FQD-gebaseerde object voor toegangscontroleregel configureren

Inhoud

Inleiding

Dit document beschrijft de configuratie van het Fully Qualified Domain Name (FQDN)-object via het Firewallbeheercentrum (FMC) en de manier waarop u FQDN-object moet gebruiken in de creatie van de toegangsregel.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER-technologie.
- Kennis van het configureren van toegangsbeheerbeleid voor FireSIGHT Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

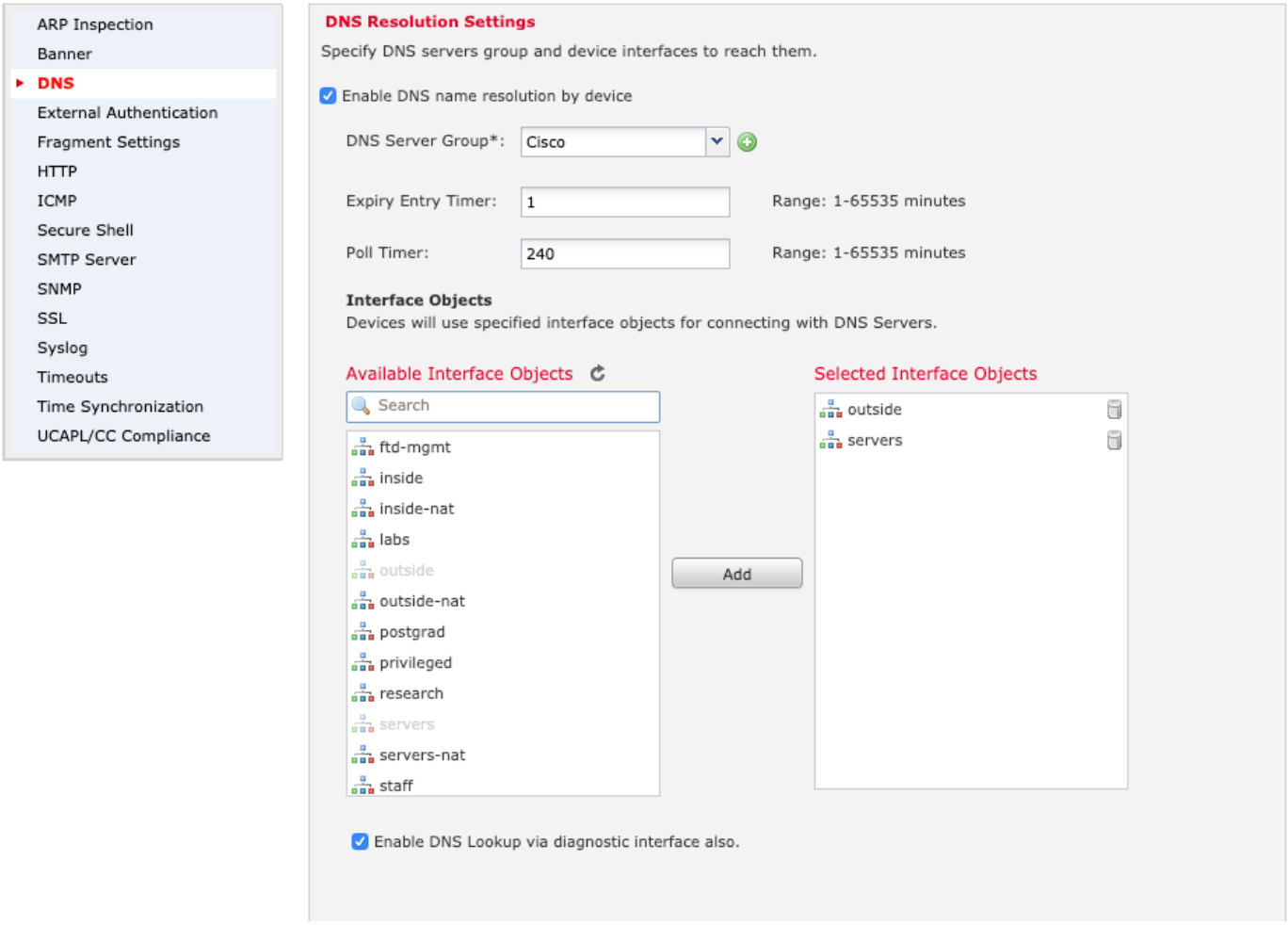
- Firepower Management Center met versie 6.3 en hoger.
- Firepower Threat Defense met versie 6.3 en hoger.

