Vastlegging NetFlow Secure Event configureren bij Firepower Threat Defence

Inhoud

Inleiding

Dit document beschrijft hoe u NetFlow Secure Event Logging (NSEL) kunt configureren op Firepower Threat Defence (FTD) via Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het VCC
- Kennis van het FTD
- Kennis van het FlexConfig-beleid

Gebruikte componenten

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

- FTD versie 6.6.1
- FMC versie 6.6.1

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

Dit document beschrijft hoe u NetFlow Secure Event Logging (NSEL) kunt configureren op Firepower Threat Defence (FTD) via Firepower Management Center (FMC).

De FlexConfig-tekstobjecten zijn gekoppeld aan variabelen die worden gebruikt in de vooraf

gedefinieerde FlexConfig-objecten. Vooraf gedefinieerde FlexConfig-objecten en bijbehorende tekstobjecten worden gevonden in FMC om NSEL te configureren. Er zijn vier vooraf gedefinieerde FlexConfig-objecten in het VCC en drie vooraf gedefinieerde tekstobjecten. Voorgedefinieerde FlexConfig-objecten worden alleen-lezen en kunnen niet worden aangepast. Om de parameters van NetFlow aan te passen, kunnen de objecten worden gekopieerd.

De vier vooraf gedefinieerde objecten worden in de tabel weergegeven:

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

De drie vooraf gedefinieerde tekstobjecten worden in de tabel weergegeven:

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.

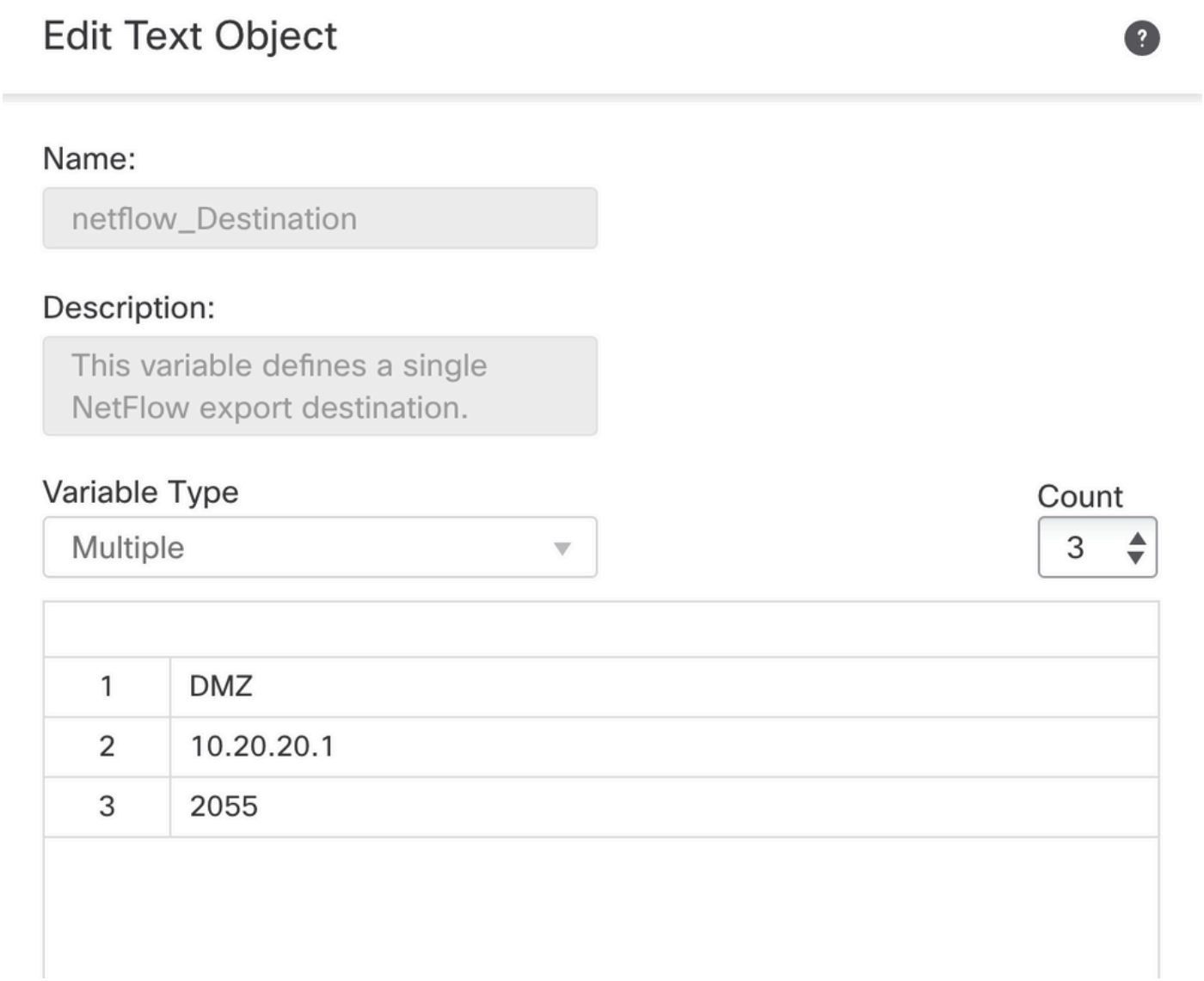
Configureren

In dit deel wordt beschreven hoe u NSEL op FMC kunt configureren via een FlexConfig-beleid.

Stap 1. Stel de parameters van de Tekstobjecten in voor NetFlow.

