Configurer l'objet basé sur FQDN pour la règle de contrôle d'accès

Contenu

Introduction

Ce document décrit la configuration de l'objet FQDN (Fully Qualified Domain Name) via le Centre de gestion du pare-feu (FMC) et comment utiliser l'objet FQDN dans la création de la règle d'accès.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower.
- Connaissance de la configuration de la stratégie de contrôle d'accès sur Firesight Management Center (FMC)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

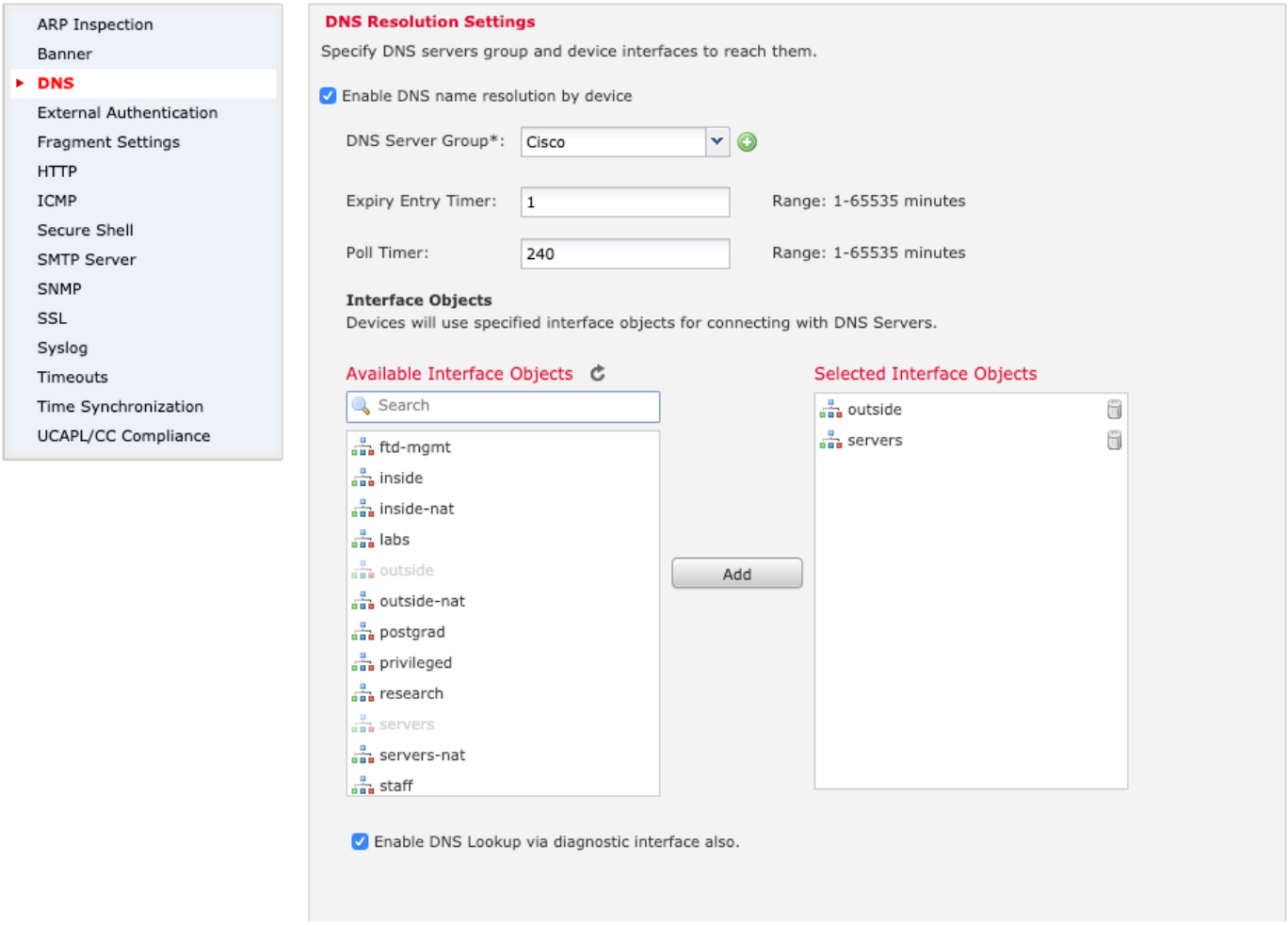
- Firepower Management Center exécutant les versions 6.3 et ultérieures.
- Firepower Threat Defense version 6.3 et ultérieure.

