ThousandEyes Agent-to-Server SD-WAN-servicekant configureren met DSCP-markering

Inhoud

Inleiding

Dit document beschrijft het configureren van ThousandEyes Agent-to-Server SD-WAN met DSCP-markering voor verkeersbewaking in een Cisco SD-WAN-overlay.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan.

- Algemeen overzicht van SD-WAN
- Sjablonen
- Duizend ogen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- Cisco Manager versie 20.15.3
- Cisco Validator versie 20.15.3
- Cisco Controller versie 20.15.3
- Integrated Service Routers (ISR)4331/K9 versie 17.12.3a
- ThousandYes-Enterprise-Agent-5.5.1.Cisco

Voorlopige configuraties

- Configureer DNS: De router kan DNS oplossen en toegang krijgen tot internet via VPN 0.
- NAT DIA configureren: de DIA-configuratie moet aanwezig zijn op de router.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Agent-naar-server testen

Om een Agent to Server-test uit te voeren, moet de ThousandEyes-agent zijn geconfigureerd op de VPN-service. In dit scenario is de server het IP-adres van TLOC dat wordt gecontroleerd. Meestal wordt een Agent-naar-server-test gebruikt om een server te bewaken. In dit geval wordt deze test echter gebruikt om een TLOC-interface te bewaken die zich op een andere locatie bevindt dan waar de agent wordt gehost.

Als er meerdere TLOC-interfaces zijn, gebruikt u NAT Direct Internet Access (DIA) en een gegevensbeleid om het verkeer om te leiden naar de gewenste VPN 0 TLOC-interface. Stel de matchcriteria in op basis van de DSCP-waarde die aan de agentzijde in ThousandEyes is geconfigureerd om naar en via de VPN 0 te worden omgeleid en tegelijkertijd de markering uit te voeren om te voorkomen dat de ISP met zijn eigen DSCP-markering wordt overschreden.

