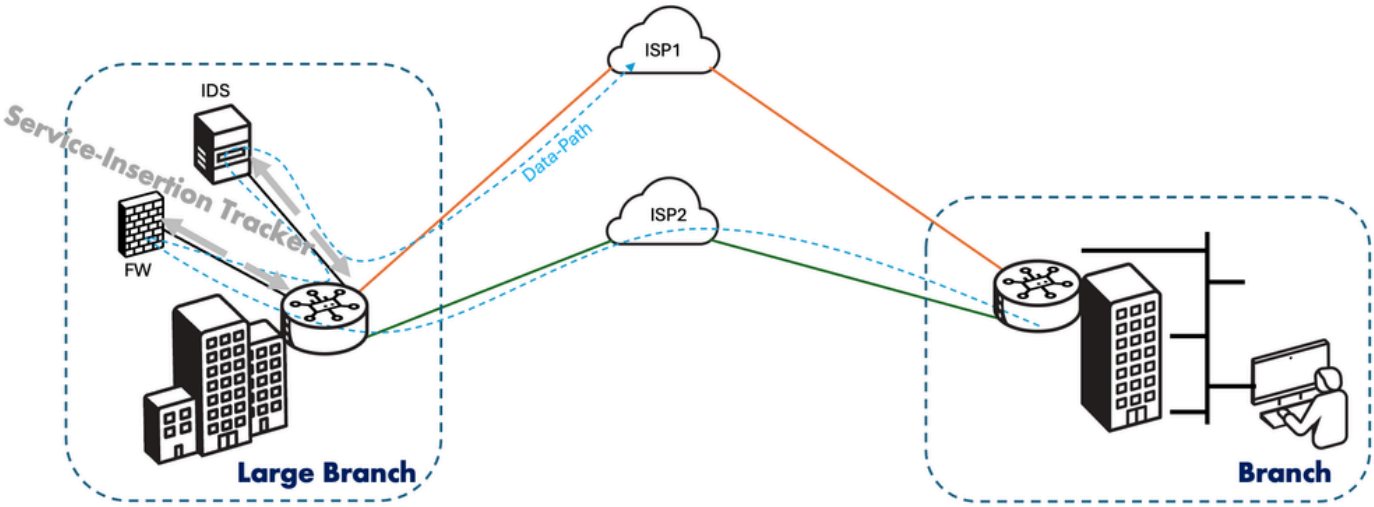
Service insertion 1.0のトラッキングの詳細については、設定ガイドを参照してください。
Service insertion 1.0(SPE)トラッキングで使用されるデフォルトの間隔は次のとおりです。

- プローブ間隔：60秒ごとに5プローブ
- 割増率：5倍
- パケット/プローブタイプ：ICMPエコー/エコー応答

Service Fabric 2.0のトラッキングは、20.13/17.13リリース以降で導入されたCisco Catalyst SD-WANのService Insertion 2.0機能の一部として提供されています。この新しいバリアントのサービス挿入では、設定プロファイルとテンプレートで使用されるデフォルトの方式に、rx/txインターフェイスごとのservice-HAペアの各定義済みサービスアドレス（または転送アドレス）を指す暗黙的なトラッカーが依然として存在します。ただし、Service Fabric 2.0では、フォワーディングアドレスをトラッキングアドレスから分割できるようになりました。これは、サービスアドレス自体とは異なるエンドポイントアドレスを追跡する別のエンドポイントトラッカーを定義するだけで簡単に実行できます。この項は、次の項でさらに詳しく説明します。

使用例

サービストラッカーの主な使用例は、サービスの到達可能性のスケーラブルなモニタリング、特にサービスチェーンのモニタリングです。サービスチェーンは、複数のVPNで構成されるネットワークに導入できます。各VPNは異なる機能または組織を表し、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します。たとえば、大規模なキャンパスネットワークでは、部門間トラフィックはファイアウォールを通過し、部門内トラフィックは直接ルーティングできます。サービスチェーンは、Payment Card Industry Data Security Standard(PCI DSS)など、オペレータが規制コンプライアンスを満たす必要があるシナリオで見られます。PCIトラフィックは、一元化された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。



コンフィギュレーション

設定は、SD-WANにService Insertion 1.0をセットアップする通常のワークフローと同じです。Service Insertion 1.0 Trackerは、すべてのサービスアドレスに対してデフォルトで有効になっています。

- Configuration group: Configuration > Configuration Groups > Service Profile > Service VPN > Serviceセクション：

1. Add Serviceボタンをクリックします。

2. サービスタイプを選択します。

3. サービスアドレスを登録します（最大4個。カンマで区切ります）。

4. トラッキングノブが有効になっていることを確認します（デフォルト）。 これは、必要に応じて無効にすることができます。

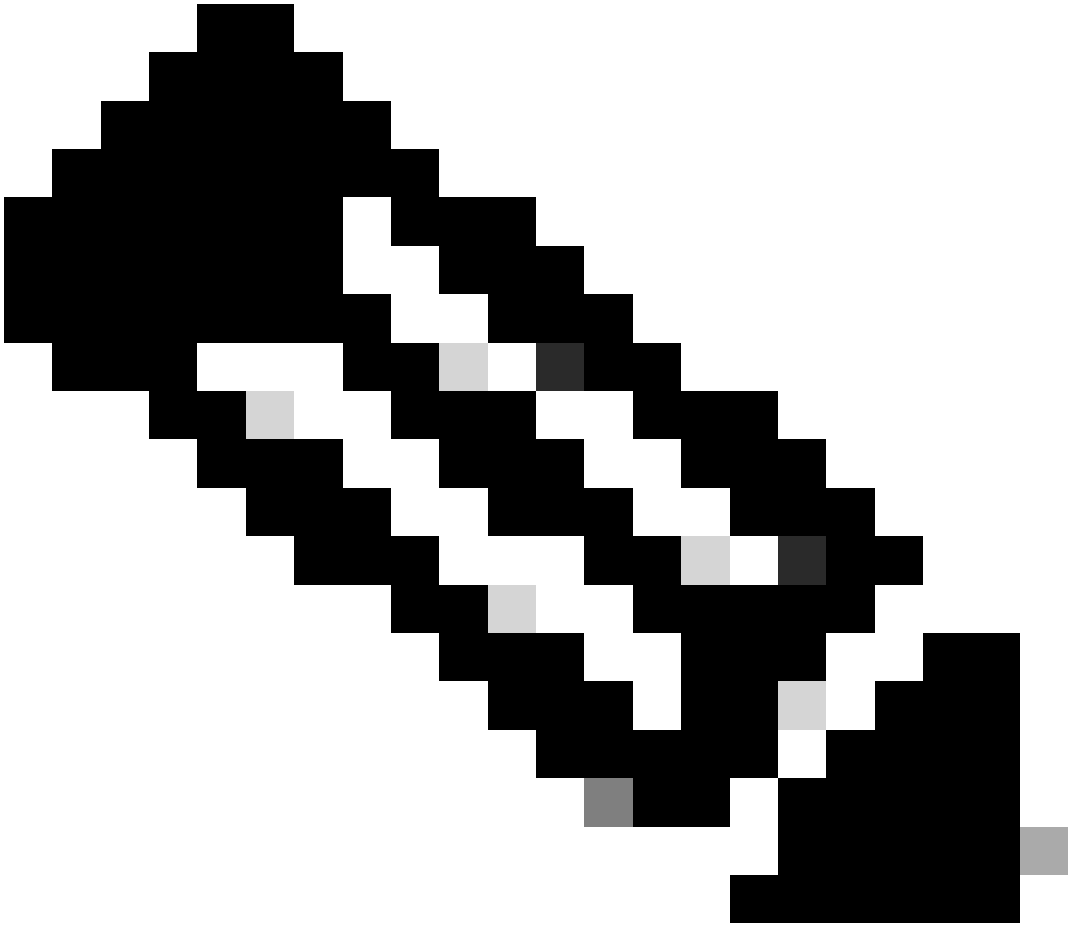
- レガシー設定：Configuration > Templates > Feature Templates > Cisco VPN (service) > Serviceセクション：

1. New Serviceボタンをクリックします

2. サービスタイプを選択します。

3. サービスアドレスを登録します（最大4個。カンマで区切ります）。

4. トラッキングノブが有効になっていることを確認します（デフォルト）。 これは、必要に応じて無効にすることができます。



注：ステップ3が（設定グループまたはレガシー設定から）設定された瞬間に、トラッカーは自動的に様々な定義済みサービスアドレスに対して開始されます

CLIの観点からは、Service Insertion 1.0の設定は次のようになります。

```
!
sdwan
 service firewall vrf 1
  ipv4 address 10.10.1.4
!
```

検証

検証の手順は、前のセクションで使用したインターフェイスベースのエンドポイントトラッカーの一部として実行される同様の手順に拡張されます。

明示的に設定されたエンドポイントトラッカーには、2つの検証オプションがあります。

- SD-WAN Manager:Monitor > Devices > {select Device-Name} > Applications > Tracker:

Individual Trackerで確認し、設定したトラッカー名に基づいて、トラッカーの統計情報（トラッカーのタイプ、ステータス、エンドポイント、エンドポイントのタイプ、VPNインデックス、ホスト名、ラウンドトリップ時間）を表示します。

- SD-WAN Manager:Monitor > Devices > {select Device-Name} > Events:

トラッカーでフラップが検出されると、このセクションの各ログに、ホスト名、アタッチポイント名、トラッカー名、新しい状態、アドレスファミリ、VPN IDなどの詳細が入力されます。

EdgeのCLIで次のコマンドを実行します。

```
Router#show endpoint-tracker
Interface                      Record Name            Status          Address Family   RTT in msecs
1:1:9:10.10.1.4                1:10.10.1.4            Up              IPv4             1

Router#show endpoint-tracker records
Record Name                    Endpoint                              EndPoint Type Threshold(ms) Mult
1:10.10.1.4                    10.10.1.4                             IP            300           3

Router#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------------
*5           icmp-echo   10.10.1.4         RTT=1       OK          51 seconds ago
```

DIAに使用されるインターフェイスエンドポイントトラッカー

NAT DIA Endpoint Trackerトラッカーは、主にSD-WANエッジプラットフォーム上のNAT DIAインターフェイス経由のアプリケーションの到達可能性を監視するために指定されます。

