Entender a usabilidade e os casos de uso do Catalyst SD-WAN Tracker

Contents

Introdução

Este documento descreve as redes de sobreposição empresarial Catalyst SD-WAN, a usabilidade do rastreador e os casos de uso.

Informações de Apoio

As redes de sobreposição corporativa Catalyst SD-WAN normalmente interagem com uma grande variedade de cargas de trabalho, aplicativos e serviços externos. qualquer um pode estar localizado na nuvem, no data center/hubs ou em filiais remotas. O plano de controle da SD-WAN é responsável por anunciar rotas para esses serviços na camada de maneira escalável. Em situações em que aplicações e serviços críticos se tornam inalcançáveis ao longo de um caminho específico, os operadores de rede normalmente devem ser capazes de detectar esses eventos e redirecionar o tráfego do usuário para caminhos mais apropriados para evitar o blackholing de tráfego indefinido. Para detectar e corrigir esses tipos de falhas de rede, o plano de controle do Catalyst SD-WAN conta com rastreadores para monitorar a integridade dos serviços externos e fazer alterações de roteamento conforme apropriado.

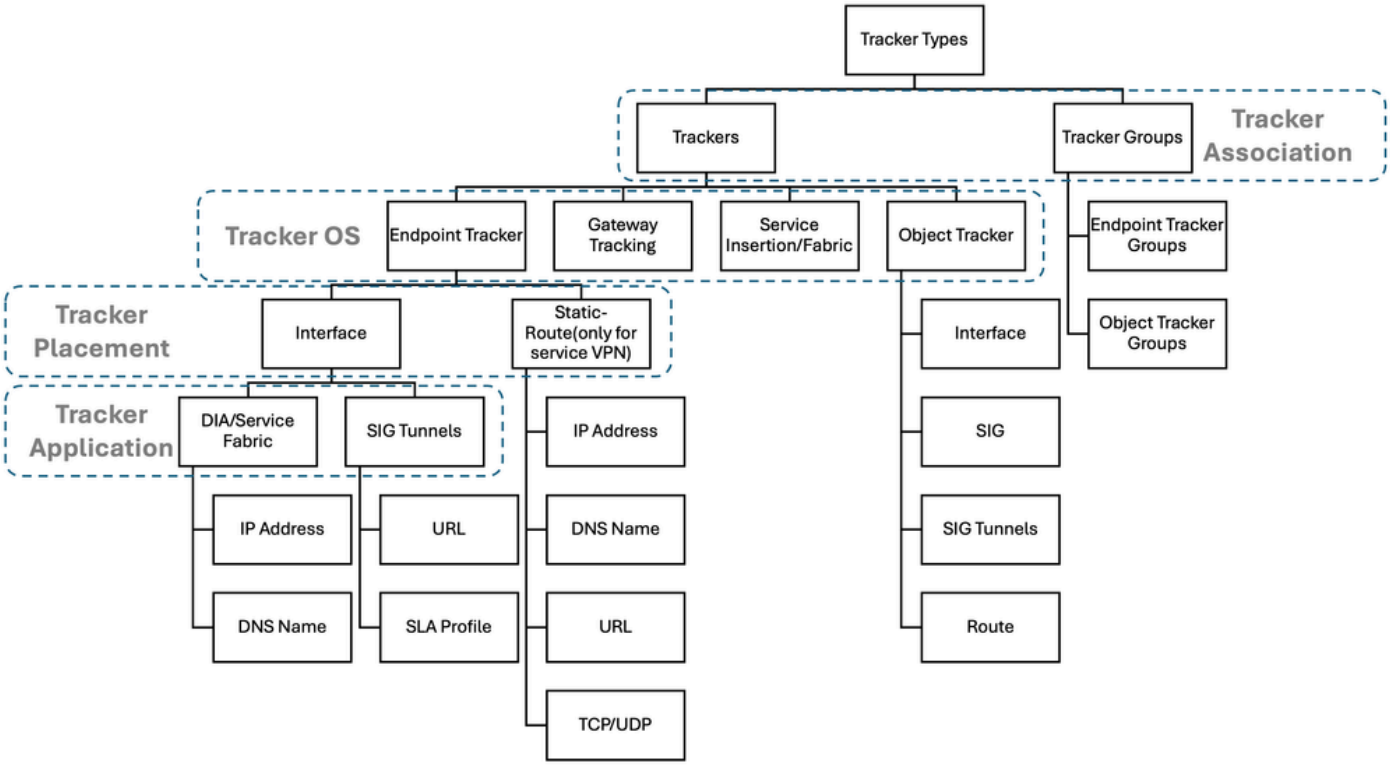
Um rastreador é um mecanismo de detecção de acessibilidade do plano de controle que envia pacotes de sondagem para um endpoint específico e notifica sobre alterações de status de acessibilidade (para cima ou para baixo) do endpoint para módulos interessados. Os rastreadores são projetados como uma abstração escalável de alto nível do recurso SLA IP nativo do Cisco IOS-XE®, que pode formar uma variedade de sondas (incluindo HTTP, ICMP e DNS). Quando um rastreador notifica um módulo cliente de uma alteração de status, esse módulo pode tomar a ação apropriada para evitar o blackholing de tráfego, como instalar ou desinstalar uma rota ou um conjunto de rotas. As aplicações atuais de rastreadores nas soluções SD-WAN e SD-Routing incluem, mas não se limitam a: Os rastreadores DIA (Direct Internet Access), SIG (Secure Internet Gateway), rastreadores de serviços, rastreadores de rotas estáticas, grupos de rastreadores, etc.

Para criar redes altamente disponíveis que sejam resilientes a falhas de serviço, é crucial entender quando usar cada tipo de configuração/modelo de rastreador. O objetivo deste artigo é explicar onde e como cada tipo de rastreador é usado. Os vários rastreadores são abordados aqui, assim como o caso de uso primário de cada rastreador, e os fluxos de trabalho de configuração básica para implementar cada solução. Por fim, este artigo introduz uma introdução de advertências gerais envolvendo rastreadores no Cisco IOS-XE®.

Este artigo estabelece uma distinção entre as soluções endpoint-tracker (específico para SD-WAN e SD-Routing) e object tracker (IOS-XE nativo), que abordam diferentes casos de uso.

Tipos de rastreadores

Este gráfico fornece uma breve visão geral de todos os tipos de rastreadores disponíveis na solução Cisco Catalyst SD-WAN:



A partir do gráfico anterior, há quatro áreas onde os rastreadores podem ser classificados: Associação de Rastreador, SO de Rastreador, Posicionamento de Rastreador e Aplicativo de Rastreador. A próxima seção descreve cada classificação:

1. Associação do rastreador: Esta classificação descreve se um rastreador é um único rastreador ou um grupo rastreador. O Cisco Catalyst SD-WAN suporta o uso de vários rastreadores em um grupo (até 2 no momento da gravação) e o status geral do grupo de rastreadores é determinado por um operador booleano AND ou OR. Os exemplos incluem um grupo endpoint-tracker ou um grupo object tracker.
2. SO do rastreador: Esta classificação descreve o sistema operacional Cisco IOS-XE® ou o modo em que o rastreador é suportado. Os roteadores Cisco Catalyst IOS-XE suportam dois modos de operação:

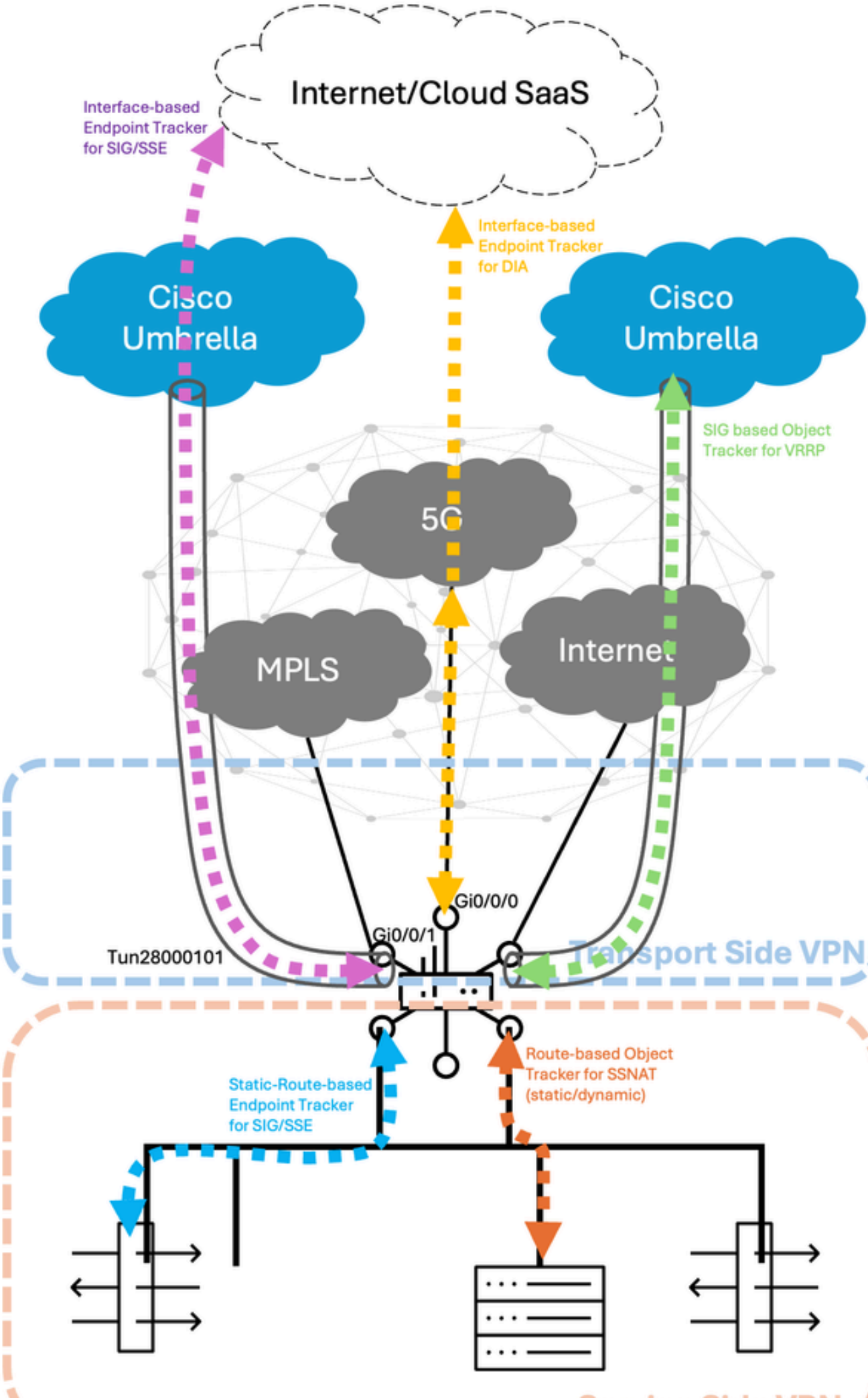
- Modo autônomo e
- Modo de controlador.

Todos os recursos endpoint-tracker e gateway tracking são destinados a casos de uso de modo de controlador (SD-WAN), enquanto o rastreador de objetos é destinado a casos de uso de modo autônomo (SD-Routing).

3. Colocação do rastreador: Esta classificação descreve o local em que o rastreador está configurado. Atualmente, o Cisco Catalyst SD-WAN suporta a aplicação de rastreadores em interfaces, rotas estáticas ou serviços.

4. Aplicativo de Rastreamento: Esta classificação descreve os casos de uso e recursos de alto nível suportados pelo Cisco Catalyst SD-WAN. Embora existam várias áreas de aplicação de rastreadores, algumas delas incluem: Acesso direto à Internet (DIA), Gateway de Internet Seguro (SIG), Borda de Serviço Segura (SSE), rastreamento de VPN no Lado do Serviço, etc.

