FTD:如何使用FlexConfig策略启用TCP状态绕行配置

目录

简介

本文档介绍如何在6.3.0之前的版本中使用FlexConfig策略，通过Firepower管理中心(FMC)在Firepower威胁防御(FTD)设备上实施传输控制协议(TCP)状态绕行功能。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解Firepower管理中心。
- Firepower威胁防御的基本知识。
- 了解TCP状态绕行功能。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower威胁防御(FTD)版本6.2.3。
- Firepower管理中心(FMC)版本6.2.3。

背景信息

TCP状态绕行是从自适应安全设备(ASA)继承的一项功能，在排除可能被TCP规范化功能、非对称路由条件和某些应用检测丢弃的流量时提供帮助。

从版本6.3.0开始，FMC本地支持此功能。建议在升级后删除Flexconfig对象，并在首次部署之前将此配置移到FMC。有关如何在版本6.3.0或更高版本中配置TCP状态绕行的详细信息，请转至此配置指南。

Firepower威胁防御使用ASA配置命令来实施某些功能，但并非所有功能。没有唯一的Firepower威胁防御配置命令集。相反，FlexConfig的要点是允许您配置尚未通过Firepower管理中心策略和设置直接支持的功能。

> 注意: TCP状态绕行仅应用于故障排除目的，或者当无法解决非对称路由时。使用此功能会禁用多个安全功能，如果未正确实施，则可能导致大量连接。

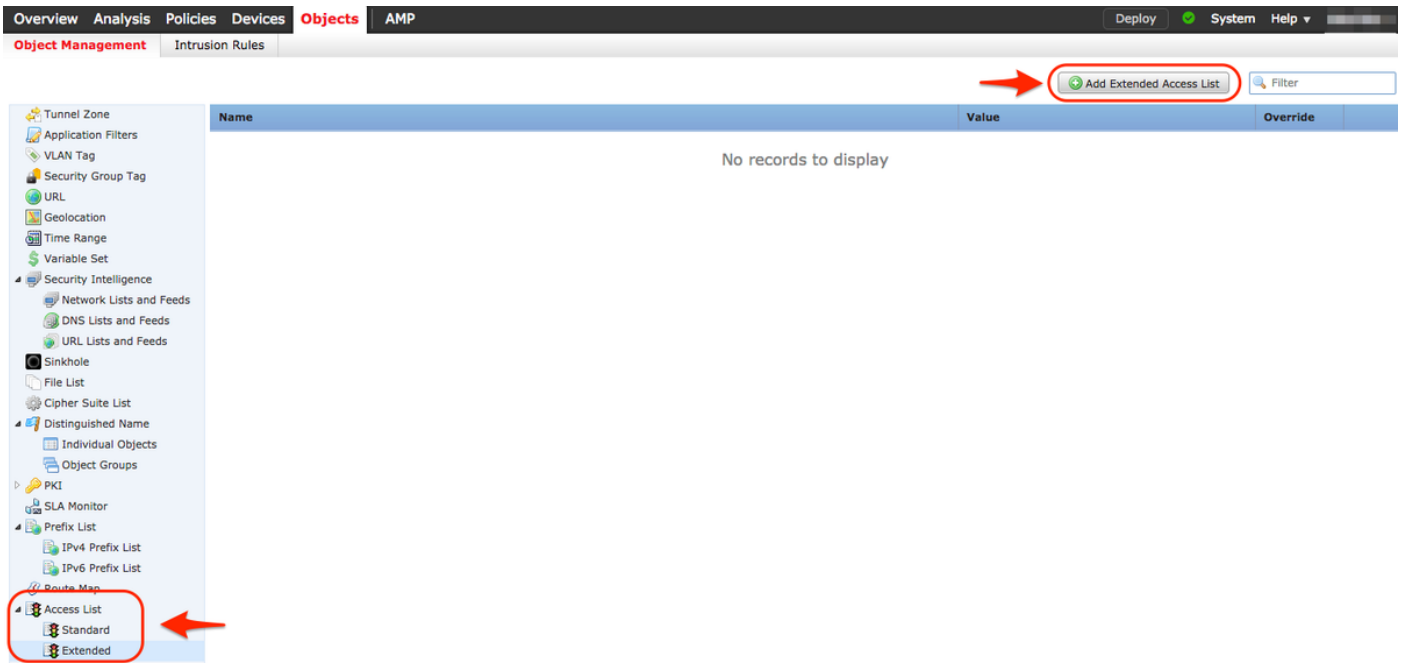
要了解有关TCP状态旁路功能或其在ASA中实施的详细信息，请参阅在ASA 5500系列和Cisco ASA 5500系列配置指南上配置TCP状态旁路功能。

