

配置FQDN访问控制规则的基于对象

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

Introduction

本文通过防火墙管理中心(FMC)在访问规则创建描述完全合格的域名(FQDN)对象的配置和如何使用FQDN对象。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Firepower技术知识。
- 配置由于Firesight管理中心(FMC)的访问控制策略知识

Components Used

本文档中的信息基于以下软件和硬件版本：

- Firepower运行版本6.3和以上的管理中心。
- Firepower运行版本6.3和以上的威胁防御。

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. 如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

Configure

步骤1.为了配置和使用FQDN根据对象，第一，配置在Firepower威胁防御的DNS。

登陆对FMC并且连接到设备>平台设置> DNS。

- ARP Inspection
- Banner
- DNS**
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP
- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

Enable DNS name resolution by device

DNS Server Group*:

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

- ftd-mgmt
- inside
- inside-nat
- labs
- outside
- outside-nat
- postgrad
- privileged
- research
- servers
- servers-nat
- staff

Selected Interface Objects

- outside
- servers

Enable DNS Lookup via diagnostic interface also.

Monitoring
Policies
Objects
Device

>
+
?
admin Administrator

System Settings ←

Management Access

Logging Settings

DHCP Server

DNS Server

Management Interface

Hostname

NTP

Cloud Services

Traffic Settings

URL Filtering Preferences

Device Summary

Configure DNS

Data Interface

Interfaces

ANY

DNS Group

FQDN DNS SETTINGS

Poll Time	Expiry
<input type="text" value="240"/> minutes	<input type="text" value="1"/> minutes
1 - 65535	1 - 65535

