Konfigurieren der Serviceseite von ThousandEyes Agent zu Server SD-WAN mit DSCP-Markierung

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von ThousandEyes Agent-to-Server SD-WAN mit DSCP-Markierung für die Datenverkehrsüberwachung in einem Cisco SD-WAN-Overlay beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen.

- SD-WAN - Allgemeiner Überblick
- Vorlagen
- Tausend Augen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen.

- Cisco Manager Version 20.15.3

- Cisco Validator-Version 20.15.3
- Cisco Controller Version 20.15.3
- Integrated Service Router (ISR)4331/K9 Version 17.12.3a
- tausandeyes-enterprise-agent-5.5.1.cisco

Vorkonfigurationen

- DNS konfigurieren: Der Router kann DNS auflösen und über VPN 0 auf das Internet zugreifen.
- NAT-DIA konfigurieren: Die DIA-Konfiguration muss auf dem Router vorhanden sein.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Agent zu Servertest

Um einen Agent-zu-Server-Test durchzuführen, muss der ThousandEyes-Agent im Service-VPN konfiguriert sein. In diesem Szenario ist der Server die überwachte TLOC-IP-Adresse. In der Regel wird ein Agent-zu-Server-Test verwendet, um einen Server zu überwachen. In diesem Fall dient sie jedoch zur Überwachung einer TLOC-Schnittstelle, die sich an einem anderen Standort als dem Host-Standort des Agenten befindet.

Wenn mehrere TLOC-Schnittstellen vorhanden sind, verwenden Sie NAT Direct Internet Access (DIA) und eine Datenrichtlinie, um den Datenverkehr an die gewünschte VPN 0 TLOC-Schnittstelle umzuleiten. Legen Sie die Abgleichkriterien basierend auf dem DSCP-Wert fest, der auf der Agentenseite in ThousandEyes konfiguriert wurde, damit er an das und durch das VPN 0 umgeleitet werden kann. Gleichzeitig führen Sie die Entmarkierung aus, um ein Übersteuern des ISP zu vermeiden. mit eigener DSCP-Markierung.