配置

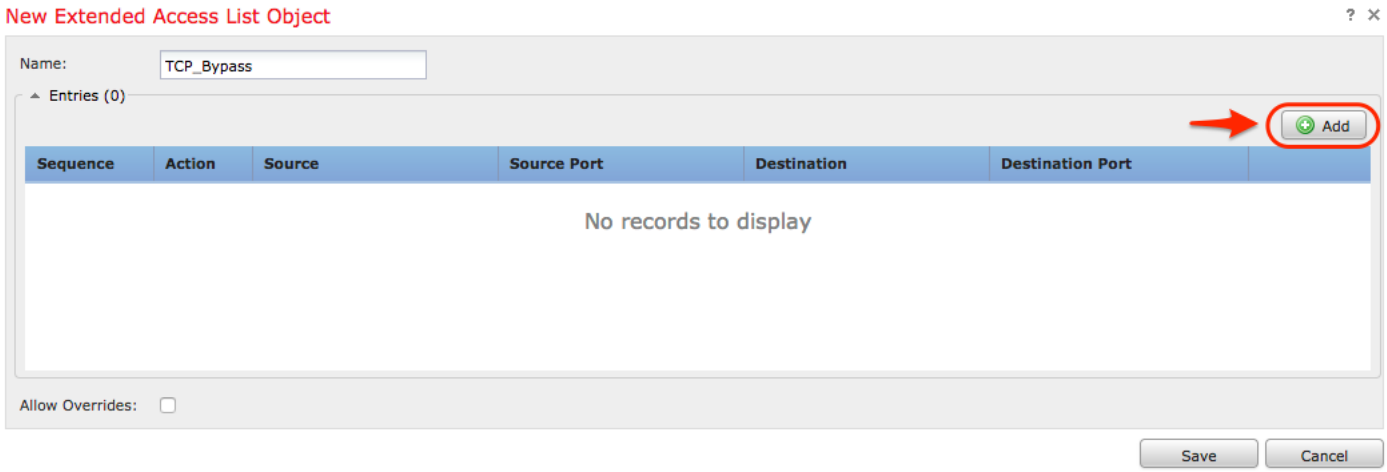
本节介绍如何通过FlexConfig策略在FMC上配置TCP状态绕行。

步骤1.配置扩展访问列表对象

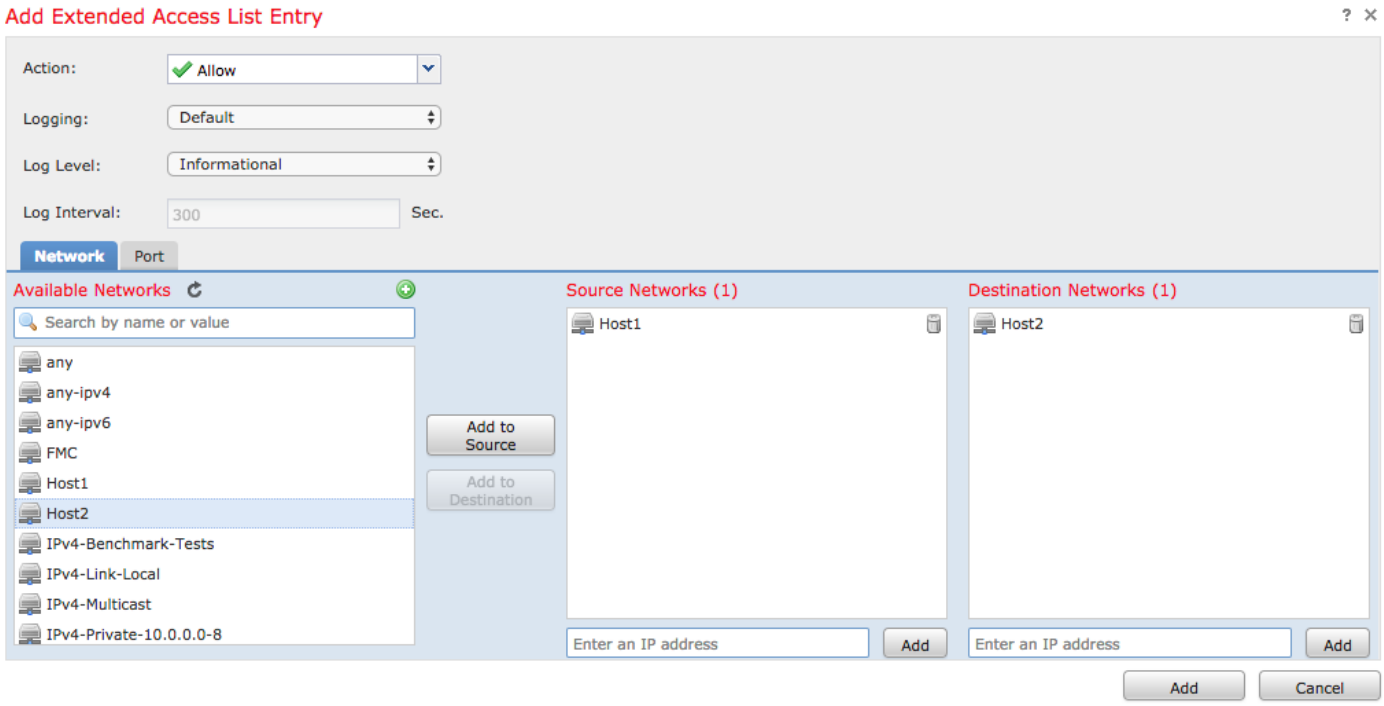
要在FMC上创建扩展访问列表，请转至对象>对象**管理，然后在左**侧菜单的访问列表下选择**扩展**访问**列表。点击添加扩展访问列表。**