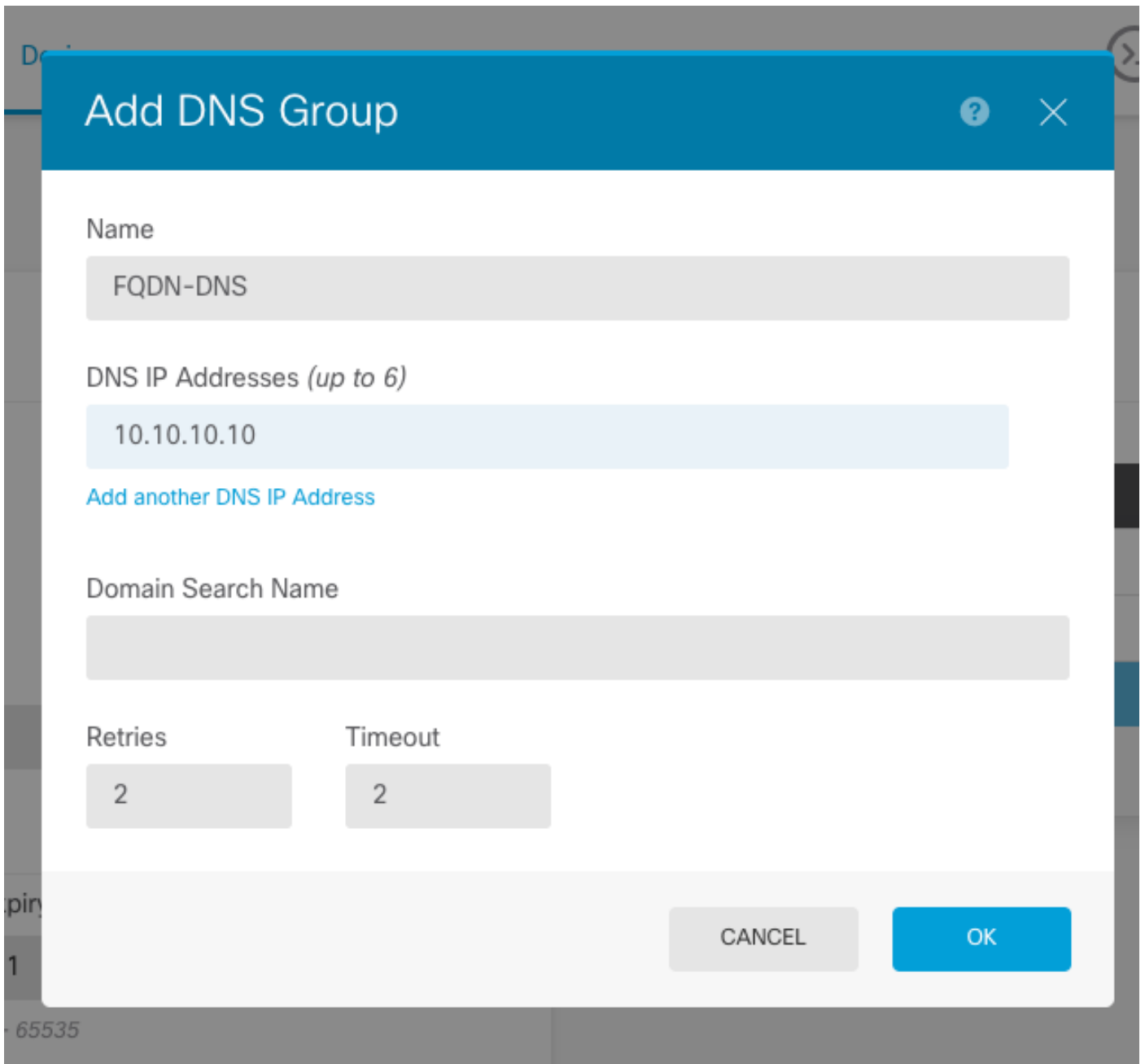
Management Interface

DNS Group

Filter

- None
- CiscoUmbrellaDNSServerGroup
- CustomDNSServerGroup

[Create DNS Group](#)



Note:保证系统策略被运用于FTD在配置DNS以后。(被配置的DNS服务器应该解决将使用)的FQDN

步骤2.创建FQDN对象，为了执行连接对对象>对象Management>添加Network > Add对象。

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.

