配置FQDN访问控制规则的基于对象

Contents

Introduction

本文通过防火墙管理中心(FMC)在访问规则创建描述完全合格的域名(FQDN)对象的配置和如何使用FQDN对象。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Firepower技术知识。
- 配置由于Firesight管理中心(FMC)的访问控制策略知识

Components Used

本文档中的信息基于以下软件和硬件版本：

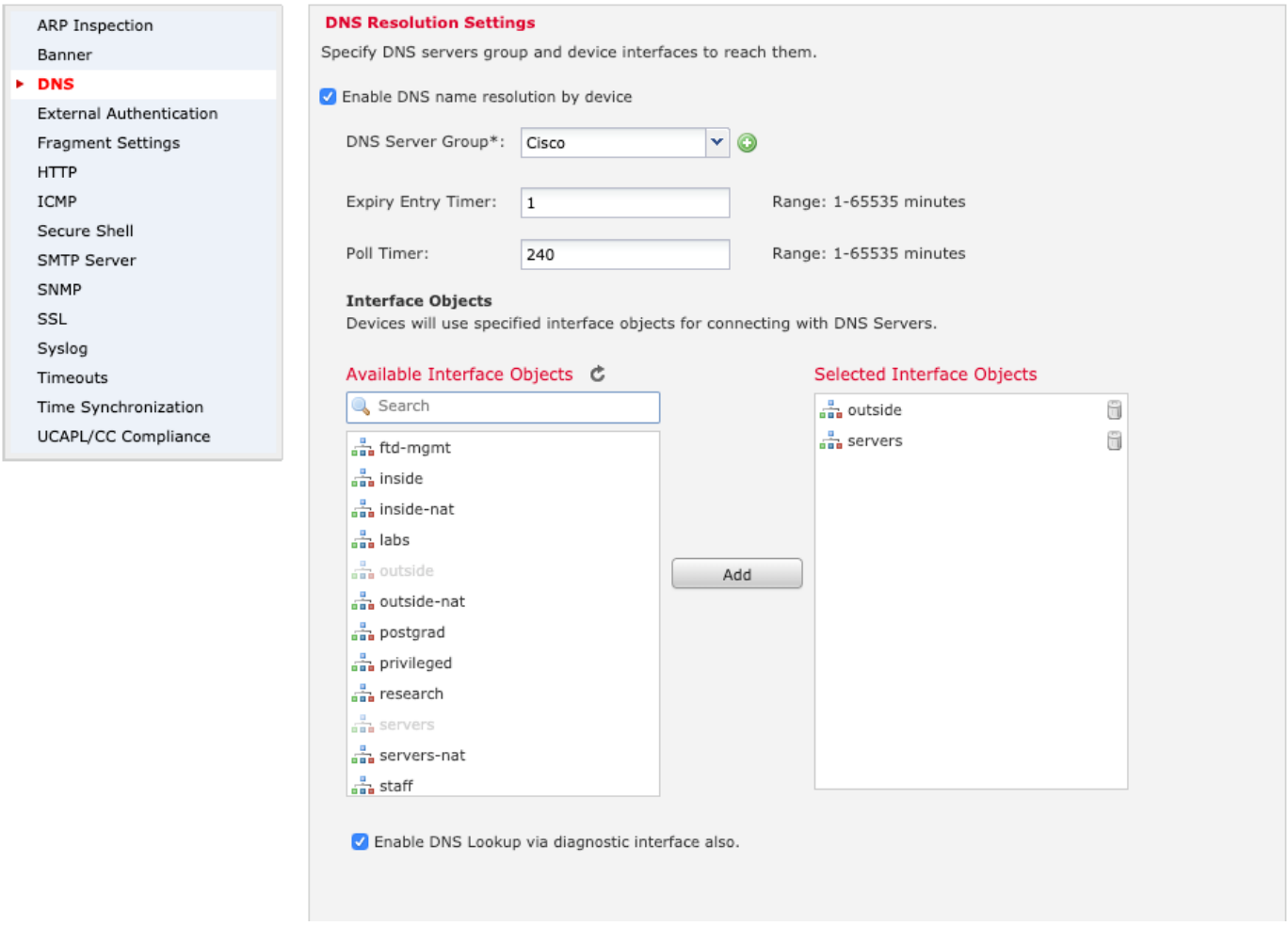
- Firepower运行版本6.3和以上的管理中心。
- Firepower运行版本6.3和以上的威胁防御。

