Configure ThousandEyes Agent-to-Server SD-WAN Service-Side com a marcação DSCP

Contents

Introdução

Este documento descreve a configuração de ThousandEyes Agent-to-Server SD-WAN com marcação DSCP para monitoramento de tráfego em uma sobreposição de Cisco SD-WAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.

- Visão geral da SD-WAN
- Modelos
- Mil olhos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- Cisco Manager versão 20.15.3
- Cisco Validator versão 20.15.3
- Cisco Controller versão 20.15.3
- Integrated Service Routers (ISR)4331/K9 versão 17.12.3a
- thousandeyes-enterprise-agent-5.5.1.cisco

Configurações preliminares

- Configurar DNS: O Roteador pode resolver o DNS e acessar a Internet na VPN 0.
- Configurar NAT DIA: A configuração de DIA precisa estar presente no roteador.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Teste de Agente para Servidor

Para executar um teste Agente para Servidor, o agente ThousandEyes deve ser configurado na VPN de Serviço. Neste cenário, o servidor é o endereço IP TLOC que é monitorado. Geralmente, um teste Agente para Servidor é usado para monitorar um servidor; no entanto, nesse caso, ele é usado para monitorar uma interface TLOC localizada em um site diferente de onde o agente está hospedado.

Se houver várias interfaces TLOC, use o NAT Direct Internet Access (DIA) e uma política de dados para redirecionar o tráfego para a interface TLOC da VPN 0 desejada. Defina os critérios de correspondência com base no valor de DSCP configurado no lado do agente em ThousandEyes para ser redirecionado para e através da VPN 0 e, ao mesmo tempo, faça a marcação para evitar qualquer ultrapassagem que o ISP possa ter com sua própria marcação de DSCP.

