使用DSCP标记配置ThousandEyes Agent-to-Server SD-WAN Service-Side

目录

简介

本文档介绍如何使用DSCP标记配置ThousandEyes Agent-to-Server SD-WAN，以便在Cisco SD-WAN重叠中监控流量。

先决条件

要求

Cisco建议您了解这些主题。

- SD-WAN概述
- 模板
- 千只眼

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco Manager版本20.15.3
- 思科验证器版本20.15.3
- 思科控制器版本20.15.3
- 集成多业务路由器(ISR)4331/K9版本17.12.3a
- thousandeyes-enterprise-agent-5.5.1.cisco

初步配置

- 配置 DNS:路由器可以解析DNS并访问VPN 0上的Internet。
- 配置NAT DIA:路由器上需要存在DIA配置。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

代理到服务器测试

要运行“代理到服务器”测试，必须在服务VPN上配置ThousandEyes代理。在此方案中，服务器是受监控的TLOC IP地址。通常，代理与服务器测试用于监控服务器；但是，在本例中，它用于监控与代理托管地位于不同站点的TLOC接口。

如果存在多个TLOC接口，请使用NAT直接互联网访问(DIA)和数据策略将流量重定向到所需的VPN 0 TLOC接口。根据在ThousandEyes中代理端配置的DSCP值设置匹配条件，以重定向到VPN 0，并通过VPN 0进行标记，同时执行标记，以避免ISP通过自己的DSCP标记可能具有的任何超步。

