使用预定义模板在FTD上配置并排除WCCP故障

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 运行原理
- 网络图
- 配置

验证

故障排除

简介

本文档介绍FTD上WCCP的配置和故障排除步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Web缓存通信协议(WCCP)第2版(v2)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙管理中心(FMCv)v7.4.2
- 安全防火墙威胁防御虚拟(FTDv)v7.4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

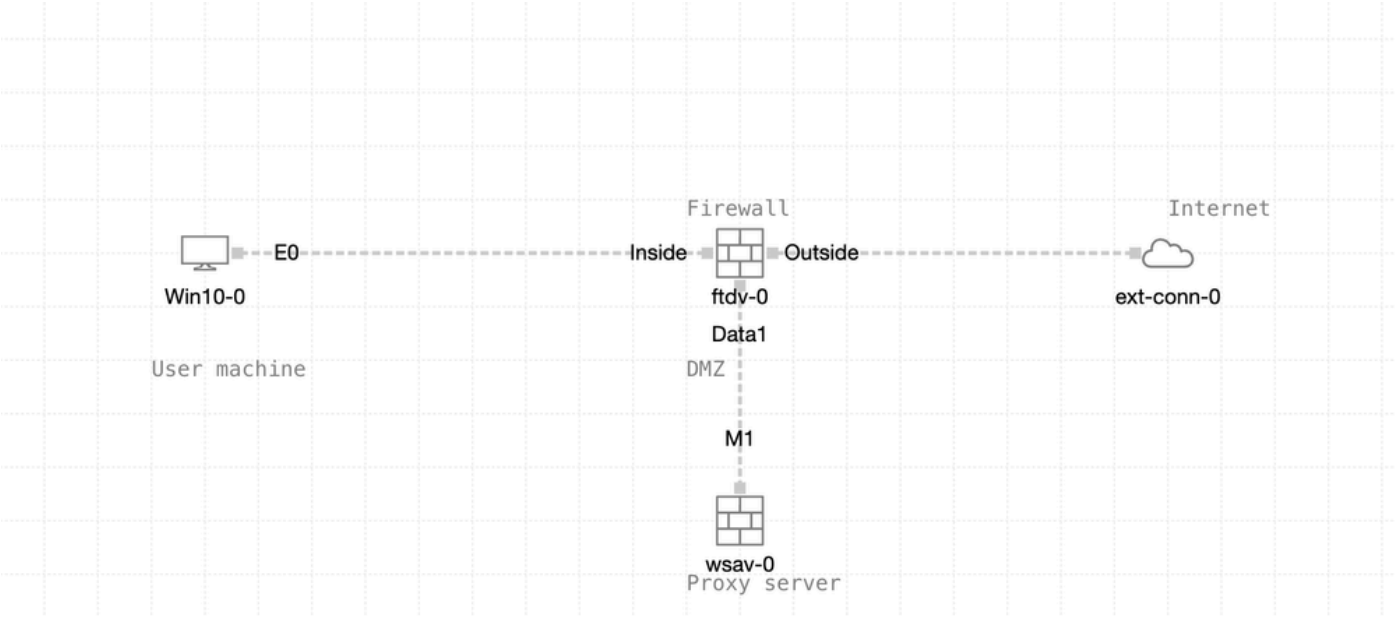
Web缓存通信协议(WCCP)用于将网络流量重定向到缓存服务器。通常在网络设备（例如Cisco路由器和防火墙）中实施，将HTTP、HTTS和FTD over HTTP请求重定向到代理服务器。

WCCP有不同的版本，包括WCCP v1、v2和v3，每个版本都提供增强的功能和可扩展性。

运行原理

- 用户计算机Win10-0发出HTTPS请求。
- 此处，FTD防火墙是用户PC的网关。接收HTTP/HTTPS请求。
- FTD了解目标端口为443，并将流量重定向至DMZ
- DMZ使用GRE封装数据包，并将请求转发到代理服务器。
- 代理服务器会查看其缓存或发起到原始服务器的新连接，并直接对用户机器做出响应。

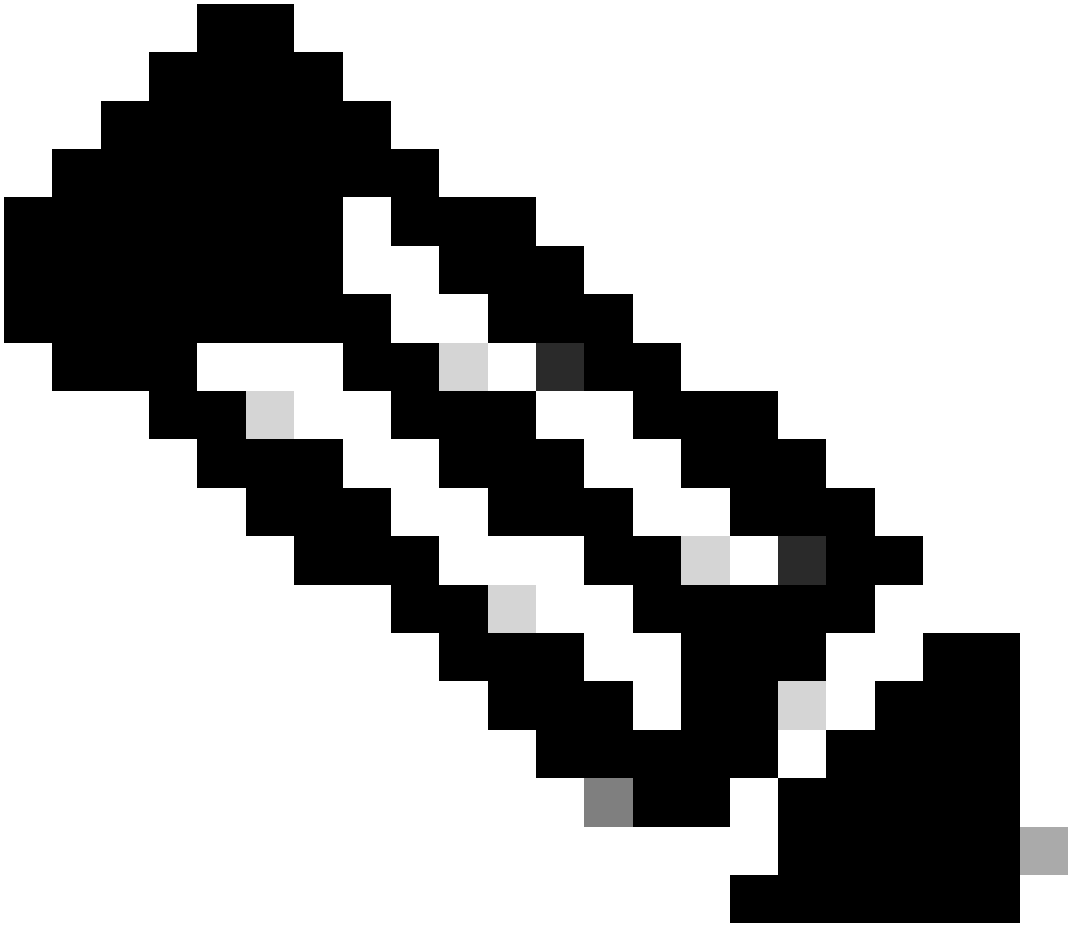
网络图



网络拓扑

配置

以下步骤演示了FMC上的WCCP配置。具有端口80和443的流量必须从Inside区域重定向到DMZ区域。

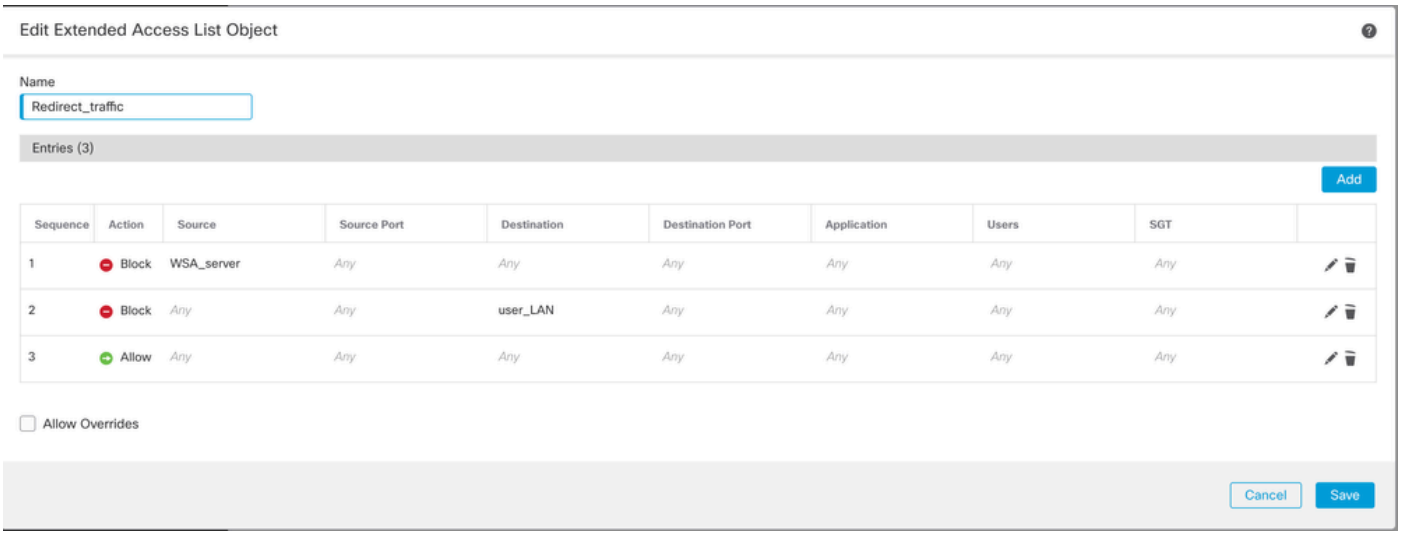


注意：本文档介绍动态服务ID的步骤。端口信息已从WCCP客户端获取。

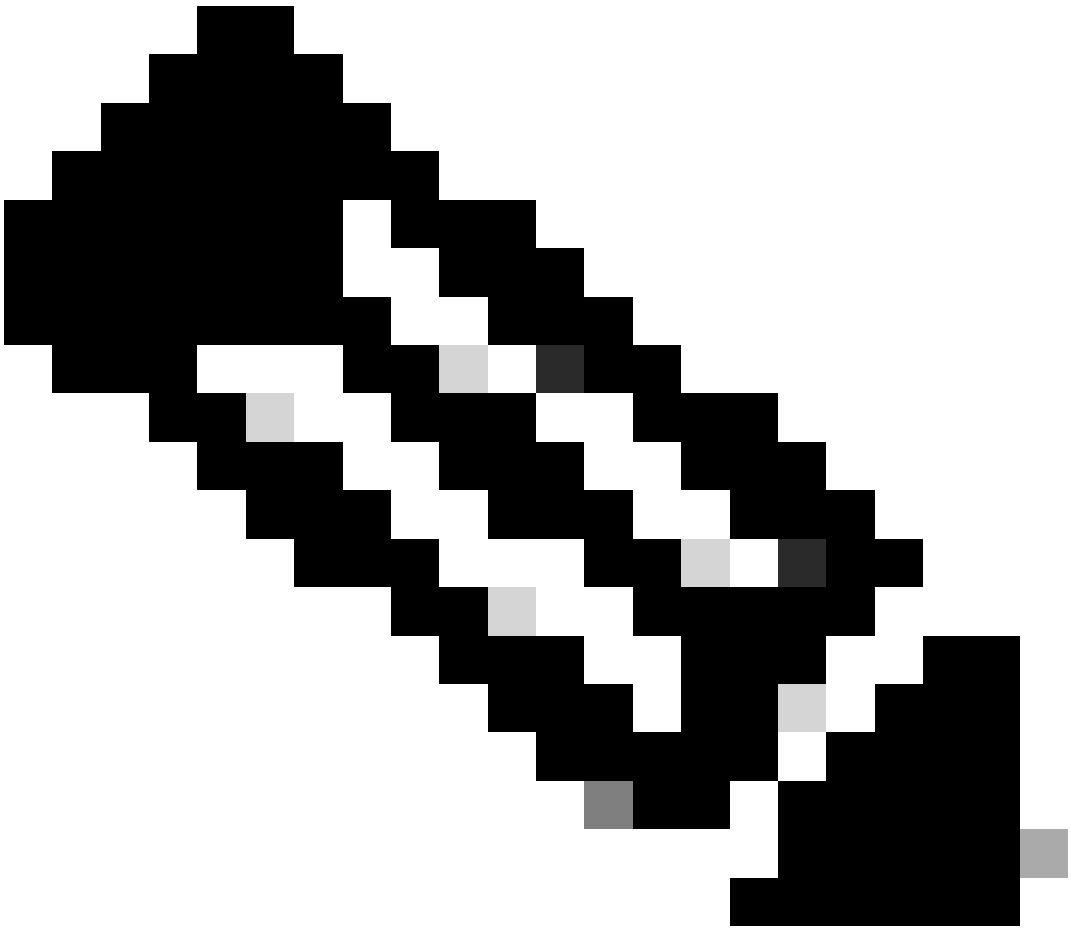
步骤 1：登录到FMC GUI，然后导航到对象(Object)>对象管理(Object Management)>访问列表(Access List)>扩展(Extended)>添加扩展访问列表(Add Extended Access List)。

