Configuration de la journalisation sécurisée des événements NetFlow sur Firepower Threat Defense

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Informations générales

Configurer

Vérifier

Informations connexes

Introduction

Ce document décrit comment configurer NetFlow Secure Event Logging (NSEL) sur Firepower Threat Defense (FTD) via Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du FMC
- Connaissance du DFT
- Connaissance de la politique FlexConfig

Composants utilisés

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

- FTD version 6.6.1
- FMC version 6.6.1

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

Ce document décrit comment configurer NetFlow Secure Event Logging (NSEL) sur Firepower Threat Defense (FTD) via Firepower Management Center (FMC).

Les objets texte FlexConfig sont associés aux variables utilisées dans les objets FlexConfig prédéfinis. Les objets FlexConfig prédéfinis et les objets texte associés se trouvent dans FMC pour configurer NSEL. Il existe quatre objets FlexConfig prédéfinis dans le FMC et trois objets texte prédéfinis. Les objets FlexConfig prédéfinis sont en lecture seule et ne peuvent pas être modifiés. Pour modifier les paramètres de NetFlow, vous pouvez copier les objets.

Les quatre objets prédéfinis sont répertoriés dans le tableau :

FlexConfig Object Name	Description
Netflow_Add_Destination	Creates and configures a NetFlow export destination
Netflow_Set_Parameters	Sets globla parameters for NetFlow export
Netflow_Delete_Destinations	Deletes a NetFlow export destination
Netwflow_Clear_Parameters	Restores Netflow export global default settings

Les trois objets de texte prédéfinis sont répertoriés dans le tableau :

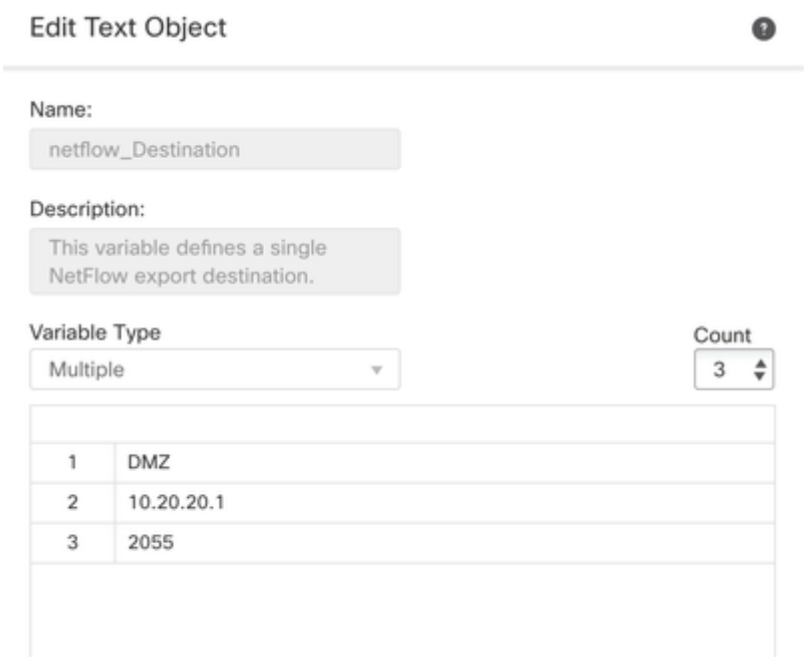
Text Object Name	Description
netflow_Destination	Define the single NetFlow export destination's interface, destination IP address and UDP port number for NetFlow.
netwflow_Event_Types	Define NetFlow events based on event type
netflow_Parameters	Define values for active refresh-interval, delay flow-create and template timeout-rate.

Configurer

Cette section décrit comment configurer NSEL sur FMC via une politique FlexConfig.

