在FMC上的PBR的扩展ACL上配置FQDN对象

目录

简介

本文档介绍在扩展访问列表(ACL)中配置FQDN对象以用于基于策略的路由(PBR)的过程。

先决条件

要求

思科建议您了解以下产品：

- 安全防火墙管理中心(FMC)
- 安全防火墙威胁防御(FTD)
- PBR

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 适用于VMware的Firepower威胁防御7.6.0版
- 适用于VMware 7.6.0版的安全防火墙管理中心

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

目前，FTD不允许使用思科漏洞ID CSCuz98322上提及的完全限定域名(FQDN)对象对非HTTP流量进行过滤。

ASA平台支持此功能，但是，在FTD上只能过滤网络和应用。

您可以使用此方法将FQDN对象添加到扩展访问列表以配置PBR。

配置

步骤1:根据需要创建FQDN对象。

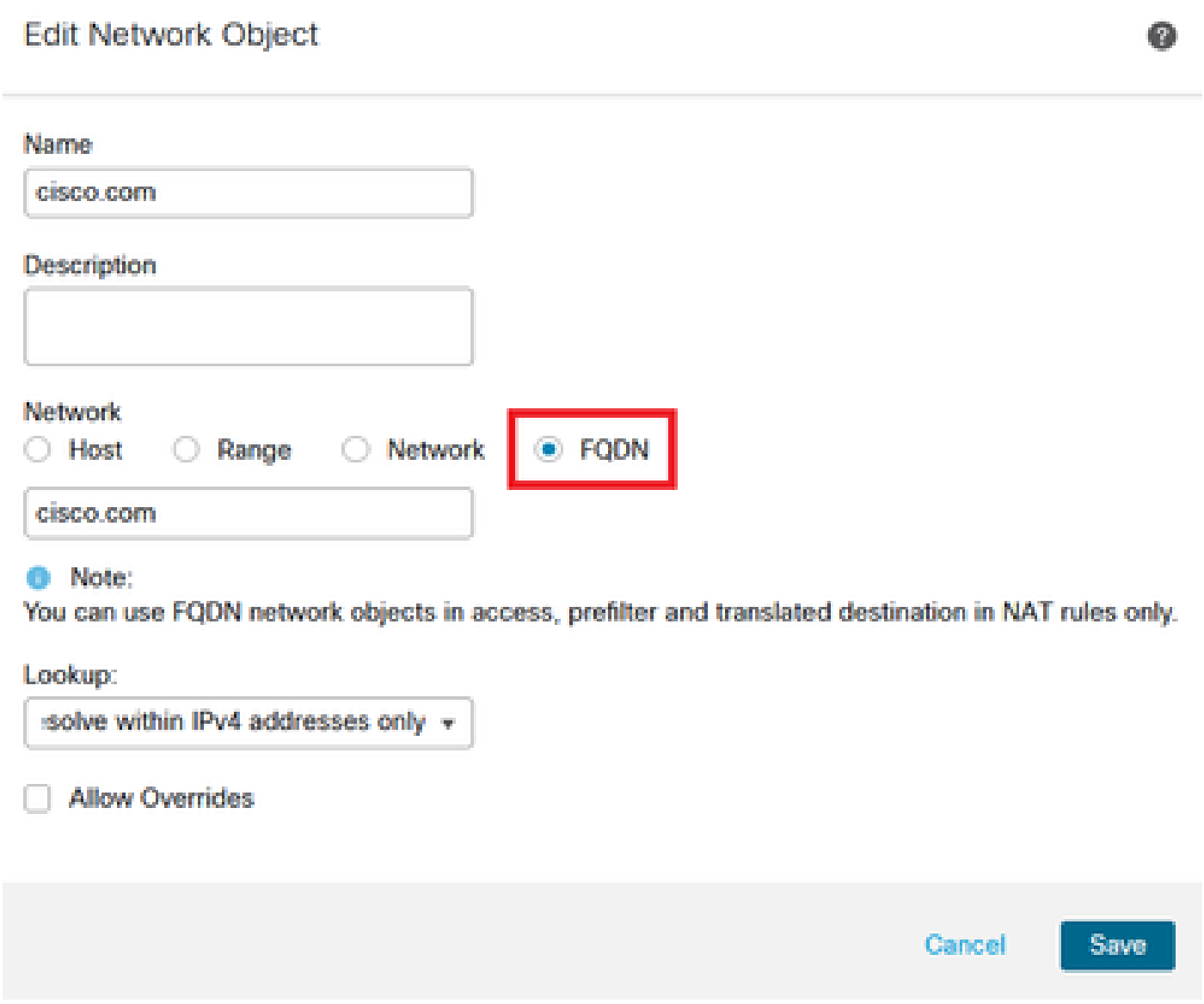

图 1.网络对象菜单

第二步：在Objects > Object Management > Access List > Extended下创建扩展访问列表。

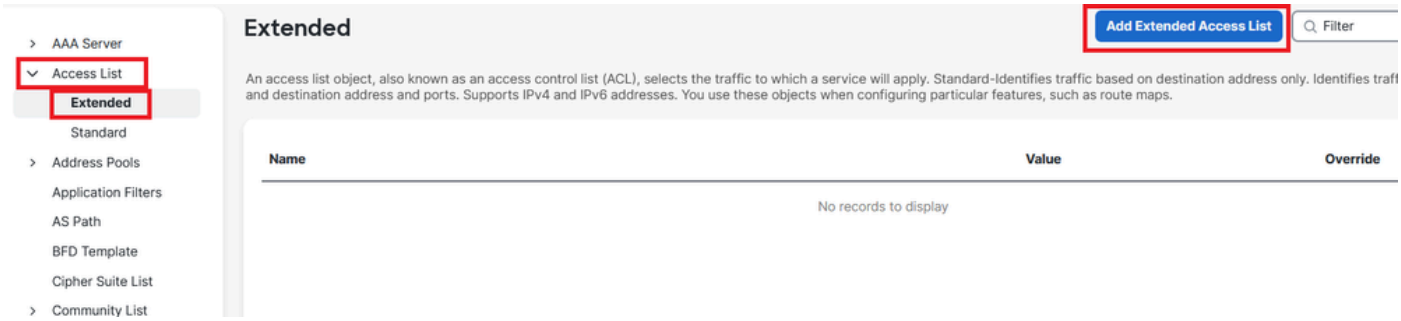

