

FQD-gebaseerde object voor toegangscontroleregel configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de configuratie van het Fully Qualified Domain Name (FQDN)-object via het Firewallbeheercentrum (FMC) en de manier waarop u FQDN-object moet gebruiken in de creatie van de toegangsregel.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER-technologie.
- Kennis van het configureren van toegangsbeheerbeleid voor FireSIGHT Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center met versie 6.3 en hoger.
- Firepower Threat Defense met versie 6.3 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap 1. Om op FQDN gebaseerd object te configureren en te gebruiken, moet u eerst DNS op de Firepower Threat Defense configureren.

Meld u aan bij het FMC en navigeer naar **Apparaten > Platform Instellingen > 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' page in the Cisco FMC interface. 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' and 'Configure DNS'. It is divided into two sections:

- 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 showing: None, CiscoUmbrellaDNSServerGroup, **CustomDNSServerGroup** (selected), and Create DNS Group.

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

Opmerking: Zorg ervoor dat het systeembeleid op de FTD wordt toegepast nadat u de DNS hebt geconfigureerd. (De DNS-server moet de FQDN-oplossing oplossen die wordt gebruikt)

Stap 2. Maak het FQDN-object, om dat te doen door te **sturen naar objecten > Objectbeheer > Add Network > Add Object**.

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

Do...

