瞭解Catalyst SD-WAN跟蹤器的可用性和使用案例

目錄

簡介

本檔案介紹Catalyst SD-WAN企業重疊網路、追蹤器可用性和使用案例。

背景資訊

Catalyst SD-WAN企業重疊網路通常與各種外部工作負載、應用和服務互動。其中任何一種均可位於雲、資料中心/集線器或遠端分支機構。SD-WAN控制平面負責以可擴展的方式在重疊上向這些服務通告路由。在關鍵應用程式和服務沿著特定路徑變得不可達的情況下，網路運營商通常必須能夠檢測這些事件並將使用者流量重定向到更合適的路徑，以防止不確定的流量黑洞。為了檢測和糾正這些型別的網路故障，Catalyst SD-WAN控制平面依靠跟蹤器來監控外部服務的運行狀況，並根據情況更改路由。

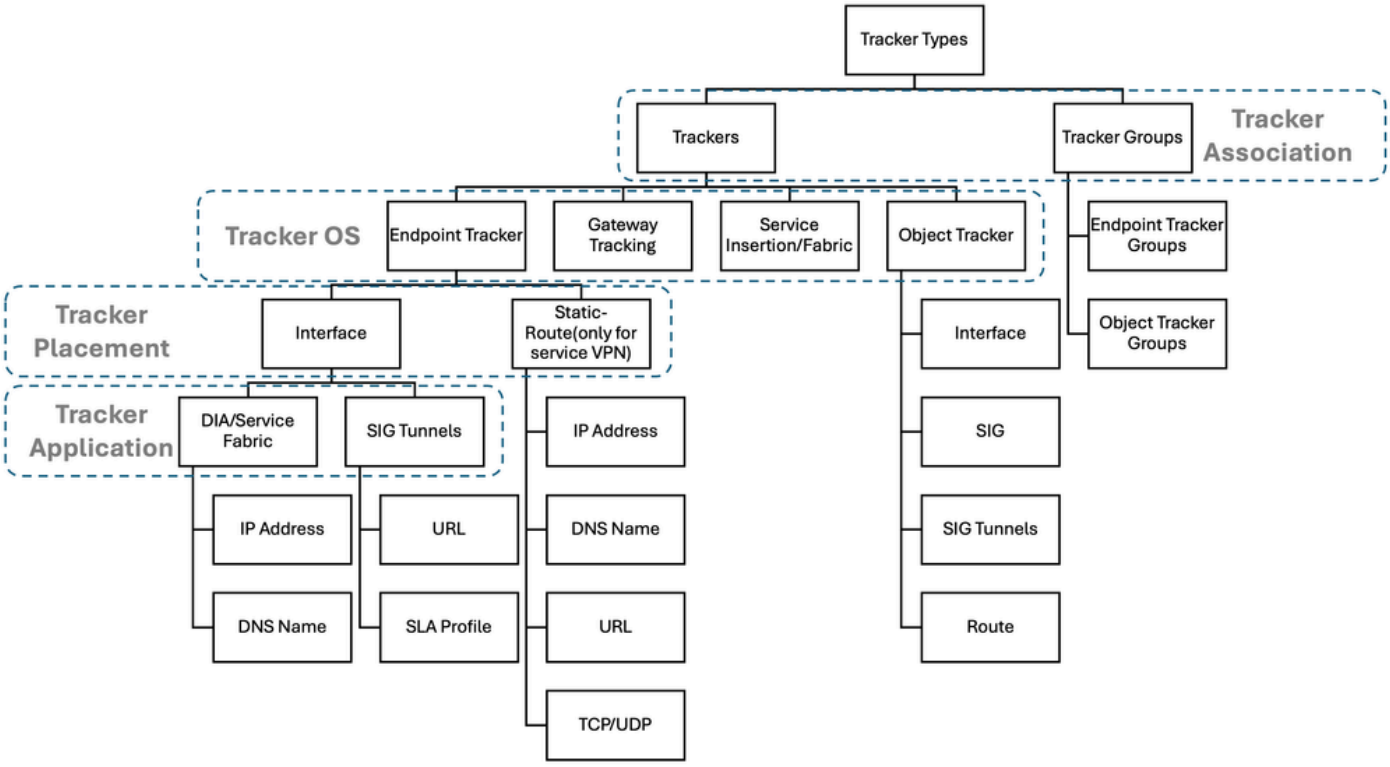
跟蹤器是一種控制平面可達性檢測機制，它向特定端點傳送探測包並將該端點的可達性狀態變化（啟動或關閉）通知到感興趣的模組。跟蹤器設計為本地Cisco IOS-XE® IP SLA功能的可擴展高級別抽象，可以形成各種探測器（包括HTTP、ICMP和DNS）。當跟蹤器通知客戶端模組狀態更改時，該模組可以採取適當的操作來防止流量黑鎖，例如安裝或解除安裝路由或路由集。SD-WAN和SD-Routing解決方案中跟蹤器的當前應用包括但不限於：DIA（直接網際網路接入）跟蹤器、SIG（安全網際網路網關）跟蹤器、服務跟蹤器、靜態路由跟蹤器、跟蹤器組等。

要構建可恢復服務故障的高可用性網路，瞭解何時使用每種型別的跟蹤器配置/模型至關重要。本文的目的是說明每種跟蹤器的使用位置和方式。本文講述了各種跟蹤器，每個跟蹤器的主要使用案例，以及實施每個解決方案的基本配置工作流。最後，本文簡要介紹了Cisco IOS-XE®中涉及跟蹤器的一般警告。

本文對endpoint-tracker（特定於SD-WAN和SD-Routing）和object tracker解決方案（本地IOS-XE）加以區分，這兩種解決方案針對不同的使用情形。

跟蹤器的型別

此圖表簡要概述了Cisco Catalyst SD-WAN解決方案中可用的各種跟蹤器：



在上一個圖表中，有四個區域可以分類跟蹤器：跟蹤器關聯、跟蹤器作業系統、跟蹤器放置和跟蹤器應用。下一節將介紹每個分類：

1. 跟蹤器關聯：此分類描述跟蹤器是單個跟蹤器還是跟蹤器組。Cisco Catalyst SD-WAN支援在一個組中使用多個跟蹤器（此時寫入時最多2個），並且跟蹤器組的整體狀態由布林型AND或OR運算子決定。示例包括終結點跟蹤器組或對象跟蹤器組。
2. 跟蹤器操作系統：此分類描述支援跟蹤器的Cisco IOS-XE®作業系統或模式。Cisco Catalyst IOS-XE路由器支援兩種操作模式：

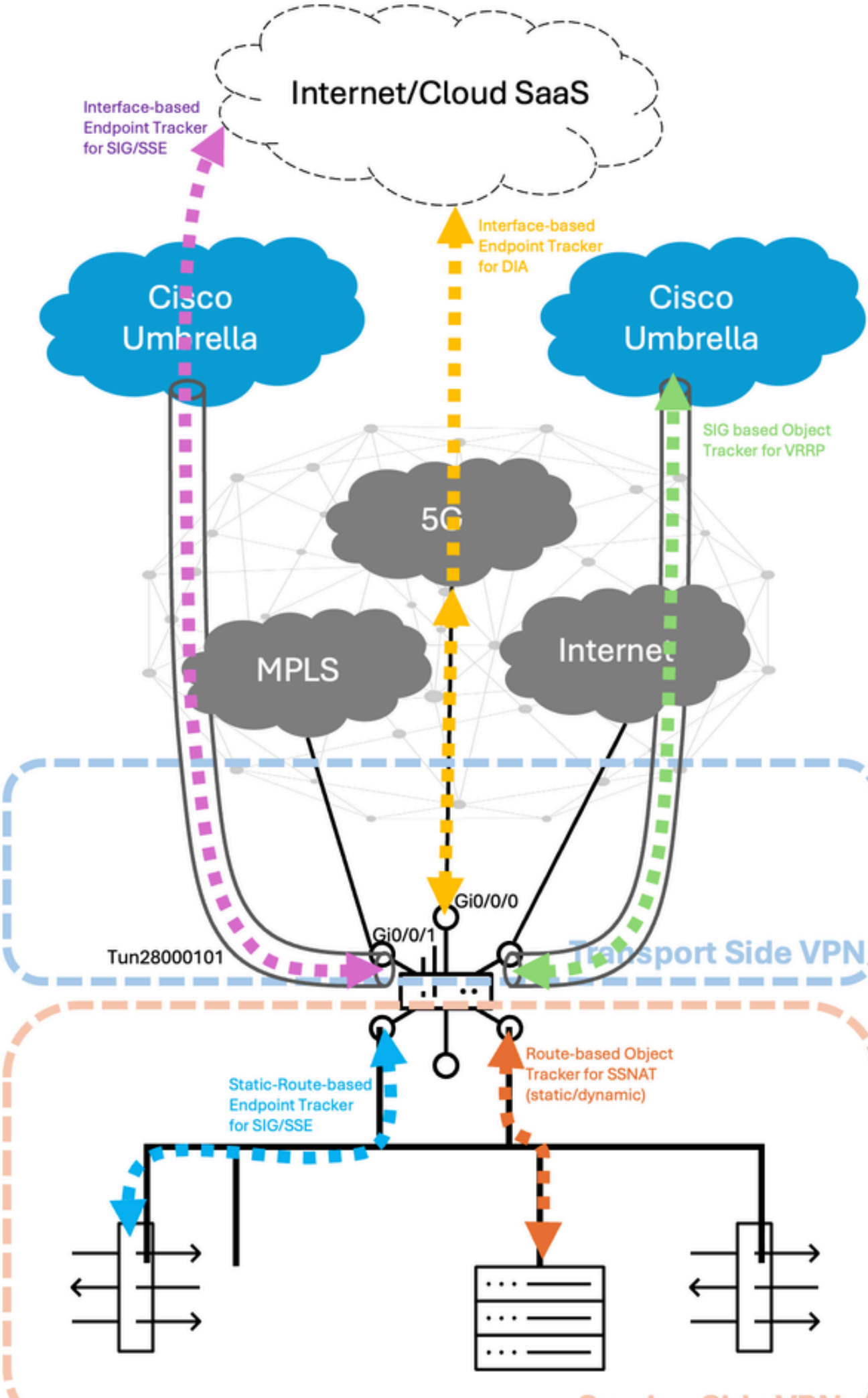
- 自主模式和
- 控制器模式。

所有endpoint-tracker和gateway tracking功能都用於控制器模式(SD-WAN)使用案例，而object tracker用於自主模式(SD-Routing)使用案例。

