تكوين NetFlow في FMC

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين NetFlow في مركز إدارة جدار الحماية الآمن من Cisco الذي يشغل الإصدار 7.4 أو الأحدث.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة جدار الحماية الآمن (FMC) من Cisco
- الدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco
- بروتوكول NetFlow

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- يقوم مركز إدارة جدار الحماية الآمن ل VMWare بتشغيل v7.4.1
- تشغيل جدار الحماية الآمن v7.4.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

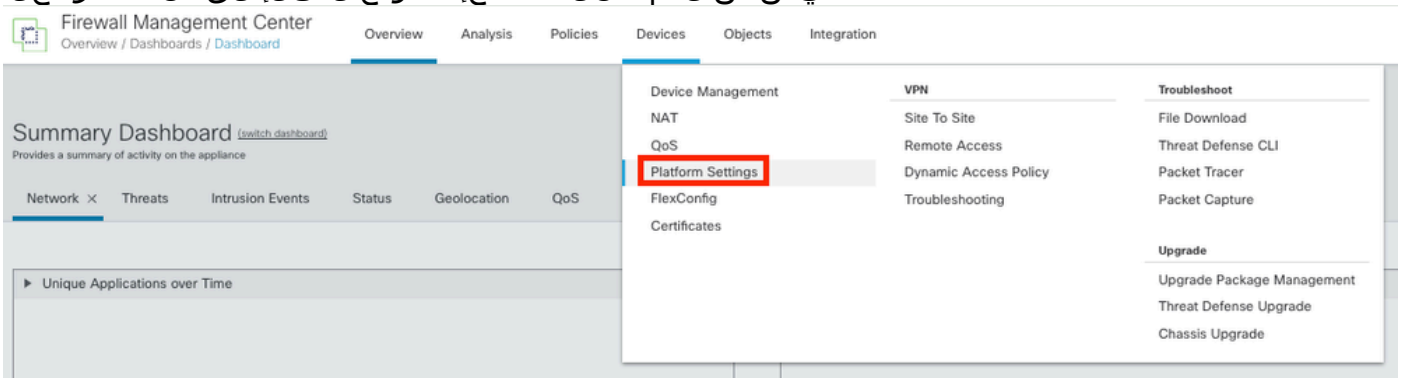
معلومات أساسية

تتضمن المتطلبات الخاصة لهذا المستند:

- Cisco Secure Firewall Threat Defense الإصدار 7.4 أو إصدار أعلى
- مركز إدارة جدار الحماية الآمن من Cisco الذي يعمل الإصدار 7.4 أو إصدار أعلى

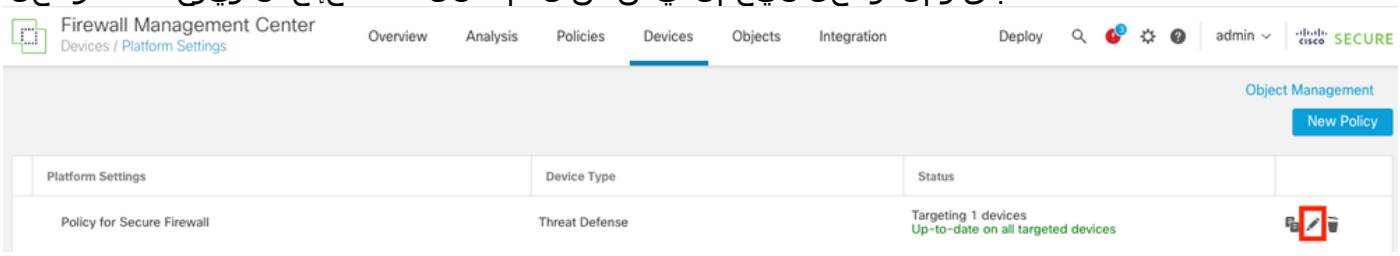
إضافة مجمع في NetFlow

الخطوة 1. انتقل إلى الأجهزة > إعدادات النظام الأساسي:



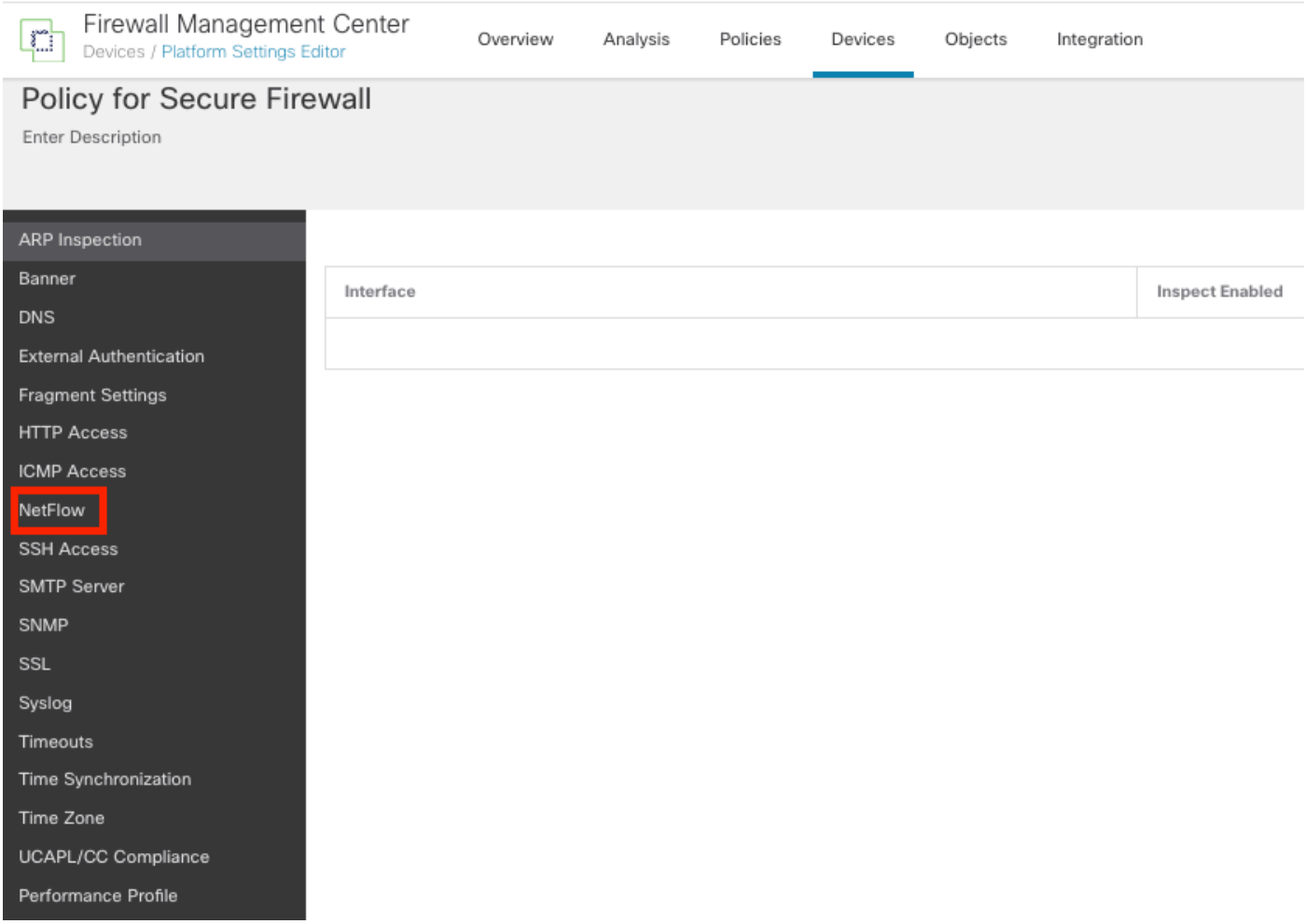
الوصول إلى إعدادات النظام الأساسي

الخطوة 2. تحرير نهج إعدادات النظام الأساسي المعين لجهاز المراقبة:



