DTF: Como habilitar a configuração de desvio de estado TCP usando a política FlexConfig

Contents

Introduction

Este documento descreve como implementar o recurso de desvio de estado do Transmission Control Protocol (TCP) em dispositivos Firepower Threat Defense (FTD) via Firepower Management Center (FMC) usando a política FlexConfig em versões anteriores à 6.3.0.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firepower Management Center.
- Conhecimento básico da Firepower Threat Defense.
- Compreensão do recurso de desvio de estado TCP.

Componentes Utilizados

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

- Firepower Threat Defense (FTD) versão 6.2.3.
- Firepower Management Center (FMC) versão 6.2.3.

Informações de Apoio

O desvio de estado do TCP é um recurso herdado do Adaptive Security Appliance (ASA) e

fornece assistência na solução de problemas de tráfego que pode ser descartado por recursos de normalização do TCP, condições de roteamento assimétrico e determinadas Application Inspetions.

Este recurso é suportado nativamente no FMC iniciando a versão 6.3.0. Recomenda-se excluir os objetos Flexconfig após a atualização e mover essa configuração para o FMC antes da primeira implantação. Para obter mais informações sobre como configurar o desvio de estado do TCP na versão 6.3.0 ou posterior, vá para este guia de configuração.

O Firepower Threat Defense usa comandos de configuração do ASA para implementar alguns recursos, mas não todos. Não há um conjunto exclusivo de comandos de configuração do Firepower Threat Defense. Em vez disso, o objetivo do FlexConfig é permitir que você configure recursos que ainda não são suportados diretamente por meio de políticas e configurações do Firepower Management Center.

> **Observação**: o desvio de estado TCP deve ser usado somente para fins de solução de problemas ou quando o roteamento assimétrico não puder ser resolvido. O uso desse recurso desabilita vários recursos de segurança e pode causar um alto número de conexões se ele não for implementado corretamente.

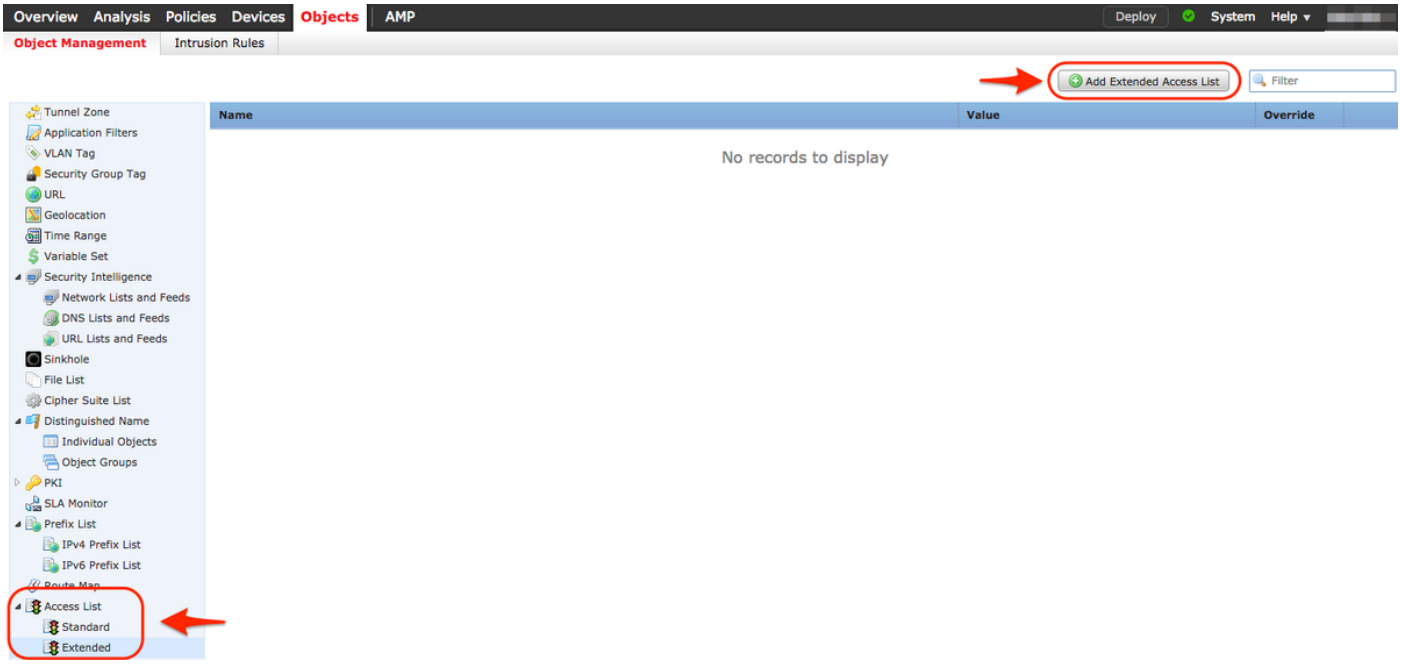
Para saber mais sobre o recurso TCP State Bypass ou sua implementação no ASA, consulte Configurar o recurso TCP State Bypass no ASA 5500 Series e o Cisco ASA 5500 Series Configuration Guide.