3.跟蹤器放置:此分類描述配置跟蹤器的位置。目前，Cisco Catalyst SD-WAN支援在介面、靜態路由或服務上應用跟蹤器。

4.跟蹤器應用:此分類介紹Cisco Catalyst SD-WAN支持的高級使用案例和功能。雖然跟蹤器的應用領域眾多，但其中有些包括：直接網際網路接入(DIA)、安全網際網路網關(SIG)、安全服務邊緣(SSE)、服務端VPN跟蹤等。

以下是在Cisco Catalyst SD-WAN邊緣（也可以稱為cEdge或vEdge）上多個使用情形下跨服務/傳輸VPN的跟蹤器探測流量的直觀描述：


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

中每個預設靜態路由下指定的下一跳地址，以確保在下一跳（也稱為網關，因此稱為名稱網關跟蹤）的可達性發生故障時進行鏈路/路由故障轉移。要瞭解有關網關跟蹤的更多資訊，請訪問配置指南。

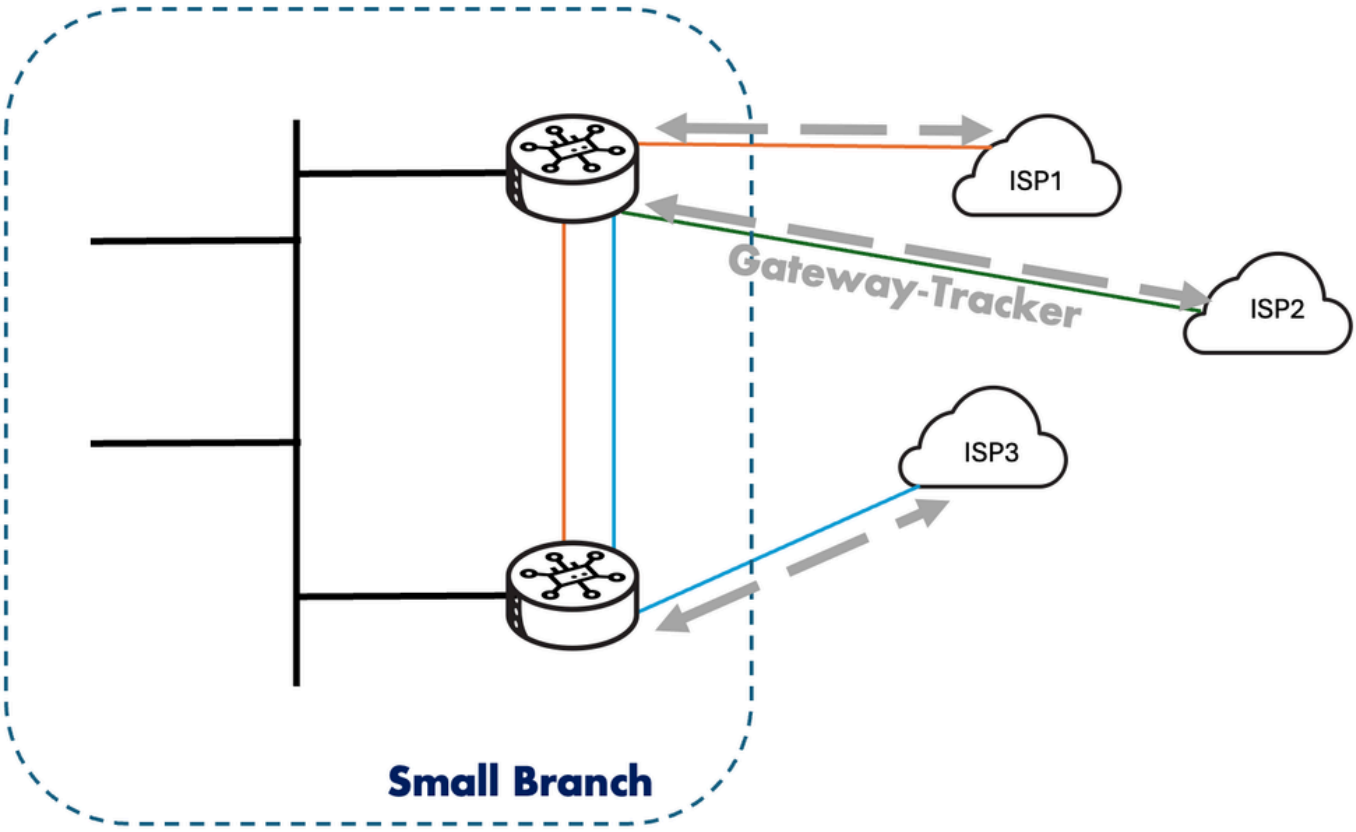
此處使用的探查型別為ARP-request unknown-unicast泛洪資料包。使用的間隔為：

- 您好：10秒
- 保持時間：100秒
- 資料包/探測型別：ARP

除了網關跟蹤，還用於SD-WAN邊緣上的傳輸跟蹤，用於檢查本地裝置與Cisco Catalyst SD-WAN驗證器之間的路由路徑。這是通過以正規間隔3s使用ICMP探測器完成的。在SD-WAN系統配置模式下使用「track-transport」關鍵字進行配置。這有助於從各自的WAN邊緣定期監控到Cisco Catalyst SD-WAN驗證器的DTLS連線。要瞭解有關傳輸跟蹤的詳細資訊，請訪問配置指南。

使用案例

網關跟蹤是一項功能，預設情況下，在SD-WAN上為屬於傳輸VPN或全域性路由表(GRT)的所有靜態預設路由隱式配置。 此功能的使用並不總是從Manager模板配置的角度出發，但在使用帶#3、#81等選項的DHCP伺服器的情況下，它還可以從接收/獲取的預設靜態路由發展而來。



組態

預設應用於Cisco Catalyst SD-WAN:

```
!
system



 track-transport
 track-default-gateway



!
```

驗證

以下是根據舊版組態和組態組驗證此內容的方法：

- 配置組：Configuration > Configuration Groups > System profile > Basic sub-profile > Track Settings section > Track Default Gateway(default:ON)
- 舊配置：Configuration > Templates > Feature Templates > System template > Advanced section > Gateway Tracking（預設：ON）

服務插入1.0和服務交換矩陣2.0跟蹤

20.3/17.3版引入了服務插入1.0跟蹤，該功能旨在確保服務地址（或轉發地址）可訪問或可用。此資訊可幫助邊緣動態新增或從控制/資料策略中撤消下一跳資訊。通過配置Service Insertion 1.0，預設情況下會針對服務地址啟用跟蹤器（或跟蹤地址）。基於此，轉發地址和服務地址在1.0中是相同的。即使服務跟蹤程式自動配置了服務，也可以使用no track-enable 命令，或通過在配置組/舊版配置中禁用tracker旋鈕來禁用這些跟蹤程式。由於這些操作是與服務插入1.0下的服務相關聯的跟蹤器僅有的兩種可能的操作（啟用/禁用），因此不能再調整其他引數（如閾值、多路複用器、間隔）。此處使用的探測型別是ICMP回應請求資料包。

要瞭解有關服務插入1.0跟蹤的詳細資訊，請訪問配置指南。服務插入1.0跟蹤中使用的預設間隔為：

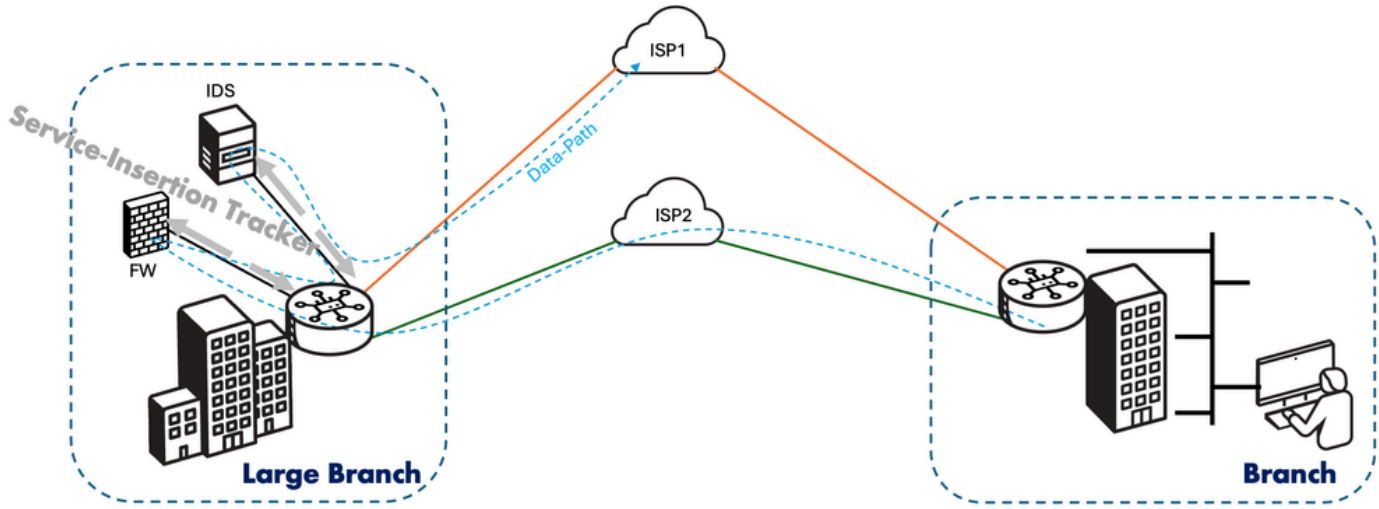
- 探測間隔：每60秒5次探測
- 乘數：5次
- 資料包/探測型別：ICMP Echo/Echo-reply

Service Fabric 2.0跟蹤是Cisco Catalyst SD-WAN中從20.13/17.13版本開始推出的服務插入2.0功能的一部分。在此服務插入的新變體中，配置檔案和模板使用的預設方法仍是讓隱式跟蹤器指向每個rx/tx介面的服務HA對中的每個已定義服務地址（或轉發地址）。但是，使用Service Fabric 2.0，您

