Konfigurieren des FQDN-basierten Objekts für Zugriffskontrollregeln

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration des Fully Qualified Domain Name (FQDN)-Objekts über das Firewall Management Center (FMC) und die Verwendung des FQDN-Objekts bei der Erstellung von Zugriffsregeln.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der FirePOWER-Technologie
- Kenntnisse der Konfiguration der Zugriffskontrollrichtlinie für das FireSIGHT Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- FirePOWER Management Center mit Version 6.3 und höher
- Firepower Threat Defense mit Version 6.3 und höher

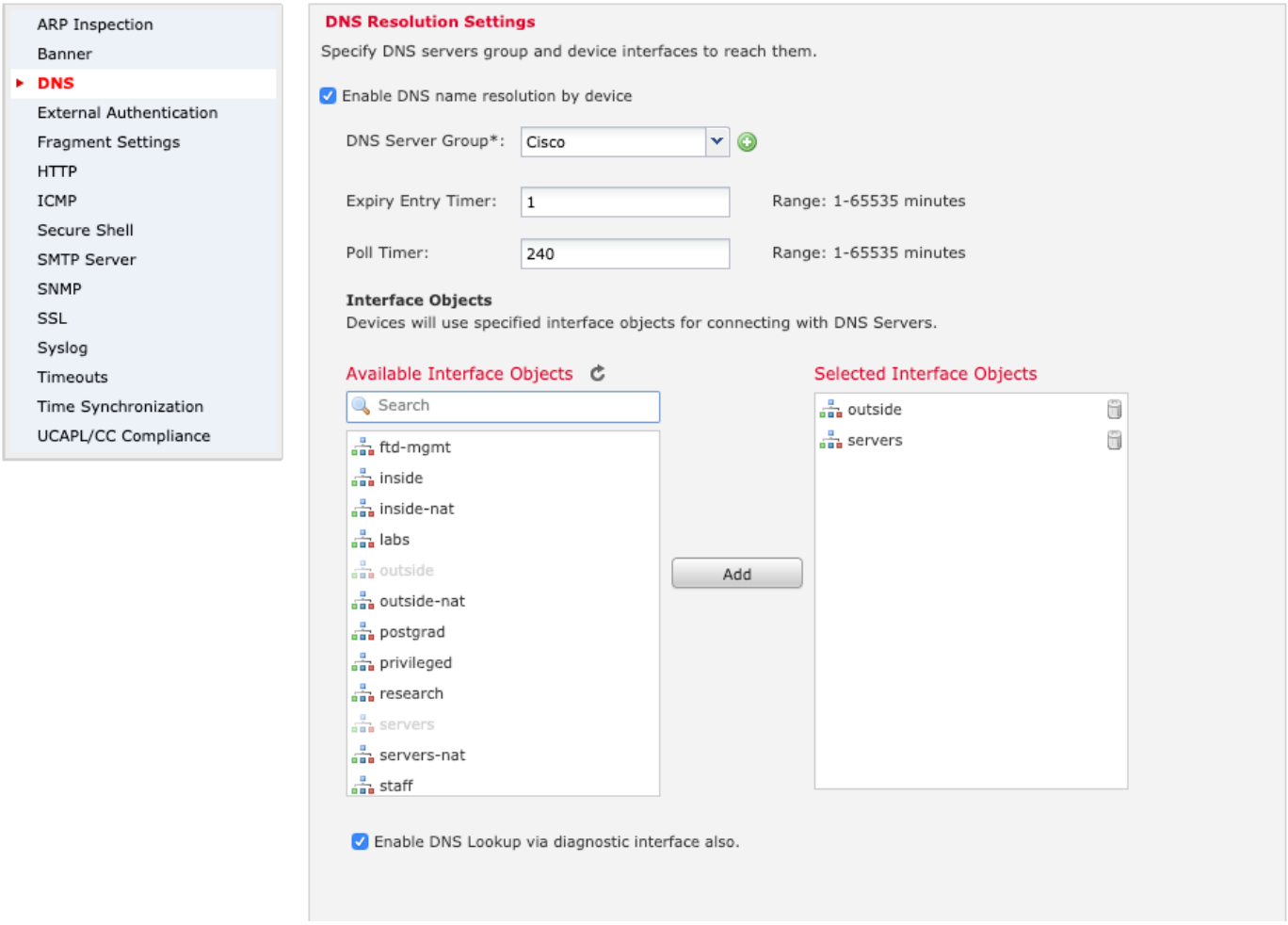
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

