



The bridge to possible

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

Andraz Piletic  
TSA / Instructor  
BRKENT-2126

CISCO *Live!*

#CiscoLive

# 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 7, 2024.

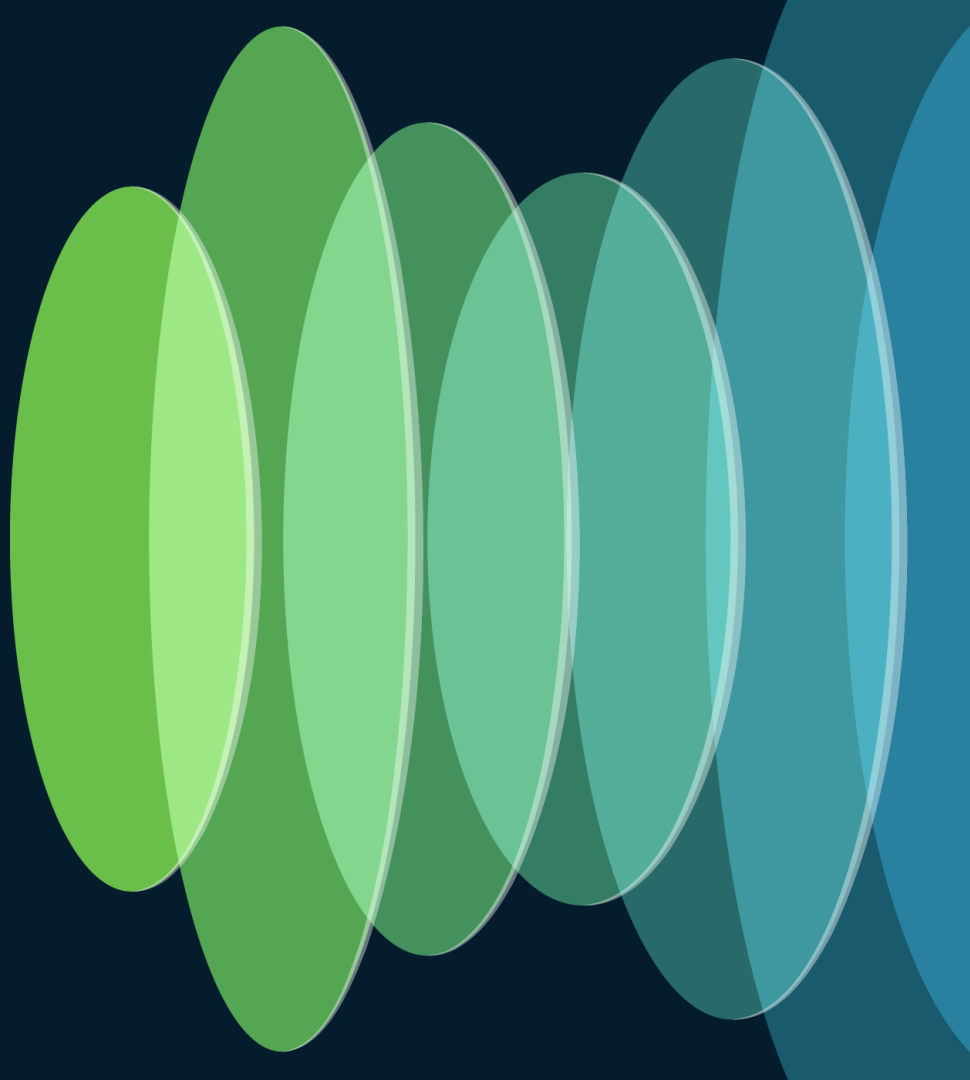




# Agenda

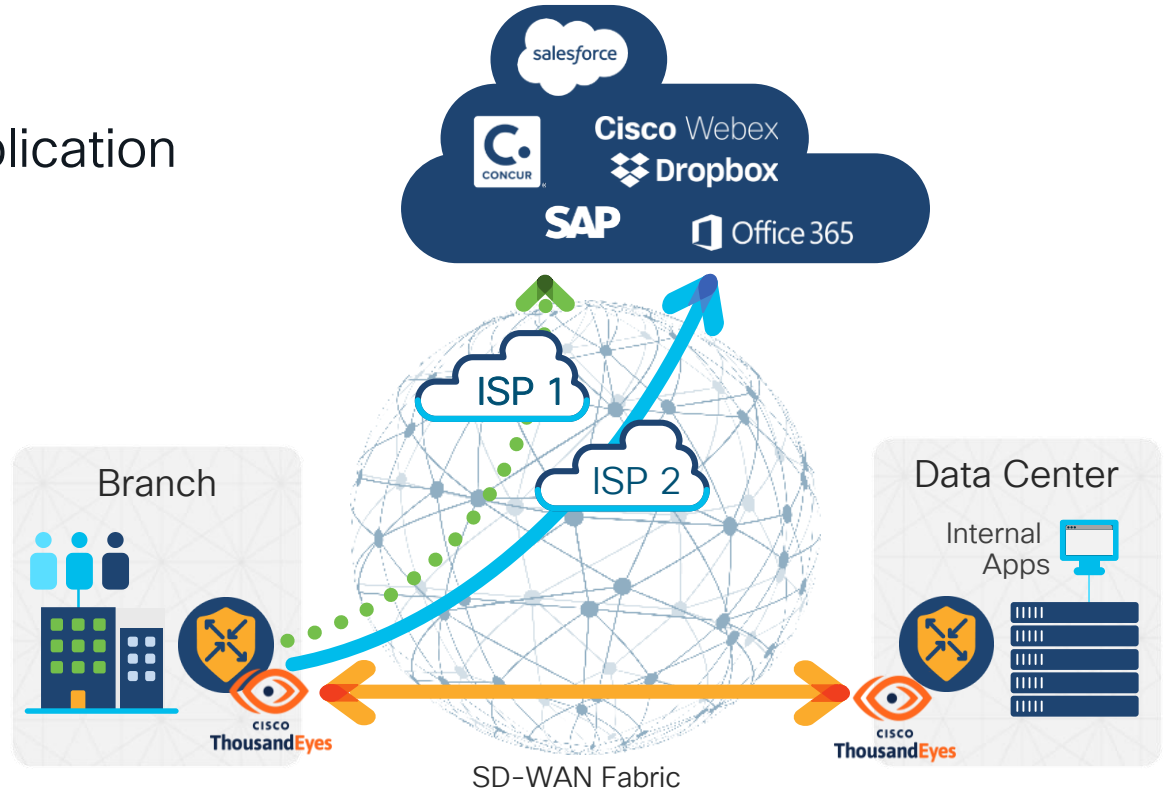
- Use Cases
- Agent Deployment Options
- Steering Test Traffic
- Configuring Tests & Viewing Results
- What If... ?
- NWPI

