Configurar o registro de eventos seguro do NetFlow no Firepower Threat Defense

Contents

Introduction

Este documento descreve como configurar o NetFlow Secure Event Logging (NSEL) no Firepower Threat Defense (FTD) através do Firepower Management Center (FMC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do CVP
- Conhecimento de FTD
- Conhecimento da política FlexConfig

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD versão 6.6.1
- FMC versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar o NetFlow Secure Event Logging (NSEL) no Firepower Threat Defense (FTD) através do Firepower Management Center (FMC).

Os objetos de texto FlexConfig são associados a variáveis usadas nos objetos FlexConfig predefinidos. Objetos FlexConfig predefinidos e objetos de texto associados são encontrados no

FMC para configurar o NSEL. Há quatro objetos FlexConfig predefinidos no FMC e três objetos de texto predefinidos. Os objetos FlexConfig predefinidos são somente leitura e não podem ser modificados. Para modificar os parâmetros do NetFlow, os objetos podem ser copiados.

Os quatro objetos predefinidos estão listados na tabela:

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

Os três objetos de texto predefinidos estão listados na tabela:

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.

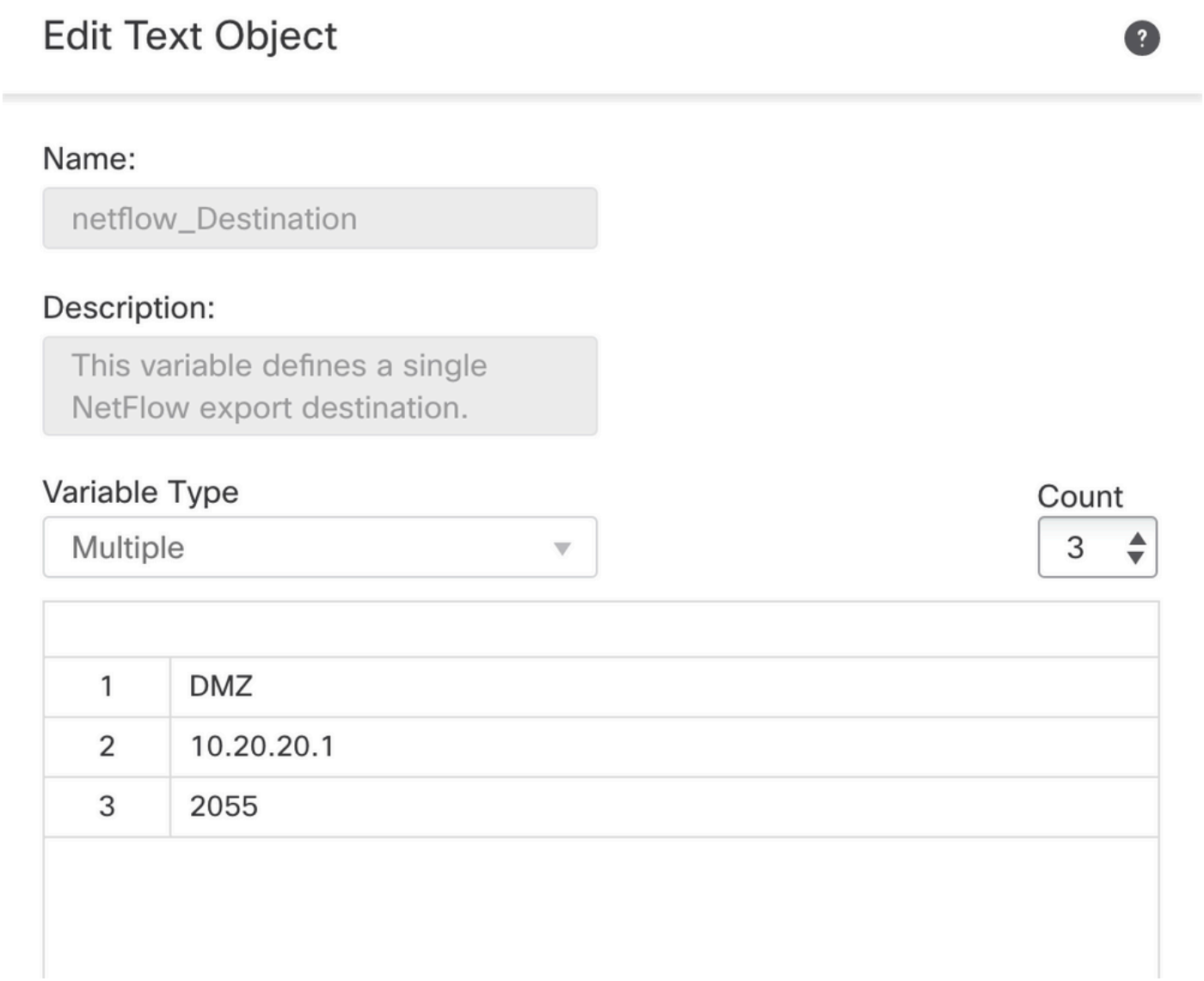
Configurar

Esta seção descreve como configurar o NSEL no FMC através de uma política FlexConfig.

Etapa 1. Defina os parâmetros dos Objetos de Texto para Netflow.

