Flow Level Flexible NetFlow Support for SD-Routing Devices

This chapter includes information on how to configure Flow Level Flexible NetFlow Support for SD-Routing devices. It contains the following sections:

- Information on Flow Level Flexible NetFlow, on page 1
- Types of Flexible NetFlow Monitoring for SD-Routing Devices, on page 2
- Benefits of Flow-level Flexible NetFlow, on page 2
- Flow-level Flexible NetFlow Components, on page 2
- Ways to Enable Flexible NetFlow Monitors on SD-Routing Devices, on page 3
- Prerequisites to Configure Flow-level Flexible NetFlow, on page 3
- Limitations to Configure Flow-level Flexible NetFlow, on page 3
- Configure Flow-level FNF on an SD-Routing Device using EzPM Profile, on page 4
- Configure Flow-level Flexible NetFlow using a Flow Monitor, on page 4
- Information on Security Unified Logging , on page 6
- Limitations to Configure Security Unified Logging on a Device, on page 6
- Configure Security Unified Logging on an SD-Routing Device using an EzPM Profile, on page 6
- Configure Security Unified Logging on an SD-Routing Device using Flow Monitor, on page 7
- Enable Flow-level Flexible NetFlow for SD-Routing Devices, on page 9

Information on Flow Level Flexible NetFlow

Flexible NetFlow is an advancement on the original NetFlow that adds the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

The Security Unified Logging (SUL) profile acts as a superset containing all the information present in an application-level and a flow-level profile.

If you do not require detailed flow-level statistics, you can use Application Visibility for your FNF monitors. Alternatively, you can enable the flow-level FNF monitor to view all the data that is captured including application-level statistics.

By enabling flow-level visibility monitor on either the LAN interface or WAN interface, you can avoid double packet counts. This prevents data redundancy which is caused by ingress and egress data traffic flow from LAN to WAN.

The IPv4 and the IPv6 protocols are enabled by default after the performance monitor context is attached to an interface. But, you can choose to enable either IPv4 or IPv6 protocols by configuring the performance monitoring context.

Types of Flexible NetFlow Monitoring for SD-Routing Devices

SD-Routing supports three types of FNF monitoring methods:

- Aggregated NetFlow Application Visibility
- Flow-level FNF
- Security Unified Logging (SUL)

Benefits of Flow-level Flexible NetFlow

Following are the benefits if you enable Flow-level FNF:

- Flow-level FNF provides statistics at a granular level.
- Flow-level FNF statistics are used in Cisco Catalyst SD-WAN Analytics and SD-WAN monitoring for On-demand troubleshooting.

Flow-level Flexible NetFlow Components

Flexible NetFlow consists of components that can be used together in several variations to perform data export and traffic analysis. The user-defined flow records and the component structure of Flexible NetFlow facilitates the creation of various configurations for exporting the data and analysing traffic on a networking device with a minimum number of configuration commands.

Each flow monitor can have a unique combination of flow record, flow exporter, and cache type. If you change a parameter such as the destination IP address for a flow exporter, it is automatically changed for all the flow monitors that use the flow exporter. The following sections provide more information on Flexible NetFlow components:

- **Flow Records**

  In Flexible NetFlow a combination of key and nonkey fields is called a record. Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data.

- **Flow Exporters**

  Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

- **Flow Monitors**

Flow monitors are the Flexible NetFlow components which are applied to interfaces to perform network traffic monitoring.

Flow monitors consist of a user-defined record, an optional flow exporter, and a cache that is automatically created at the time the flow monitor is applied to the first interface.

Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and nonkey fields in the flow record.

Ways to Enable Flexible NetFlow Monitors on SD-Routing Devices

There are two ways to enable Flow-level FNF:

- **Using an EzPM Profile**: This is a simple recommended way where you can use the existing profiles to configure flow records. By using EzPM profile, you can configure Application-visibility, Flow-level visibility, and SUL monitors.
- **Using a Flow Monitor**: This is a manual process where flow records are created and exported to a Local Exporter for Application-visibility, Flow-level visibility, and SUL.