# SD-WAN + ThousandEyes

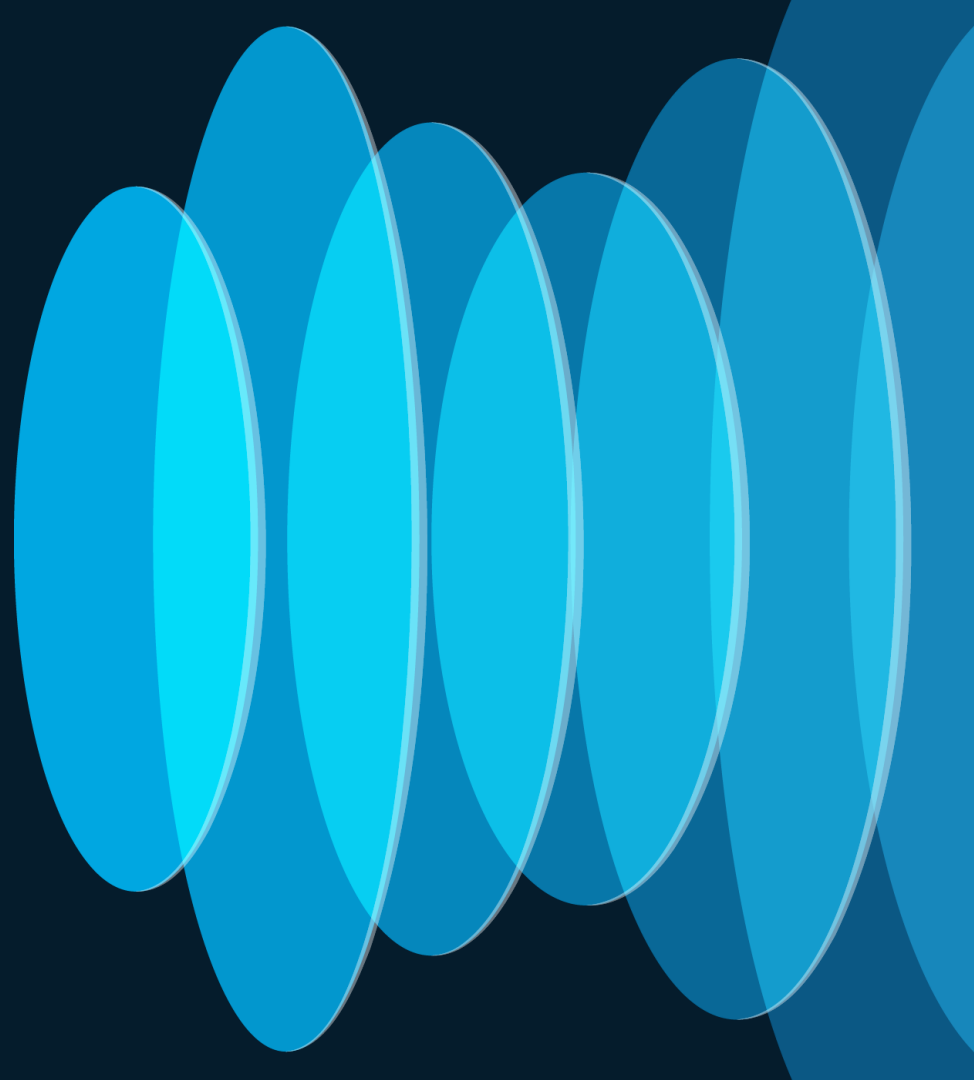


# Use Cases

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



# First Step: Deploying Embedded Agents

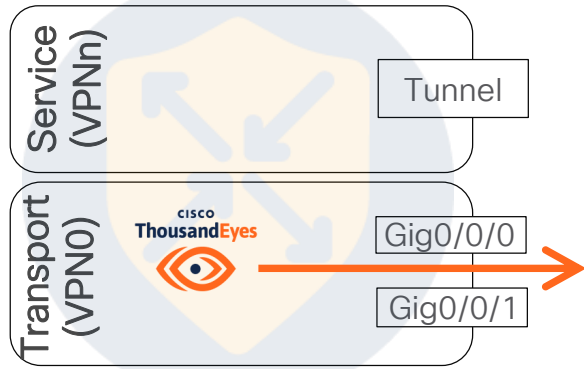


# Embedded Agent Requirements

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+		Cisco Catalyst SD-WAN Manager 20.8+
Catalyst 8500(L)				
Catalyst 8300 Catalyst 8200(L)			Not supported	
ISR44xx ISR43xx ISR42xx	Minimum 8G of RAM and Flash	IOS-XE 17.6.1+		Cisco Catalyst SD-WAN Manager 20.6+
ISR 1100X-4/6G		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	Catalyst Center 2.2.2.3+

# Deployment Options

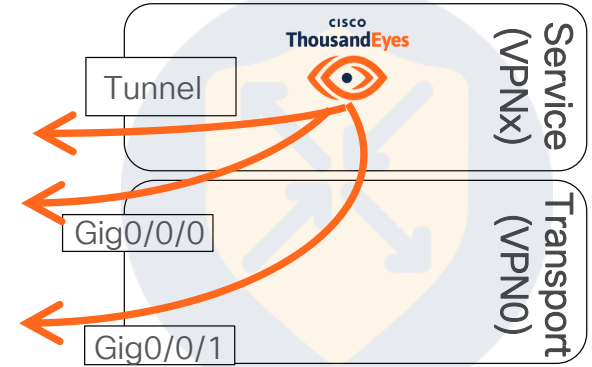
## Agent in VPN0



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



## Agent in Service VPN

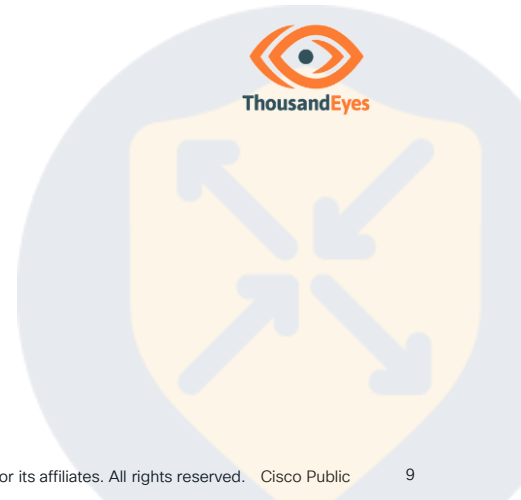


- Test traffic can follow SD-WAN policies
- Can monitor Overlay and Underlay paths
- Requires unique subnet



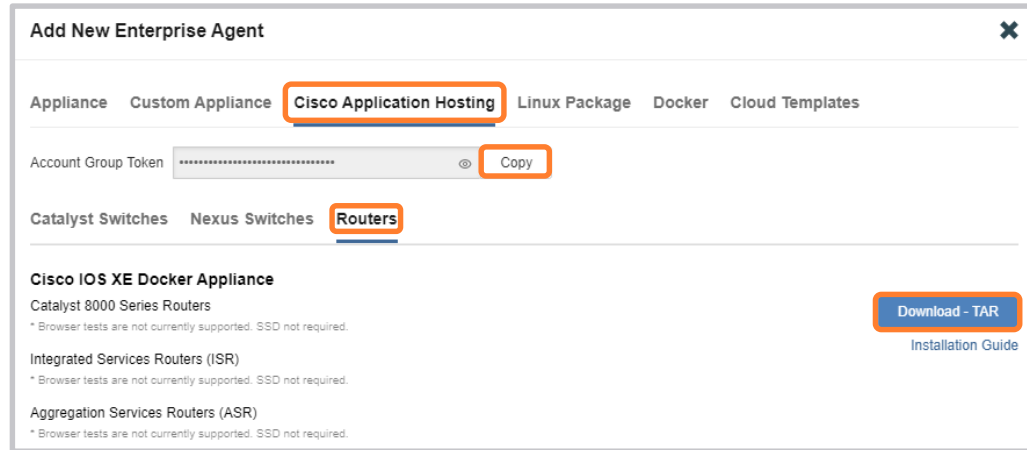
# Deploying ThousandEyes Agent Using vManage

- Download Agent Software from ThousandEyes portal
- Copy Account Group Token
- Upload Agent Software to Catalyst SD-WAN Manager (vManage)
- Define ThousandEyes Feature Template in Manager
- 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



The screenshot shows the 'Add New Enterprise Agent' window. The 'Cisco Application Hosting' tab is selected and highlighted with an orange box. Below it, the 'Account Group Token' field is shown with a 'Copy' button next to it, also highlighted with an orange box. Under the 'Catalyst Switches' section, the 'Routers' sub-tab is selected and highlighted with an orange box. In the 'Cisco IOS XE Docker Appliance' section, the 'Download - TAR' button is highlighted with an orange box, with a link to the 'Installation Guide' below it.