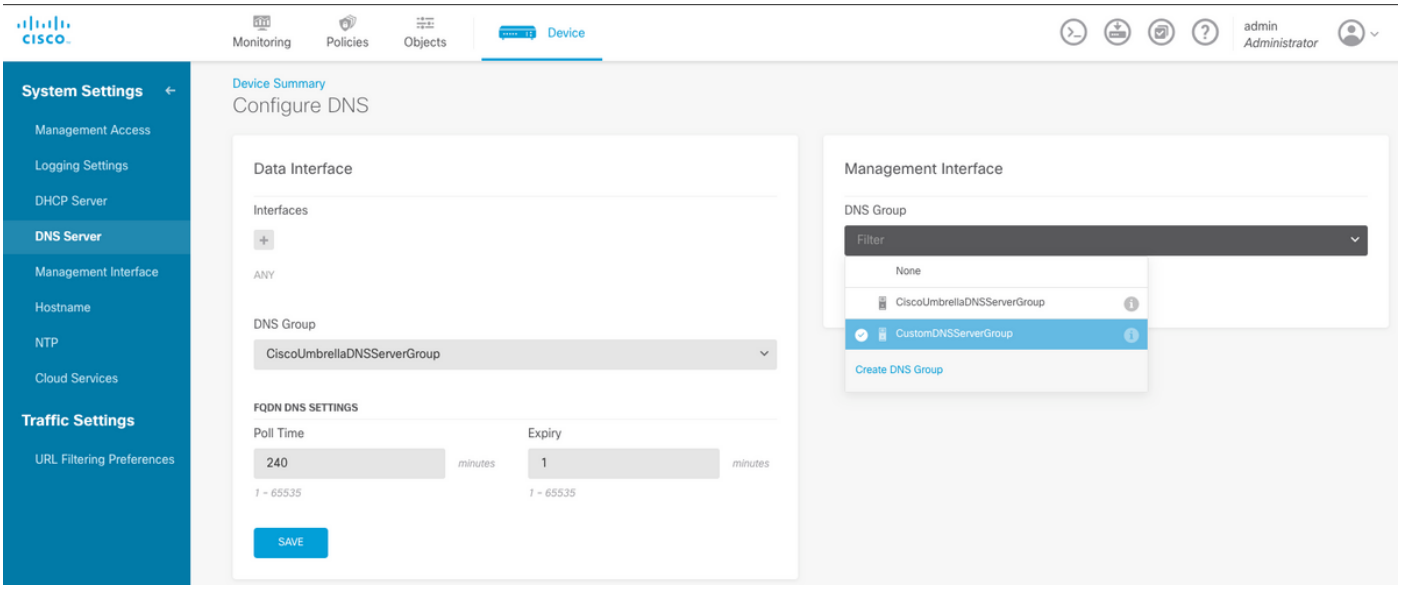
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

