DSCP 마킹을 사용하여 ThousandEyes 에이전트-서버 SD-WAN 서비스 측 구성

목차

소개

이 문서에서는 Cisco SD-WAN 오버레이에서 트래픽 모니터링을 위해 DSCP 마킹을 사용하는 ThousandEyes 에이전트-서버 SD-WAN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- SD-WAN 일반 개요
- 템플릿
- 사우전드 아이즈

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Manager 버전 20.15.3
- Cisco Validator 버전 20.15.3
- Cisco Controller 버전 20.15.3
- ISR(Integrated Service Router)4331/K9 버전 17.12.3a
- 수천 개의 엔터프라이즈 에이전트 5.5.1.cisco

예비 컨피그레이션

- DNS 구성: 라우터가 DNS를 확인하고 VPN 0에서 인터넷에 액세스할 수 있습니다.
- NAT DIA 구성: DIA 컨피그레이션이 라우터에 있어야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

에이전트-서버 테스트

에이전트-서버 테스트를 실행하려면 서비스 VPN에서 ThousandEyes 에이전트를 구성해야 합니다. 이 시나리오에서 서버는 모니터링되는 TLOC IP 주소입니다. 일반적으로 에이전트-서버 테스트는 서버를 모니터링하는 데 사용됩니다. 그러나 이 경우 에이전트가 호스팅되는 사이트와 다른 사이트에 있는 TLOC 인터페이스를 모니터링하는 데 사용됩니다.

여러 TLOC 인터페이스가 있는 경우 NAT DIA(Direct Internet Access) 및 데이터 정책을 사용하여 원하는 VPN 0 TLOC 인터페이스로 트래픽을 리디렉션합니다. ThousandEyes에서 에이전트 측에 구성된 DSCP 값을 기반으로 일치 기준을 설정하여 VPN 0으로 리디렉션하고 ISP가 자체 DSCP 마킹으로 오버스테핑을 하지 않도록 디마킹을 수행하는 동시에 VPN 0을 통해 리디렉션합니다.

