Inzicht in Catalyst SD-WAN Tracker-bruikbaarheid en -gebruikscases

Inhoud

Inleiding

Dit document beschrijft Catalyst SD-WAN overlay-netwerken voor ondernemingen, tracker-bruikbaarheid en gebruikscases.

Achtergrondinformatie

Catalyst SD-WAN overlay-netwerken voor ondernemingen interacteren doorgaans met een brede reeks externe werkbelastingen, toepassingen en services. die zich in de cloud, datacenter/hubs of verafgelegen filialen kunnen bevinden. Het SD-WAN controlevliegtuig is verantwoordelijk voor het adverteren van routes naar deze diensten over de overlay op een schaalbare manier. In situaties waarin kritieke toepassingen en diensten langs een specifieke route onbereikbaar worden, moeten netwerkexploitanten doorgaans in staat zijn deze gebeurtenissen te detecteren en gebruikersverkeer om te leiden naar meer geschikte paden om onbepaalde blokkering van verkeer te voorkomen. Om deze soorten netwerkfouten te detecteren en te corrigeren, vertrouwt het Catalyst SD-WAN-besturingsplane op trackers om de gezondheid van externe services te bewaken en routeringswijzigingen aan te brengen zoals van toepassing.

Een tracker is een control plane bereikbaarheidsdetectiemechanisme dat sonde pakketten naar een specifiek eindpunt stuurt en informeert over wijzigingen in de bereikbaarheidsstatus (omhoog of omlaag) van het eindpunt naar geïnteresseerde modules. Trackers zijn ontworpen als een schaalbare, hoogwaardige abstractie van de native Cisco IOS-XE® IP SLA-functie, die een verscheidenheid aan sondes kan vormen (waaronder HTTP, ICMP en DNS). Wanneer een tracker een clientmodule op de hoogte stelt van een statuswijziging, kan die module passende actie ondernemen om verkeersblokkering te voorkomen, zoals het installeren of verwijderen van een route of reeks routes. De huidige toepassingen van trackers binnen zowel SD-WAN als SD-Routing oplossingen omvatten, maar zijn niet beperkt tot: DICOM (Direct Internet Access)-trackers, SIG (Secure Internet Gateway)-trackers, servicetrackers, statische routertrackers, trackergroepen, enzovoort.

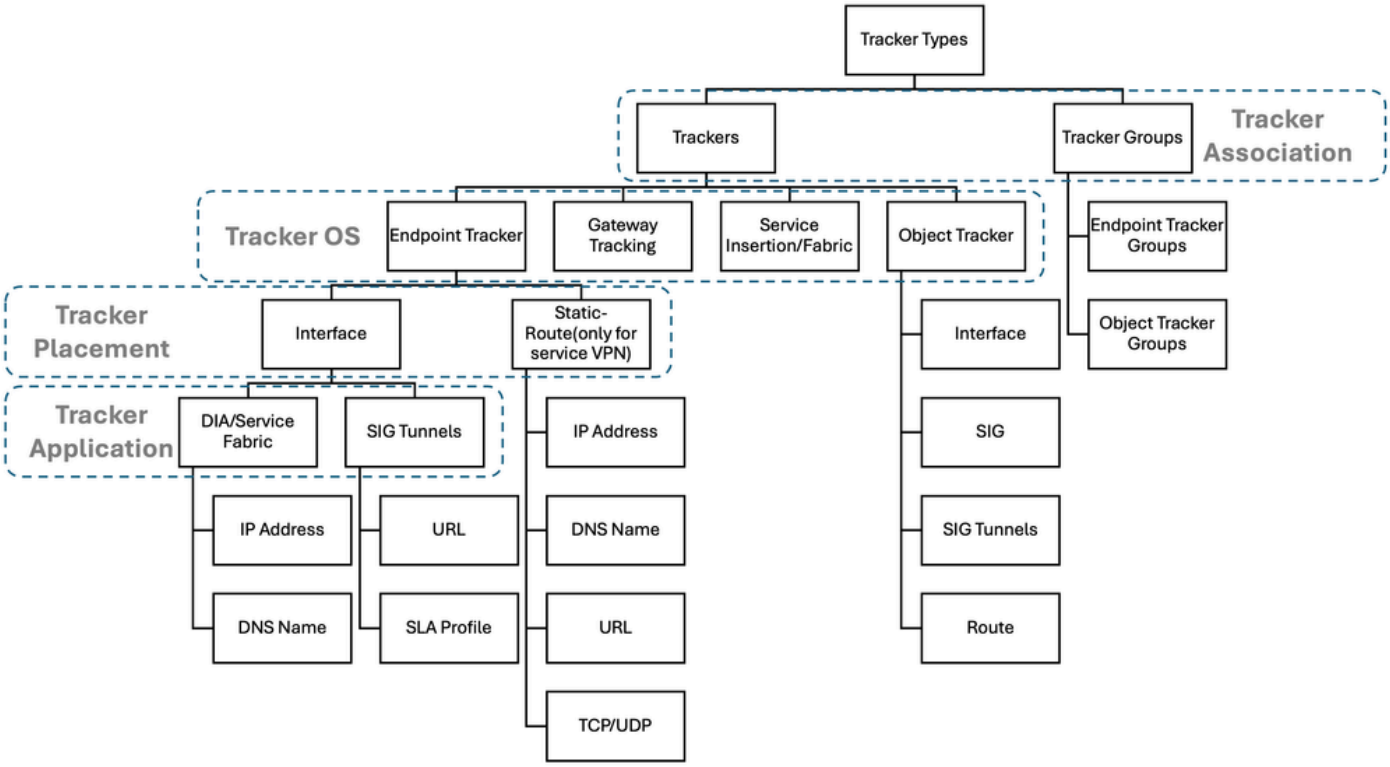
Om hoogst beschikbare netwerken te bouwen die aan de mislukkingen van de dienst veerkrachtig zijn, is het essentieel om te begrijpen wanneer om elk type van trackerconfiguratie/model te gebruiken. Het doel van dit artikel is om uit te leggen waar en hoe elk type tracker wordt gebruikt. De verschillende trackers komen hier aan bod, evenals het primaire gebruik van elke tracker en de fundamentele configuratie workflows om elke oplossing te implementeren. Ten slotte introduceert dit artikel een doorloop van algemene voorbehouden met betrekking tot trackers in Cisco IOS-XE®.

In dit artikel wordt een onderscheid gemaakt tussen de endpoint-tracker (SD-WAN en SD-Routing specifieke) en object tracker oplossingen (native IOS-XE), die verschillende gebruikscases aanpakken.

Soorten trackers

Deze tabel biedt een kort overzicht van alle typen trackers die in de Cisco Catalyst SD-WAN

oplossing beschikbaar zijn:



Vanuit de bovenstaande tabel zijn er vier gebieden waar trackers kunnen worden geclassificeerd: Tracker Association, Tracker OS, Tracker Placement en Tracker Application. In het volgende deel wordt elke classificatie beschreven:

1. Tracker Association: Deze classificatie beschrijft of een tracker een enkele tracker of een tracker groep is. Cisco Catalyst SD-WAN ondersteunt het gebruik van meerdere trackers in een groep (maximaal 2 op dit moment van schrijven) en de algemene status van de trackergroep wordt bepaald door een booleaanse EN/OF operator. De voorbeelden omvatten een endpoint-tracker groep of een object tracker groep.
2. Tracker-besturingssysteem: Deze classificatie beschrijft het Cisco IOS-XE® besturingssysteem of de modus waarin de tracker wordt ondersteund. Cisco Catalyst IOS-XE routers ondersteunen twee besturingsmodi:

- Autonome modus en
- Controllermodus.

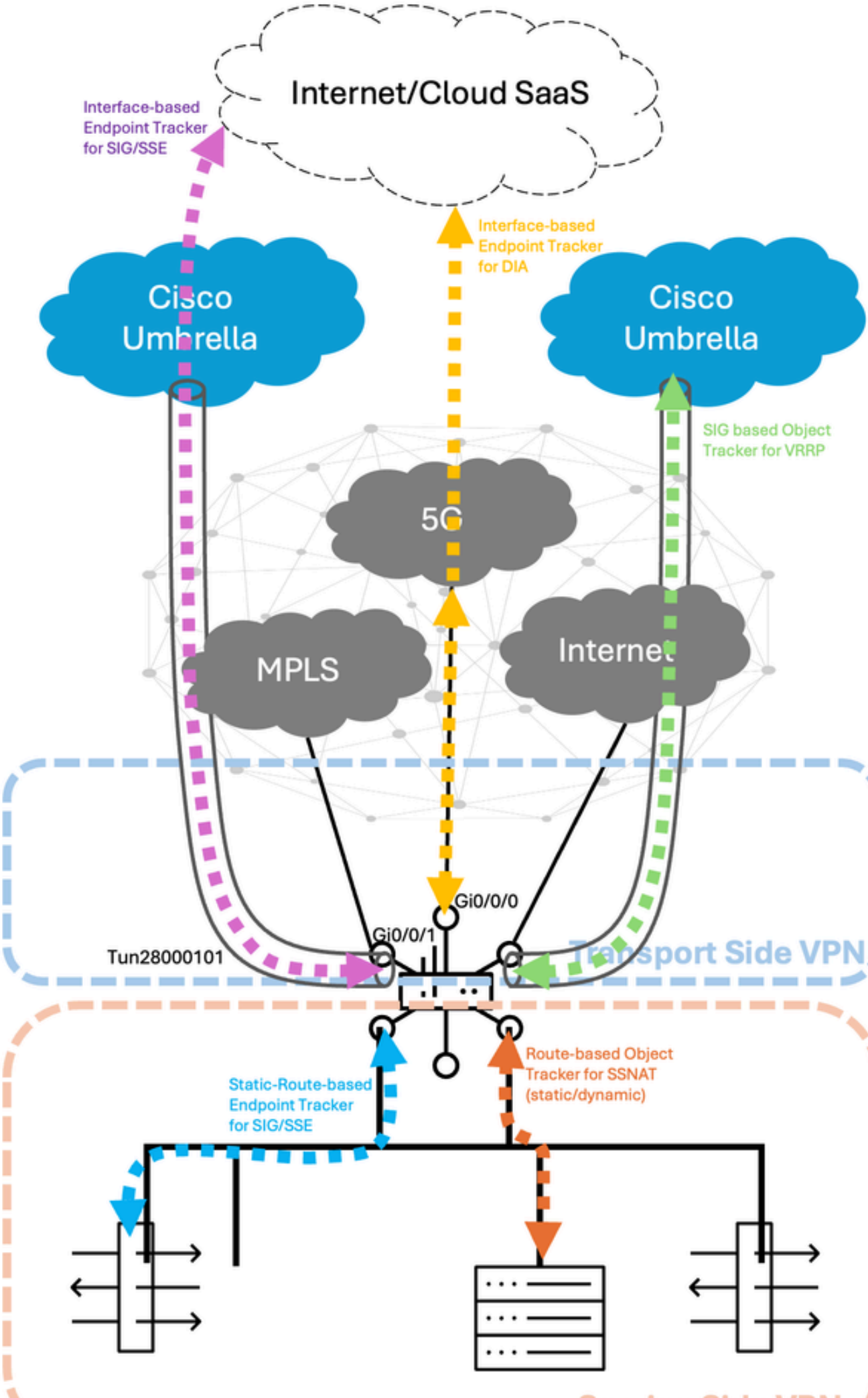
Alle endpoint-tracker en gateway tracking functies zijn beide bedoeld voor controller-mode (SD-WAN) gebruikscases, terwijl de object tracker is bedoeld voor de autonome-mode (SD-Routing) gebruikscases.

3. Tracker Placement: Deze classificatie beschrijft de locatie waarin de tracker is geconfigureerd. Momenteel ondersteunt Cisco Catalyst SD-WAN het toepassen van trackers op interfaces, statische routes of services.

