# FMC의 PBR에 대한 확장 ACL에 FQDN 개체 구성

## 목차



## 소개

이 문서에서는 PBR(Policy Based Routing)에서 사용할 확장 ACL(Access-List)의 FQDN 객체를 구성하는 절차에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 제품에 대해 알고 있는 것이 좋습니다.

- FMC(Secure Firewall Management Center)
- FTD(보안 방화벽 위협 방어)
- PBR

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower Threat Defense for VMware 버전 7.6.0
- Secure Firewall Management Center for VMware 버전 7.6.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

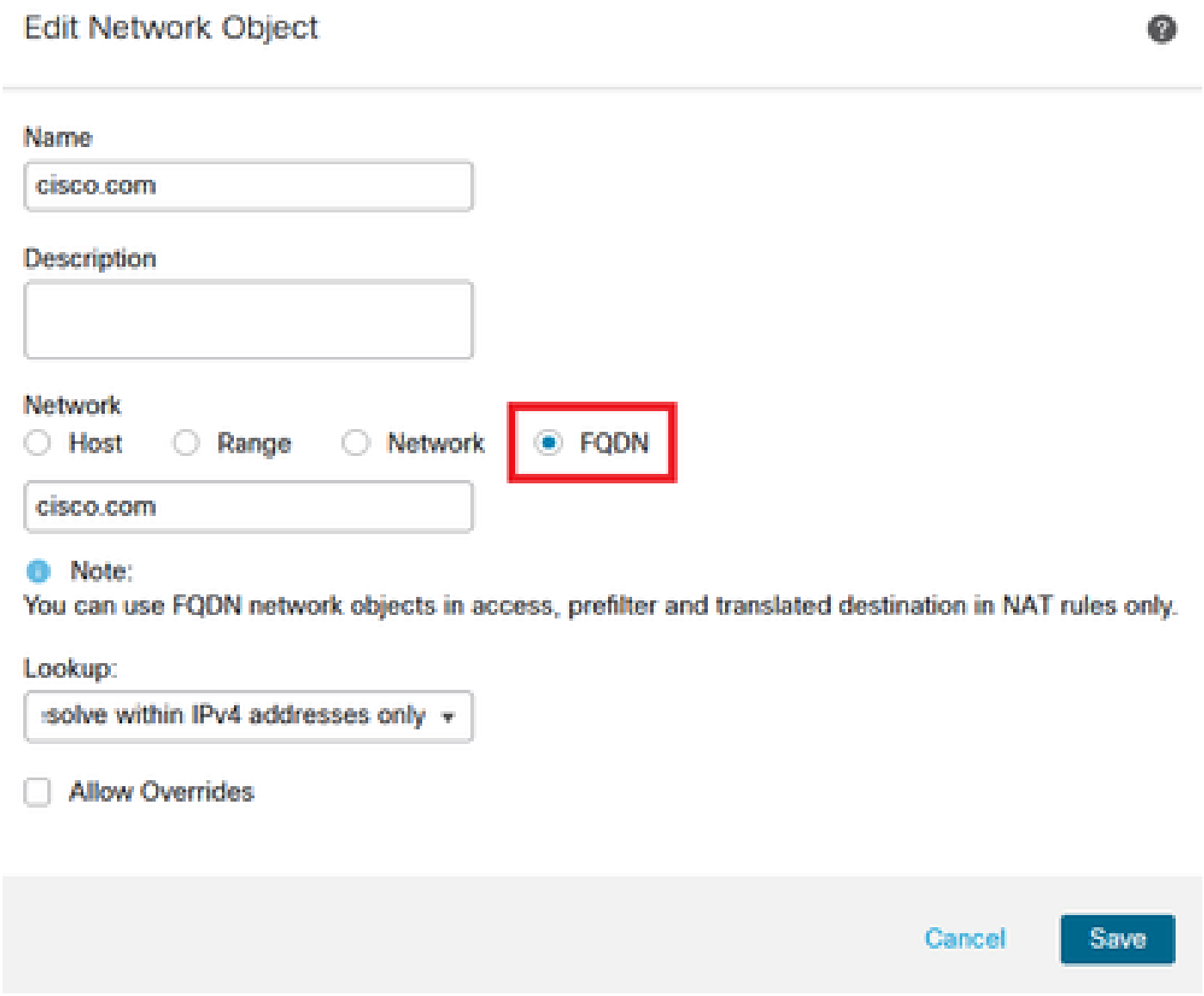
현재 FTD는 Cisco 버그 ID CSCuz98322에 언급된 대로 FQDN(Fully Qualified Domain Name) 객체를 사용하는 비 HTTP 트래픽에 대한 필터링을 허용하지 않습니다.

이 기능은 ASA 플랫폼에서 지원되지만, FTD에서는 네트워크 및 애플리케이션만 필터링할 수 있습니다.

이 방법을 사용하여 PBR을 구성하기 위해 확장 액세스 목록에 FQDN 객체를 추가할 수 있습니다.

