Configurazione della registrazione sicura degli eventi di NetFlow su Firepower Threat Defense

Sommario

Introduzione

In questo documento viene descritto come configurare NetFlow Secure Event Logging (NSEL) su Firepower Threat Defense (FTD) tramite Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del CCP
- Conoscenza di FTD
- Conoscenza dei criteri FlexConfig

Componenti usati

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

- FTD versione 6.6.1
- FMC versione 6.6.1

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

In questo documento viene descritto come configurare NetFlow Secure Event Logging (NSEL) su Firepower Threat Defense (FTD) tramite Firepower Management Center (FMC).

Gli oggetti di testo FlexConfig sono associati alle variabili utilizzate negli oggetti FlexConfig predefiniti. Gli oggetti FlexConfig predefiniti e gli oggetti di testo associati sono disponibili in FMC per configurare NSEL. In FMC sono disponibili quattro oggetti FlexConfig predefiniti e tre oggetti di testo predefiniti. Gli oggetti FlexConfig predefiniti sono di sola lettura e non possono essere modificati. Per modificare i parametri di NetFlow, è possibile copiare gli oggetti.

Nella tabella sono elencati i quattro oggetti predefiniti riportati di seguito.

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

Nella tabella sono elencati i tre oggetti di testo predefiniti riportati di seguito.

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.

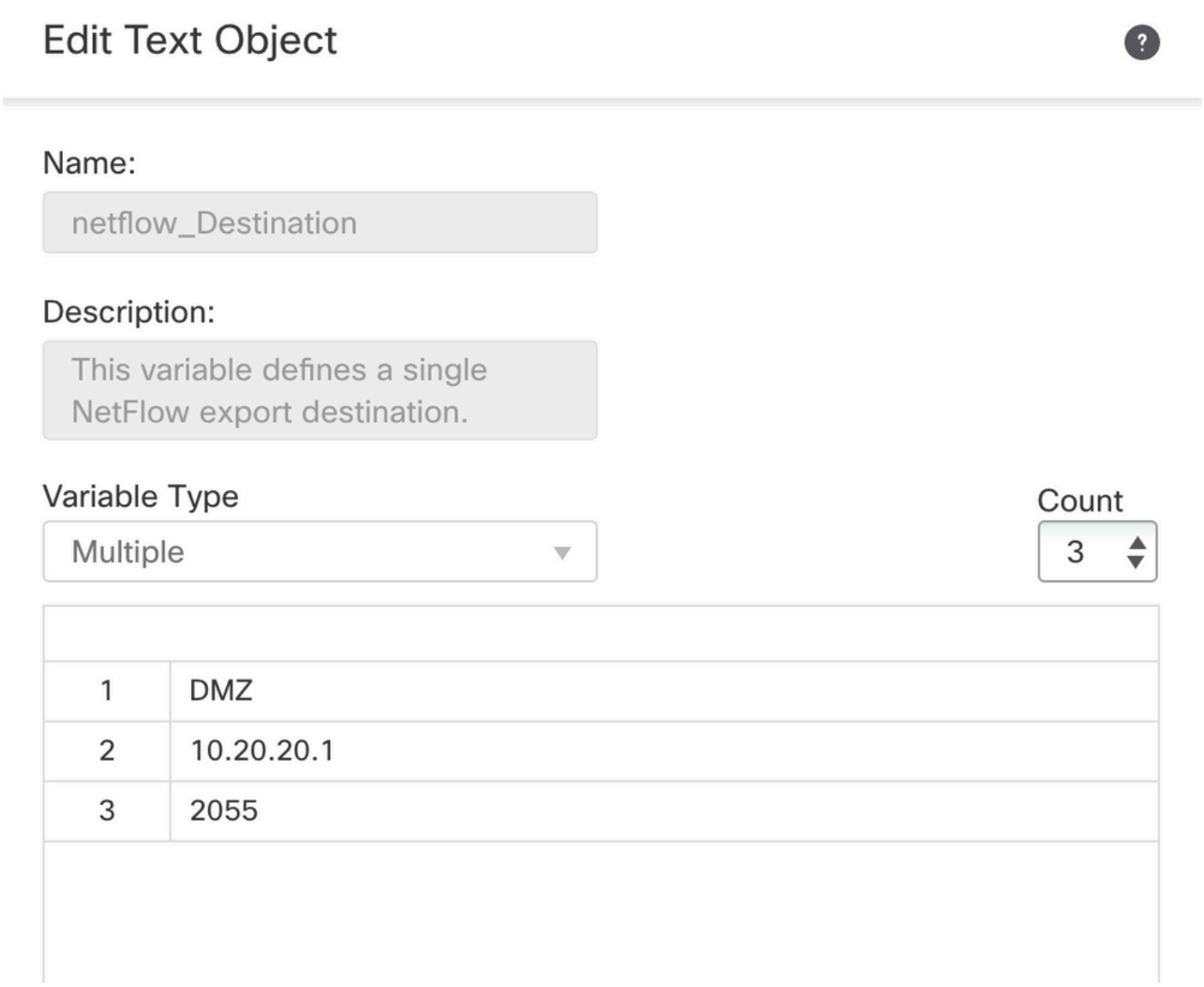
Configurazione

In questa sezione viene descritto come configurare NSEL su FMC tramite un criterio FlexConfig.

Passaggio 1. Impostare i parametri degli oggetti di testo per NetFlow.