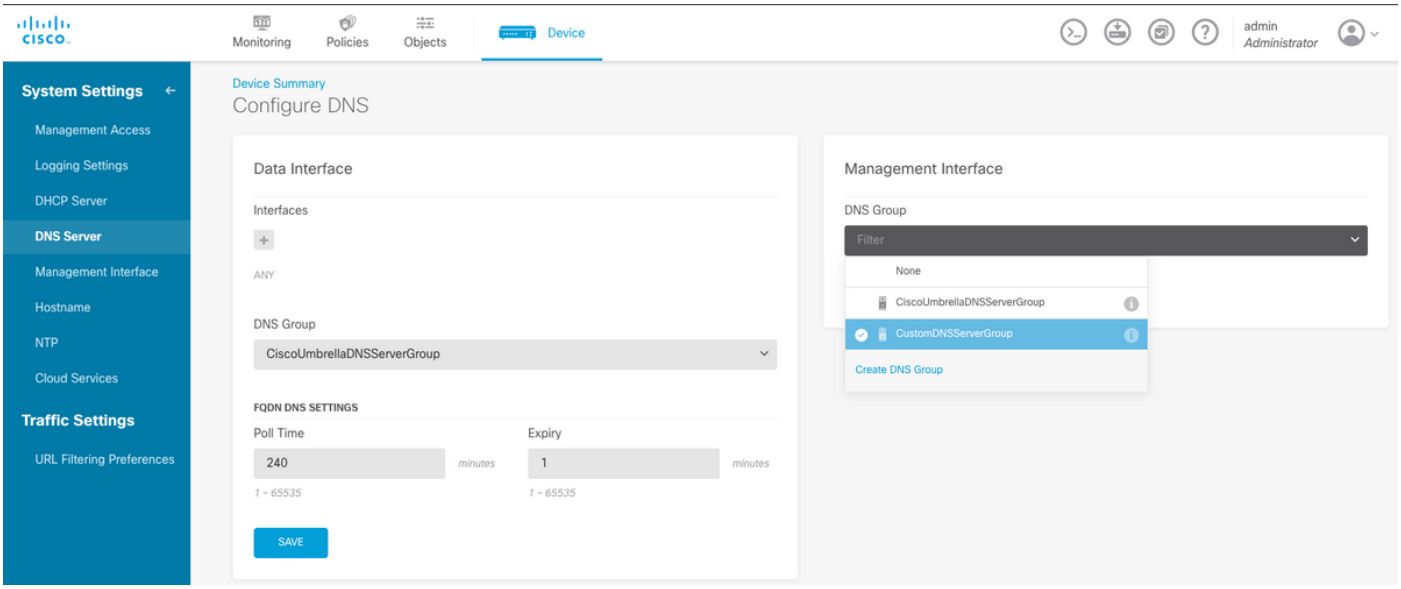
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

