Configurar objeto baseado em FQDN para regra de controle de acesso

Contents

Introduction

Este documento descreve a configuração do objeto Nome de domínio totalmente qualificado (FQDN) através do Centro de gerenciamento de firewall (FMC) e como usar o objeto FQDN na criação da regra de acesso.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower.
- Conhecimento da configuração da política de controle de acesso no Firesight Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

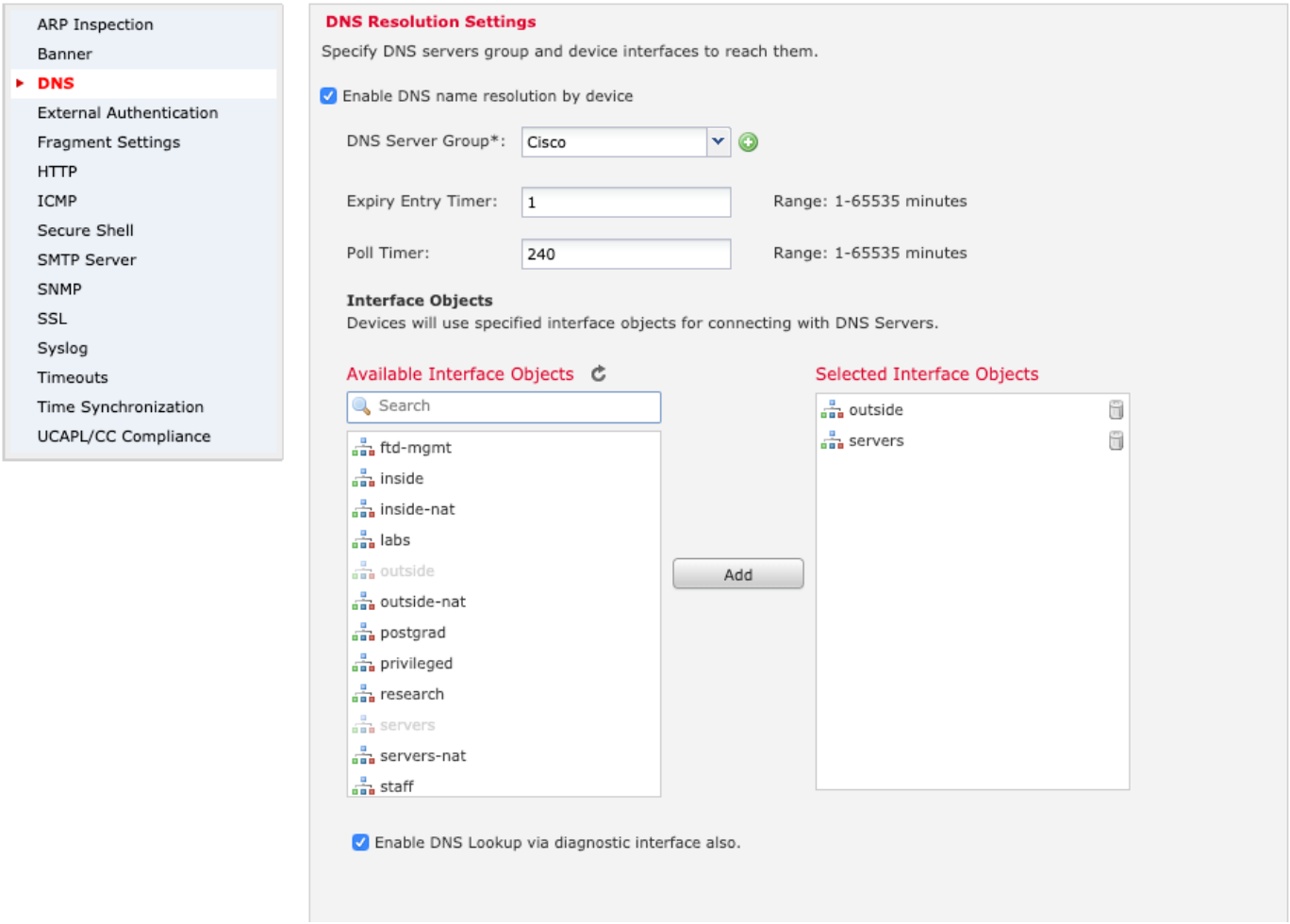
- Firepower Management Center executando a versão 6.3 e superior.
- Firepower Threat Defense executando a versão 6.3 e superior.