Direct Internet Access（DIA；ダイレクトインターネットアクセス）の使用例では、NAT DIAトラッカーは主にトランスポート側のインターフェイスを追跡し、別の利用可能なトランスポート側のインターフェイスまたはSD-WANオーバーレイトンネル（データポリシーを使用）へのフェールオーバーをトリガーするために使用されます。 この機能は20.3/17.3リリース以降で導入され、NATフォールバック機能オプションは20.4/17.4リリースから使用可能です。トラッカーがNAT DIAインターフェイスを介してローカルインターネットが利用できないと判断した場合、ルータはサービスVPNからNATルートを取り消し、ローカルルーティング設定に基づいてトラフィックを再ルーティングします。トラッカーは、インターフェイスへのパスのステータスを定期的にチェックし続けます。パスが再び機能していることを検出すると、ルータはインターネットへのNATルートを再インストールします。 DIA Trackerの詳細については、設定ガイドを参照してく

ださい。

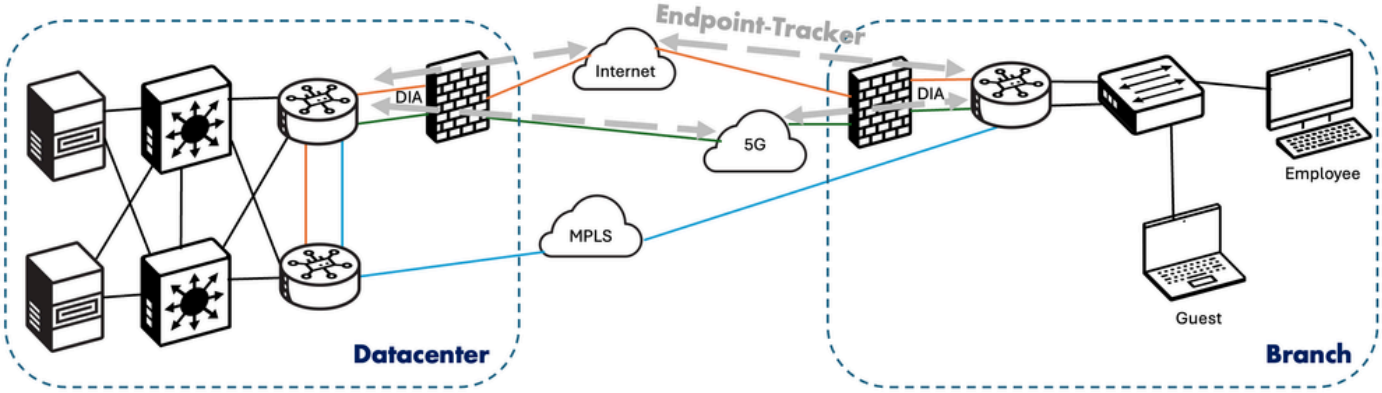
トラッカー定義では、NAT DIAインターフェイス経由で到達可能なエンドポイントのIPアドレスを指定するか（「endpoint-ip」として設定）、エンドポイントに完全修飾ドメイン名(FQDN)を提供するか（「endpoint-dns-name」として設定）を選択できます。

ここで使用されるプローブのタイプはHTTP要求パケットで、HTTP API要求のPDUスタックに非常によく似ています。使用される間隔は次のとおりです。

- プローブ間隔：60秒
- 乗数： 180秒(#retriesは3 = 3 x 60秒であるため)
- パケット/プローブタイプ：HTTP

使用例

DIAは、インターネットに向かうブランチトラフィックをデータセンターにバックホールすることを避けるために、ブランチサイトでの最適化として導入されることがよくあります。しかし、ブランチサイトのDIAを使用する場合は、NAT DIAルートに沿った到達可能性が欠如していても、ブラックホール化とサービス停止を回避するために代替パスにフォールバックする必要があります。ローカルDIAブレークアウト障害時に（NATフォールバックを使用したSD-WANオーバーレイ経由で）DCへのフォールバックを使用するサイト用。これらのインターフェイスベースのエンドポイントトラッカーをブランチ側のエッジにあるDIA対応インターフェイスで活用して、障害を検出し、バックアップ/DCパスへのフェールオーバーを開始します。これにより、DIAを使用してインターネットトラフィックを最適化しながら、企業の中断を最小限に抑えながら、インターネットサービスの高可用性を実現できます。



コンフィギュレーション

この機能セットを有効にするには、これらのインターフェイスベースのエンドポイントトラッカーを手動で設定する必要があります。ユーザが希望する設定方法のタイプに応じて、設定方法を次に示します。

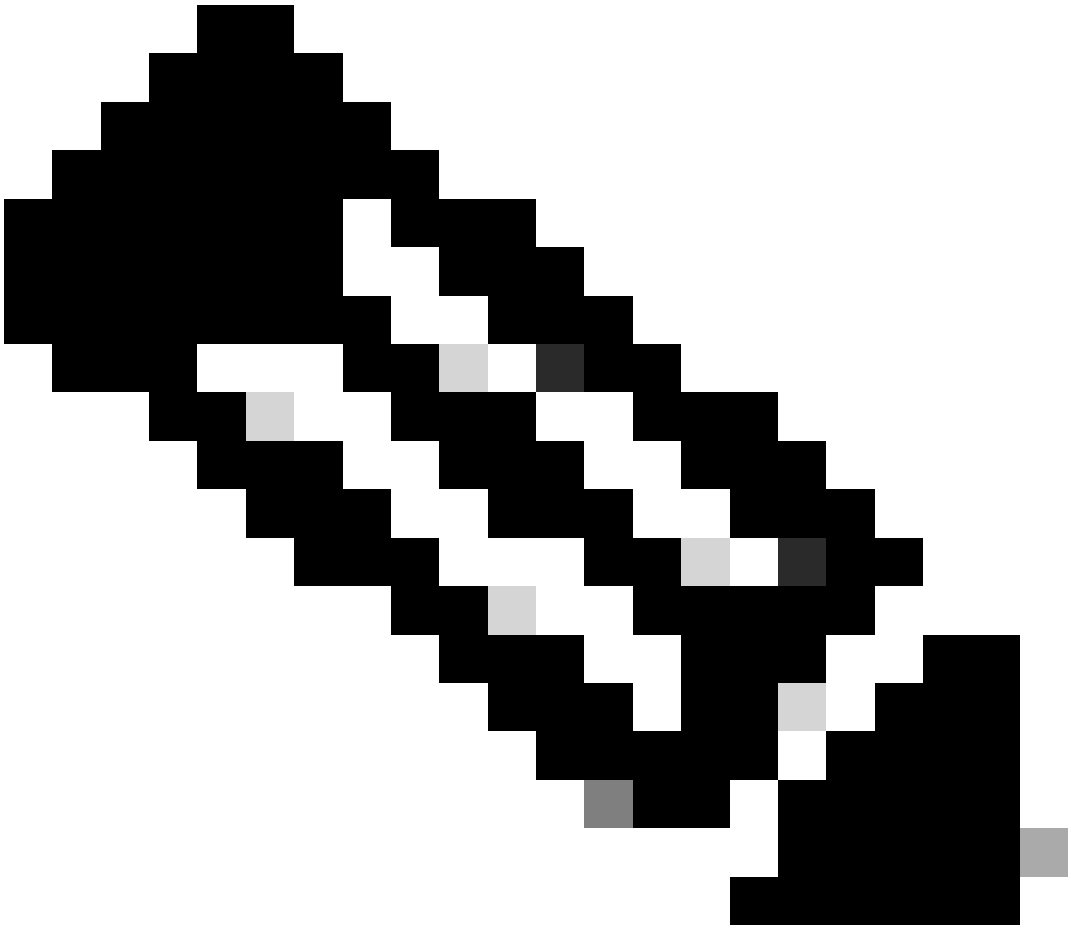
- 設定グループ：Configuration > Configuration Groups > Transport & Management Profile > Ethernet Interface > Add Feature > Tracker:

1. エンドポイントトラッカー名を定義します。

2. エンドポイントトラッカーの種類（HTTP-defaultとICMPの間）を選択します。

注：ICMPエンドポイントトラッカーのタイプは、20.13/17.13リリース以降で導入されています。

3. エンドポイントを選択します（エンドポイントIPデフォルトとエンドポイントDNS名の間）。



> 注：Endpoint DNS Nameを選択した場合は、Transport VPN/VRFでTransport VPN設定プロファイルを使用して、有効なDNSサーバまたはネームサーバが定義されていることを確認してください。

---

4. トラッカープローブの送信先のアドレスまたはDNS名(FQDN)を入力します（形式は前の手順によって異なります）。

5.（オプション）プローブ間隔（デフォルト= 60秒）と再試行回数（デフォルト= 3回）を変更して、障害検出時間を短縮できます。

- レガシー設定:

ステップ 1：インターフェイスベースのエンドポイントトラッカーの定義：設定>テンプレート>機能テンプレート>システムテンプレート>トラッカーセクション：

1. TrackerサブセクションでNew Endpoint Trackerボタンを選択します。

2.エンドポイントトラッカー名を定義します。

3. ここではDIAの使用例が問題となるため、インターフェイスとして（interface-defaultとstatic-routeの間の）Tracker Typeを選択します。

4. エンドポイントのタイプ（IP Address-defaultとDNS名の間）を選択します。

5. トラッカープローブの送信先のエンドポイントIPアドレスまたはエンドポイントDNS名を入力します（形式は前の手順によって異なります）。

6.（オプション）プローブのしきい値（デフォルト= 300ミリ秒）、間隔（デフォルト= 60秒）、およびマルチプレクサ（デフォルト= 3回）を変更できます。

ステップ 2：Interface-Based Endpoint TrackerをトランスポートVPNのインターフェイスに適用します(Templates > Feature Templates > Cisco VPN Interface Ethernet > Advancedセクション)。

1.前のステップ1で定義したEndpoint Trackerの名前をTrackerフィールドに入力します。

CLIの観点からは、設定は次のようになります。

```
(i) IP Address Endpoint :

!
endpoint-tracker t22
  tracker-type interface
  endpoint-ip 8.8.8.8
!
interface GigabitEthernet1




  endpoint-tracker t22
end
!

(ii) DNS Name Endpoint :

!
endpoint-tracker t44
tracker-type interface
endpoint-dns-name www.cisco.com
!
interface GigabitEthernet1
```

```
  endpoint-tracker t44
end
!
```

検証

明示的に設定されたエンドポイントトラッカーには、2つの検証オプションがあります。

- SD-WAN Managerで、Monitor > Devices > {select Device-Name} > Applications > Tracker:

Individual Trackerで確認し、設定したトラッカー名に基づいたトラッカーの統計情報(トラッカーのタイプ、ステータス、エンドポイント、エンドポイントのタイプ、VPNインデックス、ホスト名、ラウンドトリップ時間)を表示します。

