Flexible NetFlow Export of Cisco TrustSec Fields

Cisco TrustSec Fields in Flexible NetFlow

The Flexible NetFlow Export of Cisco TrustSec Fields feature supports the Cisco TrustSec fields in the Flexible NetFlow (FNF) flow record and helps to monitor, troubleshoot, and identify non-standard behavior for Cisco TrustSec deployments.

Note Flexible netflow records and recording of Cisco TrustSec fields in the IP packets only work on IPv4 packets. IPv6 packets do not support capture of Cisco TrustSec fields.

The Cisco TrustSec fields, source security group tag (SGT) and destination security group tag (DGT) in the Flexible NetFlow (FNF) flow records help administrators correlate the flow with identity information. It enables network engineers to gain a detailed understanding of the customer use of the network and application resources. This information can then be used to efficiently plan and allocate access and application resources and to detect and resolve potential security and policy violations.

The Cisco TrustSec fields are supported for ingress FNF and for unicast and multicast traffic.

The following table presents Netflow v9 enterprise specific field types for Cisco TrustSec that are used in the FNF templates for the Cisco TrustSec source and destination source group tags.

ID	Description
CTS_SRC_GROUP_TAG	Cisco Trusted Security Source Group Tag
CTS_DST_GROUP_TAG	Cisco Trusted Security Destination Group Tag

The Cisco TrustSec fields are configured in addition to the existing match fields under the FNF flow record. The following configurations are used to add the Cisco TrustSec flow objects to the FNF flow record as non-key fields and to configure the source and destination security group tags for the packet.

The **collect flow cts {source | destination} group-tag** command is configured under flow record to specify the Cisco TrustSec fields as non-key fields. The values in non-key fields are added to flows to provide additional information about the traffic in the flows.

The flow record is then configured under flow monitor and the flow monitor is applied to the interface. To export the FNF data, a flow exporter needs to be configured and then added under the flow monitor.

Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match ipv4 protocol**
5. **match ipv4 source address**
6. **match ipv4 destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **collect flow cts source group-tag**
10. **collect flow cts destination group-tag**
11. **collect counter packets**
12. **end**

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 record** *record-name* **Example:** `Device(config)# flow record cts-record-ipv4`	Creates a new Flexible NetFlow (FNF) flow record, or modifies an existing FNF flow record, and enters Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
Step 4	**match ipv4 protocol** **Example:** `Device(config-flow-record)# match ipv4 protocol`	(Optional) Configures the IPv4 protocol protocol as a key field for a flow record. **Note** For Cisco CSR100V, ISR 4400, and ASR 1000 platforms, Cisco TrustSec fields are supported only in IPv4 FNF records.
Step 5	**match ipv4 source address** **Example:** `Device(config-flow-record)# match ipv4 source address`	(Optional) Configures the IPv4 source address as a key field for a flow record. **Note** For Cisco CSR100V, ISR 4400, and ASR 1000 platforms, Cisco TrustSec fields are supported only in IPv4 FNF records.
Step 6	**match ipv4 destination address** **Example:** `Device(config-flow-record)# match ipv4 destination address`	(Optional) Configures the IPv4 destination address as a key field for a flow record. **Note** For Cisco CSR100V, ISR 4400, and ASR 1000 platforms, Cisco TrustSec fields are supported only in IPv4 FNF records.
Step 7	**match transport source-port** **Example:** `Device(config-flow-record)# match transport source-port`	(Optional) Configures the transport source port as a key field for a flow record.
Step 8	**match transport destination-port** **Example:** `Device(config-flow-record)# match transport destination-port`	(Optional) Configures the transport destination port as a key field for a flow record.
Step 9	**collect flow cts source group-tag** **Example:** `Device(config-flow-record)# collect flow cts source group-tag`	(Optional) Configures the Cisco TrustSec source security group tag (SGT) in the FNF flow record as non-key fields.
Step 10	**collect flow cts destination group-tag** **Example:** `Device(config-flow-record)# collect flow cts destination group-tag`	(Optional) Configures the Cisco TrustSec destination security group tag (DGT) in the FNF flow record as non-key fields.
Step 11	**collect counter packets** **Example:** `Device(config-flow-record)# collect counter packets`	(Optional) Configures the number of packets seen in a flow as a non-key field and enables collecting the total number of packets from the flow.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.

Configuring a Flow Exporter

Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

Before you begin

Ensure that you create a flow record. For more information see the "Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record" section and the "Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **end**

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 exporter** *exporter-name* **Example:** `Device(config)# flow exporter EXPORTER-1`	Creates a flow exporter or modifies an existing flow exporter, and enters Flexible NetFlow flow exporter configuration mode.
Step 4	**destination** {*ip-address*	*hostname*} [**vrf** *vrf-name*] **Example:**	Specifies the IP address or hostname of the destination system for the exporter.

	Command or Action	Purpose
	`Device(config-flow-exporter)# destination 172.16.10.2`	
Step 5	**end** **Example:** `Device(config-flow-exporter)# end`	Exits Flexible NetFlow flow exporter configuration mode and returns to privileged EXEC mode.

