FMC에서 관리하는 FTD에서 IP SLA를 사용하여 ECMP 구성

목차

소개

이 문서에서는 FMC에서 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 FMC(Secure Firewall Management Center)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 버전 7.4.1

- Cisco FMC 버전 7.4.1

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 FMC에서 관리하는 Cisco FTD에서 ECMP(Equal-Cost Multi-Path)와 IP SLA(Internet Protocol Service Level Agreement)를 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
- Cisco Secure Firewall Management Center 버전 7.1 이상

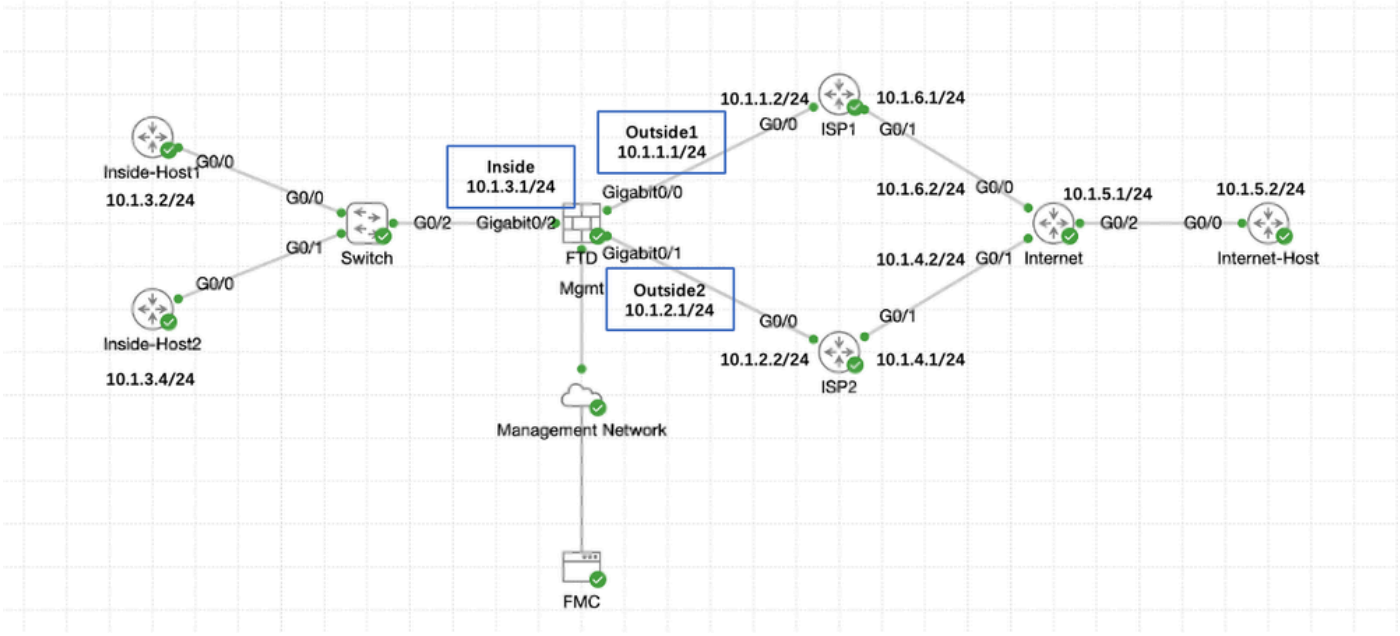
구성

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.

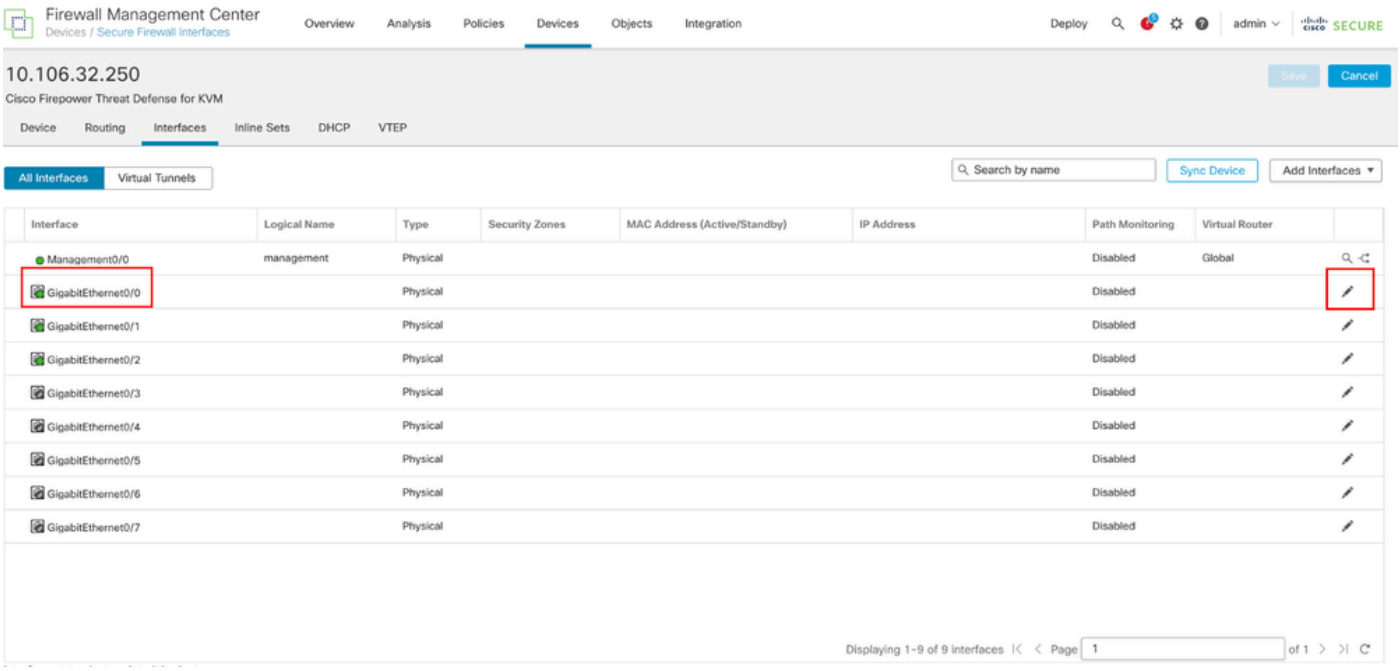


네트워크 다이어그램

설정

0단계. 인터페이스/네트워크 개체 사전 구성

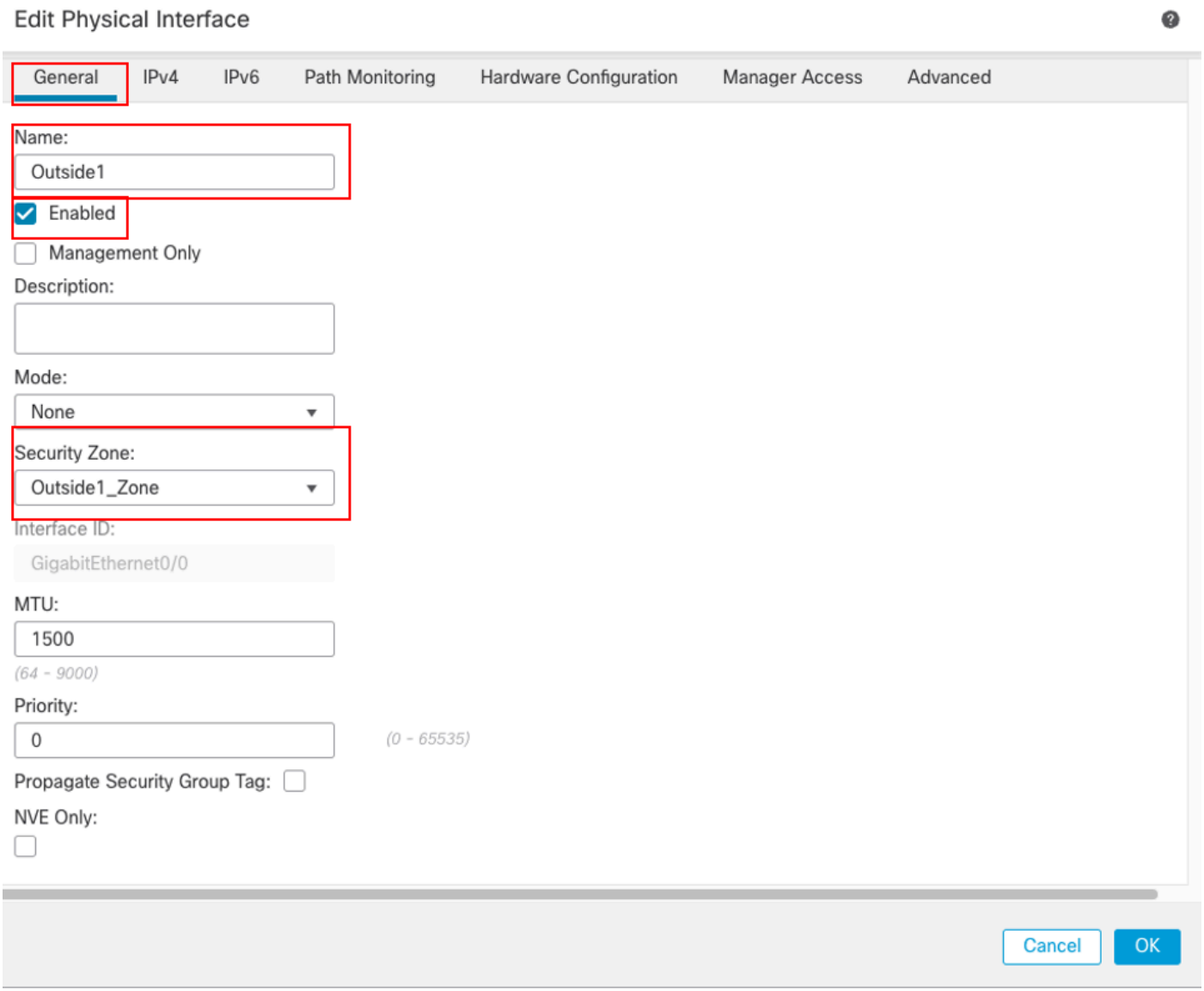
FMC 웹 GUI에 로그인하고 Devices(디바이스) >Device Management(디바이스 관리)를 선택하고 Edit(편집) 버튼을 클릭하여 위협 방어 디바이스를 확인합니다. Interfaces 페이지는 기본적으로 선택됩니다. 수정할 인터페이스에 대해 Edit(수정) 버튼을 클릭합니다(이 예에서는 GigabitEthernet0/0).