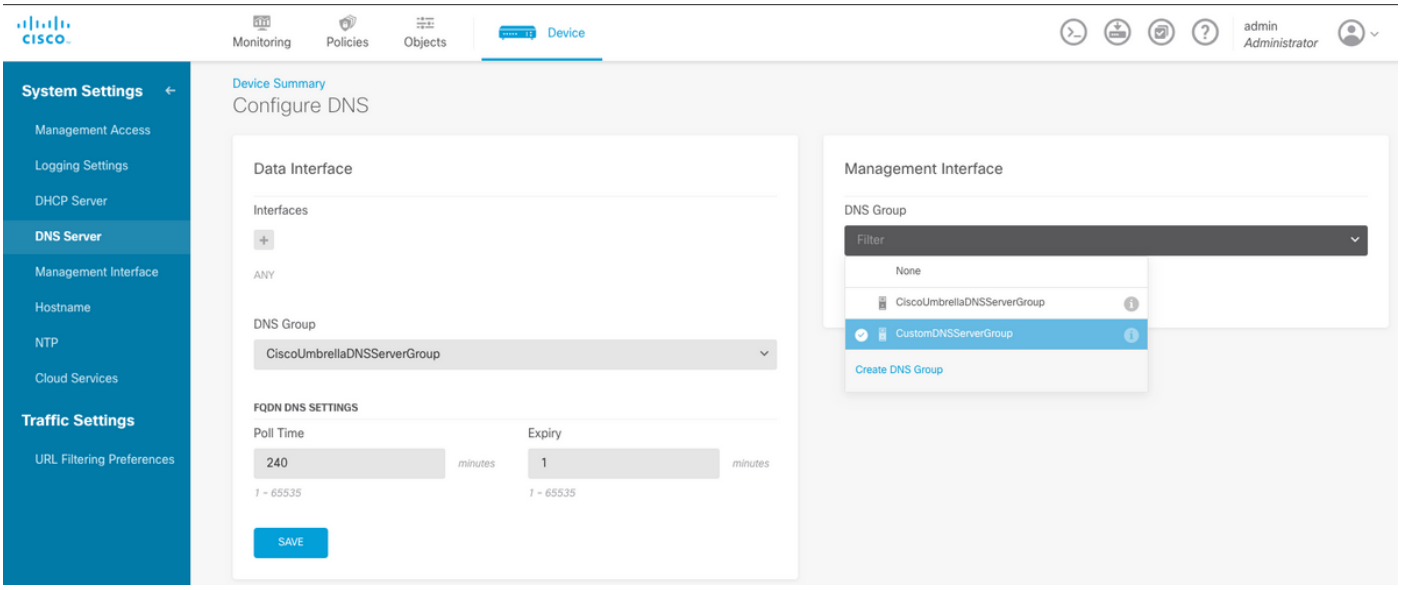
Konfigurieren

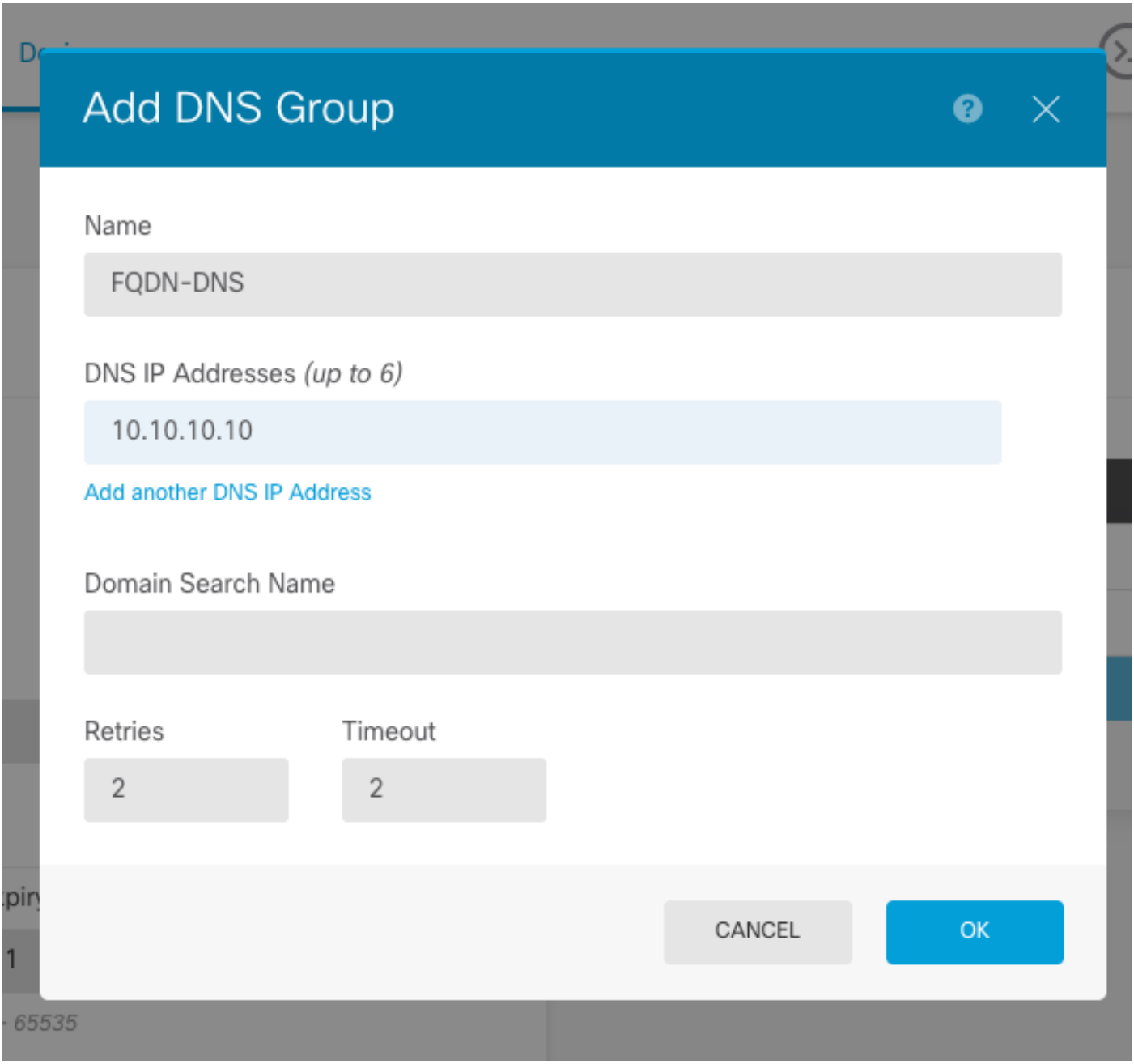
Schritt 1: Um ein FQDN-basiertes Objekt zu konfigurieren und zu verwenden, konfigurieren Sie

zunächst DNS in FirePOWER Threat Defense.

Melden Sie sich beim FMC an, und navigieren Sie zu **Devices > Platform Settings > DNS**.