Als u de variabele parameters wilt instellen, navigeer dan naar **Objecten > FlexConfig > Tekstobjecten**. Bewerk het object netflow_Destination. Definieer het meerdere variabele type en telling ingesteld op 3. Stel de interfacenaam, het IP-adres en de poort van de bestemming in.

In dit configuratievoorbeeld is de interface DMZ, is het IP-adres van NetFlow Collector 10.20.20.1 en is de UDP-poort 2055.



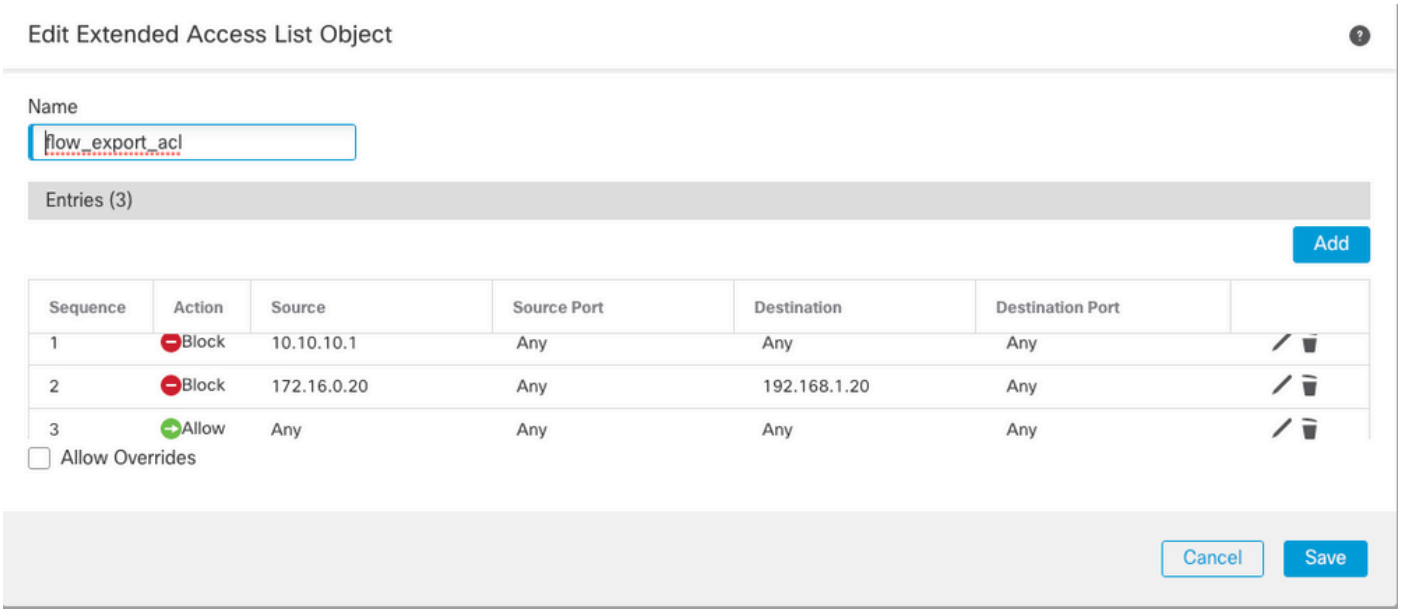
Opmerking: standaardwaarden voor netflow_Event_Types en netflow_Parameters worden gebruikt.

Stap 2. Configureer een object uitgebreide toegangslijst om specifiek verkeer aan te passen.

Om een uitgebreide toegangslijst op het VCC te maken, navigeer naar **Objecten > Objectbeheer** en in het linker menu, onder **Toegangslijst** uitkiezen **Uitgebreid.**Klik **Uitgebreide toegangslijst toevoegen.**

Vul het veld **Naam** in. In dit voorbeeld is de naam flow_export_acl. Klik op de knop **Toevoegen**. Configureer de vermeldingen **toegangscontrole** om specifiek verkeer aan te passen.

In dit voorbeeld is verkeer van host 10.10.10.1 naar elke bestemming en verkeer tussen host 172.16.0.20 en 192.168.1.20 uitgesloten. Al het andere verkeer is inbegrepen.

