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

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。

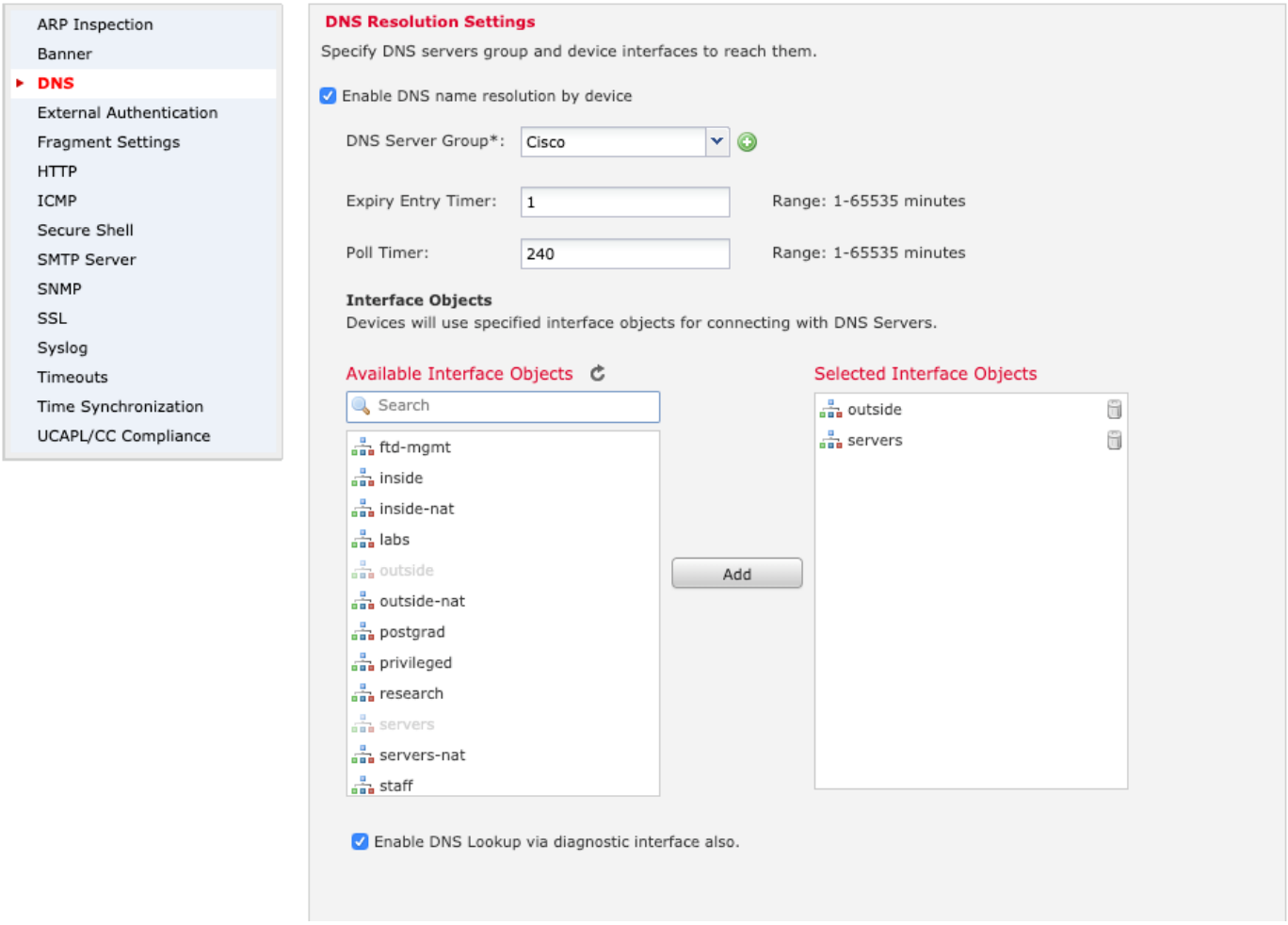
- バージョン6.3以降を実行しているFirepower Management Center(FMC)。
- バージョン6.3以降を実行するFirepower Threat Defense(FTD)。

