GlobalHost

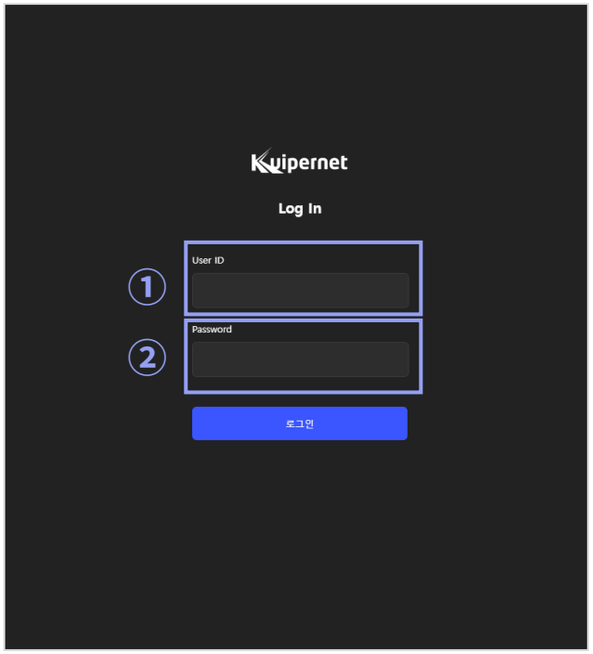
글로벌 WAF
사용 가이드

CONTENTS

I. 로그인

1-1. 로그인

관리 웹에 접속하면 로그인 화면이 표시됩니다.



ID 및 패스워드를 입력하면 정상적으로 로그인 됩니다.

① User ID 이메일 형식으로 입력
② Password 9 자 이상의 문자열, 영문 대소문자포함, 특수문자 포함

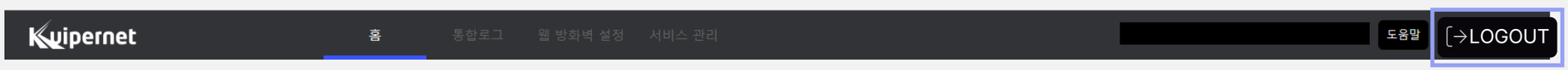
* 로그인 5 회 연속 실패 시 10 분간 접속이 차단됩니다.

I. 로그인

1-2. 로그아웃

로그아웃

관리 웹 접속에서 정상 로그 아웃을 진행합니다.



세션 타임 아웃

사용자가 로그인 후 활동을 하지 않으면 10 분(600 초) 이후 자동 로그아웃이 되며 해당 이력은 감사로그에 남도록 되어 있습니다.

II. 홈 메뉴

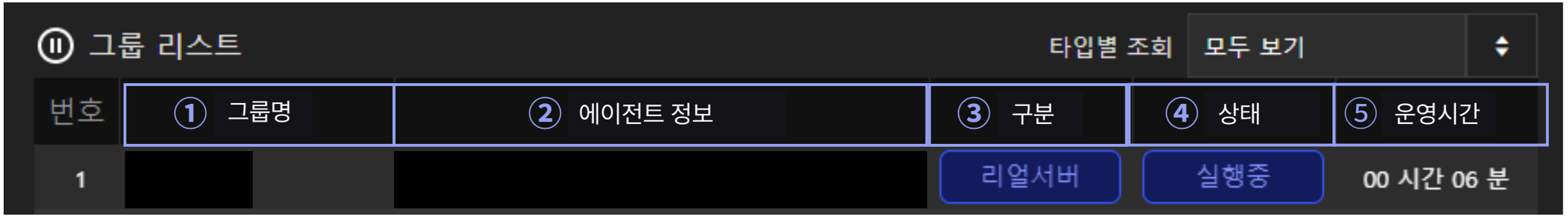
2-1. 통합 에이전트 상태

관리가 가능한 전체 그룹 리스트 및 도메인 리스트 정보, 에이전트 상태를 확인할 수 있습니다.

II. 홈 메뉴

2-2. 그룹 리스트

등록된 그룹 리스트가 표시됩니다.



① 그룹 명 등록한 서버 명이 표시됩니다. 선택하면 아래 도메인 리스트가 표시됩니다.

② 에이전트정보 동일 서버 여러 개 등록 시 각 서버의 Mac 정보로 표시됩니다.
클라우드 환경의 오토 스케일링 사용시 동일 그룹으로 여러 에이전트가 표시됩니다.

③ 구분 리얼 서버와 오토 스케일서버를 구분하여 표시됩니다.

④ 상태 현재 기준 요청 정보, 공격기록 전송을 기준으로 실행 중, 의심, 다운으로 표시됩니다.

⑤ 운영시간 에이전트가 기동 되어 운영되고 있는 시간대를 표시됩니다.

II. 홈 메뉴

2-3. 도메인 리스트

그룹 리스트에서 리스트를 클릭하면 도메인 리스트에 선택된 그룹 리스트 안에
등록된 도메인 리스트가 표시됩니다.

① **Source**	등록한 도메인 정보
② **Target**	등록된 도메인의 요청을 보낼 목적지 정보
③ **날짜**	등록 일자
④ **바로이동**	웹 방화벽 설정 화면으로 이동

* 한 개의 그룹에는 여러 개의 도메인 등록이 가능합니다.
* 그룹 리스트에 선택한 그룹에 등록된 모든 도메인 리스트가 표시됩니다.
* 리스트의 도메인 선택 시, 해당 도메인의 보안 룰셋 설정이 에이전트 상태에 표시됩니다.

