了解Catalyst SD-WAN Tracker的可用性和使用案例

目录

简介

背景信息

跟踪器的类型

网关跟踪

- 使用案例
- 配置
- 确认

服务插入1.0和服务交换矩阵2.0跟踪

- 使用案例
- 配置
- 确认

用于DIA的接口终端跟踪器

- 使用案例
- 配置
- 确认

用于SIG隧道/SSE的接口终端跟踪器

- 使用案例
- 配置
- 确认

用于服务交换矩阵2.0的接口终端跟踪器

- 使用案例
- 配置
- 确认

用于静态路由跟踪的静态路由终端跟踪器（服务端）

- 使用案例
- 配置
- 确认

用于VRRP跟踪的接口对象跟踪器

- 使用案例
- 配置
- 确认

用于服务VPN NAT跟踪的接口/路由对象跟踪器

- 使用案例
- 配置
- 确认

简介

本文档介绍Catalyst SD-WAN企业重叠网络、跟踪器可用性和使用案例。

背景信息

Catalyst SD-WAN企业重叠网络通常与各种外部工作负载、应用和服务交互。其中任何一种都可以位于云、数据中心/集线器或远程分支机构。SD-WAN控制平面负责以可扩展的方式在重叠网络上通告通向这些服务的路由。在关键应用和服务沿着特定路径变得不可达的情况下，网络运营商通常必须能够检测这些事件并将用户流量重定向到更合适的路径，以防止不确定的流量黑洞。为了检测和纠正这些类型的网络故障，Catalyst SD-WAN控制平面依靠跟踪器来监控外部服务的运行状况，并根据情况更改路由。

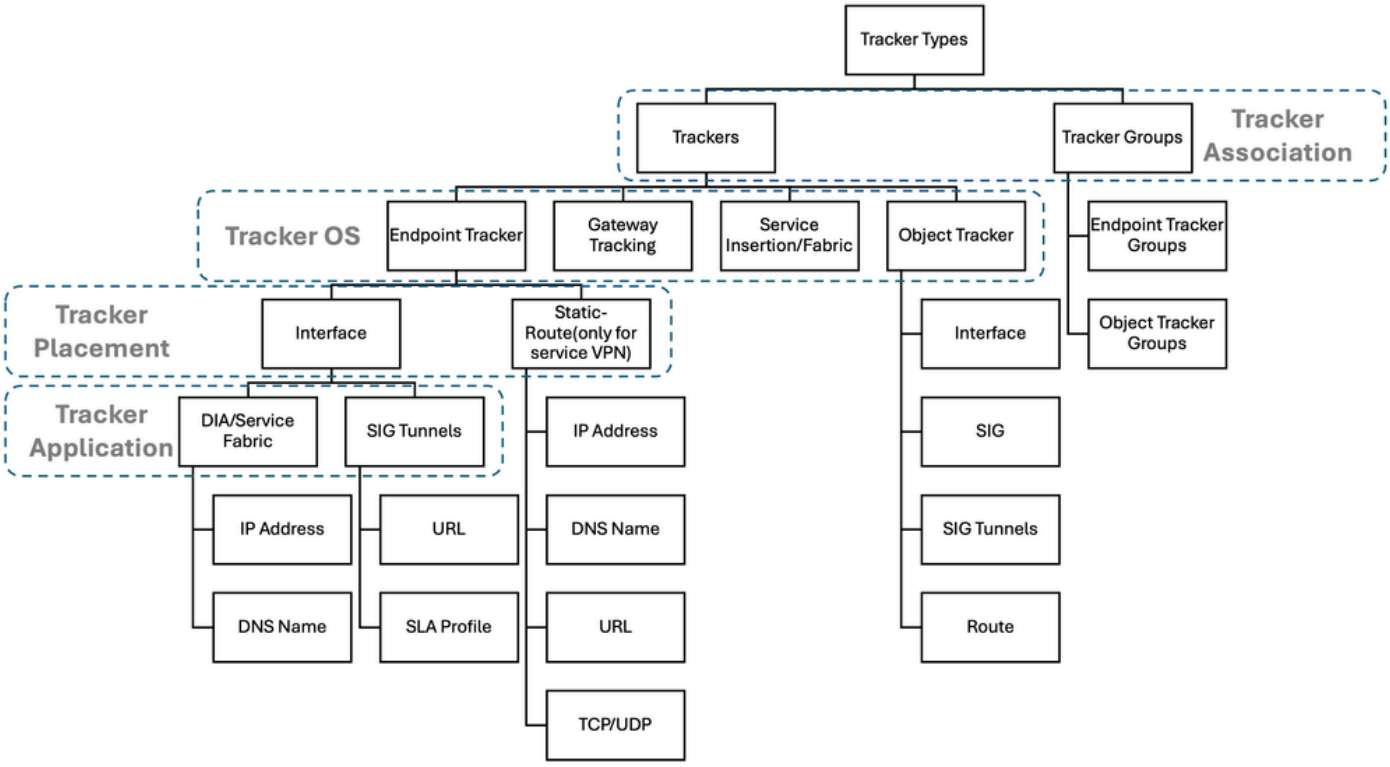
跟踪器是一种控制平面可达性检测机制，它向特定终端发送探测数据包，并向感兴趣的模块通知终端的可达性状态变化（打开或关闭）。跟踪器设计为本地Cisco IOS-XE® IP SLA功能的可扩展高级抽象，可以形成各种探测器（包括HTTP、ICMP和DNS）。当跟踪器通知客户端模块状态更改时，该模块可以采取适当操作来防止流量黑洞，例如安装或卸载路由或路由集。跟踪器在SD-WAN和SD-Routing解决方案中的当前应用包括但不限于：DIA（直接互联网接入）跟踪器、SIG（安全互联网网关）跟踪器、服务跟踪器、静态路由跟踪器、跟踪器组等。

要构建可恢复服务故障的高可用性网络，关键是要了解何时使用每种类型的跟踪器配置/模型。本文的目的是解释每种跟踪器的使用位置和方式。文中介绍了各种跟踪器，每个跟踪器的主要使用案例，以及实现每个解决方案的基本配置工作流程，最后简要介绍了Cisco IOS-XE®中跟踪器的一般注意事项。

本文对endpoint-tracker（特定于SD-WAN和SD-Routing）和对象跟踪器解决方案(本地IOS-XE)进行了区分，这两种解决方案可处理不同的使用案例。

跟踪器的类型

此图表简要概述了Cisco Catalyst SD-WAN解决方案中可用的所有类型的跟踪器：



在上一个图表中，有四个区域可以分类跟踪器：Tracker Association、Tracker OS、Tracker Placement和Tracker Application。下一部分介绍每个分类：

1. 跟踪器关联：此分类描述跟踪器是单个跟踪器还是跟踪器组。Cisco Catalyst SD-WAN支持在一个组中使用多个跟踪器（此时写入时最多2个），跟踪器组的总体状态由布尔型AND或OR运算符决定。示例包括endpoint-tracker组或对象跟踪器组。
2. 跟踪器操作系统：此分类描述支持跟踪器的Cisco IOS-XE®操作系统或模式。Cisco Catalyst IOS-XE路由器支持两种操作模式：

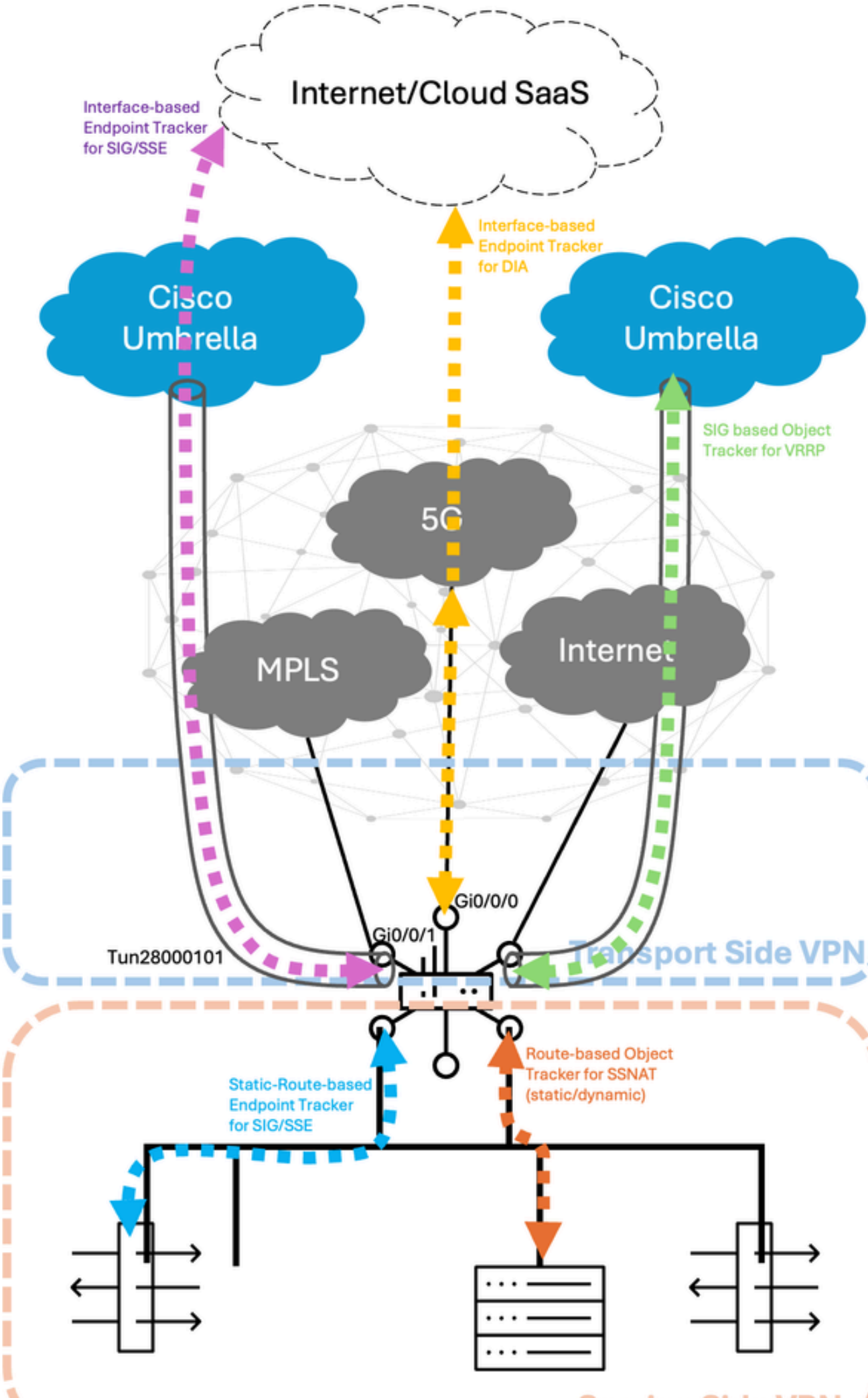
- 自主模式和
- 控制器模式.

