cisco Live!

Let's go

#CiscoLive

The bridge to possible

3 Steps to Gain Actionable Visibility in the Cisco SD-WAN Using ThousandEyes

Andraz Piletic, Technical Solutions Architect / Instructor

BRKENT-2126

Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

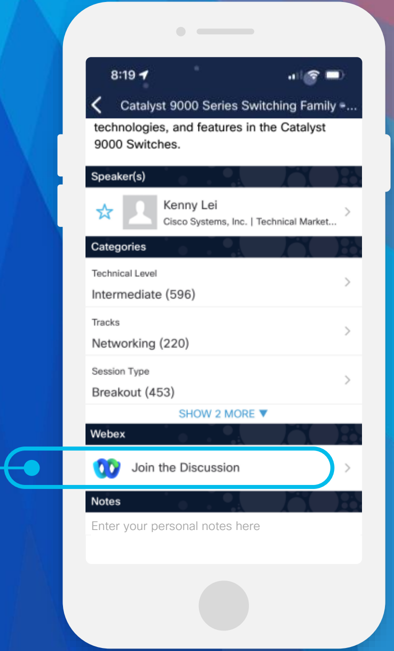
1 Find this session in the Cisco Live Mobile App

2 Click “Join the Discussion”

3 Install the Webex App or go directly to the Webex space

4 Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2126

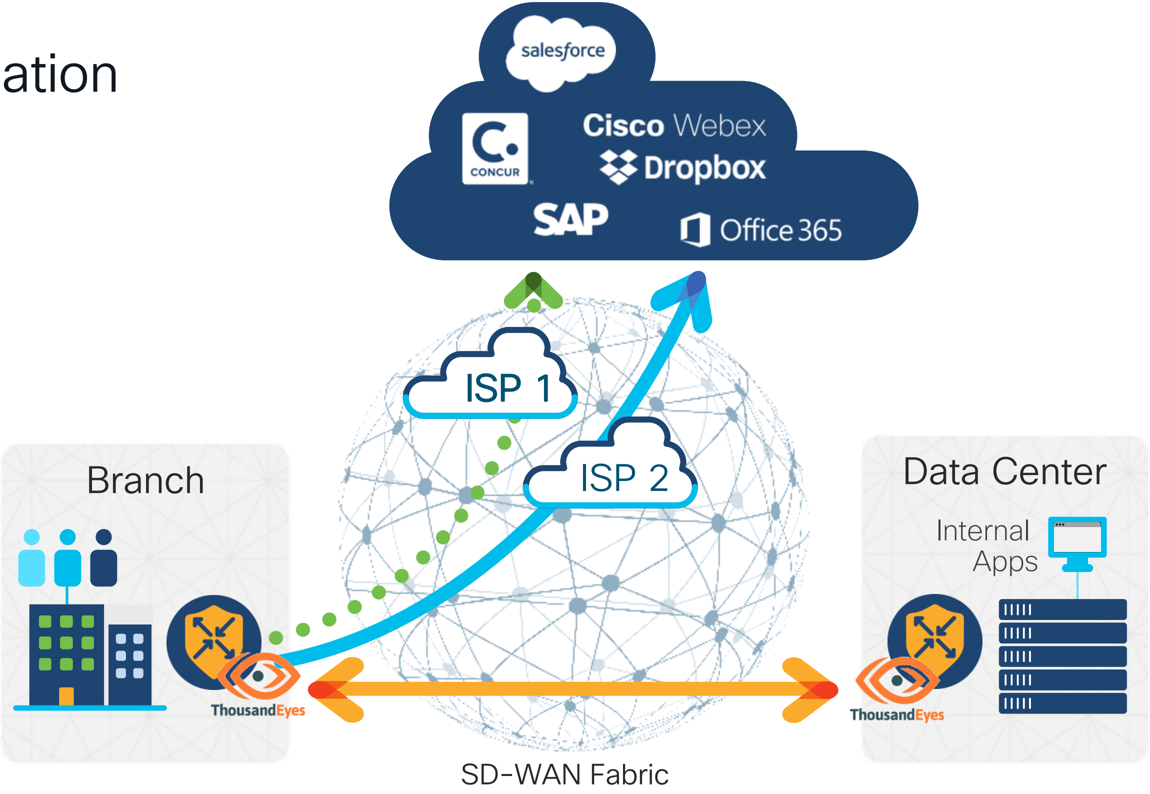
Agenda

- Use Cases
- Agent Deployment Options
- Steering Test Traffic
- Configuring Tests & Viewing Results

SD-WAN + ThousandEyes

Use Cases

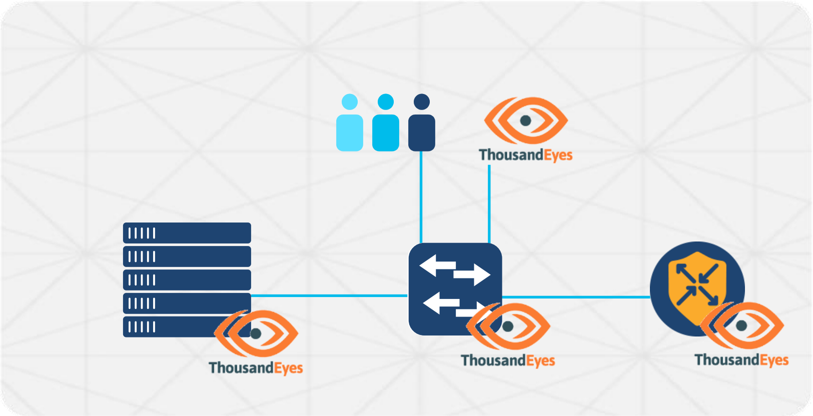
- Internal and SaaS Application
- SD-WAN Underlay
- SD-WAN Overlay



First Step: Deploying Embedded Agents

Different Agent Deployment Options

- Embedded on an SD-WAN Edge
- Embedded in a Catalyst 9000 switch
- Virtual machine
- Physical appliance

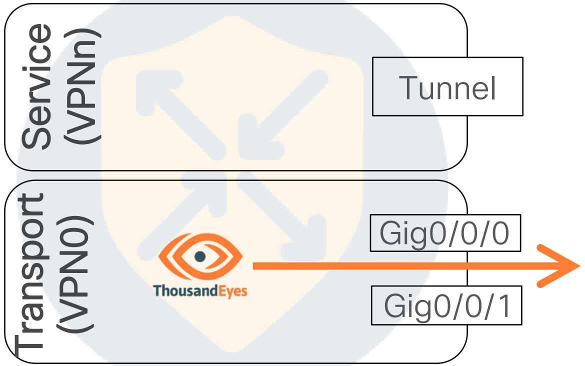


Embedded Agent Requirements

Platform	HW Requirements	SW Requirements	BrowserBot	Management*
ASR 1001-(H)X ASR 1002-(H)X ASR 1006-X	Minimum 8G of RAM and Flash	IOS-XE 17.8.1+	Not supported	vManage 20.8+
Catalyst 8500(L)				
Catalyst 8300 Catalyst 8200(L)	Minimum 8G of RAM and Flash	IOS-XE 17.6.1+		vManage 20.6+
ISR44xx ISR43xx ISR42xx				
ISR 1100x-6G		IOS-XE 17.7.1+		
Catalyst 9300(L) Catalyst 9400	SSD module for BrowserBot tests	IOS-XE 17.6.1+ DNA Advantage	Supported with SSD module	DNA Center 2.2.2.3+

