Use Cases

Use Case 1: Verify a Cisco Cloud OnRamp for SaaS Policy

Assume that you have a deployment that includes several branch sites. One of these sites, the SJC branch, with a site ID of 3, has two WAN links: an MPLS link, and a public internet link through which the Microsoft cloud can be accessed directly.

In addition, assume that a Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy, which is a part of an Application-Aware Routing (App-route) policy, has been created and enabled for Microsoft Office 365 applications.

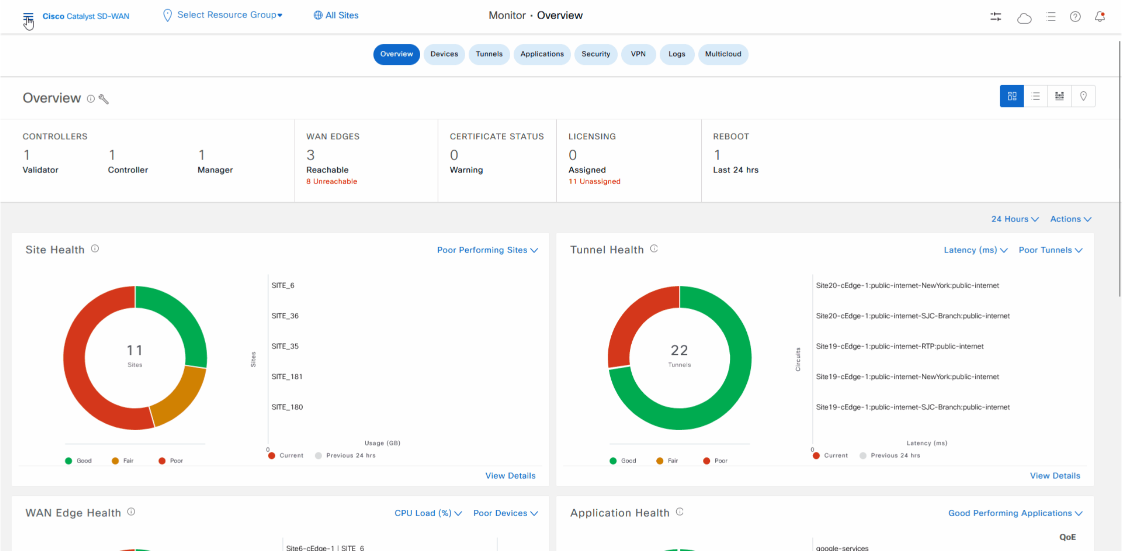
In this use case, let's see how network-wide path insight can be used to determine whether the traffic from Microsoft Office 365 applications is following the expected network path, validate that the policy is programmed correctly and operates as intended, and view the configuration of the policy.

To begin, perform the following actions to start a trace in the SJC branch:

1. From the Cisco Catalyst SD-WAN menu, choose, **Tools** > **Network Wide Path Insight**.
2. Click **New Trace**.
3. In the **Trace Name** field, enter a name for the trace.

   In this use case, we use the name **Verify-Cor-Saas-Policy**.
4. From the **VPN** drop-down list, choose **VPN - 10**.
5. Click **Start**.

Figure 1: Start a Trace



CONTROLLERS: 1 Validator, 1 Controller, 1 Manager

WAN EDGES: 3 Reachable, 8 Unreachable

CERTIFICATE STATUS: 0 Warning

LICENSING: 0 Assigned, 11 Unassigned

REBOOT: 1 Last 24 hrs

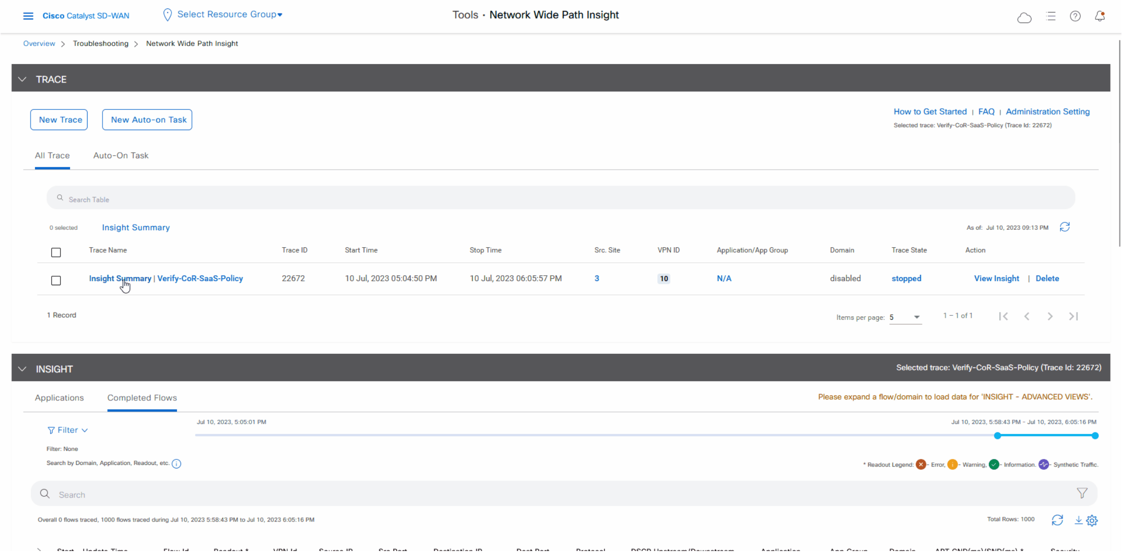
Let the trace run for approximately 5 minutes so that it can collect data, then perform the following actions to see a Sankey diagram that shows the network paths of Microsoft Office 365 applications traffic. This application-level information lets you see whether the traffic is taking the expected network path according to your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy.

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Verify-Cor-Saas-Policy** trace.

2. In the **Insight Summary** slide-in pane, choose the **App Performance Insight** tab and use the filters to see the Sankey chart that shows the network paths of Microsoft applications traffic.

   The Sankey chart shows that this traffic flows directly from the SJC branch to the SaaS cloud-based host.