Para definir os parâmetros variáveis, navegue até **Objetos > FlexConfig > Objetos de texto**. Edite o objeto netflow_Destination. Defina o tipo de variável múltipla e a contagem definida como 3. Defina o nome da interface, o endereço IP destino e a porta.

Neste exemplo de configuração, a interface é DMZ, o endereço IP do coletor NetFlow é 10.20.20.1 e a porta UDP é 2055.



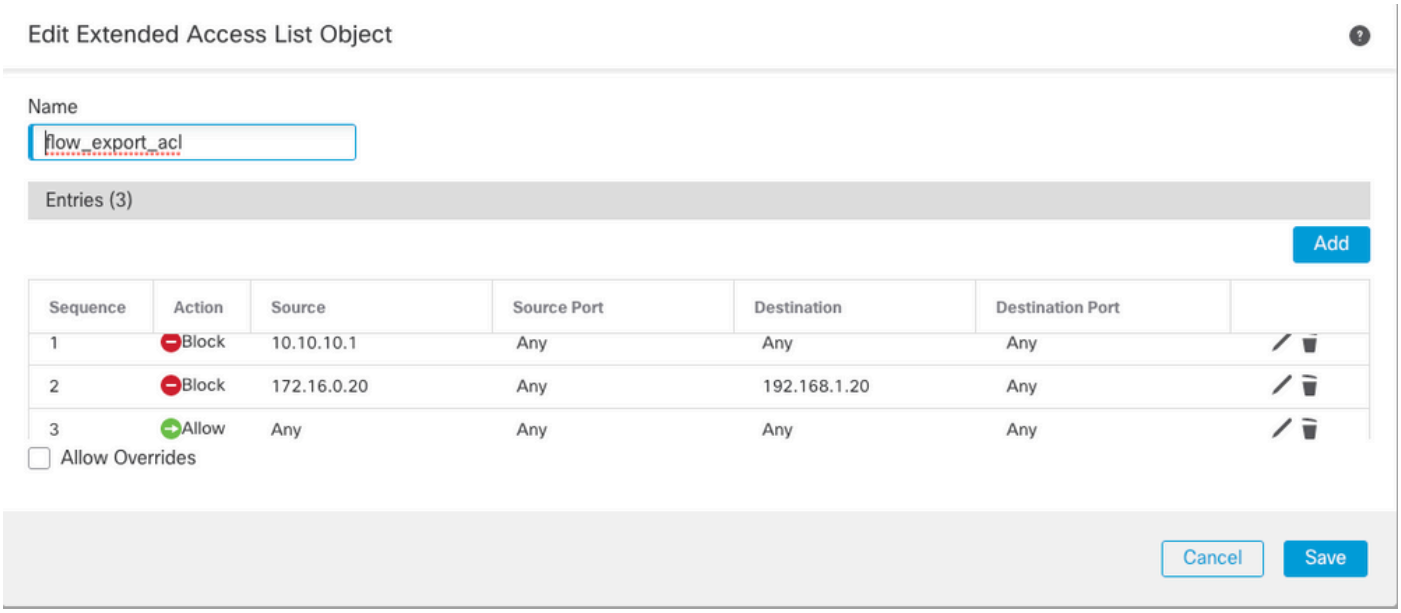
Observação: São usados valores default para netflow_Event_Types e netflow_Parameters.

Etapa 2. Configure um Objeto de Lista de Acesso Estendida para corresponder ao tráfego específico.

Para criar uma lista de acesso estendida no FMC, navegue até **Objetos > Gerenciamento de objetos** e no menu à esquerda, em **Lista de acesso** selecionar **Estendido.**Clique em **Adicionar Lista de Acesso Estendida.**

Preencha o campo **Nome**. Neste exemplo, o nome é flow_export_acl. Clique no botão Adicionar. Configure as entradas de **controle de acesso** para corresponder ao tráfego específico.

Neste exemplo, o tráfego do host 10.10.10.1 para qualquer destino e o tráfego entre os hosts 172.16.0.20 e 192.168.1.20 é excluído. Qualquer outro tráfego é incluído.