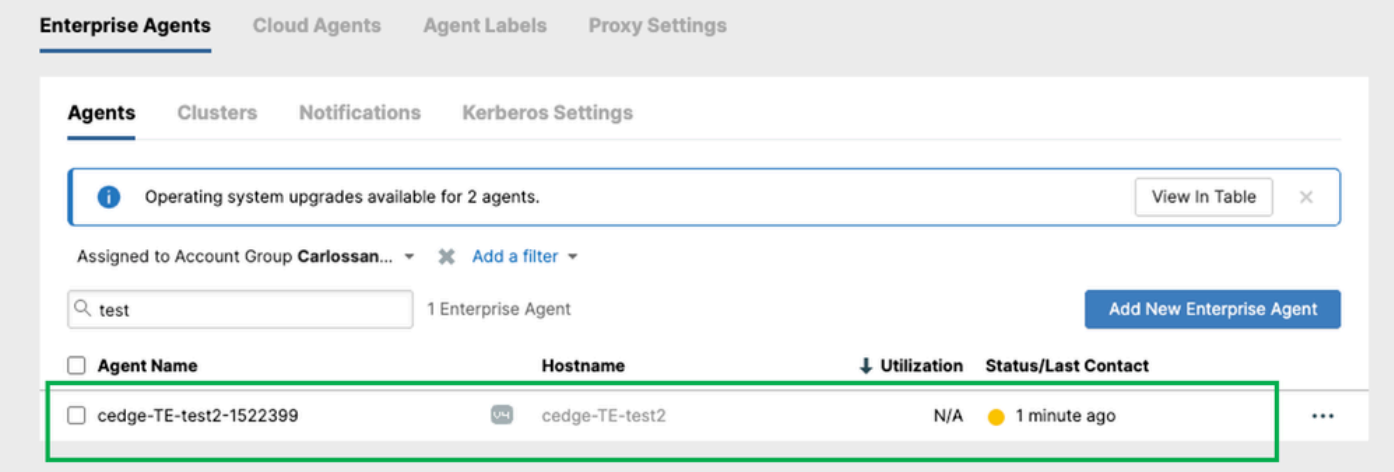
Configurar

Configurar ThousandEyes Test e DSCP

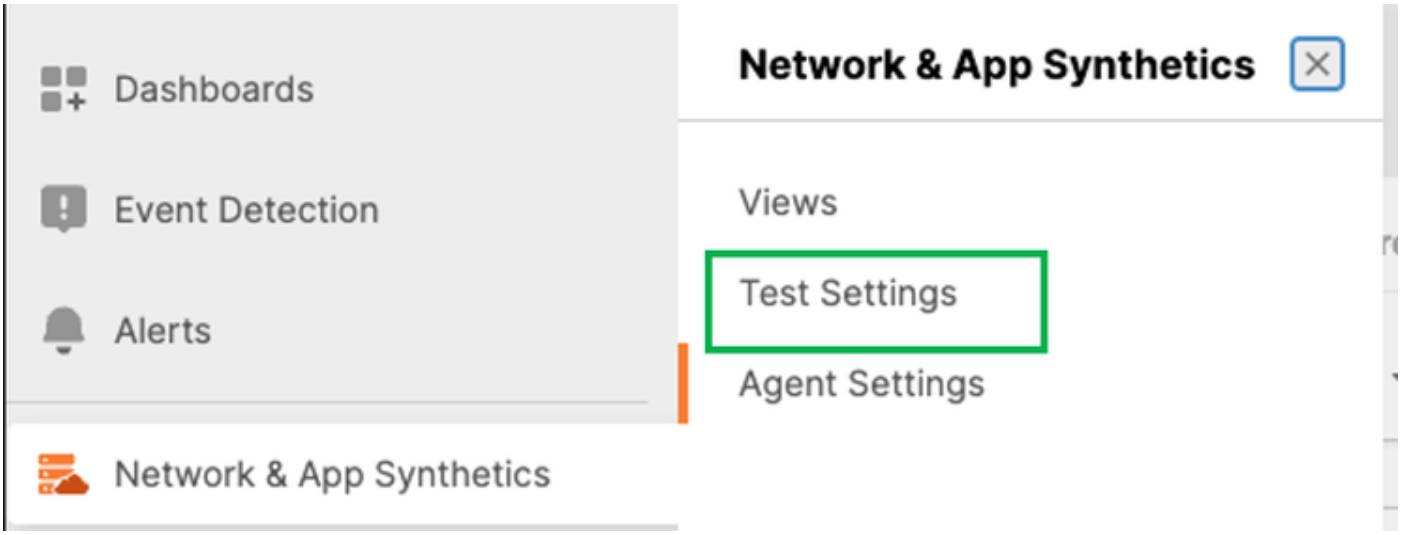
Para configurar o Differentiated Services Code Point (DSCP):

1. Faça login na conta ThousandEyes na página AgenteCisco ThousandEyes.

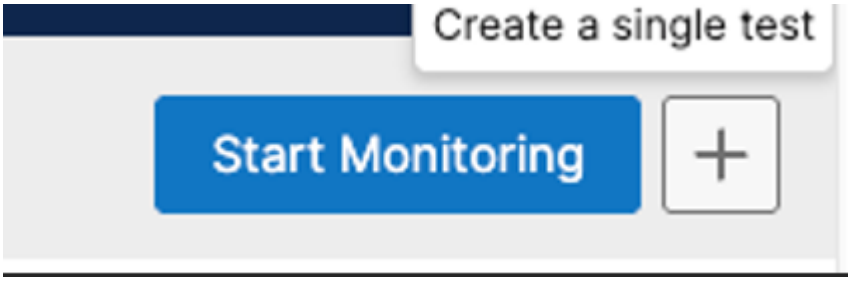
Verifique se o agente instalado no roteador tem comunicação com a nuvem ThousandEyes.



