#### 시스로그 파서

시스로그 파서는 시스로그 통신으로 데이터를 전송하는 써드파티 제품의 로그를 다루는 파서들입니다.

설정이 필요없는 파서들

다음에 열거된 시스로그 통신으로 받은 데이터를 파싱하는 파서들입니다. 이 파서들은 별도로 설정할 항목이 없습니다.

* **DB 세이퍼 파서**: 피앤피시큐어 DB세이퍼 로그 파서
* **FDX DPI 파서**: FDX네트웍스 DPI 로그 파서
* **LEEF 파서**: Long Event Extended Format 로그 파서
* **MFD 파서**: SECUI MFD 로그 파서
* **NXG D시리즈 파서**: SECUI NXG D 로그 파서
* **SRX 서비스 게이트웨이 파서**: 주니퍼네트웍스 SRX 서비스 게이트웨이 로그 파서
* **SRX3400 서비스 게이트웨이 파서**: 주니퍼네트웍스 SRX3400 서비스 게이트웨이 로그 파서
* **TESS 파서**: 코닉글로리 TESS 로그 파서
* **TESS 감사로그 파서**: 코닉글로리 TESS 감사로그 파서
* **게이트원**: 모두스윈 게이트윈 로그 파서
* **네오박스**: XN시스템즈 네오박스 로그 파서
* **다크트레이스 EIS**: 다크트레이스 EIS 로그 파서
* **더블유쉴드 안티웹쉘**: SK쉴더스 더블유쉴드 안티웹쉘 로그 파서
* **디펜스 프로**: 라드웨어 디펜스 프로 로그 파서
* **리오레이**: 모젠소프트 리오레이 로그 파서
* **브이포스 UTM**: 한솔넥스지 VForce 로그 파서
* **소닉월**: 소닉월 로그 파서
* **쉘모니터**: UMV기술 쉘모니터 로그 파서
* **스나이퍼 APTX**: 윈스 스나이퍼 APTX 로그 파서
* **스노트**: 스노트 로그 파서
* **스팸 스나이퍼**: 지란지교시큐리티 스팸 스나이퍼 로그 파서
* **스팩트라가드 엔터프라이즈**: 모조 네트웍스 스펙트라가드 엔터프라이즈 로그 파서
* **시큐어스피어**: 임퍼바 시큐어스피어 로그 파서
* **시큐어웍스**: 어울림정보기술 시큐어웍스 로그 파서
* **아이윌**: 한국통신인터넷기술 아이윌 방화벽 로그 파서
* **엑쉴드**: 시큐아이 eXshield 로그 파서
* **웹 게이트웨이**: 시만텍 웹 게이트웨이 로그 파서
* **웹디펜더**: 멜리타 웹디펜더 로그 파서
* **위가디아 WIPS**: 퓨쳐시스템 WeGuardia WIPS 로그 파서
* **이프리즘 SSL**: 수산아이엔티 ePrism SSL 로그 파서
* **지니안 NAC 스위트**: 지니네트웍스 지니안 NAC 스위트 로그 파서
* **카운터액트 NAC**: 포어스카우트 카운터액트 NAC 로그 파서
* **티핑포인트 SMS**: 티핑포인트 SMS 로그 파서
* **파이어박스 X**: 워치가드 파이어박스 X 로그 파서
* **파이어아이 CMS**: FireEye CMS 로그 파서
* **파이어아이 MPS**: FireEye MPS 로그 파서
* **파이어아이 NX**: FireEye NX 로그 파서
* **시스코 파이어파워 FTD**: Cisco Firepower FTD 로그 파서
* **펄스 커넥트 시큐어**: 펄스 시큐어 펄스 커넥트 시큐어 로그 파서
* **프로벤티아 IDS**: IBM Proventia IDS 로그 파서
* **프로텍션 엔진**: 시만텍 프로텍션 엔진 로그 파서