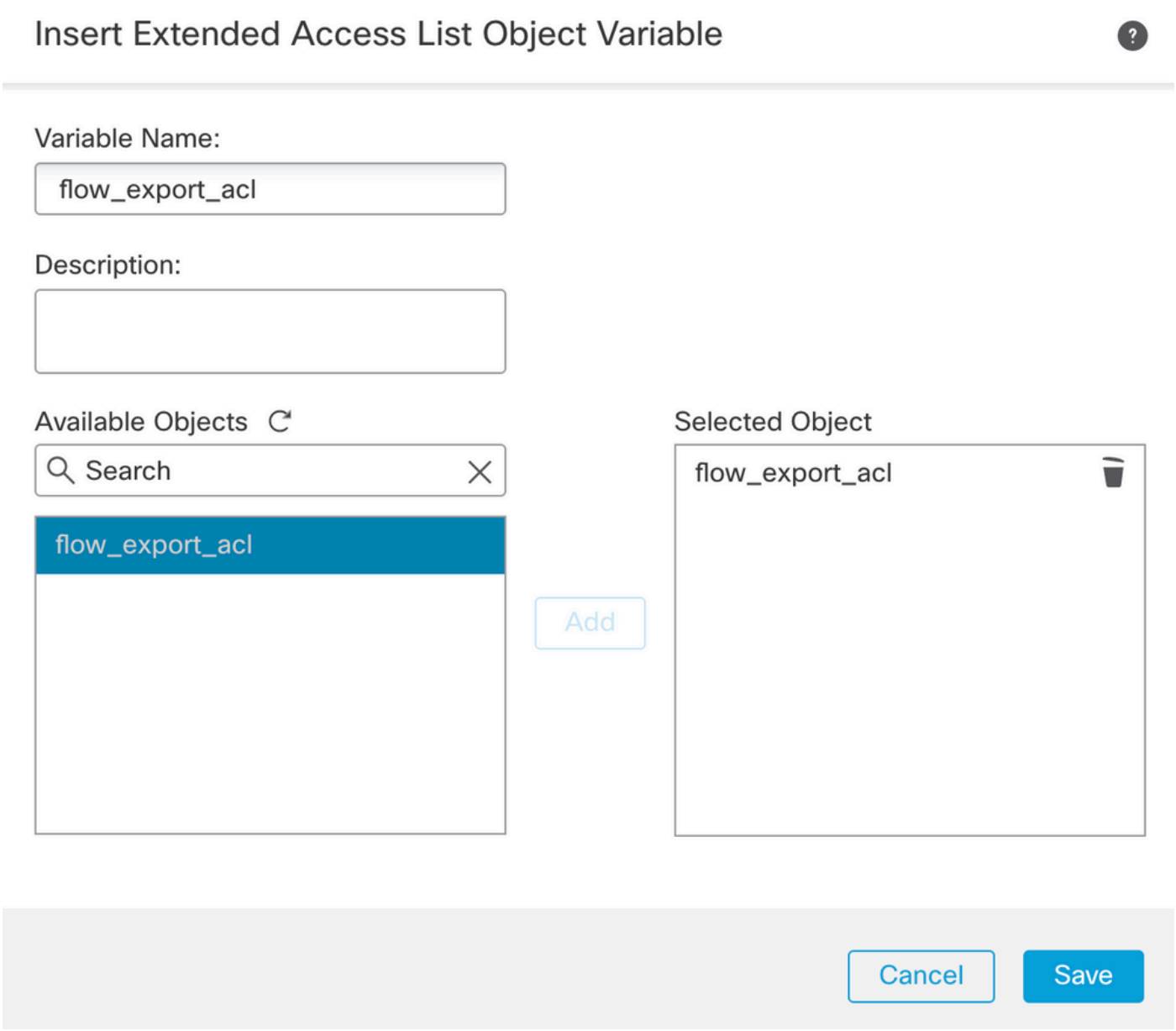


Etapa 3. Configure um objeto FlexConfig.

Para configurar os Objetos FlexConfig, navegue até **Objects > FlexConfig > FlexConfig** Objects e clique no botão **Add FlexConfig Object**.

Defina o mapa de classe que identifica o tráfego para o qual os eventos do NetFlow precisam ser exportados. Neste exemplo, o nome do objeto é flow_export_class.

Selecione a Lista de acesso criada na Etapa 2. Clique em **Insert > Insert Policy Object > Extended ACL Object** e atribua um nome. Em seguida, clique no botão **Add**. Neste exemplo, o nome da variável é flow_export_acl. Click **Save**.

