BOOTER 개발 프로젝트

관리자 매뉴얼 – 시스템 운용과 관리

발주처 : ㈜제넷 시큐리티

시행처 : (주)심포니소프트

완료일자: 2016.12.09

Document History			
버젼	일자	작성내용	작성자
1.0	2016.9.20	초기작업 내용	김호익
1.1	2016.10.28	추가 작업 내용	김호익
1.3	2016.12.9	마무리 작업 내용 추가	김호익

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 서버관리->서버	작성일 : 2016-12-09
개별 서버 전체 헬스 항목 체크			연결용도 :

ETRONIC

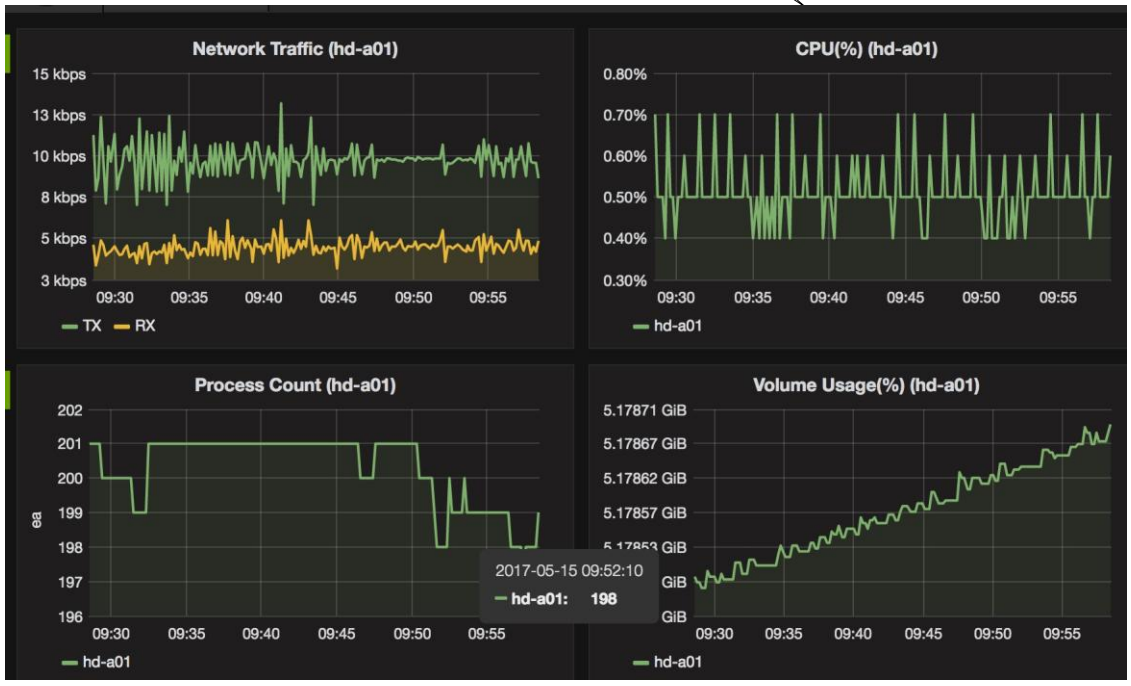
	서버 아이디	서버명	카테고리	Public IP	Net
	hd-a01	공격서버-01	1. 공격 -- California 2. 공격	23.229.98.66	eth
	hd-a03	공격서	1. 공격 -- California	23.250.125.186	eth

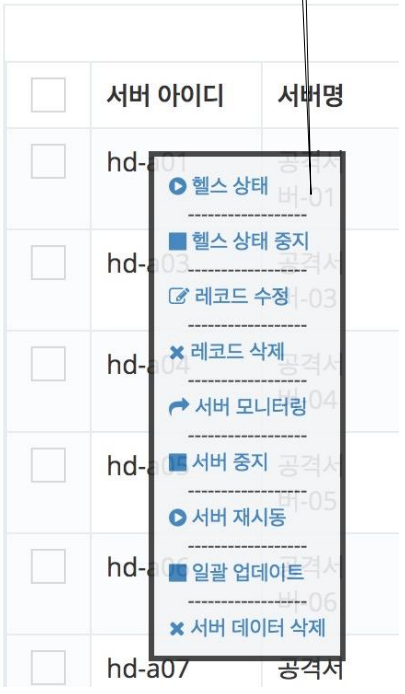
(1)먼저 특정서버를 선택한 후

(2)우측마우스로 클릭하면

"서버 모니터링"을 선택하면

(3)특정서버에 대한 모든 헬스 체크 정보를 웹브라우저의 다른 팝업 페이지로 보여준다.





진행설명설명

1.그라파나을 이용한 서버 헬스 방법을 알아본다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발		작성일 : 2016-12-09
서버 카테고리 헬스 체크			연결용도 :

진행설명설명

1.그라파나을 이용한 서버 헬스 방법을 알아본다.

특이사항

ETRONIC

	서버 아이디	서버명	카테고리	Public IP
✓	hd-a01	공격서버-01	1. 공격 -- California 2. 공격	23.229.98.66
✓	hd-a03	공격서버-03	1. 공격 -- California 2. 공격	23.250.125.186
✓	hd-a04	공격서버-04	1. 공격 -- California 2. 공격	138.128.117.170

(1)먼저 서버의 카테고리를 필터링을 통하여 선택하여 체크 마크 한 후

(2)우측마우스로 클릭하면

헬스 체크 항목을 선택하면

(3)각 항목에 대한 체크된 모든 서버에 대한 헬스 체크 정보를 웹브라우저의 다른 팝업 페이지로 보여준다.