Prerequisites to Configure Flow-level Flexible NetFlow

You need to enable license boot-level advantage on the Cisco router. This gives you the network advantage to use EzPM profile CLI support.

Limitations to Configure Flow-level Flexible NetFlow

Following are the limitations on configuring flow-level FNF:

- Flow-level configuration for SD-Routing devices is possible on the Cisco SD-WAN Manager through CLI based configuration groups, CLI templates, or CLI Add-on profiles.
- Application-level and Flow-level visibility monitors both ingress and egress data on the target interface. If configured on both service and transport interface, the packet for the same flow is counted twice.
- Customizing flow monitors with partial flow-level record fields is not allowed. If partial flow-level record fields are added to monitors, PSV data is not generated.
- You can configure either application-visibility, flow-level, or the SUL profile on one interface. You can attach only one type of EzPM profile to an interface.

Configure Flow-level FNF on an SD-Routing Device using EzPM Profile

To enable Flow-level FNF monitoring, you can use the default Easy Performance Monitor (EzPM) profile. You can read more about EzPM here.

Flow-level visibility contains both application-level statistics and flow-level statistics. This eliminates the need to enable application-level visibility for your FNF monitors.

Step 1 Create an EzPM profile.

```
Device# configure terminal
Device(config)# performance monitor context context_name profile flow-level-visibility
Device(config-perf-mon)# exporter destination local-controller source Null0
Device(config-perf-mon)# traffic-monitor flow-level-visibility-stats
Device(config-perf-mon)# end

Device# configure terminal
Device(config)# interface interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

Step 2 Apply performance monitor context to the interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

Configure Flow-level Flexible NetFlow using a Flow Monitor

To configure flow-level FNF using a flow monitor, perform the following steps:

Step 1 Create a FNF flow exporter to configure flow records.

```
Device# configure terminal
Device(config)# flow exporter exporter-name
Device(config-flow-exporter)# destination local controller
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout seconds
Device(config-flow-exporter)# option interface-table
Device(config-flow-exporter)# option vrf-table
Device(config-flow-exporter)# option application-table
Device(config-flow-exporter)# option application-attributes
Device(config-flow-exporter)# exit
```

Step 2 Create a flow record for the flow-level view for IPv4 traffic.

```
Device# configure terminal
Device(config)# flow record flow_level_visibility_ipv4
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect ipv4 dscp
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# end
```

Step 3 Create a flow record for the flow-level view for IPv6 traffic.

```
Device# configure terminal
Device(config)# flow record flow_level_visibility_ipv6
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv6 destination address
Device(config-flow-record)# match ipv6 protocol
Device(config-flow-record)# match ipv6 source address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect ipv6 dscp
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# end
```

Step 4 Enable a flow monitor to perform network traffic flow-level visibility for IPv4 traffic.

```
Device# configure terminal
Device(config)# flow monitor fnf-flow-level-visiblility-v4
Device(config-flow-monitor)# exporter fnf-1
Device(config-flow-monitor)# record flow_level_visibility_ipv4
Device(config-flow-monitor)# end
```

Step 5 Enable a flow monitor to perform network traffic flow-level visibility for IPv6 traffic.

```
Device# configure terminal
Device(config)# flow monitor fnf-flow-level-visiblility-v6
Device(config-flow-monitor)# exporter fnf-1
Device(config-flow-monitor)# record flow_level_visibility_ipv6
Device(config-flow-monitor)# end
```

Step 6 Apply the flow monitor to the interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet1
Device(config-if)# ip flow monitor fnf-flow-level-visiblility-v4 input
Device(config-if)# ip flow monitor fnf-flow-level-visiblility-v4 output
Device(config-if)# ipv6 flow monitor fnf-flow-level-visiblility-v6 input
Device(config-if)# ipv6 flow monitor fnf-flow-level-visiblility-v6 output
Device(config-if)# end
```

What to do next

Monitor Flow-level Data on the SD-Routing Device

Information on Security Unified Logging

Security Unified Logging allows you to have visibility into the log data for Zone-based Firewall and for Unified Threat Defense features such as IPS, URL-F and AMP. These features help you to understand what traffic, threats, sites or malware were blocked, and the rules that blocked the traffic or sessions with the associated port, protocol, or applications.