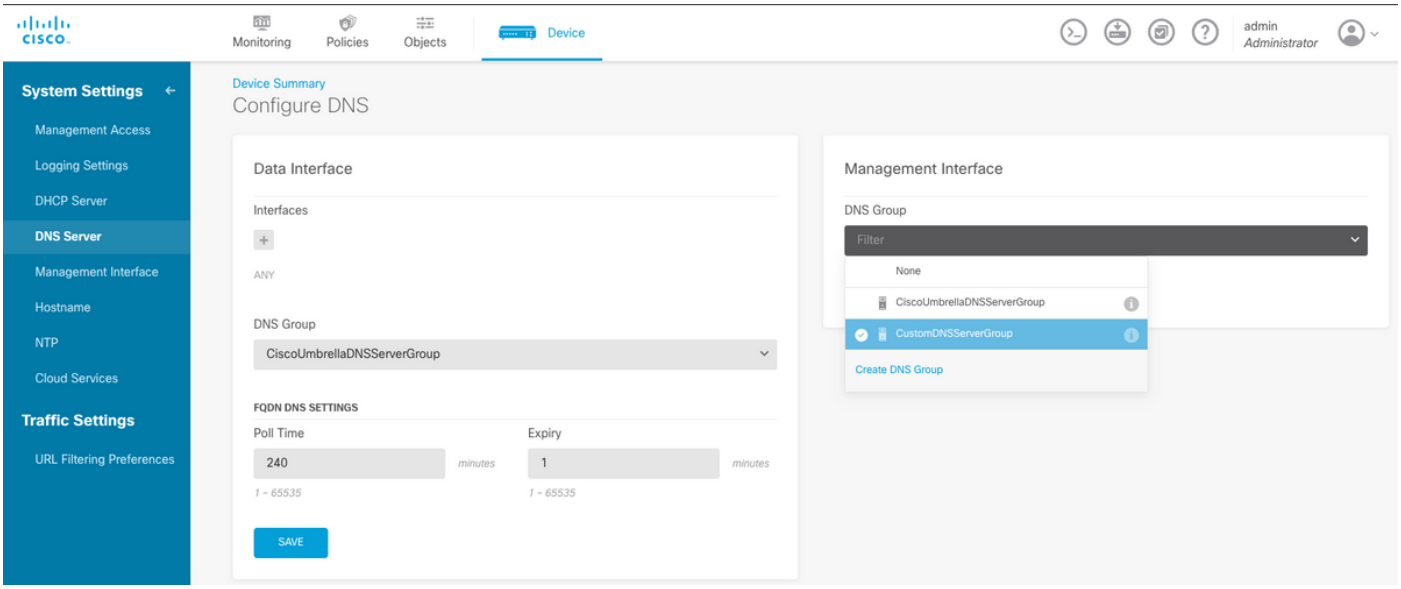
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