**Add New Enterprise Agent**

Appliance Custom Appliance **Cisco Application Hosting** Linux Package Docker Cloud Templates

Account Group Token [token] **Copy**

Catalyst Switches Nexus Switches **Routers**

**Cisco IOS XE Docker Appliance**

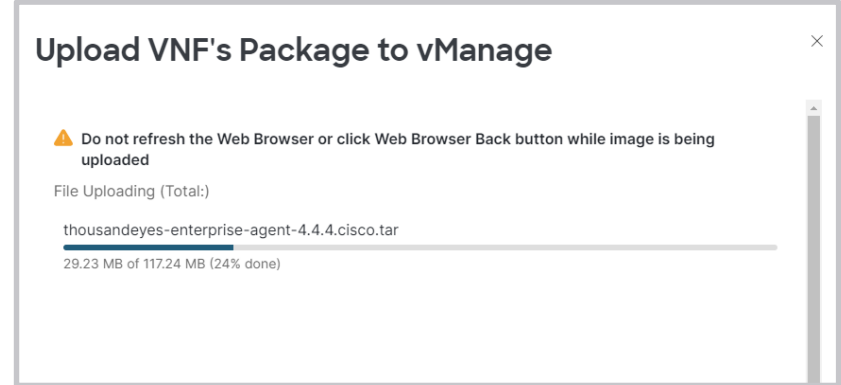
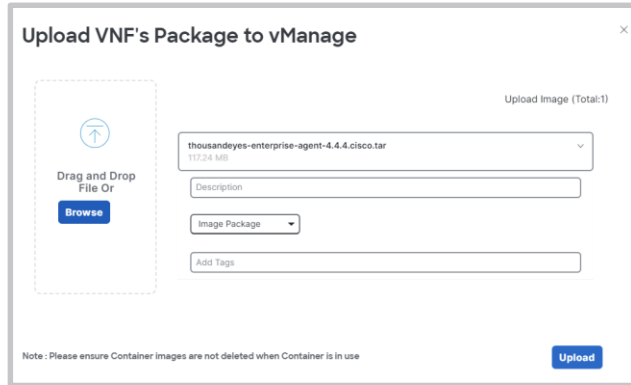
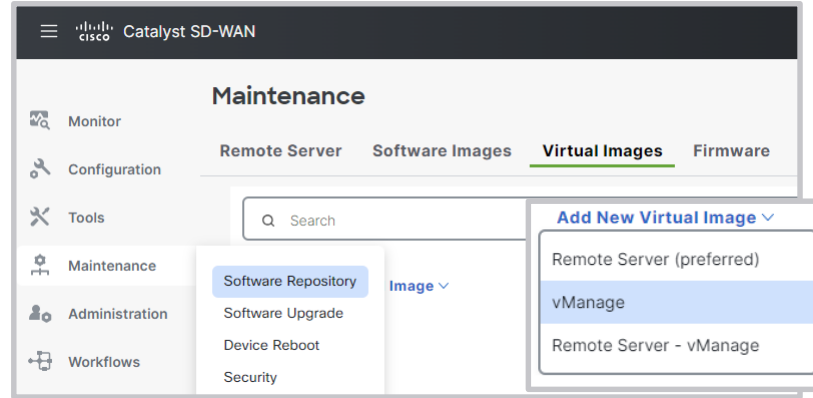
Catalyst 8000 Series Routers  
\* Browser tests are not currently supported. SSD not required.

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.

**Download - TAR**  
[Installation Guide](#)

# Uploading ThousandEyes Agent to vManage



# Defining ThousandEyes Feature Template

The screenshot displays the Cisco Catalyst SD-WAN configuration interface. The top navigation bar shows 'Catalyst SD-WAN'. The left sidebar contains a menu with 'Configuration' highlighted. The main content area is titled 'Configuration' and has two tabs: 'Device Templates' and 'Feature Templates', with the latter being the active tab. Under 'Feature Templates', there is a 'Select Devices' section with a search bar and a list of devices, including 'C8200-1N-4T' through 'C8500L-8S4X'. To the right, there is a 'Select Template' section with a grid of templates. The 'ThousandEyes Agent' template is highlighted with an orange border. Other templates include 'Cisco Banner', 'Cisco BGP', 'Cisco DHCP Server', 'Cisco IGMP', 'Cisco Logging', 'Cisco Multicast', 'Cisco OSPF', 'Cisco OSPFV3', 'Cisco PIM', 'Cisco SNMP', 'CLI Add-On Template', 'EIGRP', and 'TrustSec'.

**Configuration**

**Feature Templates**

**Select Devices**

Q c8

- ☐ C8000v
- ☒ C8200-1N-4T
- ☒ C8200L-1N-4T
- ☒ C8300-1N1S-4T2X
- ☒ C8300-1N1S-6T
- ☒ C8300-2N2S-4T2X
- ☒ C8300-2N2S-6T
- ☒ C8500-12X
- ☒ C8500-12X4QC
- ☒ C8500-20X6C
- ☒ C8500L-8S4X

**Select Template**

**OTHER TEMPLATES**

Cisco Banner	Cisco BGP WAN LAN	Cisco DHCP Server LAN
Cisco IGMP LAN	Cisco Logging	Cisco Multicast
Cisco OSPF WAN LAN	Cisco OSPFV3 WAN LAN	Cisco PIM LAN
Cisco SNMP	CLI Add-On Template WAN	EIGRP LAN
Probes	<b>ThousandEyes Agent</b>	TrustSec

# 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

## Configuration

[Device Templates](#) **[Feature Templates](#)**

[Feature Template](#) > [Add Template](#) > ThousandEyes Agent

Device Type

C8200-1N-4T,C8200L-1N-4T,C8300-1N1S-4T2X

Template Name\*

ThousandEyes-Embedded-Agent

Description\*

TE in Service VPN10

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

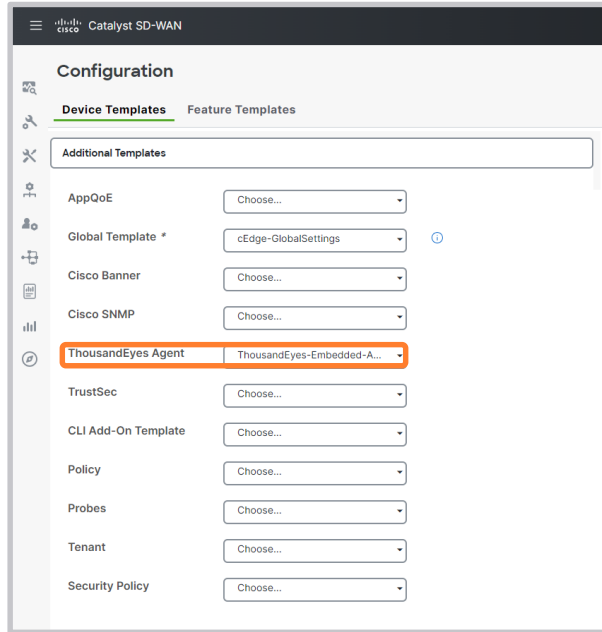
Hostname

Web Proxy Type

☒ Static

☐ PAC

# Attaching a Feature Template



```
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.DnssecTaskProcessor] {} 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://scl.thousandeyes.com  
2022-06-09 10:42:59.324 INFO [20047f00] [te.agent.ClusterMasterAdapter] {} Attempting to get controller assignment from  
https://scl.thousandeyes.com  
2022-06-09 10:43:01.369 INFO [20047f00] [te.agent.ClusterMasterAdapter] {} https://scl.thousandeyes.com told us we should talk  
to controller cl.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.
```

