FMC에서 상관관계 정책 구성

목차

소개

이 문서에서는 이벤트를 연결하고 네트워크에서 이상 징후를 탐지하도록 상관관계 정책을 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)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower Threat Defense 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.

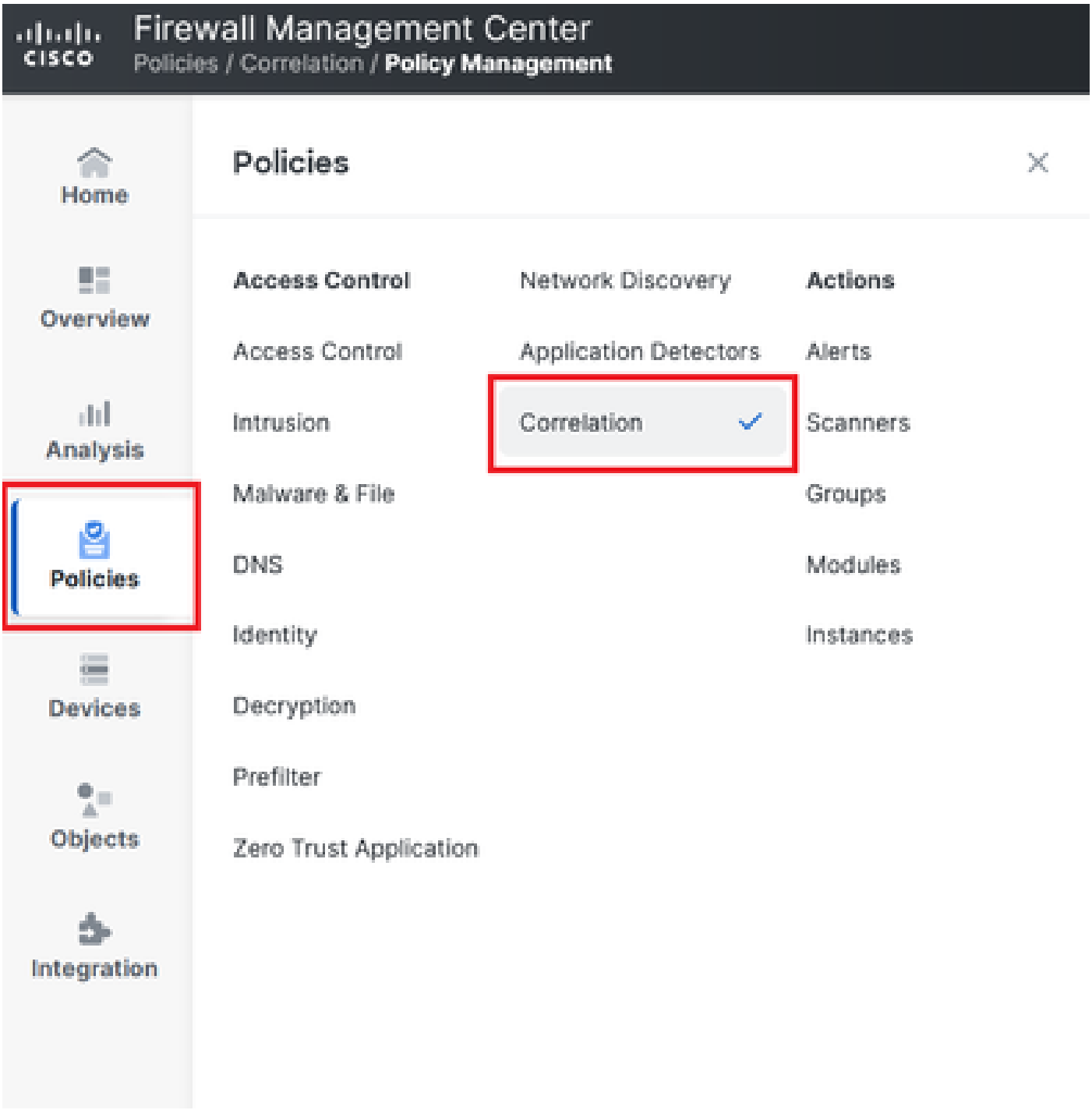
배경 정보

상관관계 정책은 다양한 유형의 이벤트를 구성하여 네트워크에서 잠재적 보안 위협을 식별하는 데 사용되며, 교정, 조건부 경고 및 트래픽 정책에 사용됩니다.