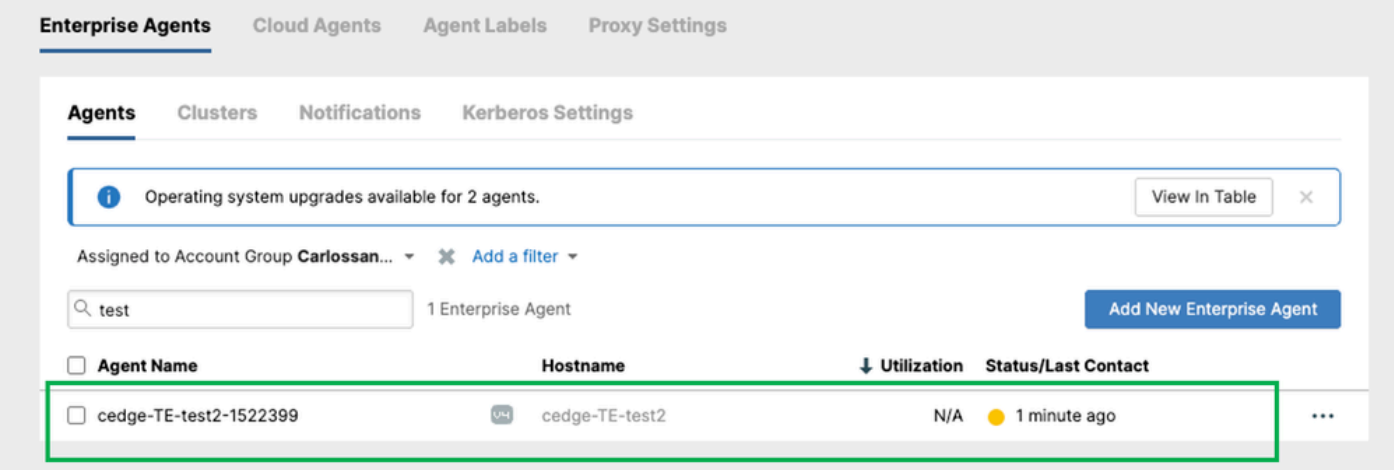
配置

配置ThousandEyes Test和DSCP

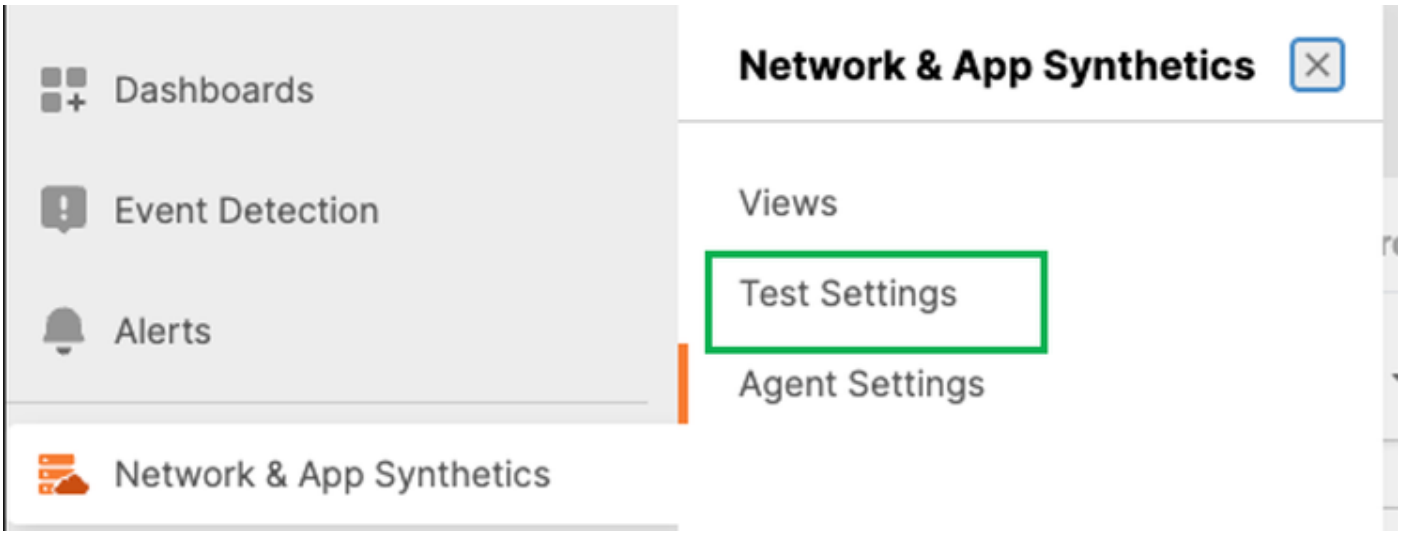
要配置差分服务代码点(DSCP)，请执行以下操作：

1. 从Cisco ThosandEyes Agentpage登录ThousandEyes帐户。

