为安全防火墙威胁防御和ASA配置控制平面访问控制策略

目录

简介

本文档介绍为安全防火墙威胁防御和自适应安全设备(ASA)配置控制平面访问规则的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全防火墙威胁防御(FTD)
- 安全防火墙设备管理器(FDM)
- 安全防火墙管理中心(FMC)
- 安全防火墙ASA
- 访问控制列表(ACL)
- FlexConfig

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙威胁防御版本7.2.5
- 安全防火墙管理器中心版本7.2.5
- 安全防火墙设备管理器7.2.5版

- 安全防火墙ASA 9.18.3版

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。

背景信息

流量通常通过防火墙并在数据接口之间路由；在某些情况下，拒绝发往“安全”防火墙的流量是有益的。思科安全防火墙可以使用控制平面访问控制列表(ACL)来限制“流向设备”流量。控制平面ACL何时有用的示例是控制哪些对等体可以建立到安全防火墙的VPN（站点到站点或远程访问VPN）隧道。

保护防火墙“机箱内”流量

流量通常从一个接口（入站）通过防火墙到达另一个接口（出站），这称为“机箱中”流量，由访问控制策略(ACP)和预过滤器规则共同管理。

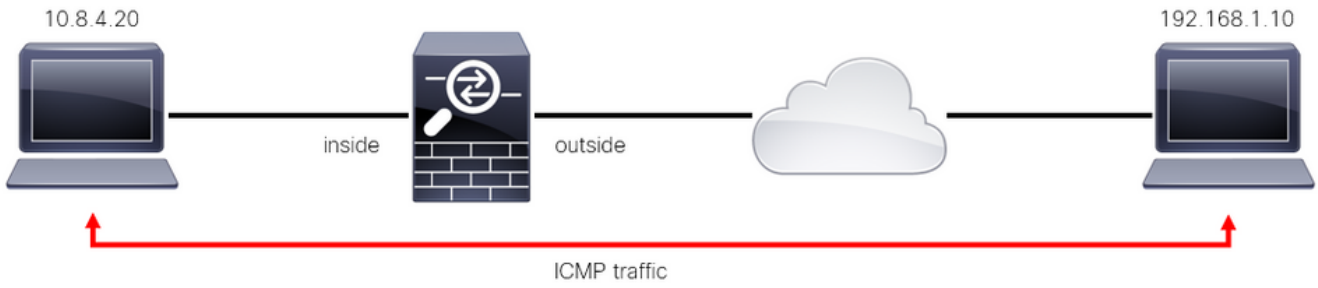

图 1.直通式流量示例

保护防火墙的“设备间”流量

在其他情况下，流量直接发往FTD接口（站点到站点或远程访问VPN），这称为“到设备”流量，由特定接口的控制平面进行管理。

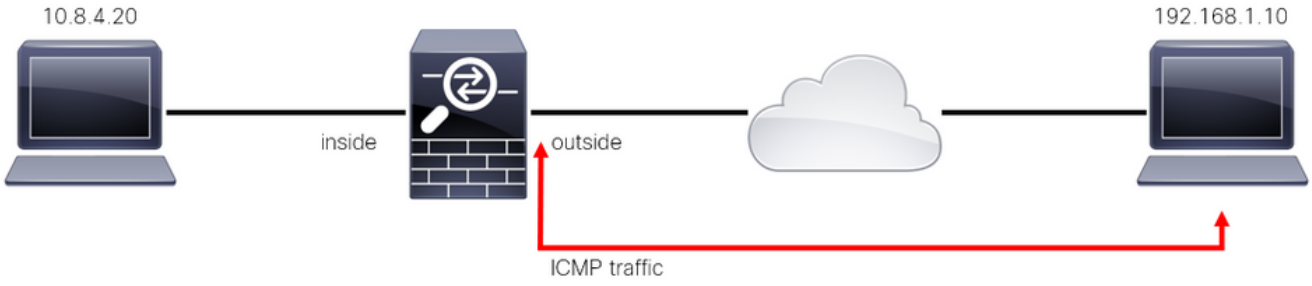

图 2.流向设备的流量示例

有关控制平面ACL的重要注意事项

- 从FMC/FTD版本7.0开始，必须使用FlexConfig配置控制平面ACL，其命令语法与ASA上相同。

- 关键字control-plane附加到访问组配置中，该配置会将流量强制到“安全防火墙”接口。如果没有在命令后附加控制平面字，ACL将限制通过安全防火墙的流量。
- 控制平面ACL不会将SSH、ICMP或TELNET限制为入站到安全防火墙接口。根据平台设置策略处理（允许/拒绝）这些策略，并且具有更高的优先级。
- 控制平面ACL将流量限制为“到”安全防火墙本身，而FTD的访问控制策略或ASA的正常ACL控制流量通过“到”安全防火墙。
- 与普通ACL不同，ACL的末尾没有隐式“deny”语句。
- 在创建本文档时，FTD地理位置功能不能用于限制“访问”FTD。

配置

在下一个示例中，来自某个国家/地区的一组IP地址尝试通过登录到FTD RAVPN来将VPN暴力强行发送到网络。保护FTD免受这些VPN暴力攻击的最佳选项是配置控制平面ACL以阻止这些连接到外部FTD接口。