创建两个扩展访问列表。

1)创建访问列表以重定向用户流量，然后点击保存。



重定向用户流量

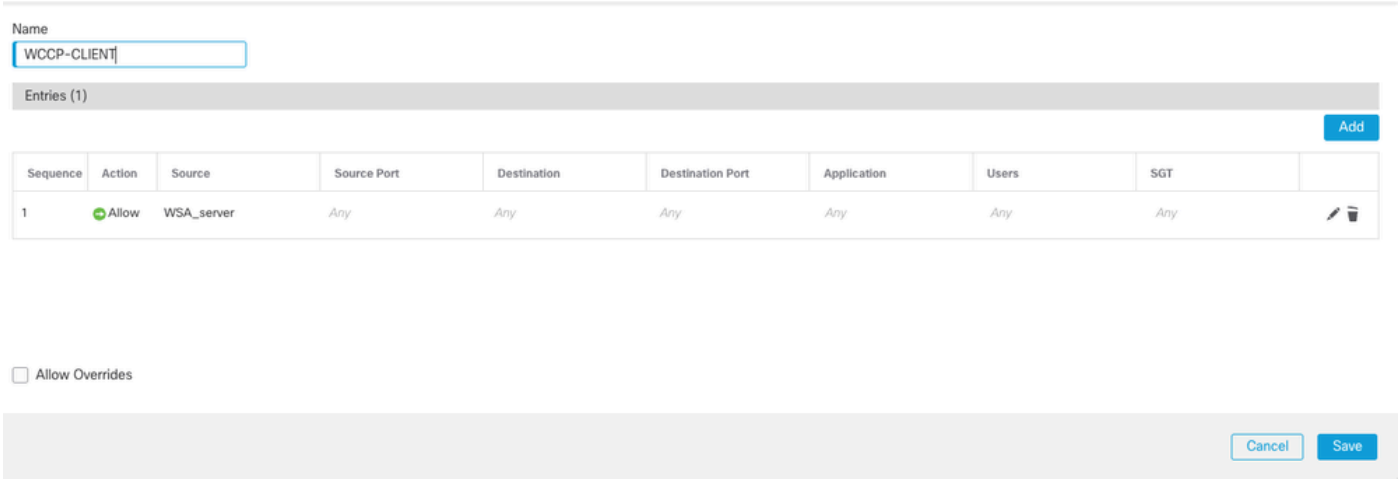


注意：此访问列表可确保您拥有从WCCP客户端流向FTD的流量的Action Block，以避免网络中出现环路。

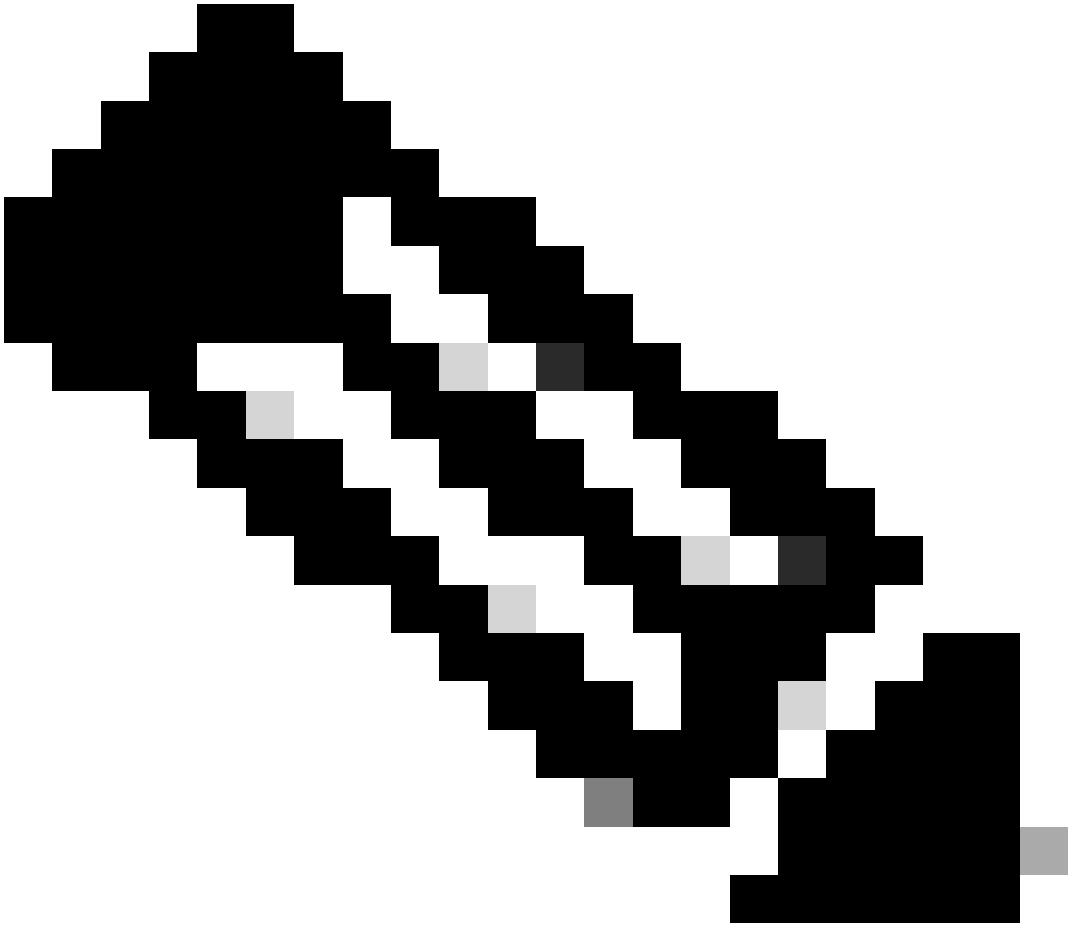
此外，还可以使用Action Block创建另一条语句，以确保内部主机之间的通信不会发送到代理服务器。

最终语句必须允许符合重定向到代理条件的所有其他流量。

2)创建访问列表以标识WCCP客户端，然后单击Save。

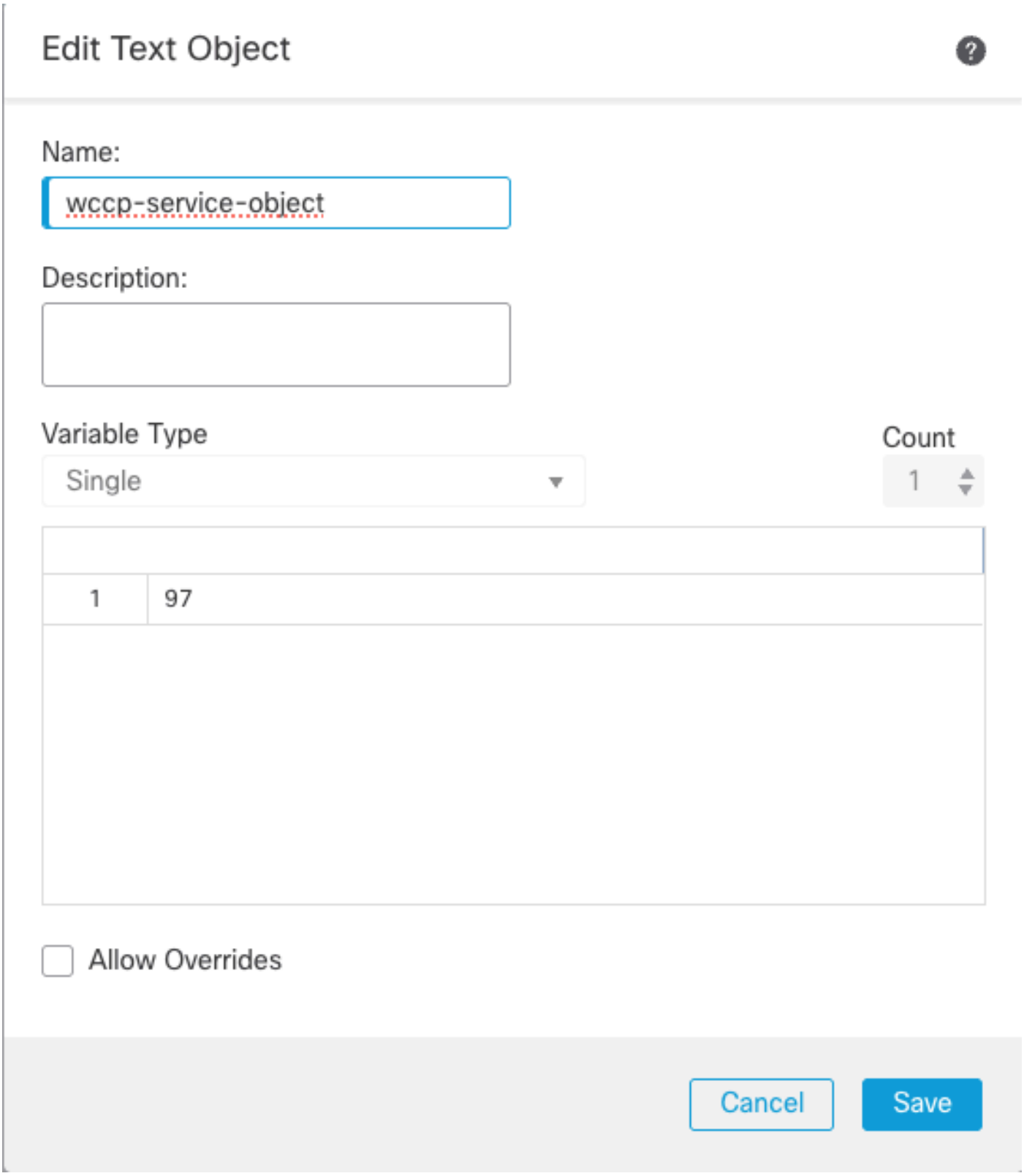


用于标识WCCP客户端的访问列表

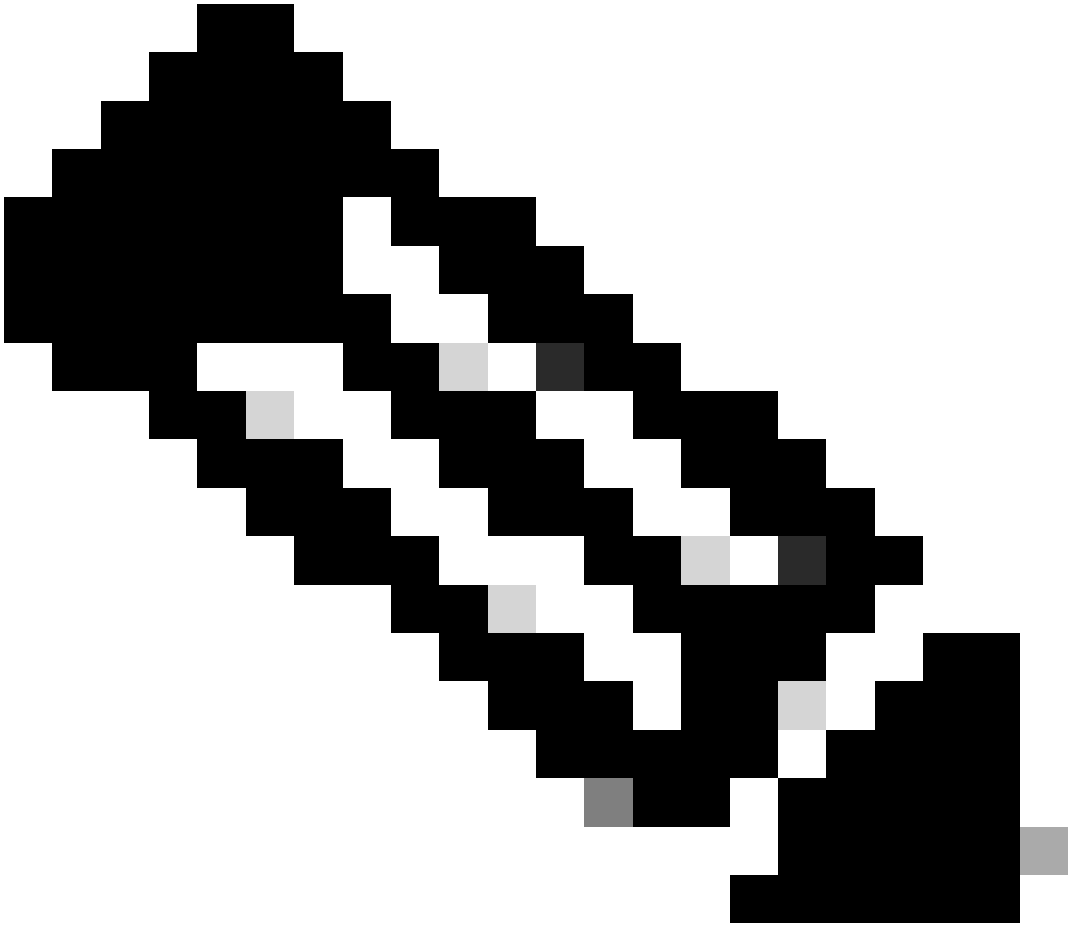


注意：配置扩展访问列表以包括WCCP服务器的IP地址。

第2步：导航到对象(Object)>对象管理(Object Management)> FlexConfig >文本对象(Text Object)>添加文本对象(Add Text Object)，以添加WCCP服务并保存(Save)。


Edit Text Object
Name:
wccp-service-object
Description:
Variable Type
Single
Count
1
1
97
Allow Overrides
Cancel
Save