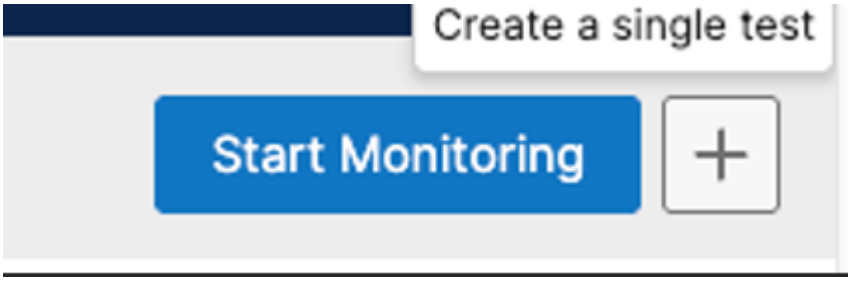
验证路由器中安装的代理是否与ThousandEyes Cloud通信。



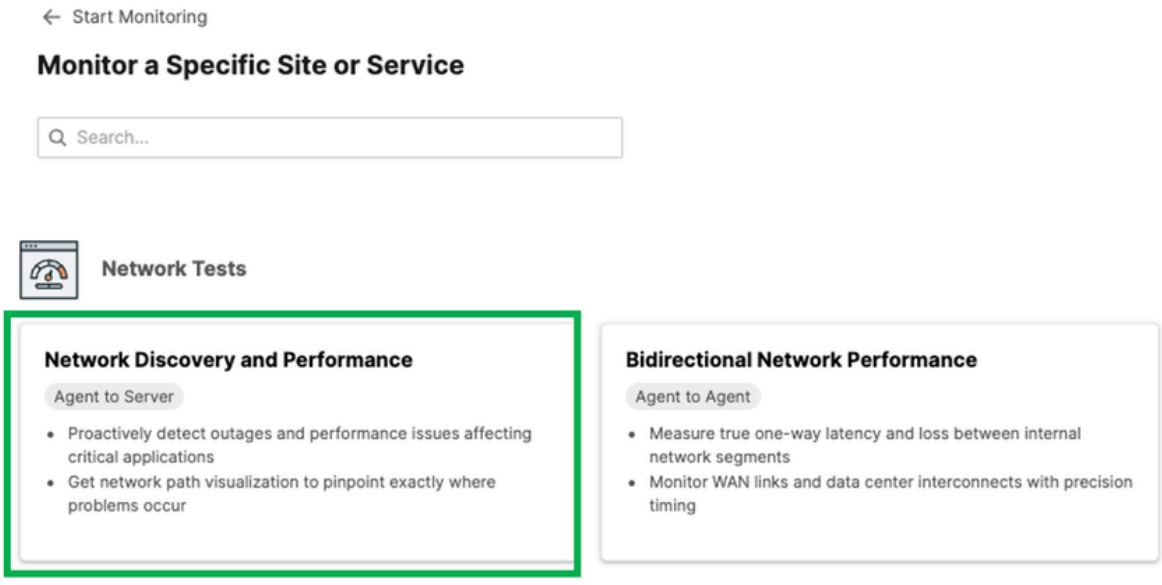
将代理安装到设备上并确认与ThousandEyes Cloud的通信后，创建测试。要创建测试，请在Network & App Synthetics > Test Settings上导航。