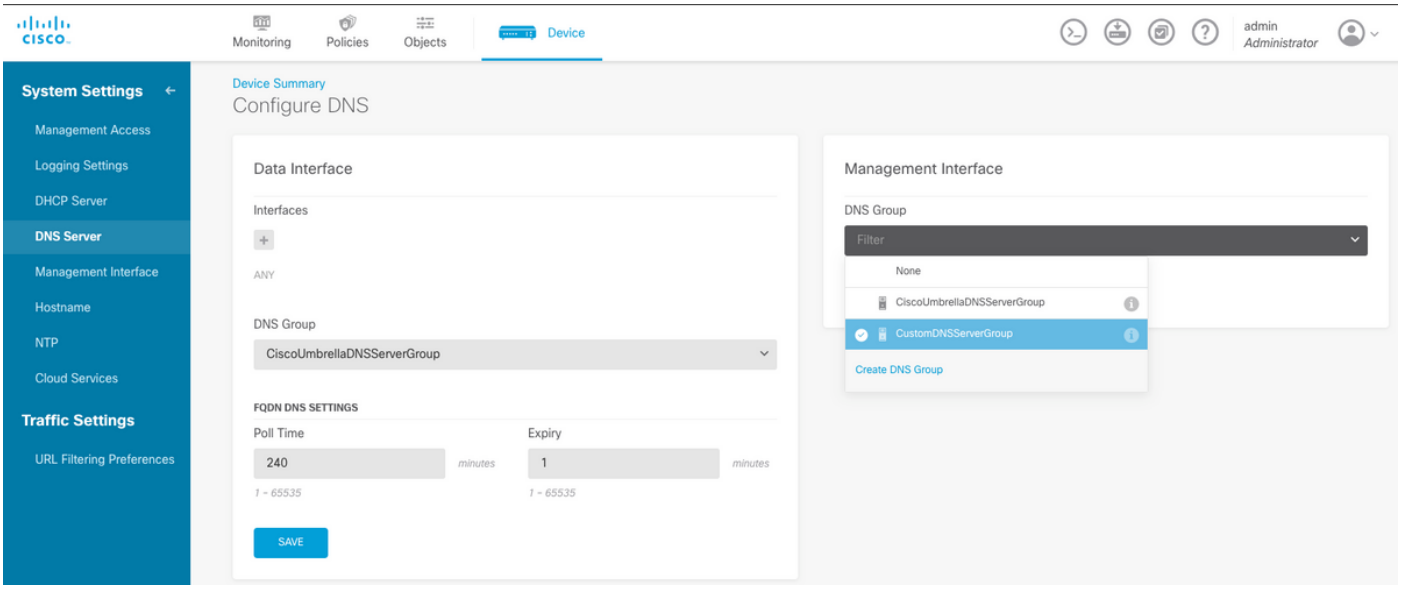
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

