為訪問控制規則配置基於FQDN的對象

目錄

簡介

本文檔介紹通過防火牆管理中心(FMC)配置完全限定域名(FQDN)對象以及在訪問規則建立中使用FQDN對象的方式。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower技術知識。
- 在Firesight管理中心(FMC)上配置訪問控制策略的知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

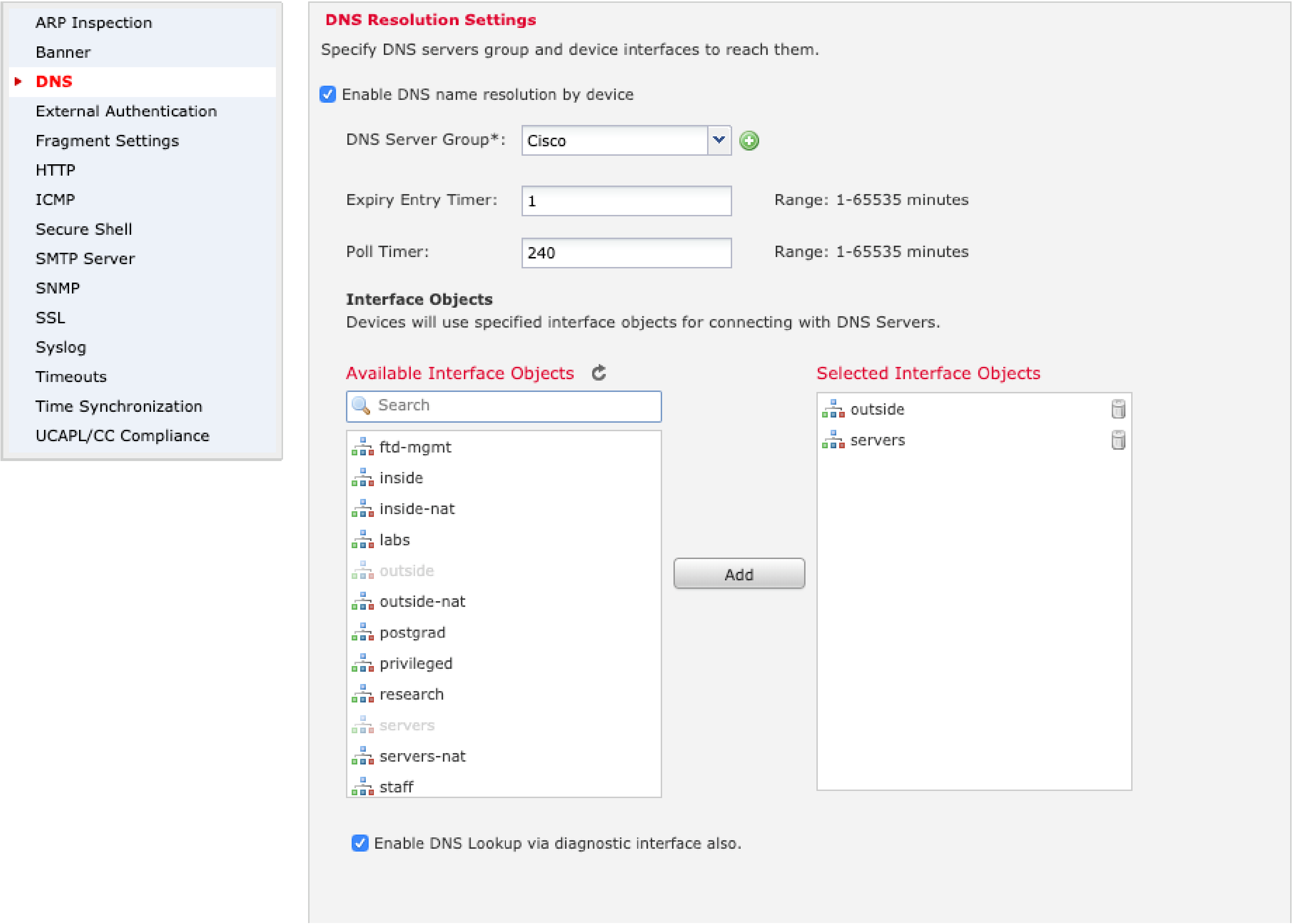
- 運行6.3及更高版本的Firepower管理中心。
- 運行6.3及更高版本的Firepower威脅防禦。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟1。若要配置和使用基於FQDN的對象，請先在Firepower威脅防禦上配置DNS。

登入FMC並導覽至**Devices > Platform Settings > DNS**。



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.

