# FMC에서 NetFlow 구성

## 목차



## 소개

이 문서에서는 버전 7.4 이상을 실행하는 Cisco Secure Firewall Management Center에서 Netflow를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Secure Firewall Management Center for VMWare 실행 v7.4.1
- 보안 방화벽 실행 v7.4.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

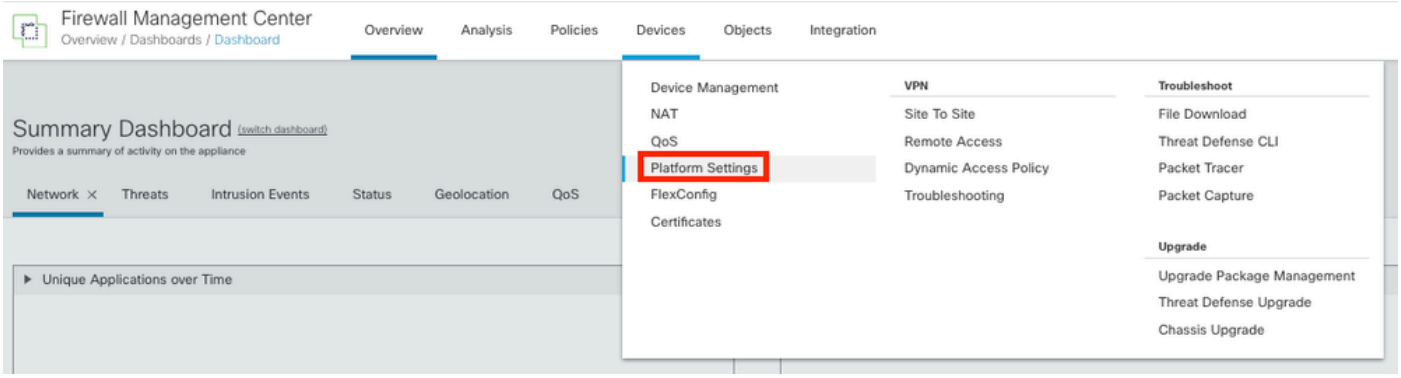
## 배경 정보

이 문서의 구체적인 요구 사항은 다음과 같습니다.

- 버전 7.4 이상을 실행하는 Cisco Secure Firewall Threat Defense
- 버전 7.4 이상을 실행하는 Cisco Secure Firewall Management Center

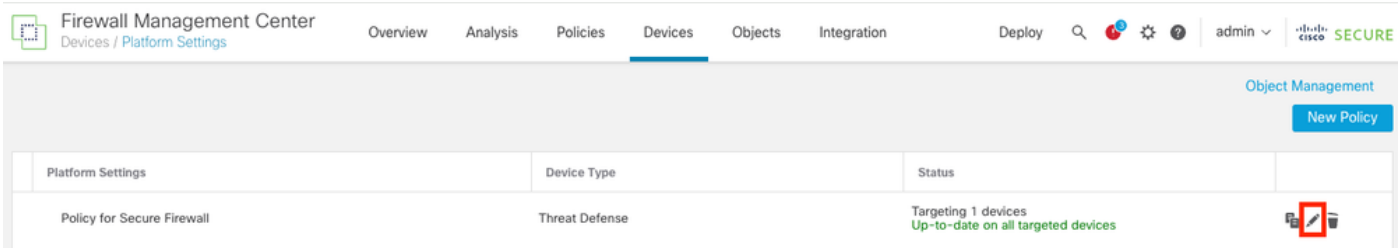
## NetFlow에서 컬렉터 추가

1단계. Devices > Platform Settings로 이동합니다.