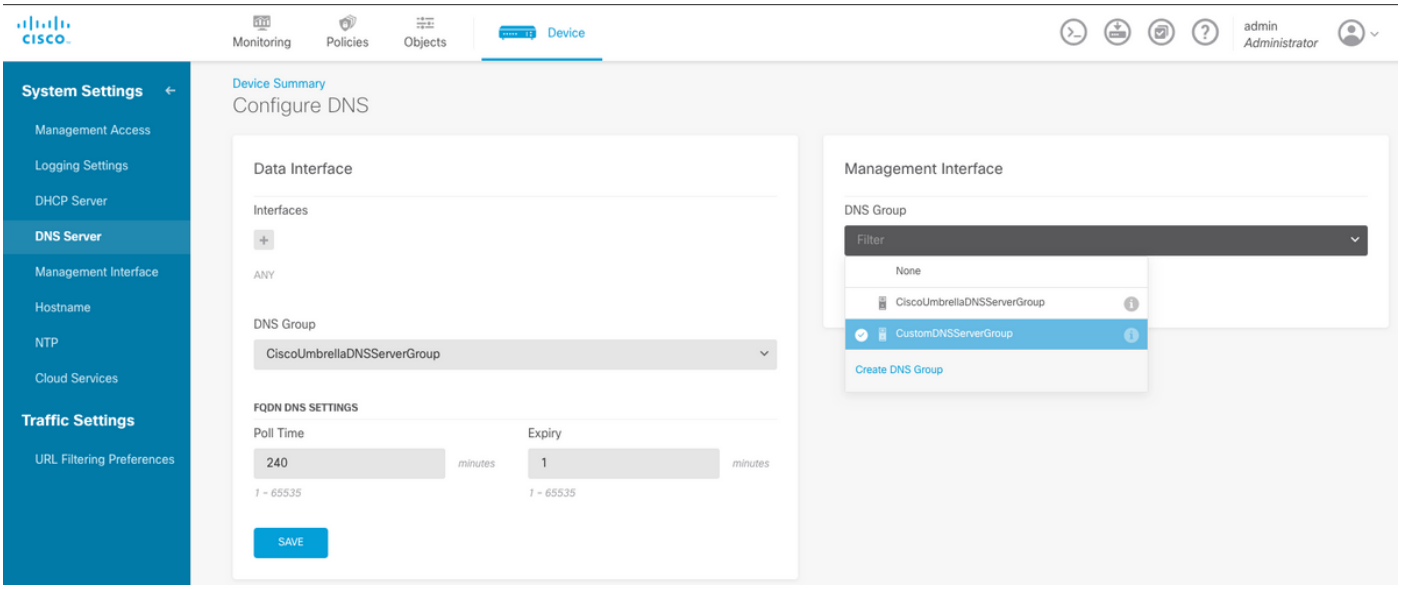
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