구성

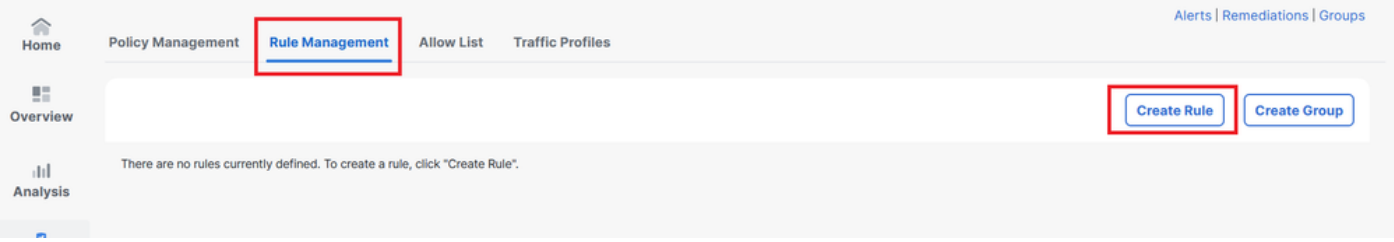
상관관계 규칙 구성

1단계. Policies(정책) > Correlation(상관관계)으로 이동하고 Rule Management(규칙 관리)를 선택합니다.



이미지 1. Correlation Policy(상관관계 정책) 메뉴로 탐색

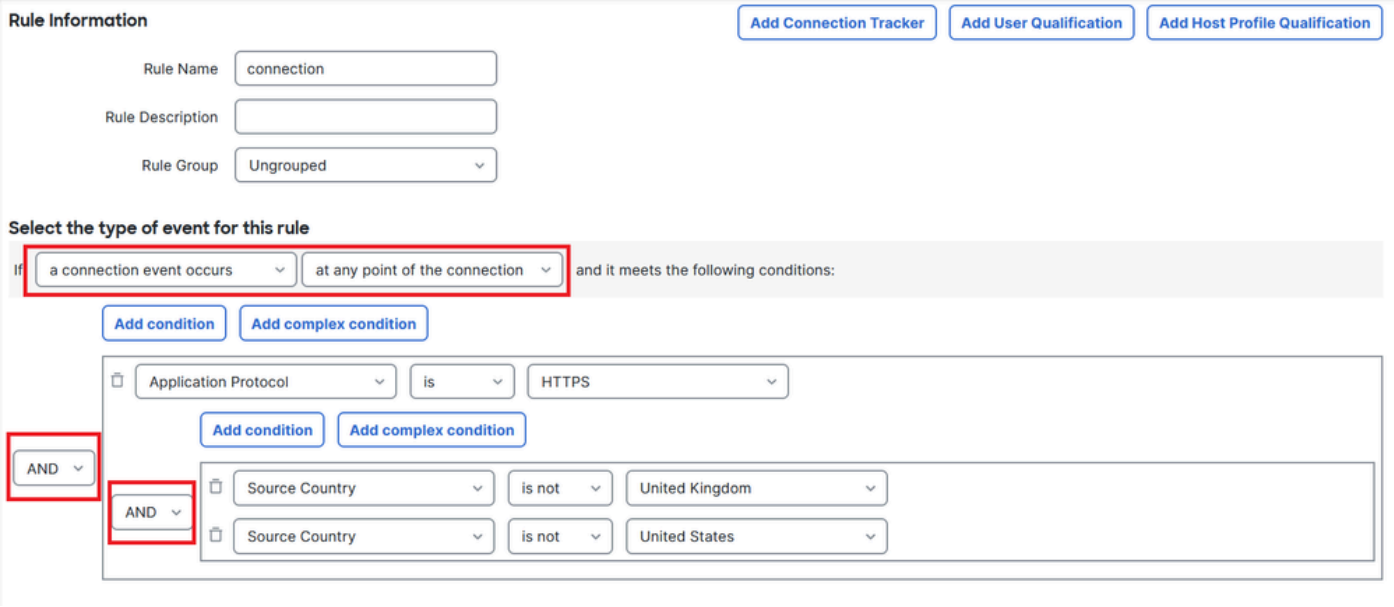
2단계. Create Rule(규칙 생성)을 선택하여 새 규칙을 생성합니다.