인터페이스 Gi0/0 편집

Edit Physical Interface(물리적 인터페이스 수정) 창의 General(일반) 탭 아래에서 다음을 수행합니다.

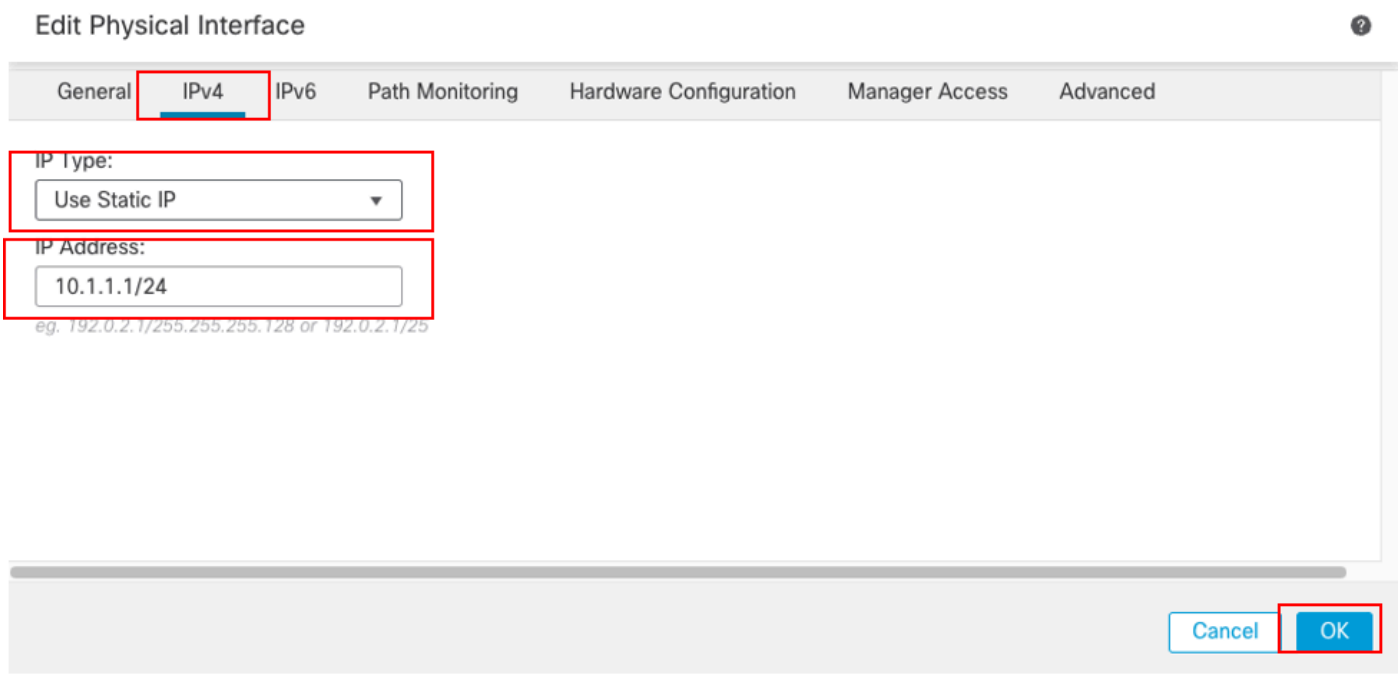
1. Name(이름)을 설정합니다(이 경우 Outside1).
2. Enabled 확인란을 선택하여 인터페이스를 활성화합니다.
3. Security Zone 드롭다운 목록에서 기존 Security Zone을 선택하거나 새 Zone을 생성합니다(이 예에서는 Outside1_Zone).



인터페이스 Gi0/0 일반

IPv4 탭 아래에서

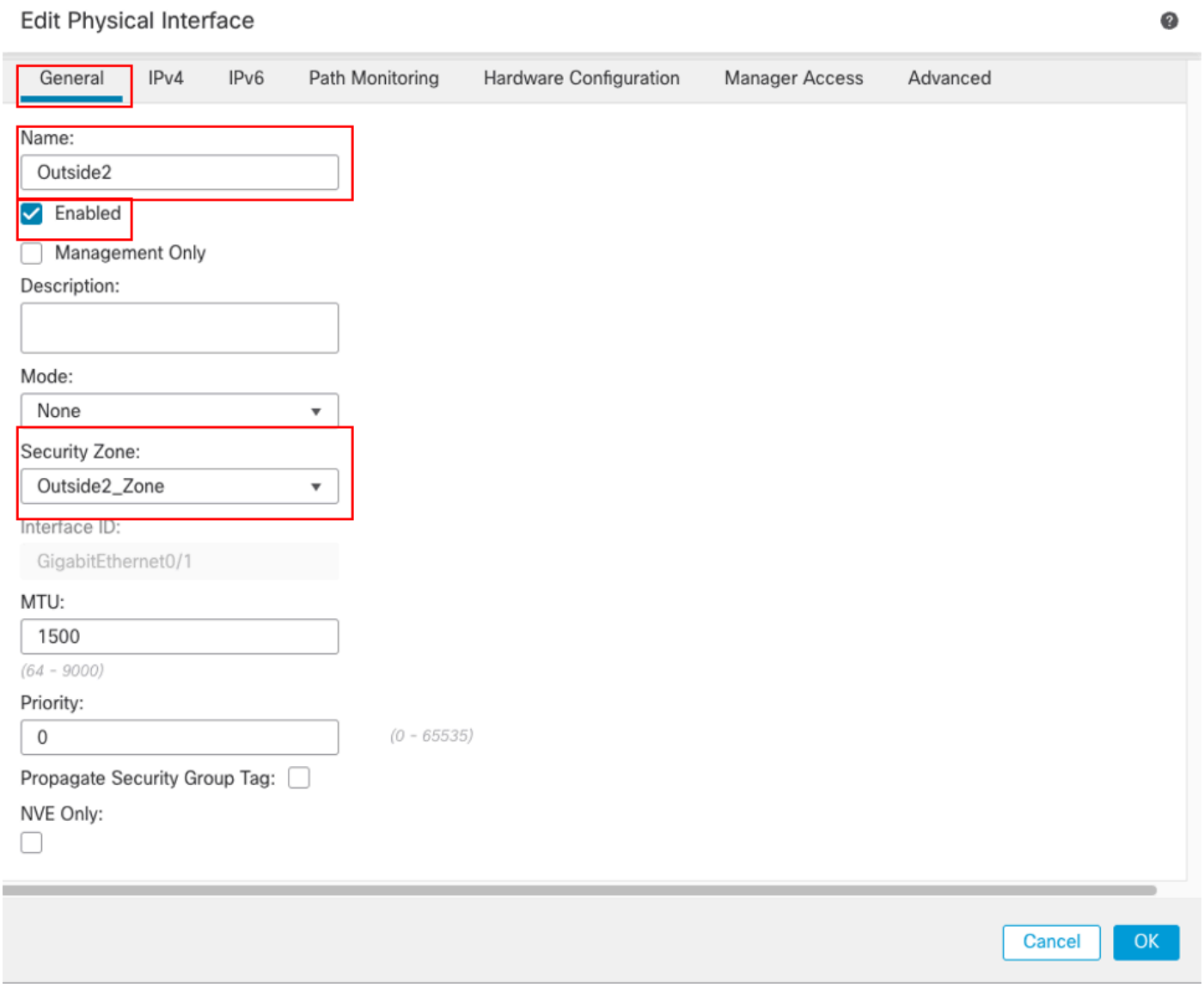
1. IP Type 드롭다운 목록에서 옵션 중 하나를 선택합니다. 이 예에서는 Use Static IP(고정 IP 사용).
2. IP 주소를 설정합니다(이 예에서는 10.1.1.1/24).
3. OK(확인)를 클릭합니다.



인터페이스 Gi0/0 IPv4

유사한 단계를 반복하여 GigabitEthernet0/1 인터페이스를 구성합니다. Edit Physical Interface 창의 General(일반) 탭에서 다음을 수행합니다.

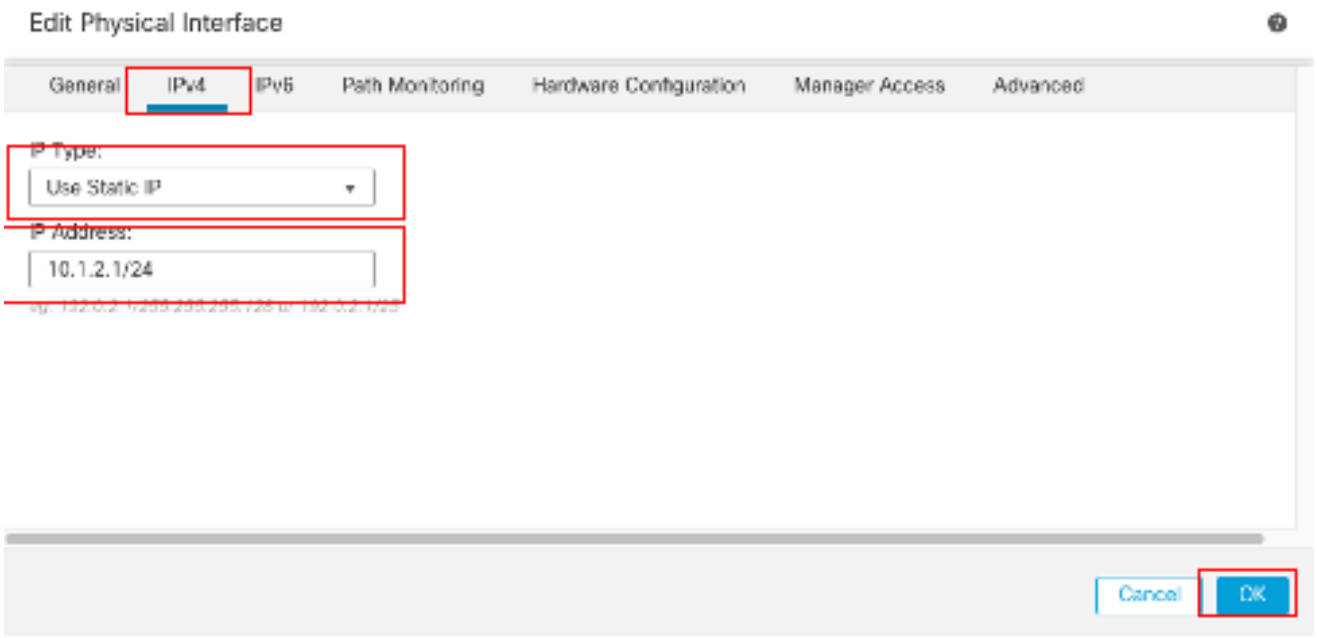
1. Name(이름)을 설정합니다(이 경우 Outside2).
2. Enabled 확인란을 선택하여 인터페이스를 활성화합니다.
3. Security Zone 드롭다운 목록에서 기존 Security Zone을 선택하거나 새 Security Zone을 생성합니다(이 예에서는 Outside2_Zone).



