在FMC中配置NetFlow

目錄

簡介

本文檔介紹如何在運行版本7.4或更高版本的Cisco Secure Firewall Management Center中配置Netflow。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)
- NetFlow通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於VMWare的安全防火牆管理中心執行7.4.1版
- 安全防火牆運行v7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

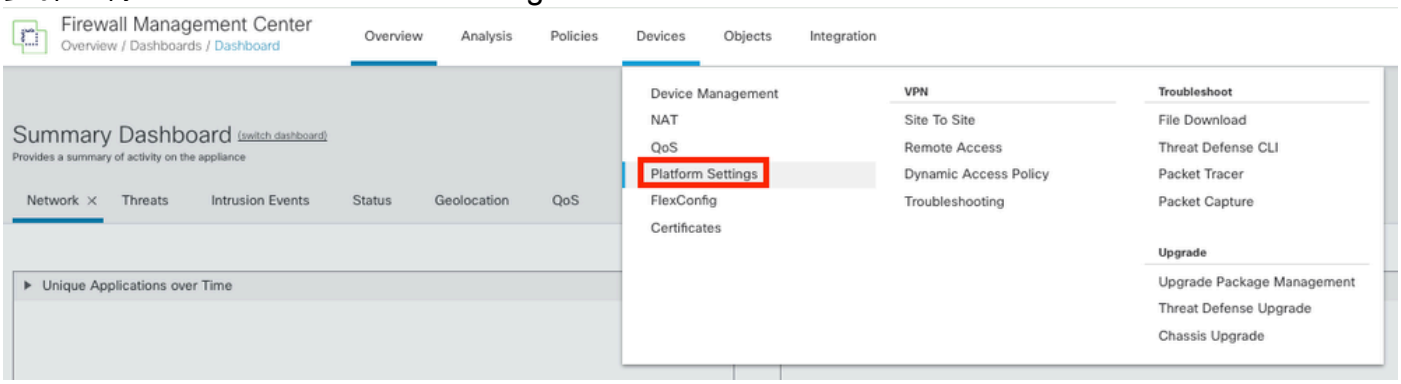
背景資訊

本文檔的特定要求包括：

- 運行版本7.4或更高版本的思科安全防火牆威脅防禦
- 運行版本7.4或更高版本的Cisco Secure Firewall Management Center

