Configuración del objeto FQDN en la ACL extendida para PBR en FMC

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Verificación
Problemas comunes
PBR deja de funcionar después de una segunda implementación
FQDN no resuelto

Introducción

Este documento describe el procedimiento para configurar un objeto FQDN en una lista de acceso ampliada (ACL) para su uso en el routing basado en políticas (PBR).

Prerequisites

Requirements

Cisco recomienda que conozca estos productos:

- Centro de gestión de firewall seguro (FMC)
- Protección frente a amenazas de firewall (FTD)
- PBR

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower Threat Defense para VMware versión 7.6.0
- Secure Firewall Management Center para VMware versión 7.6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Actualmente, el FTD no permite filtrar el tráfico no HTTP mediante objetos de nombre de dominio completo (FQDN), como se menciona en el ID de error de funcionamiento de Cisco <u>CSCuz98322</u>.

Esta funcionalidad es compatible con las plataformas ASA, sin embargo, solo las redes y las aplicaciones se pueden filtrar en FTD.

Puede agregar un objeto FQDN a una lista de acceso ampliada para configurar PBR mediante este método.

Configurar

Paso 1. Cree objetos FQDN según sea necesario.

Edit Network Object

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

Imagen 1. Menú Objeto de red

Paso 2. Cree una lista de acceso ampliada en Objetos > Administración de objetos > Lista de

acceso > Ampliada.

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 w ind ports. Supports IPv4 and IPv6 addresses. You use these objects when con	Add Extended Acc will apply. Standard-Identifies traffic based on destination nfiguring particular features, such as route maps.	ess List Q. Filter
Standard > Address Pools	Name		Value	Override
Application Filters AS Path BFD Template		No record	is to display	
Cipher Suite List				

Imagen 2. Menú de lista de acceso ampliado

Al agregar una nueva regla, observe que no puede ver el objeto FQDN configurado al realizar una búsqueda en los objetos de red para seleccionar el origen y el destino.

Edit Extended Access List Entry		0
C Allow 🔻		
Logging:		
Default		
Log Level:		
Informational v		
Log Interval:		
300 Sec.		
Network Port Application Users Sec	curity Group Tag	
Available Networks C ⁴ +	Source Networks (0)	Destination Networks (0)
Available Networks C* +	Source Networks (0) any	Destination Networks (0) any
Available Networks C [*] + C cisco ×	Source Networks (0) any dd to Source	Destination Networks (0) any
Available Networks C [*] +	Id to Source Active (0)	Destination Networks (0) any
Available Networks (* + Q. cisco × Ac	dd to Source Aetworks (0) any dd to Destination	Destination Networks (0)
Available Networks (* + Q cisco X) Ac	Source Networks (0) any dd to Source	Destination Networks (0)
Available Networks C ⁴ + Q cisco X Ac	Source Networks (0) any dd to Source dd to Destination	Destination Networks (0)
Available Networks (? + Q. cisco X Ac	dd to Source dd to Destination	Destination Networks (0)
Available Networks (* + Q cisco X Available Networks (* Ac	Source Networks (0) any dd to Source	Add Enter an IP address Add
Available Networks (* + Q cisco X Ac	Source Networks (0) any Enter an IP address	Add Enter an IP address Add
Available Networks (* + Q cisco X Available Networks (* + Q cisco X Ac	Source Networks (0) any dd to Source dd to Destination Enter an IP address	Destination Networks (0) any Add Enter an IP address Add Cancel Save

Imagen 3. Nuevo menú de reglas de lista de acceso ampliada

Paso 3. Cree una regla que no se pueda alcanzar para que la ACL extendida se cree y esté disponible para la configuración PBR.

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 😋 🛛 +		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

Imagen 4. Configuración de regla de lista de acceso que no se puede alcanzar

Paso 4. Debe crear una regla en la política de control de acceso (ACP) dirigida a su FTD con el objeto FQDN. El FMC implementa el objeto FQDN en el FTD para que pueda hacer referencia a él a través de un objeto FlexConfig.

1 Add Rule	0
Name New-Rule-#1-ALLOW	ction 💽 Allow 🔍 🖬 Logging OFF 🖪 Time Range None 🔍 Rule Enabled
Insert into Mandatory 🗸	Intrusion Policy None Variable Set V B. File Policy None V
Q Zones Networks (2) Ports Applications Users URLs Dynamic Attri	vutes 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,::/	NET ~ 1 Object NET ~ 1 Object
any-ipv4 (Network Object) 0.0.0.0/	cisco.com cisco.com
any-ipv6 (Host Object) :://	
cisco.com (Network FQDN Object) cisco.com	
IPv4-Benchmark-Tests (Network Object) 198.18.0.0/1	

Imagen 5. Regla ACP con Objeto FQDN

Paso 5. Navegue hasta el FTD en Devices > Device Management y seleccione la pestaña Routing y navegue hasta la sección Policy Based Routing .

cisco	Firewall Management Center Devices / Secure Firewall Routing			Q Search	Deploy	ତ ଏ	୬ ⑦	admin ~
Home	10.100.150.33 Cisco Secure Firewall Threat Defense f	for VMware						Cancel
Uvervie	w Device Interfaces Inline S	Ets Routing DHCP VTEP						
ilil Analys	is Global ~	Policy Based Routing Specify ingress interfaces, match criteria and egress interfaces.	erfaces to route traffic accordingly. Traffic car	n be routed across Egress interfaces accordingly	Configure In	terface Pri	ority	Add
Policie	s Virtual Router Properties ECMP	Ingress Interfaces	Match criteria and forward action There are no PBR policies defined y	ret. Start by defining the first one.				
Device	BFD OSPF	For step-by-	step guidance on configuring a policy-based	routing policy and adding applications, launch the How-1	0.			
●_ Object	OSPFv3 s EIGRP							
the Integration	Policy Based Routing							
	IPv4							
	IPv6							
	Multicast Boution							
	in in the second s							

Imagen 6. Menú PBR

Paso 6. Configure el PBR en una interfaz usando la ACL configurada anteriormente e impleméntelo.