인터페이스 Gi0/1 일반

IPv4 탭 아래에서

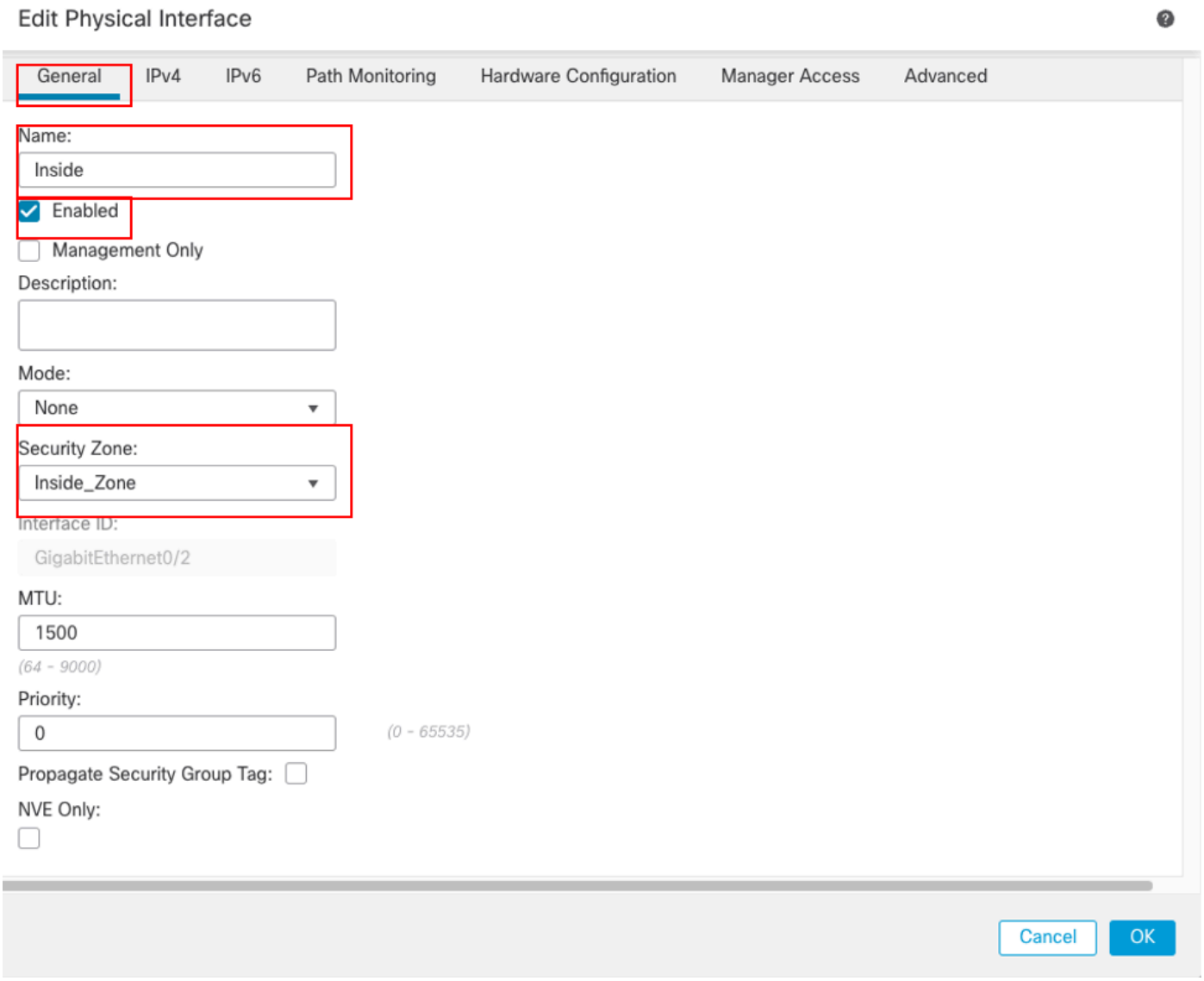
1. IP Type 드롭다운 목록에서 옵션 중 하나를 선택합니다. 이 예에서는 Use Static IP(고정 IP 사용).
2. IP 주소를 설정합니다(이 예에서는 10.1.2.1/24).
3. OK(확인)를 클릭합니다.



인터페이스 Gi0/1 IPv4

Edit Physical Interface(물리적 인터페이스 수정) 창의 General(일반) 탭에서 유사한 단계를 반복하여 인터페이스 GigabitEthernet0/2를 구성합니다.

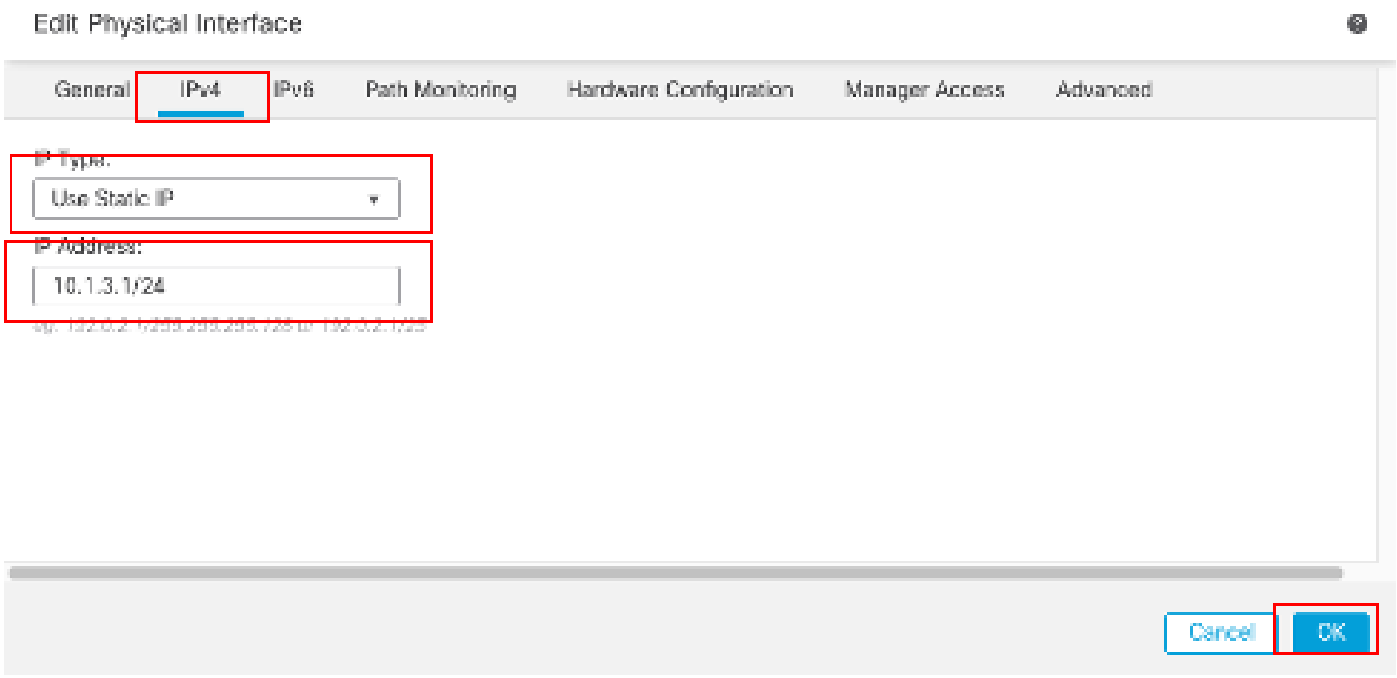
1. Name(이름)을 설정합니다(이 경우 Inside).
2. Enabled 확인란을 선택하여 인터페이스를 활성화합니다.
3. Security Zone 드롭다운 목록에서 기존 Security Zone을 선택하거나 새 Zone을 생성합니다(이 예에서는 Inside_Zone).



인터페이스 Gi0/2 일반

IPv4 탭 아래에서

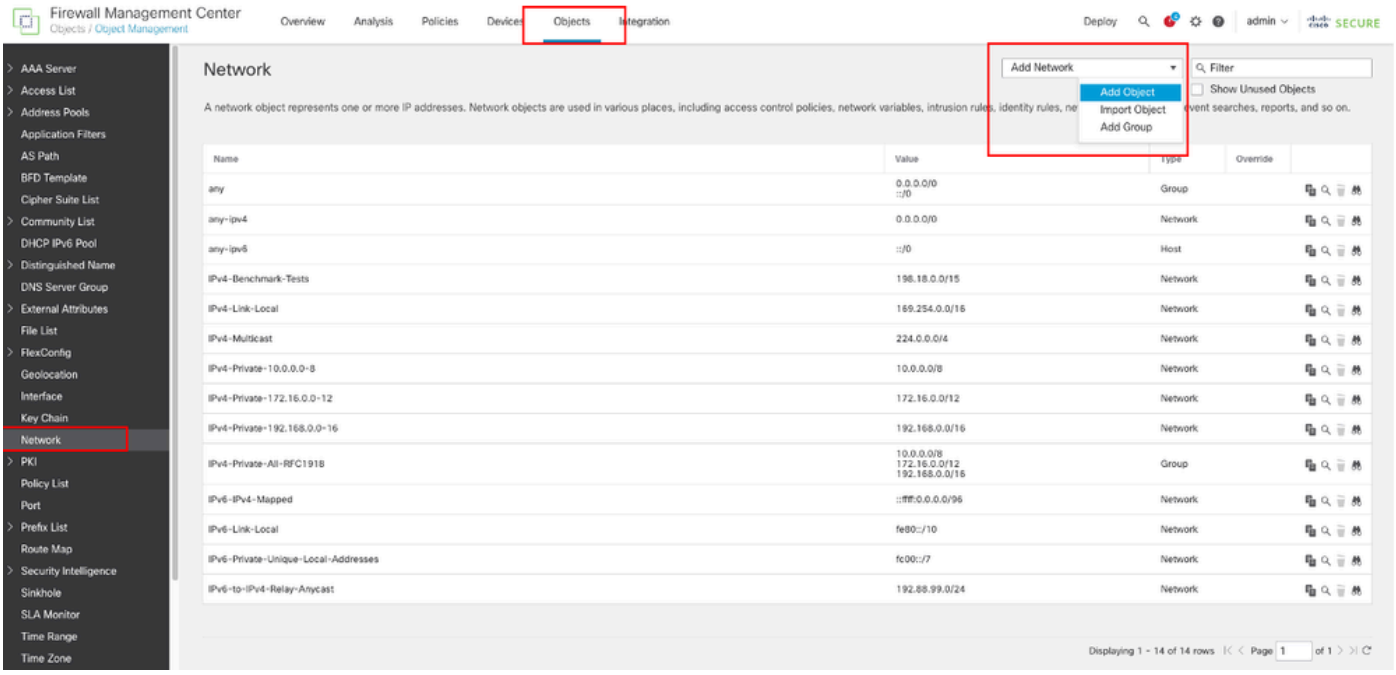
1. IP Type 드롭다운 목록에서 옵션 중 하나를 선택합니다. 이 예에서는 Use Static IP(고정 IP 사용).
2. IP 주소를 설정합니다(이 예에서는 10.1.3.1/24).
3. OK(확인)를 클릭합니다.