在右上角屏幕中，点击+图标。

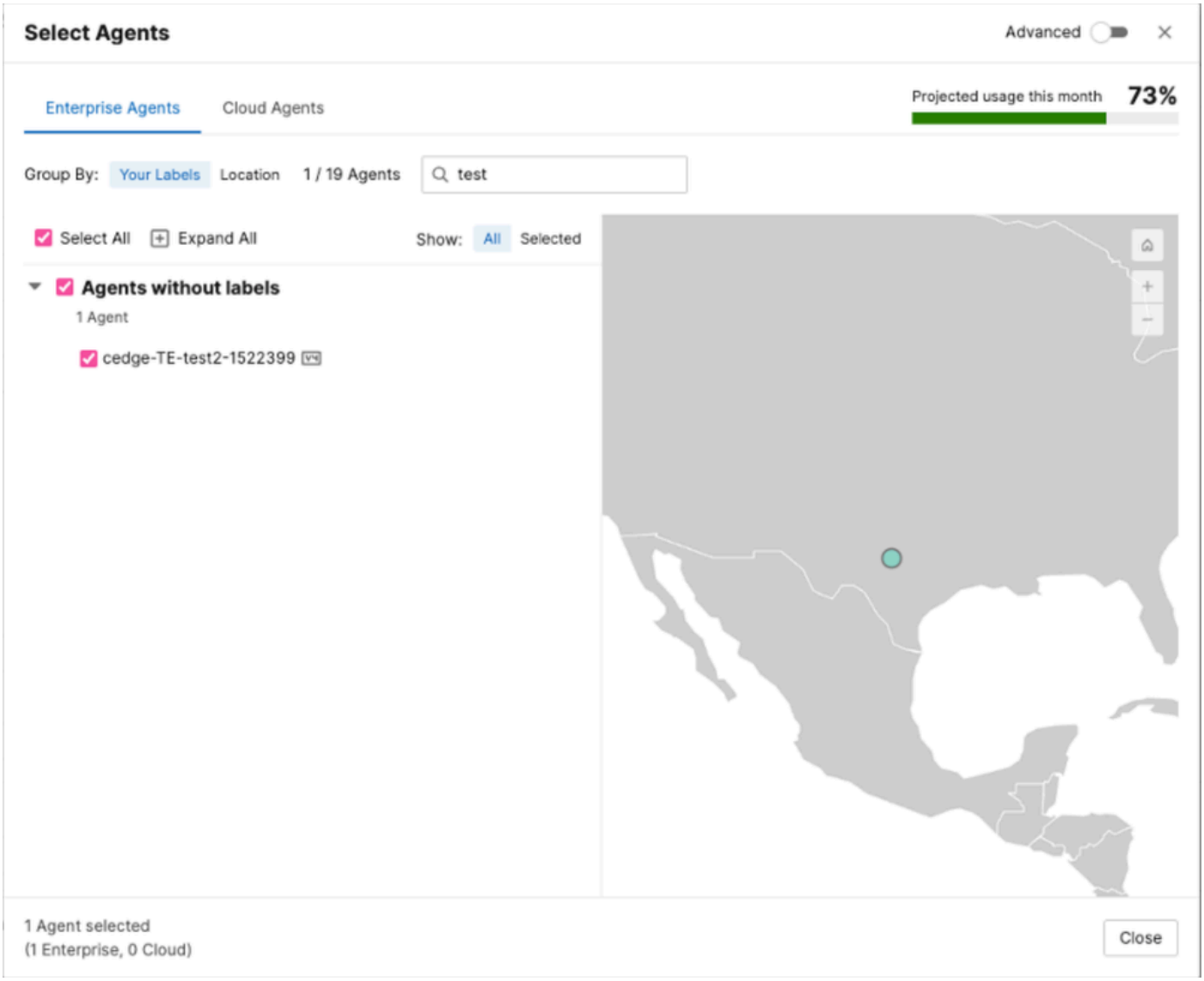


在新控制面板中，选择Agent to Server Test。



在“目标”部分，选择测试所需的IP地址。在本示例中，使用192.168.1.47，这是同一子网内不同路由器上另一个TLOC的IP地址。

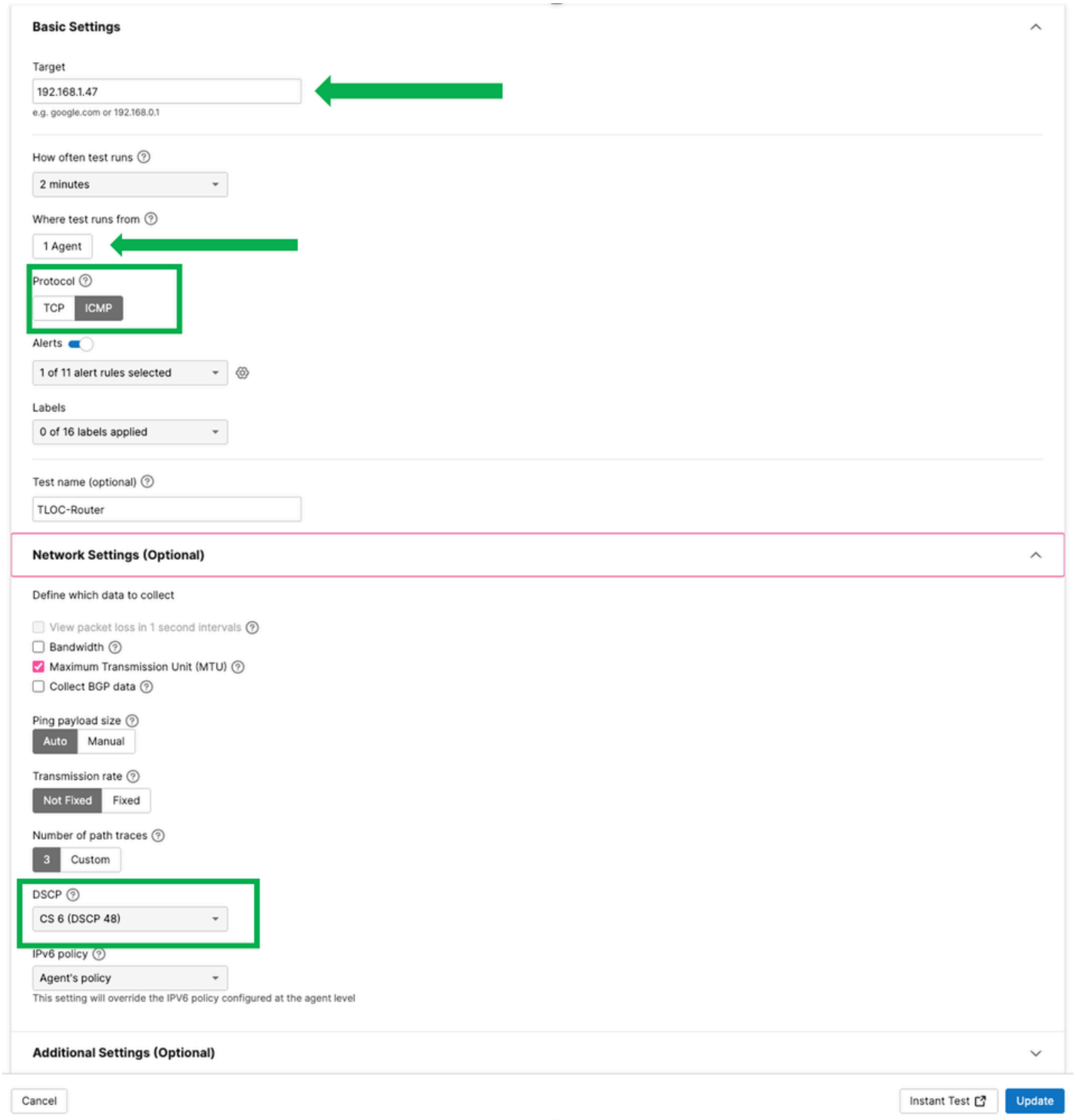
在Where test runs From中，选择为路由器创建的代理（包含路由器的主机名），如下所示：