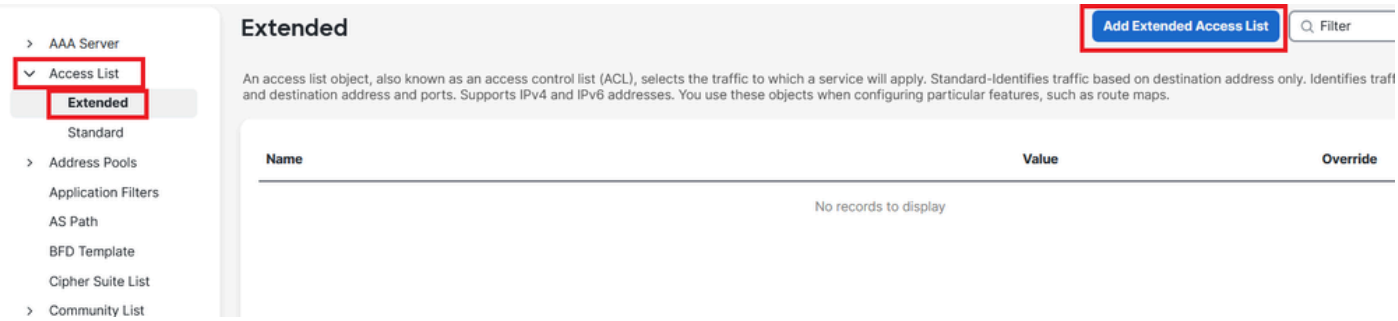
## 구성

1단계. 필요에 따라 FQDN 객체를 생성합니다.



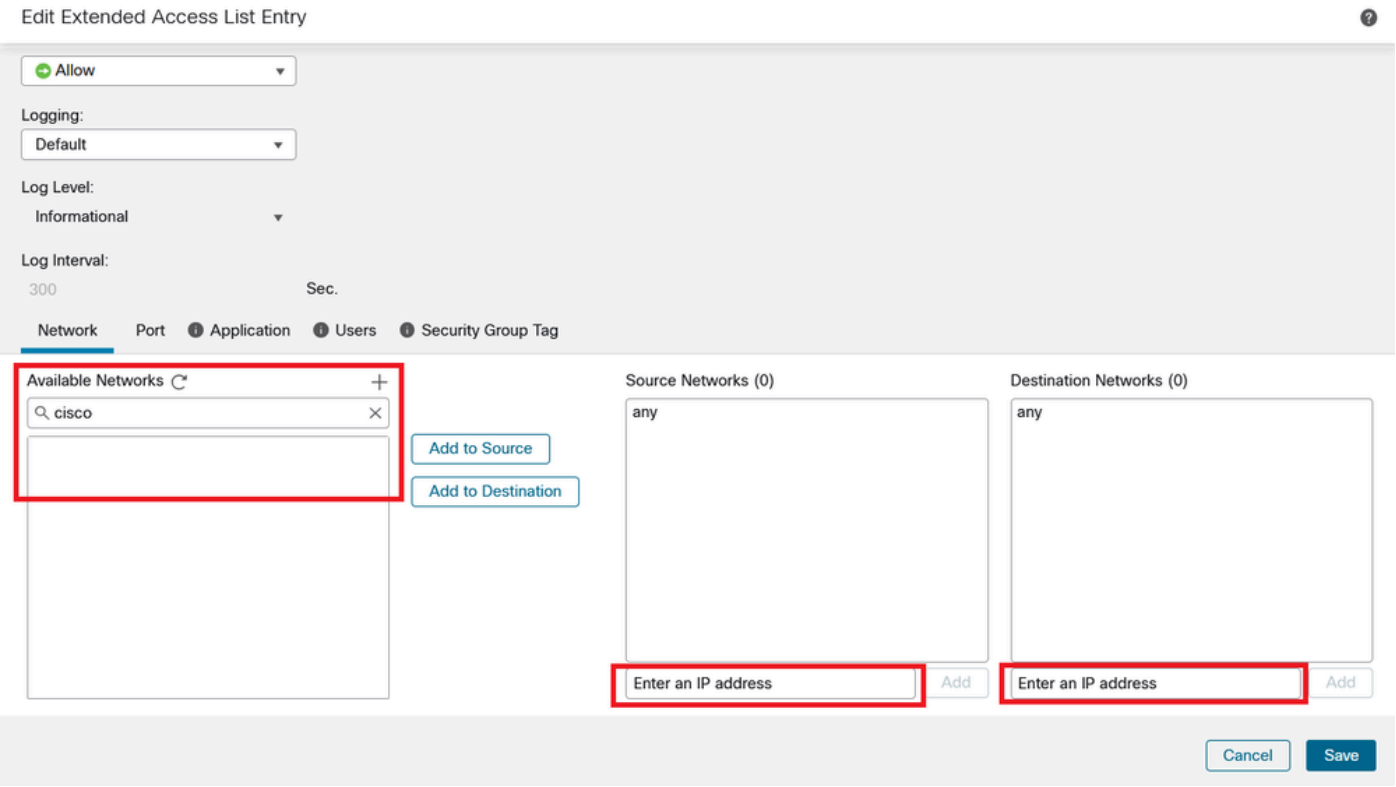

이미지 1. 네트워크 개체 메뉴

2단계. Objects(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Extended(확장)에서 확장 액세스 목록을 생성합니다.



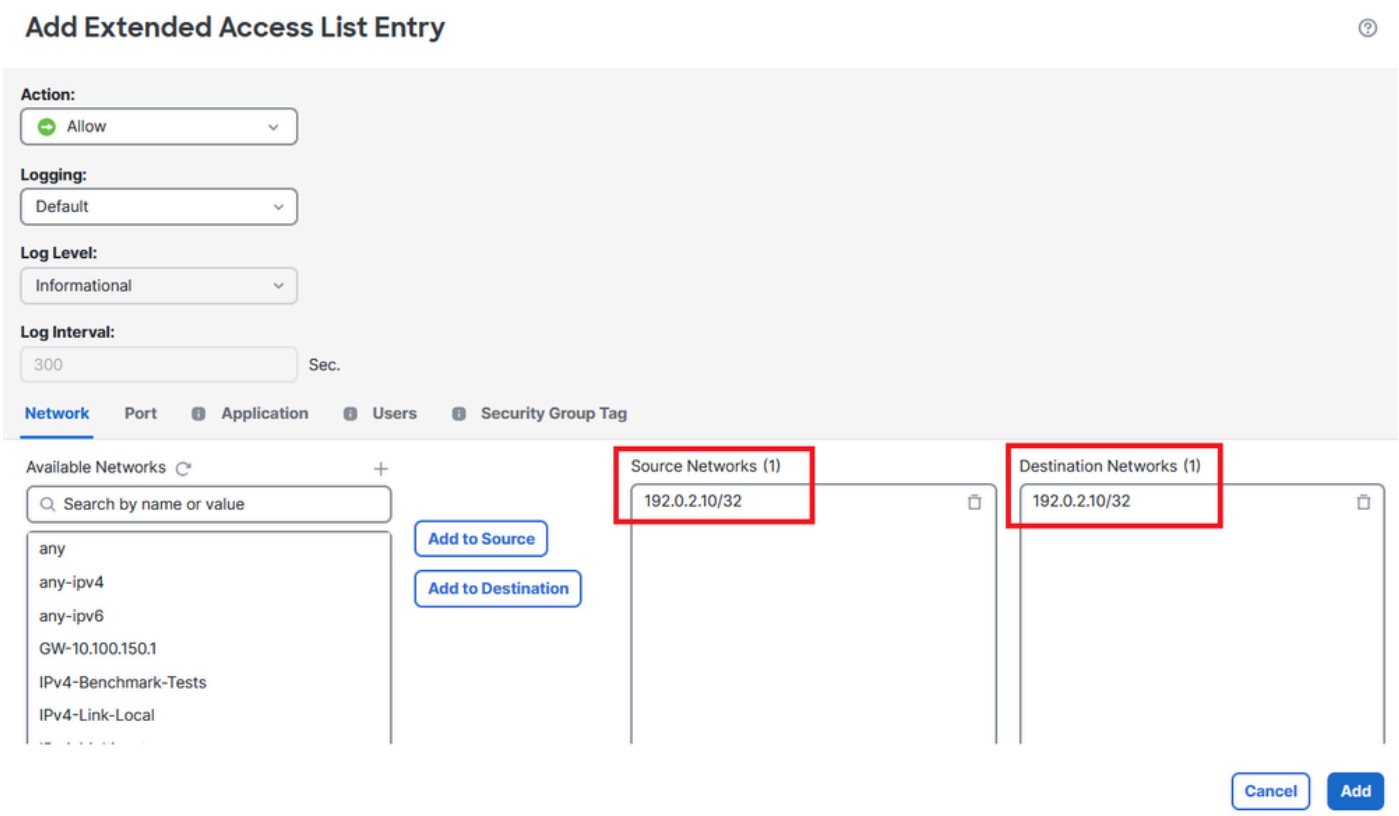

이미지 2. 확장 액세스 목록 메뉴

새 규칙을 추가할 때 소스 및 대상을 선택하기 위해 네트워크 객체를 검색할 때 구성한 FQDN 객체를 볼 수 없다는 점에 유의하십시오.



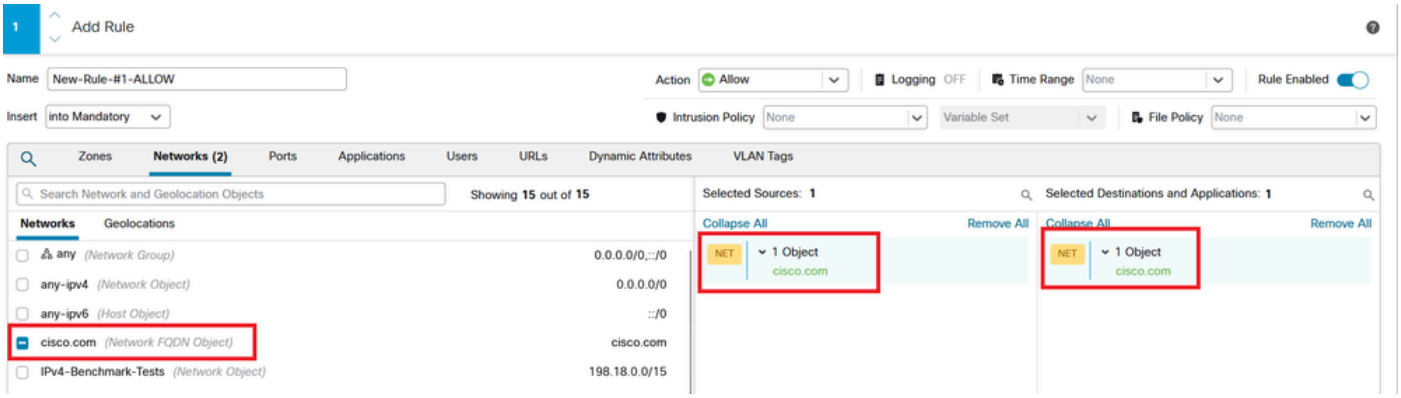

이미지 3. 새 확장 액세스 목록 규칙 메뉴

3단계. 확장 ACL이 생성되어 PBR 컨피그레이션에 사용할 수 있도록 적중할 수 없는 규칙을 생성합니다.



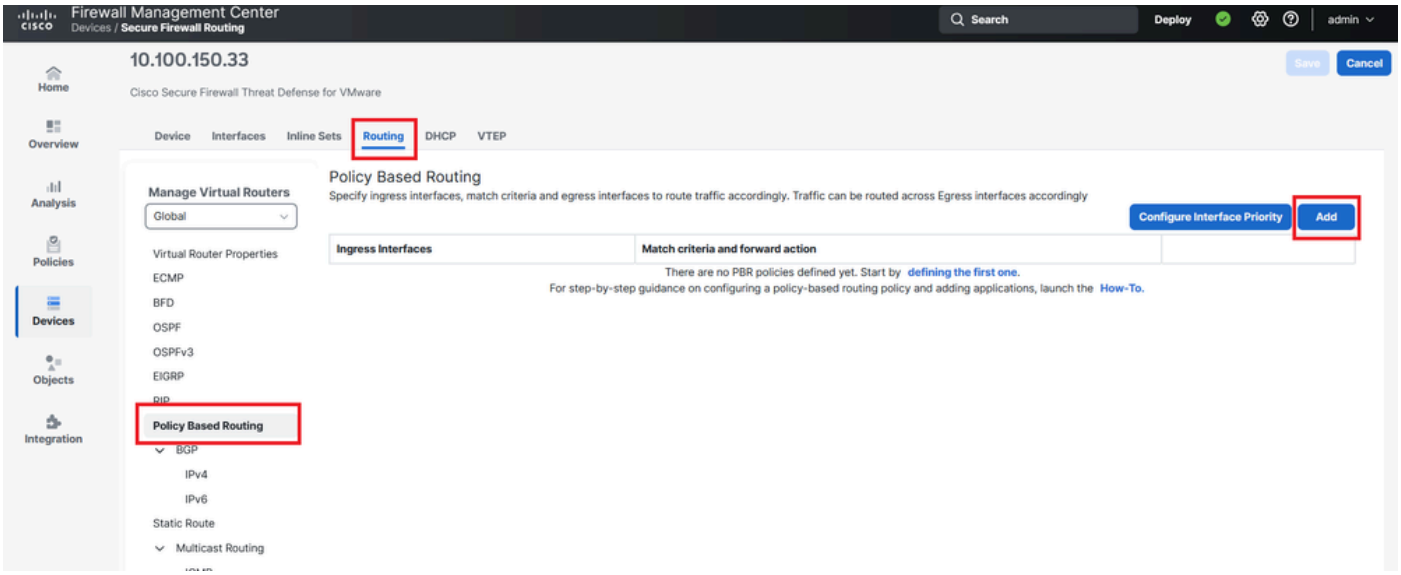

이미지 4. 적중할 수 없는 액세스 목록 규칙 컨피그레이션

4단계. FQDN 객체를 사용하여 FTD를 대상으로 하는 ACP(액세스 제어 정책)에 대한 규칙을 생성해야 합니다. FMC는 FlexConfig 개체를 통해 참조할 수 있도록 FQDN 개체를 FTD에 배포합니다.



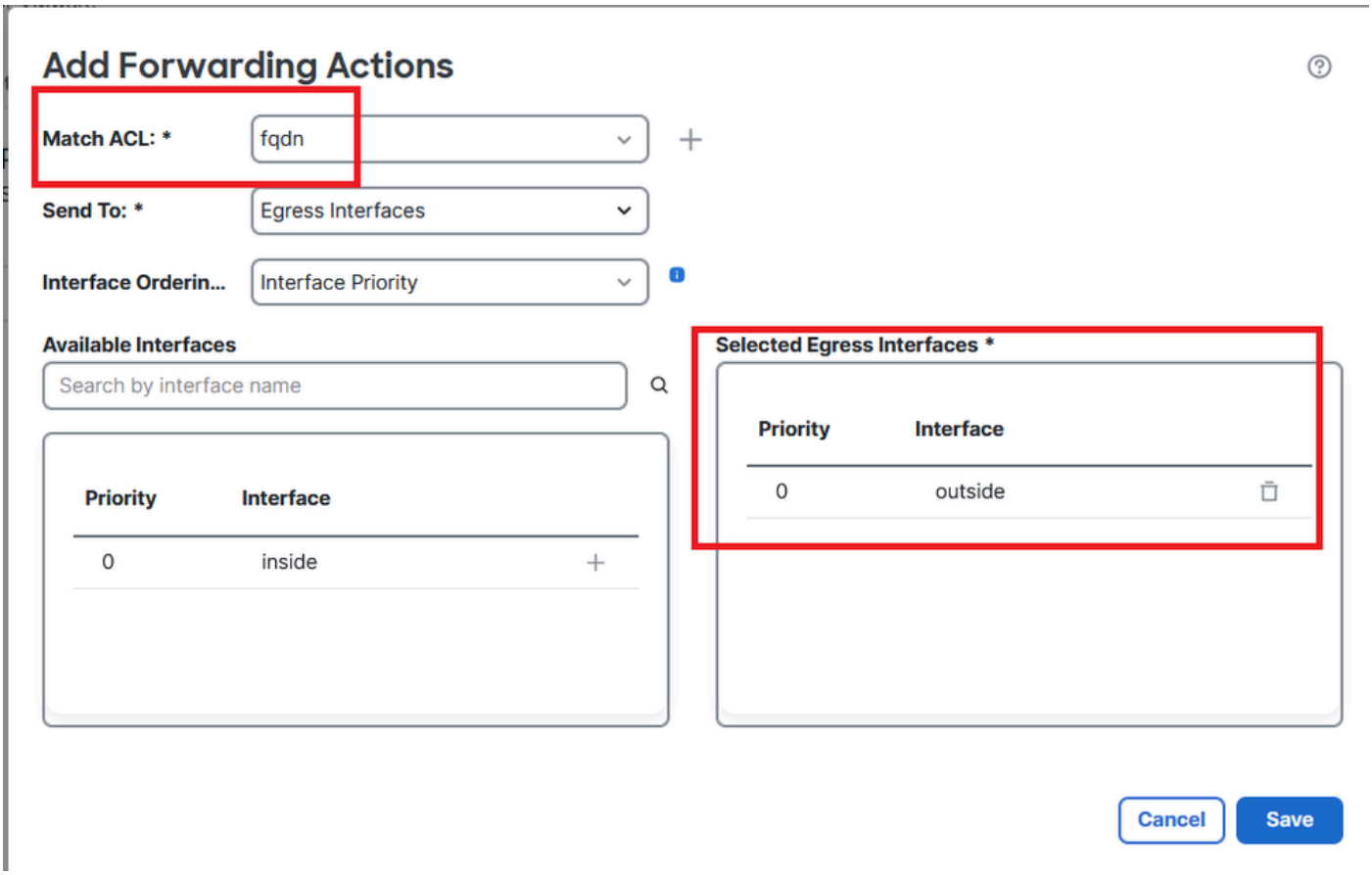

이미지 5. FQDN 개체가 있는 ACP 규칙

5단계. Devices(디바이스) > Device Management(디바이스 관리)의 FTD로 이동하고 Routing(라우팅) 탭을 선택한 다음 Policy Based Routing(정책 기반 라우팅) 섹션으로 이동합니다.



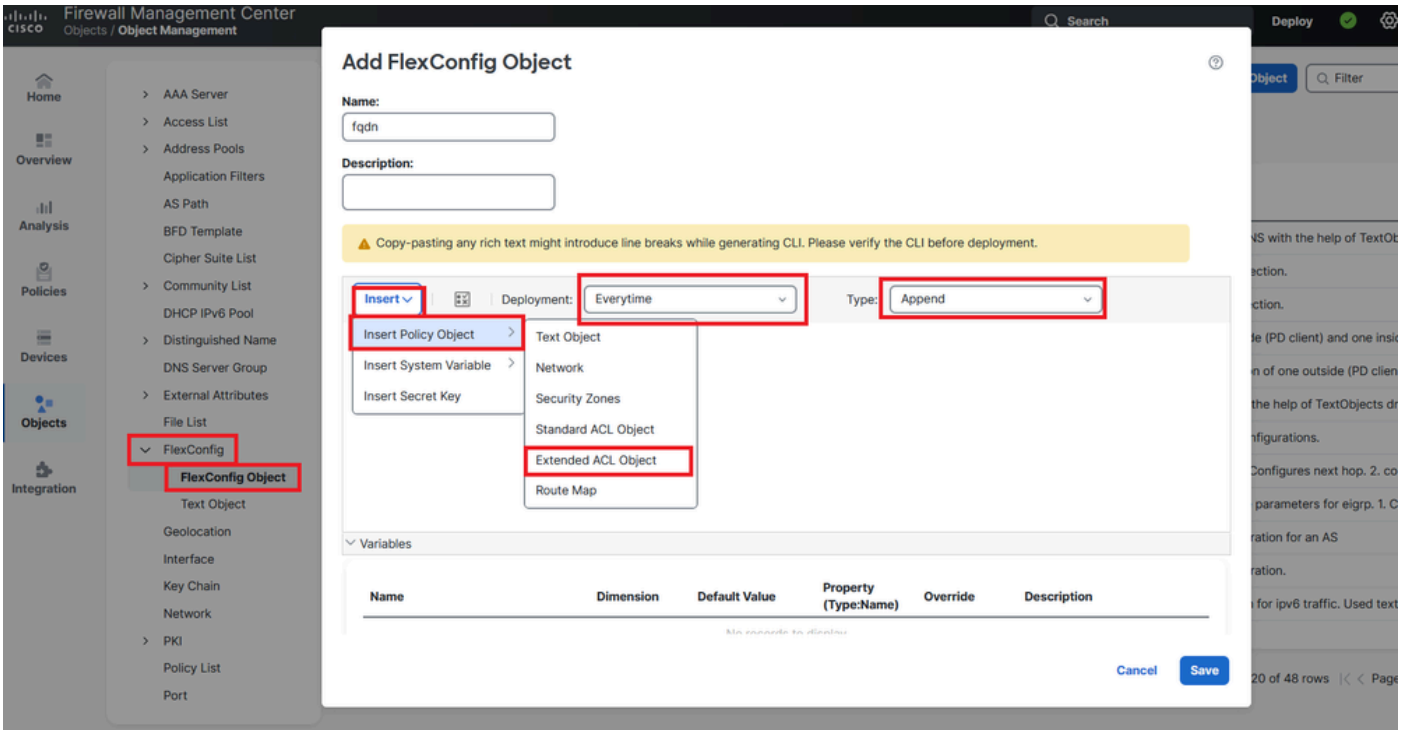

이미지 6. PBR 메뉴

6단계. 이전에 구성된 ACL을 사용하여 인터페이스에 PBR을 구성하고 구축합니다.



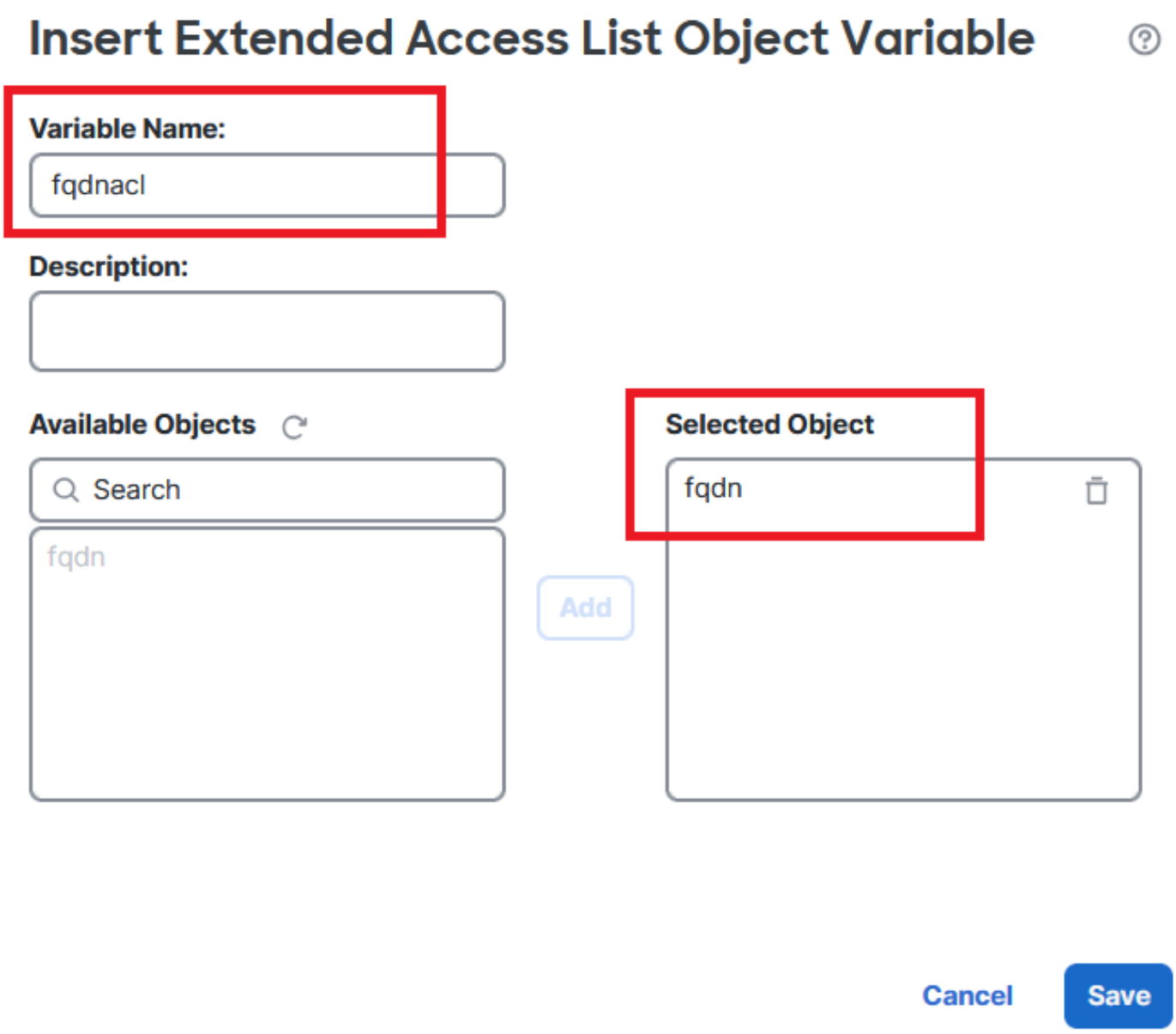

이미지 7. PBR 인터페이스 및 ACL 선택 메뉴

7단계. Objects(개체) > Object Management(개체 관리) > FlexConfig > Object(개체)로 이동하고 새 개체를 만듭니다.




이미지 8. FlexConfig 개체 컨피그레이션 메뉴

8단계. Insert(삽입) > Extended ACL Object(확장 ACL 개체)를 선택하고 변수 이름을 지정한 다음 앞서 생성한 확장 ACL을 선택합니다. 변수는 사용한 이름으로 추가됩니다.




이미지 9. FlexConfig 개체에 대한 변수 만들기

9단계. ACL에 사용할 각 FQDN 객체에 대해 이 라인을 입력합니다.

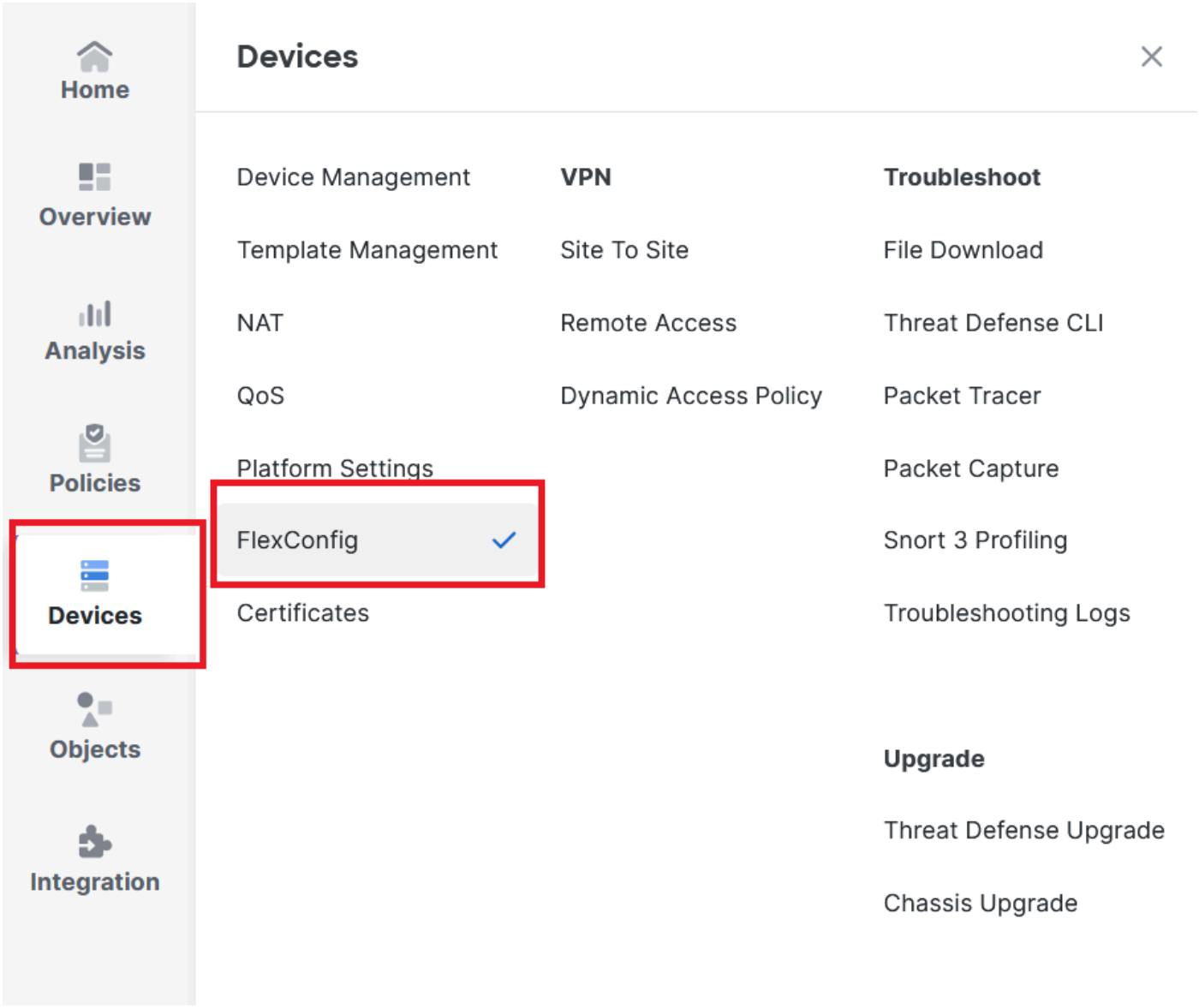
<#root>

```
access-li $
```

```
extended permit ip any object
```

10단계. FlexConfig 개체를 Everytime(항상) > Append(추가)로 저장합니다.

11단계 Devices(디바이스) > FlexConfig(FlexConfig 정책) 메뉴로 이동합니다.

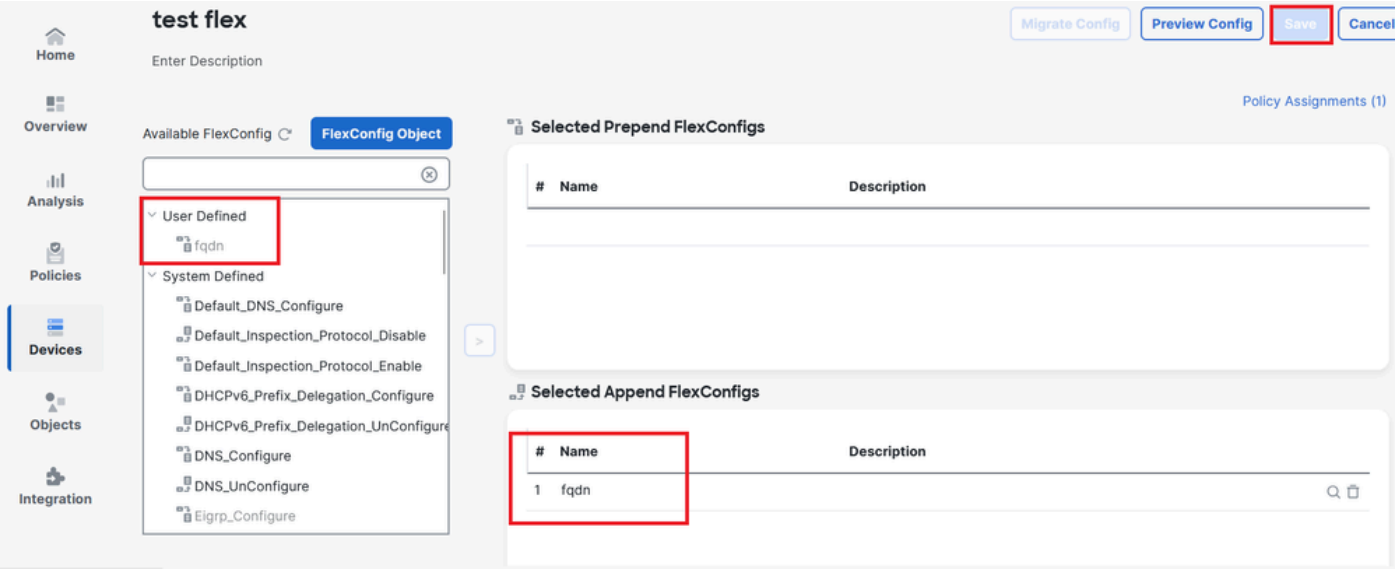



이미지 10. FlexConfig 정책 메뉴에 대한 경로

12단계. 새 FlexConfig 정책을 생성하거나 FTD에 이미 할당된 정책을 선택합니다.

이미지 11. 새 FlexConfig 정책 편집 또는 생성

13단계. Policy에 FlexConfig 객체를 추가하고, 저장하고, 구축합니다.




이미지 12. FlexConfig Policy에 FlexConfig 개체 추가

# 다음을 확인합니다.

인그레스 인터페이스에는 자동 생성된 경로 맵이 포함된 policy-route가 있습니다.

<#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**

route-map에는 사용된 대상 인터페이스가 있는 선택한 ACL이 포함됩니다.

<#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**

액세스 목록에는 참조에 사용되는 호스트와 FlexConfig를 통해 추가한 추가 규칙이 포함됩니다.

```
<#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
```

인그레스 인터페이스에서 PBR 단계에 도달했는지 확인하기 위한 소스로 패킷 추적기를 수행할 수 있습니다.

```
<#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
```

# 일반적인 문제

## 두 번째 구축 후 PBR 작동 중지

액세스 목록에 FQDN 개체 규칙이 여전히 포함되어 있는지 확인하십시오.

이 경우 규칙이 더 이상 존재하지 않음을 알 수 있습니다.

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

FlexConfig 개체가 Deployment: Everytime and Type: Append로 설정되어 있는지 확인합니다. 이 규칙은 향후 구축에 적용될 때마다 적용됩니다.

## FQDN이 확인되지 않음

FQDN을 ping하려고 하면 잘못된 호스트 이름에 대한 메시지가 표시됩니다.

```
<#root>

firepower#

ping cisco.com

               ^

ERROR: % Invalid Hostname
```

DNS 컨피그레이션을 확인합니다. 서버 그룹에서 연결 가능한 DNS 서버가 있어야 하며, 도메인 조회 인터페이스가 해당 서버에 연결할 수 있어야 합니다.

<#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.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.