

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

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

## 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.

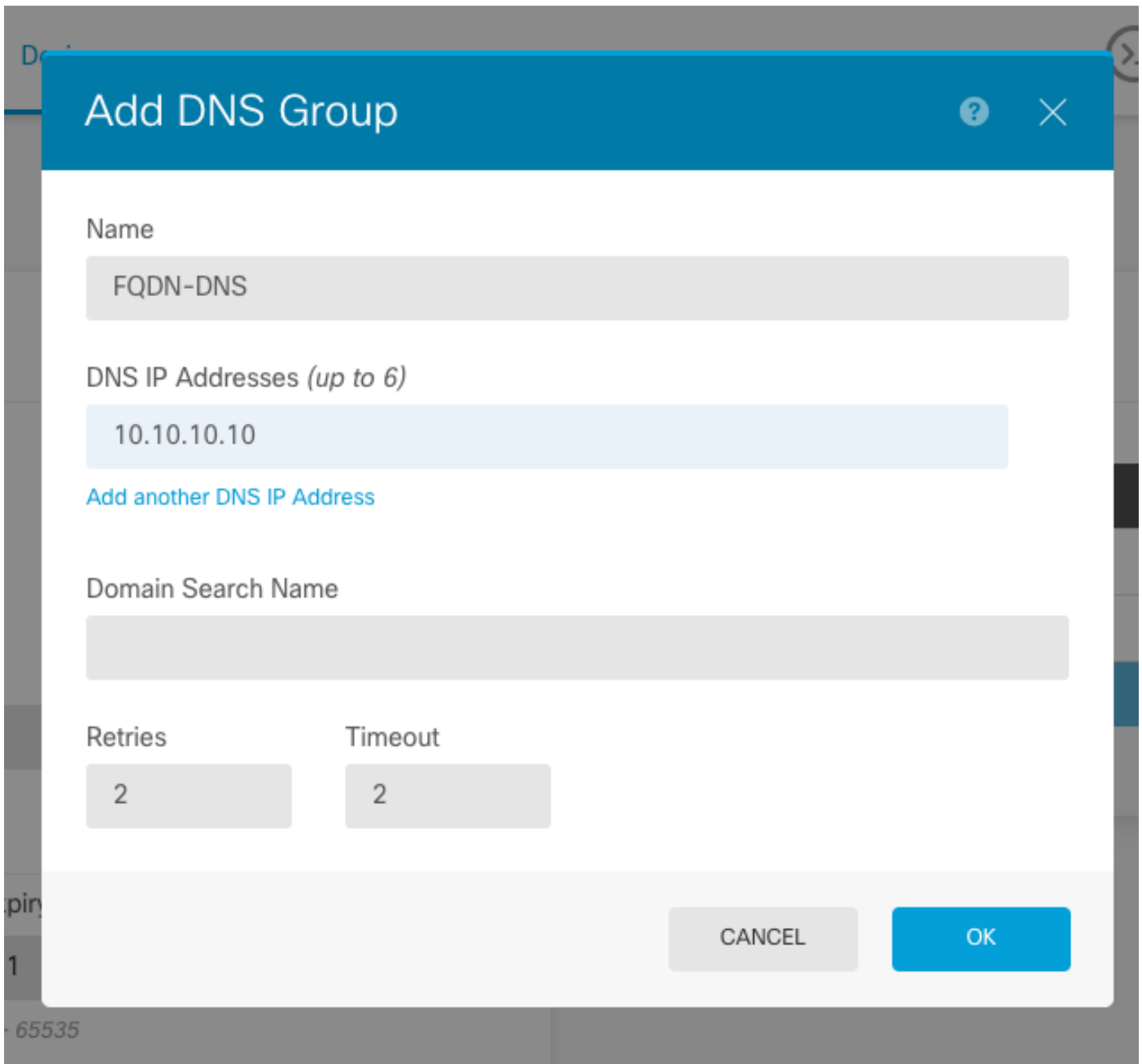
## Configurar

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**.

The screenshot shows the 'DNS Resolution Settings' configuration page. On the left is a navigation menu with 'DNS' selected. The main content area includes a title 'DNS Resolution Settings', a description 'Specify DNS servers group and device interfaces to reach them.', and a checked checkbox 'Enable DNS name resolution by device'. Below this are two input fields: 'DNS Server Group\*' set to 'Cisco' and 'Expiry Entry Timer' set to '1' (with a range of 1-65535 minutes). Another input field shows 'Poll Timer' set to '240' (with a range of 1-65535 minutes). The 'Interface Objects' section states 'Devices will use specified interface objects for connecting with DNS Servers.' It features two panels: 'Available Interface Objects' with a search bar and a list of objects (ftd-mgmt, inside, inside-nat, labs, outside, outside-nat, postgrad, privileged, research, servers, servers-nat, staff), and 'Selected Interface Objects' which currently contains 'outside' and 'servers'. An 'Add' button is positioned between these panels. At the bottom, there is a checked checkbox 'Enable DNS Lookup via diagnostic interface also.'