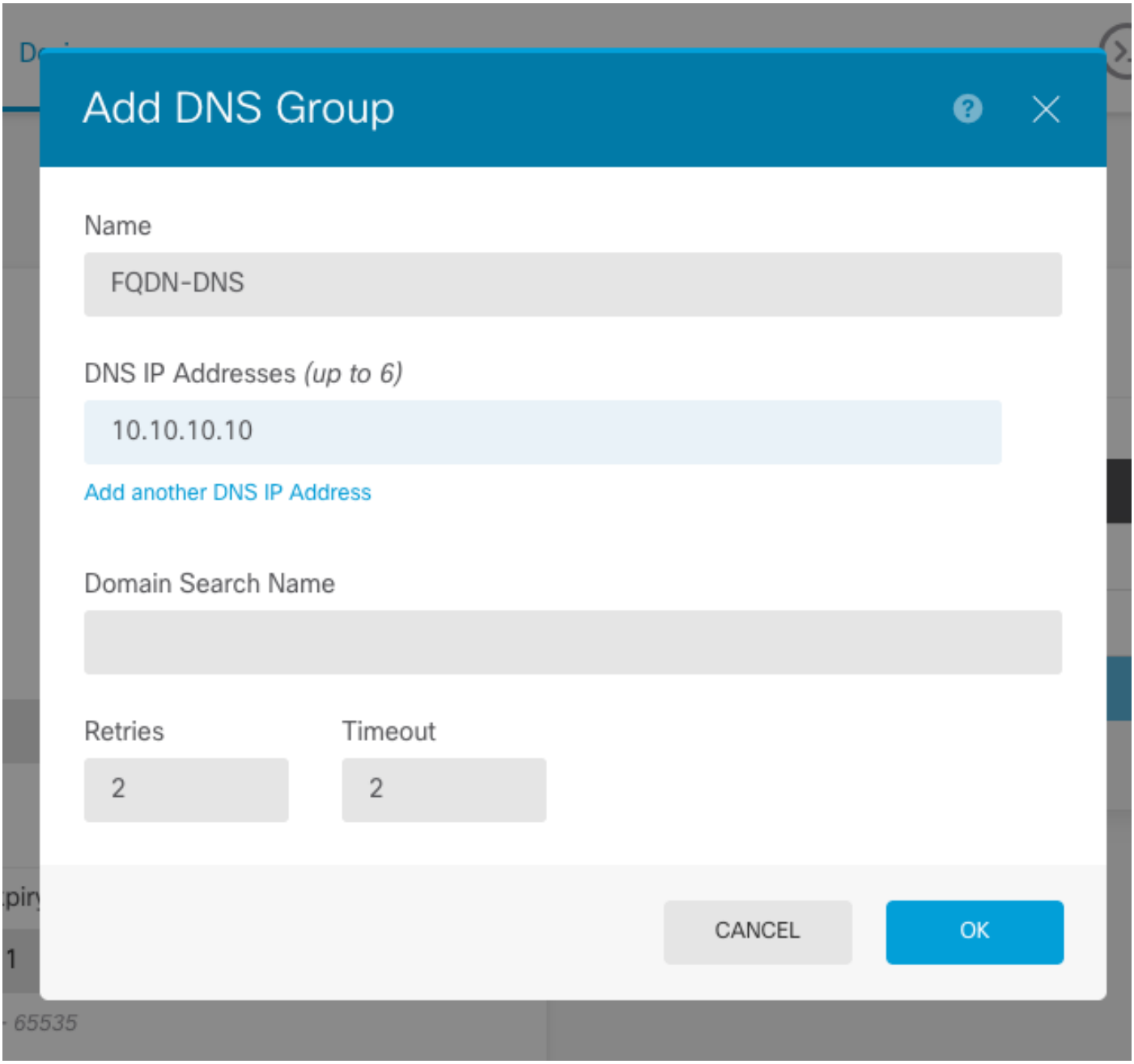
Configure

步骤1.为了配置和使用FQDN根据对象，第一，配置在Firepower威胁防御的DNS。

登陆对FMC并且连接到**设备>平台设置> DNS**。

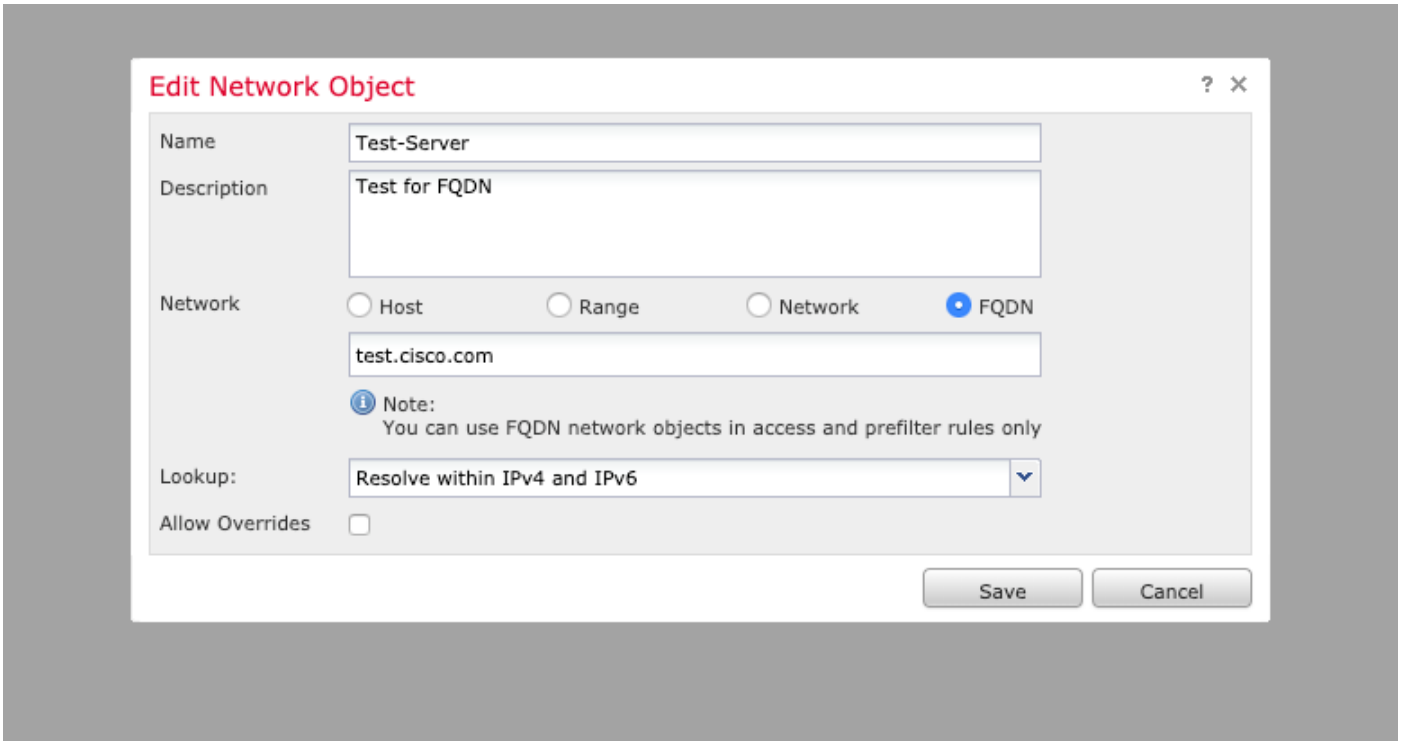

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP
ICMP
Secure Shell
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
UCAPL/CC Compliance
DNS Resolution Settings
Specify DNS servers group and device interfaces to reach them.
Enable DNS name resolution by device
DNS Server 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.