Configuring a Flow Monitor

Before you begin

To add a flow exporter to the flow monitor for data export, ensure that you create the flow exporter. For more information see the “Configuring a Flow Exporter” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **record** *record-name*
5. **exporter** *exporter-name*
6. **end**

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 or modifies an existing flow monitor, and enters Flexible NetFlow flow monitor configuration mode.
Step 4	**record** *record-name* **Example:**	Specifies the record for the flow monitor.

	Command or Action	Purpose
	`Device(config-flow-monitor)# record cts-record-ipv4`	
Step 5	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	Specifies the exporter for the flow monitor.
Step 6	**end** **Example:** `Device(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.

Applying a Flow Monitor on an Interface

To activate a flow monitor, the flow monitor must be applied to at least one interface.

Before you begin

Ensure that you create a flow monitor. For more information see the "Configuring a Flow Monitor" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* **input**
5. **end**

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 Gi1/1`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip flow monitor** *monitor-name* **input** **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	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying Flexible NetFlow Export of Cisco TrustSec Fields

SUMMARY STEPS

1. **enable**
2. **show flow record** *record-name*
3. **show flow exporter** *exporter-name*
4. **show flow monitor** *monitor-name*
5. **show flow monitor** *monitor-name* **cache**
6. **show flow interface** *type number*

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show flow record** *record-name*

Displays the details of the specified Flexible NetFlow (FNF) flow record.

Example:

```
Device> show flow record cts-recordipv4

flow record cts-recordipv4:
  Description:        User defined
```

```
  No. of users:       1
  Total field space:  30 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface output
    collect flow direction
    collect flow cts source group-tag
    collect flow cts destination group-tag
    collect counter packets
```

Step 3 **show flow exporter** *exporter-name*

Displays the current status of the specified FNF flow exporter.

Example:

```
Device> show flow exporter EXPORTER-1

Flow Exporter EXPORTER-1:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 100.100.100.1
    Source IP address:      3.3.3.2
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            65252
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

Step 4 **show flow monitor** *monitor-name*

Displays the status and statistics of the specified FNF flow monitor.

Example:

```
Device> show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       cts-recordipv4
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:                 normal (Platform cache)
    Status:               allocated
    Size:                 200000 entries
    Inactive Timeout:     60 secs
    Active Timeout:       1800 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
    Trans end aging:      off
```

Step 5 **show flow monitor** *monitor-name* **cache**

Displays the contents of the specified FNF flow monitor cache.

Example:

```
Device> show flow monitor FLOW-MONITOR-1 cache

  Cache type:                               Normal
  Cache size:                               4096
  Current entries:                          2
  High Watermark:                           2

  Flows added:                              6
  Flows aged:                               4
    - Active timeout      (1800 secs)       0
    - Inactive timeout    (15 secs)         4
    - Event aged                            0
    - Watermark aged                        0
    - Emergency aged                        0

  IPV4 SOURCE ADDRESS:                      10.1.0.1
  IPV4 DESTINATION ADDRESS:                 172.16.2.0
  TRNS SOURCE PORT:                         58817
  TRNS DESTINATION PORT:                    23
  FLOW DIRECTION:                           Input
  IP PROTOCOL:                              6
  SOURCE GROUP TAG:                         100
  DESTINATION GROUP TAG:                    200
  counter packets:                          10

  IPV4 SOURCE ADDRESS:                      172.16.2.0
  IPV4 DESTINATION ADDRESS:                 10.1.0.1
  TRNS SOURCE PORT:                         23
  TRNS DESTINATION PORT:                    58817
  FLOW DIRECTION:                           Output
  IP PROTOCOL:                              6
  SOURCE GROUP TAG:                         200
  DESTINATION GROUP TAG:                    100
  counter packets:                          8
```

Step 6 **show flow interface** *type number*

Displays the details of the FNF flow monitor applied on the specified interface. If a flow monitor is not applied on the interface, then the output is empty.

Example:

```
Device>  show flow interface Gi1/1

Interface GigabitEthernet1/1
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
```

Configuration Examples for Flexible NetFlow Export of Cisco TrustSec Fields

Example: Configuring Cisco TrustSec Fields as Non-Key Fields in the Flow Record

The following example shows how to configure the Cisco TrustSec flow objects as non-key fields in an IPv4 Flexible NetFlow flow record:

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
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 flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# end
```

Example: Configuring a Flow Exporter

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# end
```

Example: Configuring a Flow Monitor

```
Device> enable
Device# configure terminal
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record cts-record-ipv4
Device(config-flow-monitor)# exporter EXPORTER-1
Device(config-flow-monitor)# end
```

Example: Applying a Flow Monitor on an Interface

The following example shows how to activate an IPv4 flow monitor by applying it to an interface to analyze traffic. To activate an IPv6 flow monitor, replace the **ip** keyword with the **ipv6** keyword.

```
Device> enable
Device# configure terminal
Device(config)# interface Gi1/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# end
```