Comprensione dei casi di utilizzo e utilizzo di Catalyst SD-WAN Tracker

Sommario

- Introduzione
- Premesse
- Tipi di Tracker
- Tracciamento gateway
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracciamento di Service Insertion 1.0 e Service Fabric 2.0
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracker endpoint interfaccia utilizzati per DIA
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracker endpoint interfaccia utilizzati per tunnel SIG/SSE
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracker endpoint interfaccia utilizzati per Service Fabric 2.0
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracker endpoint con route statica utilizzati per il rilevamento route statica (lato servizio)
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracker oggetti interfaccia utilizzati per il rilevamento VRRP
  - Scenari d'uso
  - Configurazione
  - Verifica
- Tracker oggetti interfaccia/route utilizzati per il rilevamento NAT Service-VPN
  - Scenari d'uso
  - Configurazione
  - Verifica

Introduzione

Questo documento descrive le reti Catalyst SD-WAN Enterprise Overlay, la tracciabilità e i casi di utilizzo.

Premesse

Le reti di overlay aziendali Catalyst SD-WAN in genere interagiscono con un'ampia varietà di carichi di lavoro esterni, applicazioni e servizi. qualsiasi elemento che possa trovarsi nel cloud, nel centro dati/hub o nelle filiali remote. Il control plane SD-WAN è responsabile della pubblicità dei percorsi verso questi servizi attraverso la sovrapposizione in modo scalabile. In situazioni in cui le applicazioni e i servizi critici diventano irraggiungibili lungo un percorso specifico, gli operatori di rete devono in genere essere in grado di rilevare questi eventi e reindirizzare il traffico degli utenti verso percorsi più appropriati per evitare blocchi del traffico indefiniti. Per rilevare e correggere questi tipi di guasti di rete, il control plane Catalyst SD-WAN si basa su tracker per monitorare lo stato dei servizi esterni e apportare le modifiche appropriate al routing.

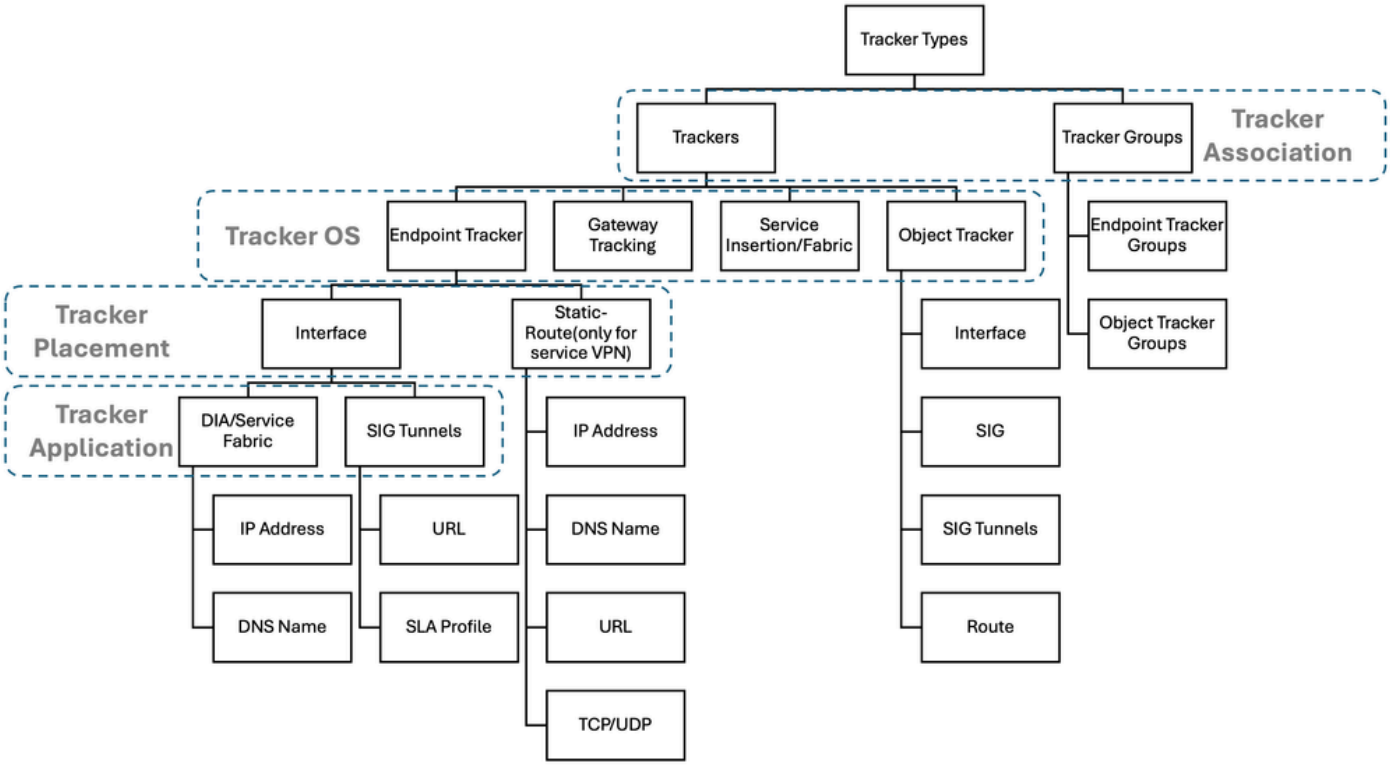
Il tracker è un meccanismo di rilevamento della raggiungibilità del piano di controllo che invia pacchetti di sonda verso un endpoint specifico e notifica le modifiche dello stato di raggiungibilità (verso l'alto o verso il basso) dell'endpoint ai moduli interessati. I tracciatori sono progettati come un'astrazione scalabile di alto livello della funzione SLA IP nativa di Cisco IOS-XE®, che può formare una varietà di sonde (tra cui HTTP, ICMP e DNS). Quando un tracciatore notifica a un modulo client un cambiamento di stato, tale modulo può adottare le misure appropriate per prevenire blocchi del traffico, come l'installazione o la disinstallazione di una route o di un set di route. Le applicazioni correnti dei tracciatori all'interno delle soluzioni SD-WAN e SD-Routing includono, tra l'altro: Tracker DIA (Direct Internet Access), SIG (Secure Internet Gateway), Service Tracker, Tracker statici, gruppi di tracciamento e così via.

Per creare reti a disponibilità elevata resilienti agli errori del servizio, è fondamentale capire quando utilizzare ogni tipo di configurazione/modello di tracciatore. L'obiettivo di questo articolo è spiegare dove e come viene utilizzato ogni tipo di tracker. In questa sezione vengono illustrati i vari tracker, il caso di utilizzo principale di ciascun tracker e i flussi di lavoro di configurazione di base per implementare ciascuna soluzione. Infine, in questo articolo viene presentata una panoramica delle avvertenze generali relative ai tracker in Cisco IOS-XE®.

In questo articolo viene fatta una distinzione tra le soluzioni endpoint-tracker (specifiche di SD-WAN e SD-Routing) e object tracker (native IOS-XE), che gestiscono diversi scenari di utilizzo.

Tipi di Tracker

Questo grafico fornisce una breve panoramica di tutti i tipi di tracker disponibili nella soluzione Cisco Catalyst SD-WAN:



Dal grafico precedente, ci sono quattro aree in cui i tracciatori possono essere classificati: Associazione tracciatore, Sistema operativo tracciatore, Posizionamento tracciatore e Applicazione tracciatore. La sezione successiva descrive ciascuna classificazione:

1. Associazione Tracker: Questa classificazione descrive se un tracciatore è un singolo tracciatore o un gruppo di tracciatori. Cisco Catalyst SD-WAN supporta l'uso di più tracker in un gruppo (fino a 2 in questo momento della scrittura) e lo stato generale del gruppo di tracker è determinato da un operatore booleano AND o OR. Gli esempi includono un gruppo di individuazione endpoint o un gruppo di individuazione oggetti.
2. Sistema operativo Tracker: Questa classificazione descrive il sistema operativo Cisco IOS-XE® o la modalità in cui è supportato il tracker. I router Cisco Catalyst IOS-XE supportano due modalità operative:

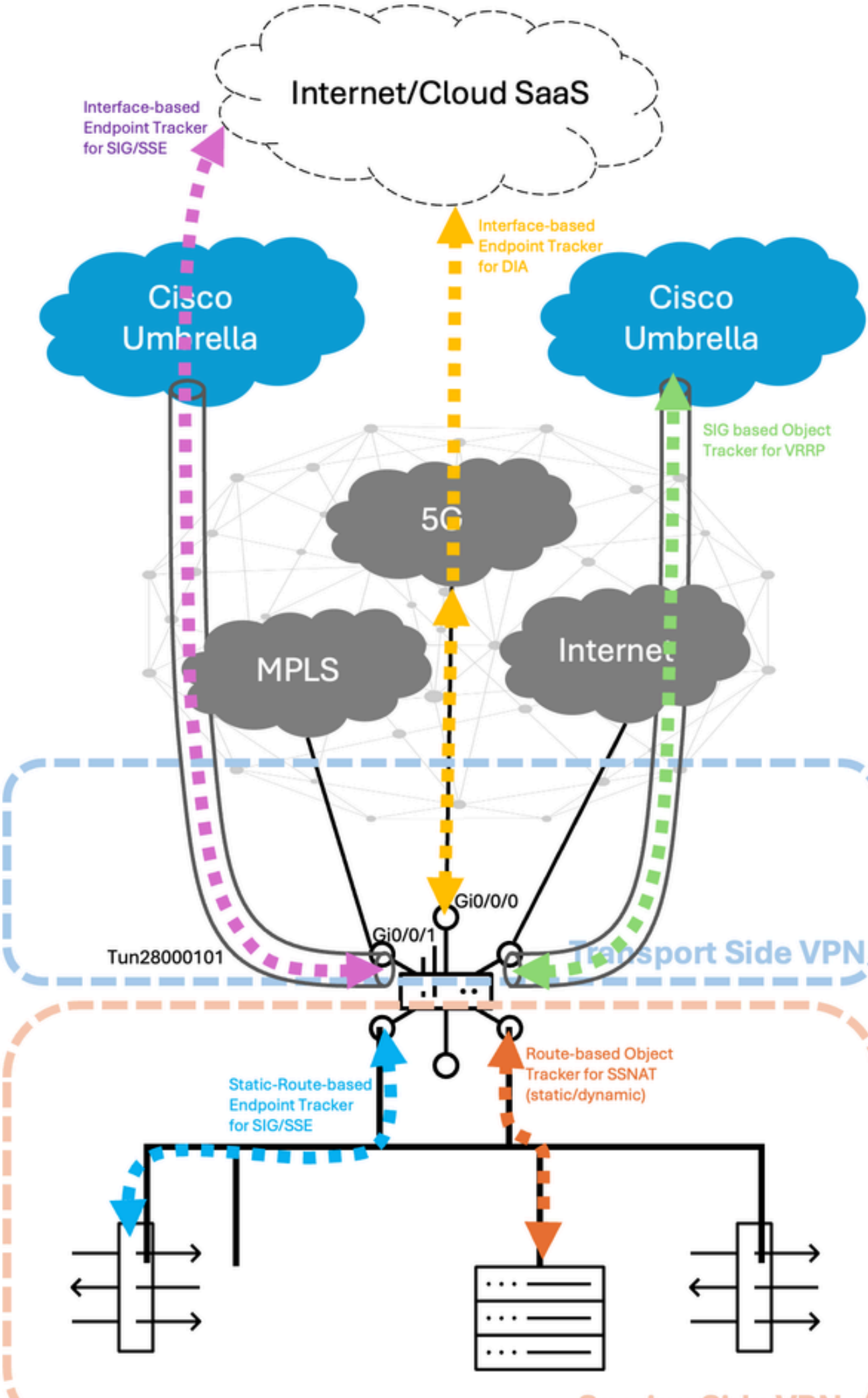
- Modalità autonoma e
- Modalità controller.

Tutte le funzioni endpoint-tracker e gateway-tracking sono entrambe progettate per i casi di utilizzo in modalità controller (SD-WAN), mentre object tracker è progettato per i casi di utilizzo in modalità autonoma (SD-Routing).