配置

为FMC管理的FTD配置控制平面ACL

在FMC中需要遵循以下步骤来配置控制平面ACL，以阻止传入VPN暴力攻击到外部FTD接口：

步骤1:通过HTTPS打开FMC图形用户界面(GUI)并使用您的凭证登录。

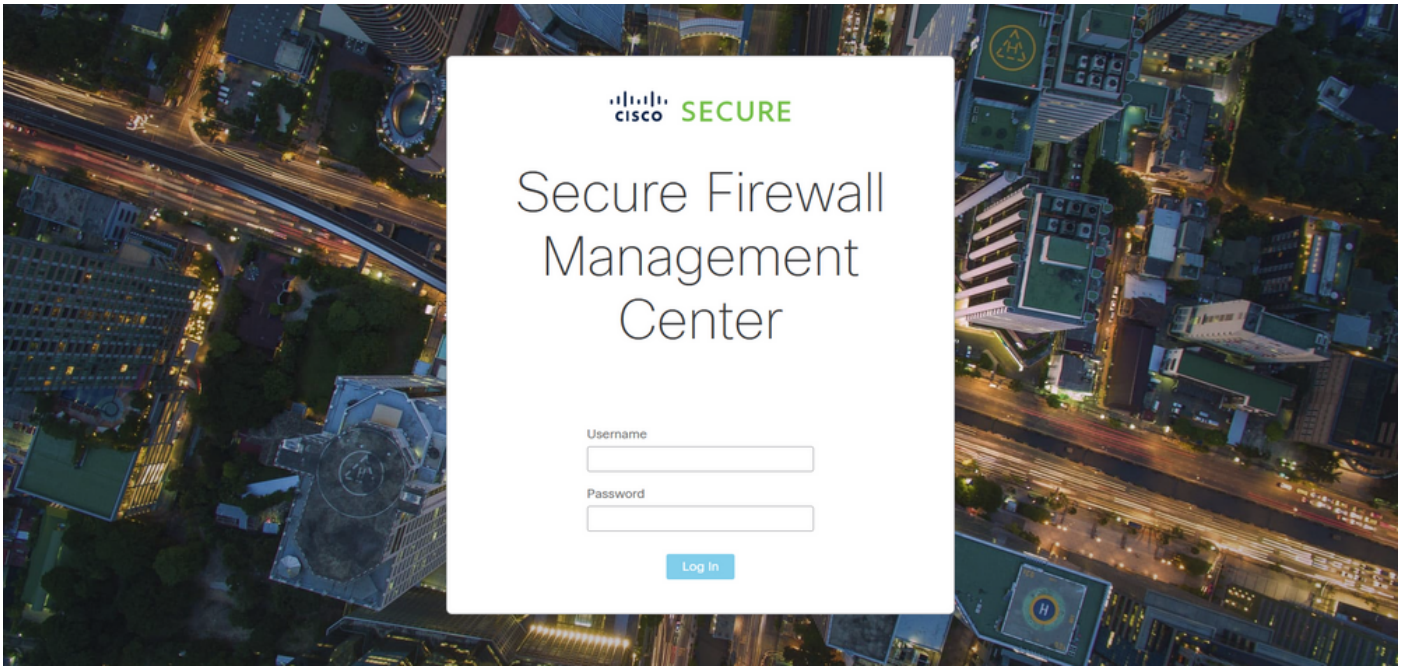

图 3.FMC登录页面

第二步：您需要创建扩展ACL。为此，请导航到Objects > Object Management。

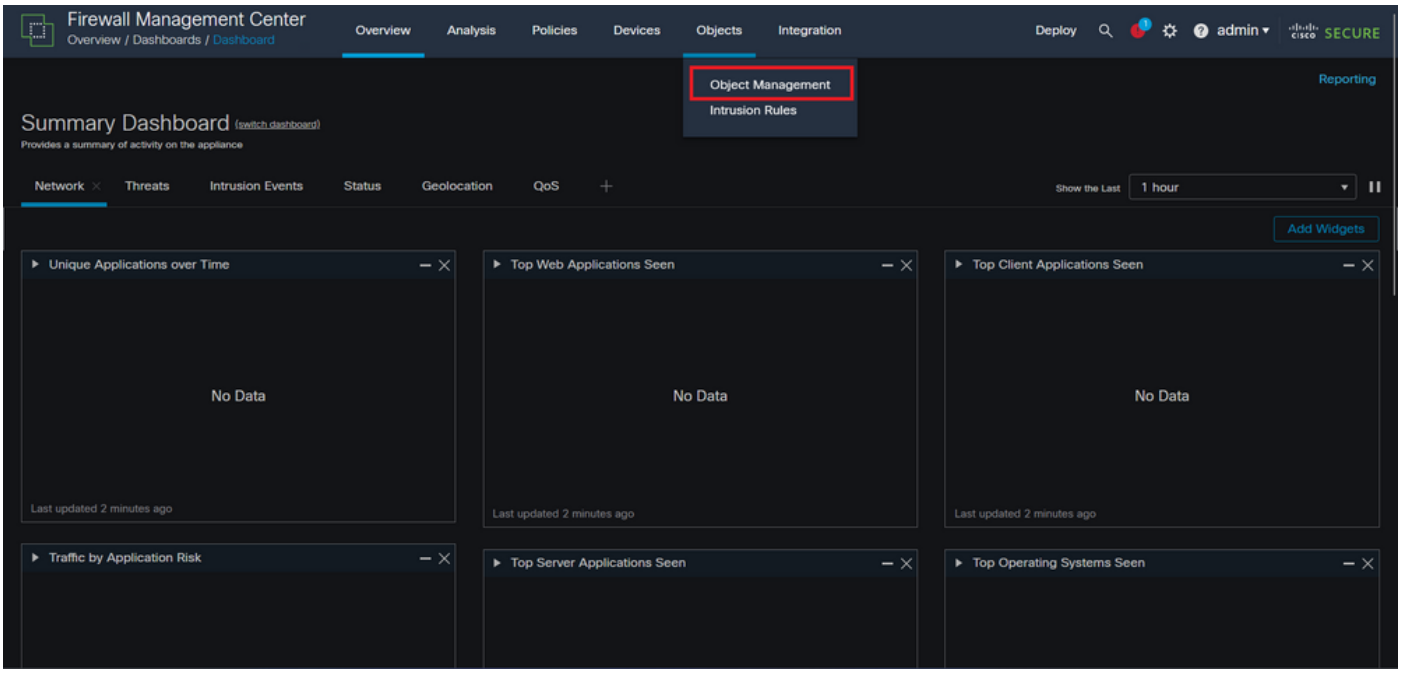

图 4.对象管理

步骤 2.1在左侧面板中，导航到Access List > Extended以创建扩展ACL。

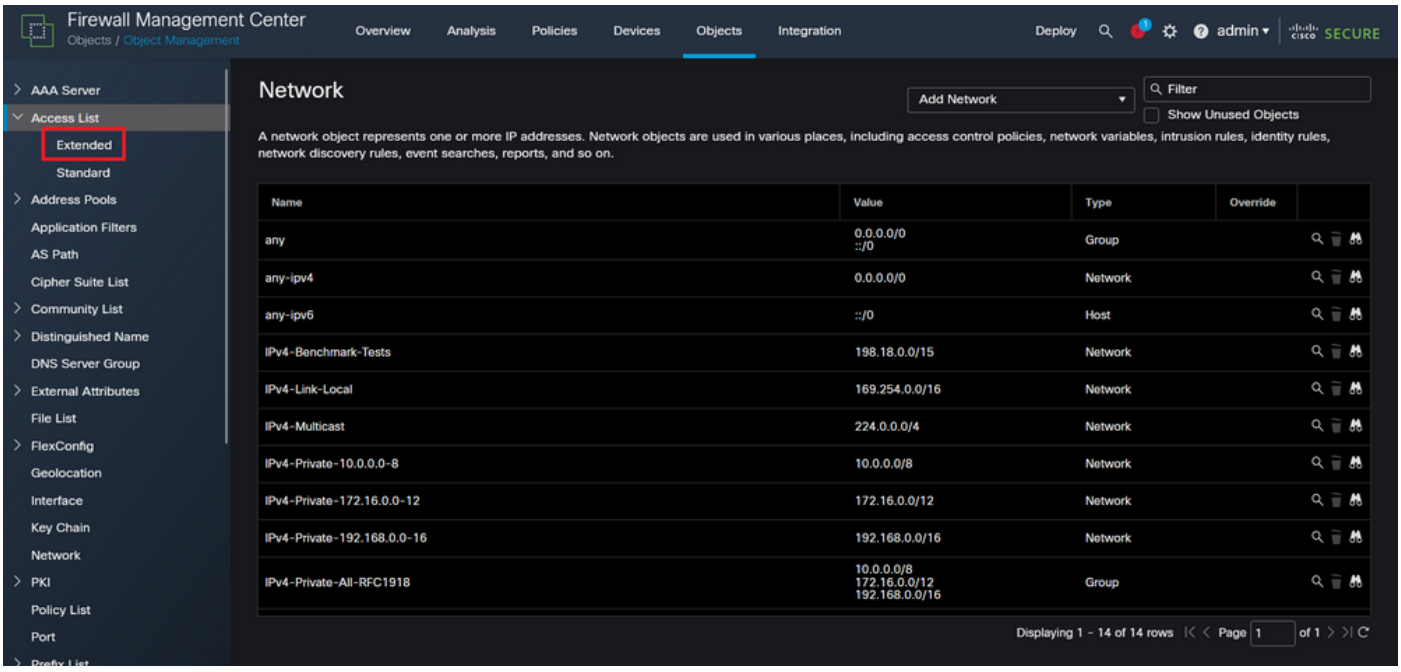

图 5.扩展ACL菜单

步骤 2.2然后，选择Add Extended Access List。

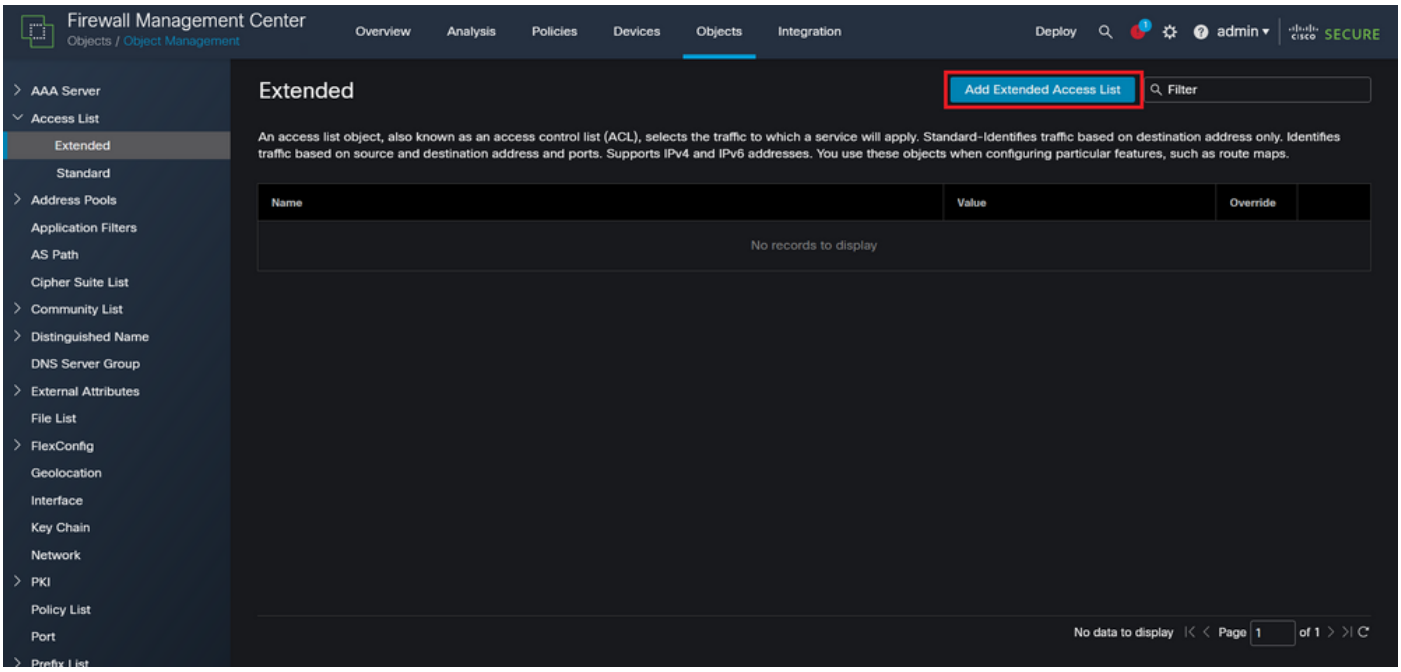

图 6.添加扩展ACL

步骤 2.3键入扩展ACL的名称，然后点击Add按钮以创建访问控制条目(ACE):

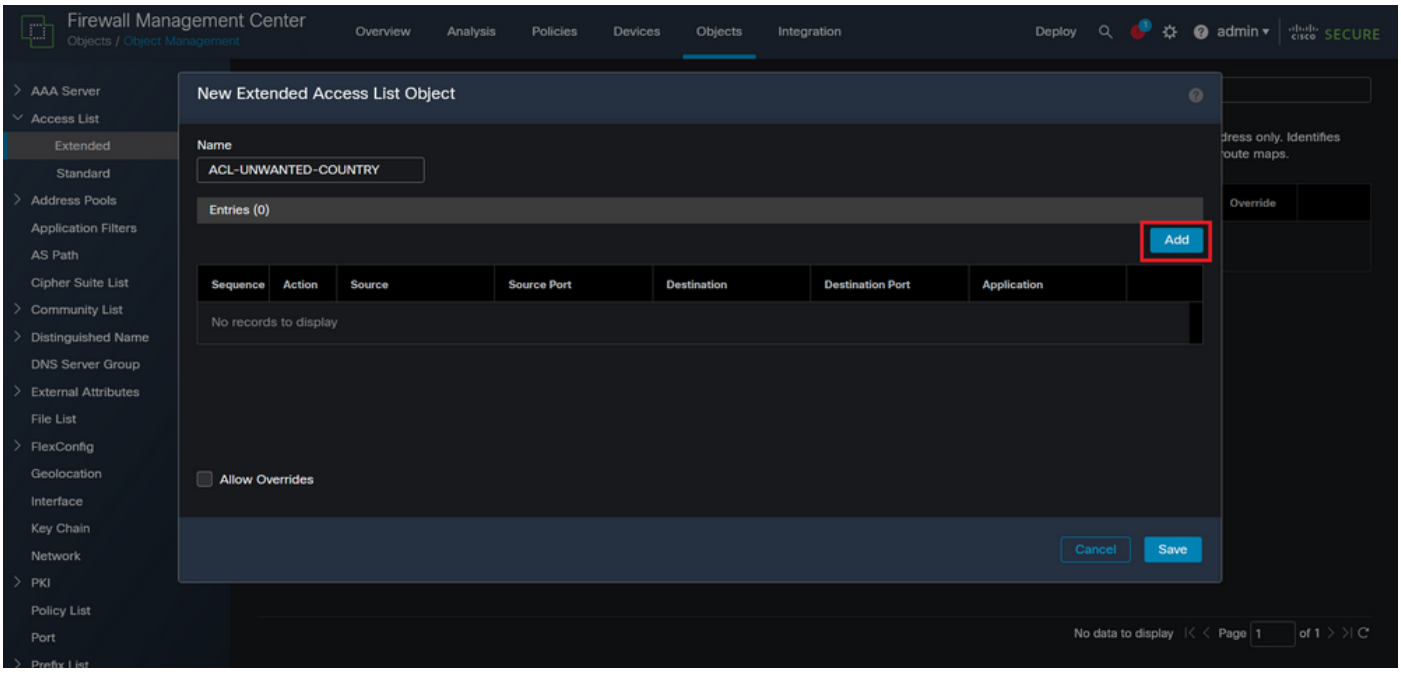

图 7.扩展ACL条目

步骤 2.4将ACE操作更改为Block，然后添加源网络以匹配需要拒绝到FTD的流量，将目标网络保留为Any，然后点击Add按钮完成ACE条目：

— 在本示例中，配置的ACE条目将阻止来自192.168.1.0/24子网的VPN暴力攻击。

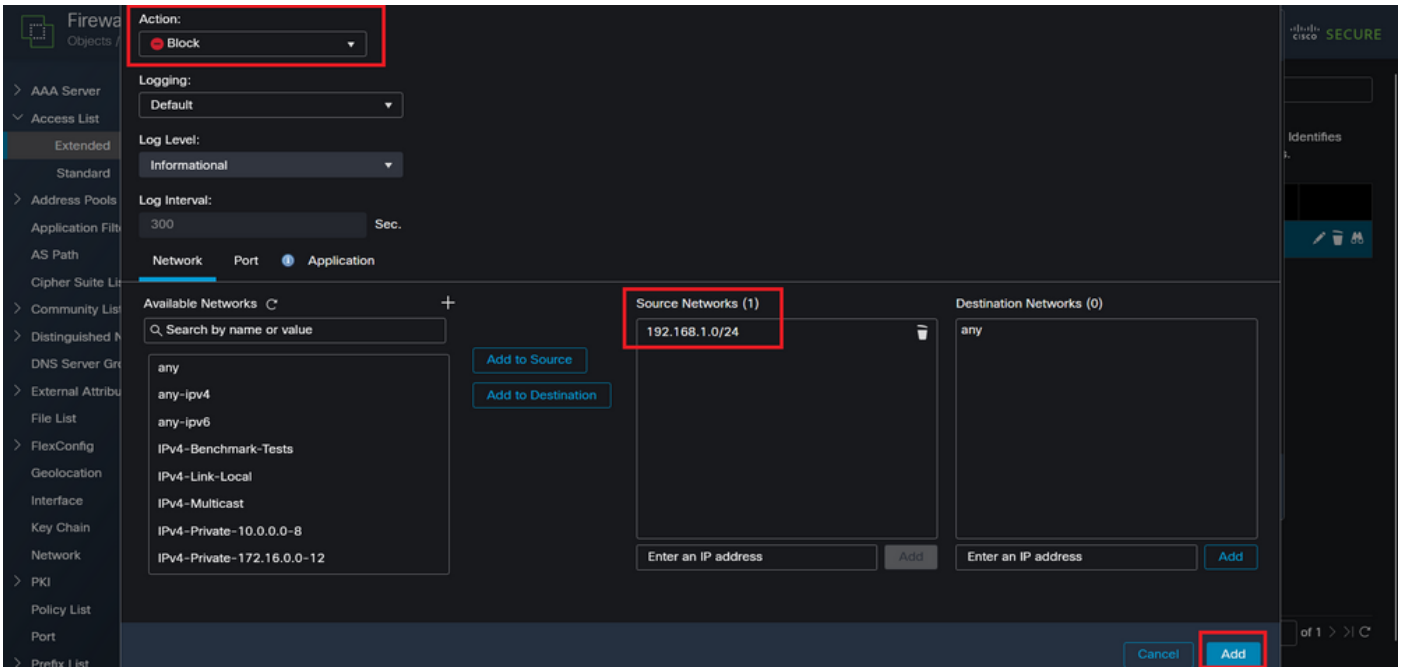

图 8.拒绝的网络

步骤 2.5如果需要添加更多ACE条目，请再次点击Add按钮并重复步骤2.4。之后，点击Save按钮完成ACL配置。

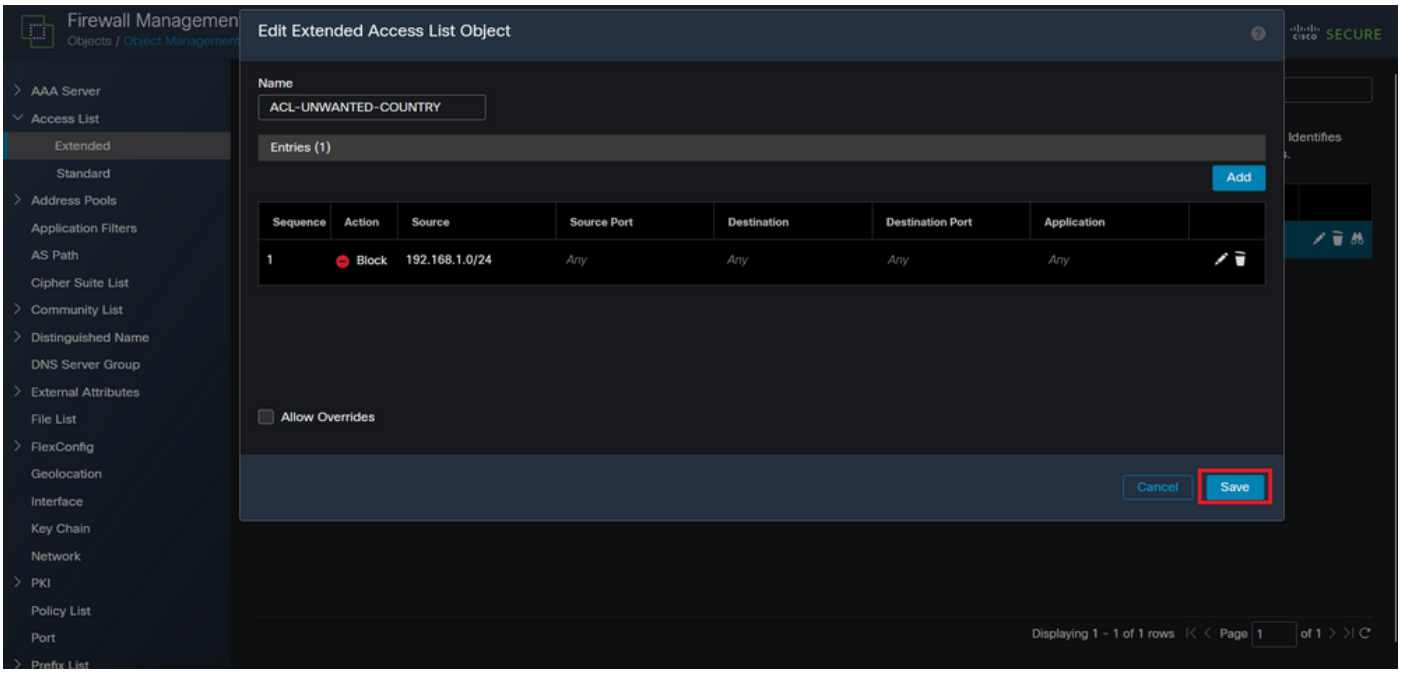

图 9.已完成的扩展ACL条目

第三步：然后，您需要配置Flex-Config对象以将控制平面ACL应用于外部FTD接口。为此，导航到左侧面板，然后选择选项FlexConfig > FlexConfig Object。

