# 為訪問控制規則配置基於FQDN的對象

### 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設設 疑難排解</u>

### 簡介

本文檔介紹通過防火牆管理中心(FMC)配置完全限定域名(FQDN)對象以及在訪問規則建立中使用 FQDN對象的方式。

### 必要條件

#### 需求

思科建議您瞭解以下主題:

- Firepower技術知識。
- 在Firesight管理中心(FMC)上配置訪問控制策略的知識

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 運行6.3及更高版本的Firepower管理中心。
- 運行6.3及更高版本的Firepower威脅防禦。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設) )的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

## 設定

步驟1。若要配置和使用基於FQDN的對象,請先在Firepower威脅防禦上配置DNS。

登入FMC並導覽至Devices > Platform Settings > DNS。

	ARP Inspection	DNS Resolution Settings										
	Banner	Specify DNS servers grou	p and device interf	aces to re	ach them	1.						
٠	DNS	Z Enable DNS name recol	ution by device									
	External Authentication											
	Fragment Settings	DNS Server Group*:	DNS Server Group*: Cisco			<b>v</b> 💿						
	НТТР											
	ICMP	Expiry Entry Timer:	1		Rang	e: 1-65535 minutes						
	Secure Shell											
	SMTP Server	Poll Timer:	240	Range: 1-65535 minutes								
	SNMP	Interface Objects										
	SSL	Devices will use specif	ied interface object	ts for conr	necting w	ith DNS Servers.						
	Syslog											
	Timeouts	Available Interface C	Objects 🖒			Selected Interface Obje	ects					
	Time Synchronization	🔍 Search				📩 outside	i					
	UCAPL/CC Compliance	📩 ftd-mamt				servers	1					
		- inside										
	🖧 inside-nat											
		📥 labs										
		- outside										
		a outside		Ad	DI							

📩 outside-nat 👬 postgrad å privileged 📩 research servers 📇 servers-nat 📩 staff

Enable DNS Lookup via diagnostic interface also.

Add

alialia cisco.	Monitoring Policies Objects	Device		> 🖄 🙆	admin Administrator
CISCO. System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Traffic Settings URL Filtering Preferences	Monitoring Policies Objects Device Summary Configure DNS Data Interface Interfaces + ANY DNS Group CiscoUmbrellaDNSServerGroup FQDN DNS SETTINGS Poll Time 240 minu 7 - 65535 SAVE	res 1 7 - 65535	Management Interf DNS Group Filter None CiscoUmbreliaDN Create DNS Group	face	Administrator

Add DNS (	Group			0	×						
Name											
FQDN-DNS											
DNS IP Addresses	; (up to 6)										
10.10.10.10											
Add another DNS IP	Address										
Domain Search Na	ame										
Patrian	Timeout										
2	2										
			CANCEL	ОК							
5											

**附註**:確保在配置DNS之後將系統策略應用於FTD。(配置的DNS伺服器應解析將使用的FQDN)

步驟2.建立FQDN對象,為此,請導航到**對象>對象管理>新增網路>新增對象。** 

Edit Network	Object				? ×
Name	Test-Server				
Description	Test for FQDN	I			
Network	🔿 Host	🔘 Range	ONetwork	FQDN	
	test.cisco.com	1			
	Note: You can us	e FQDN network obje	cts in access and prefi	ilter rules only	
Lookup:	Resolve within	n IPv4 and IPv6		~	
Allow Overrides					
				Save	Cancel

# Add Network Object

D

Name				
FQDN				
Description				
				1.
Туре				
O Network (	⊖ Host	🔵 FQDN		
() Note: You can use F	QDN network obj	ects in acces	ss rules only.	
Domain Name				
test.cisco.com				
e.g. ad.example.com				
DNS Resolution				
IPv4 and IPv6	`	-		
			CANCEL	ОК

0

 $\times$ 

步驟3.導航到Policies > Access Control,建立訪問控制規則。

**附註**:您可以根據要求建立規則或修改現有規則。FQDN對象可以在源網路和/或目標網路中 使用。

Editing Rule - FQDN				? ×
Name FQDN	🗌 Enab	led <u>Move</u>		
Action Allow	🔹 U D 2 🗠 🗖			
Zones Networks VLAN Tags 🛆 Users	Applications Ports	URLs SGT/ISE Attributes	Inspection	Logging Comments
Available Networks 🖒 📀	Source	Networks (0)	Destination Networks	(1)
Search by name or value		Source Original Clier	nt 📄 Test-Server	ĩ
Networks Geolocation	any			
109.236.93.138				
119.161.38.47	Add To Source			
119.161.38.88	Networks			
134.7.248.121	Add to			
134.7.248.137	Destination			
134.7.248.155				
190.61.4.74				
208.76.111.155	Entern	ID address		
Viewing 1-100 of 983	enter al		Enter an IP address	Add
				Save Cancel

Add Access Rule	e					8 ×	a				
Order Title 2 V Enter Rule N	lame	Action Allow									
Source/Destination App SOURCE Zones +	Networks	ntrusion Policy +	File policy     Logging       DESTINATION	+ Networks	+ Ports/Protocols	+	ļ				
ANY	Filter         Networks       Geolocation         F       FQDN-Object (FQDN)         Management-Gateway (Host)         OutsidelPv4DefaultRoute (Network)         any-ipv4 (Network)         Create New Network         CANK	1 (1) (1) (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	ANY	ANY	ANY						
Show Diagram					CANCEL	ОК					

確保在配置完成後應用該策略。



啟動來自客戶端電腦的流量,該流量應觸發所建立的基於FQDN的規則。

在FMC上,導航到Events > Connection Events,過濾特定流量。

Ju	mp to	. •																		
		★ <u>First Packet</u>	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
4		2019-06-04 16:04:56	2019-06-04 17:05:16	Allow	Intrusion Monitor	21.21.21.101	SA USA	10.123.175.6		servers	outside	61132 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4		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
4		2019-05-04 12:32:31	2019-06-04 13:32:45	Allow		21.21.21.101	usa 🛄	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4		2019-06-04 12:32:31		Allow		21.21.21.101	SA USA	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp							FTD-1
4		2019-06-04 12:13:13	2019-06-04 12:13:54	Allow	Intrusion Monitor	21.21.21.101	SA USA	10.123.175.6		servers	outside	61097 / tcp	22.(ssh)./ tcp	SSH	SSH client					FTD-1
4		2019-06-04 12:13:13		Allow	Intrusion Monitor	21.21.21.101	usa usa	10.123.175.6		servers	outside	61097 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4		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	SSH client					FTD-1
4		2019-06-04 12:01:40		Allow	Intrusion Monitor	<u>21.21.21.101</u>	SA 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 A	I Delete All																		

## 疑難排解

DNS伺服器應該能夠解析FQDN對象,這可以通過運行以下命令的CLI進行驗證:

- •系統支援diagnostic-cli
- show fqdn