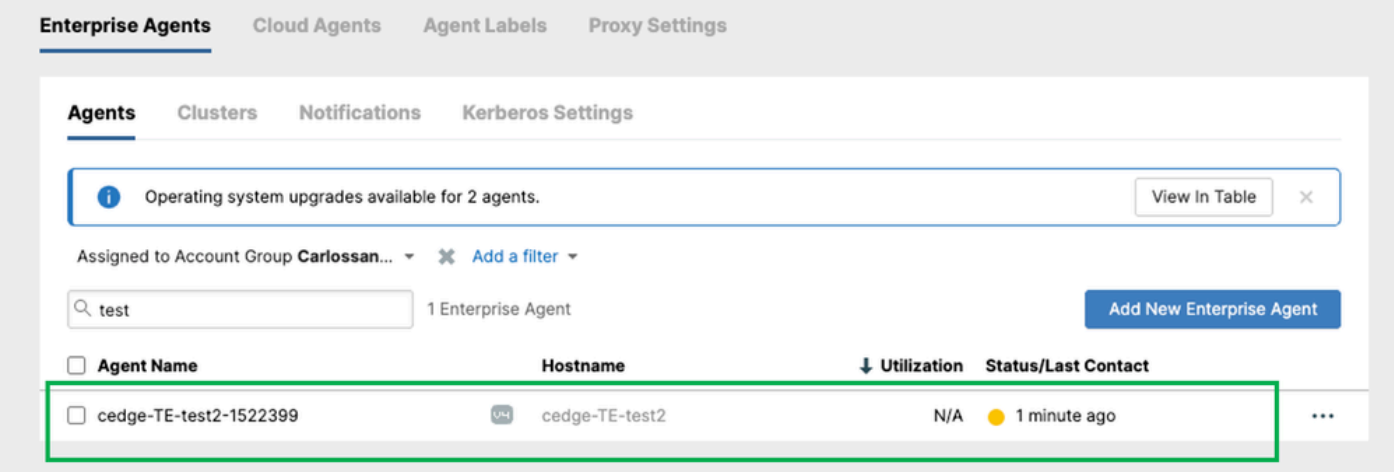
Konfigurieren

ThousandEyes-Test und DSCP konfigurieren

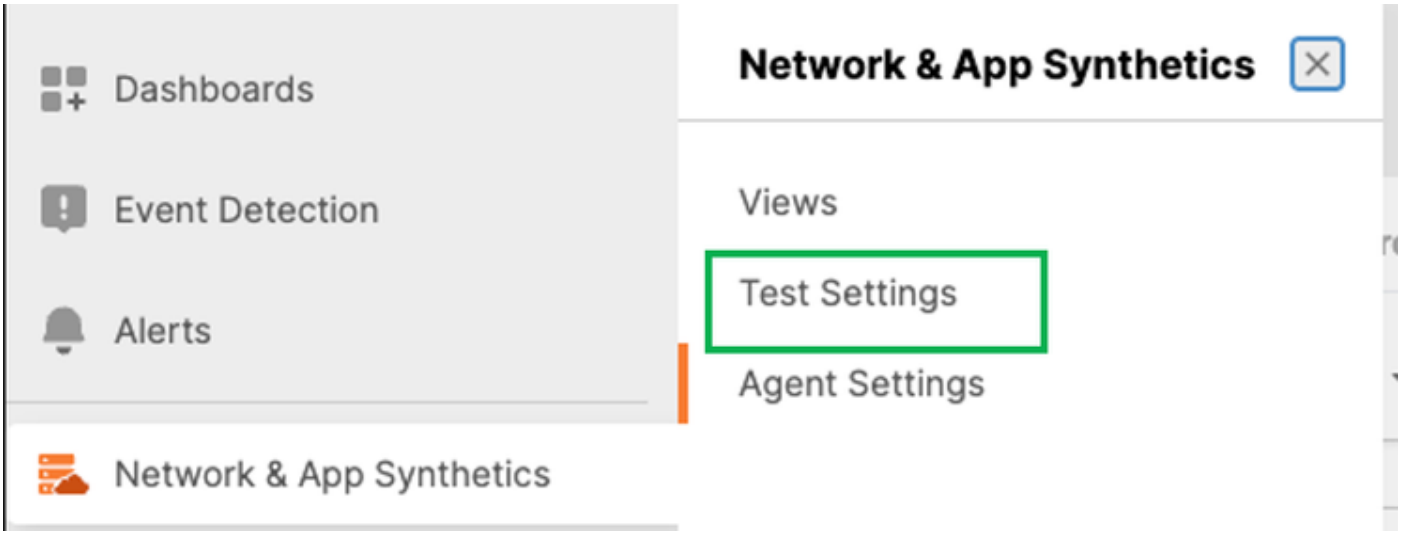
So konfigurieren Sie Differentiated Services Code Point (DSCP):

1. Melden Sie sich über den Cisco ThousandEyes Agent an.

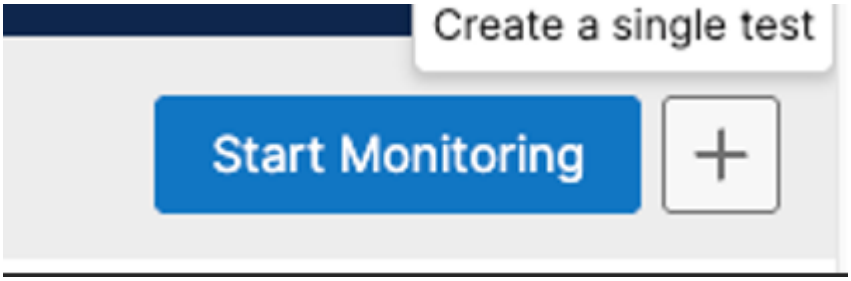
Überprüfen Sie, ob der im Router installierte Agent mit der ThousandEyes Cloud kommuniziert.