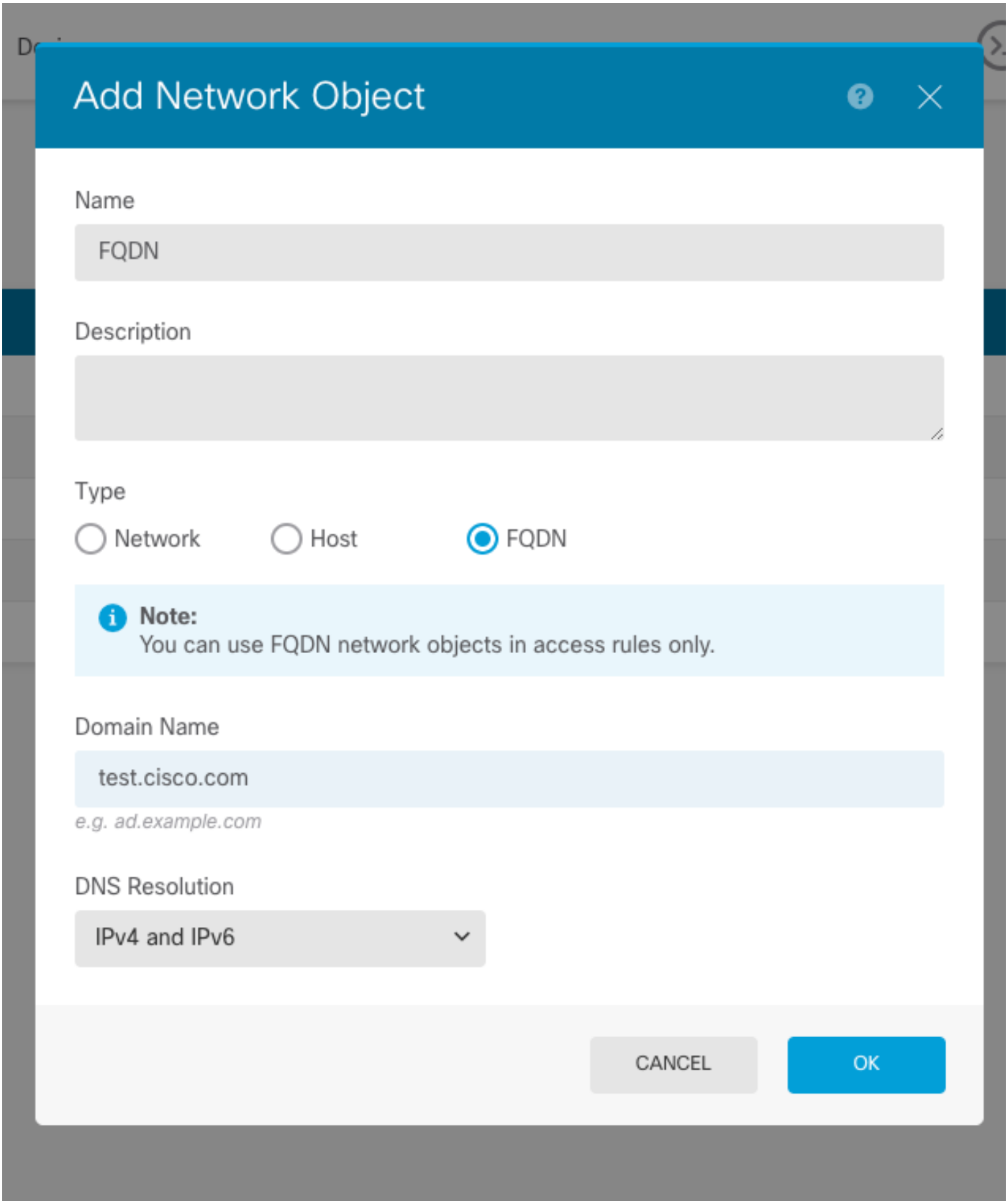

Monitoring
Policies
Objects
Device
admin
Administrator
System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
NTP
Cloud Services
Traffic Settings
URL Filtering Preferences
Device Summary
Configure DNS
Data Interface
Interfaces
ANY
DNS Group
CiscoUmbrellaDNSServerGroup
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