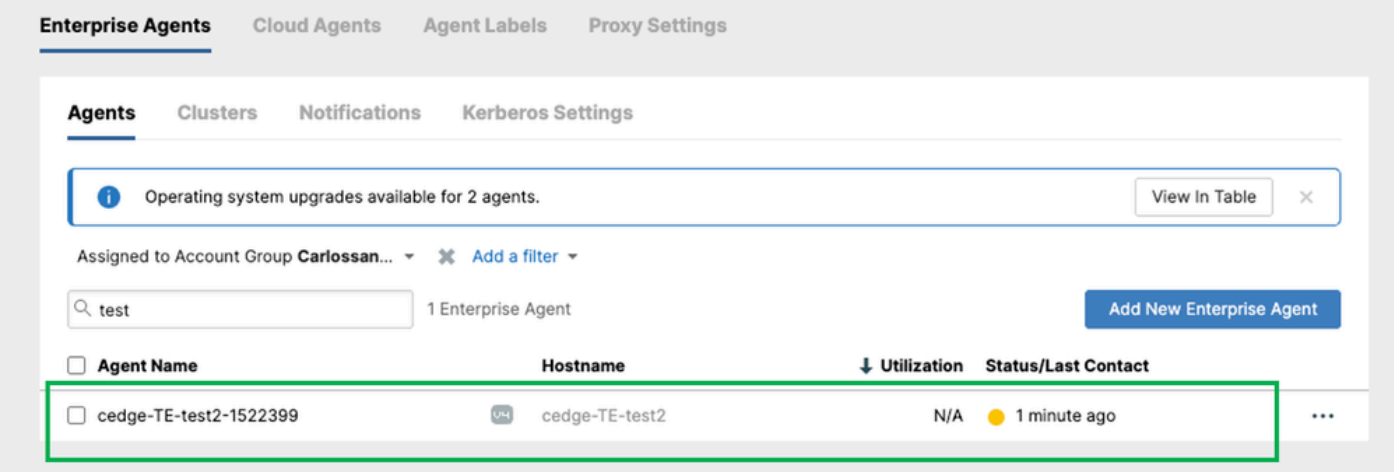
Configureren

Duizend ogen testen en DSCP configureren

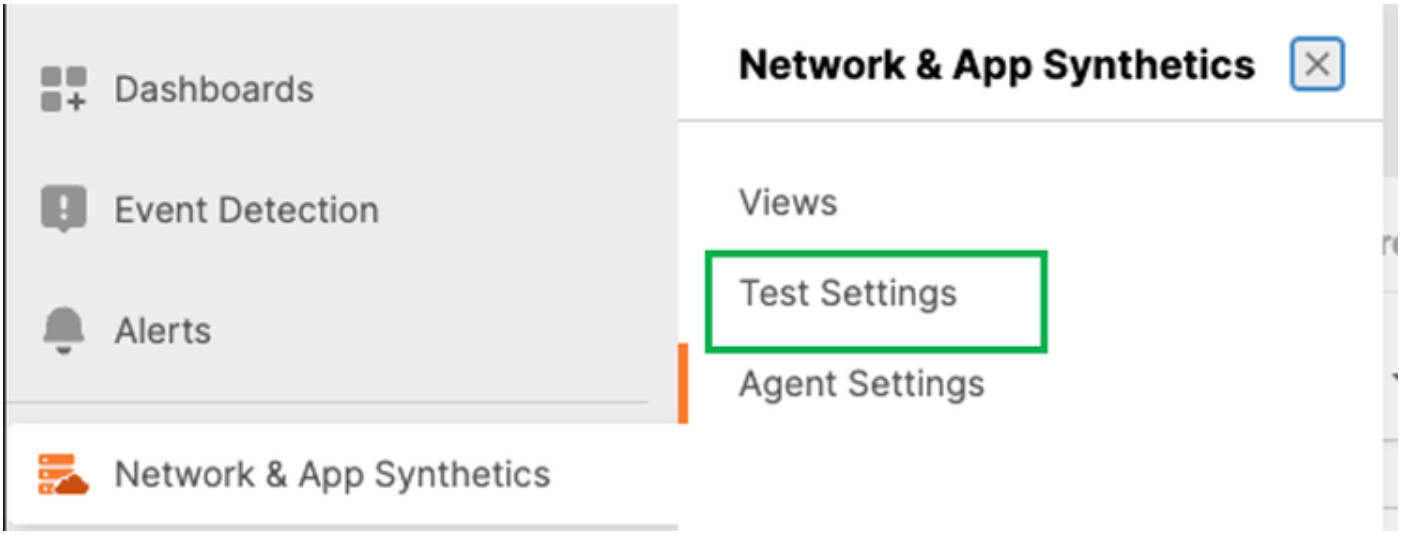
Differentiated Services Code Point (DSCP) configureren:

1. Meld u aan bij het ThousandEyes-account op de pagina van de Cisco ThousandEyes Agent.

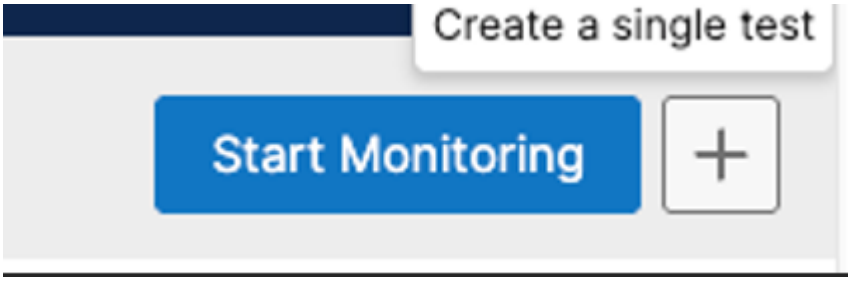
Controleer of de Agent die in de router is geïnstalleerd communicatie heeft met ThousandEyes Cloud.