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

3.跟踪器放置:此分类描述配置跟踪器的位置。目前，Cisco Catalyst SD-WAN支持在接口、静态路由或服务上应用跟踪器。

4.跟踪器应用:此分类介绍Cisco Catalyst SD-WAN支持的高级使用案例和功能。虽然跟踪器的应用领域众多，但其中有些包括：直接互联网接入(DIA)、安全互联网网关(SIG)、安全服务边缘(SSE)、服务端VPN跟踪等。

以下是Cisco Catalyst SD-WAN Edge（也可以称为cEdge或vEdge）上多个使用案例的跨服务/传输VPN的跟踪器探测流量的直观描述：


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

中每个默认静态路由下指定的下一跳地址，以确保在下一跳（也称为网关，因此称为网关跟踪）的可达性发生故障时进行链路/路由故障转移。要了解有关网关跟踪的更多信息，请访问配置指南。

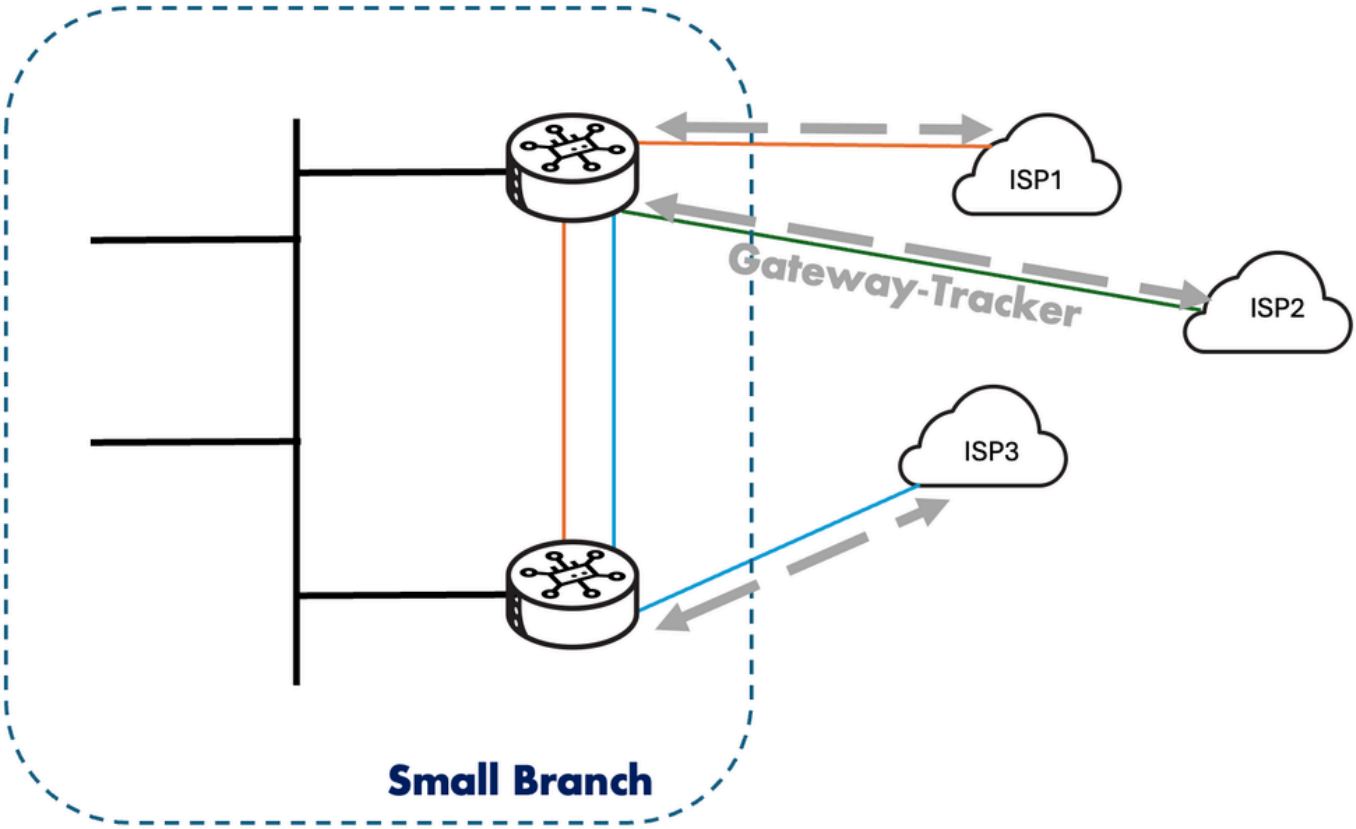
此处使用的探测类型是ARP-request unknown-unicast泛洪数据包。使用的间隔为：

- Hello:10 秒
- Holdtime :100 秒
- 数据包/探测类型：ARP

除了网关跟踪，还用于SD-WAN边缘上的tranport tracking，用于检查本地设备与Cisco Catalyst SD-WAN验证器之间的路由路径。这通过以定期间隔3s使用ICMP探针来完成。这在SD-WAN系统配置模式下使用“track-transport”关键字进行配置。这有助于从各自的WAN边缘定期监控到Cisco Catalyst SD-WAN验证器的DTLS连接。要了解有关传输跟踪的详细信息，请访问配置指南。

使用案例

“网关跟踪”(Gateway Tracking)功能默认情况下在SD-WAN上为属于传输VPN或全局路由表(GRT)的所有静态默认路由隐式配置。 使用功能并不总是从Manager模板配置的角度出发，但在使用具有选项#3、#81等的DHCP服务器的情况下，使用功能还可以从已接收/获取的默认静态路由演进。



配置

默认应用于Cisco Catalyst SD-WAN:

!

```
system


 track-transport
 track-default-gateway


!
```

确认

以下是按照旧版配置和配置组验证的方法：

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

服务插入1.0和服务交换矩阵2.0跟踪

20.3/17.3版本引入了Service Insertion 1.0跟踪，该功能旨在确保服务地址（或转发地址）可访问或可用。此信息可帮助边缘动态添加或从控制/数据策略中撤消下一跳信息。通过配置Service Insertion 1.0，默认情况下会针对服务地址启用跟踪器（或跟踪地址）。基于此，转发地址和服务地址在1.0中是相同的。即使服务跟踪器自动配置了服务，也可以使用no track-enable命令禁用这些跟踪器，也可以在配置组/旧版配置中禁用跟踪器命令。由于这些操作是与服务插入1.0下的服务关联的跟踪器仅有的两种操作（启用/禁用），因此不能再调整其他参数（如阈值、复用器、间隔）。此处使用的探测类型是ICMP回应请求数据包。

要了解有关服务插入1.0跟踪的详细信息，请访问配置指南。服务插入1.0跟踪中使用的默认间隔为：

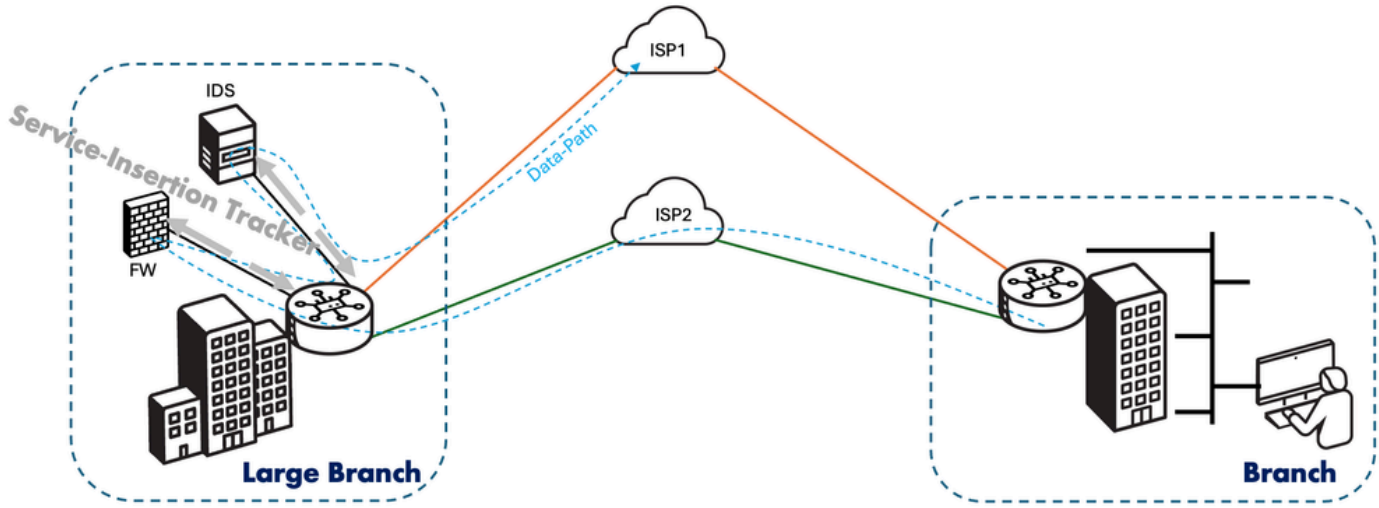
- 探测间隔：每60秒5次探测
- 乘数：5次
- 数据包/探测类型：ICMP应答/应答