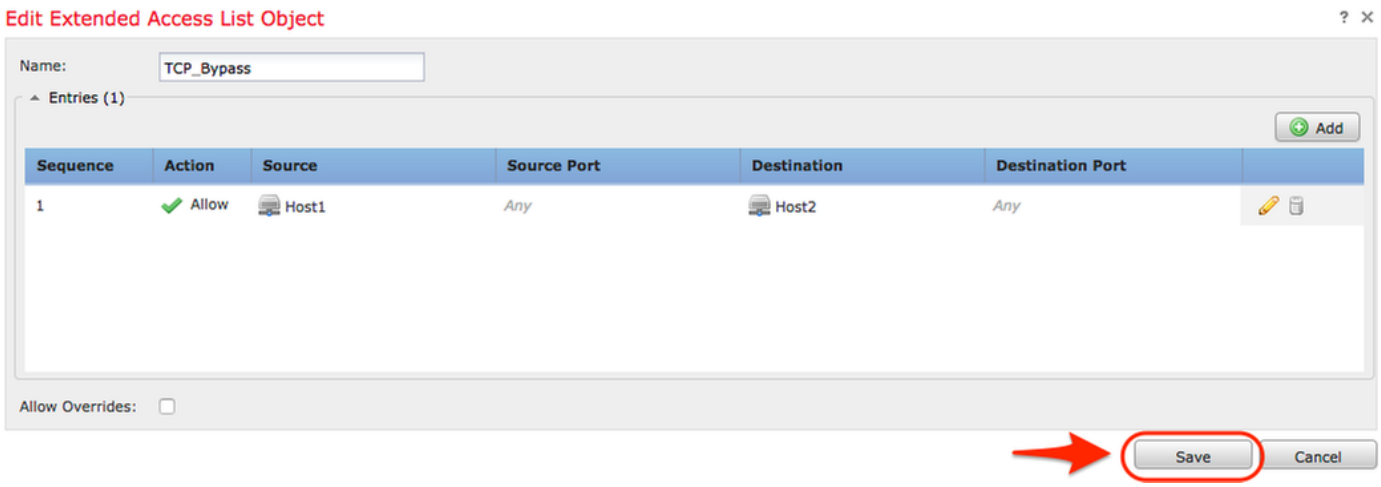
使用所需值填写“名称”字段。在本例中，名称为**TCP_Bypass**。单击**Add**按钮。



此规则的操作必须配置为**允许**。可以使用系统定义的网络，或为每个源和目标创建新的网络对象。在本示例中，访问列表匹配从主机1到主机2的IP流量，因为这是应用TCP状态绕行的通信。端口选项卡可以用于匹配特定TCP或UDP端口。单击“Add(添加)”按钮继续。

