Comprender la usabilidad y los casos prácticos de Catalyst SD-WAN Tracker

Contenido

Introducción

Este documento describe las redes de superposición empresariales Catalyst SD-WAN, la facilidad de uso del rastreador y los casos prácticos.

Antecedentes

Las redes de superposición empresariales Catalyst SD-WAN suelen interactuar con una amplia variedad de cargas de trabajo, aplicaciones y servicios externos. cualquiera de las cuales se puede ubicar en la nube, en el data center, en los hubs o en sucursales remotas. El plano de control de la SD-WAN es responsable de anunciar las rutas hacia estos servicios a través de la superposición de una manera escalable. En situaciones en las que las aplicaciones y los servicios críticos se vuelven inalcanzables a lo largo de una ruta específica, los operadores de red deben ser capaces de detectar estos eventos y redirigir el tráfico de los usuarios a rutas más adecuadas para evitar el bloqueo indefinido del tráfico. Para detectar y rectificar estos tipos de fallos de red, el plano de control de la SD-WAN de Catalyst se basa en rastreadores para supervisar el estado de los servicios externos y realizar los cambios de routing adecuados.

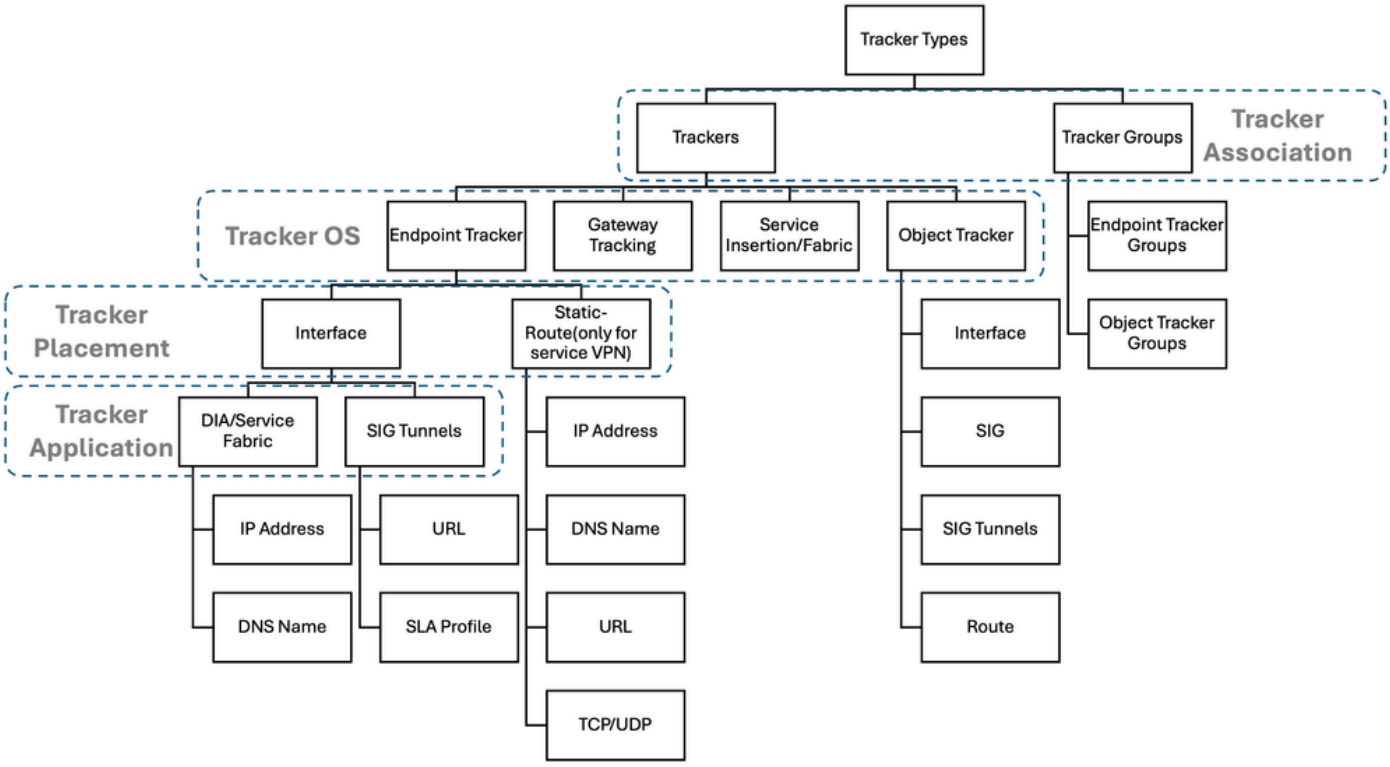
Un rastreador es un mecanismo de detección de alcance del plano de control que envía paquetes de sonda hacia un terminal específico y notifica los cambios de estado de disponibilidad (activo o inactivo) del terminal a los módulos interesados. Los rastreadores están diseñados como una abstracción escalable de alto nivel de la función nativa IP SLA de Cisco IOS-XE®, que puede formar una variedad de sondeos (incluidos HTTP, ICMP y DNS). Cuando un rastreador notifica a un módulo de cliente un cambio de estado, ese módulo puede tomar las medidas adecuadas para evitar la obstrucción del tráfico, como instalar o desinstalar una ruta o un conjunto de rutas. Las aplicaciones actuales de rastreadores en las soluciones de SD-WAN y de enrutamiento SD incluyen, entre otras: rastreadores DIA (acceso directo a Internet), rastreadores SIG (gateway de Internet seguro), rastreadores de servicio, rastreadores de ruta estática, grupos de seguimiento, etc.

Para crear redes de alta disponibilidad que sean resistentes a los fallos del servicio, es fundamental saber cuándo se debe utilizar cada tipo de configuración o modelo de seguimiento. El objetivo de este artículo es explicar dónde y cómo se utiliza cada tipo de rastreador. Aquí se abordan los diversos rastreadores, así como el caso práctico principal de cada rastreador y los flujos de trabajo de configuración básicos para implementar cada solución. Por último, este artículo presenta un recorrido por las advertencias generales que involucran a los rastreadores en Cisco IOS-XE®.

En este artículo se hace una distinción entre las soluciones endpoint-tracker (SD-WAN y SD-Routing específicas) y object tracker (Native IOS-XE), que abordan diferentes casos prácticos.

Tipos de rastreadores

Este gráfico proporciona una breve descripción general de todos los tipos de rastreadores disponibles en la solución Cisco Catalyst SD-WAN:



En el gráfico anterior, hay cuatro áreas en las que se pueden clasificar los rastreadores: Tracker Association, Tracker OS, Tracker Placement y Tracker Application. En la siguiente sección se describe cada clasificación:

1. Asociación de seguimiento: Esta clasificación describe si un rastreador es un solo rastreador o un grupo de rastreadores. Cisco Catalyst SD-WAN admite el uso de varios rastreadores en un grupo (hasta 2 en este momento de la escritura) y el estado general del grupo de seguimiento lo determina un operador AND u OR booleano. Entre los ejemplos se incluyen un grupo de seguimiento de extremos o un grupo de seguimiento de objetos.
2. Sistema operativo de seguimiento: Esta clasificación describe el sistema operativo Cisco IOS-XE® o el modo en el que se admite el rastreador. Los routers Cisco Catalyst IOS-XE admiten dos modos operativos:

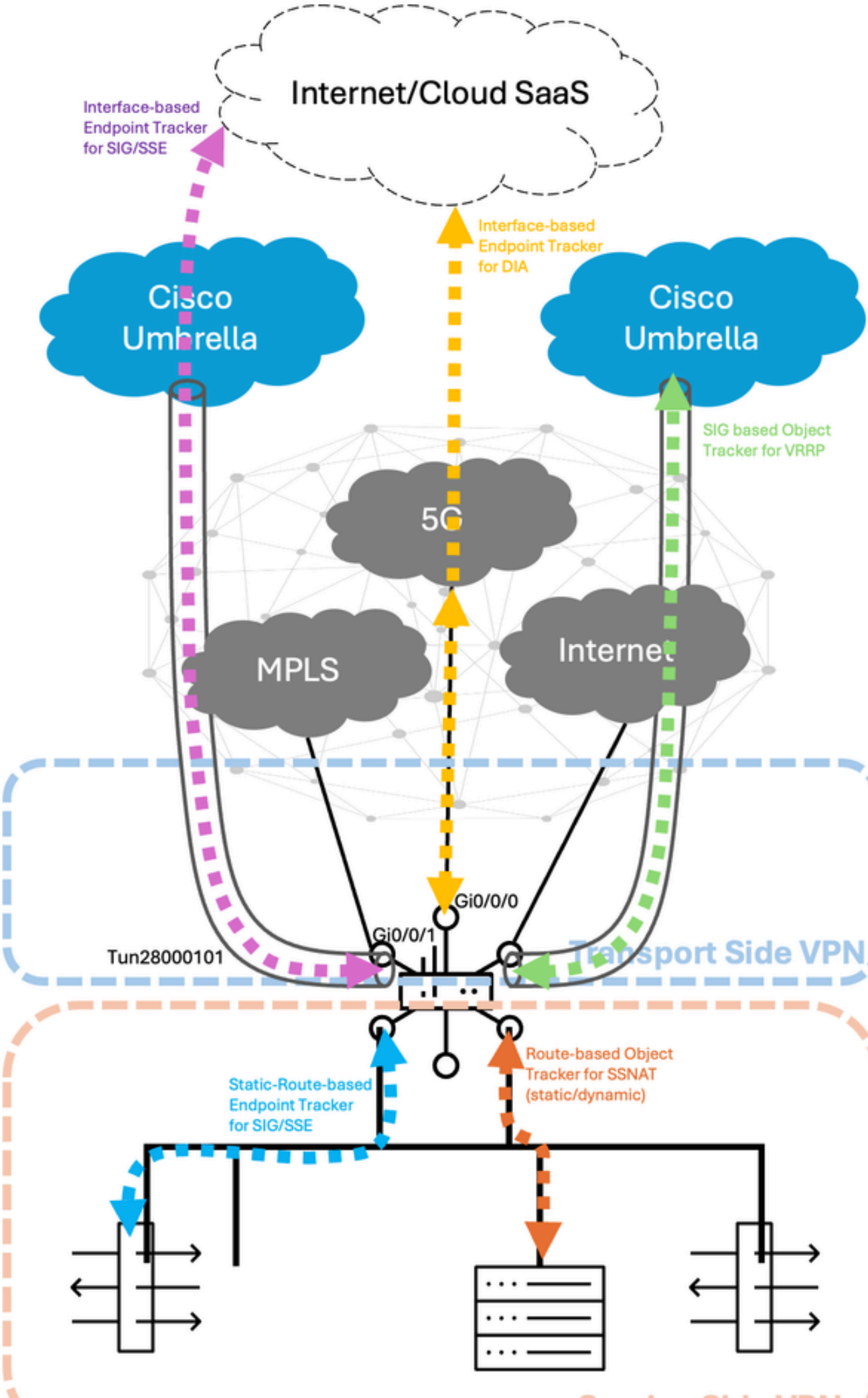
- Modo autónomo y
- Modo de controlador.

Todas las funciones de seguimiento de terminales y seguimiento de gateway están diseñadas para casos de uso en modo de controlador (SD-WAN), mientras que el seguimiento de objetos está pensado para casos de uso en modo autónomo (SD-Routing).

3. Ubicación del rastreador: Esta clasificación describe la ubicación en la que está configurado el rastreador. Actualmente, Cisco Catalyst SD-WAN admite la aplicación de rastreadores en interfaces, rutas estáticas o servicios.