Service Fabric 2.0跟踪是从20.13/17.13版本开始推出的Cisco Catalyst SD-WAN中Service Insertion 2.0功能的一部分。在这种新的服务插入变体中，配置配置文件和模板使用的默认方法仍然是让隐式跟踪器指向每个rx/tx接口的service-HA-pair中定义的每个服务地址（或转发地址）。但是，使用Service Fabric 2.0，您现在可以从跟踪地址中拆分转发地址。这可以通过定义单独的终端跟踪器来

跟踪不同于服务地址本身的终端地址来实现。本主题将在下一节中进一步扩展。

使用案例

服务跟踪器的主要使用案例是对服务可达性进行可扩展的监控，尤其是服务链。服务链可以部署在包含多个VPN的网络中，其中每个VPN代表不同的功能或组织，以确保VPN之间的流量通过防火墙。例如，在大型园区网络中，部门间流量可以通过防火墙，而部门内部流量可以直接路由。在运营商必须满足合规性的情况下，例如支付卡行业数据安全标准(PCI DSS),PCI流量必须流经集中式数据中心或区域中心的防火墙时，可以看到服务链：



配置

配置与在SD-WAN上设置服务插入1.0的常规工作流程相同。默认情况下，所有服务地址上将启用Service Insertion 1.0跟踪器。

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

1.单击Add Service按钮。

2.选择服务类型。

3.登记服务地址（最多4个，用逗号分隔）。

4.验证是否已启用“跟踪”旋钮（默认）。 如果需要，可以禁用此功能。

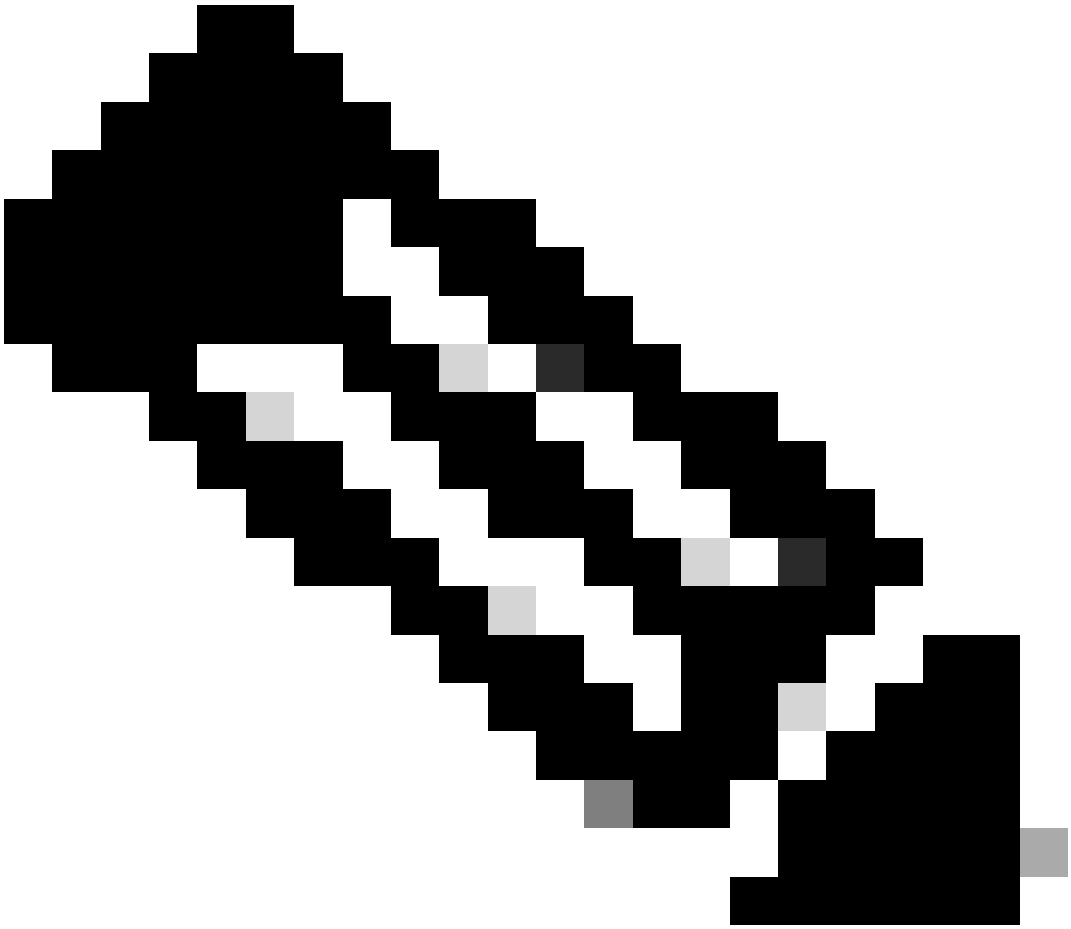
- 旧配置:Configuration > Templates > Feature Templates > Cisco VPN(service)> Service部分：

1.点击“新建服务”按钮

2.选择服务类型。

3.登记服务地址（最多4个，用逗号分隔）。

4.验证是否已启用“跟踪”旋钮（默认）。 如果需要，可以禁用此功能。



注意：在配置第3步时（从配置组或传统配置），跟踪器将自动启动到各种已定义的服务地址

从CLI的角度来看，服务插入1.0的配置如下所示：

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

确认

验证步骤扩展至前面部分中用作基于接口的终端跟踪器的一部分的类似步骤。

显式配置的终端跟踪器有两个验证选项。

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

在Individual Tracker下选中，并根据配置的跟踪器名称查看跟踪器的统计信息（跟踪器类型、状态、终端、终端类型、VPN索引、主机名、往返时间）。

- 在SD-WAN Manager上：监控(Monitor)>设备(Devices)> {select Device-Name} >事件(Events):

