FMCでのNetFlowの設定

内容

はじめに

このドキュメントでは、バージョン7.4以降を実行するCisco Secure Firewall Management Center(FMC)でNetFlowを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Threat Defense(FTD)
- NetFlowプロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Firewall Management Center for VMWareはv7.4.1を実行
- セキュアファイアウォールv7.4.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

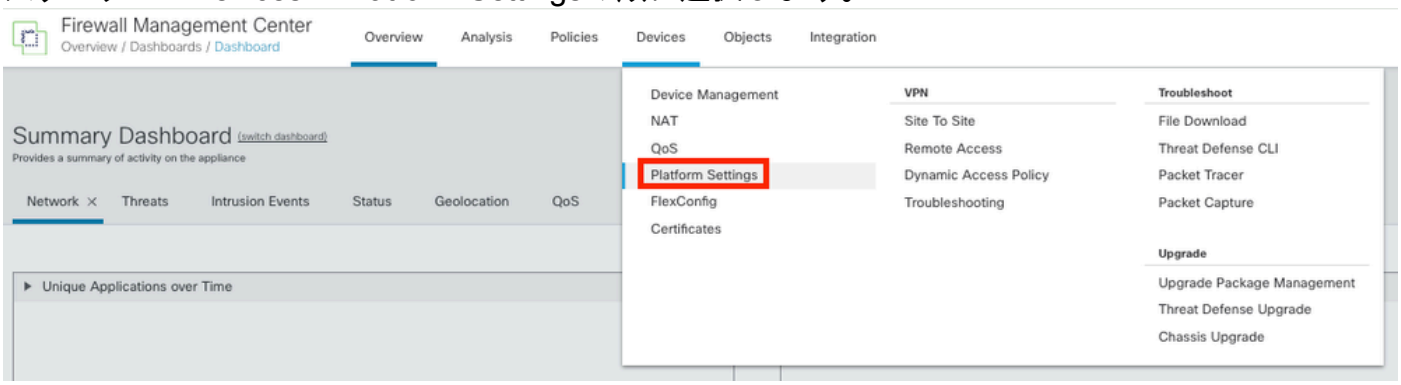
背景説明

このドキュメントに関する特定の要件は次のとおりです。

- バージョン7.4以降を実行しているCisco Secure Firewall Threat Defense
- バージョン7.4以降を実行しているCisco Secure Firewall Management Center(FMC)