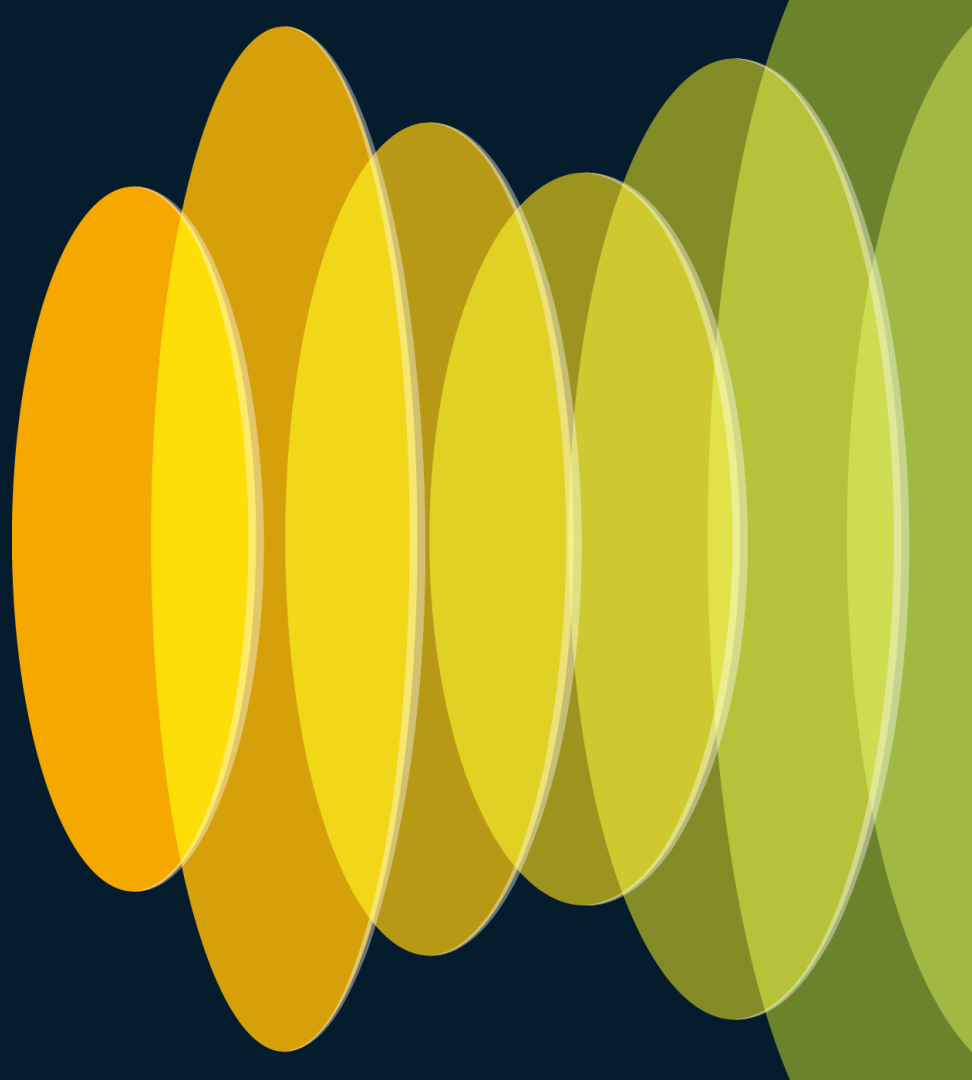
- Remove specific package (embedded agents only)

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

- Restart the agent

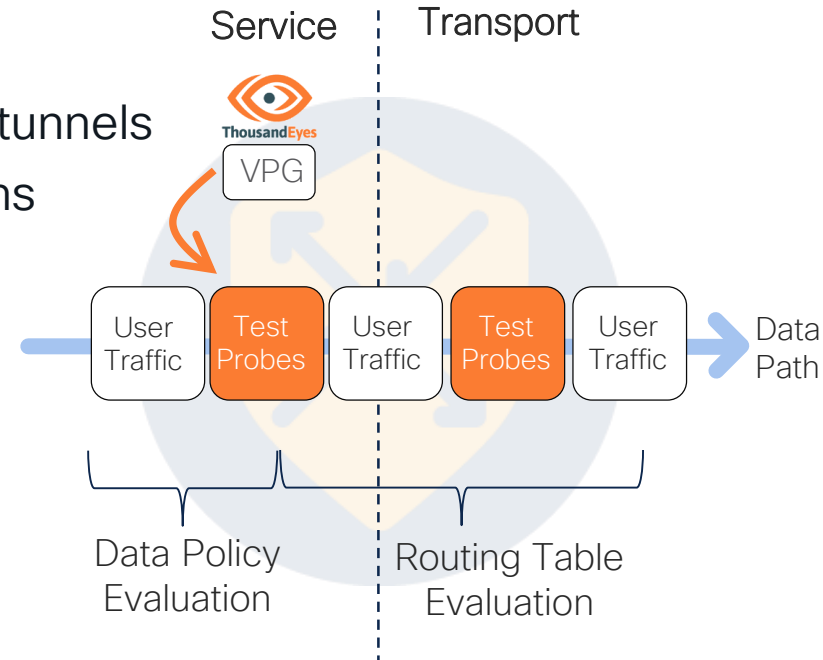
```
root@cEdge:/# sv restart te-agent
```

