액세스 제어 규칙에 대한 FQDN 기반 개체 구성

목차

소개

이 문서에서는 FMC(Firewall Management Center)를 통한 FQDN(Fully Qualified Domain Name) 객체의 컨피그레이션 및 액세스 규칙 생성에서 FQDN 객체를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 기술에 대한 지식
- FMC(FireSIGHT Management Center)에서 액세스 제어 정책 구성 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

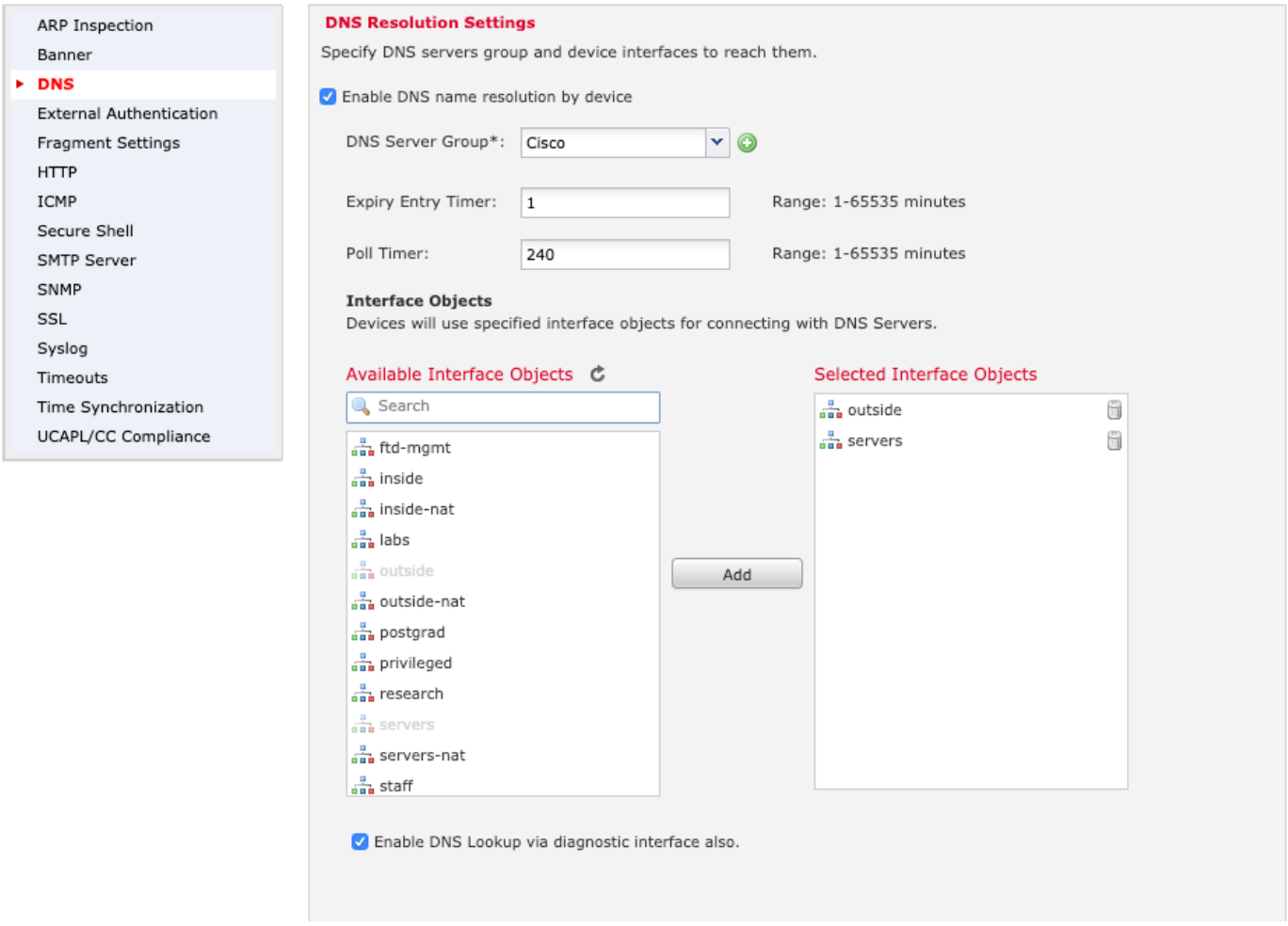
- 버전 6.3 이상을 실행하는 Firepower Management Center
- 버전 6.3 이상을 실행하는 Firepower Threat Defense

