TrustSec NetFlow IPv4 SGACL Deny and Drop Export

The TrustSec NetFlow IPv4 SGACL Deny and Drop Export feature enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv4 traffic.

- Finding Feature Information, on page 1
- Information About TrustSec NetFlow IPv4 SGACL Deny and Drop Export , on page 1
- How to Configure TrustSec NetFlow IPv4 SGACL Deny and Drop Export , on page 2
- Configuration Examples for TrustSec NetFlow IPv4 SGACL Deny and Drop Export , on page 8
- Additional References for TrustSec NetFlow IPv4 SGACL Deny and Drop Export , on page 9
- Feature Information for TrustSec NetFlow IPv4 SGACL Deny and Drop Export , on page 10

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.

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.

Information About TrustSec NetFlow IPv4 SGACL Deny and Drop Export

TrustSec NetFlow IPv4 SGACL Deny and Drop Export Overview

A Security Group Access Control List (SGACL) is used to filter untrusted packets. The TrustSec NetFlow IPv4 SGACL Deny and Drop Export feature enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv4 traffic.

How to Configure TrustSec NetFlow IPv4 SGACL Deny and Drop Export

Creating a Customized Flow Record

Perform this task to configure 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 shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {**ip** | **ipv6**} {**destination** | **source**} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {**source** | **destination**} **group-tag**
8. **collect interface** {**input** | **output**}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **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.
Step 3	**flow record** *record-name* **Example:**	Creates a flow record and enters Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
	`Device(config)# flow record FLOW-RECORD-1`	• 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** {**ip** | **ipv6**} {**destination** | **source**} **address** **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.
Step 6	Repeat Step 5 as required to configure additional key fields for the record.	—

Step 7	**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`
		Note This example configures the CTS source group tag and destination group tag 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.

	Command or Action	Purpose
		Note • Ingress: • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero

Step 8	**collect interface** {**input** | **output**}
	Example:
	`Device(config-flow-record)# collect interface input`
		Configures the input interface as a nonkey field for the record.
		Note This example configures the input interface as a nonkey field for the record.

Step 9	Repeat the above step as required to configure additional nonkey fields for the record.	—

Step 10	**end**
	Example:
	`Device(config-flow-record)# end`
		Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.

Step 11	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.
Step 12	**show running-config flow record** *record-name* **Example:**	(Optional) Displays the configuration of the specified flow record.

	Command or Action	Purpose
	`Device# show running-config flow record FLOW_RECORD-1`	

Creating a Customized Flow Monitor

Perform this required task to create a customized flow monitor.

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 a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

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.

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* | {**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:** `> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `(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:** `(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:
	`(config-flow-monitor)# record FLOW-RECORD-1`
		Specifies the record for the flow monitor.

Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(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.	—
Step 8	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.

	Command or Action	Purpose

Step 11	**end**
	Example:
	`(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:** `# 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:** `# show running-config 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. Perform this required task to activate a flow monitor.

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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.

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 GigabitEthernet 0/0/0`	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 TrustSec NetFlow IPv4 SGACL Deny and Drop Export

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
```

Additional References for TrustSec NetFlow IPv4 SGACL Deny and Drop Export

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Flexible NetFlow conceptual and configuration information	*Flexible NetFlow Configuration Guide*
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 IOS 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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for TrustSec NetFlow IPv4 SGACL Deny and Drop Export

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 IPv4 SGACL Deny and Drop Export

Feature Name	Releases	Feature Information
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.**