Catalyst SD-WAN Tracker - Nutzbarkeit und Anwendungsfälle

Inhalt

Einleitung

In diesem Dokument werden die Catalyst SD-WAN Enterprise Overlay-Netzwerke, die Nachverfolgbarkeit und Anwendungsfälle beschrieben.

Hintergrundinformationen

Die Catalyst SD-WAN-Overlay-Netzwerke interagieren in der Regel mit einer Vielzahl von externen Workloads, Anwendungen und Services. und zwar sowohl in der Cloud als auch in Rechenzentren/Hubs oder an entfernten Standorten. Die SD-WAN-Kontrollebene ist für die skalierbare Bereitstellung von Routen zu diesen Services über das Overlay verantwortlich. In Situationen, in denen kritische Anwendungen und Services entlang eines bestimmten Pfads nicht mehr erreichbar sind, müssen Netzwerkbetreiber in der Regel in der Lage sein, diese Ereignisse zu erkennen und den Benutzerdatenverkehr an geeignetere Pfade umzuleiten, um Blackholing für unbestimmten Datenverkehr zu verhindern. Zur Erkennung und Behebung derartiger Netzwerkausfälle benötigt die Catalyst SD-WAN-Kontrollebene Tracker, die den Zustand externer Services überwachen und ggf. Routing-Änderungen vornehmen.

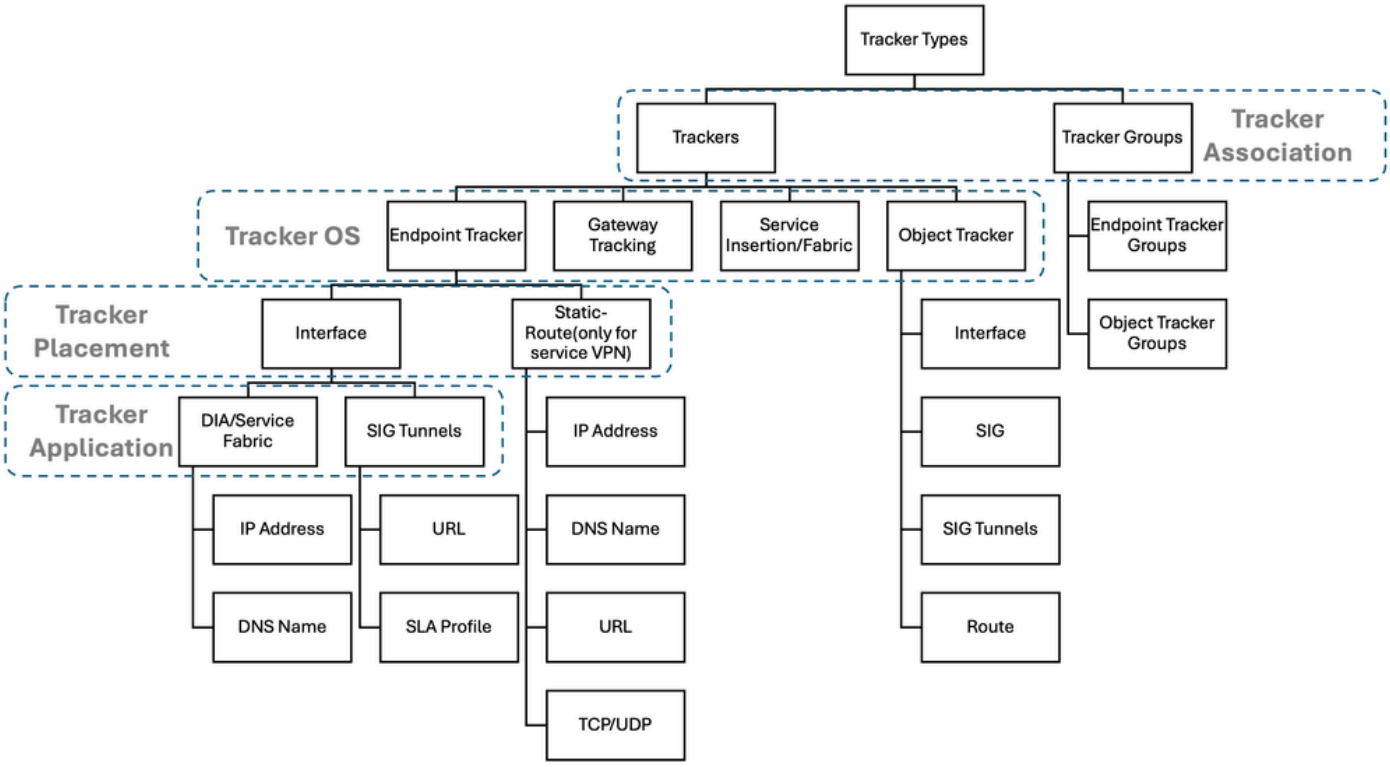
Ein Tracker ist ein Mechanismus zur Erkennung der Erreichbarkeit auf Kontrollebene, der Testpakete an ein bestimmtes Endgerät sendet und interessierte Module über Änderungen des Erreichbarkeitsstatus (aktiv oder inaktiv) des Endgeräts informiert. Trackers sind als skalierbare Abstraktion der nativen Cisco IOS-XE® IP SLA-Funktion konzipiert, die eine Vielzahl von Tests (einschließlich HTTP, ICMP und DNS) bilden kann. Wenn ein Tracker ein Client-Modul über eine Statusänderung informiert, kann dieses Modul geeignete Maßnahmen ergreifen, um Datenverkehr-Blackholing zu verhindern, z. B. die Installation oder Deinstallation einer Route oder eines Routensatzes. Die aktuellen Anwendungen von Trackern innerhalb SD-WAN- und SD-Routing-Lösungen umfassen u. a.: DIA-Tracker (Direct Internet Access), SIG-Tracker (Secure Internet Gateway), Service-Tracker, statische Routen-Tracker, Tracker-Gruppen usw.

Für den Aufbau hochverfügbarer Netzwerke, die vor Serviceausfällen geschützt sind, ist es wichtig zu wissen, wann die einzelnen Tracker-Konfigurationen/-Modelle verwendet werden müssen. Ziel dieses Artikels ist es, zu erklären, wo und wie jeder Tracker-Typ verwendet wird. Hier werden die verschiedenen Tracker sowie der primäre Anwendungsfall der einzelnen Tracker und die grundlegenden Konfigurations-Workflows zur Implementierung der einzelnen Lösungen behandelt. Schließlich wird in diesem Artikel eine schrittweise Einführung in allgemeine Probleme mit Trackern in Cisco IOS-XE® gegeben.

In diesem Artikel wird zwischen den Lösungen Endpoint-Tracker (SD-WAN- und SD-Routing-spezifisch) und Object-Tracker (natives IOS-XE) unterschieden, die verschiedene Anwendungsfälle berücksichtigen.

Arten von Trackern

Dieses Diagramm bietet eine kurze Übersicht über alle in der Cisco Catalyst SD-WAN-Lösung verfügbaren Tracker:



Aus dem vorherigen Diagramm gibt es vier Bereiche, in denen Tracker klassifiziert werden können: Tracker Association, Tracker OS, Tracker Placement und Tracker Application. Im nächsten Abschnitt werden die einzelnen Klassifizierungen beschrieben:

1. Tracker-Zuordnung: Diese Klassifizierung beschreibt, ob ein Tracker ein einzelner Tracker oder eine Tracker-Gruppe ist. Cisco Catalyst SD-WAN unterstützt die Verwendung mehrerer Tracker in einer Gruppe (bis zu zwei zum gegenwärtigen Zeitpunkt). Der Gesamtstatus der Tracker-Gruppe wird durch einen Booleschen AND- oder OR-Operator bestimmt. Beispiele sind eine Endpunkt-Nachverfolgungsgruppe oder eine Objektverfolgungsgruppe.
2. Tracker-Betriebssystem: Diese Klassifizierung beschreibt das Cisco IOS-XE® Betriebssystem bzw. den Modus, in dem der Tracker unterstützt wird. Cisco Catalyst IOS-XE-Router unterstützen zwei Betriebsmodi:

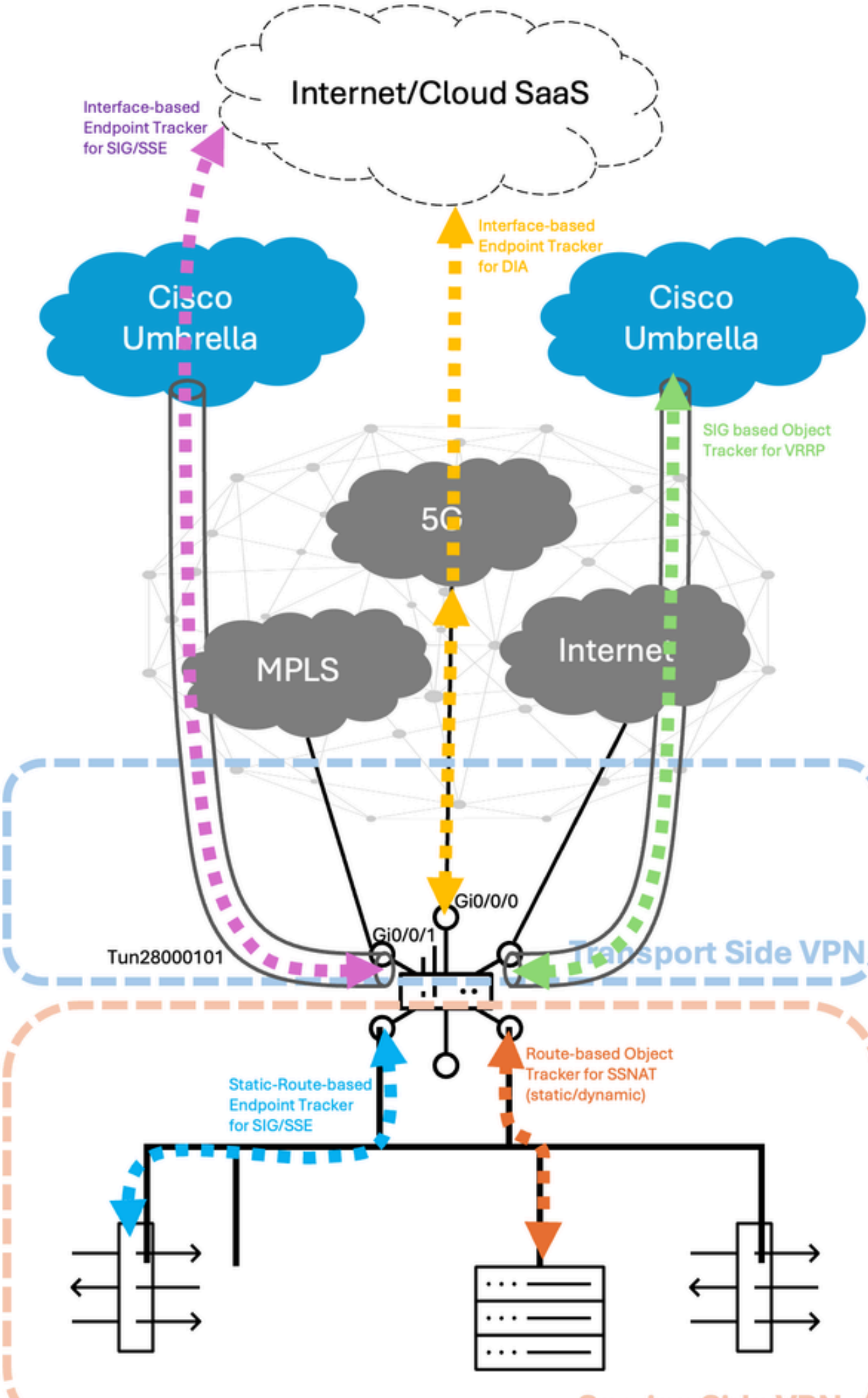
- Autonomer Modus und
- Controller-Modus.

Alle Funktionen zur Endpunktverfolgung und Gateway-Nachverfolgung sind für Anwendungsfälle im Controller-Modus (SD-WAN) vorgesehen, während der Objektverfolger für Anwendungsfälle im Autonomous-Mode (SD-Routing) vorgesehen ist.

3. Tracker-Platzierung: Diese Klassifizierung beschreibt den Ort, an dem der Tracker konfiguriert ist. Derzeit unterstützt Cisco Catalyst SD-WAN die Anwendung von Trackern auf Schnittstellen, statische Routen oder Services.

4. Tracker-Anwendung: Diese Klassifizierung beschreibt die allgemeinen Anwendungsfälle und Funktionen, die von Cisco Catalyst SD-WAN unterstützt werden. Es gibt zwar zahlreiche Anwendungsbereiche von Trackern, einige davon sind: Direct Internet Access (DIA), Secure Internet Gateway (SIG), Secure Service Edge (SSE), Service-Side VPN Tracking usw.