Étape 1 : définition des paramètres des objets texte pour Netflow

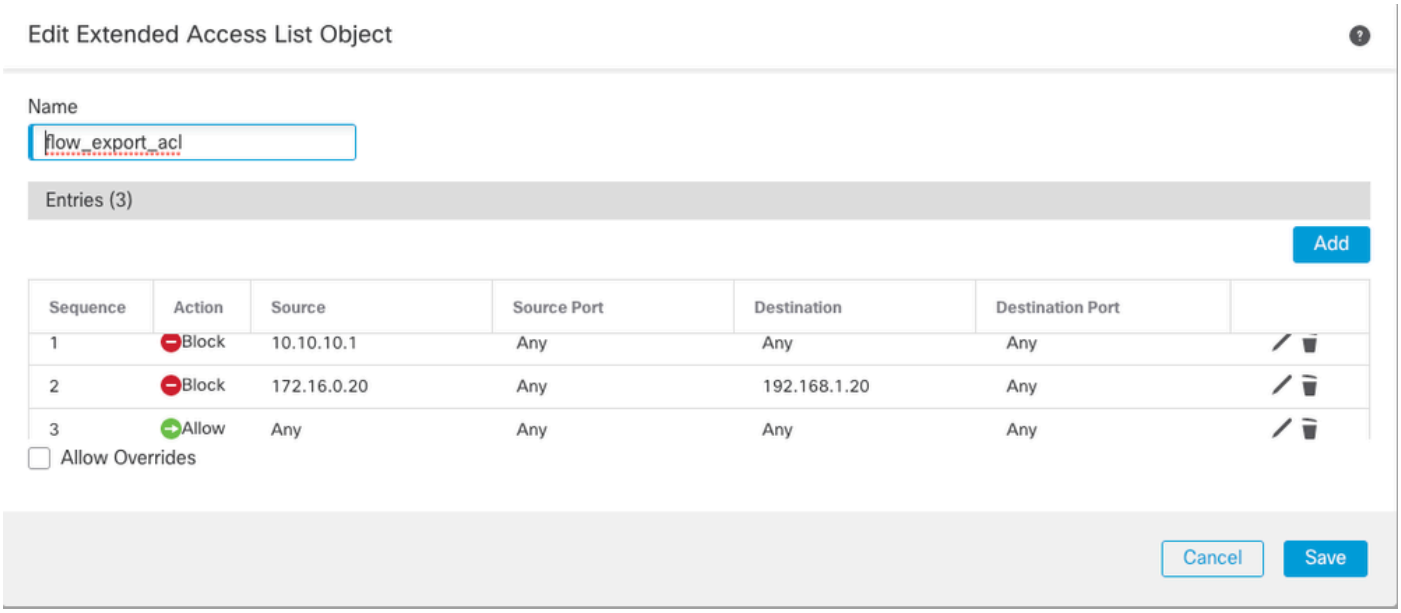
1. Pour définir les paramètres de la variable, accédez à Objets > FlexConfig > Objets texte.
2. Modifiez l'objet netflow_Destination.
3. Définissez le type de variable multiple et le jeu de nombres sur 3.
4. Définissez le nom de l'interface, l'adresse IP de destination et le port. Dans cet exemple de configuration, l'interface est DMZ, l'adresse IP du collecteur NetFlow est 10.20.20.1 et le port UDP est 2055.



Remarque : Les valeurs par défaut pour netflow_Event_Types et netflow_Parameters sont utilisées.

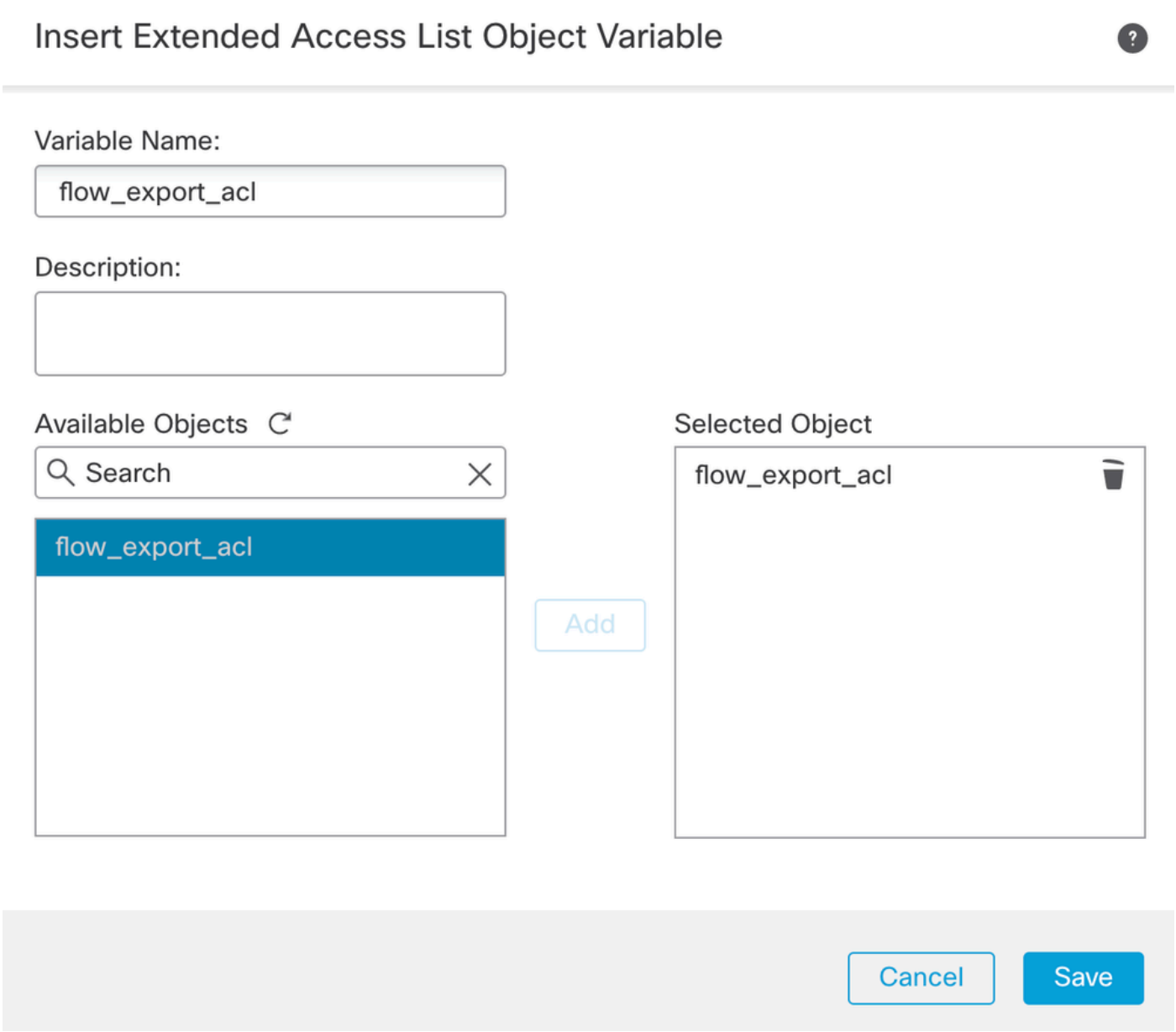
Étape 2 : configuration d’un objet de liste de contrôle d’accès étendue pour correspondre à un trafic spécifique