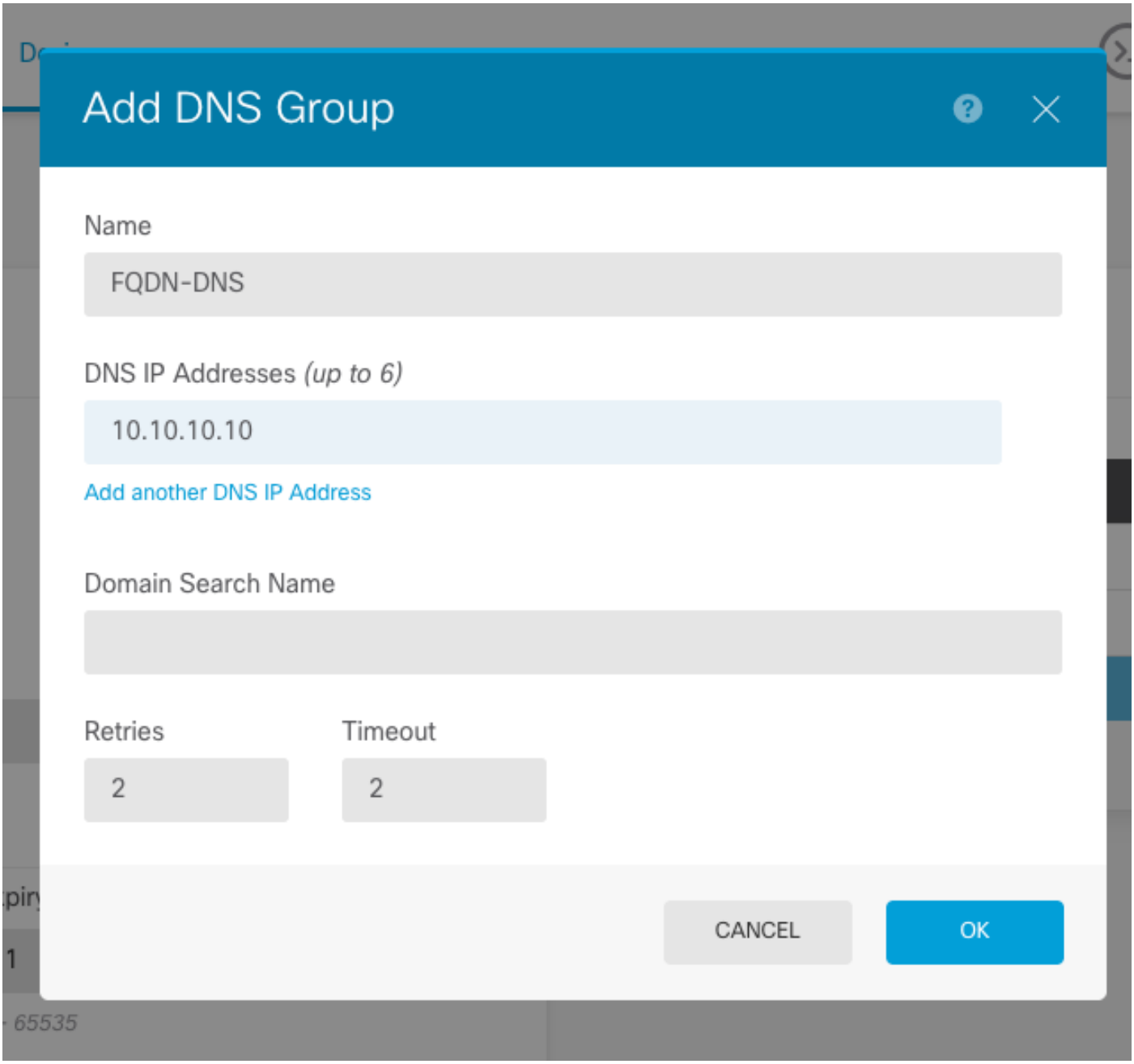
Configurar

Etapa 1. Para configurar e usar um objeto baseado em FQDN, primeiro configure o DNS no Firepower Threat Defense.

Faça login no FMC e navegue até **Devices > Platform Settings > DNS**.

