Catalyst SD-WAN Tracker 사용성 및 활용 사례 이해

목차

소개

이 문서에서는 Catalyst SD-WAN 엔터프라이즈 오버레이 네트워크, 추적기 사용 편의성 및 사용 사례에 대해 설명합니다.

배경 정보

Catalyst SD-WAN 엔터프라이즈 오버레이 네트워크는 일반적으로 다양한 외부 워크로드, 애플리케이션 및 서비스와 상호작용합니다. 클라우드, 데이터 센터/허브 또는 원격 브랜치에 모두 배치 가능 SD-WAN 제어 평면은 확장 가능한 방식으로 오버레이를 통해 이러한 서비스에 대한 경로를 광고하는 역할을 합니다. 중요한 애플리케이션과 서비스가 특정 경로에 도달할 수 없는 경우, 네트워크 운영자는 일반적으로 이러한 이벤트를 탐지하고 사용자 트래픽을 더 적절한 경로로 리디렉션하여 무제한 트래픽 블랙홀링을 방지해야 합니다. 이러한 유형의 네트워크 장애를 탐지하고 해결하기 위해 Catalyst SD-WAN 컨트롤 플레인은 외부 서비스의 상태를 모니터링하고 라우팅 변경을 적절하게 수행하는 추적기에 의존합니다.

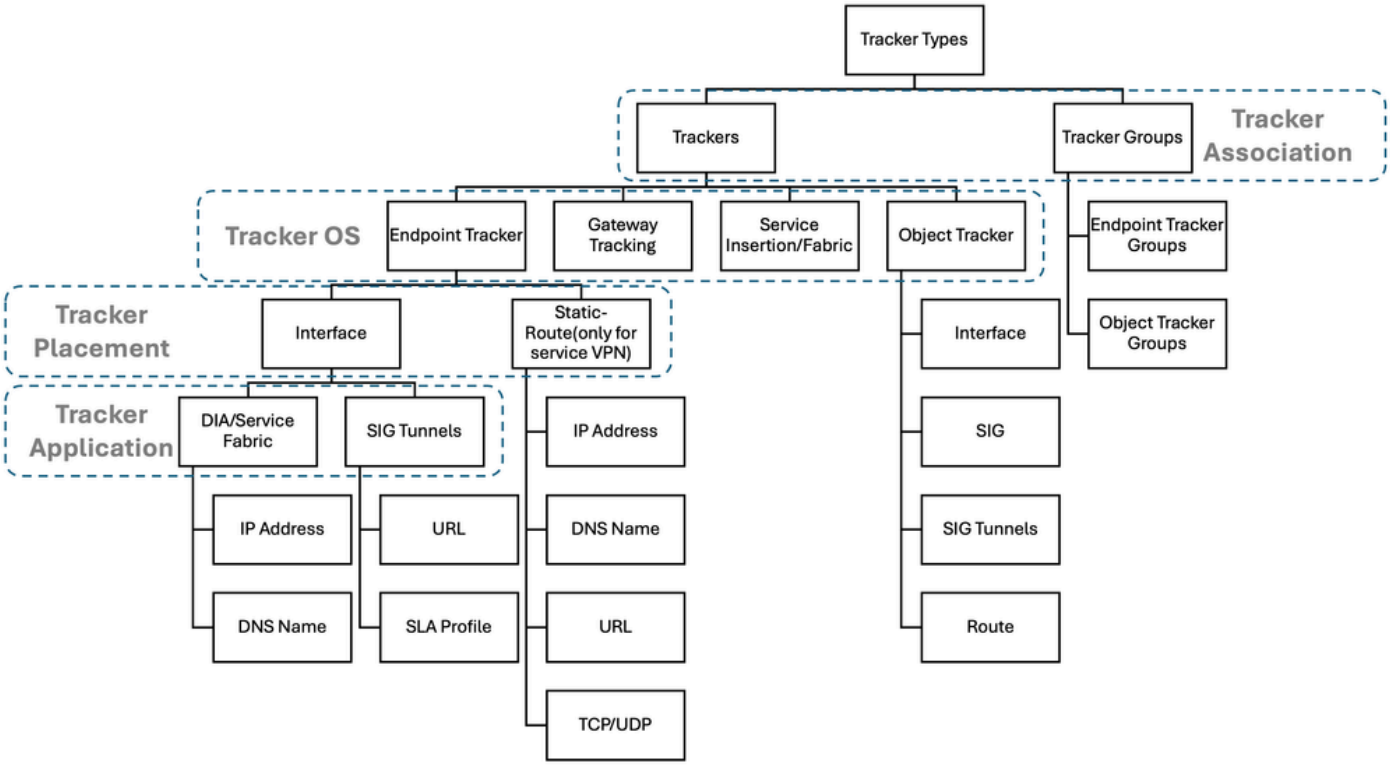
추적기는 특정 엔드포인트를 향해 프로브 패킷을 전송하고 엔드포인트의 연결 상태 변경(작동 또는 작동 중지)을 관련 모듈에 알리는 컨트롤 플레인 연결 감지 메커니즘입니다. 추적기는 다양한 프로브(HTTP, ICMP 및 DNS 포함)를 형성할 수 있는 기본 Cisco IOS-XE® IP SLA 기능의 확장 가능한 상위 수준 추상화로 설계되었습니다. 추적기가 클라이언트 모듈에 상태 변경을 통지하면 해당 모듈은 경로 또는 경로 집합을 설치 또는 제거하는 등 트래픽 블랙홀링을 방지하기 위한 적절한 조치를 취할 수 있습니다. SD-WAN 및 SD-Routing 솔루션 모두에서 추적기의 현재 애플리케이션에는 다음이 포함되지만 이에 국한되지 않습니다. DIA(Direct Internet Access) 추적기, SIG(Secure Internet Gateway) 추적기, 서비스 추적기, 고정 경로 추적기, 추적기 그룹 등.

서비스 장애에 대한 복원력을 갖춘 고가용성 네트워크를 구축하려면 각 유형의 추적기 컨피그레이션/모델을 사용할 시기를 파악하는 것이 중요합니다. 이 글의 목적은 각 유형의 추적기가 사용되는 위치와 방법을 설명하는 것입니다. 각 추적기의 기본 사용 사례와 각 솔루션을 구현하기 위한 기본 구성 워크플로는 물론 다양한 추적기가 여기에 설명되어 있습니다. 마지막으로, 이 문서에서는 Cisco IOS-XE®의 추적기와 관련된 일반적인 주의 사항을 소개합니다.

이 문서에서는 엔드포인트 추적기(SD-WAN 및 SD-Routing 전용)와 객체 추적기 솔루션(네이티브 IOS-XE)을 구별하여 다양한 사용 사례를 다룹니다.

추적기 유형

이 차트는 Cisco Catalyst SD-WAN 솔루션에서 사용할 수 있는 모든 유형의 추적기에 대한 간략한 개요를 제공합니다.



앞의 차트에서는 추적기를 분류할 수 있는 네 가지 영역이 있습니다. Tracker Association, Tracker OS, Tracker Placement 및 Tracker Application입니다. 다음 섹션에서는 각 분류에 대해 설명합니다 .

1. 추적기 연결: 이 분류는 추적기가 단일 추적기인지 아니면 추적기 그룹인지를 기술한다. Cisco Catalyst SD-WAN은 한 그룹에서 여러 추적기의 사용을 지원하며(쓰기 시 최대 2개), 추적기 그룹의 전체 상태는 부울 AND 또는 OR 연산자에 의해 결정됩니다. 예로는 엔드포인트 추적기 그룹 또는 객체 추적기 그룹이 있습니다.
2. 추적기 OS: 이 분류에서는 추적기가 지원되는 Cisco IOS-XE® 운영 체제 또는 모드에 대해 설명합니다. Cisco Catalyst IOS-XE 라우터는 두 가지 운영 모드를 지원합니다.

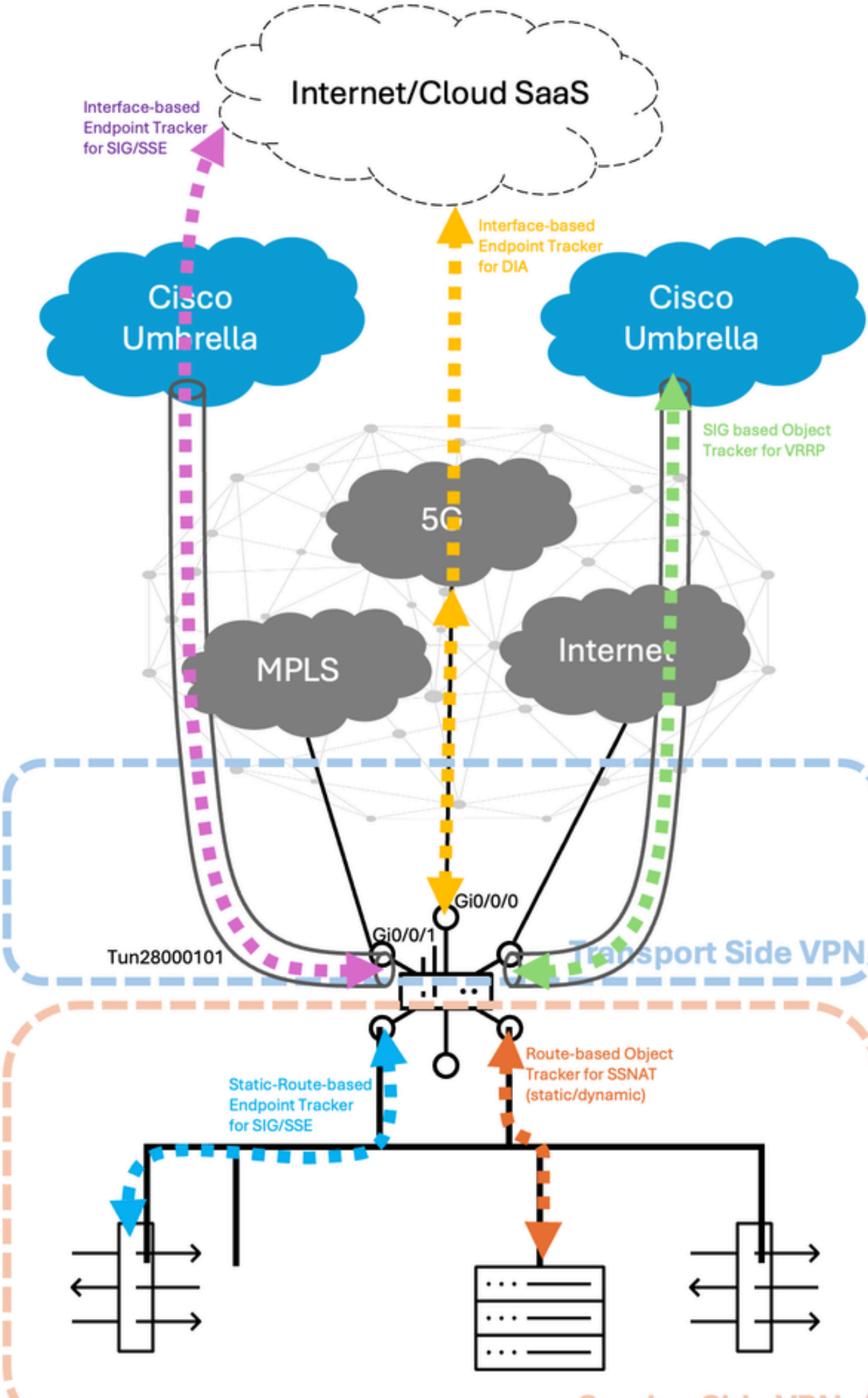
- 자동 모드 및
- 컨트롤러 모드.

모든 엔드포인트 추적기와 게이트웨이 추적 기능은 모두 컨트롤러 모드(SD-WAN) 사용 사례용인 반면, 개체 추적기는 자동 모드(SD-Routing) 사용 사례용입니다.

3. 추적기 배치: 이 분류는 추적기가 구성된 위치를 설명합니다. 현재 Cisco Catalyst SD-WAN은 인터페이스, 고정 경로 또는 서비스에서 추적기의 적용을 지원합니다.

4. 추적장치 신청 이 분류에서는 Cisco Catalyst SD-WAN에서 지원하는 상위 레벨 사용 사례 및 기능에 대해 설명합니다. 추적기의 적용 분야는 다양하지만 그 중 일부는 다음과 같습니다. DIA(Direct Internet Access), SIG(Secure Internet Gateway), SSE(Secure Service Edge), 서비스측 VPN 추적 등

다음은 Cisco Catalyst SD-WAN Edge(cEdge 또는 vEdge라고도 함)의 여러 사용 사례에 대한 서비스/전송 VPN을 지나는 추적기 프로브 트래픽에 대한 시각적 설명입니다.


