Comprendre la convivialité et les exemples d'utilisation de Catalyst SD-WAN Tracker

Table des matières

Introduction

Ce document décrit les réseaux de superposition d'entreprise SD-WAN de Catalyst, la facilité d'utilisation et les cas d'utilisation du traqueur.

Informations générales

Les réseaux d'entreprise superposés SD-WAN Catalyst interagissent généralement avec une grande variété de charges de travail, d'applications et de services externes. tout ce qui peut être situé dans le cloud, le data center/concentrateurs ou les filiales distantes. Le plan de contrôle SD-WAN est responsable de la publicité des routes vers ces services à travers la superposition de manière évolutive. Dans les situations où des applications et des services critiques deviennent inaccessibles le long d'un chemin spécifique, les opérateurs réseau doivent généralement être en mesure de détecter ces événements et de rediriger le trafic utilisateur vers des chemins plus appropriés afin d'éviter un blackholing indéfini du trafic. Pour détecter et corriger ces types de pannes réseau, le plan de contrôle SD-WAN de Catalyst s'appuie sur des pisteurs pour surveiller l'état des services externes et apporter les modifications de routage appropriées.

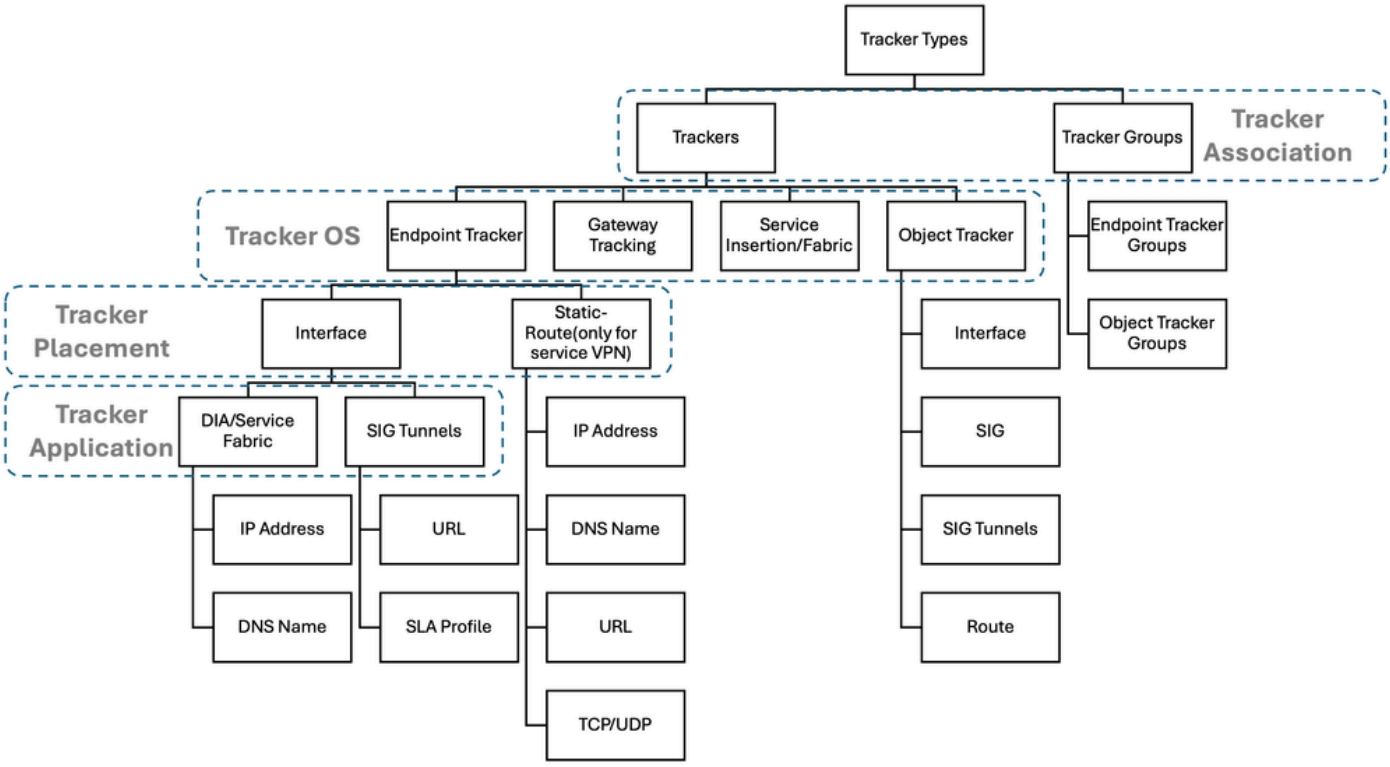
Un dispositif de suivi est un mécanisme de détection d'accessibilité du plan de contrôle qui envoie des paquets de sonde vers un point d'extrémité spécifique et notifie les changements d'état d'accessibilité (haut ou bas) du point d'extrémité aux modules intéressés. Les trackers sont conçus comme une abstraction évolutive de haut niveau de la fonctionnalité native IP SLA de Cisco IOS-XE®, qui peut former une variété de sondes (y compris HTTP, ICMP et DNS). Lorsqu'un tracker notifie un module client d'un changement d'état, ce module peut prendre les mesures appropriées pour empêcher le blocage du trafic, telles que l'installation ou la désinstallation d'une route ou d'un ensemble de routes. Les applications actuelles des trackers dans les solutions SD-WAN et SD-Routing incluent, sans s'y limiter : Suiveurs DIA (Direct Internet Access), suivi SIG (Secure Internet Gateway), suivi de service, suivi de route statique, groupes de suivi, etc.

Pour créer des réseaux à haute disponibilité qui résistent aux pannes de service, il est essentiel de comprendre quand utiliser chaque type de configuration/modèle de suivi. L'objectif de cet article est d'expliquer où et comment chaque type de traqueur est utilisé. Les différents trackers sont abordés ici, ainsi que l'exemple d'utilisation principal de chaque tracker et les workflows de configuration de base pour mettre en oeuvre chaque solution. Enfin, cet article présente une présentation des avertissements généraux concernant les trackers dans Cisco IOS-XE®.

Cet article établit une distinction entre les solutions endpoint-tracker (spécifiques au SD-WAN et au SD-Routing) et object tracker (IOS-XE natif), qui traitent de différents cas d'utilisation.

Types de traqueurs

Ce tableau présente brièvement tous les types de trackers disponibles dans la solution Cisco Catalyst SD-WAN :



Le tableau précédent présente quatre domaines dans lesquels les trackers peuvent être classés : Tracker Association, Tracker OS, Tracker Placement et Tracker Application. La section suivante décrit chaque classification :

1. Association de suivi : Cette classification décrit si un tracker est un tracker unique ou un tracker group. Cisco Catalyst SD-WAN prend en charge l'utilisation de plusieurs trackers dans un groupe (jusqu'à 2 à ce moment de l'écriture) et l'état global du groupe de trackers est déterminé par un opérateur booléen ET ou OU. Par exemple, un groupe de suivi de point d'extrémité ou un groupe de suivi d'objet.
2. Système d'exploitation Tracker : Cette classification décrit le système d'exploitation Cisco IOS-XE® ou le mode dans lequel le tracker est pris en charge. Les routeurs Cisco Catalyst IOS-XE prennent en charge deux modes de fonctionnement :

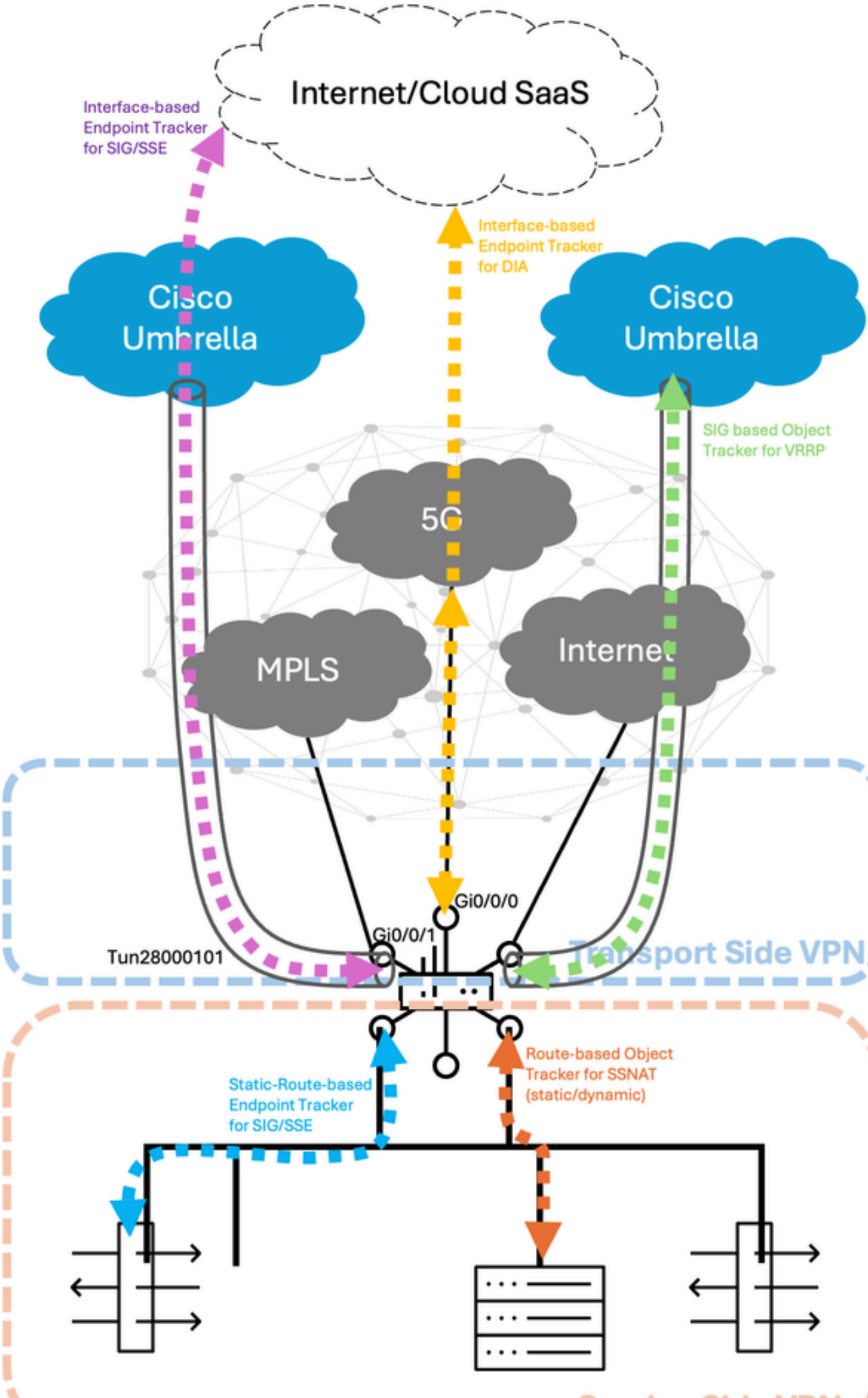
- Mode autonome et
- Mode contrôleur.

Toutes les fonctionnalités de suivi des terminaux et des passerelles sont destinées aux cas d'utilisation en mode contrôleur (SD-WAN), tandis que le suivi des objets est destiné aux cas d'utilisation en mode autonome (SD-Routing).

3. Emplacement du traqueur : Cette classification décrit l'emplacement dans lequel le dispositif de suivi est configuré. Actuellement, Cisco Catalyst SD-WAN prend en charge l'application de trackers sur les interfaces, les routes statiques ou les services.

4. Application de suivi : Cette classification décrit les cas d'utilisation et les fonctionnalités de haut niveau pris en charge par Cisco Catalyst SD-WAN. Bien qu'il existe de nombreux domaines d'application des trackers, quelques-uns d'entre eux incluent : Accès direct à Internet (DIA), passerelle Internet sécurisée (SIG), Secure Service Edge (SSE), suivi VPN côté service, etc.