인터페이스 Gi0/2 IPv4

컨피그레이션 저장 및 구축을 클릭합니다.

Objects(개체) > Object Management(개체 관리)로 이동하고, 개체 유형 목록에서 Network(네트워크)를 선택하고, Add Network(네트워크 추가) 드롭다운 메뉴에서 Add Object(개체 추가)를 선택하여 첫 번째 ISP 게이트웨이에 대한 개체를 만듭니다.

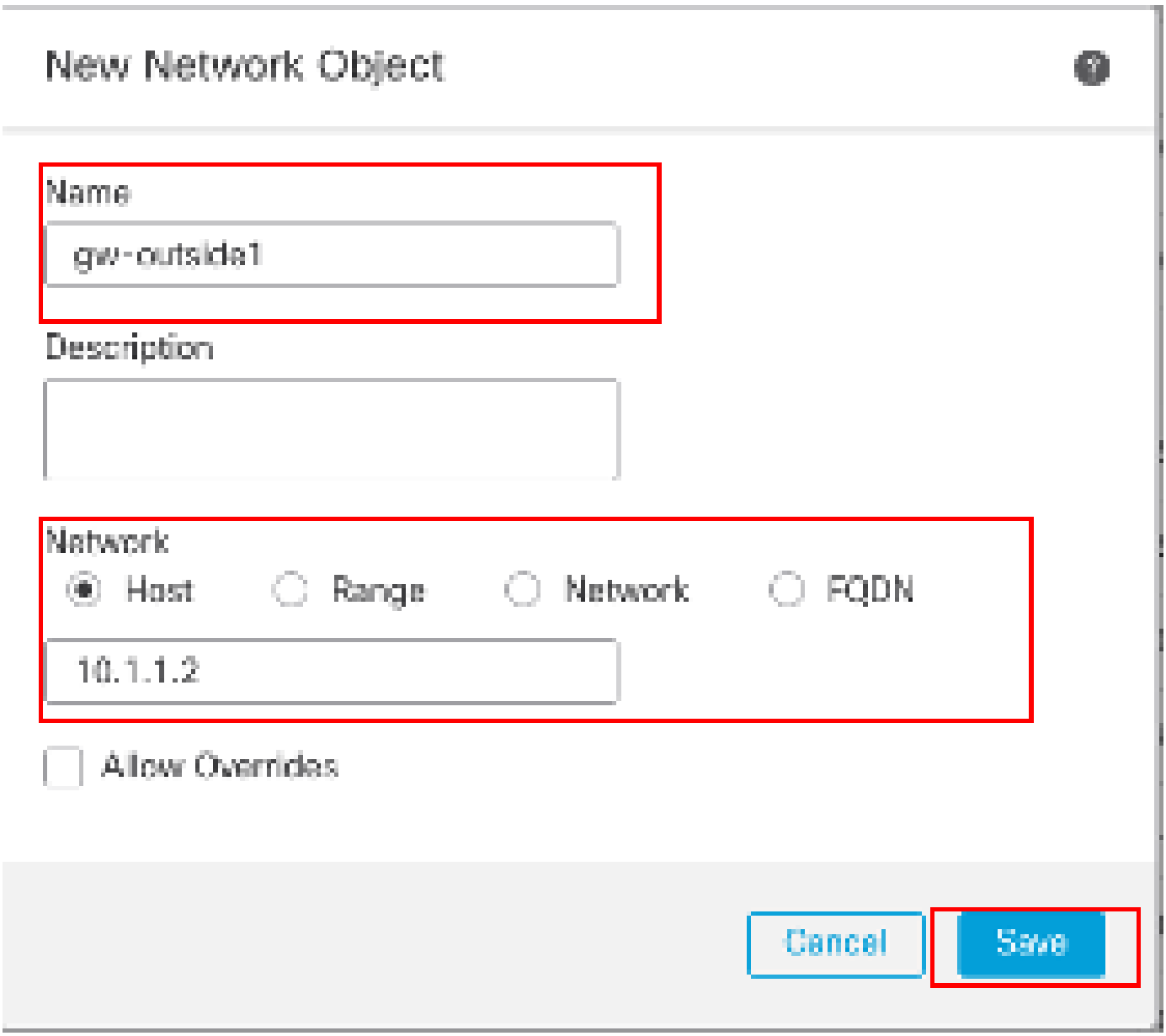


네트워크 개체

New Network Object(새 네트워크 개체) 창에서

1. Name을 설정합니다(이 예에서는 gw-outside1).
2. Network(네트워크) 필드에서 필수 옵션을 선택하고 적절한 값(이 예에서는 Host(호스트) 및 10.1.1.2)을 입력합니다.

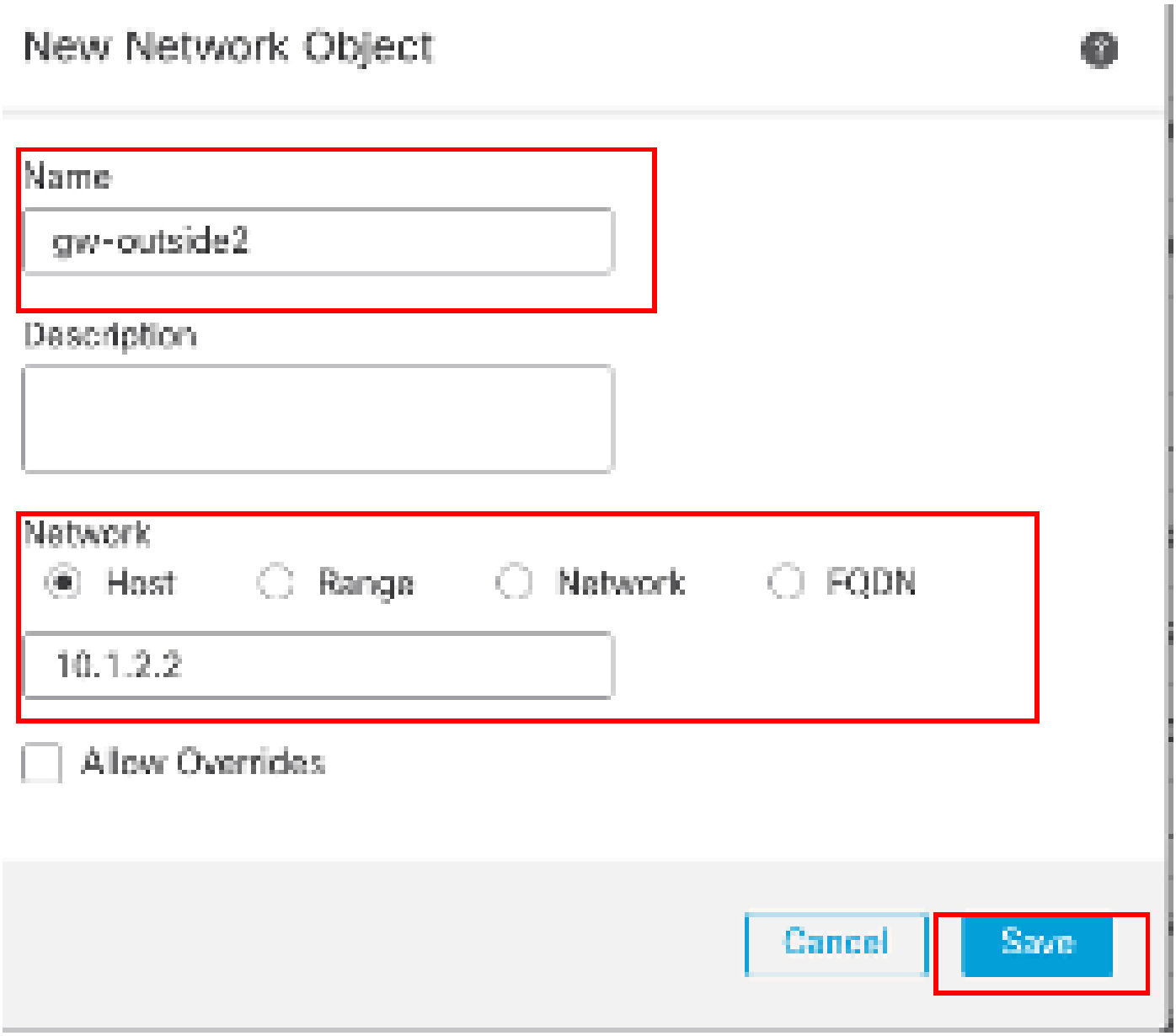
3. 저장을 클릭합니다.



객체 Gw-outside1

유사한 단계를 반복하여 두 번째 ISP 게이트웨이에 대해 다른 객체를 생성합니다. New Network Object(새 네트워크 개체) 창에서

1. Name을 설정합니다(이 예에서는 gw-outside2).
2. Network(네트워크) 필드에서 필수 옵션을 선택하고 적절한 값(이 예에서는 Host 및 10.1.2.2)을 입력합니다.
3. 저장을 클릭합니다.