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

의 각 기본 고정 경로 아래에 지정된 다음 홉 주소를 지속적으로 모니터링하여 다음 홉에 대한 연결 실패 시 링크/경로 장애 조치를 확인할 수 있습니다(게이트웨이라고도 하며, 따라서 게이트웨이 추적이라고도 함). 게이트웨이 추적에 대한 자세한 내용은 구성 설명서를 참조하십시오.

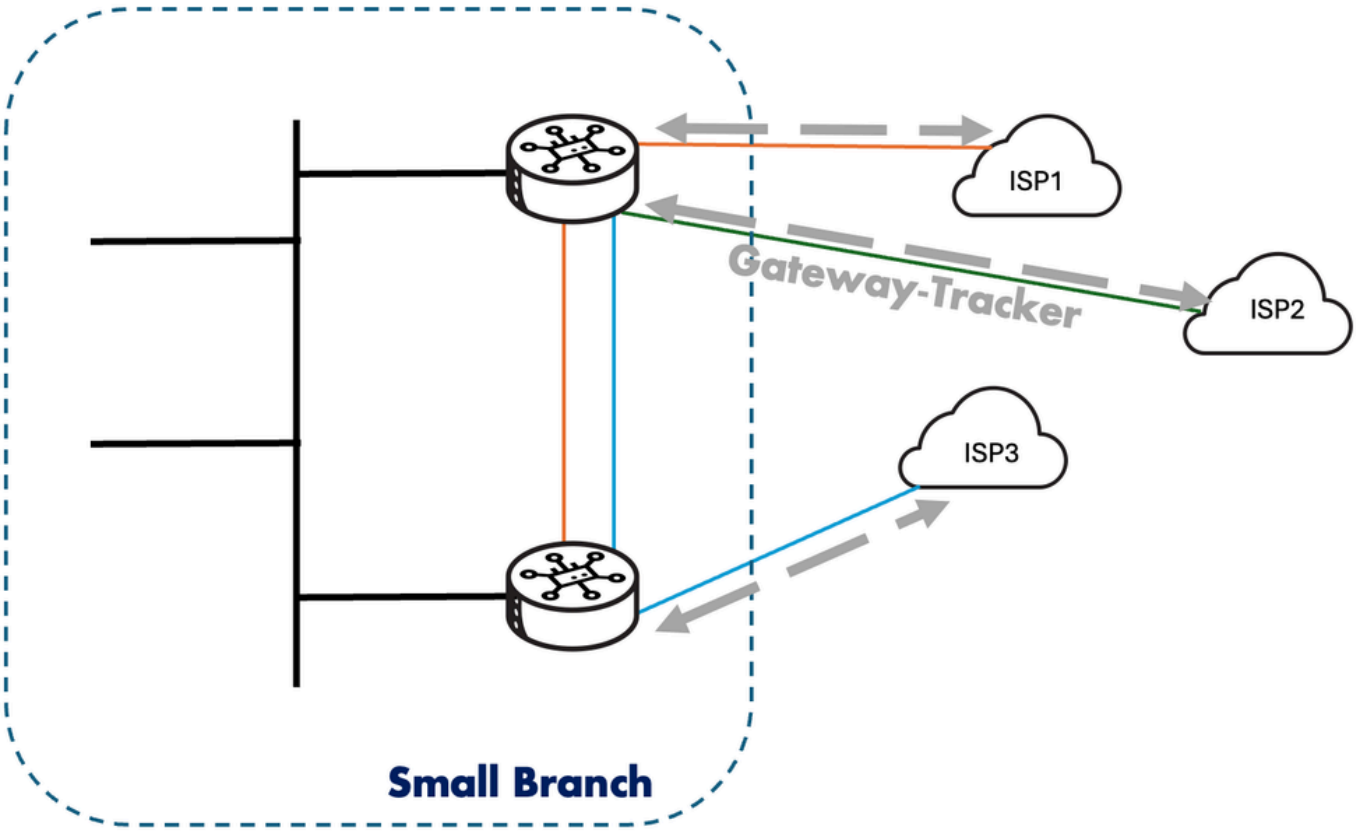
여기서 사용되는 프로브의 유형은 ARP 요청 알 수 없는 유니캐스트 플러딩 패킷입니다. 사용되는 간격은 다음과 같습니다.

- 안녕하십니까? 10초
- Holdtime: 100초
- 패킷/프로브 유형: ARP

게이트웨이 추적과 함께 로컬 디바이스와 Cisco Catalyst SD-WAN Validator 간의 라우팅된 경로를 확인하기 위한 SD-WAN Edge에 대한 전송 추적도 사용됩니다. 이 작업은 ICMP 프로브를 3s의 일정한 간격으로 사용하여 수행합니다. 이는 SD-WAN 시스템 컨피그레이션 모드에서 "track-transport" 키워드를 사용하여 구성됩니다. 이는 해당 WAN 에지에서 Cisco Catalyst SD-WAN Validator에 대한 DTLS 연결을 정기적으로 모니터링하는 데 도움이 됩니다. 전송 추적에 대한 자세한 내용은 컨피그레이션 가이드를 참조하십시오.

활용 사례

게이트웨이 추적은 전송 VPN 또는 GRT(Global Routing Table)에 속하는 모든 고정 기본 경로에 대해 SD-WAN에서 기본적으로 암시적으로 구성되는 기능입니다. 이 기능의 사용은 항상 Manager 템플릿 컨피그레이션 관점에서 발생하는 것이 아니라 옵션 #3, #81 등의 DHCP 서버를 사용하는 시나리오에서 수신/획득한 기본 고정 경로에서 발전할 수도 있습니다.



설정

Cisco Catalyst SD-WAN에 기본적으로 적용됩니다.

```
!
system




 track-transport
 track-default-gateway




!
```

확인

레거시 컨피그레이션 및 컨피그레이션 그룹에 따라 이를 확인하는 방법은 다음과 같습니다.

- 구성 그룹: Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > System profile(시스템 프로파일) > Basic sub-profile(기본 하위 프로파일) > Track Settings(설정 추적) 섹션 > Track Default Gateway (default:ON)(기본 게이트웨이 추적(기본값:ON))
- 레거시 구성: Configuration(컨피그레이션) > Templates(템플릿) > Feature Templates(기능 템플릿) > System template(시스템 템플릿) > Advanced(고급) 섹션 > Gateway Tracking(게이트웨이 추적) (default:ON)

서비스 삽입 1.0 및 서비스 패브릭 2.0 추적

Service Insertion 1.0 Tracking은 20.3/17.3 릴리스에 도입되었으며 서비스 주소(또는 전달 주소)의 도달 가능 여부를 확인하는 데 사용되는 기능입니다. 이 정보는 Edge가 제어/데이터 정책에서 next-hop 정보를 동적으로 추가하거나 제거하는 데 도움이 됩니다. Service Insertion 1.0의 컨피그레이션에서는 추적기(또는 추적 주소)가 서비스 주소에 대해 기본적으로 활성화됩니다. 이를 기준으로 전달 주소와 서비스 주소는 1.0에서 동일합니다. 서비스 추적기가 자동으로 서비스로 구성되더라도 no track-enable 명령을 사용하거나 구성 그룹/레거시 구성에서 추적기 노브를 비활성화하여 추적기를 비활성화할 수 있습니다. 이러한 작업은 서비스 삽입 1.0에서 서비스에 연결된 추적기를 사용하여 가능한 유일한 두 가지 작업(활성화/비활성화)이므로 조정할 수 있는 추가 매개 변수(예: 임계값, 다중화기, 간격)가 없습니다. 여기에 사용되는 프로브 유형은 ICMP 에코 요청 패킷입니다.

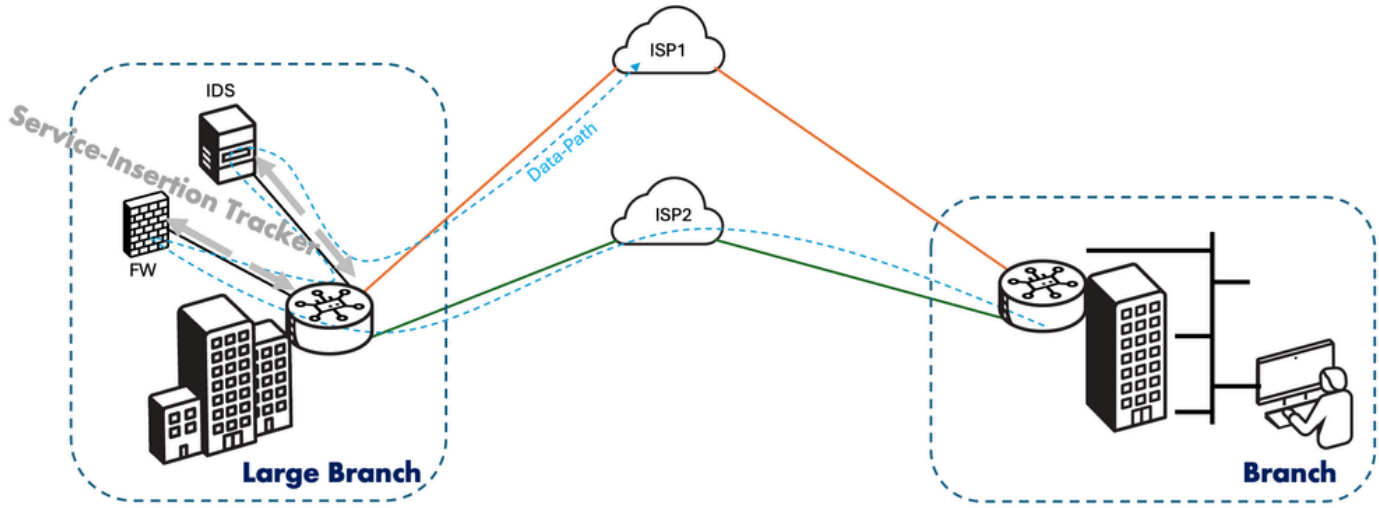
서비스 삽입 1.0 추적에 대한 자세한 내용은 구성 가이드를 참조하십시오. 서비스 삽입 1.0 추적에 사용되는 기본 간격은 다음과 같습니다.

- 프로브 간격: 60초마다 프로브 5개
- 승수: 5회
- 패킷/프로브 유형: ICMP 에코/에코-응답

Service Fabric 2.0 추적은 20.13/17.13 릴리스부터 도입된 Cisco Catalyst SD-WAN의 Service Insertion 2.0 기능의 일부로 제공됩니다. 이 새로운 유형의 서비스 삽입에서 컨피그레이션 프로필 및 템플릿에서 사용하는 기본 방법은 rx/tx 인터페이스당 서비스-HA 쌍에서 정의된 각 서비스 주소(또는 전달 주소)를 가리키는 암시적 추적기를 사용하는 것입니다. 그러나 Service Fabric 2.0에서는 이제 추적 주소에서 전달 주소를 분할할 수 있습니다. 이는 서비스 주소 자체가 아닌 다른 엔드포인트 주소를 추적하기 위해 별도의 엔드포인트 추적기를 정의하기만 하면 됩니다. 이 주제는 다음 섹션에서 더 자세히 설명합니다.

활용 사례

서비스 추적기의 주요 활용 사례는 서비스 연결, 특히 서비스 체이닝의 확장 가능한 모니터링을 위한 것입니다. 서비스 체이닝은 여러 VPN으로 구성된 네트워크에 구축할 수 있으며, 각 VPN은 서로 다른 기능 또는 조직을 나타내므로 VPN 간의 트래픽이 방화벽을 통과할 수 있습니다. 예를 들어 대규모 캠퍼스 네트워크에서는 부서 간 트래픽이 방화벽을 통과할 수 있는 반면, 부서 간 트래픽은 직접 라우팅될 수 있습니다. 서비스 체이닝은 운영자가 PCI DSS(Payment Card Industry Data Security Standard)와 같은 규정 준수를 충족해야 하는 시나리오에서 확인할 수 있으며, PCI 트래픽은 중앙 집중식 데이터 센터 또는 지역 허브의 방화벽을 통과해야 합니다.



설정

컨피그레이션은 SD-WAN에 Service Insertion 1.0을 설정하기 위한 일반 워크플로와 동일합니다. Service Insertion 1.0 추적기는 모든 서비스 주소에서 기본적으로 활성화됩니다.

- 구성 그룹: Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로파일) > Service VPN(서비스 VPN) > Service(서비스) 섹션:

1. 서비스 추가 버튼을 클릭합니다.

2. 서비스 유형을 선택합니다.

3. 서비스 주소를 입력합니다(최대 4개, 쉼표로 구분).