Per impostare i parametri delle variabili, selezionare Oggetti > FlexConfig > Oggetti di testo. Modificare l'oggetto netflow_Destination. Definite il tipo di variabile multipla e il conteggio impostato su 3. Impostare il nome interfaccia, l'indirizzo IP di destinazione e la porta.

In questo esempio di configurazione, l'interfaccia è DMZ, l'indirizzo IP di NetFlow Collector è 10.20.20.1 e la porta UDP è 2055.



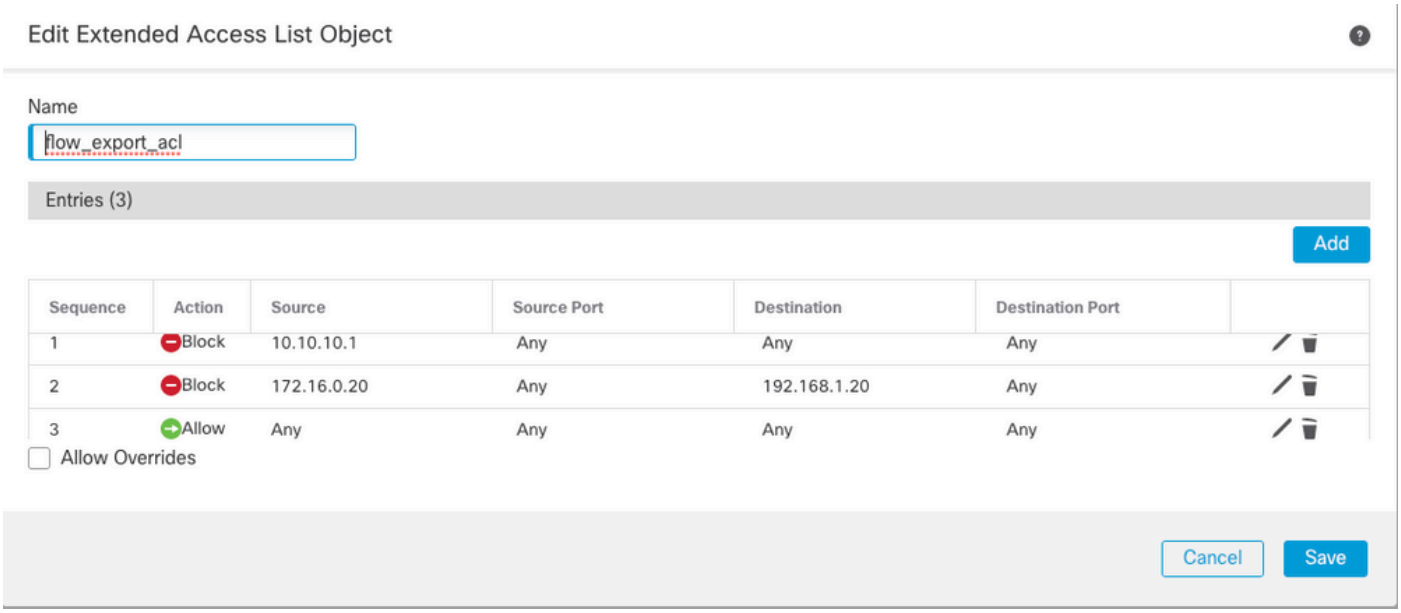
Nota: vengono utilizzati i valori predefiniti per netflow_Event_Types e netflow_Parameters.

Passaggio 2. Configurare un oggetto elenco accessi esteso in modo che corrisponda al traffico specifico.

Per creare un elenco degli accessi estesi in FMC, passare a Oggetti > Gestione oggetti e nel menu a sinistra, sotto Elenco accessi selezionare Esteso.Fare clic su Aggiungere l'elenco degli accessi estesi.

Compilare il campo Name (Nome). Nell'esempio, il nome è flow_export_acl. Fare clic sul pulsante Aggiungi. Configurare le voci di controllo di accesso in modo che corrispondano al traffico specifico.

Nell'esempio, viene escluso il traffico tra l'host 10.10.1 e qualsiasi destinazione e il traffico tra gli host 172.16.0.20 e 192.168.1.20. È incluso qualsiasi altro tipo di traffico.