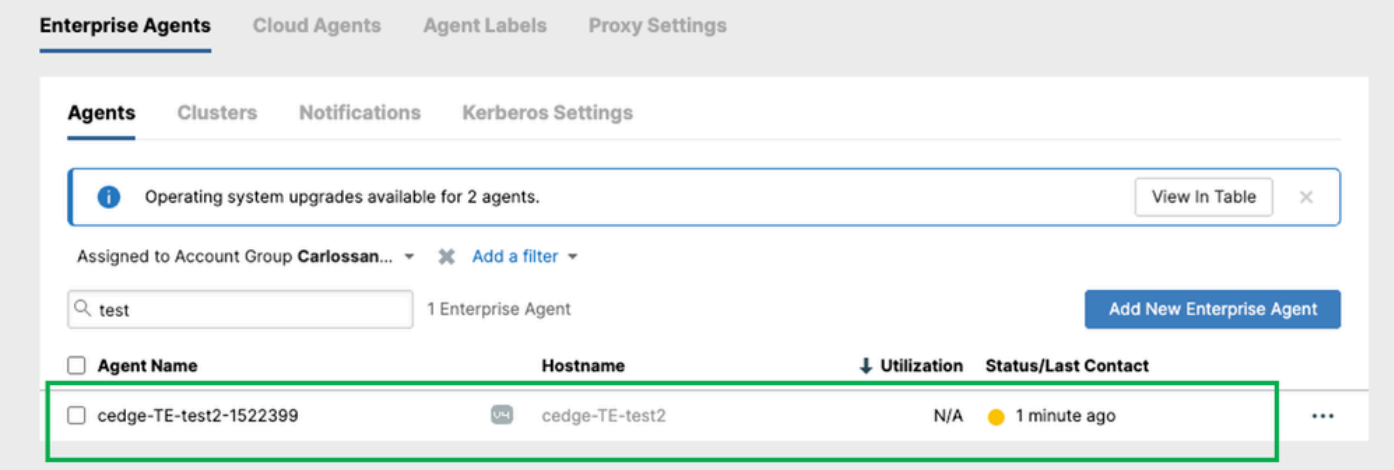
구성

ThousandEyes 테스트 및 DSCP 구성

DSCP(Differentiated Services Code Point)를 구성하려면

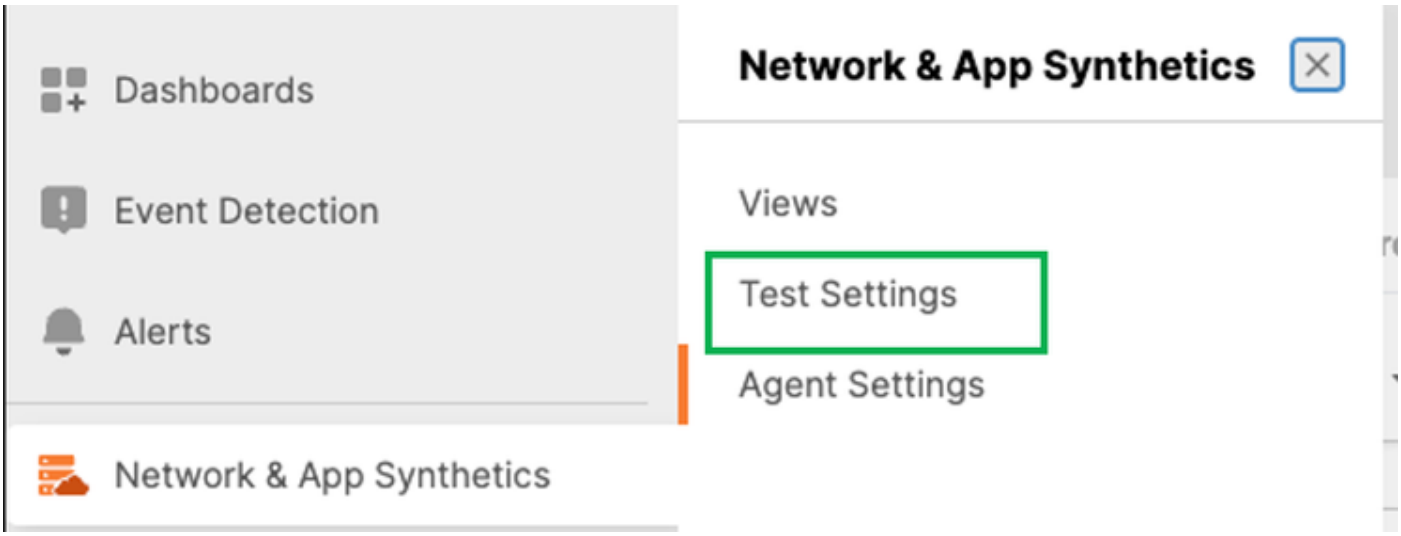
1. Cisco ThousandEyes Agentpage에서 ThousandEyes 계정에 로그인합니다.

라우터에 설치된 에이전트가 ThousandEyes Cloud와 통신하는지 확인합니다.

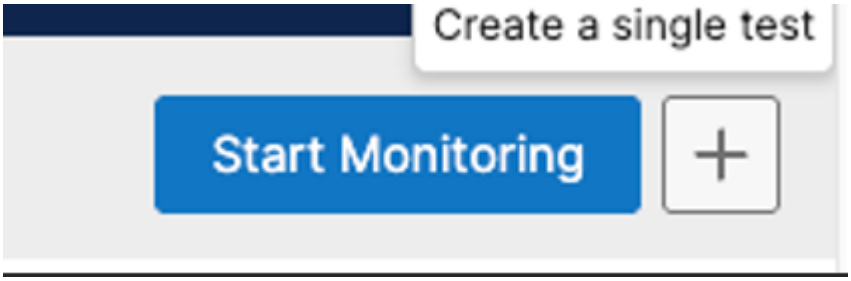


에이전트가 디바이스에 설치되고 ThousandEyes Cloud와의 통신이 확인되면 테스트를 생성합니다. 테스트를 생성하려면 Network & App Synthetics(네트워크 및 앱 합성) > Test Settings(테스트 설

