

アクセスコントロール ルールのための設定 FQDN によって基づくオブジェクト

目次

[はじめに](#)

[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

この資料はファイアウォール管理センター (FMC) によって完全修飾ドメイン名 (FQDN) オブジェクトの設定をおよびアクセス規則作成で FQDN オブジェクトを使用する方法を説明したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- Firepower テクノロジーのナレッジ。
- 設定のナレッジ Firesight 管理センター (FMC) のアクセスコントロール ポリシーの

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くものです。

- バージョン 6.3 および それ 以上を実行する Firepower Management Center。
- バージョン 6.3 および それ 以上を実行する Firepower Threat Defense。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

設定

ステップ 1. FQDN によって基づくオブジェクトを、第 1 は使用するために設定し、Firepower Threat Defense の DNS を設定します。

FMC にログインし、デバイス > プラットフォーム設定 > DNS にナビゲートして下さい。

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*: Cisco (dropdown menu)
- Expiry Entry Timer: 1 (input field) Range: 1-65535 minutes
- Poll Timer: 240 (input field) 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.
- Selected Interface Objects**: A list containing 'outside' and 'servers'.
- Enable DNS Lookup via diagnostic interface also.

The screenshot shows the 'Configure DNS' page in the Cisco FMC interface. The left sidebar contains 'System Settings' and 'Traffic Settings' sections. The main content area is titled 'Device Summary Configure DNS' and is divided into two panels:

- Data Interface**:
 - Interfaces: ANY
 - DNS Group: CiscoUmbrellaDNSServerGroup (dropdown menu)
 - FQDN DNS SETTINGS**:
 - Poll Time: 240 minutes (range 1-65535)
 - Expiry: 1 minutes (range 1-65535)
 - SAVE button
- Management Interface**:
 - DNS Group: Filter dropdown menu showing 'None', 'CiscoUmbrellaDNSServerGroup', and 'CustomDNSServerGroup' (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: システム ポリシーが FTD に DNS をことを設定した後適用されるようにして下さい。
(設定される DNSサーバは FQDN を使用する解決する必要があります)

ステップ 2. オブジェクト > オブジェクト 管理 > Add Network > Add オブジェクトにことナビゲートするために FQDN オブジェクトを、作成して下さい。

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

FQDN

Description

Type

Network Host FQDN



Note:

You can use FQDN network objects in access rules only.

