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

Inhalt

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 CSCuz98322 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.

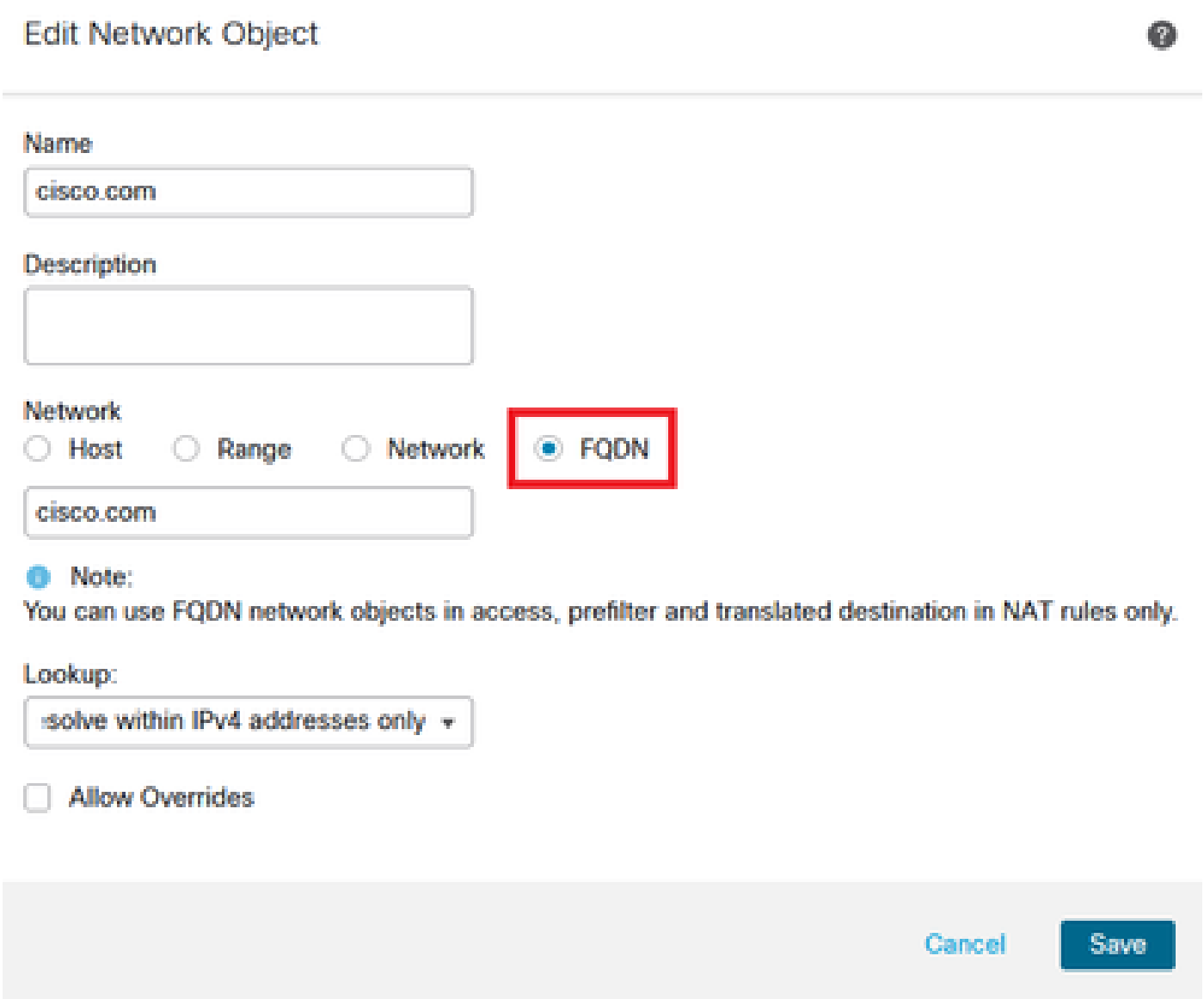

Image 1. Menü Netzwerkobjekt

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

> Erweitert.

