Configurer l'objet FQDN sur la liste de contrôle d'accès étendue pour PBR sur FMC

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Vérifier
Problèmes courants
PBR cesse de fonctionner après un second déploiement
FQDN ne résout pas

Introduction

Ce document décrit la procédure à suivre pour configurer un objet FQDN dans une liste de contrôle d'accès (ACL) étendue à utiliser dans le routage basé sur des politiques (PBR).

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des produits suivants :

- Centre de gestion du pare-feu sécurisé (FMC)
- Protection pare-feu contre les menaces (FTD)
- PBR

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Threat Defense pour VMware version 7.6.0
- Secure Firewall Management Center pour 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Actuellement, FTD ne permet pas le filtrage sur le trafic non-HTTP en utilisant des objets FQDN (Fully Qualified Domain Name) comme mentionné sur l'ID de bogue Cisco <u>CSCuz9832</u>.

Cette fonctionnalité est prise en charge sur les plates-formes ASA, mais seuls les réseaux et les applications peuvent être filtrés sur FTD.

Vous pouvez ajouter un objet FQDN à une liste de contrôle d'accès étendue pour configurer PBR à l'aide de cette méthode.

Configurer

Étape 1. Créez les objets FQDN nécessaires.

Edit Network Object

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

Image 1. Menu Objet réseau

Étape 2. Créez une liste de contrôle d'accès étendue sous Objets > Gestion des objets > Liste de

contrôle d'accès > Étendue.

> ~	AAA Server Access List Extended	Extended An access list object, also I and destination address an	mown as an access control list (ACL), selects the traffic to which a sid ports. Supports IPv4 and IPv6 addresses. You use these objects wi	rvice will apply. Standard-Identifies traf hen configuring particular features, such	Add Extended Access List ic based on destination address of as route maps.	Q Filter
>	Standard Address Pools	Name		Value		Override
	Application Filters AS Path		No	records to display		
	BFD Template					
>	Cipher Suite List Community List					

Image 2. Menu Liste d'accès étendue

Lorsque vous ajoutez une nouvelle règle, notez que vous ne pouvez pas voir l'objet FQDN que vous avez configuré lors d'une recherche sur les objets réseau pour sélectionner la source et la destination.

Edit Extended Access List Entr	ry		0
C Allow]		
Logging:			
Default •]		
Log Level:			
Informational •			
Log Interval:			
300	Sec.		
Network Port	Users Security Group Tag		
Available Networks C	+	Source Networks (0)	Destination Networks (0)
Q cisco	×	any	any
	Add to Source		
L	Add to Destination		
		Enter an IP address Add	Enter an IP address Add
			Cancel Save

Image 3. Menu Nouvelle règle de liste d'accès étendue

Étape 3. Créez une règle qui ne peut pas être atteinte afin que la liste de contrôle d'accès étendue soit créée et disponible pour la configuration PBR.

Add Extended Access List Entry

Action:					
Logging:					
Default ~					
Log Level:					
Informational ~					
Log Interval:					
300 Sec.					
Network Dark & Application & U	The second terms and the second terms and the second terms are second to the second terms and terms are second to the second terms are second terms are second to the second terms are second t	_			
Network Port g Application g U	sers 🔟 Security Group Ta	9			
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	Add to Destination				
GW-10.100.150.1					
IPv4-Benchmark-Tests					
IPv4-Link-Local					
I	1	1		1	1
					Cancel Add

Image 4. Configuration de la règle de liste d'accès qui ne peut pas être atteinte

Étape 4. Vous devez créer une règle sur la stratégie de contrôle d'accès (ACP) ciblant votre FTD avec l'objet FQDN. Le FMC déploie l'objet FQDN sur le FTD afin que vous puissiez le référencer via un objet FlexConfig.

1 Add Rule	0
Name New-Rule-#1-ALLOW Ac	ion C Allow V E Logging OFF Time Range None V Rule Enabled
Insert into Mandatory 🗸	Intrusion Policy None
Q Zones Networks (2) Ports Applications Users URLs Dynamic Attribu	tes 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 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	

Image 5. Règle ACP avec objet FQDN

Étape 5. Accédez à la FTD sur Devices > Device Management et sélectionnez l'onglet Routing et accédez à la section Policy Based Routing.

cisco	Firewall Devices / S	Management Center ecure Firewall Routing					Q Search	Deploy	0	000	admin ~
Home	0	10.100.150.33 Cisco Secure Firewall Threat Defense f	for VMware								Save Cancel
Uvervie	ew	Device Interfaces Inline S	ets Routing DHCP	VTEP							
-Hil Analys	sis	Manage Virtual Routers	Policy Based Routing Specify ingress interfaces, m	g natch criteria and egress interi	aces to route traffic accordingly.	Traffic can be routed across	Egress interfaces accordingly	Configure In	terface	Priority	Add
Policie	DS .	Virtual Router Properties	Ingress Interfaces		Match criteria and forward a There are no PBR policie	ction s defined yet. Start by defini	ing the first one.				
Device	es	BFD OSPF		For step-by-st	p guidance on configuring a pol	icy-based routing policy and	adding applications, launch the How-1	Го.			
●_= Object	ts	OSPFv3 EIGRP									
de Integrat	tion	Plip Policy Based Routing									
		IPv4									
		IPv6 Static Route									
		 Multicast Routing 									
		101.05									

Image 6. Menu PBR

Étape 6. Configurez le PBR sur une interface en utilisant la liste de contrôle d'accès configurée précédemment et déployez.