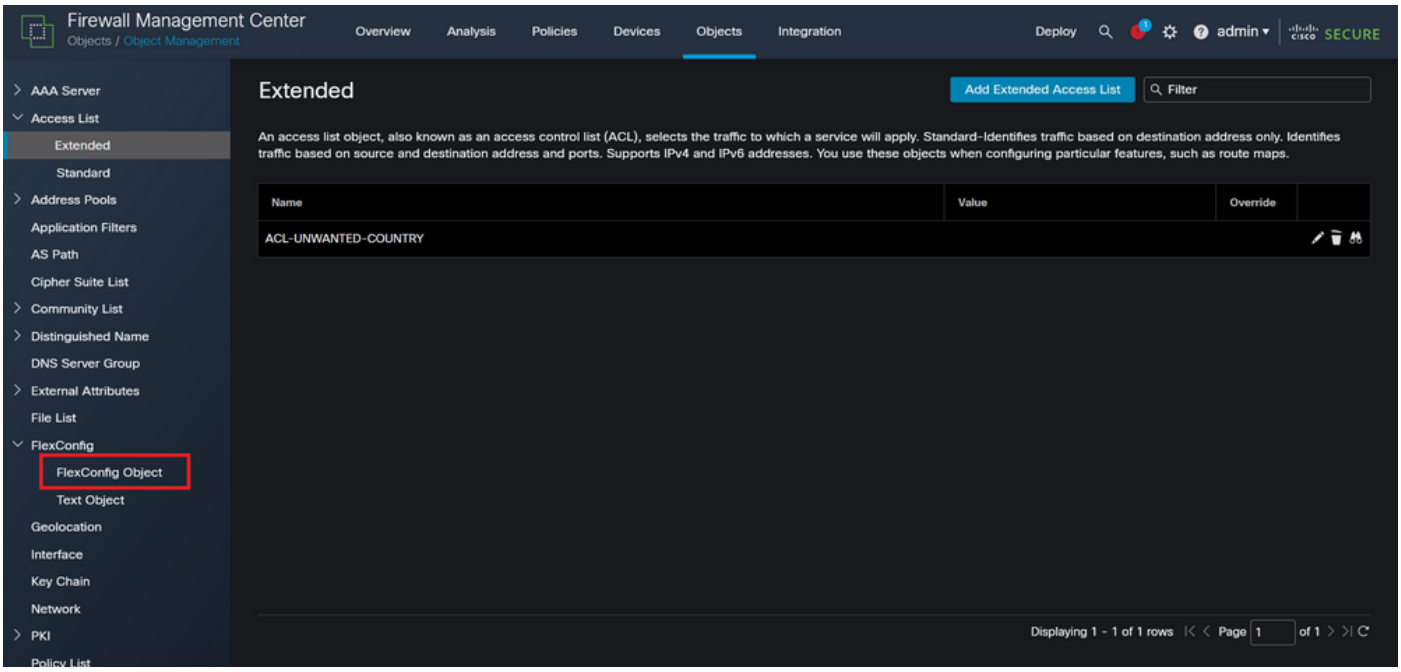

图 10.FlexConfig对象菜单

步骤 3.1点击Add FlexConfig Object。

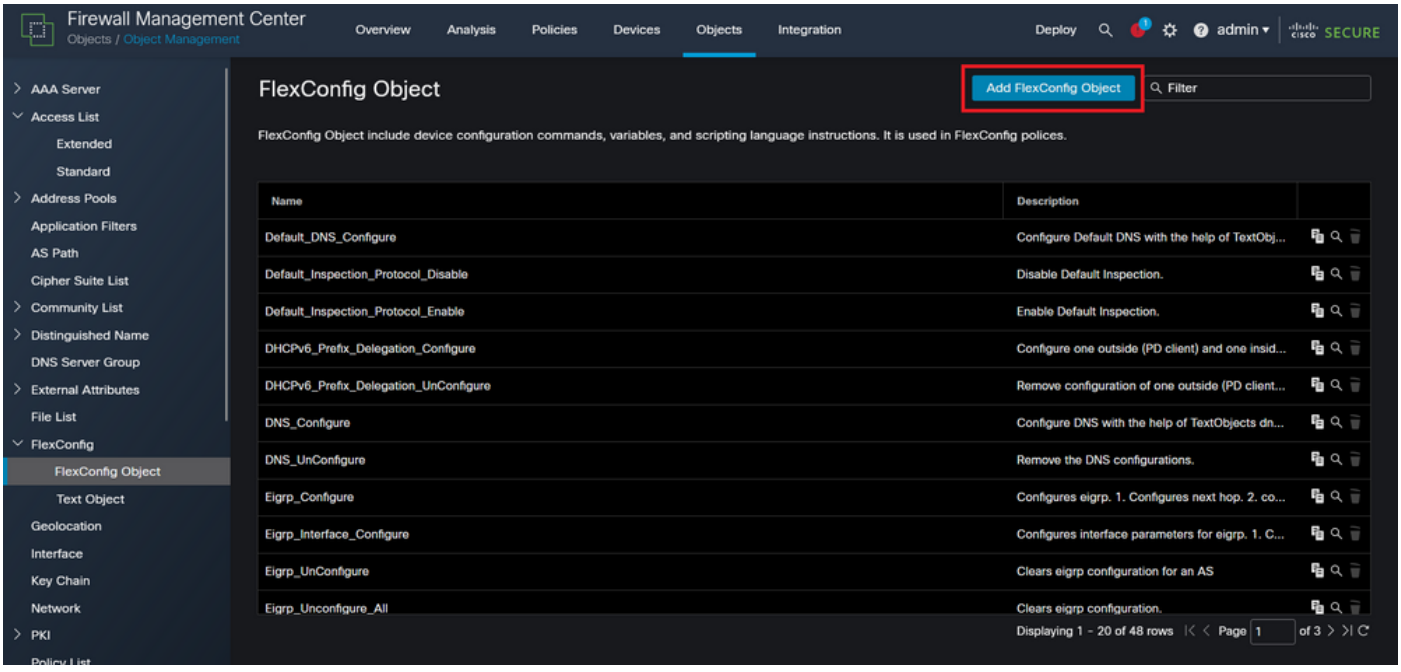

图 11.添加Flexconfig对象

步骤 3.2为FlexConfig对象添加名称，然后插入ACL策略对象。为此，请选择Insert > Insert Policy Object > Extended ACL Object。