II. 홈 메뉴

2-4. 에이전트 상태

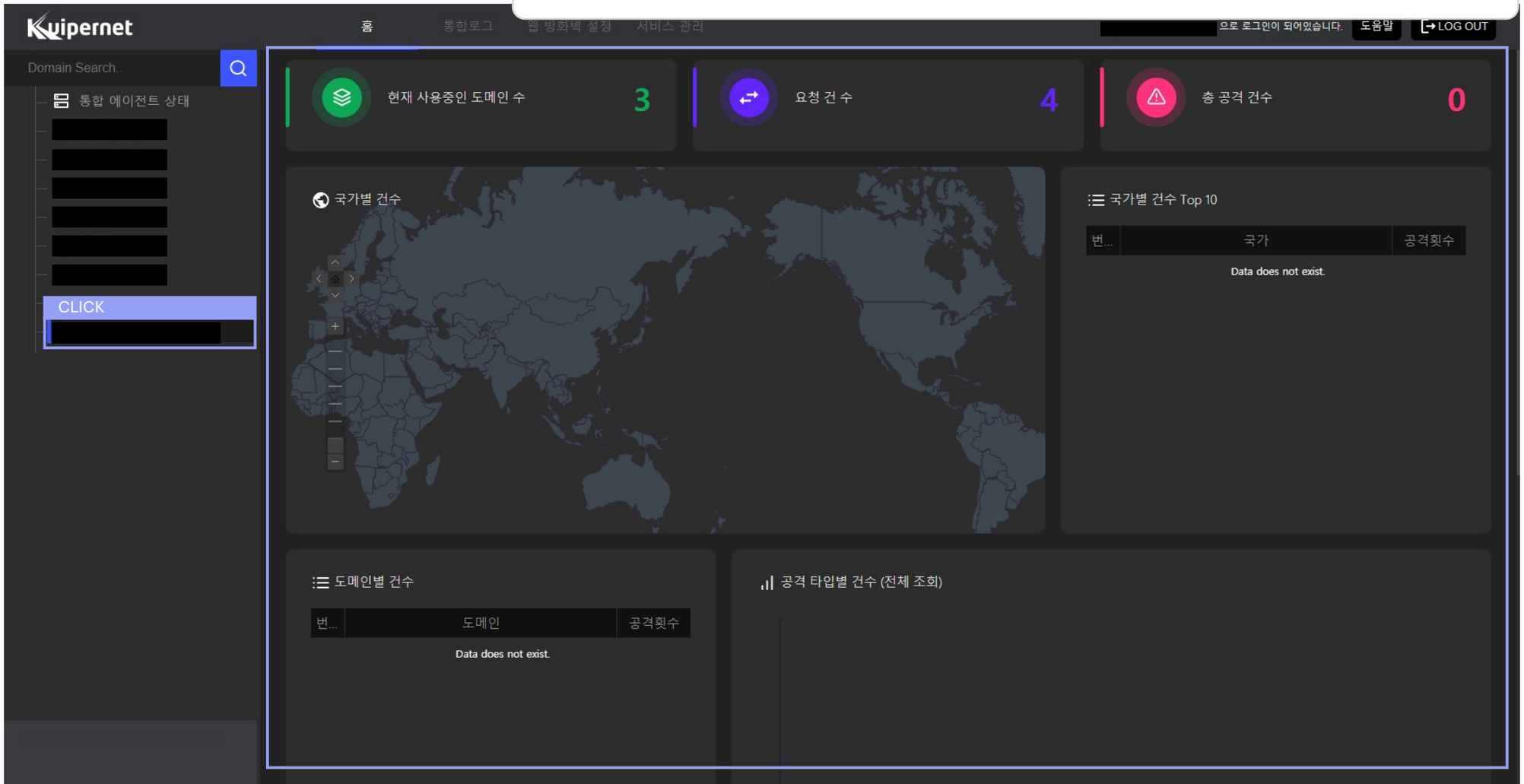
도메인 리스트에서 리스트를 클릭하면 에이전트 상태에 선택된 도메인 리스트 안에 설정된
보안 룰셋의 상태를 확인할 수 있습니다.

II. 홈 메뉴

2-5. 개별 에이전트

좌측 트리 메뉴의 도메인을 선택하면 대시보드에서 현재 사용 중인 도메인 수, 도메인 요청 건수,
총공격 건수 및 공격 현황을 확인할 수 있습니다.

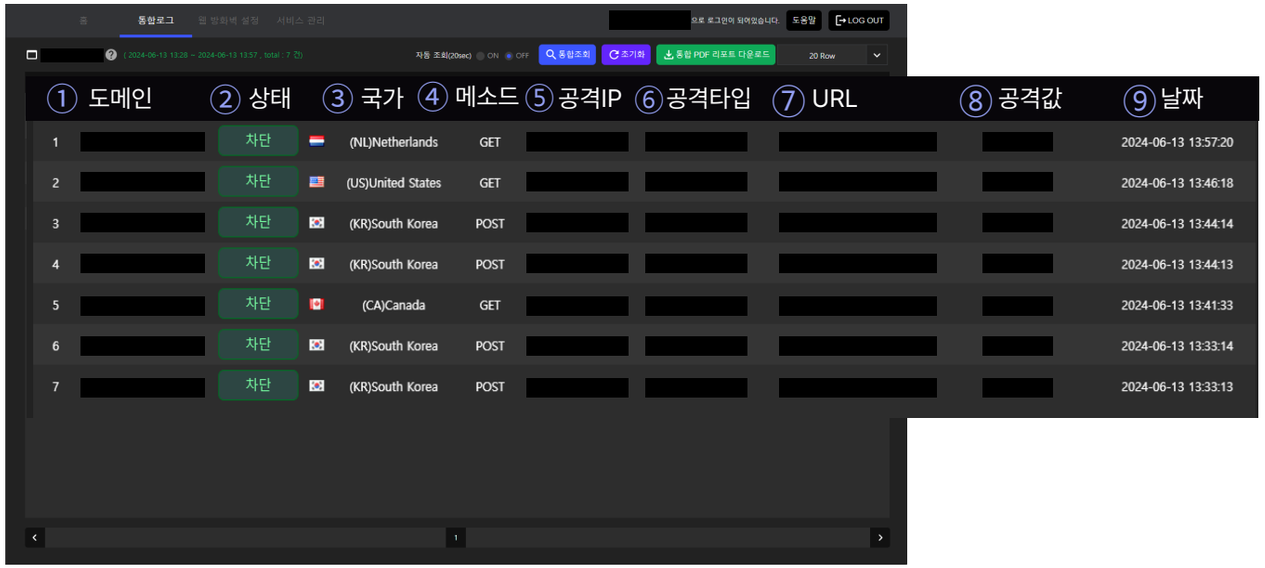
대시 보드 : 트래픽 사용량 및 공격 타입 및 국가별 공격 건수, 요청 건수, 최근 12 시간의 데이터를 가져옵니다.



III. 통합 로그

3-1. 대시 보드

통합 로그 화면에서는 보안 정책에 의해 탐지 및 차단 된 로그 기록을 확인할 수 있고, 다양한 검색 조건으로 조회할 수 있습니다.



① **도메인**	도메인 정보 표시
② **상태**	보안 설정에 따라 차단 되었는지 모니터링만 된 것인지 확인
③ **국가**	공격 IP 분석 국가 표시
④ **메소드**	요청 메소드 정보
⑤ **IP**	공격 IP 정보
⑥ **공격 타입**	위배된 보안 룰셋 정보 표시 여러 보안 룰셋에 위배된 공격 데이터도 최초 발견 룰셋만 표시
⑦ **URL**	공격 URI 표시
⑧ **공격 값**	위배된 공격 값 표시
⑨ **날짜**	공격 년,월,일,시,분,초로 표시