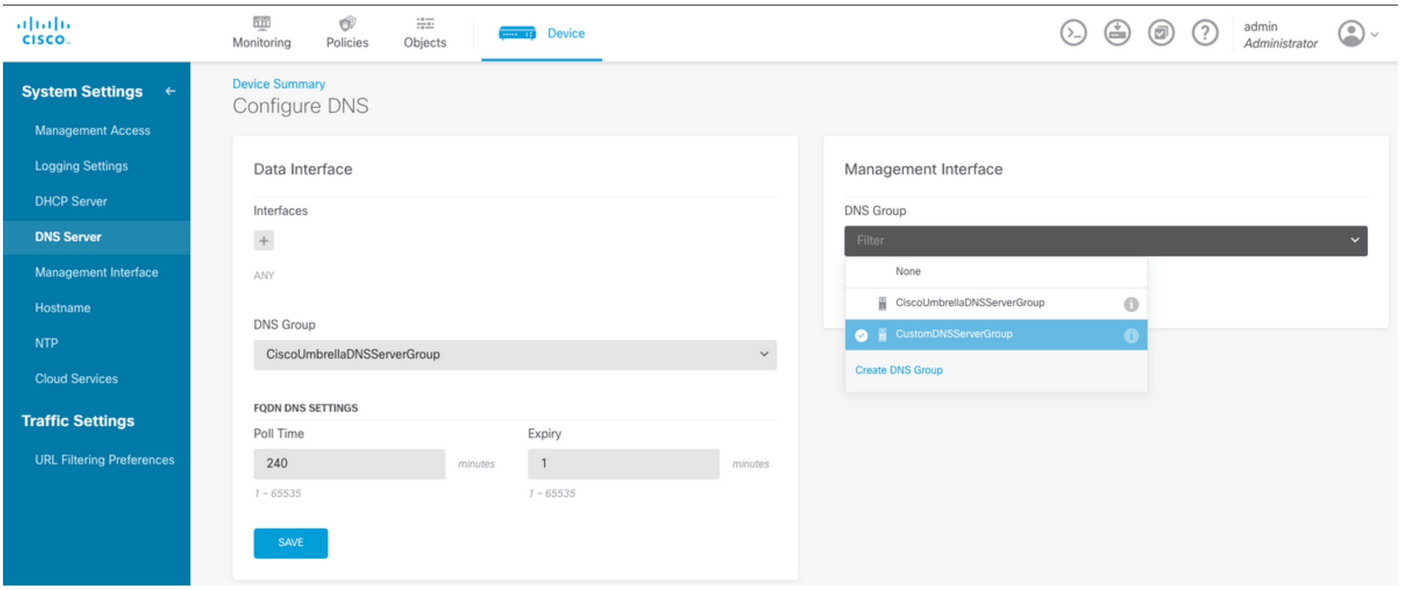
Available Interface Objects

- 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.