Deployment Options

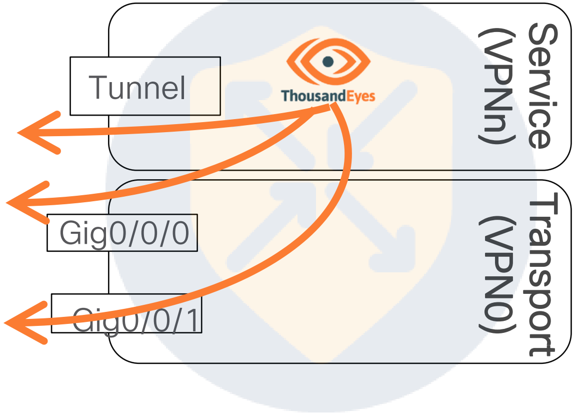
Agent in VPN0



salesforce
Cisco Webex
CONCUR
Dropbox
SAP
Office 365

- Basic setup (default)
- Test traffic routed via a VPG interface
- Still behind a NAT
- Test traffic follows best path

Agent in Service VPN



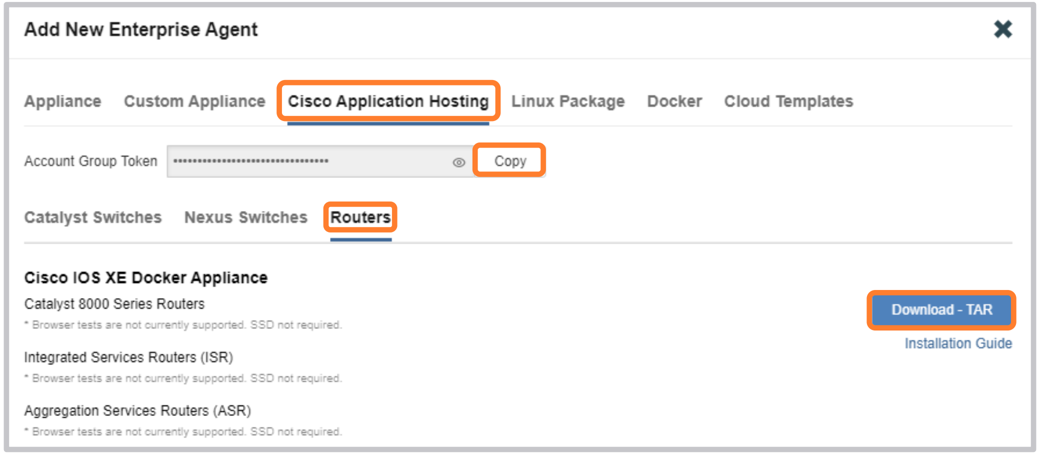
- Test traffic can follow SD-WAN policies
- Can monitor Overlay and Underlay paths
- Requires unique subnet

Deploying ThousandEyes Agent Using vManage

- Download Agent Software from ThousandEyes portal
- Copy Account Group Token
- Upload Agent Software to vManage
- Define ThousandEyes Feature Template in vManage
- Attach Feature Template to target device

Downloading Agent Software

- Cloud & Enterprise Agents > Agent Settings > Add New Ent. Agent
- Cisco Application Hosting > Routers > Download – TAR
- Note down the value of the Account Group Token



Add New Enterprise Agent

Account Group Token •••••••••••••••••••••••••••••••••

Cisco IOS XE Docker Appliance

Catalyst 8000 Series Routers

* Browser tests are not currently supported. SSD not required.

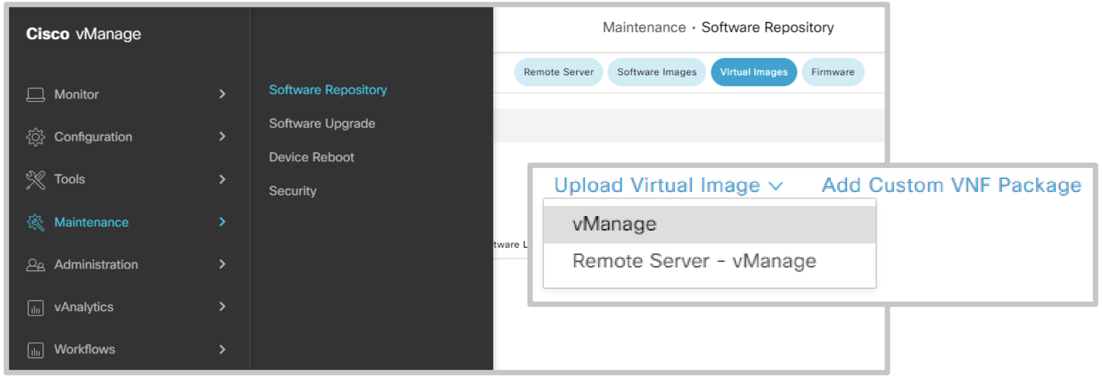
Integrated Services Routers (ISR)

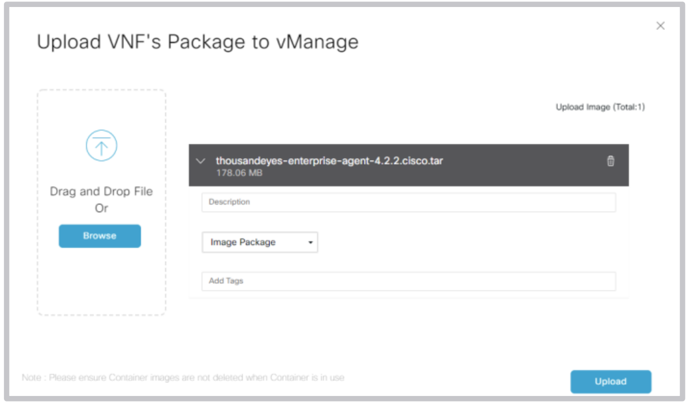
* Browser tests are not currently supported. SSD not required.

Aggregation Services Routers (ASR)

* Browser tests are not currently supported. SSD not required.