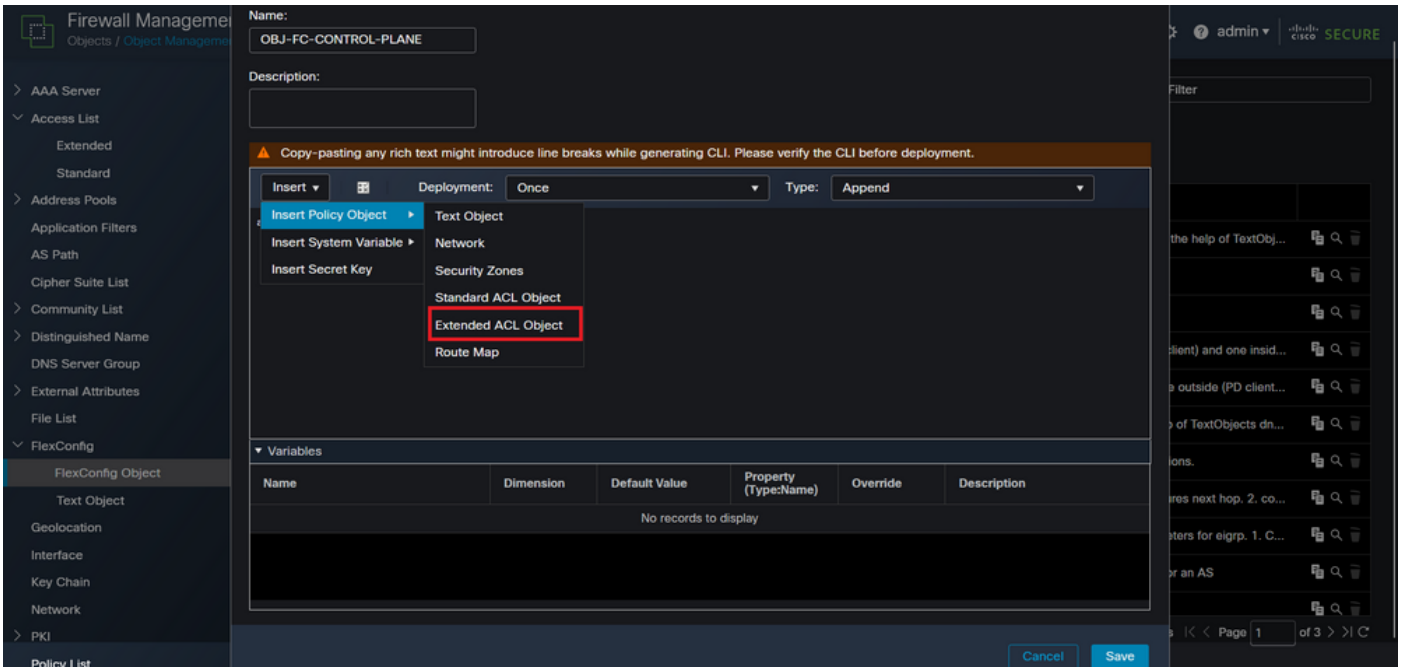

图 12.FlexConfig对象变量

步骤 3.3为ACL对象变量添加名称，然后选择在步骤2.3中创建的扩展ACL，然后点击Save按钮。

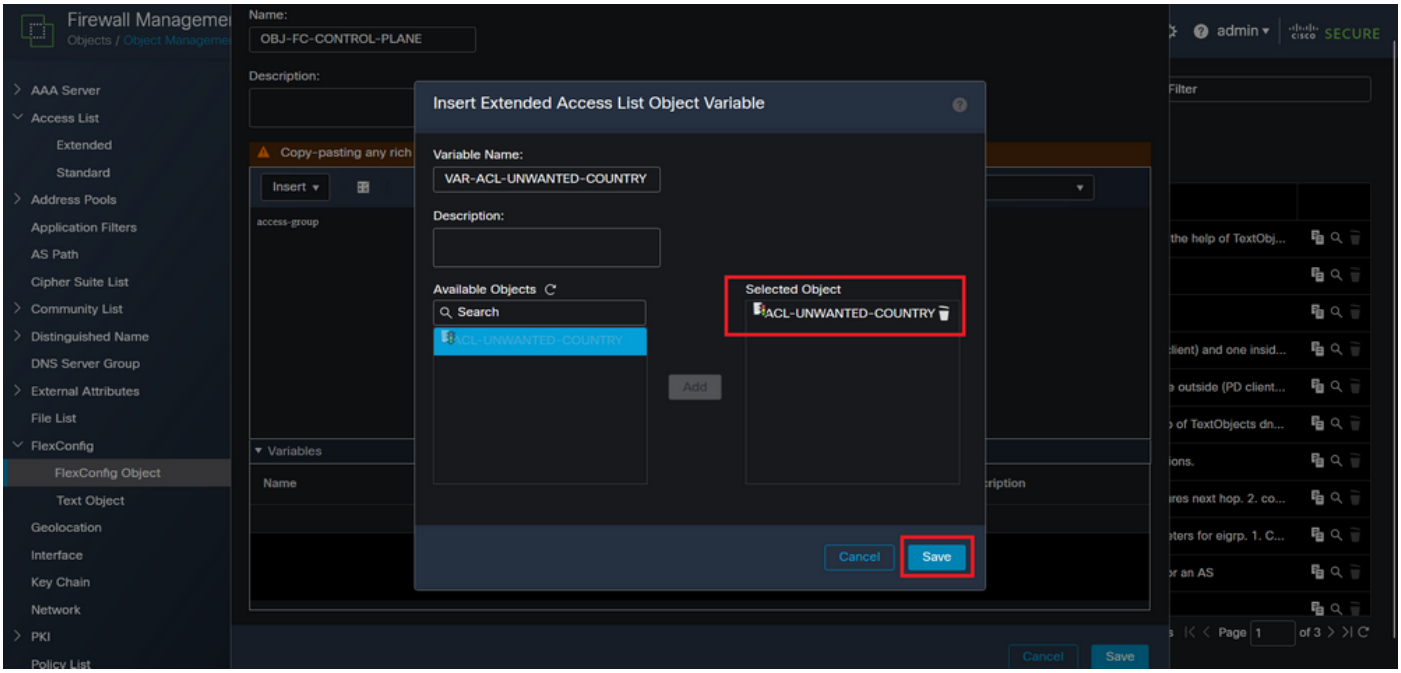

图 13.FlexConfig对象变量ACL分配

步骤 3.4然后，将控制平面ACL配置为外部接口的入站流量，如下所示。

命令行语法：

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

这转换为下一个命令示例，该示例使用上述步骤2.3“VAR-ACL-UNWANTED-COUNTRY”中创建的ACL变量，如下所示：

```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

这是在FlexConfig对象窗口中配置该对象的方法，之后，选择“保存”按钮以完成FlexConfig对象。

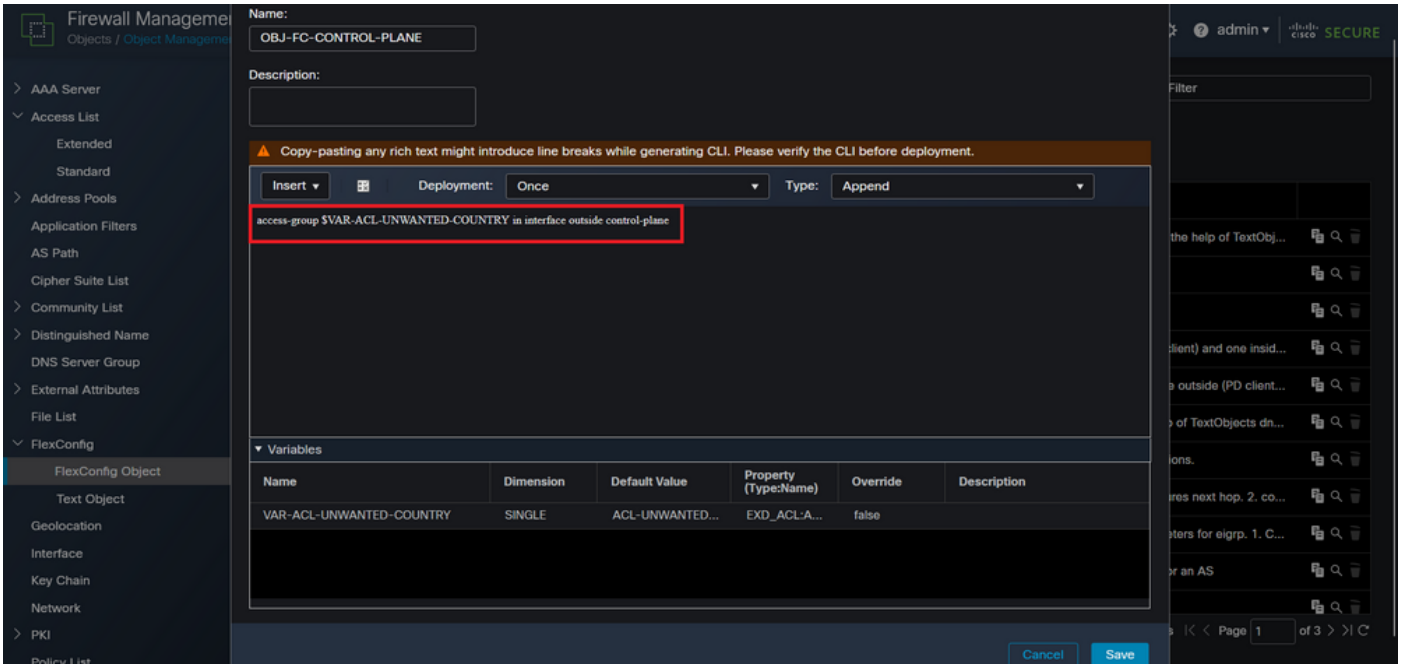

图 14.Flexconfig对象完成命令行

第四步：您需要将FlexConfig对象配置应用于FTD，为此，请转到Devices > FlexConfig。

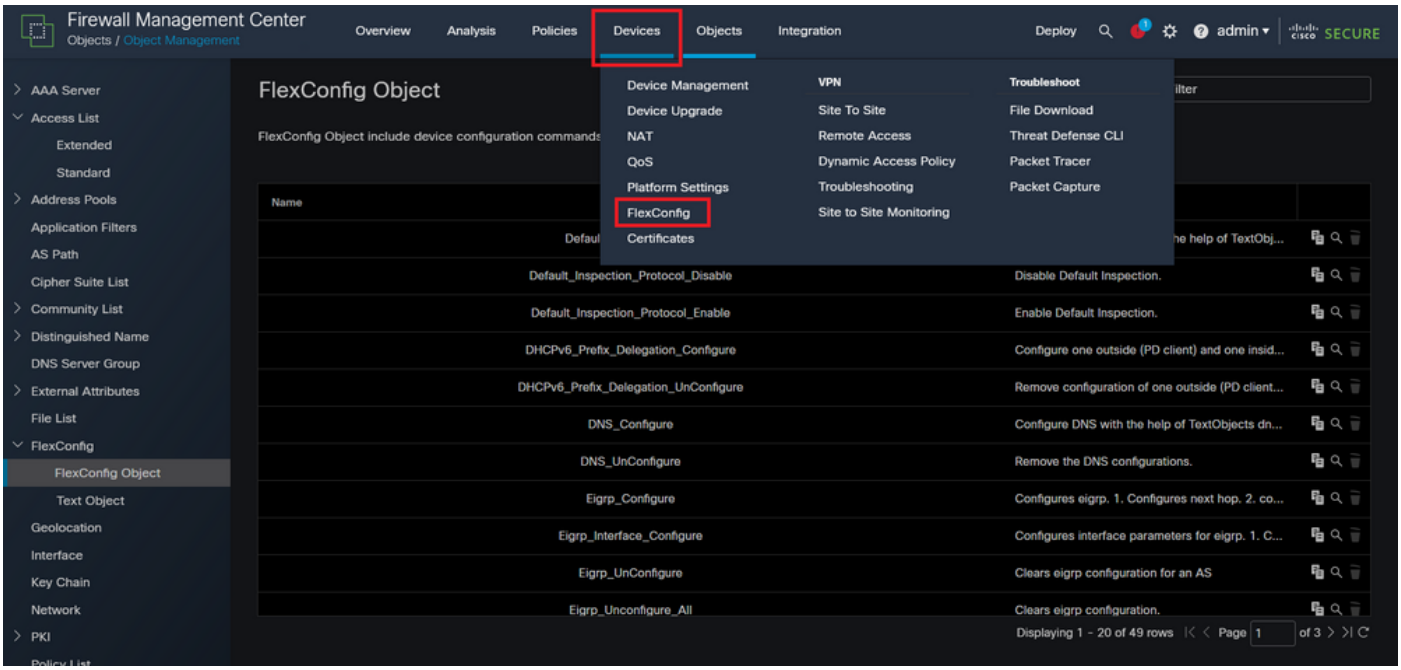

图 15.FlexConfig Policy菜单

步骤 4.1然后，如果尚未为FTD创建FlexConfig，请点击New Policy，或者编辑现有的FlexConfig策略。

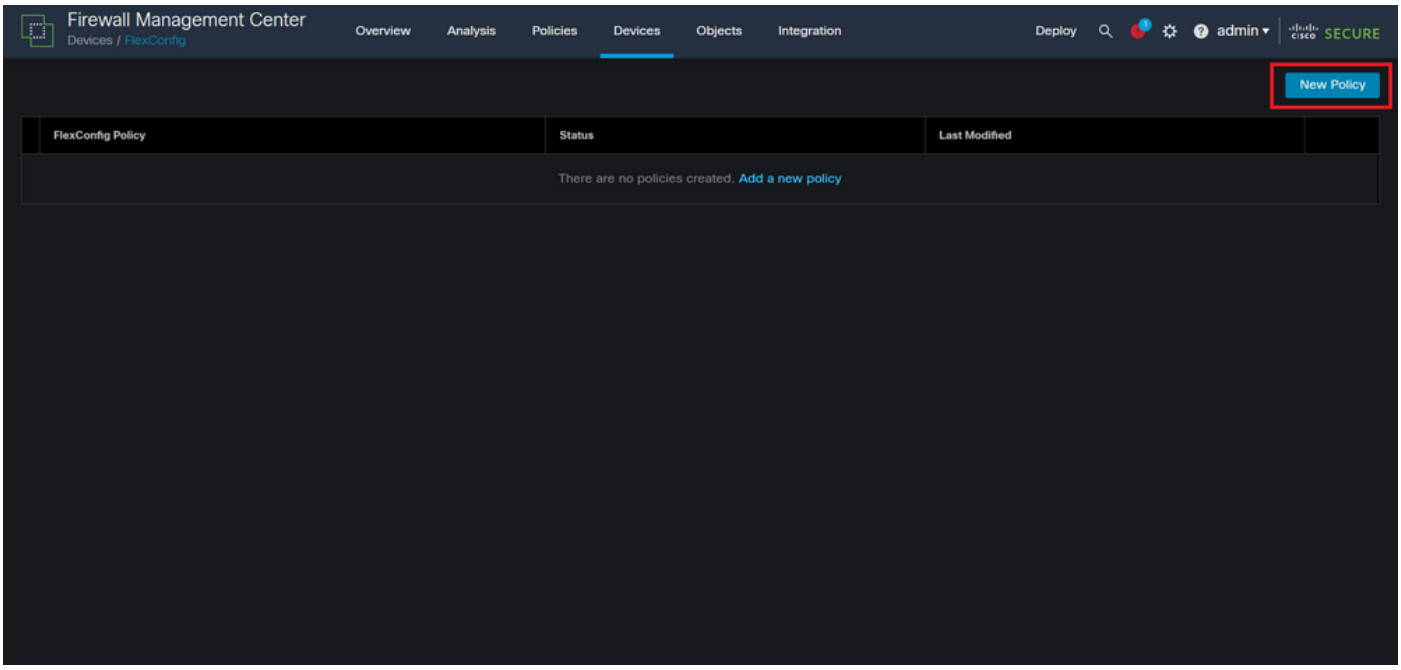

图 16.FlexConfig策略创建

步骤 4.2为新的FlexConfig策略添加名称，然后选择要应用创建的控制平面ACL的FTD。

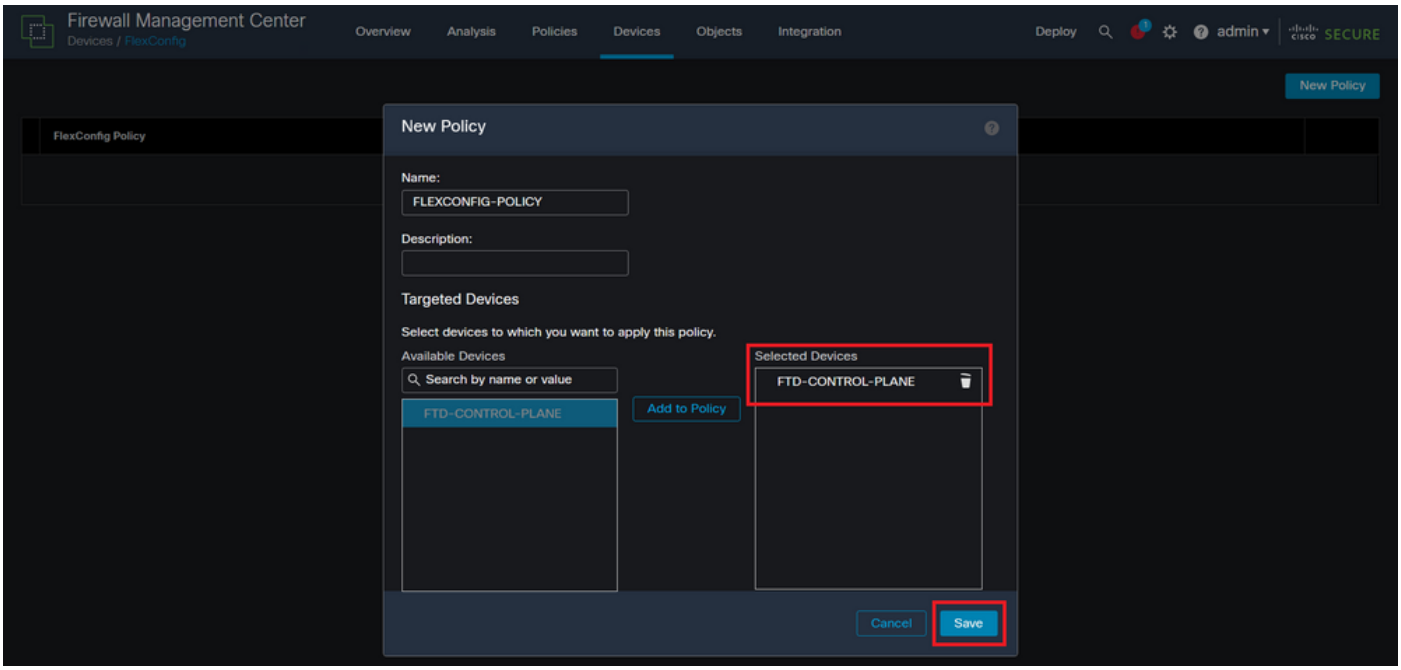