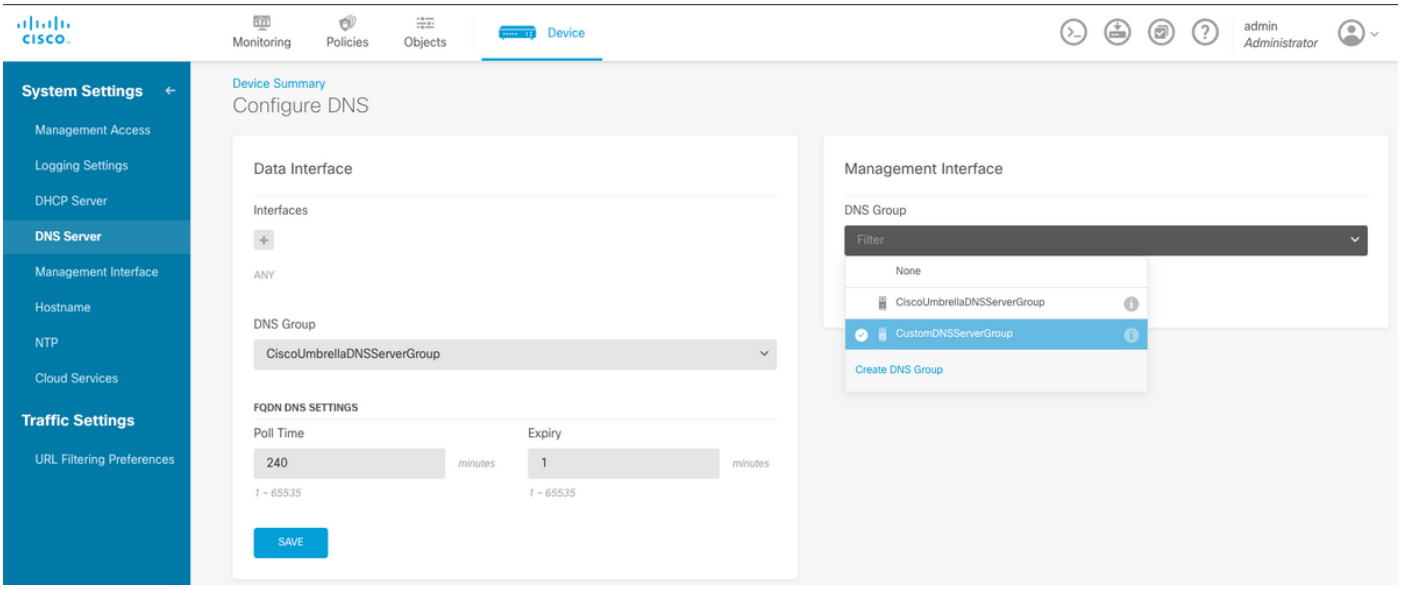
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

