

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

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração](#)

[Etapa 1. Configurar um objeto de lista de acesso estendida](#)

[Etapa 2. Configurar um objeto FlexConfig](#)

[Etapa 3. Atribuir uma política FlexConfig ao FTD](#)

[Verificação](#)

[Troubleshoot](#)

[Links relacionados](#)

## 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 Inspections.

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.

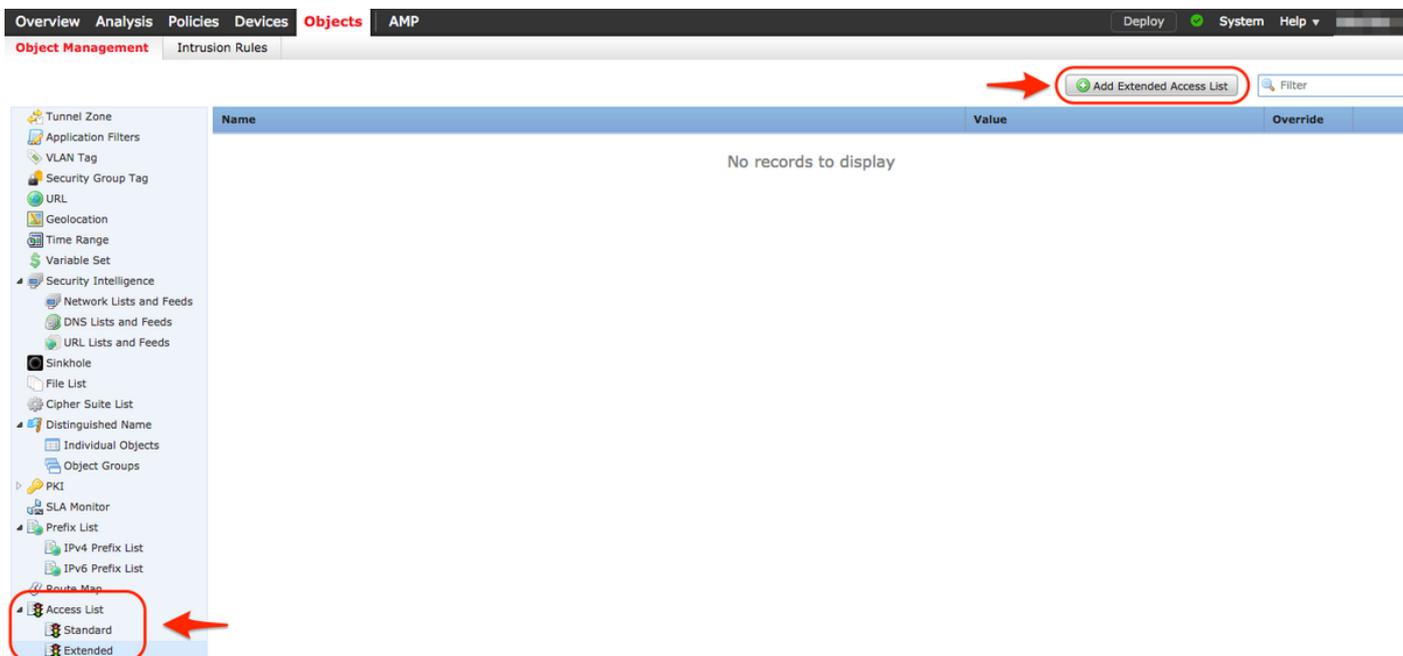
Para saber mais sobre o recurso TCP State Bypass ou sua implementação no ASA, consulte [Configurar o recurso TCP State Bypass no ASA 5500 Series](#) e o Cisco ASA 5500 Series Configuration Guide.

## Configuração

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

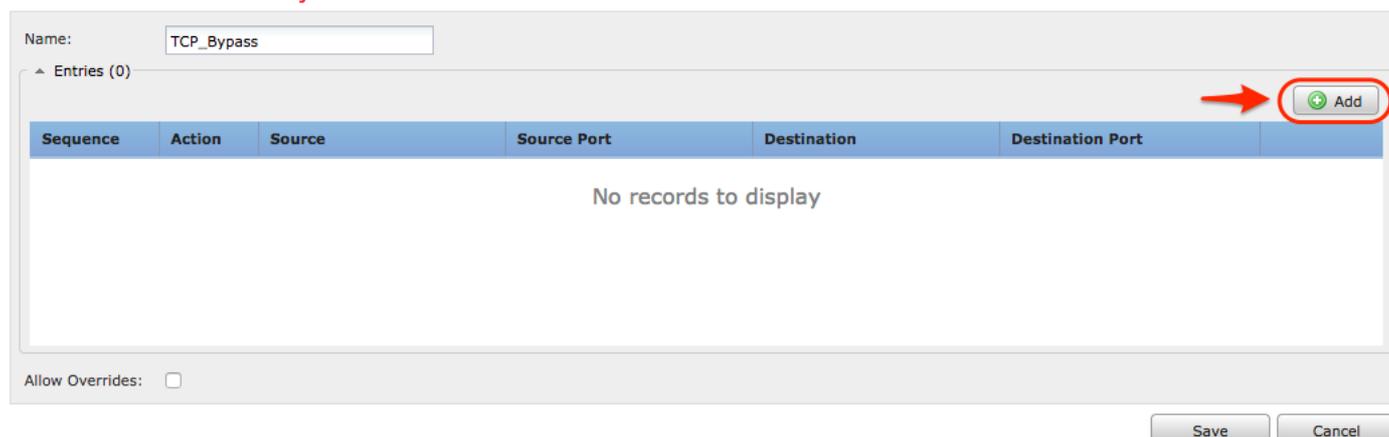
### Etapa 1. Configurar um objeto de lista de acesso estendida

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**.

