# 在FMC上的PBR的扩展ACL上配置FQDN对象

目录
简 <u>介</u>
先决条件
使用的组件
<u>背景信息</u>
<u>验证</u>
<u>常见问题</u>
PBR在第二次部署后停止工作
FQDN无法解析

## 简介

本文档介绍在扩展访问列表(ACL)中配置FQDN对象以用于基于策略的路由(PBR)的过程。

## 先决条件

要求

思科建议您了解以下产品:

- 安全防火墙管理中心(FMC)
- 安全防火墙威胁防御(FTD)
- PBR

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 适用于VMware的Firepower威胁防御7.6.0版
- 适用于VMware 7.6.0版的安全防火墙管理中心

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。

## 背景信息

目前,FTD不允许使用思科漏洞ID <u>CSCuz98322</u>上提及的完全限定域名(FQDN)对象对非HTTP流量 进行过滤。 ASA平台支持此功能,但是,在FTD上只能过滤网络和应用。

您可以使用此方法将FQDN对象添加到扩展访问列表以配置PBR。

## 配置

### 步骤1:根据需要创建FQDN对象。

Edit Network Object

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

0



图 1.网络对象菜单

第二步:在Objects > Object Management > Access List > Extended下创建扩展访问列表。

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

### 图 2.扩展访问列表菜单

### 添加新规则时,请注意您在搜索网络对象以选择源和目标时无法看到配置的FQDN对象。

Edit Extended Access List Entry				0
C Allow				
Logging:				
Default				
Log Level:				
Informational v				
Log Interval:				
300 S	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 Ad	d
			Cancel Sav	e

图 3.新建扩展访问列表规则菜单

第三步:创建无法命中的规则,以便创建扩展ACL并可用于PBR配置。

#### Add Extended Access List Entry

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

### 图 4.无法命中的访问列表规则配置

第四步:您需要在访问控制策略(ACP)上创建一个规则,以使用FQDN对象的FTD为目标。FMC将 FQDN对象部署到FTD,以便您可以通过FlexConfig对象引用它。

1 💭 Add Rule					0
Name New-Rule-#1-ALLOW	Action	C Allow	Logging OFF	inge None V	le Enabled
Insert into Mandatory 🗸	• Intr	usion Policy None	Variable Set	V File Policy None	~
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 8	elected Destinations and Applications: 1	٩
Networks Geolocations		Collapse All	Remove All	Collapse All	Remove All
& any (Network Group)	0.0.0.0/0,::/0	NET ~ 1 Object		NET v 1 Object	
any-ipv4 (Network Object)	0.0.0/0	cisco.com	L	cisco.com	
any-ipv6 (Host Object)	::/0				
cisco.com (Network FQDN Object)	cisco.com				
IPv4-Benchmark-Tests (Network Object)	198.18.0.0/15				
	1				

#### 图 5.具有FQDN对象的ACP规则

第五步:导航到设备>设备管理上的FTD,选择路由选项卡,导航到基于策略的路由部分。

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	Sets Routing DHCP VTEP						
ilil Analys	is Global Virtual Routers	Policy Based Routing Specify ingress interfaces, match criteria and egress interfa	ces to route traffic accordingly. Traffic can be route	d across Egress interfaces accordingly	Configure In	terface Pr	riority	Add
Policie	Virtual Router Properties	Ingress Interfaces	Match criteria and forward action	definition the Freek and				
Device	BFD OSPF	For step-by-step	guidance on configuring a policy-based routing po	ilicy and adding applications, launch the How	r-To.			
Object	OSPFv3 ts EIGRP							
the grat	PIP Policy Based Routing							
	IPv4							
	IPv6							
	Static Route							
	<ul> <li>Multicast Routing</li> </ul>							

### 图 6.PBR菜单

第六步:使用之前配置的ACL在接口上配置PBR并进行部署。

Add Forw	arding Actions						?
Match ACL: *	fqdn	~ -	ŀ				
Send To: *	Egress Interfaces	~					
Interface Orderir	n Interface Priority	~ 0					
Available Interfa	ces		S	elected Egress	Interfaces *		
Search by inter	face name	Q		Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Save