4. 추적 노브가 활성화되어 있는지 확인합니다(기본값). 필요한 경우 이 기능을 비활성화할 수 있습니다.

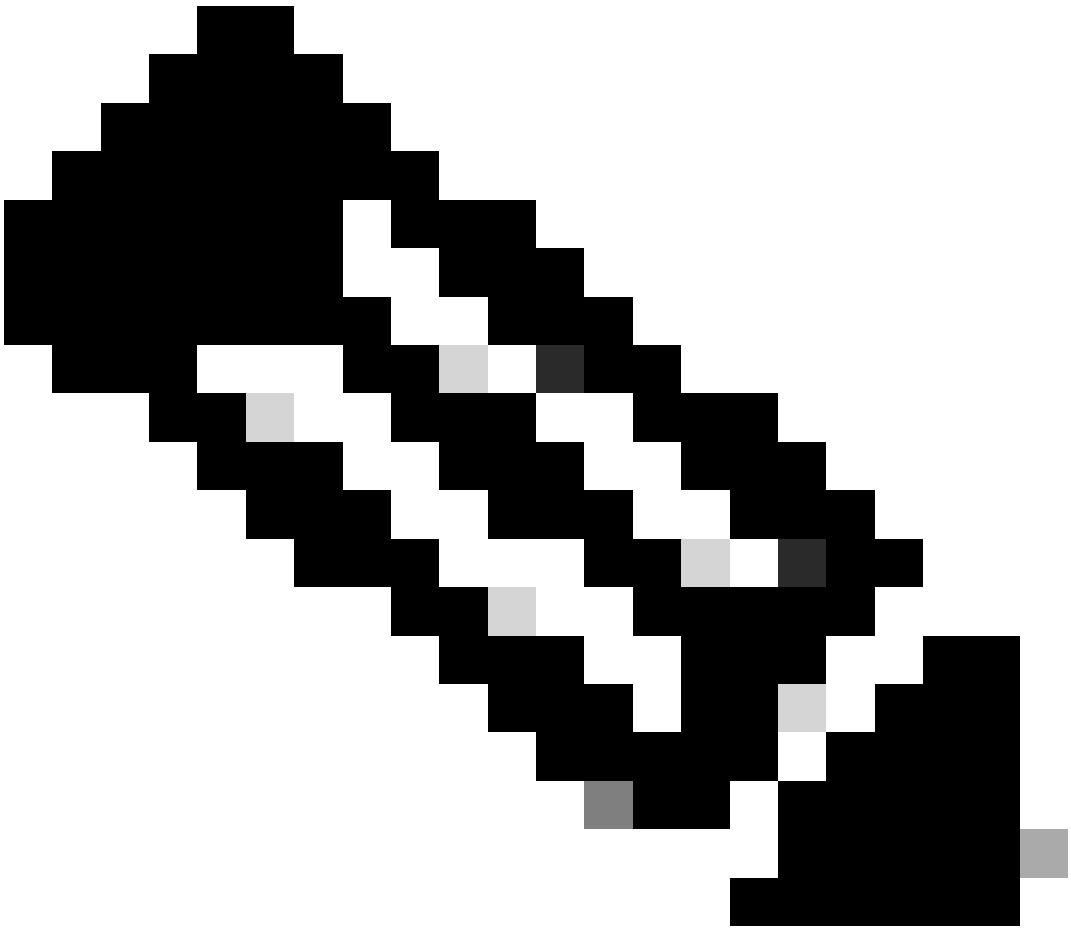
- 레거시 구성: Configuration(컨피그레이션) > Templates(템플릿) > Feature Templates(기능 템플릿) > Cisco VPN (service) > Service(서비스) 섹션:

1. New Service(새 서비스) 버튼을 클릭합니다

2. 서비스 유형을 선택합니다.

3. 서비스 주소를 입력합니다(최대 4개, 쉼표로 구분).

4. 추적 노브가 활성화되어 있는지 확인합니다(기본값). 필요한 경우 이 기능을 비활성화할 수 있습니다.



참고: 3단계가 구성되면(Configuration 그룹 또는 Legacy 컨피그레이션에서) 다양한 정의된 서비스 주소에 추적기가 자동으로 시작됩니다

CLI의 관점에서 Service Insertion 1.0의 컨피그레이션은 다음과 같이 표시됩니다.

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

확인

확인 단계는 이전 섹션에서 사용된 인터페이스 기반 엔드포인트 추적기의 일부로 이어지는 유사한 단계로 확장됩니다.

명시적으로 구성된 엔드포인트 추적기에는 두 가지 확인 옵션이 있습니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Applications(애플리케이션) > Tracker(추적기):

Individual Tracker 아래에서 확인하고 구성된 Tracker Name(추적기 이름)을 기준으로 추적기의 통계(Tracker Types(추적기 유형), Status(상태), Endpoint(엔드포인트), Endpoint Type(엔드포인트 유형), VPN Index(VPN 인덱스), Host Name(호스트 이름), Round Trip Time(왕복 시간))를 확인합니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Events(이벤트):

추적기에서 탐지된 플랩의 경우, 호스트 이름, 연결 지점 이름, 추적기 이름, 새 상태, 주소군, vpn id와 같은 세부 정보가 각 로그에 이 섹션에 입력됩니다.

엣지의 CLI에서:

```
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
```

DIA에 사용되는 인터페이스 엔드포인트 추적기

NAT DIA 엔드포인트 추적기는 주로 SD-WAN 에지 플랫폼의 NAT DIA 인터페이스를 통해 애플리케이션의 연결성을 모니터링하도록 지정됩니다.

DIA(Direct Internet Access) 사용 사례의 경우 NAT DIA 추적기를 사용하여 전송 측 인터페이스를 추적하고 사용 가능한 다른 전송 측 인터페이스 또는 SD-WAN 오버레이 터널(데이터 정책 사용)로 장애 조치를 트리거합니다. 이 기능은 20.3/17.3 릴리스부터 도입되었으며, NAT 폴백 기능 옵션은 20.4/17.4 릴리스부터 사용할 수 있습니다. 추적기에서 NAT DIA 인터페이스를 통해 로컬 인터넷을 사용할 수 없다고 판단하면 라우터는 서비스 VPN에서 NAT 경로를 철회하고 로컬 라우팅 컨피그레이션에 따라 트래픽을 다시 라우팅합니다. 추적기는 인터페이스에 대한 경로의 상태를 지속적으로 확인합니다. 경로가 다시 작동하는 것을 감지하면 라우터가 인터넷에 대한 NAT 경로를 다시 설치합니다. DIA 추적기에 대한 자세한 내용은 컨피그레이션 가이드를 참조하십시오.

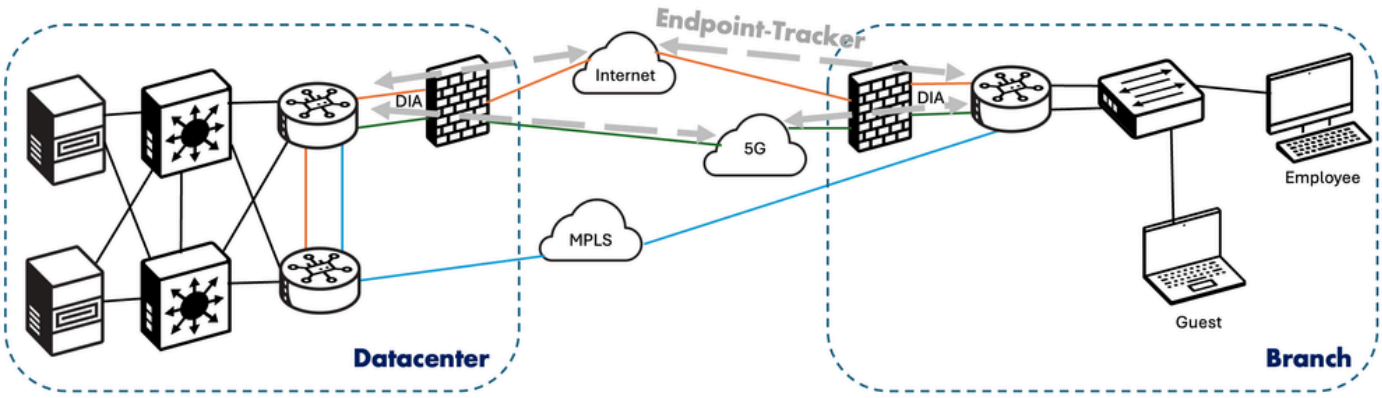
추적기 정의에서 NAT DIA 인터페이스를 통해 연결할 수 있는 엔드포인트의 IP 주소("endpoint-ip"로 구성)를 제공하거나 엔드포인트에 FQDN(Fully Qualified Domain Name)을 제공("endpoint-dns-name"으로 구성)하도록 선택할 수 있습니다.

여기서 사용되는 프로브 유형은 HTTP 요청 패킷이며, HTTP API 요청 PDU 스택과 매우 유사합니다. 사용되는 간격은 다음과 같습니다.

- 프로브 간격: 60초
- 승수: 180초(#retries은 3 = 3 x 60초이므로)
- 패킷/프로브 유형: HTTP

활용 사례

DIA는 인터넷으로 향하는 모든 브랜치 트래픽이 데이터 센터로 백홀되는 것을 방지하기 위해 브랜치 사이트에 최적화로 구축되는 경우가 많습니다. 그러나 브랜치 사이트에서 DIA를 사용하는 경우, NAT DIA 경로를 따라 연결할 수 없는 경우 블랙홀딩과 서비스 손실을 방지하기 위해 대체 경로로 돌아가야 합니다. 로컬 DIA 분리 실패 시 DC로 폴백(NAT 폴백을 사용하는 SD-WAN 오버레이를 통해)하려는 사이트의 경우. 지사 에지의 DIA 지원 인터페이스에서 이러한 인터페이스 기반 엔드포인트 추적기를 활용하여 백업/DC 경로로 페일오버를 시작하기 위해 장애를 탐지합니다. 이렇게 하면 DIA를 통해 인터넷 트래픽을 최적화하는 동시에 기업 내 업무 중단을 최소화하면서 인터넷 서비스의 고가용성을 실현할 수 있습니다.



설정

이 기능 집합을 활성화하려면 이러한 인터페이스 기반 엔드포인트 추적기를 수동으로 구성해야 합니다. 사용자가 선호하는 컨피그레이션 방법 유형에 따라 이를 구성하는 방법이 다음과 같습니다.

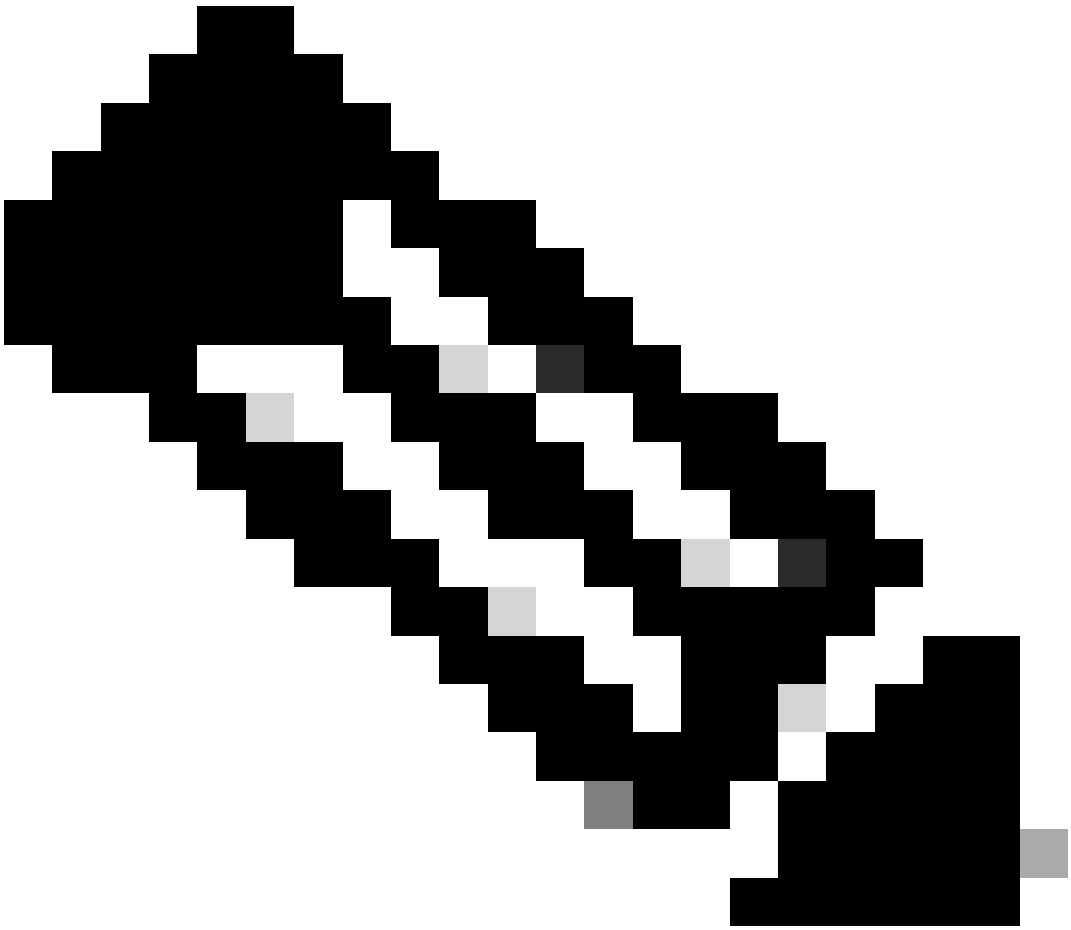
- 구성 그룹: Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Transport & Management Profile(전송 및 관리 프로파일) > Ethernet Interface(이더넷 인터페이스) > Add Feature(기능 추가) > Tracker(추적기):

1. 엔드포인트 추적기 이름을 정의합니다.