Aqui está uma representação visual do tráfego de sondagem do rastreador através de VPNs de serviço/transporte para vários casos de uso em um Cisco Catalyst SD-WAN Edge (que também pode ser chamado de 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

configuradas em plataformas de borda de SD-WAN na VPN do lado do transporte. Por padrão, isso é ativado nas configurações básicas de perfil do sistema (Gateway padrão de rastreamento) no Gerenciador Catalyst SD-WAN. Isso ajuda a monitorar continuamente o endereço do próximo salto especificado em cada rota estática padrão na VPN de transporte, para garantir o failover de link/rota, no caso de falha de acessibilidade para o próximo salto (que também é chamado de gateway, daí o nome gateway-tracking). Para saber mais sobre rastreamento de gateway, visite o guia de configuração.

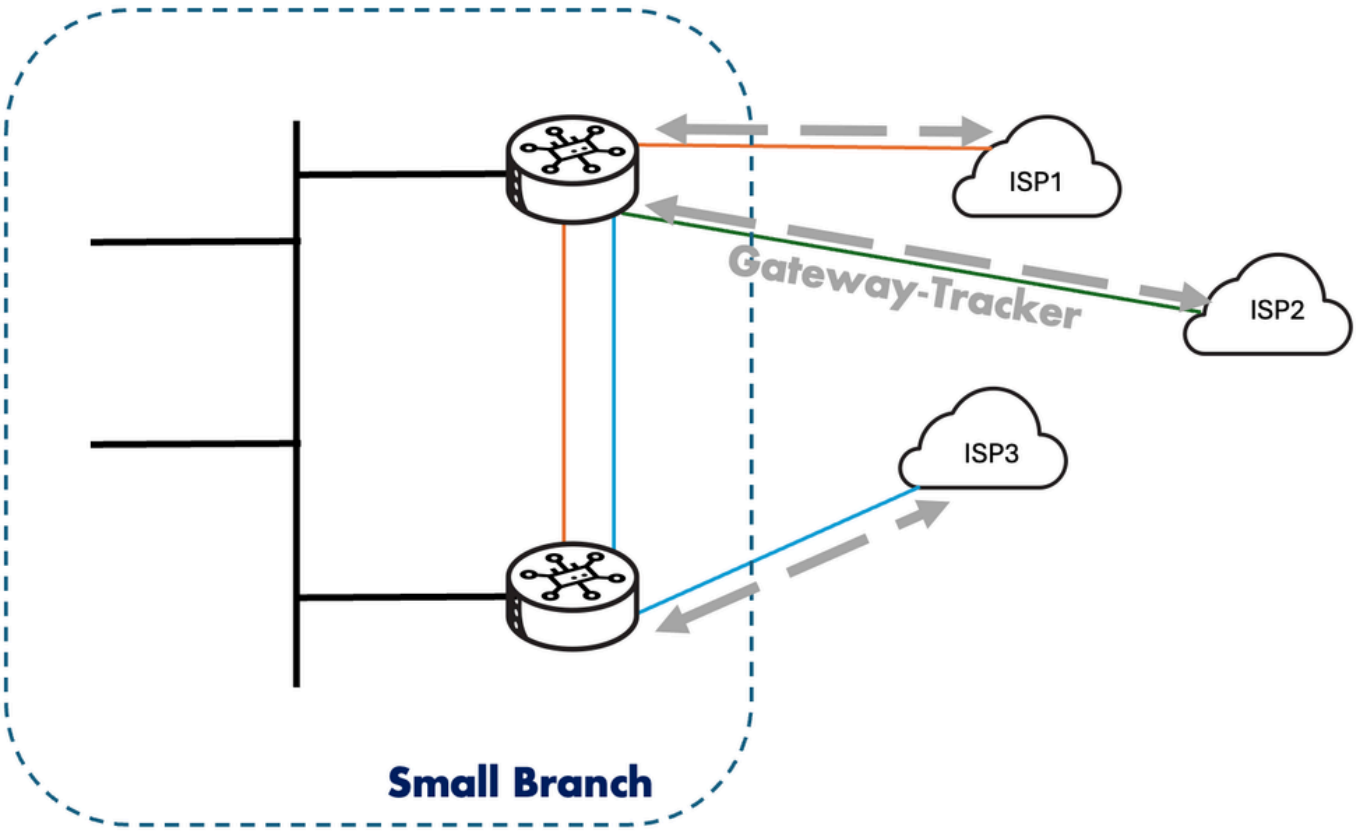
Os tipos de testes usados aqui são pacotes inundados unicast desconhecidos de solicitação ARP. Os intervalos usados são:

- Saudação: 10 segundos
- Tempo de suspensão: 100 segundos
- Tipo de pacote/sonda: ARP

Junto com o rastreamento de gateway, também é usado o rastreamento de transporte em bordas SD-WAN para verificar o caminho roteado entre o dispositivo local e um Cisco Catalyst SD-WAN Validator. Isso é feito com o uso de sondas ICMP em intervalos regulares de 3s. Isso é configurado usando a palavra-chave "track-transport" no modo de configuração do sistema SD-WAN. Isso ajuda no monitoramento regular da conexão DTLS com o Cisco Catalyst SD-WAN Validator a partir da borda da WAN respectiva. Para saber mais sobre rastreamento de transporte, visite o guia de configuração.

Casos de uso

O Rastreamento de Gateway é um recurso que é implicitamente configurado por padrão em SD-WAN para todas as rotas estáticas padrão que pertencem à VPN de transporte ou à Tabela de Roteamento Global (GRT). O uso do recurso nem sempre se origina do ponto de vista da configuração do modelo do Gerenciador, mas também pode evoluir a partir de rotas estáticas padrão recebidas/adquiridas nos cenários de uso de um servidor DHCP com opções #3, #81 e assim por diante.



Configuração

Aplicado por padrão no Cisco Catalyst SD-WAN:

```
!
system


 track-transport
 track-default-gateway


!
```

Verificação

Estas são as maneiras de verificar isso de acordo com a configuração Legada e o grupo de

Configuração:

- Grupo de configuração: Configuração > Grupos de configuração > Perfil do sistema > Subperfil básico > seção Configurações de controle > Rastrear gateway padrão (padrão:ON)
- Configuração antiga: Configuração > Modelos > Modelos de recurso > Modelo do sistema > Seção avançada > Rastreamento de gateway (padrão:ON)

Rastreamento de Service Insertion 1.0 e Service Fabric 2.0

O rastreamento da inserção de serviço 1.0 foi introduzido na versão 20.3/17.3 e é um recurso destinado a garantir que o endereço de serviço (ou endereço de encaminhamento) esteja acessível ou disponível. Essas informações ajudam a Borda a adicionar ou retirar dinamicamente as informações do próximo salto da política de Controle/Dados. Com a configuração da Inserção de serviço 1.0, o rastreador (ou endereço de rastreamento) é ativado por padrão para o endereço de serviço. Com base nisso, o endereço de encaminhamento e o endereço de serviço são os mesmos na versão 1.0. Mesmo que os rastreadores de serviço sejam configurados automaticamente com serviços, esses rastreadores podem ser desabilitados usando o comando no track-enable ou desabilitando o botão do rastreador na configuração de grupo de configuração/Legado. Como essas são as duas únicas operações possíveis (ativar/desativar) com rastreadores associados a serviços sob a Inserção de Serviço 1.0, não há nenhum parâmetro adicional que possa ser ajustado (como threshold, multipler, interval). O tipo de testes usados aqui são pacotes de solicitação de eco ICMP.

Para saber mais sobre o rastreamento da inserção de serviço 1.0, visite o guia de configuração. Os intervalos padrão usados no rastreamento da inserção de serviço 1.0 são:

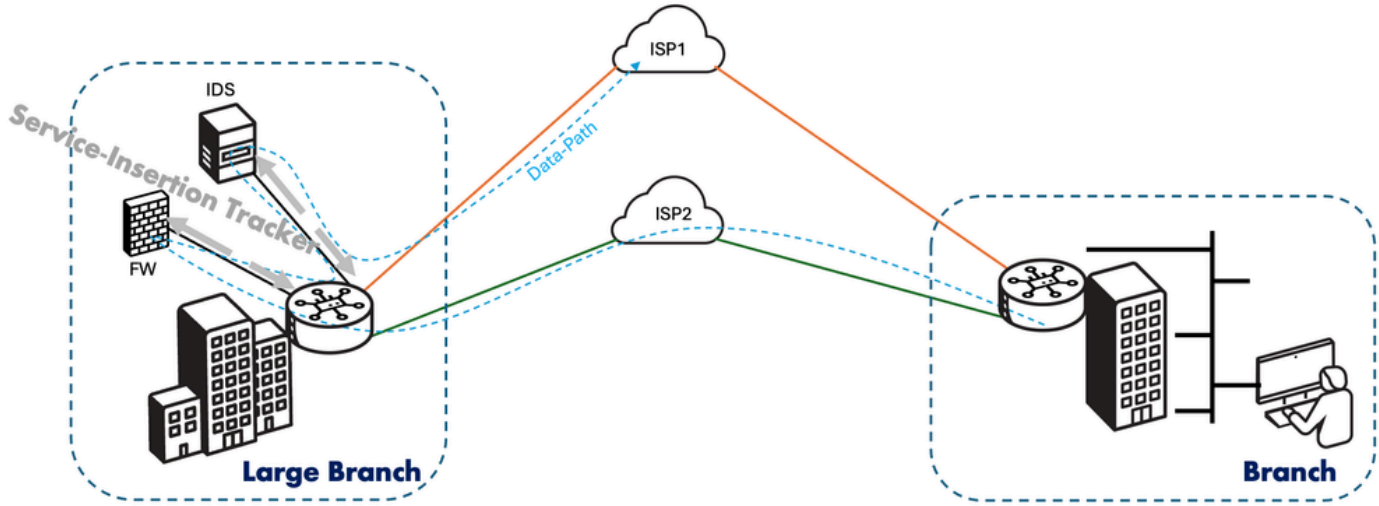
- Intervalo de sondagem: 5 sondas a cada 60 segundos
- Multiplicador: 5 vezes
- Tipo de pacote/sonda: Eco/resposta de eco ICMP

O Rastreamento do Service Fabric 2.0 vem como parte da oferta de recurso de Inserção de Serviço 2.0 no Cisco Catalyst SD-WAN, introduzida a partir da versão 20.13/17.13. Nessa nova variante de inserção de serviço, o método padrão usado pelos perfis e modelos de configuração ainda é ter um rastreador implícito apontando para cada endereço de serviço definido (ou endereço de encaminhamento) em um par de HA de serviço por interface rx/tx. No entanto, com o Service Fabric 2.0, agora você pode dividir o endereço de encaminhamento do endereço de rastreamento. Isso pode ser feito simplesmente definindo rastreadores de endpoint separados para rastrear um endereço de endpoint diferente do próprio endereço de serviço. Este tópico será mais detalhado nas próximas seções.

Casos de uso

O principal caso de uso para rastreadores de serviço é o monitoramento escalável da acessibilidade do serviço, particularmente para encadeamento de serviços. O encadeamento de serviços pode ser implantado em uma rede que consiste em várias VPNs, onde cada VPN representa uma função ou organização diferente, para garantir que o tráfego entre as VPNs flua

por um firewall. Por exemplo, em uma rede de campus grande, o tráfego interdepartamental pode passar por um firewall, enquanto o tráfego interdepartamental pode ser roteado diretamente. O encadeamento de serviços pode ser visto em cenários onde um operador deve satisfazer a conformidade regulatória, como o padrão de segurança de dados do setor de cartões de pagamento (PCI DSS), onde o tráfego de PCI deve fluir através de firewalls em um data center centralizado ou hub regional:



Configuração

As configurações são as mesmas do fluxo de trabalho normal para configurar a Inserção de serviço 1.0 em SD-WAN. Os rastreadores de inserção de serviço 1.0 seriam habilitados por padrão em todos os endereços de serviço.

