在FMC中配置NetFlow

目录

简介

本文档介绍如何在运行7.4或更高版本的Cisco安全防火墙管理中心中配置Netflow。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙管理中心(FMC)
- 思科安全防火墙威胁防御(FTD)
- NetFlow协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 适用于VMWare的安全防火墙管理中心运行7.4.1版
- 安全防火墙运行v7.4.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

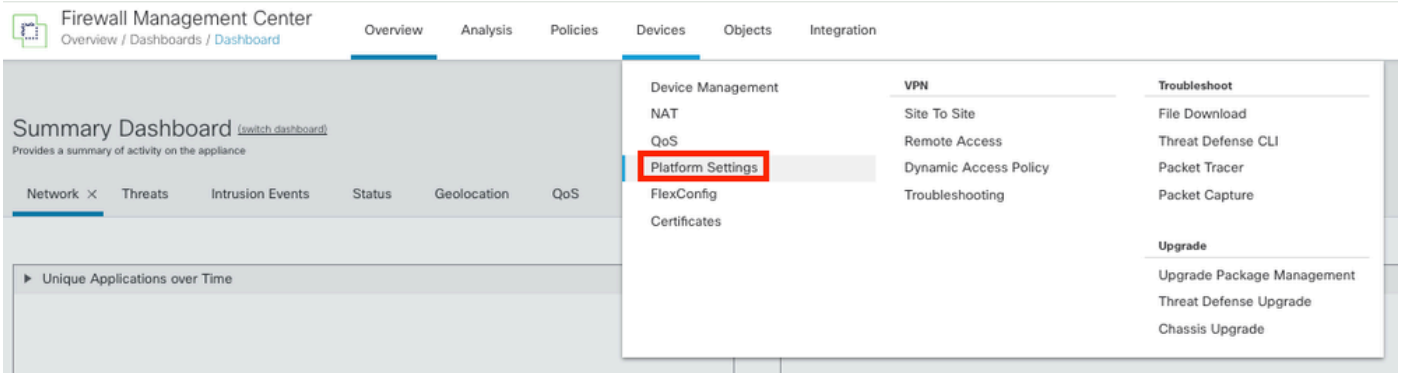
背景信息

本文档的具体要求包括：