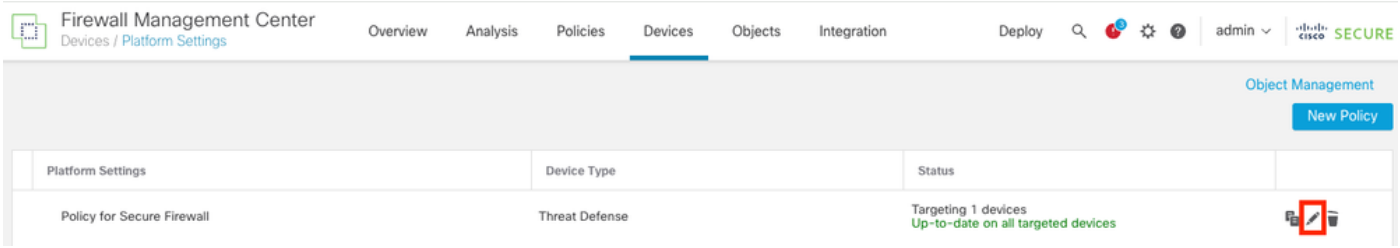
在NetFlow中增加收集器

步驟 1.轉至Devices > Platform Settings：



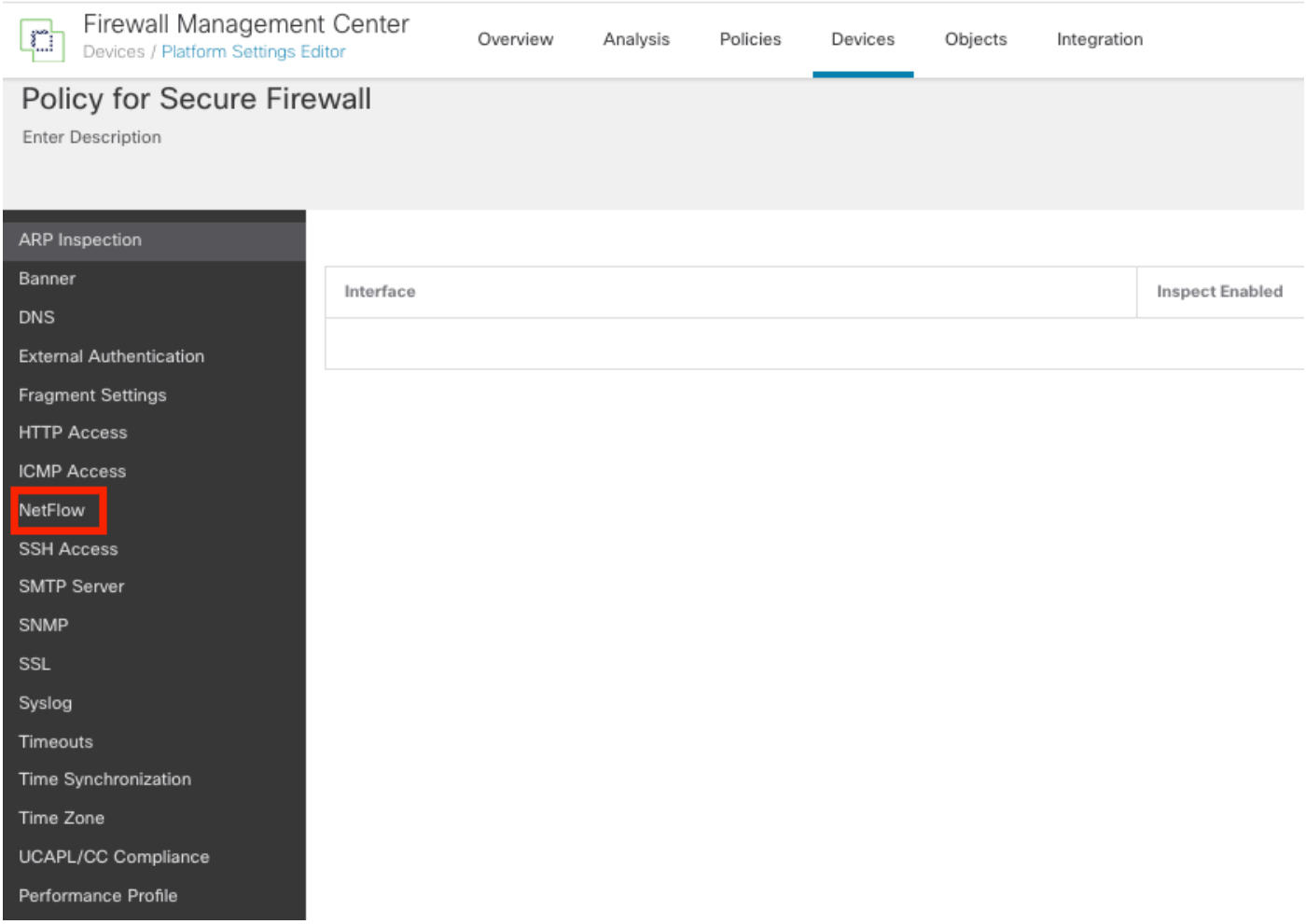