1. Pour créer une liste d'accès étendue sur FMC, accédez à Objets > Gestion des objets et dans le menu de gauche, sous Liste d'accès, sélectionnez Étendue.
2. Cliquez sur Add Extended Access List.
3. Renseignez le champ Nom. Dans cet exemple, le nom est flow_export_acl.
4. Cliquez sur Ajouter.
5. Configurez les entrées de contrôle d'accès pour qu'elles correspondent à un trafic spécifique. Dans cet exemple, le trafic de l'hôte 10.10.10.1 vers n'importe quelle destination et le trafic entre l'hôte 172.16.0.20 et 192.168.1.20 est exclu. Tout autre trafic est inclus.



Étape 3 : configuration d’un objet FlexConfig

1. Pour configurer les objets FlexConfig, accédez à Objets > FlexConfig > Objets FlexConfig et cliquez sur Ajouter un objet FlexConfig.
2. Définissez le mappage de classe qui identifie le trafic pour lequel les événements NetFlow doivent être exportés.
3. Dans cet exemple, le nom de l'objet est flow_export_class.
4. Sélectionnez la liste d'accès créée à l'étape 2.
5. Cliquez sur Insert > Insert Policy Object > Extended ACL Object et attribuez un nom.
6. Puis, cliquez sur Add (ajouter). Dans cet exemple, le nom de la variable est flow_export_acl.
7. Cliquez sur Save.



Ajoutez les lignes de configuration suivantes dans le champ vide à droite et incluez la variable précédemment définie ($flow_export_acl.) dans la ligne de configuration match access-list.

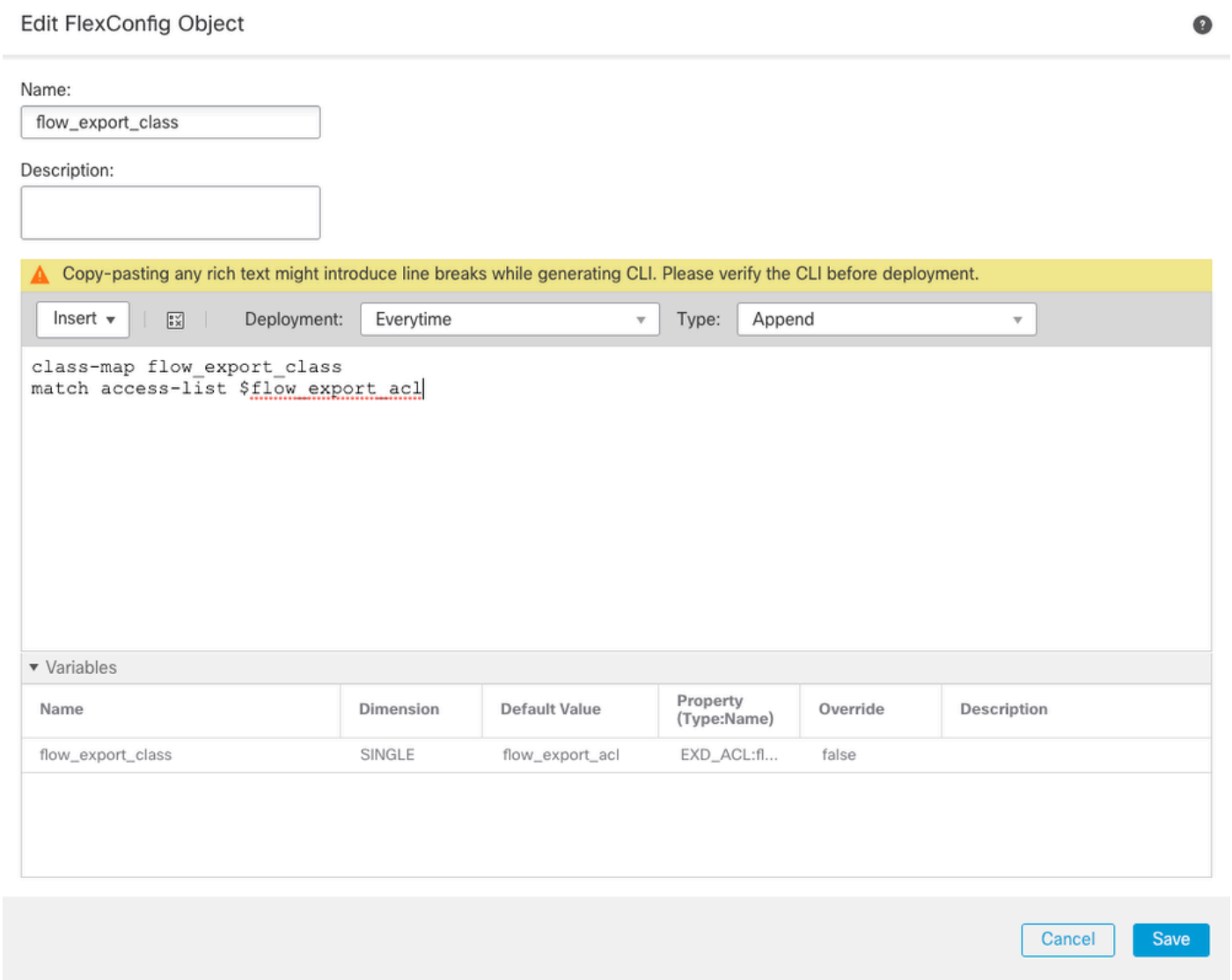
Notez qu'un symbole $ commence le nom de la variable. Cela permet de définir une variable qui vient après elle.