Figure 2: Display the Upstream Application Path & Performance Sankey Chart



Selected trace: Verify-CoR-SaaS-Policy (Trace Id: 22672)

As of: Jul 10, 2023 09:13 PM

	Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
□	Insight Summary | Verify-CoR-SaaS-Policy	22672	10 Jul, 2023 05:04:50 PM	10 Jul, 2023 06:05:57 PM	3	10	N/A	disabled	stopped	View Insight | Delete

1 Record

Items per page: 5   1 – 1 of 1

Selected trace: Verify-CoR-SaaS-Policy (Trace Id: 22672)

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Jul 10, 2023, 5:05:01 PM

Jul 10, 2023, 5:58:43 PM - Jul 10, 2023, 6:05:16 PM

Filter: None

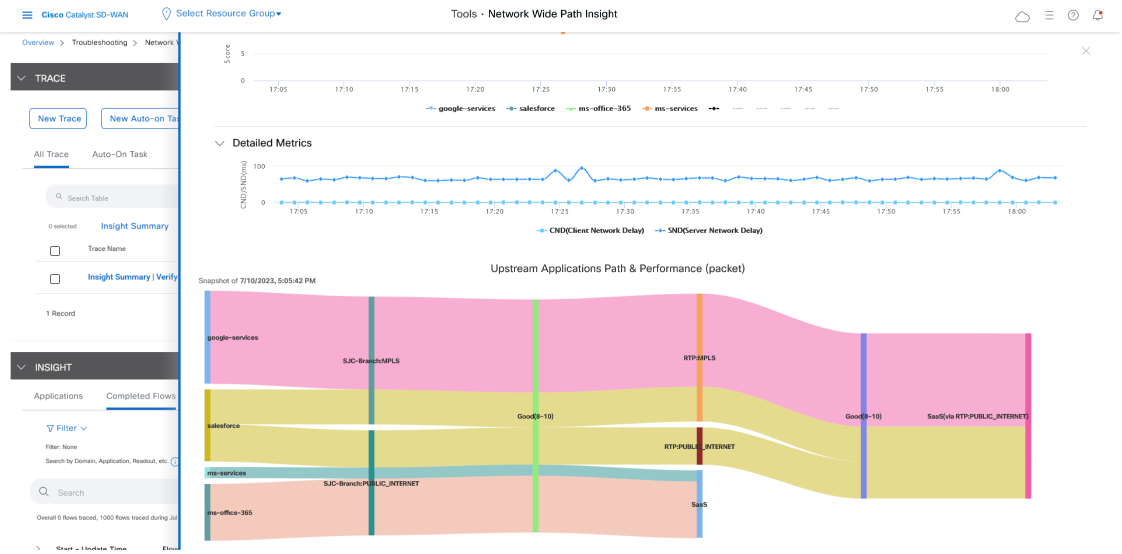
Search by Domain, Application, Readout, etc.

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

Overall 0 flows traced, 1000 flows traced during Jul 10, 2023 5:58:43 PM to Jul 10, 2023 6:05:16 PM

Total Rows: 1000

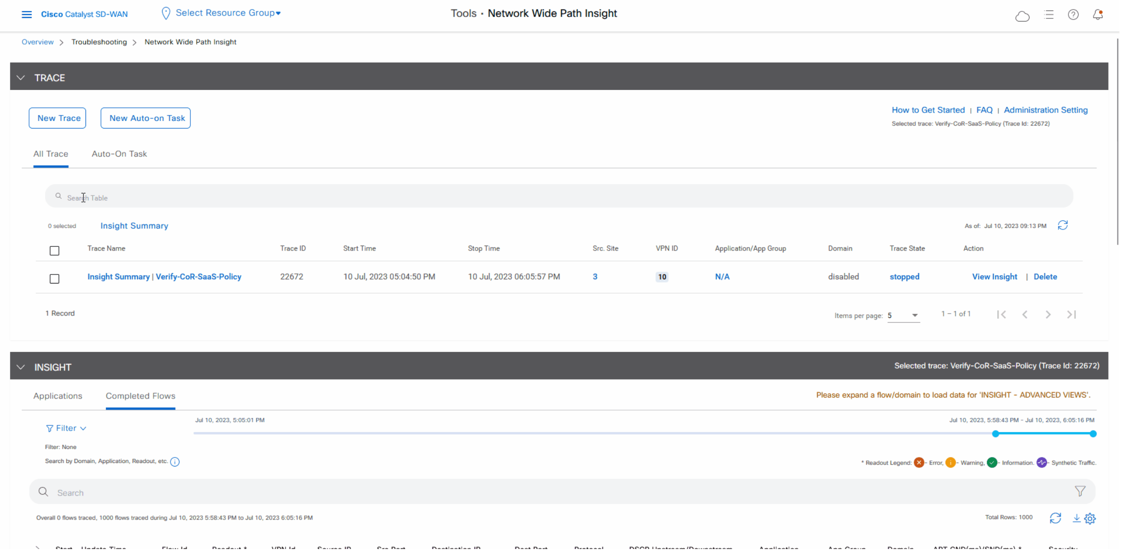
Figure 3: Upstream Application Path & Performance Sankey Chart



After reviewing application-level data, you can check whether your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy took effect for Microsoft Office 365 applications traffic. To do so, look at flow-level information for this traffic:

1. In the **All Trace** tab, go to the **Completed Flows** tab in the **Insight** area.
2. Search for **Office**.
3. For any Microsoft Office 365 flow, click the green check mark in the **Readout** column to display the **Flow Readout** slide-in pane.
4. Click the **Path Insight** tab in the **Flow Readout** pane.