Axgate UTM 파서

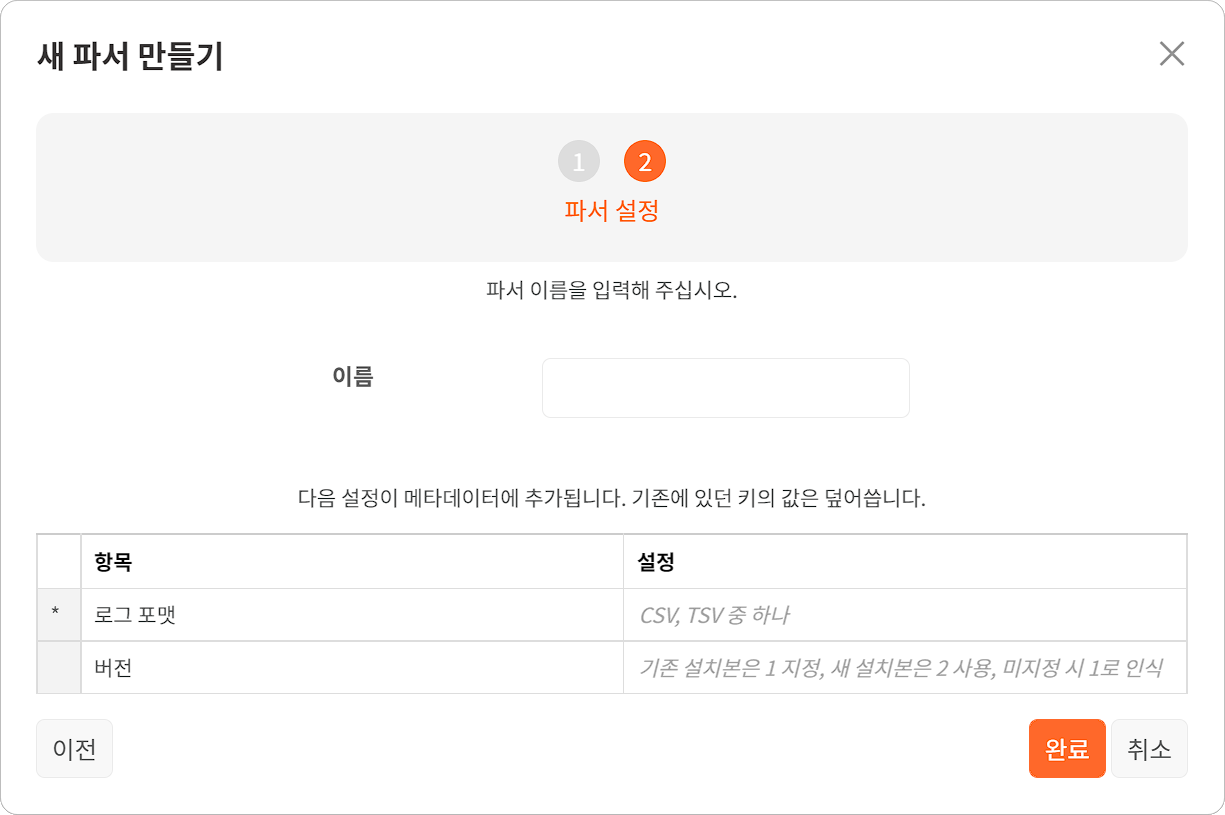
Axgate UTM 파서는 엑스게이트의 차세대방화벽인 AXGATE 시리즈의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