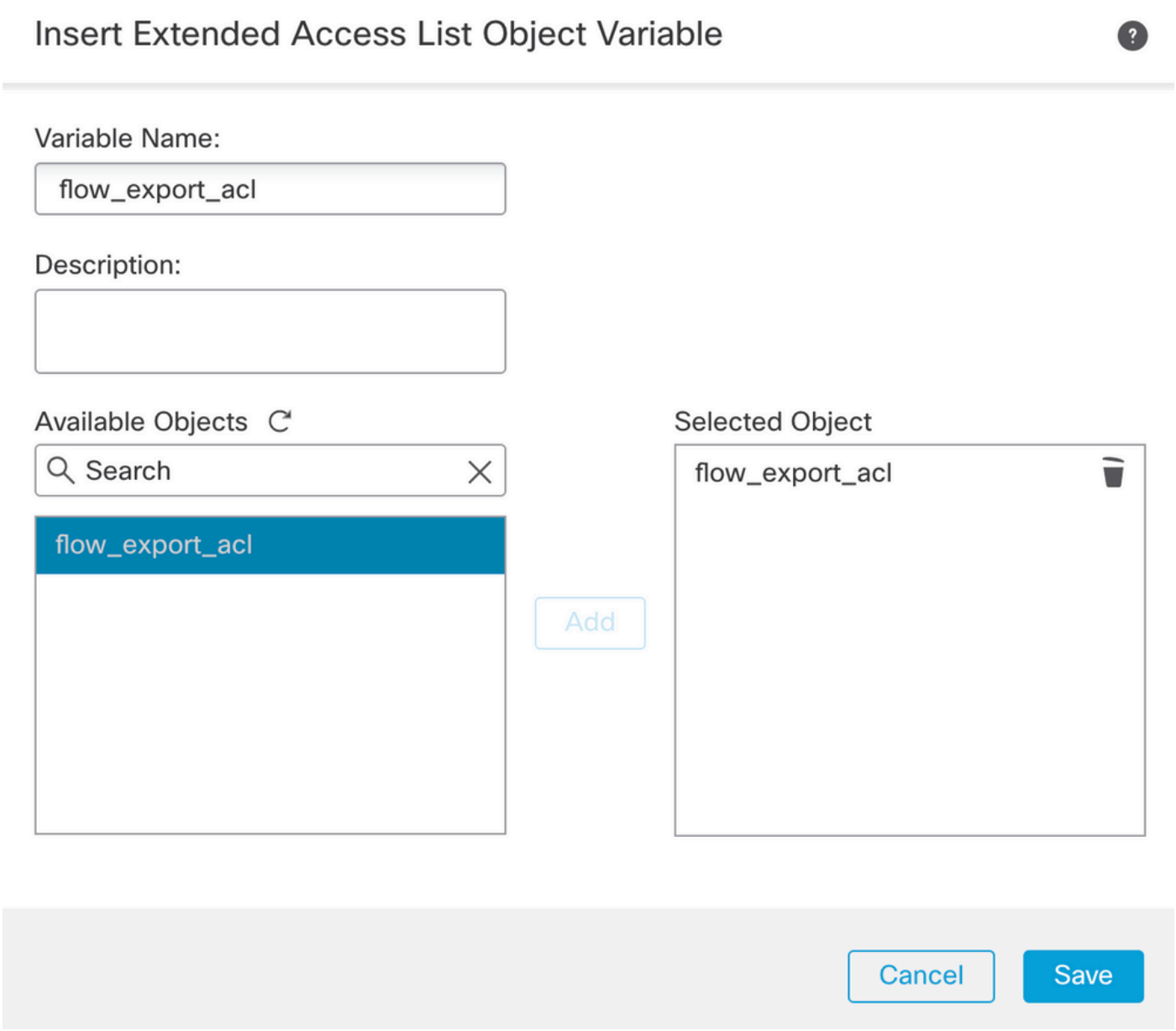


Stap 3. Configureer een FlexConfig-object.

Om de FlexConfig-objecten te configureren navigeert u naar **Objecten > FlexConfig > FlexConfig-objecten** en klikt u op de knop **Add FlexConfig Object** .

Definieer de klassekaart die verkeer identificeert waarvoor NetFlow-gebeurtenissen moeten worden geëxporteerd. In dit voorbeeld is de naam van het object flow_export_class.

Selecteer de toegangslijst die in Stap 2 is gemaakt. Klik op **Invoegen > Beleidsobject invoegen > Uitgebreid ACL-object** en wijs een naam toe. Klik vervolgens op de knop **Toevoegen**. In dit voorbeeld is de naam van de variabele flow_export_acl. Klik op **Save** (Opslaan).