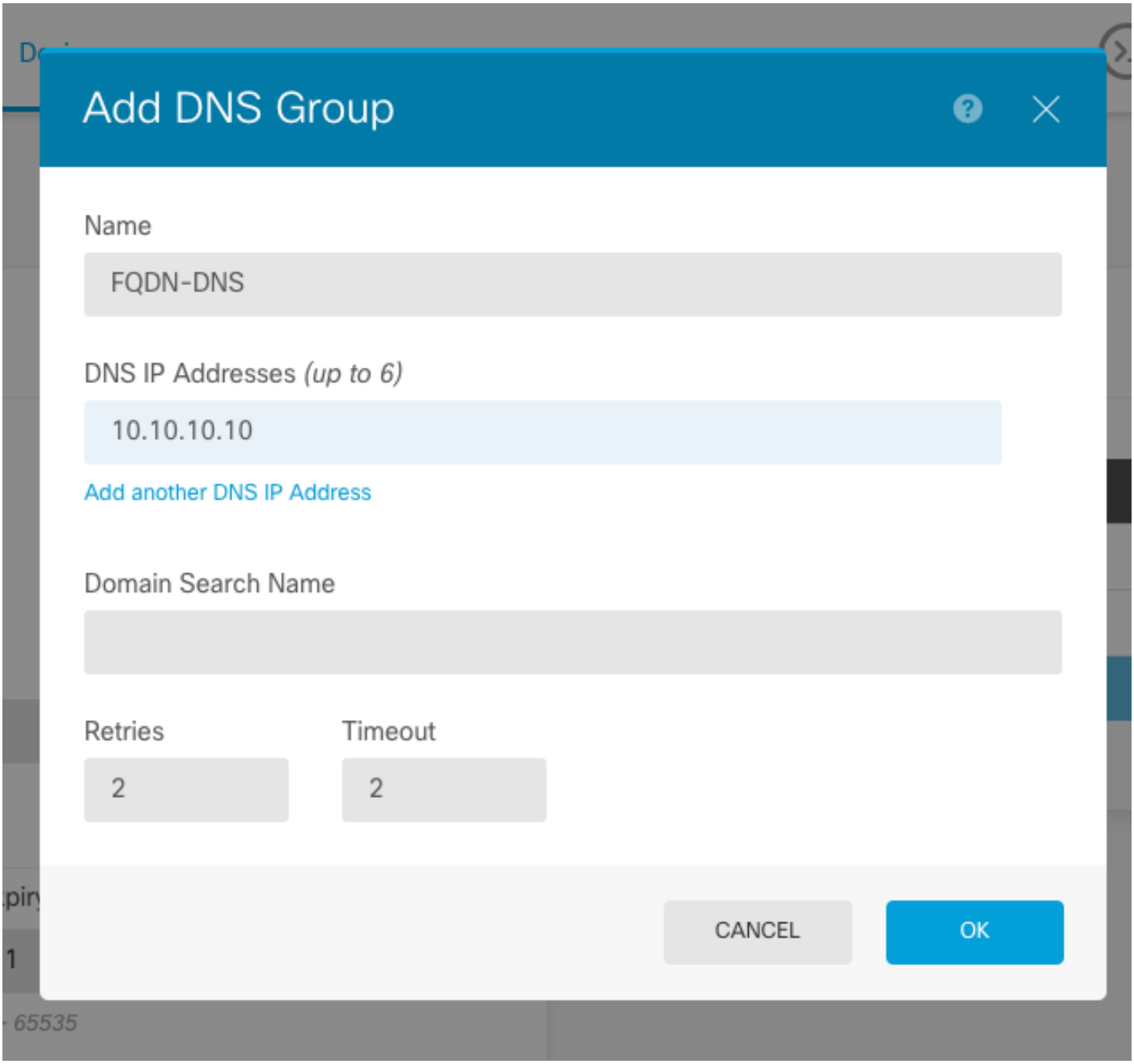
구성

1단계. FQDN 기반 개체를 구성하고 사용하려면 먼저 Firepower Threat Defense에서 DNS를 구성합니다.

FMC에 로그인하여 Devices(디바이스) **> Platform Settings(플랫폼 설정) > DNS로 이동합니다**.