Voici une représentation visuelle du trafic d'analyse de suivi sur les VPN de service/transport pour plusieurs cas d'utilisation sur une périphérie SD-WAN Cisco Catalyst (qui peut également être appelée cEdge ou 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

configurées sur les plates-formes de périphérie SD-WAN sur le VPN côté transport. Par défaut, cette option est activée dans les configurations de profil système de base (Track Default Gateway) sous Catalyst SD-WAN Manager. Cela permet de surveiller en permanence l'adresse de tronçon suivant spécifiée sous chaque route statique par défaut dans le VPN de transport, afin de garantir le basculement de liaison/route, en cas d'échec d'accessibilité au tronçon suivant (qui est également appelé passerelle, d'où le nom de suivi de passerelle). Pour en savoir plus sur le suivi de passerelle, consultez le guide de configuration.

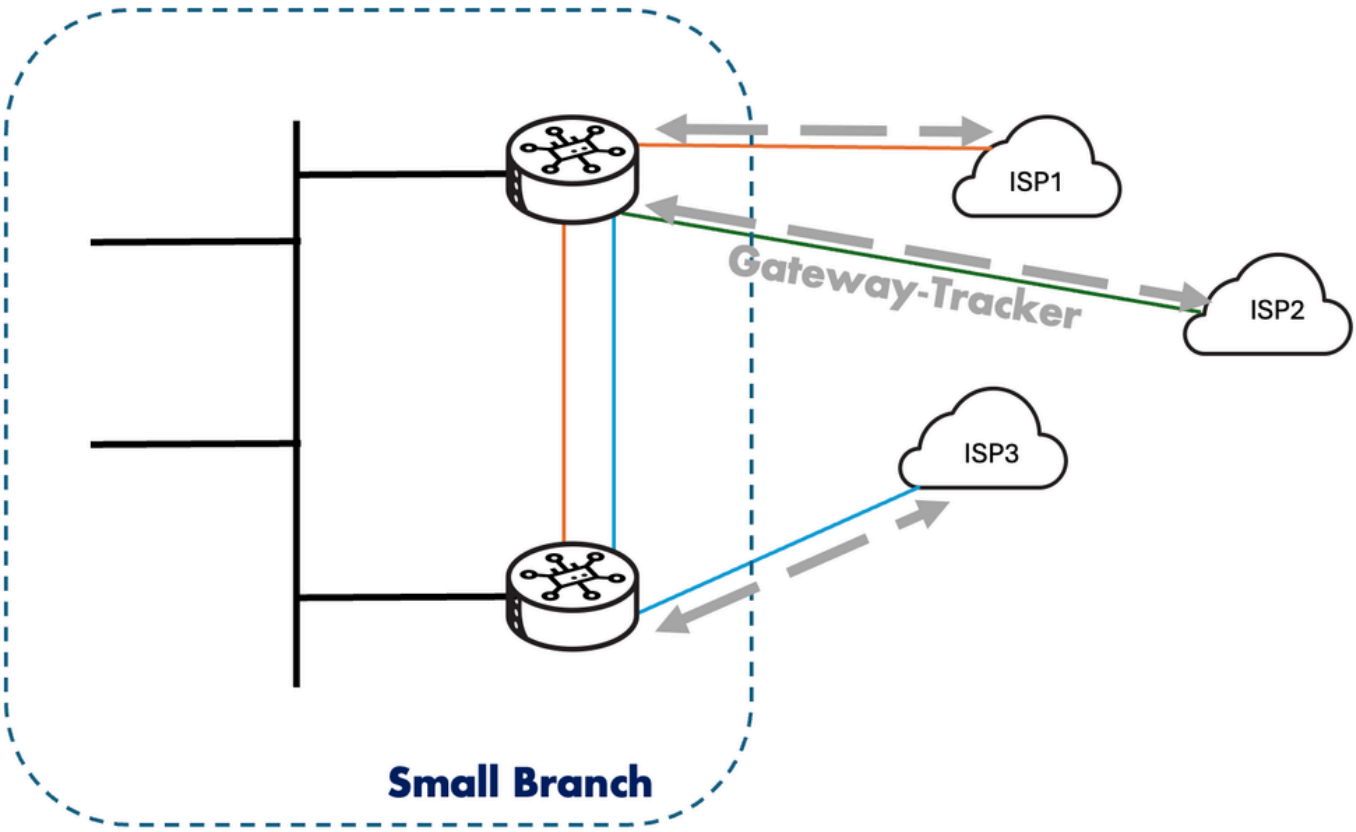
Les types de sondes utilisés ici sont des paquets inondés de type requête ARP-unknown-unicast. Les intervalles utilisés sont les suivants :

- Bonjour : 10 secondes
- Durée de conservation : 100 secondes
- Type de paquet/sonde : ARP

Outre le suivi de passerelle, il est également utilisé pour le suivi de transport sur les bords SD-WAN afin de vérifier le chemin routé entre le périphérique local et un validateur SD-WAN Cisco Catalyst. Pour ce faire, utilisez des sondes ICMP à intervalles réguliers de 3 secondes. Elle est configurée à l'aide du mot clé « track-transport » dans le mode de configuration du système SD-WAN. Cela facilite la surveillance régulière de la connexion DTLS au Cisco Catalyst SD-WAN Validator à partir de la périphérie WAN respective. Pour en savoir plus sur le suivi du transport, consultez le guide de configuration.

Scénarios :

Le suivi de passerelle est une fonctionnalité qui est implicitement configurée par défaut sur SD-WAN pour toutes les routes statiques par défaut qui appartiennent au VPN de transport ou à la table de routage globale (GRT). L'utilisation de la fonctionnalité ne provient pas toujours du point de vue de la configuration du modèle du gestionnaire, mais peut également évoluer à partir des routes statiques par défaut reçues/acquises dans les scénarios d'utilisation d'un serveur DHCP avec les options #3, #81 et ainsi de suite.



Configuration

Appliqué par défaut dans Cisco Catalyst SD-WAN :

```
!
system


 track-transport
 track-default-gateway


!
```

Vérification

Voici quelques façons de vérifier ceci selon la configuration et le groupe de configuration hérités :

- Groupe de configuration: Configuration > Configuration Groups > System profile > Basic sub-profile > Track Settings section > Track Default Gateway (par défaut : ON)
- Configuration héritée : Configuration > Templates > Feature Templates > System template > Advanced section > Gateway Tracking (par défaut : ON)

Service Insertion 1.0 et suivi de Service Fabric 2.0

Le suivi d'insertion de service 1.0 a été introduit dans la version 20.3/17.3 et est une fonctionnalité visant à garantir que l'adresse de service (ou adresse de transfert) est accessible ou disponible. Ces informations permettent à la périphérie d'ajouter ou de retirer dynamiquement des informations de tronçon suivant de la politique de contrôle/données. Avec la configuration de Service Insertion 1.0, le tracker (ou adresse de suivi) est activé par défaut vers l'adresse de service. Sur cette base, l'adresse de transfert et l'adresse de service sont les mêmes dans 1.0. Même si les suiveurs de service sont automatiquement configurés avec des services, ces suiveurs peuvent être désactivés à l'aide de la commande no track-enable, ou en désactivant le bouton de suivi dans la configuration du groupe de configuration/héritée. Étant donné qu'il s'agit des deux seules opérations possibles (activer/désactiver) avec des trackers associés à des services sous Service Insertion 1.0, il n'y a aucun autre paramètre qui peut être modifié (tel que seuil, multiplicateur, intervalle). Le type de sondes utilisé ici est un paquet de requête d'écho ICMP.

Pour en savoir plus sur le suivi de l'insertion de service 1.0, consultez le guide de configuration. Les intervalles par défaut utilisés dans le suivi de l'insertion de service 1.0 sont les suivants :

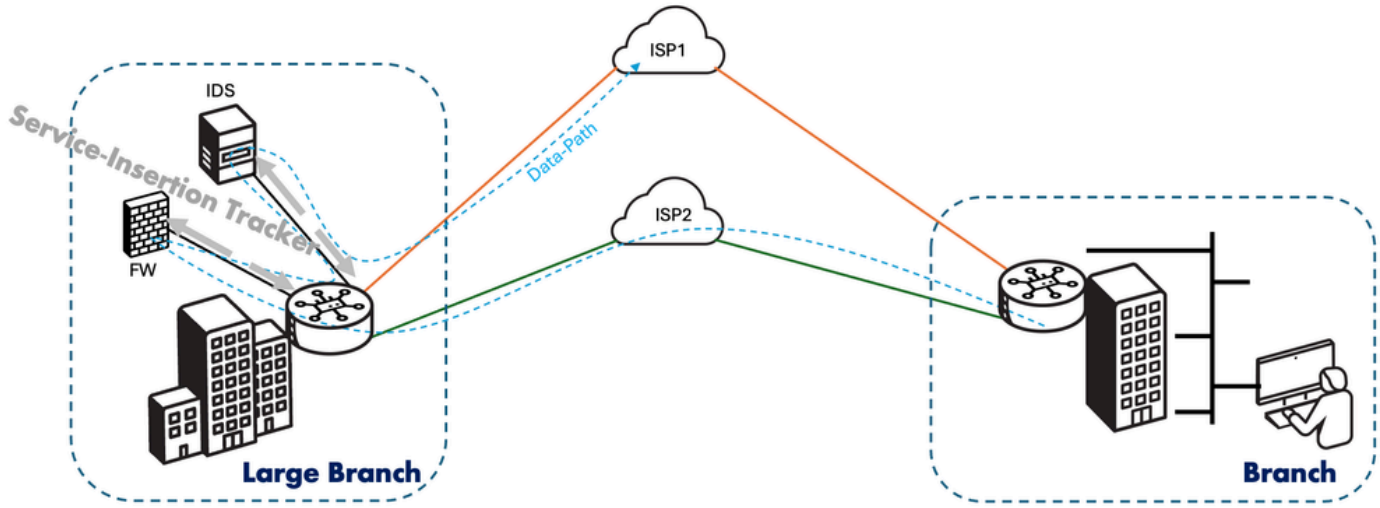
- Intervalle de sondage : 5 sondes toutes les 60 secondes
- Multiplicateur : 5 fois
- Type de paquet/sonde : Écho/réponse d'écho ICMP

Le suivi de Service Fabric 2.0 fait partie de l'offre de fonctionnalités Service Insertion 2.0 dans Cisco Catalyst SD-WAN introduite à partir de la version 20.13/17.13. Dans cette nouvelle variante de l'insertion de service, la méthode par défaut utilisée par les profils et les modèles de configuration est toujours d'avoir un traqueur implicite pointant vers chaque adresse de service définie (ou adresse de transfert) dans une paire service-HA par interface rx/tx. Toutefois, avec Service Fabric 2.0, vous pouvez désormais séparer l'adresse de transfert de l'adresse de suivi. Pour ce faire, il suffit de définir des traqueurs de point d'extrémité distincts pour suivre une adresse de point d'extrémité différente de l'adresse de service elle-même. Cette rubrique est développée plus en détail dans les sections suivantes.

Scénarios :

Le cas d'utilisation principal des services trackers est la surveillance évolutive de l'accessibilité des services, en particulier pour le chaînage de services. Le chaînage de services peut être déployé sur un réseau constitué de plusieurs VPN, chaque VPN représentant une fonction ou une organisation différente, afin de garantir que le trafic entre les VPN passe par un pare-feu. Par exemple, dans un réseau de campus de grande taille, le trafic interservice peut passer par un pare-feu, tandis que le trafic intraderparental peut être acheminé directement. Le chaînage de services peut être observé dans des scénarios où un opérateur doit se conformer à la

réglementation, tels que la norme PCI DSS (Payment Card Industry Data Security Standard), où le trafic PCI doit traverser des pare-feu dans un data center centralisé ou un concentrateur régional :



Configuration

Les configurations sont identiques au workflow normal de configuration de Service Insertion 1.0 sur SD-WAN. Les suiveurs Service Insertion 1.0 sont activés par défaut sur toutes les adresses de service.