실행 비교

- Network
- CPUs
- Memory
- Process
- Volumes
- DB Access

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 :이벤트 관리 -> 이벤트	작성일 : 2016-12-09
이벤트 관련 서버 헬스 체크			연결용도 :

진행설명설명

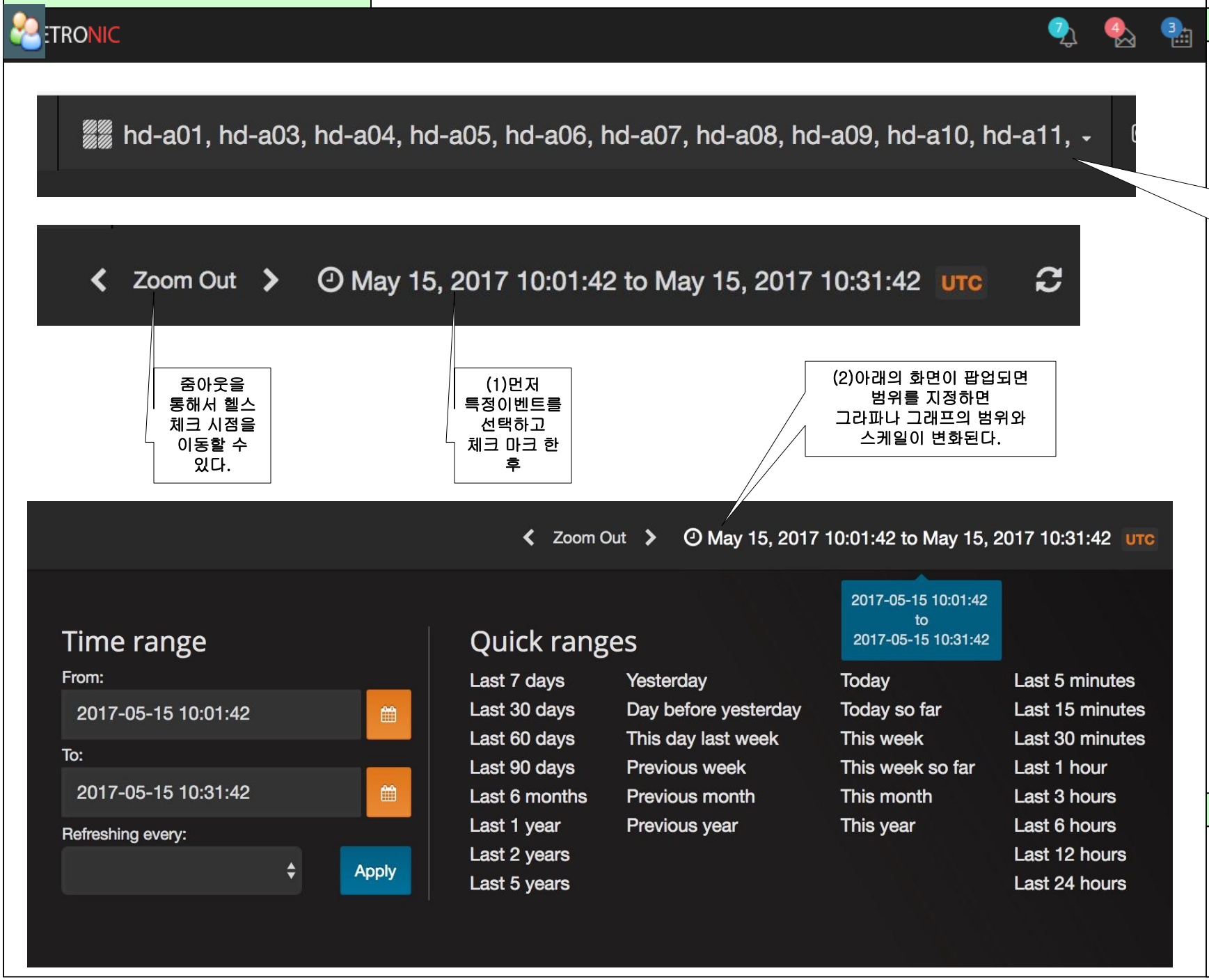
1.그라파나을 이용한 서버 헬스 방법을 알아본다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 :이벤트 관리 -> 이벤트	작성일 : 2016-12-09
일자 범위별 서버 헬스 체크			연결용도 :

진행설명설명

1.그라파나을 이용한 서버 헬스 방법을 알아본다.



특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 대시보드	작성일 : 2016-12-09
대시보드			연결용도 :

서버수 합계	사용자수 합계	탐색 보고서 개수	이벤트 개수

(1)상세 보고서보기

새 서버				
등록시간	서버아이디	카테코리	서버명	IP
년월일시	s01	탐색	탐색-1	125.209.222.141
년월일시	a02	공격	공격-2	125.209.222.142

새 보고서				
등록시간	보고서아이디	대상서버	보기	IP
년월일시	1234	s01	미리보기	125.209.222.141
년월일시	1235	a01	미리보기	125.209.222.142

통제서버 네트워크 상황	통제서버 CPU 상황
통제서버 Memory 상황	통제서버 Process 상황
통제서버 Volumn 상황	통제서버 DB 상황

진행설명설명

1. Booter 서버 상황과 탐색 공격 진행 사항을 전체를 보여준다.

2. 탐색보고서를 미리보기하면 탐색했던 상화의 상세 내용을 보여준다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 보고서 -> 탐색 보고서	작성일 : 2016-12-09
탐색 보고서			연결용도 :

보고서 추가 | 실행 ▼ | 검색창 | 검색하기

☐	이벤트아이디	대상서버-id	탐색서버-id	보기	상태	시작 시간	종료 시간	다운로드
☐	es-161023-01	s-161003-01	s-161003-01	미리보기	대기중	년월일시	년월일시	다운로드
☐	ea-161023-01	홍길동	홍길동	미리보기	공격중	년월일시	년월일시	다운로드

