# FMCのPBR用の拡張ACLでのFQDNオブジェクトの設定

内容
<u>はじめに</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>背景説明</u>
<u>設定</u>
<u>確認</u>
<u>一般的な問題</u>
<u>2回目の導入の後でPBRが動作しなくなる</u>
<u>FQDNが解決されない</u>

# はじめに

このドキュメントでは、ポリシーベースルーティング(PBR)で使用する拡張アクセスリスト (ACL)にFQDNオブジェクトを設定する手順について説明します。

# 前提条件

### 要件

次の製品に関する知識があることが推奨されます。

- ・ セキュアファイアウォール管理センター(FMC)
- セキュアファイアウォール脅威対策(FTD)
- PBR

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。

- VMware向けFirepower Threat Defenseバージョン7.6.0
- Secure Firewall Management Center for VMwareバージョン7.6.0

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、クリアな(デフォルト)設定で作業を開始していま 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。

# 背景説明

現在、FTDでは、Cisco Bug ID <u>CSCuz98322</u>で説明されているように、完全修飾ドメイン名 (FQDN)オブジェクトを使用して非HTTPトラフィックをフィルタリングすることはできません。

この機能はASAプラットフォームでサポートされていますが、FTDでフィルタリングできるのは ネットワークとアプリケーションだけです。

(2)

拡張アクセスリストにFQDNオブジェクトを追加して、この方法でPBRを設定できます。

## 設定

ステップ1:必要に応じてFQDNオブジェクトを作成します。

### Edit Network Object

Name						
cisco.com	1					
Description	1					
Network	0	Range	0	Network	۲	FQDN
cisco.com	1					

Note:

You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

### Lookup:

Ŀ	solve	within	IPv4	addresses	only	•
c	Alk	w Ove	rride	5		



画像 1.Network Objectメニュー

ステップ 2: Objects > Object Management > Access List > Extendedの順に選択して、拡張アク セスリストを作成します。

> ~	AAA Server Access List Extended	Extended An access list object, also and destination address a	known as an access control list (ACL), selects the traffic to which a service will app nd ports. Supports IPv4 and IPv6 addresses. You use these objects when configurin	Add Extended Access List y. Standard-Identifies traffic based on destination address only g particular features, such as route maps.	Q Filter
	Standard				
>	Address Pools	Name		Value	Override
	Application Filters		No secondo to di		
	AS Path		No records to de	spiay	
	BFD Template				
	Cipher Suite List				
>	Community List				

### 画像 2.拡張アクセスリストメニュー

### 新しいルールを追加する場合は、ネットワークオブジェクトで送信元と宛先を選択する検索を実 行するときに設定したFQDNオブジェクトが表示されないことに注意してください。

Edit Extended Access List Entry		Q
Allow  Allou  Logging:  Default  Log Level:		
Informational   Log Interval: 300 Sec.		
Available Networks C + Q cisco X Add to	Source Networks (0) any Destination	Destination Networks (0)
	Enter an IP address	Add Enter an IP address Add Cancel Save

画像 3.新しい拡張アクセスリストルールメニュー

ステップ3: ヒットできないルールを作成して、拡張ACLを作成し、PBR設定に使用できるよう にします。

### Add Extended Access List Entry

Action:					
C Allow ~					
Logging:					
Default					
Log Level:					
Informational ~					
Log Interval:					
300 Sec.					
Network Port  Application	sers 🚯 Security Group Ta	ag			
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					
L	1	I	1	1	1
					Cancel Add

図 4.ヒットできないアクセスリストルールの設定

ステップ 4: FQDNオブジェクトを使用してFTDを対象とするアクセスコントロールポリシー (ACP)でルールを作成する必要があります。FMCはFQDNオブジェクトをFTDに導入するため、 FlexConfigオブジェクトを介して参照できます。

1 🔷 Add Rule				0
Name New-Rule-#1-ALLOW	Action	C Allow	OFF <b>K</b> Time Range None <b>v</b>	tule Enabled
Insert into Mandatory 🗸	Intru	Ision Policy None	Variable Set Variable Set None	<b>\</b>
Q Zones Networks (2) Ports Applications User	s 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 ০
Networks Geolocations		Collapse All	Remove All Collapse All	Remove All
🗋 🎄 any (Network Group)	0.0.0.0/0,::/0	NET ~ 1 Object	NET ~ 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			

図 5.FQDNオブジェクトを含むACPルール

ステップ 5: Devices > Device ManagementでFTDに移動し、Routingタブを選択して、Policy Based Routingセクションに移動します。

cisco	Firewall Management Center Devices / Secure Firewall Routing		Q Search	Dep	Noy 🥝	ø	? adr	nin ~
Hom	10.100.150.33						Save	Cancel
	Cisco Secure Firewall Threat Defense I	for VMware						
Overvi	sw Device interfaces millions	Policy Based Routing						
-III Analy:	is Manage Virtual Routers	Specify ingress interfaces, match criteria and egress interfaces	ces to route traffic accordingly. Traffic can be routed across Egress interfac	es accordingly	ure Interfac	e Priority	Add	
Polici	Virtual Router Properties	Ingress Interfaces	Match criteria and forward action					
=	ECMP BFD	For step-by-step	guidance on configuring a policy-based routing policy and adding applicat	e. tions, launch the How-To.				
Devio	OSPF OSPFv3							
Objec	ts EIGRP							
de Integra	Policy Based Routing							
	V BGP IPv4							
	IPv6							
	<ul> <li>Multicast Routing</li> </ul>							
	101 10							
図 6	.PBRメニュー							

