

# 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**.

**DNS Resolution Settings**  
Specify DNS servers group and device interfaces to reach them.

Enable DNS name resolution by device

DNS Server Group\*:

Expiry Entry Timer:  Range: 1-65535 minutes

Poll Timer:  Range: 1-65535 minutes

**Interface Objects**  
Devices will use specified interface objects for connecting with DNS Servers.

**Available Interface Objects**

- ftd-mgmt
- inside
- inside-nat
- labs
- outside
- outside-nat
- postgrad
- privileged
- research
- servers
- servers-nat
- staff

**Selected Interface Objects**

- outside
- servers

Enable DNS Lookup via diagnostic interface also.

**System Settings** ←

- Management Access
- Logging Settings
- DHCP Server
- DNS Server**
- Management Interface
- Hostname
- NTP
- Cloud Services

**Traffic Settings**

- URL Filtering Preferences

Monitoring Policies Objects **Device** admin Administrator

Device Summary  
Configure DNS

**Data Interface**

Interfaces

ANY

DNS Group

**FQDN DNS SETTINGS**

Poll Time:  minutes (Range: 1 - 65535)

Expiry:  minutes (Range: 1 - 65535)

**Management Interface**

DNS Group

Filter

- None
- CiscoUmbrellaDNSServerGroup
- CustomDNSServerGroup**

**Add DNS Group**

Name  
FQDN-DNS

DNS IP Addresses (up to 6)  
10.10.10.10  
[Add another DNS IP Address](#)