<#root>

```
class-map flow_export_class
match access-list

$flow_export_acl
```

Cliquez sur Save lorsque vous avez terminé.



Étape 4. Configuration de la destination Netflow

1. Pour configurer la destination Netflow, accédez à Objets > FlexConfig > Objets FlexConfig et filtrez par Netflow.
2. Copiez l'objet Netflow_Add_Destination. Maintenant, Netflow_Add_Destination_Copy est créé.
3. Affectez la classe créée à l'étape 3. Vous pouvez créer une nouvelle carte de stratégie pour appliquer les actions d'exportation de flux aux classes définies. Dans cet exemple, la classe est insérée dans la stratégie actuelle (stratégie globale).

<#root>

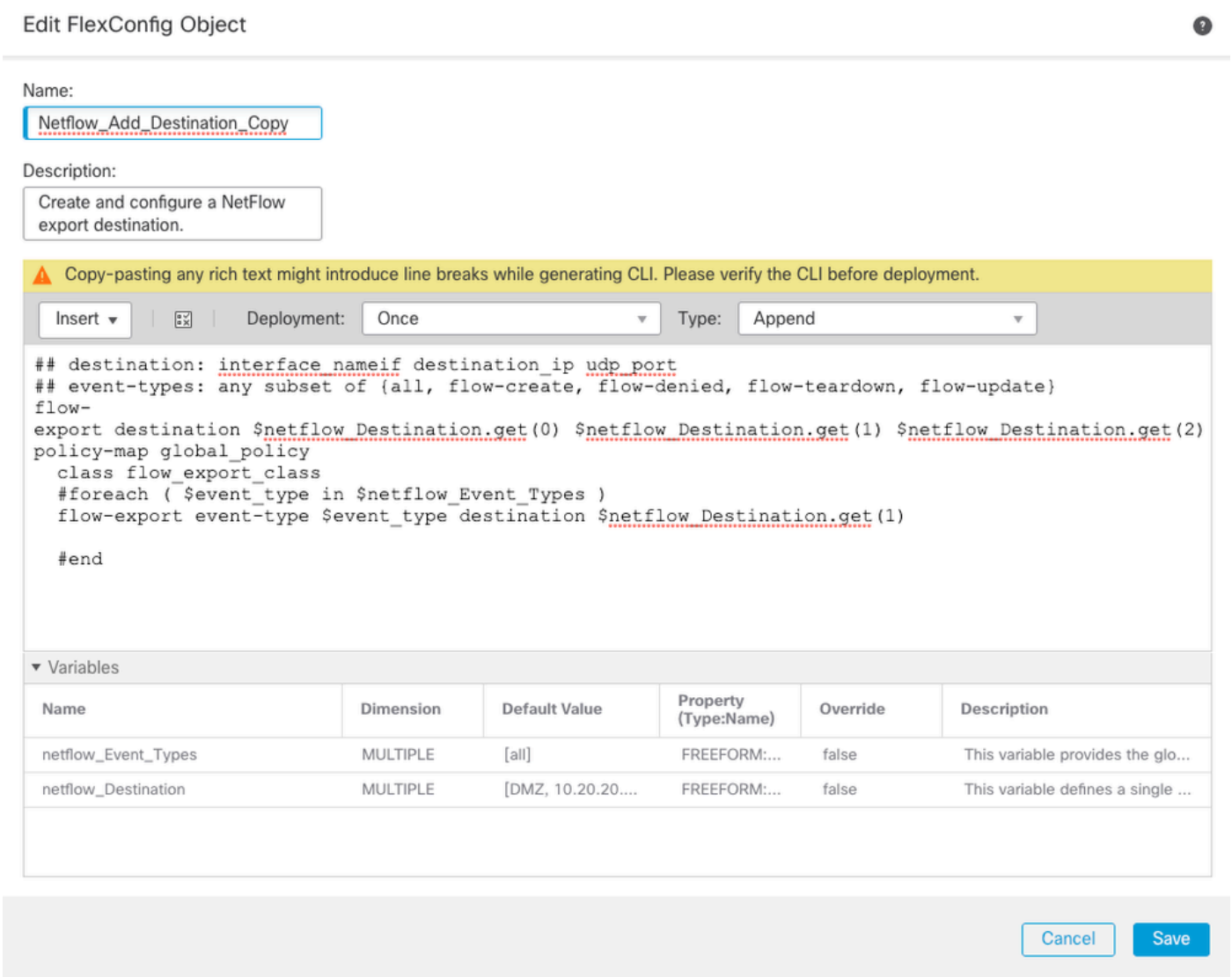
```
## destination: interface_nameif destination_ip udp_port
## event-types: any subset of {all, flow-create, flow-denied, flow-teardown, flow-update}
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.ge
```

```
policy-map global_policy
  class
```