手順6:以前に設定したACLを使用してインターフェイスにPBRを設定し、展開します。

Add Forwar	rding Actions					(?
Match ACL: *	fqdn	~ +	-			
Send To: *	Egress Interfaces	~				
Interface Orderin	Interface Priority	~ 0				
Available Interfaces	i		Selected Egre	ss Interfaces *		
Search by interface	e name	Q	Priority	Interface		
Priority	Interface		0	outside	Ū	_
0	inside	+				
					Cancel	ave

図 7.PBRインターフェイスとACL選択メニュー

手順 7: Objects > Object Management > FlexConfig > Objectの順に選択し、新しいオブジェクト を作成します。

uluilu cisco	Firewall Management Cente Objects / Object Management	Q Search	Deploy 🥑 🚫
		Add FlexConfig Object (3)	Dbject Q Filter
Home	> AAA Server	Name:	
Overview	Access List     Address Pools     Application Filters	Description:	
dd	AS Path		
Analysis	BFD Template		VS with the help of TextOr
	Cipher Suite List	Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.	to martine map or restor
Policies	> Community List		ection.
	DHCP IPv6 Pool	Insert Deployment: Everytime Type: Append	ction.
-	> Distinguished Name	Insert Policy Object > Text Object	le (PD client) and one insid
Devices	DNS Server Group	Insert System Variable >> Network	n of one outside (PD clien
•	> External Attributes	Insert Secret Key Security Zones	the help of TextOhiects dr
Objects	File List	Standard ACL Object	ine help of rexcollects a
	✓ FlexConfig	Extended ACL Object	nfigurations.
	FlexConfig Object	Perita Man	Configures next hop. 2. co
integratic	Text Object	Route Map	parameters for eigrp. 1. C
	Geolocation	∨ Variablae	ration for an AS
	Interface	tanaanoa	ration.
	Key Chain	Name Dimension Default Value Property Override Description	
	Network	(Type:Name)	i for ipv6 traffic. Used text
	> PKI	Mn snorste to dienless	
	Policy List	Cancel Save	20 of 48 rows
	Port		

図 8.FlexConfigオブジェクト設定メニュー

ステップ 8 : Insert > Extended ACL Objectの順に選択し、変数に名前を付け、前に作成した拡張 ACLを選択します。変数が使用した名前で追加されます。

# Insert Extended Access List Object Variable



Cancel Save

3

図 9.FlexConfigオブジェクトの変数の作成

ステップ9:ACLに追加する各FQDNオブジェクトに対して、この行を入力します。

<#root>

access-li \$

extended permit ip any object

ステップ 10 : FlexConfigオブジェクトをEverytime > Appendとして保存します。

ステップ11:Devices > FlexConfigの下にあるFlexConfig Policyメニューに移動します。



図 10.FlexConfigポリシーメニューへのパス

ステップ 12新しいFlexConfigポリシーを作成するか、FTDにすでに割り当てられているポリシー を選択します。

Home				New Policy
	FlexConfig Policy	Status	Last Modified	_
Overview	test flex	Targeting 1 device(s) Up-to-date on all targeted devices	2024-10-14 11:59:39 Modified by "admin"	<u>б</u> Ø Ъ́
Analysis				_
Policies				
Devices				

### 図 11.新しいFlexConfigポリシーの編集または作成

ステップ 13FlexConfigオブジェクトをポリシーに追加し、保存して展開します。

	00110	Cancel
Home Enter Description		
Point	cy Assignm	ients (1)
III (S) # Name Description		
V User Defined		_
Devices		
Default_Inspection_Protocol_Enable     Default_Inspection_Configure     Boundary Configure     Selected Append FlexConfigs		
Objects     DHCPv6_Prefix_Delegation_UnConfiguré       Image: Dht		
Integration	Q	Ū

図 12.FlexConfigオブジェクトをFlexConfigポリシーに追加

# 確認

入力インターフェイスには、自動生成されたルートマップを持つポリシールートがあります。

### <#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

ルートマップには、使用されている宛先インターフェイスを持つ選択されたACLが含まれています。

### <#root>

firepower#

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

!

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

match ip address fqdn

set adaptive-interface cost outside

アクセスリストには、参照用のホストと、FlexConfigを使用して追加した追加ルールが含まれて います。

#### <#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

送信元として入力インターフェイスからパケットトレーサを実行して、PBRフェーズに到達した ことを確認できます。

### <#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

```
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
Found next-hop 10.100.150.1 using egress ifc outside
[...]
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

Elapsed time: 1137 ns

# 一般的な問題

### 2回目の導入の後でPBRが動作しなくなる

アクセスリストにまだFQDNオブジェクトルールが含まれているかどうかを確認してください。 この場合、ルールがもはやここにないことを確認できます。

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

FlexConfigオブジェクトがDeployment: Everytime およびType: Appendとして設定されていることを確認します。このルールは、今後の展開で毎回適用されます。

### FQDNが解決されない

FQDNにpingを実行しようとすると、無効なホスト名に関するメッセージが表示されます。

<#root>

firepower#

ping cisco.com

٨

ERROR: % Invalid Hostname

DNS設定を確認します。到達可能なDNSサーバがサーバグループに存在し、ドメインルックアップインターフェイスがそれらに到達できる必要があります。

```
<#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. 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。