Configure NetFlow in FMC

Contents

Introduction

This document describes how to configure Netflow in the Cisco Secure Firewall Management Center running version 7.4 or higher.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- NetFlow Protocol

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall Management Center for VMWare runs v7.4.1
- Secure Firewall Runs v7.4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

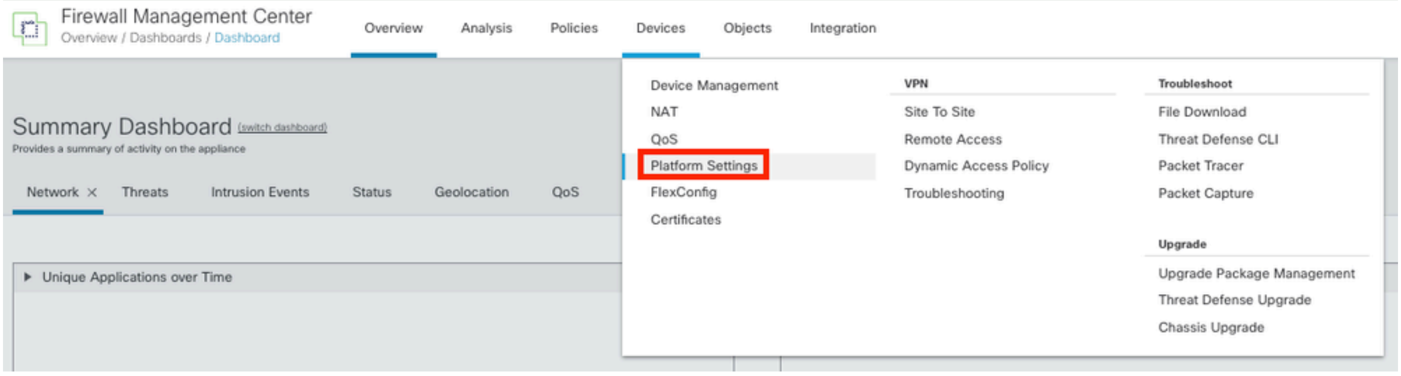
Background Information

Specific requirements for this document include:

- Cisco Secure Firewall Threat Defense running version 7.4 or higher
- Cisco Secure Firewall Management Center running version 7.4 or higher

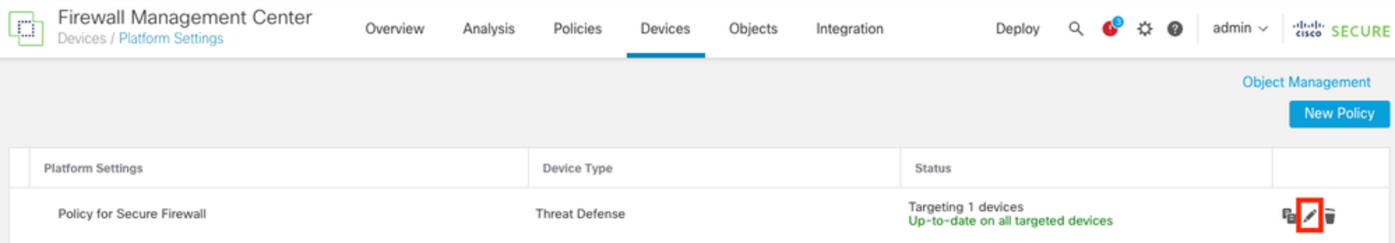
Add Collector in NetFlow

Step 1. Navigate to **Devices** > **Platform Settings**:



Accessing Platform Settings

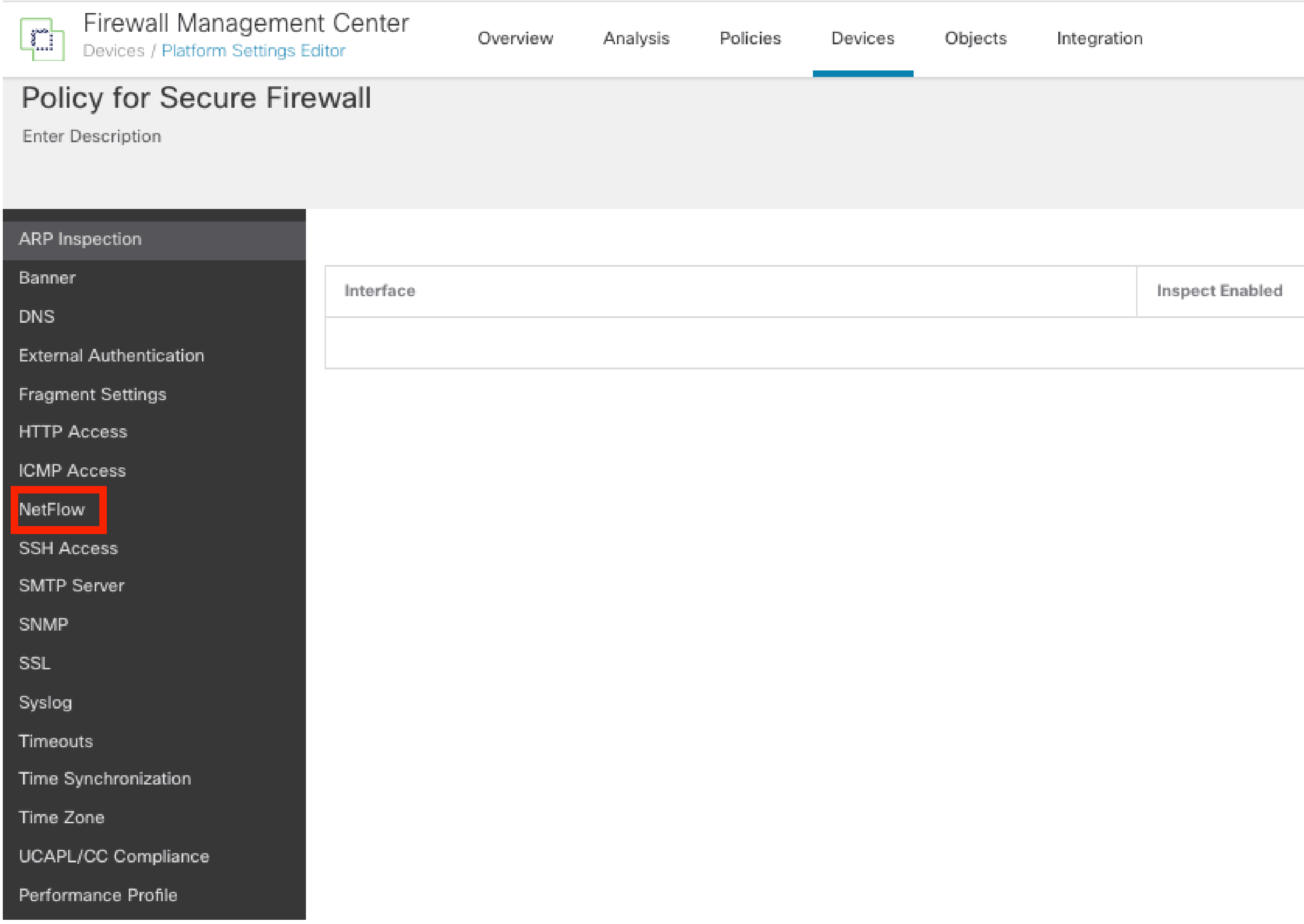
Step 2. Edit the **Platform Settings Policy** assigned to the Monitor Device:



Platform Settings	Device Type	Status
Policy for Secure Firewall	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

