

Remover ou modificar a configuração do NetFlow usando o Flexconfig

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração inicial](#)

[Remover configurações do NetFlow](#)

[Modificar as configurações do NetFlow existentes](#)

[Documentos relacionados](#)

Introdução

Este documento descreve como remover ou modificar a configuração do NetFlow no Firepower Threat Defense (FTD) através do Firepower Centro de Gestão do Tráfego Aéreo (CVP).

Pré-requisitos

Requisitos

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:

- Versão do FTD anterior à 7.4
- Versão do CVP inferior a 7.4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.



Observação: observação importante para o Firepower versões 7.2.x: ao configurar o NetFlow, há um bug da Cisco ID [CSCwh29167](#) em que o objeto Flex é reorganizado, fazendo com que a implantação falhe devido à não configuração do mapa de classes. Para resolver esse problema, implemente a solução documentada sob o bug da Cisco ID [CSCwf9848](#) (duplicata do bug da Cisco ID [CSCwh29167](#)).

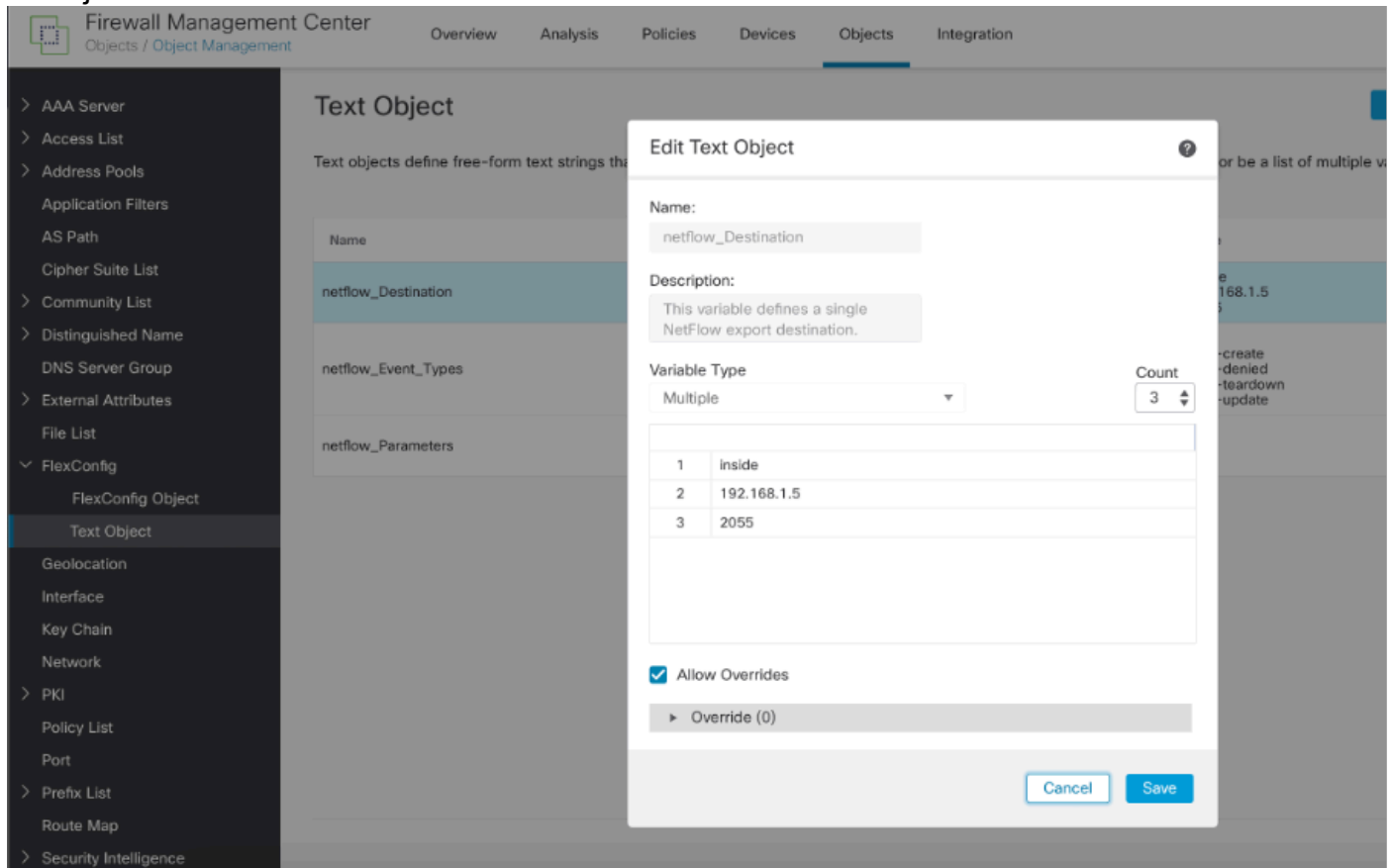
Configuração inicial

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.5
  flow-export event-type flow-denied destination 192.168.1.5
```

