为安全FTD和ASA配置控制平面访问控制

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 安全防火墙直通流量
- 保护防火墙到设备的流量
- 有关控制平面ACL的重要注意事项

配置

- 配置
  - 为FMC管理的FTD配置控制平面ACL
  - [视频]为FMC管理的FTD配置控制平面ACL
  - 为FDM管理的FTD配置控制平面ACL
  - 使用CLI为ASA配置控制平面ACL
  - 用于阻止运行Shun的安全防火墙攻击的备用配置
  - FTD配置示例
  - ASA配置示例

验证

- ASA的输出示例

相关 Bug

相关信息

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：

- Secure Firewall Threat Defense (FTD)
- 安全防火墙设备管理器(FDM)
- Secure Firewall Management Center (FMC)

- Secure Firewall 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版本9.18.3

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“到”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何时可用于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）隧道的示例。

安全防火墙直通流量

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），这称为通过设备流量，由访问控制策略(ACP)和预过滤器规则进行管理。

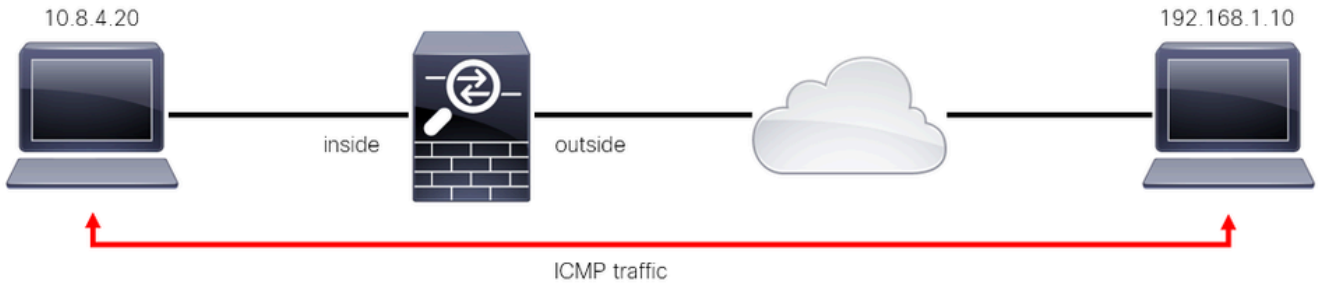


图1.通过设备的流量示例

保护防火墙到设备的流量

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），这称为流向设备的流量，由特定接口的控制平面进行管理。

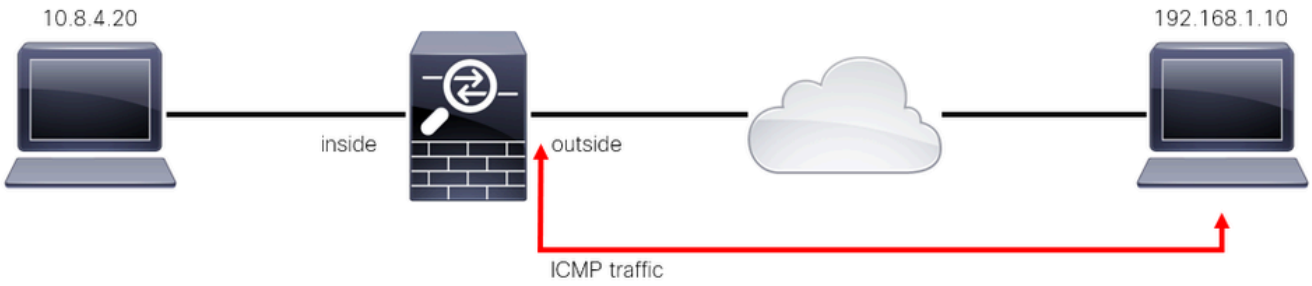


图2.流向设备的流量示例

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，使用与ASA上相同的命令语法。
- 关键词控制平面附加到访问组配置中，用于实施到安全防火墙接口的流量。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不会限制安全防火墙接口的SSH、ICMP或TELNET入站流量。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限制流向安全防火墙本身的流量，而FTD的访问控制策略或ASA的正常ACL控制通过安全防火墙的流量。
- 与普通ACL不同，ACL的末尾没有隐式“deny”语句。
- 对象组搜索(OGS)功能无法控制平面ACL，请参阅Cisco Bug ID CSCwi58818。
- 在创建本文档时，FTD地理位置功能不能用于限制对FTD的访问。

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FTD RAVPN来通过VPN强行进入网络。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中必须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：

第1步：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

步骤2.您必须创建扩展ACL。为此，请导航到对象>对象管理:

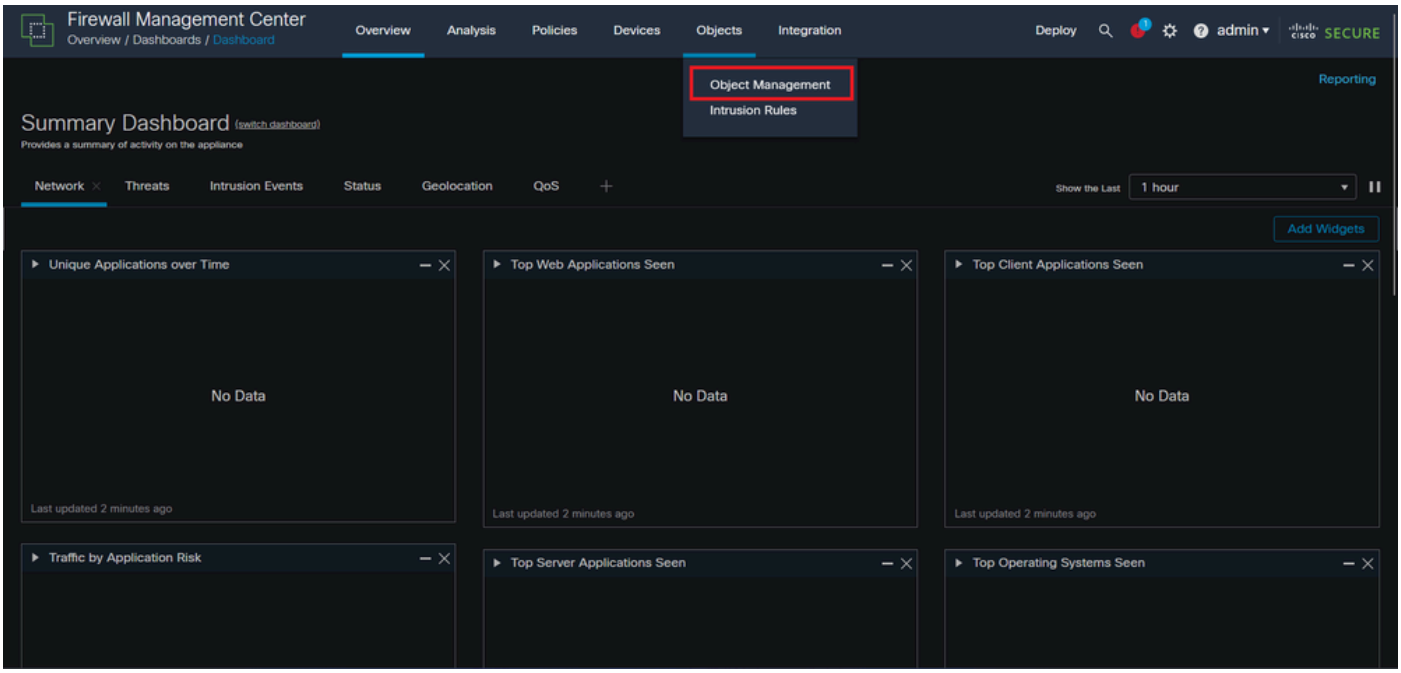


图4.对象管理

步骤2.1.从左侧面板导航到Access List > Extended以创建扩展ACL:

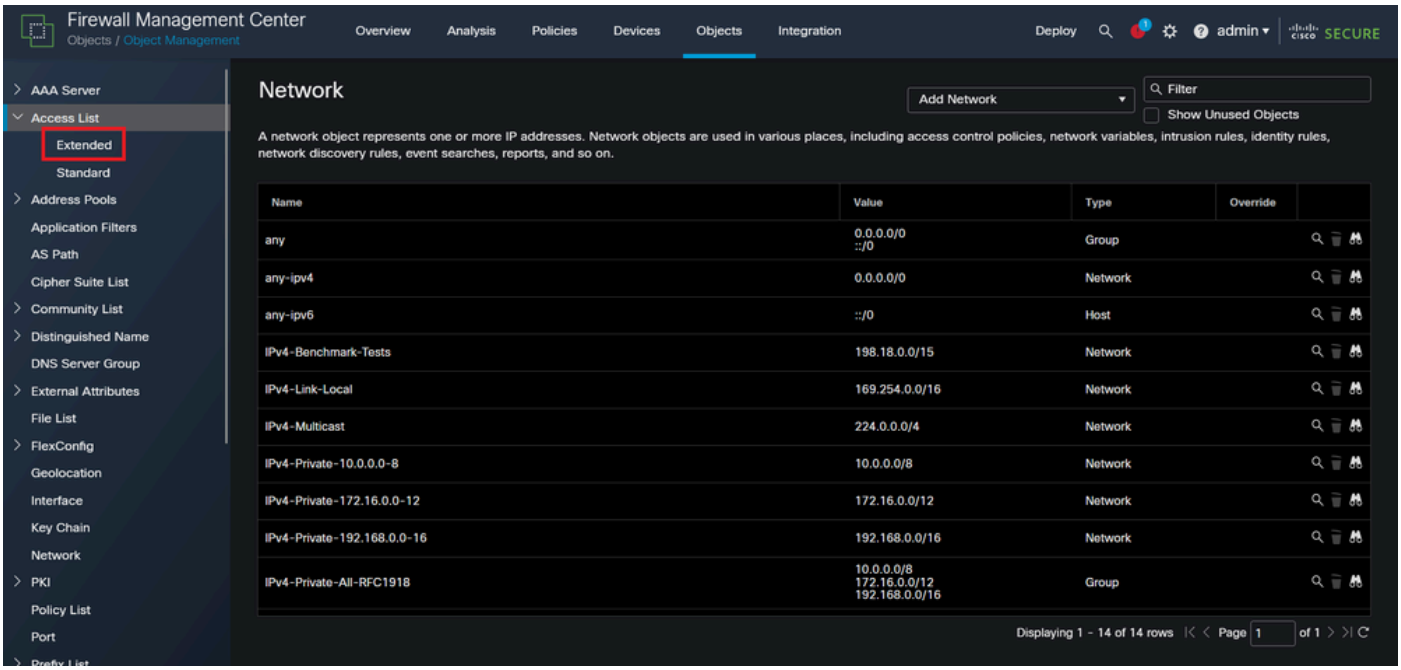


图5.扩展ACL菜单

第2.2步：选择Add Extended Access List:

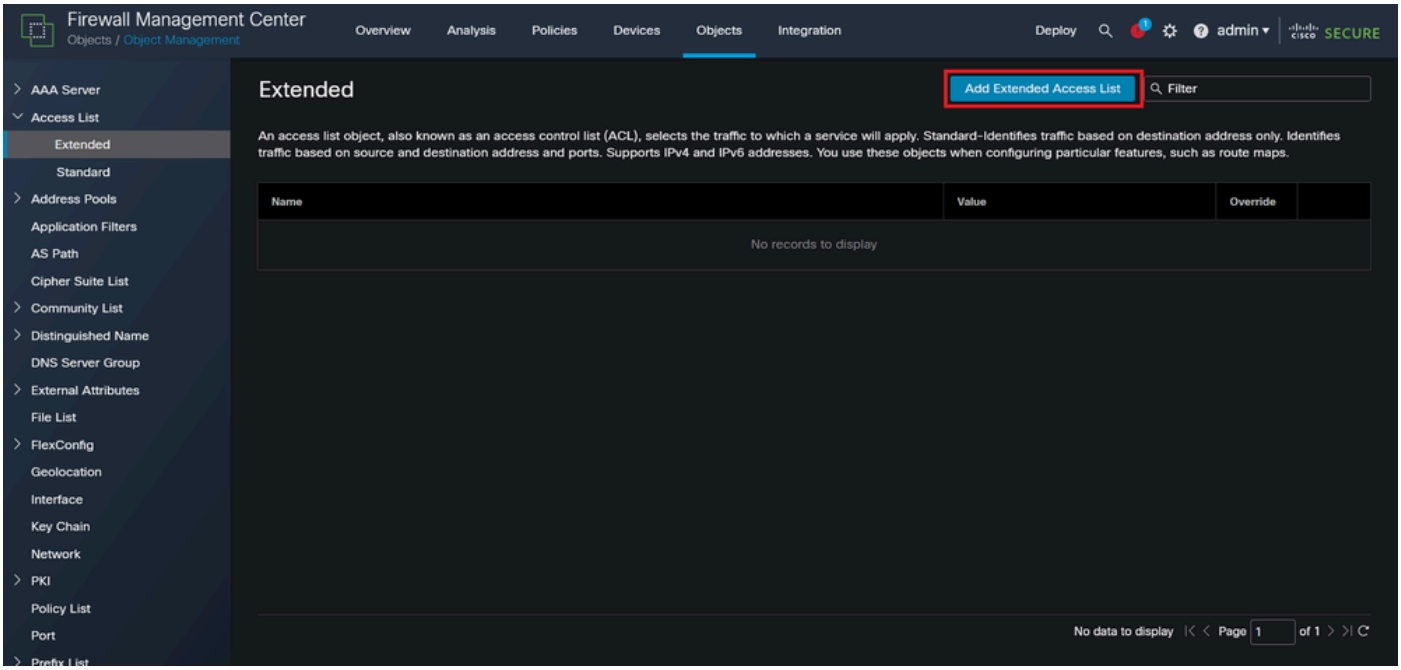


图6.添加扩展ACL

第2.3步：键入扩展ACL的名称，然后单击Add按钮以创建访问控制条目(ACE):