如果在跟踪器上检测到抖动，则相应的日志将在此部分中填充详细信息，例如主机名、连接点名称、跟踪器名称、新状态、地址系列和vpn id。

在边缘的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
```

用于DIA的接口终端跟踪器

NAT DIA终端跟踪器跟踪器主要用于通过SD-WAN边缘平台上的NAT DIA接口监控应用的可达性。

对于直接互联网接入(DIA)使用案例，NAT DIA跟踪器主要用于跟踪传输端接口，并触发到另一个可用传输端接口的故障切换，或者通过SD-WAN重叠隧道（使用数据策略）触发故障切换。 此功能从20.3/17.3版本开始引入，而NAT回退功能选项从20.4/17.4版本开始可用。如果跟踪器确定本地互联网无法通过NAT DIA接口使用，则路由器会从服务VPN撤消NAT路由，并根据本地路由配置重新路由流量。跟踪器继续定期检查到接口的路径的状态。当路由器检测到该路径再次正常运行时，会重新安装通往Internet的NAT路由。要了解有关DIA跟踪器的详细信息，请访问配置指南。

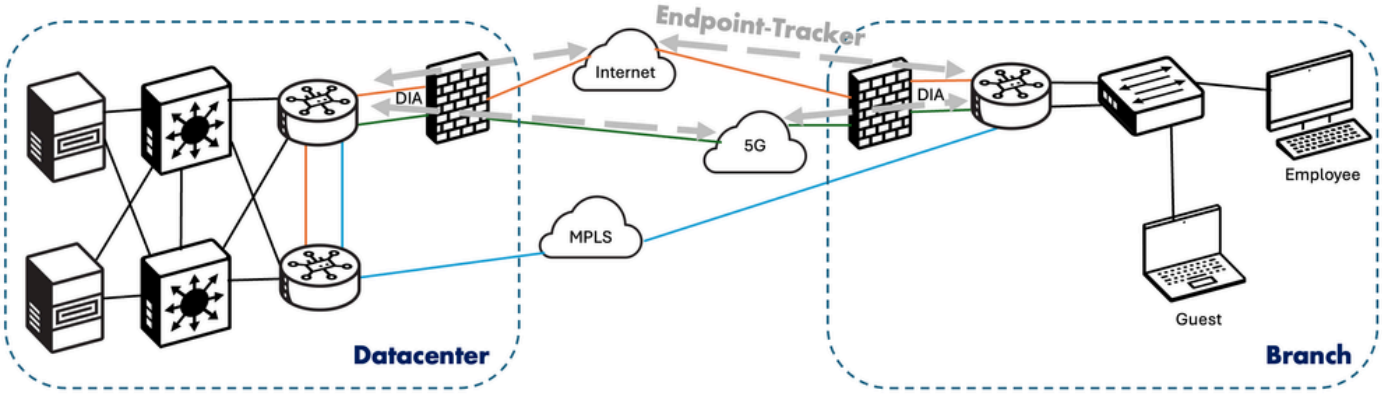
在跟踪器定义中，您可以选择提供通过NAT DIA接口可访问的终端的IP地址（配置为“endpoint-ip”），或者为终端提供完全限定域名(FQDN)（配置为“endpoint-dns-name”）。

此处使用的探针类型是HTTP请求数据包，非常类似于HTTP API请求PDU堆栈。使用的间隔为：

- 探测间隔：60 秒
- 乘数：180秒(由于#retries为3 = 3 x 60秒)
- 数据包/探测类型：HTTP

使用案例

DIA通常作为优化部署在分支机构站点，以避免将任何流向互联网的分支流量回传到数据中心。尽管如此，当在分支机构站点中使用DIA时，沿NAT DIA路由的任何不可达性仍必须回退到备用路径，以避免黑屏和失去服务。对于希望在本地DIA分流出现故障时使用回退到DC（通过SD-WAN重叠使用NAT回退）的站点。在分支侧边缘支持DIA的接口上利用这些基于接口的终端跟踪器检测故障，以启动到备份/DC路径的故障切换。通过这种方式，可以在企业中实现互联网服务的高可用性，同时最大限度地减少网络中断，同时仍然使用DIA优化互联网流量：



配置

必须手动配置这些基于接口的终端跟踪器才能启用此功能集。以下是配置方法，具体取决于用户首选的配置方法类型。

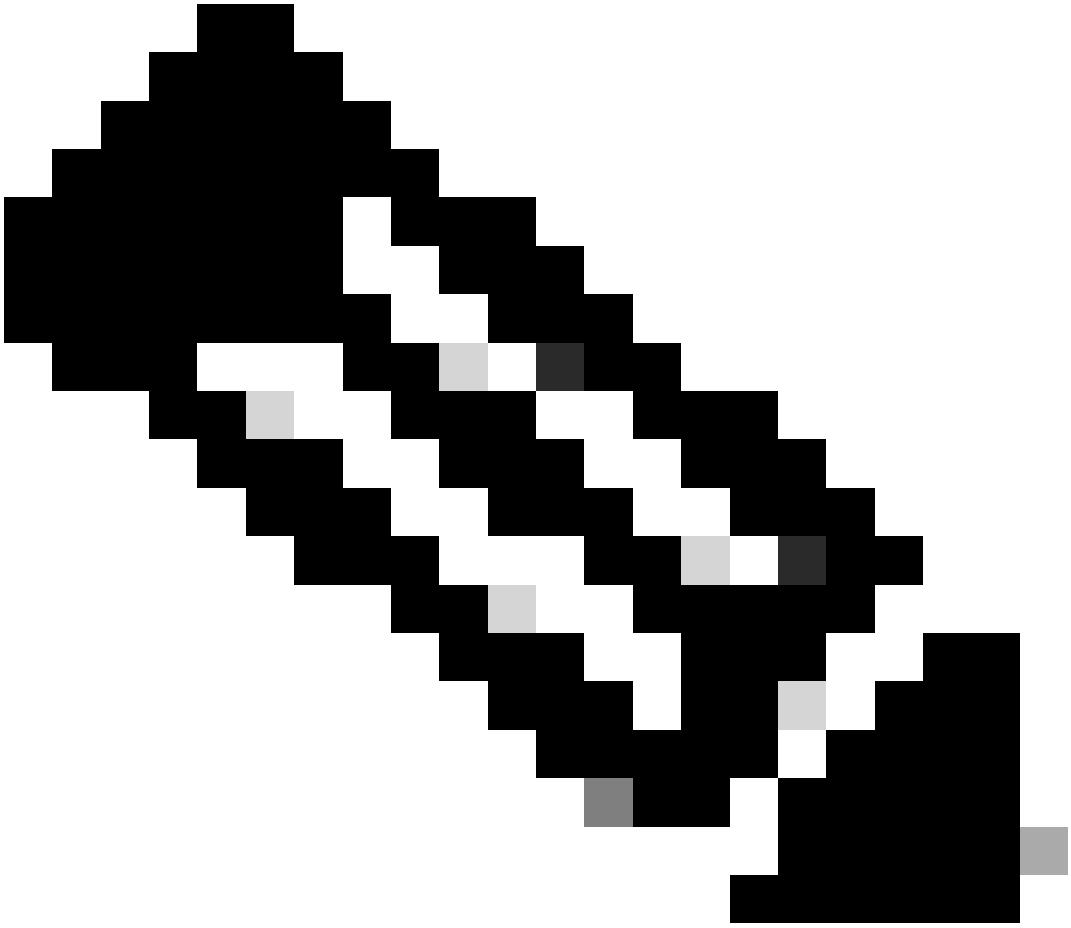
- 配置组:Configuration > Configuration Groups > Transport & Management Profile > Ethernet Interface > Add Feature > Tracker:

1.定义终端跟踪器名称。

2.选择终端跟踪器类型（在HTTP默认和ICMP之间）。

注意：自20.13/17.13版本开始引入了ICMP终端跟踪器类型。

3.选择终端（在终端IP默认和终端DNS名称之间）。



注意：如果选择终端DNS名称，请确保使用传输VPN配置配置文件在传输VPN/VRF下定义有效的DNS服务器或名称服务器。

4.输入必须向其发送跟踪器探测功能的地址或DNS名称(FQDN)（格式取决于上一步骤）。

5.（可选）您可以选择更改“探测间隔”(Probe Interval)（默认值= 60秒）和“重试次数”（默认值= 3次）以加快故障检测时间。

- 旧配置:

步骤1.基于接口的终端跟踪器的定义：Configuration > Templates > Feature Templates > System template > Tracker部分：

1.在Trackers子部分下，选择New Endpoint Tracker按钮。

2.定义终端跟踪器名称。

3.选择Tracker Type（在interface-default和static-route之间）作为接口，因为此处涉及DIA使用案例

。

4.选择Endpoint Type（在IP Address-default和DNS Name之间）。

5.输入跟踪器探测功能必须发送到的终端IP地址或终端DNS名称（格式取决于上一步骤）。

6.（可选）您可以选择更改Probe Threshold（探测阈值）（默认值= 300 ms）、Interval（默认值= 60秒）和Multipler（默认值= 3次）。

步骤2.将基于接口的终端跟踪器应用到传输VPN上的接口：Templates > Feature Templates > Cisco VPN Interface Ethernet > Advanced部分：

1.在Tracker（跟踪器）字段中输入上一步中定义的终端跟踪器的名称。

从CLI的角度来看，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
!
```

确认

显式配置的终端跟踪器有两个验证选项。

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

在Individual Tracker下检查并根据您配置的Tracker Name查看跟踪器的统计信息(Tracker Types、Status、Endpoint、Endpoint Type、VPN Index、Host Name、Round Trip Time)。

- 在SD-WAN Manager上：监控(Monitor)>设备(Devices)> {select Device-Name} >事件(Events):