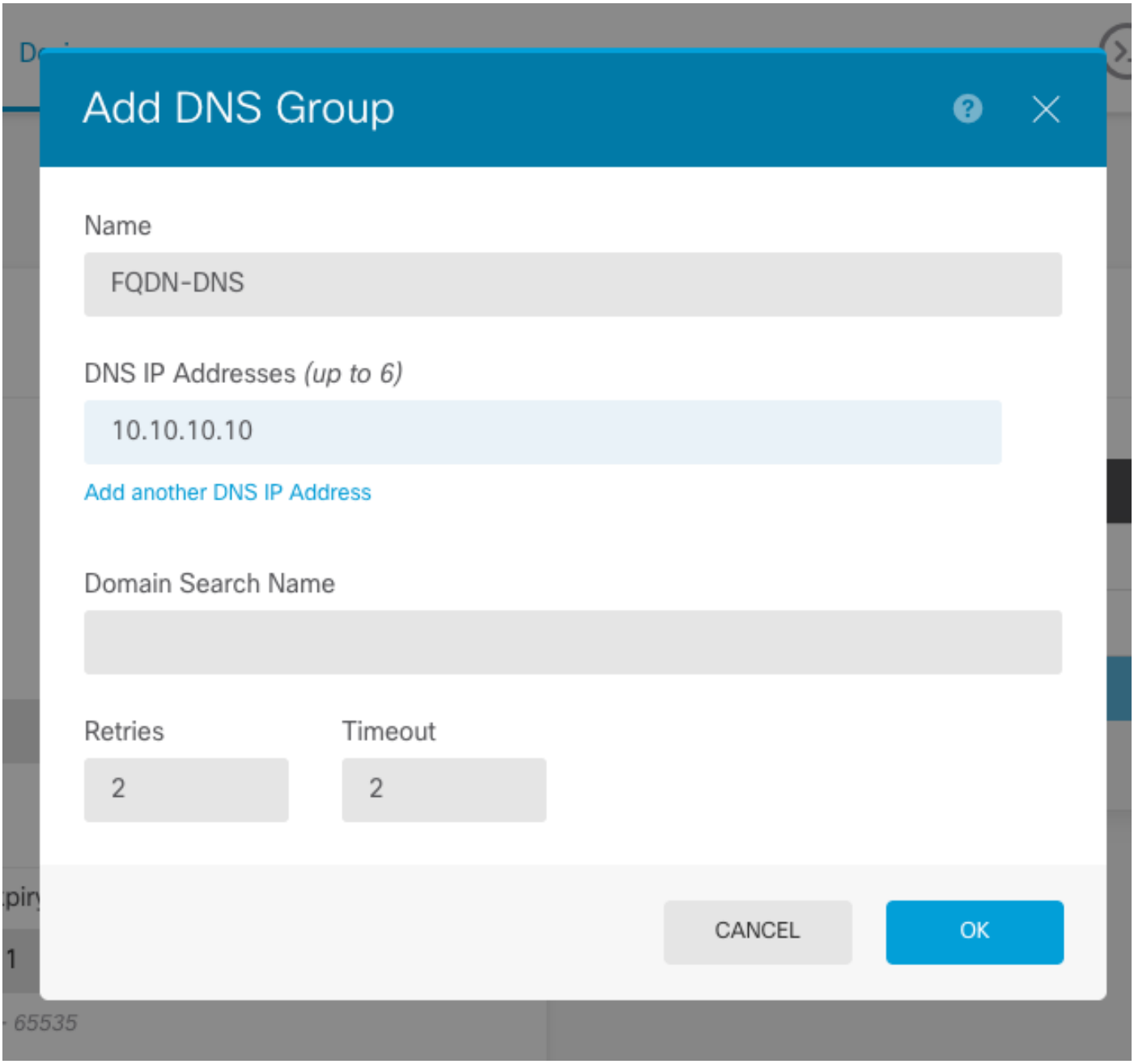
Configuration

Étape 1. Pour configurer et utiliser un objet basé sur FQDN, commencez par configurer DNS sur Firepower Threat Defense.

Connectez-vous au FMC et accédez à **Devices > Platform Settings > DNS**.

