# Configurar objeto FQDN na ACL estendida para PBR no FMC

# Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Verificar
Problemas comuns
O PBR pára de funcionar após uma segunda implantação
FQDN não Resolve

# Introdução

Este documento descreve o procedimento para configurar um objeto FQDN em uma lista de acesso estendida (ACL) para uso no Roteamento Baseado em Políticas (PBR - Policy Based Routing).

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

- · Centro de gerenciamento seguro de firewall (FMC)
- Defesa contra ameaças de firewall (FTD) segura
- PBR

## **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Threat Defense para VMware versão 7.6.0
- Secure Firewall Management Center for VMware versão 7.6.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

Atualmente, o FTD não permite a filtragem de tráfego não HTTP usando objetos Fully Qualified Domain Name (FQDN), conforme mencionado no bug da Cisco ID <u>CSCuz98322</u>.

Essa funcionalidade é suportada em plataformas ASA, no entanto, somente redes e aplicativos podem ser filtrados no FTD.

Você pode adicionar um objeto FQDN a uma lista de acesso estendida para configurar o PBR usando esse método.

2.

# Configurar

Etapa 1. Crie objetos FQDN conforme necessário.

## Edit Network Object

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

Imagem 1. Menu do objeto de rede

Etapa 2. Crie uma lista de acesso estendida em Objetos > Gerenciamento de objetos > Lista de

#### acesso > Estendida.

AAA Server     Access List     Extended	Extended An access list object, also and destination address ar	known as an access control list (ACL), selects the traffic to which a servi Id ports. Supports IPv4 and IPv6 addresses. You use these objects wher	Add ice will apply. Standard-Identifies traffic based a configuring particular features, such as route	on destination address only. Identifies traff
Standard > Address Pools	Name		Value	Override
Application Filters AS Path		No re	cords to display	
Cipher Suite List				

### Imagem 2. Menu da Lista de Acesso Estendida

Ao adicionar uma nova regra, observe que você não pode ver o objeto FQDN configurado ao fazer uma pesquisa nos Objetos de Rede para selecionar a origem e o destino.

Ear Extended / tooooo Elot Entry			Ø	)
C Allow 🔻				
Logging:				
Default <b>•</b>				
Log Level:				
Informational 👻				
Log Interval:				
300 Sec.				
Network Port	Security Group Tag			
	7	Source Networks (0)	Destination Networks (0)	
Available Networks C* +		Source Networks (0)	Desunation Networks (0)	
Available Networks C <sup>a</sup> +		any	any	
Available Networks C + Q cisco ×	Add to Source	any	any	
Available Networks C* +	Add to Source Add to Destination	any	any	
Available Networks C <sup>a</sup> + Q cisco X	Add to Source Add to Destination	any	any	
Available Networks (* +	Add to Source Add to Destination	any	any	
Available Networks (* +	Add to Source Add to Destination	any	any	
Available Networks (* +	Add to Source Add to Destination	any	any	
Available Networks (* +	Add to Source Add to Destination	any Enter an IP address	any Enter an IP address Add	
Available Networks (* +	Add to Source Add to Destination	any Enter an IP address Add	Enter an IP address Add	

Imagem 3. Novo Menu de Regra da Lista de Acesso Estendida

Etapa 3. Crie uma regra que não possa ser atingida para que a ACL estendida seja criada e disponibilizada para a configuração do PBR.

#### Add Extended Access List Entry

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

Imagem 4. Configuração de regra de lista de acesso que não pode ser atingida

Etapa 4. Você precisa criar uma regra na ACP (Access-Control Policy, Política de controle de acesso) direcionando seu FTD com o objeto FQDN. O FMC implanta o objeto FQDN no FTD para que você possa referenciá-lo por meio de um objeto FlexConfig.

1 🗘 Add Rule	٥
Name New-Rule-#1-ALLOW Action	Allow     Allow     Ison Policy     None     Variable Set     Elle Policy     None     Set
Q Zones Networks (2) Ports Applications Users URLs Dynamic Attributes	VLAN Tags
C 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
A any (Network Group) 0.0.0.0/0,::/0	NET v 1 Object NET v 1 Object
any-ipv4 (Network Object) 0.0.0.0/0	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	

Imagem 5. Regra ACP com Objeto FQDN

Etapa 5. Navegue até o FTD em Devices > Device Management e selecione a guia Routing e navegue até a seção Policy Based Routing .

cisco	Firewall Management Center Devices / Secure Firewall Routing			Q Search	Deploy	<b>e</b> (	9 9	admin ~
Home	10.100.150.33 Cisco Secure Firewall Threat Defense f	for VMware						Cancel
Uvervie	ew Device Interfaces Inline S	Routing DHCP VTEP						
ilil Analys	is Manage Virtual Routers	Policy Based Routing Specify ingress interfaces, match criteria and egress int	terfaces to route traffic accordingly. Traffic	c can be routed across Egress interfaces accordingly	Configure In	iterface Pri	iority	Add
Policie	Virtual Router Properties	Ingress Interfaces	Match criteria and forward action There are no PBR policies defin	ed yet. Start by defining the first one.				
Device	BFD OSPF	For step-by	<ul> <li>step guidance on configuring a policy-ba</li> </ul>	sed routing policy and adding applications, launch the How	-То.			
●_= Object	OSPFv3 ts EIGRP							
🍰 Integrat	Policy Based Routing							
	IPv4							
	IPv6							
	V Multicast Routing							
	in in							

## Imagem 6. Menu PBR

Etapa 6. Configure o PBR em uma interface usando a ACL configurada anteriormente e implante.

