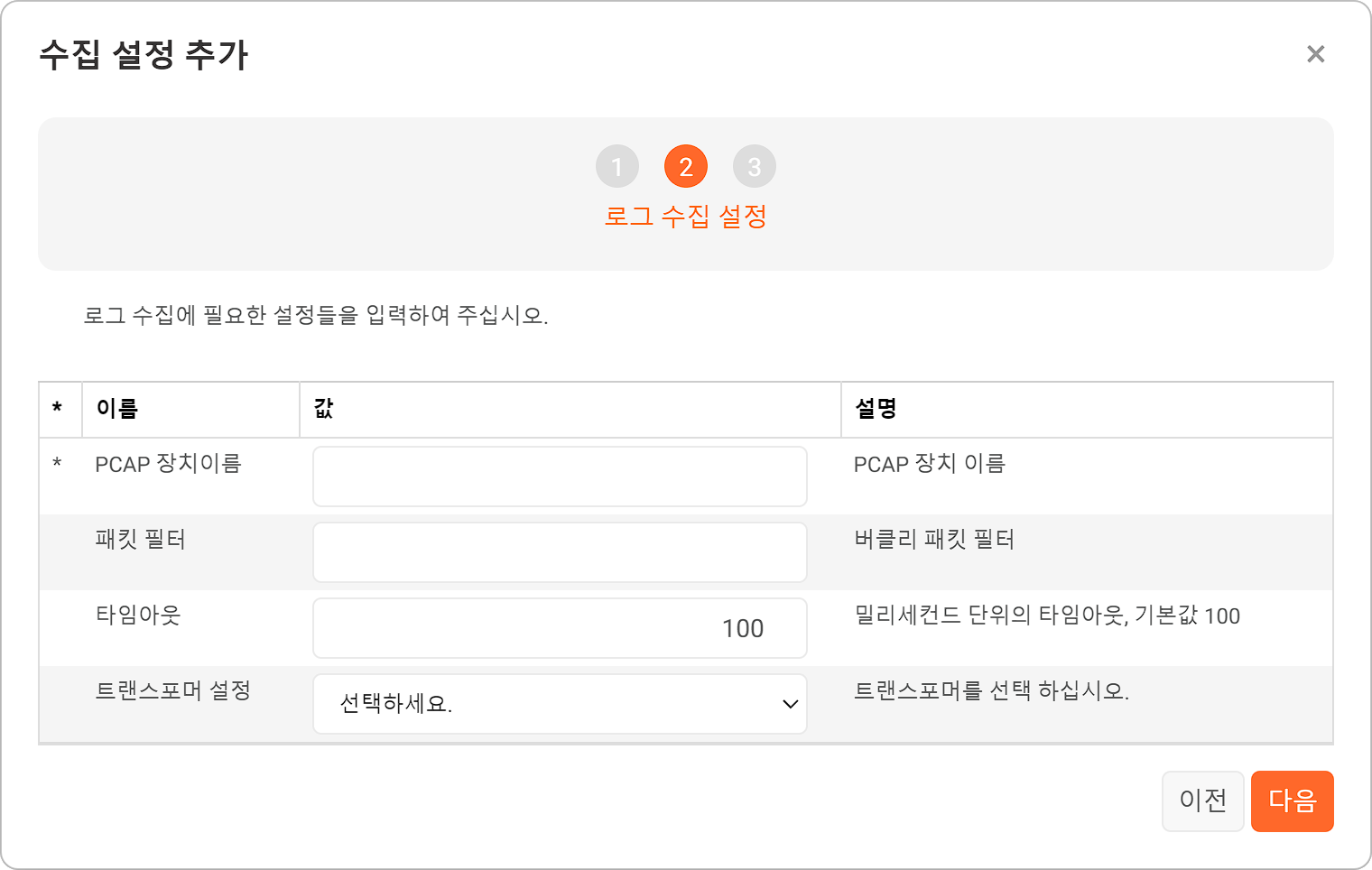
#### PCAP

PCAP 로거들은 특정한 로컬 디렉터리에 저장되는 PCAP 파일을 수집하거나, PCAP 장치로부터 패킷을 미러링하는 방식으로 데이터를 수집합니다.



DNS 스니퍼

DNS 스니퍼는 PCAP 장치로부터 네트워크를 미러링하여 DNS 패킷을 기록합니다.



**PCAP 장치이름**

패킷 데이터를 수집할 PCAP 장치. 로그프레소 셸에서 pcap.devices 명령으로 PCAP 장치 목록을 확인할 수 있습니다.