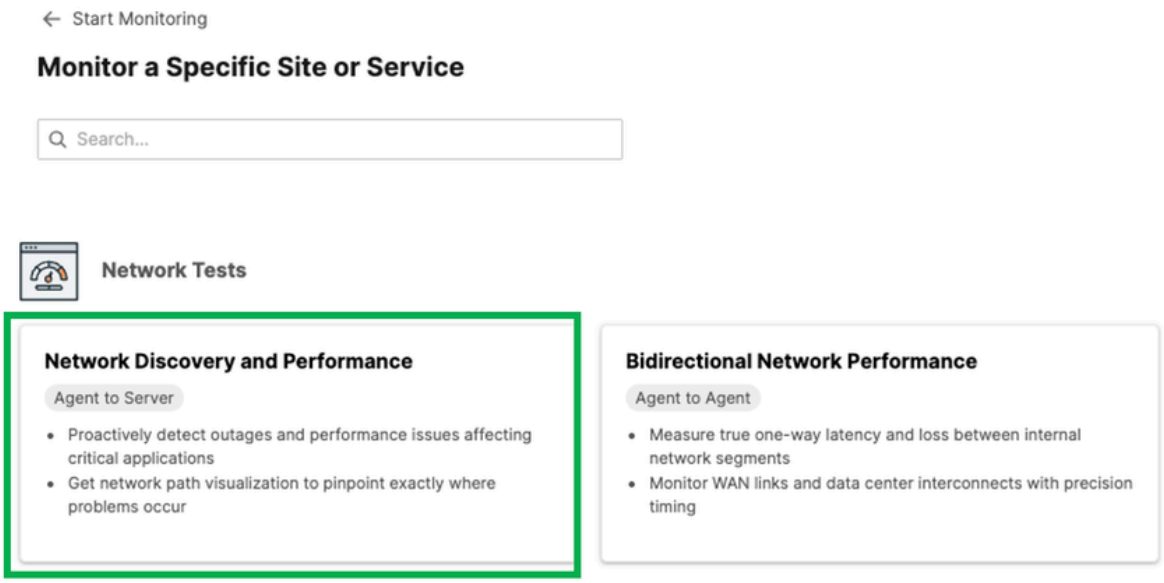
Depois que o agente for instalado no dispositivo e a comunicação com a ThousandEyes Cloud for confirmada, crie um teste. Para criar um teste, navegue em Network & App Synthetics >Test Settings.



Na tela superior direita, clique no + ícone.