4. Aplicación de seguimiento: Esta clasificación describe los casos prácticos de alto nivel y las funciones compatibles con Cisco Catalyst SD-WAN. Si bien hay numerosas áreas de aplicación de rastreadores, algunos de ellos incluyen: Acceso directo a Internet (DIA), gateway de Internet seguro (SIG), Secure Service Edge (SSE), seguimiento de VPN del lado del servicio, etc.

A continuación se muestra una representación visual del tráfico de sondeo del rastreador a través de VPN de servicio/transporte para varios casos prácticos en un Cisco Catalyst SD-WAN Edge (que también se puede denominar cEdge o vEdge):


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

configuradas en plataformas periféricas SD-WAN en la VPN del lado del transporte. De forma predeterminada, esto se habilita en las configuraciones básicas del perfil del sistema (Track Default Gateway) en Catalyst SD-WAN Manager. Esto ayuda a monitorear continuamente la dirección de siguiente salto especificada en cada ruta estática predeterminada en la VPN de transporte, para asegurar la conmutación por fallas de link/ruta, en caso de que se produzca un error de alcance en el siguiente salto (que también se denomina gateway, de ahí el nombre gateway-tracking). Para obtener más información sobre el seguimiento de la gateway, visite la guía de configuración.

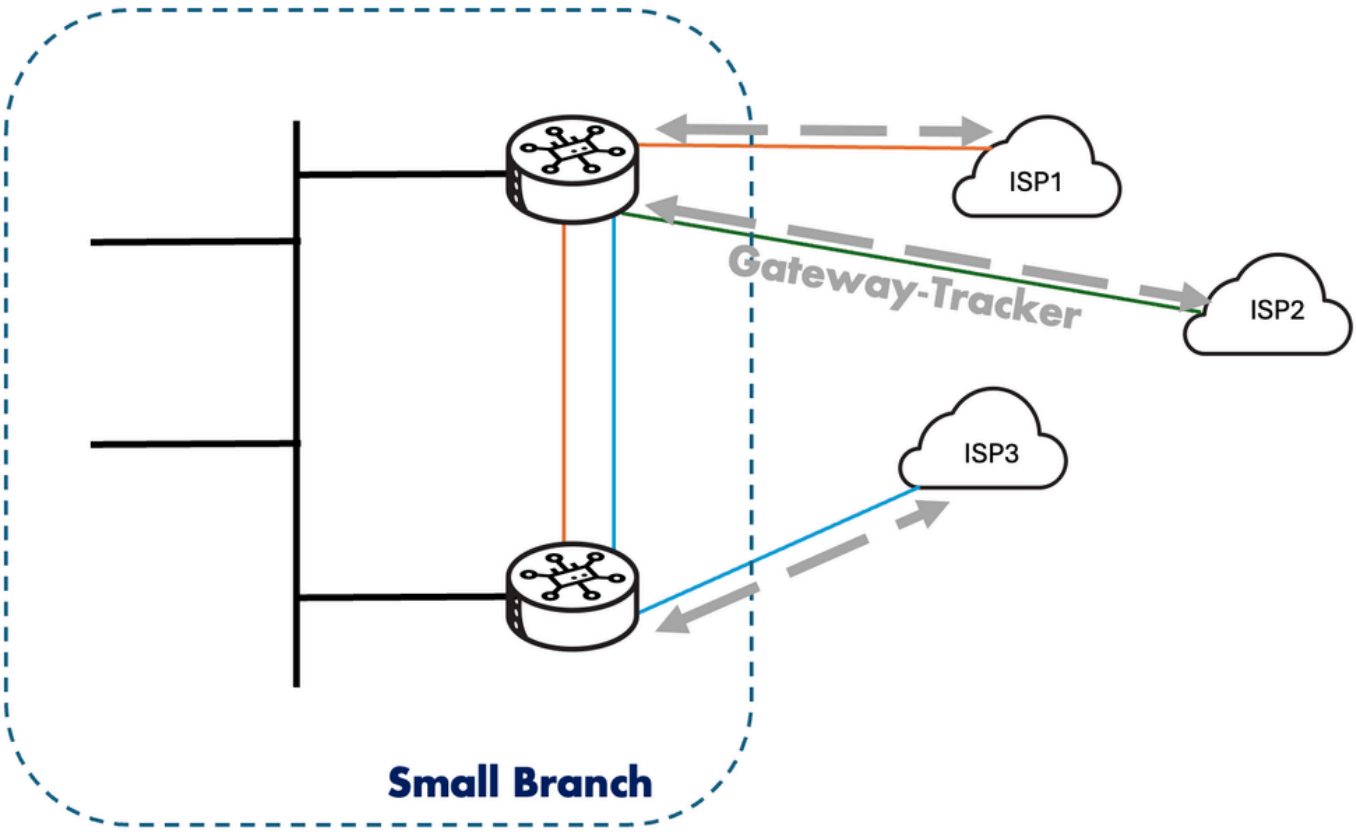
El tipo de sondeos utilizados aquí son paquetes inundados de unidifusión desconocida de solicitud ARP. Los intervalos utilizados son:

- Hello (saludo) 10 segundos
- Tiempo en espera: 100 segundos
- Tipo de paquete/sonda: ARP

Junto con el seguimiento del gateway, también se utiliza el seguimiento del transporte en los extremos de la SD-WAN para verificar la ruta enrutada entre el dispositivo local y un Cisco Catalyst SD-WAN Validator. Esto se realiza mediante sondeos ICMP a intervalos regulares de 3 segundos. Esto se configura mediante la palabra clave "track-transport" en el modo de configuración del sistema SD-WAN. Esto ayuda en la monitorización regular de la conexión DTLS al Cisco Catalyst SD-WAN Validator desde el borde WAN respectivo. Para obtener más información sobre el seguimiento del transporte, visite la guía de configuración.

Casos de uso

El rastreo de gateway es una función que se configura implícitamente de forma predeterminada en SD-WAN para todas las rutas estáticas predeterminadas que pertenecen a la VPN de transporte o a la Tabla de ruteo global (GRT). El uso de la función no siempre se origina desde el punto de vista de la configuración de la plantilla del administrador, sino que también puede evolucionar a partir de las rutas estáticas predeterminadas recibidas/adquiridas en los escenarios de uso de un servidor DHCP con las opciones #3, #81, etc.



Configuración

Aplicado de forma predeterminada en Cisco Catalyst SD-WAN:

```
!
system


 track-transport
 track-default-gateway


!
```

Verificación

A continuación, se describen formas de verificarlo según la configuración heredada y el grupo de

configuración:

- Grupo de configuración: Configuration > Configuration Groups > System profile > Basic sub-profile > Track Settings section > Track Default Gateway (predeterminado: ON)
- Configuración heredada: Configuration > Templates > Feature Templates > System template > Advanced section > Gateway Tracking (predeterminado:ON)

Seguimiento de Service Insertion 1.0 y Service Fabric 2.0

El rastreo de inserción de servicio 1.0 se introdujo en la versión 20.3/17.3, y es una función destinada a garantizar que la dirección de servicio (o dirección de reenvío) sea accesible o esté disponible. Esta información ayuda al Edge a agregar o retirar dinámicamente la información de siguiente salto de la política de Control/Datos. Con la configuración de Service Insertion 1.0, el rastreador (o dirección de rastreo) se habilita de forma predeterminada hacia la dirección de servicio. En función de esto, la dirección de reenvío y la dirección de servicio son iguales en 1.0. Aunque los rastreadores de servicio se configuran automáticamente con servicios, estos rastreadores se pueden inhabilitar mediante el comando no track-enable, o inhabilitando el control de seguimiento en la configuración de grupo de configuración/heredada. Dado que estas son las dos únicas operaciones posibles (habilitar/deshabilitar) con rastreadores asociados con servicios bajo Inserción de servicio 1.0, no hay otros parámetros que se puedan ajustar (como umbral, multiplicador, intervalo). El tipo de sondeos utilizados aquí son paquetes de solicitud de eco ICMP.

Para obtener más información sobre el seguimiento de la inserción de servicios 1.0, visite la guía de configuración. Los intervalos predeterminados utilizados en el seguimiento de la inserción de servicios 1.0 son:

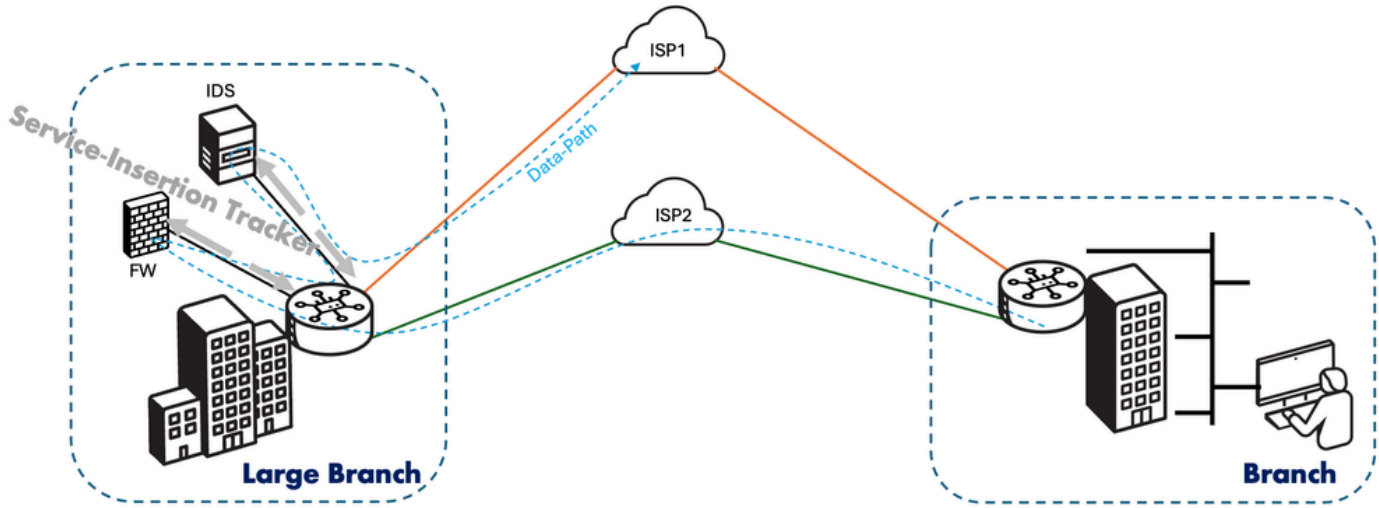
- Intervalo de sondeo: 5 sondas cada 60 segundos
- Multiplicador: 5 veces
- Tipo de paquete/sonda: Respuesta de eco/eco ICMP

El seguimiento de Service Fabric 2.0 forma parte de la oferta de la función Service Insertion 2.0 en la SD-WAN de Cisco Catalyst presentada a partir de la versión 20.13/17.13. En esta nueva variante de inserción de servicio, el método predeterminado utilizado por los perfiles de configuración y las plantillas sigue siendo tener un rastreador implícito que apunte a cada dirección de servicio definida (o dirección de reenvío) en un par service-HA por interfaz rx/tx. Sin embargo, con Service Fabric 2.0, ahora puede dividir la dirección de reenvío de la dirección de seguimiento. Esto se puede hacer simplemente definiendo rastreadores de terminales independientes para realizar el seguimiento de una dirección de terminal diferente de la dirección de servicio en sí. Este tema se trata con más detalle en las siguientes secciones.