4. Tracker-toepassing: Deze classificatie beschrijft de gebruikscases en functies op hoog niveau die worden ondersteund door Cisco Catalyst SD-WAN. Hoewel er tal van toepassingsgebieden

van trackers zijn, zijn enkele van deze gebieden: Direct Internet Access (DIA), Secure Internet Gateway (SIG), Secure Service Edge (SSE), Service-side VPN-tracering, enzovoort.

Hier is een visuele weergave van het tracker-sonde-verkeer via service-/transport-VPN's voor verschillende gebruikscases op een Cisco Catalyst SD-WAN Edge (die ook cEdge of vEdge kan worden genoemd):


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

op SD-WAN Edge-platforms aan de transportzijde van VPN zijn geconfigureerd. Standaard is dit ingeschakeld onder de basisconfiguraties van het systeemprofiel (Track Default Gateway) onder Catalyst SD-WAN Manager. Dit helpt om het volgende-hopadres dat onder elke standaard statische route in transport VPN wordt gespecificeerd voortdurend te controleren, om link/route failover te verzekeren, in het geval van de bereikbaarheidsmislukking van de volgende-hop (die ook de gateway wordt genoemd, vandaar de naam gateway-tracking). Om meer over gateway-tracking te leren, bezoek de configuratiehandleiding.

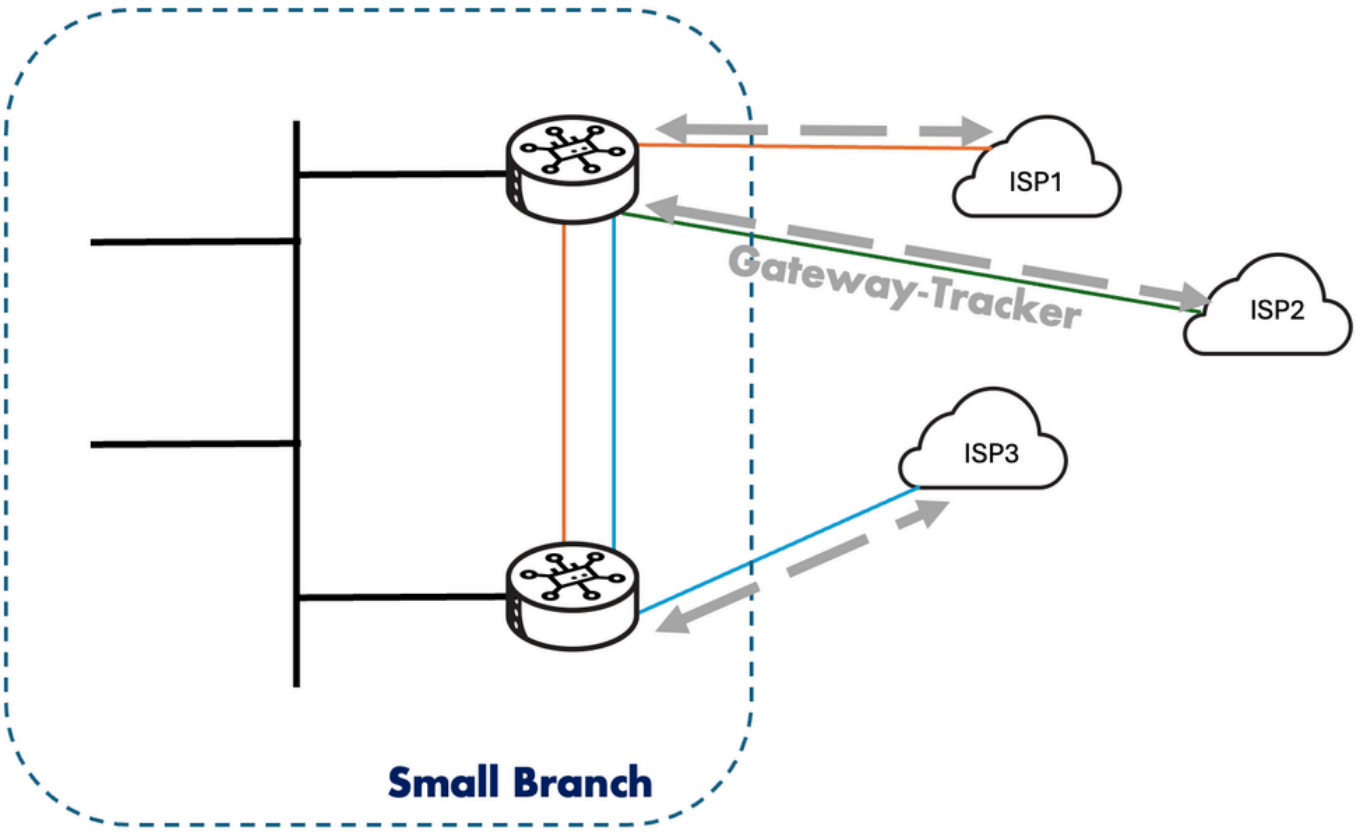
Het type van hier gebruikte sondes zijn ARP-verzoek onbekend-unicast overstroomde pakketten. De gebruikte intervallen zijn:

- Hello: 10 seconden
- Wachtstandtijd: 100 seconden
- Type pakket/sonde: ARP

Samen met gateway tracking wordt ook gebruik gemaakt van transport tracking op SD-WAN randen voor het controleren van het gerouteerde pad tussen het lokale apparaat en een Cisco Catalyst SD-WAN Validator. Dit wordt gedaan door ICMP sondes met regelmatig interval van 3s te gebruiken. Dit wordt geconfigureerd met behulp van het "track-transport" sleutelwoord onder de SD-WAN systeemconfiguratiemodus. Dit helpt bij de regelmatige bewaking van de DTLS-verbinding met Cisco Catalyst SD-WAN Validator vanuit de respectieve WAN Edge. Ga voor meer informatie over transport tracking naar de configuratiehandleiding.

Use cases

Gateway Tracking is een functie die standaard op SD-WAN impliciet is geconfigureerd voor alle statische standaardroutes die tot de transport-VPN of Global Routing Table (GRT) behoren. Het gebruik van de functie komt niet altijd voort uit de Manager sjabloon configuratie standpunt, maar kan ook evolueren van ontvangen / verworven standaard statische routes in de scenario's van het gebruik van een DHCP server met opties #3, #81 enzovoort.



Configuratie

Standaard toegepast in Cisco Catalyst SD-WAN:

```
!
system


 track-transport
 track-default-gateway


!
```

Verificatie

Hier zijn manieren om dit te verifiëren per Legacy-configuratie en -configuratiegroep:

- Configuratiegroep: Configuratie > Configuratiegroepen > Systeemprofiel > Basis subprofiel > Instellingen bijhouden > Stand. Stand. Gateway (standaard:ON)
- Verouderde configuratie: Configuratie > Sjablonen > Functiesjablonen > Systeemsjabloon > Geavanceerde sectie > Gatewaytracering (standaard:ON)

Service Fabric 2.0-tracering en Service Fabric 1.0

Service Insertion 1.0 Tracking is geïntroduceerd in versie 20.3/17.3 en is een functie die ervoor moet zorgen dat het serviceadres (of het adres voor doorsturen) bereikbaar of beschikbaar is. Deze informatie helpt de Edge om dynamisch volgende-hop informatie toe te voegen of terug te trekken uit het Control/Data-beleid. Bij de configuratie van Service Insertion 1.0 wordt de tracker (of het trackingadres) standaard ingeschakeld naar het serviceadres. Gebaseerd op dit, zijn het het door:sturen adres en het de dienstadres het zelfde in 1.0. Alhoewel de de diensttrackers automatisch met de diensten worden gevormd, kunnen deze trackers worden onbruikbaar gemaakt het gebruiken van het geen spoor-toelaten bevel, of door de trackerknop in de configuratie groep/Verouderde configuratie onbruikbaar te maken. Aangezien dit de enige twee mogelijke bewerkingen zijn (inschakelen/uitschakelen) met trackers die gekoppeld zijn aan services onder Service Insertion 1.0, zijn er geen verdere parameters die kunnen worden getweaakt (zoals drempelwaarde, multiplexer, interval). Het type sondes dat hier wordt gebruikt, is een ICMP Echo-request-pakket.

Als u meer wilt weten over het bijhouden van service-invoeging 1.0, gaat u naar de configuratiehandleiding. De standaardintervallen die in service-invoeging 1.0 worden gebruikt, zijn:

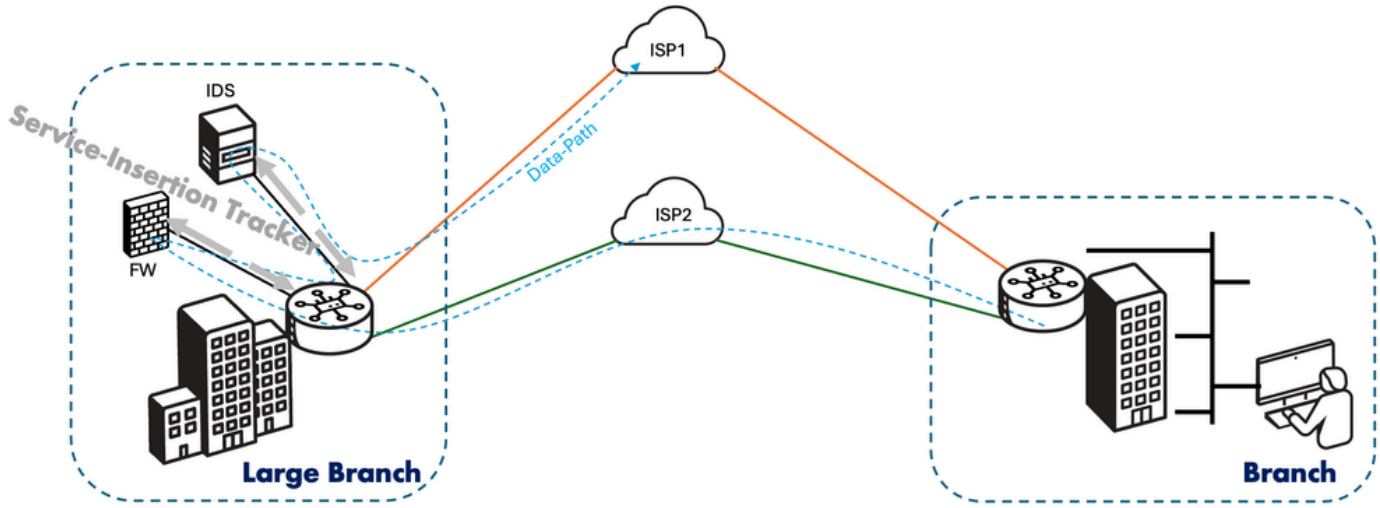
- Sonde-interval: 5 sondes om de 60 seconden
- Vermenigvuldiger: 5 keer
- Type pakket/sonde: ICMP-echo/echo-antwoord

Service Fabric 2.0-tracering wordt geleverd als deel van Service Insertion 2.0-aanbod in Cisco Catalyst SD-WAN dat vanaf release 20.13/17.13 wordt geïntroduceerd. In deze nieuwe variant van de diensttoevoeging, is de standaardmethode die door de configuratieprofielen en de malplaatjes wordt gebruikt nog om een impliciete drijver te hebben die aan elk bepaald de dienstadres (of het door:sturen adres) richten in een dienst-HA-paar per rx/tx interface. Met Service Fabric 2.0 kunt u het doorsturen adres nu splitsen van het traceeradres. Dit kan eenvoudig worden gedaan door afzonderlijke endpointtrackers te definiëren voor het bijhouden van een ander endpointadres dan het serviceadres zelf. In de volgende paragrafen wordt nader op dit onderwerp ingegaan.