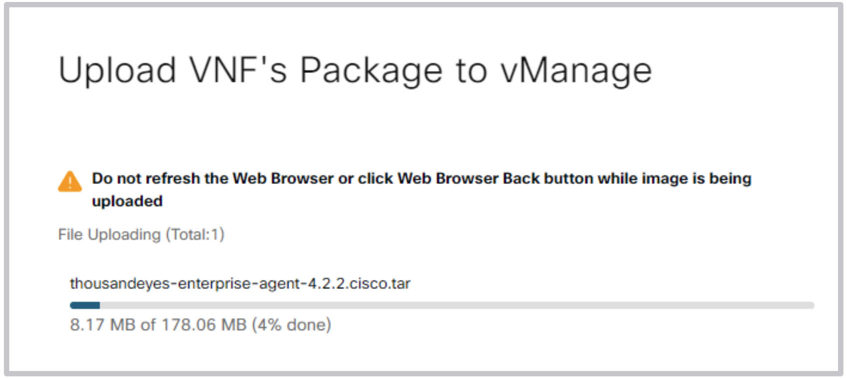
Uploading ThousandEyes Agent to vManage




Upload VNF's Package to vManage

thousandeyes-enterprise-agent-4.2.2.cisco.tar
178.06 MB

Note : Please ensure Container images are not deleted when Container is in use


Upload VNF's Package to vManage

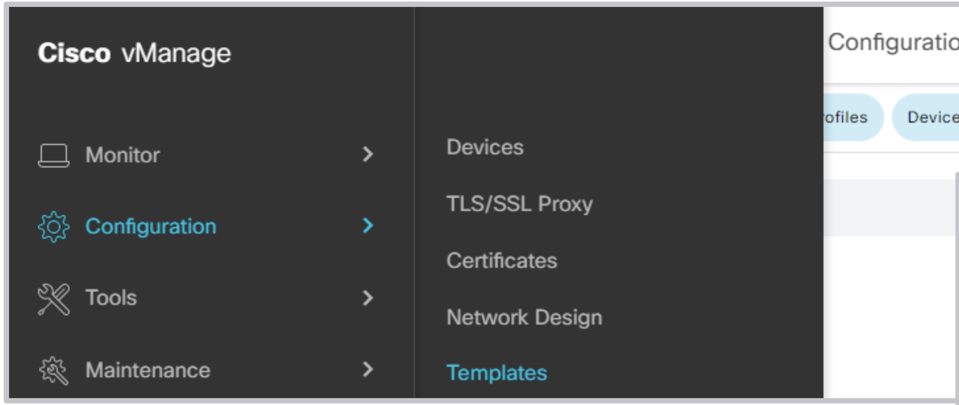
⚠ **Do not refresh the Web Browser or click Web Browser Back button while image is being uploaded**

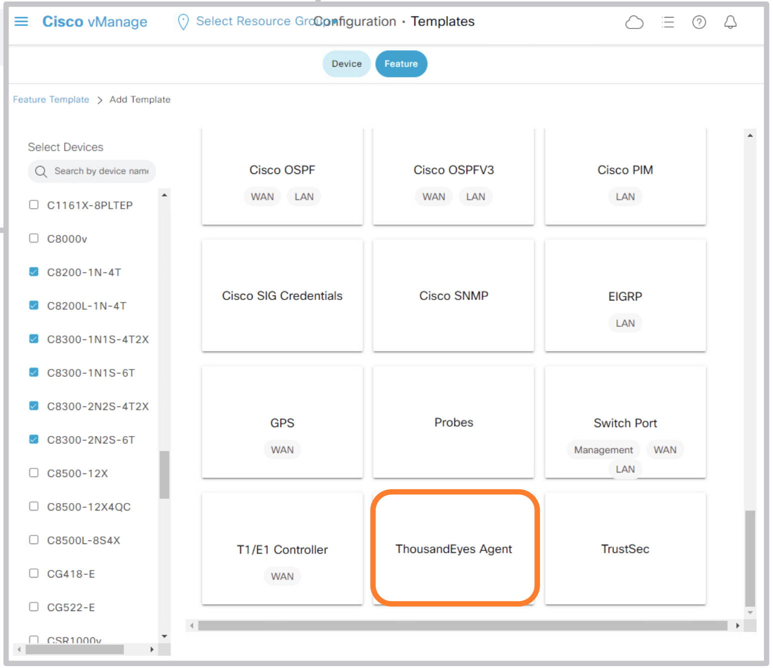
File Uploading (Total:1)

thousandeyes-enterprise-agent-4.2.2.cisco.tar

8.17 MB of 178.06 MB (4% done)

Defining ThousandEyes Feature Template





Feature Template > Add Template

Select Devices

Search by device name

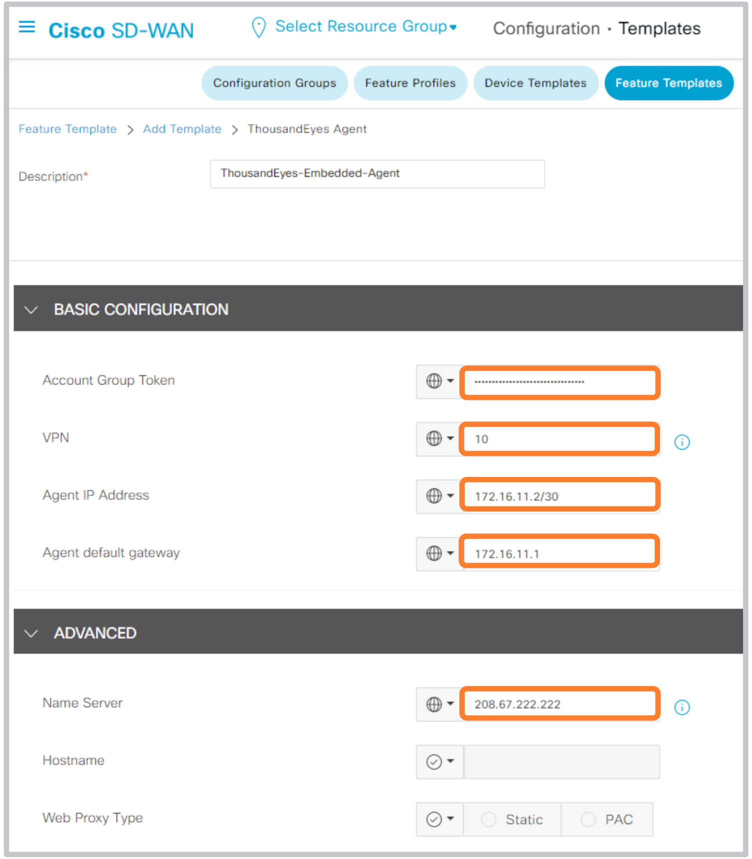
- ☐ C1161X-8PLTEP
- ☐ C8000v
- ☑ C8200-1N-4T
- ☑ C8200L-1N-4T
- ☑ C8300-1N1S-4T2X
- ☑ C8300-1N1S-6T
- ☑ C8300-2N2S-4T2X
- ☑ C8300-2N2S-6T
- ☐ C8500-12X
- ☐ C8500-12X4QC
- ☐ C8500L-8S4X
- ☐ CG418-E
- ☐ CG522-E
- ☐ CSR1000v

- Select supported devices and define ThousandEyes Agent template
- If you don’t see the template, you have selected an unsupported device

Configuring a Feature Template

- Set Account Group Token (global)
- Specify VPN
- Set device specific variable for Agent IP Address and default gateway

- Depending on your environment, you can set the Advanced settings globally, device specific or default



