Configure FQDN Based Object for Access Control Rule

Contents

Introduction

This document describes the configuration of the Fully Qualified Domain Name (FQDN) object through the Firewall Management Center (FMC) and how to use FQDN object in the access rule creation.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower Technology.
- Knowledge of configuring access control policy on Firesight Management Center (FMC)

Components Used

The information in this document is based on these software and hardware versions:

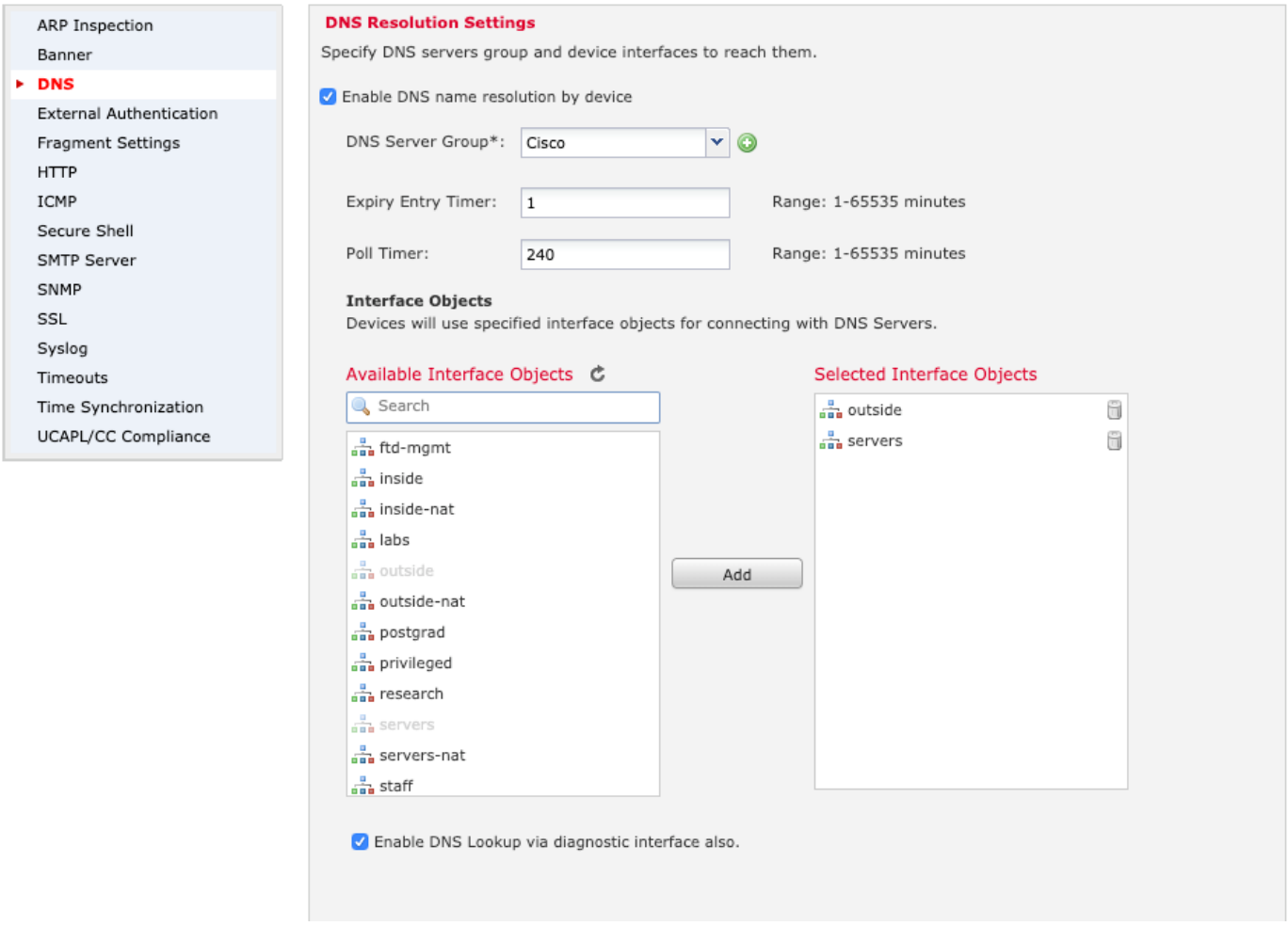
- Firepower Management Center running version 6.3 and above.
- Firepower Threat Defense running version 6.3 and above.

