# ECMP

이 장에서는 라우팅 프로토콜이 네트워크 트래픽의 로드 밸런싱에 사용하는 ECMP(Equal Cost Multi-Path) 라우팅을 구성하는 절차에 대해 설명합니다.



## ECMP 정보

Firepower Threat Defense 디바이스는 ECMP(Equal-Cost Multi-Path) 라우팅을 지원합니다. 인터페이스 그룹을 포함하도록 가상 라우터당 트래픽 영역을 구성할 수 있습니다. 하나의 영역 내에서 최대 8개의 인터페이스에 걸쳐 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 다음과 같이 영역 내 인터페이스 3개의 전 범위에 걸쳐 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

## ECMP에 대한 지침 및 제한 사항

방화벽 모드 지침

ECMP 영역은 라우팅된 방화벽 모드에서만 지원됩니다.

디바이스 지침

- Threat Defense 6.5 이상 디바이스는 management center에서 ECMP 트래픽 영역 구성을 지원합니다.
  - 버전 6.6 이상의 Threat Defense 디바이스는 가상 라우터당 ECMP를 지원합니다.
  - threat defense 6.5 이하 디바이스는 가상 라우팅을 지원하지 않으므로 전역 인터페이스를 ECMP와 연결할 수 있습니다.
- 디바이스는 최대 256개의 ECMP 영역을 가질 수 있습니다.

인터페이스 지침

- 전역 가상 라우터 및 사용자 정의 가상 라우터에서 ECMP 영역을 생성할 수 있습니다.
- 라우팅된 인터페이스만 ECMP 영역과 연결할 수 있습니다.
- 논리적 이름이 있는 인터페이스만 ECMP 영역과 연결할 수 있습니다.
- 인터페이스는 ECMP가 생성되는 가상 라우터에 속해야 합니다.
- ECMP 영역당 8개의 인터페이스만 연결할 수 있습니다.
- 인터페이스는 하나의 ECMP 영역에만 속할 수 있습니다.
- ECMP 영역에서 동일 비용 정적 경로와 연결된 인터페이스는 제거할 수 없습니다.
- 인터페이스에 동일한 비용 정적 경로가 연결된 경우 ECMP 영역을 삭제할 수 없습니다.
- 7.1 이전 버전의 Threat Defense 버전인 경우 sVTI 인터페이스는 ECMP 영역에서 사용할 수 없습니다.
- 7.1 이전 버전의 Threat Defense 버전인 경우 ECMP 영역 멤버 인터페이스는 사이트 간 VPN 또는 원격 액세스 IPsec-IKEv2 VPN에서 지원되지 않습니다.
- 다음 인터페이스는 ECMP 영역과 연결할 수 없습니다.
  - BVI 인터페이스.
  - EtherChannel의 멤버 인터페이스.
  - 페일오버 또는 상태 링크 인터페이스.
  - 관리 전용 또는 관리 액세스 인터페이스.
  - 클러스터 제어 링크 인터페이스.
  - 이중 인터페이스 및 해당 멤버.
  - VNI.
  - VLAN 인터페이스.
  - SSL이 활성화된 RA VPN 구성의 인터페이스.

업그레이드 지침

management center 7.0 이하 버전에서 업그레이드하는 경우 기존의 ECMP용 FlexConfig가 디바이스에 구축되지 않습니다. 따라서 구축에 성공하려면 UI에서 FlexConfig 트래픽 영역을 ECMP로 수동으로 마이그레이션해야 합니다.

모든 6.5 이상 라우팅 디바이스에 대해 management center UI에서 ECMP를 생성할 수 있습니다.

추가 지침

- DHCP 릴레이 - ECMP 영역과 연결된 인터페이스에서 DHCP 릴레이를 활성화하지 마십시오.
- 이중 ISP/WAN 위협 방어 구축 - 기본 및 보조 데이터 인터페이스에 대한 단일 ECMP 영역을 생성합니다. 이 구성을 사용하면 동일한 메트릭 값을 사용하여 두 인터페이스에 대한 고정 경로를 생성할 수 있습니다.
- Threat Defense는 IPsec 세션에서 NAT를 포함한 ECMP를 지원하지 않습니다. 즉, 표준 IPsec VPN(Virtual Private Network) 터널은 IPsec 패킷 전달 경로에서 NAT 포인트와 함께 작동하지 않습니다.