Configure DNS

Data Interface

Interfaces: ANY

DNS Group: CiscoUmbrellaDNSServerGroup

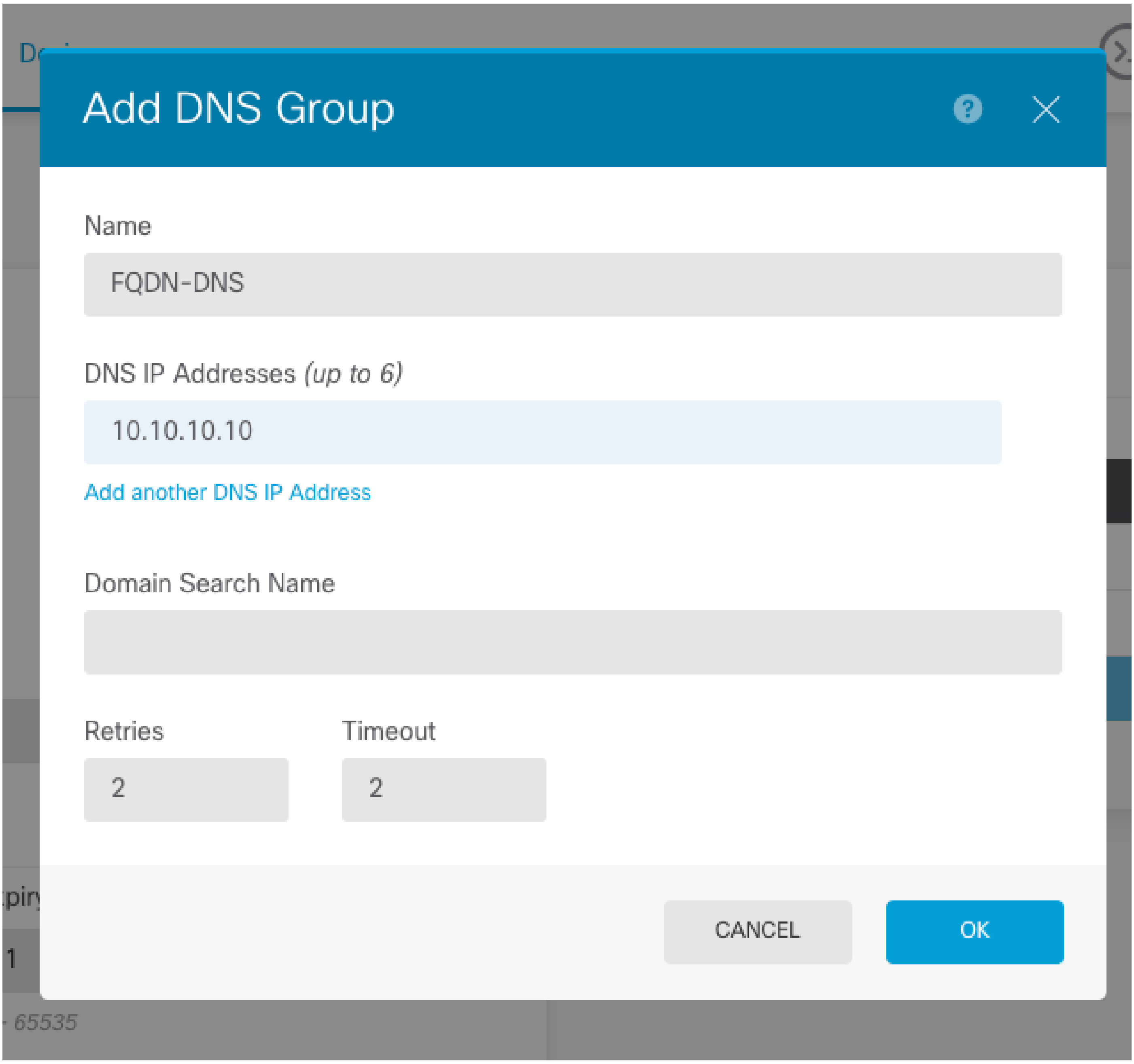
FQDN DNS SETTINGS

Poll Time: 240 minutes (1 - 65535)

Expiry: 1 minutes (1 - 65535)