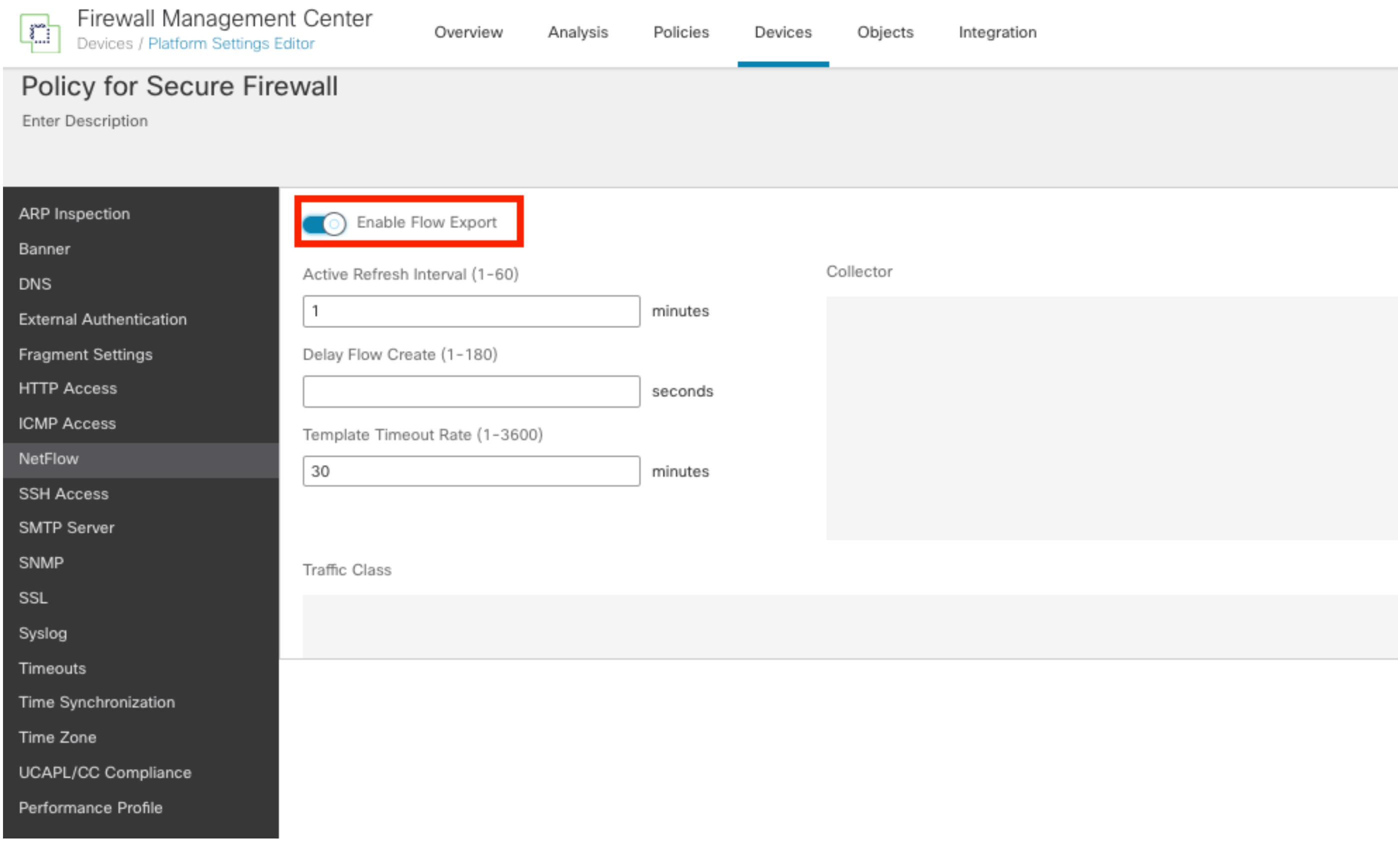
Policy Edition

Step 3. Choose **Netflow**:



Accessing NetFlow Settings

Step 4. Enable **Flow Export** toggle to enable NetFlow data export:



Policy for Secure Firewall

Enter Description

● Enable Flow Export

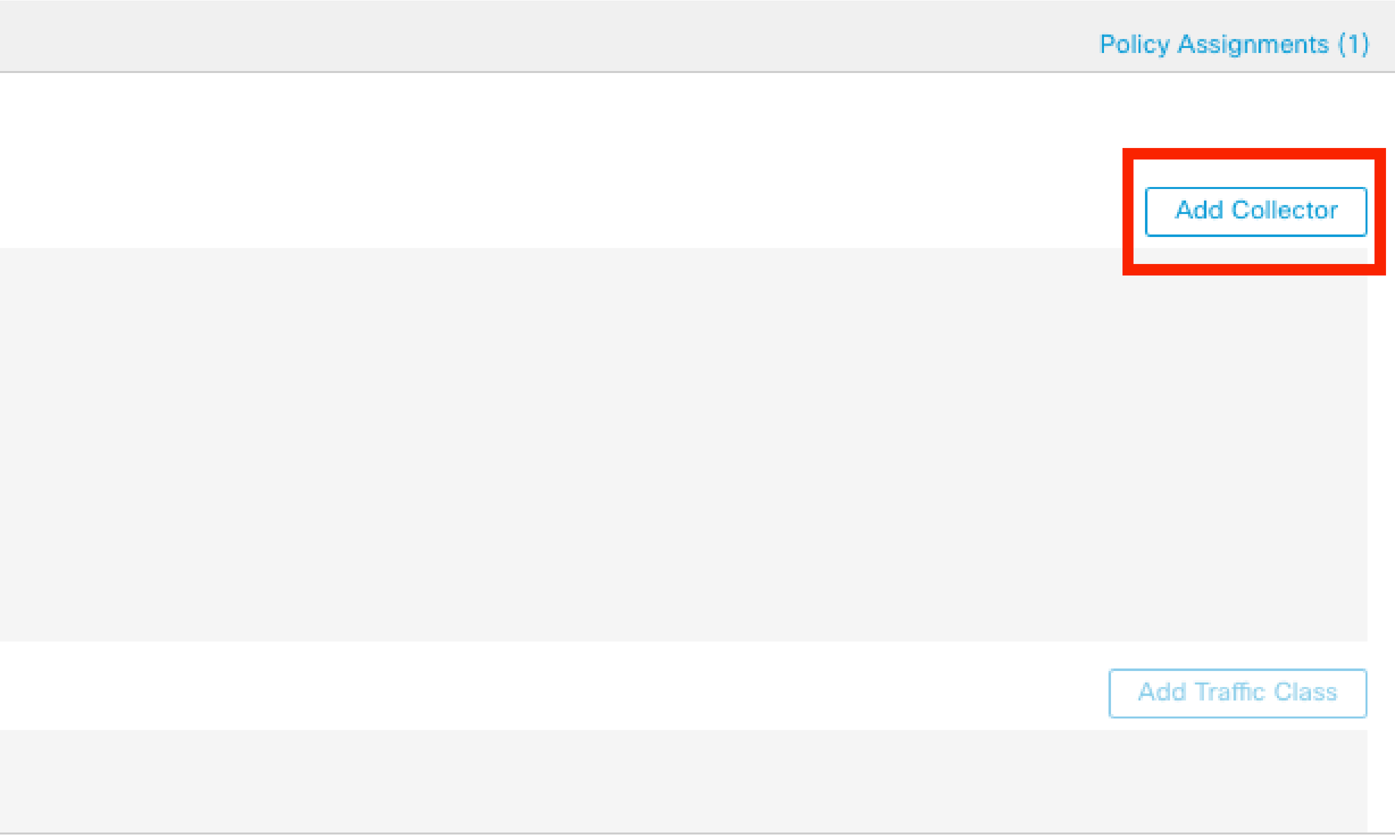
Active Refresh Interval (1-60): 1 minutes