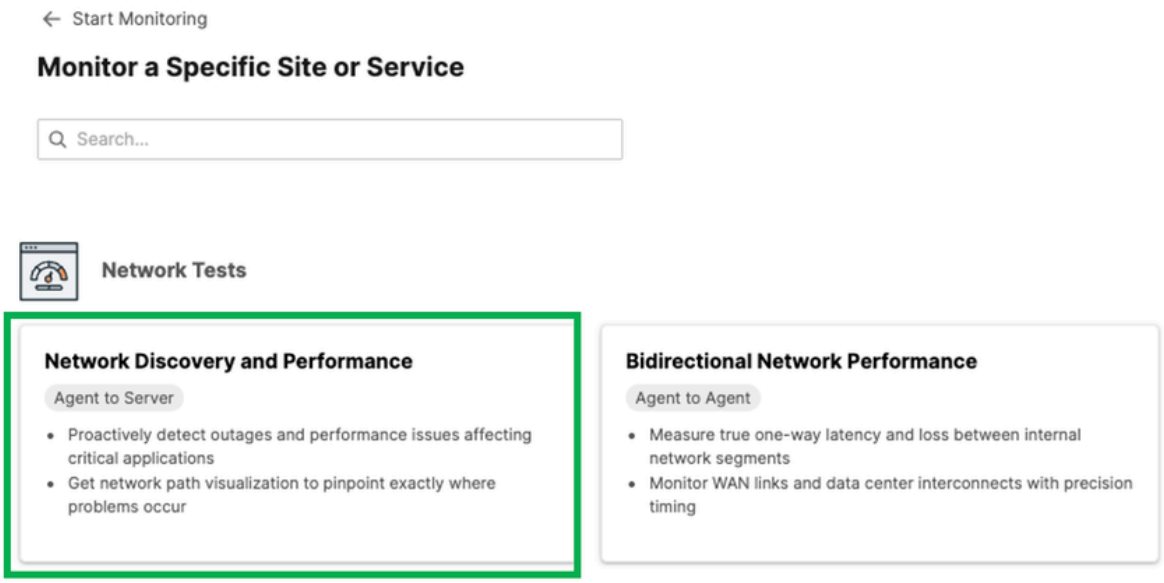
Nachdem der Agent auf dem Gerät installiert und die Kommunikation mit der ThousandEyes Cloud bestätigt wurde, erstellen Sie einen Test. Um einen Test zu erstellen, navigieren Sie zu Network & App Synthetics > Test Settings.



Klicken Sie im rechten oberen Bildschirm auf das +-Symbol.

