# **Configure FQDN Object on Extended ACL for PBR on FMC**

# Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
<u>Configure</u>
<u>Verify</u>
Common Issues
PBR Stops Working After a Second Deployment
FQDN does not Resolve

## Introduction

This document describes the procedure to configure a FQDN object in an extended Access-list (ACL) for use in Policy Based Routing (PBR).

# Prerequisites

## Requirements

Cisco recommends that you have knowledge of these products:

- Secure Firewall Management Center (FMC)
- Secure Firewall Threat Defense (FTD)
- PBR

### **Components Used**

The information in this document is based on these software and hardware versions:

- Firepower Threat Defense for VMware version 7.6.0
- Secure Firewall Management Center for VMware version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# **Background Information**

Currently, FTD does not allow filtering on non-HTTP traffic using Fully Qualified Domain Name (FQDN) objects as mentioned on Cisco bug ID <u>CSCuz98322</u>.

This functionality is supported on ASA platforms, however, only networks and applications can be filtered on FTD.

(2)

You can add a FQDN object to an extended access-list to configure PBR using this method.

# Configure

Step 1. Create FQDN objects as needed.

## Edit Network Object

Name	
cisco.com	
Description	
Network	
Host     Range     Network	FQDN
cisco.com	
<ul> <li>Note: You can use FQDN network objects in ac</li> </ul>	cess, prefilter and translated destination in NAT rules only.
Lookup:	
solve within IPv4 addresses only 👻	
Allow Overrides	
	Cancel Save

Image 1. Network Object Menu

Step 2. Create an extended access-list under **Objects > Object Management > Access List > Extended**.

>	AAA Server	Extended	Add Extended Access List	Q Filter
~	Access List Extended	An access list object, a and destination addres	Iso known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address o s and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.	only. Identifies traff
	Standard			
>	Address Pools	Name	Value	Override
	Application Filters		Ne seconde te disalas:	
	AS Path		No records to display	
	BFD Template			
	Cipher Suite List			
>	Community List			

Image 2. Extended Access List Menu

When you add a new rule, notice that you cannot see the FQDN object you configured when doing a search on the Network Objects to select source and destination.

Edit Extended Access List Entry				0
C Allow				
Logging:				
Default				
Log Level:				
Informational v				
Log Interval:				
300 Sec.	2.			
Network Port	Users 0 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	Enter an IP address	4
			Cancel Sav	e

Image 3. New Extended Access List Rule Menu

Step 3. Create a rule that cannot be hit so the extended ACL is created and available for PBR configuration.

#### Add Extended Access List Entry

Action:					
Allow ~					
Logging:					
Default					
Log Level:					
Informational ~					
Log Interval:					
300 Sec.					
Network Port  Application U	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					
	1	1	1	1	
					Cancel Add

Image 4. Access List Rule Configuration that Cannot Be Hit

Step 4. You need to create a rule on the Access-Control Policy (ACP) targeting your FTD with the FQDN object. The FMC deploys the FQDN object to the FTD so you can reference it through a FlexConfig object.

1 🗘 Add Rule					0
Name New-Rule-#1-ALLOW	Action	C Allow	Logging OFF	None V Rule Enabled	
Insert into Mandatory 🗸	Intru	sion Policy None	Variable Set	V File Policy None	~
Q Zones Networks (2) Ports Applications Use	ers URLs Dynamic Attributes	VLAN Tags			
Q. Search Network and Geolocation Objects	Showing 15 out of 15	Selected Sources: 1	Q Select	ted Destinations and Applications: 1	٩
Networks Geolocations		Collapse All	Remove All Collap	ase All Re	move All
& any (Network Group)	0.0.0/0,::/0	NET v 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				

Image 5. ACP Rule with FQDN Object

Step 5. Navigate to the FTD on **Devices > Device Management** and select the **Routing** tab and navigate to **Policy Based Routing** section.

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
Overvier	w Device Interfaces Inline S	Sets Routing DHCP VTEP						
ilil Analysi	s Global V	Policy Based Routing Specify ingress interfaces, match criteria and egre	ess interfaces to route traffic accordingly. Traffic c	an be routed across Egress interfaces accordingly	Configure In	terface i	Priority	Add
Policies	Virtual Router Properties ECMP	Ingress Interfaces	Match criteria and forward action There are no PBR policies defined	yet. Start by defining the first one.				
Devices	BFD OSPF	FOF SU	p-oy-step guidance on configuring a policy-based	routing policy and adding applications, launch the How-	10.			
©≞ Objects	OSPFv3 EIGRP							
🍰 Integratio	Policy Based Routing							
	IPv4							
	IPv6							
	Static Route							
	<ul> <li>Multicast Routing</li> </ul>							



Step 6. Configure the **PBR** on an interface using the ACL configured earlier and deploy.