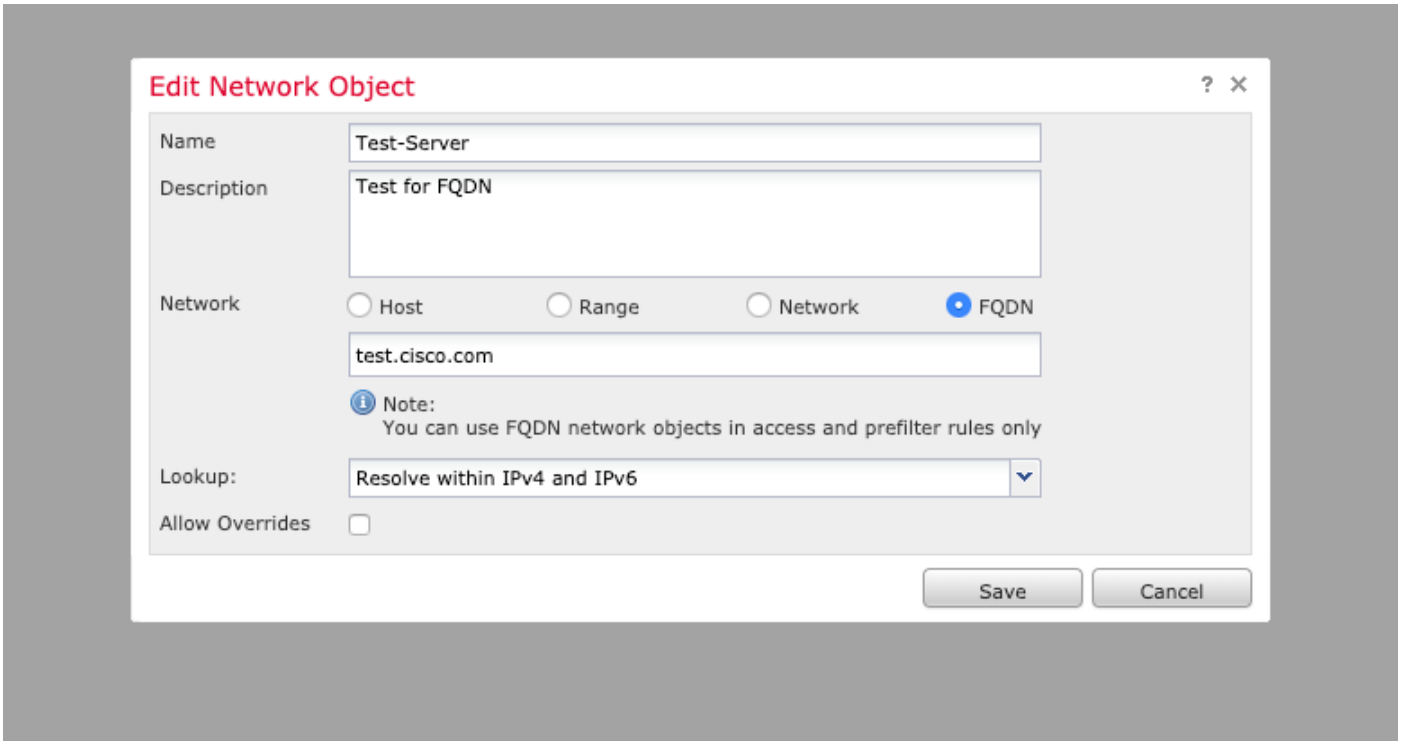

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP
ICMP
Secure Shell
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
UCAPL/CC Compliance
DNS Resolution Settings
Specify DNS servers group and device interfaces to reach them.
Enable DNS name resolution by device
DNS Server 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
Search
ftd-mgmt
inside
inside-nat
labs
outside
outside-nat
postgrad
privileged
research
servers
servers-nat
staff
Add
Selected Interface Objects
outside
servers
Enable DNS Lookup via diagnostic interface also.