Management Interface

DNS Group



Add DNS Group

Name: FQDN-DNS

DNS IP Addresses *(up to 6)*: 10.10.10.10

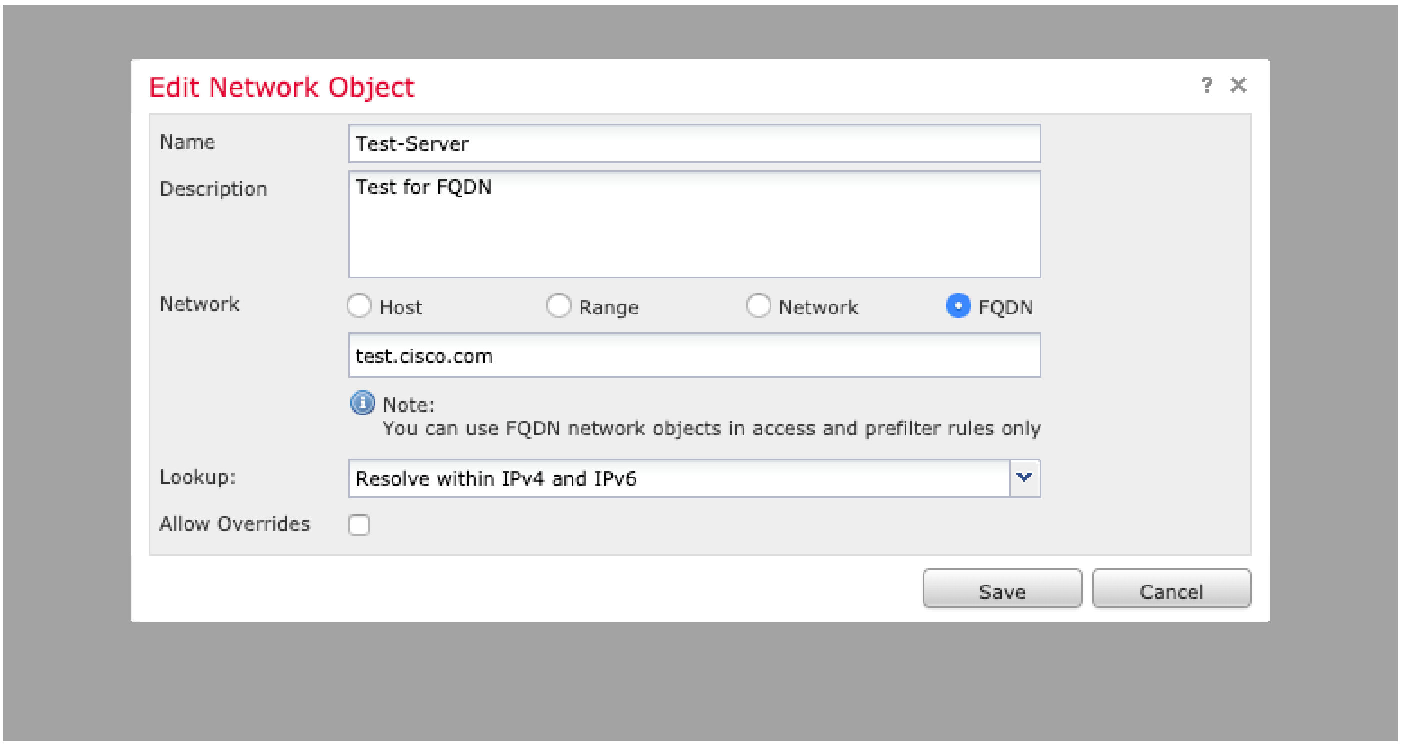
Domain Search Name:

Retries: 2

Timeout: 2

附註：確保在配置DNS之後將系統策略應用於FTD。（配置的DNS伺服器應解析將使用的FQDN）

步驟2.建立FQDN對象，為此，請導航到**對象>對象管理>新增網路>新增對象。**



Edit Network Object

Name: Test-Server

Description: Test for FQDN

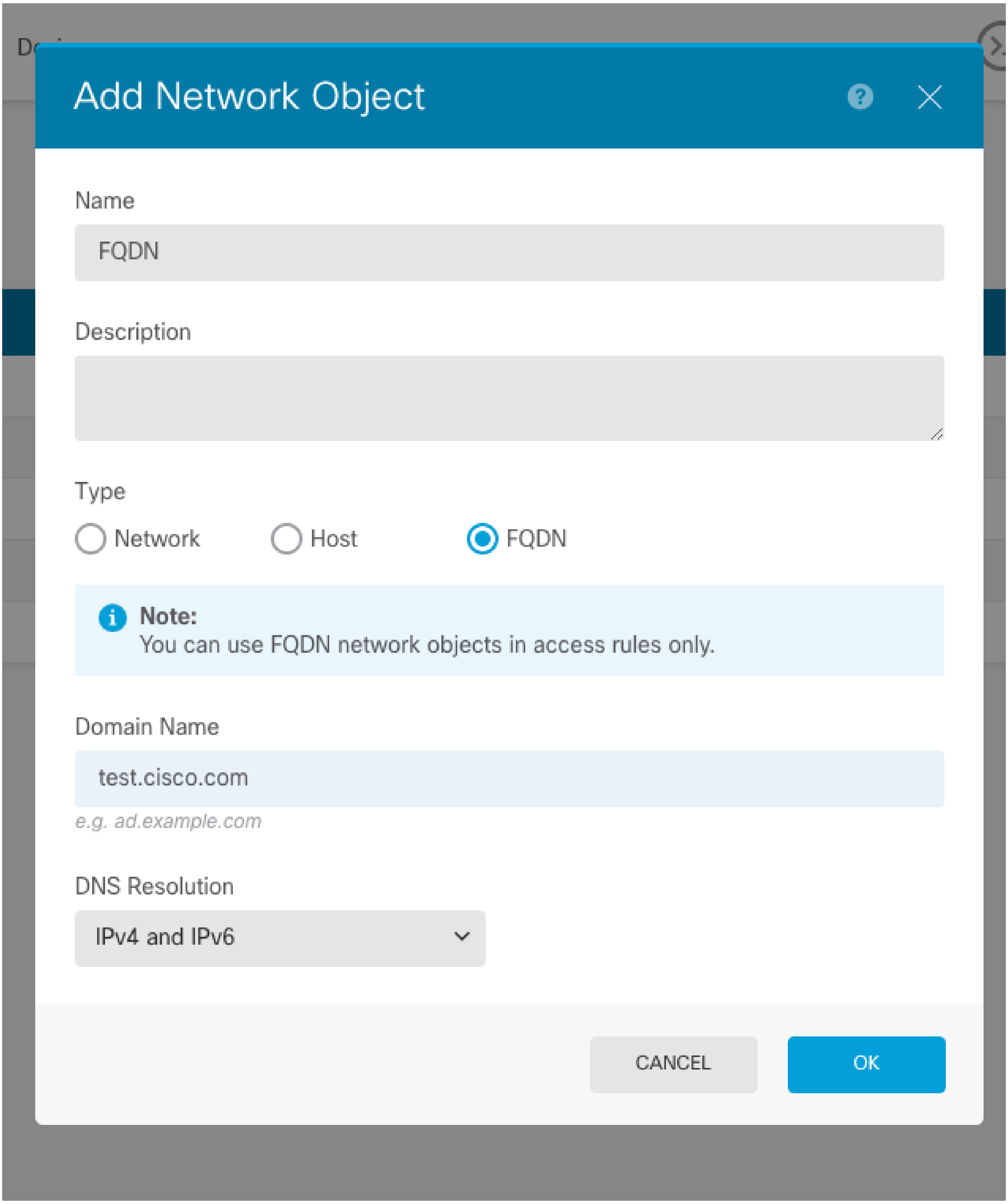
Network: ○ Host ○ Range ○ Network ● FQDN