3. Posizionamento dell'indicatore di percorso: Questa classificazione descrive la posizione in cui è configurato il tracker. Al momento, Cisco Catalyst SD-WAN supporta l'applicazione di tracciatori su interfacce, route statiche o servizi.

4. Applicazione Tracker: Questa classificazione descrive i casi di utilizzo di alto livello e le funzionalità supportate da Cisco Catalyst SD-WAN. Sebbene vi siano numerose aree di applicazione degli inseguitori, alcune di esse includono: Direct Internet Access (DIA), Secure Internet Gateway (SIG), Secure Service Edge (SSE), rilevamento VPN lato servizio e così via.

Di seguito è riportata una rappresentazione visiva del traffico della sonda di tracciamento tra le VPN di servizio/trasporto per diversi scenari di utilizzo su un perimetro Cisco Catalyst SD-WAN (a cui si può fare riferimento anche come 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

configurate sulle piattaforme SD-WAN Edge sulla VPN lato trasporto. Per impostazione predefinita, questa funzione è abilitata nelle configurazioni di base dei profili di sistema (Track Default Gateway) in Catalyst SD-WAN Manager. In questo modo è possibile monitorare continuamente l'indirizzo dell'hop successivo specificato in ogni route statica predefinita nella VPN di trasporto per garantire il failover del collegamento o della route in caso di errore di raggiungibilità dell'hop successivo (detto anche gateway, da cui il nome di traccia del gateway). Per ulteriori informazioni sulla traccia del gateway, visitare la guida alla configurazione.

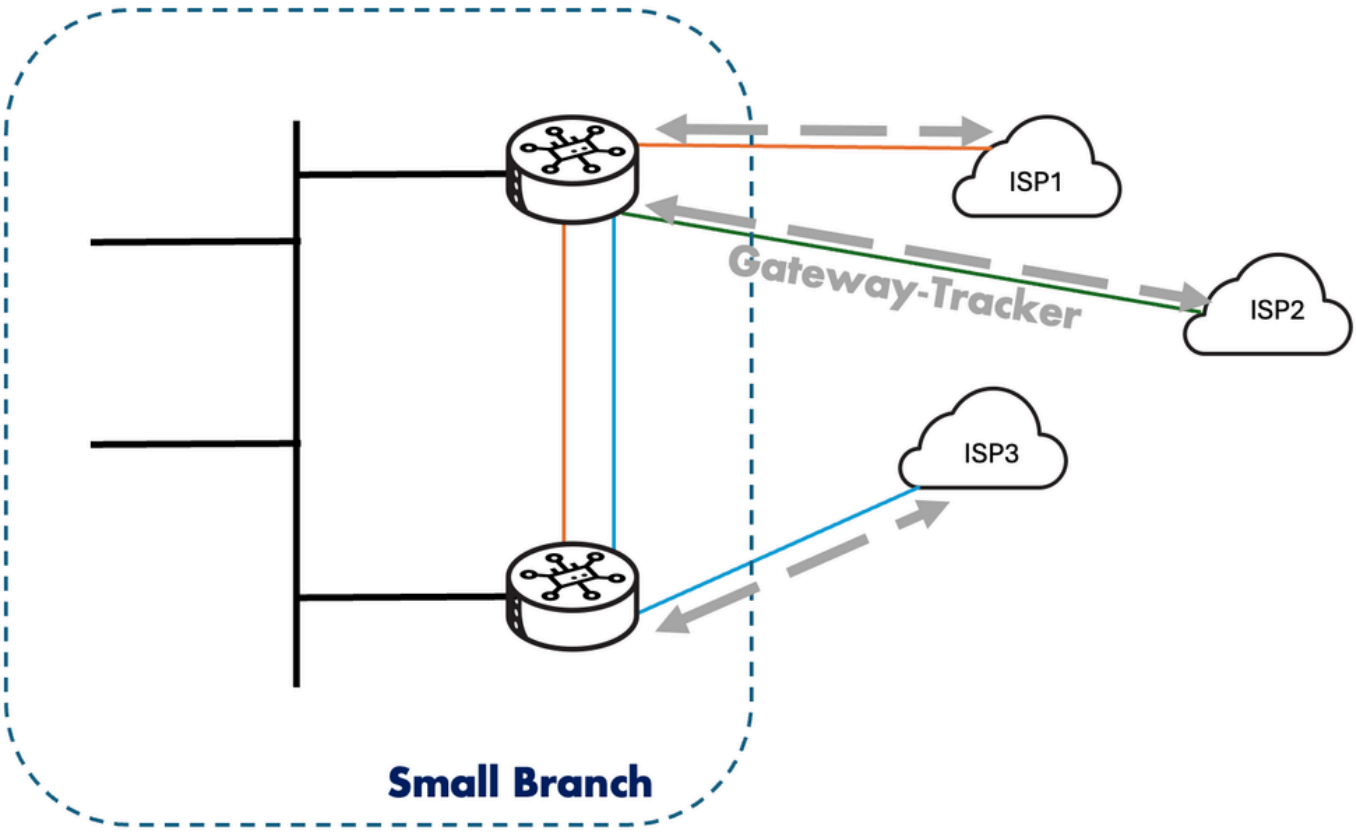
Il tipo di sonde utilizzato qui sono pacchetti flooded unicast con richiesta ARP. Gli intervalli utilizzati sono i seguenti:

- Salve: 10 secondi
- Holdtime: 100 secondi
- Tipo pacchetto/sonda: ARP

Insieme al tracciamento del gateway, viene anche usato il tracciamento del trasporto sui bordi SD-WAN per controllare il percorso indirizzato tra il dispositivo locale e un Cisco Catalyst SD-WAN Validator. A tal fine, si usano sonde ICMP a intervalli regolari di 3 s. Questa configurazione viene effettuata usando la parola chiave "track-transport" per la modalità di configurazione del sistema SD-WAN. Ciò aiuta a monitorare regolarmente la connessione DTLS al Cisco Catalyst SD-WAN Validator dal rispettivo WAN Edge. Per ulteriori informazioni sul rilevamento del trasporto, consultare la guida alla configurazione.

Scenari d'uso

Il tracciamento del gateway è una funzione configurata in modo implicito su SD-WAN per tutte le route statiche predefinite appartenenti alla VPN di trasporto o alla tabella di routing globale (GRT). L'utilizzo di questa funzionalità non sempre ha origine dal punto di vista della configurazione del modello di Manager, ma può anche evolversi dalle route statiche predefinite ricevute/acquisite negli scenari di utilizzo di un server DHCP con opzioni #3, #81 e così via.



Configurazione

Applicato per impostazione predefinita in Cisco Catalyst SD-WAN:

```
!
system
```

```
 track-transport
 track-default-gateway
```

```
!
```

Verifica

Di seguito sono riportati i modi per verificare questa condizione in base alla configurazione e al

gruppo di configurazione legacy:

- Gruppo di configurazione: Configurazione > Gruppi di configurazione > Profilo di sistema > Sottoprofilo di base > Sezione Impostazioni traccia > Traccia gateway predefinito (impostazione predefinita: ON)
- Configurazione legacy: Configurazione > Modelli > Modelli funzionalità > Modello di sistema > Sezione Avanzate > Tracciamento gateway (impostazione predefinita: ATTIVATO)

Tracciamento di Service Insertion 1.0 e Service Fabric 2.0

Service Insertion 1.0 Tracking è stato introdotto nella versione 20.3/17.3 ed è una funzione mirata a garantire che l'indirizzo del servizio (o indirizzo di inoltro) sia raggiungibile o disponibile. Queste informazioni aiutano Edge ad aggiungere o a prelevare dinamicamente le informazioni dell'hop successivo dalla policy Control/Data. Con la configurazione di Service Insertion 1.0, per impostazione predefinita il tracker (o indirizzo di rilevamento) viene abilitato verso l'indirizzo del servizio. In base a questo, l'indirizzo di inoltro e l'indirizzo del servizio sono gli stessi della versione 1.0. Anche se i tracker del servizio sono configurati automaticamente con i servizi, questi tracker possono essere disabilitati usando il comando no track-enable o disabilitando la manopola tracker nella configurazione del gruppo di configurazione/legacy. Poiché si tratta delle uniche due operazioni possibili (abilitazione/disabilitazione) con rilevatori associati ai servizi di Service Insertion 1.0, non sono disponibili altri parametri modificabili (come soglia, moltiplicatore, intervallo). Il tipo di sonde utilizzato qui è un pacchetto di richiesta echo ICMP.

Per ulteriori informazioni sul rilevamento di Service Insertion 1.0, visitare la guida alla configurazione. Gli intervalli predefiniti utilizzati nel rilevamento di Service Insertion 1.0 sono:

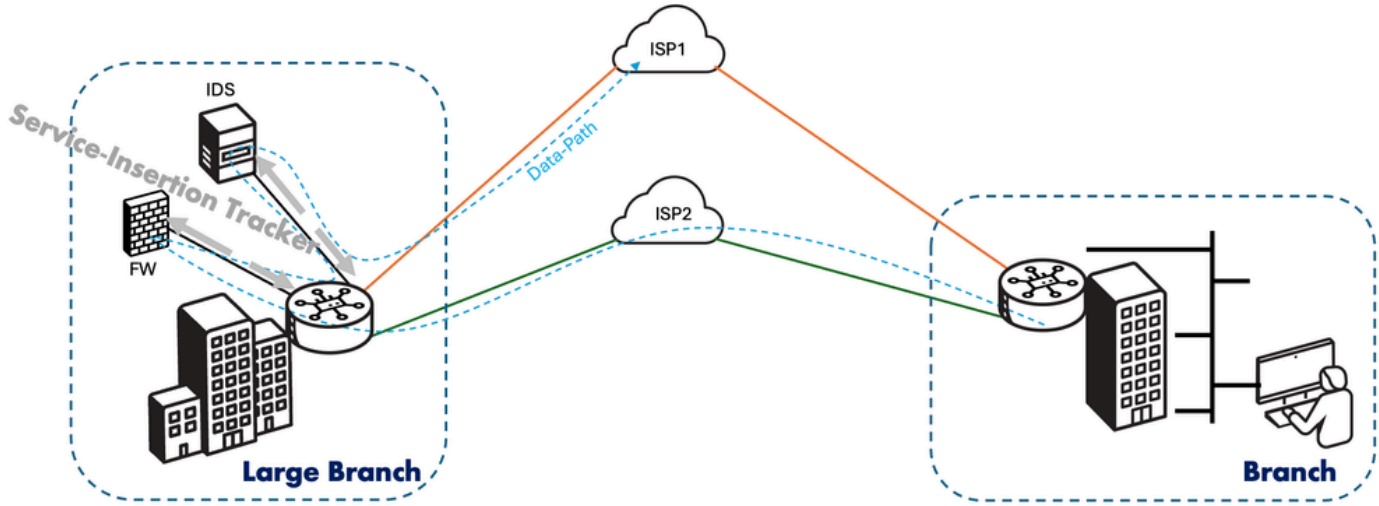
- Intervallo probe: 5 sonde ogni 60 secondi
- Moltiplicatore: 5 volte
- Tipo pacchetto/sonda: ICMP Echo/Echo-reply

Service Fabric 2.0 Tracking fa parte dell'offerta di funzionalità Service Insertion 2.0 in Cisco Catalyst SD-WAN introdotta a partire dalla versione 20.13/17.13. In questa nuova variante di inserimento del servizio, il metodo predefinito utilizzato dai profili e dai modelli di configurazione deve ancora avere un tracciatore implicito che punti a ciascun indirizzo di servizio definito (o indirizzo di inoltro) in una coppia di servizi HA per interfaccia rx/tx. Tuttavia, con Service Fabric 2.0 è ora possibile dividere l'indirizzo di inoltro dall'indirizzo di rilevamento. A tale scopo, è sufficiente definire rilevatori di endpoint distinti per tenere traccia di un indirizzo di endpoint diverso dall'indirizzo di servizio stesso. Nelle sezioni successive di questo argomento vengono fornite ulteriori informazioni.