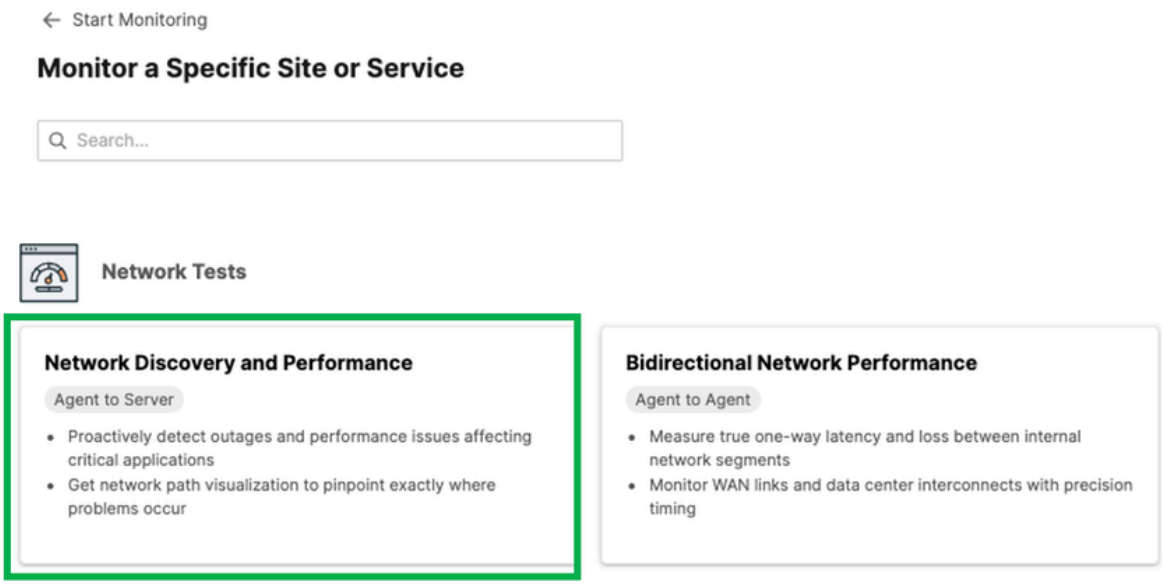
정)로 이동합니다.



오른쪽 상단 화면에서 + 아이콘을 클릭합니다.