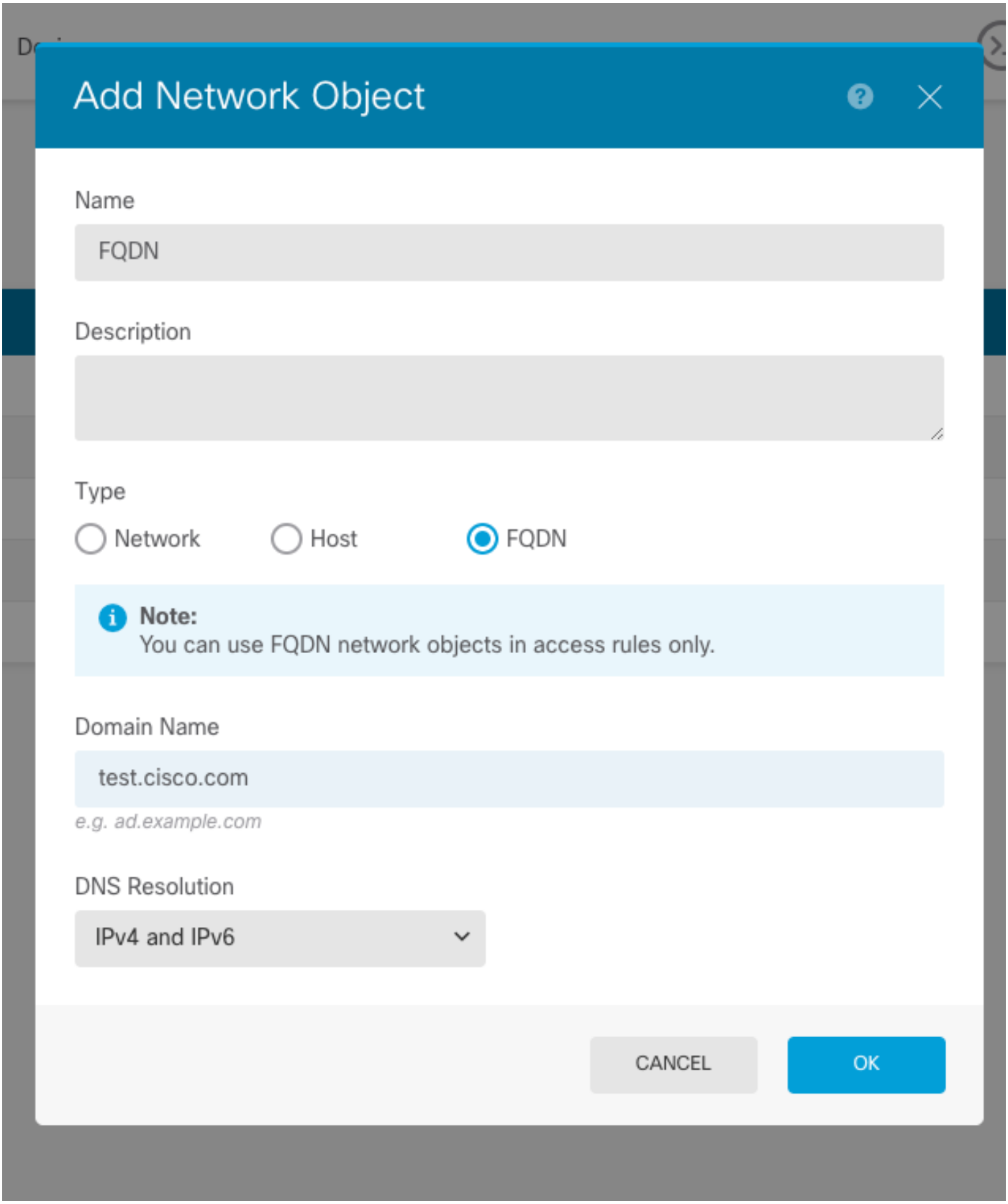

Monitoring
Policies
Objects
Device
admin
Administrator
System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
NTP
Cloud Services
Traffic Settings
URL Filtering Preferences
Device Summary
Configure DNS
Data Interface
Interfaces
ANY
DNS Group
CiscoUmbrellaDNSServerGroup
FQDN DNS SETTINGS
Poll Time
240
minutes
1 - 65535
Expiry
1
minutes
1 - 65535
SAVE
Management Interface
DNS Group
Filter
None
CiscoUmbrellaDNSServerGroup
CustomDNSServerGroup
Create DNS Group



참고:DNS를 구성한 후 시스템 정책이 FTD에 적용되는지 확인합니다. (구성된 DNS 서버는 사용할 FQDN을 확인해야 합니다.)