Configuração

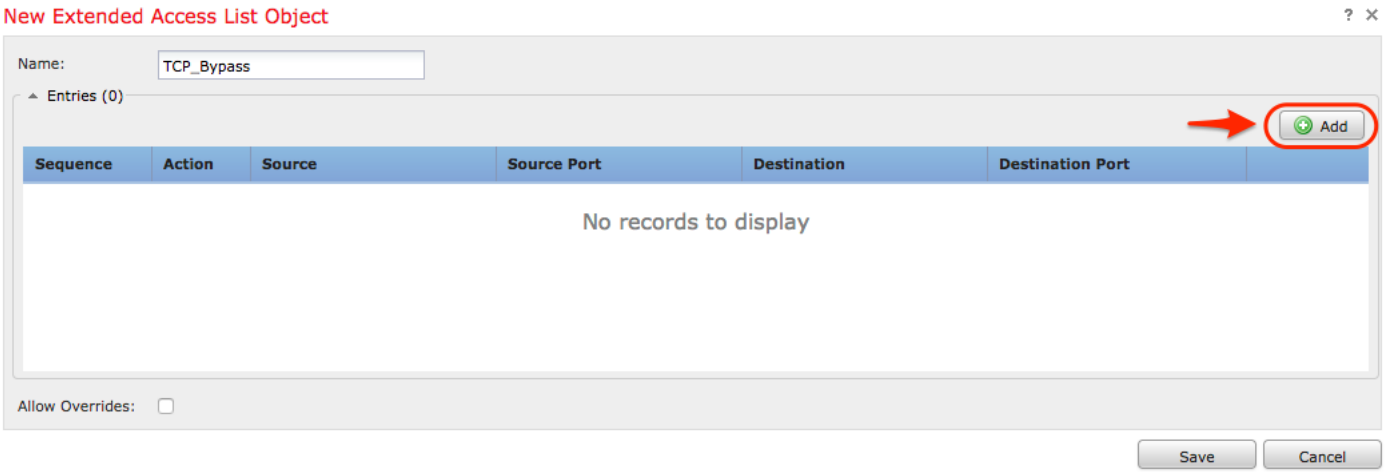
Esta seção descreve como configurar o desvio de estado TCP no FMC através de uma política FlexConfig.

Etapa 1. Configurar um objeto de lista de acesso estendida

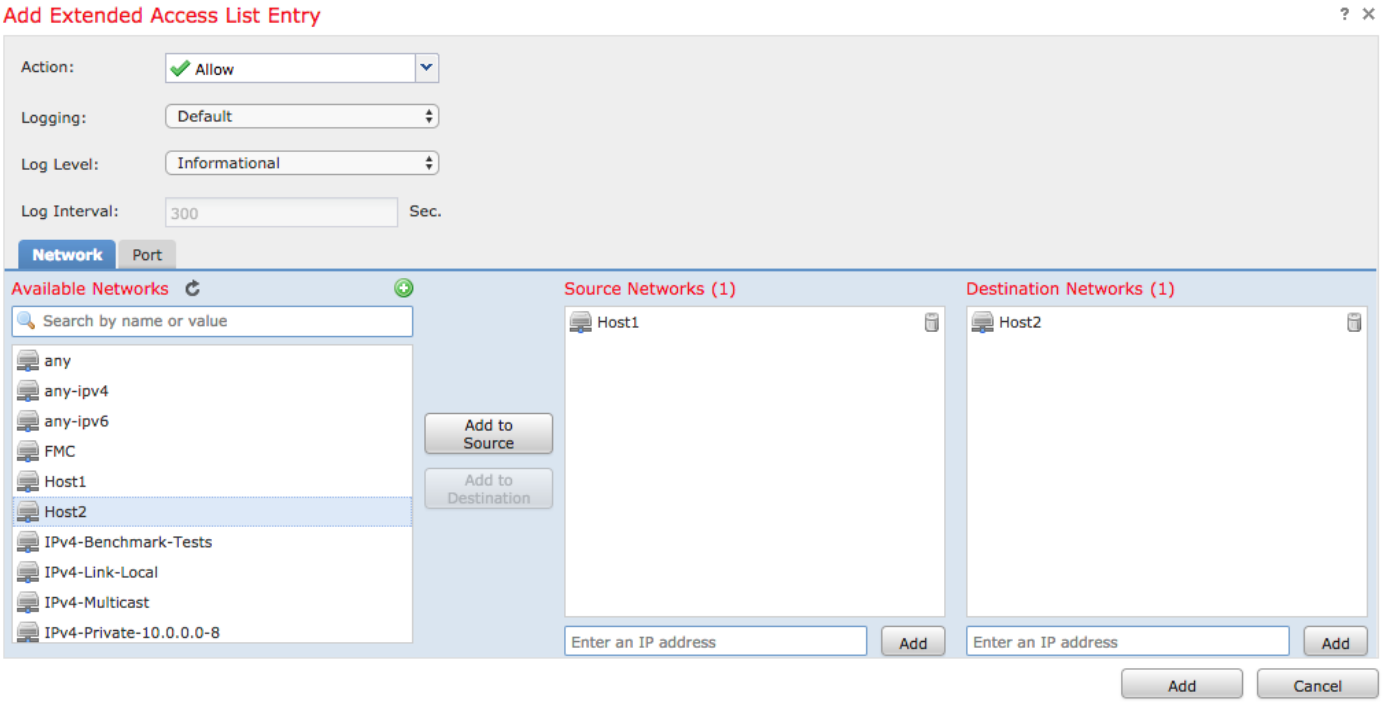
Para criar uma lista de acesso estendida no FMC, vá para **Objetos >Gerenciamento de objetos** e, no menu à esquerda, em **Lista de acesso,** selecione **Estendida. Clique em Adicionar lista de acesso estendida.**



