NetFlow configureren in VCC

Inhoud

Inleiding

Dit document beschrijft hoe u NetFlow kunt configureren in het Cisco Secure Firewall Management Center dat versie 7.4 of hoger uitvoert.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)
- NetFlow-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall Management Center voor VMWare voert v7.4.1 uit
- Secure Firewall versie 7.4.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

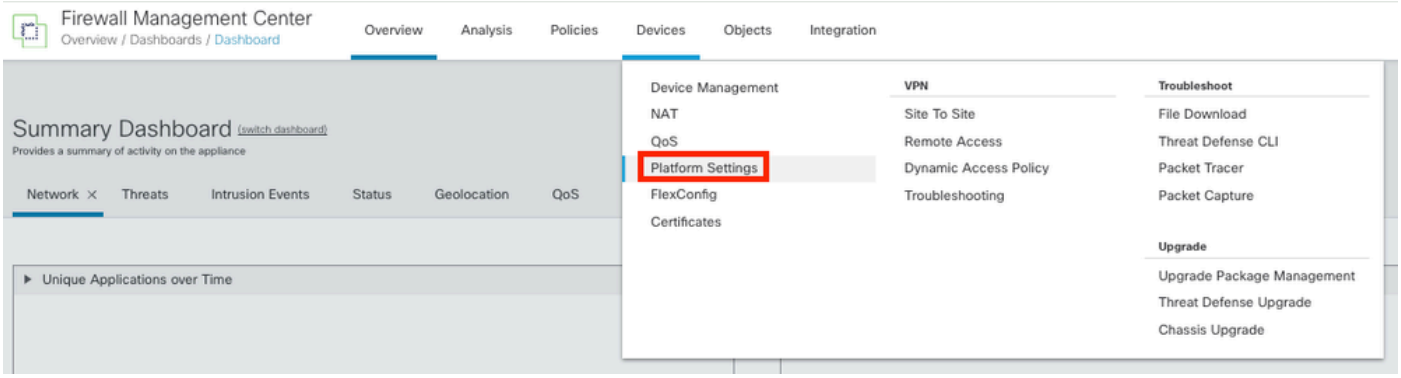
Achtergrondinformatie

Specifieke eisen voor dit document zijn onder meer:

- Cisco Secure Firewall Threat Defense, versie 7.4 of hoger
- Cisco Secure Firewall Management Center met versie 7.4 of hoger

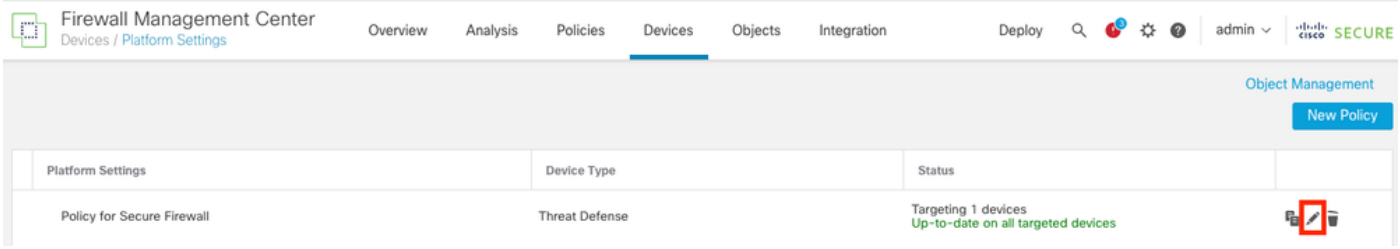
Collector toevoegen in NetFlow

Stap 1. Ga naar Apparaten > Platform-instellingen:



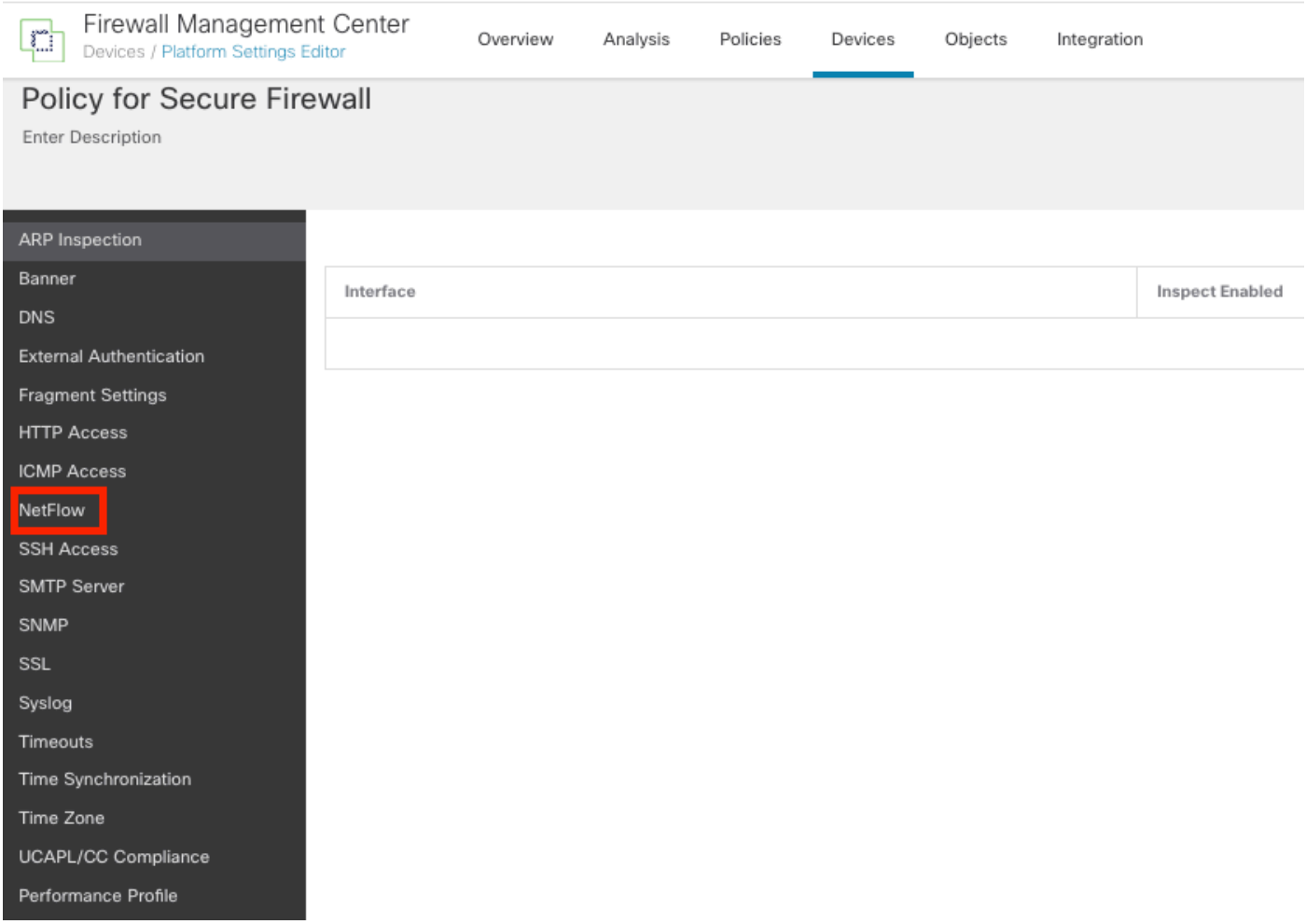
Platform-instellingen gebruiken

Stap 2. Het beleid voor platforminstellingen bewerken dat is toegewezen aan het monitorapparaat:



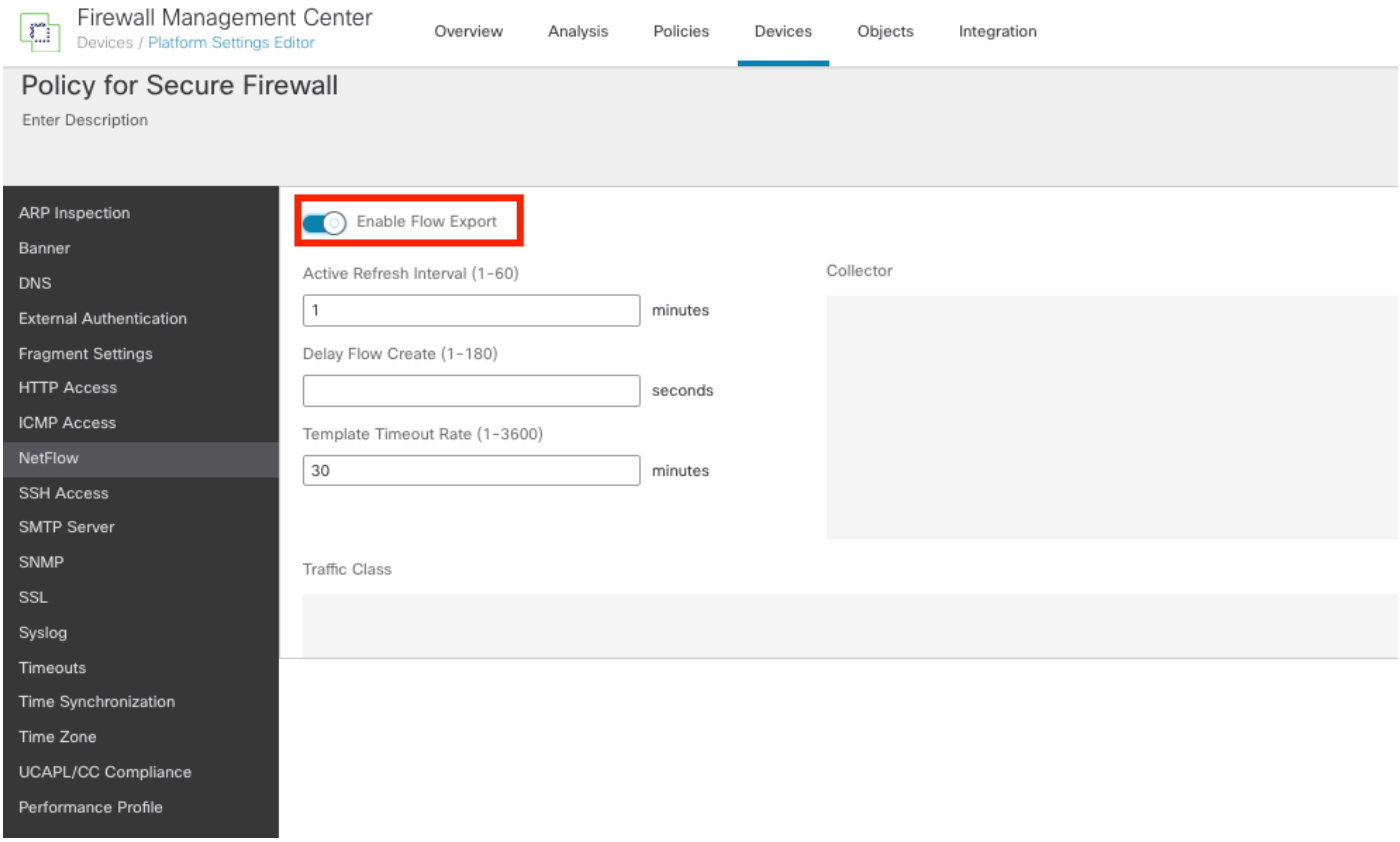
Policy Edition

Stap 3. Kies NetFlow:



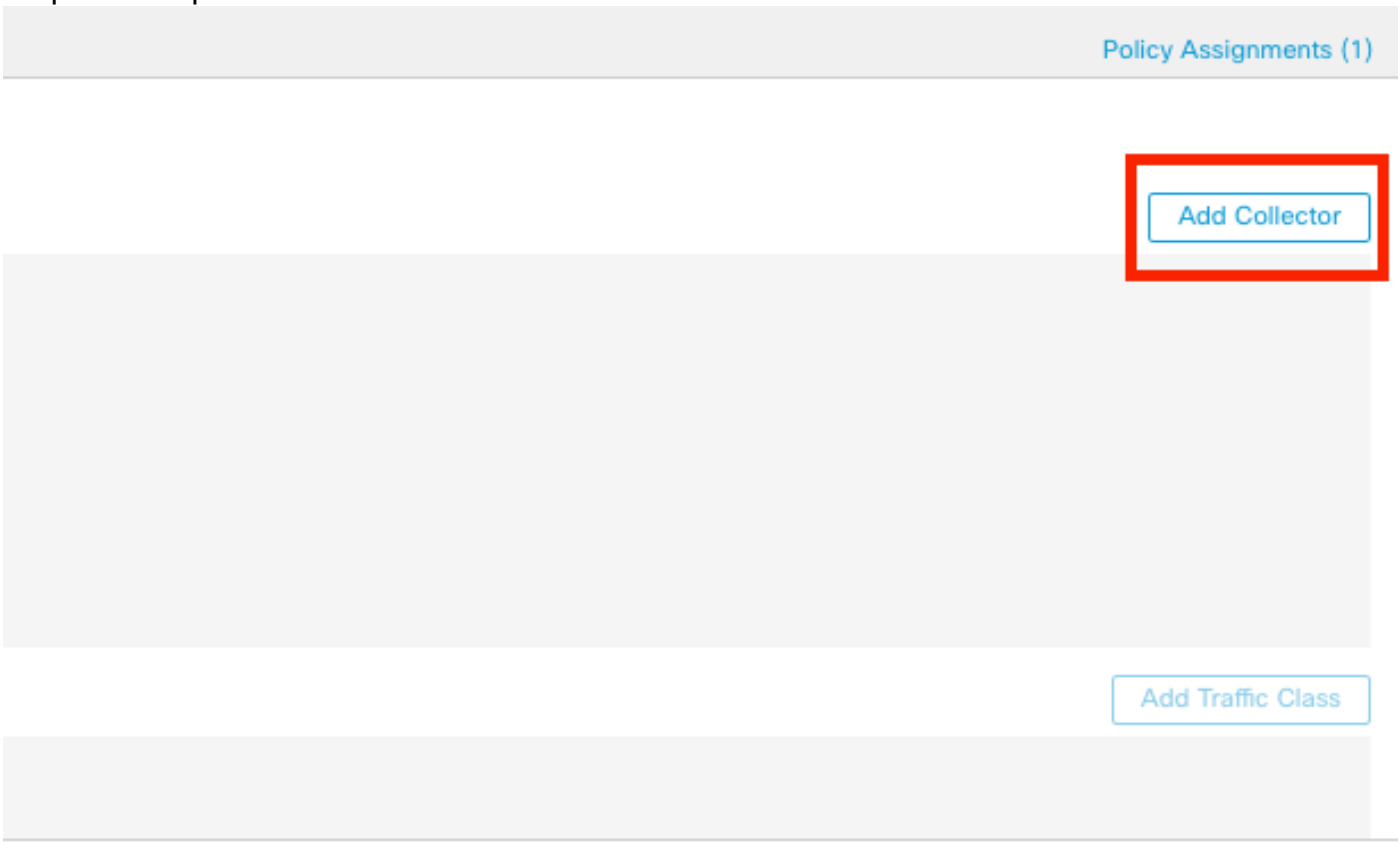
NetFlow-instellingen gebruiken

Stap 4. Schakel Flow Export in om NetFlow-gegevensexport mogelijk te maken:



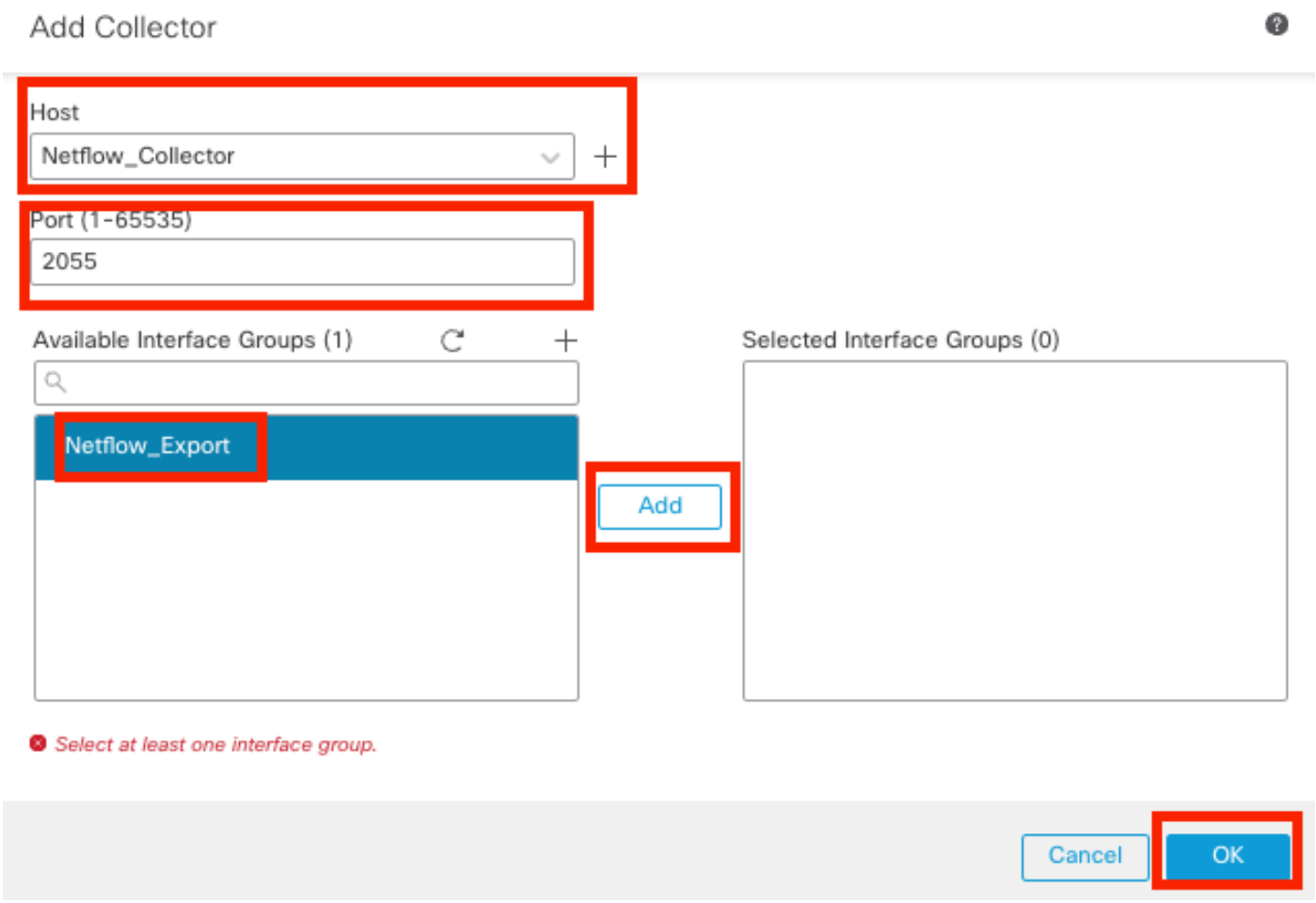
NetFlow inschakelen

Stap 5. Klik op Add Collector:



Collector toevoegen

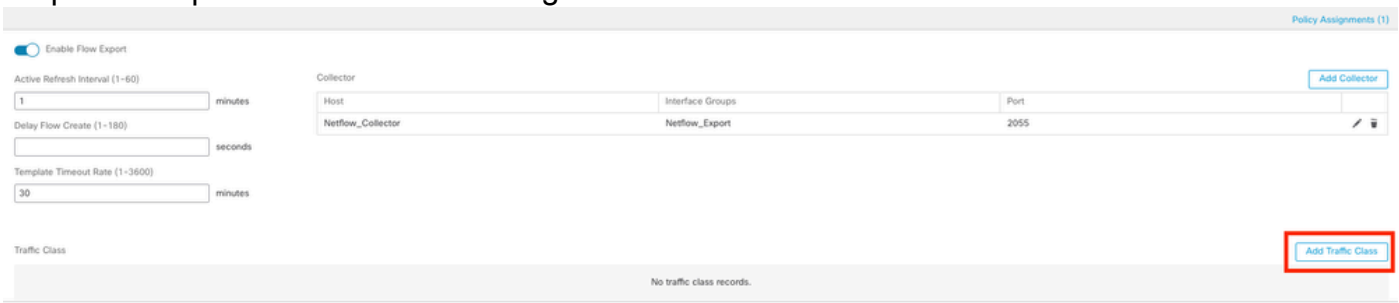
Stap 6. Kies het collector host IP object van de NetFlow event collector, de UDP-poort op de collector waarnaar de NetFlow-pakketten moeten worden verzonden, kies de interfacegroep waardoor de collector moet worden bereikt en klik op OK:



Collector-instellingen

Verkeersklasse aan NetFlow toevoegen

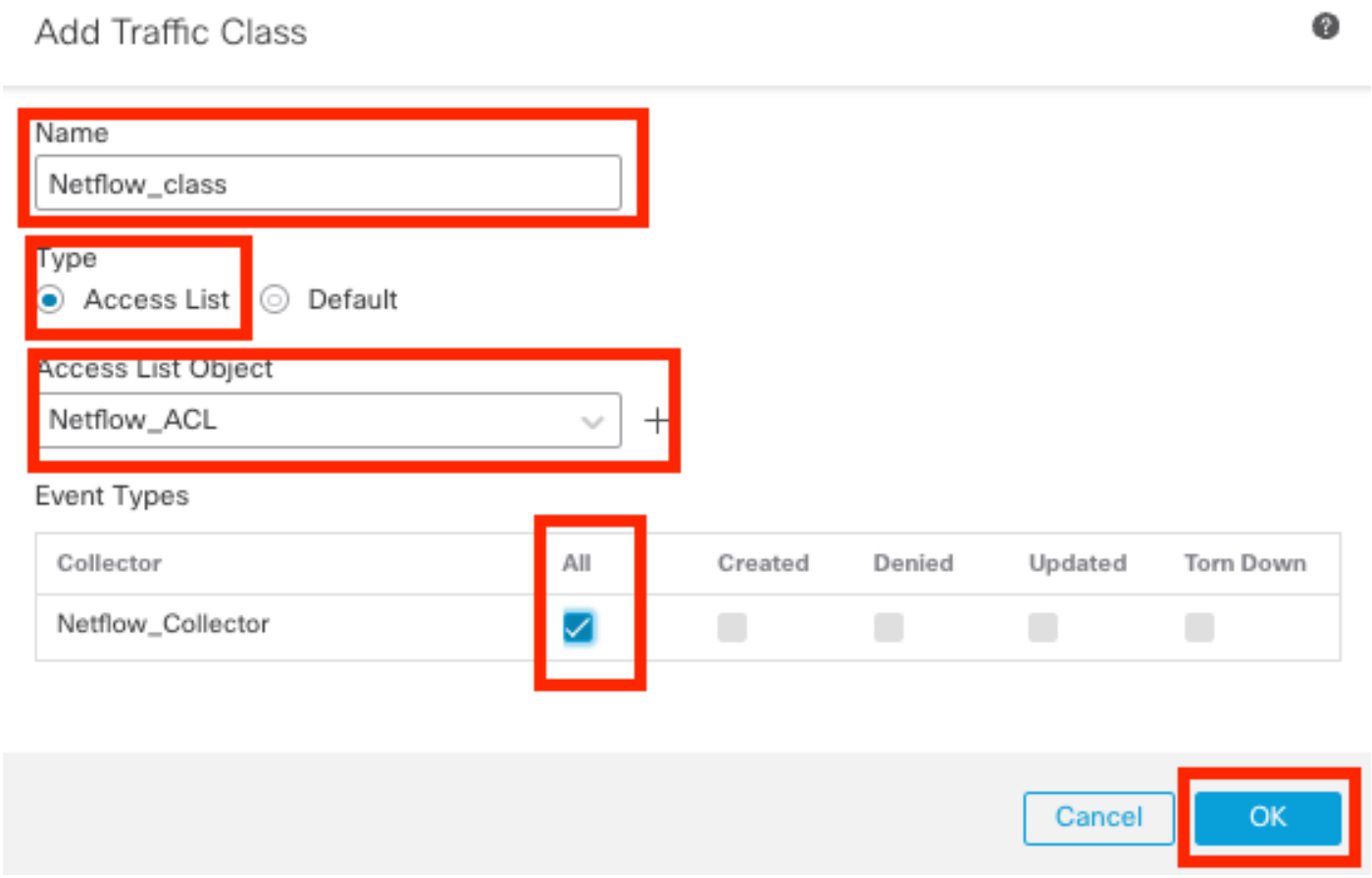
Stap 1. Klik op Verkeersklasse toevoegen:



Verkeersklasse toevoegen

Stap 2. Voer het naamveld in van de verkeersklasse die moet overeenkomen met de NetFlow-gebeurtenissen, de ACL om de verkeersklasse te specificeren die moet overeenkomen met het verkeer dat is opgenomen voor de NetFlow-gebeurtenissen, selecteer de selectievakjes voor de

verschillende NetFlow-gebeurtenissen die u naar de verzamelaars wilt verzenden en klik op OK:



Instellingen verkeersklasse

Probleemoplossing

Stap 1. U kunt de configuratie verifiëren via FTD CLI.