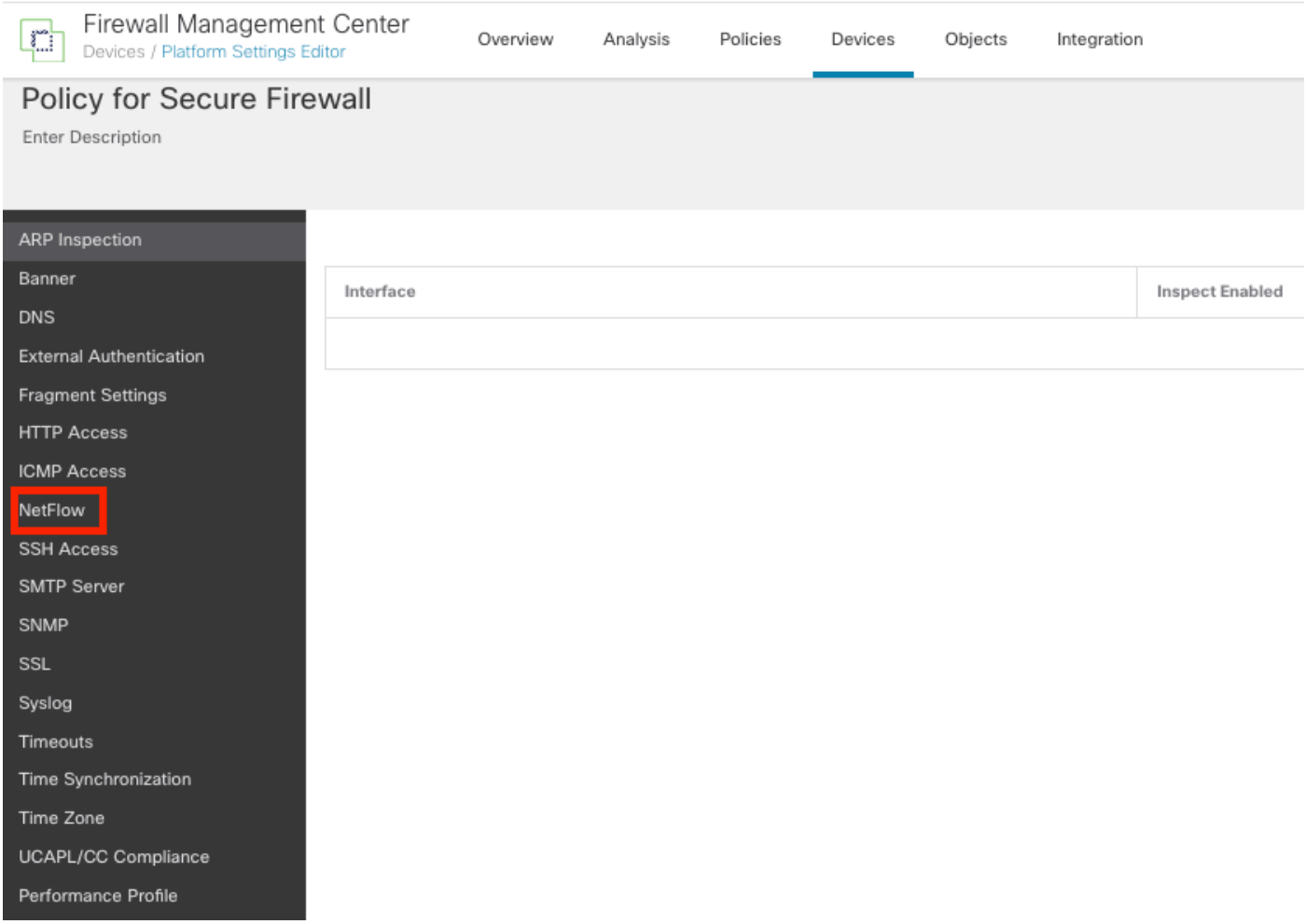

플랫폼 설정 액세스

2단계. 모니터 디바이스에 할당된 플랫폼 설정 정책을 수정합니다.



