# Konfigurieren eines FQDN-Objekts auf erweiterter ACL für PBR auf FMC

# Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Überprüfung
Häufige Probleme
PBR funktioniert nach einer zweiten Bereitstellung nicht mehr
FQDN kann nicht aufgelöst werden

# Einleitung

In diesem Dokument wird das Verfahren zum Konfigurieren eines FQDN-Objekts in einer erweiterten Zugriffsliste (ACL) zur Verwendung in Policy Based Routing (PBR) beschrieben.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Produkten vertraut sind:

- Secure Firewall Management Center (FMC)
- Sichere Firewall-Bedrohungsabwehr (FTD)
- PBR

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Firepower Threat Defense für VMware Version 7.6.0
- Secure Firewall Management Center für VMware Version 7.6.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Derzeit lässt FTD keine Filterung von Nicht-HTTP-Datenverkehr mithilfe von FQDN-Objekten (Fully Qualified Domain Name) zu, wie unter der Cisco Bug-ID <u>CSCuz98322</u> erwähnt.

Diese Funktion wird auf ASA-Plattformen unterstützt, allerdings können nur Netzwerke und Anwendungen über FTD gefiltert werden.

Sie können einer erweiterten Zugriffsliste ein FQDN-Objekt hinzufügen, um den PBR mit dieser Methode zu konfigurieren.

## Konfigurieren

Schritt 1: Erstellen Sie bei Bedarf FQDN-Objekte.

## Edit Network Object

Name		
cisco.com		
Description		
Network O Host O Range O Network	k 💽 FQDN	
cisco.com		
Note: You can use FQDN network objects in a Lookup:	access, prefilter and translated destination in NAT rule	is only.
solve within IPv4 addresses only +		
Allow Overrides		
	Cancel	ave

Image 1. Menü Netzwerkobjekt

Schritt 2: Erstellen Sie eine erweiterte Zugriffsliste unter Objekte > Objektverwaltung > Zugriffsliste

#### > Erweitert.

<ul> <li>AAA Server</li> <li>Access List</li> </ul>	Extended An access list object, also k and destination address an	Add Ex snown as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on d ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route ma	tended Access List Q. Filter
Standard > Address Pools	Name	Value	Override
Application Filters AS Path		No records to display	
BFD Template Cipher Suite List			

Image 2. Menü "Erweiterte Zugriffsliste"

Beachten Sie beim Hinzufügen einer neuen Regel, dass das von Ihnen konfigurierte FQDN-Objekt nicht angezeigt wird, wenn Sie die Netzwerkobjekte nach Quelle und Ziel durchsuchen.

		Ø
C Allow		
Logging:		
Default		
Log Level:		
Informational 👻		
Log Interval:		
300 Sec.		
Network Port  Application Users Security Group Tag		
Available Networks C +	Source Networks (0)	Destination Networks (0)
	[	
	any	any
Add to Source	any	any
Add to Source Add to Destination	any	any
Add to Source Add to Destination	any	any
Add to Source Add to Destination	any	any
Add to Source Add to Destination	any	any
Add to Source Add to Destination	any	any
Add to Source Add to Destination	Enter an IP address	Enter an IP address
Add to Source Add to Destination	Enter an IP address	any Enter an IP address Add

Image 3. Menü für neue erweiterte Zugriffslistenregel

Schritt 3: Erstellen Sie eine Regel, die nicht aufgerufen werden kann, damit die erweiterte Zugriffskontrollliste erstellt wird und für die PBR-Konfiguration verfügbar ist.

#### Add Extended Access List Entry

Action:					
C Allow ~					
Logging:					
Default ~					
Log Level:					
Informational ~					
Log Interval:					
300 Sec.					
Network Port  Port  Veta	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	Ũ
any	Add to Source				•
any-ipv4	Add to Destination				
any-ipv6					
GW-10.100.150.1					
IPv4-Benchmark-Tests					
IPv4-Link-Local					
I	I	1	1	1	1
					Cancel Add

Image 4. Konfiguration der Zugriffslistenregel, die nicht getroffen werden kann

Schritt 4: Sie müssen eine Regel für die Zugriffskontrollrichtlinie (ACP) erstellen, die auf Ihre FTD mit dem FQDN-Objekt abzielt. Das FMC stellt das FQDN-Objekt für das FTD bereit, sodass Sie über ein FlexConfig-Objekt darauf verweisen können.

1 Add Rule	0
Name New-Rule-#1-ALLOW Action	Allow V BLogging OFF B Time Range None V Rule Enabled
Insert into Mandatory 🗸 🔍	usion Policy None Variable Set V By File Policy None V
Q Zones Networks (2) Ports Applications Users URLs Dynamic Attributes	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. ACP-Regel mit FQDN-Objekt

Schritt 5: Navigieren Sie zu FTD on Devices (Geräte) > Device Management (Geräteverwaltung), und wählen Sie die Registerkarte Routing (Routing) aus, und navigieren Sie zum Abschnitt Policy Based Routing (Richtlinienbasiertes Routing).