SUL profiles have all the flow-level fields in it, so you do not need to attach flow-level visibility to an interface if the SUL profile is already attached to it. SUL supports both IPv4 and IPv6 protocols.

Limitations to Configure Security Unified Logging on a Device

Following are the limitations to configure SUL on a device:

- The SUL profile should not be configured if other FNF profiles are configured, such as application-visibility (aggregate FNF) or flow-visibility. These three profiles should be mutually exclusive to avoid data redundancy.
- Customizing flow monitors with partial SUL record fields is not allowed. If partial SUL record fields are added to monitors, PSV data is not generated.
- Due to a design limitation, by default, SUL needs to be applied to both LAN and WAN interface since SUL monitor only collects the output direction.

Configure Security Unified Logging on an SD-Routing Device using an EzPM Profile

There are two ways defined below to configure SUL on an SD-Routing device.

Step 1 Configure an EzPM profile.

```
Device# configure terminal
Device(config)# performance monitor context context_name profile security-unified-logging
Device(config-perf-mon)# exporter destination local-controller source Null0
Device(config-perf-mon)# traffic-monitor sul-fnf-config
Device(config-perf-mon)# end
```

Step 2 Apply the performance monitor context to the interface.

```
Device# configure terminal
Device(config)# interface interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

What to do next

Monitor Security Unified Logging Data on the SD-Routing Device

Configure Security Unified Logging on an SD-Routing Device using Flow Monitor

To configure SUL using a flow monitor, perform the following steps:

SUMMARY STEPS

1. Create a flow exporter for SUL.
2. Configure the flow records.
3. Enable a flow monitor for SUL.
4. Apply the flow monitor to the interface.

DETAILED STEPS

Step 1 Create a flow exporter for SUL.

```
Device# configure terminal
Device(config)# flow exporter sul-1
Device(config-flow-exporter)# destination local controller
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# option interface-table
Device(config-flow-exporter)# option vrf-table
Device(config-flow-exporter)# option application-table
Device(config-flow-exporter)# option utd-category-table
Device(config-flow-exporter)# option utd-file-type-table
Device(config-flow-exporter)# option application-attributes
Device(config-flow-exporter)# option c3pl-class-table
Device(config-flow-exporter)# option c3pl-policy-table
Device(config-flow-exporter)# option fw-zone-pair-table
Device(config-flow-exporter)# option fw-zone-table
Device(config-flow-exporter)# option fw-proto-table
Device(config-flow-exporter)# option utd-drop-reason-table
```

```
Device(config-flow-exporter)# option sdvt-drop-reason-table
Device(config-flow-exporter)# exit
```

Step 2 Configure the flow records.

