Configuración de ThousandEyes Agent-to-Server SD-WAN Service-Side con marcación DSCP

Contenido

Introducción

Este documento describe la configuración de ThousandEyes Agent-to-Server SD-WAN con marcado DSCP para el monitoreo de tráfico en una superposición SD-WAN de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- Descripción general de SD-WAN
- Plantillas
- Mil ojos

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco Manager versión 20.15.3
- Cisco Validator Versión 20.15.3
- Controlador de Cisco versión 20.15.3

- Routers de servicios integrados (ISR)4331/K9 versión 17.12.3a
- thousandeyes-enterprise-agent-5.5.1.cisco

Configuraciones preliminares

- Configurar DNS: El router puede resolver el DNS y acceder a Internet en VPN 0.
- Configuración de DIA NAT: La configuración DIA debe estar presente en el router.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Prueba de agente a servidor

Para ejecutar una prueba de agente a servidor, el agente ThousandEyes debe estar configurado en la VPN de servicio. En este escenario, el servidor es la dirección IP de TLOC que se monitorea. Normalmente, una prueba de Agente a Servidor se utiliza para supervisar un servidor; sin embargo, en este caso, se utiliza para supervisar una interfaz TLOC ubicada en un sitio diferente del que alberga el agente.

Si hay varias interfaces TLOC, utilice el acceso directo a Internet (DIA) de NAT y una política de datos para redirigir el tráfico a la interfaz TLOC VPN 0 deseada. Establezca los criterios de coincidencia basados en el valor DSCP configurado en el lado del agente en ThousandEyes para ser redirigido a y a través de VPN 0, mientras que al mismo tiempo realiza la demarcación para evitar cualquier sobrepaso que el ISP pueda tener con su propia marcación DSCP.