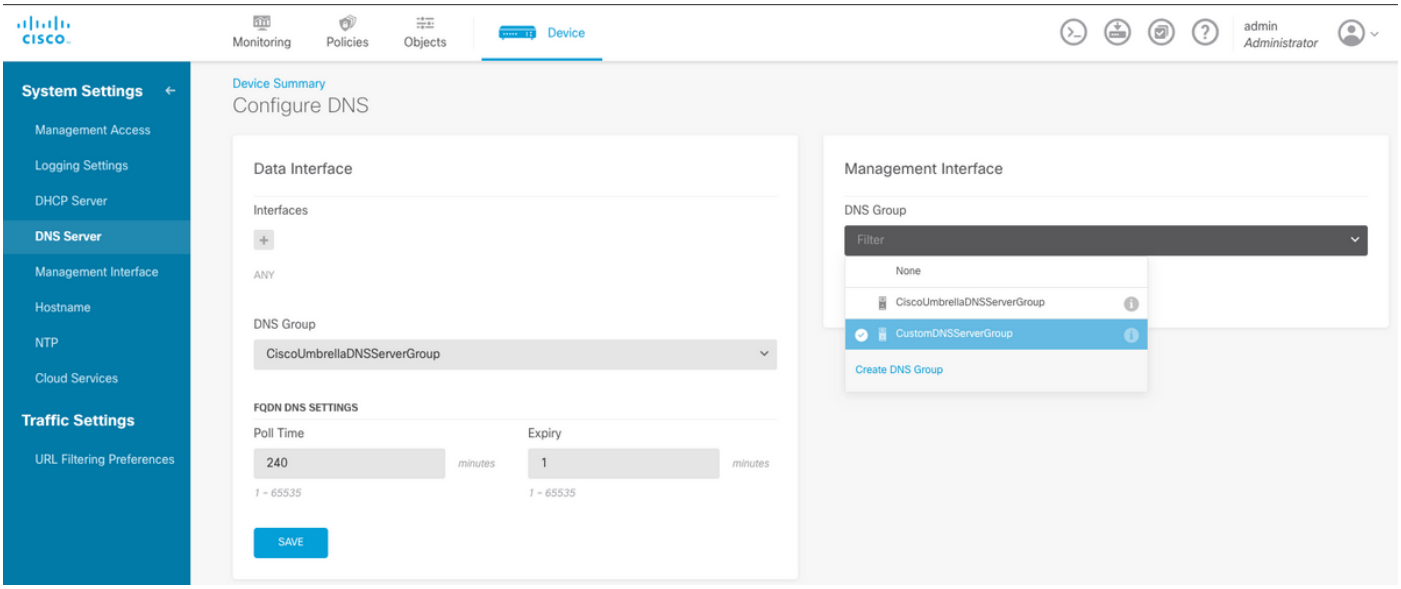
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