`flow_export_class`

```
  #foreach ( $event_type in $netflow_Event_Types )
  flow-export event-type $event_type destination $netflow_Destination.get(1)
  #end
```

4. Cliquez sur Enregistrer lorsque vous avez terminé.

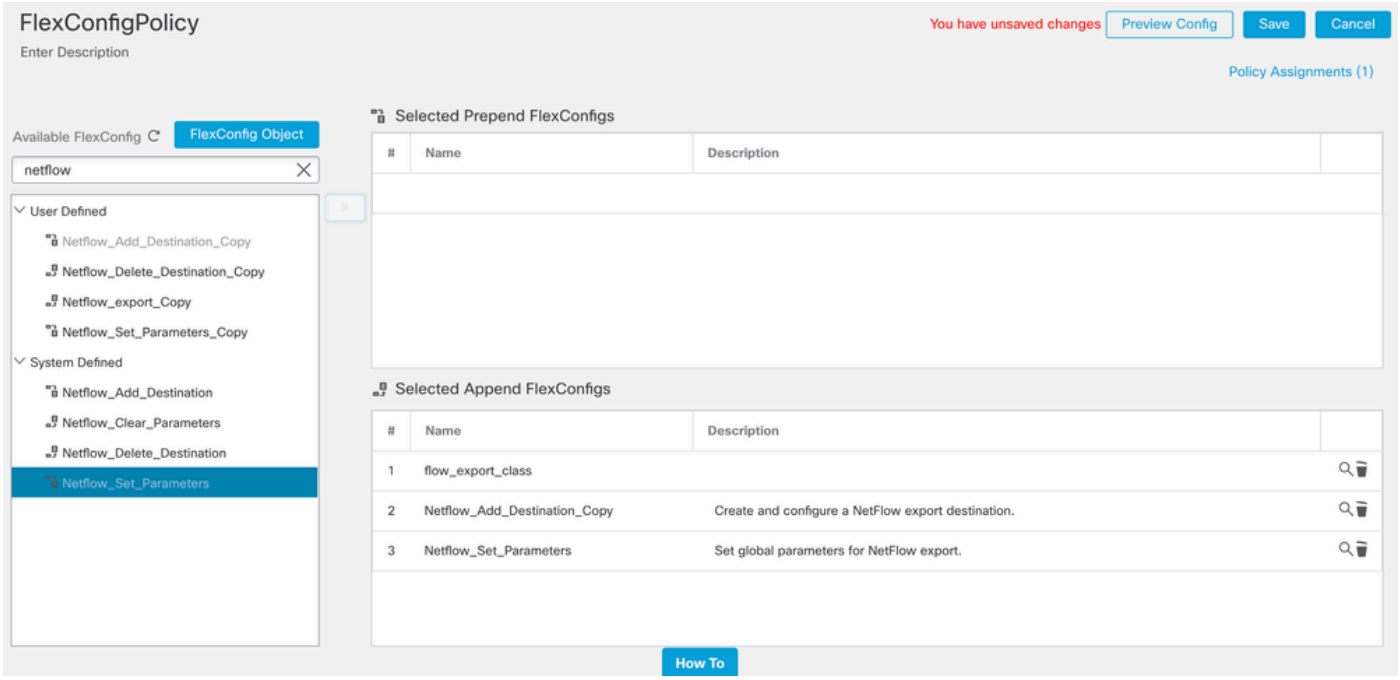


Étape 5. Attribution de la stratégie FlexConfig au FTD

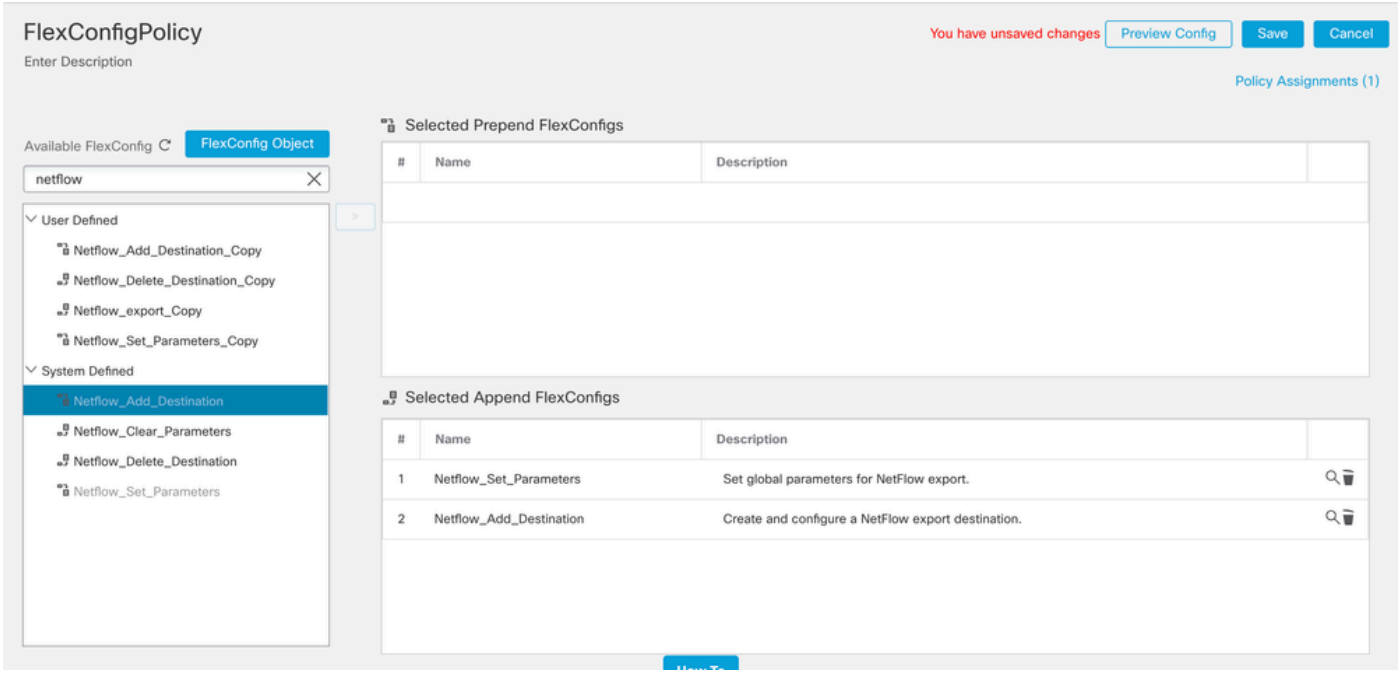
1. Accédez à Devices > FlexConfig et créez une nouvelle stratégie (sauf si une stratégie a déjà été créée à une autre fin et attribuée au même FTD). Dans cet exemple, la configuration FlexConfig est déjà créée.
2. Modifiez la politique FlexConfig et sélectionnez les objets FlexConfig créés lors des étapes