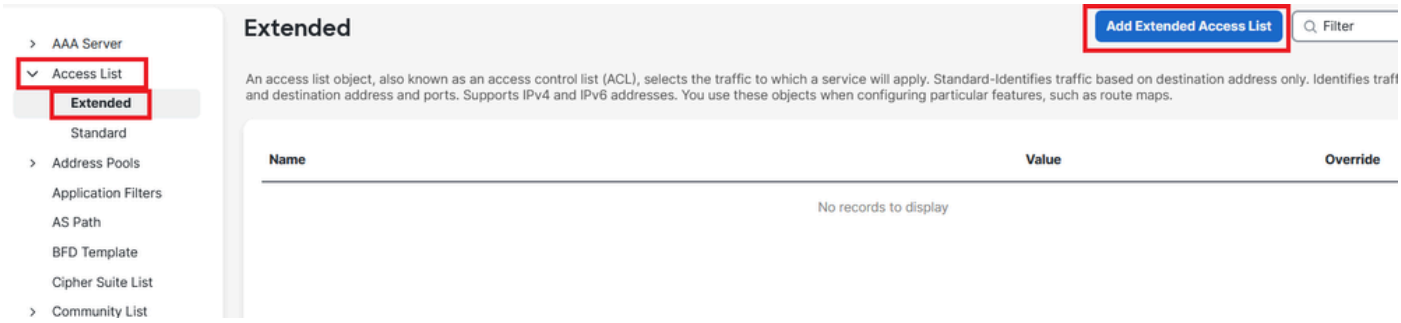

Image 2. Menü "Erweiterte Zugriffsliste"

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.