Add Forwar	ding Actions						?
Match ACL: *	fqdn	~ -	ł				
Send To: *	Egress Interfaces	~					
Interface Orderin	Interface Priority	~ 0					
Available Interfaces			Se	elected Egress	Interfaces *		
Search by interface	e name	a		Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Save

Image 7. Interface PBR et menu de sélection ACL

Étape 7. Accédez à Objets > Gestion des objets > FlexConfig > Objet et créez un nouvel objet.

cisco Ob	rewall Management Center ojects / Object Management	Q Search	Deploy 🥥 🐼
^		Add FlexConfig Object ©	Dbject Q Filter
Home	> AAA Server	Name:	
Uverview	Access List Address Pools Application Filters	fqdn Description:	
dd	AS Path		
Analysis	BFD Template	Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.	VS with the help of TextOb
0	Cipher Suite List		action.
Policies	> Community List	Insert V B Deployment: Everytime V Type: Append V	ction
	DHCP IPv6 Pool		6000 B
Devices	> 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 TextObjects dr
Objects	File List	Standard ACL Object	ofigurations
	V FlexConfig	Extended ACI Object	ingurations.
	FlexConfig Object	Paule Man	Configures next hop. 2. co
integration	Text Object	Route wap	parameters for eigrp. 1. C
	Geolocation	V/ Variablas	ration for an AS
	Interface	- valiaures	ration
	Key Chain	Name Dimension Default Value Property Quantide Description	ration.
	Network	Type:Name) Override Description	for ipv6 traffic. Used text
	> PKI	Ma saasda ta diantau	
	Policy List	Cancel Save	
	Port		20 of 48 rows IC < Page

Image 8. Menu FlexConfig Object Configuration

Étape 8. Sélectionnez Insert > Extended ACL Object, nommez votre variable et sélectionnez votre liste de contrôle d'accès étendue que vous avez créée précédemment. La variable est ajoutée avec le nom que vous avez utilisé.

Insert Extended Access List Object Variable



Cancel Save

3

Image 9. Création de variable pour objet FlexConfig

Étape 9. Entrez cette ligne pour chaque objet FQDN que vous souhaitez ajouter à votre liste de contrôle d'accès.

<#root>

access-li \$

extended permit ip any object

Étape 10. Enregistrez votre objet FlexConfig sous Everytime > Append.

Étape 11.Accédez au menu FlexConfig Policy sous Devices > FlexConfig.



Image 10. Chemin d'accès au menu FlexConfig Policy

Étape 12. Créez une nouvelle stratégie FlexConfig ou sélectionnez une stratégie déjà affectée à votre FTD.

Home				New Policy
	FlexConfig Policy	Status	Last Modified	_
CVCI VICW	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 Ъ
III Analysis				_
Policies				
Devices				

Image 11. Modifier ou créer une nouvelle stratégie FlexConfig

Étape 13. Ajoutez votre objet FlexConfig à la stratégie, enregistrez et déployez.

	test flex				Migrate Config Preview Config Save Cancel
Home	Enter Description				
Overview	Available FlexConfig C FlexConfig Object		Selected Prepend Fle	exConfigs	Policy Assignments (1)
III Analysis			# Name	Description	
Policies	 ✓ User Defined [™]B fqdn ✓ System Defined 				
Devices	Default_DNS_Configure	>			
•=	DHCPv6_Prefix_Delegation_Configure		Selected Append Fle	xConfigs	
Objects	DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure		# Name	Description	
5 Integration	BNS_UnConfigure		1 fqdn		Q 🗇
	L]				

Image 12. Ajout d'un objet FlexConfig à la stratégie FlexConfig

Vérifier

Votre interface d'entrée dispose de la route de stratégie avec la route-map générée automatiquement.

<#root>
firepower#
show run interface gi0/0
!
interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 10.100.151.2 255.255.0

policy-route route-map FMC_GENERATED_PBR_1727116778384

La route-map contient la liste de contrôle d'accès sélectionnée avec l'interface de destination utilisée.

<#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

Votre liste d'accès contient l'hôte utilisé comme référence et la règle supplémentaire que vous avez ajoutée 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

Vous pouvez effectuer un traceur de paquets à partir de l'interface d'entrée en tant que source pour vérifier que vous avez atteint la phase 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

Problèmes courants

PBR cesse de fonctionner après un second déploiement

Vérifiez si la liste de contrôle d'accès contient toujours la règle d'objet FQDN.

Dans ce cas, vous pouvez voir que la règle n'est plus ici.

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

Vérifiez que l'objet FlexConfig est configuré comme Deployment : Everytime et Type : Append. La règle est appliquée à chaque fois lors de futurs déploiements.

FQDN ne résout pas

Lorsque vous essayez d'envoyer une requête ping au nom de domaine complet, un message s'affiche à propos d'un nom d'hôte non valide.

Vérifiez la configuration DNS. Vous devez disposer de serveurs DNS accessibles sur votre groupe de serveurs et les interfaces de recherche de domaine doivent pouvoir les atteindre.

<#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.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.