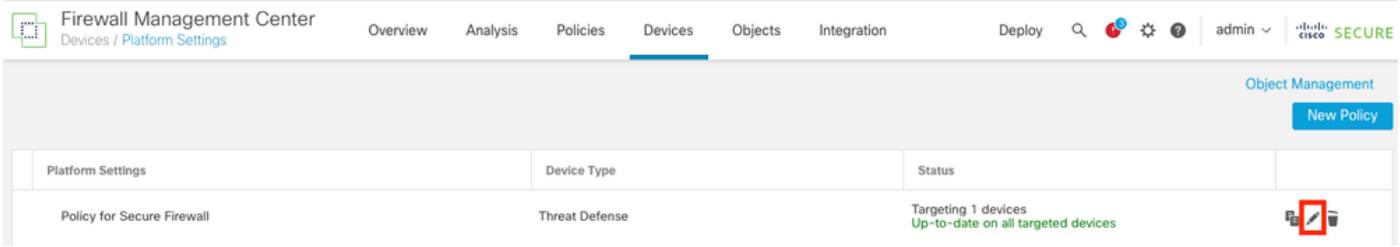
NetFlowでのコレクタの追加

ステップ 1：Devices > Platform Settingsの順に選択します。



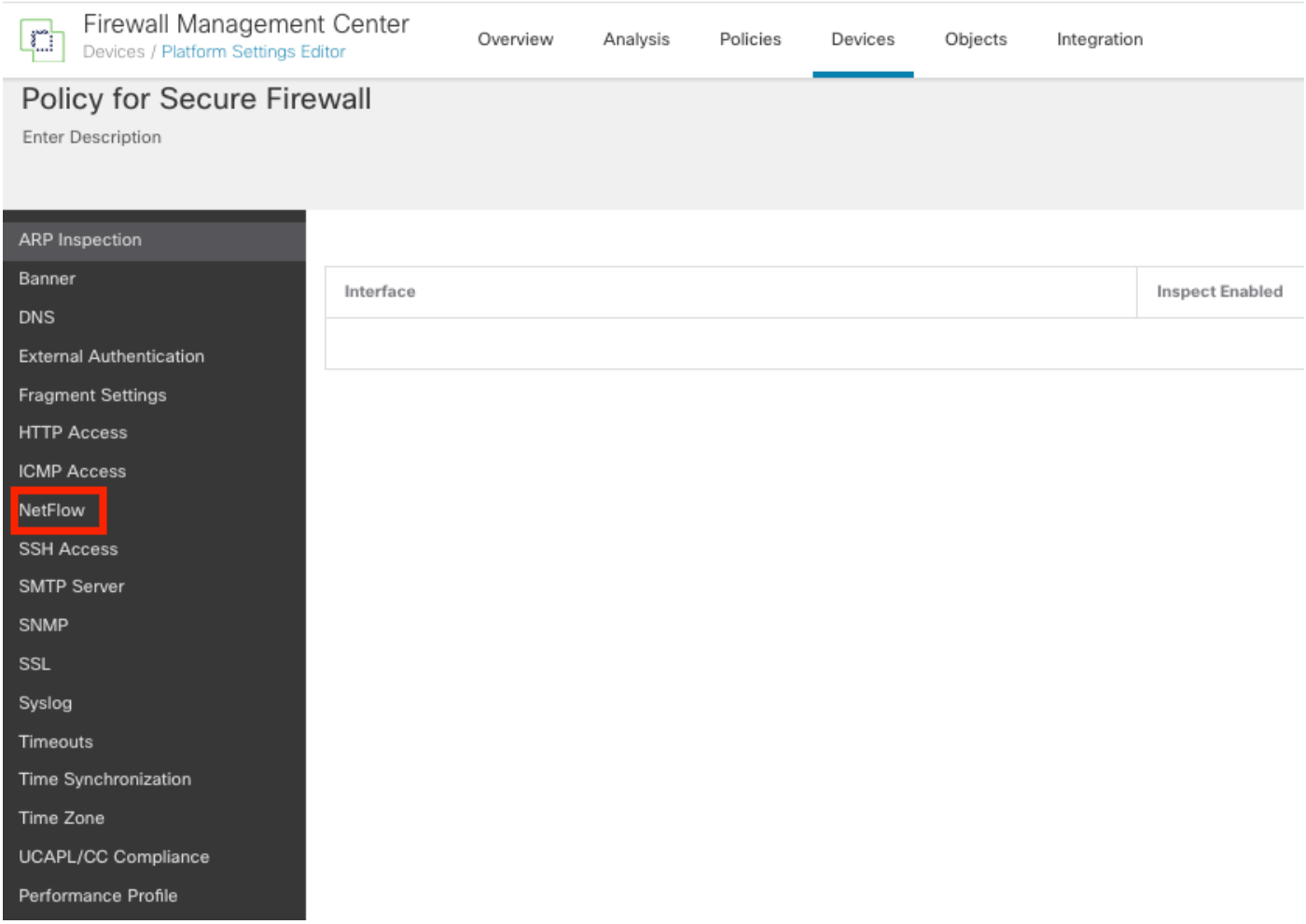
プラットフォーム設定へのアクセス