Domain Search Name

Retries: 2      Timeout: 2

CANCEL      OK

**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**

Name  
FQDN

Description

Type  
 Network  Host  FQDN

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

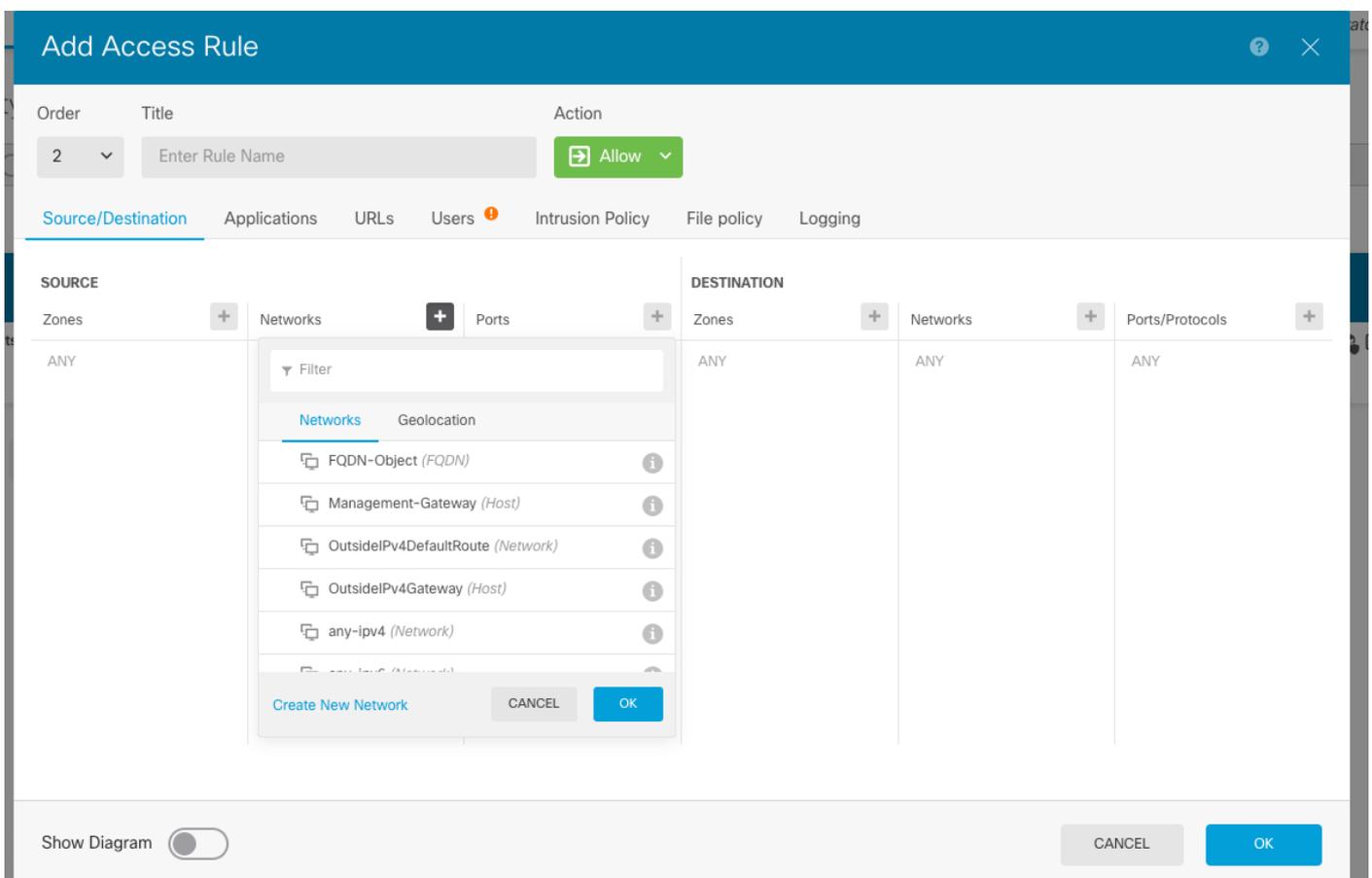
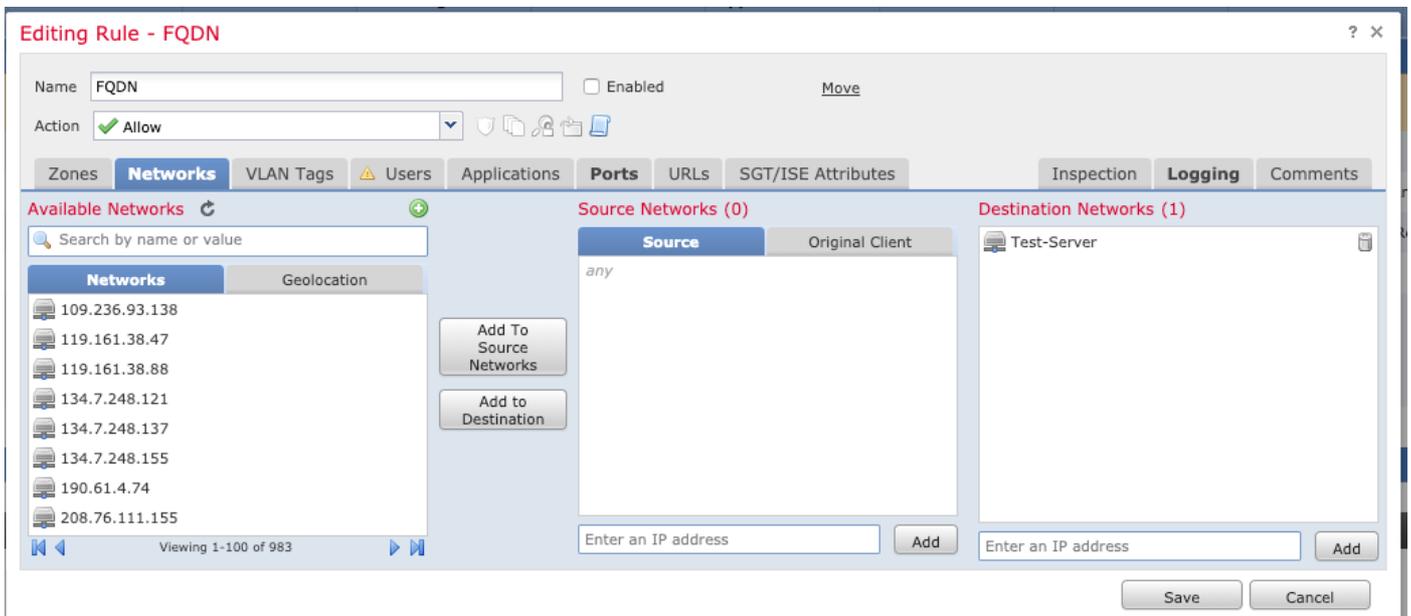
Domain Name  
test.cisco.com  
*e.g. ad.example.com*

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.

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	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`