Die folgende Abbildung zeigt den Tracker-Probe-Verkehr über Service-/Transport-VPNs für verschiedene Anwendungsfälle am Cisco Catalyst SD-WAN-Edge (auch als cEdge oder vEdge bezeichnet):


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

verwendet wird, die auf SD-WAN-Edge-Plattformen im transportseitigen VPN konfiguriert sind. Diese Funktion ist standardmäßig unter den grundlegenden Systemprofilkonfigurationen (Track Default Gateway) im Catalyst SD-WAN Manager aktiviert. Dies hilft, die Next-Hop-Adresse, die unter jeder statischen Standardroute im Transport-VPN angegeben ist, kontinuierlich zu überwachen, um ein Link-/Routen-Failover sicherzustellen, falls die Erreichbarkeit zum Next-Hop (der auch als Gateway bezeichnet wird, daher der Name Gateway-Tracking) ausfällt. Weitere Informationen zur Gateway-Tracking finden Sie im Konfigurationsleitfaden.

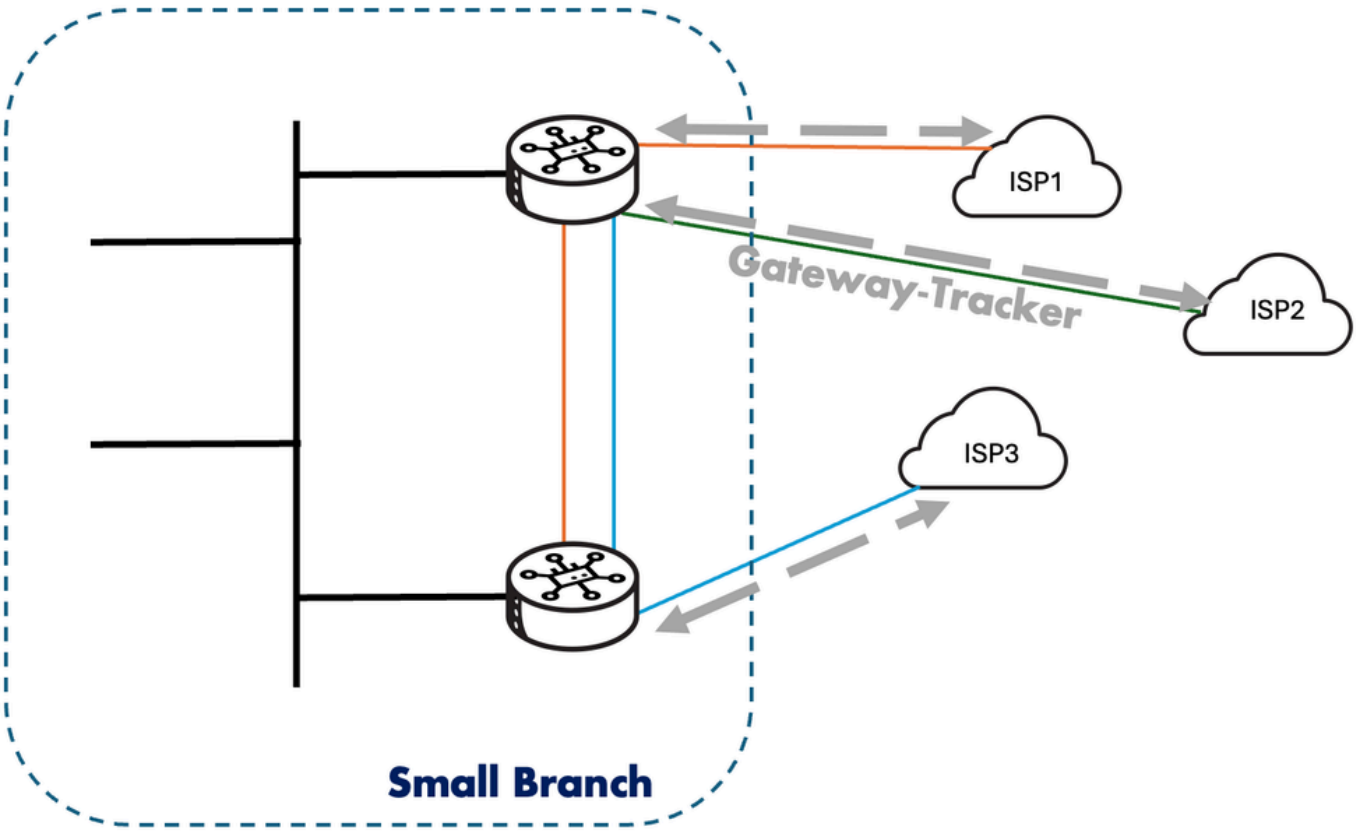
Bei den hier verwendeten Tests handelt es sich um geflutete Pakete mit ARP-Anforderungen und Unicast-Status. Folgende Intervalle werden verwendet:

- Hello: 10 Sekunden
- Haltefrist: 100 Sekunden
- Paket-/Testtyp: ARP

Neben der Gateway-Verfolgung wird auch die Transportverfolgung an SD-WAN-Edges verwendet, um den gerouteten Pfad zwischen dem lokalen Gerät und einem Cisco Catalyst SD-WAN Validator zu überprüfen. Dies geschieht durch die Verwendung von ICMP-Tests in einem regelmäßigen Intervall von 3 Sekunden. Dies wird mithilfe des Schlüsselworts "track-transport" im SD-WAN-Systemkonfigurationsmodus konfiguriert. Dies erleichtert die regelmäßige Überwachung der DTLS-Verbindung zum Cisco Catalyst SD-WAN Validator vom jeweiligen WAN-Edge aus. Weitere Informationen zur Transportüberwachung finden Sie im Konfigurationsleitfaden.

Anwendungsfälle

Die Gateway-Nachverfolgung ist eine Funktion, die standardmäßig auf dem SD-WAN für alle statischen Standardrouten konfiguriert wird, die zum Transport-VPN oder zur globalen Routing-Tabelle (GRT) gehören. Die Verwendung der Funktion stammt nicht immer vom Standpunkt der Manager-Vorlagenkonfiguration, sondern kann auch aus empfangenen/empfangenen statischen Standardrouten bei Verwendung eines DHCP-Servers mit den Optionen #3, #81 usw. abgeleitet werden.



Konfiguration

Standardmäßig angewendet im Cisco Catalyst SD-WAN:

```
!
system


 track-transport
 track-default-gateway


!
```

Verifizierung

Dies kann anhand der Legacy-Konfiguration und der Konfigurationsgruppe überprüft werden:

- Konfigurationsgruppe: Konfiguration > Konfigurationsgruppen > Systemprofil > Einfaches Unterprofil > Abschnitt "Track Settings" > Track Default Gateway (Standard: EIN)
- Legacy-Konfiguration: Konfiguration > Vorlagen > Funktionsvorlagen > Systemvorlage > Abschnitt "Erweitert" > Gateway-Verfolgung (Standard:EIN)

Nachverfolgung von Service Insertion 1.0 und Service Fabric 2.0

Service Insertion 1.0 Tracking wurde in Version 20.3/17.3 eingeführt und ist eine Funktion, die sicherstellen soll, dass die Service-Adresse (oder Weiterleitungsadresse) erreichbar oder verfügbar ist. Diese Informationen helfen dem Edge, Next-Hop-Informationen dynamisch zu der Steuerungs-/Datenrichtlinie hinzuzufügen oder aus dieser zu entfernen. Bei der Konfiguration von Service Insertion 1.0 wird der Tracker (oder die Nachverfolgungsadresse) standardmäßig für die Dienstadresse aktiviert. Basierend darauf sind Weiterleitungsadresse und Dienstadresse in 1.0 identisch. Obwohl Service Tracker automatisch mit Diensten konfiguriert werden, können diese Tracker mit dem Befehl no track-enable oder durch Deaktivieren des Tracker-Reglers in der Konfigurationsgruppe/Legacy-Konfiguration deaktiviert werden. Da dies die einzigen beiden möglichen Operationen (enable/disable) mit Trackern sind, die unter Service Insertion 1.0 mit Diensten verbunden sind, gibt es keine weiteren Parameter, die angepasst werden können (z.B. Schwellenwert, Multipler, Intervall).

Weitere Informationen zur Nachverfolgung von Diensteinfügungen 1.0 finden Sie im Konfigurationsleitfaden. Die Standardintervalle für die Nachverfolgung von Diensteinfügungen 1.0 sind:

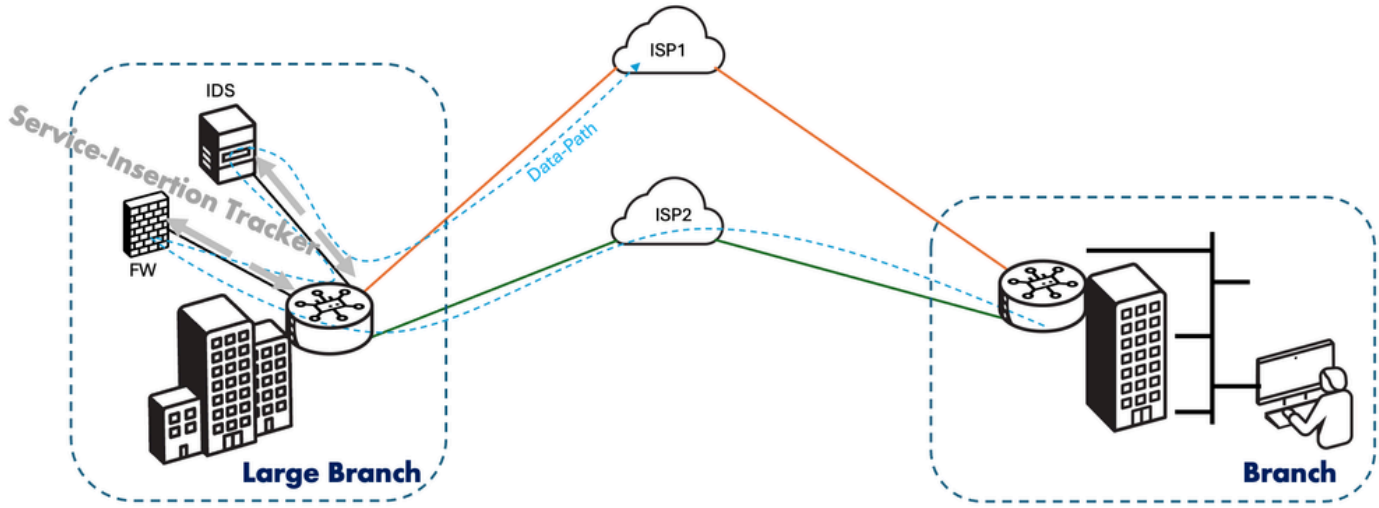
- Testintervall: 5 Sonden alle 60 Sekunden
- Multiplikator: 5 Mal
- Paket-/Testtyp: ICMP-Echo/Echo-Antwort

Service Fabric 2.0 Tracking ist Teil des Service Insertion 2.0-Feature-Angebots von Cisco Catalyst SD-WAN, das ab der Version 20.13/17.13 eingeführt wurde. Bei dieser neuen Variante der Diensteinfügung wird von den Konfigurationsprofilen und Vorlagen standardmäßig immer noch ein impliziter Tracker verwendet, der auf jede definierte Dienstadresse (oder Weiterleitungsadresse) in einem Service-HA-Paar pro rx/tx-Schnittstelle verweist. Mit Service Fabric 2.0 können Sie jetzt die Weiterleitungsadresse von der Nachverfolgungsadresse trennen. Hierzu können Sie einfach separate Endpunkt-Tracker definieren, mit denen eine andere Endpunkt-Adresse als die Service-Adresse verfolgt wird. In den nächsten Abschnitten wird dieses Thema noch ausführlicher behandelt.

Anwendungsfälle

Service Tracker dienen in erster Linie der skalierbaren Überwachung der Service-Erreichbarkeit, insbesondere der Service-Verkettung. Die Serviceverkettung kann in einem aus mehreren VPNs bestehenden Netzwerk bereitgestellt werden, wobei jedes VPN eine andere Funktion oder Organisation repräsentiert, um sicherzustellen, dass der Datenverkehr zwischen VPNs durch eine Firewall fließt. In einem großen Campus-Netzwerk kann der abteilungsübergreifende Datenverkehr beispielsweise durch eine Firewall geleitet werden, während der abteilungsinterne

Datenverkehr direkt weitergeleitet werden kann. Die Serviceverkettung kann in Szenarien gesehen werden, in denen ein Betreiber gesetzliche Auflagen erfüllen muss, wie z. B. beim Payment Card Industry Data Security Standard (PCI DSS), bei dem der PCI-Datenverkehr über Firewalls in einem zentralisierten Rechenzentrum oder regionalen Hub fließen muss:



Konfiguration

Die Konfigurationen entsprechen dem normalen Workflow für die Einrichtung von Service Insertion 1.0 im SD-WAN. Die Trackers von Service Insertion 1.0 sind standardmäßig für alle Service-Adressen aktiviert.

- Konfigurationsgruppe: Konfiguration > Konfigurationsgruppen > Serviceprofil > Service-VPN > Service-Abschnitt:

1. Klicken Sie auf die Schaltfläche Service hinzufügen.

2. Wählen Sie einen Servicetyp.

3. Geben Sie die Dienstadresse an (maximal 4 möglich, durch Komma getrennt).

4. Überprüfen Sie, ob der Regler Tracking (Verfolgung) standardmäßig aktiviert ist. Dies kann bei Bedarf deaktiviert werden.