- Grupo de configuração: Configuração > Grupos de configuração > Perfil de serviço > VPN de serviço > Seção de serviço:

1. Clique no botão Add Service.

2. Escolha um Tipo de Serviço.

3. Inscreva o Endereço de Serviço (máximo de 4 possíveis, separados por vírgula).

4. Verifique se o botão Rastreamento está ativado (por padrão). Ela pode ser desativada, se necessário.

- Configuração antiga: Configuration > Templates > Feature Templates > Cisco VPN (serviço) > Service section:

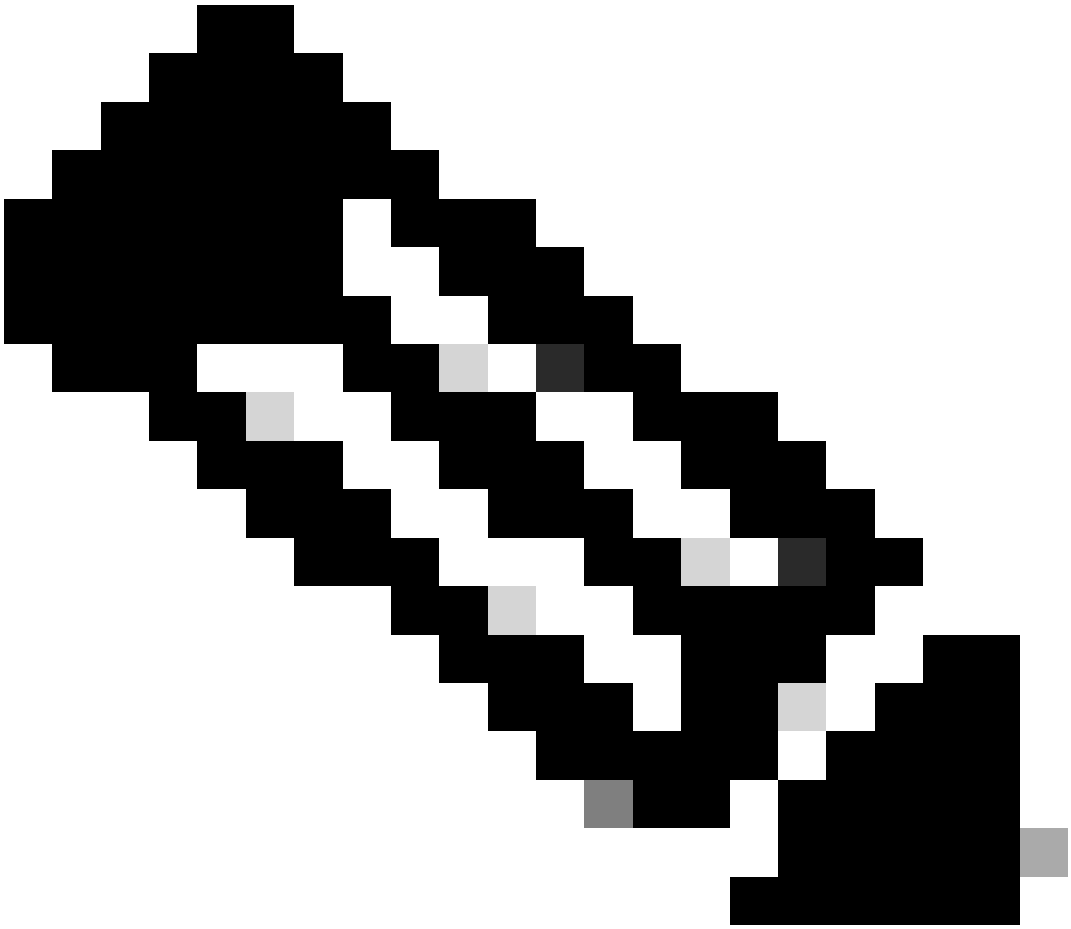
1. Clique no botão New Service

2. Escolha um Tipo de Serviço.

3. Inscreva o Endereço de Serviço (máximo de 4 possíveis, separados por vírgula).

4. Verifique se o botão Rastreamento está ativado (por padrão). Ela pode ser desativada, se

necessário.



Note: No momento em que a Etapa 3 é configurada (do grupo de Configuração ou da configuração Legada), o rastreador é iniciado automaticamente para os vários endereços de serviço definidos

Do ponto de vista da CLI, a configuração para a inserção de serviço 1.0 é exibida da seguinte forma:

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

Verificação

As etapas de verificação se estendem às etapas semelhantes seguidas como parte dos rastreadores de endpoint baseados em interface usados nas seções anteriores.

Há duas opções de verificação do rastreador de endpoint explicitamente configurado.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Aplicativos > Rastreador:

Verifique em Controlador individual e visualize as estatísticas do rastreador (tipos de rastreador, status, endpoint, tipo de endpoint, índice de VPN, nome do host, tempo de ida e volta) com base no seu nome de rastreador configurado.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Eventos:

No caso de flaps detectados no rastreador, os respectivos logs seriam preenchidos nesta seção com detalhes como nome do host, nome do ponto de anexo, nome do rastreador, novo estado, família de endereços e id de vpn.

Na CLI da borda:

```
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
```

Rastreadores de ponto final de interface usados para DIA

Os rastreadores de endpoint NAT DIA são designados principalmente para monitorar o alcance de aplicativos por meio de uma interface NAT DIA em plataformas de borda SD-WAN.

Para casos de uso de Acesso Direto à Internet (DIA), os rastreadores NAT DIA são usados principalmente para rastrear a interface do lado do transporte e acionar um failover para outra interface do lado do transporte disponível ou através de túneis de sobreposição SD-WAN (usando

a política de dados). Este recurso foi introduzido a partir da versão 20.3/17.3 e a opção de recurso de recuo NAT está disponível a partir da versão 20.4/17.4. Se o rastreador determinar que a Internet local não está disponível através da interface NAT DIA, o roteador retira a rota NAT da VPN de serviço e reencaminha o tráfego com base na configuração de roteamento local. O rastreador continua a verificar periodicamente o status do caminho para a interface. Quando ele detecta que o caminho está funcionando novamente, o roteador reinstala a rota NAT para a Internet. Para saber mais sobre rastreadores DIA, visite o guia de configuração.

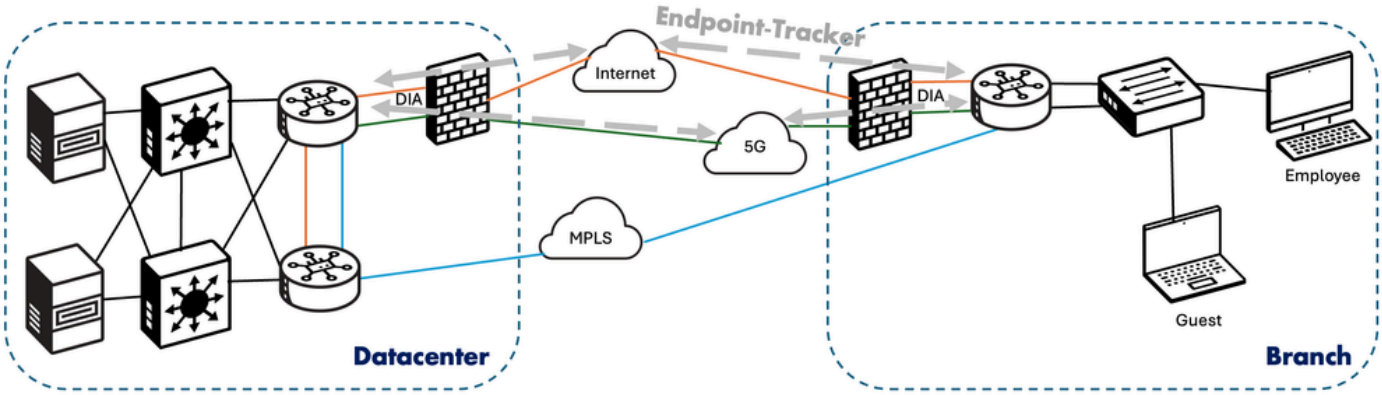
Na definição do rastreador, você pode optar por fornecer um endereço IP de um endpoint acessível por meio da interface NAT DIA (configurada como "endpoint-ip") OU fornecer um FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) para o endpoint (configurado como "endpoint-dns-name").

O tipo de sondas usado aqui é um pacote de solicitação HTTP, muito semelhante a uma pilha de PDU de solicitação de API HTTP. Os intervalos usados são:

- Intervalo de sondagem: 60 segundos
- Multiplicador: 180 segundos (já que #retries é 3 = 3 x 60 segundos)
- Tipo de pacote/sonda: HTTP

Casos de uso

O DIA é frequentemente implantado como uma otimização em filiais para evitar o backhaul para um data center de qualquer tráfego de filial destinado à Internet. No entanto, quando o DIA nas filiais é usado, qualquer falta de alcance nas rotas do NAT DIA ainda precisa retornar a caminhos alternativos para evitar a retenção de dados e a perda de serviço. Para locais que desejam usar fallback para DC (via sobreposição de SD-WAN usando fallback de NAT) no caso de falha de breakout de DIA local. Aproveite esses rastreadores de endpoint baseados em interface nas interfaces compatíveis com DIA nas bordas da filial para detectar falhas e iniciar um failover para o caminho de backup/DC. Dessa forma, a alta disponibilidade do serviço de Internet é alcançada com o mínimo de interrupção na empresa, ao mesmo tempo em que se otimiza o tráfego de Internet com DIA:



Configuração

Esses rastreadores de endpoint baseados em interface devem ser configurados manualmente

para ativar esse conjunto de recursos. Estas são as maneiras de configurá-lo, dependendo do tipo de método de configuração preferido pelo usuário.

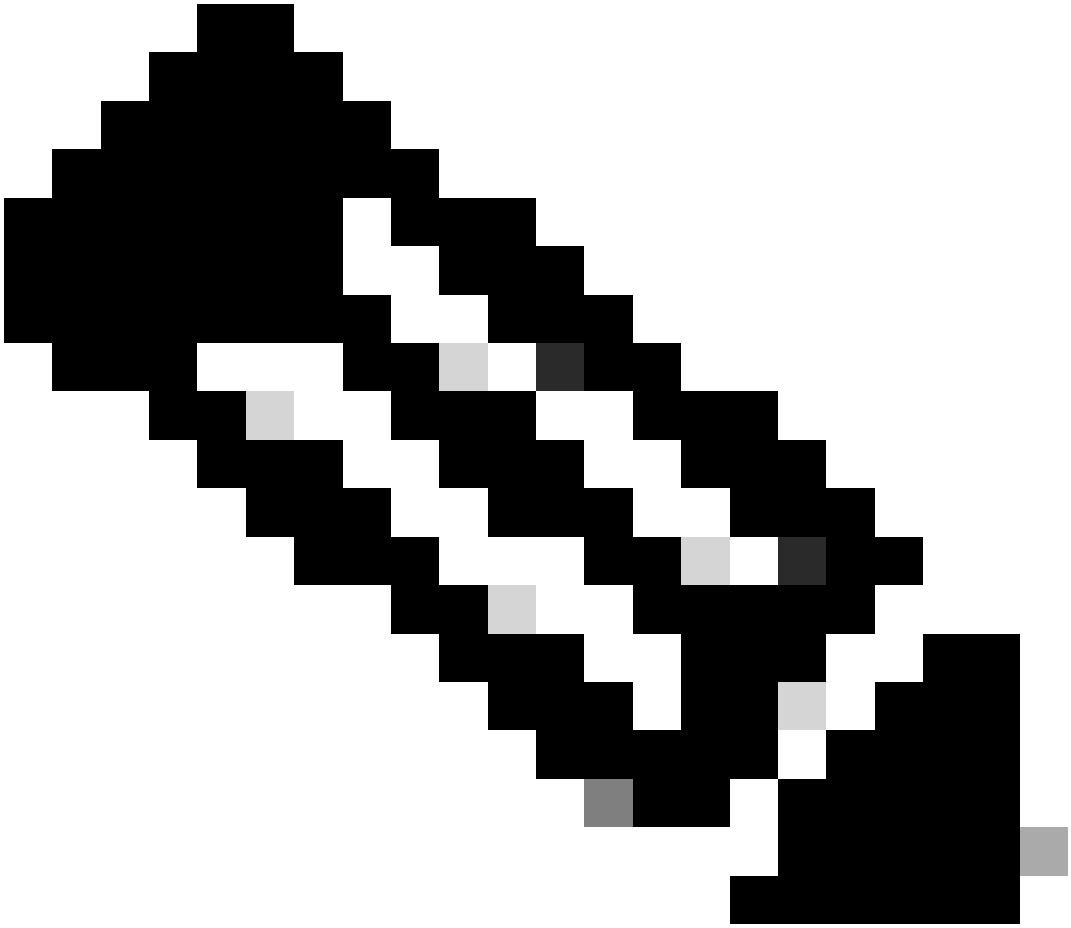
- Grupo de configuração: Configuração > Grupos de configuração > Perfil de transporte e gerenciamento > Interface Ethernet > Adicionar recurso > Rastreador:

1. Defina um nome de rastreador de ponto final.

2. Escolha um tipo de rastreador de ponto final (entre HTTP-padrão e ICMP).

Nota: O tipo de rastreador de endpoint ICMP foi introduzido a partir da versão 20.13/17.13.