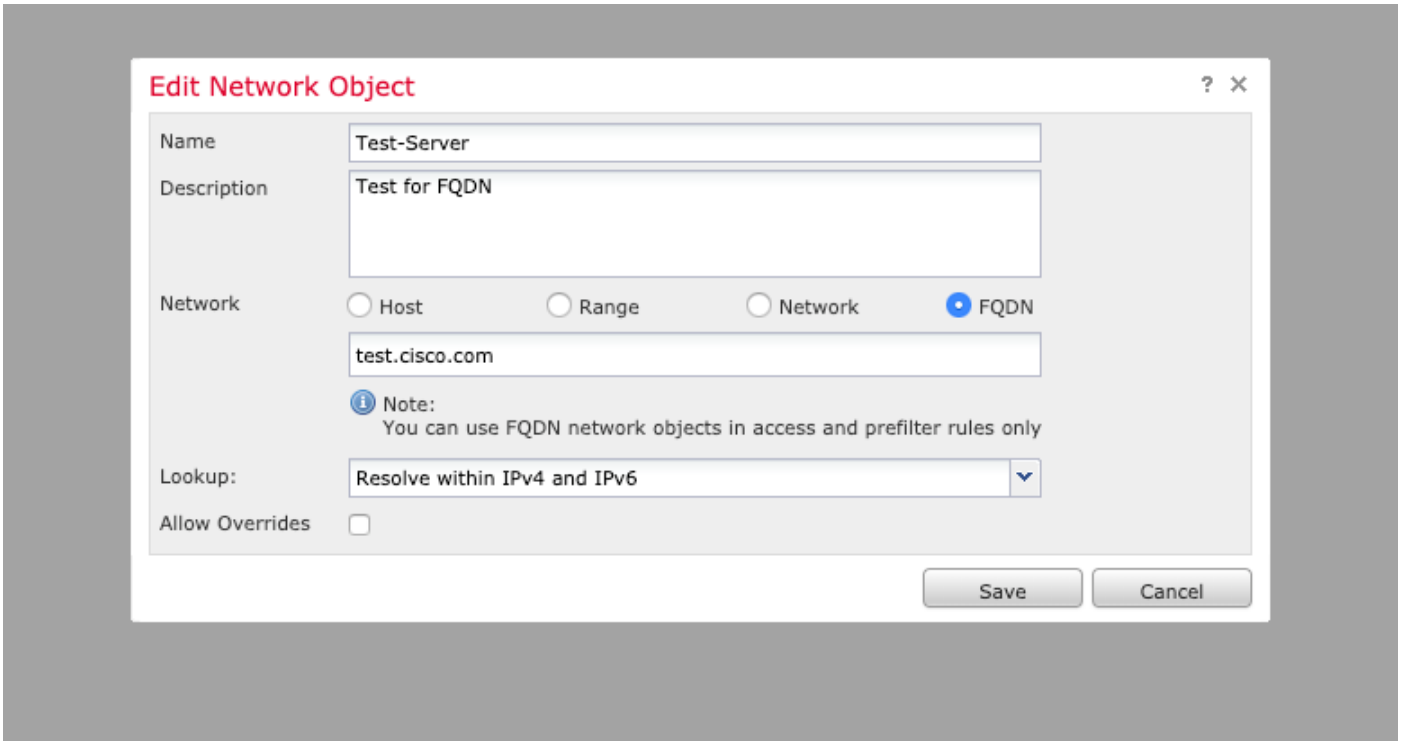


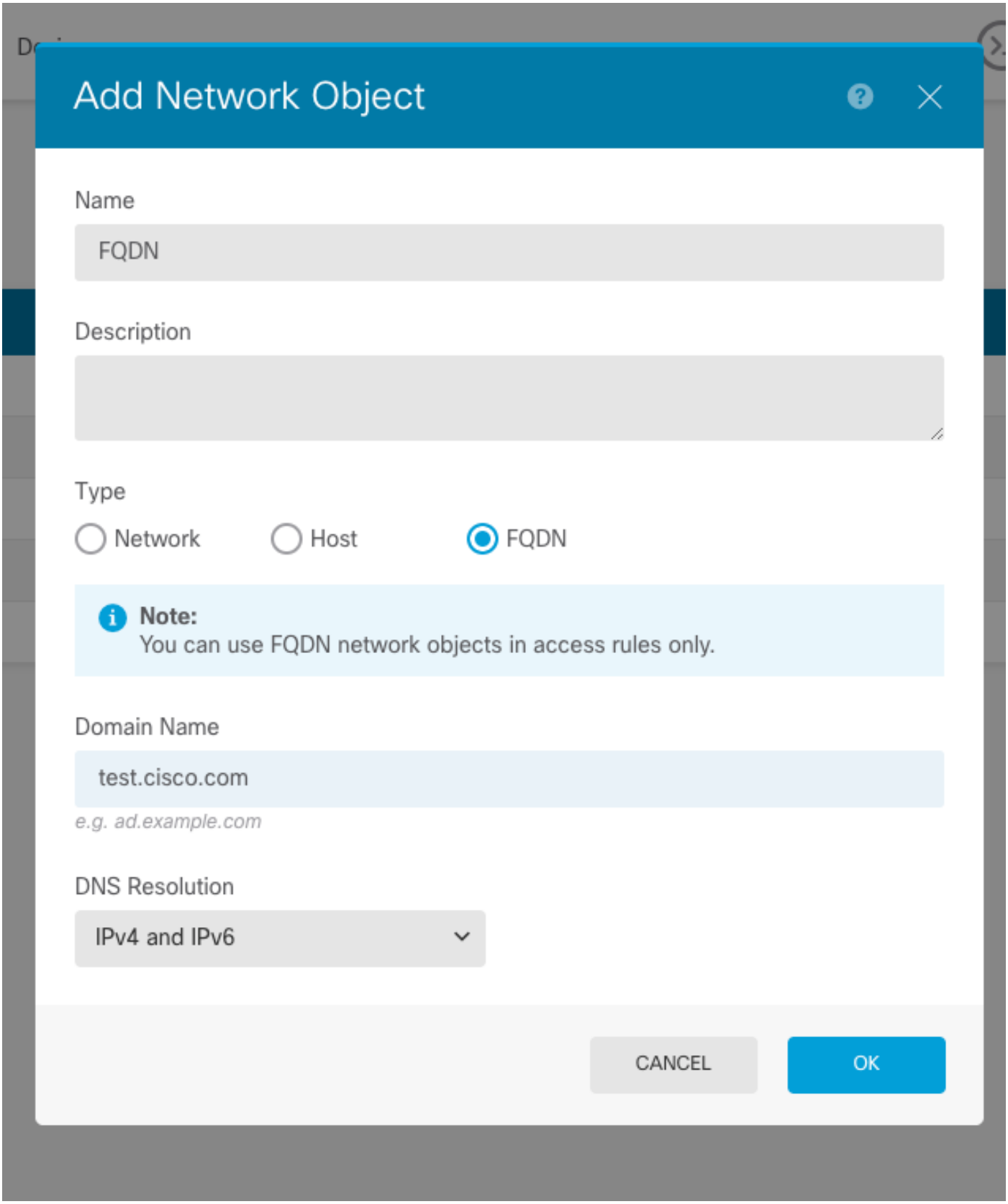




Hinweis: Stellen Sie sicher, dass die Systemrichtlinie nach der Konfiguration des DNS auf die FTD angewendet wird. (Der konfigurierte DNS-Server sollte den verwendeten FQDN auflösen.)