2. 엔드포인트 추적기 유형(HTTP-default와 ICMP 사이)을 선택합니다.

참고: ICMP 엔드포인트 추적기 유형은 20.13/17.13 이후에 도입되었습니다.

3. 엔드포인트를 선택합니다(엔드포인트 IP-default와 엔드포인트 DNS 이름 사이).



참고: Endpoint DNS Name(엔드포인트 DNS 이름)을 선택한 경우 Transport VPN 구성 프

로필을 사용하여 전송 VPN/VRF 아래에 올바른 DNS-server 또는 네임서버가 정의되어 있는지 확인하십시오.

4. 추적기 프로브를 보낼 주소 또는 DNS 이름(FQDN)을 입력합니다(형식은 이전 단계에 따라 다름).

5. (선택 사항) Probe Interval(프로브 간격)(기본값 = 60초) 및 Number of Retries(재시도 횟수)(기본값 = 3회)를 변경하여 오류 감지 시간을 유지하도록 선택할 수 있습니다.

- 레거시 구성:

1단계. 인터페이스 기반 엔드포인트 추적기의 정의: Configuration(구성) > Templates(템플릿) > Feature Templates(기능 템플릿) > System template(시스템 템플릿) > Tracker(추적기) 섹션:

1. Trackers(추적기) 하위 섹션에서 New Endpoint Tracker(새 엔드포인트 추적기) 버튼을 선택합니다.

2. 엔드포인트 추적기 이름을 정의합니다.

3. 여기서 DIA 사용 사례가 문제가 되므로 추적기 유형(interface-default와 static-route 사이)을 인터페이스로 선택합니다.

4. 엔드포인트 유형(IP Address-default와 DNS Name 사이)을 선택합니다.

5. 추적기 프로브가 전송되어야 하는 엔드포인트 IP 주소 또는 엔드포인트 DNS 이름을 입력합니다(형식은 이전 단계에 따라 다름).

6. (선택 사항) Probe Threshold(프로브 임계값)(기본값 = 300ms), Interval(간격)(기본값 = 60초) 및 Multiplier(기본값 = 3회)를 변경하도록 선택할 수 있습니다.

2단계. 인터페이스 기반 엔드포인트 추적기를 전송 VPN의 인터페이스에 적용합니다. Templates(템플릿) > Feature Templates(기능 템플릿) > Cisco VPN Interface Ethernet(Cisco VPN 인터페이스 이더넷) > Advanced(고급) 섹션:

1. 이전 단계 1에 정의된 엔드포인트 추적기의 이름을 추적기 필드에 입력합니다.

CLI의 관점에서 컨피그레이션은 다음과 같습니다.

```
(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
!
```

확인

명시적으로 구성된 엔드포인트 추적기에는 두 가지 확인 옵션이 있습니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Applications(애플리케이션) > Tracker(추적기):

Individual Tracker(개별 추적기)에서 확인하고 구성된 추적기 이름을 기준으로 추적기의 통계(Tracker Types(추적기 유형), Status(상태), Endpoint(엔드포인트), Endpoint Type(엔드포인트 유형), VPN Index(VPN 인덱스), Host Name(호스트 이름), Round Trip Time(왕복 시간))를 확인합니다.

- SD-WAN Manager에서 Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Events(이벤트):

추적기에서 탐지된 플랩의 경우, 호스트 이름, 연결 지점 이름, 추적기 이름, 새 상태, 주소군, vpn id와 같은 세부 정보가 각 로그에 이 섹션에 입력됩니다.