创建wccp服务对象

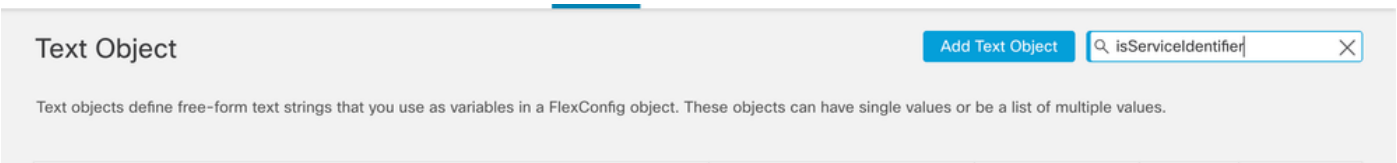


注意：在本示例中，服务ID为97。建议选择介于90和97之间的服务ID，因为这些是通常与分配给特定协议的其他服务ID不冲突的自定义服务ID。

有关详细信息，请参阅ASA上的WCCP:概念、限制和配置

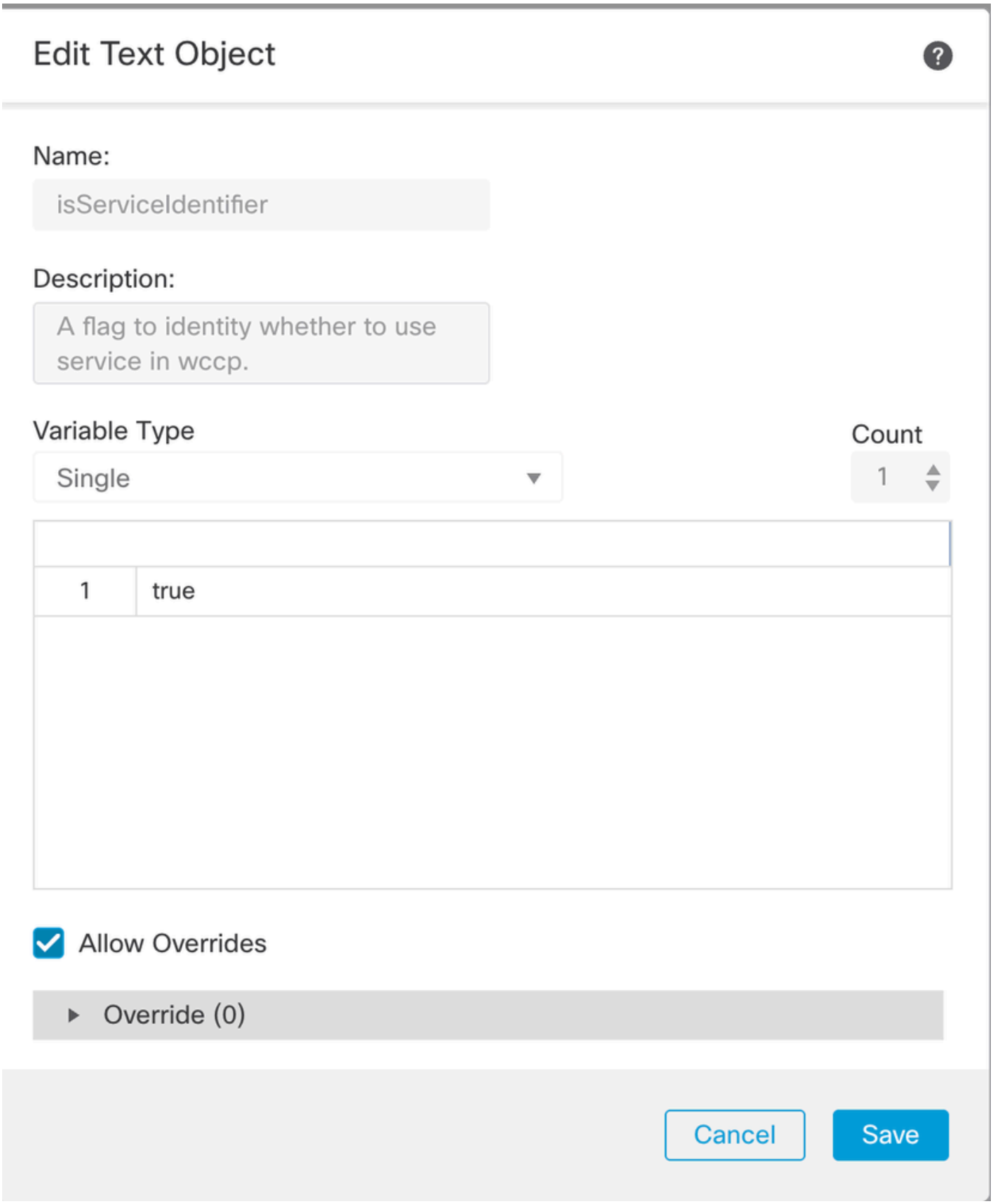
步骤 3：

- 导航到对象>对象管理> FlexConfig >文本对象，并搜索isServiceIdentifer。

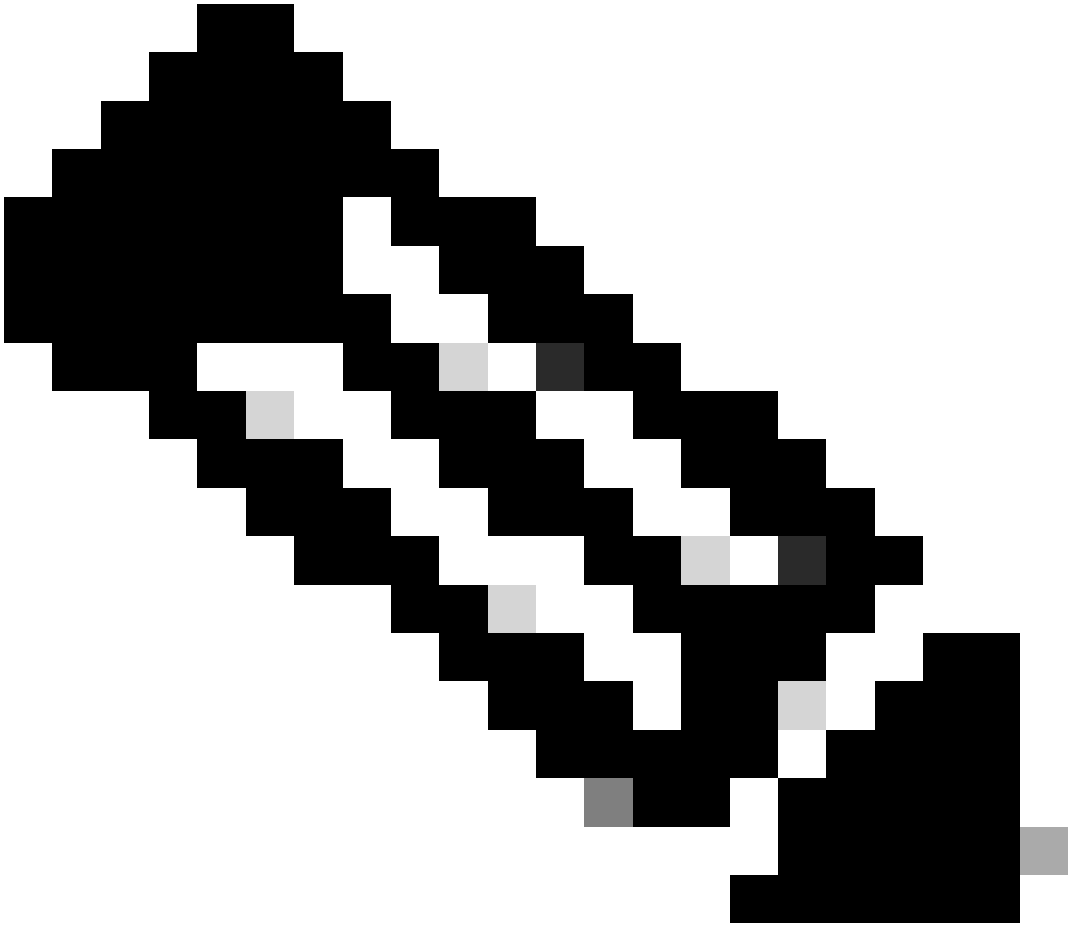


为isServiceIdentifer搜索

- 将isServiceIdentifer从false修改为true。
- isServiceIdentifer -如果为false，则使用standard web-cacheservice标识符。请参阅文档



