Konfigurieren von NetFlow in FMC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Netflow im Cisco Secure Firewall Management Center mit Version 7.4 oder höher konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Firewall Management Center für VMWare läuft in Version 7.4.1
- Sichere Firewall mit Version 7.4.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

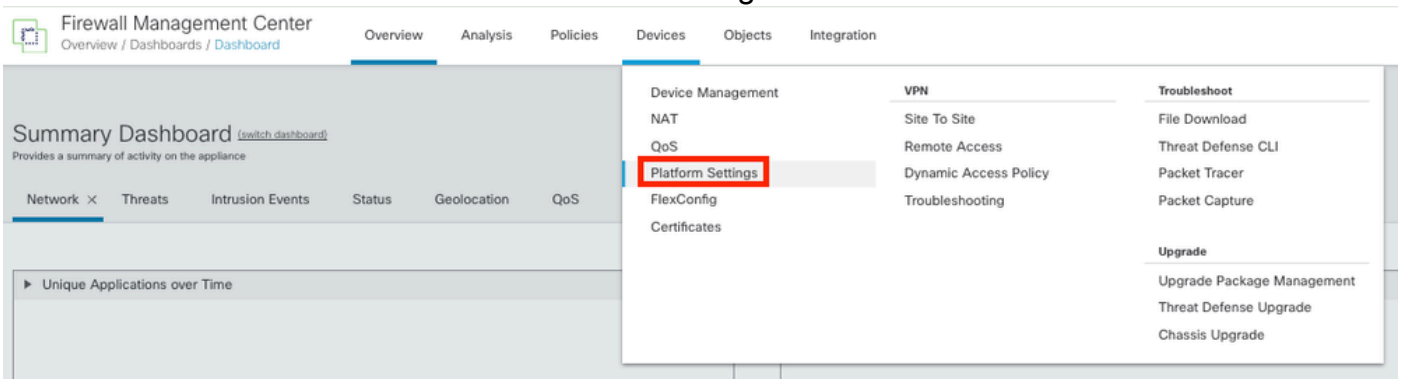
Hintergrundinformationen

Spezifische Anforderungen für dieses Dokument:

- Cisco Secure Firewall Threat Defense mit Version 7.4 oder höher
- Cisco Secure Firewall Management Center mit Version 7.4 oder höher

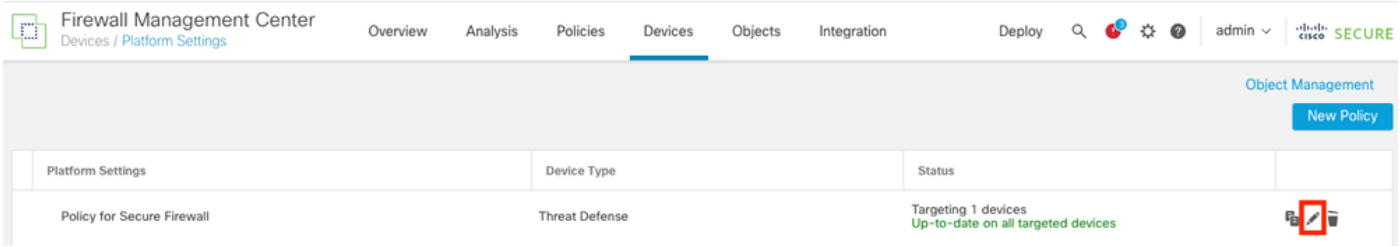
Collector in NetFlow hinzufügen

Schritt 1: Gehen Sie zu Geräte > Plattformeinstellungen:



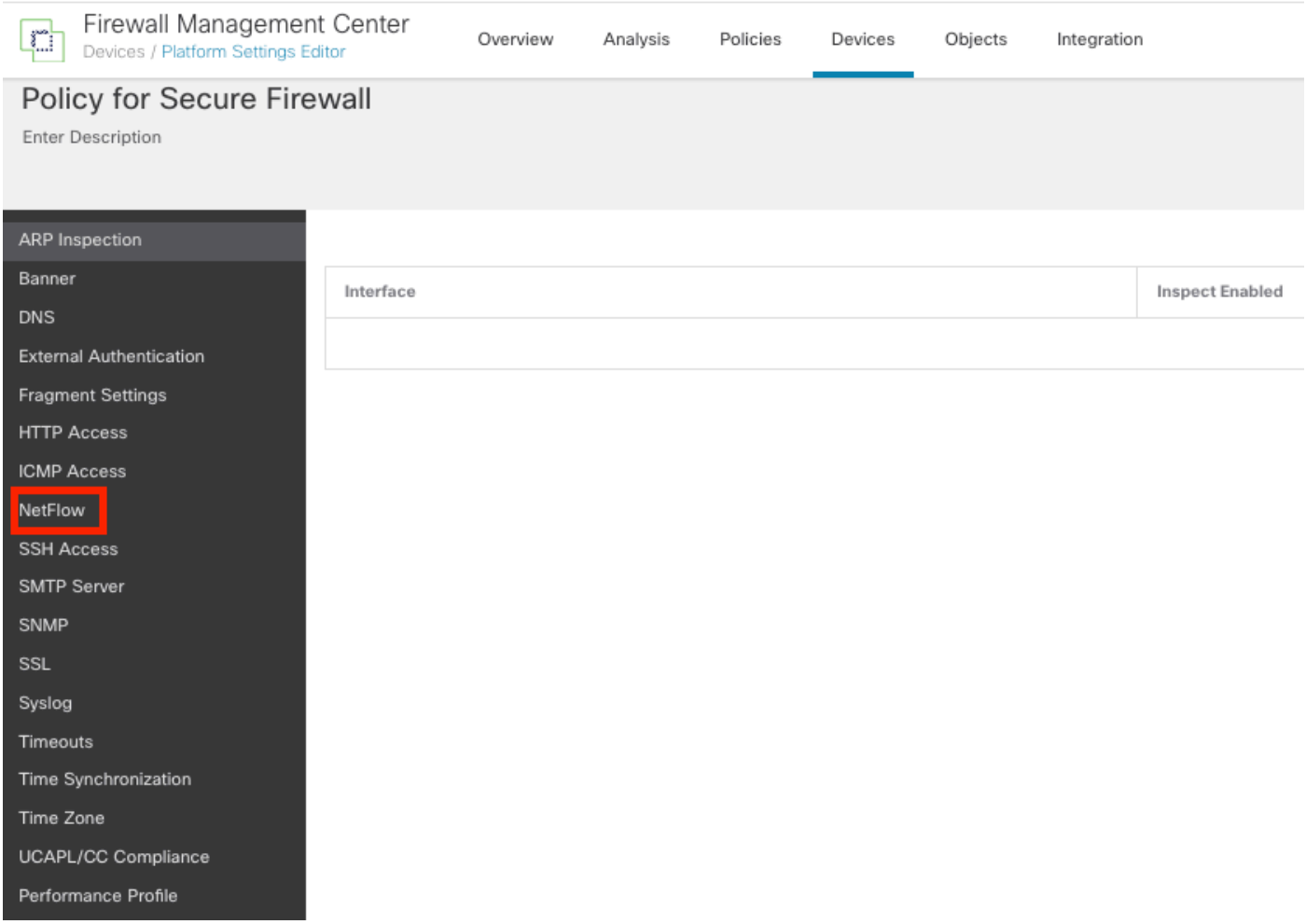
Zugriff auf Plattformeinstellungen

Schritt 2: Bearbeiten Sie die dem Überwachungsgerät zugewiesene Richtlinie für die Plattformeinstellungen:



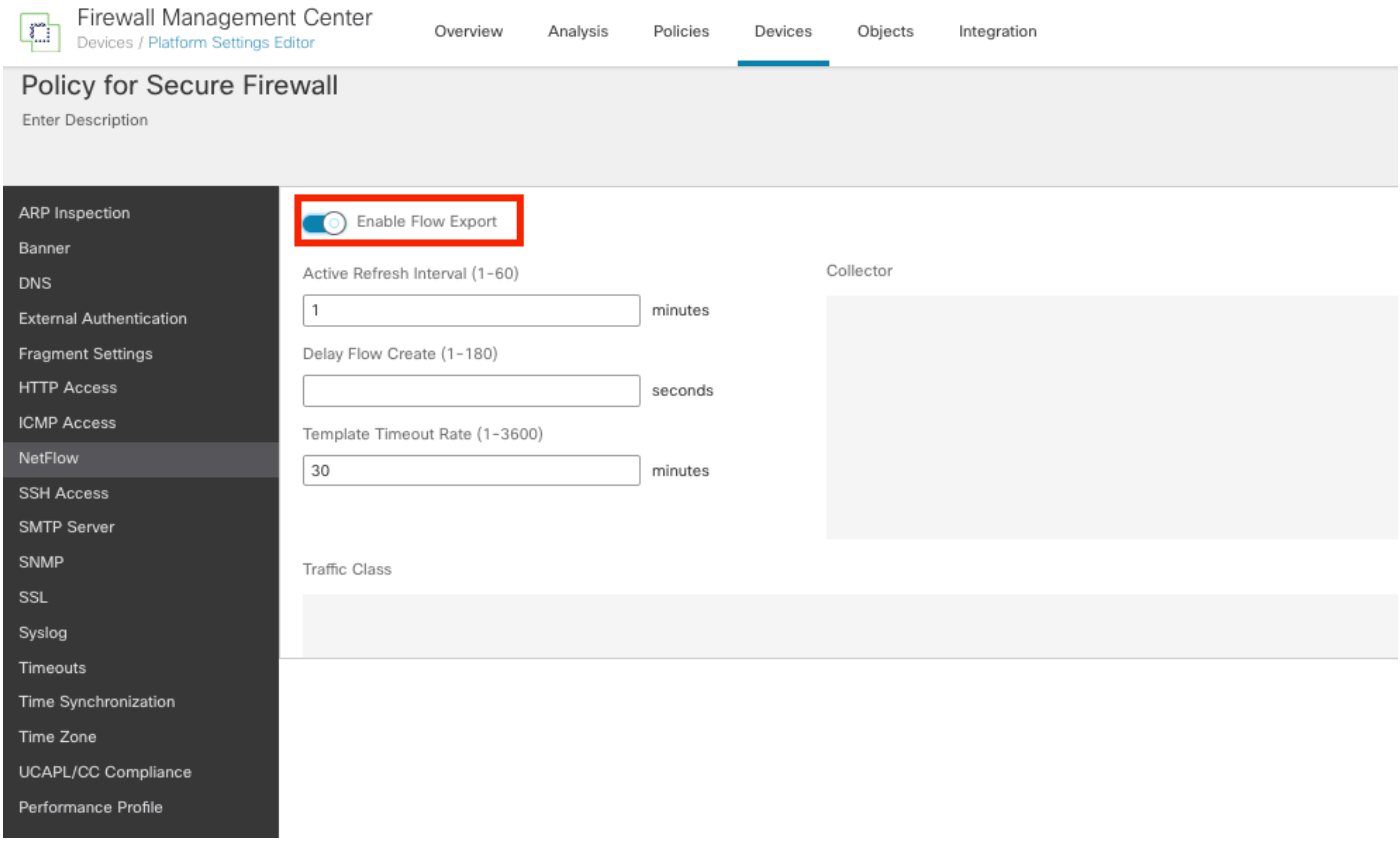
Richtlinienausgabe

Schritt 3: Wählen Sie NetFlow:



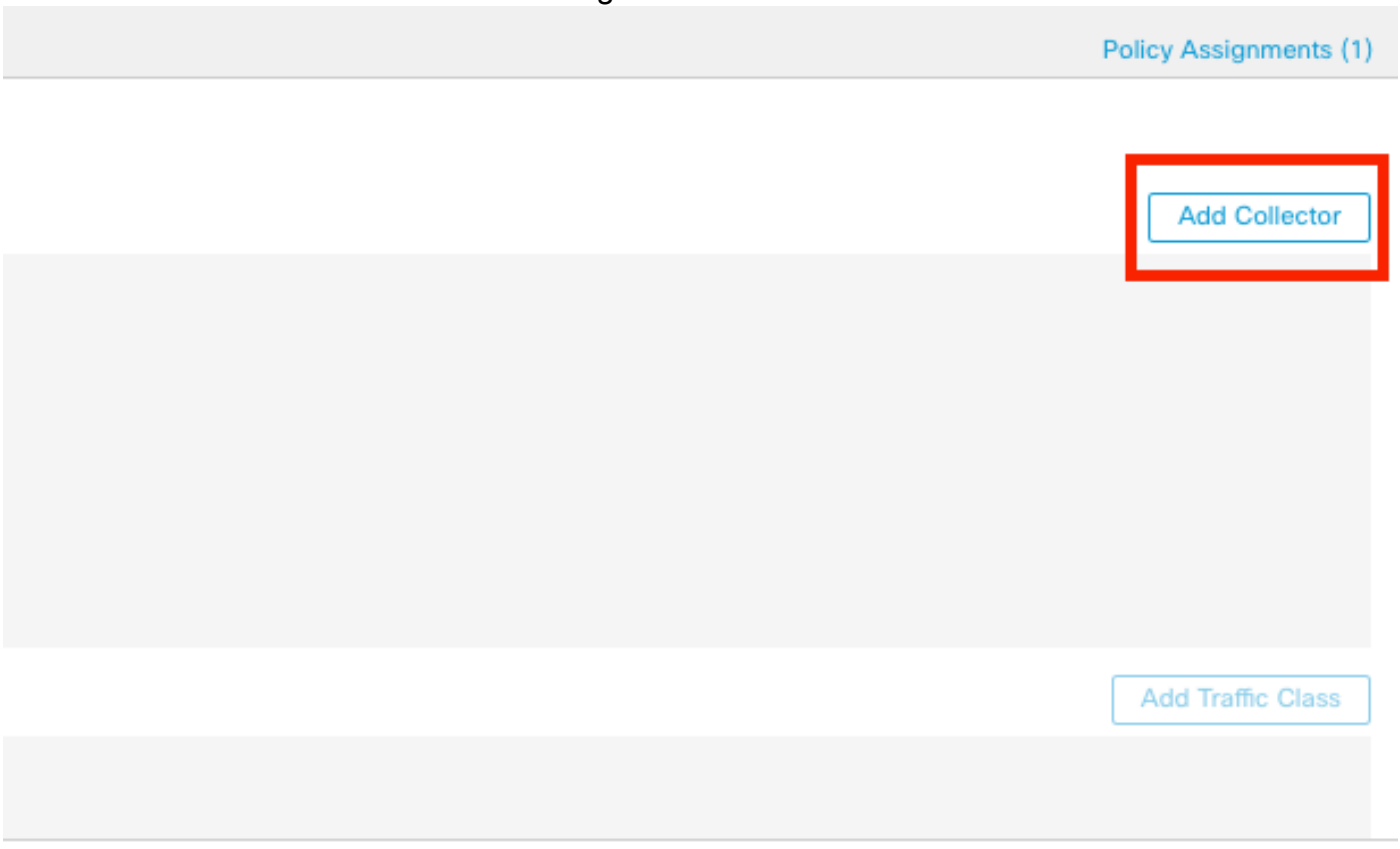
Zugriff auf NetFlow-Einstellungen

Schritt 4: Umschalter "Flow-Export" aktivieren, um NetFlow-Datenexport zu aktivieren:



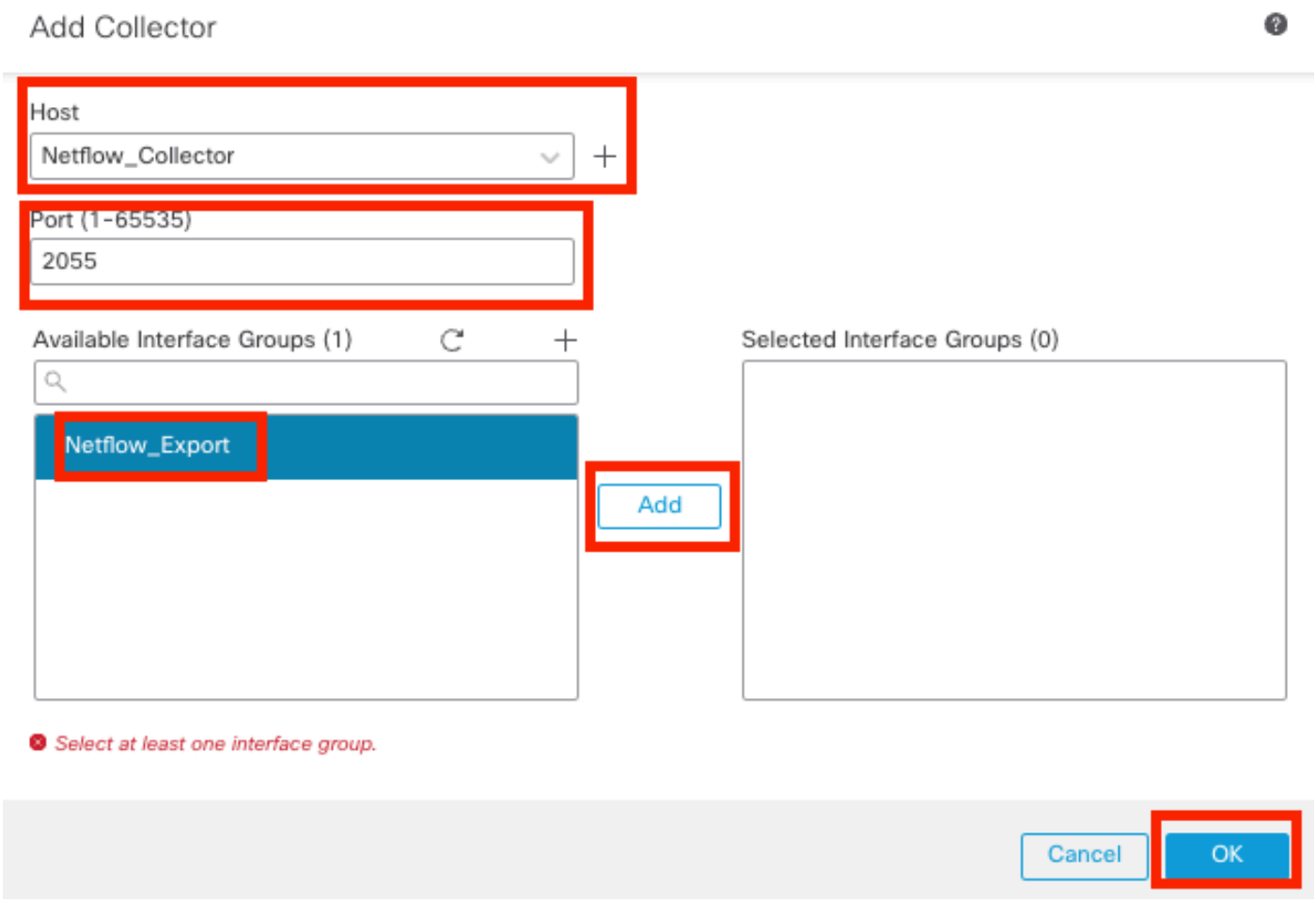
Aktivieren von NetFlow

Schritt 5: Klicken Sie auf Collector hinzufügen:



Collector hinzufügen

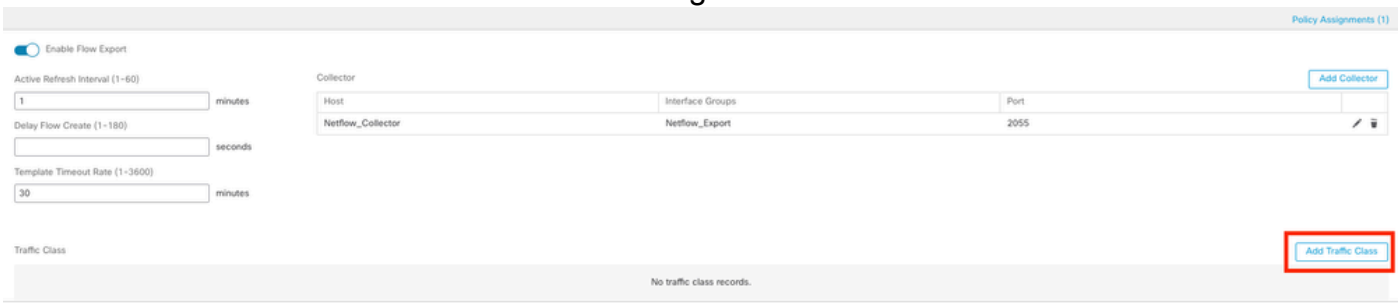
Schritt 6: Wählen Sie das Collector-Host-IP-Objekt des NetFlow-Ereignissammlers, den UDP-Port am Collector, an den die NetFlow-Pakete gesendet werden müssen, wählen Sie die Schnittstellengruppe aus, über die der Collector erreicht werden muss, und klicken Sie auf OK:



Collector-Einstellungen

Hinzufügen einer Datenverkehrsklasse zu NetFlow

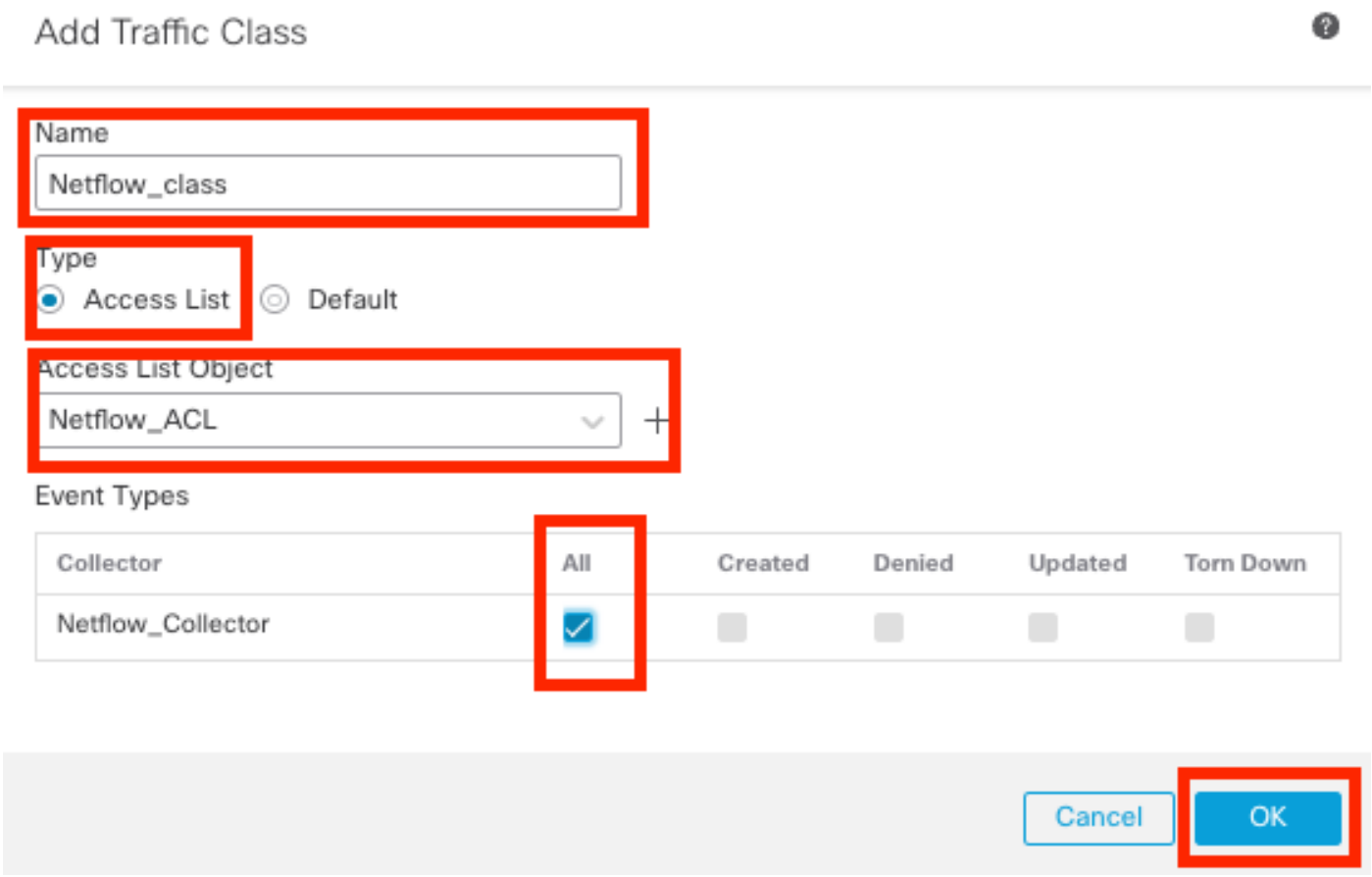
Schritt 1: Klicken Sie auf Verkehrsklasse hinzufügen:



Hinzufügen einer Datenverkehrsklasse

Schritt 2: Geben Sie das Namensfeld der Datenverkehrsklasse ein, die mit den NetFlow-Ereignissen übereinstimmen muss, die ACL, um die Datenverkehrsklasse anzugeben, die mit dem für die NetFlow-Ereignisse erfassten Datenverkehr übereinstimmen muss, aktivieren Sie die

Kontrollkästchen für die verschiedenen NetFlow-Ereignisse, die Sie an die Collectors senden möchten, und klicken Sie auf OK:



Einstellungen der Datenverkehrsklasse

Fehlerbehebung

Schritt 1: Sie können die Konfiguration über FTD CLI überprüfen.

