FQDN-object op uitgebreide ACL voor PBR op FMC configureren

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Configureren
Verifiëren
Veelvoorkomende problemen
PBR stopt met werken na een tweede implementatie
FQDN lost niet op

Inleiding

Dit document beschrijft de procedure om een FQDN-object in een uitgebreide toegangslijst (ACL) te configureren voor gebruik in op beleid gebaseerde routing (PBR).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze producten:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Threat Defence voor VMware versie 7.6.0
- Secure Firewall Management Center voor VMware versie 7.6.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Op dit moment is het niet toegestaan om op niet-HTTP verkeer te filteren met FFull Qualified Domain Name (FQDN)-objecten zoals vermeld op Cisco bug-id <u>CSCuz98322</u>.

Deze functionaliteit wordt ondersteund op ASA-platforms, maar alleen netwerken en toepassingen kunnen worden gefilterd op FTD.

U kunt een FQDN-object toevoegen aan een uitgebreide toegangslijst om PBR met deze methode te configureren.

Configureren

Stap 1. Indien nodig FQDN-objecten maken.

Edit Network Object

	1		
• FQDN			
ccess, prefilter	and translated	destination in NA	T rules only.
		Cancel	Save
	FQDN cess, prefilter	FQDN cess, prefilter and translated	FQDN cess, prefilter and translated destination in NA Cancel

Afbeelding 1. Menu Netwerkobject

Stap 2. Maak een uitgebreide toegangslijst onder Objecten > Objectbeheer > Toegangslijst >

Uitgebreid.

> . ~ .	AAA Server Access List Extended	Extended An access list object, also k and destination address an	nown as an access control list (ACL), selects the traffic to which a service w I ports. Supports IPv4 and IPv6 addresses. You use these objects when con	Add Extended Access List ill apply. Standard-Identifies traffic based on destination address of figuring particular features, such as route maps.	Q Filter
>	Standard Address Pools	Name		Value	Override
-	Application Filters AS Path		No record:	s to display	
	BFD Template				
	Cipher Suite List				
>	Community List				

Afbeelding 2. Uitgebreid menu toegangslijst

Wanneer u een nieuwe regel toevoegt, merk op dat u het object FQDN niet kunt zien dat u hebt geconfigureerd tijdens het zoeken op de netwerkobjecten om bron en bestemming te selecteren.

Edit Extended Access List Entry		0
O Allow		
Logging:		
Default		
Log Level:		
Informational 🔹		
Log Interval:		
300 Sec.		
Network Port Application Users	Security Group Tag	
Available Networks C ^e +	Source Networks (0)	Destination Networks (0)
Q. cisco X	Add to Source Add to Destination	any
	Enter an IP address	Add Enter an IP address Add

Afbeelding 3. Nieuw menu Regel uitgebreide toegangslijst

Stap 3. Maak een regel die niet kan worden geraakt, zodat de uitgebreide ACL wordt gemaakt en beschikbaar is voor PBR configuratie.

Add Extended Access List Entry

Action:					
Logging:					
Default					
Log Level:					
Informational ~					
Log Interval:					
300 Sec.					
Network Port () Application () Us	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	1	1
					Cancel Add

Afbeelding 4. Configuratie van toegangslijst die niet kan worden geraakt

Stap 4. U moet een regel maken over het Access-Control Policy (ACS) dat uw FTD richt op het FQDN-object. Het FMC implementeert het FQDN-object naar het FTD zodat u het kunt doorverwijzen naar een FlexConfig-object.

1 🗘 Add Rule	٥
Name New-Rule-#1-ALLOW Act	on C Allow V Logging OFF 5 Time Range None V Rule Enabled
Q Zones Networks (2) Ports Applications Users URLs Dynamic Attribu	les VLAN Tags
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,::/0	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	

Afbeelding 5. ACS-regel met FQDN-object

Stap 5. Navigeer naar de FTD on Devices > Device Management en selecteer het Routing tabblad en navigeer naar de sectie Policy Based Routing.

cisco	Firewall Management Center Devices / Secure Firewall Routing			Q Search	Deploy	0	0		admin ~
Home	10.100.150.33 Cisco Secure Firewall Threat Defense	for VMware							Cancel
Uvervie	Device Interfaces Inline S	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 routed acros	ss Egress interfaces accordingly	Configure In	terface	Priority	Ad	٩
Policie	virtual Router Properties	Ingress Interfaces	Match criteria and forward action There are no PBR policies defined yet. Start by def	ining the first one.				-	
Device	BFD OSPF	For step-by-step	guidance on configuring a policy-based routing policy an	d adding applications, launch the How-To	5 .				
Object	OSPFv3 ts EIGRP								
ntegrat	Policy Based Routing								
	IPv4								
	IPv6								
	Static Route								
	ioung loung								

Afbeelding 6. PBR-menu

Stap 6. Configureer de PBR op een interface met de eerdere ACL en implementeer deze.