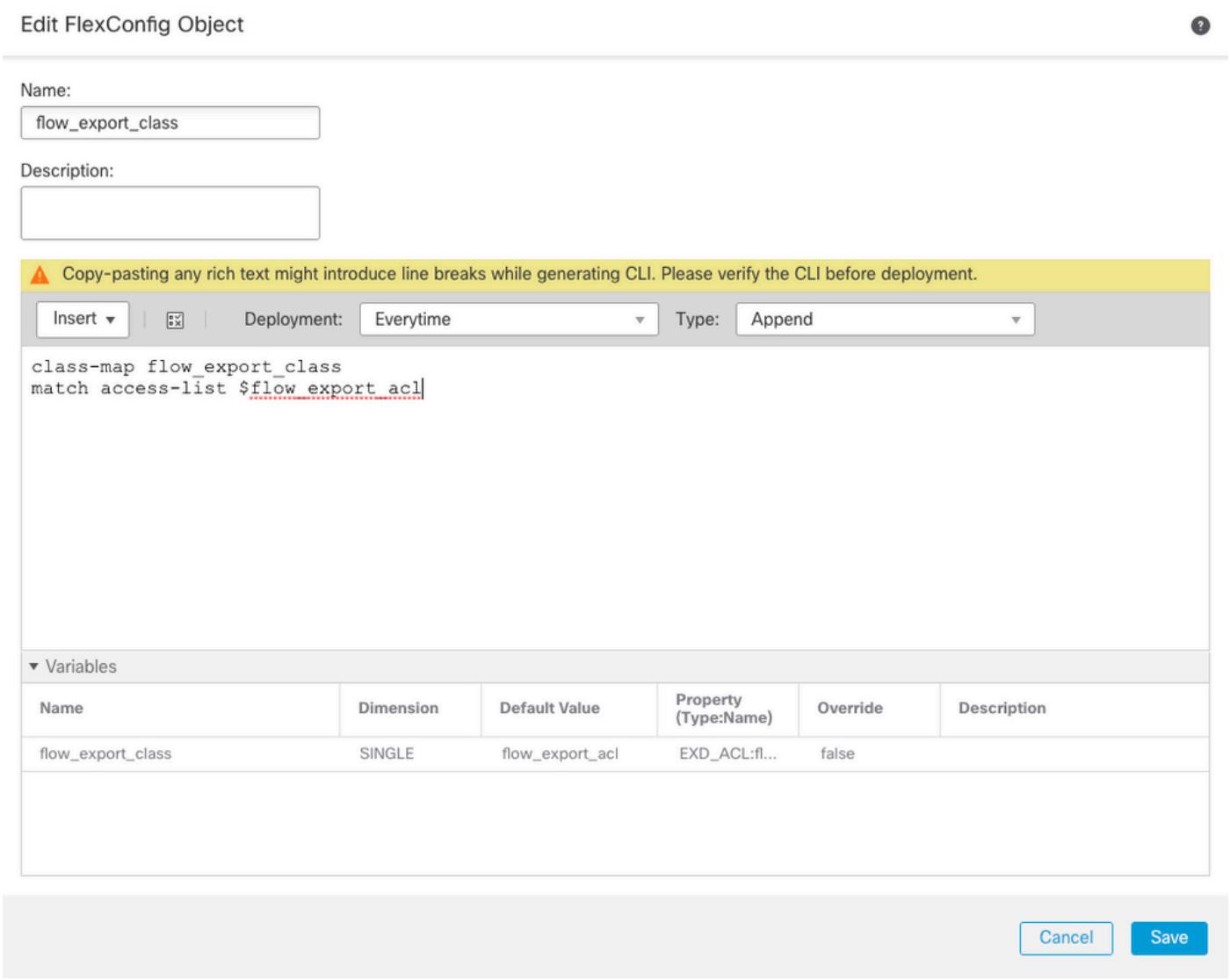


Adicione as próximas linhas de configuração no campo em branco à direita e inclua a variável definida anteriormente (**$flow_export_acl.**) na linha de configuração match access-list.

Observe que um **$** símbolo inicia o nome da variável. Isso ajuda a definir que uma variável vem depois dela.

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

Clique em **Save** quando terminar.



Etapa 4. Configurar o destino do Netflow

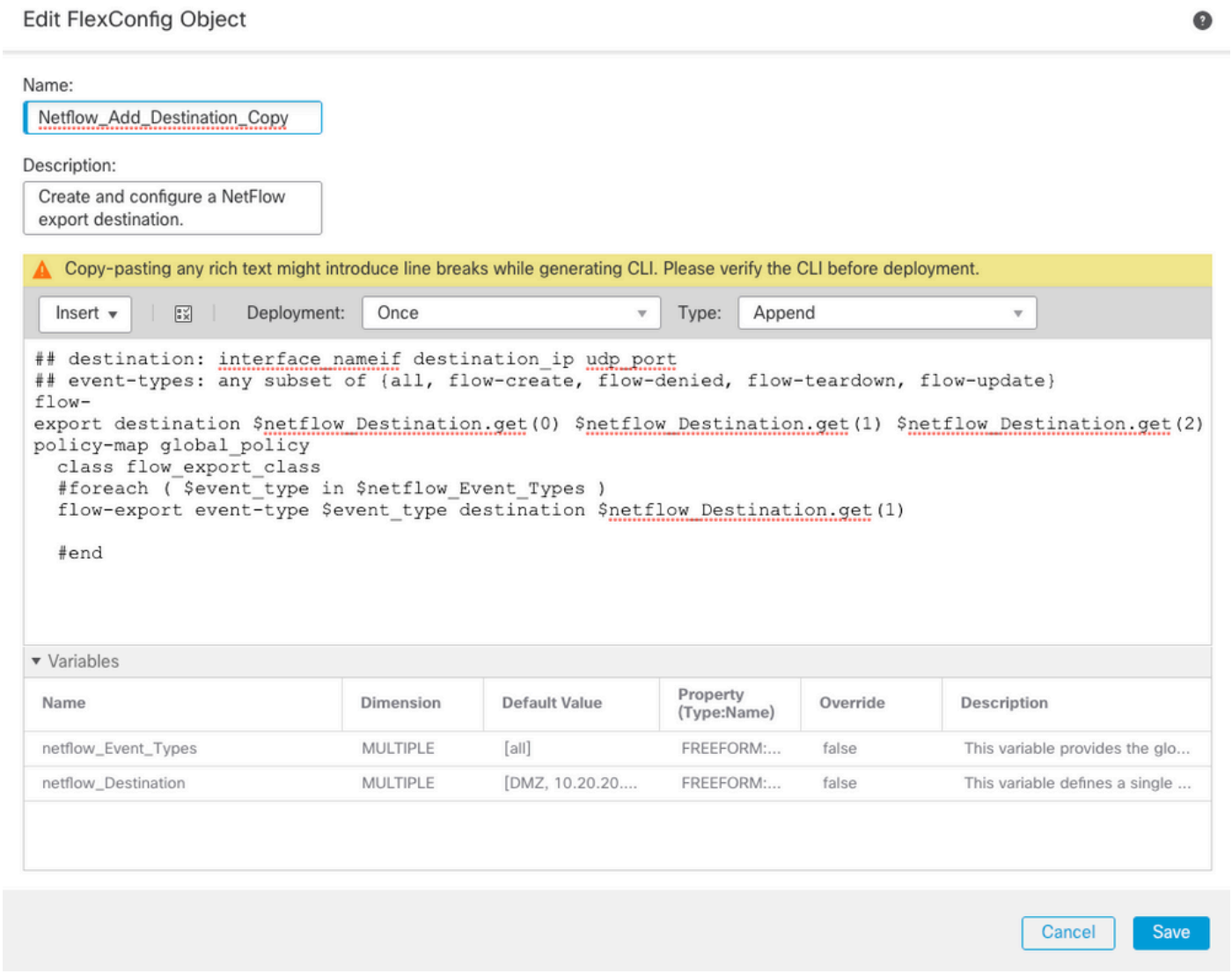
Para configurar o destino do Netflow, navegue até **Objects** > **FlexConfig** > **FlexConfig** Objects e filtre por Netflow. **Copie** o objeto Netflow_Add_Destination. O Netflow_Add_Destination_Copy é criado.