이미지 2. Rule Management(규칙 관리) 메뉴의 규칙 생성

3단계. 규칙과 일치시킬 이벤트 유형 및 조건을 선택합니다.

규칙에 여러 조건이 포함된 경우 AND 또는 OR 연산자와 연결해야 합니다.

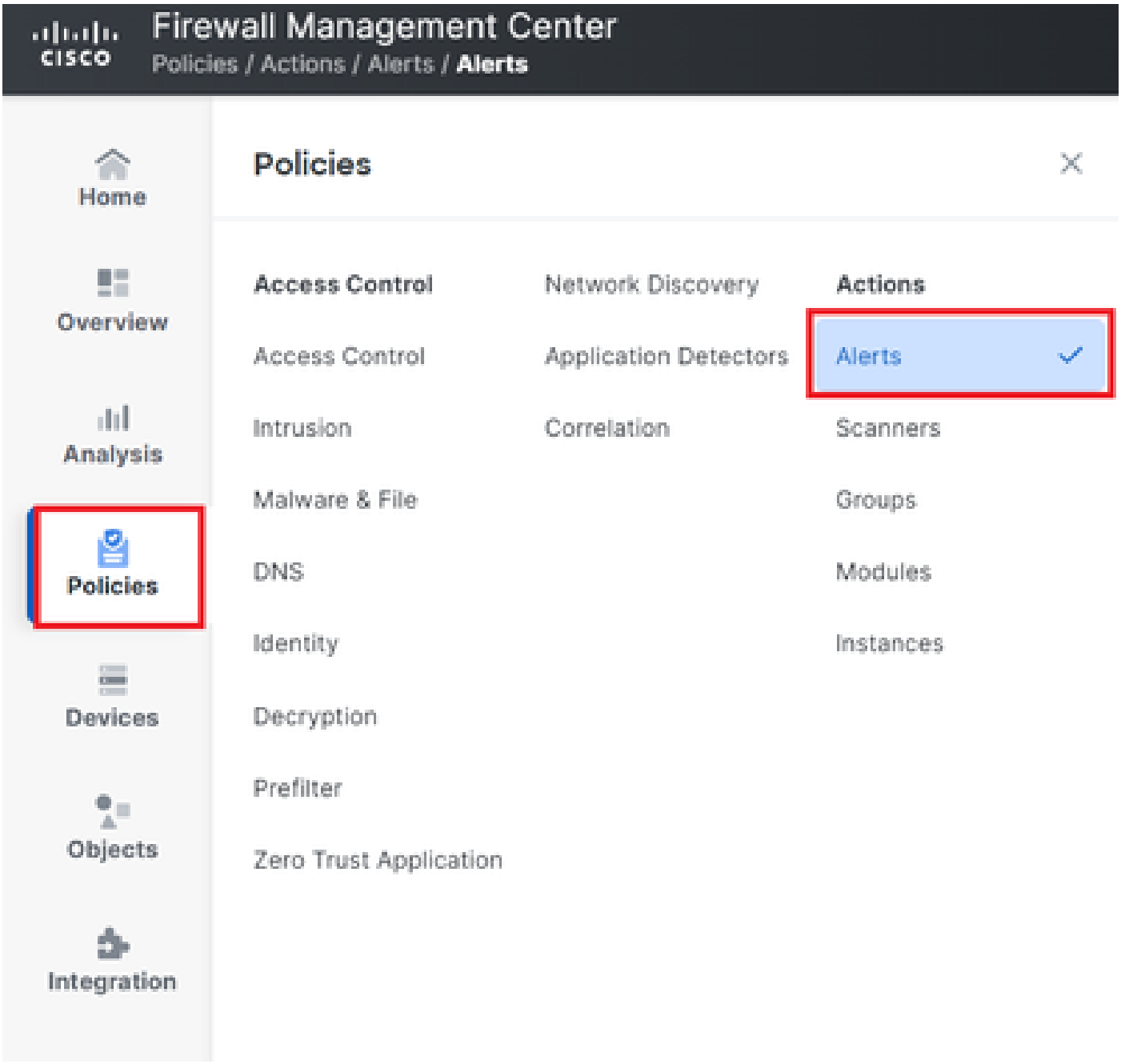


이미지 3. 규칙 생성 메뉴

참고: 상관관계 규칙은 일반적이지 않아야 하며, 규칙이 일반 트래픽에 의해 지속적으로 트리거되면 추가 CPU가 소모되고 FMC 성능에 영향을 줄 수 있습니다.