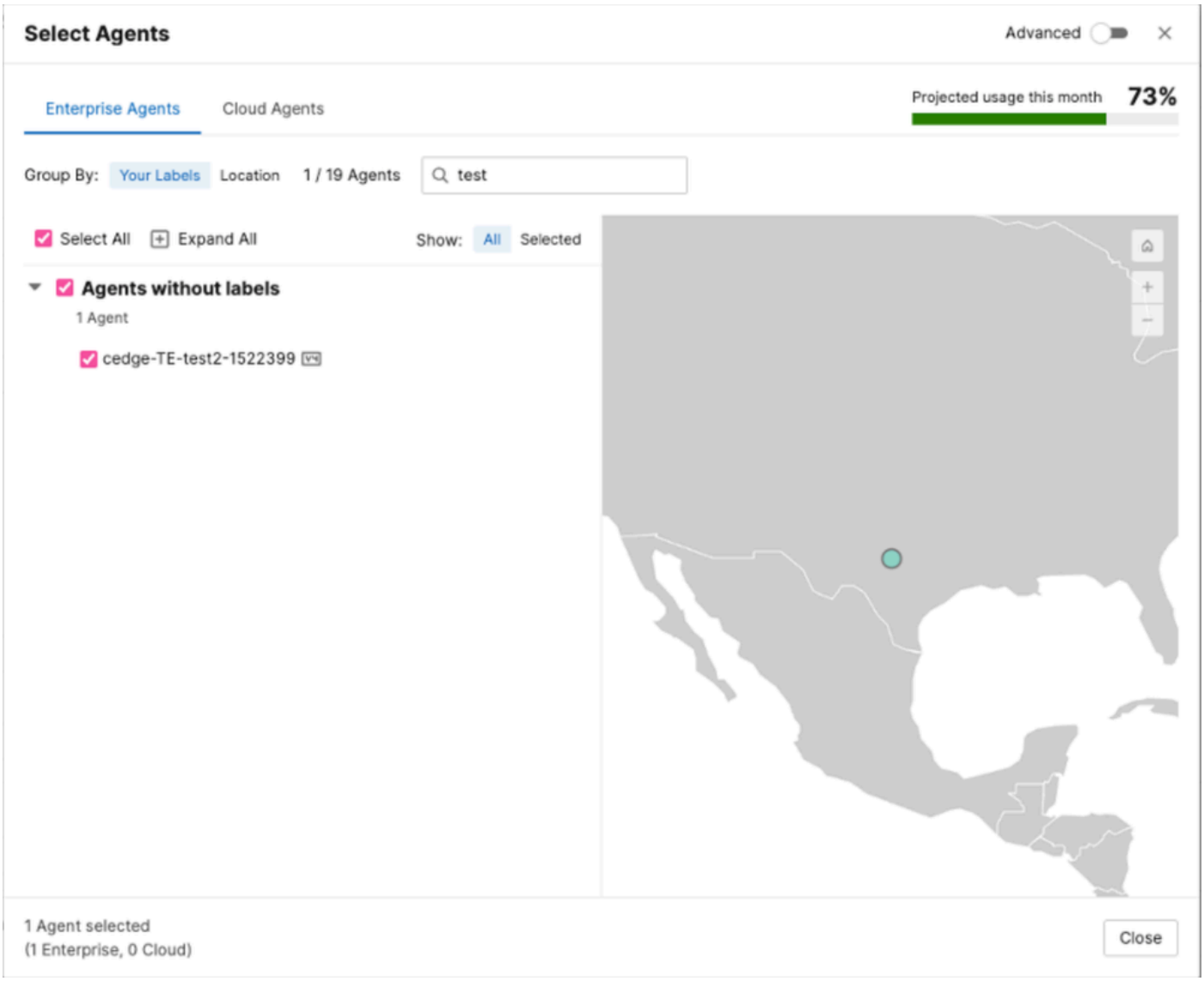


No novo Painel, selecione Teste de agente para servidor.



Na seção "Target", selecione o endereço IP necessário para usar o teste. Neste exemplo, foi usado 192.168.1.47, que é o endereço IP de outro TLOC em um roteador diferente dentro da mesma sub-rede.

