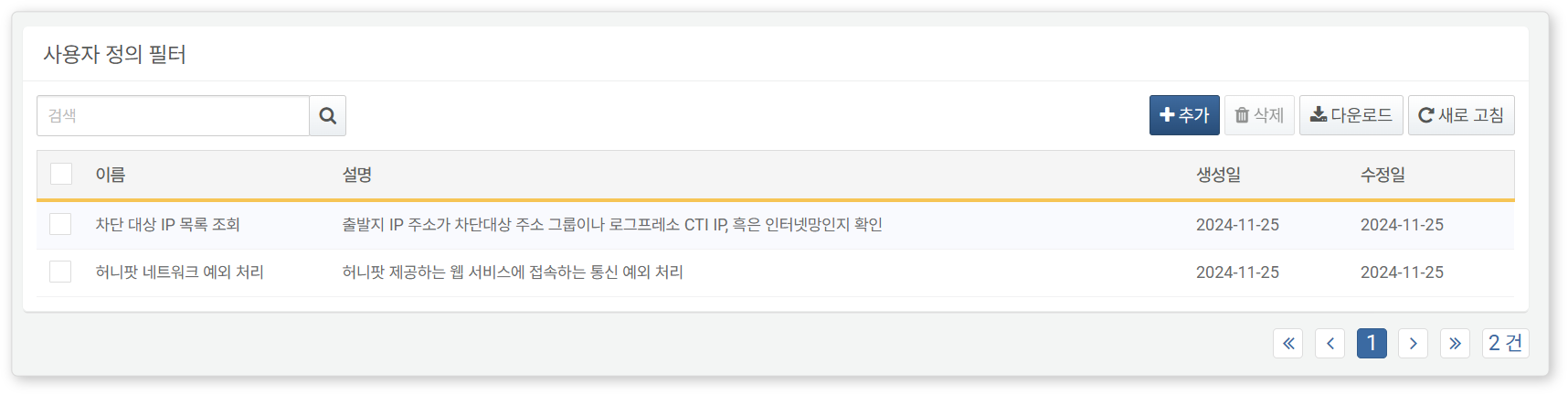
### 사용자 정의 필터

#### 개요

사용자 정의 필터를 통해 탐지 시나리오 정책에 특정 필터링 조건을 적용하여 데이터를 분석하고 탐지할 수 있습니다. 이러한 필터는 반복적으로 사용되는 복잡한 조건을 모듈화하여, 여러 탐지 시나리오에서 동일한 조건을 쉽게 적용할 수 있도록 합니다. 이를 통해 실시간 또는 배치 탐지 시나리오에서 필요한 필터를 효율적으로 수행할 수 있습니다. 사용자 정의 필터를 사용하면 정확한 데이터 필터링과 조건에 맞는 분석 및 탐지가 가능합니다.

#### 사용자 정의 필터 목록 조회/검색

**정책 > 사용자 정의 필터**에서 사용자 정의 필터 목록을 조회하거나 검색할 수 있습니다.



* **이름**: 사용자 정의 필터의 고유 이름
* **설명**: 사용자 정의 필터에 대한 설명
* **생성일**: 사용자 정의 필터가 생성된 날짜
* **수정일**: 사용자 정의 필터가 마지막으로 수정된 날짜

사용자 정의 필터 목록에서 특정 사용자 정의 필터를 찾으려면 도구 모음에 있는 검색 도구를 사용하세요. 검색 도구는 입력한 단어가 **이름**, **설명**에 포함된 사용자 정의 필터를 찾아서 보여줍니다. 검색 도구는 대소문자를 구분하지 않습니다.

목록 다운로드

사용자 정의 필터 목록을 로컬 PC에 파일로 다운로드하려면 도구 모음에서 **다운로드**를 클릭하세요.

목록 새로 고침

사용자 정의 필터의 목록을 최신 정보로 조회하려면 도구 모음에서 **새로 고침**을 클릭하세요.