Casos de uso

El caso práctico principal de los rastreadores de servicios es la supervisión escalable de la disponibilidad de los servicios, especialmente para el encadenamiento de servicios. El encadenamiento de servicios se puede implementar en una red que consta de varias VPN, donde

cada VPN representa una función u organización diferente, para garantizar que el tráfico entre las VPN fluye a través de un firewall. Por ejemplo, en una red de grandes instalaciones, el tráfico interdepartamental puede atravesar un firewall, mientras que el tráfico intradepartamental se puede enrutar directamente. El encadenamiento de servicios se puede ver en situaciones en las que un operador debe cumplir con la normativa, como el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), donde el tráfico PCI debe fluir a través de firewalls en un Data Center centralizado o un hub regional:



Configuración

Las configuraciones son las mismas que las del flujo de trabajo normal para configurar Service Insertion 1.0 en SD-WAN. Los rastreadores de inserción de servicio 1.0 se habilitarían de forma predeterminada en todas las direcciones de servicio.

- Grupo de configuración: Configuration > Configuration Groups > Service Profile > Service VPN > Service section:

1. Haga clic en el botón Add Service.

2. Seleccione un tipo de servicio.

3. Inscriba la dirección de servicio (máximo de 4 posibles, separados por una coma).

4. Compruebe que el botón Seguimiento está activado (de forma predeterminada). Si es necesario, se puede desactivar.

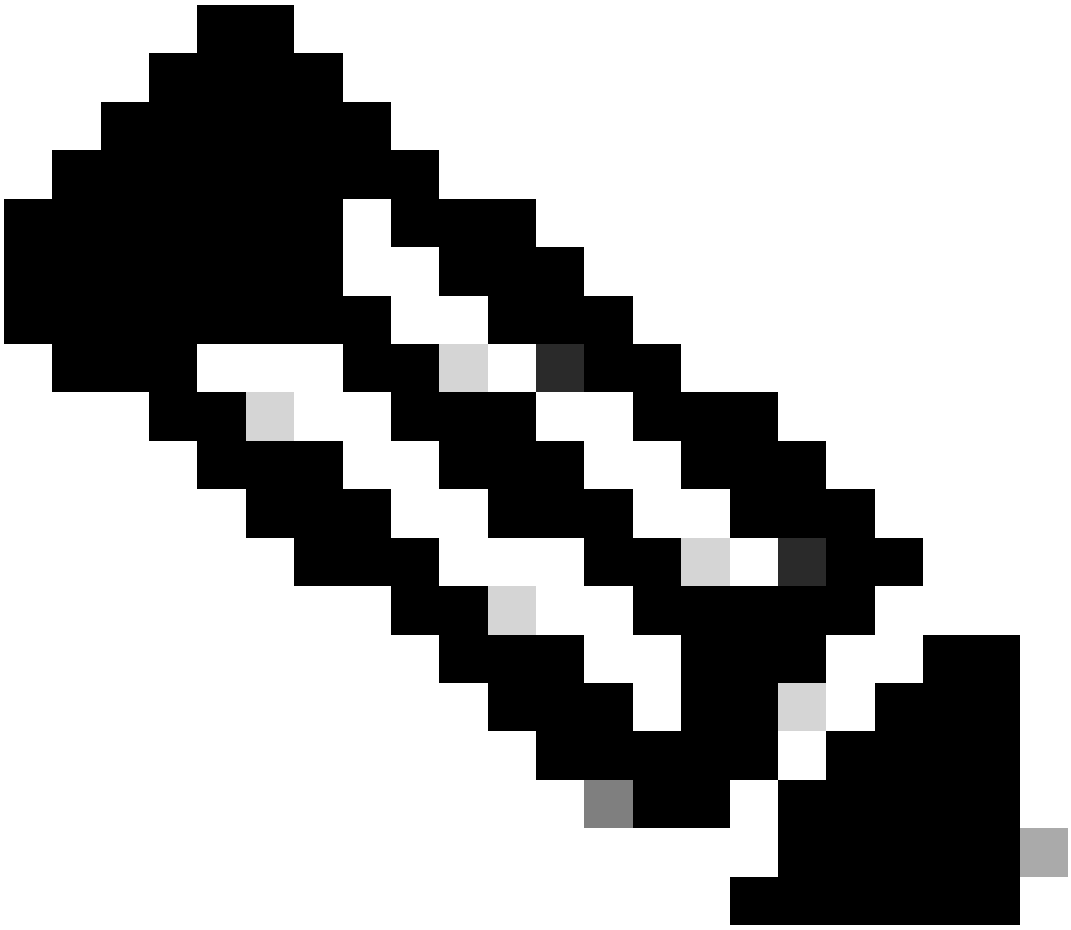
- Configuración heredada: Configuration > Templates > Feature Templates > Cisco VPN (service) > Service section:

1. Haga clic en el botón Nuevo servicio

2. Seleccione un tipo de servicio.

3. Inscriba la dirección de servicio (máximo de 4 posibles, separados por una coma).

4. Compruebe que el botón Seguimiento está activado (de forma predeterminada). Si es necesario, se puede desactivar.



> Nota: En el momento en que se configura el paso 3 (desde el grupo de configuración o desde la configuración heredada), el rastreador se inicia automáticamente en las diversas direcciones de servicio definidas

---

Desde el punto de vista de la CLI, la configuración para la inserción de servicios 1.0 se muestra de la siguiente manera:

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

Verificación

Los pasos para la verificación se extienden a los pasos similares seguidos como parte de los rastreadores de terminales basados en interfaz utilizados en las secciones anteriores.

Hay dos opciones de verificación del rastreador de extremos configurado explícitamente.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Aplicaciones > Rastreador:

Marque en Rastreador individual y vea las estadísticas del rastreador (tipos de rastreador, estado, punto final, tipo de punto final, índice VPN, nombre de host, tiempo de ida y vuelta) según su nombre de rastreador configurado.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Eventos:

En el caso de que se detecten inestabilidades en el rastreador, los registros respectivos se completarán en esta sección con detalles como el nombre de host, el nombre de punto de conexión, el nombre del rastreador, el nuevo estado, la familia de direcciones, y el id de vpn.

En la CLI del extremo:

```
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
```

Seguimiento de terminales de interfaz utilizado para DIA

Los rastreadores de terminales NAT DIA están diseñados principalmente para supervisar el alcance de las aplicaciones a través de una interfaz NAT DIA en plataformas periféricas SD-WAN.

Para los casos prácticos de acceso directo a Internet (DIA), los rastreadores DIA de NAT se utilizan principalmente para realizar un seguimiento de la interfaz del lado del transporte y activar

una conmutación por error a otra interfaz del lado del transporte disponible o a través de túneles superpuestos SD-WAN (mediante política de datos). Esta función se introdujo a partir de la versión 20.3/17.3 y la opción de la función de reserva NAT está disponible a partir de la versión 20.4/17.4. Si el rastreador determina que el Internet local no está disponible a través de la interfaz DIA de NAT, el router retira la ruta NAT de la VPN de servicio y vuelve a enrutar el tráfico según la configuración de ruteo local. El rastreador continúa verificando periódicamente el estado de la trayectoria a la interfaz. Cuando detecta que la ruta está funcionando de nuevo, el router reinstala la ruta NAT a Internet. Para obtener más información sobre los rastreadores DIA, visite la guía de configuración.

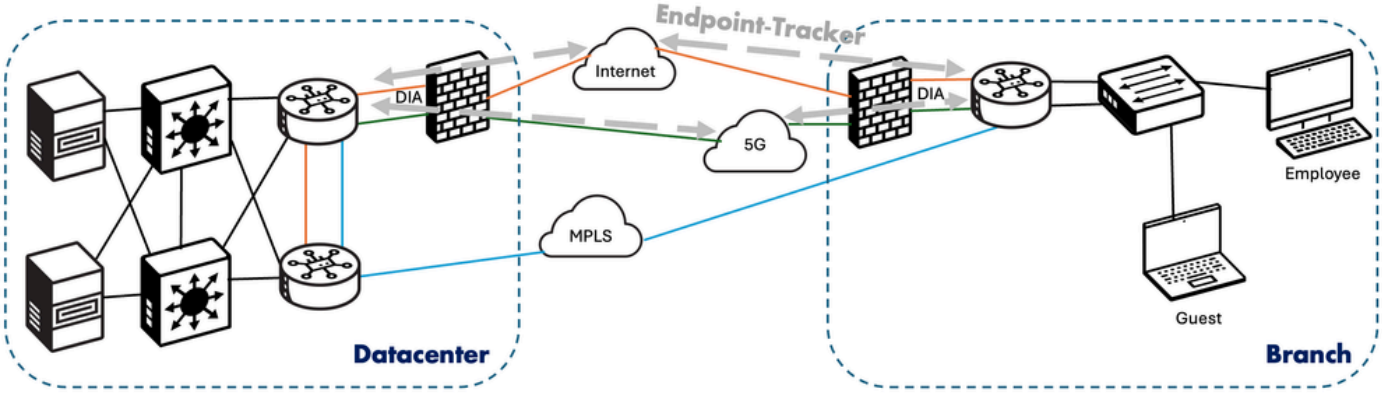
En la definición del rastreador, puede optar por proporcionar una dirección IP de un terminal accesible a través de la interfaz DIA de NAT (configurada como "IP de terminal") O proporcionar un nombre de dominio completamente calificado (FQDN) al terminal (configurado como "nombre-dns de terminal").

El tipo de sondeos que se utilizan aquí es un paquete de solicitud HTTP, muy similar a una pila PDU de solicitud de API HTTP. Los intervalos utilizados son:

- Intervalo de sondeo: 60 segundos
- Multiplicador: 180 segundos (puesto que #retries es 3 = 3 x 60 segundos)
- Tipo de paquete/sonda: HTTP

Casos de uso

A menudo, el DIA se implementa como optimización en las sucursales para evitar que el tráfico de la sucursal destinado a Internet pase al Data Center. Sin embargo, cuando se utiliza DIA en las sucursales, cualquier falta de disponibilidad a lo largo de las rutas DIA NAT tiene que recurrir a rutas alternativas para evitar la retención y la pérdida de servicio. Para los sitios que deseen utilizar el recurso alternativo al DC (a través de la superposición de SD-WAN mediante el recurso alternativo de NAT) en caso de que se produzca un fallo de interrupción de DIA local. Aproveche estos rastreadores de terminales basados en interfaz en las interfaces compatibles con DIA en los bordes de la sucursal para detectar fallas a fin de iniciar un failover a la trayectoria de DC/respaldo. De este modo, se logra una alta disponibilidad del servicio de Internet con una interrupción mínima en la empresa y, al mismo tiempo, se optimiza el tráfico de Internet con DIA:



Configuración

Estos rastreadores de terminales basados en interfaz deben configurarse manualmente para habilitar este conjunto de funciones. A continuación se indican las formas de configurarlo, en función del tipo de método de configuración preferido por el usuario.