存取平台設定

步驟 2.編輯分配給監控裝置的平台設定策略：



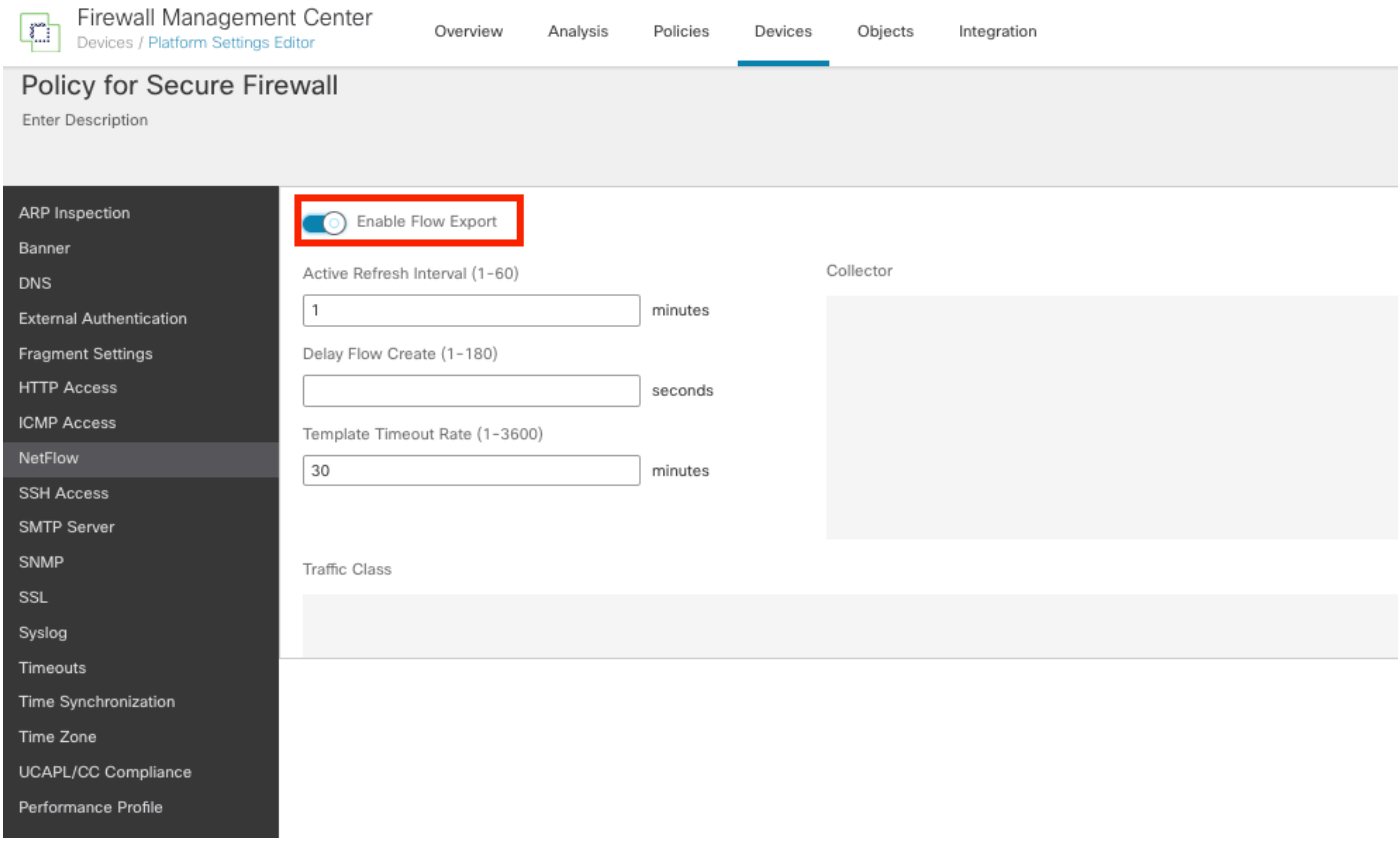
策略版本

步驟 3.選擇Netflow：



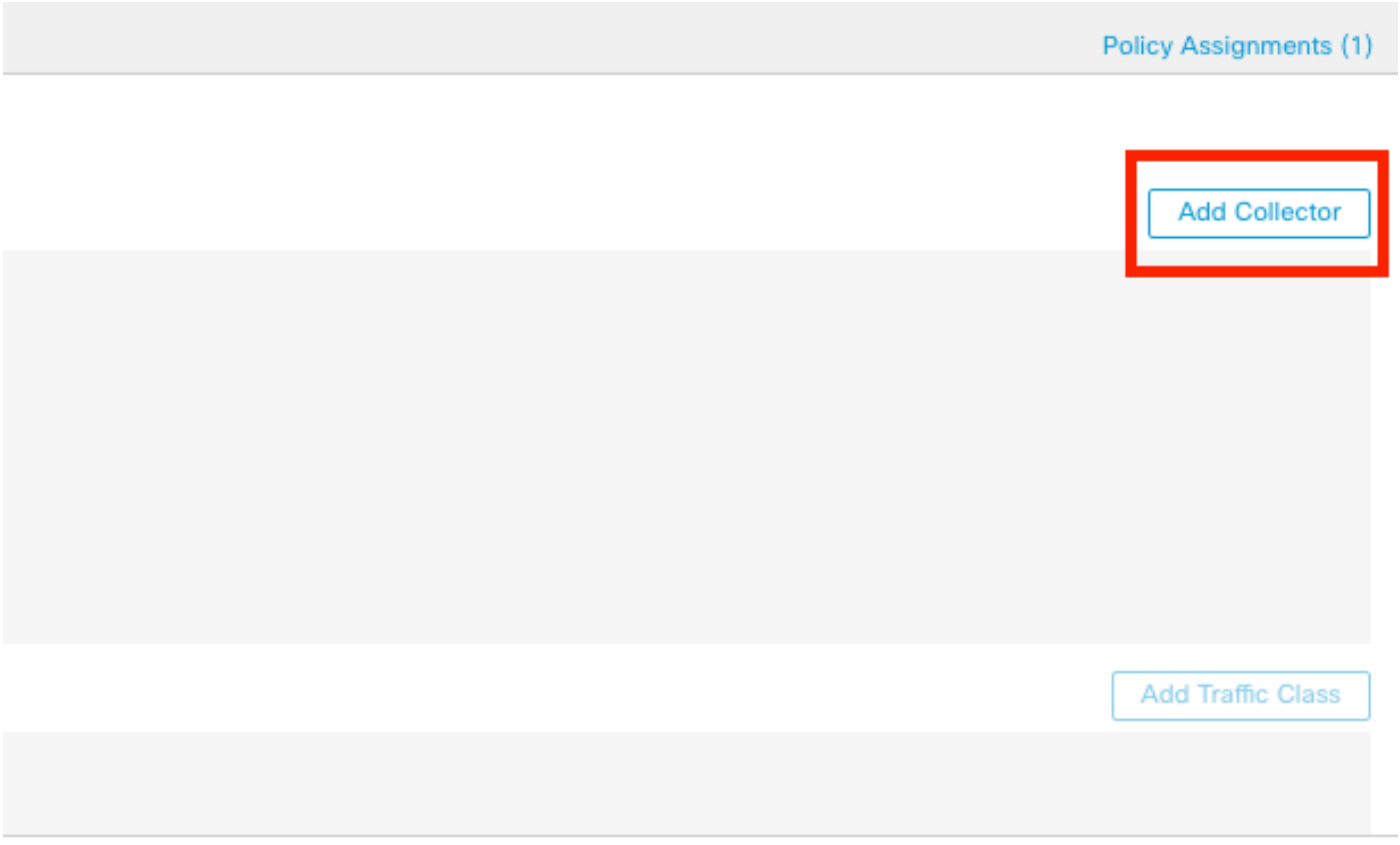
