为访问控制规则配置基于FQDN的对象

目录

简介

本文档介绍如何通过防火墙管理中心(FMC)配置完全限定域名(FQDN)对象，以及如何在访问规则创建中使用FQDN对象。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解Firepower技术。
- 了解在Firesight管理中心(FMC)上配置访问控制策略

使用的组件

本文档中的信息基于以下软件和硬件版本：

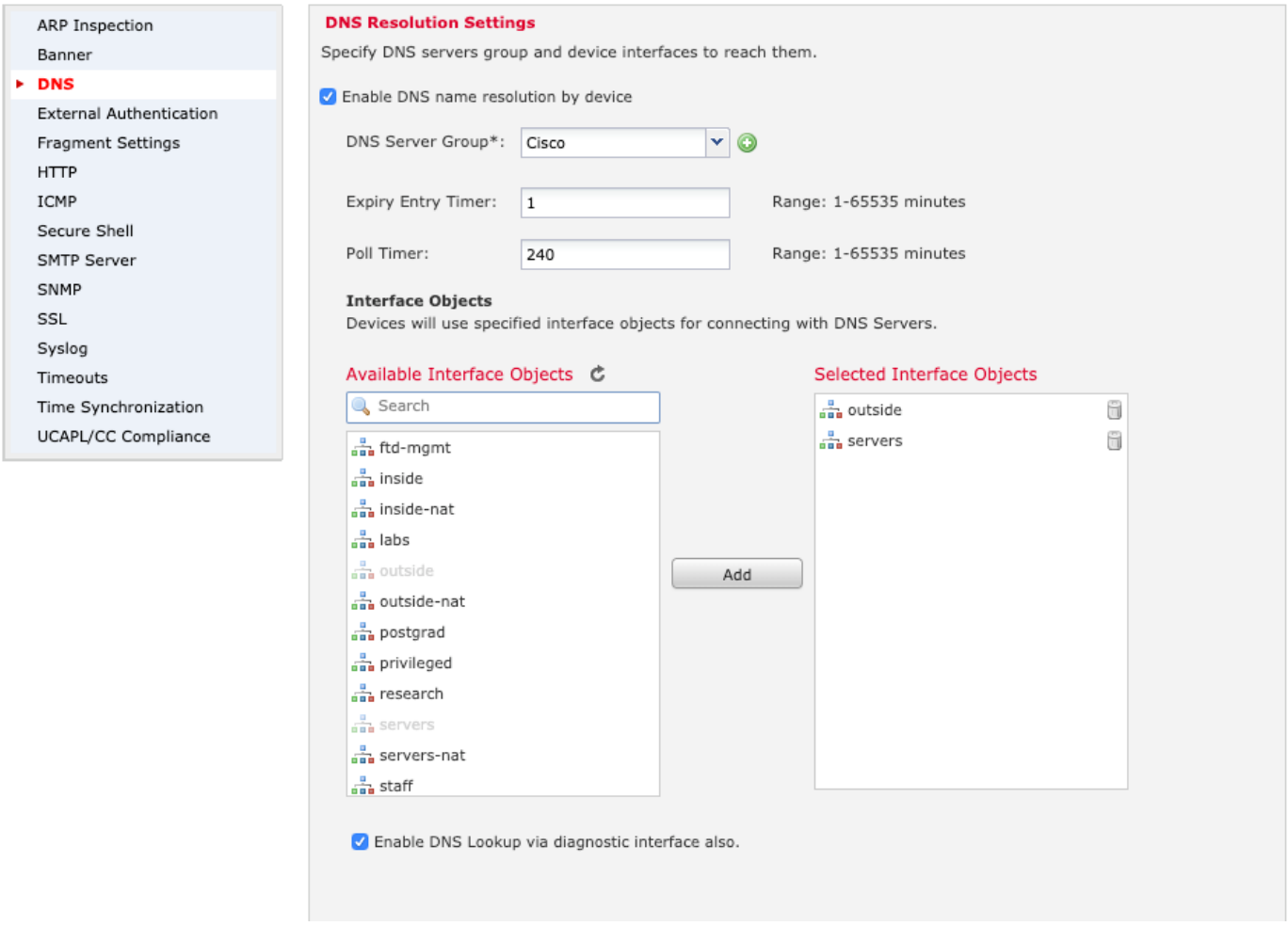
- 运行版本6.3及更高版本的Firepower管理中心。
- 运行版本6.3及更高版本的Firepower威胁防御。