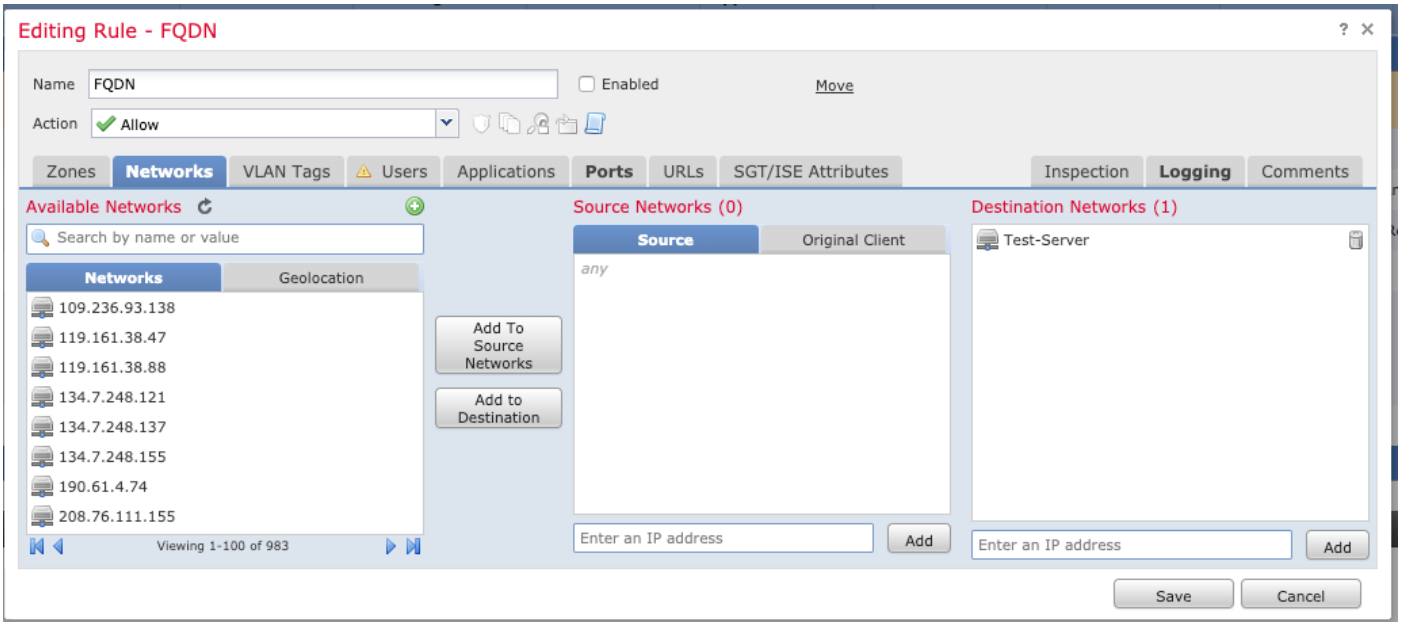
2단계. Objects(개체) > Object Management(개체 **관리) > Add Network(네트워크 추가) > Add Object(개체 추가)로 이동하려면 FQDN 개체를 만듭니다.**