訪問NetFlow設定

步驟 4.啟用流導出切換以啟用NetFlow資料導出：



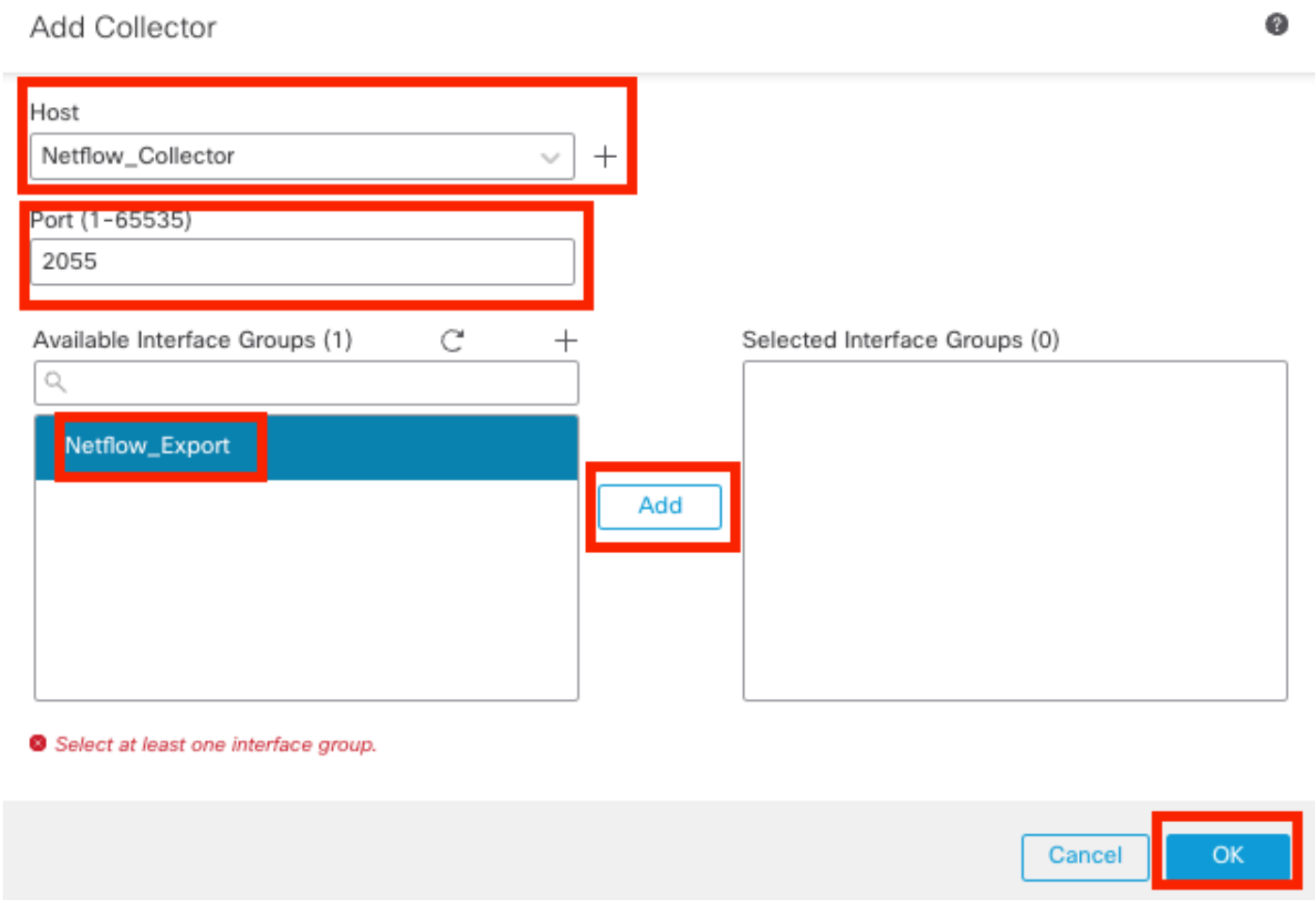
啟用NetFlow

步驟 5.按一下Add Collector：