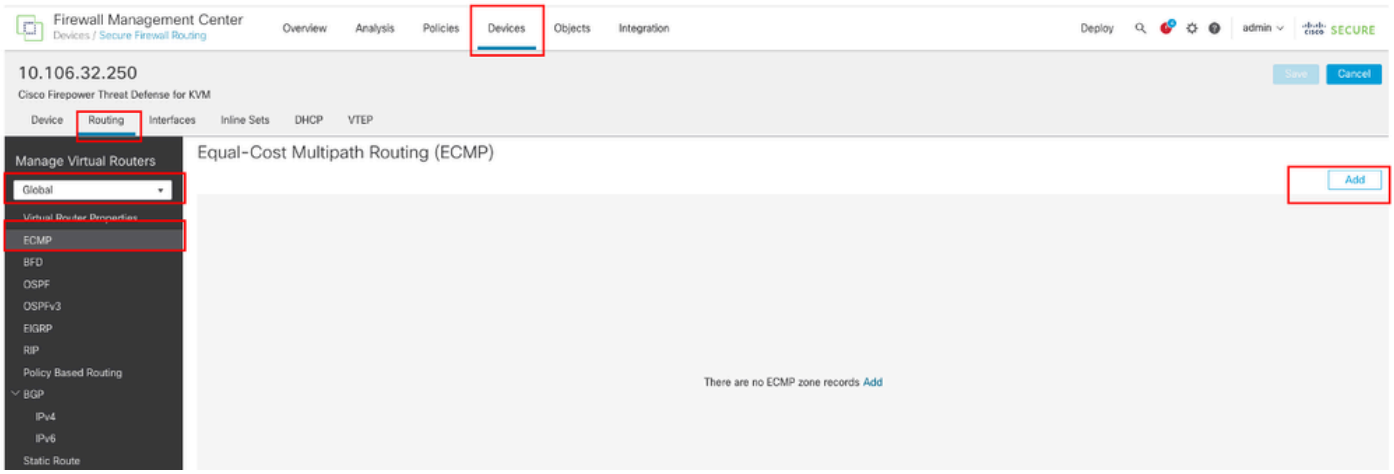


객체 Gw-outside2

1단계. ECMP 영역 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 위협 방어 디바이스를 편집한 다음 Routing(라우팅)을 클릭합니다. virtual router 드롭다운에서 ECMP 영역을 생성할 가상 라우터를 선택합니다. 전역 가상 라우터 및 사용자 정의 가상 라우터에서 ECMP 영역을 생성할 수 있습니다. 이 예에서는 Global을 선택합니다.

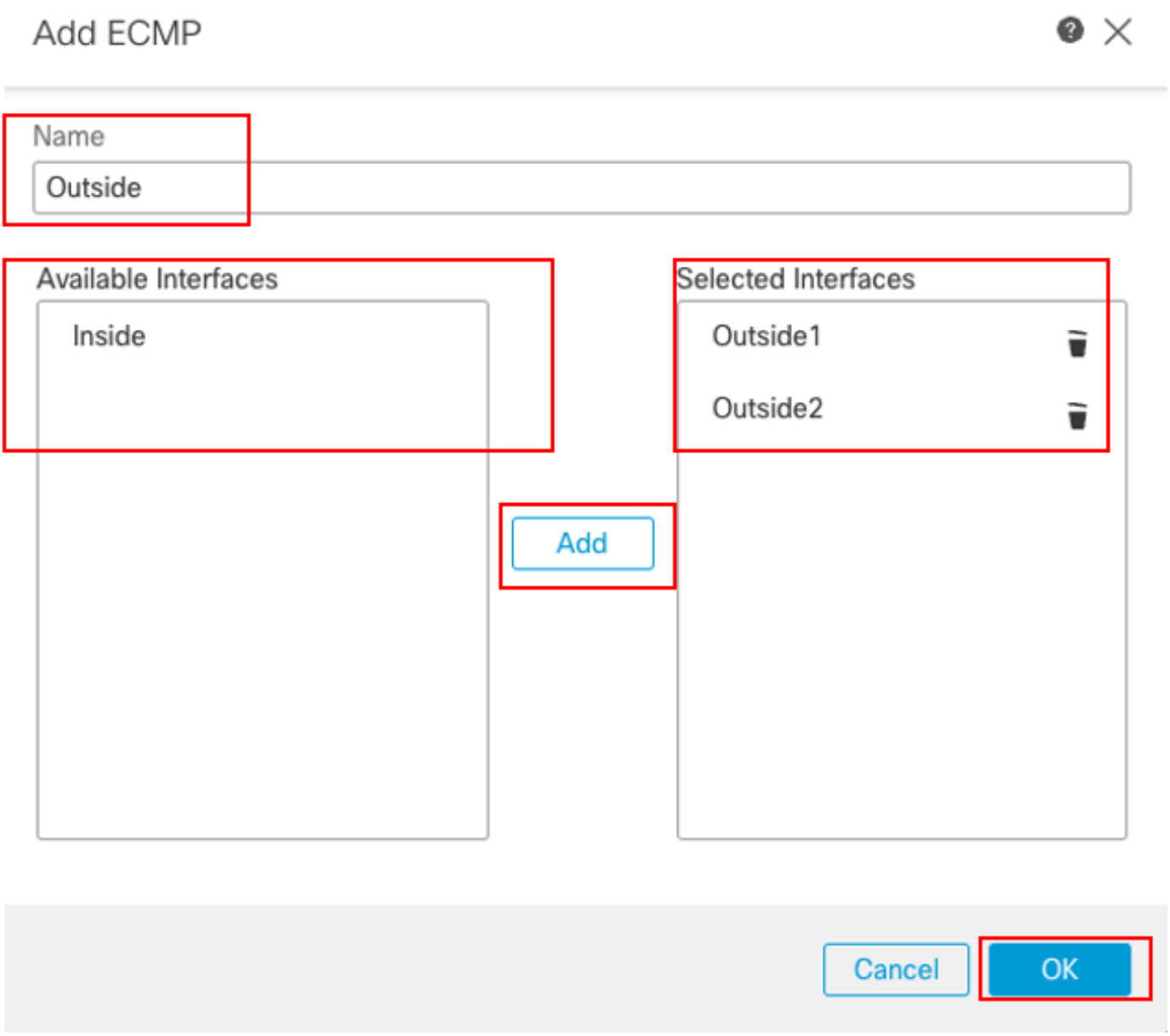
ECMP(ECMP)를 클릭한 다음 Add(추가)를 클릭합니다.



ECMP 영역 구성

Add ECMP(ECMP 추가) 창에서

1. ECMP 영역의 Name(이름)을 설정합니다(이 예에서는 Outside).
2. 인터페이스를 연결하려면 Available Interfaces 상자 아래에서 인터페이스를 선택한 다음 Add를 클릭합니다. 이 예에서는 Outside1 및 Outside2입니다.
3. OK(확인)를 클릭합니다.

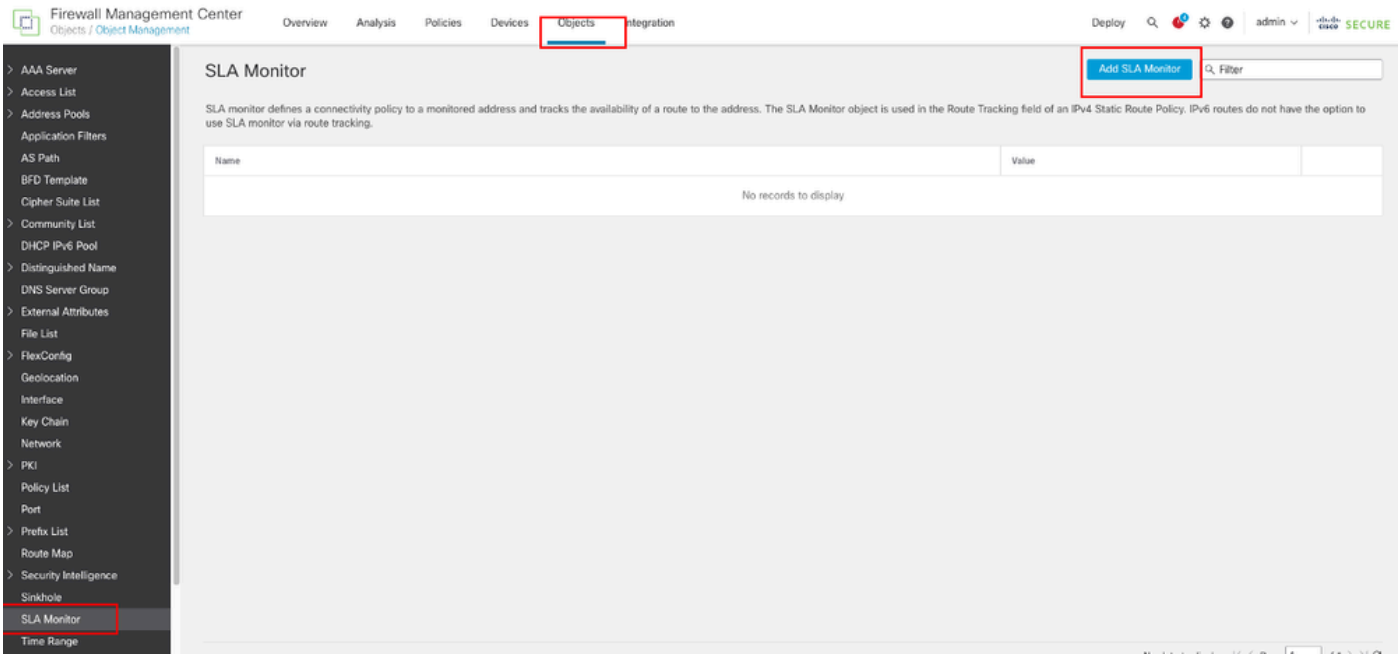


ECMP 영역 외부 구성

컨피그레이션 저장 및 구축을 클릭합니다.