# Second Step: Steering Test Traffic

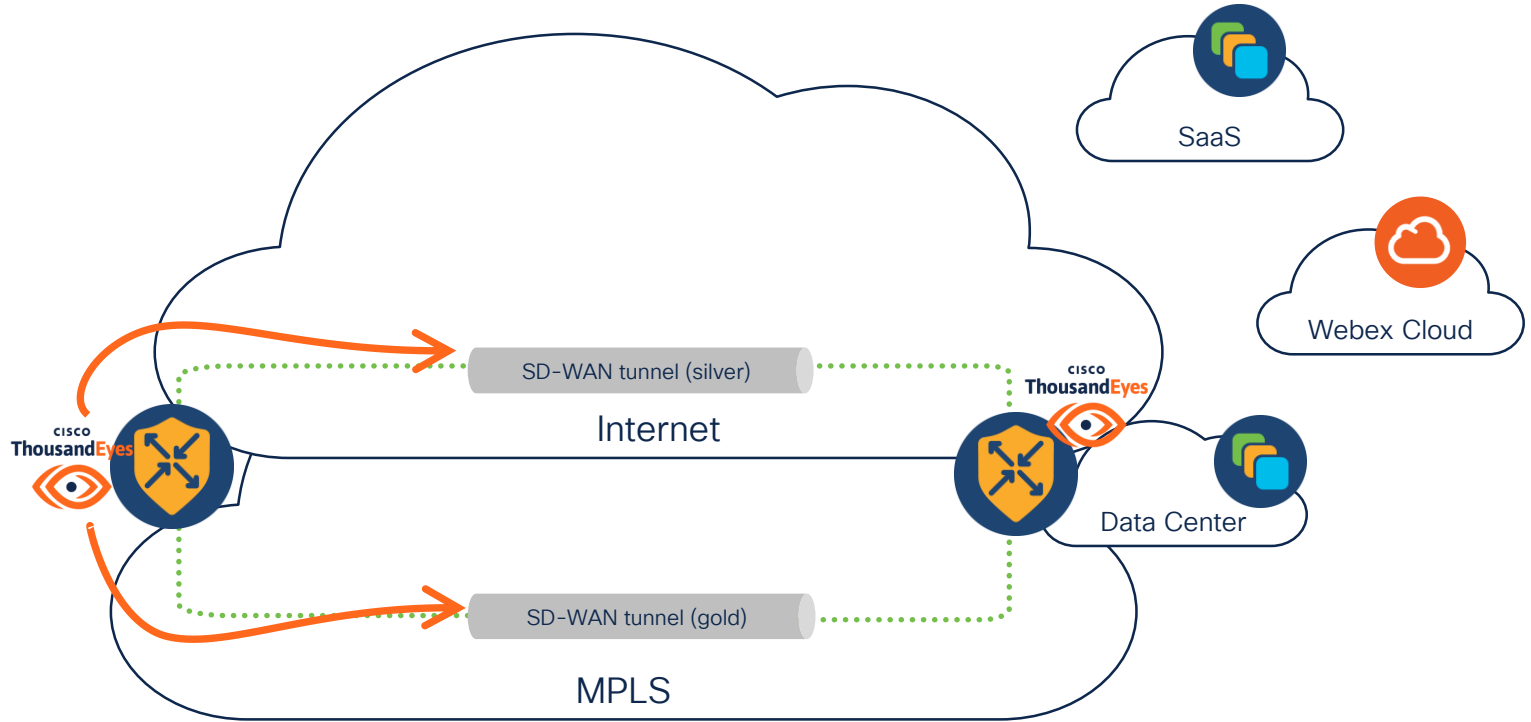


# Common Objectives

- 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
    encaps 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
    encaps 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
```

The screenshot displays a network configuration interface with a sidebar on the left and a main content area. The sidebar has a 'Sequence Type' button and a 'Custom' section with a 'Default Action' button. The main content area is titled 'Custom' and shows two sequence rules, numbered 1 and 2. Each rule has a 'Match Conditions' table and an 'Actions' table.

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

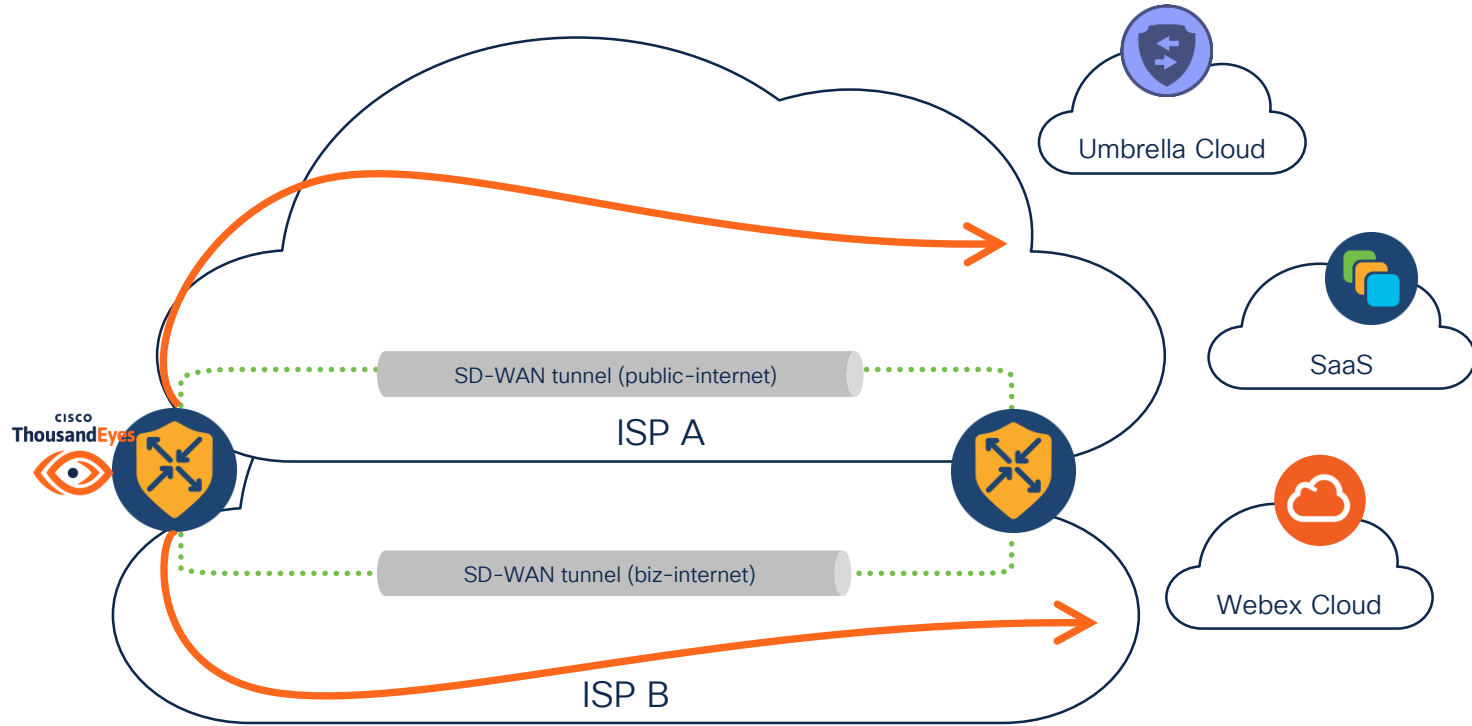
Actions	
Accept	
Local TLOC List:	gold
Encapsulation	IPSEC
Restrict	true

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

Actions	
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

Sequence Type

Drag & drop to reorder

Custom

Default Action

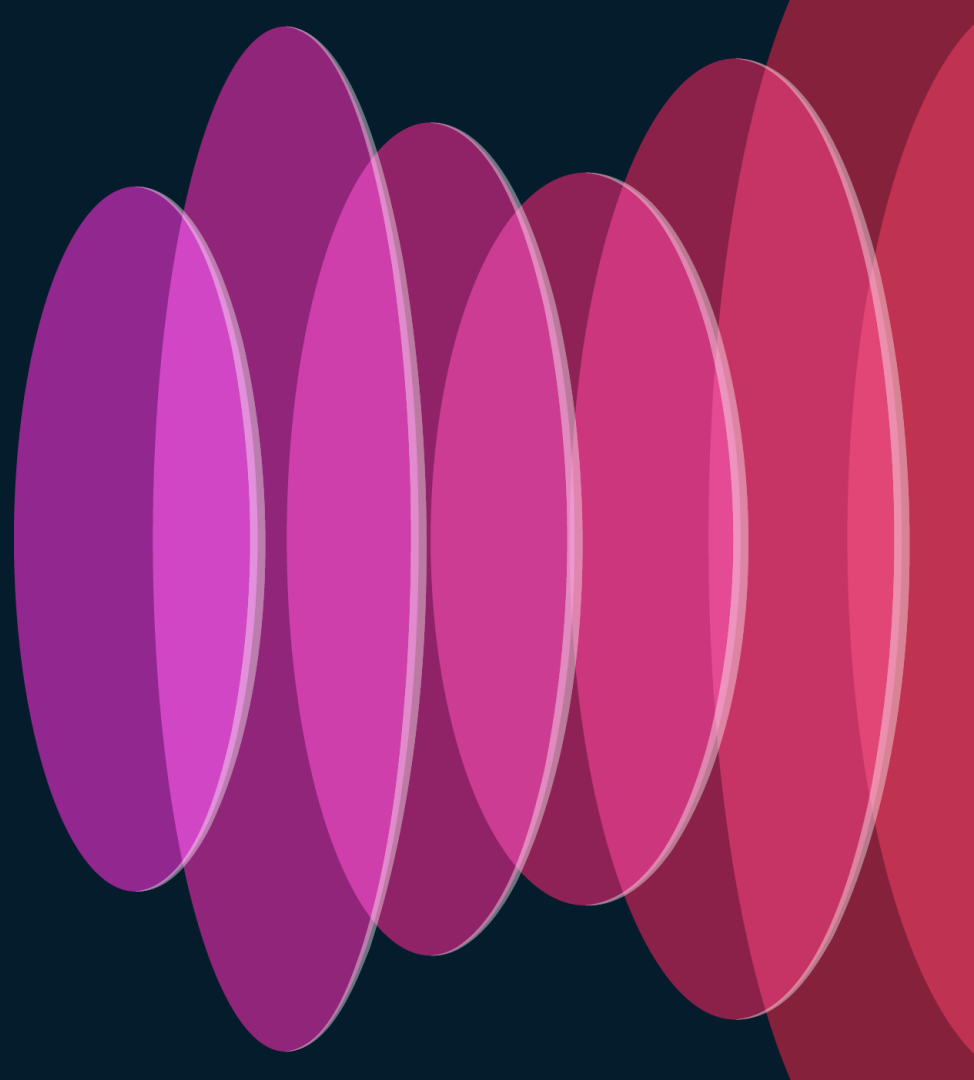
1

Match Conditions	Actions
DSCP: 46	Accept
Source Data Prefix List: All_TE_Agents	NAT VPN: 0
Source: IP	Fallback
	Local TLOC List: public-internet
	Encapsulation IPSEC
	Restrict true
	DSCP: 0

2

Match Conditions	Actions
DSCP: 40	Accept
Source Data Prefix List: All_TE_Agents	NAT VPN: 0
Source: IP	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

The screenshot shows the 'New Test' configuration window. The 'Layer' tab is set to 'Network'. The 'Test Type' is 'Agent to Agent'. The 'Test Name' is 'A2A-SDWAN' and the 'Test Description' is 'BRKENT-2126'. The 'Basic Configuration' tab is active, showing the 'NETWORK' section. The 'Server Port' is set to 49153. The 'MSS' is set to 'Auto'. The 'Collect BGP data' checkbox is checked, with a note 'All public BGP monitors will be included'. The 'Transmission Rate' checkbox is unchecked. The 'No. of Path Traces' is set to 'Default (3)'. The 'DSCP' is set to 'Best Effort (DSCP 0)'. The 'Server Port' and 'DSCP' fields are highlighted with orange boxes.