Add Forwar	ding Actions						?
Match ACL: *	fqdn	~ -	F				
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	Save

Afbeelding 7. PBR-interface en ACL-selectiemenu

Stap 7. Navigeer naar Objecten > Objectbeheer > FlexConfig > Object en maak een nieuw object.

altalta cisco	Firewall N Objects / Obj	lanager ect Manag	nent Center							Q Search	n		Deploy 📀 🙆
Home		> AAA SI	rver	Add Fle	exConfig Ol	bject						3	Dbject Q Filter
Overvie	w	 Access Address Applica 	List s Pools tion Filters	fqdn Description:									
ili Analysi	is	AS Pat BFD Te Cipher	n mplate Suite List	Copy-I	pasting any rich tex	t might introduce line breaks	while generating CLI.	Please verify the	CLI before deploy	ment.			VS with the help of TextO
Policie	s	> Comm DHCP	unity List Pv6 Pool	Insert ~	licy Object	Doloyment: Everytime)	Type:	Append	~)			ection. ction.
Device	s	> Disting	erver Group	Insert Sy	stem Variable	Network							n of one outside (PD clien
Object	s r	File Lis ElevCo	t	Insert Se	cret Key	Security Zones Standard ACL Object							the help of TextObjects d
j. Integrati	ion	Flex	Config Object			Extended ACL Object Route Map	J						Configures next hop. 2. co parameters for eigrp. 1. C
		Geoloc Interfa	ation	✓ Variables									ration for an AS
		Key Ch Netwo	ain k	Name		Dimension	Default Value	Property (Type:Name)	Override	Description		_	for ipv6 traffic. Used text
		 PKI Policy Port 	ist								Cancel	Save	20 of 48 rows I < < Page

Afbeelding 8. Configuratiemenu van FlexConfig-objecten

Stap 8. Selecteer Invoegen > Uitgebreid ACL-object, geef uw variabele een naam en selecteer de uitgebreide ACL die u eerder hebt gemaakt. De variabele wordt toegevoegd met de naam die u hebt gebruikt.

Insert Extended Access List Object Variable



Cancel Save

3

Afbeelding 9. Variabele maken voor FlexConfig-object

Stap 9. Voer deze regel in voor elk FQDN-object dat u aan uw ACL wilt toevoegen.

<#root>

access-li \$

extended permit ip any object

Stap 10. Sla uw FlexConfig-object op als altijd > Toevoegen.

Stap 1.Navigeer naar het menu FlexConfig-beleid onder Apparaten > FlexConfig.

Home	Devices		×
	Device Management	VPN	Troubleshoot
Overview	Template Management	Site To Site	File Download
III Analysis	NAT	Remote Access	Threat Defense CLI
	QoS	Dynamic Access Policy	Packet Tracer
Policies	Platform Settings	1	Packet Capture
	FlexConfig 🗸 🗸		Snort 3 Profiling
Devices	Certificates	•	Troubleshooting Logs
•=			
Objects			Upgrade
5			Threat Defense Upgrade
Integration			Chassis Upgrade

Afbeelding 10. Pad naar FlexConfig beleidsmenu

Stap 12. Maak een nieuw FlexConfig-beleid of selecteer een beleid dat al aan uw FTD is toegewezen.

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> ØЪ
⊣II Analysis				_
Policies				
Devices				

Afbeelding 11. Een nieuw FlexConfig-beleid bewerken of maken

Stap 13. Voeg uw FlexConfig-object toe aan het beleid, sla het op en implementeer het.

	test flex			Migrate Config	Preview Config Save Cancel
Home	Enter Description				
51					Policy Assignments (1)
Overview	Available FlexConfig C ^e FlexConfig Object	Selected Prepend Fle	exConfigs		
dil	8	# Name	Description		
Analysis	V User Defined				
0	🖺 fqdn				
Policies	Y System Defined				
	Default_DNS_Configure				
Devices	Default_Inspection_Protocol_Disable				
Devices	Default_Inspection_Protocol_Enable				
•=	DHCPv6_Prefix_Delegation_Configure	Selected Append Fle	xConfigs		
Objects	DHCPv6_Prefix_Delegation_UnConfigure				
	DNS_Configure	# Name	Description		
5 -		1 fgdn			QŪ
Integration	Eigrp_Configure				

Afbeelding 12. Toegevoegd FlexConfig-object in FlexConfig-beleid

Verifiëren

Uw toegangsinterface heeft de beleidsroute met auto-gegenereerde route-kaart.

<#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

De routekaart bevat de geselecteerde ACL met de gebruikte doelinterface.

```
<#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

Uw toegangslijst bevat de host die wordt gebruikt voor referentie en de extra regel die u hebt toegevoegd via 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

U kunt een pakkettracer vanuit de toegangsinterface als bron uitvoeren om te controleren of u de PBR-fase hebt geraakt.

<#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

Veelvoorkomende problemen

PBR stopt met werken na een tweede implementatie

Controleer of de toegangslijst nog steeds de FQDN-objectregel bevat.

In dit geval zie je dat de regel er niet meer is.

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

regel wordt elke keer toegepast op toekomstige implementaties.

FQDN lost niet op

Wanneer u probeert de FQDN te pingen, krijgt u een bericht over ongeldige hostname.

<#root>
firepower#
ping cisco.com
^

ERROR: % Invalid Hostname

Controleer de DNS-configuratie. U moet bereikbare DNS-servers op uw servergroep hebben, en de domein-lookup interfaces moeten ze kunnen bereiken.

<#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.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.