2단계. IP SLA 개체 구성

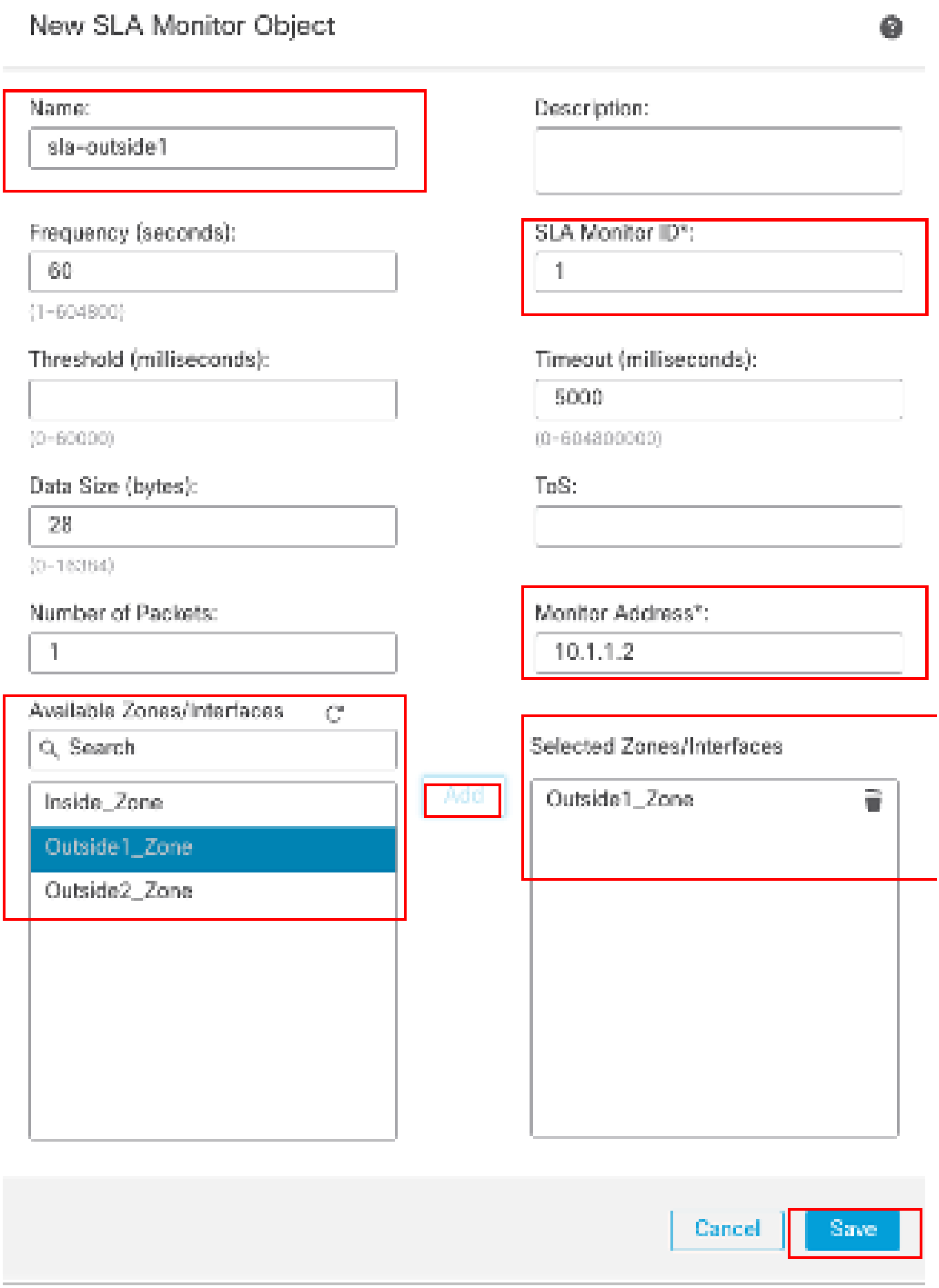
Objects(개체) > Object Management(개체 관리)로 이동하고, 개체 유형 목록에서 SLA Monitor(SLA 모니터)를 선택하고 Add SLA Monitor(SLA 모니터 추가)를 클릭하여 첫 번째 ISP 게이트웨이에 대한 새 SLA 모니터를 추가합니다.



SLA 모니터 생성

New SLA Monitor Object(새 SLA 모니터 개체) 창에서

1. SLA 모니터 객체의 Name을 설정합니다(이 경우 sla-outside1).
2. SLA Monitor ID 필드에 SLA 작업의 ID 번호를 입력합니다. 값의 범위는 1~2147483647입니다. 디바이스에서 최대 2000개의 SLA 작업을 생성할 수 있습니다. 각 ID 번호는 정책 및 디바이스 컨피그레이션에 대해 고유해야 합니다. 이 예에서는 1입니다.
3. SLA 작업에 의해 가용성이 모니터링되는 IP 주소를 Monitored Address(모니터링되는 주소) 필드에 입력합니다. 이 예에서는 10.1.1.2입니다.
4. Available Zones/Interfaces 목록에는 영역 및 인터페이스 그룹이 모두 표시됩니다. Zones/Interfaces(영역/인터페이스) 목록에서 디바이스가 관리 스테이션과 통신하는 데 사용되는 인터페이스를 포함하는 영역 또는 인터페이스 그룹을 추가합니다. 단일 인터페이스를 지정하려면 인터페이스에 대한 영역 또는 인터페이스 그룹을 생성해야 합니다. 이 예에서는 Outside1_Zone입니다.
5. 저장을 클릭합니다.

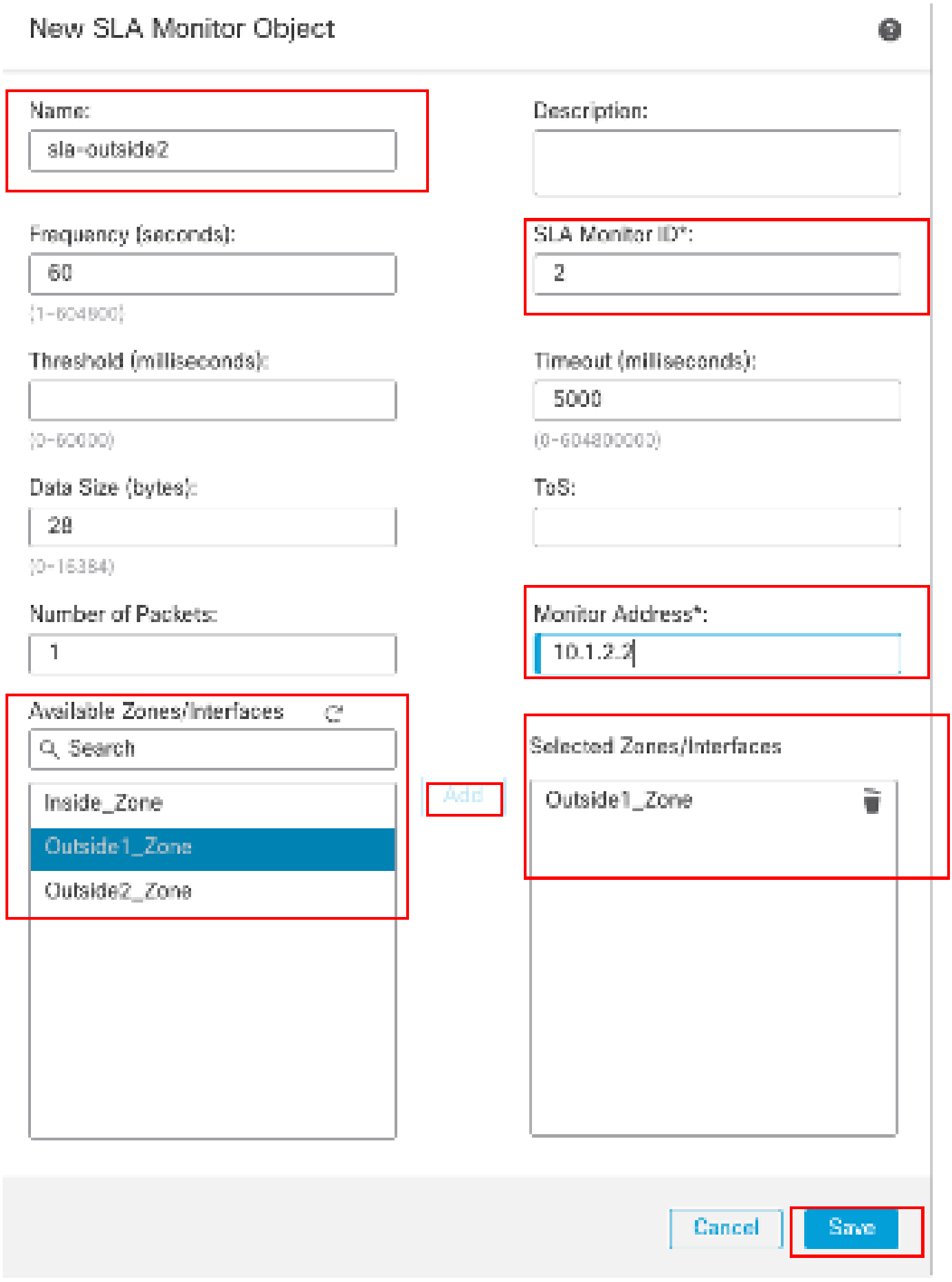


SLA 객체 Sla-outside1

유사한 단계를 반복하여 두 번째 ISP 게이트웨이에 대해 다른 SLA 모니터를 생성합니다.

New SLA Monitor Object(새 SLA 모니터 개체) 창에서

1. SLA 모니터 객체의 Name을 설정합니다(이 경우 sla-outside2).
2. SLA Monitor ID 필드에 SLA 작업의 ID 번호를 입력합니다. 값의 범위는 1~2147483647입니다. 디바이스에서 최대 2000개의 SLA 작업을 생성할 수 있습니다. 각 ID 번호는 정책 및 디바이스 컨피그레이션에 대해 고유해야 합니다. 이 예에서는 2.
3. SLA 작업에 의해 가용성이 모니터링되는 IP 주소를 Monitored Address(모니터링되는 주소) 필드에 입력합니다. 이 예에서는 10.1.2.2입니다.
4. Available Zones/Interfaces 목록에는 영역 및 인터페이스 그룹이 모두 표시됩니다. Zones/Interfaces(영역/인터페이스) 목록에서 디바이스가 관리 스테이션과 통신하는 데 사용되는 인터페이스를 포함하는 영역 또는 인터페이스 그룹을 추가합니다. 단일 인터페이스를 지정하려면 인터페이스에 대한 영역 또는 인터페이스 그룹을 생성해야 합니다. 이 예에서는 Outside2_Zone입니다.
5. 저장을 클릭합니다.