# 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)

The screenshot shows the configuration page for an agent named TEA-1. The 'Advanced Settings' tab is active. Under 'IPV6 SETTING', the 'Policy' is set to 'IPv4 Only'. The 'TARGET FOR TESTS' section is highlighted with an orange box and contains the IP address '203.0.113.2' and a checkbox for 'Behind a NAT'. The 'General Information' section on the right shows the agent is 'Online' and lists system details. Two fields, 'Private IP Address' and 'Public IP Address', are also highlighted with orange boxes.

General 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

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

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)

# Web Layer Tests

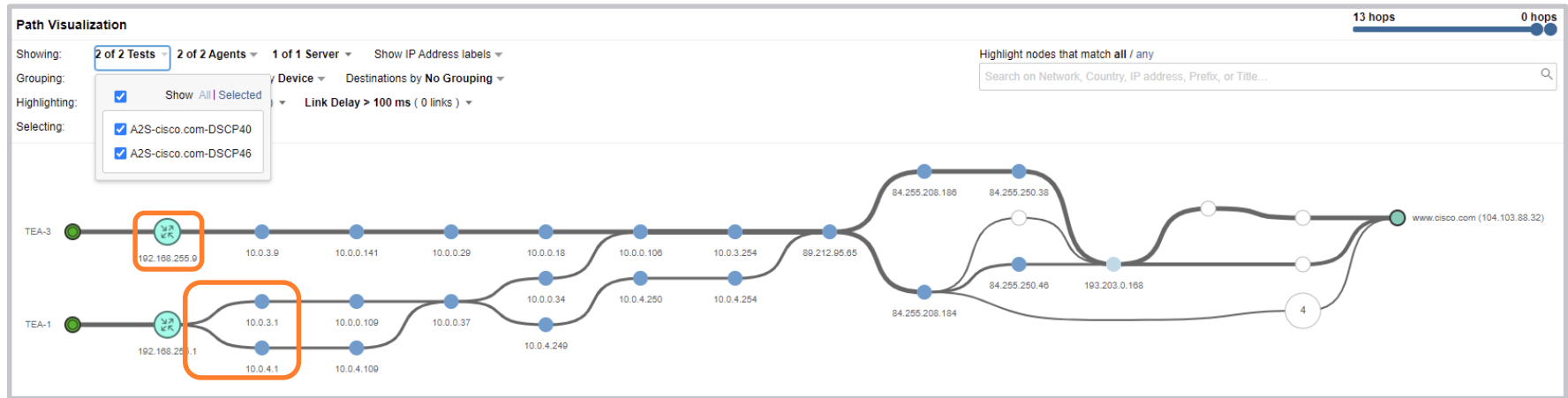
- Matching different web test traffic with an SD-WAN data policy becomes a challenge:
  - No DSCP coloring options, source ports settings, etc.
  - Only HTTP Server test supports different source interfaces\*
- BrowserBot is needed for Page Load and Transaction tests
- Alternative – Multiple agents in a branch

# What about SASE?

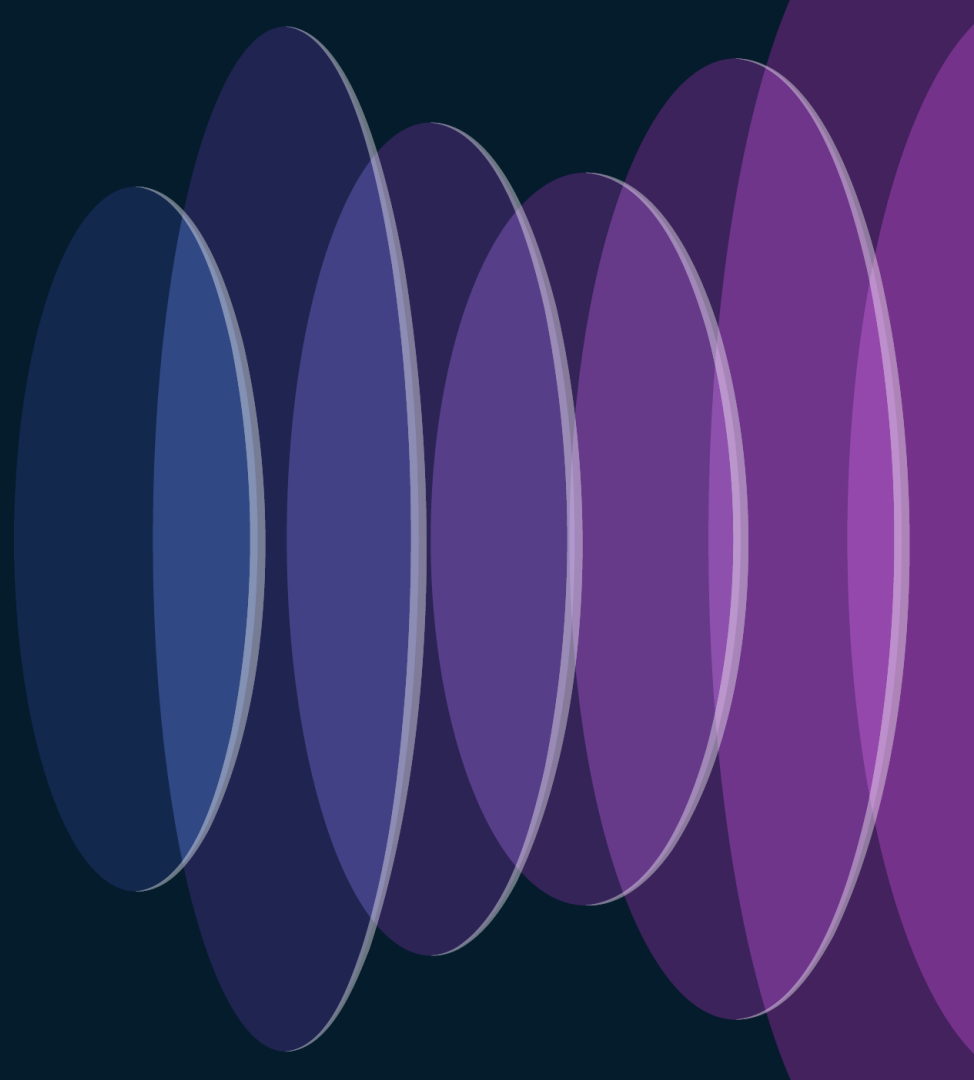
- Secure Internet Gateways (proxies) break network visibility
  - Utilize web tests for end-to-end application performance and visibility
  - Monitor underlay to IPsec/GRE gateways using A2S network tests
- HTTPs/SSL decryption requires additional installation step on agents
  - Import utilized CA certificate ([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



# Demo



# Sharelinks

- Dual DIA towards CiscoLive.com

<https://aznerwsgznptcxfgabhpvcxgkhsvmsu.share.thousandeyes.com>

- A2A SDWAN Branch (1|3) <-> HQ (UDP)

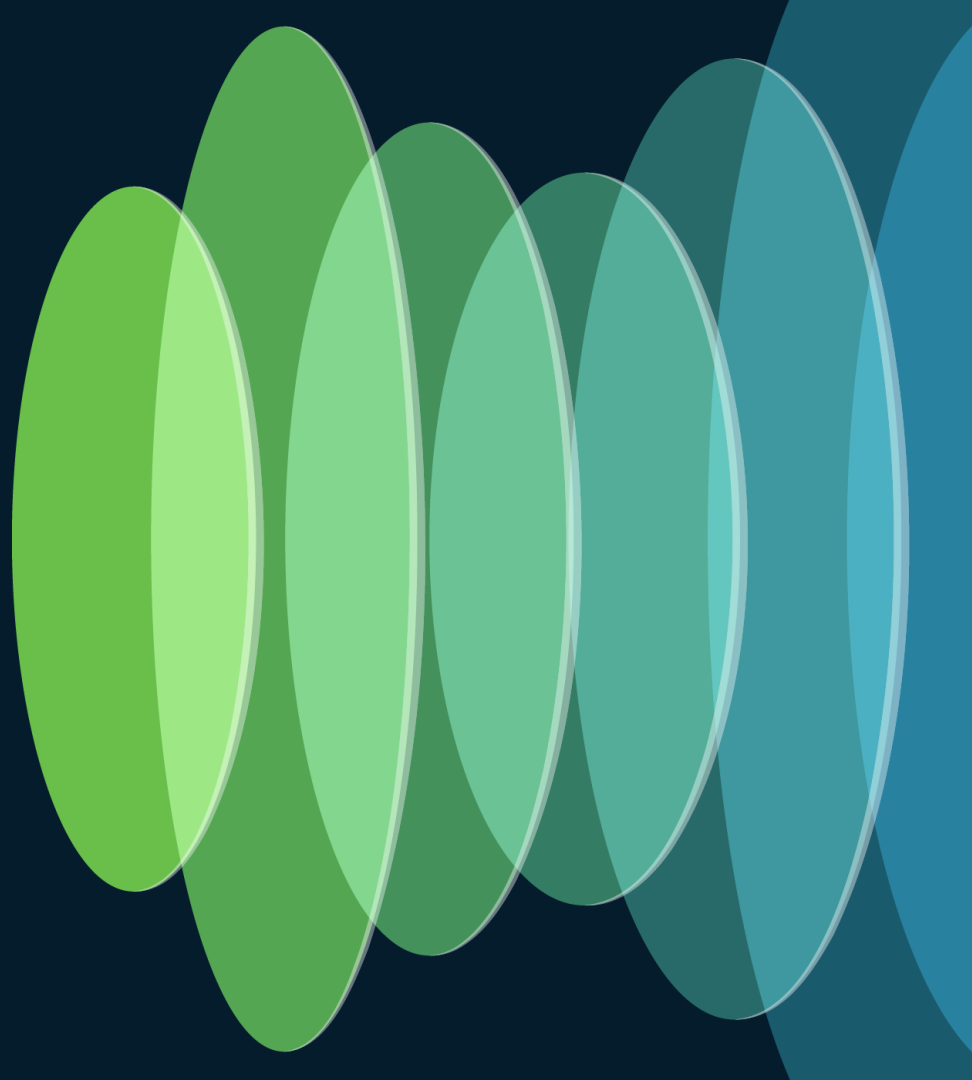
<https://abqtqardmprnawyxhlzvzgrwbnxvmgbf.share.thousandeyes.com>

- CiscoLive.com via Umbrella SIG

<https://akdnblkhoqxsosyrbybtdcqfieamwbel.share.thousandeyes.com>



# What If... ?



# Unsupported Platforms

Catalyst SD-WAN

Feature Template > Add Template > **CLI Add-On Template**

Device Type: C8000v

Template Name: NoTEonC8000v

Description: NoTEonC8000v

CLI CONFIGURATION