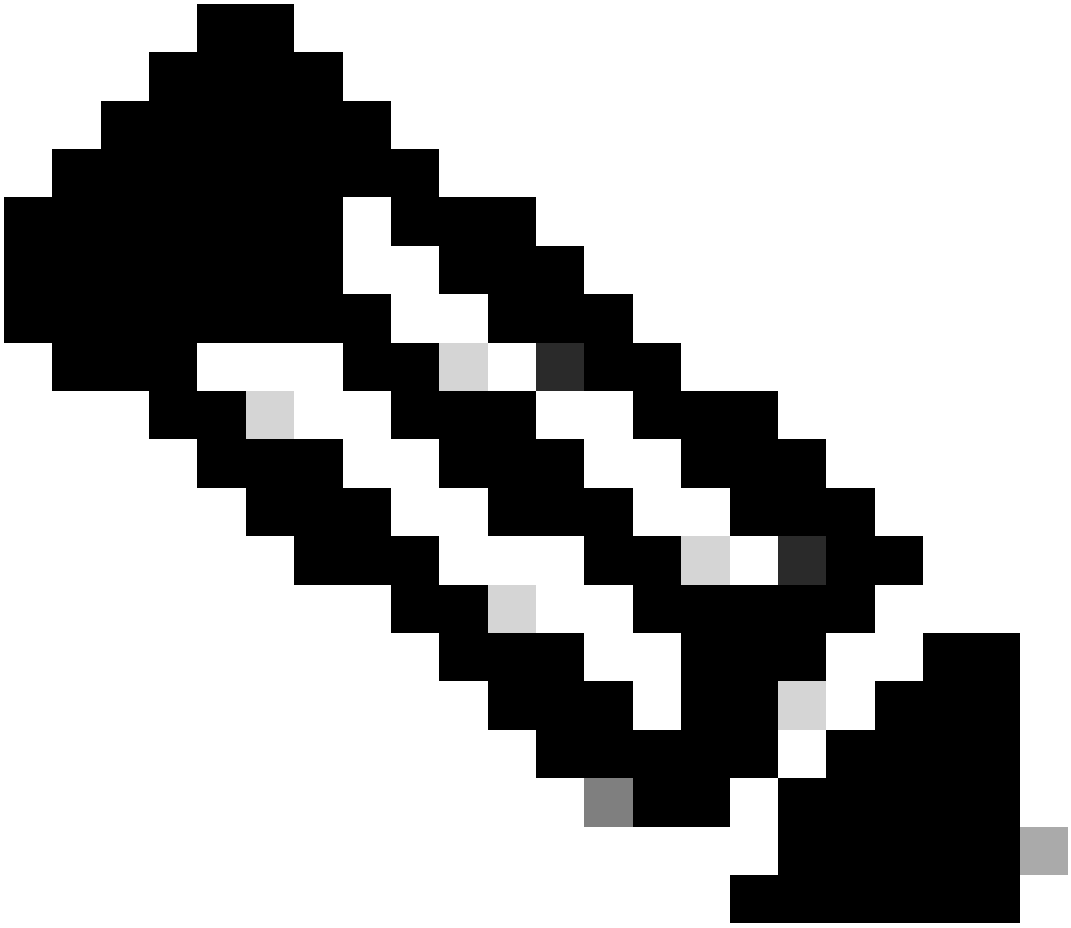
- Legacy-Konfiguration: Konfiguration > Vorlagen > Funktionsvorlagen > Cisco VPN (Service) > Service-Abschnitt:

1. Klicken Sie auf die Schaltfläche Neuer Service

2. Wählen Sie einen Servicetyp.

3. Geben Sie die Dienstadresse an (maximal 4 möglich, durch Komma getrennt).

4. Überprüfen Sie, ob der Regler Tracking (Verfolgung) standardmäßig aktiviert ist. Dies kann bei Bedarf deaktiviert werden.



Anmerkung: Sobald Schritt 3 konfiguriert ist (entweder aus der Konfigurationsgruppe oder der Legacy-Konfiguration), wird der Tracker automatisch für die verschiedenen definierten Dienstadressen initiiert.

Aus Sicht der CLI sieht die Konfiguration für Service Insertion 1.0 folgendermaßen aus:

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

Verifizierung

Die Schritte zur Verifizierung umfassen ähnliche Schritte, die im Rahmen der in den vorherigen

Abschnitten verwendeten schnittstellenbasierten Endpunkt-Tracker durchgeführt werden.

Es gibt zwei Verifizierungsoptionen für den explizit konfigurierten Endpunkt-Tracker.

- Auf SD-WAN-Manager: Überwachung > Geräte > {Gerätename auswählen} > Anwendungen > Tracker:

Überprüfen Sie den Tracker unter Individueller Tracker, und zeigen Sie die Statistiken des Trackers (Trackertypen, Status, Endpunkt, Endpunkttyp, VPN-Index, Hostname, Round-Trip Time) basierend auf Ihrem konfigurierten Tracker-Namen an.

- Auf SD-WAN-Manager: Überwachung > Geräte > {Gerätename auswählen} > Ereignisse:

Im Fall von Flaps, die auf dem Tracker erkannt werden, werden in diesem Abschnitt die entsprechenden Protokolle mit Details wie Hostname, Name des Anfügepunkts, Trackername, neuer Status, Adressfamilie und VPN-ID gefüllt.

Auf CLI des 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 Endpoint Trackers für DIA

NAT DIA Endpoint Trackers Tracker dienen primär dazu, die Erreichbarkeit von Anwendungen über eine NAT DIA-Schnittstelle auf SD-WAN Edge-Plattformen zu überwachen.

Für Anwendungsfälle von Direct Internet Access (DIA) werden NAT DIA-Tracker hauptsächlich verwendet, um die transportseitige Schnittstelle zu verfolgen und ein Failover auf eine andere verfügbare transportseitige Schnittstelle oder über SD-WAN-Overlay-Tunnel (mithilfe von Datenrichtlinien) auszulösen. Diese Funktion wurde ab Version 20.3/17.3 eingeführt, und die NAT-Fallback-Option ist ab Version 20.4/17.4 verfügbar. Wenn der Tracker feststellt, dass das lokale Internet über die NAT-DIA-Schnittstelle nicht verfügbar ist, zieht der Router die NAT-Route aus

dem Service-VPN zurück und leitet den Datenverkehr auf Basis der lokalen Routing-Konfiguration um. Der Tracker überprüft weiterhin regelmäßig den Status des Pfads zur Schnittstelle. Wenn er erkennt, dass der Pfad wieder funktioniert, installiert der Router die NAT-Route zum Internet neu. Weitere Informationen zu DIA-Trackern finden Sie in der Konfigurationsanleitung.

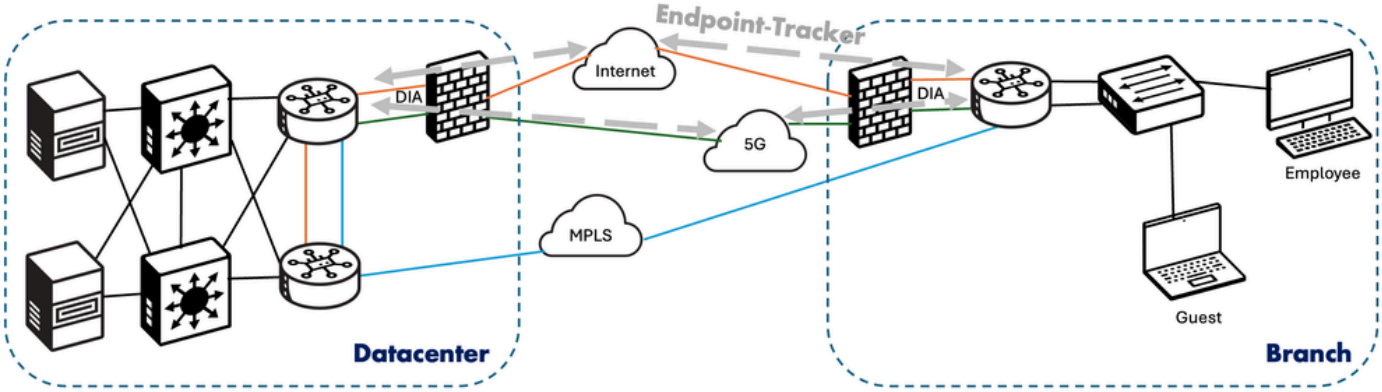
In der Tracker-Definition können Sie entweder eine IP-Adresse eines Endpunkts angeben, die über die NAT DIA-Schnittstelle erreichbar ist (konfiguriert als "endpoint-ip"), ODER einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) für den Endpunkt (konfiguriert als "endpoint-dns-name").

Der hier verwendete Sondentyp ist ein HTTP-Anforderungspaket, das einem HTTP-API-Anforderungs-PDU-Stack sehr ähnlich ist. Folgende Intervalle werden verwendet:

- Testintervall: 60 Sekunden
- Multiplikator: 180 Sekunden (da #retries 3 = 3 x 60 Sekunden ist)
- Paket-/Testtyp: HTTP

Anwendungsfälle

DIA wird häufig als Optimierung in Zweigstellen eingesetzt, um Backhaul von Zweigstellendatenverkehr in ein Rechenzentrum zu vermeiden, der in Richtung Internet geht. Wenn jedoch DIA in Zweigstellen verwendet wird, muss jede fehlende Erreichbarkeit entlang der NAT-DIA-Routen auf alternative Pfade zurückgreifen, um Blackholding und Dienstverluste zu vermeiden. Bei Standorten, die Fallback zum Rechenzentrum verwenden möchten (über SD-WAN-Overlay mit NAT-Fallback), falls ein lokales DIA-Breakout ausfällt. Nutzen Sie diese schnittstellenbasierten Endgeräte-Tracker an den DIA-fähigen Schnittstellen an den Außenstellen, um Fehler zu erkennen und ein Failover auf den Backup-/DC-Pfad zu initiieren. Auf diese Weise wird eine hohe Verfügbarkeit des Internetdiensts bei minimaler Unterbrechung des Geschäftsbetriebs erreicht und gleichzeitig der Internetverkehr durch DIA optimiert:



Konfiguration

Diese schnittstellenbasierten Endpunkt-Tracker müssen manuell konfiguriert werden, um dieses Feature-Set zu aktivieren. Hier sind die Möglichkeiten, es zu konfigurieren, je nach Art der von dem Benutzer bevorzugten Konfigurationsmethode.

- Konfigurationsgruppe: Konfiguration > Konfigurationsgruppen > Transport & Management

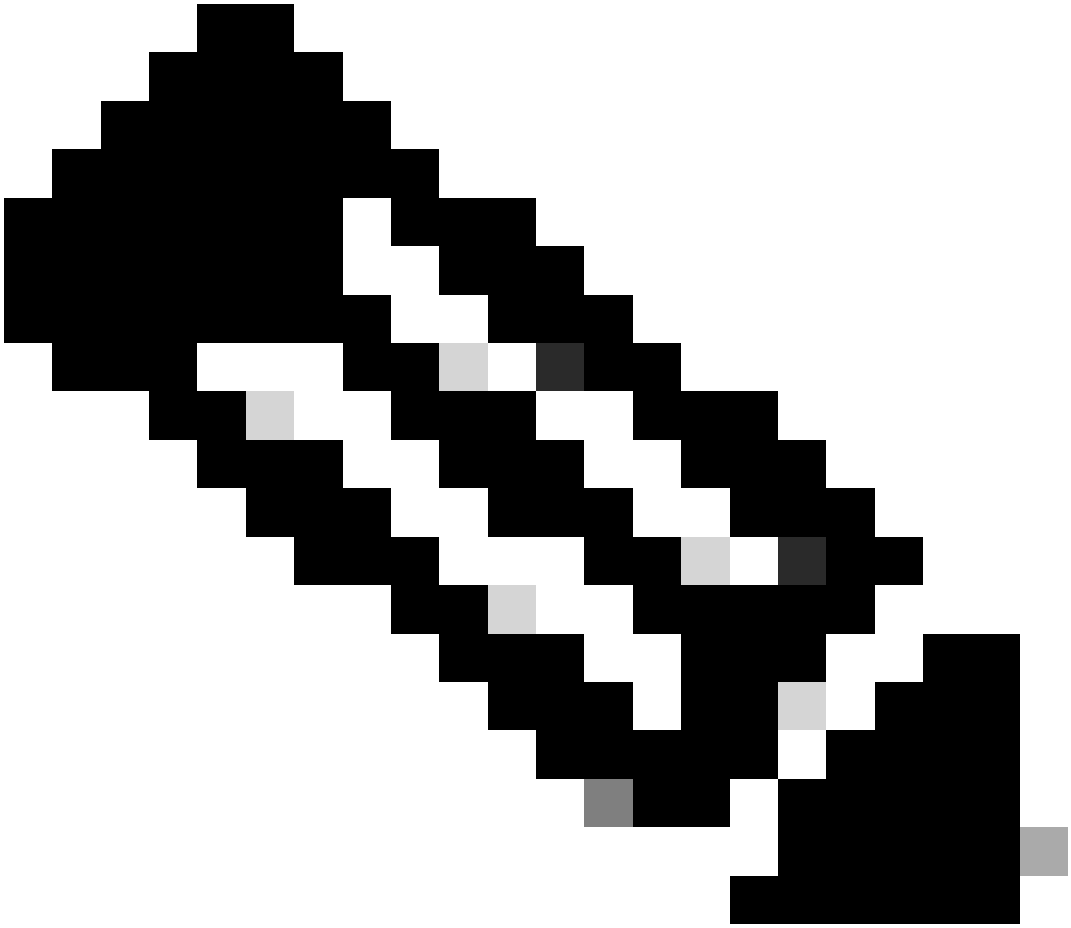
Profile > Ethernet Interface > Funktion hinzufügen > Tracker:

1. Definieren Sie einen Endpunkt-Trackernamen.

2. Wählen Sie einen Endpunkt-Tracker-Typ (zwischen HTTP-Standard und ICMP).

Hinweis: Der ICMP-Endpunkt-Tracker-Typ wurde seit der Version 20.13/17.13 eingeführt.

