FMC GUI에서 Unified Event Viewer를 사용하여 이벤트 모니터링

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

탐색

- Unified Event 페이지의 예

이벤트 검토

열 맞춤 설정

- 열 세트 저장

이벤트 검색

- 검색 저장

타임 윈도우

- 라이브

CSV(쉼표로 구분된 값)로 이벤트 다운로드

관련 정보

소개

이 문서에서는 FMC(Firewall Management Center)의 GUI(그래픽 사용자 인터페이스)에서 Unified Event Viewer를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 관리자 또는 보안 분석가 권한으로 FMC에 액세스
- 버전 v7.0 이상의 FMC

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Secure Firewall Management Center for VMware v7.2.5

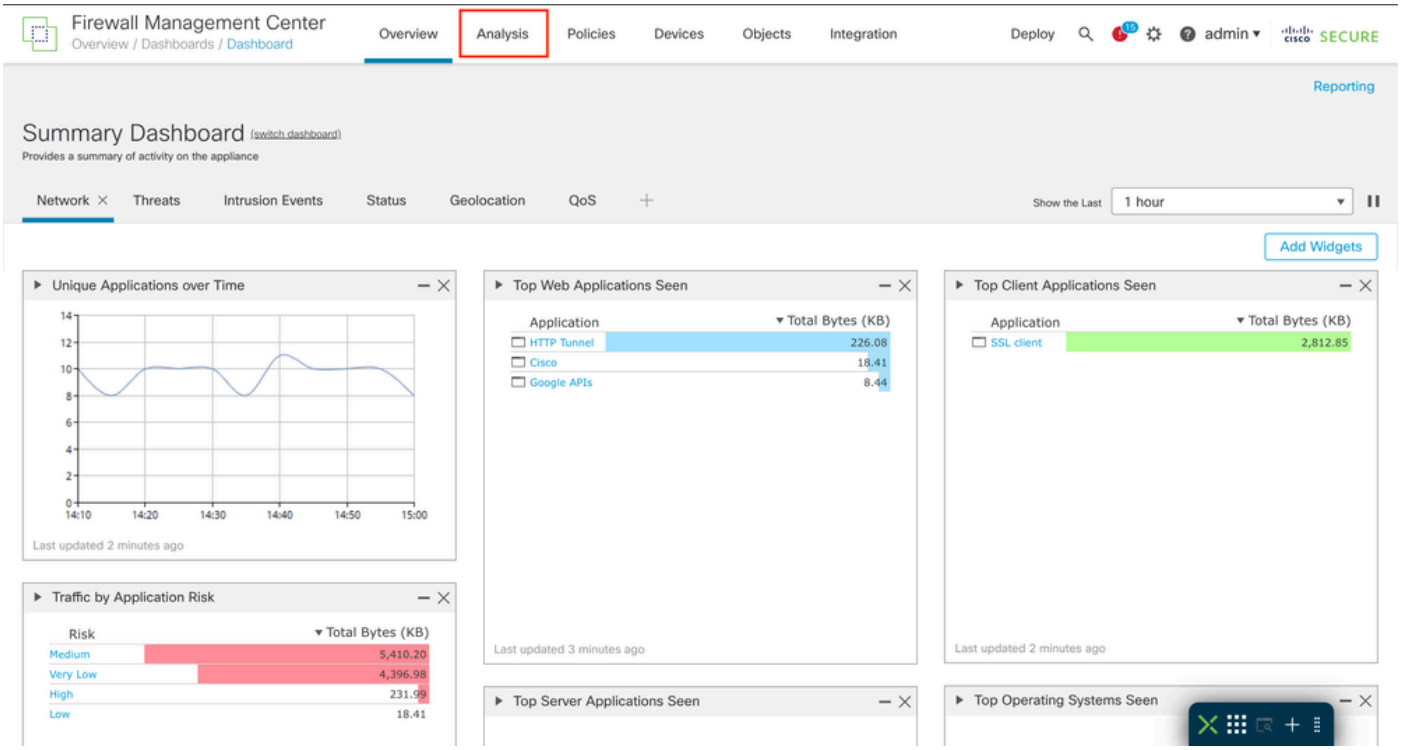
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

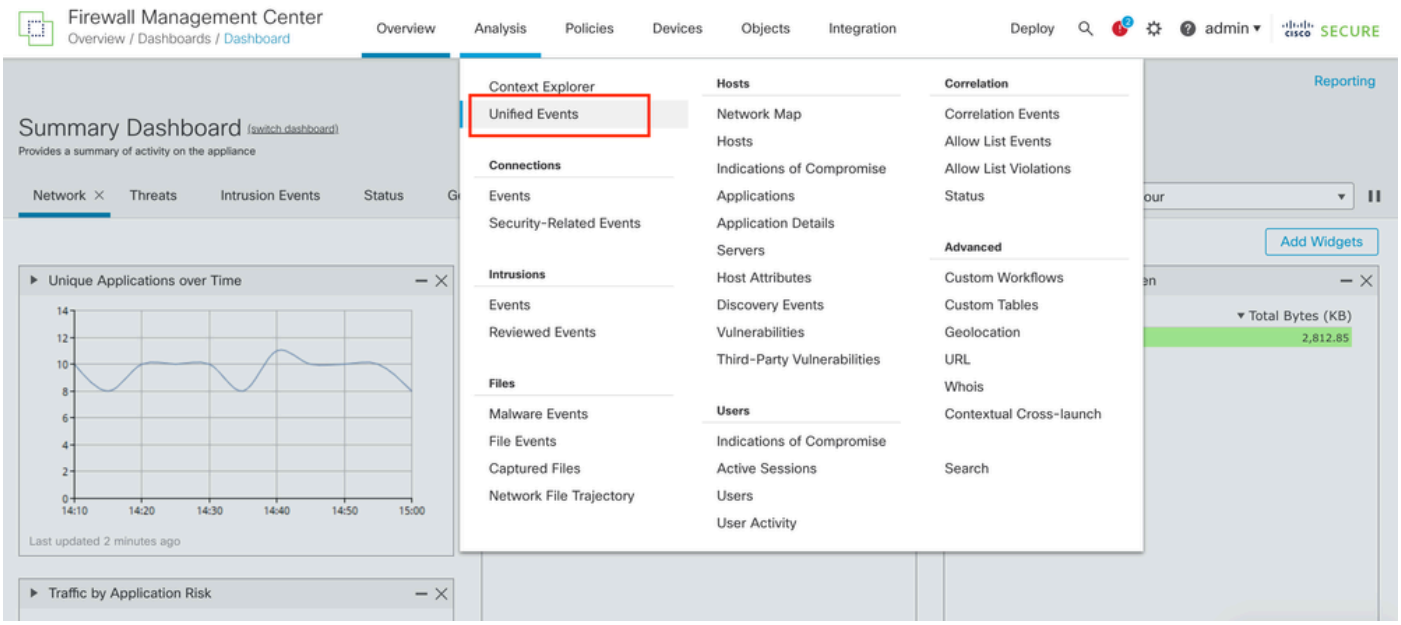
탐색

1단계. FMC GUI에 로그인합니다.

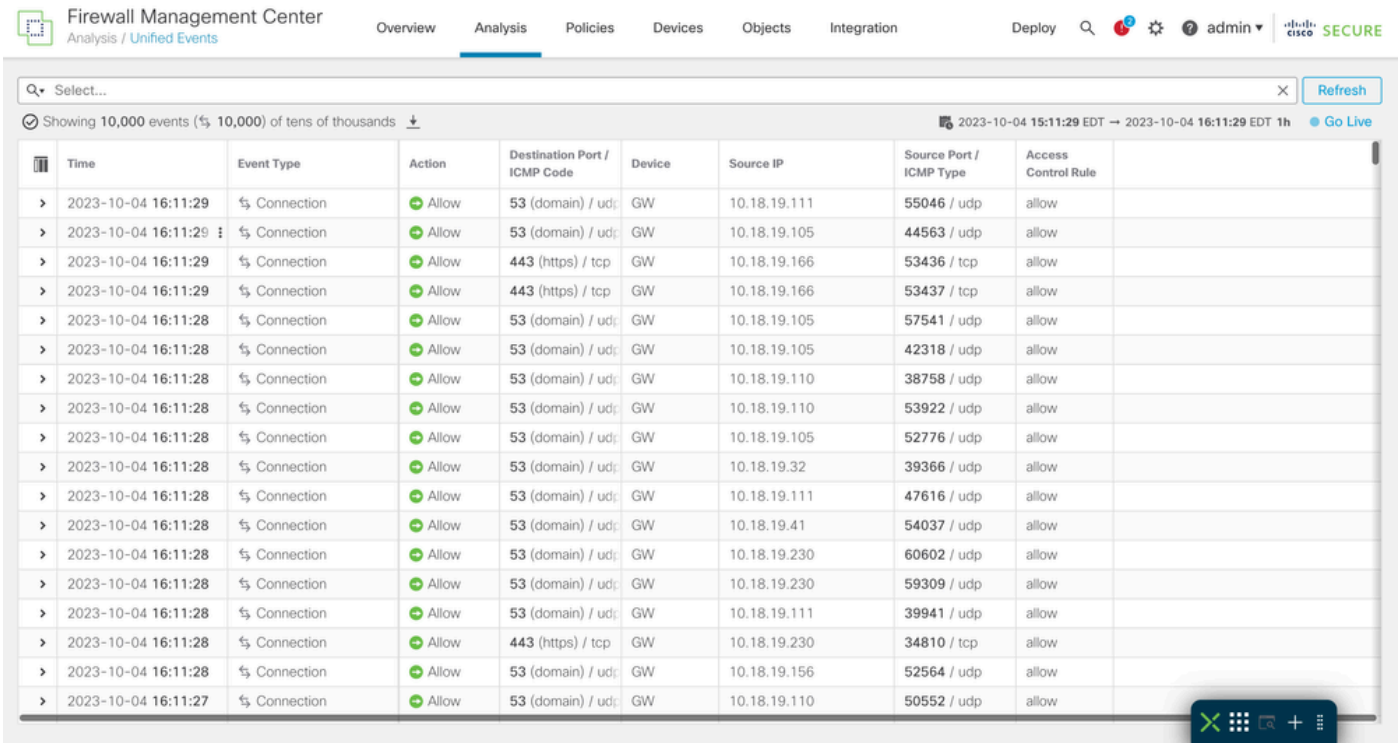
2단계. 분석 탭으로 이동합니다.



3단계. 드롭다운 메뉴에서 Unified Events를 클릭합니다.