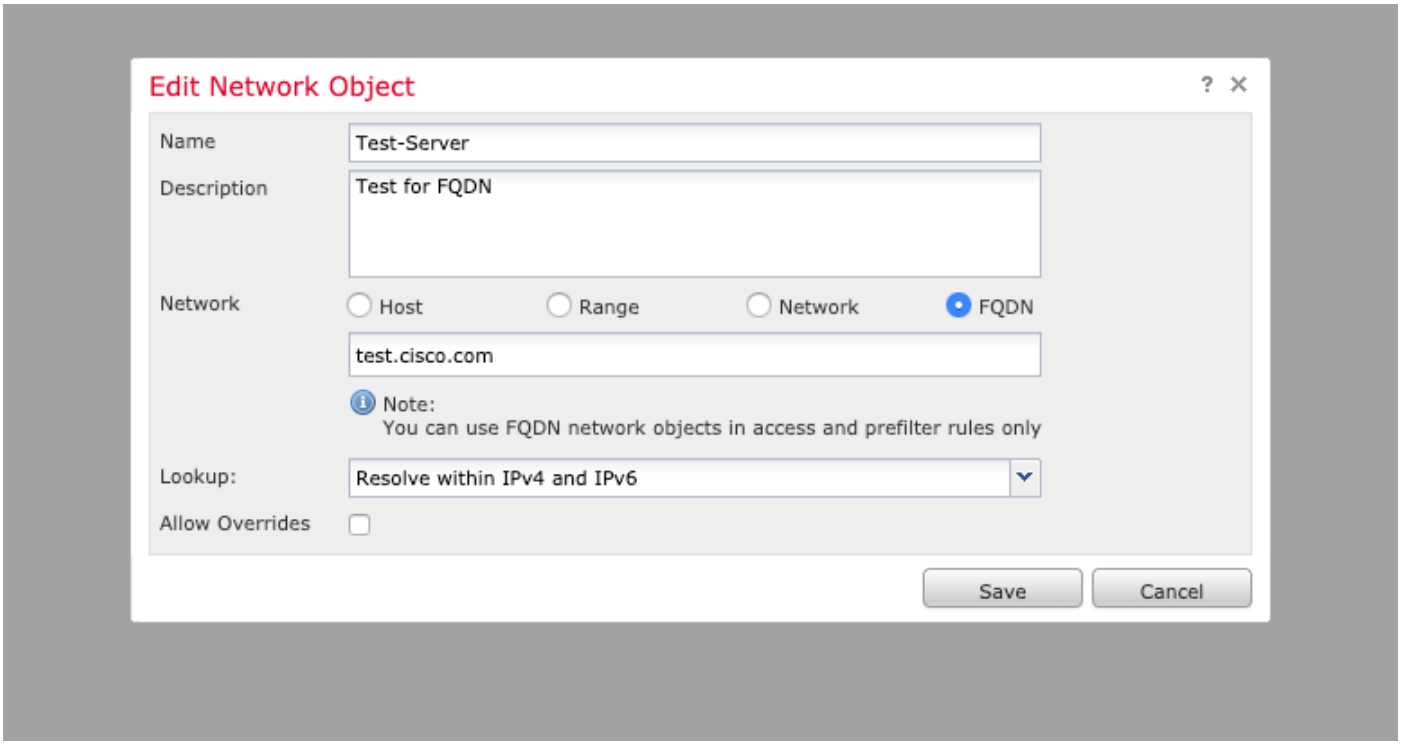


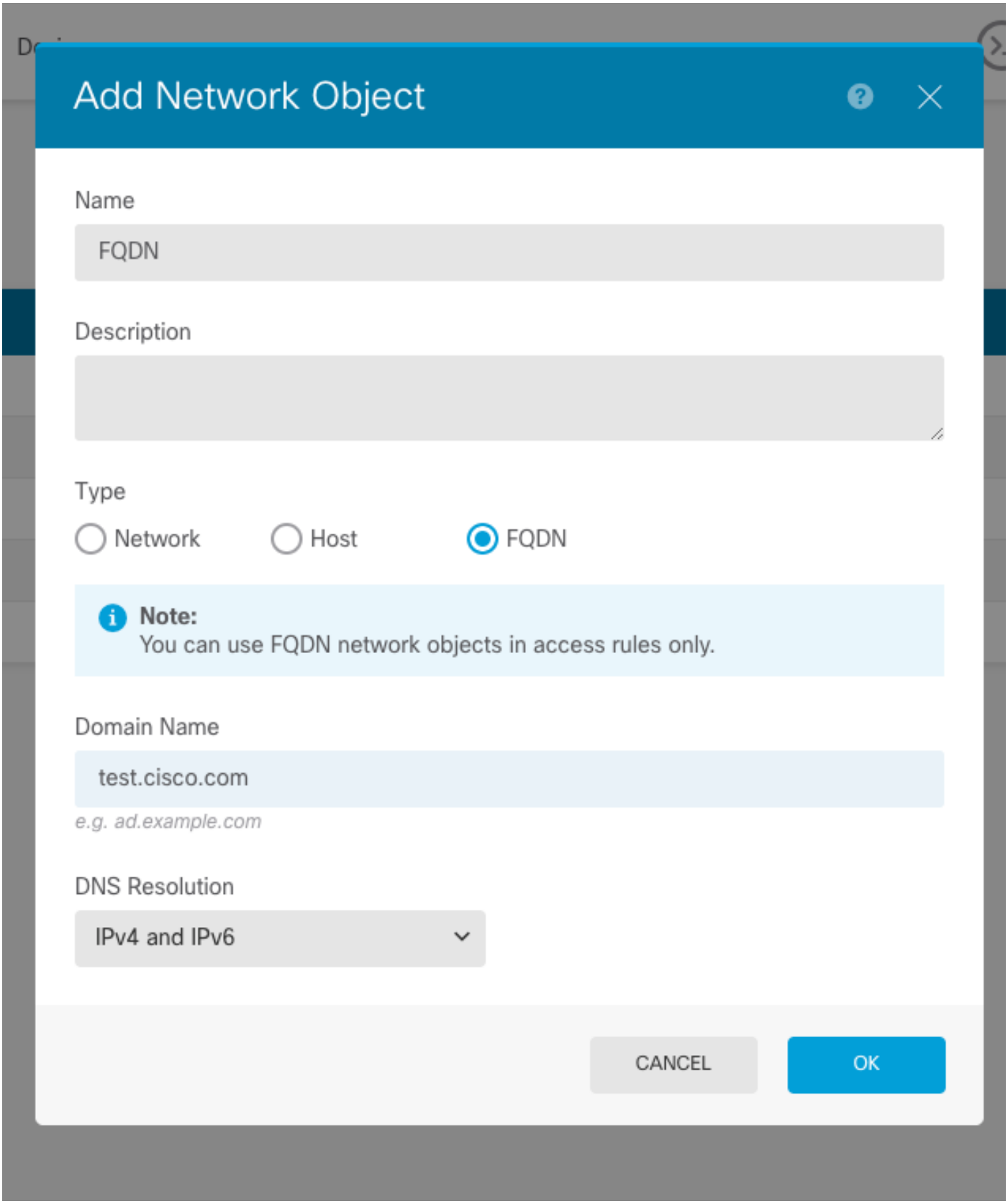




Note: Assurez-vous que la stratégie système est appliquée au FTD après avoir configuré le DNS. (Le serveur DNS configuré doit résoudre le nom de domaine complet qui sera utilisé)