précédentes. Dans cet exemple, les paramètres d'exportation Netflow par défaut sont utilisés, par conséquent, Netflow_Set_Parameters est sélectionné.

3. Enregistrez vos modifications et déployez.

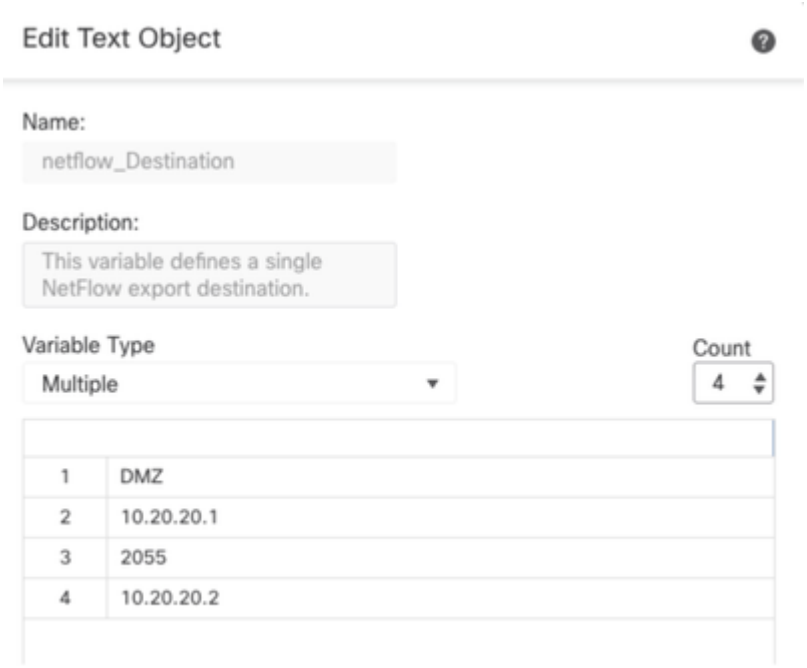


Remarque : Pour faire correspondre tout le trafic sans avoir à faire correspondre un trafic spécifique, vous pouvez passer des étapes 2 à 4 et utiliser les objets NetFlow prédéfinis.



Remarque : Pour ajouter un second collecteur NSEL où les paquets NetFlow sont

envoyés. À l'étape 1, ajoutez 4 variables à ajouter à la deuxième adresse IP du collecteur Netflow.