Scenari d'uso

Il caso di utilizzo principale per i tracciatori dei servizi è il monitoraggio scalabile della raggiungibilità dei servizi, in particolare per il concatenamento dei servizi. Il concatenamento dei servizi può essere implementato in una rete costituita da più VPN, in cui ogni VPN rappresenta una funzione o un'organizzazione diversa, per garantire che il traffico tra le VPN passi attraverso

un firewall. Ad esempio, in una grande rete di campus, il traffico interdipartimentale può passare attraverso un firewall, mentre il traffico interdipartimentale può essere indirizzato direttamente. Il concatenamento dei servizi può essere visto in scenari in cui un operatore deve soddisfare i requisiti di conformità alle normative, ad esempio lo standard PCI DSS (Payment Card Industry Data Security Standard), in cui il traffico PCI deve passare attraverso i firewall in un centro dati centralizzato o in un hub regionale:



Configurazione

Le configurazioni sono le stesse del normale flusso di lavoro per la configurazione di Service Insertion 1.0 su SD-WAN. I Tracker di Service Insertion 1.0 verranno abilitati per impostazione predefinita su tutti gli indirizzi di servizio.

- Gruppo di configurazione: Configurazione > Gruppi di configurazione > Profilo servizio > VPN servizio > Sezione Servizio:

1. Fare clic sul pulsante Add Service.

2. Scegliere un tipo di servizio.

3. Integrare l'indirizzo del servizio (massimo 4 possibili, separati da una virgola).

4. Verificare che la manopola Tracciamento sia attivata (impostazione predefinita). Se necessario, è possibile disattivare questa funzione.

- Configurazione legacy: Configurazione > Modelli > Modelli funzionalità > Cisco VPN (servizio) > Sezione Servizio:

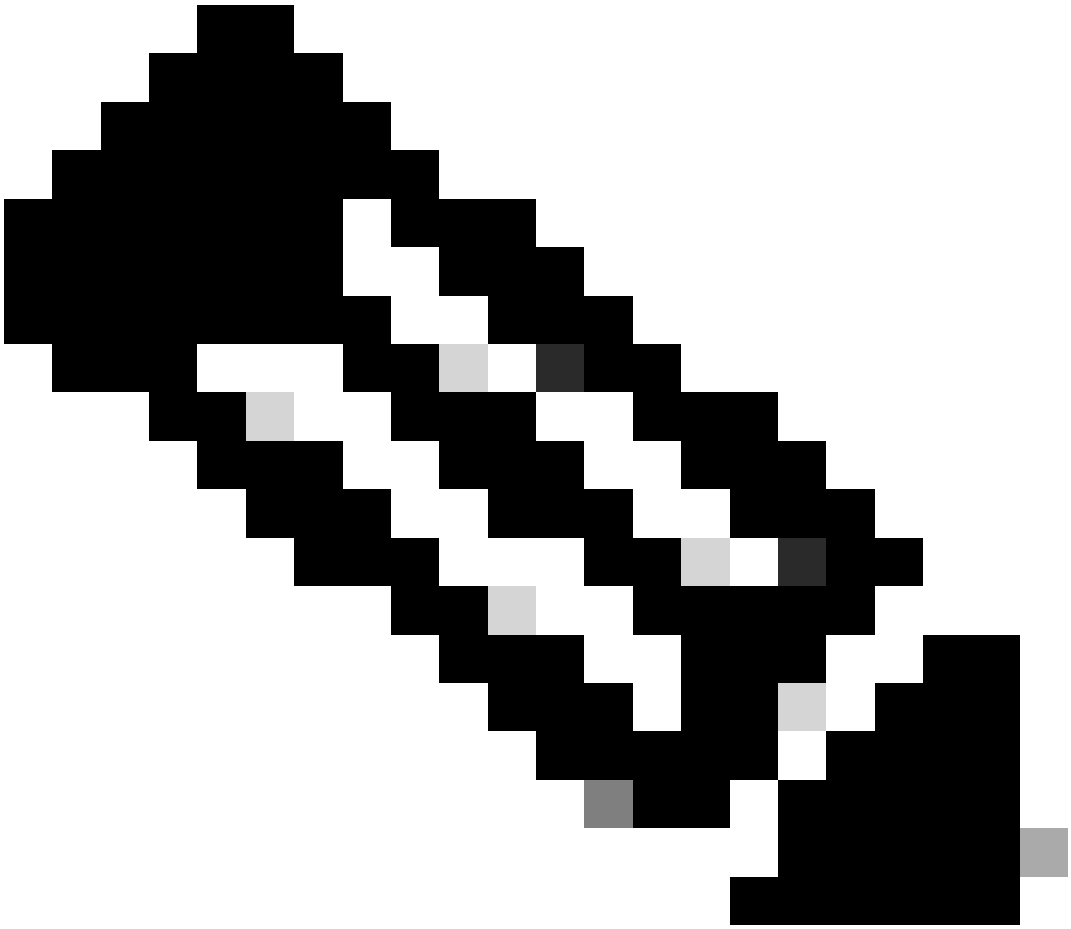
1. Fare clic sul pulsante Nuovo servizio

2. Scegliere un tipo di servizio.

3. Integrare l'indirizzo del servizio (massimo 4 possibili, separati da una virgola).

4. Verificare che la manopola Tracciamento sia attivata (impostazione predefinita). Se necessario,

è possibile disattivare questa funzione.



> Nota: Quando il passo 3 viene configurato (dal gruppo di configurazione o dalla configurazione legacy), il tracker viene avviato automaticamente ai vari indirizzi di servizio definiti

---

Dal punto di vista della CLI, la configurazione per Service Insertion 1.0 è la seguente:

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

Verifica

I passaggi per la verifica si estendono agli stessi passaggi seguiti nell'ambito dei tracciatori di endpoint basati sull'interfaccia utilizzati nelle sezioni precedenti.

Sono disponibili due opzioni di verifica per l'individuazione degli endpoint configurati in modo esplicito.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Applicazioni > Tracker:

Controllare in Individual Tracker e visualizzare le statistiche del tracciatore (Tipi di tracciatore, Stato, Endpoint, Tipo di endpoint, Indice VPN, Nome host, Tempo andata e ritorno) in base al nome del tracciatore configurato.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Eventi:

Nel caso di flap rilevati sul tracciatore, i rispettivi log vengono compilati in questa sezione con dettagli quali nome host, nome del punto di collegamento, nome del tracciatore, nuovo stato, famiglia di indirizzi e ID vpn.

Dalla CLI del perimetro:

```
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
```

Tracker endpoint interfaccia utilizzati per DIA

I tracker NAT DIA Endpoint Trackers sono progettati principalmente per monitorare la raggiungibilità delle applicazioni tramite un'interfaccia NAT DIA su piattaforme SD-WAN Edge.

Nei casi di utilizzo di Direct Internet Access (DIA), i tracker NAT DIA vengono utilizzati principalmente per tracciare l'interfaccia lato trasporto e attivare un failover su un'altra interfaccia lato trasporto disponibile o tramite tunnel di sovrapposizione SD-WAN (utilizzando la policy di dati). Questa funzione è stata introdotta a partire dalla versione 20.3/17.3 e l'opzione per la

funzione di fallback NAT è disponibile dalla versione 20.4/17.4. Se il tracciatore determina che l'Internet locale non è disponibile tramite l'interfaccia NAT DIA, il router ritira il percorso NAT dalla VPN del servizio e reindirizza il traffico in base alla configurazione del routing locale. Il tracker continua a controllare periodicamente lo stato del percorso all'interfaccia. Quando rileva che il percorso è nuovamente funzionante, il router reinstalla il percorso NAT su Internet. Per ulteriori informazioni sui tracciatori DIA, consultare la guida alla configurazione.

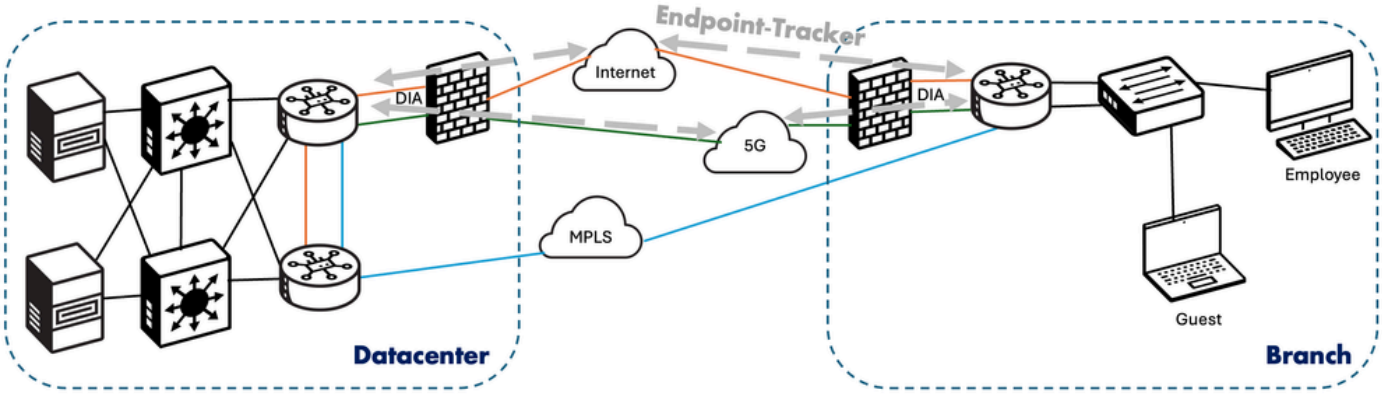
Nella definizione tracker, è possibile scegliere di fornire un indirizzo IP di un endpoint raggiungibile tramite l'interfaccia DIA NAT (configurata come "endpoint-ip") OPPURE un nome di dominio completo (FQDN) all'endpoint (configurata come "endpoint-dns-name").

Il tipo di sonde utilizzato in questo caso è un pacchetto di richiesta HTTP, molto simile a uno stack PDU di richiesta API HTTP. Gli intervalli utilizzati sono i seguenti:

- Intervallo probe: 60 secondi
- Moltiplicatore: 180 secondi (poiché #retries è 3 = 3 x 60 secondi)
- Tipo pacchetto/sonda: HTTP

Scenari d'uso

DIA viene spesso implementata come ottimizzazione nei siti delle filiali per evitare il backhauling a un centro dati di qualsiasi traffico di filiali destinato a Internet. Tuttavia, quando si utilizza la DIA nei siti delle filiali, qualsiasi mancanza di raggiungibilità lungo le rotte NAT DIA deve ancora ricadere su percorsi alternativi per evitare il blackhold e la perdita del servizio. Per i siti che desiderano utilizzare il fallback al controller di dominio (tramite overlay SD-WAN con fallback NAT) in caso di guasto locale del DIA breakout. Questi tracker di endpoint basati sull'interfaccia sulle interfacce con supporto DIA sui bordi delle filiali per rilevare eventuali guasti e avviare un failover al percorso di backup/controller di dominio. In questo modo, l'elevata disponibilità del servizio Internet viene ottenuta con un'interruzione minima delle attività aziendali, ottimizzando al contempo il traffico Internet con DIA:



Configurazione

Per abilitare questo gruppo di funzionalità, questi tracker di endpoint basati sull'interfaccia devono essere configurati manualmente. Di seguito sono indicati i metodi di configurazione, a seconda del tipo di metodo di configurazione preferito dall'utente.