Description* ThousandEyes-Embedded-Agent

BASIC CONFIGURATION

Account Group Token ································

VPN 10

Agent IP Address 172.16.11.2/30

Agent default gateway 172.16.11.1

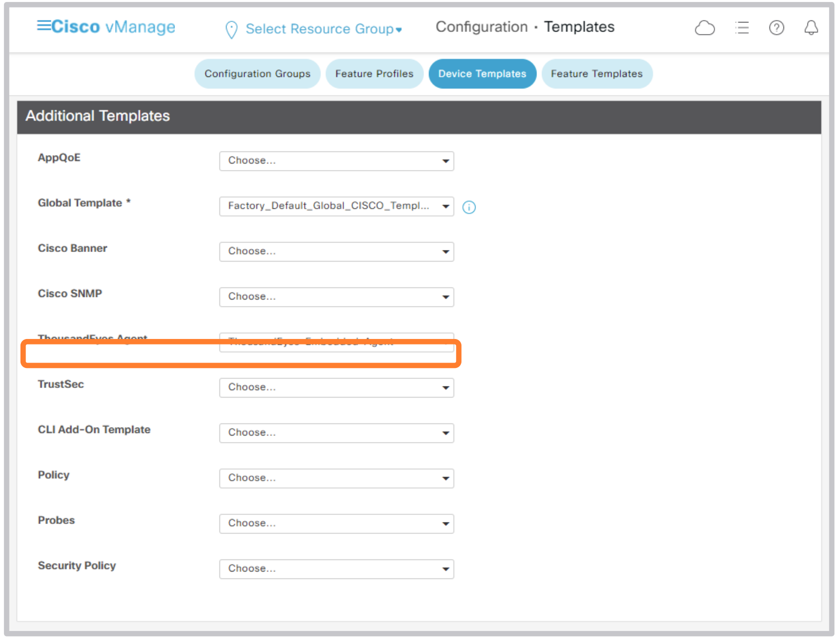
ADVANCED

Name Server 208.67.222.222

Hostname

Web Proxy Type ○ Static ○ PAC

Attaching a Feature Template



Additional Templates

AppQoE	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ...
Cisco Banner	Choose...
Cisco SNMP	Choose...
ThousandEyes Agent	ThousandEyes-Embedded-Agent
TrustSec	Choose...
CLI Add-On Template	Choose...
Policy	Choose...
Probes	Choose...
Security Policy	Choose...

```
interface VirtualPortGroup4
 no shutdown
 vrf forwarding 10
 ip address 172.16.11.1 255.255.255.252
!
iox
app-hosting appid te
 app-default-gateway 172.16.11.1 guest-interface 0
 app-resource docker
  prepend-pkg-opts
  run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=BRKENT2126"
 !
 app-vnic gateway0 virtualportgroup 4 guest-interface 0
  guest-ipaddress 172.16.11.2 netmask 255.255.255.252
 !
 name-server0 208.67.222.222
 start
```

Troubleshooting

```
cEdge# show app-hosting list
App id                                   State
---------------------------------------------------------
te                                       RUNNING
cEdge# app-hosting connect appid te session /bin/bash

root@te: more /var/log/agent/te-agent.log
2022-06-09 10:42:59.307 INFO  [20047f00] [te.agent.status] {} ThousandEyes Agent starting up
2022-06-09 10:42:59.309 DEBUG [20047f00] [te.agent.AptPackageInterface] {} Initialized APT package interface
2022-06-09 10:42:59.309 INFO  [20047f00] [te.agent.main] {} Agent version 1.138.0 starting.
2022-06-09 10:42:59.310 DEBUG [20047f00] [te.agent.db] {} Vacuuming database
2022-06-09 10:42:59.311 INFO  [20047f00] [te.agent.db] {} Found version 53, expected version 53
2022-06-09 10:42:59.322 DEBUG [20047f00] [te.agent.DnssecTaskProceessor] {} Agent is not running bind
2022-06-09 10:42:59.323 INFO  [20047f00] [te.agent.main] {} Configured crash report to
https://crashreports.thousandeyes.com/submit
2022-06-09 10:42:59.324 INFO  [20047f00] [te.agent.main] {} Found id 504516
2022-06-09 10:42:59.324 INFO  [20047f00] [te.agent.ClusterMasterAdapter] {} Set clustermaster URL to
https://sc1.thousandeyes.com
2022-06-09 10:42:59.324 INFO  [20047f00] [te.agent.ClusterMasterAdapter] {} Attempting to get controller assignment from
https://sc1.thousandeyes.com
2022-06-09 10:43:01.369 INFO  [20047f00] [te.agent.ClusterMasterAdapter] {} https://sc1.thousandeyes.com told us we should talk
to controller c1.thousandeyes.com
2022-06-09 10:43:01.397 DEBUG [20047f00] [te.agent.NtpClient] {} Sending NTP packet to pool.ntp.org (193.2.78.228)
<-- output omitted -->
```

Installing Agent Behind a SIG

- Agent fails to register due to untrusted certificate

```
cEdge# app-hosting connect appid te session /bin/bash
root@cEdge:/# tail /var/log/agent/te-agent.log
2023-02-02 09:01:19.890 ERROR [d7825f00] [te.agent.status] {} Error calling createAgent: Curl error -
Peer certificate cannot be authenticated with given CA certificates
```

- Manually copy/paste the missing root CA in a PEM format

```
root@cEdge:/# vi /usr/share/ca-certificates/UmbrellaRootCA.pem
-----BEGIN CERTIFICATE-----
<-- output omitted -->
-----END CERTIFICATE-----
```

- Or transfer it directly (unsecure)

```
root@cEdge:/# curl --insecure https://xzy.cloudfront.net/certificates/Cisco_Umbrella_Root_CA.cer -o
/usr/share/ca-certificates/UmbrellaRootCA.pem
```

Installing Agent Behind a SIG (Cont.)

- Append a new certificate name to the configuration file

```
root@cEdge:/# echo ‘UmbrellaRootCA.pem' >> /etc/ca-certificates.conf
```

- Execute *update-ca-certificates* command

```
root@cEdge:/# update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
```

- Remove specific package (embedded agents only)

```
root@cEdge:/# apt remove --purge cisco-core-trsb
```

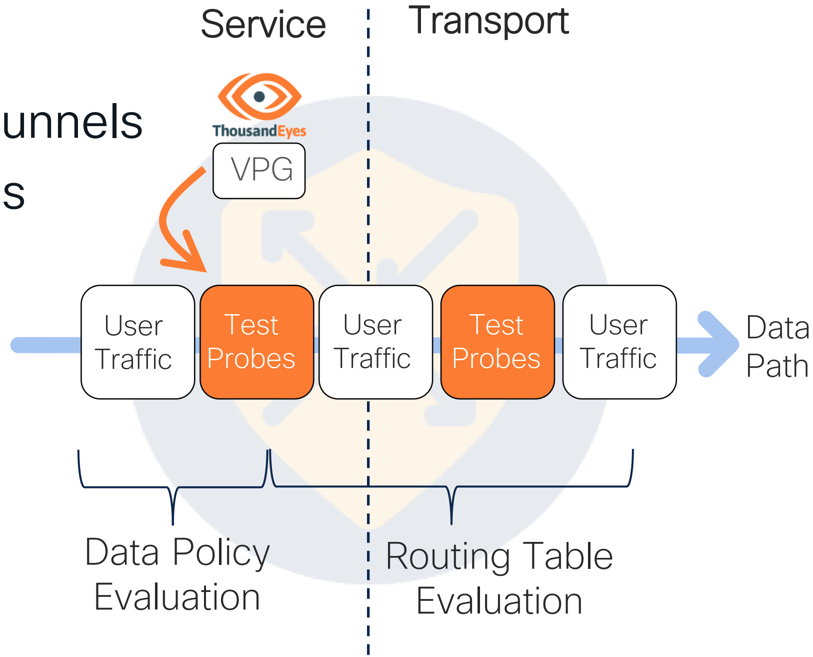
- Restart the agent

```
root@cEdge:/# sv restart te-agent
```