Figure 4: View Flow-Level Information



Selected trace: Verify-CoR-SaaS-Policy (Trace Id: 22672)

0 selected

As of: Jul 10, 2023 09:13 PM

□	Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
□	Insight Summary | Verify-CoR-SaaS-Policy	22672	10 Jul, 2023 05:04:50 PM	10 Jul, 2023 06:05:57 PM	3	10	N/A	disabled	stopped	View Insight | Delete

1 Record

Items per page: 5 1 – 1 of 1

Selected trace: Verify-CoR-SaaS-Policy (Trace Id: 22672)

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Jul 10, 2023, 5:05:01 PM

Jul 10, 2023, 5:58:43 PM - Jul 10, 2023, 6:05:16 PM

Filter: None

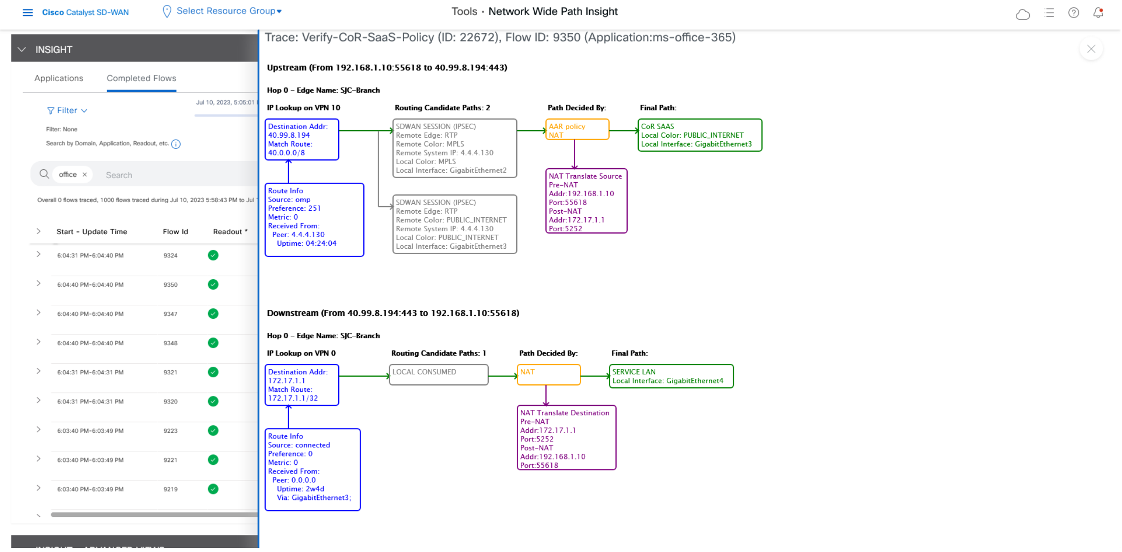
Search by Domain, Application, Readout, etc.

* Readout Legend: ✕- Error, !- Warning, ✓- Information, - Synthetic Traffic.

Overall 0 flows traced, 1000 flows traced during Jul 10, 2023 5:58:43 PM to Jul 10, 2023 6:05:16 PM

Total Rows: 1000

Figure 5: Flow-Level Information



Filter: None

Search by Domain, Application, Readout, etc.

office × Search

Overall 0 flows traced, 1000 flows traced during Jul 10, 2023 5:58:43 PM to Jul

Start - Update Time	Flow Id	Readout *
6:04:31 PM-6:04:40 PM	9324	✓
6:04:40 PM-6:04:40 PM	9350	✓
6:04:40 PM-6:04:40 PM	9347	✓
6:04:40 PM-6:04:40 PM	9348	✓
6:04:31 PM-6:04:31 PM	9321	✓
6:04:31 PM-6:04:31 PM	9320	✓
6:03:40 PM-6:03:49 PM	9223	✓
6:03:40 PM-6:03:49 PM	9221	✓
6:03:40 PM-6:03:49 PM	9219	✓

Trace: Verify-CoR-SaaS-Policy (ID: 22672), Flow ID: 9350 (Application:ms-office-365)

Upstream (From 192.168.1.10:55618 to 40.99.8.194:443)

Hop 0 – Edge Name: SJC-Branch

IP Lookup on VPN 10

Destination Addr:
40.99.8.194
Match Route:
40.0.0.0/8

Route Info
Source: omp
Preference: 251
Metric: 0
Received From:
Peer: 4.4.4.130
Uptime: 04:24:04

Routing Candidate Paths: 2

SDWAN SESSION (IPSEC)
Remote Edge: RTP
Remote Color: MPLS
Remote System IP: 4.4.4.130
Local Color: MPLS
Local Interface: GigabitEthernet2

SDWAN SESSION (IPSEC)
Remote Edge: RTP
Remote Color: PUBLIC_INTERNET
Remote System IP: 4.4.4.130
Local Color: PUBLIC_INTERNET
Local Interface: GigabitEthernet3

Path Decided By:

AAR policy
NAT

NAT Translate Source
Pre-NAT
Addr:192.168.1.10
Port:55618
Post-NAT
Addr:172.17.1.1
Port:5252

Final Path:

CoR SAAS
Local Color: PUBLIC_INTERNET
Local Interface: GigabitEthernet3

Downstream (From 40.99.8.194:443 to 192.168.1.10:55618)

Hop 0 – Edge Name: SJC-Branch

IP Lookup on VPN 0

Destination Addr:
172.17.1.1
Match Route:
172.17.1.1/32

Route Info
Source: connected
Preference: 0
Metric: 0
Received From:
Peer: 0.0.0.0
Uptime: 2w4d
Via: GigabitEthernet3;

Routing Candidate Paths: 1

LOCAL CONSUMED

Path Decided By:

NAT

NAT Translate Destination
Pre-NAT
Addr:172.17.1.1
Port:5252
Post-NAT
Addr:192.168.1.10
Port:55618

Final Path:

SERVICE LAN
Local Interface: GigabitEthernet4

Finally, you can confirm how the App-route policy is programmed. This information lets you validate that Microsoft Office 365 applications traffic flows through the link that is intended according to your Cisco Catalyst SD-WAN Cloud OnRamp for SaaS policy, which is a part of the App-route policy.