**패킷 필터**

버클리 패킷 필터 문법에 따라 패킷 캡처 규칙을 입력(tcpdump에서 사용하는 문법과 동일)

**타임아웃**

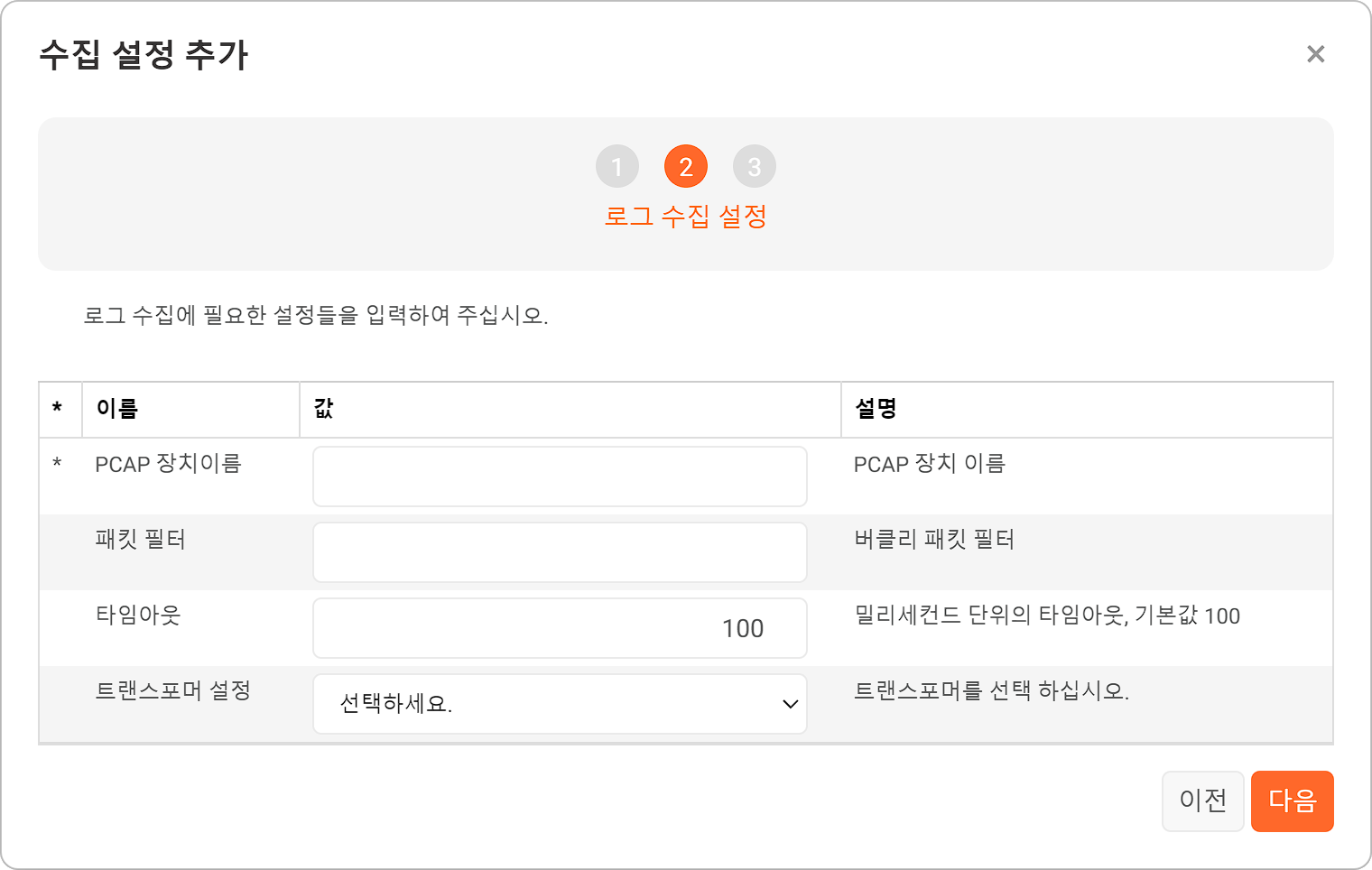
타임아웃 시간(기본값: 100 밀리초)

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

HTTP 스니퍼

HTTP 스니퍼는 PCAP 장치로부터 네트워크를 미러링하여 HTTP 패킷을 기록합니다.



**PCAP 장치이름**

패킷 데이터를 수집할 PCAP 장치. 로그프레소 셸에서 pcap.devices 명령으로 PCAP 장치 목록을 확인할 수 있습니다.

**패킷 필터**

버클리 패킷 필터 문법에 따라 패킷 캡처 규칙을 입력(tcpdump에서 사용하는 문법과 동일)

**타임아웃**

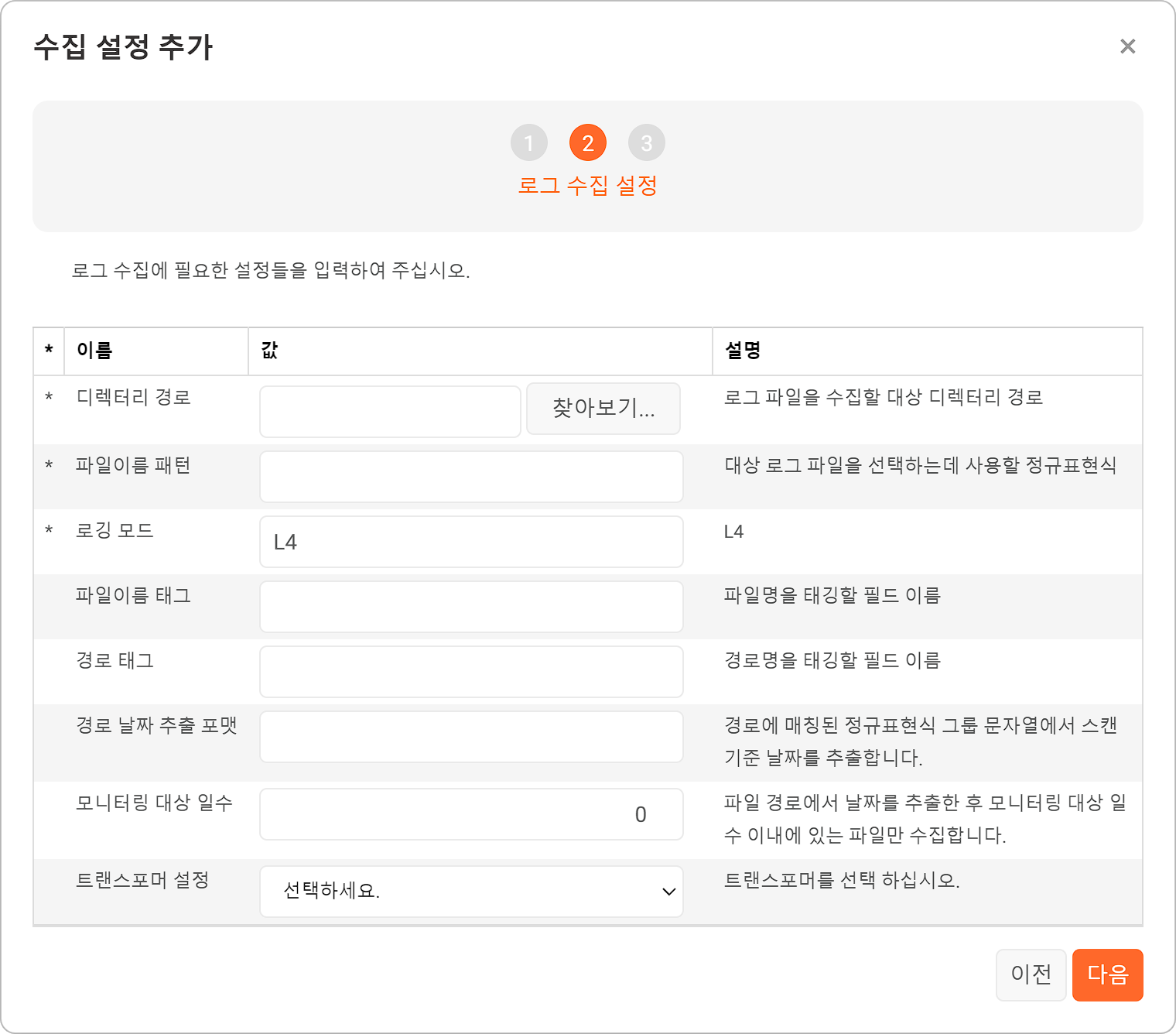
타임아웃 시간(기본값: 100 밀리초)

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

PCAP 디렉터리 와처

PCAP 디렉터리 와처는 디렉터리에서 PCAP 파일을 수집합니다.



**디렉터리 경로**

파일을 수집할 대상 디렉터리 경로

**파일이름 패턴**

수집할 파일의 이름을 검색할 때 사용할 정규표현식

**로깅 모드**

데이터 수집 모드(기본값: L4). 현재는 L4만 지원합니다.

**파일이름 태그**

수집한 파일 이름을 기록할 필드 이름

**경로 태그**

디렉터리 경로를 기록할 필드 이름

**경로 날짜 추출 포맷**

디렉터리 경로 문자열에서 날짜 문자열 검색에 사용할 정규표현식. 디렉터리가 날짜를 기준 생성될 때(예: /var/log/foo/2022-11-02/bar) 디렉터리 경로 문자열에서 GZIP 파일의 스캔 기준 날짜를 추출할 때 사용합니다.