現在可以從跟蹤地址中拆分轉發地址。這可以通過定義單獨的端點跟蹤器來跟蹤與服務地址本身不同的端點地址來實現。本主題將在下一節中進一步擴展。

使用案例

服務跟蹤器的主要用例是可擴展地監控服務可達性，尤其是服務鏈的可達性。服務連結可以部署在包含多個VPN的網路中，其中每個VPN代表不同的功能或組織，以確保VPN之間的流量通過防火牆。例如，在大型園區網路中，部門間流量可以通過防火牆，而部門內部流量可以直接路由。在運營商必須滿足合規性的情況下，例如支付卡行業資料安全標準(PCI DSS),PCI流量必須流經集中式資料中心或區域中心的防火牆時，可以發現服務鏈：



組態

這些配置與在SD-WAN上設定Service Insertion 1.0的正常工作流程相同。預設情況下，將在所有服務地址上啟用Service Insertion 1.0 Tracker。

- 配置組：Configuration > Configuration Groups > Service Profile > Service VPN > Service部分：

1.按一下Add Service按鈕。

2.選擇服務型別。

3.登記服務地址（最多4個，用逗號分隔）。

4.驗證「跟蹤」旋鈕是否已啟用（預設）。 如果需要，可以禁用此功能。

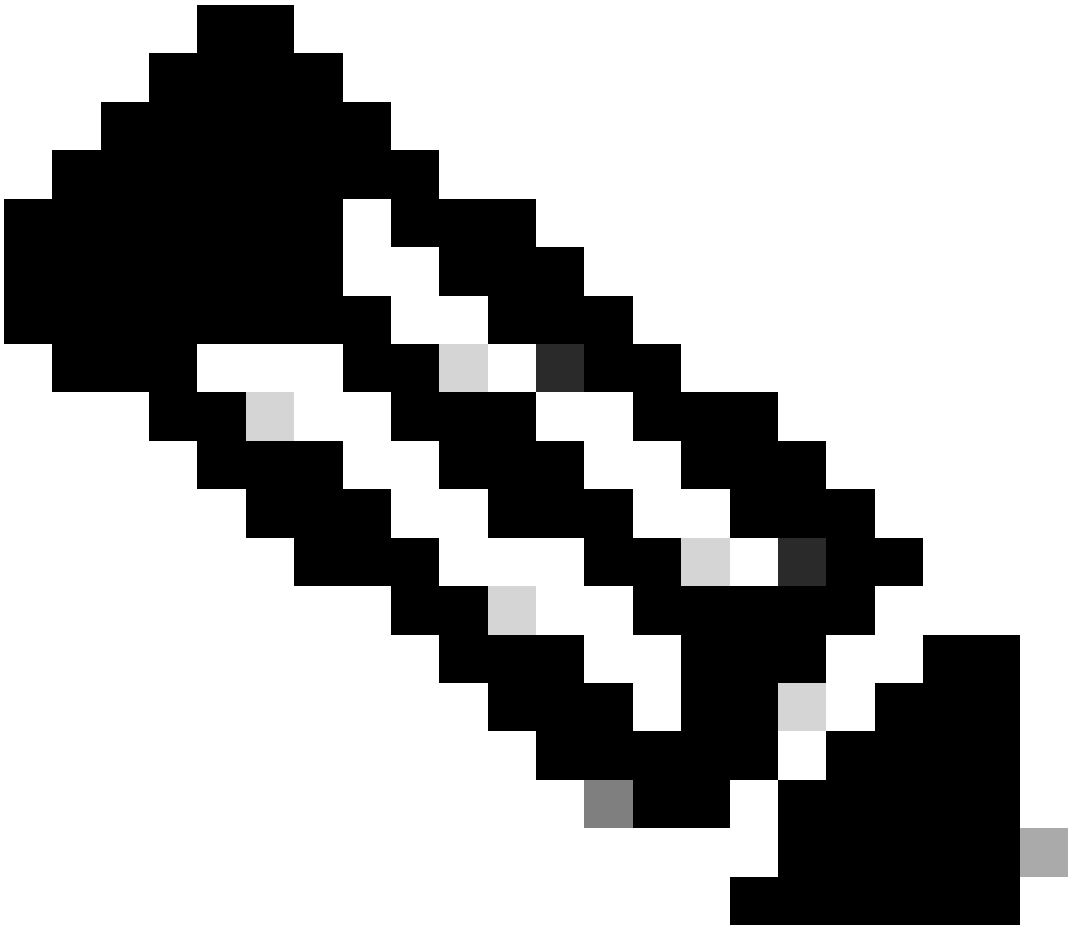
- 舊配置：Configuration > Templates > Feature Templates > Cisco VPN(service)> Service部分：

1.按一下「新建服務」按鈕

2.選擇服務型別。

3.登記服務地址（最多4個，用逗號分隔）。

4.驗證「跟蹤」旋鈕是否已啟用（預設）。 如果需要，可以禁用此功能。



附註：在配置步驟3時（從配置組或舊版配置），跟蹤器會自動啟動到各種定義的服務地址

從CLI的角度來看，Service Insertion 1.0的配置如下所示：

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

驗證

驗證步驟擴展為前面部分中使用的基於介面的端點跟蹤器中的類似步驟。

顯式配置的終端跟蹤器有兩個驗證選項。

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

在Individual Tracker下檢查並根據配置的跟蹤器名稱檢視跟蹤器的統計資訊（跟蹤器型別、狀態、端點、端點型別、VPN索引、主機名、往返時間）。

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

如果在跟蹤器上檢測到翻動，相應的日誌將填充在此部分中的詳細資訊，如主機名、連線點名稱、跟蹤器名稱、新狀態、地址系列和vpn id。

在邊緣的CLI上：

```
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
```

適用於DIA的介面終端追蹤器

NAT DIA終端跟蹤器跟蹤器主要用於通過SD-WAN邊緣平台上的NAT DIA介面監控應用的可達性。

對於直接網際網路接入(Direct Internet Access， DIA)使用案例，NAT DIA跟蹤器主要用於跟蹤傳輸端介面，並觸發到另一個可用傳輸端介面的故障切換，或通過SD-WAN重疊隧道（使用資料策略）觸發故障切換。 此功能是從20.3/17.3版本開始引入的，而NAT回退功能選項則從20.4/17.4版本開始提供。如果跟蹤器確定本地網際網路無法通過NAT DIA介面使用，則路由器將從服務VPN撤消NAT路由，並根據本地路由配置重新路由流量。跟蹤器將繼續定期檢查到介面的路徑的狀態。當路由器檢測到該路徑再次正常運行時，會重新安裝通往Internet的NAT路由。要瞭解有關DIA跟蹤器的詳細信息，請訪問配置指南。

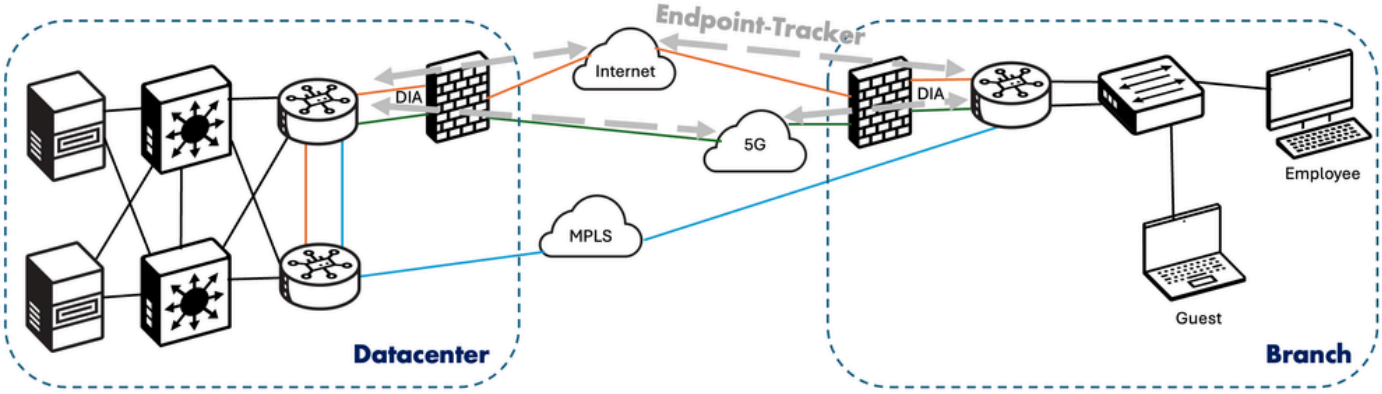
在跟蹤器定義中，您可以選擇為通過NAT DIA介面可訪問的終端提供IP地址（配置為「endpoint-ip」），或者為終端提供完全限定域名(FQDN)（配置為「endpoint-dns-name」）。

此處使用的探測器型別是HTTP請求資料包，非常類似於HTTP API請求PDU堆疊。使用的間隔為：

- 探測間隔：60秒
- 乘數：180秒(因為#retries是3 = 3 x 60秒)
- 資料包/探測型別：HTTP

使用案例

DIA通常作為最佳化部署在分支站點，以避免將任何目的地為網際網路的分支流量回送到資料中心。儘管如此，當使用分支站點中的DIA時，沿NAT DIA路由的任何不可達性仍必須回退到備用路徑，以避免黑屏和失去服務。適用於當本地DIA分支發生故障時，希望使用回退到DC的站點（通過SD-WAN重疊使用NAT回退）。在分支端邊緣支援DIA的介面上利用這些基於介面的終端跟蹤器來檢測故障，以啟動到備份/DC路徑的故障切換。通過這種方式，實現了網際網路服務的高可用性，在企業中實現了最小的中斷，同時仍然使用DIA最佳化網際網路流量：