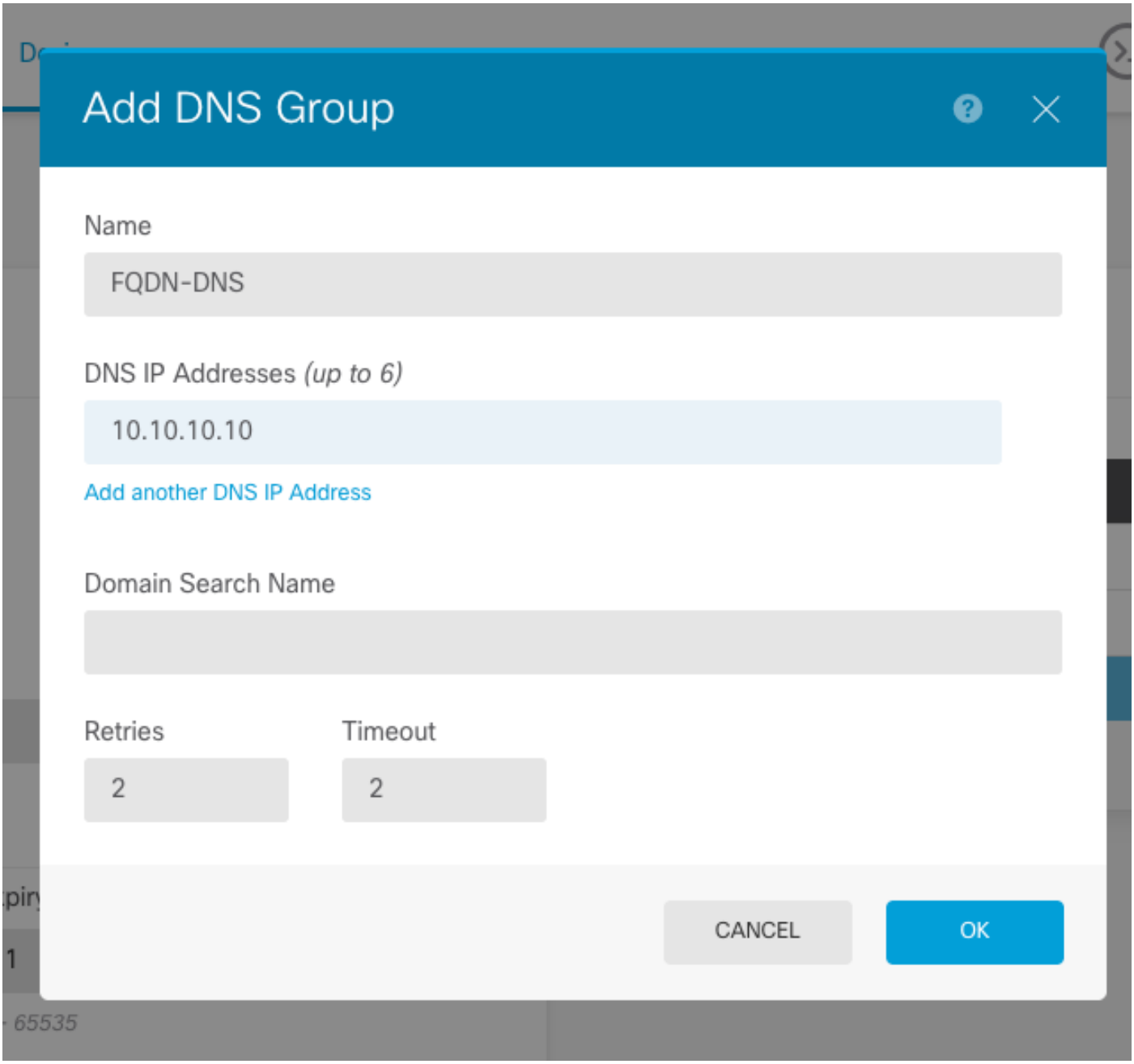
Configureren

Stap 1. Om op FQDN gebaseerd object te configureren en te gebruiken, moet u eerst DNS op de Firepower Threat Defense configureren.

Meld u aan bij het FMC en navigeer naar **Apparaten > Platform Instellingen > DNS**.