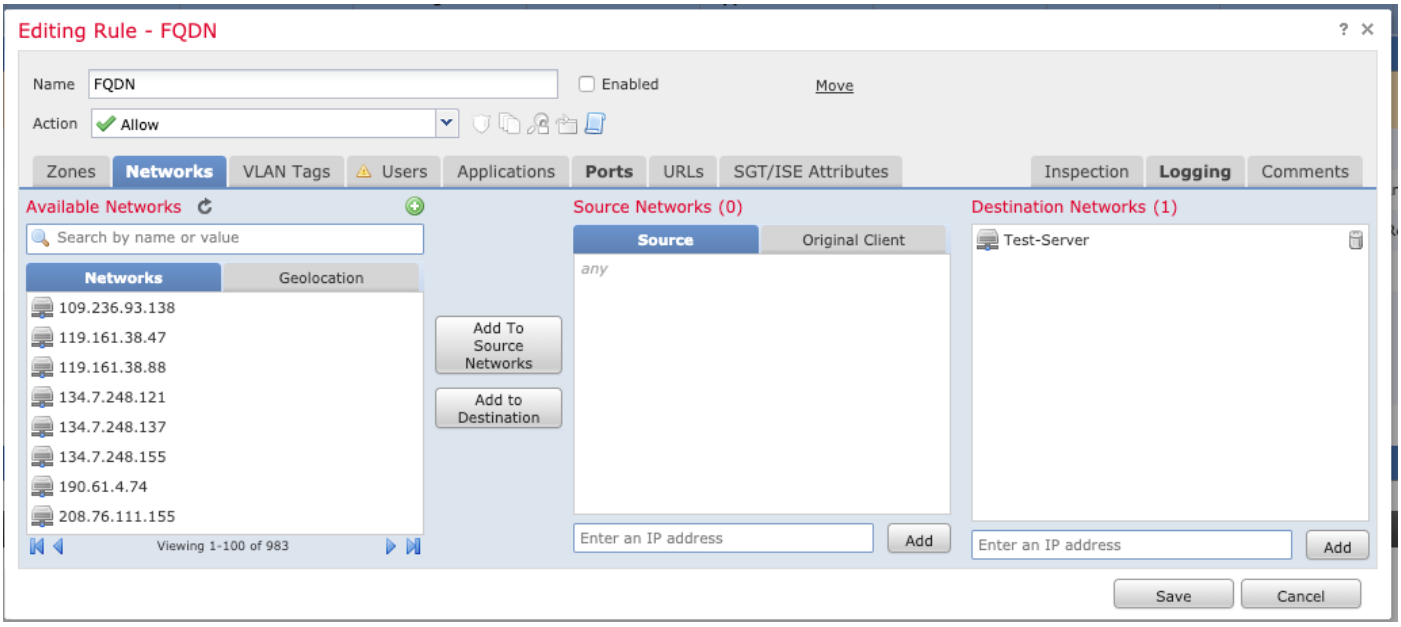
Étape 2. Créez l'objet FQDN, afin de faire cela naviguez jusqu'à **Objets > Gestion des objets > Ajouter un réseau > Ajouter un objet.**