3. Wählen Sie den Endpunkt aus (zwischen Endpunkt-IP-Standard und Endpunkt-DNS-Name).



Anmerkung: Wenn Endpunkt-DNS-Name ausgewählt wird, stellen Sie sicher, dass unter Transport-VPN/VRF mithilfe des VPN-Konfigurationsprofils "Transport" ein gültiger DNS-Server oder Nameserver definiert ist.

---

4. Geben Sie die Adresse oder den DNS-Namen (FQDN) ein, an die die Tracker-Tests gesendet werden müssen (das Format hängt vom vorherigen Schritt ab).

5. (Optional) Sie können das Testintervall (Standard = 60 Sekunden) und die Anzahl der

Wiederholungen (Standard = 3 Mal) ändern, um die Fehlererkennungszeit zu verkürzen.

- Legacy-Konfiguration:

Schritt 1. Definition des schnittstellenbasierten Endpunkt-Trackers: Konfiguration > Vorlagen > Funktionsvorlagen > Systemvorlage > Tracker-Abschnitt:

1. Wählen Sie im Unterabschnitt "Trackers" die Schaltfläche New Endpoint Tracker.

2. Definieren Sie einen Endpunkt-Trackernamen.

3. Wählen Sie den Tracker-Typ (zwischen interface-default und static-route) als Schnittstelle, da DIA-Anwendungsfälle hier von Bedeutung sind.

4. Wählen Sie den Endgerätetyp (zwischen IP-Standardadresse und DNS-Name).

5. Geben Sie die IP-Adresse des Endpunkts oder den DNS-Namen des Endpunkts ein, an den die Tracker-Tests gesendet werden müssen (das Format hängt vom vorherigen Schritt ab).

6. (Optional) Sie können den Prüfschwellenwert (Standard = 300 ms), das Intervall (Standard = 60 Sekunden) und den Multiplikator (Standard = 3 Mal) ändern.

Schritt 2: Wenden Sie den schnittstellenbasierten Endpunkt-Tracker auf eine Schnittstelle im Transport-VPN an: Vorlagen > Funktionsvorlagen > Cisco VPN Interface Ethernet > Erweiterter Abschnitt:

1. Geben Sie den Namen des im vorhergehenden Schritt 1 definierten Endpunkt-Trackers in das Feld Tracker ein.

Aus Sicht der CLI sehen die Konfigurationen wie folgt aus:

```
(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
!
```

Verifizierung

Es gibt zwei Verifizierungsoptionen für explizit konfigurierte Endpunkt-Tracker.

- Auf SD-WAN-Manager: Überwachung > Geräte > {Gerätename auswählen} > Anwendungen > Tracker:

Überprüfen Sie den Tracker unter Individual Tracker, und zeigen Sie die Statistiken des Trackers (Tracker-Typen, Status, Endpunkt, Endgerätetyp, VPN-Index, Hostname, Round Trip Time) basierend auf dem von Ihnen konfigurierten Tracker-Namen an.

- Auf SD-WAN Manager: Überwachung > Geräte > {Gerätename auswählen} > Ereignisse:

Im Fall von Flaps, die auf dem Tracker erkannt werden, werden in diesem Abschnitt die entsprechenden Protokolle mit Details wie Hostname, Name des Anfügepunkts, Trackername, neuer Status, Adressfamilie und VPN-ID gefüllt.