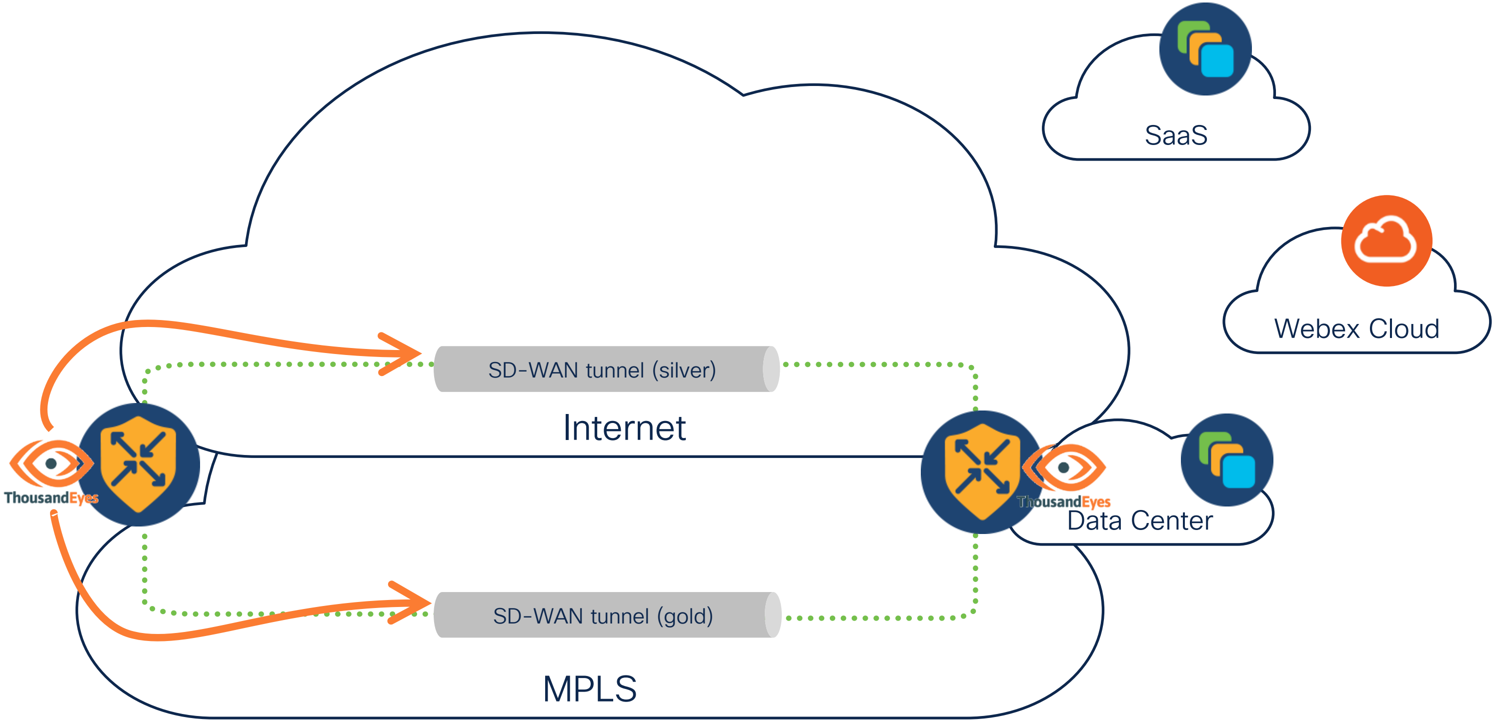
Second Step:
Steering Test Traffic

Common Objectives

- Basic approach: follow preferred/best paths
- Advanced approach:
  - Steer test traffic over redundant overlay tunnels
  - Steer test traffic over redundant DIA paths
- Options for matching test traffic
  - Source IPs
  - Destination IPs & ports
  - DSCP coloring



Steering Test Traffic over Redundant Overlay Paths

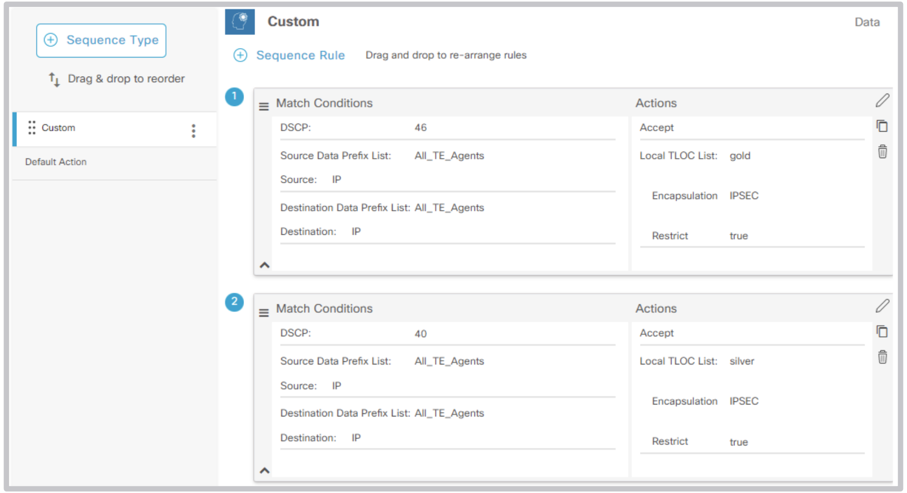


Steering Test Traffic over Redundant Overlay Paths

```
data-policy Overlay-A2A
 vpn-list VPN10
  sequence 1
   match
    dscp 46
    source-data-prefix-list All_TE_Agents
    destination-data-prefix-list All_TE_Agents
   !
   action accept
    set
     local-tloc-list
      color gold
      encap ipsec
      restrict
     !
   !
  !
  sequence 11
   match
    dscp 40
    source-data-prefix-list All_TE_Agents
    destination-data-prefix-list All_TE_Agents
   !
   action accept
    set
     local-tloc-list
      color silver
      encap ipsec
      restrict
     !

default-action accept
```

```
 lists
  data-prefix-list All_TE_Agents
   ip-prefix 192.168.255.0/24
  !
  site-list all-sites
   site-id 1-1000
  vpn-list VPN10
   vpn 10
!
apply-policy
 site-list all-sites
  data-policy Overlay-A2A from-service
```