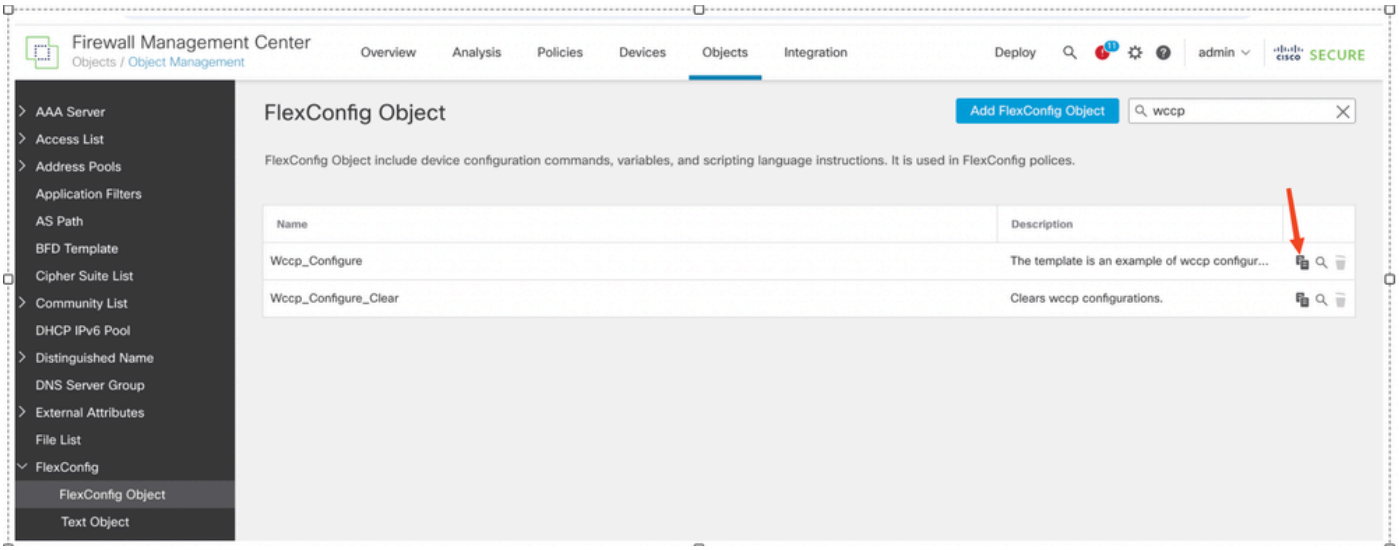
将值从false修改为true



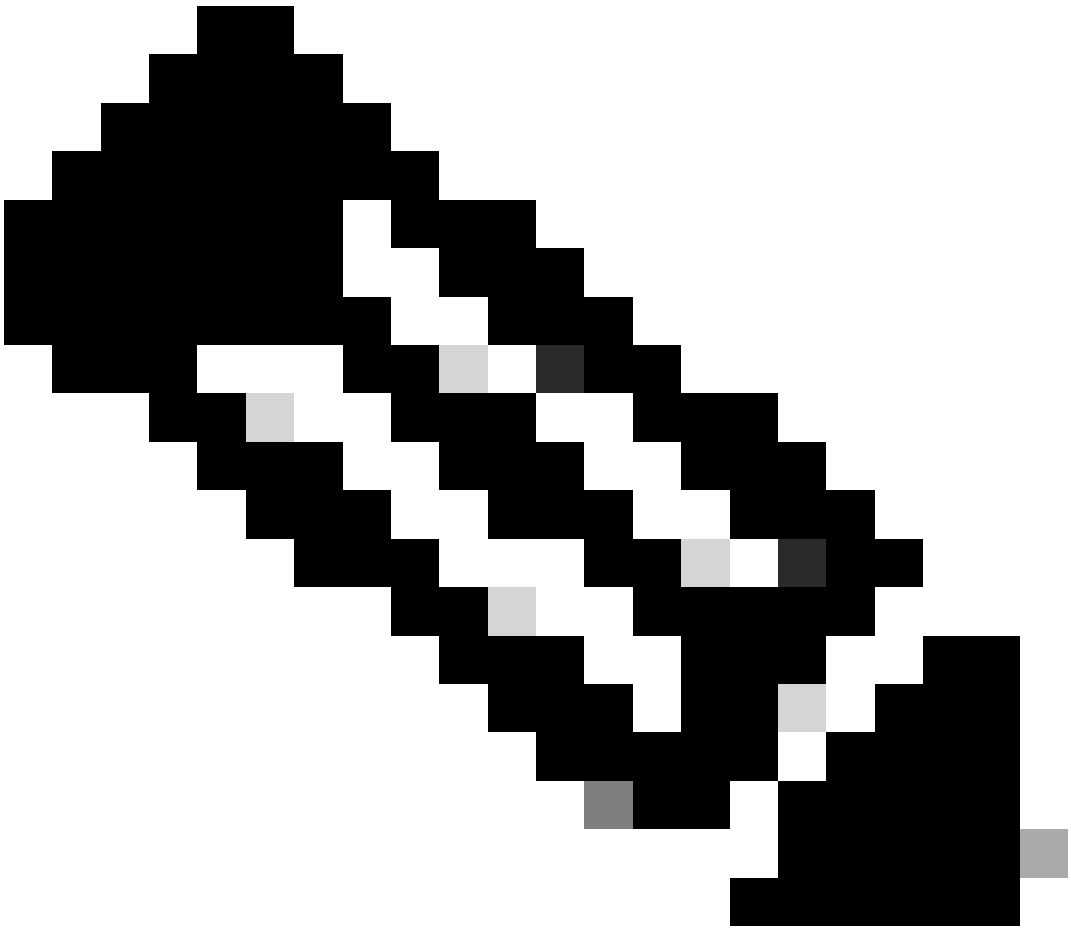
注意：此外，您可以创建用户定义的文本对象，如步骤2所示。

步骤 4：

- 导航到对象>对象管理> Flex配置> FlexConfig对象。
- 搜索关键字wccp。
- 单击Wccp_Configure模板的Clone选项。



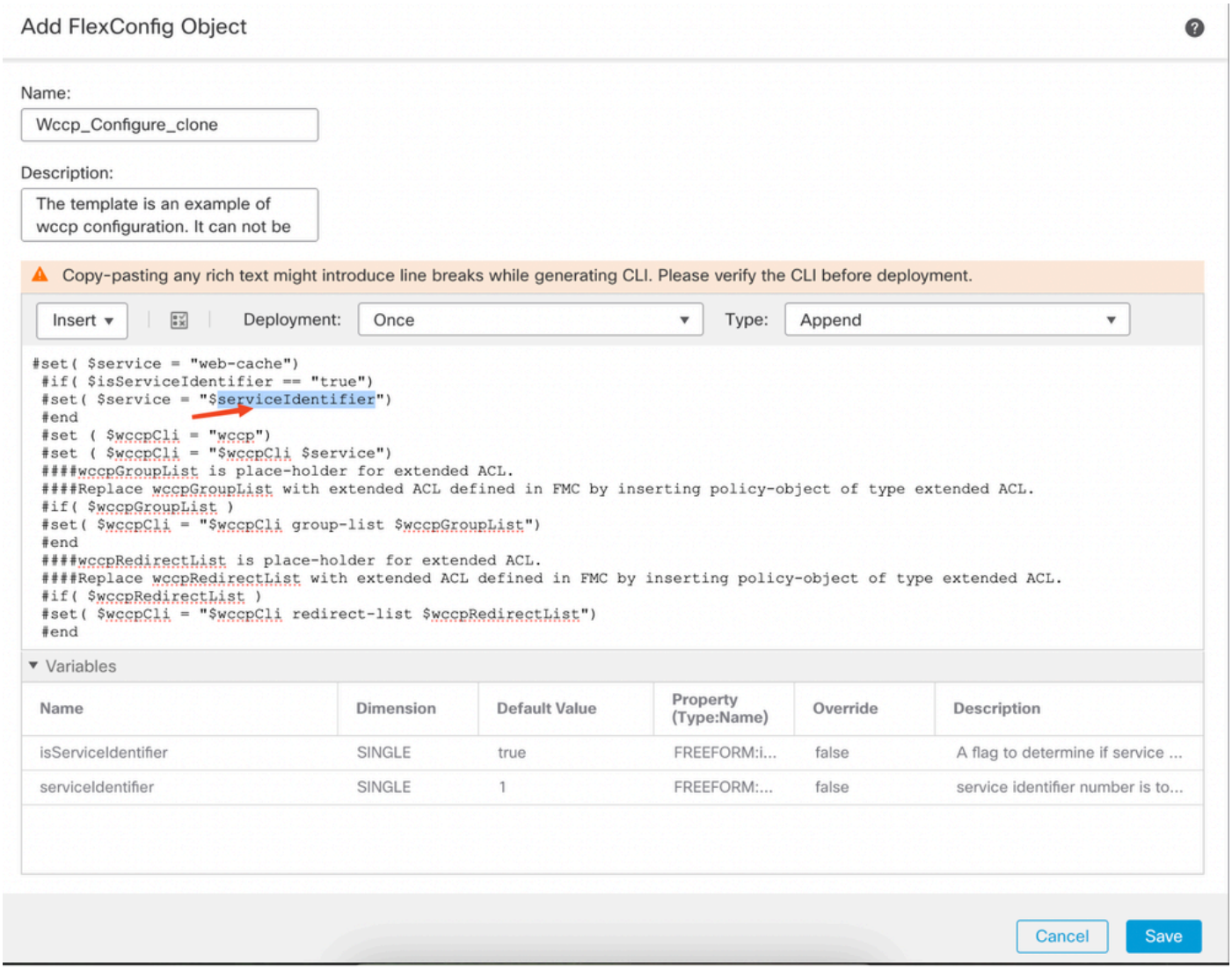
克隆wccp_configure模板



注意：FlexConfig对象有一个预定义的模板：Wccp_Configure。无法将模板附加到设备。您必须克隆它。

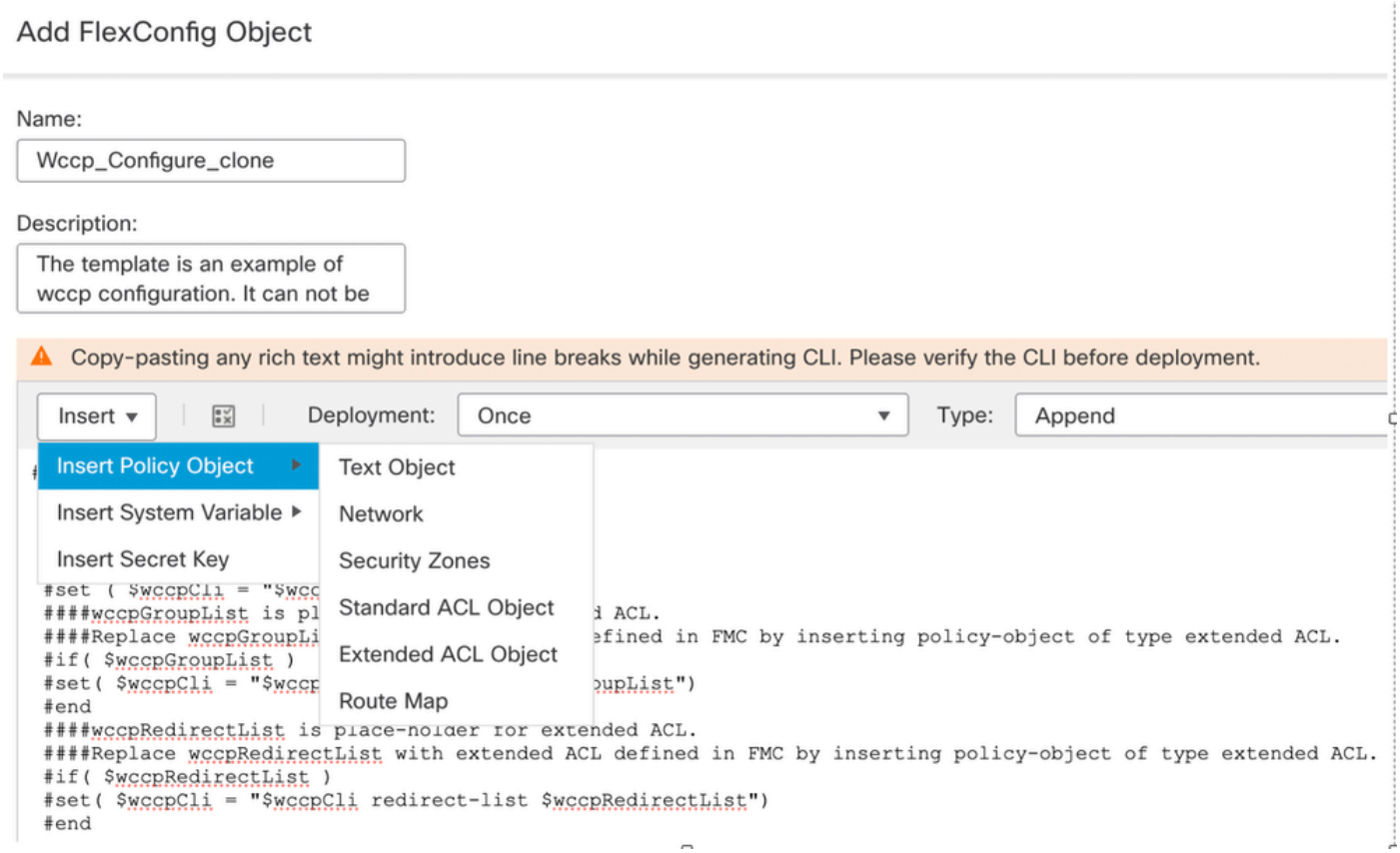
步骤 5：

- 从第三行删除$serviceIdentifier变量并提供您自己的变量。



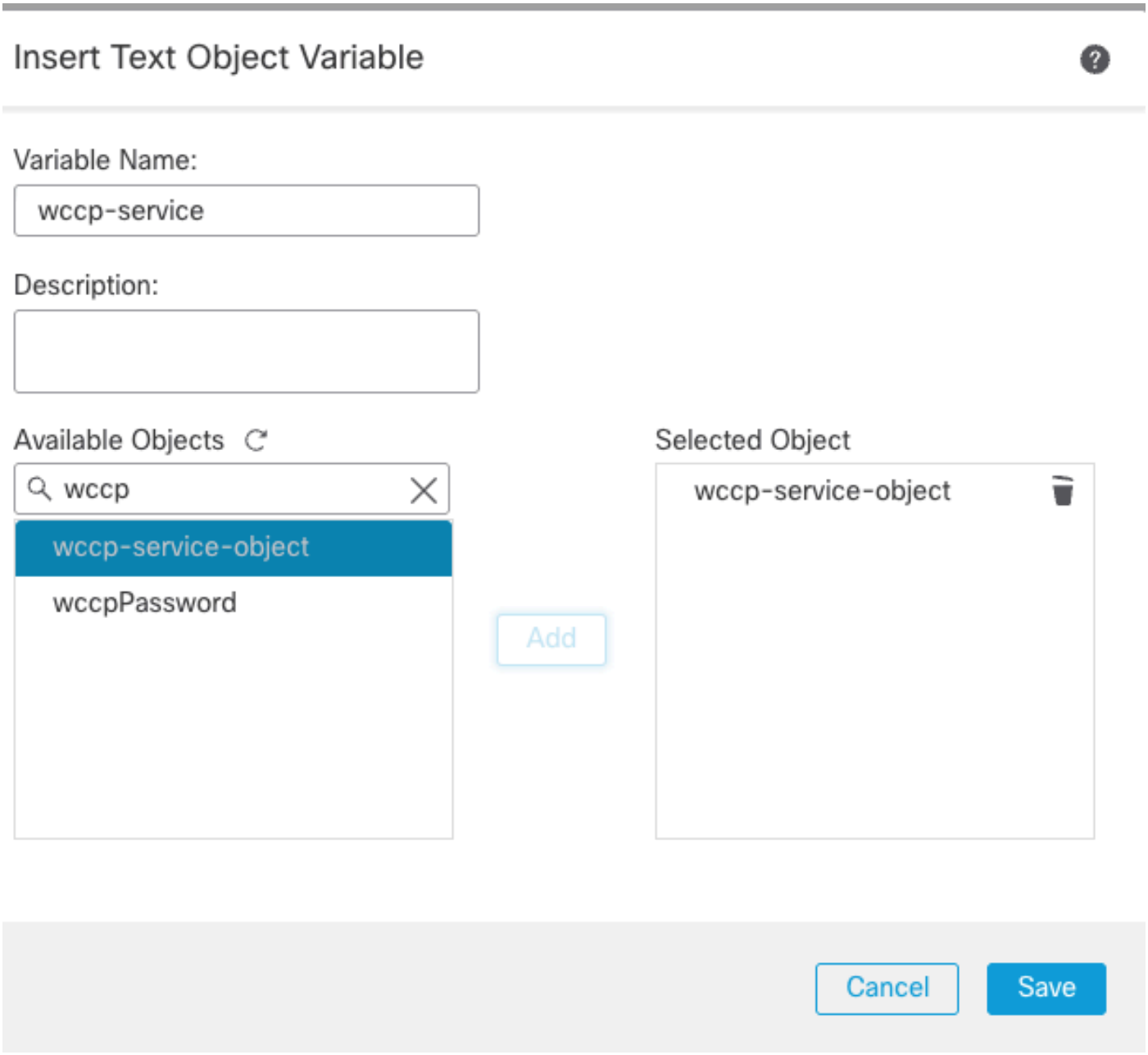
删除服务标识符

- 将Text Objectwccp-service插入为步骤2中创建的变量。
- 从下拉菜单中，选择插入>插入策略对象>文本对象



将wccp-service对象作为变量插入

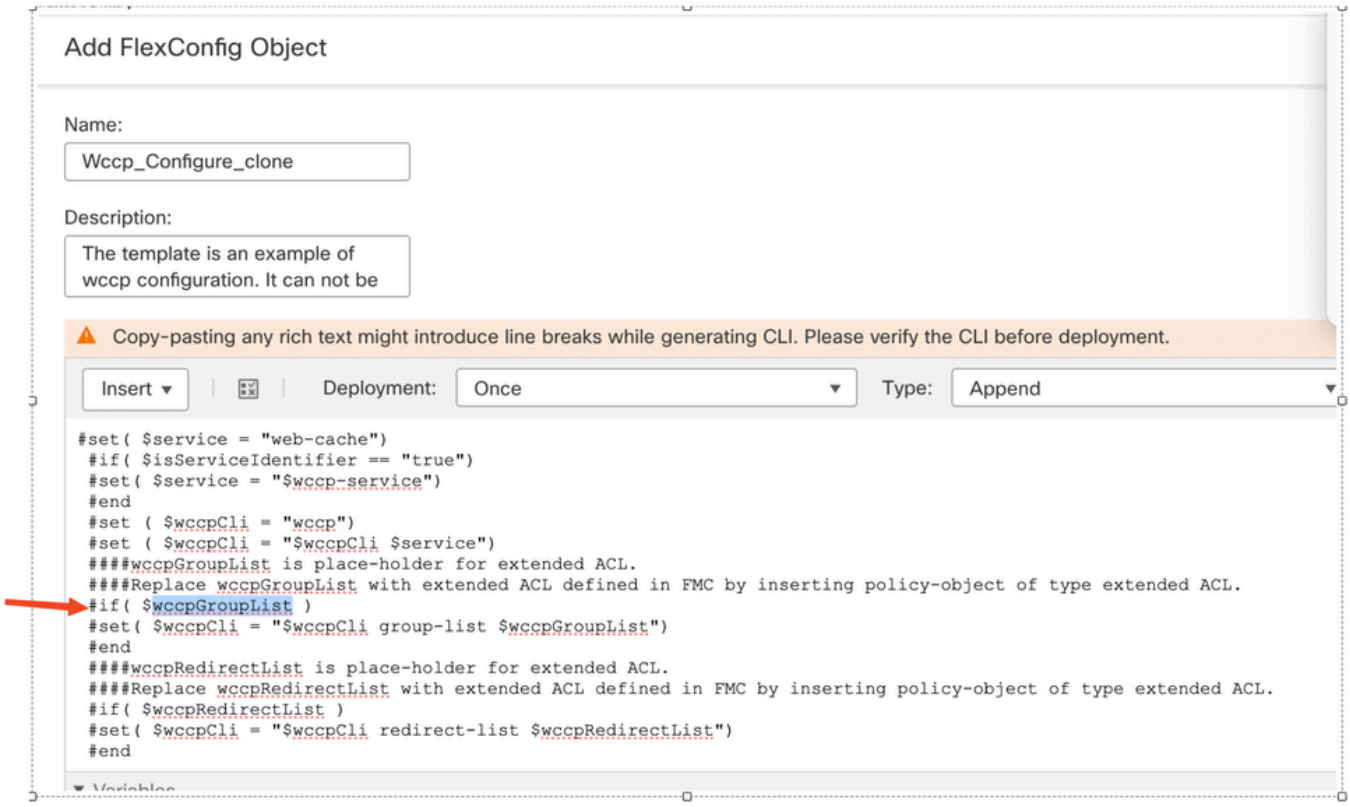
- 提供变量Namewccp-service。
- 在Available Object中搜索wccp-service-object。
- 添加对象并保存。



添加*wccp-service*对象

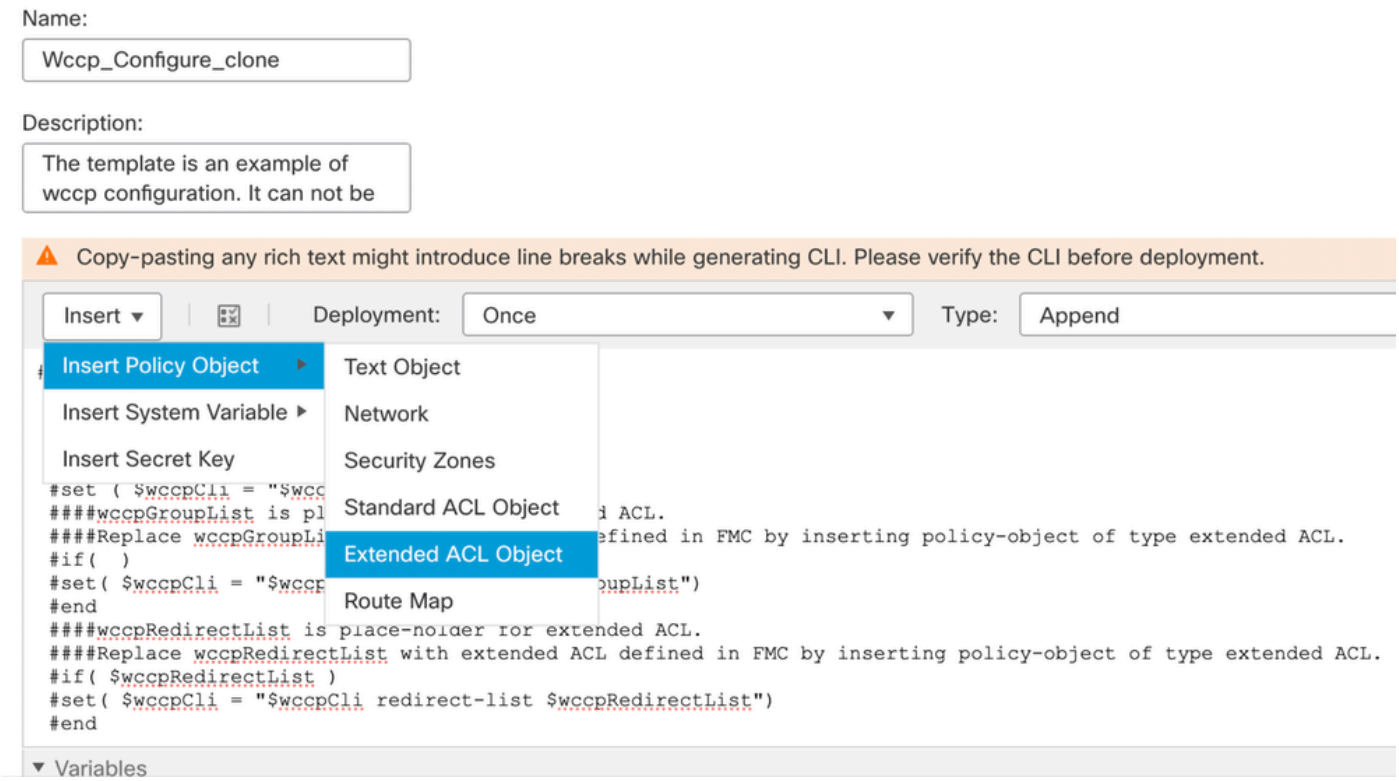
步骤 6：

- 复制wccpGroupList变量名称，并提供您自己的变量。



删除预定义的wccpGroupList变量

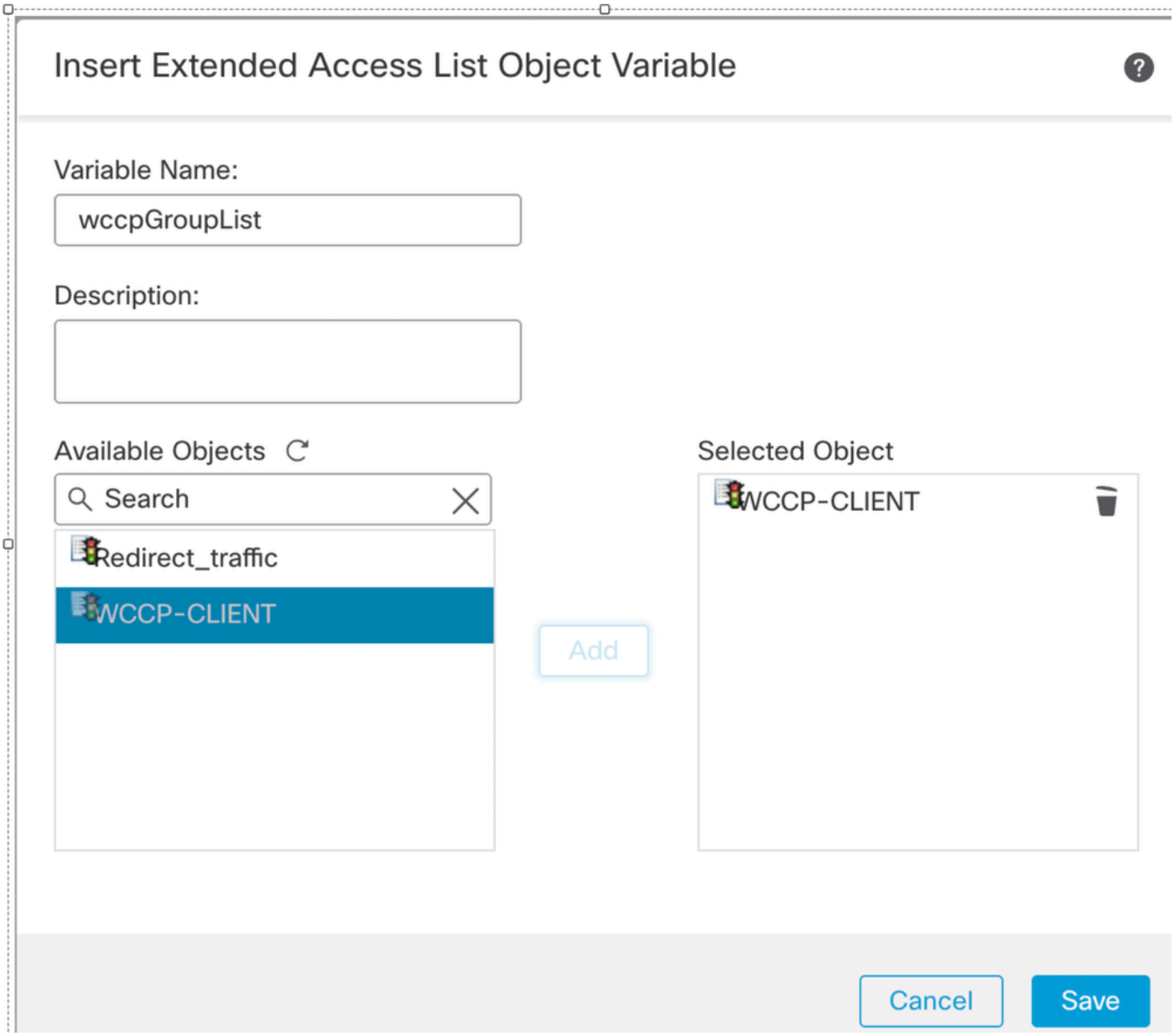
- 从下拉菜单Insert > Insert Policy Object > Extended ACL Object。