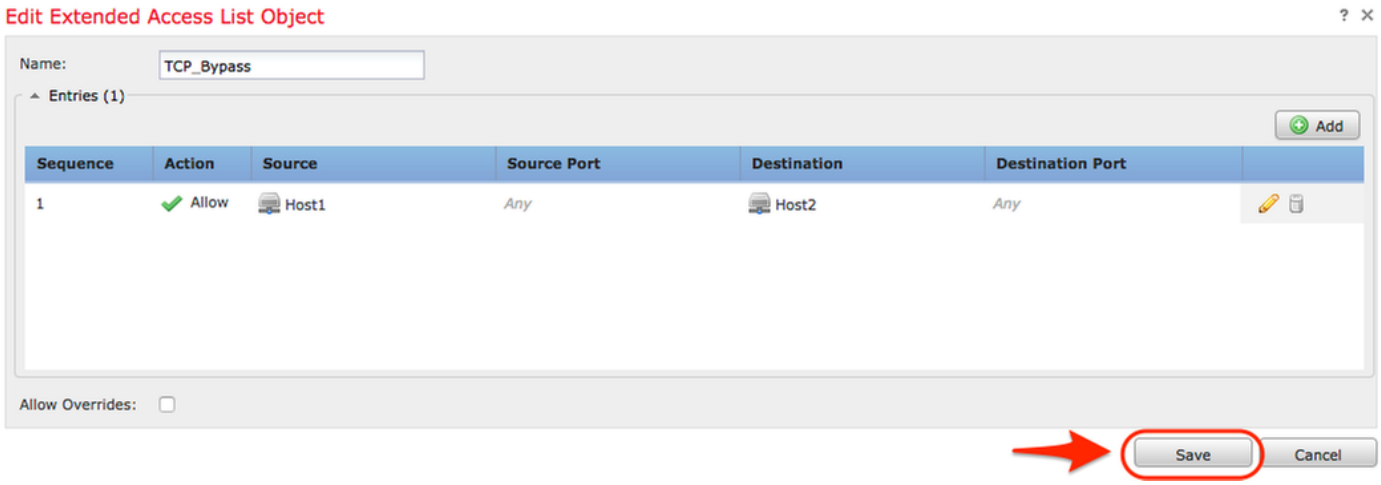
Preencha o campo Nome com o valor desejado. neste exemplo, o nome é **TCP_Bypass**. Clique no botão **Adicionar**.



A ação para esta regra deve ser configurada como **Permitir.** Uma rede definida pelo sistema pode ser usada ou um novo objeto de rede pode ser criado para cada origem e destino. Neste exemplo, a lista de acesso corresponde ao tráfego IP do Host 1 para o Host 2, pois essa é a comunicação para aplicar o desvio de estado do TCP. Opcionalmente, a guia Porta pode ser usada para corresponder a uma porta TCP ou UDP específica. Clique no botão **Adicionar** para continuar.

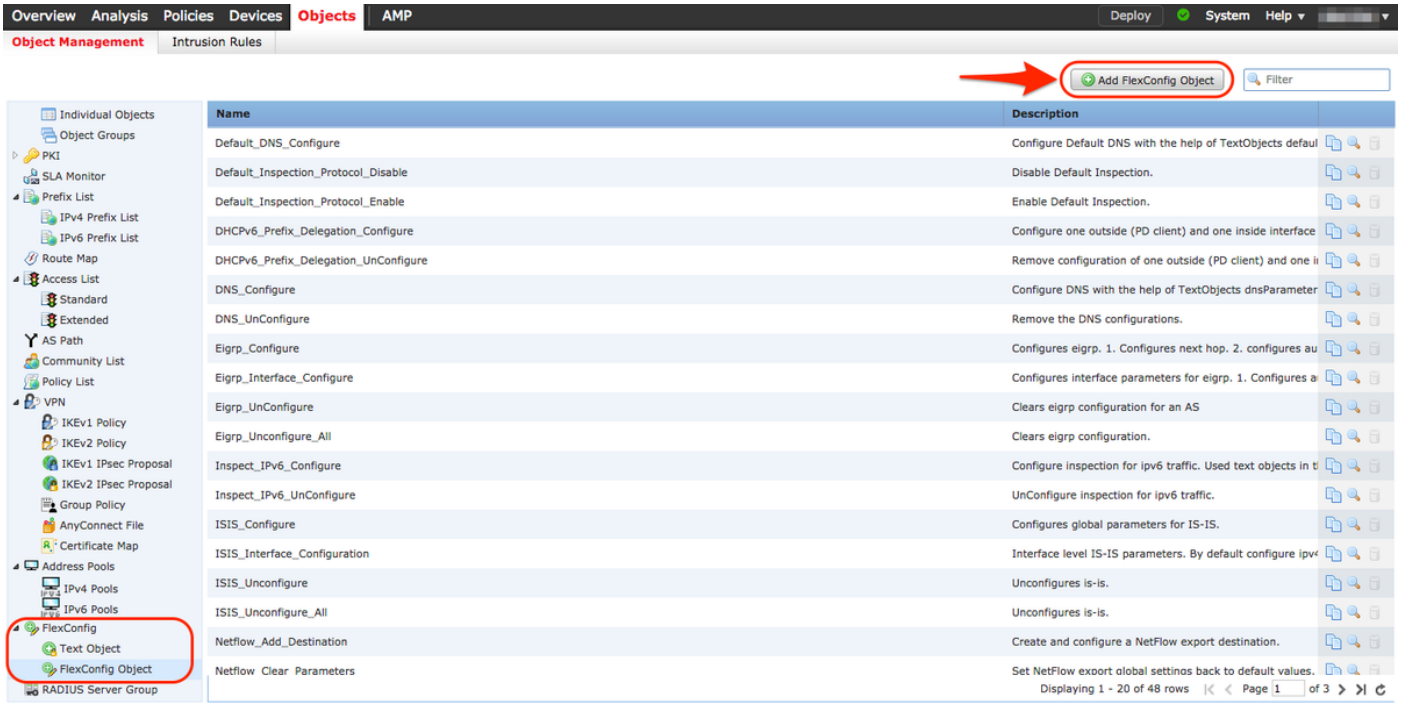


Depois que as redes ou hosts de origem e destino estiverem selecionados, clique em **Salvar**.