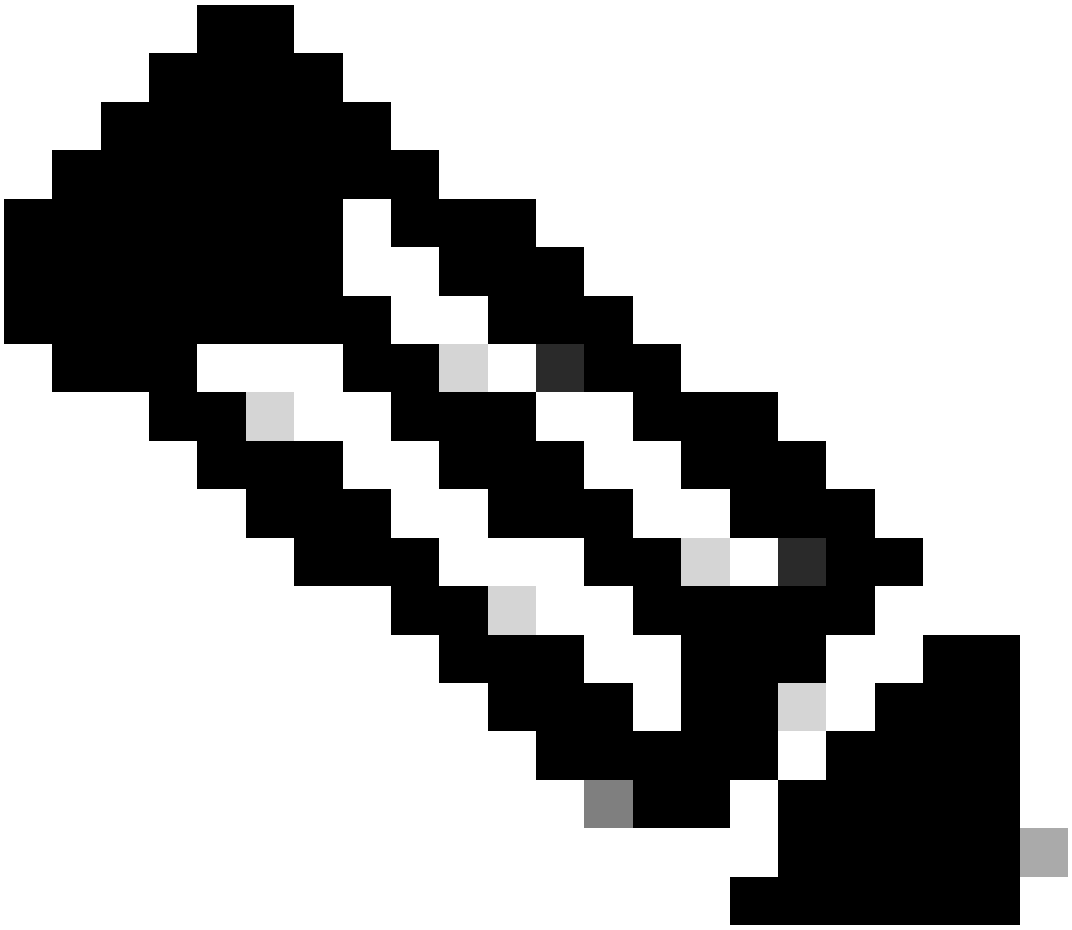
- Grupo de configuración: Configuration > Configuration Groups > Transport & Management Profile > Ethernet Interface > Add Feature > Tracker:

1. Defina un nombre de rastreador de punto final.

2. Elija un tipo de rastreador de punto final (entre HTTP predeterminado e ICMP).

Nota: El tipo de rastreador de punto final ICMP se introdujo desde la versión 20.13/17.13 en adelante.

3. Seleccione el terminal (entre IP de terminal predeterminada y nombre DNS de terminal).



Nota: Si elige el nombre DNS del terminal, asegúrese de que se haya definido un servidor DNS o un servidor de nombres válidos en el transporte VPN/VRF mediante el perfil de

configuración de Transport VPN.

4. Introduzca la dirección o el nombre DNS (FQDN) al que se deben enviar los sondeos de seguimiento (el formato depende del paso anterior).

5. (Opcional) Puede cambiar el intervalo de sondeo (valor predeterminado = 60 segundos) y el número de reintentos (valor predeterminado = 3 veces) para reducir el tiempo de detección de fallos.

- Configuración heredada:

Paso 1. Definición de Interface-Based Endpoint Tracker: Configuration > Templates > Feature Templates > System template > Tracker section:

1. En la subsección Rastreadores, seleccione el botón Rastreador de nuevos terminales.

2. Defina un nombre de seguimiento de terminales.

3. Elija el Tipo de Rastreador (entre interface-default y static-route) como interfaz, ya que los casos de uso de DIA son de interés aquí.

4. Seleccione el tipo de terminal (entre Dirección IP por defecto y Nombre DNS).

5. Introduzca la dirección IP del terminal o el nombre DNS del terminal al que se deben enviar los sondeos de seguimiento (el formato depende del paso anterior).

6. (Opcional) Puede elegir cambiar el umbral de sondeo (valor predeterminado = 300 ms), el intervalo (valor predeterminado = 60 segundos) y el multiplicador (valor predeterminado = 3 veces).

Paso 2. Aplique el Rastreador de Extremos Basado en Interfaz a una interfaz en la sección Transport VPN: Templates > Feature Templates > Cisco VPN Interface Ethernet > Advanced:

1. Introduzca el nombre del Rastreador de terminales definido en el Paso 1 anterior en el campo Rastreador.

Desde el punto de vista de la CLI, las configuraciones tienen el siguiente aspecto:

```
(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
!
```

Verificación

Hay dos opciones de verificación de rastreadores de extremos configurados explícitamente.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Aplicaciones > Tracker:

Marque en Rastreador individual y vea las estadísticas del rastreador (Tipos de Rastreador, Estado, Punto final, Tipo de punto final, Índice VPN, Nombre de host, Tiempo de ida y vuelta) según su Nombre de Rastreador configurado.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Eventos:

En el caso de que se detecten inestabilidades en el rastreador, los registros respectivos se completarán en esta sección con detalles como el nombre de host, el nombre de punto de conexión, el nombre del rastreador, el nuevo estado, la familia de direcciones, y el id de vpn.

En la CLI del extremo:

```
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
```

Seguidores de Terminales de Interfaz Utilizados para Túneles SIG/SSE

Cuando se utilizan rastreadores de terminales para casos prácticos de SIG Tunnel/SSE, esto indica principalmente que la empresa busca una oferta de pila de seguridad basada en la nube que esté disponible fácilmente en la actualidad con la ayuda de proveedores de Secure Internet Gateway (SIG) o Secure Service Edge (SSE), como Cisco, Cloudflare, Netskope, ZScalar, etc. Tanto SIG Tunnels como SSE forman parte del modelo de implementación de seguridad en la nube, en el que la sucursal utiliza la nube para ofrecer las soluciones de seguridad necesarias que necesita. El caso práctico de SIG Tunnels fue la oferta inicial de integración de Cisco Catalyst SD-WAN con dichos proveedores de SIG (a partir de la versión 20.4/17.4); sin embargo, con la evolución de las ofertas de seguridad proporcionadas en la nube, se presentó el caso práctico de SSE (a partir de la versión 20.13/17.13) para cubrir casos prácticos con proveedores como Cisco (a través de Cisco Secure Access) y ZScalar.

La TI requiere un enfoque fiable y explícito para proteger la agilidad y conectarse con ella. Ahora es habitual proporcionar a los empleados remotos acceso directo a aplicaciones en la nube, como Microsoft 365 y Salesforce, con seguridad adicional. La demanda de seguridad y redes proporcionadas por la nube aumenta cada día, ya que contratistas, partners, dispositivos de Internet of Things (IoT), etc., requieren acceso a la red. La convergencia de las funciones de seguridad y de red más cercanas a los dispositivos finales, en el extremo de la nube, se conoce como modelo de servicio llamado Cisco SASE. Cisco SASE combina las funciones de seguridad y de red proporcionadas en la nube para proporcionar acceso seguro a las aplicaciones para todos los usuarios o dispositivos, desde cualquier lugar y en cualquier momento. Secure Service Edge (SSE) es un enfoque de seguridad de red que ayuda a las organizaciones a mejorar el estado de seguridad de su entorno de trabajo a la vez que reduce la complejidad para los usuarios finales y los departamentos de TI. Para obtener más información sobre los rastreadores SIG Tunnel/SSE, visite la guía de configuración.

Casos de uso

Estos rastreadores de terminales basados en interfaz se utilizan en casos de uso de SIG Tunnel/SSE, en los que desea realizar un seguimiento de un terminal URL de aplicación SaaS conocido o de un terminal URL específico de interés. Hoy en día, SSE es el escenario más

utilizado desde que la arquitectura SASE se dividió en funcionalidades de núcleo SSE y funcionalidades SD-WAN. A continuación, debe elegir entre funciones activas y en espera dentro de los túneles IPSec creados a partir de un sitio (en este caso, el DC). El usuario tiene la opción de adjuntar el rastreador en la interfaz de túnel respectiva.

En el caso de los proveedores de SSE, como Cisco Secure Access (de Cisco), se utiliza un rastreador de terminales implícito que se configura de forma predeterminada. Sin embargo, el usuario tiene la opción de crear un rastreador de extremos personalizado y de conseguir que se adjunte a la interfaz de túnel IPSec. Los parámetros del rastreador de punto final predeterminado/implícito utilizado en SSE son:

Para Cisco SSE:

Nombre del rastreador: DefaultTracker

Terminal objeto de seguimiento: http://service.sig.umbrella.com

Tipo de terminal: API_URL

Umbral: 300 m

Multiplicar: 3

Intervalo: 60 seg.

Para ZScaler SSE:

Nombre del rastreador: DefaultTracker

Terminal objeto de seguimiento: http://gateway.zscalerthree.net/vpnte

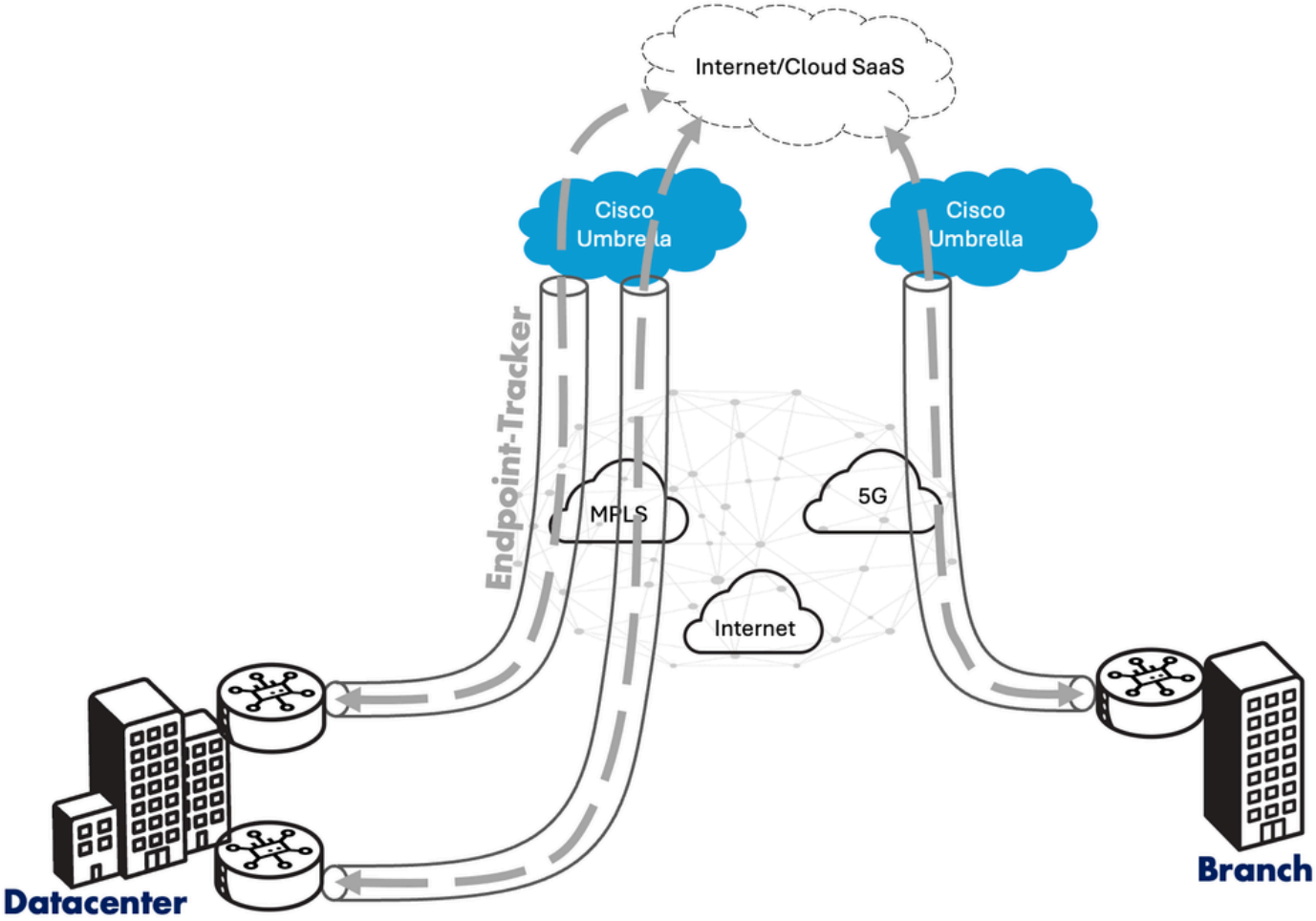
Tipo de terminal: API_URL

Umbral: 300 m

Multiplicador: 3

Intervalo: 60 seg.