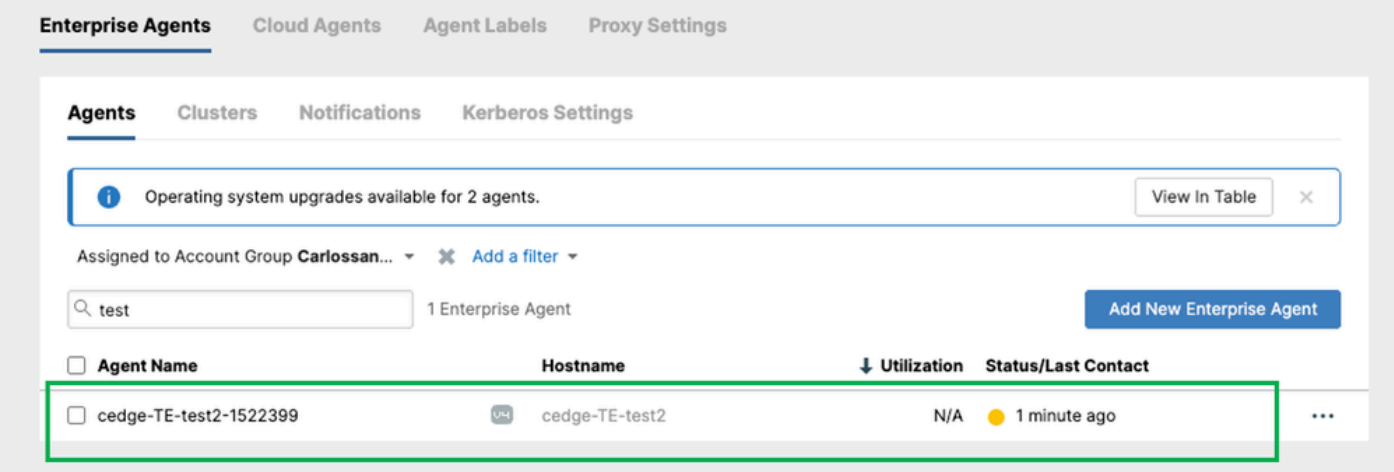
Configurar

Configuración de la prueba ThousandEyes y DSCP

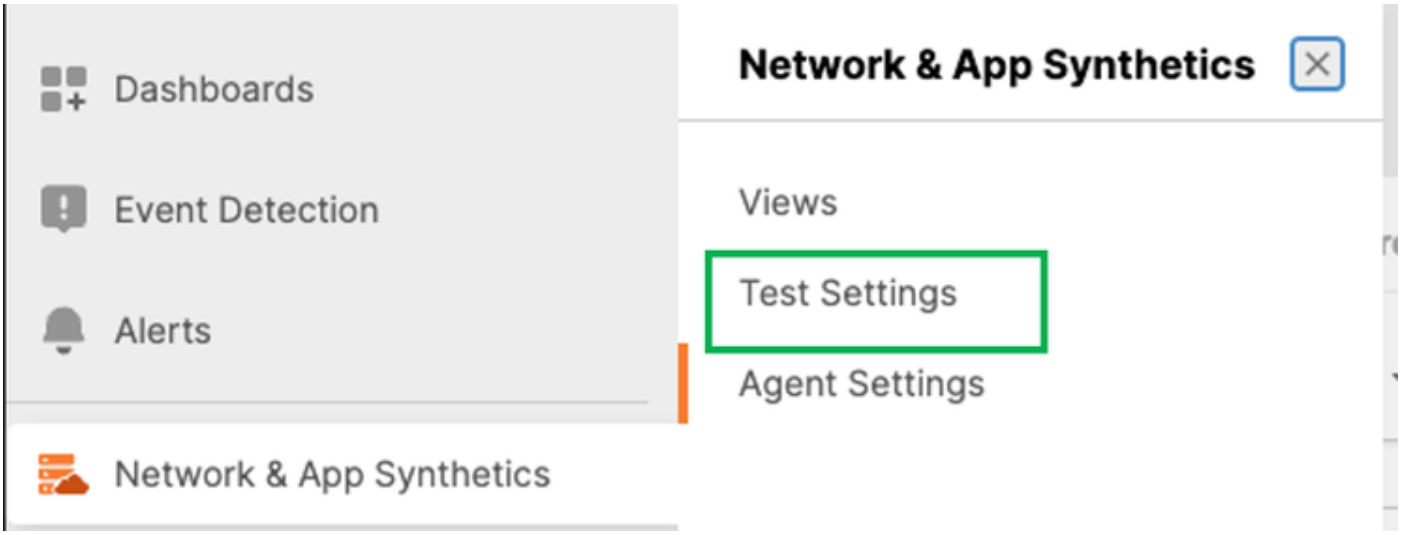
Para configurar el punto de código de servicios diferenciados (DSCP):

1. Inicie sesión en la cuenta ThousandEyes desde la páginaCisco ThosandEyes Agent.

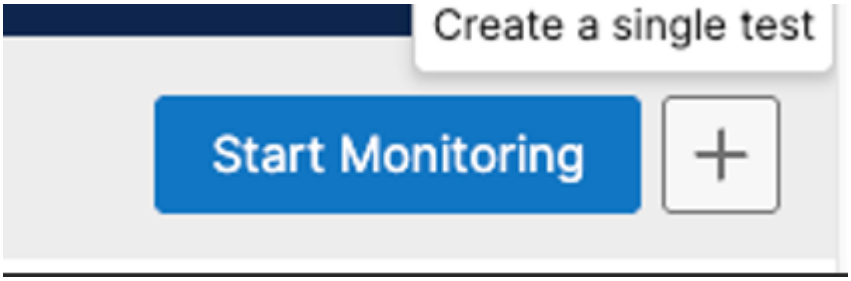
Compruebe que el agente instalado en el router tiene comunicación con la nube de ThousandEyes.



