FDM에서 관리하는 FTD에서 IP SLA를 사용하여 ECMP 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소
- 배경 정보

구성

- 네트워크 다이어그램
- 설정
  - 0단계. 인터페이스/개체 사전 구성
  - 1단계. ECMP 영역 구성
  - 2단계. IP SLA 개체 구성
  - 3단계. 경로 추적을 사용하여 고정 경로 구성

다음을 확인합니다.

- 로드 밸런싱
- 잃어버린 경로

문제 해결

관련 정보

소개

이 문서에서는 FDM에서 관리하는 FTD에서 IP SLA와 함께 ECMP를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Secure Firewall Threat Defense)의 ECMP 컨피그레이션
- Cisco FTD(Secure Firewall Threat Defense)의 IP SLA 컨피그레이션
- Cisco FDM(Secure Firewall Device Manager)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 버전 7.4.1(빌드 172)

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

이 문서에서는 Cisco FDM에서 관리하는 Cisco FTD에서 ECMP(Equal-Cost Multi-Path)를 IP SLA(Internet Protocol Service Level Agreement)와 함께 구성하는 방법에 대해 설명합니다 . ECMP를 사용하면 FTD에서 인터페이스를 함께 그룹화하고 여러 인터페이스 간에 트래픽을 로드 밸런싱할 수 있습니다. IP SLA는 일반 패킷 교환을 통해 엔드 투 엔드 연결을 모니터링하는 메커니즘입니다. ECMP와 함께 IP SLA를 구현하여 다음 홉의 가용성을 보장할 수 있습니다. 이 예에서는 ECMP를 사용하여 두 ISP(Internet Service Provider) 회로에 패킷을 균등하게 분산시킵니다. 동시에 IP SLA는 연결을 추적하여 장애 발생 시 사용 가능한 회로로의 원활한 전환을 보장합니다.

이 문서의 구체적인 요구 사항은 다음과 같습니다.

- 관리자 권한이 있는 사용자 계정으로 디바이스에 액세스
- Cisco Secure Firewall Threat Defense 버전 7.1 이상

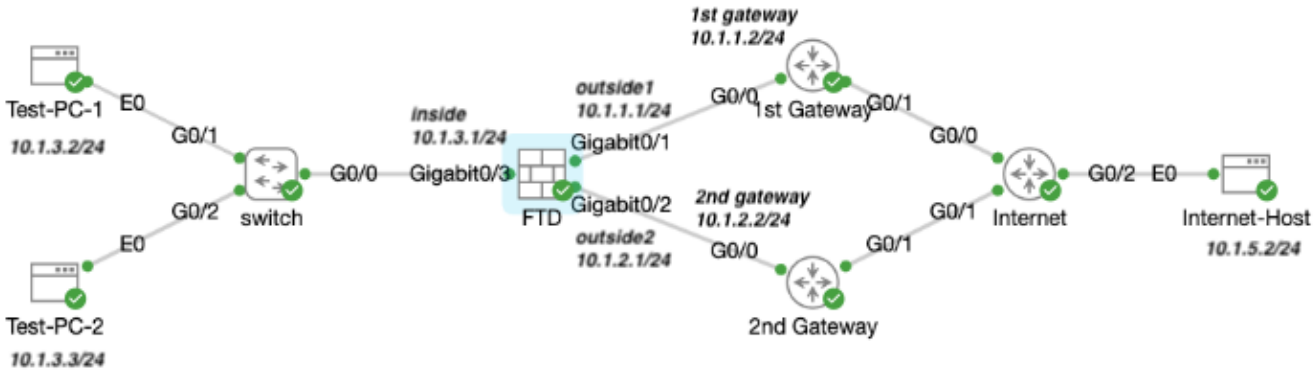
구성

네트워크 다이어그램

이 예에서 Cisco FTD에는 두 개의 외부 인터페이스(outside1 및 outside2)가 있습니다. 각 ISP 게이트웨이에 연결하면 outside1과 outside2는 outside라는 동일한 ECMP 영역에 속합니다.

내부 네트워크의 트래픽은 FTD를 통해 라우팅되고 두 ISP를 통해 인터넷으로 로드 밸런싱됩니다.

동시에 FTD는 각 ISP 게이트웨이에 대한 연결을 모니터링하기 위해 IP SLA를 사용합니다. ISP 회로에 장애가 발생하는 경우 FTD는 다른 ISP 게이트웨이로 장애 조치하여 비즈니스 연속성을 유지합니다.

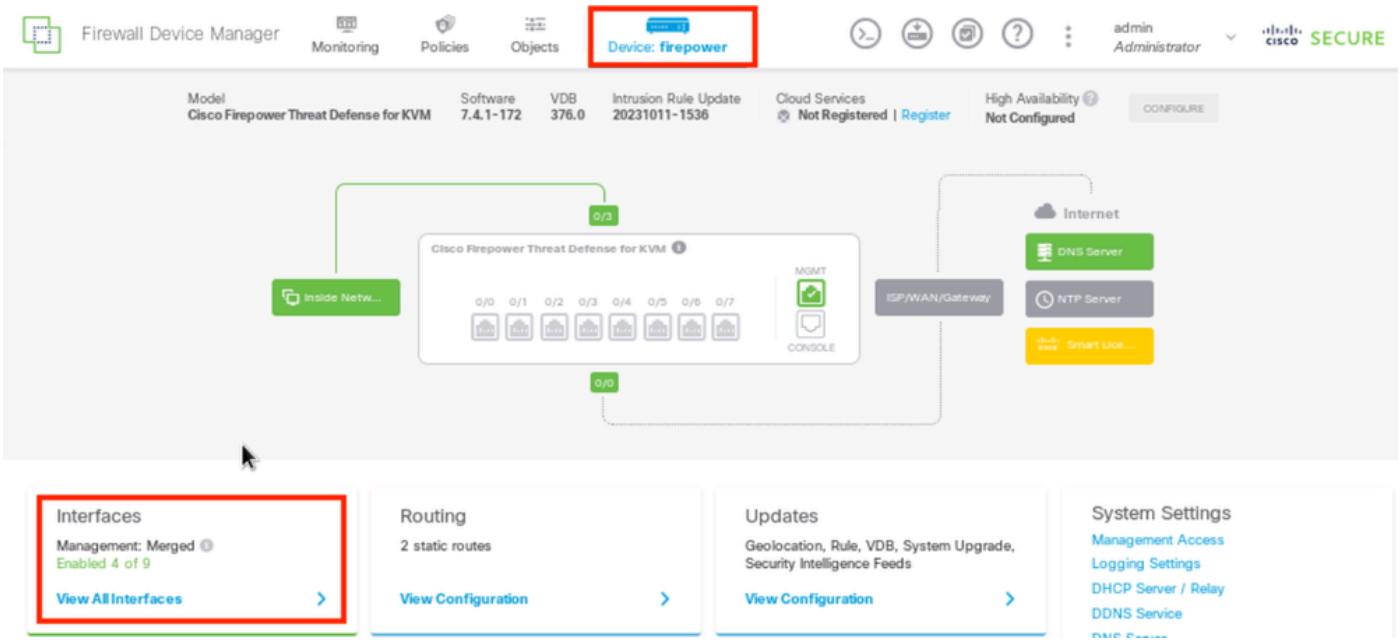


네트워크 다이어그램

설정

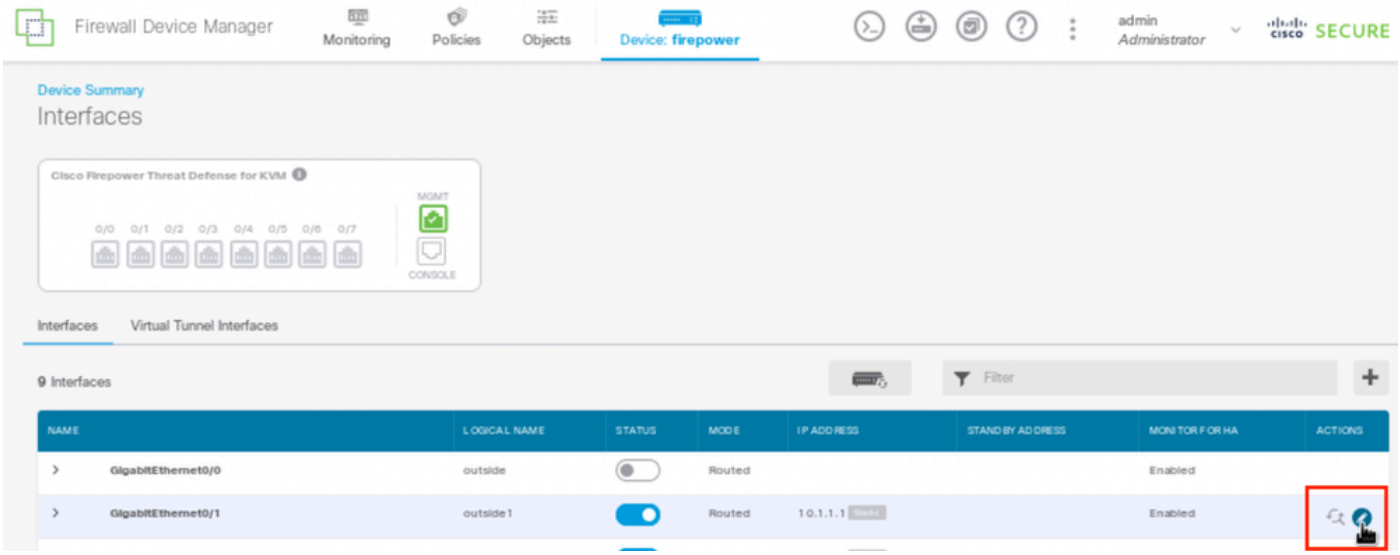
0단계. 인터페이스/개체 사전 구성

FDM 웹 GUI에 로그인하고 Device(디바이스)를 클릭한 다음 Interfaces(인터페이스) 요약에서 링크를 클릭합니다. Interfaces 목록은 사용 가능한 인터페이스, 이름, 주소 및 상태를 표시합니다.



FDM 장치 인터페이스

수정하려는 물리적 인터페이스의 수정 아이콘( )을 클릭합니다. 이 예에서는 GigabitEthernet0/1입니다.

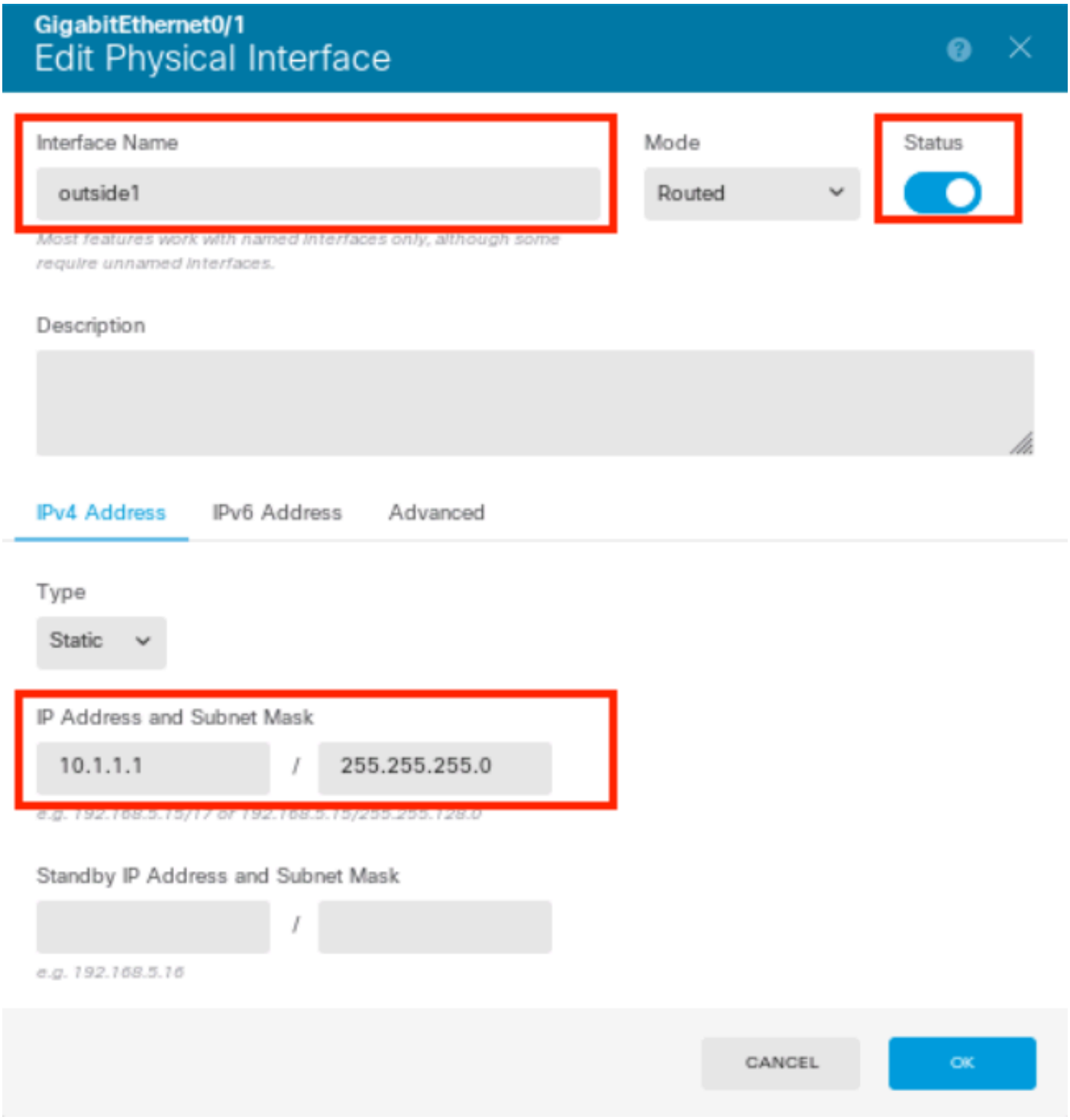


단계 0 인터페이스 Gi0/1

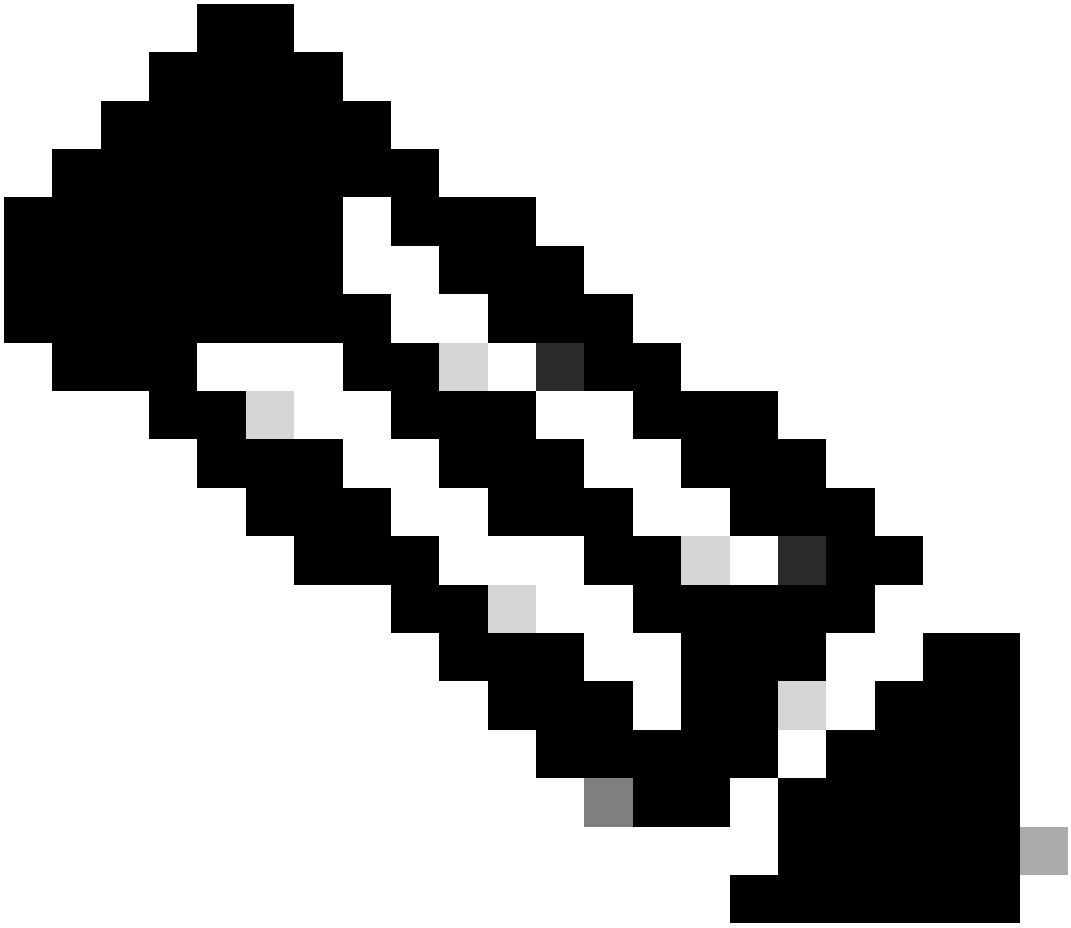
Edit Physical Interface(물리적 인터페이스 편집) 창에서

1. 인터페이스 이름(이 경우 outside1)을 설정합니다.

2. 상태 슬라이더를 사용 설정( )으로 설정합니다.
3. IPv4 Address(IPv4 주소) 탭을 클릭하고 IPv4 주소(이 경우 10.1.1.1/24)를 구성합니다.
4. OK(확인)를 클릭합니다.



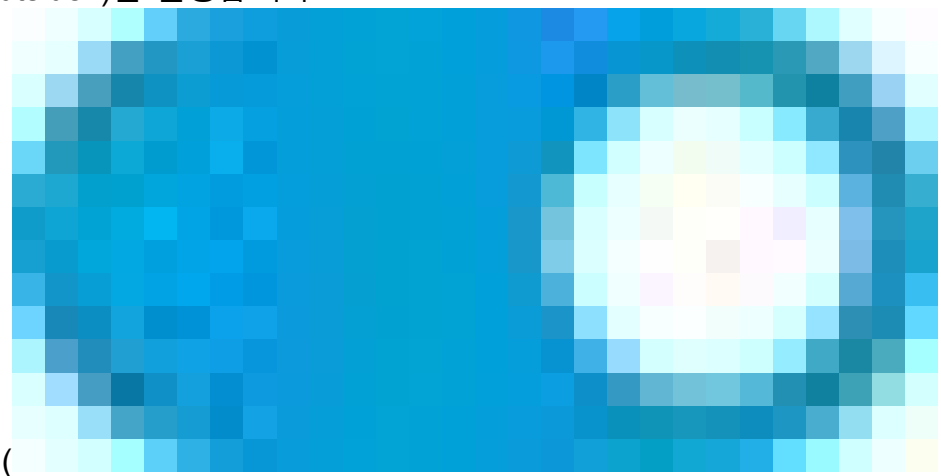
단계 0 인터페이스 Gi0/1 수정



참고: 라우티드 인터페이스만 ECMP 영역과 연결할 수 있습니다.

유사한 단계를 반복하여 보조 ISP 연결을 위한 인터페이스를 구성합니다. 이 예에서 물리적 인터페이스는 GigabitEthernet0/2입니다. Edit Physical Interface(물리적 인터페이스 편집) 창에서

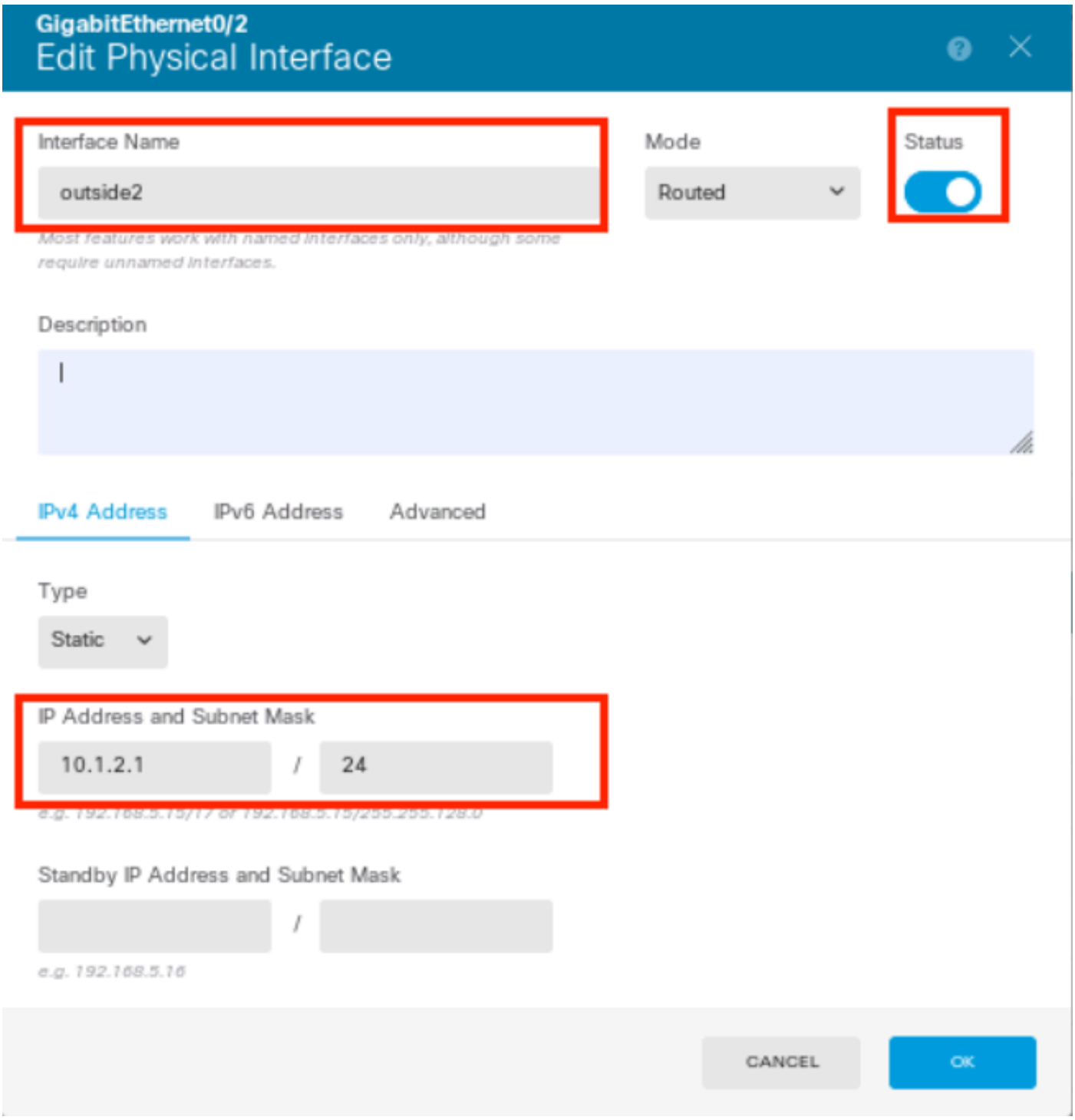
1. 인터페이스 이름(이 경우 outside2)을 설정합니다.



2. 상태 슬라이더를 사용 설정(

)으로 설정합니다.

3. IPv4 Address(IPv4 주소) 탭을 클릭하고 IPv4 주소(이 경우 10.1.2.1/24)를 구성합니다.
4. OK(확인)를 클릭합니다.

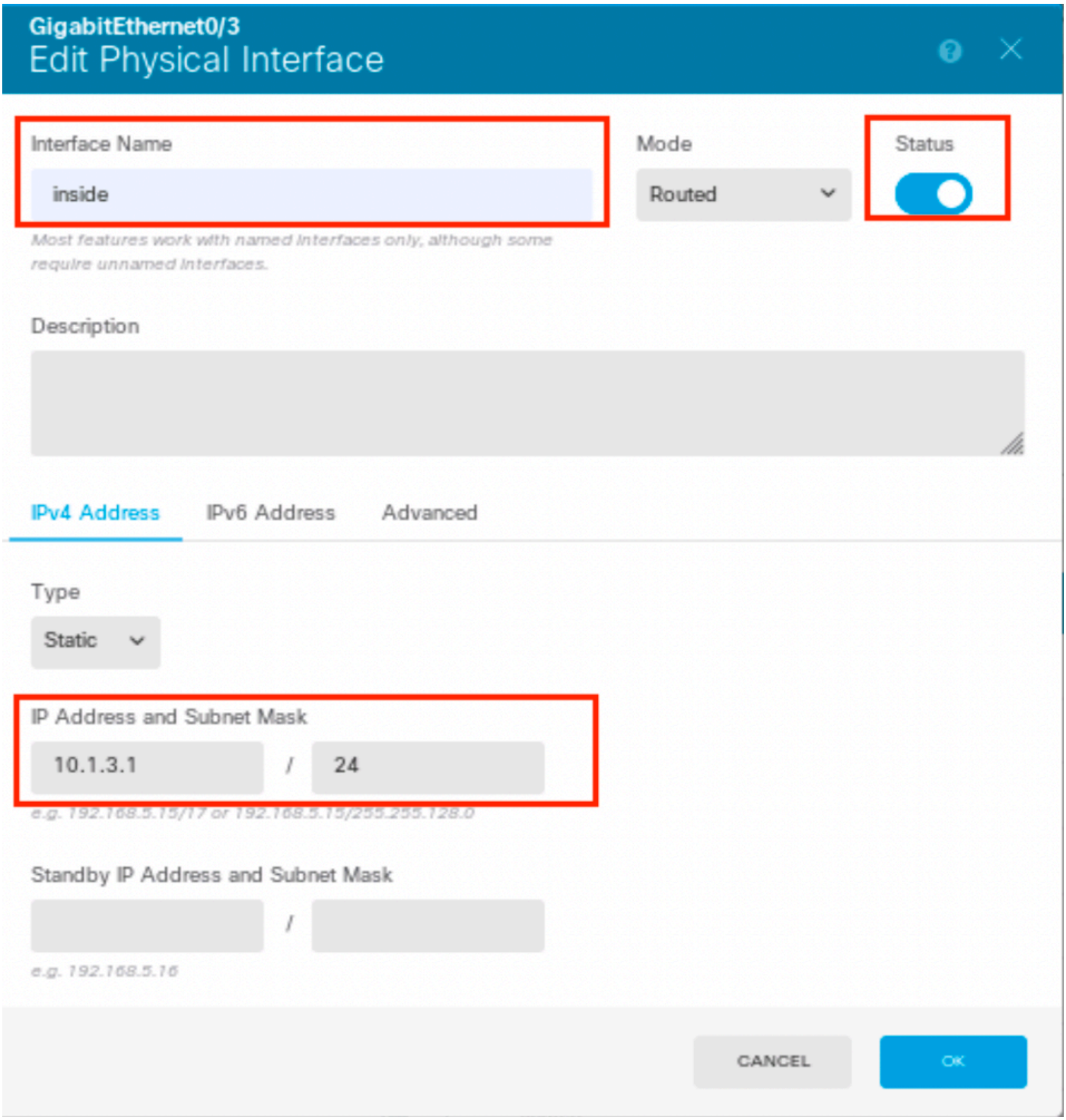


단계 0 인터페이스 Gi0/2 수정

유사한 단계를 반복하여 내부 연결을 위한 인터페이스를 구성합니다. 이 예에서 물리적 인터페이스는 GigabitEthernet0/3입니다. Edit Physical Interface(물리적 인터페이스 편집) 창에서

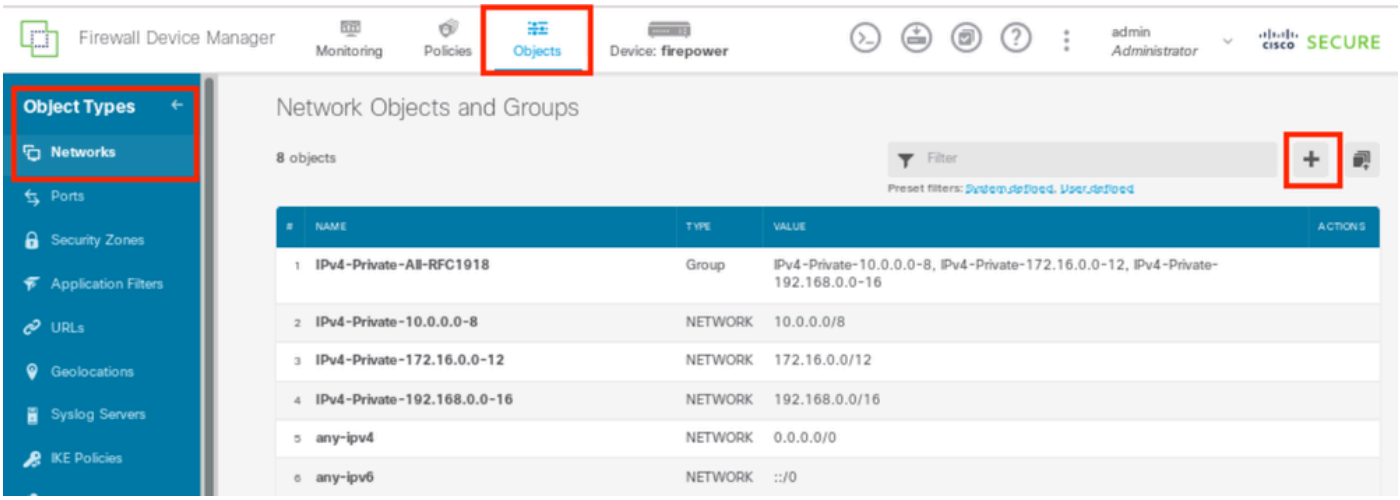
1. 인터페이스 이름(이 경우 내부)을 설정합니다.

2. 상태 슬라이더를 사용 설정(
)으로 설정합니다.
3. IPv4 Address(IPv4 주소) 탭을 클릭하고 IPv4 주소(이 경우 10.1.3.1/24)를 구성합니다.
4. OK(확인)를 클릭합니다.



단계 0 인터페이스 Gi0/3 수정

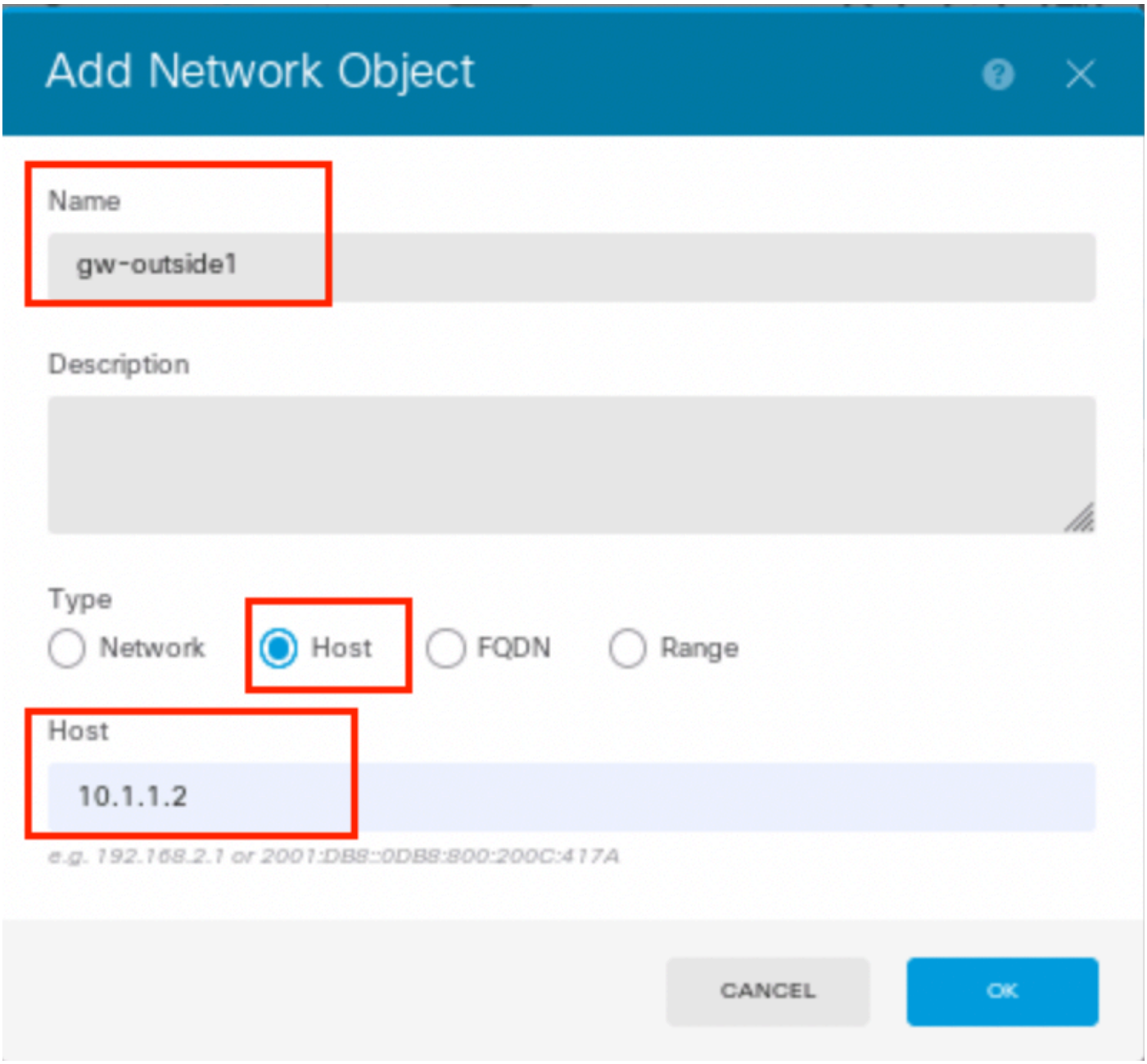
Objects(개체) > Object Types(개체 유형) > Networks(네트워크)로 이동하고 추가 아이콘( )을 클릭하여 새 개체를 추가합니다.



0단계 개체1

Add Network Object(네트워크 개체 추가) 창에서 첫 번째 ISP 게이트웨이를 구성합니다.

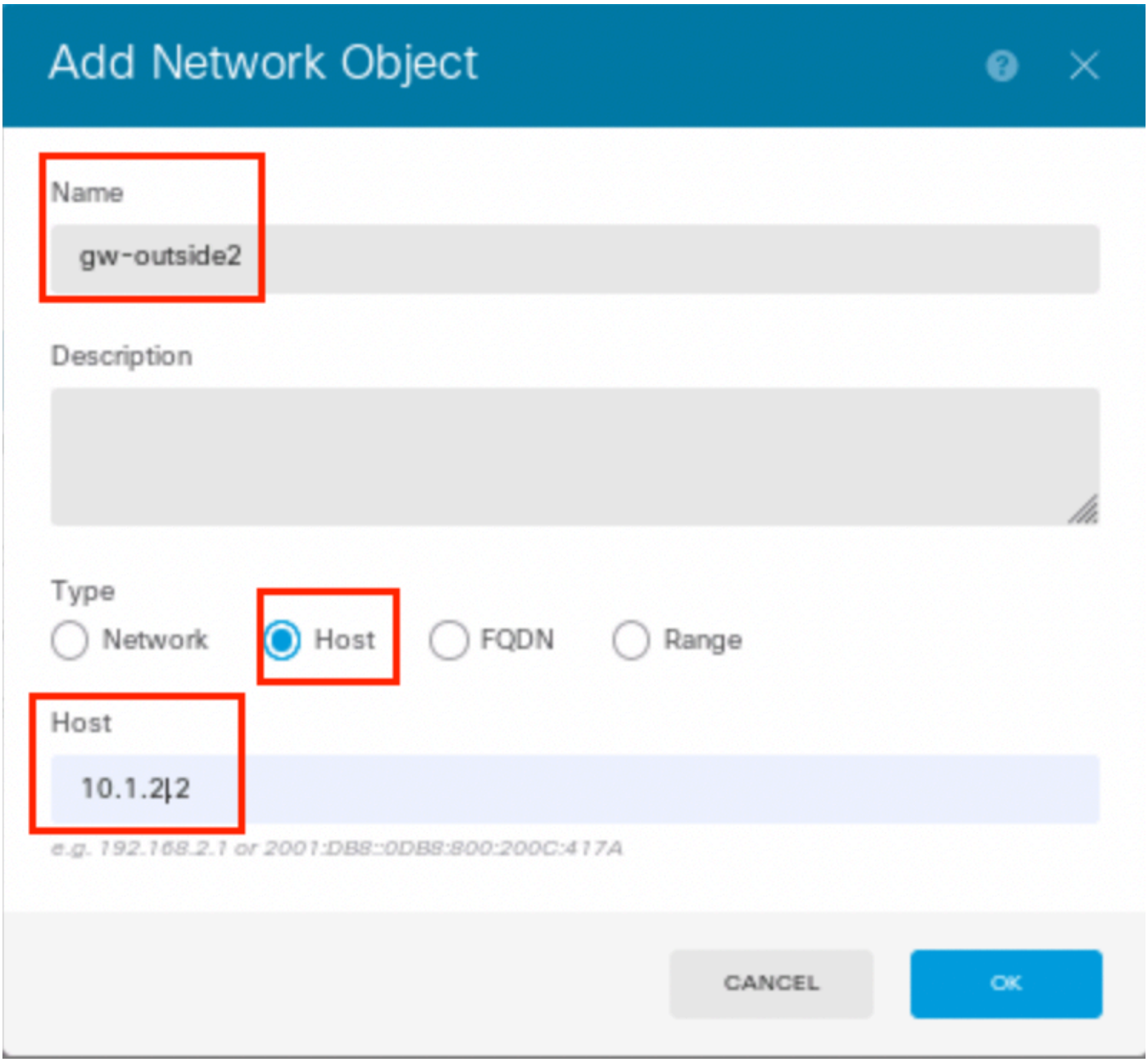
1. 객체의 이름(이 경우 gw-outside1)을 설정합니다.
2. 객체의 유형(이 경우 호스트)을 선택합니다.
3. 호스트의 IP 주소를 설정합니다(이 경우 10.1.1.2).
4. OK(확인)를 클릭합니다.



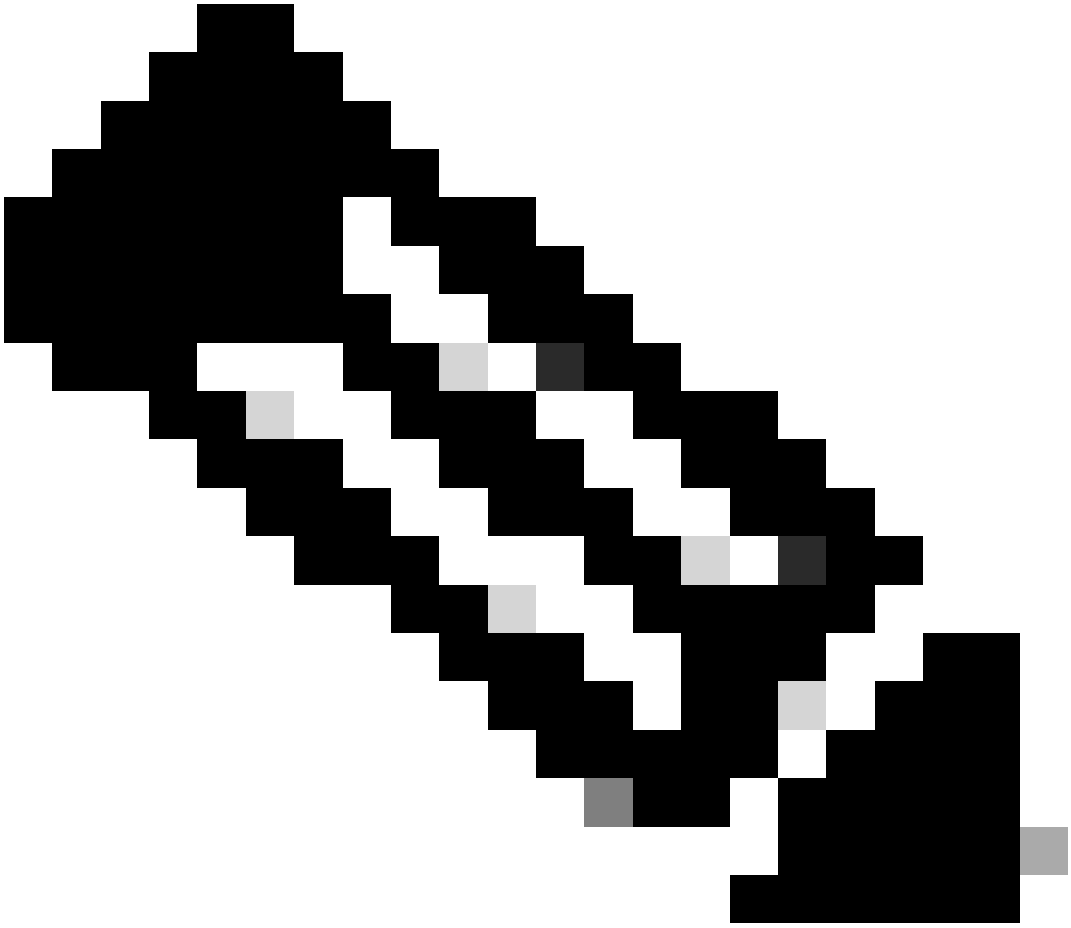
0단계 개체2

유사한 단계를 반복하여 두 번째 ISP 게이트웨이에 다른 네트워크 객체를 구성합니다.

1. 객체의 Name(이름)을 설정합니다(이 경우 gw-outside2).
2. 객체의 유형(이 경우 호스트)을 선택합니다.
3. 호스트의 IP 주소를 설정합니다(이 경우 10.1.2.2).
4. OK(확인)를 클릭합니다.


Add Network Object
Name
gw-outside2
Description
Type
Network
Host
FQDN
Range
Host
10.1.2.2
e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A
CANCEL
OK

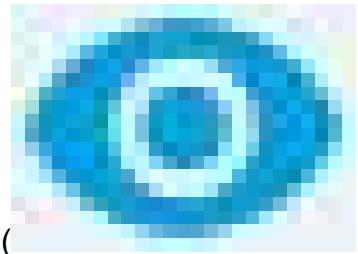
0단계 개체3



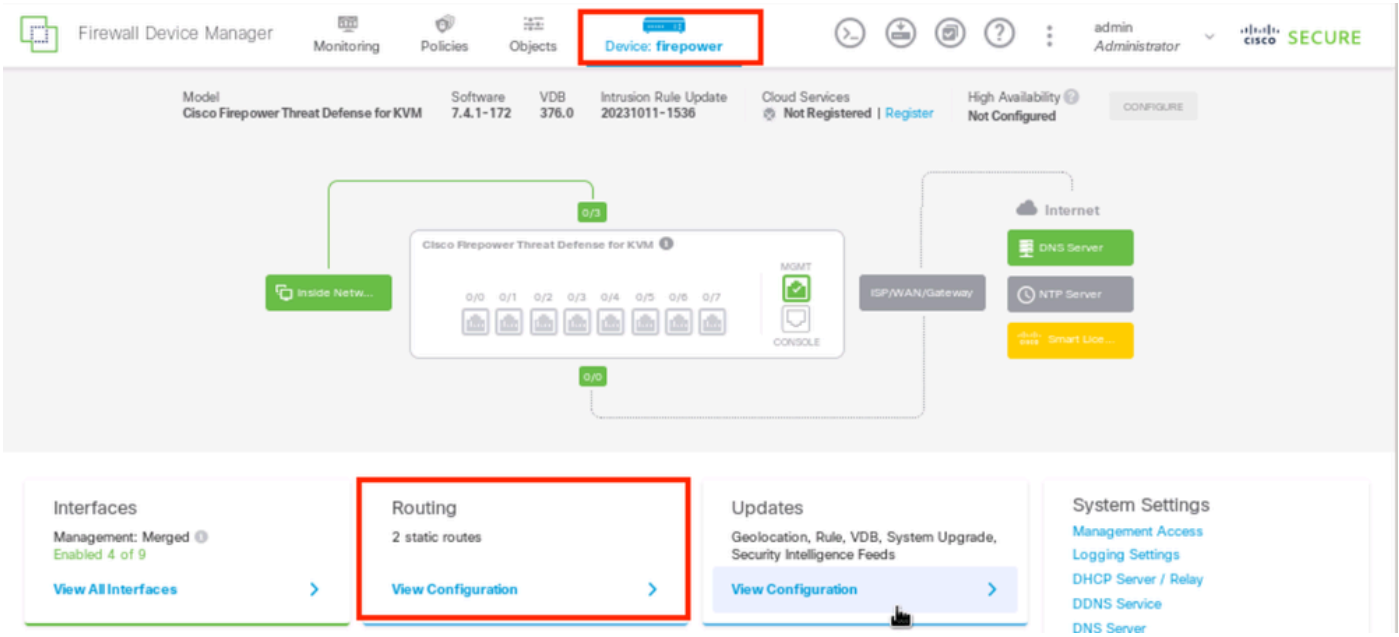
참고: 트래픽을 허용하려면 FTD에서 액세스 제어 정책을 구성해야 합니다. 이 부분은 이 문서에 포함되어 있지 않습니다.

1단계. ECMP 영역 구성

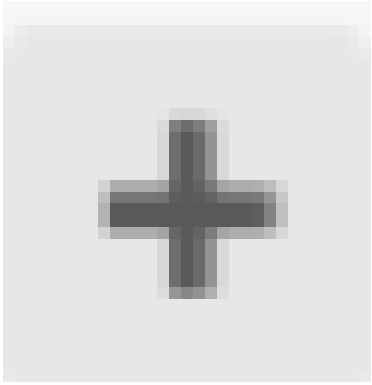
Device(디바이스)로 이동한 다음 Routing(라우팅) 요약의 링크를 클릭합니다.



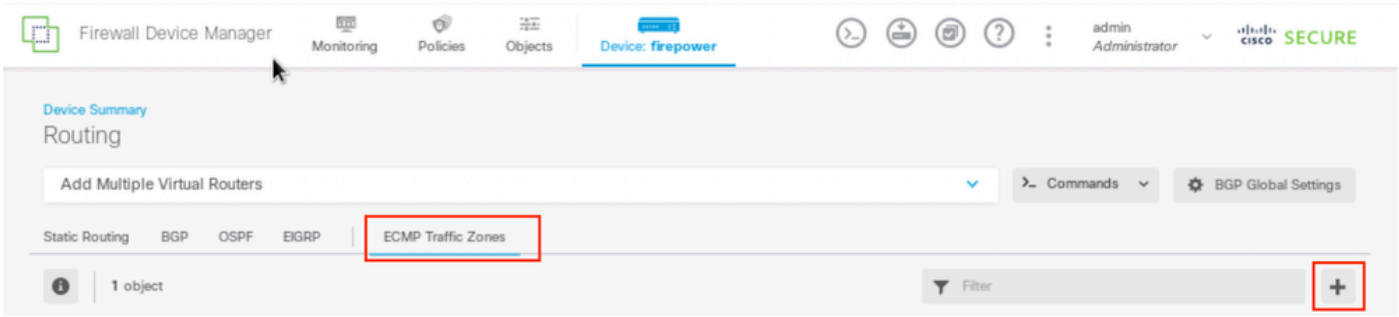
가상 라우터를 활성화한 경우 고정 경로를 구성하는 라우터의 보기 아이콘( )을 클릭합니다. 이 경우에는 가상 라우터가 활성화되지 않습니다.



1단계 ECMP Zone1



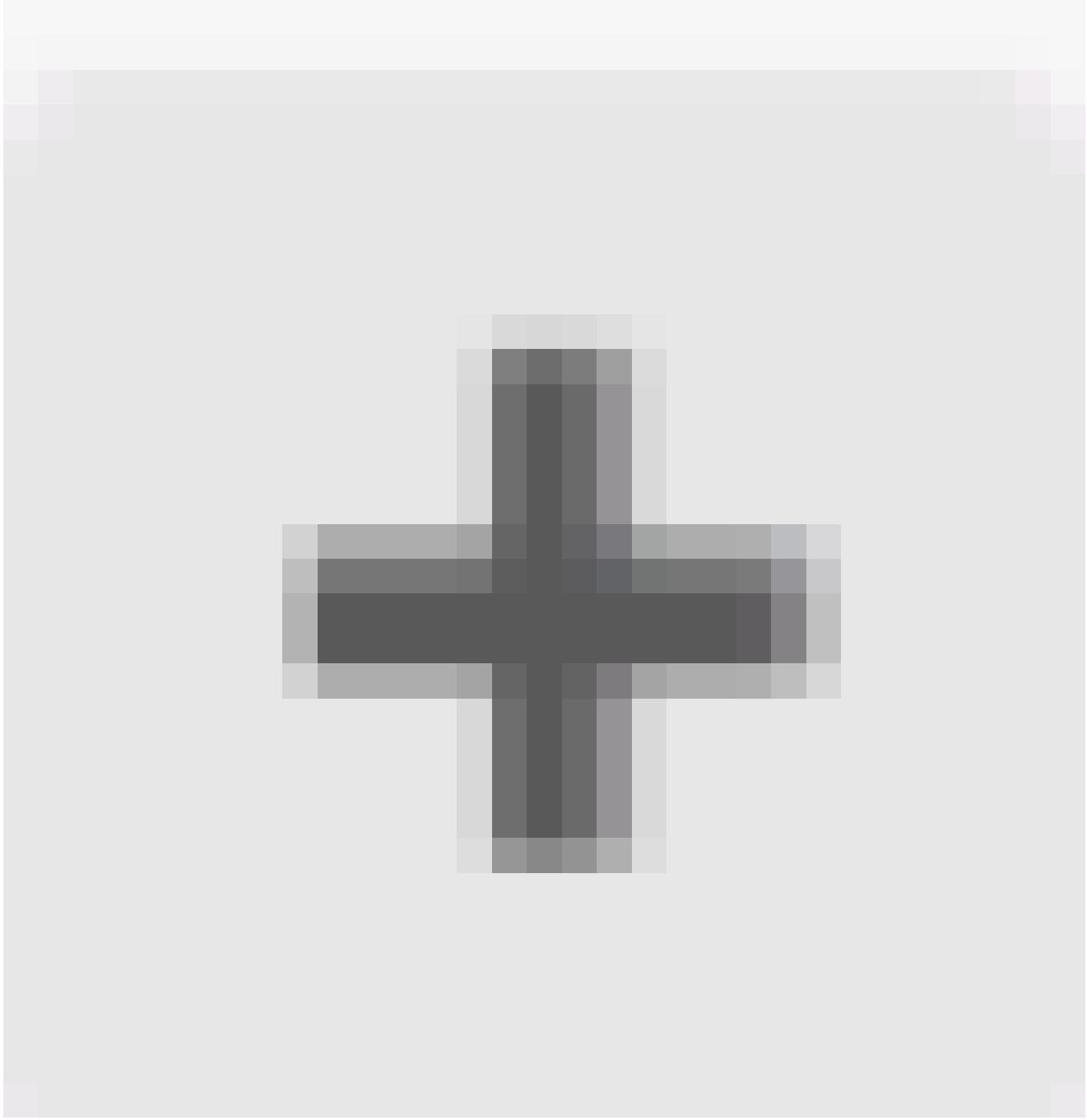
ECMP Traffic Zones(ECMP 트래픽 영역) 탭을 클릭한 다음 추가 아이콘( )을 클릭하여 새 영역을 추가합니다.



1단계 ECMP Zone2

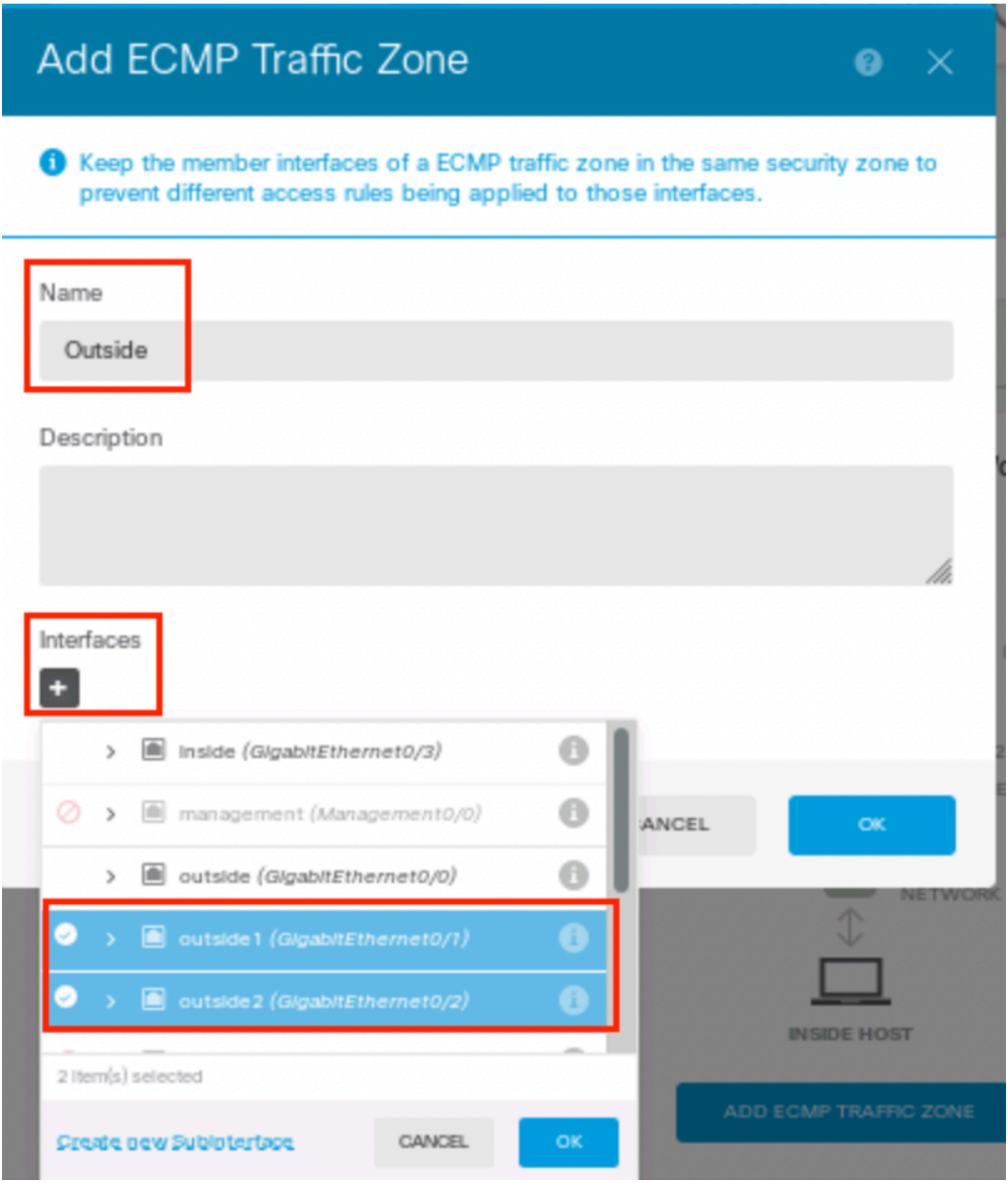
Add ECMP Traffic Zone(ECMP 트래픽 영역 추가) 창에서

1. ECMP 영역의 Name(이름) 및 선택적으로 설명을 설정합니다.
2. 영역에 포함할 최대 8개의 인터페이스를 선택하려면 추가 아이콘(



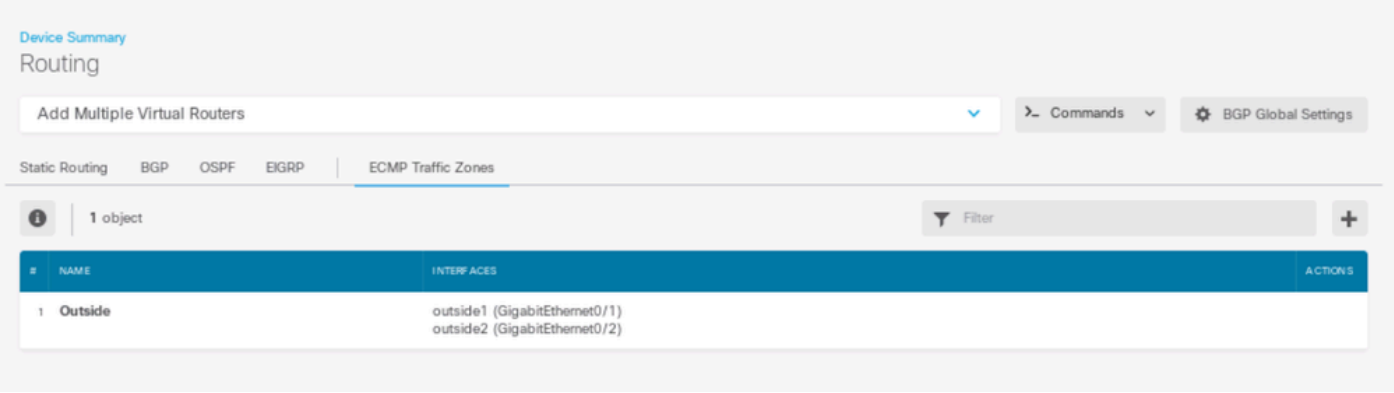
)을 클릭합니다. 이 예에서는 ECMP 이름이 Outside이고, interface outside1 및 outside2가 영역에 추가됩니다.

3. OK(확인)를 클릭합니다.

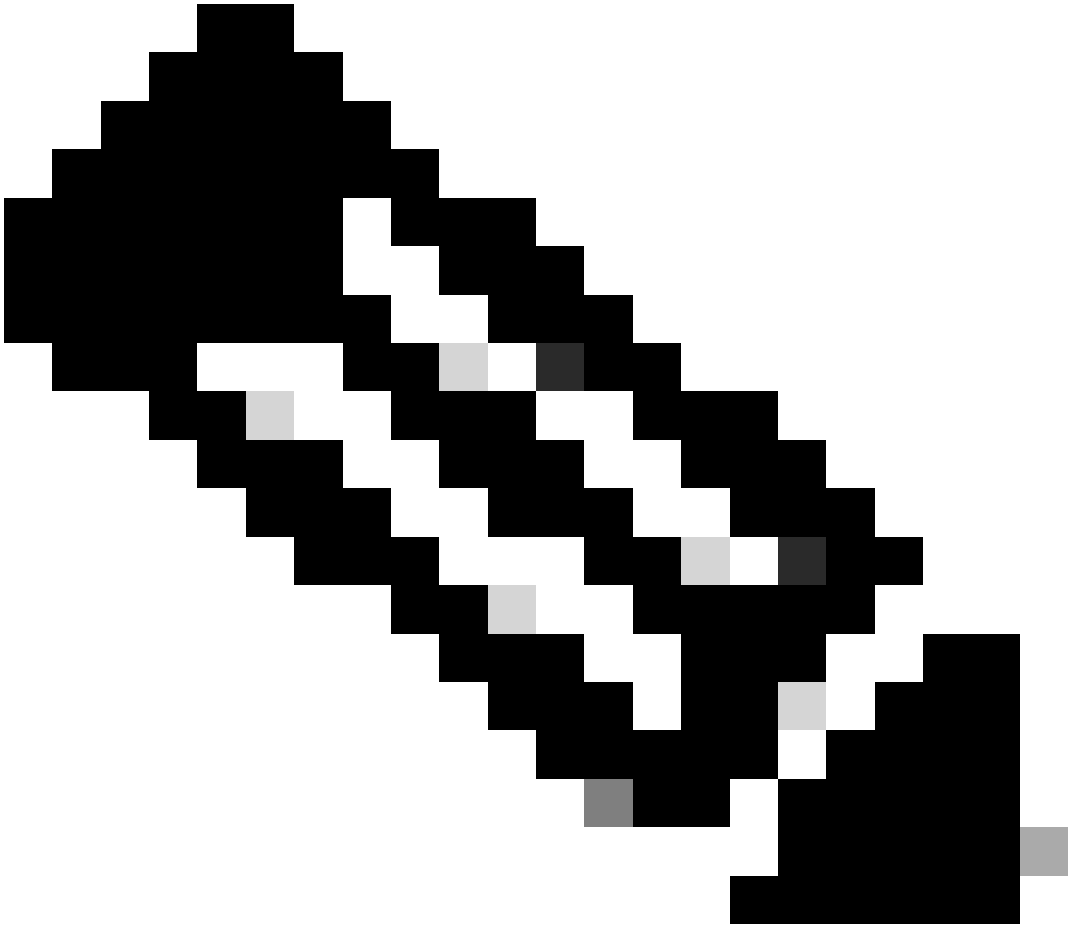


1단계 ECMP Zone3

outside1 및 outside2의 두 인터페이스가 모두 ECMP 영역에 추가되었습니다.



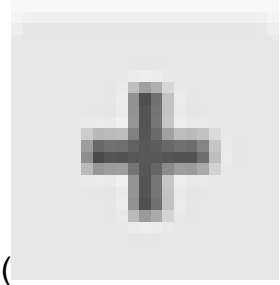
1단계 ECMP Zone4



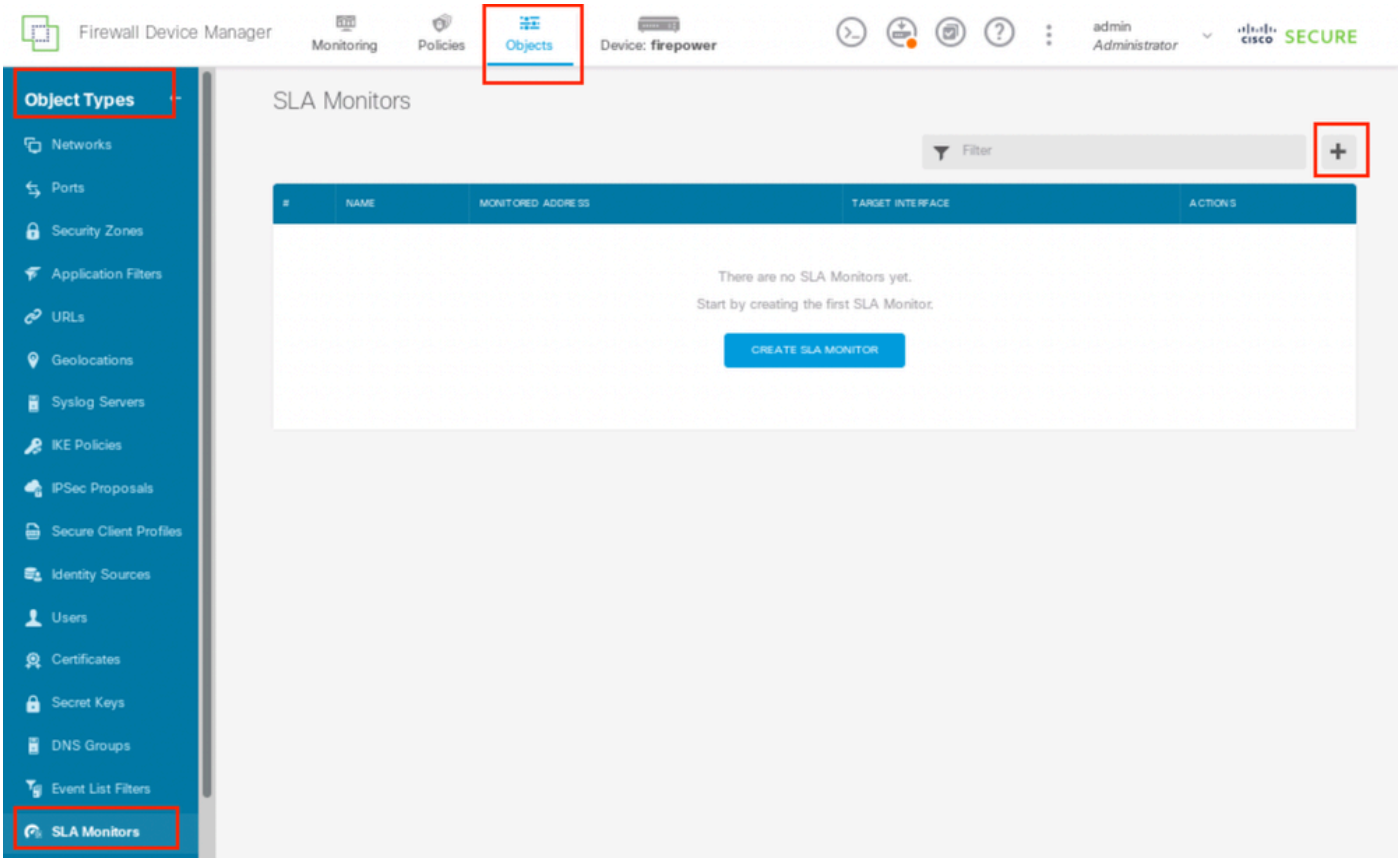
참고: ECMP 라우팅 트래픽 영역은 보안 영역과 관련이 없습니다. outside1 및 outside2 인터페이스를 포함하는 보안 영역을 생성해도 ECMP 라우팅 목적의 트래픽 영역은 구현되지 않습니다.

2단계. IP SLA 개체 구성

각 게이트웨이에 대한 연결을 모니터링하는 데 사용되는 SLA 객체를 정의하려면 Objects(객체) >



Object Types(객체 유형) > SLA Monitors(SLA 모니터)로 이동하고, 추가 아이콘( )을 클릭하여 첫 번째 ISP 연결에 대한 새 SLA 모니터를 추가합니다.



2단계 IP SLA1

Add SLA Monitor Object(SLA 모니터 개체 추가) 창에서 다음을 수행합니다.

1. SLA 모니터 객체의 이름 및 선택적으로 설명을 설정합니다(이 경우 sla-outside1).
2. 모니터 주소를 설정합니다(이 경우 gw-outside1(첫 번째 ISP 게이트웨이).
3. 모니터 주소를 연결할 수 있는 대상 인터페이스를 설정합니다(이 경우 outside1).
4. 또한 시간 초과 및 임계값을 조정할 수도 있습니다. OK(확인)를 클릭합니다.

Add SLA Monitor Object

Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

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

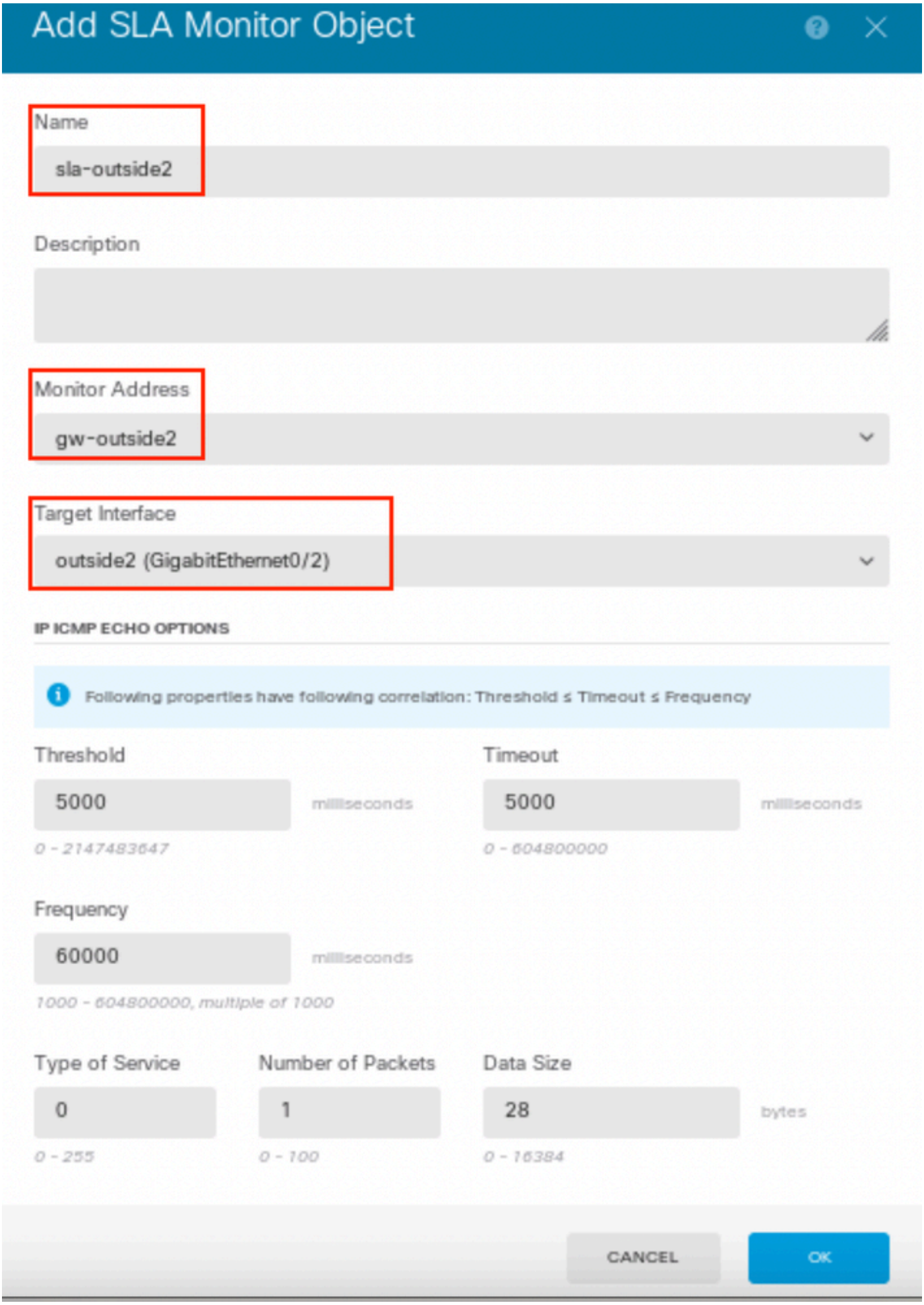
28 bytes

0 - 16384

CANCEL OK

Add SLA Monitor Object(SLA 모니터 개체 추가) 창에서 유사한 단계를 반복하여 두 번째 ISP 연결에 대해 다른 SLA 모니터 개체를 구성합니다.

1. SLA 모니터 객체의 이름 및 선택적으로 설명을 설정합니다(이 경우 sla-outside2).
2. 모니터 주소를 설정합니다(이 경우 gw-outside2)(두 번째 ISP 게이트웨이).
3. 모니터 주소를 연결할 수 있는 대상 인터페이스(이 경우 outside2)를 설정합니다.
4. 또한 시간 초과 및 임계값을 조정할 수도 있습니다. OK(확인)를 클릭합니다.

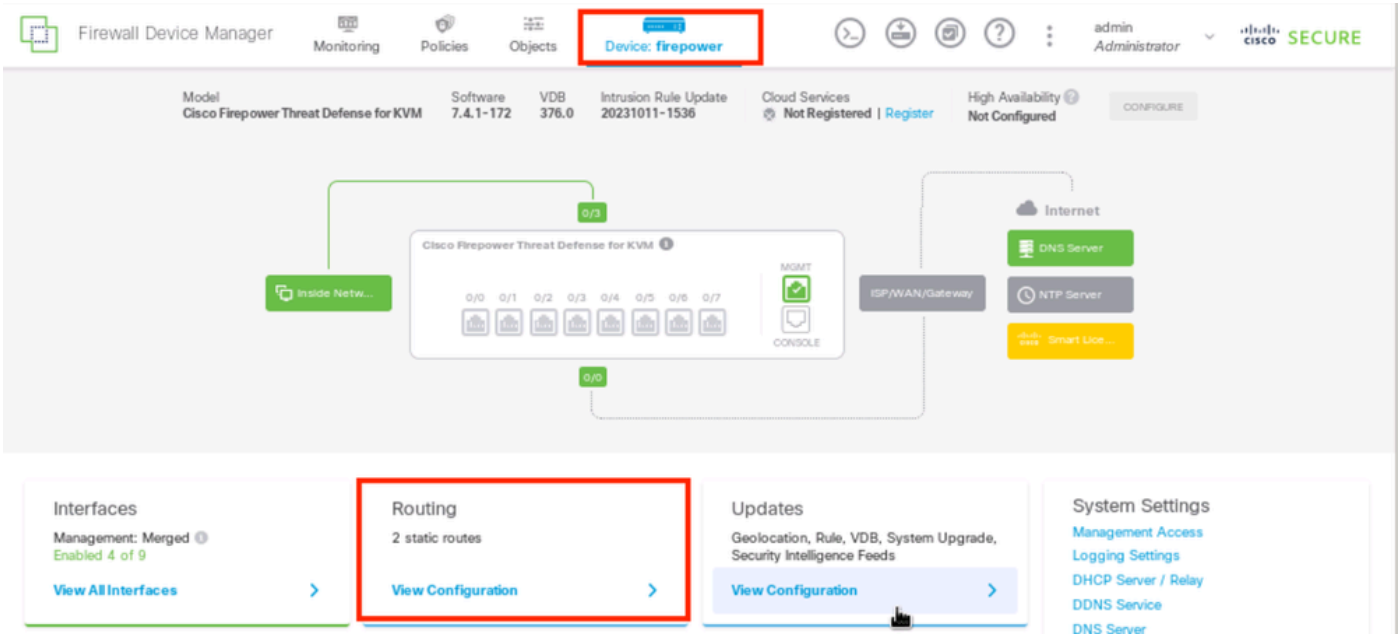

Add SLA Monitor Object
Name
sla-outside2
Description
Monitor Address
gw-outside2
Target Interface
outside2 (GigabitEthernet0/2)
IP ICMP ECHO OPTIONS
Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency
Threshold
5000
milliseconds
0 - 2147483647
Timeout
5000
milliseconds
0 - 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

2단계 IP SLA3

3단계. 경로 추적을 사용하여 고정 경로 구성

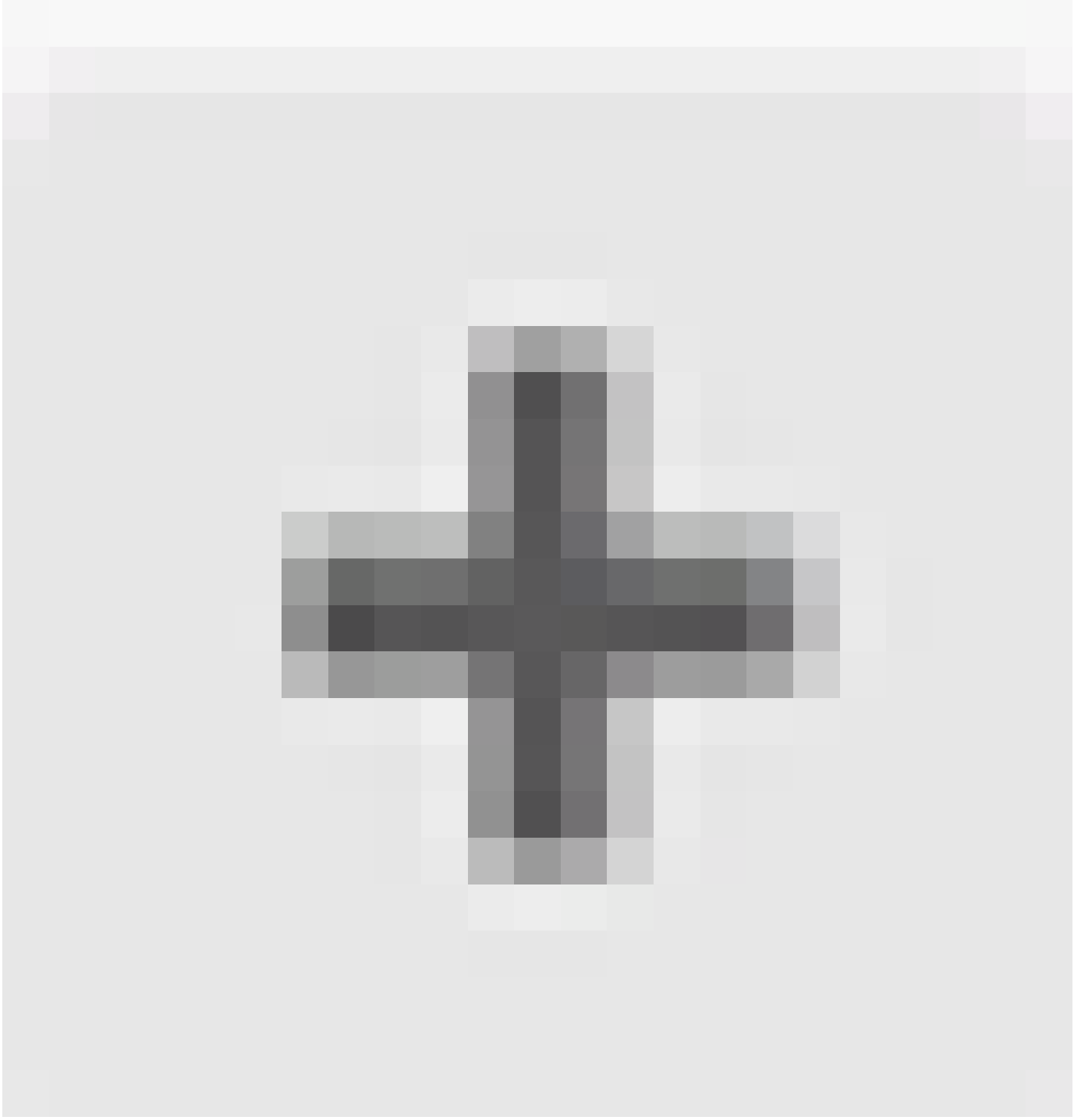
Device(디바이스)로 이동한 다음 Routing(라우팅) 요약의 링크를 클릭합니다.

가상 라우터를 활성화한 경우 고정 경로를 구성하는 라우터의 보기 아이콘( )을 클릭합니다. 이 경우에는 가상 라우터가 활성화되지 않습니다.



3단계 경로1

Static Routing 페이지에서 추가 아이콘(

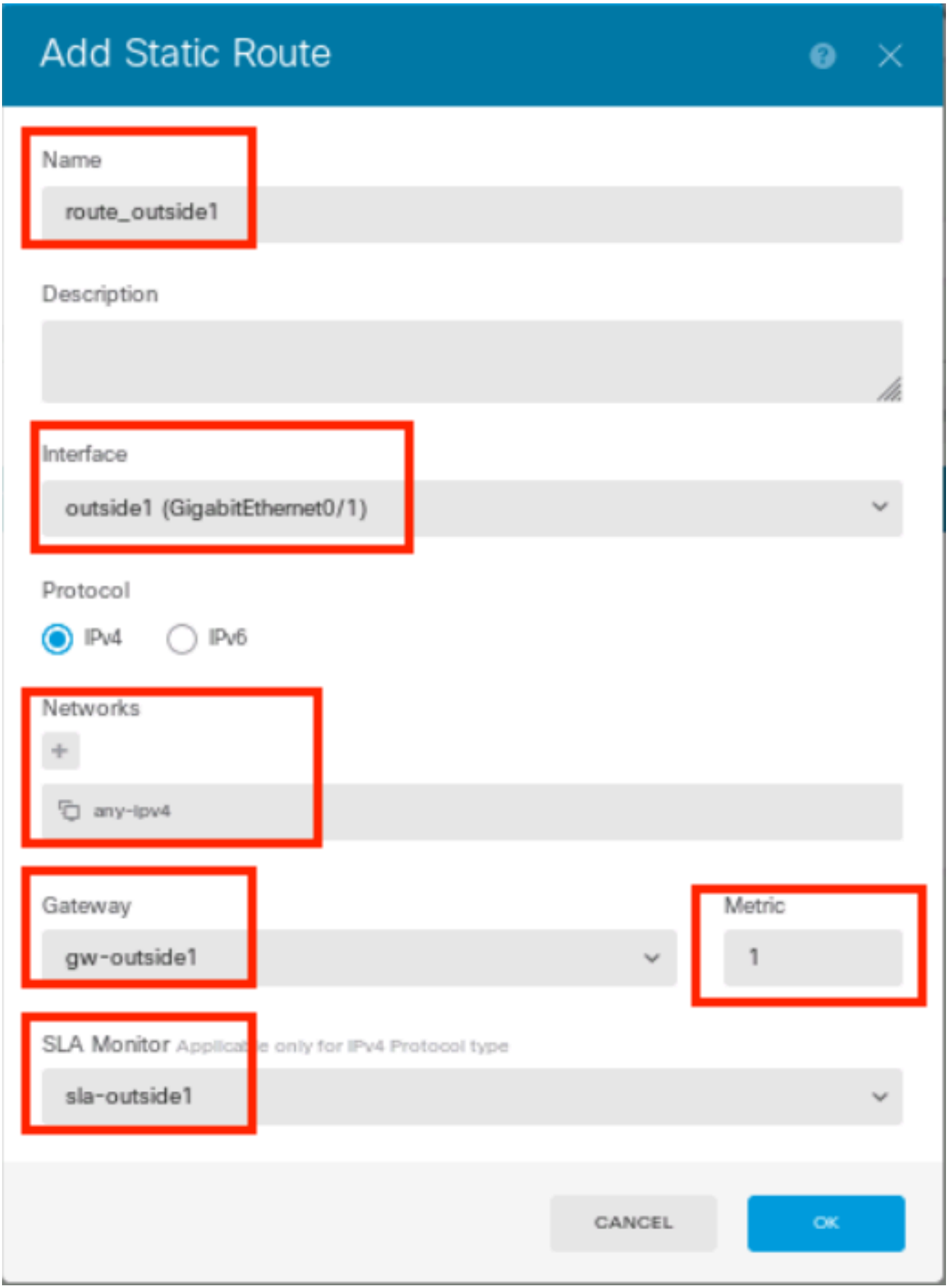


)을 클릭하여 첫 번째 ISP 링크에 새 고정 경로를 추가합니다.

Add Static Route(고정 경로 추가) 창에서

1. 경로의 이름 및 선택적으로 설명을 설정합니다. 이 경우 route_outside1입니다.
2. Interface 드롭다운 목록에서 트래픽을 전송할 인터페이스를 선택합니다. 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다. 이 경우 outside1(GigabitEthernet0/1).
3. 이 경로에서 게이트웨이를 사용하는 대상 네트워크 또는 호스트를 식별하는 네트워크를 선택합니다. 이 경우 미리 정의된 any-ipv4가 사용됩니다.
4. Gateway 드롭다운 목록에서 게이트웨이의 IP 주소를 식별하는 네트워크 객체를 선택합니다. 트래픽이 이 주소로 전송됩니다. 이 경우 gw-outside1(첫 번째 ISP 게이트웨이).
5. 경로의 메트릭(1~254)을 설정합니다. 이 예에서는 1입니다.

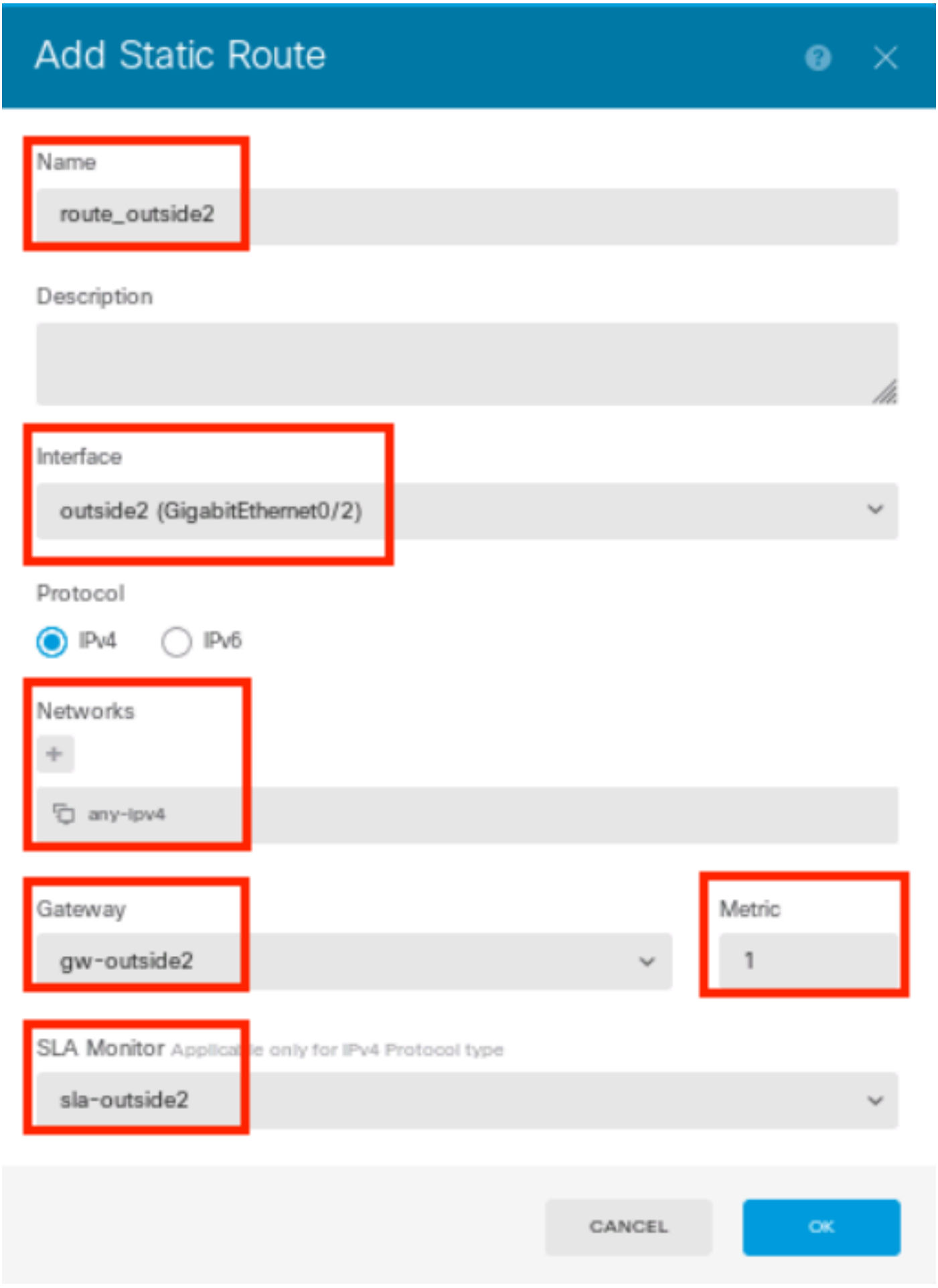
6. SLA Monitor 드롭다운 목록에서 SLA 모니터 객체를 선택합니다. 이 경우에는 sla-outside1입니다.
7. OK(확인)를 클릭합니다.


Add Static Route
Name
route_outside1
Description
Interface
outside1 (GigabitEthernet0/1)
Protocol
IPv4
IPv6
Networks
any-ipv4
Gateway
gw-outside1
Metric
1
SLA Monitor
sla-outside1
CANCEL
OK

3단계 경로2

Add Static Route(고정 경로 추가) 창에서 유사한 단계를 반복하여 두 번째 ISP 연결에 또 다른 고정 경로를 구성합니다.

1. 경로의 이름 및 선택적으로 설명을 설정합니다. 이 경우 route_outside2입니다.
2. Interface 드롭다운 목록에서 트래픽을 전송할 인터페이스를 선택합니다. 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다. 이 경우 outside2(GigabitEthernet0/2).
3. 이 경로에서 게이트웨이를 사용하는 대상 네트워크 또는 호스트를 식별하는 네트워크를 선택합니다. 이 경우 미리 정의된 any-ipv4가 사용됩니다.
4. Gateway 드롭다운 목록에서 게이트웨이의 IP 주소를 식별하는 네트워크 객체를 선택합니다. 트래픽이 이 주소로 전송됩니다. 이 경우 gw-outside2(두 번째 ISP 게이트웨이)입니다.
5. 경로의 메트릭(1~254)을 설정합니다. 이 예에서는 1입니다.
6. SLA Monitor 드롭다운 목록에서 SLA 모니터 객체를 선택합니다. 이 시나리오에서는 sla-outside2입니다.
7. OK(확인)를 클릭합니다.


Add Static Route
Name
route_outside2
Description
Interface
outside2 (GigabitEthernet0/2)
Protocol
IPv4
IPv6
Networks
any-ipv4
Gateway
gw-outside2
Metric
1
SLA Monitor
sla-outside2
CANCEL
OK

3단계 경로3

경로 트랙이 있는 outside1 및 outside2 인터페이스를 통한 2개의 경로가 있습니다.

3단계 경로4

FTD에 변경 사항을 구축합니다.

다음을 확인합니다.

FTD의 CLI에 로그인하고 명령을 실행하여 각 영역 show zone 에 속한 인터페이스를 포함하여 ECMP 트래픽 영역에 대한 정보를 확인합니다.

<#root>

> show zone
Zone:

Outside

ecmp
Security-level: 0

Zone member(s): 2

outside2 GigabitEthernet0/2

outside1 GigabitEthernet0/1

명령을 실행하여 라우팅 컨피그레이션에 show running-config route 대한 실행 중인 컨피그레이션을 확인합니다. 이 경우 경로 트랙이 있는 고정 경로가 2개 있습니다.

<#root>

> show running-config route

route outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1

route outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2

라우팅 테이블 show route 을 확인하려면 명령을 실행합니다. 이 경우 인터페이스 outside1과 outside2를 통해 동일한 비용으로 2개의 기본 경로를 사용할 수 있으며, 트래픽이 두 ISP 회로 간에 분산될 수 있습니다.

<#root>

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

[1/0] via 10.1.1.2, outside1

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

SLA 모니터 show sla monitor configuration 의 컨피그레이션을 확인하려면 명령을 실행합니다.

<#root>

> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1037119999
Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.1.2

Interface: outside1

Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
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:

Entry number: 1631063762
Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.2.2

Interface: outside2

Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
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:

SLA 모니터 show sla monitor operational-state 상태를 확인하려면 명령을 실행합니다. 이 경우 명령 출력에서 "Timeout occurred: FALSE"를 찾을 수 있으며, 이는 게이트웨이에 대한 ICMP 에코가 회신하고 있음을 나타냅니다. 따라서 대상 인터페이스를 통과하는 기본 경로가 활성화되어 라우팅 테이블에 설치됩니다.

<#root>

> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never

Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

로드 밸런싱

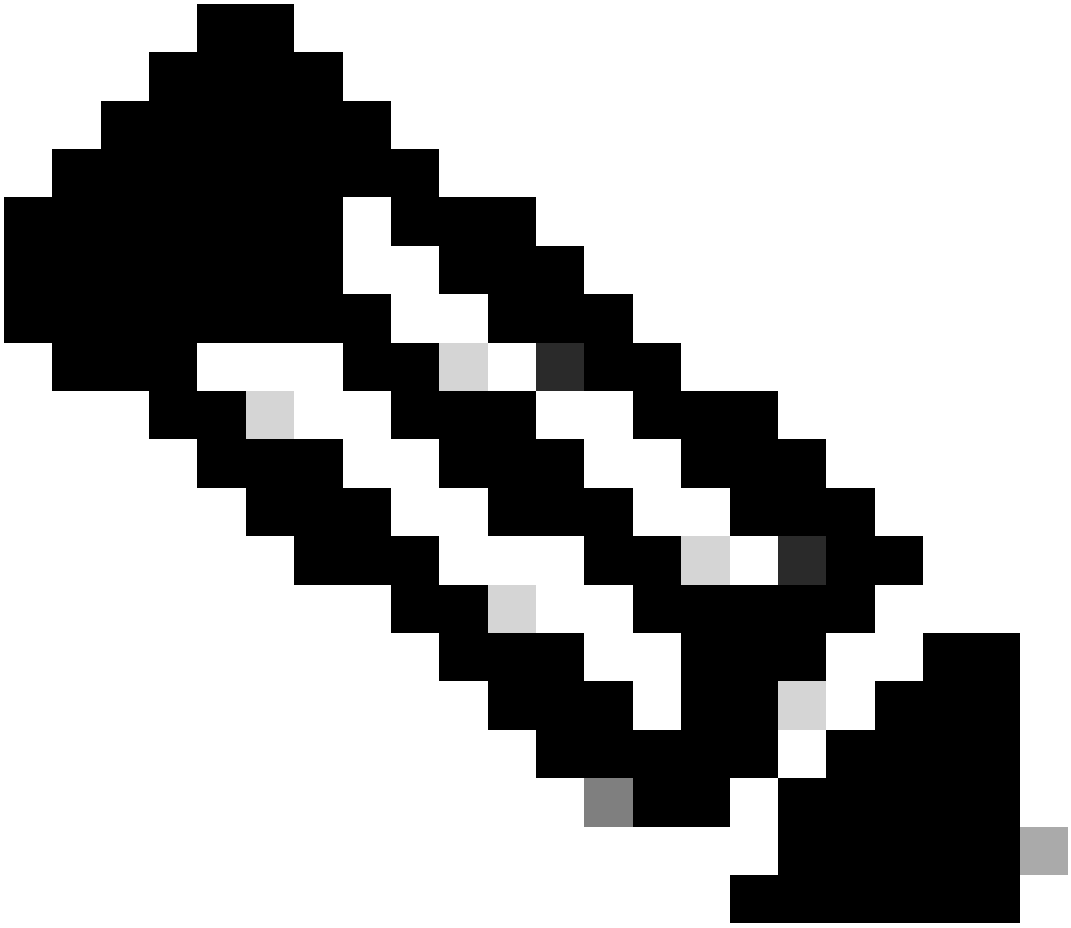
ECMP 로드가 ECMP 영역의 게이트웨이 간에 트래픽 밸런싱을 수행하는지 확인하기 위해 FTD를 통한 초기 트래픽. show conn 이 경우, Test-PC-1(10.1.3.2) 및 Test-PC-2(10.1.3.4)에서 인터넷 호스트(10.1.5.2)로 SSH 연결을 시작하고, 명령을 실행하여 두 ISP 링크 간에 트래픽이 로드 밸런싱되는지 확인하고, Test-PC-1(10.1.3.2)은 interface outside1을, Test-PC-2(10.1.3.4)는 interface outside2를 거칩니다.

<#root>

> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, flags UIO N1



주: 소스 및 목적지 IP 주소, 수신 인터페이스, 프로토콜, 소스 및 목적지 포트를 해시하는 알고리즘에 따라 지정된 게이트웨이 간에 트래픽이 로드 밸런싱됩니다. 테스트를 실행할 때 시뮬레이션하는 트래픽은 해시 알고리즘 때문에 동일한 게이트웨이로 라우팅될 수 있습니다. 이는 6개의 튜플(소스 IP, 목적지 IP, 수신 인터페이스, 프로토콜, 소스 포트, 목적지 포트) 중에서 값을 변경하여 해시 결과를 변경할 수 있습니다.

잃어버린 경로

첫 번째 ISP 게이트웨이에 대한 링크가 중단되면 첫 번째 게이트웨이 라우터를 종료하여 시뮬레이션합니다. FTD가 SLA Monitor 개체에 지정된 임계값 타이머 내에서 첫 번째 ISP 게이트웨이로부터 에코 응답을 받지 못하면 호스트에 연결할 수 없는 것으로 간주되고 중단된 것으로 표시됩니다. 첫 번째 게이트웨이에 대한 추적 경로도 라우팅 테이블에서 제거됩니다.

SLA 모니터 show sla monitor operational-state 의 현재 상태를 확인하려면 명령을 실행합니다. 이 경우 명령 출력에서 "Timeout

occurred: True"를 찾을 수 있으며, 이는 첫 번째 ISP 게이트웨이에 대한 ICMP 에코가 응답하지 않음을 나타냅니다.

<#root>

> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: TRUE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 06:14:32.801 UTC Tue Jan 30 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 06:14:32.802 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

명령을 실행하여 현재 라우팅 테이블 **show route** 을 확인하고 인터페이스 outside1을 통해 첫 번째 ISP 게이트웨이로 향하는 경로가 제거되며, 인터페이스 outside2를 통해 두 번째 ISP 게이트웨이로 향하는 활성 기본 경로는 하나뿐입니다.

<#root>

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

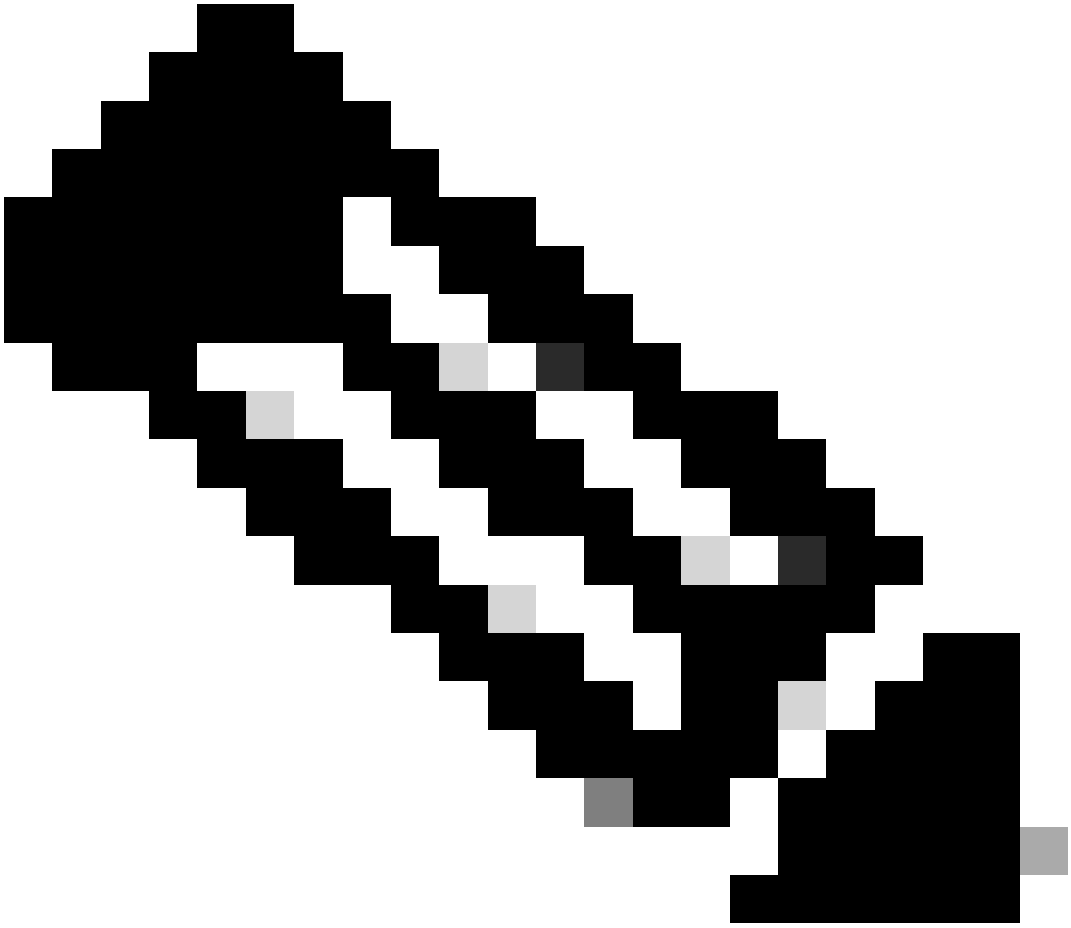
명령을 실행하면 show conn 두 개의 연결이 여전히 작동 중인 것을 확인할 수 있습니다. SSH 세션은 Test-PC-1(10.1.3.2) 및 Test-PC-2(10.1.3.4)에서도 중단 없이 활성화됩니다.

<#root>

> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, flags UIO N1



참고: 라우팅 테이블에서show conn interface outside1을 통한 기본 경로가 제거되었지만, Test-PC-1(10.1.3.2)의 , SSH 세션은 interface outside1을 통해 계속 유지되고 있음을 알 수 있습니다. 이는 설계에 따라 interface outside2를 통해 실제 트래픽이 흐르는 것으로 예상됩니다. Test-PC-1(10.1.3.2)에서 Internet-Host(10.1.5.2)로의 새 연결을 시작하면 interface outside2를 통해 모든 트래픽이 처리됨을 확인할 수 있습니다.

문제 해결

라우팅 테이블 변경을 검증하려면 명령을 실행합니다 debug ip routing.

이 예에서는 첫 번째 ISP 게이트웨이에 대한 링크가 중단되면 인터페이스 outside1을 통한 경로가 라우팅 테이블에서 제거됩니다.

<#root>

> debug ip routing
IP routing debugging is on

RT:

ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, outside1

ha_cluster_synced 0 routetype 0

RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0

RT(mgmt-only):

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2

NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, outside2

명령을 실행하여 현재 라우팅 테이블을 확인합니다 show route .

<#root>

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

첫 번째 ISP 게이트웨이에 대한 링크가 다시 작동하면 인터페이스 outside1을 통한 경로가 라우팅 테이블에 다시 추가됩니다.

<#root>

> debug ip routing
IP routing debugging is on

RT(mgmt-only):

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, outside2

NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, outside2
via 10.1.1.2, outside1

명령을 실행하여 현재 라우팅 테이블을 확인합니다 show route .

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
[1/0] via 10.1.1.2, outside1
C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

관련 정보

- Cisco 기술 지원 및 다운로드

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.