ステップ 2：モニタデバイスに割り当てられたプラットフォーム設定ポリシーを編集します。



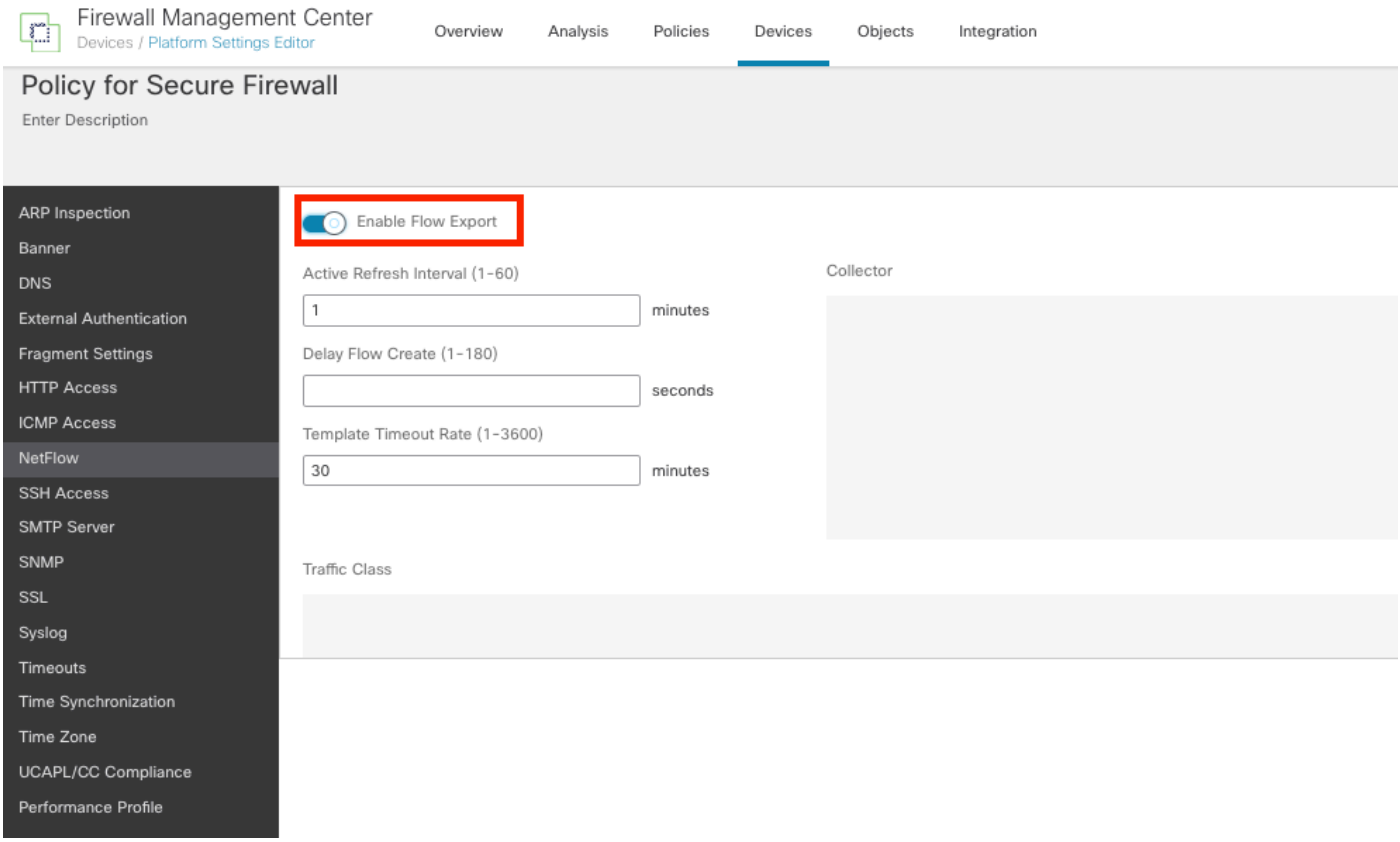
ポリシー版

ステップ 3：Netflowを選択します。



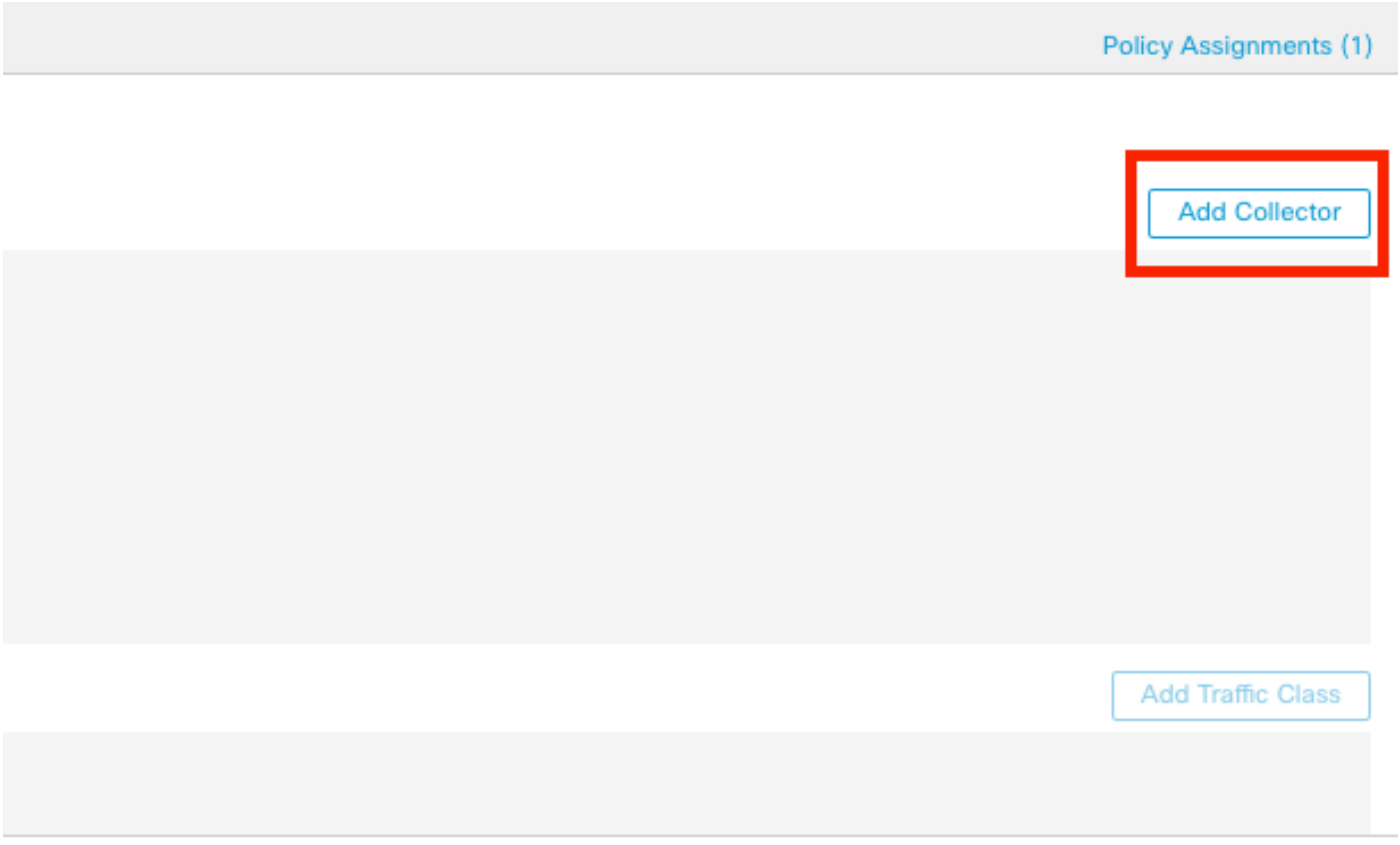