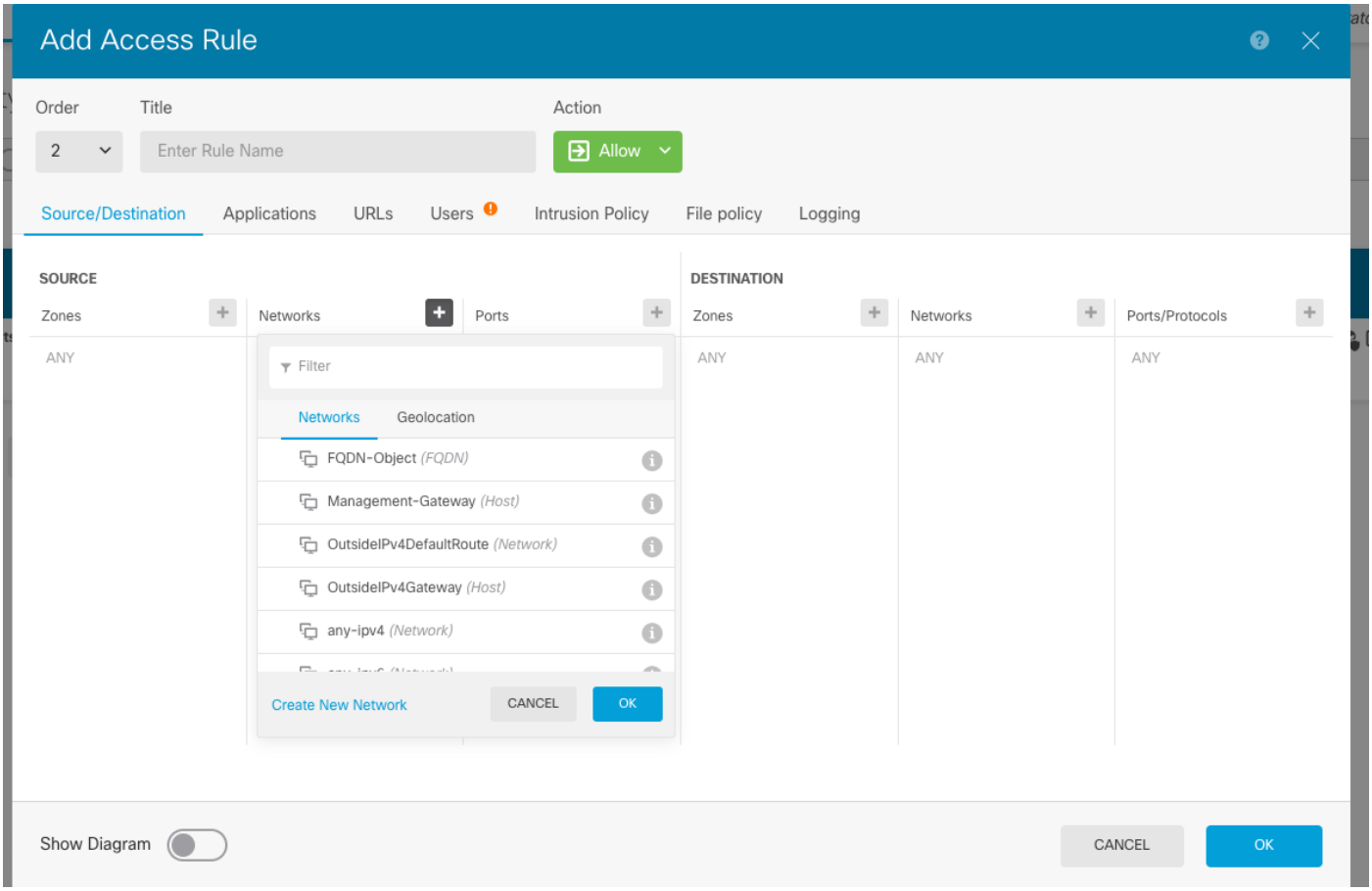

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



Étape 3. Créez une règle de contrôle d'accès en accédant à **Politiques > Contrôle d'accès.**

Note: Vous pouvez créer une règle ou modifier la règle existante en fonction de la condition requise. L'objet FQDN peut être utilisé dans les réseaux source et/ou de destination.



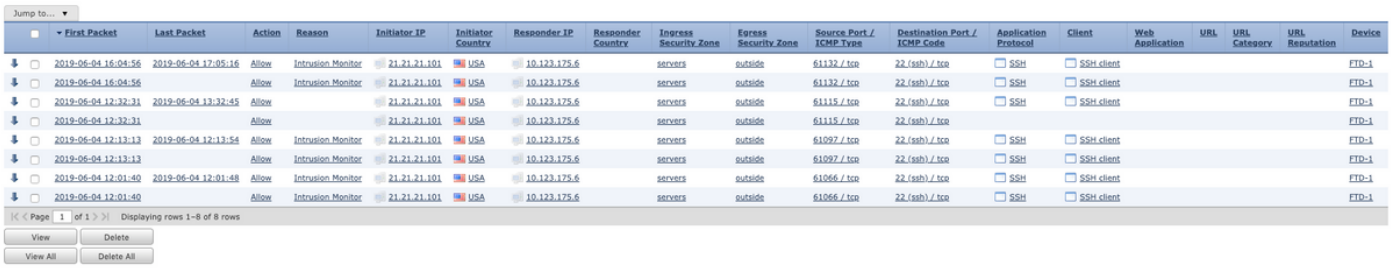


Assurez-vous que la stratégie est appliquée une fois la configuration terminée.

Vérification

Lancez le trafic à partir de la machine cliente qui devrait déclencher la règle basée sur FQDN créée.

Sur le FMC, accédez à **Events > Connection Events, filtrez le trafic spécifique.**



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

Dépannage

Le serveur DNS doit être en mesure de résoudre l'objet FQDN, ceci peut être vérifié à partir de l'interface de ligne de commande exécute la commande suivante :

- **support système diagnostic-cli**
- **show fqdn**

.