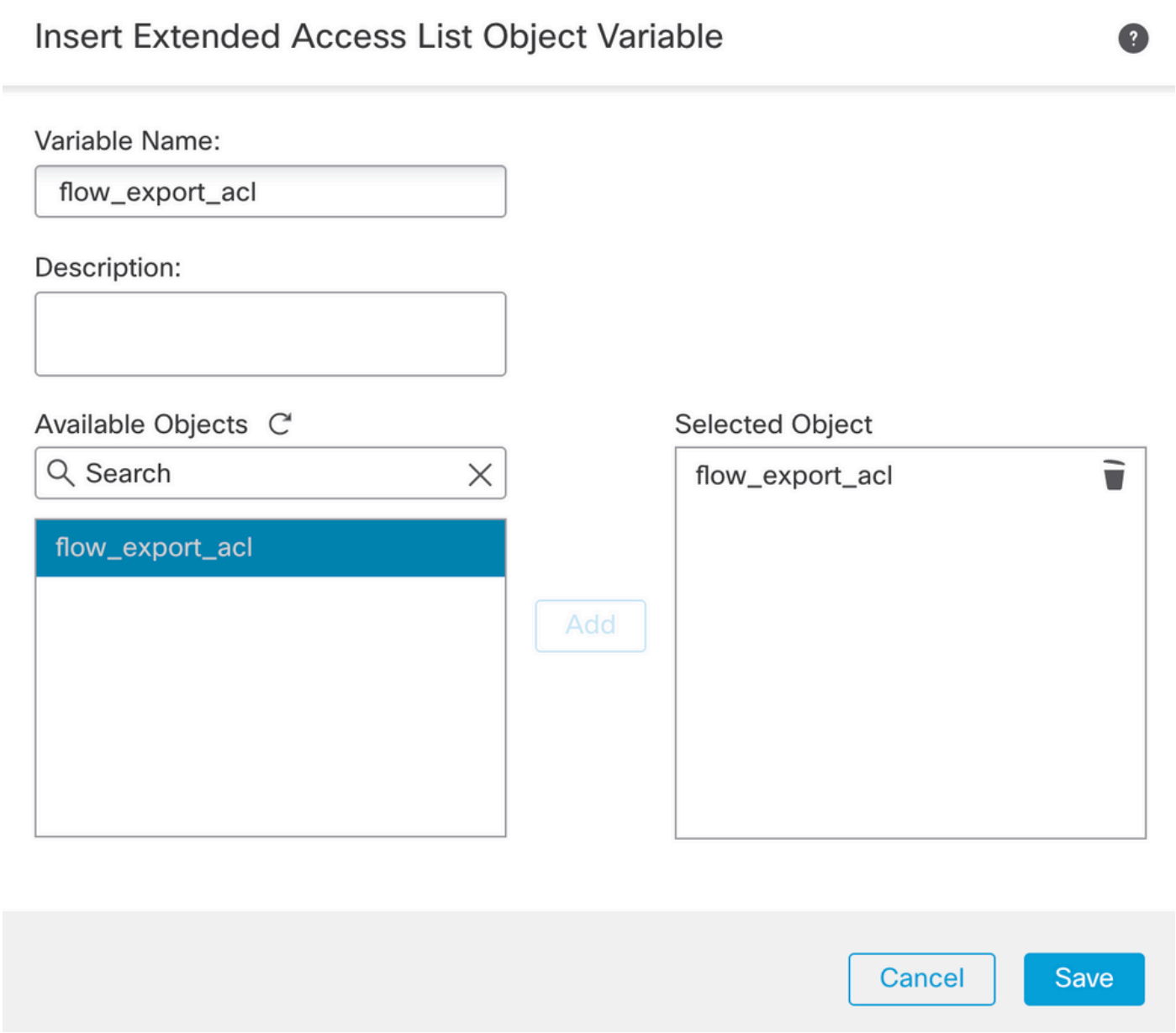


Passaggio 3. Configurare un oggetto FlexConfig.

Per configurare gli oggetti FlexConfig, passare a Oggetti > FlexConfig > FlexConfig Oggetti e fare clic sul pulsante Add FlexConfig Object.

Definire la mappa delle classi che identifica il traffico per cui è necessario esportare gli eventi NetFlow. In questo esempio, il nome dell'oggetto è flow_export_class.

Selezionare l'elenco degli accessi creato nel passaggio 2. Fare clic su Inserisci > Inserisci oggetto criterio > Oggetto ACL esteso e assegnare un nome. Quindi fai clic sul pulsante Aggiungi. In questo esempio, il nome della variabile è flow_export_acl. Fare clic su Salva.



Aggiungere le righe di configurazione successive nel campo vuoto a destra e includere la variabile precedentemente definita ($flow_export_acl.) nella riga di configurazione corrispondenza access-list.