- Groupe de configuration: Configuration > Configuration Groups > Service Profile > Service VPN > Service section :

1. Cliquez sur le bouton Ajouter un service.

2. Choisissez un type de service.

3. Inscrivez l'adresse du service (4 max. possibles, séparés par une virgule).

4. Vérifiez que le bouton Suivi est activé (par défaut). Cette option peut être désactivée, si nécessaire.

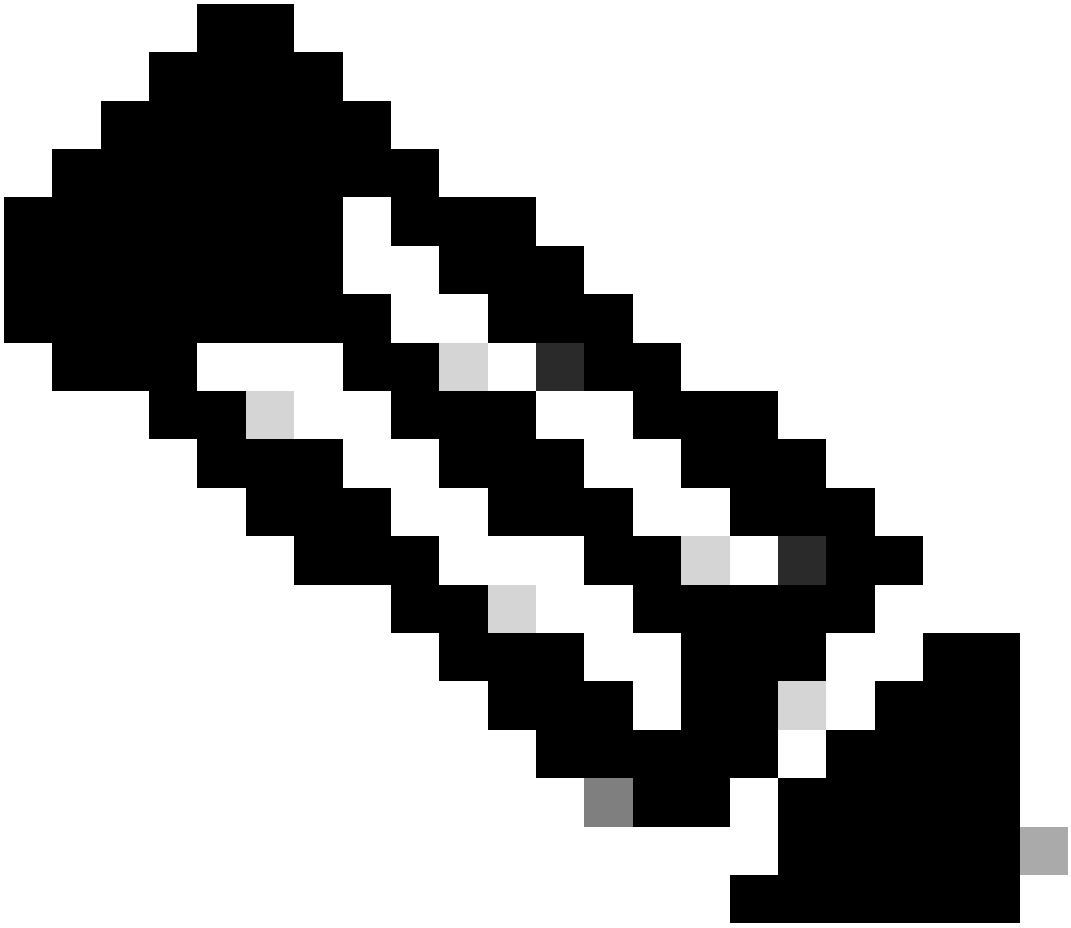
- Configuration héritée : Configuration > Templates > Feature Templates > Cisco VPN (service) > Service section :

1. Cliquez sur le bouton Nouveau service

2. Choisissez un type de service.

3. Inscrivez l'adresse du service (4 max. possibles, séparés par une virgule).

4. Vérifiez que le bouton Suivi est activé (par défaut). Cette option peut être désactivée, si nécessaire.



Remarque : Au moment où l'étape 3 est configurée (à partir du groupe de configuration ou de la configuration héritée), le traqueur est automatiquement initié aux différentes adresses de service définies

Du point de vue de l'interface de ligne de commande, la configuration de Service Insertion 1.0 apparaît comme suit :

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

Vérification

Les étapes de vérification s'étendent aux étapes similaires suivies dans le cadre des dispositifs de suivi des points d'extrémité basés sur l'interface utilisés dans les sections précédentes.

Il existe deux options de vérification du dispositif de suivi des terminaux explicitement configuré.

- Sur le gestionnaire SD-WAN : Monitor > Devices > {select Device-Name} > Applications > Tracker :

Cochez la case Individual Tracker et affichez les statistiques du tracker (Tracker Types, Status, Endpoint, Endpoint Type, VPN Index, Host Name, Round Trip Time) en fonction de votre Tracker Name configuré.

- Sur le gestionnaire SD-WAN : Monitor > Devices > {select Device-Name} > Events :

Dans le cas où des failles sont détectées sur le tracker, les journaux respectifs renseignent dans cette section avec des détails tels que le nom d'hôte, le nom du point d'attachement, le nom du tracker, le nouvel état, la famille d'adresses et l'id de vpn.

Sur l'interface de ligne de commande de la périphérie :

```
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 utilisée pour DIA

Les trackers NAT DIA Endpoint Trackers sont principalement conçus pour surveiller l'accessibilité des applications via une interface NAT DIA sur les plates-formes SD-WAN Edge.

Pour les cas d'utilisation DIA (Direct Internet Access), les traqueurs NAT DIA sont principalement utilisés pour suivre l'interface côté transport et déclencher un basculement vers une autre interface côté transport disponible ou via des tunnels de superposition SD-WAN (à l'aide de la politique de données). Cette fonctionnalité a été introduite à partir de la version 20.3/17.3, et NAT fallback feature-option est disponible à partir de la version 20.4/17.4. Si le traqueur détermine que l'Internet

local n'est pas disponible via l'interface NAT DIA, le routeur retire la route NAT du VPN de service et réachemine le trafic en fonction de la configuration de routage local. Le traqueur continue de vérifier régulièrement l'état du chemin vers l'interface. Lorsqu'il détecte que le chemin fonctionne à nouveau, le routeur réinstalle la route NAT vers Internet. Pour en savoir plus sur les traqueurs DIA, consultez le guide de configuration.

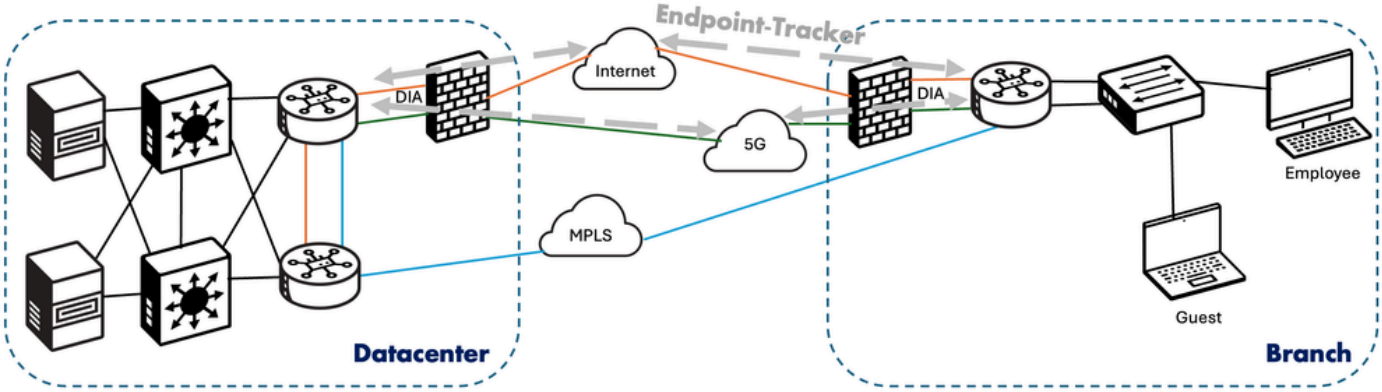
Dans la définition du traqueur, vous pouvez choisir de donner une adresse IP d'un terminal accessible via l'interface NAT DIA (configurée comme « endpoint-ip ») OU de fournir un nom de domaine complet (FQDN) au terminal (configuré comme « endpoint-dns-name »).

Le type de sonde utilisé ici est un paquet de requête HTTP, très similaire à une pile de PDU de requête d'API HTTP. Les intervalles utilisés sont les suivants :

- Intervalle de sondage : 60 secondes
- Multiplicateur : 180 secondes (puisque #retries est 3 = 3 x 60 secondes)
- Type de paquet/sonde : HTTP

Scénarios :

L'architecture DIA est souvent déployée en tant qu'optimisation sur les sites des filiales afin d'éviter le réacheminement vers un data center de tout trafic des filiales destiné à Internet. Néanmoins, lorsque le DIA dans les sites d'agence est utilisé, tout manque d'accessibilité le long des routes DIA NAT doit toujours revenir à des chemins alternatifs pour éviter la mise en attente et la perte de service. Pour les sites qui souhaitent utiliser la reprise sur le data center (via la superposition SD-WAN à l'aide de la reprise NAT) en cas de panne locale de l'interface DIA. Tirez parti de ces dispositifs de suivi des points d'extrémité basés sur les interfaces compatibles DIA sur les bords côté filiale pour détecter les défaillances afin de lancer un basculement vers le chemin de sauvegarde/DC. De cette manière, la haute disponibilité du service Internet est obtenue avec un minimum d'interruption dans l'entreprise tout en optimisant le trafic Internet avec DIA :



Configuration

Ces dispositifs de suivi des terminaux basés sur l'interface doivent être configurés manuellement pour activer cet ensemble de fonctionnalités. Voici comment le configurer, selon le type de méthode de configuration préféré par l'utilisateur.

- Groupe de configuration: Configuration > Configuration Groups > Transport & Management

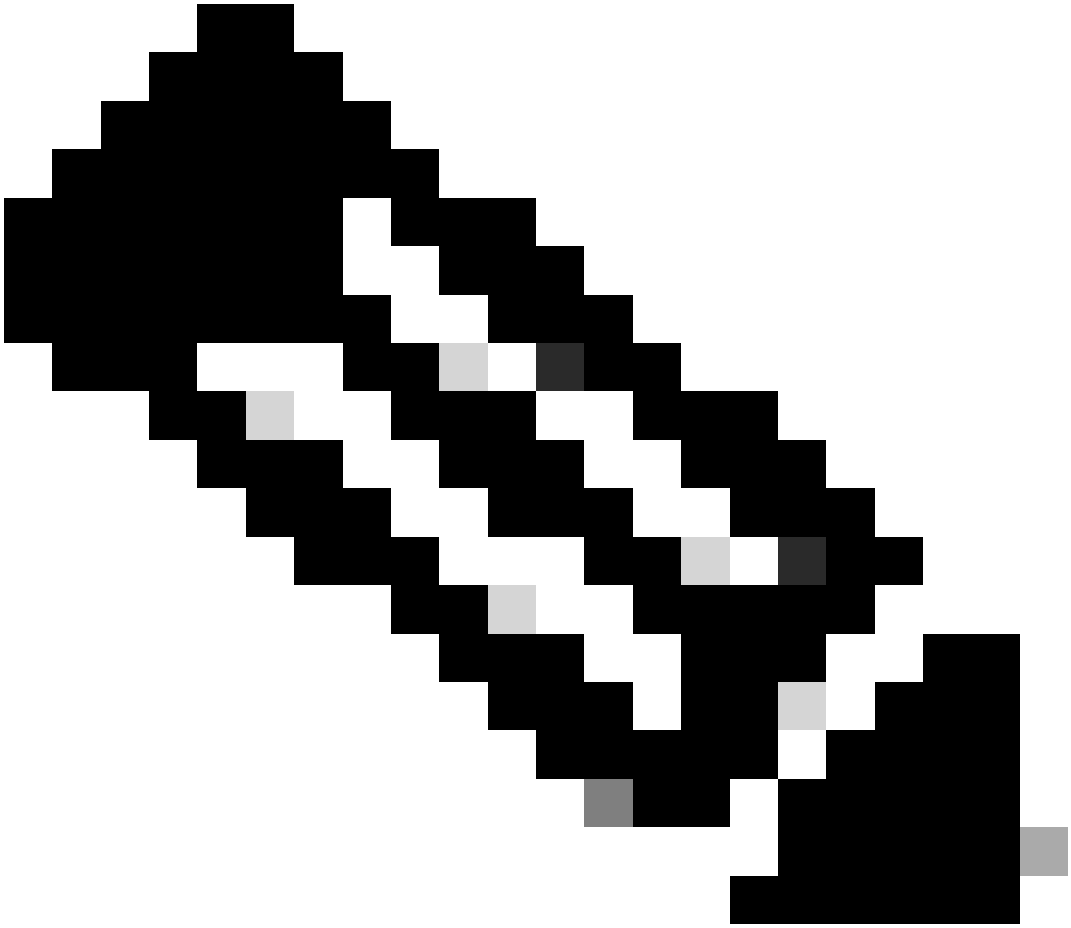
Profile > Ethernet Interface > Add Feature > Tracker :

1. Définissez un nom de suivi de point de terminaison.

2. Choisissez un type de suivi de point de terminaison (entre HTTP-default et ICMP).

Remarque: Le type de suivi des terminaux ICMP a été introduit à partir de la version 20.13/17.13.

3. Sélectionnez le point de terminaison (entre Endpoint IP-default et Endpoint DNS Name).



Remarque : Si le nom DNS du point de terminaison est choisi, assurez-vous qu'un serveur DNS ou un serveur de noms valide est défini sous le VPN/VRF de transport à l'aide du profil de configuration VPN de transport.

---

4. Entrez l'adresse ou le nom DNS (FQDN) vers lequel les sondes de suivi doivent être envoyées (le format dépend de l'étape précédente).

5. (Facultatif) Vous pouvez choisir de modifier l'intervalle de détection (par défaut = 60 secondes)

et le nombre de tentatives (par défaut = 3 fois) pour fixer le délai de détection de l'échec.

- Configuration héritée :

Étape 1. Définition de l'outil Interface-Based Endpoint Tracker : Configuration > Templates > Feature Templates > System template > Tracker section :

1. Sous la sous-section Trackers, sélectionnez le bouton New Endpoint Tracker.

2. Définissez un nom de suivi de point de terminaison.

3. Choisissez le type de suivi (entre interface-default et static-route) comme interface, puisque les cas d'utilisation DIA sont préoccupants ici.

4. Choisissez le type de point de terminaison (entre Adresse IP par défaut et Nom DNS).

5. Entrez l'adresse IP ou le nom DNS du point de terminaison vers lequel les analyseurs doivent être envoyés (le format dépend de l'étape précédente).

6. (Facultatif) Vous pouvez choisir de modifier le seuil d'analyse (par défaut = 300 ms), l'intervalle (par défaut = 60 secondes) et le multiplicateur (par défaut = 3 fois).

Étape 2. Appliquez le dispositif de suivi des points d'extrémité basés sur l'interface à une interface sur le VPN de transport : Modèles > Modèles de fonctionnalités > Interface VPN Cisco Ethernet > section Avancée :

1. Entrez le nom du dispositif de suivi des terminaux défini à l'étape 1 précédente dans le champ Dispositif de suivi.

Du point de vue de l'interface de ligne de commande, les configurations sont les suivantes :

