Configurare NetFlow in FMC

Sommario

Introduzione

In questo documento viene descritto come configurare Netflow in Cisco Secure Firewall Management Center con versione 7.4 o successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall Management Center per VMWare in esecuzione versione 7.4.1
- Secure Firewall Runs v7.4.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

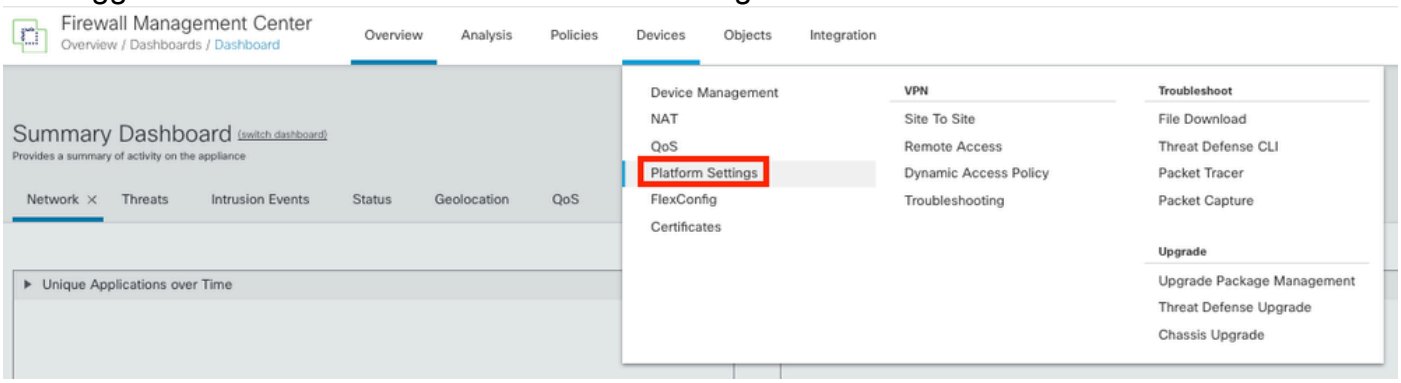
Premesse

I requisiti specifici per questo documento includono:

- Cisco Secure Firewall Threat Defense con versione 7.4 o superiore
- Cisco Secure Firewall Management Center con versione 7.4 o superiore

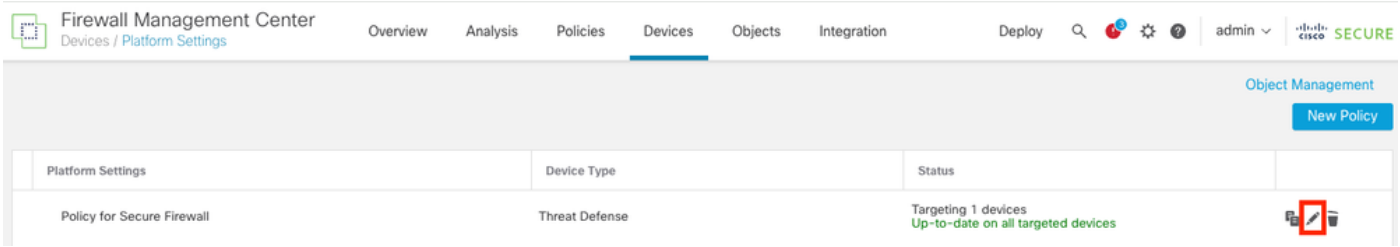
Aggiungi agente di raccolta in NetFlow

Passaggio 1. Selezionare Devices > Platform Settings:



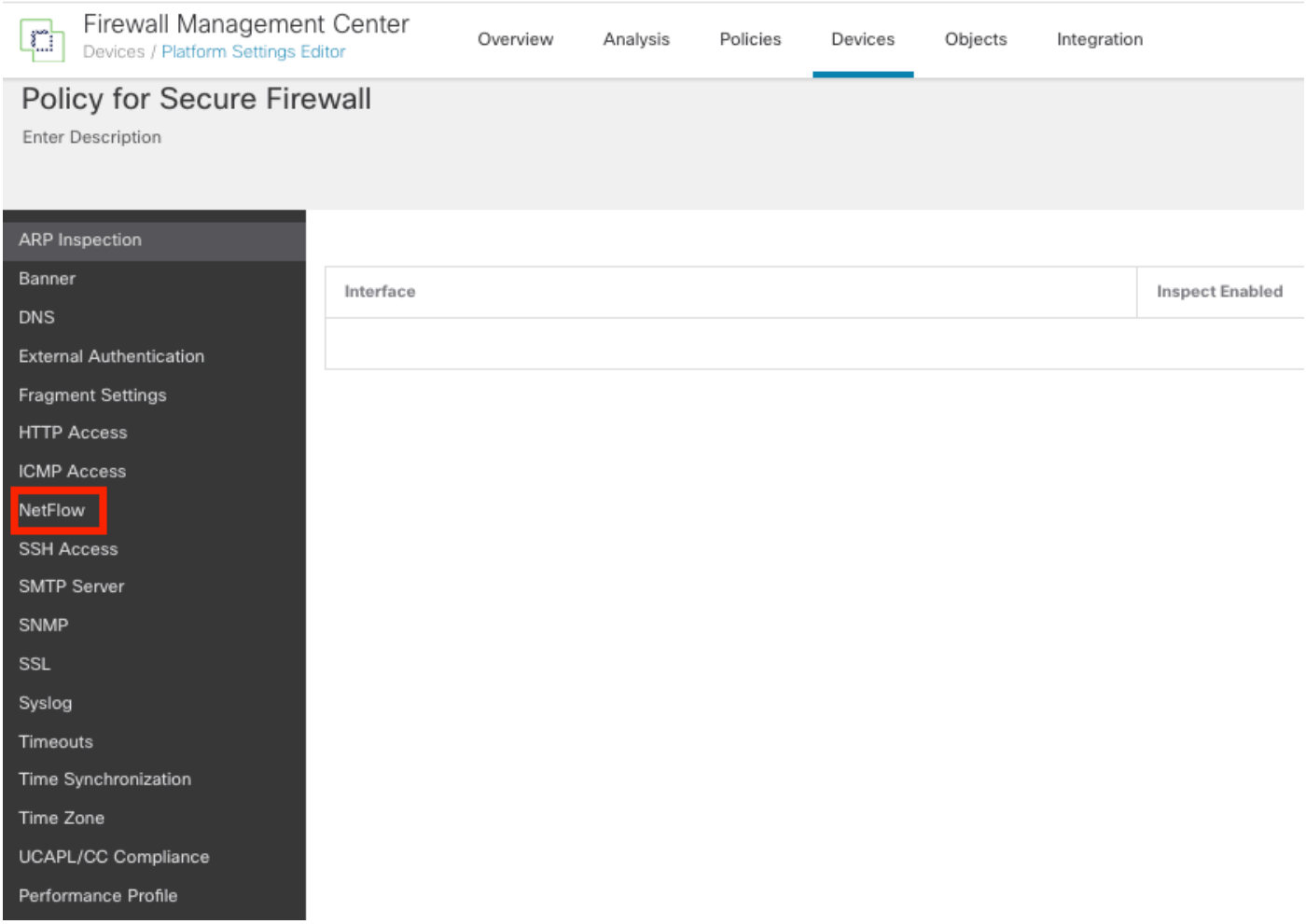
Accesso alle impostazioni della piattaforma

Passaggio 2. Modificare il criterio Impostazioni piattaforma assegnato al dispositivo di monitoraggio:



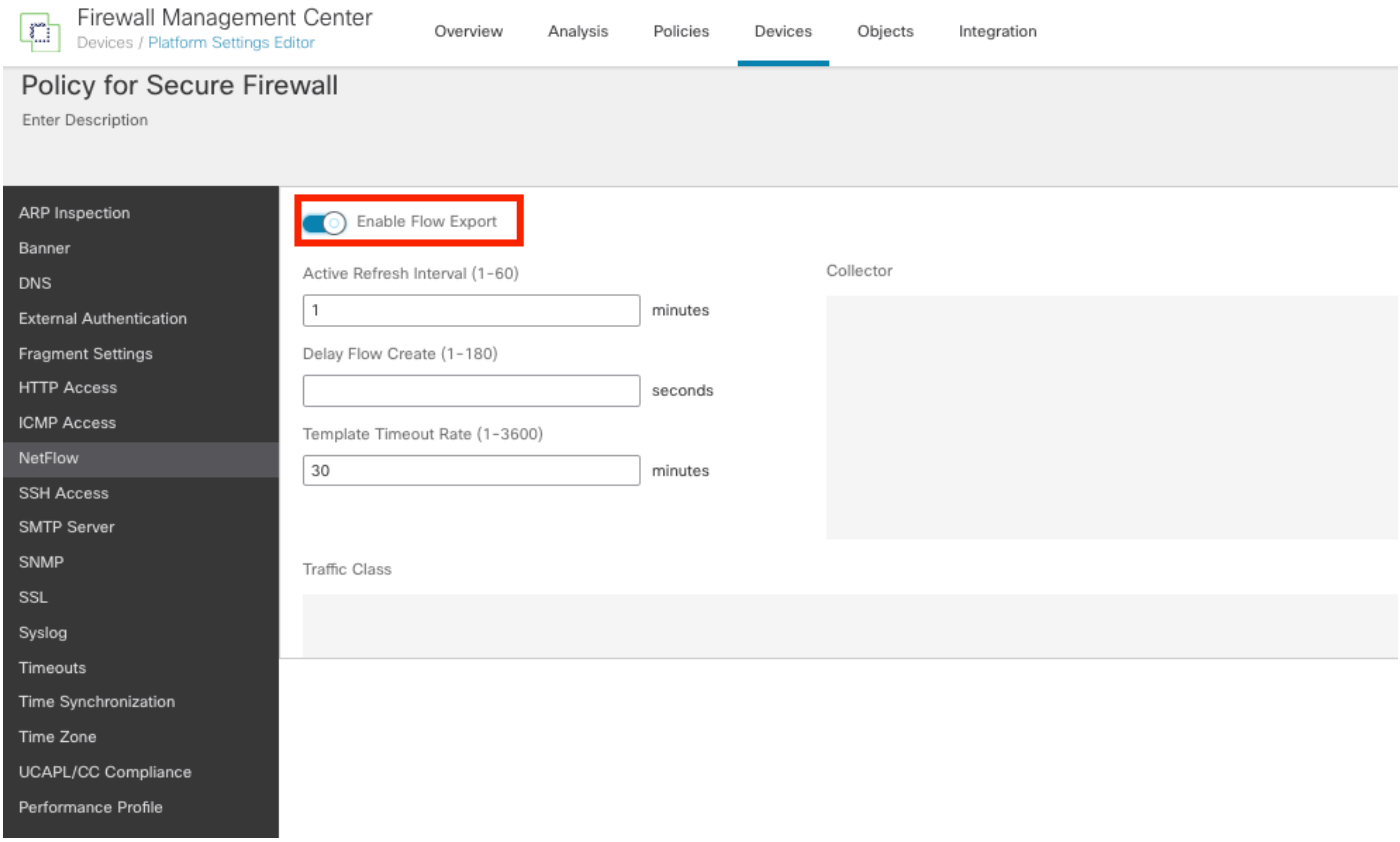
Edizione criterio

Passaggio 3. Scegliere NetFlow:



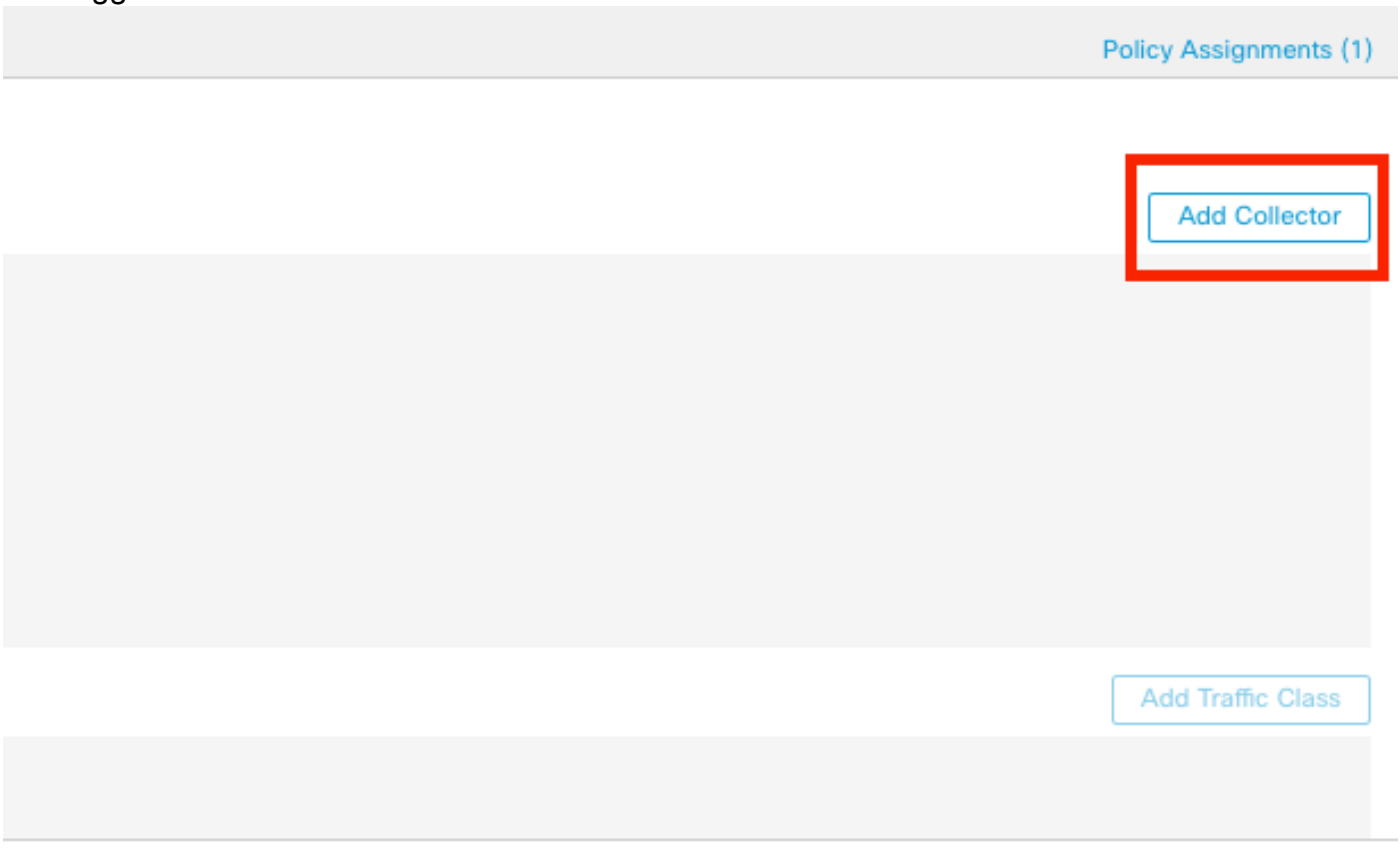
Accesso alle impostazioni di NetFlow

Passaggio 4. Attiva/disattiva esportazione flusso per abilitare l'esportazione dati NetFlow:



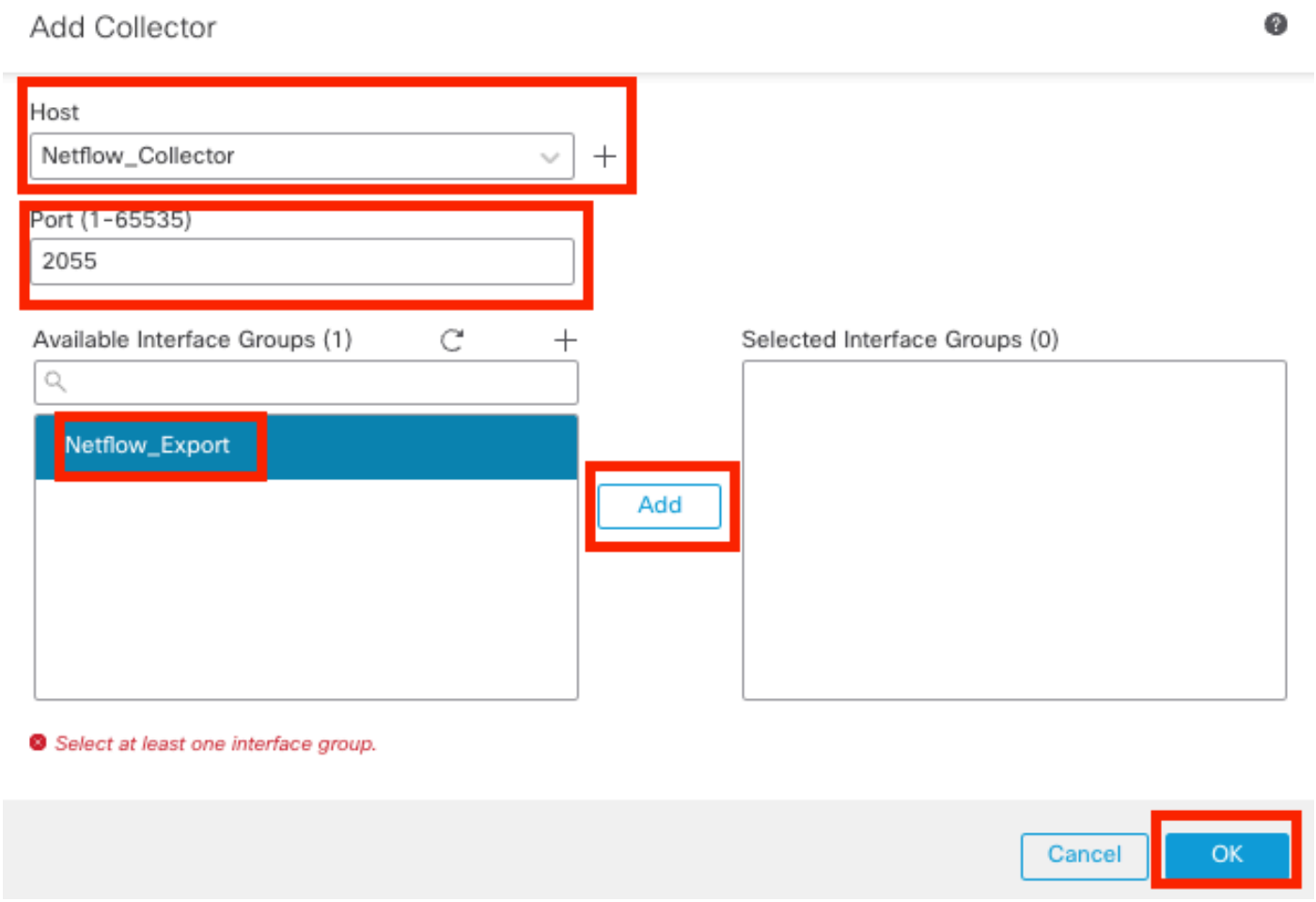
Abilitazione di NetFlow

Passaggio 5. Fare clic su Add Collector:



Aggiunta agente di raccolta

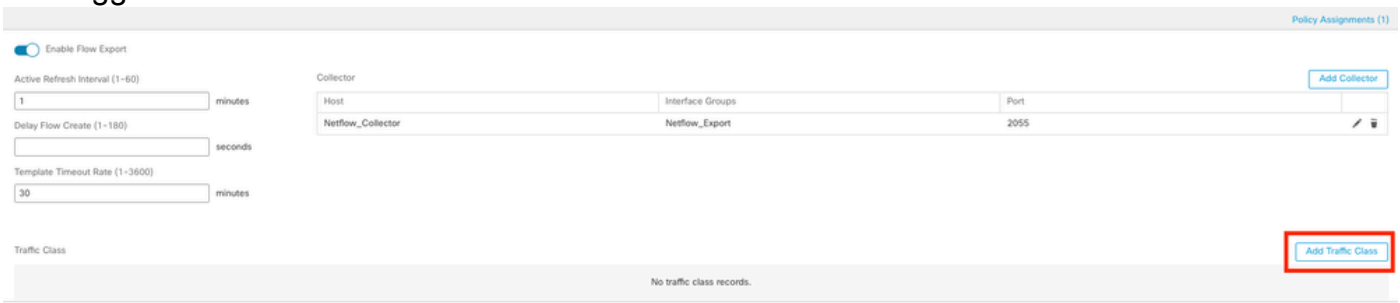
Passaggio 6. Scegliere l'oggetto IP dell'host del collector per l'agente di raccolta eventi NetFlow, la porta UDP sul collector a cui devono essere inviati i pacchetti NetFlow, scegliere il gruppo di interfacce attraverso cui deve essere raggiunto il collector e fare clic su OK:



Impostazioni agente di raccolta

Aggiungi classe traffico a NetFlow

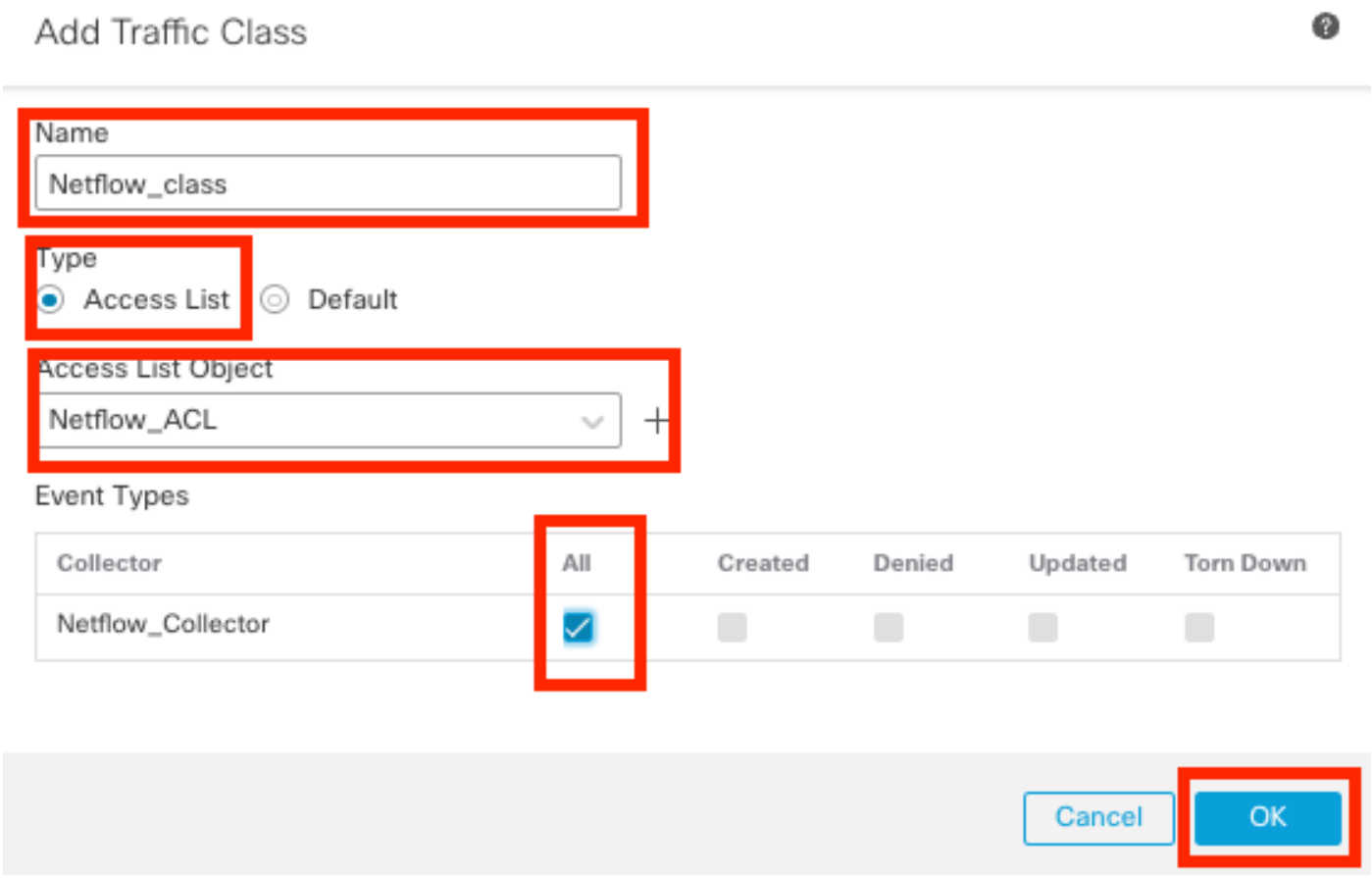
Passaggio 1. Fare clic su Add Traffic Class:



Aggiunta di una classe di traffico

Passaggio 2. Immettere il campo del nome della classe di traffico che deve corrispondere agli eventi NetFlow, l'ACL per specificare la classe di traffico che deve corrispondere al traffico acquisito per gli eventi NetFlow, selezionare le caselle di controllo per i diversi eventi NetFlow che

si desidera inviare agli agenti di raccolta e fare clic su OK:



Impostazioni classe traffico

Risoluzione dei problemi

Passaggio 1. È possibile verificare la configurazione dalla CLI FTD.