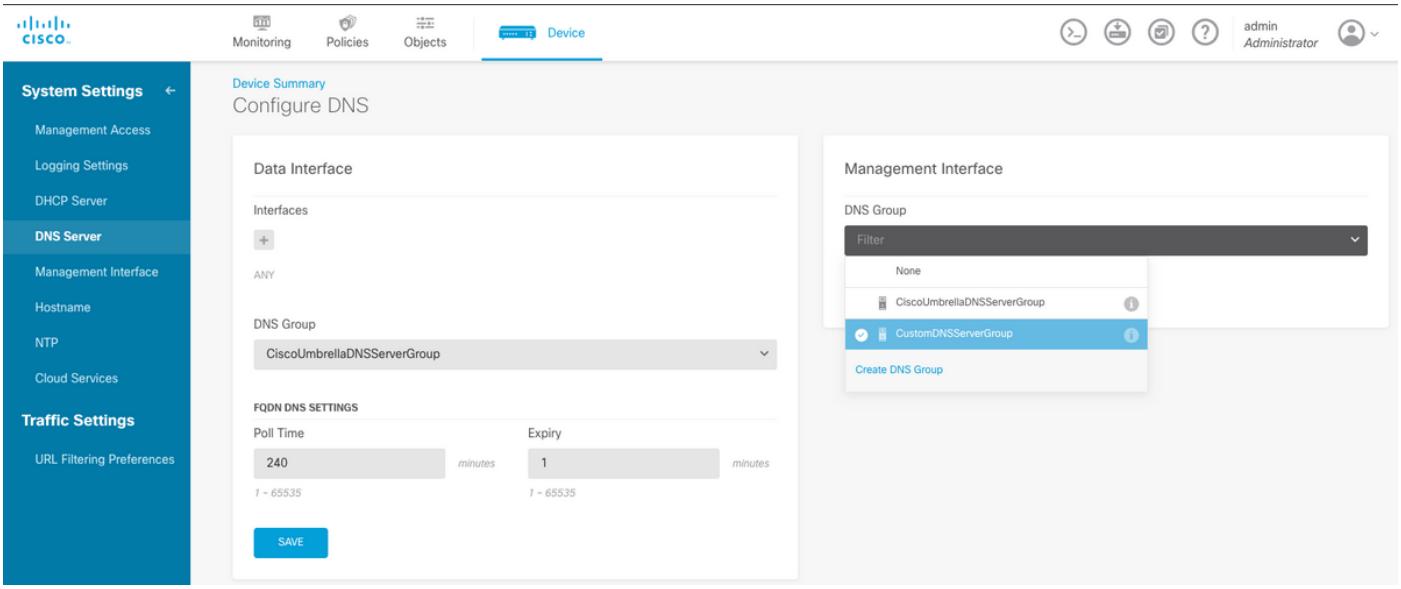
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