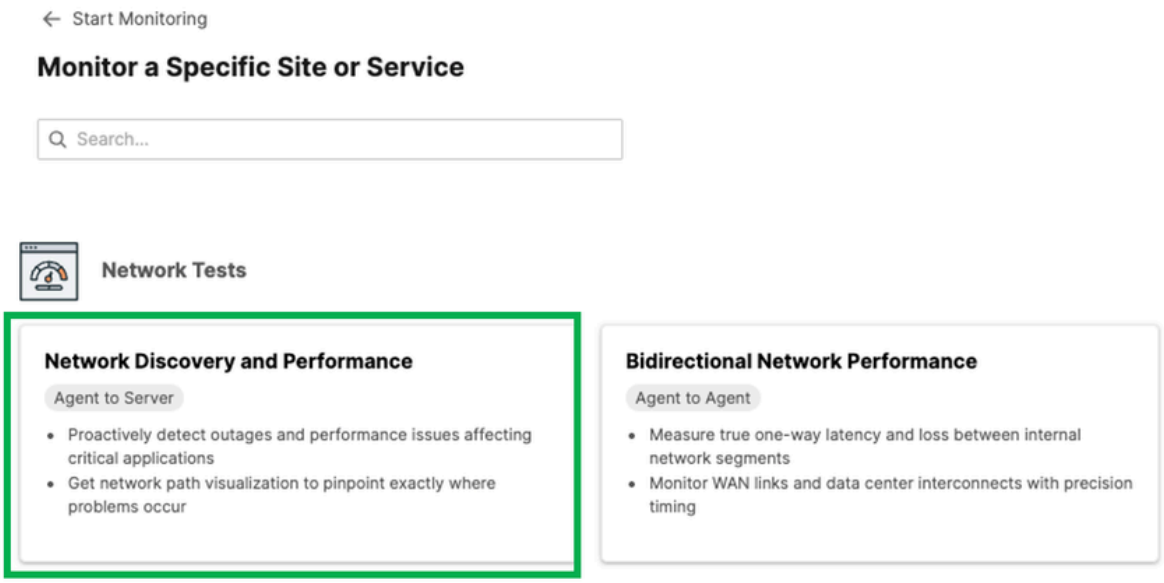
Una vez que el agente esté instalado en el dispositivo y se confirme la comunicación con la nube de ThousandEyes, cree una prueba. Para crear una prueba, navegue en Network & App Synthetics >Test Settings .



En la pantalla superior derecha, haga clic en el icono +.

