

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

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.

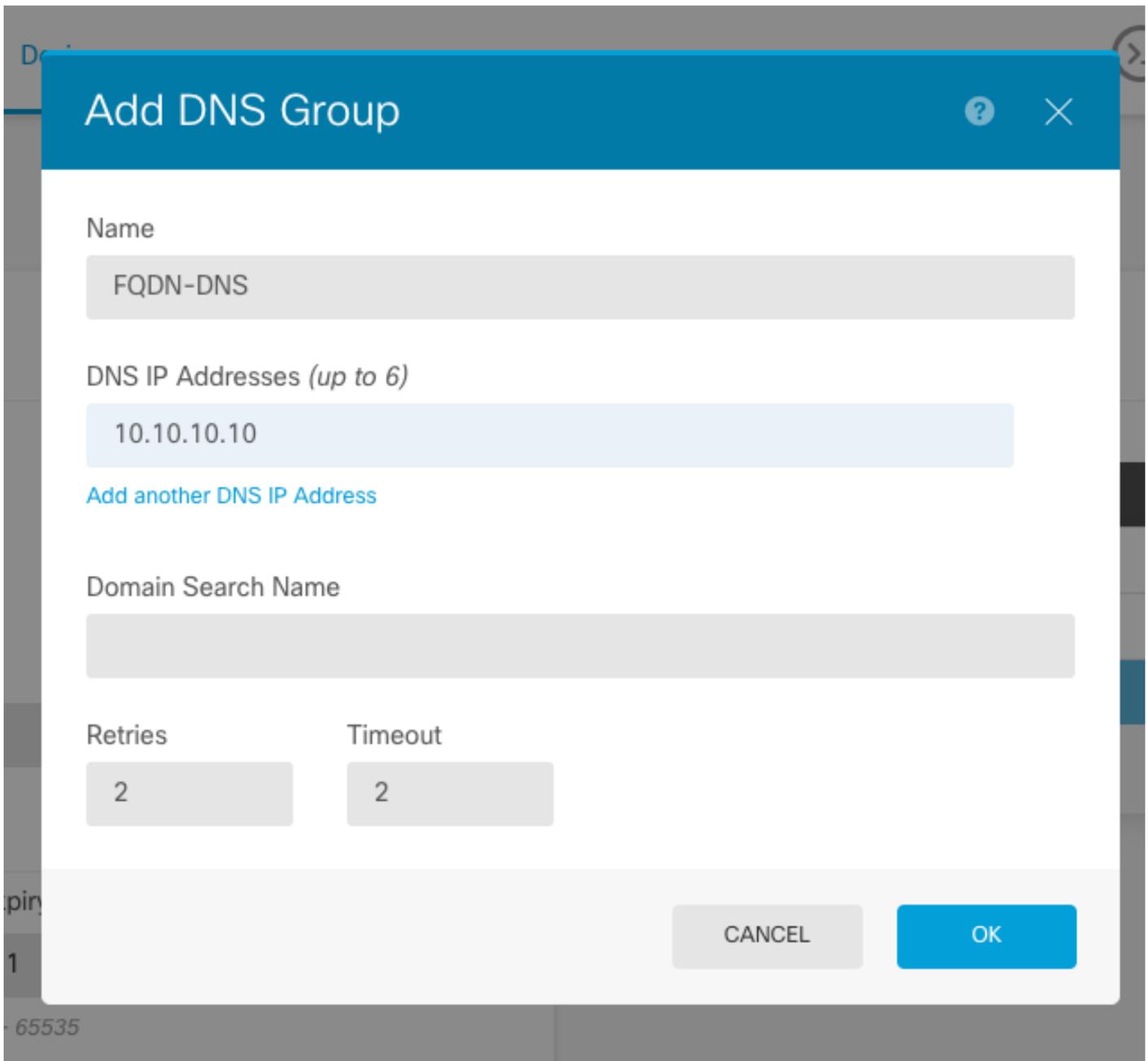
Connectez-vous au FMC et accédez à **Devices > Platform Settings > DNS**.