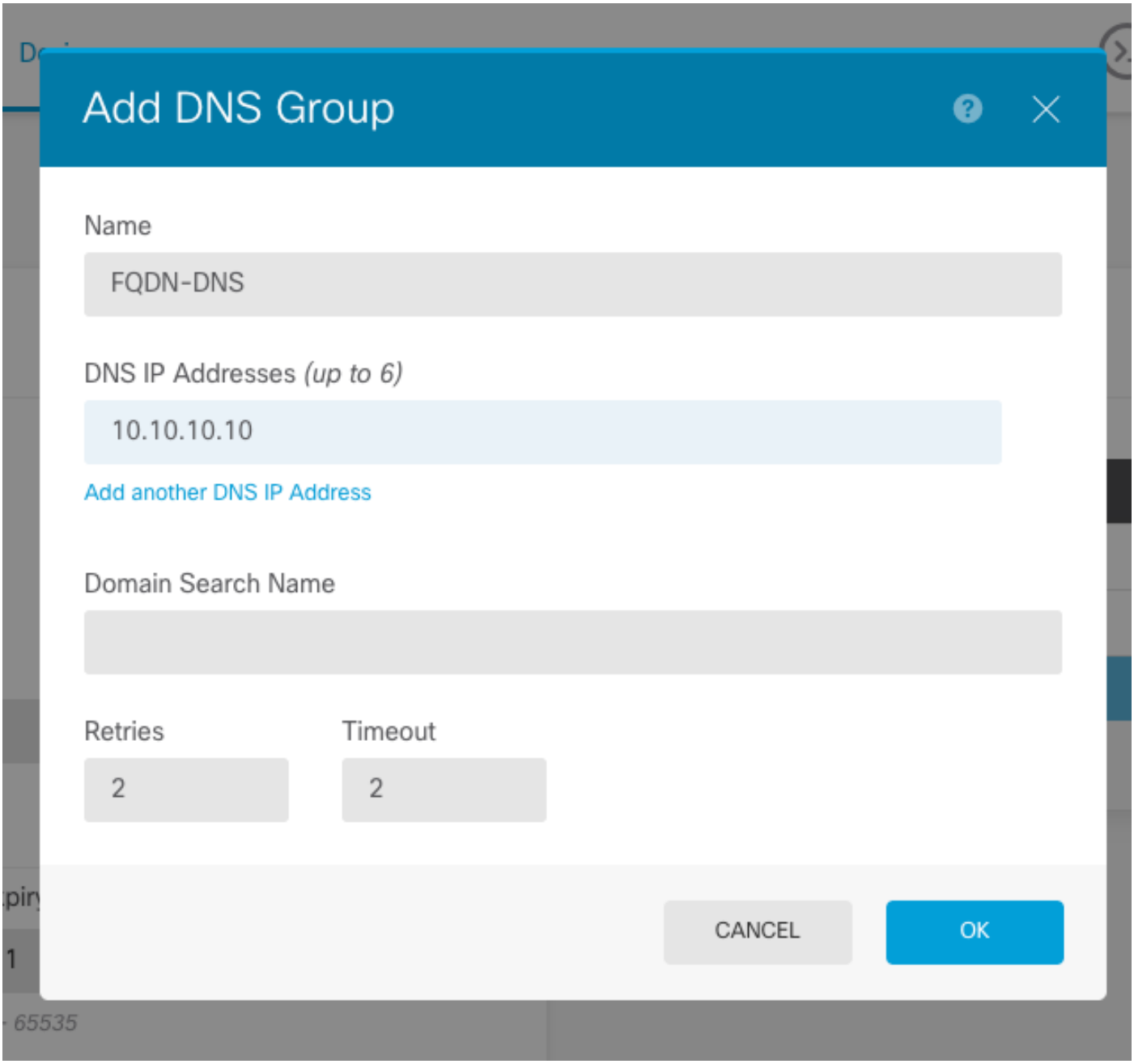
配置

步骤1.要配置和使用基于FQDN的对象，请首先在Firepower威胁防御上配置DNS。

登录FMC并导航至Devices **> Platform Settings > DNS**。

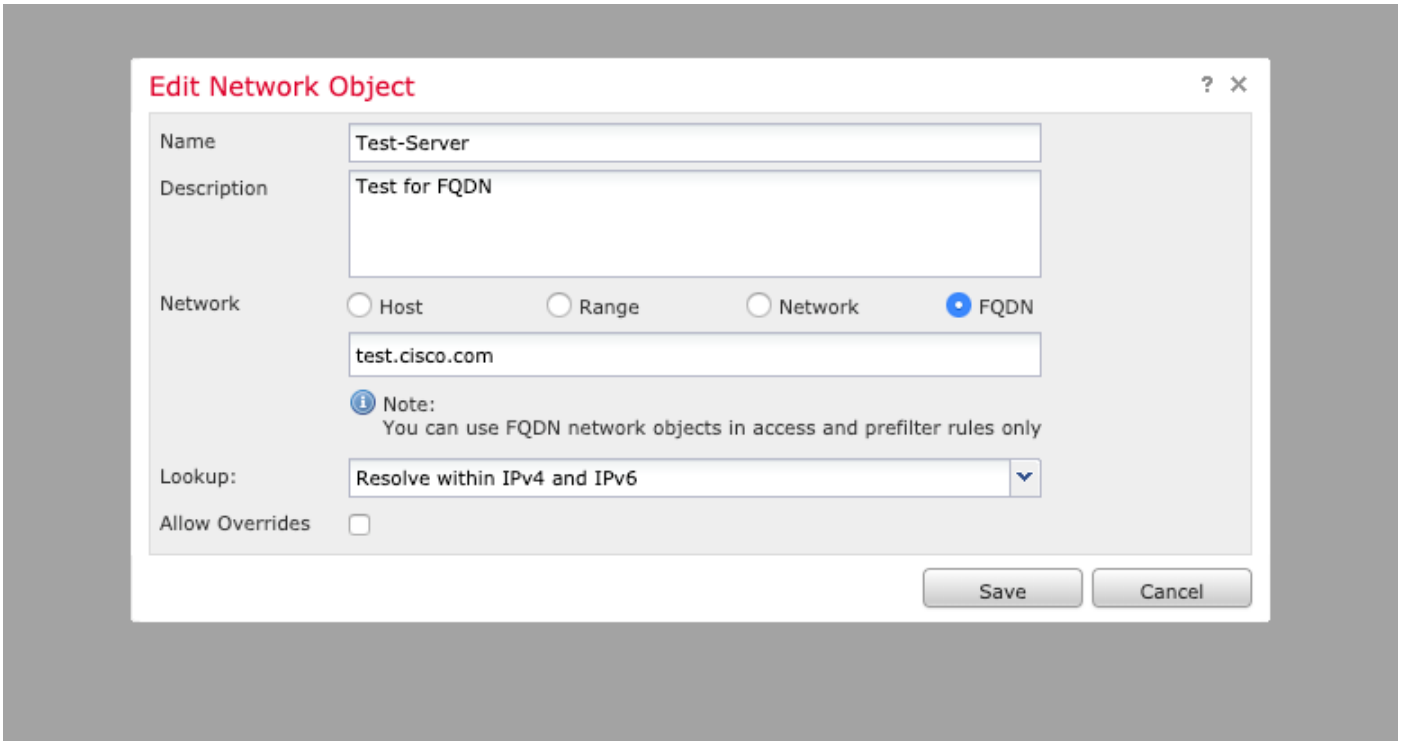

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP
ICMP
Secure Shell
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
UCAPL/CC Compliance
DNS Resolution Settings
Specify DNS servers group and device interfaces to reach them.
Enable DNS name resolution by device
DNS Server Group*:
Cisco
Expiry Entry Timer:
1
Range: 1-65535 minutes
Poll Timer:
240
Range: 1-65535 minutes
Interface Objects
Devices will use specified interface objects for connecting with DNS Servers.
Available Interface Objects
Search
ftd-mgmt
inside
inside-nat
labs
outside
outside-nat
postgrad
privileged
research
servers
servers-nat
staff
Add
Selected Interface Objects
outside
servers
Enable DNS Lookup via diagnostic interface also.