NetFlow設定へのアクセス

ステップ 4：NetFlowデータエクスポートを有効にするには、フローエクスポートの切り替えを有効にします。



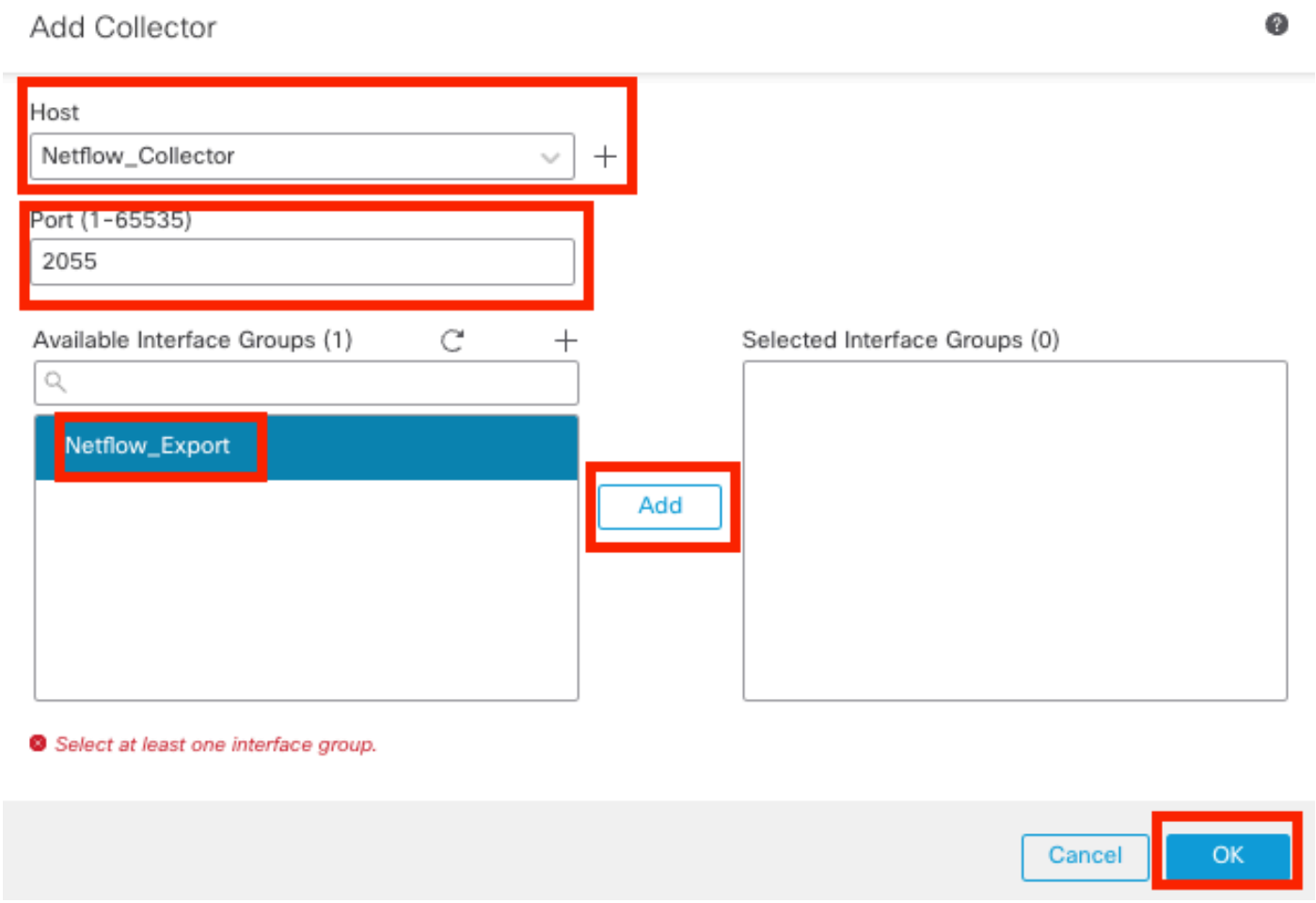
NetFlowの有効化

ステップ 5：Add Collectorをクリックします。



コレクタの追加

