FDM을 사용하여 FTD에 이중 ISP 구성

목차

소개

이 문서에서는 보안 방화벽 시리즈용 FDM(Firewall Device Manager)을 사용하여 이중 ISP(Internet Service Provider) 장애 조치를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 라우팅
- 방화벽 장치 관리자 대시보드 지식

- 최소 2개의 인터넷 서비스 공급자가 보안 방화벽에 연결되었습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

· 7.7.X 버전 이상을 실행하는 Cisco Secure Firewall

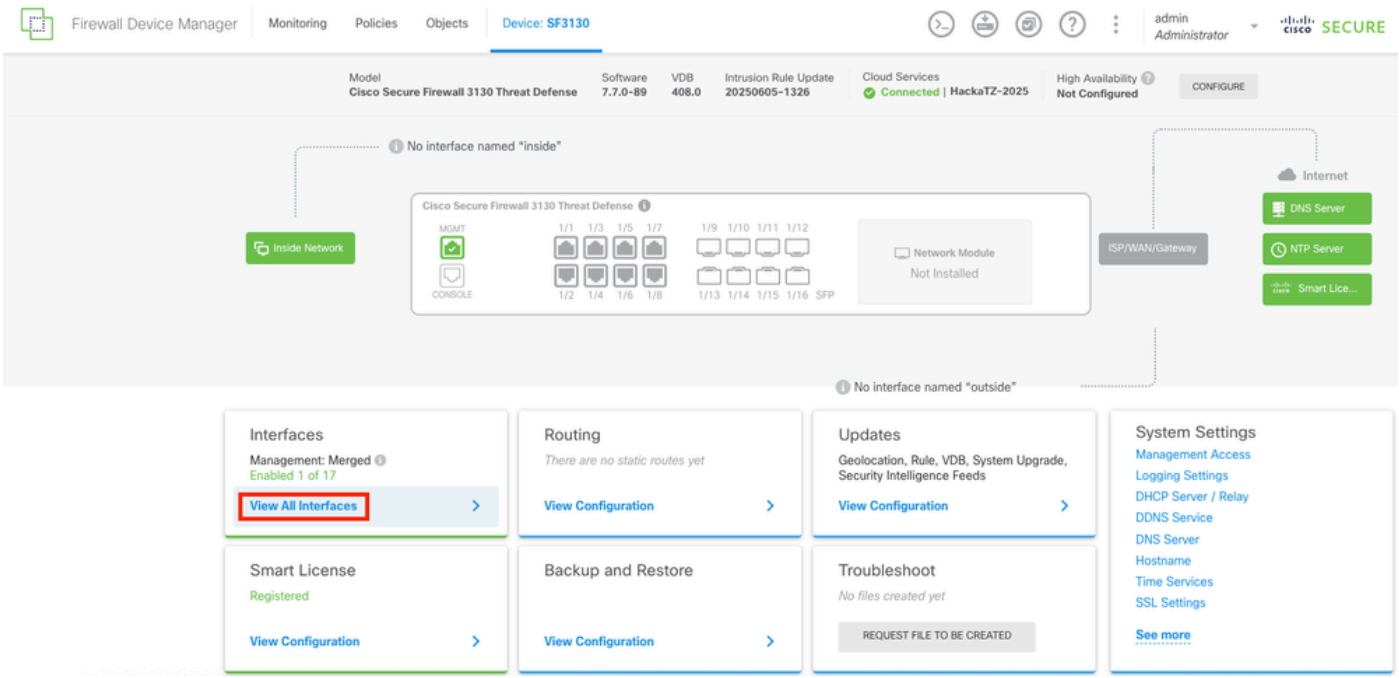
· 7.7.0 버전의 Secure Firewall 3130

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.

구성

1단계.

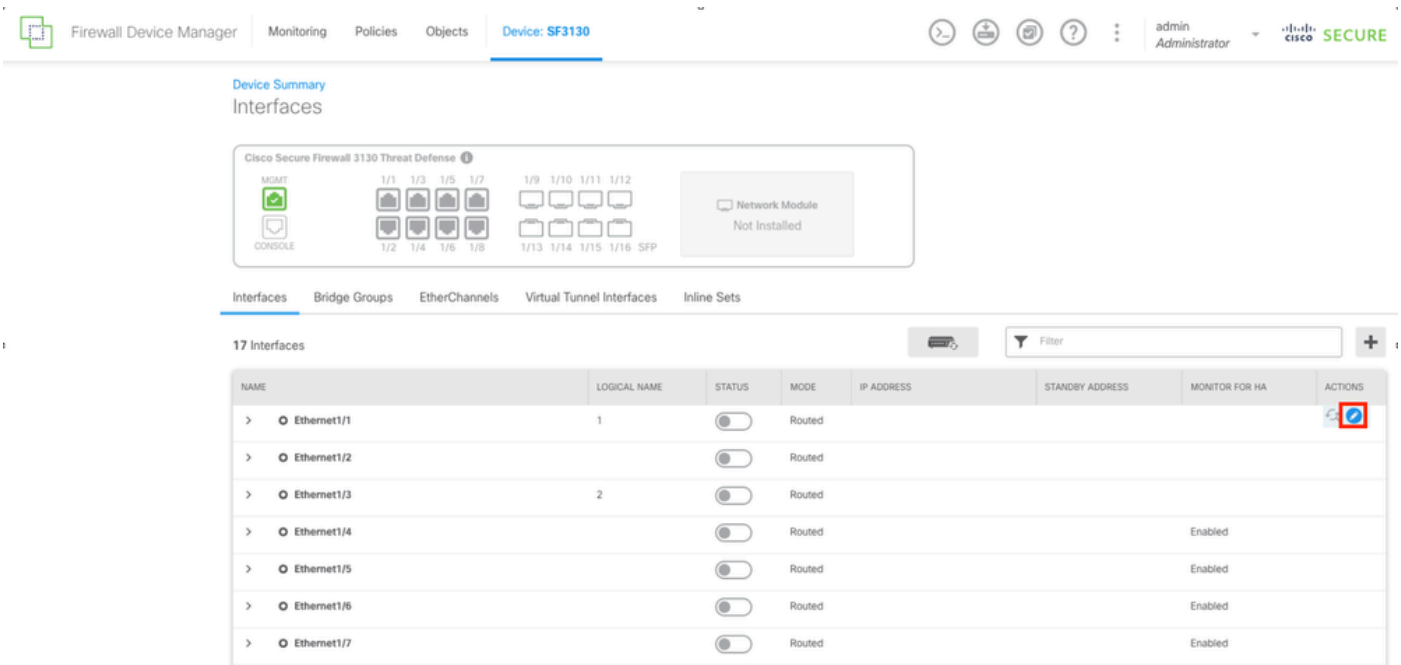
보안 방화벽의 FDM에 로그인하고 [모든 인터페이스 보기] 단추를 선택하여 인터페이스 섹션으로 이동합니다.



FDM 기본 대시보드

2단계.

기본 ISP 연결을 위한 인터페이스를 구성하려면 원하는 인터페이스를 선택하여 시작합니다. 계속하려면 해당 인터페이스 버튼을 선택합니다. 이 예에서 사용되는 인터페이스는 Ethernet1/1입니다.

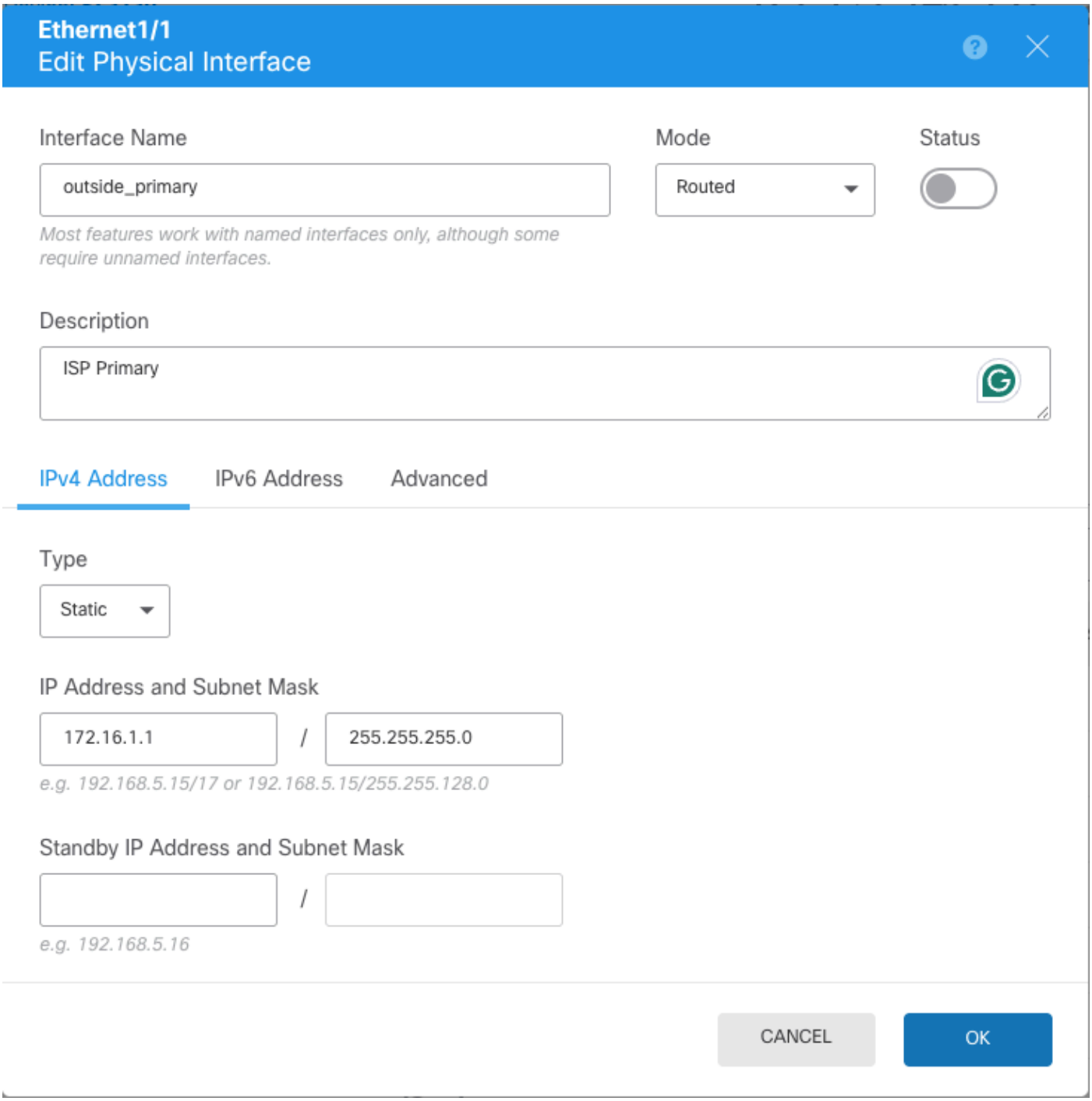


Interfaces 탭

3단계.

기본 ISP 연결을 위한 올바른 매개변수로 인터페이스를 구성합니다. 이 예에서 인터페이스는

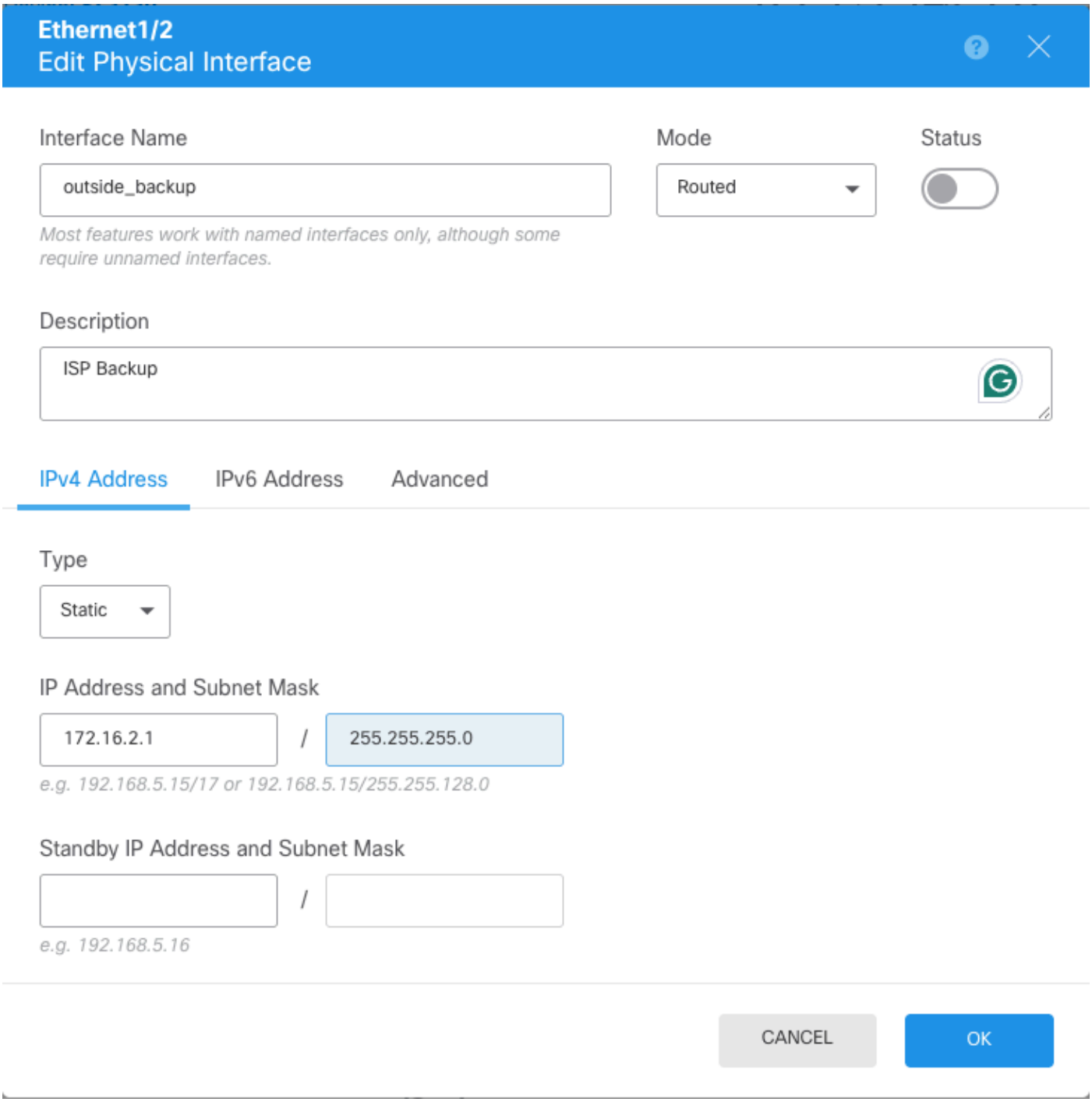
outside_primary입니다.



기본 ISP 인터페이스 컨피그레이션

4단계.

보조 ISP 인터페이스에 대해 동일한 프로세스를 반복합니다. 이 예에서는 인터페이스 Ethernet1/2가 사용됩니다.

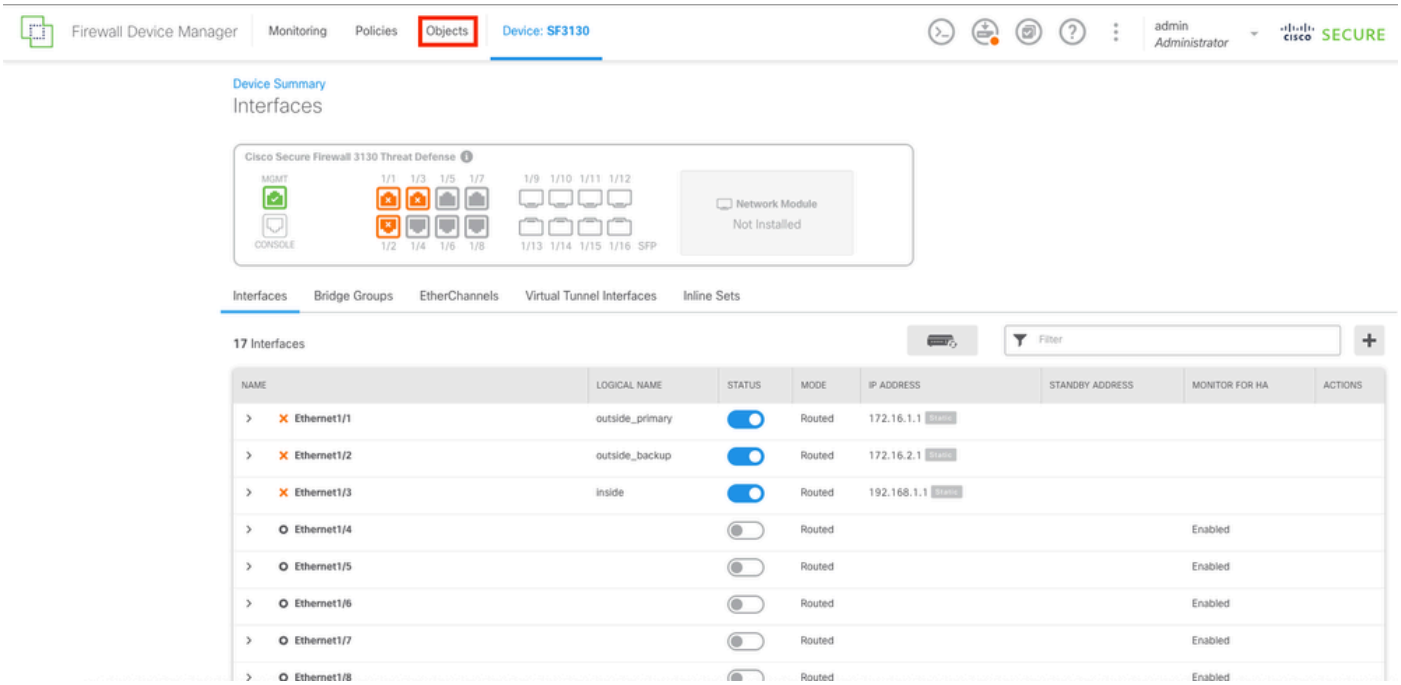


보조 ISP 인터페이스 컨피그레이션

5단계.

ISP에 대해 2개의 인터페이스를 구성한 후 다음 단계는 기본 인터페이스에 대한 SLA 모니터를 설정하는 것입니다.

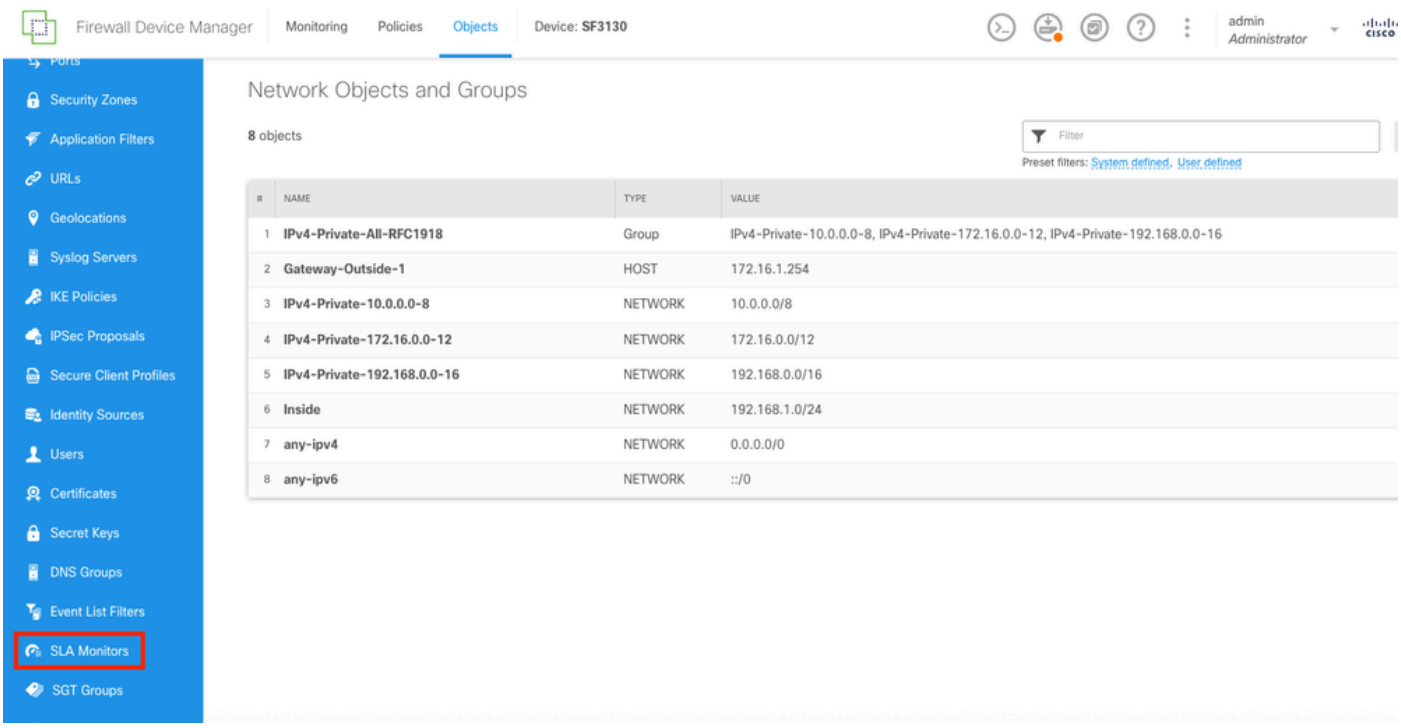
메뉴 상단에 위치한 객체 버튼을 선택하여 객체 섹션으로 이동합니다.



구성된 인터페이스

6단계.

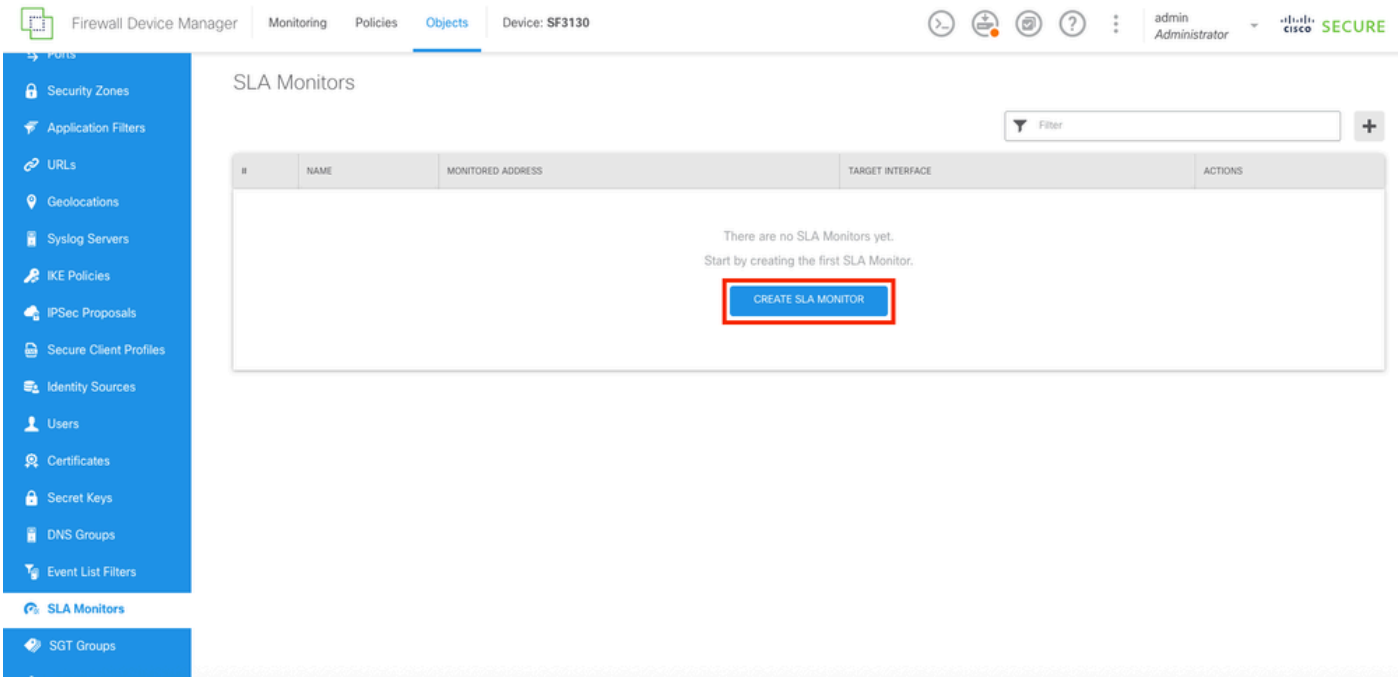
왼쪽 열에서 SLA Monitors(SLA 모니터) 버튼을 선택합니다.



Objects 화면

7단계.

Create SLA Monitor(SLA 모니터 생성) 버튼을 선택하여 새 SLA 모니터를 생성합니다.



SLA 모니터 섹션

8단계.

기본 ISP 연결을 위한 매개변수를 구성합니다.

Add SLA Monitor Object

Name

Outside_Primary_ISP

Description

Monitor for ISP Primary

Monitor Address

Gateway-Outside-1

Target Interface

outside_primary (Ethernet1/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000 milliseconds

0 - 2147483647

Timeout

5000 milliseconds

0 - 604800000

Frequency

60000 milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28 bytes

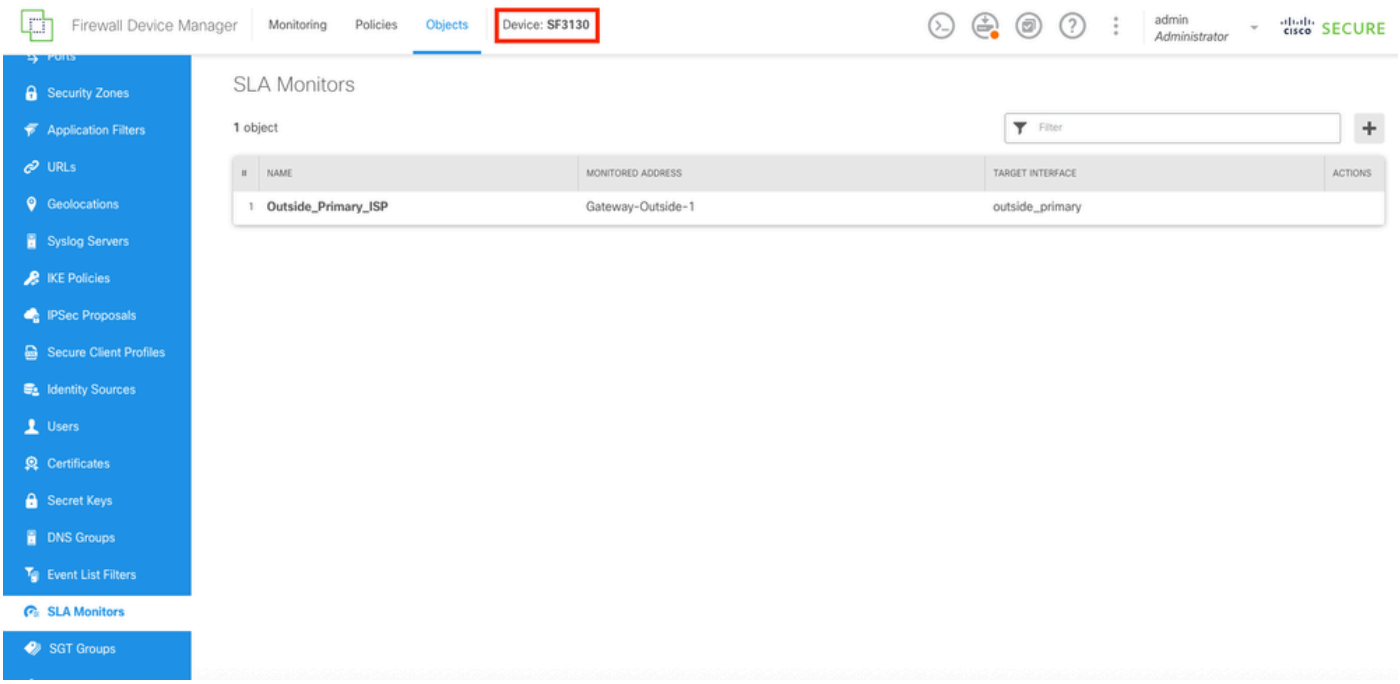
0 - 16384

CANCEL OK

SLA 객체 생성

9단계.

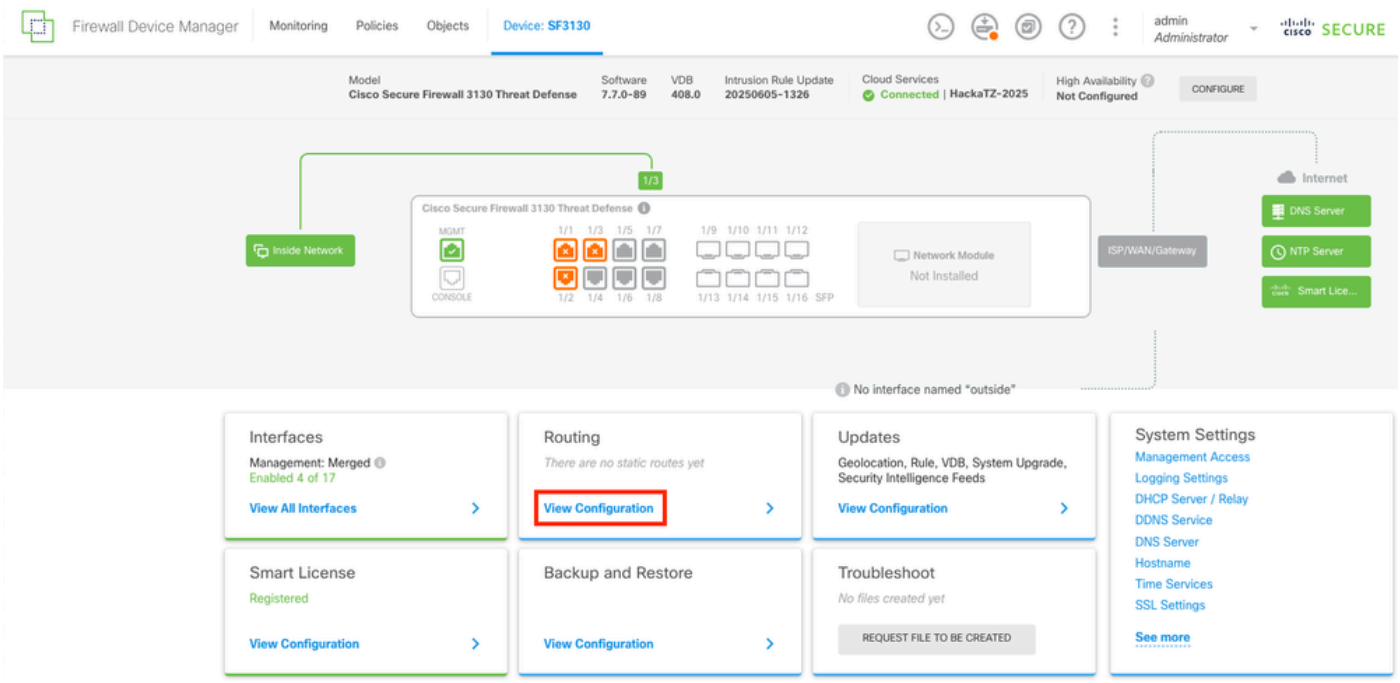
객체가 생성되면 인터페이스에 대한 고정 경로가 객체를 생성해야 합니다. Device 버튼을 선택하여 기본 대시보드로 이동합니다.



SLA 모니터 생성됨

10단계.

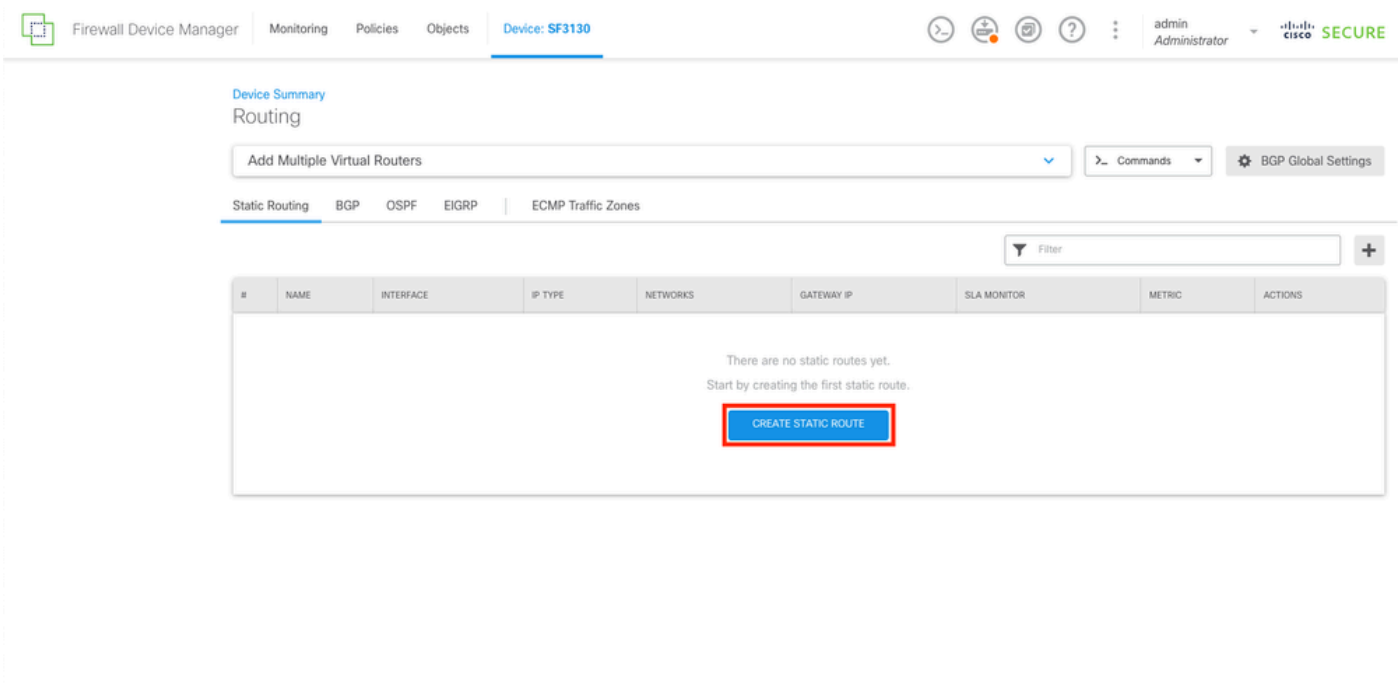
라우팅 패널에서 구성 보기를 선택하여 라우팅 섹션으로 이동합니다.



기본 대시보드

11단계.

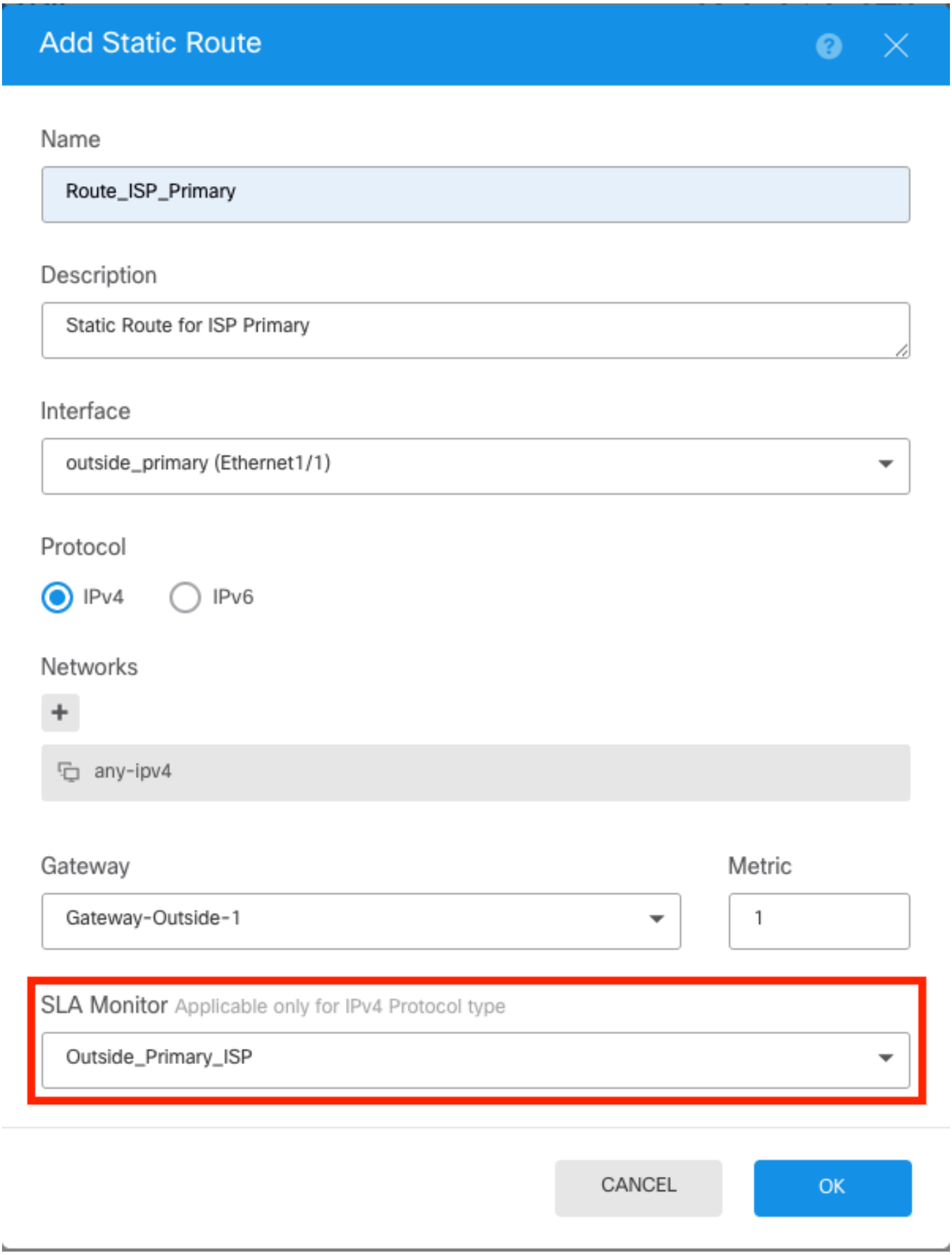
Static Routing 탭에서 두 ISP에 대한 2개의 기본 고정 경로를 생성합니다. 새 고정 경로를 생성하려면 CREATE STATIC ROUTE 버튼을 선택합니다.



정적 라우팅 섹션

12단계.

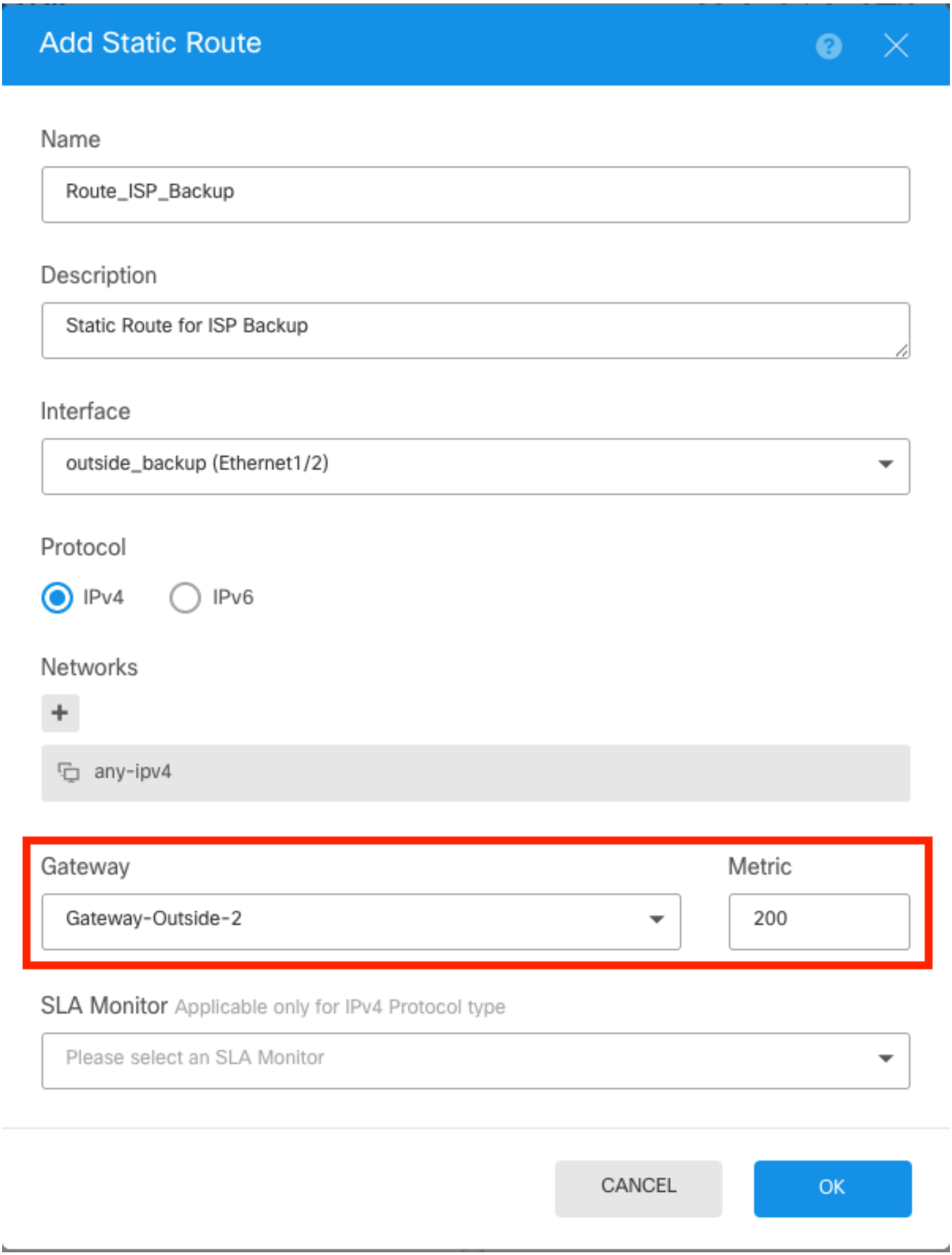
먼저 기본 ISP에 대한 고정 경로를 생성합니다. 마지막에 마지막 단계에서 생성한 SLA 모니터 객체를 추가합니다.



기본 ISP의 고정 경로

13단계.

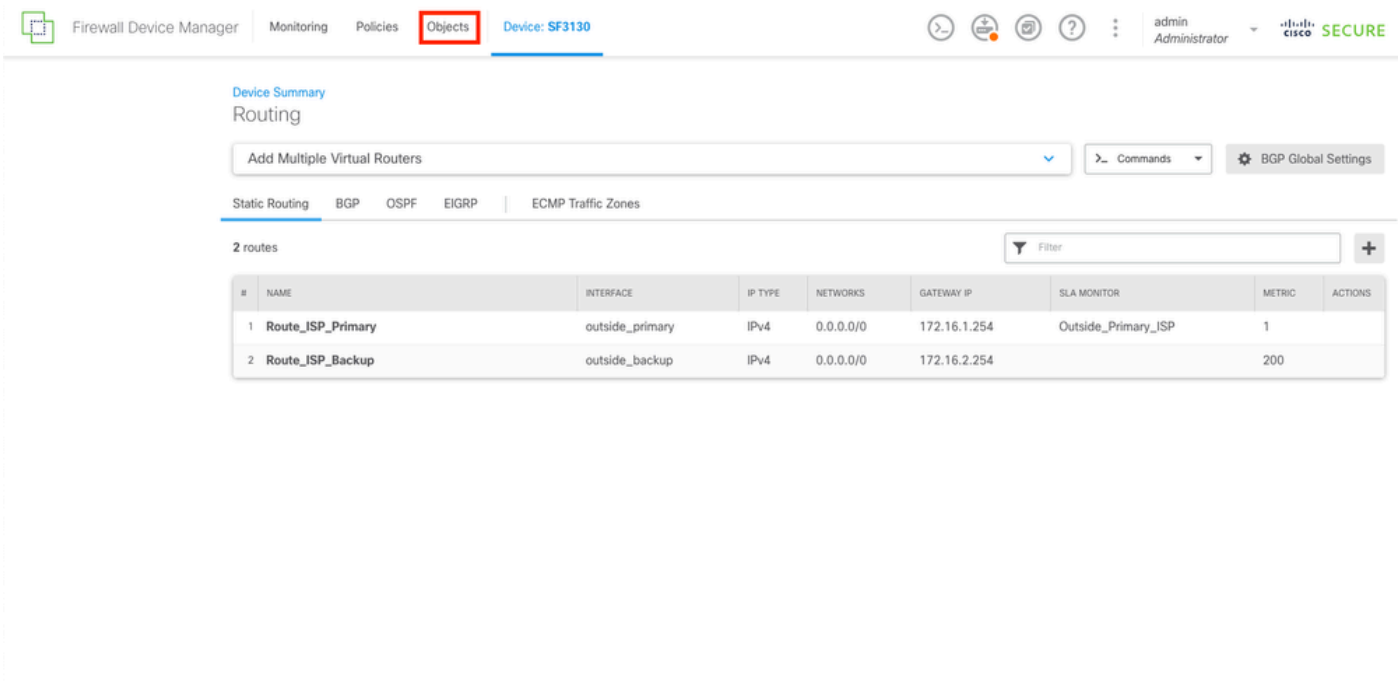
마지막 단계를 반복하여 ISP 보조에 대해 적절한 게이트웨이와 다른 메트릭을 갖는 기본 경로를 생성합니다. 이 예에서는 200으로 증가했습니다.



보조 ISP에 대한 고정 경로

14단계.

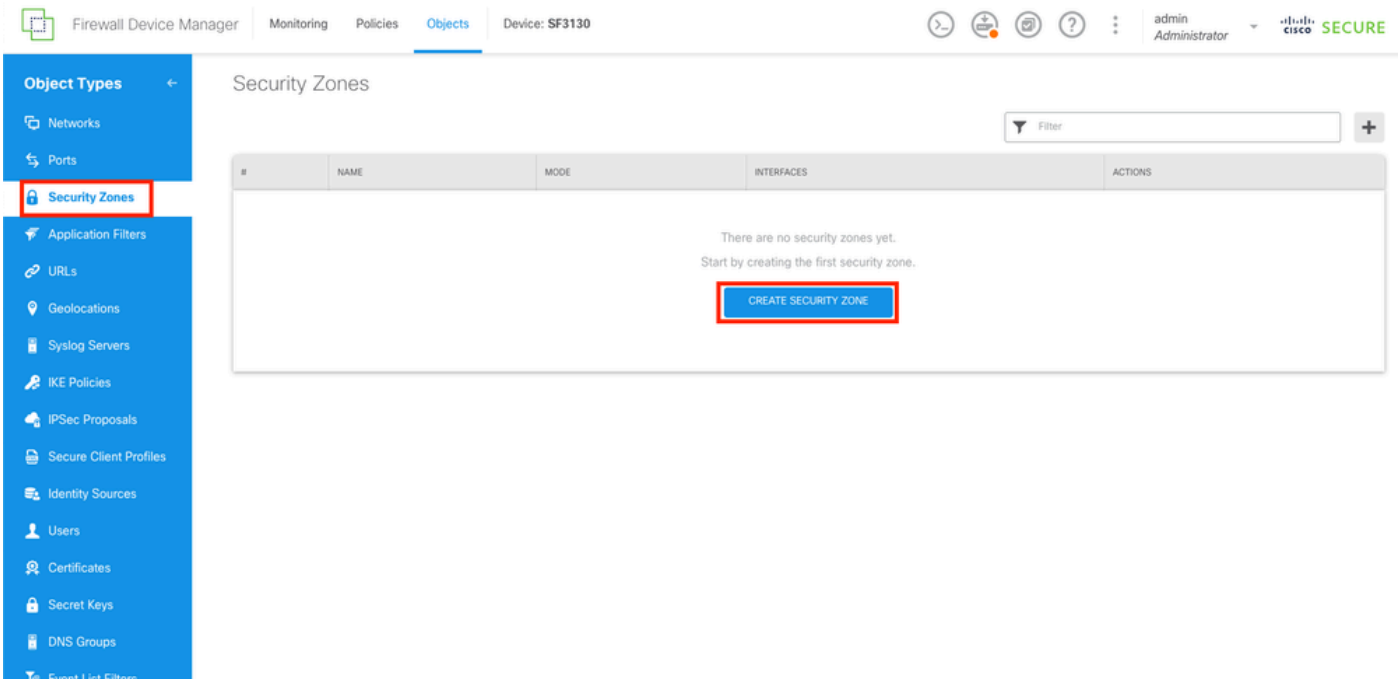
두 고정 경로가 모두 생성되면 보안 영역을 생성해야 합니다. 맨 위의 Objects 버튼을 선택하여 Objects 섹션으로 이동합니다.



생성된 고정 경로

15단계.

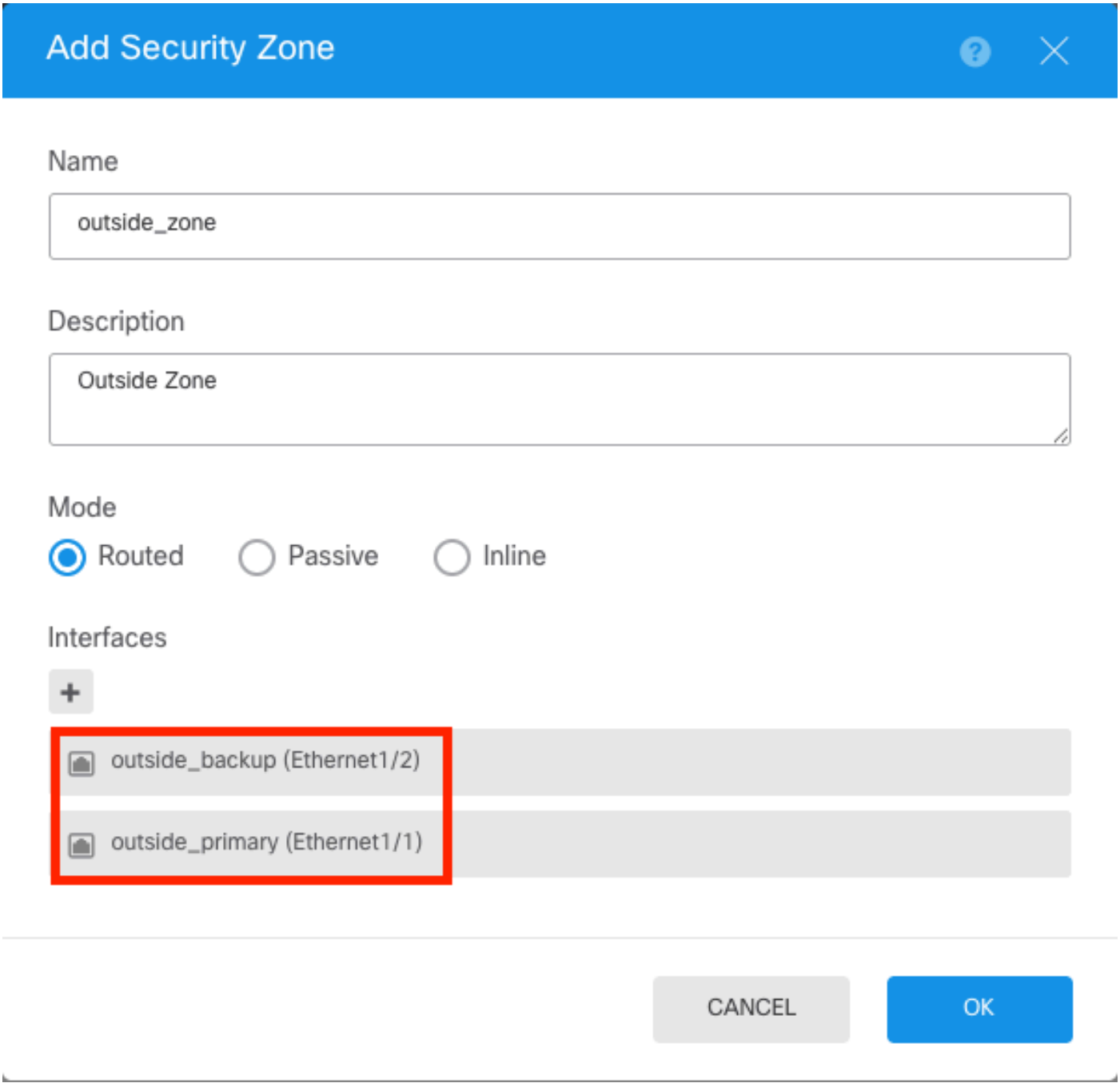
왼쪽 열에서 Security Zones(보안 영역) 버튼을 선택하여 Security Zones(보안 영역) 섹션으로 이동한 다음 CREATE SECURITY ZONE(보안 영역 생성) 버튼을 선택하여 새 영역을 생성합니다.



보안 영역 섹션

16단계.

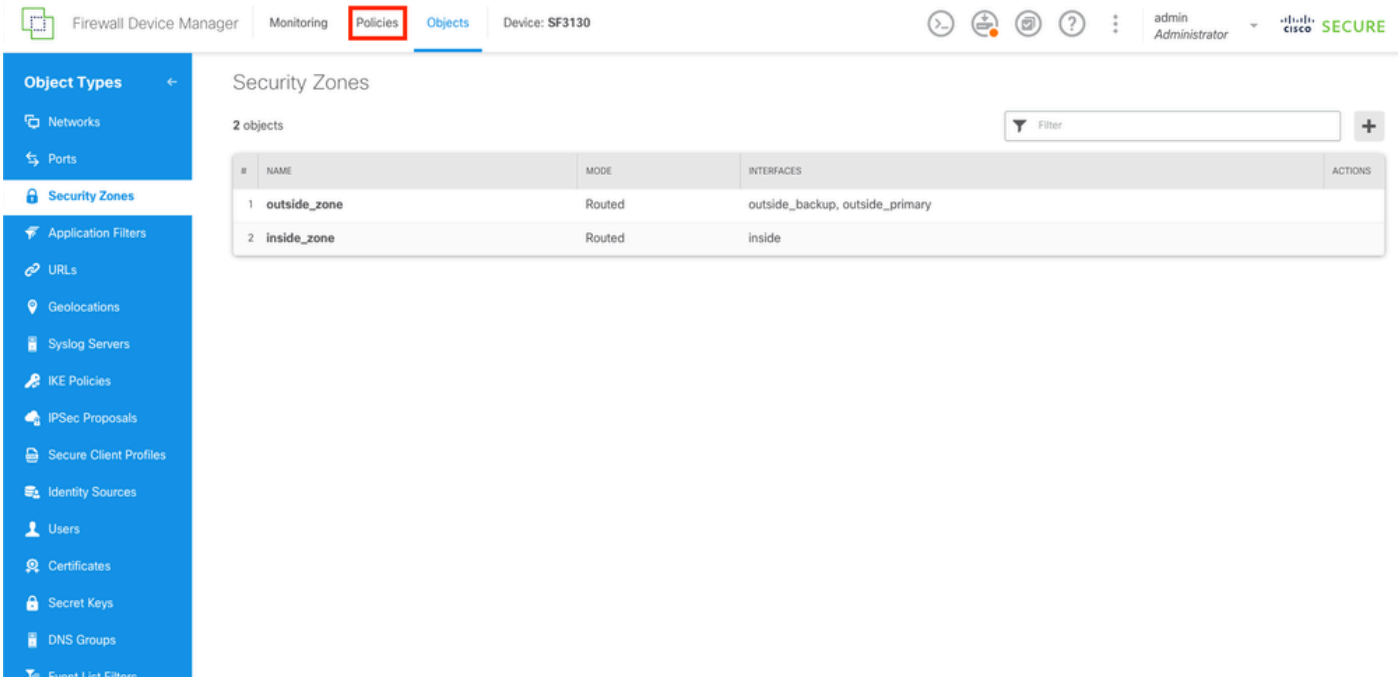
ISP 연결을 위한 두 외부 인터페이스로 Outside Security Zone을 생성합니다.



외부 보안 영역

17단계.

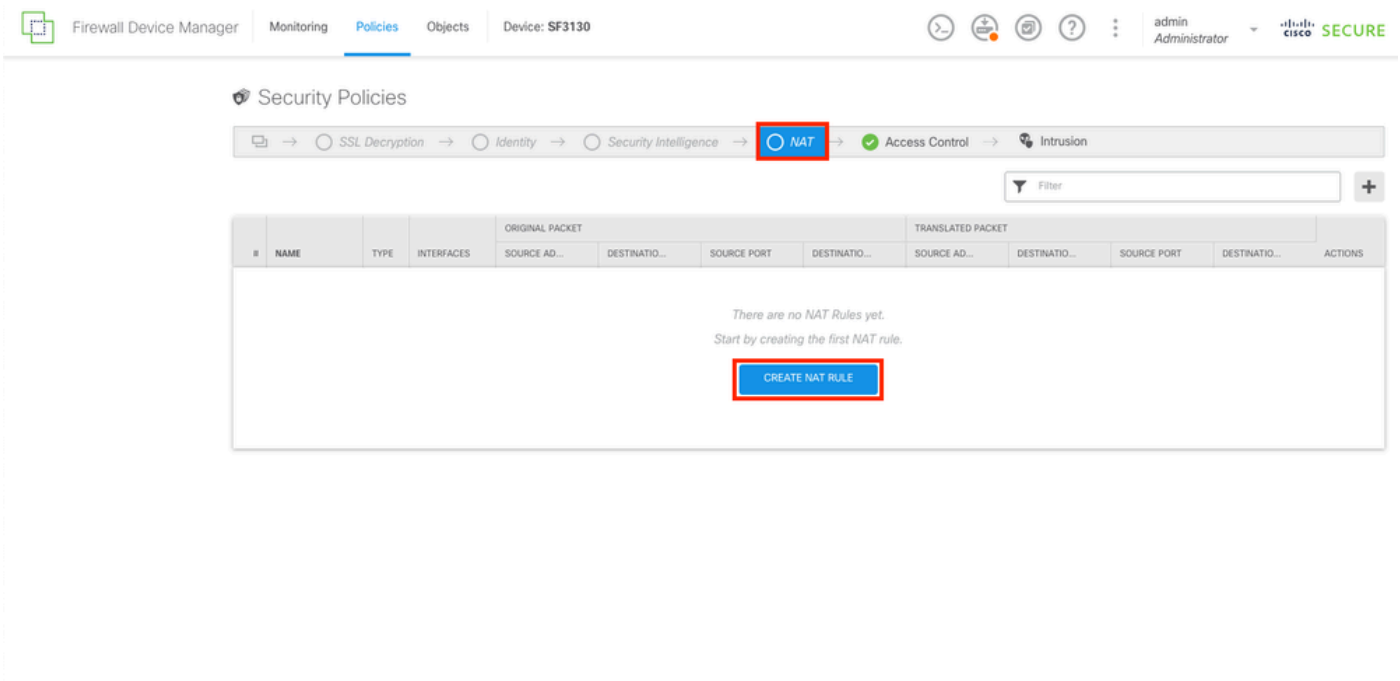
보안 영역이 생성되면 NAT를 생성해야 합니다. 상단의 Policies 버튼을 선택하여 Policies 섹션으로 이동합니다.



보안 영역 생성됨

18단계.

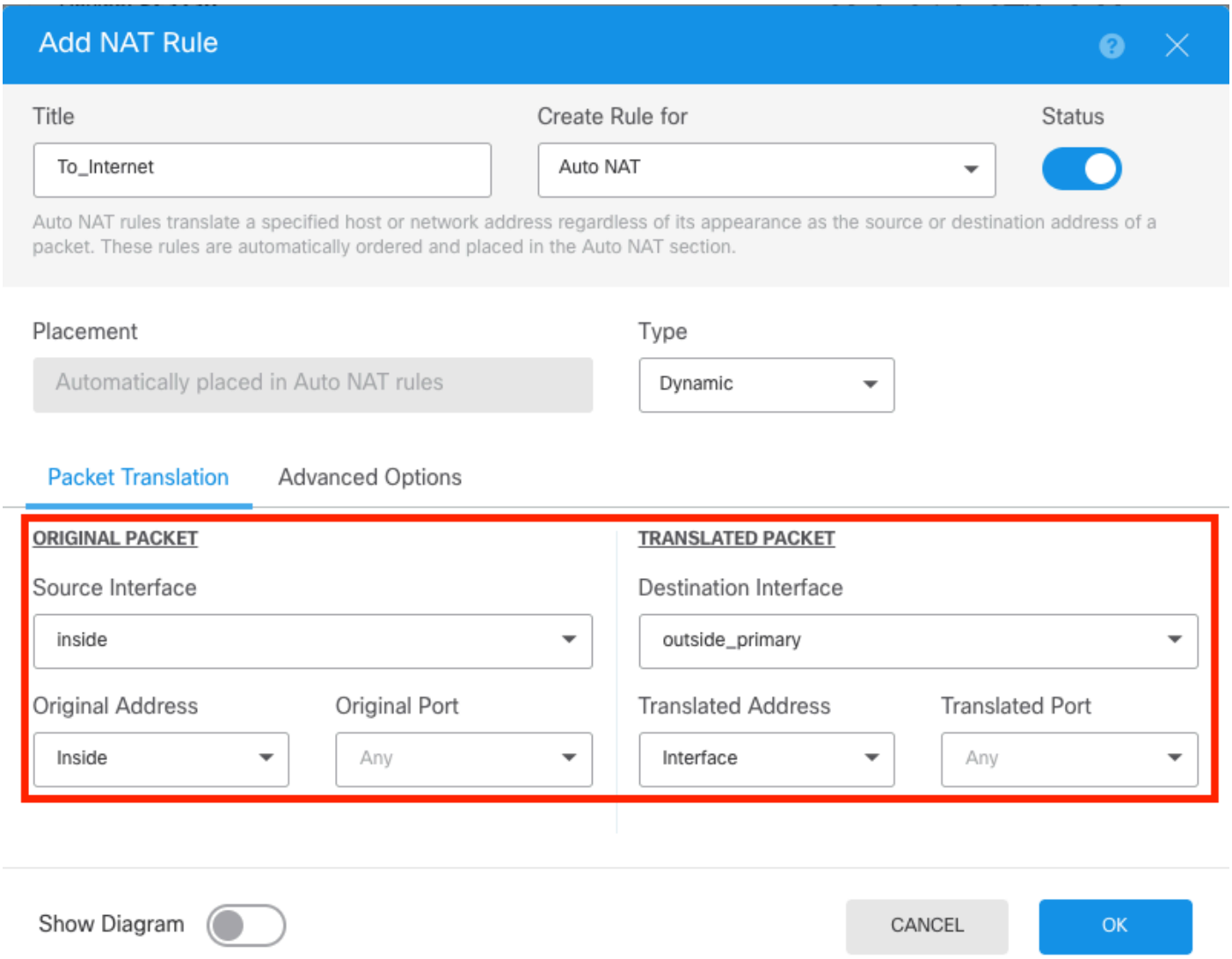
NAT 버튼을 선택하여 NAT 섹션으로 이동한 다음 CREATE NAT RULE 버튼을 선택하여 새 규칙을 생성합니다.



NAT 섹션

19단계.

ISP 장애 조치를 수행하려면 컨피그레이션에 외부 인터페이스를 통한 경로 2개가 있어야 합니다. 먼저, 기본 외부 인터페이스에서 기본 ISP에 연결합니다.

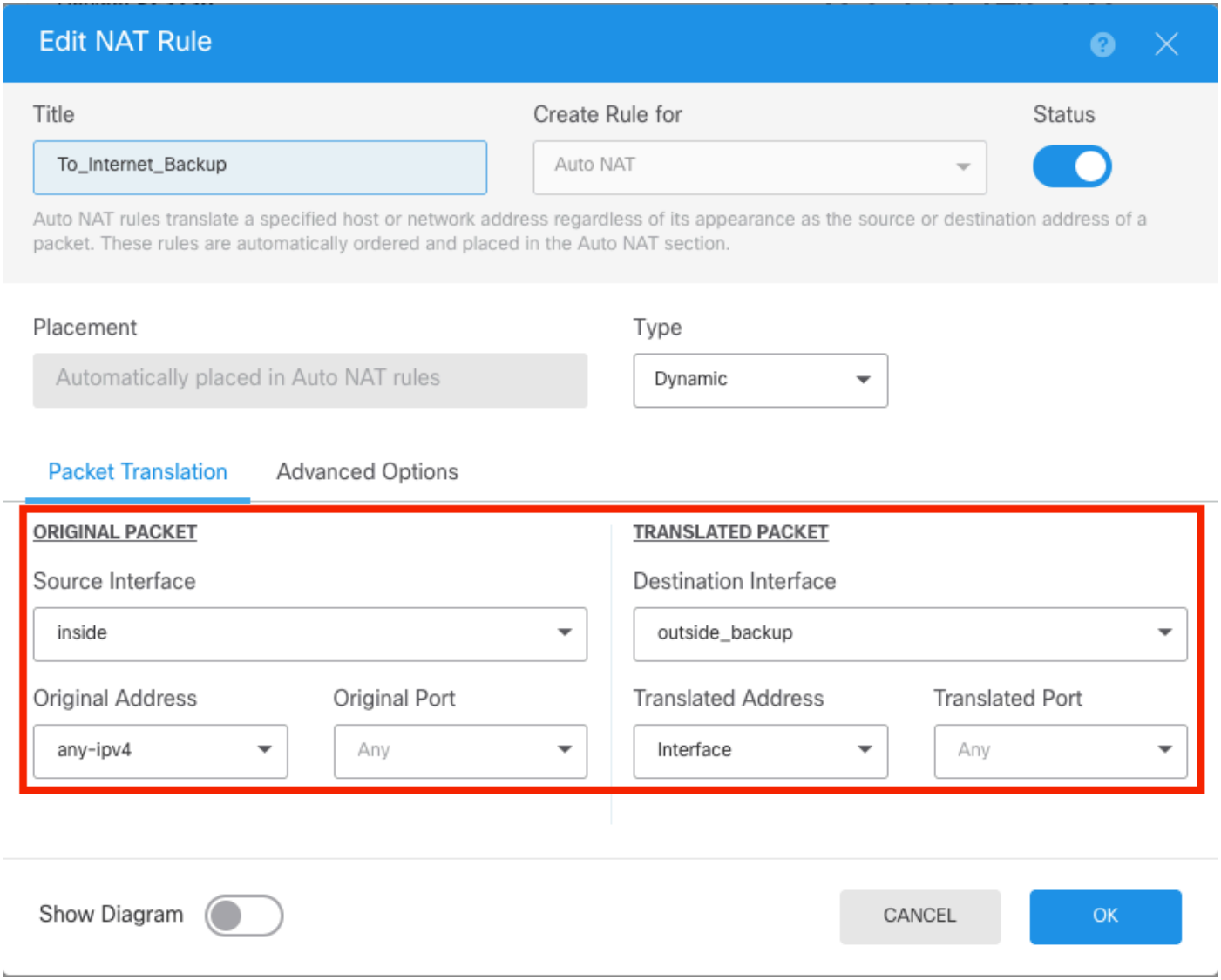


기본 ISP용 NAT

20단계.

이제 보조 ISP 연결을 위한 두 번째 NAT입니다.

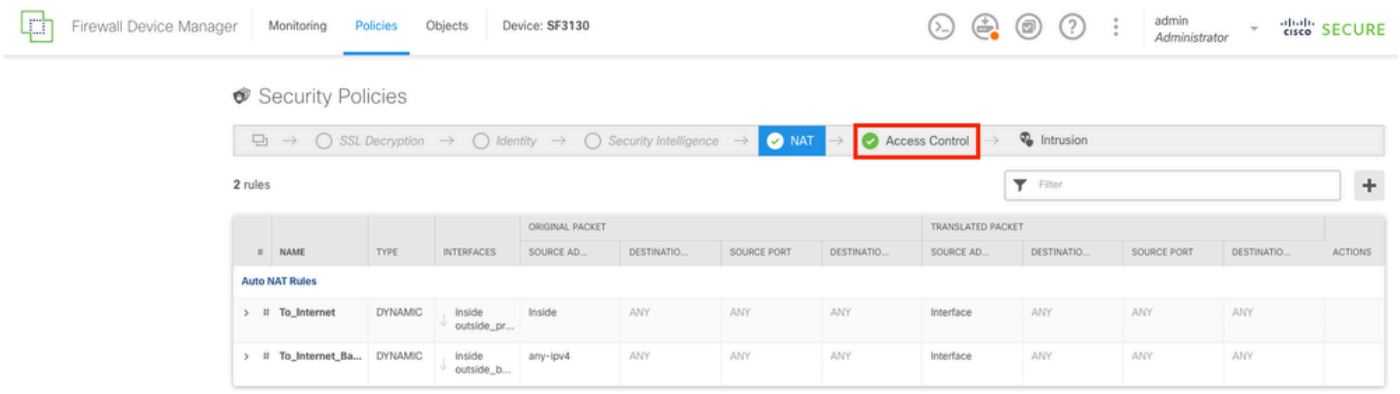
참고: 원래 주소에는 동일한 네트워크를 사용할 수 없습니다. 이 예에서 보조 ISP의 경우 Original Address는 object any-ipv4입니다.



보조 ISP용 NAT

21단계.

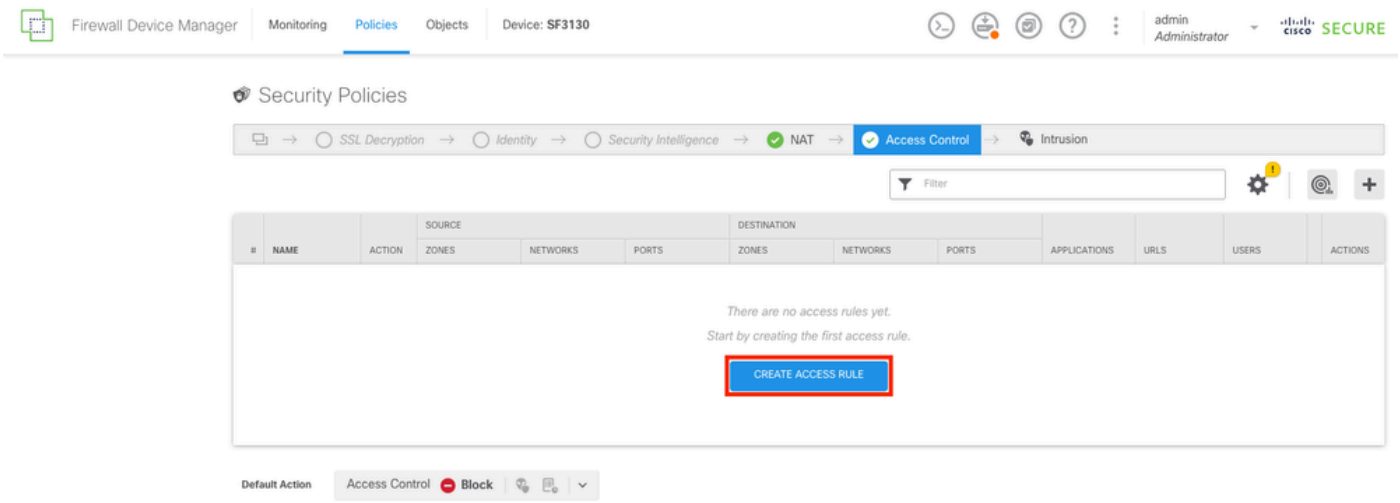
두 NAT 규칙을 모두 생성한 후에는 아웃바운드 트래픽을 허용하도록 액세스 제어 규칙을 설정해야 합니다. Access Control(액세스 제어) 버튼을 선택합니다.



NAT 규칙 생성됨

22단계.

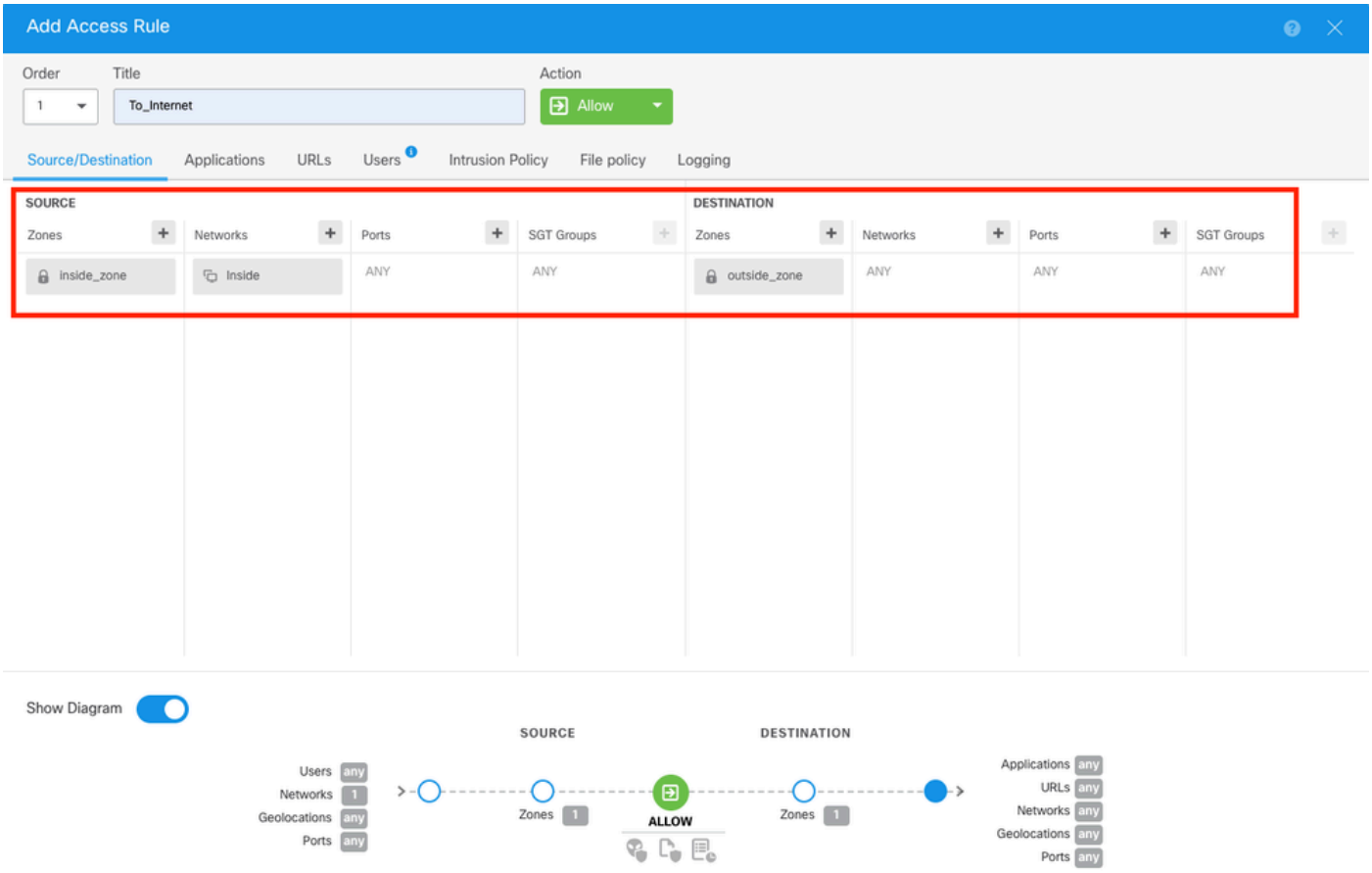
액세스 제어 규칙을 생성하려면 CREATE ACCESS RULE(액세스 규칙 생성) 버튼을 선택합니다.



액세스 제어 섹션

23단계.

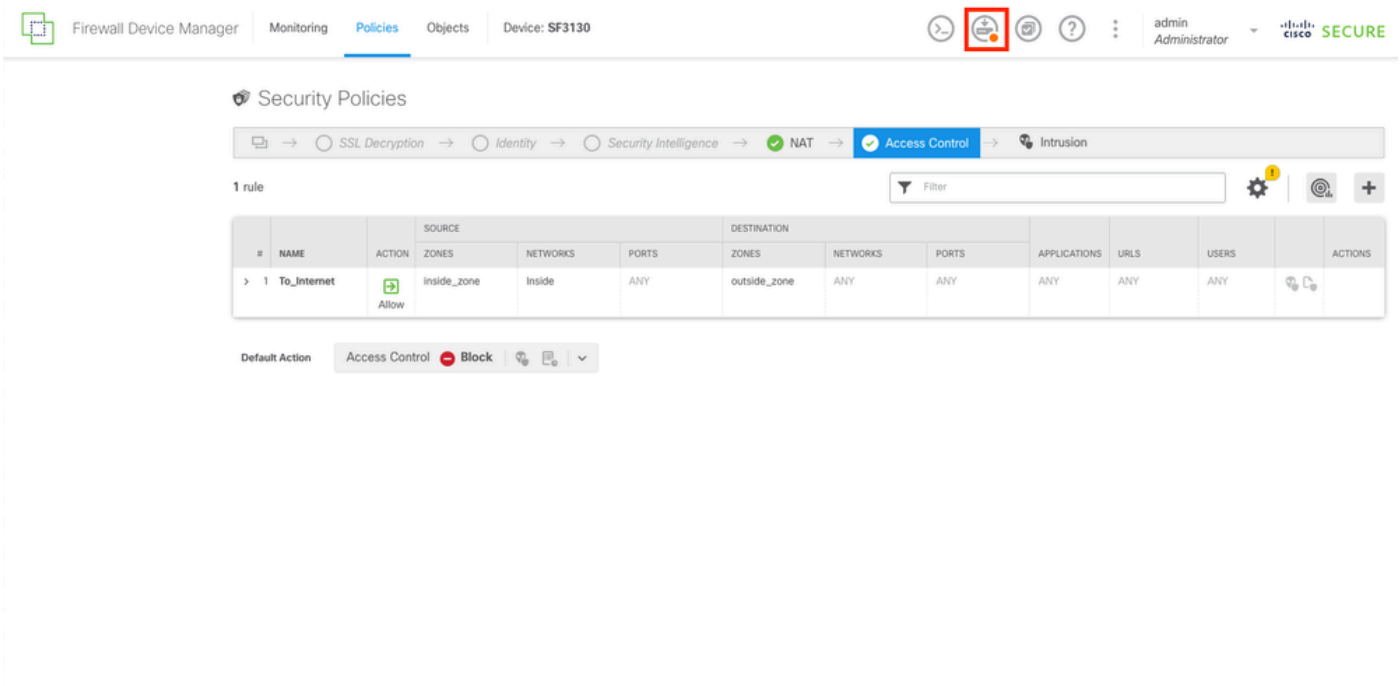
원하는 영역 및 네트워크를 선택합니다.



액세스 제어 규칙

24단계.

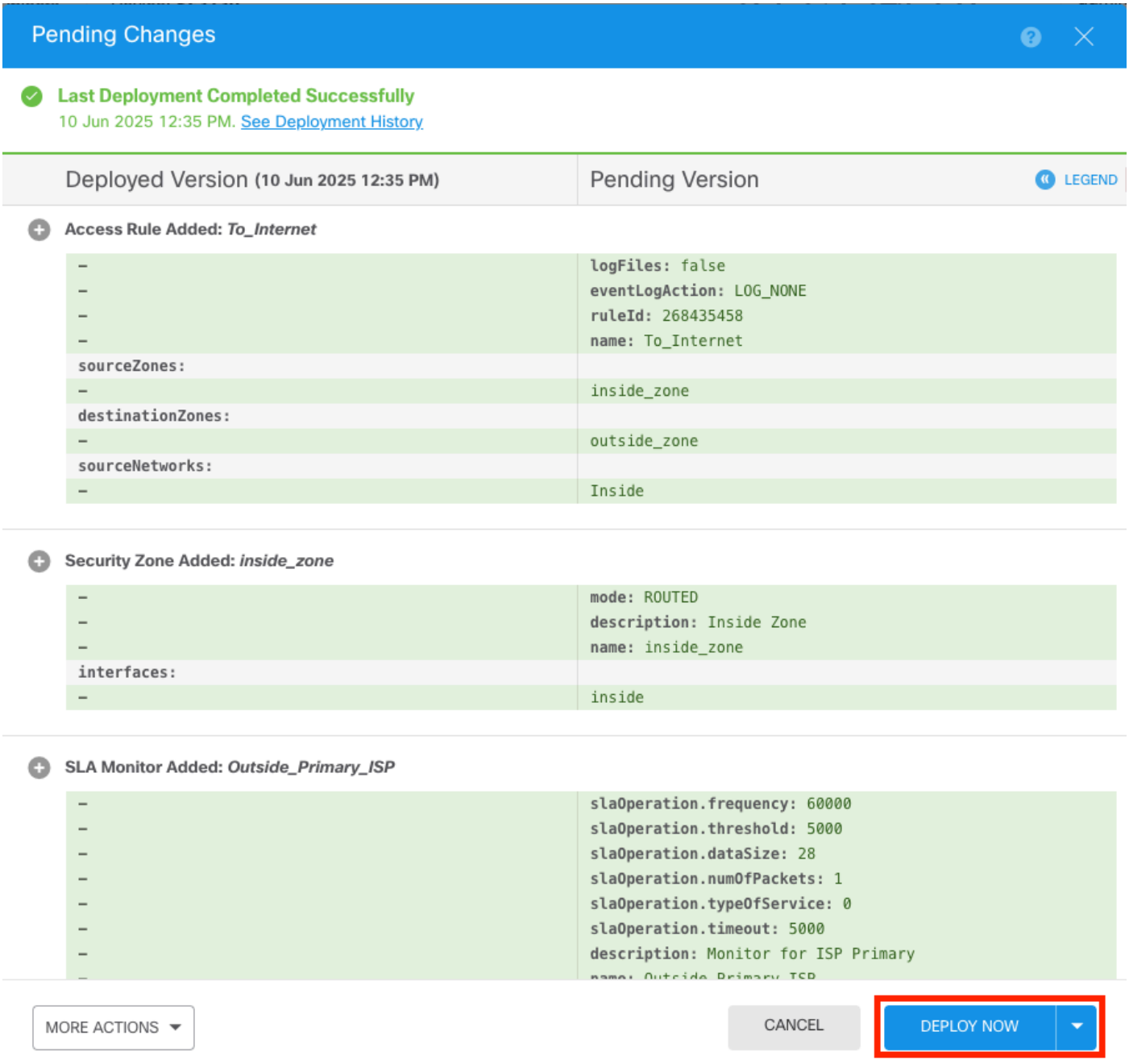
액세스 제어 규칙이 생성되면 상단의 Deploy(구축) 버튼을 선택하여 모든 변경 사항을 구축합니다.



액세스 제어 규칙 생성됨

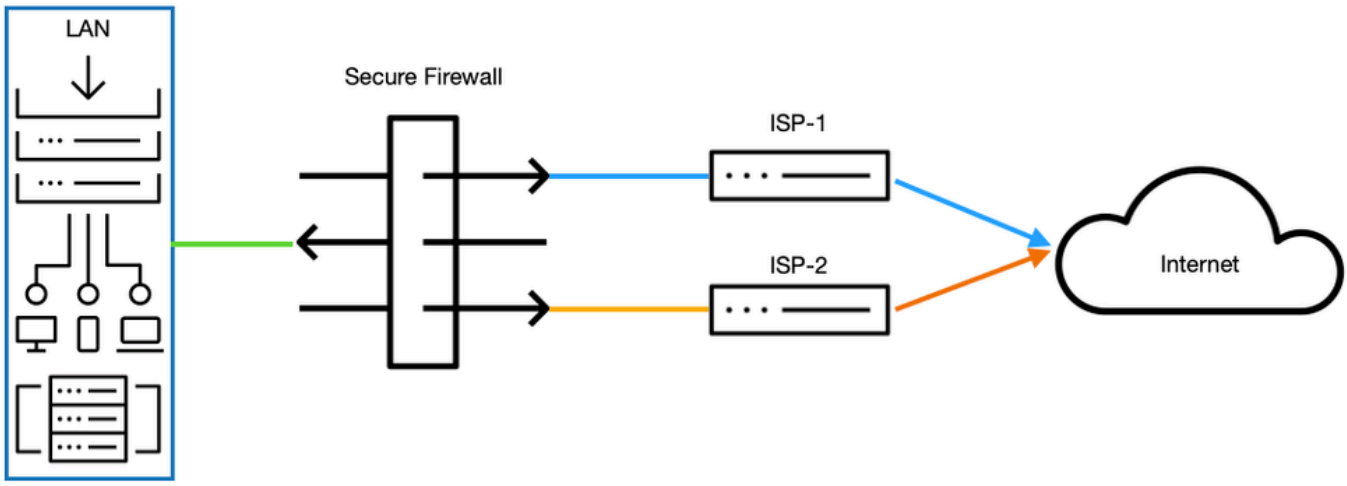
25단계.

변경 사항을 확인한 다음 Deploy Now(지금 구축) 버튼을 선택합니다.



구축 확인

네트워크 다이어그램



네트워크 다이어그램

다음을 확인합니다.

<#root>

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

SF3130#

show ip

System IP Addresses:
Interface Name IP address Subnet mask Method
Ethernet1/1 outside_primary 172.16.1.1 255.255.255.0 manual

------------> THE PRIMARY INTERFACE OF THE ISP IS SET

Ethernet1/2 outside_backup 172.16.2.1 255.255.255.0 manual

------------> THE SECONDARY INTERFACE OF THE ISP IS SET

Ethernet1/3 inside 192.168.1.1 255.255.255.0 manual

SF3130#

show interface ip brief

Interface IP-Address OK? Method Status Protocol
Ethernet1/1 172.16.1.1 YES manual up up

------------------> THE INTERFACE IS UP AND RUNNING

```
Ethernet1/2 172.16.2.1  YES manual   up      up
```

------------------> THE INTERFACE IS UP AND RUNNING

```
Ethernet1/3 192.168.1.1 YES manual   up      up

SF3130#
```

show route

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

----> THE DEFAULT ROUTE IS CONNECTED THROUGH THE PRIMARY ISP

```
C  172.16.1.0  255.255.255.0   is directly connected, outside_primary
L  172.16.1.1  255.255.255.255 is directly connected, outside_primary
C  172.16.2.0  255.255.255.0   is directly connected, outside_backup
L  172.16.2.1  255.255.255.255 is directly connected, outside_backup
C  192.168.1.0 255.255.255.0   is directly connected, inside
L  192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#
```

show run route

```
route outside_primary 0.0.0.0 0.0.0.0 172.16.1.254 1 track 1
route outside_backup  0.0.0.0 0.0.0.0 172.16.2.254 200

SF3130#
```

show sla monitor configuration

---> CHECKING THE SLA MONITOR CONFIGURATION

```
SA Agent, Infrastructure Engine-II
Entry number: 539523651
Owner:
Tag:
Type of operation to perform: echo
Target address: 172.16.1.254
Interface: outside_primary
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 3000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

SF3130#
```

show sla monitor operational-state

```
Entry number: 739848060
Modification time: 01:24:11.029 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
```

---------------------------> THE ISP PRIMARY IS IN A HEALTHY STATE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

AFTERARGBSETHBNDGFSHNDFGSDBFB

SF3130#
```

show interface ip brief

```
Interface   IP-Address  OK? Method Status Protocol
Ethernet1/1 172.16.1.1  YES manual  down   down
```

------------------> THE PRIMARY ISP IS DOWN

```
Ethernet1/2 172.16.2.1  YES manual   up     up
Ethernet1/3 192.168.1.1 YES manual   up     up

SF3130#
```

show route

```
Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [200/0] via 172.16.2.254, outside_backup
```

---------> AFTER THE ISP PRIMARY FAILS, INSTANTLY THE ISP BACKUP IS FAILOVER AND IS INSTALL IN THE ROUTI

```
C  172.16.2.0 255.255.255.0    is directly connected, outside_backup
L  172.16.2.1 255.255.255.255  is directly connected, outside_backup
C  192.168.1.0 255.255.255.0   is directly connected, inside
L  192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#
```

show sla monitor operational-state

```
Entry number: 739848060
Modification time: 01:24:11.140 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
```

```
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
```

----------> AFTER THE DOWNTIME OF THE PRIMARY ISP THE TIMEOUT IS FLAGGED

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

SF3130#
```

show route

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

----------> AFTER A FEW SECONDS ONCE THE PRIMARY INTERFACE IS BACK THE DEFAULT ROUTE INSTALLS AGAIN IN

```
C 172.16.1.0 255.255.255.0    is directly connected, outside_primary
L 172.16.1.1 255.255.255.255  is directly connected, outside_primary
C 172.16.2.0 255.255.255.0    is directly connected, outside_backup
L 172.16.2.1 255.255.255.255  is directly connected, outside_backup
C 192.168.1.0 255.255.255.0   is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside
```

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.