选择ICMP协议

在网络设置（可选）部分中，选择DSCP并点击更新。

在同一部分中单击Instant Test。



配置SD-WAN

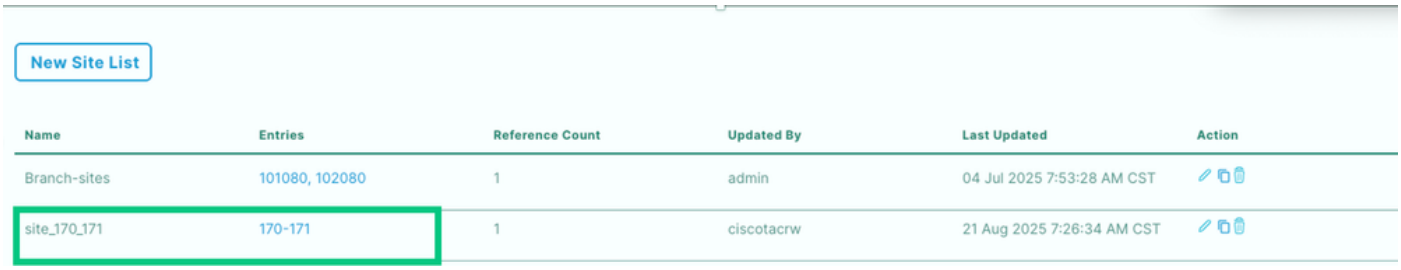
使用参考文档在边缘路由器上配置Thousand Eyes Agent[在SD-WAN设备上配置ThousandEyes]

