

アクセスコントロールルールのFQDNベースオブジェクトの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、ファイアウォール管理センター(FMC)を介した完全修飾ドメイン名(FQDN)オブジェクトの設定と、アクセスルールの作成でFQDNオブジェクトを使用する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識.
- Firesight Management Center(FMC)でのアクセスコントロールポリシーの設定に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン6.3以降を実行しているFirepower Management Center(FMC)。
- バージョン6.3以降を実行するFirepower Threat Defense(FTD)。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップ1:FQDNベースのオブジェクトを設定して使用するには、まずFirepower Threat DefenseでDNSを設定します。

FMCにログインし、[Devices] > [Platform Settings] > [DNS]に移動します。

The screenshot shows the 'DNS Resolution Settings' configuration page in Cisco FMC. 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*: Cisco (with a refresh icon)
- 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**: 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 in Cisco FMC. The page is divided into two main sections:

- Data Interface**:
 - Interfaces: ANY
 - DNS Group: CiscoUmbrellaDNSServerGroup
 - FQDN DNS SETTINGS**:
 - Poll Time: 240 minutes (Range: 1 - 65535)
 - Expiry: 1 minutes (Range: 1 - 65535)
 - SAVE button
- Management Interface**:
 - DNS Group: A dropdown menu is open, showing options: None, CiscoUmbrellaDNSServerGroup, and CustomDNSServerGroup (which is selected).
 - Create DNS Group button

Add DNS Group

Name
FQDN-DNS

DNS IP Addresses (up to 6)
10.10.10.10
[Add another DNS IP Address](#)

Domain Search Name

Retries: 2 Timeout: 2

CANCEL OK

注：DNSの設定後、システムポリシーがFTDに適用されていることを確認します（設定されたDNSサーバが、使用されるFQDNを解決する必要があります）。

ステップ2:FQDNオブジェクトを作成します。作成するには、[Objects] > [Object Management] > [Add Network] > [Add Object]に移動します。

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.