(1)선택하고

(2)우측마우스로 클릭하면

레코드 수정

레코드 삭제

(3)클릭하면

보고서 미리보기

(4)클릭하면

보고서 다운로드

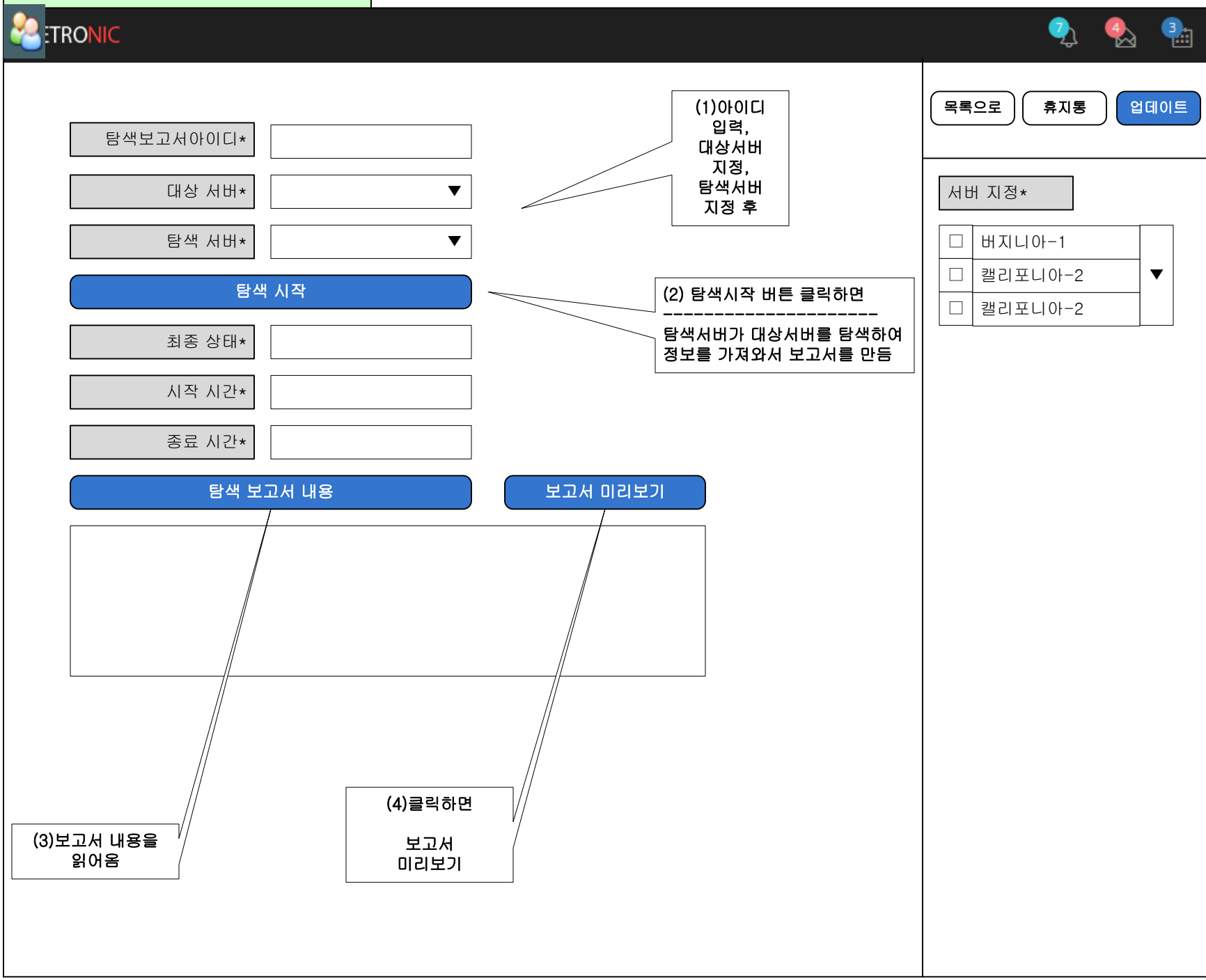
(이전) 1 2 3 4 5 6 7 8 9 10 (다음)

진행설명설명

1. 작성된 탐색보고서를 확인하고 필요시 다운로드 한다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 보고서 -> 새 탐색 보고서	작성일 : 2016-12-09
새탐색 보고서			연결용도 :



진행설명설명

(1) 탐색보고서 아이디는 임의로 지정한다.
(2) 탐색시
1. NMAP scan 통하여 대상서버가 running 되고 있는지 여부를 확인한다.

특이사항

UI는 뒷장에 첨부된 서버등록 참조 이미지를 참조한다..

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 이벤트 관리 -> 이벤트	작성일 : 2016-12-09
이벤트			연결용도 :

이벤트 추가 | 실행 ▼ | 검색창 | 검색하기

필터링 OFF | 필터링 ON | 필터링할 카테고리를 선택해 주세요. ▼ | 검색창 | 검색하기

☐	이벤트아이디	이벤트명	이벤트카테코리	공격종류	pps	실행서버	대상서버-id	서버상태	이벤트상태	시작종료
☐	es-161023-01	dasfdsaf	탐색	ICMP	10000	Hd-a01외 23	s-1613-01	On	대기중	~
☐	ea-161023-01	sdfaaf	공격	TCP_SYN	500000	Hd-a01외 23	홍길동	Off	대기중	~

(1)선택하고

(2)우측마우스로 클릭하면

탐색중지

공격중지

탐색 재시작

공격 재시작

레코드 수정

레코드 삭제

Network 비교

CPU 비교

Memory 비교

Process 비교

Volumn 비교

DB Access 비교

대상 서버 상태

****
(1) 선택이전에 서버의 카테고리를 필터할 수 있다.

****
(1) 선택이전에 검색으로 표시 서버를 필터할 수 있다.

(이전) 1 2 3 4 5 6 7 8 9 10 (다음)

진행설명설명

1. 모니터링 시작과 중지 명령은 해당화면에서 수행된다.