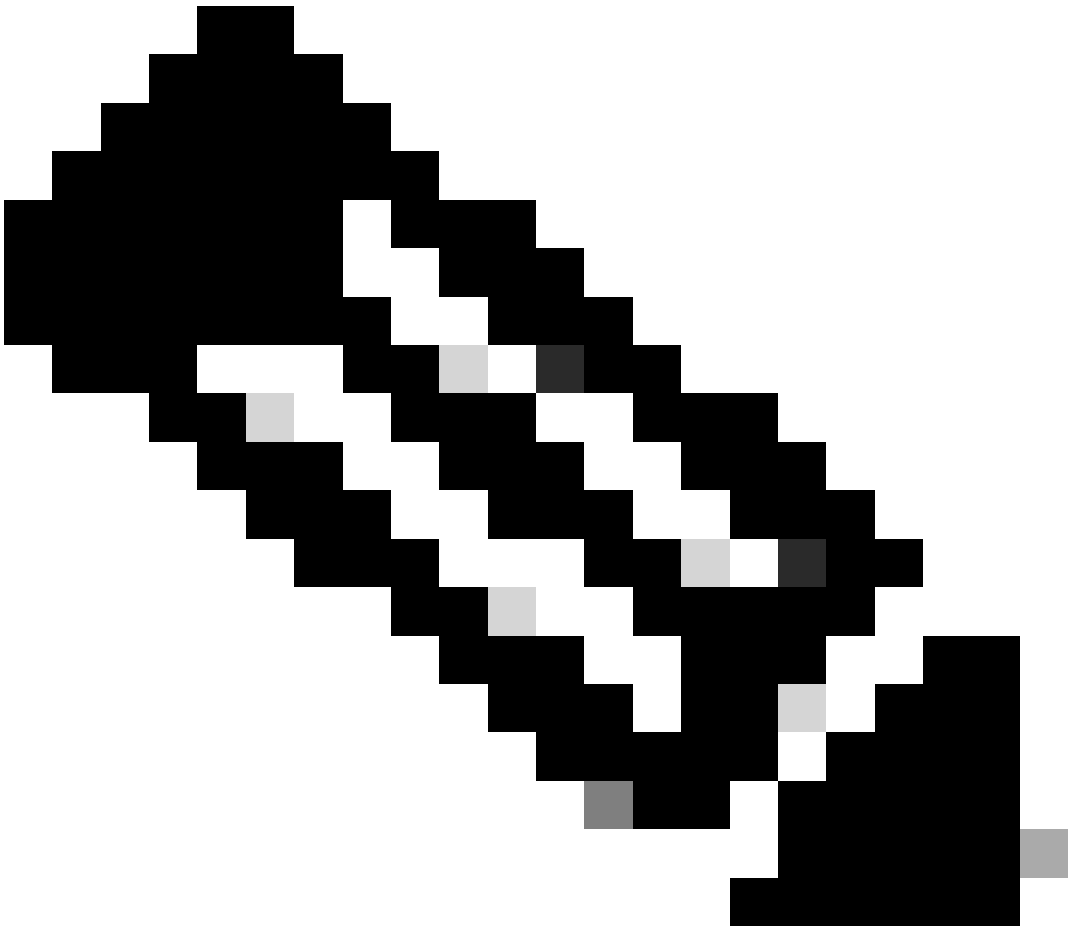
- Gruppo di configurazione: Configurazione > Gruppi di configurazione > Profilo di trasporto e gestione > Interfaccia Ethernet > Aggiungi funzionalità > Tracker:

1. Definire un nome di individuazione endpoint.

2. Scegliere un tipo di rilevamento endpoint (tra HTTP-default e ICMP).

Nota: Il tipo di tracciatore dell'endpoint ICMP è stato introdotto a partire dalla versione 20.13/17.13.

3. Selezionare l'endpoint (tra IP-predefinito endpoint e Nome DNS endpoint).



Nota: Se si sceglie il nome DNS dell'endpoint, verificare che sia definito un server DNS o un server dei nomi valido nella VPN/VRF di trasporto utilizzando il profilo di configurazione della VPN di trasporto.

---

4. Immettere l'indirizzo o il nome DNS (FQDN) verso cui devono essere inviate le richieste di individuazione (il formato dipende dal passaggio precedente).

5. (Facoltativo) Potete scegliere di modificare l'intervallo della sonda (impostazione predefinita = 60 secondi) e il numero di tentativi (impostazione predefinita = 3 volte) per ridurre il tempo di rilevamento degli errori.

- Configurazione legacy:

Passaggio 1. Definizione di Tracker endpoint basato sull'interfaccia: Configurazione > Modelli > Modelli funzionalità > Modello di sistema > Sezione Tracker:

1. In Sottosezione Tracker, selezionare il pulsante New Endpoint Tracker.

2. Definire un nome di individuazione endpoint.

3. Scegliere il tipo di tracciatore (tra interfaccia predefinita e route statica) come interfaccia, poiché i casi di utilizzo di DIA rappresentano un problema.

4. Scegliere il tipo di endpoint (tra Indirizzo IP predefinito e Nome DNS).

5. Immettere l'indirizzo IP dell'endpoint o il nome DNS dell'endpoint verso cui devono essere inviate le richieste di rilevamento (il formato dipende dal passaggio precedente).

6. (Facoltativo) È possibile scegliere di modificare le impostazioni Soglia sonda (valore predefinito = 300 ms), Intervallo (valore predefinito = 60 secondi) e Multiplatore (valore predefinito = 3 volte).

Passaggio 2. Applicare Interface-Based Endpoint Tracker a un'interfaccia sulla VPN di trasporto: Modelli > Modelli funzionalità > Cisco VPN Interface Ethernet > Sezione Avanzata:

1. Inserire il nome di Endpoint Tracker definito nel passo 1 precedente nel campo Tracker.

Dal punto di vista della CLI, le configurazioni hanno il seguente aspetto:

```
(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
!
```

Verifica

Sono disponibili due opzioni di verifica per i tracciatori degli endpoint configurati in modo esplicito.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Applicazioni > Tracker:

Controllare in Individual Tracker e visualizzare le statistiche del tracciatore (Tipi di tracciatore, Stato, Endpoint, Tipo di endpoint, Indice VPN, Nome host, Tempo andata e ritorno) in base al nome del tracciatore configurato.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Eventi:

Nel caso di flap rilevati sul tracciatore, i rispettivi log vengono compilati in questa sezione con dettagli quali nome host, nome del punto di collegamento, nome del tracciatore, nuovo stato, famiglia di indirizzi e ID vpn.

Dalla CLI del perimetro:

```
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
```

Tracker endpoint interfaccia utilizzati per tunnel SIG/SSE

Quando si utilizzano i tracker degli endpoint per i casi di utilizzo del tunnel SIG/SSE, ciò indica principalmente che l'azienda è alla ricerca di un'offerta di stack di sicurezza basata su cloud che possa essere facilmente resa disponibile al giorno d'oggi con l'aiuto di provider SIG (Secure Internet Gateway) o SSE (Secure Service Edge), quali Cisco, Cloudflare, Netskope, ZScalar e così via. Sia i tunnel SIG che l'SSE fanno parte del modello di implementazione della sicurezza del cloud, in cui la filiale utilizza il cloud per fornire le soluzioni di sicurezza necessarie. Il caso di utilizzo dei tunnel SIG è stata l'offerta iniziale di integrazione di Cisco Catalyst SD-WAN con tali provider SIG (versione 20.4/17.4), tuttavia con l'evoluzione delle offerte di sicurezza fornite dal cloud - il caso di utilizzo SSE è stato introdotto (versione 20.13/17.13) per coprire i casi di utilizzo con provider come Cisco (tramite Cisco Secure Access) e ZScalar.

L'IT richiede un approccio affidabile ed esplicito per proteggere e collegarsi con agilità. È ormai comune fornire ai dipendenti remoti l'accesso diretto alle applicazioni cloud, ad esempio Microsoft 365 e Salesforce, con una maggiore sicurezza. La richiesta di reti e sicurezza distribuite tramite cloud si espande ogni giorno, poiché fornitori, partner, dispositivi Internet of Things (IoT) e così via richiedono l'accesso alla rete. La convergenza delle funzioni di rete e sicurezza più vicine ai dispositivi finali, al limite del cloud, è nota come modello di servizio Cisco SASE. Cisco SASE combina le funzioni di rete e sicurezza fornite dal cloud per fornire un accesso sicuro alle applicazioni per tutti gli utenti o i dispositivi, da qualsiasi luogo e in qualsiasi momento. Secure Service Edge (SSE) è un approccio alla sicurezza di rete che aiuta le organizzazioni a migliorare la postura di sicurezza del proprio ambiente di lavoro riducendo al contempo la complessità per gli utenti finali e i reparti IT. Per ulteriori informazioni sui tracker SIG Tunnel/SSE, visitare la guida alla configurazione.

Scenari d'uso

Tali tracker di endpoint basati sull'interfaccia vengono utilizzati in questi casi di utilizzo del tunnel SIG/SSE, in cui si desidera tenere traccia di un endpoint URL di applicazioni SaaS conosciuto o di un endpoint URL specifico che desta preoccupazione. Oggi, SSE è lo scenario più comunemente utilizzato da quando l'architettura SASE è stata suddivisa in funzionalità SSE e funzionalità SD-WAN. È quindi possibile scegliere tra ruoli attivi e in standby all'interno dei tunnel IPSec creati da un sito (in questo caso, il controller di dominio). L'utente può scegliere di collegare il tracker nell'interfaccia del tunnel corrispondente.

Nel caso dei provider SSE, ad esempio Cisco Secure Access (di Cisco), viene utilizzato un tracker implicito dell'endpoint configurato per impostazione predefinita. Tuttavia, l'utente può scegliere di creare un tracker di endpoint personalizzato e di collegarlo all'interfaccia del tunnel IPSec. I parametri del tracker endpoint predefinito/implicito utilizzato in SSE sono:

Per Cisco SSE:

Nome Tracker: TrackerPredefinito

Endpoint di cui si tiene traccia: http://service.sig.umbrella.com

Tipo di endpoint: URL_API

Soglia: 300 ms

Multipla: 3

Intervallo 60 sec.

Per ZScaler SSE:

Nome Tracker: TrackerPredefinito

Endpoint di cui si tiene traccia: http://gateway.zscalerthree.net/vpnte

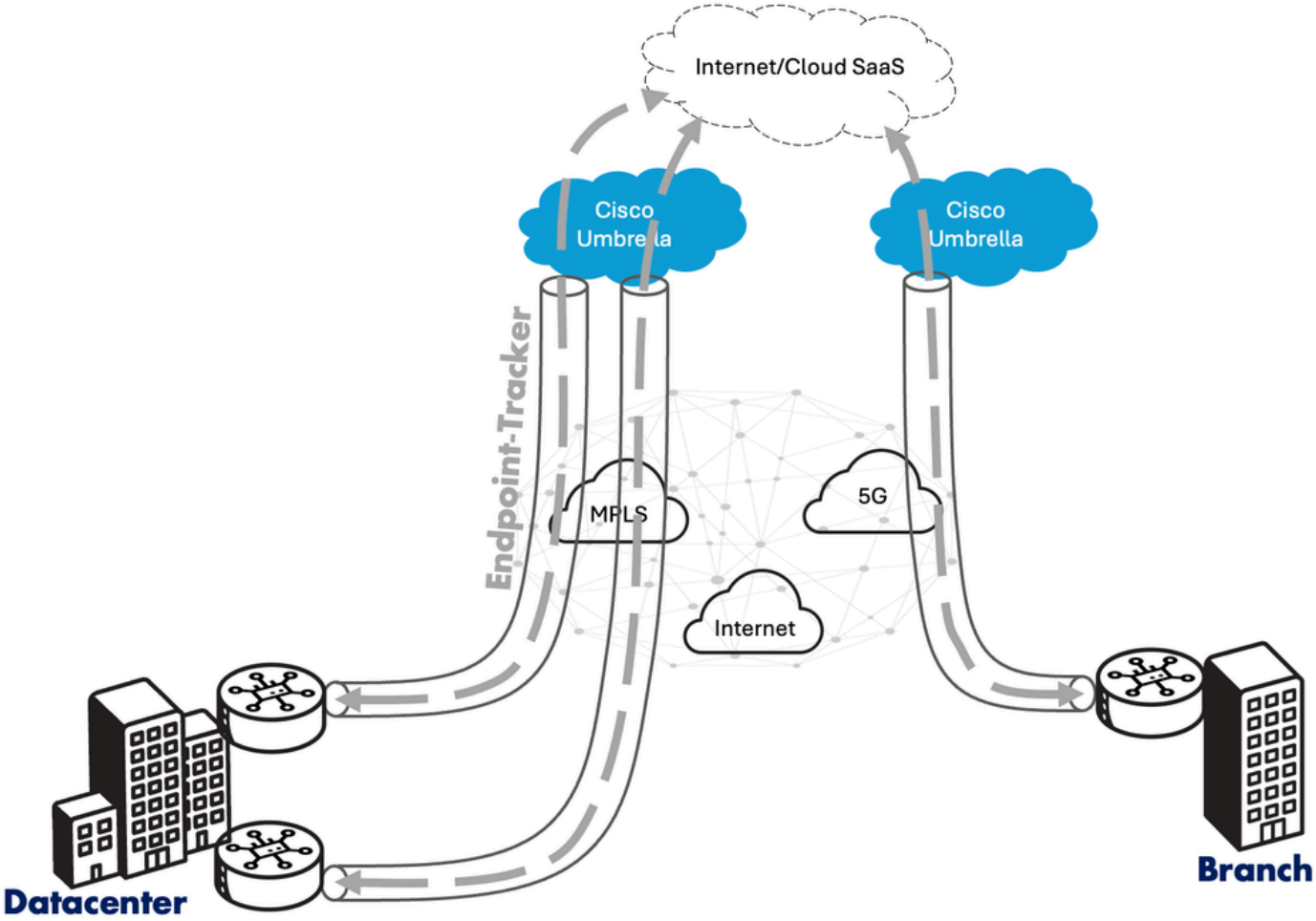
Tipo di endpoint: URL_API

Soglia: 300 ms

Moltiplicatore: 3

Intervallo 60 sec.