cisco	Firewall Management Cer Devices / Secure Firewall Routing	hter				Q Search	Deploy	0	@ (	🔊 📔 admin 🗸
Home	e Cisco Secure Firewall Th	reat Defense for VMware								Save Cancel
Uvervie	ew Device Interfac	es Inline Sets Routing DHCF	VTEP							
ilil Analys	sis Global	outers Policy Based Rou Specify ingress interface	ting is, match criteria and egress int	terfaces to route traffic accordingly	y. Traffic can be routed acro	oss Egress interfaces accordingly	Configure In	terface	Priority	Add
Policie	es Virtual Router Prope ECMP	rties Ingress Interfaces		Match criteria and forward There are no PBR polici	action ies defined yet. Start by de	fining the first one.				
Device	es OSPF		For step-by	<ul> <li>step guidance on configuring a po</li> </ul>	olicy-based routing policy a	nd adding applications, launch the How	-То.			
Q Object	OSPFv3 EIGRP									
🍰 Integrat	Policy Based Routin	9								
	IPv4									
	IPv6 Static Poulte									
	<ul> <li>Multicast Routin</li> </ul>	g								
	10110									

Image 6. PBR-Menü

Schritt 6: Konfigurieren Sie den PBR mithilfe der zuvor konfigurierten ACL auf einer Schnittstelle, und stellen Sie ihn bereit.

Add Forwa	rding Actions						?
Match ACL: *	fqdn	~	ł				
Send To: *	Egress Interfaces	~					
Interface Orderin	Interface Priority	0					
Available Interfaces	5		Se	elected Egress	Interfaces *		
Search by interfact	e name	a		Priority	Interface		
Priority	Interface			0	outside		Ū
0	inside	+					
						Cancel	Save

Image 7. PBR-Schnittstelle und ACL-Auswahlmenü

Schritt 7. Navigieren Sie zu Objects > Object Management > FlexConfig > Object, und erstellen Sie ein neues Objekt.

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

Image 8. Konfigurationsmenü für FlexConfig-Objekte

Schritt 8: Wählen Sie Einfügen > Erweitertes ACL-Objekt, geben Sie der Variablen einen Namen, und wählen Sie die zuvor erstellte erweiterte ACL aus. Die Variable wird mit dem von Ihnen verwendeten Namen hinzugefügt.

# Insert Extended Access List Object Variable



Cancel Save

3

Image 9. Variablenerstellung für FlexConfig-Objekt

Schritt 9. Geben Sie diese Zeile für jedes FQDN-Objekt ein, das Sie in die ACL aufnehmen möchten.

<#root>

access-li \$

Schritt 10. Speichern Sie Ihr FlexConfig-Objekt als Jederzeit > Anfügen.

Schritt 11:Navigieren Sie zum Menü FlexConfig Policy (FlexConfig-Richtlinie) unter Devices (Geräte) > FlexConfig.



Image 10. Pfad zum Menü "FlexConfig Policy"

Schritt 12: Erstellen Sie eine neue FlexConfig-Richtlinie, oder wählen Sie eine Richtlinie aus, die Ihrem FTD bereits zugewiesen ist.

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> Ø Ъ́
Analysis				_
Policies				
Devices				

Image 11. Bearbeiten oder Erstellen einer neuen FlexConfig-Richtlinie

Schritt 13: Fügen Sie das FlexConfig-Objekt zur Policy hinzu, speichern und bereitstellen.

	test flex			Migrate Config Preview Config Save Cancel
Home	Enter Description			
Overview	Available FlexConfig C <sup>o</sup> FlexConfig Object	Selected Prepend Fle	xConfigs	Policy Assignments (1)
dil	8	# Name	Description	
Analysis	V User Defined			
	e fqdn			
Policies	System Defined			
=	Default_Inspection_Protocol_Disable			
Devices	Default_Inspection_Protocol_Enable			
•=	DHCPv6_Prefix_Delegation_Configure	📲 Selected Append Flex	Configs	
Objects	■ DHCPv6_Prefix_Delegation_UnConfigure			
	DNS_Configure	# Name	Description	
Integration	DNS_UnConfigure	1 fqdn		QĪ
	Eigrp_Configure			

Image 12. FlexConfig-Objekt zur FlexConfig-Richtlinie hinzugefügt

# Überprüfung

Die Eingangsschnittstelle verfügt über die Richtlinienroute mit automatisch generierter Routenübersicht.

```
<#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

Die Route Map enthält die ausgewählte ACL mit der verwendeten Zielschnittstelle.

#### <#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

Ihre Zugriffsliste enthält den Host, der als Referenz verwendet wird, sowie die zusätzliche Regel, die Sie über FlexConfig hinzugefügt haben.

#### <#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

Sie können einen Paket-Tracer von der Eingangsschnittstelle aus durchführen, um zu überprüfen, ob Sie die PBR-Phase erreicht haben.

#### <#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

## Häufige Probleme

PBR funktioniert nach einer zweiten Bereitstellung nicht mehr

Überprüfen Sie, ob die Zugriffsliste noch die FQDN-Objektregel enthält.

In diesem Fall sehen Sie, dass die Regel nicht mehr vorhanden ist.

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

(Bereitstellungszeit) und Type: Append (Anfügen) eingerichtet ist. Die Regel wird bei zukünftigen Bereitstellungen immer angewendet.

### FQDN kann nicht aufgelöst werden

Wenn Sie versuchen, den FQDN zu pingen, erhalten Sie eine Meldung über einen ungültigen Hostnamen.

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

Überprüfen der DNS-Konfiguration Sie benötigen erreichbare DNS-Server in Ihrer Servergruppe, und die Schnittstellen für die Domänensuche müssen in der Lage sein, diese zu erreichen.

<#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.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.