엣지의 CLI에서:

```
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 터널/SSE에 사용되는 인터페이스 엔드포인트 추적기

엔드포인트 추적기가 SIG 터널/SSE 활용 사례에 사용되는 경우, 주로 기업이 Cisco, Cloudflare, Netskope, ZScalar 등과 같은 SIG(Secure Internet Gateway) 또는 SSE(Secure Service Edge) 제공업체의 도움을 받아 현재 손쉽게 사용할 수 있는 클라우드 기반 보안 스택 제품을 찾고 있음을 나타냅니다. SIG 터널과 SSE는 모두 클라우드 보안 구축 모델의 일부로 제공되며, 지사는 클라우드를 사용하여 필요한 보안 솔루션을 제공합니다. SIG Tunnels 활용 사례는 Cisco Catalyst SD-WAN을 그러한 SIG 제공자(20.4/17.4 릴리스)와 통합하기 위한 초기 사례였지만, 클라우드 제공 보안 제품의 진화에 따라 SSE 활용 사례(20.13/17.13 릴리스)가 도입되었습니다. 이 활용 사례는 Cisco(Cisco Secure Access를 통해) 및 ZScalar와 같은 제공자의 활용 사례를 다루기 위한 것입니다.

IT는 민첩성을 보호하고 연결할 수 있는 안정적이고 명시적인 접근 방식이 필요합니다. 이제는 원격 직원이 Microsoft 365 및 Salesforce와 같은 클라우드 애플리케이션에 직접 액세스하여 보안을 강화하는 것이 일반적입니다. 하청업체, 파트너, IoT(Internet of Things) 장치 등에 네트워크 액세스가 요구됨에 따라 클라우드 기반 네트워킹 및 보안에 대한 수요가 매일 증가하고 있습니다. 클라우드 에지에서 최종 장치에 더 가까운 네트워크 및 보안 기능의 통합은 Cisco SASE라는 서비스 모델로 알려져 있습니다. Cisco SSE(Secure Service Edge)는 클라우드에서 제공되는 네트워킹 및 보안 기능을 결합하여 언제 어디서나 모든 사용자 또는 장치에 대해 애플리케이션에 안전하게 액세스할 수 있도록 합니다. SSE는 조직이 작업 환경의 보안 상태를 개선하는 동시에 최종 사용자 및 IT 부서의 복잡성을 줄일 수 있도록 지원하는 네트워크 보안 접근 방식입니다. SIG 터널/SSE 추적기에 대한 자세한 내용은 구성 설명서를 참조하십시오.

활용 사례

이러한 인터페이스 기반 엔드포인트 추적기는 잘 알려진 SaaS 애플리케이션 URL 엔드포인트 또는 문제가 되는 특정 URL 엔드포인트를 추적하고자 하는 SIG 터널/SSE 사용 사례에 사용됩니다. 현재 SSE는 SSE 아키텍처가 SSE 코어 기능과 SD-WAN 기능으로 분할되었기 때문에 더 자주 사용되는 시나리오입니다. 그런 다음 사이트(이 경우 DC)에서 생성된 IPSec 터널 내에서 활성 역할과 대기 역할 중에서 선택할 수 있습니다. 사용자는 각 터널 인터페이스 아래에 추적기를 연결할 수 있습니다.

Cisco Secure Access와 같은 SSE 제공자의 경우(Cisco에서 사용), 암시적 엔드포인트 추적기가 기본적으로 구성됩니다. 그러나 사용자 지정 엔드포인트 추적기를 생성하고 이를 IPSec 터널 인터페이스에 연결할지 선택할 수 있습니다. SSE에서 사용되는 기본/암시적 엔드포인트 추적기의 매개변수는 다음과 같습니다.

Cisco SSE:

추적기 이름: 기본추적기

추적 중인 끝점: http://service.sig.umbrella.com

엔드포인트 유형: API_URL

임계값: 300밀리초

곱하기: 3

간격: 60초

ZScaler SSE의 경우:

추적기 이름: 기본추적기

추적 중인 끝점: http://gateway.zscalerthree.net/vpnte

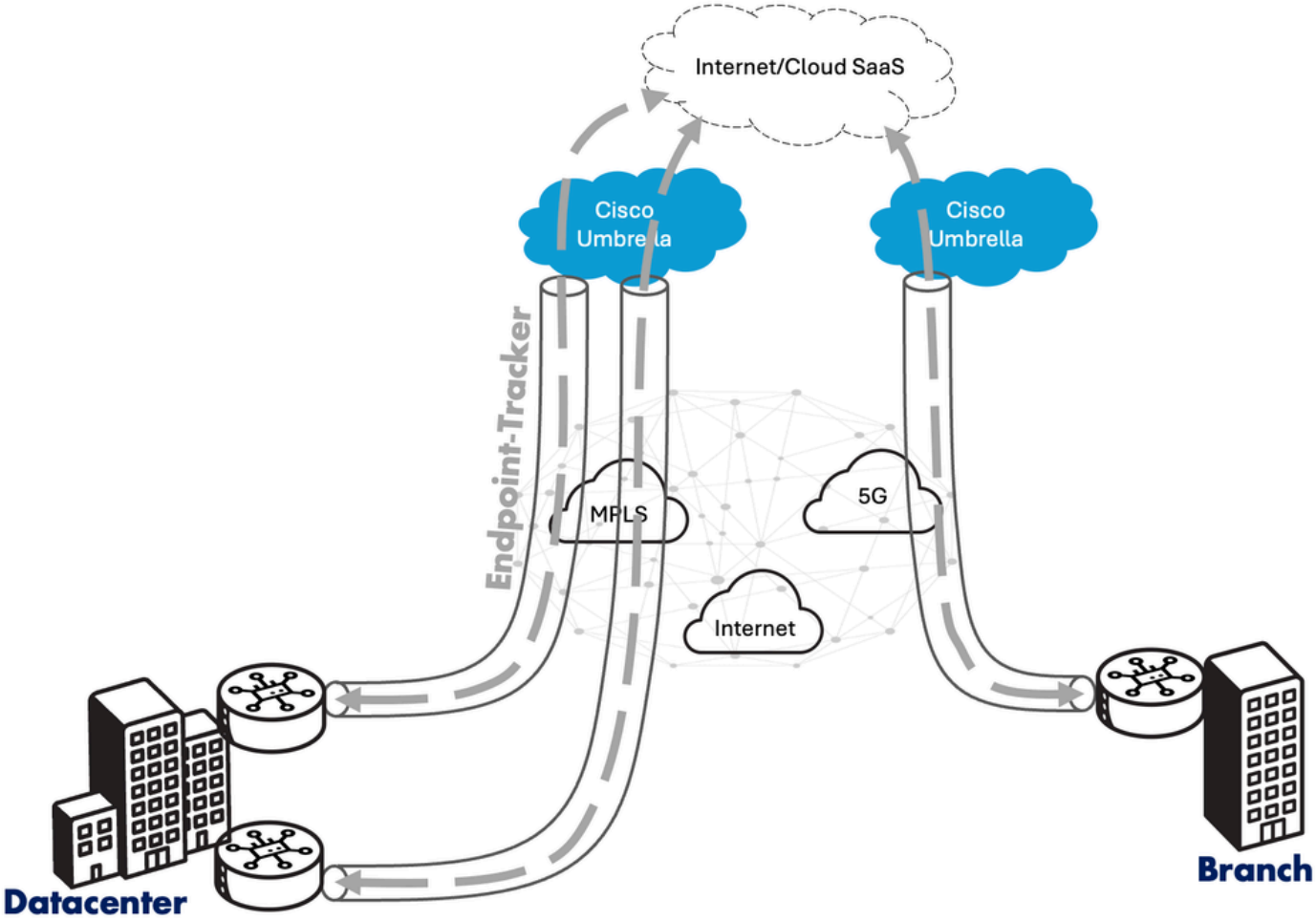
엔드포인트 유형: API_URL

임계값: 300밀리초

승수: 3

간격: 60초

SIG 터널의 경우 기본/암시적 엔드포인트 추적기가 정의되지 않습니다. 따라서 사용자는 SIG 제공자-클라우드를 향하는 IPSec 터널 인터페이스를 추적하고자 하는 경우 인터페이스 기반 엔드포인트 추적기를 수동으로 구성해야 합니다.



설정

SSE 제공자의 경우, 사용자는 엔드포인트 추적기를 명시적으로 정의하지 않아도 됩니다(원하는 경우 제외). 그러나 워크플로는 컨피그레이션 유형에 따라 다릅니다.

사전 요구 사항으로 SIG/SSE 자격 증명 관리 > 설정 > 외부 서비스 > 클라우드 자격 증명을 정의해야 합니다.

1. Cloud Provider Credentials(Cloud Provider Credentials)에서 Umbrella 또는 Cisco SSE(또는 둘 다) 옵션을 전환합니다.

2. 조직 ID, API 키, 비밀과 같은 매개변수를 정의합니다.

Configuration(컨피그레이션) > Policy Groups(정책 그룹) > Secure Internet Gateway/Secure Service Edge(보안 인터넷 게이트웨이/보안 서비스 에지)를 설정합니다.

1. Add Secure Internet Gateway 또는 Add Secure Service Edge(보안 인터넷 게이트웨이 추가 또는 보안 서비스 에지 추가)를 클릭합니다.

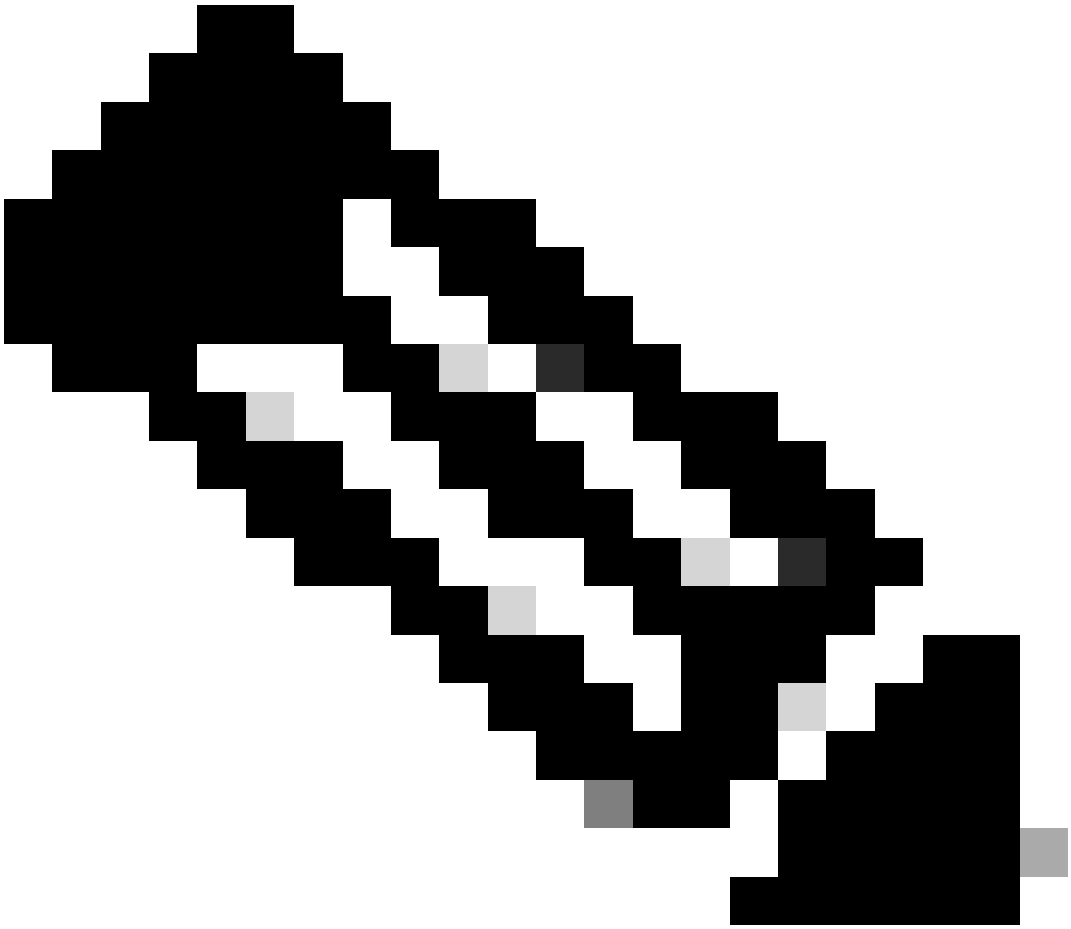
2. 이름과 내용을 정의합니다.

3. SIG/SSE Provider(SIG/SSE 제공자) 아래의 라디오 버튼 중 하나(Umbrella 또는 Cisco SSE)를 선택합니다.

4. [추적기] 섹션에서 추적기 프로브의 소스에 사용되는 소스 IP 주소를 정의합니다.

5. 명시적/사용자 지정 끝점 추적기를 정의하도록 선택한 경우 [추적기 추가]를 클릭한 다음 끝점 추적기의 매개 변수(이름, 끝점 API URL, 임계값, 프로브 간격 및 승수)를 입력합니다.

6. Configuration 섹션에서 매개변수를 정의할 수 있는 터널 인터페이스를 생성합니다(예: Interface Name, Description, Tracker, Tunnel Source Interface, Datacenter Primary/Secondary).



참고: 6단계에서는 정의된 엔드포인트 추적기를 각 IPSec 터널에 연결할 수 있는 옵션이 제공됩니다. 이 필드는 선택 항목입니다.

---

7. High Availability(고가용성) 섹션에서 인터페이스 쌍을 생성하고 액티브 인터페이스 및 백업 인터페이스와 각각의 가중치를 정의합니다. 그런 다음 앞서 구성된 정책 그룹을 관련 에지에 적용합니다.

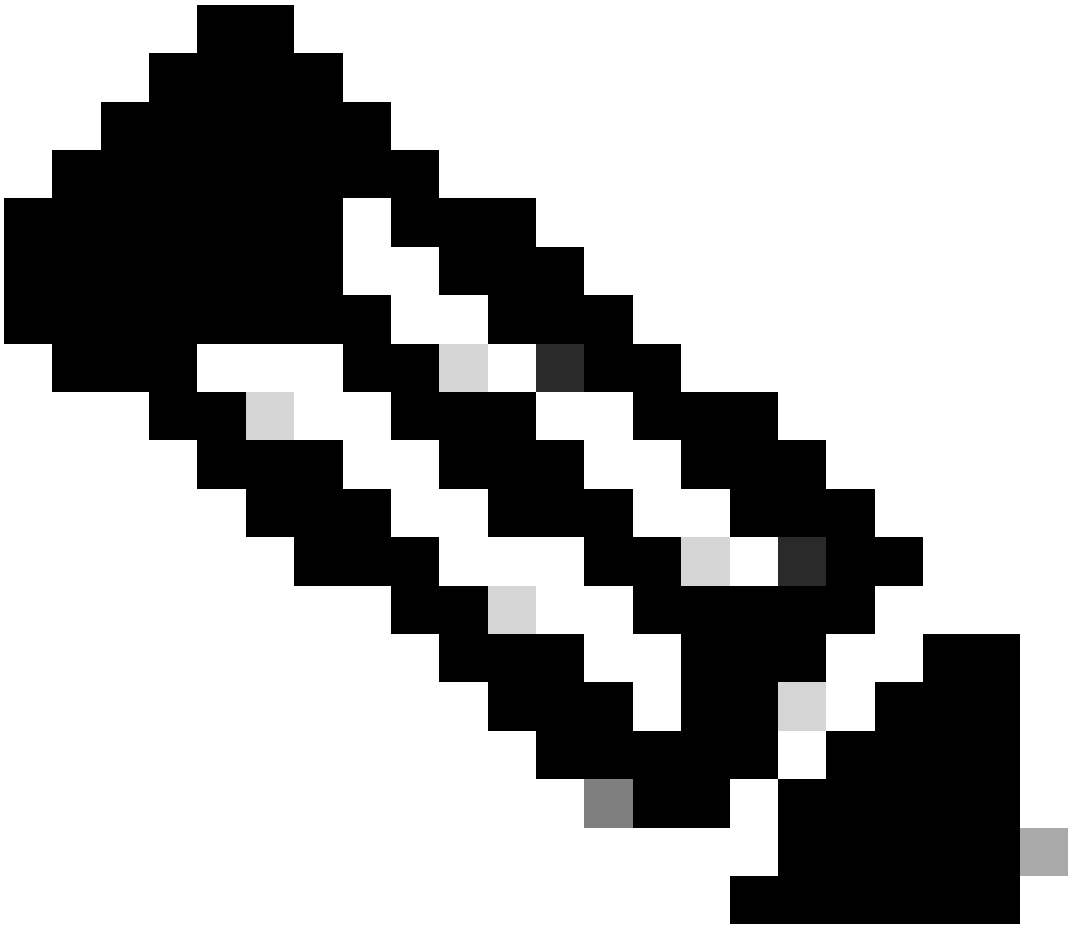
레거시 컨피그레이션 설정 > 템플릿 > 기능 템플릿 > Cisco Secure Internet Gateway 기능 템플릿:

1. SIG 제공자(Umbrella, ZScalar 또는 Generic) 아래의 라디오 버튼 중 하나를 선택합니다.

2. Tracker (BETA) 섹션에서 추적기 프로브를 소싱하는 데 사용되는 소스 IP 주소를 정의합니다.

5. 명시적/사용자 지정 끝점 추적기를 정의하도록 선택한 경우 New Tracker를 누르고 끝점 추적기의 매개 변수(이름, 끝점 API url, 임계값, 간격 및 승수)를 입력합니다.

6. Configuration 섹션 아래에서 Add Tunnel(터널 추가)을 클릭하여 터널 인터페이스를 생성합니다. 여기서 매개변수(인터페이스 이름, 설명, 추적기, 터널 소스 인터페이스, 데이터 센터 기본/보조)를 정의할 수 있습니다.



참고: 6단계에서는 정의된 엔드포인트 추적기를 각 IPSec 터널에 연결할 수 있는 옵션이 제공됩니다. 이 필드는 선택 항목입니다.

---

7. High Availability 섹션에서 액티브 인터페이스와 백업 인터페이스를 각각의 가중치와 함께 정의합니다.

CLI의 관점에서 컨피그레이션은 다음과 같습니다.

```
(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
!
```

확인

명시적으로 구성된 엔드포인트 추적기의 확인 옵션이 있습니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Applications(애플리케이션) > Tracker(추적기):

Individual Tracker 아래에서 확인하고 구성된 Tracker Name(추적기 이름)을 기준으로 추적기의 통계(Tracker Types(추적기 유형), Status(상태), Endpoint(엔드포인트), Endpoint Type(엔드포인트 유형), VPN Index(VPN 인덱스), Host Name(호스트 이름), Round Trip Time(왕복 시간))를 확인합니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Events(이벤트):

추적기에서 탐지된 플랩의 경우, 호스트 이름, 연결 지점 이름, 추적기 이름, 새 상태, 주소군, vpn id와 같은 세부사항이 이 섹션에 채워집니다.

엣지의 CLI에서:

```
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 2.0에 사용되는 인터페이스 엔드포인트 추적기

20.13/17.13 릴리스에 도입된 서비스 패브릭 2.0 추적은 서비스 삽입 1.0 추적의 향상된 변형입니다. 사용자는 이를 통해 더 큰 범위에서 추적기를 사용자 정의할 수 있습니다. 기본 동작은 이전 버전의 Service Insertion(1.0)에서 유지되며, 기본적으로 추적기는 rx/tx당 service-HA 쌍으로 각 서비스 주소(또는 전달 주소)를 정의하여 시작됩니다. 그러나 Service Insertion 2.0에서는 추적 주소(추적된 항목의 IP/엔드포인트)를 전달 주소(일반적으로 서비스 주소)에서 분리할 수 있습니다. 이 작업은 VPN 수준에 정의된 사용자 지정 끝점 추적기를 사용하여 수행됩니다. 서비스 패브릭 2.0 추적기에 대한 자세한 내용은 구성 설명서를 참조하십시오.

사용자가 기본 추적기를 사용하도록 선택하는 경우 추적기 프로브의 사양은 다음과 같습니다.

- 안녕하십니까? 30초마다 프로브 1개
- 승수: 3회
- 패킷/프로브 유형: ICMP 에코/에코-응답

사용자가 사용자 지정 추적기를 사용하도록 선택하는 경우 추적기 프로브의 사양은 다음과 같습니다.

- 안녕하십니까? 60초마다 프로브 1개
- 승수: 3회
- 패킷/프로브 유형: ICMP 에코 요청/응답

활용 사례

앞의 섹션에서 언급한 Service Insertion 1.0의 활용 사례도 여기에 적용됩니다.