MF2 파서

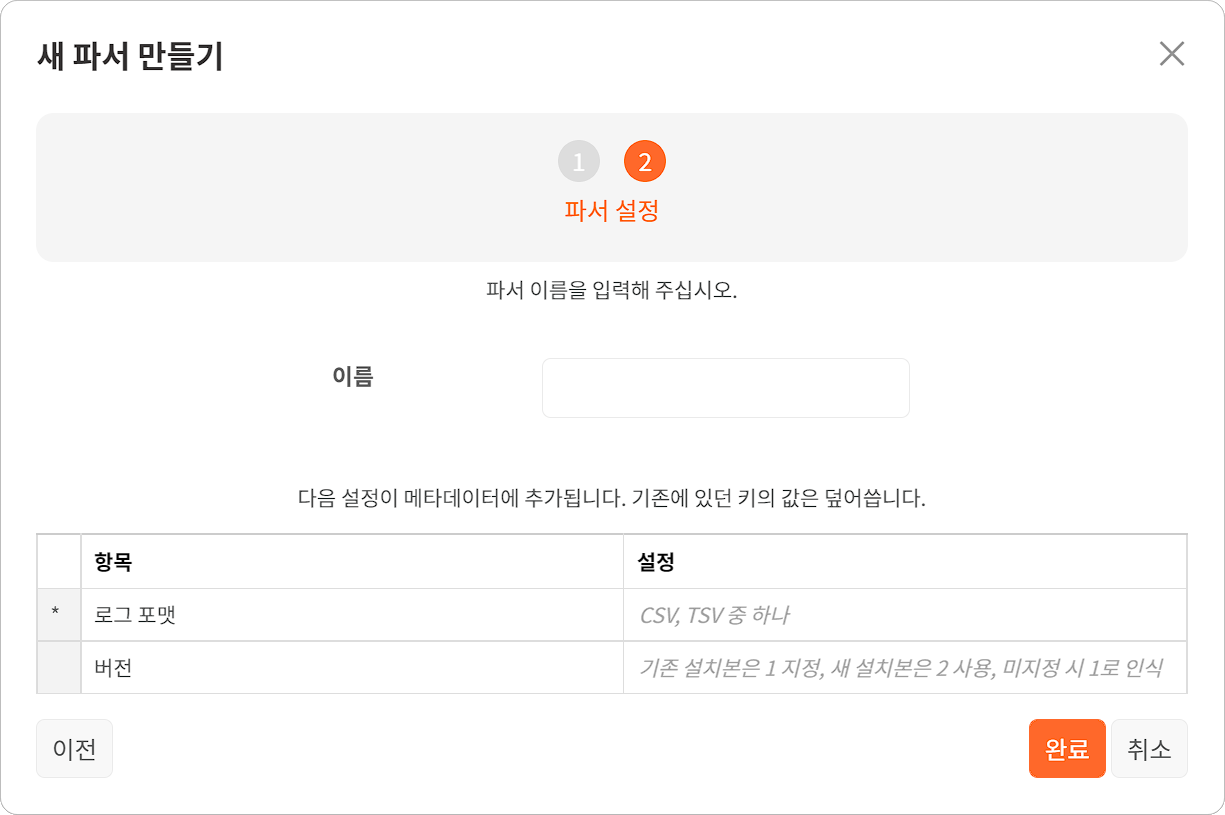
MF2 파서는 시큐아이의 UTM인 SECUI MF2의 시스로그를 파싱합니다.



* **로그 포맷**: **CSV**, **TSV** 중에서 선택
* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

MFI 파서

MFI 파서는 시큐아이의 IPS 장비인 SECUI MFI의 시스로그를 파싱합니다.



* **로그 포맷**: **CSV**, **TSV** 중에서 선택
* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

NXG 파서

NXG 파서는 시큐아이의 UTM인 SECUI NXG의 시스로그를 파싱합니다.

PA 시리즈 파서

PA 시리즈 파서는 팔로알토네트웍스의 차세대 방화벽 PA 시리즈의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

넥스지 FW 파서

넥스지 FW 파서는 한솔넥스지의 차세대 방화벽 NexG FW의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

넷스크린 파서

넷스크린 파서는 주니퍼 넷스크린 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

사이버롬 UTM 파서

사이버롬 UTM 파서는 CyberroamWorks의 UTM인 Cyberoam UTM의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

스나이퍼 IPS 파서

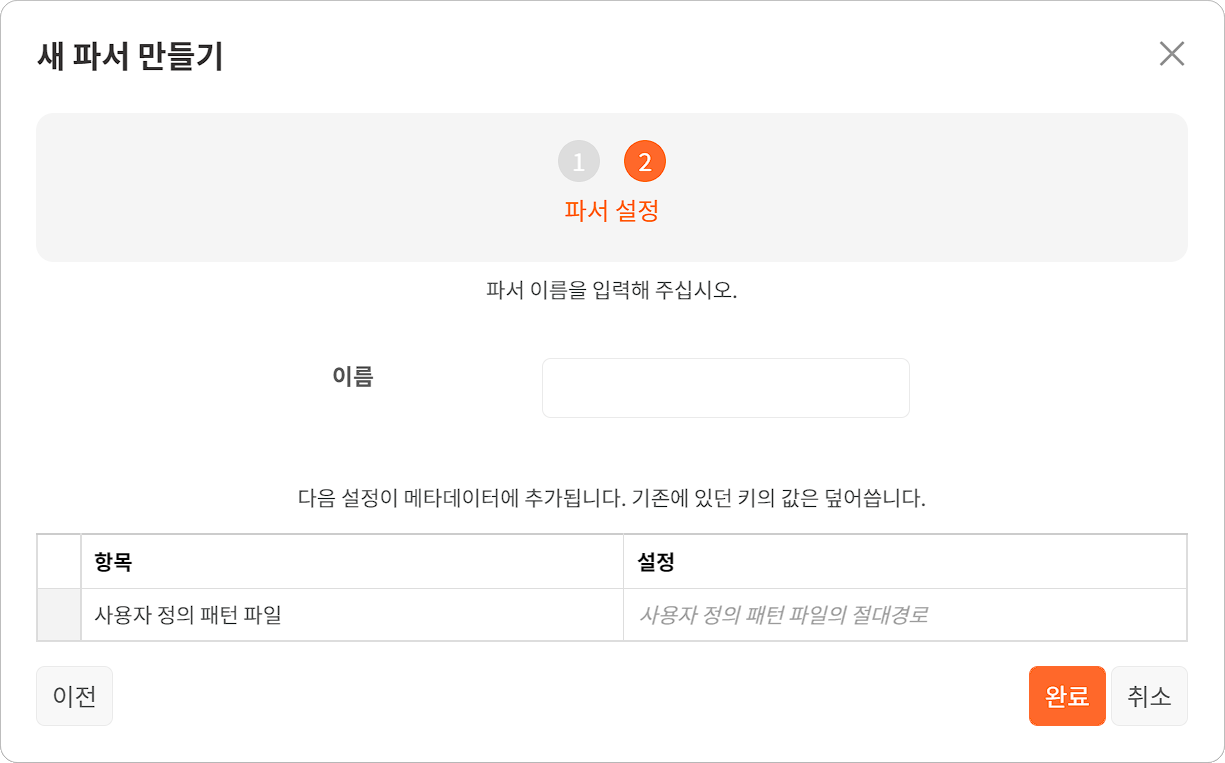
스나이퍼 IPS 파서는 윈스의 Sniper IPS 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

