보안관제 솔루션
CHAOSEND 제품소개

2011. 10

S2info
에스2정보(주)

목 차

1. 회사소개

2. 개념

3. 구성도

4. 주요기능 소개

5. 상세기능 소개

6. 구축 사례

7. 제품 스펙

Copyright © by S2INFO All rights reserved.

S2info
에스2정보 (주)

1. 회사 소개

㈜에스2정보는 IT 전문기업으로 강한 회사, 충실한 회사, 도덕적인 회사를 지향합니다.

저희 ㈜에스2정보 직원들은 지난 15년간 KT 전문 협력회사로 근무해 오면서 국내 최다 경험의 장비/망 관리 기술, 네트워크 망 설계, 접근제어를 통한 통신망 보안 체계확립등 거미줄망처럼 복잡한 ISP망에서 보다 정확하고 안전한 네트워킹 구현을 위해 노력해왔습니다.

회사 개요

구 분	세부 내역
회사 명	에스2정보 ㈜
대표 자	우 정 우
사업 분야	소프트웨어 패기지 공급 / 컨설팅 서비스 / 소프트웨어 연구개발
주 소	서울시 강남구 역삼동 707-38 테헤란 오피스빌딩 1212호
연락처	02) 553-5860 FAX 02) 553-5870 http://www.s2info.co.kr
설립 연도	2009/07/09

주요 사업

2011 "SCI 서울 신용평가 정보 회사 신용도 평가 B0 획득"

04. KTDS 접근제어 시스템 고도화 사업수주
05. KT Managed Service 기업고객 SECU-1 보안솔류션 상품화 진행
    한국 저작권 위원회 프로그램 등록 – ChaosEND
07. KT U-Cloud 시스템 접근보안 컨설팅 및 시스템 구축 / 프로젝트 진행
07. KT NSG_Keeper 시스템 Middle Gateway 개발 프로젝트 진행

2010 "SCI 서울 신용평가 정보 회사 신용도 평가 B- 획득"

03. KT 캐피텔 접근제어 솔류션 공급
05. KT-DS 접근제어 시스템 프로젝트 수주
06. KT_IDC CISCO Guard 보안관제 솔루션 공급
08. RIOREY DDOS 장비 보안관제 솔류션 공급
    한국저작권 위원회 프로그램 등록 – CISCO Guard View
09. KT ISM망,BCN망,초고속망,QookTV망,KORNET망,3G망 접근제어 망 통합사업 수주
11. KT NSG_Keeper 시스템 고도화 사업수주
12. 특허 출원 : 서버 장애 방지 시스템 및 방법

2009

07. 에스2정보 설립
09. KT ISM망 접근제어 시스템 구축 / 프로젝트 수주
10. KT BCN망 접근제어 시스템 구축 / 프로젝트 수주
    한국저작권 위원회 프로그램 등록 – RIOREY MView
10. KT QOOK TV망 접근제어 시스템 구축 / 프로젝트 수주
11. KT 국가정보통신망 보안관제 시스템 구축
12. KT TACS 시스템 고도화 프로젝트 수주

Copyright © by S2INFO All rights reserved.

S2INFO 에스2정보 (주)

2. 제품 개요

- 비정상트래픽 탐지 및 분석을 통한 **침해사고 대응기반** 마련
- 네트워크 기반 **통합 보안 관리서비스** 제공
- 신속한 비정상트래픽 탐지를 통한 **망 위협 대응체제 구축**
- 위협 발생 시 신속한 대비를 통한 **안정성 강화**