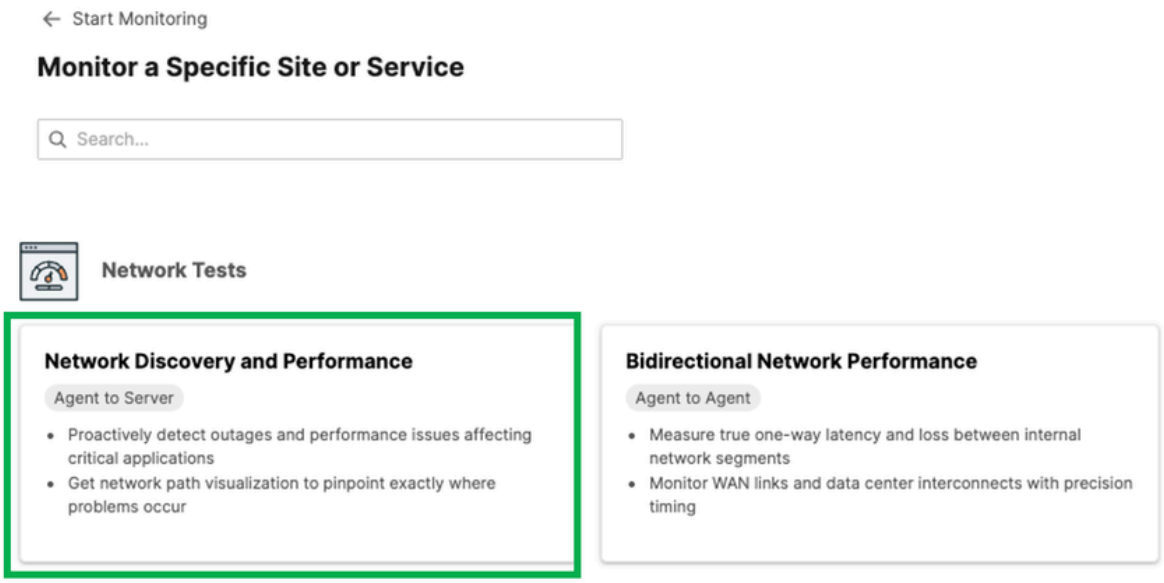
Nadat de agent op het apparaat is geïnstalleerd en de communicatie met de ThousandEyes Cloud is bevestigd, maakt u een test. Om een test aan te maken, navigeert u op Netwerk & App Synthetiek > Testinstellingen.



Klik in het scherm rechtsboven op het +-pictogram.