# ECMP 관리 페이지

Routing(라우팅) 창에서 **ECMP**를 클릭하면 가상 라우터에 해당하는 ECMP 페이지가 나타납니다. 이 페이지에는 가상 라우터의 연결된 인터페이스가 있는 기존 ECMP 영역이 표시됩니다. 이 페이지에서 가상 라우터에 ECMP 영역을 추가할 수 있습니다. **Edit(**수정**)** ( ) 및 **Delete(**삭제**)** ( ) ECMP도 가능합니다.

다음을 수행할 수 있습니다.

- ECMP 영역 생성, 3 페이지
- 동일 비용 정적 경로 구성, 4 페이지
- ECMP 영역 수정, 6 페이지
- ECMP 영역 제거, 6 페이지

# ECMP 영역 생성

ECMP 영역은 가상 라우터별로 생성됩니다. 따라서 ECMP가 생성되는 가상 라우터의 인터페이스만 ECMP와 연결될 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** 가상 라우터 드롭다운에서 ECMP 영역을 생성할 가상 라우터를 선택합니다.

전역 가상 라우터 및 사용자 정의 가상 라우터에서 ECMP 영역을 생성할 수 있습니다. 가상 라우터 생성에 대한 자세한 내용은 가상 라우터 생성의 내용을 참조하십시오.

단계 **4** **ECMP**를 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Add ECMP(ECMP** 추가**)** 상자에 ECMP 영역의 이름을 입력합니다.

참고 ECMP 이름은 라우팅된 디바이스에 대해 고유해야 합니다.

단계 **7** 인터페이스를 연결하려면 **Available Interface(**사용 가능한 인터페이스**)** 상자에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.

다음 사항에 유의하십시오.

- 가상 라우터에 속한 인터페이스만 할당에 사용할 수 있습니다.
- **Available Interface(**사용 가능한 인터페이스**)** 상자 아래에는 논리적 이름이 있는 인터페이스만 나열됩니다. **Interface(**인터페이스**)**에서 논리적 이름을 제공하고 인터페이스를 편집할 수 있습니다. 설정이 적용되려면 변경 사항을 저장해야 합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

이제 ECMP 페이지에 새로 생성된 ECMP가 표시됩니다.

단계 **9** **Save(**저장**)**를 클릭하고 구성을 **Deploy(**구축**)**합니다.

---

동일한 대상 및 메트릭 값으로 정의하여 ECMP 영역 인터페이스를 동일한 비용의 정적 경로와 연결할 수 있지만 다른 게이트웨이를 사용합니다.

다음에 수행할 작업

- 동일 비용 정적 경로 구성, 4 페이지
- ECMP 영역 수정, 6 페이지
- ECMP 영역 제거, 6 페이지

# 동일 비용 정적 경로 구성

| 스마트 라이선스 | 기본 라이선스 | 지원되는 장치 | 지원되는 도메인 | 액세스 |
|---|---|---|---|---|
| 모두 | 해당 없음 | threat defense 및 threat defense virtual | 모두 | 관리자/네트워크 관리자/보안 승인자 |

전역 및 사용자 정의 가상 라우터의 인터페이스를 디바이스의 ECMP 영역에 할당할 수 있습니다.

시작하기 전에

- 인터페이스에 대해 동일 비용 고정 경로를 구성하려면 이를 ECMP 영역과 연결해야 합니다. ECMP 영역 생성, 3 페이지의 내용을 참조하십시오.
- 비 VRF 가능 디바이스의 모든 라우팅 구성 설정은 글로벌 가상 라우터에도 사용할 수 있습니다.
- 인터페이스를 ECMP 영역과 연결하지 않고는 대상 및 메트릭이 동일한 인터페이스에 대해 정적 경로를 정의할 수 없습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 threat defense 디바이스를 편집합니다. 라우팅 탭을 클릭합니다.

단계 **2** 드롭다운 목록에서 인터페이스가 ECMP 영역과 연결된 가상 라우터를 선택합니다.