1. In the **All Trace** tab, go to the **Completed Flows** tab in the **Insight** area.

2. Expand any Microsoft Office 365 flow by clicking the right-arrow icon at the beginning of the row.

3. Scroll down to the **Insight – Advanced Views** area.

4. In the **Upstream Feature** tab:

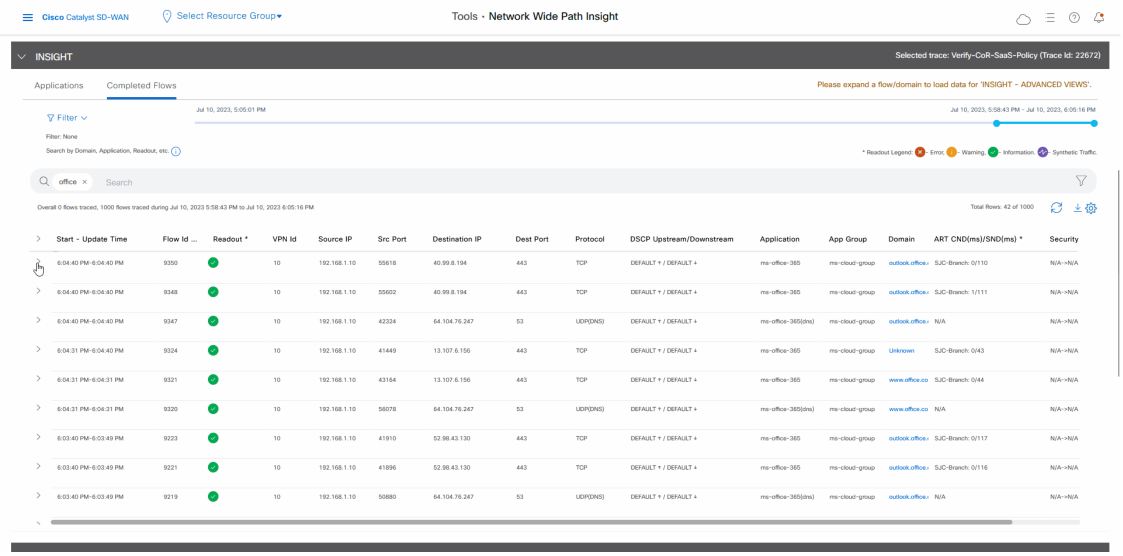
    a. Choose an event from the **Event List** drop-down list.

    b. Click **Expand All Features** to see detailed ingress and egress information about the features that are executed for the flow, then click **Collapse All Features**.

    c. In the **Ingress Feature** area, expand **SDWAN App Route Policy** to see policy information.

    d. Click **View Policy** next to **SDWAN App Route Policy** to see the policy programming.

Figure 6: Confirm the Programming of the App-Route Policy


Cisco Catalyst SD-WAN
Select Resource Group
Tools · Network Wide Path Insight
INSIGHT
Applications
Completed Flows
Filter
Search
* Readout Legend: ✕ - Error, ! - Warning, ✓ - Information. ∿ - Synthetic Traffic.

Selected trace: Verify-CoR-SaaS-Policy (Trace Id: 22672)

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Jul 10, 2023, 5:05:01 PM

Jul 10, 2023, 5:58:43 PM - Jul 10, 2023, 6:05:16 PM

Filter: None

Search by Domain, Application, Readout, etc.

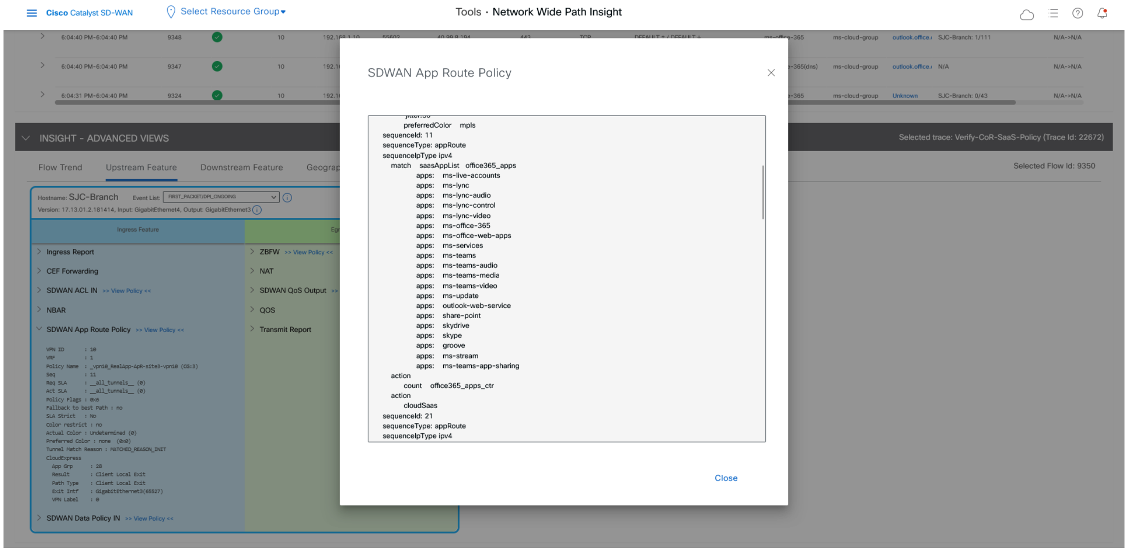
office ×

Overall 0 flows traced, 1000 flows traced during Jul 10, 2023 5:58:43 PM to Jul 10, 2023 6:05:16 PM