- 运行版本7.4或更高版本的思科安全防火墙威胁防御
- 运行版本7.4或更高版本的Cisco安全防火墙管理中心

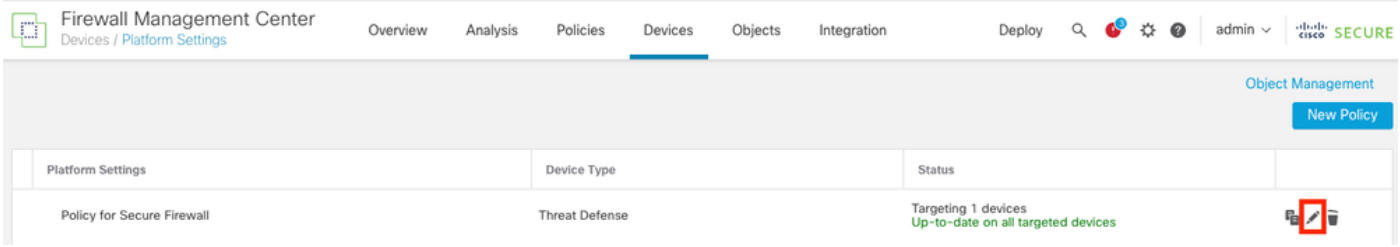
在NetFlow中添加收集器

步骤1:转至Devices > Platform Settings：



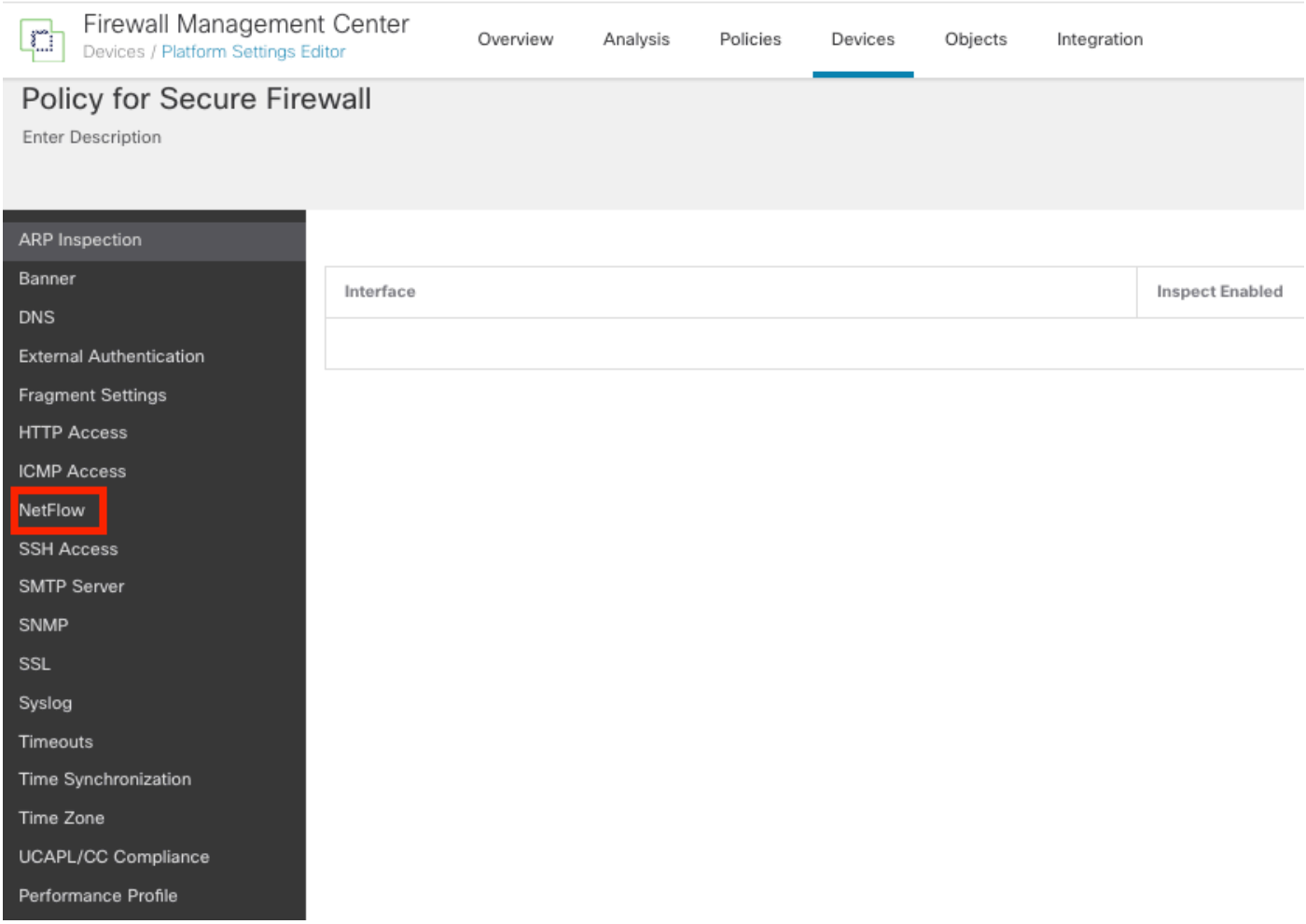
访问平台设置