Add Forw	arding Actions						0
Match ACL: *	fqdn	~	F				
Send To: *	Egress Interfaces	~					
Interface Orderin	Interface Priority	~ 0					
Available Interfac	ces		Se	lected Egress	Interfaces *		
Search by inter	face name	Q		Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Save

Image 7. PBR Interface and ACL Selection Menu

Step 7. Navigate to **Objects > Object Management > FlexConfig > Object** and create a **new object**.

uluulu cisco	Firewa Objects /	all Mar Object	nagement Center Management								Q Search	h		Deploy 🥑 🚫
Home		,	AAA Server	A	dd FlexC	onfig Ok	oject						0	Dbject Q Filter
Overvie	ew	>	Access List Address Pools Application Filters		me: qdn scription:									
ilil Analys	iis		AS Path BFD Template Cipher Suite List		Copy-pastin	g any rich text	might introduce line break	s while generating CLI	I. Please verify the	CLI before deplo	/ment.			VS with the help of TextO
Policie	25	>	Community List DHCP IPv6 Pool	F	Insert ~	biect	loyment: Everytime	) )	Type:	Append	Ŷ			ection. ction.
Device	es	>	DNS Server Group	L î	Insert System	Variable >	Network							n of one outside (PD clien
Object	ts	, ,	External Attributes File List		Insert Secret k	'ey	Security Zones Standard ACL Object							the help of TextObjects dr nfigurations.
â. Integrat	tion	Ť	FlexConfig Object Text Object	L			Extended ACL Object Route Map							Configures next hop. 2. co parameters for eigrp. 1. C
			Geolocation Interface	~ 1	Variables									ration for an AS
			Key Chain Network		Name		Dimension	Default Value	Property (Type:Name)	Override	Description		_	i for ipv6 traffic. Used text
		>	PKI Policy List Port					no rocorde tr	- Provident			Cancel	Save	20 of 48 rows I < < Page

Image 8. FlexConfig Object Configuration Menu

Step 8. Select **Insert > Extended ACL Object**, name your **variable** and select your **extended ACL** you created earlier. The variable is added with the name you used.

# Insert Extended Access List Object Variable



Cancel Save

3

Image 9. Variable Creation for FlexConfig Object

Step 9. Enter this line for each FQDN object you want to your ACL.

<#root>

access-li \$<your\_ACL\_variable> extended permit ip any object <your\_FQDN\_object\_name>

Step 10. Save your **FlexConfig Object** as **Everytime > Append**.

Step 11.Navigate to the **FlexConfig Policy** menu under **Devices** > **FlexConfig**.



Image 10. Path to FlexConfig Policy Menu

Step 12. Create a new **FlexConfig Policy** or select a **Policy** already assigned to your FTD.

New Lastendar Nephysikerst Disk of USA Der Der Frager ander

Image 11. Edit or Create a New FlexConfig Policy

Step 13. Add your **FlexConfig object** to the Policy, **save** and **deploy**.

~	test flex				Migrate Config Preview Config Save Cance
Home	Enter Description				
Overview	Available FlexConfig C FlexConfig Object		Selected Prepend Fle	exConfigs	Policy Assignments (1)
III Analysis	8		# Name	Description	
Patialas	✓ User Defined The second				
Policies	<ul> <li>System Derined</li> <li>Default_DNS_Configure</li> </ul>				
Devices	Default_Inspection_Protocol_Disable	>			
•=	DHCPv6_Prefix_Delegation_Configure		Selected Append Fle	xConfigs	
Objects	DHCPv6_Prefix_Delegation_UnConfigure			Bernsteller	
1ntegration	DNS_Configure		# Name 1 fqdn	Description	QŰ

Image 12. Added FlexConfig Object into FlexConfig Policy

# Verify

Your ingress interface has the policy-route with auto-generated route-map.

```
<#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
```

The route-map contains the selected ACL with the used destination interface.

<#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

Your access list contains the host used for reference and the additional rule you added through FlexConfig.

<#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

You can do a packet tracer from the ingress interface as a source to verify you hit the PBR phase.

<#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

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
```

## **Common Issues**

#### **PBR Stops Working After a Second Deployment**

Please verify if the access-list still contains the FQDN object rule.

In this case, you can see the rule is no longer here.

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

Verify that the FlexConfig Object is set up as **Deployment: Everytime** and **Type: Append**. The rule is applied every time on future deployments.

#### **FQDN** does not Resolve

When you attempt to ping the FQDN, you get a message about invalid hostname.

<#root> firepower# ping cisco.com ^ ERROR: % Invalid Hostname

Verify DNS configuration. You must have reachable DNS servers on your server group, and the domainlookup interfaces must be able to reach them.

<#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.