如果在跟踪器上检测到抖动，则相应的日志将在此部分中填充详细信息，例如主机名、连接点名称、跟踪器名称、新状态、地址系列和vpn id。

在边缘的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
```

用于SIG隧道/SSE的接口终端跟踪器

当终端跟踪器用于SIG隧道/SSE使用案例时，它主要表明企业正在寻找基于云的安全堆栈产品，现在可通过安全互联网网关(SIG)或安全服务边缘(SSE)提供商（例如思科、Cloudflare、Netskope、ZScalar等）的帮助，轻松提供这些产品。SIG隧道和SSE均作为云安全部署模式的一部分，其中分支机构使用云提供其所需的必要安全解决方案。SIG Tunnels使用案例是将Cisco Catalyst SD-WAN与这些SIG提供商集成（从20.4/17.4版本开始）的初始产品，但是随着云交付安全产品的发展，引入了SSE使用案例（从20.13/17.13版本开始），用于覆盖思科（通过思科安全访问）和ZScalar等提供商的使用案例。

IT需要可靠且明确的方法来保护和连接以保持灵活性。现在，为远程员工提供直接访问云应用（如

Microsoft 365和Salesforce）的常见方法是提供额外的安全性。随着承包商、合作伙伴、物联网(IoT)设备等需要网络访问，对云交付网络和安全性的需求每天都在增长。在云边缘，网络和安全功能与终端设备相近的融合，被称为称为Cisco SASE的服务模型。Cisco SASE结合了云交付的网络和安全功能，使所有用户或设备可以随时随地安全地访问应用。安全服务边缘(SSE)是一种网络安全方法，可帮助组织改进其工作环境的安全状态，同时降低最终用户和IT部门的复杂性。要了解有关SIG隧道/SSE跟踪器的更多信息，请访问配置指南。

使用案例

此类基于接口的终端跟踪器用于这种SIG隧道/SSE使用案例，其中您希望跟踪已知的SaaS应用URL终端或关注的特定URL终端。如今，SSE是较为常用的场景版本，因为SASE架构分为SSE核心功能和SD-WAN功能。然后，您需要在从站点创建的IPSec隧道（在本例中为DC）内的主用和备用角色之间进行选择。 用户可以选择在各自的隧道接口下连接跟踪器。

对于SSE提供商，例如思科安全访问（由思科提供）— 使用默认配置的隐式终端跟踪器。但是，用户确实可以选择创建自定义终端跟踪器并将该跟踪器连接到IPSec隧道接口。SSE中使用的默认/隐式终端跟踪器的参数如下：

对于Cisco SSE:

跟踪器名称：DefaultTracker

正在跟踪的终端：http://service.sig.umbrella.com

端点类型:API_URL

阈值:300 ms

倍数：3

间隔:60 sec

对于ZScaler SSE:

跟踪器名称：DefaultTracker

正在跟踪的终端：http://gateway.zscalerthree.net/vpnte

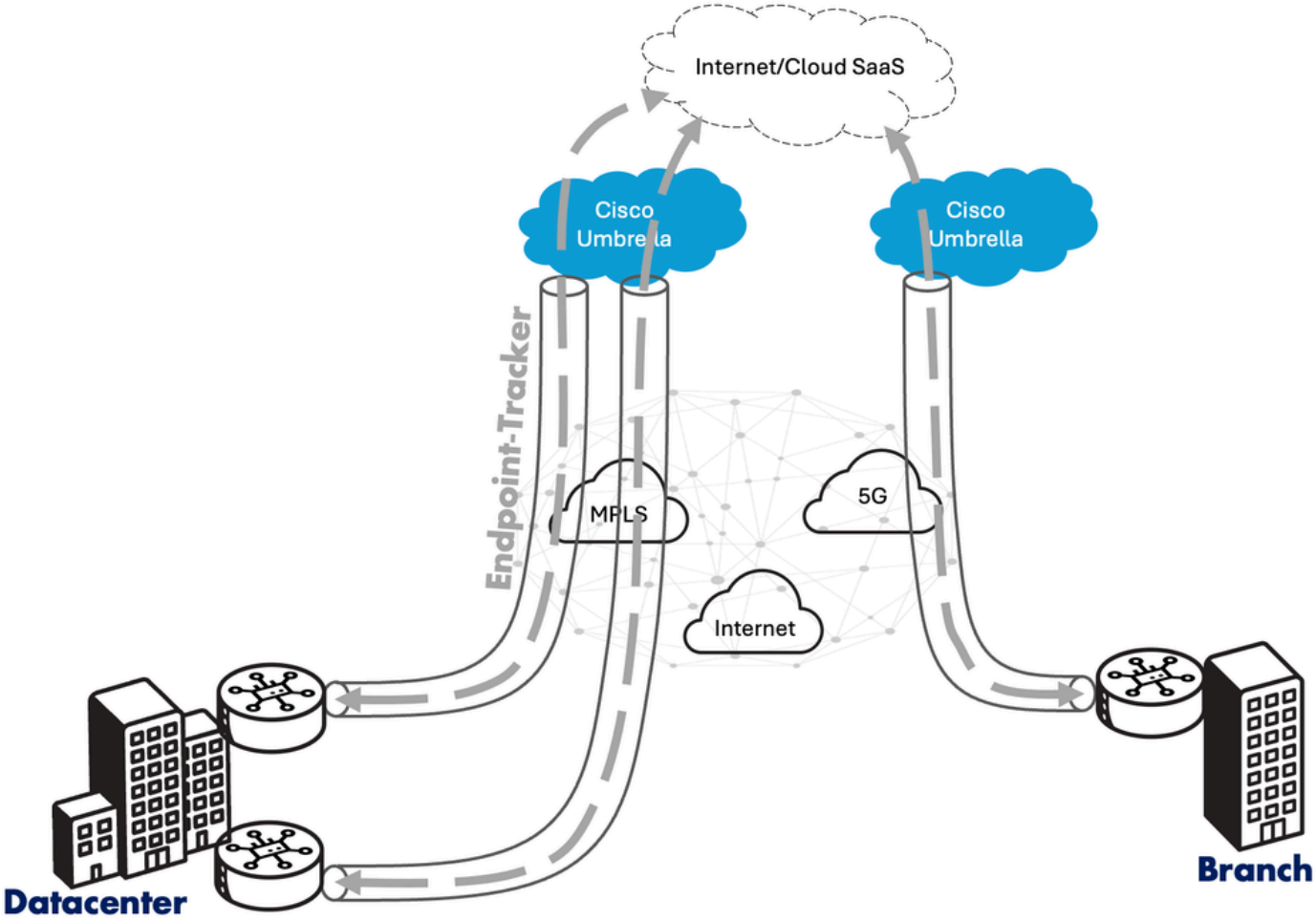
终端类型：API_URL

阈值:300 ms

乘数：3

间隔:60 sec

对于SIG隧道，未定义默认/隐式终端跟踪器。因此，如果用户想要跟踪指向SIG提供商云的IPSec隧道接口，则必须手动配置基于接口的终端跟踪器：



配置

对于SSE提供商，用户无需明确定义任何终端跟踪器（除非需要）。 但是，工作流程因配置类型而异。

作为前提条件，您必须定义SIG/SSE凭证管理>设置>外部服务>云凭证:

1.在Cloud Provider Credentials下，切换Umbrella或Cisco SSE（或两者）的选项。

2.定义参数，如组织ID、API密钥、密钥)。

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

1.单击Add Secure Internet Gateway或Add Secure Service Edge。

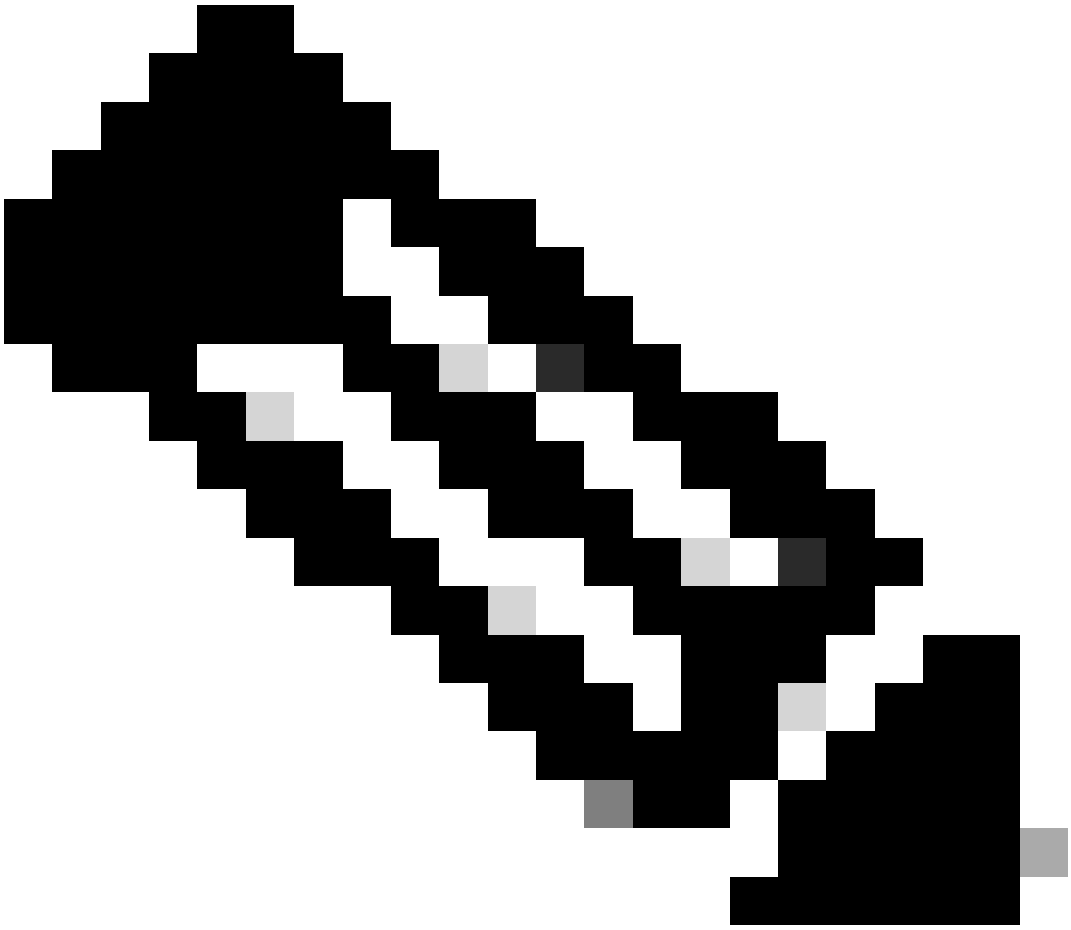
2.定义名称和说明。

3.选择SIG/SSE Provider（SIG/SSE提供商）(Umbrella或Cisco SSE)下的单选按钮之一。

4.在Tracker部分下，定义用于生成跟踪器探测器源的源IP地址。

5.如果选择定义显式/自定义终端跟踪器，请单击Add Tracker，然后填写终端跟踪器的参数(Name、终端API URL、阈值、探测间隔和乘数)。

6.在Configuration部分下，创建隧道接口，可以在其中定义参数(如Interface Name、Description、Tracker、Tunnel Source Interface、Datacenter Primary/Secondary)。



注意：在第6步中，用户可选择将定义的终端跟踪器连接到各自的IPSec隧道。请注意，这是一个可选字段。

7.在高可用性部分下，创建接口对并定义活动接口和备份接口及其各自的权重。然后，将之前配置的策略组应用到相关边缘。

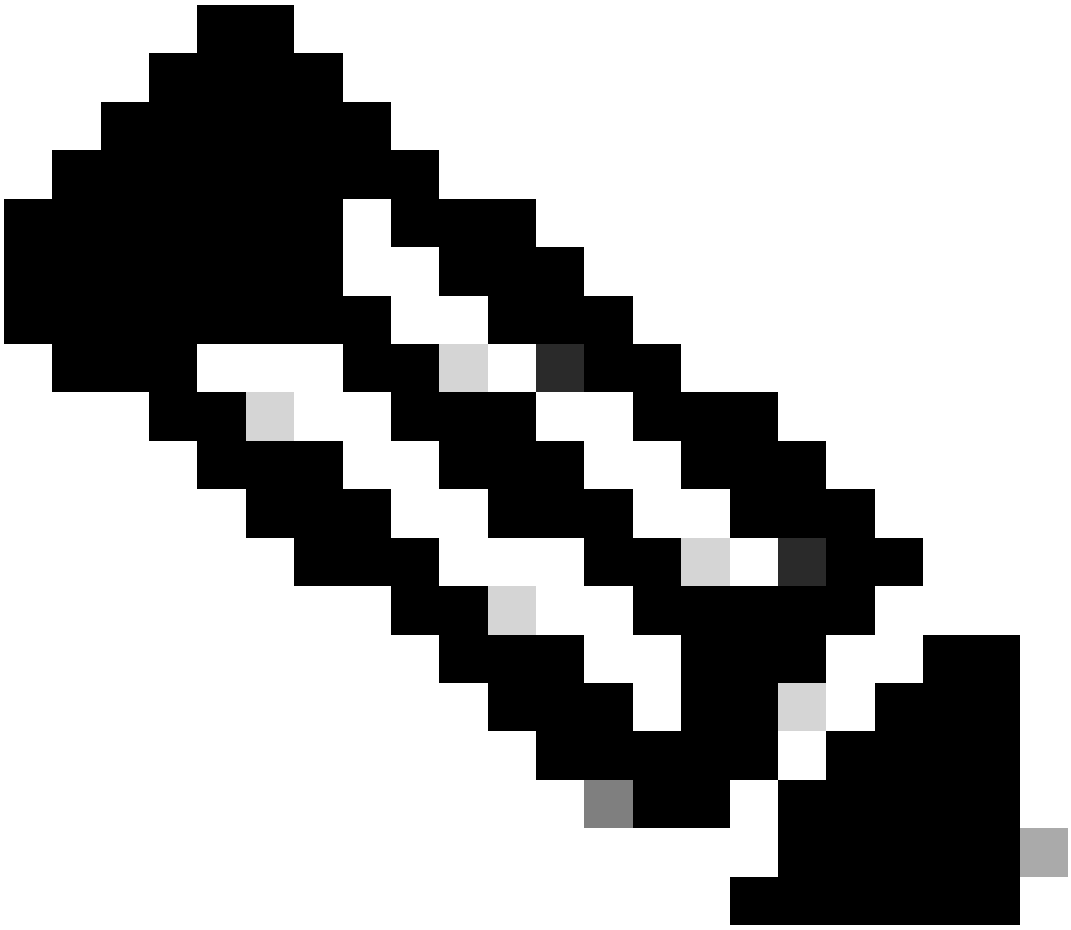
设置传统配置配置(Configuration)>模板(Templates)>功能模板(Feature Templates)>思科安全互联网网关(Cisco Secure Internet Gateway)功能模板：

1.选择“SIG提供商”(SIG Provider)下的单选按钮（“Umbrella”、“ZScalar”或“Generic”）。

2.在“跟踪器(BETA)”部分下，定义用于获取跟踪器探测功能的源IP地址。

5.如果选择定义显式/自定义终端跟踪器，请单击“新建跟踪器”，然后填写终端跟踪器的参数(Name、终端的API url、Threshold、Interval和Multiplier)。

6.在Configuration部分下，创建隧道接口(通过单击Add Tunnel)，您可以在其中定义参数(例如Interface Name、Description、Tracker、Tunnel Source Interface、Datacenter Primary/Secondary)。



注意：在第6步中，用户可选择将定义的终端跟踪器连接到各自的IPSec隧道。请注意，这是一个可选字段。

7.在高可用性部分下，定义活动接口和备份接口及其各自的权重。

从CLI的角度来看，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
!
```