단계 **3** 인터페이스에 대해 동일 비용 고정 경로를 구성하려면 **Static Route(**고정 경로**)**를 클릭합니다.

단계 **4** **Add Route(**경로 추가**)**를 클릭하여 새 경로를 추가하거나 기존 경로에 대해 **Edit(**수정**)** ( )를 클릭합니다.

단계 **5** **Interface(**인터페이스**)** 드롭다운에서 가상 라우터 및 ECMP 영역에 속한 인터페이스를 선택합니다.

단계 **6** **Available Networks(**사용 가능한 네트워크**)** 상자에서 대상 네트워크를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **7** 네트워크의 게이트웨이를 입력합니다.

단계 **8** 메트릭 값을 입력합니다. 1~254 범위의 숫자일 수 있습니다.

단계 **9** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **10** 동일 비용 고정 라우팅을 구성하려면 동일한 대상 네트워크 및 메트릭 값을 사용하여 동일한 ECMP 영역에서 다른 인터페이스에 대한 고정 경로를 구성하는 단계를 반복합니다. 다른 게이트웨이를 제공해야 합니다.

다음에 수행할 작업

- ECMP 영역 수정, 6 페이지
- ECMP 영역 제거, 6 페이지

# ECMP 영역 수정

프로시저

단계 1 **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing(**라우팅**)**을 클릭합니다.

단계 3 **ECMP**를 클릭합니다.

연결된 인터페이스가 있는 ECMP 영역이 **ECMP** 페이지에 표시됩니다.

단계 4 ECMP를 수정하려면 원하는 ECMP에 대해 **Edit(**수정**)** ( )를 클릭합니다. **Edit ECMP(ECMP** 편집**)** 상자에서 다음을 수행할 수 있습니다.

- ECMP Name(ECMP 이름) - 변경된 이름이 디바이스에 대해 고유한지 확인합니다.
- Interfaces(인터페이스) - 인터페이스를 추가하거나 제거할 수 있습니다. 이미 다른 ECMP와 연결된 인터페이스는 포함할 수 없습니다. 또한 동일 비용 고정 경로와 연결된 인터페이스는 제거할 수 없습니다.

단계 5 **OK(**확인**)**를 클릭합니다.

단계 6 변경 사항을 저장하려면 **Save(**저장**)**을 클릭합니다.

다음에 수행할 작업

- 동일 비용 정적 경로 구성, 4 페이지
- ECMP 영역 제거, 6 페이지

# ECMP 영역 제거

프로시저

단계 1 **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing(**라우팅**)**을 클릭합니다.

단계 3 **ECMP**를 클릭합니다.

연결된 인터페이스가 있는 ECMP 영역이 **ECMP** 페이지에 표시됩니다.

단계 4 ECMP 영역을 제거하려면 ECMP 영역에 대해 **Delete(**삭제**)** ( )을 클릭합니다.

인터페이스가 동일 비용 정적 경로와 연결된 경우 ECMP 영역을 삭제할 수 없습니다.

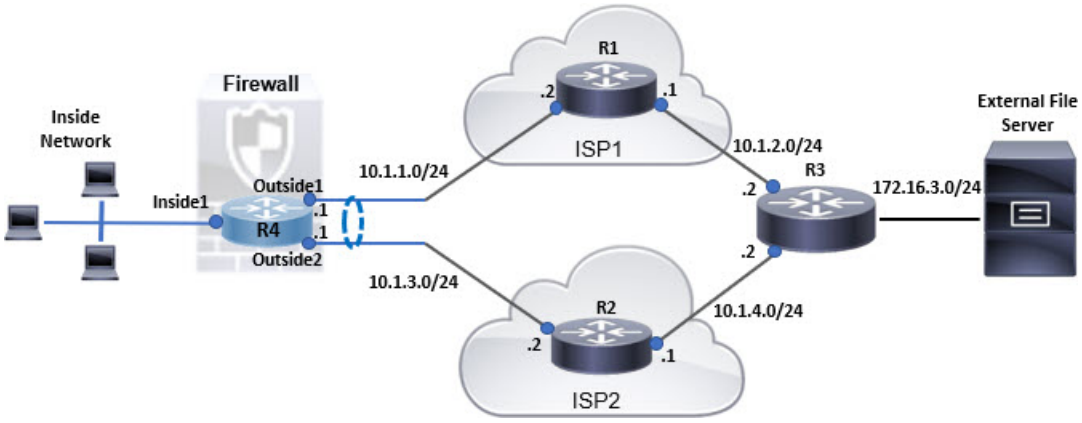
단계 **5** 확인 메시지에서 **Delete(**삭제**)**를 클릭합니다.