Note:保证系统策略被运用于FTD在配置DNS以后。(被配置的DNS服务器应该解决将使用)的FQDN

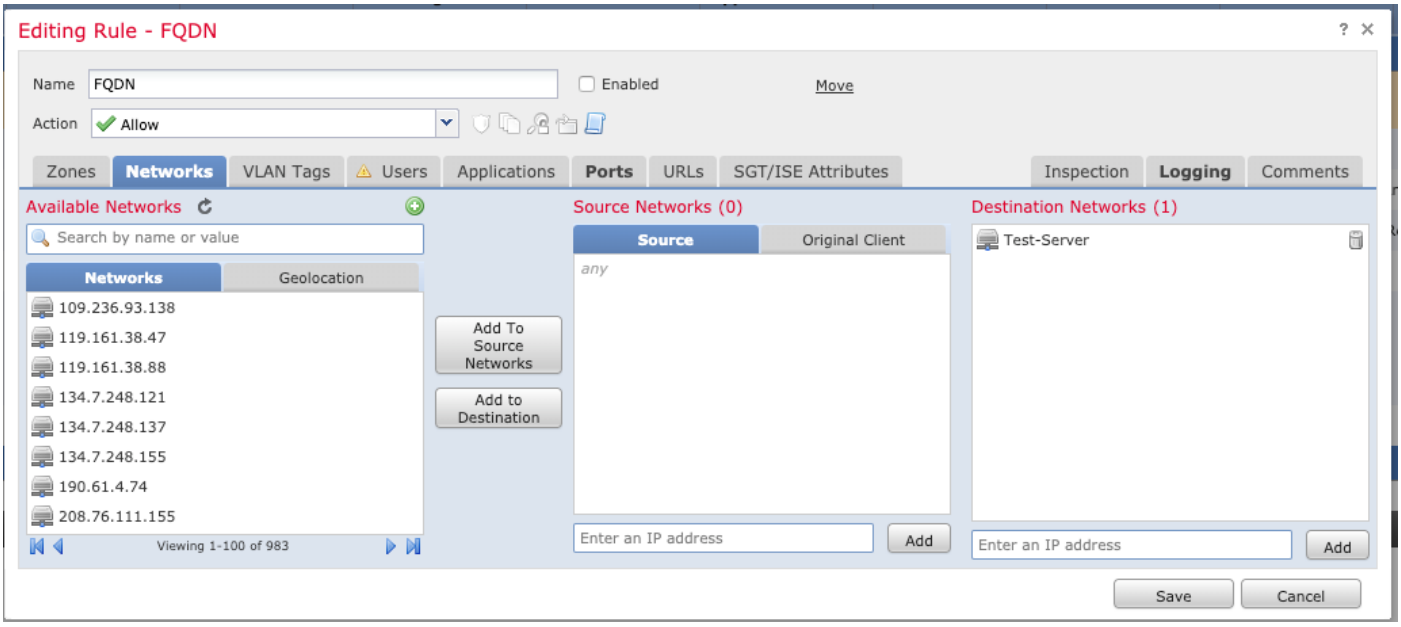
步骤2.创建FQDN对象，为了执行连接对**对象>对象Management>添加Network > Add对象。**