2. 탐색/공격과 같은

3. 실행 내용
 탐색중지: 탐색진행중 내용 중지
 공격중지: 공격진행중 내용 중지
 탐색재시작: 중지 내용 재개
 공격재시작: 중지내용 재개

 레코드 수정: 해당 레코드 수정
 레코드 삭제: 해당 레코드 삭제

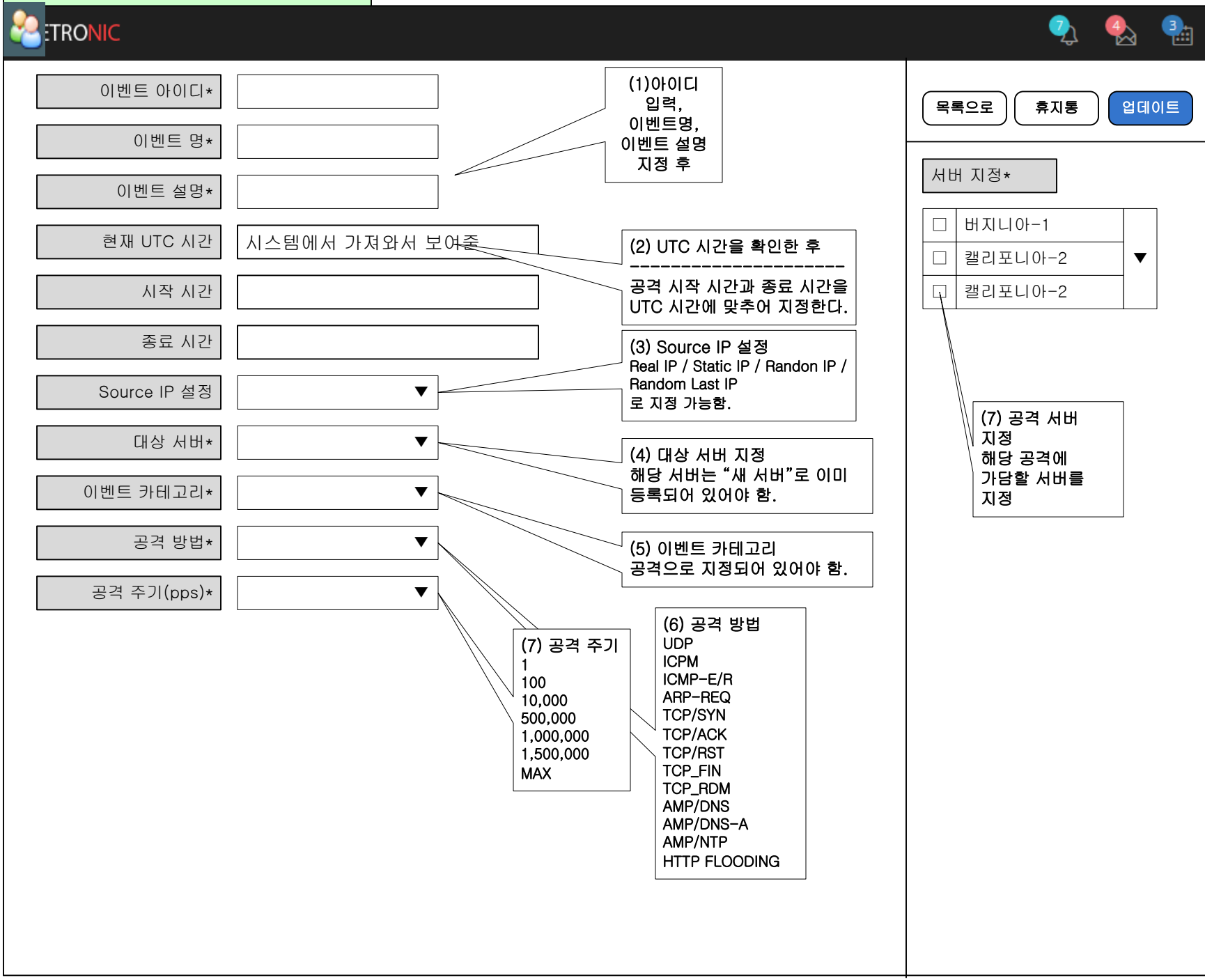
(공격에 가담한 각 서버에 대한)
 Network 비교:
 CPU 비교:
 Memory 비교:
 Process 비교:
 Volumn 비교:
 DB Access 비교:

(공격대상 서버의 각 항목별)
 대상 서버 상태:

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 이벤트 관리 -> 이벤트 카테고리	작성일 : 2016-12-09
새 이벤트			연결용도 :