En el caso de los túneles SIG, no se ha definido ningún rastreador de punto final predeterminado/implícito. Por lo tanto, el usuario debe configurar manualmente un rastreador de terminales basado en interfaz en caso de que desee rastrear la interfaz de túnel IPSec hacia la nube del proveedor SIG:



Configuración

En el caso de los proveedores SSE, el usuario no tiene que definir ningún rastreador de terminales explícitamente (a menos que se desee). Sin embargo, los flujos de trabajo son diferentes en función del tipo de configuración.

Como requisito previo, debe definir las credenciales de SIG/SSE Administration > Settings > External Services > Cloud Credentials:

1. En Credenciales del proveedor de la nube, alterne la opción de Umbrella o Cisco SSE (o ambos).

2. Defina los parámetros, como ID de organización, Clave API, Secreto).

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

1. Haga clic en Add Secure Internet Gateway o Add Secure Service Edge.

2. Defina un nombre y una descripción.

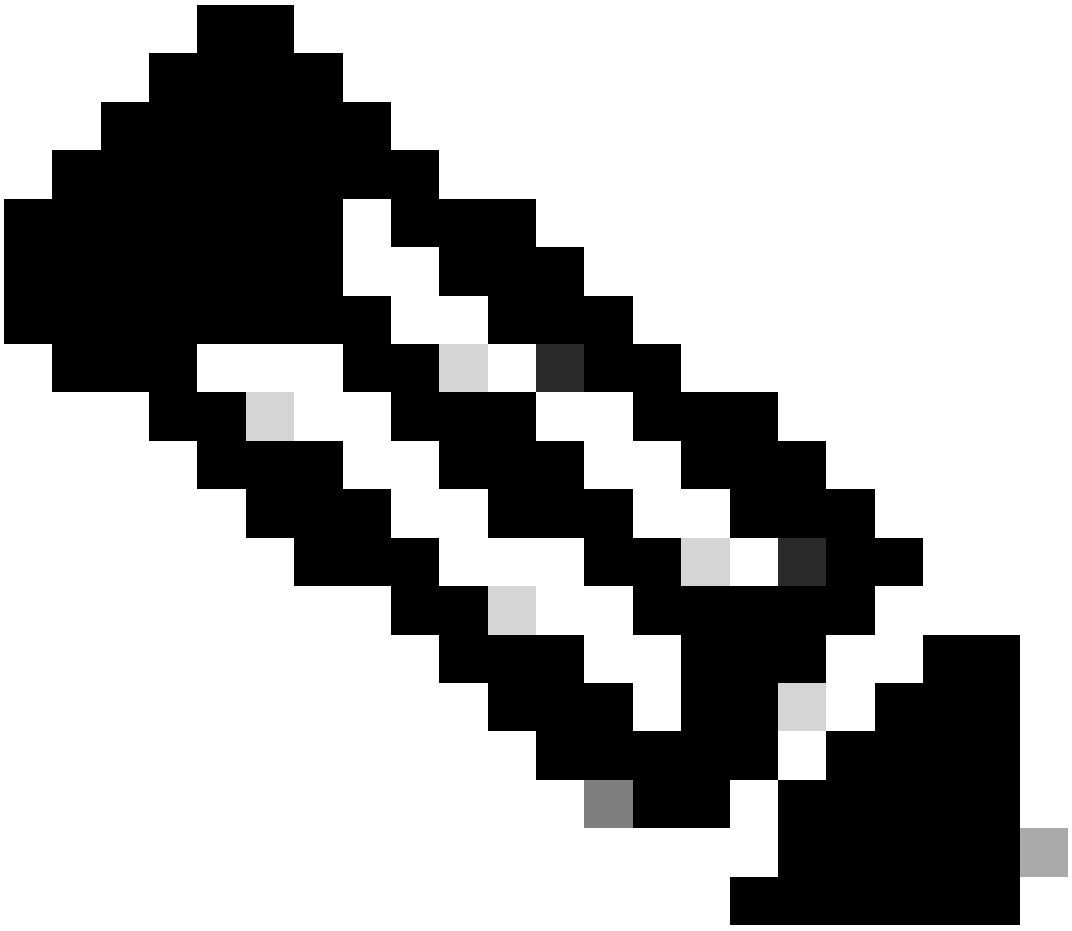
3. Seleccione uno de los botones de opción de Proveedor SIG/SSE (Umbrella o Cisco SSE).

4. En la sección Rastreador, defina la dirección IP de origen que se utiliza para obtener los

sondeos de seguimiento.

5. Si decide definir un rastreador de extremos explícito/personalizado, haga clic en Agregar Rastreador, a continuación, rellene los parámetros para el rastreador de extremos (Nombre, URL de API de Extremo, Umbral, Intervalo de Sonda y Multiplicador).

6. En la sección Configuración, cree las interfaces de túnel en las que puede definir los parámetros (como Nombre de Interfaz, Descripción, Rastreador, Interfaz de Origen de Túnel, Data Center Principal/Secundario).



Nota: En el paso 6, el usuario tiene la opción de conectar el controlador de terminales definido al túnel IPSec correspondiente. Tenga en cuenta que este campo es opcional.

---

7. En la sección Alta Disponibilidad, cree un par de interfaces y defina la interfaz activa y la interfaz de copia de seguridad junto con sus respectivos pesos. A continuación, aplique el grupo de políticas configurado anteriormente a las aristas relevantes.

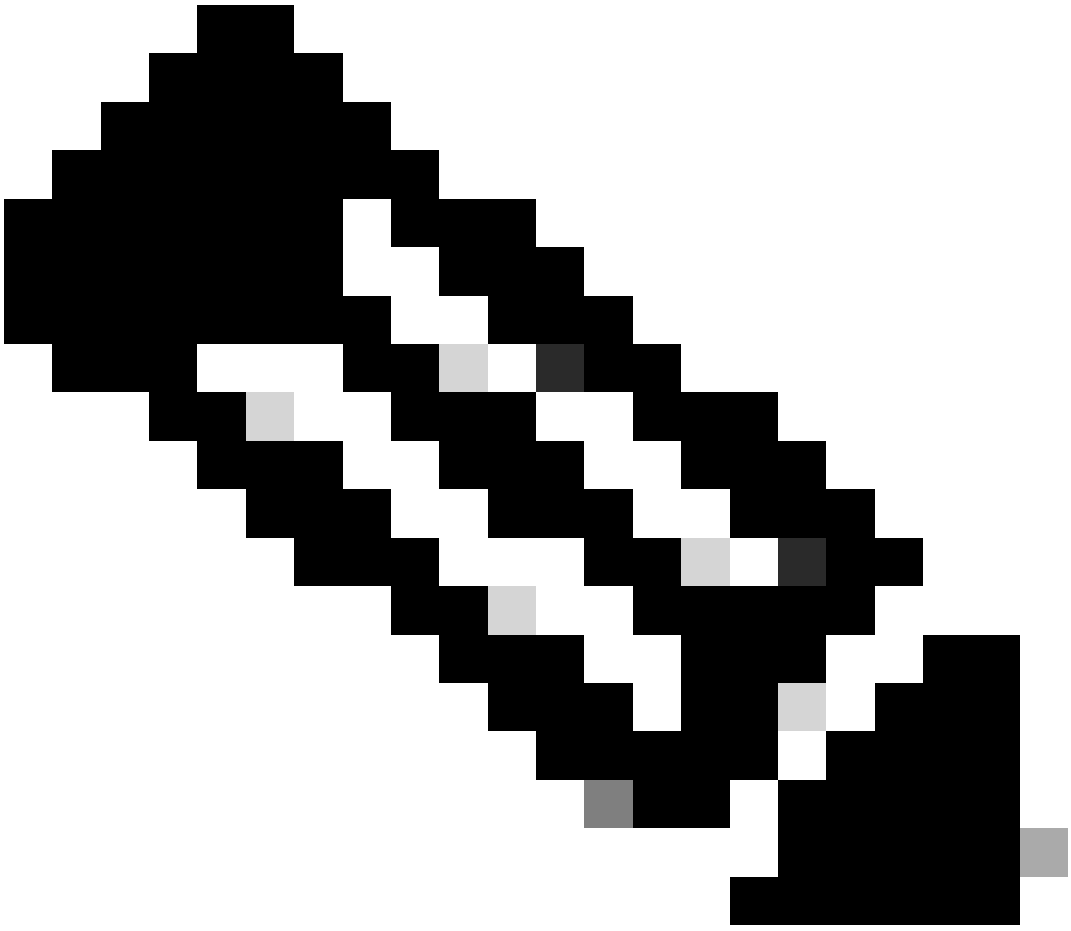
Set legacy configuration Configuration > Templates > Feature Templates > Cisco Secure Internet Gateway feature template:

1. Seleccione uno de los botones de opción de Proveedor SIG (Umbrella, ZScalar o Generic).

2. En la sección Rastreador (BETA), defina la dirección IP de origen que se utiliza para obtener los sondeos de seguimiento.

5. Si decide definir un rastreador de extremos explícito/personalizado, haga clic en Nuevo Rastreador y rellene los parámetros del rastreador de extremos (Nombre, URL de API del terminal, Umbral, Intervalo y Multiplicador).

6. En la sección Configuración, cree las interfaces de túnel (haciendo clic en Añadir Túnel) en las que puede definir los parámetros (como Nombre de Interfaz, Descripción, Rastreador, Interfaz de Origen de Túnel, Data Center Primario/Secundario).



Nota: En el paso 6, el usuario tiene la opción de conectar el controlador de terminales definido al túnel IPSec correspondiente. Tenga en cuenta que este campo es opcional.

---

7. En la sección Alta Disponibilidad, defina la interfaz activa y la interfaz de copia de seguridad junto con sus ponderaciones respectivas.

Desde el punto de vista de la CLI, las configuraciones tienen el siguiente aspecto:

```
(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
!
```

Verificación

Hay opciones de verificación de rastreadores de terminales configurados explícitamente.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Aplicaciones > Rastreador:

Marque en Rastreador individual y vea las estadísticas del rastreador (tipos de rastreador, estado,

punto final, tipo de punto final, índice VPN, nombre de host, tiempo de ida y vuelta) según su nombre de rastreador configurado.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Eventos:

En el caso de que se detecten inestabilidades en el rastreador, los registros respectivos se completarán en esta sección con detalles como el nombre de host, el nombre de punto de conexión, el nombre del rastreador, el nuevo estado, la familia de direcciones, y el id de vpn.