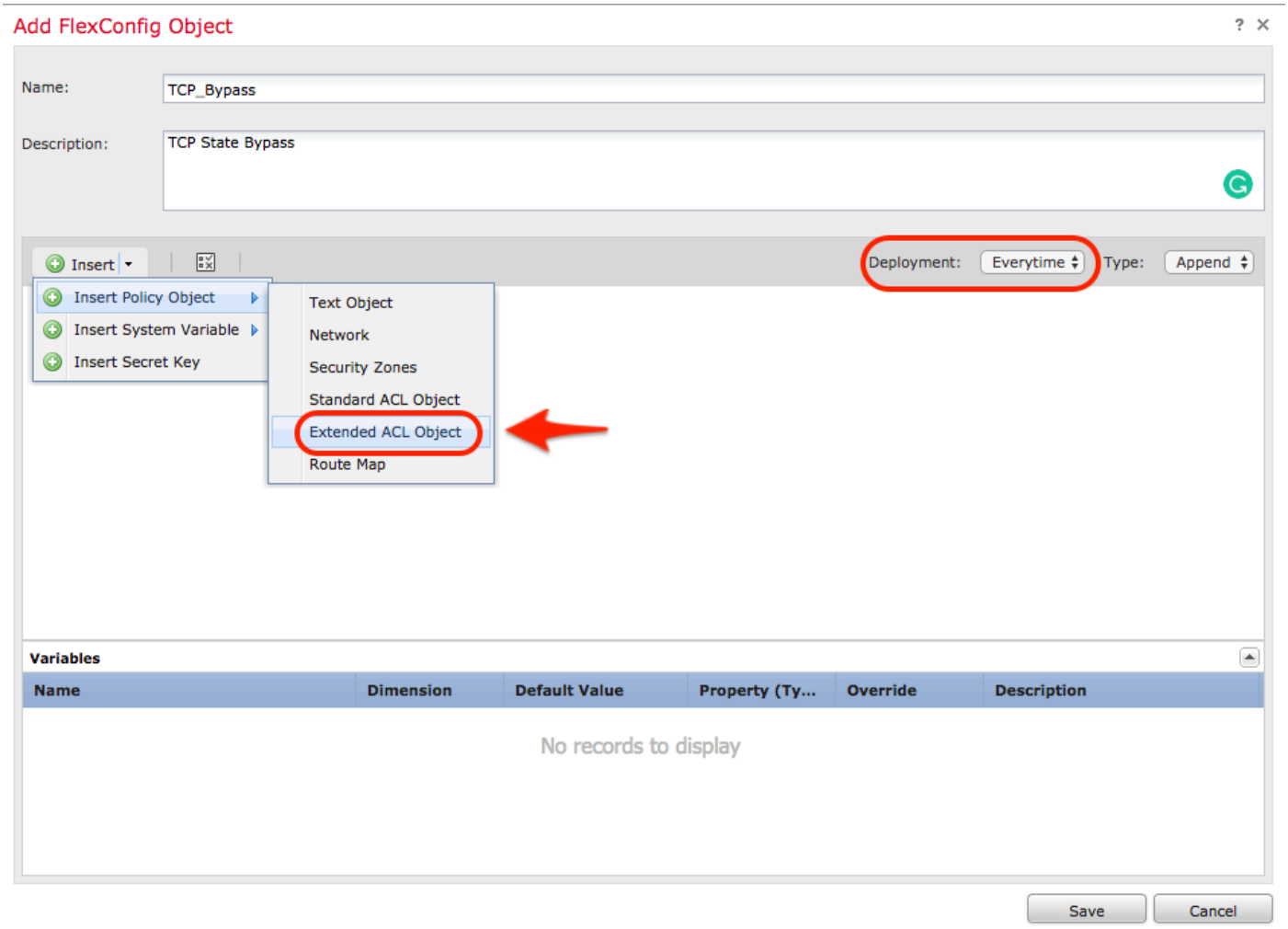
Etapa 2. Configurar um objeto FlexConfig

Navegue até **Objects > Object Management > FlexConfig > FlexConfig Object** e clique no botão **Add FlexConfig Object**.



O nome do objeto para este exemplo é chamado de **TCP_Bypass** exatamente como a Lista de acesso. Este nome não precisa corresponder ao nome da lista de acesso.