#### New Extended Access List Object



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.

### Add Extended Access List Entry

? x

Action:  Allow

Logging:  Default

Log Level:  Informational

Log Interval:  Sec.

**Network** Port

Available Networks

- any
- any-ipv4
- any-ipv6
- FMC
- Host1
- Host2
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Add to Source

Add to Destination

Source Networks (1)

- Host1

Destination Networks (1)

- Host2

Enter an IP address  Add

Enter an IP address  Add

Add Cancel

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

### Edit Extended Access List Object

? x

Name:

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	
1	<input checked="" type="checkbox"/> Allow	Host1	Any	Host2	Any	<input type="checkbox"/> <input type="checkbox"/>

Allow Overrides:

Save  Cancel

## Etapa 2. Configurar um objeto FlexConfig

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

Overview Analysis Policies Devices **Objects** AMP Deploy System Help

Object Management Intrusion Rules

**Add FlexConfig Object** Filter

Name	Description
Default_DNS_Configure	Configure Default DNS with the help of TextObjects default
Default_Inspection_Protocol_Disable	Disable Default Inspection.
Default_Inspection_Protocol_Enable	Enable Default Inspection.
DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface
DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one i
DNS_Configure	Configure DNS with the help of TextObjects dnsParameter
DNS_UnConfigure	Remove the DNS configurations.
Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures au
Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures a
Eigrp_UnConfigure	Clears eigrp configuration for an AS
Eigrp_Unconfigure_All	Clears eigrp configuration.
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in t
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
ISIS_Configure	Configures global parameters for IS-IS.
ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv6
ISIS_Unconfigure	Unconfigures is-is.
ISIS_Unconfigure_All	Unconfigures is-is.
Netflow_Add_Destination	Create and configure a NetFlow export destination.
Netflow_Clear_Parameters	Set NetFlow export global settings back to default values.

Displaying 1 - 20 of 48 rows Page 1 of 3

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**.

**Add FlexConfig Object** ? x

Name: TCP\_Bypass

Description: TCP State Bypass

Deployment: **Everytime** Type: Append

- Insert Policy Object
  - Text Object
  - Network
  - Security Zones
  - Standard ACL Object
  - Extended ACL Object**
  - Route Map
- Insert System Variable
- Insert Secret Key

**Variables**

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

Save Cancel

**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**.

### Insert Extended Access List Object Variable

The screenshot shows a dialog box titled "Insert Extended Access List Object Variable". It has a search bar and a refresh icon. Below the search bar, there are two lists: "Available Objects" and "Selected Object". In the "Available Objects" list, "TCP\_Bypass" is selected. In the "Selected Object" list, "TCP\_Bypass" is also listed. An "Add" button is located between the two lists. At the bottom right, there are "Save" and "Cancel" buttons. The "Variable Name" field at the top contains "TCP\_Bypass" and the "Description" field is empty.

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.

## Add FlexConfig Object

Name:

Description:

Deployment:  Type:

```
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
```

**Variables**

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

Save Cancel

### 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 FlexConfig é chamada de **TCP\_Bypass**.



Atribua política **TCP\_Bypass** FlexConfig ao dispositivo FTD.

## New Policy



Name:

Description:

**Targeted Devices**

Select devices to which you want to apply this policy.

**Available Devices**

FTD

**Selected Devices**

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.

Overview Analysis Policies **Devices** Objects AMP Deploy System Help

Device Management NAT VPN QoS Platform Settings **FlexConfig** Certificates

**TCP\_Bypass** You have unsaved changes

TCP State Bypass

Policy Assignments (1)

**Available FlexConfig**

- User Defined
  - TCP\_Bypass**
- System Defined
  - Default\_DNS\_Configure
  - Default\_Inspection\_Protocol\_Disable
  - Default\_Inspection\_Protocol\_Enable
  - DHCPv6\_Prefix\_Delegation\_Configure
  - DHCPv6\_Prefix\_Delegation\_UnConfigure
  - DNS\_Configure
  - DNS\_UnConfigure
  - Eigrp\_Configure
  - Eigrp\_Interface\_Configure
  - Eigrp\_UnConfigure
  - Eigrp\_Unconfigure\_All
  - Inspect\_IPv6\_Configure
  - Inspect\_IPv6\_UnConfigure
  - ISIS\_Configure
  - ISIS\_Interface\_Configuration
  - ISIS\_UnConfigure
  - ISIS\_Unconfigure\_All
  - Netflow\_Add\_Destination
  - Netflow\_Clear\_Parameters

**Selected Prepend FlexConfigs**

#	Name	Description
---	------	-------------

**Selected Append FlexConfigs**

#	Name	Description
1	TCP_Bypass	TCP State Bypass

Salvar as alterações e implantar,

Device	Group	Current Version
<input checked="" type="checkbox"/> <input type="checkbox"/> FTD		2017-08-18 01:06 AM
✔ Nat Policy: NAT-Lab		
✔ NGFW Settings: Platform_Lab		
🔄 FlexConfig Policy: TCP_Bypass		
✔ Access Control Policy: Policy_FTD		
✔ Intrusion Policy: Balanced Security and Connectivity		
✔ DNS Policy: Default DNS Policy		
✔ Prefilter Policy: Default Prefilter Policy		
✔ Network Discovery		
✔ Device Configuration( <a href="#">Details</a> )		

Selected devices: 1

Deploy

Cancel

## 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\\_configuration/conns\\_connlimits.html](https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_configuration/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-configuration-guide-v62/flexconfig\\_policies.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configuration-guide-v62/flexconfig_policies.html)