3. Selecione o Ponto Final (entre IP-padrão do Ponto Final e Nome DNS do Ponto Final).



Note: Se o Nome DNS do ponto de extremidade for escolhido, verifique se um servidor DNS ou um servidor de nome válido está definido no VPN/VRF de transporte usando o perfil de configuração de VPN de transporte.

---

4. Insira o endereço ou o nome DNS (FQDN) para onde as sondas do rastreador devem ser enviadas (o formato depende da etapa anterior).

5. (Opcional) Você pode optar por alterar o Intervalo de Sondagem (default = 60 segundos) e o Número de Repetições (default = 3 vezes) para acelerar o tempo de detecção de falha.

- Configuração antiga:

Etapa 1. Definição do rastreador de endpoint baseado em interface: Configuração > Modelos > Modelos de recurso > Modelo do sistema > seção Rastreador:

1. Na subseção Rastreadores, selecione o botão Novo Rastreador de Ponto Final.

2. Defina um nome de rastreador de ponto final.

3. Escolha o Tipo de Rastreador (entre interface-default e rota estática) como interface, uma vez que os casos de uso de DIA são de interesse aqui.

4. Escolha o Tipo de Ponto Final (entre Endereço IP - padrão e Nome DNS).

5. Insira o Endereço IP do Ponto Final ou o Nome DNS do Ponto Final para onde as sondas do rastreador devem ser enviadas (o formato depende da etapa anterior).

6. (Opcional) Você pode optar por alterar o Limite de sondagem (padrão = 300 ms), Intervalo (padrão = 60 segundos) e Multiplicador (padrão = 3 vezes).

Etapa 2. Aplique o Rastreador de Ponto Final Baseado em Interface a uma interface na seção VPN de transporte: Modelos > Modelos de Recurso > Cisco VPN Interface Ethernet > Avançado:

1. Insira o nome do Rastreador de Ponto Final definido na Etapa 1 anterior no campo Rastreador.

Do ponto de vista da CLI, as configurações são assim:

```
(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
!
```

Verificação

Há duas opções de verificação de rastreadores de endpoint configurados explicitamente.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Aplicativos > Rastreador:

Verifique em Controlador individual e visualize as estatísticas do rastreador (tipos de rastreador, status, endpoint, tipo de endpoint, índice de VPN, nome do host, tempo de ida e volta) com base no nome do rastreador configurado.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Eventos:

No caso de flaps detectados no rastreador, os respectivos logs seriam preenchidos nesta seção com detalhes como nome do host, nome do ponto de anexo, nome do rastreador, novo estado, família de endereços e id de vpn.