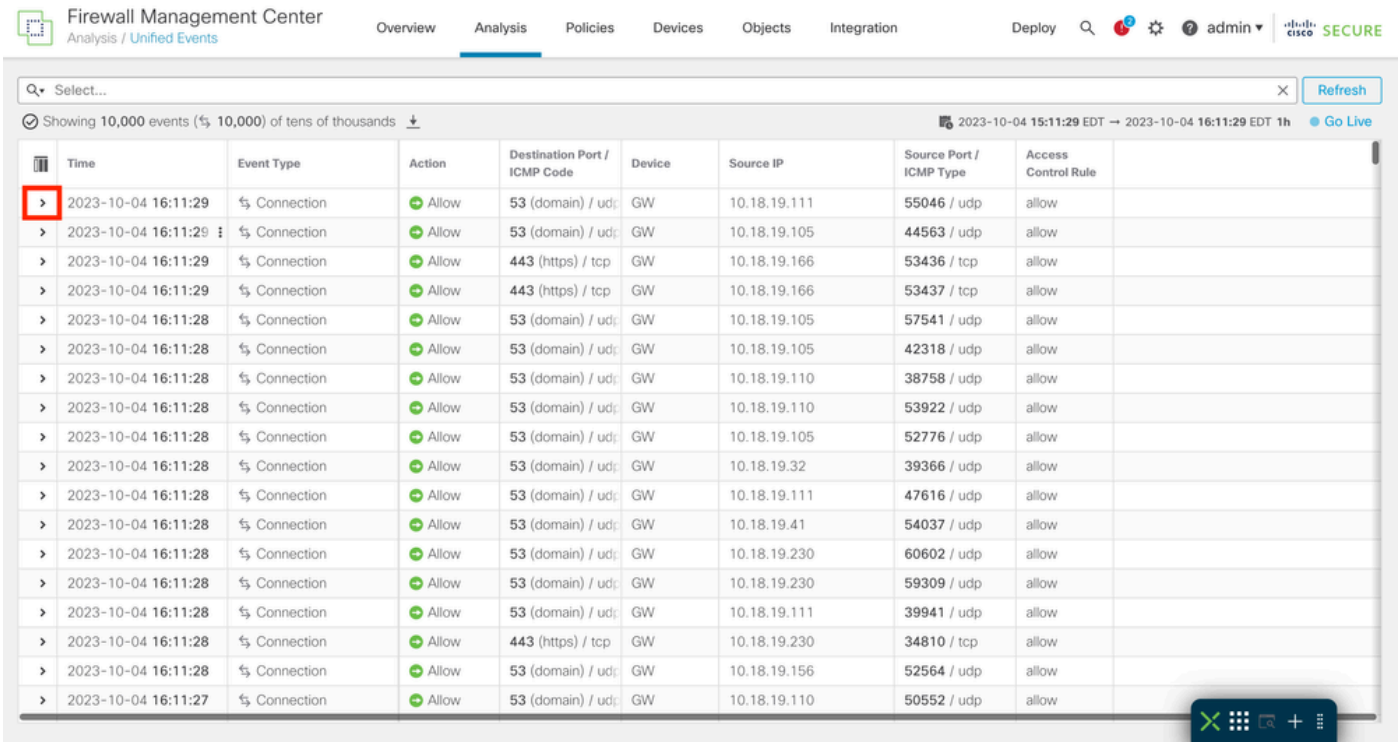


Unified Event 페이지의 예

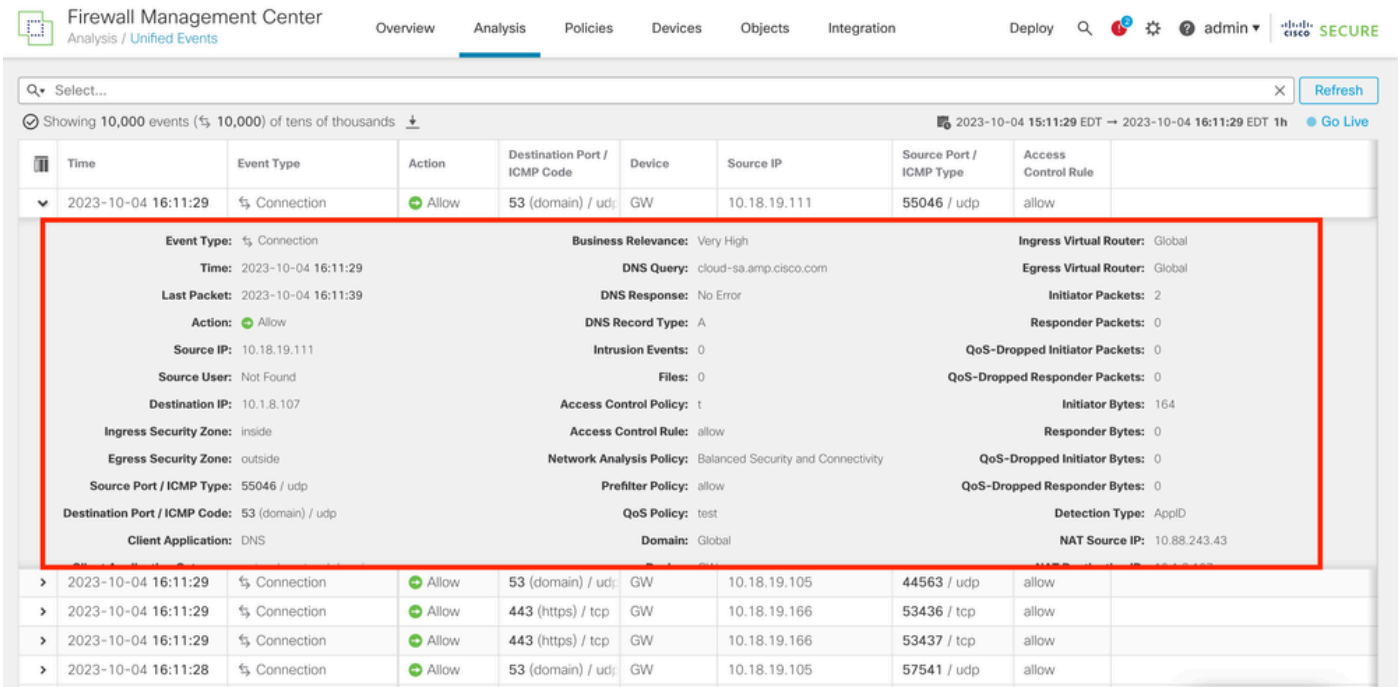


이벤트 검토

1단계. > 아이콘을 클릭합니다.

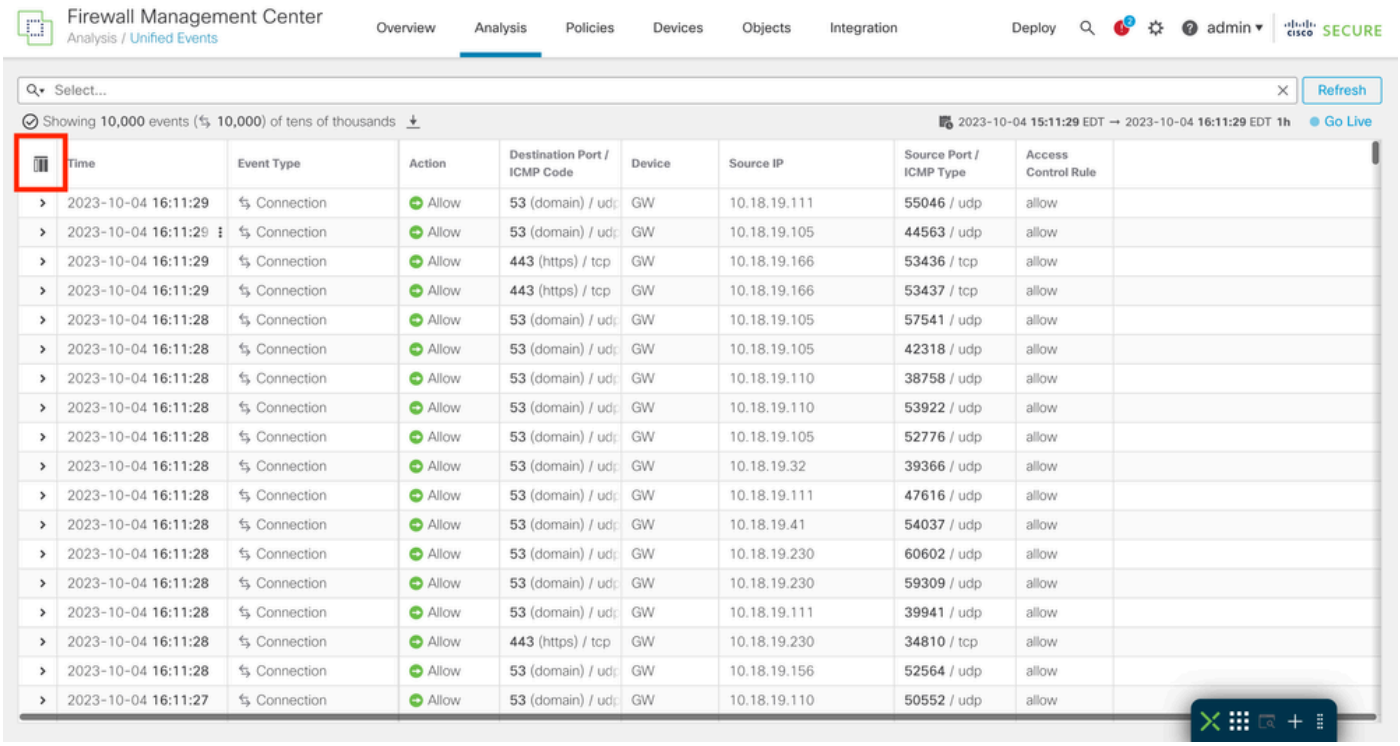


2단계. 이벤트의 세부 정보가 표시됩니다.

