Flexible NetFlow Application Visibility on SD-Routing Devices

This chapter includes information on how to configure Flexible NetFlow Application Visibility on SD-Routing devices. It contains the following sections:

Information About Flexible Netflow Application Visibility

The Flexible NetFlow (FNF) provides statistics on packets flowing through the device. The FNF on WAN or LAN interfaces provide visibility for all the traffic (both ingress and egress) hitting the WAN or LAN interfaces on Cisco SD-Routing devices by using the Application Intelligence Engine (SAIE). The Application Intelligence Engine flow provides the ability to look into the packet past the basic header information. The SAIE flow determines the contents of a particular packet, and then either records that information for statistical purposes or performs an action on the packet.

Note You can apply FNF only on WAN or LAN interfaces. You should not apply on both WAN and LAN interfaces.

To enable t he Flexible Netflow Application Visibility on the device, you must enable the flow data aggregation using Cisco SD-WAN Manager in the following ways:

- Performance monitor context profile (recommended method)

- Flow exporter to local controller

Note	If you have a existed FNF monitors, to avoid performance impact by adding a new performance monitor, add the flow exporter to local controller as flow exporter of existed FNF monitor. Otherwise, you can use the performance monitor context profile.

Prerequisites for Flexible NetFlow Application Visibility with SAIE Flows

The following are the prerequisites:

- Ensure that the device run the Cisco IOS XE 17.13.1 image.

- Ensure that you enable flow data aggregation in Cisco SD-WAN Manager.

Limitations

The following are the limitations:

- Only Aggregated statistics by Cisco SD-WAN Application Intelligence Engine (SAIE) is suppotted.

- On-demand troubleshooting is not supported.

- If context profile and FNF exporter uses the same name, the **show flow exporter name** command will display only one of them.

- The performance monitor context profile and flow exporter to local controller can only use either the context profile or flow exporter to local controller. Otherwise, it will dobule count the packets.

- Only CLI based configuration group is supported.

Enabling Flexible NetFlow Application Visibility

You can enahle the FNF Application Visibility either using the context profile or flow exporter on the device.

Configuring Context Profile Option-1

It is recommended to use this option. This example shows how to enable flow data aggregation using Context Profile on the device:

```
performance monitor context FNF profile app-visibility
 exporter destination local-controller source Null0
 traffic-monitor app-visibility-stats

interface GigabitEthernet5
 performance monitor context FNF
```

Device will apply this profile to FNF flow monitor when it is attached to an interface.

Configuring Flow Exporter Option-2

This example shows how to enable flow data aggregation using Flow Exporter on the device:

```
flow exporter fnf-1
 destination local controller
 export-protocol ipfix
 template data timeout 300
 option interface-table timeout 300
 option vrf-table timeout 300
 option application-table timeout 300
 option application-attributes timeout 300

flow record fnf-app-visiblility
 match routing vrf input
 match interface input
 match interface output
 match application name
 collect counter bytes long
 collect counter packets long

flow monitor fnf-app-visiblility
 exporter fnf-1
 cache timeout inactive 10
 cache timeout active 60
 cache entries 5000
 record fnf-app-visiblility

interface GigabitEthernet5
 ip flow monitor fnf-app-visiblility input
 ip flow monitor fnf-app-visiblility output
 ipv6 flow monitor fnf-app-visiblility input
 ipv6 flow monitor fnf-app-visiblility output
```

Configuring Flexible NetFlow Application Visibility

To configure FNF Application Visibility, on the SD-Routing device, perform these steps:

Procedure

Step 1	From Cisco IOS XE Catalyst SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Add CLI based Configuration Group** .
Step 2	In the **Add CLI configuration Group** pop-up dialog box, enter the configuration group name.
Step 3	Click the **Solution Type** drop-down list and select the solution type as **sd-routing** for the SD-Routing devices.
Step 4	In the **Description** field, enter a description for the feature
Step 5	Click **Next**
	The new configuration group page is displayed with the Feature Profiles and Associated Device tabs.
Step 6	In the **Feature Profiles** section, add the corresponding configuration.
Step 7	Click **Save** to save the configuration.
Step 8	Click (**…**) adjacent to the configuration group name and choose **Edit**
Step 9	Click **Associated Devices**.
Step 10	Choose one or more devices, and then click **Deploy**

Note   Flexible Netflow does not support performance monitor context profile and flow monitor change when the performance monitor context profile and flow monitor are attached to an interface.