图 2.扩展访问列表菜单

添加新规则时，请注意您在搜索网络对象以选择源和目标时无法看到配置的FQDN对象。

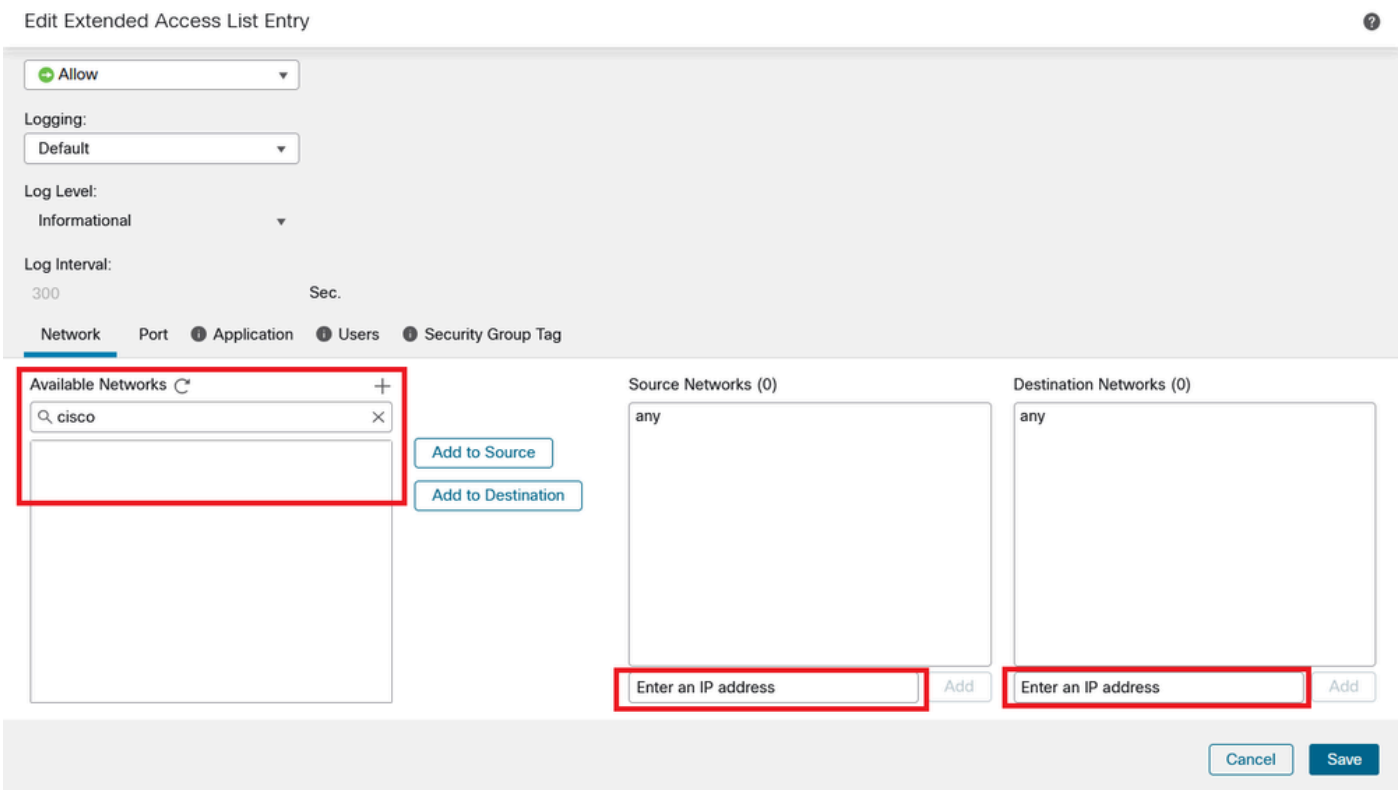

图 3.新建扩展访问列表规则菜单

第三步：创建无法命中的规则，以便创建扩展ACL并可用于PBR配置。

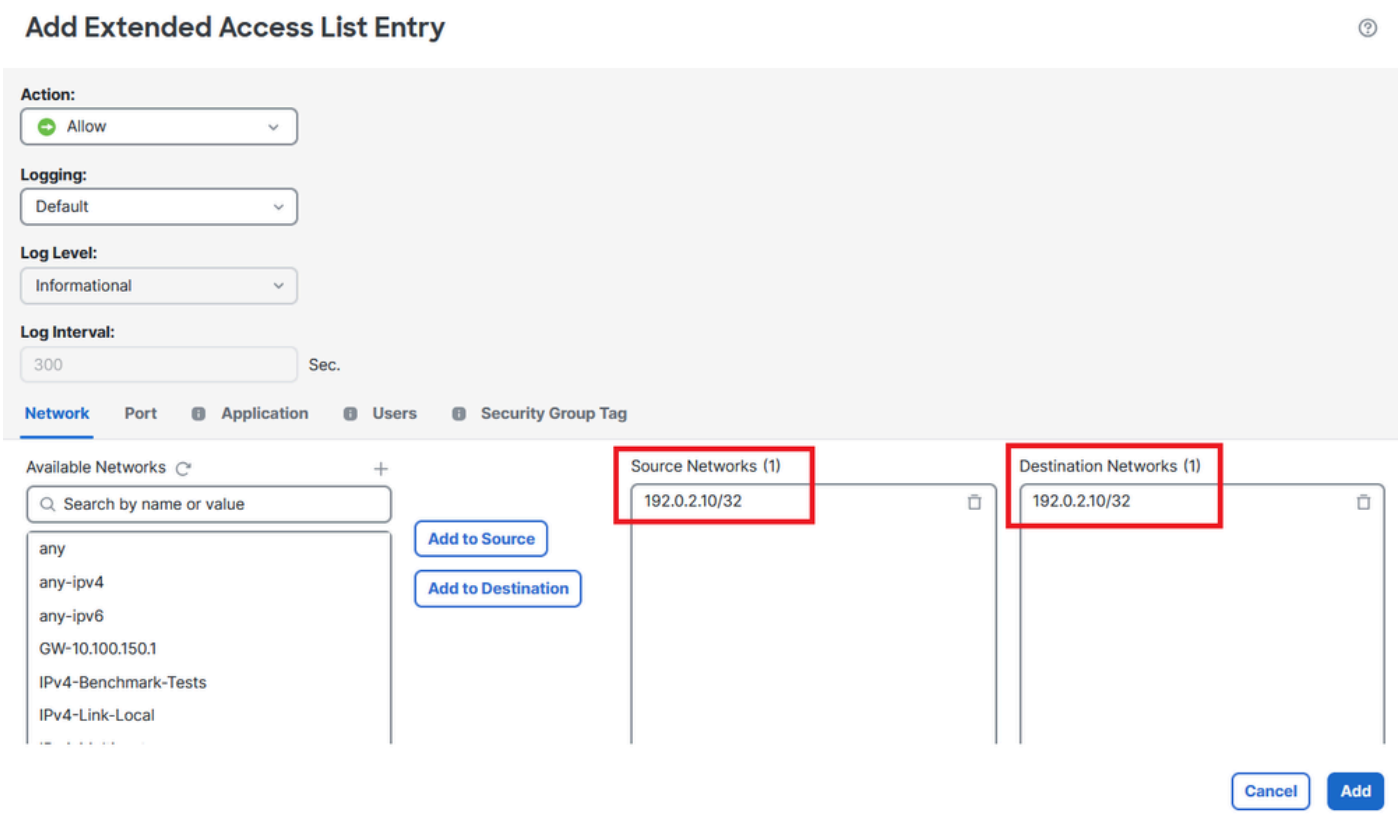

图 4.无法命中的访问列表规则配置

第四步：您需要在访问控制策略(ACP)上创建一个规则，以使用FQDN对象的FTD为目标。FMC将FQDN对象部署到FTD，以便您可以通过FlexConfig对象引用它。