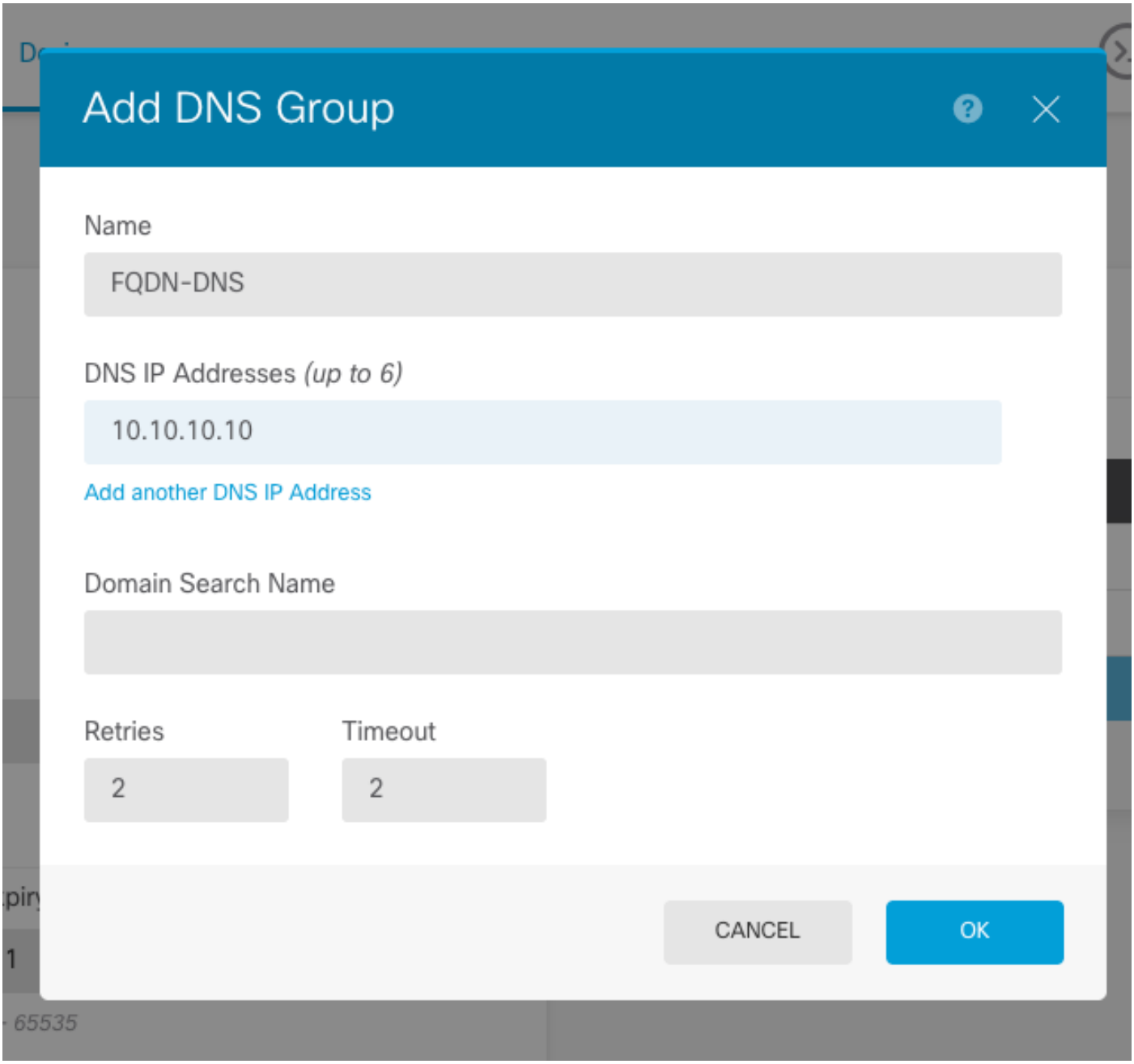
設定

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。

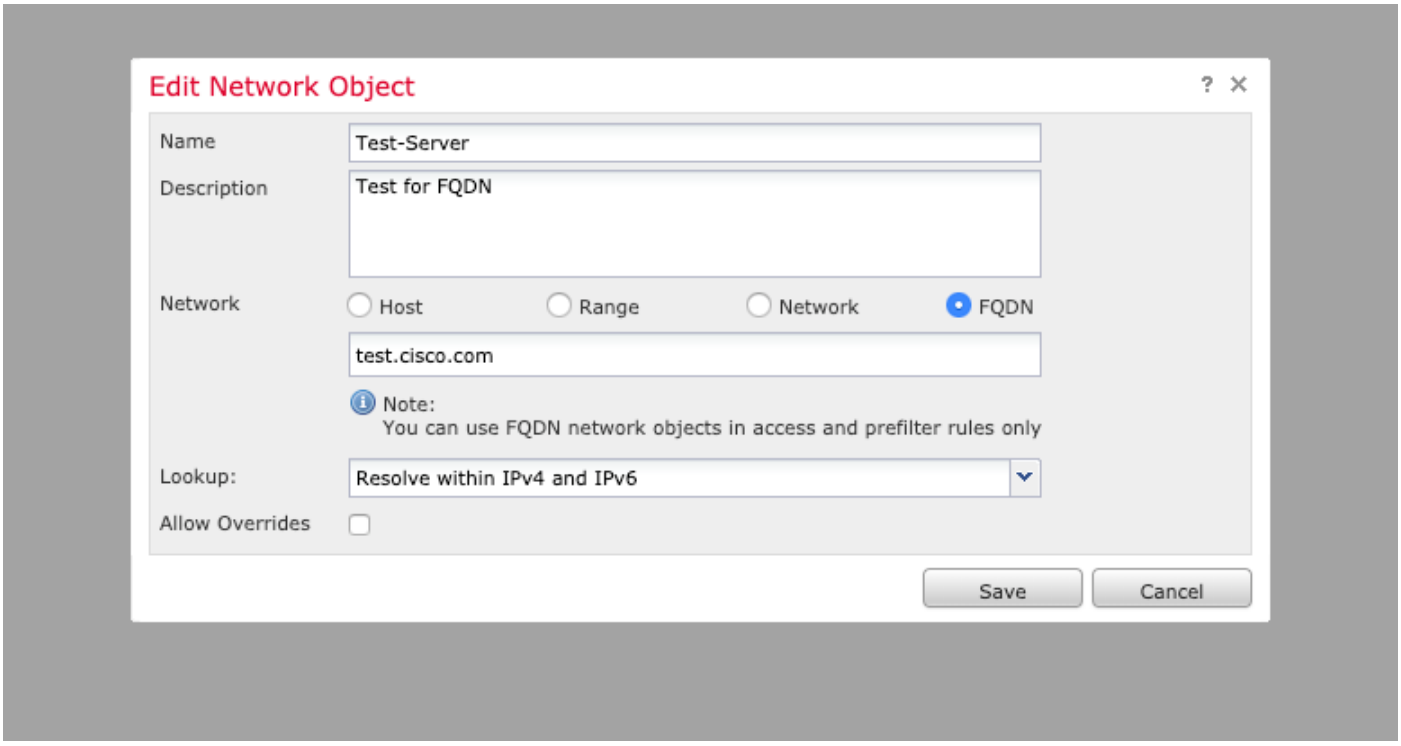