- SD-WAN Manager:Monitor > Devices > {select Device-Name} > Events:

トラッカーでフラップが検出されると、このセクションの各ログに、ホスト名、アタッチポイント名、トラッカー名、新しい状態、アドレスファミリ、VPN IDなどの詳細が入力されます。

EdgeのCLIで次のコマンドを実行します。

```
Router#show endpoint-tracker interface GigabitEthernet1
Interface                      Record Name            Status          Address Family   RTT in msecs
GigabitEthernet1             t22                    Up              IPv4             2               2

Router#sh ip sla sum
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------
*2           http        8.8.8.8           RTT=4       OK          56 seconds ag
                                                                   o

Router#show endpoint-tracker records
Record Name                    Endpoint                          EndPoint Type Threshold(ms) Mult
t22                            8.8.8.8                           IP            300           3
t44                          www.cisco.com                       DNS_NAME      300           3
```

SIGトンネル/SSEに使用されるインターフェイスエンドポイントトラッカー

エンドポイントトラッカーがSIGトンネル/SSEのユースケースに使用されている場合、主に企業がクラウドベースのセキュリティスタックの提供を求めていることを示しています。これは、Secure Internet Gateway(SIG)またはSecure Service Edge(SSE)プロバイダー（Cisco、Cloudflare、Netskope、ZScalarなど）を利用することで、簡単に利用できるようになりつつあります。SIGトンネルとSSEはどちらも、クラウドセキュリティ導入モデルの一部として提供され、ブランチはクラウドを使用して必要なセキュリティソリューションを提供します。SIGトンネルのユースケースは、Cisco Catalyst SD-WANをそのようなSIGプロバイダー（20.4/17.4リリース以降）と統合する最初の製品でしたが、クラウド提供のセキュリティオファリングの進化に伴い、Cisco（Cisco Secure Access経由）やZScalarなどのプロバイダーのユースケースをカバーするために、SSEのユースケース（20.13/17.13リリース以降）が導入されました。

IT部門は、保護と接続を俊敏性を高めるために、信頼性の高い明確なアプローチを必要としています。現在では、Microsoft 365やSalesforceなどのクラウドアプリケーションへの直接アクセスをリモート従業員に提供して、セキュリティを強化することが一般的になっています。請負業者、パートナー、Internet of Things(IoT)デバイスなどがネットワークアクセスを必要としているため、クラウドで提供されるネットワーキングとセキュリティに対する需要は日々拡大しています。 クラウドエッジにおいて、エンドデバイスにより近いネットワーク機能とセキュリティ機能の統合は、Cisco SASEと呼ばれるサービスモデルとして知られています。Cisco SASEは、クラウドで提供されるネットワーキング機能とセキュリティ機能を組み合わせて、いつでもどこからでも、すべてのユーザやデバイスにアプリケーションへの安全なアクセスを提供します。 Secure Service Edge(SSE)は、組織が作業環境のセキュリティを向上させると同時に、エンドユーザとIT部門の複雑さを軽減できるようにするネットワークセキュリティアプローチです。 SIGトンネル/SSEトラッカーの詳細については、設定ガイドを参照してください。

使用例

このようなインターフェイスベースのエンドポイントトラッカーは、よく知られたSaaSアプリケーションURLエンドポイントや特定のURLエンドポイントに関する情報を追跡する必要がある、SIGトンネル/SSEのユースケースで使用されます。現在、SSEアーキテクチャはSSEコア機能とSD-WAN機能に分割されているため、SSEの方がより一般的に使用されるシナリオとなっています。次に、サイト（この場合はDC）から作成されたIPSecトンネル内で、アクティブまたはスタンバイのロールを選択します。 ユーザは、該当するトンネルインターフェイスの下にトラッカーを接続するかどうかを選択できます。

Cisco Secure Access（シスコによる）などのSSEプロバイダーの場合、デフォルトで設定されている暗黙のエンドポイントトラッカーが使用されます。ただし、ユーザは、カスタムエンドポイントトラッカーを作成し、それをIPSecトンネルインターフェイスに接続するかどうかを選択できます。SSEで使用されるdefault/implicit endpoint trackerのパラメータは次のとおりです。

Cisco SSEの場合:

トラッカー名： DefaultTracker

追跡中のエンドポイント：http://service.sig.umbrella.com

エンドポイントの種類： API_URL

しきい値：300ミリ秒

乗算： 3

間隔：60秒

Zscaler SSEの場合:

トラッカー名： DefaultTracker

追跡中のエンドポイント：http://gateway.zscalerthree.net/vpnte

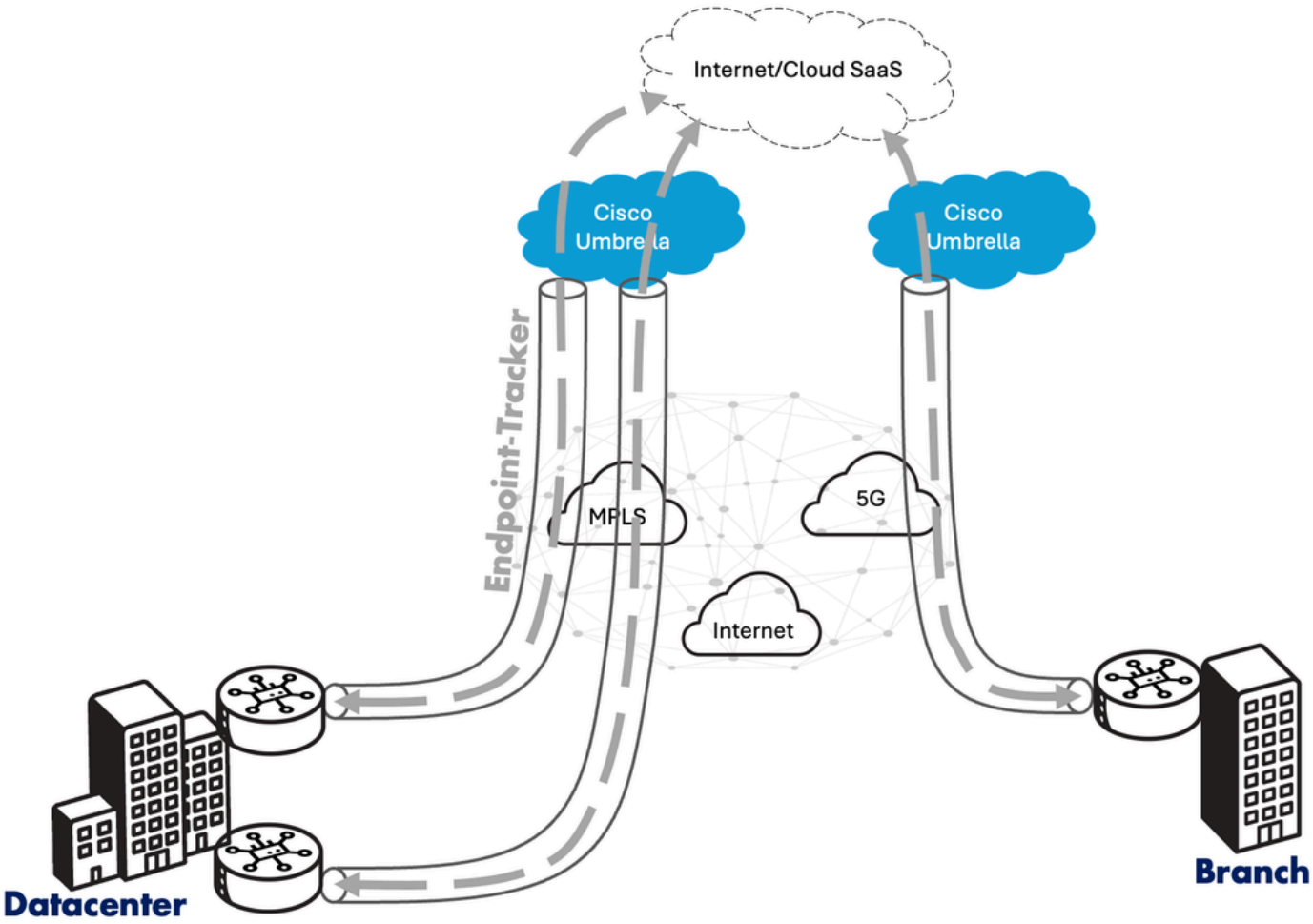
エンドポイントの種類： API_URL

しきい値：300ミリ秒

乗数： 3

間隔：60秒

SIGトンネルの場合、デフォルト/暗黙的なエンドポイントトラッカーは定義されていません。したがって、SIGプロバイダークラウドに向かうIPSecトンネルインターフェイスを追跡する場合、ユーザはインターフェイスベースのエンドポイントトラッカーを手動で設定する必要があります。



コンフィギュレーション

SSEプロバイダーの場合、ユーザはエンドポイントトラッカーを明示的に定義する必要はありません（必要な場合を除く）。 ただし、ワークフローは設定のタイプによって異なります。

前提条件として、SIG/SSEクレデンシャルをAdministration > Settings > External Services > Cloud Credentialsの順に定義する必要があります。

1. Cloud Provider Credentialsで、UmbrellaまたはCisco SSE（あるいはその両方）のオプションを切り替えます。

2. パラメータ(組織ID、APIキー、シークレットなど)を定義します。

Set configuration group Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edgeの順に選択します。