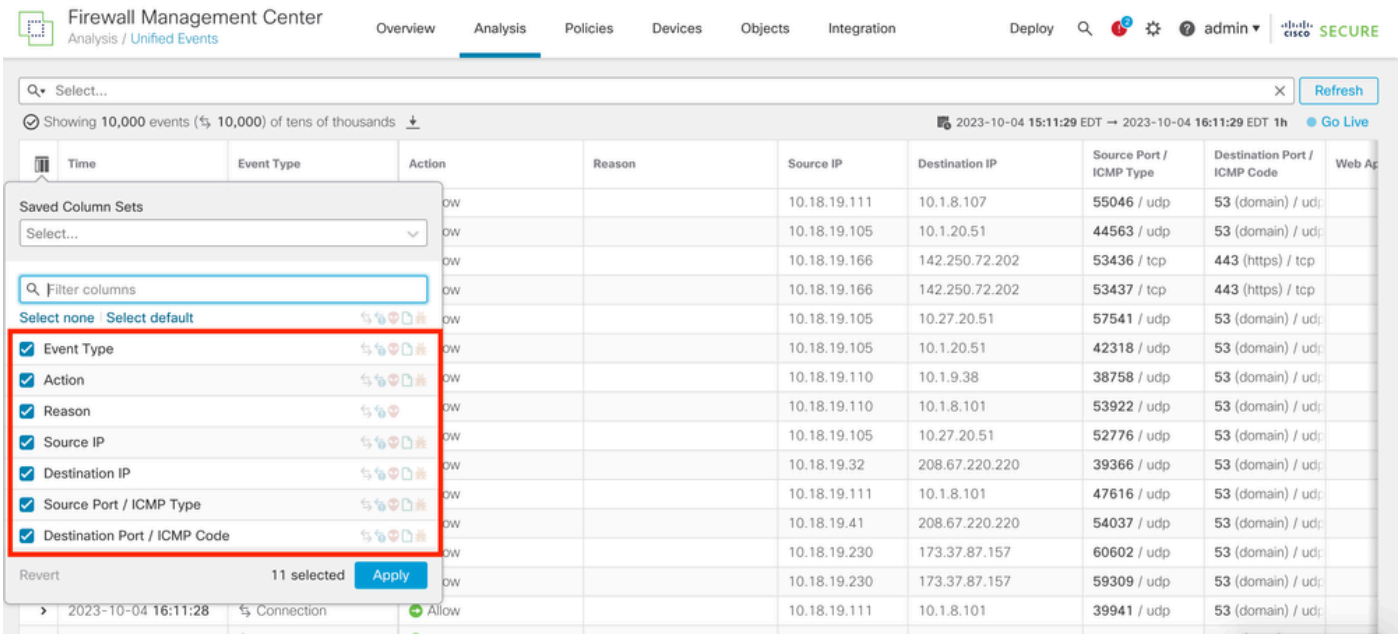


열 맞춤 설정

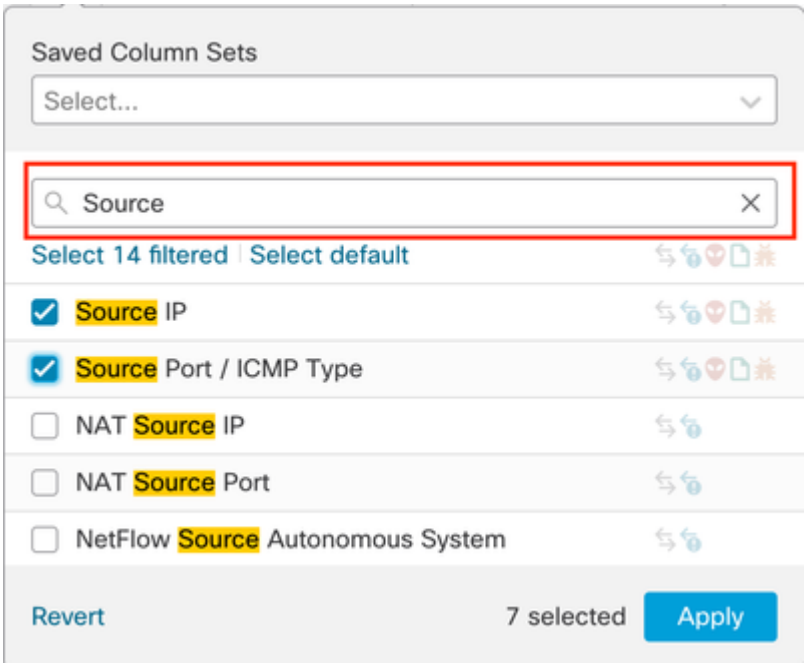
1단계. 아이콘을 클릭합니다. .



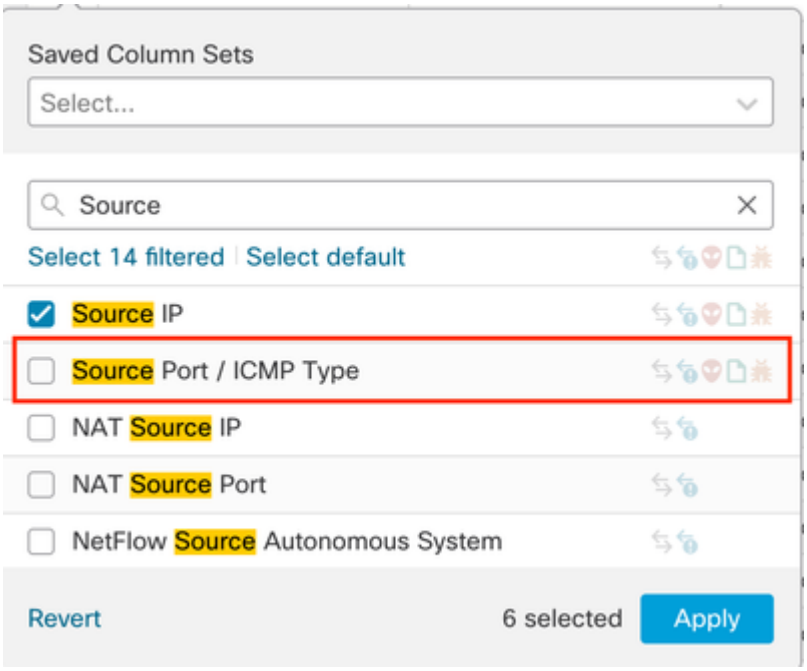
2단계. 테이블에서 원하는 이벤트 필드를 선택합니다.



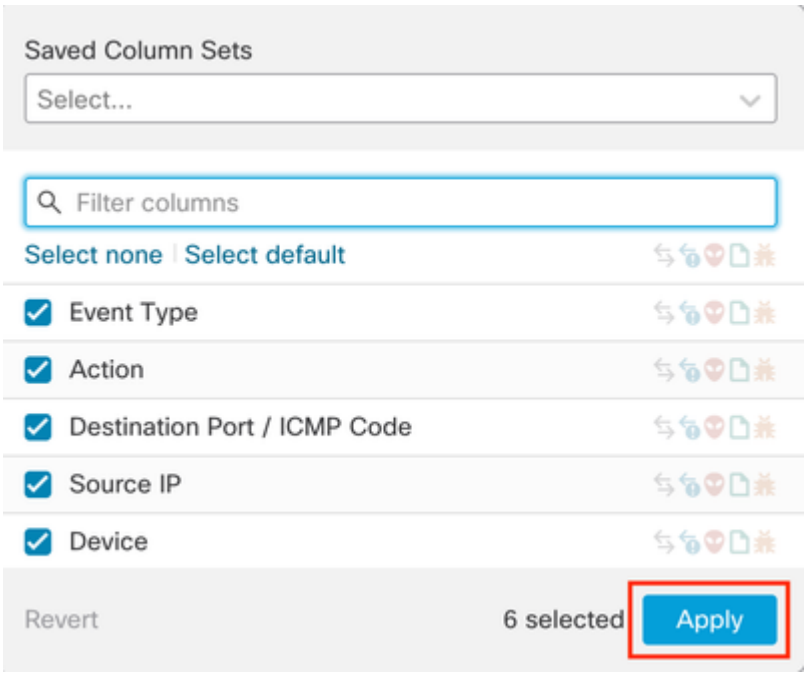
3단계. (선택 사항) 더 쉽게 탐색할 수 있도록 필드를 검색합니다.



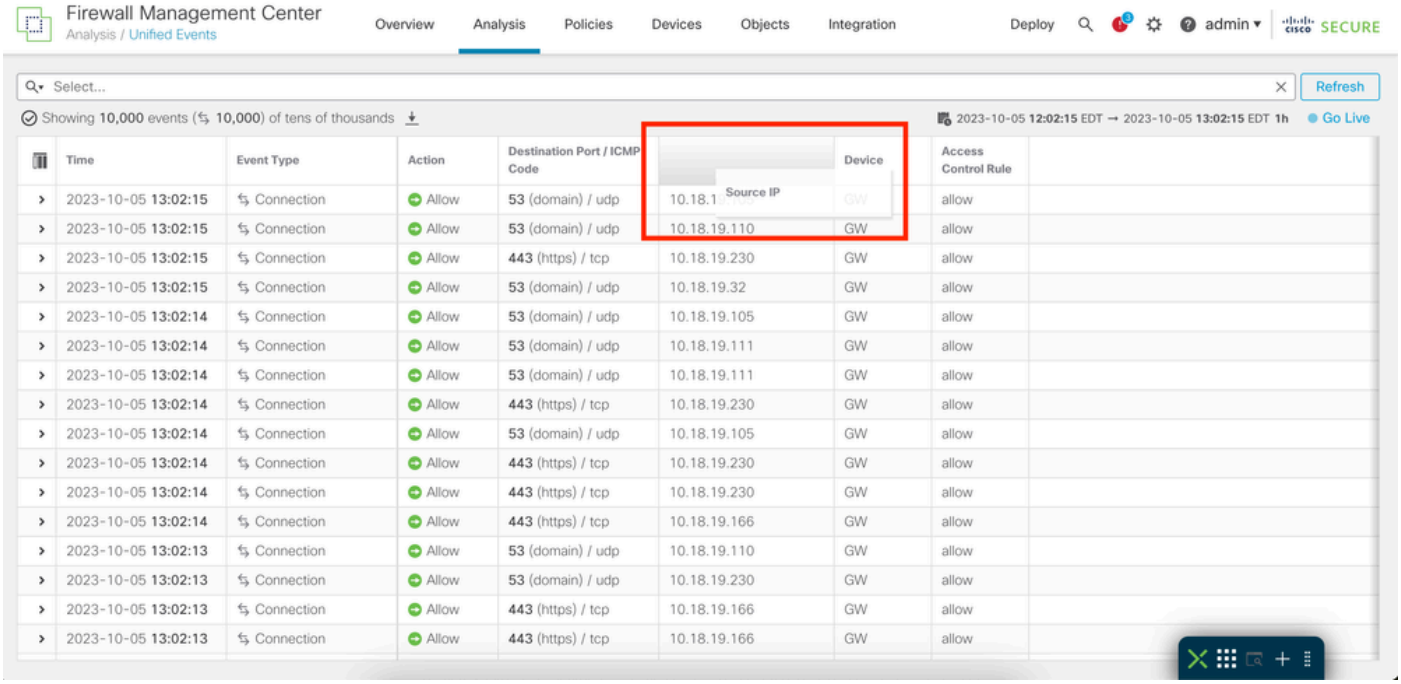
4단계. 비활성화하거나 활성화하려면 이벤트 필드를 클릭합니다.



5단계. Apply(적용)를 클릭합니다.

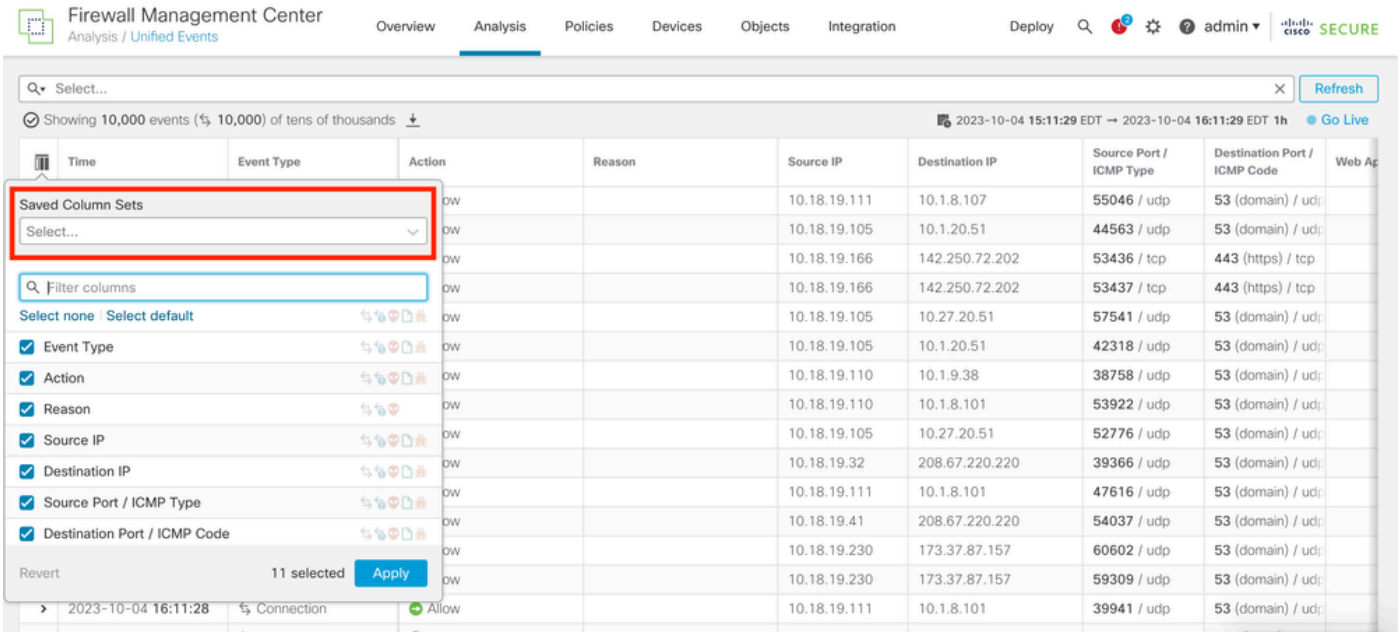


6단계(선택 사항) 각 열을 다른 위치로 끌어 열 위치를 변경할 수 있습니다.