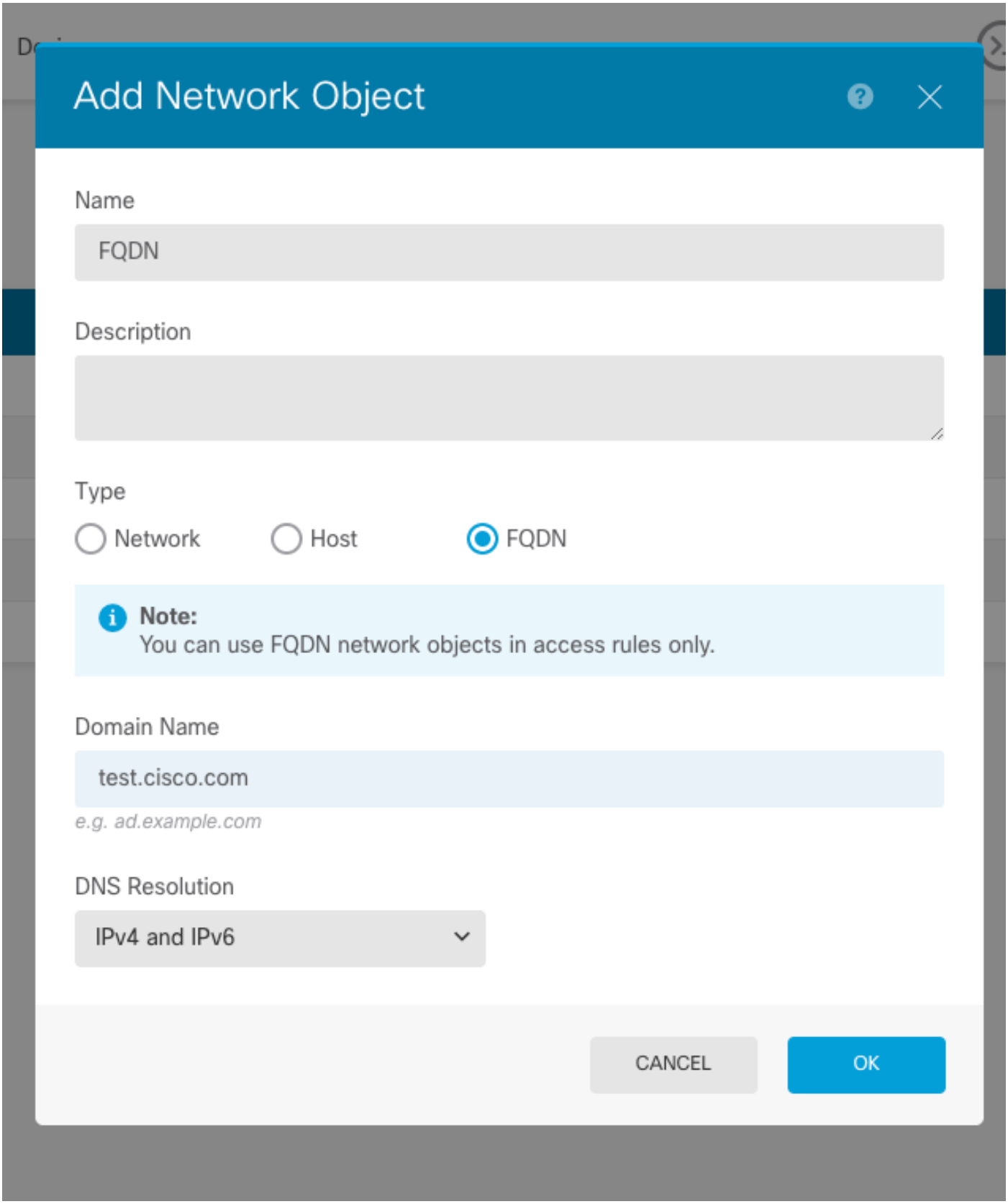

Monitoring
Policies
Objects
Device
admin
Administrator
System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
NTP
Cloud Services
Traffic Settings
URL Filtering Preferences
Device Summary
Configure DNS
Data Interface
Interfaces
ANY
DNS Group
CiscoUmbrellaDNSServerGroup
FQDN DNS SETTINGS
Poll Time
240
minutes
1 - 65535
Expiry
1
minutes
1 - 65535
SAVE
Management Interface
DNS Group
Filter
None
CiscoUmbrellaDNSServerGroup
CustomDNSServerGroup
Create DNS Group