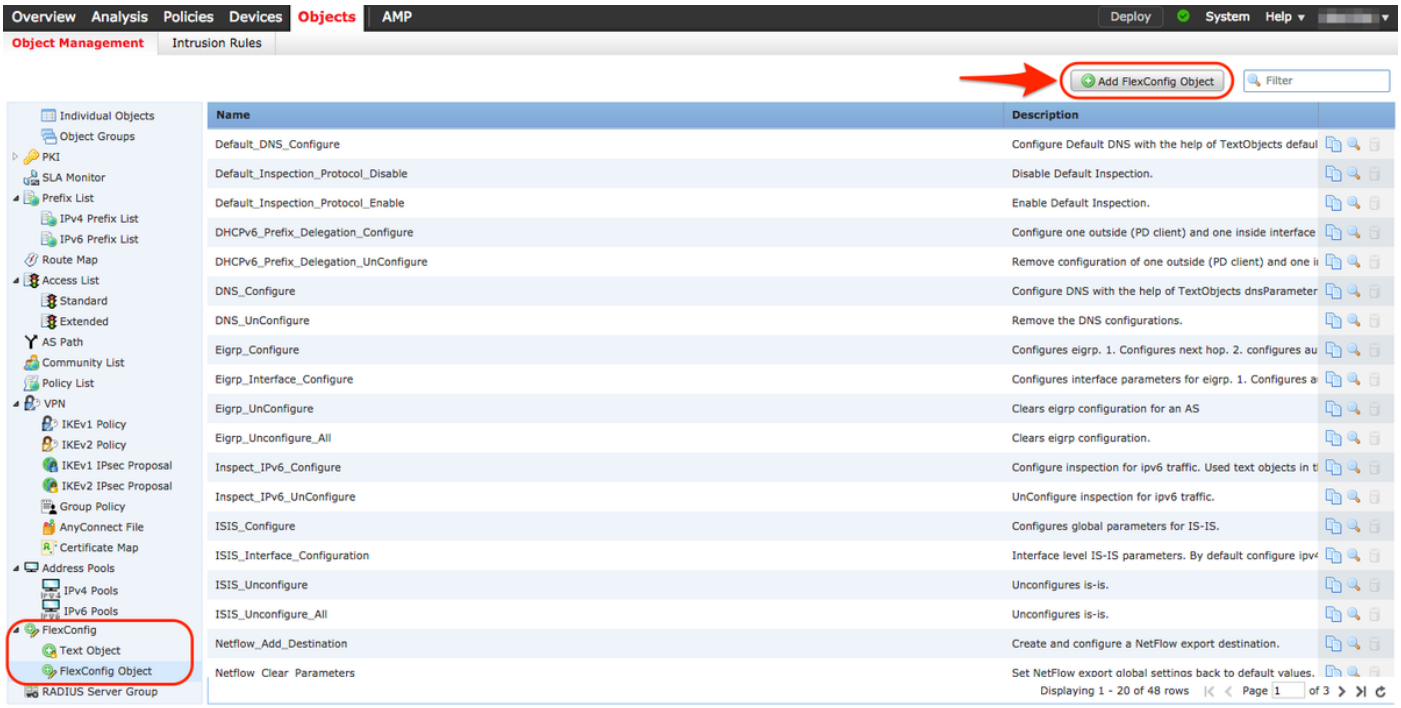


选择源网络和目标网络或主机后，单击**Save**。



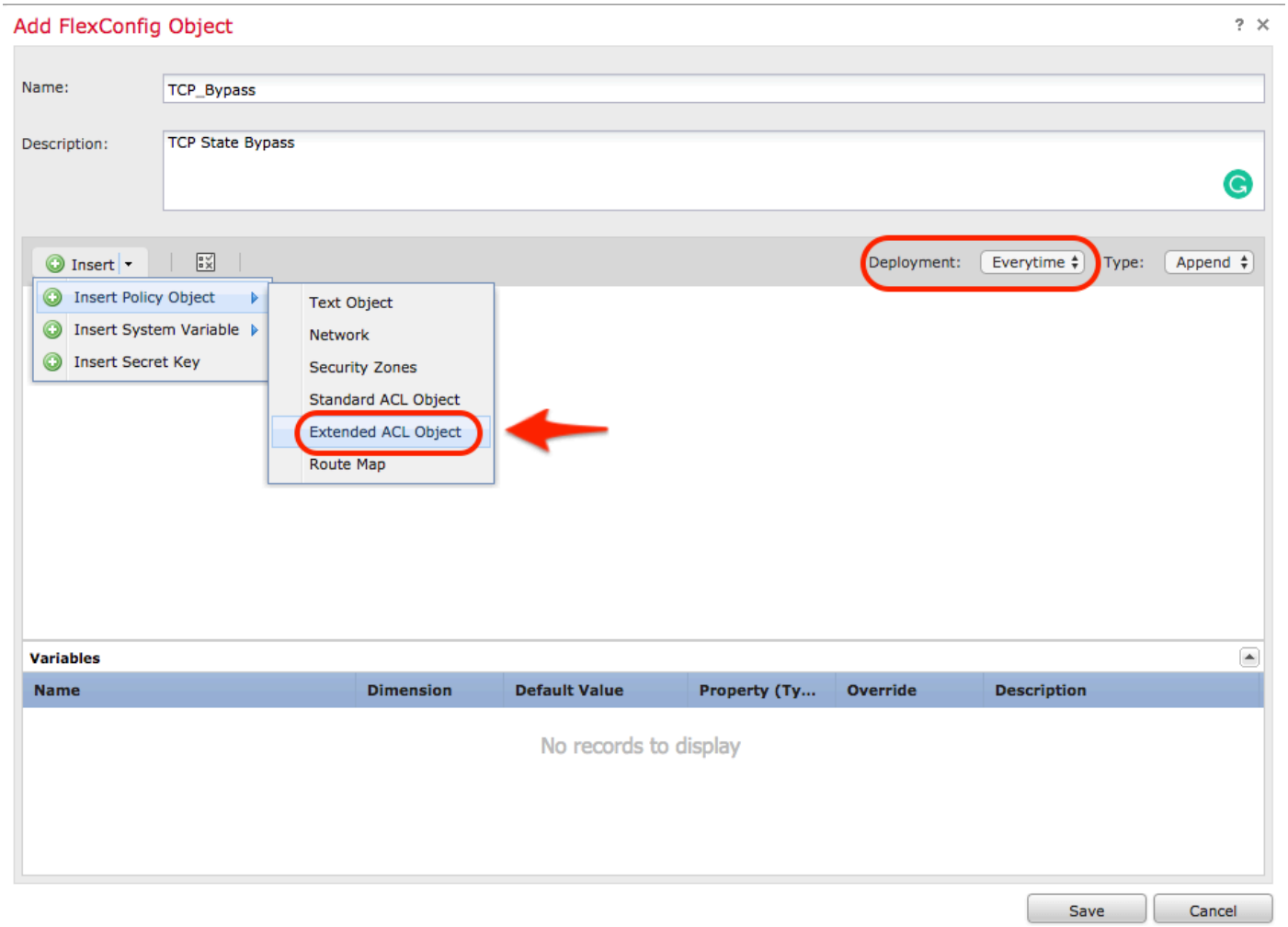
步骤2.配置FlexConfig对象

导航至“**对象**”>“**对象管理**”>“**FlexConfig**”>“**FlexConfig对象**”，然后单击“**添加FlexConfig对象**”按钮。