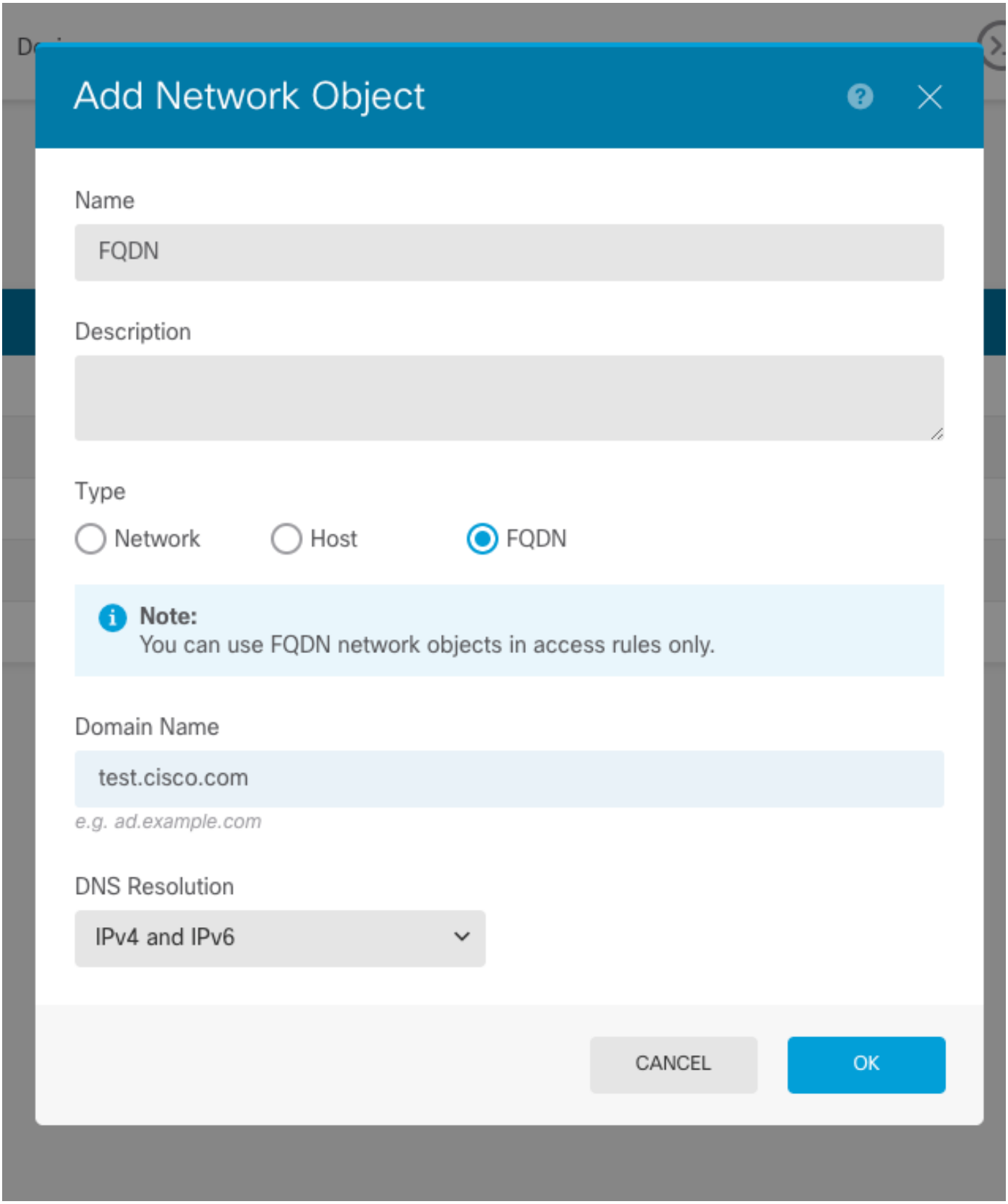




注：DNSの設定後、システムポリシーがFTDに適用されていることを確認します（設定されたDNSサーバが、使用されるFQDNを解決する必要があります）。