图 17.FlexConfig策略设备分配

步骤 4.3在左侧面板中，搜索在上面的步骤3.2中创建的FlexConfig对象，然后通过单击位于窗口中间的右箭头将其添加到FlexConfig策略中，然后点击Save按钮。

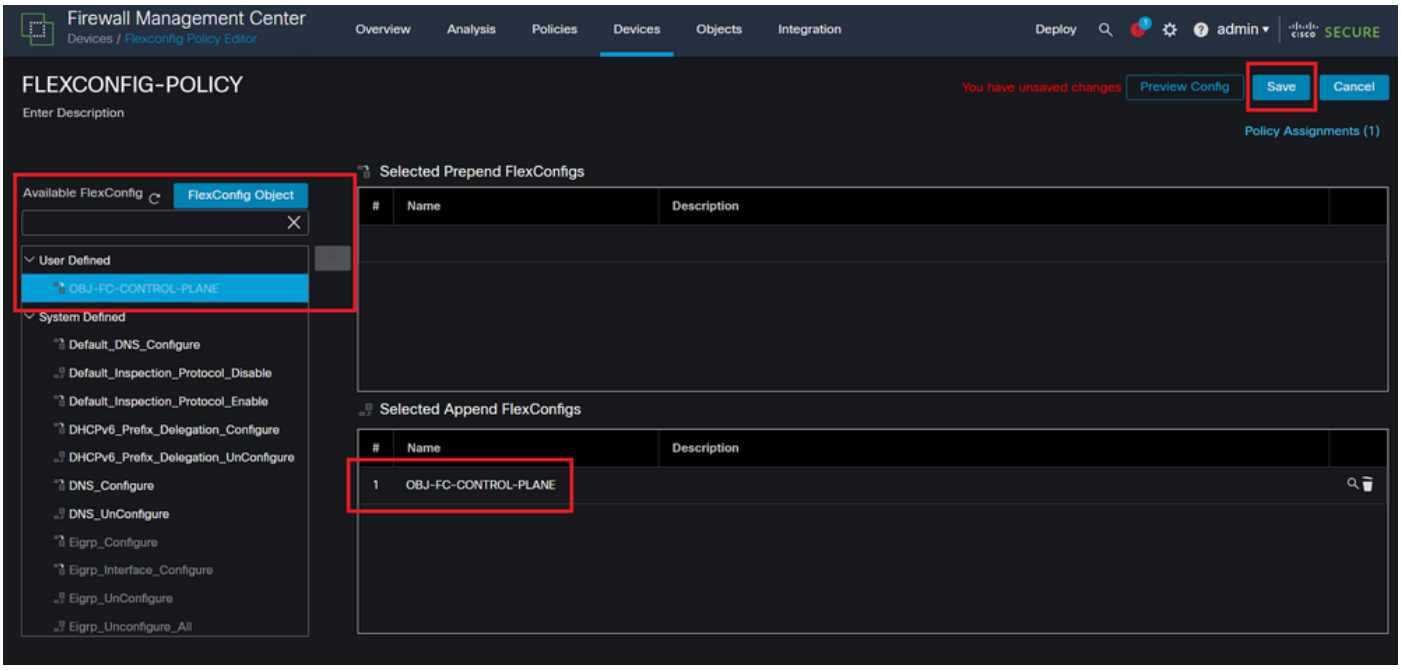

图 18.FlexConfig策略对象分配

第五步：继续将配置更改部署到FTD，为此，请导航到Deploy > Advanced Deploy。

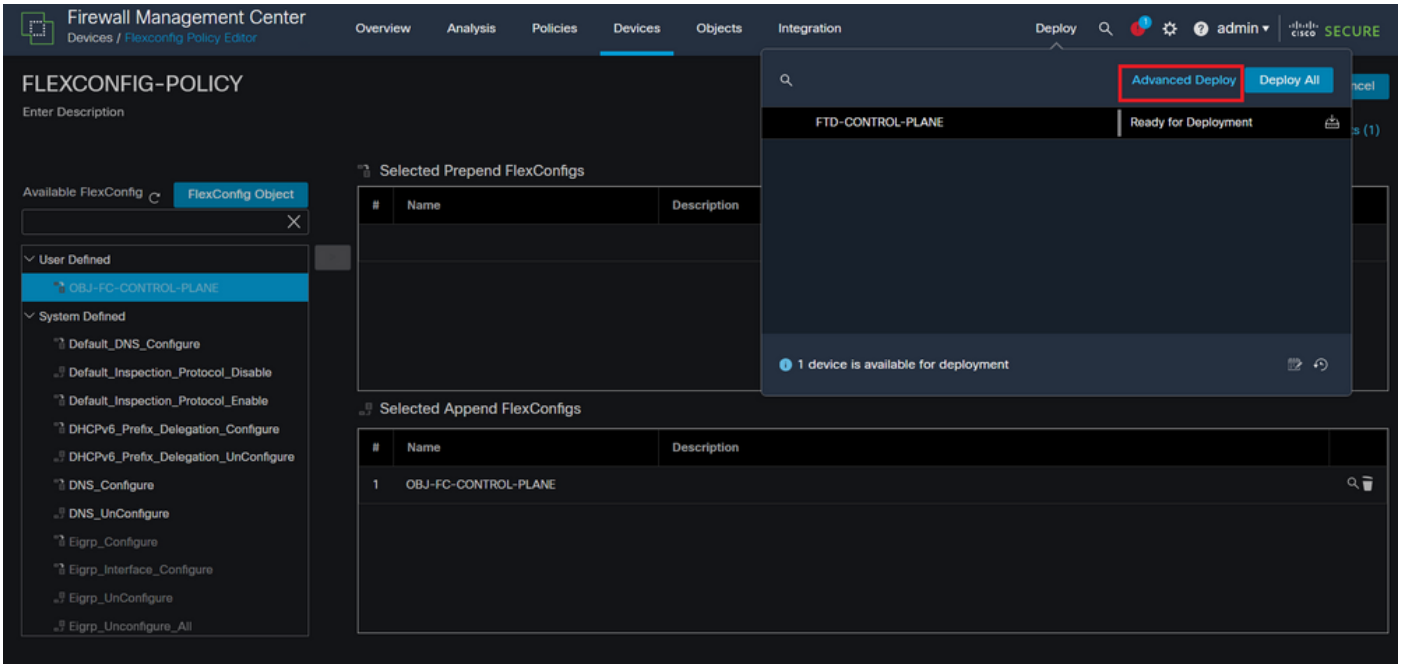

图 19.FTD高级部署

步骤 5.1然后，选择要应用FlexConfig策略的FTD。如果一切正确，则点击Deploy。

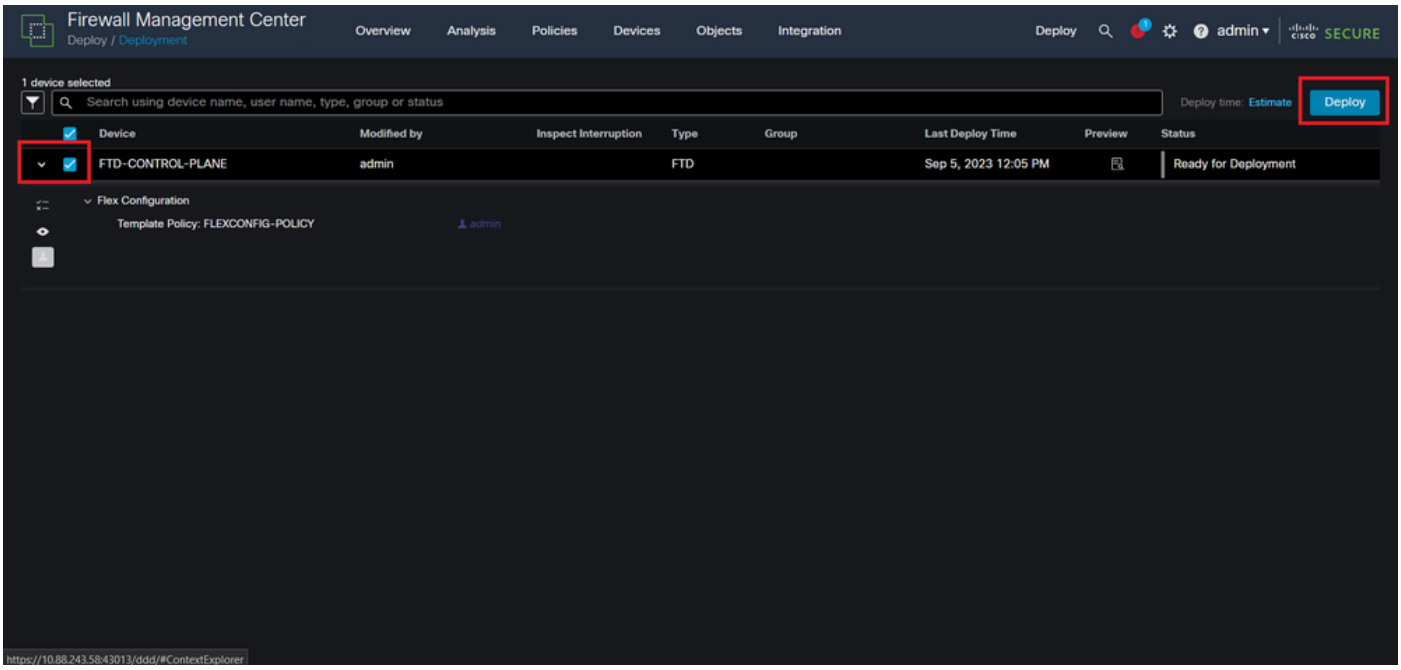

图 20.FTD部署验证

步骤 5.2之后，系统将弹出“部署确认”(Deployment Confirmation)窗口，添加注释以跟踪部署并继续部署。

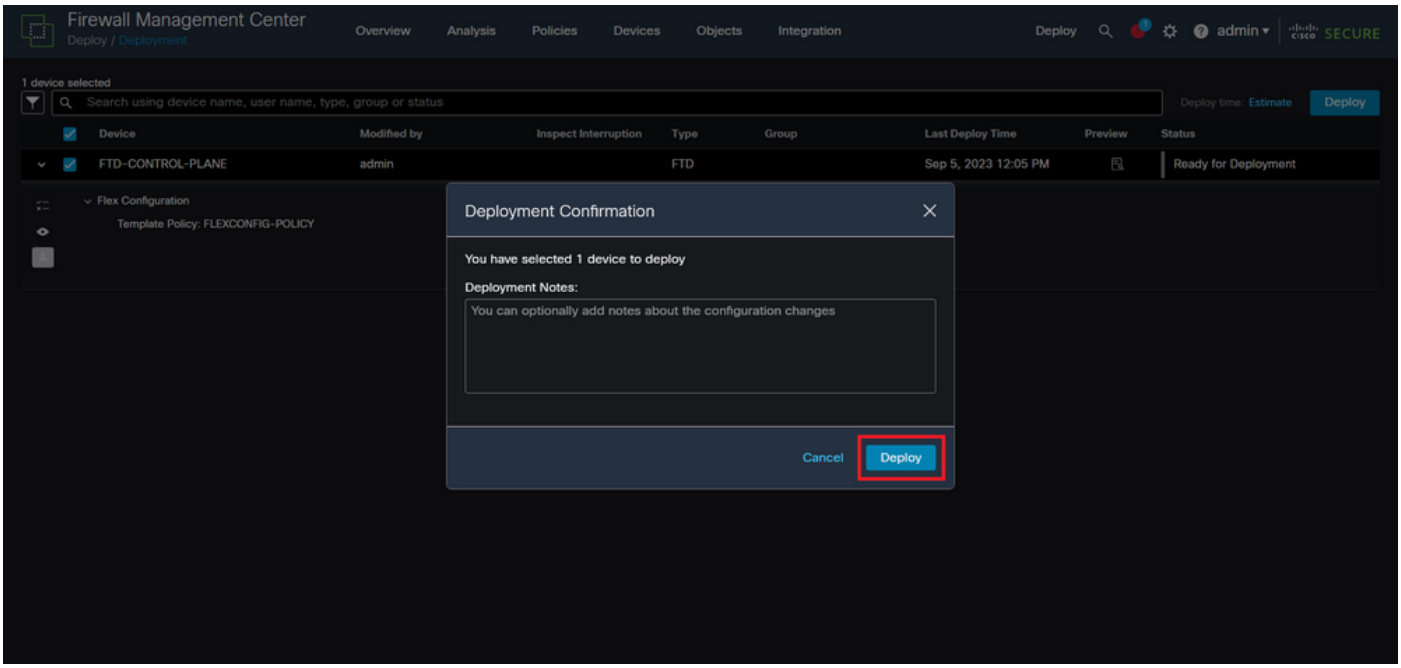

图 21.FTD部署注释

步骤 5.3部署FlexConfig更改时可能会出现警告消息。只有当您完全确定策略配置正确时，才点击Deploy。

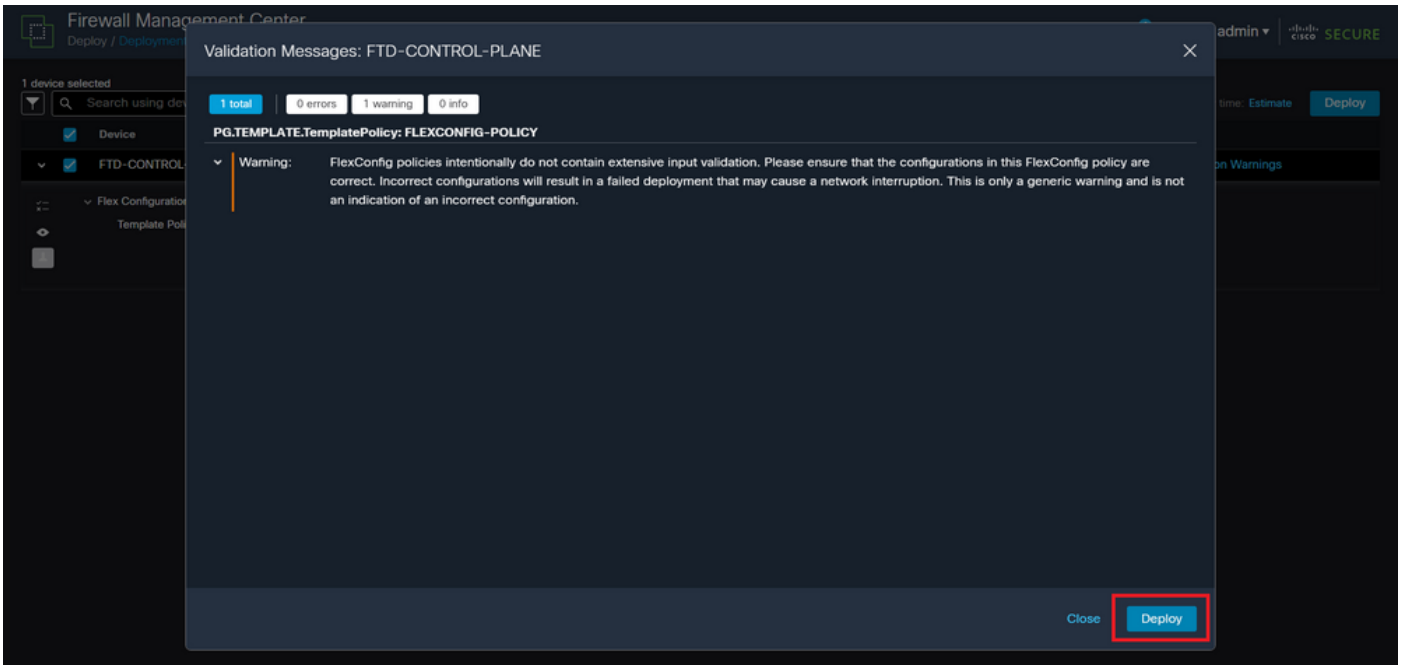

图 22.FTD部署Flexconfig警告

步骤 5.4确认FTD的策略部署成功。

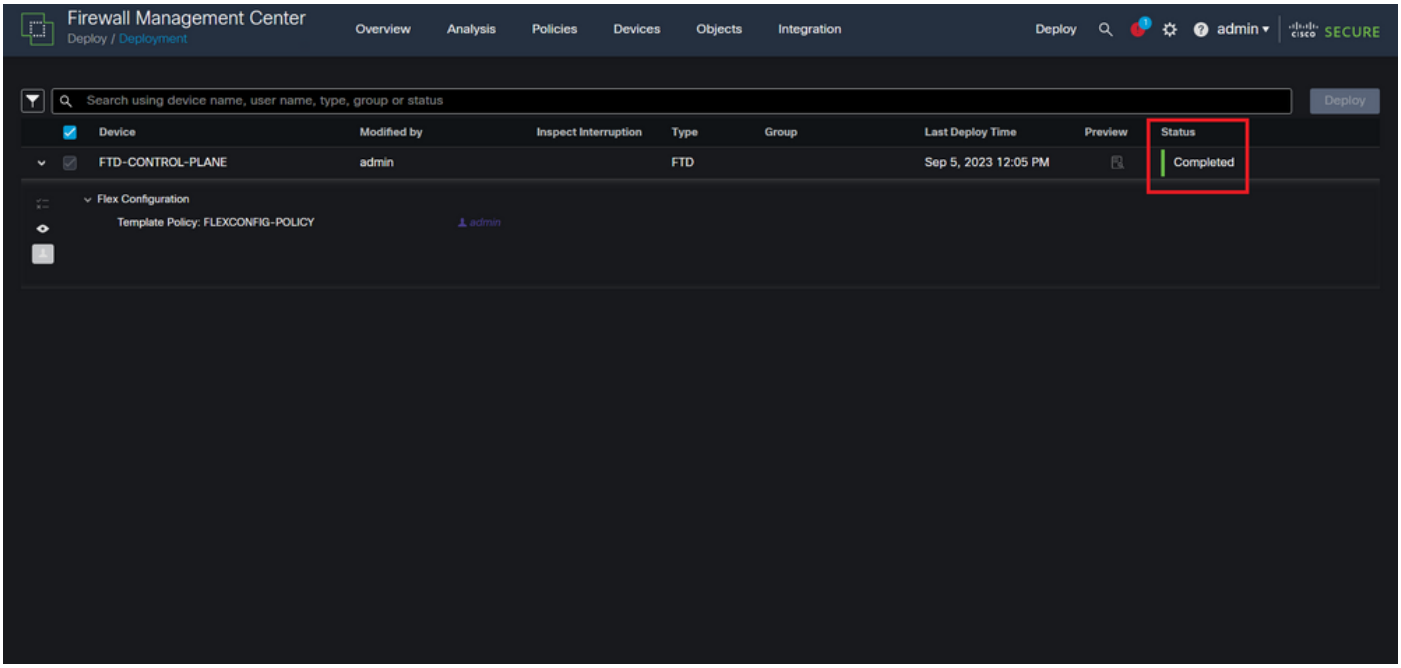

图 23.FTD部署成功

第六步： 如果为FTD创建新的控制平面ACL，或者编辑了正在使用的现有控制平面ACL，则必须强调所做的配置更改不适用于已建立的FTD连接，因此，您需要手动清除对FTD的活动连接尝试。为此，请连接到FTD的CLI并清除活动连接，如下所示。

要清除特定主机IP地址的活动连接，请执行以下操作：