설정

Service Insertion 2.0에는 워크플로 기반 컨피그레이션이 지원되는데, 이는 마법사 중심 접근 방식으로서 표준 컨피그레이션 그룹 워크플로 단계를 준수하면서 사용자 경험을 단순화하는 데 도움이 됩니다.

1. "구성" > "서비스 삽입" > "서비스 체인 정의" 섹션에서 서비스 체인 - 구성 그룹을 정의합니다.

a. Add Service Chain Definition(서비스 체인 정의 추가) 버튼을 클릭합니다.

b. 서비스의 이름 및 설명에 대한 세부사항을 입력합니다.

c. 드롭다운 목록에서 선택하여 목록 형식인 서비스 유형을 입력합니다.

2. "구성" > "서비스 삽입" > "서비스 체인 구성" 섹션에서 서비스 체인 인스턴스 - 구성 그룹을 정의합니다.

a. Add Service Chain Configuration을 클릭합니다.

b. Service Chain Definition(서비스 체인 정의) 단계에서 Select Existing(기존 선택)이라는 라디오 버튼을 선택하고 이전에 정의한 서비스를 선택합니다.

c. 서비스 체인 구성 시작 단계의 이름 및 설명을 제공합니다.

d. 수동으로 연결된 서비스에 대한 서비스 체인 컨피그레이션 단계에서 서비스 체인 VPN-ID를 선택합니다.

e. 그런 다음 서비스 체인 인스턴스(하위 탭에 표시됨)에 정의된 각 서비스에 대해 서비스 세부사항 아래에 첨부 유형(IPv4, IPv6 또는 Tunnel Connected)을 제공합니다.

f. Advanced(고급) 확인란을 선택합니다. 활성 백업/HA 활용 사례가 필요한 경우(백업 노브의 매개변수 추가 활성화) 또는 사용자 지정 엔드포인트 추적기를 정의해야 하는 경우에도(사용자 지정 추적기 노브도 활성화).

g. 이그레스(tx) 트래픽이 하나의 인터페이스를 통해 서비스로 이동하고 서비스의 반환 트래픽이 다른 인터페이스를 통해 인그레스(rx)되는 시나리오가 있는 경우 다른 인터페이스 노브에서 Traffic from service received를 켭니다.

h. Advanced 및 Custom Tracker 노브가 활성화된 상태에서 서비스 IPv4 주소(전달 주소), SD-WAN 라우터 인터페이스(서비스가 연결된) 및 추적기 엔드포인트(추적 주소)를 정의합니다. 또한 (편집 버튼을 클릭하여) 간격 및 승수와 같은 사용자 지정 추적기 매개변수를 수정할 수 있습니다.

i. 이후에 정의된 각 서비스에 대해 (e), (f), (g) 및 (h) 단계를 반복합니다.

3. Configuration(구성) > Configuration Groups(구성 그룹) > Service Profile(서비스 프로파일) > Service VPN(서비스 VPN) > Add Feature(기능 추가) > Service Chain Attachment Gateway(서비스 체인 연결 게이트웨이)에서 Edge - Configuration(에지 - 구성) 그룹의 구성 프로파일에 서비스 체인 인스턴스를 연결합니다.

a. 이 Service Chain Attachment Gateway 소포에 이름 및 설명을 입력하십시오.

b. 1단계에서 이전에 정의한 서비스 체인 정의를 선택합니다.

c. 2단계에서 수행한 세부 정보를 다시 추가/확인합니다. 추적기 정의의 경우, 이전 2단계와의 유일한 차이점은 추적기 이름을 지정하고 추적기 유형(service-icmp에서 ipv6-service-icmp로)을 선택할 수 있다는 것입니다.

CLI의 관점에서 컨피그레이션은 다음과 같습니다.

```
!
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
!
```

확인

- SD-WAN Manager Monitor(SD-WAN 관리자 모니터) > Devices(디바이스) > {select Device-Name} > Applications(애플리케이션) > Tracker(추적기)에서 다음을 수행합니다.

Individual Tracker 아래에서 확인하고 구성된 Tracker Name(추적기 이름)을 기준으로 추적기의 통계(Tracker Types(추적기 유형), Status(상태), Endpoint(엔드포인트), Endpoint Type(엔드포인트 유형), VPN Index(VPN 인덱스), Host Name(호스트 이름), Round Trip Time(왕복 시간))를 확인합니다.

- SD-WAN Manager Monitor(SD-WAN 관리자 모니터) > Devices(디바이스) > {select Device-Name} > Events(이벤트)에서 다음을 수행합니다.

추적기에서 탐지된 플랩의 경우, 호스트 이름, 연결 지점 이름, 추적기 이름, 새 상태, 주소군, vpn id와 같은 세부사항이 이 섹션에 채워집니다.

엣지의 CLI에서:

```
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
```

고정 경로 추적에 사용되는 고정 경로 엔드포인트 추적기(서비스 측)

두 번째 유형의 엔드포인트 추적기를 고정 경로 기반 엔드포인트 추적기라고 합니다. 이름 자체에서 알 수 있듯이 이러한 유형의 추적기는 주로 서비스 측 VPN에 정의된 고정 경로의 다음 홉 주소를 추적하는 데 사용됩니다. 기본적으로 모든 "연결됨" 및 "고정" 경로 유형은 OMP 프로토콜로 광고됩니다. 즉, 해당 서비스 VPN을 포함하는 모든 원격 사이트에서 해당 대상 접두사(시작 사이트의 TLOC에 대한 다음 홉 지점)를 인식하게 됩니다. 시작 사이트는 특정 고정 경로가 시작된 사이트입니다.

그러나 고정 경로의 next-hop 주소에 연결할 수 없는 경우 경로가 OMP로 광고되는 것을 멈추지 않습니다. 이로 인해 트래픽이 원래 사이트로 향하는 흐름에 블랙홀화되는 문제가 발생할 수 있습니다. 따라서 다음 홉 주소에 도달할 수 있을 때만 OMP에 대한 고정 경로의 광고를 보장하기 위해 고정 경로에 추적기를 연결해야 합니다. 이 기능은 기본 IP 주소 유형 고정 경로 기반 엔드포인트 추적기를 위해 20.3/17.3 릴리스에 도입되었습니다. 20.7/17.7 이후 릴리스에서는 다음 홉 IP 주소의 특정 TCP 또는 UDP 포트에만 추적기 프로브를 전송하기 위한 지원이 추가되었습니다(추적을 위해 특정 포트만 열기 위해 방화벽을 사용하는 경우). 고정 경로 추적기에 대한 자세한 내용은 구성 설명

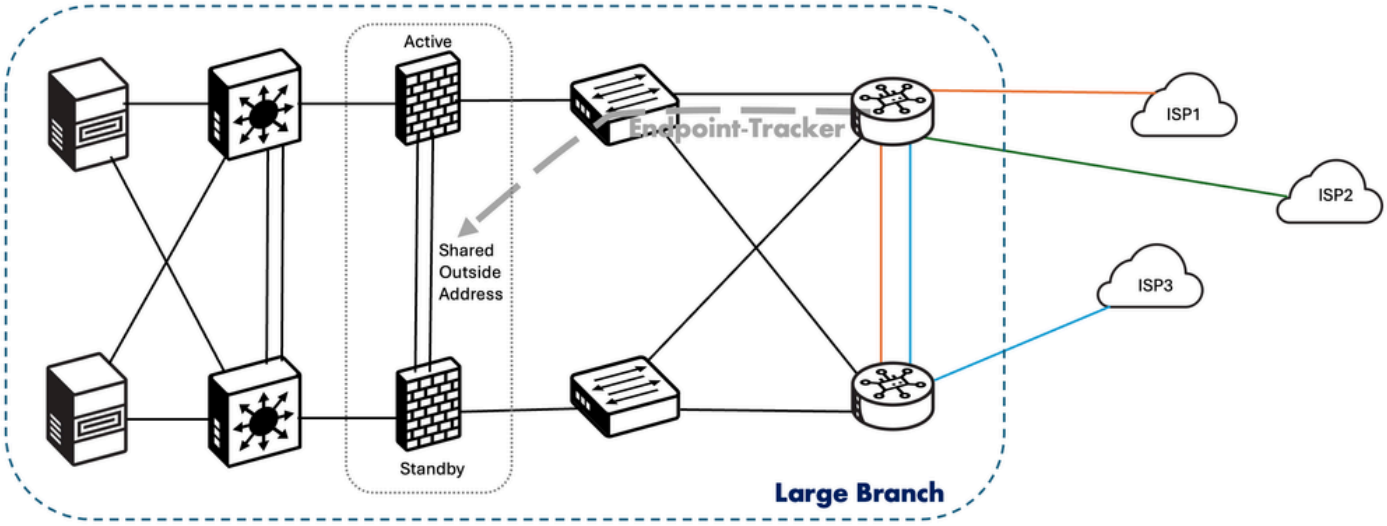
서를 참조하십시오.

여기에서 사용되는 프로브의 유형은 단순 ICMP 에코 요청 패킷입니다. 사용되는 간격은 다음과 같습니다.

- 안녕하십니까? 60초
- Holdtime: 180초(#retries은 3 = 3 x 60초이므로)
- 패킷/프로브 유형: ICMP 에코/에코-응답

활용 사례

이러한 유형의 고정 경로 기반 엔드포인트 추적기는 고정 경로에서 next-hop 주소의 서비스 측 추적에 사용됩니다. 한 가지 일반적인 시나리오는 액티브/스탠바이 방화벽 쌍에 해당하는 LAN측 next-hop 주소를 추적하는 것입니다. 이는 외부 인터페이스가 "액티브" 방화벽의 역할을 수행하는 외부 IP 주소를 기반으로 합니다. 방화벽 규칙이 엄격하게 적용되는 경우, 특정 포트만 사용 사례에 따라 열리면 고정 경로 추적기를 사용하여 LAN 측 방화벽 외부 인터페이스에 속하는 다음 홉 IP 주소에 대한 특정 TCP/UDP 포트를 추적할 수 있습니다.



설정

이 기능 집합을 활성화하려면 이러한 고정 경로 기반 엔드포인트 추적기를 수동으로 구성해야 합니다. 사용자가 선호하는 컨피그레이션 방법 유형에 따라 이를 구성하는 방법이 다음과 같습니다.

- Configuration(컨피그레이션) 그룹 Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로파일) > Service VPN(서비스 VPN) > Add Feature(기능 추가) > Tracker(추적기):

1. 정의 중인 새 (엔드포인트) 추적기에 대한 이름, 설명 및 추적기 이름을 제공합니다.

2. next-hop IP 주소만 추적해야 하는지(주소 라디오 버튼 선택) 또는 특정 TCP/UDP 포트만 추적해야 하는지(프로토콜 라디오 버튼 선택)에 따라 엔드포인트 유형을 선택합니다.

3. IP 주소 형식으로 주소를 입력합니다. 이전 단계에서 엔드포인트 유형으로 Protocol을 선택한 경우 프로토콜(TCP 또는 UDP)과 포트 번호도 입력합니다.

4. 필요한 경우 프로브 간격, 재시도 횟수 및 레이턴시 제한에 대해 제공된 기본값을 변경할 수 있습니다.

- Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로파일) > Service VPN(서비스 VPN) > Route(경로) 섹션:

1. Add IPv4/IPv6 Static Route(IPv4/IPv6 고정 경로 추가) 버튼을 선택합니다.

2. 네트워크 주소, 서브넷 마스크, 다음 홉, 주소, 광고 등의 세부 정보를 입력합니다.

3. Add Next Hop With Tracker(추적기와 함께 다음 홉 추가) 버튼을 클릭합니다.

4. Next-Hop 주소, AD를 다시 입력하고 이전에 생성한(엔드포인트) 추적기 이름 드롭다운에서 선택합니다.

- 레거시 구성 > 템플릿 > 기능 템플릿 > 시스템 템플릿 > 추적기 섹션:

1. 새 끝점 추적기 단추를 선택합니다.

2. 정의할 새(엔드포인트) 추적기의 이름을 제공합니다.

3. Tracker Type(추적기 유형) 라디오 버튼을 static-route로 변경합니다.

4. 엔드포인트 유형을 next-hop IP 주소로 선택합니다(IP 주소 라디오 버튼 선택).

5. IP 주소 형식으로 엔드포인트 IP를 입력합니다.

6. 필요한 경우 프로브 간격, 재시도 횟수 및 레이턴시 제한에 대해 제공된 기본값을 변경할 수 있습니다.