1. Add Secure Internet GatewayまたはAdd Secure Service Edgeをクリックします。

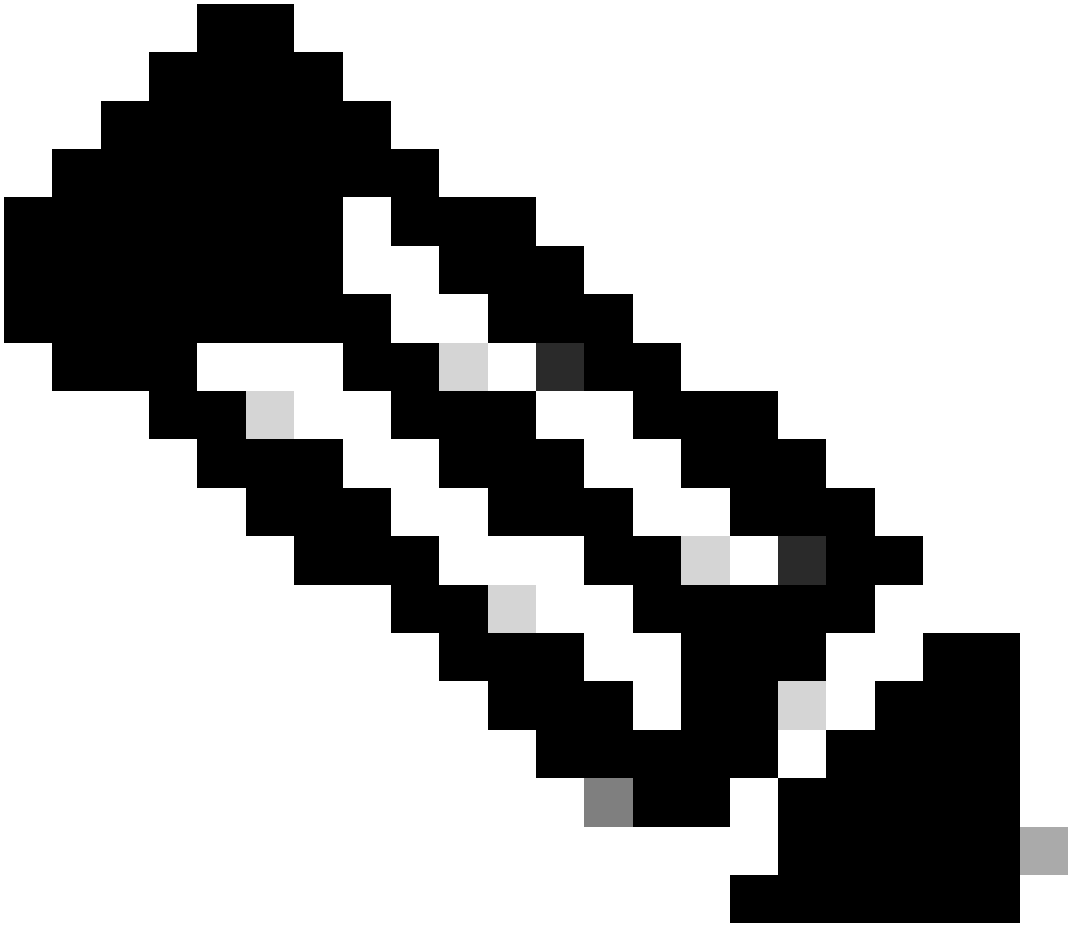
2. 名前と説明を定義します。

3. SIG/SSE Providerの下にあるオプションボタンを1つ選択します(UmbrellaまたはCisco SSE)。

4. Trackerセクションで、トラッカープローブの送信元に使用する送信元IPアドレスを定義します。

5. 明示的/カスタムエンドポイントトラッカーを定義することを選択した場合は、トラッカーの追加をクリックし、エンドポイントトラッカーのパラメータ(名前、エンドポイントのAPI URL、しきい値、プローブ間隔、および乗数)を入力します。

6. Configurationセクションで、パラメータ(Interface Name、Description、Tracker、Tunnel Source Interface、Datacenter Primary/Secondaryなど)を定義できるトンネルインターフェイスを作成します。



注：ステップ6では、ユーザに対して、定義されたエンドポイントトラッカーを各IPSecトンネルに接続するオプションが提供されます。これはオプションのフィールドです。

---

7. High Availabilityセクションで、インターフェイスペアを作成し、アクティブインターフェイスとバックアップインターフェイスを、それぞれの重みとともに定義します。次に、上記の設定済みポリシーグループを関連するエッジに適用します。

レガシー設定を設定します。Configuration > Templates > Feature Templates > Cisco Secure Internet Gateway feature template:

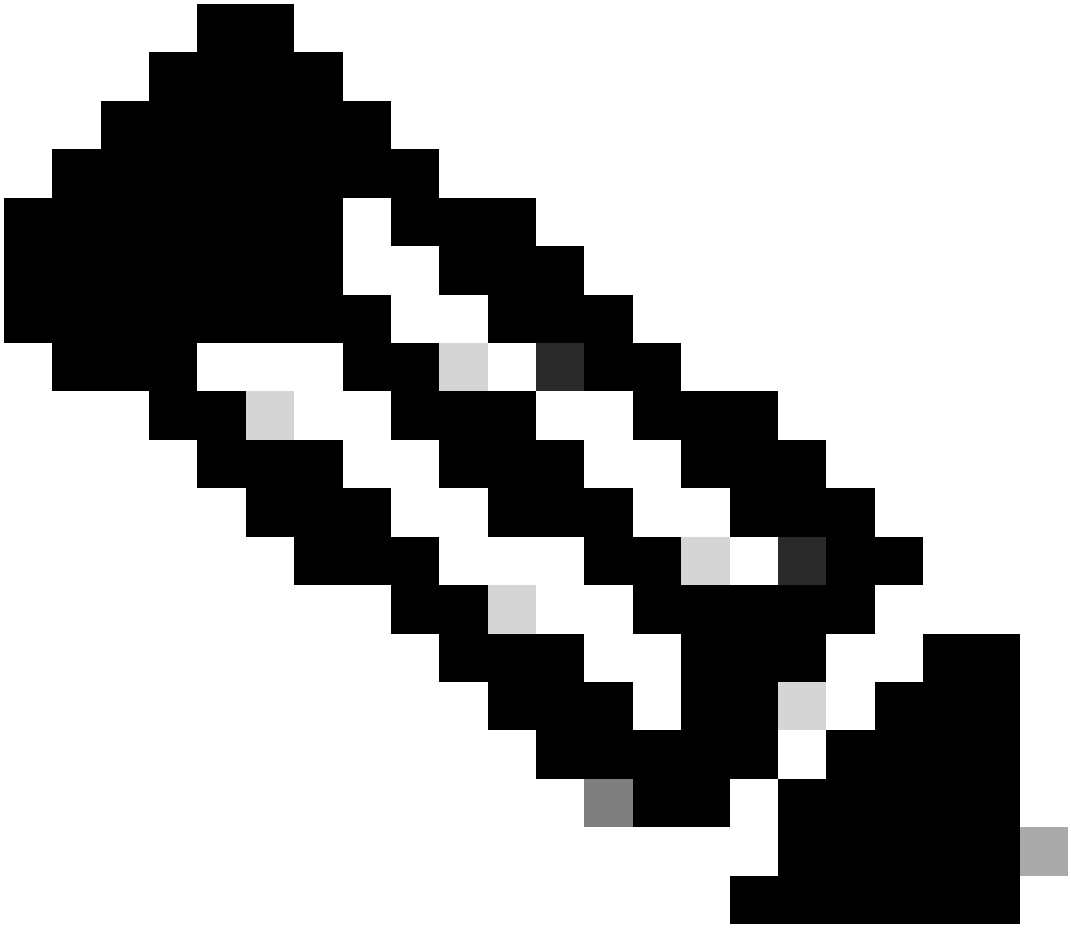
1. SIG Providerの下にあるラジオボタンの1つ（Umbrella、ZScalar、またはGeneric）を選択します。

2. [Tracker (BETA)]セクションで、トラッカープローブの送信元として使用する送信元IPアドレスを定義します。

5. 明示的/カスタムエンドポイントトラッカーを定義することを選択した場合は、[新しいトラッ

カー]をクリックし、エンドポイントトラッカーのパラメータ(名前、エンドポイントのAPI URL、しきい値、間隔、および乗数)を入力します。

6. Configurationセクションで、Add Tunnelをクリックしてトンネルインターフェイスを作成します。トンネルインターフェイスでは、パラメータ(Interface Name、Description、Tracker、Tunnel Source Interface、Datacenter Primary/Secondaryなど)を定義できます。



> 注：ステップ6では、定義されたエンドポイントトラッカーを各IPSecトンネルに接続するオプションがユーザに提供されます。これはオプションのフィールドです。

---

7. High Availabilityセクションで、アクティブインターフェイスとバックアップインターフェイスを、それぞれの重みとともに定義します。

CLIの観点からは、設定は次のようになります。

```
(i) For the default interface-based endpoint tracker applied with SSE
!
```

```
endpoint-tracker DefaultTracker
 tracker-type     interface
 endpoint-api-url http://service.sig.umbrella.com
!
interface Tunnel16000101
 description auto primary-dc
 ip unnumbered GigabitEthernet1
 ip mtu 1400
 endpoint-tracker DefaultTracker




end
!

(ii) For the custom interface-based endpoint tracker (can be applied in SIG & SSE use-cases)
!
endpoint-tracker cisco-tracker
 tracker-type     interface
 endpoint-api-url http://www.cisco.com
!
interface Tunnel16000612
 ip unnumbered GigabitEthernet1
 ip mtu 1400
 endpoint-tracker cisco-tracker




end
!
```

検証

明示的に設定されたエンドポイントトラッカーの検証オプションがあります。

- SD-WAN Managerで、Monitor > Devices > {select Device-Name} > Applications > Trackerの順に選択します。

Individual Trackerで確認し、設定したトラッカー名に基づいて、トラッカーの統計情報 (トラッカーのタイプ、ステータス、エンドポイント、エンドポイントのタイプ、VPNインデックス、ホスト名、ラウンドトリップ時間) を表示します。

- SD-WAN Managerで、Monitor > Devices > {select Device-Name} > Eventsの順に選択します。

トラッカーでフラップが検出されると、このセクションのそれぞれのログに、ホスト名、アタッチポイント名、トラッカー名、新しい状態、アドレスファミリ、およびVPN IDなどの詳細が記録

されます。

EdgeのCLIで次のコマンドを実行します。

```
Router#show endpoint-tracker interface Tunnel16000612
Interface                      Record Name            Status          Address Family   RTT in msecs
t Hop
Tunnel16000612               cisco-tracker          Up              IPv4             26              31

Router#show endpoint-tracker interface Tunnel16000101
Interface                      Record Name            Status          Address Family   RTT in msecs
t Hop
Tunnel16000101               DefaultTracker         Up              IPv4             1               10

Router#show endpoint-tracker records
Record Name                    Endpoint                              EndPoint Type Threshold(ms) Mult
s) Tracker-Type
DefaultTracker                 http://gateway.zscalerthree.net/vpnte API_URL       300           3
   interface
cisco-tracker                  http://www.cisco.com                  API_URL       300           3
   interface
```