Auf CLI des 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
```

Schnittstellen-Endpunkt-Trackers für SIG-Tunnel/SSE

Wenn Endgeräte-Tracker für SIG-Tunnel/SSE-Anwendungsfälle verwendet werden, weist dies in erster Linie darauf hin, dass das Unternehmen nach einem Cloud-basierten Security-Stack-Angebot sucht, das heutzutage mithilfe von Secure Internet Gateway (SIG)- oder Secure Service Edge (SSE)-Anbietern wie Cisco, Cloudflare, Netskope, ZScalar usw. leicht verfügbar gemacht werden kann. Sowohl SIG-Tunnel als auch SSE sind Teil des Bereitstellungsmodells für Cloud-Sicherheit, bei dem die Zweigstelle die Cloud nutzt, um die erforderlichen Sicherheitslösungen bereitzustellen. Der Anwendungsfall für SIG-Tunnel war das erste Angebot zur Integration von Cisco Catalyst SD-WAN mit solchen SIG-Anbietern (ab Version 20.4/17.4), jedoch mit der Weiterentwicklung von Cloud-basierten Sicherheitsangeboten. Der Anwendungsfall für SSE wurde eingeführt (ab Version 20.13/17.13), um Anwendungsfälle mit Anbietern wie Cisco (über Cisco Secure Access) und ZS abzudecken. Kalar.

IT-Abteilungen benötigen einen zuverlässigen und expliziten Ansatz zum Schutz vor und zur Verbindung mit Flexibilität. Mittlerweile ist es üblich, Mitarbeitern an Remote-Standorten direkten Zugriff auf Cloud-Anwendungen wie Microsoft 365 und Salesforce zur Verfügung zu stellen, und das mit zusätzlicher Sicherheit. Die Nachfrage nach Cloud-basierten Netzwerken und Sicherheitslösungen steigt täglich, da Auftragnehmer, Partner, IoT-Geräte usw. Netzwerkzugriff benötigen. Die Konvergenz von Netzwerk- und Sicherheitsfunktionen näher an den Endgeräten am Cloud-Edge wird als Servicemodell namens Cisco SASE bezeichnet. Cisco SASE kombiniert Cloud-basierte Netzwerk- und Sicherheitsfunktionen, um einen sicheren Zugriff auf Anwendungen für alle Benutzer oder Geräte zu ermöglichen - jederzeit und überall. Secure Service Edge (SSE) ist ein Netzwerksicherheitsansatz, mit dem Unternehmen den Sicherheitsstatus ihrer Arbeitsumgebung verbessern und gleichzeitig die Komplexität für Endbenutzer und IT-Abteilungen reduzieren können. Weitere Informationen zu SIG Tunnel/SSE-Trackern finden Sie im Konfigurationsleitfaden.

Anwendungsfälle

Solche schnittstellenbasierten Endpunkt-Tracker werden in solchen SIG Tunnel/SSE-Anwendungsfällen verwendet, bei denen Sie den Überblick über einen bekannten SaaS-Anwendungs-URL-Endpunkt oder einen bestimmten URL-Endpunkt behalten möchten. Heutzutage ist SSE das gebräuchlichere Szenario, seit die SASE-Architektur in SSE-Core- und SD-WAN-Funktionen aufgeteilt wurde. Anschließend können Sie zwischen aktiven und Standby-Rollen innerhalb der IPSec-Tunnel wählen, die von einem Standort (in diesem Fall dem Rechenzentrum) aus erstellt werden. Der Benutzer hat die Wahl, den Tracker unter der jeweiligen Tunnelschnittstelle anzubringen.

Im Fall von SSE-Anbietern, wie Cisco Secure Access (von Cisco), wird ein impliziter Endpunkt-Tracker verwendet, der standardmäßig konfiguriert wird. Der Benutzer hat jedoch die Wahl, einen benutzerdefinierten Endpunkt-Tracker zu erstellen und diesen an die IPSec-Tunnelschnittstelle anzufügen. Die in SSE verwendeten Parameter des standardmäßigen/impliziten Endpunkt-Trackers sind:

Für Cisco SSE:

Nachverfolgungsname: DefaultTracker

Nachverfolgter Endpunkt: http://service.sig.umbrella.com

Endgerätetyp: API_URL

Schwellenwert: 300 ms

Multiplizieren: 3

Intervall: 60 s

Für ZScaler SSE:

Nachverfolgungsname: DefaultTracker

Nachverfolgter Endpunkt: http://gateway.zscalerthree.net/vpnte

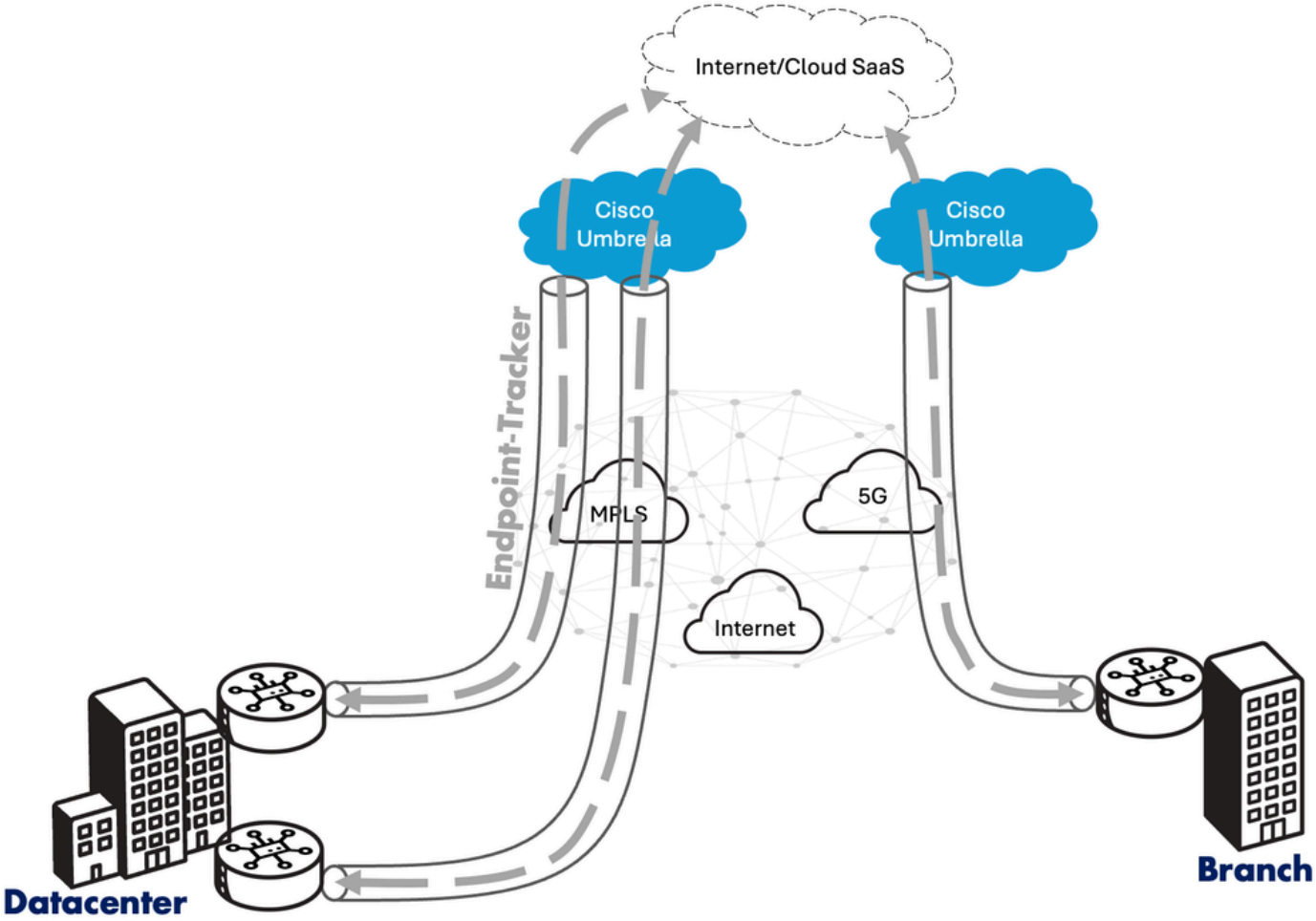
Endgerätetyp: API_URL

Schwellenwert: 300 ms

Multiplikator: 3

Intervall: 60 s

Im Fall von SIG-Tunneln ist kein standardmäßiger/impliziter Endpunkt-Tracker definiert. Daher muss der Benutzer manuell einen schnittstellenbasierten Endpunkt-Tracker konfigurieren, wenn er die IPSec-Tunnelschnittstelle zur SIG-Provider-Cloud verfolgen möchte:



Konfiguration

Bei SSE-Anbietern muss der Benutzer keinen Endpunkt-Tracker explizit definieren (sofern nicht gewünscht). Die Workflows unterscheiden sich jedoch je nach Konfigurationstyp.

Als Voraussetzung müssen Sie die SIG/SSE-Anmeldeinformationen Administration > Settings > External Services > Cloud Credentials definieren:

1. Aktivieren Sie unter Cloud Provider Credentials (Anmeldeinformationen für Cloud-Anbieter) die Option Umbrella oder Cisco SSE (oder beide).

2. Definieren Sie die Parameter wie Organisations-ID, API-Schlüssel, Geheim).

Konfigurationsgruppenkonfiguration festlegen > Richtliniengruppen > Sicheres Internet-Gateway/Sicherer Service-Edge:

1. Klicken Sie auf Add Secure Internet Gateway oder Add Secure Service Edge.

2. Definieren Sie einen Namen und eine Beschreibung.

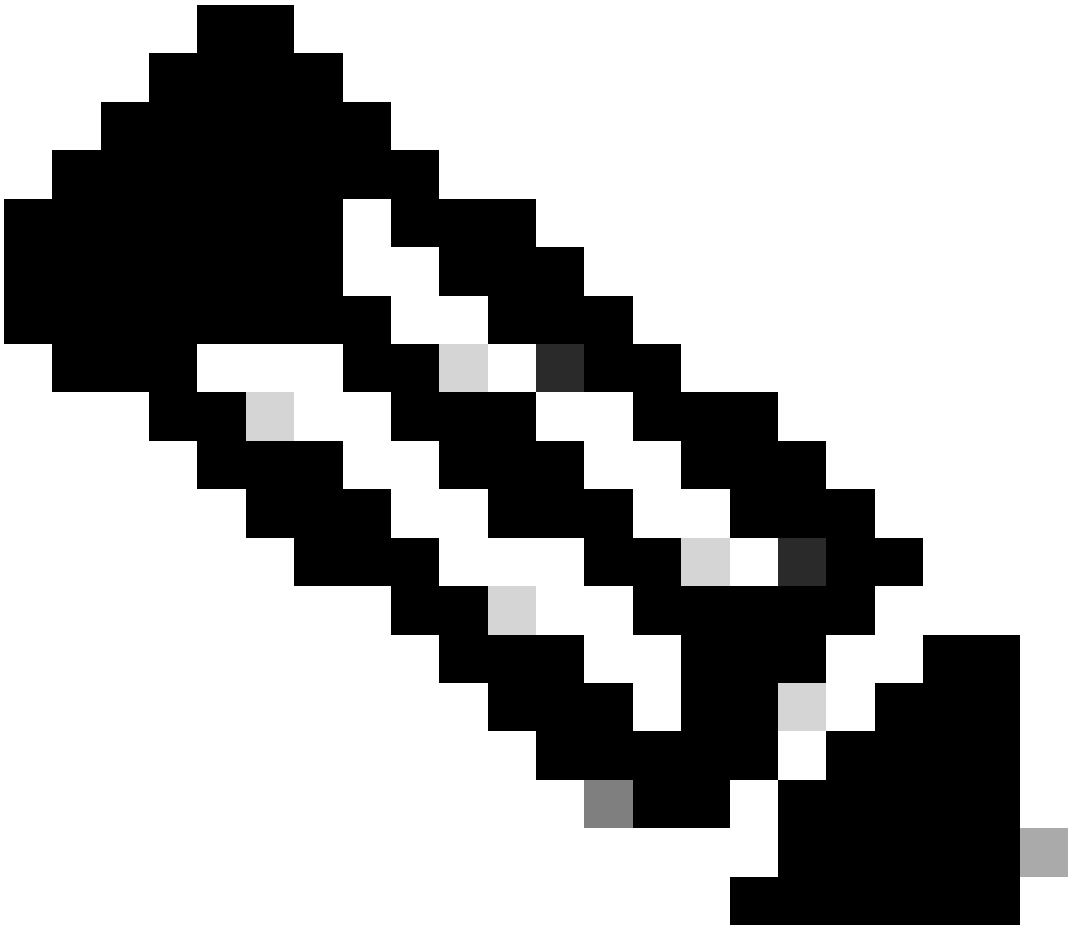
3. Wählen Sie eine der Optionsschaltflächen unter SIG/SSE Provider (entweder Umbrella oder Cisco SSE).

4. Legen Sie im Abschnitt Tracker die Quell-IP-Adresse fest, die für die Quell-Probes verwendet

wird.

5. Wenn Sie einen expliziten/benutzerdefinierten Endpunkt-Tracker definieren möchten, klicken Sie auf Tracker hinzufügen, und geben Sie dann die Parameter für den Endpunkt-Tracker ein (Name, API-URL des Endpunkts, Schwellenwert, Testintervall und Multiplikator).

6. Erstellen Sie im Abschnitt "Konfiguration" die Tunnelschnittstellen, in denen Sie die Parameter definieren können (z. B. Schnittstellenname, Beschreibung, Tracker, Tunnelquellenschnittstelle, Primär-/Sekundäres Rechenzentrum).



> Anmerkung: In Schritt 6 erhält der Benutzer die Möglichkeit, den definierten Endpunkt-Tracker an den entsprechenden IPSec-Tunnel anzufügen. Beachten Sie, dass es sich um ein optionales Feld handelt.

---

7. Erstellen Sie im Abschnitt Hochverfügbarkeit ein Schnittstellenpaar und definieren Sie Ihre aktive Schnittstelle und Ihre Backup-Schnittstelle zusammen mit ihren jeweiligen Gewichtungen. Wenden Sie dann die zuvor konfigurierte Richtliniengruppe auf die relevanten Edges an.

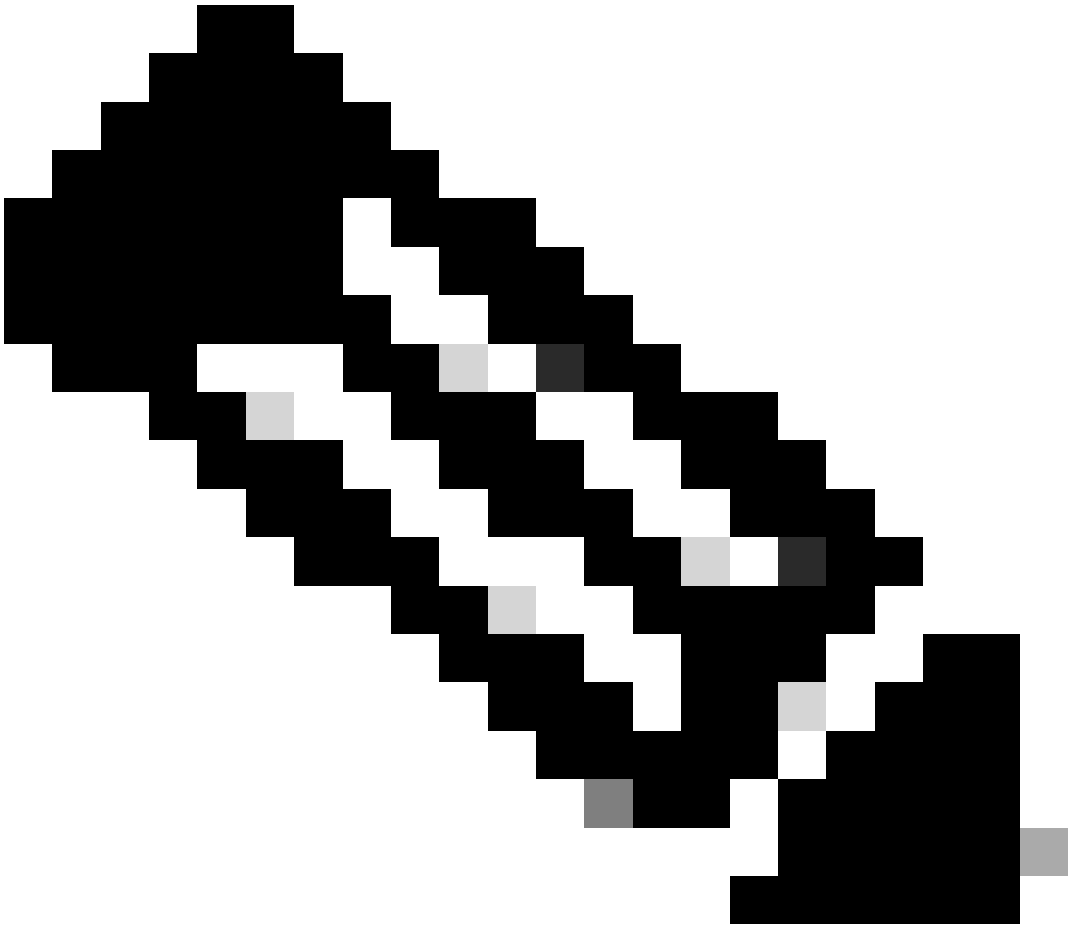
Legacy-Konfiguration festlegen Konfiguration > Vorlagen > Funktionsvorlagen > Cisco Secure Internet Gateway-Funktionsvorlage:

1. Wählen Sie eine der Optionsschaltflächen unter SIG Provider (entweder Umbrella, ZScalar oder Generic).

2. Definieren Sie im Abschnitt Tracker (BETA) die Quell-IP-Adresse, die für die Quell-Probes verwendet wird.

5. Wenn Sie einen expliziten/benutzerdefinierten Endpunkt-Tracker definieren, klicken Sie auf Neuer Tracker und geben Sie die Parameter für den Endpunkt-Tracker ein (Name, API-URL des Endpunkts, Schwellenwert, Intervall und Multiplikator).

6. Erstellen Sie im Abschnitt "Konfiguration" die Tunnelschnittstellen (durch Klicken auf "Tunnel hinzufügen"), in denen Sie die Parameter definieren können (z. B. Schnittstellenname, Beschreibung, Tracker, Tunnelquellenschnittstelle, Primär-/Sekundäres Rechenzentrum).



Anmerkung: In Schritt 6 erhält der Benutzer die Möglichkeit, den definierten Endpunkt-

---

Tracker an den jeweiligen IPSec-Tunnel anzufügen. Beachten Sie, dass es sich um ein optionales Feld handelt.

7. Definieren Sie im Abschnitt Hochverfügbarkeit Ihre aktive Schnittstelle und Ihre Backup-Schnittstelle zusammen mit ihren jeweiligen Gewichtungen.

Aus Sicht der CLI sehen die Konfigurationen wie folgt aus:

```
(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
!
```

Verifizierung

Es gibt Überprüfungsoptionen für explizit konfigurierte Endpunkt-Tracker.

- Auf SD-WAN-Manager: Überwachung > Geräte > {Gerätename auswählen} > Anwendungen > Tracker:

Überprüfen Sie den Tracker unter Individueller Tracker, und zeigen Sie die Statistiken des Trackers (Trackertypen, Status, Endpunkt, Endpunkttyp, VPN-Index, Hostname, Round-Trip Time) basierend auf Ihrem konfigurierten Tracker-Namen an.

- Auf SD-WAN-Manager: Überwachung > Geräte > {Gerätename auswählen} > Ereignisse:

Im Fall von Flaps, die auf dem Tracker erkannt werden, werden in diesem Abschnitt die entsprechenden Protokolle mit Details wie Hostname, Name des Anfügepunkts, Trackername, neuer Status, Adressfamilie und VPN-ID gefüllt.

Auf CLI des 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
```

Für Service Fabric 2.0 verwendete Schnittstellen-Endpunkt-Trackers

Service Fabric 2.0 Tracking, das in der Version 20.13/17.13 eingeführt wurde, ist eine erweiterte Variante der Nachverfolgung für Service Insertion 1.0, bei der Benutzer die Möglichkeit haben, die Nachverfolger in größerem Umfang anzupassen. Das Standardverhalten wird von der vorherigen Version von Service Insertion (1.0) beibehalten. Ein Tracker wird standardmäßig mit der Definition jeder Service-Adresse (oder Weiterleitungsadresse) in einem Service-HA-Paar pro rx/tx initiiert. Mit Service Insertion 2.0 kann jedoch die Nachverfolgungsadresse (IP/Endpunkt zum nachverfolgten Gerät) von der Weiterleitungsadresse (in der Regel die Dienstadresse) getrennt werden. Dies erfolgt über benutzerdefinierte Endpunkt-Tracker, die auf VPN-Ebene definiert sind. Weitere Informationen zu Service Fabric 2.0-Trackern finden Sie im Konfigurationsleitfaden.

Wenn der Benutzer den Standard-Tracker verwendet, gelten folgende Spezifikationen:

- Hello: 1 Tastkopf alle 30 Sekunden
- Multiplikator: 3 Mal
- Paket-/Testtyp: ICMP-Echo/Echo-Antwort

Wenn der Benutzer einen benutzerdefinierten Tracker verwendet, gelten folgende Spezifikationen:

- Hello: 1 Probe alle 60 Sekunden
- Multiplikator: 3 Mal
- Paket-/Testtyp: ICMP-Echoanfrage/Antwort

Anwendungsfälle

Auch hier gelten die in den vorhergehenden Abschnitten erwähnten Anwendungsfälle von Service Insertion 1.0.