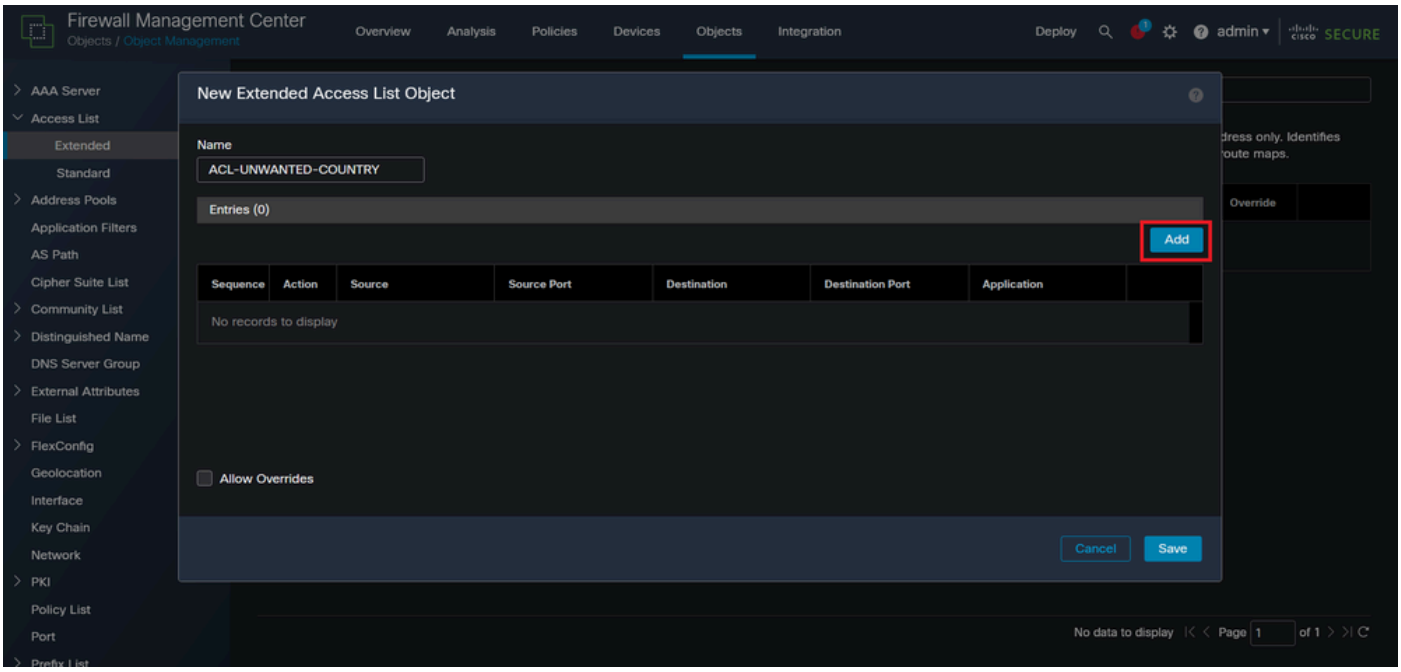


图7.扩展ACL条目

第2.4步：将ACE操作更改为Block，然后添加源网络以匹配必须拒绝到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条目阻止来自192.168.1.0/24子网的VPN暴力攻击：

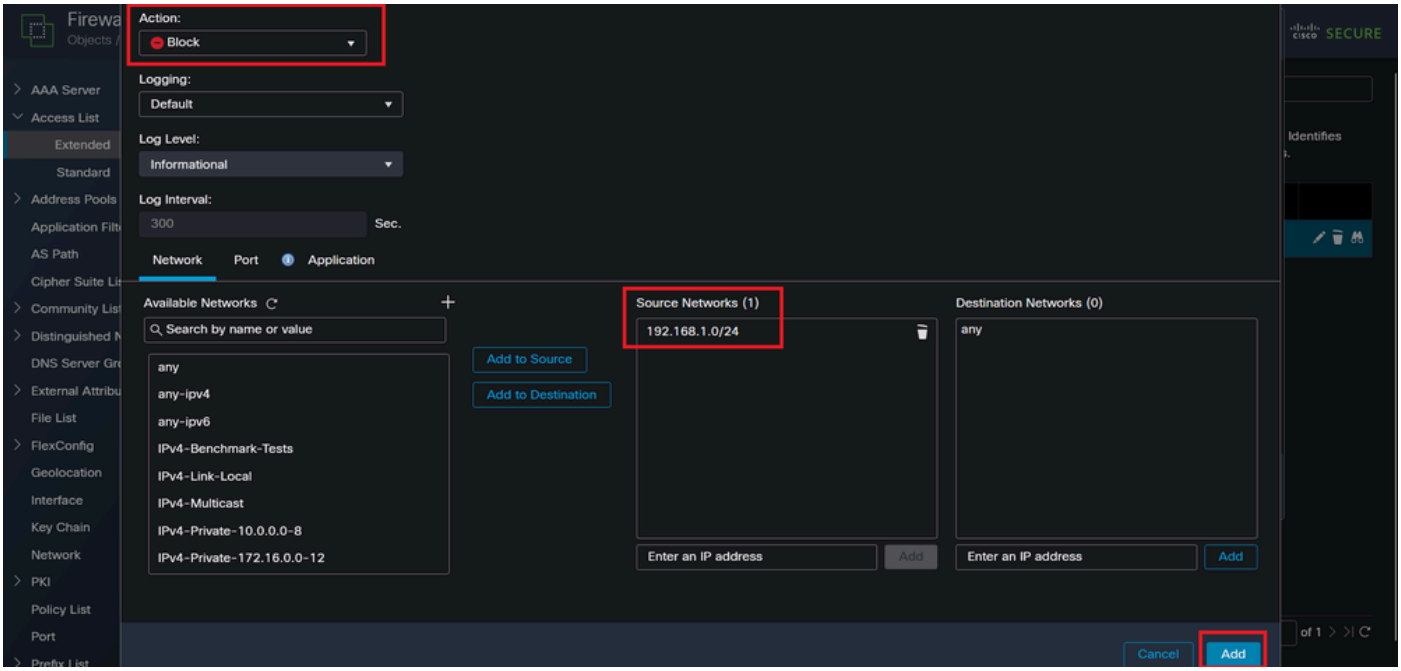


图8.拒绝的网络

第2.5步。如果需要添加更多ACE条目，请再次单击Add按钮，然后重复第2.4步。在此之后，单击Save按钮完成ACL配置：

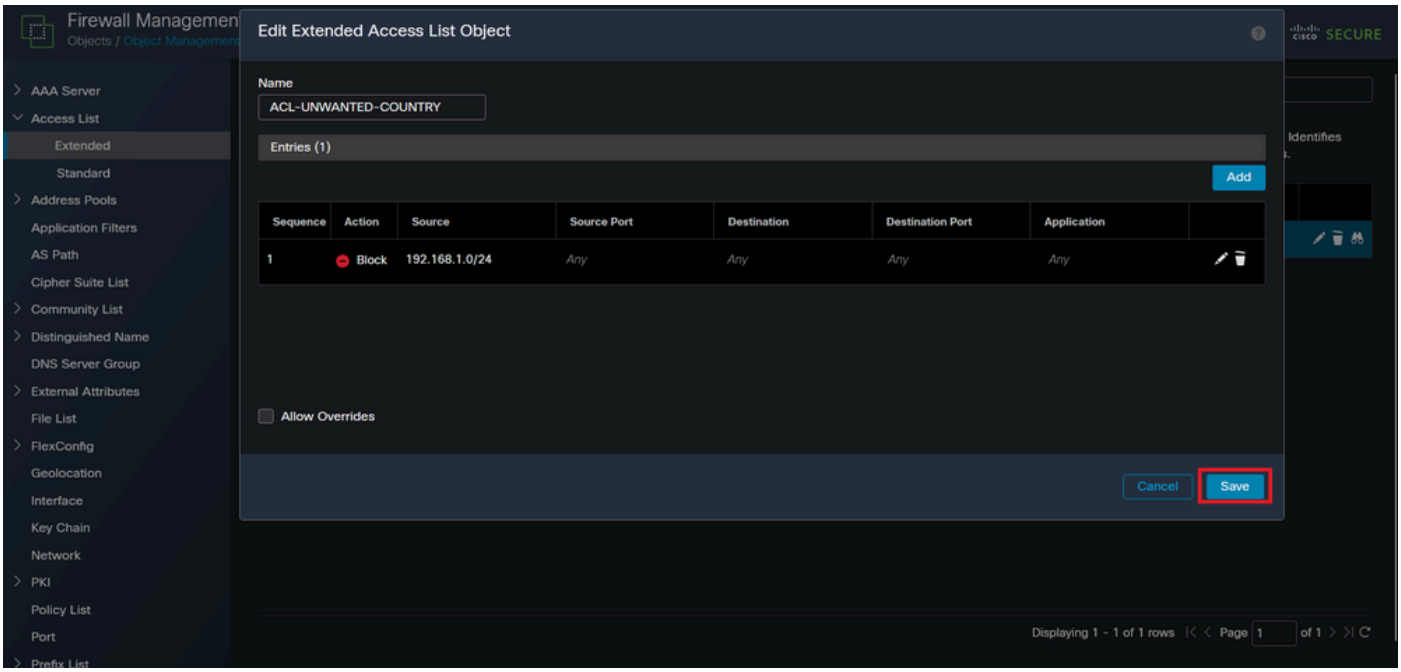


图9.完成的扩展ACL条目

步骤3.下一步，必须配置Flex-Config对象以将控制平面ACL应用于外部FTD接口。导航到左侧面板，然后选择选项FlexConfig > FlexConfig Object。

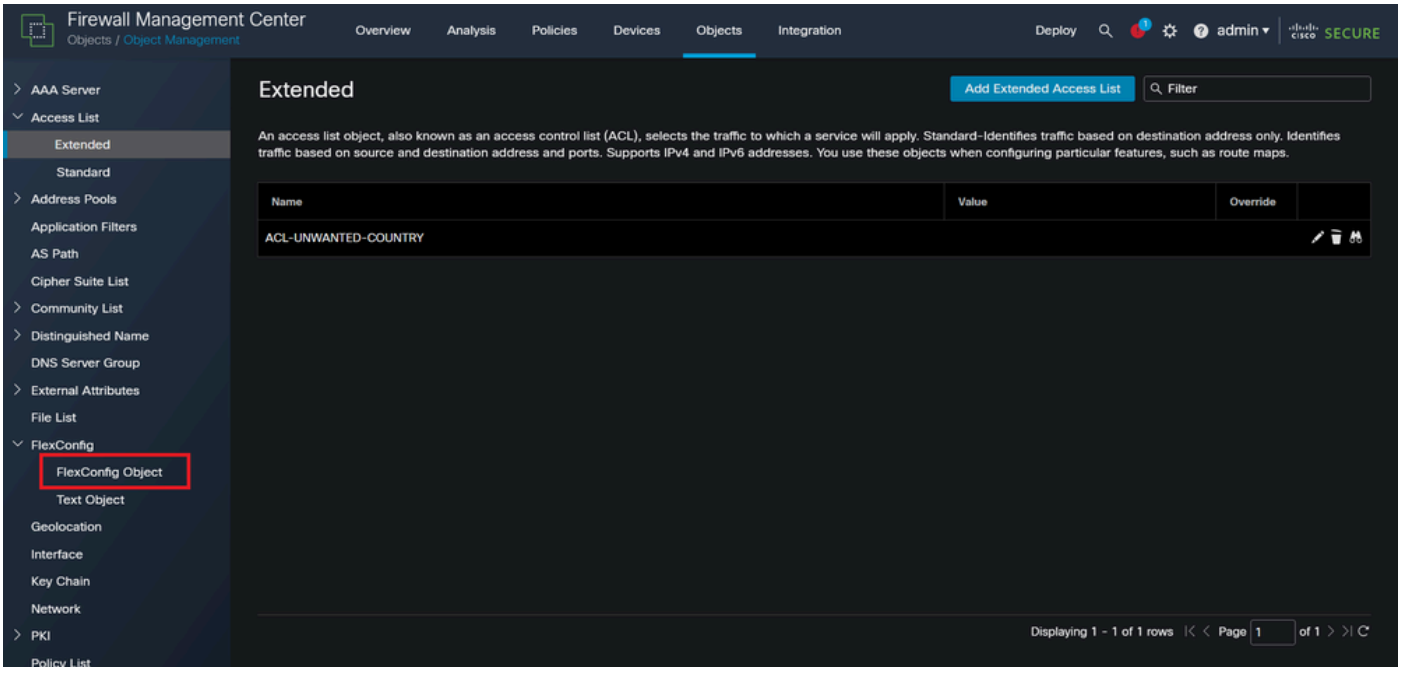


图10. FlexConfig对象菜单

第3.1步。单击添加FlexConfig对象：

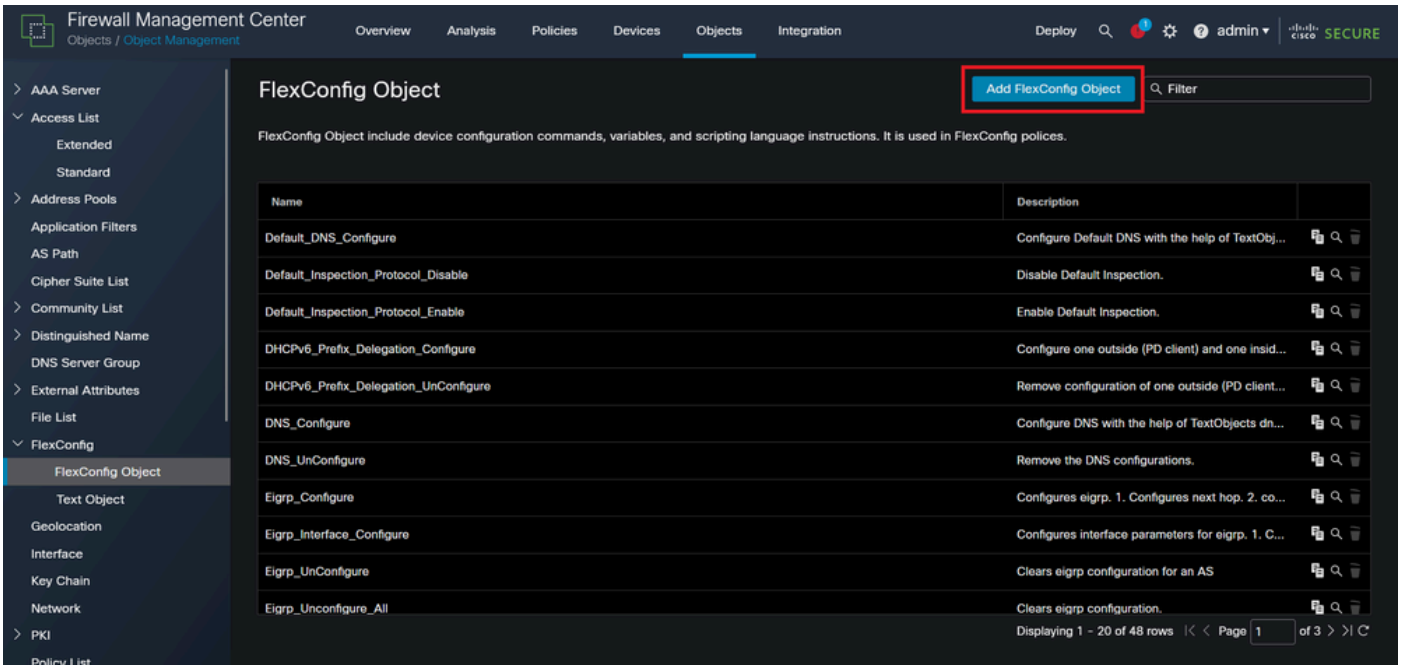


图11.添加Flexconfig对象

步骤3.2.为FlexConfig对象添加名称并插入ACL策略对象。选择插入>插入策略对象>扩展ACL对象:

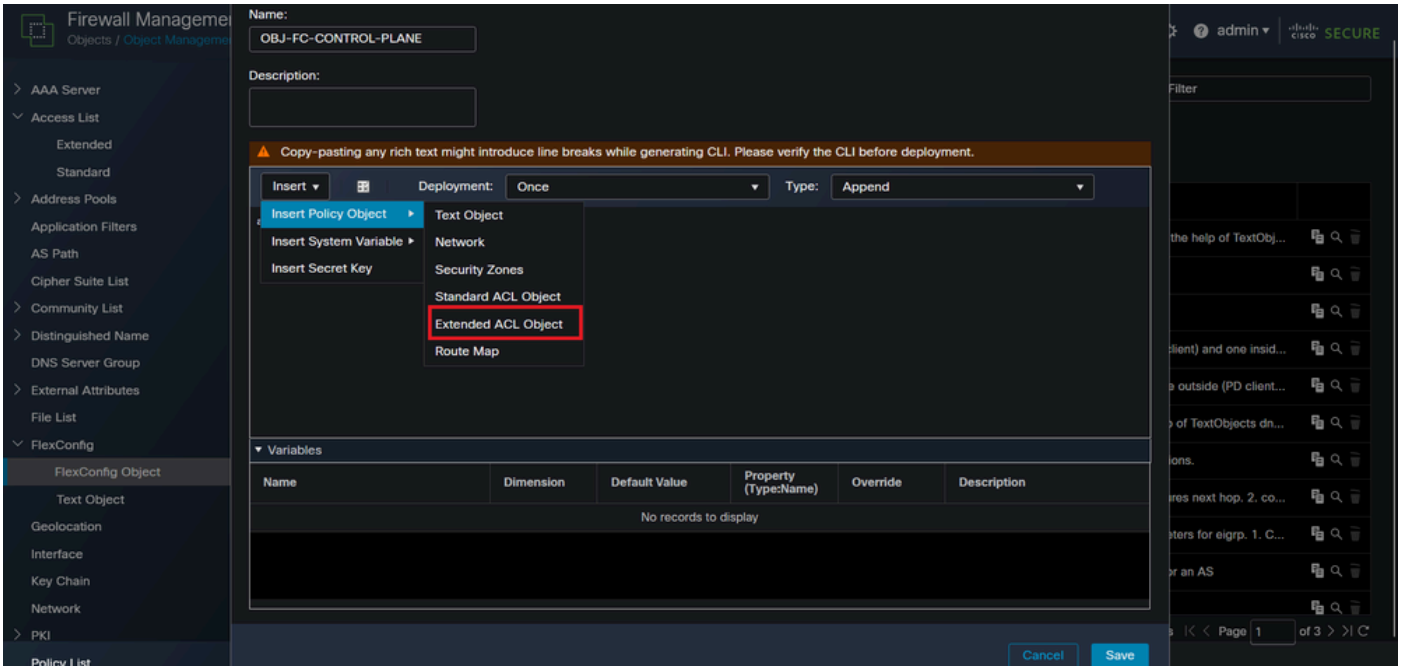


图12. FlexConfig对象变量

第3.3步：为ACL对象变量添加名称，并选择在第2.3步中创建的扩展ACL，点击Save按钮：

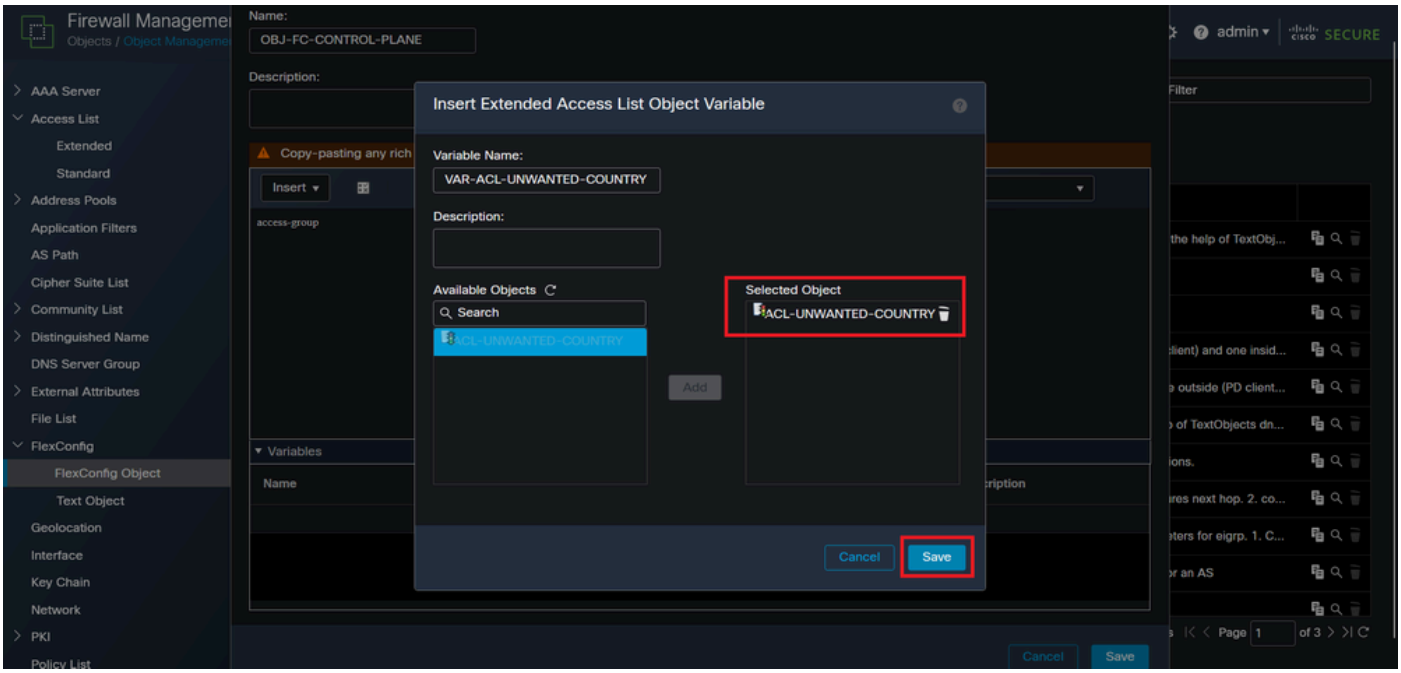


图13. FlexConfig对象变量ACL分配

步骤3.4.将控制平面ACL配置为外部接口的入站流量。

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，该示例使用第2.3步VAR-ACL-UNWANTED-COUNTRY中创建的ACL变量：

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

这是必须配置FlexConfig对象窗口的方式，之后，选择Save按钮以完成FlexConfig对象：

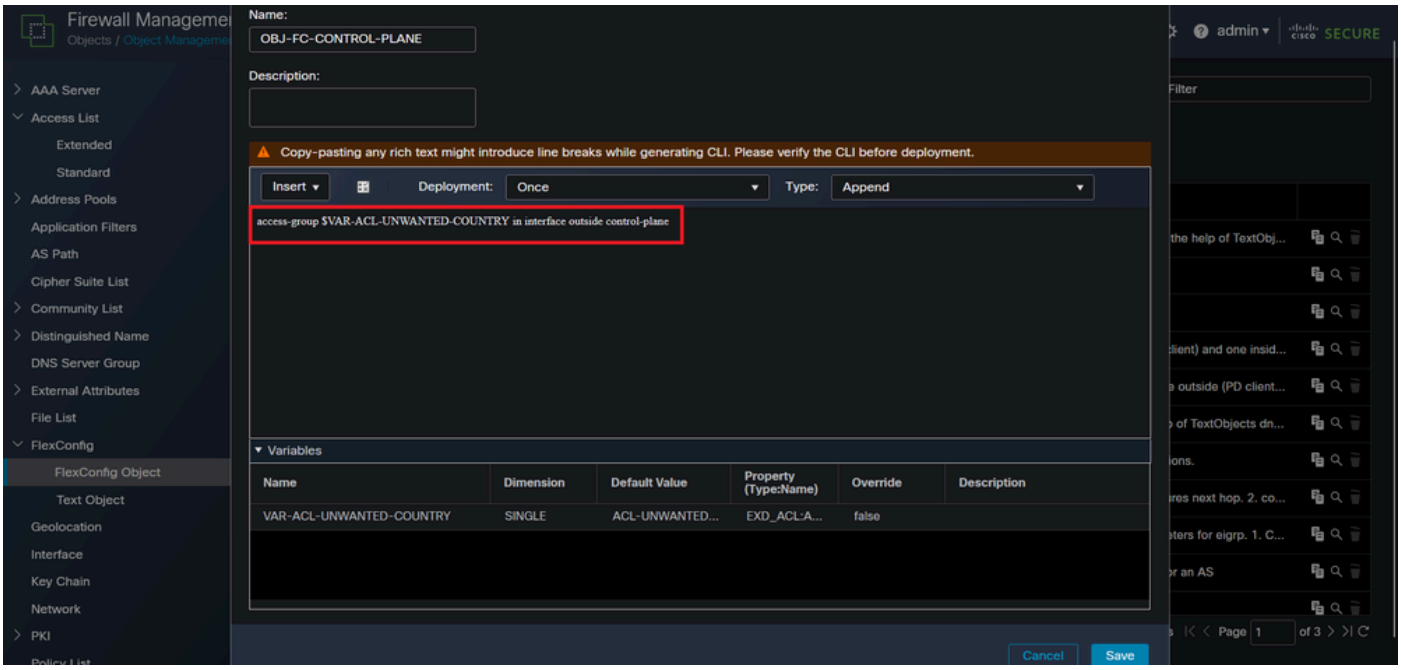


图14. Flexconfig Object完成命令行

注意：强烈建议仅在安全防火墙中接收传入远程访问VPN会话的接口（如外部接口）上配置控制平面ACL。

步骤4.您必须将FlexConfig对象配置应用到FTD，导航到设备> FlexConfig:

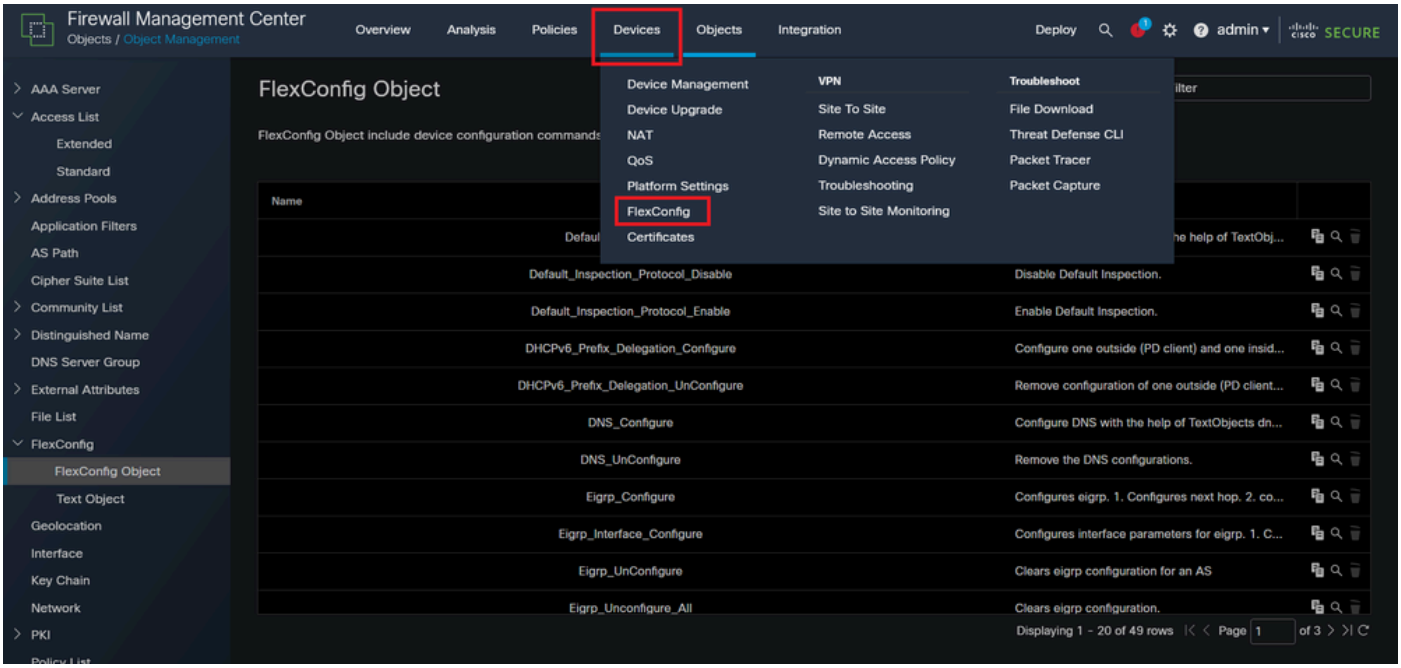
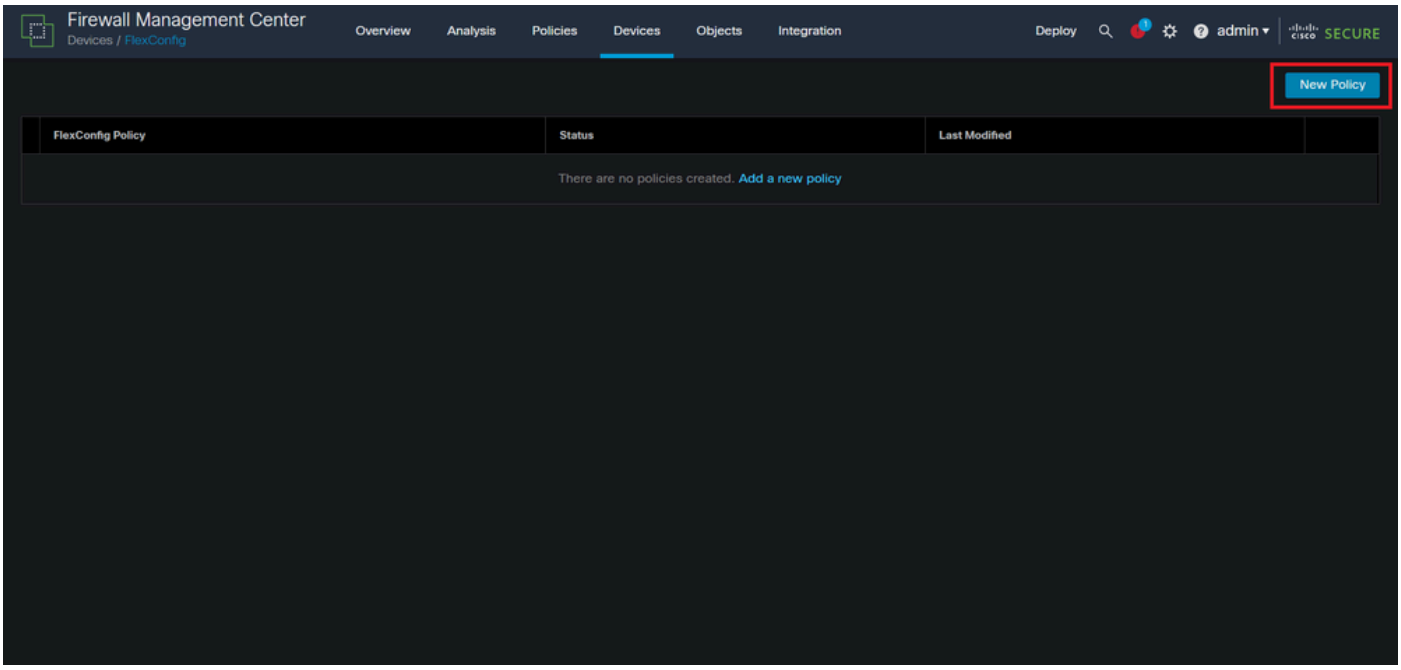