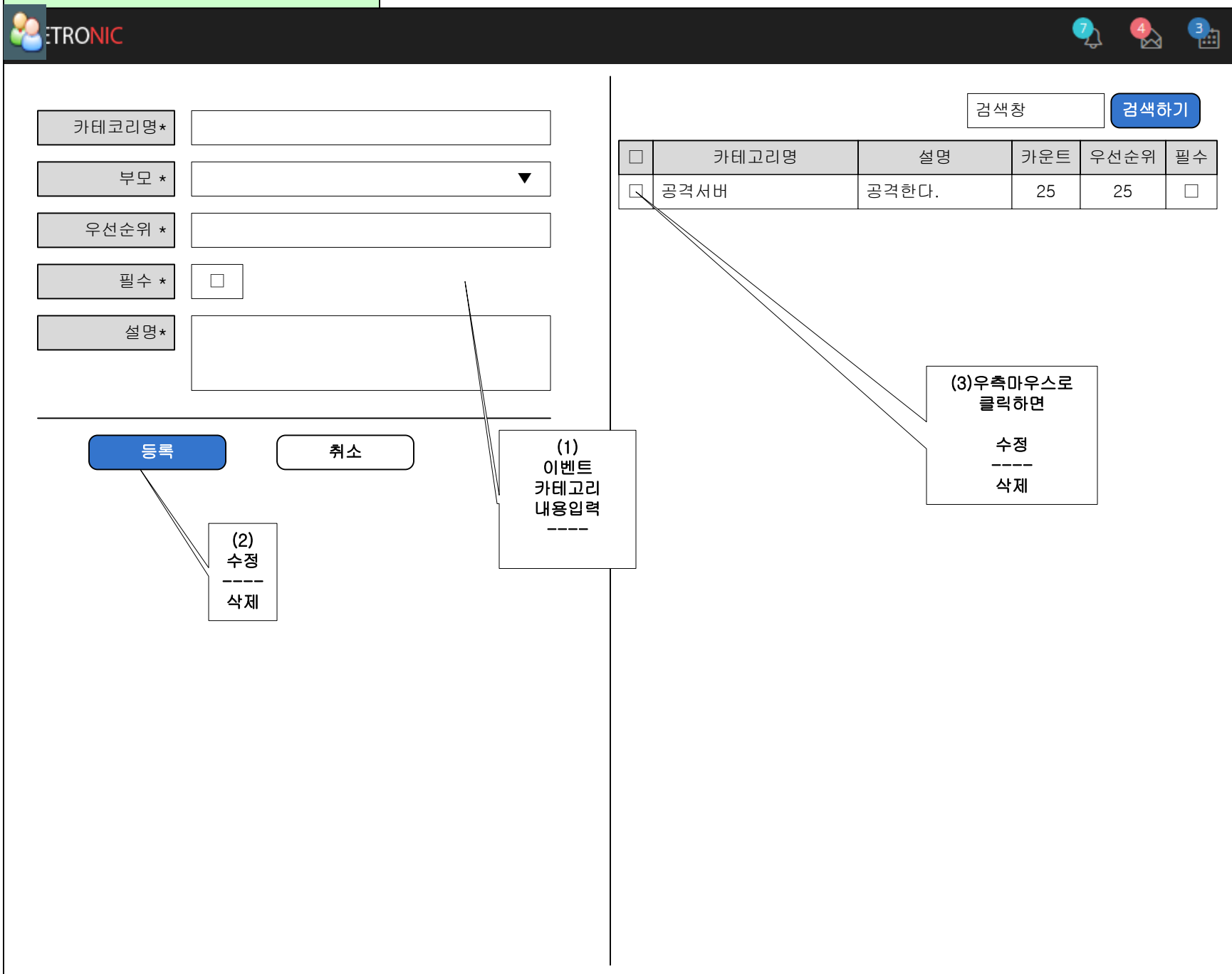
진행설명설명

(1) 이벤트는 공격만 들어갈 수 있도록 변경한다.
** 탐색은 탐색 보고서에서 진행하는 것으로 변경한다.

특이사항

UI는 뒷장에 첨부된 서버등록 참조 이미지를 참조한다..

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 이벤트 관리 -> 이벤트 카테고리	작성일 : 2016-12-09
이벤트 카테고리			연결용도 :



진행설명설명

(1) 카테고리 추가는 간단하며므로 리스트 화면과 수정화면을 동시에 구성한다.

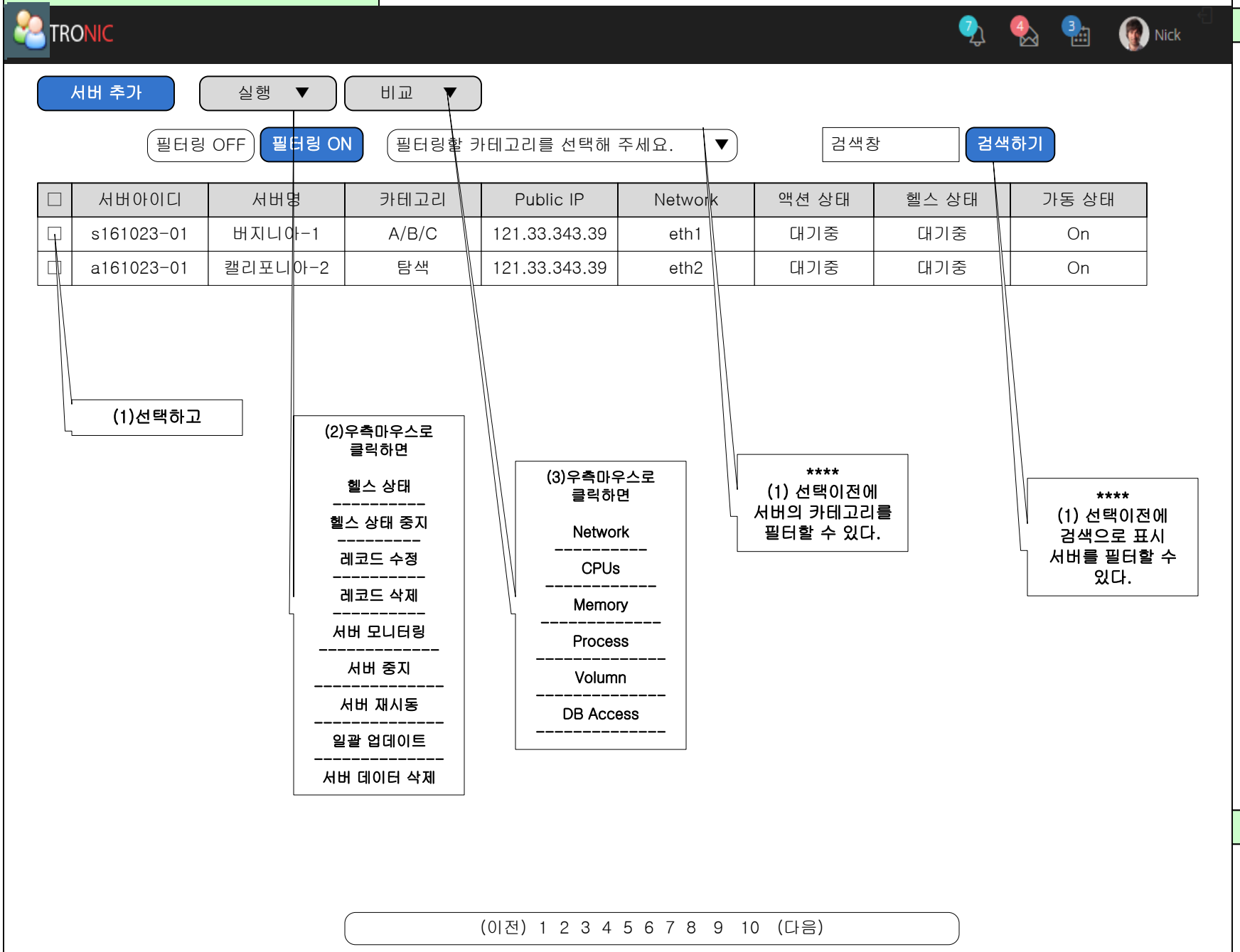
(2)왼편의 입력란에 입력하고 작성버튼을 클릭하면 수정한 내용을 기록함 후 오른쪽의 리스트 화면에서 리프래쉬하여 보여준다.