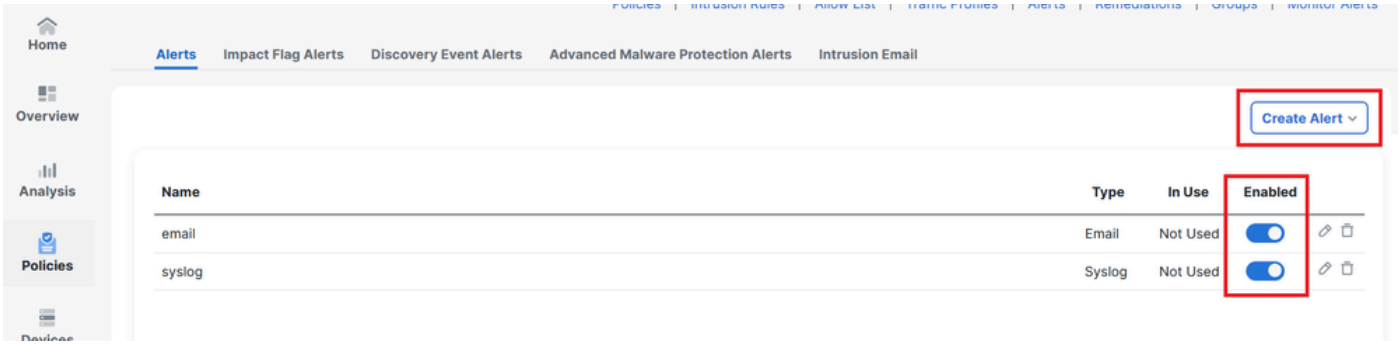
알림 구성

1단계. Policies > Actions > Alerts로 이동합니다.



이미지 4. Alerts(경고) 메뉴로 탐색

2단계. Create Alert(경고 생성)를 선택하고 Syslog, SNMP 또는 이메일 경고를 생성합니다.