Delay Flow Create (1-180): seconds

Template Timeout Rate (1-3600): 30 minutes

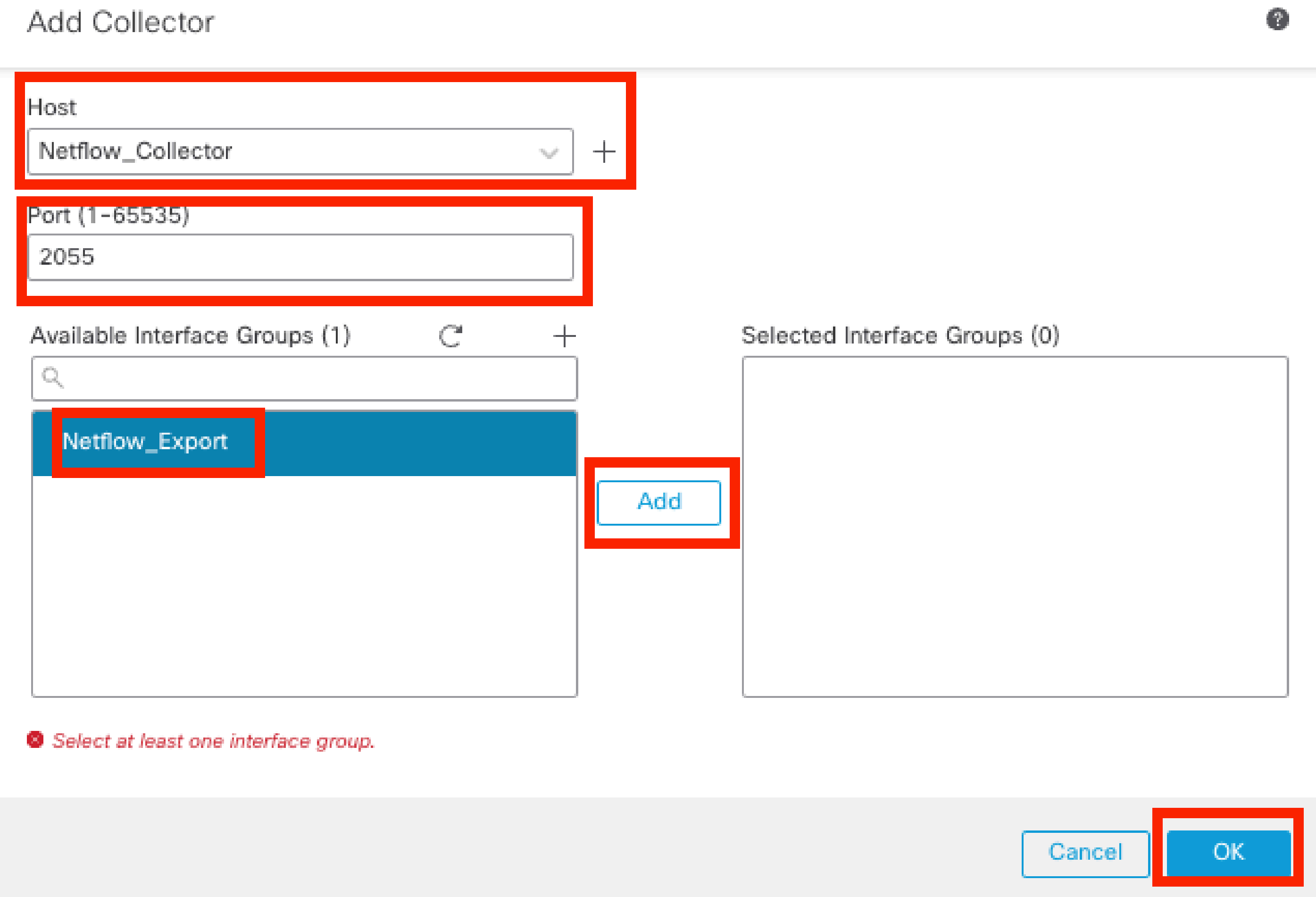
Enabling NetFlow

Step 5. Click **Add Collector**:



Adding Collector

Step 6. Choose the **collector host IP object** of the NetFlow event collector, the UDP port on the collector to which the NetFlow packets must be sent, choose the **interface group** through which the collector must be reached, and click **OK**:



Host: Netflow_Collector

Port (1-65535): 2055

Available Interface Groups (1): Netflow_Export

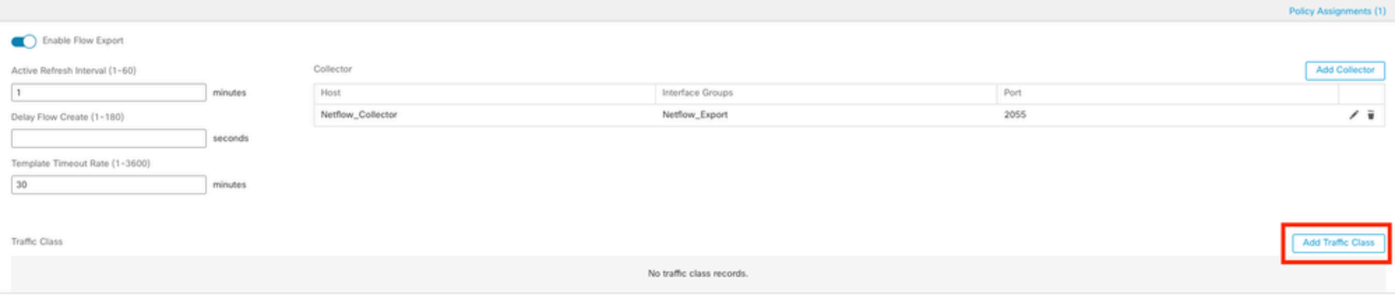
Selected Interface Groups (0)

Select at least one interface group.

Collector Settings

Add Traffic Class to NetFlow

Step 1. Click **Add Traffic Class**:



Enable Flow Export

Active Refresh Interval (1-60): 1 minutes

Delay Flow Create (1-180): seconds

Template Timeout Rate (1-3600): 30 minutes

Collector

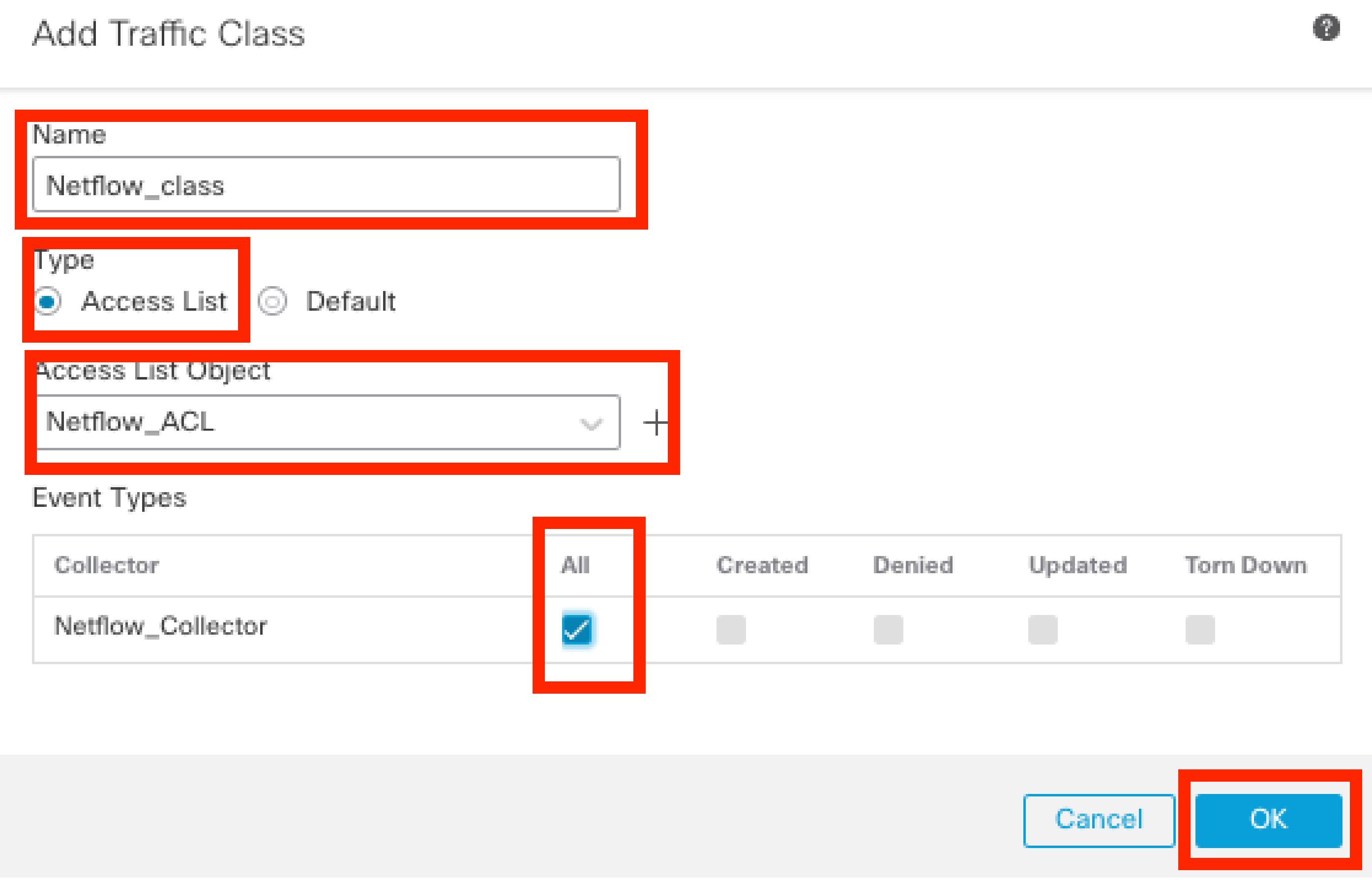
Host	Interface Groups	Port
Netflow_Collector	Netflow_Export	2055