1.1. Dalla CLI FTD, accedere al supporto di sistema diagnostic-cli:

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

1.2 Controllare la configurazione della mappa dei criteri:

<#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

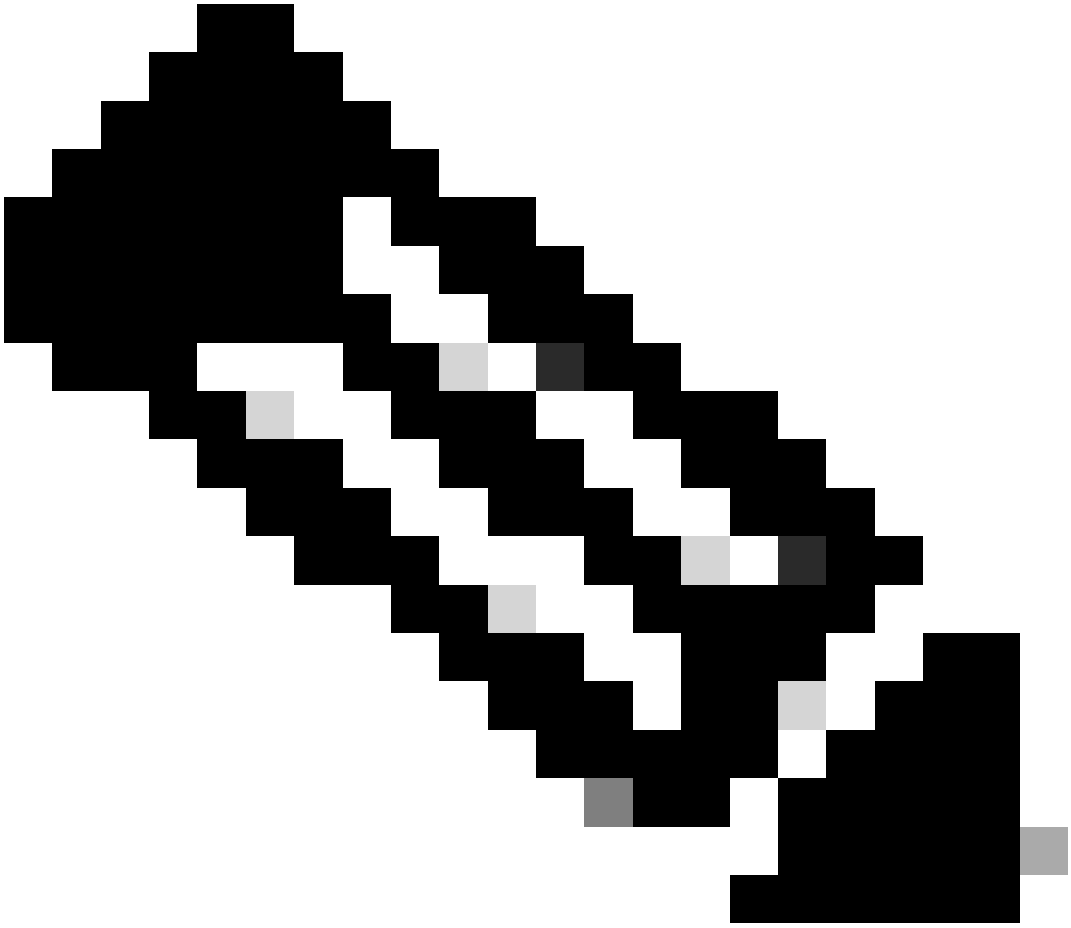
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Controllare la configurazione del flusso di esportazione:

<#root>

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

flow-export destination Inside 192.168.31.1 2055



Nota: nell'esempio, "Inside" è il nome dell'interfaccia configurata nel gruppo di interfacce denominato Netflow_Export

Passaggio 2. Verificare il numero di passaggi per l'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
```

Passaggio 3. Verificare i contatori NetFlow:

<#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
```

Informazioni correlate

- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.4

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).