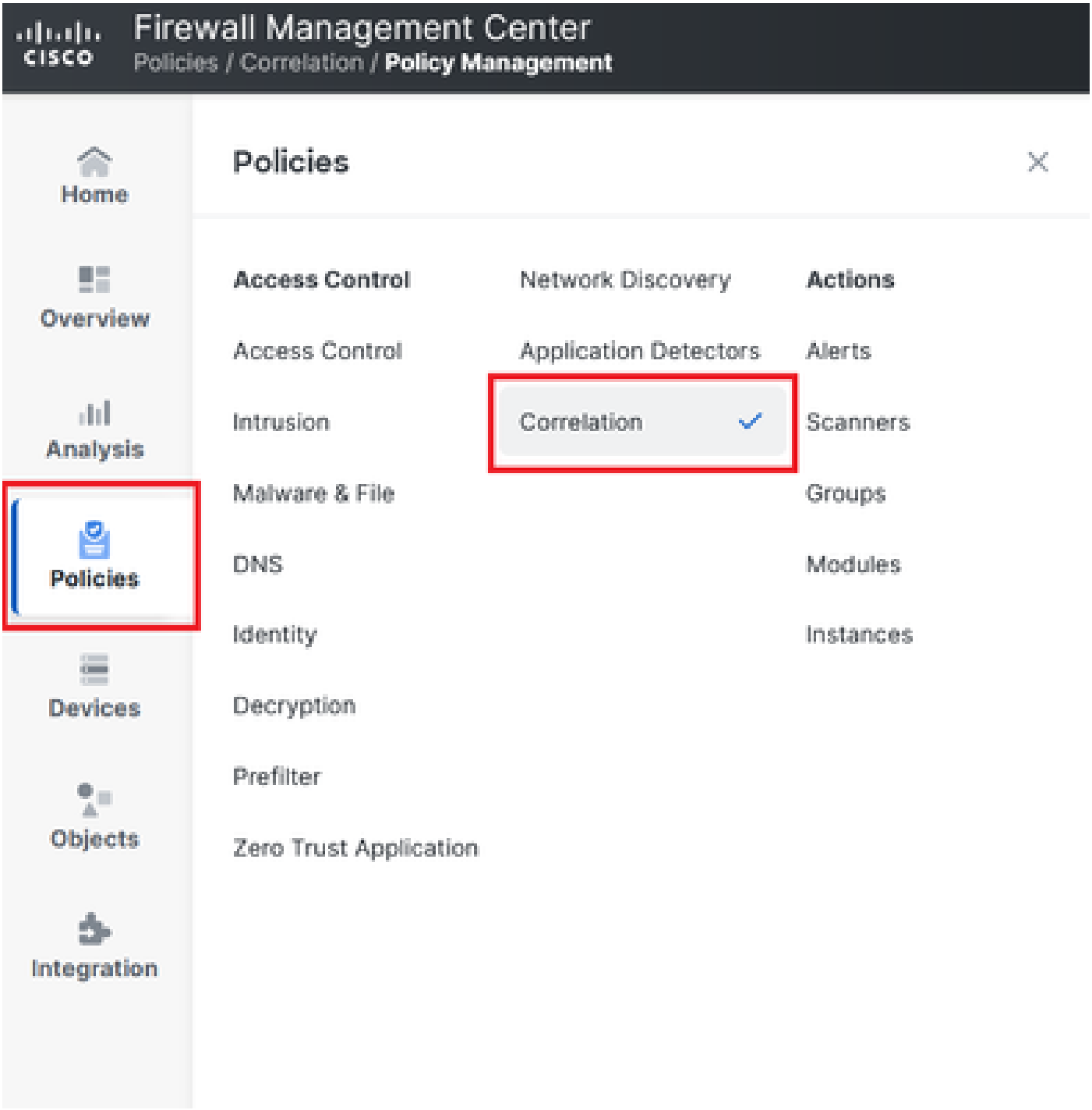


이미지 5. 경고 생성

3단계. 알림이 활성화되었는지 확인합니다.

상관관계 정책 구성

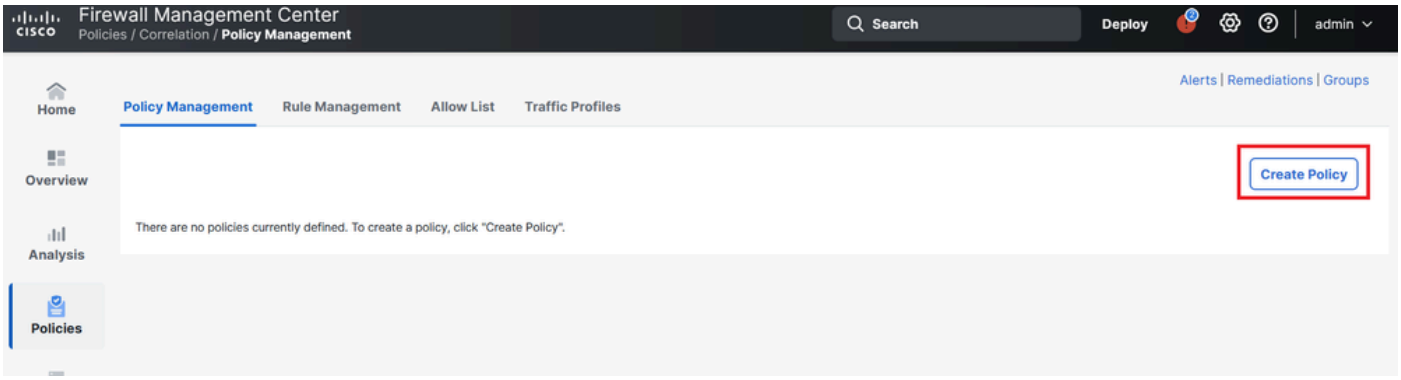
1단계. Policies > Correlation으로 이동합니다.