Use cases

Het primaire gebruiksgeval voor de diensttrackers is voor schaalbare controle van de dienst bereikbaarheid, in het bijzonder voor de dienst ketenen. Service chaining kan worden geïmplementeerd in een netwerk dat uit meerdere VPN's bestaat, waarbij elke VPN een andere functie of organisatie vertegenwoordigt, om er zeker van te zijn dat verkeer tussen VPN's door een firewall stroomt. Bijvoorbeeld, in een groot campusnetwerk, kan het interdepartementale verkeer door een firewall gaan, terwijl het intradepartementale verkeer direct kan worden geleid. Service

chaining kan worden gezien in scenario's waarin een operator moet voldoen aan de wettelijke vereisten, zoals de Payment Card Industry Data Security Standard (PCI DSS), waar PCI-verkeer door firewalls moet stromen in een gecentraliseerd datacenter of een regionale hub:



Configuratie

De configuraties zijn hetzelfde als de normale workflow voor het instellen van Service Insertion 1.0 op SD-WAN. De Service Insertion 1.0 Trackers zouden standaard ingeschakeld worden op alle serviceadressen.

- Configuratiegroep: Configuratie > Configuratiegroepen > Serviceprofiel > Service VPN > Service sectie:

1. Klik op de knop Service toevoegen.

2. Kies een servicetype.

3. Serviceadres opgeven (max. 4 mogelijke tekens, gescheiden door een komma).

4. Controleer of de traceerknop is ingeschakeld (standaard). Dit kan desgewenst worden uitgeschakeld.

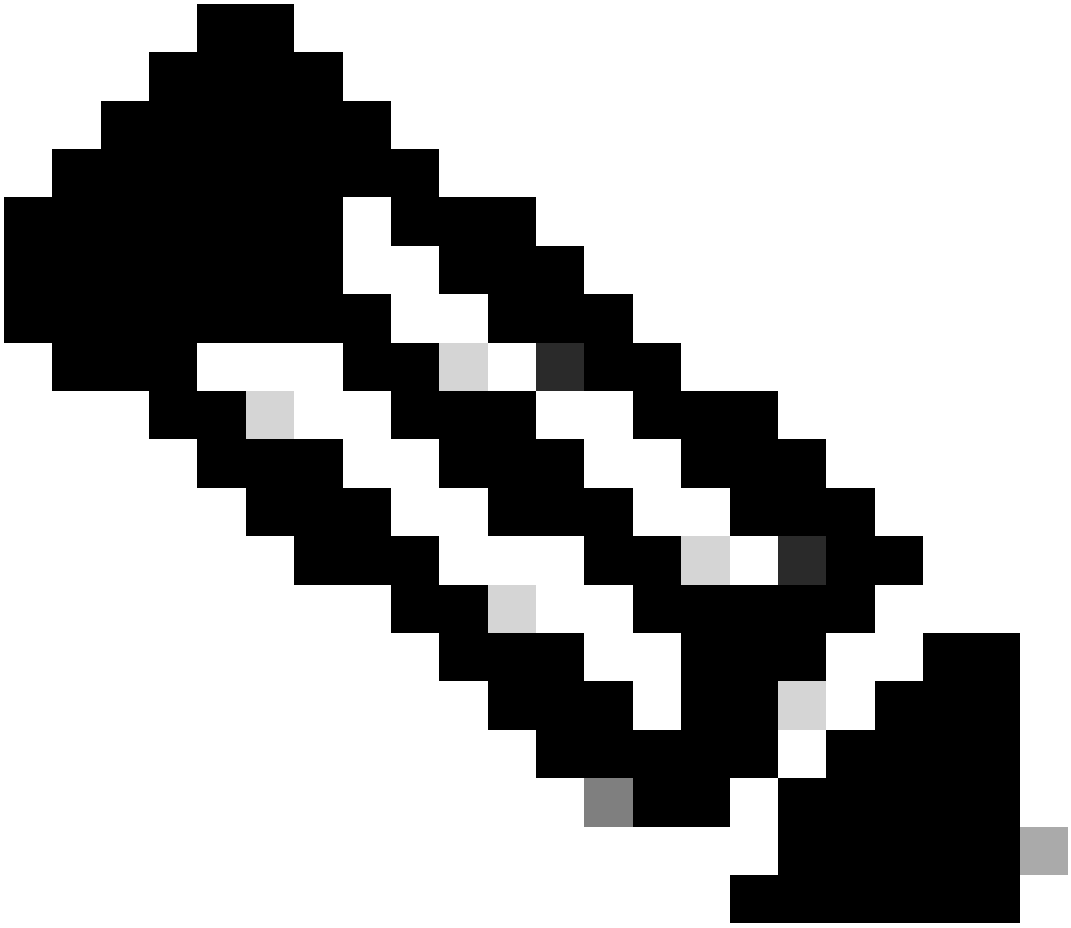
- Verouderde configuratie: Configuratie > Sjablonen > Functiesjablonen > Cisco VPN (service) > Servicesectie:

1. Klik op de knop New Service

2. Kies een servicetype.

3. Serviceadres opgeven (max. 4 mogelijke tekens, gescheiden door een komma).

4. Controleer of de traceerknop is ingeschakeld (standaard). Dit kan desgewenst worden uitgeschakeld.



Opmerking: Zodra Stap 3 is geconfigureerd (van de configuratie of van de oudere configuratie), wordt de tracker automatisch geïnitieerd naar de verschillende gedefinieerde servicesadressen

Vanuit het CLI-standpunt verschijnt de configuratie voor Service Insertion 1.0 als volgt:

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

Verificatie

De stappen voor controle strekken zich uit tot de gelijkaardige stappen die als deel van op

interface-gebaseerde eindpunttrackers worden gevolgd die in de voorafgaande secties worden gebruikt.

Er zijn twee verificatieopties voor expliciet geconfigureerde endpointtracker.

- Op SD-WAN Manager: Monitor > Apparaten > {selecteer Apparaat-Naam} > Toepassingen > Tracker:

Controleer onder Individuele Tracker en bekijk de statistieken van de tracker (Tracker Types, Status, Endpoint Type, Endpoint Type, VPN Index, Host Name, Round Trip Time) op basis van uw geconfigureerde Tracker Naam.

- Op SD-WAN Manager: Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van klappen die op de tracker worden gedetecteerd, zouden de betreffende logboeken in deze sectie worden ingevuld met details zoals hostnaam, aanhechtingspunt-naam, tracker-naam, nieuwe staat, adresfamilie, en VPN-id.

Op CLI (CLI) van de edge:

```
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
```

Interface-endpointtrackers gebruikt voor DIA

NAT DIA Endpoint Trackers zijn in de eerste plaats bedoeld om de bereikbaarheid van toepassingen te bewaken via een NAT DIA-interface op SD-WAN Edge-platforms.

Voor Direct Internet Access (DIA)-gebruikscases worden NAT DIA-trackers voornamelijk gebruikt om de interface aan de transportzijde te volgen en een failover te starten naar een andere beschikbare interface aan de transportzijde of via SD-WAN-overlay tunnels (met behulp van databeleid). Deze functie werd geïntroduceerd vanaf 20.3/17.3 release en NAT fallback feature-

optie is beschikbaar vanaf 20.4/17.4 release. Als de tracker bepaalt dat het lokale internet niet beschikbaar is via de NAT DIA-interface, trekt de router de NAT-route uit Service VPN terug en herleidt het verkeer op basis van de lokale routerconfiguratie. De tracker blijft periodiek de status van het pad naar de interface controleren. Wanneer het ontdekt dat de weg opnieuw functioneert, installeert de router de NAT route aan het internet opnieuw. Om meer over de trackers van de dia te leren, te bezoeken gelieve de configuratiegids.

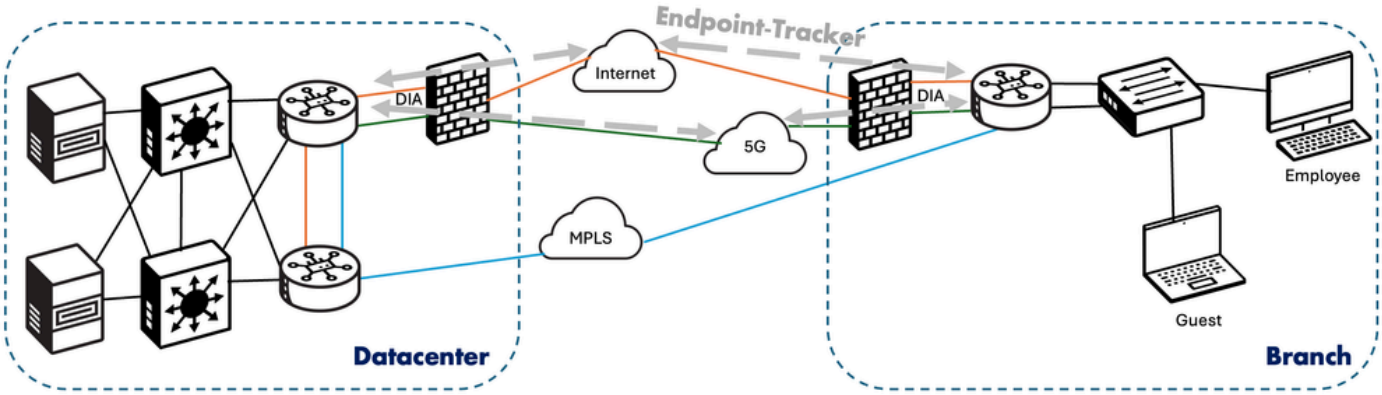
In de tracker-definitie kunt u ervoor kiezen om een IP-adres van een eindpunt te geven dat bereikbaar is via de NAT DIA-interface (geconfigureerd als "endpoint-ip") OF een volledig gekwalificeerde domeinnaam (FQDN) te leveren aan het eindpunt (geconfigureerd als "endpoint-dns-name").

Het type sondes dat hier wordt gebruikt is een HTTP-verzoekpakket, dat erg lijkt op een HTTP API-aanvraag PDU-stack. De gebruikte intervallen zijn:

- Sonde-interval: 60 seconden
- Vermenigvuldiger: 180 seconden (aangezien #retries 3 = 3 x 60 seconden is)
- Type pakket/sonde: HTTP

Use cases

DICOM wordt vaak ingezet als een optimalisatie op filialen om backhauling naar een datacenter te voorkomen. Desalniettemin, wanneer de DIB in filialen wordt gebruikt, moet elk gebrek aan bereikbaarheid langs NAT DIA-routes nog steeds terugvallen op alternatieve paden om zwart houden en verlies van service te voorkomen. Voor sites die terugval naar de DC wensen te gebruiken (via SD-WAN overlay met NAT fallback) in het geval van een lokale DIA-doorbraakfout. Maak gebruik van deze op interfaces gebaseerde endpointtrackers op de met DIA geschikte interfaces op de randen aan de zijkant van de tak om storingen te detecteren om een failover naar het back-up/DC-pad te starten. Op deze manier wordt een hoge beschikbaarheid van internetservice bereikt met een minimale onderbreking in de onderneming terwijl het internetverkeer nog steeds wordt geoptimaliseerd met DIA:



Configuratie

Deze op interfaces gebaseerde endpointtrackers moeten handmatig worden geconfigureerd om deze functieset in te schakelen. Hier zijn de manieren om het, afhankelijk van het type van

configuratiemethode te vormen die door de gebruiker de voorkeur heeft.