Na CLI da borda:

```
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

Rastreadores de ponto final de interface usados para túneis SIG/SSE

Quando rastreadores de endpoint estão sendo usados para casos de uso de Túnel SIG/SSE, isso indica principalmente que a empresa está procurando uma oferta de pilha de segurança baseada em nuvem que é facilmente disponibilizada hoje em dia usando a ajuda de provedores de Secure Internet Gateway (SIG) ou Secure Service Edge (SSE), como Cisco, Cloudflare, Netskope, ZScalar e assim por diante. Os túneis SIG e SSE são parte do modelo de implantação de segurança de nuvem, no qual a filial usa a nuvem para fornecer as soluções de segurança necessárias. O caso de uso Túneis SIG foi a oferta inicial de integração do Cisco Catalyst SD-WAN com esses provedores SIG (a partir da versão 20.4/17.4), no entanto, com a evolução das ofertas de segurança fornecidas em nuvem - o caso de uso SSE foi introduzido (a partir da versão 20.13/17.13) para cobrir casos de uso com provedores como Cisco (via Cisco Secure Access) e ZScalar.

A TI exige uma abordagem confiável e explícita para proteger e conectar-se com agilidade. Agora é comum fornecer aos funcionários remotos acesso direto a aplicativos em nuvem, como Microsoft 365 e Salesforce, com segurança adicional. A demanda por redes e segurança oferecidas em nuvem se expande diariamente à medida que fornecedores, parceiros, dispositivos da Internet das Coisas (IoT), etc., exigem acesso à rede. A convergência das funções de rede e segurança mais próximas aos dispositivos finais, na borda da nuvem, é conhecida como um modelo de serviço chamado Cisco SASE. O Cisco SASE combina funções de rede e segurança fornecidas em nuvem para fornecer acesso seguro a aplicativos para todos os usuários ou dispositivos, de qualquer lugar e a qualquer momento. O Secure Service Edge (SSE) é uma abordagem de segurança de rede que ajuda as organizações a melhorar a postura de segurança de seu ambiente de trabalho, reduzindo a complexidade para usuários finais e departamentos de TI. Para saber mais sobre rastreadores de Túnel SIG/SSE, visite o guia de configuração.

Casos de uso

Esses rastreadores de endpoint baseados em interface são usados em casos de uso de Túnel SIG/SSE, nos quais você deseja controlar um endpoint de URL de aplicativo SaaS bem conhecido ou um endpoint de URL específico que seja motivo de preocupação. Atualmente, o SSE é o cenário mais usado desde que a arquitetura SASE foi dividida em funcionalidades de núcleo SSE e funcionalidades SD-WAN. Em seguida, você deseja escolher entre as funções ativa e standby dentro dos túneis IPSec criados a partir de um site (neste caso, o DC). O usuário tem a opção de anexar o rastreador na respectiva interface de túnel.

No caso de provedores SSE, como o Cisco Secure Access (da Cisco) - um rastreador de endpoint implícito é usado e configurado por padrão. No entanto, o usuário tem a opção de criar um rastreador de endpoint personalizado e conectá-lo à interface de túnel IPSec. Os parâmetros

do rastreador de ponto final padrão/implícito usados no SSE são:

Para o Cisco SSE:

Nome do Controlador: RastreadorPadrão

Ponto de extremidade sendo rastreado: http://service.sig.umbrella.com

Tipo de ponto final: URL_API

Limite: 300 ms

Multiplicar: 3

Intervalo: 60 s

Para ZScaler SSE:

Nome do Controlador: RastreadorPadrão

Ponto de extremidade sendo rastreado: http://gateway.zscalerthree.net/vpnte

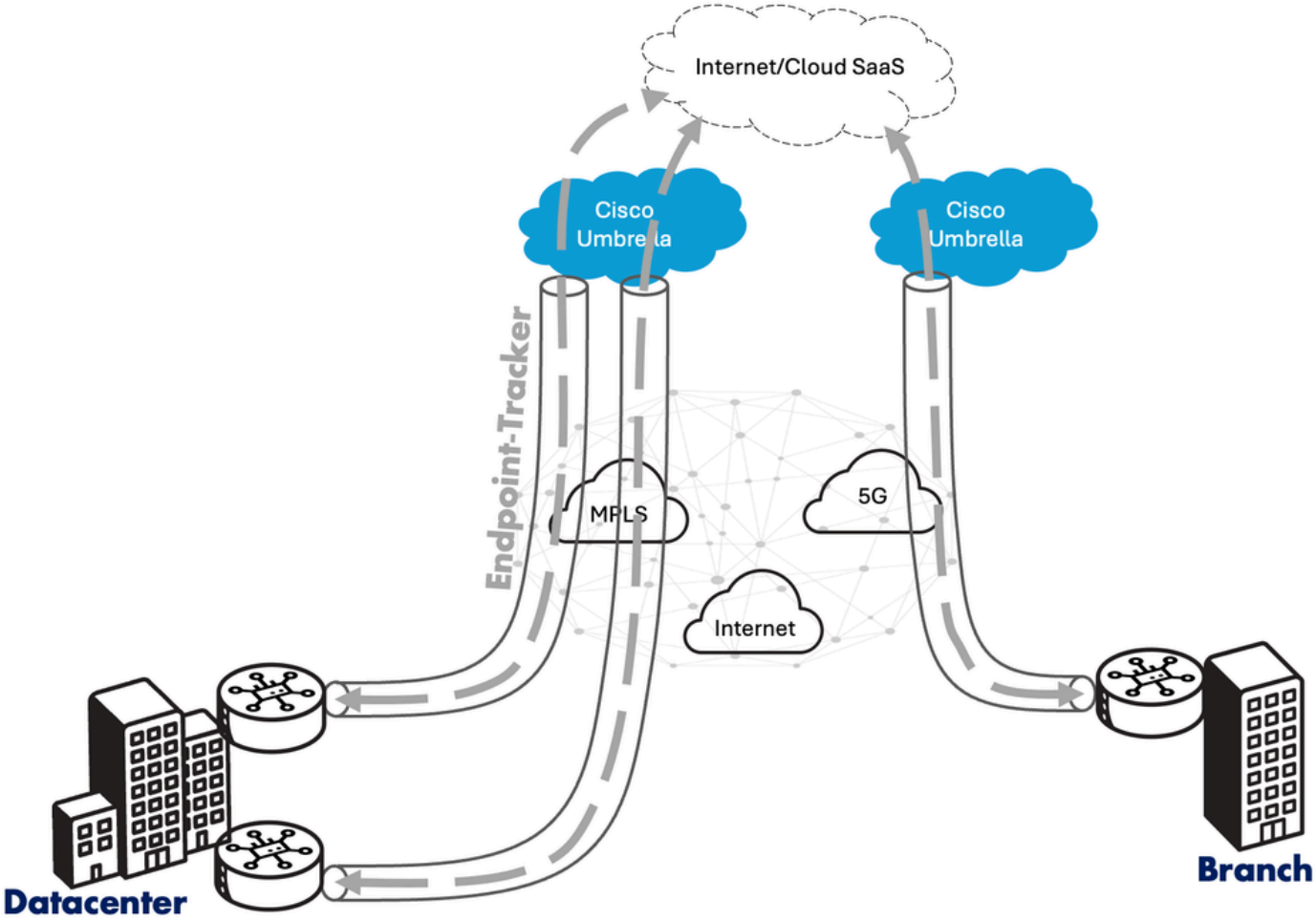
Tipo de endpoint: URL_API

Limite: 300 ms

Multiplicador: 3

Intervalo: 60 s

No caso de Túneis SIG, não há rastreador de endpoint padrão/implícito definido. Assim, o usuário precisa configurar manualmente um rastreador de endpoint baseado em interface caso deseje rastrear a interface de túnel IPSec em direção à nuvem do provedor SIG:



Configuração

No caso de provedores SSE, o usuário não precisa definir nenhum rastreador de endpoint explicitamente (a menos que desejado). No entanto, os fluxos de trabalho são diferentes com base no tipo de configuração.

Como pré-requisito, você deve definir as credenciais SIG/SSE Administração > Configurações > Serviços Externos > Credenciais da Nuvem:

1. Em Cloud Provider Credentials, alterne a opção de Umbrella ou Cisco SSE (ou ambos).

2. Defina os parâmetros, como ID da Organização, Chave API, Segredo).

Defina o grupo de configuração Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge:

1. Clique em Add Secure Internet Gateway ou em Add Secure Service Edge.

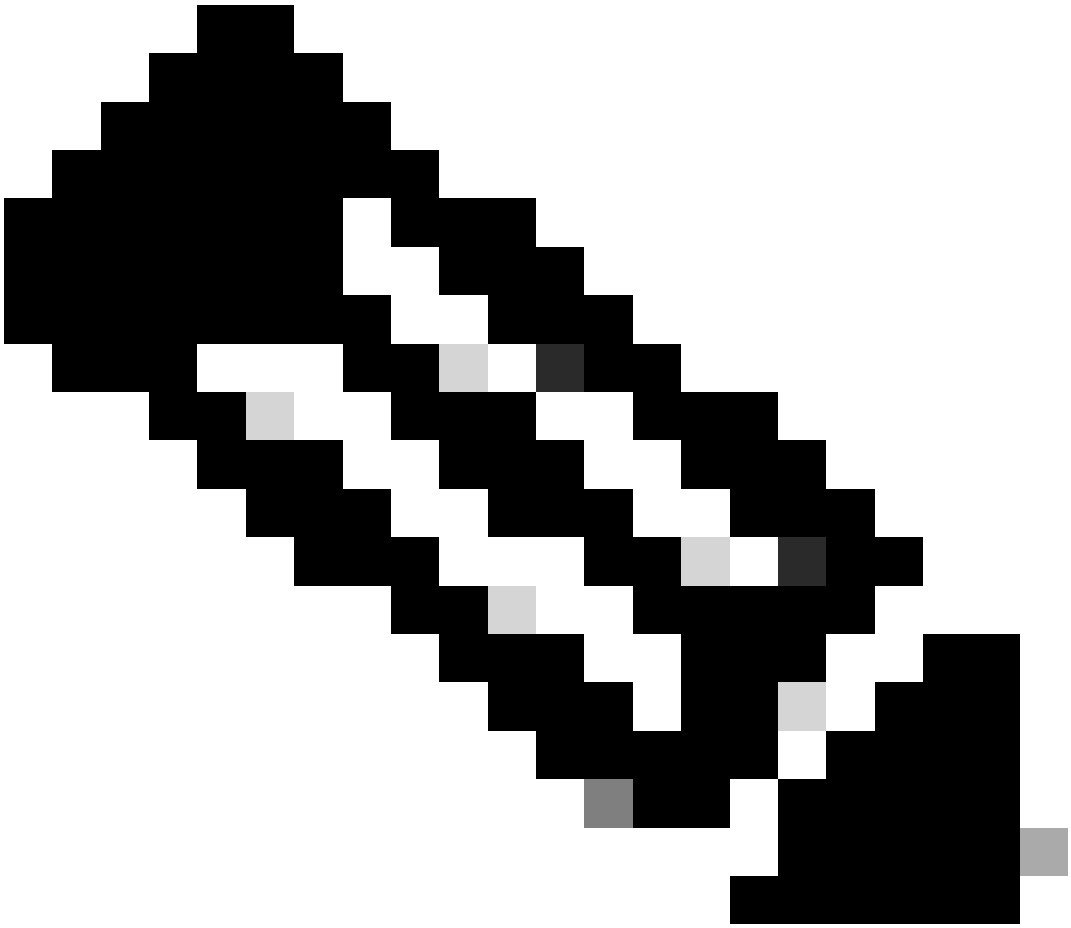
2. Defina um nome e uma descrição.

3. Selecione um dos botões de opção em SIG/SSE Provider (Umbrella ou Cisco SSE).

4. Na seção Rastreador, defina o endereço IP origem que é usado para originar as sondas do rastreador.

5. Se você optar por definir um rastreador de ponto final explícito/personalizado, clique em Adicionar Rastreador e preencha os parâmetros do rastreador de ponto final (Nome, URL da API do Ponto Final, Limite, Intervalo de Sondagem e Multiplicador).

6. Na seção Configuração, crie as interfaces de túnel nas quais você pode definir os parâmetros (como Nome da Interface, Descrição, Rastreador, Interface de Origem do Túnel, Datacenter Primary/Secondary).



Note: Na Etapa 6, o usuário recebe a opção de anexar o rastreador de endpoint definido ao respectivo túnel IPSec. Observe que esse é um campo opcional.

---

7. Na seção Alta Disponibilidade, crie um Par de Interfaces e defina sua Interface Ativa e Interface de Backup juntamente com seus respectivos pesos. Em seguida, aplique o grupo de política configurado anterior às bordas relevantes.

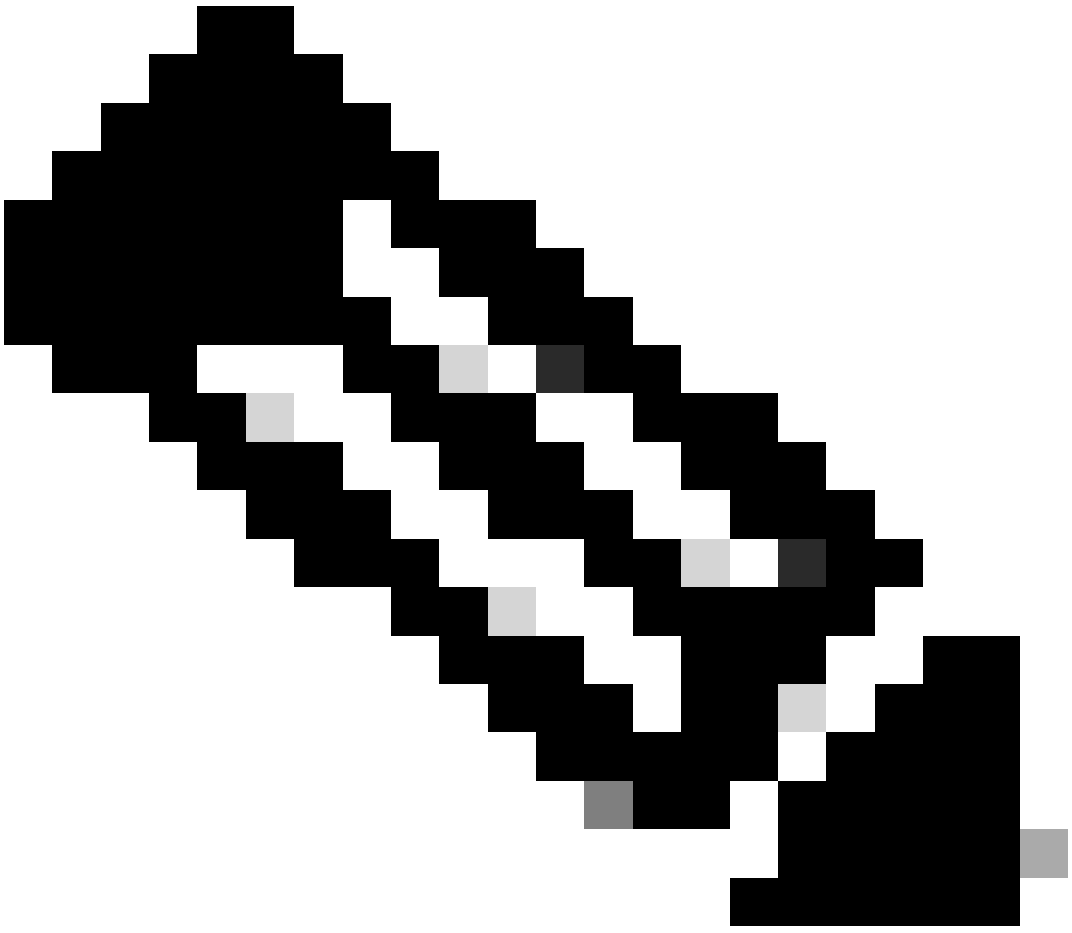
Defina a configuração herdada Configuração > Modelos > Modelos de recurso > Cisco Secure Internet Gateway modelo de recurso:

1. Selecione um dos botões de opção em SIG Provider (Umbrella, ZScalar ou Generic).

2. Na seção Rastreador (BETA), defina o endereço IP origem que é usado para originar as sondas do rastreador.

5. Se você optar por definir um rastreador de ponto final explícito/personalizado, clique em Novo Rastreador e preencha os parâmetros do rastreador de ponto final (Nome, URL da API do ponto final, Limite, Intervalo e Multiplicador).

6. Na seção Configuração, crie as interfaces de túnel (clicando em Adicionar túnel) nas quais você pode definir os parâmetros (como Nome da interface, Descrição, Rastreador, Interface de origem do túnel, Datacenter Primary/Secondary).



Note: Na etapa 6, o usuário recebe a opção de anexar o rastreador de endpoint definido ao respectivo túnel IPSec. Observe que esse é um campo opcional.

---

7. Na seção Alta Disponibilidade, defina a Interface Ativa e a Interface de Backup juntamente com

seus respectivos pesos.

Do ponto de vista da CLI, as configurações são assim:

```
(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
!
```

Verificação

Há opções de verificação de rastreadores de endpoint configurados explicitamente.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Aplicativos > Rastreador:

Verifique em Controlador individual e visualize as estatísticas do rastreador (tipos de rastreador, status, endpoint, tipo de endpoint, índice de VPN, nome do host, tempo de ida e volta) com base

no seu nome de rastreador configurado.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Eventos:

No caso de flaps detectados no rastreador, os respectivos registros seriam preenchidos nesta seção com detalhes como nome do host, nome do ponto de anexo, nome do rastreador, novo estado, família de endereços e id vpn.

Na CLI da borda:

```
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
```

Rastreadores de endpoint de interface usados para o Service Fabric 2.0

O Rastreamento do Service Fabric 2.0, que foi introduzido na versão 20.13/17.13, é uma variante aprimorada do rastreamento da inserção de serviço 1.0, em que os usuários podem personalizar os rastreadores em uma extensão maior. O comportamento padrão é mantido da versão anterior da Inserção de serviço (1.0), um rastreador seria iniciado por padrão com a definição de cada endereço de serviço (ou endereço de encaminhamento) em um par de HA de serviço por rx/tx. Mas com a Inserção de serviço 2.0, o endereço de rastreamento (IP/ponto final para o rastreado) pode ser separado do endereço de encaminhamento (geralmente o endereço de serviço). Isso é feito usando rastreadores de ponto de extremidade personalizados definidos no nível de VPN. Para saber mais sobre rastreadores do Service Fabric 2.0, visite o guia de configuração.

Se o usuário optar por usar o rastreador padrão, as especificações dos testes do rastreador são:

- Saudação: 1 sonda a cada 30 segundos
- Multiplicador: 3 vezes
- Tipo de pacote/sonda: Eco/resposta de eco ICMP

Se o usuário optar por usar um rastreador personalizado, as especificações dos testes do

rastreador serão:

- Saudação: 1 sonda a cada 60 segundos
- Multiplicador: 3 vezes
- Tipo de pacote/sonda: Solicitação/resposta de eco ICMP

Casos de uso

Os casos de uso da Inserção de serviço 1.0 mencionados nas seções anteriores também se aplicam aqui.

Configuração

Há suporte para a configuração baseada em fluxo de trabalho para a Inserção de serviço 2.0, que é uma abordagem orientada por assistente, ajudando a simplificar a experiência do usuário, enquanto segue as etapas de fluxo de trabalho do grupo de configuração padrão.

1. Defina o grupo Cadeia de Serviço - Configuração na seção Configuração > Inserção de Serviço > Definições da Cadeia de Serviço:

a. Clique no botão Add Service Chain Definition.

b. Preencha os detalhes do Nome e da Descrição do Serviço.

c. Preencha um formato de lista (selecionando na lista suspensa), o Tipo de serviço.

2. Defina o grupo Instância da Cadeia de Serviços - Configuração na seção Configuração > Inserção de Serviço > Configurações da Cadeia de Serviços:

a. Clique em Add Service Chain Configuration.

b. Na etapa Definição da Cadeia de Serviços, selecione o botão de opção Selecionar Existente e escolha o Serviço definido anteriormente.

c. Forneça um Nome e uma Descrição para a etapa Start Service Chain Configuration.

d. Na etapa Service Chain Configuration for Manually Connected Services, selecione o Service Chain VPN-ID.

e. Em seguida, para cada serviço definido na instância da cadeia de serviços (representada em subguias), em detalhes do serviço, forneça o Tipo de anexo (IPv4, IPv6 ou Túnel conectado).

f. Marque a caixa de seleção Avançado. Se você precisar ter casos de uso de backup ativo/HA (habilite também o botão Adicionar parâmetros para Backup) ou mesmo se precisar definir um rastreador de endpoint personalizado (habilite também o botão Rastreador personalizado).

g. Se você tiver cenários em que o tráfego de saída (tx) vai para o serviço por meio de uma interface e o tráfego de retorno do serviço é ingressado (rx) por meio de outra interface, ative o Tráfego do serviço é recebido em um botão de interface diferente.

h. Com os botões Advanced e Custom Tracker ativados, defina o Service IPv4 Address (endereço de encaminhamento), a interface do roteador SD-WAN (à qual o serviço está conectado) e o Tracker Endpoint (endereço de rastreamento). Você também pode modificar os parâmetros personalizados do rastreador, como intervalo e multiplicador (clicando no botão editar).

i. Repita as etapas (e), (f), (g) e (h) para cada serviço definido subsequentemente.

3. Anexe a Instância da Cadeia de Serviços ao Perfil de Configuração da Borda - Grupo de Configuração em Configuração > Grupos de Configuração > Perfil de Serviço > VPN de Serviço > Adicionar Recurso > Gateway de Anexo da Cadeia de Serviços:

a. Forneça um Nome e uma Descrição para este pacote do Gateway de Anexo da Cadeia de Serviços.

b. Selecione a Definição da Cadeia de Serviços definida anteriormente (na etapa 1).

c. Adicione/verifique novamente os detalhes conforme executado na etapa 2. Para a definição do rastreador, a única diferença da etapa 2 anterior é que você tem a chance de fornecer um Nome de Rastreador e também selecionar o Tipo de Rastreador (de service-icmp a ipv6-service-icmp).

Do ponto de vista da CLI, as configurações são assim:

```
!
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
!
```

Verificação

- No SD-WAN Manager Monitor > Devices > {select Device-Name} > Applications > Tracker:

Verifique em Controlador individual e visualize as estatísticas do rastreador (tipos de rastreador, status, endpoint, tipo de endpoint, índice de VPN, nome do host, tempo de ida e volta) com base no seu nome de rastreador configurado.

- No SD-WAN Manager Monitor > Devices > {select Device-Name} > Events:

No caso de flaps detectados no rastreador, os respectivos registros seriam preenchidos nesta seção com detalhes como nome do host, nome do ponto de anexo, nome do rastreador, novo

estado, família de endereços e id vpn.

Na CLI da borda:

```
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
```

Rastreadores de ponto final de rota estática usados para rastreamento de rota estática (lado do serviço)

O segundo tipo de rastreadores de endpoint é chamado de rastreadores de endpoint baseados em rota estática. Como o próprio nome indica, esses tipos de rastreadores são usados principalmente para rastrear o endereço do próximo salto de qualquer rota estática definida na VPN do lado do serviço. Por padrão, todos os tipos de rota "conectada" e "estática" são

anunciados no protocolo OMP - post que todos os locais remotos que contêm o respectivo serviço VPN se tornam cientes desse prefixo de destino (onde o ponto do próximo salto para o TLOC do local de origem). O local de origem é o local de onde a rota estática específica foi iniciada.

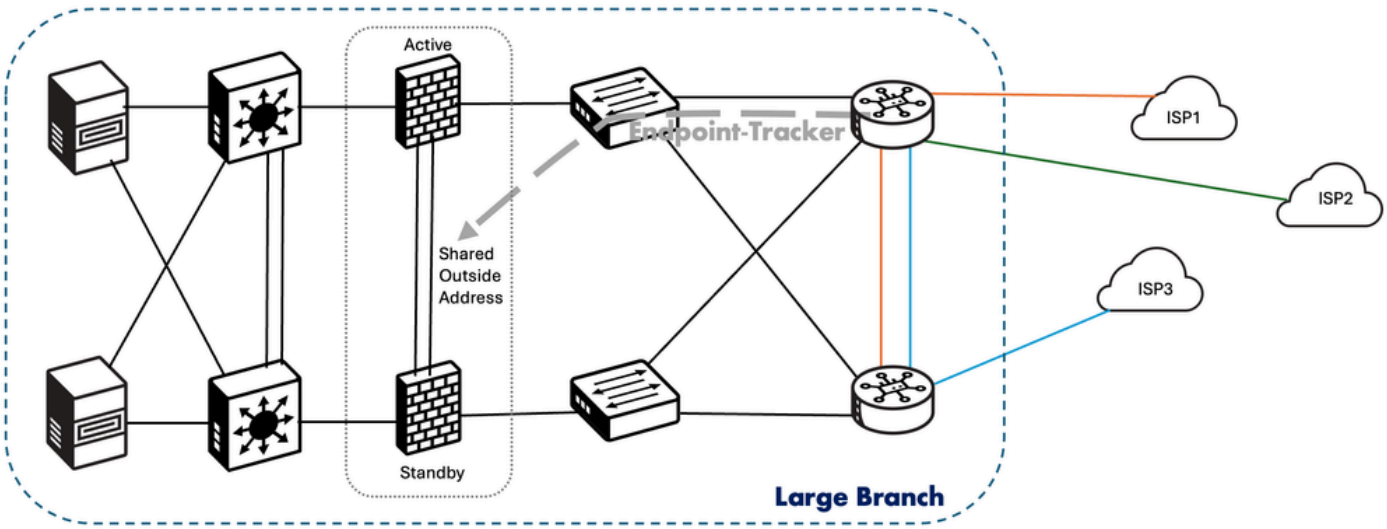
No entanto, caso o endereço do próximo salto na rota estática se torne inalcançável, a rota não pára de ser anunciada no OMP. Isso causaria problemas de bloqueio de tráfego para fluxos destinados ao local de origem. Isso gera a necessidade de anexar um rastreador à rota estática, para garantir o anúncio da rota estática no OMP SOMENTE quando o endereço do próximo salto for alcançável. Esse recurso foi introduzido na versão 20.3/17.3 para rastreadores de endpoint baseados em rota estática de tipo de endereço IP básico. A partir da versão 20.7/17.7, o suporte foi adicionado para enviar sondas de rastreador somente a portas TCP ou UDP específicas do endereço IP do próximo salto (em casos em que se usa firewalls para abrir apenas certas portas para fins de rastreamento). Para saber mais sobre rastreadores de rota estática, visite o guia de configuração.

Os tipos de sondas usados aqui são um pacote ICMP de solicitação de eco simples. Os intervalos usados são:

- Saudação: 60 segundos
- Tempo de suspensão: 180 segundos (já que #retries é 3 = 3 x 60 segundos)
- Tipo de pacote/sonda: Eco/resposta de eco ICMP

Casos de uso

Esse tipo de rastreador de endpoint baseado em rota estática é usado para rastreamento do lado do serviço de endereços do próximo salto em rotas estáticas. Um cenário comum seria rastrear o endereço do próximo salto do lado da LAN correspondente a um par de firewalls ativos/em espera, que compartilham o endereço IP externo com base no qual a interface externa desempenha a função de firewall "ativo". Nos casos em que as regras de firewall parecem ser altamente restritivas, em que apenas certas portas são abertas para fins de uso com base em casos específicos, o rastreador de rota estática pode ser usado para rastrear a porta TCP/UDP específica para o endereço IP do próximo salto que pertence à interface externa do firewall do lado da LAN.



Configuração

Esses rastreadores de endpoint baseados em rota estática devem ser configurados manualmente para ativar esse conjunto de recursos. Estas são as maneiras de configurá-lo, dependendo do tipo de método de configuração preferido pelo usuário.

- Grupo de configuração Configuração > Grupos de configuração > Perfil de serviço > VPN de serviço > Adicionar recurso > Rastreador:

1. Forneça um Nome, Descrição e Nome do Controlador para o novo rastreador (endpoint) que está sendo definido.

2. Escolha o tipo de ponto final, dependendo se você precisa apenas rastrear o endereço IP do próximo salto (botão de opção Escolher endereço) ou até mesmo portas TCP/UDP específicas (botão de opção Escolher Protocolo).

3. Informe o Endereço, em um formato de endereço IP. Além disso, insira o protocolo (TCP ou UDP) e o número da porta, caso tenha escolhido Protocol como o tipo de endpoint na etapa anterior.

4. Você pode alterar os valores default fornecidos para Intervalo de Sondagem, Número de Repetições e Limite de Latência, se necessário.

- Seção Configuração > Grupos de Configuração > Perfil de Serviço > VPN de Serviço > Rota:

1. Selecione o botão Add IPv4/IPv6 Static Route.

2. Preencha os detalhes, como Endereço de rede, Máscara de sub-rede, Próximo salto, Endereço, AD.

3. Clique no botão Add Next Hop With Tracker.

4. Digite novamente o endereço do próximo salto, AD e escolha na lista suspensa o nome do rastreador (endpoint) criado anteriormente.

- Configuração legada Configuração > Modelos > Modelos de recurso > Modelo do sistema > Rastreador seção:

1. Selecione o botão Novo Rastreador de Ponto Final.

2. Forneça um Nome para o novo rastreador (endpoint) sendo definido.

3. Altere o botão de opção Tipo de Rastreador para rota estática.

4. Escolha o tipo de ponto final, como endereço IP do próximo salto (botão de opção Escolher endereço IP).

5. Insira o IP do endpoint, em um formato de endereço IP.

6. Você pode alterar os valores default fornecidos para Intervalo de Sondagem, Número de Repetições e Limite de Latência, se necessário.

- Configuração > Modelos > Modelos de recurso > Cisco VPN (SOMENTE do lado do serviço) > seção Rota IPv4/IPv6:

1. Selecione o botão New IPv4/IPv6 Route.

2. Preencha os detalhes, como Prefixo, Gateway.

3. Clique no botão Add Next Hop With Tracker.

4. Insira novamente o endereço do próximo salto, AD (distância), e insira manualmente o nome do rastreador (endpoint) criado anteriormente.

Do ponto de vista da CLI, as configurações são assim:

```
(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
!
```

Verificação

Há duas áreas de verificação de rastreadores de endpoint configurados explicitamente.

- No Monitor do gerenciador SD-WAN > Dispositivos > {selecione Device-Name} > Tempo real:

1. Em Device Options, digite "Endpoint Tracker Info".

2. Verifique em Rastreador Individual (Nome do Ponto de Anexo) e veja as estatísticas do rastreador (Estado do Rastreador, Nome do Registro do Rastreador Associado, Latência em mx do dispositivo para o ponto final, carimbo de data/hora da Última Atualização) com base em seu

Nome do Rastreador configurado.

- No Monitor do gerenciador de SD-WAN > Dispositivos > {select Device-Name} > Eventos:

No caso de flaps detectados no rastreador, os respectivos logs seriam preenchidos nesta seção com detalhes como nome do host, nome do ponto de anexo, nome do rastreador, novo estado, família de endereços e id de vpn.

Na CLI da borda:

```
Router#sh endpoint-tracker static-route
Tracker Name                    Status          RTT in msec     Probe ID
nh10.10.1.4-s10.20.1.0          UP              1               3

Router#show track endpoint-tracker
Track nh10.10.1.4-s10.20.1.0
  Ep_tracker-object
  State is Up
    2 changes, last change 00:01:54, by Undefined
  Tracked by:
    Static IP Routing 0

Router#sh endpoint-tracker records
Record Name                     Endpoint                                EndPoint Type Threshold(ms) Mult
nh10.10.1.4-s10.20.1.0          10.10.1.4                               IP            300           3

Router#sh ip sla summ
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------
*3           icmp-echo   10.10.1.4         RTT=1       OK          58 seconds ago

EFT-BR-11#sh ip static route vrf 1
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       D1 - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng, LI - LIIN
       IR - ICMP Redirect, Vx - VXLAN static route
       LT - Cellular LTE, Ev - L2EVPN static route
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - permanent, -T Default Tr


Codes in (): UP - up, DN - Down, AD-DN - Admin-Down, DL - Deleted
Static local RIB for 1

M  10.20.1.0/24 [1/0] via 10.10.1.4 [A]
T               [1/0] via 10.10.1.4 [A]
```

Rastreadores de objeto de interface usados para rastreamento de VRRP

Os Rastreadores de objetos são rastreadores projetados para o consumo do modo autônomo (casos de uso). Esses rastreadores têm casos de uso que variam de rastreamento de túnel/interface baseado em VRRP a rastreamento de NAT de VPN de serviço.

Para casos de uso de rastreamento de VRRP, o estado de VRRP é determinado com base no status do link do túnel. Se o túnel ou a interface estiver inoperante no VRRP principal, o tráfego será direcionado para o VRRP secundário. O roteador VRRP secundário no segmento de LAN torna-se o VRRP principal para fornecer gateway para o tráfego do lado do serviço. Este caso de uso só é aplicável para o serviço VPN e ajuda no failover da função VRRP no lado da LAN em caso de falha na sobreposição de SD-WAN (Interface ou Túneis no caso de SSE). Para anexar rastreadores a grupos VRRP, SOMENTE rastreadores de objetos podem ser usados (não rastreadores de endpoint). Esse recurso foi introduzido na versão 20.7/17.7 para Cisco Catalyst SD-WAN Edges.

Não há sondas usadas aqui pelo rastreador. Em vez disso, ele usa o estado de protocolo de linha para decidir sobre o estado do rastreador (up/down). Não há intervalos de reação nos rastreadores baseados em protocolo de linha de interface - no momento em que o protocolo de linha de interface/túnel é DESATIVADO, o estado de rastreamento também é colocado no estado DESATIVADO. Em seguida, dependendo da ação de desligar ou decrementar, o grupo VRRP reconvergiria de acordo. Para saber mais sobre rastreadores de interface VRRP, visite o guia de configuração.

Casos de uso

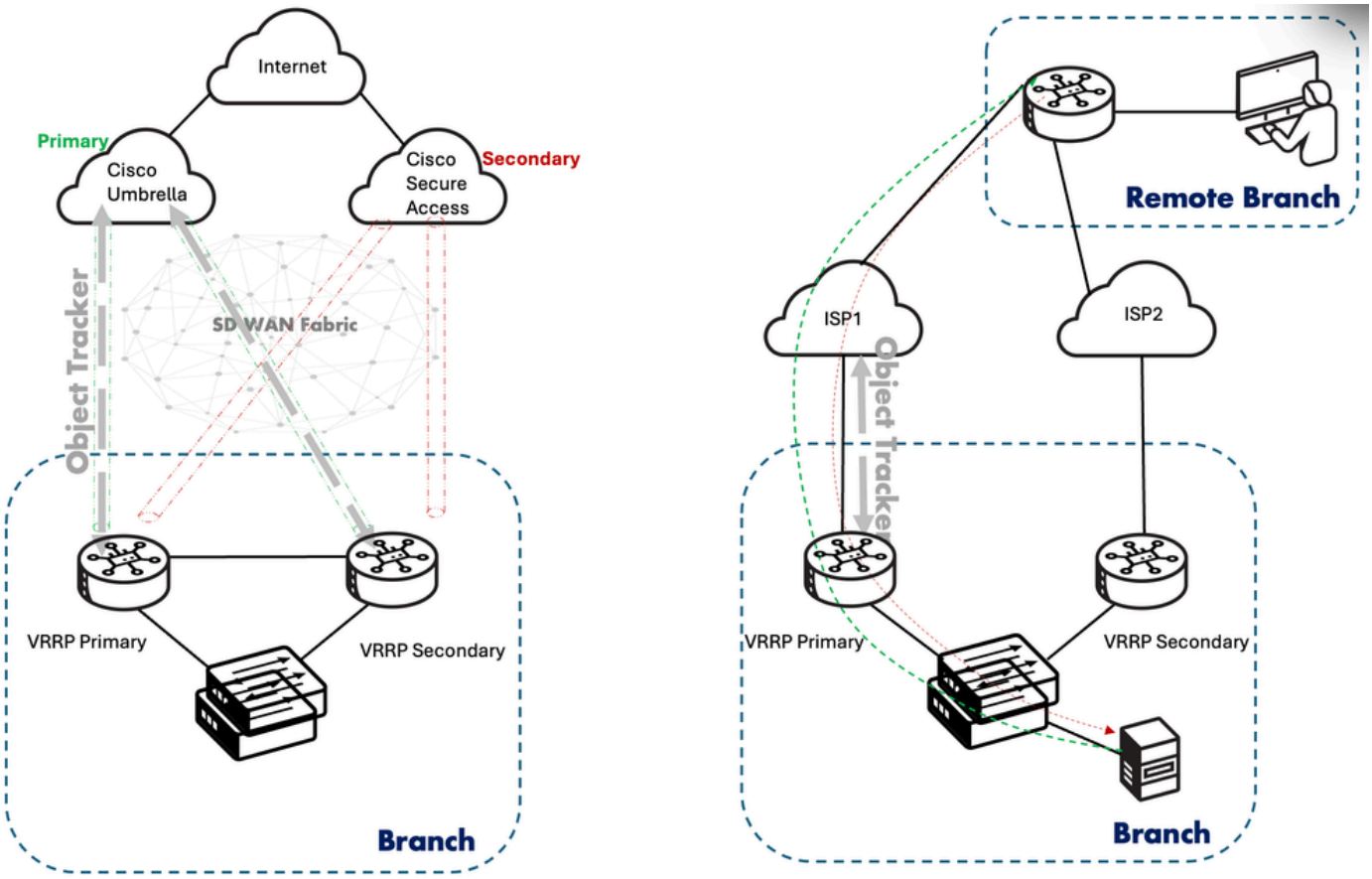
Há vários casos de uso com base nos critérios necessários para implementar o rastreamento de interface baseado em VRRP. Atualmente, os dois modos suportados são: (i) interface (ou seja, qualquer interface de túnel que esteja ligada a um TLOC local) ou (ii) interface SIG (relacionada às interfaces de túnel SIG). Em cada caso, a peça que está sendo rastreada é o protocolo de linha de interface.

Roteador duplo com Internet: O objeto de controle está associado ao grupo VRRP. Caso o objeto do rastreador (que, nesse caso, é a interface de túnel SIG) fique inativo, isso notificará o roteador principal VRRP para disparar a transição de estado de Primário para backup e o roteador de backup para se tornar Primário. Essa alteração de estado pode ser influenciada ou acionada por dois tipos de operações:

1. Diminuição: Onde a prioridade VRRP para a interface na qual o VIP VRRP está configurado é reduzida ou diminuída em um determinado valor, no caso de o estado do objeto de rastreamento passar de UP para DOWN.
2. Fechamento: Este é um método em que o processo VRRP é desligado na interface aplicada, no caso de o estado do objeto de rastreamento passar de UP para DOWN. Este método não é recomendado em casos de uso onde há instâncias de encaminhamento

assimétrico.

Preferência de alteração de TLOC: para evitar o tráfego assimétrico proveniente de outros sites de SDWAN para o site onde o VRRP é executado no serviço VPN, a preferência de TLOC do roteador primário VRRP é aumentada em 1, se configurado. Você pode até mesmo modificar esse valor em grupos de configuração. Isso garante que o tráfego da WAN para a LAN seja atraído pelo próprio roteador principal VRRP. O tráfego de LAN para WAN é atraído pelo mecanismo VRRP de VRRP Primário. Esse recurso é independente do rastreador de interface VRRP. Este é um comando opcional (tloc-change-pref) do ponto de vista da CLI.



Configuração

A configuração de rastreadores de objetos é feita através de modelos de sistema na configuração Legacy e, em seguida, anexando o rastreador de objetos ao respectivo grupo VRRP no modelo de recurso de interface Ethernet de VPN de serviço. No grupo Configuração, este mecanismo foi simplificado pela obtenção direta de uma opção para adicionar o rastreador de objetos ao respectivo perfil de serviço Perfil de Interface Ethernet. Aqui estão as formas de configurá- lo, dependendo do tipo de método de configuração preferido pelo usuário.

- Grupo de configuração Configuração > Grupos de configuração > Perfil de serviço > Interface Ethernet > Adicionar recurso > Rastreador de objeto:

1. Forneça um Nome e uma Descrição para o novo rastreador de objetos que está sendo definido.
2. Selecione o Tipo de rastreador (entre Interface e SIG).

3. Alocar uma ID do Rastreador de Objetos.
4. Forneça o nome da interface (dependendo da opção escolhida na etapa 2).

- Seção Configuração > Grupos de Configuração > Perfil de Serviço > Interface Ethernet > VRRP:

1. Em IPv4 Settings, clique em Add VRRP IPv4.
2. Defina uma ID do grupo VRRP e forneça uma prioridade local para esta interface ethernet do lado do serviço.
3. Forneça o endereço IP virtual (VIP) VRRP.
4. Ative o botão TLOC Preference Change e também forneça o TLOC Preference Change Value (para lidar com o roteamento assimétrico).
5. Clique em Adicionar Objeto de Rastreamento VRRP.
6. Em Associate Object Tracker, selecione no menu suspenso no Object Tracker (com base no Nome) que você criou antes
7. Escolha uma Ação do rastreador (Desligamento ou Decremento).
8. Insira o valor de diminuição (dependendo da opção escolhida na etapa 7).

- Configuração legada Configuração > Modelos > Modelos de recurso > Sistema > Rastreador seção:

1. Clique no botão New Object Tracker.
2. Selecione o Tipo de rastreador (entre Interface e SIG).
3. Alocar uma ID de objeto.
4. Forneça o nome da interface (dependendo da opção escolhida na etapa 2).

- Configuração > Modelos > Interface Ethernet (pertencente ao lado do serviço) > seção VRRP:

1. Clique no botão New VRRP.
2. Defina uma ID do grupo VRRP e forneça uma Prioridade local (opcional, o valor padrão de 100 é escolhido) para esta interface ethernet do lado do serviço.
3. Forneça o endereço IP virtual (VIP) VRRP.
4. Ative o botão Alteração de Preferência de TLOC e também forneça o Valor de Alteração de Preferência de TLOC (para manipular o roteamento assimétrico).
5. Em Controlador de objetos, clique em Adicionar objeto de rastreamento.
6. Insira a ID do Controlador de Objetos (definida no modelo do sistema).
7. Escolha uma Ação do rastreador (Desligamento ou Decremento).
8. Insira o valor de diminuição (dependendo da opção escolhida na etapa 7).

Do ponto de vista da CLI, as configurações são assim:

```
(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
!
```

Verificação

Há duas opções para verificar rastreadores de objetos configurados explicitamente para casos de uso de VRRP.

- No Monitor do gerenciador SD-WAN > Dispositivos > {selecione Device-Name} > Tempo real:

1. Em Device Options, digite "VRRP Information".

2. Verifique em Grupo VRRP Individual (ID do Grupo) e veja as estatísticas do rastreador (Nome do Prefixo de Rastreamento, Estado de Rastreamento, Hora da Descontinuidade e Hora da Última Alteração de Estado) com base nas IDs do Rastreador de Objeto configuradas.

- No Monitor do gerenciador de SD-WAN > Dispositivos > {select Device-Name} > Eventos:

No caso de alteração de estado detectada no rastreador de objetos, o Grupo VRRP correspondente ao qual ele está anexado altera seu estado. Os respectivos logs seriam preenchidos nesta seção (com o Nome como Alteração do Estado do Grupo Vrrp) com detalhes como nome do host, if number, grp id, addr type, if name, vrrp group-state, state change-reason e vpn id.

Na CLI da borda:

```
Router#show vrrp 10 GigabitEthernet 3
GigabitEthernet3 - Group 10 - Address-Family IPv4
  State is MASTER
  State duration 59 mins 56.703 secs
  Virtual IP address is 10.10.1.1
  Virtual MAC address is 0000.5E00.010A
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 120
  State change reason is VRRP_TRACK_UP
  Tloc preference configured, value 120
    Track object 10 state UP decrement 40
  Master Router is 10.10.1.3 (local), priority is 120
  Master Advertisement interval is 1000 msec (expires in 393 msec)
  Master Down interval is unknown
  FLAGS: 1/1

Router#show track 10
Track 10
  Interface Tunnel1 line-protocol
  Line protocol is Up
    7 changes, last change 01:00:47
  Tracked by:
    VRRPv3 GigabitEthernet3 IPv4 group 10

Router#show track 10 brief
Track Type        Instance                  Parameter        State Last Change
10    interface   Tunnel1                   line-protocol    Up    01:01:02

Router#show interface Tunnel1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of GigabitEthernet1 (172.25.12.1)
  MTU 9980 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.25.12.1 (GigabitEthernet1)
```

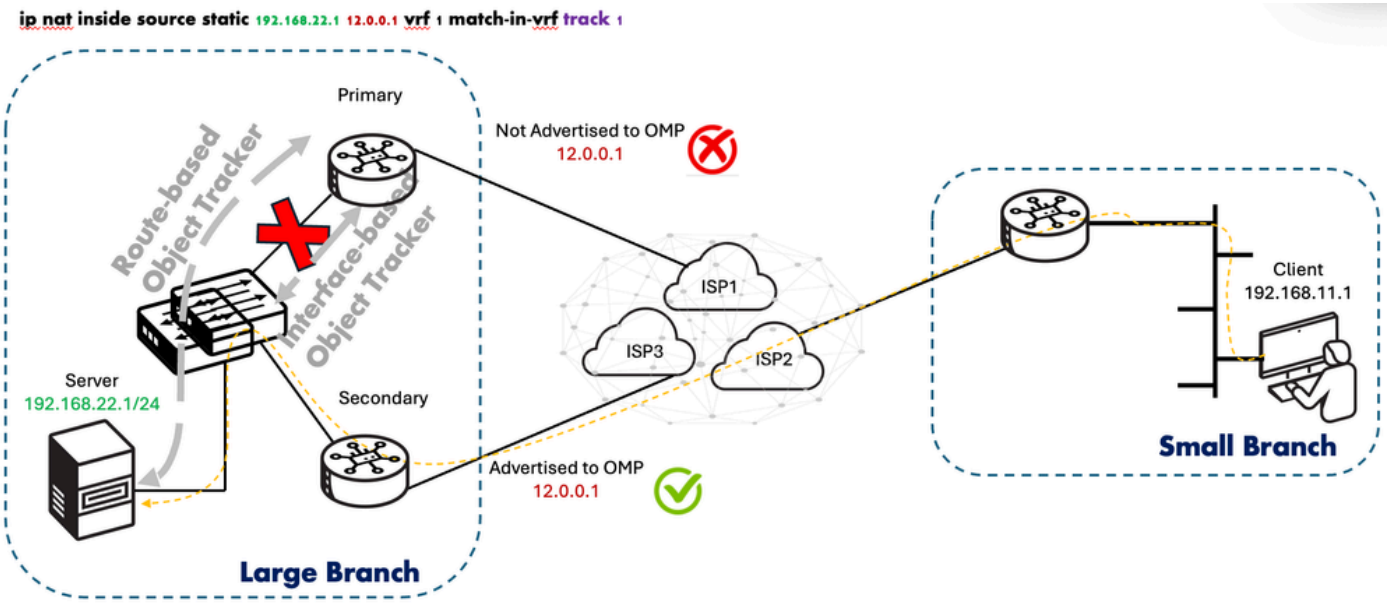
Rastreadores de objeto de interface/rota usados para rastreamento de NAT de VPN de serviço

O Rastreador de Objetos NAT do lado do serviço foi um recurso introduzido na versão 20.8/17.8, em que o endereço global interno usado no NAT de VPN de serviço (NAT estático interno e NAT dinâmico interno) só é anunciado no OMP se (i) o endereço local interno for considerado alcançável OU (ii) o protocolo de linha da interface LAN/do lado do serviço for UP conforme o rastreador de objetos anexado. Portanto, os tipos de rastreador de objetos que podem ser usados são (i) rota ou (ii) interface. Dependendo do estado do prefixo de LAN ou da interface de LAN, os anúncios de rota NAT através do OMP são adicionados ou removidos. Você pode visualizar registros de eventos no Cisco SD-WAN Manager para monitorar quais anúncios de rotas NAT são adicionados ou removidos.

Não há sondas usadas aqui pelo rastreador. Em vez disso, ele usa (i) a presença de uma entrada de roteamento na tabela de roteamento OU (ii) o estado do protocolo de linha para decidir o estado do rastreador (ativo/inativo). Não há intervalos de reação na presença de uma entrada de roteamento ou de rastreadores baseados em protocolo de linha de interface - no momento em que a entrada de roteamento ou o protocolo de linha de interface fica INATIVO, o estado de rastreamento também é colocado no estado INATIVO. Imediatamente, o endereço global interno usado na instrução NAT associada ao rastreador de objetos é impedido de ser anunciado no OMP. Para saber mais sobre rastreadores NAT de VPN de serviço, visite o guia de configuração.

Casos de uso

Se uma interface de LAN ou um prefixo de LAN estiver inativo, o rastreador de objetos do NAT do lado do serviço será desativado automaticamente. Você pode exibir logs de eventos em Cisco SD-WAN Manager para monitorar quais anúncios de rotas NAT são adicionados ou removidos. No próximo caso de uso, o cliente precisa acessar o servidor na filial grande. No entanto, o problema surge em situações em que a rota que aponta para o servidor nas bordas da filial grande (em HA) é removida OU quando a interface do lado da LAN (lado do serviço) cai em qualquer borda na filial grande. Nessas situações, ao aplicar o NAT do lado do serviço com o rastreador de objetos, certifique-se de que o tráfego de entrada do cliente seja sempre direcionado para a borda correta localizada na filial grande, controlando o anúncio de endereço global interno no OMP. Caso esse controle não seja aplicado no anúncio de rota no OMP, o tráfego acaba ficando bloqueado devido à inacessibilidade dessa borda respectiva para o servidor na filial grande.



Configuração

A configuração de rastreadores de objetos é feita através de modelos de sistema na configuração Legacy e, em seguida, anexando o rastreador de objetos à respectiva instrução NAT (dentro estático ou dentro dinâmico) no modelo de recurso de VPN de serviço. No grupo Configuração, este mecanismo foi simplificado pela obtenção direta de uma opção para adicionar o rastreador de objetos ao respectivo perfil de serviço Perfil de Interface Ethernet. Aqui estão as formas de configurá- lo, dependendo do tipo de método de configuração preferido pelo usuário.

- Grupo de configuração Configuração > Grupos de configuração > Perfil de serviço > Adicionar recurso > Rastreador de objeto:

1. Forneça um Nome e uma Descrição para o novo rastreador de objetos que está sendo definido.
2. Selecione o tipo de rastreador (entre Interface e rota).
3. Alocar uma ID do Rastreador de Objetos.
4. Forneça o nome da interface OU forneça o IP da rota, a máscara do IP da rota e a VPN (dependendo da opção escolhida na etapa 2).

- Seção Configuração > Grupos de configuração > Perfil de serviço > NAT:

1. Crie um pool de NAT (obrigatório para acionar o SSNAT) clicando no botão Add NAT Pool.

2. Forneça os detalhes do pool de NAT, como Nome do pool de NAT, Comprimento do prefixo, Início do intervalo, Fim do intervalo e Direção.

3. Vá para NAT estático na mesma seção e clique no botão Add New Static NAT. (Você também pode optar por anexar o rastreador de objetos ao NAT de pool dinâmico interno).

4. Forneça os detalhes, como IP de Origem, IP de Origem Convertida e Direção de NAT Estático.

5. No campo Associar Rastreador de Objeto, escolha na lista dropdown o rastreador de objeto criado anteriormente.

- Configuração legada Configuração > Modelos > Modelos de recurso > Sistema > Rastreador seção:

1. Clique no botão New Object Tracker.
2. Selecione o Tipo de rastreador (entre Interface e rota).
3. Alocar uma ID de objeto.
4. Forneça o nome da interface OU o IP da rota, a máscara IP da rota e a VPN (dependendo da opção escolhida na etapa 2).

- Configuração > Modelos > Cisco VPN (pertencente ao lado do serviço) > seção NAT:

1. Crie um pool de NAT (obrigatório para acionar o SSNAT) clicando no botão New NAT Pool.

2. Forneça os detalhes do pool de NAT, como Nat Pool Name, NAT Pool Prefix Length, NAT Pool Range Start, NAT Pool Range End e NAT Direction.

3. Mova para NAT estático na mesma seção e clique no botão New Static NAT. (Você também pode optar por anexar o rastreador de objetos ao NAT de pool dinâmico interno).

4. Forneça os detalhes, como Endereço IP de Origem, Endereço IP de Origem Convertido, Direção de NAT Estático.

5. No campo Adicionar Rastreador de Objeto, digite o nome do rastreador de objeto criado anteriormente.

Do ponto de vista da CLI, as configurações são assim:

```
(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
!
```

A suposição com o caso de uso de SSNAT é que os usuários aplicam a política de dados para corresponder o tráfego de entrada -> saída e saída -> em fluxos de NAT.

Verificação

Há duas áreas de verificação de rastreadores de objetos configurados explicitamente para casos de uso de NAT.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Tempo real:

1. Em Device Options, digite "IP NAT Translation".

2. Verifique em Individual NAT Translation e veja as estatísticas da entrada (Endereço/porta local interno, Endereço/porta global interno, Endereço/porta local externo, Endereço/porta global externo, ID VRF, Nome e protocolo VRF) com base nas IDs do Object Tracker configuradas.

- No SD-WAN Manager: Monitorar > Dispositivos > {select Device-Name} > Eventos:

No caso de alteração de estado detectada no rastreador de objetos correspondente à rota NAT que está sendo podada no OMP, eventos denominados "Alteração de rota NAT" aparecem, que contêm detalhes como nome do host, rastreador de objetos, endereço, máscara, tipo de rota e atualização. Aqui, o endereço e a máscara são mapeados para o endereço global interno conforme configurado na instrução NAT estático.

Na CLI da borda:

```
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
```

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.