Configurar el objeto basado en FQDN para la regla de control de acceso

Contenido

Introducción

Este documento describe la configuración del objeto Full Qualified Domain Name (FQDN) a través de Firewall Management Center (FMC) y cómo utilizar el objeto FQDN en la creación de la regla de acceso.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower.
- Conocimiento de la configuración de la política de control de acceso en Firesight Management Center (FMC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

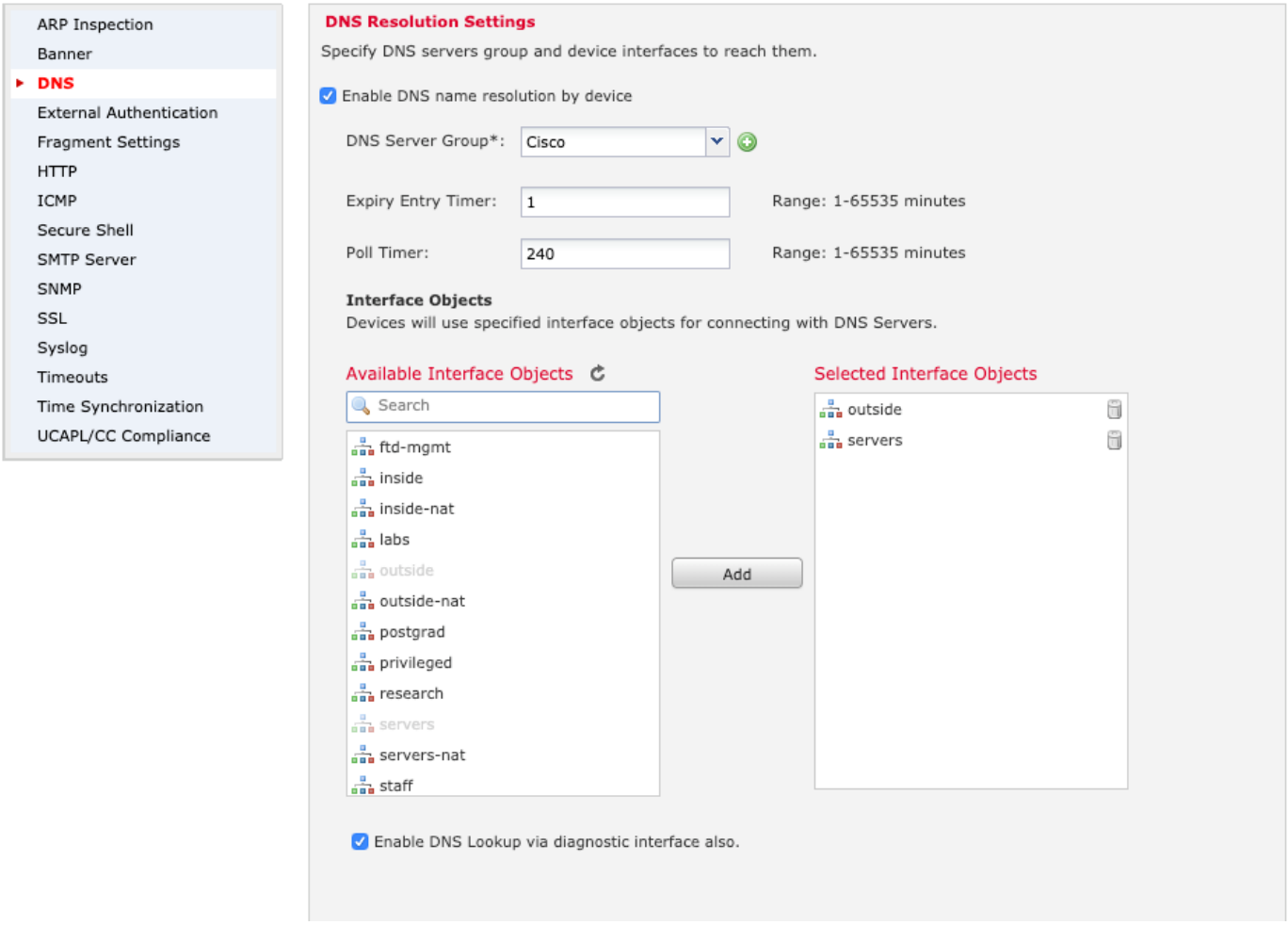
- Firepower Management Center que ejecuta la versión 6.3 y posteriores.
- Firepower Threat Defense que ejecuta la versión 6.3 y superiores.

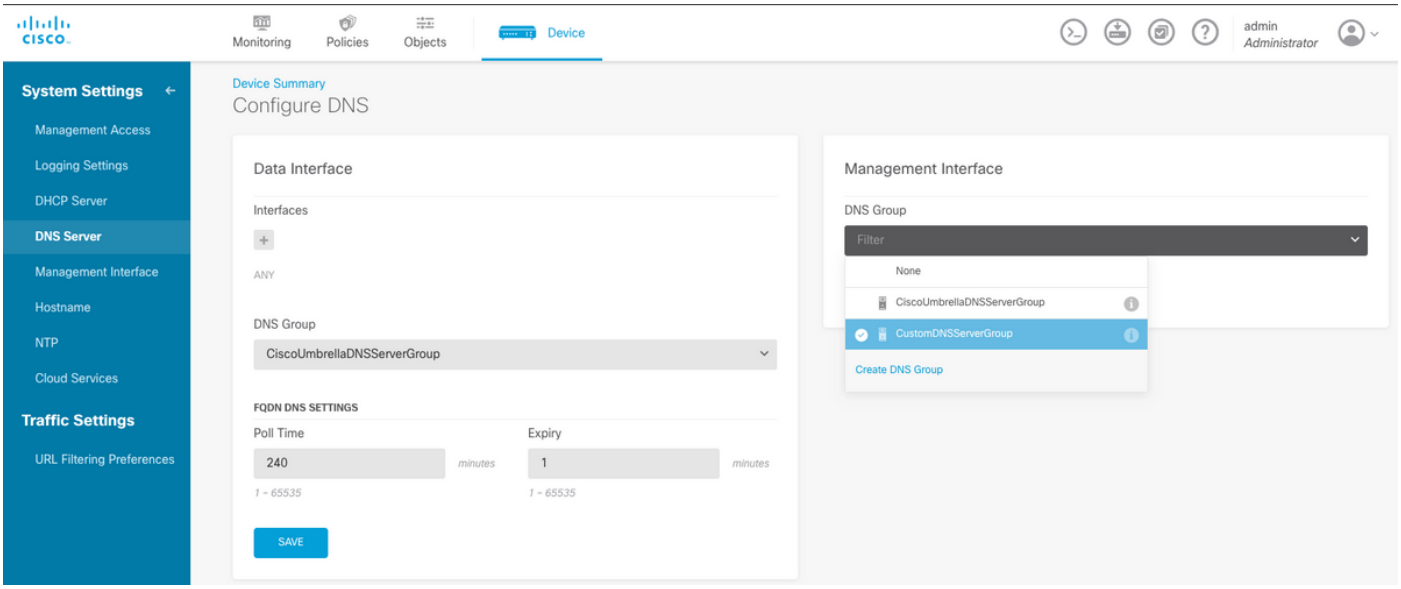
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

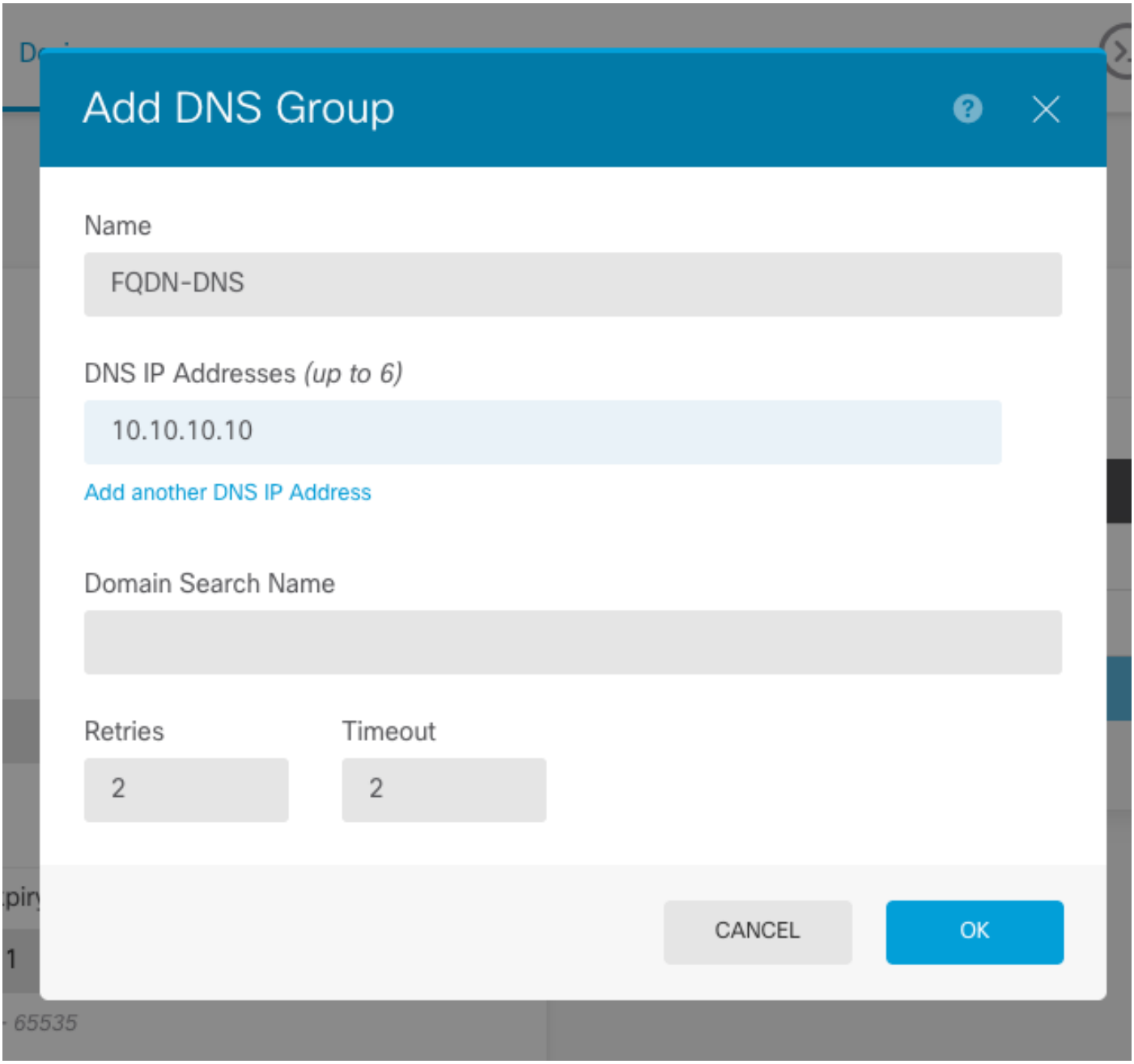
Configurar

Paso 1. Para configurar y utilizar el objeto basado en FQDN, primero, configure DNS en Firepower Threat Defense.

Inicie sesión en el FMC y navegue hasta **Dispositivos > Configuración de plataforma > DNS**.

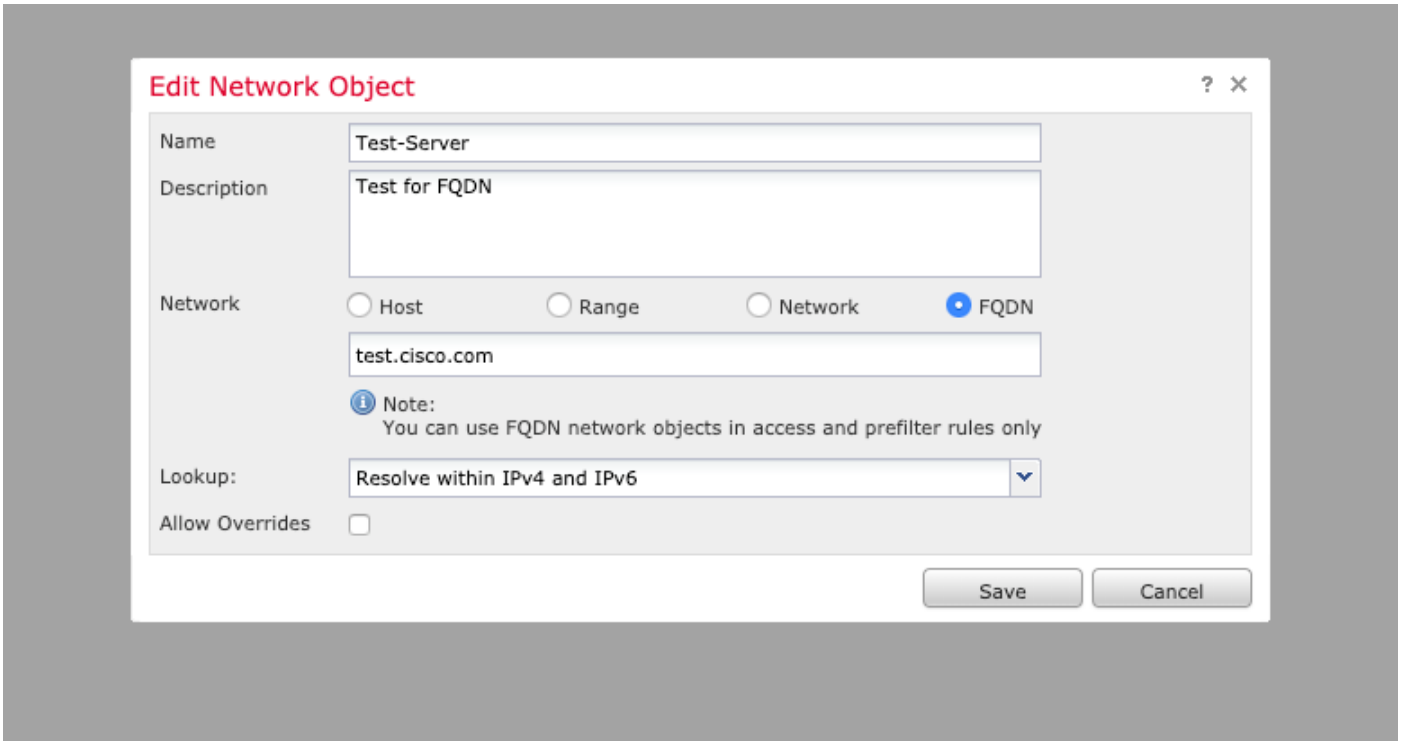


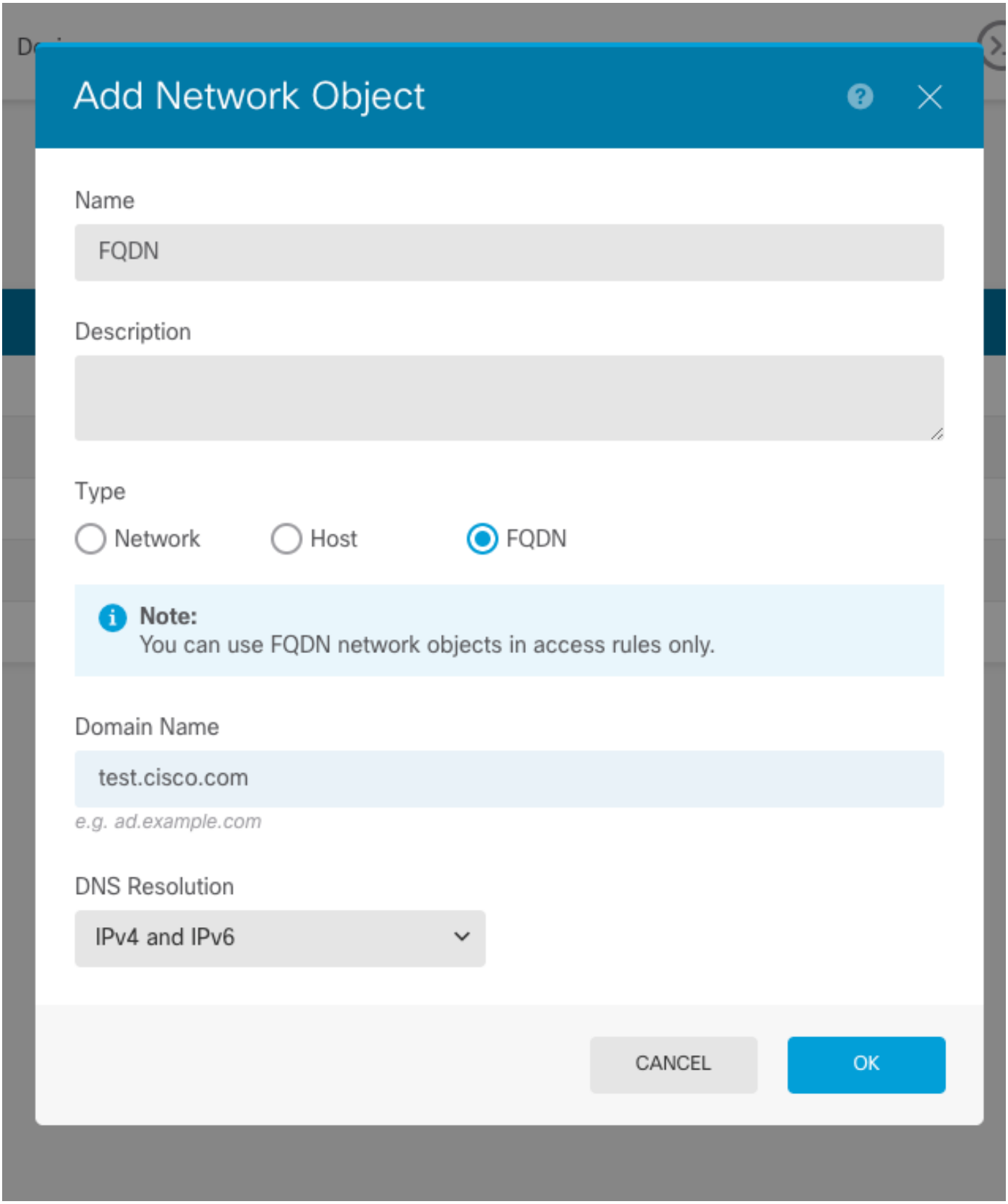




Nota: Asegúrese de que la política del sistema se aplique al FTD después de configurar el DNS. (El servidor DNS configurado debe resolver el FQDN que se utilizará)

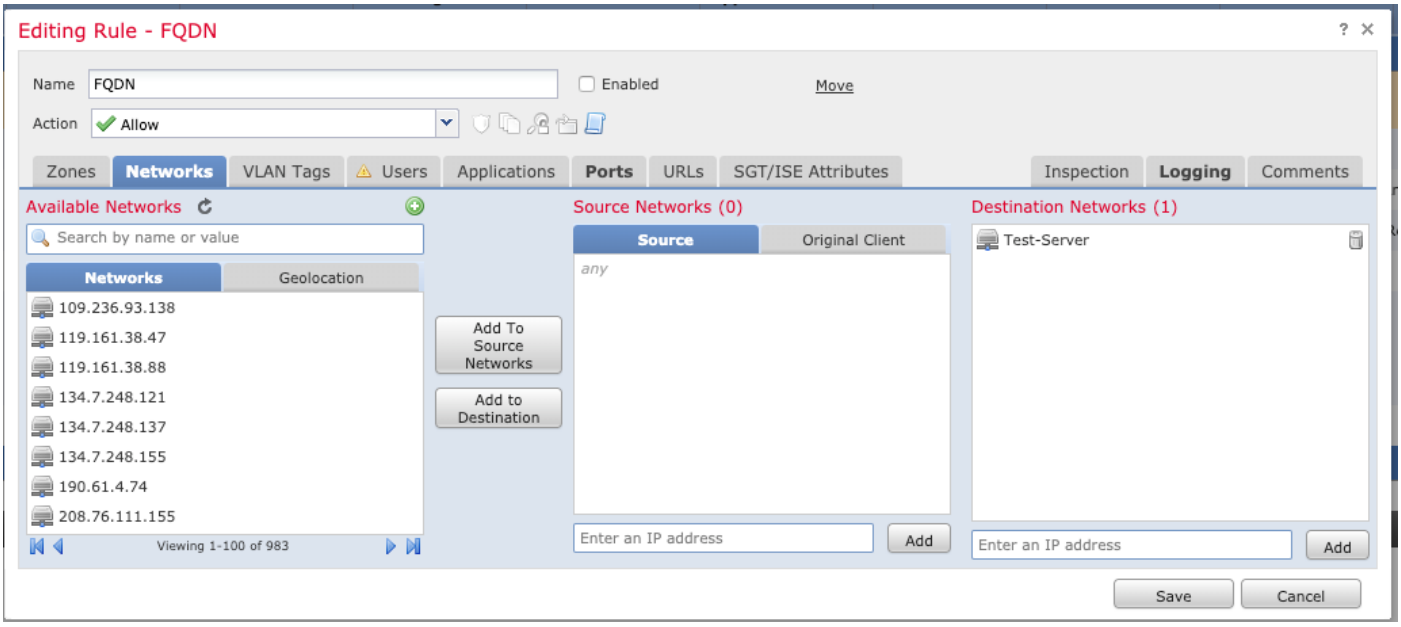
Paso 2. Cree el Objeto FQDN, para ello navegue hasta **Objetos > Administración de objetos > Agregar red > Agregar objeto.**

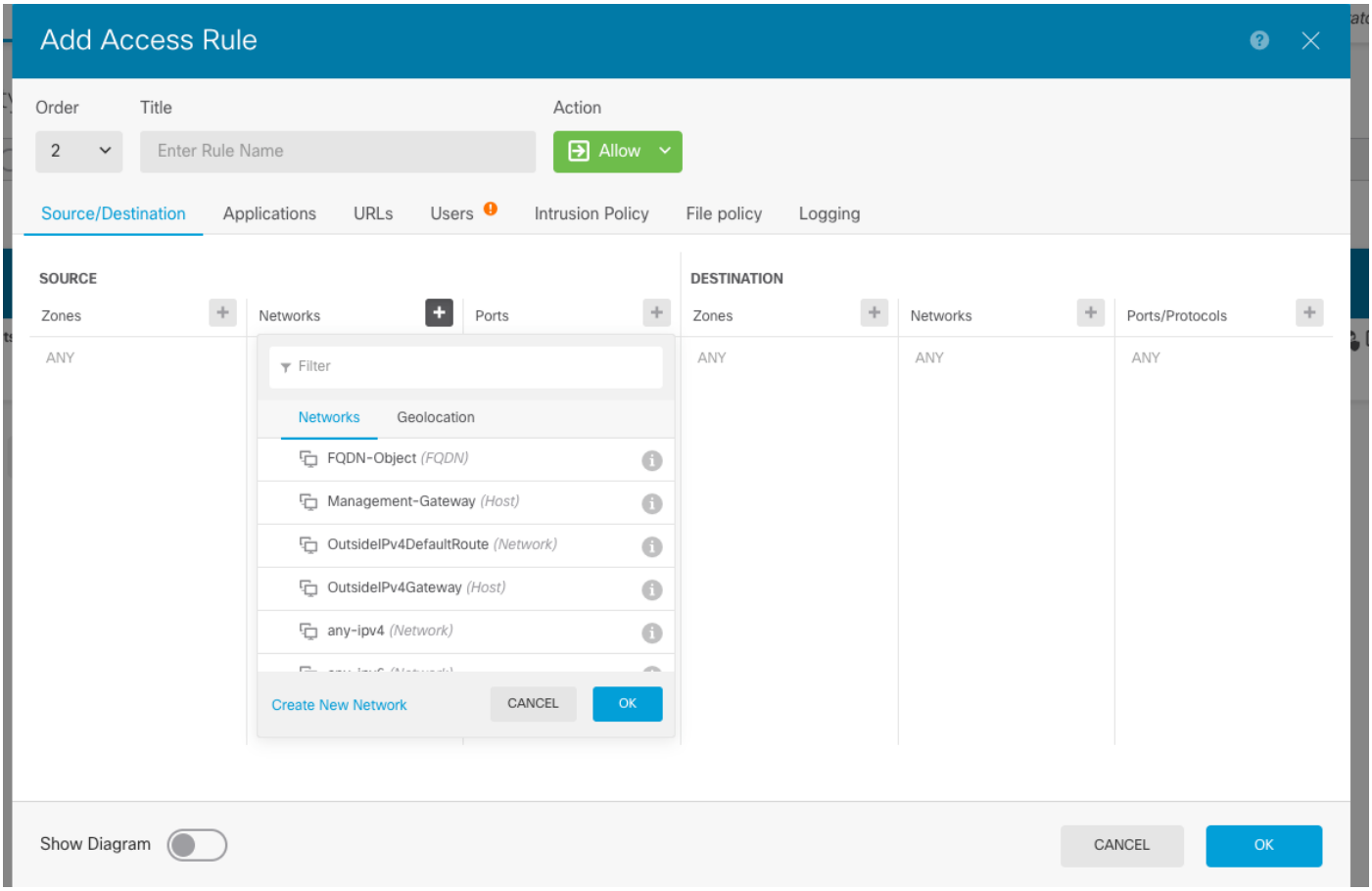

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



Paso 3. Cree una regla de control de acceso navegando hasta **Políticas > Control de acceso.**

Nota: Puede crear una regla o modificar la regla existente en función del requisito. El objeto FQDN se puede utilizar en redes de origen o de destino.



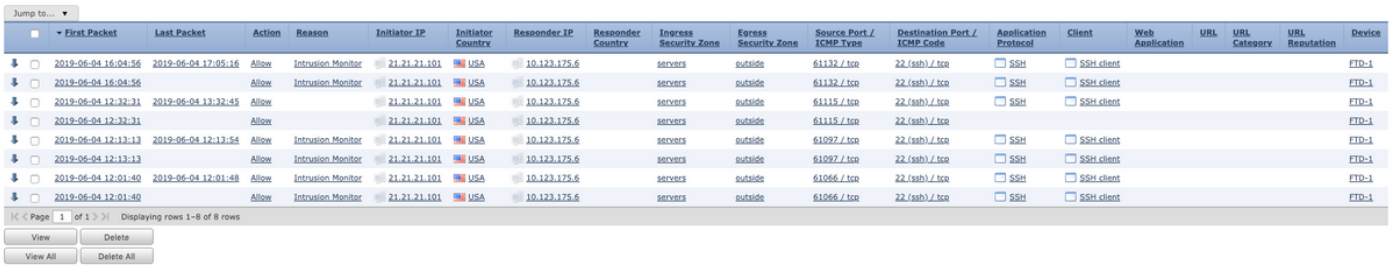


Asegúrese de que la política se aplique después de completar la configuración.

Verificación

Inicie el tráfico desde el equipo cliente que se espera active la regla basada en FQDN creada.

En el FMC, navegue hasta **Eventos > Eventos de conexión, filtre para el tráfico específico.**



Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
	2019-06-04 16:04:56	2019-06-04 17:05:16	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61132 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
	2019-06-04 16:04:56		Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61132 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
	2019-06-04 12:32:31	2019-06-04 13:32:45	Allow		21.21.21.101	USA	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
	2019-06-04 12:32:31		Allow		21.21.21.101	USA	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp							FTD-1
	2019-06-04 12:13:13	2019-06-04 12:13:54	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61097 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
	2019-06-04 12:13:13		Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61097 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
	2019-06-04 12:01:40	2019-06-04 12:01:48	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61066 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
	2019-06-04 12:01:40		Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61066 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1

Page 1 of 1 Displaying rows 1–8 of 8 rows

View Delete

View All Delete All

Troubleshoot

El servidor DNS debe ser capaz de resolver el objeto FQDN; esto se puede verificar desde la CLI ejecuta este comando:

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

.