注意：确保在配置DNS后将系统策略应用到FTD。（配置的DNS服务器应解析将使用的FQDN）

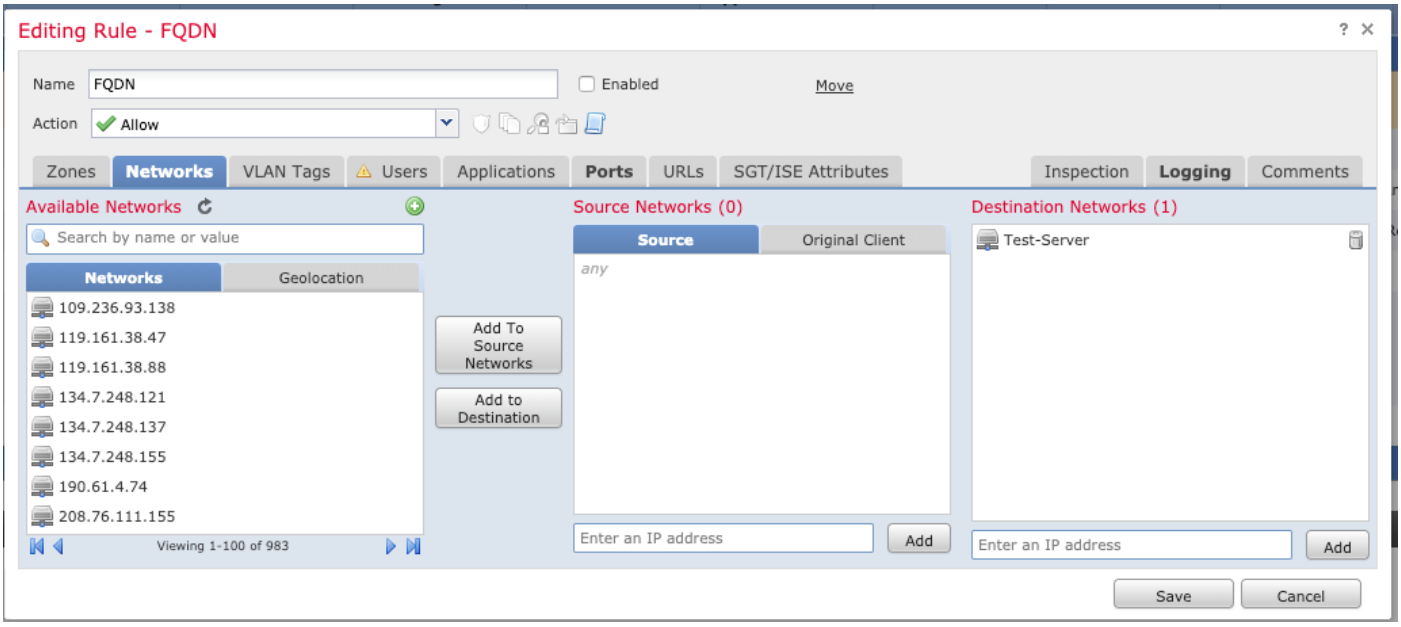
步骤2.创建FQDN对象，以便导航到**Objects > Object Management > Add Network > Add Object。**