第二步：编辑分配给监控设备的平台设置策略：



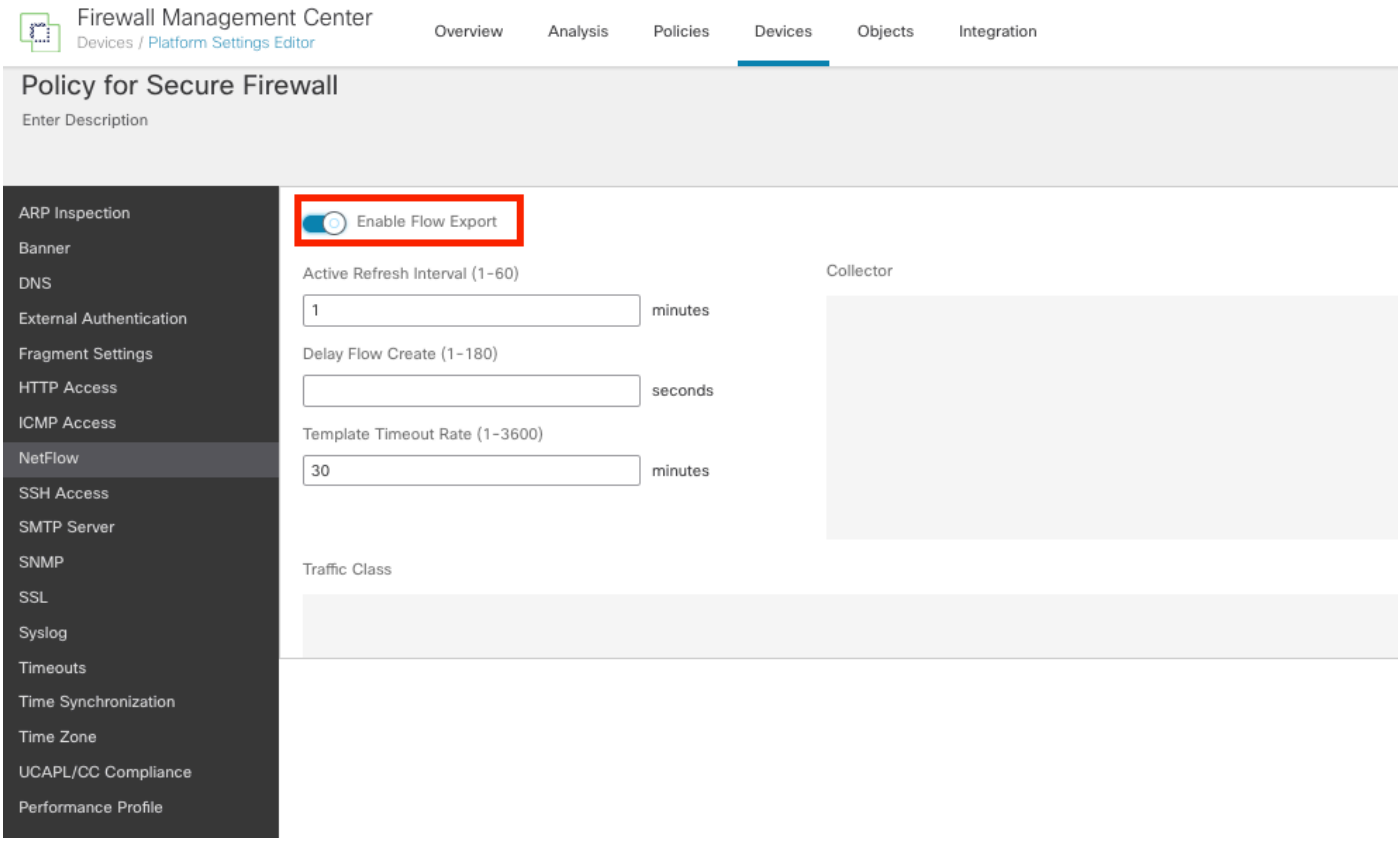
策略版

第三步：选择Netflow：



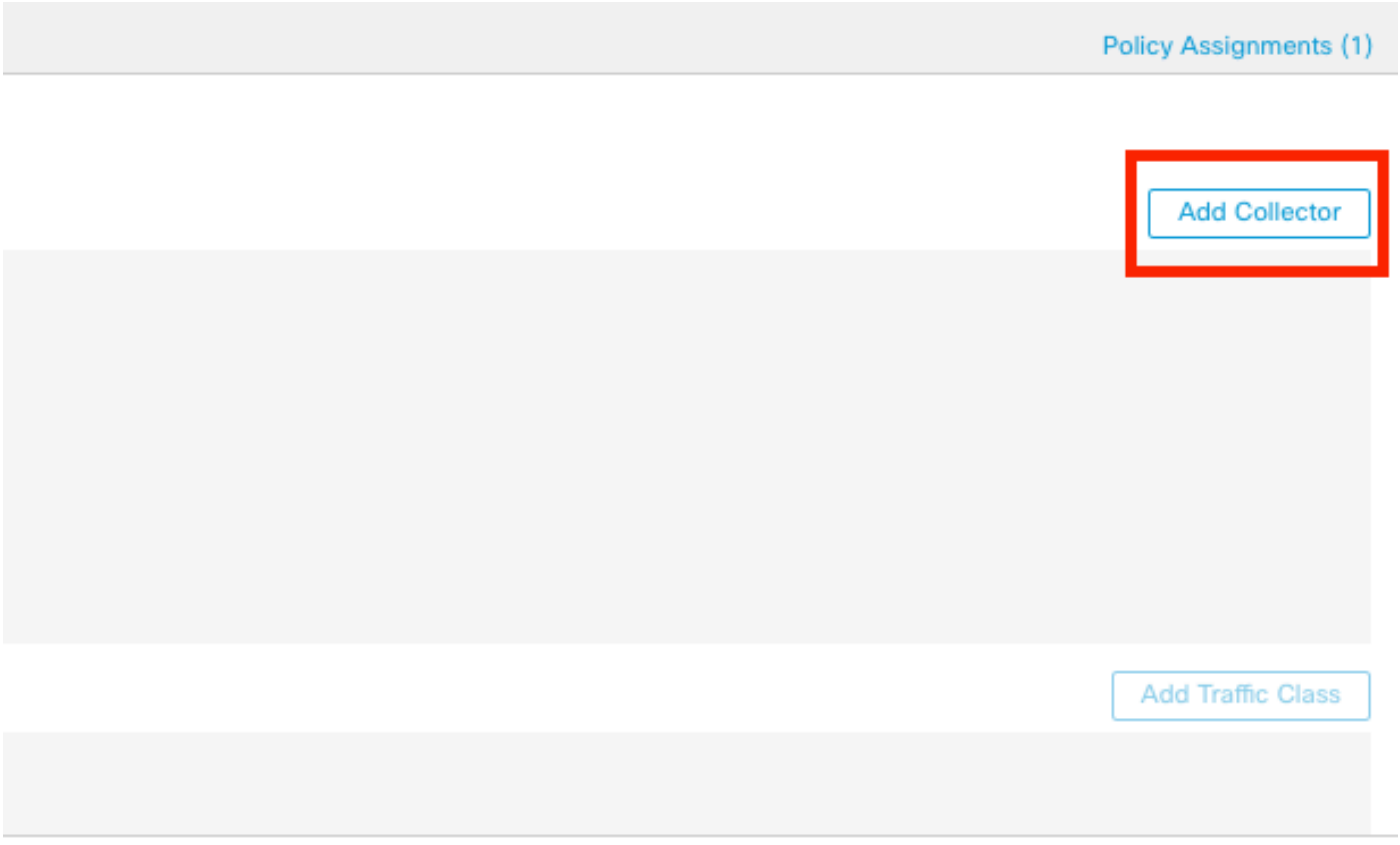
访问NetFlow设置

第四步：启用流导出切换以启用NetFlow数据导出：



