Configuración de NetFlow en FMC

Contenido

Introducción

Este documento describe cómo configurar Netflow en Cisco Secure Firewall Management Center que ejecuta la versión 7.4 o superior.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)
- Protocolo NetFlow

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Secure Firewall Management Center para VMWare ejecuta la versión 7.4.1
- Secure Firewall ejecuta la versión 7.4.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

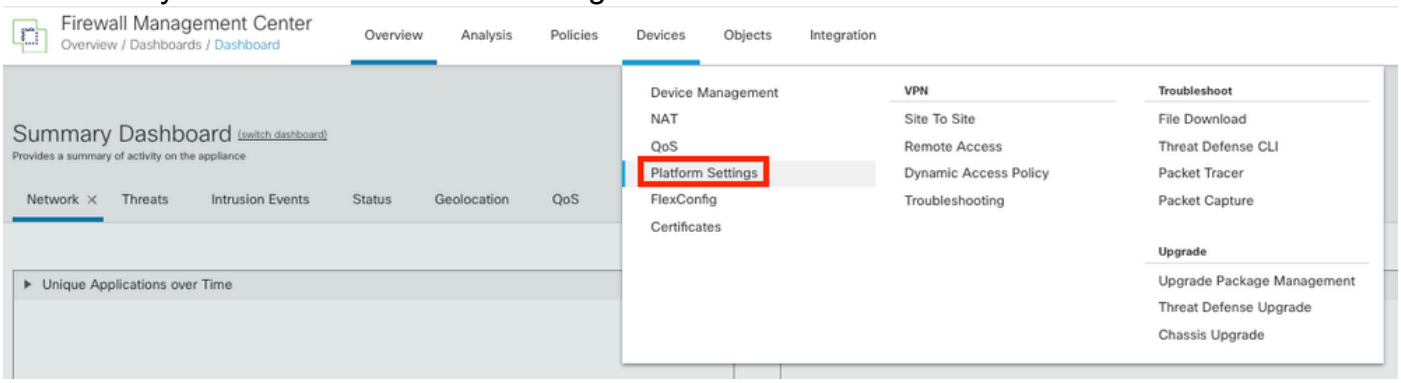
Antecedentes

Los requisitos específicos para este documento incluyen:

- Cisco Secure Firewall Threat Defence con versión 7.4 o superior
- Cisco Secure Firewall Management Center con versión 7.4 o superior

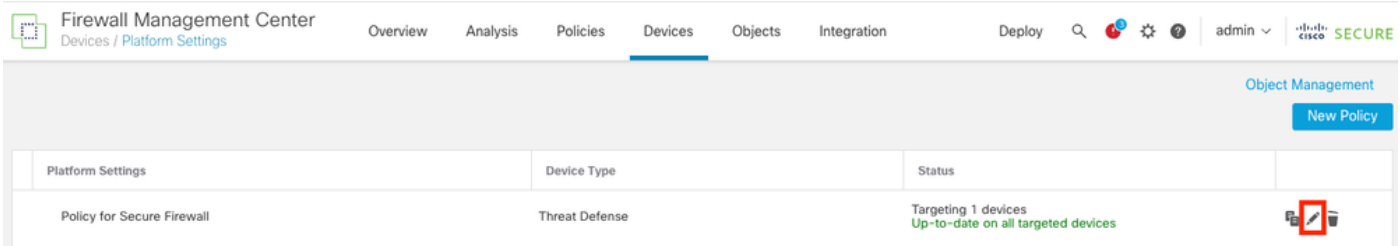
Agregar recopilador en NetFlow

Paso 1. Vaya a Devices > Platform Settings:



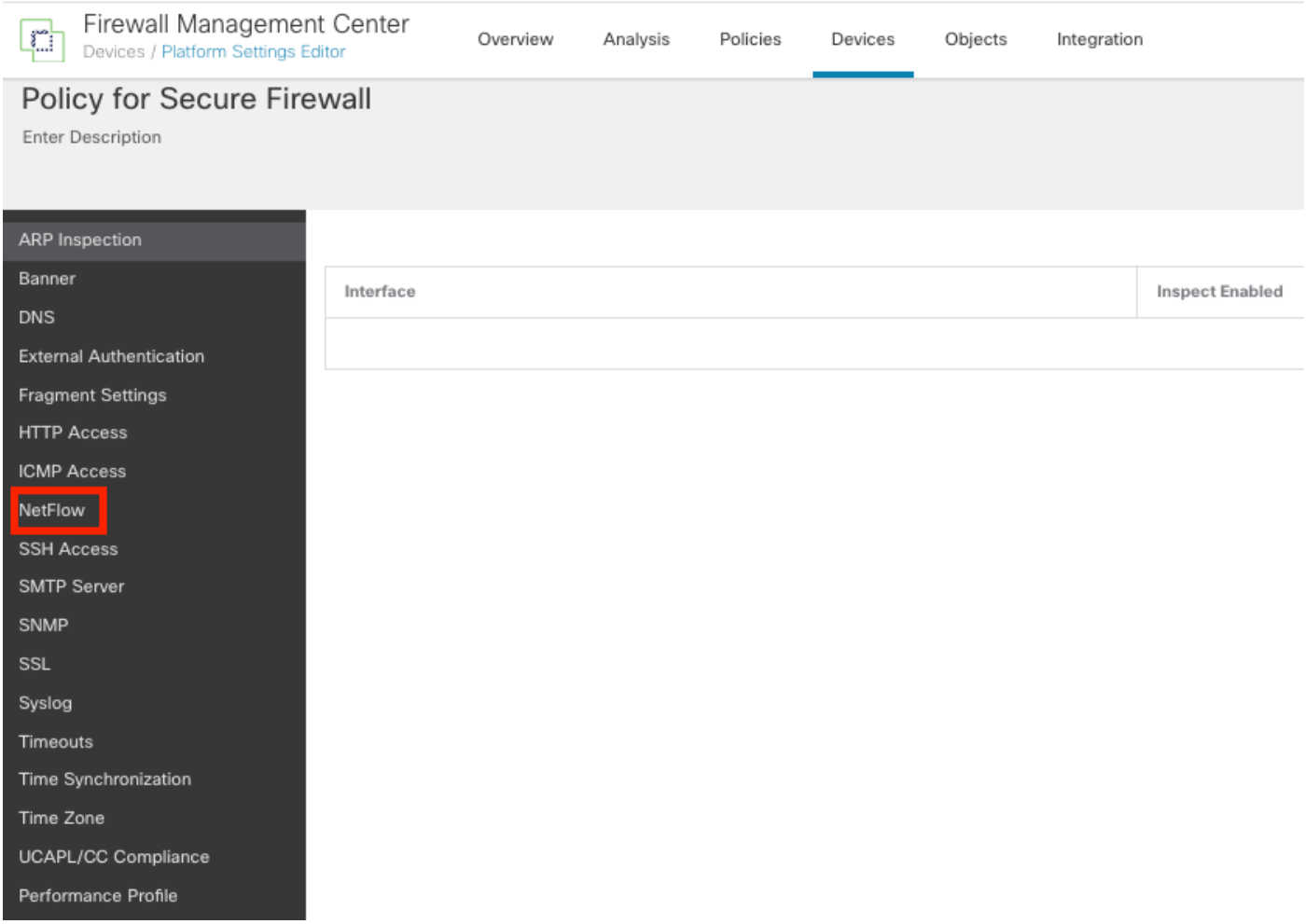
Acceso a configuración de plataforma

Paso 2. Edite la política de configuración de la plataforma asignada al dispositivo de supervisión:



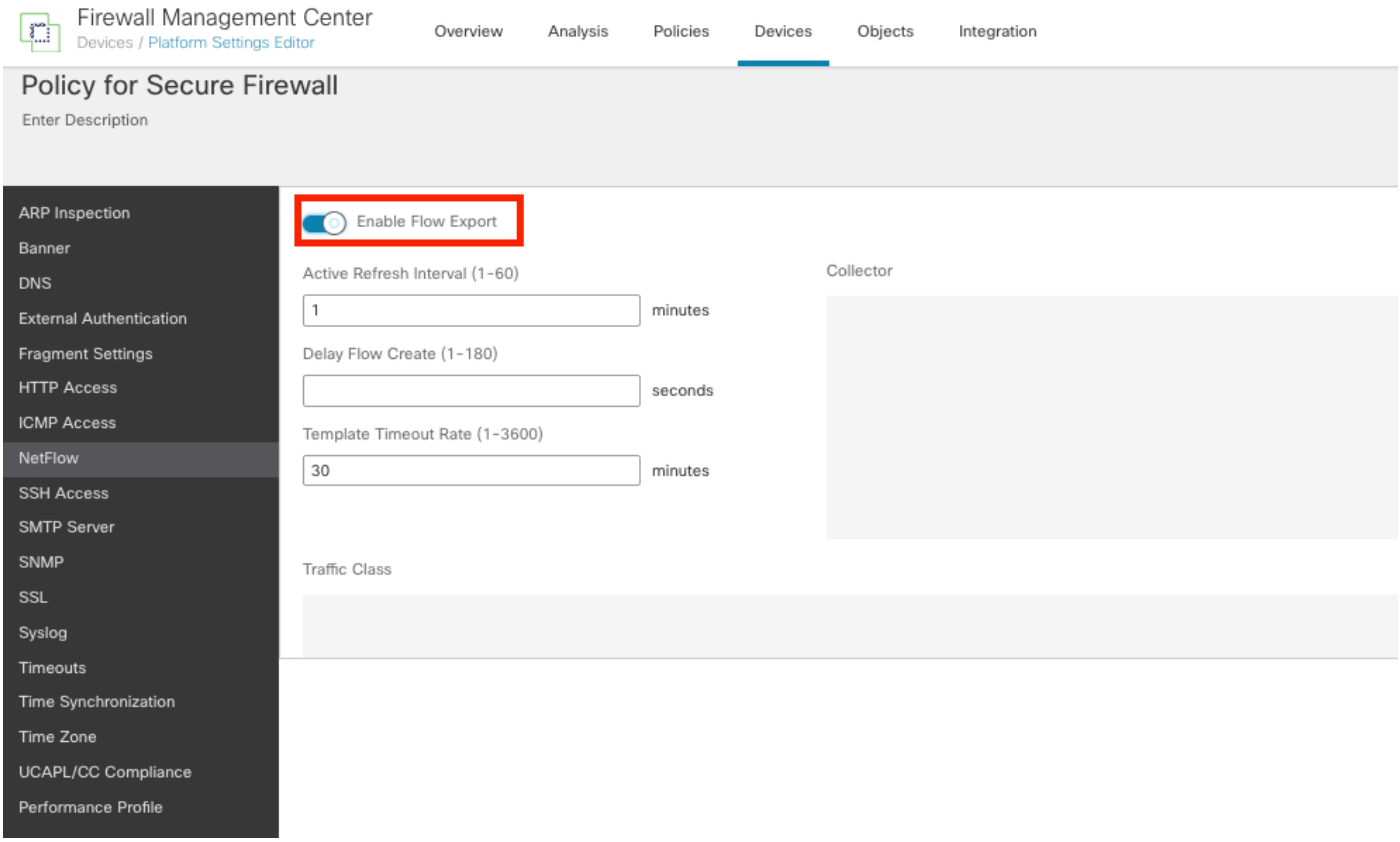
Edición de políticas

Paso 3. Elija Netflow:



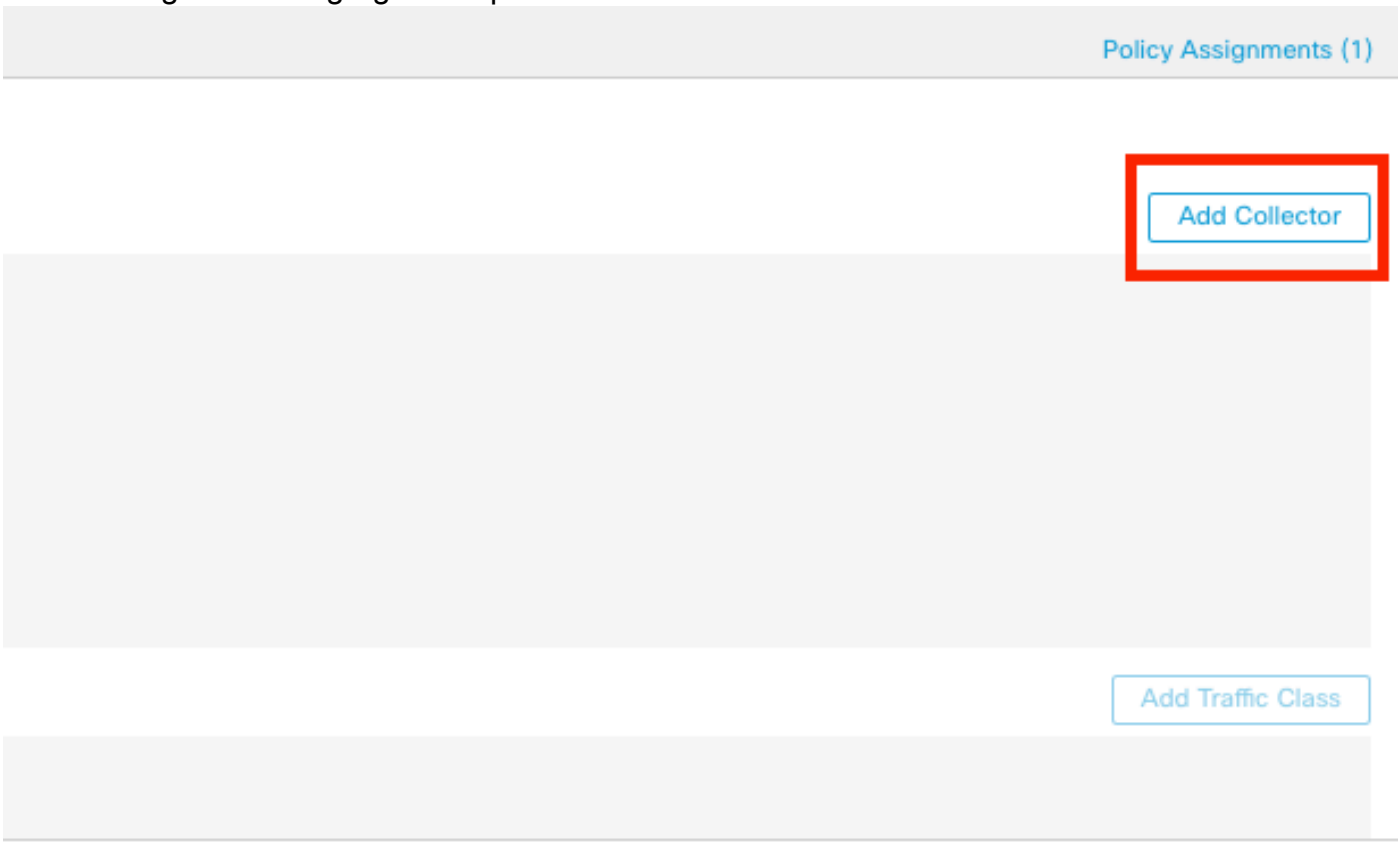
Acceso a la configuración de NetFlow

Paso 4. Active la opción Exportar Flujo para activar la exportación de datos de NetFlow:



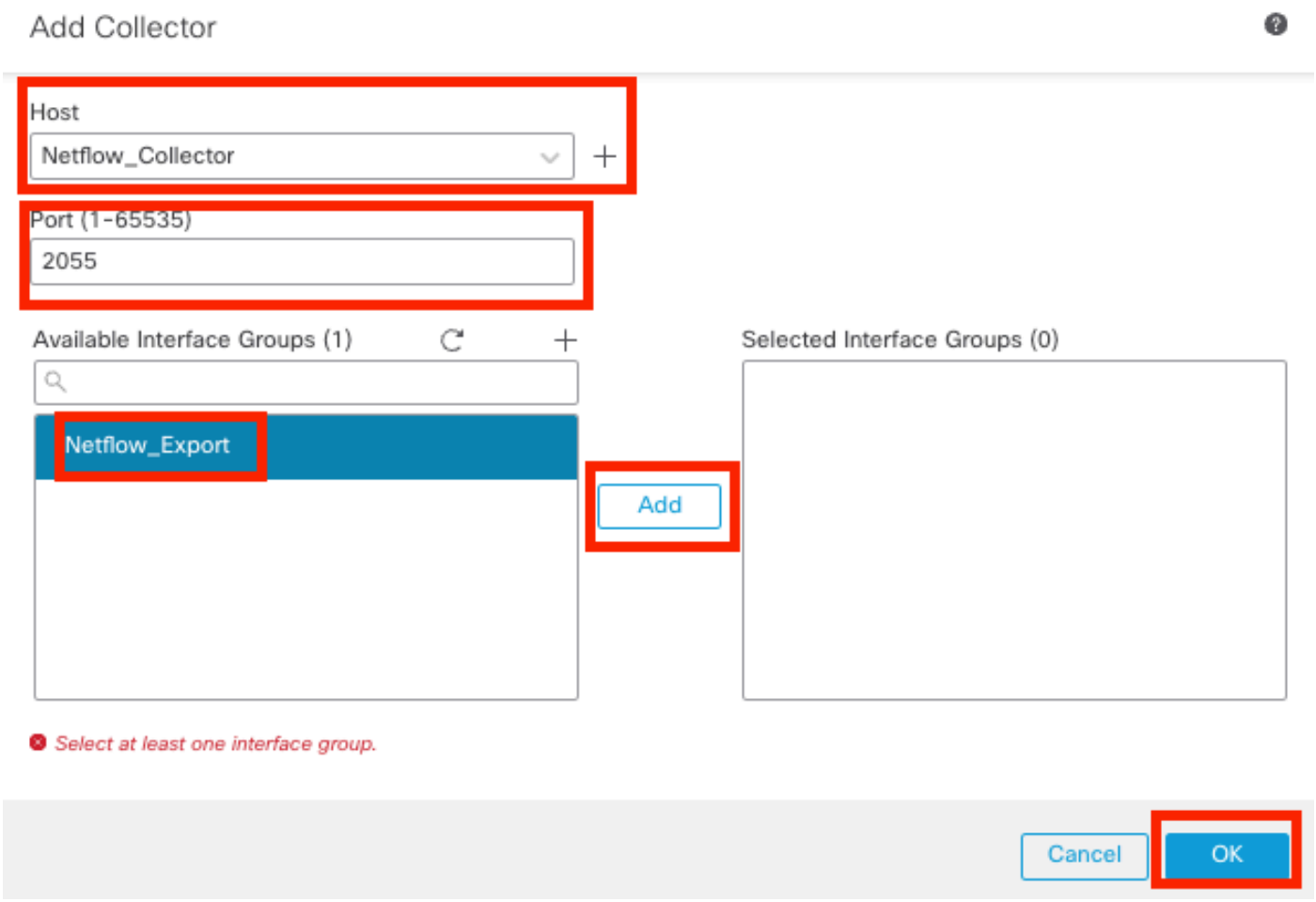
Habilitación de NetFlow

Paso 5. Haga clic en Agregar recopilador:



Adición de recopilador

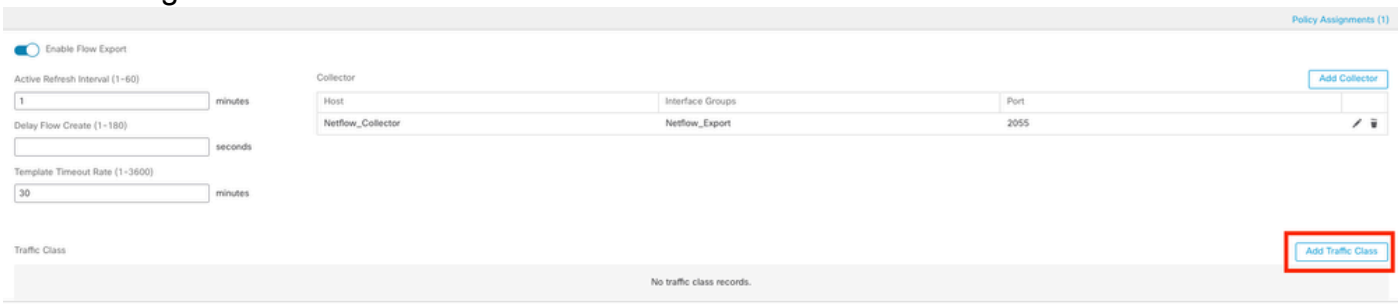
Paso 6. Elija el objeto IP de host del colector del colector de eventos de NetFlow, el puerto UDP en el colector al que se deben enviar los paquetes de NetFlow, elija el grupo de interfaz a través del cual se debe alcanzar el colector y haga clic en Aceptar:



Configuración del recopilador

Agregar clase de tráfico a NetFlow

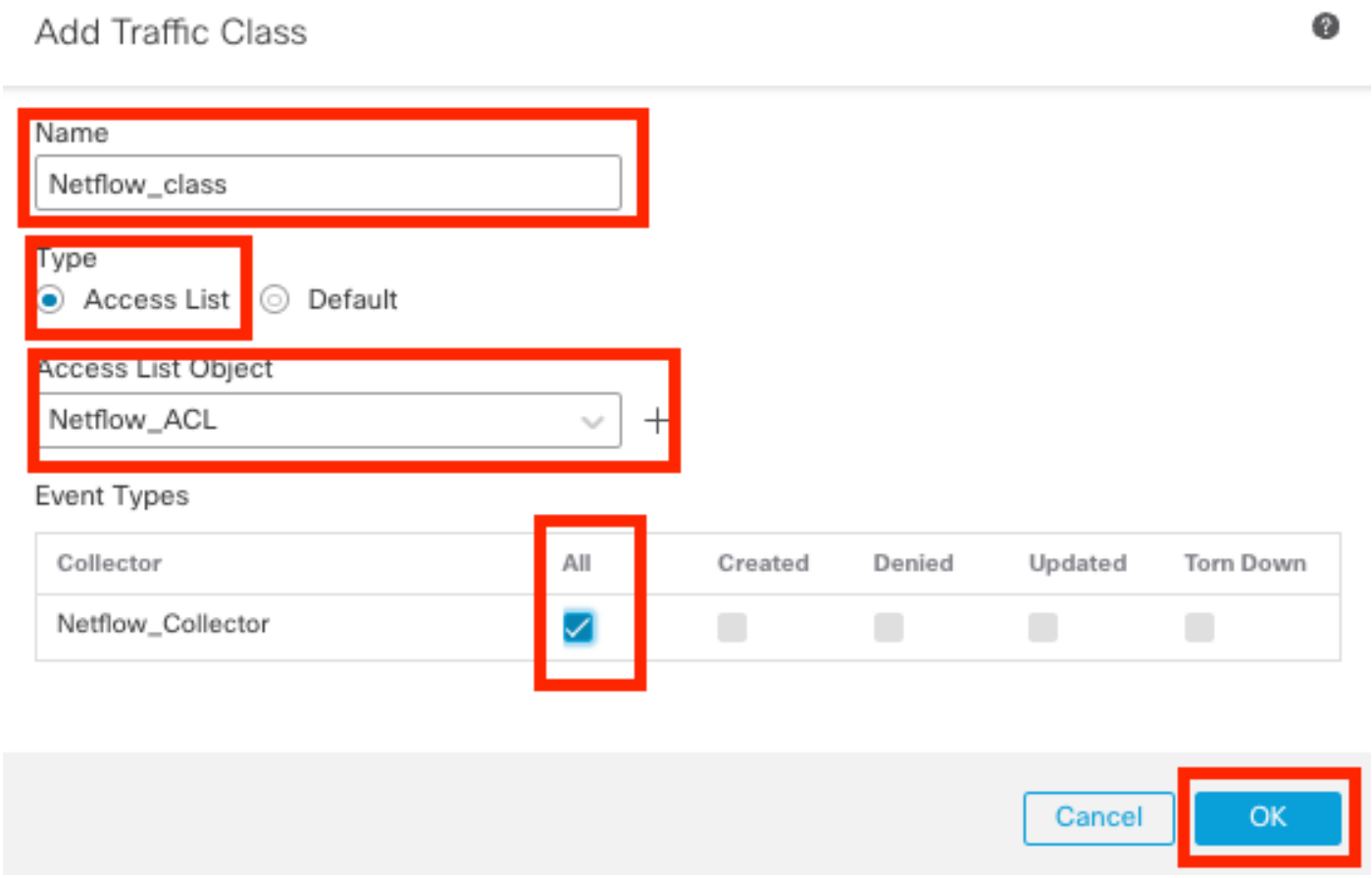
Paso 1. Haga clic en Add Traffic Class:



Adición de clase de tráfico

Paso 2. Ingrese el campo de nombre de la clase de tráfico que debe coincidir con los eventos de NetFlow, la ACL para especificar la clase de tráfico que debe coincidir con el tráfico capturado para los eventos de NetFlow, seleccione las casillas de verificación para los diferentes eventos de

NetFlow que desea enviar a los recopiladores y haga clic en Aceptar:



Configuración de clase de tráfico

Resolución de problemas

Paso 1. Puede verificar la configuración desde la CLI de FTD.