在路由器上安装ThousandEyes Agent后，ThousandEyes模板将显示以下信息：

配置DSCP

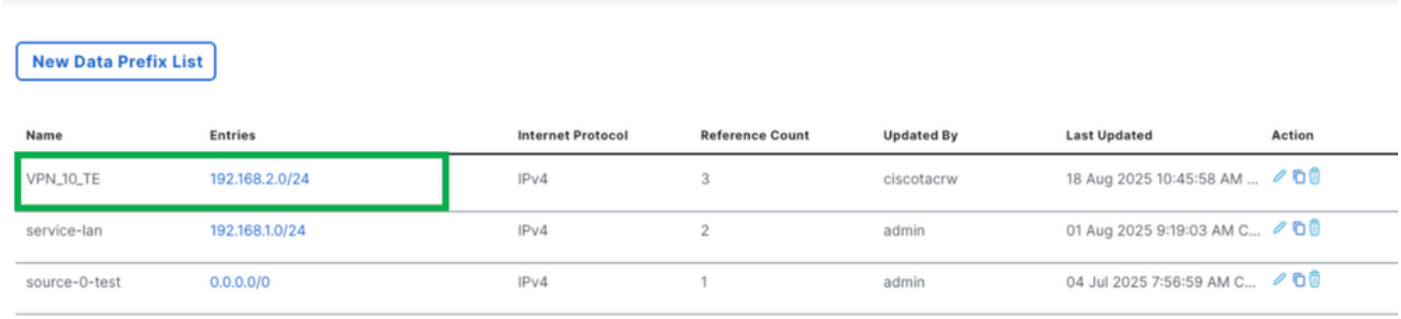
导航到Configuration> Policies >Centralized Policy >Click Add policy。在创建兴趣组时，添加站点、VPN和数据前缀。

站点（安装ThousandEyes Agent的站点）



VPN（服务VPN）

本示例中的数据前缀（包括在ThousandEyes模板上配置的子网）使用子网192.168.2.0/24。



单击Next > Next，在Configure Traffic Rules部分，选择Traffic Data，然后单击Add Policy。

选择DSCP，在此示例中使用48

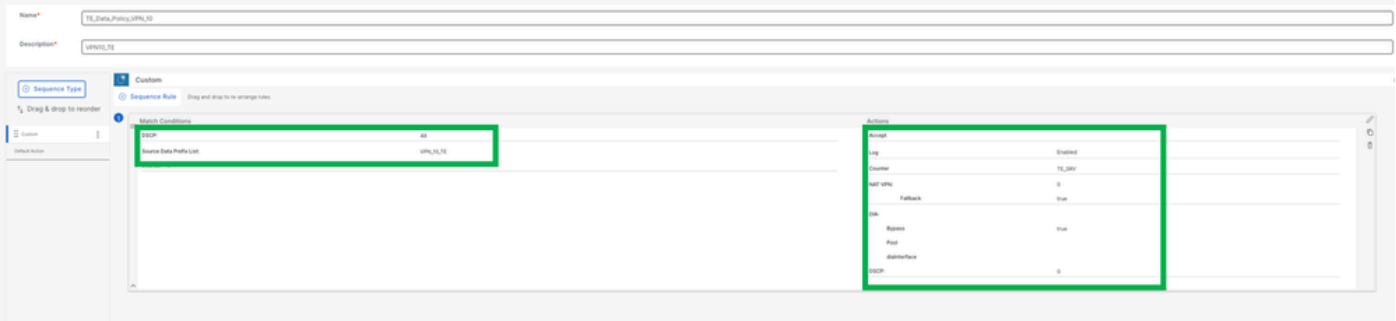
选择“源数据前缀列表”选项。使用"VPN_10_TE"（如前所述），这是用于路由器上ThousandEyes配置的网络。

在操作部分：

选择NAT VPN

回退

在本示例中，配置的DSCP为0



默认操作已启用。

单击Next，添加Policy name和Policy Description。在Traffic Data部分，点击New Site/WAN Region List and VPN List，保存策略并激活它。

激活策略后，在路由器中验证应用的策略：

运行show sdwan policy from-vsmart命令

```
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
```