Nel caso dei tunnel SIG, non è stato definito alcun tracker di endpoint predefinito/implicito. Pertanto, l'utente deve configurare manualmente un tracker di endpoint basato sull'interfaccia nel caso in cui desideri tenere traccia dell'interfaccia del tunnel IPSec verso il provider-cloud SIG:



Configurazione

Nel caso dei provider SSE, l'utente non deve definire in modo esplicito alcun tracker endpoint (a meno che non lo desideri). Tuttavia, i flussi di lavoro variano in base al tipo di configurazione.

Come prerequisito, è necessario definire le credenziali SIG/SSE Amministrazione > Impostazioni > Servizi esterni > Credenziali cloud:

1. In Credenziali provider cloud, attivare o disattivare l'opzione Umbrella o Cisco SSE (o entrambe).

2. Definire i parametri, ad esempio ID organizzazione, Chiave API, Segreto).

Impostare il gruppo di configurazione Configurazione > Gruppi di criteri > Secure Internet Gateway/Secure Service Edge:

1. Fare clic su Add Secure Internet Gateway o su Add Secure Service Edge.

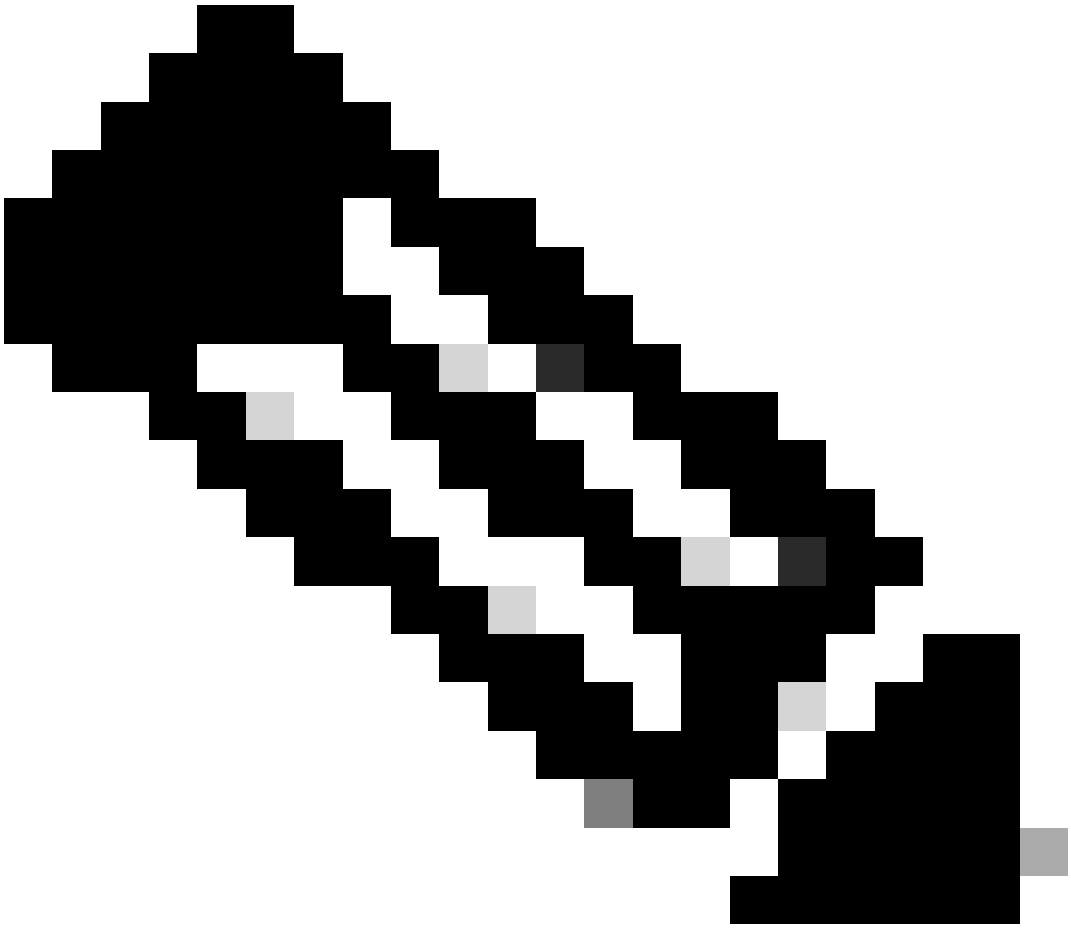
2. Definire un nome e una descrizione.

3. Selezionare uno dei pulsanti di opzione sotto il provider SIG/SSE (Umbrella o Cisco SSE).

4. Nella sezione Tracker, definire l'indirizzo IP di origine usato per originare le sonde di tracciamento.

5. Se si sceglie di definire un rilevatore di endpoint esplicito/personalizzato, fare clic su Aggiungi rilevatore, quindi specificare i parametri per il rilevatore di endpoint (Nome, URL API dell'endpoint, Soglia, Intervallo probe e Moltiplicatore).

6. Nella sezione Configurazione, creare le interfacce tunnel in cui è possibile definire i parametri (ad esempio Nome interfaccia, Descrizione, Tracker, Interfaccia origine tunnel, Primario/secondario datacenter).



> Nota: Nel passaggio 6 viene offerta all'utente la possibilità di connettere l'endpoint tracker definito al rispettivo tunnel IPSec. Si noti che questo campo è facoltativo.

---

7. Nella sezione Alta disponibilità, creare una coppia di interfacce e definire l'interfaccia attiva e l'interfaccia di backup con i rispettivi pesi. Applicare quindi il gruppo di criteri configurato in precedenza agli spigoli rilevanti.

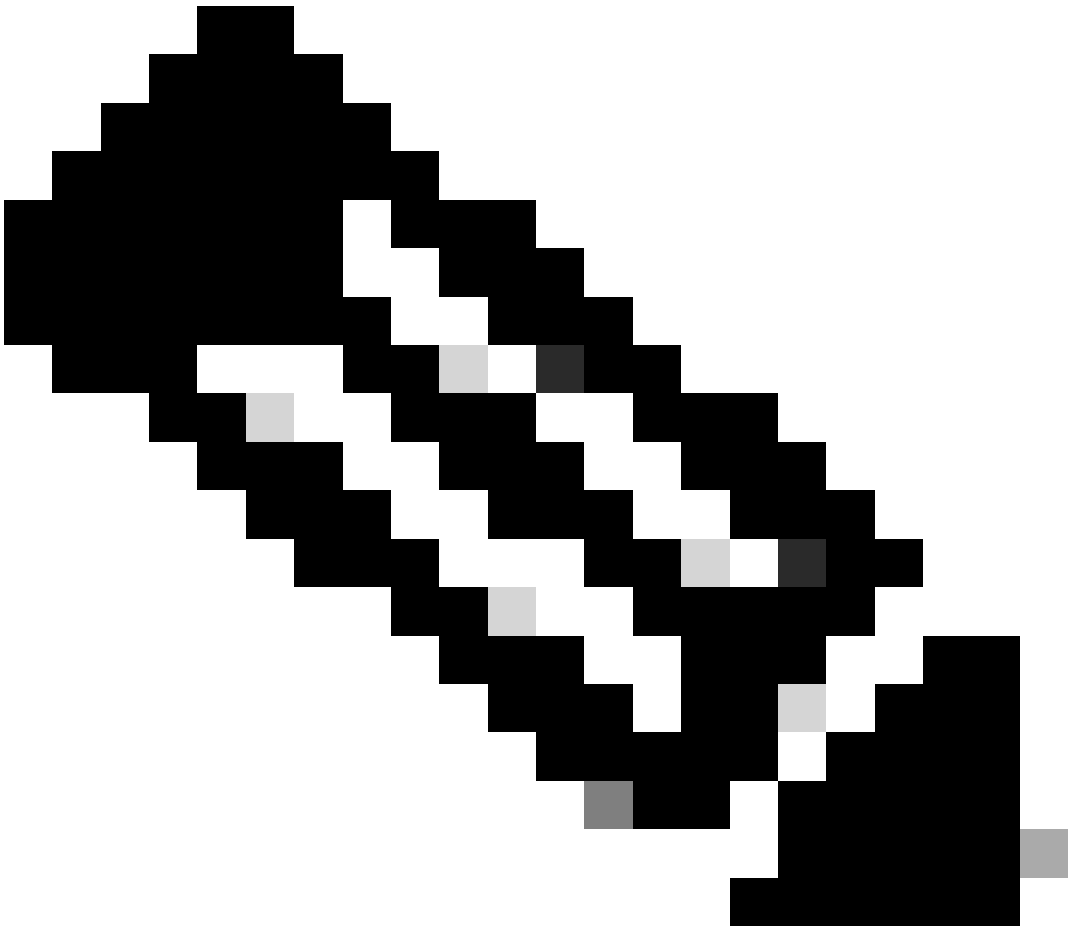
Impostare la configurazione legacy Configurazione > Modelli > Modelli funzionalità > Modello funzionalità Cisco Secure Internet Gateway:

1. Selezionare uno dei pulsanti di opzione sotto SIG Provider (Umbrella, ZScalar o Generic).

2. Nella sezione Tracker (BETA), definire l'indirizzo IP di origine utilizzato per originare le sonde di tracciamento.

5. Se si sceglie di definire un rilevatore endpoint esplicito/personalizzato, fare clic su Nuovo rilevatore e specificare i parametri per il rilevatore endpoint (Nome, URL API dell'endpoint, Soglia, Intervallo e Moltiplicatore).

6. Nella sezione Configurazione, creare le interfacce tunnel (facendo clic su Aggiungi tunnel) in cui è possibile definire i parametri (ad esempio, Nome interfaccia, Descrizione, Tracker, Interfaccia origine tunnel, Primario/secondario datacenter).



> Nota: Nel passaggio 6 viene offerta all'utente la possibilità di connettere l'endpoint tracker definito al rispettivo tunnel IPSec. Si noti che questo campo è facoltativo.

---

7. Nella sezione Alta disponibilità, definire l'interfaccia attiva e l'interfaccia di backup con i rispettivi

pesi.

Dal punto di vista della CLI, le configurazioni hanno il seguente aspetto:

```
(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
!
```

Verifica

Sono disponibili opzioni di verifica per i tracciatori endpoint configurati in modo esplicito.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Applicazioni > Tracker:

Controllare in Individual Tracker e visualizzare le statistiche del tracciatore (Tipi di tracciatore, Stato, Endpoint, Tipo di endpoint, Indice VPN, Nome host, Tempo andata e ritorno) in base al

nome del tracciatore configurato.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Eventi:

Nel caso di flap rilevati sul tracker, i rispettivi log vengono popolati in questa sezione con dettagli come il nome host, il nome del punto di collegamento, il nome del tracker, il nuovo stato, la famiglia di indirizzi e l'ID vpn.