탐지센서

DDOS 공격 탐지
DDOS 정보 탐지
DDOS 트래픽 정보 수집

정보가공/분석

SECU-1 서버

허용/거부에 대한
트래픽/이벤트 별
통계 생성

보안이벤트/트래픽수집

SECU-1 보안관제

분석/가공데이터 저장
-허용탐지로그
-거부탐지로그
-트래픽 분석로그
분석레포트 저장

보안 통계
트래픽 정보 제공

관리자

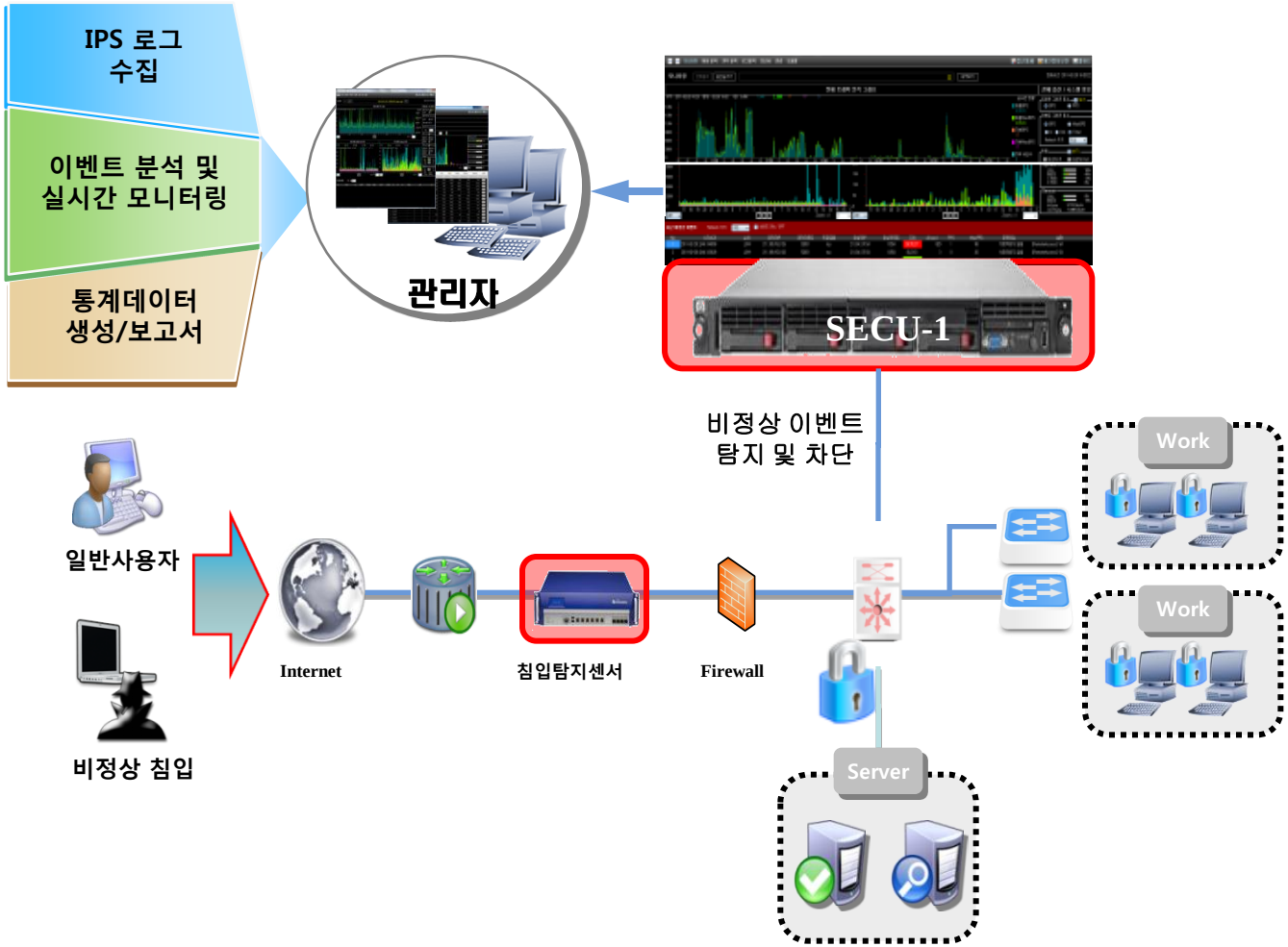
보안관제 실시간 모니터링
비정상 침입 탐지 및 차단

Copyright © by S2INFO All rights reserved.

S2info
에스2정보 (주)

3. 구성도

⊙ 비정상 침입 탐지 및 차단을 위한 보안관제 시스템



주요 기능

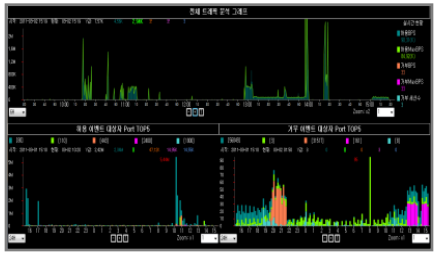
- 실시간 보안관제 모니터링 기능
- 공격발생시 경보기능
- 이벤트 허용/거부 분석 기능
- 비정상 이벤트 및 허용/거부
- 로그 분석 기능
- 월/주/일별 통계 보고서기능

Copyright © by S2INFO All rights reserved.

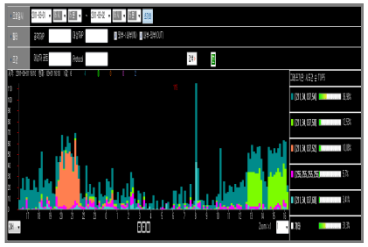
S2INFO 에스2정보(주)

4. 주요기능 소개

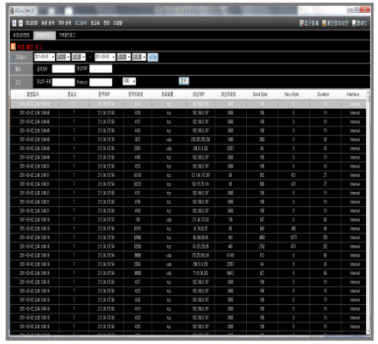
실시간 모니터링 및 비정상 이벤트 탐지 → 허용/거부 패킷 분석 → 로그 분석 → 일간/주간/월간 통계 보고서