图15. FlexConfig策略菜单

第4.1步。单击New Policy，如果尚未为FTD创建FlexConfig，请编辑现有FlexConfig策略：



映像16.创建FlexConfig策略

第4.2步：为新的FlexConfig策略添加名称，然后选择要应用已创建的控制平面ACL的FTD:

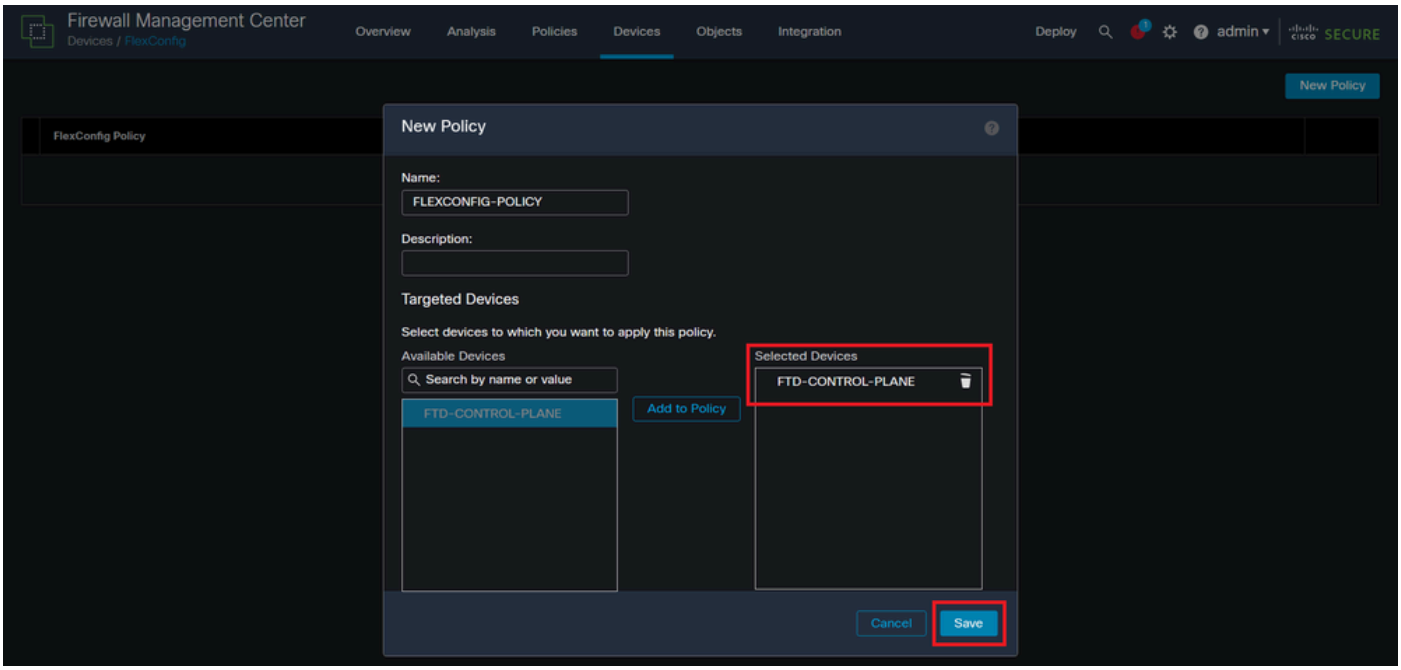


图17. FlexConfig策略设备分配

第4.3步：在左侧面板中，搜索在第3.2步中创建的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。然后，单击Save按钮：

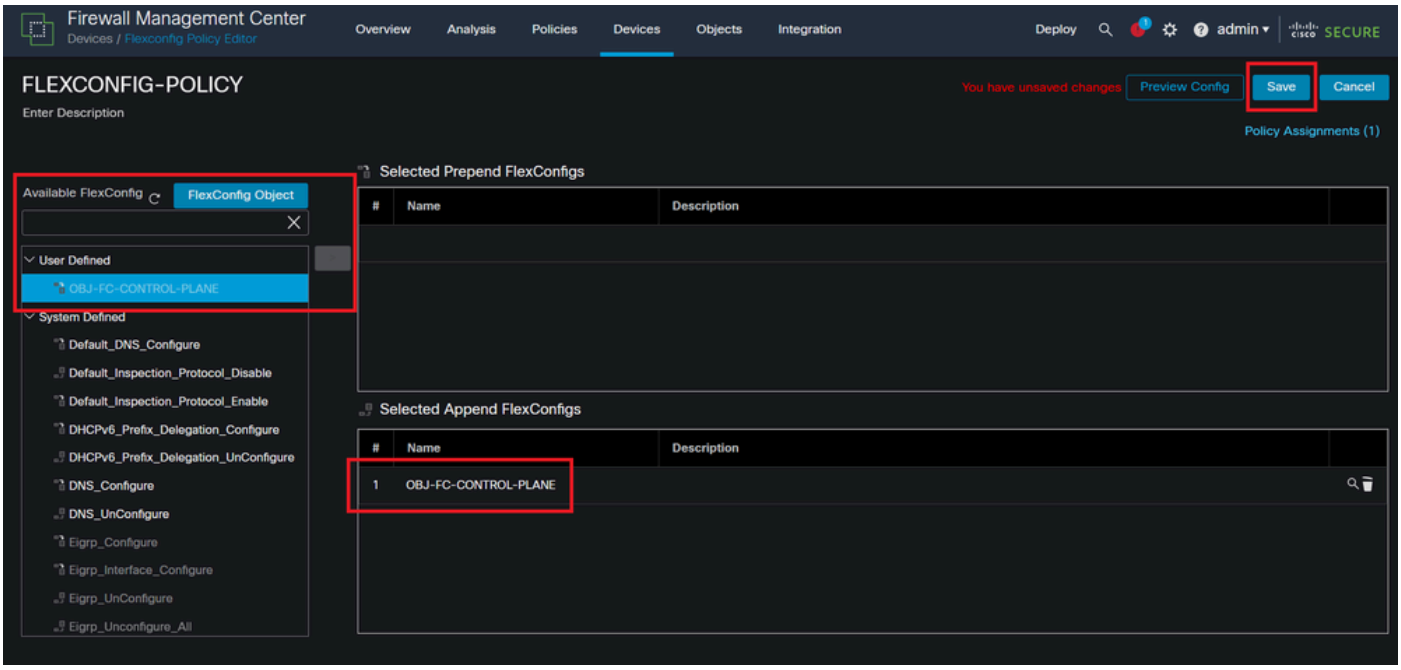


图18. FlexConfig策略对象分配

第5步：通过导航到Deploy > Advanced Deploy，继续将配置更改部署到FTD:

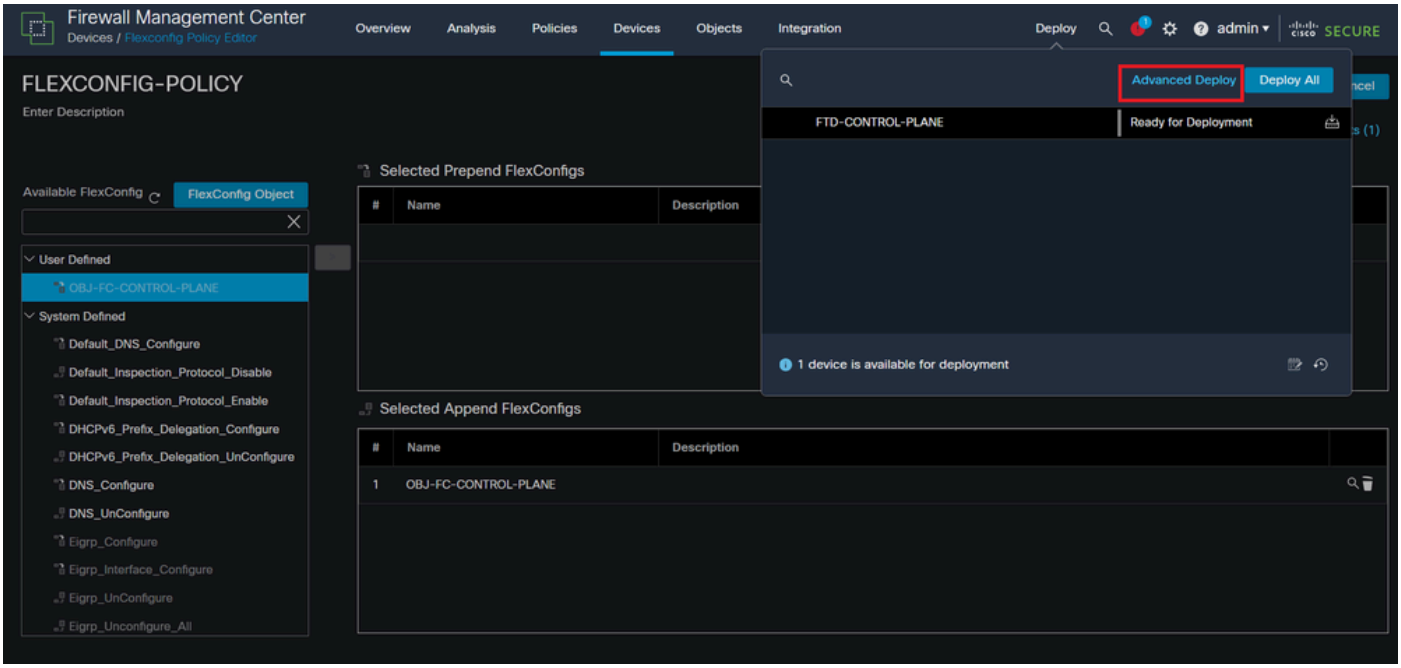
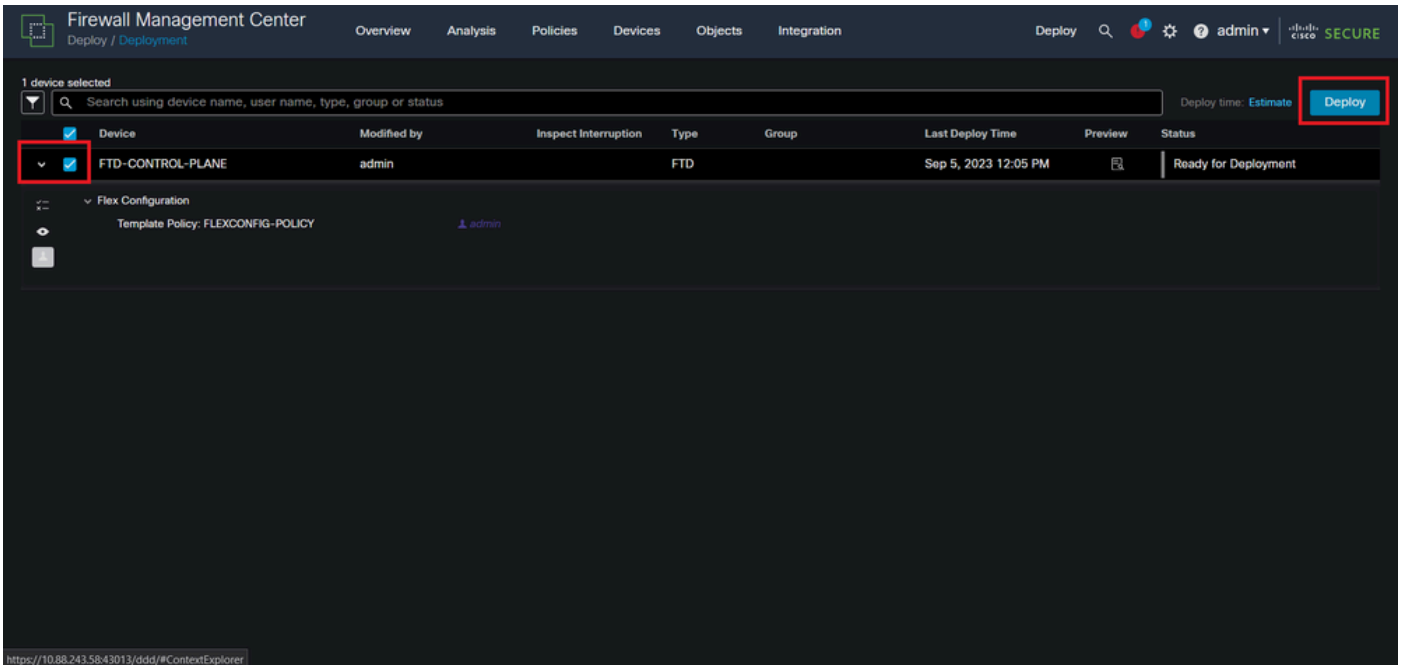