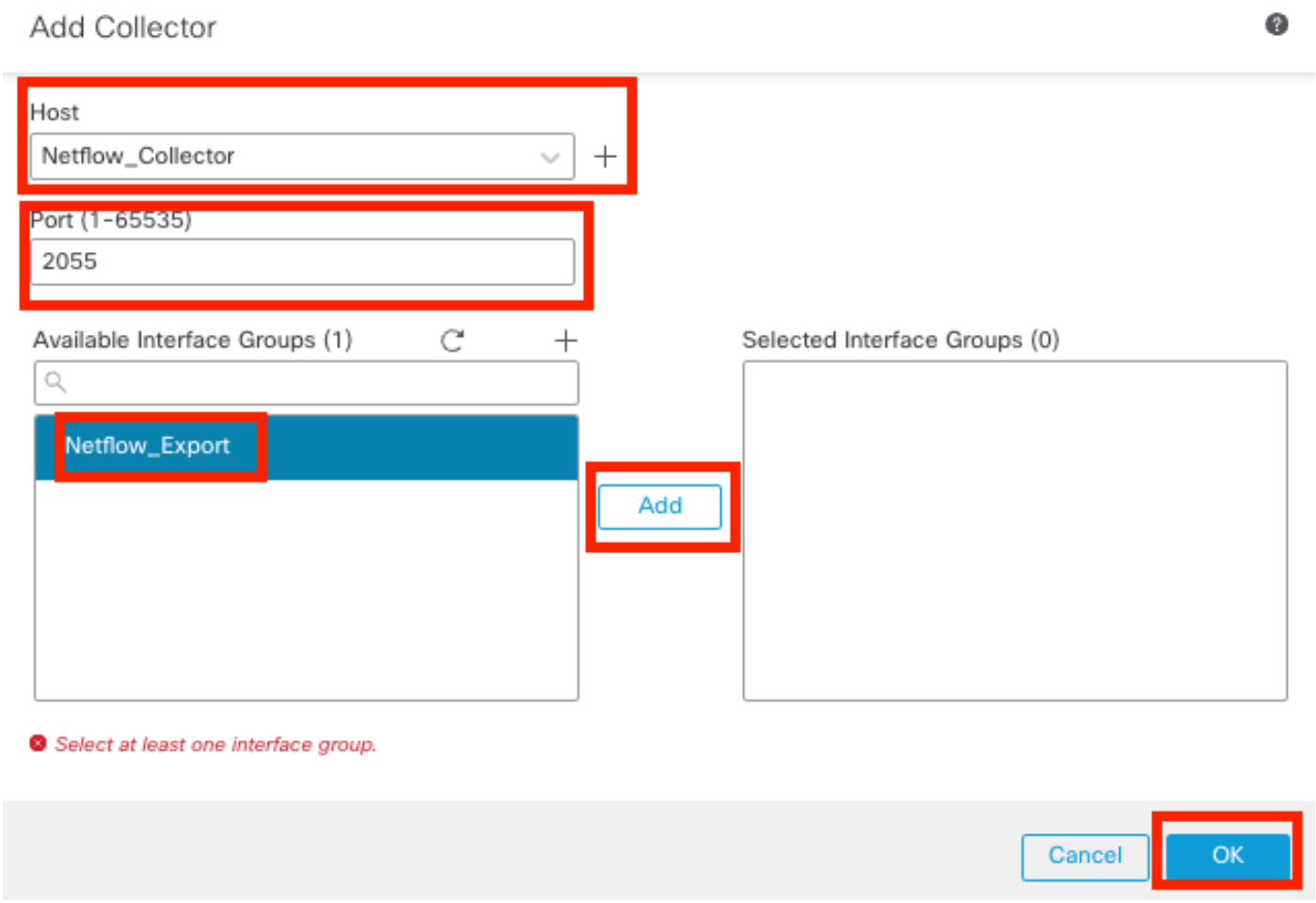
启用NetFlow

第五步：点击Add Collector：



添加收集器

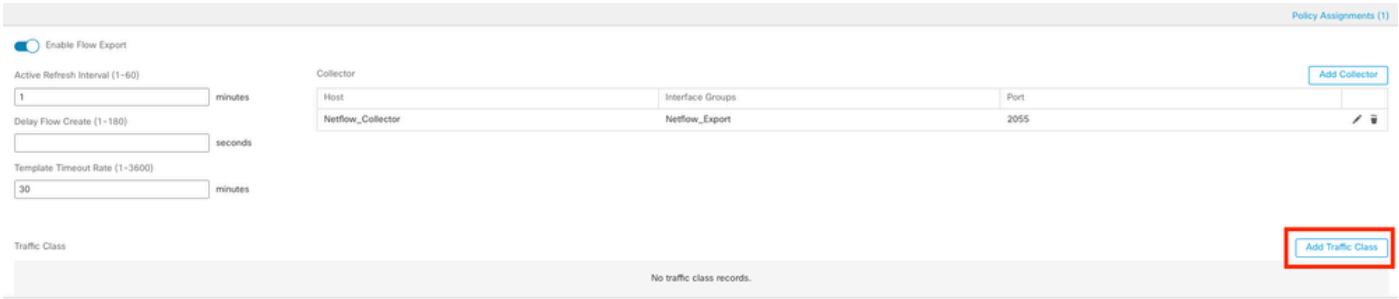
第六步：选择NetFlow事件收集器的收集器主机IP对象（收集器上必须向其发送NetFlow数据包的UDP端口），选择必须访问收集器的接口组，然后单击OK：