- Configuration(컨피그레이션) > Templates(템플릿) > Feature Templates(기능 템플릿) > Cisco VPN (service-side only) > IPv4/IPv6 Route(IPv4/IPv6 경로) 섹션:

1. New IPv4/IPv6 Route(새 IPv4/IPv6 경로) 버튼을 선택합니다.

2. 접두사, 게이트웨이 등 세부사항을 입력합니다.

3. [추적기와 함께 다음 홉 추가] 단추를 클릭합니다.

4. Next-Hop Address, AD(Distance)를 다시 입력하고 이전에 생성한 (엔드포인트) 추적기 이름을 수동으로 입력합니다.

CLI의 관점에서 컨피그레이션은 다음과 같습니다.

```
(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
!
```

확인

명시적으로 구성된 엔드포인트 추적기의 확인에는 두 가지 영역이 있습니다.

- SD-WAN Manager Monitor(SD-WAN 관리자 모니터) > Devices(디바이스) > {select Device-Name} > Real Time(실시간)에서 다음을 수행합니다.

1. Device Options(디바이스 옵션)에서 "Endpoint Tracker Info(엔드포인트 추적기 정보)"를 입력합니다.

2. Individual Tracker(Attach Point Name)에서 확인하고 구성된 Tracker Name에 따라 추적기의 통계(Tracker State(추적기 상태), Associated Tracker Record Name(연결된 추적기 레코드 이름), Latency in mx from device to endpoint(디바이스에서 엔드포인트로의 지연 시간), Last Updated timestamp(마지막 업데이트된 타임스탬프))를 확인합니다.

- SD-WAN Manager Monitor(SD-WAN 관리자 모니터) > Devices(디바이스) > {select Device-Name}(디바이스 이름 선택) > Events(이벤트)에서 다음을 수행합니다.

추적기에서 탐지된 플랩의 경우, 호스트 이름, 연결 지점 이름, 추적기 이름, 새 상태, 주소군, vpn id와 같은 세부 정보가 각 로그에 이 섹션에 입력됩니다.

엣지의 CLI에서:

```
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 추적에 사용되는 인터페이스 개체 추적기

개체 추적기는 자동 모드 사용을 위해 설계된 추적기입니다(사용 사례). 이러한 추적기는 VRRP 기반 인터페이스/터널 추적에서 서비스 VPN NAT 추적에 이르기까지 다양한 사용 사례를 가지고 있습니다.

VRRP 추적 활용 사례의 경우 VRRP 상태는 터널 링크 상태를 기반으로 결정됩니다. 터널이나 인터페이스가 기본 VRRP에서 다운된 경우 트래픽은 보조 VRRP로 전달됩니다. LAN 세그먼트의 보조 VRRP 라우터가 기본 VRRP가 되어 서비스 측 트래픽에 대한 게이트웨이를 제공합니다. 이 활용 사례는 service-VPN에만 적용되며 SD-WAN 오버레이(SSE의 경우 인터페이스 또는 터널)에 장애가 발생할 경우 LAN 측에서 VRRP 역할을 장애 조치할 수 있습니다. VRRP 그룹에 추적기를 연결할 경우, 개체 추적기만 사용할 수 있습니다(엔드포인트 추적기는 아님). 이 기능은 Cisco Catalyst SD-WAN Edge의 20.7/17.7 릴리스에서 도입되었습니다.

추적기에서 사용하는 프로브가 없습니다. 대신, 추적기 상태(up/down)를 결정하기 위해 라인 프로토콜 상태를 사용합니다. 인터페이스 라인 프로토콜 기반 추적기에는 반응 간격이 없습니다. 인터페이스/터널 라인 프로토콜이 DOWN되는 순간 트랙 상태도 DOWN 상태가 됩니다. 그런 다음 종료 또는 감소 작업에 따라 VRRP 그룹이 다시 통합됩니다. VRRP 인터페이스 추적기에 대한 자세한 내용은 구성 가이드를 참조하십시오.

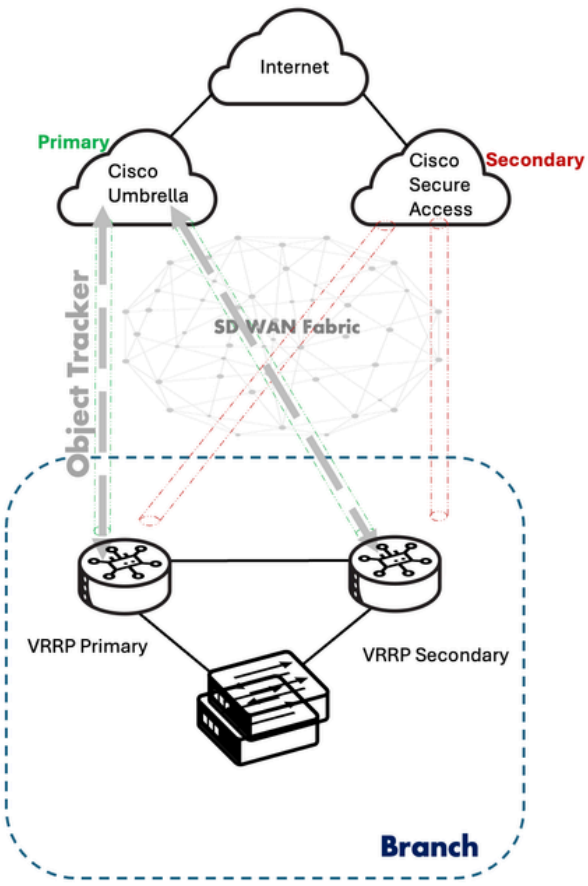
활용 사례

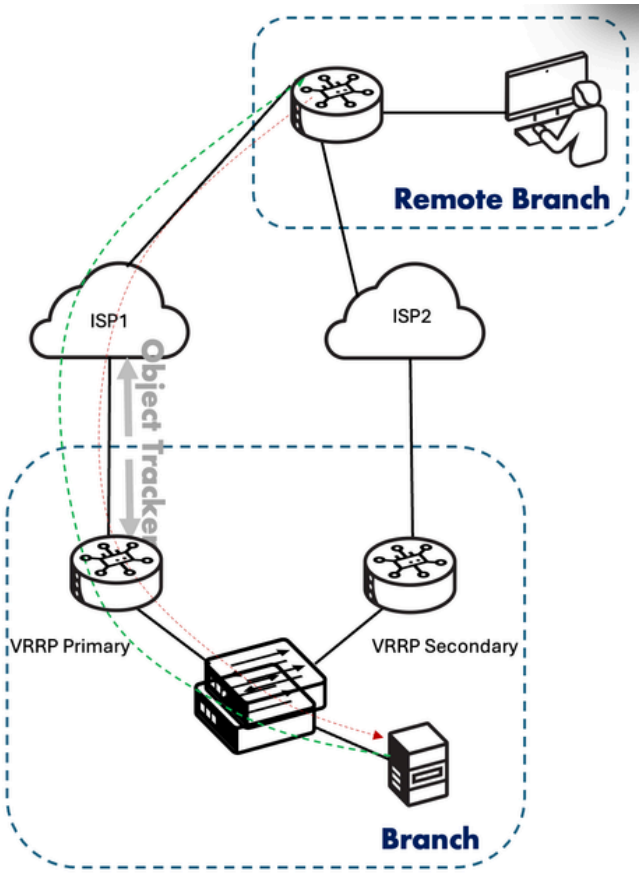
VRRP 기반 인터페이스 추적을 구현하는 데 필요한 기준에 따라 여러 사용 사례가 있습니다. 현재 지원되는 두 가지 모드는 (i) 인터페이스(로컬 TLOC로 바인딩된 모든 터널 인터페이스 의미) 또는 (ii) SIG 인터페이스(SIG 터널 인터페이스와 관련)입니다. 각각의 경우, 추적되는 부분은 인터페이스 라인-프로토콜이다.

인터넷이 연결된 듀얼 라우터: 트랙 개체가 VRRP 그룹에 바인딩되어 있습니다. 추적기의 객체(이 경우 SIG 터널 인터페이스)가 다운되는 경우, 이는 VRRP 기본 라우터에 통지하여 기본 라우터에서 백업 라우터로 상태 전환을 트리거하고 백업 라우터가 기본 라우터가 되도록 합니다. 이 상태 변경은 두 가지 작업 유형을 통해 영향을 받거나 트리거될 수 있습니다.

1. 감소: 여기서 VRRP VIP가 구성된 인터페이스의 VRRP 우선 순위는 추적 객체 상태가 UP에서 DOWN으로 전환될 때 특정 값만큼 감소되거나 감소됩니다.
2. 셧다운: 이는 트랙 개체 상태가 UP에서 DOWN으로 전환되는 경우 적용된 인터페이스에서 VRRP 프로세스가 종료되는 방법입니다. 비대칭 전달의 인스턴스가 있는 사용 사례에서는 이 방법을 사용하지 않는 것이 좋습니다.

TLOC 변경 환경 설정: 다른 SDWAN 사이트에서 서비스 VPN에서 VRRP가 실행되는 사이트로 비대칭 트래픽이 들어오는 것을 방지하기 위해 VRRP 기본 라우터의 TLOC 환경 설정은 구성된 경우 1씩 부스팅됩니다. 컨피그레이션 그룹 아래에서 이 값을 수정할 수도 있습니다. 이렇게 하면 WAN에서 LAN으로의 트래픽이 VRRP 기본 라우터 자체에서 끌어옵니다. LAN에서 WAN으로의 트래픽은 VRRP Primary의 VRRP 메커니즘에 의해 끌어당겨집니다. 이 기능은 VRRP 인터페이스 추적기와 무관합니다. CLI 관점에서 선택적 명령(tloc-change-pref)입니다.





설정

객체 추적기의 컨피그레이션은 레거시 컨피그레이션의 시스템 템플릿을 통해 수행된 다음, 서비스-VPN 이더넷 인터페이스 기능 템플릿 아래의 각 VRRP 그룹에 객체 추적기를 연결합니다. 구성 그룹에서 각 서비스 프로파일 이더넷 인터페이스 프로파일에 객체 추적기를 추가하는 옵션을 직접 가져옴으로써 이 메커니즘이 간소화되었습니다. 사용자가 선호하는 구성 방법 유형에 따라 이 메커니즘을 구성하는 방법이 다음과 같습니다.

- Configuration(컨피그레이션) 그룹 Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로필) > Ethernet Interface(이더넷 인터페이스) > Add Feature(기능 추가) > Object Tracker(개체 추적기):

1. 정의 중인 새 객체 추적기의 Name(이름) 및 Description(설명)을 제공합니다.
2. Tracker Type(추적기 유형)을 선택합니다(Interface 및 SIG 중).
3. 객체 추적기 ID를 할당합니다.
4. 인터페이스 이름(2단계에서 선택한 옵션에 따라 다름)을 입력합니다.

- Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로파일) > Ethernet Interface(이더넷 인터페이스) > VRRP 섹션:

1. IPv4 Settings(IPv4 설정)에서 Add VRRP IPv4(VRRP IPv4 추가)를 클릭합니다.
2. VRRP 그룹 ID를 정의하고 이 서비스측 이더넷 인터페이스에 대한 로컬 우선순위를 제공합니다.
3. VRRP VIP(가상 IP) 주소를 제공합니다.
4. TLOC 기본 설정 변경 노브를 활성화하고 TLOC 기본 설정 변경 값을 제공합니다(비대칭 라우팅 처리).
5. Add VRRP Tracking Object(VRRP 추적 개체 추가)를 클릭합니다.
6. Associate Object Tracker(개체 추적기 연결) 아래에서 이전에 만든 개체 추적기(이름 기준)의 드롭다운에서 선택합니다
7. 추적기 작업(종료 또는 감소)을 선택합니다.
8. 7단계에서 선택한 옵션에 따라 감소 값을 입력합니다.

- 레거시 구성 > 템플릿 > 기능 템플릿 > 시스템 > 추적기 섹션:

1. 새 개체 추적기 단추를 클릭합니다.
2. Tracker Type(추적기 유형)을 선택합니다(Interface 및 SIG 중).
3. 객체 ID를 할당합니다.
4. 인터페이스 이름(2단계에서 선택한 옵션에 따라 다름)을 입력합니다.

- Configuration(컨피그레이션) > Templates(템플릿) > Ethernet Interface(이더넷 인터페이스)(서비스 측에 속함) > VRRP 섹션:

1. New VRRP(새 VRRP) 버튼을 클릭합니다.
2. VRRP 그룹 ID를 정의하고 이 서비스 측 이더넷 인터페이스에 대한 로컬 우선순위(선택 사항이며 기본값 100이 선택됨)를 제공합니다.
3. VRRP VIP(가상 IP) 주소를 제공합니다.
4. TLOC 기본 설정 변경 노브를 활성화하고 TLOC 기본 설정 변경 값을 제공합니다(비대칭 라우팅을 처리할 수 있도록).

5. Object Tracker(개체 추적기)에서 Add Tracking Object(추적 개체 추가)를 클릭합니다.
6. 시스템 템플릿에 정의된 객체 추적기 ID를 입력합니다.
7. 추적기 작업(종료 또는 감소)을 선택합니다.
8. 7단계에서 선택한 옵션에 따라 감소 값을 입력합니다.

CLI의 관점에서 컨피그레이션은 다음과 같습니다.