Service Fabric 2.0に使用されるインターフェイスエンドポイントトラッカー

20.13/17.13リリースで導入されたService Fabric 2.0トラッキングは、Service Insertion 1.0トラッキングの拡張バリアントです。このリリースでは、ユーザがトラッカーをより大きくカスタマイズできるようになっています。デフォルトの動作は、以前のバージョンのService Insertion(1.0)から維持され、rx/txごとのservice-HAペアの各サービスアドレス（または転送アドレス）の定義を使用して、デフォルトでトラッカーが開始されます。ただし、Service Insertion 2.0では、トラッキングアドレス（トラッキング対象のIP/エンドポイント）をフォワーディングアドレス（通常はサービスアドレス）から分離できます。 これは、VPNレベルで定義されたカスタムエンドポイントトラッカーを使用して行われます。 Service Fabric 2.0トラッカーの詳細については、構成ガイドを参照してください。

デフォルトのトラッカーを使用する場合、トラッカープローブの仕様は次のようになります。

- Hello:30秒ごとに1プローブ
- 割増率：3倍
- パケット/プローブタイプ：ICMPエコー/エコー応答

ユーザーがカスタムトラッカーを使用することを選択した場合、トラッカープローブの仕様は次のようになります。

- Hello:60秒ごとに1プローブ
- 割増率：3倍
- パケット/プローブタイプ：ICMPエコー要求/応答

使用例

前のセクションで説明したService Insertion 1.0の使用例もここでも適用されます。

コンフィギュレーション

サービス挿入2.0のワークフローベースの設定がサポートされています。これはウィザードによるアプローチであり、標準的な設定グループのワークフロー手順に従いながら、ユーザエクスペリエンスを簡素化するのに役立ちます。

1. Configuration > Service Insertion > Service Chain DefinitionsセクションでService Chain - Configurationグループを定義します。

a. Add Service Chain Definitionボタンをクリックします。

b.サービスの名前と説明の詳細を入力します。

c.ドロップダウンから選択して、リスト形式のサービスタイプを入力します。

2. Configuration > Service Insertion > Service Chain ConfigurationsセクションでService Chain Instance - Configurationグループを定義します。

a. Add Service Chain Configurationをクリックします。

b. Service Chain Definitionステップで、Select Existingというタイトルのオプションボタンを選択し、以前に定義したサービスを選択します。

c. サービスチェーンコンフィギュレーションの開始ステップの名前と説明を入力します。

d. Service Chain Configuration for Manually Connected Servicesステップで、Service Chain VPN-IDを選択します。

e.次に、サービスチェーンインスタンス（サブタブで表示）で定義されている各サービスについて、サービス詳細で接続タイプ（IPv4、IPv6、またはトンネル接続）を指定します。

f. Advancedチェックボックスを選択します。アクティブバックアップ/HAのユースケースが必要な場合(バックアップノブのパラメータ追加も有効にする)、またはカスタムエンドポイントトラッカーを定義する必要がある場合（カスタムトラッカノブも有効にする）でも同様です。

g.出力(tx)トラフィックが1つのインターフェイスを介してサービスに向かい、サービスからのリターントラフィックが別のインターフェイスを介して入力(rx)されるシナリオの場合は、サービスからのトラフィックは別のインターフェイスで受信されますノブをオンにします。

h. AdvancedおよびCustom Trackerノブを有効にして、サービスIPv4アドレス（フォワーディングアドレス）、SD-WANルータインターフェイス（サービスの接続先）、およびトラッカーエンドポイント（トラッキングアドレス）を定義します。 間隔や乗数などのカスタムトラッカーパラメータを変更することもできます（[編集]ボタンをクリックします）。

i.その後に定義する各サービスについて、手順(e)、(f)、(g)および(h)を繰り返します。

3. Configuration > Configuration Groups > Service Profile > Service VPN > Add Feature > Service Chain Attachment Gatewayの下で、Service Chain InstanceをEdge - Configurationグループの設定プロファイルに接続します。

a.このService Chain Attachment Gatewayパーセルの名前と説明を入力します。

b.以前に定義したサービスチェーン定義を選択します（ステップ1）。

c.ステップ2で実行した詳細を再度追加/確認します。トラッカーの定義に関しては、前の手順2との唯一の違いは、トラッカー名を指定する機会が得られ、トラッカータイプも選択できることです（service-icmpからipv6-service-icmpまで）。

CLIの観点からは、設定は次のようになります。

```
!
endpoint-tracker tracker-service
 tracker-type service-icmp
 endpoint-ip  10.10.1.4
!
service-chain SC1
 service-chain-description FW-Insertion-Service-1
 service-chain-vrf 1
 service firewall
  sequence 1
  service-transport-ha-pair 1
   active
    tx ipv4 10.10.1.4 GigabitEthernet3 endpoint-tracker tracker-service
!
```

検証

- SD-WAN Managerで、Monitor > Devices > {select Device-Name} > Applications > Trackerの順に選択します。

Individual Trackerで確認し、設定したトラッカー名に基づいて、トラッカーの統計情報（トラッカーのタイプ、ステータス、エンドポイント、エンドポイントのタイプ、VPNインデックス、ホスト名、ラウンドトリップ時間）を表示します。

- SD-WAN ManagerでMonitor > Devices > {select Device-Name} > Eventsの順に選択します。

トラッカーでフラップが検出されると、このセクションのそれぞれのログに、ホスト名、アタッチポイント名、トラッカー名、新しい状態、アドレスファミリ、およびVPN IDなどの詳細が記録されます。

EdgeのCLIで次のコマンドを実行します。

```
Router#show endpoint-tracker
```

```
Interface                      Record Name          Status        Address Family   RTT in msecs
1:101:9:tracker-service        tracker-service      Up            IPv4             10

Router#show endpoint-tracker records
Record Name                    Endpoint                          EndPoint Type Threshold(ms) Mult
tracker-service                10.10.1.4                         IP            300           3

Router#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------
*6           icmp-echo   10.10.1.4         RTT=1       OK          53 seconds ago

Router#show platform software sdwan service-chain database

Service Chain: SC1
   vrf: 1
   label: 1005
   state: up
   description: FW-Insertion-Service-1

   service: FW
      sequence: 1
      track-enable: true
      state: up
      ha_pair: 1
         type: ipv4
         posture: trusted
         active: [current]
            tx: GigabitEthernet3, 10.10.1.4
                endpoint-tracker: tracker-service
                state: up
            rx: GigabitEthernet3, 10.10.1.4
                endpoint-tracker: tracker-service
                state: up
```

スタティックルートトラッキングに使用されるスタティックルートエンドポイントトラッカー（サービス側）

2つ目のタイプのエンドポイントトラッカーは、スタティックルートベースのエンドポイントトラッカーと呼ばれます。名前が示すように、これらのタイプのトラッカーは主に、サービス側VPNで定義されたスタティックルートのネクストホップアドレスを追跡するために使用されます。デフォルトでは、「接続」および「スタティック」ルートタイプはすべてOMPプロトコルにアドバタイズされます。その後、それぞれのサービスVPNを含むすべてのリモートサイトがその宛先プレフィックス（ネクストホップは発信元サイトのTLOCを指す）を認識します。 発信側サイトは、特定のスタティックルートが開始されたサイトです。

ただし、スタティックルートのネクストホップアドレスが到達不能になった場合、ルートはOMPにアドバタイズされるのを停止しません。これにより、発信元サイト宛てのフローに対して

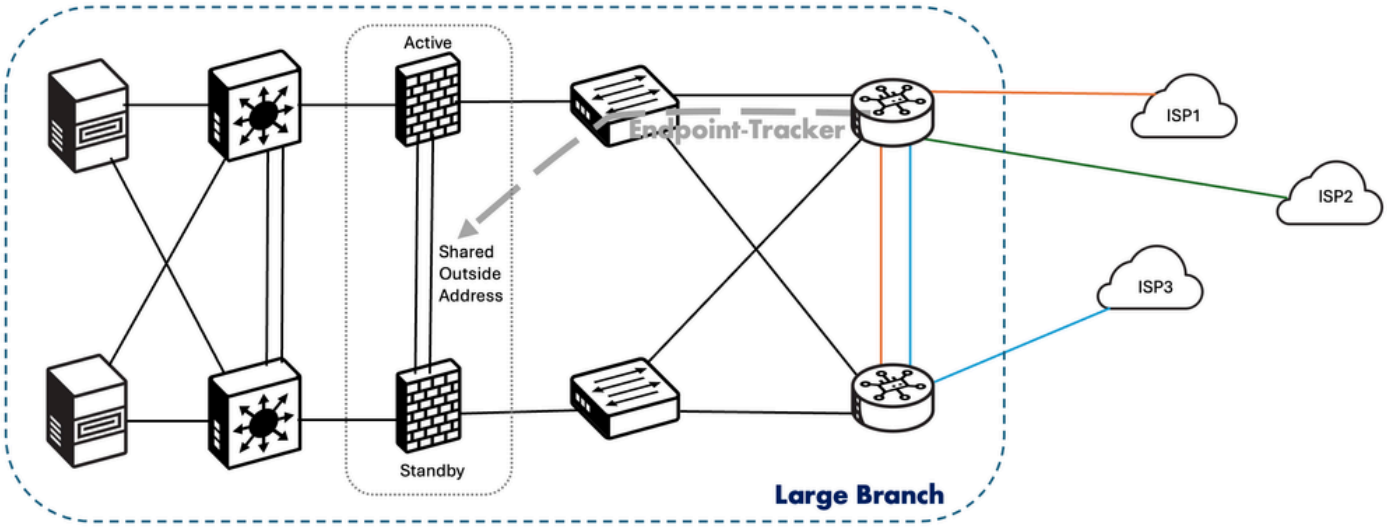
トラフィックがブラックホール化する問題が発生します。このため、ネクストホップアドレスが到達可能な場合にだけスタティックルートをOMPにアドバタイズできるように、スタティックルートにトラッカーを接続する必要があります。この機能は、基本的なIPアドレスタイプのスタティックルートベースのエンドポイントトラッカー用に20.3/17.3リリースで導入されました。20.7/17.7リリース以降では、トラッカープローブをネクストホップIPアドレスの特定のTCPポートまたはUDPポートにのみ送信する機能がサポートされるようになりました（ファイアウォールを使用してトラッキング目的でのみ特定のポートを開く場合）。 スタティックルートトラッカーの詳細については、設定ガイドを参照してください。

ここで使用されるプローブのタイプは、単純なICMPエコー要求パケットです。使用される間隔は次のとおりです。

- Hello:60秒
- ホールドタイム：180秒(#retriesは3 = 3 x 60秒であるため)
- パケット/プローブタイプ：ICMPエコー/エコー応答