Add Forwar	ding Actions						(?)
Match ACL: *	fqdn	~ -	-				
Send To: *	Egress Interfaces	~					
Interface Orderin	Interface Priority	~ 3					
Available Interfaces			Se	lected Egress	Interfaces *		
Search by interface	name	Q		Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Save

Imagem 7. Interface PBR e menu de seleção de ACL

Passo 7. Navegue até Objetos > Gerenciamento de objetos > FlexConfig > Objeto e crie um novo objeto.

uluulu cisco	Firewall Management Center Objects / Object Management			Q Search		Deploy 📀 🐼
Home	> AAA Server	Add FlexConfig Object			٢	Dbject Q Filter
Overvie	Access List     Address Pools     Address Pools     Application Filters	rame: fqdn Description:				
ilil Analysi	AS Path IS BFD Template Cipher Suite List	Copy-pasting any rich text might introduce line br	aks while generating CLI. Please verify the C	LI before deployment.		NS with the help of TextOl
Policie	s > Community List DHCP IPv6 Pool	Insert V E Deployment: Everytime	V Type: Ap	spend v		ection.
Device	Distinguished Name     DNS Server Group	Insert System Variable > Network				n of one outside (PD clien
Object	s File List	Security Zones Standard ACL Object				the help of TextObjects de
🍰 Integrati	ion Text Object	Extended ACL Object Route Map				Configures next hop. 2. co parameters for eigrp. 1. C
	Geolocation	∨ Variables				ration for an AS
	Key Chain Network	Name Dimension	Default Value Property (Type:Name)	Override Description	_	i for ipv6 traffic. Used text
	Policy List Port			Cancel	Save	20 of 48 rows  < < Page

Imagem 8. Menu de configuração do objeto FlexConfig

Etapa 8. Selecione Insert > Extended ACL Object, nomeie sua variável e selecione sua ACL estendida criada anteriormente. A variável é adicionada com o nome que você usou.

# Insert Extended Access List Object Variable



Cancel Save

3

Imagem 9. Criação de variável para objeto FlexConfig

Etapa 9. Insira esta linha para cada objeto FQDN que deseja acessar sua ACL.

<#root>

access-li \$

extended permit ip any object

Etapa 10. Salve o Objeto FlexConfig como Todos os dias > Anexar.

Etapa 11.Navegue até o menu FlexConfig Policy em Devices > FlexConfig.



Imagem 10. Caminho para o menu de política FlexConfig

Etapa 12. Crie uma nova Política FlexConfig ou selecione uma Política já atribuída ao seu FTD.

- Imagem 11. Editar ou criar uma nova política do FlexConfig
- Etapa 13. Adicione o objeto FlexConfig à política, salve e implante.

	test flex						Migrate Config Preview Config Savo Cance
Home	Enter Description						
Overview	Available FlexConfig C* FlexConfig Object		"à Sel	lected Prepend Flo	exConfigs		Policy Assignments (1)
dil	8	)	#	Name		Description	
Analysis	✓ User Defined		_				
Policies	i fqdn						
Devices	Default_DNS_Configure	A					
•=	DHCPv6_Prefix_Delegation_Configure			lected Append Fle	xConfigs		
Objects	DHCPv6_Prefix_Delegation_UnConfigur	¢	_				
1ntegration	BDNS_Configure DNS_UnConfigure Bigrp_Configure		1	Name fqdn		Description	QŪ

Imagem 12. Objeto FlexConfig adicionado à política FlexConfig

## Verificar

Sua interface de entrada tem a rota de política com o mapa de rota gerado automaticamente.

#### <#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

O mapa de rota contém a ACL selecionada com a interface de destino usada.

#### <#root>

firepower#

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

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

match ip address fqdn

Sua lista de acesso contém o host usado para referência e a regra adicional adicionada por meio do 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

Você pode fazer um packet tracer a partir da interface de entrada como uma origem para verificar se atingiu a fase PBR.

#### <#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

## Problemas comuns

O PBR pára de funcionar após uma segunda implantação

Verifique se a lista de acesso ainda contém a regra de objeto FQDN.

Nesse caso, você pode ver que a regra não está mais aqui.

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

Verifique se o objeto FlexConfig está configurado como Deployment: Everytime e Type: Append. A regra é aplicada sempre em implantações futuras.

#### FQDN não Resolve

Ao tentar fazer ping no FQDN, você recebe uma mensagem sobre o nome de host inválido.

<#root>
firepower#
ping cisco.com

ERROR: % Invalid Hostname

Verifique a configuração do DNS. Você deve ter servidores DNS acessíveis em seu grupo de servidores, e as interfaces de pesquisa de domínio devem ser capazes de acessá-los.

<#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.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.