En la CLI del extremo:

```
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
```

Seguimiento de terminales de interfaz utilizado para Service Fabric 2.0

El seguimiento de Service Fabric 2.0, que se introdujo en la versión 20.13/17.13, es una variante mejorada del seguimiento de la inserción de servicios 1.0, en el que los usuarios tienen la capacidad de personalizar los rastreadores en mayor medida. El comportamiento predeterminado se conserva de la versión anterior de Inserción de servicio (1.0), un rastreador se iniciaría de forma predeterminada con la definición de cada dirección de servicio (o dirección de reenvío) en un par de servicio-HA por rx/tx. Sin embargo, con la inserción de servicios 2.0, la dirección de seguimiento (IP/punto final a la dirección de seguimiento) se puede separar de la dirección de reenvío (normalmente la dirección de servicio). Esto se realiza mediante rastreadores de terminales personalizados definidos en el nivel de VPN. Para obtener más información sobre los rastreadores de Service Fabric 2.0, visite la guía de configuración.

Si el usuario elige utilizar el rastreador predeterminado, las especificaciones de los sondeos del rastreador son:

- Hello (saludo) 1 sonda cada 30 segundos
- Multiplicador: 3 veces
- Tipo de paquete/sonda: Respuesta de eco/eco ICMP

Si el usuario elige utilizar un rastreador personalizado, las especificaciones de los sondeos del rastreador son:

- Hello (saludo) 1 sonda cada 60 segundos
- Multiplicador: 3 veces
- Tipo de paquete/sonda: Solicitud/respuesta de eco ICMP

Casos de uso

Aquí también se aplican los casos prácticos de inserción de servicios 1.0 mencionados en las secciones anteriores.

Configuración

Se admite la configuración basada en flujos de trabajo para la inserción de servicios 2.0, que es un enfoque guiado por asistentes que ayuda a simplificar la experiencia del usuario, a la vez que se adhiere a los pasos de flujo de trabajo de grupo de configuración estándar.

1. Defina el grupo Cadena de Servicio - Configuración en la sección Configuración > Inserción de Servicio > Definiciones de Cadena de Servicio:

a. Haga clic en el botón Add Service Chain Definition.

b. Complete los detalles del Nombre y la Descripción del Servicio.

c. Rellene un formato de lista (seleccionando en la lista desplegable), el Tipo de servicio.

2. Defina el grupo Instancia de Cadena de Servicio - Configuración en la sección Configuración > Inserción de Servicio > Configuraciones de Cadena de Servicio:

a. Haga clic en Add Service Chain Configuration.

b. En el paso Service Chain Definition (Definición de la cadena de servicio), seleccione el botón de opción Select Existing (Seleccionar existente) y elija el servicio definido anteriormente.

c. Proporcione un nombre y una descripción para el paso Start Service Chain Configuration.

d. En el paso Service Chain Configuration for Manually Connected Services, seleccione el Service Chain VPN-ID.

e. A continuación, para cada servicio definido en la instancia de la cadena de servicio (representado en subpestañas), en detalles del servicio, proporcione el tipo de conexión (IPv4, IPv6 o túnel conectado).

f. Seleccione la casilla de verificación Advanced. Si necesita tener casos prácticos de backup/HA

activos (también active el botón Agregar parámetros para Backup) o incluso si necesita definir un rastreador de punto final personalizado (también active el control de seguimiento personalizado).

g Si tiene escenarios en los que el tráfico de salida (tx) va al servicio a través de una interfaz y el tráfico de retorno del servicio se ingresa (rx) a través de otra interfaz, active el comando Tráfico desde el servicio se recibe en un botón de interfaz diferente.

h. Con los botones Advanced y Custom Tracker habilitados, defina la dirección IPv4 del servicio (dirección de reenvío), la interfaz del router SD-WAN (a la que está conectado el servicio) y el punto final del rastreador (dirección de seguimiento). También puede modificar los parámetros de seguimiento personalizados, como el intervalo y el multiplicador (haciendo clic en el botón de edición).

i. Repita los pasos (e), (f), (g) y (h) para cada servicio definido posteriormente.

3. Adjunte la instancia de la cadena de servicio al perfil de configuración del grupo de configuración perimetral en Configuration > Configuration Groups > Service Profile > Service VPN > Add Feature > Service Chain Attachment Gateway:

a. Proporcione un nombre y una descripción para este paquete Service Chain Attachment Gateway.

b. Seleccione la definición de cadena de servicio definida anteriormente (en el paso 1).

c. Vuelva a agregar/verificar los detalles como se realizó en el paso 2. Para la definición de seguimiento, la única diferencia con el paso 2 anterior es que tiene la oportunidad de dar un nombre de seguimiento y también seleccionar el tipo de seguimiento (de service-icmp a ipv6-service-icmp).

Desde el punto de vista de la CLI, las configuraciones tienen el siguiente aspecto:

```
!
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
!
```

Verificación

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

Marque en Rastreador individual y vea las estadísticas del rastreador (tipos de rastreador, estado, punto final, tipo de punto final, índice VPN, nombre de host, tiempo de ida y vuelta) según su nombre de rastreador configurado.

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

En el caso de que se detecten inestabilidades en el rastreador, los registros respectivos se completarán en esta sección con detalles como el nombre de host, el nombre de punto de conexión, el nombre del rastreador, el nuevo estado, la familia de direcciones, y el id de vpn.

En la CLI del extremo:

```
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
```

Seguidores de Extremos de Ruta Estática Utilizados para el Seguimiento de Rutas Estáticas (Lado de Servicio)

El segundo tipo de rastreadores de terminales se denomina rastreadores de terminales basados en ruta estática. Como indica el propio nombre, estos tipos de rastreadores se utilizan principalmente para rastrear la dirección de siguiente salto de cualquier ruta estática definida en la VPN del lado de servicio. De forma predeterminada, todos los tipos de rutas "conectadas" y "estáticas" se anuncian en el protocolo OMP, puesto que todos los sitios remotos que contienen la VPN de servicio respectiva detectan ese prefijo de destino (donde el siguiente salto apunta al TLOC del sitio de origen). El sitio de origen es el sitio desde el que se inició la ruta estática específica.

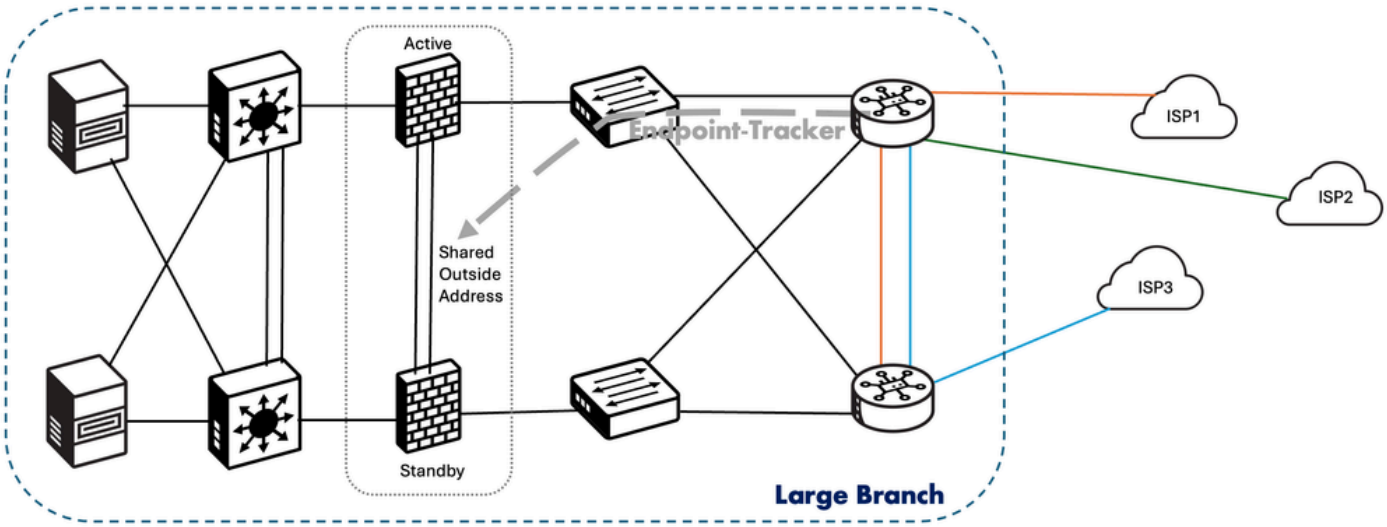
Sin embargo, en el caso de que la dirección de siguiente salto en la ruta estática sea inalcanzable, la ruta no deja de ser anunciada en OMP. Esto provocaría problemas de tráfico que se agota para los flujos destinados al sitio de origen. Esto genera la necesidad de adjuntar un rastreador a la ruta estática, para garantizar la publicidad de la ruta estática en OMP SOLAMENTE cuando la dirección de salto siguiente es accesible. Esta función se introdujo en la versión 20.3/17.3 para los rastreadores de terminales basados en ruta estática de tipo de dirección IP básica. A partir de la versión 20.7/17.7, se agregó soporte para el envío de sondas de seguimiento sólo a determinados puertos TCP o UDP de la dirección IP del siguiente salto (en casos en los que se usan firewalls para abrir solamente ciertos puertos con fines de seguimiento). Para obtener más información sobre los rastreadores de ruta estática, visite la guía de configuración.

El tipo de sondeos que se utilizan aquí es un paquete de solicitud de eco ICMP simple. Los intervalos utilizados son:

- Hello (saludo) 60 segundos
- Tiempo en espera: 180 segundos (puesto que #retries es 3 = 3 x 60 segundos)
- Tipo de paquete/sonda: Respuesta de eco/eco ICMP

Casos de uso

Este tipo de rastreadores de extremos basados en ruta estática se utilizan para el seguimiento del lado del servicio de las direcciones de siguiente salto en rutas estáticas. Uno de estos escenarios comunes sería el seguimiento de la dirección de próximo salto del lado LAN correspondiente a un par de firewalls activos/en espera, que comparten la dirección IP externa basada en la cual la interfaz externa está desempeñando el papel de firewall "activo". En los casos en los que las reglas del firewall parecen ser altamente restrictivas, en los que sólo se abren ciertos puertos para fines basados en casos de uso, el rastreador de ruta estática se puede utilizar para rastrear el puerto TCP/UDP específico a la dirección IP de siguiente salto que pertenece a la interfaz externa del firewall del lado de la LAN.



Configuración

Estos rastreadores de terminales basados en ruta estática deben configurarse manualmente para habilitar este conjunto de características. A continuación se indican las formas de configurarlo, en función del tipo de método de configuración preferido por el usuario.

- Grupo de configuración Configuration > Configuration Groups > Service Profile > Service VPN > Add Feature > Tracker:

1. Proporcione un nombre, descripción y nombre del rastreador para el nuevo rastreador (punto final) que se está definiendo.

2. Elija el tipo de terminal, en función de si sólo necesita realizar un seguimiento de la dirección IP del siguiente salto (seleccione el botón de radio Dirección) o incluso de puertos TCP/UDP específicos (seleccione el botón de radio Protocolo).

3. Introduzca la dirección en un formato de dirección IP. Introduzca también el protocolo (TCP o UDP) y el número de puerto, en caso de que haya seleccionado Protocol como tipo de terminal en el paso anterior.