```
flow-export event-type flow-teardown destination 192.168.1.5
flow-export event-type flow-update destination 192.168.1.5
!
flow-export destination Inside 192.168.1.5 2055
```

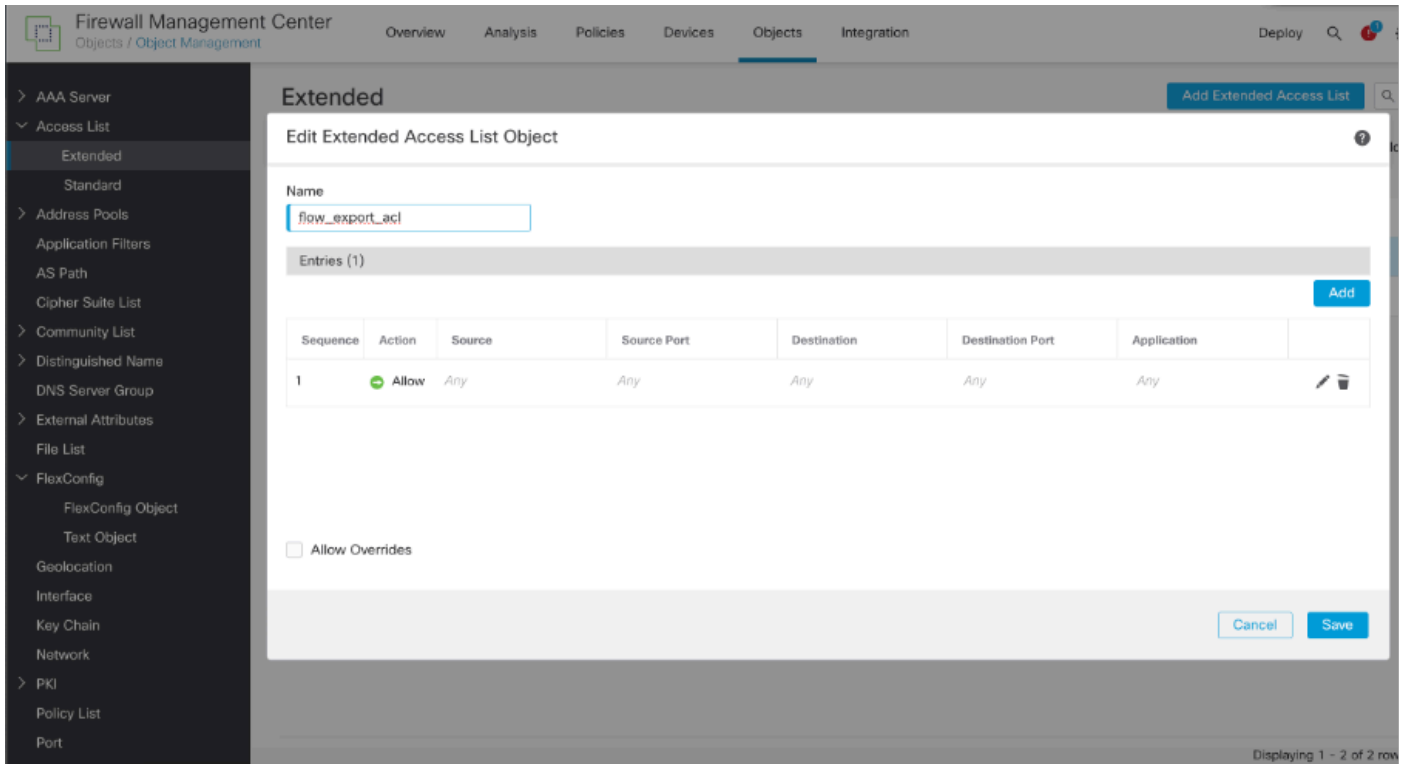
Para configurar essas configurações iniciais, os objetos flex config usados são:

1. Objeto de texto de destino do Netflow



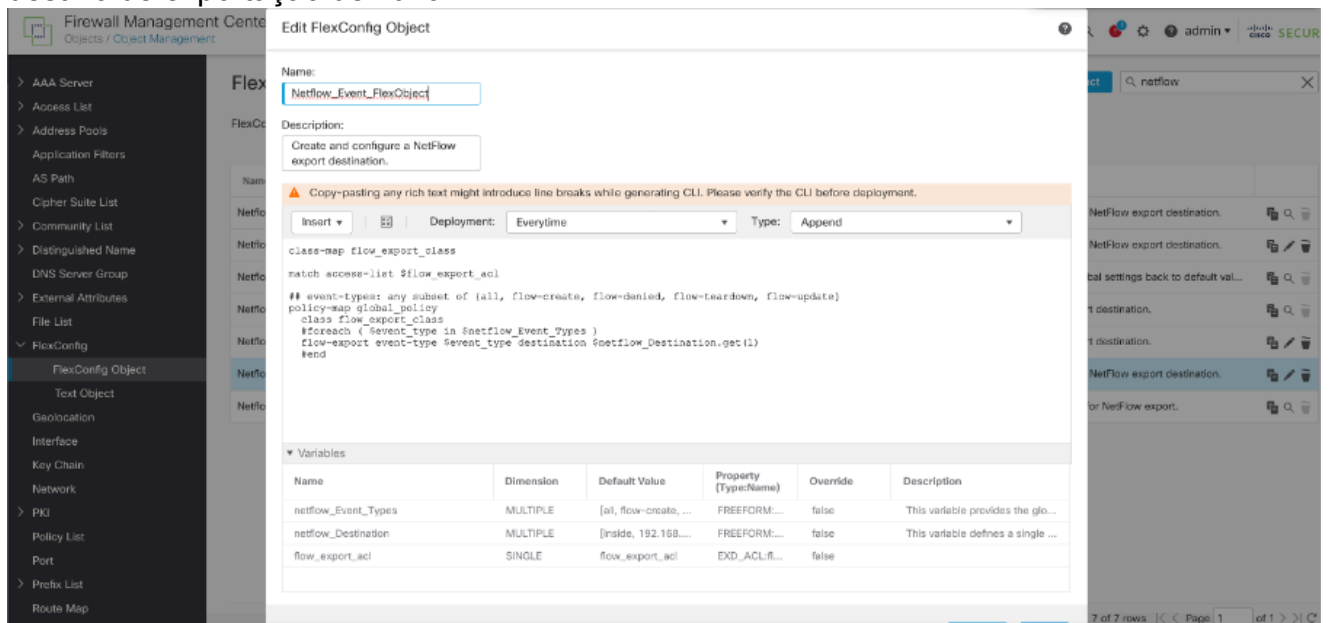
Objeto de Texto de Destino do Netflow

2. ACL estendida chamada: flow_export_acl



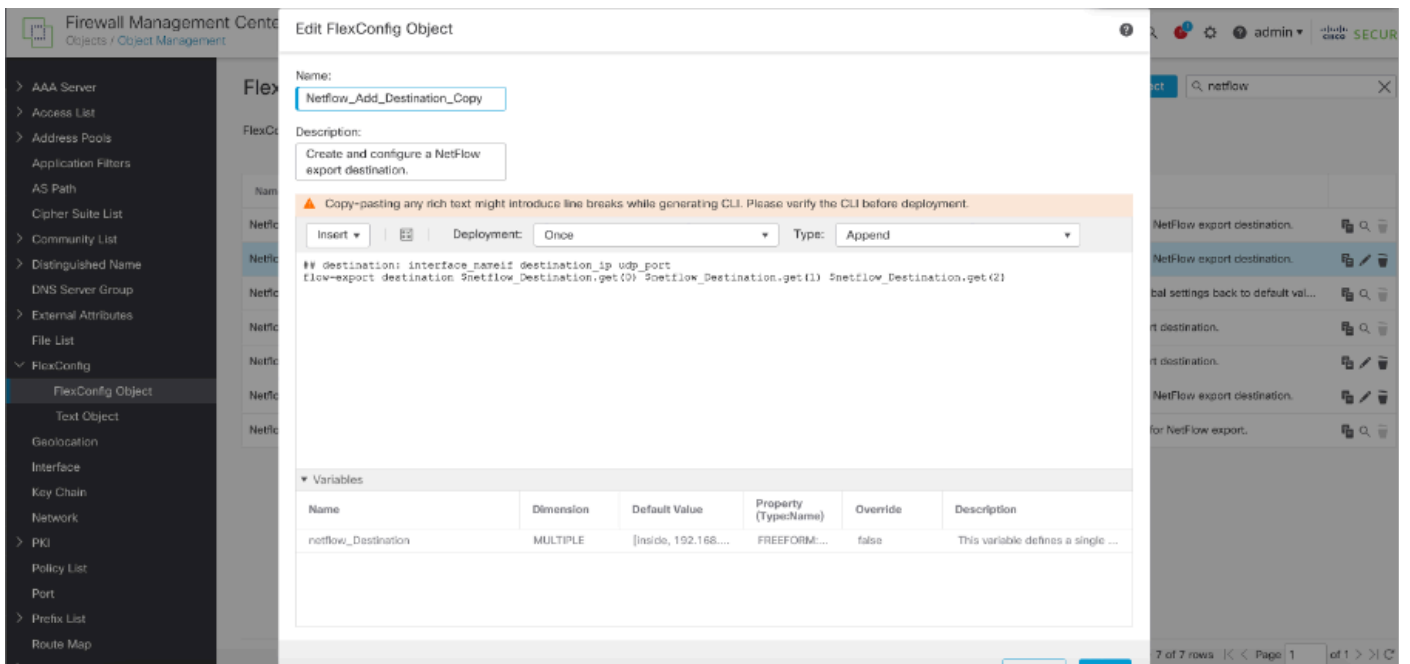
ACL de exportação de fluxo

3. Mapeamento de classe e política de serviço usados para aplicar esse mapa de classe com destino de exportação de fluxo



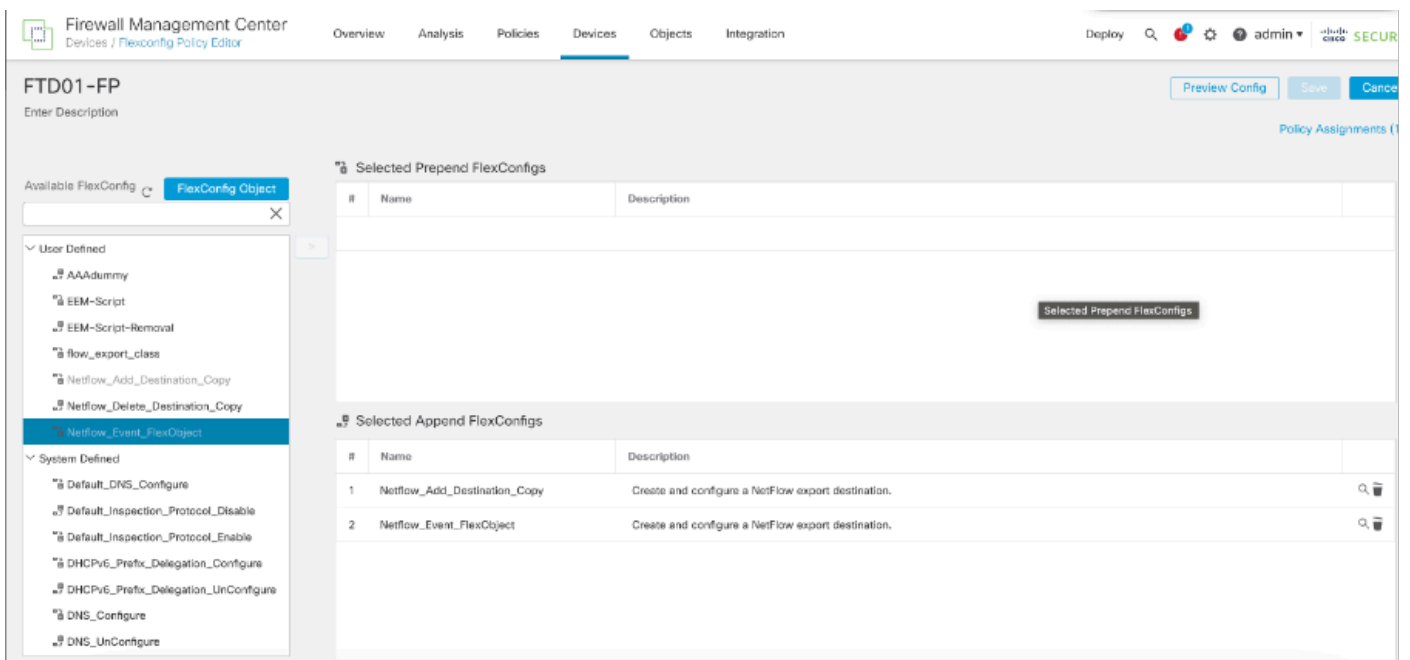
Mapa de classe e política de serviço

4. Destino da exportação do fluxo



Destino da exportação de fluxo