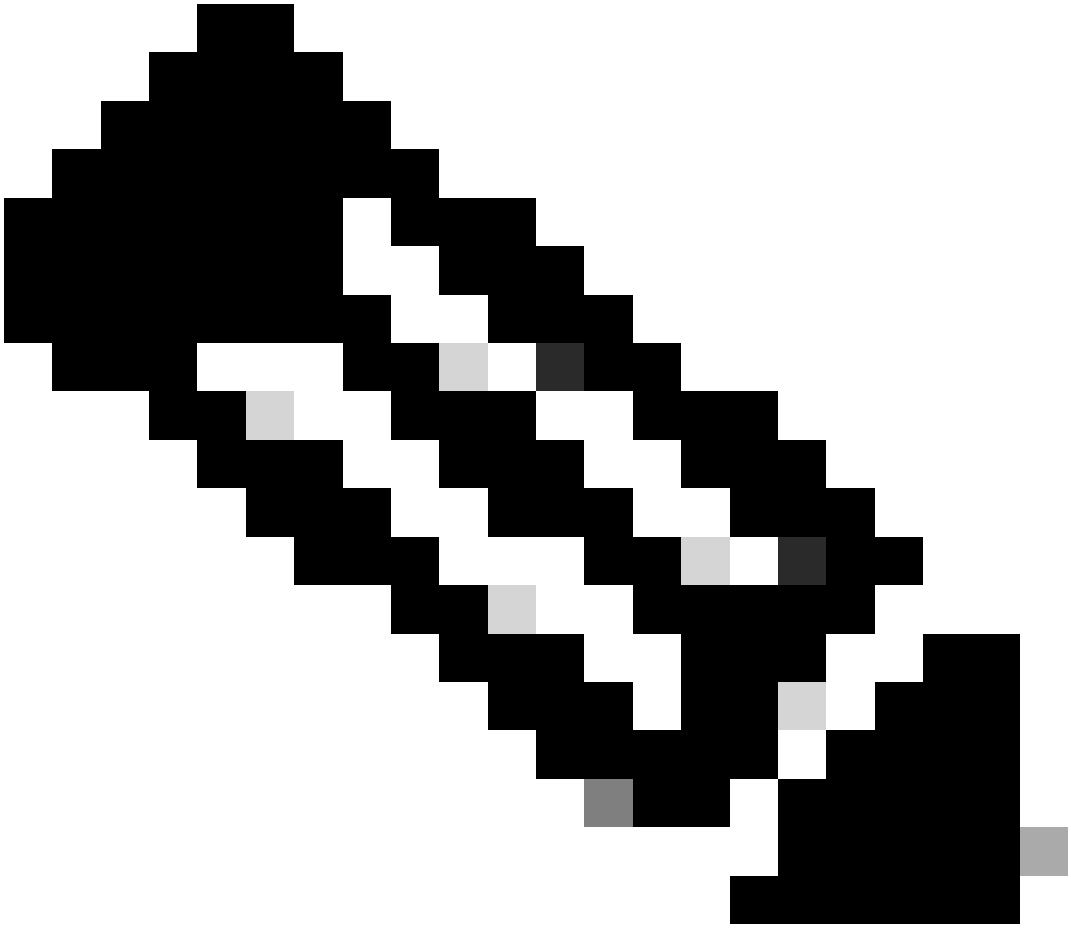
- Configuratiegroep: Configuratie > Configuratiegroepen > Transport & Management Profile > Ethernet Interface > Add Feature > Tracker:

1. Bepaal een naam van de endpointtracker.

2. Kies een type endpointtracker (tussen HTTP-standaard en ICMP).

Opmerking: Het type ICMP-endpointtracker is geïntroduceerd sinds 20.13/17.13 release.

3. Selecteer het Endpoint (tussen IP-standaard endpoints en DNS-naam endpoints).



Opmerking: Als Endpoint DNS Name is gekozen, dient u ervoor te zorgen dat een geldige DNS-server of naamserver is gedefinieerd onder het transport VPN/VRF met behulp van het configuratieprofiel voor transport VPN.

---

4. Voer het adres of de DNS-naam (FQDN) in waarnaar de trackersondes moeten worden

verzonden (het formaat hangt af van de vorige stap).

5. (Optioneel) U kunt ervoor kiezen het sonde-interval (standaard = 60 seconden) en het aantal pogingen (standaard = 3 keer) te wijzigen om de foutdetectietijd te bevestigen.

- Verouderde configuratie:

Stap 1. Definitie van de op interfaces gebaseerde Endpoint Tracker: Configuratie > Sjablonen > Functiesjablonen > Systeemsjabloon > Tracker-sectie:

1. Selecteer onder het kopje Trackers de knop New Endpoint Tracker.

2. Bepaal een naam van de endpointtracker.

3. Kies het Tracker-type (tussen interface-default en statische route) als interface, aangezien de DIA-gebruikscases hier van belang zijn.

4. Kies het Endpoint Type (tussen IP-adres en DNS-naam).

5. Voer het IP-adres of de DNS-naam van het eindpunt in waarnaar de trackersondes moeten worden verzonden (de indeling is afhankelijk van de vorige stap).

6. (Optioneel) U kunt ervoor kiezen de sonde drempelwaarde (standaard = 300 ms), het interval (standaard = 60 seconden) en de multiplexer (standaard = 3 keer) te wijzigen.

Stap 2. Pas de op interfaces gebaseerde Endpoint Tracker toe op een interface op het transport VPN: Templates > Feature Templates > Cisco VPN Interface Ethernet > Advanced paragraaf:

1. Voer de naam van de Endpoint Tracker die in de vorige stap 1 is gedefinieerd, in in het veld Tracker.

Vanuit het CLI-standpunt zien de configuraties er zo uit:

```
(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
!
```

Verificatie

Er zijn twee verificatieopties voor expliciet geconfigureerde endpointtrackers.

- Via SD-WAN Manager: Monitor > Apparaten > {selecteer Apparaat-Naam} > Toepassingen > Tracker:

Controleer onder Individuele Tracker en bekijk de statistieken van de tracker (Tracker Types, Status, Endpoint Type, Endpoint Type, VPN Index, Host Name, Round Trip Time) op basis van uw geconfigureerde Tracker Naam.

- Via SD-WAN Manager: Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van klappen die op de tracker worden gedetecteerd, zouden de betreffende logboeken in deze sectie worden ingevuld met details zoals hostnaam, aanhechtingspunt-naam, tracker-naam, nieuwe staat, adresfamilie, en VPN-id.

Op CLI (CLI) van de edge:

```
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
```

Interface-endpointtrackers gebruikt voor SIG-tunnels/SSE

Wanneer endpointtrackers worden gebruikt voor SIG Tunnel/SSE use cases, geeft dit voornamelijk aan dat de onderneming op zoek is naar een cloudgebaseerde security stack die tegenwoordig eenvoudig beschikbaar is met behulp van Secure Internet Gateway (SIG) of Secure Service Edge (SSE) providers, zoals Cisco, Cloudflare, Netskope, ZScalar, enzovoort. Zowel SIG Tunnels als SSE zijn onderdeel van het cloud security implementatiemodel, waarbij de tak de cloud gebruikt om de benodigde beveiligingsoplossingen te leveren. De SIG Tunnels use case was het allereerste aanbod van het integreren van Cisco Catalyst SD-WAN met dergelijke SIG-providers (vanaf 20.4/17.4 release), maar met de evolutie van het door de cloud geleverde security aanbod - de SSE use case werd geïntroduceerd (vanaf 20.13/17.13 release) voor het dekken van gebruikscases met providers zoals Cisco (via Cisco Secure Access) en ZScalar.

IT vereist een betrouwbare en expliciete benadering om te beschermen en te verbinden met behendigheid. Het is nu gebruikelijk om externe medewerkers directe toegang te bieden tot cloudtoepassingen, zoals Microsoft 365 en Salesforce met extra beveiliging. De vraag naar cloud-geleverde netwerken en beveiliging groeit dagelijks als contractanten, partners, Internet of Things (IoT)-apparaten, enzovoort, netwerktoegang vereisen. De convergentie van netwerk- en beveiligingsfuncties dichter bij eindapparaten, aan de cloud edge, staat bekend als een servicemodel genaamd Cisco SASE. Cisco SASE combineert cloudgeleverde netwerk- en beveiligingsfuncties om beveiligde toegang tot toepassingen te bieden voor alle gebruikers of apparaten, vanaf elke locatie en op elk moment. Secure Service Edge (SSE) is een netwerkbeveiligingsbenadering die organisaties helpt de beveiligingshouding van hun werkomgeving te verbeteren en tegelijk de complexiteit voor eindgebruikers en IT-afdelingen te verminderen. Raadpleeg de configuratiehandleiding voor meer informatie over SIG Tunnel/SSE-trackers.

Use cases

Dergelijke op interfaces gebaseerde endpointtrackers worden gebruikt in dergelijke SIG Tunnel/SSE-gebruikscases, waarin u een bekend URL-endpoint van een SaaS-toepassing of een specifiek URL-endpoint van zorg wilt bijhouden. Tegenwoordig is SSE het meest gebruikte scenario sinds de SASE architectuur werd opgesplitst in SSE kernfunctionaliteiten en SD-WAN functionaliteiten. U wilt dan kiezen tussen actieve & stand-by rollen binnen de IPSec Tunnels gemaakt van een site (in dit geval, de DC). De gebruiker krijgt de keuze om de tracker aan te sluiten onder de respectieve tunnelinterface.

In het geval van SSE-providers, zoals Cisco Secure Access (door Cisco) - wordt een impliciete endpointtracker gebruikt die standaard is geconfigureerd. De gebruiker kan echter wel een aangepaste endpointtracker maken en die aan de IPSec Tunnel-interface toevoegen. De

parameters van de standaard/impliciete eindpunttracker die in SSE worden gebruikt, zijn:

Voor Cisco SSE:

Naam tracker: Default Tracker

Endpoint dat wordt getraceerd: http://service.sig.umbrella.com

Type eindpunt: API_URL

Drempel: 300 ms

Vermenigvuldigen: 3

Interval: 60 sec.

Voor ZScaler SSE:

Naam tracker: Default Tracker

Endpoint dat wordt getraceerd: http://gateway.zscalerthree.net/vpnte

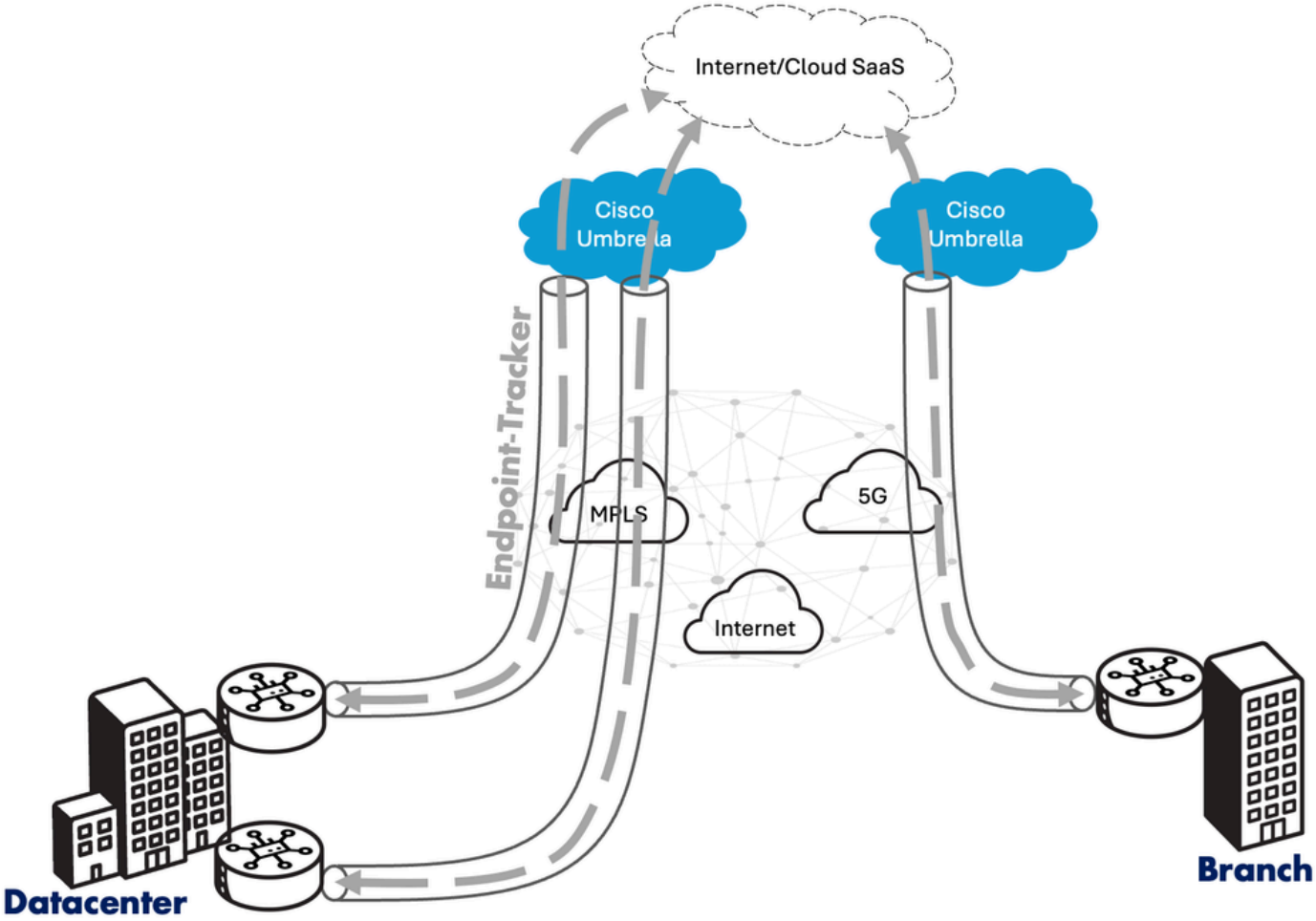
Type eindpunt: API_URL

Drempel: 300 ms

Vermenigvuldiger: 3

Interval: 60 sec.