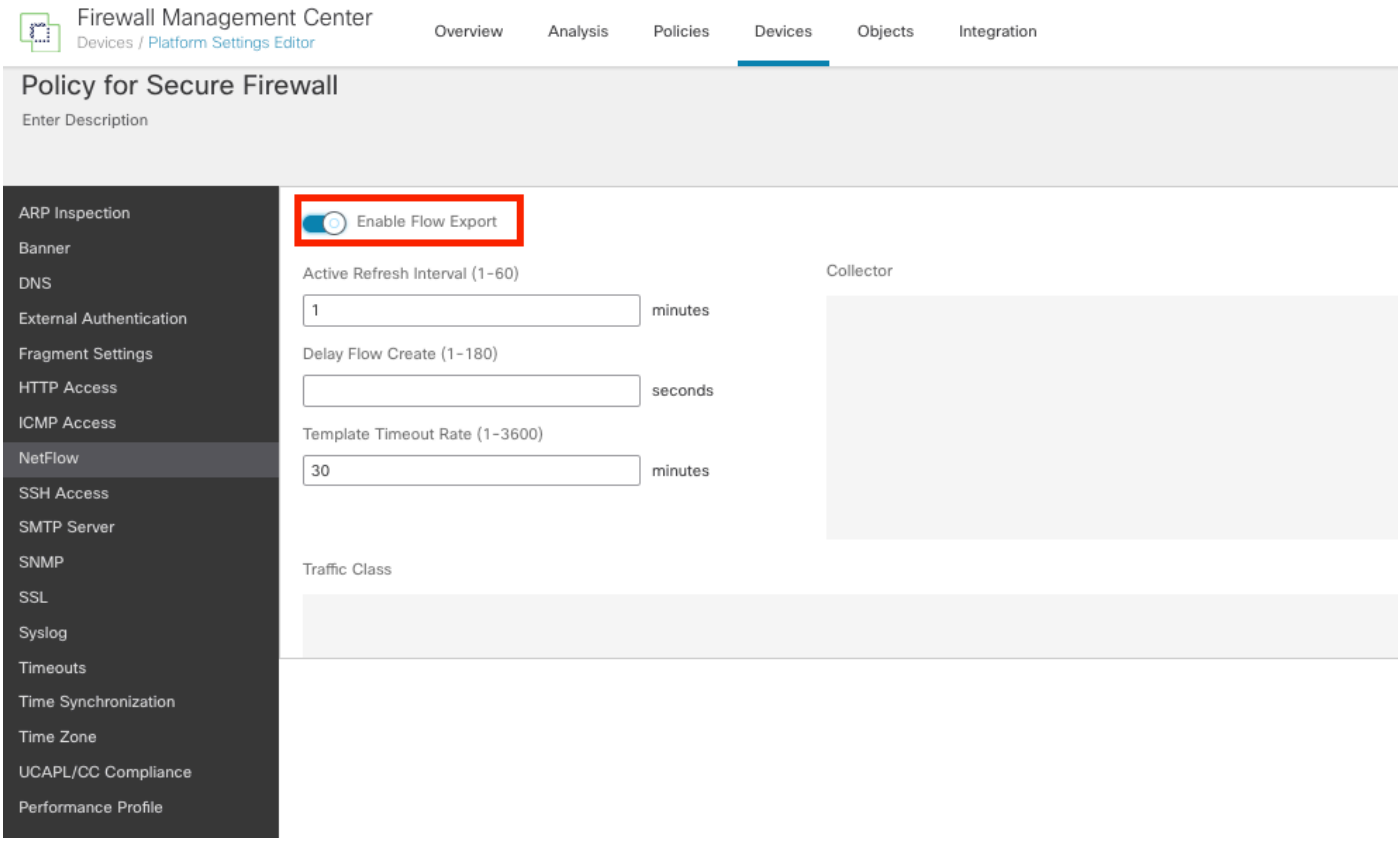
إصدار النهج

الخطوة 3. أختر NetFlow:



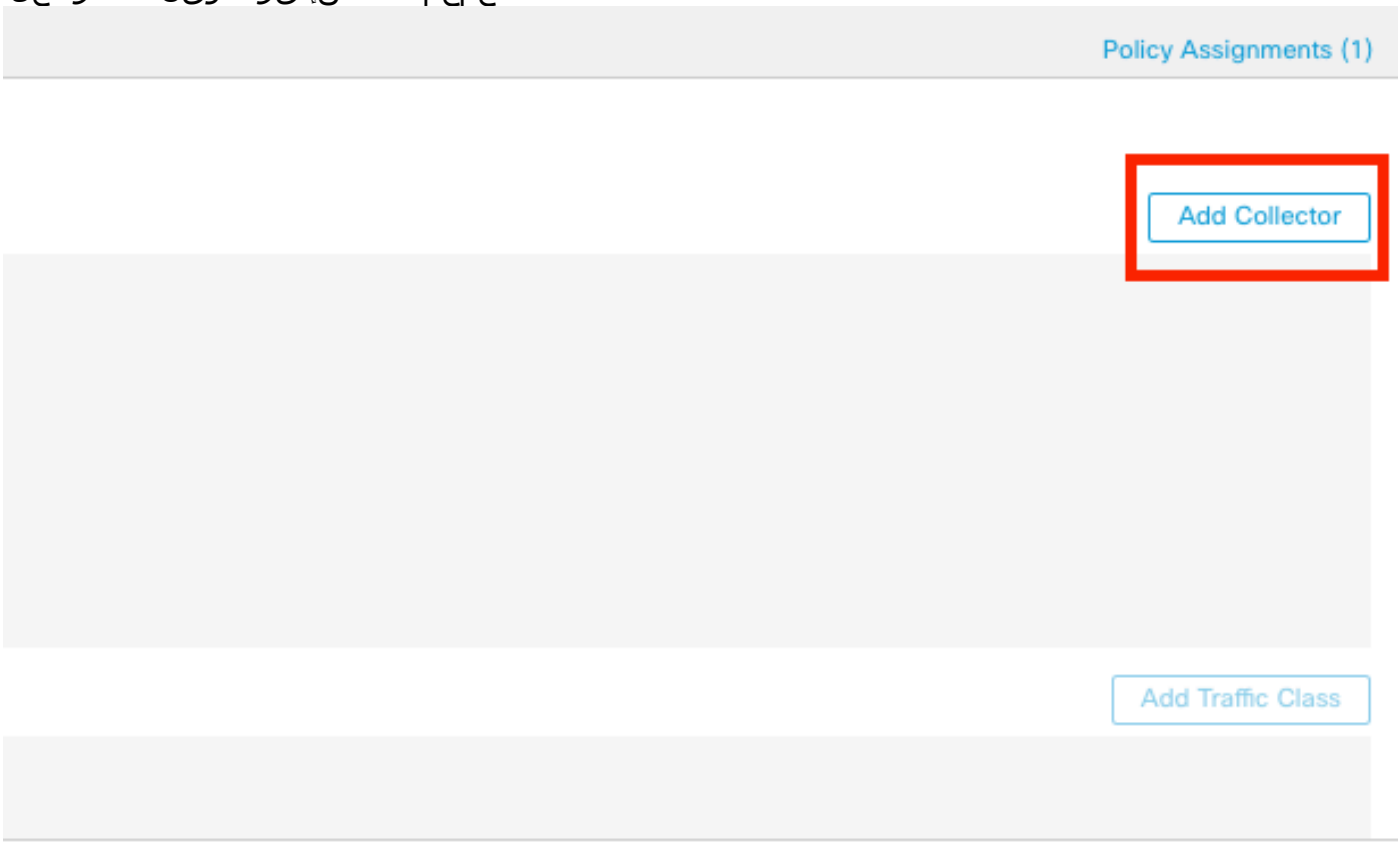
الوصول الى إعدادات NetFlow

الخطوة 4. تمكين تحويل تصدير التدفق لتمكين تصدير بيانات NetFlow:



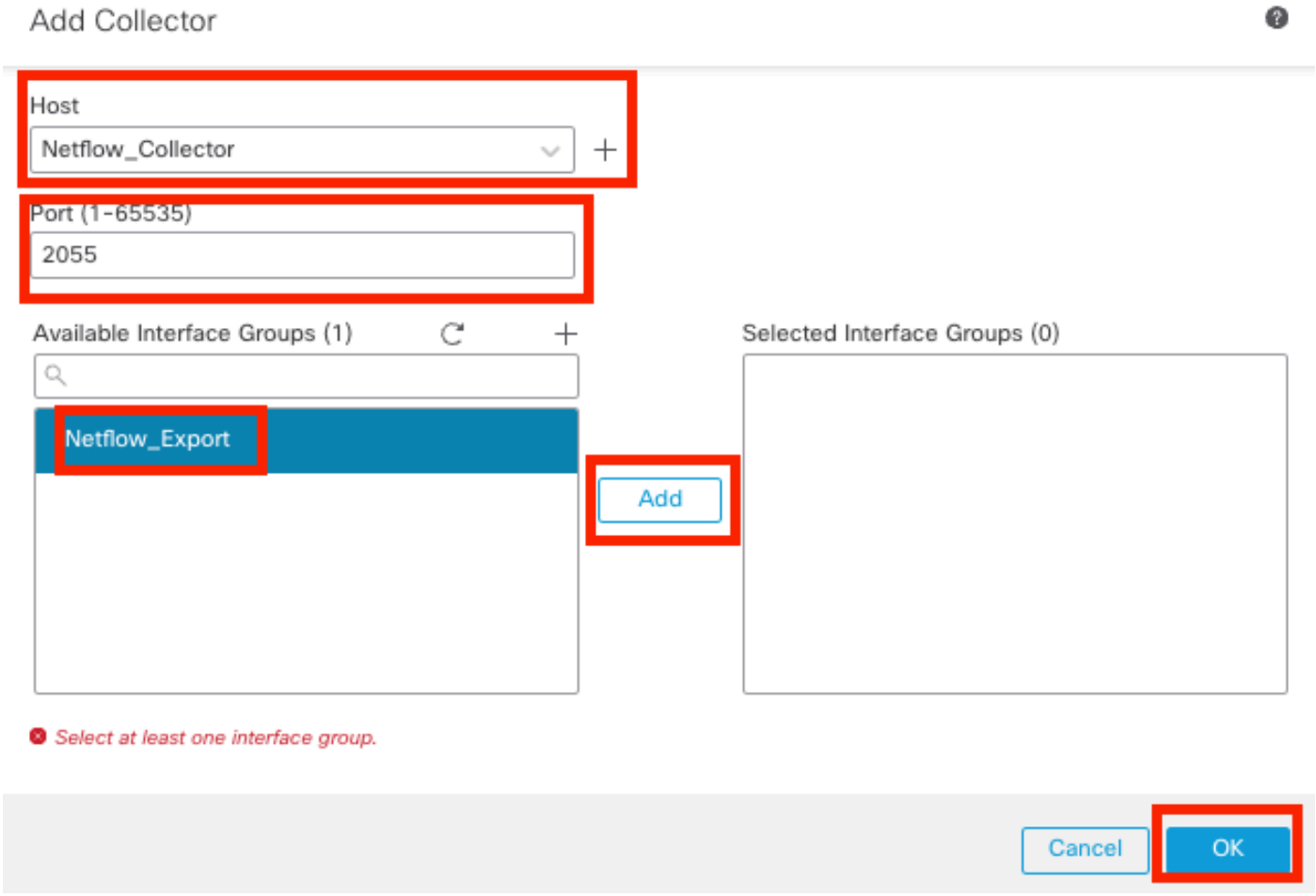
تمكين NetFlow

الخطوة 5. انقر فوق إضافة مجمع:



مجمع إضافة

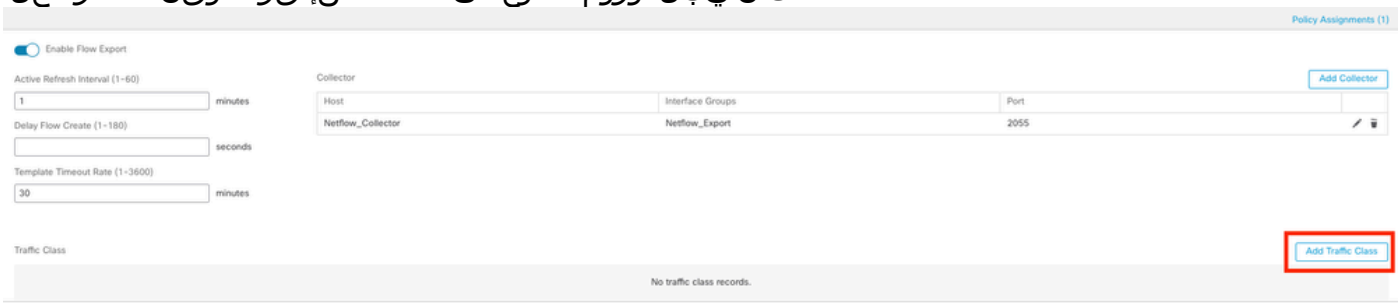
الخطوة 6. أختر كائن IP لمضيف المجمع الخاص بمجمع أحداث NetFlow، ومنفذ UDP على مجمع البيانات الذي يجب إرسال حزم NetFlow إليه، واختر مجموعة الواجهة التي يجب الوصول إلى مجمع البيانات من خلالها، وانقر فوق موافق:



إعدادات مجمع البيانات

إضافة فئة حركة مرور البيانات إلى NetFlow

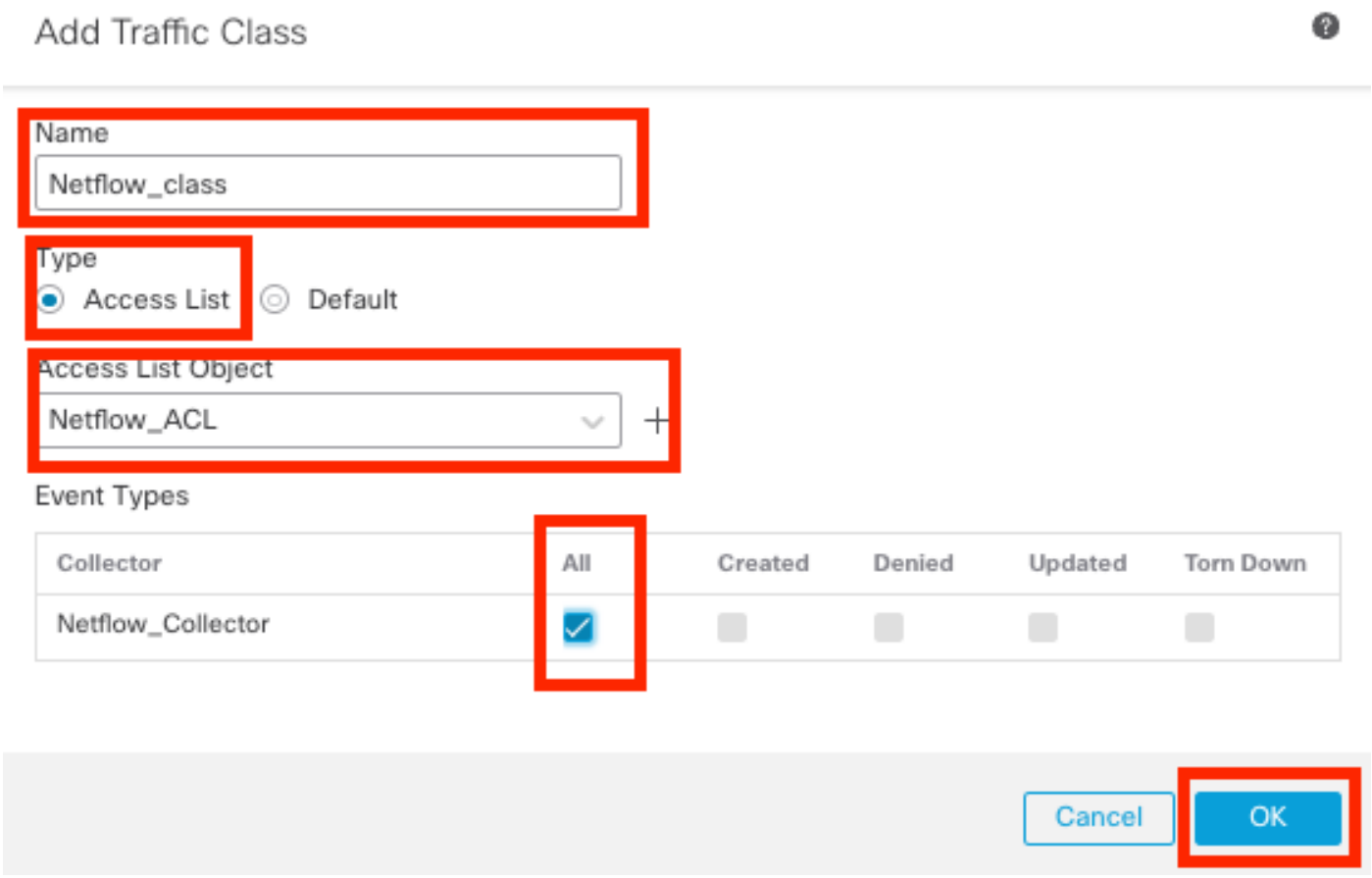
الخطوة 1. انقر فوق إضافة فئة حركة مرور البيانات:



إضافة فئة حركة المرور

الخطوة 2. أدخل حقل الاسم لفئة حركة المرور التي يجب أن تطابق أحداث NetFlow، قائمة التحكم في الوصول (ACL) لتحديد فئة حركة المرور التي يجب أن تطابق حركة المرور التي يتم التقاطها لأحداث NetFlow، حدد خانات الاختيار الخاصة بأحداث NetFlow المختلفة التي

تريد إرسالها إلى أدوات التجميع وانقر فوق موافق:



إعدادات فئة حركة مرور البيانات

استكشاف الأخطاء وإصلاحها

الخطوة 1. يمكنك التحقق من التكوين من واجهة سطر الأوامر (CLI) ل FTD.