test.cisco.com

Note:
You can use FQDN network objects in access and prefilter rules only

Lookup: Resolve within IPv4 and IPv6

Allow Overrides □



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

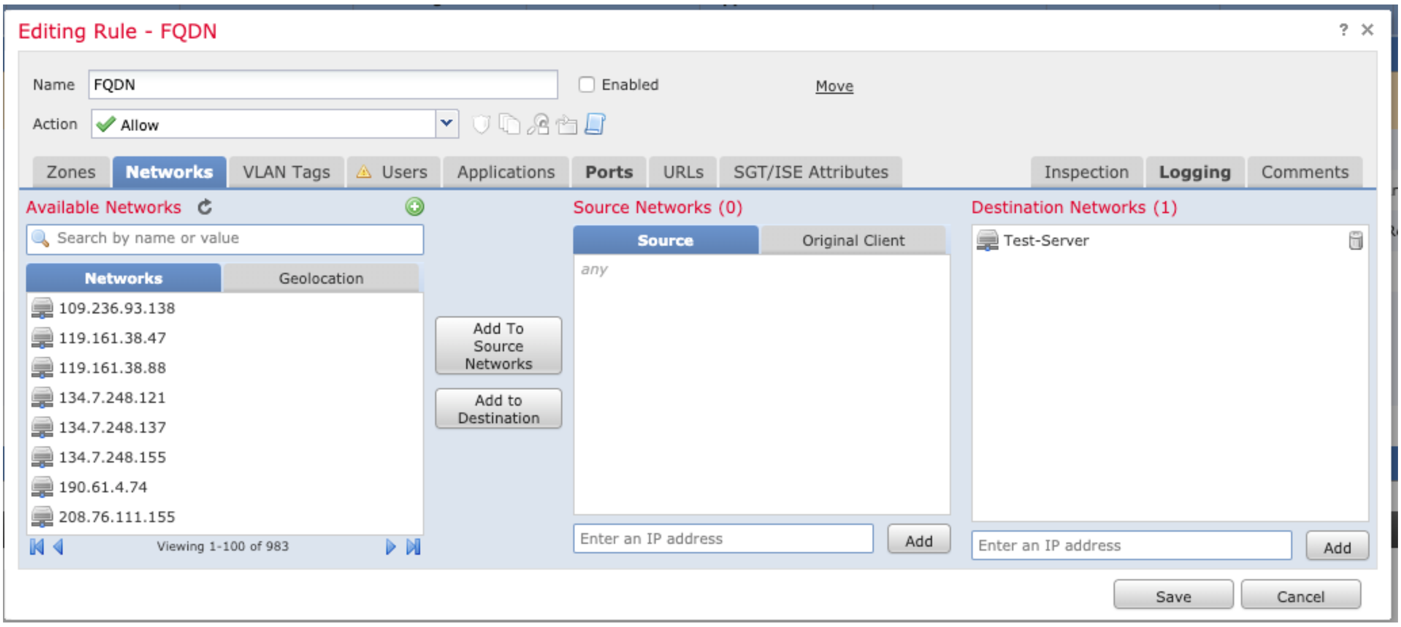
e.g. ad.example.com

DNS Resolution

IPv4 and IPv6

步驟3.導航到**Policies > Access Control**，建立訪問控制規則。

> **附註**：您可以根據要求建立規則或修改現有規則。FQDN對象可以在源網路和/或目標網路中使用。



Editing Rule - FQDN

Name: FQDN

□ Enabled

Action: Allow

Available Networks

109.236.93.138
119.161.38.47
119.161.38.88
134.7.248.121
134.7.248.137
134.7.248.155
190.61.4.74
208.76.111.155