The screenshot shows the 'DNS Resolution Settings' configuration page. On the left is a navigation menu with 'DNS' selected. The main content area includes:

- DNS Resolution Settings**: Specify DNS servers group and device interfaces to reach them.
- Enable DNS name resolution by device
- DNS Server Group*: (with a refresh icon)
- Expiry Entry Timer: Range: 1-65535 minutes
- Poll Timer: Range: 1-65535 minutes
- Interface Objects**: Devices will use specified interface objects for connecting with DNS Servers.
- Available Interface Objects**: A list of interface objects including ftd-mgmt, inside, inside-nat, labs, outside, outside-nat, postgrad, privileged, research, servers, servers-nat, and staff. A search bar is at the top.
- Selected Interface Objects**: A list containing 'outside' and 'servers'.
- Enable DNS Lookup via diagnostic interface also.

The screenshot shows the 'Configure DNS' configuration page. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device'. The left sidebar shows 'System Settings' with 'DNS Server' selected. The main content area is titled 'Device Summary Configure DNS' and is split into two panels:

- Data Interface**:
 - Interfaces:
 - DNS Group:
 - FQDN DNS SETTINGS**:
 - Poll Time: minutes (range: 1 - 65535)
 - Expiry: minutes (range: 1 - 65535)
 -
- Management Interface**:
 - DNS Group:
 - Dropdown menu: None, CiscoUmbrellaDNSServerGroup, CustomDNSServerGroup (selected)
 -



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

? X

Name	<input type="text" value="Test-Server"/>
Description	<input type="text" value="Test for FQDN"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input type="radio"/> Network <input checked="" type="radio"/> FQDN
	<input type="text" value="test.cisco.com"/>
	Note: You can use FQDN network objects in access and prefilter rules only
Lookup:	<input type="text" value="Resolve within IPv4 and IPv6"/> ▼
Allow Overrides	<input type="checkbox"/>

