

Configurar objeto baseado em FQDN para regra de controle de acesso

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve a configuração do objeto Nome de domínio totalmente qualificado (FQDN) através do Centro de gerenciamento de firewall (FMC) e como usar o objeto FQDN na criação da regra de acesso.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower.
- Conhecimento da configuração da política de controle de acesso no Firesight Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center executando a versão 6.3 e superior.
- Firepower Threat Defense executando a versão 6.3 e superior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa 1. Para configurar e usar um objeto baseado em FQDN, primeiro configure o DNS no Firepower Threat Defense.

Faça login no FMC e navegue até **Devices > Platform Settings > 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:
 - Filter dropdown menu is open, showing options: 'None', 'CiscoUmbrellaDNSServerGroup', and 'CustomDNSServerGroup' (which is highlighted).
 -

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

Note: Certifique-se de que a Diretiva do Sistema seja aplicada ao FTD após a configuração do DNS. (O servidor DNS configurado deve resolver o FQDN que será usado)

Etapa 2. Crie o objeto FQDN, para fazer isso, navegue até **Objects > Object Management > 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

Add Network Object

Name
FQDN

Description

Type
 Network Host FQDN

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

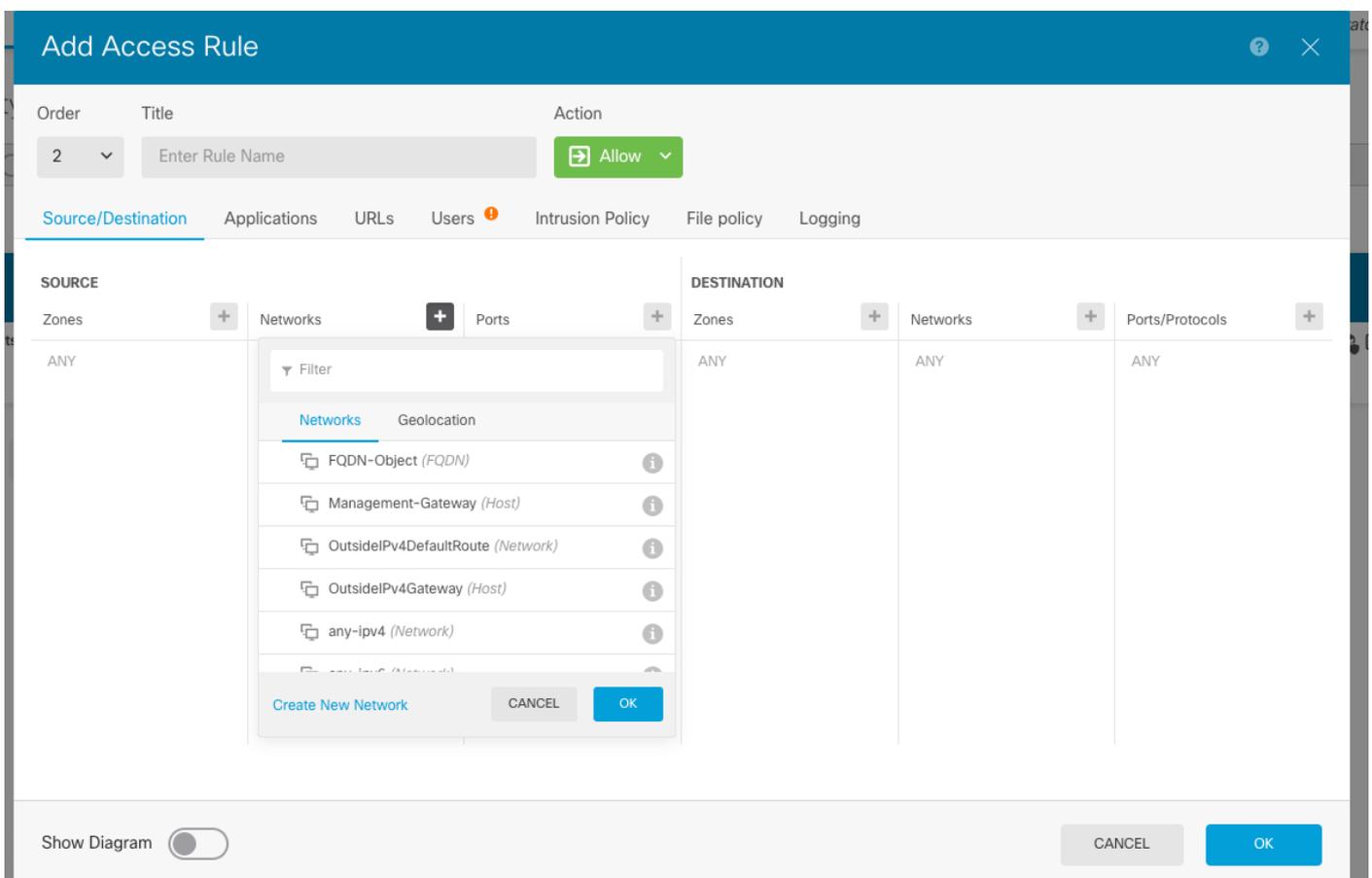
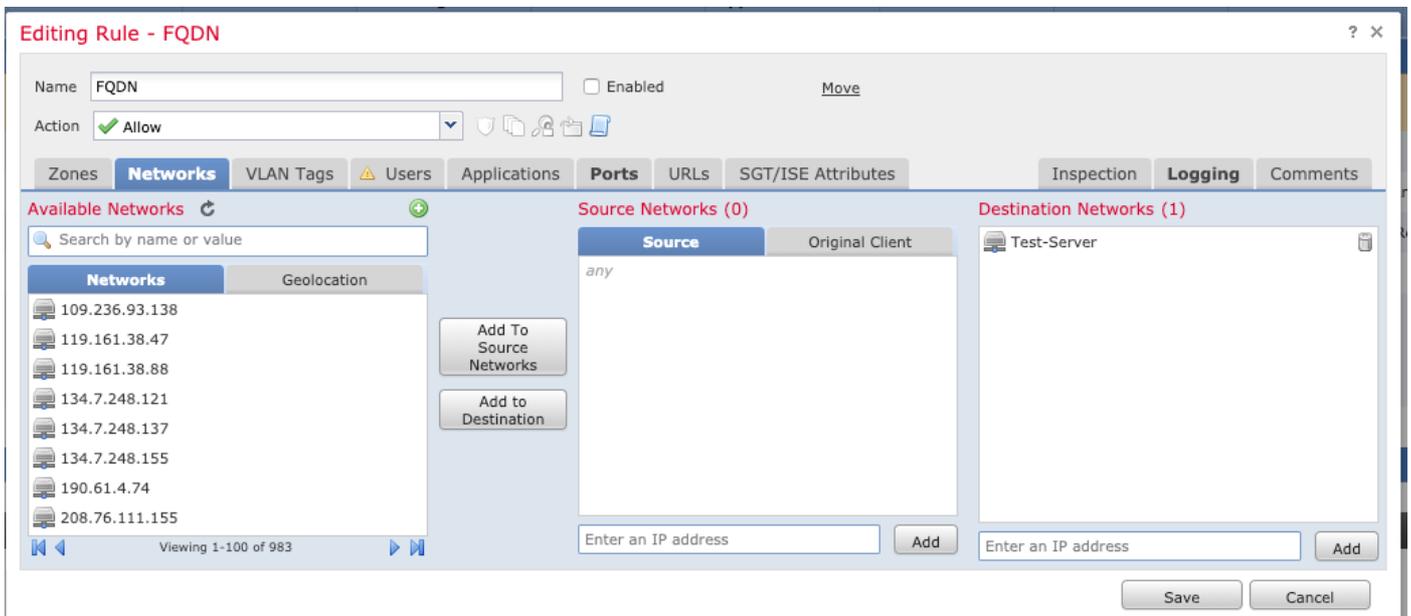
Domain Name
test.cisco.com
e.g. ad.example.com

DNS Resolution
IPv4 and IPv6

CANCEL OK

Etapa 3. Crie uma regra de controle de acesso navegando para **Políticas > Controle de acesso**.

Note: Você pode criar uma regra ou modificar a regra existente com base no requisito. O objeto FQDN pode ser usado em redes de origem e/ou destino.



Certifique-se de que a diretiva seja aplicada depois que a configuração for concluída.

Verificar

Inicie o tráfego da máquina cliente que deve disparar a regra baseada em FQDN criada.

No FMC, navegue até **Eventos > Eventos de Conexão**, filtre o tráfego específico.

| Jump to... | 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

Troubleshoot

O servidor DNS deve ser capaz de resolver o objeto FQDN, isso pode ser verificado a partir da CLI que executa estes comandos:

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