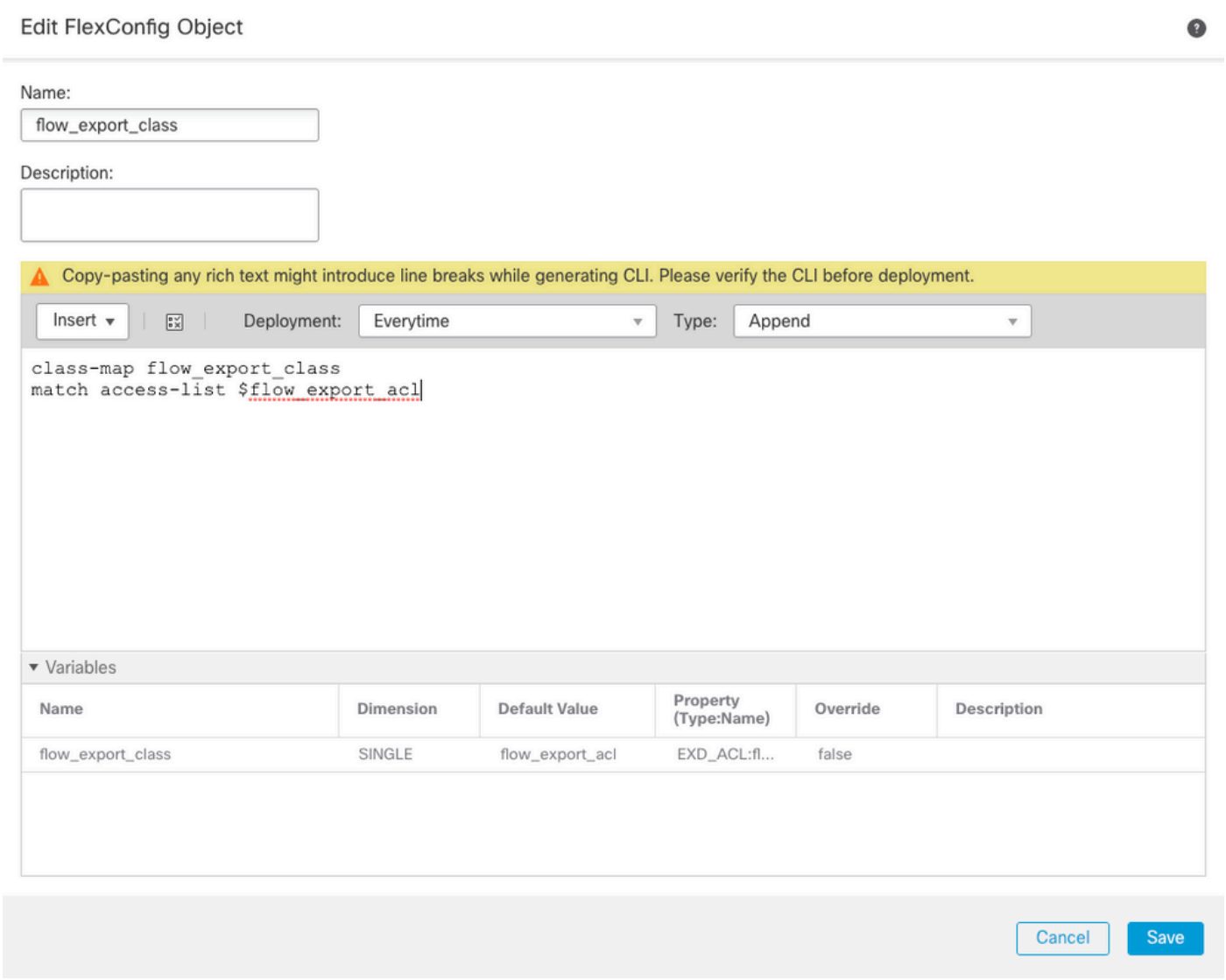


Voeg de volgende configuratielijnen toe in het lege veld rechts en neem de variabele die eerder is gedefinieerd (**$flow_export_acl.**) op in de configuratielijn voor overeenkomende toegangslijsten.

Het is een **$** Het symbool begint met de variabele naam. Dit helpt te definiëren dat een variabele erna komt.

```
class-map flow_export_class
match access-list $flow_export_acl
```

Klik op **Opslaan** als u klaar bent.



Stap 4. De NetFlow-bestemming configureren

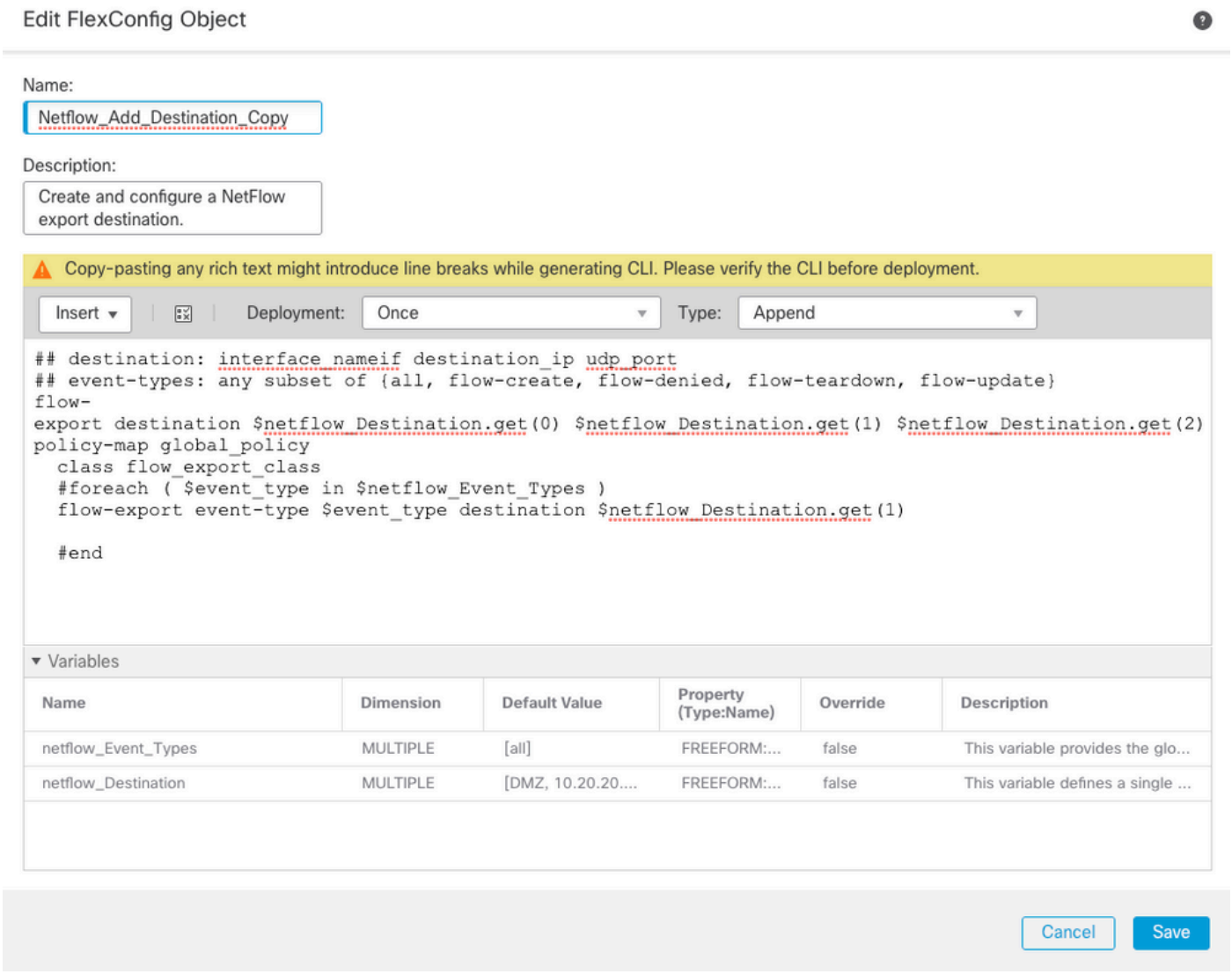
Als u de NetFlow-bestemming wilt configureren, navigeert u naar **Objecten** > **FlexConfig** > **FlexConfig**-objecten en filter via NetFlow. **Kopieert** het object NetFlow_Add_Destination. De NetFlow_Add_Destination_Copy wordt aangemaakt.