In het geval van SIG-tunnels is er geen standaard/impliciete eindpunttracker gedefinieerd. Daarom moet de gebruiker handmatig een op een interface gebaseerde endpointtracker configureren in het geval ze de IPSec Tunnel-interface willen volgen naar de SIG-provider-cloud:



Configuratie

In het geval van SSE-providers hoeft de gebruiker geen endpointtracker expliciet te definiëren (tenzij gewenst). De werkstromen zijn echter verschillend op basis van het type configuratie.

Als vereiste moet u de SIG/SSE-referenties Administratie > Instellingen > Externe diensten > Cloud Credentials definiëren:

1. Schakel onder Cloud Provider Credentials de optie Umbrella of Cisco SSE (of beide) om.

2. Definieer de parameters, zoals Organisatie-ID, API-sleutel, geheim).

Stel configuratie groep in > Beleidsgroepen > Secure Internet Gateway/Secure Service Edge:

1. Klik op Add Secure Internet Gateway of Add Secure Service Edge.

2. Bepaal een naam en een beschrijving.

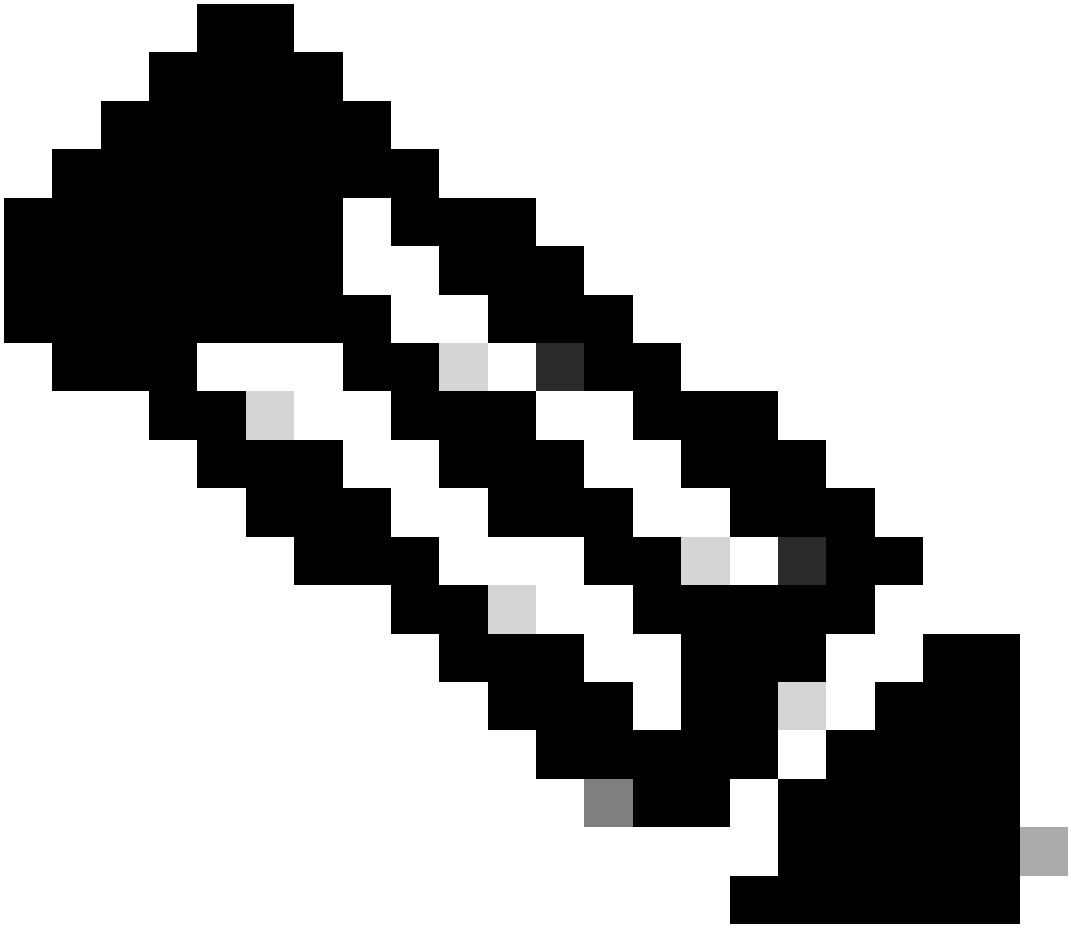
3. Selecteer een van de radioknoppen onder SIG/SSE Provider (Umbrella of Cisco SSE).

4. Onder de sectie Tracker definieert u het IP-bronadres dat wordt gebruikt om de tracker-sondes te bronnen.

5. Als u ervoor kiest om een expliciete/aangepaste endpointtracker te definiëren, klik dan op Add

Tracker, en vul vervolgens de parameters in voor de endpointtracker (Naam, API-URL van Endpoint, Threshold, Probe Interval, en Multiplier).

6. Onder de sectie Configuration maakt u de tunnelinterfaces waarin u de parameters kunt definiëren (zoals interfacenaam, beschrijving, tracker, tunnelbroninterface, primair/secundair datacenter).



> Opmerking: In Stap 6 is waar de gebruiker de optie krijgt om de gedefinieerde endpointtracker aan de respectievelijke IPSec Tunnel te verbinden. Dit is een optioneel veld.

---

7. Voer in het gedeelte Hoge beschikbaarheid een interfacepaar in en definieer uw actieve interface en back-upinterface samen met de respectieve gewichten. Pas vervolgens de vorige geconfigureerde beleidsgroep toe op de relevante randen.

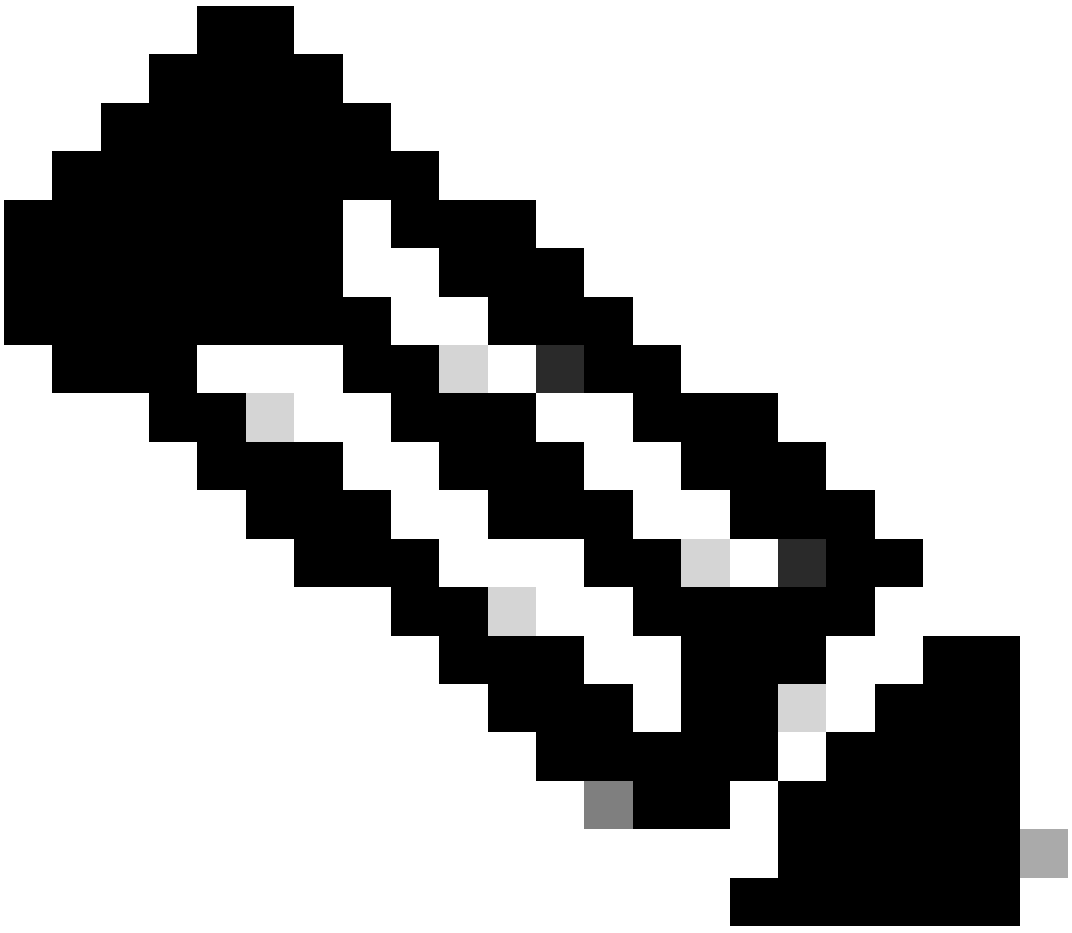
Verouderde configuratie instellen Configuratie > Sjablonen > Functiesjablonen > Cisco Secure Internet Gateway-functiesjabloon:

1. Selecteer een van de radioknoppen onder SIG Provider (Umbrella, ZScalar of Generiek).

2. Definieer onder de sectie Tracker (BETA) het IP-bronadres dat wordt gebruikt om de tracker-sondes te bronnen.

5. Als u ervoor kiest om een expliciete/aangepaste endpointtracker te definiëren, klik dan op New Tracker en vul de parameters in voor de endpointtracker (Naam, API-URL van endpoint, Threshold, Interval, en Multiplier).

6. Onder de sectie Configuration maakt u de tunnelinterfaces (door op Tunnel toevoegen te klikken) waarin u de parameters kunt definiëren (zoals interfacenaam, beschrijving, tracker, tunnelbroninterface, primair/secundair datacenter).



Opmerking: In stap 6 is waar de gebruiker de optie krijgt om de gedefinieerde endpointtracker aan de respectievelijke IPSec Tunnel te verbinden. Dit is een optioneel veld.

---

7. Definieer in het gedeelte Hoge beschikbaarheid uw Active Interface en Backup Interface, samen met de bijbehorende gewichten.

Vanuit het CLI-standpunt zien de configuraties er zo uit:

```
(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
!
```

Verificatie

Er zijn verificatieopties voor expliciet geconfigureerde endpointtrackers.

- Via SD-WAN Manager: Monitor > Apparaten > {selecteer Apparaat-Naam} > Toepassingen > Tracker:

Controleer onder Individuele Tracker en bekijk de statistieken van de tracker (Tracker Types,

Status, Endpoint Type, Endpoint Type, VPN Index, Host Name, Round Trip Time) op basis van uw geconfigureerde Tracker Naam.

- Via SD-WAN Manager: Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van klappen die op de tracker worden gedetecteerd, zouden de betreffende logboeken in deze sectie worden ingevuld met details zoals hostnaam, aanhechtingspunt-naam, tracker-naam, nieuwe staat, adresfamilie, en VPN-id.