添加*wccpGrouplist*扩展*ACL*

- 将上一步中复制的名称wccpGroupList粘贴到变量名部分。

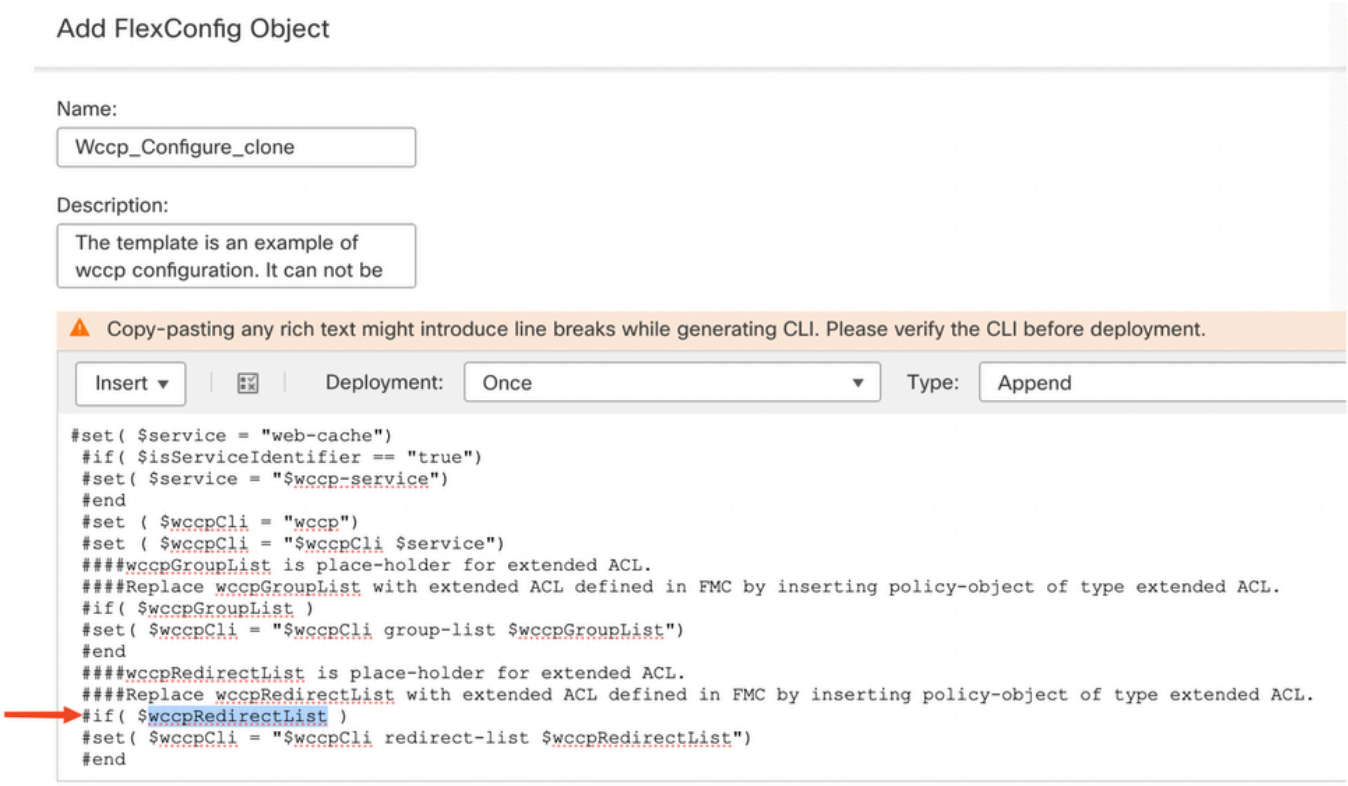
- 在步骤1中创建的可用对象中搜索WCCP-CLIENT。
- 添加并保存它。



添加*WCCP*客户端扩展列表

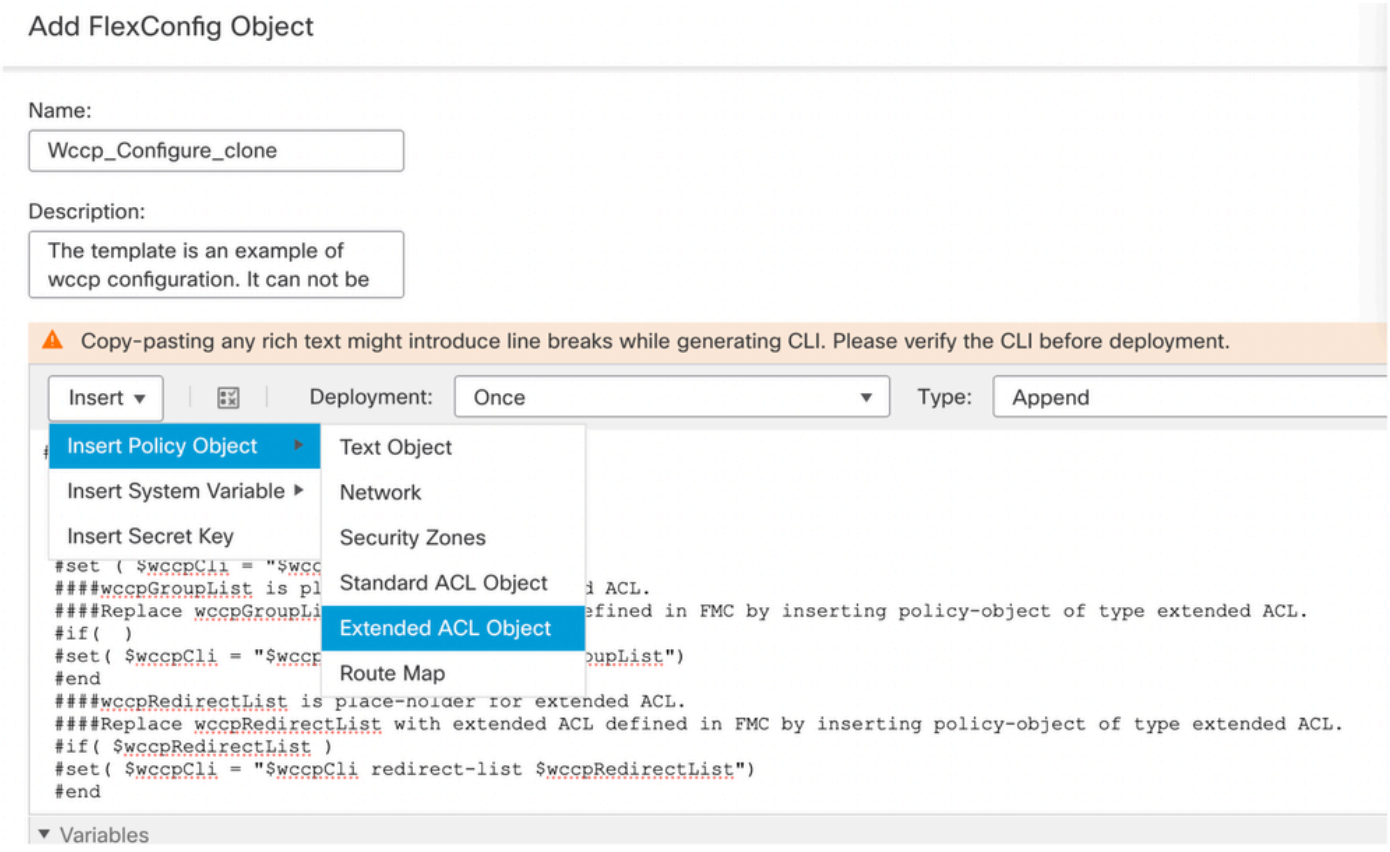
步骤 7：

- 选择wccpRedirectList以复制和提供您自己的变量。



删除*wccpRedirectList*

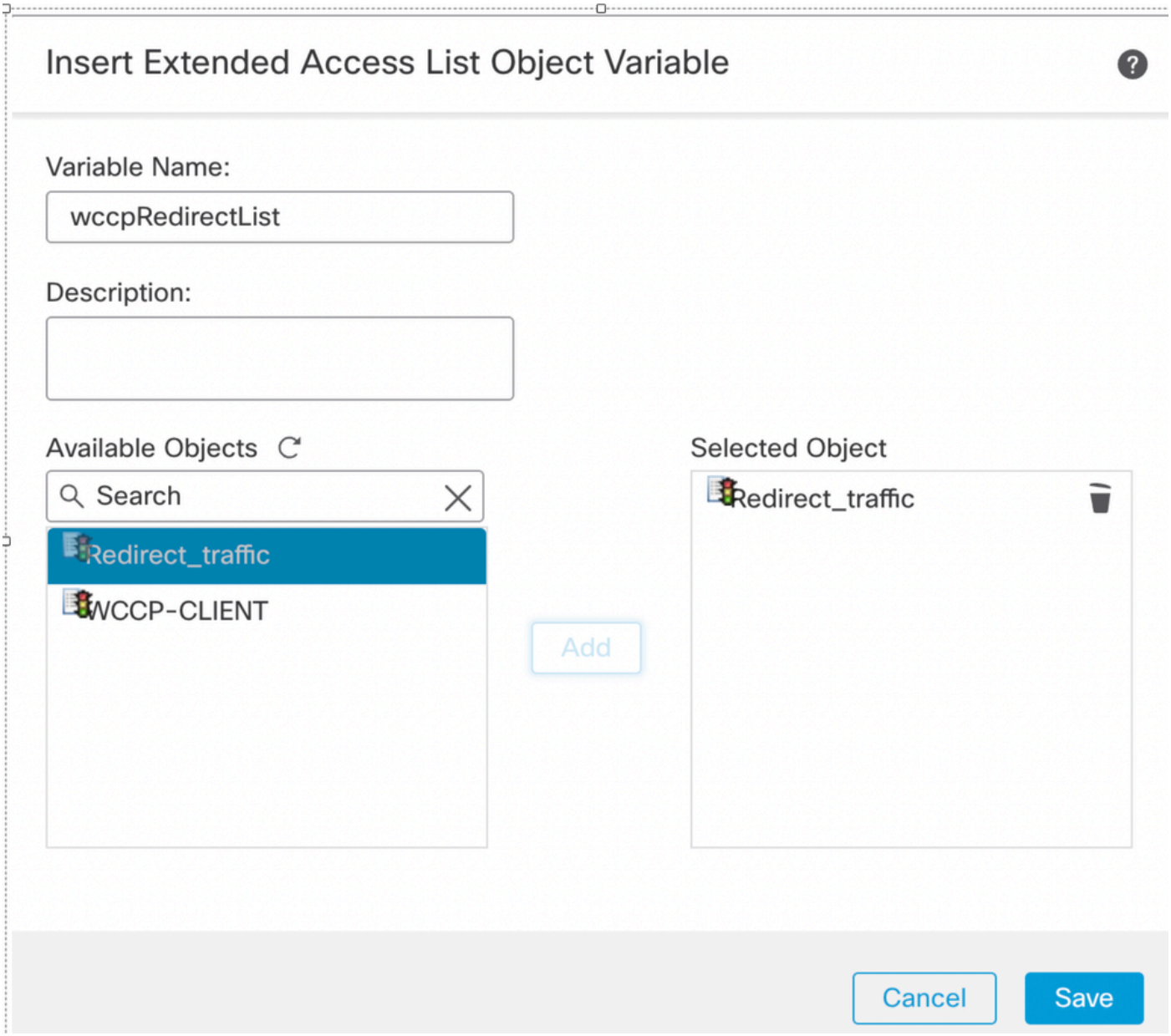
- 从下拉菜单中，选择插入>插入策略对象>扩展ACL对象。



为wccpRedirectList选择扩展ACL对象

- 将wccpRedirectList粘贴到变量名称。

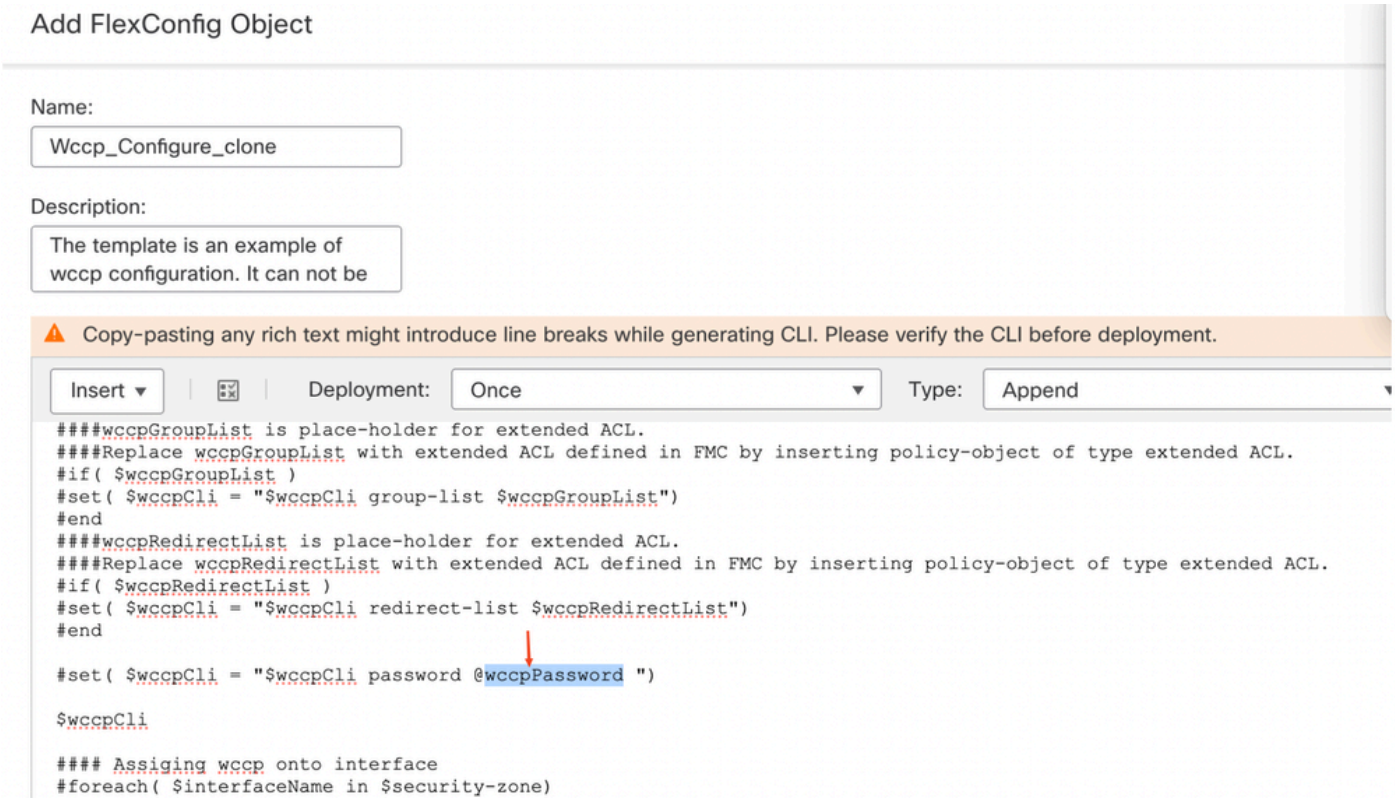
- 在可用对象中搜索Redirect_traffic。
- 选择Add并Save。