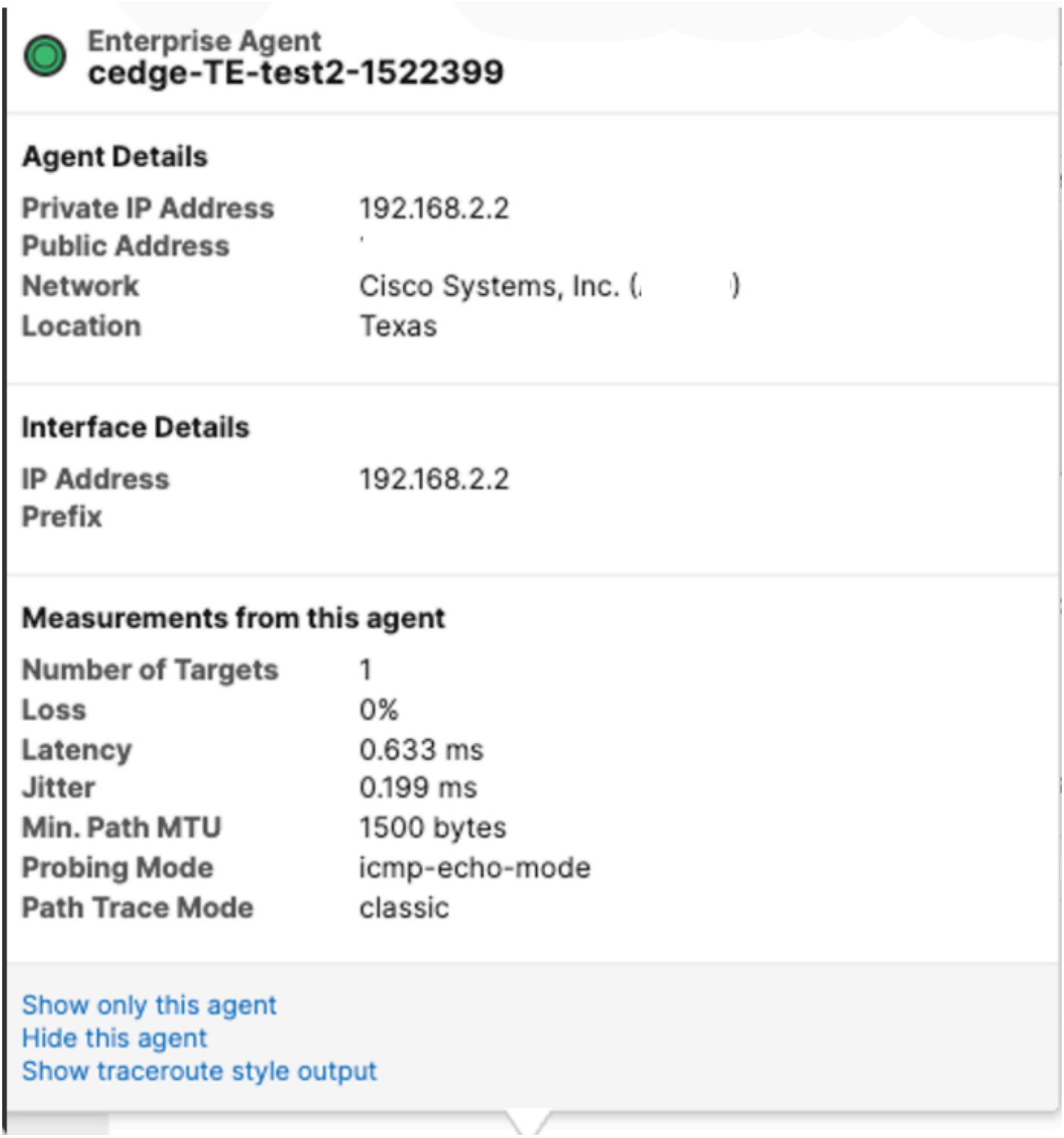
验证

要运行测试，请单击Install Test并打开一个新窗口。

测试完成后，您可以看到到达192.168.1.47所用的路径

Agent 192.168.2.2 >>>>>DG TE 192.168.2.1 >>>>>Test 192.168.1.47

其中，在去下层之前标记为dscp48，在去下层之后标记为0。



在边缘路由器上配置FIA跟踪：

```
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
```

打开数据包：

<#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
```

相关信息

- 在SD-WAN设备上配置ThousandEyes
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。