Selecione **Inserir objeto de política > Objeto de ACL estendida.**

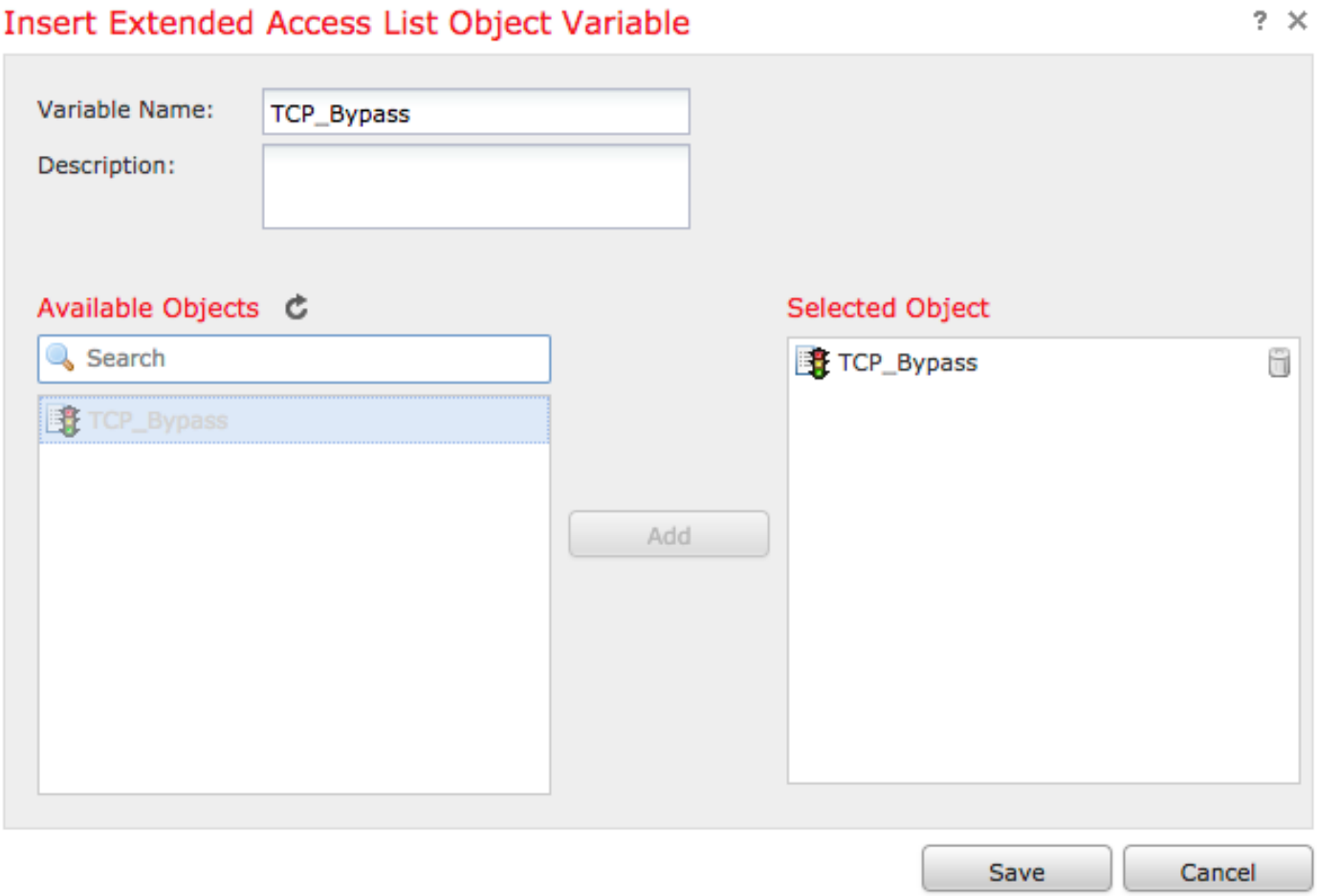


Note: Escolha a opção "Sempre". Isso permite preservar essa configuração durante outras

implantações e atualizações.

Selecione a Lista de acesso criada na Etapa 1 na seção **Objetos disponíveis** e atribua um Nome de variável. Em seguida, clique no botão **Adicionar**. Neste exemplo, o Nome da variável é **TCP_Bypass**.

Clique em **Salvar**.