Atribua a classe criada na Etapa 3. Você pode criar um novo mapa de política para aplicar as ações de exportação de fluxo às classes definidas.

Neste exemplo, a classe é inserida na política atual (política global).

```
## 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
```

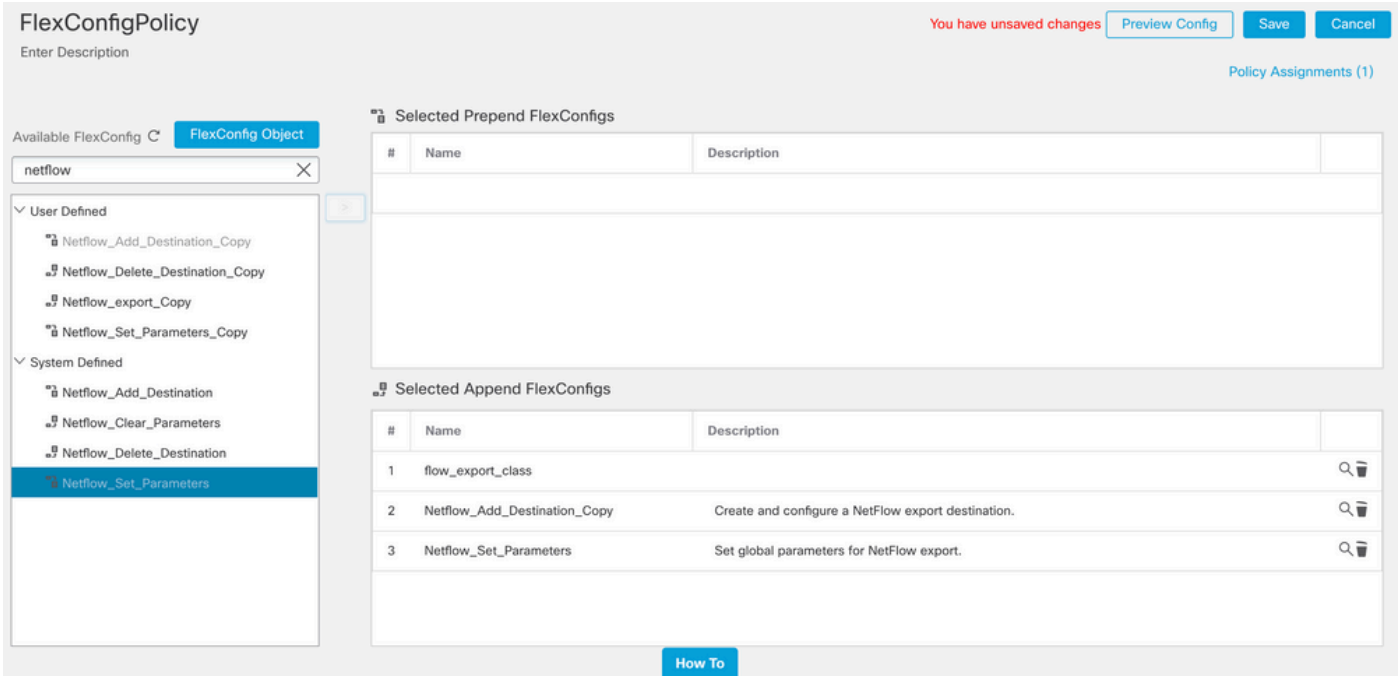
Clique em **Save** quando terminar.