```
(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
!
```

Vérification

Il existe deux options de vérification pour les trackers de point d'extrémité configurés explicitement.

- Sur le gestionnaire SD-WAN : Monitor > Devices > {select Device-Name} > Applications > Tracker :

Cochez la case Individual Tracker et affichez les statistiques du tracker (Tracker Types, Status, Endpoint, Endpoint Type, VPN Index, Host Name, Round Trip Time) en fonction de votre Tracker Name configuré.

- Sur le gestionnaire SD-WAN : Monitor > Devices > {select Device-Name} > Events :

Dans le cas où des failles sont détectées sur le tracker, les journaux respectifs renseignent dans cette section avec des détails tels que le nom d'hôte, le nom du point d'attachement, le nom du tracker, le nouvel état, la famille d'adresses et l'id de vpn.

Sur l'interface de ligne de commande de la périphérie :

```
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
```

Interface Endpoint Trackers utilisée pour les tunnels SIG/SSE

Lorsque des dispositifs de suivi de terminaux sont utilisés pour des cas d'utilisation de tunnel SIG/SSE, cela indique principalement que l'entreprise recherche une pile de sécurité basée sur le cloud qui est facilement disponible de nos jours à l'aide de fournisseurs de passerelle Internet sécurisée (SIG) ou de périphérie de service sécurisée (SSE), tels que Cisco, Cloudflare, Netskope, ZScalar, etc. Les tunnels SIG et SSE font tous deux partie du modèle de déploiement de la sécurité cloud, dans lequel la filiale utilise le cloud pour fournir les solutions de sécurité nécessaires dont elle a besoin. L'exemple d'utilisation des tunnels SIG était l'offre initiale d'intégration de Cisco Catalyst SD-WAN avec ces fournisseurs SIG (à partir de la version 20.4/17.4), mais avec l'évolution des offres de sécurité fournies dans le cloud, l'exemple d'utilisation SSE a été introduit (à partir de la version 20.13/17.13) pour couvrir les cas d'utilisation avec des fournisseurs tels que Cisco (via Cisco Secure Access) et ZScalar.

L'IT nécessite une approche fiable et explicite pour protéger et se connecter avec agilité. Il est désormais courant de fournir aux employés distants un accès direct aux applications cloud, telles que Microsoft 365 et Salesforce, avec une sécurité supplémentaire. La demande en matière de sécurité et de mise en réseau dans le cloud s'accroît chaque jour, car les sous-traitants, les partenaires, les périphériques IoT (Internet of Things), etc. ont besoin d'un accès réseau. La convergence des fonctions de réseau et de sécurité plus près des périphériques finaux, à la périphérie du cloud, est connue sous le nom de modèle de service Cisco SASE. Cisco SASE combine des fonctions de mise en réseau et de sécurité fournies dans le cloud pour fournir un accès sécurisé aux applications pour tous les utilisateurs ou périphériques, en tout lieu et à tout moment. Secure Service Edge (SSE) est une approche de sécurité réseau qui aide les organisations à améliorer la sécurité de leur environnement de travail tout en réduisant la complexité pour les utilisateurs finaux et les services informatiques. Pour en savoir plus sur les trackers de tunnel SIG/SSE, consultez le guide de configuration.

Scénarios :

De tels dispositifs de suivi de points d'extrémité basés sur une interface sont utilisés dans de tels cas d'utilisation de tunnel SIG/SSE, dans lesquels vous souhaitez effectuer le suivi d'un point d'extrémité d'URL d'application SaaS bien connu ou d'un point d'extrémité d'URL spécifique préoccupant. Aujourd'hui, SSE est le scénario le plus couramment utilisé depuis que l'architecture SASE a été scindée en fonctionnalités de base SSE et fonctionnalités SD-WAN. Vous souhaitez ensuite choisir entre les rôles actif et en veille au sein des tunnels IPSec créés à partir d'un site (dans ce cas, le DC). L'utilisateur a le choix d'attacher le traqueur sous l'interface de tunnel respective.

Dans le cas des fournisseurs SSE, tels que Cisco Secure Access (by Cisco), un dispositif de suivi implicite des terminaux est utilisé et configuré par défaut. Cependant, l'utilisateur a le choix de créer un dispositif de suivi de point d'extrémité personnalisé et de le connecter à l'interface du tunnel IPSec. Les paramètres du dispositif de suivi de point de terminaison implicite/par défaut

utilisés dans SSE sont les suivants :

Pour Cisco SSE :

Nom du suivi : DefaultTracker

Point de terminaison suivi : http://service.sig.umbrella.com

Type de terminal : URL_API

Seuil : 300 ms

Multiplier : 3

Intervalle : 60 sec

Pour ZScaler SSE :

Nom du suivi : DefaultTracker

Point de terminaison suivi : http://gateway.zscalerthree.net/vpnte

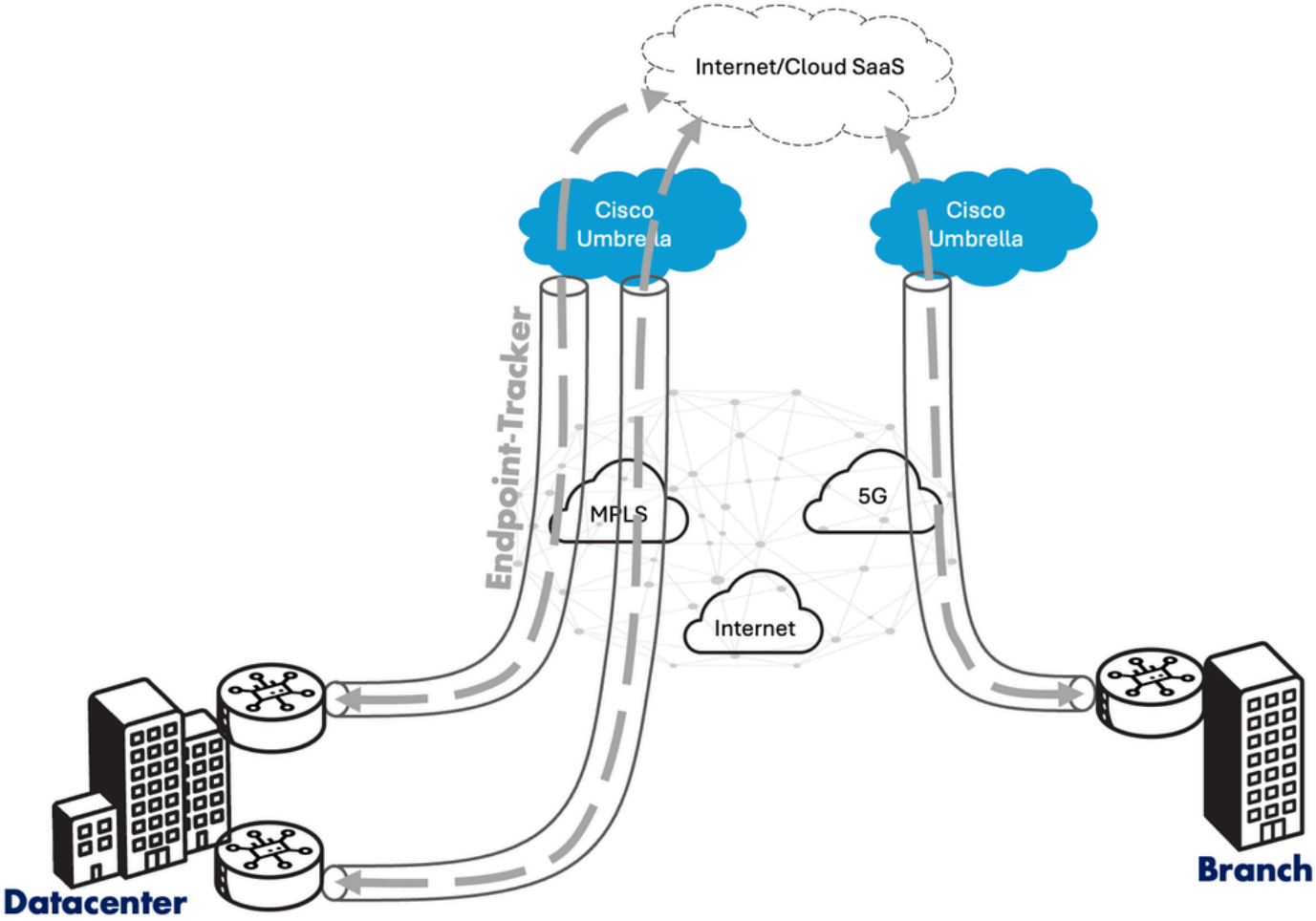
Type de terminal : URL_API

Seuil : 300 ms

Multiplicateur : 3

Intervalle : 60 sec