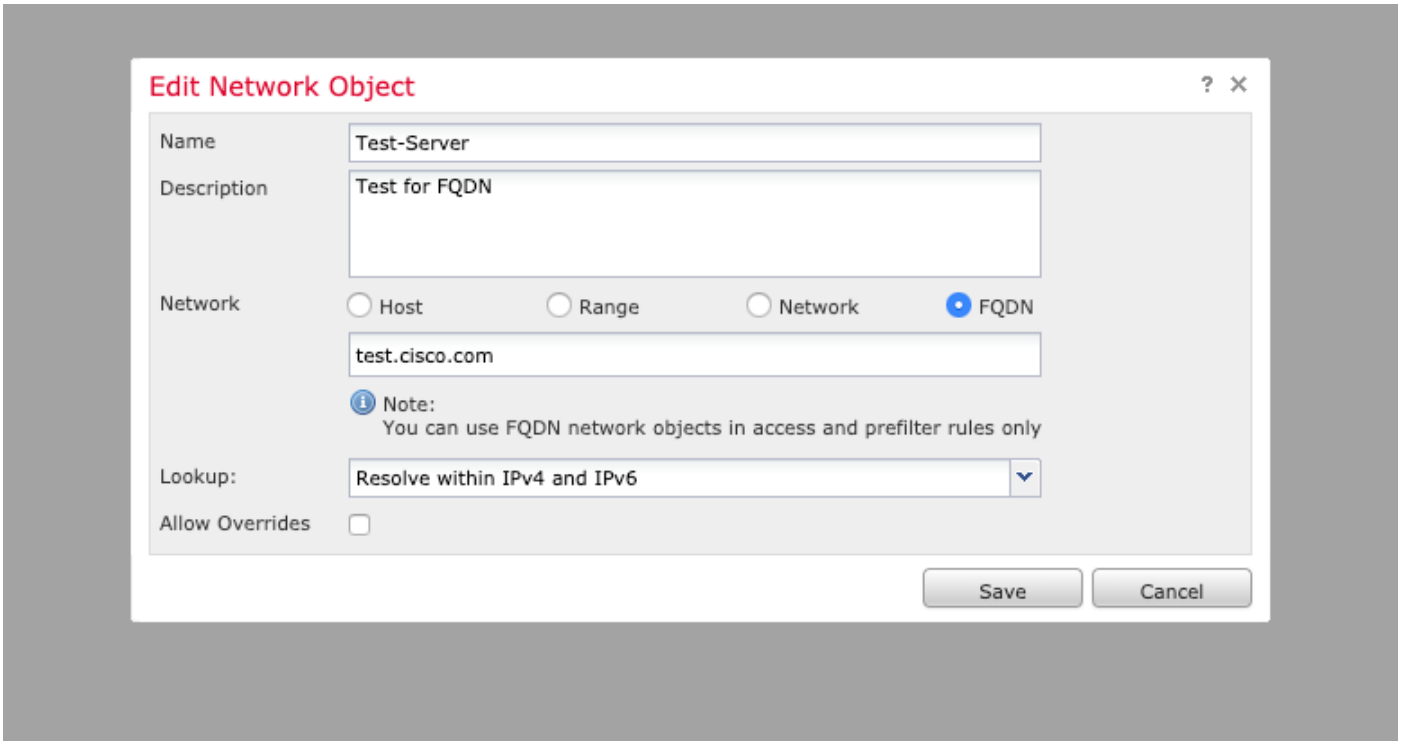


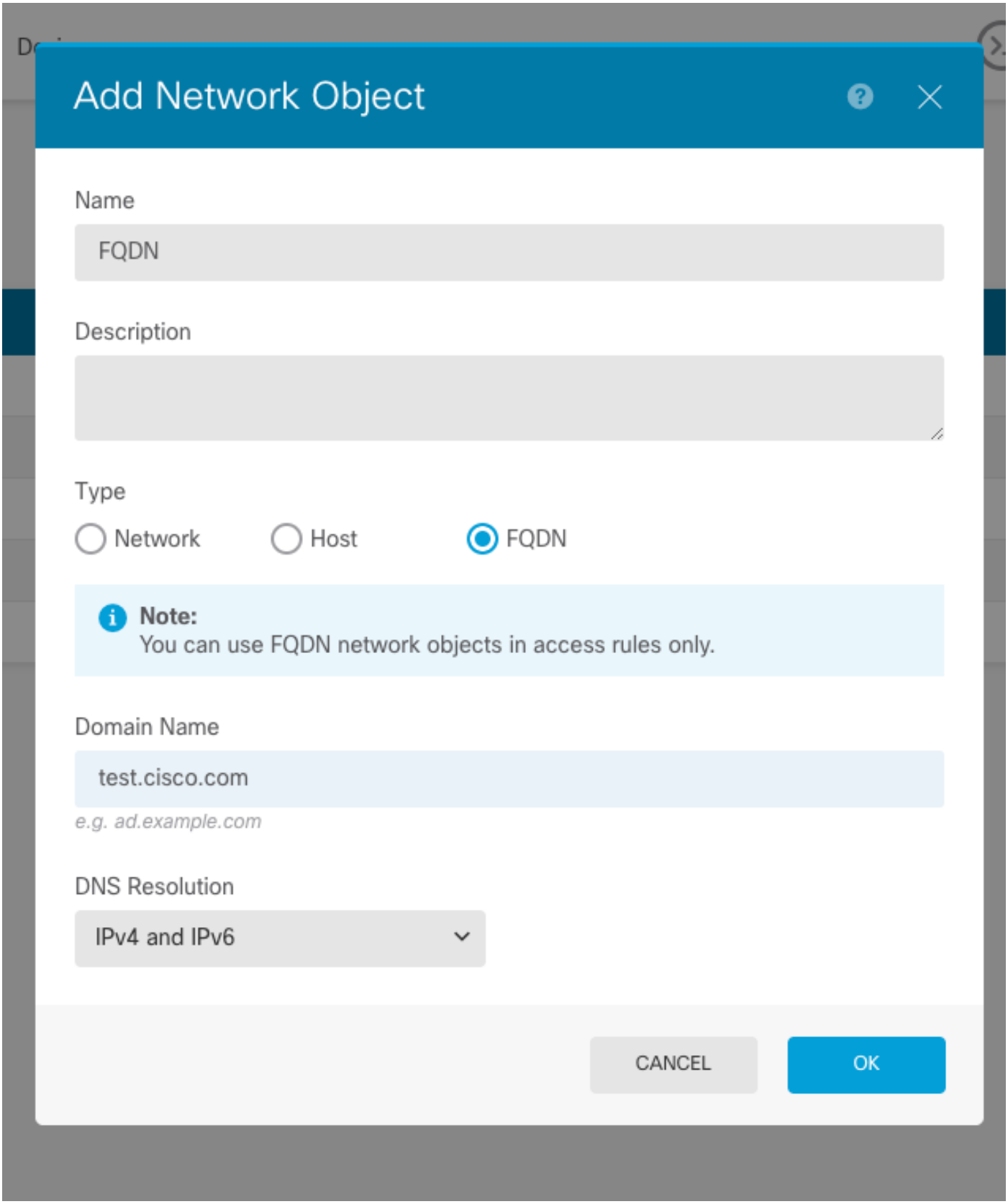




Opmerking: Zorg ervoor dat het systeembeleid op de FTD wordt toegepast nadat u de DNS hebt geconfigureren. (De DNS-server moet de FQDN-oplossing oplossen die wordt gebruikt)