Traffic Class

No traffic class records.

Adding Traffic Class

Step 2. Enter the **name** field of the traffic class that must match the NetFlow events, the **ACL** to specify the traffic class that must match the traffic captured for the NetFlow events, select the **checkboxes** for the different NetFlow events that you want to send to the collectors and click **OK**:


Add Traffic Class

Name

Netflow_class

Type

● Access List ○ Default

Access List Object

Netflow_ACL

Event Types

Collector	All	Created	Denied	Updated	Torn Down
Netflow_Collector	☑	□	□	□	□

Traffic Class Settings

Troubleshooting

Step 1. You can verify the configuration from FTD CLI.

1.1. From FTD CLI, enter to system support diagnostic-cli:

```
>system support diagnostic-cli
```

1.2 Check policy-map configuration:

<#root>

```
firepower#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
```

```
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class_snmp
inspect snmp
```

class Netflow_class_Netflow_ACL

flow-export event-type all destination 192.168.31.1

```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Check the flow-export configuration:

<#root>

```
firepower#show running-config flow-export
```

flow-export destination Inside 192.168.31.1 2055

Note: In this example, Inside, is the name of the interface configured in the Interface Group called Netflow_Export.

Step 2. Verify the hit count for the ACL:

<#root>

```
firepower#show access-list Netflow_ACL
access-list Netflow_ACL; 1 elements; name hash: 0xbad5d4bf
access-list Netflow_ACL line 1 extended permit ip object Inside_Network any (

hitcnt=44

) 0xb704fc5b
access-list Netflow_ACL line 1 extended permit ip 10.1.2.0 255.255.255.0 any (

hitcnt=44

) 0xb704fc5b
```

Step 3. Verify Netflow counters:

<#root>

```
firepower#show flow-export counters

destination: Inside 192.168.31.1 2055
Statistics:


packets sent                                              101


Errors:
block allocation failure                                    0
invalid interface                                           0
template send failure                                       0
no route to collector                                       0
failed to get lock on block                                 0
source port allocation failure                              0
```

Related Information

- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4