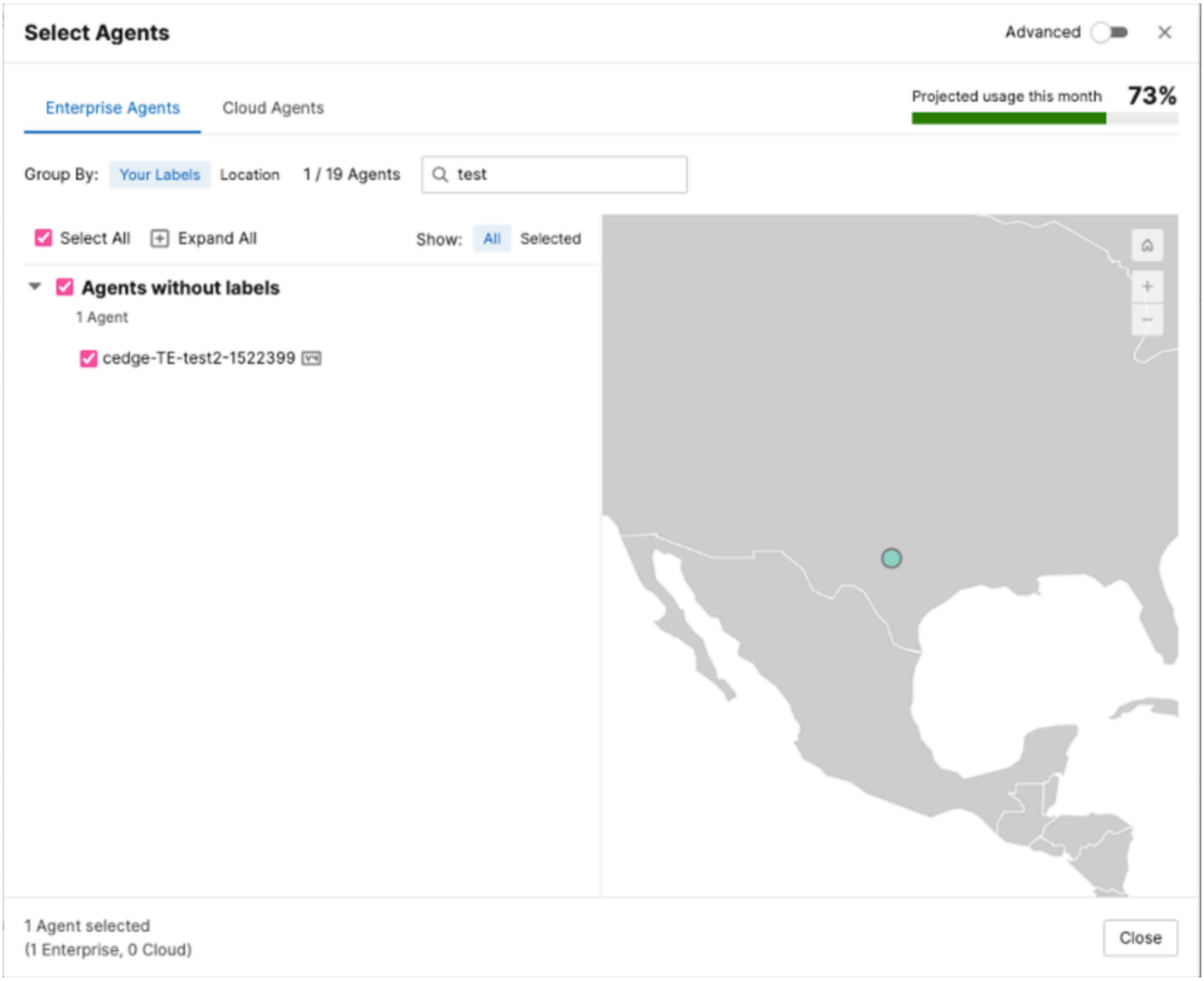


Wählen Sie im neuen Dashboard die Option Agent zu Servertest aus.



Wählen Sie im Abschnitt "Target" (Ziel) die für den Test benötigte IP-Adresse aus. In diesem Beispiel wurde 192.168.1.47 verwendet. Dies ist die IP-Adresse eines anderen TLOC auf einem anderen Router im gleichen Subnetz.