Add Forwar	rding Actions						(
Match ACL: *	fqdn	~	+				
Send To: *	Egress Interfaces	~					
Interface Orderin	Interface Priority	~ 0)				
Available Interfaces			Se	elected Egress	Interfaces *		
Search by interface	e name			Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Sava
						Cancel	Save

Imagen 7. Menú de selección de ACL e interfaz PBR

Paso 7. Navegue hasta Objetos > Administración de objetos > FlexConfig > Objeto y cree un nuevo objeto.

uluulu cisco	Firewall Management Center Objects / Object Management			Q Sea	rch	Deploy 🥝 🚫
Home	> AAA Server	Add FlexConfig Object	t		(2)	Dbject Q Filter
Overvie	Access List Address Pools Application Filters	fqdn Description:				
ili Analys	AS Path BFD Template Cipher Suite List	Copy-pasting any rich text might	introduce line breaks while generating CLI.	Please verify the CLI before deployment.		VS with the help of TextO
Policie	s > Community List DHCP IPv6 Pool	Insert V E Deploymen	nt: Everytime v	Type: Append		ection. ction.
Device	S DNS Server Group	Insert System Variable > Net	work			n of one outside (PD clien
Object	> External Attributes s File List	Insert Secret Key Secret Secret Key	urity Zones Idard ACL Object			the help of TextObjects dr
3 Integrati	FlexConfig FlexConfig Object Text Object	Exte	nded ACL Object te 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
	> PKI Policy List Port		Min zooozele to	Allen et hus	Cancel Save	20 of 48 rows < < Page

Imagen 8. Menú de configuración de objetos FlexConfig

Paso 8. Seleccione Insert > Extended ACL Object, asigne un nombre a la variable y seleccione la ACL extendida que creó anteriormente. La variable se agrega con el nombre que ha utilizado.

Insert Extended Access List Object Variable



Cancel Save

3

Imagen 9. Creación de variables para el objeto FlexConfig

Paso 9. Introduzca esta línea para cada objeto FQDN que desee agregar a su ACL.

<#root>

access-li \$

extended permit ip any object

Paso 10. Guarde el objeto FlexConfig como Everytime > Append.

Paso 11.Vaya al menú Política de FlexConfig en Dispositivos > FlexConfig.



Imagen 10. Ruta al menú de la política FlexConfig

Paso 12. Cree una nueva política FlexConfig o seleccione una política ya asignada a su FTD.

Imagen 1. Editar o crear una nueva política FlexConfig

Paso 13. Agregue su objeto FlexConfig a la directiva, guarde e implemente.

~	test flex				Migrate Config Preview Config Save Cancel
Home	Enter Description				
Overview	Available FlexConfig C FlexConfig Object		Selected Prepend Fle	xConfigs	Policy Assignments (1)
dil			# Name	Description	
Analysis	V User Defined				
Policies	System Defined				
Devices	Default_DNS_Configure Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable	>			
•_=	DHCPv6_Prefix_Delegation_Configure		Selected Append Flex	xConfigs	
Objects	DHCPv6_Prefix_Delegation_UnConfigure				
1ntegration	DNS_Configure DNS_UnConfigure		# Name 1 fqdn	Description	QŪ

Imagen 12. Se ha agregado el objeto FlexConfig a la política FlexConfig

Verificación

Su interfaz de ingreso tiene la ruta de política con route-map generado automáticamente.

<#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

El route-map contiene la ACL seleccionada con la interfaz de destino utilizada.

<#root>

firepower#

show run route-map FMC_GENERATED_PBR_1727116778384

!
route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn

La lista de acceso contiene el host utilizado como referencia y la regla adicional que ha agregado mediante 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

Puede hacer un seguimiento de paquetes desde la interfaz de ingreso como fuente para verificar que se alcanza la 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 comunes

PBR deja de funcionar después de una segunda implementación

Verifique si la lista de acceso aún contiene la regla de objeto FQDN.

En este caso, puede ver que la regla ya no está aquí.

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

Verifique que el objeto FlexConfig esté configurado como Deployment: Everytime y Type: Append. La regla se aplica cada vez en futuras implementaciones.

FQDN no resuelto

Cuando intenta hacer ping al FQDN, aparece un mensaje sobre un nombre de host no válido.

<#root>
firepower#
ping cisco.com
^

ERROR: % Invalid Hostname

Verifique la configuración de DNS. Debe tener servidores DNS accesibles en su grupo de servidores y las interfaces de búsqueda de dominio deben poder alcanzarlos.

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

<#root>

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.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).