图19. FTD高级部署

第5.1步。选择要应用FlexConfig策略的FTD。如果一切正确，请单击Deploy:



映像20. FTD部署验证

第5.2步：接下来，显示Deployment Confirmation窗口，添加备注以跟踪部署并继续Deploy:

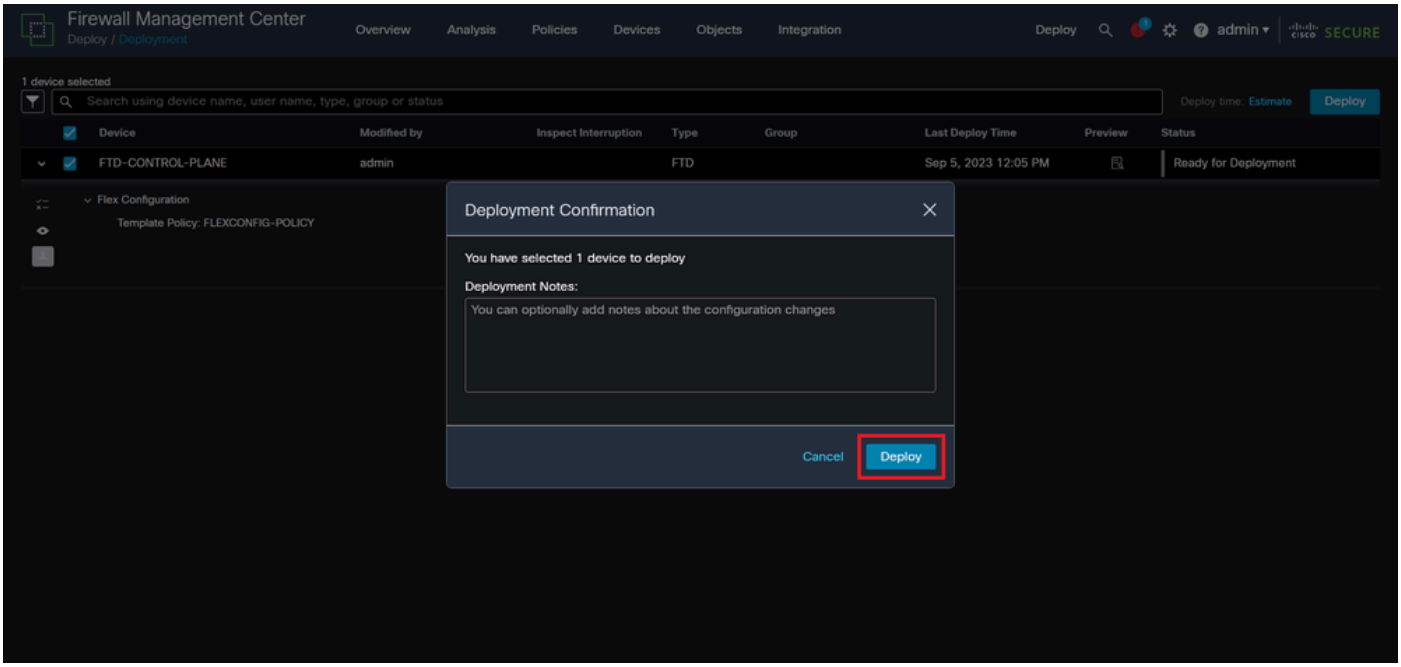
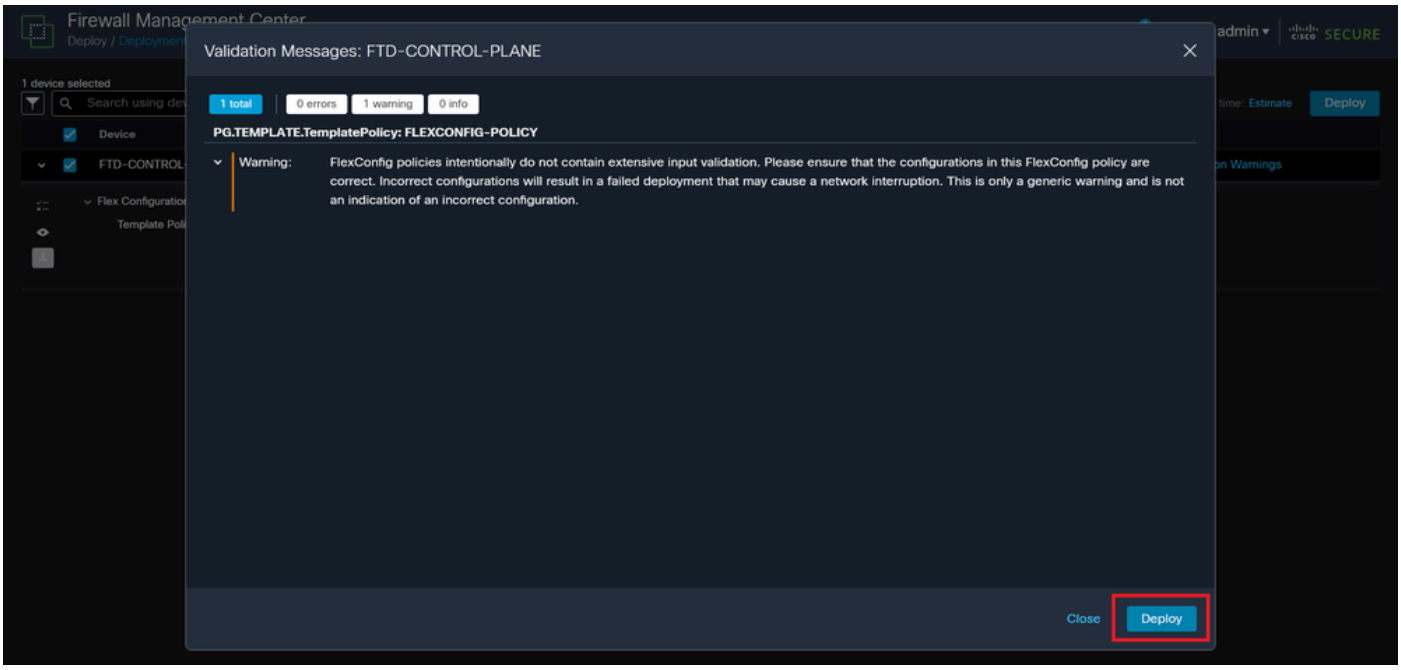


图21. FTD部署备注

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，才单击Deploy:



映像22. FTD部署Flexconfig警告

第5.4步：确认FTD的策略部署成功：

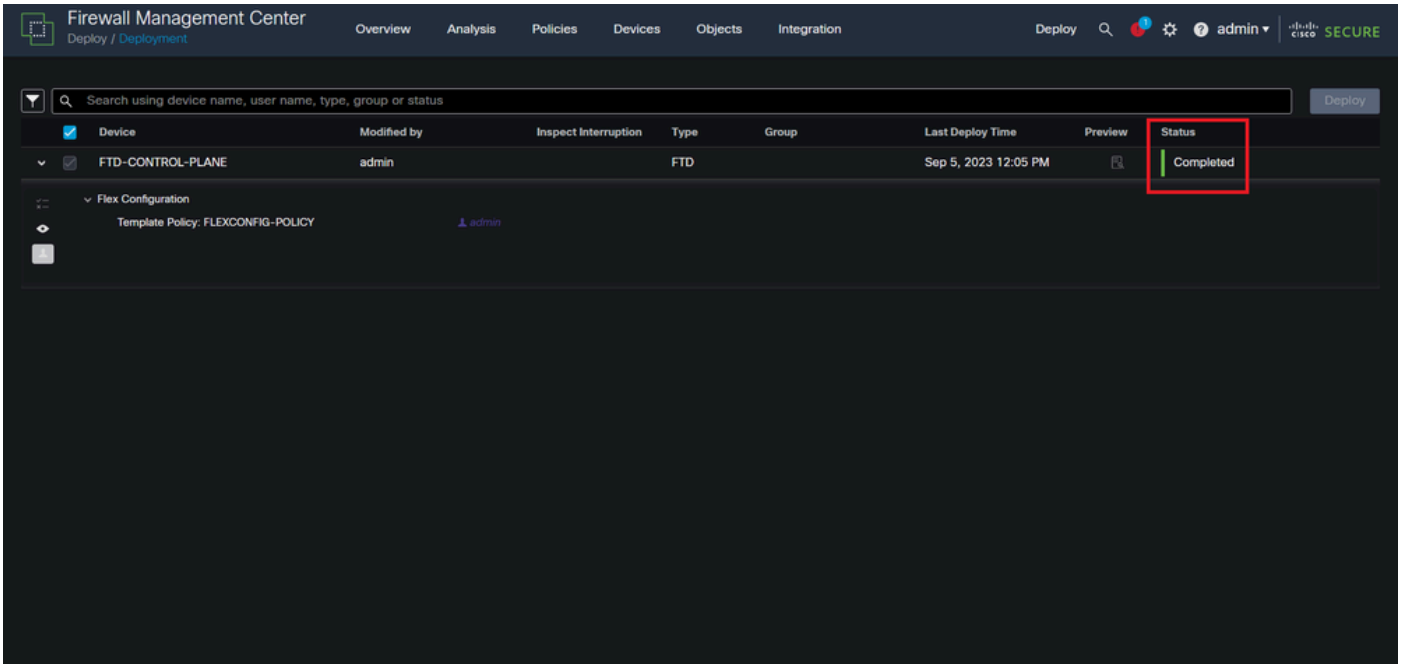


图23. FTD部署成功

步骤6.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，请务必突出显示所做的配置更改。这些不适用于FTD的已建立连接。必须手动清除到FTD的活动连接尝试，连接到FTD的CLI，并清除活动连接。

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强制清除安全防火墙的活动VPN暴力连接尝试。这主要是当VPN暴力攻击的性质是不断发起大量连接尝试时。

[视频]为FMC管理的FTD配置控制平面ACL

为FDM管理的FTD配置控制平面ACL

要配置控制平面ACL以阻止传入VPN暴力攻击到外部FTD接口，必须遵循以下步骤：

步骤1.通过HTTPS打开FDM GUI，然后使用您的凭据登录：

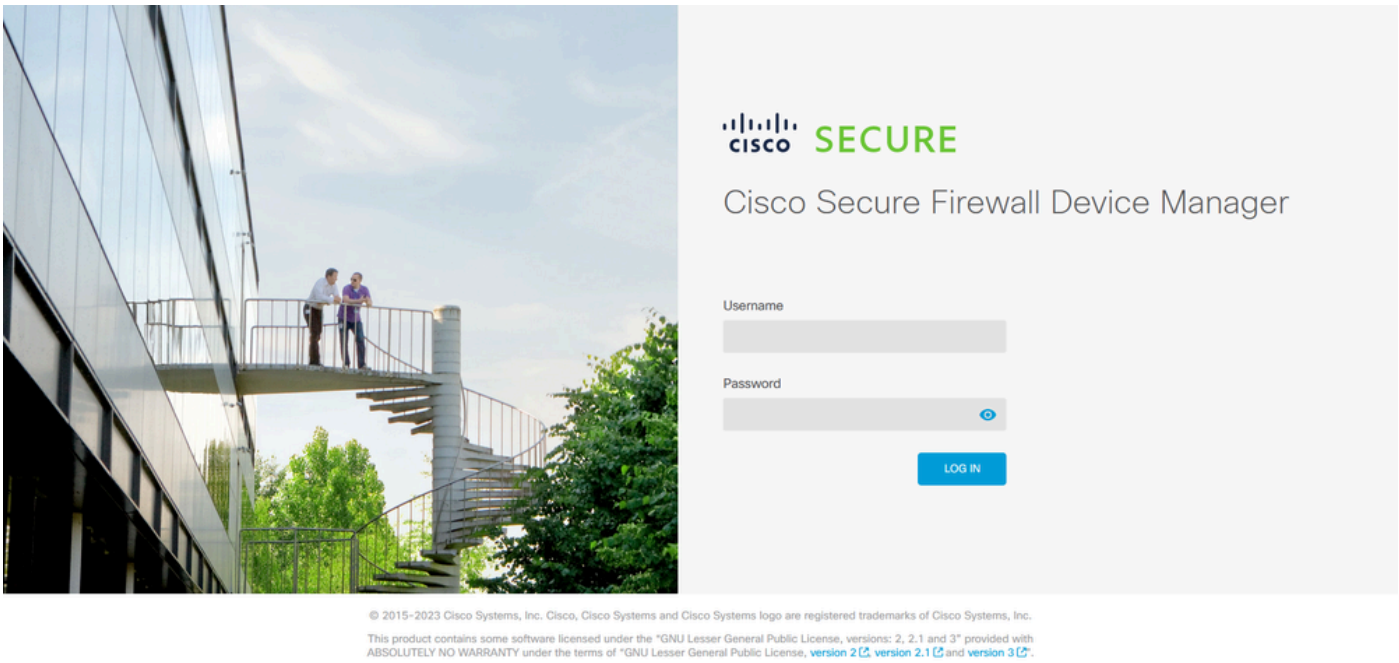


图24. FDM登录页

步骤2.您必须创建对象网络。导航到对象:

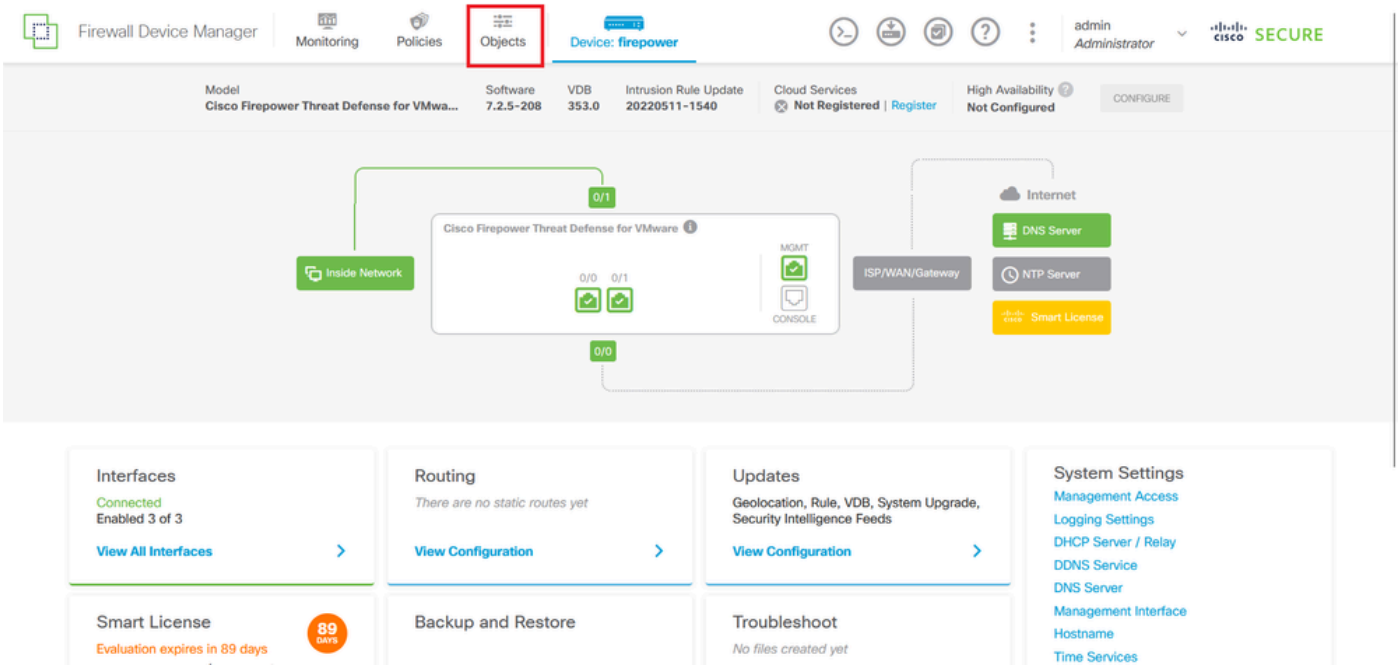


图25. FDM主仪表板

第2.1步：从左侧面板中选择Networks，然后点击“+”按钮以创建新的网络对象：

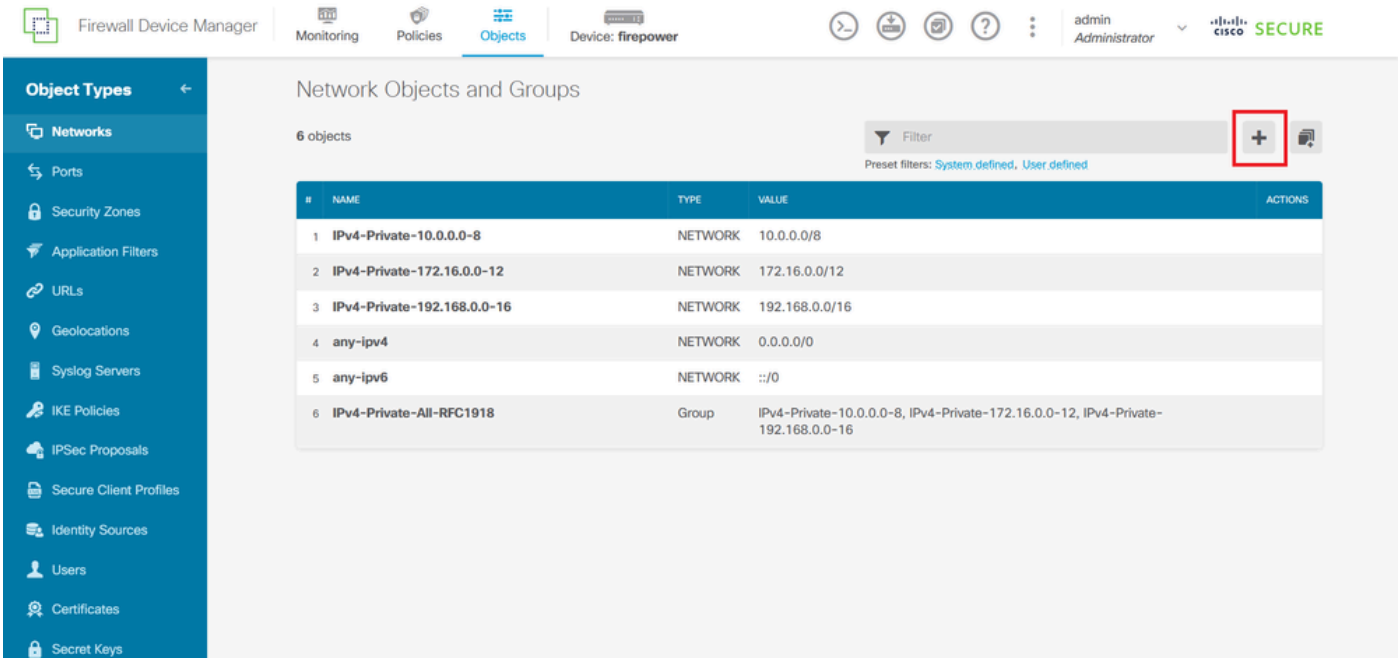


图26.创建对象

第2.2步：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范围以匹配必须拒绝到FTD的流量。然后，单击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：