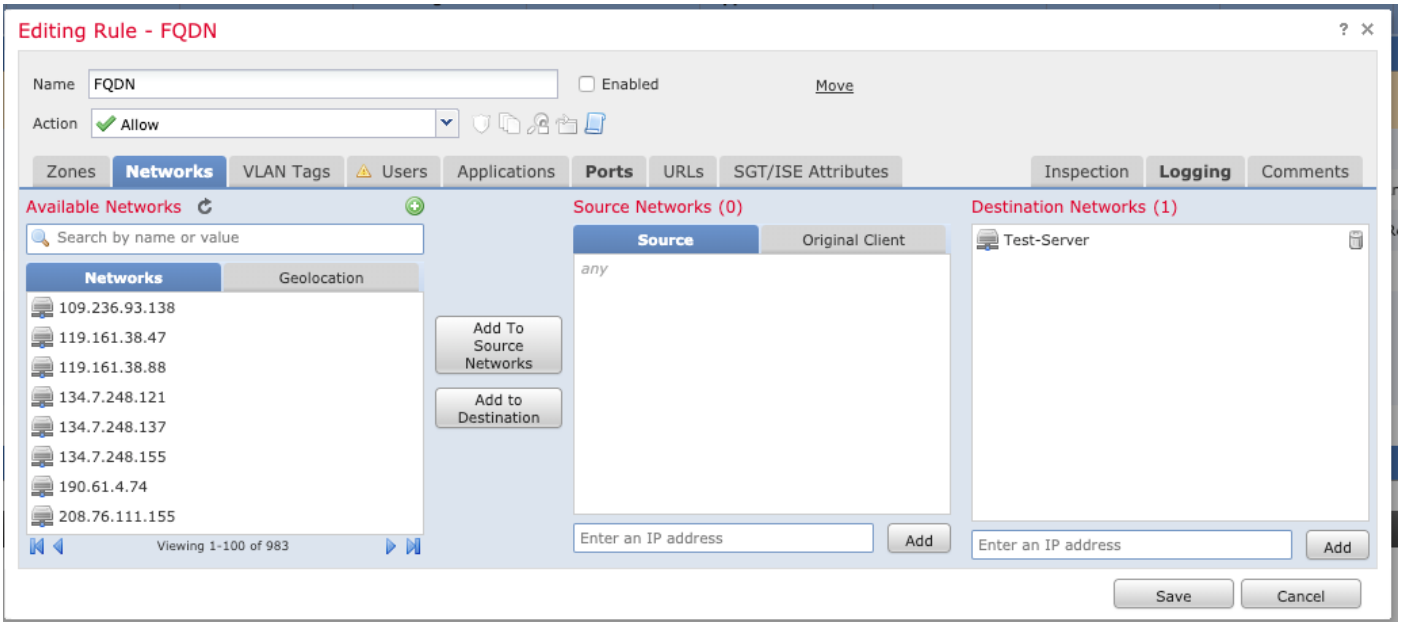
Stap 2. Maak het FQDN-object, om dat te doen door te **sturen naar objecten > Objectbeheer > Add Network > Add Object.**