```
Device# configure terminal
Device(config)# flow record sul-sul-monitor-v4
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect ipv4 dscp
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect ulogging fw-zp-id
Device(config-flow-record)# collect ulogging fw-zone-id-array
Device(config-flow-record)# collect ulogging fw-class-id
Device(config-flow-record)# collect ulogging fw-policy-id
Device(config-flow-record)# collect ulogging fw-proto-id
Device(config-flow-record)# collect ulogging fw-action
Device(config-flow-record)# collect ulogging fw-src-ipv4-addr-translated
Device(config-flow-record)# collect ulogging fw-dst-ipv4-addr-translated
Device(config-flow-record)# collect ulogging fw-src-port-translated
Device(config-flow-record)# collect ulogging fw-dst-port-translated
Device(config-flow-record)# collect ulogging utd-ips-pri
Device(config-flow-record)# collect ulogging utd-ips-sid
Device(config-flow-record)# collect ulogging utd-ips-gid
Device(config-flow-record)# collect ulogging utd-ips-cid
Device(config-flow-record)# collect ulogging utd-urlf-url-hash
Device(config-flow-record)# collect ulogging utd-urlf-url-category
Device(config-flow-record)# collect ulogging utd-urlf-url-reputation
Device(config-flow-record)# collect ulogging utd-urlf-app-name
Device(config-flow-record)# collect ulogging utd-amp-dispos
Device(config-flow-record)# collect ulogging utd-amp-filename-hash
Device(config-flow-record)# collect ulogging utd-amp-file-type
Device(config-flow-record)# collect ulogging utd-amp-file-hash
Device(config-flow-record)# collect ulogging utd-amp-malname-hash
Device(config-flow-record)# collect ulogging utd-drop-reason-id
Device(config-flow-record)# collect ulogging sdvt-drop-reason-id
Device(config-flow-record)# collect ulogging utd-ips-policy-id
Device(config-flow-record)# collect ulogging utd-ips-action-id
Device(config-flow-record)# collect ulogging utd-urlf-policy-id
Device(config-flow-record)# collect ulogging utd-urlf-action-id
Device(config-flow-record)# collect ulogging utd-amp-policy-id
Device(config-flow-record)# collect ulogging utd-amp-action-id
Device(config-flow-record)# collect ulogging utd-urlf-reason-id
Device(config-flow-record)# collect ulogging flow-direction
Device(config-flow-record)# collect ulogging fw-user-name
Device(config-flow-record)# collect ulogging fw-src-ipv6-addr-translated
```

```
Device(config-flow-record)# collect ulogging fw-dst-ipv6-addr-translated
Device(config-flow-record)# end
```

Step 3 Enable a flow monitor for SUL.

```
Device# configure terminal
Device(config)# flow monitor sul-sul-monitor-v4
Device(config-flow- monitor)# exporter sul-1
Device(config-flow- monitor)# record sul-sul-monitor-v4
Device(config-flow- monitor)# end
```

Step 4 Apply the flow monitor to the interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet1
Device(config-if)# ip flow monitor sul-sul-monitor-v4 output
Device(config-if)# end
```

What to do next

Monitor Security Unified Logging Data on the SD-Routing Device

Enable Flow-level Flexible NetFlow for SD-Routing Devices

To enable flow-level FNF using Cisco SD-WAN manager, begin with creating a configuration group followed by the steps provided below.

Create a Configuration Group

To create a configuration group, perform the following steps:

Step 1 From Cisco Catalyst SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** and select the solution as **SD-Routing** from the **Solution** drop-down list.

Step 2 Click **Create Configuration Group** and in the dialog box, enter a name and description, select the CLI Configuration Group and click **Create**.

Step 3 From the **Load Running Config from Reachable Device** drop-down list, select the device.

Step 4 Once the CLI has loaded into the Config Preview section, click **Save**.

Associate a Device and Deploy the Configuration Group

To associate and deploy the configurations of the device, perform the following steps:

Step 1 Click **(…)** adjacent to the configuration group name and choose **Edit**.

Step 2 In the **Deployment** pane, click **Add**and select the device to be associated.

Step 3 Choose one or more devices, and then click **Deploy**.

Step 4 Click **Save**.

Monitor Flow-level Data on the SD-Routing Device

To view and monitor the flow-level information like destination IP, destination port, the source IP of a device, perform the following steps:

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

Step 2 From the left pane, choose **SAIE Applications** > **Filter**.

Step 3 In the **Filter By** dialog box, select the VPN and click **Search** to search the flow records based on the selected filters.

Step 4 Click **Export** to export the flow records to your local system.

Monitor Security Unified Logging Data on the SD-Routing Device

To monitor the SUL data on the device, perform the following steps:

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

Step 2 From the left pane, choose **Connection Events** > **Filter**.

Step 3 In the **Filter By** dialog box, select the VPN and click **Search** to search the flow records based on the selected filters.