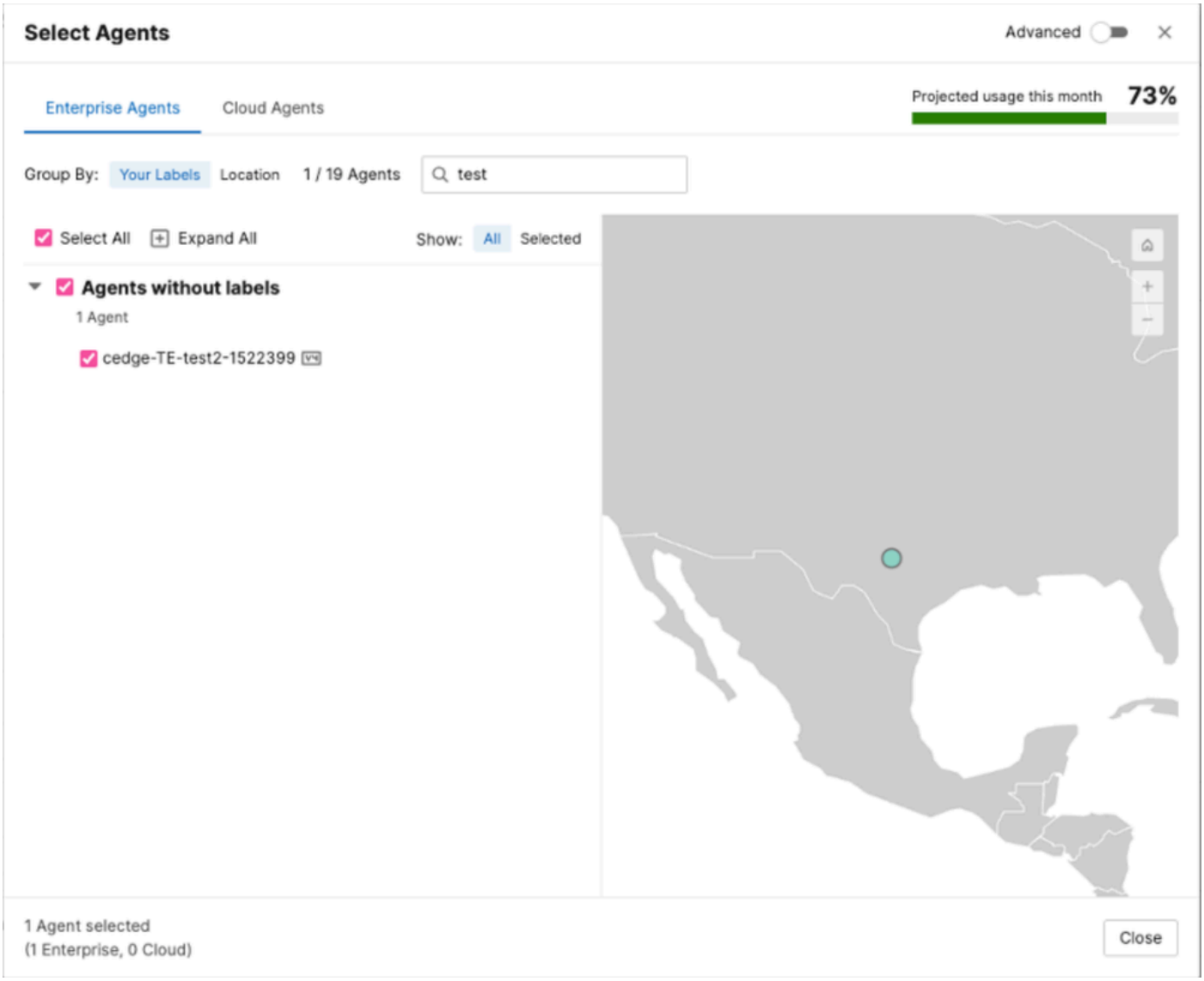


새 대시보드에서 Agent to Server Test를 선택합니다.



"대상" 섹션에서 테스트에 사용할 IP 주소를 선택합니다. 이 예에서는 동일한 서브넷 내의 다른 라우터에 있는 다른 TLOC의 IP 주소인 192.168.1.47을 사용했습니다.