确认

存在显式配置的终端跟踪器的验证选项。

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

在Individual Tracker下选中，并根据配置的跟踪器名称查看跟踪器的统计信息（跟踪器类型、状态、终端、终端类型、VPN索引、主机名、往返时间）。

- 在SD-WAN管理器上：监控(Monitor)>设备(Devices)> {select Device-Name} >事件(Events):

如果在跟踪器上检测到抖动，则相应的日志将在此部分中填充详细信息，例如主机名、连接点名称、跟踪器名称、新状态、地址系列和vpn id。

在边缘的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
```

用于服务交换矩阵2.0的接口终端跟踪器

Service Fabric 2.0跟踪是20.13/17.13版本中引入的，是服务插入1.0跟踪的增强型变体，其中用户可以更大范围地自定义跟踪器。默认行为保留自上一版本的服务插入(1.0)，默认情况下，会启动跟踪器，每个rx/tx的service-HA-pair中定义每个服务地址（或转发地址）。但是使用Service Insertion 2.0，跟踪地址（被跟踪的IP/终端）可以与转发地址（通常为服务地址）分开。 这通过VPN级别上定义的自定义终端跟踪器来完成。要了解有关Service Fabric 2.0跟踪器的详细信息，请访问配置指南。

如果用户选择使用默认跟踪器，则跟踪器探测的规范为：

- Hello:每30秒1次探测
- 乘数：3次
- 数据包/探测类型：ICMP应答/应答

如果用户选择使用自定义跟踪器，则跟踪器探测的规范为：

- Hello:每60秒1次探测
- 乘数：3次
- 数据包/探测类型：ICMP回应请求/应答

使用案例

前面部分中提到的服务插入1.0的使用案例也在这里适用。

配置

支持Service Insertion 2.0的基于工作流的配置，这是一种向导引导的方法，有助于简化用户体验，同时遵循标准配置组工作流程步骤。

1.在配置>服务插入>服务链定义部分下定义“服务链 — 配置”组：

a.单击Add Service Chain Definition按钮。

b.填写服务的名称和说明。

c.填写列表格式（通过从下拉列表中选择）Service Type。

2.在配置>服务插入>服务链配置部分下定义“服务链实例 — 配置”组：

a.点击添加服务链配置。

b.在Service Chain Definition步骤中，选择标题为Select Existing的单选按钮，然后选择之前定义的服务。

c.提供启动服务链配置步骤的名称和说明。

d.在“手动连接的服务的服务链配置”步骤中，选择服务链VPN-ID。

e.然后，对于服务链实例中定义的每个服务（以子选项卡表示），在服务详细信息下提供附件类型（IPv4、IPv6或隧道连接）。

f.选中Advanced复选框。如果需要具有active-backup/HA使用案例(同时启用Add parameters for Backup命令)，或者即使需要定义自定义终端跟踪器（同时启用Custom Tracker命令）。

g.如果有出口(tx)流量通过一个接口进入服务，而来自服务的返回流量通过另一个接口进入(rx)的情况，请打开Traffic from service is received on a different interface knop。

h.启用Advanced和Custom Tracker旋钮后，定义服务IPv4地址（转发地址）、SD-WAN路由器接口（服务连接到该接口）和跟踪器终端（跟踪地址）。 您还可以修改自定义跟踪器参数，例如间隔和乘数（通过点击edit按钮）。

i.对每个后续定义的服务重复步骤(e)、(f)、(g)和(h)。

3.将Service Chain Instance附加到Configuration > Configuration Groups > Service Profile > Service VPN > Add Feature > Service Chain Attachment Gateway下的Edge - Configuration组的配置配置文件中：

a.提供此服务链附件网关地块的名称和说明。

b.选择先前定义的服务链定义（步骤1）。

c.重新添加/验证步骤2中执行的详细信息。对于跟踪器定义，与前一步的唯一区别在于您有机会指定跟踪器名称，并选择跟踪器类型（从service-icmp到ipv6-service-icmp）。

从CLI的角度来看，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
!
```

确认

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

在Individual Tracker下选中，并根据配置的跟踪器名称查看跟踪器的统计信息（跟踪器类型、状态、终端、终端类型、VPN索引、主机名、往返时间）。

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

如果在跟踪器上检测到抖动，则相应的日志将在此部分中填充详细信息，例如主机名、连接点名称、跟踪器名称、新状态、地址系列和vpn id。

在边缘的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
```

用于静态路由跟踪的静态路由终端跟踪器（服务端）

第二种类型的终端跟踪器称为基于静态路由的终端跟踪器。正如名称本身所示，这些类型的跟踪器主要用于跟踪服务端VPN下定义的任何静态路由的下一跳地址。默认情况下，所有“已连接”和“静态”路由类型都会通告到OMP协议中，在该协议后，包含相应服务VPN的所有远程站点将获知该目标前缀（其中下一跳指向始发站点的TLOC）。 始发站点是从其发起特定静态路由的站点。

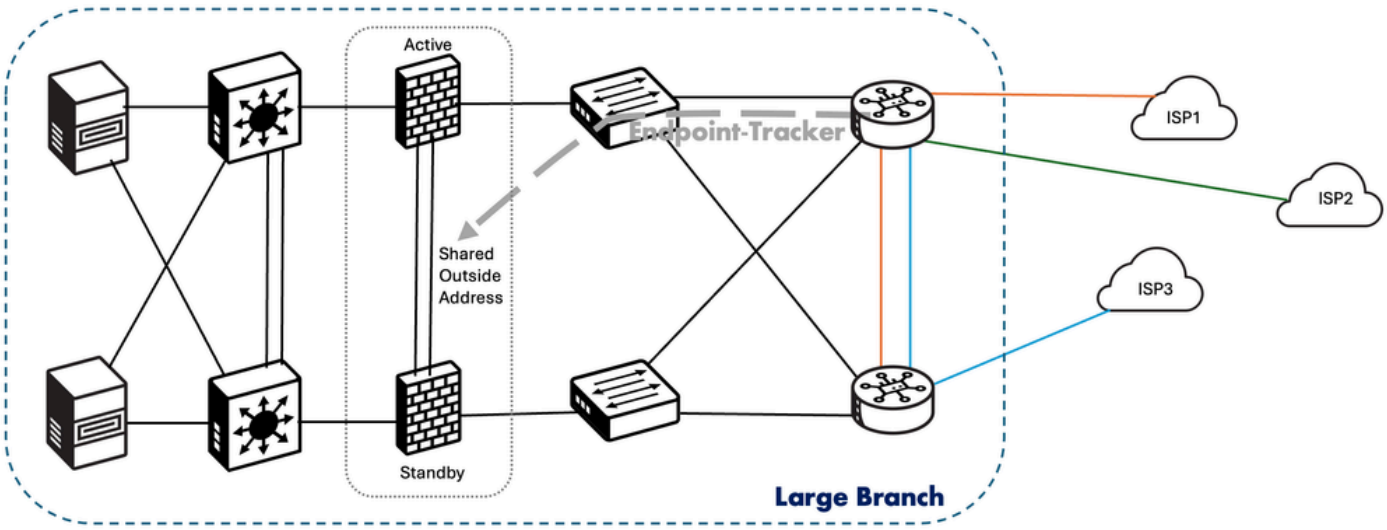
但是，如果静态路由中的下一跳地址无法到达，该路由不会停止通告到OMP。这会导致流量被黑洞锁定到指向源站点的流量。这就需要将跟踪器连接到静态路由，以确保只有当下一跳地址可到达时，才将静态路由通告到OMP。此功能在20.3/17.3版本中引入，用于基本IP地址类型基于静态路由的终端跟踪器。从20.7/17.7版本起，添加了对仅向下一跳IP地址的特定TCP或UDP端口发送跟踪器探测功能的支持(在使用防火墙仅打开某些端口进行跟踪的情况下)。要了解有关静态路由跟踪器的详细信息，请访问配置指南。

此处使用的探针类型是一个简单的ICMP回应请求数据包。使用的间隔为：

- Hello:60 秒
- Holdtime :180秒(由于#retries为3 = 3 x 60秒)
- 数据包/探测类型：ICMP应答/应答

使用案例

这种基于静态路由的终端跟踪器用于服务端跟踪静态路由中的下一跳地址。其中一种常见情况是跟踪与一对主用/备用防火墙对应的LAN端下一跳地址，这些防火墙共享基于外部IP地址的外部接口，外部接口根据外部接口来扮演“主用”防火墙的角色。当防火墙规则似乎非常严格，只为基于使用案例的目的打开某些端口时，静态路由跟踪器可用于跟踪特定TCP/UDP端口到属于LAN端防火墙外部接口的下一跳IP地址。



配置

必须手动配置这些基于静态路由的终端跟踪器才能启用此功能集。以下是配置方法，具体取决于用户首选的配置方法类型。

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

1.为正在定义的新（终端）跟踪器提供名称、描述和跟踪器名称。

2.选择终端类型，具体取决于您是否需要仅跟踪下一跳IP地址(选择Address单选按钮)，还是甚至特定TCP/UDP端口(选择Protocol单选按钮)。

3.以IP地址格式输入地址。如果在上一步中选择Protocol作为终端类型，则还要输入协议（TCP或UDP）和端口号。

4.如果需要，您可以更改探测间隔、重试次数和延迟限制的默认值。

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

1.选择Add IPv4/IPv6 Static Route按钮。

2.填写详细信息，例如网络地址、子网掩码、下一跳、地址和AD。

3.单击Add Next Hop With Tracker按钮。

4.重新输入下一跳地址AD，然后从下拉列表中选择先前创建的（终端）跟踪器名称。

- 传统配置Configuration > Templates > Feature Templates > System Template > Tracker部分：

1.选择“新建终端跟踪器”按钮。

2.为正在定义的新（终端）跟踪器提供名称。

3.将“跟踪器类型”(Tracker Type)单选按钮更改为static-route。

4.选择终端类型，作为下一跳IP地址（选择IP地址单选按钮）。

5.以IP地址格式输入终端IP。

6.如果需要，您可以更改探测间隔、重试次数和延迟限制的默认值。

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

1.选择New IPv4/IPv6 Route按钮。

2.填写详细信息，例如前缀、网关。

3.单击Add Next Hop With Tracker按钮。

4.重新输入下一跳地址AD（距离），并手动输入先前创建的（终端）跟踪器名称。

从CLI的角度来看，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
!
```