```
(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
!
```

확인

VRRP 사용 사례에 대해 명시적으로 구성된 개체 추적기를 확인하는 두 가지 옵션이 있습니다.

- SD-WAN Manager Monitor(SD-WAN 관리자 모니터) > Devices(디바이스) > {select Device-Name} > Real Time(실시간)에서 다음을 수행합니다.

1. Device Options(디바이스 옵션)에서 "VRRP Information(VRRP 정보)"을 입력합니다.

2. Individual VRRP Group(Group ID)에서 확인하고 구성된 Object Tracker ID를 기준으로 추적기의 통계(Track Prefix Name(추적 접두사 이름), Track State(추적 상태), Discontinuity Time(무중단 시간) 및 Last State Change Time(마지막 상태 변경 시간))를 확인합니다.

- SD-WAN Manager Monitor(SD-WAN 관리자 모니터) > Devices(디바이스) > {select Device-Name}(디바이스 이름 선택) > Events(이벤트)에서 다음을 수행합니다.

객체 추적기에서 탐지된 상태 변경의 경우, 연결된 해당 VRRP 그룹이 상태를 변경합니다. 각 로그는 이 섹션에 호스트 이름, if number, grp id, addr type, if name, vrrp group-state, state change-reason, vpn id 등의 세부 정보로 채워집니다(Name as Vrrp Group State Change).

엣지의 CLI에서:

```
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)
```

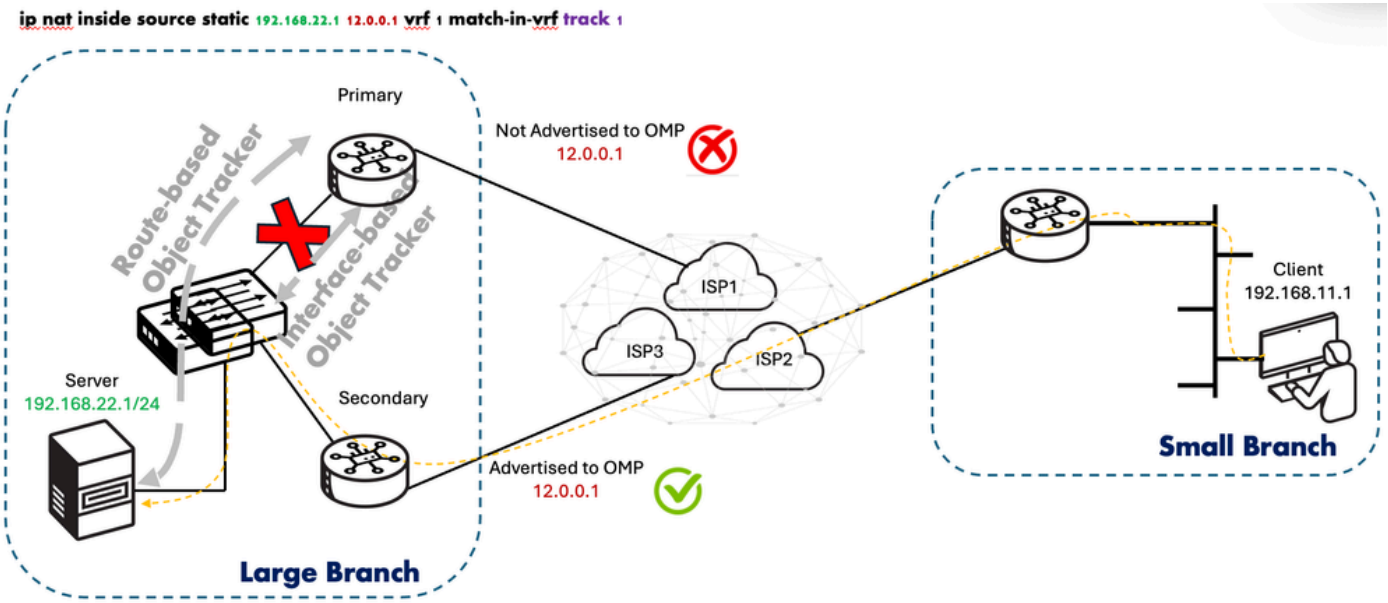
Service-VPN NAT 추적에 사용되는 인터페이스/경로 개체 추적기

서비스 측 NAT 객체 추적기는 20.8/17.8 릴리스에 도입된 기능으로, 서비스-VPN NAT에 사용되는 내부 글로벌 주소(내부 고정 NAT 및 내부 동적 NAT)는 (i) 내부 로컬 주소가 도달 가능한 것으로 확인되거나 (ii) LAN/서비스 측 인터페이스의 라인 프로토콜이 연결된 객체 추적기에 따라 UP인 경우에만 OMP로 광고됩니다. 따라서 사용할 수 있는 객체 추적기 유형은 (i) 경로 또는 (ii) 인터페이스입니다. LAN 접두사 또는 LAN 인터페이스의 상태에 따라 OMP를 통한 NAT 경로 알림이 추가되거나 제거됩니다. 어떤 NAT 경로 알림이 추가 또는 제거되는지 모니터링하기 위해 Cisco SD-WAN Manager에서 이벤트 로그를 볼 수 있습니다.

추적기에서 사용하는 프로브가 없습니다. 대신 (i) 라우팅 테이블에 라우팅 항목이 있거나 (ii) 라인 프로토콜 상태를 사용하여 추적기 상태(up/down)를 결정합니다. 라우팅 엔트리 또는 인터페이스 라인 프로토콜 기반 추적기가 있으면 반응 간격이 없습니다. 라우팅 엔트리 또는 인터페이스 라인 프로토콜이 다운되는 순간 트랙 상태도 다운됩니다. 개체 추적기와 연결된 NAT 문에 사용된 내부 전역 주소가 OMP로 광고되는 것이 즉시 중단됩니다. 서비스 VPN NAT 추적기에 대한 자세한 내용은 구성 가이드를 참조하십시오.

활용 사례

LAN 인터페이스 또는 LAN 접두사가 다운되면 서비스 측 NAT 객체 추적기가 자동으로 다운됩니다. 이벤트 로그를 볼 수 있습니다. Cisco SD-WAN Manager 어떤 NAT 경로 광고가 추가되거나 제거되는지 모니터링합니다. 다음 활용 사례에서는 클라이언트가 대규모 지사의 서버에 액세스해야 합니다. 그러나 큰 브랜치 에지(HA)에서 서버를 가리키는 경로가 제거되거나 큰 브랜치의 어느 한 에지에서 LAN 측(서비스 측) 인터페이스가 다운되는 경우 문제가 발생합니다. 이러한 상황에서 서비스 측 NAT를 개체 추적기와 함께 적용할 경우 - OMP에 대한 내부 전역 주소 광고를 제어하여 클라이언트에서 들어오는 트래픽이 항상 큰 브랜치에 있는 올바른 에지로 전달되는지 확인합니다. OMP로의 경로 알림에 이러한 제어가 적용되지 않을 경우, 해당 에지에서 대규모 브랜치의 서버로 연결할 수 없기 때문에 트래픽이 블랙홀링됩니다.



설정

객체 추적기의 컨피그레이션은 레거시 컨피그레이션의 시스템 템플릿을 통해 수행된 다음, 서비스 VPN 기능 템플릿의 각 NAT 문(내부 고정 또는 내부 동적)에 객체 추적기를 연결합니다. 구성 그룹에서 각 서비스 프로파일 이더넷 인터페이스 프로파일에 객체 추적기를 추가하는 옵션을 직접 가져옴으로써 이 메커니즘이 간소화되었습니다. 사용자가 선호하는 구성 방법 유형에 따라 이 메커니즘을 구성하는 방법이 다음과 같습니다.

- Configuration(컨피그레이션) 그룹 Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로파일) > Add Feature(기능 추가) > Object Tracker(개체 추적기):

1. 정의 중인 새 객체 추적기의 Name(이름) 및 Description(설명)을 제공합니다.
2. Tracker Type(추적기 유형)을 Interface(인터페이스)와 Route(경로) 중에서 선택합니다.
3. 객체 추적기 ID를 할당합니다.
4. Interface Name(인터페이스 이름)을 제공하거나 Route IP(경로 IP), Route IP Mask(경로 IP 마스크) 및 VPN(단계 2에서 선택한 옵션에 따라 다름)을 제공합니다.

- Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Service Profile(서비스 프로파일) > NAT 섹션:

1. Add NAT Pool(NAT 풀 추가) 버튼을 클릭하여 NAT 풀을 생성합니다(SSNAT를 트리거하는 데 필수).

2. NatPool 이름, 접두사 길이, 범위 시작, 범위 끝 및 방향과 같은 NAT 풀의 세부 정보를 제공합니다.

3. 동일한 섹션에서 고정 NAT로 이동하고 새 고정 NAT 추가 버튼을 클릭합니다. 내부 동적 풀 NAT에 객체 추적기를 연결하도록 선택할 수도 있습니다.

4. 소스 IP, 변환된 소스 IP, 고정 NAT 방향 등 세부 정보를 제공합니다.

5. Associate Object Tracker(객체 추적기 연결) 필드 아래의 드롭다운 목록에서 이전에 생성한 객체

추적기를 선택합니다.

- 레거시 구성 > 템플릿 > 기능 템플릿 > 시스템 > 추적기 섹션:

1. 새 개체 추적기 단추를 클릭합니다.
2. Tracker Type(추적기 유형)을 Interface(인터페이스)와 Route(경로) 중에서 선택합니다.
3. 객체 ID를 할당합니다.
4. 인터페이스 이름 또는 경로 IP, 경로 IP 마스크 및 VPN을 제공합니다(단계 2에서 선택한 옵션에 따라 다름).

- Configuration(컨피그레이션) > Templates(템플릿) > Cisco VPN(Cisco VPN(서비스 측에 속함)) > NAT 섹션:

1. New NAT Pool(새 NAT 풀) 버튼을 클릭하여 NAT 풀을 생성합니다(SSNAT 트리거에 필수).

2. NAT 풀 이름, NAT 풀 접두사 길이, NAT 풀 범위 시작, NAT 풀 범위 끝, NAT 방향 등 NAT 풀의 세부사항을 제공합니다.

3. 동일한 섹션에서 고정 NAT로 이동하고 New Static NAT(새 고정 NAT) 버튼을 클릭합니다. 내부 동적 풀 NAT에 객체 추적기를 연결하도록 선택할 수도 있습니다.

4. 소스 IP 주소, 변환된 소스 IP 주소, 고정 NAT 방향 등의 세부사항을 제공합니다.

5. [객체 추적기 추가] 필드 아래에 이전에 생성한 객체 추적기의 이름을 입력합니다.

CLI의 관점에서 컨피그레이션은 다음과 같습니다.

```
(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 활용 사례의 가정은 사용자가 NAT 흐름에서 in -> out 및 out -> 모두에 대한 트래픽을 매칭하기 위해 데이터 정책을 적용한다는 것입니다.

확인

NAT 사용 사례에 대해 명시적으로 구성된 개체 추적기를 확인하는 두 가지 영역이 있습니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Real Time(실시간):

1. Device Options에서 "IP NAT Translation"을 입력합니다.

2. Individual NAT Translation(개별 NAT 변환)에서 확인하고 구성된 Object Tracker ID를 기준으로 항목(Inside Local address/port(내부 로컬 주소/포트), Inside Global address/port(내부 글로벌 주소/포트), Outside Local address/port(외부 로컬 주소/포트), Outside Global address/port(외부 글로벌 주소/포트), VRF ID, VRF Name and Protocol(VRF 이름 및 프로토콜) 통계를 확인합니다.

- SD-WAN Manager에서: Monitor(모니터링) > Devices(디바이스) > {select Device-Name} > Events(이벤트):

OMP로 프루닝되는 NAT 경로에 해당하는 객체 추적기에서 상태 변경이 탐지된 경우 호스트 이름, 객체 추적기, 주소, 마스크, 경로 유형 및 업데이트와 같은 세부사항이 포함된 "NAT Route Change"라는 이름의 이벤트가 나타납니다. 여기서 주소 및 마스크는 고정 NAT 문 아래에 구성된 대로 내부 전역 주소에 매핑됩니다.

엣지의 CLI에서:

```
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
```

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE 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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.