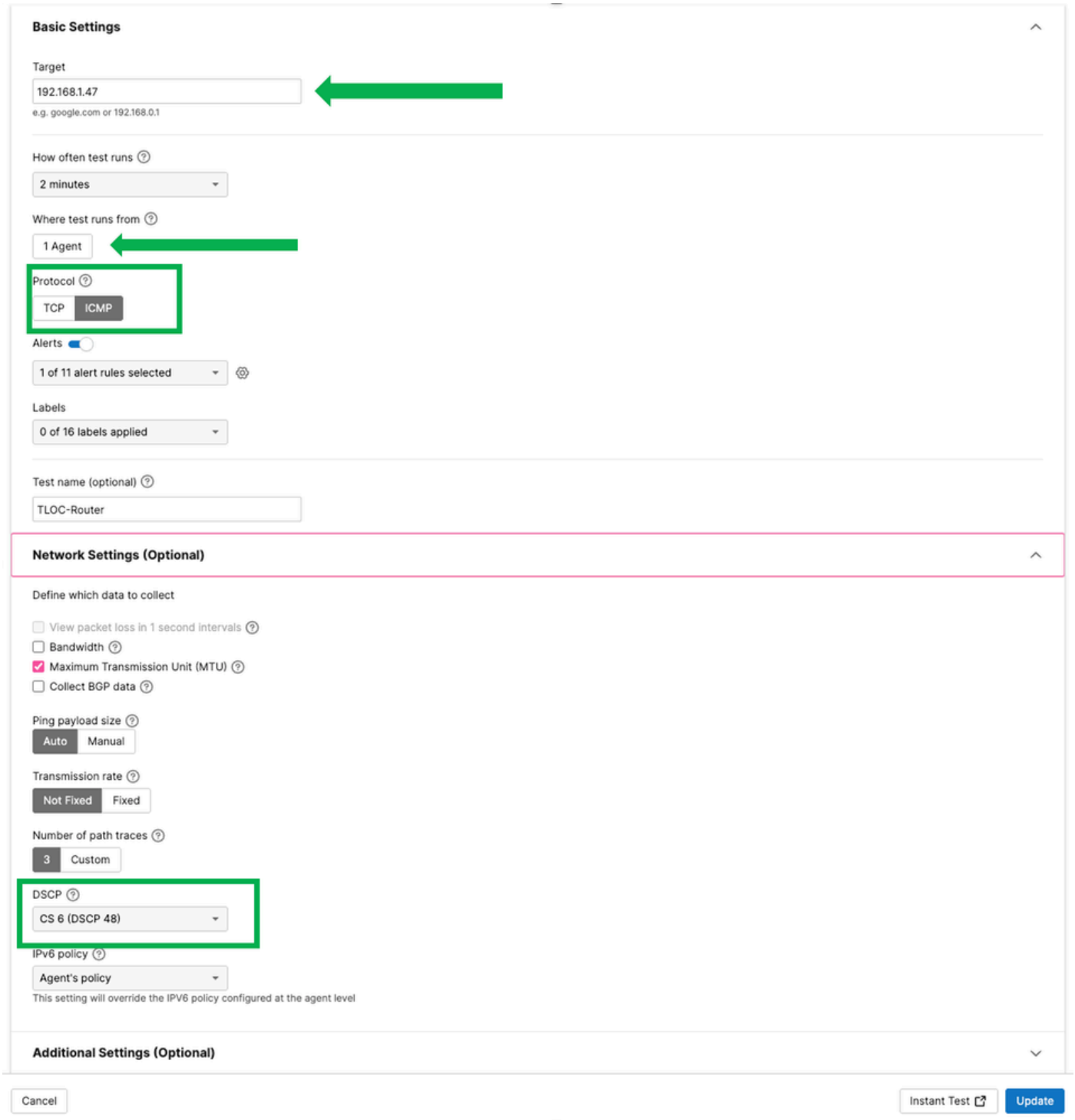
"테스트가 실행되는 위치"에서 아래 표시된 대로 라우터에 대해 생성된 에이전트(라우터의 호스트 이름 포함)를 선택합니다.



ICMP 프로토콜 선택

Network Settings (Optional)(네트워크 설정(선택 사항) 섹션에서 DSCP를 선택하고 Update(업데이트)를 클릭합니다.

같은 섹션에서 Instant Test(인스턴트 테스트)를 클릭합니다.



SD-WAN 구성

참조 문서를 사용하여 Thousand Eyes Agent on Edge Router 구성 [SD-WAN 디바이스에 ThousandEyes 구성]

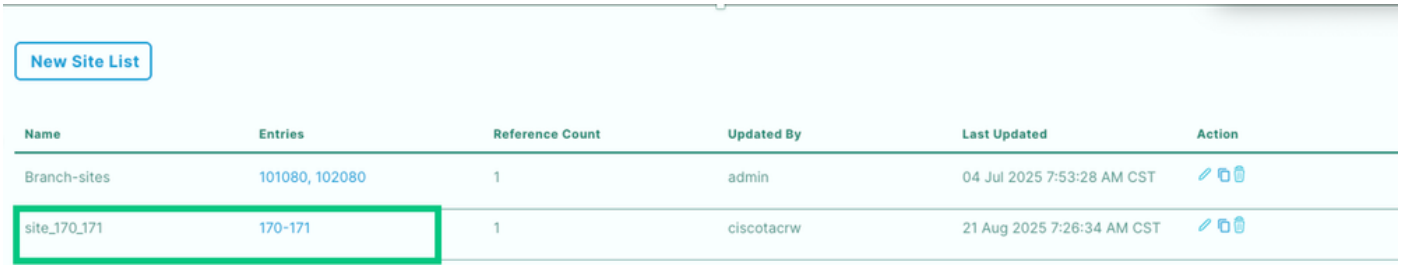
ThousandEyes 에이전트가 라우터에 설치되면 ThousandEyes 템플릿에 다음 정보가 표시됩니다.