Dans le cas des tunnels SIG, aucun tracker de point d'extrémité implicite/par défaut n'est défini. Par conséquent, l'utilisateur doit configurer manuellement un dispositif de suivi des terminaux basé sur l'interface s'il souhaite suivre l'interface du tunnel IPSec vers le cloud fournisseur SIG :



Configuration

Dans le cas des fournisseurs SSE, l'utilisateur n'a pas à définir explicitement un tracker de point d'extrémité (sauf si désiré). Cependant, les workflows sont différents en fonction du type de configuration.

Comme condition préalable, vous devez définir les informations d'identification SIG/SSE Administration > Settings > External Services > Cloud Credentials :

1. Sous Cloud Provider Credentials, activez l'option Umbrella ou Cisco SSE (ou les deux).

2. Définissez les paramètres, tels que l'ID de l'organisation, la clé API, le secret).

Définissez le groupe de configuration Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge :

1. Cliquez sur Add Secure Internet Gateway ou sur Add Secure Service Edge.

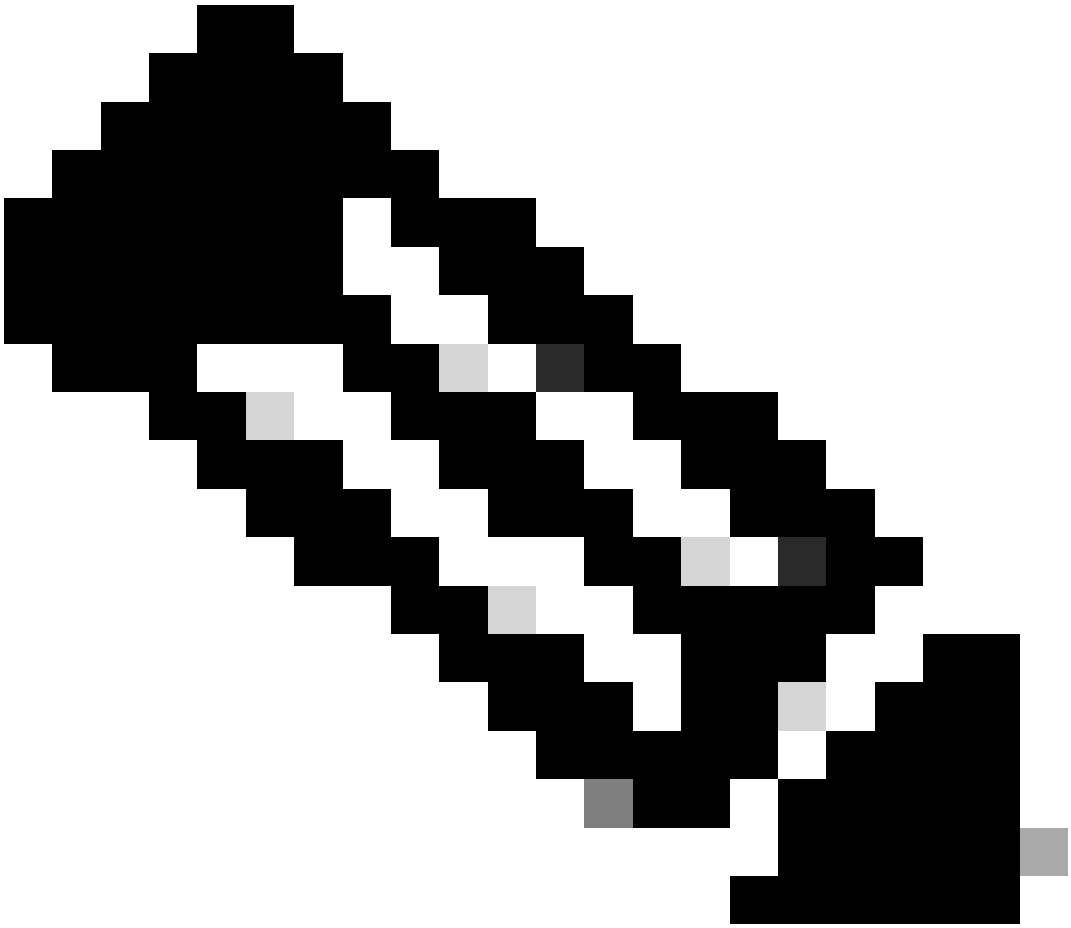
2. Définissez un nom et une description.

3. Sélectionnez l'un des boutons radio sous SIG/SSE Provider (Umbrella ou Cisco SSE).

4. Dans la section Tracker, définissez l'adresse IP source utilisée pour fournir les sondes de suivi.

5. Si vous choisissez de définir un suivi de point de terminaison explicite/personnalisé, cliquez sur Ajouter un suivi, puis renseignez les paramètres du suivi de point de terminaison (Nom, URL API du point de terminaison, Seuil, Intervalle d'analyse et Multiplicateur).

6. Dans la section Configuration, créez les interfaces de tunnel dans lesquelles vous pouvez définir les paramètres (tels que le nom de l'interface, la description, le traqueur, l'interface source du tunnel, le data center principal/secondaire).



> Remarque : À l'étape 6, l'utilisateur a la possibilité d'attacher le dispositif de suivi de point d'extrémité défini au tunnel IPSec correspondant. Veuillez noter qu'il s'agit d'un champ facultatif.

---

7. Dans la section Haute disponibilité, créez une paire d'interfaces et définissez votre interface active et votre interface de sauvegarde avec leurs pondérations respectives. Appliquez ensuite le groupe de stratégies configuré précédent aux arêtes appropriées.

Définir la configuration héritée Configuration > Modèles > Modèles de fonctionnalités > Modèle de

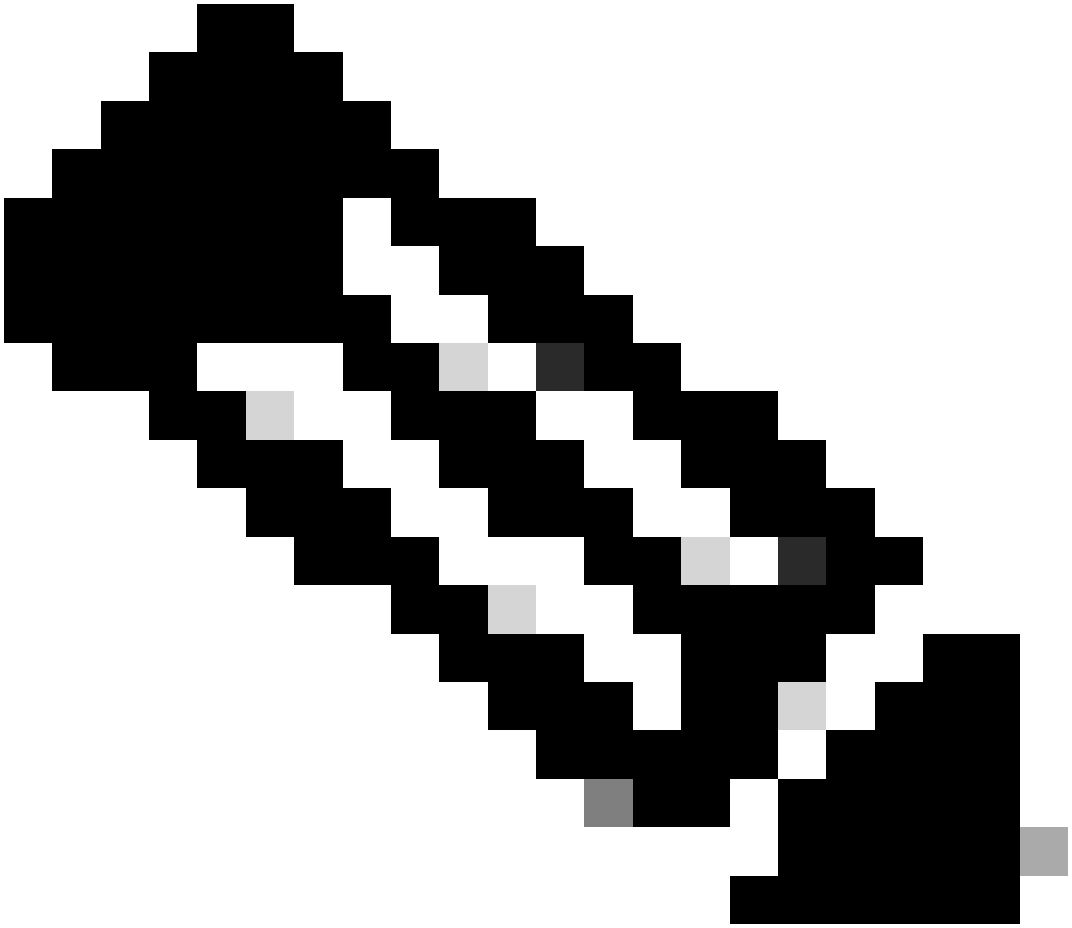
fonctionnalité Cisco Secure Internet Gateway :

1. Sélectionnez l'une des cases d'option sous SIG Provider (Umbrella, ZScalar ou Generic).

2. Dans la section Tracker (BETA), définissez l'adresse IP source utilisée pour fournir les sondes de suivi.

5. Si vous choisissez de définir un suivi de point de terminaison explicite/personnalisé, cliquez sur Nouveau suivi et renseignez les paramètres du suivi de point de terminaison (Nom, URL API du point de terminaison, Seuil, Intervalle et Multiplicateur).

6. Dans la section Configuration, créez les interfaces de tunnel (en cliquant sur Add Tunnel) dans lesquelles vous pouvez définir les paramètres (tels que le nom de l'interface, la description, le suivi, l'interface source du tunnel, le data center principal/secondaire).



Remarque : À l'étape 6, l'utilisateur a la possibilité d'attacher le dispositif de suivi de point d'extrémité défini au tunnel IPSec correspondant. Veuillez noter qu'il s'agit d'un champ facultatif.

---

7. Dans la section Haute disponibilité, définissez votre interface active et votre interface de sauvegarde avec leurs pondérations respectives.

Du point de vue de l'interface de ligne de commande, les configurations sont les suivantes :

```
(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
!
```

Vérification

Il existe des options de vérification pour les trackers de terminaux explicitement configurés.

- Sur le gestionnaire SD-WAN : Monitor > Devices > {select Device-Name} > Applications > Tracker :

Cochez la case Individual Tracker et affichez les statistiques du tracker (Tracker Types, Status,

Endpoint, Endpoint Type, VPN Index, Host Name, Round Trip Time) en fonction de votre Tracker Name configuré.

- Sur le gestionnaire SD-WAN : Monitor > Devices > {select Device-Name} > Events :

Dans le cas où des failles sont détectées sur le tracker, les journaux respectifs renseignent dans cette section avec des détails tels que le nom d'hôte, le nom du point d'attachement, le nom du tracker, le nouvel état, la famille d'adresses, et l'id de vpn.

Sur l'interface de ligne de commande de la périphérie :

```
Router#show endpoint-tracker interface Tunnel16000612
Interface                      Record Name            Status          Address Family   RTT in msecs
t Hop
Tunnel16000612               cisco-tracker          Up              IPv4             26              31