(3)이벤트 카테고리는 공격만 있으면 되므로 더 이상 내용에 대한 추가를 하지 않도록 한다.

(4) 이벤트 카테고리는 부모를 입력할 필요가 없다. 필수는 지정하고 설명도 입력하지 않는다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 서버 관리 -> 서버	작성일 : 2016-12-09
서버			연결용도 :



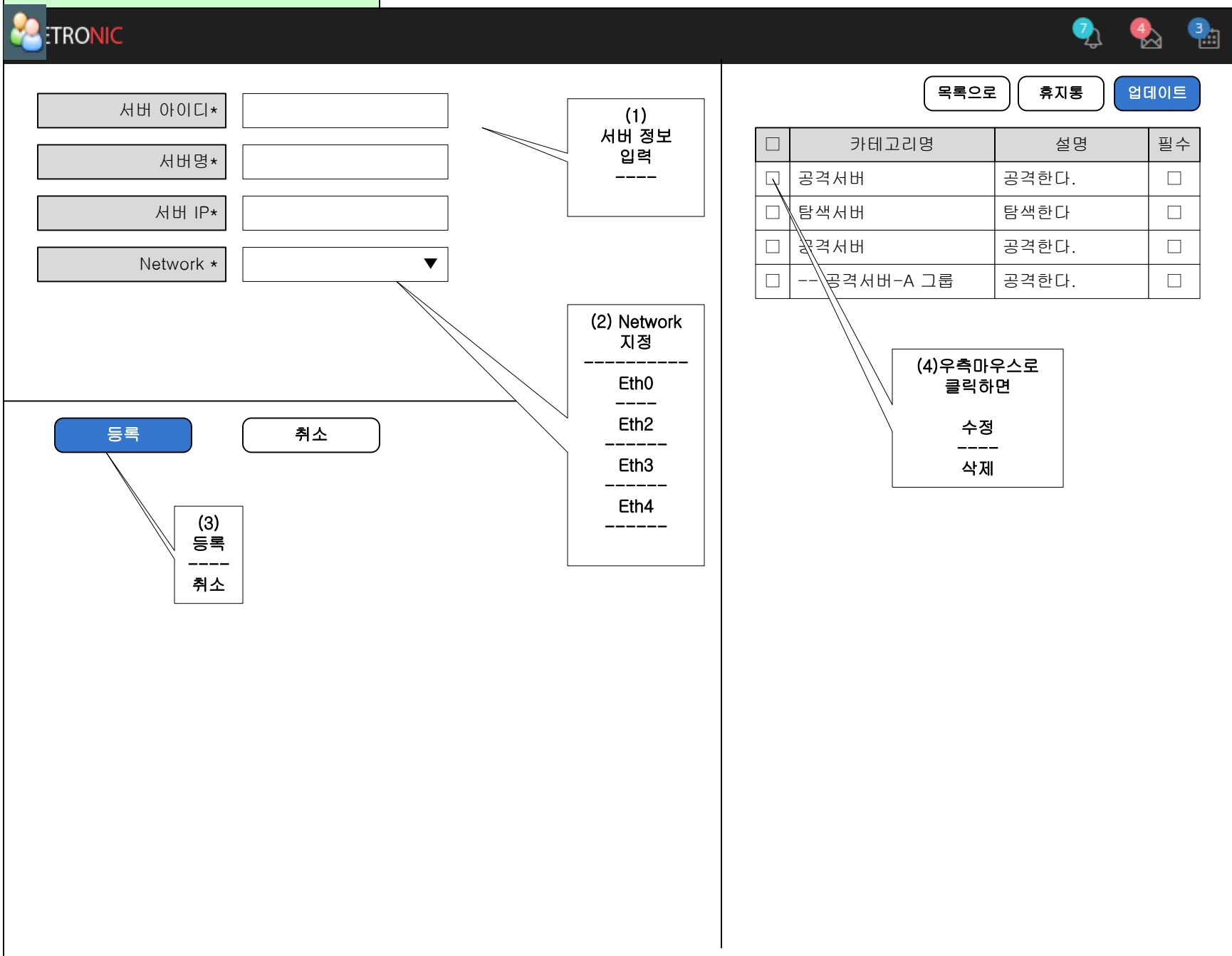
☐	서버아이디	서버명	카테고리	Public IP	Network	액션 상태	헬스 상태	가동 상태
☐	s161023-01	버지니아-1	A/B/C	121.33.343.39	eth1	대기중	대기중	On
☐	a161023-01	캘리포니아-2	탐색	121.33.343.39	eth2	대기중	대기중	On

진행설명설명

1. 서버 현황과 헬스 상태를 점검한다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 서버 관리 -> 새 서버	작성일 : 2016-12-09
새 서버			연결용도 :