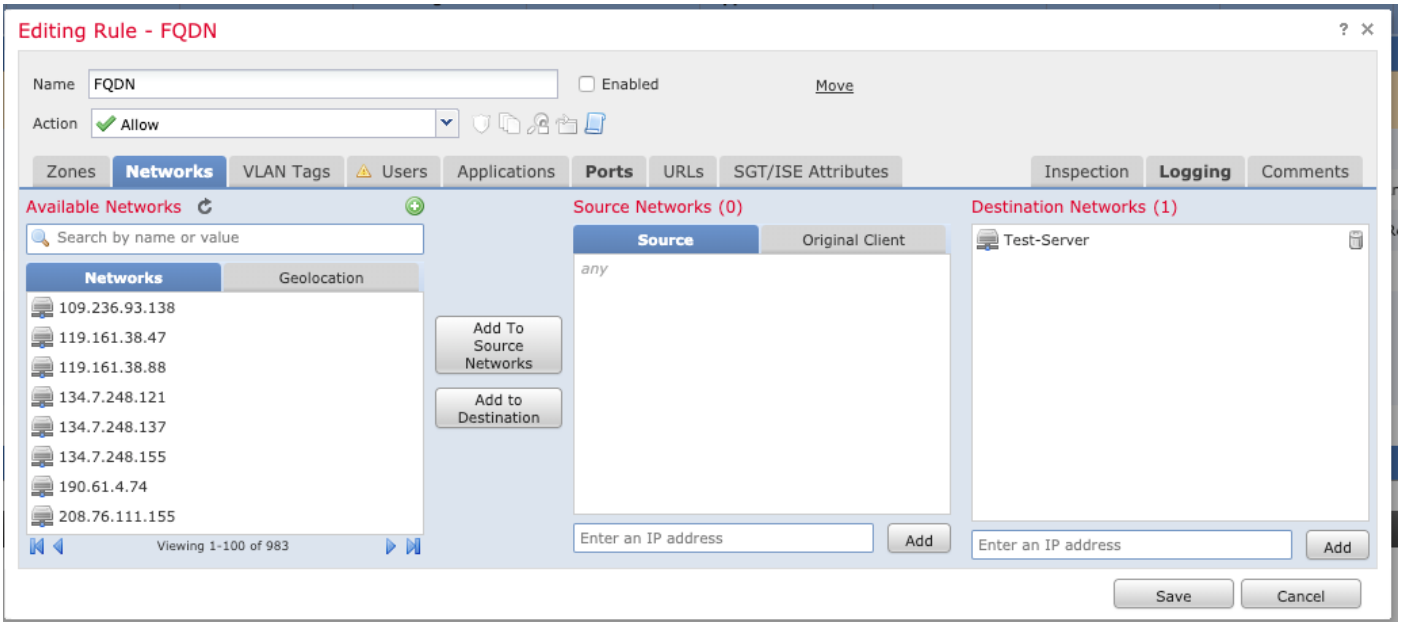
ステップ2:FQDNオブジェクトを作成します。作成するには、**[Objects] > [Object Management] > [Add Network] > [Add Object]に移動します。**