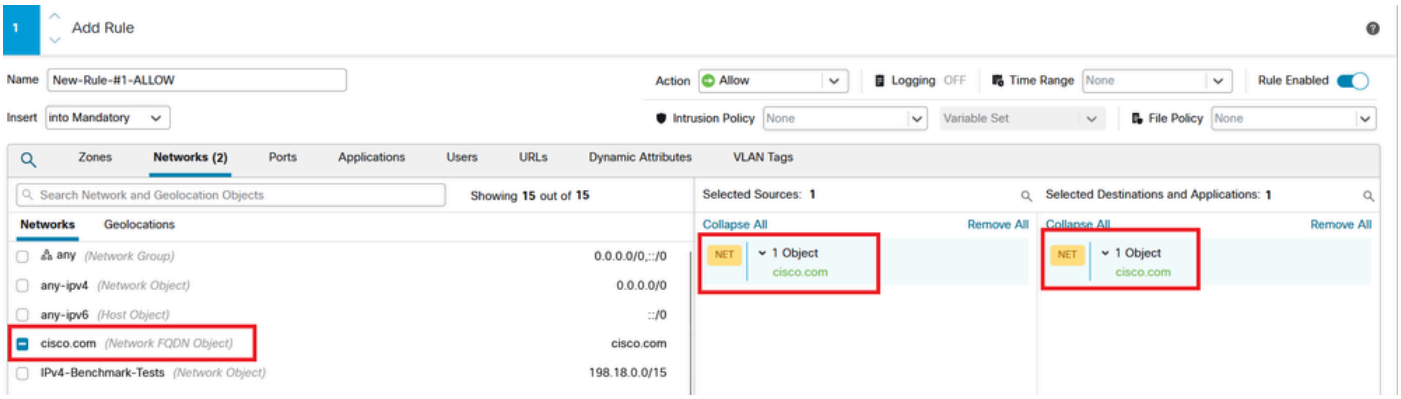

图 5.具有FQDN对象的ACP规则

第五步：导航到设备>设备管理上的FTD，选择路由选项卡，导航到基于策略的路由部分。

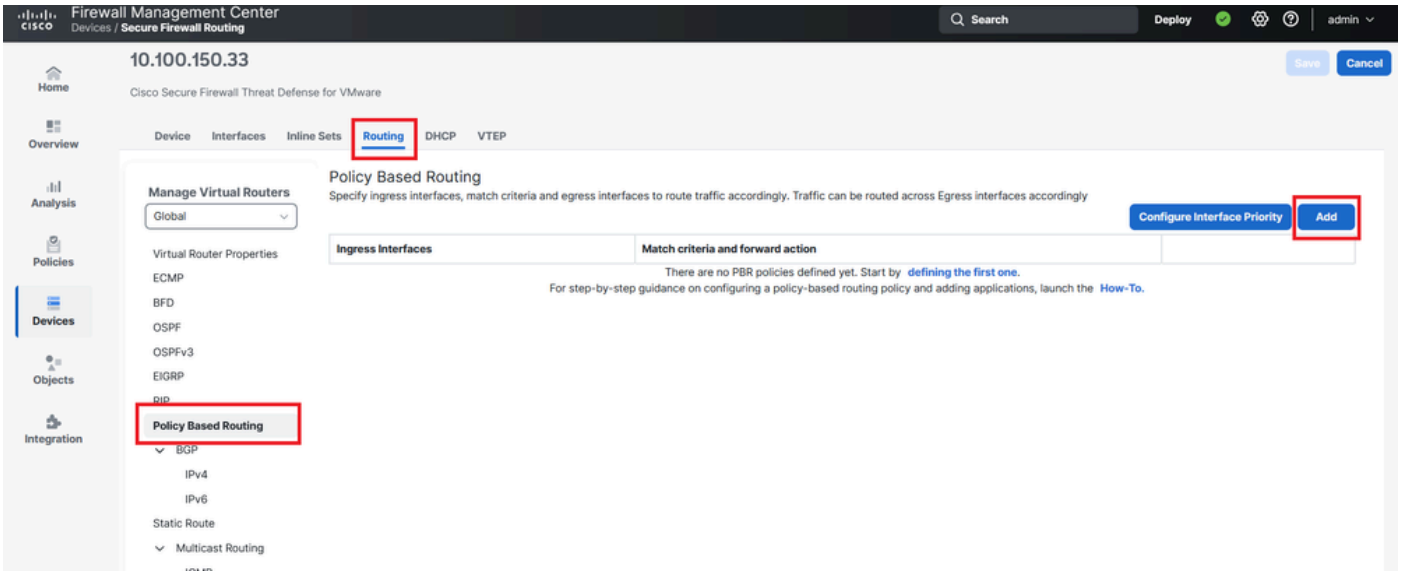

图 6.PBR菜单

第六步：使用之前配置的ACL在接口上配置PBR并进行部署。

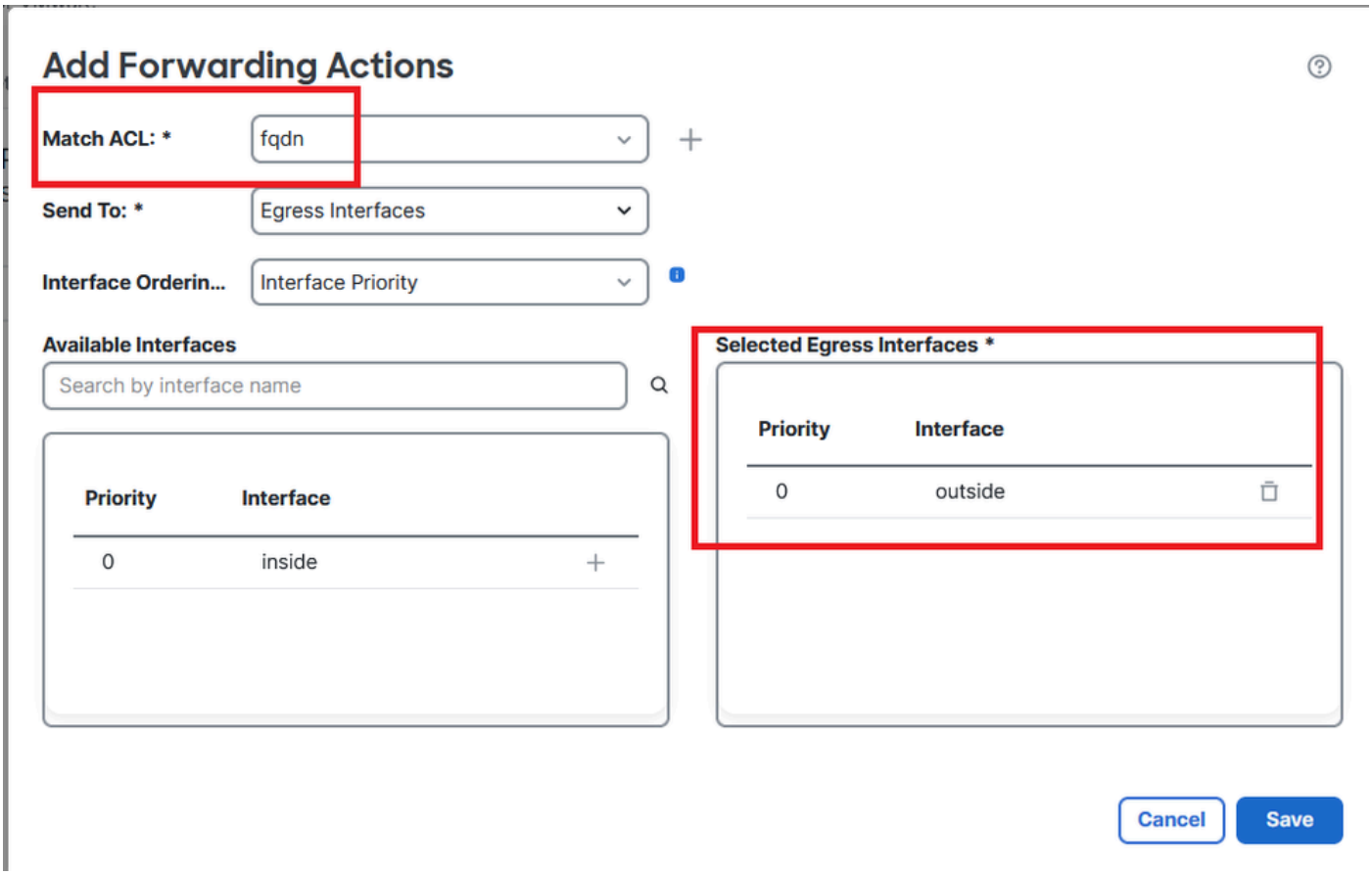

图 7.PBR接口和ACL选择菜单

步骤 7.导航到对象>对象管理> FlexConfig >对象，然后创建新对象。

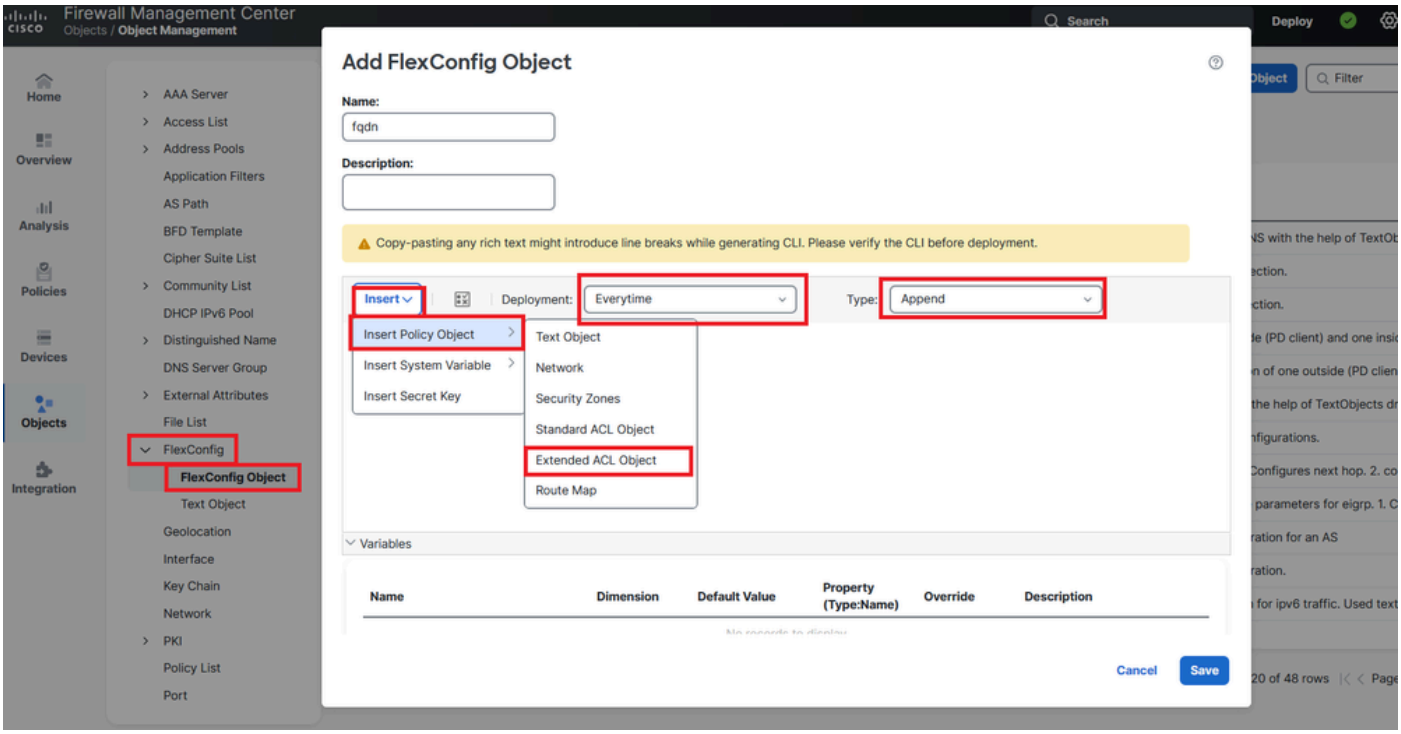

图 8.FlexConfig对象配置菜单

步骤 8选择Insert > Extended ACL Object，命名变量并选择之前创建的扩展ACL。该变量将使用您使用的名称进行添加。

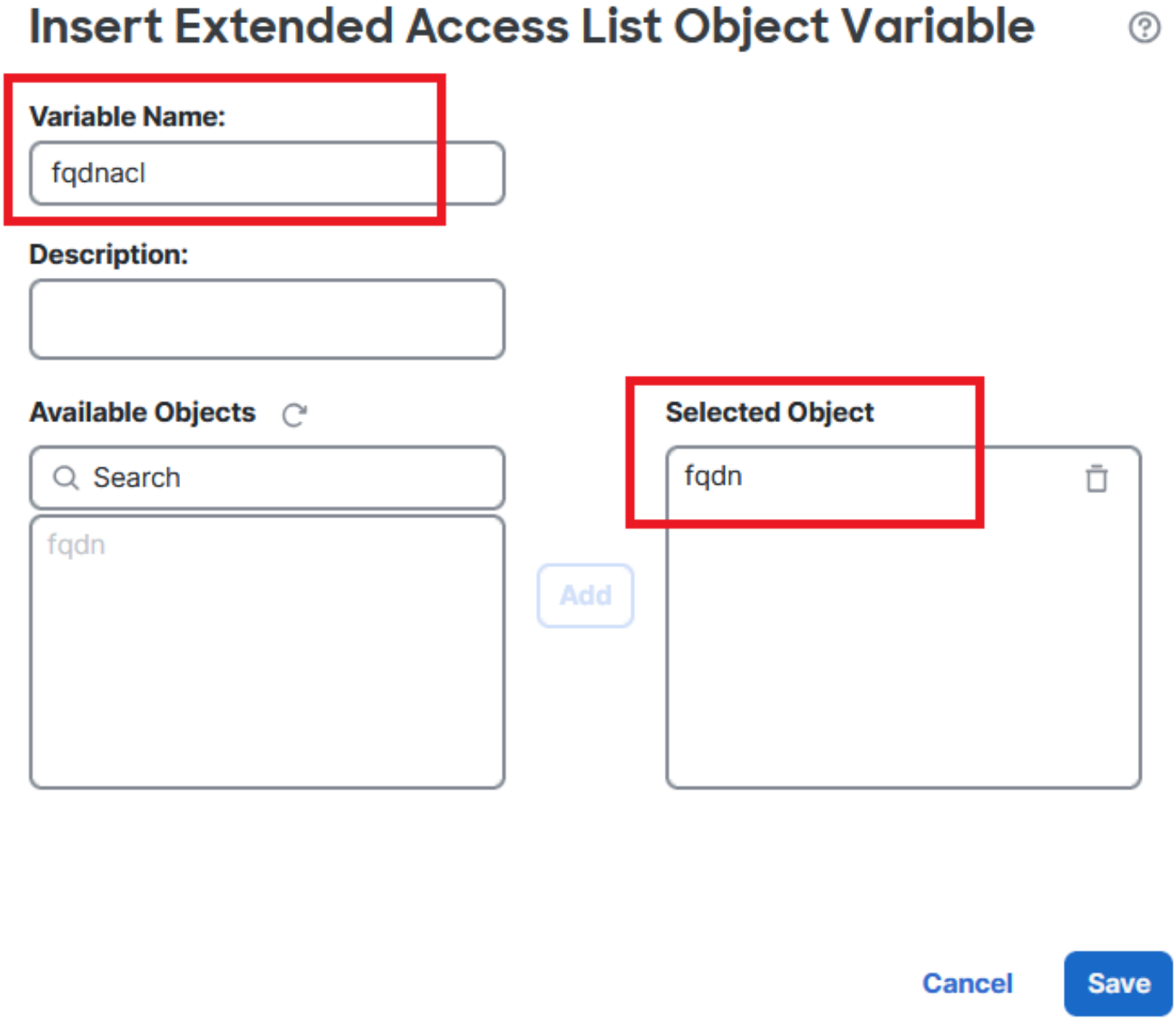

图 9.FlexConfig对象的变量创建

步骤 9为要使用ACL的每个FQDN对象输入此行。

<#root>

```
access-li $
```

```
extended permit ip any object
```

步骤 10将您的FlexConfig对象另存为Everytime > Append。

第11步：导航到设备> FlexConfig下的FlexConfig Policy菜单。