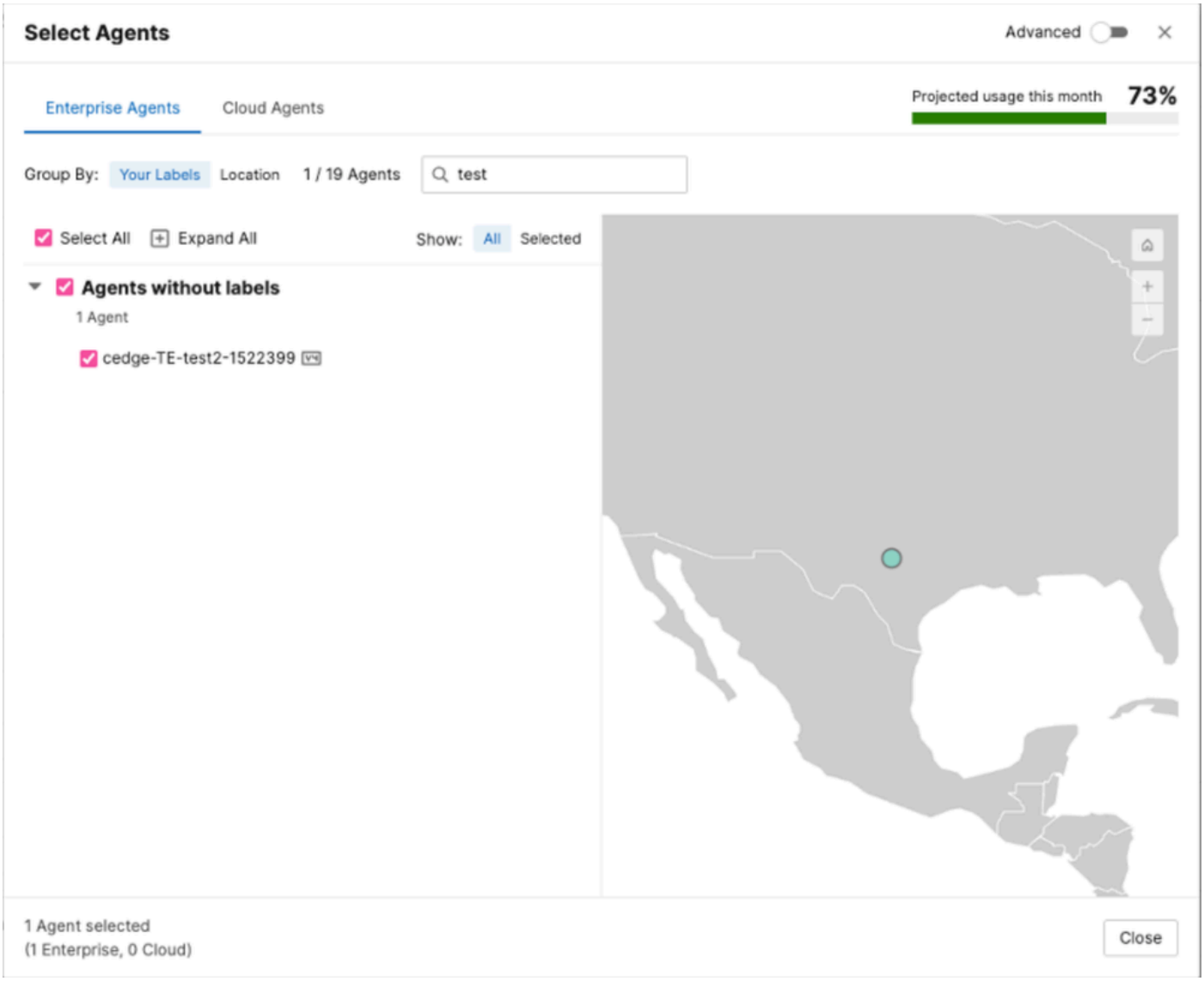


Selecteer in het nieuwe Dashboard Agent to Server Test.



Selecteer in het gedeelte "Doel" het IP-adres dat voor de test moet worden gebruikt. In dit voorbeeld wordt in dit voorbeeld 192.168.1.47 gebruikt, wat het IP-adres is van een andere TLOC op een andere router binnen hetzelfde subnet.

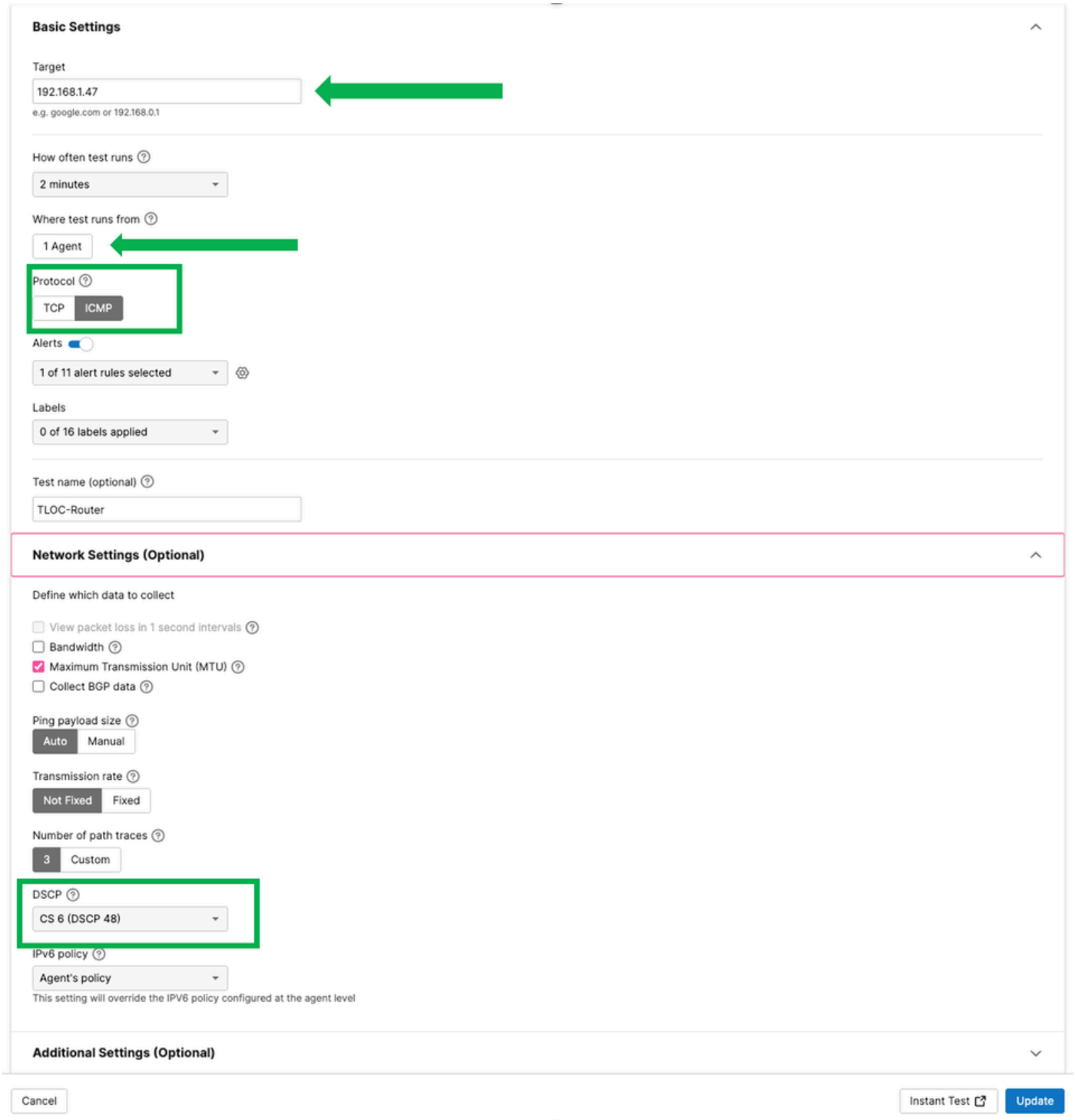
Selecteer in "Where test runs From" de agent die is gemaakt voor uw router (bevat de hostnaam van uw router), zoals hieronder wordt weergegeven:



ICMP-protocol selecteren

Selecteer in het gedeelte Netwerkinstellingen (optioneel) de optie DSCP en klik op Bijwerken.

Klik in hetzelfde gedeelte op Instant Test.



SD-WAN configureren

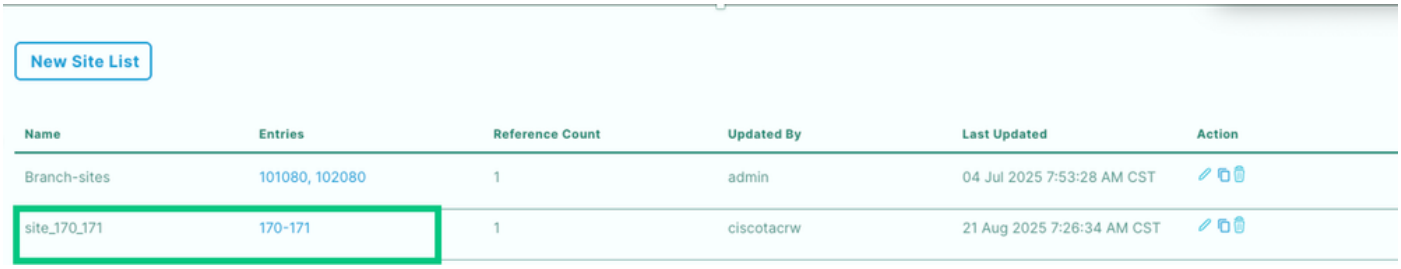
Gebruik het referentiedocument om Thousand Eyes Agent on Edge Router te configureren [Duizend ogen op SD-WAN-apparaten configureren]

Zodra de ThousandEyes Agent op de router is geïnstalleerd, geeft de ThousandEyes-sjabloon de volgende informatie weer:

DSCP configureren

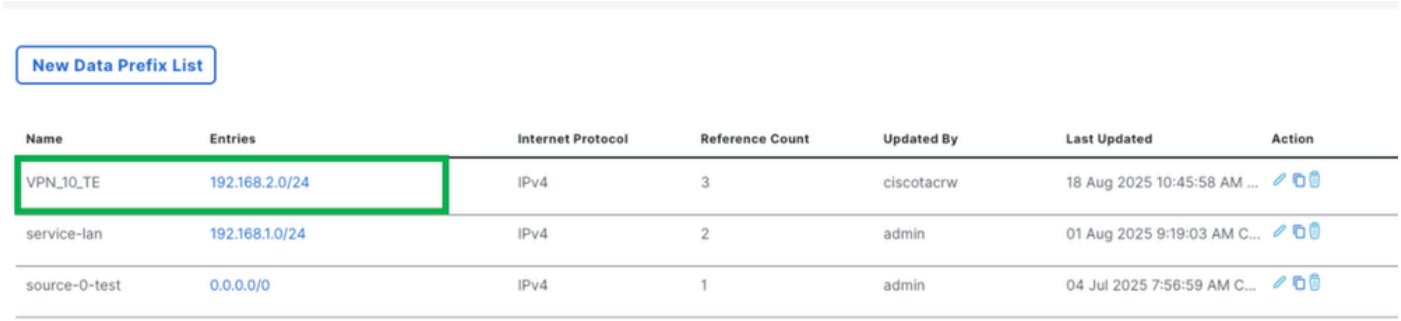
Navigeer naar Configuratie > Beleid >Gecentraliseerd Beleid > Klik op Beleid toevoegen. Voeg bij het maken van een groep van interesses Site, VPN en Data Prefix toe.

Site (Site waarop ThousandEyes Agent is geïnstalleerd)



VPN-service (VPN)

Data Prefix (Inclusief het subnet geconfigureerd op ThousandEyes Template) in dit voorbeeld gebruikt het subnet 192.168.2.0/24.



Klik op Volgende > Volgende, in het gedeelte Verkeersregels configureren, selecteer Verkeersgegevens en klik op Beleid toevoegen.

Selecteer DSCP, in dit voorbeeld gebruikt 48

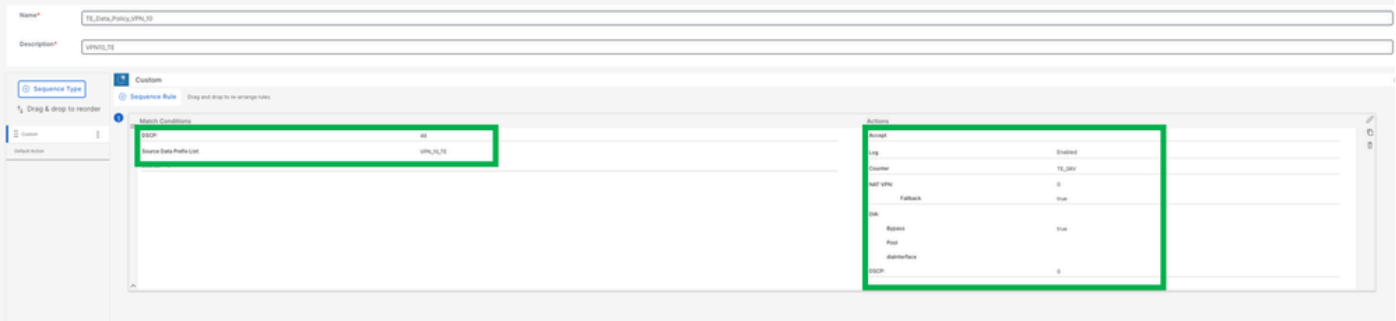
Kies de optie "Brongegevens prefix lijst". Gebruik "VPN_10_TE" (zoals eerder gedocumenteerd), het netwerk dat wordt gebruikt voor de ThousandEyes-configuratie op de router.

Over het gedeelte Acties:

Selecteer NAT VPN

noodlanding

DSCP in dit voorbeeld is de geconfigureerde DSCP 0



Standaardactie ingeschakeld.

Klik op Volgende, voeg de naam van het beleid en de beschrijving van het beleid toe. Klik in het gedeelte Verkeersgegevens op Nieuwe site/WAN-regiolijst en VPN-lijst, sla het beleid op en activeer het,

Nadat het beleid is geactiveerd, controleert u in de router het beleid dat is toegepast:

Voer de opdracht show sdwan policy from-vsmart uit

```
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
```