新增收集器

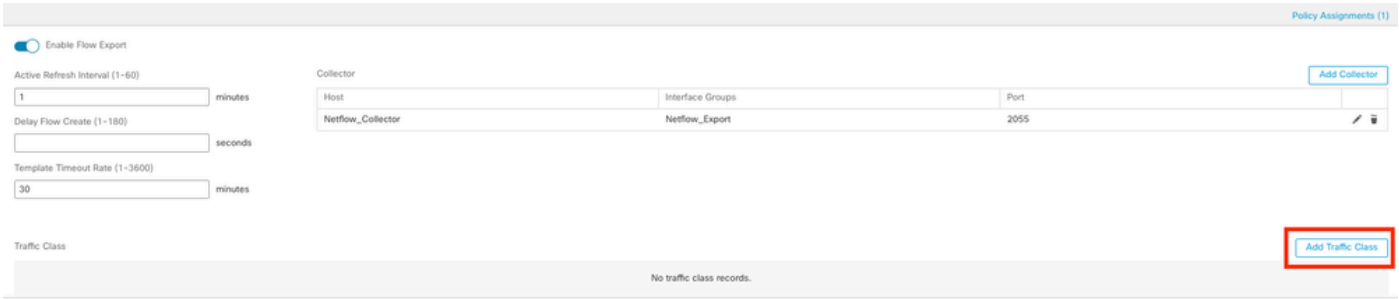
步驟 6.選擇NetFlow事件收集器的收集器主機IP對象、收集器上必須向其傳送NetFlow資料包的UDP埠、選擇必須透過該收集器訪問的介面組，然後按一下OK：