**모니터링 대상 일수**

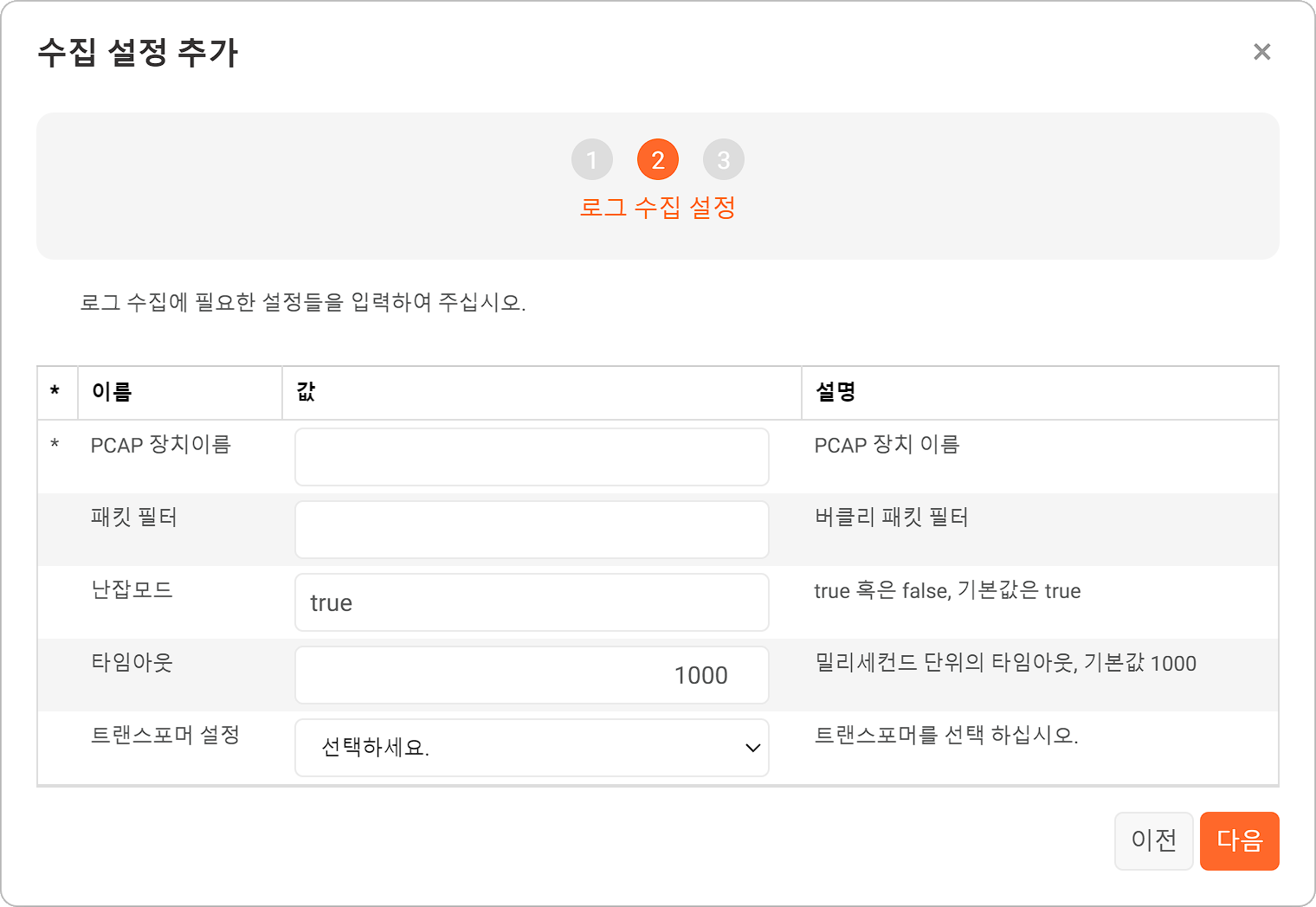
파일 경로에서 날짜를 추출한 후 모니터링 대상 일수 이내에 있는 파일만 수집합니다(기본값: 0(기간 제한 없이 파일에 있는 로그 수집)).

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

PCAP 패킷

PCAP 패킷 로거는 PCAP 장치로부터 패킷을 수집합니다.



**PCAP 장치이름**

패킷 데이터를 수집할 PCAP 장치. 로그프레소 셸에서 pcap.devices 명령으로 PCAP 장치 목록을 확인할 수 있습니다.

**패킷 필터**

버클리 패킷 필터 문법에 따라 패킷 캡처 규칙을 입력(tcpdump에서 사용하는 문법과 동일)

**난잡 모드**

난잡 모드(promiscuous mode) 사용 여부를 나타내는 불리언 값(기본값: true)

**타임아웃**

타임아웃 시간(기본값: 1000 밀리초)

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.