添加Redirect_traffic ACL

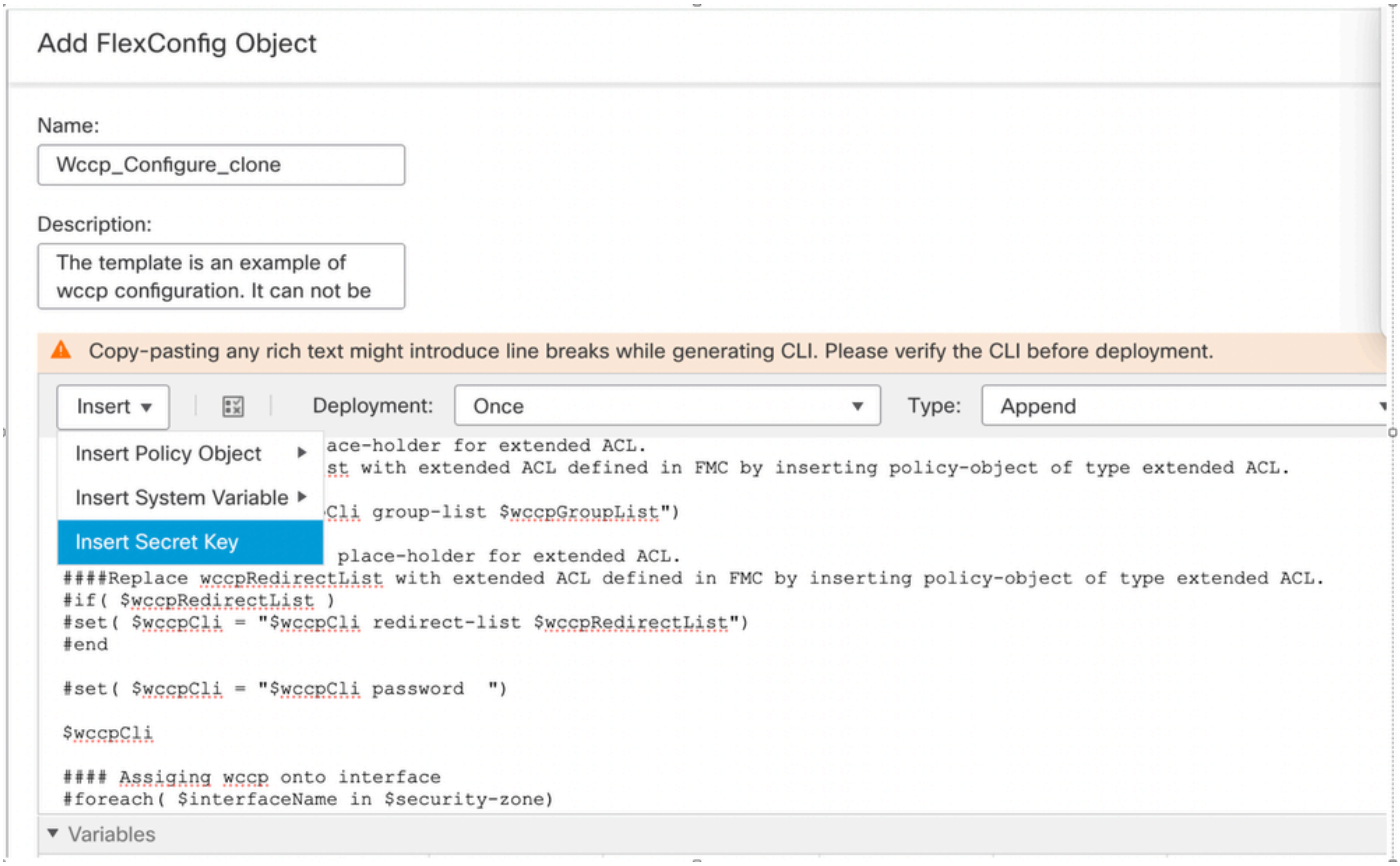
步骤 8::

- 删除**@wccpPassword**



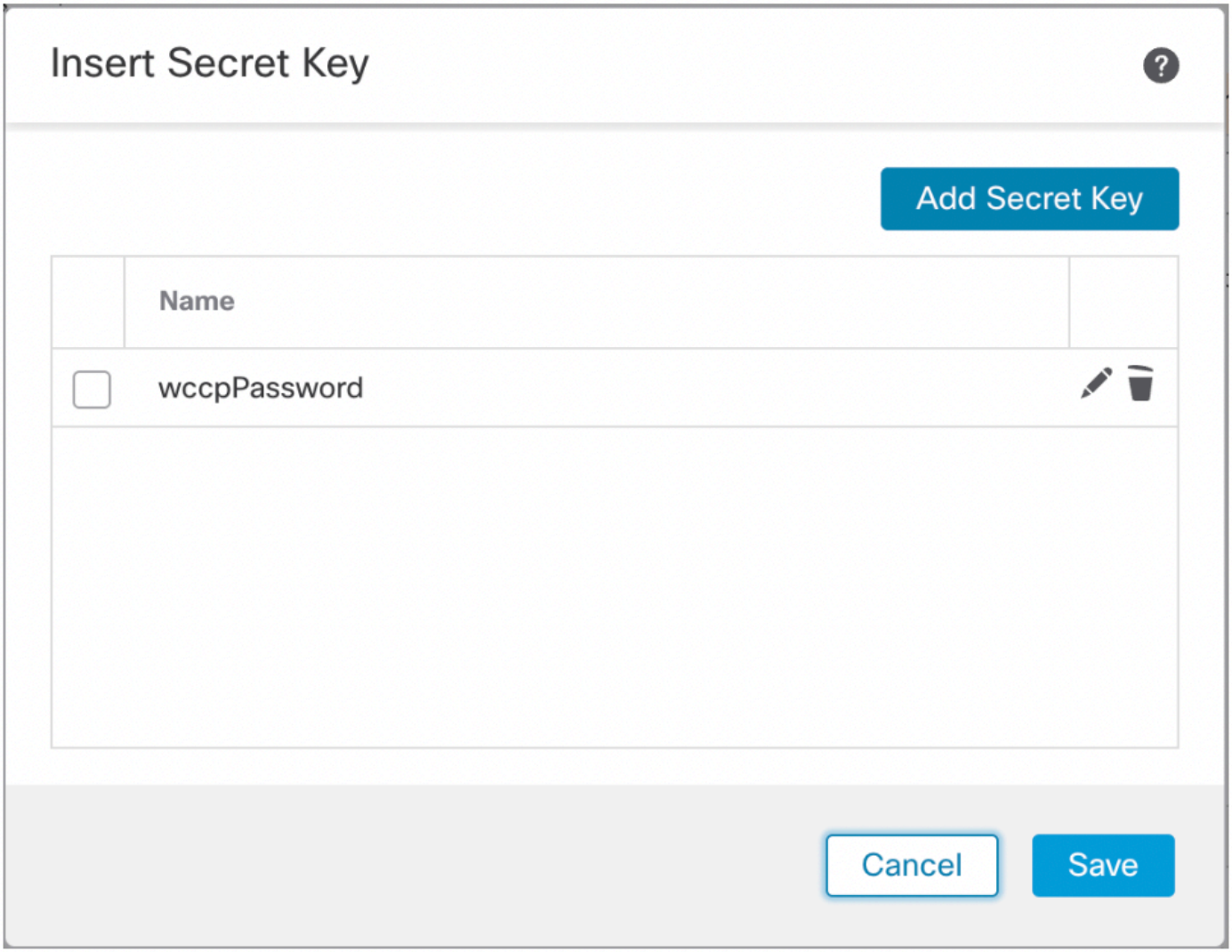
已删除预定义的*wccppassword*

- 从下拉菜单Insert > Insert Secret Key中选择Key。



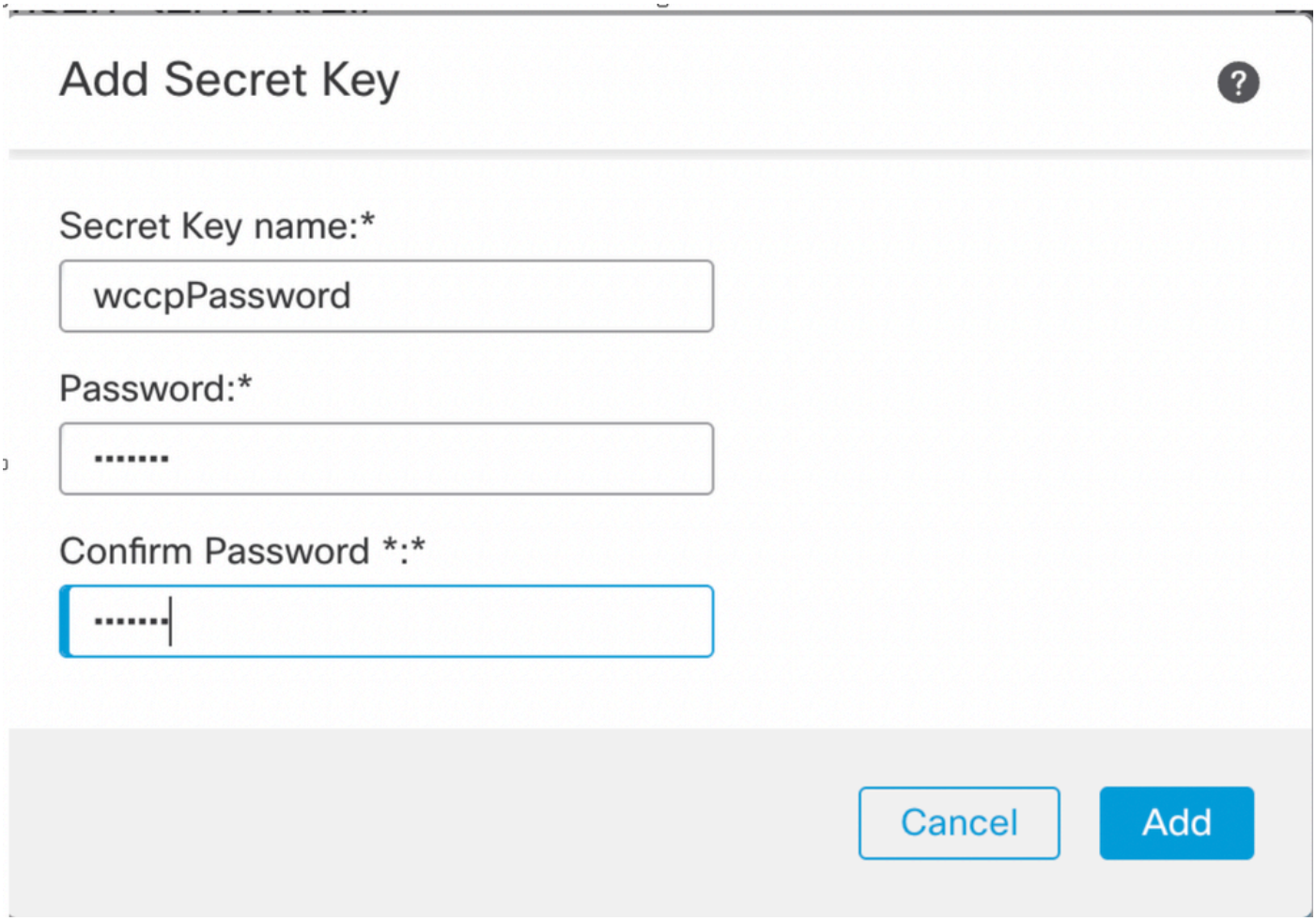
选择密钥

- 点击添加密钥。

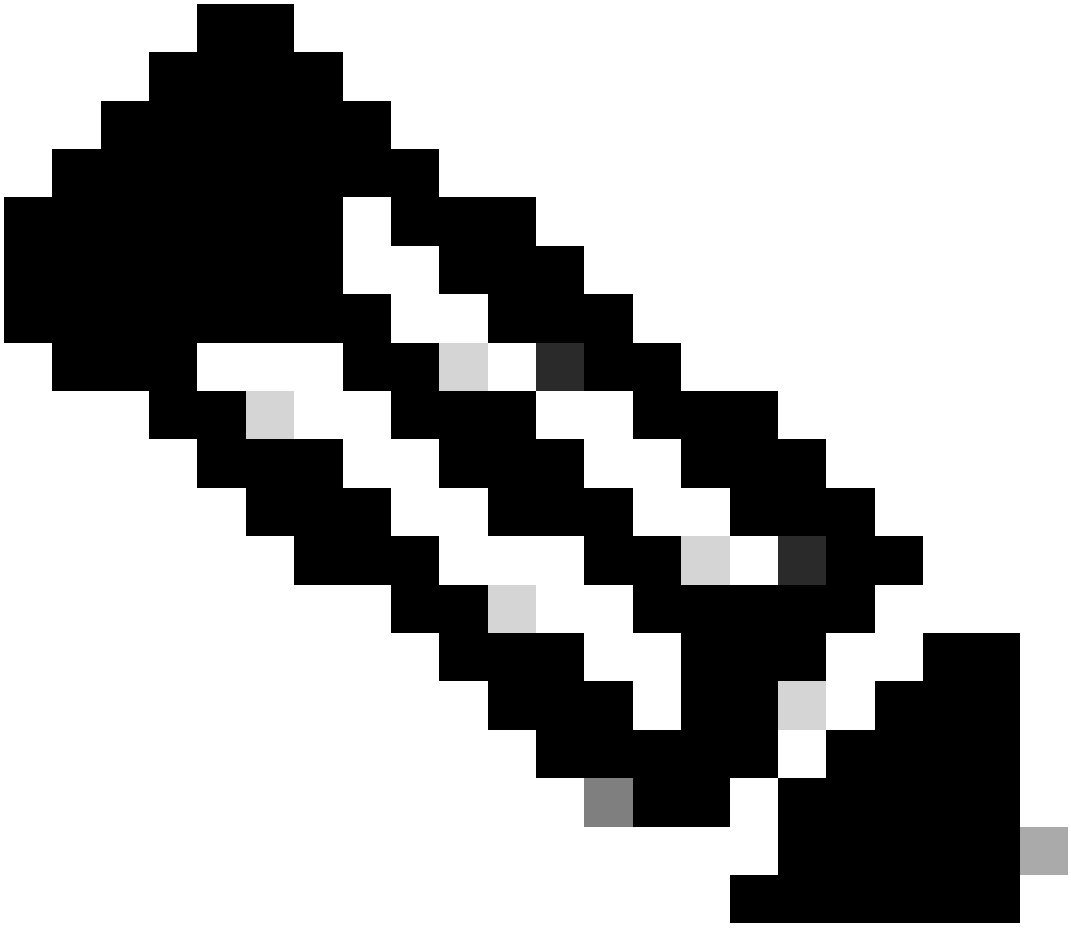


添加密钥

- 在Secret Key name中输入名称。
- 输入密码。
- 在Confirm Password中输入相同的密码，然后单击Add。


Add Secret Key
Secret Key name:*
wccpPassword
Password:*
Confirm Password *:*
Cancel
Add