The screenshot shows the 'Configure DNS' configuration page. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device'. The left sidebar shows 'System Settings' with 'DNS Server' selected. The main content area is titled 'Device Summary Configure DNS' and is split into two panels. The 'Data Interface' panel has an 'Interfaces' section with a plus sign and 'ANY' listed. Below is a 'DNS Group' dropdown menu set to 'CiscoUmbrellaDNSServerGroup'. The 'FQDN DNS SETTINGS' section has 'Poll Time' set to '240' minutes and 'Expiry' set to '1' minutes, both with a range of 1-65535. A 'SAVE' button is at the bottom. The 'Management Interface' panel has a 'DNS Group' dropdown menu with a filter set to 'None'. The dropdown list shows 'CiscoUmbrellaDNSServerGroup' and 'CustomDNSServerGroup' (which is selected). A 'Create DNS Group' link is at the bottom of the dropdown.



**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

? X

Name	<input type="text" value="Test-Server"/>
Description	<input type="text" value="Test for FQDN"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input type="radio"/> Network <input checked="" type="radio"/> FQDN
	<input type="text" value="test.cisco.com"/>
	<b>Note:</b> You can use FQDN network objects in access and prefilter rules only
Lookup:	<input type="text" value="Resolve within IPv4 and IPv6"/> ▼
Allow Overrides	<input type="checkbox"/>