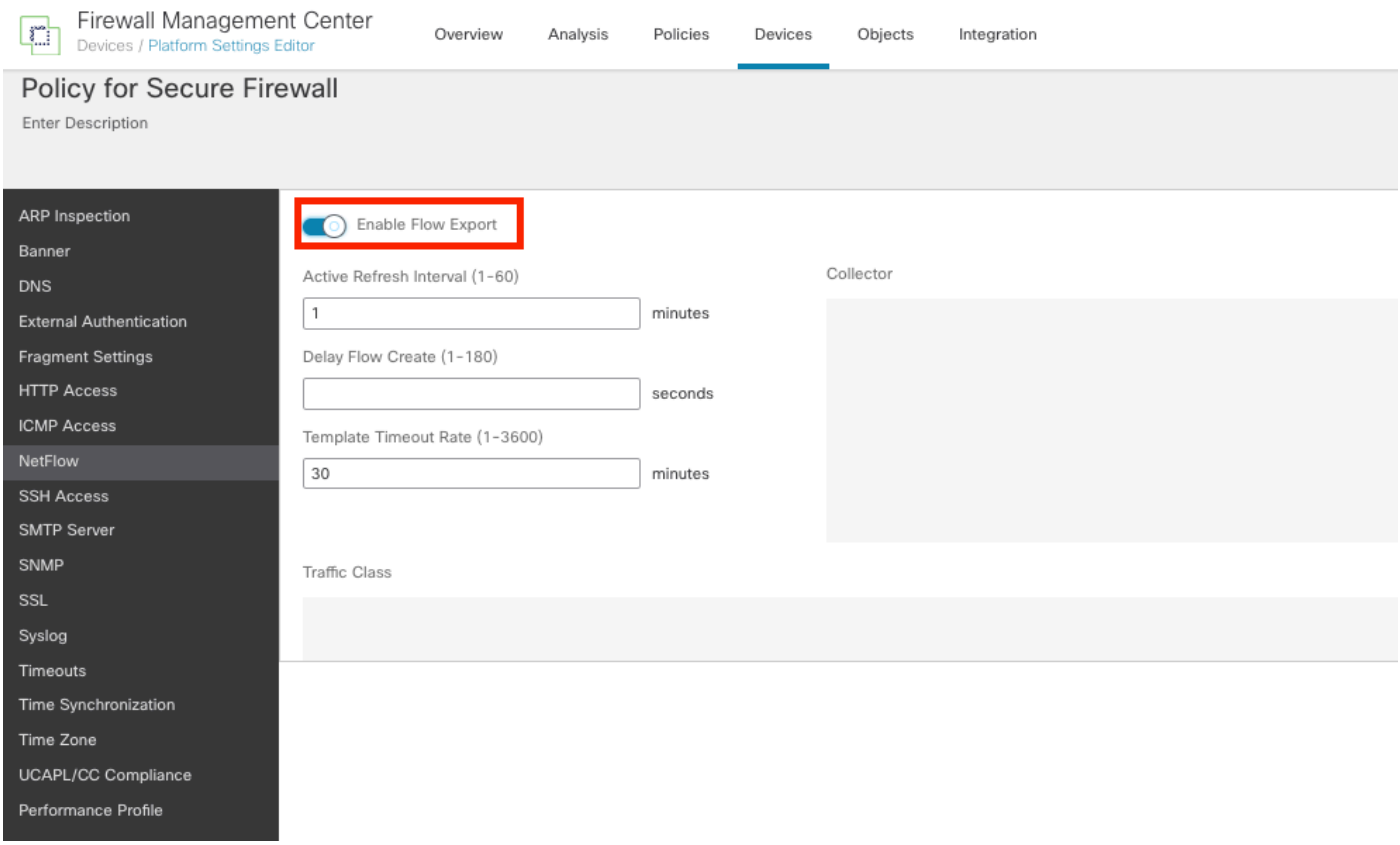

정책 버전

3단계. Netflow를 선택합니다.