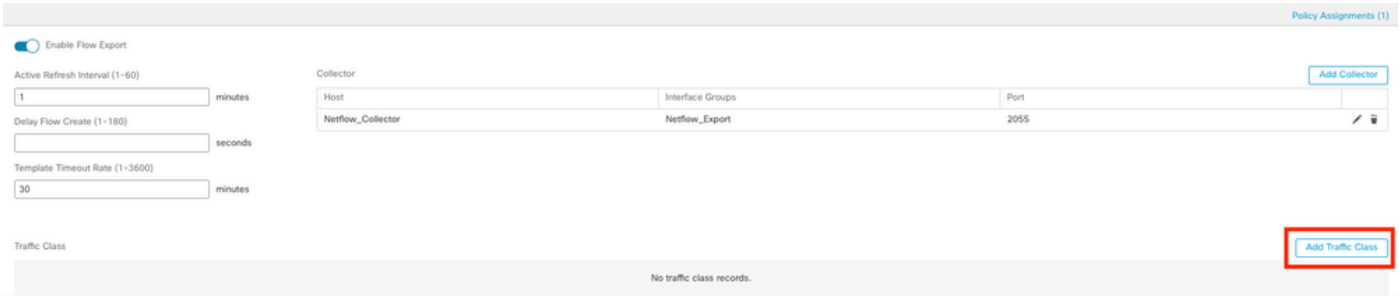
手順 6：NetFlowイベントコレクタのコレクタホストIPオブジェクト、NetFlowパケットの送信先となるコレクタのUDPポートを選択し、コレクタに到達するために経由するインターフェイスグループを選択して、OKをクリックします。