Wijs de klasse toe die in Stap 3 is gemaakt. U kunt een nieuwe beleidskaart maken om de flow-export-acties op de gedefinieerde klassen toe te passen.

In dit voorbeeld wordt de klasse ingevoegd in het huidige beleid (globaal beleid).

```
## 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.
get(2)
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
```

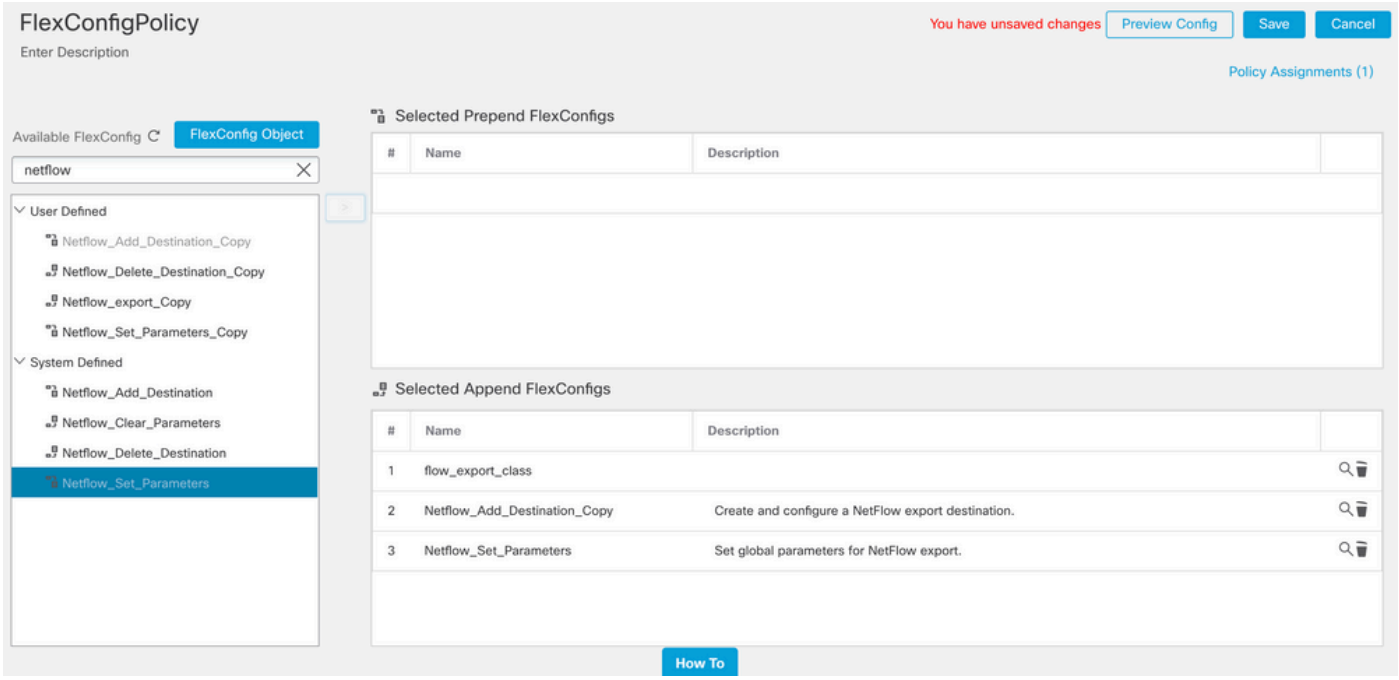
Klik op **Opslaan** als u klaar bent.