5. Em seguida, adicionou estes dois objetos na política de configuração flexível e implantou:



Política FlexConfig

Remover configurações do NetFlow

Etapa 1: Exclua os objetos flex da política flex.

Excluir flexconfig existente

Etapa 2: Implante a política. Na linha de comando, veríamos que as configurações removidas são:

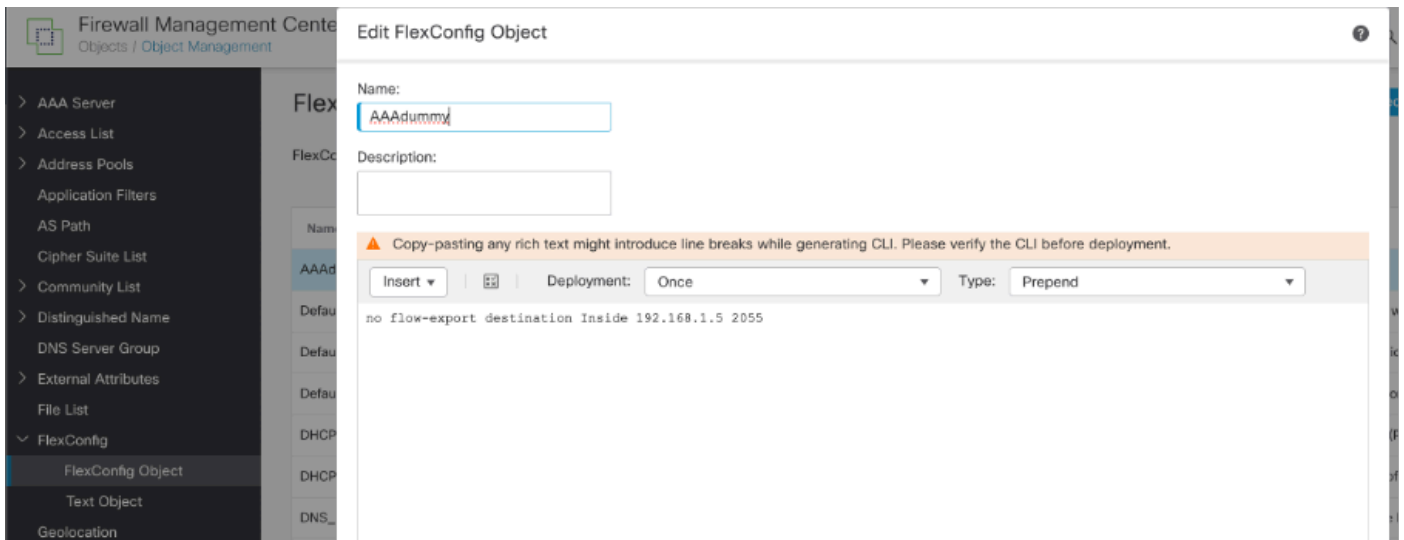
```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
  match access-list flow_export_acl
!
policy-map global_policy
  class flow_export_class
    flow-export event-type flow-create destination 192.168.1.5
    flow-export event-type flow-denied destination 192.168.1.5
    flow-export event-type flow-teardown destination 192.168.1.5
    flow-export event-type flow-update destination 192.168.1.5
```

Considerando que a configuração que não é removida é:

```
flow-export destination Inside 192.168.1.5 2055
```

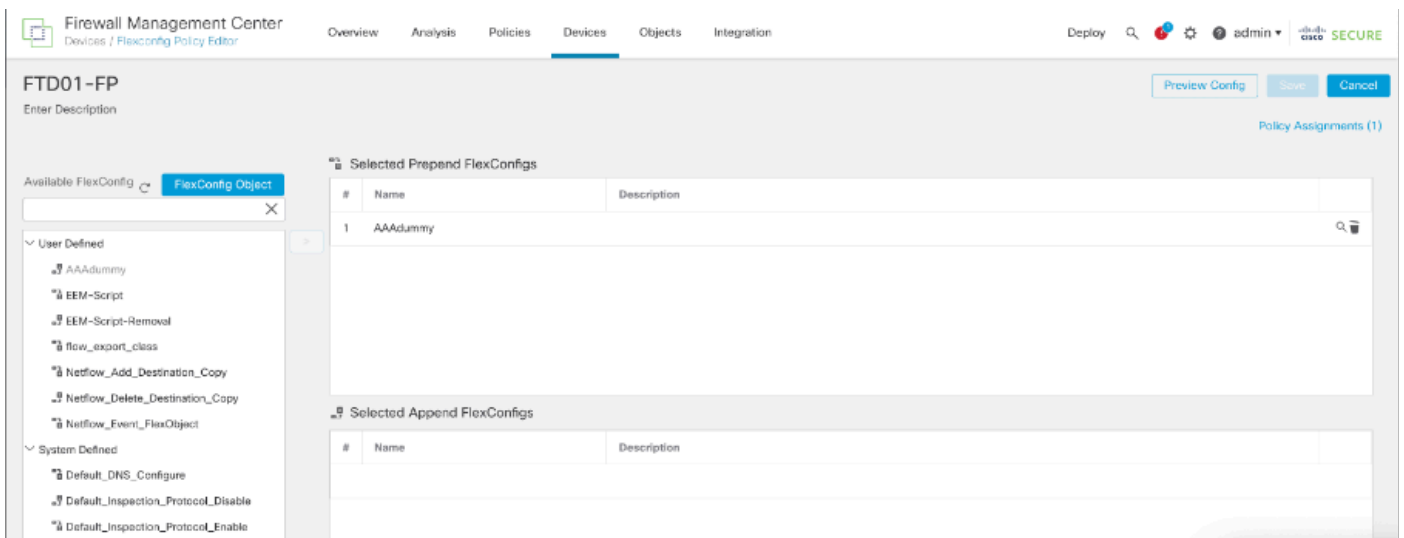
Etapa 3: Para remover isso, precisamos criar um objeto flex com o Tipo 'prepend' e adicionar a configuração:

```
no flow-export destination Inside 192.168.1.5 2055
```



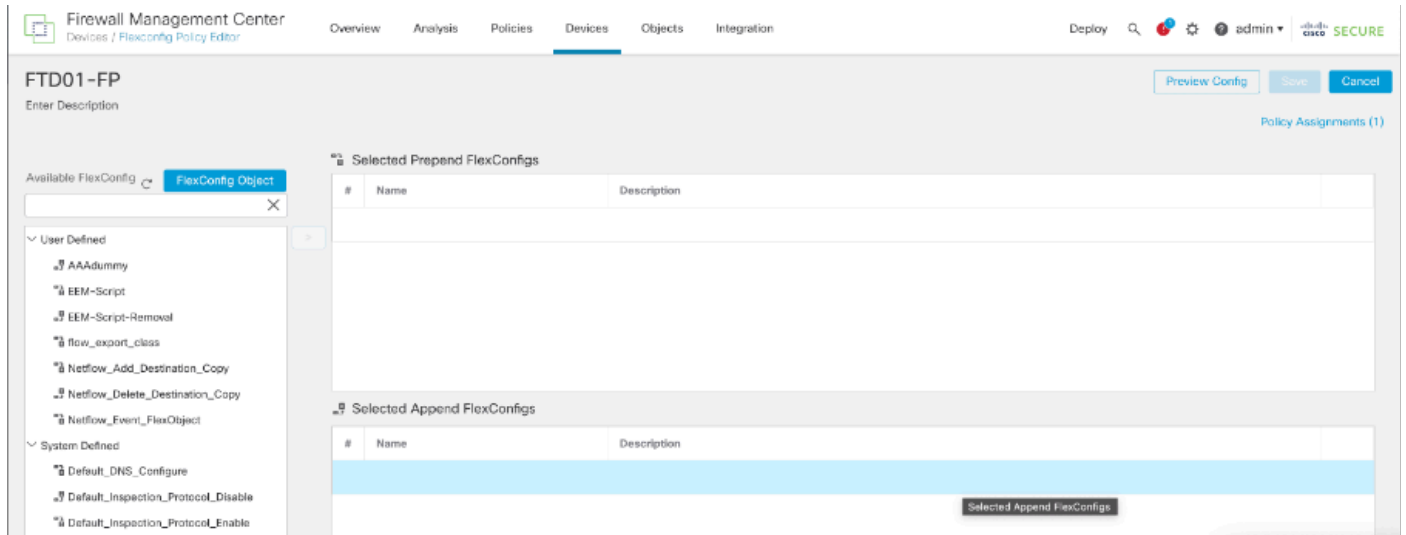
Excluir destino de configuração flexível

Etapa 4: em política flex, chame o objeto prefixo recém-criado na Etapa 3 e implante a política.



Adicione isso na política de configuração flexível

Etapa 5: Exclua esse objeto de prefixo da política flex e implante novamente.



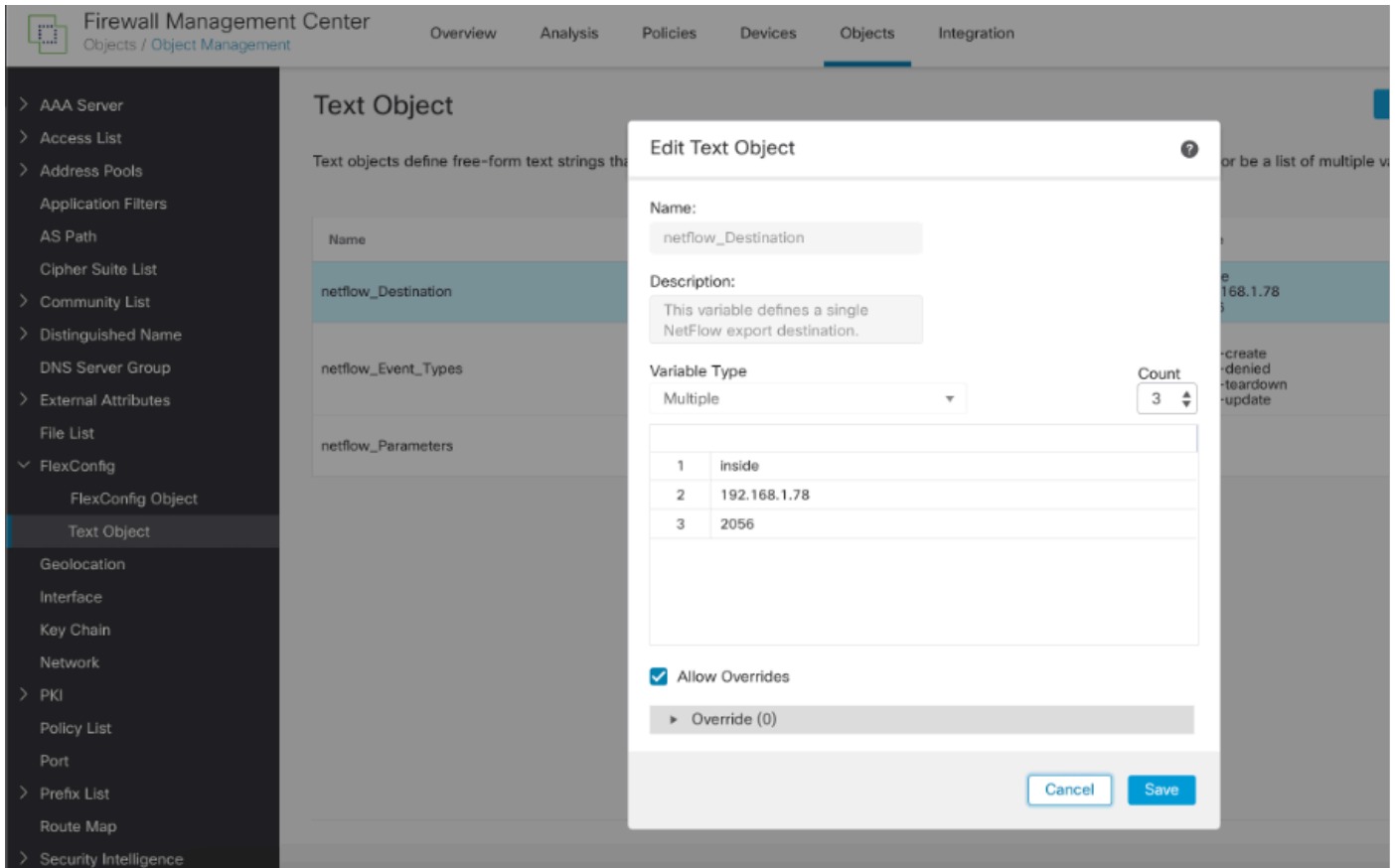
Excluir o objeto precedente

Toda a configuração relacionada à exportação de fluxo é removida agora.

Modificar as configurações do NetFlow existentes

Etapa 1: edite o objeto Texto criado para o destino do Netflow. Altere os parâmetros necessários: IP, nome da interface ou Porta.