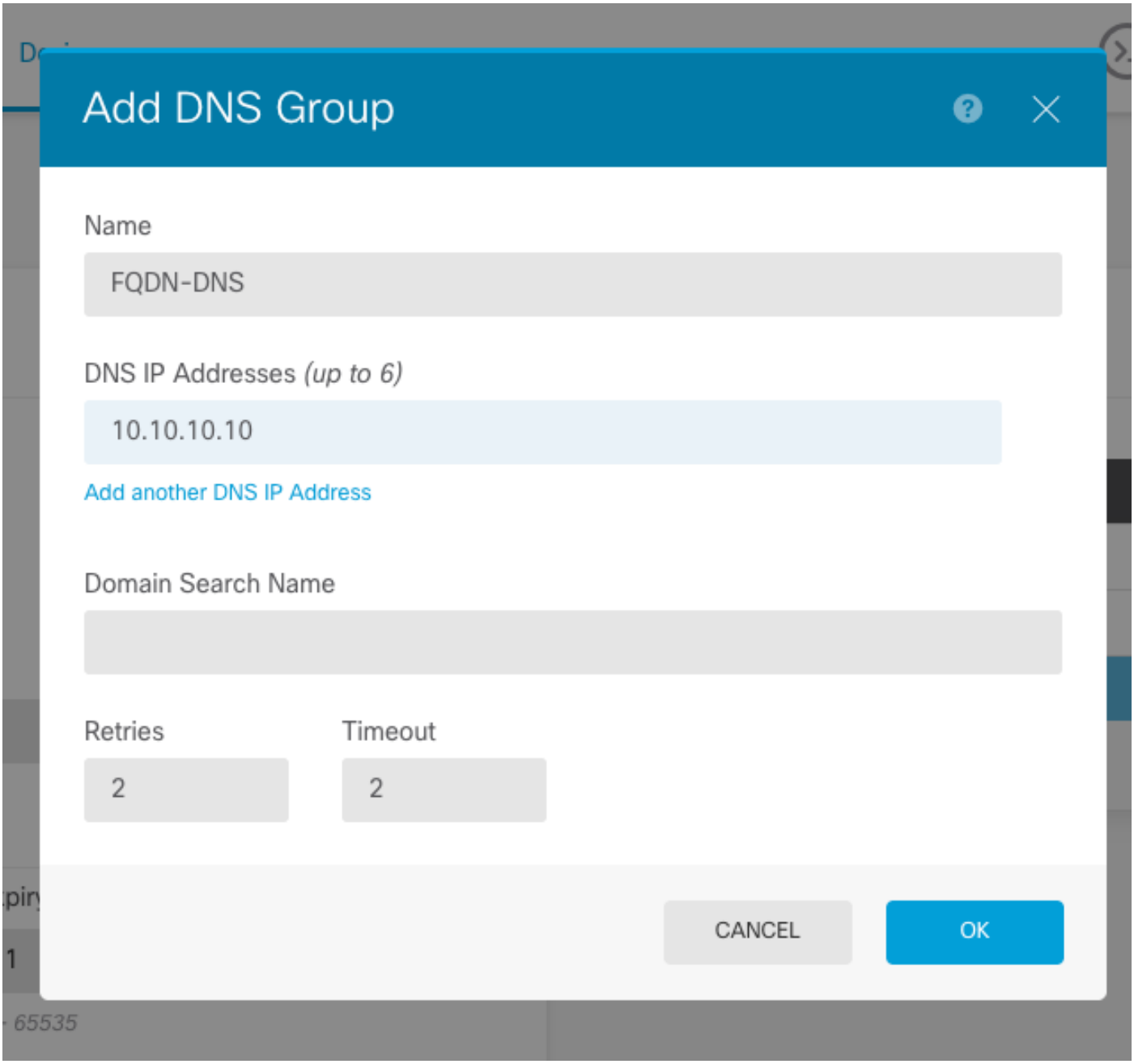
Configure

Step 1. In order to configure and use FQDN based object, first, configure DNS on the Firepower Threat Defense.

Login to the FMC and navigate to **Devices > Platform Settings > DNS**.