收集器設定

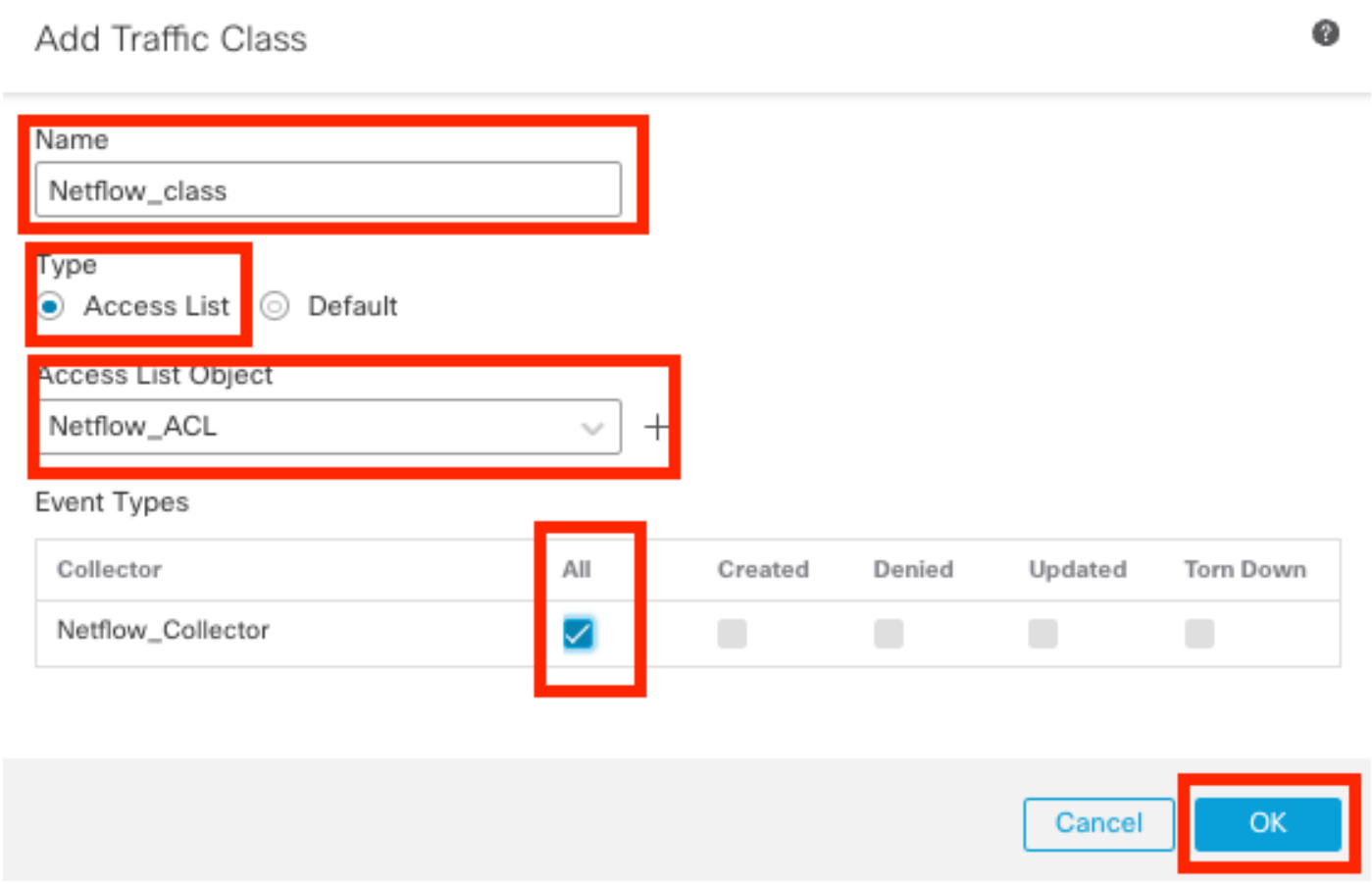
向NetFlow增加流量類

步驟 1.按一下Add Traffic Class：



增加流量類

步驟 2.輸入必須與NetFlow事件匹配的流量類的名稱欄位，用於指定必須與NetFlow事件捕獲的流量匹配的流量類的ACL，選中要傳送到收集器的不同NetFlow事件的覈取方塊，然後按一下OK：