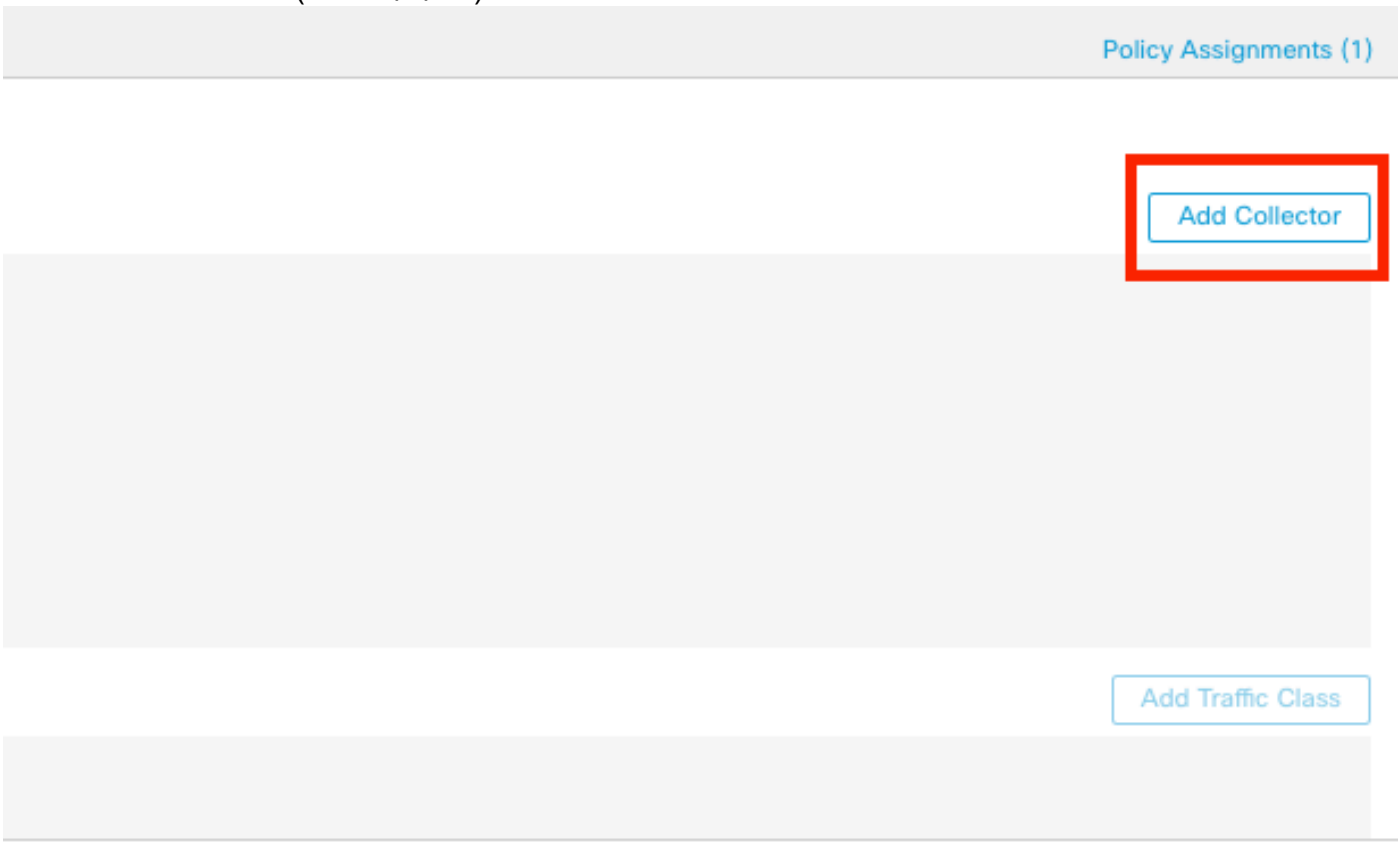

NetFlow 설정 액세스

4단계. NetFlow 데이터 내보내기를 활성화하려면 Flow Export 토글 활성화:



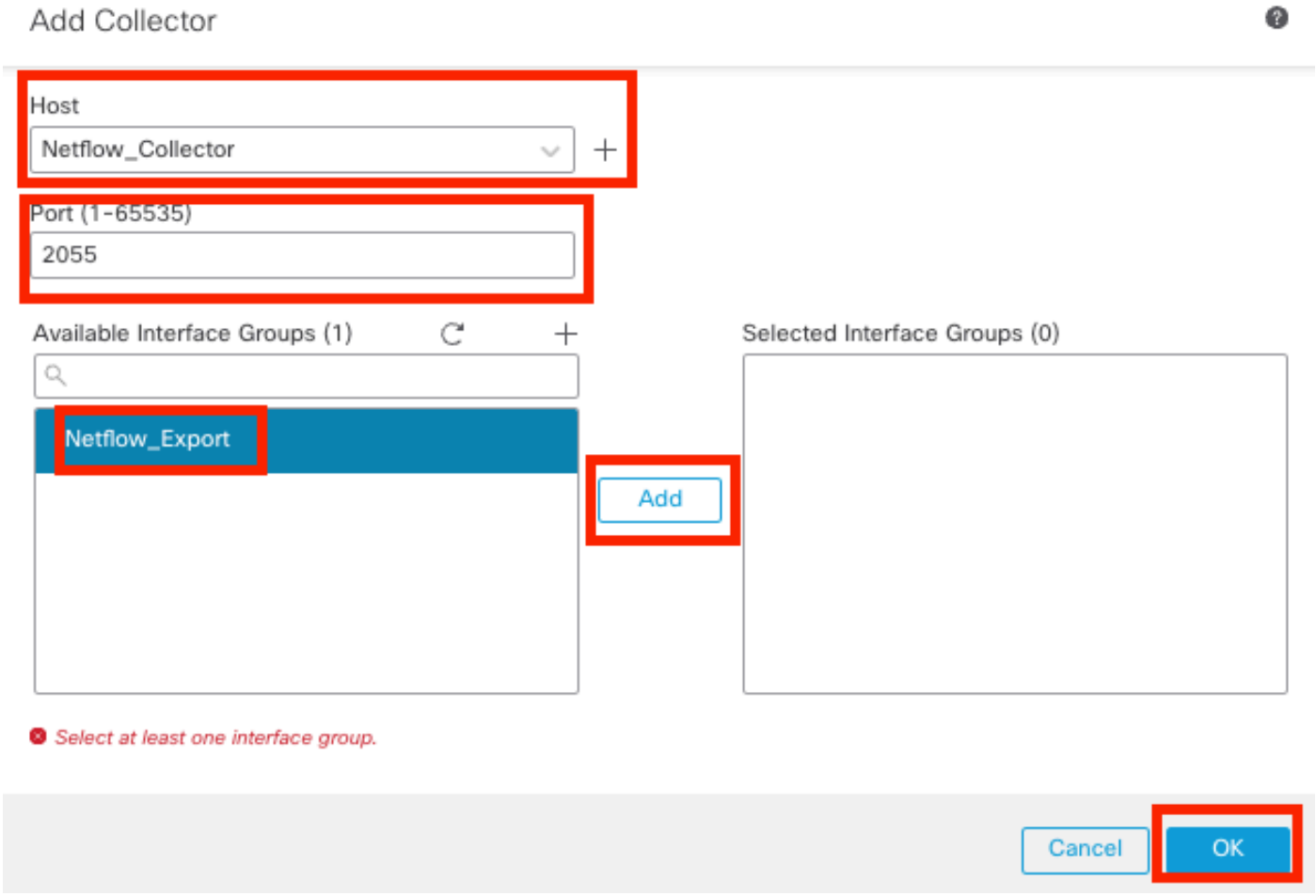

NetFlow 활성화

5단계. Add Collector(컬렉터 추가)를 클릭합니다.




컬렉터 추가

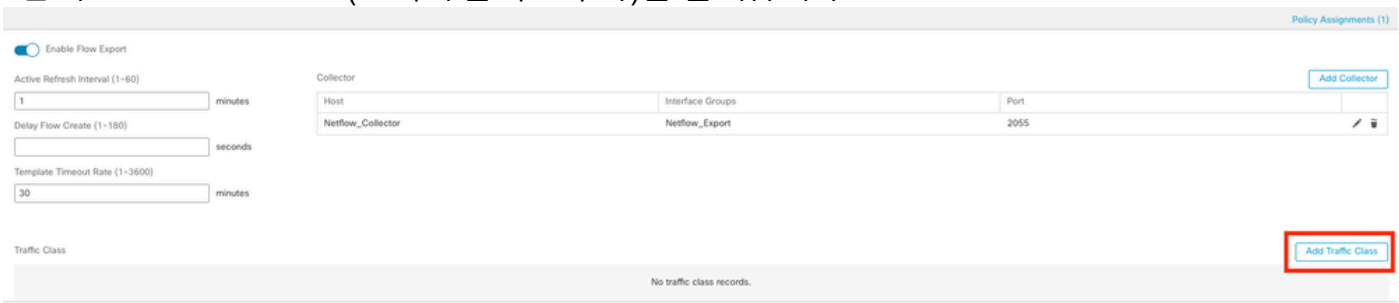
6단계. NetFlow 이벤트 컬렉터의 컬렉터 호스트 IP 객체, NetFlow 패킷을 전송해야 하는 컬렉터의 UDP 포트, 컬렉터에 연결할 인터페이스 그룹을 선택하고 OK를 클릭합니다.