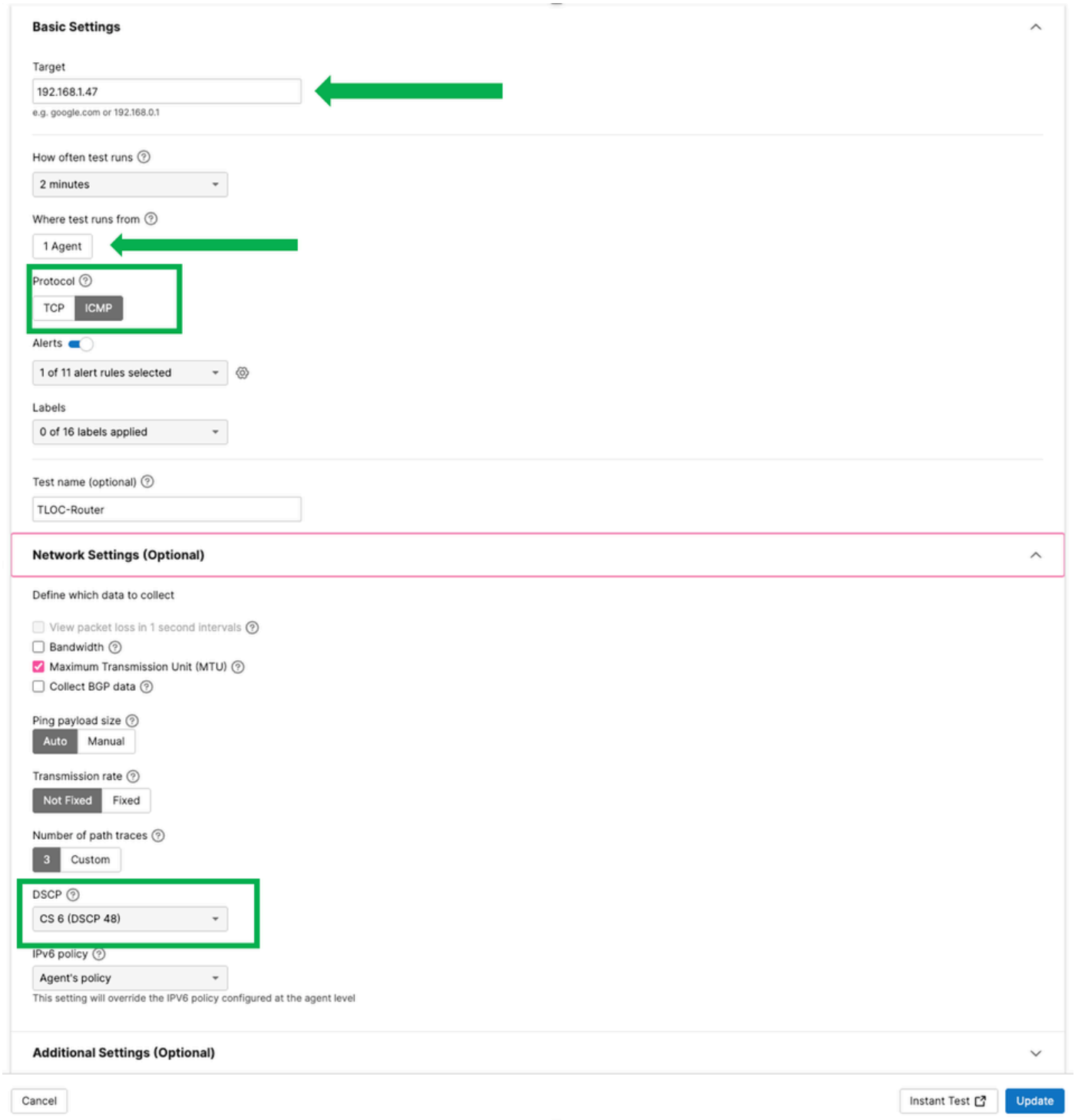
Em "Where test runs From", selecione o agente criado para o roteador (contém o nome de host do roteador) conforme mostrado abaixo:



Selecionar protocolo ICMP

Na seção Network Settings (Optional), selecione o DSCP e clique em Update.

Na mesma seção, clique em Instant Test.



Configurar SD-WAN

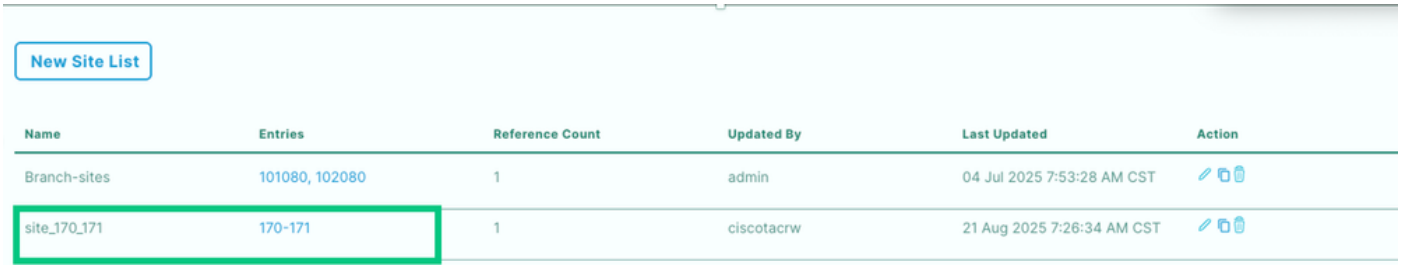
Use o documento de referência para configurar o Agente de Mil Olhos no Roteador de Borda [Configurar Mil Olhos em Dispositivos SD-WAN]