#### 사용자 정의 필터 추가

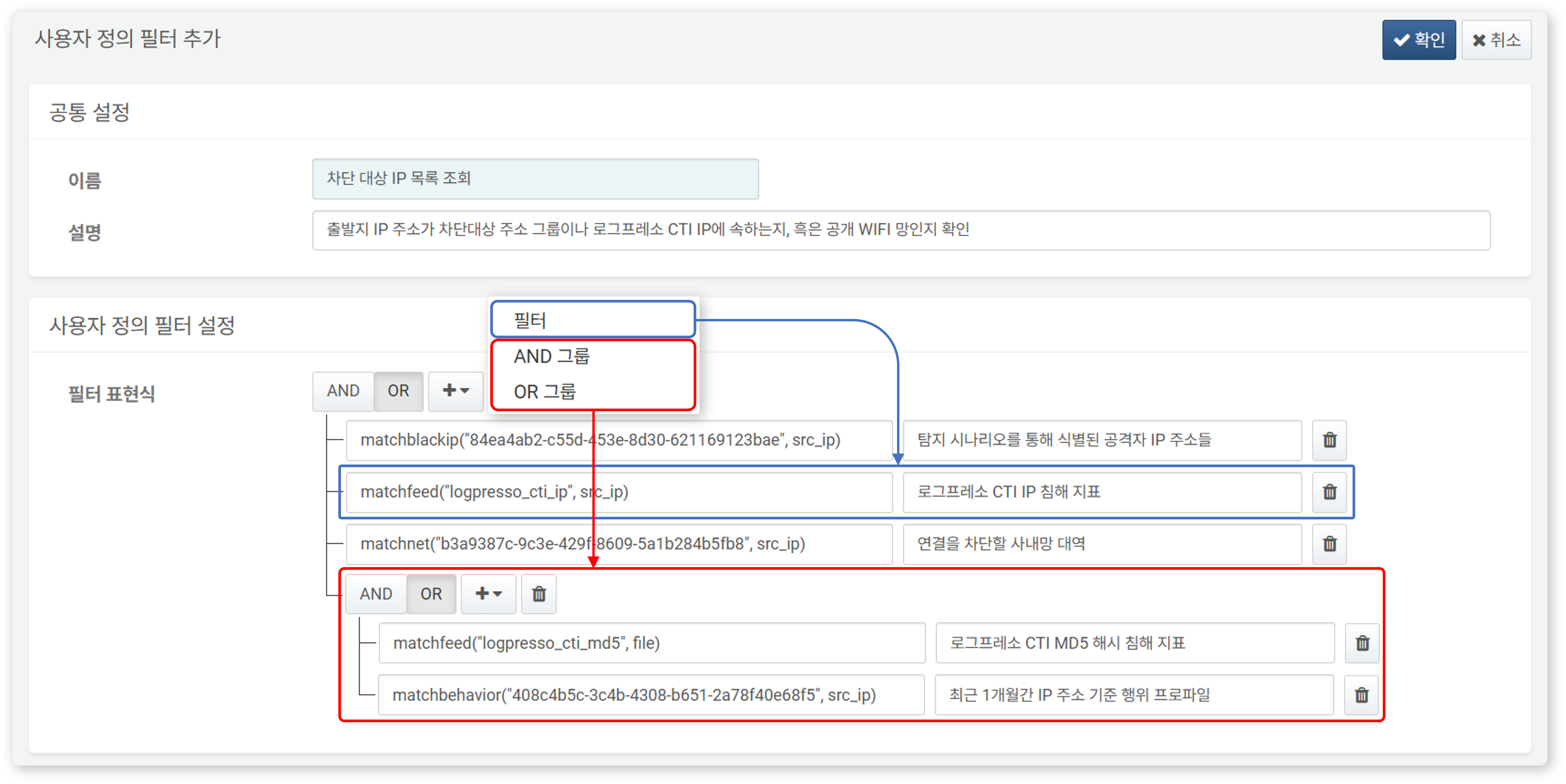
사용자 정의 필터를 추가하려면,

**정책 > 사용자 정의 필터**에서 도구 모음에 있는 **추가**를 클릭하세요.

**사용자 정의 필터 추가** 화면에서 **공통 설정** 속성을 입력하세요.

* **이름**: 사용자 정의 필터의 고유 이름(최대 50자). 필터를 추가한 후에는 이름을 수정할 수 없습니다.
* **설명**: 사용자 정의 필터에 대한 설명(최대 2,000자)

**사용자 정의 필터 설정**에서 **필터 표현식**을 입력한 다음, **확인**을 클릭하세요.



* 처음에는 **필터 표현식** 입력란이 하나만 제공됩니다. 여기에 로그프레소 쿼리로 작성된 불리언 표현식과 설명을 입력하세요(필터 표현식, 설명 각각 최대 1,000자).
* "**+**"을 클릭하면 단일 필터 표현식이나 하위 필터 표현식 그룹을 추가할 수 있습니다. 그룹은 최대 3 단계까지 추가할 수 있습니다.
* 필터 표현식의 논리곱(AND, 조건이 모두 참일 때만 참을 반환)이나 논리합(OR, 두 조건 중 하나라도 참이면 참을 반환)이 필요한 경우, **AND**, **OR**을 클릭하세요.
* 필터 표현식 또는 필터 표현식 그룹을 삭제하려면 우측에 있는 휴지통 아이콘을 클릭하세요.

#### 사용자 정의 필터 수정

사용자 정의 필터를 수정하려면,

[사용자 정의 필터 목록](https://docs.logpresso.com/ko/sonar/4.0/ui/section-udf)에서 수정할 사용자 정의 필터의 이름을 클릭하세요.