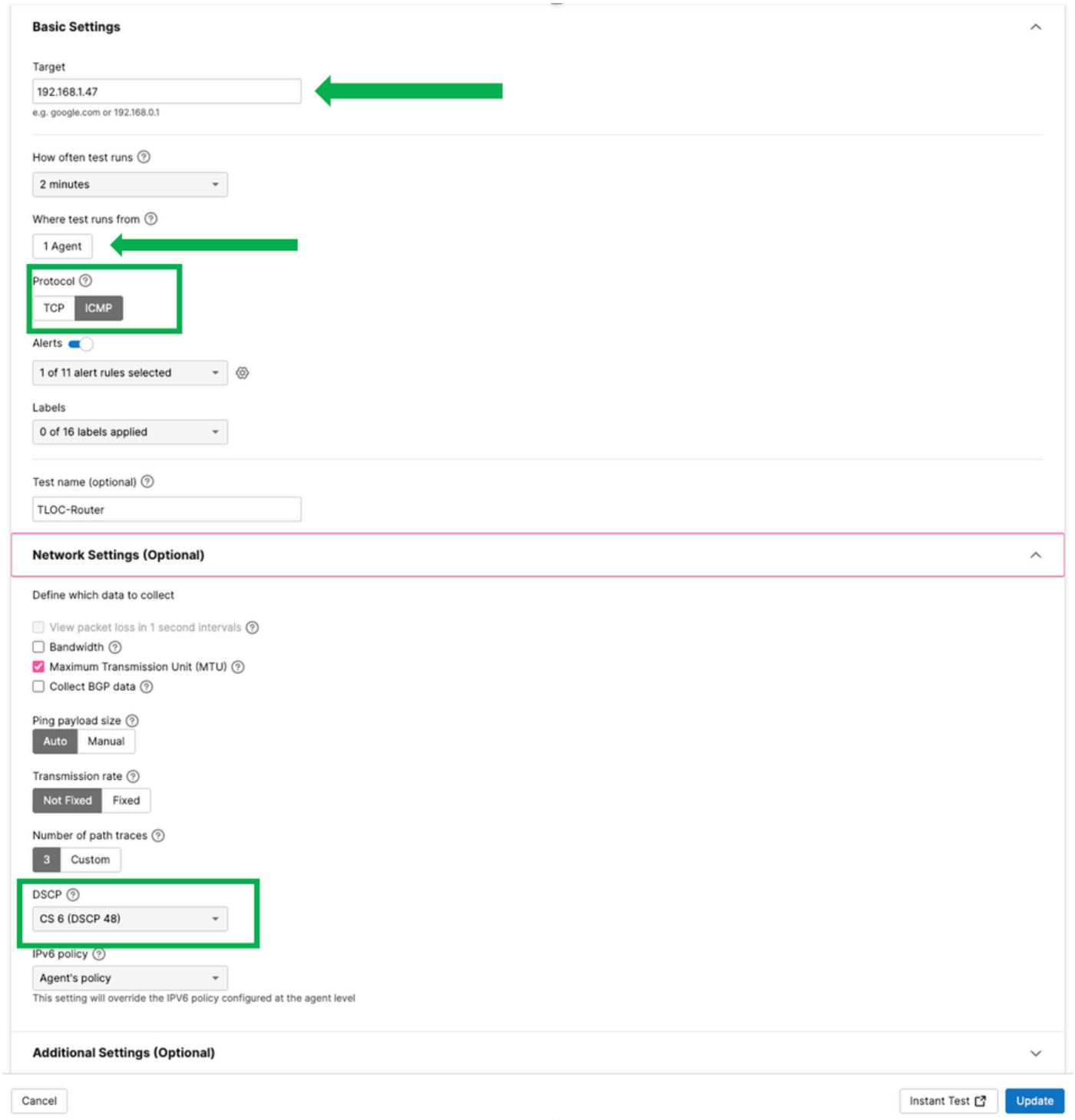
Wählen Sie unter "Where test runs From" (Wo Test läuft von) den Agenten aus, der für Ihren Router erstellt wurde (enthält den Hostnamen Ihres Routers), wie unten gezeigt:



ICMP-Protokoll auswählen

Wählen Sie im Abschnitt "Netzwerkeinstellungen (optional)" den DSCP aus, und klicken Sie auf Aktualisieren.

Klicken Sie im gleichen Abschnitt auf Instant Test (Soforttest).



Konfigurieren des SD-WAN

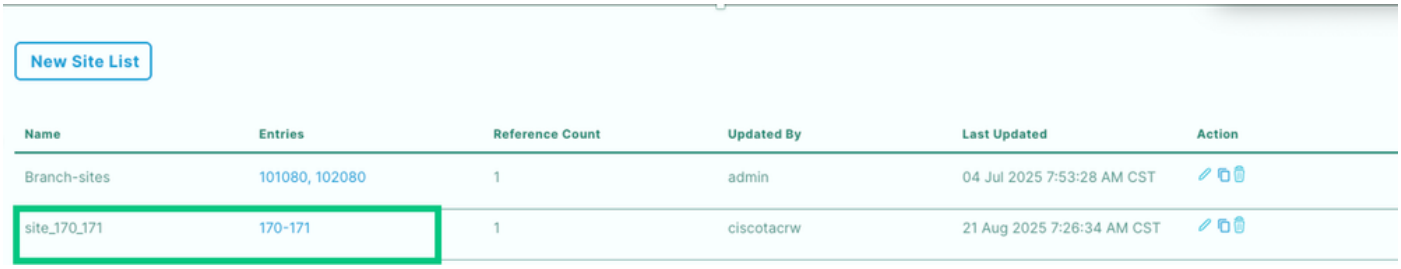
Verwenden Sie das Referenzdokument, um den Thousand Eyes Agent auf dem Edge-Router zu konfigurieren [ThousandEyes auf SD-WAN-Geräten konfigurieren]

Sobald der ThousandEyes Agent auf dem Router installiert ist, zeigt die ThousandEyes-Vorlage die folgenden Informationen an:

Konfigurieren von DSCP

Navigieren Sie zu Konfiguration > Richtlinien > Zentrale Richtlinie > Klicken Sie auf Richtlinie hinzufügen. Fügen Sie bei der Erstellung der Interessengruppe Site, VPN und Datenpräfix hinzu.