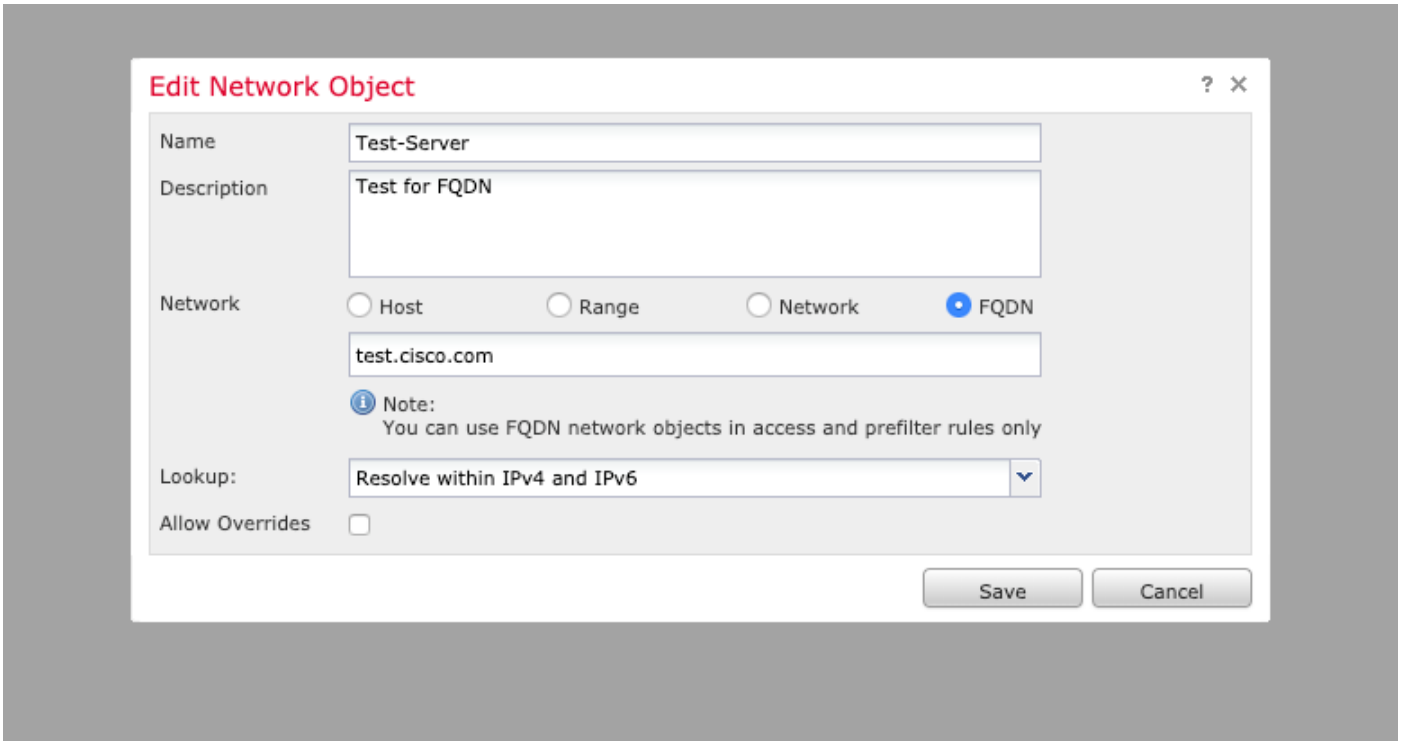


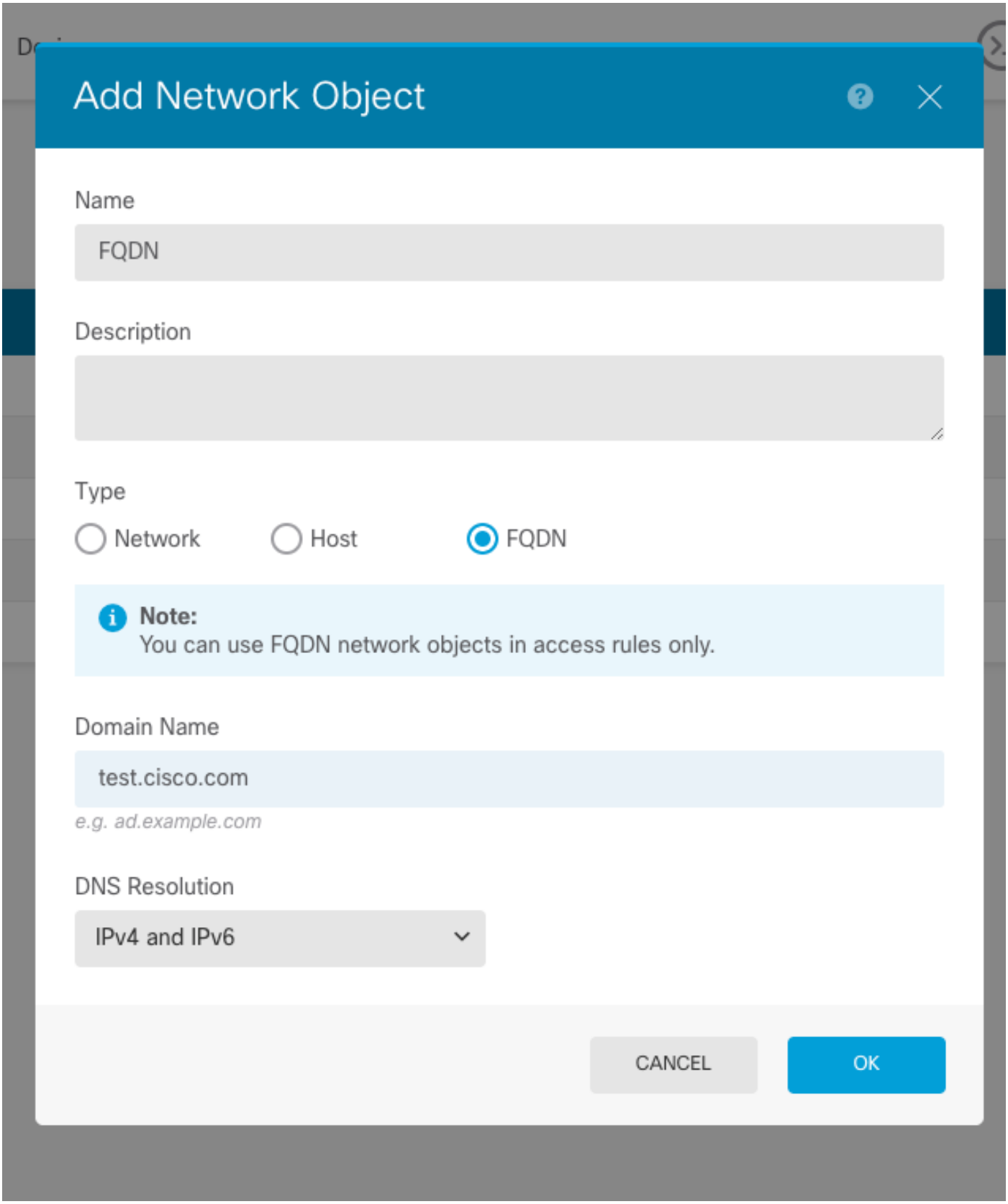




Note: Certifique-se de que a Diretiva do Sistema seja aplicada ao FTD após a configuração do DNS. (O servidor DNS configurado deve resolver o FQDN que será usado)