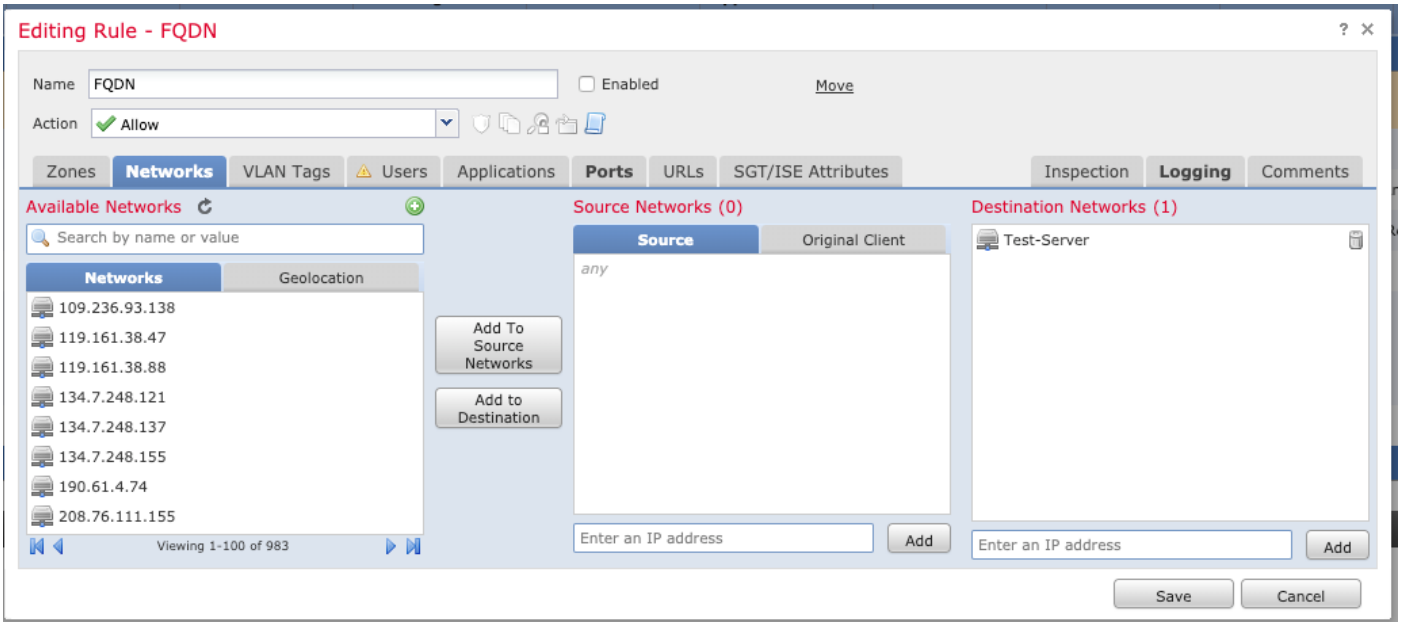
Schritt 2: Erstellen Sie dazu das FQDN-Objekt, indem Sie zu **Objekte > Objektverwaltung > Netzwerk hinzufügen > Objekt hinzufügen** navigieren.