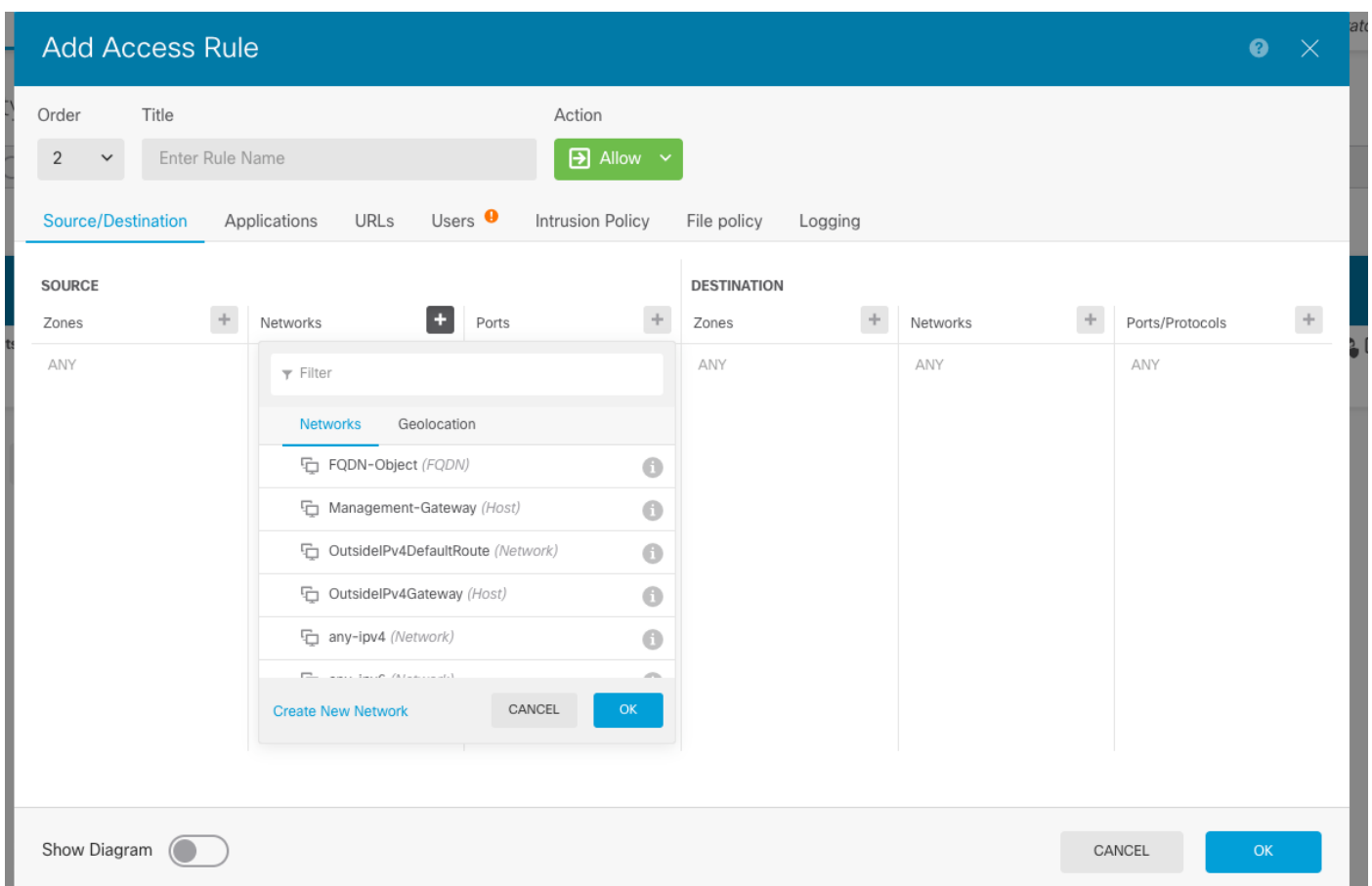
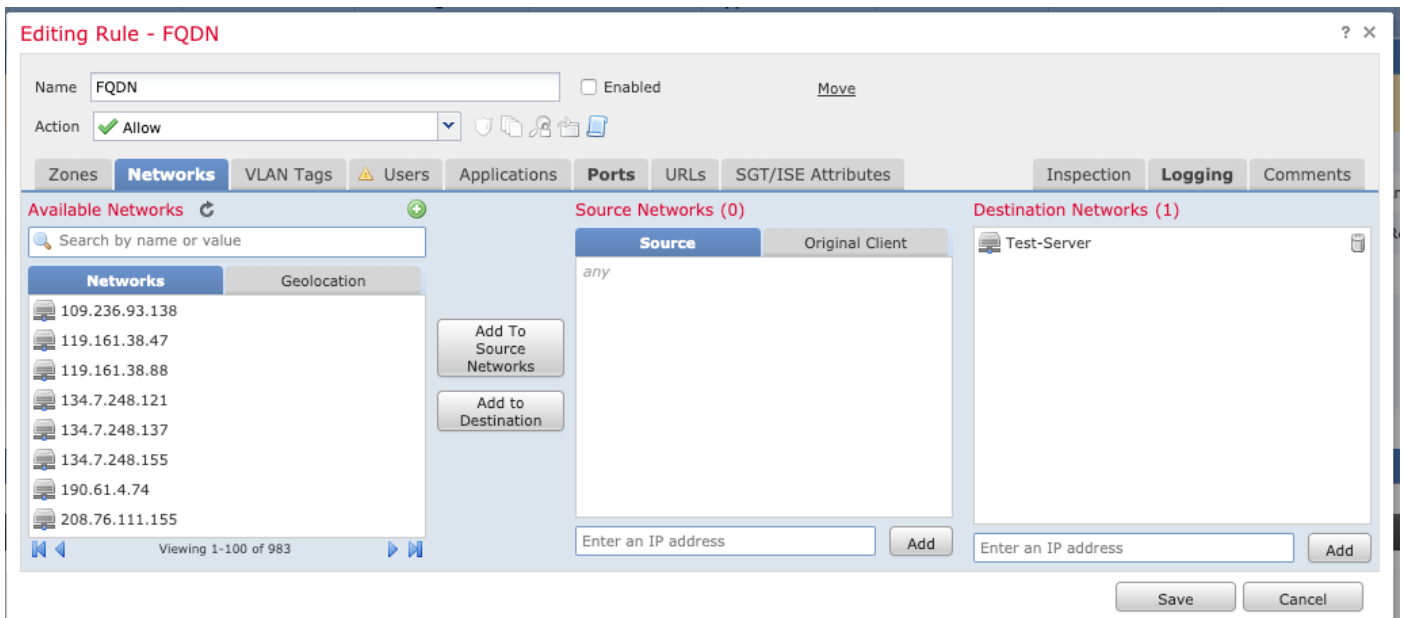
Domain Name
test.cisco.com
e.g. ad.example.com

DNS Resolution
IPv4 and IPv6

CANCEL OK

步骤3.通过连接创建访问控制规则到**策略>访问控制**。

Note:您能创建规则或修改根据需求的现有的规则。FQDN对象可以或者用于来源和目的地网络。



保证策略适用，在配置完成后。

Verify

初始化从预计触发被创建的FQDN基于规则的客户端机器的数据流。

在FMC，请连接对事件>连接事件，特定的流量的过滤器。

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

DNS服务器应该能解决FQDN对象，这可以从CLI被验证运行这些命令：

- 系统支持诊断CLI
- 显示fqdn

• 0