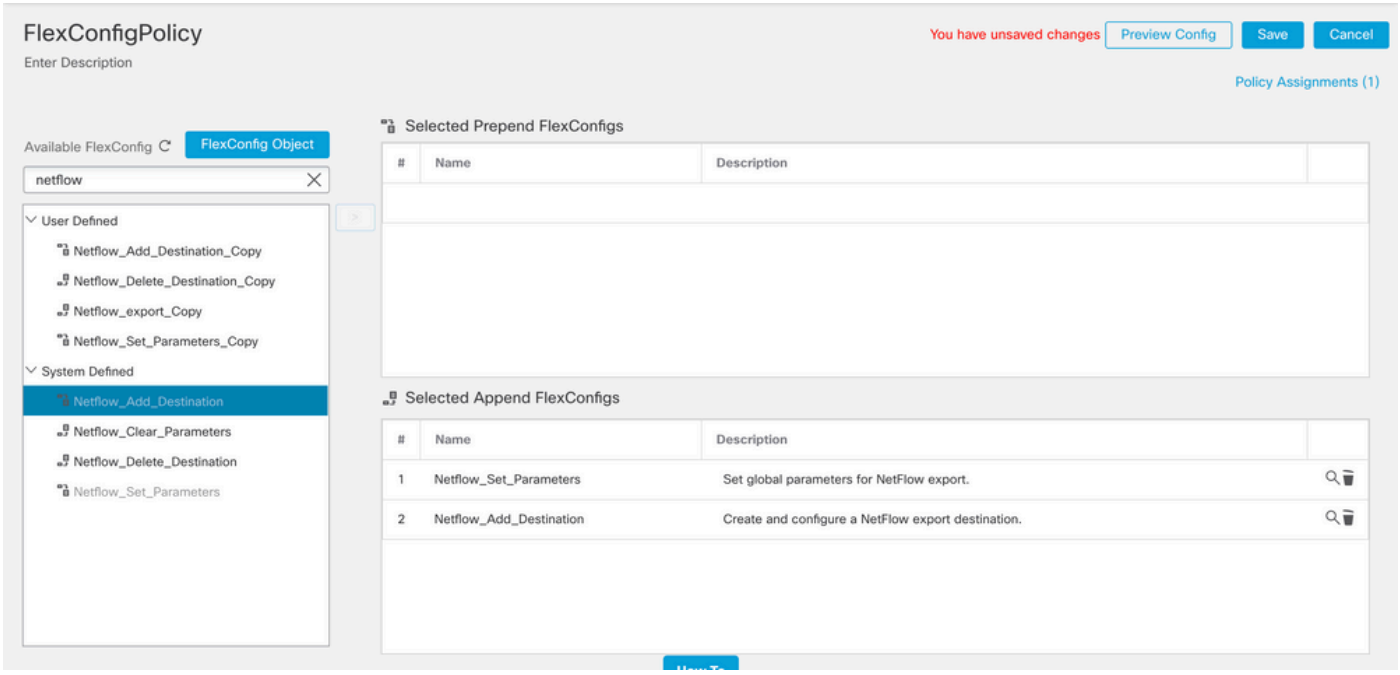
Etapa 5. Atribuir a política FlexConfig ao FTD

Navegue até **Devices > FlexConfig** e crie uma nova política (a menos que já haja uma criada para outra finalidade e atribuída ao mesmo FTD). Neste exemplo, o FlexConfig já foi criado. Edite a Política FlexConfig e **Selecione** os objetos FlexConfig criados nas etapas anteriores.

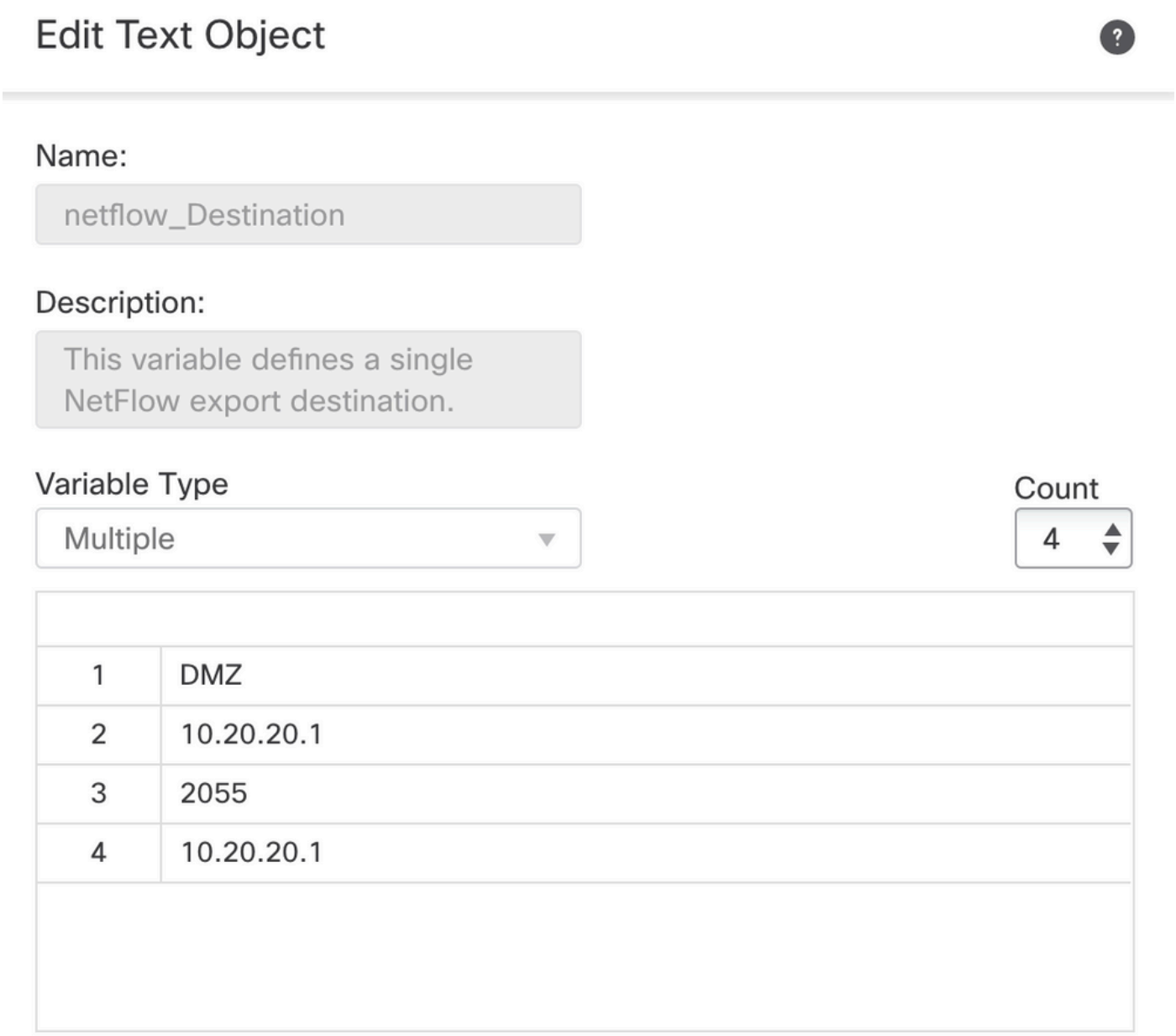
Neste exemplo, os parâmetros de exportação padrão do Netflow são usados, portanto, o Netflow_Set_Parameters é selecionado. **Salve a alteração e implante-a.**