단계 **6** 변경 사항을 저장하려면 **Save(**저장**)**을 클릭합니다.

# ECMP에 대한 구성 예

이 예에서는 management center를 사용하여 디바이스를 통과하는 트래픽이 효율적으로 처리되도록 threat defense에서 ECMP 영역을 구성하는 방법을 보여줍니다. ECMP가 구성된 경우 threat defense는 영역별로 라우팅 테이블을 유지하므로 가능한 최적의 경로에서 패킷을 다시 라우팅할 수 있습니다. 따라서 ECMP는 비대칭 라우팅, 로드 밸런싱을 지원하고 손실된 트래픽을 원활하게 처리합니다. 이 예에서 R4는 외부 파일 서버에 연결하기 위해 두 개의 경로를 기록합니다.

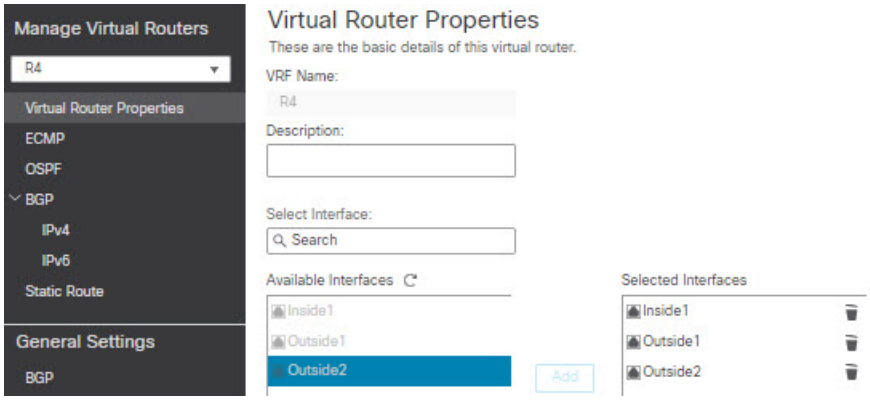
그림 ***1: ECMP***에 대한 구성 예




프로시저

단계 **1** 가상 라우터 생성 — *Inside1*, *Outside1* 및 *Outside2* 인터페이스가 있는 *R4*:

그림 ***2: R4*** 가상 라우터 구성



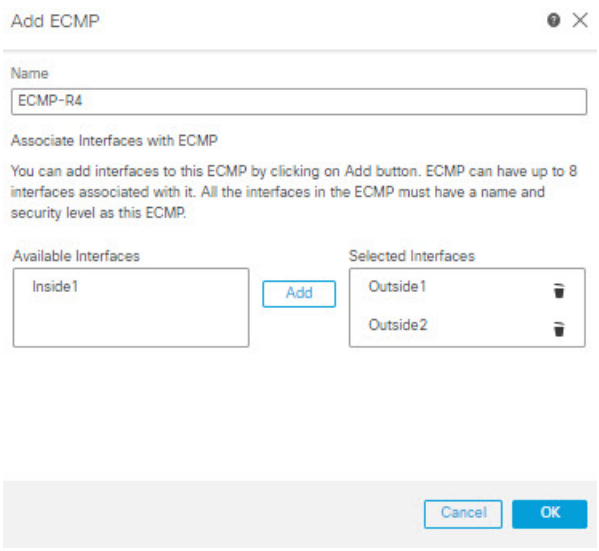
단계 **2** ECMP 영역을 생성합니다.

a) **Routing(**라우팅**)** 탭에서 R4 사용자 정의 가상 라우터를 선택하고 **ECMP**를 클릭합니다.

b) **Add(**추가**)**를 클릭합니다.

c) ECMP 이름을 입력하고 **Available Interfaces(**사용 가능한 인터페이스**)** 목록에서 *Outside1* 및 *Outside2*를 선택합니다.