1.1. Voer vanuit de FTD CLI naar de systeemondersteuning van de diagnostische client:

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

1.2 Controleer de configuratie van het beleidsplan:

<#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

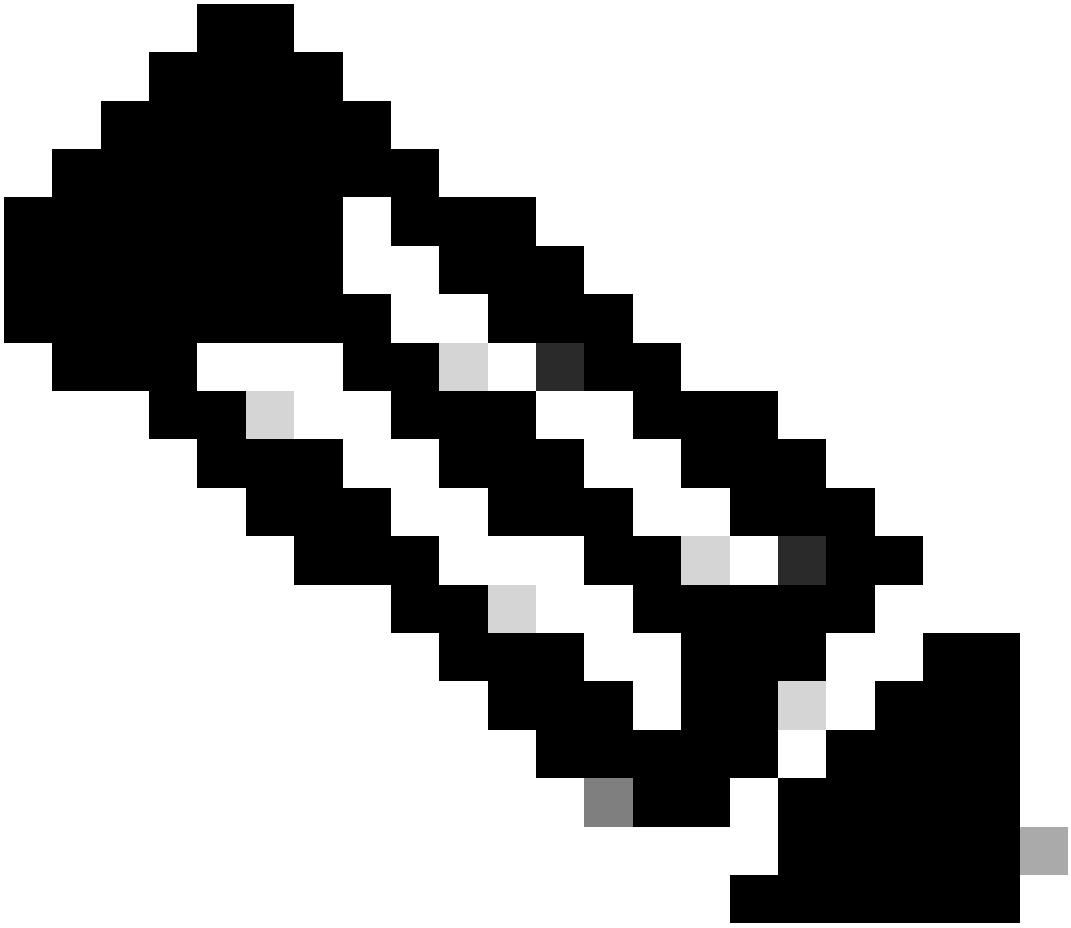
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Controleer de flow-export-configuratie:

<#root>

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

flow-export destination Inside 192.168.31.1 2055



Opmerking: in dit voorbeeld is "Binnen" de naam van de interface die is geconfigureerd in de interfacegroep NetFlow_Export

Stap 2. Controleer het aantal treffers voor de 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
```

Stap 3. Controleer NetFlow-tellers:

<#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
```

Gerelateerde informatie

- Handleiding voor configuratie van apparaat in Cisco Secure Firewall Management Center, 7.4

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.