在FMC的PBR的擴展ACL上配置FQDN對象

目錄	
<u>必要條件</u>	
採用元件	
<u>背景資訊</u>	
<u>設定</u>	
<u>驗證</u>	
<u>常見問題</u>	
PBR在第二次部署後停止工作	
<u>FQDN未解析</u>	

簡介

本檔案介紹在延伸存取清單(ACL)中設定FQDN物件以用於原則型路由(PBR)的程式。

必要條件

需求

思科建議您瞭解以下產品:

- 安全防火牆管理中心(FMC)
- 安全防火牆威脅防禦(FTD)
- PBR

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 適用於VMware的Firepower威脅防禦7.6.0版
- 適用於VMware的安全防火牆管理中心7.6.0版

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。

背景資訊

目前,FTD不允許使用思科錯誤ID <u>CSCuz98322</u>上提到的完整網域名稱(FQDN)物件在非HTTP流量 上進行過濾。 ASA平台支援此功能,但是,在FTD上只能過濾網路和應用。

您可以使用此方法將FQDN對象增加到擴展訪問清單以配置PBR。

設定

步驟 1.根據需要建立FQDN對象。

Edit Network Object

Name	
cisco.com	
Description	
Network Host Range Network cisco.com Note: You can use FQDN network objects in ac Lookup: solve within IPv4 addresses only •	FQDN ccess, prefilter and translated destination in NAT rules only.
Allow Overrides	
	Cancel Save

0

圖1.網路物件功能表

步驟 2.在Objects > Object Management > Access List > Extended下建立擴展訪問清單。

>	AAA Server	Extended	Add Extended Access List	Q Filter
~	Access List Extended	An access list object, also kno and destination address and p	wn as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address onl oorts. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.	y. Identifies traff
	Standard			
>	Address Pools	Name	Value	Override
	Application Filters		Na zasazis ta display	
	AS Path		No records to display	
	BFD Template			
	Cipher Suite List			
>	Community List			

圖2.擴展訪問清單選單

增加新規則時,請注意在搜尋網路對象以選擇源和目標時看不到配置的FQDN對象。

Edit Extended Access List Entry	У			0
C Allow 💌				
Logging:				
Default •				
Log Level:				
Informational v				
Log Interval:				
	Sec.			
Network Port	Users Security Group Tag			
Available Networks C*	+	Source Networks (0)	Destination Networks (0)	
Q cisco	×	any	any	
	Add to Source			
	Add to Destination			
		Enter an IP address Add	Enter an IP address	E.
			Cancel Sav	e

圖3.新建擴展訪問清單規則選單

步驟 3.建立無法命中的規則,以便建立擴展ACL並可用於PBR配置。

Add Extended Access List Entry

Action:					
Allow ~					
Logging:					
Default					
Log Level:					
Informational ~					
Log Interval:					
300 Sec.					
Network Port Application	sers 🕕 Security Group Ta	g			
Available Networks C* +		Source Networks (1)		Destination Networks (1)	
Q Search by name or value)	192.0.2.10/32	ū	192.0.2.10/32	ū
any	Add to Source				•
any-ipv4	Add to Destination				
any-ipv6					
GW-10.100.150.1					
IPv4-Benchmark-Tests					
IPv4-Link-Local					
	I	1	1	1	1
					Cancel Add

圖4.無法命中的訪問清單規則配置

步驟 4.您需要在以FQDN物件為FTD目標的存取控制原則(ACP)上建立規則。FMC會將FQDN物件 部署到FTD,以便您可以透過FlexConfig物件來參考它。

1 🗘 Add Rule			ବ
Name New-Rule-#1-ALLOW	Action	C Allow	Logging OFF Time Range None Rule Enabled
nsert into Mandatory 🗸	Intro	usion Policy None	Variable Set V File Policy None V
Q Zones Networks (2) Ports Applications	Users URLs Dynamic Attributes	VLAN Tags	
Q Search Network and Geolocation Objects	Showing 15 out of 15	Selected Sources: 1	Q Selected Destinations and Applications: 1 Q
Networks Geolocations		Collapse All	Remove All Collapse All Remove All
& any (Network Group)	0.0.0.0/0,::/0	NET V 1 Object	NET V 1 Object
any-ipv4 (Network Object)	0.0.0/0	cisco.com	cisco.com
any-ipv6 (Host Object)	::/0		
cisco.com (Network FQDN Object)	cisco.com		
IPv4-Benchmark-Tests (Network Object)	198.18.0.0/15		