收集器设置

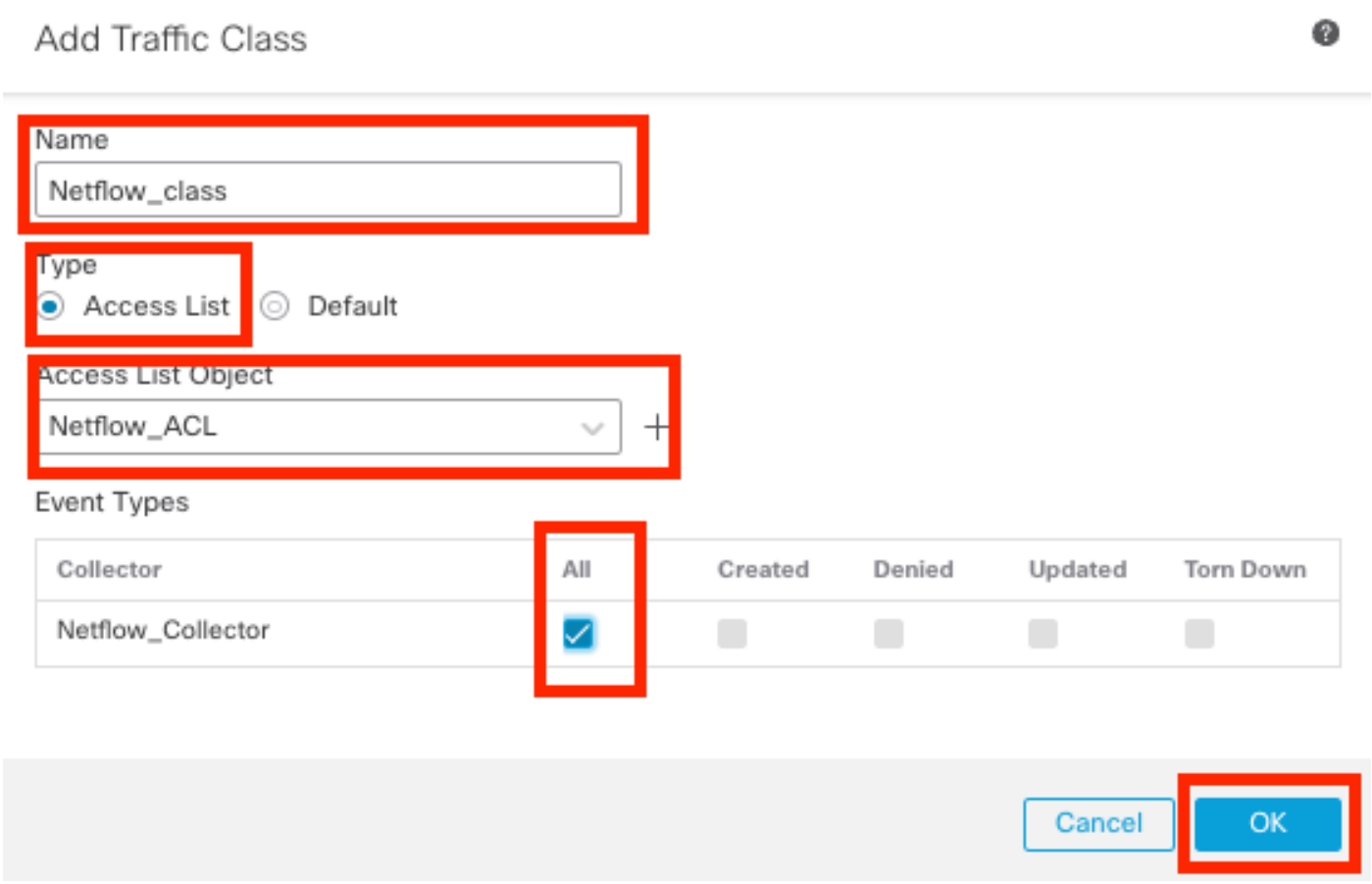
将流量类添加到NetFlow

步骤1:单击Add Traffic Class：



添加流量类

第二步：输入必须与NetFlow事件匹配的流量类的名称字段，用于指定必须与为NetFlow事件捕获的流量匹配的流量类的ACL，选中要发送到收集器的不同NetFlow事件的复选框，然后单击OK：