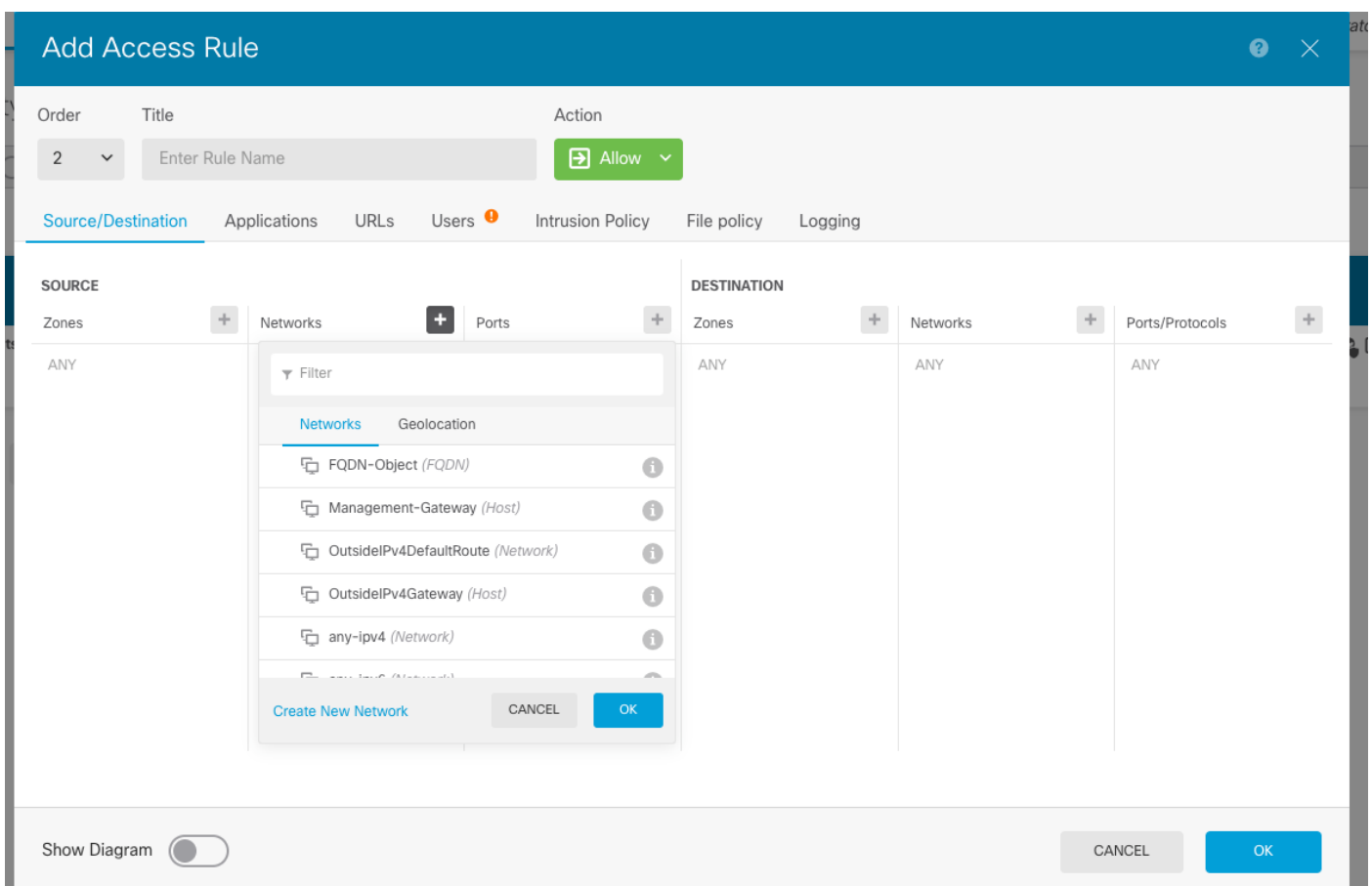
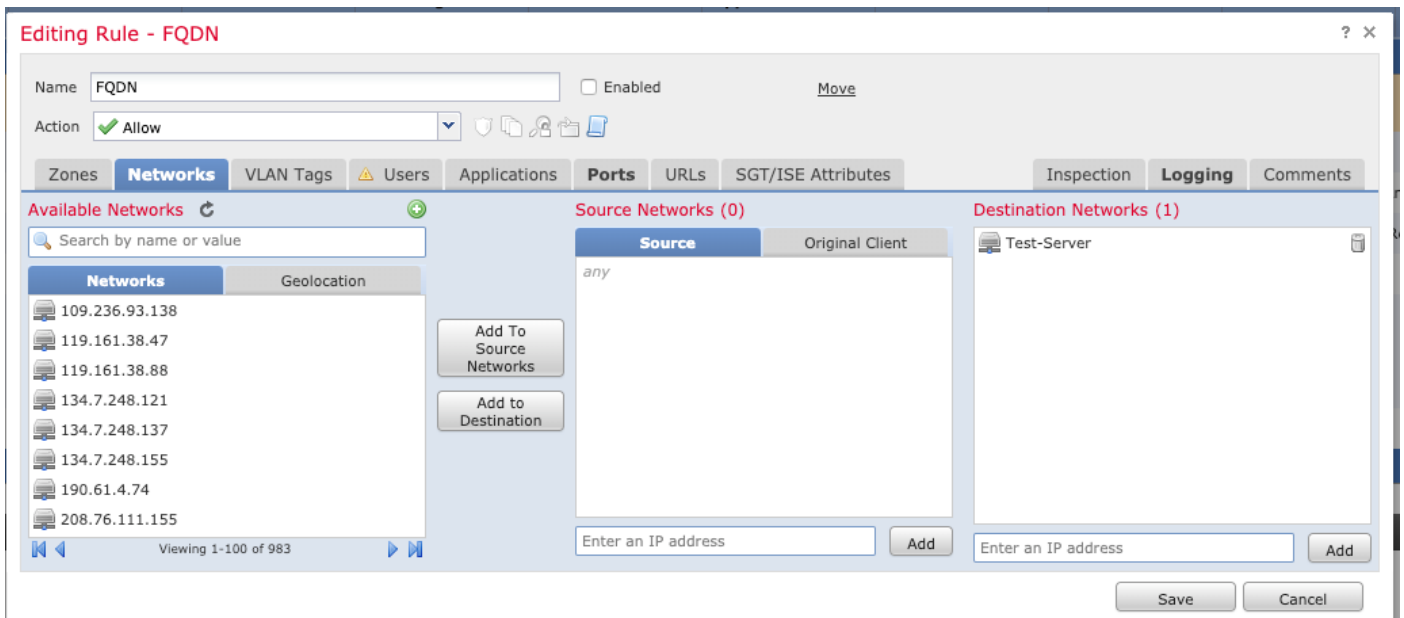
Domain Name

e.g. ad.example.com

DNS Resolution

ステップ3:[Policies] > [Access Control]の順に移動して、アクセスコントロールルールを作成します。

注：ルールを作成するか、要件に基づいて既存のルールを変更できます。FQDNオブジェクトは、送信元または宛先ネットワークで使用できます。



設定が完了したら、ポリシーが適用されていることを確認します。

確認

作成されたFQDNベースのルールをトリガーすると予想されるクライアントマシンからトラフィックを開始します。

FMCで、[Events] > [Connection Events]に移動し、特定のトラフィックをフィルタします。

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

トラブルシューティング

DNSサーバはFQDNオブジェクトを解決できる必要があります。これは、CLIから次のコマンドを実行して確認できます。

- `system support diagnostic-cli`
- `show fqdn`