此示例的对象名称称为**TCP_Bypass**，与访问列表一样。此名称不需要与访问列表名称匹配。

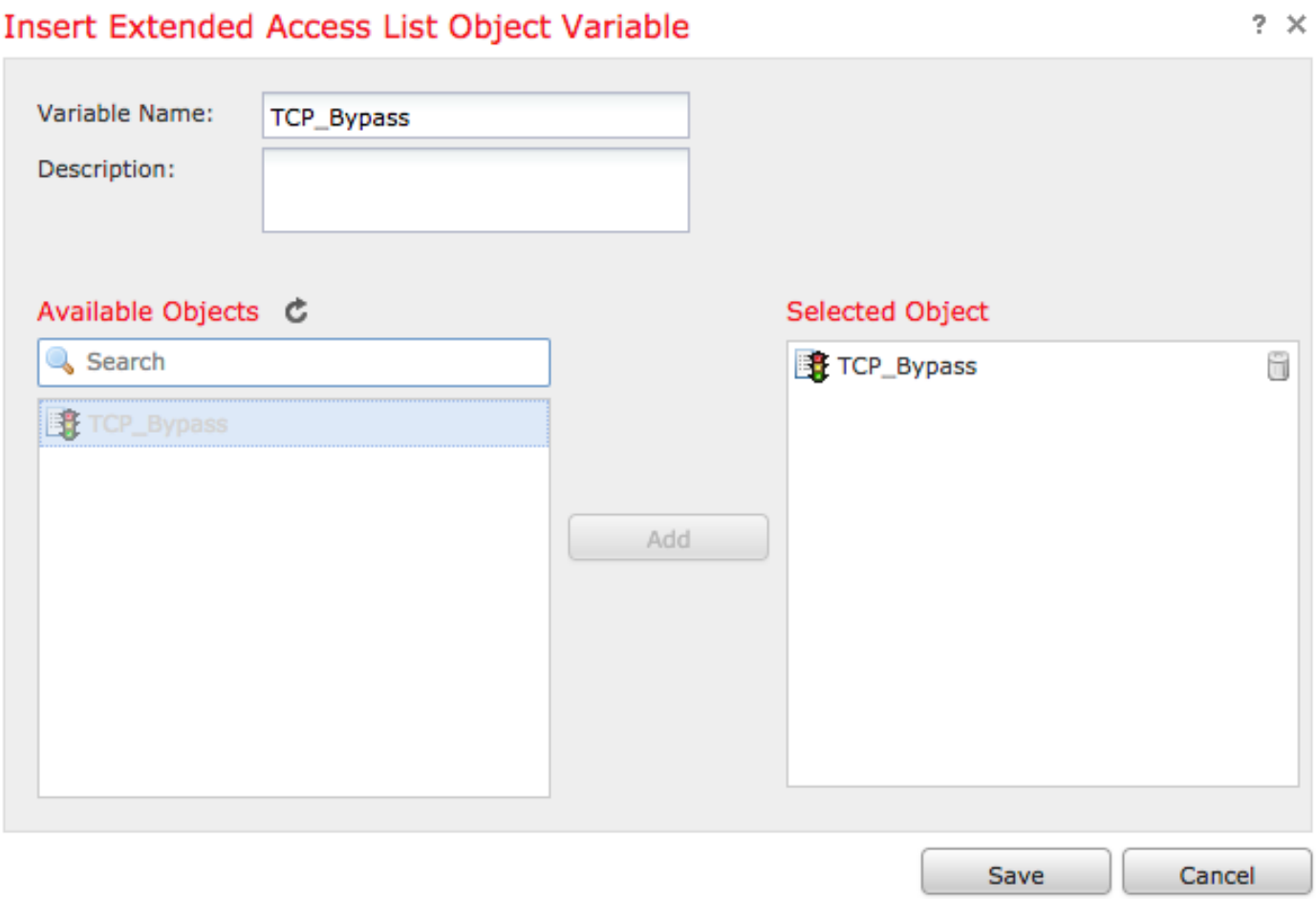
选择**插入策略对象>扩展ACL对象。**



注意：确保选择“Everytime”选项。这允许在其他部署和升级期间保留此配置。

从“可用对象”(Available Objects)部分选择在步骤1中创**建的访**问列表并分配变量名称。然后，单击“Add(添**加)”**按钮。在本例中，变量名称为**TCP_Bypass**。