```
> clear conn address 192.168.1.10 all
```

要清除整个子网网络的活动连接，请执行以下操作：

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

要清除IP地址范围的活动连接，请执行以下操作：

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

注意：强烈建议在clear conn address命令末尾使用关键字“all”强制清除对安全防火墙的活动VPN暴力连接尝试，主要当VPN暴力攻击的性质是不断发起大量连接尝试时。

为FDM管理的FTD配置控制平面ACL

在FDM中，您需要遵循以下步骤配置控制平面ACL以阻止传入VPN暴力攻击到外部FTD接口：

步骤1:通过HTTPS打开FDM GUI并使用您的凭据登录。

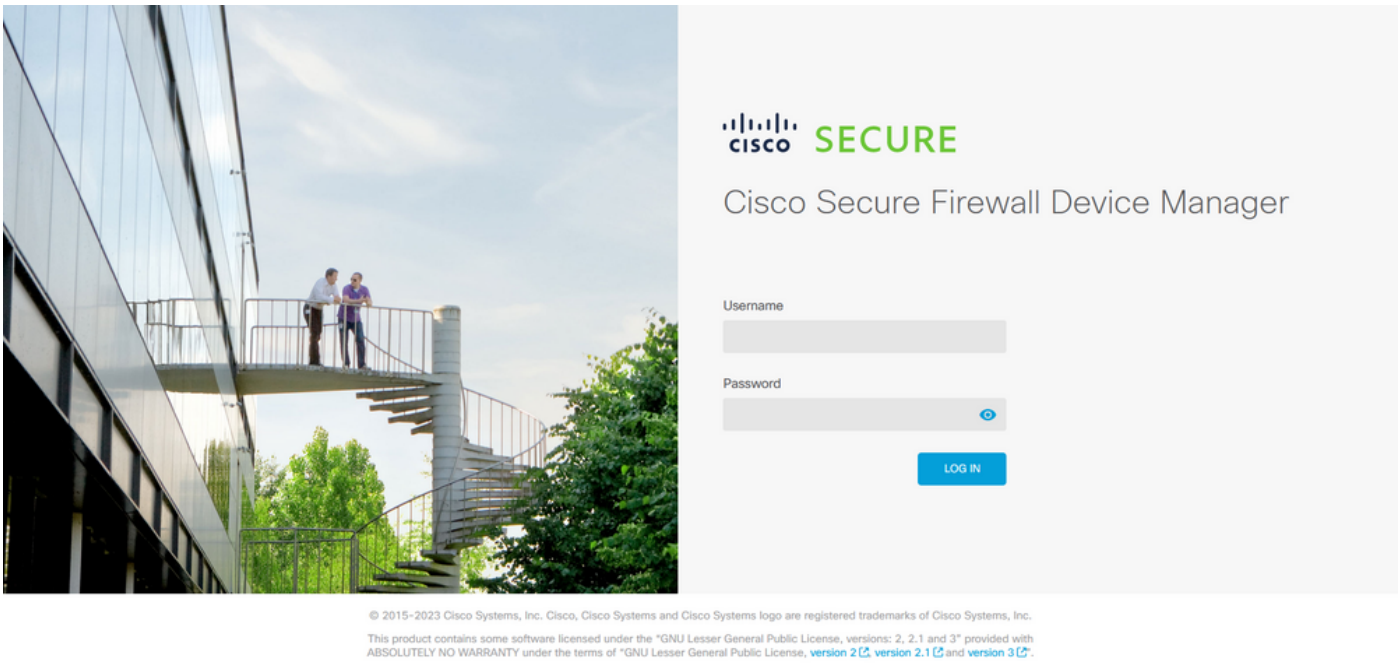

图 24.“FDM登录”页

第二步：您需要创建对象网络。为此，请导航至Objects:

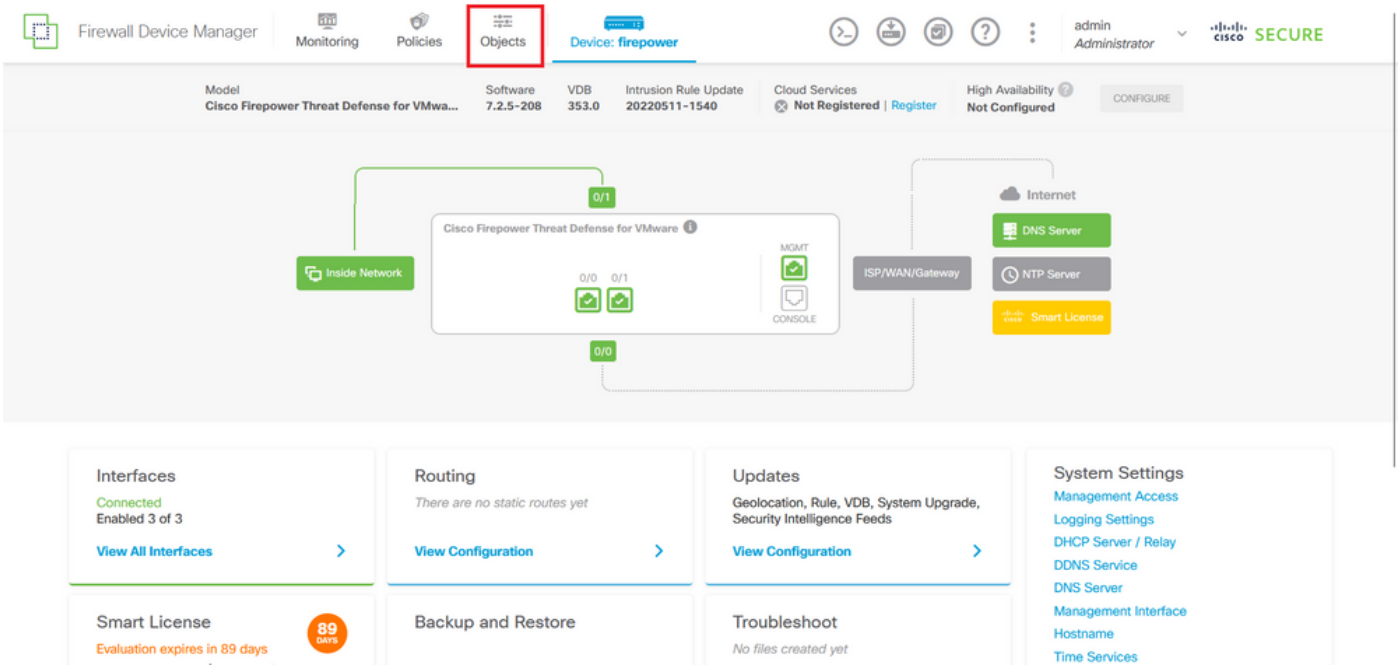

图 25.FDM主仪表板

步骤 2.1从左侧面板中选择Networks，然后单击“+”按钮以创建新的网络对象。

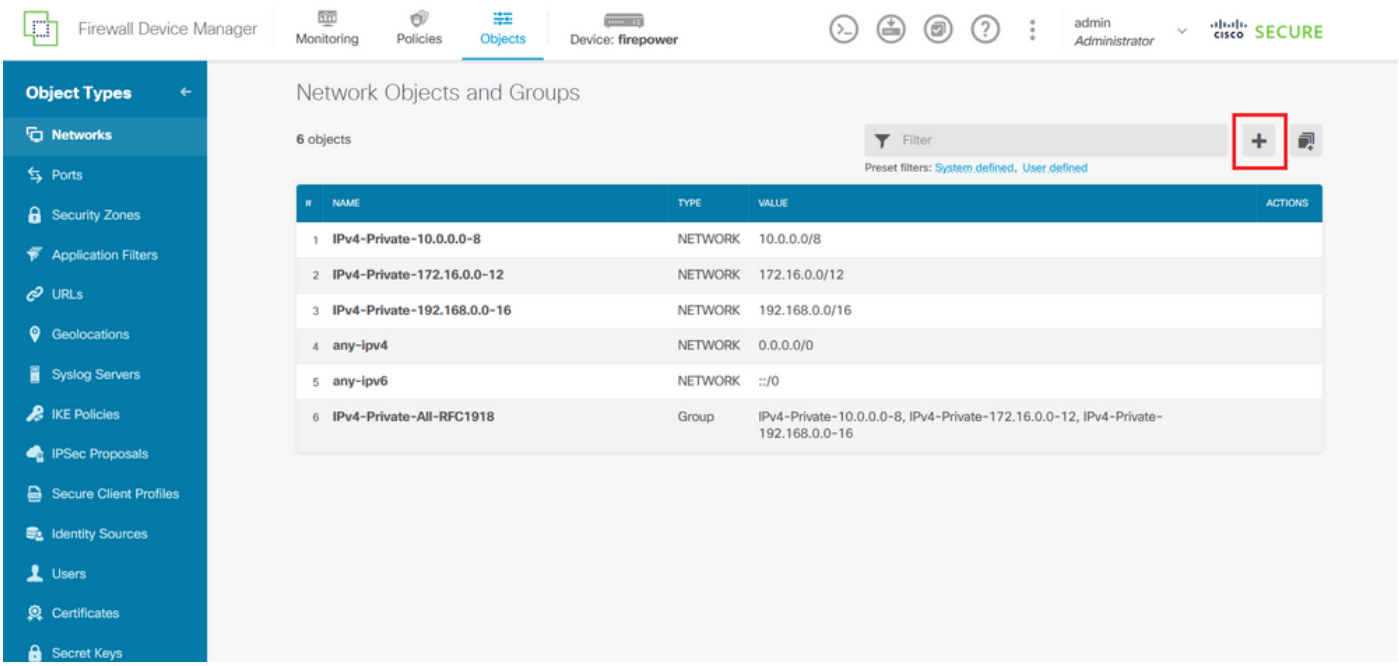

图 26.创建对象

步骤 2.2为网络对象添加名称，选择对象的Network类型，添加IP地址、网络地址或IP范围以匹配需要拒绝到FTD的流量。然后，单击“确定”(Ok)按钮完成对象网络。

— 在本示例中，配置的对象网络旨在阻止来自192.168.1.0/24子网的VPN暴力攻击。

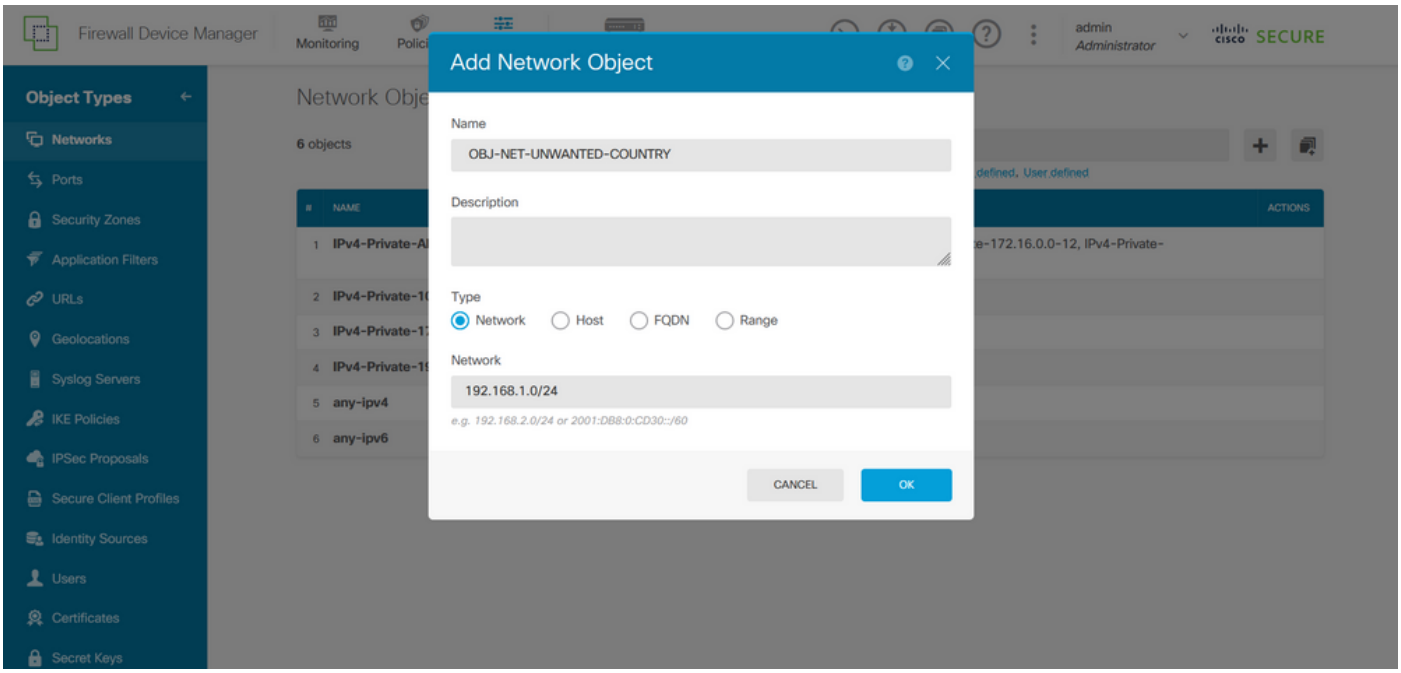

图 27.添加网络对象

第三步：然后，您需要创建一个扩展ACL，为此，请导航到顶部菜单中的Device选项卡。

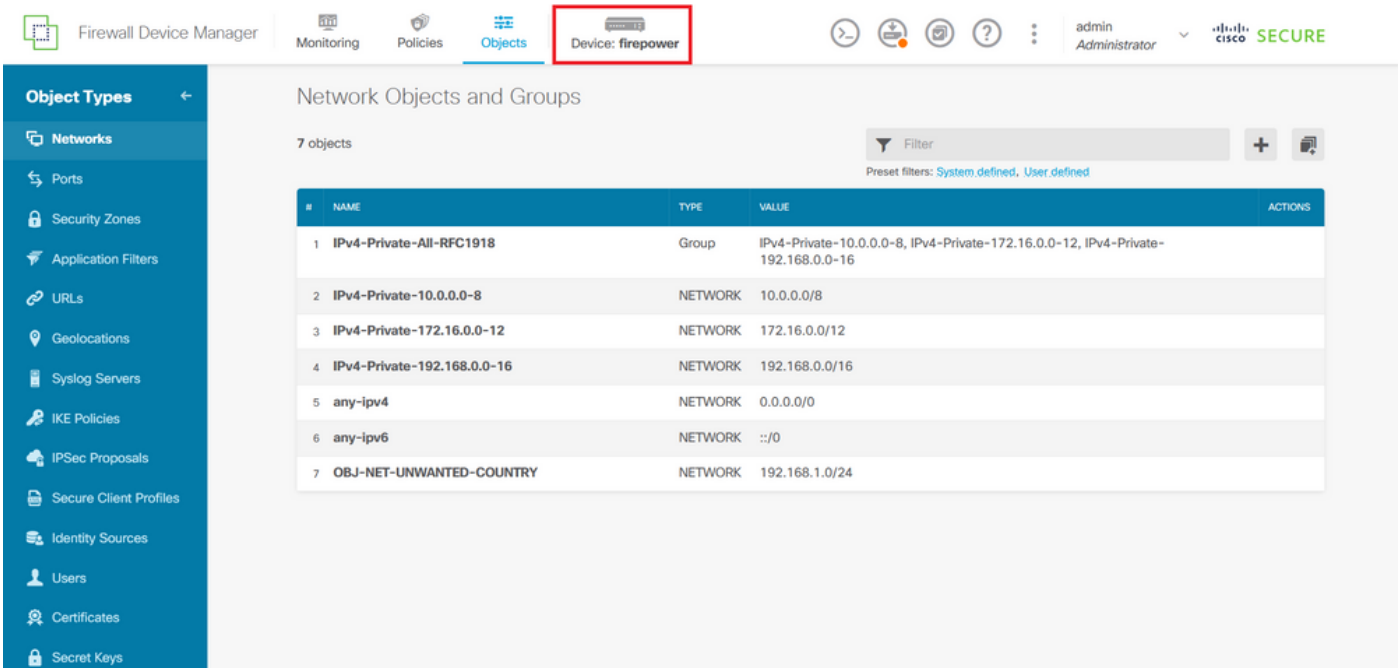

图 28.设备设置页面

步骤 3.1向下滚动并从高级配置方块中选择查看配置，如下所示。

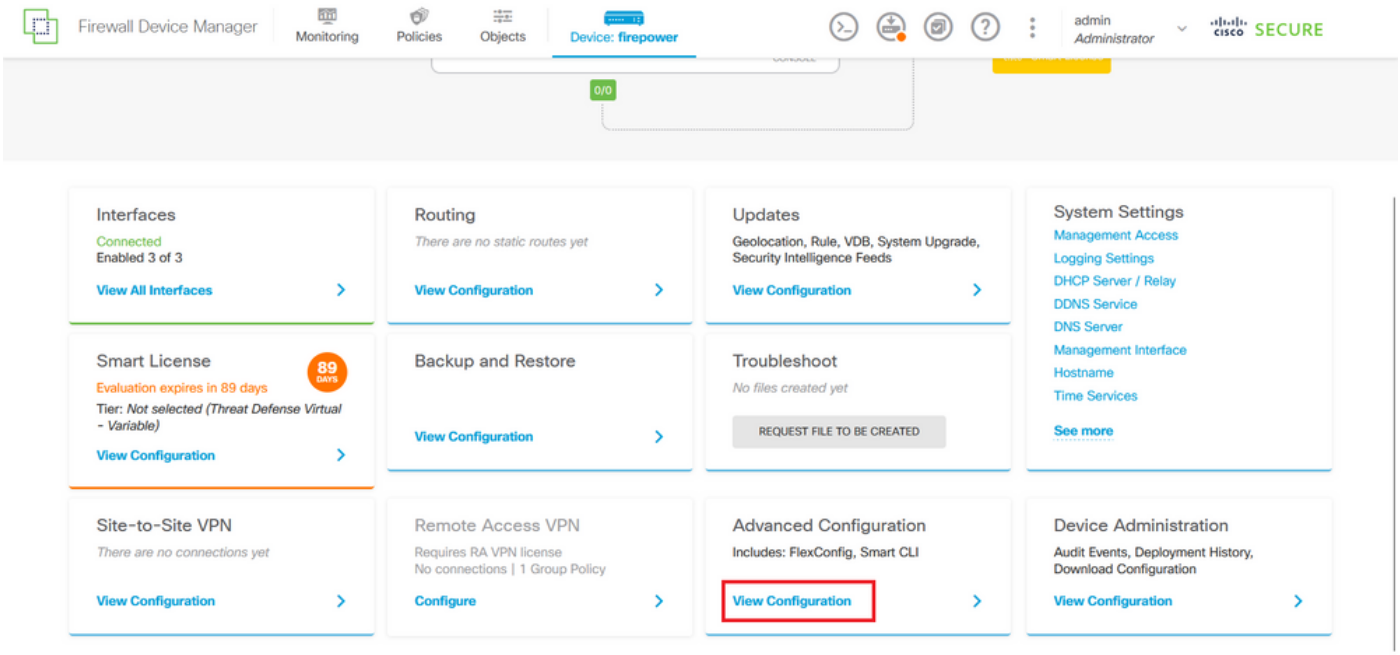

图 29.FDM高级配置

步骤 3.2然后，从左侧面板导航到Smart CLI > Objects，然后点击CREATE SMART CLI OBJECT。

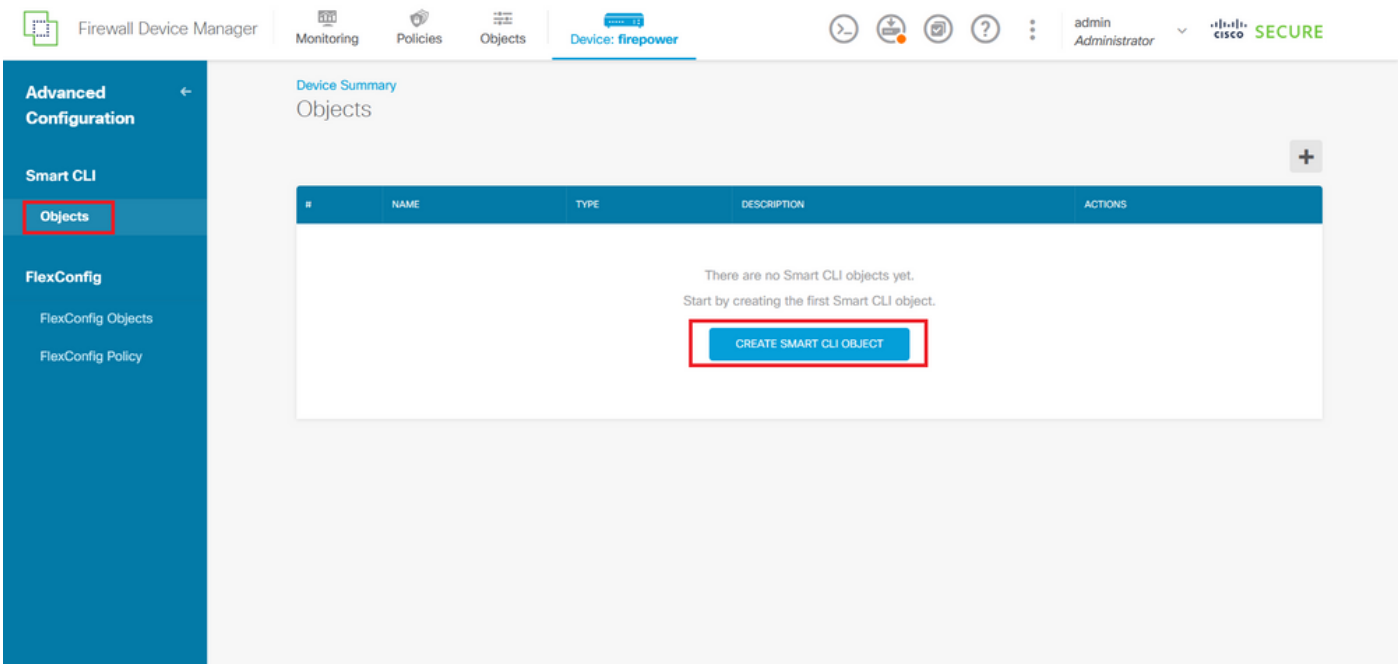

图 30.Smart CLI对象

步骤 3.3为要创建的扩展ACL添加名称，从CLI模板下拉菜单中选择Extended Access List，使用上述步骤2.2中创建的网络对象配置所需的ACE，然后点击OK按钮完成ACL。

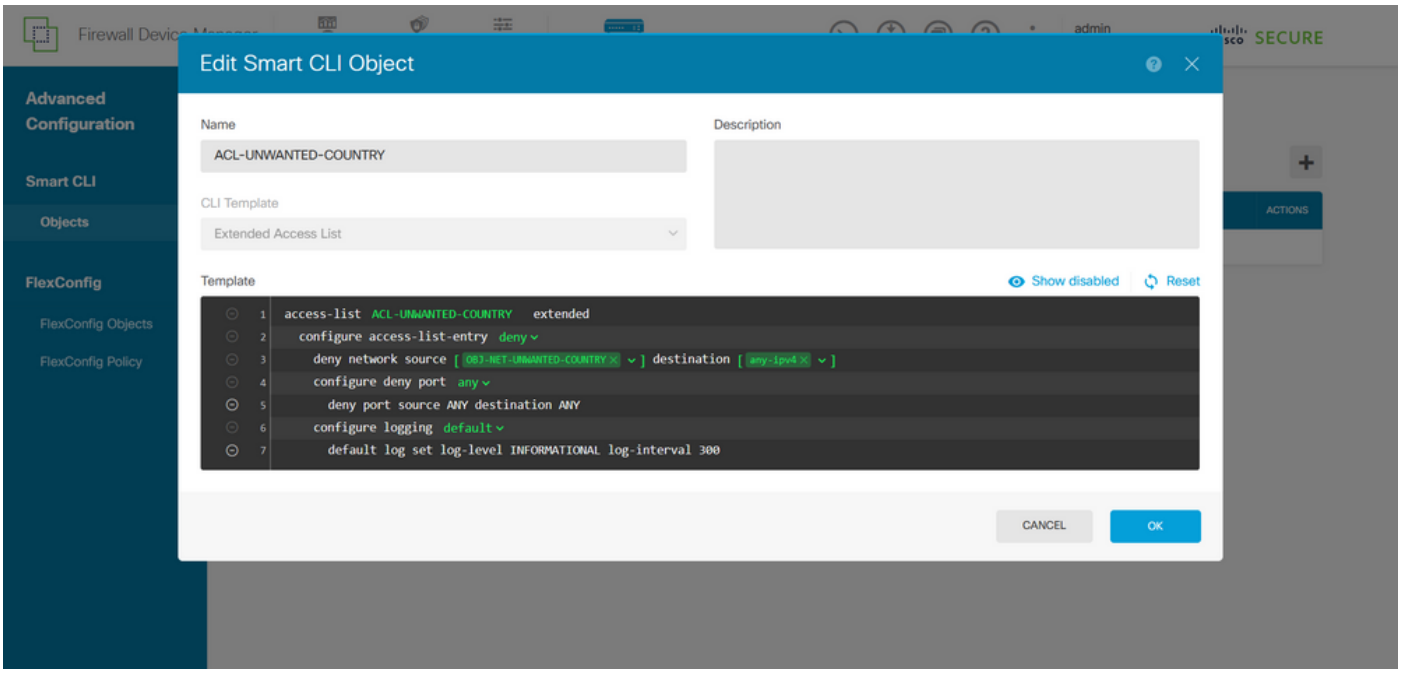

图 31.创建扩展ACL

> 注意：如果需要为ACL添加更多ACE，可以通过将鼠标悬停在当前ACE的左侧来执行此操作；然后将显示三个可点击的点。点击它们并选择复制(Duplicate)以添加更多ACE。

第四步：然后，您需要创建FlexConfig对象，为此，请导航到左侧面板并选择FlexConfig > FlexConfig Objects，然后点击CREATE FLEXCONFIG OBJECT。

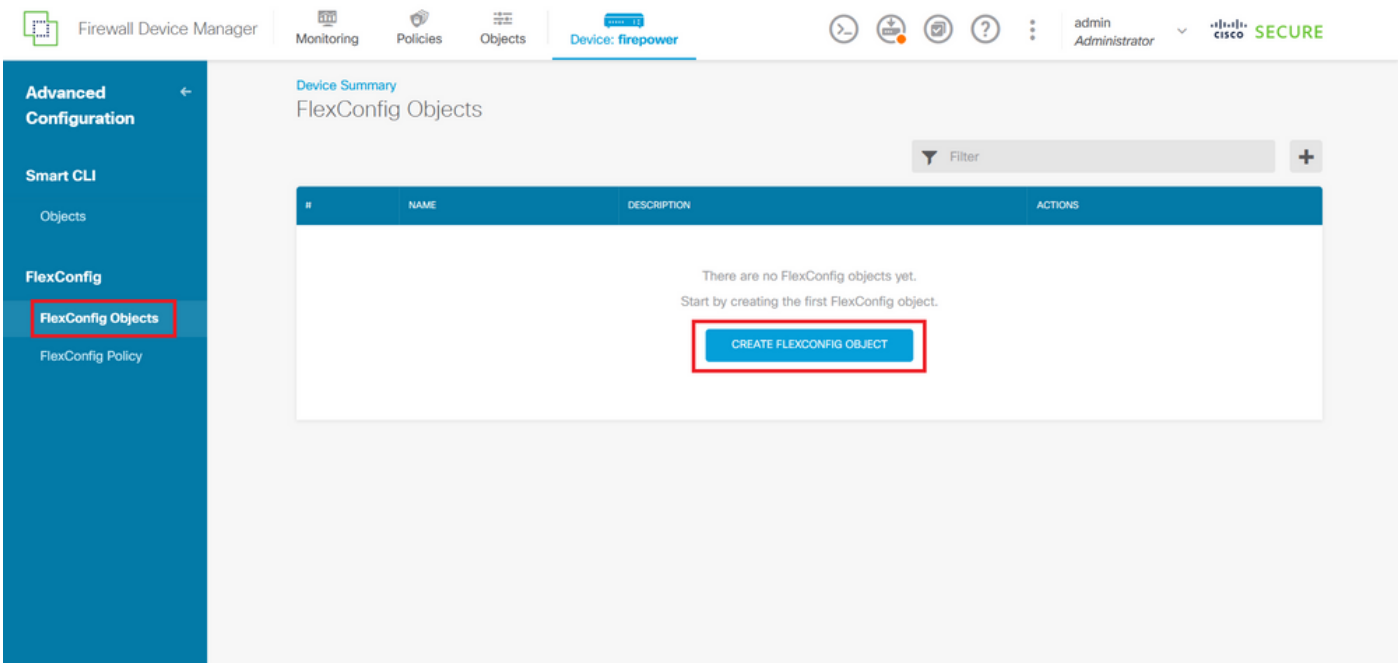

图 32.FlexConfig对象

步骤 4.1为FlexConfig对象添加名称，以创建控制平面ACL并将其配置为外部接口的入站流量，如下所示。

命令行语法：