컬렉터 설정

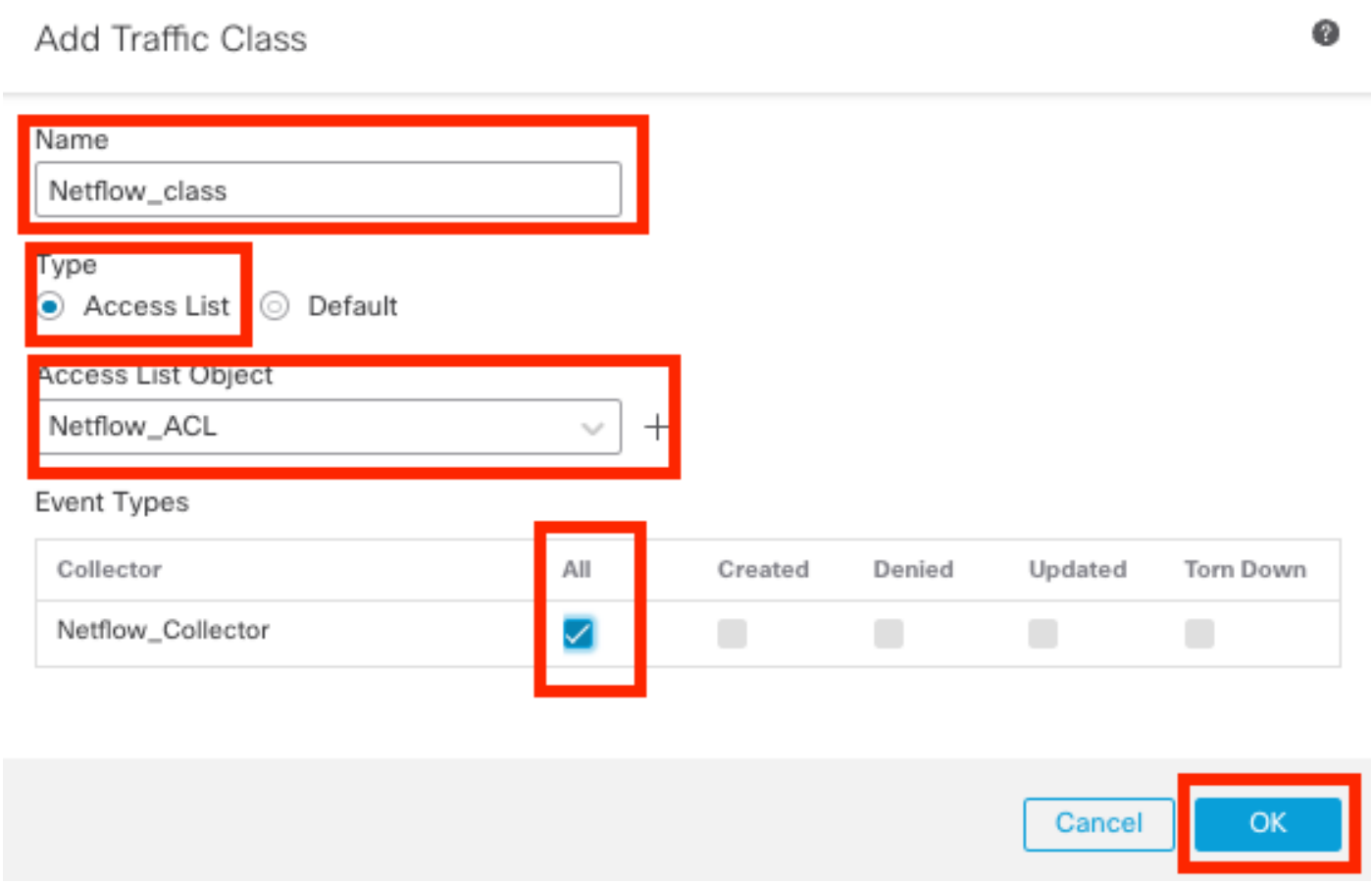
# NetFlow에 트래픽 클래스 추가

1단계. Add Traffic Class(트래픽 클래스 추가)를 클릭합니다.




트래픽 클래스 추가

2단계. NetFlow 이벤트와 일치해야 하는 트래픽 클래스의 이름 필드, NetFlow 이벤트에 대해 캡처된 트래픽과 일치해야 하는 트래픽 클래스를 지정하는 ACL을 입력하고, 컬렉터에 전송할 다른 NetFlow 이벤트에 대한 확인란을 선택하고 OK를 클릭합니다.