Total Rows: 42 of 1000

Start - Update Time	Flow Id ...	Readout *	VPN Id	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART CND(ms)/SND(ms) *	Security
6:04:40 PM-6:04:40 PM	9350	✓	10	192.168.1.10	55618	40.99.8.194	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.	SJC-Branch: 0/110	N/A->N/A
6:04:40 PM-6:04:40 PM	9348	✓	10	192.168.1.10	55602	40.99.8.194	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.	SJC-Branch: 1/111	N/A->N/A
6:04:40 PM-6:04:40 PM	9347	✓	10	192.168.1.10	42324	64.104.76.247	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365(dns)	ms-cloud-group	outlook.office.	N/A	N/A->N/A
6:04:31 PM-6:04:40 PM	9324	✓	10	192.168.1.10	41449	13.107.6.156	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	Unknown	SJC-Branch: 0/43	N/A->N/A
6:04:31 PM-6:04:31 PM	9321	✓	10	192.168.1.10	43164	13.107.6.156	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	www.office.co	SJC-Branch: 0/44	N/A->N/A
6:04:31 PM-6:04:31 PM	9320	✓	10	192.168.1.10	56078	64.104.76.247	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365(dns)	ms-cloud-group	www.office.co	N/A	N/A->N/A
6:03:40 PM-6:03:49 PM	9223	✓	10	192.168.1.10	41910	52.98.43.130	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.	SJC-Branch: 0/117	N/A->N/A
6:03:40 PM-6:03:49 PM	9221	✓	10	192.168.1.10	41896	52.98.43.130	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.	SJC-Branch: 0/116	N/A->N/A
6:03:40 PM-6:03:49 PM	9219	✓	10	192.168.1.10	50880	64.104.76.247	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365(dns)	ms-cloud-group	outlook.office.	N/A	N/A->N/A

Figure 7: Detailed Information about the App-Route Policy



Selected trace: Verify-CoR-SaaS-Policy (Trace Id: 22672)

Selected Flow Id: 9350

Hostname: SJC-Branch Event List: FIRST_PACKET/DPI_ONGOING

Version: 17.13.01.2.181414, Input: GigabitEthernet4, Output: GigabitEthernet3

```
VPN ID       : 10
VRF          : 1
Policy Name  : _vpn10_RealApp-ApR-site3-vpn10 (CG:3)
Seq          : 11
Req SLA      : __all_tunnels__ (0)
Act SLA      : __all_tunnels__ (0)
Policy Flags : 0x6
Fallback to best Path : no
SLA Strict   : No
Color restrict : no
Actual Color : Undetermined (0)
Preferred Color : none  (0x0)
Tunnel Match Reason : MATCHED_REASON_INIT
CloudExpress
  App Grp      : 28
  Result       : Client Local Exit
  Path Type    : Client Local Exit
  Exit Intf    : GigabitEthernet3(65527)
  VPN Label    : 0
```

SDWAN App Route Policy

```
        preferredColor   mpls
    sequenceId: 11
    sequenceType: appRoute
    sequenceIpType ipv4
      match   saasAppList   office365_apps
              apps:   ms-live-accounts
              apps:   ms-lync
              apps:   ms-lync-audio
              apps:   ms-lync-control
              apps:   ms-lync-video
              apps:   ms-office-365
              apps:   ms-office-web-apps
              apps:   ms-services
              apps:   ms-teams
              apps:   ms-teams-audio
              apps:   ms-teams-media
              apps:   ms-teams-video
              apps:   ms-update
              apps:   outlook-web-service
              apps:   share-point
              apps:   skydrive
              apps:   skype
              apps:   groove
              apps:   ms-stream
              apps:   ms-teams-app-sharing
      action
          count   office365_apps_ctr
      action
          cloudSaas
    sequenceId: 21
    sequenceType: appRoute
    sequenceIpType ipv4
```

Use Case 2: Troubleshoot Network Quality on a Website

Assume that your users have trouble accessing the Google website and experience slowness after they are able to access.

In this use case, you’ll see how to use network-wide path insight to determine the root cause of these issues.

To begin, perform the following actions to start a trace in the SJC branch:

1. From the Cisco Catalyst SD-WAN menu, choose, **Tools** > **Network Wide Path Insight**.
2. Click **New Trace**.

3. In the **Trace Name** field, enter a name for the trace.

   In this use case, we use the name **Troubleshooting-Google**.

4. Click **Start**.

Let the trace run for approximately 5 minutes so that it can collect data, then follow these steps to determine the root cause of the issue:

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Troubleshooting-Google** trace.

   A slide-in pane with detailed insight information appears. The **Overview** tab shows that 243 google-services flows are affected by local drop events and provides related detailed information for these flows.

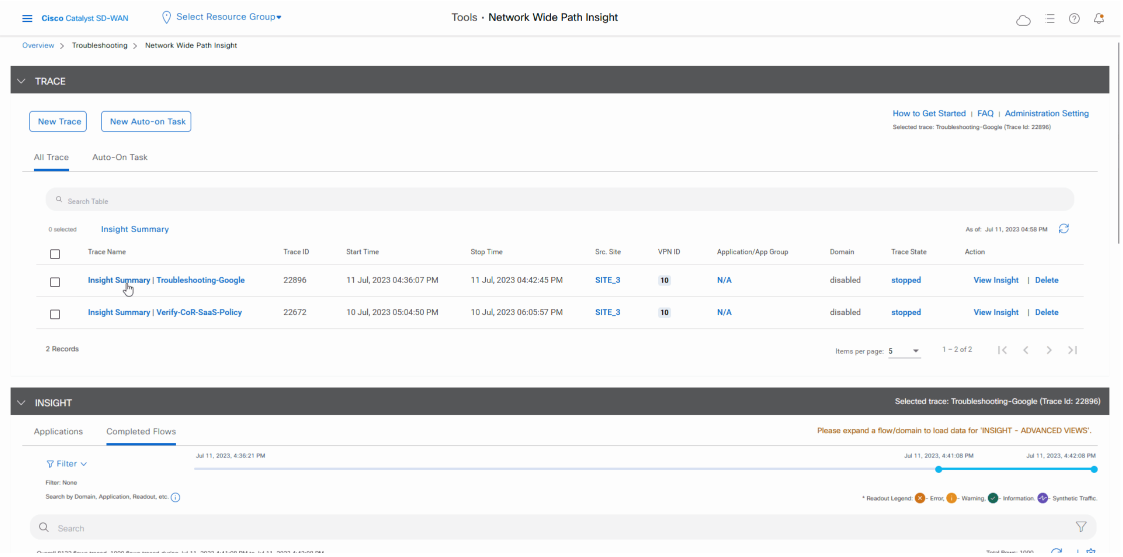
2. In the **Events** area, click the link under "impacted 243 google-services flows" to display the **Completed Flows** tab in the **Insight** area on the **All Trace** tab.

   Based on the link that you clicked, the table on the **Completed Flows** tab displays only information for google-services application flows that have a local drop event.