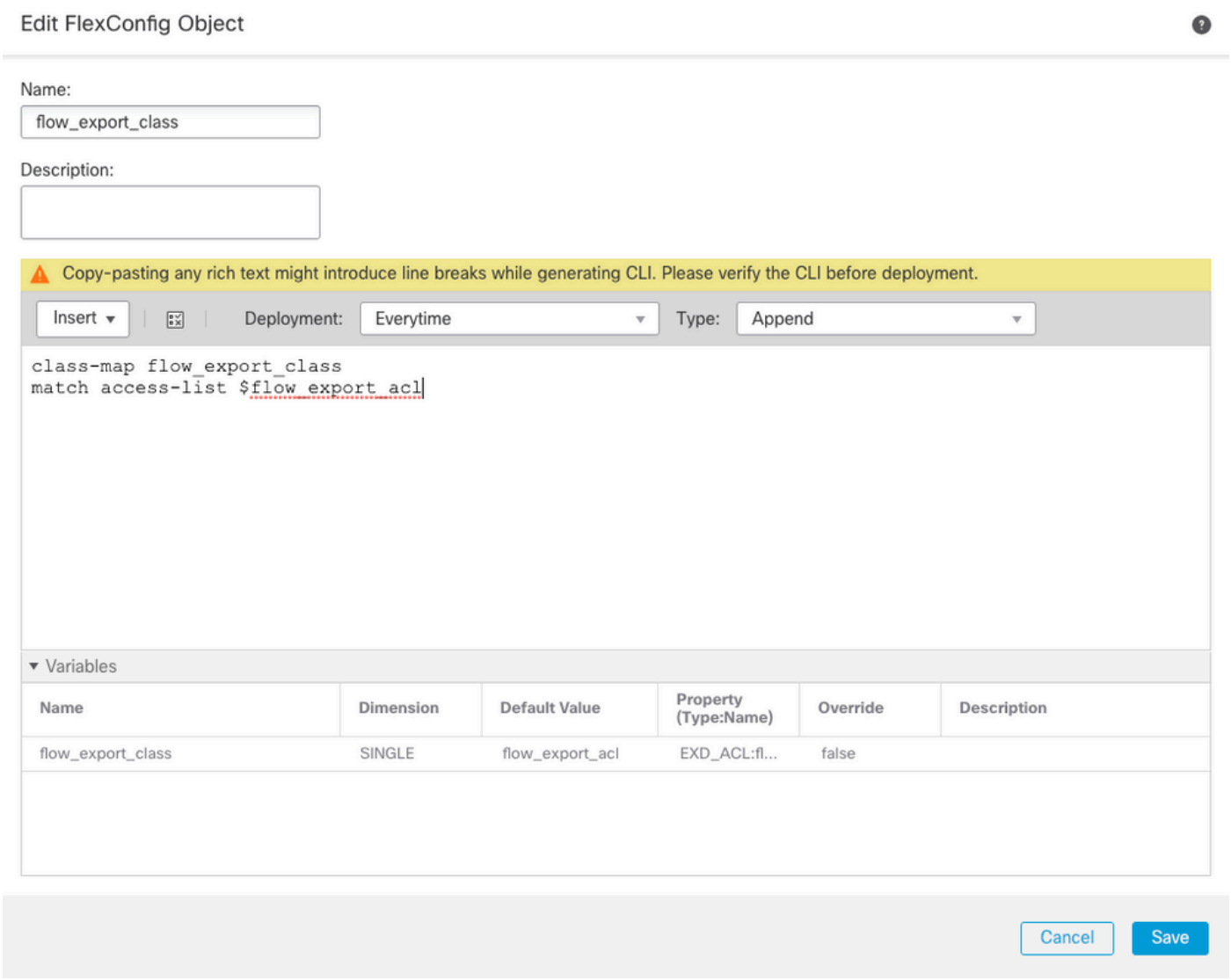
Si noti che un $ inizia il nome della variabile. In questo modo è possibile definire che una variabile viene dopo di essa.

<#root>

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

$flow_export_acl

Al termine, fare clic su Save (Salva).



Passaggio 4. Configurare la destinazione NetFlow

Per configurare la destinazione NetFlow, selezionare Oggetti > FlexConfig > FlexConfig Oggetti e filtrare in base a NetFlow. Copiare l'oggetto Netflow_Add_Destination. Viene creato Netflow_Add_Destination_Copy.

Assegnare la classe creata al passo 3. È possibile creare una nuova mappa dei criteri per applicare le azioni di esportazione del flusso alle classi definite.

In questo esempio, la classe viene inserita nel criterio corrente (criterio globale).

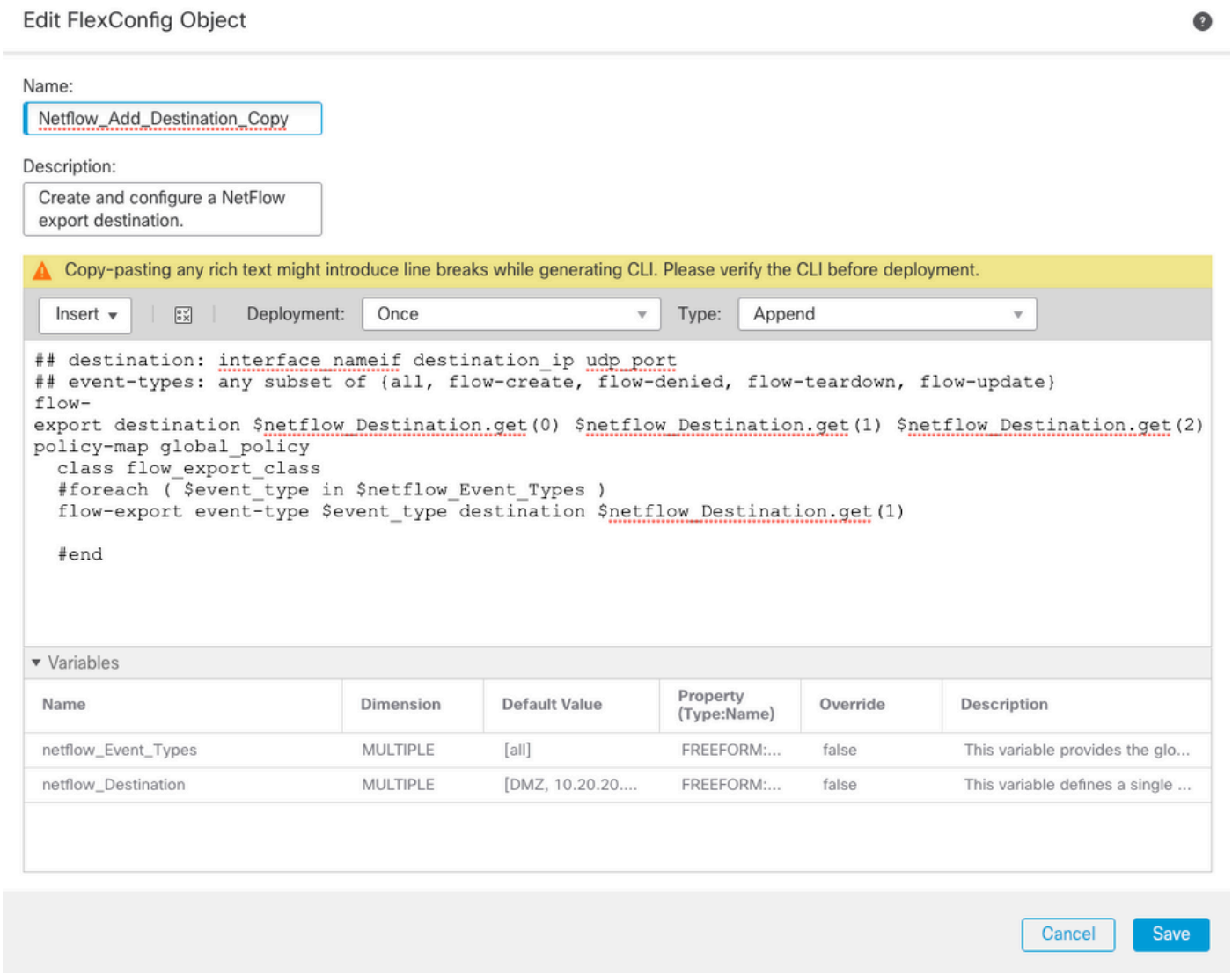
<#root>

```
## 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
```