圖5.具有FQDN物件的ACP規則

步驟 5.導覽至Devices > Device Management上的FTD,然後選擇Routing索引標籤,然後導覽至 Policy Based Routing區段。

cisco	Firewall Management Center Devices / Secure Firewall Routing			Q Search	Deploy	0	@ @	admin ~
Home	10.100.150.33 Cisco Secure Firewall Threat Defense	for VMware						Save Cancel
Uvervie	ew Device Interfaces Inline S	Bets Routing DHCP VTEP						
ilil Analys	is Global Virtual Routers	Policy Based Routing Specify ingress interfaces, match criteria and egress interfaces	ces to route traffic accordingly. Traffic can be route	ed across Egress interfaces accordingly	Configure In	terface P	riority	Add
Policie	Virtual Router Properties	Ingress Interfaces	Match criteria and forward action					
Device	ECMP BFD OSPF	For step-by-step	There are no PBR policies defined yet. Start guidance on configuring a policy-based routing p	by defining the first one. olicy and adding applications, launch the How-	То.			
€ Object	OSPFv3 ts EIGRP							
🍰 Integrat	Policy Based Routing							
	IPv4							
	IPv6							
	 Multicast Routing 							
	intin							

圖6.PBR選單

步驟 6.使用之前配置的ACL在介面上配置PBR並進行部署。

Add Forwa	Irding Actions						(?)
Match ACL: *	fqdn	~	+				
Send To: *	Egress Interfaces	~					
Interface Orderin	Interface Priority	~ ()				
Available Interface	S		S	elected Egress	Interfaces *		
Search by interfa	ce name			Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Save

圖7.PBR介面和ACL選擇選單

步驟 7.導航到對象>對象管理> FlexConfig >對象並建立新對象。

uluulu cisco	Firewall N Objects / Obj	lanagement ect Management	Center						Q Search			Deploy 🥏 🚫
~			4	Add FlexConfig O	bject						(?)	Object Q. Filter
Home	Ð	> AAA Server	N	lame:								
Overvie	ew	 Access List Address Pool Application Fi 	s D	fqdn Description:								
ad		AS Path	l l									
Analys	is	BFD Template		A Convensation any rich tax	t might introduce line breaks	while generating CLL	Diageo vorify the (21 Libefore deployme	ot			S with the help of TextOb
0		Cipher Suite I	ist	a copy pasting any nen tes	trangit introduce inte breaks	the generating oct.	riouse verify the c	servere deployme				action
Policie	s	> Community L	st		ployment: Everytime		Type	nnend				scuon.
		DHCP IPv6 Pc	lool	ax De			Type.	ppena				ction.
		> Distinguished	Name	Insert Policy Object	Text Object							le (PD client) and one insid
Device	25	DNS Server G	roup	Insert System Variable >	Network							n of one outside (PD clien
•=		External Attril	outes	Insert Secret Key	Security Zones							the help of TextObjects dr
Object	ts	File List			Standard ACL Object							oficurations
		 FlexConfig 			Extended ACL Object	1						ingurations.
Integrat	tion	FlexConfig	Object		Route Map	•						Configures next hop. 2. co
		Text Object	t									parameters for eigrp. 1. C
		Geolocation		✓ Variables								ration for an AS
		Interface										ration.
		Key Chain		Name	Dimension	Default Value	Property (Type:Name)	Override	Description			for ipv6 traffic. Used text
		Network				No records to	dientau					
		> PKI										-
		Policy List								Cancel	Save	20 of 48 rows < < Page
		Port	-							_		

圖8.FlexConfig物件組態功能表

步驟 8.選擇Insert > Extended ACL Object,命名變數並選擇之前建立的擴展ACL。該變數會以您使 用的名稱加入。

Insert Extended Access List Object Variable



Cancel Save

(?)