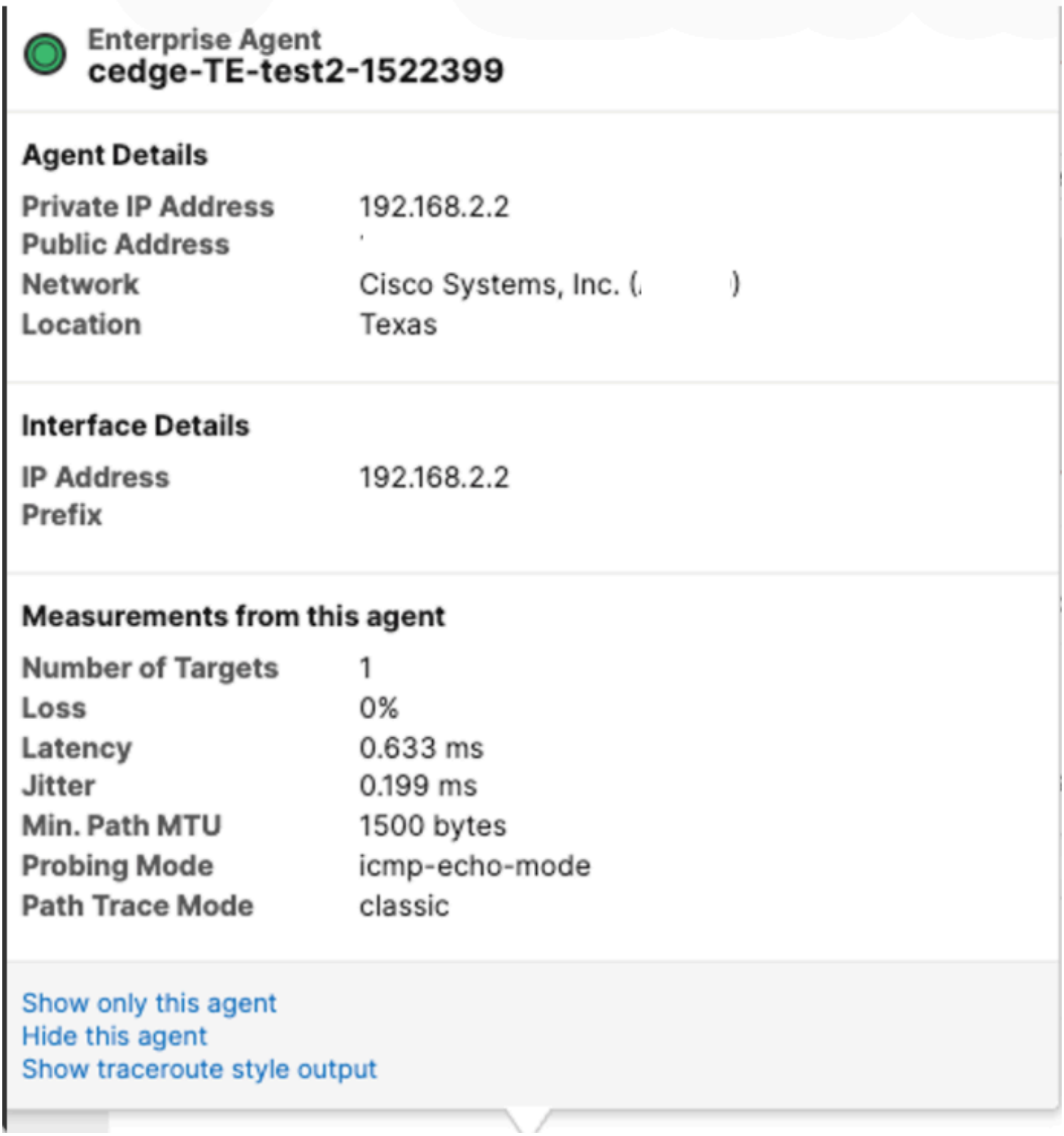
Verifiëren

Als u een test wilt uitvoeren, klikt u op Instat Test en opent u een nieuw venster.

Zodra de test is voltooid, kunt u het pad zien dat nodig was om de 192.168.1.47 te bereiken

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

Waar was gemarkeerd als dscp48 voordat te gaan voor de onderlaag en na gaan over de onderlaag is gemarkeerd als 0.



Een FIA-trace configureren op de Edge Router:

```
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
```

Open een pakket:

<#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
```

Gerelateerde informatie

- Duizend ogen configureren op SD-WAN-apparaten
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.