Add Network Object

Name

FQDN

Description

Type

Network Host FQDN

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

Domain Name

test.cisco.com

e.g. ad.example.com

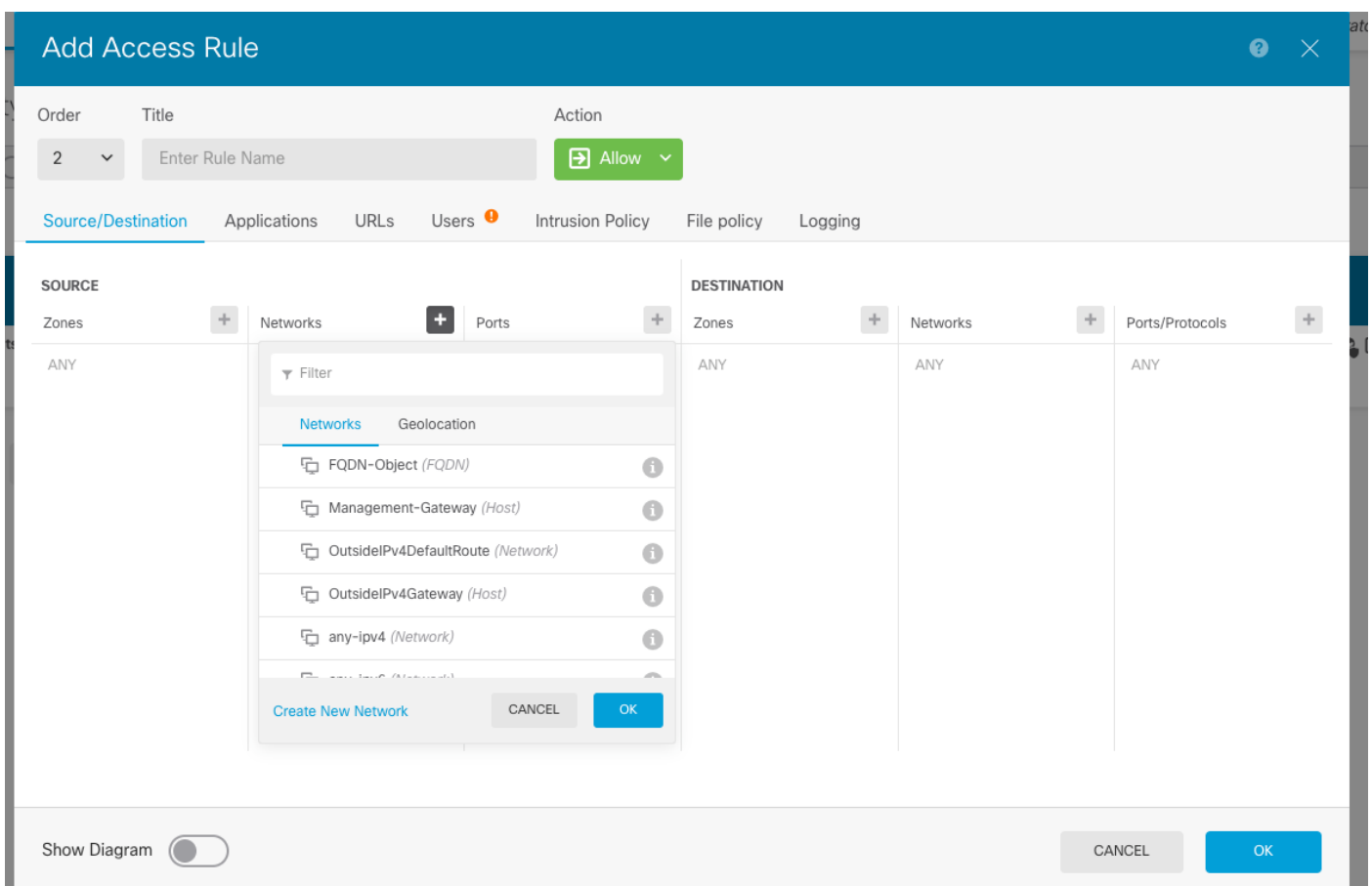
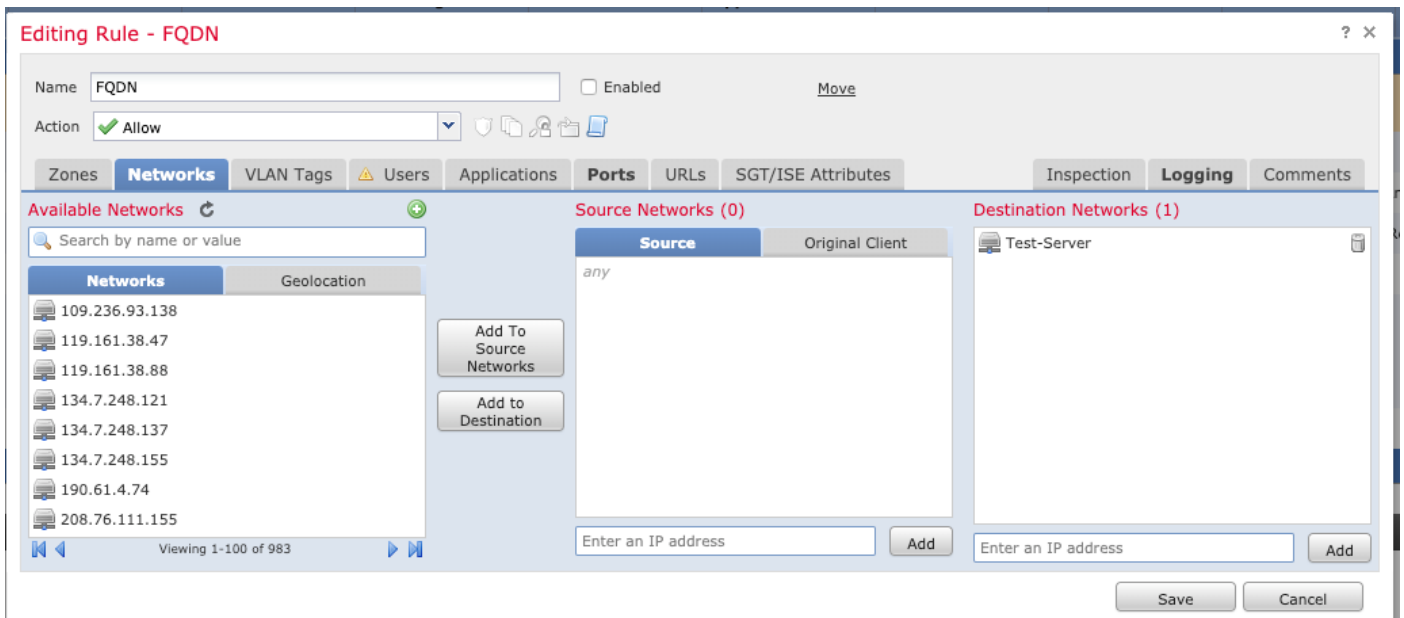
DNS Resolution

IPv4 and IPv6

CANCEL OK

Stap 3. Maak een toegangscontroleregel door naar **beleid > Toegangsbeheer** te navigeren.

Opmerking: U kunt een regel maken of de bestaande regel wijzigen op basis van de vereiste. Het FQDN-object kan in bron- en/of doelnetwerken worden gebruikt.



Zorg ervoor dat het beleid wordt toegepast nadat de configuratie is voltooid.

Verifiëren

Initieer verkeer vanaf de clientmachine, wat naar verwachting de op FQDN gebaseerde regel zal activeren.

Op het VCC, navigeer aan **Gebeurtenissen > gebeurtenis**, filter voor het specifieke verkeer.

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

Problemen oplossen

De DNS server zou het FQDN object moeten kunnen oplossen, dit kan worden geverifyerd vanuit de CLI-instelling die deze opdracht uitvoert:

- systeemondersteuning voor diagnostische cli
- tonen fqdn