1 Match Conditions | Actions

DSCP: 46

Source Data Prefix List: All_TE_Agents

Source: IP

Destination Data Prefix List: All_TE_Agents

Destination: IP

Accept

Local TLOC List: gold

Encapsulation IPSEC

Restrict true

2 Match Conditions | Actions

DSCP: 40

Source Data Prefix List: All_TE_Agents

Source: IP

Destination Data Prefix List: All_TE_Agents

Destination: IP

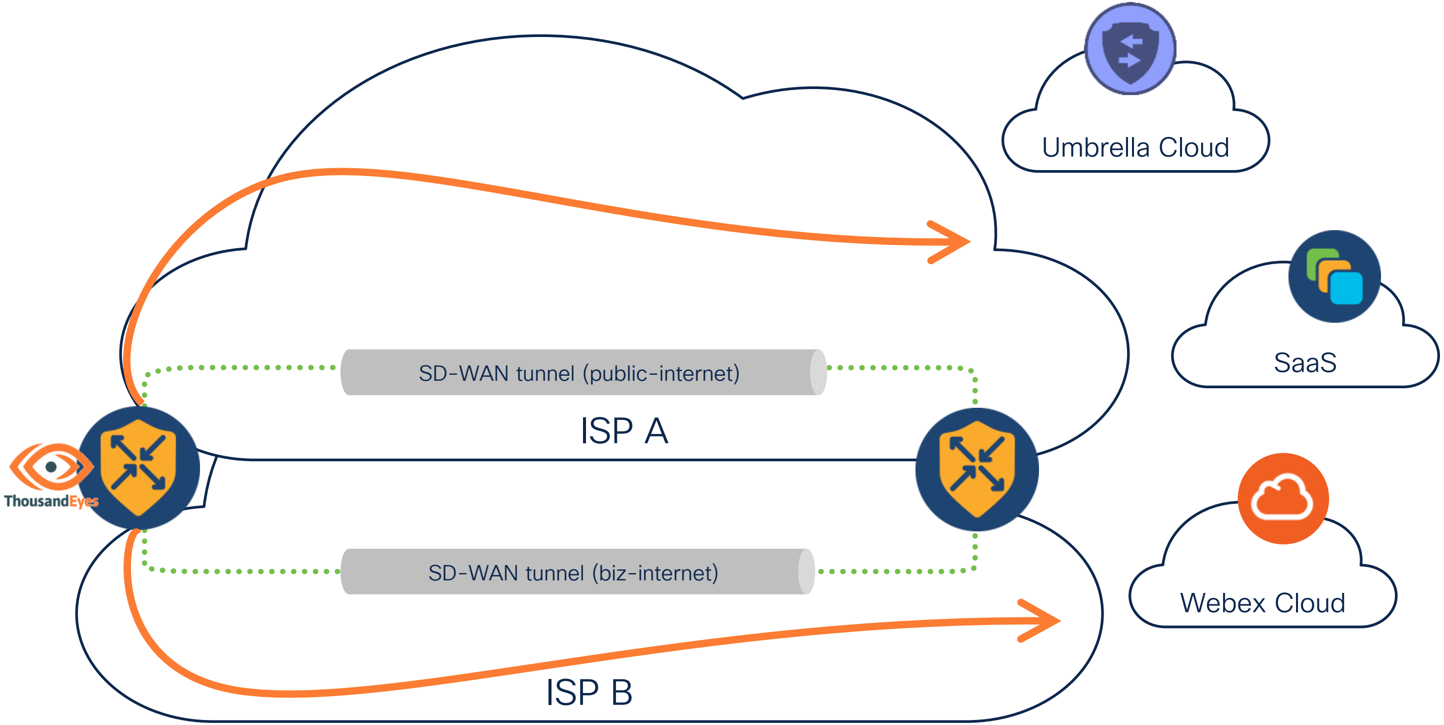
Accept

Local TLOC List: silver

Encapsulation IPSEC

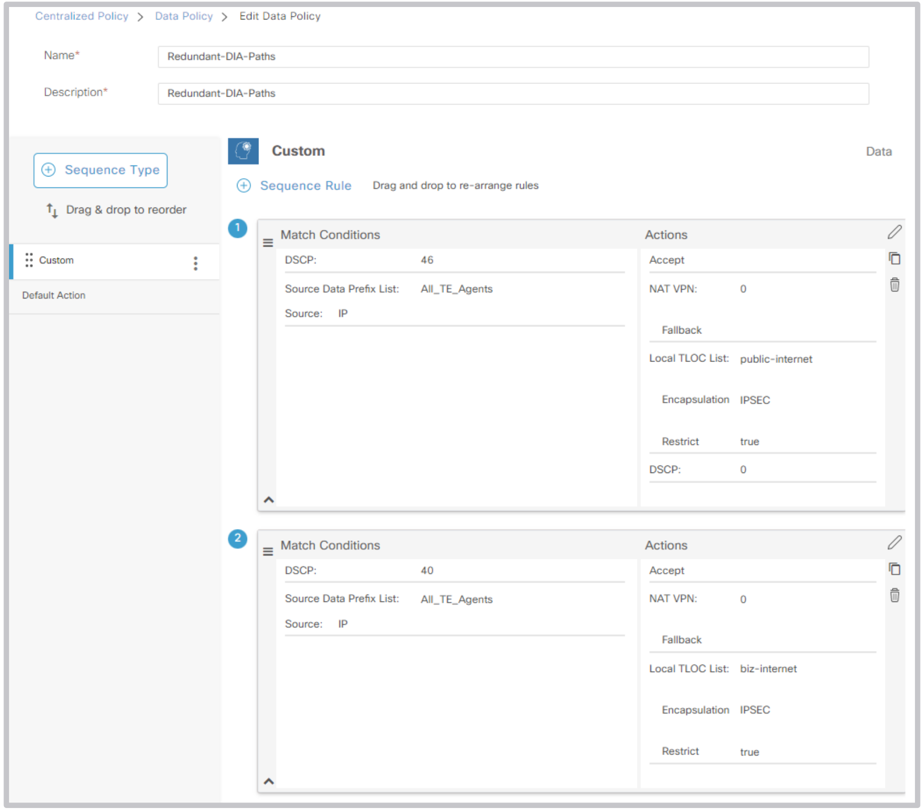
Restrict true

Steering Test Traffic over Redundant DIA Paths



Steering Test Traffic over Redundant DIA Paths

```
data-policy VPN10-Redundant-DIA-Paths
 vpn-list VPN10
   sequence 1
    match
     dscp 46
     source-data-prefix-list All_TE_Agents
    !
    action accept
     nat use-vpn 0
     set
      local-tloc-list
       color public-internet
       encap ipsec
       restrict
      dscp 0
   !
   sequence 11
    match
     dscp 40
     source-data-prefix-list All_TE_Agents
    !
    action accept
     nat use-vpn 0
     set
      local-tloc-list
       color biz-internet
       encap ipsec
       restrict
    !
 default-action accept
```



Centralized Policy > Data Policy > Edit Data Policy

Name*: Redundant-DIA-Paths

Description*: Redundant-DIA-Paths

1

Match Conditions
DSCP: 46
Source Data Prefix List: All_TE_Agents
Source: IP

Actions
Accept
NAT VPN: 0
Fallback
Local TLOC List: public-internet
Encapsulation IPSEC
Restrict true
DSCP: 0

2

Match Conditions
DSCP: 40
Source Data Prefix List: All_TE_Agents
Source: IP

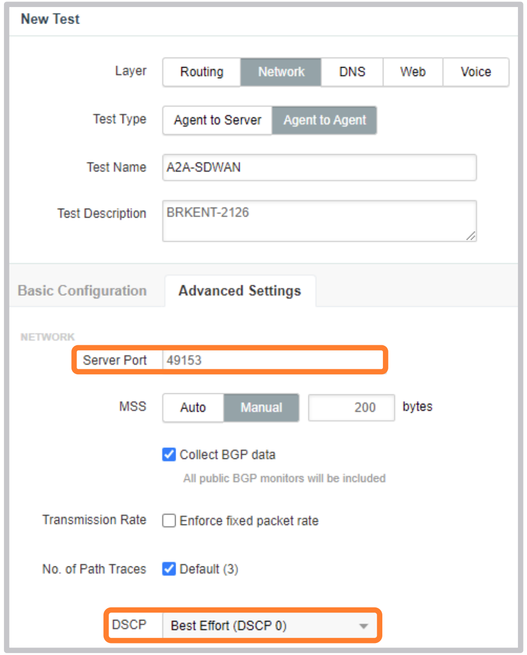
Actions
Accept
NAT VPN: 0
Fallback
Local TLOC List: biz-internet
Encapsulation IPSEC
Restrict true

Last Step: Configuring Tests

Network Test: Agent-to-Agent

- Prefer A2A tests over A2S whenever possible
  - Supports bidirectional testing
  - Detects asymmetrical paths
  - Supports also UDP