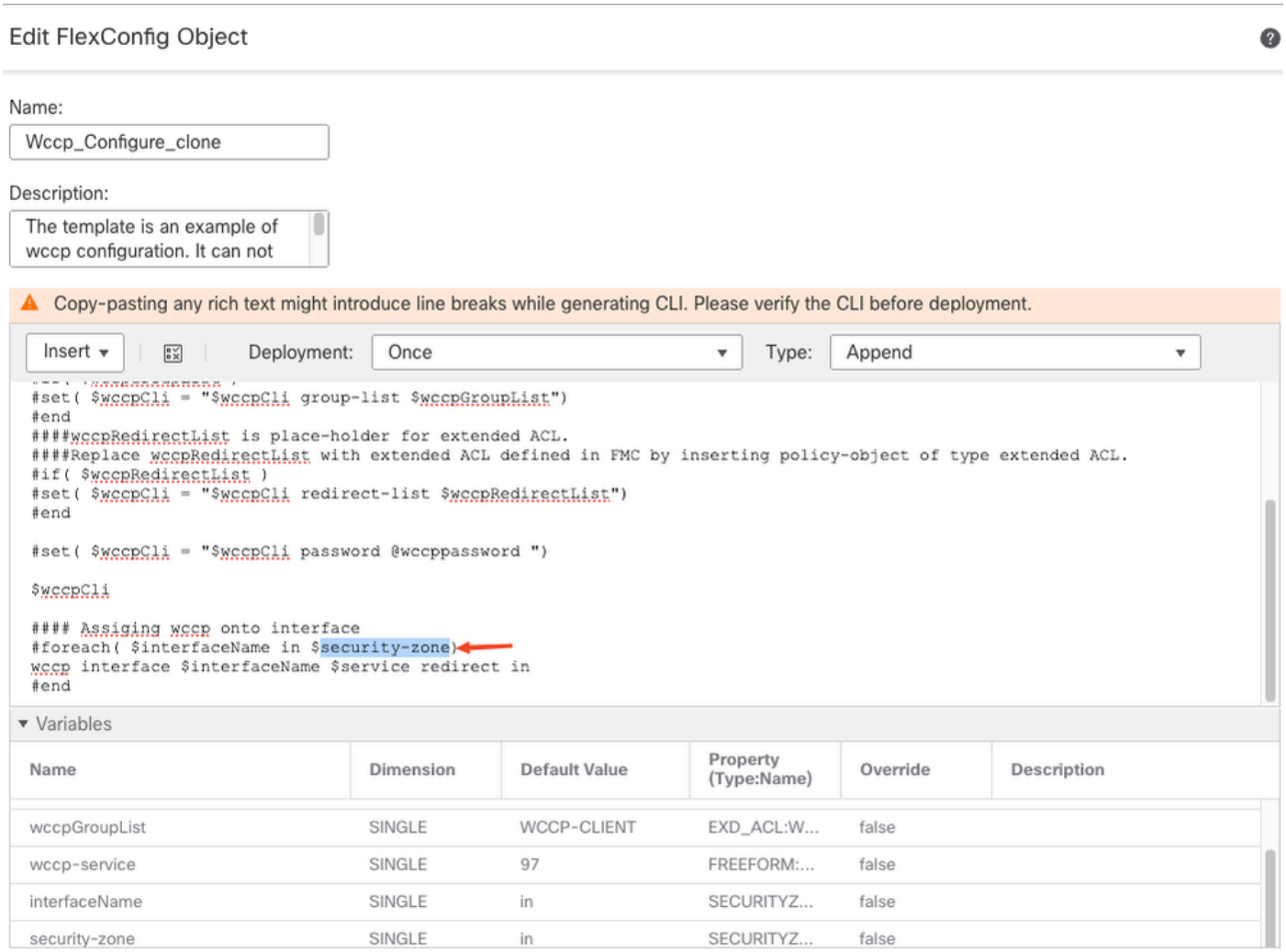
添加用户定义的密钥



注意：在本示例中，内部接口属于中的安全区域。

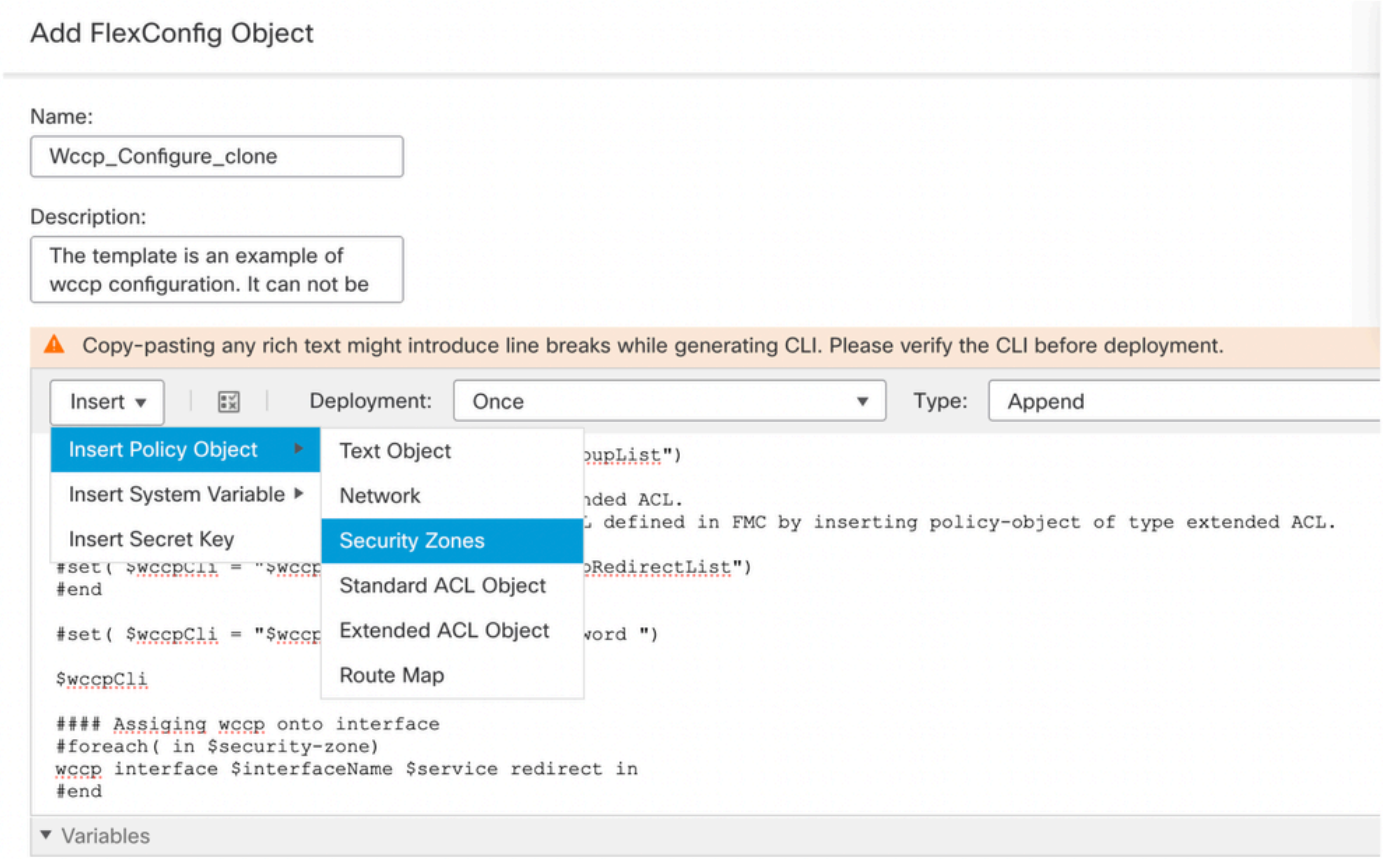
步骤 9：

- 复制预定义的security-zone，并将$security-zone替换为自己的变量。



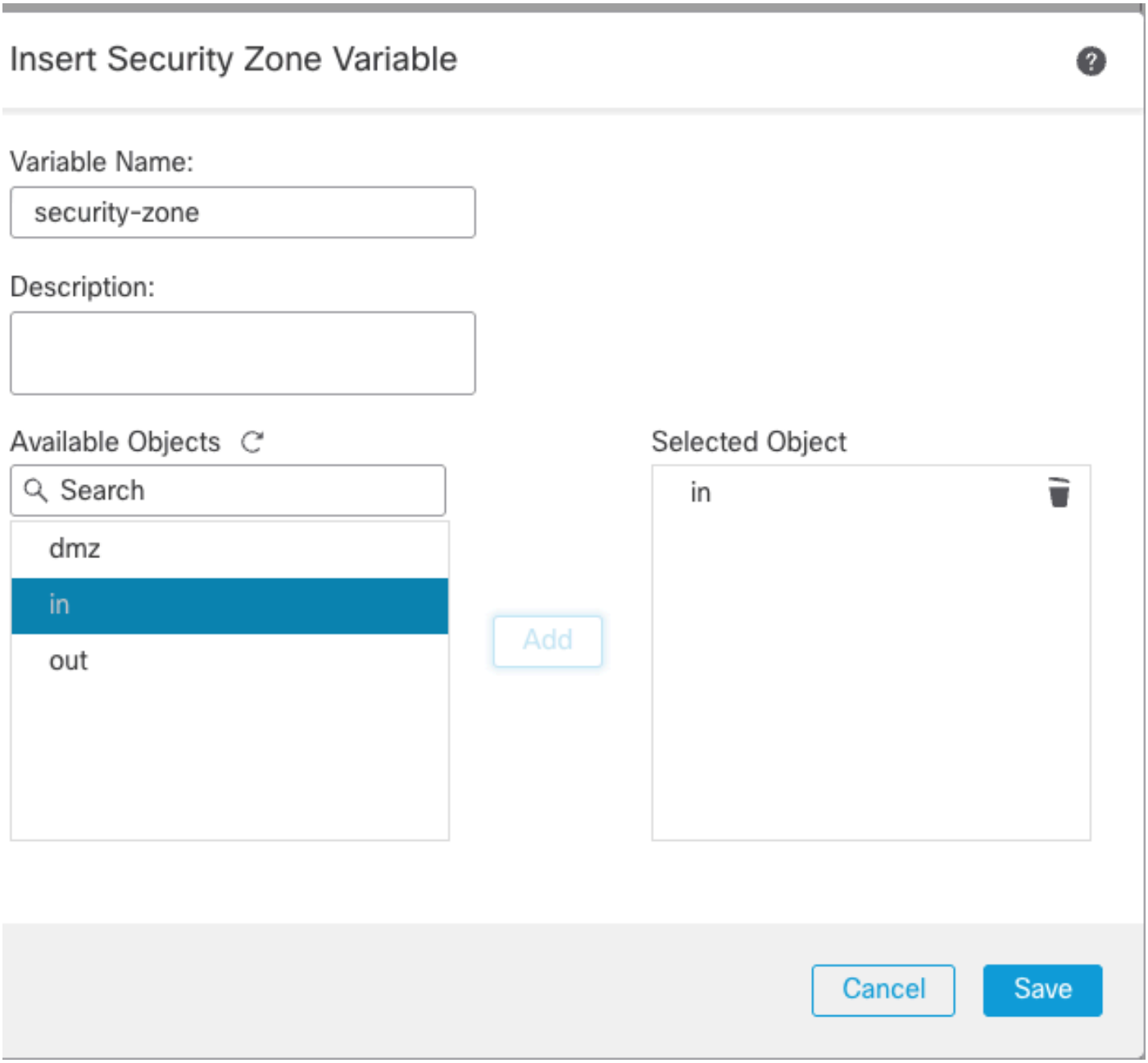
复制名称security-zone

- 从下拉菜单中选择Security Zones，然后选择Insert > Insert Policy Object。



选择安全区域

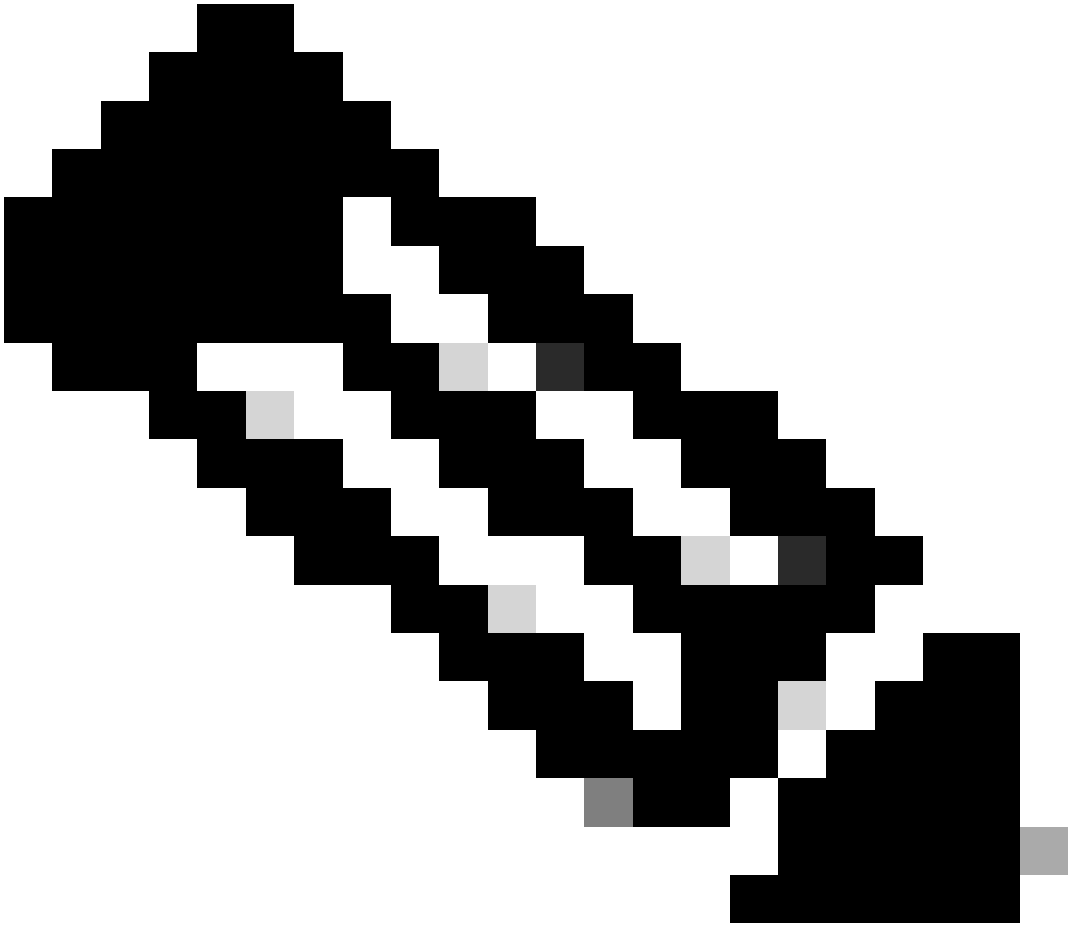
- 将变量名称粘贴为security-zone
- 从Available Objects中选择要添加的接口。
- Click Save.