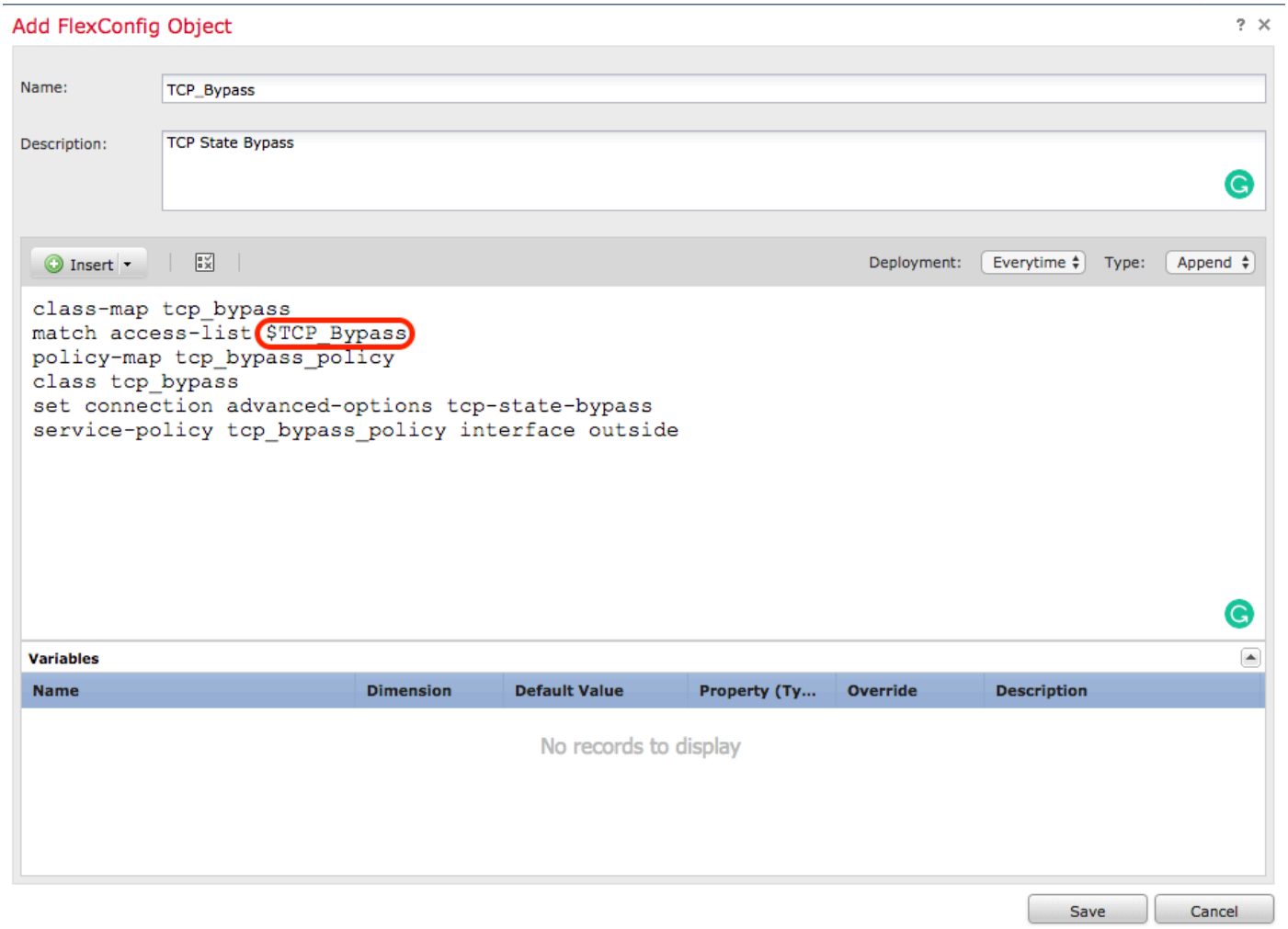


Adicione as próximas linhas de configuração no campo em branco logo abaixo do botão **Inserir** e inclua a variável previamente definida (**$TCP_Bypass**) na linha de configuração *match access-list*. Observe que um símbolo **$** é anexado ao nome da variável. Isso ajuda a definir que uma variável segue depois dela.

```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

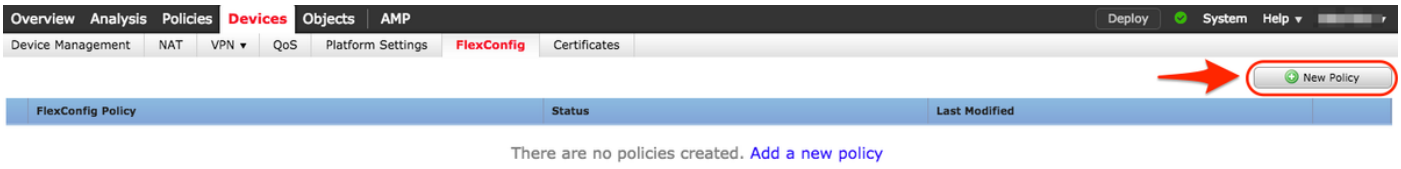
Neste exemplo, um mapa de política é criado e aplicado à interface externa. Se o desvio de estado do TCP exigir a configuração como parte da política de serviço global, o mapa de classe tcp_bypass pode ser aplicado a global_policy.

Clique em **Salvar** quando terminar.

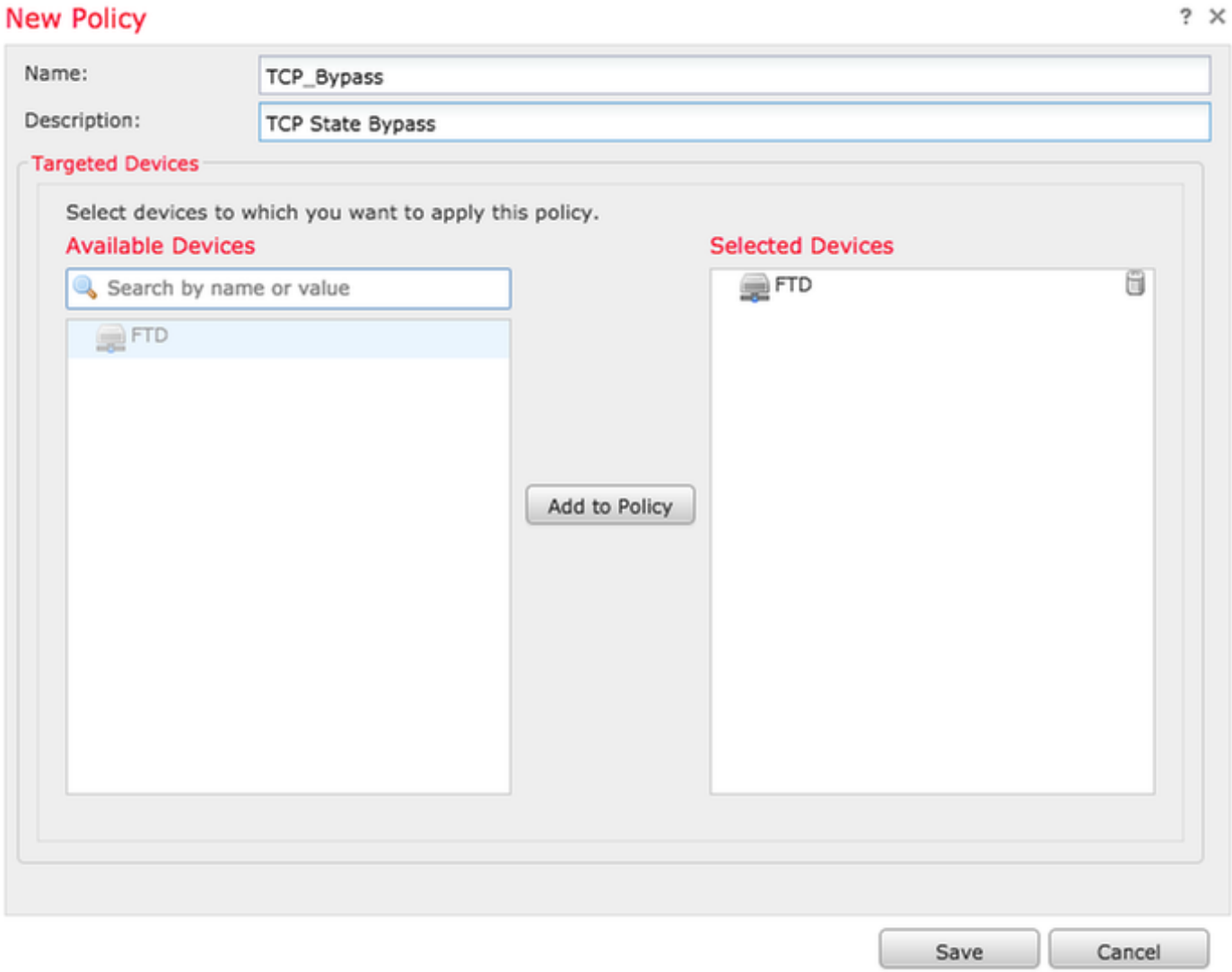


Etapa 3. Atribuir uma política FlexConfig ao FTD

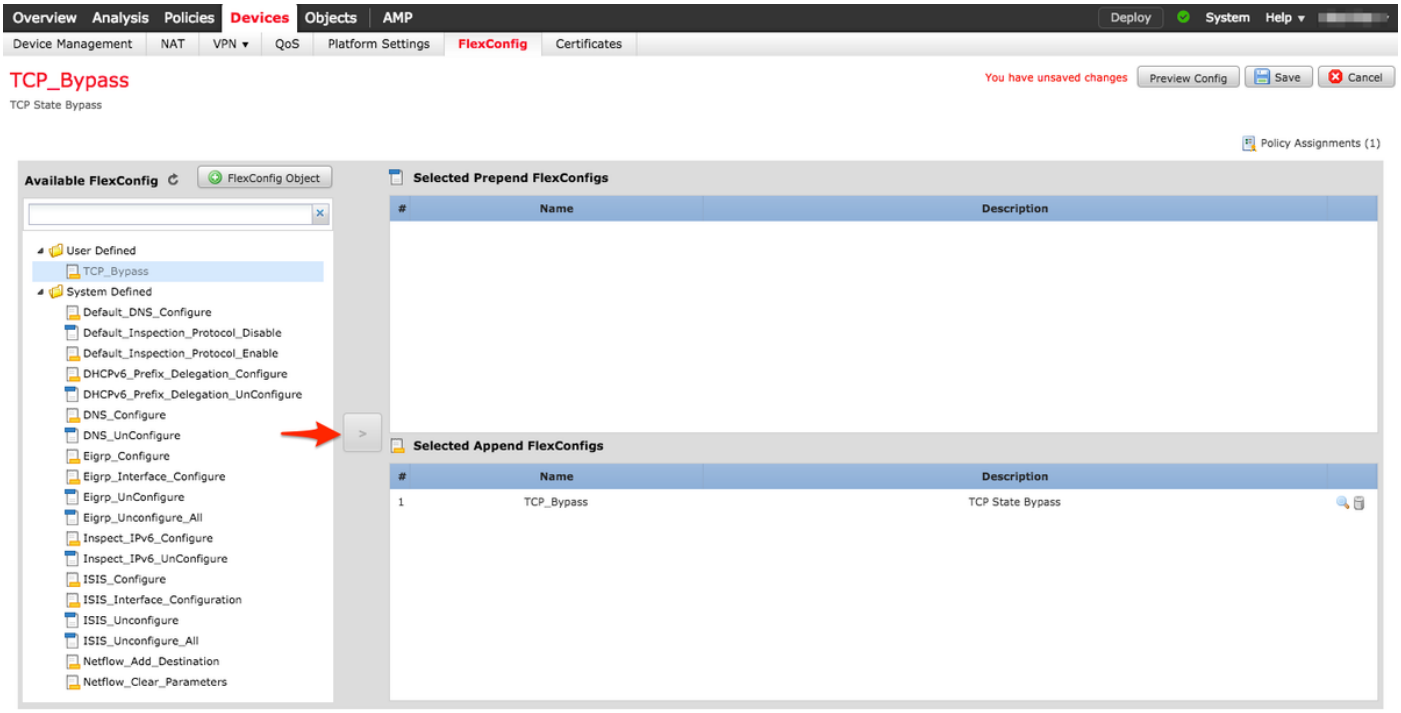