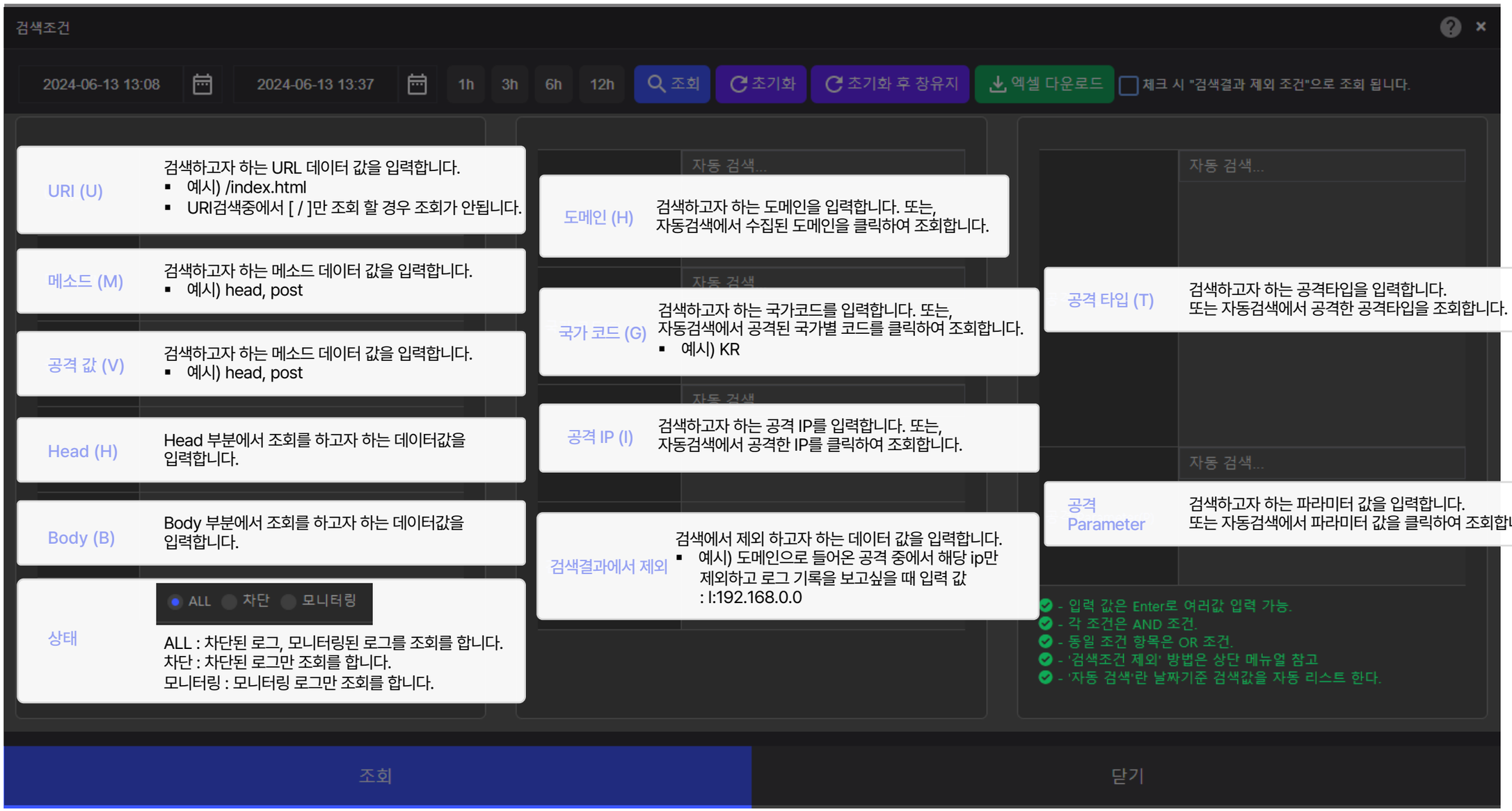
로그	기본적으로 30 분 동안 표시되며, 원하는 날짜/시간으로 정보를 볼 수 있습니다.
자동 조회(20sec)	ON / OFF는 ON으로 설정 할 경우 20초 마다 로그 기록이 갱신되어 보여줍니다.
통합조회	도메인,공격 IP, URI, 공격국가, 메소드 검색을 할 수 있습니다.
초기화	검색한 화면에서 처음으로 되돌아 갈 때 사용합니다.
통합 PDF 리포트 다운로드	웹 방화벽 설정 및 보안 정책에 의한 차단 및 탐지된 이력을 통계하여 보고서 형태로 보여줍니다.

IP 기반 검색
국가별 및 개수
공격 유형 및 횟수
공격 세부 정보

III. 통합 로그

3-2. 수동 로그 조회

통합조회 버튼을 클릭하면 수동 로그 조회 팝업창이 열립니다.



III. 통합 로그

3-3. 자동 로그 조회

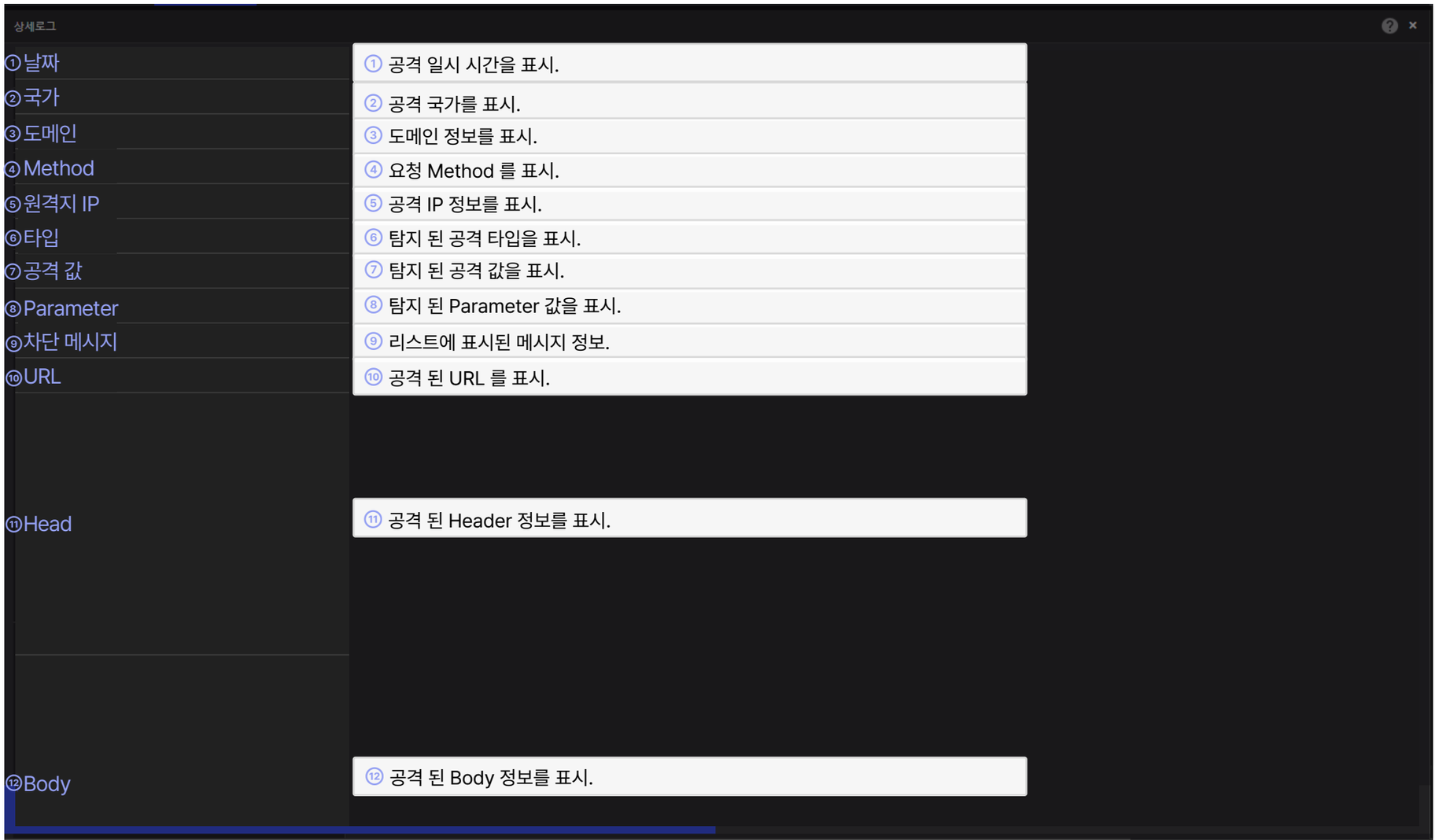
공격 리스트에서 마우스 오른쪽 클릭하면 화이트 IP 등록 / 블랙 IP 등록 / 예외처리 등록 및 현재 클릭된
리스트의 PDF 리포트를 다운로드 기능을 사용 가능하고,
공격 리스트에서 해당 검색 조건들을 추가 / 추가 후 조회 / 제외 후 조회를 할 수 있습니다.

III. 통합 로그

3-4. 상세 로그

탐지된 로그를 상세하게 보고 싶을 때 탐지된 리스트에서 해당 항목을 더블 클릭하게 되면 상세보기 팝업 창이 나옵니다.

* 예외 등록 : 해당 로그가 정상적인 데이터일시 예외 등록 버튼을 클릭하시면
자동으로 웹 방화벽 설정에서 보안 룰셋 오류 예외 처리에 등록됩니다.



IV. 웹 방화벽 설정

4-1. 대시보드

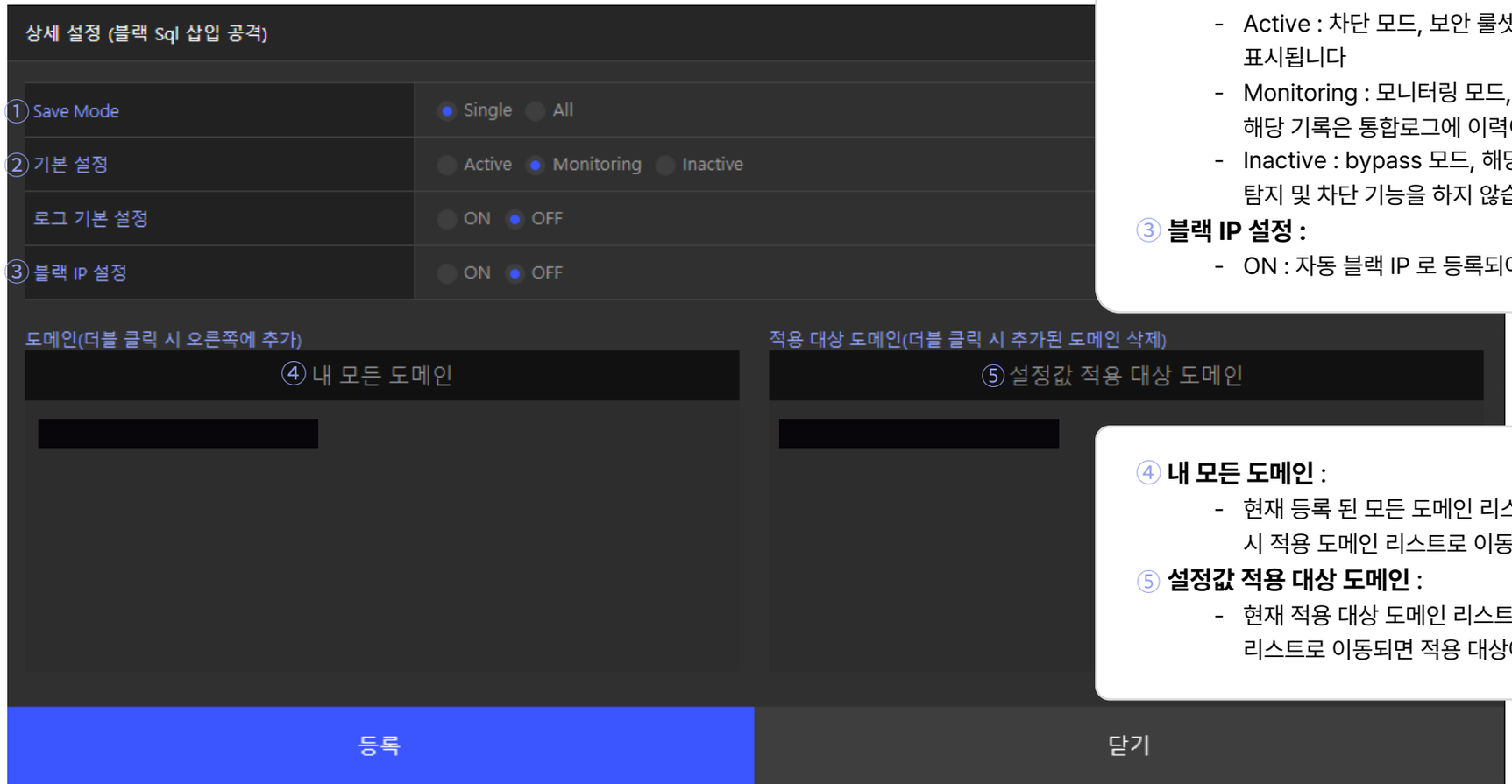
웹 방화벽 설정 화면에서는 탐지 상태 설정 및 기본 제공하는 보안 패턴 이외에
추가로 사용자가 차단하고자 하는 보안 패턴을 설정할 수 있습니다.

① **에이전트 수신 상태**	웹 방화벽 보안 설정 값이 Agent에 정상적으로 동기화 되었는지 상태를 알려줍니다.
② **명칭**	기본 제공하는 보안 패턴을 보여줍니다.
③ **보안 룰셋**	웹 방화벽 보안 항목별 정책이 구성되어 있습니다.
④ **탐지 상태 설정**	탐지상태가 현재 차단 모드인지 모니터링 모드인지 확인 할 수 있습니다.
⑤ **로그 수집 설정**	보안 룰셋 별로 로그 기록을 ON/OFF 할 수 있으며 OFF 할 경우 해당 기록은 남지 않습니다.
⑥ **블랙 IP 등록 설정**	블랙 IP 등록의 활성화/비활성화 상태를 확인 할 수 있습니다.
⑦ **룰셋 RESTORE**	이전에 적용된 보안 룰셋 데이터를 복구 처리됩니다.

IV. 웹 방화벽 설정

4-2. 탐지 상태 설정

웹 방화벽 설정 화면에서는 탐지 상태 설정 및 기본 제공하는 보안 패턴 이외에
추가로 사용자가 차단하고자 하는 보안 패턴을 설정할 수 있습니다.



① **Save Mode :**
- Single : 선택한 한 개의 도메인에 보안 룰셋을 적용합니다.
- All : 등록된 모든 도메인에 보안 룰셋을 적용합니다.

② **기본설정 :**
- Active : 차단 모드, 보안 룰셋에 위배되면 차단 되며 통합로그에 차단으로 표시됩니다
- Monitoring : 모니터링 모드, 보안 룰셋에 위배되어도 정상 응답 되며 해당 기록은 통합로그에 이력이 남으며 모니터링으로 표시됩니다.
- Inactive : bypass 모드, 해당 보안 룰셋을 중지 합니다. bypass 되며 탐지 및 차단 기능을 하지 않습니다.

③ **블랙 IP 설정 :**
- ON : 자동 블랙 IP 로 등록되어 해당 IP 는 정상 요청도 차단됩니다.

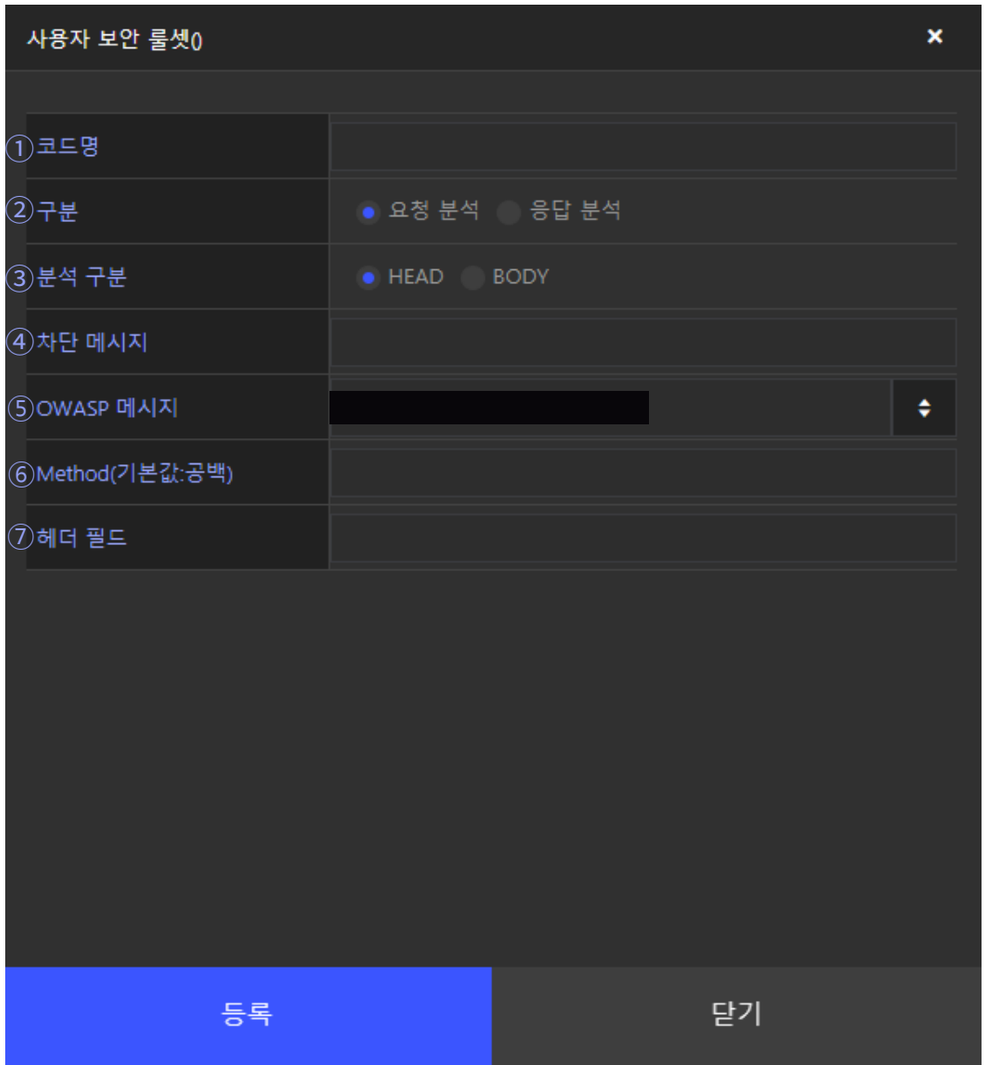
④ **내 모든 도메인** :
- 현재 등록 된 모든 도메인 리스트가 표시된다. 적용 할 도메인을 더블 클릭 시 적용 도메인 리스트로 이동됩니다.

⑤ **설정값 적용 대상 도메인** :
- 현재 적용 대상 도메인 리스트 더블 클릭 시 해당 도메인은 전체 도메인 리스트로 이동되면 적용 대상에서 제외됩니다.

IV. 웹 방화벽 설정

4-3. 사용자 보안 룰셋 등록

제공 하는 기본 룰 셋 외 사용자자가 직접 정의하여 룰 셋 추가 하는 기능입니다.
보안 룰 셋을 추가 하면 해당 정의 이름으로 탐지되어 통합 로그에 표시됩니다.

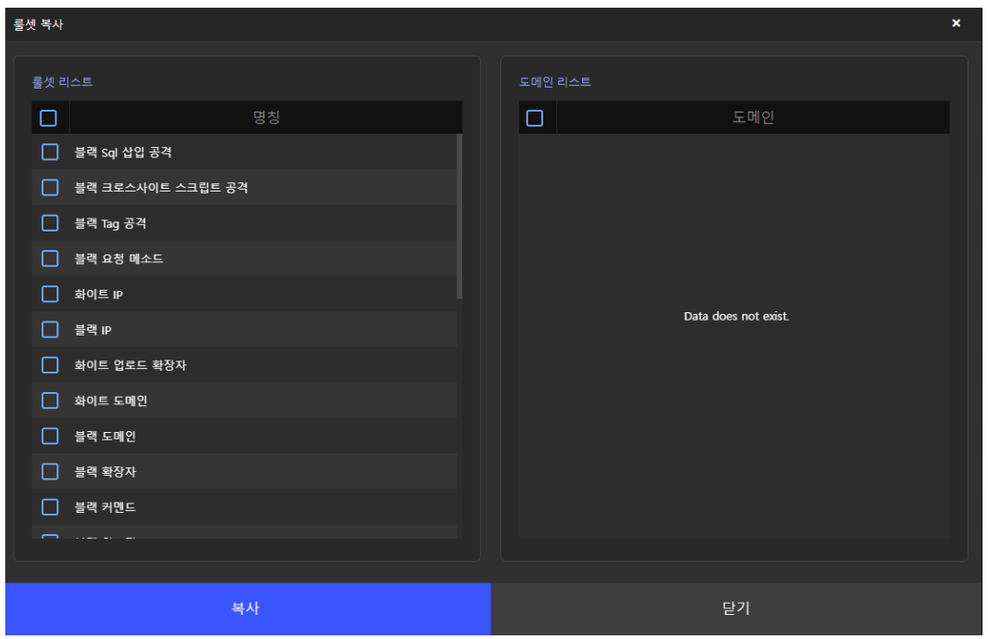


① **코드명**	사용자 룰셋 명칭을 입력 합니다.
② **구분**	HTTP 로 들어오는 요청 및 응답에 대하여 분석할 부분을 체크 합니다.
③ **분석 구분**	HTTP 로 들어오는 정보 중에서 분석할 부분을 체크 합니다.
④ **차단 메시지**	사용자가 설정한 룰셋에 의해 차단 메시지를 설정 합니다.
⑤ **OWASP 메시지**	사용자 등록 룰셋으로 차단 될 경우 OWASP 메시지 설정
⑥ **Method(기본값:공백)**	Method 부분 설정 기본값은 공백 입니다.
⑦ **헤더 필드**	설정한 헤더 필드 값을 감시합니다.

IV. 웹 방화벽 설정

4-4. 룰셋 복사

서비스 운영/관리를 효과적으로 하기위한 기능으로, 이미 보안 룰셋이 설정되어있는
도메인의 룰셋을 그대로 복사하여 다른 도메인에 적용 하는 기능 입니다.



1. 좌측 트리 메뉴에서 복사 하고자 하는 도메인을 선택 후 룰셋 복사 버튼을 클릭합니다.

2. 복사 하고자 하는 룰셋을 선택 체크합니다.

3. 복사 대상이 되는 도메인을 선택 체크합니다.

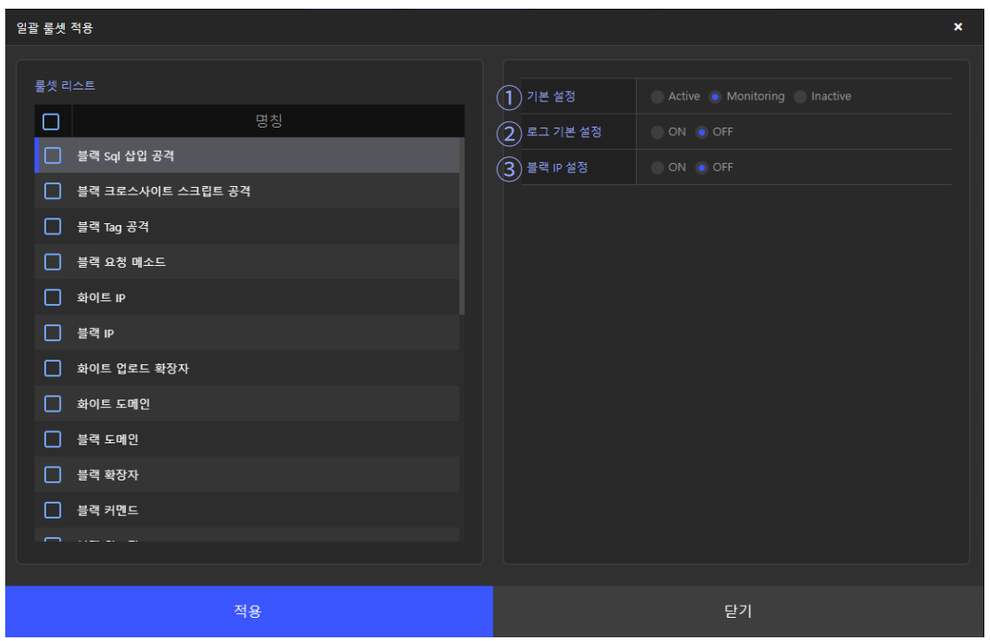
4. 복사 버튼을 클릭하면 해당 룰셋이 복사됩니다.

5. 전체 복사 또는 일부 보안 룰셋을 선택하여 복사 가능합니다.

IV. 웹 방화벽 설정

4-5. 일괄 룰셋 적용

각각의 보안 항목에 대하여 전체 설정 값을 변경할 수 있습니다.



① **기본 설정**

- **Active**
  - 차단 모드를 활성화합니다.
  - 보안 정책에 위배된 요청은 차단합니다.
  - 차단된 요청 정보는 웹 방화벽 모니터링 로그에서 확인합니다.
- **Monitoring**
  - 모니터링 모드로 활성화합니다.
  - ※ 보안 정책에 위반한 요청 정보는 모니터링 로그에서 확인이 가능하지만 차단 기능은 없습니다.
  - 모든 요청 정보의 내용과 분석 결과를 모니터링 로그에 남깁니다.
  - 일정 기간 웹서버의 요청 정보를 수집하여 악의적인 공격 요청이나 정상 요청을 구분하여 알맞은 보안 정책 설정을 위해 사용하는 기능입니다.
- **InActive**
  - 웹 방화벽 기능을 중지합니다.
  - 설정된 모든 정책/기능이 중지합니다.
  - ※ 차단도 안 하고 로그도 남기지 않습니다. (By-pass)

② **로그 기본 설정**

- On 모니터링 로그 기록을 남깁니다.
- Off 모니터링 로그를 남기지 않습니다.

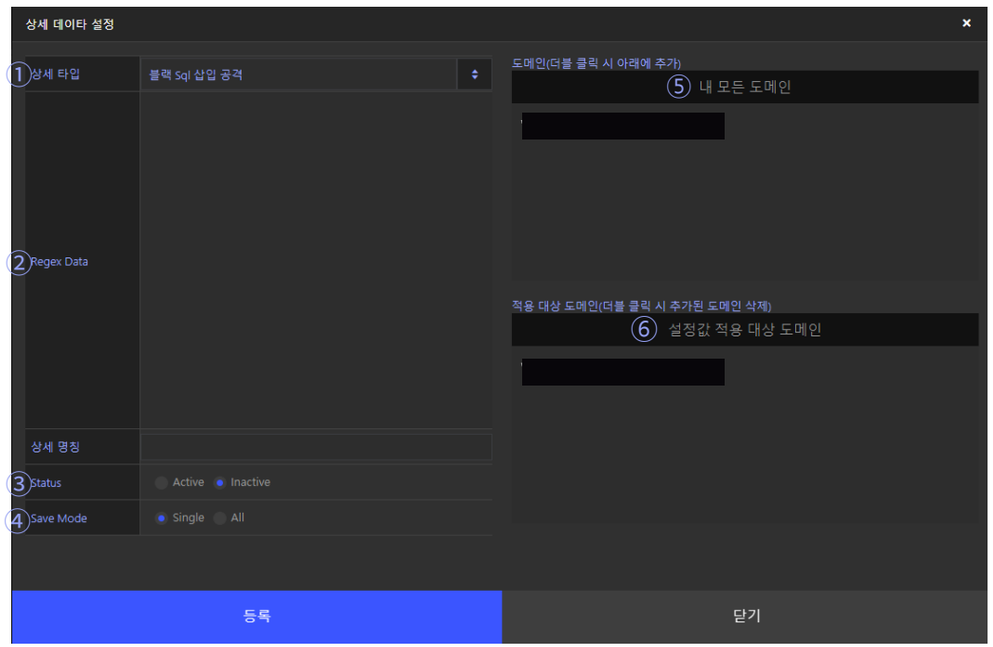
③ **블랙 IP 설정**

- On 해당 룰셋으로 들어오는 공격 IP 에 대하여 자동으로 블랙 IP 로 등록합니다.
- Off 해당 룰셋으로 들어오는 공격 IP 에 대하여 블랙 IP 로 등록하지 않습니다.