### 图 7.PBR接口和ACL选择菜单

步骤 7.导航到对象>对象管理> FlexConfig >对象,然后创建新对象。

cisco	Firewall Management Cen Objects / Object Management	Q. Search	Deploy 📀 🚫
\$		Add FlexConfig Object ©	Object Q Filter
Home	> AAA Server	Name:	
Uvervie	Access List     Address Pools     Application Filters	fqdn Description:	
ad	AS Path		
Analysi	s BFD Template	A. Consu postion one deb tost might introduce line branks while concretion CLI Blance undfu the CLI before deployment	VS with the help of TextOb
	Cipher Suite List	Copy-passing any rich text might introduce line breaks while generating CLL Please verify the CL before deployment.	
Policies	s Community List		ection.
	DHCP IPv6 Pool	Insert V III Deployment: Everytime V Type: Append V	ction.
-	> Distinguished Name	Insert Policy Object > Text Object	le (PD client) and one insid
Device	s DNS Server Group	Insert System Variable > Network	n of one outside (PD clien
•••	> External Attributes	Insert Secret Key Security Zones	the help of TextObjects dr
Object	s File List	Standard ACL Object	and help of reactory costs an
	✓ FlexConfig	Extended ACI Object	ntigurations.
<b>3</b> -	FlexConfig Obje	ct	Configures next hop. 2. co
integrati	Text Object	Route Map	parameters for eigrp. 1. C
	Geolocation	V Veriablee	ration for an AS
	Interface	· Yanawas	ration
	Key Chain	Name Dimension Default Value Property Override Description	
	Network	(Type:Name)	for ipv6 traffic. Used text
	> PKI	Ma maarda ta diantau	
	Policy List	Cancel Save	20 of 48 rows 1/ / Page
	Port		

### 图 8.FlexConfig对象配置菜单

步骤 8选择Insert > Extended ACL Object,命名变量并选择之前创建的扩展ACL。该变量将使用您 使用的名称进行添加。

## Insert Extended Access List Object Variable



Cancel Save

(?)

图 9.FlexConfig对象的变量创建

步骤 9为要使用ACL的每个FQDN对象输入此行。

<#root>

access-li \$

extended permit ip any object

步骤 10将您的FlexConfig对象另存为Everytime > Append。

第11步:导航到设备> FlexConfig下的FlexConfig Policy菜单。

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		Packet Capture	
_	FlexConfig 🗸 🗸		Snort 3 Profiling	
Devices	Certificates		Troubleshooting Logs	5
•	-			
Objects			Upgrade	
<b>5</b> -			Threat Defense Upgr	ade
Integration			Chassis Upgrade	

图 10.FlexConfig策略菜单的路径

步骤 12创建新的FlexConfig策略或选择已分配给您的FTD的策略。

000

图 11.编辑或创建新的FlexConfig策略

步骤 13将FlexConfig对象添加到策略、保存和部署。

	test flex						Migrate Config Preview Config Save Cance
Home	Enter Description						
Overview	Available FlexConfig C* FlexConfig Object		"ì :	Selected Prepend Fl	exConfigs		Policy Assignments (1)
dil	8	J		# Name		Description	
Analysis	✓ User Defined						
Polisias	i fqdn						
Policies	Default_DNS_Configure						
Daviasa	Default_Inspection_Protocol_Disable						
Devices	Default_Inspection_Protocol_Enable	$\cup$					
■	DHCPv6_Prefix_Delegation_Configure			Selected Append Fle	exConfigs		
Objects	DHCPv6_Prefix_Delegation_UnConfigur		-			-	
	DNS_Configure		Ľ	# Name		Description	
Integration	DNS_UnConfigure			l fqdn			Q 🗇
	Eigrp_Configure		-				

图 12.已将FlexConfig对象添加到FlexConfig策略中

## 验证

您的入口接口具有带有自动生成的路由映射的策略路由。

#### <#root>

firepower#

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

! interface GigabitEthernet0/0 nameif inside security-level 0 ip address 10.100.151.2 255.255.255.0

policy-route route-map FMC\_GENERATED\_PBR\_1727116778384

#### 路由映射包含具有已用目标接口的选定ACL。

#### <#root>

firepower#

show run route-map FMC\_GENERATED\_PBR\_1727116778384

!

route-map FMC\_GENERATED\_PBR\_1727116778384 permit 5

match ip address fqdn

您的访问列表包含用于参考的主机以及通过FlexConfig添加的其他规则。

<#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

您可以从入口接口执行Packet Tracer作为源,以验证您是否已进入PBR阶段。

#### <#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

### 常见问题

### PBR在第二次部署后停止工作

请验证访问列表是否仍包含FQDN对象规则。

在这种情况下,您可以看到此规则已不存在。

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

验证FlexConfig对象是否设置为Deployment: Everytime和Type: Append。该规则每次都应用于 未来部署。

FQDN无法解析

当您尝试ping FQDN时,您会收到有关无效主机名的消息。

<#root>

firepower#

ping cisco.com

٨

ERROR: % Invalid Hostname

检验DNS配置。您的服务器组上必须有可访问的DNS服务器,并且域名查找接口必须能够访问它们

#### <#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

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。