Op CLI (CLI) van de edge:

```
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
```

Interface-endpointtrackers gebruikt voor Service Fabric 2.0

Service Fabric 2.0 Tracking, die werd geïntroduceerd in 20.13/17.13 release, is een verbeterde versie van de service insertion 1.0 tracking - waarbij gebruikers de mogelijkheid krijgen om de trackers op grotere schaal aan te passen. Het standaardgedrag wordt behouden van de vorige versie van Service Insertion (1.0), zou een tracker geïnitieerd worden door standaard met de definitie van elk serviceadres (of het doorsturen van adres) in een service-HA-paar per rx/tx. Maar met Service Insertion 2.0 kan het traceringsadres (IP/endpoint naar het bijgehouden adres) worden gescheiden van het verzendadres (gewoonlijk het serviceadres). Dit gebeurt met behulp van aangepaste endpointtrackers die op VPN-niveau zijn gedefinieerd. Ga voor meer informatie over Service Fabric 2.0-trackers naar de configuratiehandleiding.

Als de gebruiker ervoor kiest om de standaard tracker te gebruiken, zijn de specificaties van de tracker sondes:

- Hello: 1 sonde om de 30 seconden
- Vermenigvuldiger: 3 keer
- Type pakket/sonde: ICMP-echo/echo-antwoord

Als de gebruiker ervoor kiest om een aangepaste tracker te gebruiken, dan zijn de specificaties van de tracker sondes:

- Hello: 1 sonde om de 60 seconden
- Vermenigvuldiger: 3 keer
- Type pakket/sonde: ICMP-echo-verzoek/antwoord

Use cases

Ook hier zijn de in de voorgaande secties vermelde gebruikscases van Service Insertion 1.0 van toepassing.

Configuratie

Er is ondersteuning voor workflowgebaseerde configuratie voor Service Insertion 2.0, een benadering waarbij gebruik wordt gemaakt van een wizard, waardoor de gebruikerservaring wordt vereenvoudigd, terwijl de standaard workflowstappen van de Configuratiegroep worden gevolgd.

1. Definieer de groep Serviceketen - Configuratie onder de sectie Configuratie > Service insertion > Serviceketendefinities:

a. Klik op de knop Add Service Chain Definition.

b. Vul de details van de Naam en Beschrijving van de Dienst in.

c. Vul een lijstformaat in (door uit de vervolgkeuzelijst te selecteren), het Type van Dienst.

2. Definieer de groep Service Chain Instance - Configuration onder de sectie Configuration > Service insertion > Service Chain Configuration:

a. Klik op Servicekettingconfiguratie toevoegen.

b. Selecteer in de stap Service Chain Definition de radioknop Select Existing en kies de eerder gedefinieerde Service.

c. Geef een naam en beschrijving voor de stap Start Service Chain Configuration.

d. Selecteer in de stap Service Chain Configuration voor Handmatig verbonden services de Service Chain VPN-ID.

e. Geef vervolgens voor elke gedefinieerde service in de service chain-instantie (weergegeven in subtabs), onder servicedetails, het type bijlage (IPv4, IPv6 of Tunnel Connected).

f. Selecteer het selectievakje Geavanceerd. Als u actieve back-up/HA-gebruikscases nodig hebt (laat ook de Add parameters voor Backup knop toe) of zelfs als u een aangepaste endpointtracker moet definiëren (laat ook de Custom Tracker knop toe).

g. Als u scenario's hebt waarin het uitgaande (tx) verkeer via één interface naar de service gaat en het terugkeerverkeer van de service via een andere interface wordt ingedrukt (rx), zet u het Traffic

from service aan op een andere knop.

h. Met de knoppen Advanced en Custom Tracker ingeschakeld definieert u het IPv4-adres voor services (adres voor doorsturen), de SD-WAN-routerinterface (verbinding met de service) en het Tracker-endpoint (trackingadres). U kunt ook de aangepaste tracker-parameters wijzigen zoals interval en multiplier (door op de bewerkingsknop te klikken).

i. Herhaal de stappen (e), (f), (g) en (h) voor elke later gedefinieerde service.

3. Hang de instantie voor de serviceketen aan het configuratieprofiel van de Edge - Configuration-groep onder Configuratie > Configuratiegroepen > Serviceprofiel > Service VPN > Add Feature > Service Chain Attachment Gateway:

a. Geef een naam en beschrijving aan dit pakket voor de Service Chain Attachment Gateway.

b. Selecteer de eerder gedefinieerde Service Chain Definition (in stap 1).

c. Voeg de details opnieuw toe/controleer deze zoals uitgevoerd in stap 2. Voor de definitie van tracker is het enige verschil met de voorgaande stap 2 dat u de kans krijgt om een Tracker-naam te geven en ook het Tracker-type te selecteren (van service-icmp tot ipv6-service-icmp).

Vanuit het CLI-standpunt zien de configuraties er zo uit:

```
!
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
!
```

Verificatie

- Op SD-WAN Manager Monitor > Apparaten > {selecteer Apparaat-Naam} > Toepassingen > Tracker:

Controleer onder Individuele Tracker en bekijk de statistieken van de tracker (Tracker Types, Status, Endpoint Type, Endpoint Type, VPN Index, Host Name, Round Trip Time) op basis van uw geconfigureerde Tracker Naam.

- Op SD-WAN Manager Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van klappen die op de tracker worden gedetecteerd, zouden de betreffende logboeken in deze sectie worden ingevuld met details zoals hostnaam, aanhechtingspunt-naam, tracker-naam, nieuwe staat, adresfamilie, en VPN-id.

Op CLI (CLI) van de edge:

```
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
```

Statische-route-endpointtrackers gebruikt voor statische routertracering (servicekant)

Het tweede type van endpointtrackers wordt aangeduid als statische-route-gebaseerde endpointtrackers. Zoals de naam zelf aangeeft, worden deze soorten trackers voornamelijk

gebruikt om het volgende-hop adres van elke statische route te volgen die is gedefinieerd onder de Service-Side VPN. Standaard worden alle "verbonden" en "statische" routetypen geadverteerd in het OMP-protocol - post waar alle externe sites die de respectievelijke service VPN bevatten zich bewust worden van dat doelprefix (waar het volgende-hop punt naar de TLOC van de oorspronkelijke site). De bronlocatie is de locatie waar de specifieke statische route is geïnitieerd.

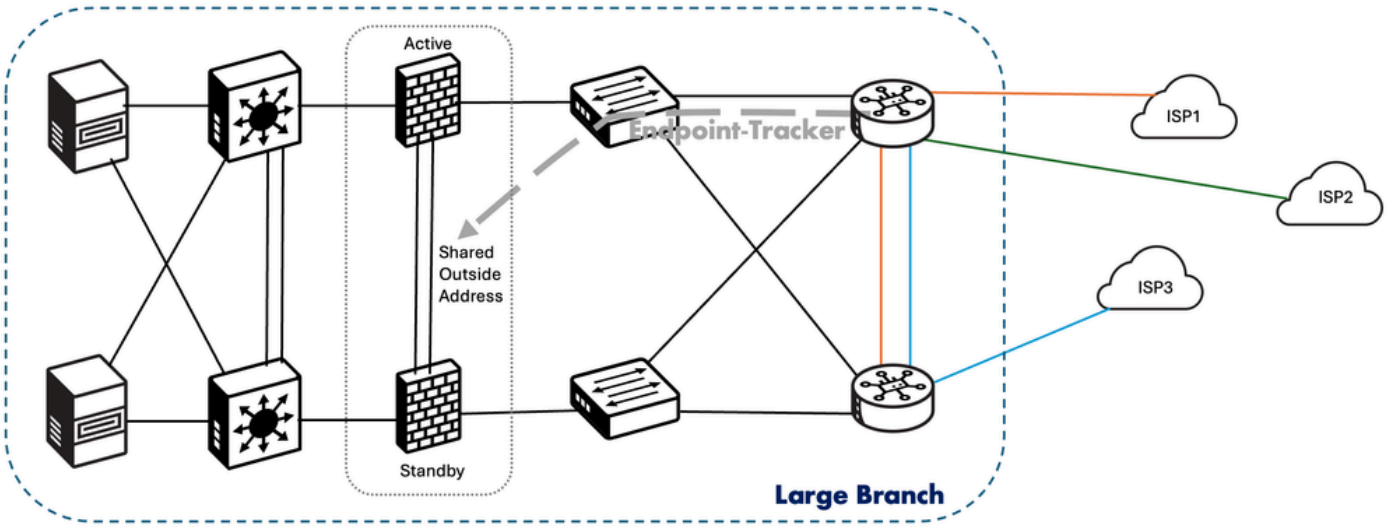
Echter, in het geval dat het volgende-hop adres in de statische route onbereikbaar wordt, stopt de route niet geadverteerd in OMP. Hierdoor zou het verkeer gehinderd worden voor stromen die bestemd zijn voor de plaats van oorsprong. Dit brengt de noodzaak met zich mee om een tracker aan de statische route te koppelen, om er zeker van te zijn dat de advertentie van de statische route alleen in OMP wordt geplaatst wanneer het volgende-hop adres bereikbaar is. Deze functie is geïntroduceerd in 20.3/17.3 release voor standaard IP-adrestype statische-route-gebaseerde endpointtrackers. Vanaf de release 20.7/17.7 werd ondersteuning toegevoegd voor het verzenden van trackersondes naar alleen bepaalde TCP- of UDP-poorten van het IP-adres van de volgende hop (in gevallen waarin firewalls worden gebruikt om alleen bepaalde poorten te openen voor traceringsdoeleinden). Om meer te weten te komen over statische routertrackers, bezoek de configuratiehandleiding.

Het type sondes dat hier wordt gebruikt, is een eenvoudig ICMP echo-request pakket. De gebruikte intervallen zijn:

- Hello: 60 seconden
- Wachtstandtijd: 180 seconden (aangezien #retries 3 = 3 x 60 seconden is)
- Type pakket/sonde: ICMP-echo/echo-antwoord

Use cases

Dit type van statisch-route-gebaseerde endpointtrackers wordt gebruikt voor het volgen van de servicekant van next-hop adressen in statische routes. Eén zo'n gemeenschappelijk scenario zou zijn het volgen van het LAN-side next-hop adres dat overeenkomt met een paar actieve/stand-by firewalls, die het Outside IP-adres delen op basis waarvan de Outside interface de rol van "actieve" firewall speelt. In gevallen waarin firewallregels zeer restrictief lijken te zijn, waarbij alleen bepaalde poorten worden geopend voor gebruik op case gebaseerde doeleinden, kan de statische routertracker worden gebruikt om de specifieke TCP/UDP-poort te volgen naar het IP-adres van de volgende hop dat behoort tot de LAN-side firewall Outside interface.



Configuratie

Deze op statische route gebaseerde endpointtrackers moeten handmatig worden geconfigureerd om deze functieset in te schakelen. Hier zijn de manieren om het, afhankelijk van het type van configuratiemethode te vormen die door de gebruiker de voorkeur heeft.

- Configuratie-groep Configuratie > Configuratiegroepen > Serviceprofiel > Service VPN > Functie toevoegen > Tracker:

1. Geef een naam, beschrijving en trackernaam op voor de nieuwe (endpoint) tracker die wordt gedefinieerd.

2. Kies het type eindpunt, afhankelijk van of u alleen het IP-adres van de volgende hop moet volgen (kies radioknop Adres), of zelfs specifieke TCP/UDP-poorten (kies radioknop Protocol).

3. Voer het adres in als IP-adresformaat. Voer ook het protocol (TCP of UDP) en het poortnummer in voor het geval u in de vorige stap Protocol hebt gekozen als type eindpunt.

4. U kunt de standaardwaarden voor sonde-interval, aantal pogingen en Latency Limit, indien nodig wijzigen.

- Configuratie > Configuratiegroepen > Serviceprofiel > Service VPN > Route sectie:

1. Selecteer de knop IPv4/IPv6 statische route toevoegen.

2. Vul de details in, zoals Netwerkadres, Subnetmasker, Next-hop, Adres, AD.

3. Klik op de knop Volgende hop met tracker toevoegen.

4. Voer het adres van de volgende hop opnieuw in, AD en kies uit de vervolgkeuzelijst de naam van de vorige gemaakte (endpoint) tracker.