1.1. Desde FTD CLI, ingrese a system support diagnostic-cli:

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

1.2 Comprobar la configuración de policy-map:

<#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

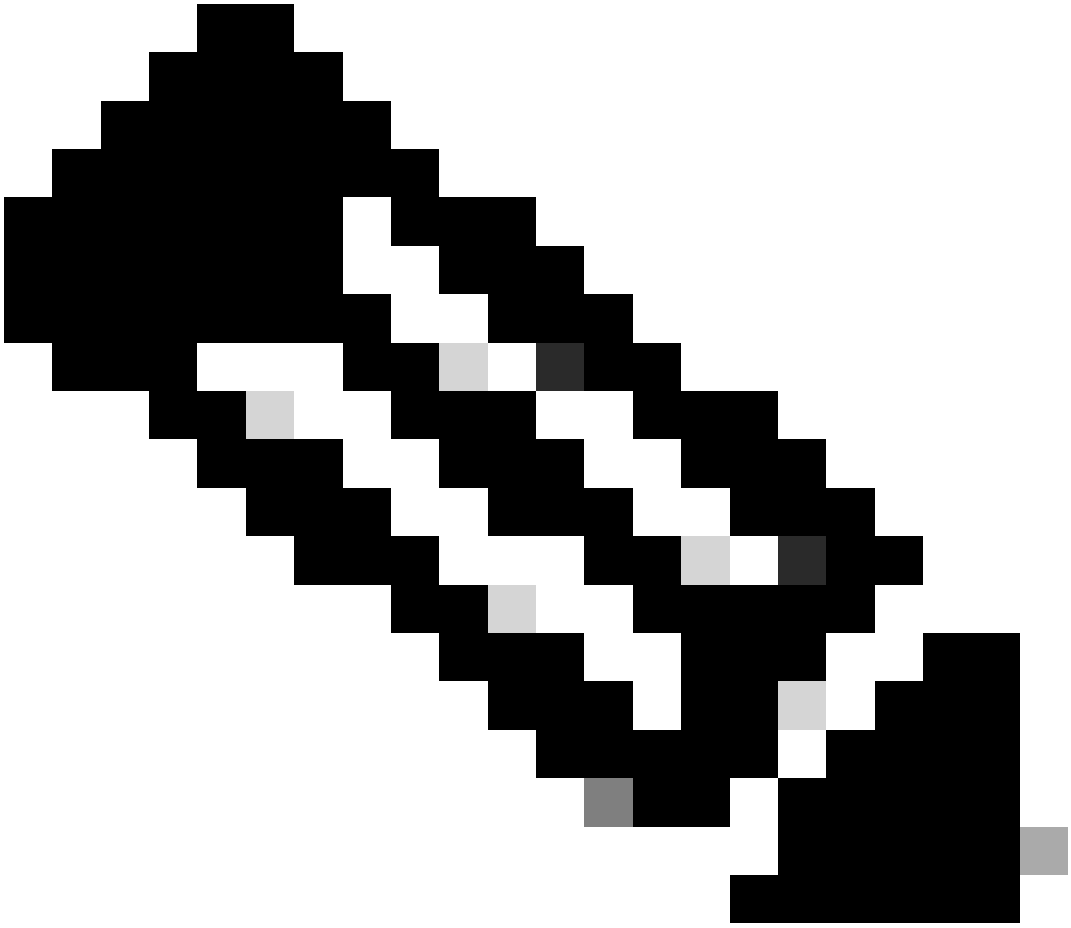
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Comprobar la configuración de exportación de flujo:

<#root>

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

flow-export destination Inside 192.168.31.1 2055



Nota: En este ejemplo, "Inside" es el nombre de la interfaz configurada en el grupo de interfaces denominado Netflow_Export

Paso 2. Verifique el conteo de aciertos para la 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
```

Paso 3. Verificar contadores de Netflow:

<#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
```

Información Relacionada

- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).