```
access-group "ACL-name" in interface "interface-name" control-plane
```

这转换为下一个命令示例，该示例使用上述步骤3.3“ACL-UNWANTED-COUNTRY”中创建的扩展ACL，如下所示：

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

这是在FlexConfig对象窗口中配置该对象的方法，之后，选择“确定”(OK)按钮完成FlexConfig对象。

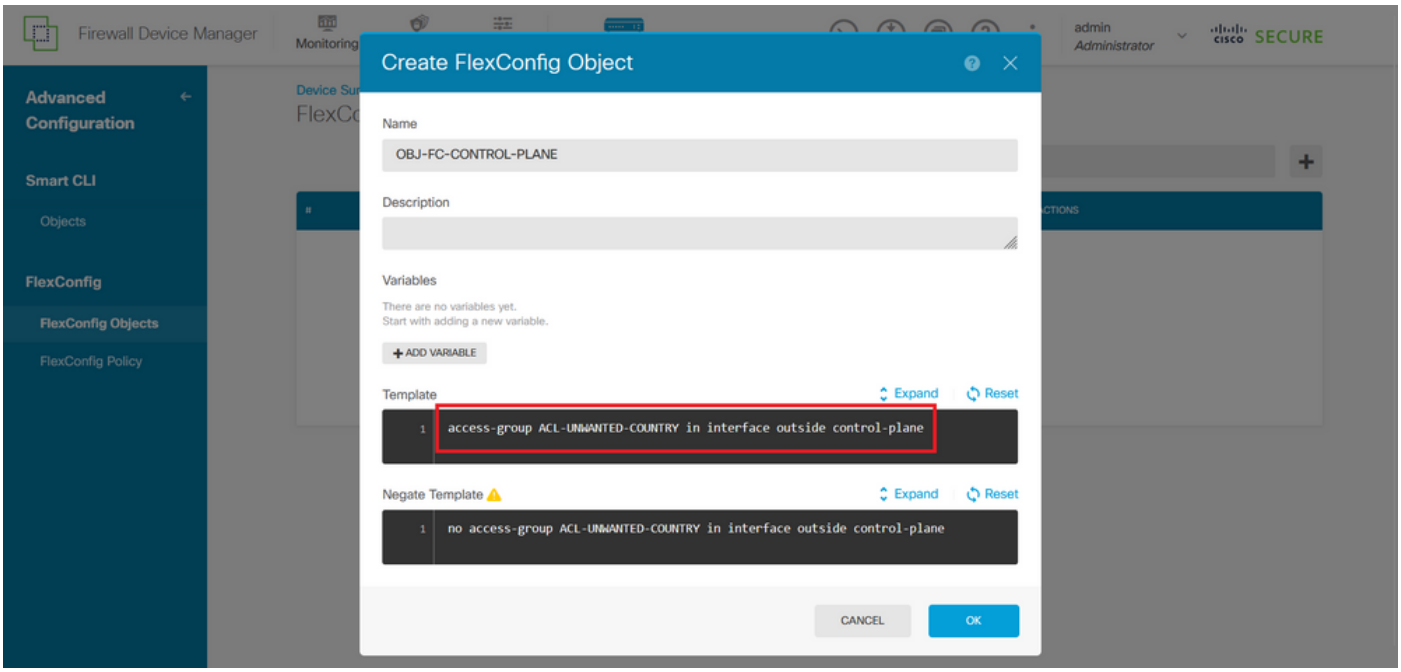

图 33.FlexConfig对象创建

第五步：继续创建FlexConfig策略，为此，请导航到Flexconfig > FlexConfig Policy，点击“+”按钮，并选择在上面的步骤4.1中创建的FlexConfig对象。

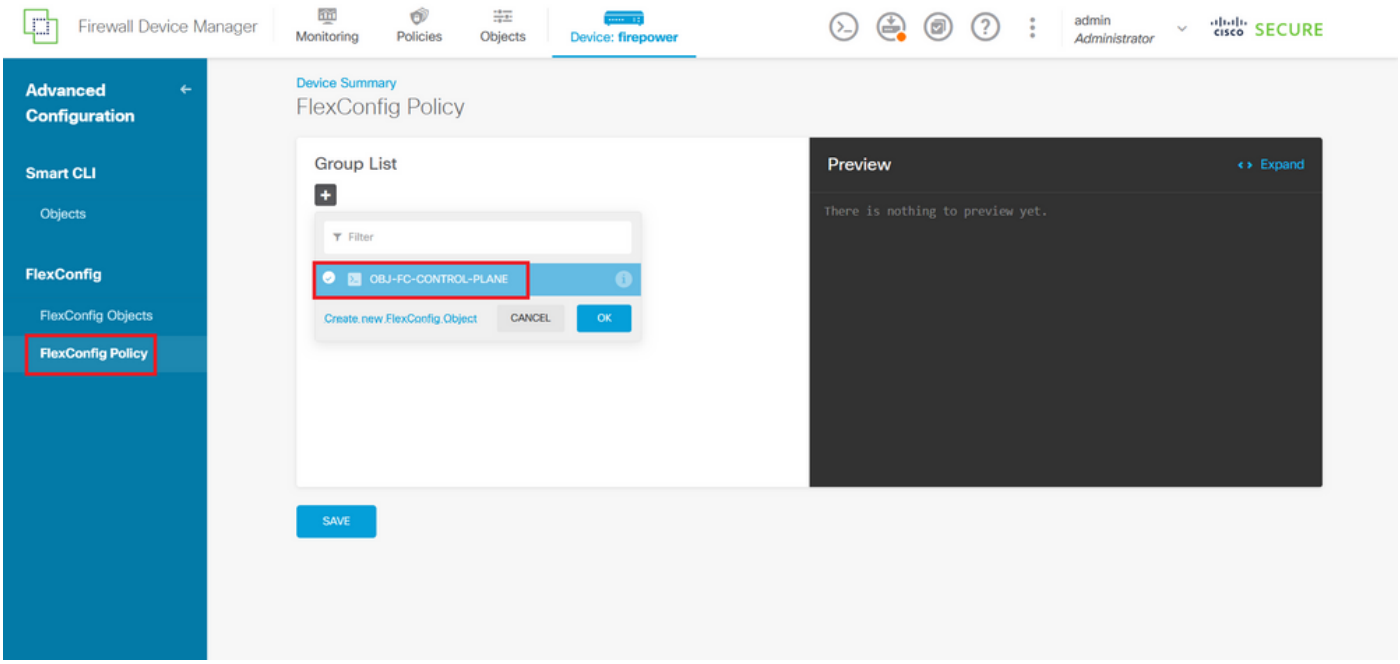

图 34.FlexConfig策略

步骤 5.1验证FlexConfig预览显示已创建的控制平面ACL的正确配置，然后点击Save按钮。

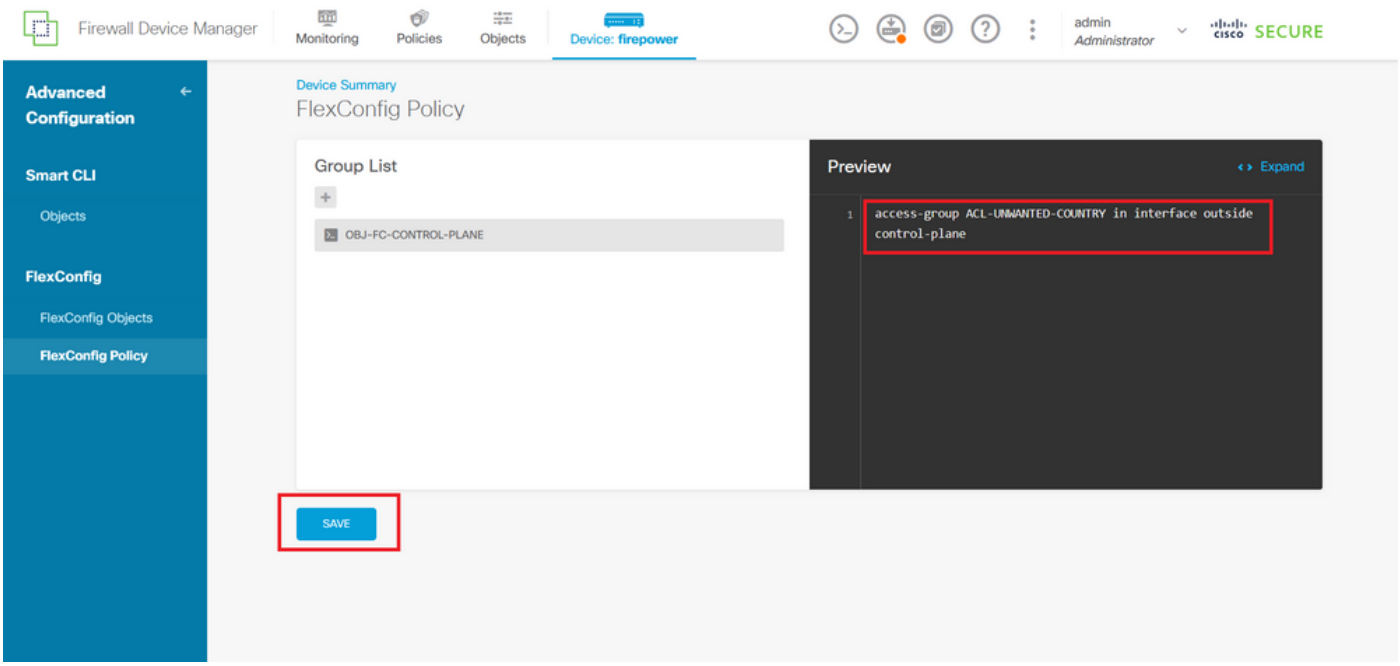

图 35.FlexConfig策略预览

第六步：将配置更改部署到要防御VPN暴力攻击的FTD，为此，请点击顶部菜单中的Deployment按钮，验证要部署的配置更改是否正确，然后点击DEPLOY NOW。

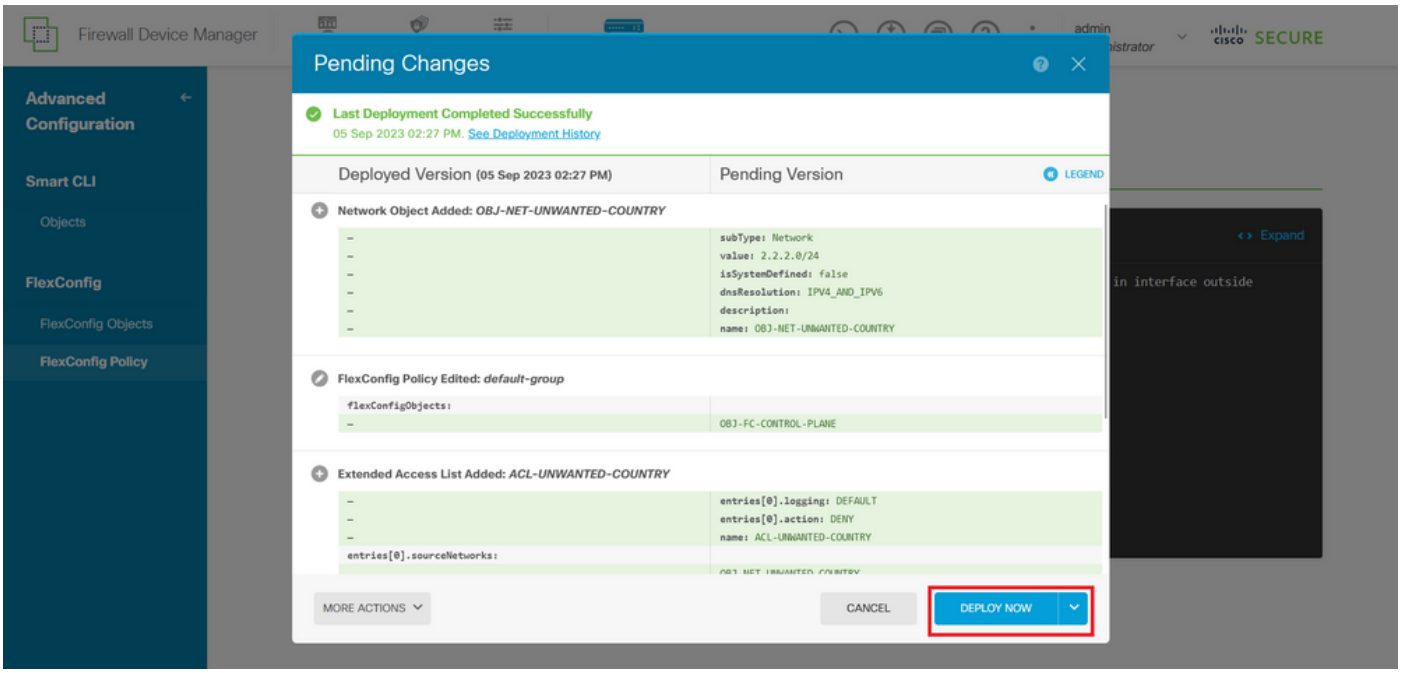

图 36.待定部署

步骤 6.1验证策略部署是否成功。

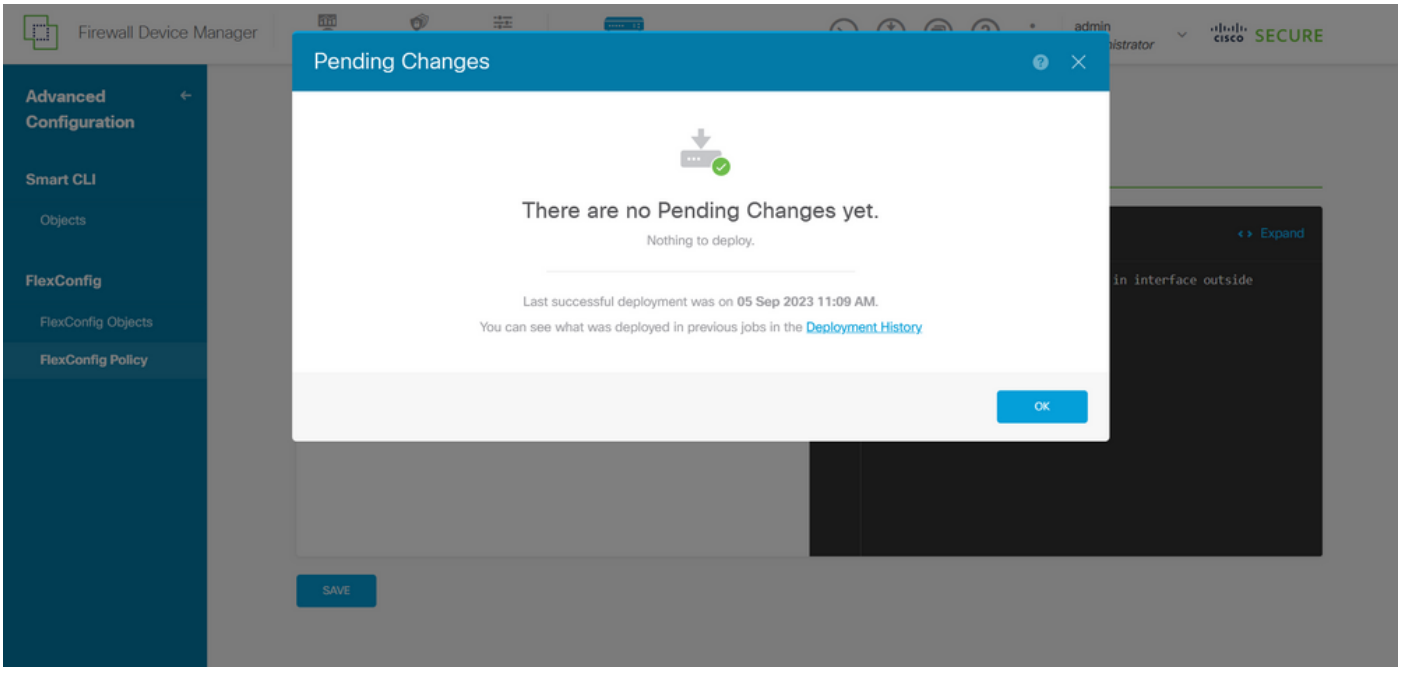

图 37.部署成功

步骤 7. 如果为FTD创建新的控制平面ACL，或者编辑了正在使用的现有控制平面ACL，则必须强调所做的配置更改不适用于已建立的FTD连接，因此，您需要手动清除对FTD的活动连接尝试。为此，请连接到FTD的CLI并清除活动连接，如下所示。

要清除特定主机IP地址的活动连接，请执行以下操作：