```
1 interface VirtualPortGroup4
2   no shutdown
3   vrf forwarding 10
4   ip address 172.16.11.1 255.255.255.252
5   iox
6   app-hosting appid te
7   app-default-gateway 172.16.11.1 guest-interface 0
8   app-resource docker
9     prepend-pkg-opts
10    run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=BRKENT2126"
11   app-vnic gateway0 virtualportgroup 4 guest-interface 0
12   guest-ipaddress 172.16.11.2 netmask 255.255.255.252
13   name-server0 208.67.222.222
```

Cancel Save

# Manual Agent Installation

- Objective: keep device in vManage mode

```
C8000v# copy https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.4.4.cisco.tar
bootflash:
Destination filename [thousandeyes-enterprise-agent-4.4.4.cisco.tar]?
Accessing https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.4.4.cisco.tar...
Loading https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.4.4.cisco.tar
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
122931200 bytes copied in 98.909 secs (1242872 bytes/sec)
```

```
C8000v# app-hosting install appid te package bootflash:thousandeyes-enterprise-agent-4.4.4.cisco.tar
Installing package 'bootflash:thousandeyes-enterprise-agent-4.4.4.cisco.tar' for 'te'.
Use 'show app-hosting list' for progress.
```

```
C8000v# show app-hosting list
```

App id	State
te	DEPLOYED

# Manual Agent Activation

```
C8000v# app-hosting activate appid te
te activated successfully
Current state is: ACTIVATED
```

```
C8000v# show app-hosting list
App id                               State
-----
te                                   ACTIVATED
```

```
C8000v# app-hosting start appid te
te started successfully
Current state is: RUNNING
```

```
C8000v# show app-hosting list
App id                               State
-----
te                                   RUNNING
```

# Multiple Agents?

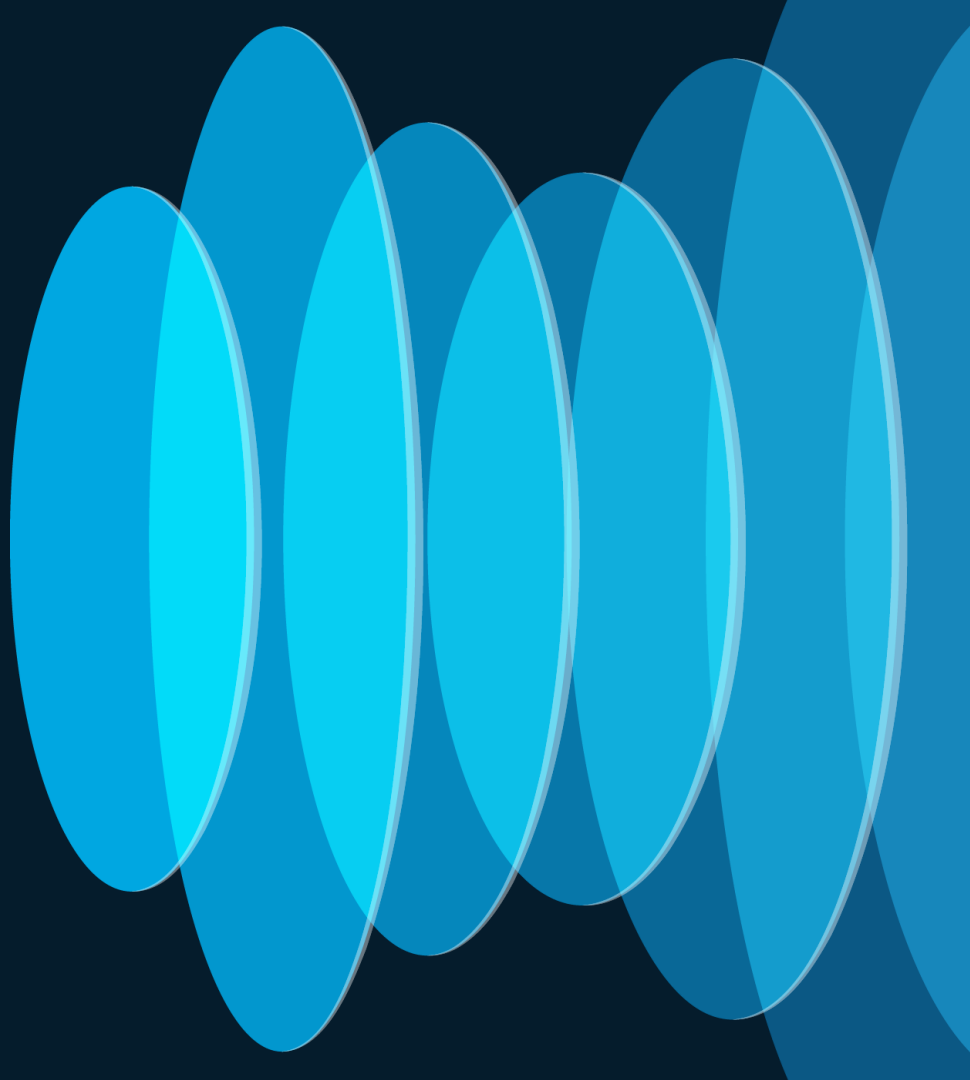
```
interface VirtualPortGroup5
  no shutdown
  vrf forwarding 12
  ip address 172.16.12.1 255.255.255.252
  iox
  app-hosting appid te2
  app-default-gateway 172.16.12.1 guest-interface 0
  app-resource docker
  prepend-pkg-opts
  run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=BRKENT2126"
  app-vnic gateway0 virtualportgroup5 guest-interface 0
  guest-ipaddress 172.16.12.2 netmask 255.255.255.252
  name-server0 208.67.222.222
```