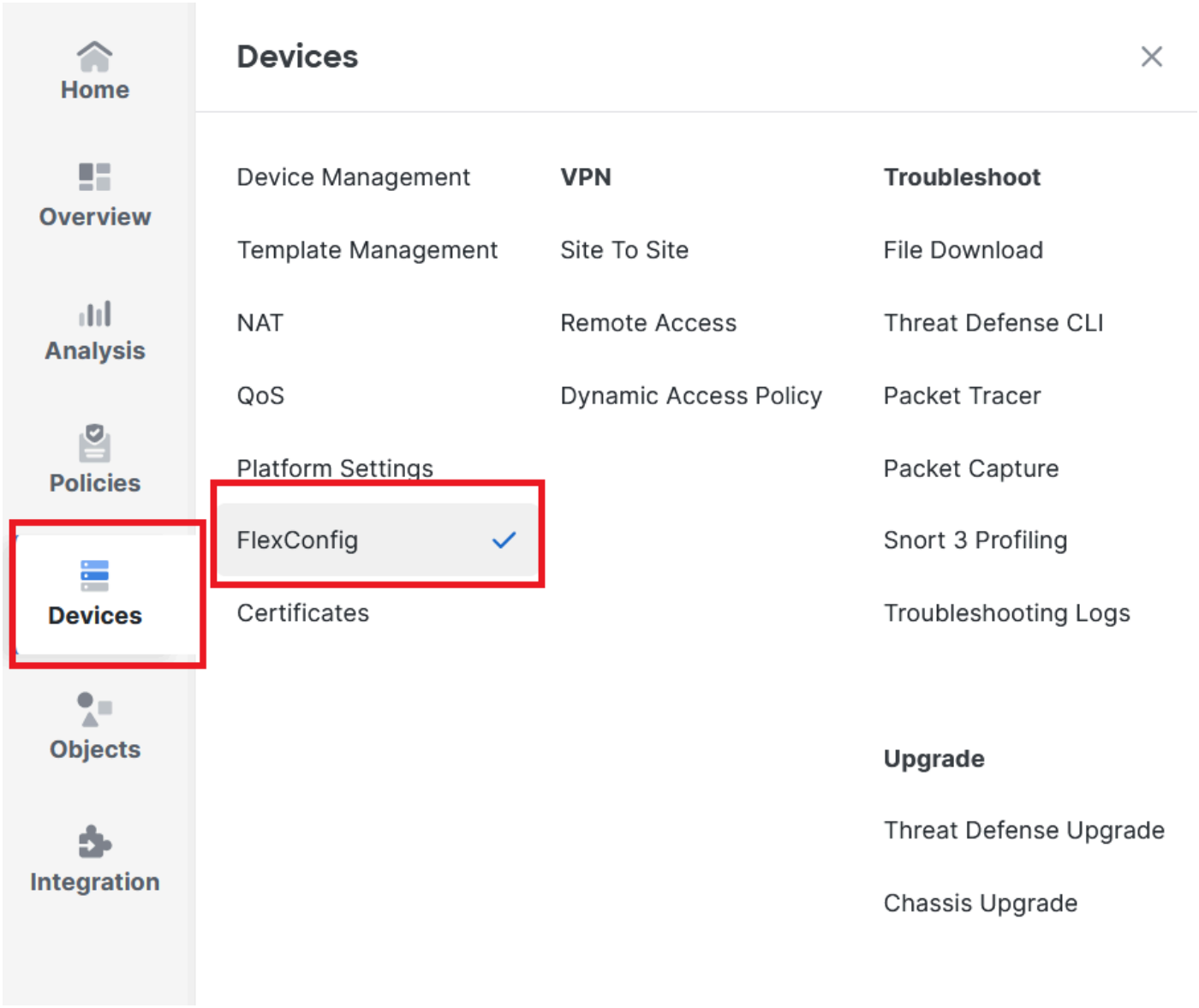

图 10.FlexConfig策略菜单的路径

步骤 12创建新的FlexConfig策略或选择已分配给您的FTD的策略。

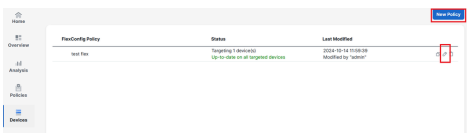

图 11.编辑或创建新的FlexConfig策略

步骤 13将FlexConfig对象添加到策略、保存和部署。

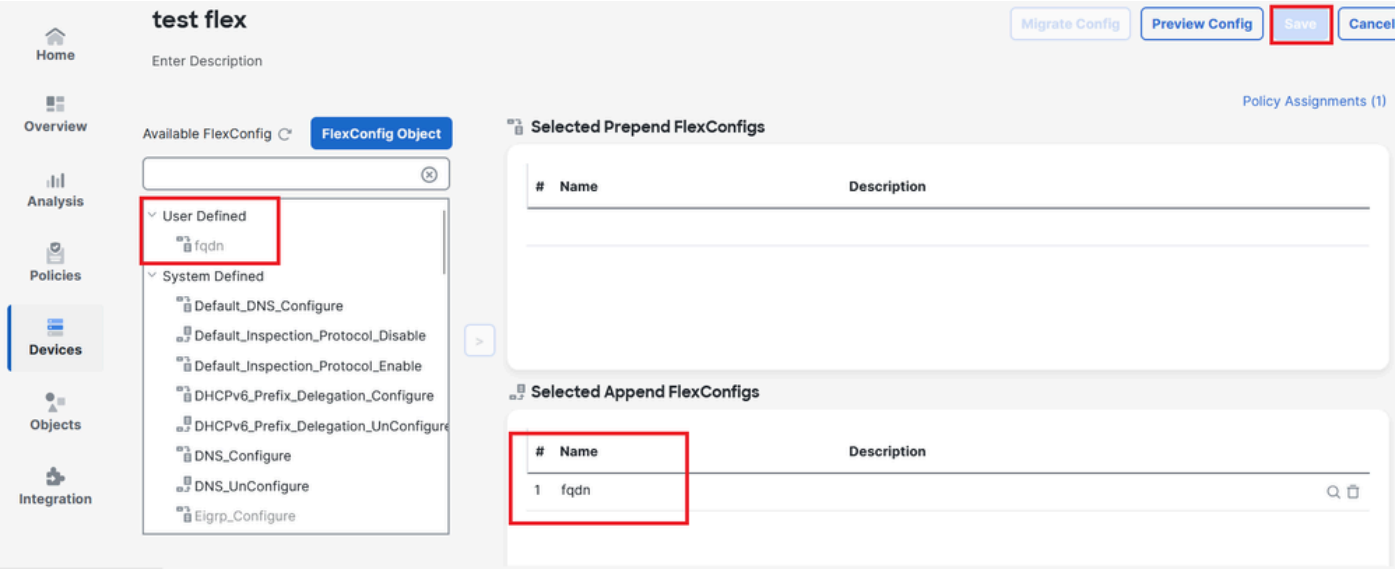

图 12.已将FlexConfig对象添加到FlexConfig策略中

验证

您的入口接口具有带有自动生成的路由映射的策略路由。

<#root>

firepower#

show run interface gi0/0

!
interface GigabitEthernet0/0
 nameif inside
 security-level 0
 ip address 10.100.151.2 255.255.255.0

policy-route route-map FMC_GENERATED_PBR_1727116778384

路由映射包含具有已用目标接口的选定ACL。

<#root>

firepower#

show run route-map FMC_GENERATED_PBR_1727116778384

!
route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn

set adaptive-interface cost outside

您的访问列表包含用于参考的主机以及通过FlexConfig添加的其他规则。

```
<#root>
firepower#
show run access-list fqdn

access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
access-list fqdn extended permit ip any object cisco.com
```

您可以从入口接口执行Packet Tracer作为源，以验证您是否已进入PBR阶段。

```
<#root>
firepower#
packet-tracer input inside tcp 10.100.150.1 12345 fqdn cisco.com 443

Mapping FQDN cisco.com to IP address 72.163.4.161

[...]
Phase: 3
Type: PBR-LOOKUP

Subtype: policy-route
Result: ALLOW
Elapsed time: 1137 ns
Config:

route-map FMC_GENERATED_PBR_1727116778384 permit 5

 match ip address fqdn

 set adaptive-interface cost outside

Additional Information:

 Matched route-map FMC_GENERATED_PBR_1727116778384, sequence 5, permit

 Found next-hop 10.100.150.1 using egress ifc outside
```

```
[...]
Result:

input-interface: inside(vrfid:0)


input-status: up
input-line-status: up

output-interface: outside(vrfid:0)


output-status: up
output-line-status: up
Action: allow
Time Taken: 140047752 ns
```

常见问题

PBR在第二次部署后停止工作

请验证访问列表是否仍包含FQDN对象规则。

在这种情况下，您可以看到此规则已不存在。

```
firepower# show run access-list fqdn
access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
firepower#
```

验证FlexConfig对象是否设置为Deployment： Everytime和Type： Append。该规则每次都应用于未来部署。

FQDN无法解析

当您尝试ping FQDN时，您会收到有关无效主机名的消息。

```
<#root>

firepower#

ping cisco.com

                ^

ERROR: % Invalid Hostname
```

检验DNS配置。您的服务器组上必须有可访问的DNS服务器，并且域名查找接口必须能够访问它们

◦

<#root>

firepower#

show run dns

dns domain-lookup outside

DNS server-group DefaultDNS
DNS server-group dns

name-server 208.67.222.222

name-server 208.67.220.220

dns-group dns

firepower#

ping 208.67.222.222

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.67.222.222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 170/202/280 ms
firepower#

ping cisco.com

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.163.4.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/190 ms.

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）。