Quando o Agente ThousandEyes estiver instalado no roteador, o modelo ThousandEyes exibirá as informações:

Configurar DSCP

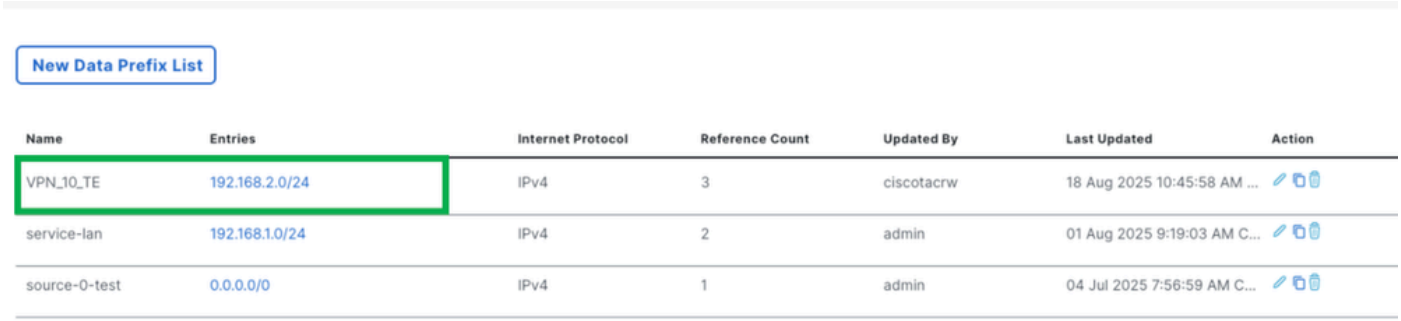
Navegue até Configuration > Policies >Centralized Policy > Clique em Add policy. Ao criar grupo de interesse, adicione Site, VPN e Prefixo de Dados.

Site (Site onde o Agente ThousandEyes foi instalado)



VPN (Serviço VPN)

O Prefixo de Dados (Incluir a sub-rede configurada no Modelo ThousandEyes) neste exemplo usou a sub-rede 192.168.2.0/24.



Clique em Next > Next, na seção Configure Traffic Rules, selecione Traffic Data e clique em Add Policy.

Selecione DSCP, neste exemplo, used 48

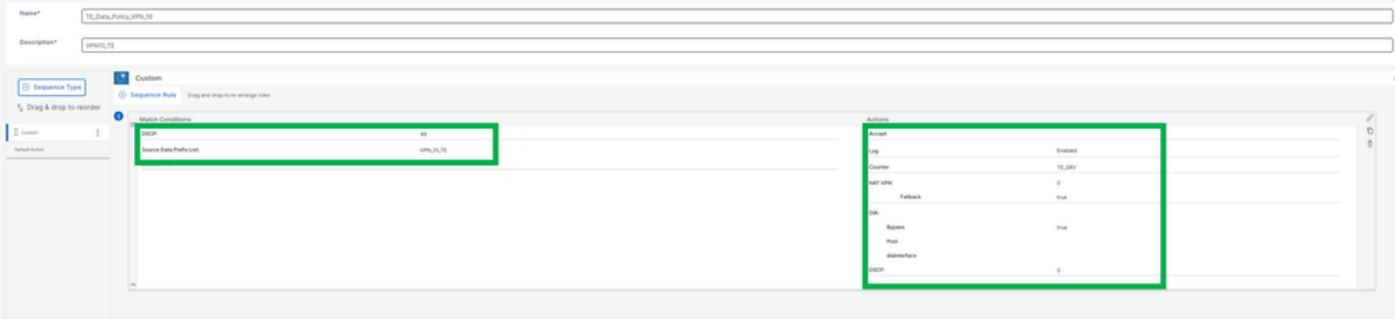
Escolha a opção "Lista de prefixos de dados de origem". Use "VPN_10_TE" (conforme documentado anteriormente), que é a rede usada para a configuração ThousandEyes no roteador.

