为访问控制规则配置基于FQDN的对象

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 验证 故障排除

简介

本文档介绍如何通过防火墙管理中心(FMC)配置完全限定域名(FQDN)对象,以及如何在访问规则创 建中使用FQDN对象。

先决条件

要求

Cisco 建议您了解以下主题:

- 了解Firepower技术。
- •了解在Firesight管理中心(FMC)上配置访问控制策略

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行版本6.3及更高版本的Firepower管理中心。
- •运行版本6.3及更高版本的Firepower威胁防御。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。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。

配置

步骤1.要配置和使用基于FQDN的对象,请首先在Firepower威胁防御上配置DNS。

登录FMC并导航至Devices > Platform Settings > DNS。

	ARP Inspection	DNS Resolution Settin	gs									
	Banner	Specify DNS servers grou	1.									
٠	DNS	Z Enable DNS name recol	ution by device									
	External Authentication		action by device									
	Fragment Settings	DNS Server Group*:	DNS Server Group*: Cisco			▼ ③						
	НТТР											
	ICMP	Expiry Entry Timer:		Rang	e: 1-65535 minutes							
	Secure Shell											
	SMTP Server	Poll Timer:	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 G	àroup		•								
Name											
FQDN-DNS											
DNS IP Addresses (up to 6)											
10.10.10											
Add another DNS IP	Address										
Domain Search Na	ame										
Retries	Timeout										
2	2										
		CANCEL	ОК								

注意:确保在配置DNS后将系统策略应用到FTD。(配置的DNS服务器应解析将使用的 FQDN)

步骤2.创建FQDN对象,以便导航到**Objects > Object Management > Add Network > Add Object**。

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

Add Network Object

D

Name				
FQDN				
Description				
Туре				
O Network	◯ Host	🔘 FQDN		
i Note: You can us	e FQDN network	objects in acce	ss rules only.	
Domain Name				
test.cisco.com				
e.g. ad.example.col	m			
DNS Resolution				
IPv4 and IPv6		~		
			CANCEL	ок

0

 \times

步骤3.导航至Policies > Access Control,创建访问控制规则。

注意:您可以根据要求创建规则或修改现有规则。FQDN对象可在源和/或目标网络中使用。

Editing Rule - FQDN								? ×
Name FQDN		Enabled Move						
Action Allow	• • • 2 4							
Zones Networks VLAN Tags 🛆 Users	Applications	Ports	URLs SC	GT/ISE Attributes		Inspection	Logging	Comments
Available Networks 🖒 😳	S	Source Net	works (0)			Destination Networks	(1)	
Search by name or value		Sou	ırce	Original Client	t	Test-Server		ũ
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								
Viewing 1-100 of 983		Enter an IP	address		Add	Enter an IP address		Add
							Save	Cancel

Add Access Rule	9					0 ×			
Order Title 2 Enter Rule N Source/Destination App	ame Dications URLs Users 9	Action Allow							
SOURCE Zones +	Networks + Ports	+	DESTINATION Zones +	Networks +	Ports/Protocols	+			
ANY	Filter Networks Geolocation For FQDN-Object (FQDN) For Management-Gateway (Host) For OutsidelPv4DefaultRoute (Network) For any-ipv4 (Network) Create New Network	ork)	ANY	ANY	ANY				
Show Diagram				C	CANCEL	ок			

确保在配置完成后应用策略。

验证

从客户端计算机发起流量,该流量应触发创建的基于FQDN的规则。

在FMC上,导航至**Events > Connection Events,过滤特定流量。**

Jump 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
4.0	2019-06-04 16:04:5	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 0	2019-06-04 16:04:5	ł	Allow	Intrusion Monitor	21.21.21.101	usa 🔜	10.123.175.6		servers	outside	61132 / tcp	22.(ssh) / tcp	SSH	SSH client					FTD-1
4.0	2019-05-04 12:32:3	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 0	2019-06-04 12:32:3	L	Allow		21.21.21.101	SA USA	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp							FTD-1
4.0	2019-06-04 12:13:1	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 0	2019-05-04 12:13:1	ł	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
4.0	2019-06-04 12:01:4	2019-06-04 12:01:48	Allow	Intrusion Monitor	21.21.21.101	SA USA	10.123.175.6		servers	outside	61066 / tcp	22_(ssh)_/ tcp	SSH	SSH client					FTD-1
4 0	2019-06-04 12:01:4	1	Allow	Intrusion Monitor	21.21.21.101	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																			
1	Tiew Delete																		
Vi	w All Delete All																		

故障排除

DNS服务器应该能够解析FQDN对象,这可以通过CLI运行以下命令来验证:

- •系统支持diagnostic-cli
- show fqdn

o