单击“**Save(保存)”**。

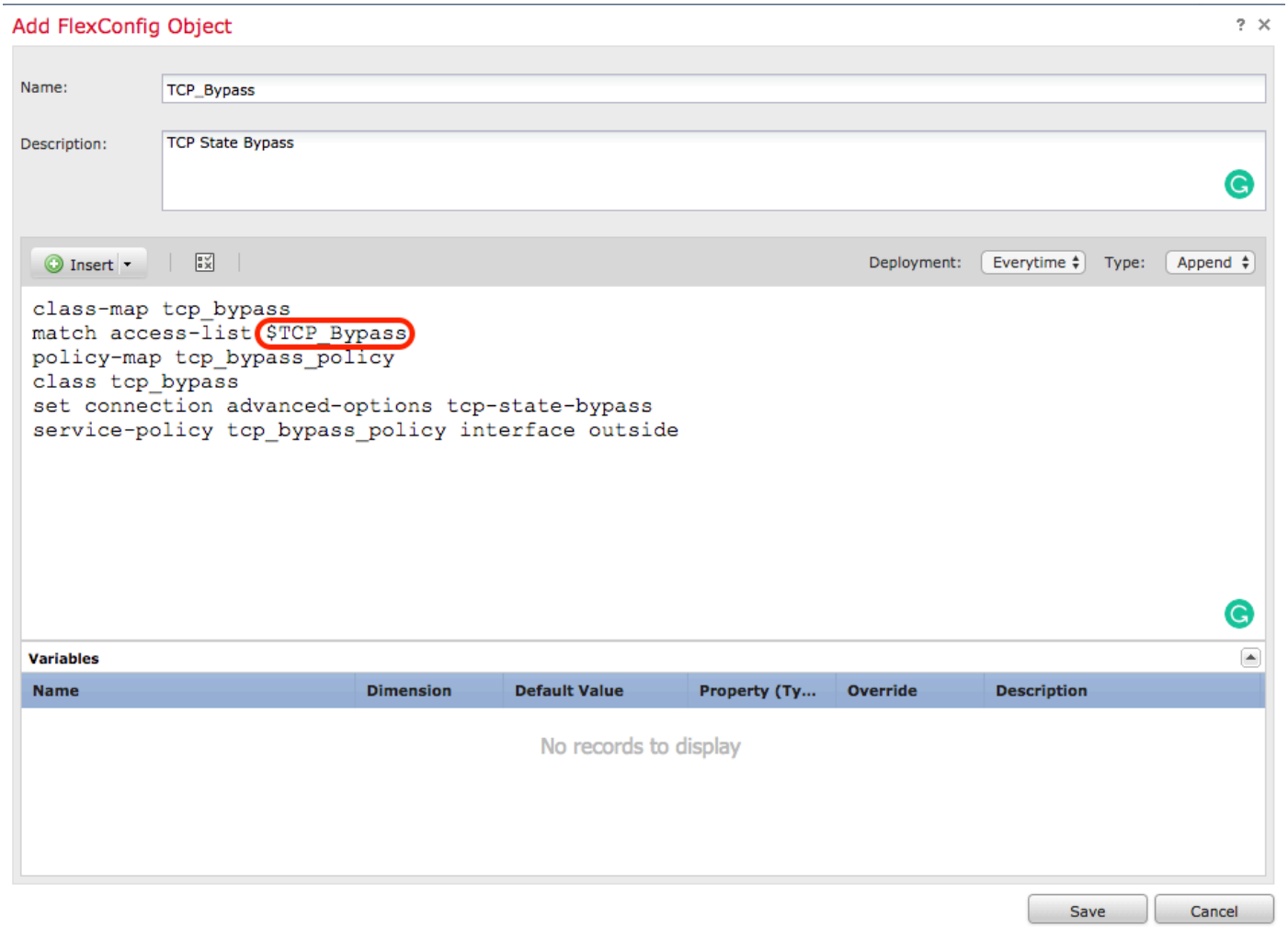


在空白字段中的“插入”按钮正下**方添**加下一行配置行，并在*match access-list*配置行中包含以前定义的变量(**$TCP_Bypass**)。请注意，**$**符号在变量名称前面。这有助于定义变量后跟。

```
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
```

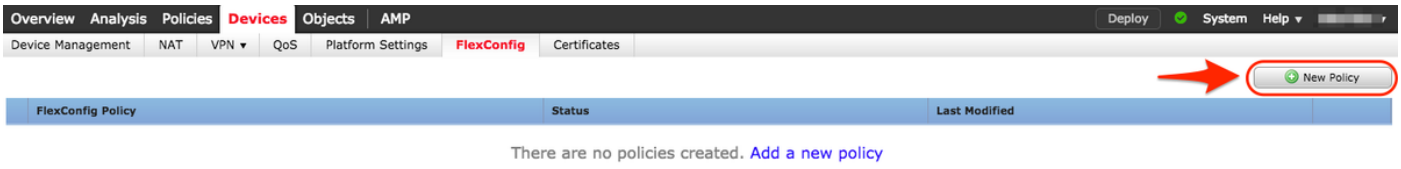
在本示例中，会创建策略映射并将其应用到外部接口。如果TCP状态绕行需要配置为全局服务策略的一部分，则tcp_bypass类映射可应用于global_policy。