Standort (Standort, an dem ThousandEyes Agent installiert wurde)



VPN (Service-VPN)

Das Datenpräfix (einschließlich des auf der ThousandEyes-Vorlage konfigurierten Subnetzes) in diesem Beispiel verwendete das Subnetz 192.168.2.0/24.

Klicken Sie auf Weiter > Weiter, wählen Sie im Abschnitt Traffic Rules konfigurieren die Option Traffic Data aus, und klicken Sie auf Add Policy (Richtlinie hinzufügen).

Wählen Sie DSCP aus, in diesem Beispiel verwendet 48

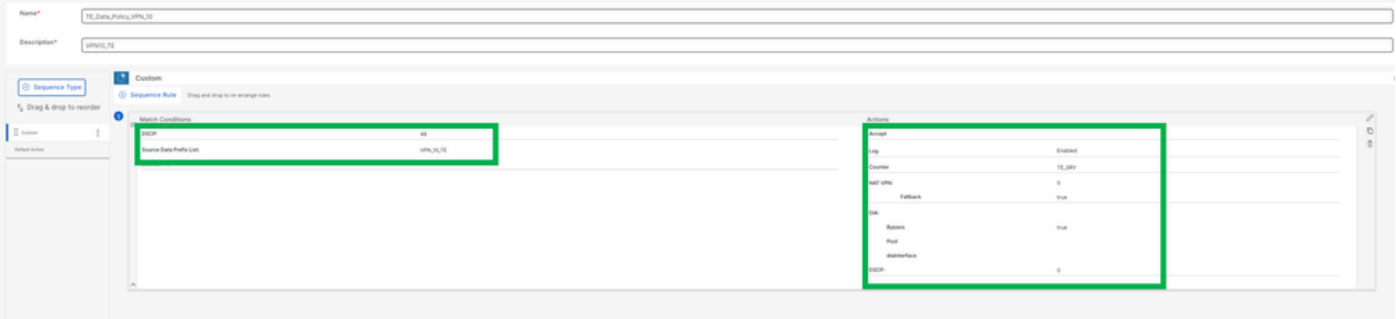
Wählen Sie die Option "Präfixliste für Quelldaten". Verwenden Sie "VPN_10_TE" (wie zuvor dokumentiert), das Netzwerk, das für die ThousandEyes-Konfiguration auf dem Router verwendet wird.

Abschnitt "Aktionen":

NAT VPN auswählen

Fallback

DSCP in diesem Beispiel: Der konfigurierte DSCP ist 0.



Standardaktion aktiviert.

Klicken Sie auf Weiter, und fügen Sie den Richtliniennamen und die Richtlinienbeschreibung hinzu. Klicken Sie im Abschnitt "Verkehrsdaten" auf Neue Standort-/WAN-Regionsliste und VPN-Liste, speichern Sie die Richtlinie, und aktivieren Sie sie.

Nachdem die Richtlinie aktiviert wurde, überprüfen Sie im Router, ob die Richtlinie angewendet wurde:

Führen Sie den Befehl show sdwan policy from-vsmart aus

```
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
```