Vá para **Dispositivos > FlexConfig** e crie uma nova política (a menos que já exista uma criada para outra finalidade e atribuída ao mesmo FTD).Neste exemplo, a nova política FelxConfig é chamada de **TCP_Bypass**.



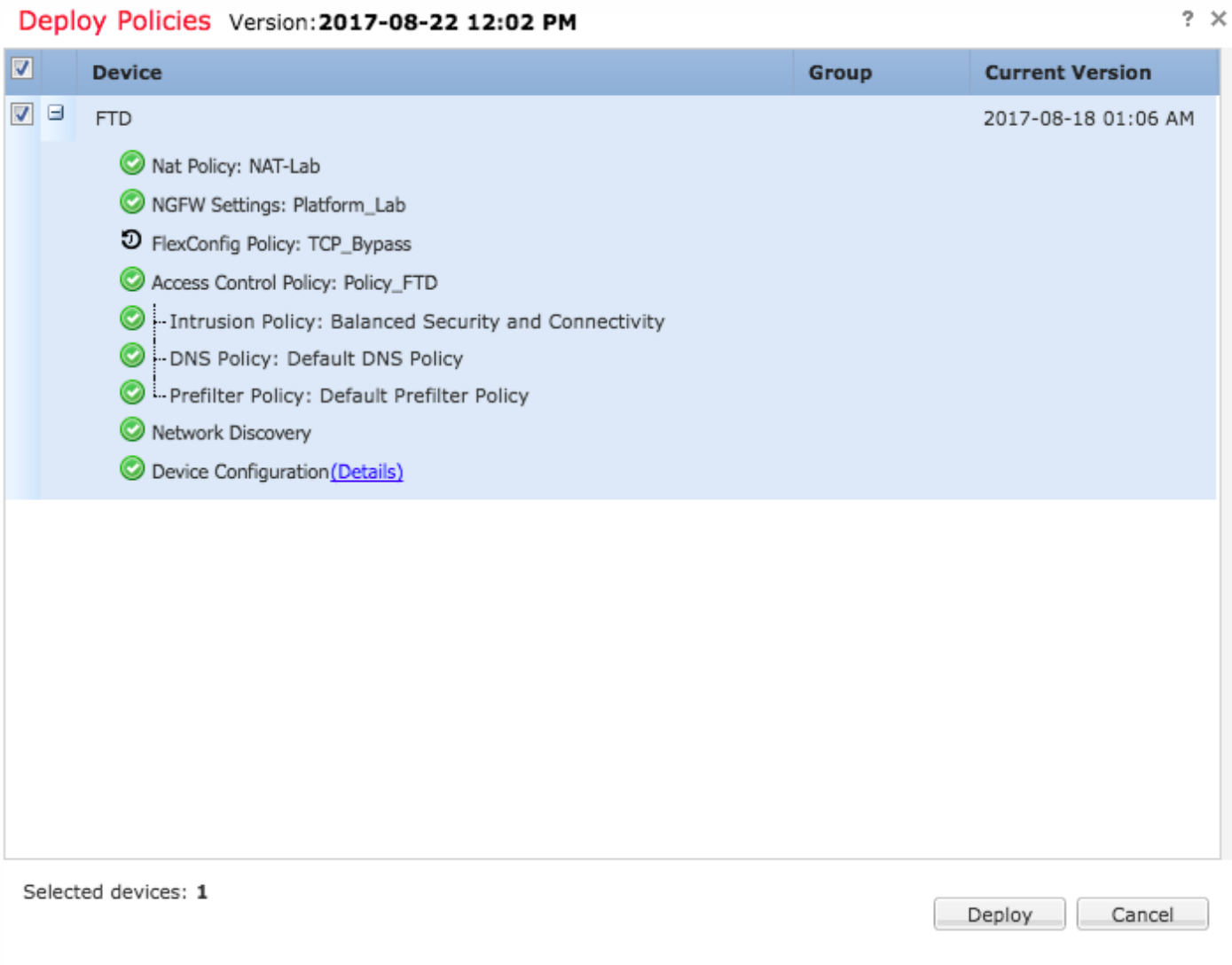
Atribua política **TCP_Bypass** FlexConfig ao dispositivo FTD.



Selecione o objeto FlexConfig chamado **TCP_Bypass** criado na Etapa 2 na seção **Definido pelo usuário** e clique na seta para adicionar esse objeto à política.



Salvar as alterações e implantar,



Verificação

Acesse o FTD por SSH ou console e use o comando **system support diagnostic-cli.**

```
> 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 TCP_Bypass
access-list TCP_Bypass; 1 elements; name hash: 0xec2b41eb
access-list TCP_Bypass line 1 extended permit object-group ProxySG_ExtendedACL_34359739205
object Host1 object Host2 log informational interval 300 (hitcnt=0) 0x42940b0e
access-list TCP_Bypass line 1 extended permit ip host 1.1.1.1 host 1.1.1.2 log informational
interval 300 (hitcnt=0) 0x769561fc

firepower# show running-config class-map
!
class-map inspection_default
match default-inspection-traffic
class-map tcp_bypass
match access-list TCP_Bypass
!
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
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
!
```

Troubleshoot

Para solucionar problemas desse recurso, esses comandos resultam em ajuda.

- show conn [detail]
Shows connection information. Detailed information uses flags to indicate special connection characteristics.
For example, the “b” flag indicates traffic subject to TCP State Bypass

- show service-policy
Shows service policy statistics, including Dead Connection Detection (DCD) statistics

Links relacionados

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/conns_connlimits.html

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118995-configure-asa-00.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html