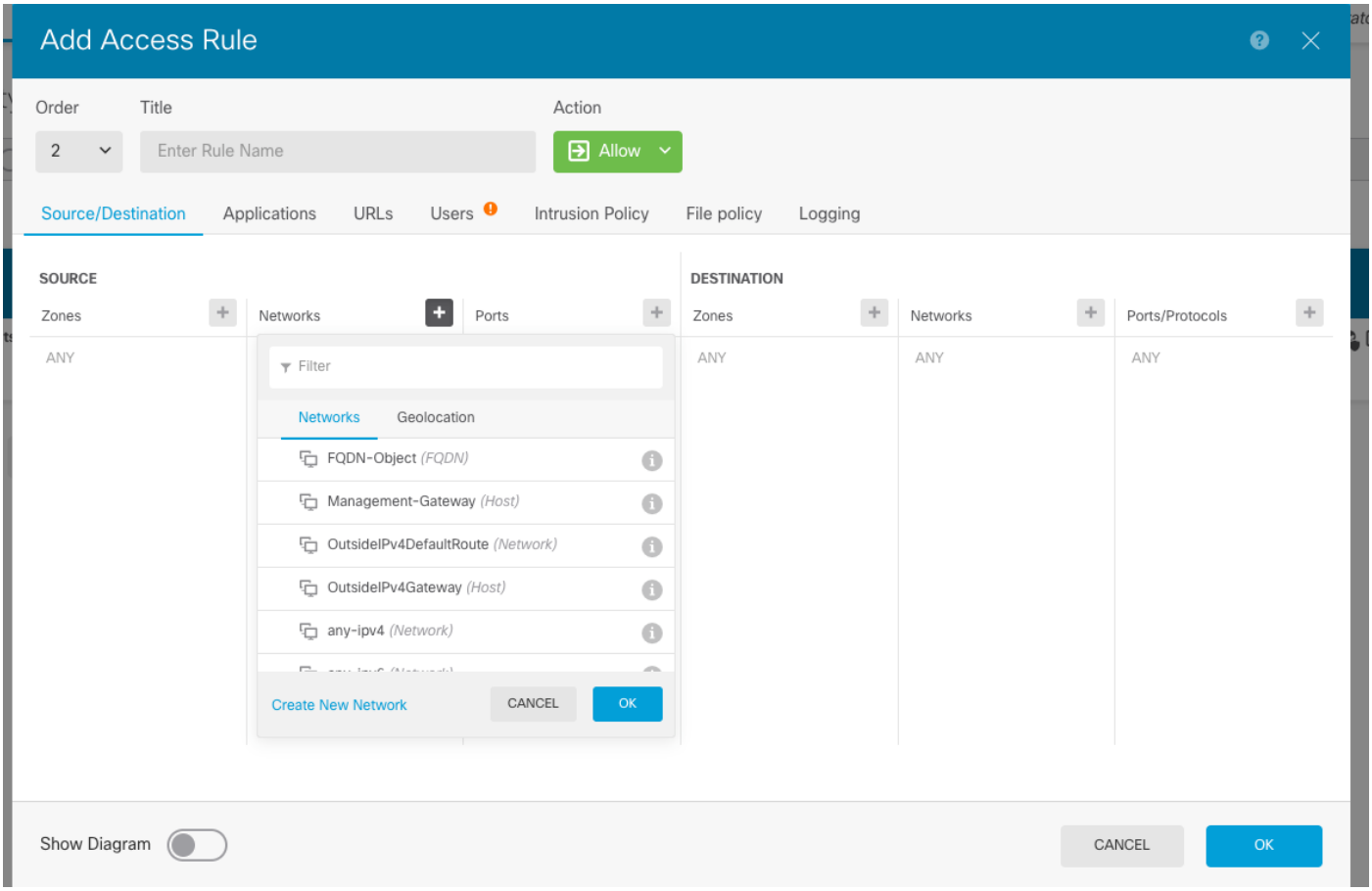

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



步骤3.导航至Policies > Access Control，创建访**问控制规则。**

注意：您可以根据要求创建规则或修改现有规则。FQDN对象可在源和/或目标网络中使用。



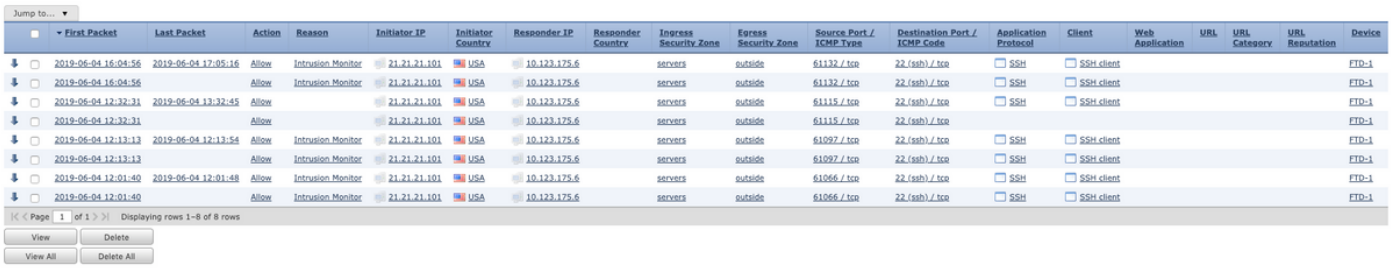


确保在配置完成后应用策略。

验证

从客户端计算机发起流量，该流量应触发创建的基于FQDN的规则。

在FMC上，导航至**Events > Connection Events，过滤特定流量。**



故障排除

DNS服务器应该能够解析FQDN对象，这可以通过CLI运行以下命令来验证：

- **系统支持diagnostic-cli**
- **show fqdn**

∘