3. To see additional information for a particular flow, click the red X in the **Readout** column for the flow to display the **Flow Readout** slide-in pane.

   The **Overview** tab on the **Flow Readout** slide-in pane shows that the flow is affected by a local drop event and provides related detailed information.

Figure 8: View Insight and Readout Information for Flows



Selected trace: Troubleshooting-Google (Trace Id: 22896)

0 selected

As of: Jul 11, 2023 04:58 PM

	Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
□	Insight Summary | Troubleshooting-Google	22896	11 Jul, 2023 04:36:07 PM	11 Jul, 2023 04:42:45 PM	SITE_3	10	N/A	disabled	stopped	View Insight | Delete
□	Insight Summary | Verify-CoR-SaaS-Policy	22672	10 Jul, 2023 05:04:50 PM	10 Jul, 2023 06:05:57 PM	SITE_3	10	N/A	disabled	stopped	View Insight | Delete

2 Records

Items per page: 5

1 – 2 of 2

Selected trace: Troubleshooting-Google (Trace Id: 22896)

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Jul 11, 2023, 4:36:21 PM

Jul 11, 2023, 4:41:08 PM

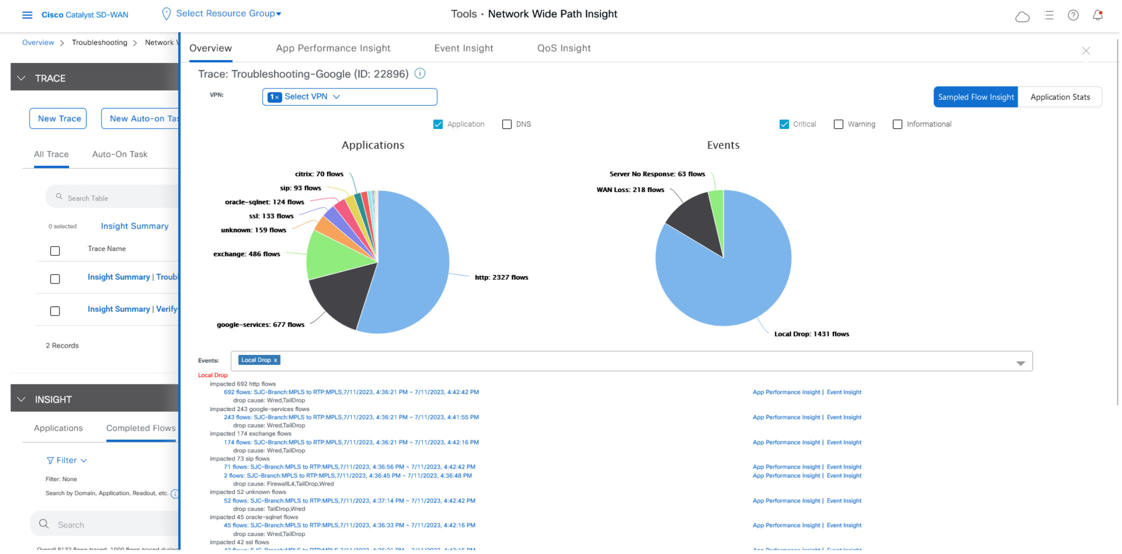
Jul 11, 2023, 4:42:08 PM

Filter: None

Search by Domain, Application, Readout, etc.

* Readout Legend: ✕ - Error, ! - Warning, ✓ - Information, ∿ - Synthetic Traffic.

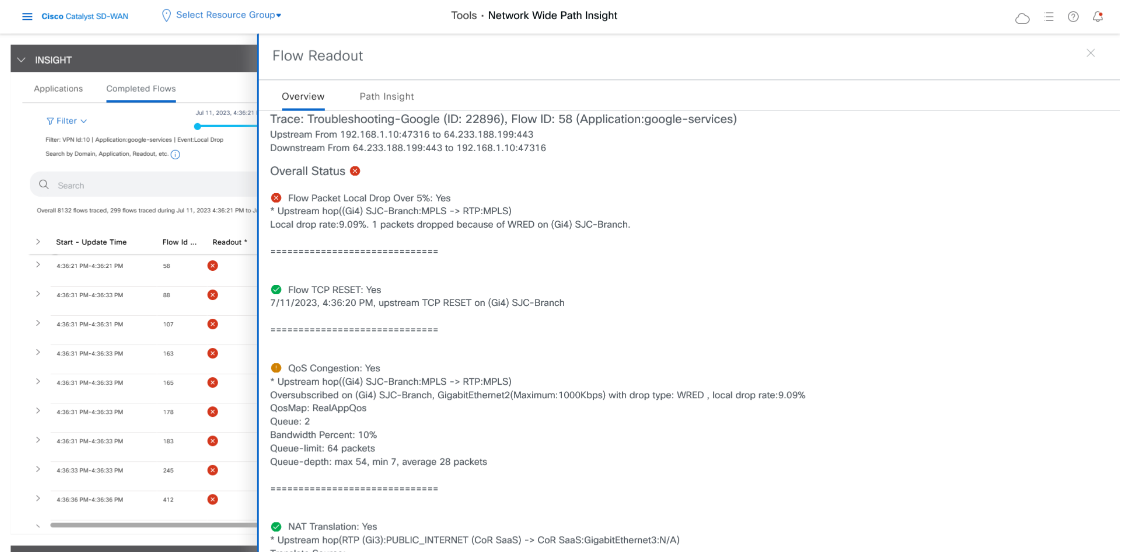
Figure 9: Flow Insight Information



Trace: Troubleshooting-Google (ID: 22896)

```
Local Drop
  impacted 692 http flows
    692 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:36:21 PM ~ 7/11/2023, 4:42:42 PM      App Performance Insight | Event Insight
      drop cause: Wred,TailDrop
  impacted 243 google-services flows
    243 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:36:21 PM ~ 7/11/2023, 4:41:55 PM      App Performance Insight | Event Insight
      drop cause: Wred,TailDrop
  impacted 174 exchange flows
    174 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:36:21 PM ~ 7/11/2023, 4:42:16 PM      App Performance Insight | Event Insight
      drop cause: Wred,TailDrop
  impacted 73 sip flows
    71 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:36:56 PM ~ 7/11/2023, 4:42:42 PM       App Performance Insight | Event Insight
    2 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:36:45 PM ~ 7/11/2023, 4:36:48 PM        App Performance Insight | Event Insight
      drop cause: FirewallL4,TailDrop,Wred
  impacted 52 unknown flows
    52 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:37:14 PM ~ 7/11/2023, 4:42:42 PM       App Performance Insight | Event Insight
      drop cause: TailDrop,Wred
  impacted 45 oracle-sqlnet flows
    45 flows: SJC-Branch:MPLS to RTP:MPLS,7/11/2023, 4:36:33 PM ~ 7/11/2023, 4:42:16 PM       App Performance Insight | Event Insight
      drop cause: Wred,TailDrop
  impacted 42 ssl flows
```