确认

明确配置的终端跟踪器有两个验证区域。

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

1.在Device Options下，键入“Endpoint Tracker Info”。

2.在Individual Tracker(Attach Point Name)下检查，并根据已配置的Tracker Name查看跟踪器的统计信息(Tracker State、Associated Tracker Record Name、从设备到终端的mx延迟、上次更新时间戳)。

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

如果在跟踪器上检测到抖动，则相应的日志将在此部分中填充详细信息，例如主机名、连接点名称、跟踪器名称、新状态、地址系列和vpn id。

在边缘的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 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]
```

用于VRRP跟踪的接口对象跟踪器

对象跟踪器是为自主模式消耗（使用案例）设计的跟踪器。 这些跟踪器的使用案例从基于VRRP的接口/隧道跟踪到服务VPN NAT跟踪不等。

对于VRRP跟踪使用案例,VRRP状态根据隧道链路状态确定。如果主VRRP上的隧道或接口关闭，流量将定向到辅助VRRP。LAN网段中的辅助VRRP路由器成为主要VRRP，为服务端流量提供网关。此使用案例仅适用于service-VPN，并有助于在SD-WAN重叠上发生故障时在LAN端对VRRP角色进行故障转移（在SSE上为接口或隧道）。 要将跟踪器连接到VRRP组，只能使用对象跟踪器（而非终端跟踪器）。 此功能是从20.7/17.7版本引入的，适用于Cisco Catalyst SD-WAN Edge。

跟踪器此处未使用任何探测器。相反，它使用线路协议状态来决定跟踪器状态（打开/关闭）。 基于

接口线路协议的跟踪器中没有反应间隔 — 当接口/隧道线路协议关闭时，跟踪状态也会变为DOWN状态。然后，根据关闭或递减操作，VRRP组将相应地重新收敛。要了解有关VRRP接口跟踪器的详细信息，请访问配置指南。

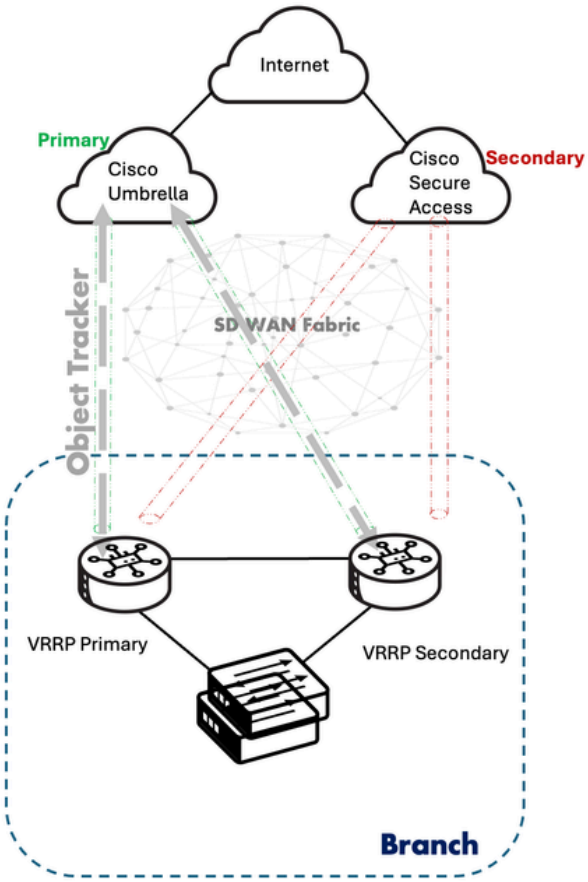
使用案例

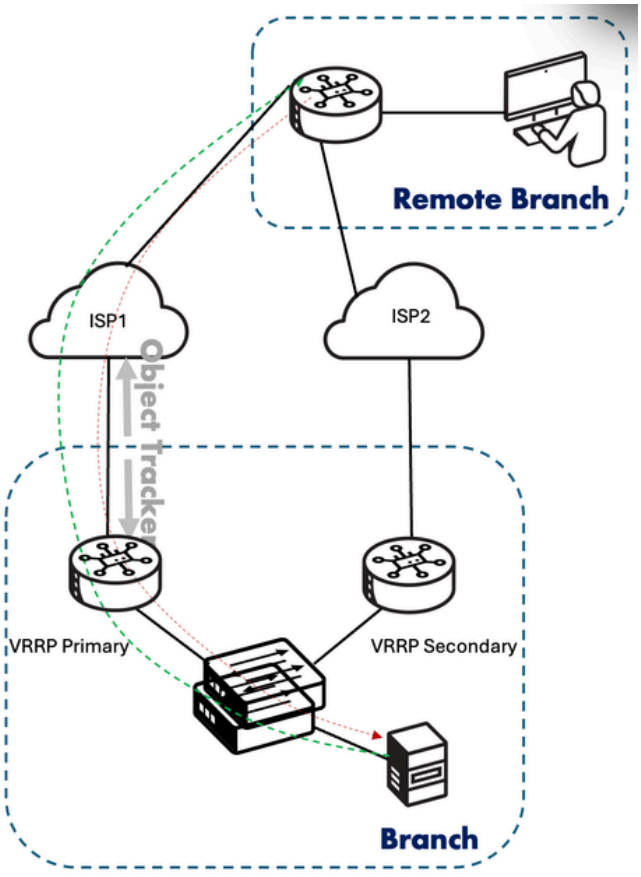
根据实施基于VRRP的接口跟踪所需的标准，存在多个使用案例。目前，支持的两种模式是(i)接口（指与本地TLOC绑定的任何隧道接口）或(ii)SIG接口（与SIG隧道接口相关）。 在每种情况下，被跟踪的部分都是接口线路协议。

带互联网的双路由器:跟踪对象已绑定到VRRP组。如果跟踪器的对象（在本例中为SIG隧道接口）发生故障，这将通知VRRP主路由器触发从主到备份的状态转换，并通知备用路由器成为主路由器。此状态更改可以通过两种类型的操作影响或触发：

1. 递减：其中，在跟踪对象状态从UP转换到DOWN的情况下，用于在其上配置VRRP VIP的接口的VRRP优先级被减少或减少某个值。
2. 关闭：这是一种方法，在跟踪对象状态从UP转换到DOWN时，VRRP进程在应用的接口上关闭。在有非对称转发实例的使用案例中，不建议使用此方法。

TLOC更改首选项：为避免来自其他SDWAN站点的非对称流量进入在服务VPN上运行VRRP的站点，如果已配置，则VRRP主路由器的TLOC首选项将提升1。您甚至可以在配置组下修改此值。这可确保从WAN到LAN的流量被VRRP主路由器本身所吸引。从LAN到WAN的流量被VRRP主节点的VRRP机制所吸引。此功能独立于VRRP接口跟踪器。从CLI角度来看，这是一个可选命令(tloc-change-pref)。





配置

对象跟踪器的配置通过旧版配置中的系统模板完成，然后随后在service-VPN以太网接口功能模板下将对象跟踪器连接到相应的VRRP组。在配置组中，通过直接获取将对象跟踪器添加到相应服务配置文件以太网接口配置文件的选项，已简化了此机制。下面是配置它的方法，具体取决于用户首选的配置方法类型。

- Configuration group Configuration > Configuration Groups > Service Profile > Ethernet Interface > Add Feature > Object Tracker:

1. 为定义的新对象跟踪器提供名称和说明。
2. 选择Tracker Type(在Interface和SIG之间)。
3. 分配对象跟踪器ID。
4. 提供接口名称（具体取决于步骤2中选择的选项）。

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

1. 在IPv4 Settings下，单击Add VRRP IPv4。
2. 定义VRRP组ID并为此服务端以太网接口提供本地优先级。
3. 提供VRRP虚拟IP(VIP)地址。
4. 启用TLOC Preference Change命令并提供TLOC Preference Change Value（用于处理非对称路由）。
5. 点击Add VRRP Tracking Object。
6. 在Associate Object Tracker下，从之前创建的Object Tracker(基于Name)下拉列表中选择
7. 选择Tracker Action(Shutdown或Decrement)。
8. 输入Decrement Value（具体取决于在步骤7中选择的选项）。

- 传统配置Configuration > Templates > Feature Templates > System > Tracker部分：

1. 单击New Object Tracker按钮。
2. 选择Tracker Type(在Interface和SIG之间)。
3. 分配对象ID。
4. 提供接口名称（具体取决于步骤2中选择的选项）。

- Configuration > Templates > Ethernet Interface（属于服务端）> VRRP部分：

1. 单击New VRRP按钮。
2. 定义VRRP组ID并为此服务端以太网接口提供本地优先级（可选，默认值为100）。
3. 提供VRRP虚拟IP(VIP)地址。
4. 启用TLOC Preference Change命令并提供TLOC Preference Change Value（用于处理非对称路由）。
5. 在Object Tracker下，单击Add Tracking Object。
6. 输入对象跟踪器ID（在系统模板下定义）。
7. 选择Tracker Action(Shutdown或Decrement)。
8. 输入Decrement Value（具体取决于在步骤7中选择的选项）。

从CLI的角度来看，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
!
```