Router#show endpoint-tracker interface Tunnel16000101
Interface                      Record Name            Status          Address Family   RTT in msecs
t Hop
Tunnel16000101               DefaultTracker         Up              IPv4             1               10

Router#show endpoint-tracker records
Record Name                    Endpoint                              EndPoint Type Threshold(ms) Mult
s) Tracker-Type
DefaultTracker                 http://gateway.zscalerthree.net/vpnte API_URL       300           3
   interface
cisco-tracker                  http://www.cisco.com                  API_URL       300           3
   interface
```

Interface Endpoint Trackers utilisée pour Service Fabric 2.0

Le suivi de Service Fabric 2.0, introduit dans la version 20.13/17.13, est une variante améliorée du suivi de l'insertion de service 1.0, dans laquelle les utilisateurs ont la possibilité de personnaliser les suivis dans une plus grande mesure. Le comportement par défaut est conservé de la version précédente de Service Insertion (1.0), un tracker serait initié par défaut avec la définition de chaque adresse de service (ou adresse de transfert) dans une paire service-HA par rx/tx. Mais avec Service Insertion 2.0, l'adresse de suivi (IP/point d'extrémité vers le suivi) peut être séparée de l'adresse de transfert (généralement l'adresse de service). Ceci est effectué à l'aide de trackers de points d'extrémité personnalisés définis au niveau VPN. Pour en savoir plus sur les trackers de Service Fabric 2.0, consultez le guide de configuration.

Si l'utilisateur choisit d'utiliser le tracker par défaut, les spécifications des sondes de tracker sont les suivantes :

- Bonjour : 1 sonde toutes les 30 secondes
- Multiplicateur : 3 fois
- Type de paquet/sonde : Écho/réponse d'écho ICMP

Si l'utilisateur choisit d'utiliser un dispositif de suivi personnalisé, les spécifications des sondes de suivi sont les suivantes :

- Bonjour : 1 sonde toutes les 60 secondes
- Multiplicateur : 3 fois
- Type de paquet/sonde : Demande/réponse d’écho ICMP

Scénarios :

Les cas d'utilisation de Service Insertion 1.0 mentionnés dans les sections précédentes s'appliquent également ici.

Configuration

La configuration basée sur le workflow est prise en charge pour Service Insertion 2.0, une approche guidée par un assistant qui simplifie l'expérience utilisateur tout en respectant les étapes de workflow standard du groupe Configuration.

1. Définissez le groupe Chaîne de services - Configuration dans la section Configuration > Insertion de services > Définitions de chaîne de services :

a. Cliquez sur le bouton Ajouter une définition de chaîne de services.

b. Renseignez les détails du Nom et de la Description du Service.

c. Remplissez un format de liste (en sélectionnant dans la liste déroulante), le Type de service.

2. Définissez le groupe Instance de chaîne de service - Configuration dans la section Configuration > Insertion de service > Configurations de chaîne de service :

a. Cliquez sur Ajouter une configuration de chaîne de services.

b. Dans l'étape Définition de la chaîne de services, sélectionnez la case d'option Sélectionner existant, et choisissez le service précédemment défini.

c. Fournissez un nom et une description pour l'étape Start Service Chain Configuration.

d. Dans l'étape Configuration de la chaîne de services pour les services connectés manuellement, sélectionnez l'ID VPN de la chaîne de services.

e. Ensuite, pour chaque service défini dans l'instance de la chaîne de services (représentée dans des sous-onglets), sous les détails du service, indiquez le type de pièce jointe (IPv4, IPv6 ou Tunnel Connected).

f. Cochez la case Avancé. Si vous avez besoin de cas d'utilisation de sauvegarde active/haute disponibilité (activez également le bouton Ajouter des paramètres pour la sauvegarde) ou même si vous devez définir un traqueur de point d'extrémité personnalisé (activez également le bouton de traqueur personnalisé).

g. Si vous avez des scénarios dans lesquels le trafic de sortie (tx) va au service via une interface et le trafic de retour du service est entré (rx) via une autre interface, activez le Trafic du service est reçu sur un bouton d'interface différent.

h. Lorsque les boutons Advanced et Custom Tracker sont activés, définissez l'adresse IPv4 du service (adresse de transfert), l'interface du routeur SD-WAN (à laquelle le service est connecté) et le point d'extrémité du tracker (adresse de suivi). Vous pouvez également modifier les paramètres de suivi personnalisés tels que l'intervalle et le multiplicateur (en cliquant sur le bouton Modifier).

i. Répétez les étapes (e), (f), (g) et (h) pour chaque service défini ultérieurement.

3. Attachez l'instance de chaîne de services au profil de configuration du groupe Périphérie - Configuration sous Configuration > Groupes de configuration > Profil de service > VPN de service > Ajouter une fonctionnalité > Passerelle d'attachement de chaîne de services :

a. Indiquez un nom et une description pour ce colis de la passerelle d'attachement de la chaîne de services.

b. Sélectionnez la définition de chaîne de services précédemment définie (à l'étape 1).

c. Ajoutez à nouveau/vérifiez les détails comme effectué à l'étape 2. Pour la définition du suivi, la seule différence par rapport à l'étape 2 précédente est que vous avez la possibilité de donner un nom de suivi et de sélectionner également le type de suivi (de service-icmp à ipv6-service-icmp).

Du point de vue de l'interface de ligne de commande, les configurations sont les suivantes :

```
!
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
!
```

Vérification

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

Cochez la case Individual Tracker et affichez les statistiques du tracker (Tracker Types, Status, Endpoint, Endpoint Type, VPN Index, Host Name, Round Trip Time) en fonction de votre Tracker

Name configuré.

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

Dans le cas où des failles sont détectées sur le tracker, les journaux respectifs renseignent dans cette section avec des détails tels que le nom d'hôte, le nom du point d'attachement, le nom du tracker, le nouvel état, la famille d'adresses, et l'id de vpn.

Sur l'interface de ligne de commande de la périphérie :

```
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
```

Suiveurs de terminaux de route statique utilisés pour le suivi de

route statique (côté service)

Le deuxième type de trackers de point d'extrémité est appelé trackers de point d'extrémité basés sur la route statique. Comme son nom l'indique, ces types de trackers sont principalement utilisés pour suivre l'adresse de tronçon suivant de toute route statique définie sous le VPN côté service. Par défaut, tous les types de routes « connectées » et « statiques » sont annoncés dans le protocole OMP - post auquel tous les sites distants qui contiennent le VPN de service respectif prennent connaissance de ce préfixe de destination (dans lequel le point de tronçon suivant vers le TLOC du site d'origine). Le site d'origine est le site à partir duquel la route statique spécifique a été initiée.

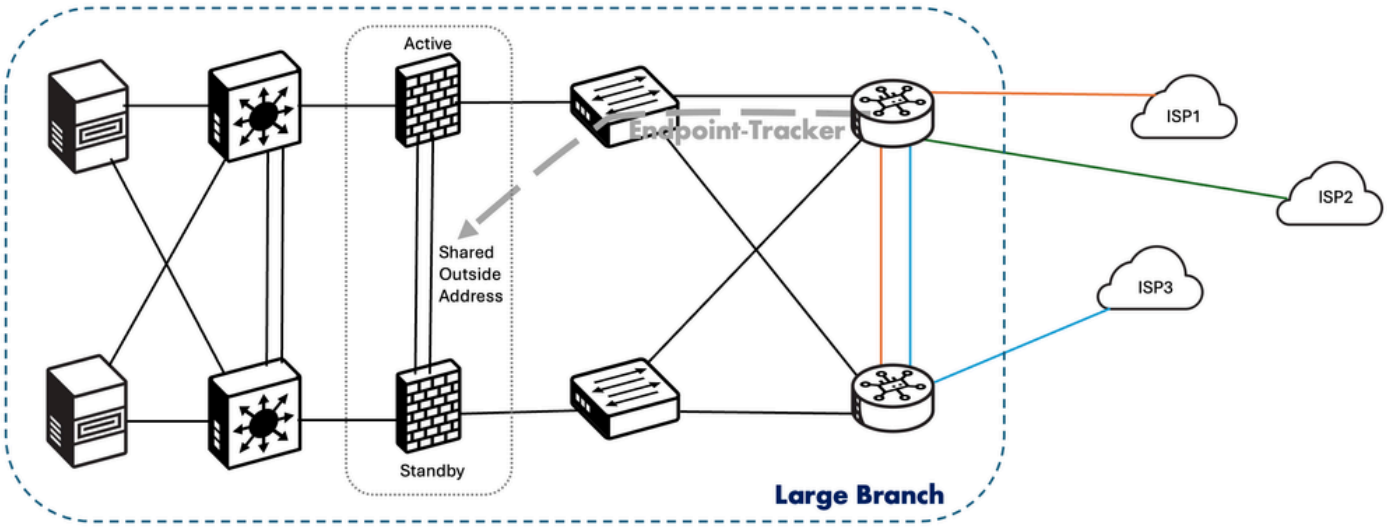
Toutefois, si l'adresse de tronçon suivant de la route statique devient inaccessible, la route n'arrête pas d'être annoncée dans OMP. Cela entraînerait des problèmes de blocage du trafic pour les flux destinés au site d'origine. Cela implique la nécessité d'attacher un traqueur à la route statique, pour assurer l'annonce de la route statique dans OMP UNIQUEMENT lorsque l'adresse de tronçon suivant est accessible. Cette fonctionnalité a été introduite dans la version 20.3/17.3 pour les trackers de terminaux basés sur la route statique de type adresse IP de base. À partir de la version 20.7/17.7, la prise en charge a été ajoutée pour l'envoi de sondes de suivi uniquement vers des ports TCP ou UDP particuliers de l'adresse IP de tronçon suivant (dans certains cas, lors de l'utilisation de pare-feu pour ouvrir uniquement certains ports à des fins de suivi). Pour en savoir plus sur les traqueurs de route statique, consultez le guide de configuration.

Le type de sondes utilisé ici est un simple paquet de requête d'écho ICMP. Les intervalles utilisés sont les suivants :

- Bonjour : 60 secondes
- Durée de conservation : 180 secondes (puisque #retries est 3 = 3 x 60 secondes)
- Type de paquet/sonde : Écho/réponse d'écho ICMP

Scénarios :

Ce type de trackers de point d'extrémité basés sur la route statique est utilisé pour le suivi côté service des adresses de tronçon suivant dans les routes statiques. Un tel scénario commun serait de suivre l'adresse de tronçon suivant côté LAN correspondant à une paire de pare-feu actifs/en veille, qui partagent l'adresse IP externe en fonction de laquelle l'interface externe joue le rôle de pare-feu « actif ». Dans les cas où les règles de pare-feu semblent être très restrictives, où seuls certains ports sont ouverts à des fins d'utilisation basée sur des cas, le traqueur de route statique peut être utilisé pour suivre le port TCP/UDP spécifique à l'adresse IP de tronçon suivant qui appartient sur l'interface externe du pare-feu côté LAN.



Configuration

Ces dispositifs de suivi des points d'extrémité basés sur des routes statiques doivent être configurés manuellement pour activer ce jeu de fonctions. Voici comment le configurer, selon le type de méthode de configuration préféré par l'utilisateur.

- Groupe de configuration Configuration > Groupes de configuration > Profil de service > Service VPN > Ajouter une fonctionnalité > Tracker :

1. Fournissez un nom, une description et un nom de suivi pour le nouveau suivi (point de terminaison) en cours de définition.

2. Choisissez le type de point de terminaison, selon que vous devez uniquement suivre l'adresse IP du tronçon suivant (case d'option Address) ou même des ports TCP/UDP spécifiques (case d'option Protocol).

3. Entrez l'adresse, dans un format d'adresse IP. Entrez également le protocole (TCP ou UDP) et le numéro de port, au cas où vous choisiriez Protocol comme type de point d'extrémité à l'étape précédente.

4. Vous pouvez modifier les valeurs par défaut fournies pour Intervalle d'exploration, Nombre de tentatives et Limite de latence, si nécessaire.

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

1. Cliquez sur le bouton Add IPv4/IPv6 Static Route.

2. Complétez les détails, tels que l'adresse réseau, le masque de sous-réseau, le tronçon suivant, l'adresse, AD.

3. Cliquez sur le bouton Add Next Hop With Tracker.

4. Saisissez à nouveau l'adresse de tronçon suivant, AD, puis choisissez dans la liste déroulante le nom de suivi (point de terminaison) créé précédemment.

- Configuration de la configuration héritée > Modèles > Modèles de fonction > Modèle système > section Suivi :

1. Cliquez sur le bouton Nouveau suivi des terminaux.

2. Indiquez un nom pour le nouveau suivi (point de terminaison) en cours de définition.

3. Activez la case d'option Tracker Type sur static-route.

4. Sélectionnez le type de point de terminaison, comme adresse IP de tronçon suivant (case d'option Choisir une adresse IP).

5. Entrez l'adresse IP du point de terminaison, dans un format d'adresse IP.

6. Vous pouvez modifier les valeurs par défaut fournies pour Intervalle d'exploration, Nombre de tentatives et Limite de latence, si nécessaire.

- Configuration > Templates > Feature Templates > Cisco VPN (côté service UNIQUEMENT) > IPv4/IPv6 Route section :

1. Sélectionnez le bouton New IPv4/IPv6 Route.

2. Complétez les détails, tels que Préfixe, Passerelle.

3. Cliquez sur le bouton Add Next Hop With Tracker.

4. Saisissez à nouveau l'adresse de tronçon suivant, distance, puis saisissez manuellement le nom de suivi (point d'extrémité) créé précédemment.

Du point de vue de l'interface de ligne de commande, les configurations sont les suivantes :