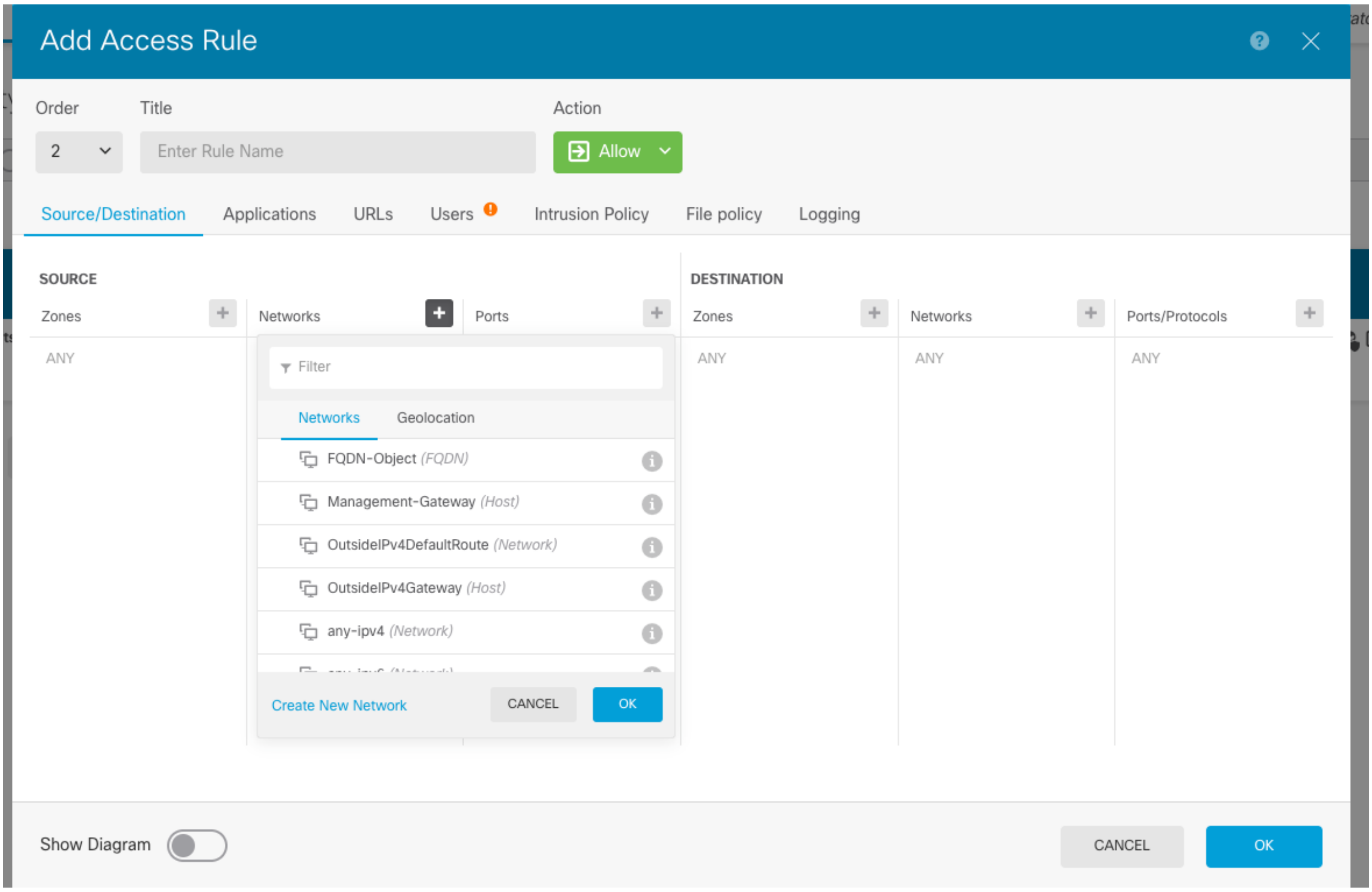
Viewing 1-100 of 983

Source Networks (0)

any

Destination Networks (1)

Test-Server



Add Access Rule

Order: 2

Title: Enter Rule Name

Action: Allow

SOURCE

Zones: ANY

DESTINATION

Zones: ANY

Networks: ANY

Ports/Protocols: ANY

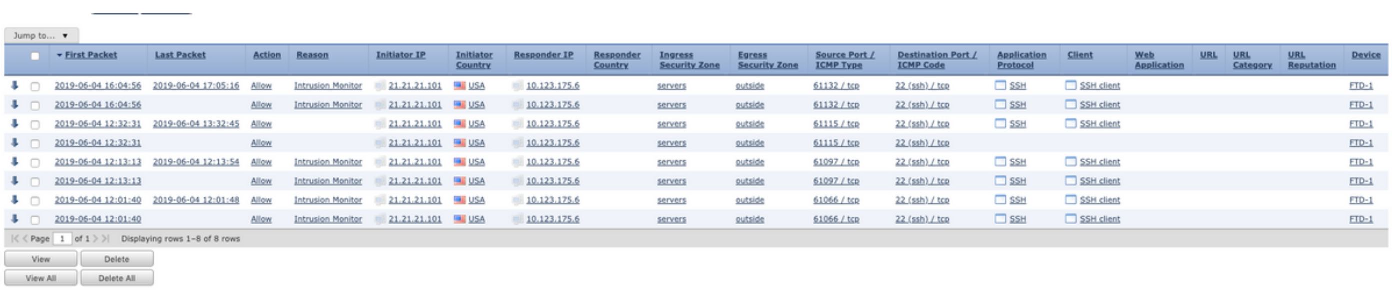
FQDN-Object *(FQDN)*
Management-Gateway *(Host)*
OutsideIPv4DefaultRoute *(Network)*
OutsideIPv4Gateway *(Host)*
any-ipv4 *(Network)*

確保在配置完成後應用該策略。

驗證

啟動來自客戶端電腦的流量，該流量應觸發所建立的基於FQDN的規則。

在FMC上，導航到**Events > Connection Events，過濾特定流量。**



	☐	▾ 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

疑難排解

DNS伺服器應該能夠解析FQDN對象，這可以通過運行以下命令的CLI進行驗證：

- **系統支援diagnostic-cli**
- **show fqdn**

.