À l'étape 4, ajoutez la ligne de configuration : flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)

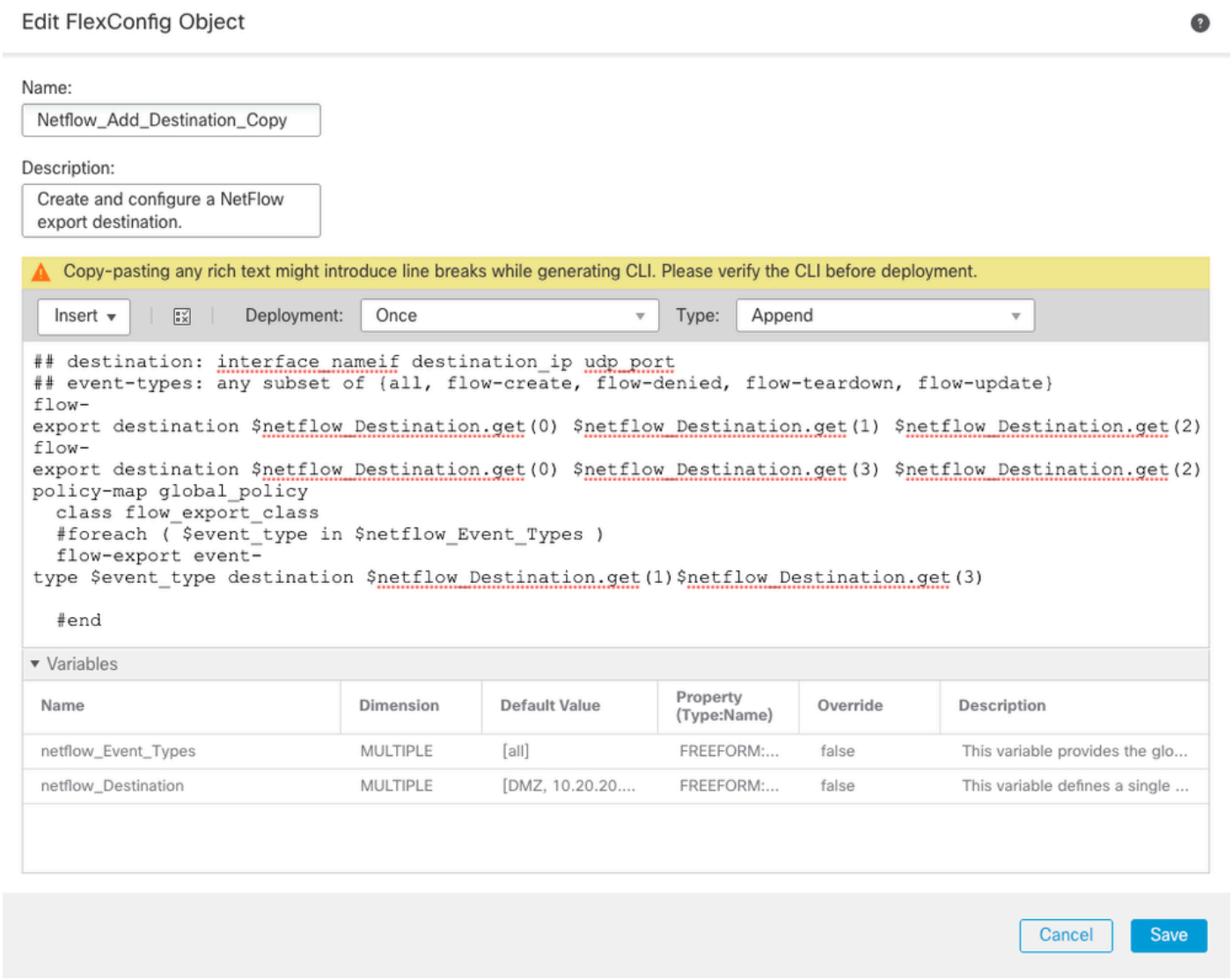
Modifiez la variable $netflow_Destination.get pour la variable de correspondance. Dans cet exemple, la valeur de la variable est 3. Par exemple :