Konfiguration

Es besteht Unterstützung für eine Workflow-basierte Konfiguration für Service Insertion 2.0. Hierbei handelt es sich um einen assistentengestützten Ansatz, der die Benutzererfahrung vereinfacht und gleichzeitig die standardmäßigen Workflow-Schritte der Konfigurationsgruppe einhält.

1. Definieren Sie die Gruppe "Service-Kette - Konfiguration" im Abschnitt "Konfiguration > Serviceeinfügung > Serviceverkettungsdefinitionen":

antwort: Klicken Sie auf die Schaltfläche Add Service Chain Definition (Servicekettendefinition hinzufügen).

b. Geben Sie die Details des Namens und der Beschreibung des Service an.

c. Füllen Sie ein Listenformat (durch Auswahl aus dem Dropdown-Menü) und den Servicetyp aus.

2. Definieren Sie die Gruppe "Serviceketteninstanz - Konfiguration" im Abschnitt Konfiguration > Serviceeinfügung > Servicekettenkonfigurationen:

antwort: Klicken Sie auf Servicekettenkonfiguration hinzufügen.

b. Wählen Sie im Schritt "Service Chain Definition" das Optionsfeld Select Existing (Bestehenden auswählen) und anschließend den zuvor definierten Service aus.

c. Geben Sie einen Namen und eine Beschreibung für den Schritt zum Starten der Servicekette an.

d. Wählen Sie im Schritt Service Chain Configuration for Manually Connected Services (Servicekettenkonfiguration für manuell verbundene Services) die Service Chain VPN-ID aus.

e. Geben Sie dann für jeden definierten Service in der Serviceketteninstanz (dargestellt in Unterregisterkarten) unter "Servicedetails" den Typ des Anhangs (IPv4, IPv6 oder Tunnel Connected) an.

f. Aktivieren Sie das Kontrollkästchen Erweitert. Wenn Sie Anwendungsfälle für Active-Backup/HA benötigen (aktivieren Sie auch den Knopf Parameter für Backup hinzufügen) oder auch wenn Sie einen benutzerdefinierten Endpunkt-Tracker definieren müssen (aktivieren Sie auch den Knopf Benutzerdefinierter Tracker).

g. Wenn Sie Szenarien haben, bei denen der ausgehende (tx) Datenverkehr über eine Schnittstelle an den Dienst geht und der zurückkehrende Datenverkehr vom Dienst über eine andere Schnittstelle aufgenommen wird (rx), aktivieren Sie den Datenverkehr vom Dienst, der über einen anderen Schnittstellenknopf empfangen wird.

h. Definieren Sie mit den Reglern Advanced und Custom Tracker die IPv4-Adresse (Weiterleitungsadresse), die SD-WAN-Router-Schnittstelle (mit der der Dienst verbunden ist) und den Tracker-Endpunkt (Nachverfolgungsadresse). Sie können auch die benutzerdefinierten Tracker-Parameter wie Intervall und Multiplikator ändern (indem Sie auf die Schaltfläche Bearbeiten klicken).

i. Wiederholen Sie die Schritte e), f), g) und h) für jeden nachfolgend definierten Dienst.

3. Hängen Sie die Serviceketteninstanz dem Konfigurationsprofil der Gruppe Edge - Konfiguration unter Konfiguration > Konfigurationsgruppen > Serviceprofil > Service-VPN > Funktion hinzufügen > Servicekettenanlagen-Gateway an:

antwort: Geben Sie einen Namen und eine Beschreibung für dieses Service Chain Attachment Gateway-Paket ein.

b. Wählen Sie die zuvor definierte Servicekettendefinition (in Schritt 1) aus.

c. Fügen Sie die Details wie in Schritt 2 ausgeführt erneut hinzu bzw. überprüfen Sie sie. Für die Tracker-Definition besteht der einzige Unterschied zum vorherigen Schritt 2 darin, dass Sie die Möglichkeit erhalten, einen Tracker-Namen zu vergeben und auch den Tracker-Typ auszuwählen (von service-icmp bis ipv6-service-icmp).

Aus Sicht der CLI sehen die Konfigurationen wie folgt aus:

```
!
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
!
```

Verifizierung

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

Überprüfen Sie den Tracker unter Individueller Tracker, und zeigen Sie die Statistiken des Trackers (Trackertypen, Status, Endpunkt, Endpunkttyp, VPN-Index, Hostname, Round-Trip Time) basierend auf Ihrem konfigurierten Tracker-Namen an.

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

Im Fall von Flaps, die auf dem Tracker erkannt werden, werden in diesem Abschnitt die entsprechenden Protokolle mit Details wie Hostname, Name des Anfügepunkts, Trackername, neuer Status, Adressfamilie und VPN-ID gefüllt.

Auf CLI des 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
```

Endpunktverfolgungsgeräte für statische Routen und statische Routen (serviceseitig)

Der zweite Typ von Endpunkt-Trackern wird als statisch-route-basierte Endpunkt-Tracker bezeichnet. Wie der Name bereits andeutet, werden diese Tracker in erster Linie verwendet, um die Next-Hop-Adresse einer statischen Route zu verfolgen, die im serviceseitigen VPN definiert ist. Standardmäßig werden alle "verbundenen" und "statischen" Routentypen in OMP-Protokoll angekündigt - post, das alle entfernten Standorte, die den jeweiligen Dienst VPN erkennen, dass Ziel-Präfix (wobei der Next-Hop-Punkt auf die TLOC des Ursprungs-Standort). Der Ursprungsstandort ist der Standort, von dem aus die spezifische statische Route initiiert wurde.

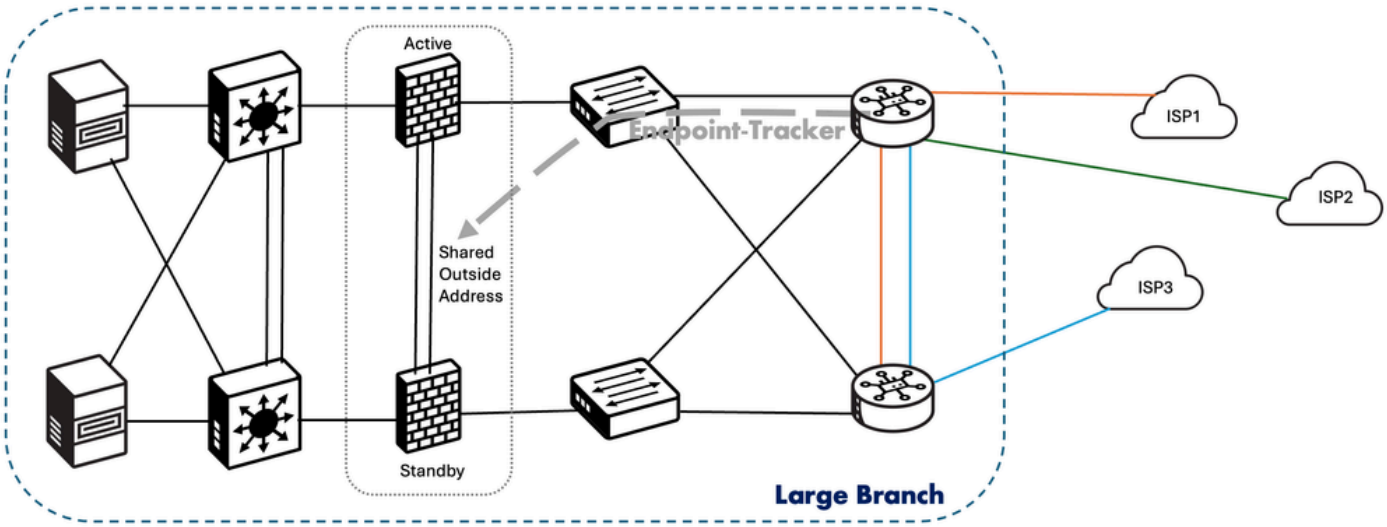
Falls jedoch die Next-Hop-Adresse in der statischen Route nicht erreichbar ist, wird die Route nicht in OMP angekündigt. Dies würde dazu führen, dass Datenverkehr für Datenflüsse, die an den Ursprungsstandort gerichtet sind, blockiert wird. Dies führt dazu, dass ein Tracker an die statische Route angehängt werden muss, um sicherzustellen, dass die statische Route NUR dann in OMP angekündigt wird, wenn die Next-Hop-Adresse erreichbar ist. Diese Funktion wurde in Version 20.3/17.3 für Basis-IP-Adresstyp-Endgeräte-Tracker auf Basis statischer Routen eingeführt. Ab der Version 20.7/17.7 wird das Senden von Tracker-Tests nur an bestimmte TCP- oder UDP-Ports der Next-Hop-IP-Adresse unterstützt (in Fällen, in denen Firewalls nur zum Öffnen bestimmter Ports zu Verfolgungszwecken verwendet werden). Weitere Informationen zu statischen Route-Trackern finden Sie im Konfigurationsleitfaden.

Die hier verwendeten Sonden sind einfache ICMP-Echoanforderungspakete. Folgende Intervalle werden verwendet:

- Hello: 60 Sekunden
- Haltefrist: 180 Sekunden (da #retries 3 = 3 x 60 Sekunden ist)
- Paket-/Testtyp: ICMP-Echo/Echo-Antwort

Anwendungsfälle

Diese Art von Endpunkt-Trackern auf der Basis statischer Routen wird für die serviceseitige Nachverfolgung von Next-Hop-Adressen in statischen Routen verwendet. Ein solches allgemeines Szenario wäre die Nachverfolgung der LAN-seitigen Next-Hop-Adresse, die einem Paar von aktiven/Standby-Firewalls entspricht, die die gemeinsame externe IP-Adresse verwenden, wobei die externe Schnittstelle die Rolle der "aktiven" Firewall übernimmt. In Fällen, in denen Firewall-Regeln stark eingeschränkt zu sein scheinen und nur bestimmte Ports zu Anwendungsfallzwecken geöffnet werden, kann der statische Routen-Tracker verwendet werden, um den spezifischen TCP/UDP-Port zur Next-Hop-IP-Adresse zu verfolgen, die zu der LAN-seitigen externen Firewall-Schnittstelle gehört.



Konfiguration

Diese Endpunkt-Tracker auf Basis statischer Routen müssen manuell konfiguriert werden, um dieses Feature-Set zu aktivieren. Hier sind die Möglichkeiten, es zu konfigurieren, je nach Art der von dem Benutzer bevorzugten Konfigurationsmethode.

- Konfigurationsgruppe Konfiguration > Konfigurationsgruppen > Serviceprofil > Service-VPN > Funktion hinzufügen > Tracker:

1. Geben Sie einen Namen, eine Beschreibung und einen Nachverfolgungsnamen für den neuen (Endpunkt-) Nachverfolger an, der definiert wird.

2. Wählen Sie den Endgerätetyp aus, je nachdem, ob Sie nur die Next-Hop-IP-Adresse (Optionsfeld Adresse auswählen) oder sogar bestimmte TCP/UDP-Ports (Optionsfeld Protokoll auswählen) verfolgen müssen.

3. Geben Sie die Adresse im IP-Adressformat ein. Geben Sie auch das Protokoll (TCP oder UDP) und die Portnummer ein, falls Sie im vorherigen Schritt Protokoll als Endgerätetyp ausgewählt haben.

4. Sie können die Standardwerte für das Testintervall, die Anzahl der Wiederholungen und das Latenzlimit ändern, falls erforderlich.

- Konfiguration > Konfigurationsgruppen > Serviceprofil > Service-VPN > Routenabschnitt:

1. Wählen Sie die Schaltfläche Statische IPv4/IPv6-Route hinzufügen.

2. Geben Sie Details wie Netzwerkadresse, Subnetzmaske, Next-Hop, Adresse, AD ein.

3. Klicken Sie auf Add Next Hop With Tracker Schaltfläche.

4. Geben Sie die Next-Hop-Adresse erneut ein, und wählen Sie aus dem Dropdown-Menü den zuvor erstellten (Endpunkt-) Tracker-Namen aus.

- Legacy-Konfiguration > Vorlagen > Funktionsvorlagen > Systemvorlage > Abschnitt Tracker:

1. Klicken Sie auf die Schaltfläche Neue Endpunktverfolgung.

2. Geben Sie einen Namen für den neu zu definierenden (Endpunkt-)Tracker an.

3. Ändern Sie das Optionsfeld Tracker-Typ in Static-route.

4. Wählen Sie den Endgerätetyp als Next-Hop-IP-Adresse (wählen Sie das Optionsfeld IP-Adresse).

5. Geben Sie die Endpunkt-IP im IP-Adressformat ein.

6. Sie können die Standardwerte für das Testintervall, die Anzahl der Wiederholungen und das Latenzlimit ändern, falls erforderlich.

- Konfiguration > Vorlagen > Funktionsvorlagen > Cisco VPN (NUR serviceseitig) > IPv4/IPv6-Routenabschnitt:

1. Wählen Sie die Schaltfläche Neue IPv4/IPv6-Route.

2. Geben Sie Details ein, z. B. Präfix, Gateway.

3. Klicken Sie auf die Schaltfläche Add Next Hop With Tracker.

4. Geben Sie die Next-Hop-Adresse, AD (Distanz) und manuell den zuvor erstellten Tracker-Namen (Endpunkt) ein.

Aus Sicht der CLI sehen die Konfigurationen wie folgt aus:

```
(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
!
```

Verifizierung

Es gibt zwei Verifizierungsbereiche für explizit konfigurierte Endpunkt-Tracker.

- Auf dem SD-WAN Manager-Monitor > Geräte > {Gerätename auswählen} > Echtzeit:

1. Geben Sie unter Device Options (Geräteoptionen) "Endpoint Tracker Info" ein.

2. Aktivieren Sie das Kontrollkästchen unter Individueller Tracker (Name des Anfügepunkts), und zeigen Sie die Statistiken des Trackers (Tracker-Status, Name des zugeordneten Tracker-Datensatzes, Latenz in MX vom Gerät bis zum Endpunkt, Zeitstempel der letzten Aktualisierung) basierend auf Ihrem konfigurierten Tracker-Namen an.

- Auf dem SD-WAN-Manager-Monitor > Geräte > {Gerätename auswählen} > Ereignisse:

Im Fall von Flaps, die auf dem Tracker erkannt werden, werden in diesem Abschnitt die entsprechenden Protokolle mit Details wie Hostname, Name des Anfügepunkts, Trackername, neuer Status, Adressfamilie und VPN-ID gefüllt.

Auf CLI des 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]
```

Für die VRRP-Nachverfolgung verwendete Schnittstellen-Objektverfolgung

Object Trackers sind Tracker, die für die Nutzung im autonomen Modus (Anwendungsfälle) entwickelt wurden. Diese Tracker bieten Anwendungsfälle, die von VRRP-basierter Schnittstelle/Tunnel-Nachverfolgung bis hin zu Service-VPN NAT-Nachverfolgung reichen.