組態

必須手動配置這些基於介面的終端跟蹤器才能啟用此功能集。以下是設定方法，具體取決於使用者首選的設定方法型別。

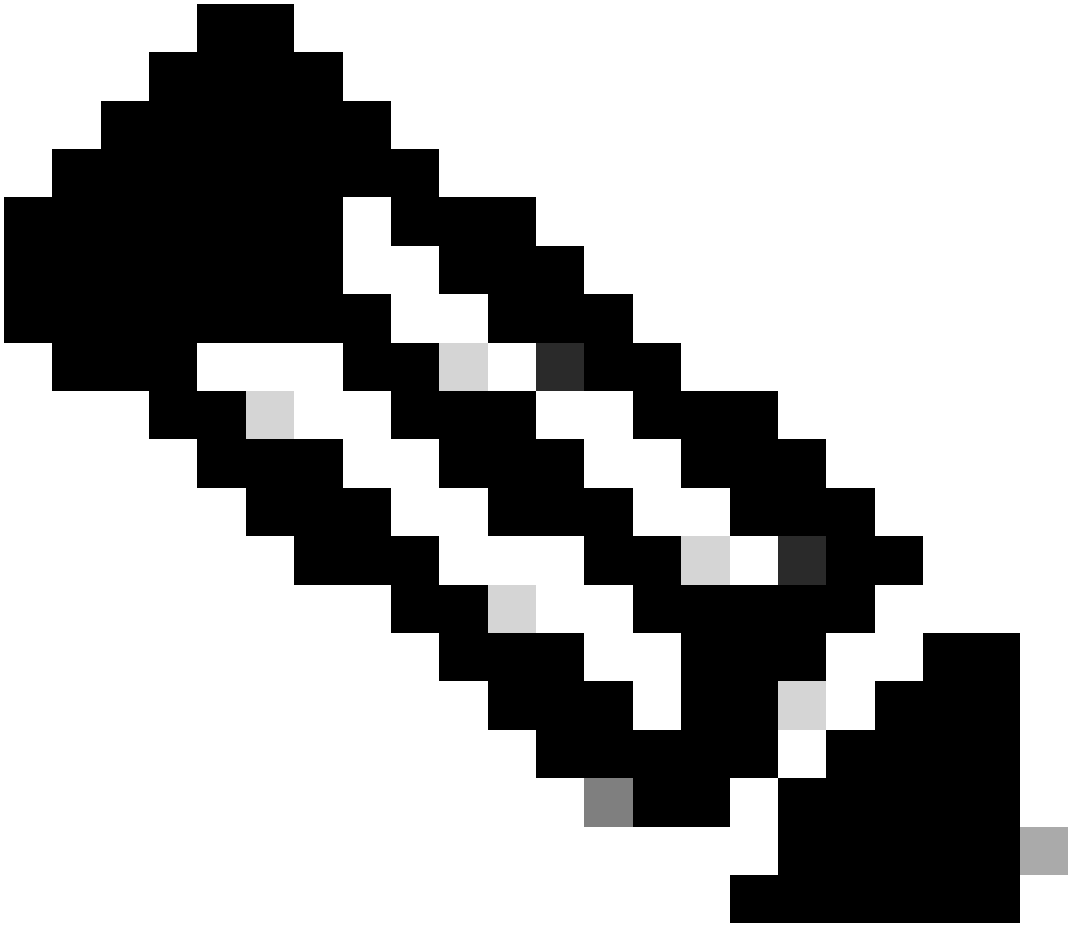
- 配置組：Configuration > Configuration Groups > Transport & Management Profile > Ethernet Interface > Add Feature > Tracker:

1.定義端點跟蹤器名稱。

2.選擇終端跟蹤器型別（在HTTP預設和ICMP之間）。

附註：自20.13/17.13發行以來引入了ICMP終端跟蹤器型別。

3.選擇終端（在終端IP預設和終端DNS名稱之間）。



附註：如果選擇終端DNS名稱，請確保使用傳輸VPN配置配置檔案在傳輸VPN/VRF下定義有效的DNS伺服器或名稱伺服器。

4.輸入必須向其傳送跟蹤器探測器的地址或DNS名稱(FQDN)（格式取決於上一步驟）。

5.（可選）您可以選擇更改「探測時間間隔」（預設值= 60秒）和「重試次數」（預設值= 3次），以加快故障檢測時間。

- 舊配置:

步驟1.基於介面的終端跟蹤器的定義：Configuration > Templates > Feature Templates > System template > Tracker部分：

1.在「跟蹤器」子部分下，選擇New Endpoint Tracker按鈕。

2.定義終端跟蹤器名稱。

3.選擇Tracker Type（介於介面預設和靜態路由之間）作為介面，因為DIA使用案例在此是需要考慮

的。

4.選擇Endpoint Type（在IP Address-default和DNS Name之間）。

5.輸入必須將跟蹤器探測器傳送到的終端IP地址或終端DNS名稱（格式取決於上一步驟）。

6.（可選）您可以選擇更改探測閾值（預設值= 300毫秒）、間隔（預設值= 60秒）和多路器（預設值= 3次）。

步驟2.將基於介面的終端跟蹤器應用到傳輸VPN上的介面： Templates > Feature Templates > Cisco VPN Interface Ethernet > Advanced部分：

1.在Tracker（跟蹤器）欄位中輸入在前步驟1中定義的終端跟蹤器名。

從CLI的角度來看，配置如下所示：

```
(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
!
```

驗證

顯式配置的終端跟蹤器有兩個驗證選項。

- 在SD-WAN管理器上：Monitor > Devices > {select Device-Name} > Applications > Tracker:

在Individual Tracker下檢查並根據配置的跟蹤器名稱檢視跟蹤器的統計資訊(跟蹤器類型、狀態、端點、端點型別、VPN索引、主機名、往返時間)。

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

如果在跟蹤器上檢測到翻動，相應的日誌將填充在此部分中的詳細資訊，如主機名、連線點名稱、跟蹤器名稱、新狀態、地址系列和vpn id。

在邊緣的CLI上：

```
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
```

適用於SIG通道/SSE的介面終端追蹤器

當終端跟蹤器用於SIG隧道/SSE使用案例時，主要表明企業正在尋找基於雲的安全堆疊產品，現今可通過安全網際網路網關(SIG)或安全服務邊緣(SSE)提供商（例如Cisco、Cloudflare、Netskope、ZScalar等）輕鬆獲得這些產品。SIG隧道和SSE均作為雲安全部署模式的一部分，其中分支機構使用雲提供其所需的必要安全解決方案。SIG隧道使用案例是將Cisco Catalyst SD-WAN與這些SIG提供商整合（從20.4/17.4版本開始）的初始產品，但是隨著雲交付安全產品的發展，SSE使用案例（從20.13/17.13版本開始）被引入，用於覆蓋思科（通過思科安全訪問）和ZScalar等提供商的使用案例。

IT需要一種可靠且明確的方法來保護和靈活地連線。現在，為遠端員工提供直接訪問雲應用（如Microsoft 365和Salesforce）的常見做法是提供額外的安全性。隨著承包商、合作夥伴、物聯網

(IoT)裝置等需要網路訪問，對雲交付的網路和安全性的需求每天都在增長。在雲邊緣，網路和安全功能與終端裝置相融合，稱為服務模型Cisco SASE。Cisco SASE結合了雲提供的網路和安全功能，可為所有使用者或裝置提供隨時隨地的安全應用程式訪問。安全服務邊緣(SSE)是一種網路安全方法，可幫助組織改善其工作環境的安全狀態，同時降低終端使用者和IT部門的複雜性。要瞭解有關SIG隧道/SSE跟蹤器的詳細資訊，請訪問配置指南。

使用案例

這種基於介面的端點跟蹤器用於這樣的SIG隧道/SSE使用案例，其中您要跟蹤公認的SaaS應用URL端點或關注的特定URL端點。現在，SSE是比較常用的場景，因為SASE架構被分為SSE核心功能和SD-WAN功能。然後，您需要在從站點建立的IPSec隧道內（在本例中為DC）選擇活動角色和備用角色。 使用者可以選擇在相應的隧道介面下連線跟蹤器。

對於SSE提供商，例如Cisco Secure Access（由Cisco提供） — 使用預設配置的隱式終端跟蹤器。但是，使用者確實可以選擇建立自定義終端跟蹤器並將該跟蹤器連線到IPSec隧道介面。SSE中使用的預設/隱式終結點跟蹤器的引數為：

對於Cisco SSE:

跟蹤器名稱：預設跟蹤器

正在跟蹤的終結點：http://service.sig.umbrella.com

終端型別：API_URL

閾值：300毫秒

倍數：3

Interval:60秒

對於ZScaler SSE:

跟蹤器名稱：預設跟蹤器

正在跟蹤的終結點：http://gateway.zscalerthree.net/vpnte

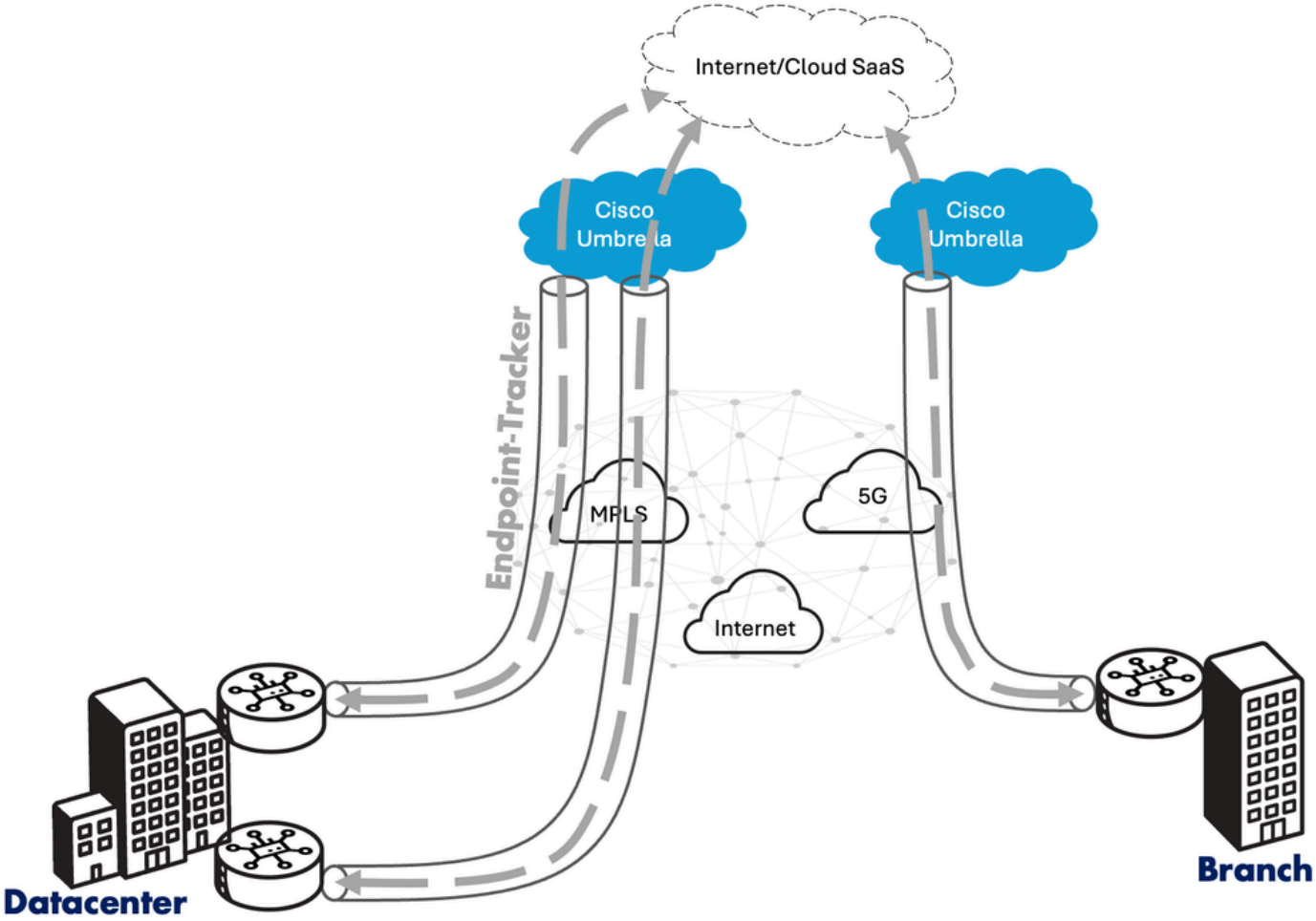
終端型別：API_URL

閾值：300毫秒

乘數：3

Interval:60秒

對於SIG隧道，未定義預設/隱式端點跟蹤器。因此，如果使用者想要向SIG提供商雲跟蹤IPSec隧道介面，則必須手動配置基於介面的終端跟蹤器：



組態

在SSE提供商的情況下，使用者不必明確定義任何終端跟蹤器（除非需要）。 但是，工作流程因配置型別而異。

作為前提條件，您必須定義SIG/SSE憑證管理>設定>外部服務>雲憑證:

1.在Cloud Provider Credentials下，切換Umbrella或Cisco SSE（或同時切換）選項。

2.定義引數，如組織ID、API金鑰、密鑰)。

Set configuration group Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge:

1.按一下Add Secure Internet Gateway或Add Secure Service Edge。

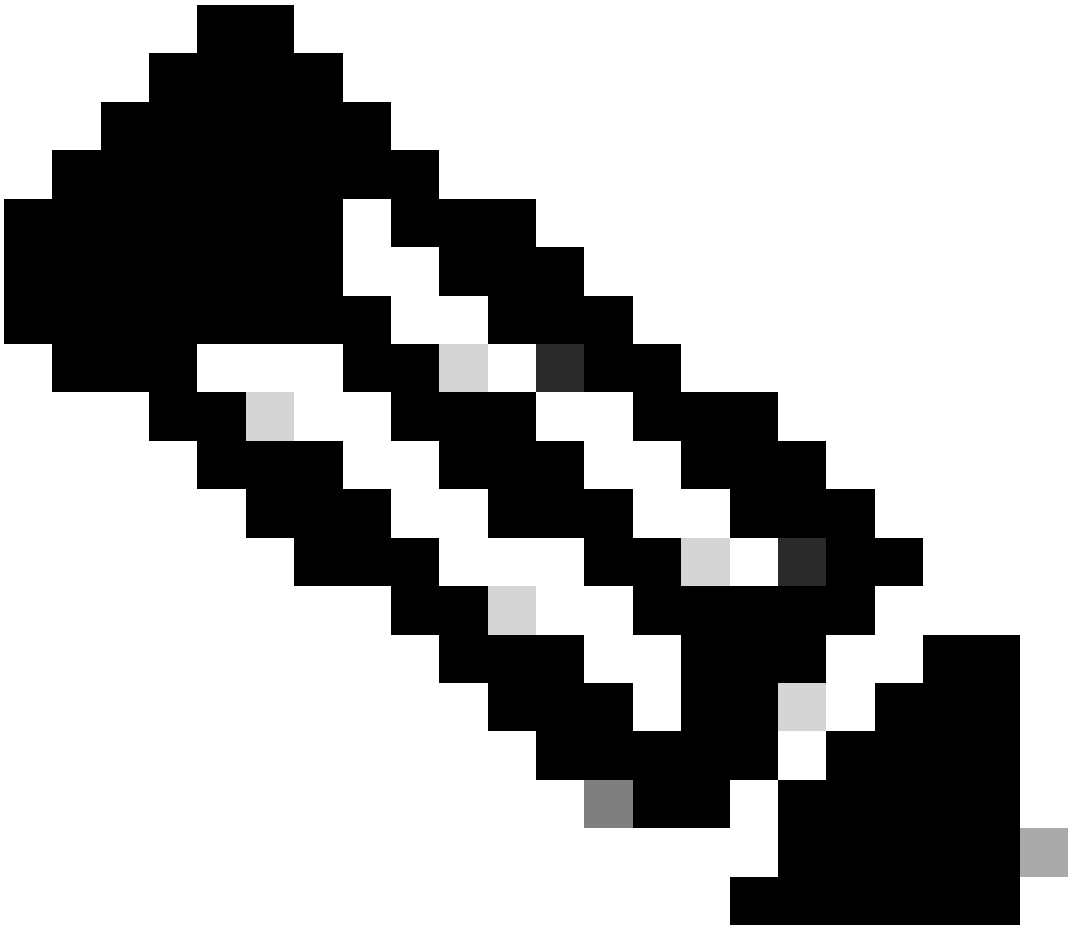
2.定義名稱和說明。

3.選擇SIG/SSE Provider（SIG/SSE提供商）(Umbrella或Cisco SSE)下的單選按鈕。

4.在跟蹤器部分下，定義用於為跟蹤器探測器提供源的源IP地址。

5.如果選擇定義顯式/自定義端點跟蹤器，請按一下新增跟蹤器，然後填寫端點跟蹤器的引數(名稱、端點的API URL、閾值、探測間隔和乘數)。

6.在配置部分下，建立可以定義引數(如介面名稱、說明、跟蹤器、隧道源介面、資料中心主/輔助)的隧道介面。



附註：在步驟6中，使用者可選擇將定義的終端跟蹤器連線到各自的IPSec隧道。請注意，這是一個可選欄位。

7.在高可用性部分下，建立介面對並定義活動介面和備份介面及其各自的權重。然後將前面配置的策略組應用到相關邊緣。

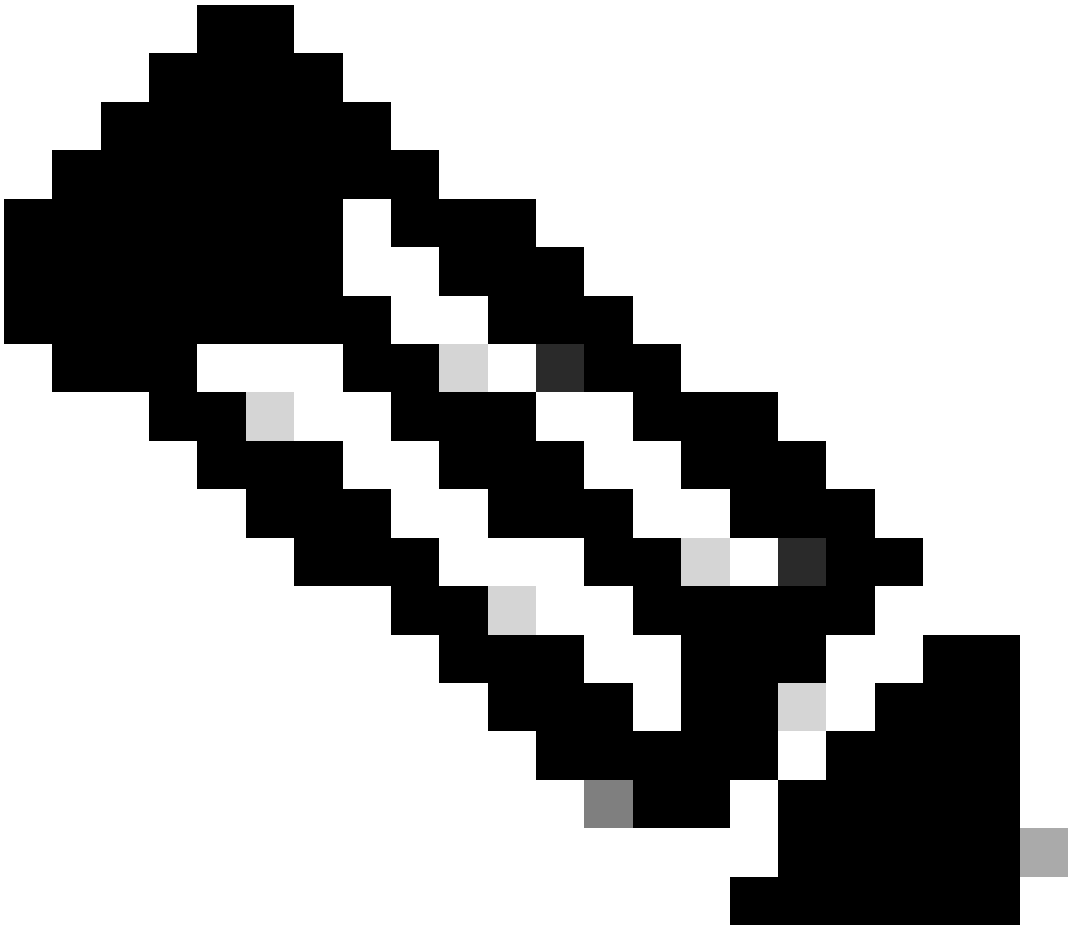
設定舊配置配置>模板>功能模板>Cisco Secure Internet Gateway功能模板：

