Flexible NetFlow Export of Cisco TrustSec Fields

• Flexible NetFlow Export of Cisco TrustSec Fields, on page 1

Flexible NetFlow Export of Cisco TrustSec Fields

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 nonstandard behavior for Cisco TrustSec deployments.

This module describes the interaction between Cisco TrustSec and FNF and how to configure and export Cisco TrustSec fields in the NetFlow Version 9 flow records.

Restrictions for Flexible NetFlow Export of Cisco TrustSec Fields

- The security group tag (SGT) value that is exported in FNF records is zero in the following scenarios:
  - The corresponding packet is received with an SGT value of zero from a trusted interface.
  - The corresponding packet is received without an SGT.
  - The SGT is not found during the IP-SGT lookup. (The SGT is not found in the same packet because the packet is received without an SGT.)
  - When a flow record has SGT and Destination Group Tag (DGT) fields (or only either of the two), and if both these values are not applicable, a flow will still be created with zero values for SGT and DGT. The flow records are expected to include source and destination IP addresses, along with SGT and DGT fields.

Information About Flexible NetFlow Export of Cisco TrustSec Fields

Cisco TrustSec Fields in Flexible NetFlow

The Cisco TrustSec fields, source SGT and destination sSGT, in FNF flow records help administrators correlate the flow with identity information. It enables network engineers to gain a detailed understanding how customers use 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.

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

The following table lists NetFlow Version 9 enterprise-specific field types for Cisco TrustSec, which are used in FNF templates for the Cisco TrustSec source and destination SGTs.

Flow Field Type	Description
CTS_SRC_GROUP_TAG	Cisco TrustSec sourceSGT
CTS_DST_GROUP_TAG	Cisco TrustSec destination SGT

Cisco TrustSec fields are configured in addition to the existing match fields under the FNF flow record. The following configurations are used to add Cisco TrustSec flow objects to the FNF flow record as key or nonkey fields and to configure source and destination SGTs for a packet.

The **match flow cts {source | destination} group-tag** command is configured under the corresponding flow record to specify Cisco TrustSec fields as key fields. The key fields differentiate flows, with each flow having a unique set of values. A flow record requires at least one key field, before it can be used in a flow monitor. You can configure the **match** command to a source SGT, destination SGT or both, at the same time.

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

How to Configure Flexible NetFlow Export of Cisco TrustSec Fields

The following sections provide information about the various tasks that comprise FNF export of Cisco TrustSec fields.

Configuring Cisco TrustSec Fields as Key Fields in Flow Record

Procedure

	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 FNF flow record, or modifies an existing FNF flow record, and enters Flexible NetFlow flow record configuration mode. • This command also allows you to modify an existing flow record.

	Command or Action	Purpose
Step 4	**match ipv4 protocol** **Example:** `Device(config-flow-record)# match ipv4 protocol`	(Optional) Configures the IPv4 protocol as a key field for a flow record.
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.
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.
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	**match flow direction** **Example:** `Device(config-flow-record)# match flow direction`	(Optional) Configures the direction in which the flow is monitored as a key field.

Step 10	**match flow cts** {**source** | **destination**} **group-tag**
	Example:
	`Device(config-flow-record)# match flow cts source group-tag`
	`Device(config-flow-record)# match flow cts destination group-tag`
		Configures the Cisco TrustSec source group tag or destination group tag as a key field for the record in the FNF flow record.
		• Ingress:
		  • In an incoming packet, if a header is present, SGT reflects the same value as the header. If no value is present, it will show zero.
		  • The DGT value does not depend on the ingress port SGACL configuration.

	Command or Action	Purpose
		• Egress: • If either the **propagate-sgt** command, or Cisco TrustSec is disabled on the egress interface, SGT will be zero. • In an outgoing packet, if the SGACL configuration that corresponds to the SGT or DGT exists, DGT will be a numeral other than zero. • If SGACL is disabled on the egress port or VLAN, or if global SGACL enforcement is disabled, DGT will be zero.
Step 11	**end** **Example:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.

Configuring SGT Name Export in NetFlow

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.

Procedure

	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.

	Command or Action	Purpose
Step 4	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `Device(config-flow-exporter)# destination 172.16.10.2`	Specifies the IP address or hostname of the destination system for the exporter.
Step 5	**option cts-sgt-table** [**timeout** *seconds*] **Example:** `Device(config-flow-exporter)# option cts-sgt-table timeout 1200`	Selects the SGT ID-to-name table option for the exporter. • This option allows FNF to export Cisco TrustSec environmental data tables that map SGTs to Security Group Names.
Step 6	**end** **Example:** `Device(config-flow-exporter)# end`	Exits Flexible NetFlow flow exporter configuration mode and returns to privileged EXEC mode.

Configuration Examples for Flexible NetFlow Export of Cisco TrustSec Fields

The following sections provide examples relating to the configuration of FNF export of Cisco TrustSec fields.

Example: Configuring Cisco TrustSec Fields as Key Fields in Flow Record

The following example shows how to configure the Cisco TrustSec flow objects as 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)# match flow direction
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# end
```

Example: Configuring SGT Name Export in NetFlow

The following example shows how to configure SGT Name Export in NetFlow.

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

```
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# option cts-sgt-table timeout 1200
Device(config-flow-exporter)# end
```

Feature History for Flexible NetFlow Export of Cisco TrustSec Fields

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.9.2	Flexible NetFlow Export of Cisco TrustSec Fields	The Flexible NetFlow Export of Cisco TrustSec Fields feature supports the Cisco TrustSec fields in the FNF flow record and helps to monitor, troubleshoot, and identify nonstandard behavior for Cisco TrustSec deployments.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.