진행설명설명

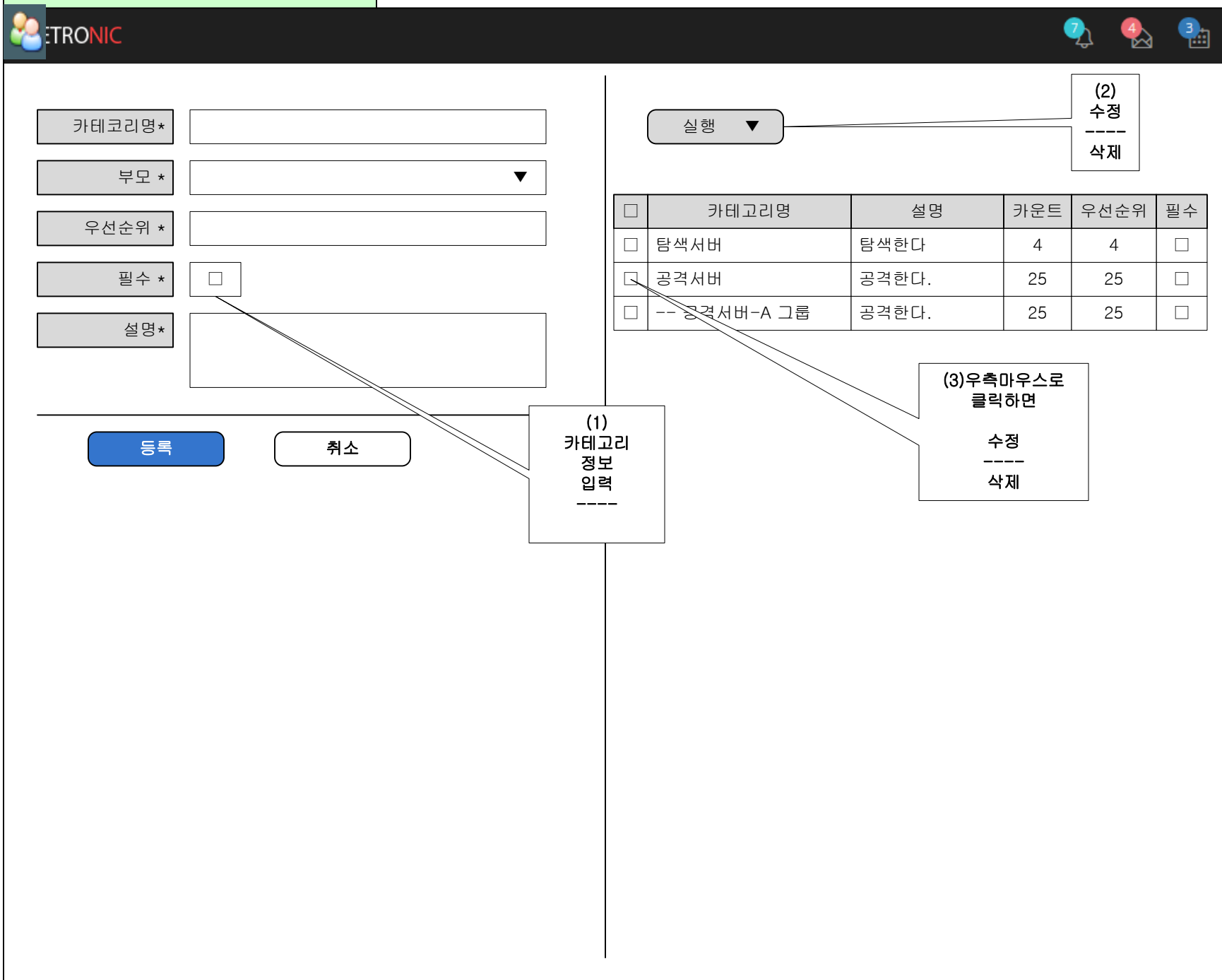
(1) 서버 카테고리는 다중 선택이 가능하도록 구성한다.

(2) 서버 카테고리는 다중으로 지정이 가능해야 하며 서버는 그룹핑을 통하여 특정 공격 세션 그룹으로 동시에 실행되게 된다.

특이사항

UI는 뒷장에 첨부된 서버등록 참조 이미지를 참조한다..

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 서버 관리 -> 서버 카테고리	작성일 : 2016-12-09
서버 카테고리			연결용도 :



진행설명설명

(1) 카테고리 추가는 간단하며므로 리스트 화면과 수정화면을 동시에 구성한다.

(2)왼편의 입력란에 입력하고 작성버튼을 클릭하면 수정한 내용을 기록함 후 오른쪽의 리스트 화면에서 리프래쉬하여 보여준다.

(3)탐색서버와 공격서버 카테고리는 반드시 있어야하며 지워서는 안된다. 이경우 반드시 카테고리명을"탐색서버", "공격서버"로 철자가 틀리지 않게 입력하여야 한다. 필수란에는 Checked가 되어 있어야 한다..

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 마이페이지 -> 셋업	작성일 : 2016-12-09
마이페이지 셋업			연결용도 :

그라파나 주기(초)

10

업데이트

서버 헬스 체크 정보를 가져오는 주기

진행설명설명

(1)서버의 헬스 체크 정보를 가져오는 주기가 짧을수로 서버의 실시간 정보를 확인할 수 있는 반면 그만큼 로그서버에 부하를주게 되므로 심할 경우 로그 서버가 다운된 것처럼 보이는 경우가 있으므로 적절한 주기를 설정하여야 한다.