Dalla CLI del perimetro:

```
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
```

Tracker endpoint interfaccia utilizzati per Service Fabric 2.0

Service Fabric 2.0 Tracking, introdotto nella versione 20.13/17.13, è una variante avanzata del service insertion 1.0 tracking, in cui gli utenti possono personalizzare i tracker in misura maggiore. Il comportamento predefinito è mantenuto dalla versione precedente di Service Insertion (1.0), un tracker viene avviato per impostazione predefinita con la definizione di ogni indirizzo di servizio (o indirizzo di inoltro) in una coppia di servizi HA per rx/tx. Con Service Insertion 2.0, invece, l'indirizzo di rilevamento (IP/endpoint sul quale viene eseguito il rilevamento) può essere separato dall'indirizzo di inoltro (di solito l'indirizzo del servizio). Questa operazione viene eseguita utilizzando i tracker degli endpoint personalizzati definiti a livello VPN. Per ulteriori informazioni sui tracker di Service Fabric 2.0, visitare la guida alla configurazione.

Se l'utente sceglie di utilizzare il tracciatore predefinito, le specifiche delle sonde di tracciamento sono:

- Salve: 1 sonda ogni 30 secondi
- Moltiplicatore: 3 volte
- Tipo pacchetto/sonda: ICMP Echo/Echo-reply

Se l'utente sceglie di utilizzare un tracciatore personalizzato, le specifiche delle sonde di

tracciamento sono:

- Salve: 1 sonda ogni 60 secondi
- Moltiplicatore: 3 volte
- Tipo pacchetto/sonda: ICMP Echo-request/risposta

Scenari d'uso

Si applicano anche in questo caso i casi di utilizzo di Service Insertion 1.0 citati nelle sezioni precedenti.

Configurazione

È disponibile il supporto per la configurazione basata sul flusso di lavoro per Service Insertion 2.0, un approccio guidato che consente di semplificare l'esperienza dell'utente, rispettando i passaggi standard del flusso di lavoro del gruppo di configurazione.

1. Definire il gruppo Catena di assistenza - Configurazione nella sezione Configurazione > Inserimento servizi > Definizioni catena di assistenza:

r. Fare clic sul pulsante Aggiungi definizione catena di servizi.

b. Immettere i dettagli relativi al Nome e alla Descrizione del Servizio.

c. Compilare un elenco (selezionandolo dall'elenco a discesa), selezionando Service Type (Tipo di servizio).

2. Definire il gruppo Istanza catena di assistenza - Configurazione nella sezione Configurazione > Inserimento servizi > Configurazioni catena di assistenza:

r. Fare clic su Aggiungi configurazione catena di servizi.

b. Nella fase Definizione catena di servizi, selezionare il pulsante di opzione Seleziona esistente, quindi scegliere il servizio definito in precedenza.

c. Fornire un nome e una descrizione per il passo Avvia configurazione catena di servizi.

d. Nel passo Configurazione catena di servizi per servizi connessi manualmente, selezionare l'ID VPN della catena di servizi.

e. Quindi, per ogni servizio definito nell'istanza della catena di servizi (rappresentata in schede secondarie), in Dettagli servizio specificare il Tipo di allegato (IPv4, IPv6 o Connesso al tunnel).

f. Selezionare la casella di controllo Avanzate. Se è necessario disporre di Use Case di backup attivo/HA (abilitare anche Aggiungi parametri per il manopola Backup) o se è necessario definire un tracciatore endpoint personalizzato (abilitare anche il manopola Tracciatore personalizzato).

g. In caso di scenari in cui il traffico in uscita (tx) raggiunge il servizio tramite un'interfaccia e il traffico di ritorno dal servizio (rx) passa attraverso un'altra interfaccia, attivare il comando Traffic

from service viene ricevuto su un'altra manopola di interfaccia.

h. Con i manopole Advanced e Custom Tracker abilitati, definire l'indirizzo IPv4 del servizio (indirizzo di inoltro), l'interfaccia del router SD-WAN (a cui il servizio è connesso) e l'endpoint del tracciamento (indirizzo di tracciamento). È inoltre possibile modificare i parametri di rilevamento personalizzati, ad esempio intervallo e moltiplicatore, facendo clic sul pulsante Modifica.

i. Ripetere le fasi e), f), g) e h) per ciascun servizio definito successivamente.

3. Collegare l'istanza della catena di servizi al profilo di configurazione del gruppo Edge - Configurazione in Configurazione > Gruppi di configurazione > Profilo di servizio > VPN servizio > Aggiungi funzionalità > Gateway allegati della catena di servizi:

r. Fornire un nome e una descrizione per il pacchetto gateway di allegati della catena di servizi.

b. Selezionare la definizione della catena di servizi definita in precedenza (passo 1).

c. Aggiungere/verificare nuovamente i dettagli come eseguito nel passaggio 2. Per la definizione del tracker, l'unica differenza rispetto al passaggio precedente 2 è che si ha la possibilità di assegnare un nome al tracker e selezionare anche il tipo di tracker (da service-icmp a ipv6-service-icmp).

Dal punto di vista della CLI, le configurazioni hanno il seguente aspetto:

```
!
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
!
```

Verifica

- Su SD-WAN Manager Monitor > Dispositivi > {select Device-Name} > Applicazioni > Tracker:

Controllare in Individual Tracker e visualizzare le statistiche del tracciatore (Tipi di tracciatore, Stato, Endpoint, Tipo di endpoint, Indice VPN, Nome host, Tempo andata e ritorno) in base al nome del tracciatore configurato.

- Su SD-WAN Manager Monitor > Dispositivi > {select Device-Name} > Eventi:

Nel caso di flap rilevati sul tracker, i rispettivi log vengono popolati in questa sezione con dettagli come il nome host, il nome del punto di collegamento, il nome del tracker, il nuovo stato, la famiglia di indirizzi e l'ID vpn.

Dalla CLI del perimetro:

```
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
```

Tracker endpoint con route statica utilizzati per il rilevamento route statica (lato servizio)

Il secondo tipo di rilevatori di endpoint viene definito come rilevatori di endpoint basati su route statica. Come indica il nome stesso, questi tipi di tracker vengono utilizzati principalmente per

tenere traccia dell'indirizzo dell'hop successivo di qualsiasi route statica definita nella VPN sul lato servizio. Per impostazione predefinita, tutti i tipi di route "connessa" e "statica" vengono pubblicizzati nel protocollo OMP. Questo messaggio viene inviato a tutti i siti remoti che contengono la VPN del servizio corrispondente e viene a conoscenza del prefisso di destinazione (dove l'hop successivo punta al TLOC del sito di origine). Il sito di origine è il sito da cui è stata avviata la route statica specifica.

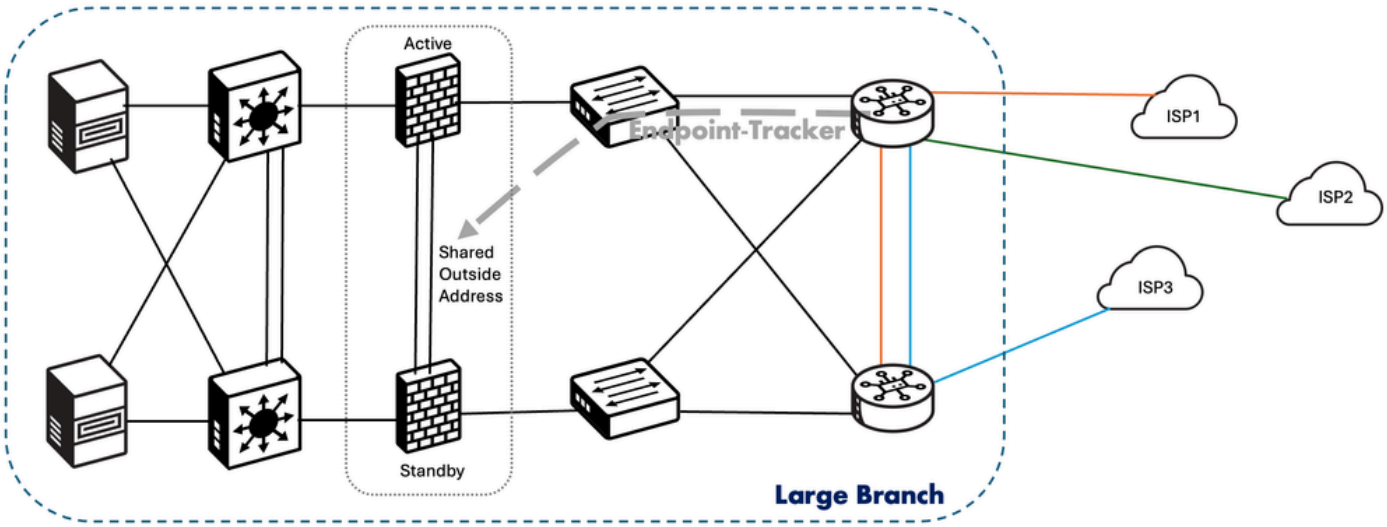
Tuttavia, nel caso in cui l'indirizzo dell'hop successivo nella route statica diventi irraggiungibile, la route non interrompe l'annuncio in OMP. Ciò provocherebbe problemi di traffico che verrebbero intasati per i flussi destinati al sito di origine. Ciò comporta la necessità di collegare un tracciatore alla route statica, per garantire la pubblicità della route statica in OMP SOLO quando l'indirizzo dell'hop successivo è raggiungibile. Questa funzione è stata introdotta nella versione 20.3/17.3 per i tracciatori di endpoint basati su route statica con tipo di indirizzo IP di base. A partire dalla versione 20.7/17.7, è stato aggiunto il supporto per l'invio di sonde di tracciamento solo a porte TCP o UDP specifiche dell'indirizzo IP dell'hop successivo (nei casi in cui si utilizzino firewall per aprire solo alcune porte a scopo di tracciamento). Per ulteriori informazioni sui tracciatori di route statici, visitare la guida alla configurazione.

Il tipo di sonde utilizzato qui è un semplice pacchetto di richiesta echo ICMP. Gli intervalli utilizzati sono i seguenti:

- Salve: 60 secondi
- Holdtime: 180 secondi (poiché #retries è 3 = 3 x 60 secondi)
- Tipo pacchetto/sonda: ICMP Echo/Echo-reply

Scenari d'uso

Questo tipo di rilevatori di endpoint basati su route statica viene utilizzato per il rilevamento lato servizio degli indirizzi dell'hop successivo nelle route statiche. Uno scenario comune di questo tipo sarebbe il monitoraggio dell'indirizzo dell'hop successivo della LAN corrispondente a una coppia di firewall attivo/standby, che condividono l'indirizzo IP esterno in base al quale l'interfaccia esterna svolge il ruolo di firewall "attivo". Nei casi in cui le regole del firewall sembrano essere molto restrittive, in cui solo alcune porte sono aperte per scopi basati su use case, il tracciatore di route statico può essere utilizzato per tracciare la porta TCP/UDP specifica sull'indirizzo IP dell'hop successivo che appartiene all'interfaccia esterna del firewall sul lato LAN.



Configurazione

Per abilitare questa funzionalità, è necessario configurare manualmente i tracciatori di endpoint basati su route statica. Di seguito sono indicati i metodi di configurazione, a seconda del tipo di metodo di configurazione preferito dall'utente.

- Gruppo di configurazione Configurazione > Gruppi di configurazione > Profilo servizio > VPN servizio > Aggiungi funzionalità > Tracker:

1. Fornire il nome, la descrizione e il nome del tracciatore per il nuovo tracciatore (endpoint) da definire.

2. Scegliere il tipo di endpoint, a seconda che si debba solo tenere traccia dell'indirizzo IP dell'hop successivo (scegliere il pulsante di opzione Indirizzo) o anche di porte TCP/UDP specifiche (scegliere il pulsante di opzione Protocollo).

3. Inserire l'indirizzo nel formato indirizzo IP. Immettere anche il protocollo (TCP o UDP) e il numero di porta, nel caso in cui si sia scelto Protocollo come tipo di endpoint nel passaggio precedente.

4. È possibile modificare i valori predefiniti specificati per Intervallo probe, Numero di nuovi tentativi e Limite latenza, se necessario.