コレクタの設定

NetFlowへのトラフィッククラスの追加

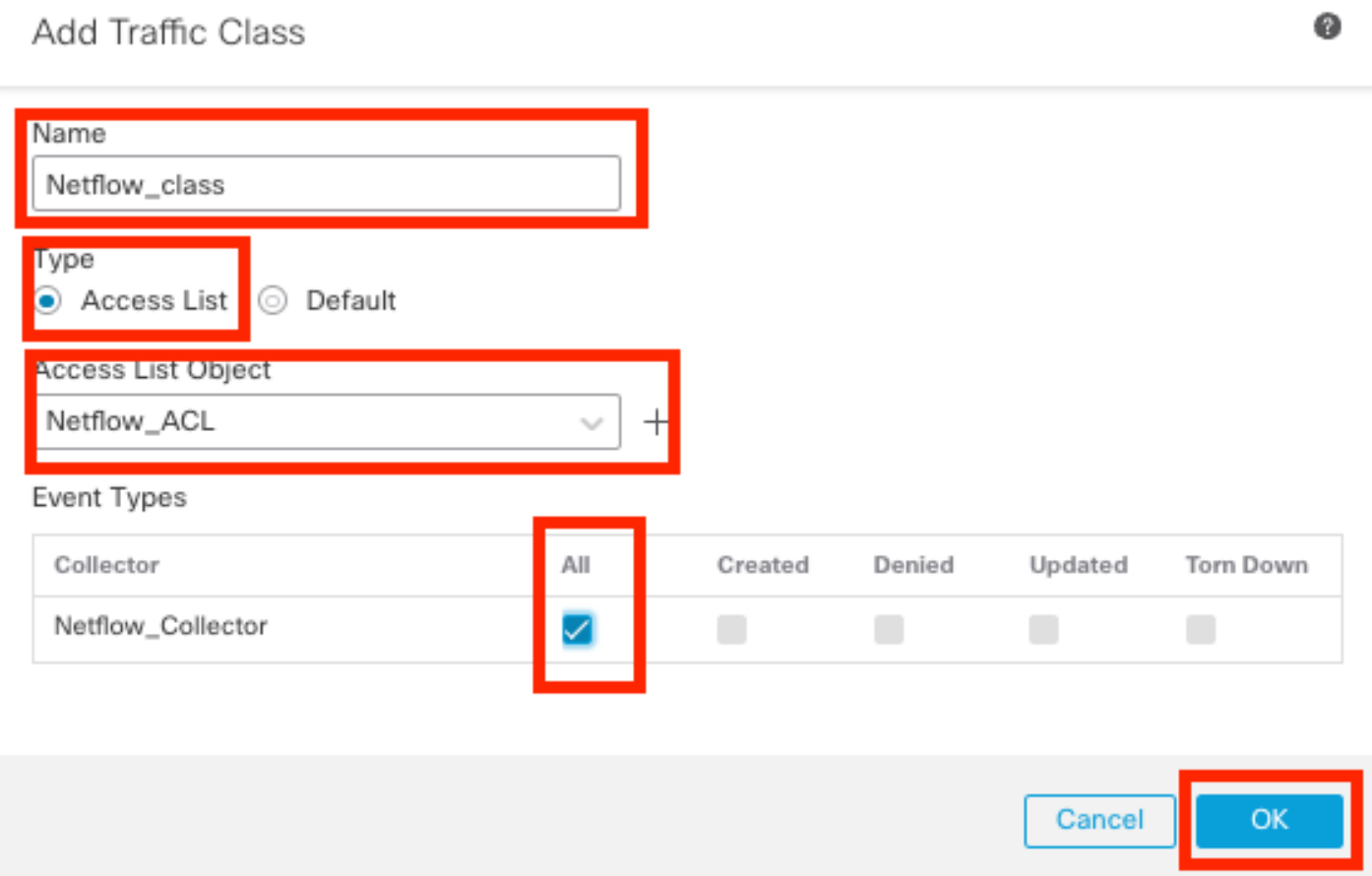
ステップ 1：Add Traffic Classをクリックします。



トラフィッククラスの追加

ステップ 2：NetFlowイベントに一致する必要があるトラフィッククラスの名前フィールドを入力し、ACLを入力して、NetFlowイベント用にキャプチャされたトラフィックに一致する必要があるトラフィッククラスを指定し、コレクタに送信するさまざまなNetFlowイベントのチェックボ