Exemplo: alteramos o IP e a porta de (192.168.1.5, 2055) para (192.168.1.78, 2056)



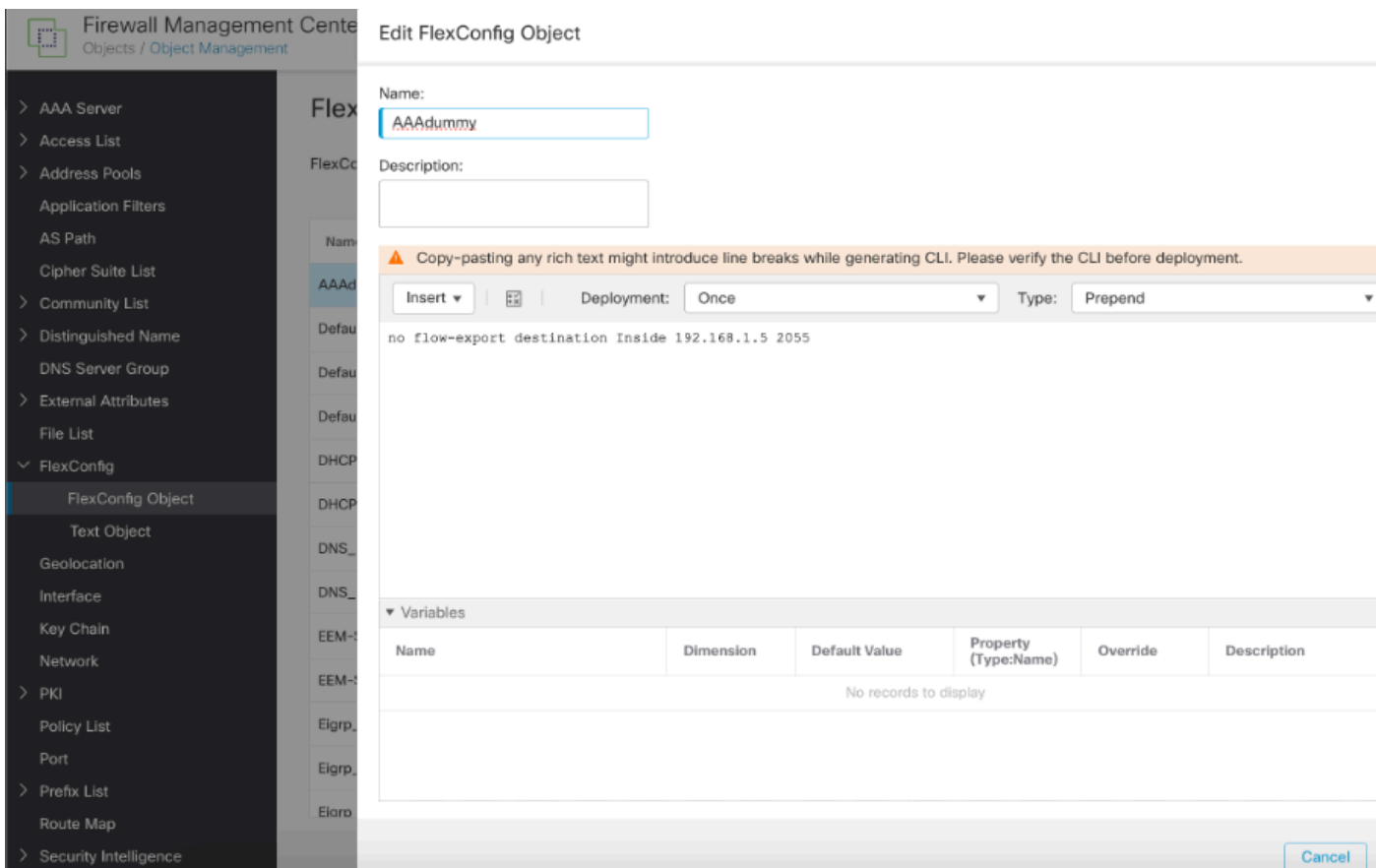
Objeto de texto de destino do Netflow

Etapa 2: Implante a política. Você verá que as alterações são refletidas como esperado, mas junto com a antiga configuração de destino do Netflow:

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.78
  flow-export event-type flow-denied destination 192.168.1.78
  flow-export event-type flow-teardown destination 192.168.1.78
  flow-export event-type flow-update destination 192.168.1.78
!
flow-export destination Inside 192.168.1.78 2056
flow-export destination Inside 192.168.1.5 2055
```