Bei VRRP-Tracking-Anwendungsfällen wird der VRRP-Status auf Basis des Tunnelverbindungsstatus bestimmt. Wenn der Tunnel oder die Schnittstelle am primären VRRP ausgefallen ist, wird der Datenverkehr zum sekundären VRRP geleitet. Der sekundäre VRRP-Router im LAN-Segment wird zum primären VRRP, um das Gateway für den serviceseitigen Datenverkehr bereitzustellen. Dieser Anwendungsfall gilt nur für das Service-VPN und hilft bei einem Failover der VRRP-Rolle auf der LAN-Seite im Fall eines Ausfalls auf dem SD-WAN-Overlay (Schnittstelle oder Tunnel im Fall von SSE). Zum Anhängen von Trackern an VRRP-Gruppen können NUR Objekt-Tracker (keine Endpunkt-Tracker) verwendet werden. Diese Funktion wurde in der Version 20.7/17.7 für Cisco Catalyst SD-WAN-Edges eingeführt.

Es werden hier keine Sonden vom Tracker verwendet. Stattdessen wird der Status des Leitungsprotokolls verwendet, um den Tracker-Status zu bestimmen (aktiv/inaktiv). Es gibt keine Reaktionsintervalle bei Line-Protocol-basierten Trackern für Schnittstellen - sobald das Line-Protocol für Tunnel ausfällt, wird auch der Track-Status auf den DOWN-Status zurückgesetzt. Abhängig von der Aktion "Herunterfahren" oder "Dekrementieren" würde die VRRP-Gruppe dementsprechend neu konvergiert. Weitere Informationen zu VRRP Interface Trackern finden Sie im Konfigurationsleitfaden.

Anwendungsfälle

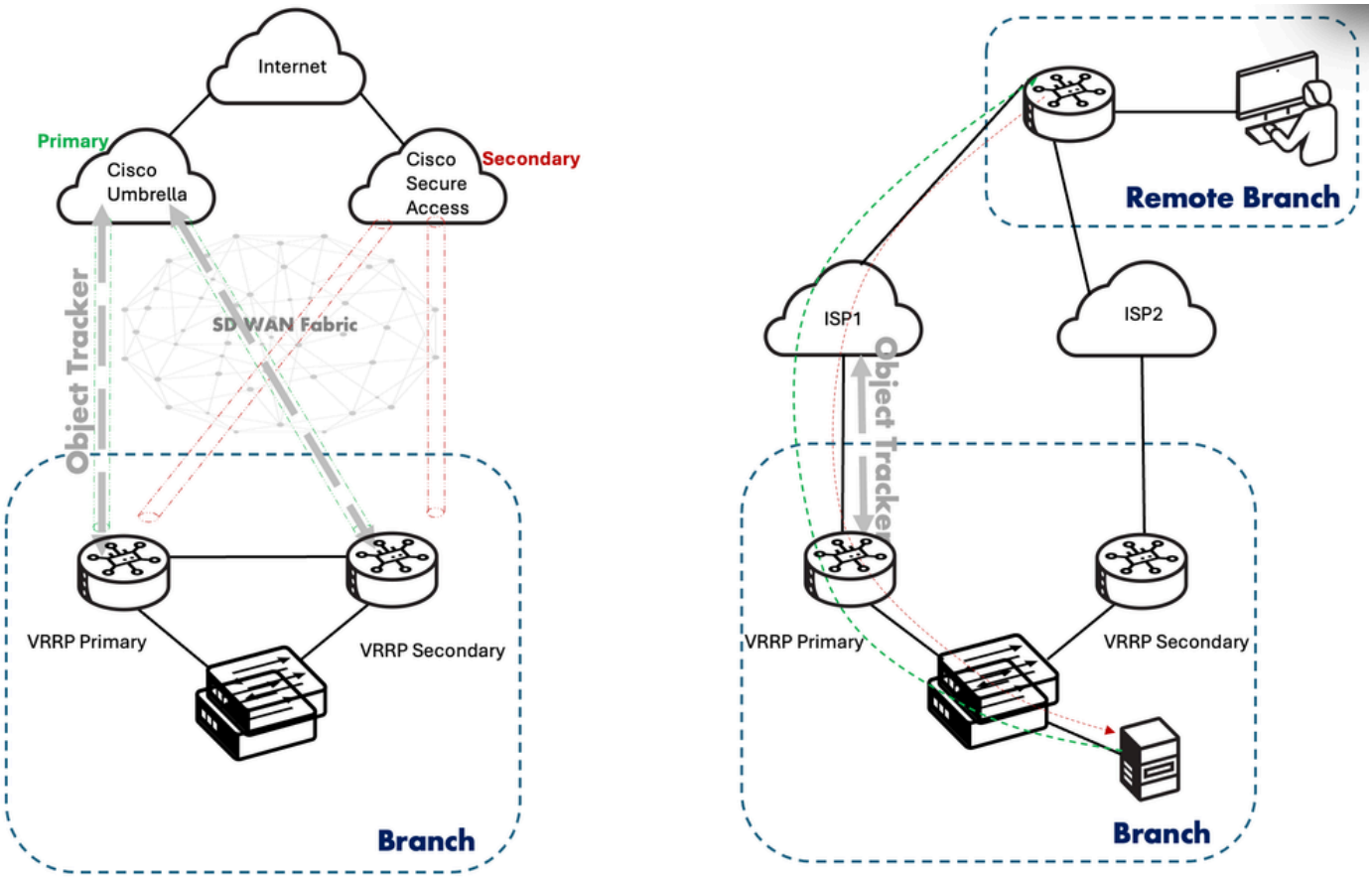
Je nach den Kriterien für die Implementierung der VRRP-basierten Schnittstellenverfolgung gibt es mehrere Anwendungsfälle. Derzeit werden die beiden Modi unterstützt: (i) Schnittstelle (d. h. jede Tunnelschnittstelle, die an ein lokales TLOC gebunden ist) oder (ii) SIG-Schnittstelle (in Bezug auf SIG-Tunnelschnittstellen). In jedem Fall handelt es sich bei dem verfolgten Teil um ein Schnittstellenleitungsprotokoll.

Dual-Router mit Internet: Das Track-Objekt ist an die VRRP-Gruppe gebunden. Wenn das Objekt des Trackers (in diesem Fall die SIG-Tunnelschnittstelle) ausfällt, wird der primäre VRRP-Router

benachrichtigt, dass der Statusübergang von Primär zu Backup und der Backup-Router Primär erfolgt. Diese Zustandsänderung kann durch zwei Arten von Operationen beeinflusst oder ausgelöst werden:

1. Dekret: Hierbei wird die VRRP-Priorität für die Schnittstelle, auf der VRRP VIP konfiguriert ist, um einen bestimmten Wert reduziert oder dekrementiert, falls der Track-Objekt-Zustand von UP nach DOWN wechselt.
2. Herunterfahren: Bei dieser Methode wird der VRRP-Prozess auf der angewendeten Schnittstelle beendet, wenn der Status des Verfolgungsobjekts von UP nach DOWN wechselt. Diese Methode wird nicht für Anwendungsfälle empfohlen, bei denen eine asymmetrische Weiterleitung vorliegt.

TLOC Change Preference (TLOC-Änderungspräferenz): Um zu verhindern, dass asymmetrischer Datenverkehr von anderen SDWAN-Standorten an den Standort gelangt, an dem VRRP auf Service-VPN ausgeführt wird, wird die TLOC-Präferenz des primären VRRP-Routers (falls konfiguriert) um 1 erhöht. Sie können diesen Wert sogar unter Konfigurationsgruppen ändern. Auf diese Weise wird sichergestellt, dass der Datenverkehr vom WAN zum LAN vom primären VRRP-Router angezogen wird. Der Datenverkehr vom LAN zum WAN wird vom VRRP-Mechanismus des primären VRRP angezogen. Diese Funktion ist unabhängig vom VRRP Interface Tracker. Aus CLI-Sicht ist dies ein optionaler Befehl (tloc-change-pref).



Konfiguration

Die Konfiguration von Object Trackern erfolgt über Systemvorlagen in der Legacy-Konfiguration. Anschließend wird der Object Tracker der entsprechenden VRRP-Gruppe unter der Feature-

Vorlage für die Service-VPN-Ethernet-Schnittstelle hinzugefügt. In der Konfigurationsgruppe wurde dieser Mechanismus vereinfacht, indem direkt eine Option zum Hinzufügen des Objektverfolgungsgeräts zum entsprechenden Serviceprofil-Ethernet-Schnittstellenprofil abgerufen wurde. Nachfolgend sind die Möglichkeiten zur Konfiguration aufgeführt, je nach vom Benutzer bevorzugter Konfigurationsmethode.

- Konfigurationsgruppe Konfiguration > Konfigurationsgruppen > Serviceprofil > Ethernet-Schnittstelle > Funktion hinzufügen > Object Tracker:

1. Geben Sie einen Namen und eine Beschreibung für den neu zu definierenden Objekt-Tracker an.
2. Wählen Sie den Tracker-Typ aus (zwischen Schnittstelle und SIG).
3. Weisen Sie eine Objektverfolgungskennung zu.
4. Geben Sie den Schnittstellennamen an (abhängig von der in Schritt 2 gewählten Option).

- Konfiguration > Konfigurationsgruppen > Serviceprofil > Ethernet-Schnittstelle > VRRP-Abschnitt:

1. Klicken Sie unter IPv4-Einstellungen auf VRRP IPv4 hinzufügen.
2. Definieren Sie eine VRRP-Gruppen-ID, und stellen Sie eine lokale Priorität für diese serviceseitige Ethernet-Schnittstelle bereit.
3. Geben Sie die VRRP Virtual IP (VIP)-Adresse an.
4. Aktivieren Sie den Regler TLOC Preference Change (TLOC-Voreinstellungsänderung), und stellen Sie auch den TLOC Preference Change Value (zur Verarbeitung von asymmetrischem Routing) bereit.
5. Klicken Sie auf VRRP-Nachverfolgungsobjekt hinzufügen.
6. Wählen Sie unter Objektverfolgung zuordnen aus dem Dropdown-Menü des Objektverfolgungssystems (basierend auf Name), das Sie zuvor erstellt haben
7. Wählen Sie eine Tracker-Aktion aus (entweder Herunterfahren oder Absetzen).
8. Geben Sie den Abgangswert ein (abhängig von der in Schritt 7 gewählten Option).

- Legacy-Konfiguration > Vorlagen > Funktionsvorlagen > System > Tracker-Abschnitt:

1. Klicken Sie auf die Schaltfläche New Object Tracker.
2. Wählen Sie den Tracker-Typ aus (zwischen Schnittstelle und SIG).
3. Weisen Sie eine Objekt-ID zu.
4. Geben Sie den Schnittstellennamen an (abhängig von der in Schritt 2 gewählten Option).

- Konfiguration > Vorlagen > Ethernet-Schnittstelle (die zur Serviceseite gehört) > VRRP-Abschnitt:

1. Klicken Sie auf die Schaltfläche New VRRP.
2. Definieren Sie eine VRRP-Gruppen-ID, und stellen Sie eine lokale Priorität (optional, Standardwert 100 ist ausgewählt) für diese serviceseitige Ethernet-Schnittstelle bereit.
3. Geben Sie die VRRP Virtual IP (VIP)-Adresse an.
4. Aktivieren Sie den Regler TLOC Preference Change (TLOC-Voreinstellungsänderung), und geben Sie den Wert für die Änderung der TLOC-Voreinstellung an (zur Verarbeitung von asymmetrischem Routing).

