Customizing Flexible NetFlow Flow Records and Flow Monitors

Last Updated: October 12, 2012

This document contains information about and instructions for customizing Cisco IOS Flexible NetFlow flow records and flow monitors. If the tasks and configuration examples in the "Getting Started with Configuring Cisco IOS Flexible NetFlow" module and the "Configuring Cisco IOS Flexible NetFlow with Predefined Records" module were not suitable for your traffic analysis requirements, you can use the information and instructions in this document to customize Flexible NetFlow to meet your traffic analysis requirements.

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to support network and security monitoring, network planning, traffic analysis, and IP accounting.

Flexible NetFlow improves on original NetFlow by adding 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Customizing Flexible NetFlow Flow Records and Flow Monitors

- You are familiar with the information in the " Cisco IOS Flexible NetFlow Overview " module.
- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands in the *Cisco IOS Flexible NetFlow Command Reference* :
  - **match flow**
  - **match interface**
  - **match** {**ipv4** | **ipv6**}
  - **match routing**
  - **match transpor**t
- You are familiar with the Flexible NetFlow nonkey fields as they are defined in the following commands in the *Cisco IOS Flexible NetFlow Command Reference* :
  - **collect counter**
  - **collect flow**
  - **collect interface**
  - **collect**{**ipv4** | **ipv6**}
  - **collect routing**
  - **collect timestamp sys-uptime**
  - **collect transport**
- The networking device must be running a Cisco IOS release that supports Flexible NetFlow.

IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding or distributed Cisco Express Forwarding.

IPv6 Traffic

- The networking device must be configured for IPv6 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 or distributed Cisco Express Forwarding.

Information About Customizing Flexible NetFlow Flow Records and Flow Monitors

Criteria for Identifying Traffic To Be Used in Analysis in Flexible NetFlow

If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a user-defined (custom) record using the Flexible NetFlow **collect** and **match** commands. Before you can

create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields.

If you want to create a customized record for detecting network attacks, you must include the appropriate key and nonkey fields in the record to ensure that the router creates the flows and captures the data that you need to analyze the attack and respond to it. For example, SYN flood attacks are a common denial of service (DoS) attack in which TCP flags are used to flood open TCP requests to a destination host. When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake." While the destination host waits for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly because the ACK is expected to arrive a few milliseconds after the SYN ACK. The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Because the SYN ACK is destined for an incorrect or nonexistent host, the last part of the TCP three-way handshake is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. Rapid generation by the source of TCP SYN packets from random IP addresses can fill the connection queue and cause denial of TCP services (such as e-mail, file transfer, or WWW) to legitimate users.

The information needed for a security monitoring record for this type of DoS attack might include the following key and nonkey fields:

- Key fields:
  - Destination IP address or destination IP subnet
  - TCP flags
  - Packet count
- Nonkey fields
  - Destination IP address
  - Source IP address
  - Interface input and output

Tip Many users configure a general Flexible NetFlow monitor that triggers a more detailed Flexible NetFlow view of a DoS attack using these key and nonkey fields.

How to Customize Flexible NetFlow Flow Records and Flow Monitors

Note Only the keywords and arguments required for the Flexible NetFlow commands used in these tasks are explained in these tasks. For information about the other keywords and arguments available for these Flexible NetFlow commands, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

- Configuring a Customized Flow Record, page 4

Configuring a Customized Flow Record

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task explains the steps that are used to create one of the possible permutations. Modify the steps in these tasks as appropriate to create a customized flow record for your requirements.

To configure a customized flow record, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {**ipv4** | **ipv6**}{**destination** | **source**} {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **collect** {**ipv4** | **ipv6**} **source** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
8. Repeat Step 7 as required to configure additional nonkey fields for the record.
9. **end**
10. **show flow record** *record-name*
11. **show running-config flow record** *record-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**flow record** *record-name* **Example:** `Device(config)# flow record FLOW-RECORD-1`	Creates a flow record and enters Flexible NetFlow flow record configuration mode. • This command also allows you to modify an existing flow record.
Step 4	**description** *description* **Example:** `Device(config-flow-record)# description Used for basic traffic analysis`	(Optional) Creates a description for the flow record.
Step 5	**match** {**ipv4** | **ipv6**}{**destination** | **source**} {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]} **Example:** `Device(config-flow-record)# match ipv4 destination address`	Configures a key field for the flow record. **Note** This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the **match ipv4** command, and the other **match** commands that are available to configure key fields, refer to the *Cisco IOS Flexible NetFlow Command Reference* .
Step 6	Repeat Step 5 as required to configure additional key fields for the record.	--
Step 7	**collect** {**ipv4** | **ipv6**} **source** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]} **Example:** `Device(config-flow-record)# collect ipv4 source address`	Configures one or more of the IPv4 source fields in the flow as a nonkey field for the record. **Note** This example configures the IPv4 source address as a nonkey field for the record. For information on the other **collect** commands that are available to configure nonkey fields, refer to the *Cisco IOS Flexible NetFlow Command Reference* .
Step 8	Repeat Step 7 as required to configure additional nonkey fields for the record.	--
Step 9	**end** **Example:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 10	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.