Figure 10: Flow Readout Information



Filter: VPN Id:10 | Application:google-services | Event:Local Drop

Overall 8132 flows traced, 299 flows traced during Jul 11, 2023 4:36:21 PM to J

Start - Update Time	Flow Id ...	Readout *
4:36:21 PM-4:36:21 PM	58	☒
4:36:31 PM-4:36:33 PM	88	☒
4:36:31 PM-4:36:31 PM	107	☒
4:36:31 PM-4:36:33 PM	163	☒
4:36:31 PM-4:36:33 PM	165	☒
4:36:31 PM-4:36:33 PM	178	☒
4:36:31 PM-4:36:33 PM	183	☒
4:36:33 PM-4:36:33 PM	245	☒
4:36:36 PM-4:36:36 PM	412	☒

```
Trace: Troubleshooting-Google (ID: 22896), Flow ID: 58 (Application:google-services)
Upstream From 192.168.1.10:47316 to 64.233.188.199:443
Downstream From 64.233.188.199:443 to 192.168.1.10:47316

Overall Status ☒

☒ Flow Packet Local Drop Over 5%: Yes
* Upstream hop((Gi4) SJC-Branch:MPLS -> RTP:MPLS)
Local drop rate:9.09%. 1 packets dropped because of WRED on (Gi4) SJC-Branch.

=============================

✓ Flow TCP RESET: Yes
7/11/2023, 4:36:20 PM, upstream TCP RESET on (Gi4) SJC-Branch

=============================

! QoS Congestion: Yes
* Upstream hop((Gi4) SJC-Branch:MPLS -> RTP:MPLS)
Oversubscribed on (Gi4) SJC-Branch, GigabitEthernet2(Maximum:1000Kbps) with drop type: WRED , local drop rate:9.09%
QosMap: RealAppQos
Queue: 2
Bandwidth Percent: 10%
Queue-limit: 64 packets
Queue-depth: max 54, min 7, average 28 packets

=============================

✓ NAT Translation: Yes
* Upstream hop(RTP (Gi3):PUBLIC_INTERNET (CoR SaaS) -> CoR SaaS:GigabitEthernet3:N/A)
```

You've now determined that the issue is related to local drop events. These events occur due to packets that are dropped because of network congestion, and they affect the quality of traffic flows on your network. Next, you can use network-wide path insight to answer the following questions that relate to QoS:

- Which queue is google-services traffic sent to?
- What applications besides google-services are consuming the bandwidth on this queue?

With the answers to these questions, you can take steps to reduce the congestion on the queue.

1. In the list of traces in the **All Trace** tab, click **Insight Summary** in the row that shows the **Troubleshooting-Google** trace.

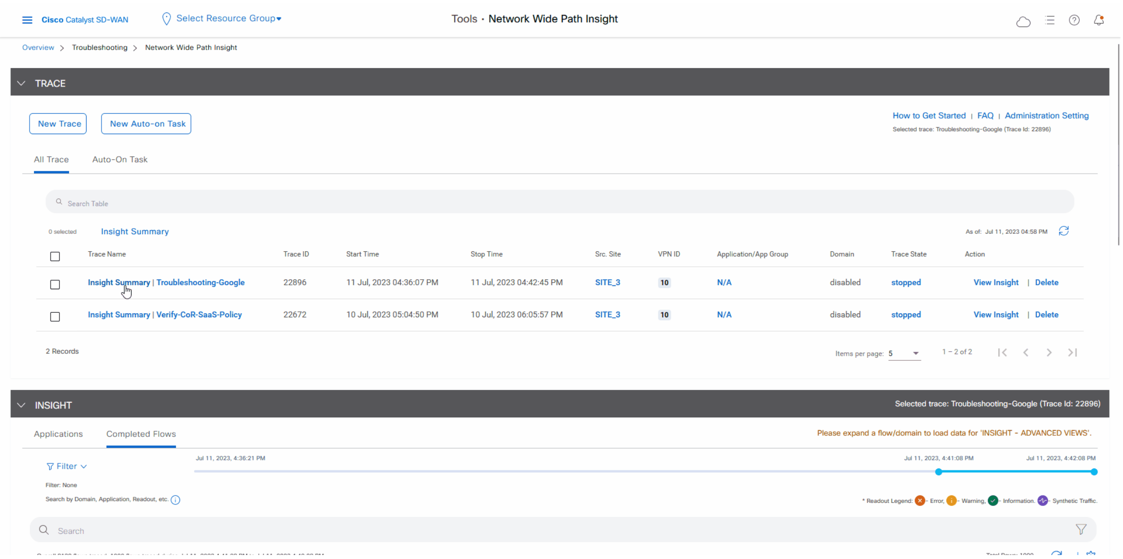
2. In the **Insight Summary** slide-in pane, choose the **QoS Insight** tab.
3. In the **Applications** field, choose all applications to see which applications are consuming bandwidth on which queue, then choose the **google-services** application to see which queue is used by this application.

   You can see that Google applications use queue 2, but many other applications also use this queue. These applications using the same queue are causing congestion.