시스코 ASA 파서

시스코 ASA 파서는 시스코 ASA 시리즈의 시스로그를 파싱합니다.



* **사용자 정의 패턴 파일**: 사용자 정의 패턴 파일의 절대 경로

시큐위즈 SSLVPN 파서

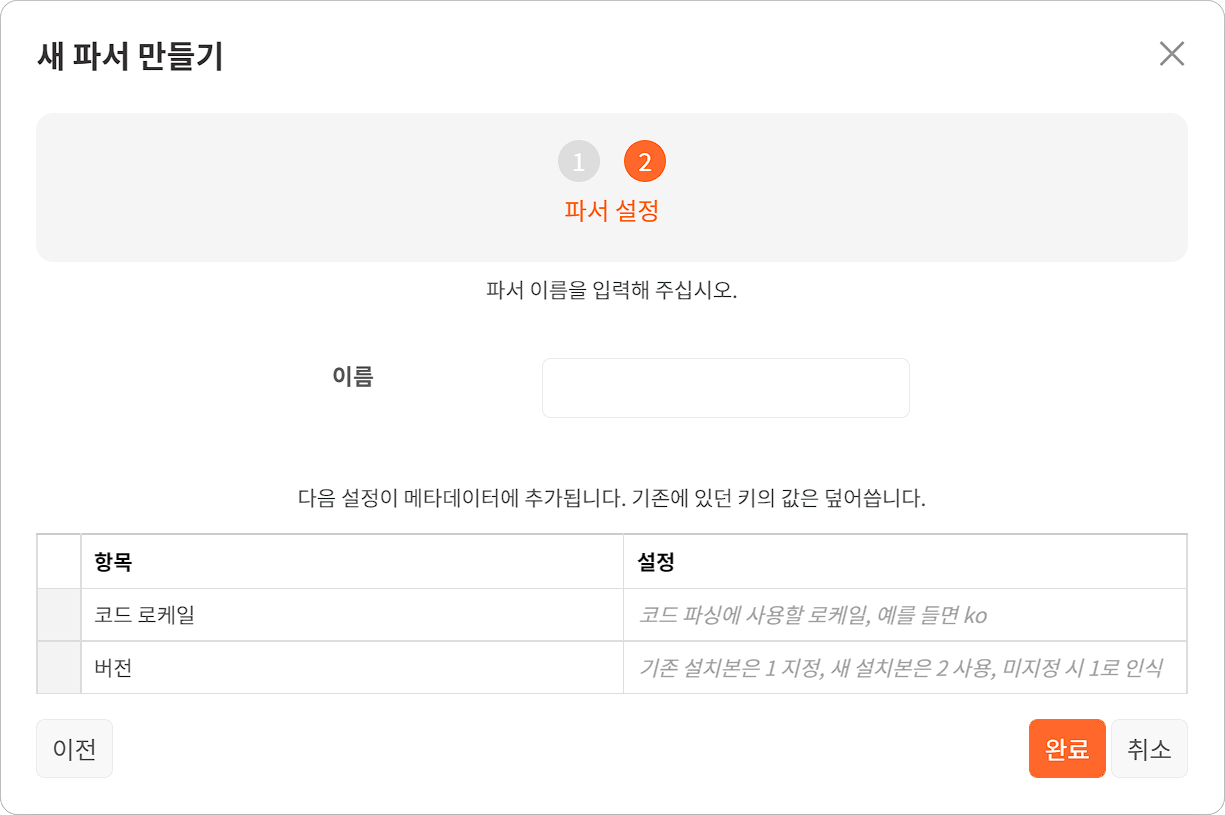
시큐위즈 SSLVPN 파서는 시큐위즈의 SSL VPN 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

안랩 MDS 파서

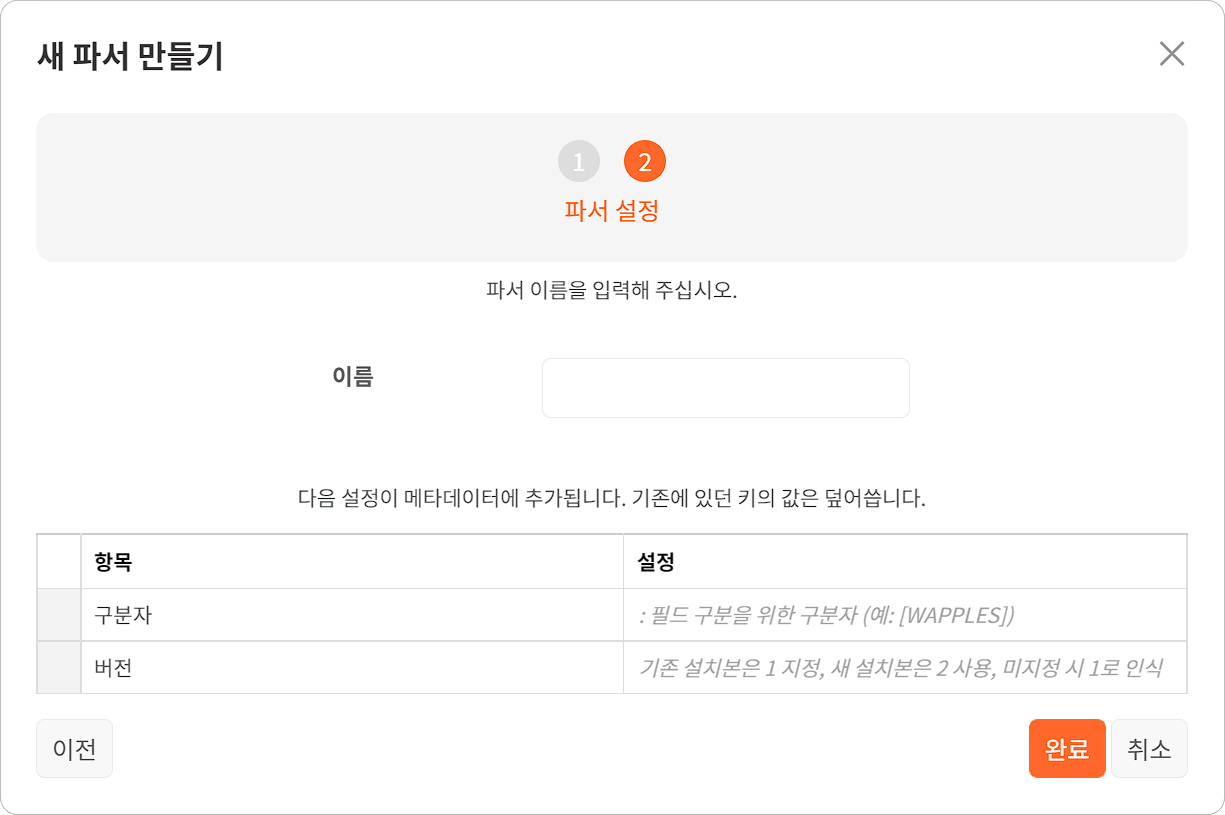
안랩 MDS 파서는 안랩의 APT 대응 솔루션 AhnLab MDS의 시스로그를 파싱합니다.



* **코드 로케일**: 코드 파싱에 사용할 언어 로케일(ko, en)
* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

와플 SYSLOG 파서

와플 SYSLOG 파서는 펜타시큐리티의 웹 방화벽 WAPPLES의 시스로그를 파싱합니다.



웹 인사이트 파서

웹 인사이트 파서는 모니터랩의 웹 방화벽인 웹 인사이트 WAF의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

웹 프론트 파서

웹 프론트 파서는 파이오링크의 웹 방화벽인 WEBFRONT 시리즈의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

위가디아 XTM 파서

위가디아 XTM 파서는 퓨쳐시스템의 UTM인 WeGuardia XTM 시리즈의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

큐브디펜스 파서

큐브디펜스 파서는 트라이큐브랩의 큐브디펜스 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

트러스가드 파서

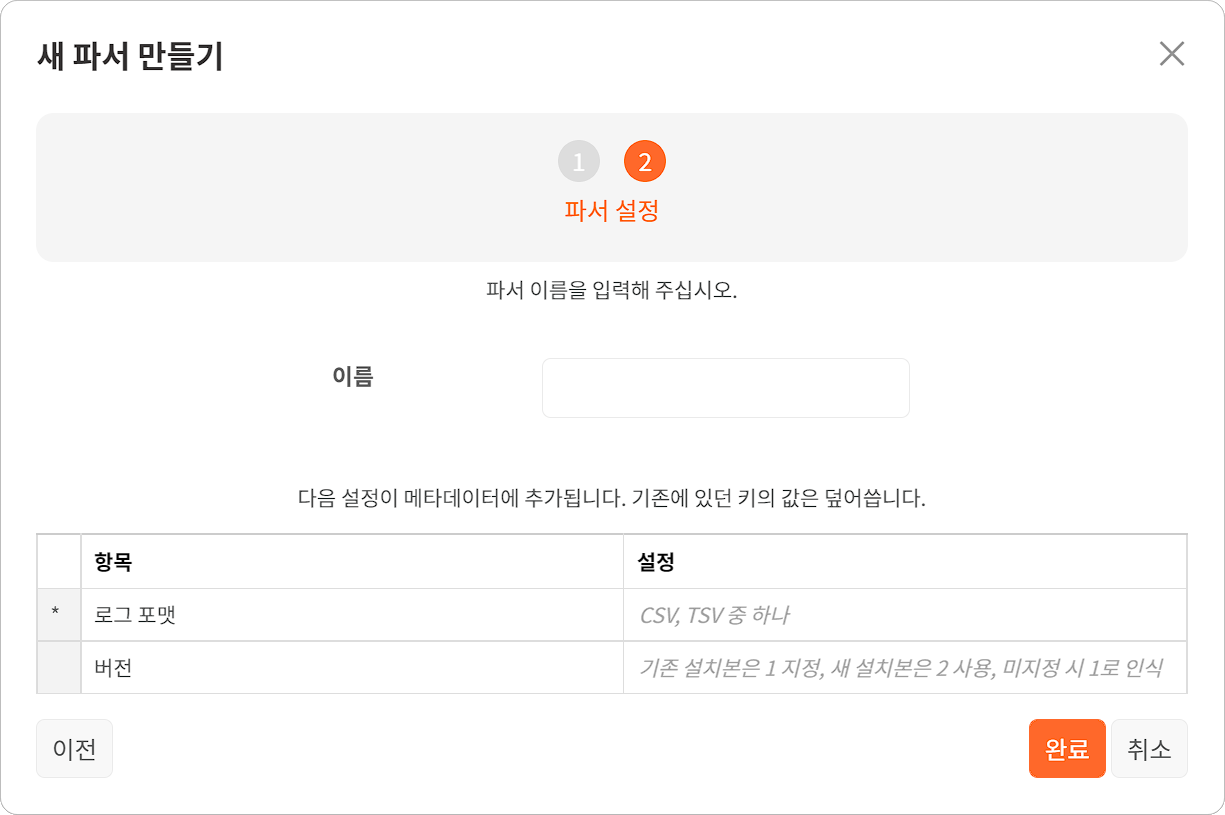
트러스가드 파서는 안랩의 차세대 통합 보안 방화벽인 AhnLab TrusGuard의 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

티핑포인트 IPS

티핑포인트 IPS 파서는 티핑포인트의 IPS 시스로그를 파싱합니다.



* **로그 포맷**: **CSV**, **TSV** 중에서 선택
* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

파이어파워 파서

파이어파워 파서는 시스코의 파이어파워 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)

포티게이트 파서

포티게이트 파서는 WELF(WebTrends Enhanced Log Format) 형식으로 작성된 Fortigate 시스로그를 파싱합니다.



* **버전**: 로그 형식(1: 기존 설치본(기본값), 2: 새 설치본)