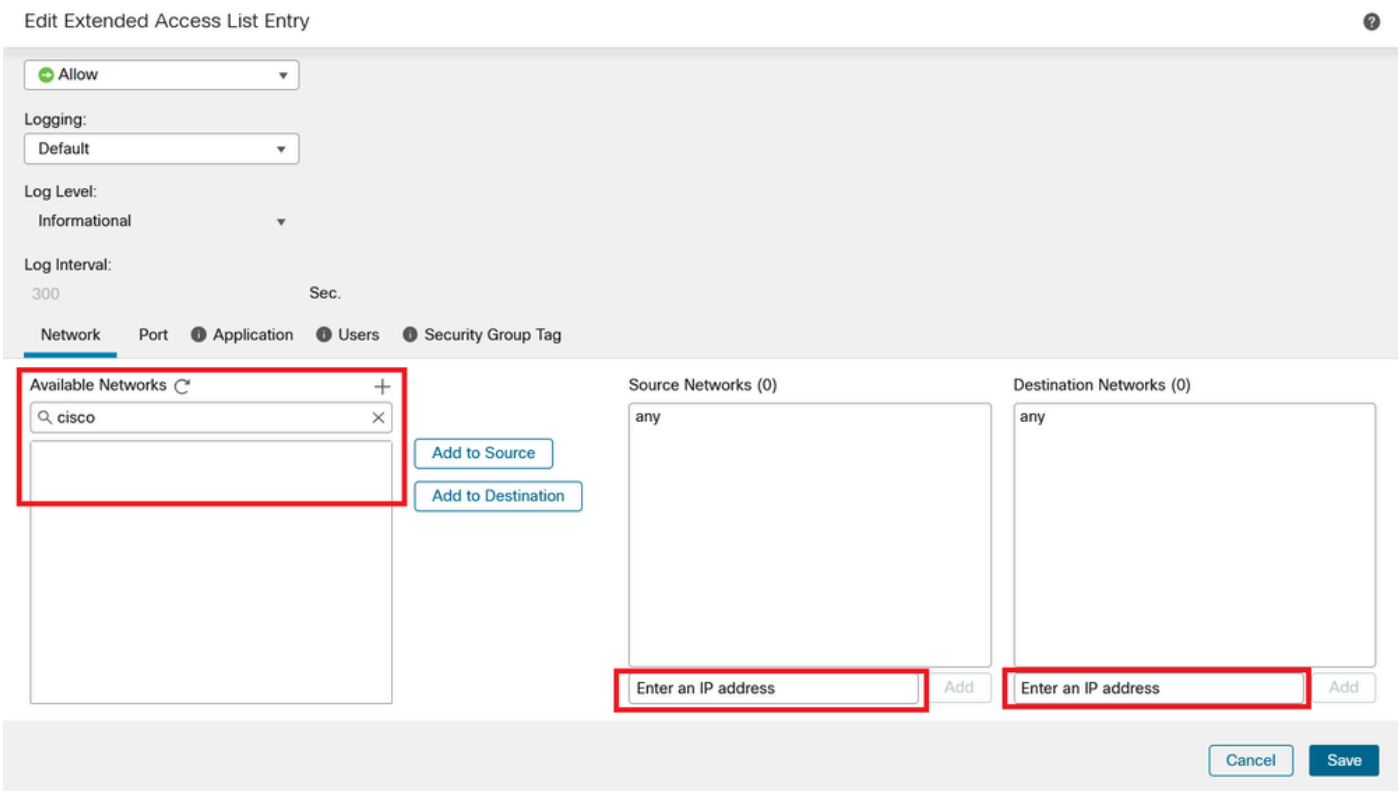

Image 3. Menü für neue erweiterte Zugriffslistenregel

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

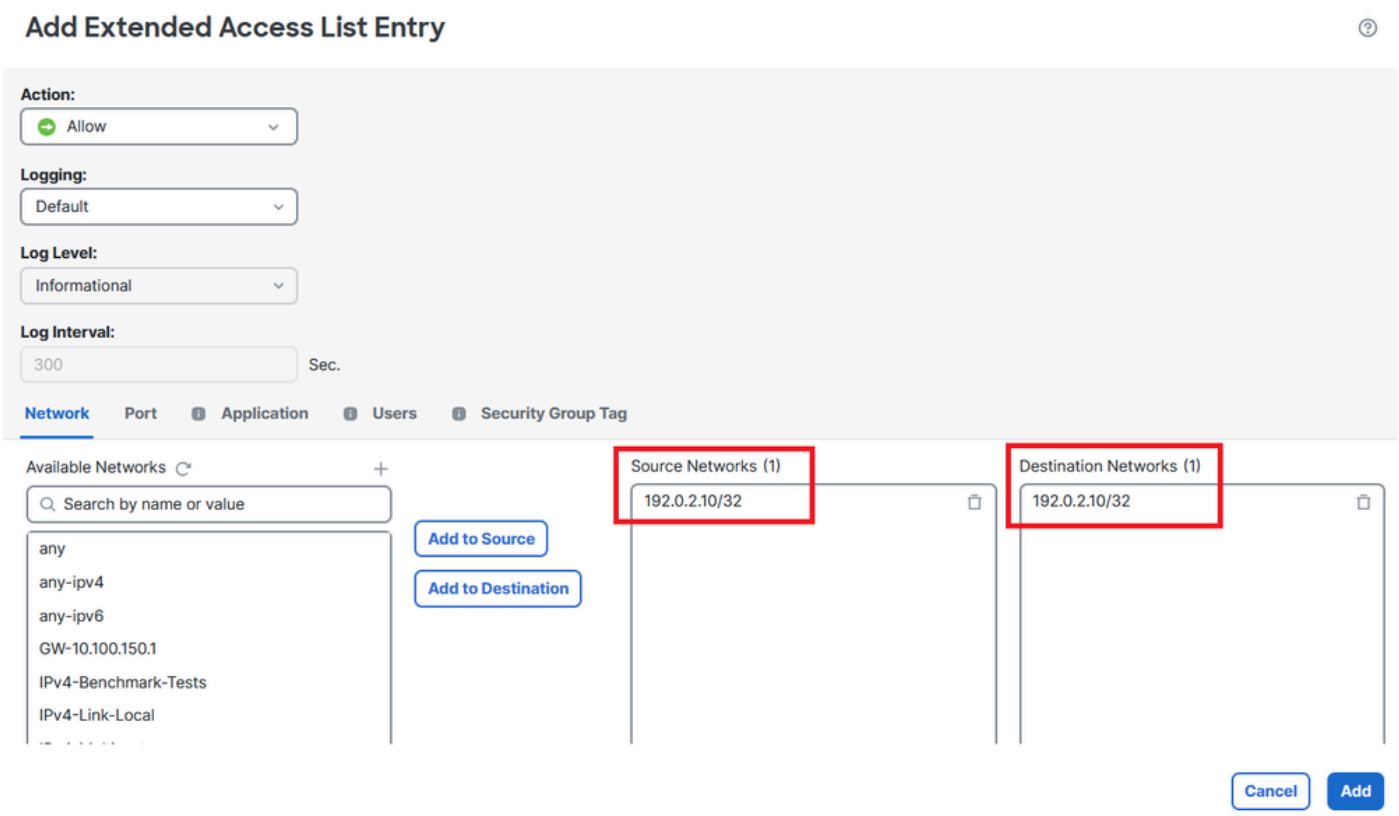

Image 4. Konfiguration der Zugriffslistenregel, die nicht getroffen werden kann

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.