Correlation Policy(상관관계 정책) 메뉴로 탐색

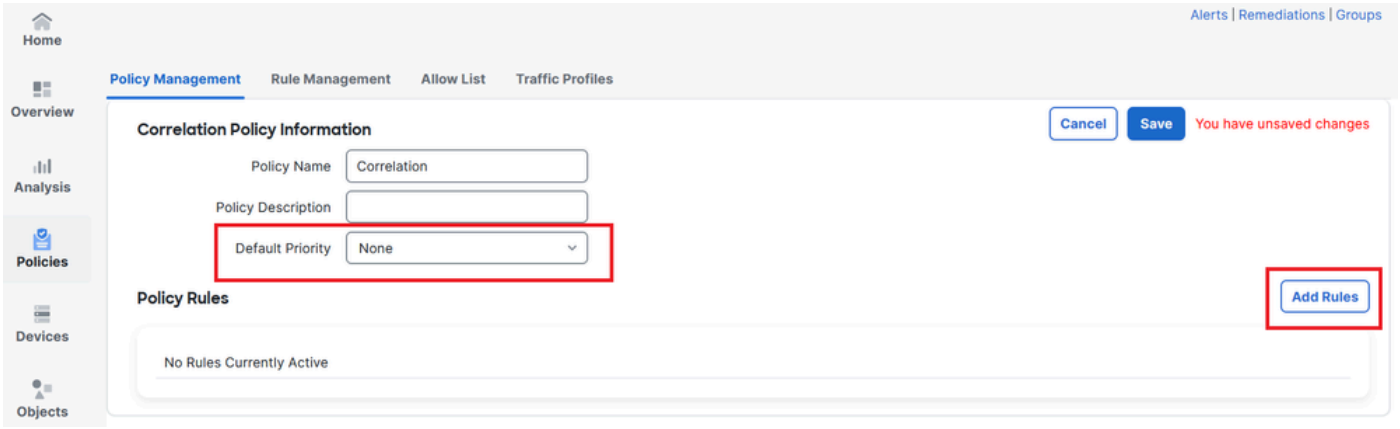
이미지 6. Correlation Policy(상관관계 정책) 메뉴로 탐색

2단계. 새 상관관계 정책을 생성합니다. 기본 우선 순위를 선택합니다. 특정 규칙의 우선 순위를 사용하려면 None을 사용합니다.

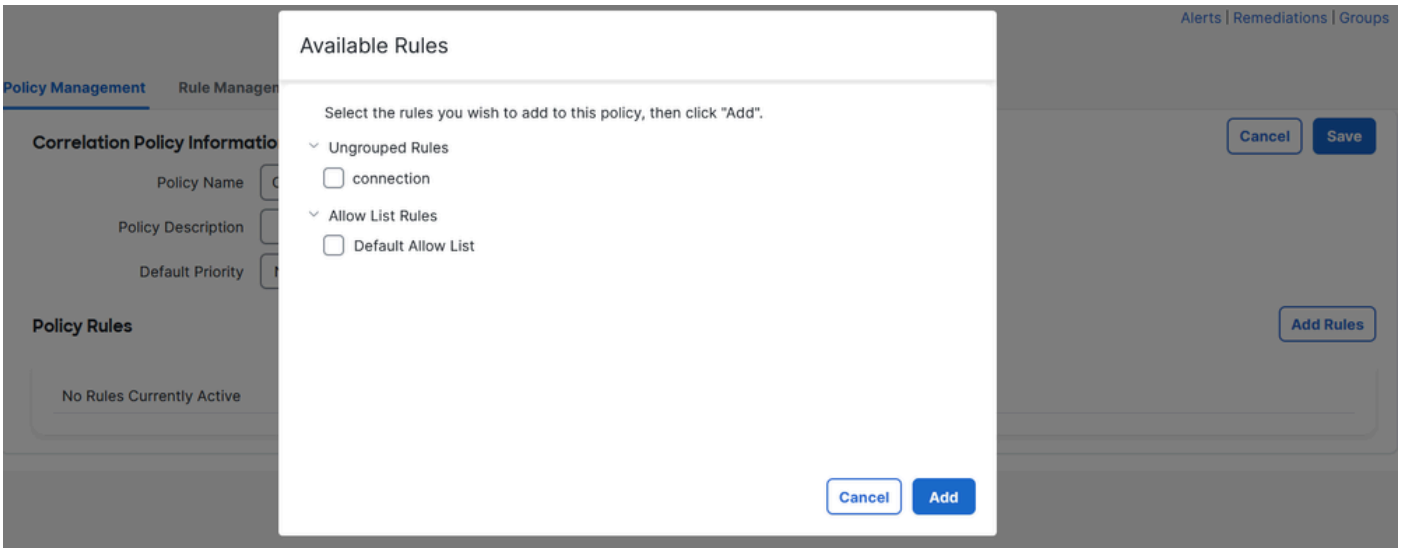


이미지 7. 새 상관관계 정책 생성

3단계. Add Rules(규칙 추가)를 선택하여 정책에 규칙을 추가합니다.