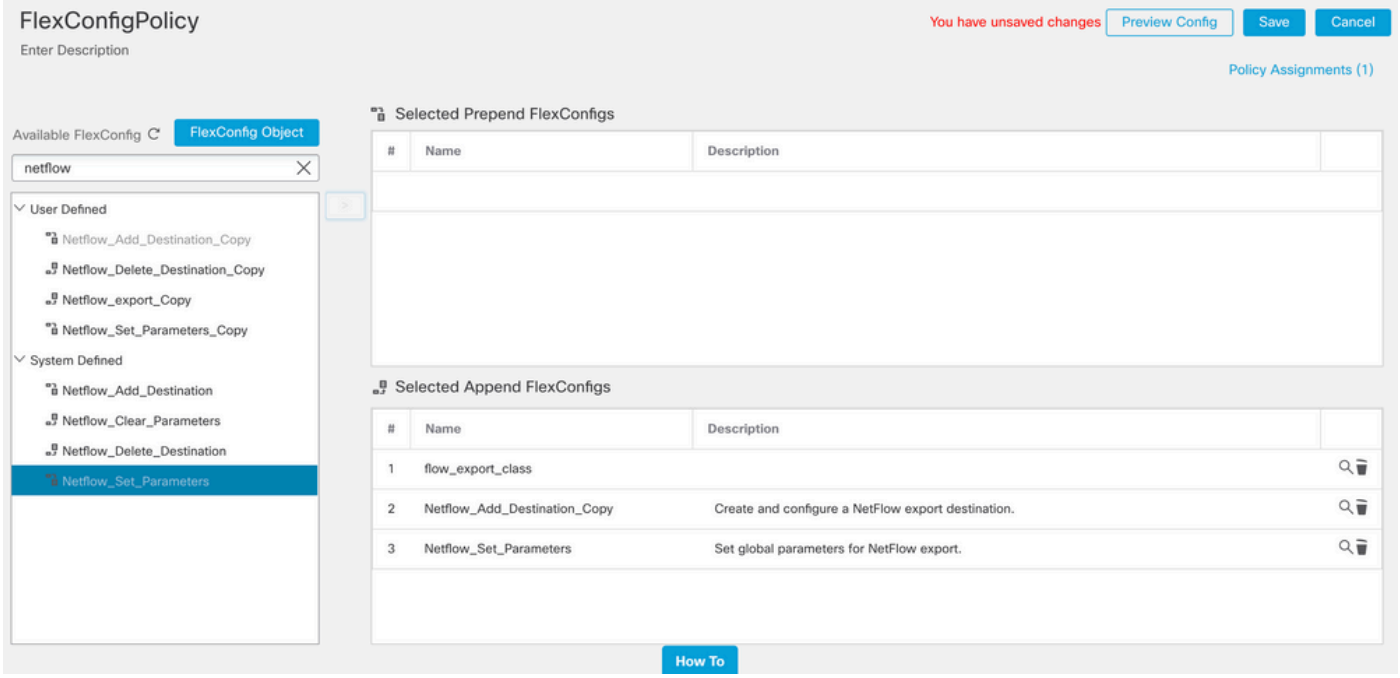
Al termine, fare clic su Save (Salva).