```
C8000v# show app-hosting list
```

App id	State
te	RUNNING
te2	RUNNING



# Network Wide Path Insights Integration



# NWPI Integration with Cisco ThousandEyes

- NWPI Trace data and ThousandEyes test data is auto correlated (Since 20.14)
- Underlay Measurement and Tracing Service (UMTS) results are combined with ThousandEyes test results.

Applications

Completed Flows

Selected Flow Id: 1206

Filter

Feb 19, 2024, 10:30:07 AM

Feb 19, 2024, 10:32:10 AM

Feb 19, 2024, 10:38:16 AM

ThousandEyes Test: 4877322

Flow Id: 1206

Search by Domain, Application, Readout, etc.

\* Readout Legend: Error, Warning, Information, Synthetic Traffic, ThousandEyes.

Search

Overall 4830 flows traced, 1 flows traced during Feb 19, 2024 10:32:10 AM to Feb 19, 2024 10:38:16 AM

Total Rows: 1

irt - Update Time	Flow Id	Readout *	VPN Id	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART C
32:13 AM-10:32:13 AM	1206		1	192.130.1.2	55889	10.20.25.110	443	TCP	DEFAULT ↑ / DEFAULT ↓	ssl	other	www.box.ar	vm5:
Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms) *	Latency(ms) *	ART CND(ms)/SND(ms) *		
Upstream	0	(VirtualPortGroup0) vm5	vm6	LTE	LTE	0.00	0.00	0.00	< 1	19	vm5: 1/60		
Upstream	1	vm6 (Gi5)	LAN Side	Service LAN	N/A	0.00	N/A	N/A	N/A	N/A	vm6: 40/21		
Downstream	0	LAN Side	(Gi5)vm6	N/A	Service LAN	N/A	N/A	0.00	N/A	N/A	N/A		
Downstream	1	vm6	vm5(VirtualPortGroup0)	LTE	LTE	0.00	0.00	0.00	< 1	19	N/A		

Flow Readout

Overview

Path Insight

Underlay Insight

Trace: te\_insight-test (ID: 32), Flow ID: 1041 (Application:rtp-audio)

Upstream From 192.130.1.2:51851 to 192.130.3.2:49152

Downstream From 192.130.3.2:49152 to 192.130.1.2:51851

Overall Status

This flow is normal without special event observed.

=====

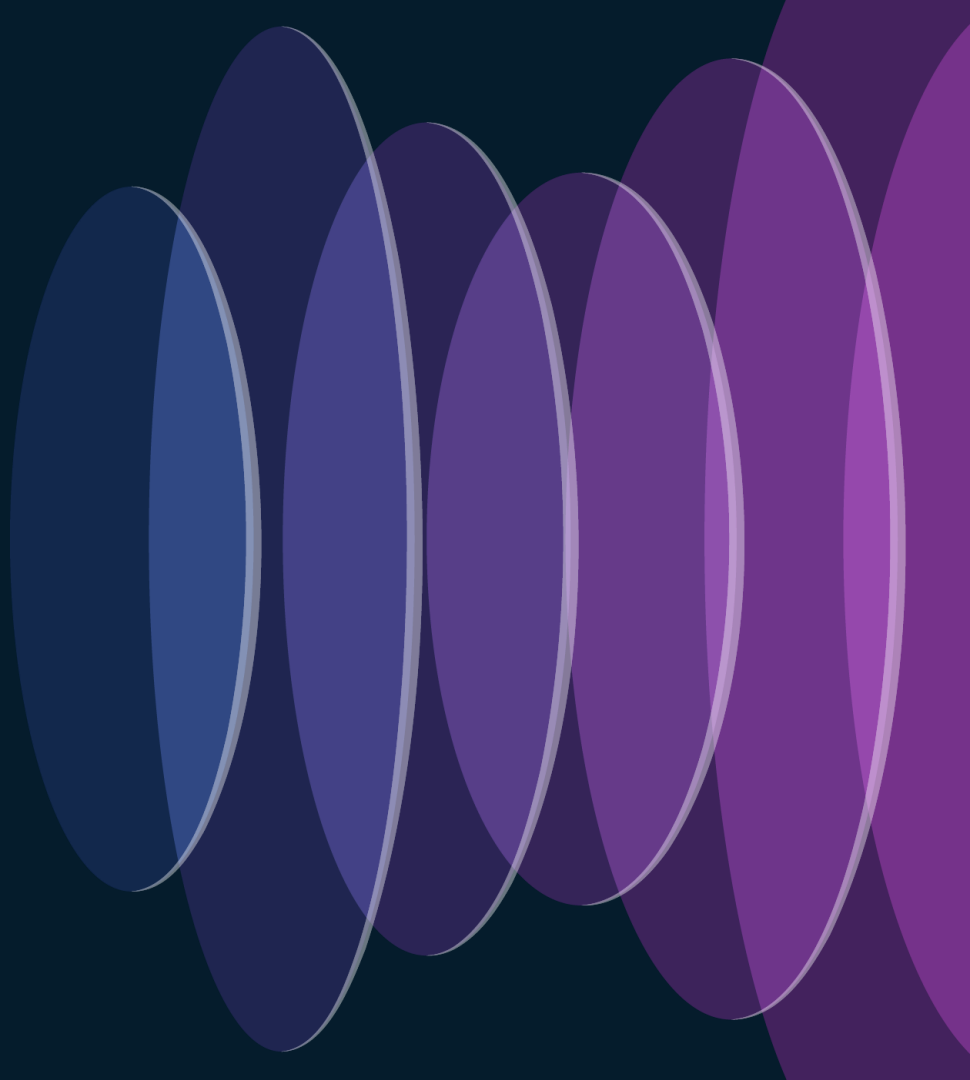
This flow belongs to a ThousandEyes test.

Test name: 1721840222-vm5voice (Agent: 1721840222-vm5,

Go To ThousandEyes Go To Insight Summary

=====

# Q&A





# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

---



**Earn 100 points** per survey completed and compete on the Cisco Live Challenge leaderboard.

---



Level up and earn **exclusive prizes!**

---



Complete your surveys in the **Cisco Live mobile app**.

# 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](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive