FQDN-object op uitgebreide ACL voor PBR op FMC configureren

Inhoud

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

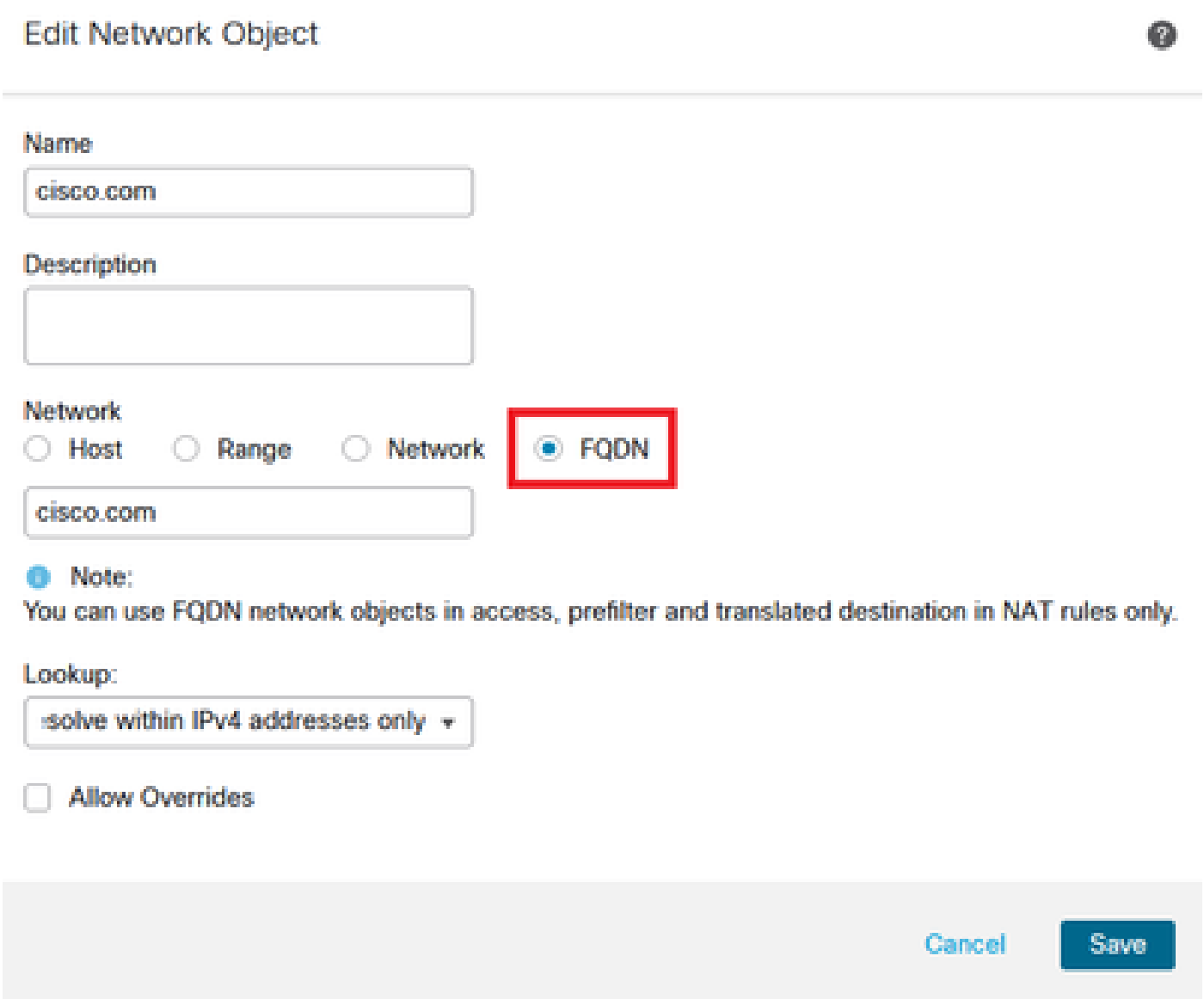
Op dit moment is het niet toegestaan om op niet-HTTP verkeer te filteren met FFull Qualified Domain Name (FQDN)-objecten zoals vermeld op Cisco bug-id CSCuz98322.

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

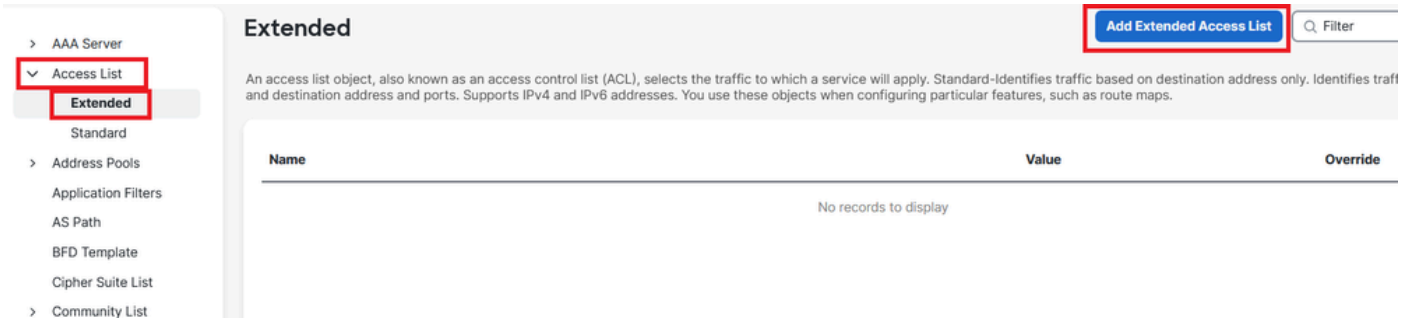
Stap 1. Indien nodig FQDN-objecten maken.



Afbeelding 1. Menu Netwerkobject

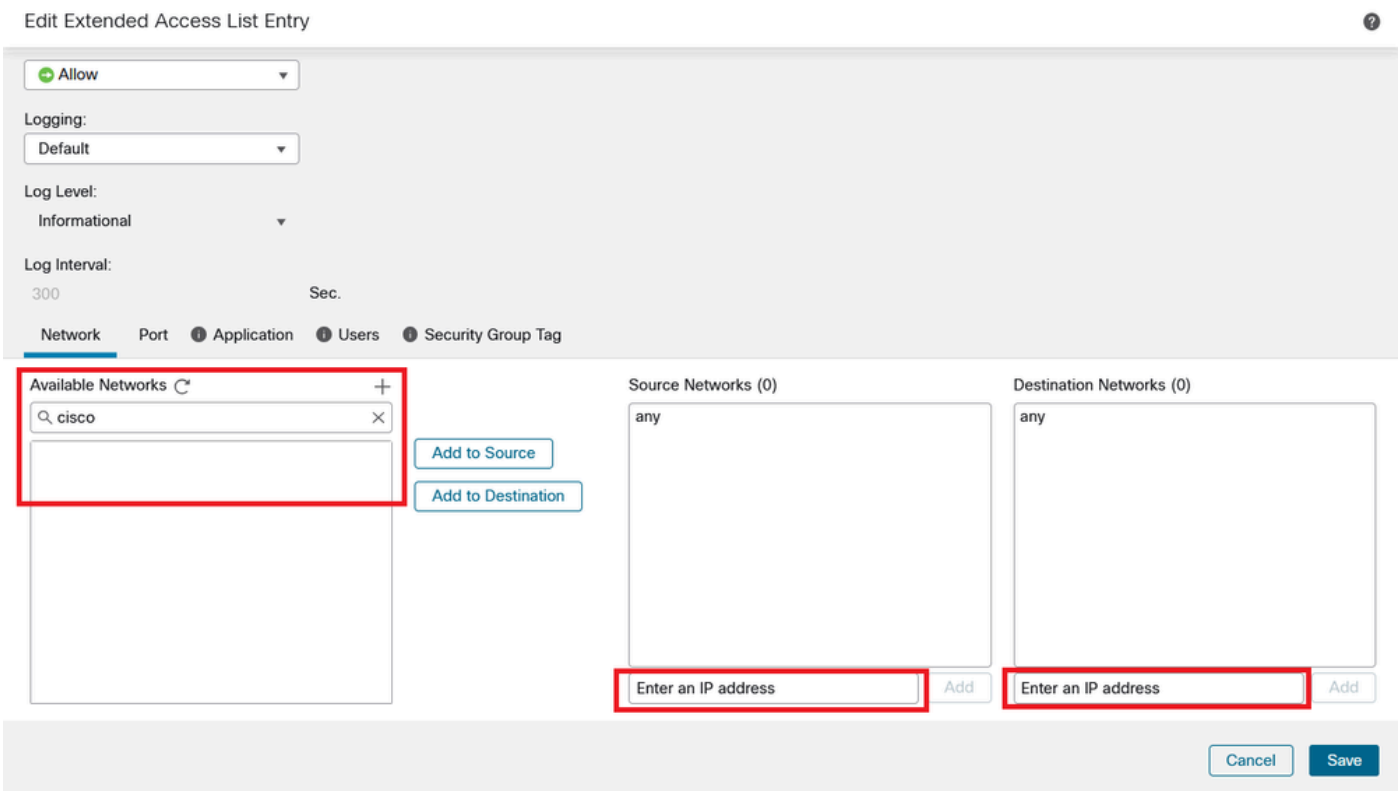
Stap 2. Maak een uitgebreide toegangslijst onder Objecten > Objectbeheer > Toegangslijst >

Uitgebreid.



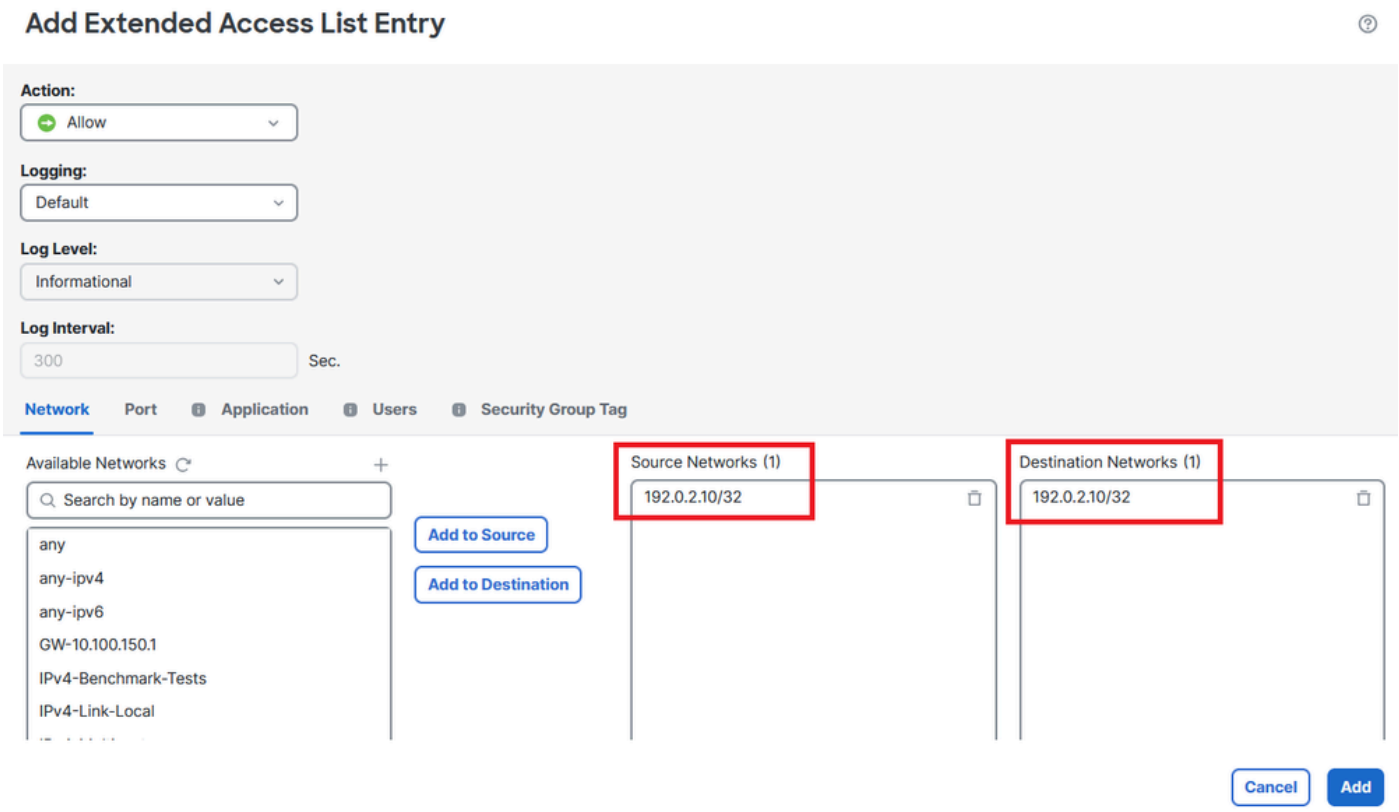
Afbeelding 2. Uitgebreid menu toegangslijst

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.



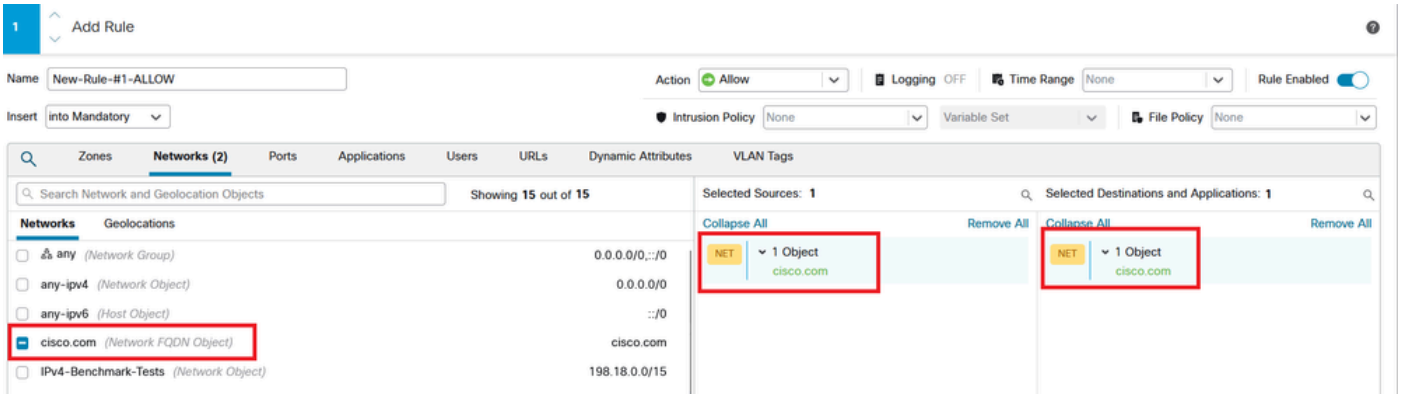
Afbeelding 3. Nieuw menu Regel uitgebreide toegangslijst

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



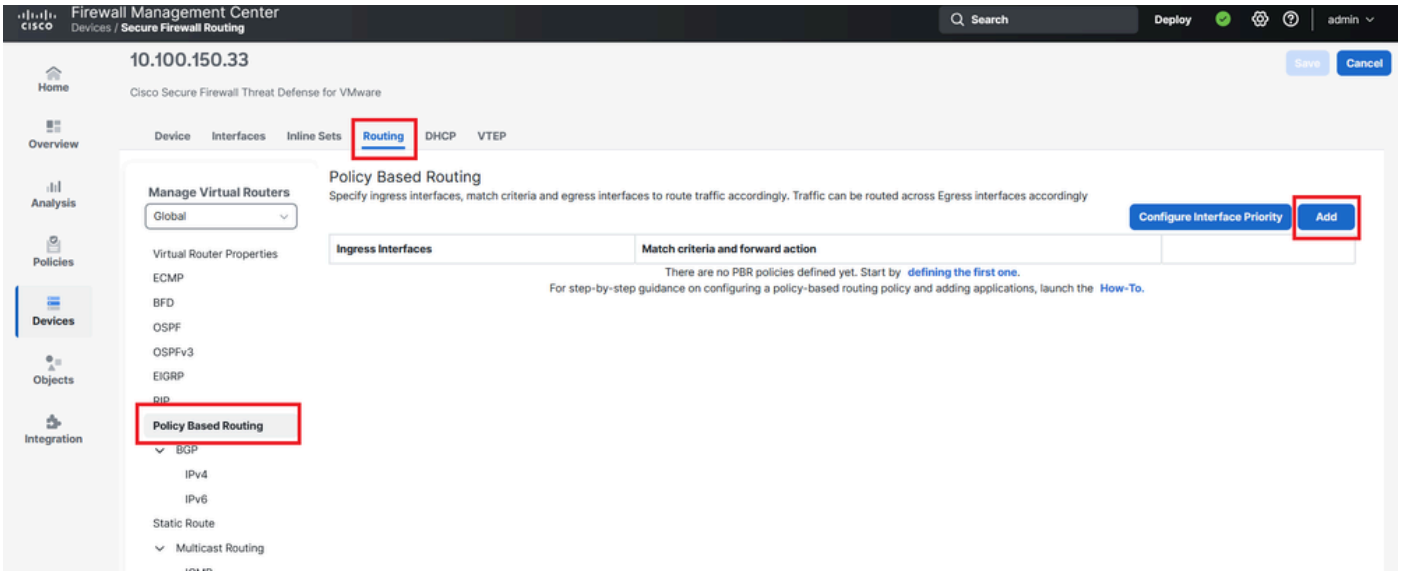
Afbeelding 4. Configuratie van toegangslijst die niet kan worden geraakt

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.



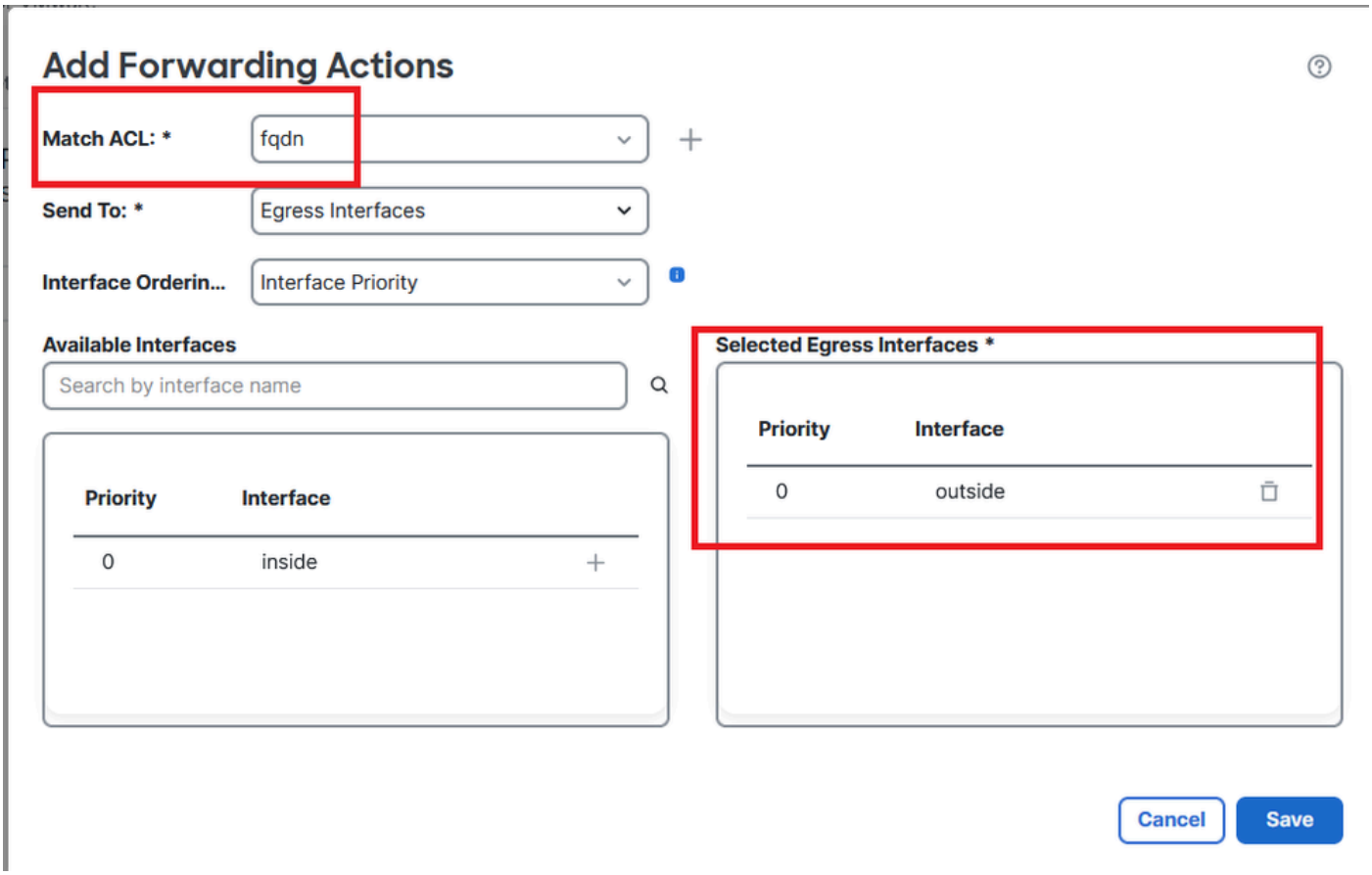
Afbeelding 5. ACS-regel met FQDN-object

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



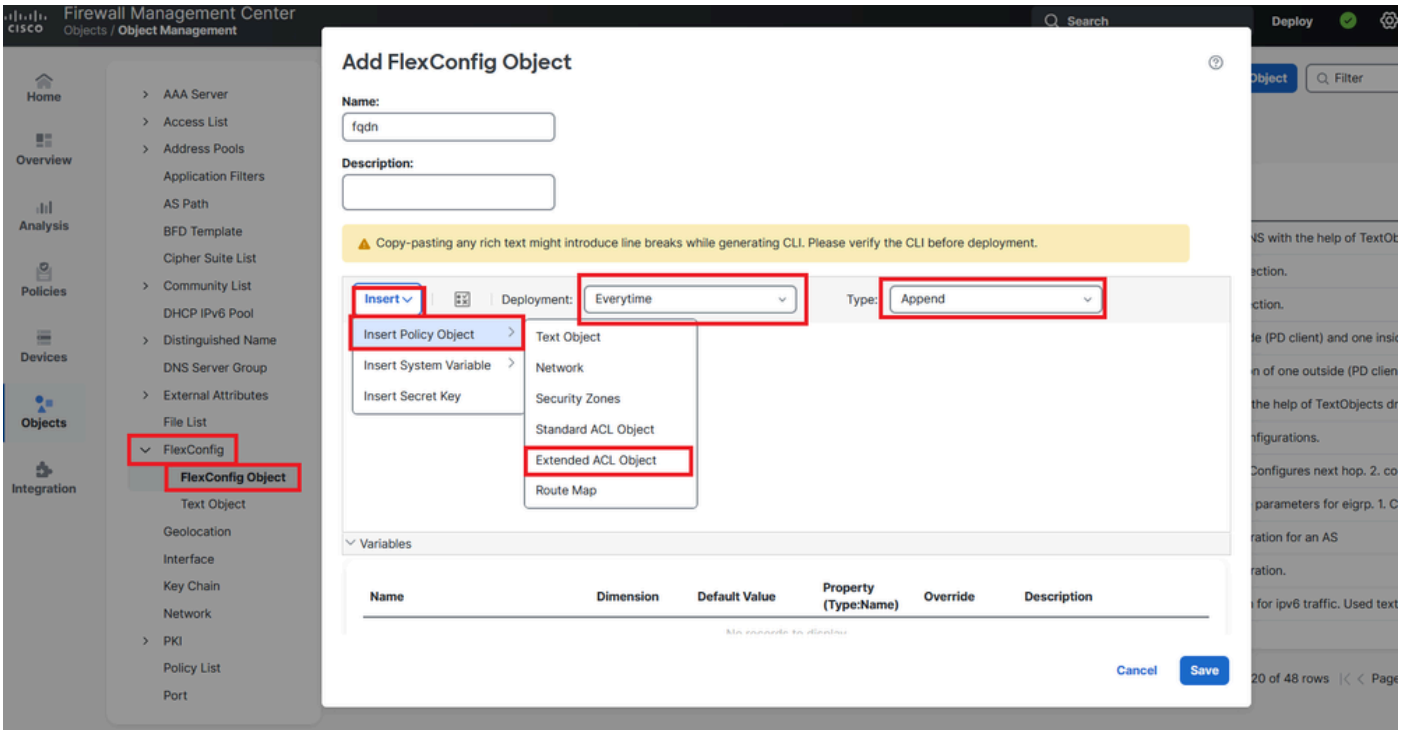
Afbeelding 6. PBR-menu

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



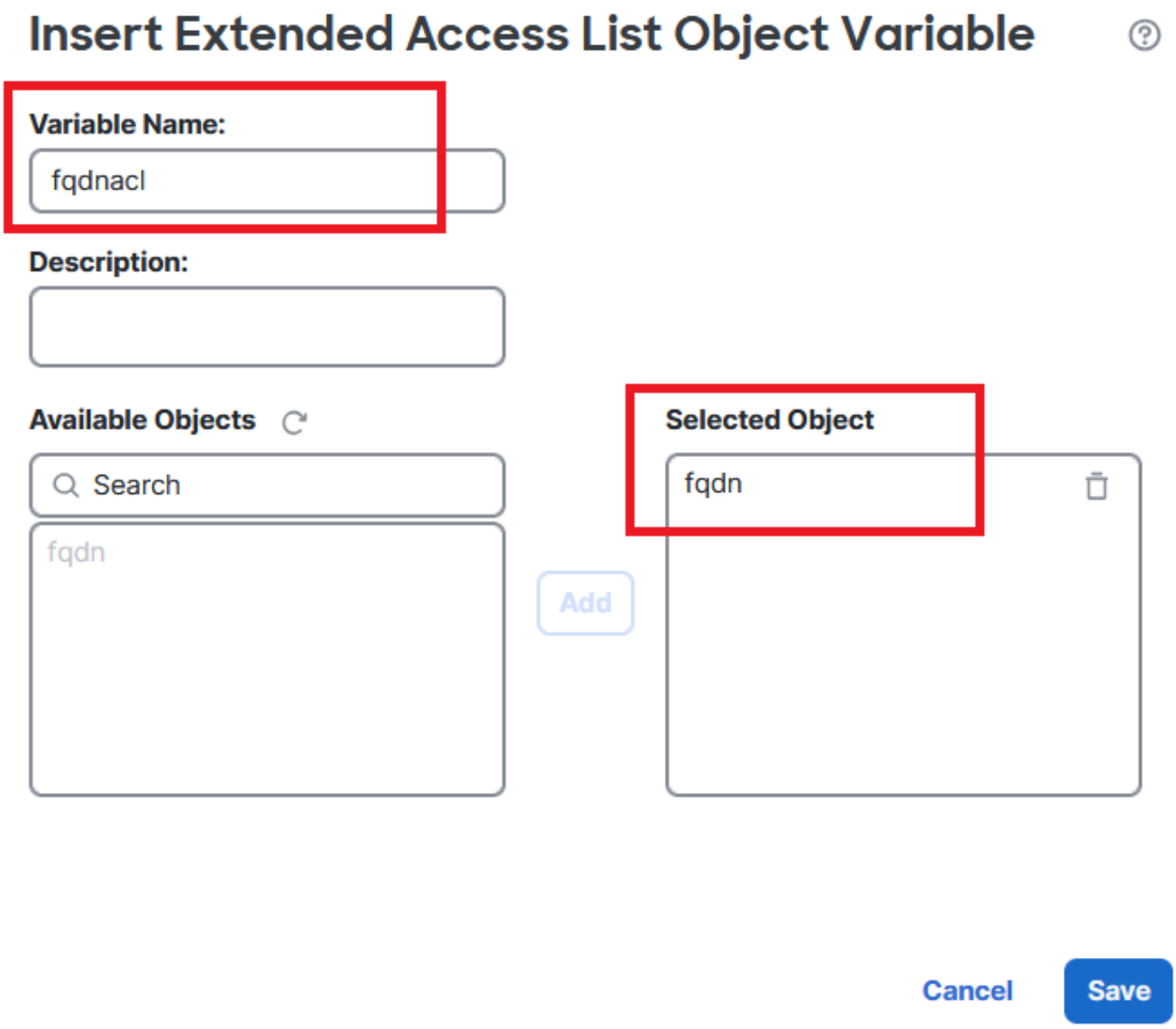
Afbeelding 7. PBR-interface en ACL-selectiemenu

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



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.



Afbeelding 9. Variabele maken voor FlexConfig-object

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

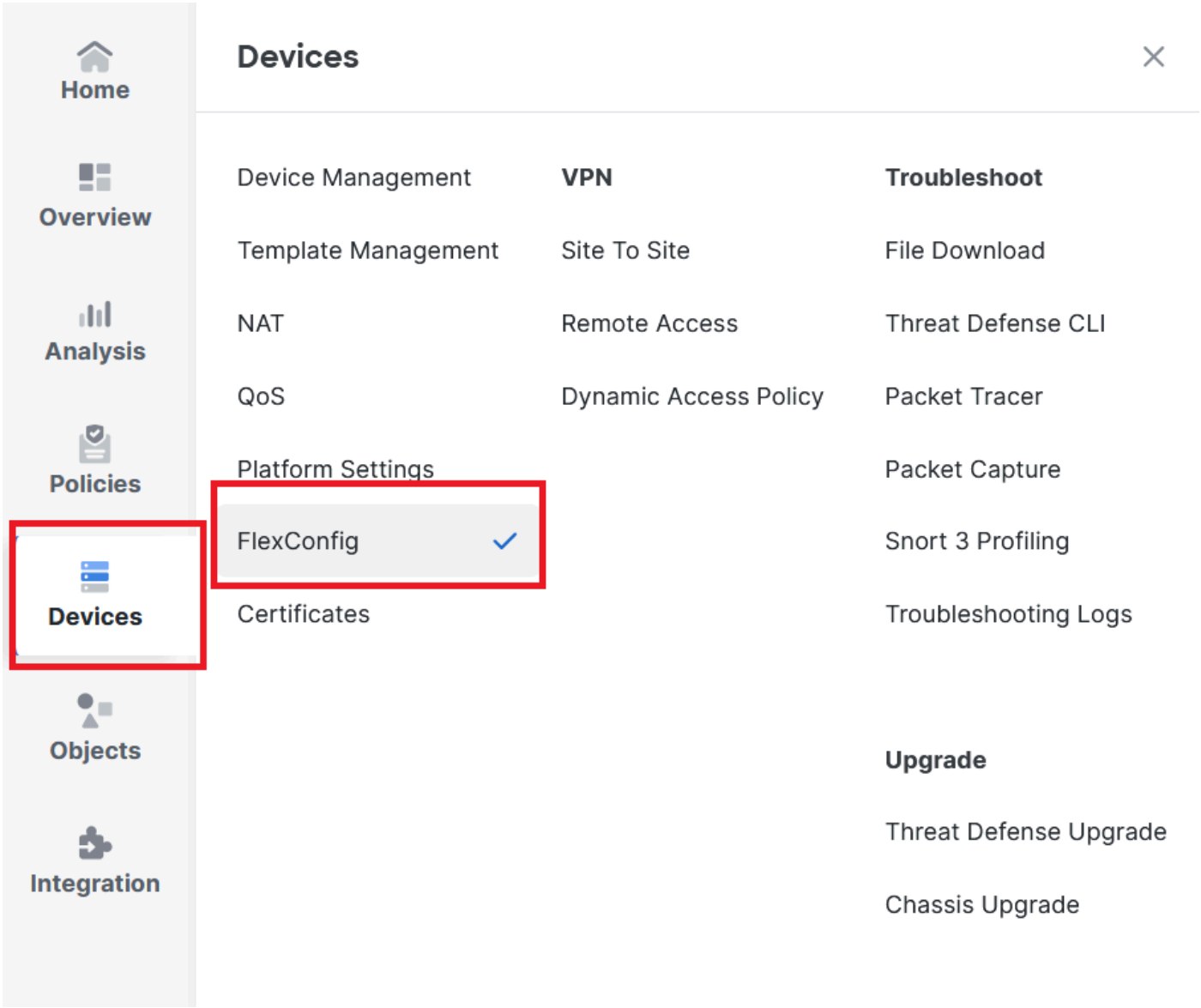
<#root>

```
access-li $
```

```
extended permit ip any object
```

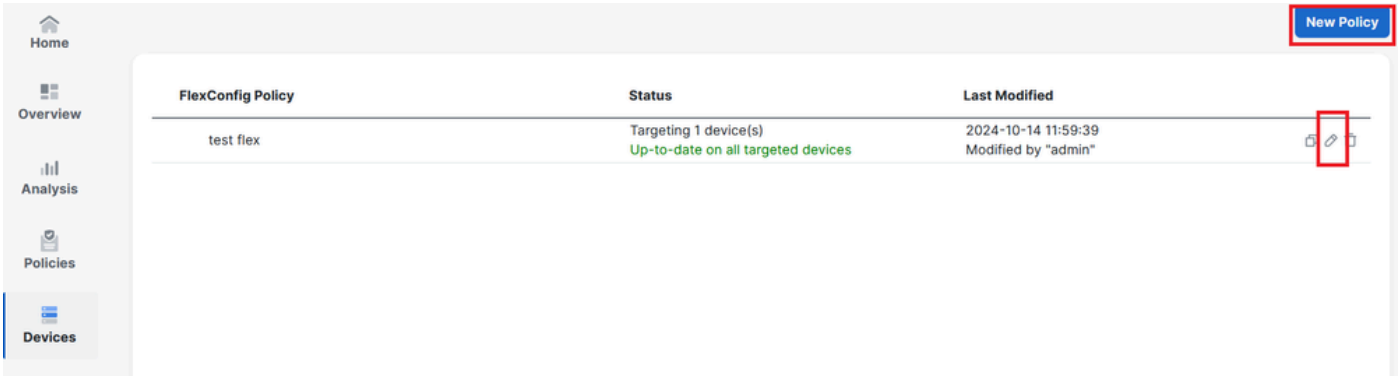
Stap 10. Sla uw FlexConfig-object op als altijd > Toevoegen.

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



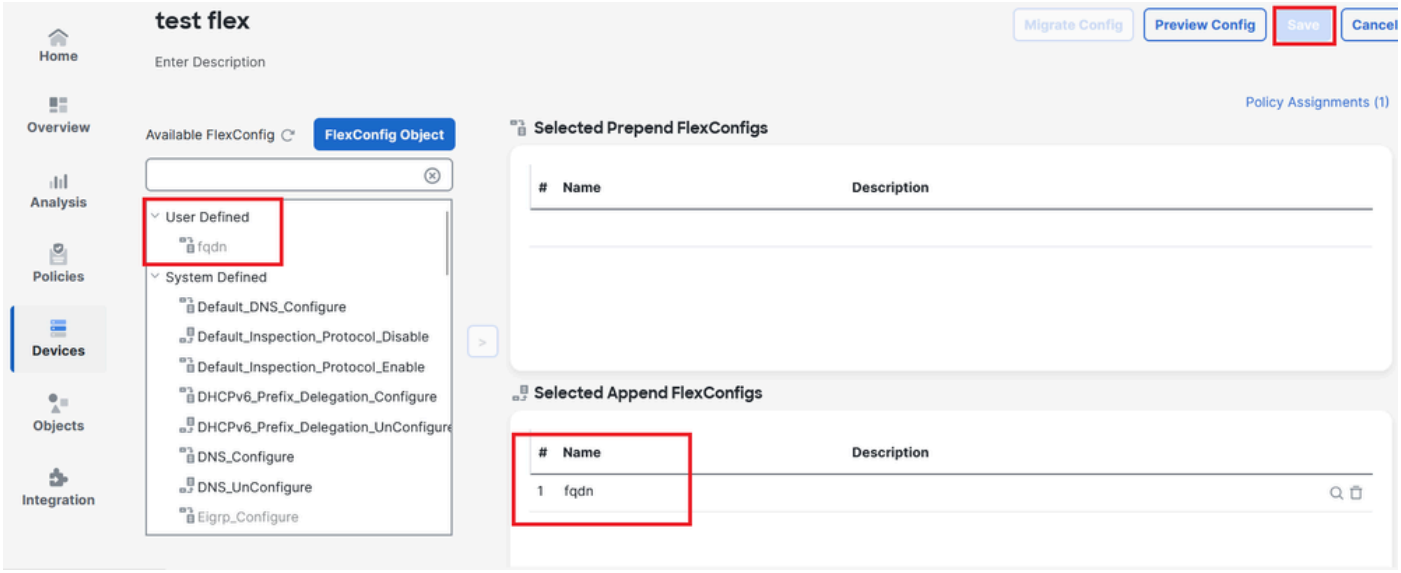
Afbeelding 10. Pad naar FlexConfig beleidsmenu

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



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.



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#
```

Controleer of het FlexConfig-object als implementatie is ingesteld: Everytime and Type: Add. De

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.