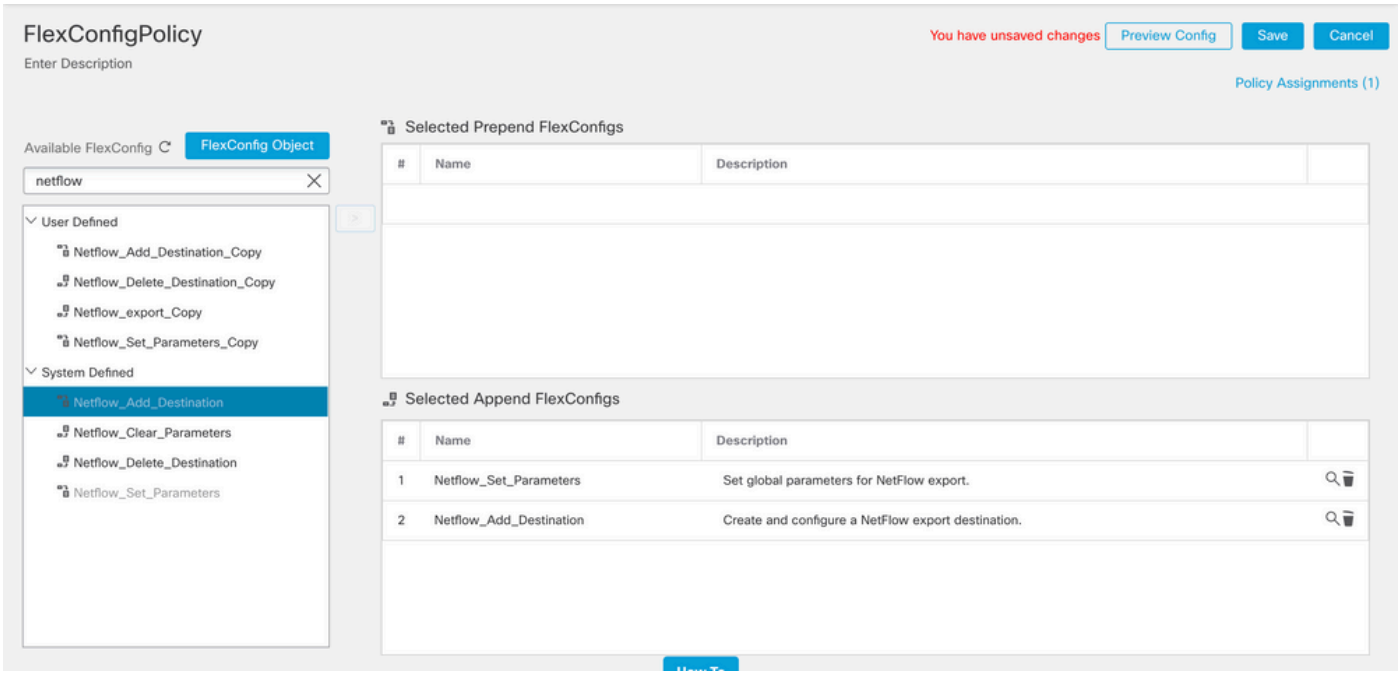
Passaggio 5. Assegnare il criterio FlexConfig all'FTD

Selezionare Dispositivi > FlexConfig e creare un nuovo criterio (a meno che non ne sia già stato creato uno per un altro scopo e assegnato allo stesso FTD). In questo esempio, FlexConfig è già stato creato. Modificare il criterio FlexConfig e selezionare gli oggetti FlexConfig creati nei passaggi precedenti.

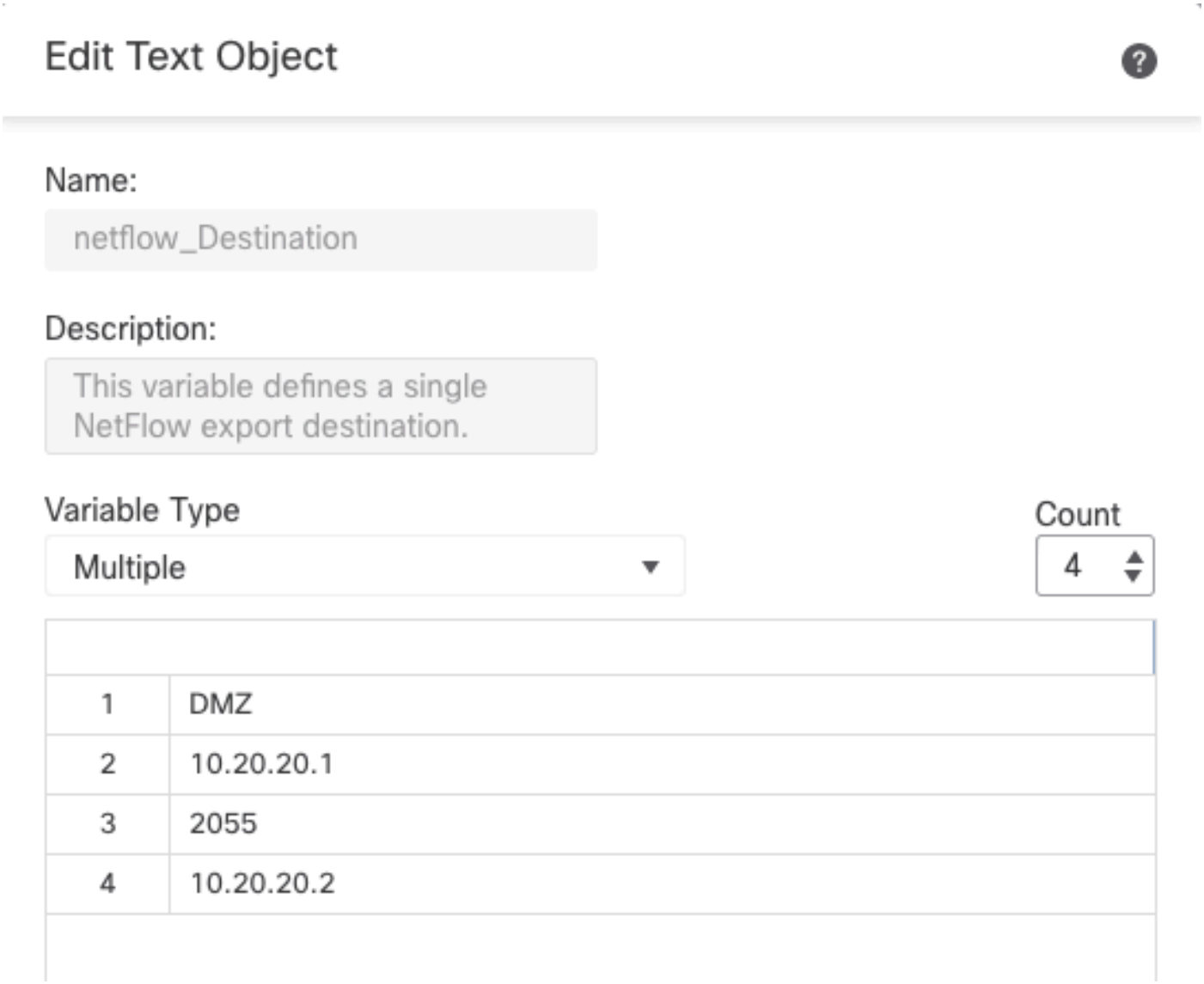
In questo esempio vengono utilizzati i parametri di esportazione Netflow di default, pertanto è selezionato Netflow_Set_Parameters. Salvare le modifiche e distribuire.