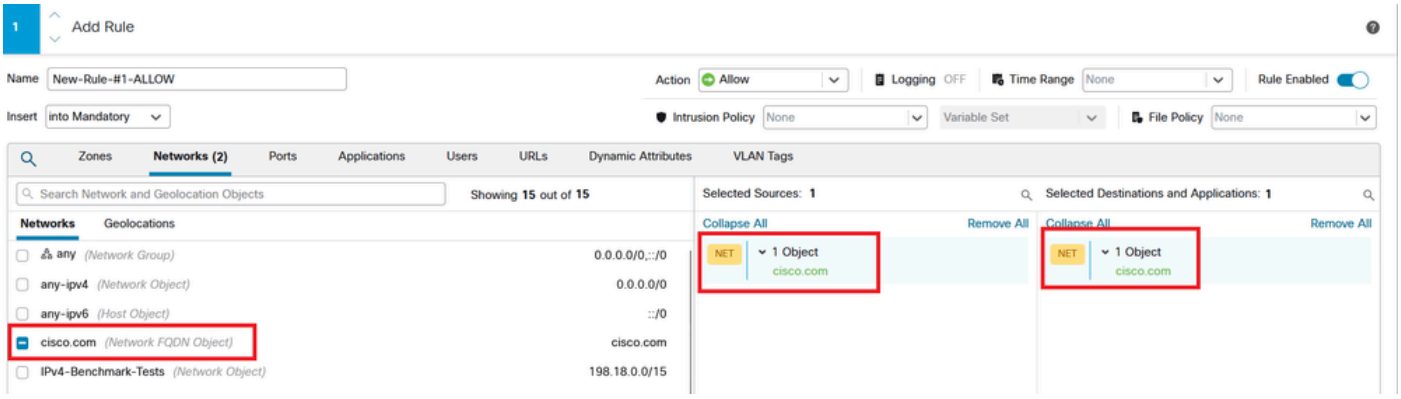

Image 5. ACP-Regel mit FQDN-Objekt

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).

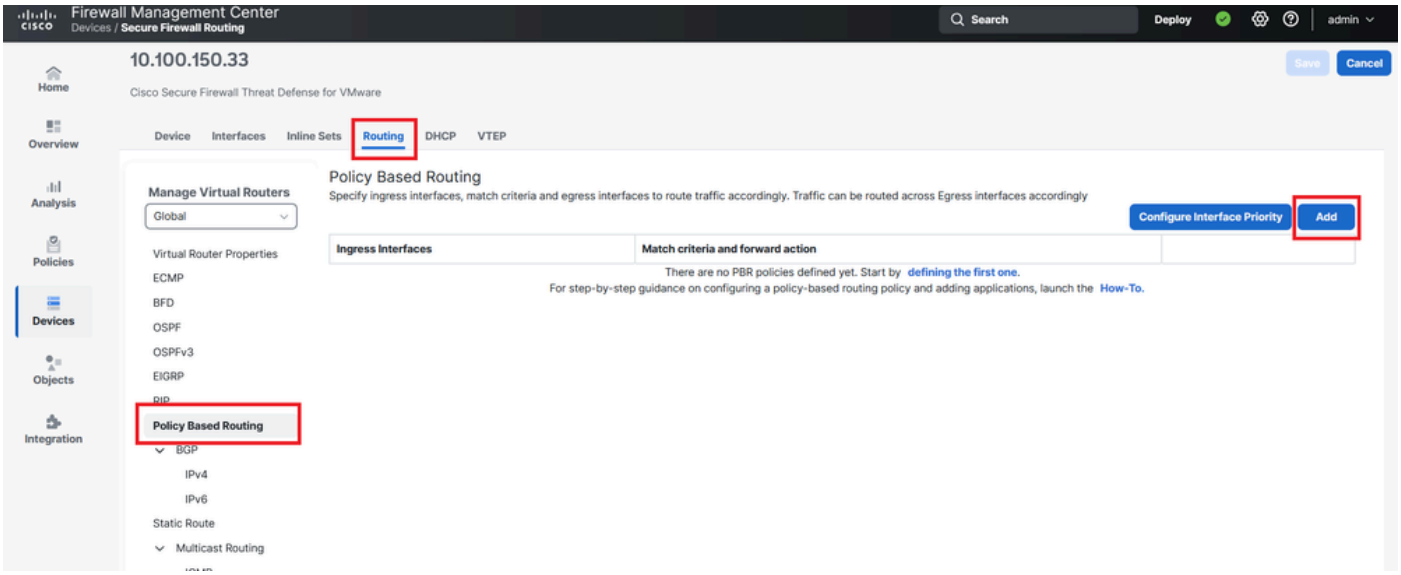

Image 6. PBR-Menü

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

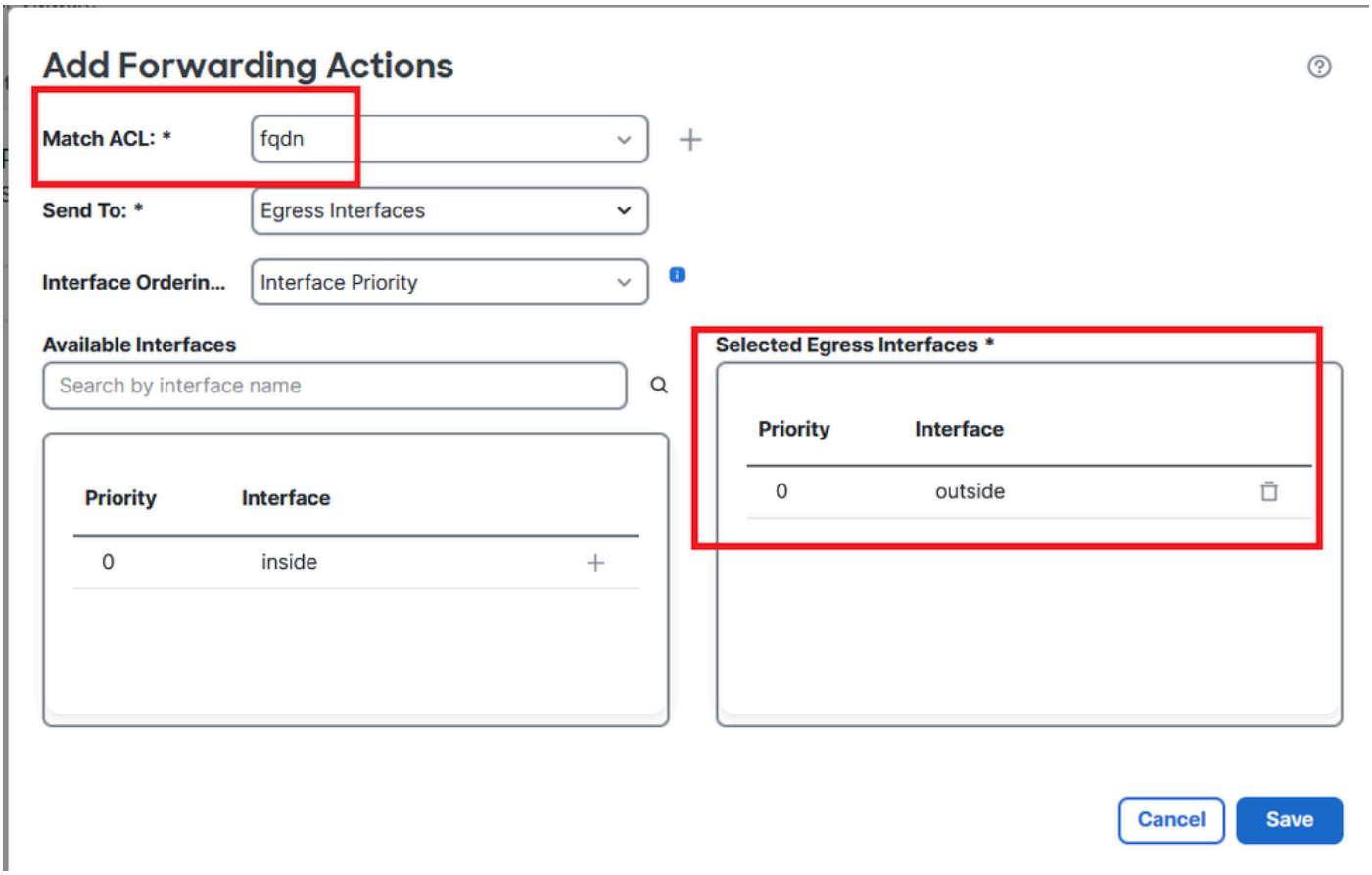

Image 7. PBR-Schnittstelle und ACL-Auswahlmenü

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

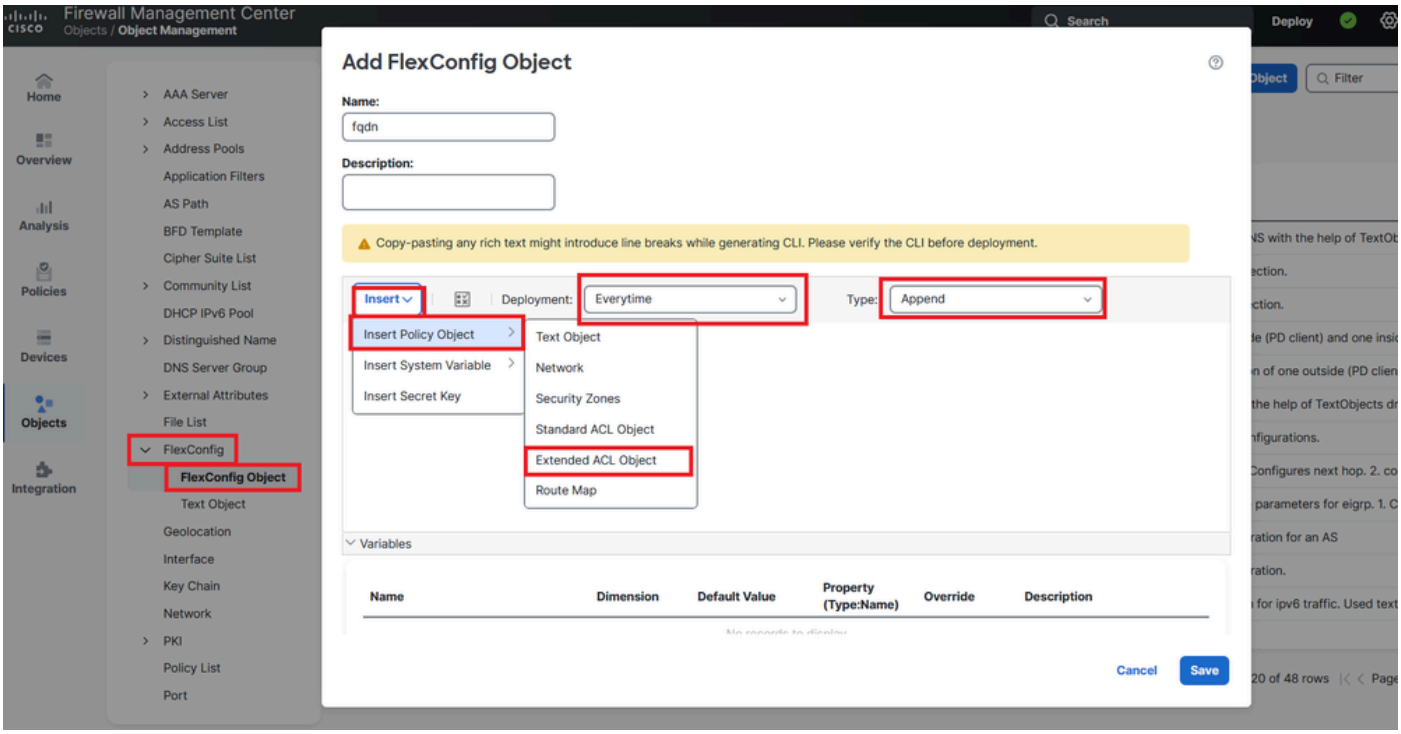

Image 8. Konfigurationsmenü für FlexConfig-Objekte

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.