```
(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
!
```

Vérification

Il existe deux zones de vérification des dispositifs de suivi de point d'extrémité configurés explicitement.

- Dans Moniteur du gestionnaire SD-WAN > Périphériques > {select Device-Name} > Temps réel :

1. Sous Device Options, tapez « Endpoint Tracker Info ».

2. Cochez la case Individual Tracker (Attach Point Name) et affichez les statistiques du tracker (Tracker State, Associated Tracker Record Name, Latency in mx from device to the endpoint, Last Updated timestamp) en fonction de votre Tracker Name configuré.

- Dans Moniteur du gestionnaire SD-WAN > Périphériques > {select Device-Name} > Événements :

Dans le cas où des failles sont détectées sur le tracker, les journaux respectifs renseignent dans cette section avec des détails tels que le nom d'hôte, le nom du point d'attachement, le nom du tracker, le nouvel état, la famille d'adresses et l'id de vpn.

Sur l'interface de ligne de commande de la périphérie :

```
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]
```

Suiveurs d'objets d'interface utilisés pour le suivi VRRP

Les Object Trackers sont des trackers conçus pour la consommation en mode autonome (cas d'utilisation). Ces traqueurs ont des cas d'utilisation qui varient du suivi d'interface/tunnel basé sur VRRP au suivi NAT de service-VPN.

Pour les cas d'utilisation de suivi VRRP, l'état VRRP est déterminé en fonction de l'état de la liaison du tunnel. Si le tunnel ou l'interface est hors service sur le VRRP principal, le trafic est dirigé vers le VRRP secondaire. Le routeur VRRP secondaire dans le segment LAN devient le VRRP principal pour fournir une passerelle pour le trafic côté service. Cet exemple d'utilisation s'applique uniquement au service-VPN et permet de basculer le rôle VRRP côté LAN en cas de défaillance sur la superposition SD-WAN (interface ou tunnels dans le cas de SSE). Pour attacher des trackers à des groupes VRRP, SEULS les trackers d'objet peuvent être utilisés (pas les trackers de point d'extrémité). Cette fonctionnalité a été introduite à partir de la version 20.7/17.7 pour Cisco Catalyst SD-WAN Edge.

Aucune sonde n'est utilisée ici par le traqueur. Au lieu de cela, il utilise l'état de protocole de ligne pour décider de l'état du tracker (up/down). Il n'y a pas d'intervalles de réaction dans les trackers basés sur le protocole de ligne d'interface - au moment où le protocole de ligne d'interface/tunnel devient DOWN, l'état de la piste est également amené à l'état DOWN. Ensuite, en fonction de l'action d'arrêt ou de décrémentation, le groupe VRRP reconvergerait en conséquence. Pour en savoir plus sur les trackers d'interface VRRP, consultez le guide de configuration.

Scénarios :

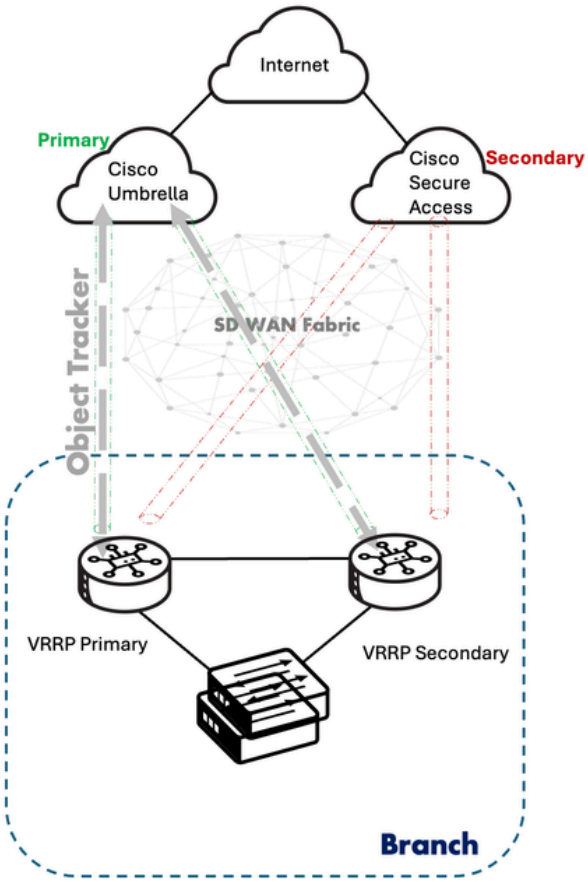
Il existe plusieurs cas d'utilisation basés sur les critères requis pour implémenter le suivi d'interface basé sur VRRP. Actuellement, les deux modes pris en charge sont (i) interface (c'est-à-dire toute interface de tunnel liée à un TLOC local) ou (ii) interface SIG (relative aux interfaces de tunnel SIG). Dans chaque cas, la partie suivie est l'interface line-protocol.

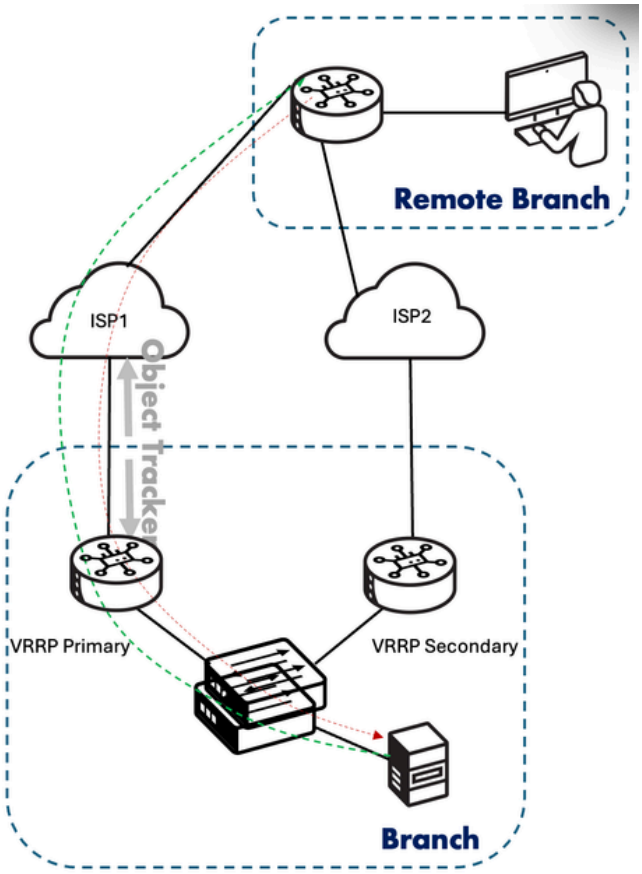
Routeur double avec Internet : L'objet de piste est lié au groupe VRRP. En cas de défaillance de

l'objet du traqueur (qui dans ce cas est l'interface du tunnel SIG), cela indique au routeur principal VRRP de déclencher la transition d'état du routeur principal au routeur de secours et au routeur de secours de devenir principal. Ce changement d'état peut être influencé ou déclenché par deux types d'opérations :

1. Décrément : Dans lequel la priorité VRRP pour l'interface sur laquelle VRRP VIP est configuré est réduite ou décrémentée d'une certaine valeur, dans le cas où l'état de l'objet de piste passe de UP à DOWN.
2. Arrêter : Il s'agit d'une méthode dans laquelle le processus VRRP est arrêté sur l'interface appliquée, dans le cas où l'état de l'objet de piste passe de UP à DOWN. Cette méthode n'est pas recommandée dans les cas d'utilisation où il existe des instances de transfert asymétrique.

TLOC Change Preference : pour éviter le trafic asymétrique provenant d'autres sites SDWAN vers le site où le VRRP s'exécute sur le VPN de service, la préférence TLOC du routeur principal VRRP est amplifiée par 1 si elle est configurée. Vous pouvez même modifier cette valeur dans les groupes de configuration. Cela garantit que le trafic du WAN au LAN est attiré par le routeur principal VRRP lui-même. Le trafic du LAN au WAN est attiré par le mécanisme VRRP du VRRP principal. Cette fonctionnalité est indépendante de VRRP interface tracker. Il s'agit d'une commande facultative (tloc-change-pref) du point de vue de l'interface de ligne de commande.





Configuration

La configuration des dispositifs de suivi d'objets est effectuée via des modèles système dans la configuration héritée, puis en attachant le dispositif de suivi d'objets au groupe VRRP respectif

sous le modèle de fonctionnalité d'interface Ethernet service-VPN. Dans le groupe Configuration, ce mécanisme a été simplifié en obtenant directement une option permettant d'ajouter le traqueur d'objets au profil d'interface Ethernet du profil de service correspondant. Voici les façons de le configurer, selon le type de méthode de configuration préféré par l'utilisateur.

- Groupe de configuration Configuration > Groupes de configuration > Profil de service > Interface Ethernet > Ajouter une fonctionnalité > Object Tracker :

1. Fournissez un nom et une description pour le nouveau traqueur d'objets en cours de définition.
2. Sélectionnez le type de suivi (parmi Interface et SIG).
3. Allouer un ID de suivi d'objet.
4. Indiquez le nom de l'interface (selon l'option choisie à l'étape 2).

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

1. Sous IPv4 Settings, cliquez sur Add VRRP IPv4.
2. Définissez un ID de groupe VRRP et fournissez une priorité locale pour cette interface Ethernet côté service.
3. Indiquez l'adresse IP virtuelle (VIP) VRRP.
4. Activez le bouton Modification des préférences TLOC et indiquez également la valeur de modification des préférences TLOC (pour gérer le routage asymétrique).
5. Cliquez sur Ajouter un objet de suivi VRRP.
6. Sous Associer un traqueur d'objets, sélectionnez dans la liste déroulante du traqueur d'objets (en fonction du nom) que vous avez créé avant
7. Choisissez une action de suivi (Arrêt ou Décrément).
8. Entrez la valeur de décrément (selon l'option choisie à l'étape 7).

- Configuration héritée > Modèles > Modèles de fonction > Système > Tracker section :

1. Cliquez sur le bouton Nouveau traqueur d'objets.
2. Sélectionnez le type de suivi (parmi Interface et SIG).
3. Allouer un ID d'objet.
4. Saisissez le nom de l'interface (selon l'option choisie à l'étape 2).

- Configuration > Templates > Ethernet Interface (appartenant au côté service) > VRRP section :

1. Cliquez sur le bouton New VRRP.
2. Définissez un ID de groupe VRRP et fournissez une priorité locale (facultatif, la valeur par défaut 100 est choisie) pour cette interface Ethernet côté service.
3. Indiquez l'adresse IP virtuelle (VIP) VRRP.
4. Activez le bouton TLOC Preference Change et indiquez également la valeur TLOC Preference Change Value (pour gérer le routage asymétrique).
5. Sous Object Tracker, cliquez sur Add Tracking Object.
6. Saisissez l'ID du traqueur d'objets (défini sous le modèle système).
7. Choisissez une action de suivi (Arrêt ou Décrément).

8. Entrez la valeur de décrément (selon l'option choisie à l'étape 7).

Du point de vue de l'interface de ligne de commande, les configurations sont les suivantes :