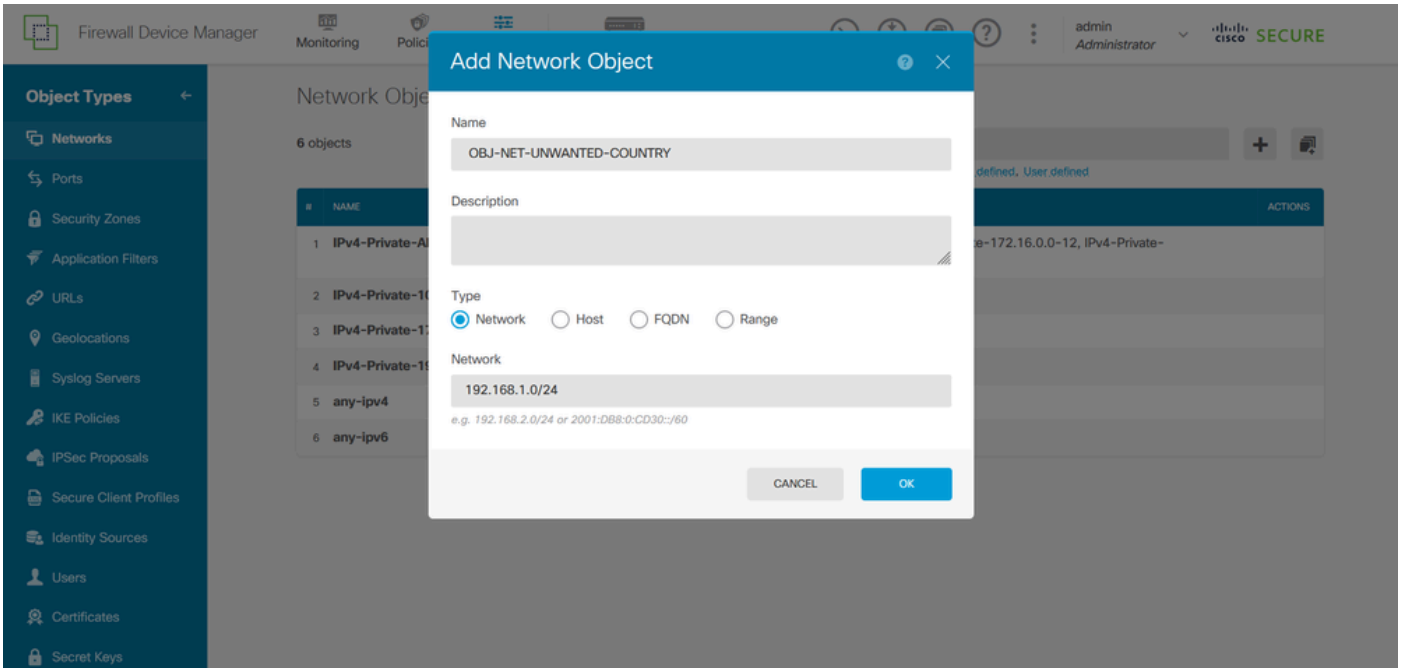


图27.添加网络对象

步骤3.然后，您必须创建扩展ACL，然后导航到顶部菜单中的Device选项卡：

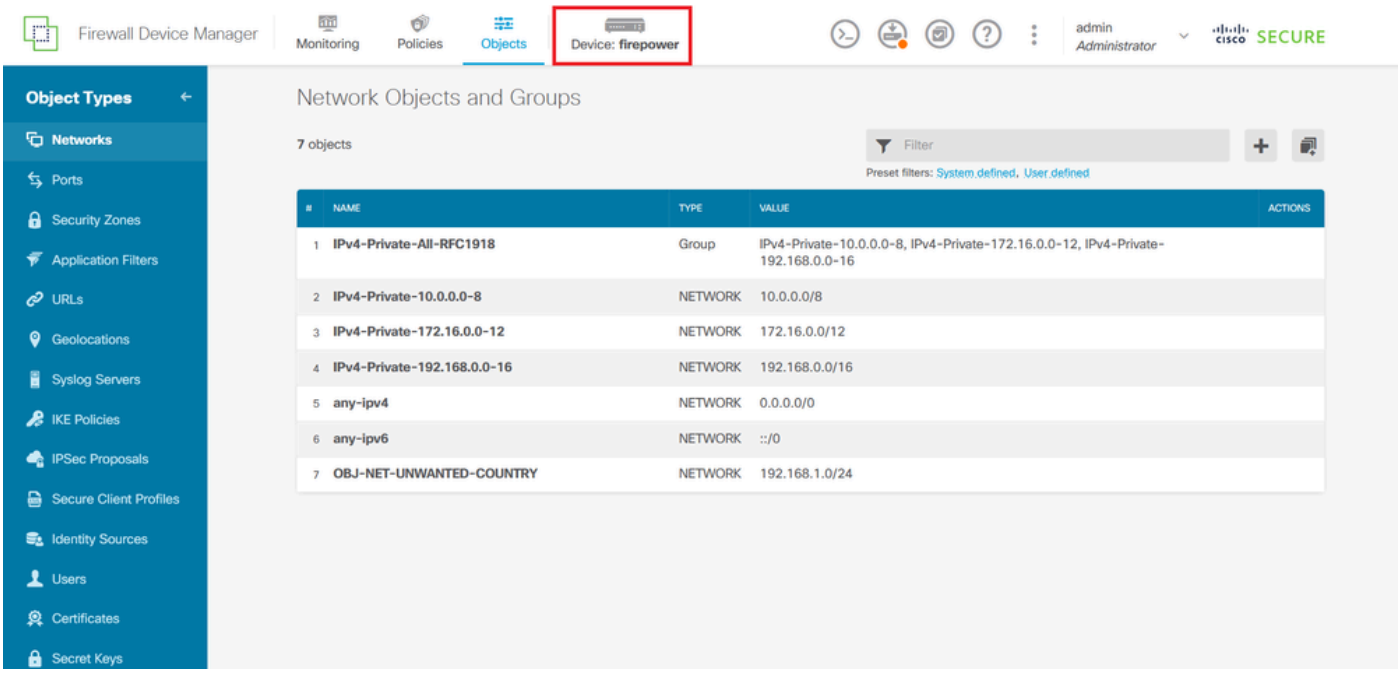


图28.设备设置页面

第3.1步：向下滚动，从“高级配置”方块中选择View Configuration，如图所示：

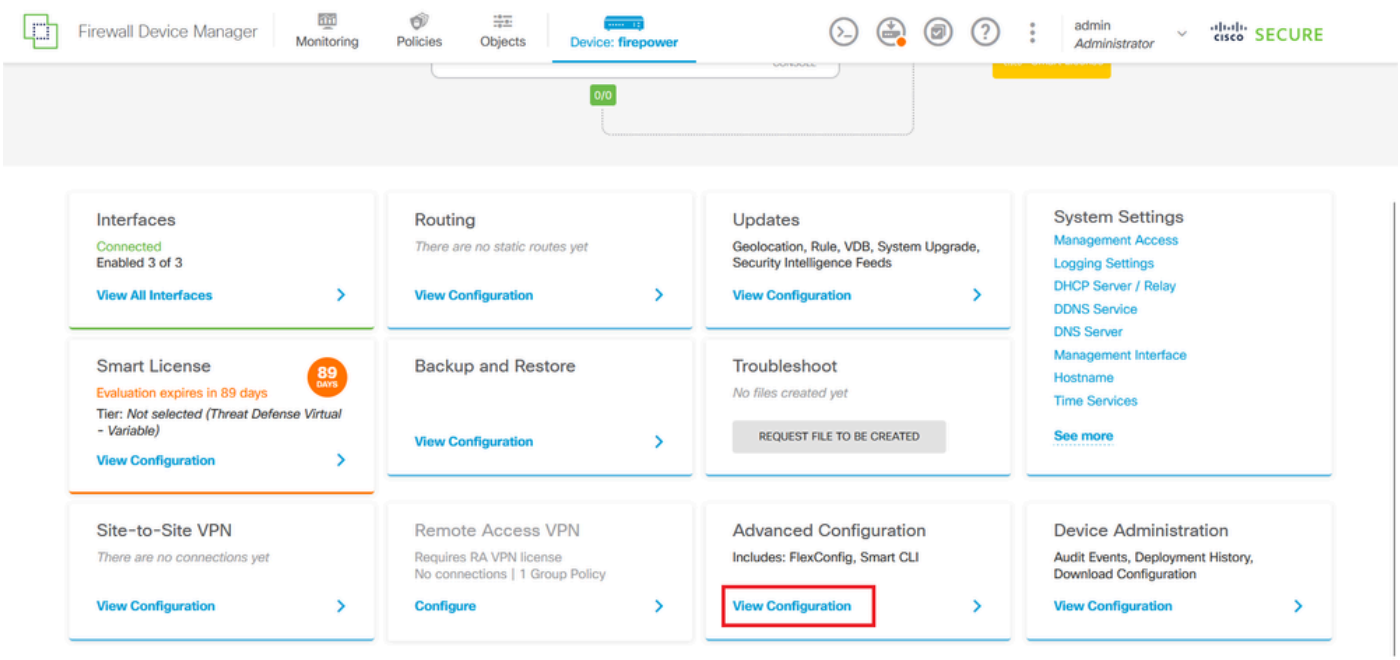


图29. FDM高级配置

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

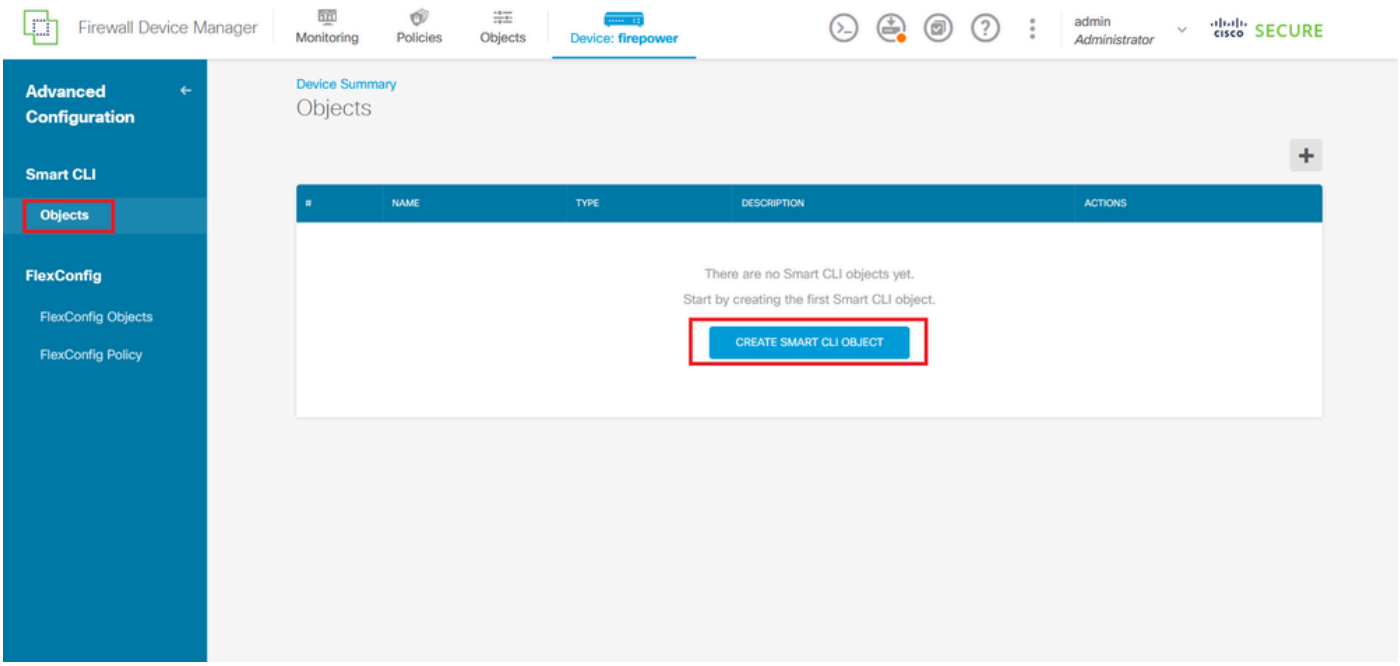


图30. Smart CLI对象

步骤3.3.为扩展ACL添加名称。要创建，请从CLI模板下拉菜单中选择Extended Access List，然后使用步骤2.2中创建的网络对象配置所需的ACE。然后，单击OK按钮完成ACL:

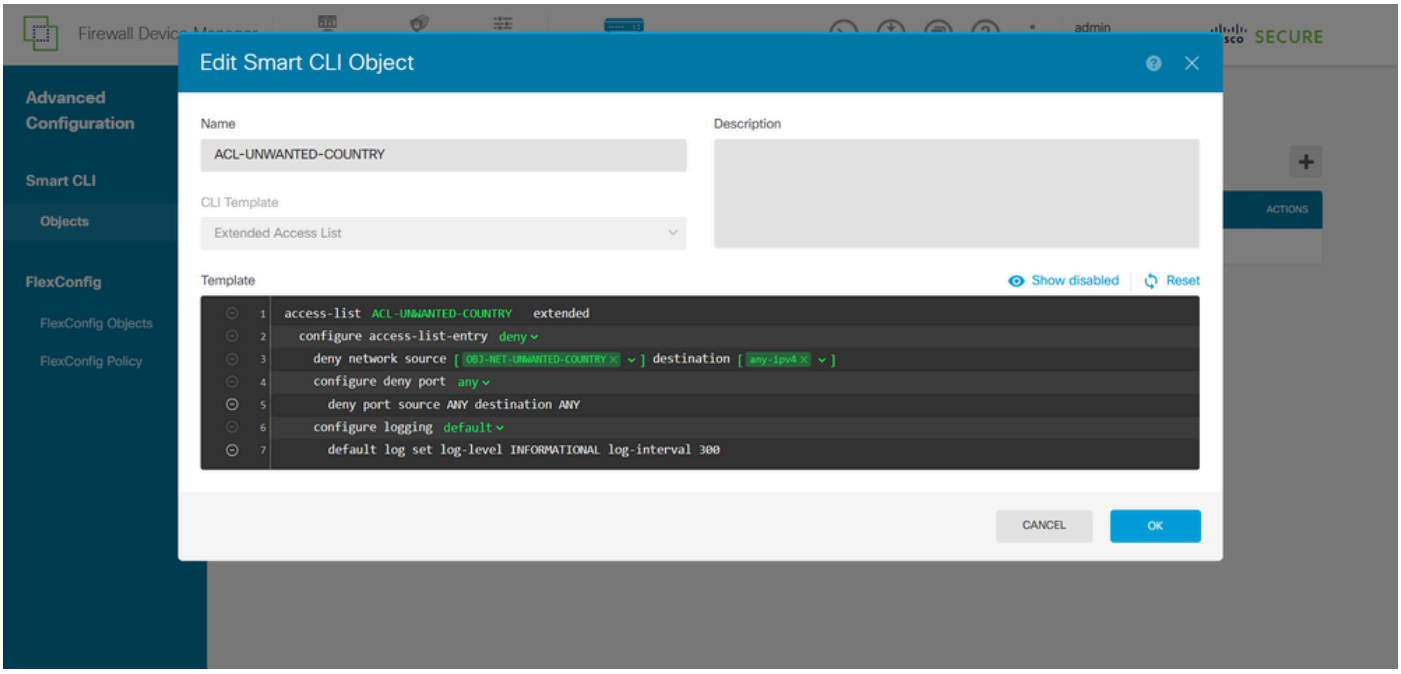


图31.创建扩展ACL

注意：如果需要为ACL添加更多ACE，可以将鼠标悬停在当前ACE的左侧；则不会出现三个可点击的点。单击此按钮并选择复制以添加更多ACE。

步骤4.下一步，必须创建FlexConfig对象，导航到左侧面板并选择FlexConfig > FlexConfig

Objects，然后点击CREATE FLEXCONFIG OBJECT:

，

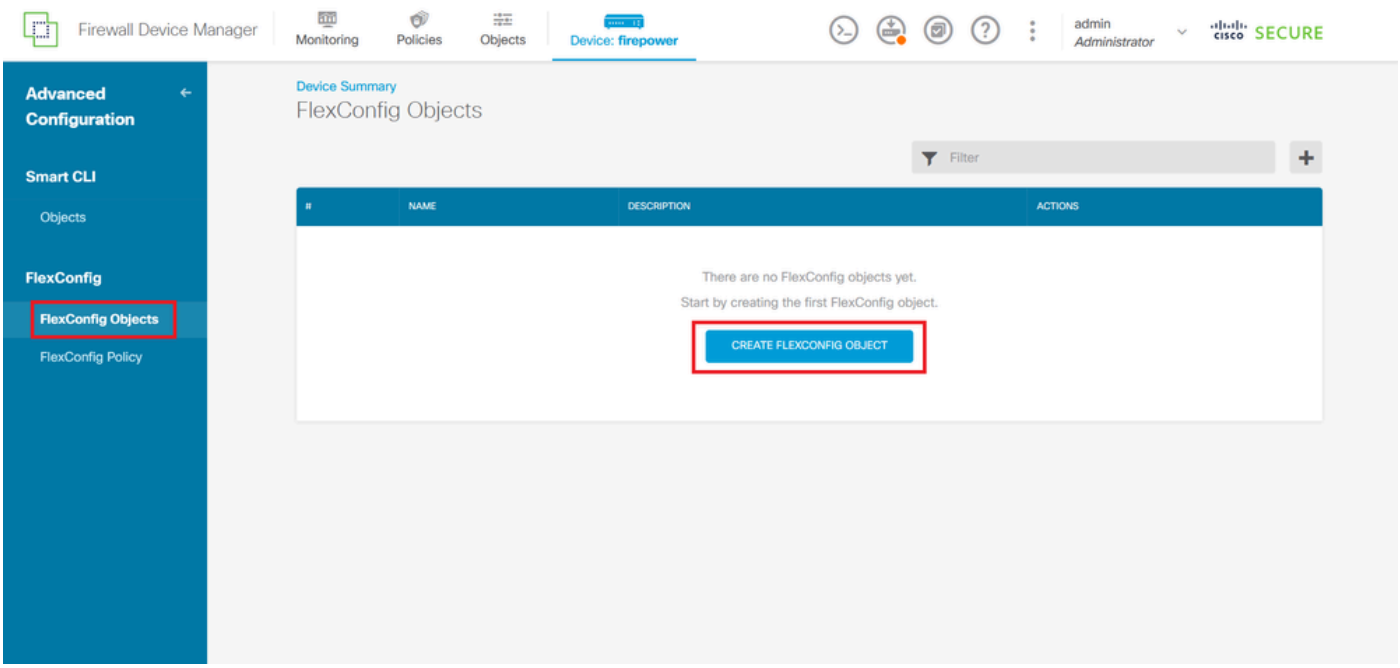


图32. FlexConfig对象

第4.1步：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。

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，该示例使用第3.3步ACL-UNWANTED-COUNTRY中创建的扩展ACL:

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

这是将其配置到FlexConfig对象窗口的方式。选择OK按钮以完成FlexConfig对象：

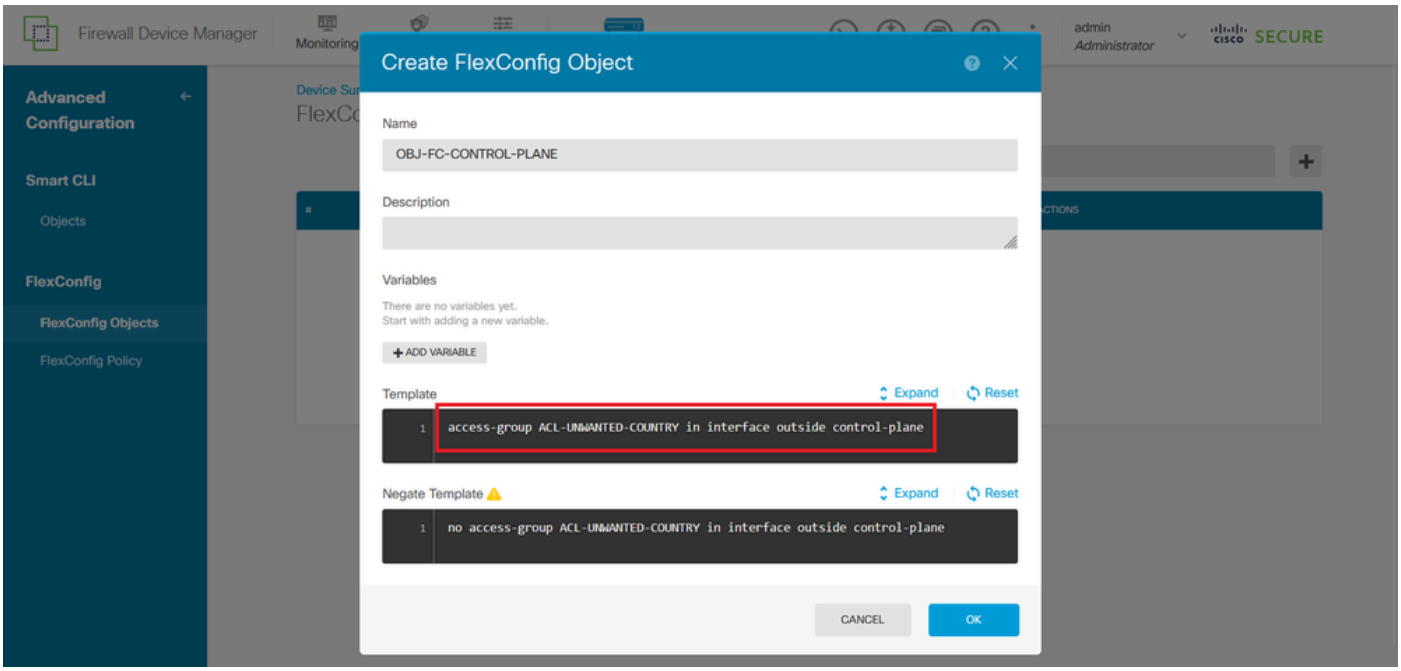


图33.创建FlexConfig对象

> 注意：强烈建议仅在安全防火墙中接收传入远程访问VPN会话的接口（如外部接口）上配置控制平面ACL。

步骤5.继续创建FlexConfig策略。导航到Flexconfig > FlexConfig Policy，单击“+”按钮，并选择在步骤4.1中创建的FlexConfig对象：