4. Si es necesario, puede cambiar los valores por defecto de Intervalo de Sondeo, Número de Reintentos y Límite de Latencia.

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

1. Seleccione el botón Agregar ruta estática IPv4/IPv6.

2. Rellene los detalles, como Dirección de red, Máscara de subred, Siguiente salto, Dirección y AD.

3. Haga clic en el botón Add Next Hop With Tracker.

4. Vuelva a introducir la dirección de próximo salto, AD, y elija en la lista desplegable el nombre del rastreador (punto final) creado anteriormente.

- Configuración heredada Configuration > Templates > Feature Templates > System Template > Tracker section:

1. Seleccione el botón New Endpoint Tracker.

2. Proporcione un nombre para el nuevo rastreador (punto final) que se está definiendo.

3. Cambie el botón de opción Tracker Type a static-route.

4. Seleccione el tipo de terminal, como dirección IP de próximo salto (seleccione el botón de radio Dirección IP).

5. Introduzca la IP del terminal, en formato de dirección IP.

6. Si es necesario, puede cambiar los valores por defecto de Intervalo de Sondeo, Número de Reintentos y Límite de Latencia.

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

1. Seleccione el botón Ruta IPv4/IPv6 nueva.

2. Rellene los detalles, como Prefijo, Puerta de enlace.

3. Haga clic en el botón Agregar salto siguiente con rastreador.

4. Vuelva a introducir la dirección de próximo salto, AD (distancia) e introduzca manualmente el nombre del rastreador (punto final) creado anteriormente.

Desde el punto de vista de la CLI, las configuraciones tienen el siguiente aspecto:

```
(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
!
```

Verificación

Hay dos áreas de verificación de rastreadores de terminales configurados explícitamente.

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

1. En Opciones de dispositivo, escriba "Información de seguimiento de terminales."

2. Marque Rastreador individual (Nombre del punto de conexión) y vea las estadísticas del rastreador (Estado del rastreador, Nombre del registro del rastreador asociado, Latencia en mx desde el dispositivo al terminal, marca de tiempo de la última actualización) en función del Nombre del rastreador configurado.

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

En el caso de que se detecten inestabilidades en el rastreador, los registros respectivos se completarán en esta sección con detalles como el nombre de host, el nombre de punto de conexión, el nombre del rastreador, el nuevo estado, la familia de direcciones, y el id de vpn.

En la CLI del extremo:

```
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]
```

Rastreadores de Objetos de Interfaz Utilizados para el Seguimiento VRRP

Los Object Trackers son rastreadores diseñados para el consumo en modo autónomo (casos prácticos). Estos rastreadores que tienen casos de uso que varían desde el seguimiento de interfaz/túnel basado en VRRP hasta el seguimiento de NAT de VPN de servicio.

Para los casos prácticos de seguimiento de VRRP, el estado de VRRP se determina en función del estado del link de túnel. Si el túnel o la interfaz está fuera de servicio en el VRRP primario, el tráfico se dirige al VRRP secundario. El router VRRP secundario en el segmento LAN se convierte en VRRP principal para proporcionar gateway para el tráfico del lado de servicio. Este caso práctico solo se aplica al servicio VPN y ayuda a conmutar por error la función VRRP en el lado de la LAN en caso de fallo en la superposición SD-WAN (interfaz o túneles en el caso de SSE). Para conectar rastreadores a grupos VRRP, SOLO se pueden utilizar rastreadores de objetos (no rastreadores de extremos). Esta función se introdujo desde la versión 20.7/17.7 para Cisco Catalyst SD-WAN Edges.

No hay sondas usadas aquí por el rastreador. En su lugar, utiliza el estado de protocolo de línea para decidir el estado del rastreador (activo/inactivo). No hay intervalos de reacción en los rastreadores basados en el protocolo de línea de la interfaz - en el momento en que el protocolo de línea de la interfaz/túnel se DESACTIVA, el estado de la pista también se lleva al estado DOWN. Luego, dependiendo de la acción de apagado o decremento, el grupo VRRP volvería a converger en consecuencia. Para obtener más información sobre los rastreadores de la interfaz VRRP, visite la guía de configuración.

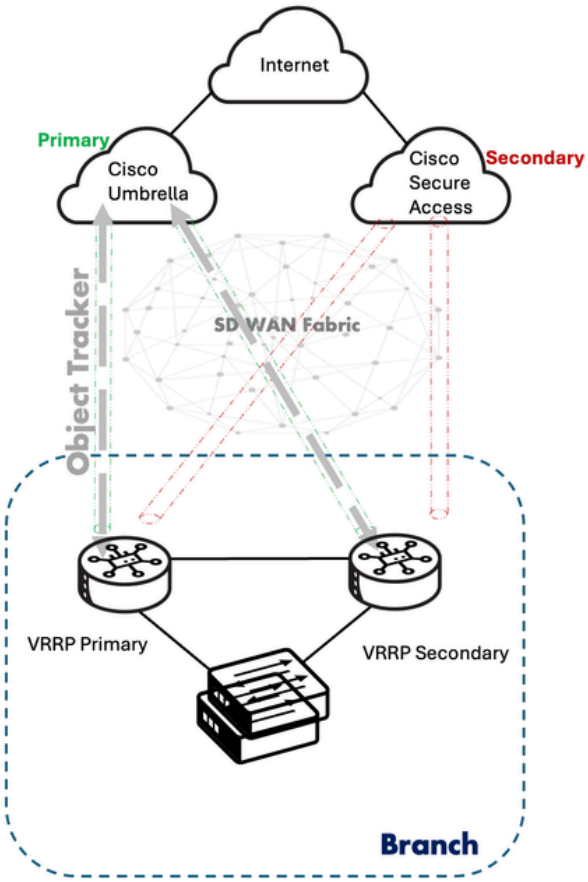
Casos de uso

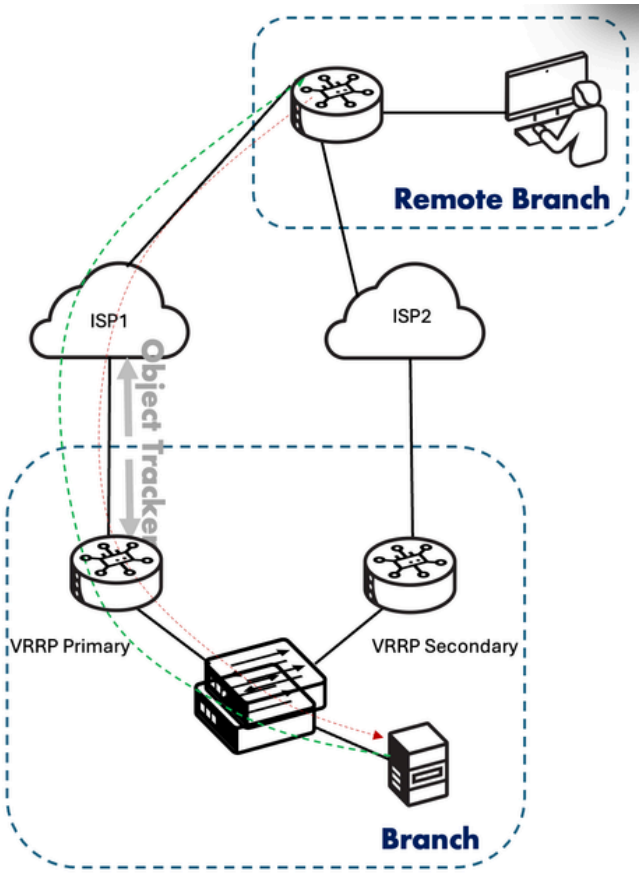
Hay varios casos prácticos basados en los criterios requeridos para implementar el seguimiento de interfaz basado en VRRP. Actualmente, los dos modos admitidos son (i) interfaz (es decir, cualquier interfaz de túnel que esté vinculada a un TLOC local) o (ii) interfaz SIG (relacionada con interfaces de túnel SIG). En cada caso, la parte de la que se realiza el seguimiento es el protocolo de línea de interfaz.

Router dual con Internet: El objeto de seguimiento está enlazado al grupo VRRP. En caso de que el objeto del rastreador (que en este caso es la interfaz de túnel SIG) deje de funcionar, esto notifica al router primario VRRP que active la transición de estado del primario al de respaldo y al router de respaldo que pase a ser primario. Este cambio de estado se puede influir o desencadenar a través de dos tipos de operaciones:

1. Reducción: Donde la prioridad VRRP para la interfaz en la que se configura VRRP VIP se reduce o disminuye con un determinado valor, en el caso de que el estado del objeto de seguimiento pase de ARRIBA a ABAJO.
2. Apagado: Este es un método donde el proceso VRRP se apaga en la interfaz aplicada, en el caso de que el estado del objeto de seguimiento pase de ARRIBA a ABAJO. Este método no se recomienda en los casos prácticos en los que hay casos de reenvío asimétrico.

Preferencias de cambio de TLOC: para evitar que el tráfico asimétrico provenga de otros sitios SDWAN hacia el sitio donde se ejecuta VRRP en la VPN de servicio, la preferencia de TLOC del router primario VRRP se incrementa en 1 si se configura. Incluso puede modificar este valor en grupos de configuración. Esto garantiza que el tráfico de WAN a LAN sea atraído por el propio router primario VRRP. El tráfico de LAN a WAN se ve atraído por el mecanismo VRRP de VRRP principal. Esta función es independiente del rastreador de interfaz VRRP. Este es un comando opcional (tloc-change-pref) desde el punto de vista de la CLI.





Configuración

La configuración de los rastreadores de objetos se realiza a través de plantillas de sistema en la configuración heredada y, posteriormente, adjuntando el rastreador de objetos al grupo VRRP

respectivo bajo la plantilla de la función de interfaz Ethernet de VPN de servicio. En el grupo de configuración, este mecanismo se ha simplificado obteniendo directamente una opción para agregar el rastreador de objetos al perfil de servicio correspondiente del perfil de interfaz Ethernet. A continuación se indican las formas de configurarlo, en función del tipo de método de configuración preferido por el usuario.

- Grupo de configuración Configuration > Configuration Groups > Service Profile > Ethernet Interface > Add Feature > Object Tracker:

1. Proporcione un nombre y una descripción para el nuevo rastreador de objetos que se está definiendo.
2. Seleccione el Tipo de Rastreador (entre Interface y SIG).
3. Asigne un ID de Rastreador de objetos.
4. Proporcione el nombre de la interfaz (en función de la opción elegida en el paso 2).

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

1. En Configuración de IPv4, haga clic en Agregar VRRP IPv4.
2. Defina un ID de grupo VRRP y proporcione una prioridad local para esta interfaz Ethernet del lado del servicio.
3. Proporcione la dirección IP virtual (VIP) de VRRP.
4. Habilite el botón TLOC Preference Change y también proporcione el TLOC Preference Change Value (para manejar el ruteo asimétrico).
5. Haga clic en Agregar Objeto de Seguimiento VRRP.
6. En Asociar Rastreador de Objetos, seleccione en el menú desplegable del Rastreador de Objetos (basado en el nombre) que creó antes
7. Elija una Acción de seguimiento (Apagar o Reducir).
8. Introduzca el valor de disminución (en función de la opción elegida en el paso 7).

- Configuración heredada Configuration > Templates > Feature Templates > System > Tracker section:

1. Haga clic en el botón New Object Tracker.
2. Seleccione el Tipo de Rastreador (entre Interfaz y SIG).
3. Asigne un ID de objeto.
4. Proporcione el nombre de la interfaz (en función de la opción elegida en el paso 2).