Na seção Ações:

Selecione NAT VPN

Fallback

O DSCP neste exemplo é configurado como 0



Ação padrão ativada.

Clique em Avançar, adicione o nome da política e a Descrição da política. Na seção Dados de tráfego, clique em Novo site/Lista de regiões de WAN e Lista VPN, salve a política e ative-a.

Depois que a política tiver sido ativada, verifique no roteador a política aplicada:

Execute o comando show sdwan policy from-vsmart

```
cedge-TE-test2#show sdwan  policy from-vsmart
from-vsmart data-policy _VPN_10_TE_Data_Policy_VPN_10
 direction from-service
 vpn-list VPN_10
  sequence 1
   match
    source-data-prefix-list VPN_10_TE
    dscp                    48
   action accept
    count TE_SRV_1549695060
    nat use-vpn 0
    nat fallback
    log
    set
     dscp 0

  default-action accept
from-vsmart lists vpn-list VPN_10
 vpn 10
from-vsmart lists data-prefix-list VPN_10_TE
 ip-prefix 192.168.2.0/24
```

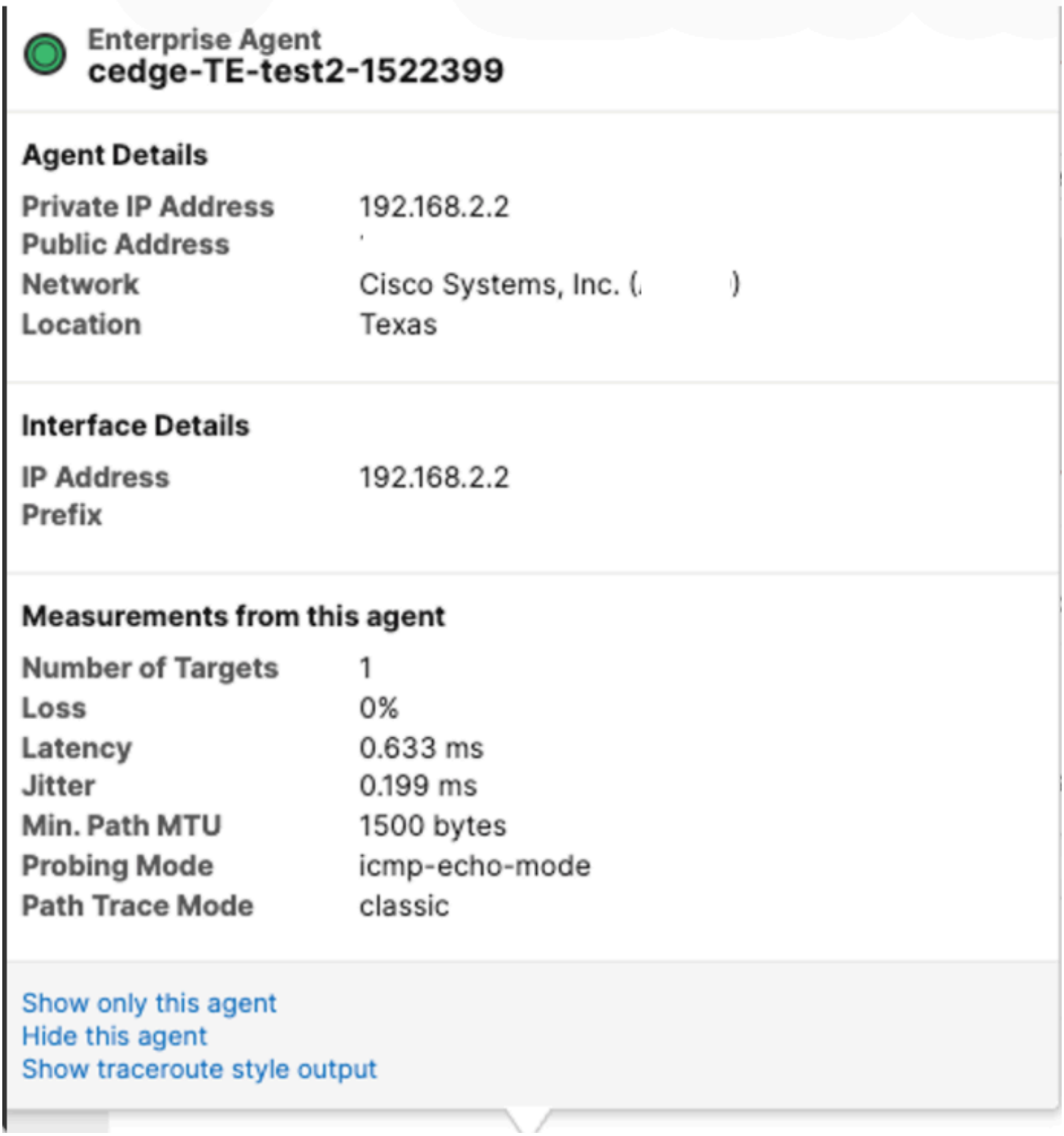
Verificar

Para executar um Teste, clique em Instat Test e abra uma nova janela.

Uma vez que o teste tenha terminado, você pode ver o caminho que tomou para alcançar o 192.168.1.47

Agent192.168.2.2 >>>>>DG TE 192.168.2.1 >>>>>Test 192.168.1.47

Onde foi marcado como dscp48 antes de ir para a subjacência e depois de ir para a subjacência é marcado como 0.



Configure um rastreamento FIA no roteador de borda:

```
debug platform condition ipv4 <ip address> both

debug platform packet-trace packet 2048 circular fia-trace data-size 4096

debug platform packet-trace copy packet both size 128 L2
```

Abrir um pacote:

<#root>

```
cedge-TE-test2#show platform  packet-trace  packet 0 decode
Packet: 0           CBUG ID: 3480
Summary
  Input     : VirtualPortGroup4
  Output    : GigabitEthernet0/0/0
  State     : FWD