完成后单**击“**保存”。

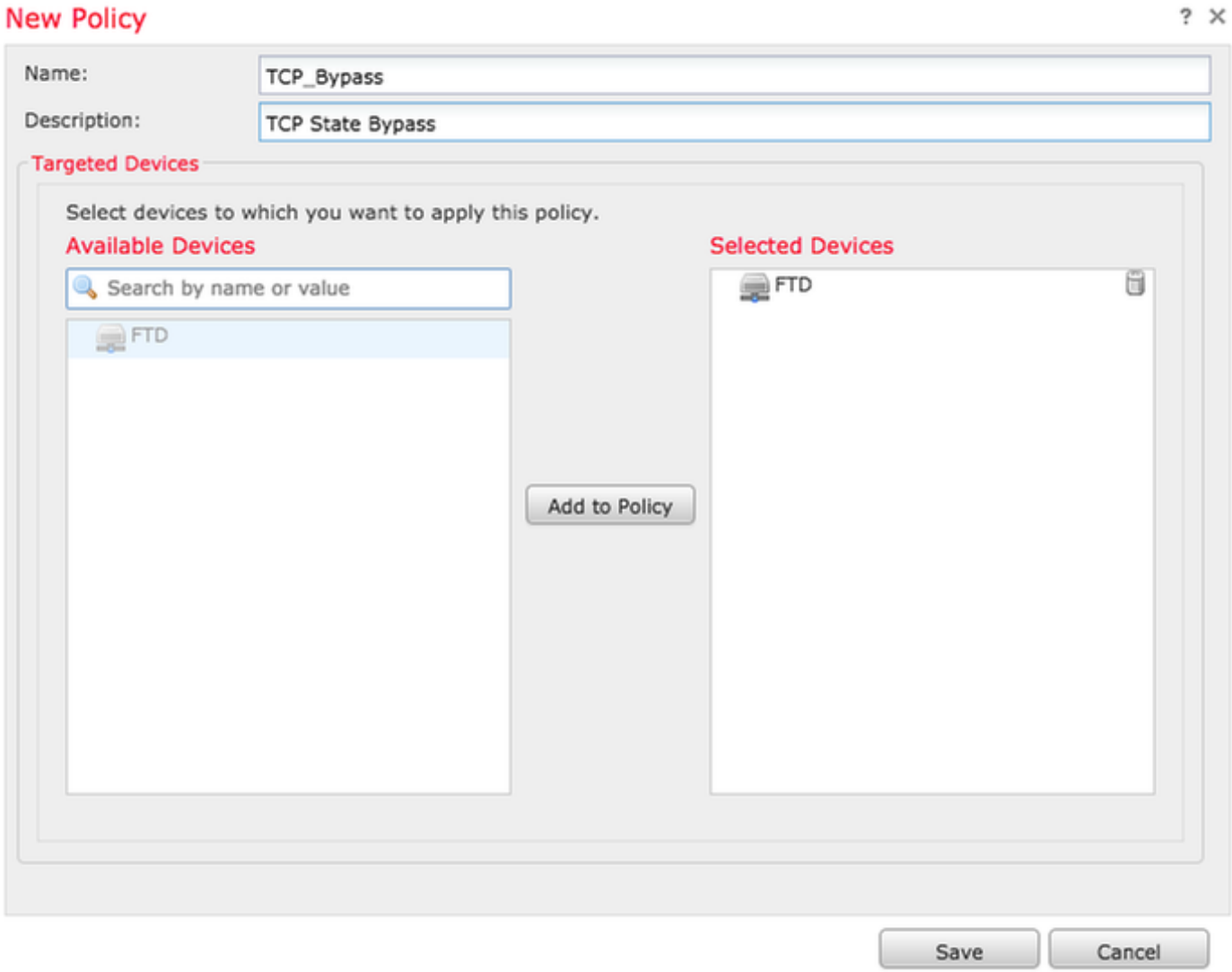


步骤3.为FTD分配FlexConfig策略

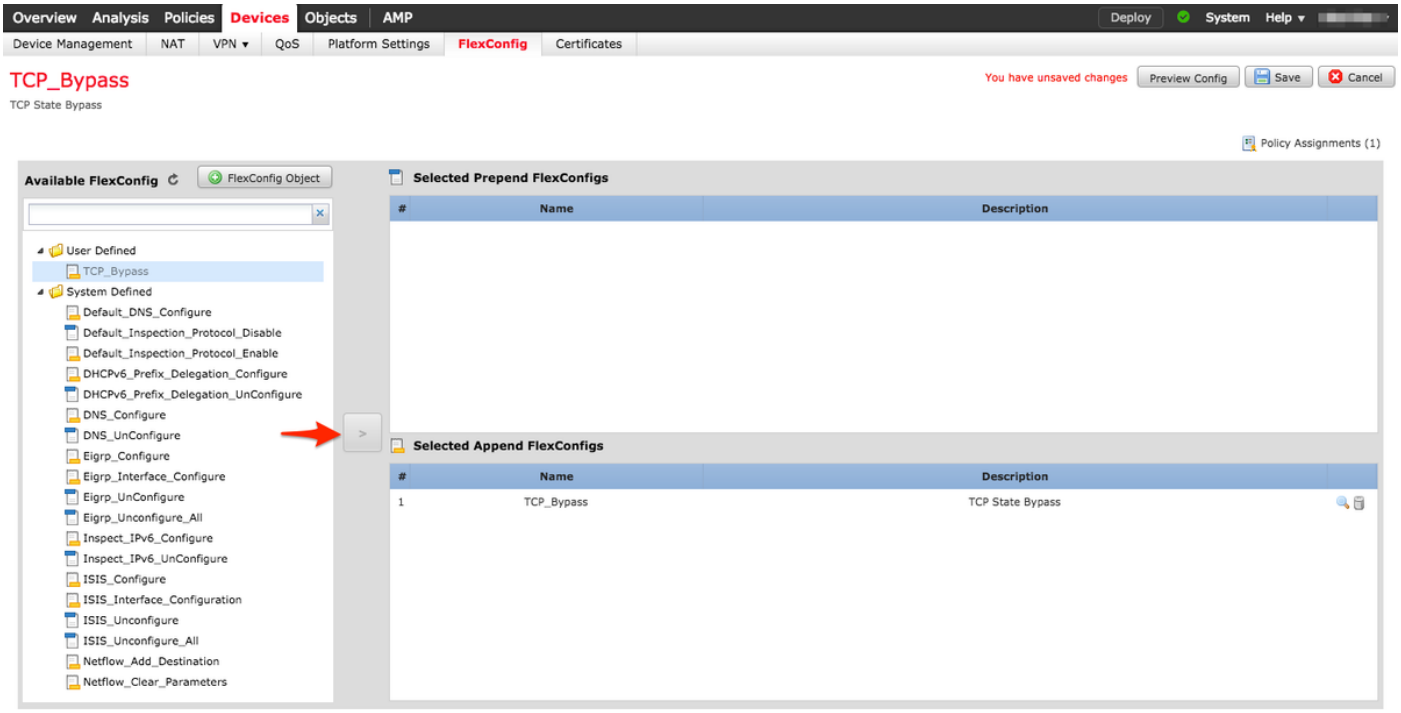
转到**Devices > FlexConfig**并创建新策略（除非已为其他用途创建策略并将其分配给同一FTD）。在本例中，新的FelxConfig策略称为**TCP_Bypass**。