1.1. Geben Sie in der FTD-CLI Folgendes ein, um die Diagnose-CLI des Systems zu erhalten:

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

1.2 Überprüfen der Konfiguration der Richtlinienzuweisung:

<#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

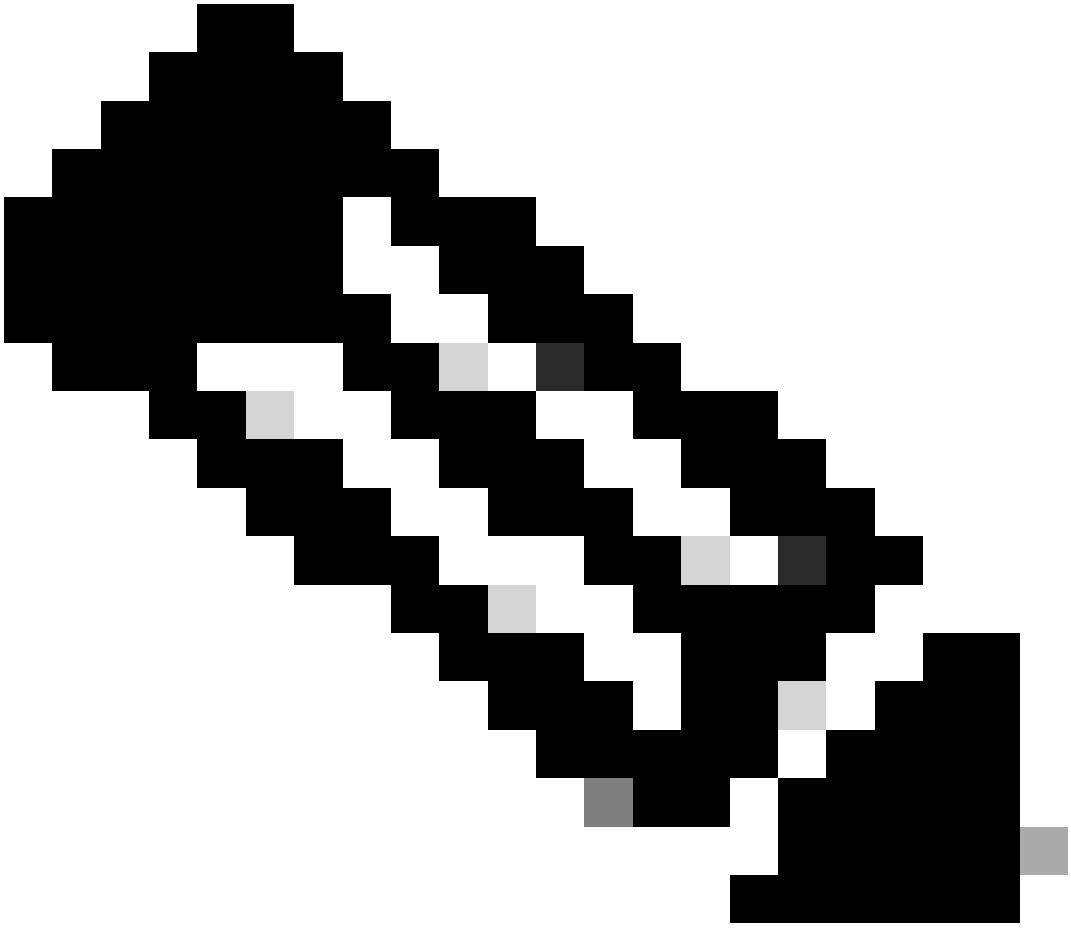
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Überprüfen Sie die Flow-Export-Konfiguration:

<#root>

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

flow-export destination Inside 192.168.31.1 2055



Hinweis: In diesem Beispiel ist "Inside" der Name der Schnittstelle, die in der Schnittstellengruppe NetFlow_Export konfiguriert wurde.

Schritt 2: Überprüfen Sie die Trefferanzahl für die 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
```

Schritt 3: NetFlow-Zähler überprüfen:

<#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
```

Zugehörige Informationen

- Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.4

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.