IV. 웹 방화벽 설정

4-6. 보안 룰셋 등록

웹 방화벽 보안 항목별 정책이 구성되어 있습니다.
각 보안 항목별로 사용자 직접 정책을 등록, 수정, 삭제가 가능합니다.



① **상세 타입**
- 등록할 상세 보안 항목을 선택할 수 있습니다.

② **Regex Data**
- 등록하고자 하는 룰셋을 등록합니다.
- 형식은 Text 또는 Java 정규식을 포함합니다.

③ **Status**
- Active : 차단 모드 입니다.
- Monitoring : 모니터링 모드 입니다.

④ **Save Mode**
- Single : 현재 선택된 도메인에만 등록 합니다.
- All : 등록된 모든 도메인에 등록 합니다.

⑤ **전체 도메인**
- 현재 등록 된 모든 도메인 리스트가 표시됩니다.
- 적용 할 도메인을 더블 클릭 시 적용 도메인 리스트로 이동됩니다.

⑥ **적용 도메인**
- 현재 적용 대상 도메인 리스트 입니다.
- 더블 클릭 시 해당 도메인은 전체 도메인 리스트로 이동되면 적용 대상에서 제외된다.

V. 보안 패턴

5-1. 블랙 SQL 삽입 공격

- **보안 룰셋**

  공격 난이도가 쉬워 가장 많이 시도 되는 공격입니다.
  또한 가장 많은 피해를 입히고 있습니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-2. 블랙 크로스사이트 스크립트 공격

- **보안 룰셋**

  XSS(크로스사이트스크립트)는 스크립트 (JavaScript, VBScript, Flash, ActiveX, XML/XSL, DHTML 등)삽입 공격을 하여 피해를 발생시키는 공격입니다. 또한, 공격 방식이 다양한 형태로서, 다른 공격들과 혼합 형태로 많이 이용되어 그 위험성과 피해가 매우 큰 해킹 기법입니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-3. 블랙 Tag 공격

- **보안 룰셋**

  XSS 변형 형태로 각종 태그를 활용한 공격입니다.
  피싱, 파밍 공격에 많이 활용됩니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-4. 블랙 요청 메소드

- **보안 룰셋**

  HTTP 요청가운데 GET, POS 를 제외한 Method 를 기본 차단합니다.
  - PUT/DELETE 메서드가 허용된 경우 소스 수정, 삭제가 가능해 심각한 피해가 발생됩니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-5. 화이트 IP

- **보안 룰셋**

  특정 IP 를 화이트 IP 에 등록하면, 해당 IP 는 모든 차단 정책에서 제외되는 기능입니다.
  - IP 기반으로 접근을 제어합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-6. 블랙 IP

- **보안 룰셋**

  특정 IP 를 블랙 IP 에 등록하면, 해당 IP 를 통한 접근을 모두 차단하는 기능입니다.
  - 공격 기록에서 바로 블랙 IP 등록이 가능합니다.
  - 블랙 IP 등록 시 모니터링 모드에서 차단됩니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-7. 화이트 업로드 확장자

- **보안 룰셋**

  등록된 파일 확장자 목록 기반으로 등록되지 않은 파일에 대한 업로드를 차단하는 기능입니다. 기본적으로 화이트 업로드 확장자에 등록하지 않은 모든 파일의 생성(복사, FTP, 업로드)을 차단합니다. 이는 치명적인 피해를 줄 수 있는 트로이목마, web shell 등과 같은 실행 코드의 유입을 막고자 하기 때문입니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-8. 화이트 도메인

- **보안 룰셋**

  화이트 도메인에 특정 도메인을 등록하면, 요청 HTTP Header 중 referer header 의 값을 검사하여 해당 도메인을 경유한 요청을 모든 접근을 허용합니다. 입력 예시는 다음과 같습니다. http://www.test.com(X), www.test.com(o)

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-9. 블랙 도메인

- **보안 룰셋**

  블랙 도메인에 특정 도메인을 등록하면, 해당 도메인을 경유한 모든 요청을 차단합니다.

  - 블랙 리스트 정책으로 해당 도메인을 통한 모든 접근을 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-10. 블랙 확장자

- **보안 룰셋**

  웹 서버의 내부 파일에 대한 접근 권한이 잘못되어 있을 경우 악의적인 접근으로 인한 피해를 입을 수 있습니다.
  URL 검사 기반으로 URL 의 확장자를 검사하여 등록된 확장자의 접근을 차단합니다.
  요청하지 말아야 하는 블랙 확장자 리스트가 기본적으로 등록 되어있습니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-11. 블랙 커맨드

- **보안 룰셋**

웹 서버를 통하여 OS 명령어를 실행하는 공격을 차단하는 기능입니다.

- 요청 URL 을 검사하여 OS shell 명령어를 탐지하면 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-12. 블랙 인코딩

- **보안 룰셋**

요청 URL 검사하여 변환된(인코딩) 문자열을 통한 공격을 탐지하여 차단합니다.
Encoding 된 문자열 요청을 허용해 줄 경우의 문제점은 해커들이 SQL Injection /XSS 공격을 시도할 시 IDS/IPS/WAF 등의 보안 장비를 우회하기 위해서 공격 구문을 인코딩하여 요청합니다.
코딩 된 공격 문자열을 통해 웹 서버의 오류를 유발하고 오류 응답 값을 통해 대상 웹 서버의 취약점을 찾아내어 해킹을 시도합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-13. 블랙 명령 실행

- **보안 룰셋**

  웹 서버 요청 데이터에 포함시켜 명령어를 실행하는 공격 방식을 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-14. 블랙 프로딩

- **보안 룰셋**

  요청 URL 검사를 통한 풋프린트 및 웹 프로브 시도의 정보 공개를 방지합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-15. 블랙 코드 삽입

- **보안 룰셋**

이미 웹 서버에 상주한 악의적인 WebShell 을 실행하지 못하게 하는 기능입니다.

- WebShell 에 주로 사용되는 POST 파라미터 값이 기본적으로 등록 되어있습니다.
- POST 파라미터에 등록된 정책의 값이 넘어오면 차단합니다.
- POST 차단 방법 HTTP body 데이터에 WebShell 을 컨트롤 하기 위한 파라미터 값을 가지고 접근을 시도할 경우, 이를 감지하고 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-16. 블랙 윈도우 디렉터리 및 파일

- **보안 룰셋**

서버 정보, 백업 파일, 환경 설정 파일, 기본 샘플 페이지, 데이터를 획득하기 위한 웹 서버 요청 데이터를 통한 공격을 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-17. 블랙 단어

- **보안 룰셋**

자동 글 등록 봇 또는 악성 유해 글(게임, 욕설, 광고)을 차단하기 위한 기능입니다.