Observação: para fazer a correspondência de todo o tráfego sem a necessidade de correspondência com tráfego específico, você pode pular das Etapas 2 a 4 e usar os Objetos NetFlow predefinidos.



Observação: para adicionar um segundo coletor NSEL ao qual os pacotes NetFlow são enviados. Na Etapa 1, adicione 4 variáveis para adicionar o segundo endereço IP do coletor Netflow.



Na Etapa 4, adicione a linha de configuração: flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)

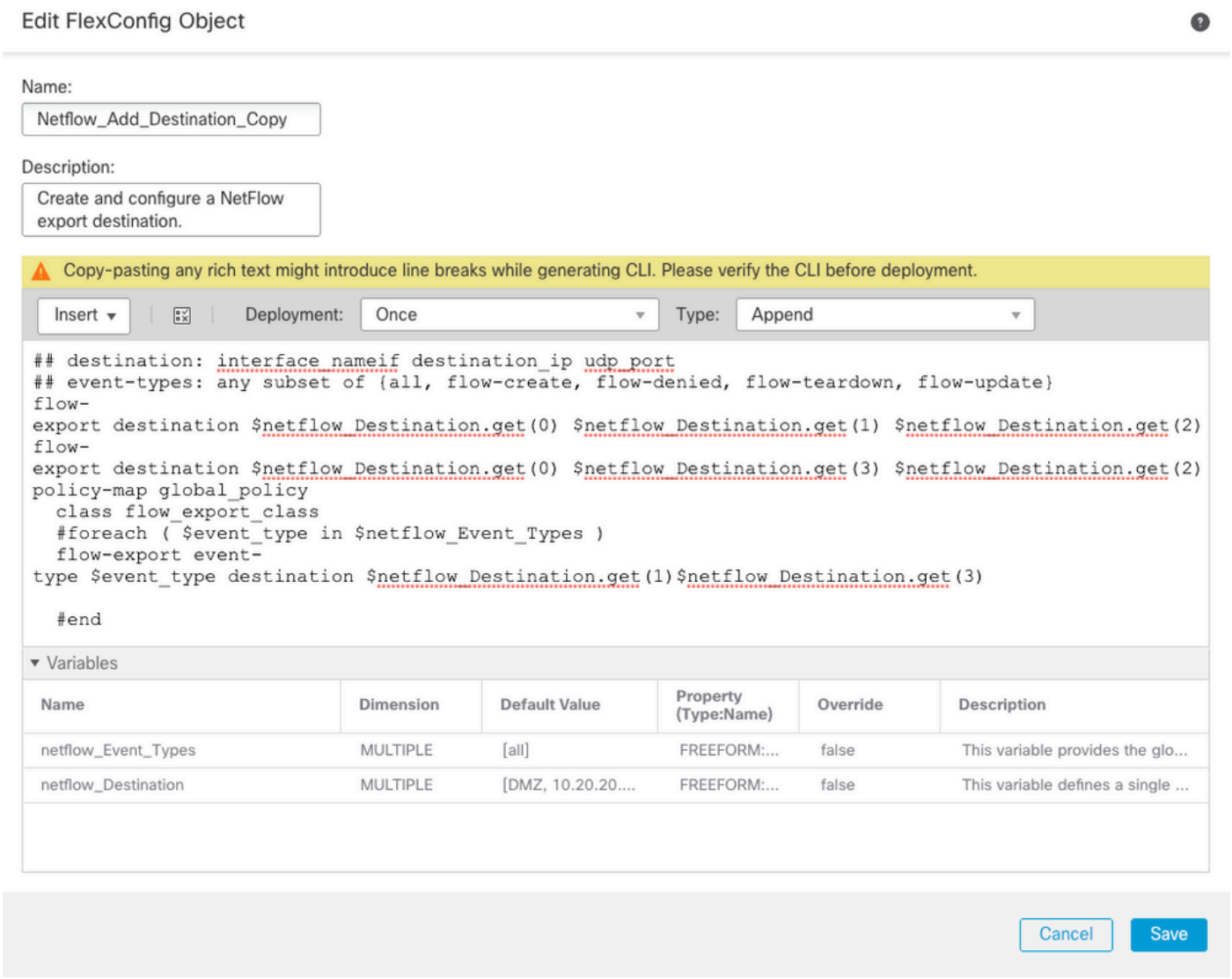
Edite a variável $netflow_Destination.get para a variável de correspondência. Neste exemplo, o valor da variável é 3. Por exemplo:

```
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)
```