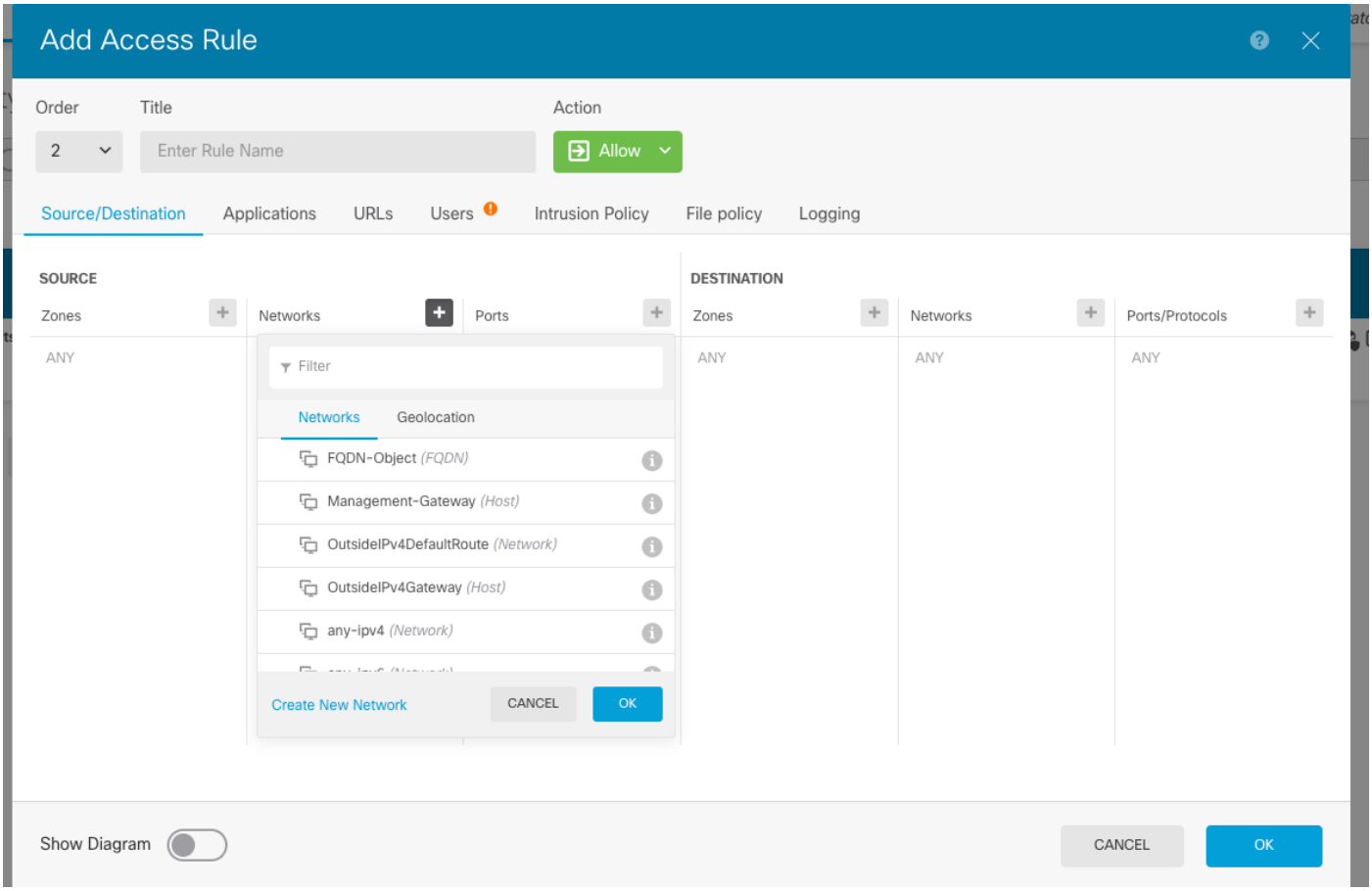

Edit Network Object
Name
Test-Server
Description
Test for FQDN
Network
Host
Range
Network
FQDN
test.cisco.com
Note:
You can use FQDN network objects in access and prefilter rules only
Lookup:
Resolve within IPv4 and IPv6
Allow Overrides
Save
Cancel



Schritt 3: Erstellen Sie eine Zugriffskontrollregel, indem Sie zu **Richtlinien > Zugriffskontrolle** navigieren.

Hinweis: Sie können eine Regel erstellen oder die vorhandene Regel entsprechend der Anforderung ändern. Das FQDN-Objekt kann entweder in Quell- und/oder Zielnetzwerken verwendet werden.



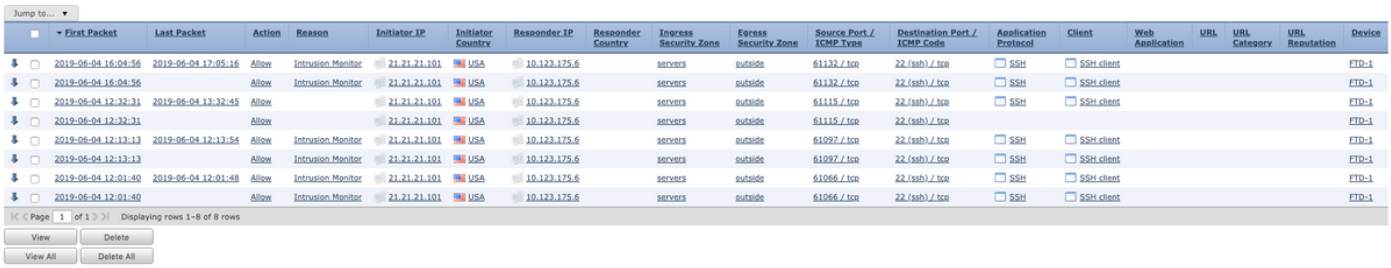


Stellen Sie sicher, dass die Richtlinie nach Abschluss der Konfiguration angewendet wird.

Überprüfen

Initiieren Sie Datenverkehr vom Client-Computer, der die erstellte FQDN-basierte Regel auslösen soll.

Navigieren Sie im FMC zu **Events > Connection Events (Ereignisse > Verbindungsereignisse), und filtern Sie nach dem spezifischen Datenverkehr.**



Fehlerbehebung

Der DNS-Server sollte in der Lage sein, das FQDN-Objekt aufzulösen. Dies kann über die CLI überprüft werden, die diesen Befehl ausführt:

- **Systemunterstützung für Diagnose-CLI**
- **show fqdn**

.