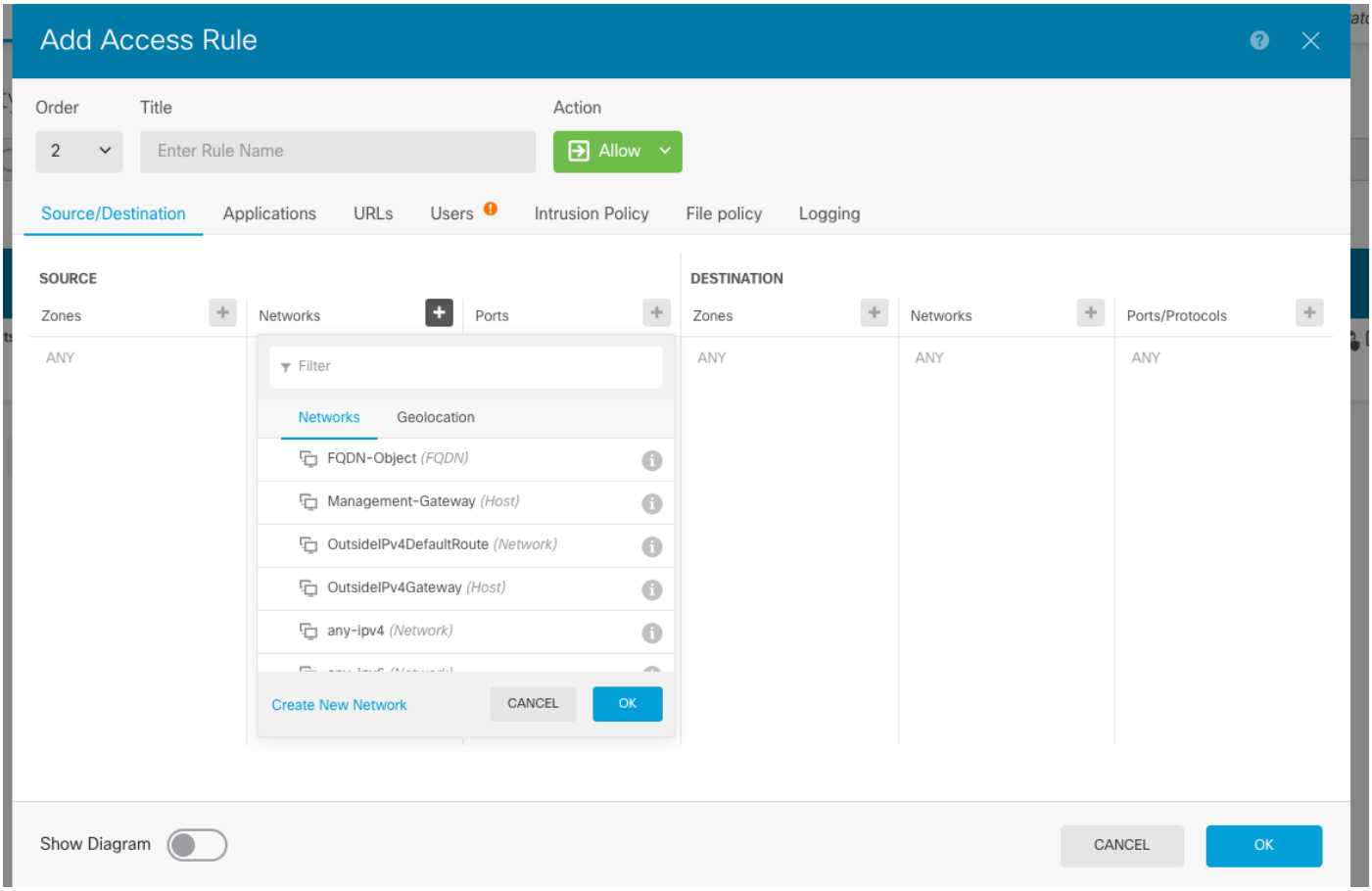

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



Stap 3. Maak een toegangscontroleregel door naar **beleid > Toegangsbeheer** te navigeren.

Opmerking: U kunt een regel maken of de bestaande regel wijzigen op basis van de vereiste. Het FQDN-object kan in bron- en/of doelnetwerken worden gebruikt.



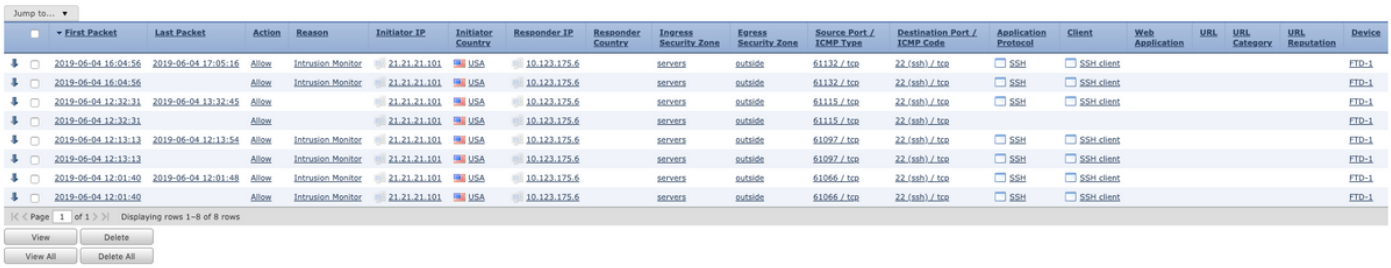


Zorg ervoor dat het beleid wordt toegepast nadat de configuratie is voltooid.

Verifiëren

Initieer verkeer vanaf de clientmachine, wat naar verwachting de op FQDN gebaseerde regel zal activeren.

Op het VCC, navigeer aan **Gebeurtenissen > gebeurtenis, filter voor het specifieke verkeer.**



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

Problemen oplossen

De DNS server zou het FQDN object moeten kunnen oplossen, dit kan worden geverifieerd vanuit de CLI-instelling die deze opdracht uitvoert:

- systeemondersteuning voor diagnostische cli
- tonen fqdn

.