- Configurazione > Gruppi di configurazione > Profilo servizio > VPN servizio > Sezione Route:

1. Selezionare il pulsante Aggiungi route statica IPv4/IPv6.

2. Inserire i dettagli, ad esempio l'indirizzo di rete, la subnet mask, l'hop successivo, l'indirizzo e AD.

3. Fare clic sul pulsante Add Next Hop With Tracker.

4. Reimmettere l'indirizzo dell'hop successivo, AD e scegliere dall'elenco a discesa il nome del tracciatore (endpoint) creato in precedenza.

- Configurazione legacy Configurazione > Modelli > Modelli funzionalità > Modello di sistema > Sezione Tracker:

1. Selezionare il pulsante Nuovo Tracker endpoint.

2. Fornire un nome per il nuovo tracker (endpoint) da definire.

3. Modificare il pulsante di scelta Tipo di tracciatore in statico-route.

4. Scegliere il tipo di endpoint, come indirizzo IP dell'hop successivo (pulsante di opzione Scegli indirizzo IP).

5. Inserire l'indirizzo IP dell'endpoint in formato indirizzo IP.

6. È possibile modificare i valori predefiniti specificati per Intervallo probe, Numero di nuovi tentativi e Limite latenza, se necessario.

- Configurazione > Modelli > Modelli funzionalità > Cisco VPN (SOLO sul lato servizio) > Sezione Route IPv4/IPv6:

1. Selezionare il pulsante Nuova route IPv4/IPv6.

2. Inserire i dettagli, ad esempio Prefisso, Gateway.

3. Fare clic sul pulsante Aggiungi hop successivo con tracciatore.

4. Reimmettere l'indirizzo dell'hop successivo, AD (Distanza) e immettere manualmente il nome del tracciatore (endpoint) creato in precedenza.

Dal punto di vista della CLI, le configurazioni hanno il seguente aspetto:

```
(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
!
```

Verifica

Sono disponibili due aree di verifica per i tracciatori degli endpoint configurati in modo esplicito.

- Su SD-WAN Manager Monitor > Dispositivi > {select Device-Name} > Tempo reale:

1. In Opzioni dispositivo, digitare "Informazioni su Endpoint Tracker".

2. Controllare in Individual Tracker (Attach Point Name) e visualizzare le statistiche del tracker (stato del tracker, nome del record del tracker associato, latenza in mx dal dispositivo all'endpoint, timestamp ultimo aggiornamento) in base al nome del tracker configurato.

- Su Monitor SD-WAN Manager > Dispositivi > {select Device-Name} > Eventi:

Nel caso di flap rilevati sul tracciatore, i rispettivi log vengono compilati in questa sezione con dettagli quali nome host, nome del punto di collegamento, nome del tracciatore, nuovo stato, famiglia di indirizzi e ID vpn.

Dalla CLI del perimetro:

```
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]
```

Tracker oggetti interfaccia utilizzati per il rilevamento VRRP

Object Tracker sono tracker progettati per il consumo in modalità autonoma (casi di utilizzo). Questi tracker hanno casi di utilizzo che variano da interface/tunnel tracking basato su VRRP a service-VPN NAT tracking.

Nei casi di utilizzo del rilevamento VRRP, lo stato VRRP viene determinato in base allo stato del collegamento del tunnel. Se il tunnel o l'interfaccia è inattivo sul VRRP primario, il traffico viene indirizzato al VRRP secondario. Il router VRRP secondario nel segmento LAN diventa il VRRP primario per fornire il gateway per il traffico sul lato servizio. Questo caso d'uso è applicabile solo alla VPN di servizio e consente di eseguire il failover del ruolo VRRP sul lato LAN in caso di guasto sulla sovrapposizione SD-WAN (interfaccia o tunnel nel caso di SSE). Per collegare i tracciatori ai gruppi VRRP, è possibile utilizzare SOLO i tracciatori di oggetti (non i tracciatori di endpoint). Questa funzione è stata introdotta dalla versione 20.7/17.7 per i bordi SD-WAN di Cisco Catalyst.

Non ci sono sonde usate qui dal tracciatore. Al contrario, utilizza lo stato del protocollo di linea per decidere sullo stato del tracciatore (su/giù). Non ci sono intervalli di reazione nei tracciatori basati sul protocollo di linea dell'interfaccia - nel momento in cui l'interfaccia/protocollo di linea del tunnel diventa DOWN, anche lo stato del tracciato viene portato su DOWN. A seconda dell'azione di arresto o decremento, il gruppo VRRP eseguirà nuovamente la convergenza. Per ulteriori informazioni sui tracker dell'interfaccia VRRP, visitare la guida alla configurazione.

Scenari d'uso

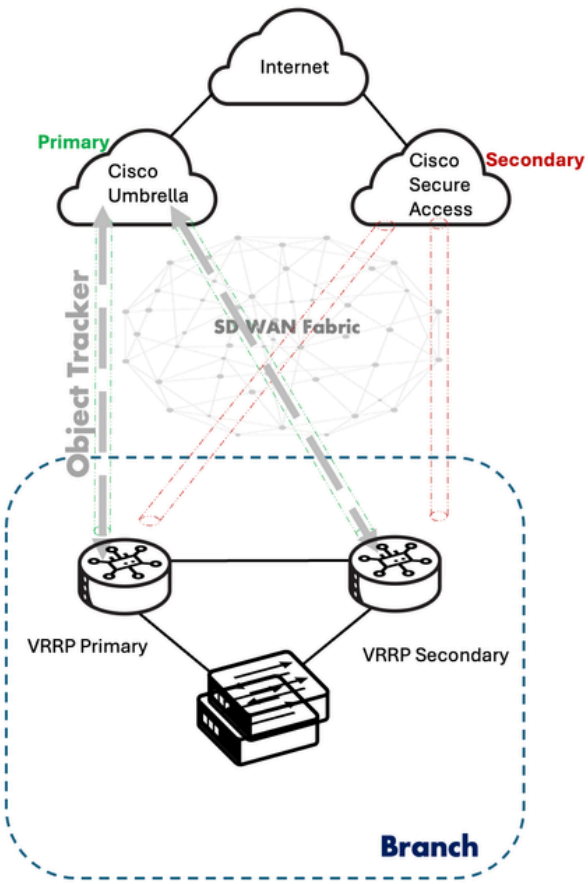
Esistono più casi di utilizzo basati sui criteri richiesti per l'implementazione del rilevamento dell'interfaccia basato su VRRP. Al momento, le due modalità supportate sono (i) l'interfaccia (ossia qualsiasi interfaccia tunnel collegata a un TLOC locale) o (ii) l'interfaccia SIG (relativa alle interfacce tunnel SIG). In ogni caso, la parte monitorata è il protocollo di linea dell'interfaccia.

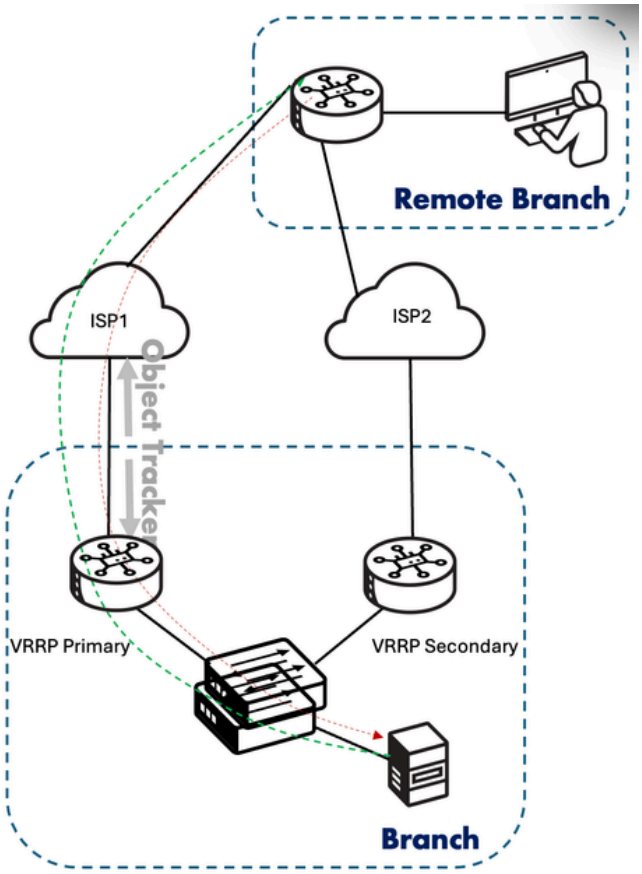
Doppio router con Internet: L'oggetto traccia è associato al gruppo VRRP. Nel caso in cui l'oggetto del tracker (in questo caso l'interfaccia del tunnel SIG) si guasti, viene inviata una notifica al router primario VRRP per attivare la transizione di stato da primario a di backup e il router di backup diventa primario. Questo cambiamento di stato può essere influenzato o attivato da due tipi di

operazioni:

1. Decremento: Quando la priorità VRRP per l'interfaccia su cui è configurato il VIP VRRP viene ridotta o diminuita di un certo valore, nel caso in cui lo stato dell'oggetto traccia passi da UP a DOWN.
2. Shutdown: Questo è un metodo in cui il processo VRRP viene arrestato sull'interfaccia applicata, nel caso in cui lo stato dell'oggetto traccia passi da UP a DOWN. Questo metodo non è consigliato in casi di utilizzo in cui sono presenti istanze di inoltro asimmetrico.

Preferenza modifica TLOC: per evitare il traffico asimmetrico proveniente da altri siti SDWAN nel sito in cui il protocollo VRRP viene eseguito sulla VPN del servizio, la preferenza TLOC del router primario VRRP viene aumentata di 1 se configurata. È anche possibile modificare questo valore nei gruppi di configurazione. In questo modo, il traffico tra la WAN e la LAN viene attratto dal router principale VRRP. Il traffico da LAN a WAN viene attratto dal meccanismo VRRP del primario VRRP. Questa funzionalità è indipendente dal tracker dell'interfaccia VRRP. Questo è un comando opzionale (tloc-change-pref) dal punto di vista della CLI.





Configurazione

La configurazione degli object tracker viene eseguita tramite i modelli di sistema nella configurazione legacy e quindi collegando l'object tracker al rispettivo gruppo VRRP in base al modello di funzionalità dell'interfaccia Ethernet service-VPN. Nel gruppo Configurazione, questo meccanismo è stato semplificato ottenendo direttamente un'opzione per aggiungere il tracciatore oggetti al rispettivo profilo di servizio Ethernet Interface profile. Di seguito sono riportati i modi per configurarlo, in base al tipo di metodo di configurazione preferito dall'utente.

- Gruppo di configurazione Configurazione > Gruppi di configurazione > Profilo di servizio > Interfaccia Ethernet > Aggiungi funzionalità > Object Tracker:

1. Fornire un nome e una descrizione per il nuovo tracciatore oggetti definito.
2. Selezionare il tipo di tracciatore (tra Interfaccia e SIG).
3. Alloca un ID Tracker oggetti.
4. Specificare il nome dell'interfaccia (a seconda dell'opzione scelta al passaggio 2).

- Configurazione > Gruppi di configurazione > Profilo di servizio > Interfaccia Ethernet > Sezione VRRP:

1. In Impostazioni IPv4, fare clic su Add VRRP IPv4.
2. Definire un ID gruppo VRRP e fornire una priorità locale per questa interfaccia ethernet sul lato servizio.
3. Specificare l'indirizzo IP virtuale (VIP) del VRRP.
4. Abilitare la manopola Modifica preferenza TLOC e fornire anche il valore Modifica preferenza TLOC (per gestire il routing asimmetrico).
5. Fare clic su Aggiungi oggetto di rilevamento VRRP.
6. In Associa Tracker oggetti, selezionare dall'elenco a discesa di Tracker oggetti (in base al nome) creato in precedenza
7. Scegliere un'azione Tracker (Shutdown o Decrement).
8. Immettere il valore di decremento (a seconda dell'opzione scelta al punto 7).

- Configurazione legacy Configurazione > Modelli > Modelli funzionalità > Sistema > Sezione Tracker:

1. Fare clic sul pulsante Nuovo Tracker oggetti.
2. Selezionare il tipo di tracciatore (tra Interfaccia e SIG).
3. Alloca un ID oggetto.
4. Fornire il nome dell'interfaccia (a seconda dell'opzione scelta nel passaggio 2).

