アクセスコントロールルールのFQDNベースオ ブジェクトの設定

内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>設定</u>
確認
トラブルシュート

概要

このドキュメントでは、ファイアウォール管理センター(FMC)を介した完全修飾ドメイン名 (FQDN)オブジェクトの設定と、アクセスルールの作成でFQDNオブジェクトを使用する方法につ いて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識.
- Firesight Management Center(FMC)でのアクセスコントロールポリシーの設定に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

・バージョン6.3以降を実行しているFirepower Management Center(FMC)。

• バージョン6.3以降を実行するFirepower Threat Defense(FTD)。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

ステップ1:FQDNベースのオブジェクトを設定して使用するには、まずFirepower Threat DefenseでDNSを設定します。

FMCにログインし、[Devices] > [Platform Settings] > [DNS]に移動します。

	ARP Inspection	DNS Resolution Settin	gs									
	Banner	Specify DNS servers group and device interfaces to reach them.										
٠	DNS	Enable DNS name resolution by device										
	External Authentication	Enable DNS name resolution by device										
	Fragment Settings	DNS Server Group*:	Cisco	▼ ③								
	НТТР											
	ICMP	Expiry Entry Timer:	1	R	ange: 1-65535 minutes							
	Secure Shell											
	SMTP Server	Poll Timer:	240	R	ange: 1-65535 minutes							
	SNMP	Interface Objects										
	SSL	Devices will use specif	fied interface object	ts for connectin	g with DNS Servers.							
	Syslog				_							
	Timeouts	Available Interface 0	Objects 🖒		Selected Interface Obj	Selected Interface Objects						
	Time Synchronization	🔍 Search			📇 outside	6						
	UCAPL/CC Compliance	🖧 ftd-mamt		1	🚔 servers	6						
		- inside										
		📥 inside-nat										
		- labs										
		- outside-pat		Add								
		- privileged										
		- research										
		- servers										
		servers-nat										
		servers-nat										
		starr										

alialia cisco.	Monitoring Policies		Device) (2)	?	admin Administrator	•
System Settings ← Management Access	Device Summary Configure DNS									
Logging Settings	Data Interface				Management Ir	nterface				
DHCP Server	Interfaces +				DNS Group Filter					~
Management Interface	ANY				None	ellaDNSServerGroup	0			
NTP	DNS Group CiscoUmbrellaDNSServ	erGroup		~	CustomDN:	SServerGroup	0			
Cloud Services	FQDN DNS SETTINGS				Create DNS Group					
URL Filtering Preferences	Poll Time 240	minute	s 1	minutes						
	1 - 65535 SAVE		1 - 65535							

Add DNS (Group		9	×
Name				
FQDN-DNS				
DNS IP Addresse	s (up to 6)			
10.10.10.10				
Add another DNS IP	Address			
Domain Search N	ame			
Retries	Timeout			
2	2			
		CANCEL	ок	
5				

注:DNSの設定後、システムポリシーがFTDに適用されていることを確認します(設定されたDNSサーバが、使用されるFQDNを解決する必要があります)。

ステップ2:FQDNオブジェクトを作成します。作成するには、[**Objects**] > [**Object Management**] > [Add Network] > [Add Object]に移動します。

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 or											
Lookup:	Resolve within	n IPv4 and IPv6		~									
Allow Overrides													
				Save	Cancel								

Add Network Object

D

Name		
FQDN		
Description		
Type		1,
O Network O Host O 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	ОК

0

 \times

ステップ3:[Policies] > [Access Control]の順に移動して、アクセスコントロールルー**ルを作成しま す。**

注:ルールを作成するか、要件に基づいて既存のルールを変更できます。FQDNオブジェクトは、送信元または宛先ネットワークで使用できます。

Editing Rule - FQDN							? ×
Name FQDN		Enabled	Move				
Action Allow	▼ V D 2 th [3					
Zones Networks VLAN Tags 🛆 User	s Applications P	orts URLs	SGT/ISE Attributes		Inspection	Logging	Comments
Available Networks C) So	urce Networks ((0)	Destina	ation Networks	(1)	
Search by name or value		Source	Original Client	📄 Tes	t-Server		1
Networks Geolocation	an	<i>iy</i>					
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							
i90.61.4.74							
208.76.111.155							
Viewing 1-100 of 983	En	iter an IP address		Add Enter a	an IP address		Add
						Save	Cancel

Add Access Rule	Э					፼ × ⁸
Order Title 2 Conter Rule N Source/Destination App	Action	Allow Y	icy Logging			
SOURCE Zones +	Networks + Ports	DESTIN + Zones	ATION +	Networks +	Ports/Protocols	+
ANY	▼ Filter Networks Geolocation G FQDN-Object (FQDN) G Management-Gateway (Host) G OutsidelPv4DefaultRoute (Network) G OutsidelPv4Gateway (Host) G any-ipv4 (Network) Create New Network CANCEL	ANY ANY C		ANY	ANY	
Show Diagram					CANCEL	ок

設定が完了したら、ポリシーが適用されていることを確認します。

確認

作成されたFQDNベースのルールをトリガーすると予想されるクライアントマシンからトラフィックを開始します。

FMCで、[Events] > [Connection Events]に移動し、特定のトラフィックをフィルタします。

•																				
		★ <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 16:04:56	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	<u>21.21.21.101</u>	SA 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		<u>21.21.21.101</u>	SA 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	<u>61115 / tcp</u>	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 (2019-05-04 12:13:13		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 12:01:40	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.		2019-06-04 12:01:40		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
< < 1	Page	1 of 1 >> Displa	ying rows 1-8 of 8 rows																	

View Delete
View All
Delete All

トラブルシュート

DNSサーバはFQDNオブジェクトを解決できる必要があります。これは、CLIから次のコマンドを 実行して確認できます。

- system support diagnostic-cli
- show fqdn

.