

Configuration de NetFlow dans FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Ajouter un collecteur dans NetFlow](#)

[Ajouter une classe de trafic à NetFlow](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer Netflow dans Cisco Secure Firewall Management Center exécutant la version 7.4 ou ultérieure.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Secure Firewall Management Center pour VMWare exécute v7.4.1
- Le pare-feu sécurisé exécute v7.4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

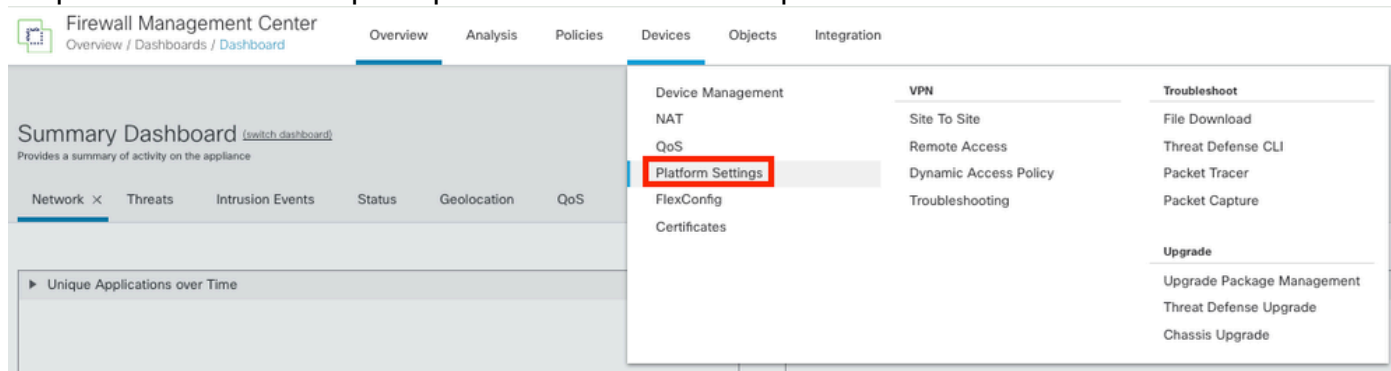
Informations générales

Les exigences spécifiques de ce document sont les suivantes :

- Cisco Secure Firewall Threat Defense version 7.4 ou ultérieure
- Cisco Secure Firewall Management Center version 7.4 ou ultérieure

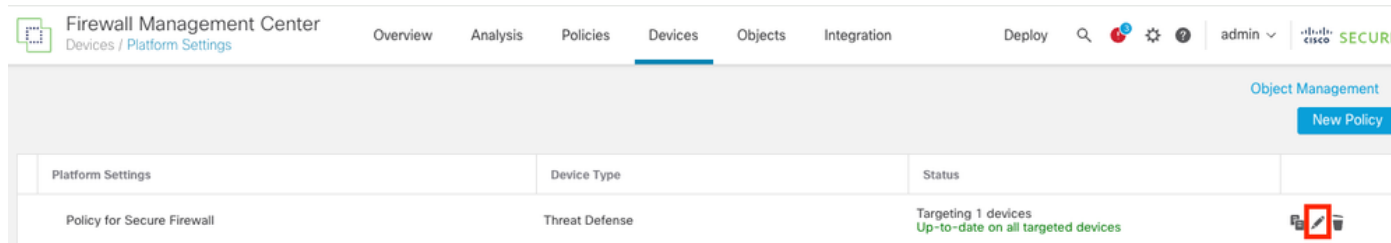
Ajouter un collecteur dans NetFlow

Étape 1. Accédez à Périphériques > Paramètres de la plate-forme :



Accès aux paramètres de plateforme

Étape 2. Modifiez la stratégie des paramètres de plate-forme attribuée au périphérique de surveillance :



Édition Politique

Étape 3. Choisissez Netflow :



Policy for Secure Firewall

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Interface

Inspect Enabled

Accès aux paramètres NetFlow

Étape 4. Activez l'option d'exportation de flux pour activer l'exportation de données NetFlow :

Policy for Secure Firewall

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Enable Flow Export

Active Refresh Interval (1-60)

minutes

Delay Flow Create (1-180)

seconds

Template Timeout Rate (1-3600)

minutes

Collector

Traffic Class

Activation de NetFlow

Étape 5. Cliquez sur Add Collector :

Policy Assignments (1)

Add Collector

Add Traffic Class

Ajout du collecteur

Étape 6. Choisissez l'objet IP hôte collecteur du collecteur d'événements NetFlow, le port UDP sur le collecteur auquel les paquets NetFlow doivent être envoyés, choisissez le groupe d'interfaces par lequel le collecteur doit être atteint, et cliquez sur OK :

Add Collector

Host
Netflow_Collector

Port (1-65535)
2055

Available Interface Groups (1) +
Netflow_Export

Selected Interface Groups (0)

Add

Select at least one interface group.