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.ge
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(3) $netflow_Destination.ge
```

Ajoutez également la deuxième variable $netflow_Destination.get dans la ligne de configuration : flow-export event-type $event_type destination $netflow_Destination.get(1). Exemple :

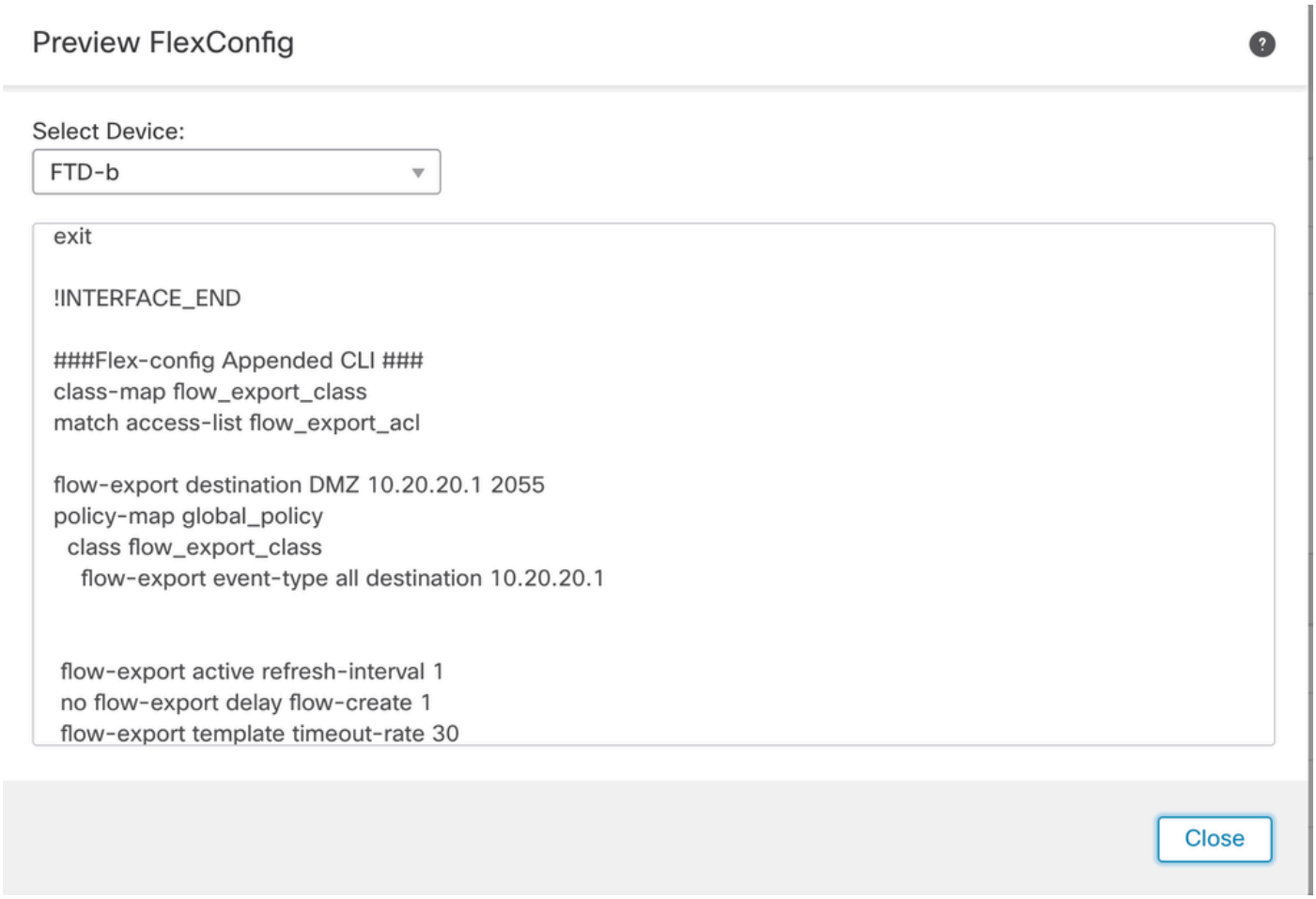
```
flow-export event-type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

Validez cette configuration comme indiqué dans l'image ci-dessous :



Vérifier

La configuration NetFlow peut être vérifiée dans la politique FlexConfig. Pour prévisualiser la configuration, cliquez sur Preview Config et sélectionnez le FTD et vérifiez la configuration.



Accédez au FTD via Secure Shell (SSH), exécutez la commande system support diagnostic-cli et exécutez les commandes suivantes :

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower# show access-list flow_export_acl
access-list flow_export_acl; 3 elements; name hash: 0xe30f1adf
access-list flow_export_acl line 1 extended deny object-group ProxySG_ExtendedACL_34359742097 object 10
access-list flow_export_acl line 1 extended deny ip host 10.10.10.1 any (hitcnt=0) 0x3d4f23a4
access-list flow_export_acl line 2 extended deny object-group ProxySG_ExtendedACL_34359742101 object 17
access-list flow_export_acl line 2 extended deny ip host 172.16.0.20 host 192.168.1.20 (hitcnt=0) 0x134
access-list flow_export_acl line 3 extended permit object-group ProxySG_ExtendedACL_30064776111 any any
access-list flow_export_acl line 3 extended permit ip any any (hitcnt=0) 0x759f5ecf
```

```
firepower# sh running-config class-map flow_export_class
class-map flow_export_class
match access-list flow_export_acl
```

```
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 xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
inspect snmp
class flow_export_class
flow-export event-type all destination 10.20.20.1
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
```

```
firepower# show running-config | include flow
access-list flow_export_acl extended deny object-group ProxySG_ExtendedACL_34359742097 object 10.10.10.
access-list flow_export_acl extended deny object-group ProxySG_ExtendedACL_34359742101 object 172.16.0.
access-list flow_export_acl extended permit object-group ProxySG_ExtendedACL_30064776111 any any
flow-export destination DMZ 10.20.20.1 2055
class-map flow_export_class
match access-list flow_export_acl
class flow_export_class
flow-export event-type all destination 10.20.20.1
```

Informations connexes

- Assistance technique de Cisco et téléchargements

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.