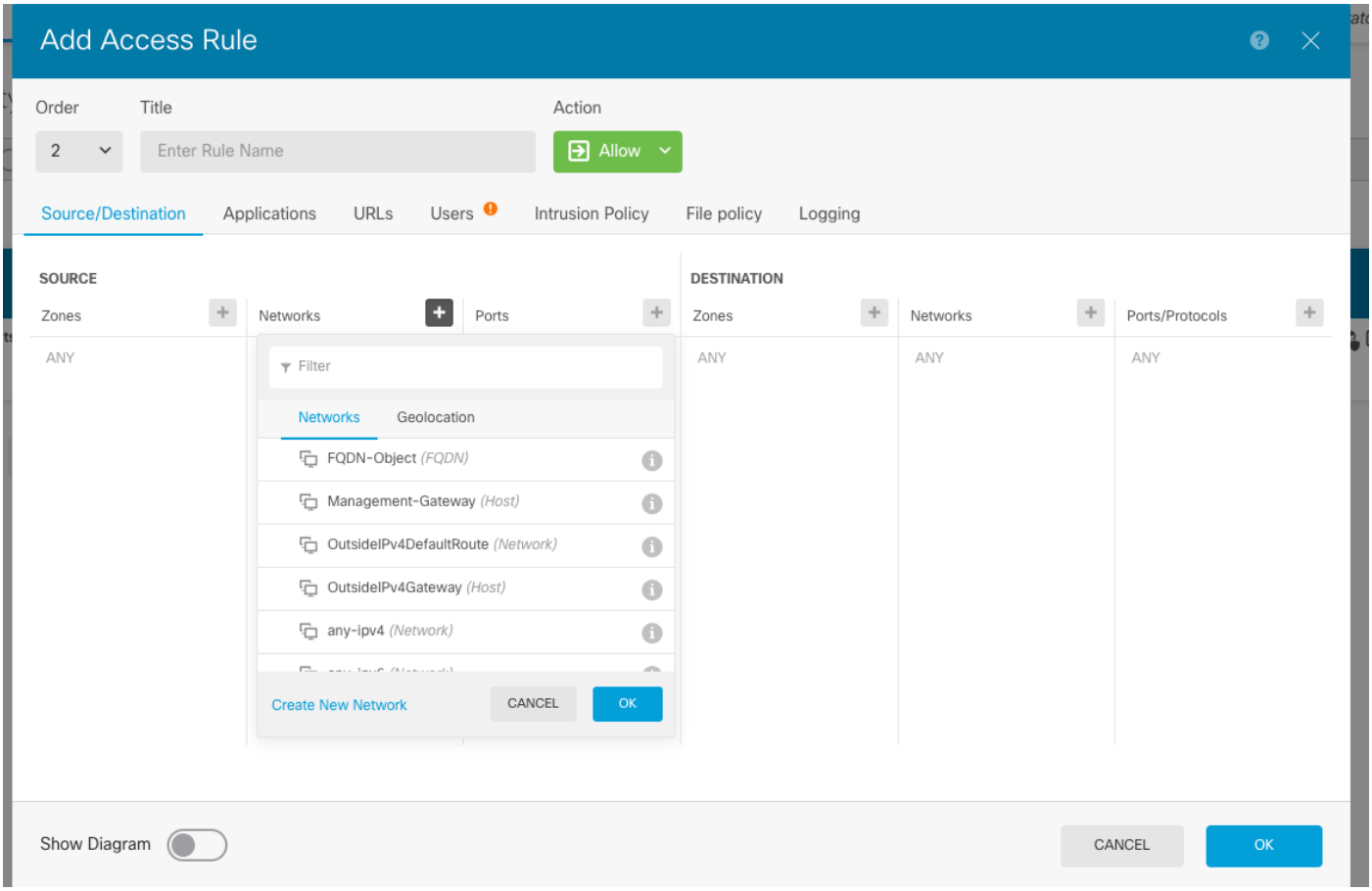

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



3단계. Policies(정책) **> Access Control(액세스 제어)**로 이동하여 액세스 제어 규칙**을 생성합니다.**

참고:요구 사항을 기반으로 규칙을 생성하거나 기존 규칙을 수정할 수 있습니다.FQDN 개체는 소스 및/또는 대상 네트워크에서 사용할 수 있습니다.



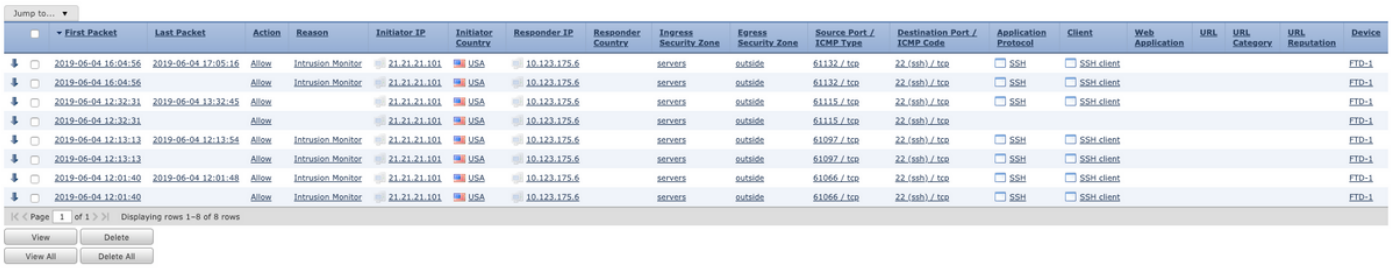


컨피그레이션이 완료된 후 정책이 적용되는지 확인합니다.

다음을 확인합니다.

생성된 FQDN 기반 규칙을 트리거할 것으로 예상되는 클라이언트 컴퓨터에서 트래픽을 시작합니다.

FMC에서 **Events > Connection Events**로 이동하여 특정 트래픽을 필터링합니다.



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

문제 해결

DNS 서버는 FQDN 객체를 확인할 수 있어야 하며, CLI에서 다음 명령을 실행하여 확인할 수 있습니다.

- **시스템 지원 진단 cli**
- **FQDN 표시**

.