1.選擇SIG Provider（SIG提供商）下的單選按鈕之一（Umbrella、ZScalar或Generic）。

2.在「跟蹤器(BETA)」部分下，定義用於源跟蹤器探測的源IP地址。

5.如果選擇定義顯式/自定義端點跟蹤器，請按一下「新跟蹤器」，然後填寫端點跟蹤器的引數(名稱、端點的API url、閾值、間隔和乘數)。

6.在「配置」部分下，建立隧道介面(通過按一下新增隧道)，您可以在其中定義引數(例如介面名稱、說明、跟蹤器、隧道源介面、資料中心主/輔助)。



附註：在步驟6中，使用者可選擇將定義的終端跟蹤器連線到各自的IPSec隧道。請注意，這是一個可選欄位。

7.在高可用性部分下，定義活動介面和備份介面及其各自的權重。

從CLI的角度來看，配置如下所示：

```
(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
!
```

驗證

存在顯式配置的終端跟蹤器的驗證選項。

- 在SD-WAN管理器上：Monitor > Devices > {select Device-Name} > Applications > Tracker:

在Individual Tracker下檢查並根據配置的跟蹤器名稱檢視跟蹤器的統計資訊（跟蹤器型別、狀態、端點、端點型別、VPN索引、主機名、往返時間）。

- 在SD-WAN管理器上：Monitor > Devices > {select Device-Name} > Events:

如果在跟蹤器上檢測到翻動，相應的日誌將填充在此部分中的詳細資訊，如主機名、連線點名稱、跟蹤器名稱、新狀態、地址系列和vpn id。

在邊緣的CLI上：

```
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
```

適用於服務光纖2.0的介面終端追蹤器

Service Fabric 2.0跟蹤是在20.13/17.13版中引入的，是服務插入1.0跟蹤的增強型變體 — 其中使用者可以在更大程度上自定義跟蹤器。預設行為保留自以前版本的Service Insertion(1.0)，在預設情況下，會根據每個rx/tx的服務HA對中每個服務地址（或轉發地址）的定義啟動跟蹤器。但是在Service Insertion 2.0中，跟蹤地址（跟蹤的IP/端點）可以與轉發地址（通常是服務地址）分離。這是使用VPN級別上定義的自定義終端跟蹤器完成的。要瞭解有關Service Fabric 2.0跟蹤器的詳細資訊，請訪問配置指南。

如果使用者選擇使用預設跟蹤器，則跟蹤器探測的規範為：

- 您好：每30秒1次探測
- 乘數：3次
- 資料包/探測型別：ICMP Echo/Echo-reply

如果使用者選擇使用自定義跟蹤器，則跟蹤器探測的規範為：

- 您好：每60秒1次探測
- 乘數：3次
- 資料包/探測型別：ICMP Echo-request/reply

使用案例

前面部分中提到的服務插入1.0用例也在這裡適用。

組態

支援Service Insertion 2.0基於工作流的配置，這是一種嚮導引導的方法，有助於簡化使用者體驗，同時遵守標準Configuration組工作流程步驟。

1.在配置>服務插入>服務鏈定義部分下定義「服務鏈 — 配置」組：

a.按一下Add Service Chain Definition按鈕。

b.填寫服務的名稱和說明的詳細資訊。

c.填寫清單格式（通過從下拉選單中選擇）Service Type。

2.在Configuration > Service Insertion > Service Chain Configurations部分下定義「服務鏈例項 — 配置」組：

a.按一下Add Service Chain Configuration。

b.在「服務鏈定義」步驟中，選擇標題為選擇現有的單選按鈕，然後選擇先前定義的服務。

c.提供啟動服務鏈配置步驟的名稱和說明。

d.在Service Chain Configuration for Manually Connected Services步驟中，選擇Service Chain VPN-ID。

e.然後，對於服務鏈例項中定義的每個服務（在子頁籤中表示），在服務詳細資訊下提供連線型別（IPv4、IPv6或隧道連線）。

f.選中Advanced覈取方塊。如果您需要具有active-backup/HA使用案例(同時啟用Add parameters for Backup命令)，或者即使您需要定義自定義終端跟蹤程式（同時啟用Custom Tracker命令）。

g.如果您遇到這樣的情況：出口(tx)流量通過一個介面流向服務，而來自服務的返回流量通過另一個介面進入(rx)，則開啟Traffic from service is received on a different interface switchon。

h.啟用Advanced 和Custom Tracker旋鈕後，定義服務IPv4地址（轉發地址）、SD-WAN路由器介面（服務所連線到的）和跟蹤器終端（跟蹤地址）。 您還可以修改自定義跟蹤器引數，如間隔和乘數（通過按一下「編輯」按鈕）。

i.對每個後續定義的服務重複步驟(e)、(f)、(g)和(h)。

3.將Service Chain Instance連線到Configuration > Configuration Groups > Service Profile > Service VPN > Add Feature > Service Chain Attachment Gateway下邊緣 — 配置組的配置配置檔案：

a.為此服務鏈附件網關包提供名稱和說明。

b.選擇先前定義的服務鏈定義（在步驟1中）。

c.重新新增/驗證步驟2中執行的詳細資訊。對於跟蹤器定義，與前一步驟的唯一區別是，您有機會指定跟蹤器名稱，並選擇跟蹤器型別（從service-icmp到ipv6-service-icmp）。

從CLI的角度來看，配置如下所示：

```
!
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
!
```

驗證

- 在SD-WAN管理器的Monitor > Devices > {select Device-Name} > Applications > Tracker上:

在Individual Tracker下檢查並根據配置的跟蹤器名稱檢視跟蹤器的統計資訊（跟蹤器型別、狀態、端點、端點型別、VPN索引、主機名、往返時間）。

- 在SD-WAN ManagerMonitor > Devices > {select Device-Name} > Events上:

如果在跟蹤器上檢測到翻動，相應的日誌將填充在此部分中的詳細資訊，如主機名、連線點名稱、跟蹤器名稱、新狀態、地址系列和vpn id。

在邊緣的CLI上：

```
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
```

用於靜態路由跟蹤的靜態路由終端跟蹤器（服務端）

第二種型別的端點跟蹤器被稱為基於靜態路由的端點跟蹤器。如名稱本身所示，這些型別的跟蹤器主要用於跟蹤服務端VPN下定義的任何靜態路由的下一跳地址。預設情況下，所有「已連線」和「靜態」路由型別都通告到OMP協定中，包含相應服務VPN的所有遠端站點都在該協定後知道該目的地字首（其中下一跳指向始發站點的TLOC）。 始發站點是從其發起特定靜態路由的站點。

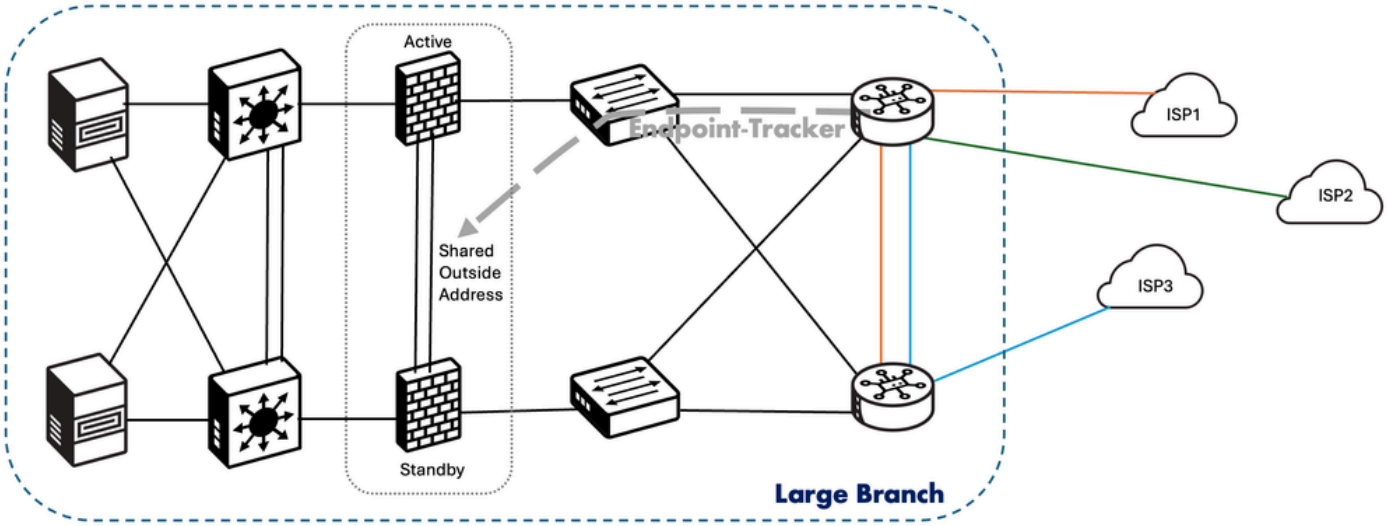
但是，如果靜態路由中的下一跳地址無法訪問，該路由不會停止通告到OMP中。這將導致流向源站點的流量被黑洞。這就需要將跟蹤器連線到靜態路由，以確保僅當下一跳地址可到達時才將靜態路由通告到OMP中。20.3/17.3版為基本IP地址型別基於靜態路由的終端跟蹤器引入了此功能。從20.7/17.7版本起，新增了對僅向下一跳IP地址的特定TCP或UDP埠傳送跟蹤器探測功能的支援(在使用防火牆僅開啟某些埠進行跟蹤的情況下)。要瞭解有關靜態路由跟蹤器的詳細資訊，請訪問配置指南。

此處使用的探測器型別是簡單的ICMP回應請求資料包。使用的間隔為：

- 您好：60秒
- 保持時間：180秒(因為#retries是3 = 3 x 60秒)
- 資料包/探測型別：ICMP Echo/Echo-reply

使用案例

這種基於靜態路由的終端跟蹤器用於服務端跟蹤靜態路由中的下一跳地址。其中一個常見場景是跟蹤與一對主用/備用防火牆對應的LAN端下一跳地址，這些防火牆共用基於外部IP地址的外部，外部介面根據此地址扮演「主用」防火牆的角色。在防火牆規則似乎非常嚴格（只為基於使用案例的目的開啟某些埠）的情況下，靜態路由跟蹤器可用於跟蹤特定TCP/UDP埠到屬於LAN端防火牆外部介面上的下一跳IP地址。



組態

必須手動配置這些基於靜態路由的終端跟蹤器才能啟用此功能集。以下是設定方法，具體取決於使用者首選的設定方法型別。

- 配置組配置>配置組>服務配置檔案>服務VPN>新增功能>跟蹤器:

1.為正在定義的新（端點）跟蹤器提供名稱、說明和跟蹤器名稱。

2.選擇終端型別，具體取決於您是需要僅跟蹤下一跳IP地址（選擇「地址」單選按鈕），還是甚至特定TCP/UDP埠（選擇「協定」單選按鈕）。

3.以IP地址格式輸入地址。如果在上一步中選擇了Protocol作為終端型別，請輸入協定（TCP或UDP）和埠號。

4.如果需要，您可以更改探測間隔、重試次數和延遲限制的預設值。

- Configuration > Configuration Groups > Service Profile > Service VPN > Route部分：

1.選擇Add IPv4/IPv6 Static Route按鈕。

2.填寫詳細資訊，如網路地址、子網掩碼、下一跳、地址、AD。

3.按一下Add Next Hop With Tracker按鈕。

4.重新輸入下一跳地址AD，然後從下拉選單中選擇先前建立的（終端）跟蹤器名稱。

- Legacy configuration Configuration > Templates > Feature Templates > System Template > Tracker部分：

1.選擇「新建端點跟蹤器」按鈕。

2.為正在定義的新（端點）跟蹤器提供名稱。

3.將Tracker Type單選按鈕更改為static-route。

4.選擇終端型別，作為下一跳IP地址（選擇「IP地址」單選按鈕）。

5.以IP地址格式輸入終端IP。

6.如果需要，您可以更改探測間隔、重試次數和延遲限制的預設值。

- Configuration > Templates > Feature Templates > Cisco VPN(Service-side ONLY)> IPv4/IPv6 Route部分：

1.選擇New IPv4/IPv6 Route按鈕。

2.填寫詳細資訊，如字首、網關。

3.按一下Add Next Hop With Tracker 按鈕。

4.重新輸入下一跳地址AD（距離），並手動輸入先前建立的（終端）跟蹤器名稱。

從CLI的角度來看，配置如下所示：

```
(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
!
```

驗證

對明確配置的終端跟蹤器有兩個驗證區域。

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

1.在Device Options下，鍵入「Endpoint Tracker Info」。

2.在Individual Tracker(Attach Point Name)下檢查，並根據配置的跟蹤器名稱檢視跟蹤器的統計資訊(Tracker State、Associated Tracker Record Name、從裝置到終端的mx延遲、上次更新時間戳)。

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

如果在跟蹤器上檢測到翻動，相應的日誌將填充在此部分中的詳細資訊，如主機名、連線點名稱、跟蹤器名稱、新狀態、地址系列和vpn id。

在邊緣的CLI上：

```
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 Tra


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]
```

用於VRRP跟蹤的介面對象跟蹤器

對象跟蹤器是為自主模式消耗（使用案例）設計的跟蹤器。 這些跟蹤器的使用案例從基於VRRP的介面/隧道跟蹤到服務VPN NAT跟蹤不等。

對於VRRP跟蹤使用案例,VRRP狀態根據隧道鏈路狀態確定。如果主VRRP上的隧道或介面關閉，流量將定向到輔助VRRP。LAN網段中的輔助VRRP路由器成為主要VRRP，為服務端流量提供網關。此使用案例僅適用於service-VPN，並且有助於在SD-WAN重疊（SSE情況下為介面或隧道）發生故障時在LAN端對VRRP角色進行故障轉移。 要將跟蹤器附加到VRRP組，只能使用對象跟蹤器（而非終端跟蹤器）。 此功能是從Cisco Catalyst SD-WAN邊緣的20.7/17.7版本引入的。

跟蹤器此處未使用任何探測器。相反，它使用線路協定狀態來決定跟蹤器狀態（開啟/關閉）。 在基

於介面線路協定的跟蹤器中沒有反應間隔 — 當介面/隧道線路協定關閉時，跟蹤狀態也會變為DOWN狀態。然後，根據關閉或減少的操作，VRRP組將相應地重新收斂。要瞭解有關VRRP介面跟蹤器的詳細資訊，請訪問配置指南。

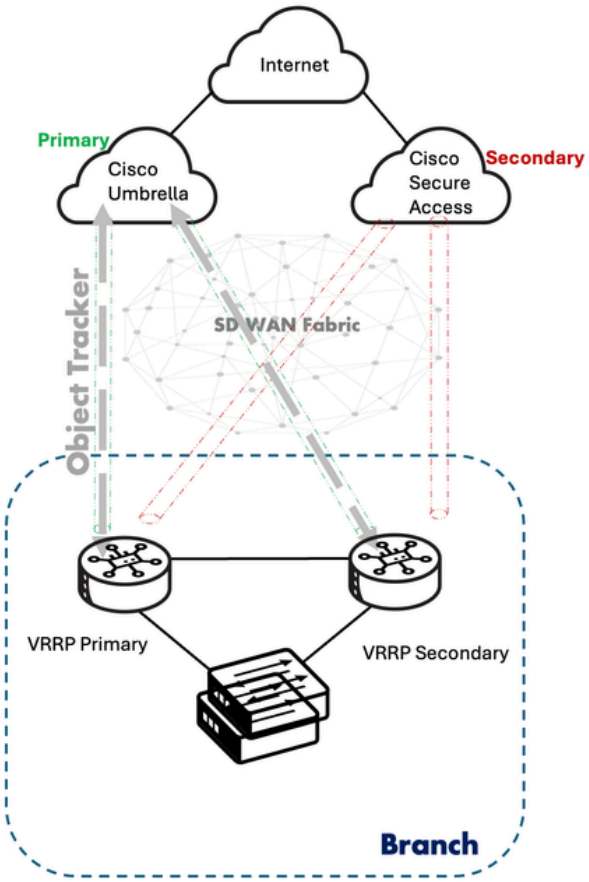
使用案例

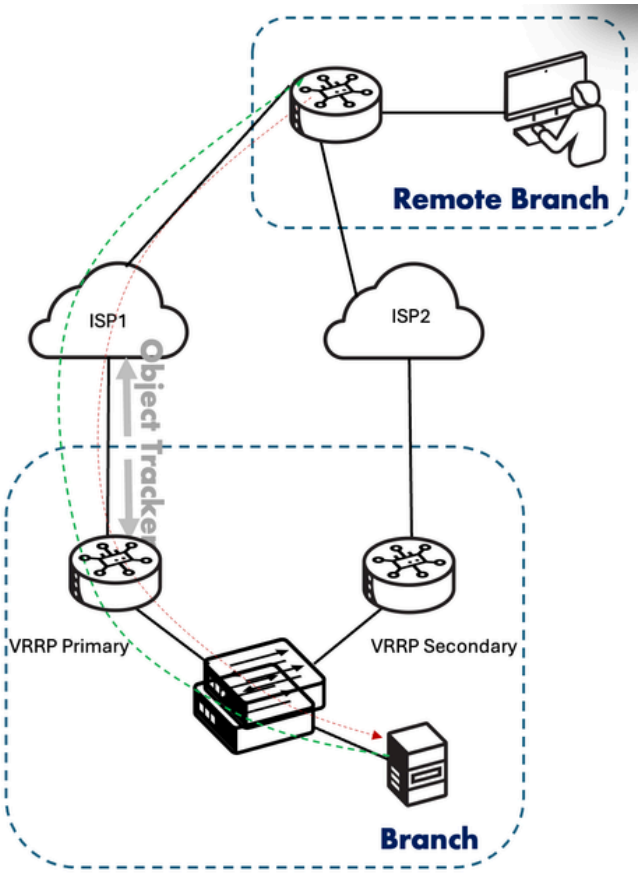
基於實施基於VRRP的介面跟蹤所需的標準，存在多個使用案例。目前，支援的兩種模式是(i)介面（指與本地TLOC繫結的任何隧道介面）或(ii)SIG介面（與SIG隧道介面相關）。 在每種情況下，被跟蹤的部分都是介面線路協定。

帶網際網路的雙路由器:跟蹤對象繫結到VRRP組。在跟蹤器的對象（在這種情況下是SIG隧道介面）關閉的情況下，這將通知VRRP主路由器觸發從主路由器到備份的狀態轉換，並通知備份路由器成為主路由器。此狀態更改可以通過兩種型別的操作來影響或觸發：

1. 遞減：其中，在軌道對象狀態從UP轉變到DOWN的情況下，用於在其上配置VRRP VIP的介面的VRRP優先順序被減少或減少某個值。
2. 關機:這是一種方法，在軌跡對象狀態從UP轉變為DOWN時，VRRP進程在應用的介面上關閉。在有非對稱轉發例項的使用案例中，不建議使用此方法。

TLOC更改首選項：為避免來自其他SDWAN站點的非對稱流量進入在服務VPN上運行VRRP的站點，如果已配置VRRP主路由器的TLOC首選項，則其提升為1。您甚至可以在配置組下修改此值。這可確保VRRP主路由器本身能夠吸引從WAN到LAN的流量。從LAN到WAN的流量被VRRP主節點的VRRP機制吸引。此功能與VRRP介面跟蹤器無關。從CLI角度來看，這是一個可選命令(tloc-change-pref)。





組態

對象跟蹤器的配置通過舊版配置中的系統模板完成，然後隨後在服務 — VPN乙太網介面功能模板下將對象跟蹤器連線到各自的VRRP組。在配置組中，通過直接獲取將對象跟蹤器新增到相應服務配置檔案乙太網介面配置檔案的選項，已簡化了此機制。以下是配置它的方法，具體取決於使用者首選的配置方法型別。

- 配置組配置>配置組>服務配置檔案>乙太網介面>新增功能>對象跟蹤器:

1. 為正在定義的新對象跟蹤器提供名稱和說明。
2. 選擇Tracker Type(在Interface和SIG之間)。
3. 分配對象跟蹤器ID。
4. 提供介面名稱（取決於步驟2中選擇的選項）。

- Configuration > Configuration Groups > Service Profile > Ethernet Interface > VRRP部分：

1. 在「IPv4設定」下，按一下Add VRRP IPv4。
2. 定義VRRP組ID並為此服務端乙太網介面提供本地優先順序。
3. 提供VRRP虛擬IP(VIP)地址。
4. 啟用TLOC Preference Change按鈕並提供TLOC Preference Change Value（處理非對稱路由）。
5. 按一下新增VRRP跟蹤對象。
6. 在Associate Object Tracker下，從之前建立的Object Tracker(基於Name)下拉選單中選擇
7. 選擇跟蹤器操作(Shutdown或Decrement)。
8. 輸入遞減值值（取決於在步驟7中選擇的選項）。