Save

Cancel

Add Network Object

Name

Description

Type

Network Host FQDN

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

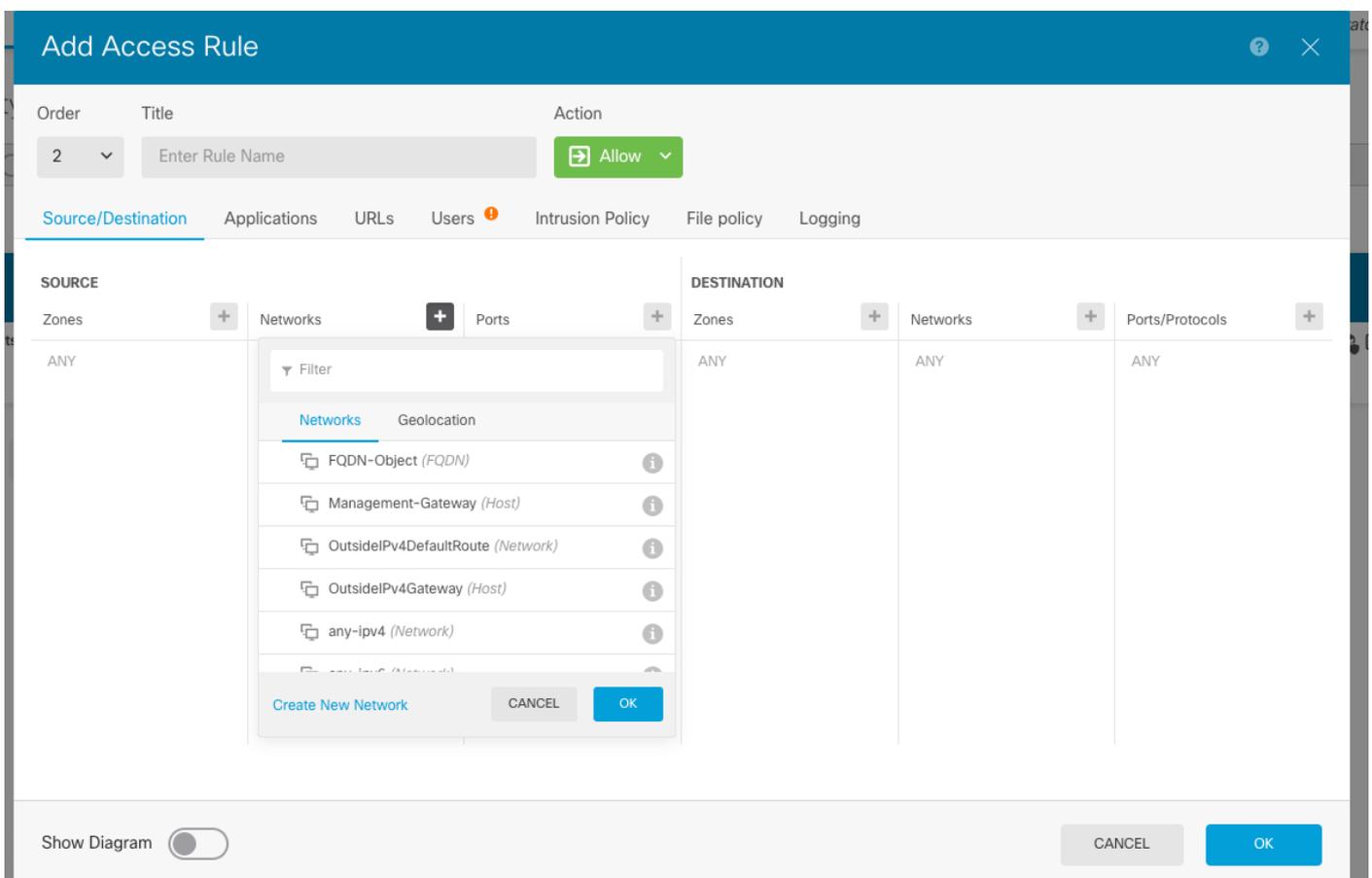
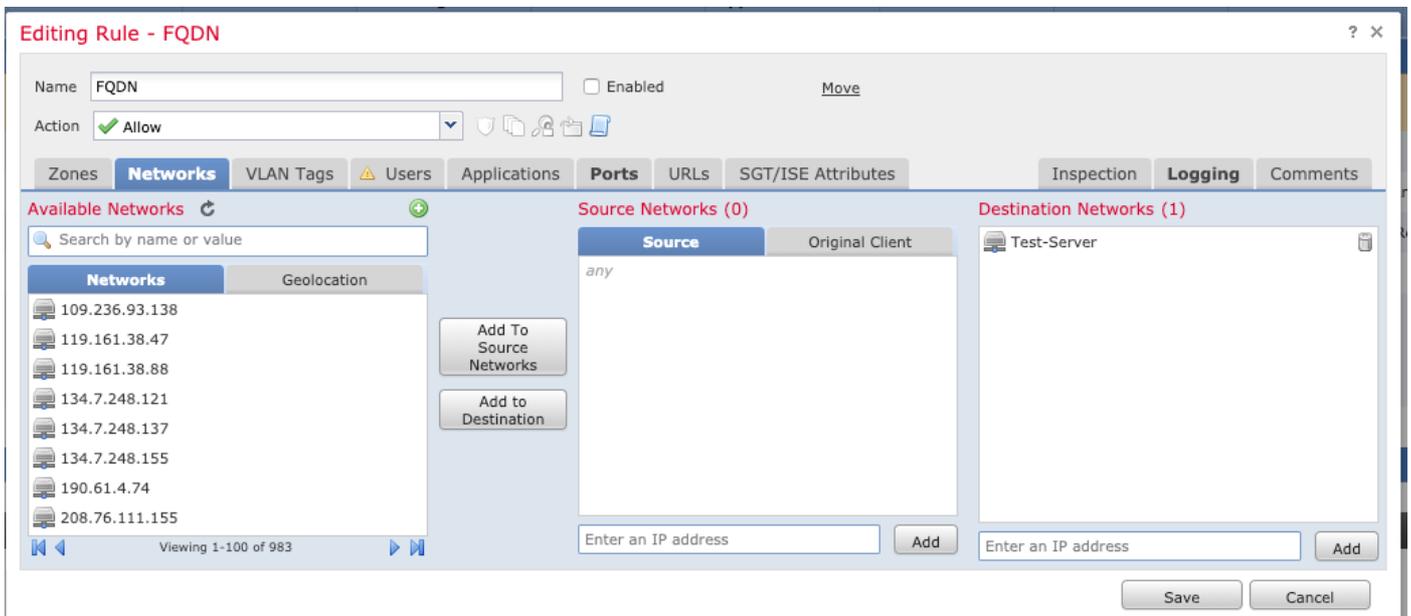
Domain Name

e.g. ad.example.com

DNS Resolution

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.

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	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	Intrusion Monitor	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	2019-06-04 12:32:31	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61115 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:13:13	2019-06-04 12:13:58	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	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	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