  Timestamp
    Start   : 149091925690917 ns (08/19/2025 19:30:43.807639 UTC)
    Stop    : 149091925874126 ns (08/19/2025 19:30:43.807822 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : VirtualPortGroup4
    Output      : <unknown>
    Source      : 192.168.2.2
    Destination : 192.168.1.47
    Protocol    : 1 (ICMP)
  <Omitted output>
  Feature: NBAR
    Packet number in flow: N/A
    Classification state: Final
    Classification name: ping
    Classification ID: 1404 [CANA-L7:479]
    Candidate classification sources:
      DPI: ping [1404]
    Early cls priority: 0
    Permit apps list id: 0
    Sdavc Early prioirty as app: 0
    Classification visibility name: ping
    Classification visibility ID: 1404 [CANA-L7:479]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
    Is FIF (first in flow) packet: False
    TPH-MQC bitmask value: 0x0
    Source MAC address: 52:54:DD:82:B5:F8
    Destination MAC address: 00:27:90:64:D6:D0
    Traffic Categories: N/A
  Feature: IPV4_INPUT_STILE_LEGACY
    Entry       : Input - 0x8142ecc0
    Input       : VirtualPortGroup4
    Output      : <unknown>
    Lapsed time : 23615 ns
 <Omitted output>
  Feature: SDWAN Data Policy IN
    VPN ID      : 10
    VRF         : 2
    Policy Name  :

_VPN_10_DP_VPN10_TLOC-VPN_10 (CG:5)

 <<<<<<<<<<<
    Seq         : 1
    DNS Flags   : (0x0) NONE
    Policy Flags : 0x80210018
    Policy Flags2: 0x0
    Action      : POL_LOG
    Action      :

SET_DSCP default(0)

   <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

```
Action       : REDIRECT_NAT
Action       : NAT_FALLBACK
```

Informações Relacionadas

- Configure ThousandEyes em dispositivos SD-WAN
- Suporte Técnico e Documentação - Cisco Systems

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.