```
> clear conn address 192.168.1.10 all
```

要清除整个子网网络的活动连接，请执行以下操作：

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

要清除IP地址范围的活动连接，请执行以下操作：

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

注意：强烈建议在clear conn address命令末尾使用关键字“all”强制清除对安全防火墙的活动VPN暴力连接尝试，主要当VPN暴力攻击的性质是不断发起大量连接尝试时。

使用CLI为ASA配置控制平面ACL

您需要在ASA CLI中按照以下步骤配置控制平面ACL以阻止传入VPN暴力攻击到外部接口：

步骤1:通过CLI登录安全防火墙ASA，然后按如下方式访问“configure terminal”。

```
asa# configure terminal
```

第二步：使用next命令配置扩展ACL，以阻止需要阻止到ASA的流量的主机IP地址或网络地址。

— 在本示例中，您将创建一个名为“ACL-UNWANTED-COUNTRY”的新ACL，并且配置的ACE条目将阻止来自192.168.1.0/24子网的VPN暴力攻击。

```
asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

第三步：使用next access-group命令将“ACL-UNWANTED-COUNTRY”ACL配置为外部ASA接口的控制平面ACL。

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

第四步： 如果创建新的控制平面ACL或编辑了正在使用的现有控制平面ACL，则必须强调所做的配

置更改不适用于已建立的与ASA的连接，因此，您需要手动清除对ASA的活动连接尝试。为此，请清除活动连接，如下所示。

要清除特定主机IP地址的活动连接，请执行以下操作：

```
asa# clear conn address 192.168.1.10 all
```

要清除整个子网网络的活动连接，请执行以下操作：

```
asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

要清除IP地址范围的活动连接，请执行以下操作：

```
asa# clear conn address 192.168.1.1-192.168.1.10 all
```

注意：强烈建议在clear conn address命令末尾使用关键字“all”强制清除对安全防火墙的活动VPN暴力连接尝试，主要当VPN暴力攻击的性质是不断发起大量连接尝试时。

使用“shun”命令阻止安全防火墙攻击的备用配置

如果立即选择阻止安全防火墙的攻击，则可以使用“shun”命令。通过thhuncommand，可以阻止来自攻击主机的连接。

— 一旦您避开了IP地址，来自源IP地址的所有未来连接都会被丢弃并记录，直到手动删除阻止功能为止。

- theshuncommand的阻止功能适用于具有指定主机地址的连接当前是否处于活动状态。

— 如果指定目标地址、源端口和目标端口以及协议，则丢弃匹配的连接，并对来自源IP的所有未来连接设置一个避开值

地址；避免将来的所有连接，而不仅仅是那些匹配这些特定连接参数的连接。

— 每个源IP地址只能使用oneshuncommand。

— 由于theshuncommand用于动态阻止攻击，因此它不会显示在威胁防御设备配置中。

— 每次删除接口配置时，也会删除连接到该接口的所有分路。

- shun命令语法：

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

— 要禁用回避，请使用此命令的no形式：

```
no shun source_ip [ vlan vlan_id]
```

要避开主机IP地址，请按照以下步骤操作安全防火墙。 在本示例中，“shun”命令用于阻止来自源IP地址192.168.1.10的VPN暴力攻击。

FTD的配置示例。

步骤1:通过CLI登录FTD并应用shun命令，如下所示。

```
<#root>

>

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

第二步： 您可以使用以下show命令确认FTD中的shun IP地址并监控每个IP地址的shun命中数：

```
<#root>

>

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0

>

show shun statistics

diagnostic=OFF, cnt=0
outside=ON, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

ASA配置示例

步骤1:通过CLI登录到ASA并应用shun命令，如下所示。

```
<#root>

asa#

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf


Shun 192.168.1.10 successful
```

第二步： 您可以使用以下show命令确认ASA中的shun IP地址并监控每个IP地址的shun命中数：

```
<#root>

asa#

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0

asa#

show shun statistics

outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
mgmt=OFF, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:01:39)
```

注意：有关secure firewall shun命令的详细信息，请查看Cisco Secure Firewall Threat Defense Command Reference

验证

要确认安全防火墙的控制平面ACL配置已就绪，请继续操作：

步骤1:通过CLI登录到安全防火墙并运行以下命令以确认控制平面ACL配置已应用。

FMC管理的FTD的输出示例：

<#root>

>

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

>

show running-config access-group

OUTPUT OMITTED FOR BREVITY
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

FDM管理的FTD的输出示例：

<#root>

> show running-config object id OBJ-NET-UNWANTED-COUNTRY

object network OBJ-NET-UNWANTED-COUNTRY
subnet 192.168.1.0 255.255.255.0

>

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default

> show running-config access-group

OUTPUT OMITTED FOR BREVITY
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

ASA的输出示例：

<#root>

asa#

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

asa#

show running-config access-group

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

第二步： 要确认控制平面ACL阻止了所需的流量，请使用packet-tracer命令模拟到安全防火墙外部接口的传入TCP 443连接，然后使用show access-list <acl-name> 命令，每次控制平面ACL阻止到安全防火墙的VPN暴力连接时，ACL命中计数都会增加：

— 在本示例中，packet-tracer命令模拟从主机192.168.1.10发往安全防火墙外部IP地址的传入TCP 443连接。“packet-tracer”输出确认流量被丢弃，而“show access-list”输出显示已设置的控制平面ACL的命中计数增量：

FTD的输出示例

<#root>

>

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443

Phase: 1
Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 21700 ns
Config:
Additional Information:

Result:
input-interface: outside(vrfid:0)
input-status: up
input-line-status: up

Action: drop

Time Taken: 21700 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA

>

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf

ASA的输出示例

<#root>

```
asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 19688 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 17833 ns
Config:
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up

Action: drop

Time Taken: 37521 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA

asa#

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any

(hitcnt=1)

 0x9b4d26ac
```

注意：如果在安全防火墙中实施类似Cisco安全客户端VPN的RAVPN解决方案，则可能会执行到安全防火墙的真实连接尝试，以确认控制平面ACL是否如预期一样工作，从而阻止所需的流量。

相关 Bug

- 增强版 | 基于地理位置的AnyConnect客户端连接:Cisco Bug ID CSCvs65322

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）。