流量类设置

故障排除

步骤1:您可以从FTD CLI验证配置。

1.1.从FTD CLI输入至system support diagnostic-cli：

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

1.2检查策略映射配置：

<#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

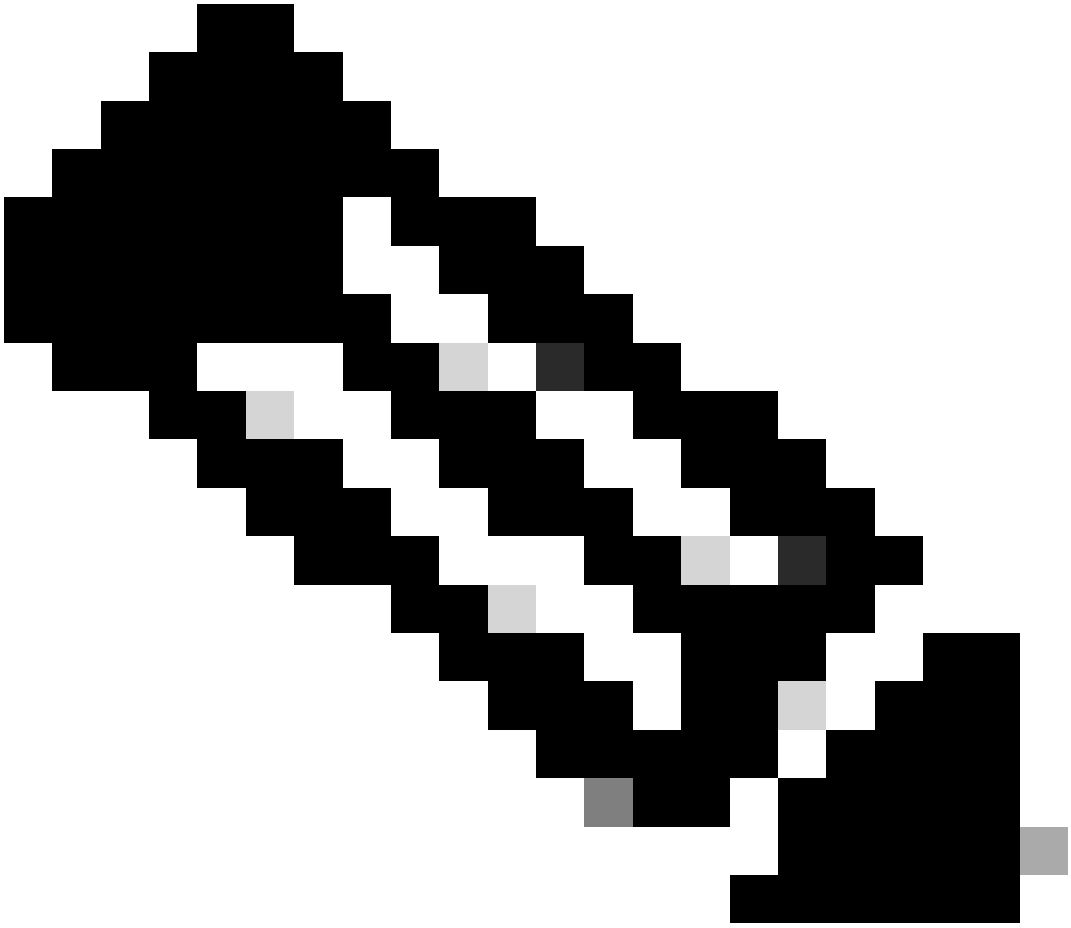
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3.检查flow-export配置：

<#root>

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

flow-export destination Inside 192.168.31.1 2055



注意：在本示例中，“Inside”是名为Netflow_Export的接口组中配置的接口名称

第二步：验证ACL的命中次数：

<#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
```

第三步：验证Netflow计数器：

<#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
```

相关信息

- Cisco安全防火墙管理中心设备配置指南7.4

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。