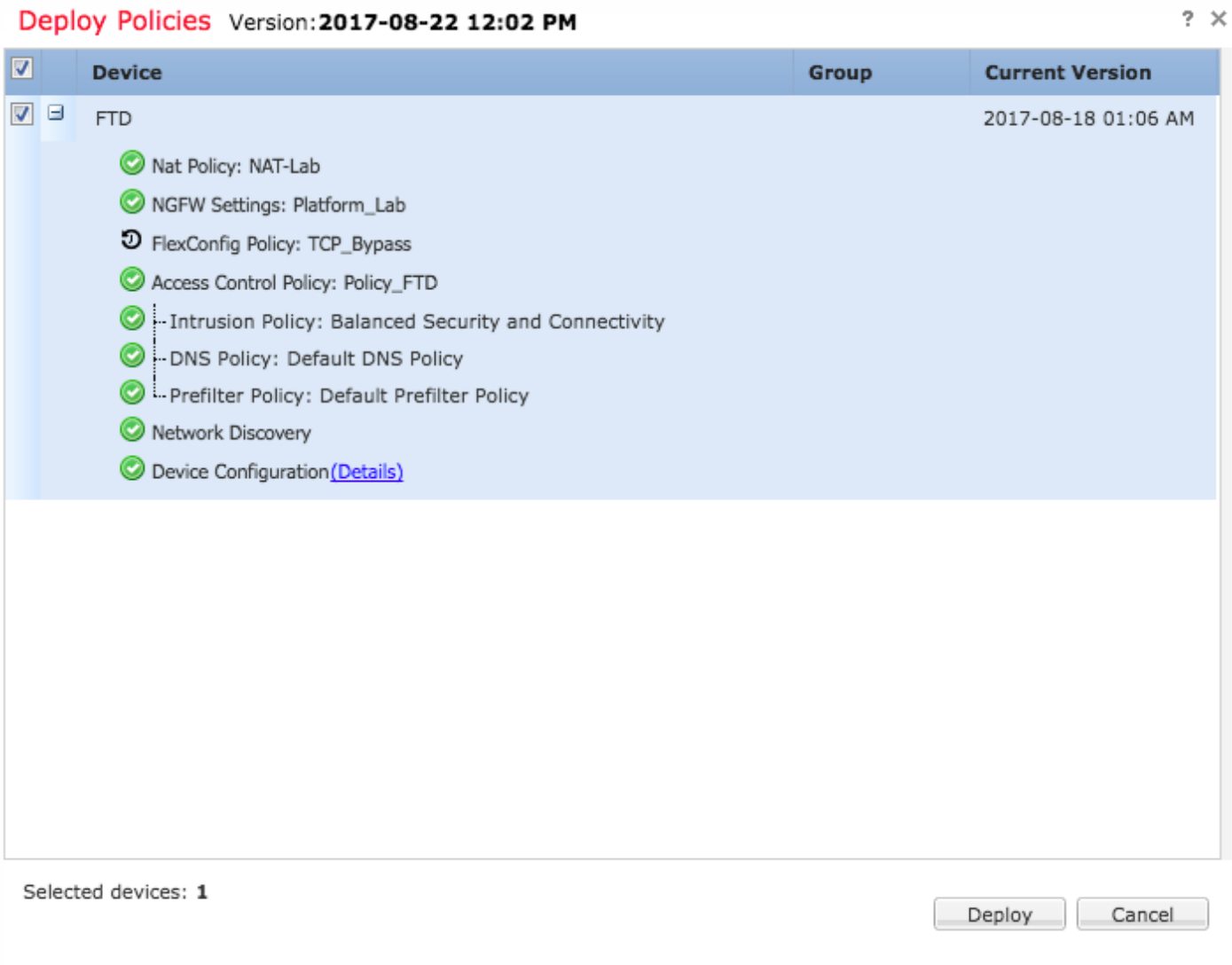
将TCP_**Bypass FlexConfig策**略分配给FTD设备。



选择在步骤2中“**用户定义**”部分下创建的名为**TCP_Bypass的**FlexConfig对象，然后单击箭头将该对象添加到策略。



保存更改并部署，



确认

通过SSH或控制台访问FTD，并使用命令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
!
```

故障排除

要排除此功能故障，这些命令会有所帮助。

- 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

相关链接

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