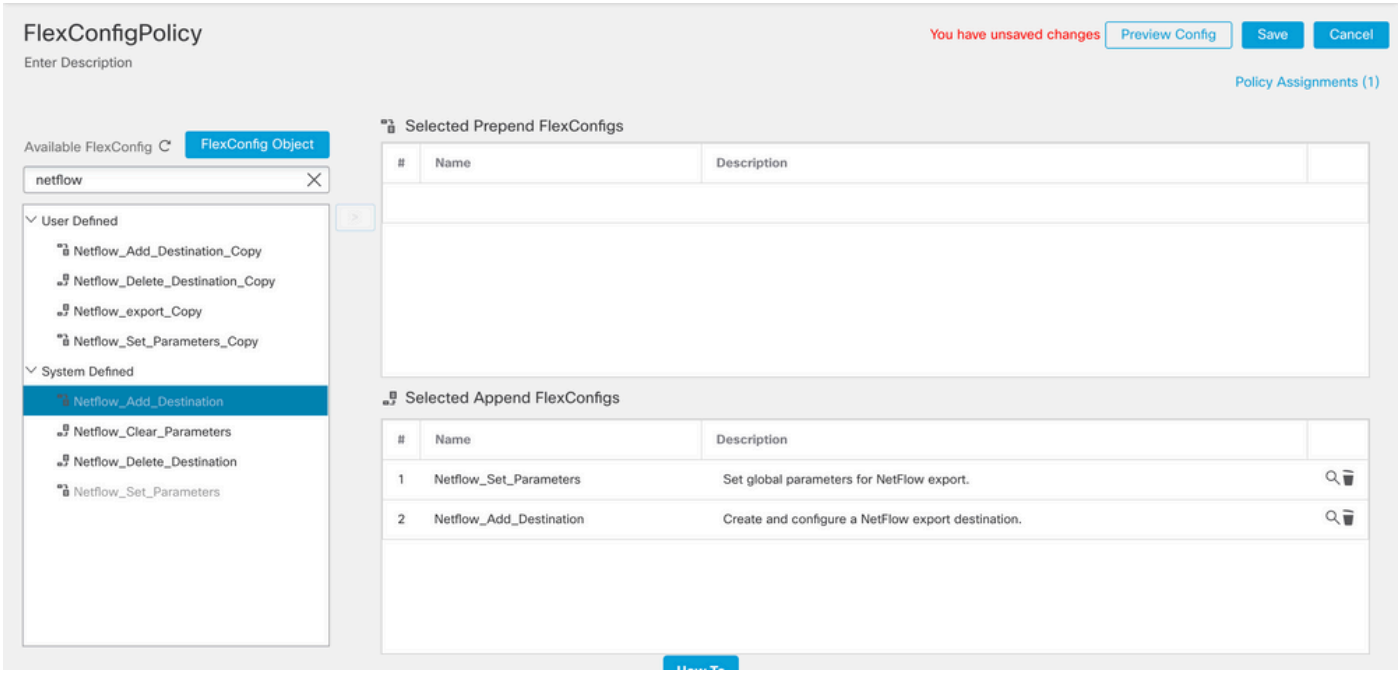
Stap 5. Wijs het FlexConfig-beleid toe aan de FTD

Navigeer naar **Apparaten > FlexConfig** en maak een nieuw beleid (tenzij er al een beleid is gemaakt voor een ander doel en toegewezen aan hetzelfde FTD). In dit voorbeeld is FlexConfig al gemaakt. Bewerk het FlexConfig-beleid en **selecteer** de FlexConfig-objecten die in de vorige stappen zijn gemaakt.

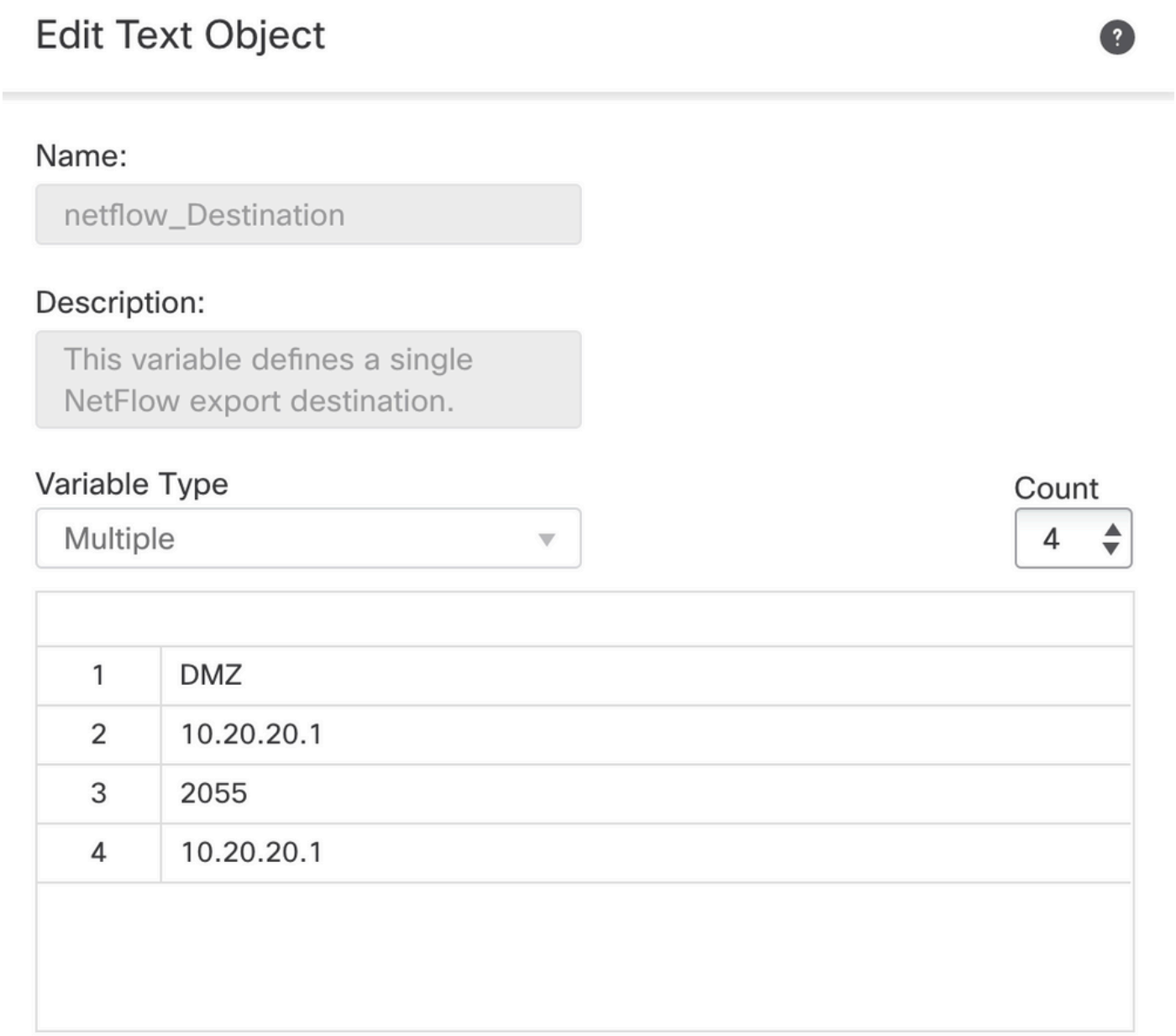
In dit voorbeeld worden de standaard NetFlow export parameters gebruikt, daarom wordt de NetFlow_Set_Parameters geselecteerd. **Sla de wijzigingen op en implementeer deze.**