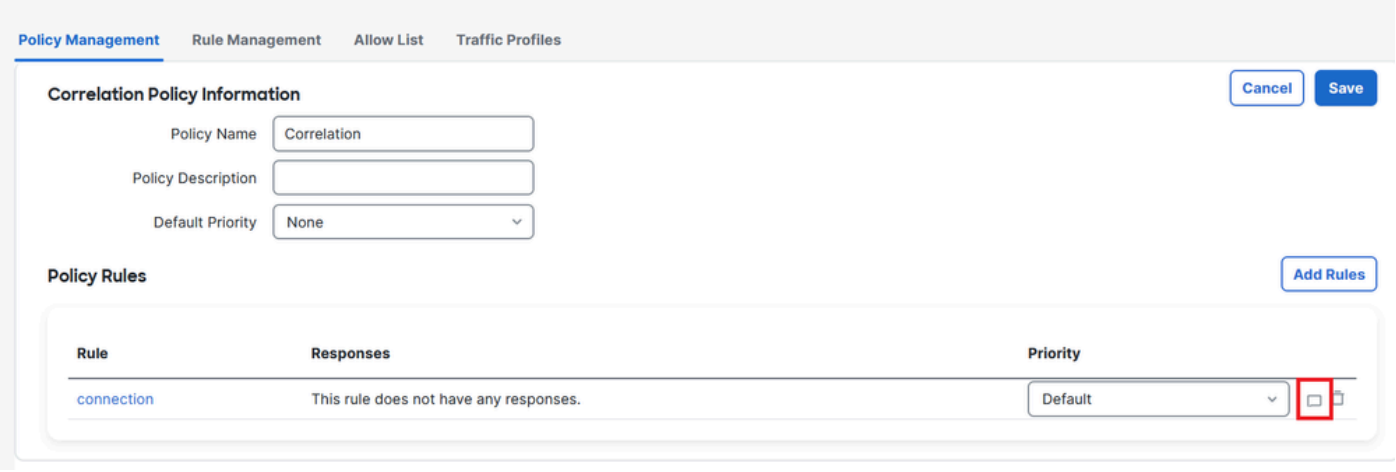


이미지 8. 규칙 추가 및 상관관계 정책의 우선순위 선택

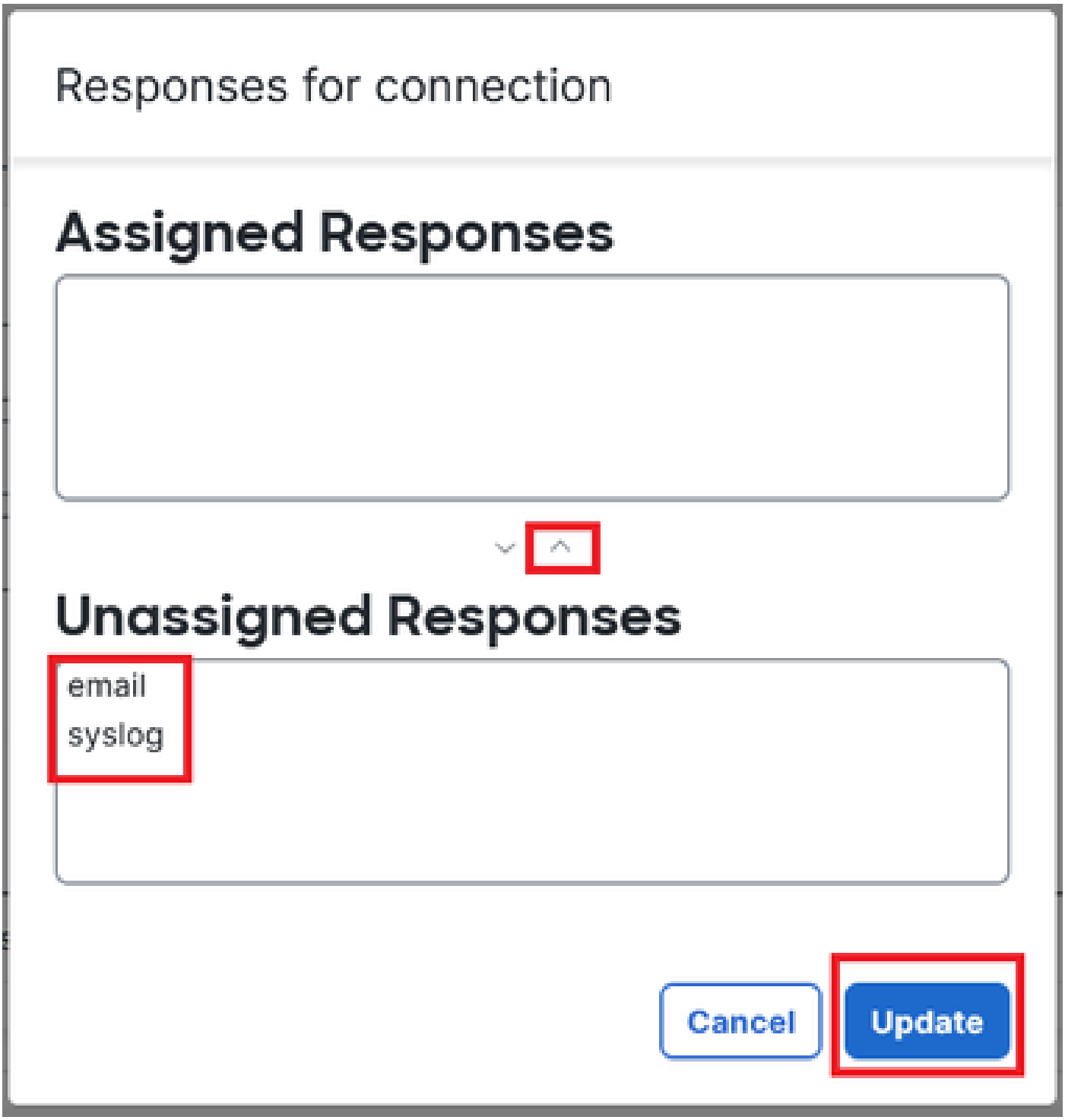


이미지 9. 상관관계 정책에 추가할 규칙 선택

4단계. 생성한 알림에서 규칙에 응답을 할당하여 트리거될 때마다 선택한 알림 유형을 전송합니다.