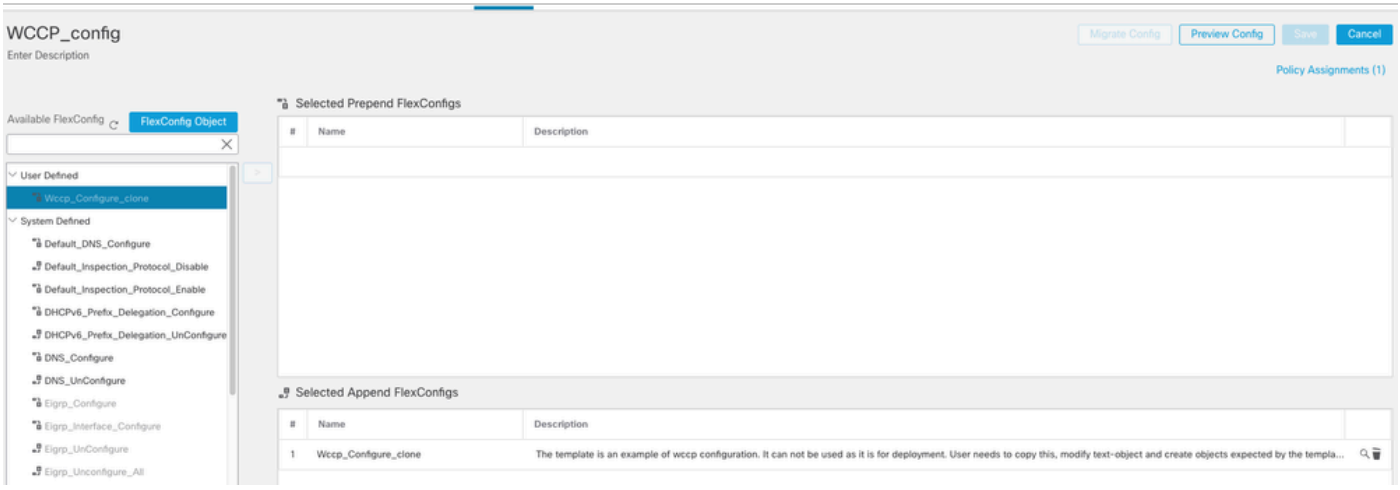
添加安全区域

步骤 10：

- 导航到设备> FlexConfig，点击New Policy或Edit现有策略。
- 选择已配置的Wccp_configure_clone对象，然后单击>进行分配。
- Click Save.



注意：对于新策略，请确保将策略分配给FTD设备。对于现有策略，必须已分配该策略。



将配置的*FlexConfig*分配给设备

第11步：导航到部署>选择FTD设备>点击部署。

验证

步骤 1：检查运行配置。

登录到FTD CLI并运行命令show running-config wccp。

配置示例：

```
wccp 97 redirect-list Redirect_traffic group-list WCCP-CLIENT password *****
wccp interface inside 97 redirect in
```

要确保配置具有正确的密码，请运行命令。

1) system support diagnostic-cli

2） enable

3)按Enter，不输入密码

4） more system:running-config | include wccp

步骤 2：检验WCCP状态

运行命令 show wccp

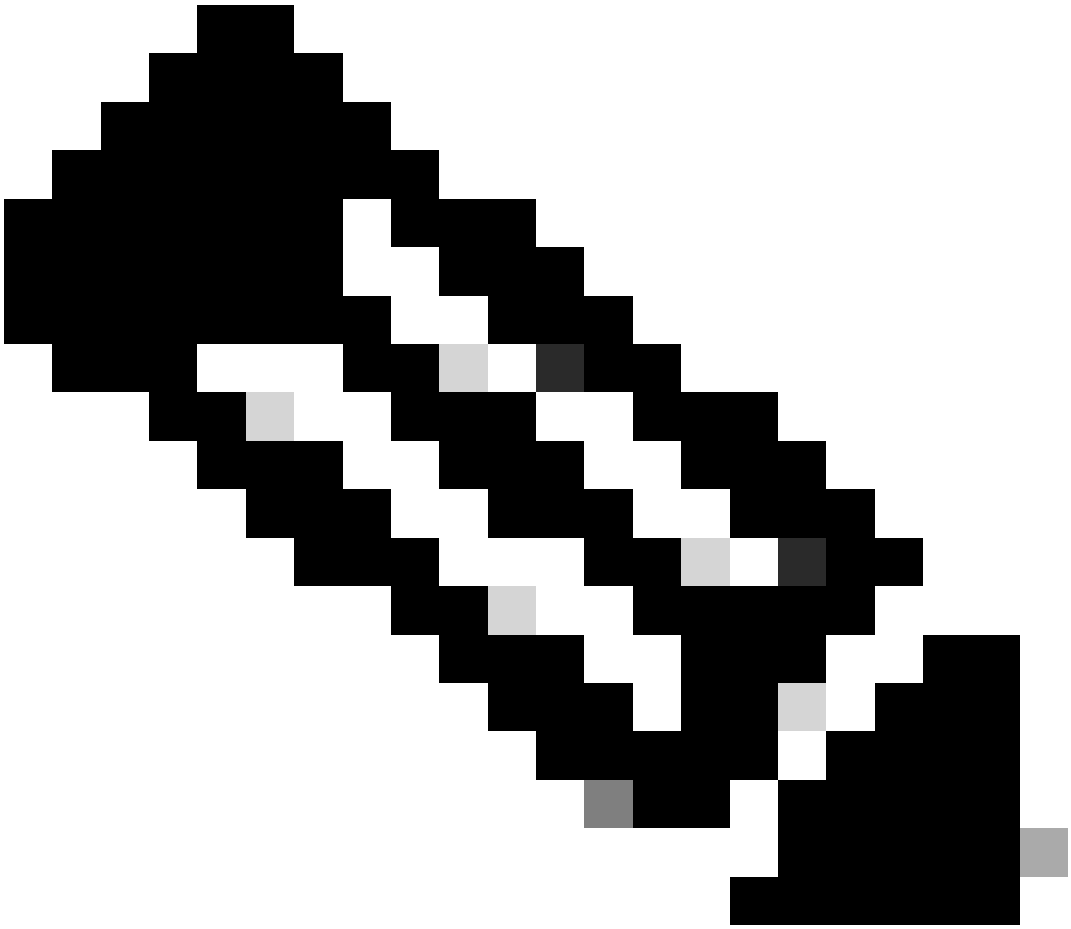
```
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: 97
        Number of Cache Engines:             1
        Number of routers:                   2
        Total Packets Redirected:            0
        Redirect access-list:                Redirect_traffic
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   WCCP-CLIENT
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
```

运行命令 show wccp 97 service

```
WCCP service information definition:
```

```
Type:          Dynamic
Id:            97
Priority:      240
Protocol:      6
Options:       0x00000012
--------
    Hash:      DstIP
    Alt Hash:  -none-
    Ports:     Destination:: 80 443 0 0 0 0 0 0
```



注意：此处97是服务ID。请确保可以在端口中看到从WCCP客户端获知的端口号：部分。

---

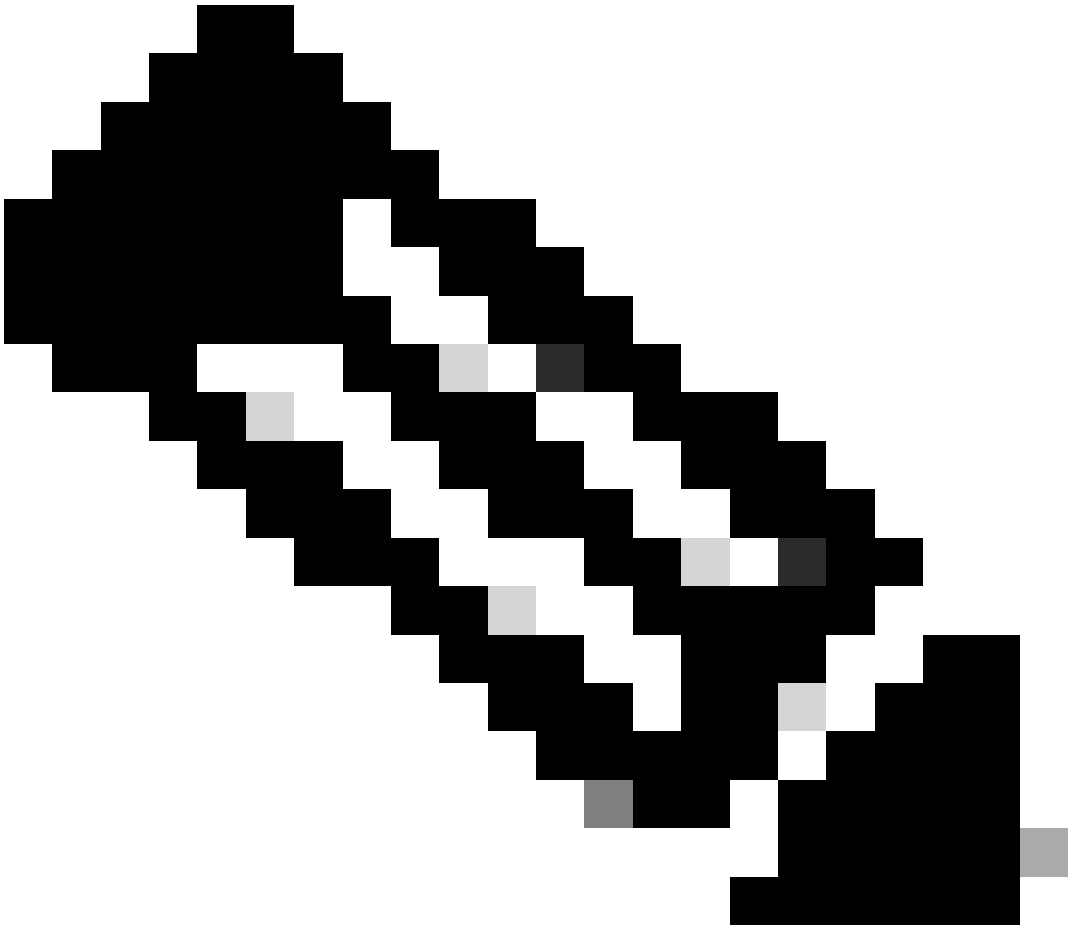
3) Run the command show wccp 97 view

故障排除

步骤 1：检验FTD是否具有来自从代理服务器收到WCCP请求的相同接口的路由。

在本示例中，流量被重定向到themz接口。

```
>show route
S        10.xx.xx.xx 255.yyy.yyy.yyy [1/0] via 10.zz.zz.z, dmz
```



注意：此处10.xx.xx.xx是代理服务器IP，255.yyy.yyy.yyy是网络掩码， 10.zz.zz.z是下一跳网关。

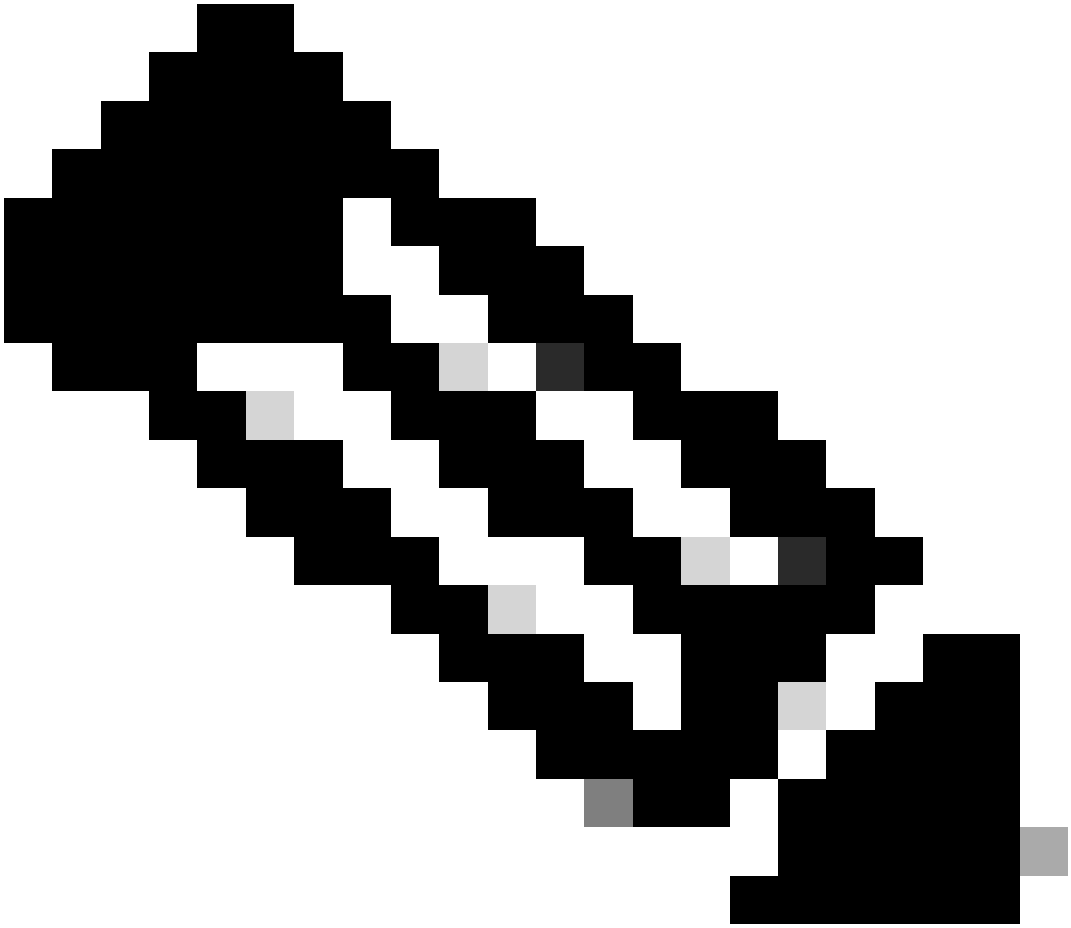
步骤 2：在inside和dmz接口上获取捕获，确保流量被重定向。

在端口443的内部接口上捕获

```
capture capinside interface inside trace detail  match tcp any any eq 443
```

在dmz接口上捕获：

```
capture capdmz interface dmz trace detail match gre any any
```



> 注意：在dmz接口上，必须使用GRE协议进行过滤。重定向数据包封装到wccp客户端的GRE数据包中。

步骤 3：Wccp调试

运行以下命令：

```
debug wccp event debu wccp packet
```

Cisco Bug IDCSCvn90518已提出用于增强功能，以便为WCCP配置提供FDM和FMC本机模式支持。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。