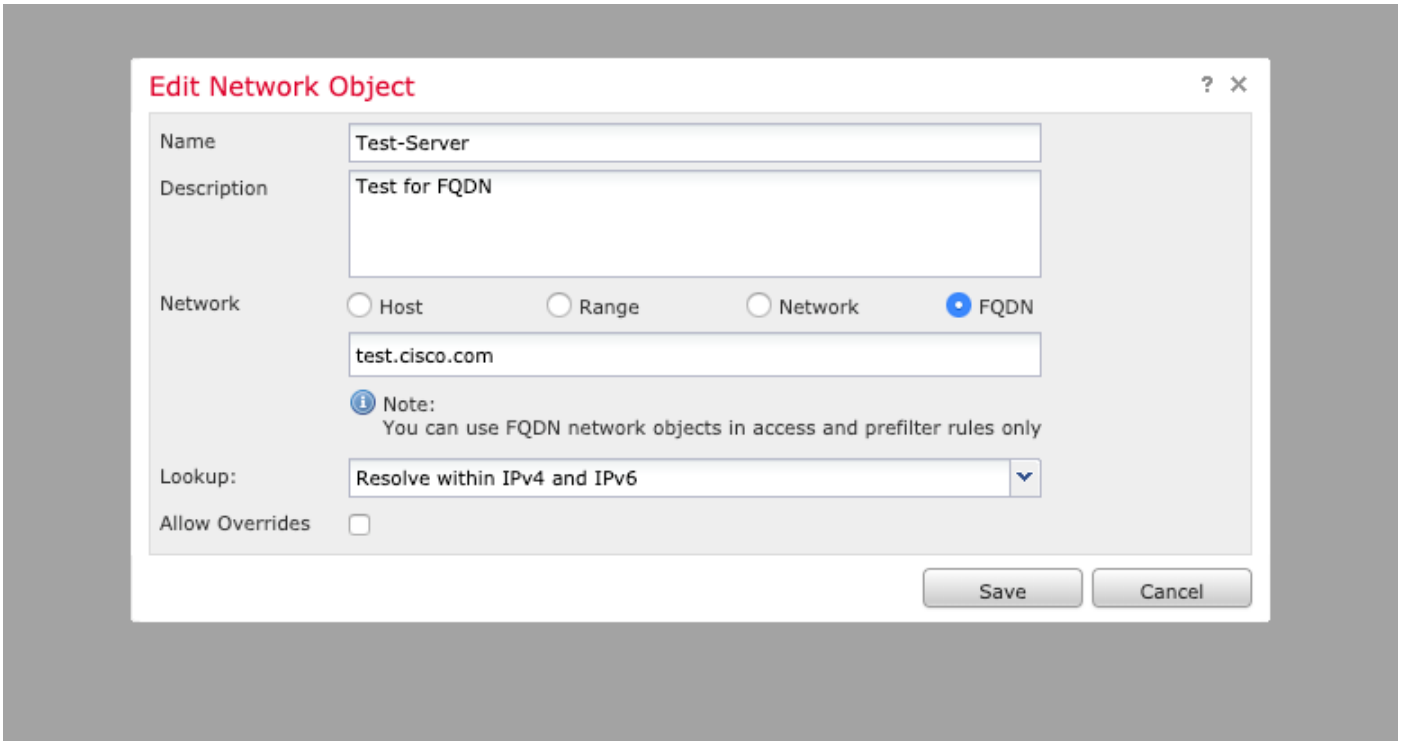

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP
ICMP
Secure Shell
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
UCAPL/CC Compliance
DNS Resolution Settings
Specify DNS servers group and device interfaces to reach them.
Enable DNS name resolution by device
DNS Server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

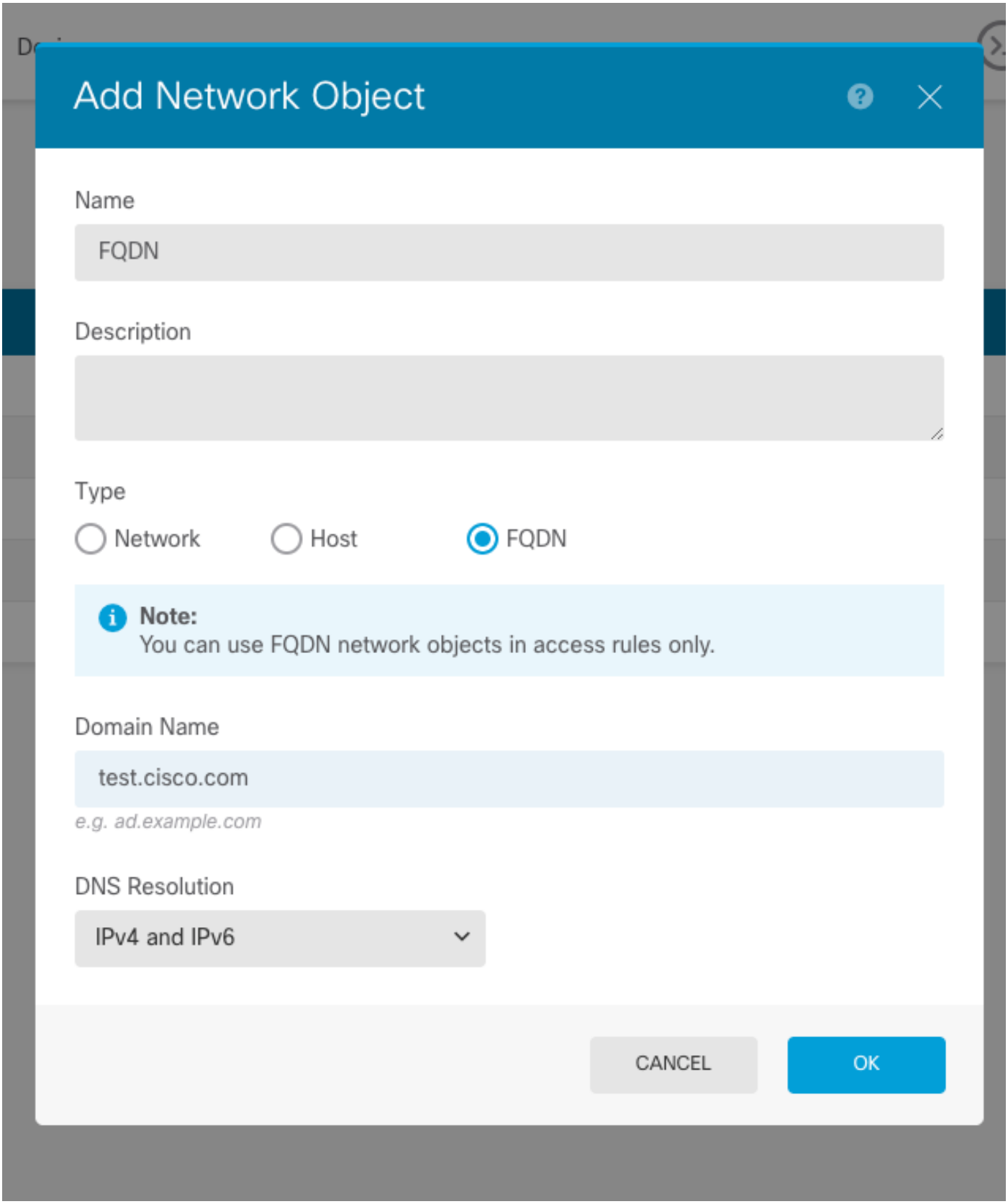

Monitoring
Policies
Objects
Device
admin
Administrator
System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
NTP
Cloud Services
Traffic Settings
URL Filtering Preferences
Device Summary
Configure DNS
Data Interface
Interfaces
ANY
DNS Group
CiscoUmbrellaDNSServerGroup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



Note: Ensure that the System Policy is applied to the FTD after configuring the DNS. (The DNS server configured should resolve the FQDN that will be used)

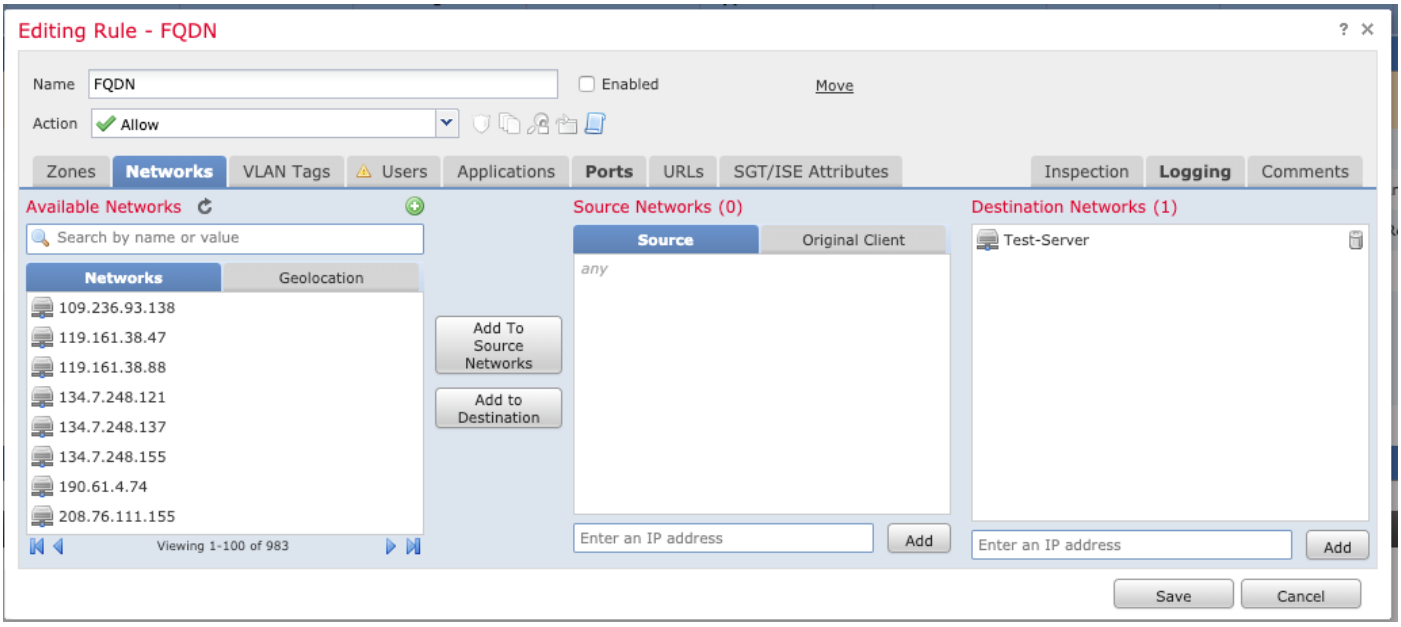
Step 2. Create the FQDN Object, in order to do that navigate to **Objects > Object Management > Add Network > Add Object.**

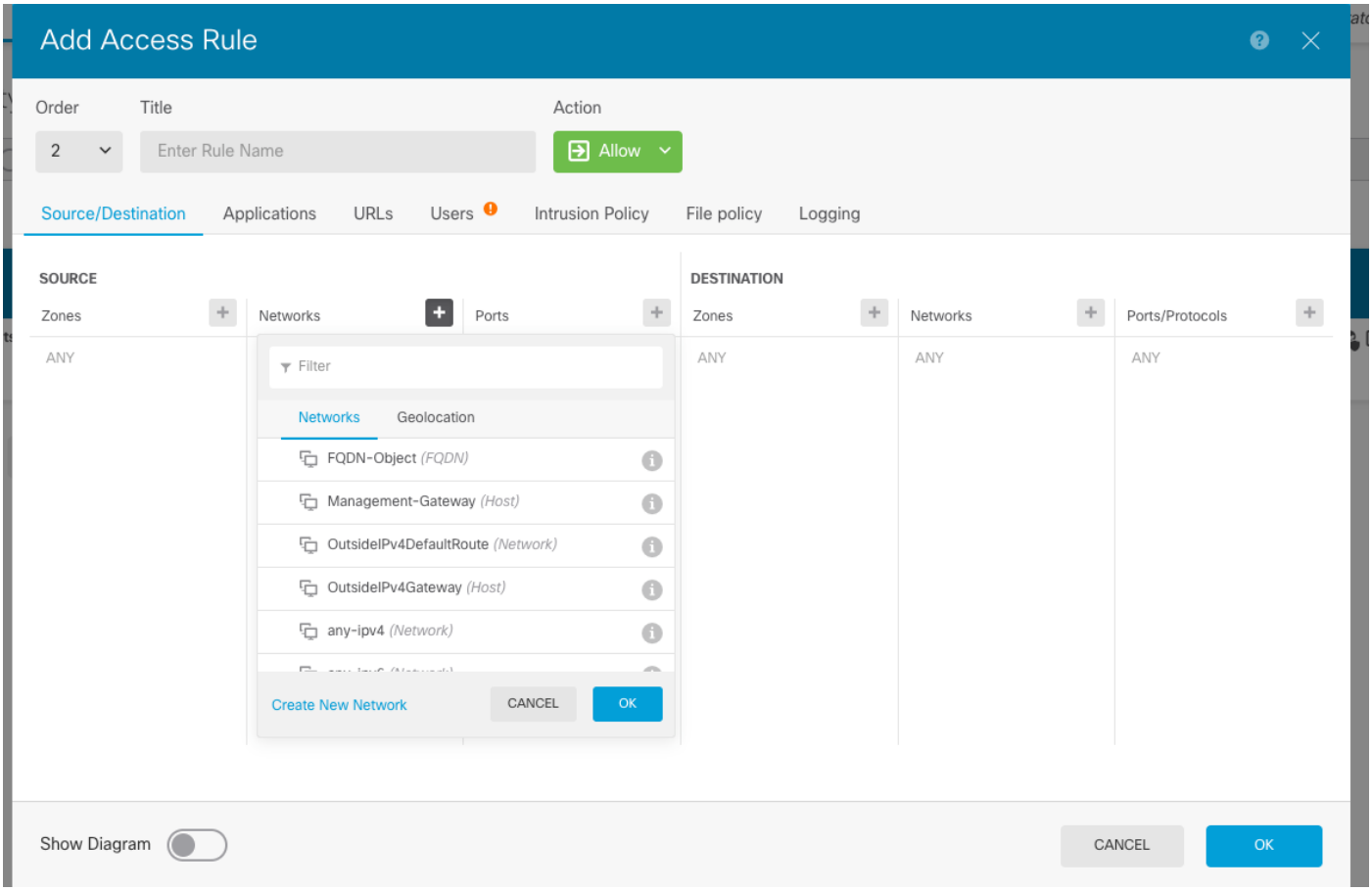

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



Step 3. Create an access control rule by navigating to **Policies > Access Control.**

Note: You can create a rule or modify the existing rule based on the requirement. The FQDN object can be either used in Source and/or Destination Networks.



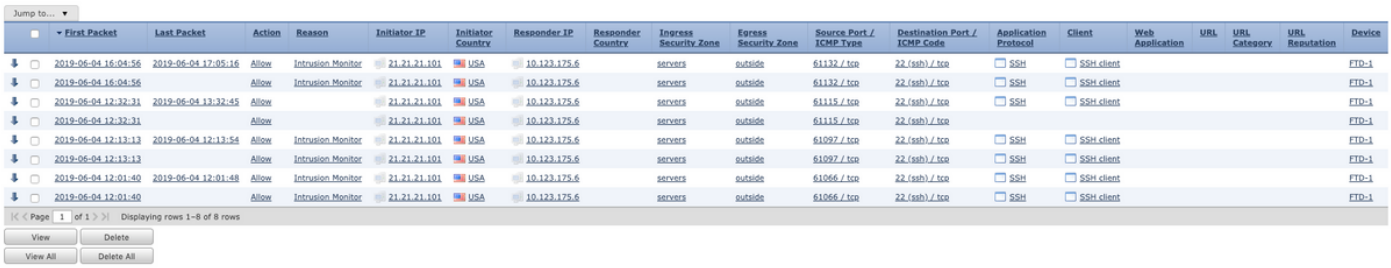


Ensure that the policy is applied after the configuration is completed.

Verify

Initiate traffic from the client machine which is expected to trigger the FQDN based rule created.

On the FMC, navigate to **Events > Connection Events, filter for the specific traffic.**



Troubleshoot

The DNS server should be able to resolve the FQDN object, this can be verified from the CLI runs these command:

- **system support diagnostic-cli**
- **show fqdn**

.