**사용자 정의 필터 수정** 화면에서 정보를 수정한 후 **저장**을 클릭하세요.

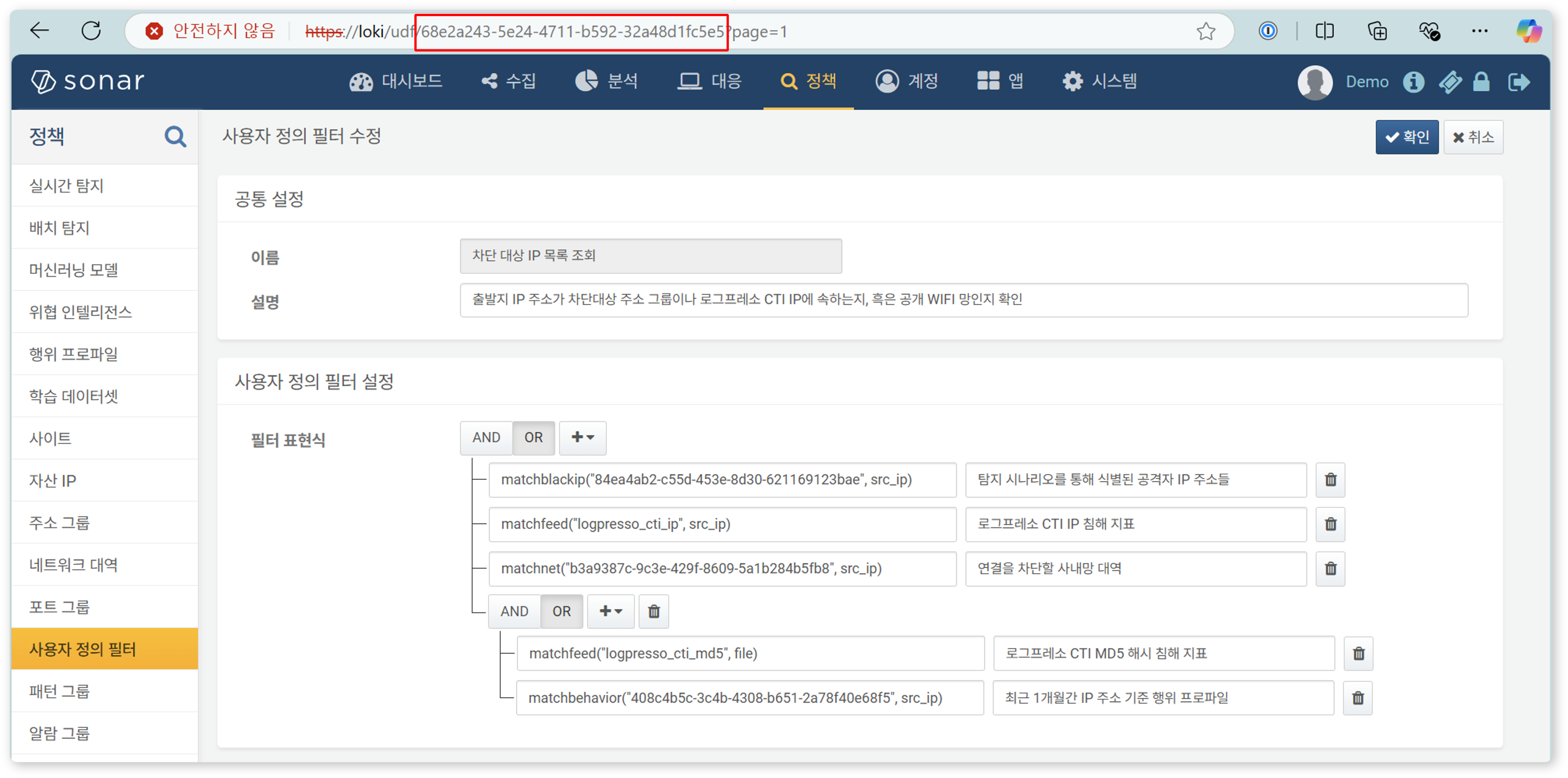
#### 사용자 정의 필터 활용

사용자 정의 필터는 다음과 같은 방법으로 설정 및 사용할 수 있습니다.

쿼리

사용자 정의 필터는 쿼리문 작성 시 [matchfilter()](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/query/matchfilter-function) 함수를 호출하여 사용할 수 있습니다. 예를 들어 사용자 정의 필터를 사용하여 특정 IP 주소를 필터링하려는 경우, search matchfilter("사용자 정의 필터 GUID") 형식으로 쿼리를 작성하세요.

matchfilter() 함수를 사용하려면 사용자 정의 필터의 GUID를 알아야 합니다. GUID는 웹 브라우저의 주소 표시줄에서 확인할 수 있습니다.



#### 사용자 정의 필터 삭제

사용자 정의 필터를 삭제하려면,

사용자 정의 필터 목록에서 삭제할 사용자 정의 필터 행의 체크박스를 선택하세요.

도구 모음에서 **삭제**를 클릭하세요.

**사용자 정의 필터 삭제** 대화상자에서 삭제할 사용자 정의 필터 목록을 확인한 후 **삭제**를 클릭하세요. 삭제하지 않으려면 **취소**를 클릭하세요.

실시간 탐지 또는 배치 탐지 시나리오에서 참조하는 사용자 정의 필터를 삭제하면 탐지 시나리오가 의도한 대로 동작하지 않을 수 있으므로 주의하세요.