Step 11   Click **Configuration** > **Configuration Groups** > **Deploy**

Step 12   Click **(…)** adjacent to the configuration group name and choose **Edit** to modify performance monitor context profile and flow monitor and re-attach it to the interface.

Step 13   Click **Deploy**.

Step 14   Click **Save**.

Verifying Flexible NetFlow Application Visibility Using Cisco SD-WAN Manager

To verify the FNF Application Visibility, perform the following steps:

Procedure

Step 1   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select a SD-Routing device from the list.

Step 2   In the left pane, choose **SAIE Applications**> **Fliter**.

Step 3   In the **Filter By** dialog box, select the VPN.

Step 4   For the Traffic Source, check either the **LAN** or **Remote Access** check box.

Step 5   Click **Search** to search the flow records based on the selected filters.

The flow records are displayed.

Step 6   Click **Export** to export the flow records to your local system.

Step 7   Click **Reset All** to reset all the search filters.

Verifying Flexible NetFlow Application Visibility

To check the basic network metrics that are used to calculate the the SD-Routing FNF application visibility, use the **show performance monitor context** [profile name] **configuration**, **show platform sofware td-l database content dta fnf-statistics**, and **show performance monitor context fnf traffic monitoring app-visibility-stats cache** commands.

```
Device #show performance monitor context fnf configuration
!===============================================================================
! Equivalent Configuration of Context fnf !
!===============================================================================
!Exporters
!=========
!
flow exporter fnf-1
description performance monitor context fnf exporter
destination local controller
export-protocol ipfix
```

```
template data timeout 300
option interface-table timeout 300 export-spread 0
option vrf-table timeout 300 export-spread 0
option application-table timeout 300 export-spread 0
option application-attributes timeout 300 export-spread 0
!
!Access Lists
!=============
!Class-maps
!===========
!Samplers
!=========
!Records and Monitors
!====================
!
flow record fnf-app-visiblility-v4
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visiblility-v4
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visiblility-v4
!
!
flow record fnf-app-visiblility-v6
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visiblility-v6
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visibility-v6
!
!Interface Attachments
!======================
interface GigabitEthernet5
ip flow monitor fnf-app-visiblility-v4 input
ip flow monitor fnf-app-visiblility-v4 output
ipv6 flow monitor fnf-app-visiblility-v6 input
ipv6 flow monitor fnf-app-visiblility-v6 output

Device# show performance context fnf traffic-monitor app-visibility stats cache
Monitor fnf-app-visibility-v4

Cache  type:                      Normal (platform cache)
Cache  size :                           10000
```

```
Current entries:                          2
High Watermark:                           4

Flows added:                              6
Flows aged:                               4
 - Inactive timeout          (10sec)      4

IP VRF   ID INPUT   INFE INPUT   INTF OUTPUT   APP Name            bytese long    pkts long
======   =======    =========    ===========   ================    ===========    ==========
1         (1)        Gi3          Gi5          layer7 share-point   1517476         3277
1         (1)        Gi5          Gi3          layer7 share-point   1306568         3463
```

Feature Information for Flexible NetFlow Application Visibility on SD-Routing Devices

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for Flexible NetFlow Application Visibility on SD-Routing Devices

Feature Name	Releases	Feature Information
Flexible NetFlow Application Visibility on SD-Routing Devices	Cisco IOS XE Release 17.13.1a	The Flexible NetFlow (FNF) feature provides statistics on packets flowing through the device and helps to identify the tunnel or service VPNs. Also, it provides visibility for all the traffic that passes through the VPN0 on Cisco SD-Routing devices by using the SD-Routing Application Intelligence Engine (SAIE).