Domain Name

test.cisco.com

e.g. ad.example.com

DNS Resolution

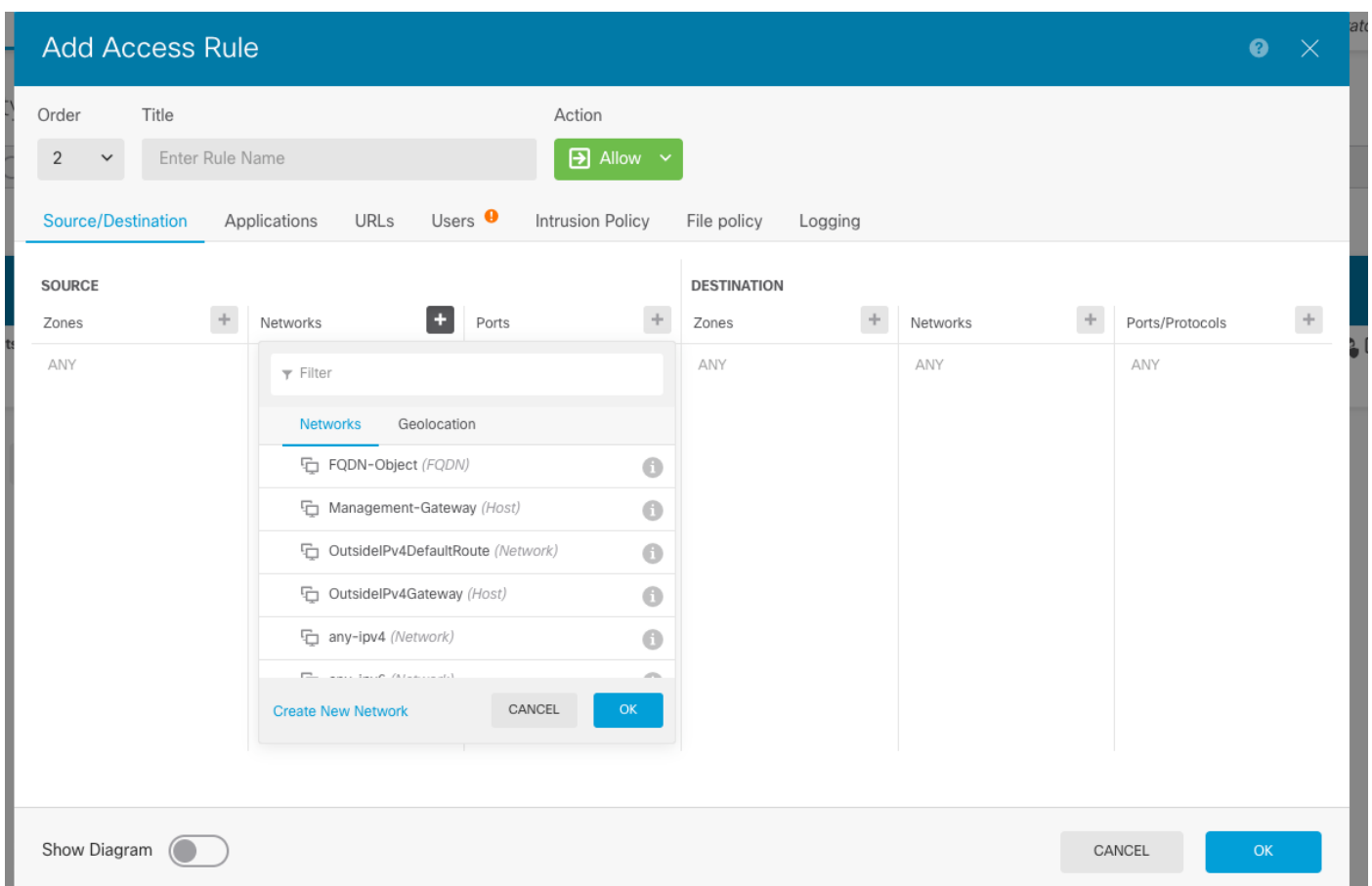
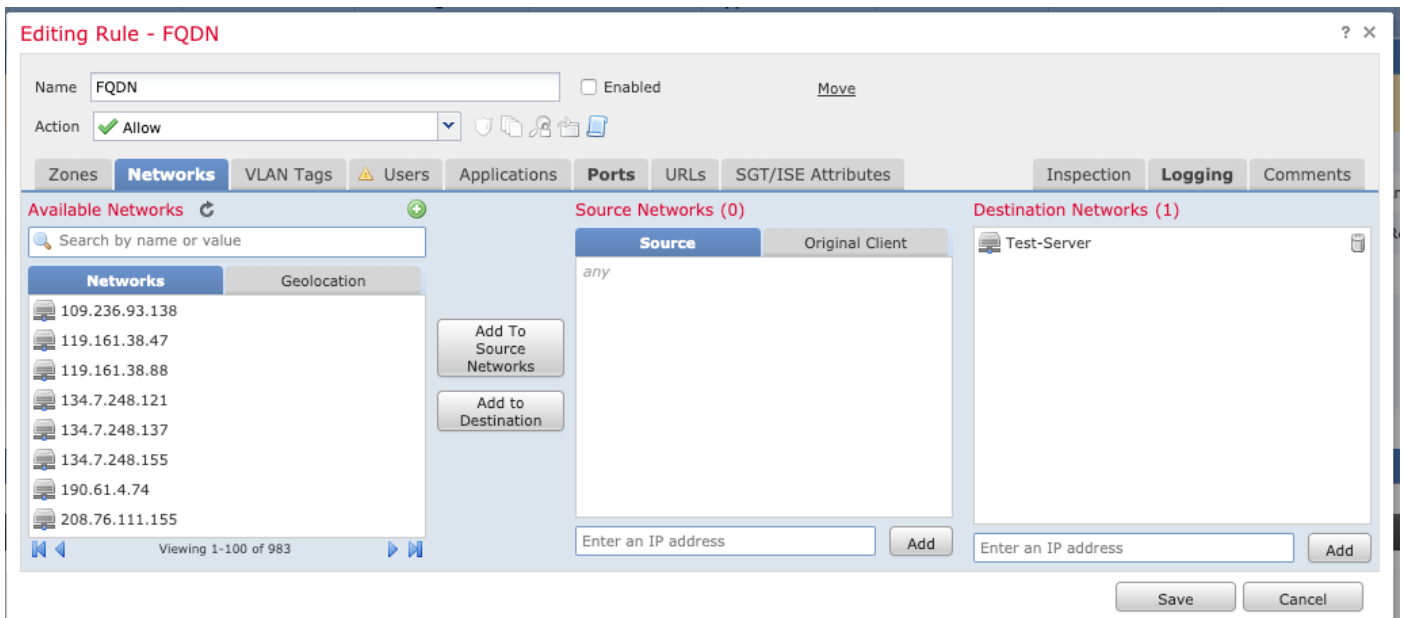
IPv4 and IPv6

CANCEL

OK

ステップ 3. ポリシー > アクセスコントロールへのナビゲートによってアクセスコントロール ルールを作成して下さい。

注: ルールを作成するか、または要件に基づいて既存のルールを修正できます。 FQDN オブジェクトは出典や宛先ネットワークで使用することができます。



設定が完了した後ポリシーが適用することを確認して下さい。

確認

作成される FQDN によって基づくルールを引き起こすと期待されるクライアントマシンからのトラフィックを初期化して下さい。

FMC で、特定のトラフィックのためのフィルタはイベント > 接続イベントにナビゲートします

。

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 CLI から FQDN オブジェクトを解決これ確認することができます実行しますこれらのコマンドをできるはずです:

- システム 支援診断 cli
 - fqdn を示して下さい
- を探します。