- Configuración > Plantillas > Interfaz Ethernet (perteneciente al lado del servicio) > Sección VRRP:

1. Haga clic en el botón New VRRP.
2. Defina un ID de grupo VRRP y proporcione una Prioridad local (se elige un valor opcional predeterminado de 100) para esta interfaz Ethernet del lado del servicio.
3. Proporcione la dirección IP virtual (VIP) de VRRP.
4. Habilite el botón TLOC Preference Change y también proporcione el TLOC Preference Change Value (para manejar el ruteo asimétrico).
5. En Rastreador de objetos, haga clic en Agregar objeto de seguimiento.
6. Ingrese el ID del Rastreador de Objetos (definido en la plantilla del sistema).

7. Elija una Acción de seguimiento (Apagar o Reducir).
8. Introduzca el valor de disminución (en función de la opción elegida en el paso 7).

Desde el punto de vista de la CLI, las configuraciones tienen el siguiente aspecto:

```
(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
!
```

Verificación

Hay dos opciones para verificar los rastreadores de objetos explícitamente configurados para los casos de uso de VRRP.

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

1. En Opciones de dispositivo, escriba "Información VRRP".

2. Active en Grupo VRRP Individual (ID de grupo) y vea las estadísticas del rastreador (Nombre del prefijo de seguimiento, Estado de seguimiento, Tiempo de discontinuidad y Hora del último cambio de estado) en función de los ID del Rastreador de objetos configurados.

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

En el caso de que se detecte un cambio de estado en el rastreador de objetos, el grupo VRRP correspondiente al que está conectado cambia su estado. Los registros respectivos se rellenarían en esta sección (con el nombre como cambio de estado de grupo Vrrp) con detalles como el nombre de host, si el número, el id de grp, el tipo de dirección, si el nombre, el estado de grupo vrrp, el motivo de cambio de estado, y el id de vpn.

En la CLI del extremo:

```
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)
```

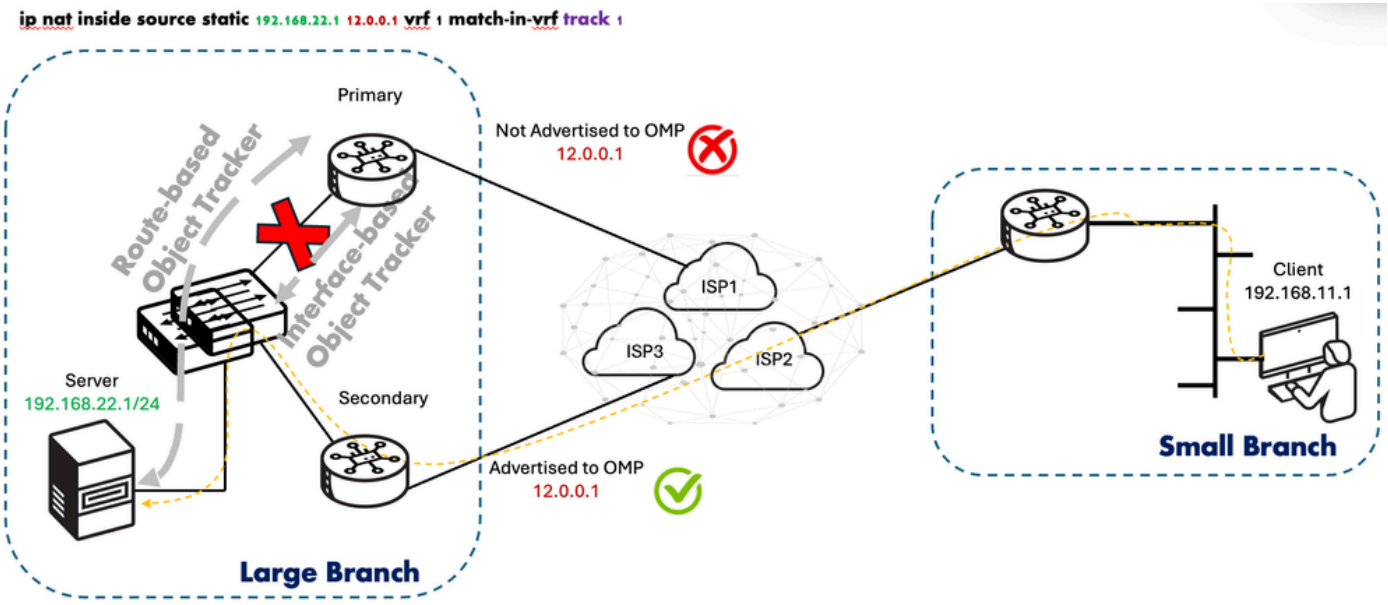
Rastreadores de Objetos de Ruta/Interfaz Utilizados para el Seguimiento de NAT de VPN de Servicio

El rastreador de objetos NAT del lado de servicio fue una función introducida en la versión 20.8/17.8, donde la dirección global interna utilizada en la NAT de servicio-VPN (NAT estática interna y NAT dinámica interna) se anuncia solamente en OMP si (i) se encuentra que la dirección local interna es alcanzable O (ii) el protocolo de línea de la interfaz LAN/del lado de servicio es UP según el rastreador de objetos conectado. Por lo tanto, los tipos de rastreador de objetos que se pueden utilizar son (i) ruta o (ii) interfaz. Dependiendo del estado del prefijo LAN o de la interfaz LAN, los anuncios de ruta NAT a través de OMP se agregan o se eliminan. Puede ver los registros de eventos en Cisco SD-WAN Manager para controlar qué anuncios de ruta NAT se agregan o eliminan.

No hay sondas usadas aquí por el rastreador. En su lugar, utiliza (i) la presencia de una entrada de ruteo en la tabla de ruteo O (ii) el estado del protocolo de línea para decidir el estado del rastreador (activo/inactivo). No hay intervalos de reacción en presencia de una entrada de ruteo o rastreadores basados en el protocolo de línea de interfaz - en el momento en que la entrada de ruteo o el protocolo de línea de interfaz se DESACTIVA, el estado de la pista también se lleva al estado INACTIVO. Inmediatamente, la dirección global interna utilizada en la instrucción NAT asociada con el rastreador de objetos deja de anunciarse en OMP. Para obtener más información sobre los rastreadores NAT de VPN de servicio, visite la guía de configuración.

Casos de uso

Si una interfaz LAN o un prefijo LAN está inactivo, el rastreador de objetos NAT del lado del servicio se desactiva automáticamente. Puede ver los registros de eventos en Administrador SD-WAN de Cisco para supervisar qué anuncios de ruta NAT se agregan o eliminan. En el siguiente caso práctico, se requiere que el cliente acceda al servidor en la sucursal grande. Sin embargo, el problema surge en situaciones en las que se elimina la ruta que apunta al servidor en los bordes de la sucursal grande (en HA) O cuando la interfaz del lado LAN (lado de servicio) deja de funcionar en cualquiera de los bordes de la sucursal grande. En tales situaciones, cuando aplique la NAT del lado del servicio con el rastreador de objetos, asegúrese de que el tráfico entrante del cliente siempre se dirija al borde correcto ubicado en la sucursal grande mediante el control del anuncio de dirección global interna en OMP. En caso de que dicho control no se aplique en el anuncio de ruta en OMP, el tráfico termina quedando en un agujero negro debido a la falta de disponibilidad desde ese borde respectivo al servidor en la sucursal grande.



Configuración

La configuración de los rastreadores de objetos se realiza a través de plantillas de sistema en la configuración heredada y, posteriormente, adjuntando el rastreador de objetos a la instrucción NAT respectiva (dentro de estática o dentro de dinámica) en la plantilla de función de VPN de servicio. En el grupo de configuración, este mecanismo se ha simplificado obteniendo directamente una opción para agregar el rastreador de objetos al perfil de servicio correspondiente del perfil de interfaz Ethernet. A continuación se indican las formas de configurarlo, en función del tipo de método de configuración preferido por el usuario.

- Grupo de configuración Configuration > Configuration Groups > Service Profile > Add Feature > Object Tracker:

1. Proporcione un nombre y una descripción para el nuevo rastreador de objetos que se está definiendo.
2. Seleccione el tipo de rastreador (entre Interface y route).
3. Asigne un ID de Rastreador de objetos.
4. Proporcione el nombre de la interfaz O proporcione la IP de ruta, la máscara IP de ruta y VPN (según la opción elegida en el paso 2).

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

1. Cree un conjunto NAT (obligatorio para activar NAT) haciendo clic en el botón Add NAT Pool.

2. Proporcione los detalles del conjunto NAT, como el nombre del conjunto NAT, la longitud del prefijo, el inicio del rango, el final del rango y la dirección.

3. Muévase a NAT estática en la misma sección y haga clic en el botón Add New Static NAT. (También puede optar por adjuntar el rastreador de objetos a la NAT del grupo dinámico interno).

4. Proporcione los detalles como IP de origen, IP de origen traducida y dirección NAT estática.

5. En el campo Asociar Rastreador de Objetos, seleccione en la lista desplegable el rastreador de

objetos creado anteriormente.

- Configuración heredada Configuration > Templates > Feature Templates > System > Tracker section:

1. Haga clic en el botón New Object Tracker.
2. Seleccione el Tipo de Rastreador (entre Interfaz y Ruta).
3. Asigne un ID de objeto.
4. Proporcione el nombre de interfaz O la IP de ruta, la máscara IP de ruta y VPN (en función de la opción elegida en el paso 2).

- Configuración > Plantillas > Cisco VPN (perteneciente al lado del servicio) > sección NAT:

1. Cree un conjunto NAT (obligatorio para activar NAT) haciendo clic en el botón Nuevo conjunto NAT.

2. Proporcione los detalles del conjunto NAT, como el nombre del conjunto NAT, la longitud del prefijo del conjunto NAT, el inicio del intervalo del conjunto NAT, el final del intervalo del conjunto NAT y la dirección NAT.

3. Muévase a NAT estática en la misma sección y haga clic en el botón New Static NAT. (También puede optar por adjuntar el rastreador de objetos a la NAT del grupo dinámico interno).

4. Proporcione detalles como la dirección IP de origen, la dirección IP de origen traducida y la dirección NAT estática.

5. En el campo Agregar Rastreador de Objetos, escriba el nombre del rastreador de objetos creado anteriormente.

Desde el punto de vista de la CLI, las configuraciones tienen el siguiente aspecto:

```
(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
!
```

La suposición con el caso práctico de NAT es que los usuarios aplican la política de datos para hacer coincidir el tráfico tanto en -> fuera como en -> en los flujos NAT.

Verificación

Hay dos áreas de verificación de los rastreadores de objetos configurados explícitamente para los casos de uso de NAT.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Tiempo real:

1. En Opciones de dispositivo, escriba "Traducción NAT IP".

2. Marque Traducción NAT individual y vea las estadísticas de la entrada (Dirección/puerto local interno, Dirección/puerto global interna, Dirección/puerto local externa, Dirección/puerto global externa, ID de VRF, Nombre de VRF y Protocolo) basándose en sus ID de Rastreador de objetos configurados.

- En el Administrador de SD-WAN: Supervisar > Dispositivos > {select Device-Name} > Eventos:

En el caso de que se detecte un cambio de estado en el rastreador de objetos correspondiente a la ruta NAT que se va a eliminar en OMP, aparecen los eventos denominados "Cambio de ruta NAT", que contienen detalles como el nombre de host, el rastreador de objetos, la dirección, la máscara, el tipo de ruta y la actualización. Aquí, la dirección y la máscara se asignan a la dirección global interna según la configuración de la instrucción NAT estática.

En la CLI del extremo:

```
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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).