- Use different ports or DSCP for matching test traffic with data policy



New Test

Layer: Routing | **Network** | DNS | Web | Voice

Test Type: Agent to Server | **Agent to Agent**

Test Name: A2A-SDWAN

Test Description: BRKENT-2126

Basic Configuration | **Advanced Settings**

NETWORK

Server Port: 49153

MSS: Auto | **Manual** | 200 bytes

☑ Collect BGP data

All public BGP monitors will be included

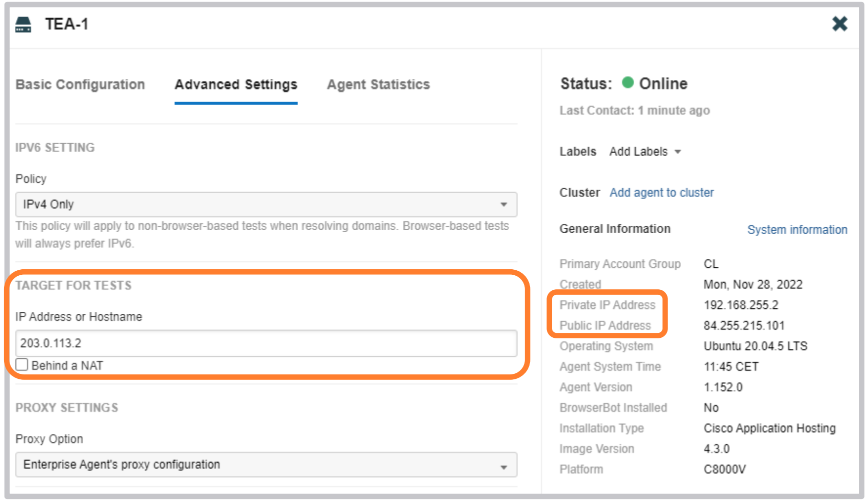
Transmission Rate: □ Enforce fixed packet rate

No. of Path Traces: ☑ Default (3)

DSCP: Best Effort (DSCP 0)

Network Test: A2A Challenges

- Single target IP for tests
  - Difficult to support both overlay & underlay A2A tests concurrently
- Monitoring underlay - reachability of the target agent
  - Place agent directly into the underlay as VA or utilize PAT* (since 20.9)



TEA-1

IPV6 SETTING

Policy: IPv4 Only

This policy will apply to non-browser-based tests when resolving domains. Browser-based tests will always prefer IPv6.

TARGET FOR TESTS

IP Address or Hostname: 203.0.113.2

□ Behind a NAT

PROXY SETTINGS

Proxy Option: Enterprise Agent's proxy configuration

Status: ● Online

Last Contact: 1 minute ago

Labels: Add Labels

Cluster: Add agent to cluster

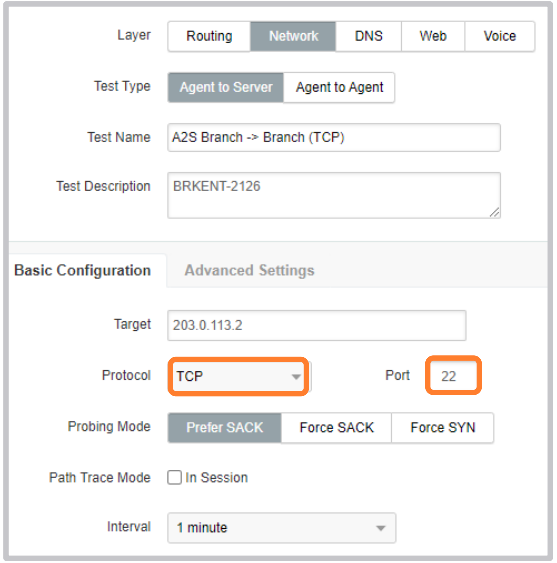
General Information — System information

Primary Account Group	CL
Created	Mon, Nov 28, 2022
Private IP Address	192.168.255.2
Public IP Address	84.255.215.101
Operating System	Ubuntu 20.04.5 LTS
Agent System Time	11:45 CET
Agent Version	1.152.0
BrowserBot Installed	No
Installation Type	Cisco Application Hosting
Image Version	4.3.0
Platform	C8000V

```
ip nat inside source static tcp 192.168.255.2 49153 203.0.113.2 49153 vrf 10 egress-interface GigabitEthernet1
ip nat inside source static udp 192.168.255.2 49153 203.0.113.2 49153 vrf 10 egress-interface GigabitEthernet1
```

Network Test: Agent-to-Server

- Use when no agent available at test destination
- Prefer TCP over ICMP
- SDWAN underlay interfaces are locked down by default
- Utilize DSCP for data policy actions
- With 1 minute interval measurements can be spread in 1 second intervals



Layer: Routing | **Network** | DNS | Web | Voice

Test Type: **Agent to Server** | Agent to Agent

Test Name: A2S Branch -> Branch (TCP)

Test Description: BRKENT-2126

Basic Configuration | Advanced Settings

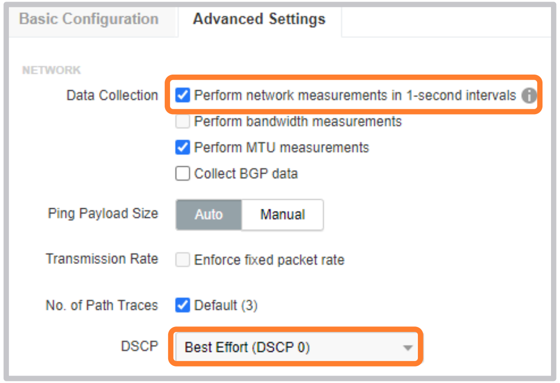
Target: 203.0.113.2

Protocol: TCP Port: 22

Probing Mode: **Prefer SACK** | Force SACK | Force SYN

Path Trace Mode: □ In Session

Interval: 1 minute



Basic Configuration | **Advanced Settings**

NETWORK

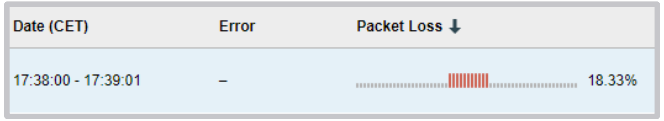
Data Collection:
☑ Perform network measurements in 1-second intervals
□ Perform bandwidth measurements
☑ Perform MTU measurements
□ Collect BGP data

Ping Payload Size: **Auto** | Manual

Transmission Rate: □ Enforce fixed packet rate

No. of Path Traces: ☑ Default (3)

DSCP: Best Effort (DSCP 0)



Date (CET)	Error	Packet Loss ⬇
17:38:00 - 17:39:01	–	18.33%

Web Layer Tests

- Matching different web test traffic with an SD-WAN data policy becomes a challenge:
  - No DSCP coloring options, source ports settings, etc.
  - Only HTTP Server test supports different source interfaces*