圖9.FlexConfig物件的變數建立

步驟 9.為要用於ACL的每個FQDN對象輸入此行。

<#root>

access-li \$

extended permit ip any object

步驟 10.將FlexConfig對象儲存為Everytime > Append。

第11步: 導航到Devices > FlexConfig下的FlexConfig Policy選單。

Home	Devices		×	
Overview	Device Management	VPN	Troubleshoot	
	Template Management	Site To Site	File Download	
III Analysis	NAT	Remote Access	Threat Defense CLI	
	QoS	Dynamic Access Policy	Packet Tracer	
Policies	Platform Settings	1	Packet Capture	
	FlexConfig 🗸 🗸		Snort 3 Profiling	
Devices	Certificates	•	Troubleshooting Logs	
•				
Objects			Upgrade	
5			Threat Defense Upgrade	
Integration			Chassis Upgrade	
圖10.FlexConfig	策略選單的路徑			

E: Overview

test flex

 Status
 Last Medified

 Torgeting 1 device(s)
 2024-13-14 1150-39

 Up-to-data on all targeted devices
 ModRed by "schnin"

600

-til Analysis Policies 步驟 12.建立新的FlexConfig策略或選擇已分配給FTD的策略。

圖11.編輯或建立新的FlexConfig策略

步驟 13.將FlexConfig對象增加到策略,儲存和部署。

~	test flex				Migrate Config Preview Config Save Cance
Home	Enter Description				
Overview	Available FlexConfig C FlexConfig Object		Selected Prepend Fl	exConfigs	Policy Assignments (1)
dil	×		# Name	Description	
Analysis	✓ User Defined				
Policies	<pre> fqdn</pre> ✓ System Defined				
-	Default_DNS_Configure				
Devices	Default_Inspection_Protocol_Disable				
•_=	DHCPv6_Prefix_Delegation_Configure		Selected Append Fle	xConfigs	
Objects	DHCPv6_Prefix_Delegation_UnConfigure				
4	DNS_Configure		# Name	Description	
Integration	Eigrp_Configure		1 fqdn		Q 🗇

圖12.已將FlexConfig對象增加到FlexConfig策略中

驗證

您的輸入介面具有帶有自動生成的路由對映的策略路由。

<#root>

firepower#

```
show run interface gi0/0
```

!
interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 10.100.151.2 255.255.0

policy-route route-map FMC_GENERATED_PBR_1727116778384

路由對映包含具有已使用目標介面的選定ACL。

<#root>

firepower#

show run route-map FMC_GENERATED_PBR_1727116778384

!

route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn

您的訪問清單包含用於參考的主機以及透過FlexConfig增加的其他規則。

<#root>

firepower#

show run access-list fqdn

access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10 access-list fqdn extended permit ip any object cisco.com

您可以從入口介面執行Packet Tracer作為源,以驗證您是否進入PBR階段。

<#root>

firepower#

packet-tracer input inside tcp 10.100.150.1 12345 fqdn cisco.com 443

Mapping FQDN cisco.com to IP address 72.163.4.161

[...] Phase: 3

Type: PBR-LOOKUP

Subtype: policy-route Result: ALLOW Elapsed time: 1137 ns

Config:

route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn

set adaptive-interface cost outside

Additional Information:

Matched route-map FMC_GENERATED_PBR_1727116778384, sequence 5, permit

[...] Result:

input-interface: inside(vrfid:0)

input-status: up
input-line-status: up

output-interface: outside(vrfid:0)

output-status: up output-line-status: up Action: allow Time Taken: 140047752 ns

常見問題

PBR在第二次部署後停止工作

請驗證訪問清單是否仍包含FQDN對象規則。

在這種情況下,您可以看到規則已不存在。

firepower# show run access-list fqdn
access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
firepower#

驗證FlexConfig對象是否設定為Deployment: Everytime和Type: Append。該規則每次都應用於 未來的部署。

FQDN未解析

嘗試對FQDN執行ping操作時,會收到有關主機名無效的消息。

<#root>

firepower#

ping cisco.com

٨

ERROR: % Invalid Hostname

驗證DNS配置。您的伺服器組上必須有可訪問的DNS伺服器,並且域名查詢介面必須能夠訪問它們

<#root>

firepower#

show run dns

dns domain-lookup outside

DNS server-group DefaultDNS DNS server-group dns

name-server 208.67.222.222

name-server 208.67.220.220

dns-group dns

firepower#

ping 208.67.222.222

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 208.67.222.222, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 170/202/280 ms firepower#

ping cisco.com

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 72.163.4.161, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/190 ms.

o

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。