Opmerking: om al het verkeer aan te passen zonder dat u specifiek verkeer hoeft aan te passen, kunt u de stappen 2 tot en met 4 overslaan en de vooraf gedefinieerde NetFlow-objecten gebruiken.



Opmerking: Om een tweede NSEL-collector toe te voegen waarnaar NetFlow-pakketten worden verzonden. In Stap 1, voeg 4 variabelen toe om het tweede NetFlow Collector IP adres toe te voegen.



In Stap 4., voeg de configuratie regel toe: flow-export bestemming $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)

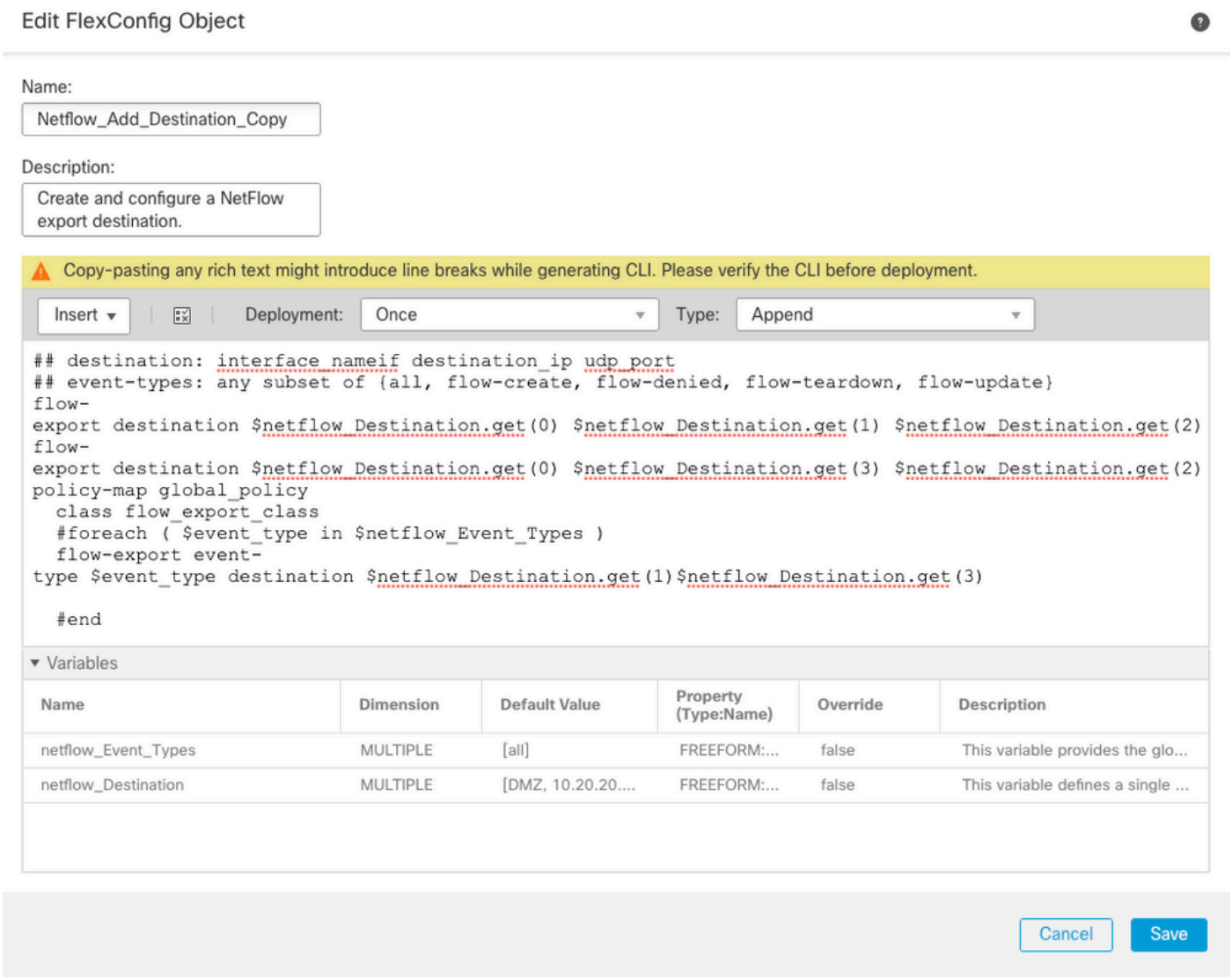
Bewerk de variabele $netflow_Destination.get voor de correspondentievariabele. In dit voorbeeld is de variabele waarde 3. Voorbeeld:

```
flow-
export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.
get(2)
flow-
export destination $netflow_Destination.get(0) $netflow_Destination.get(3) $netflow_Destination.
get(2)
```