DSCP 구성

Configuration(컨피그레이션) > Policies(정책) >Centralized Policy(중앙 집중식 정책) > Add

policy(정책 추가)를 클릭합니다. 관심 그룹 생성에서 사이트, VPN 및 데이터 접두사를 추가합니다.

사이트(ThousandEyes Agent가 설치된 사이트)



VPN(서비스 VPN)

이 예에서 데이터 접두사(ThousandEyes 템플릿에 구성된 서브넷 포함)는 서브넷 192.168.2.0/24을 사용했습니다.

Next(다음) > Next(다음)를 클릭하고 Configure Traffic Rules(트래픽 규칙 구성) 섹션에서 Traffic Data(트래픽 데이터)를 선택한 후 Add Policy(정책 추가)를 클릭합니다.

DSCP를 선택합니다. 이 예에서는 48을 사용했습니다.

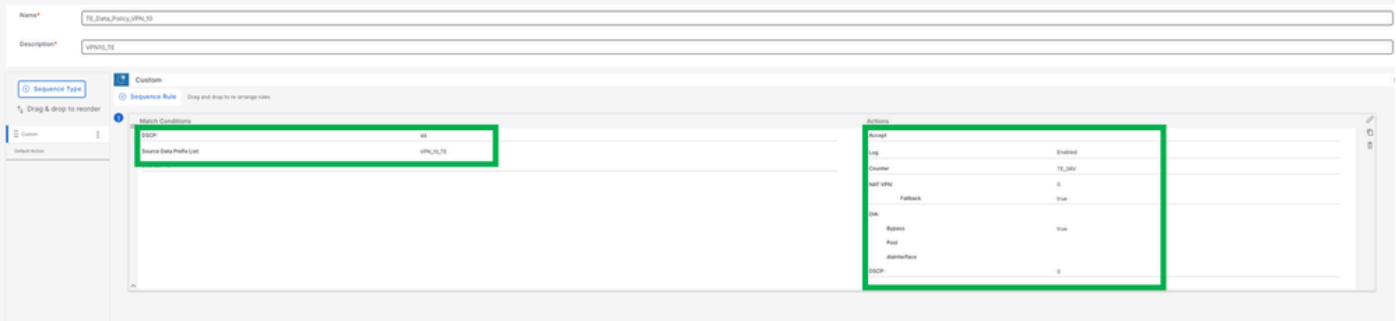
"소스 데이터 접두사 목록" 옵션을 선택합니다. 라우터의 ThousandEyes 컨피그레이션에 사용되는 네트워크인 "VPN_10_TE"(앞에서 설명함)를 사용합니다.

작업 섹션의 경우

NAT VPN 선택

폴백

DSCP 이 예에서는 구성된 DSCP가 0입니다



기본 작업 사용

Next(다음)를 클릭하고 Policy name(정책 이름) 및 Policy Description(정책 설명)을 추가합니다. Traffic Data(트래픽 데이터) 섹션에서 New Site/WAN Region List and VPN List(새 사이트/WAN 영역 목록 및 VPN 목록)를 클릭하고 정책을 저장한 다음 활성화합니다.