使用例

このタイプのスタティックルートベースのエンドポイントトラッカーは、スタティックルートのネクストホップアドレスのサービス側トラッキングに使用されます。このような一般的なシナリオの1つは、アクティブ/スタンバイファイアウォールのペアに対応するLAN側のネクストホップアドレスを追跡することです。この場合、どの外部インターフェイスが「アクティブ」ファイアウォールの役割を果たしているかによって、外部IPアドレスが共有されます。特定のポートだけがユースケースに基づく目的で開かれているファイアウォール規則が非常に制限されていると思われる場合は、スタティックルートトラッカーを使用して、LAN側ファイアウォールの外部インターフェイスに属するネクストホップIPアドレス宛ての特定のTCP/UDPポートを追跡できます。



コンフィギュレーション

これらのスタティックルートベースのエンドポイントトラッカーは、この機能セットを有効にするために手動で設定する必要があります。ユーザが希望する設定方法のタイプに応じて、設定方法を次に示します。

- Configuration group Configuration > Configuration Groups > Service Profile > Service VPN > Add Feature > Tracker:

1. 定義する新しい（エンドポイント）トラッカーの名前、説明、およびトラッカー名を入力してください。

2. ネクストホップIPアドレスだけを追跡する必要があるか(Addressオプションボタンを選択)、または特定のTCP/UDPポートだけを追跡する必要があるか(Protocolオプションボタンを選択)に応じて、エンドポイントのタイプを選択します。

3. アドレスをIPアドレス形式で入力します。また、前のステップでエンドポイントタイプとしてプロトコルを選択した場合は、プロトコル（TCPまたはUDP）とポート番号を入力します。

4. 必要に応じて、プローブ間隔、再試行回数、および遅延制限に指定されたデフォルト値を変更できます。

- Configuration > Configuration Groups > Service Profile > Service VPN > Routeセクション：

1. [IPv4/IPv6スタティックルートの追加]ボタンを選択します。

2. ネットワークアドレス、サブネットマスク、ネクストホップ、アドレス、ADなどの詳細を入力します。

3. Add Next Hop With Trackerボタンをクリックします。

4. ネクストホップアドレスとADを再入力し、前に作成した（エンドポイント）トラッカー名をドロップダウンリストから選択します。

- レガシー設定Configuration > Templates > Feature Templates > System Template > Trackerセクション：

1. [新しいエンドポイントトラッカー]ボタンを選択します。

2. 定義する新しい（エンドポイント）トラッカーの名前を指定します。

3. Tracker Typeオプションボタンをstatic-routeに変更します。

4. ネクストホップIPアドレスとしてエンドポイントタイプを選択します（「IPアドレス」ラジオボタンを選択）。

5. エンドポイントIPをIPアドレス形式で入力します。

6. 必要に応じて、プローブ間隔、再試行回数、および遅延制限に指定されたデフォルト値を変更できます。

- Configuration > Templates > Feature Templates > Cisco VPN （サービス側のみ） > IPv4/IPv6 Routeセクション：

1. New IPv4/IPv6 Routeボタンを選択します。

2. プレフィックス、ゲートウェイなどの詳細を入力します。

3. Add Next Hop With Trackerボタンをクリックします。

4. ネクストホップアドレス、AD（距離）を再入力し、以前に作成した（エンドポイント）トラッカー名を手動で入力します。

CLIの観点からは、設定は次のようになります。

```
(i) For the static-route-based endpoint tracker being used with IP address :
!
endpoint-tracker nh10.10.1.4-s10.20.1.0
 tracker-type static-route
 endpoint-ip  10.10.1.4
!
track nh10.10.1.4-s10.20.1.0 endpoint-tracker
!
ip route vrf 1 10.20.1.0 255.255.255.0 10.10.1.4 track name nh10.10.1.4-s10.20.1.0
!

(ii) For the static-route-based endpoint tracker being used with IP address along with TCP/UDP port :
!
endpoint-tracker nh10.10.1.4-s10.20.1.0-tcp-8484
 tracker-type static-route
 endpoint-ip  10.10.1.4 tcp 8484
!
track nh10.10.1.4-s10.20.1.0-tcp-8484 endpoint-tracker
!
ip route vrf 1 10.20.1.0 255.255.255.0 10.10.1.4 track name nh10.10.1.4-s10.20.1.0-tcp-8484
!
```

検証

明示的に設定されたエンドポイントトラッカーの検証には、2つのエリアがあります。

- SD-WAN Manager Monitor > Devices > {select Device-Name} > Real Time:

1. デバイスオプションで、「エンドポイントトラッカー情報」を入力します。

2. Individual Tracker (Attach Point Name)で確認し、設定したトラッカー名に基づいたトラッカーの統計情報(トラッカーの状態、関連するトラッカーレコード名、デバイスからエンドポイントまでの待機時間、最終更新タイムスタンプ)を確認します。

- SD-WAN Manager Monitor > Devices > {select Device-Name} > Eventsの順に選択します。

トラッカーでフラップが検出されると、このセクションの各ログに、ホスト名、アタッチポイント名、トラッカー名、新しい状態、アドレスファミリ、VPN IDなどの詳細が入力されます。

EdgeのCLIで次のコマンドを実行します。

```
Router#sh endpoint-tracker static-route
Tracker Name                   Status          RTT in msec     Probe ID
```

```
nh10.10.1.4-s10.20.1.0         UP              1               3

Router#show track endpoint-tracker
Track nh10.10.1.4-s10.20.1.0
  Ep_tracker-object
  State is Up
    2 changes, last change 00:01:54, by Undefined
  Tracked by:
    Static IP Routing 0

Router#sh endpoint-tracker records
Record Name                     Endpoint                                EndPoint Type Threshold(ms) Mult
nh10.10.1.4-s10.20.1.0          10.10.1.4                               IP            300           3

Router#sh ip sla summ
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------
*3           icmp-echo   10.10.1.4         RTT=1       OK          58 seconds ago

EFT-BR-11#sh ip static route vrf 1
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       D1 - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng, LI - LIIN
       IR - ICMP Redirect, Vx - VXLAN static route
       LT - Cellular LTE, Ev - L2EVPN static route
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - permanent, -T Default Tr


Codes in (): UP - up, DN - Down, AD-DN - Admin-Down, DL - Deleted
Static local RIB for 1

M  10.20.1.0/24 [1/0] via 10.10.1.4 [A]
T               [1/0] via 10.10.1.4 [A]
```

VRRPトラッキングに使用されるインターフェイスオブジェクトトラッカー

オブジェクトトラッカーは、自律モードでの使用を目的として設計されたトラッカーです（使用例）。 これらのトラッカーの使用例は、VRRPベースのインターフェイス/トンネルトラッキングからサービスVPN NATトラッキングまでさまざまです。

VRRPトラッキングの使用例では、VRRP状態はトンネルリンクステータスに基づいて決定されます。トンネルまたはインターフェイスがプライマリVRRPでダウンしている場合、トラフィック

はセカンダリVRRPに転送されます。LANセグメントのセカンダリVRRPルータがプライマリVRRPになり、サービス側トラフィックにゲートウェイを提供します。この使用例はservice-VPNにのみ適用され、SD-WANオーバーレイ（SSEの場合はインターフェイスまたはトンネル）で障害が発生した場合にLAN側のVRRPロールのフェールオーバーに役立ちます。 トラッカーをVRRPグループにアタッチするには、オブジェクトトラッカーのみを使用できます（エンドポイントトラッカーは使用できません）。 この機能は、Cisco Catalyst SD-WANエッジ用の20.7/17.7リリースから導入されました。

この場合、トラッカーによって使用されるプローブはありません。代わりに、回線プロトコルの状態を使用してトラッカーの状態（アップ/ダウン）が決定されます。 インターフェイス回線プロトコルベースのトラッカーには反応間隔がありません。インターフェイス/トンネル回線プロトコルがダウンすると、トラック状態もダウン状態になります。シャットダウンまたはデクリメントのいずれかのアクションに応じて、VRRPグループはそれに応じて再コンバージェンスします。 VRRPインターフェイストラッカーの詳細については、設定ガイドを参照してください。