- Verouderde configuratie Configuratie > Sjablonen > Functiesjablonen > Systeemsjabloon > sectie Tracker:

1. Selecteer de knop New Endpoint Tracker.

2. Geef een naam op voor de nieuwe (endpoint) tracker die wordt gedefinieerd.

3. Verander de radioknop Tracker Type in statische route.

4. Kies het type eindpunt als IP-adres van de volgende hop (kies de keuze voor de radio IP-adres).

5. Voer het IP-eindpunt in in een IP-adresformaat.

6. U kunt de standaardwaarden voor sonde-interval, aantal pogingen en Latency Limit, indien nodig wijzigen.

- Configuratie > Sjablonen > Functiesjablonen > Cisco VPN (ALLEEN servicekant) > IPv4/IPv6-routesectie:

1. Selecteer de knop Nieuwe IPv4/IPv6-router.

2. Vul de details in, zoals Prefix, Gateway.

3. Klik op de knop Volgende hop met tracker toevoegen.

4. Voer het adres van de volgende hop, de AD (Afstand) opnieuw in en voer handmatig de vorige naam van de tracker in die is gemaakt (eindpunt).

Vanuit het CLI-standpunt zien de configuraties er zo uit:

```
(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
!
```

Verificatie

Er zijn twee gebieden van verificatie van expliciet geconfigureerde endpointtrackers.

- Op SD-WAN Manager Monitor > Apparaten > {selecteer Apparaat-Naam} > Real Time:

1. Typ onder Apparaatopties "Endpoint Tracker Info."

2. Controleer onder Individuele Tracker (Attach Point Name) en bekijk de statistieken van de tracker (Tracker State, Associated Tracker Record Name, Latency in mx van apparaat naar het eindpunt, Laatst bijgewerkt tijdstempel) op basis van uw geconfigureerde Tracker Name.

- Op SD-WAN Manager Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van klappen die op de tracker worden gedetecteerd, zouden de betreffende logboeken in deze sectie worden ingevuld met details zoals hostnaam, aanhechtingspunt-naam, tracker-naam, nieuwe staat, adresfamilie, en VPN-id.

Op CLI (CLI) van de edge:

```
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]
```

Interfaceobjecttrackers gebruikt voor VRRP-tracering

Object Trackers zijn trackers ontworpen voor autonoom verbruik (use cases). Deze trackers hebben gebruikscases die variëren van VRRP-gebaseerde interface/tunneltracering tot Service-VPN NAT-tracering.

Voor VRRP-tracering wordt de VRRP-status bepaald op basis van de tunnellinkstatus. Als de tunnel of de interface op de primaire VRRP onderaan is, wordt het verkeer geleid naar de secundaire VRRP. De secundaire VRRP-router in het LAN-segment wordt de primaire VRRP om gateway te bieden voor dienstverkeer. Deze use case is alleen van toepassing voor service-VPN en helpt bij falen via de VRRP-rol aan de LAN-kant in het geval van storing op de SD-WAN overlay (interface of tunnels in het geval van SSE). Voor het aansluiten van trackers op VRRP-groepen kunnen ALLEEN objecttrackers worden gebruikt (geen endpointtrackers). Deze functie is geïntroduceerd vanaf 20.7/17.7 release voor Cisco Catalyst SD-WAN randen.

Er worden hier geen sondes gebruikt door de tracker. In plaats daarvan, gebruikt het de lijn-protocol staat om over de tracker staat (up/down) te beslissen. Er zijn geen reactieintervallen in op interfacelijn-protocol gebaseerde trackers - het moment dat het interface/tunnellijn-protocol omlaag gaat, wordt de spoorstaat ook naar beneden gebracht. Afhankelijk van de actie van ofwel shutdown of decrement, zou de VRRP groep dienovereenkomstig opnieuw samenkomen. Om meer te weten te komen over VRRP-interfacetrackers, bezoek de configuratiehandleiding.

Use cases

Er zijn meerdere gebruikscases gebaseerd op de criteria die vereist zijn voor het implementeren van VRRP-gebaseerde interface tracking. Momenteel zijn de twee ondersteunde modi (i) interface (dat wil zeggen elke tunnelinterface die is gebonden met een lokale TLOC) of (ii) SIG interface (die betrekking heeft op SIG tunnelinterfaces). In elk geval is het deel dat wordt bijgehouden het protocol van de interfacelijn.

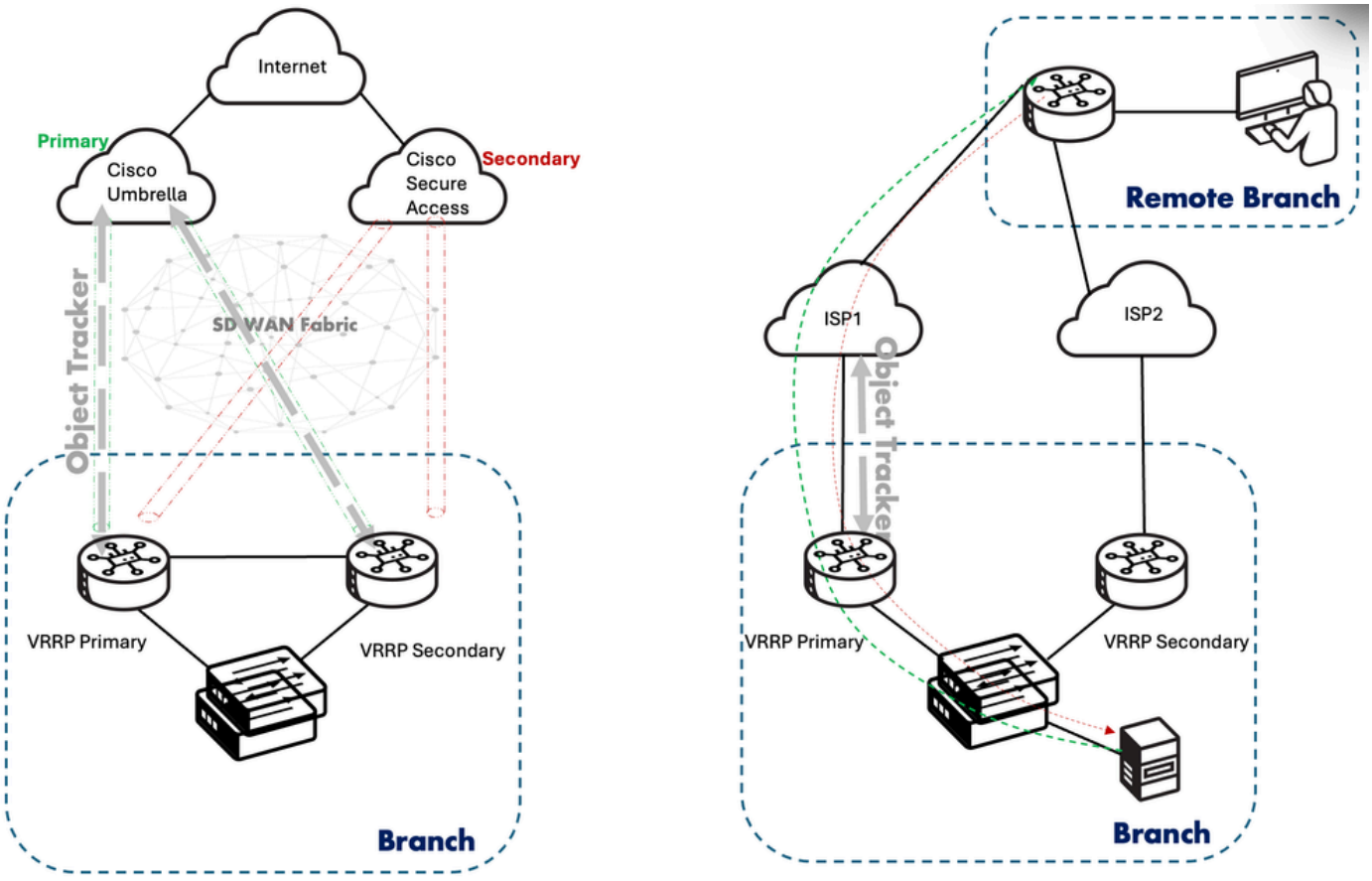
Dubbele router met internet: Het object track is gebonden aan de VRRP-groep. In het geval dat het object van de tracker (die in dit geval de SIG tunnelinterface is) daalt, waarschuwt dit de VRRP Primaire router om de staatsovergang van Primair naar back-up te activeren en de back-uprouter om Primair te worden. Deze toestandsverandering kan door twee types van verrichtingen worden beïnvloed of worden teweeggebracht:

1. Besluit : Waar de VRRP-prioriteit voor de interface waarop VRRP VIP is geconfigureerd

wordt verminderd of verlaagd met een bepaalde waarde, in het geval de spoorobjecten staat overgangen van UP naar DOWN.

2. Shutdown: Dit is een methode waarbij het VRRP-proces wordt afgesloten op de toegepaste interface, in het geval dat de spoorobject status overgaat van UP naar DOWN. Deze methode wordt niet aanbevolen bij gebruik in gevallen waarin sprake is van asymmetrische doorsturen.

TLOC-wijzigingsvoorkeur: om te voorkomen dat asymmetrisch verkeer van andere SDWAN-sites naar de site komt waar VRRP op service VPN draait, wordt de TLOC-voorkeur van de VRRP Primaire router, indien geconfigureerd, vergroot met 1. U kunt deze waarde zelfs aanpassen onder configuratiegroepen. Dit zorgt ervoor dat verkeer van WAN naar LAN wordt aangetrokken door de VRRP Primaire router zelf. Het verkeer van LAN naar WAN wordt aangetrokken door VRRP-mechanisme van VRRP Primary. Deze optie is onafhankelijk van de VRRP-interfacetracker. Dit is een optionele opdracht (tloc-change-pref) vanuit het CLI-standpunt.



Configuratie

De configuratie van objecttrackers gebeurt via systeemsjablonen in Verouderde configuratie, en vervolgens de objecttracker toevoegen aan de betreffende VRRP-groep onder de service-VPN Ethernet-interfacekaart. In de Configuratiegroep is dit mechanisme vereenvoudigd door direct een optie te krijgen om de objecttracker toe te voegen aan het betreffende Ethernet-interfaceprofiel van het serviceprofiel. Hier zijn de manieren om het te configureren, afhankelijk van het type configuratiemethode waaraan de gebruiker de voorkeur geeft.

- Configuratie groep Configuratie > Configuratiegroepen > Serviceprofiel > Ethernet-interface

> Functie toevoegen > Objecttracker:

1. Geef een naam en beschrijving voor de nieuwe objecttracker die wordt gedefinieerd.
2. Selecteer het Tracker-type (tussen Interface en SIG).
3. Wijs een Object Tracker-id toe.
4. Geef de interfacenaam op (afhankelijk van de optie die in stap 2 is gekozen).

- Configuratie > Configuratiegroepen > Serviceprofiel > Ethernet-interface > VRRP-sectie:

1. Klik onder IPv4-instellingen op VRRP IPv4 toevoegen.
2. Definieer een VRRP Group-id en geef een lokale prioriteit aan voor deze Ethernet-interface aan servicekant.
3. Geef het VRRP Virtual IP (VIP) adres op.
4. Schakel de knop TLOC Preference Change in en geef ook de TLOC Preference Change Value (om asymmetrische routing te verwerken).
5. Klik op VRRP-traceringsobject toevoegen.
6. Selecteer onder Associate Object Tracker uit de vervolgkeuzelijst op de Object Tracker (gebaseerd op naam) die u eerder hebt gemaakt
7. Kies een Tracker-actie (ofwel sluiting of beslissing).
8. Voer de drempelwaarde in (afhankelijk van de in stap 7 gekozen optie).

- Verouderde configuratie Configuratie > Sjablonen > Functiesjablonen > Systeem > Tracker-sectie:

1. Klik op de knop New Object Tracker.
2. Selecteer het Tracker-type (tussen Interface en SIG).
3. Wijs een object-id toe.
4. Geef de interfacenaam op (afhankelijk van de optie die in stap 2 is gekozen).