	Command or Action	Purpose
Step 11	**show running-config flow record** *record-name* **Example:** `Device# show running-config flow record FLOW_RECORD-1`	(Optional) Displays the configuration of the specified flow record.

Creating a Customized Flow Monitor

To create a customized flow monitor, perform the following required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be one of the predefined formats, or an advanced user can create a customized format using the **flow record** command.

If you want to use a customized record instead of using one of the Flexible NetFlow predefined records, you must create the customized record before you can perform this task.

If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.

Note You must use the **no ip flow monitor**command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor. For information about the **ip flow monitor** command, refer to the *Cisco IOS Flexible NetFlow Command Reference* .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **cache** {**entries** *number* | **timeout** {**active** |**inactive**|**update**} *seconds* | **type** {**immediate** | **normal** | **permanent**}}
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **statistics packet protocol**
9. **statistics packet size**
10. **exporter** *exporter-name*
11. **end**
12. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]]
13. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor FLOW-MONITOR-1`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.
Step 4	**description** *description* **Example:** `Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `Device(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** |**inactive**|**update**} *seconds* | **type** {**immediate** | **normal** | **permanent**}} **Example:** `Device(config-flow-monitor)# cache entries 1000`	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. • The values for the keywords associated with the **timeout** keyword have no effect when the cache type is set to **immediate**.
Step 7	Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.	--

	Command or Action	Purpose
Step 8	**statistics packet protocol** **Example:** `Device(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `Device(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously. • Refer to the "Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters" module for information about and instructions for configuring flow exporters.
Step 11	**end** **Example:** `Device(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]] **Example:** `Device# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `Device# show flow monitor FLOW_MONITOR-1`	(Optional) Displays the configuration of the specified flow monitor.

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. To activate a flow monitor, perform the following required task.

Note When you specify the "NetFlow original" or the "NetFlow IPv4 original input" or the "NetFlow IPv6 original input" predefined record for the flow monitor to emulate original NetFlow, the Flexible NetFlow flow monitor can be used only for analyzing input (ingress) traffic.

When you specify the "NetFlow IPv4 original output" or the "NetFlow IPv6 original output" predefined record for the flow monitor to emulate the Egress NetFlow Accounting feature, the Flexible NetFlow flow monitor can be used only for analyzing output (egress) traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**} **Example:** `Device(config-if)# ip flow monitor FLOW-MONITOR-1 input`	Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic.
Step 5	Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.	--
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show flow interface** *type number* **Example:** `Device# show flow interface ethernet 0/0`	Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface.
Step 8	**show flow monitor name** *monitor-name* **cache format record** **Example:** `Device# show flow monitor name FLOW_MONITOR-1 cache format record`	Displays the status, statistics, and flow data in the cache for the specified flow monitor.

Configuration Examples for Customizing Flow Records and Flow Monitors

Example: Configuring a Permanent Flow Record Cache with a Limited Number of Flows

The following example is designed to monitor the type of service (ToS) field usage on all interfaces in the router. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor**command.

This sample starts in global configuration mode:

```
!
ip cef
!
flow record QOS_RECORD
 description UD: Flow Record to monitor the use of TOS within this router/network
 match interface input
 match interface output
 match ipv4 tos
 collect counter packets
 collect counter bytes
 exit
!
flow monitor QOS_MONITOR
 description UD: Flow Monitor which watches the limited combinations of interface and TOS
 record QOS_RECORD
 cache type permanent
 cache entries 8192   ! 2^5 (combos of interfaces) * 256 (values of TOS)
 exit
!
interface ethernet0/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface ethernet0/1
 ip flow monitor QOS_MONITOR input
 exit
!
interface ethernet0/2
 ip flow monitor QOS_MONITOR input
 exit
!
interface serial2/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface serial2/1
 ip flow monitor QOS_MONITOR input
!
```

The display from the **show flow monitor** command shows the current status of the cache.

```
Router# show flow monitor QOS_MONITOR cache
  Cache type:                           Permanent
  Cache size:                                8192
  Current entries:                              2
  High Watermark:                               2
  Flows added:                                  2
  Updates sent         (  1800 secs)            0
```

Example: Configuring a Customized Flow Record Cache for Monitoring IPv6 Traffic

The following example creates a customized flow record cache for monitoring IPv6 traffic.