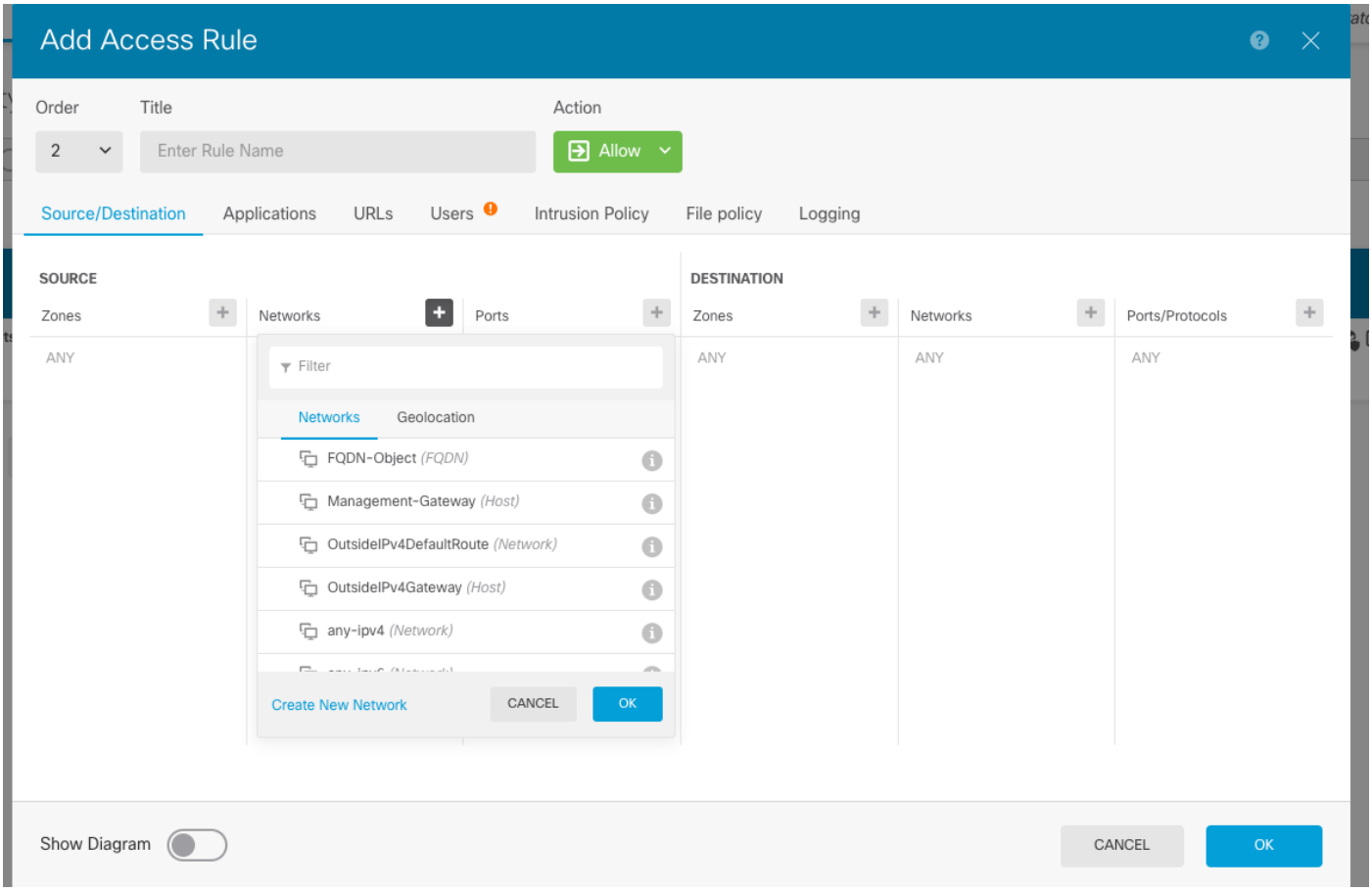

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



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。



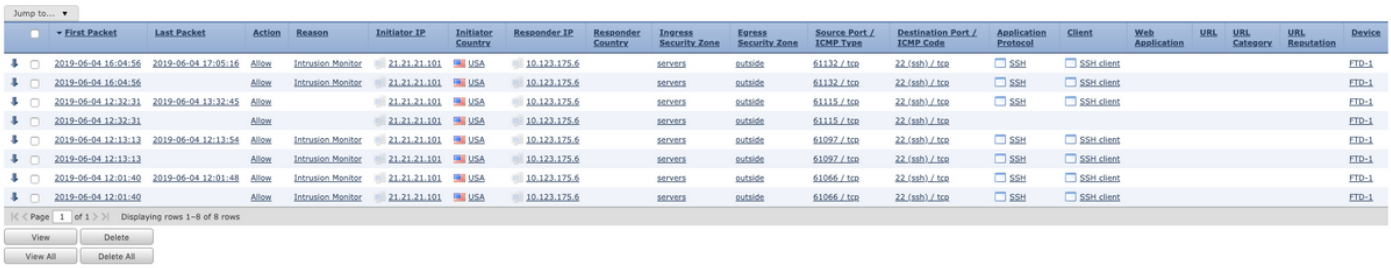


設定が完了したら、ポリシーが適用されていることを確認します。

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。**



トラブルシュート

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

.