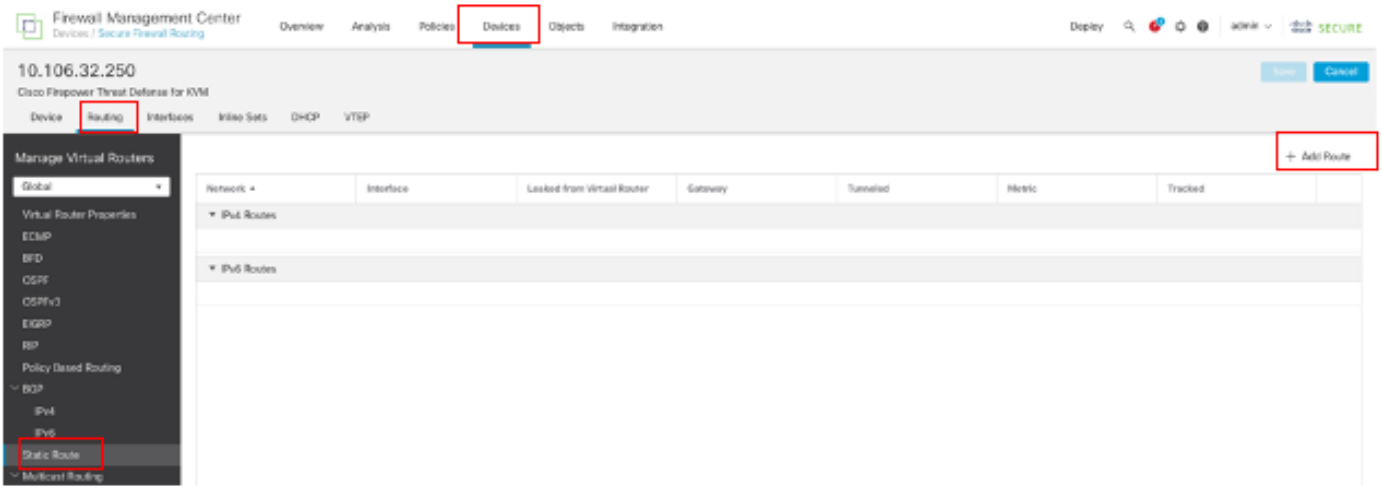


SLA 객체 Sla-outside2

3단계. 경로 추적을 사용하여 고정 경로 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 위협 방어 디바이스를 편집한 Routing(라우팅)을 클릭합니다. 가상 라우터 드롭다운 목록에서 고정 경로를 구성할 가상 라우터를 선택합니다. 이 예에서는 Global입니다.

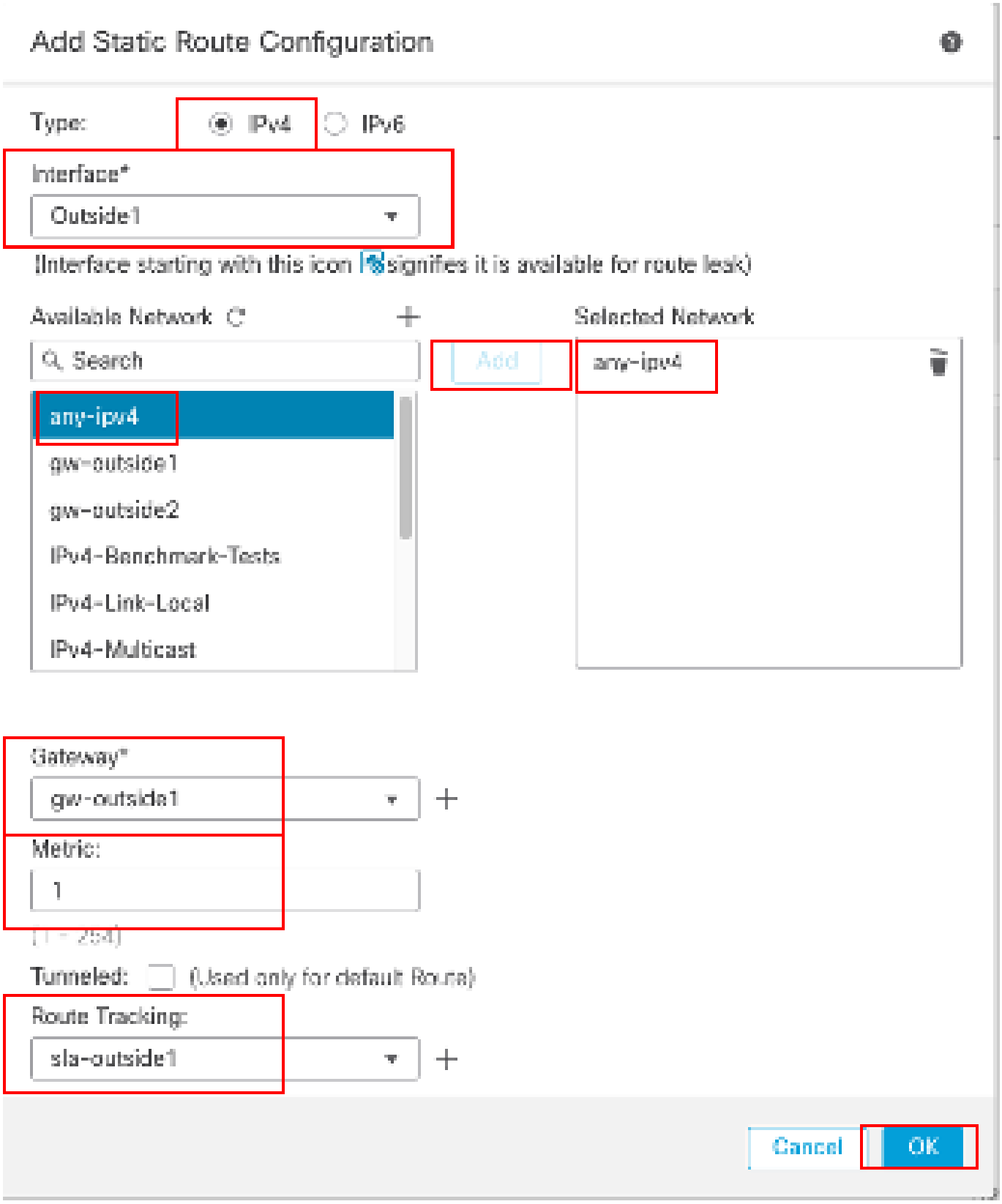
Static Route를 선택하고 Add Route를 클릭하여 첫 번째 ISP 게이트웨이에 기본 경로를 추가합니다.



고정 경로 구성

Add Static Route Configuration(고정 경로 컨피그레이션 추가) 창에서

1. 추가하는 고정 경로의 유형에 따라 IPv4 또는 IPv6을 클릭합니다. 이 예에서는 IPv4입니다.
2. 이 고정 경로가 적용되는 인터페이스를 선택합니다. 이 예에서는 Outside1입니다.
3. Available Network 목록에서 대상 네트워크를 선택합니다. 이 예에서는 any-ipv4입니다.
4. Gateway or IPv6 Gateway(게이트웨이 또는 IPv6 게이트웨이) 필드에 이 경로의 다음 홉인 게이트웨이 라우터를 입력하거나 선택합니다. IP 주소 또는 Networks/Hosts 객체를 제공할 수 있습니다. 이 예에서는 gw-outside1입니다.
5. Metric(메트릭) 필드에 대상 네트워크로의 홉 수를 입력합니다. 유효한 값의 범위는 1~255이며 기본값은 1입니다. 이 예에서는 1입니다.
6. 경로 가용성을 모니터링하려면 Route Tracking(경로 추적) 필드에 모니터링 정책을 정의하는 SLA Monitor(SLA 모니터링) 객체의 이름을 입력하거나 선택합니다. 이 예에서는 sla-outside1입니다.
7. OK(확인)를 클릭합니다.

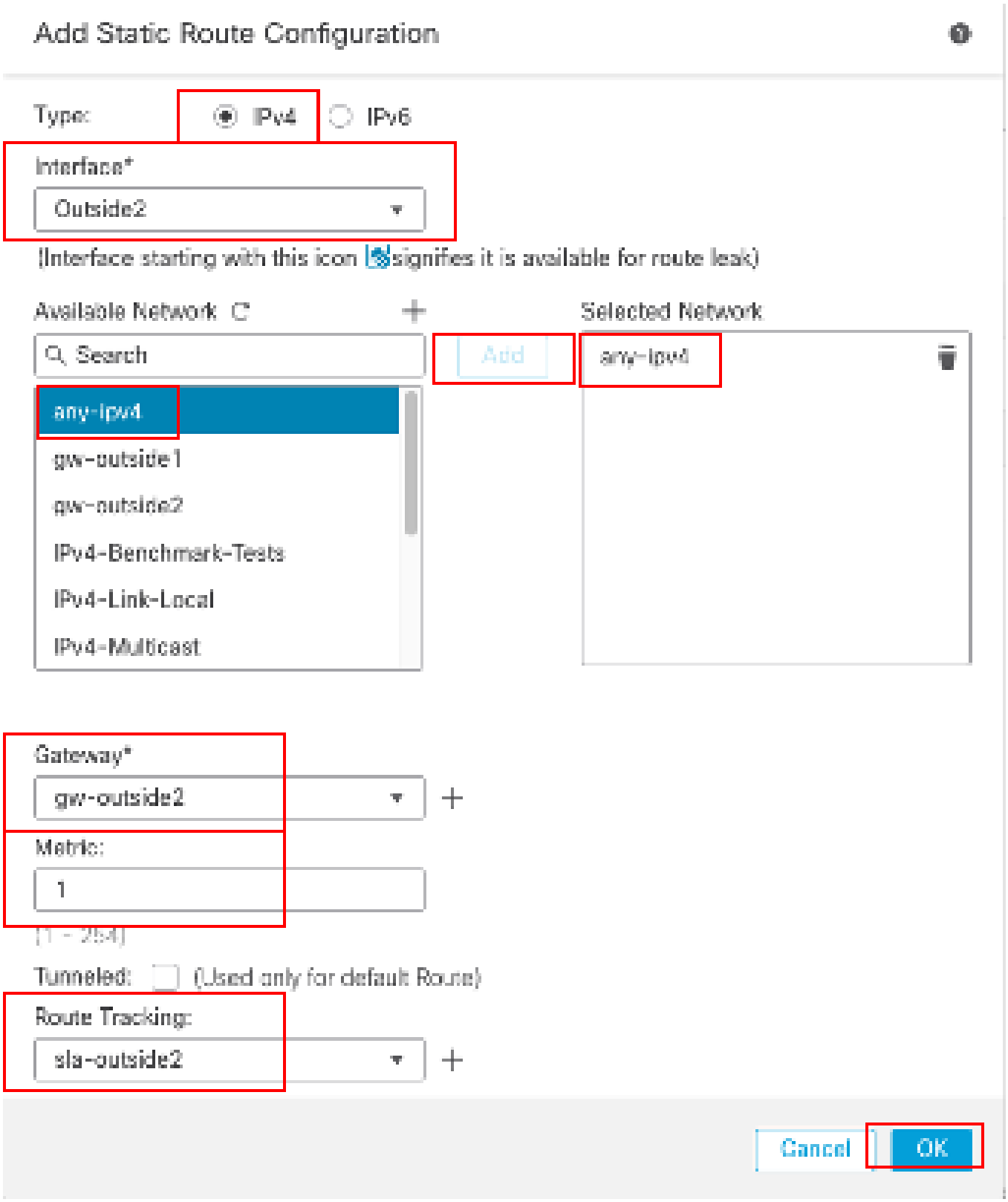


고정 경로 첫 번째 ISP 추가

유사한 단계를 반복하여 두 번째 ISP 게이트웨이에 기본 경로를 추가합니다. Add Static Route Configuration(고정 경로 컨피그레이션 추가) 창에서

1. 추가하는 고정 경로의 유형에 따라 IPv4 또는 IPv6을 클릭합니다. 이 예에서는 IPv4입니다.
2. 이 고정 경로가 적용되는 인터페이스를 선택합니다. 이 예에서는 Outside2입니다.
3. Available Network 목록에서 대상 네트워크를 선택합니다. 이 예에서는 any-ipv4입니다.