- 관리자가 지정 단어를 등록하여 차단합니다.
- POST 파라미터로 넘어오는 값만 필터링이 가능합니다.
- GET 파라미터는 검사를 하지 않습니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-18. 블랙 에이전트

- **보안 룰셋**

User-agent 라는 헤더 필드를 통해 전달되는 웹 크롤러와 같은 봇을 차단합니다.

- 관리자가 지정 웹 크롤러와 봇을 등록하여 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-19. 블랙 민감 정보

- **보안 룰셋**

  응답 데이터 주민번호, 전화번호, 카드 번호와 같은 주요 개인정보가 포함 된 데이터가 있으면 차단됩니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

5-20. 블랙 SSRF

- **보안 룰셋**

  서버의 직접적인 접근이 제한된 서버의 자원에 접근하여 외부로 데이터 유출 및 서버 오동작을 유발하는 공격을 차단합니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

V. 보안 패턴

5-21. 화이트 URL 접근

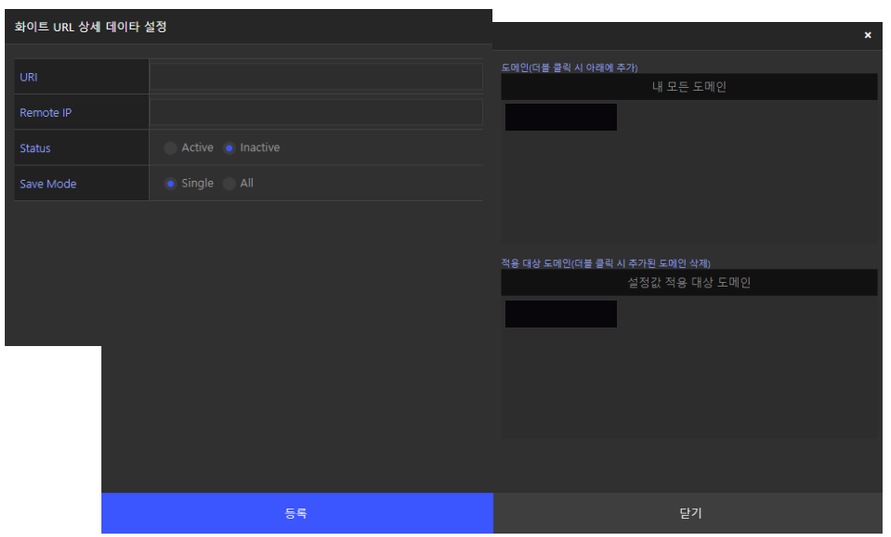
특정 URL에 대하여 사용자 접근을 허용합니다.
특정 URL에 특정 IP 만 접근할 수 있도록 설정할 수 있습니다.

필터 대상

구분	설명
Method	GET, POST
URI	모든 항목
Headers	모든 항목
Body	모든 항목
위험 등급	상

- 등록

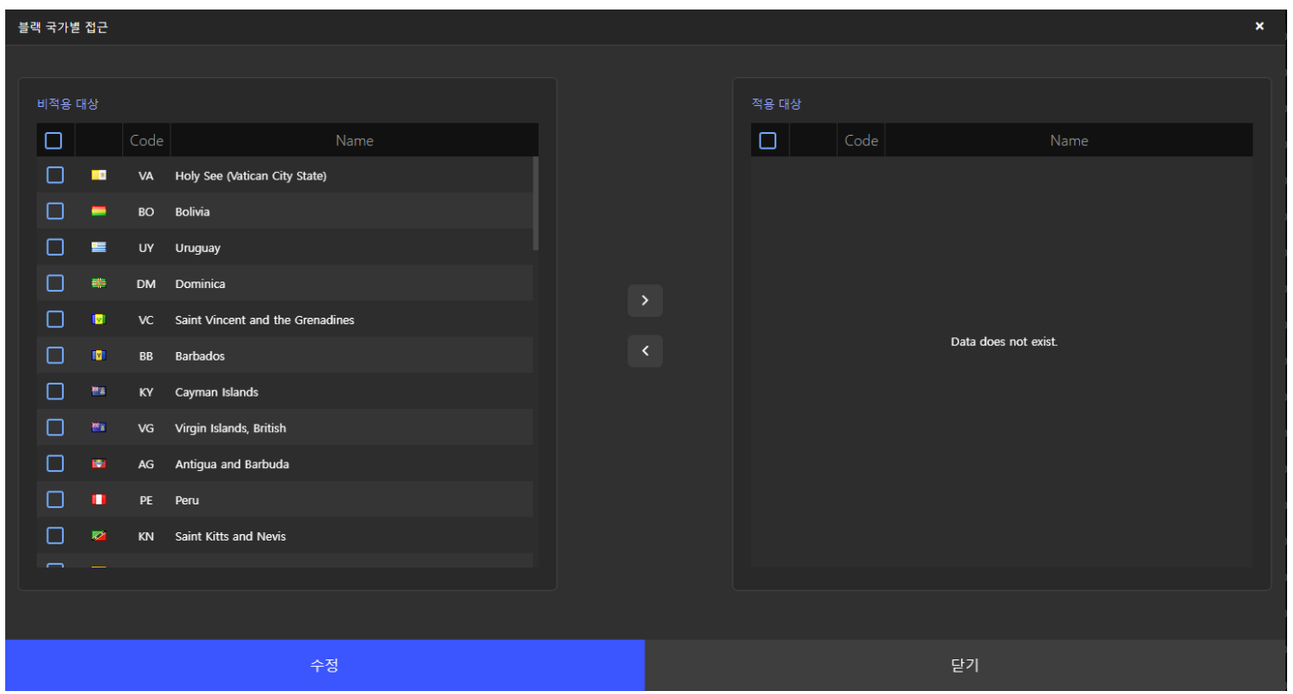
1. **URL** : 접근을 허용할 URI 를 입력합니다.
2. **Remote IP** : 입력한 URI 의 접근을 허용 할 IP 를 입력합니다.
3. **Status** : 기본 설정 차단(Active)/ 기능 중지(InActive)를 선택합니다.
   (활성화 : Active, 비활성화 : Inactive)
4. **Save Mode** : 보안 룰셋 적용 대상 도메인을 선택합니다.
   (single : 선택한 도메인만 적용, All : 등록된 도메인 전부 적용)



V. 보안 패턴

5-22. 블랙 국가별 접근

접근을 차단 및 허용할 해외 국가를 선택합니다.
요청 정보를 통해 해외에서 원치 않은 접근이 확인된 경우 특정 국가의 접근을 차단할 수 있습니다.



1. **비적용 대상** : 허용할 해외 국가
2. **적용 대상** : 차단할 해외 국가

GlobalHost

TEL 02-6091-1180 (내선1)
MAIL sales@kcinfra.co.kr
WEBSITE www.globalhost.co.kr

WAF 보안 관련 서비스

글로벌 웹방화벽 서비스
https://www.globalhost.co.kr/waf_service

24시 보안관제 서비스
https://www.globalhost.co.kr/global_security