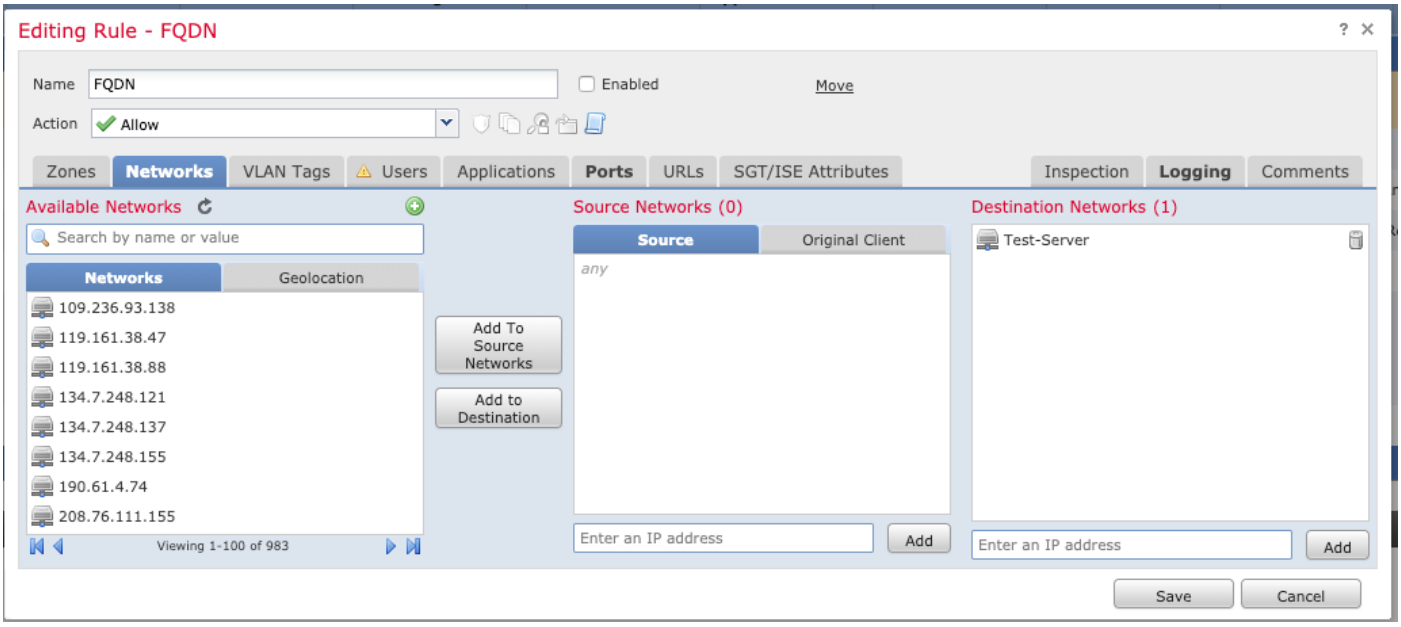
Etapa 2. Crie o objeto FQDN, para fazer isso, navegue até **Objects > Object Management > Add Network > Add Object.**