ックスを選択して、OKをクリックします。



トラフィッククラスの設定

トラブルシューティング

ステップ 1：FTD CLIから設定を確認できます。

1.1. FTDのCLIで、system support diagnostic-cliと入力します。

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

1.2ポリシーマップ設定のチェック：

<#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

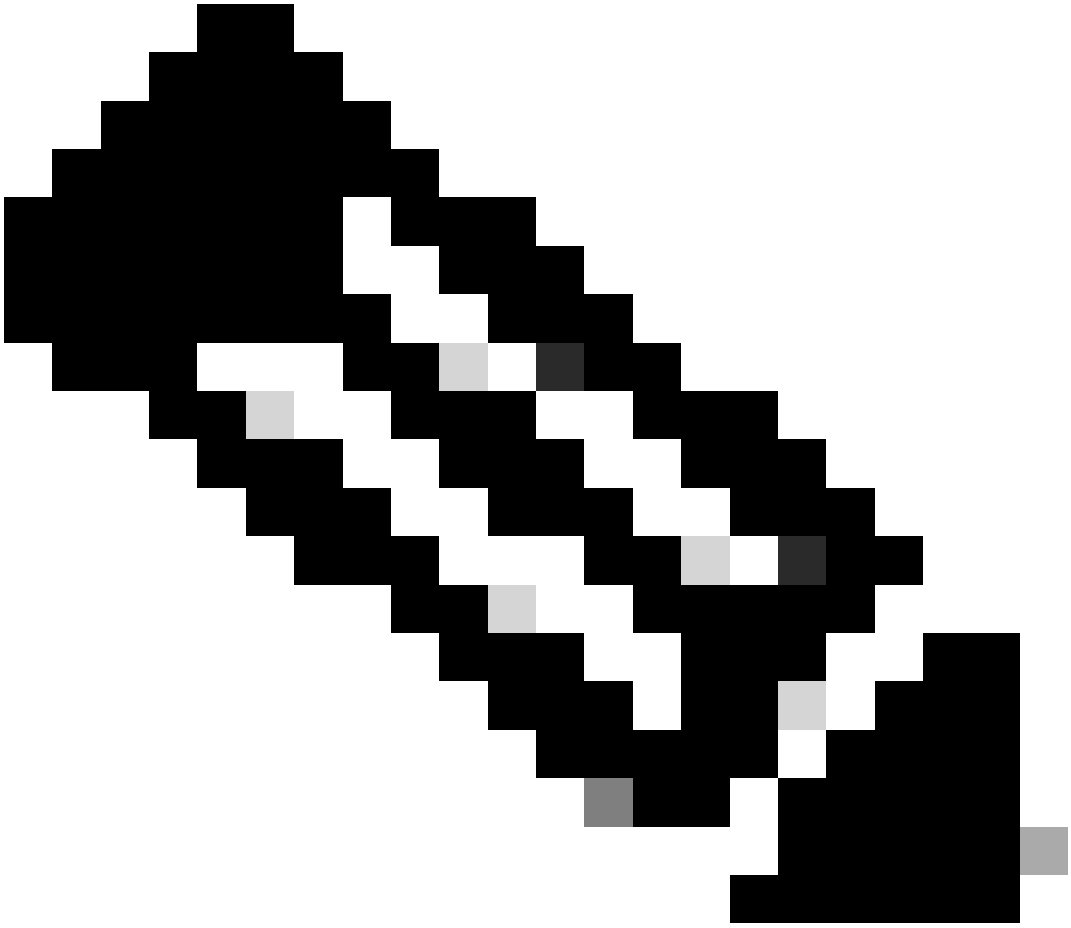
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3.フローエクスポート設定を確認します。

<#root>

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

flow-export destination Inside 192.168.31.1 2055



注：この例で、「Inside」はNetflow_Exportというインターフェイスグループで設定されたインターフェイスの名前です

ステップ 2：ACLのヒットカウントを確認します。

<#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
```

ステップ 3：Netflowカウンタを確認します。

<#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
```

関連情報

- Cisco Secure Firewall Management Centerデバイス設定ガイド、7.4

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。