流量類設定

疑難排解

步驟 1.您可以從FTD CLI驗證設定。

1.1.從FTD CLI輸入系統支援diagnostic-cli：

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

1.2檢查策略對映配置：

<#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

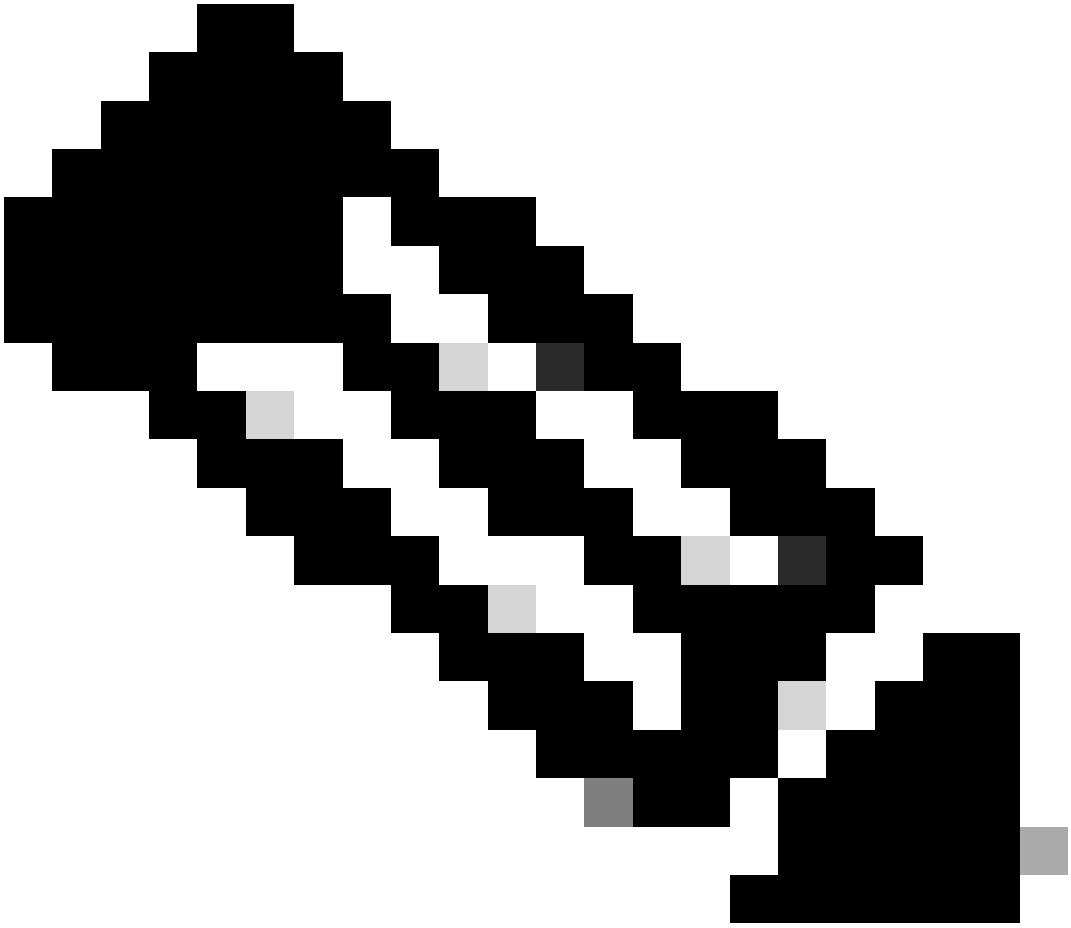
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3.檢查流導出配置：

<#root>

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

flow-export destination Inside 192.168.31.1 2055



注意：在本示例中，「Inside」是在名為Netflow_Export的介面組中配置的介面名稱

步驟 2.檢驗ACL的命中數：

<#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
```

步驟 3.驗證Netflow計數器：

<#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
```

相關資訊

- 思科安全防火牆管理中心裝置配置指南7.4

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。