This sample starts in global configuration mode:

```
!
ip cef
ipv6 cef
!
flow record FLOW-RECORD-2
 description Used for basic IPv6 traffic analysis
 match ipv6 destination address
 collect ipv6 protocol
 collect ipv6 source address
 collect transport source-port
 collect transport destination-port
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
flow monitor FLOW-MONITOR-2
 description Used for basic IPv6 traffic analysis
 record FLOW-RECORD-2
 cache entries 1000
 statistics packet protocol
 statistics packet size
!
interface Ethernet0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 input
!
interface Ethernet1/0
 ipv6 address 2001:DB8:3:ABCD::1/48
 ipv6 flow monitor FLOW-MONITOR-2 output
!
```

Example Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics

The following example shows how to configure Flexible NetFlow for monitoring MAC and VLAN statistics.

This sample starts in global configuration mode:

```
!
 flow record LAYER-2-FIELDS-1
 match ipv4 source address
 match ipv4 destination address
 collect datalink dot1q vlan output
 collect datalink mac source address input
 collect datalink mac source address output
 collect datalink mac destination address input
 collect flow direction
 collect counter bytes
 collect counter packets
!
 exit
!
!
flow monitor FLOW-MONITOR-4
 record LAYER-2-FIELDS-1
 exit
!
ip cef
!
interface Ethernet0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

Example Configuring Flexible NetFlow for Ingress VRF Support

The following example configures the collection of the virtual routing and forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key field.

This sample starts in global configuration mode:

```
!
flow record rm_1
match routing vrf input
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface Serial2/0
ip vrf forwarding green
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 output
!
end
```

Example Configuring Flexible NetFlow for Network-Based Application Recognition

The following example uses Network-based Application recognition (NBAR) to create different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key field.

This sample starts in global configuration mode:

```
!
flow record rm_1
match application name
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

Example Configuring Flexible NetFlow for CTS Fields

This following example configures the collection of the Cisco TrustSec (CTS) fields, source Security Group Tag (SGT) and destination Security Group Tag (DGT), in IPv4 traffic.