- Configuratie > Sjablonen > Ethernet-interface (aan servicekant) > VRRP-sectie:

1. Klik op de knop Nieuwe VRRP.
2. Definieer een VRRP Group ID en geef een lokale Prioriteit (optioneel, standaardwaarde van 100 is gekozen) voor deze Ethernet-interface aan servicekant.
3. Geef het VRRP Virtual IP (VIP) adres op.
4. Schakel de knop TLOC Preference Change in en geef ook de TLOC Preference Change Value (om asymmetrische routing te verwerken).
5. Klik onder Object Tracker op Add Tracking Object.
6. Voer de Object Tracker-id in (gedefinieerd onder systeemsjabloon).
7. Kies een Tracker-actie (ofwel sluiting of beslissing).
8. Voer de drempelwaarde in (afhankelijk van de in stap 7 gekozen optie).

Vanuit het CLI-standpunt zien de configuraties er zo uit:

```
(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
!
```

Verificatie

Er zijn twee opties om expliciet geconfigureerd object trackers te verifiëren voor VRRP use cases.

- Op SD-WAN Manager Monitor > Apparaten > {selecteer Apparaat-Naam} > Real Time:

1. Typ onder Apparaatopties "VRRP-informatie".

2. Controleer onder Individuele VRRP Group (Group ID) en bekijk de statistieken van de tracker (Track Prefix Name, Track State, Discontinuity Time, en Last State Change Time) op basis van uw geconfigureerde Object Tracker ID’s.

- Op SD-WAN Manager Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van staatsverandering die op de objecttracker is gedetecteerd, verandert de corresponderende VRRP-groep waaraan het is gekoppeld zijn status. De respectievelijke logs worden ingevuld in deze sectie (met de naam als Vrp Group State Change) met details zoals hostnaam, if number, grp id, addtype, if name, vrp group-state, state change-rede, en vpn id.

Op CLI (CLI) van de edge:

```
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)
```

Interface-/routeobjecttrackers gebruikt voor Service-VPN NAT-

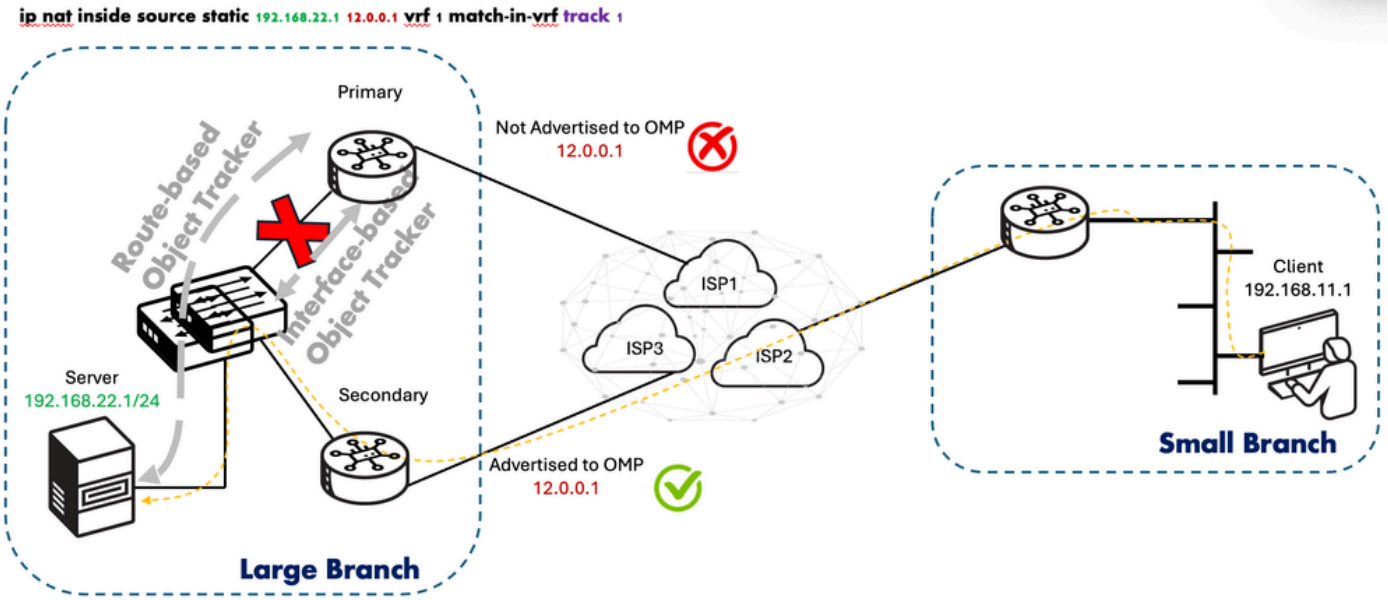
tracering

De service-side NAT Object Tracker was een functie die werd geïntroduceerd in 20.8/17.8 release, waarin het ingebouwde globale adres dat wordt gebruikt in service-VPN NAT (binnen statische NAT en binnen dynamische NAT) alleen wordt geadverteerd in OMP als (i) het binnen lokale adres bereikbaar blijkt te zijn OF (ii) het lijnprotocol van de LAN/service-side interface UP is zoals in de bijgevoegde object tracker. De objecttracker die kan worden gebruikt is dan ook i) route of ii) interface. Afhankelijk van de status van het LAN prefix of LAN interface, NAT route advertenties via OMP worden toegevoegd of verwijderd. U kunt gebeurtenislogboeken in Cisco SD-WAN Manager bekijken voor de controle van welke NAT routeradvertenties worden toegevoegd of verwijderd.

Er worden hier geen sondes gebruikt door de tracker. In plaats daarvan maakt het gebruik van (i) de aanwezigheid van een routinginvoer in de routeringstabel OF (ii) de lijnprotocolstaat om te beslissen over de trackerstaat (up/down). Er zijn geen reactie-intervallen in de aanwezigheid van een routinginvoer of op interfacelijn-protocol gebaseerde trackers - het moment dat de routinginvoer of het interfacelijn-protocol omlaag gaat, wordt de spoorstaat ook naar de DOWN-staat gebracht. Onmiddellijk wordt het binnen globale adres dat in de NAT verklaring wordt gebruikt verbonden aan de objecten tracker tegengehouden van geadverteerd in OMP. Om meer over Service VPN NAT trackers te leren, gelieve de configuratiegids te bezoeken.

Use cases

Als een LAN interface of LAN prefix neer is, gaat de dienst-kant NAT objecten tracker automatisch omlaag. U kunt eventlogboeken bekijken Cisco SD-WAN Manager voor controle welke NAT routeradvertenties worden toegevoegd of verwijderd. In de volgende use case moet de client toegang hebben tot de server in de grote branch. Het probleem doet zich echter voor in situaties waarin de route die naar de server wijst op de grote randen van de vertakking (in HA) wordt verwijderd OF wanneer de LAN-kant (service-side) interface naar beneden gaat op elke rand in de grote vertakking. In dergelijke situaties, wanneer u de dienst-kant NAT met objecten tracker toepast, zorg ervoor - dat het verkeer dat van de cliënt binnenkomend komt altijd wordt geleid naar de juiste rand in de grote tak door de binnen globale adresreclame in OMP te controleren. Als een dergelijke controle niet wordt afgedwongen op de routeradvertentie in OMP, wordt het verkeer uiteindelijk zwart gegrepen door de onbereikbaarheid van die respectieve rand naar de server in de grote tak.



Configuratie

De configuratie van objecttrackers gebeurt via systeemsjablonen in Verouderde configuratie, en vervolgens de objecttracker aan de respectievelijke NAT-verklaring (binnen statisch of binnen dynamisch) in de service-VPN-functiemaljabloon. In de Configuratiegroep is dit mechanisme vereenvoudigd door direct een optie te krijgen om de objecttracker toe te voegen aan het betreffende Ethernet-interfaceprofiel van het serviceprofiel. Hier zijn de manieren om het te configureren, afhankelijk van het type configuratiemethode waaraan de gebruiker de voorkeur geeft.

- Configuratie groep > Configuratiegroepen > Serviceprofiel > Functie toevoegen > Objecttracker:

1. Geef een naam en beschrijving voor de nieuwe objecttracker die wordt gedefinieerd.
2. Selecteer het type tracker (tussen interface en route).
3. Wijs een Object Tracker-id toe.
4. De interfacenaam opgeven OF de routeopties IP, IP-masker en VPN leveren (afhankelijk van de optie die in stap 2 is gekozen).

- Configuratie > Configuratiegroepen > Serviceprofiel > NAT-sectie:

1. Maak een NAT-pool (verplicht voor het activeren van SNAT) door op de knop NAT-pool toevoegen te klikken.

2. Geef de details van de NAT-pool op, zoals de naam van de NatPool, de prefixlengte, het begin van het bereik, het einde van het bereik en de richting.

3. Verplaats naar Statische NAT in dezelfde sectie en klik op de knop Nieuwe Statische NAT toevoegen. (U kunt er ook voor kiezen om de objecttracker aan te sluiten op de binnenzijde van de dynamische pool NAT).

4. Verstrek de details zoals Bron IP, Vertaalde Bron IP, en Statische NAT Richting.

5. Kies in het veld Associate Object Tracker uit de vervolgkeuzelijst de eerder gemaakte objecttracker.

- Verouderde configuratie Configuratie > Sjablonen > Functiesjablonen > Systeem > Tracker-sectie:

1. Klik op de knop New Object Tracker.
2. Selecteer het type tracker (tussen interface en route).
3. Wijs een object-id toe.
4. Geef de interfacenaam OF routebeschrijving op voor IP, routeIP-masker en VPN (afhankelijk van de optie die in stap 2 is gekozen).

- Configuratie > Sjablonen > Cisco VPN (aan servicekant) > NAT-sectie:

1. Maak een NAT-pool (verplicht voor het activeren van SNAT) door op de knop New NAT Pool te klikken.

2. Verstrek de details van de NAT-pool, zoals de naam van de NAT-pool, de lengte van het NAT-poolprefix, het begin van het NAT-poolbereik, het einde van de NAT-poolbereik en de NAT-richting.

3. Verplaats naar Statische NAT in dezelfde sectie en klik op de knop Nieuwe Statische NAT. (U kunt er ook voor kiezen om de objecttracker aan te sluiten op de binnenzijde van de dynamische pool NAT).

4. Geef de details zoals IP-bronadres, vertaald IP-bronadres en statische NAT-richting.

5. Typ onder het veld Add Object Tracker de naam van de eerder gemaakte objecttracker.

Vanuit het CLI-standpunt zien de configuraties er zo uit:

```
(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
!
```

Veronderstelling met SSNAT-gebruikscase is dat gebruikers databeleid toepassen om verkeer aan te passen voor zowel in -> uit als uit -> in NAT-stromen.

Verificatie

Er zijn twee gebieden van verificatie van expliciet geconfigureerde objecttrackers voor NAT-gebruikscases.

- Op SD-WAN Manager : Monitor > Apparaten > {selecteer Apparaat-Naam} > Real Time:

1. Typ onder Apparaatopties "IP NAT-omzetting".

2. Controleer onder Individuele NAT-omzetting en bekijk de statistieken van de ingang (Binnen lokaal adres/poort, Binnen mondiaal adres/poort, Buiten lokaal adres/poort, Buiten mondiaal adres/poort, VRF-id, VRF-naam en protocol) op basis van uw geconfigureerde Object Tracker-id's.

- Op SD-WAN Manager : Monitor > Apparaten > {selecteer Apparaat-Naam} > Gebeurtenissen:

In het geval van staatsverandering die op de objecttracker wordt gedetecteerd die overeenkomt met de NAT-route die in OMP wordt gesnoeid, worden gebeurtenissen met de naam "NAT Route Change" weergegeven, die details bevatten zoals hostnaam, objecttracker, adres, masker, routetype en update. Hier, de adres en maskerkaarten aan het binnen globale adres zoals gevormd onder de statische NAT- verklaring.

Op CLI (CLI) van de edge:

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.