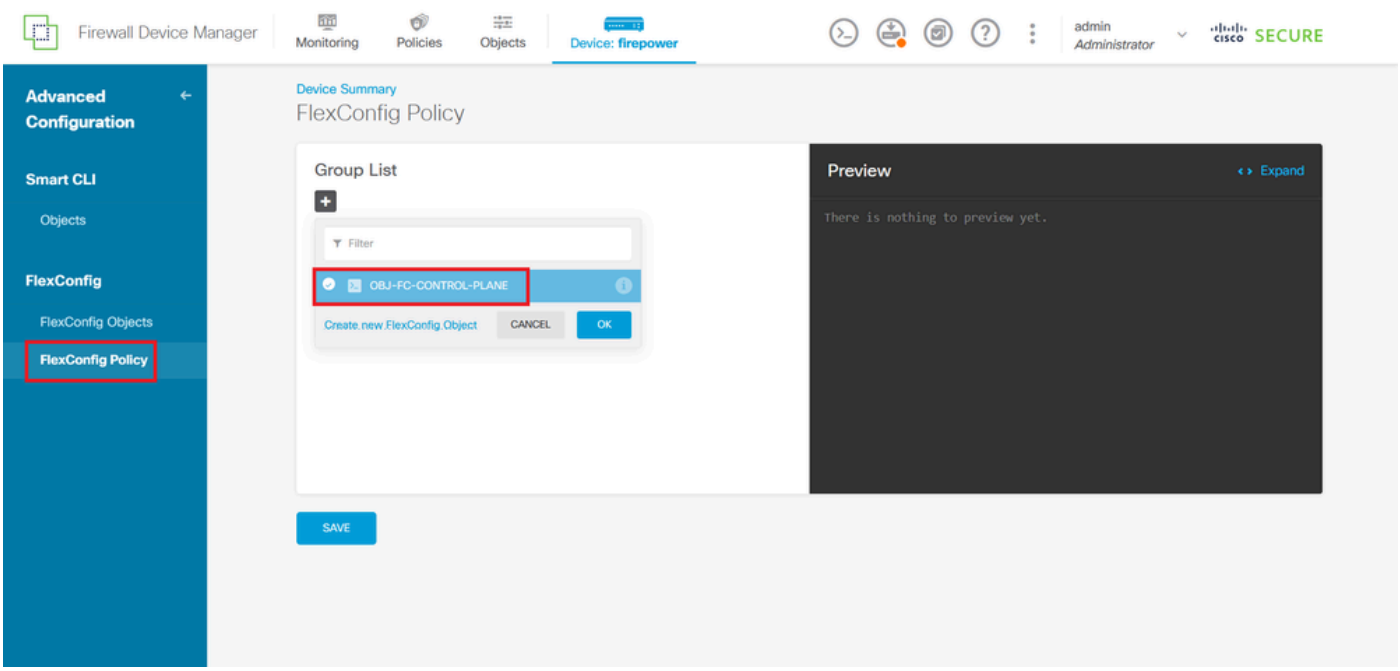


图34. FlexConfig策略

第5.1步：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：

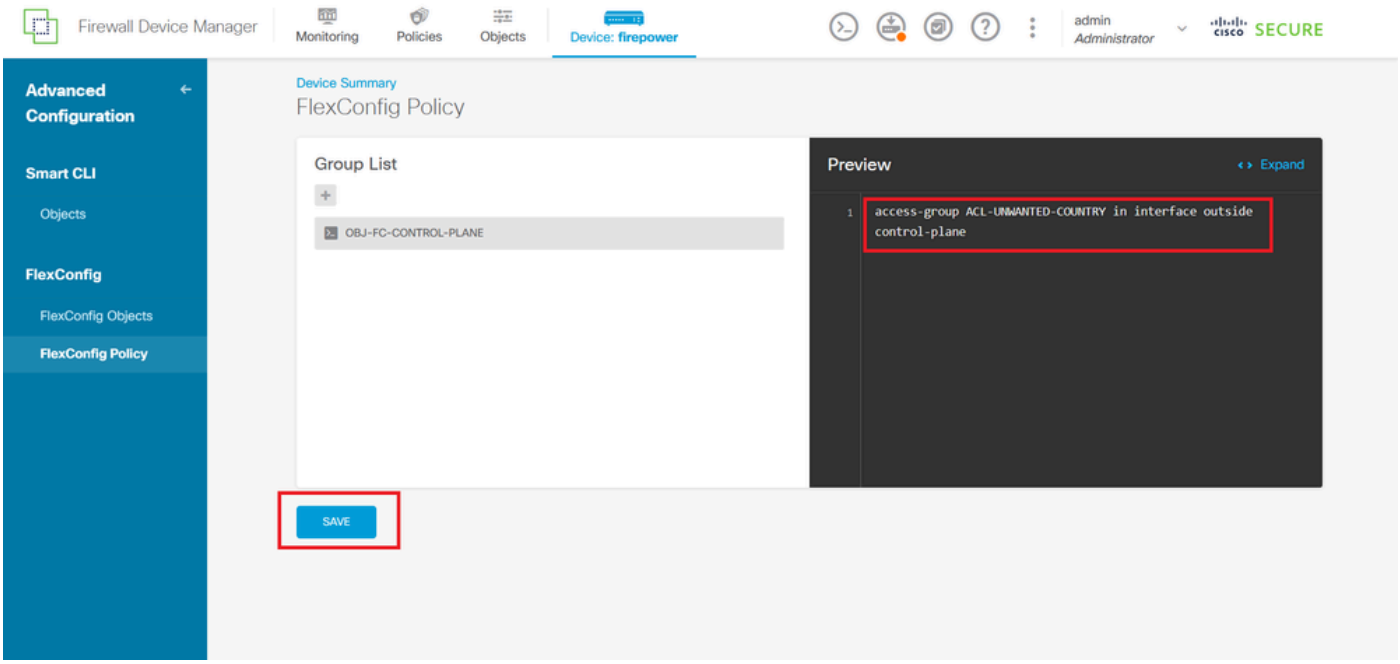


图35. FlexConfig策略预览

步骤6.将配置更改部署到要防御VPN暴力攻击的FTD。然后，点击顶部菜单上的Deployment按钮并验证要部署的配置更改是否正确，然后点击DEPLOY NOW:

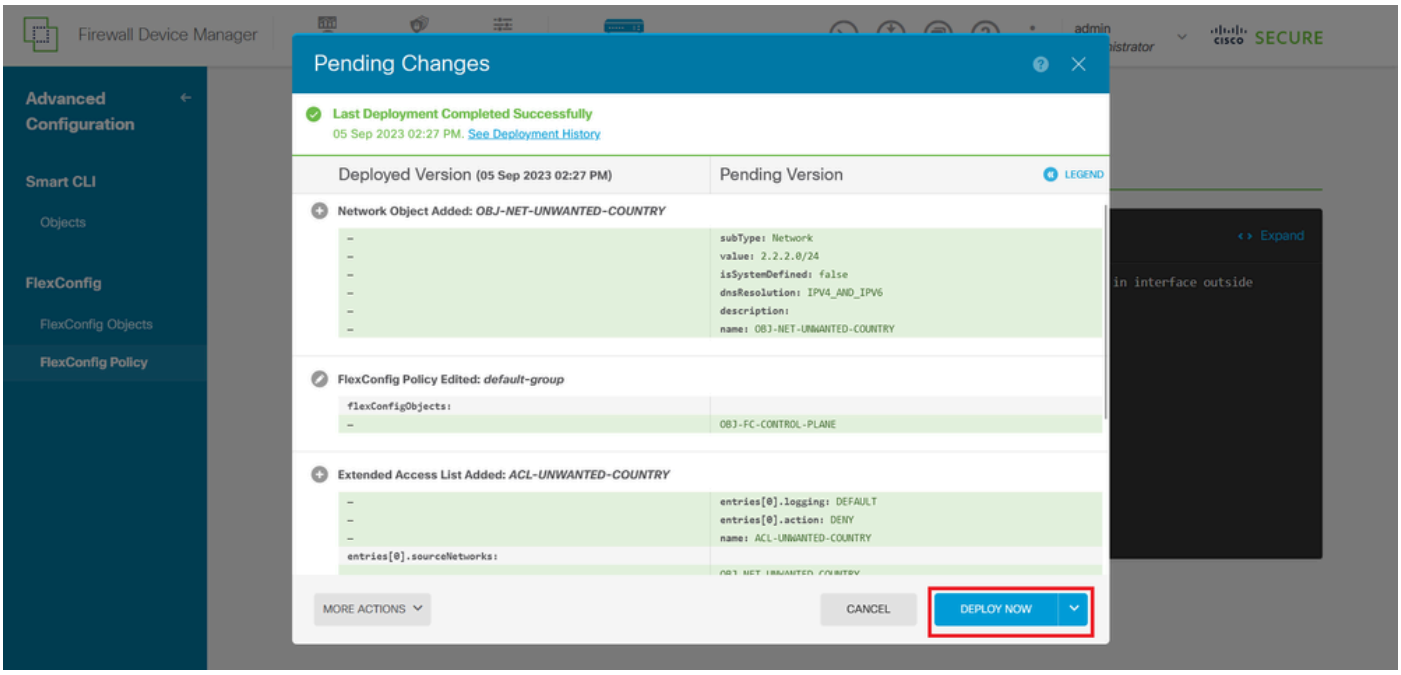


图36.待定部署

第6.1步：验证策略部署是否成功：

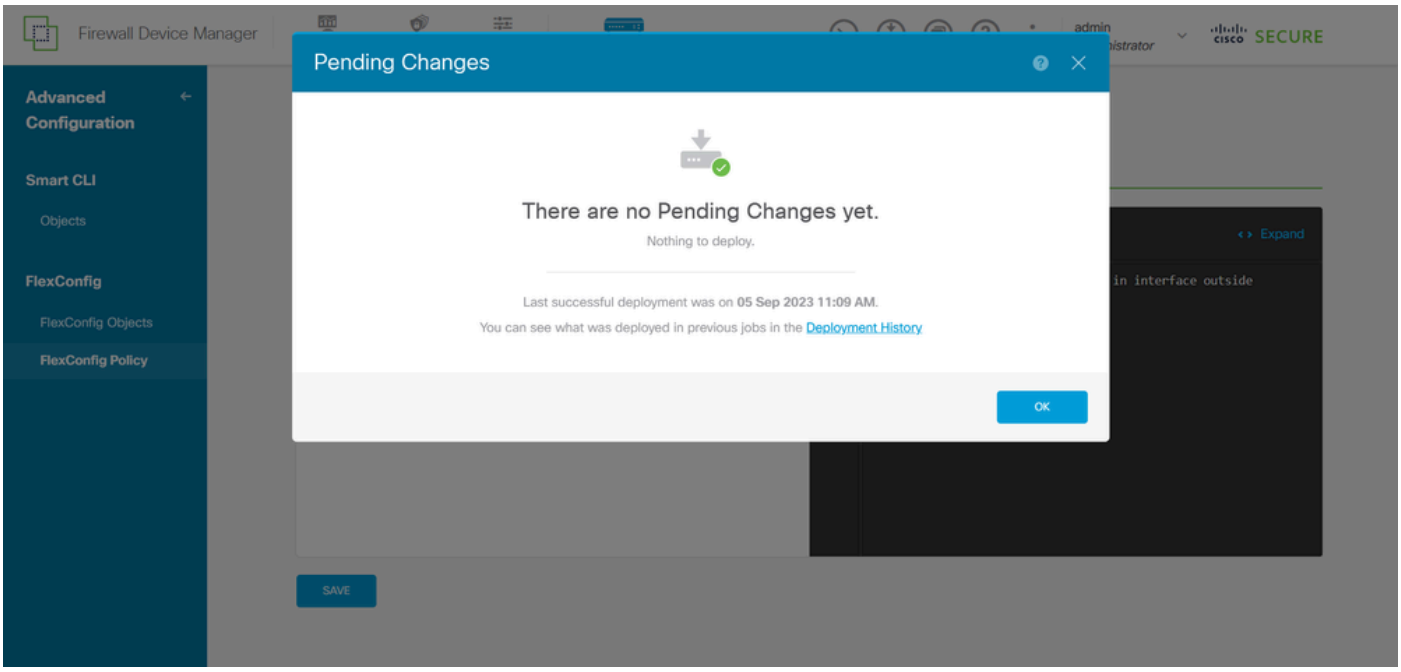


图37.部署成功

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，请务必突出显示所做的配置更改。这些不适用于FTD的已建立连接。必须手动清除到FTD的活动连接尝试，连接到FTD的CLI，并清除活动连接。

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强制清除安全防火墙的活动VPN暴力连接尝试。这主要是当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

这是必须遵守ASA CLI的程序，这是要配置控制平面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并访问configure terminal命令。

```
asa# configure terminal
```

步骤2.运行下一命令配置扩展ACL，这将阻止必须阻止到ASA的流量的主机IP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
```

步骤3.运行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
```


注意：强烈建议仅在安全防火墙中接收传入远程访问VPN会话的接口（如外部接口）上配置控制平面ACL。

步骤4.如果创建新的控制平面ACL，或者编辑了正在使用的现有控制平面ACL，请务必突出显示所做的配置更改。这些选项不适用于已建立到ASA的连接，您必须手动清除到ASA的活动连接尝试并清除活动连接。

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强制清除安全防火墙的活动VPN暴力连接尝试。这主要是当VPN暴力攻击的性质是不断发起大量连接尝试时。

用于阻止运行Shun的安全防火墙攻击的备用配置

对于安全防火墙的即时阻止攻击，您可以运行shun命令。shun命令允许您阻止来自攻击主机的连接，查看有关shun命令的详细信息：

- 回避IP地址后，源IP地址的所有后续连接都会被丢弃并记录，直到您手动删除阻止功能为止。
- 无论具有指定主机地址的连接当前是否处于活动状态，都会应用shun命令的阻止功能。
- 如果指定目标地址、源端口和目标端口以及协议，则会丢弃匹配的连接，并对来自源IP地址的所有未来连接设置回避。所有未来连接都将遭到拒绝，而不仅仅是那些与这些特定连接参数匹配的连接。
- 每个源IP地址只能有一个shun命令。
- 由于shun命令用于动态阻止攻击，因此它不会显示在威胁防御设备配置中。
- 每当删除接口配置时，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shun，请运行此命令的no形式：

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

要避开主机IP地址，请继续参阅此安全防火墙示例。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配置示例

步骤1.通过CLI登录FTD并运行shun命令：

```
<#root>

>

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf



Shun 192.168.1.10 successful
```

步骤2.您可以运行show命令来确认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：

```
<#root>

asa#

 shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf



Shun 192.168.1.10 successful
```

步骤2.您可以运行show命令来确认ASA中的shun IP地址，并监控每个IP地址的shun命中计数：

<#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，请参阅思科安全防火墙威胁防御命令参考。

验证

要确认安全防火墙的控制平面ACL配置已就绪，请执行以下步骤：

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
```

步骤2.要确认控制平面ACL阻止了所需的流量，请运行packet-tracer命令来模拟到安全防火墙外部接口的传入TCP 443连接。然后，运行show access-list <acl-name> 命令，每当控制平面ACL阻止与安全防火墙的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，show access-list输出显示已部署的控制平面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，则可以执行到安全防火墙的实际连接尝试，以确认控制平面ACL是否按预期运行，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
- 文档：ASA/FTD对象组搜索不支持控制平面ACL:Cisco Bug ID CSCwi58818

相关信息

- 在安全防火墙威胁防御上为远程访问VPN配置基于地理定位的策略
- 缓解远程VPN安全防火墙上的密码喷雾攻击
- Cisco VPN技术参考指南

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）。