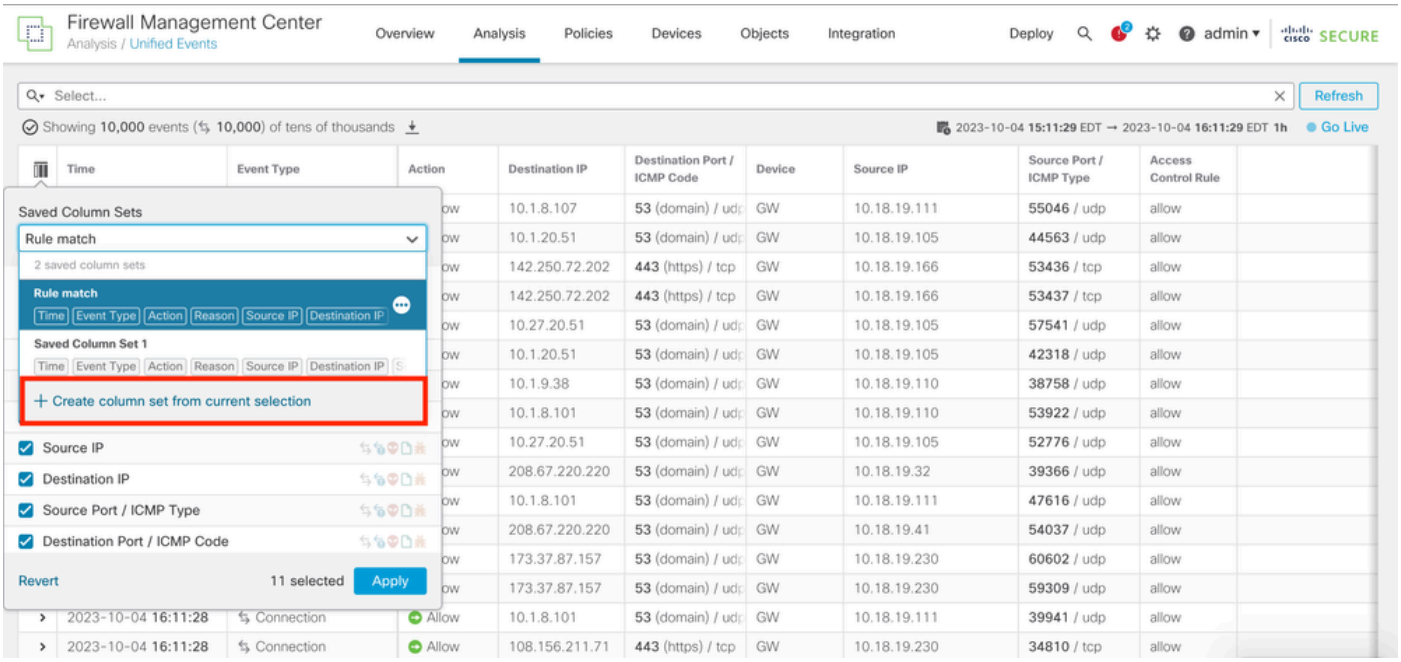


열 세트 저장

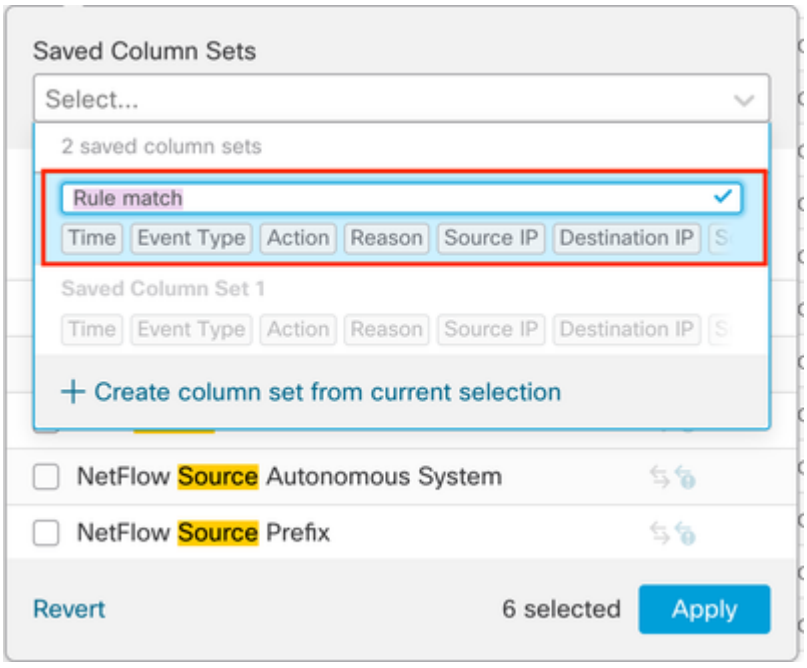
1단계. Saved Column Sets(저장된 열 세트)를 클릭합니다.



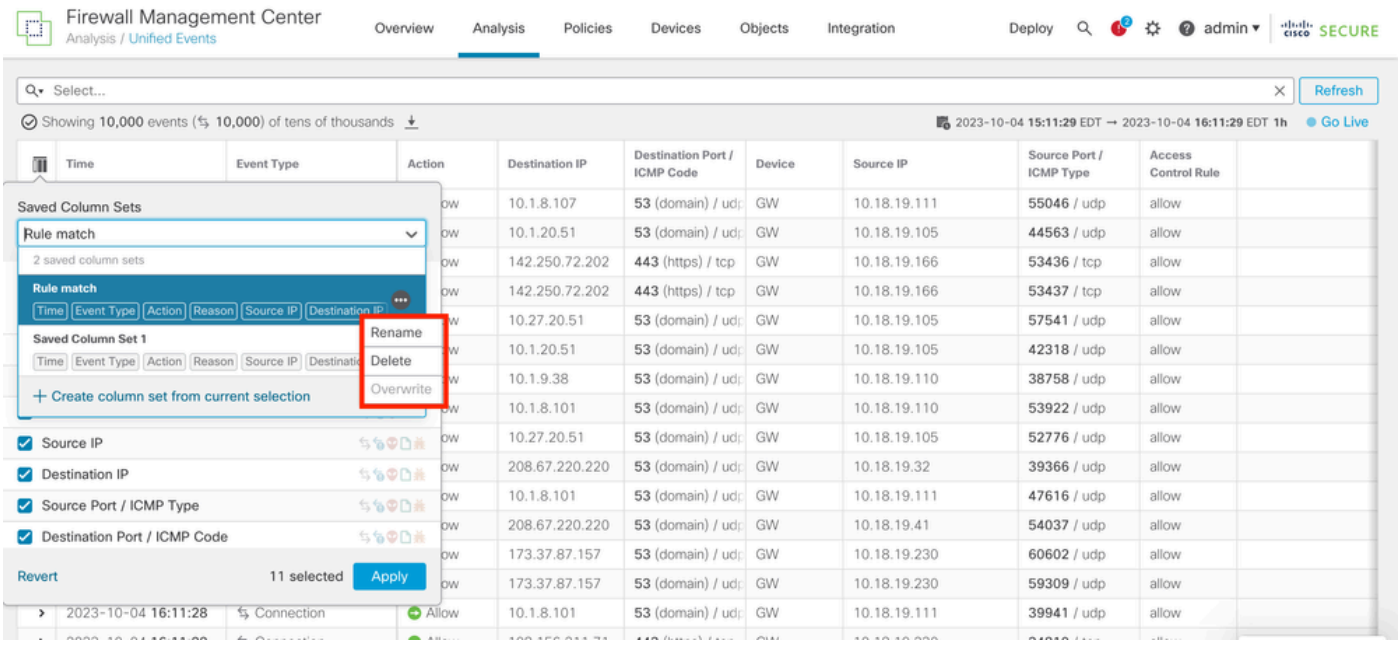
2단계. 현재 선택에서 열 세트 생성을 클릭합니다.



3단계. (선택사항) 열 세트의 이름을 변경합니다.

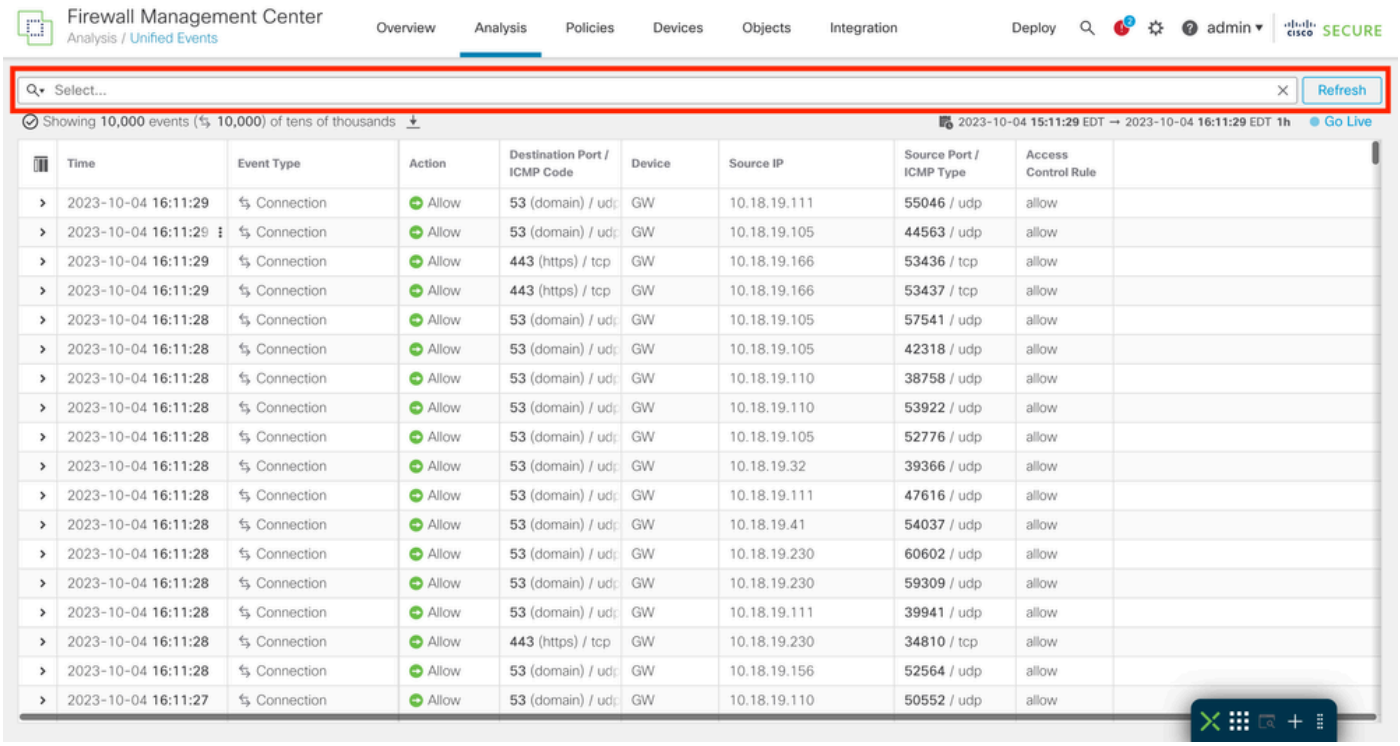


4단계. 생략 부호(...)를 클릭하여 기존 집합을 편집할 수 있습니다.

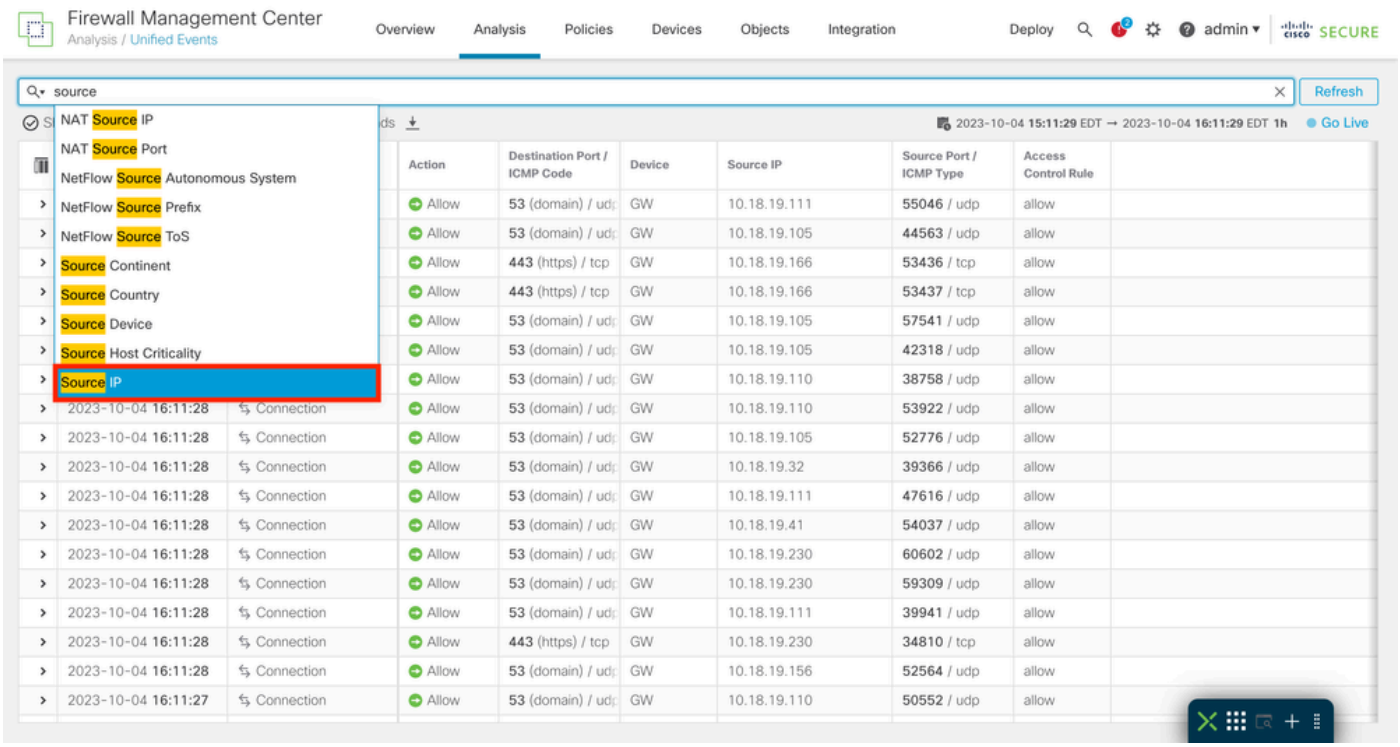


이벤트 검색

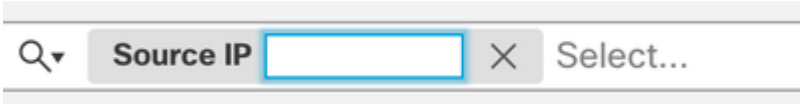
1단계. 특정 이벤트 검색을 시작하려면 Select(선택)를 클릭합니다.



2단계. 필터를 적용할 필드를 선택합니다.

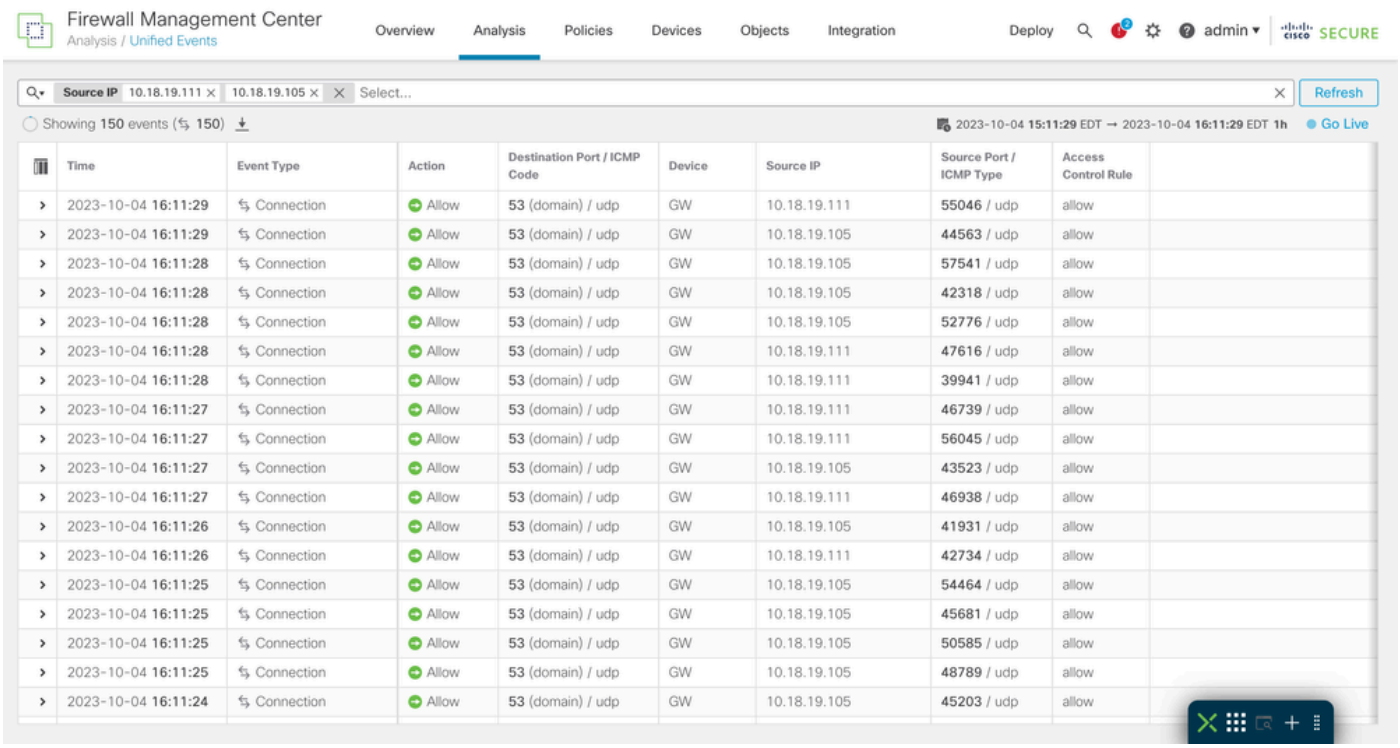


3단계. 필터로 사용할 값을 작성합니다.

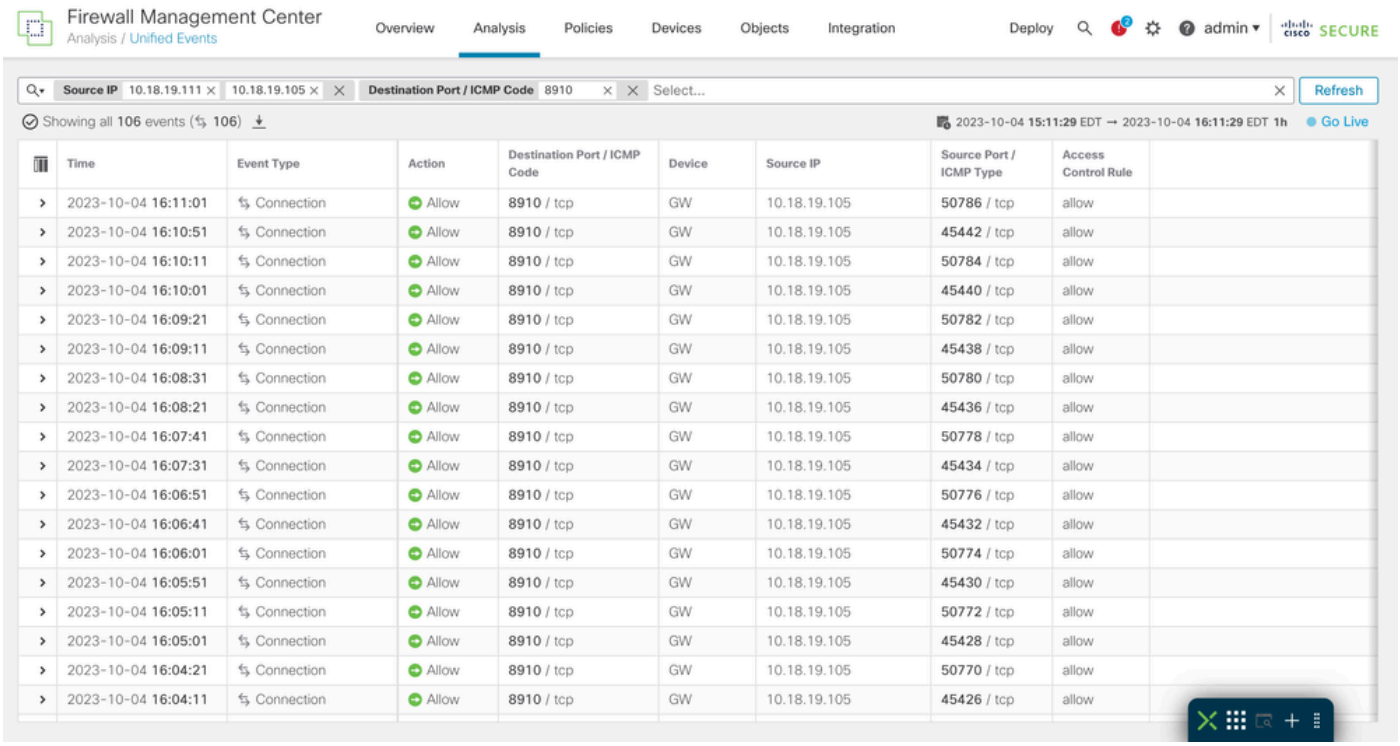


4단계. Apply(적용)를 클릭하여 필터를 구성합니다.

5단계. (선택 사항) 각 필터에 여러 값을 추가할 수 있습니다.



6단계. (선택 사항) 필요한 만큼 필터를 추가합니다.

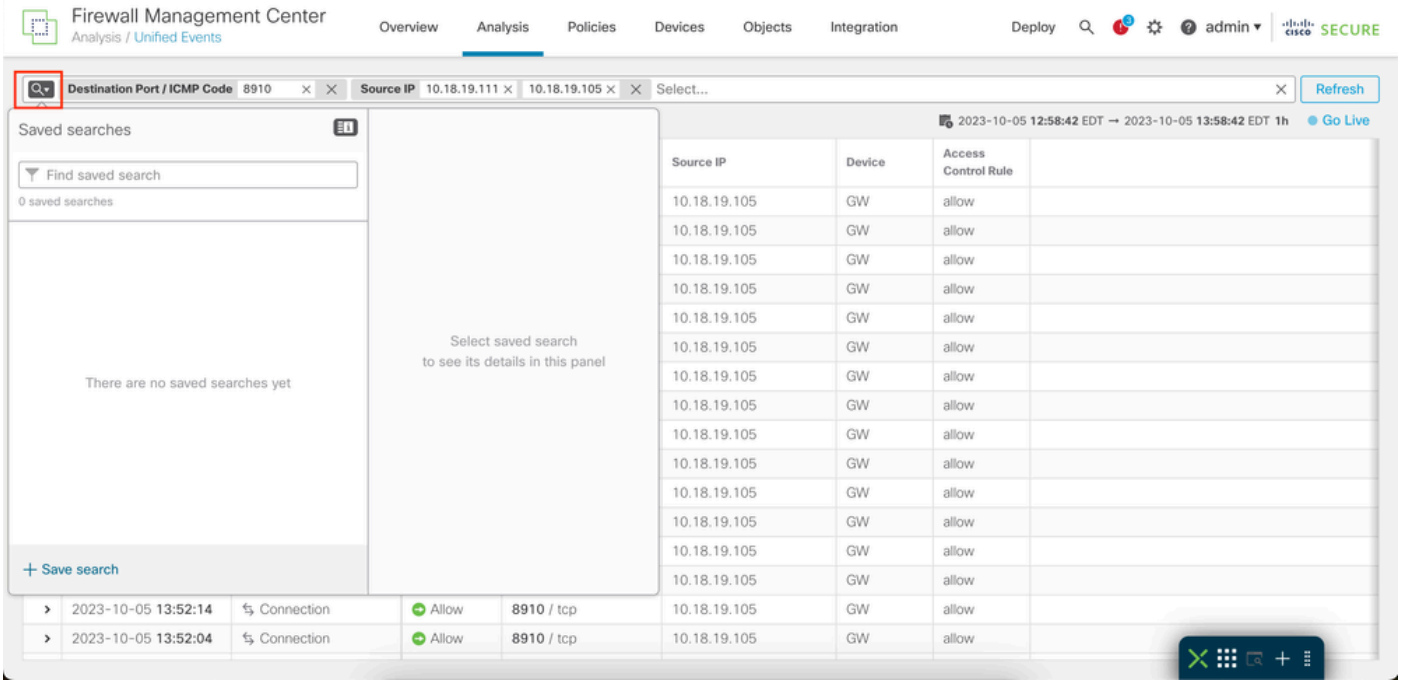


팁: 값을 쓰는 동안 연산자(>,<, ! 등)를 사용할 수 있습니다.

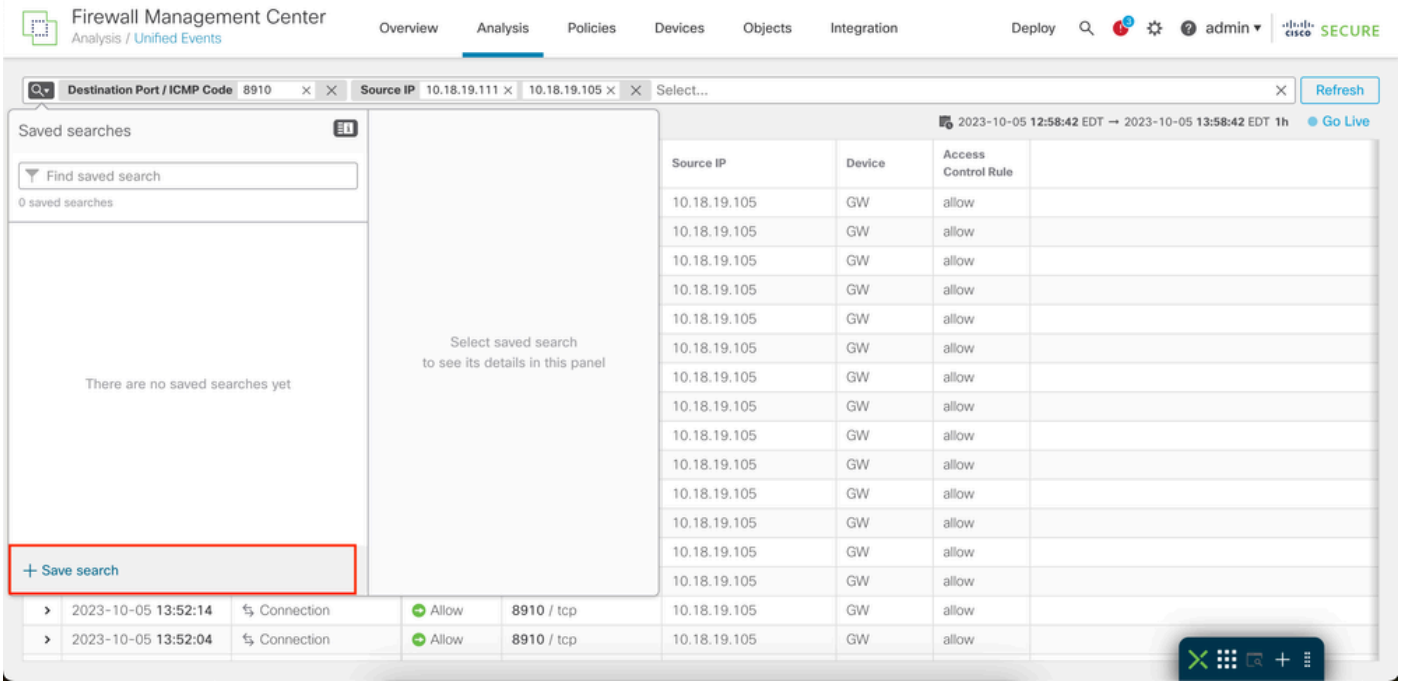
검색 저장

생성한 필터를 다시 사용할 수 있도록 검색을 저장할 수 있습니다.

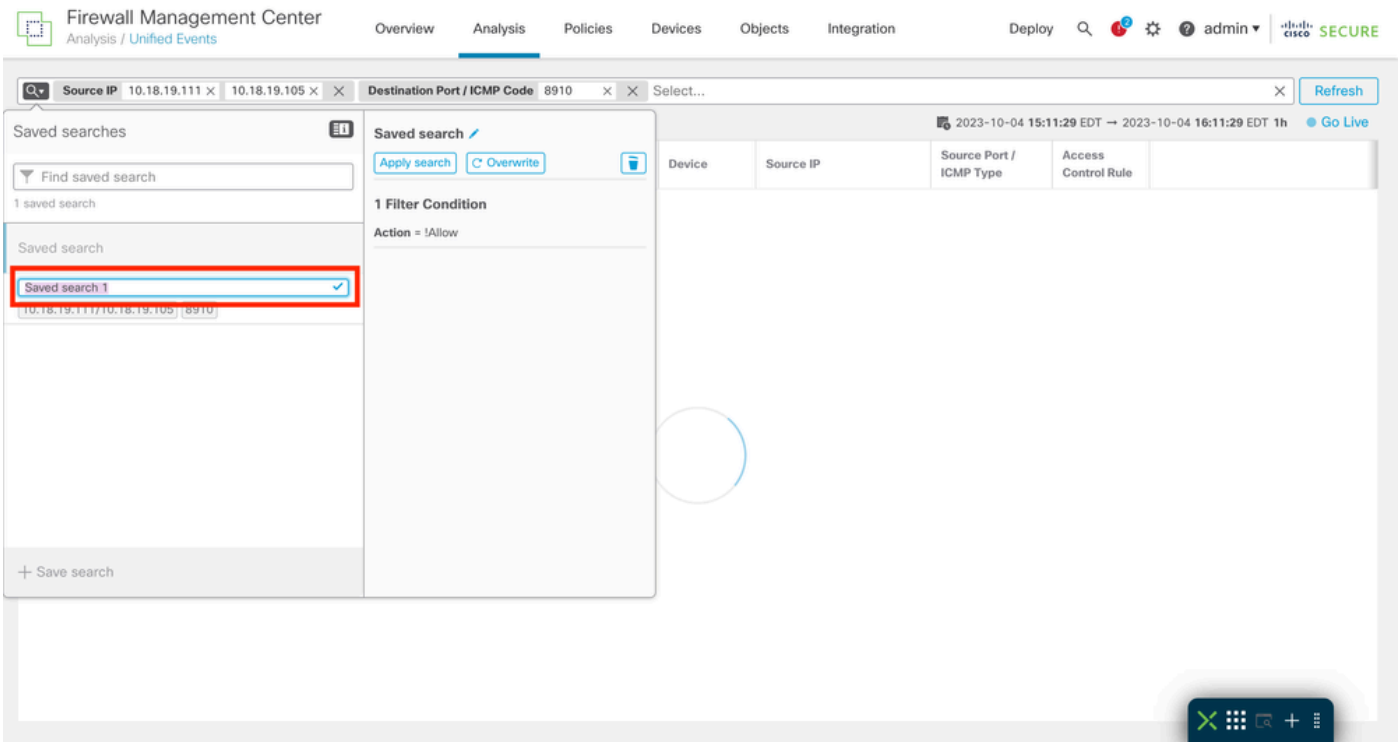
1단계. 돋보기 아이콘을 클릭합니다.



2단계. 검색 저장을 클릭합니다.



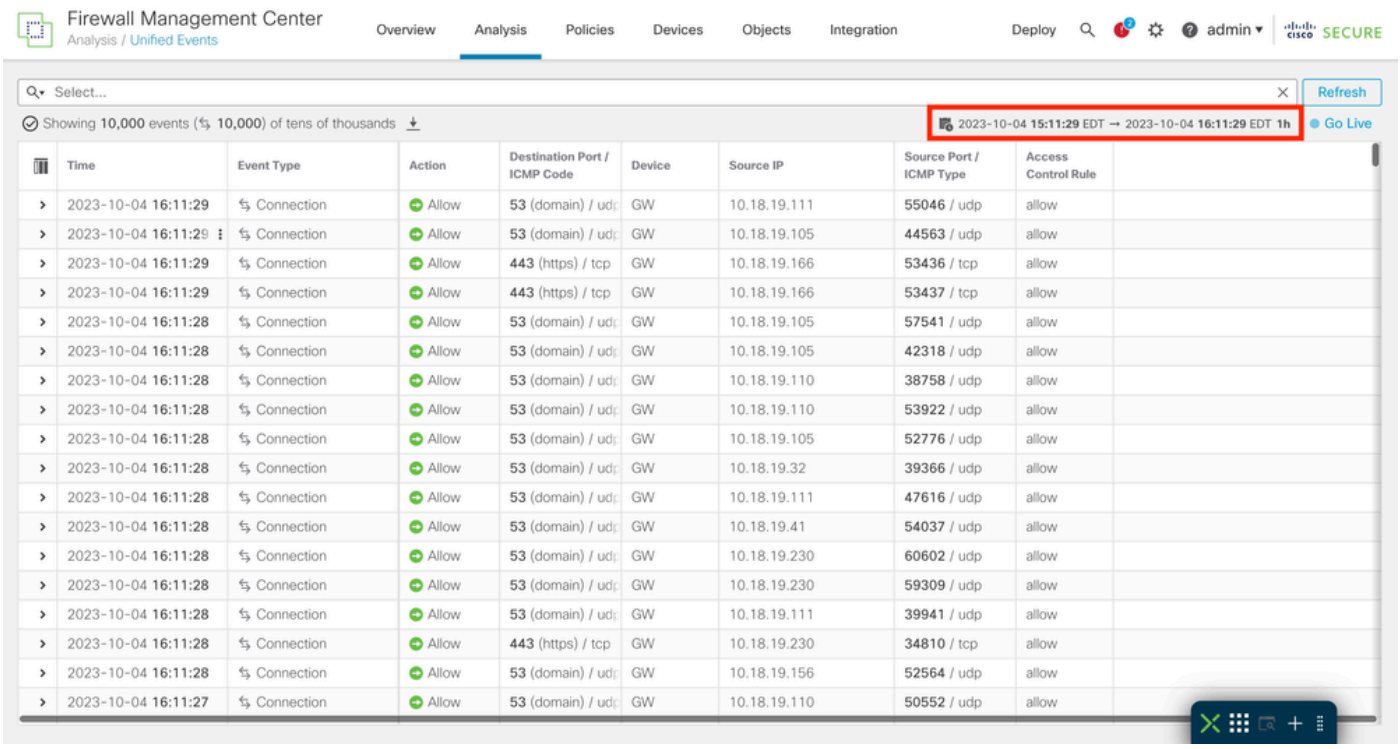
3단계. (선택 사항) 검색의 이름을 변경합니다.



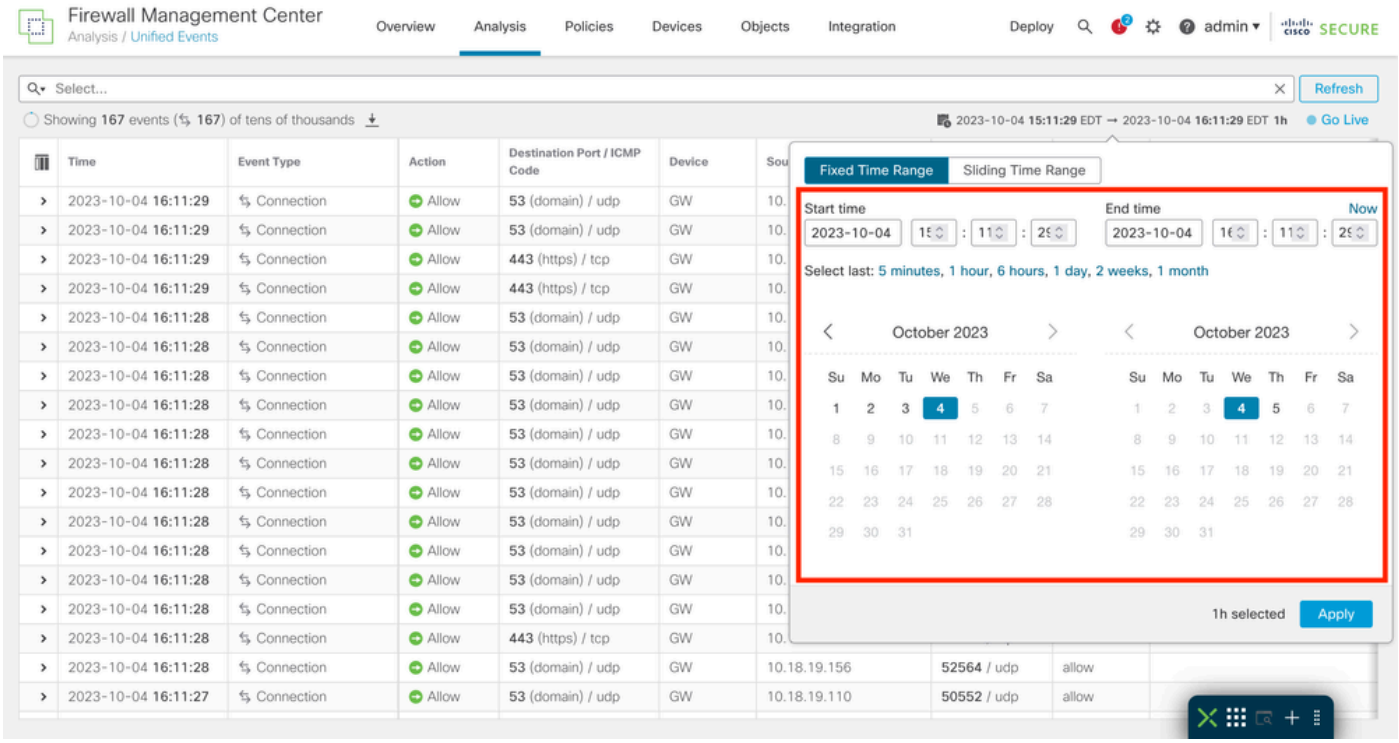
타임 윈도우

타임 윈도우를 수정하여 특정 시간을 기준으로 관련 이벤트를 좁히는 것이 더 쉽습니다.

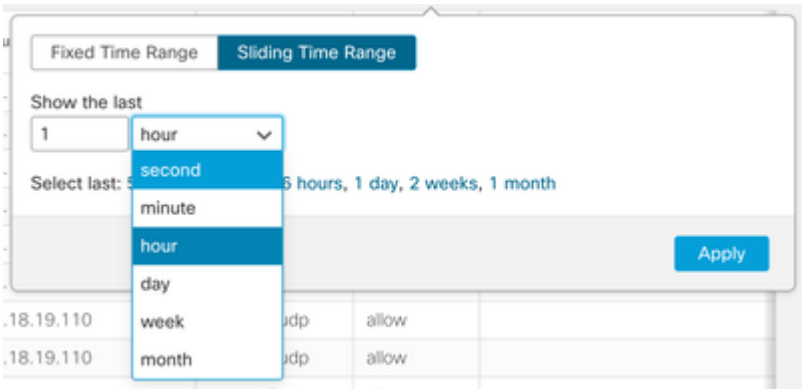
1단계. 이벤트의 창 프레임을 수정하려면 날짜 범위를 클릭합니다.



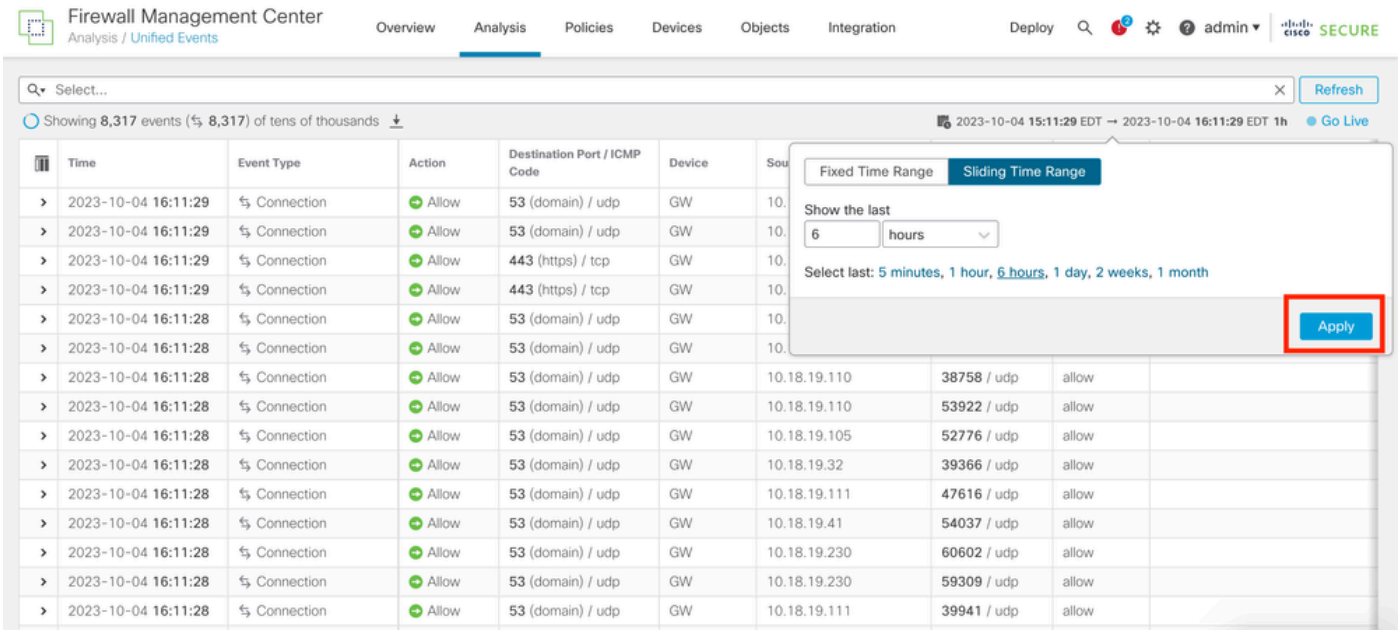
2단계. 팝업 창에서 시간 범위를 선택합니다.



3단계. (선택 사항) 슬라이딩 시간 범위를 사용하여 특정 시간부터 현재 시간까지의 이벤트를 표시합니다.