1.1. من واجهة سطر الأوامر (CLI) الخاصة ب FTD، أدخل إلى واجهة سطر الأوامر (CLI) الخاصة بدعم النظام:

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

1.2 فحص تكوين خريطة السياسة:

<#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

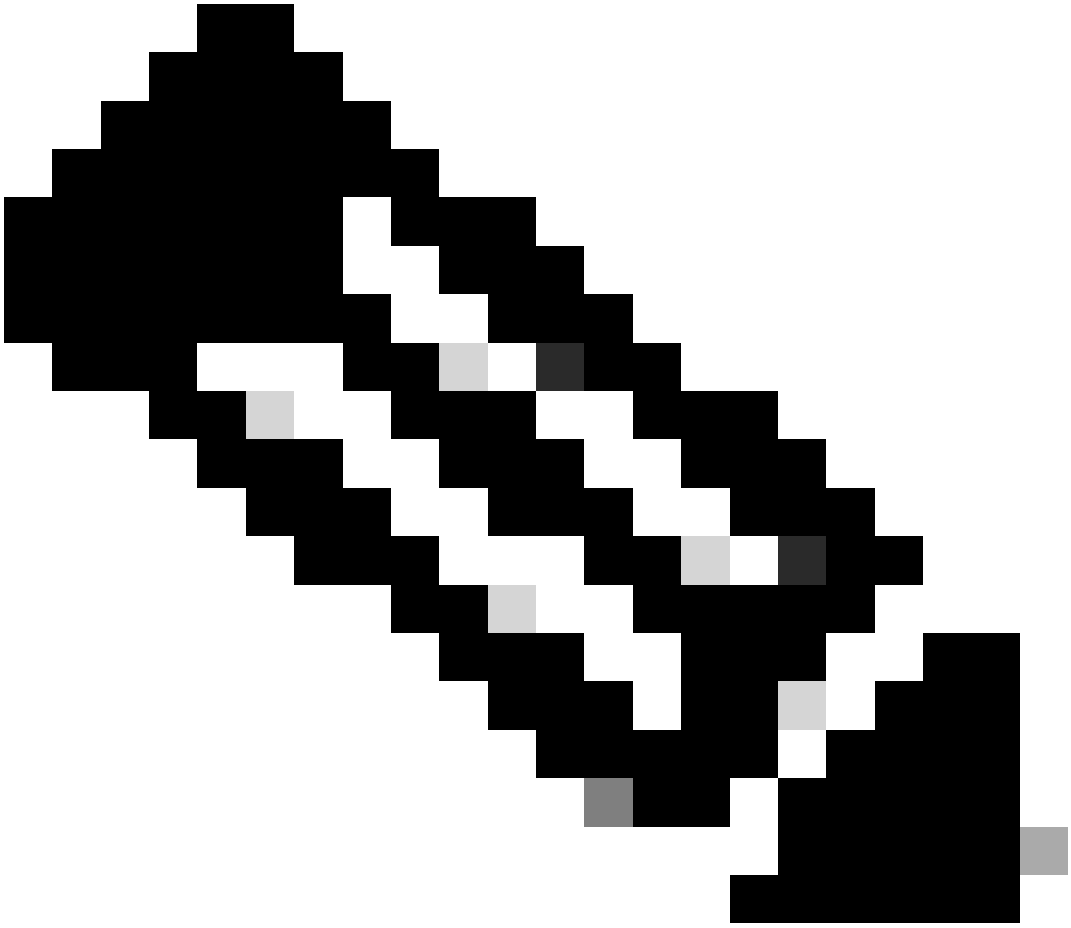
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. تحقق من تكوين تدفق-تصدير:

<#root>

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

flow-export destination Inside 192.168.31.1 2055



ملاحظة: في هذا المثال، "Inside" هو اسم الواجهة التي تم تكوينها في مجموعة الواجهة التي تسمى NetFlow_Export

الخطوة 2. التحقق من عدد مرات الوصول لقائمة التحكم في الوصول (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
```

الخطوة 3. التحقق من عدادات 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
```

معلومات ذات صلة

- [دليل تكوين جهاز مركز إدارة جدار الحماية الآمن من Cisco، الإصدار 7.4]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).