This sample starts in global configuration mode:

```
!
```

```
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
exit
flow record rm_1
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match flow direction
match flow cts source group-tag
match flow cts destination group-tag
collect routing source as
collect routing destination as
collect routing source as peer
collect routing destination as peer
collect routing next-hop address ipv4
collect routing next-hop address ipv4 bgp
collect ipv4 source prefix
collect ipv4 source mask
collect ipv4 destination prefix
collect ipv4 destination mask
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor mm_1
record rm_1
exporter EXPORTER-1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

Where to Go Next

If you want to configure data export for Flexible NetFlow, refer to the "Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters" module.

If you want to configure flow sampling to reduce the CPU overhead of analyzing traffic, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module.

If you want to configure any of the predefined records for Flexible NetFlow, refer to the "Configuring Cisco IOS Flexible NetFlow with Predefined Records" module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Flexible NetFlow	"Cisco IOS Flexible NetFlow Overview"

Related Topic	Document Title
Flexible NetFlow Feature Roadmap	"Cisco IOS Flexible NetFlow Features Roadmap"
Emulating original NetFlow with Flexible NetFlow	"Getting Started with Configuring Cisco IOS Flexible NetFlow"
Configuring flow exporters to export Flexible NetFlow data.	"Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters"
Configuring flow sampling to reduce the overhead of monitoring traffic with Flexible NetFlow	"Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic"
Configuring Flexible NetFlow using predefined records	"Configuring Cisco IOS Flexible NetFlow with Predefined Records"
Using Flexible NetFlow Top N Talkers to analyze network traffic	"Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic"
Configuring IPv4 multicast statistics support for Flexible NetFlow	"Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow"
Configuration commands for Flexible NetFlow	*Cisco IOS Flexible NetFlow Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Flexible NetFlow

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Information
Flexible NetFlow	12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1	Flexible NetFlow is introduced. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **cache** (Flexible NetFlow), **clear flow exporter**, **clear flow monitor**, **clear sampler**, **collect counter**, **collect flow**, **collect interface**, **collect ipv4**, **collect ipv4 destination**, **collect ipv4 fragmentation**, **collect ipv4 section**, **collect ipv4 source**, **collect ipv4 total-length**, **collect ipv4 ttl**, **collect routing**, **collect timestamp sys-uptime**, **collect transport**, **collect transport icmp ipv4**, **collect transport tcp**, **collect transport udp**, **debug flow exporter**, **debug flow monitor**, **debug flow record**, **debug sampler**, **description** (Flexible NetFlow), **destination**, **dscp** (Flexible NetFlow), **exporter**, **flow exporter**, **flow monitor**, **flow platform**, **flow record**, **ip flow monitor**, **match flow**, **match interface** (Flexible NetFlow), **match ipv4**, **match ipv4 destination**, **match ipv4 fragmentation**, **match ipv4 section**, **match ipv4 source**, **match ipv4 total-length**, **match ipv4 ttl**, **match routing**, **match transport**, **match transport icmp ipv4**, **match transport tcp**, **match transport udp**, **mode** (Flexible NetFlow), **option** (Flexible NetFlow), **record**, **sampler**, **show flow exporter**, **show flow interface**, **show flow monitor**, **show flow record**, **show sampler**, **source** (Flexible NetFlow), **statistics packet**,

Feature Name	Releases	Feature Information
		template data timeout, **transport** (Flexible NetFlow).
Flexible NetFlow--IPv4 Unicast Flows	12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to monitor IPv4 traffic. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **collect routing**, **debug flow record**, **collect ipv4**, **collect ipv4 destination**, **collect ipv4 fragmentation**, **collect ipv4 section**, **collect ipv4 source**, **ip flow monitor**, **match ipv4**, **match ipv4 destination**, **match ipv4 fragmentation**, **match ipv4 section**, **match ipv4 source**, **match routing**, **record**, **show flow monitor**, **show flow record**.
Flexible NetFlow--Layer 2 Fields	12.2(33)SRE 12.4(22)T	Enables collecting statistics for Layer 2 fields such as MAC addresses and virtual LAN (VLAN) IDs from traffic. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **collect datalink dot1q vlan** , **collect datalink mac**, **match datalink dot1q vlan**, **match datalink mac**.

Feature Name	Releases	Feature Information
Flexible NetFlow--IPv6 Unicast Flows	12.2(33)SRE 12.2(50)SY 12.4(20)T 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to monitor IPv6 traffic. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **collect routing**, **debug flow record**, **match routing**, **record**, **show flow monitor**, **show flow record**, **collect ipv6**, **collect ipv6 destination**, **collect ipv6 extension map**, **collect ipv6 fragmentation**, **collect ipv6 hop-limit**, **collect ipv6 length**, **collect ipv6 section**, **collect ipv6 source**, **collect transport icmp ipv6**, **ipv6 flow monitor**, **match ipv6**, **match ipv6 destination**, **match ipv6 extension map**, **match ipv6 fragmentation**, **match ipv6 hop-limit**, **match ipv6 length**, **match ipv6 section**, **match ipv6 source**, **match transport icmp ipv6**.
Flexible NetFlow--Ingress VRF Support	12.2(33)SRE 12.2(50)SY 15.0(1)M 15.0(1)SY 15.0(1)SY1	Enables collecting the virtual routing and forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key or a nonkey field. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **collect routing, match routing, option (Flexible NetFlow), show flow monitor.**

Feature Name	Releases	Feature Information
Flexible NetFlow--NBAR Application Recognition	15.0(1)M	Network-based Application recognition (NBAR) enables creation of different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key or a nonkey field. The following commands were introduced or modified: **collect application name, match application name, option** (Flexible NetFlow), **show flow monitor.**
TrustSec NetFlow IPv4 SGACL Deny and Drop Export	12.2(50)SY 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv4 traffic. The following commands were introduced or modified: **collect flow, match flow, show flow monitor.**
TrustSec NetFlow IPv6 SGACL Deny and Drop ExportS	12.2(50)SY 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv6 traffic. The following commands were introduced or modified: **collect flow, match flow, show flow monitor.**