Nota: per individuare la corrispondenza tra tutto il traffico e non il traffico specifico, è possibile ignorare i passaggi da 2 a 4 e utilizzare gli oggetti NetFlow predefiniti.



Nota: per aggiungere un secondo raccoglitore NSEL a cui inviare i pacchetti NetFlow. Nel passo 1, aggiungere 4 variabili per aggiungere il secondo indirizzo IP del raccoglitore Netflow.



Multiple-Netflow-Text-Object

Nel passaggio 4. aggiungere la riga di configurazione: flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)

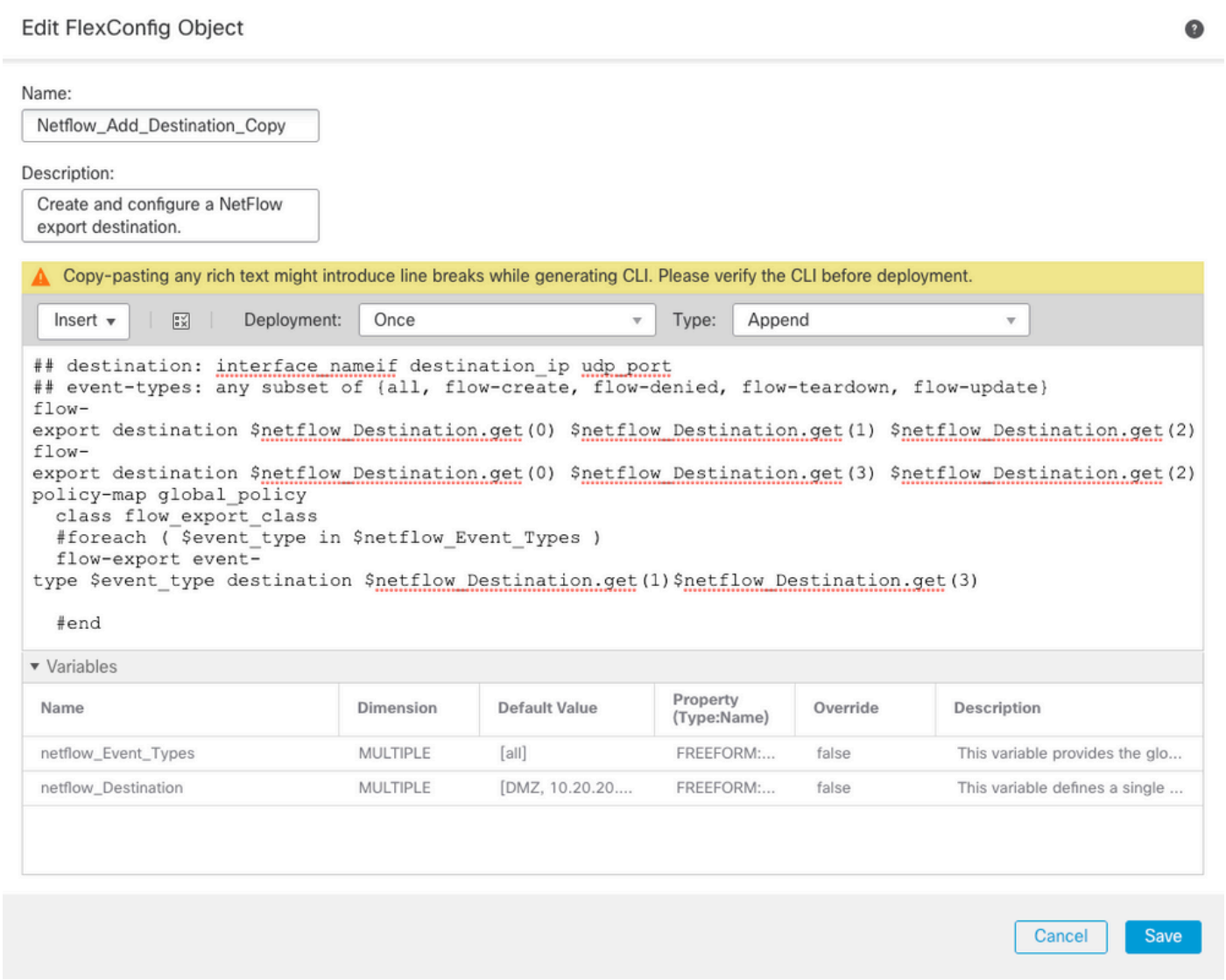
Modificare la variabile $netflow_Destination.get per la variabile di corrispondenza. In questo esempio il valore della variabile è 3. Ad esempio:

```
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
```