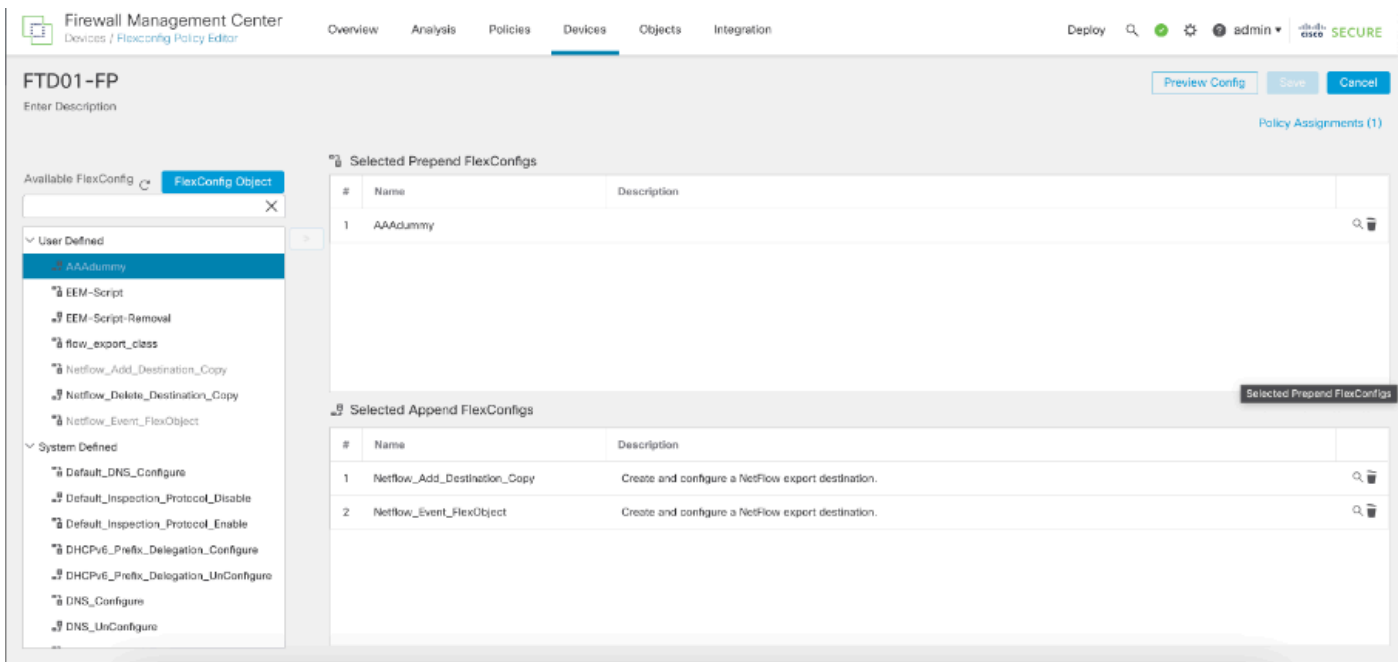
Etapa 3: Para remover isso, você precisa criar um objeto flex com o Tipo 'prepend' e adicionar a configuração:

no flow-export destination Inside 192.168.1.5 2055

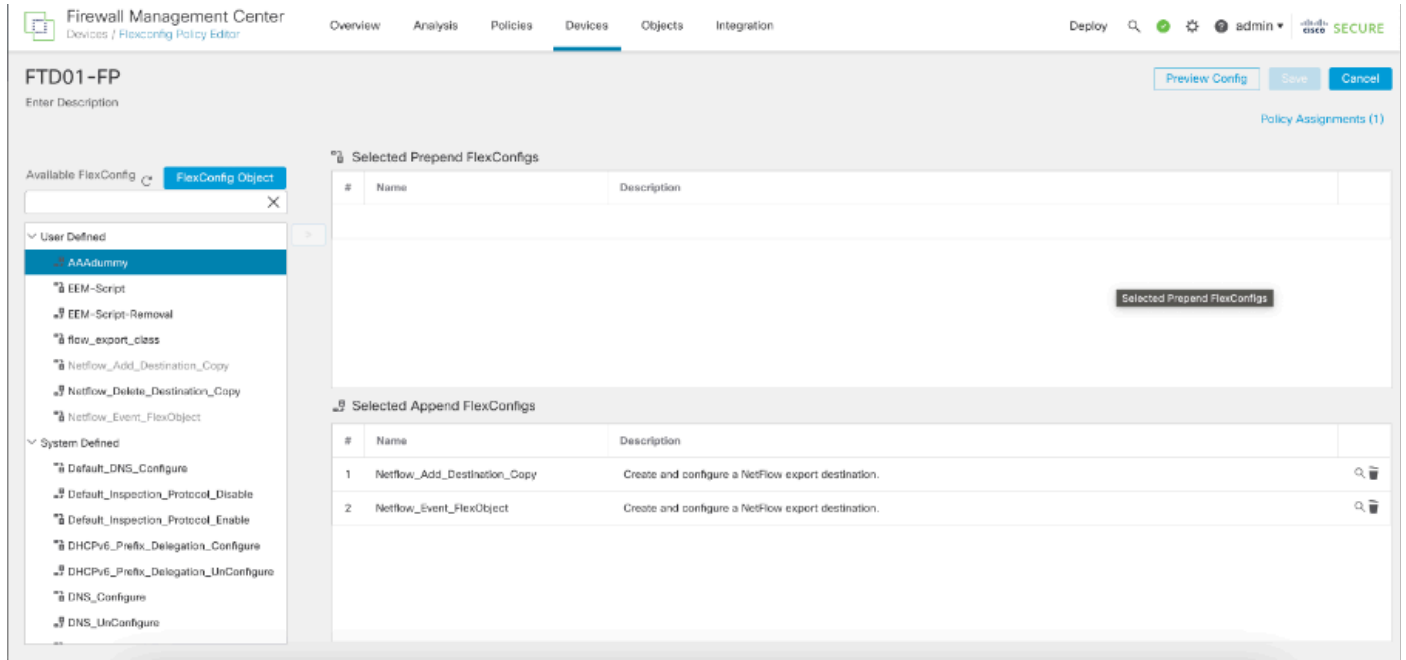


Excluir destino do netflow

Etapa 4: em política flex, chame o objeto prefixo recém-criado na Etapa 3 e implante a política.



Etapa 5: Exclua esse objeto de prefixo da política flex e implante novamente.



Excluir o prefixo FlexConfig

A configuração relacionada ao NetFlow foi modificada com êxito.

```
access-list flow_export_acl extended permit ip any any
!
flow-export destination Inside 192.168.1.78 2056
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.78
  flow-export event-type flow-denied destination 192.168.1.78
  flow-export event-type flow-teardown destination 192.168.1.78
  flow-export event-type flow-update destination 192.168.1.78
```

Documentos relacionados

<https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html>

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.