- Legacy configuration Configuration > Templates > Feature Templates > System > Tracker部分：

1. 按一下New Object Tracker按鈕。
2. 選擇Tracker Type(在Interface和SIG之間)。
3. 分配對象ID。
4. 提供介面名稱（取決於步驟2中選擇的選項）。

- Configuration > Templates > Ethernet Interface（屬於服務端）> VRRP部分：

1. 按一下New VRRP按鈕。
2. 定義VRRP組ID並為此服務端乙太網介面提供本地優先順序（可選，預設值為100）。
3. 提供VRRP虛擬IP(VIP)地址。
4. 啟用TLOC Preference Change按鈕並提供TLOC Preference Change Value（處理非對稱路由）。
5. 在「對象跟蹤器」下，按一下新增跟蹤對象。
6. 輸入對象跟蹤器ID（在系統模板下定義）。
7. 選擇跟蹤器操作(Shutdown或Decrement)。
8. 輸入遞減值值（取決於在步驟7中選擇的選項）。

從CLI的角度來看，配置如下所示：

```
(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
!
```

驗證

有兩個選項可用於驗證針對VRRP使用案例顯式配置的對象跟蹤器。

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

1.在Device Options下，鍵入「VRRP Information」。

2.在單個VRRP組（組ID）下檢查，並根據配置的對象跟蹤者ID檢視跟蹤者的統計資訊(跟蹤字首名

稱、跟蹤狀態、不連續時間和上次狀態更改時間)。

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

如果在對象跟蹤器上檢測到狀態更改，則與其連線的相應VRRP組會更改其狀態。相應的日誌將填充在此部分（名稱顯示為Vrrp組狀態更改），並帶有詳細資訊，如主機名、if編號、grp id、addr型別、if name、vrrp group-state、state change-reason和vpn id。

在邊緣的CLI上：

```
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)
```

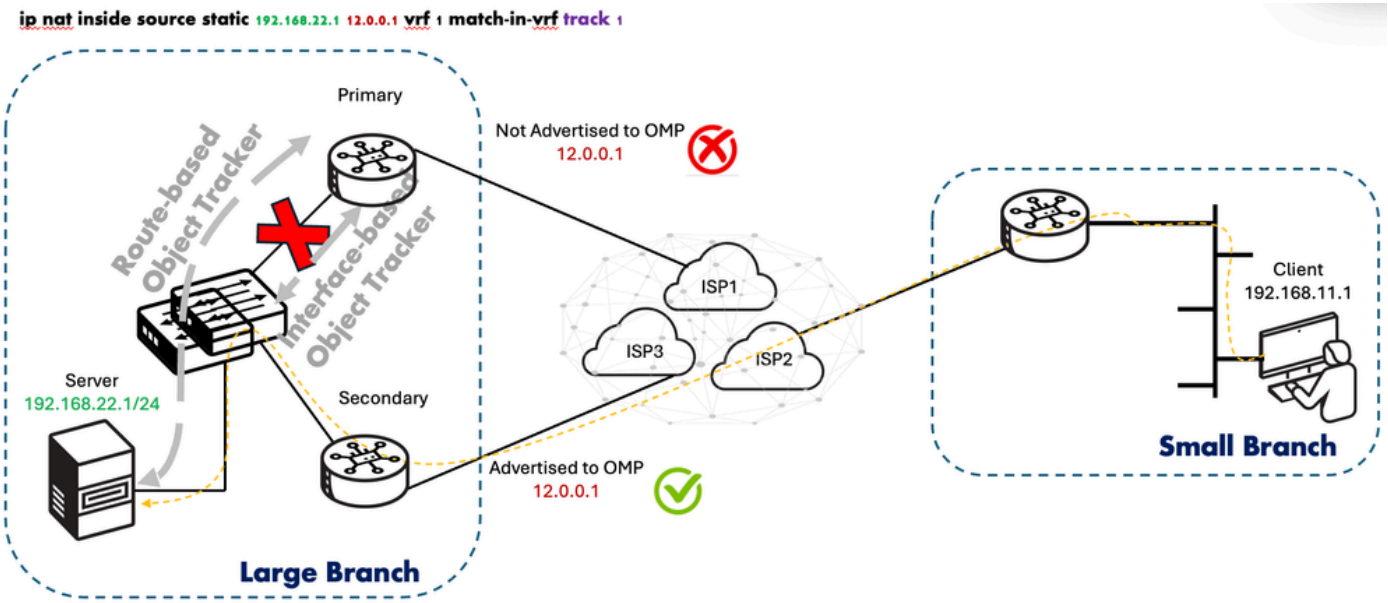
用於服務VPN NAT跟蹤的介面/路由對象跟蹤器

服務端NAT對象跟蹤器是20.8/17.8版中引入的一項功能，其中服務VPN NAT中使用的內部全域性地址（內部靜態NAT和內部動態NAT）僅在(i)發現內部本地地址可訪問或(ii)LAN/服務端介面的線路協定根據連線的對象跟蹤器為UP的情況下才通告到OMP中。因此，可以使用的對象跟蹤器型別是(i)路由或(ii)介面。根據LAN字首或LAN介面的狀態，通過OMP新增或刪除NAT路由通告。您可以在Cisco SD-WAN Manager中檢視事件日誌，以監控新增或刪除的NAT路由通告。

跟蹤器此處未使用任何探測器。而是使用(i)路由表中存在路由條目，或者(ii)線路協定狀態來決定跟蹤器狀態（開啟/關閉）。 在存在路由條目或基於介面線路協定的跟蹤器時，不存在反應時間間隔 — 當路由條目或介面線路協定關閉時，跟蹤狀態也會變為DOWN狀態。與對象跟蹤器關聯的NAT語句中使用的內部全域性地址立即被停止通告到OMP中。要瞭解有關服務VPN NAT跟蹤器的詳細資訊，請訪問配置指南。

使用案例

如果LAN介面或LAN字首關閉，服務端NAT對象跟蹤器將自動關閉。您可以在中檢視事件日誌 Cisco SD-WAN管理員 用於監控新增或刪除了哪些NAT路由通告。在下一個使用案例中，客戶端需要訪問大型分支中的伺服器。但是，當指向大型分支邊緣上的伺服器的路由（在HA中）被刪除，或者LAN端（服務端）介面在大型分支中的任何一條邊緣上關閉時，會出現問題。在這種情況下，當您使用對象跟蹤器應用服務端NAT時，請確保 — 通過控制內部全域性地址通告進入OMP，確保來自客戶端的入站流量始終定向到位於大型分支中的正確邊緣。如果對進入OMP的路由通告未實施此類控制，則流量最終會因為無法到達從相應邊緣到大型分支中的伺服器而進入黑洞。



組態

對象跟蹤器的配置通過舊版配置中的系統模板完成，然後隨後將對象跟蹤器附加到服務VPN功能模板中各自的NAT語句（內部靜態或內部動態）。在配置組中，通過直接獲取將對象跟蹤器新增到相應服務配置檔案乙太網介面配置檔案的選項，已簡化了此機制。以下是配置它的方法，具體取決於使用者首選的配置方法型別。

- 配置組配置>配置組>服務配置檔案>新增功能>對象跟蹤器:

1. 為正在定義的新對象跟蹤器提供名稱和說明。
2. 選擇Tracker Type(在Interface和route之間)。
3. 分配對象跟蹤器ID。
4. 提供介面名稱或提供路由IP、路由IP掩碼和VPN（取決於步驟2中選擇的選項）。

- Configuration > Configuration Groups > Service Profile > NAT部分：

1.通過按一下Add NAT Pool按鈕建立NAT池（對於觸發SSNAT是必需的）。

2.提供NAT池的詳細資訊，如NatPool Name、Prefix Length、Range Start、Range End和Direction。

3.移到同一部分中的靜態NAT，然後按一下Add New Static NAT按鈕。（還可以選擇將對象跟蹤器連線到內部動態池NAT）。

4.提供詳細資訊，如源IP、轉換後的源IP和靜態NAT方向。

5.在關聯對象跟蹤器欄位下，從下拉選單中選擇先前建立的對象跟蹤器。

- Legacy configuration Configuration > Templates > Feature Templates > System > Tracker部分：

1. 按一下New Object Tracker按鈕。
2. 選擇Tracker Type(在Interface和route之間)。
3. 分配對象ID。
4. 提供介面名稱或路由IP、路由IP掩碼和VPN(取決於步驟2中選擇的選項)。

- Configuration > Templates > Cisco VPN（屬於服務端）> NAT部分：

1.按一下New NAT Pool（新建NAT池）按鈕建立NAT池(觸發SSNAT必須)。

2.提供NAT池的詳細資訊，如Nat池名稱、NAT池字首長度、NAT池範圍開始、NAT池範圍結束和NAT方向。

3.移到同一部分中的靜態NAT，然後按一下New Static NAT按鈕。（還可以選擇將對象跟蹤器連線到內部動態池NAT）。

4.提供源IP地址、轉換後的源IP地址、靜態NAT方向等詳細資訊。

5.在「新增對象跟蹤器」欄位下，鍵入先前建立的對象跟蹤器的名稱。

從CLI的角度來看，配置如下所示：

```
(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使用案例的假設是使用者應用資料策略來匹配NAT流中的傳入 — >傳出和傳出流量。

驗證

驗證針對NAT使用案例的明確配置的對象跟蹤器有兩個方面。

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

1.在Device Options下，鍵入「IP NAT Translation」。

2.在Individual NAT Translation下檢查，並根據配置的對象跟蹤者ID檢視條目的統計資訊（內部本地地址/埠、內部全域性地址/埠、外部本地地址/埠、外部全域性地址/埠、VRF ID、VRF名稱和協定）。

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

如果在與NAT路由對應的NAT跟蹤器上檢測到狀態更改，則顯示名為「NAT路由更改」的事件，其中包含諸如主機名、對象跟蹤器、地址、掩碼、路由型別和更新等詳細資訊。這裡，地址和掩碼對映到靜態NAT語句下配置的內部全域性地址。

在邊緣的CLI上：

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。