4. Gateway or IPv6 Gateway(게이트웨이 또는 IPv6 게이트웨이) 필드에 이 경로의 다음 홉인 게이트웨이 라우터를 입력하거나 선택합니다. IP 주소 또는 Networks/Hosts 객체를 제공할 수 있습니다. 이 예에서는 gw-outside2입니다.
5. Metric(메트릭) 필드에 대상 네트워크로의 홉 수를 입력합니다. 유효한 값의 범위는 1~255이며 기본값은 1입니다. 이 예 1에서 첫 번째 경로와 동일한 메트릭을 지정해야 합니다.
6. 경로 가용성을 모니터링하려면 Route Tracking(경로 추적) 필드에 모니터링 정책을 정의하는 SLA Monitor(SLA 모니터링) 객체의 이름을 입력하거나 선택합니다. 이 예에서는 sla-outside2입니다.
7. OK(확인)를 클릭합니다.



고정 경로 보조 ISP 추가

컨피그레이션 저장 및 구축을 클릭합니다.

다음을 확인합니다.

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

show running-config route

<#root>

```
> show zone
Zone: Outside ecmp
Security-level: 0
```

Zone member(s): 2

Outside2 GigabitEthernet0/1

Outside1 GigabitEthernet0/0

명령을 실행하여 라우팅 컨피그레이션의 실행 중인 컨피그레이션을 확인합니다. 이 경우 경로 트랙이 있는 고정 경로가 2개 있습니다.

show route

<#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

명령을 실행하여 라우팅 테이블을 확인합니다. 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
```

명령을 실행하여 **show sla monitor configuration** SLA 모니터의 컨피그레이션을 확인합니다.

<#root>

```
> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1
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: 2
```

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 모니터show 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: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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

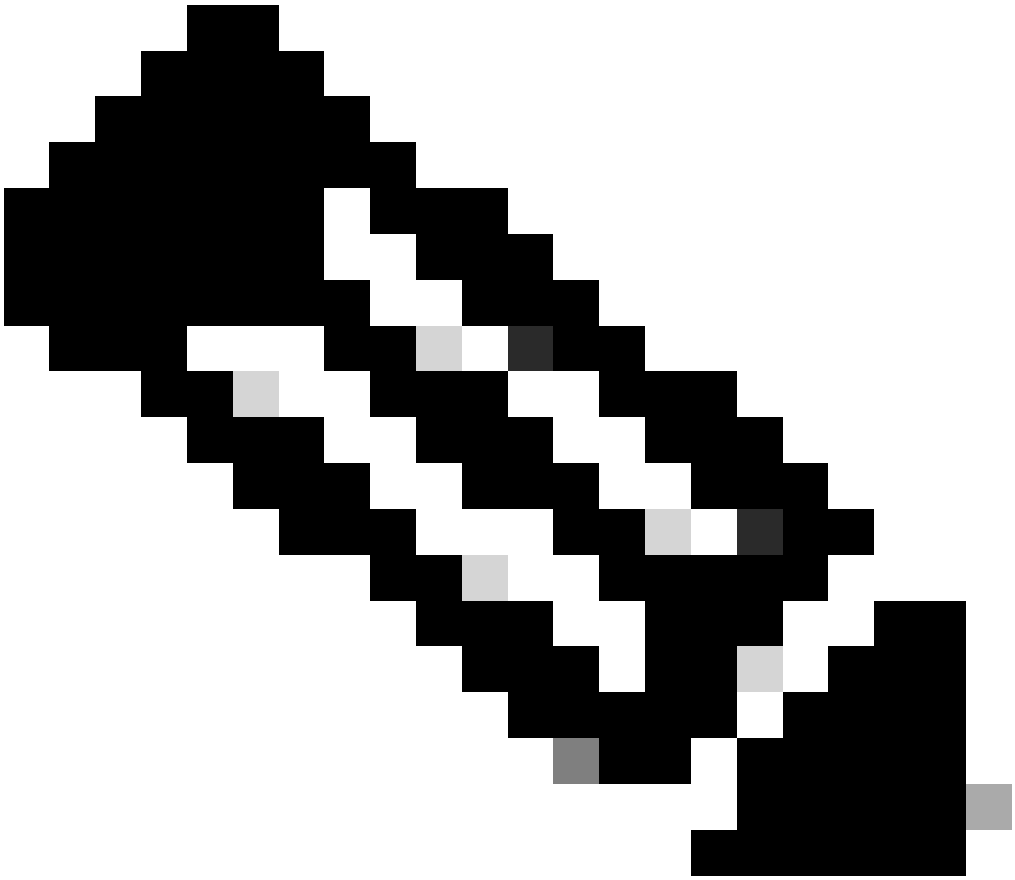
```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

로드 밸런싱

ECMP 로드가 ECMP 영역의 게이트웨이 간에 트래픽 밸런싱을 수행하는지 확인하기 위해 FTD를 통한 초기 트래픽. 이 경우 Inside-Host1(10.1.3.2) 및 Inside-Host2(10.1.3.4)에서 Internet-Host(10.1.5.2)로 텔넷 연결을 시작하고, 명령을 실행하여 두 ISP 링크 간 **show conn** 에 트래픽이 로드 밸런싱되는지 확인하고, Inside-Host1(10.1.3.2)은 interface outside1을 통해, Inside-Host2(10.1.3.4)는 interface outside2를 통해 트래픽을 전달합니다.

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, 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.

명령을 show sla monitor operational-state 실행하여 SLA 모니터의 현재 상태를 확인합니다. 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: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
```

```
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 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
```

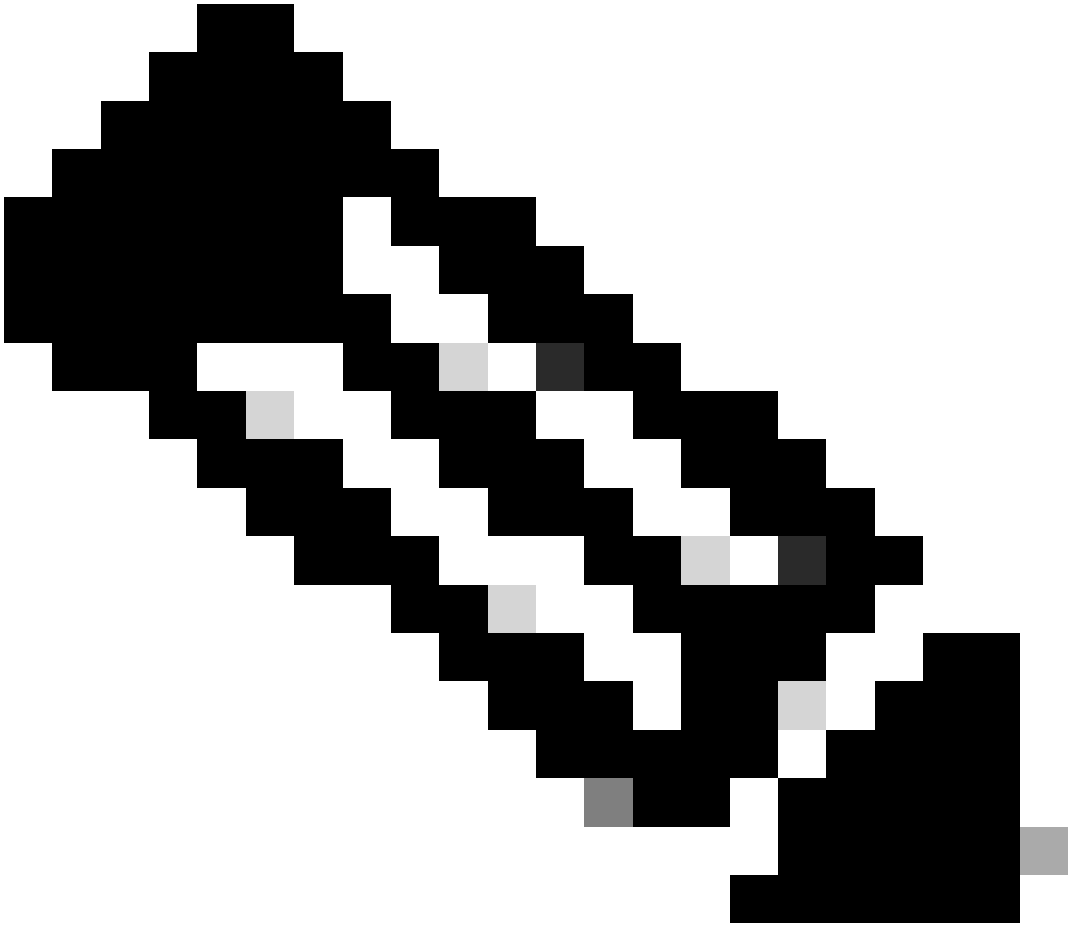
명령을 show conn 실행하면 두 연결이 여전히 작동 중인 것을 확인할 수 있습니다. 텔넷 세션은 Inside-Host1(10.1.3.2) 및 Inside-Host2(10.1.3.4)에서도 중단 없이 활성화됩니다.

<**#root**>

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1
```

```
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```



참고: 인터페이스 outside1을 통한show conn 기본 경로가 라우팅 테이블에서 제거되었지만, Inside-Host1(10.1.3.2)의 텔넷 세션이 여전히 인터페이스 outside1을 통해 있다는 것을 출력에서 확인할 수 있습니다. 이는 설계에 따라 인터페이스 outside2를 통해 실제 트래픽이 이동하는 것으로 예상됩니다. Inside-Host1(10.1.3.2)에서 Internet-Host(10.1.5.2)로의 새 연결을 시작하면 interface outside2를 통해 모든 트래픽이 전달됨을 확인할 수 있습니다.

문제 해결

라우팅 테이블 변경을 검증하려면 명령을 debug ip routing 실행합니다.

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 확인합니다show 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.


```
> debug ip routing
IP routing debugging is on
```

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 확인합니다show 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

[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
```

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.