Inoltre, aggiungere la seconda variabile $netflow_Destination.get nella riga di configurazione: flow-export event-type destination $netflow_Destination.get(1). Ad esempio:

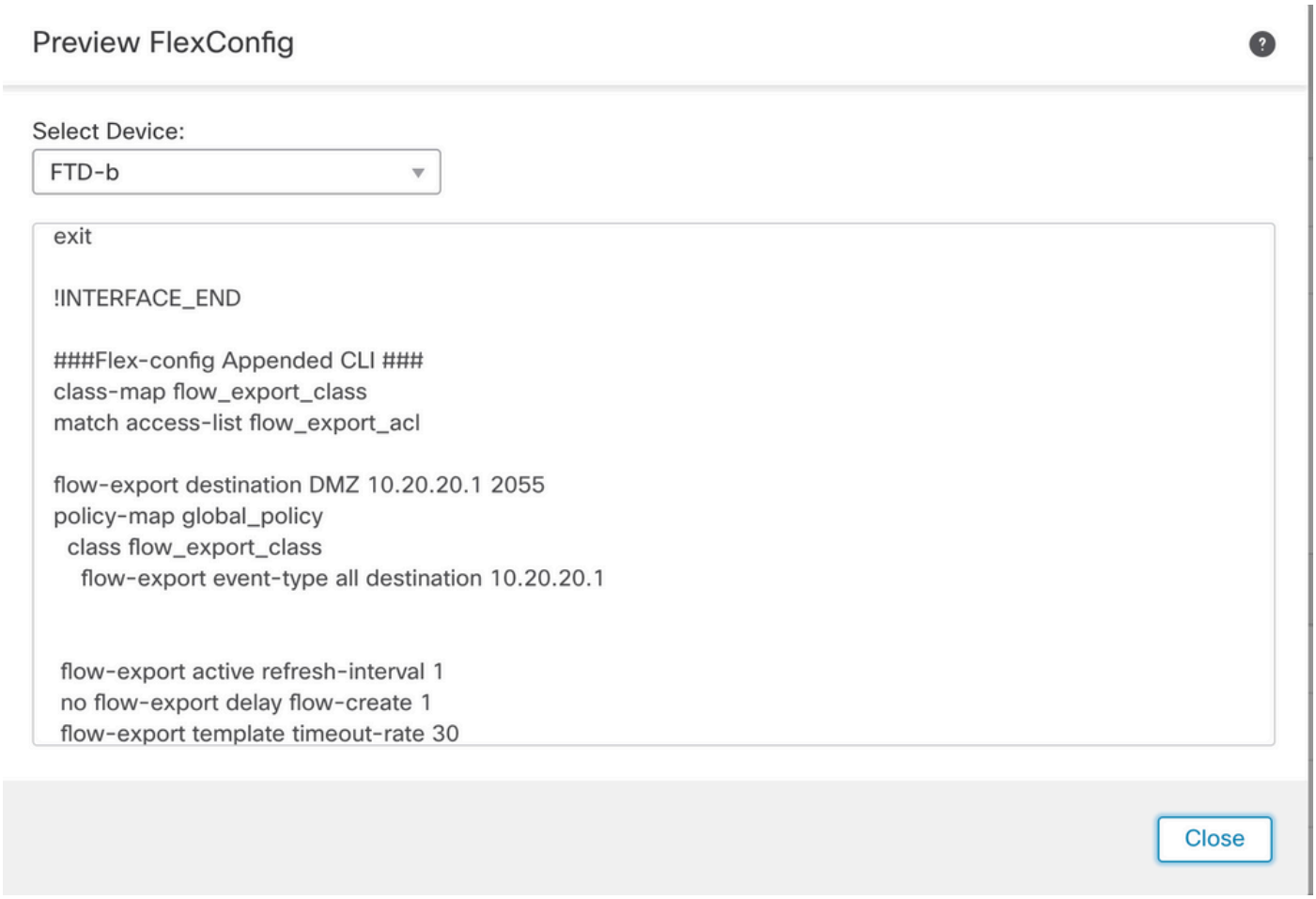
```
flow-export event-type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

Convalidare questa configurazione come mostrato nell'immagine seguente:



Verifica

La configurazione NetFlow può essere verificata nei criteri FlexConfig. Per visualizzare l'anteprima della configurazione, fare clic su Preview Config (Anteprima configurazione). Selezionare l'FTD e verificare la configurazione.



Accedere all'FTD tramite Secure Shell (SSH) e usare il comando system support diagnostic-cli ed eseguire questi comandi:

```
> 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
```

Informazioni correlate

- Supporto tecnico Cisco e download

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).