Save

Cancel

**Add Network Object** ? X

Name  
FQDN

Description

Type  
 Network  Host  FQDN

**Note:**  
You can use FQDN network objects in access rules only.

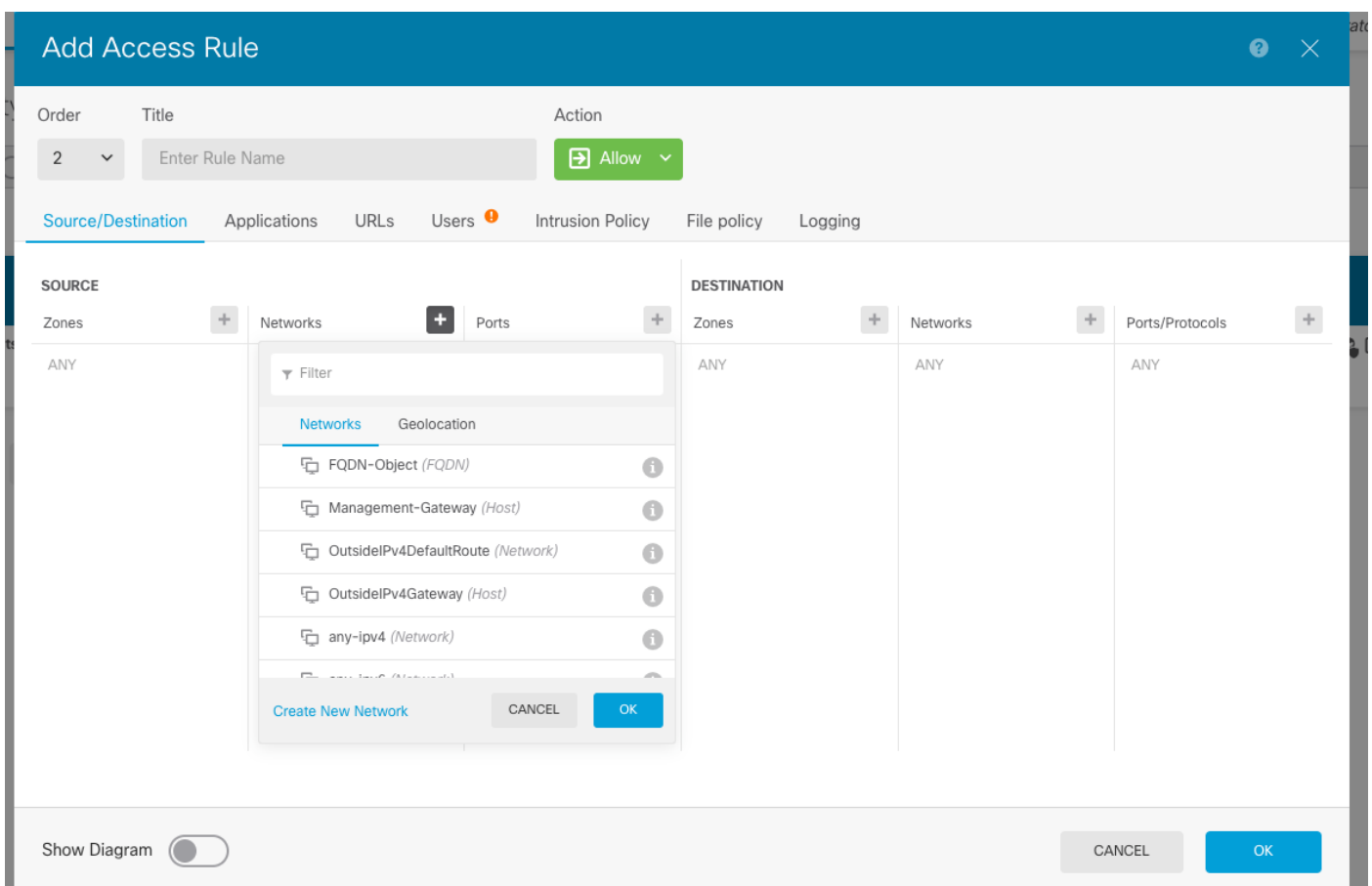
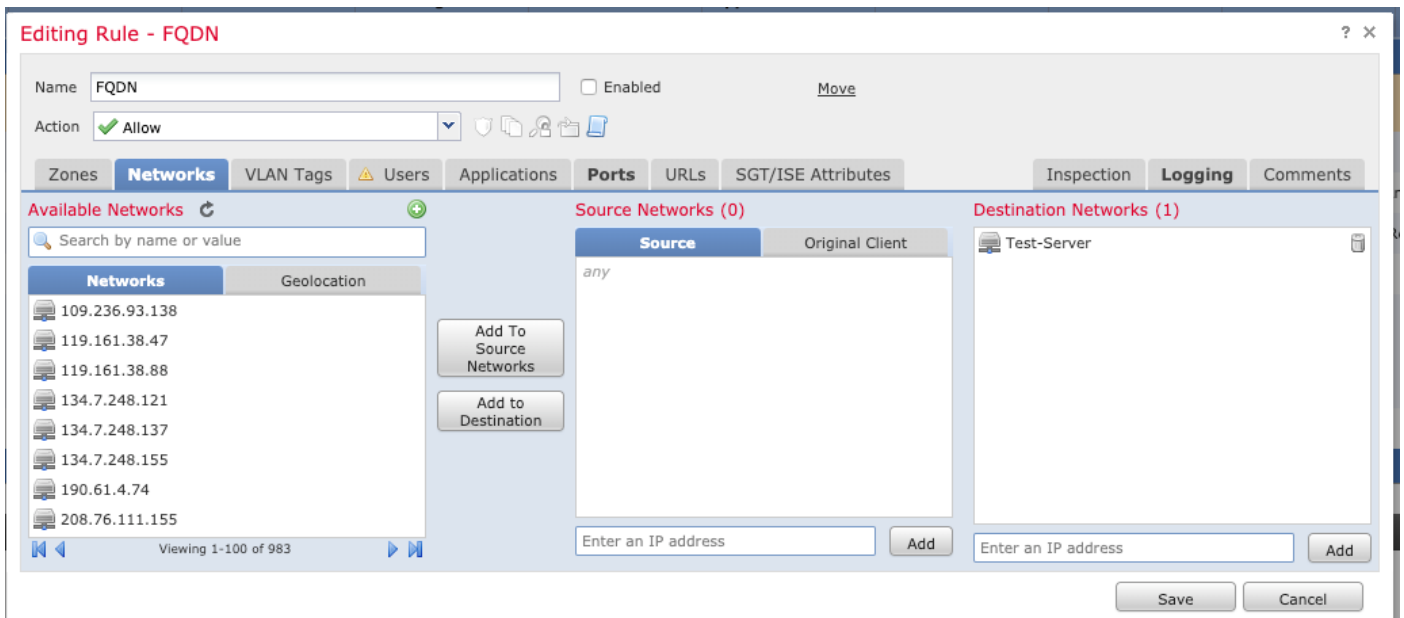
Domain Name  
test.cisco.com  
*e.g. ad.example.com*

DNS Resolution  
IPv4 and IPv6

CANCEL OK

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.

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	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	Intrusion Monitor	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	2019-06-04 12:32:31	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61115 / tcp	22 / ssh / tcp	SSH	SSH client					FTD-1
2019-06-04 12:13:13	2019-06-04 12:13:58	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	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	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`