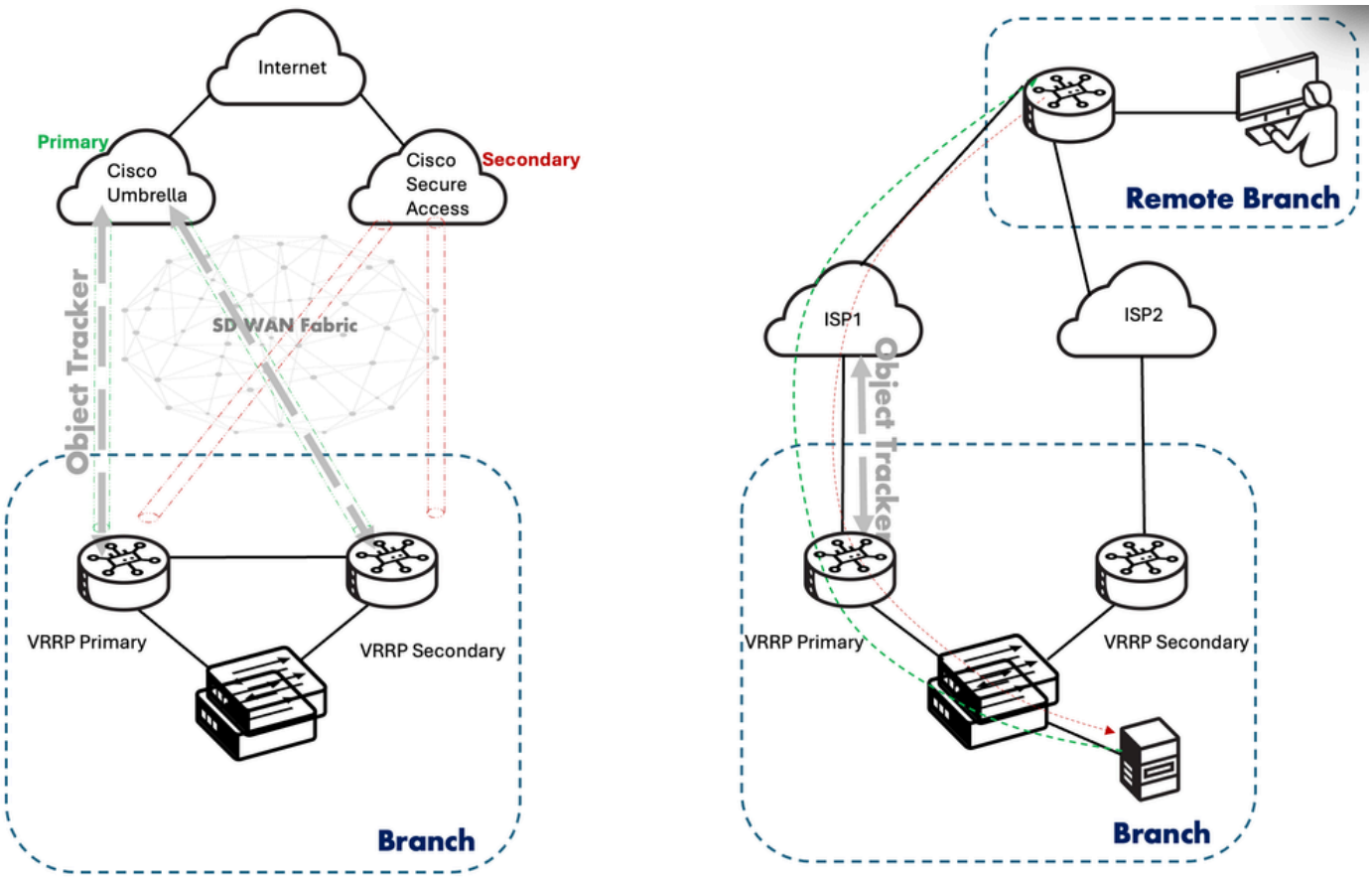
使用例

VRRPベースのインターフェイストラッキングを実装するために必要な基準に基づいて、複数の使用例があります。現在サポートされている2つのモードは、(i)インターフェイス（ローカルTLOCにバインドされた任意のトンネルインターフェイスを意味します）または(ii) SIGインターフェイス（SIGトンネルインターフェイスに関連します）です。 いずれの場合も、追跡される部分はインターフェイス回線プロトコルです。

インターネットを使用したデュアルルータ：トラックオブジェクトはVRRPグループにバインドされます。トラッカーのオブジェクト（この場合はSIGトンネルインターフェイス）がダウンした場合、VRRPプライマリルータに通知され、プライマリからバックアップへの状態遷移がトリガーされ、バックアップルータがプライマリになります。この状態の変化は、次の2種類の動作によって影響を受けたり、トリガーしたりできます。

1. Decrement（デクリメント）：トラックオブジェクトの状態がUPからDOWNに移行した場合、VRRP VIPが設定されているインターフェイスのVRRPプライオリティが特定の値だけ減少または減少します。
2. Shutdown（シャットダウン）：これは、トラックオブジェクトの状態がアップからダウンに移行した場合に、適用されているインターフェイスでVRRPプロセスがシャットダウンされる方式です。この方法は、非対称フォワーディングのインスタンスが存在する場合には推奨されません。

TLOCの優先度の変更：他のSDWANサイトから、VRRPがサービスVPN上で実行されているサイトに着信する非対称トラフィックを回避するために、VRRPプライマリルータのTLOCの優先度は、設定されている場合に1ずつ上げられます。この値は、設定グループで変更することもできます。これにより、WANからLANへのトラフィックがVRRPプライマリルータ自体に引き付けられるようになります。LANからWANへのトラフィックは、VRRPプライマリのVRRPメカニズムによって引き付けられます。この機能は、VRRPインターフェイストラッカーとは独立しています。これは、CLIから見たオプションのコマンド(tloc-change-pref)です。



コンフィギュレーション

オブジェクトトラッカーの設定は、レガシー設定のシステムテンプレートを使用して行います。その後、service-VPNイーサネットインターフェイス機能テンプレートの下で、オブジェクトトラッカーをそれぞれのVRRPグループに接続します。構成グループでは、オブジェクトトラッカーを各サービスプロファイルのイーサネットインターフェイスプロファイルに追加するオプションを直接取得することで、このメカニズムが簡素化されています。 ユーザが希望する設定方法のタイプに応じて、設定方法を次に示します。

- Configurationグループ Configuration > Configuration Groups > Service Profile > Ethernet Interface > Add Feature > Object Tracker:

1. 定義する新しいオブジェクトトラッカーの名前と説明を入力してください。
2. Tracker Type(InterfaceおよびSIG内)を選択します。
3. オブジェクトトラッカーIDを割り当てます。
4. Interface Nameを入力します（ステップ2で選択したオプションに応じて異なります）。

- Configuration > Configuration Groups > Service Profile > Ethernet Interface > VRRPセクション：

1. IPv4 Settingsで、Add VRRP IPv4をクリックします。
2. VRRPグループIDを定義して、このサービス側のイーサネットインターフェイスにローカルプライオリティを設定します。
3. VRRP仮想IP(VIP)アドレスを入力します。
4. TLOC Preference Changeノブを有効にし、TLOC Preference Change Value（非対称ルーテ

ィングを処理するため）を指定します。
5. Add VRRP Tracking Objectをクリックします。
6. Associate Object Trackerで、前に作成したObject Tracker（名前に基づく）のドロップダウンから選択します
7. トラッカーアクション(シャットダウンまたはデクリメント)を選択します。
8. 減少値を入力します（ステップ7で選択したオプションによって異なります）。

- レガシー設定Configuration > Templates > Feature Templates > System > Trackerセクション：

1. New Object Trackerボタンをクリックします。
2. Tracker Type(InterfaceおよびSIG内)を選択します。
3. オブジェクトIDを割り当てます。
4. インターフェイス名を入力します（ステップ2で選択したオプションによって異なります）。

- Configuration > Templates > Ethernet Interface （サービス側に所属） > VRRPセクション：

1. New VRRPボタンをクリックします。
2. VRRPグループIDを定義して、このサービス側イーサネットインターフェイスのローカルプライオリティを指定します（オプションで、デフォルト値の100が選択されます）。
3. VRRP仮想IP(VIP)アドレスを入力します。
4. TLOC Preference Changeノブを有効にし、TLOC Preference Change Valueを指定します（非対称ルーティングを処理するため）。
5. Object TrackerでAdd Tracking Objectをクリックします。
6. オブジェクトトラッカーID（システムテンプレートで定義）を入力します。
7. トラッカーアクション(シャットダウンまたはデクリメント)を選択します。
8. 減少値を入力します（ステップ7で選択したオプションによって異なります）。

CLIの観点からは、設定は次のようになります。

```
(i) Using interface (Tunnel) Object Tracking :
!
track 10 interface Tunnel1 line-protocol
!
interface GigabitEthernet3
 description   SERVICE VPN 1
 no shutdown




 vrrp 10 address-family ipv4
  vrrpv2
  address 10.10.1.1
  priority 120
  timers advertise 1000
  track 10 decrement 40
  tloc-change increase-preference 120
 exit
exit
```

```
!
(ii) Using SIG interface Object Tracking :
!
track 20 service global
!
interface GigabitEthernet4
 description   SERVICE VPN 1
 no shutdown




 vrrp 10 address-family ipv4
  vrrpv2
  address 10.10.2.1
  priority 120
  timers advertise 1000
  track 20 decrement 40
  tloc-change increase-preference 120
 exit
exit
!
```

検証

VRRPのユースケースで明示的に設定されたオブジェクトトラッカーを確認するには、2つのオプションがあります。

- SD-WAN Manager Monitor > Devices > {select Device-Name} > Real Time:

1. Device Optionsの下で、「VRRP Information」と入力します。

2.個々のVRRPグループ（グループID）で確認し、設定したオブジェクトトラッカーIDに基づいてトラッカーの統計情報(トラックプレフィックス名、トラック状態、不連続時間、および最終状態変更時間)を表示します。

- SD-WAN Manager Monitor > Devices > {select Device-Name} > Eventsの順に選択します。

オブジェクトトラッカーで状態変化が検出されると、それに対応するVRRPグループにアタッチされているによってその状態が変更されます。このセクションには、host name、if number、grp id、addr type、if name、vrrp group-state、state change-reason、vpn idなどの詳細が、それぞれのログ(名前はVrrp Group State Change)として入力されます。

EdgeのCLIで次のコマンドを実行します。

```
Router#show vrrp 10 GigabitEthernet 3
GigabitEthernet3 - Group 10 - Address-Family IPv4
  State is MASTER
```

```
  State duration 59 mins 56.703 secs
  Virtual IP address is 10.10.1.1
  Virtual MAC address is 0000.5E00.010A
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 120
  State change reason is VRRP_TRACK_UP
  Tloc preference configured, value 120
    Track object 10 state UP decrement 40
  Master Router is 10.10.1.3 (local), priority is 120
  Master Advertisement interval is 1000 msec (expires in 393 msec)
  Master Down interval is unknown
  FLAGS: 1/1

Router#show track 10
Track 10
  Interface Tunnel1 line-protocol
  Line protocol is Up
    7 changes, last change 01:00:47
  Tracked by:
    VRRPv3 GigabitEthernet3 IPv4 group 10

Router#show track 10 brief
Track Type        Instance                  Parameter        State Last Change
10    interface   Tunnel1                   line-protocol    Up    01:01:02

Router#show interface Tunnel1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of GigabitEthernet1 (172.25.12.1)
  MTU 9980 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.25.12.1 (GigabitEthernet1)
```

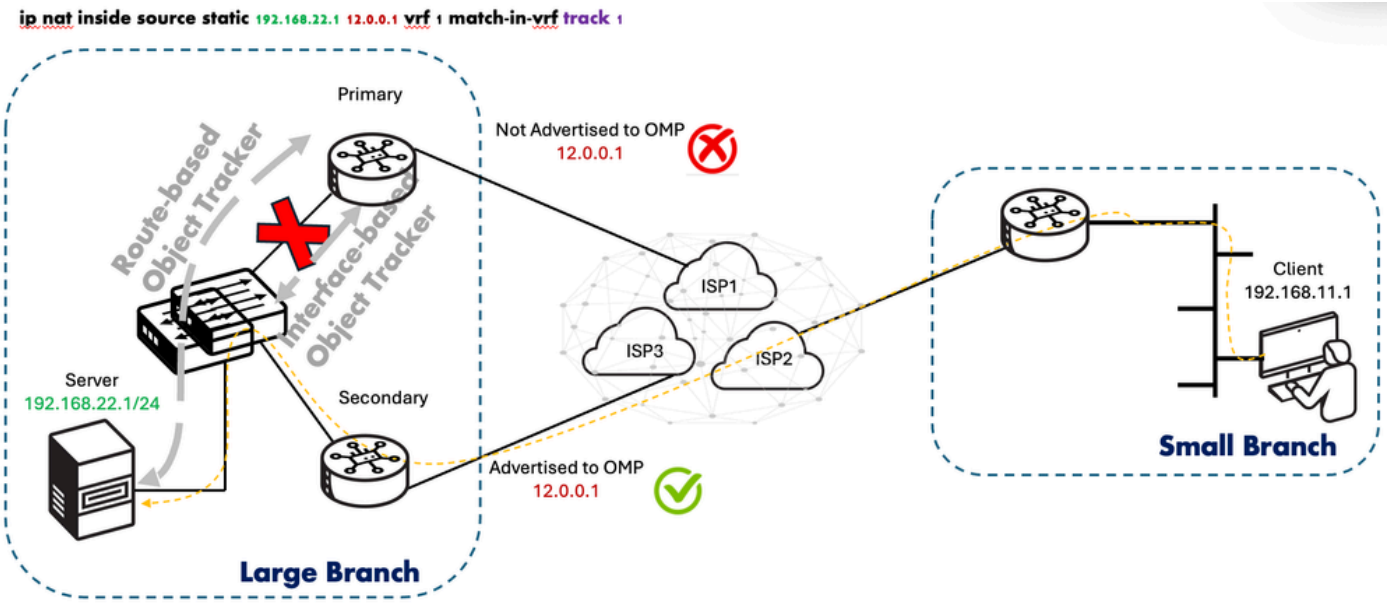
Service-VPN NATトラッキングに使用されるインターフェイス/ルートオブジェクトトラッカー