그림 ***3: ECMP*** 영역 생성




d) **OK(**확인**)**를 클릭한 다음 **Save(**저장**)**를 클릭합니다.

단계 **3** 영역 인터페이스에 대한 고정 경로를 생성합니다.

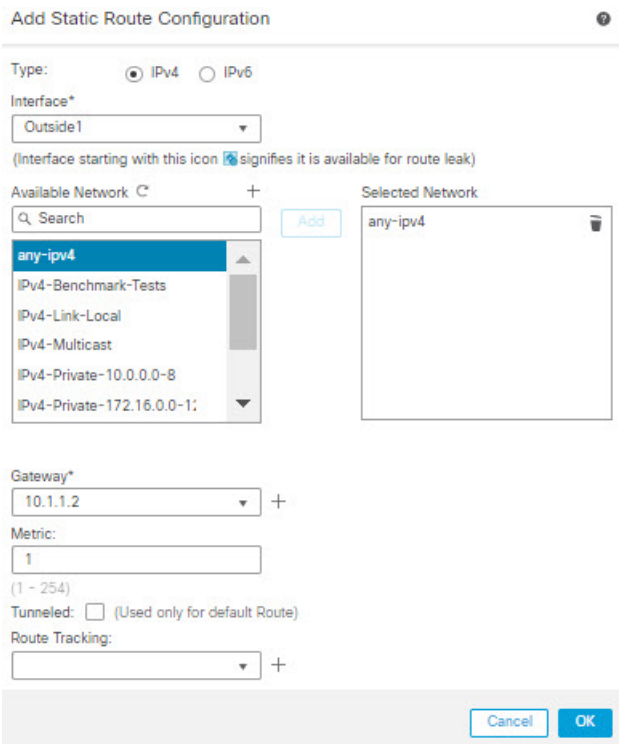
a) **Routing(**라우팅**)** 탭에서 **Static Route(**고정 경로**)**를 클릭합니다.

b) **Interface(**인터페이스**)** 드롭다운 목록에서 Outside1을 선택합니다.

c) **Available Network(**사용 가능한 네트워크**)** 아래에서 any-ipv4를 선택하고 **Add(**추가**)**를 클릭합니다.

d) **Gateway(**게이트웨이**)** 필드에 다음 홉 주소(10.1.1.2)를 지정합니다.

그림 ***4: Outside1***에 대한 고정 경로 구성




e) 3b단계부터 3d단계까지 반복하여 Outside2에 대한 고정 경로를 구성합니다.

고정 경로에 대해 동일한 메트릭을 지정하지만 다른 게이트웨이를 지정해야 합니다.

그림 ***5: ECMP*** 영역 인터페이스의 구성된 고정 경로


단계 **4** **Save(**저장**)**하고 **Deploy(**구축**)**합니다.

---

대상 R3에 도달하기 위한 네트워크 패킷은 ECMP 알고리즘에 따라 R4>R1>R3 또는 R4>R2>R3를 따릅니다. R1>R3 경로가 손실되면 패킷이 삭제되지 않고 R2를 통해 트래픽이 흐릅니다. 마찬가지로, 패킷이 *Outside1*에서 전송된 경우에도 *Outside2*에서 R3의 응답을 수신할 수 있습니다. 또한 네트워크 트래픽이 많은 경우 R4는이를 두 경로 간에 분산하여 부하를 분산합니다.

# Firepower Threat Defense의 ECMP 히스토리

| 기능 | 버전 | 세부 사항 |
|---|---|---|
| 라우팅 정책으로 ECMP 지원 | 7.1 | Secure Firewall Threat Defense가 FlexConfig 정책을 통해 ECMP 라우팅을 지원하고 있었습니다. 이 릴리스에서는 인터페이스를 트래픽 영역으로 그룹화하고 Secure Firewall Management Center에 ECMP 라우팅을 구성할 수 있습니다.<br>신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **ECMP** |