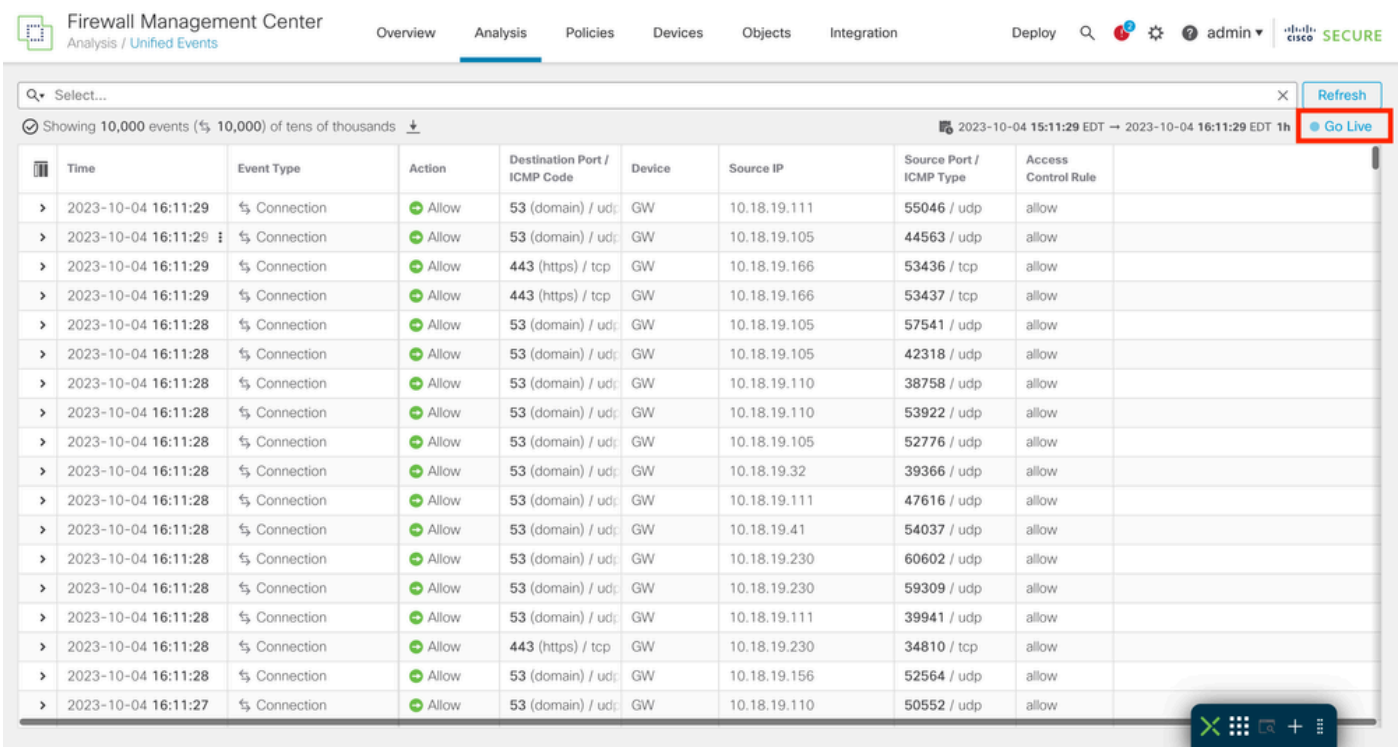
4단계. 구성된 시간 범위에서 이벤트를 필터링하려면 Apply(적용)를 클릭합니다.



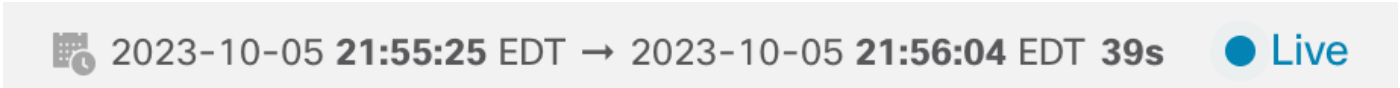
라이브

Go Live 기능을 활성화하여 실시간으로 이벤트를 표시할 수 있습니다. 이벤트는 생성된 대로 표시됩니다.

활성화하려면 Go Live를 클릭합니다.



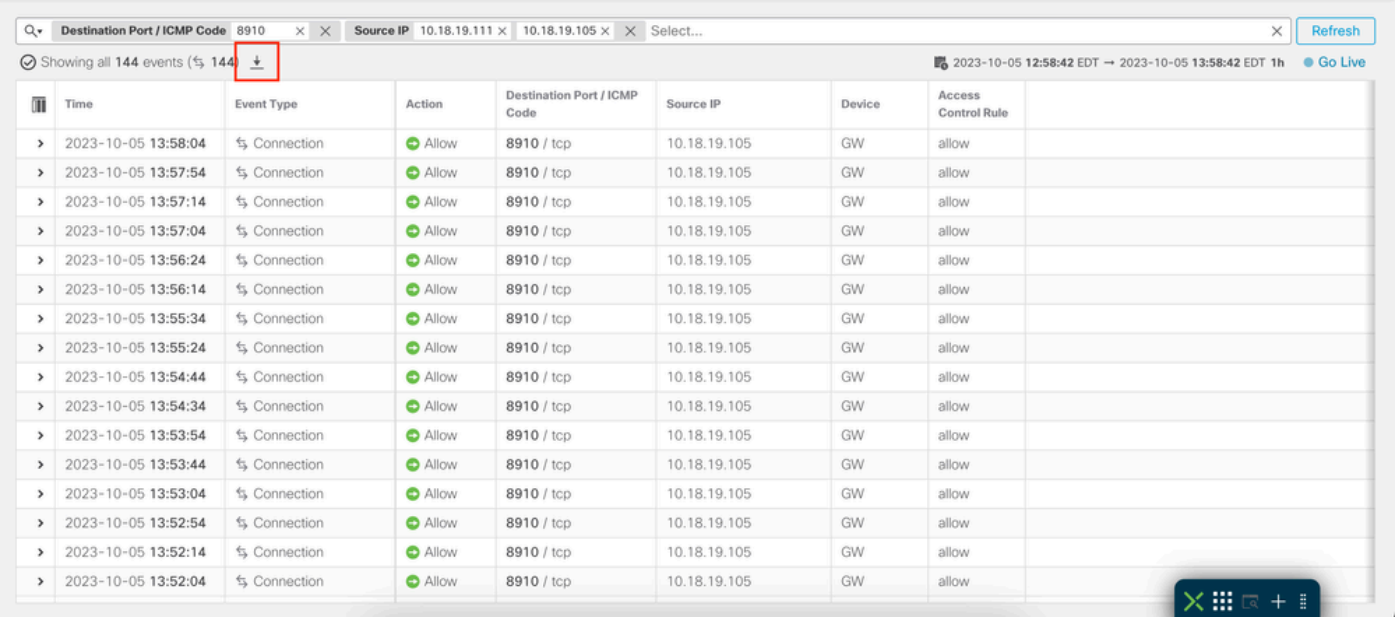
활성화된 후에는 Live라는 단어가 표시됩니다.



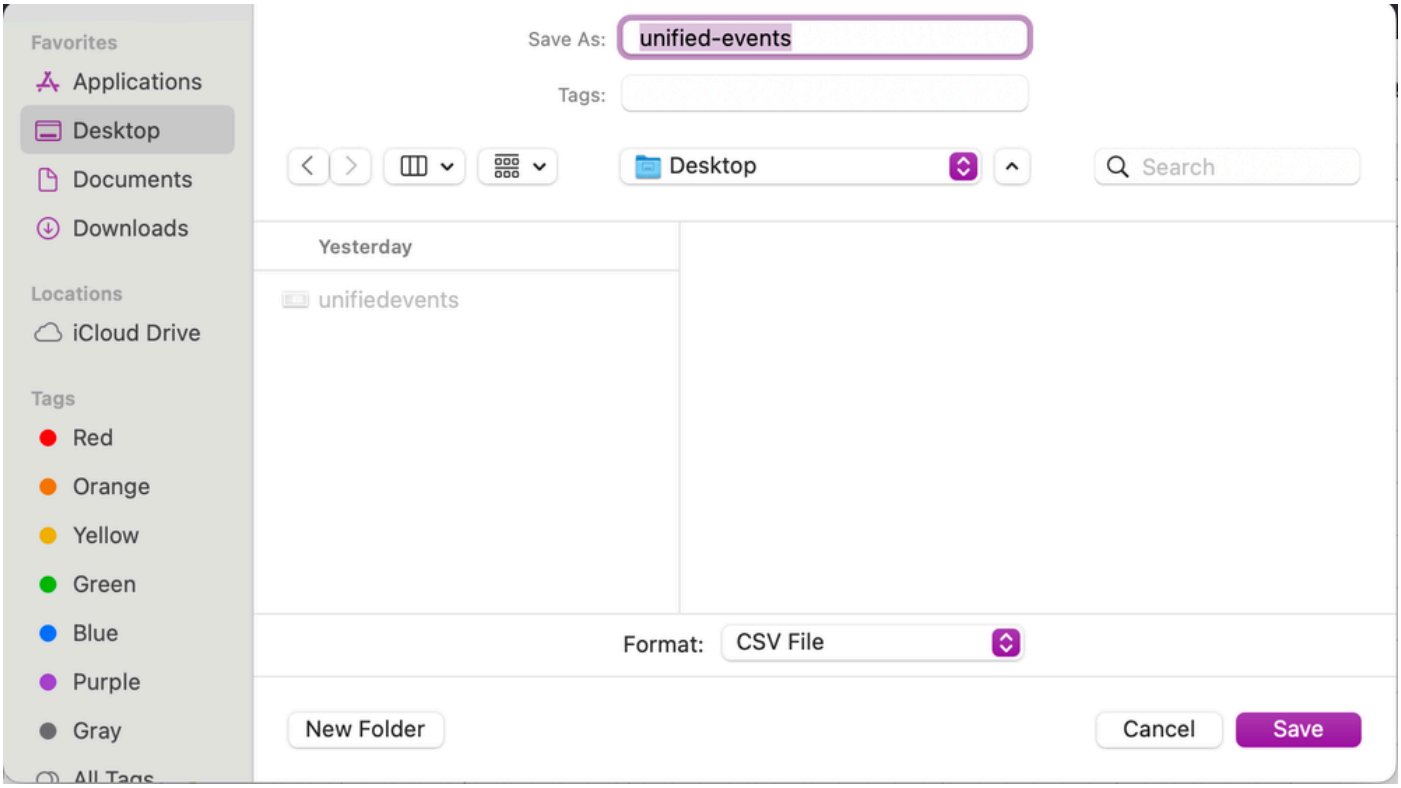
⚠ 주의: Live가 활성화된 경우 타임 윈도우를 수정할 수 없습니다. 타임 윈도우를 수정하려면 먼저 라이브 옵션을 다시 클릭하여 비활성화하십시오.

이벤트 다운로드 형식 쉼표로 구분된 값(CSV)

1단계. 다운로드 아이콘을 클릭하여 페이지에 현재 표시된 이벤트를 포함하는 파일을 생성합니다.



2단계. 다운로드 폴더와 이름을 선택하고 저장을 클릭합니다.



3단계. CSV 파일을 확인합니다.

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	37412 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	54766 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.166	54279 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	55185 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	46312 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	36785 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	57394 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	57395 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	38278 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44865 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	58387 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	49873 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	51060 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	34103 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.31	60020 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	43410 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47406 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	43359 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	43336 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	42658 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52923 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	46485 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.201	52178 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55864 / udp	allow

관련 정보

- Unified Event Viewer 작업
- Cisco Secure Firewall - Unified Events Viewer: 팁과 요령
- 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.

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.