サービス側NATオブジェクトトラッカーは20.8/17.8リリースで導入された機能であり、service-VPN NATで使用される内部グローバルアドレス (内部スタティックNATおよび内部ダイナミックNAT) は、(i)内部ローカルアドレスが到達可能であると見つかった場合、または(ii) LAN/サービス側インターフェイスの回線プロトコルが接続されているオブジェクトトラッカーに従ってアップしている場合にのみ、OMPにアドバタイズされます。したがって、使用できるオブジェクトトラッカータイプは、(i)ルートまたは(ii)インターフェイスです。 LANプレフィクスまたはLANインターフェイスの状態に応じて、OMPを介したNATルートアドバタイズメントは追加または削除されます。Cisco SD-WAN Managerでイベントログを表示して、どのNATルートアドバタイズメントが追加または削除されたかを監視できます。

この場合、トラッカーによって使用されるプローブはありません。代わりに、(i)ルーティングテーブル内にルーティングエントリが存在するか、(ii)回線プロトコルの状態を使用して、トラッカーの状態（アップ/ダウン）が決定されます。 ルーティングエントリまたはインターフェイスの回線プロトコルに基づくトラッカーが存在する場合、対応する間隔はありません。ルーティングエントリまたはインターフェイスの回線プロトコルがダウンすると、トラックの状態もダウンの状態になります。オブジェクトトラッカーに関連付けられたNAT文で使用される内部グローバルアドレスは、ただちにOMPにアドバタイズされなくなります。 Service VPN NATトラッカーの詳細については、設定ガイドを参照してください。

使用例

LANインターフェイスまたはLANプレフィクスがダウンすると、サービス側のNATオブジェクトトラッカーが自動的にダウンします。イベントログは Cisco SD-WANマネージャ どのNATルートアドバタイズメントが追加または削除されるかを監視します。次の使用例では、クライアントは大規模ブランチのサーバにアクセスする必要があります。ただし、大きなブランチエッジ（HAの場合）のサーバを指すルートが削除された場合や、LAN側（サービス側）インターフェイスが大きなブランチのいずれかのエッジでダウンした場合に、問題が発生します。このような場合、オブジェクトトラッカーでサービス側NATを適用するときは、OMPへの内部グローバルアドレスアドバタイズメントを制御することで、クライアントからのインバウンド方向のトラフィックが常に大きなブランチ内の正しいエッジに向いていることを確認してください。OMPへのルートアドバタイズメントでこのような制御が強制されない場合、各エッジから大規模ブランチ内のサーバへの到達不能が原因で、トラフィックがブラックホール化してしまいます。



コンフィギュレーション

オブジェクトトラッカーの設定は、レガシー設定のシステムテンプレートを介して行われます。その後、オブジェクトトラッカーをservice-VPN機能テンプレートのそれぞれのNATステートメント（内部スタティックまたは内部ダイナミック）にアタッチします。構成グループでは、オブジェクトトラッカーを各サービスプロファイルのイーサネットインターフェイスプロファイルに追加するオプションを直接取得することで、このメカニズムが簡素化されています。 ユーザが希望する設定方法のタイプに応じて、設定方法を次に示します。

- Configurationグループ Configuration > Configuration Groups > Service Profile > Add Feature > Object Tracker:

1. 定義する新しいオブジェクトトラッカーの名前と説明を入力してください。
2. Tracker Type(Interfaceとrouteの中)を選択します。
3. オブジェクトトラッカーIDを割り当てます。
4. Interface Name(インターフェイス名)を入力するか、ルートIP、ルートIPマスク、およびVPN（ステップ2で選択したオプションに応じて）を入力します。

- Configuration > Configuration Groups > Service Profile > NATセクション：

1. Add NAT Poolボタンをクリックして、NATプールを作成します（SSNATをトリガーするために必須）。

2. NatPool Name、Prefix Length、Range Start、Range End、およびDirectionなどのNATプールの詳細を指定します。

3. 同じセクションのStatic NATに移動し、Add New Static NATボタンをクリックします。（オブジェクトトラッカーを内部ダイナミックプールNATに接続することもできます）。

4. 送信元IP、変換済み送信元IP、スタティックNAT方向などの詳細を指定します。

5. Associate Object Trackerフィールドで、ドロップダウンリストから以前に作成したオブジェクトトラッカーを選択します。

- レガシー設定Configuration > Templates > Feature Templates > System > Trackerセクション：

1. New Object Trackerボタンをクリックします。
2. トラッカータイプ(インターフェイスとルートの中)を選択します。
3. オブジェクトIDを割り当てます。
4. インターフェイス名またはルートIP、ルートIPマスク、およびVPN(ステップ2で選択したオプションに応じて)を入力します。

- Configuration > Templates > Cisco VPN（サービス側に所属）> NATセクション：

1. New NAT Poolボタンをクリックして、NAT Poolを作成します（SSNATをトリガーするために必須）。

2. NATプール名、NATプールプレフィックス長、NATプール範囲の開始、NATプール範囲の終了、NAT方向などのNATプールの詳細を提供します。

3. 同じセクションのスタティックNATに移動し、New Static NATボタンをクリックします。（オブジェクトトラッカーを内部ダイナミックプールNATに接続することもできます）。

4. 送信元IPアドレス、変換済み送信元IPアドレス、スタティックNAT方向などの詳細を提供します。

5.「オブジェクト・トラッカーの追加」フィールドに、以前に作成したオブジェクト・トラッカーの名前を入力します。

CLIの観点からは、設定は次のようになります。

```
(i) Using route-based object tracking on SSNAT (inside static or inside dynamic) :
!
track 20 ip route 192.168.10.4 255.255.255.255 reachability
 ip vrf 1
!
ip nat pool natpool10 14.14.14.1 14.14.14.5 prefix-length 24
ip nat inside source list global-list pool natpool10 vrf 1 match-in-vrf overload
ip nat inside source static 10.10.1.4 15.15.15.1 vrf 1 match-in-vrf track 20
!
(ii) Using interface-based object tracking on SSNAT (inside static or inside dynamic) :
!
track 20 interface GigabitEthernet3 line-protocol
!
ip nat pool natpool10 14.14.14.1 14.14.14.5 prefix-length 24
ip nat inside source list global-list pool natpool10 vrf 1 match-in-vrf overload
ip nat inside source static 10.10.1.4 15.15.15.1 vrf 1 match-in-vrf track 20
!
```

SSNATの使用例では、NATフローのin -> outおよびout ->の両方のトラフィックを照合するためにユーザがデータポリシーを適用することを前提としています。

検証

NATの使用例では、明示的に設定されたオブジェクトトラッカーの確認には2つの領域があります。

- SD-WAN Manager:Monitor > Devices > {select Device-Name} > Real Time:

1. デバイスオプションで、「IP NAT Translation」と入力します。

2. Individual NAT Translationで、設定したObject Tracker IDに基づいてエントリの統計情報（Insideローカルアドレス/ポート、Insideグローバルアドレス/ポート、Outsideローカルアドレス/ポート、Outsideグローバルアドレス/ポート、VRF ID、VRF名およびプロトコル）を表示します。

- SD-WAN Manager:Monitor > Devices > {select Device-Name} > Events:

OMPにプルーニングされているNATルートに対応するオブジェクトトラッカーで状態変化が検出されると、「NAT Route Change」という名前のイベントが表示されます。このイベントには、ホスト名、オブジェクトトラッカー、アドレス、マスク、ルートタイプ、更新などの詳細が含まれています。このアドレスとマスクは、スタティックNAT文の下で設定された内部グローバルアドレスにマッピングされます。

EdgeのCLIで次のコマンドを実行します。

```
Router#show ip nat translations vrf 1
Pro  Inside global         Inside local          Outside local         Outside global
---  15.15.15.1            10.10.1.4             ---                   ---
```

```
icmp 15.15.15.1:4          10.10.1.4:4           20.20.1.1:4           20.20.1.1:4
Total number of translations: 2

Router#show track 20
Track 20
  IP route 192.168.10.4 255.255.255.255 reachability
  Reachability is Up (OSPF)
    4 changes, last change 00:02:56
  VPN Routing/Forwarding table "1"
  First-hop interface is GigabitEthernet3
  Tracked by:
    NAT 0

Router#show track 20 brief
Track Type        Instance                  Parameter        State Last Change
20    ip route    192.168.10.4/32           reachability     Up    00:03:04

Remote-Router#show ip route vrf 1 15.15.15.1

Routing Table: 1
Routing entry for 15.15.15.1/32
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via ospf 1
  Advertised by ospf 1 subnets
  Last update from 10.10.10.12 on Sdwan-system-intf, 00:03:52 ago
  Routing Descriptor Blocks:
  * 10.10.10.12 (default), from 10.10.10.12, 00:03:52 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1

Remote-Router#show sdwan omp routes 15.15.15.1/32

                                                    PATH                    ATTRIBUTE
TENANT    VPN     PREFIX              FROM PEER     ID     LABEL    STATUS    TYPE       TLOC IP
-------------------------------------------------------------------------------------------------
0         1       15.15.15.1/32       1.1.1.3       1      1003     C,I,R     installed  10.10.10.12
                                      1.1.1.3       2      1003     Inv,U     installed  10.10.10.12
                                      1.1.1.3       3      1003     C,I,R     installed  10.10.10.12
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。