Voeg ook de tweede variabele $netflow_Destination.get toe in de configuratielijn: flow-export event-type $event_type bestemming $netflow_Destination.get(1). Voorbeeld:

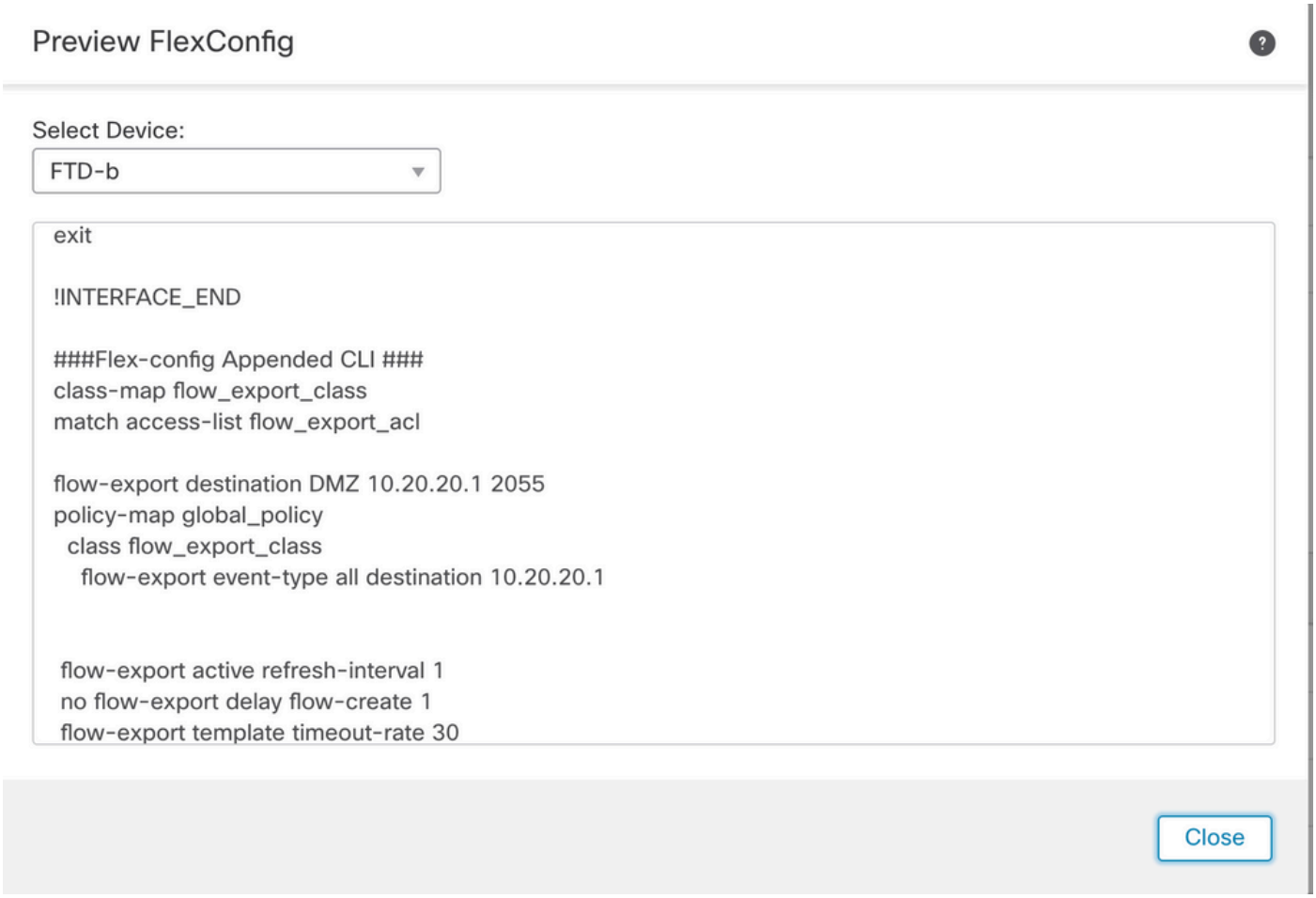
```
flow-export event-
type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

Valideer deze configuratie zoals weergegeven in de afbeelding hieronder:



Verifiëren

De NetFlow-configuratie kan worden geverifieerd binnen het FlexConfig-beleid. Klik om de configuratie te bekijken op **Preview Config**. **Selecteer** de FTD en controleer de configuratie.



Toegang tot de FTD via Secure Shell (SSH) en gebruik de diagnostische client voor opdrachtsysteem en voer deze opdrachten uit:

```
> 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 10.10.10.1 any (hitcnt=0) 0x8edff419
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 172.16.0.20 object 192.168.1.20 (hitcnt=0) 0x0ec22ecf
access-list flow_export_acl line 2 extended deny ip host 172.16.0.20 host 192.168.1.20
(hitcnt=0) 0x134aaeea
access-list flow_export_acl line 3 extended permit object-group ProxySG_ExtendedACL_30064776111
any any (hitcnt=0) 0x3726277e
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
10.10.10.1 any
access-list flow_export_acl extended deny object-group ProxySG_ExtendedACL_34359742101 object
172.16.0.20 object 192.168.1.20
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
```

Gerelateerde informatie

- [Cisco technische ondersteuning en downloads]

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.