Cancel OK

Paramètres du collecteur

Ajouter une classe de trafic à NetFlow

Étape 1. Cliquez sur Ajouter une classe de trafic :

Enable Flow Export

Active Refresh Interval (1-60)
1 minutes

Delay Flow Create (1-180)
seconds

Template Timeout Rate (1-3600)
30 minutes

Host	Interface Groups	Port	
Netflow_Collector	Netflow_Export	2055	<input type="button" value="Add Collector"/>

Traffic Class

No traffic class records.

Ajout de classe de trafic

Étape 2. Entrez le champ de nom de la classe de trafic qui doit correspondre aux événements NetFlow, la liste de contrôle d'accès pour spécifier la classe de trafic qui doit correspondre au trafic capturé pour les événements NetFlow, sélectionnez les cases à cocher pour les différents

événements NetFlow que vous souhaitez envoyer aux collecteurs et cliquez sur OK :

Add Traffic Class ?

Name
Netflow_class

Type
 Access List Default

Access List Object
Netflow_ACL

Event Types

Collector	All	Created	Denied	Updated	Torn Down
Netflow_Collector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Paramètres de classe de trafic

Dépannage

Étape 1. Vous pouvez vérifier la configuration à partir de l'interface CLI FTD.

1.1. À partir de l'interface de ligne de commande FTD, entrez sur system support diagnostic-cli:

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

1.2 Vérification de la configuration de la carte de stratégie :

```
<#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
```

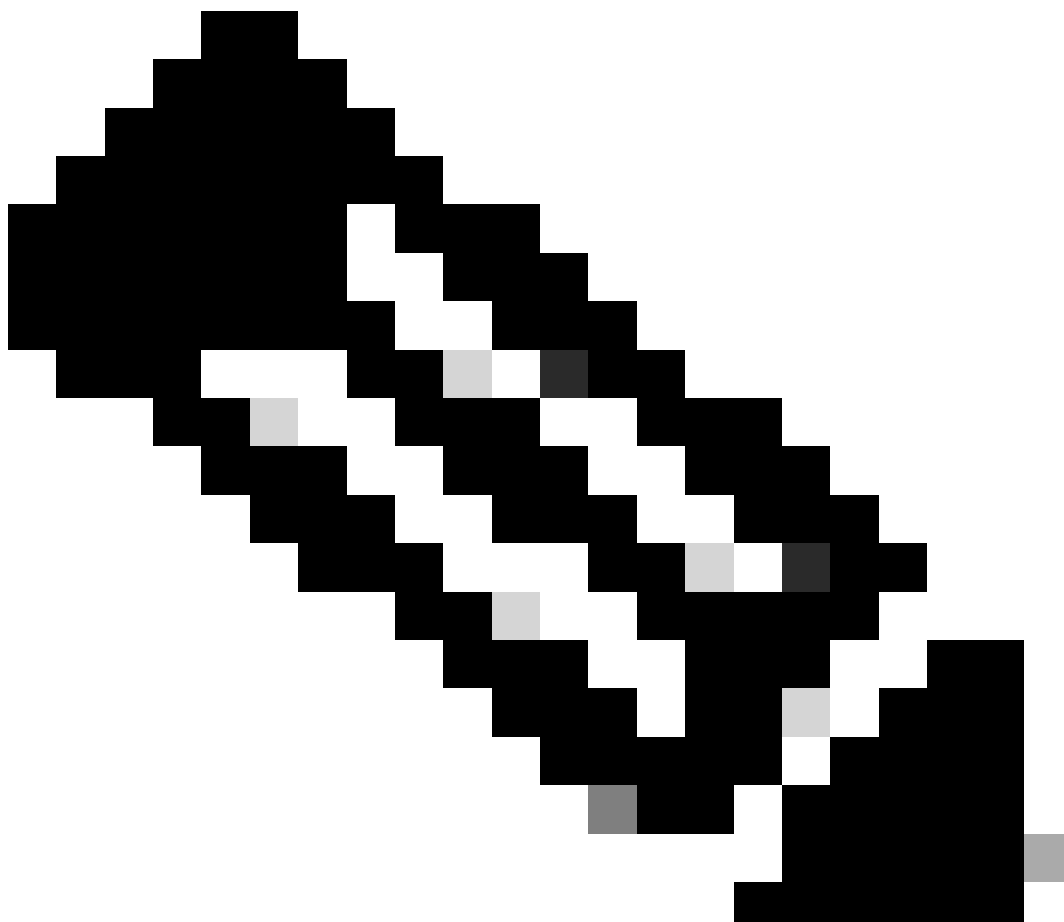
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Vérifiez la configuration flow-export :

```
<#root>
```

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

```
flow-export destination Inside 192.168.31.1 2055
```



Remarque : dans cet exemple, « Inside » est le nom de l'interface configurée dans le groupe d'interfaces appelé Netflow_Export

Étape 2. Vérifiez le nombre d'occurrences de la liste de contrôle d'accès :

```
<#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
```


Étape 3. Vérifiez les compteurs 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
```

Informations connexes

- [Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.4](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.