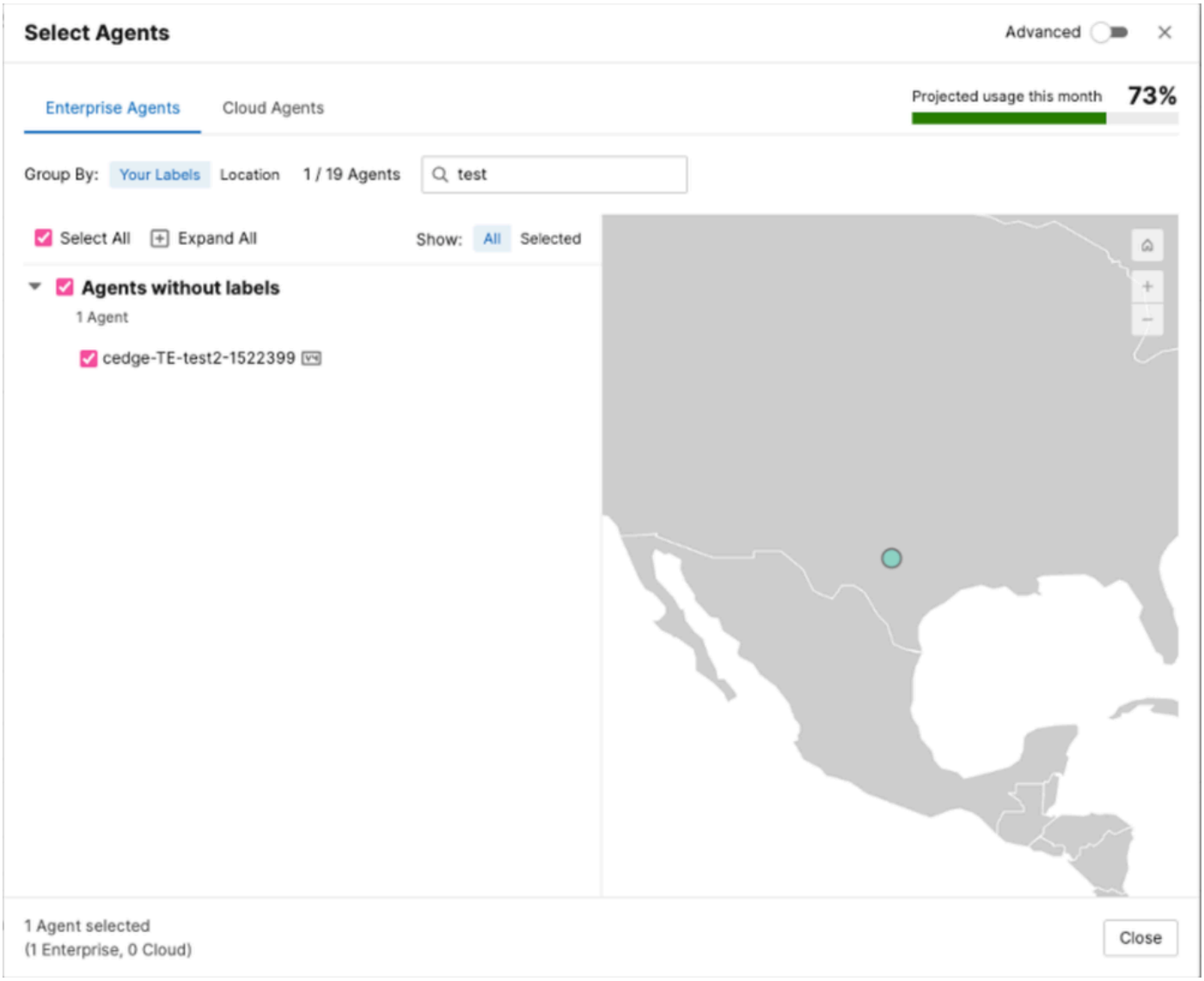


En el nuevo panel, seleccione Prueba de agente a servidor.



En la sección "Destino", seleccione la dirección IP necesaria para la prueba. En este ejemplo, en este ejemplo se utilizó 192.168.1.47, que es la dirección IP de otro TLOC en un router diferente dentro de la misma subred.

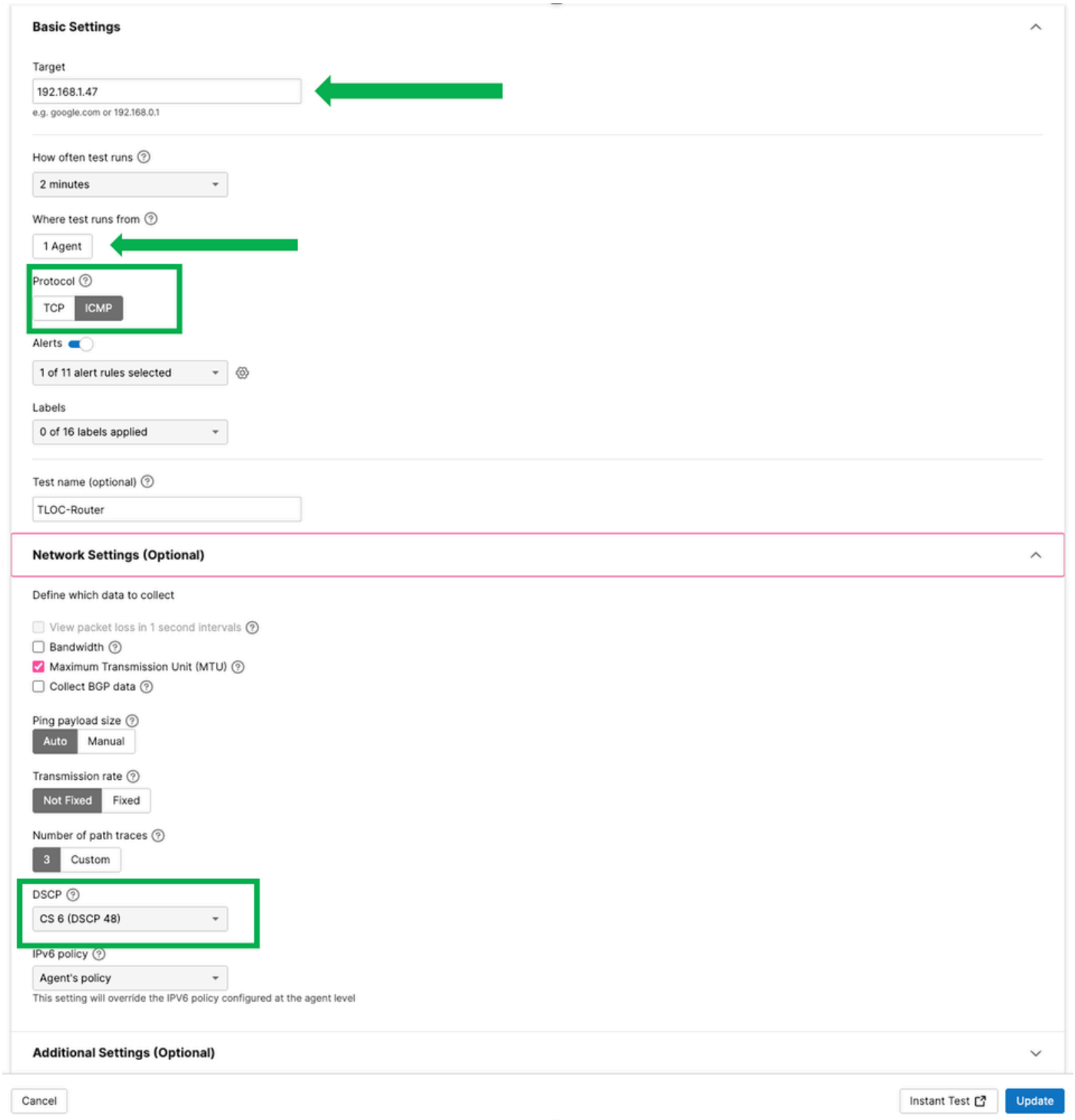
En "De dónde se ejecuta la prueba", seleccione el agente creado para el router (que contiene el nombre de host del router) como se muestra a continuación:



Seleccionar protocolo ICMP

En la sección Network Settings (Optional), seleccione el DSCP y haga clic en Update.

En la misma sección, haga clic en Instant Test.



Configuración de SD-WAN

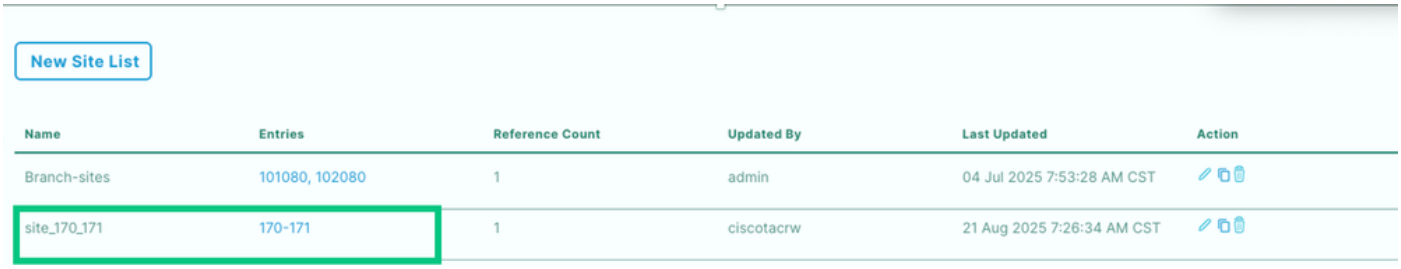
Utilice el documento de referencia para configurar Thousand Eyes Agent en el router de borde [Configure ThousandEyes en dispositivos SD-WAN]

Una vez que ThousandEyes Agent está instalado en el router, la plantilla ThousandEyes muestra la información:

Configurar DSCP

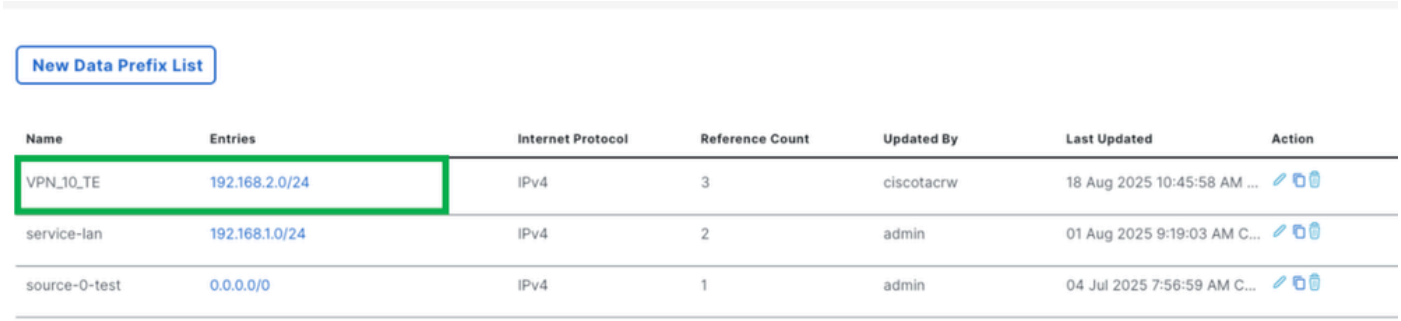
Vaya a Configuración > Políticas >Política centralizada > Haga clic en Agregar política. Al crear un grupo de interés, agregue Sitio, VPN y Prefijo de datos.

Sitio (sitio donde se instaló ThousandEyes Agent)



VPN (VPN de servicio)

El prefijo de datos (que incluye la subred configurada en la plantilla ThousandEyes) de este ejemplo utilizó la subred 192.168.2.0/24.



Haga clic en Next > Next, en la sección Configure Traffic Rules, seleccione Traffic Data y haga clic en Add Policy.

Seleccione DSCP; en este ejemplo se utilizó 48

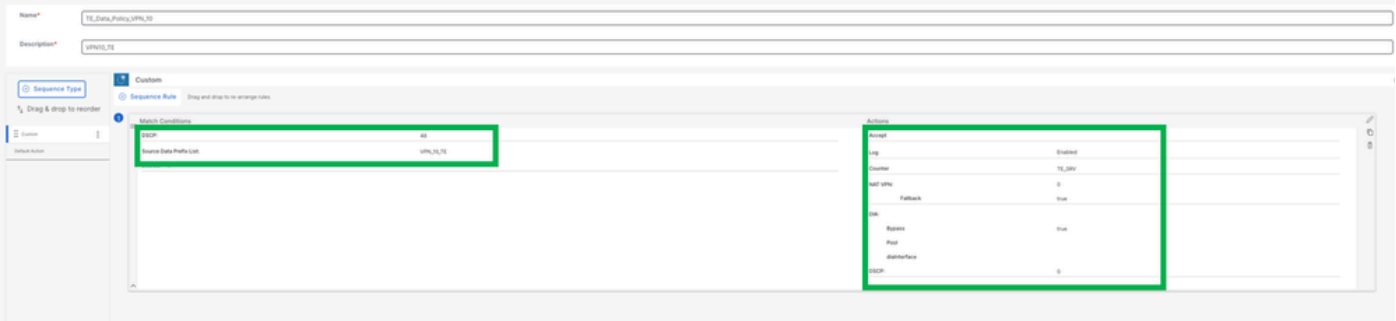
Elija la opción "Source Data Prefix List". Utilice "VPN_10_TE" (como se ha documentado anteriormente), que es la red utilizada para la configuración ThousandEyes en el router.

En la sección de acciones:

Seleccione NAT VPN

Reserva

DSCP en este ejemplo el DSCP configurado es 0



Acción predeterminada habilitada.

Haga clic en Siguiente, agregue el nombre y la descripción de la política. En la sección Traffic Data (Datos de tráfico), haga clic en New Site/WAN Region List (Nueva lista de sitios/región WAN y lista VPN), guarde la política y actívela.