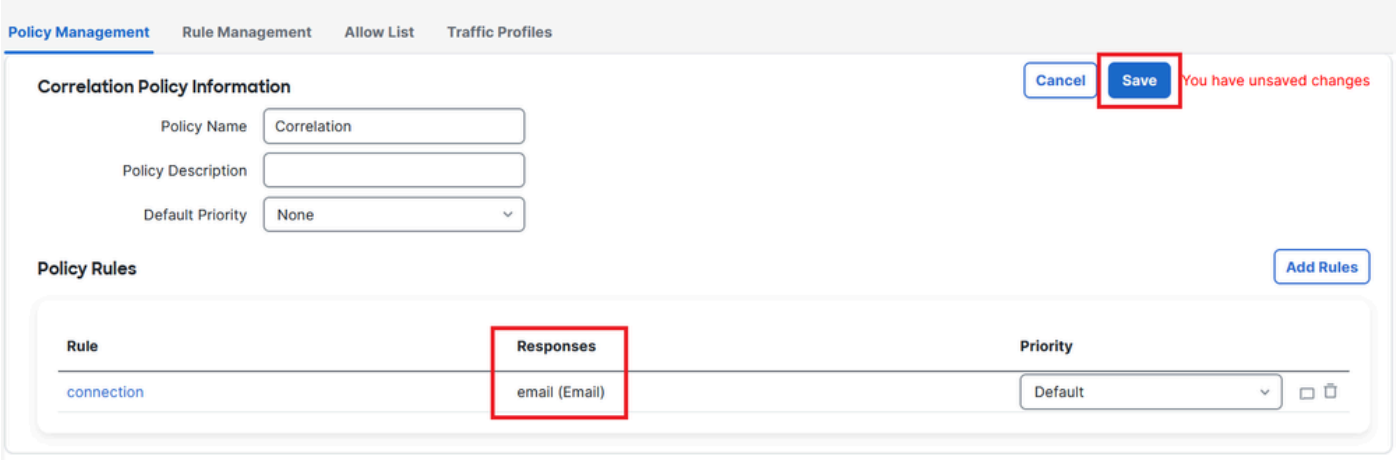


이미지 10. 응답 추가 단추



이미지 11. 상관관계 규칙에 응답 할당

5단계. 상관관계 정책을 저장하고 활성화합니다.



이미지 12. 상관관계 규칙에 올바르게 추가된 응답

이미지 13. 상관관계 정책 사용

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.