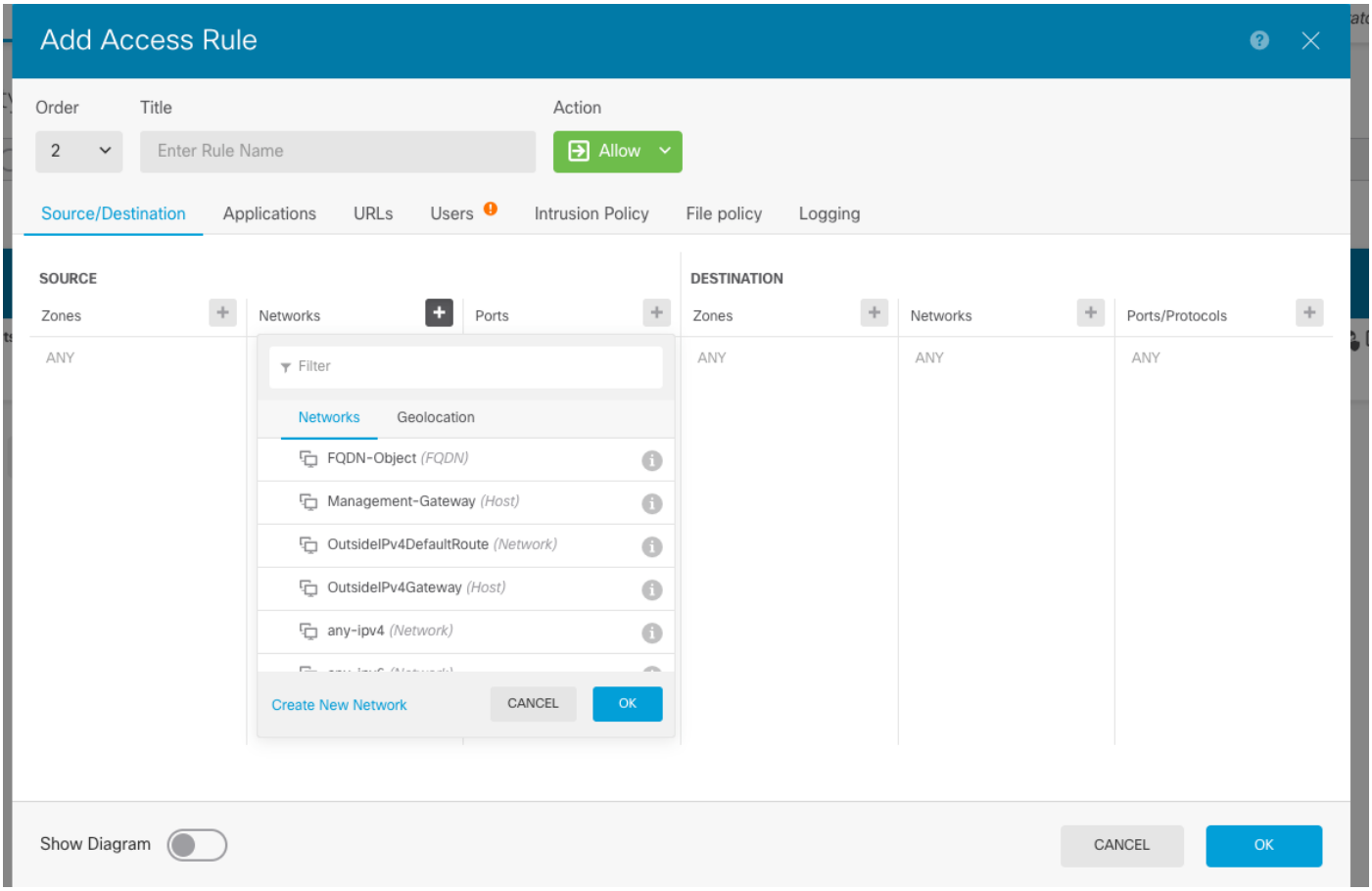

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



步骤3.通过连接创建访问控制规则到**策略>访问控制。**

Note:您能创建规则或修改根据需求的现有的规则。FQDN对象可以或者用于来源和目的地网络。



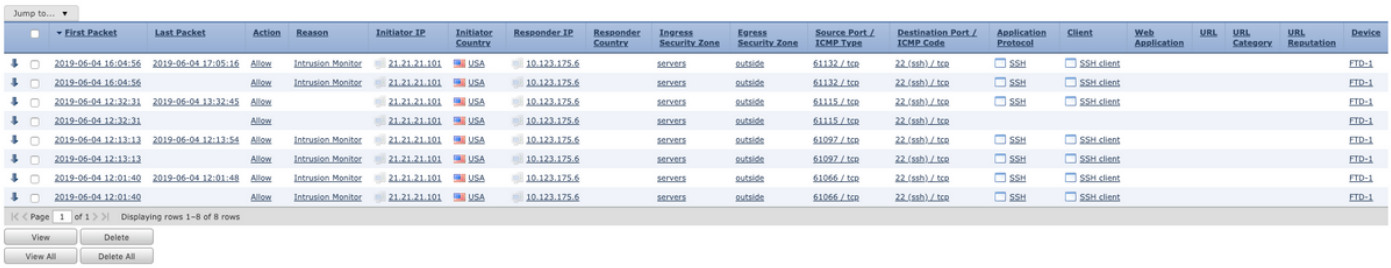


保证策略适用，在配置完成后。

Verify

初始化从预计触发被创建的FQDN基于规则的客户端机器的数据流。

在FMC，请连接对**事件>连接事件，特定的流量的过滤器。**



Troubleshoot

DNS服务器应该能解决FQDN对象，这可以从CLI被验证运行这些命令：

- **系统支持诊断CLI**
- **显示fqdn**

.o