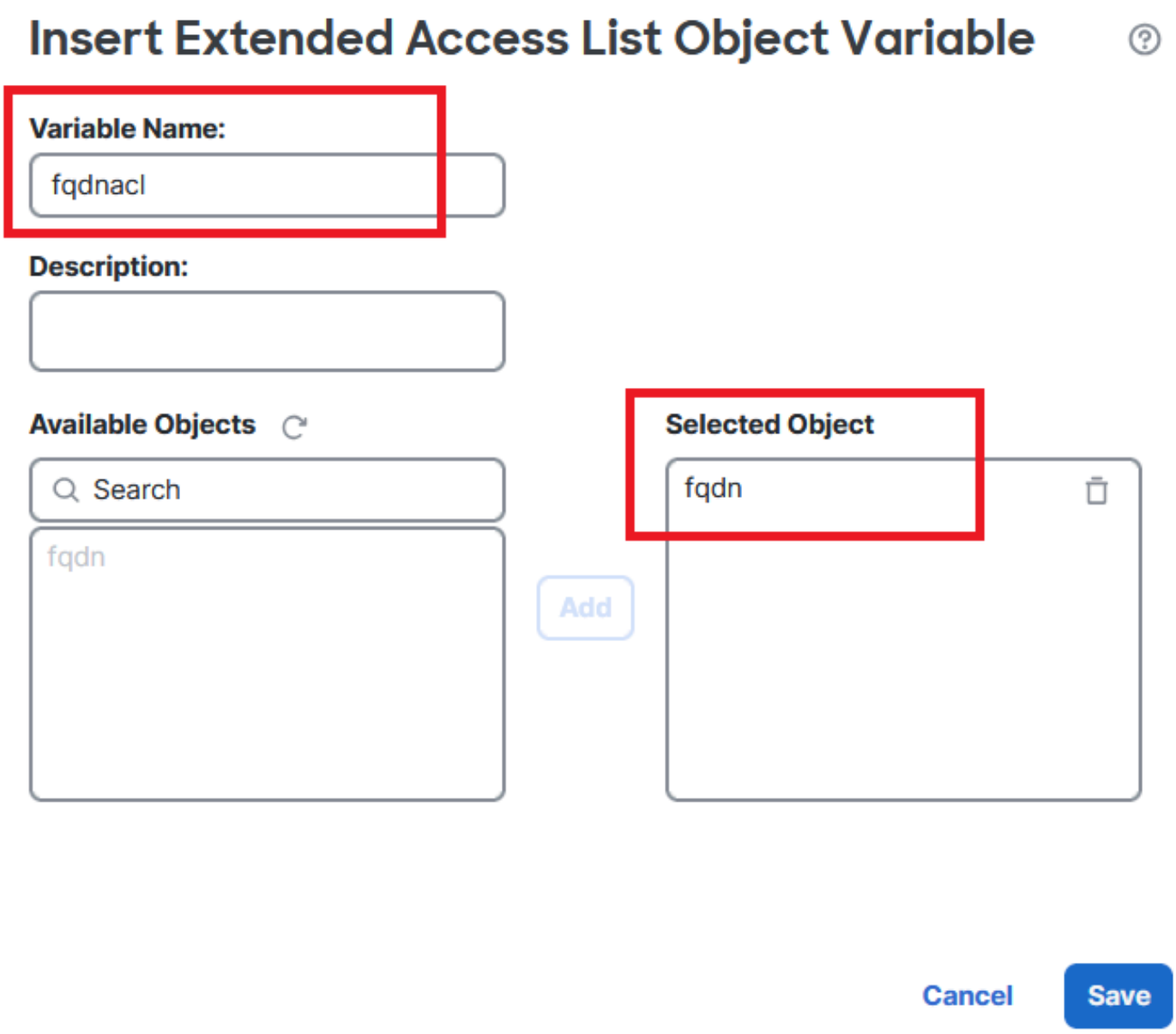

Image 9. Variablenerstellung für FlexConfig-Objekt

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

<#root>

```
access-li $
```

```
extended permit ip any object
```

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

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

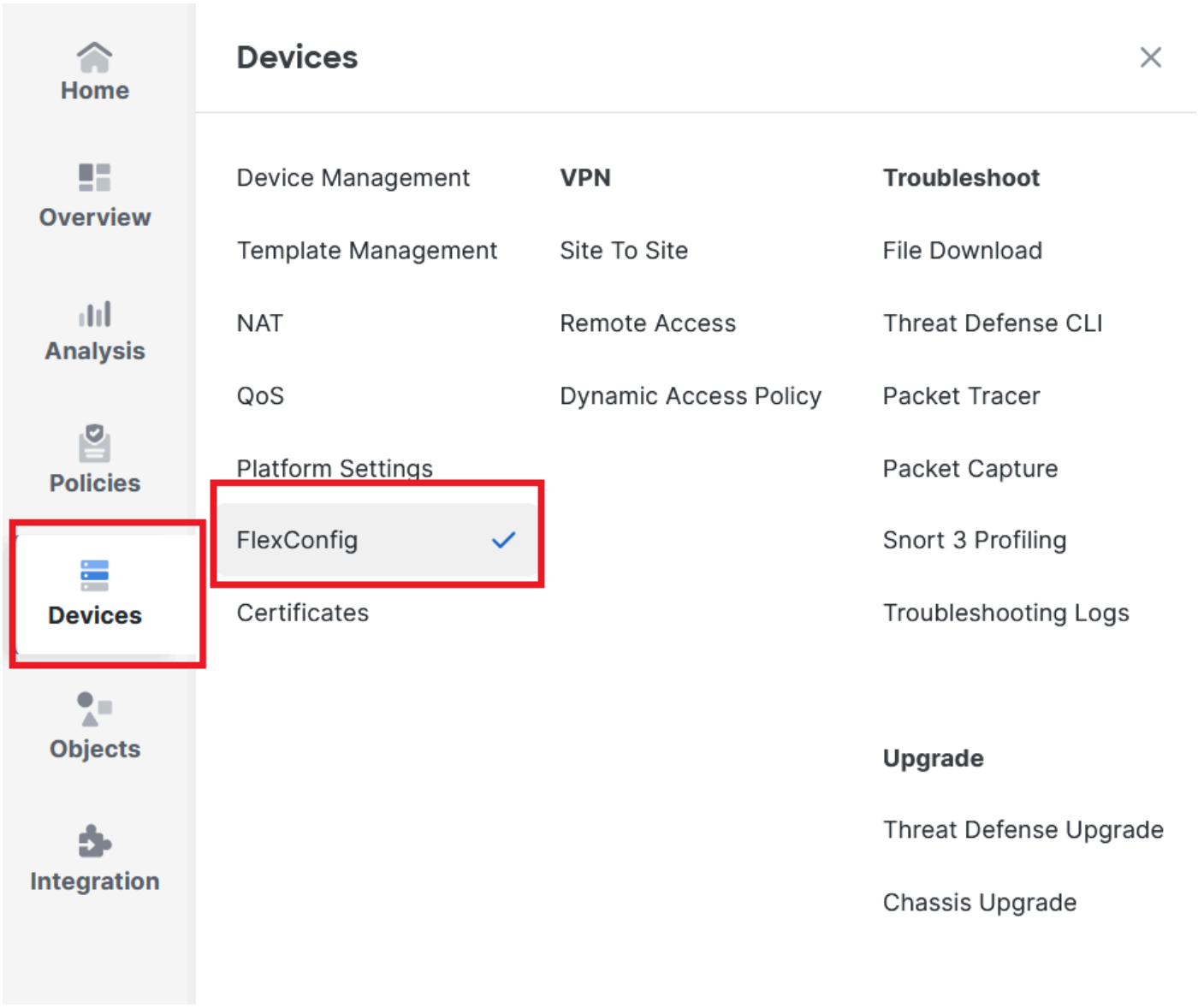

Image 10. Pfad zum Menü "FlexConfig Policy"