정책이 활성화되었으면 라우터에서 정책이 적용되었는지 확인합니다.

show sdwan policy from-vsmart 명령을 실행합니다

```
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
```

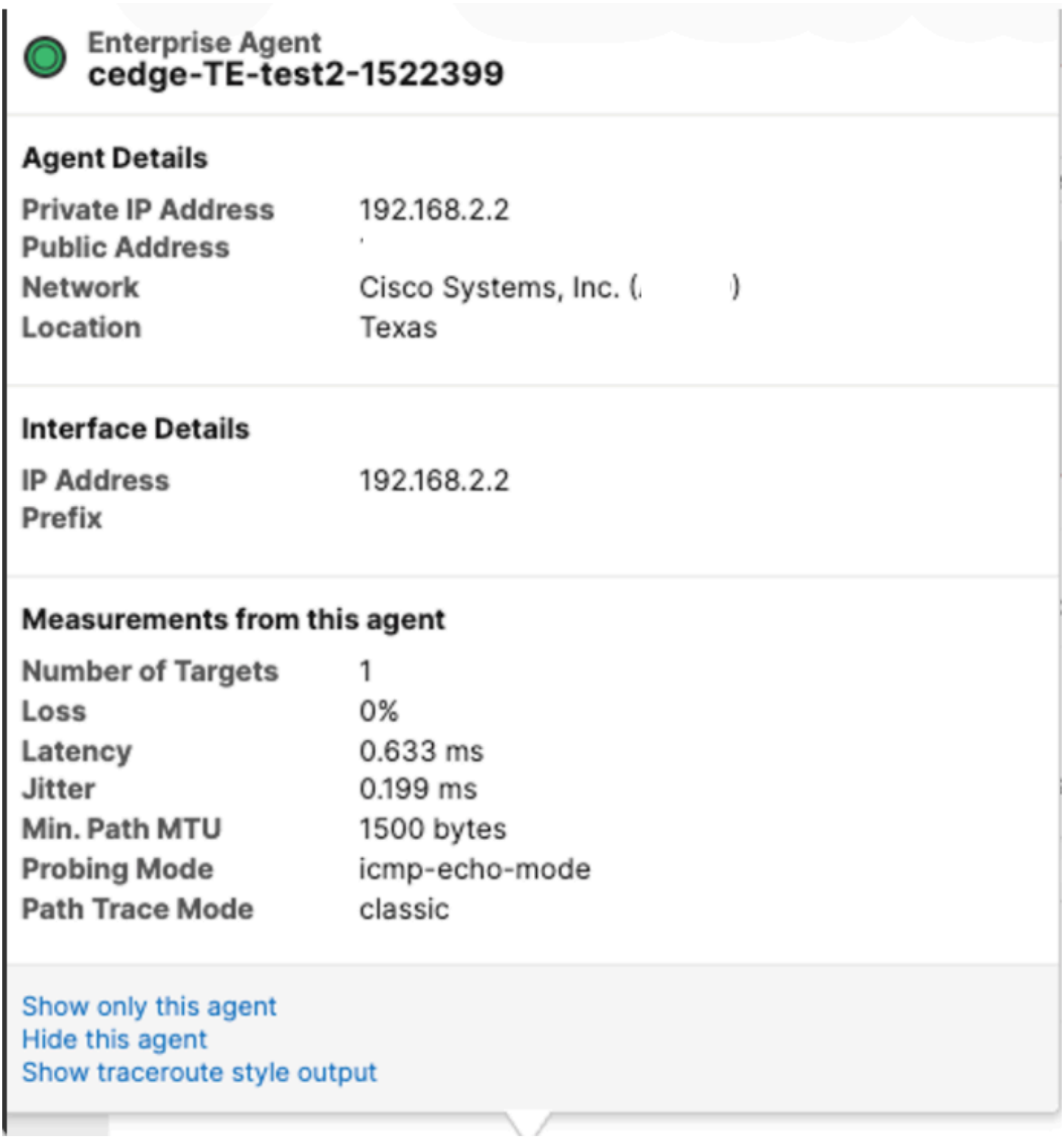
다음을 확인합니다.

테스트를 실행하려면 Instat Test를 클릭하고 새 창을 엽니다.

테스트가 완료되면 192.168.1.47에 도달하는 데 걸린 경로를 확인할 수 있습니다

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

언더레이로 가기 전 dscp48로 표시된 곳과 언더레이로 넘어간 뒤에는 0으로 표시합니다.



에지 라우터에서 FIA 추적을 구성합니다.

```
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
```

패킷 열기:

<#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
```

관련 정보

- SD-WAN 디바이스에 ThousandEyes 구성
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.