- BrowserBot is needed for Page Load and Transaction tests

- Alternative - Multiple agents in a branch

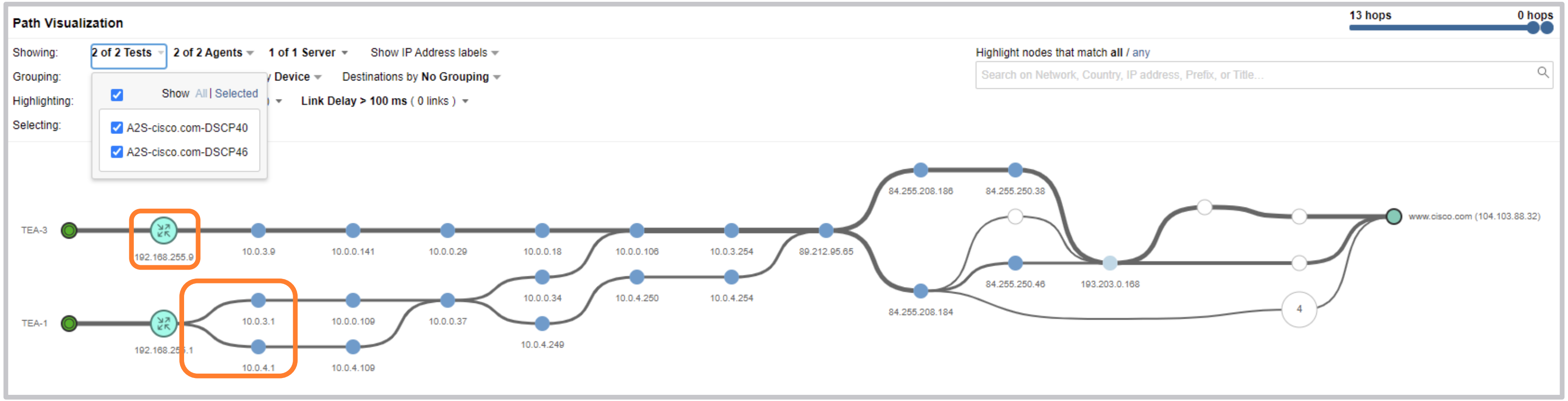
What about SASE?

- Secure Internet Gateways (proxies) break network visibility
  - Utilize web tests for end-to-end application performance and visibility
  - Monitor underlay to IPsec/GRE gateways using A2S network tests

- HTTPs/SSL decryption requires additional installation step on agents
  - Import utilized CA certificate (documentation)

Improving Visualization

- Combine individual tests using multi-views
- Enable SNMP on SD-WAN edges and utilize Device Layer monitoring
  - Make sure data policy does not match such traffic for DIA action



Path Visualization

13 hops — 0 hops

Showing: 2 of 2 Tests ▾ 2 of 2 Agents ▾ 1 of 1 Server ▾ Show IP Address labels ▾

Grouping: y Device ▾ Destinations by No Grouping ▾

Highlighting:) ▾ Link Delay > 100 ms (0 links) ▾

Selecting:

☑ Show All | Selected

☑ A2S-cisco.com-DSCP40

☑ A2S-cisco.com-DSCP46

Highlight nodes that match all / any

Search on Network, Country, IP address, Prefix, or Title...

Demo

Sharelinks

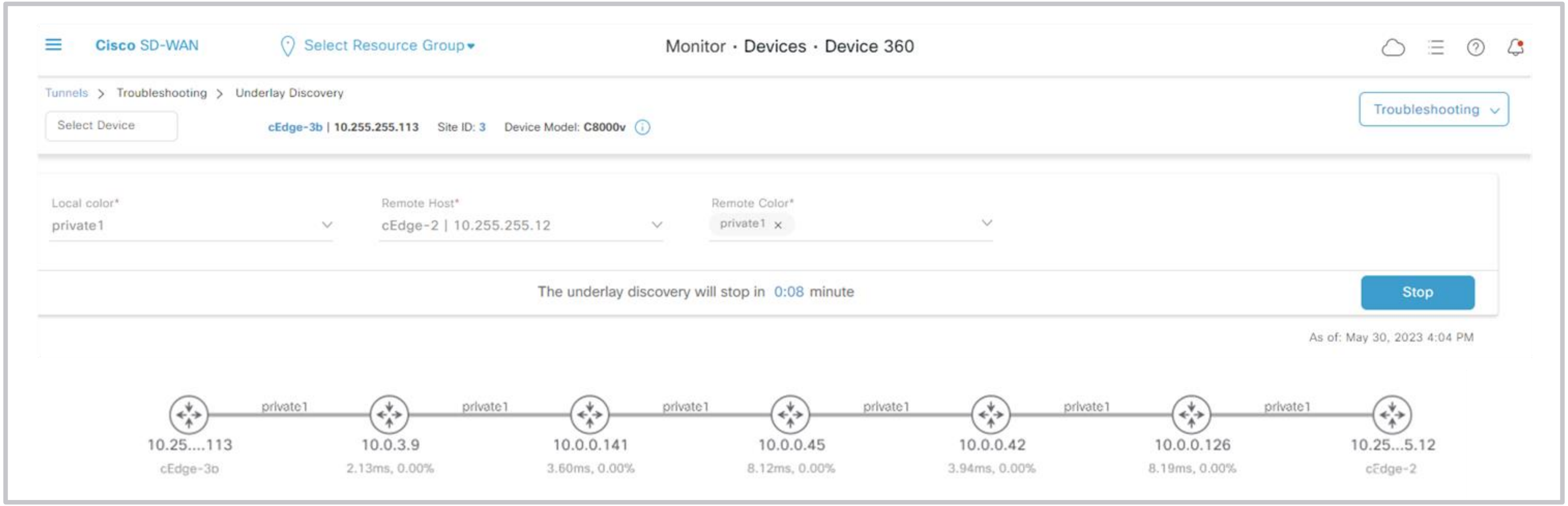
- Dual DIA towards CiscoLive.com
  https://aznerwsgznptcxfgabhpvcoxgkhsvmsu.share.thousandeyes.com

- A2A SDWAN Branch (1|3) <-> HQ (UDP)
  https://abqtqardmprnawyxhlzvzgrwbnxvmgbf.share.thousandeyes.com

- CiscoLive.com via Umbrella SIG
  https://akdnblkhoqxsosyrbybtdcqfieamwbel.share.thousandeyes.com

UMTS

Underlay Measurement and Tracing Services



Cisco SD-WAN   Select Resource Group   Monitor · Devices · Device 360

Tunnels > Troubleshooting > Underlay Discovery

Select Device   cEdge-3b | 10.255.255.113   Site ID: 3   Device Model: C8000v

Troubleshooting

Local color*: private1

Remote Host*: cEdge-2 | 10.255.255.12

Remote Color*: private1

The underlay discovery will stop in 0:08 minute

Stop

As of: May 30, 2023 4:04 PM

Q&A

Summary

- 1st step: choose agent deployment model that fits you best
- 2nd step: steer test traffic using SD-WAN data policy
- 3rd step: configure tests and improve test results

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

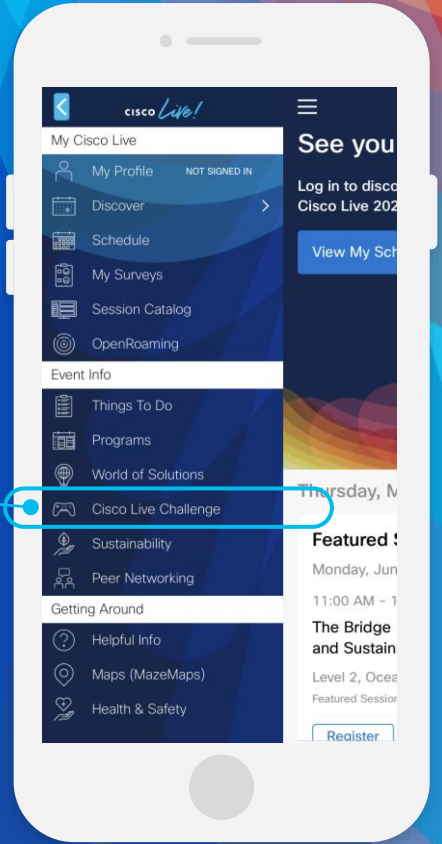
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let's go

#CiscoLive