Adicione também a segunda variável $netflow_Destination.get na linha de configuração: flow-export event-type $event_type destination $netflow_Destination.get(1). Por exemplo:

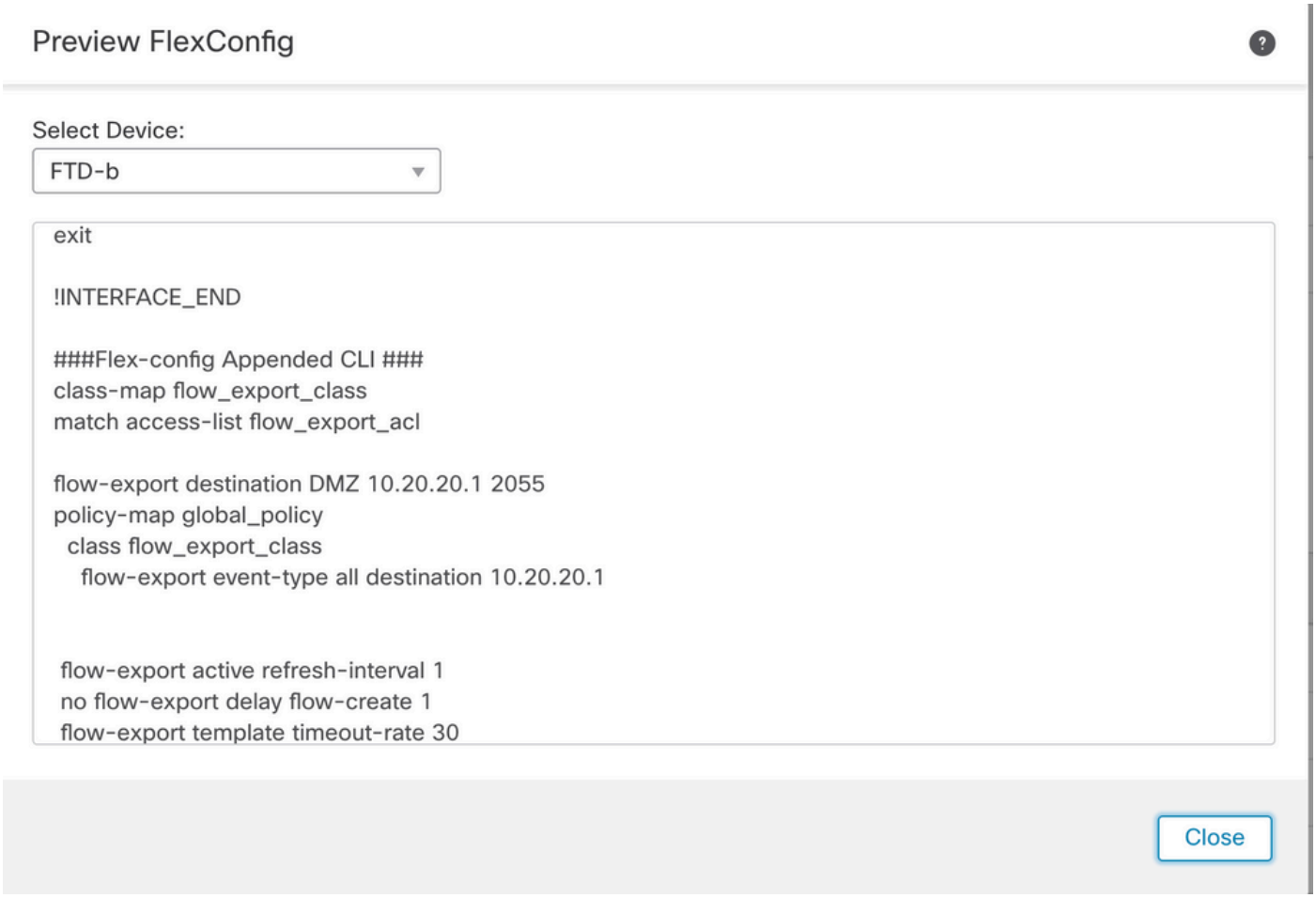
```
flow-export event-
type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

Valide essa configuração conforme visto na imagem abaixo:



Verificar

A configuração do NetFlow pode ser verificada na Política FlexConfig. Para visualizar a configuração, clique em **Preview Config**. **Selecione** o FTD e verifique a configuração.



Acesse o FTD por meio do Secure Shell (SSH), use o comando system support diagnostic-cli e execute estes comandos:

```
> 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
```

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.