트래픽 클래스 설정

# 문제 해결

1단계. FTD CLI에서 컨피그레이션을 확인할 수 있습니다.

1.1. FTD CLI에서 시스템 지원 diagnostic-cli에 다음을 입력합니다.

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

1.2 정책 맵 컨피그레이션 확인:

<#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**

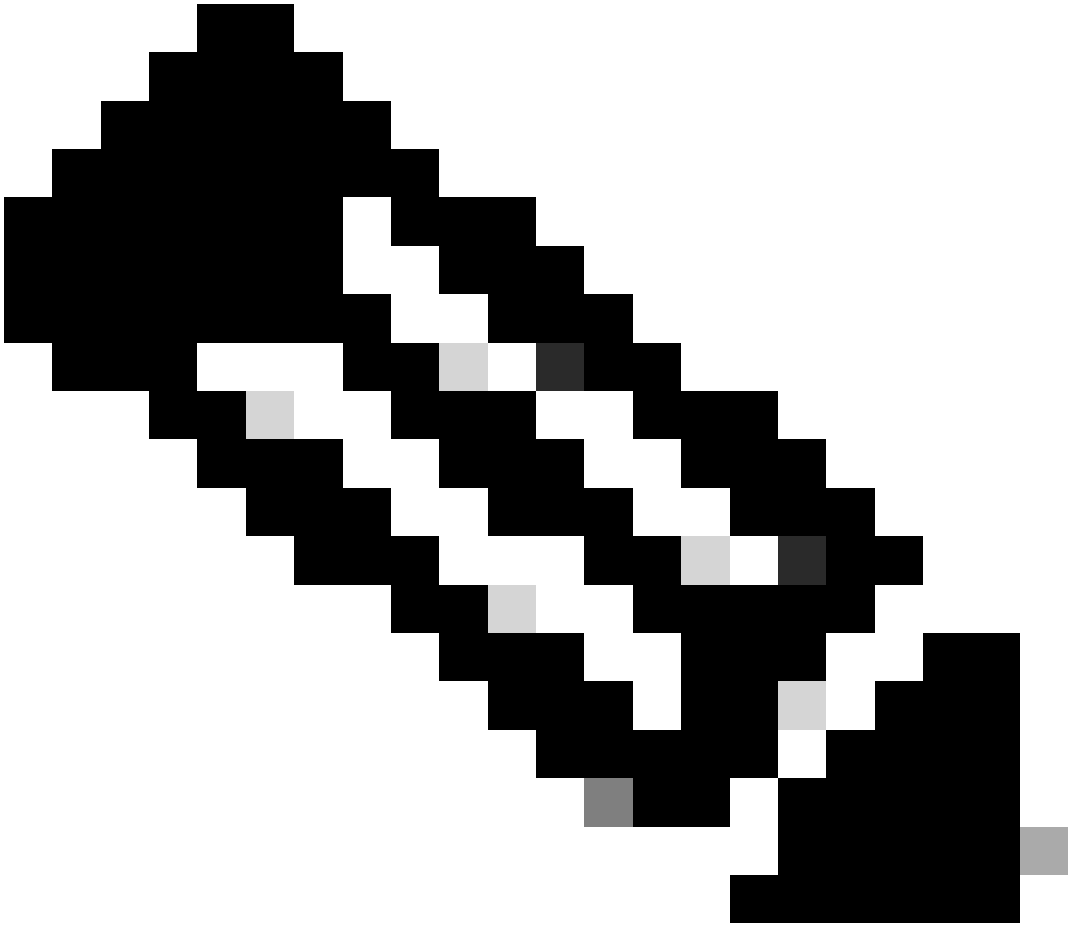
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. flow-export 컨피그레이션을 확인합니다.

<#root>

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

**flow-export destination Inside 192.168.31.1 2055**



참고: 이 예에서 "Inside"는 Netflow_Export라는 인터페이스 그룹에 구성된 인터페이스의 이름입니다

2단계. ACL에 대한 적중 횟수를 확인합니다.

<#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
```

3단계. Netflow 카운터 확인:

<#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
```

# 관련 정보

- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.