- Configurazione > Modelli > Interfaccia Ethernet (appartenente al lato servizio) > Sezione VRRP:

1. Fare clic sul pulsante Nuovo VRRP.
2. Definire un ID gruppo VRRP e fornire una priorità locale (viene scelto un valore predefinito opzionale di 100) per questa interfaccia ethernet sul lato servizio.
3. Specificare l'indirizzo IP virtuale (VIP) del VRRP.
4. Abilitare la manopola Modifica preferenza TLOC e fornire anche il valore di modifica della preferenza TLOC (per gestire il routing asimmetrico).
5. In Tracciatore oggetti, fare clic su Aggiungi oggetto di rilevamento.
6. Immettere l'ID Tracker oggetti (definito nel modello di sistema).
7. Scegliere un'azione Tracker (Shutdown o Decrement).
8. Immettere il valore di decremento (a seconda dell'opzione scelta al punto 7).

Dal punto di vista della CLI, le configurazioni hanno il seguente aspetto:

```
(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
!
```

Verifica

Sono disponibili due opzioni per verificare in modo esplicito gli object tracker configurati per i casi di utilizzo del protocollo VRRP.

- Su SD-WAN Manager Monitor > Dispositivi > {select Device-Name} > Tempo reale:

1. In Opzioni periferica, digitare "Informazioni VRRP".

2. Controllare in Gruppo singolo VRRP (ID gruppo) e visualizzare le statistiche del tracker (Nome prefisso traccia, Stato traccia, Ora discontinuità e Ora ultima modifica stato) in base agli ID di Tracker oggetti configurati.

- Su Monitor SD-WAN Manager > Dispositivi > {select Device-Name} > Eventi:

In caso di modifica dello stato rilevata nel Tracker oggetti, lo stato del gruppo VRRP corrispondente a cui è associato viene modificato. I rispettivi log vengono popolati in questa sezione (con il Nome come VRRP Group State Change) con dettagli quali nome host, numero, ID GRP, tipo di indirizzo, nome, stato-gruppo VRRP, motivo-modifica stato e ID VPN.

Dalla CLI del perimetro:

```
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)
```

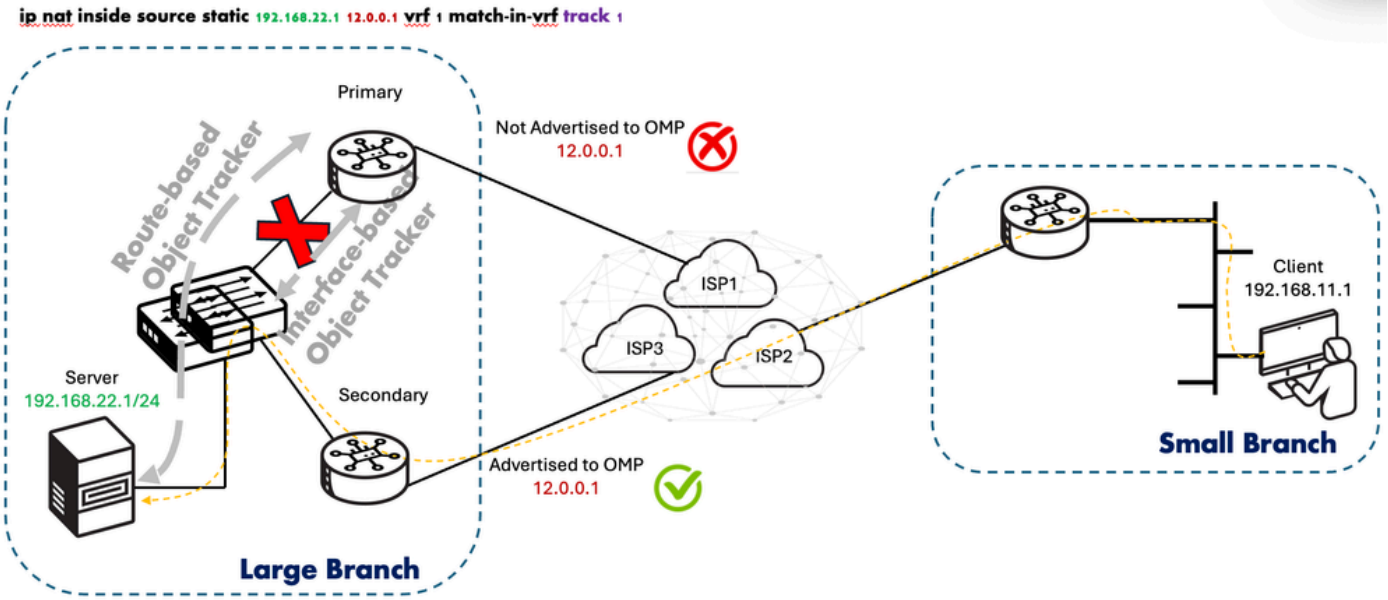
Tracker oggetti interfaccia/route utilizzati per il rilevamento NAT Service-VPN

Il Service-side NAT Object Tracker è una funzione introdotta nella versione 20.8/17.8, in cui l'indirizzo globale interno utilizzato in service-VPN NAT (all'interno di NAT statico e all'interno di NAT dinamico) viene pubblicizzato in OMP solo se (i) l'indirizzo locale interno risulta raggiungibile OPPURE (ii) il protocollo di linea dell'interfaccia LAN/service-side è attivo in base al rilevamento oggetti collegato. Pertanto, i tipi di individuazione oggetti che è possibile utilizzare sono (i) route o (ii) interface. A seconda dello stato del prefisso LAN o dell'interfaccia LAN, gli annunci di route NAT tramite OMP vengono aggiunti o rimossi. È possibile visualizzare i log eventi in Cisco SD-WAN Manager per controllare quali annunci di route NAT vengono aggiunti o rimossi.

Non ci sono sonde usate qui dal tracciatore. Al contrario, usa (i) la presenza di una voce di routing nella tabella di routing O (ii) lo stato del protocollo di linea per decidere sullo stato del tracker (attivo/inattivo). Non ci sono intervalli di reazione in presenza di tracciatori basati su una voce di routing o su un protocollo di linea dell'interfaccia - nel momento in cui la voce di routing o il protocollo della linea dell'interfaccia diventa inattivo, anche lo stato della traccia viene portato allo stato INATTIVO. Immediatamente l'indirizzo globale interno utilizzato nell'istruzione NAT associata a Object Tracker non viene più annunciato in OMP. Per ulteriori informazioni sui tracker NAT della VPN del servizio, visitare la guida alla configurazione.

Scenari d'uso

Se un'interfaccia LAN o un prefisso LAN non è attivo, il tracciatore oggetti NAT del lato servizio si interrompe automaticamente. È possibile visualizzare i registri eventi in Cisco SD-WAN Manager per controllare quali annunci di route NAT vengono aggiunti o rimossi. Nel caso di utilizzo successivo, il client deve accedere al server nella filiale di grandi dimensioni. Tuttavia, il problema si verifica in situazioni in cui il percorso che punta al server sui bordi della diramazione di grandi dimensioni (in HA) viene rimosso OPPURE quando l'interfaccia del lato LAN (lato servizio) si interrompe su un bordo della diramazione di grandi dimensioni. In tali situazioni, quando si applica il NAT sul lato servizio con object tracker, assicurarsi che il traffico in entrata dal client sia sempre indirizzato al bordo corretto nella filiale di grandi dimensioni controllando l'annuncio di indirizzo globale interno in OMP. Nel caso in cui tale controllo non venga applicato sull'annuncio del percorso in OMP, il traffico finisce per essere bloccato a causa della non raggiungibilità dal rispettivo margine al server nella filiale di grandi dimensioni.



Configurazione

La configurazione dei tracciatori di oggetti viene eseguita tramite modelli di sistema nella configurazione Legacy, quindi collegando il tracciatore di oggetti alla rispettiva istruzione NAT (all'interno statica o dinamica interna) nel modello della funzionalità service-VPN. Nel gruppo Configurazione, questo meccanismo è stato semplificato ottenendo direttamente un'opzione per aggiungere il tracciatore oggetti al rispettivo profilo di servizio Ethernet Interface profile. Di seguito sono riportati i modi per configurarlo, in base al tipo di metodo di configurazione preferito dall'utente.

- Gruppo di configurazione Configurazione > Gruppi di configurazione > Profilo servizio > Aggiungi funzionalità > Object Tracker:

1. Fornire un nome e una descrizione per il nuovo tracciatore oggetti definito.
2. Selezionare il tipo di Tracker (tra Interfaccia e route).
3. Alloca un ID Tracker oggetti.
4. Fornire il nome dell'interfaccia O il percorso IP, la maschera IP della route e la VPN (a seconda dell'opzione scelta nel passaggio 2).

- Configurazione > Gruppi di configurazione > Profilo servizio > Sezione NAT:

1. Creare un pool NAT (obbligatorio per l'attivazione di SNAT) facendo clic sul pulsante Aggiungi pool NAT.

2. Fornire i dettagli del pool NAT, ad esempio il nome del pool Nat, la lunghezza del prefisso, l'inizio dell'intervallo, la fine dell'intervallo e la direzione.

3. Passare a NAT statico nella stessa sezione e fare clic sul pulsante Aggiungi nuovo NAT statico. È inoltre possibile scegliere di collegare il tracciatore oggetti al pool dinamico NAT.

4. Fornire dettagli quali IP origine, IP origine convertita e direzione NAT statica.

5. Nel campo Associa Tracker oggetto, scegliere dall'elenco a discesa il Tracker oggetto creato in

precedenza.

- Configurazione legacy Configurazione > Modelli > Modelli funzionalità > Sistema > Sezione Tracker:

1. Fare clic sul pulsante Nuovo Tracker oggetti.
2. Selezionare il tipo di Tracker (tra Interfaccia e route).
3. Alloca un ID oggetto.
4. Fornire il nome dell'interfaccia OR Route IP, Route IP Mask e VPN (a seconda dell'opzione scelta nel passaggio 2).

- Configurazione > Modelli > Cisco VPN (appartenente al lato servizio) > Sezione NAT:

1. Creare un pool NAT (obbligatorio per l'attivazione di SSNAT) facendo clic sul pulsante Nuovo pool NAT.

2. Fornire i dettagli del pool NAT, ad esempio il nome del pool NAT, la lunghezza del prefisso del pool NAT, l'inizio dell'intervallo del pool NAT, la fine dell'intervallo del pool NAT e la direzione NAT.

3. Passare a NAT statico nella stessa sezione e fare clic sul pulsante Nuovo NAT statico. È inoltre possibile scegliere di collegare il tracciatore oggetti al pool dinamico NAT.

4. Fornire dettagli quali l'indirizzo IP di origine, l'indirizzo IP di origine tradotto e la direzione NAT statica.

5. Sotto il campo Aggiungi Tracker oggetti, immettere il nome del Tracker oggetti creato in precedenza.

Dal punto di vista della CLI, le configurazioni hanno il seguente aspetto:

```
(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
!
```

Lo scenario SSNAT prevede che gli utenti applichino criteri dati per abbinare il traffico sia in entrata che in uscita nei flussi NAT.

Verifica

Sono disponibili due aree di verifica degli object tracker configurati in modo esplicito per i casi di utilizzo NAT.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Tempo reale:

1. In Device Options (Opzioni dispositivo), digitare "IP NAT Translation".

2. Controllare in Traduzione NAT individuale e visualizzare le statistiche della voce (indirizzo/porta locale interno, indirizzo/porta globale interno, indirizzo/porta locale esterno, indirizzo/porta globale esterno, ID VRF, nome VRF e protocollo) in base agli ID di Object Tracker configurati.

- Su SD-WAN Manager: Monitor > Dispositivi > {select Device-Name} > Eventi:

In caso di modifica dello stato rilevata nel tracciatore oggetti corrispondente alla route NAT eliminata in OMP, vengono visualizzati gli eventi denominati "NAT Route Change", che contengono dettagli quali il nome host, il tracciatore oggetti, l'indirizzo, la maschera, il tipo di route e l'aggiornamento. In questo caso, l'indirizzo e la maschera sono mappati all'indirizzo globale interno come configurato nell'istruzione NAT statica.

Dalla CLI del perimetro:

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).