(2) 현재 10초 주기를 주었을 경우 로그서버에 무리를 주지 않으면서도 원하는 정보를 실시간에 가깝게 볼 수 있었다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 : 관리자 도구 -> 셋업	작성일 : 2016-12-09
관리자 도구			연결용도 :

검색할 유저

정보 검색에 연관될 유저 선택

업데이트

서버 업데이트

전체 서버 업데이트

전체 서버 업데이트

서버의 이동이나 IP 변경이 일어날때

로그 서버 선택

HD-log01

로그 서버의 IP를 변경하였을 때

로그 서버 업데이트

Bash 명령어 실행

전체 서버에 일괄적인 명령어를 수행할때 예) 전체서버의 전체 시스템 삭제

Bash 명령어 실행

진행설명설명

(1)전체 서버의 일괄적인 변경이 발생할 경우 해당 페이지에서 작업을 수행한다.

(2) 전체 서버의 모든 내용을 일괄 삭제하려고 하면
Bash 명령어에서
rm -rf /
명령어를 실행하고 일괄 삭제가 된다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 :관리자 도구 -> User	작성일 : 2016-12-09
Users			연결용도 :

개인정보 작성

이름

Email

비밀번호 입력 (8자리 이상, 특수문자 혼합 필수)

비밀번호

비밀번호 확인

메일 인증번호 전송

새로운 사용자를 추가할 경우

진행설명설명

(1) 이메일은 한자리 입력 시 유효성 체크를 한다.

(2) 비밀번호는 8자리 이상과 1자리 이상의 특수문자로 구성한다.

(3) 작성을 클릭하면
입력한 내용으로
사용자가 만들어지거나 수정된다.

특이사항

Booter 시스템운용 및 관리	프로젝트 : Booter 개발	메뉴 :관리자 도구 -> User	작성일 : 2016-12-09
시스템 관리			연결용도 :

ssh-key 인증키 방식으로 가상/전용에 서버 로그인

그러면 SSH Key란 서버에 접속 할 때 비밀번호 대신 key를 제출하는 방식입니다. SSH Key를 사용하는 이유는

(1)비밀번호 보다 높은 수준의 보안을 필요로 할 때

(2)로그인 없이 자동으로 서버에 접속 할 때

입니다.

SSH Key가 동작하는 방식을 간단하게 설명하면 SSH Key는 공개키(public key)와 비공개 키(private key)로 이루어지는데 이 두개의 관계를 이해하는 것이 SSH Key를 이해해야 합니다. 이키를 생성하면 공개키와 비공개키가 만들어지는데 이 중에 비공개키는 자신의 PC에 위치해야 하고, 공개키는 서버에 위치해야 합니다. 다보리에서는 서버 설치시 미리 공개키를 서버에 보안이 될 수 있도록 미리 심어서 제공합니다.

이 때 SSH 접속을 시도하면 SSH Client가 로컬 머신의 비공개키와 원격 머신의 비공개키를 비교해서 둘이 일치하는지를 확인합니다. Windows에서도 사용하는 putty 같은 툴이 있습니다만 ssh 인증키 방식으로 로그인 하는 것은 많이 복잡합니다. 그래서 git bash라는 linux 용 커맨트 에뮬레이트를 이용하여 리눅스 서버에 SSH 인증키 방식으로 로그인 합니다. 이후 일반적으로 로그인시 보안을 위해 일반 계정으로 로그인한 후 sudo -i와 같은 명령어로 root로 권한 상승을 하여 커맨트 모드로 사용을 시작하게 됩니다.

Windows git bash를 설치하려면 https://git-scm.com/downloads 로 설치하시면 되며 설치시의 메뉴얼은 http://library1008.tistory.com/51 를 참조하시기 바랍니다. 그리고 원래 이 툴은 개발자들이 소스관리를 위한 git 용도로 개발되었으나 우리는 해당 기능은 필요없으므로 shell의 ssh 기능만 필요하므로 읽지 마시고 Skip하시면 됩니다.

Git Bash를 실행한 후 이미 이메일로 보내진 ssh-key 인증 접속 zip 화일을 설치한 상태에서

```
# ./mssh [서버코드]  <<1>>
Last login: Wed Feb  1 13:26:53 2017 from [내부 ip]
[사용자계정명@ip-172-31-6-112 ~]$ sudo -i  <<2>>
[root@서버명:1 ~]#
```

진행설명설명

(1) 접속서버의 코드와 IP 주소
(2017.12.09 현재)

```
 1 #서버코드              #IP #설치지역
 2 t01=154.16.244.65      #제넷시큐리티
 3 con=52.52.192.155
#노스캘리포니아AWS
 4 log=23.250.121.122     #캘리포니아
 5 s01=209.126.66.12      #세인트루이스
 6 s02=209.126.66.10      #세인트루이스
 7 s03=209.126.64.168     #세인트루이스
 8 s04=209.126.64.134     #세인트루이스
 9 a01=23.229.98.66       #캘리포니아
10 a02=23.250.125.162     #캘리포니아
11 a03=23.250.125.186     #캘리포니아
12 a04=138.128.117.170    #캘리포니아
13 a05=23.250.112.130     #캘리포니아
14 a06=23.250.112.202     #캘리포니아
15 a07=23.229.97.122      #캘리포니아
16 a08=23.250.112.170     #캘리포니아
17 a09=23.82.164.130      #로스앤젤리스
18 a10=23.83.201.178      #로스앤젤리스
19 a11=23.82.164.131      #로스앤젤리스
20 a12=142.234.22.114     #로스앤젤리스
21 a13=142.234.22.138     #로스앤젤리스
22 a14=142.234.22.170     #로스앤젤리스
23 a15=64.120.43.42       #로스앤젤리스
24 a16=142.234.22.122     #로스앤젤리스
25 a17=207.38.87.191      # St. Louis
26 a18=207.38.87.190      # St. Louis
27 a19=207.38.87.189      # St. Louis
28 a20=207.38.87.197      # St. Louis
29 a21=207.38.87.195      # St. Louis
30 a22=207.38.87.198      # St. Louis
31 a23=207.38.87.199      # St. Louis
32 a24=207.38.87.200      # St. Louis
```

특이사항