5. Klicken Sie unter Objektverfolgung auf Verfolgungsobjekt hinzufügen.
6. Geben Sie die Objektverfolgungs-ID ein (definiert unter Systemvorlage).
7. Wählen Sie eine Tracker-Aktion aus (entweder Herunterfahren oder Absetzen).
8. Geben Sie den Abgangswert ein (abhängig von der in Schritt 7 gewählten Option).

Aus Sicht der CLI sehen die Konfigurationen wie folgt aus:

```
(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
!
```

Verifizierung

Es gibt zwei Optionen zum Überprüfen der explizit konfigurierten Objektverfolgung für VRRP-Anwendungsfälle.

- Auf dem SD-WAN Manager-Monitor > Geräte > {Gerätename auswählen} > Echtzeit:

1. Geben Sie unter Device Options (Geräteoptionen) "VRRP Information" (VRRP-Informationen) ein.

2. Aktivieren Sie das Kontrollkästchen unter Individuelle VRRP-Gruppe (Gruppen-ID), und zeigen Sie die Statistiken des Trackers (Track-Präfixname, Track-Status, Diskontinuitätszeit und Zeit der letzten Statusänderung) basierend auf den konfigurierten Objekttracker-IDs an.

- Auf dem SD-WAN-Manager-Monitor > Geräte > {Gerätename auswählen} > Ereignisse:

Bei einer auf dem Objekt-Tracker erkannten Zustandsänderung ändert die entsprechende VRRP-Gruppe, an die sie angefügt ist, ihren Zustand. Die entsprechenden Protokolle würden in diesem Abschnitt (mit dem Namen "Vrrp Group State Change") Details wie Hostname, If-Nummer, grp id, addr type, if name, vrrp group-state, state change-reason und vpn id ausfüllen.

Auf CLI des 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)
```

Für die Service-VPN NAT-Verfolgung verwendete Schnittstellen-/Routen-Objektverfolgung

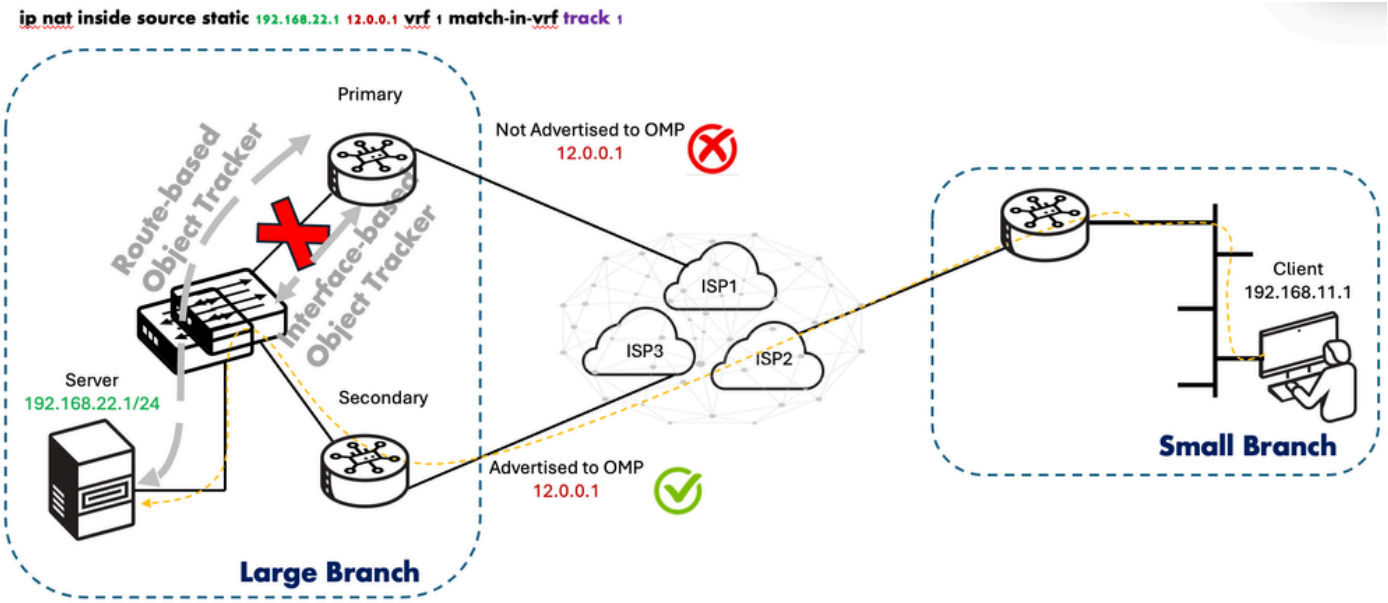
Der serviceseitige NAT-Objekttracker war eine Funktion, die in der Version 20.8/17.8 eingeführt wurde, bei der die im Service-VPN-NAT verwendete globale interne Adresse (innerhalb statischer NAT und innerhalb dynamischer NAT) nur dann in OMP angekündigt wird, wenn (i) die interne lokale Adresse erreichbar ist ODER (ii) das Leitungsprotokoll der LAN-/serviceseitigen Schnittstelle gemäß dem angeschlossenen Objekttracker verfügbar ist. Die Objektverfolgungsarten, die verwendet werden können, sind daher (i) route oder (ii) interface. Je nach Status des LAN-Präfix oder der LAN-Schnittstelle werden NAT-Routenankündigungen über OMP entweder hinzugefügt oder entfernt. Sie können im Cisco SD-WAN Manager Ereignisprotokolle anzeigen, um zu überwachen, welche NAT-Routenankündigungen hinzugefügt oder entfernt werden.

Es werden hier keine Sonden vom Tracker verwendet. Stattdessen verwendet es (i) das Vorhandensein eines Routing-Eintrags in der Routing-Tabelle ODER (ii) den Line-Protocol-Zustand, um den Tracker-Zustand (up/down) zu bestimmen. Bei Vorhandensein eines Routing-Eintrags oder von auf dem Line-Protocol der Schnittstelle basierenden Trackern gibt es keine Reaktionsintervalle - sobald der Routing-Eintrag oder das Line-Protocol der Schnittstelle den DOWN-Status erreicht, wird auch der Track-Status auf den DOWN-Status gebracht. Unmittelbar wird verhindert, dass die globale interne Adresse, die in der NAT-Anweisung verwendet wird, die dem Objektverfolgungsdienst zugeordnet ist, in OMP angekündigt wird. Weitere Informationen zu Service VPN NAT-Verfolgern finden Sie in der Konfigurationsanleitung.

Anwendungsfälle

Wenn eine LAN-Schnittstelle oder ein LAN-Präfix ausfällt, wird der serviceseitige NAT-Objekttracker automatisch deaktiviert. Sie können Ereignisprotokolle anzeigen in Cisco SD-WAN-Manager zur Überwachung, welche NAT-Routenankündigungen hinzugefügt oder entfernt werden. Im nächsten Anwendungsfall muss der Client auf den Server in der großen Außenstelle zugreifen. Das Problem tritt jedoch in Situationen auf, in denen entweder die Route zum Server an den großen Zweigstellen (in HA) entfernt wird ODER wenn die LAN-seitige (serviceseitige) Schnittstelle an einem beliebigen Edge in der großen Zweigstelle ausfällt. Wenn Sie in solchen Situationen dienstseitige NAT mit dem Objekt-Tracker anwenden, stellen Sie sicher, dass der vom

Client eingehende Datenverkehr immer an die richtige Kante in der großen Außenstelle geleitet wird, indem Sie die globale interne Adressanzeige in OMP steuern. Falls eine solche Kontrolle nicht in der Routenankündigung in OMP erzwungen wird, wird der Datenverkehr aufgrund der Nicht-Erreichbarkeit von diesem entsprechenden Edge zum Server in der großen Außenstelle blockiert.



Konfiguration

Die Konfiguration von Objekt-Trackern erfolgt über Systemvorlagen in der Legacy-Konfiguration. Anschließend wird der Objekt-Tracker der jeweiligen NAT-Anweisung (innerhalb statischer oder innerhalb dynamischer) in der Service-VPN-Funktionsvorlage hinzugefügt. In der Konfigurationsgruppe wurde dieser Mechanismus vereinfacht, indem direkt eine Option zum Hinzufügen des Objektverfolgungsgeräts zum entsprechenden Serviceprofil-Ethernet-Schnittstellenprofil abgerufen wurde. Nachfolgend sind die Möglichkeiten zur Konfiguration aufgeführt, je nach vom Benutzer bevorzugter Konfigurationsmethode.

- Konfigurationsgruppe Konfiguration > Konfigurationsgruppen > Serviceprofil > Funktion hinzufügen > Object Tracker:

1. Geben Sie einen Namen und eine Beschreibung für den neu zu definierenden Objekt-Tracker an.
2. Wählen Sie den Tracker-Typ aus (zwischen Schnittstelle und Route).
3. Weisen Sie eine Objektverfolgungskennung zu.
4. Geben Sie den Schnittstellennamen ODER die Route-IP, Route-IP-Maske und das VPN an (abhängig von der in Schritt 2 gewählten Option).

- Konfiguration > Konfigurationsgruppen > Serviceprofil > NAT-Abschnitt:

1. Erstellen Sie einen NAT-Pool (erforderlich für das Auslösen von SSNAT), indem Sie auf die Schaltfläche Add NAT Pool (NAT-Pool hinzufügen) klicken.

2. Geben Sie Details zum NAT-Pool an, z. B. NatPool-Name, Präfixlänge, Bereichsstart,

Bereichsende und Richtung.

3. Wechseln Sie zu Static NAT im gleichen Abschnitt, und klicken Sie auf die Schaltfläche Add New Static NAT (Neue statische NAT hinzufügen). (Sie können den Objekt-Tracker auch innerhalb des dynamischen Pool-NAT anhängen).

4. Geben Sie Details wie Quell-IP, umgewandelte Quell-IP und statische NAT-Richtung an.

5. Wählen Sie unter dem Feld Objektverfolgung zuordnen aus der Dropdownliste den zuvor erstellten Objektverfolgungsdienst aus.

- Legacy-Konfiguration > Vorlagen > Funktionsvorlagen > System > Tracker-Abschnitt:

1. Klicken Sie auf die Schaltfläche New Object Tracker.
2. Wählen Sie den Tracker-Typ aus (zwischen Schnittstelle und Route).
3. Weisen Sie eine Objekt-ID zu.
4. Geben Sie den Schnittstellennamen OR Route IP, Route IP Mask und VPN an (abhängig von der in Schritt 2 gewählten Option).

- Konfiguration > Vorlagen > Cisco VPN (Service-seitig) > Abschnitt "NAT":

1. Erstellen Sie einen NAT-Pool (erforderlich für das Auslösen von SSNAT), indem Sie auf die Schaltfläche Neuer NAT-Pool klicken.

2. Geben Sie Details zum NAT-Pool an, z. B. NAT-Poolname, NAT-Poolpräfixlänge, NAT-Poolbereichsstart, NAT-Poolbereichsende und NAT-Richtung.

3. Wechseln Sie im gleichen Abschnitt zu Static NAT, und klicken Sie auf die Schaltfläche New Static NAT (Neue statische NAT). (Sie können den Objekt-Tracker auch innerhalb des dynamischen Pool-NAT anhängen).

4. Geben Sie Details wie die IP-Quelladresse, die umgewandelte IP-Quelladresse und die statische NAT-Richtung an.

5. Geben Sie im Feld Objektverfolgung hinzufügen den Namen des zuvor erstellten Objektverfolgungssystems ein.

Aus Sicht der CLI sehen die Konfigurationen wie folgt aus:

```
(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
!
```

Im Anwendungsfall von SSNAT wird angenommen, dass Benutzer Datenrichtlinien anwenden, um den Datenverkehr in NAT-Datenflüssen an die in -> out und out -> anzupassen.

Verifizierung

Es gibt zwei Verifizierungsbereiche für explizit konfigurierte Object Tracker für NAT-Anwendungsfälle.

- Auf SD-WAN Manager: Überwachung > Geräte > {Gerätename auswählen} > Echtzeit:

1. Geben Sie unter "Device Options" (Geräteoptionen) "IP NAT Translation" ein.

2. Aktivieren Sie das Kontrollkästchen unter Individual NAT Translation (Einzelne NAT-Übersetzung), und zeigen Sie die Statistiken des Eintrags (Inside Local address/port, Inside Global address/port, Outside Local address/port, Outside Global address/port, VRF-ID, VRF-Name und Protokoll) basierend auf Ihren konfigurierten Object Tracker-IDs an.

- Auf SD-WAN Manager: Überwachung > Geräte > {Gerätename auswählen} > Ereignisse:

Bei einer auf dem Objekttracker erkannten Zustandsänderung, die der in OMP abgeschnittenen NAT-Route entspricht, werden Ereignisse mit dem Namen "NAT Route Change" angezeigt, die Details wie Hostname, Objekttracker, Adresse, Maske, Routentyp und Aktualisierung enthalten. Dabei werden die Adresse und die Maske der globalen internen Adresse zugeordnet, die unter der statischen NAT-Anweisung konfiguriert wurde.

Auf CLI des 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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.