确认

有两个选项可用于验证为VRRP使用案例显式配置的对象跟踪器。

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

1.在Device Options下，键入“VRRP Information”。

2.在Individual VRRP Group(Group ID)下，根据已配置的对象跟踪器ID查看跟踪器的统计信息

(Track Prefix Name、Track State、Discontinuity Time和Last State Change Time)。

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

如果在对象跟踪器上检测到状态更改，则与其连接的相应VRRP组会更改其状态。相应的日志将填充在此部分（名称显示为Vrrp组状态更改），其中包含详细信息，例如主机名、if编号、grp id、addr类型、if名称、vrrp group-state、state change-reason和vpn id。

在边缘的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)
```

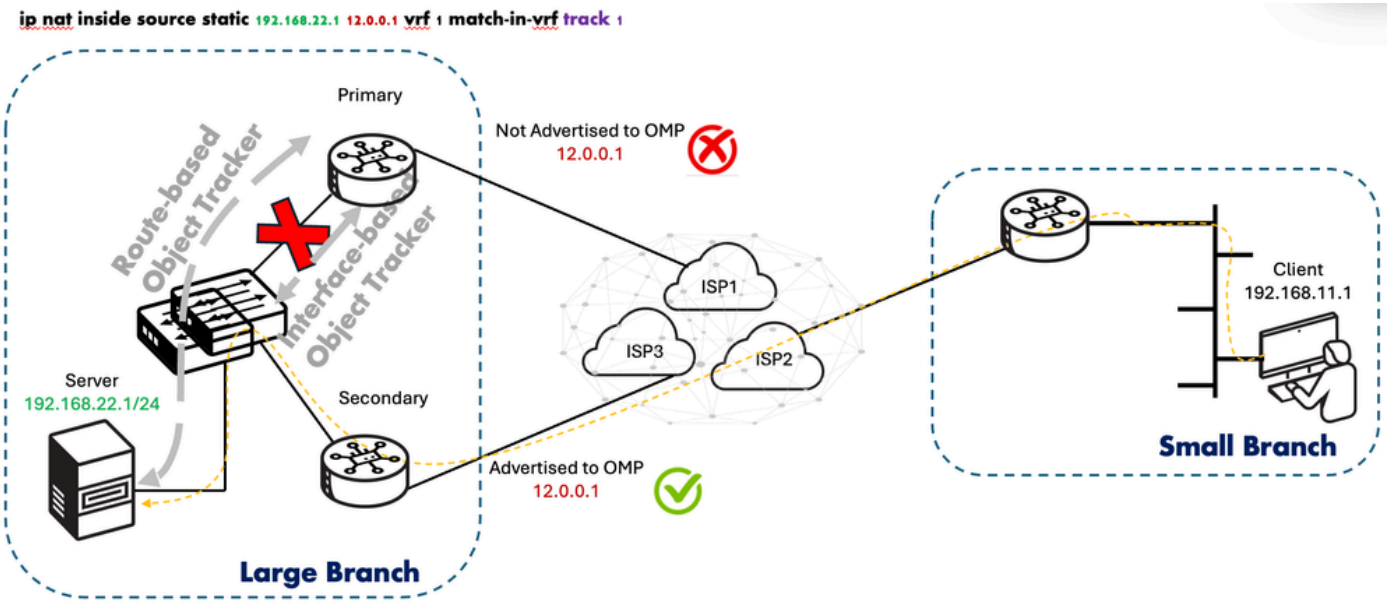
用于服务VPN NAT跟踪的接口/路由对象跟踪器

服务端NAT对象跟踪器是20.8/17.8版本中引入的一项功能，其中服务端VPN NAT中使用的内部全局地址（内部静态NAT和内部动态NAT）仅会在(i)发现内部本地地址可访问或(ii)LAN/服务端接口的线路协议根据连接的对象跟踪器为UP时通告到OMP。因此，可以使用的对象跟踪器类型是(i)路由或(ii)接口。根据LAN前缀或LAN接口的状态，通过OMP添加或删除NAT路由通告。您可以在Cisco SD-WAN Manager中查看事件日志，以监控添加或删除了哪些NAT路由通告。

跟踪器此处未使用任何探测器。相反，它使用(i)路由表中存在路由条目，或(ii)线路协议状态来确定跟踪器状态（打开/关闭）。 存在路由条目或基于接口线路协议的跟踪器时，不存在反应间隔 — 路由条目或接口线路协议关闭时，跟踪状态也会变为DOWN状态。与对象跟踪器关联的NAT语句中使用的内部全局地址立即被停止通告到OMP中。要了解有关服务VPN NAT跟踪器的详细信息，请访问配置指南。

使用案例

如果LAN接口或LAN前缀关闭，服务端NAT对象跟踪器会自动关闭。您可以在中查看事件日志 思科SD-WAN管理器 用于监控添加或删除了哪些NAT路由通告。在下一个使用案例中，客户端需要访问大型分支中的服务器。但是，当指向大型分支边缘（在HA中）上的服务器的路由被删除，或者LAN-side（服务端）接口在大型分支中的任一边缘断开时，会出现此问题。在这种情况下，当您使用对象跟踪器应用服务端NAT时，请确保 — 通过控制内部全局地址通告进入OMP，确保来自客户端的入站流量始终指向位于大型分支中的正确边缘。如果在进入OMP的路由通告上未实施此类控制，则流量最终会由于无法从该相应边缘到达大型分支中的服务器而进入黑洞。



配置

对象跟踪器的配置通过旧版配置中的系统模板完成，然后随后将对象跟踪器附加到服务VPN功能模板中的相应NAT语句（内部静态或内部动态）。在配置组中，通过直接获取将对象跟踪器添加到相应服务配置文件以太网接口配置文件的选项，已简化了此机制。下面是配置它的方法，具体取决于用户首选的配置方法类型。

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

1. 为定义的新对象跟踪器提供名称和说明。
2. 选择Tracker Type(在Interface和route之间)。
3. 分配对象跟踪器ID。
4. 提供接口名称或提供路由IP、路由IP掩码和VPN（具体取决于步骤2中选择的选项）。

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

1.单击Add NAT Pool按钮，创建NAT池(对于触发SSNAT是必需的)。

2.提供NAT池的详细信息，例如NatPool Name、Prefix Length、Range Start、Range End和Direction。

3.在同一部分中转到Static NAT，然后单击Add New Static NAT按钮。（还可以选择将对象跟踪器连接到内部动态池NAT）。

4.提供详细信息，例如源IP、转换后的源IP和静态NAT方向。

5.在关联对象跟踪器字段下，从下拉列表中选择先前创建的对象跟踪器。

- 传统配置Configuration > Templates > Feature Templates > System > Tracker部分：

1. 单击New Object Tracker按钮。
2. 选择Tracker Type(在Interface和route之间)。
3. 分配对象ID。
4. 提供接口名称或路由IP、路由IP掩码和VPN(具体取决于步骤2中选择的选项)。

- Configuration > Templates > Cisco VPN（属于服务端）> NAT部分：

1.单击New NAT Pool（新建NAT池）按钮创建NAT池(触发SNAT必需)。

2.提供NAT池的详细信息，如Nat池名称、NAT池前缀长度、NAT池范围开始、NAT池范围结束和NAT方向。

3.移至同一部分中的静态NAT，然后单击New Static NAT按钮。（还可以选择将对象跟踪器连接到内部动态池NAT）。

4.提供源IP地址、转换后的源IP地址、静态NAT方向等详细信息。

5.在“添加对象跟踪器”(Add Object Tracker)字段下，键入先前创建的对象跟踪器的名称。

从CLI的角度来看，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使用案例的假设是，用户应用数据策略来匹配NAT流中的传入 — >传出和传出流量。

确认

对于NAT使用案例，对显式配置的对象跟踪器有两个验证区域。

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

1.在Device Options下，键入“IP NAT Translation”。

2.在Individual NAT Translation下检查，并根据配置的对象跟踪器ID查看条目的统计信息（内部本地地址/端口、内部全局地址/端口、外部本地地址/端口、外部全局地址/端口、VRF ID、VRF名称和协议）。

- 在SD-WAN Manager上：监控(Monitor)>设备(Devices)> {选择设备名称} >事件(Events):

如果在与NAT路由对应的对象跟踪器上检测到状态更改，并将其修剪到OMP中，则会显示名为“NAT路由更改”的事件，其中包含诸如主机名、对象跟踪器、地址、掩码、路由类型和更新等详细信息。在这里，地址和掩码映射到静态NAT语句下配置的内部全局地址。

在边缘的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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。