Using the information that you found, you can reduce congestion and address the issues that your users experience when they visit the Google website by performing any of the following actions:

- Adjust the QoS policy for the queue,
- Move the Google application to another queue
- Move other applications to another queue

Figure 11: View QoS Information



Selected trace: Troubleshooting-Google (Trace Id: 22896)

As of: Jul 11, 2023 04:58 PM

□	Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
□	Insight Summary | Troubleshooting-Google	22896	11 Jul, 2023 04:36:07 PM	11 Jul, 2023 04:42:45 PM	SITE_3	10	N/A	disabled	stopped	View Insight | Delete
□	Insight Summary | Verify-CoR-SaaS-Policy	22672	10 Jul, 2023 05:04:50 PM	10 Jul, 2023 06:05:57 PM	SITE_3	10	N/A	disabled	stopped	View Insight | Delete

2 Records

Selected trace: Troubleshooting-Google (Trace Id: 22896)

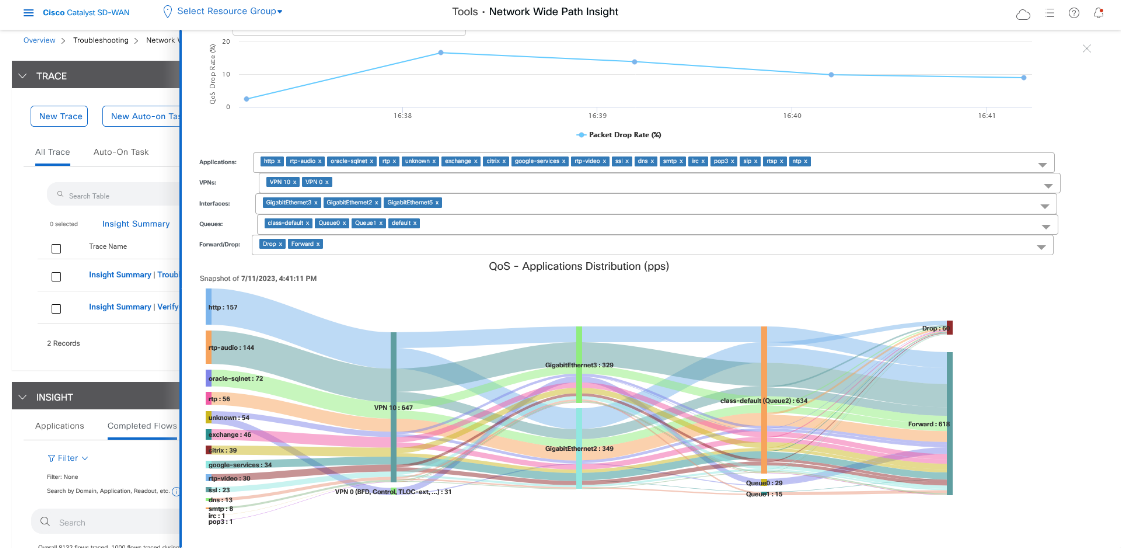
Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Filter: None

Search by Domain, Application, Readout, etc.

* Readout Legend: ✕- Error, i- Warning, ✓- Information. ∿- Synthetic Traffic.

Figure 12: QoS Information for All Applications



Applications: http x rtp-audio x oracle-sqlnet x rtp x unknown x exchange x citrix x google-services x rtp-video x ssl x dns x smtp x irc x pop3 x sip x rtsp x ntp x

VPNs: VPN 10 x VPN 0 x

Interfaces: GigabitEthernet3 x GigabitEthernet2 x GigabitEthernet5 x

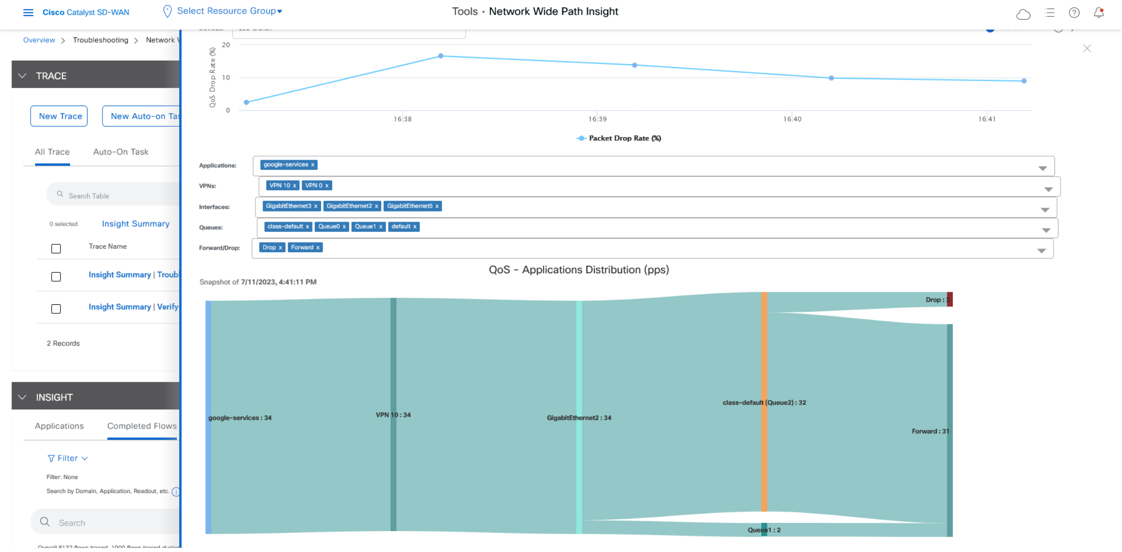
Queues: class-default x Queue0 x Queue1 x default x

Forward/Drop: Drop x Forward x

QoS - Applications Distribution (pps)

Snapshot of 7/11/2023, 4:41:11 PM

Figure 13: QoS Information for the google-services Application



Applications: google-services x

VPNs: VPN 10 x VPN 0 x

Interfaces: GigabitEthernet3 x GigabitEthernet2 x GigabitEthernet5 x

Queues: class-default x Queue0 x Queue1 x default x

Forward/Drop: Drop x Forward x

QoS - Applications Distribution (pps)

Snapshot of 7/11/2023, 4:41:11 PM