```
(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
!
```

Vérification

Deux options permettent de vérifier les traqueurs d'objets configurés explicitement pour les cas

d'utilisation du protocole VRRP.

- Dans Moniteur du gestionnaire SD-WAN > Périphériques > {select Device-Name} > Temps réel :

1. Sous Device Options, saisissez « VRRP Information ».

2. Cochez la case Groupe VRRP individuel (ID de groupe) et affichez les statistiques du suivi (Nom du préfixe de suivi, État du suivi, Heure de discontinuité, et Heure du dernier changement d'état) en fonction de vos ID de suivi d'objets configurés.

- Dans Moniteur du gestionnaire SD-WAN > Périphériques > {select Device-Name} > Événements :

En cas de changement d'état détecté sur le traqueur d'objet, le groupe VRRP auquel il est rattaché change d'état. Les journaux respectifs renseignent cette section (avec le nom comme Vrrp Group State Change) avec des détails tels que le nom d'hôte, le numéro if, l'id grp, le type addr, le nom if, l'état vrrp group-state, le changement d'état-reason, et l'id vpn.

Sur l'interface de ligne de commande de la périphérie :

```
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)
```

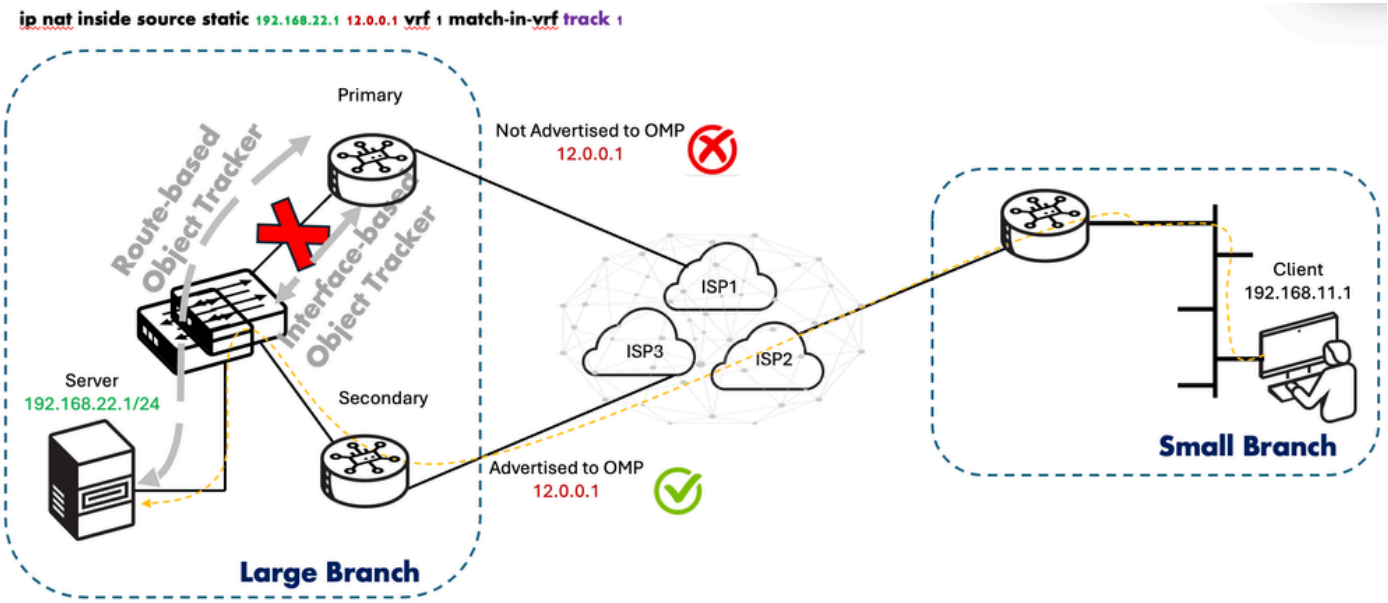
Suiveurs d'objets d'interface/de route utilisés pour le suivi NAT Service-VPN

Le NAT Object Tracker côté service est une fonctionnalité introduite dans la version 20.8/17.8, dans laquelle l'adresse globale interne utilisée dans le NAT service-VPN (NAT statique interne et NAT dynamique interne) n'est annoncée dans OMP que si (i) l'adresse locale interne est trouvée accessible OU (ii) le protocole de ligne de l'interface LAN/côté service est UP selon le traqueur d'objet attaché. Par conséquent, les types de traqueurs d'objets qui peuvent être utilisés sont (i) route ou (ii) interface. Selon l'état du préfixe LAN ou de l'interface LAN, les annonces de route NAT via OMP sont ajoutées ou supprimées. Vous pouvez afficher les journaux d'événements dans Cisco SD-WAN Manager pour surveiller quelles annonces de route NAT sont ajoutées ou supprimées.

Aucune sonde n'est utilisée ici par le traqueur. Au lieu de cela, il utilise (i) la présence d'une entrée de routage dans la table de routage OU (ii) l'état de protocole de ligne pour décider de l'état de suivi (up/down). Il n'y a pas d'intervalles de réaction en présence d'une entrée de routage ou de trackers basés sur le protocole de ligne d'interface : au moment où l'entrée de routage ou le protocole de ligne d'interface tombe en panne, l'état de la piste passe également à l'état DOWN. Immédiatement, l'adresse globale interne utilisée dans l'instruction NAT associée au traqueur d'objets ne peut plus être annoncée dans OMP. Pour en savoir plus sur les traqueurs NAT VPN de service, consultez le guide de configuration.

Scénarios :

Si une interface LAN ou un préfixe LAN est désactivé, le traqueur d'objet NAT côté service s'arrête automatiquement. Vous pouvez afficher les journaux des événements dans Cisco SD-WAN Manager pour contrôler quelles annonces de routes NAT sont ajoutées ou supprimées. Dans l'exemple d'utilisation suivant, le client doit accéder au serveur dans la grande filiale. Cependant, le problème se pose dans des situations où soit la route pointant vers le serveur sur les bords de grande branche (dans HA) est supprimée OU quand l'interface côté LAN (côté service) tombe en panne sur un bord dans la grande branche. Dans de telles situations, lorsque vous appliquez la NAT côté service avec le traqueur d'objet, assurez-vous que le trafic entrant en provenance du client est toujours dirigé vers le bon bord situé dans la grande branche en contrôlant l'annonce d'adresse globale interne dans OMP. Dans le cas où un tel contrôle n'est pas appliqué sur l'annonce de route dans OMP, le trafic finit par obtenir un trou noir en raison de l'inaccessibilité de cette périphérie respective au serveur dans la grande filiale.



Configuration

La configuration des traqueurs d'objets s'effectue via des modèles système dans la configuration héritée, puis en attachant le traqueur d'objets à l'instruction NAT respective (statique interne ou dynamique interne) dans le modèle de fonctionnalité service-VPN. Dans le groupe Configuration, ce mécanisme a été simplifié en obtenant directement une option permettant d'ajouter le traqueur d'objets au profil d'interface Ethernet du profil de service correspondant. Voici les façons de le configurer, selon le type de méthode de configuration préféré par l'utilisateur.

- Groupe de configuration Configuration > Groupes de configuration > Profil de service > Ajouter une fonctionnalité > Object Tracker :

1. Fournissez un nom et une description pour le nouveau traqueur d'objets en cours de définition.
2. Sélectionnez le type de suivi (parmi Interface et route).
3. Allouer un ID de suivi d'objet.
4. Indiquez le nom de l'interface OU indiquez l'adresse IP de la route, le masque IP de la route et le VPN (selon l'option choisie à l'étape 2).

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

1. Créez un pool NAT (obligatoire pour le déclenchement de la fonction NAT) en cliquant sur le bouton Add NAT Pool.

2. Fournissez les détails du pool NAT, tels que le nom du pool NAT, la longueur du préfixe, le début de la plage, la fin de la plage et la direction.

3. Passez à la NAT statique dans la même section et cliquez sur le bouton Add New Static NAT. (Vous pouvez également choisir d'attacher le traqueur d'objets à la NAT de pool dynamique interne).

4. Fournissez les détails tels que l'IP source, l'IP source traduite et la direction NAT statique.

5. Dans le champ Associer un traqueur d'objets, sélectionnez dans la liste déroulante le traqueur d'objets précédemment créé.

- Configuration héritée > Modèles > Modèles de fonction > Système > Tracker section :

1. Cliquez sur le bouton Nouveau traqueur d'objets.
2. Sélectionnez le type de suivi (parmi Interface et route).
3. Allouer un ID d'objet.
4. Fournissez le nom d'interface OU l'adresse IP de la route, le masque IP de la route et le VPN (selon l'option choisie à l'étape 2).

- Configuration > Templates > Cisco VPN (appartenant au côté service) > section NAT :

1. Créez un pool NAT (obligatoire pour déclencher la traduction d'adresses de réseau) en cliquant sur le bouton Nouveau pool NAT.

2. Fournissez les détails du pool NAT, tels que le nom du pool NAT, la longueur du préfixe du pool NAT, le début de la plage du pool NAT, la fin de la plage du pool NAT et la direction NAT.

3. Passez à la NAT statique dans la même section et cliquez sur le bouton New Static NAT. (Vous pouvez également choisir d'attacher le traqueur d'objets à la NAT de pool dynamique interne).

4. Fournissez les détails tels que l'adresse IP source, l'adresse IP source traduite, la direction NAT statique.

5. Dans le champ Ajouter un traqueur d'objets, tapez le nom du traqueur d'objets précédemment créé.

Du point de vue de l'interface de ligne de commande, les configurations sont les suivantes :

```
(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
!
```

L'hypothèse avec l'exemple d'utilisation de la NAT est que les utilisateurs appliquent la politique de données pour faire correspondre le trafic pour les flux entrants -> sortants et sortants -> dans la NAT.

Vérification

Il existe deux zones de vérification des traqueurs d'objets explicitement configurés pour les cas d'utilisation de la NAT.

- Sur le gestionnaire SD-WAN : Surveillance > Périphériques > {select Device-Name} > Temps réel :

1. Sous Device Options, tapez « IP NAT Translation ».

2. Cochez la case Traduction NAT individuelle et affichez les statistiques de l'entrée (adresse/port local interne, adresse/port global interne, adresse/port local externe, adresse/port global externe, ID VRF, nom VRF et protocole) en fonction de vos ID de suivi d'objets configurés.

- Sur le gestionnaire SD-WAN : Contrôle > Périphériques > {select Device-Name} > Événements :

En cas de changement d'état détecté sur le traqueur d'objet correspondant à la route NAT élaguée dans OMP, des événements nommés "NAT Route Change" apparaissent, qui contiennent des détails tels que le nom d'hôte, le traqueur d'objet, l'adresse, le masque, le type de route et la mise à jour. Ici, l'adresse et le masque correspondent à l'adresse globale interne configurée sous l'instruction NAT statique.

Sur l'interface de ligne de commande de la périphérie :

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.