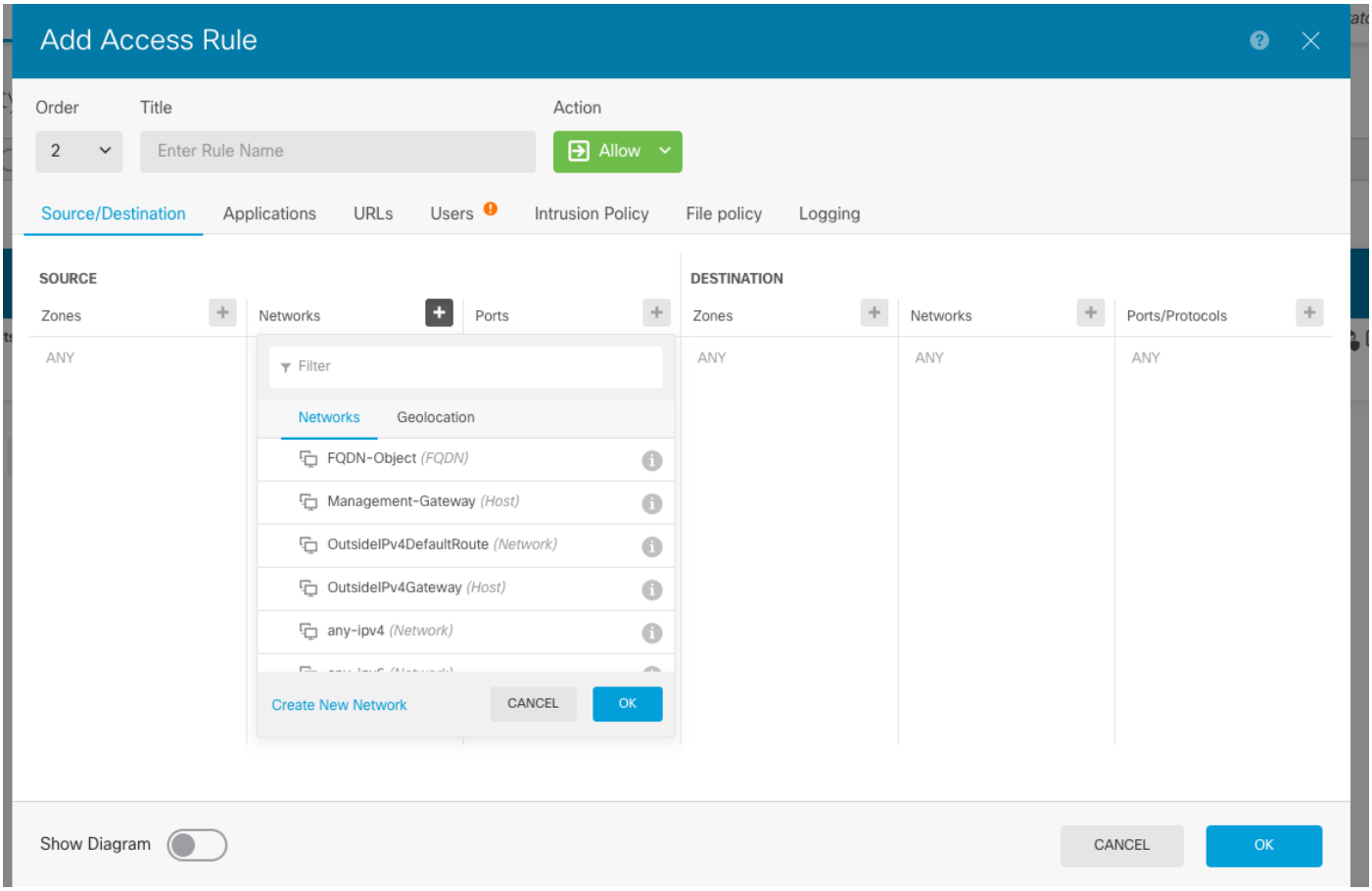

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



Etapa 3. Crie uma regra de controle de acesso navegando para **Políticas > Controle de acesso.**

Note: Você pode criar uma regra ou modificar a regra existente com base no requisito. O objeto FQDN pode ser usado em redes de origem e/ou destino.



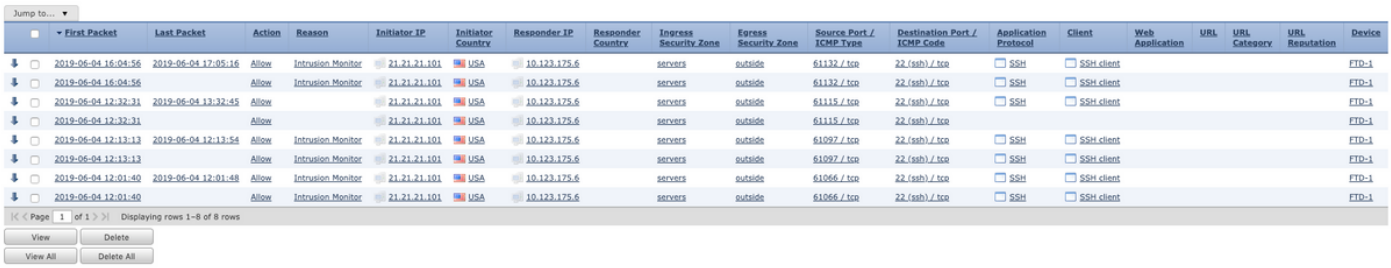


Certifique-se de que a diretiva seja aplicada depois que a configuração for concluída.

Verificar

Inicie o tráfego da máquina cliente que deve disparar a regra baseada em FQDN criada.

No FMC, navegue até **Eventos > Eventos de Conexão, filtre o tráfego 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

O servidor DNS deve ser capaz de resolver o objeto FQDN, isso pode ser verificado a partir da CLI que executa estes comandos:

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

.