Una vez activada la política, verifique en el router la política aplicada:

Ejecute el 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
```

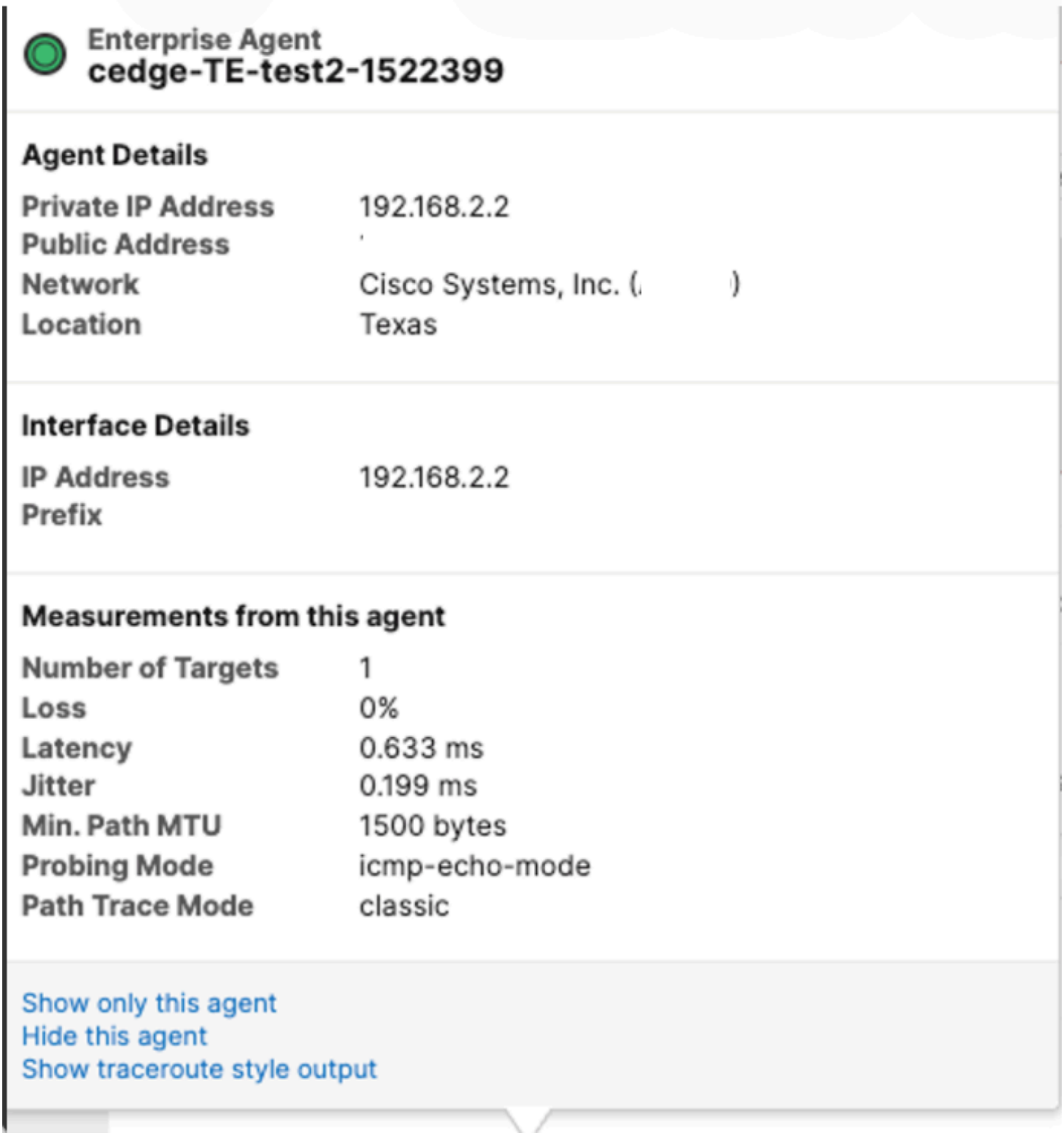
Verificación

Para ejecutar una prueba, haga clic en Instant Test y abra una nueva ventana.

Una vez finalizada la prueba, puede ver la ruta que tardó en alcanzar 192.168.1.47

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

Donde fue marcado como dscp48 antes de ir para la capa de base y después de ir sobre la capa de base es marca como 0.



Configure un seguimiento FIA en el router de borde:

```
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
```

Abra un paquete:

<#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
```

Información Relacionada

- Configuración de ThousandEyes en dispositivos SD-WAN
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).