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

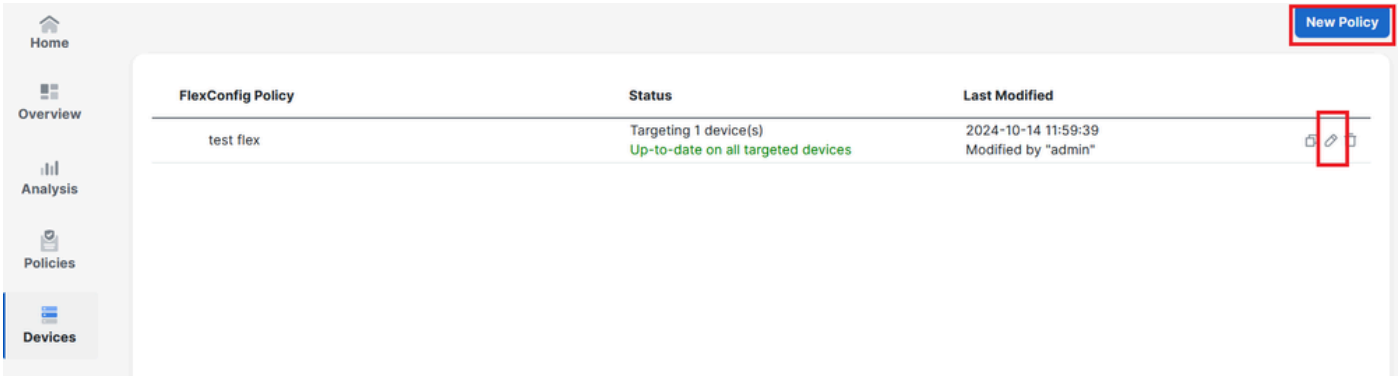

Image 11. Bearbeiten oder Erstellen einer neuen FlexConfig-Richtlinie

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

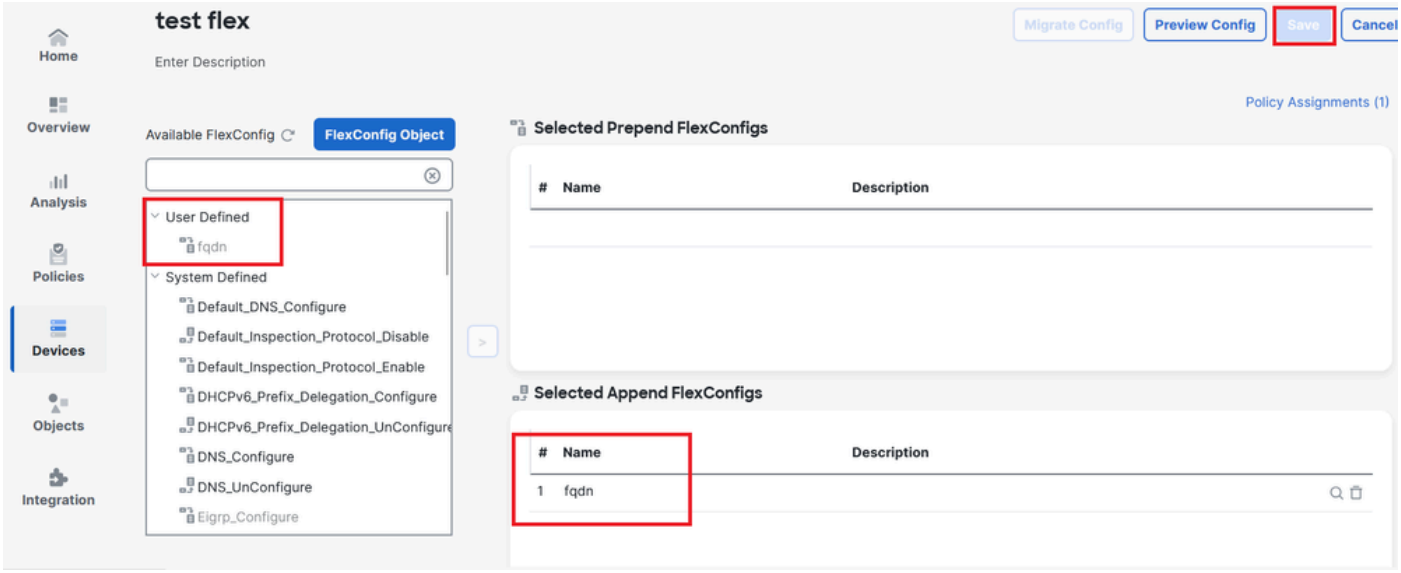

Image 12. FlexConfig-Objekt zur FlexConfig-Richtlinie hinzugefügt

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#
```

Vergewissern Sie sich, dass das FlexConfig-Objekt als Deployment: Everytime

(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.