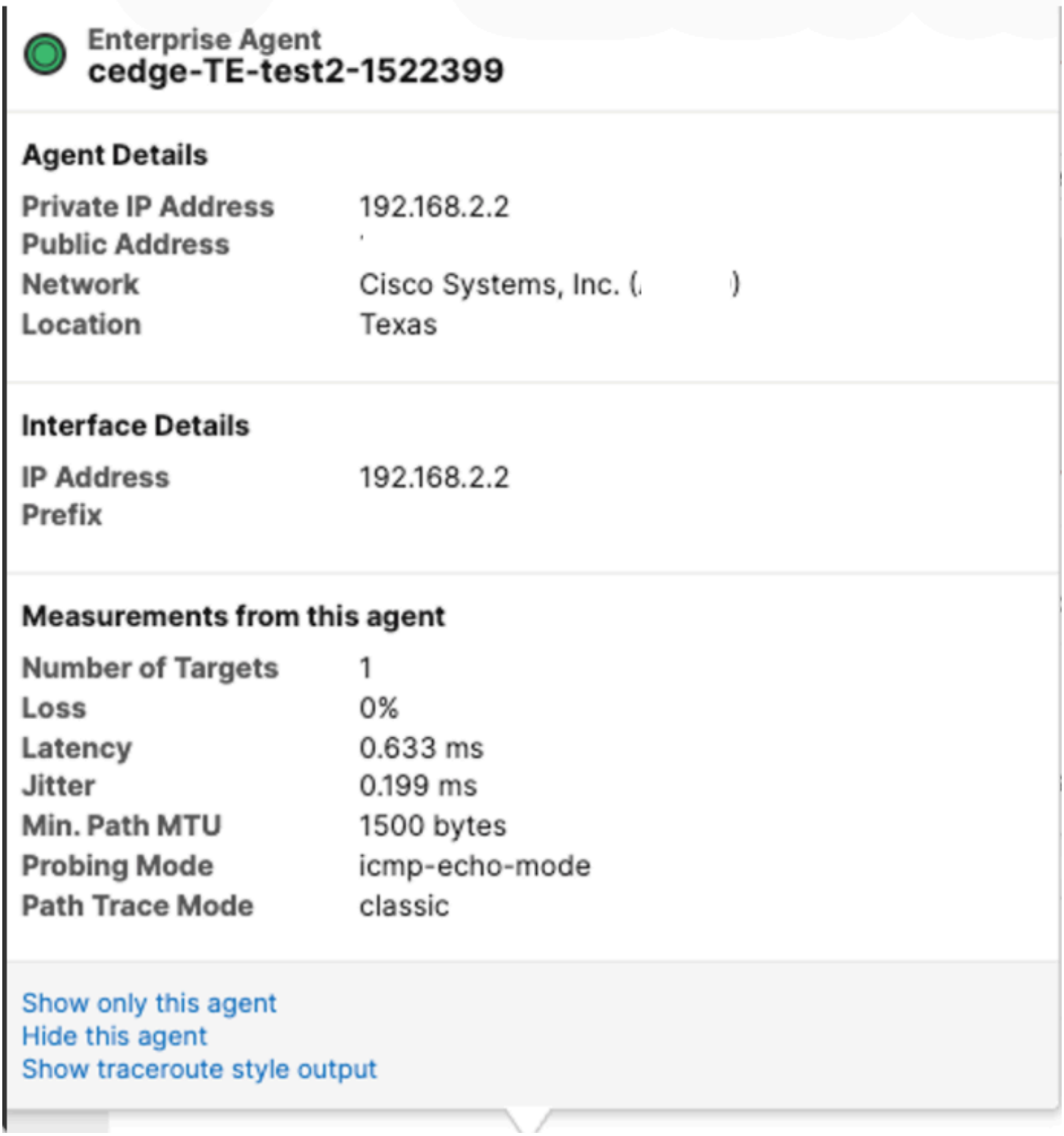
Überprüfung

Um einen Test auszuführen, klicken Sie auf Test starten und öffnen ein neues Fenster.

Nach Abschluss des Tests können Sie den Pfad sehen, über den Sie 192.168.1.47 erreicht haben.

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

Wo wurde als dscp48 vor für die Underlay zu gehen und nach dem Gehen über die Underlay markiert ist als 0.



Konfigurieren Sie eine FIA-Ablaufverfolgung auf dem 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
```

Öffnen Sie ein Paket:

<#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
```

Zugehörige Informationen

- Konfigurieren von "ThousandEyes" auf SD-WAN-Geräten
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.