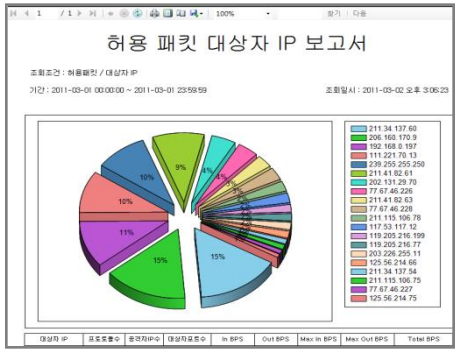
실시간 트래픽/이벤트 그래프



허용/거부 Top5 그래프

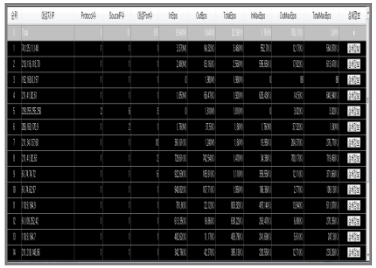


비정상이벤트/허용/거부 로그 분석



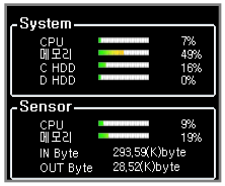
통계보고서

최근 비정상 침입 탐지



허용/거부 Top20 리스트

관제 옵션 설정



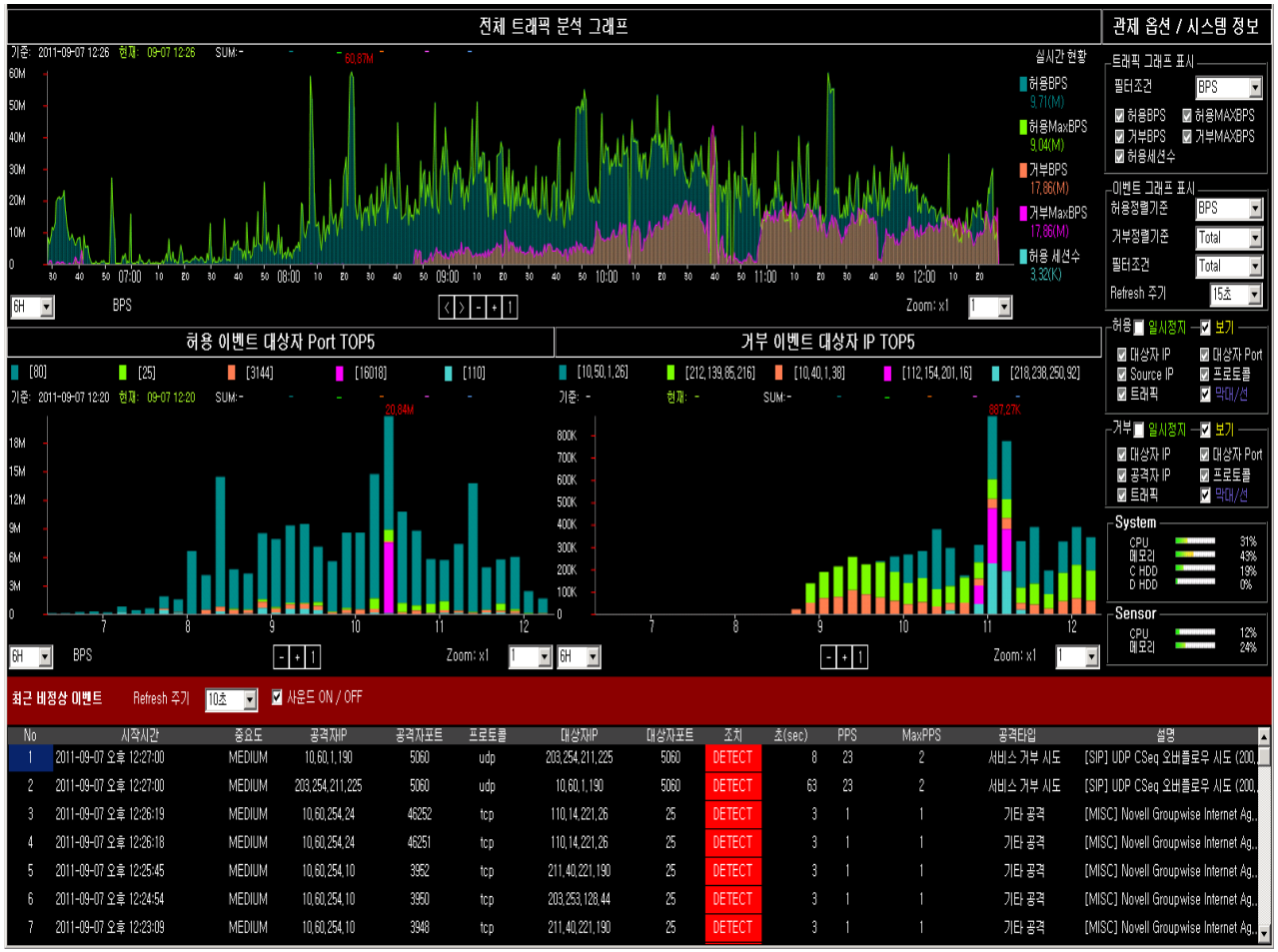
시스템/센서 리소스 모니터링

Copyright © by S2INFO All rights reserved.

S2info 에스2정보(주)

5. 상세기능 소개

모니터링



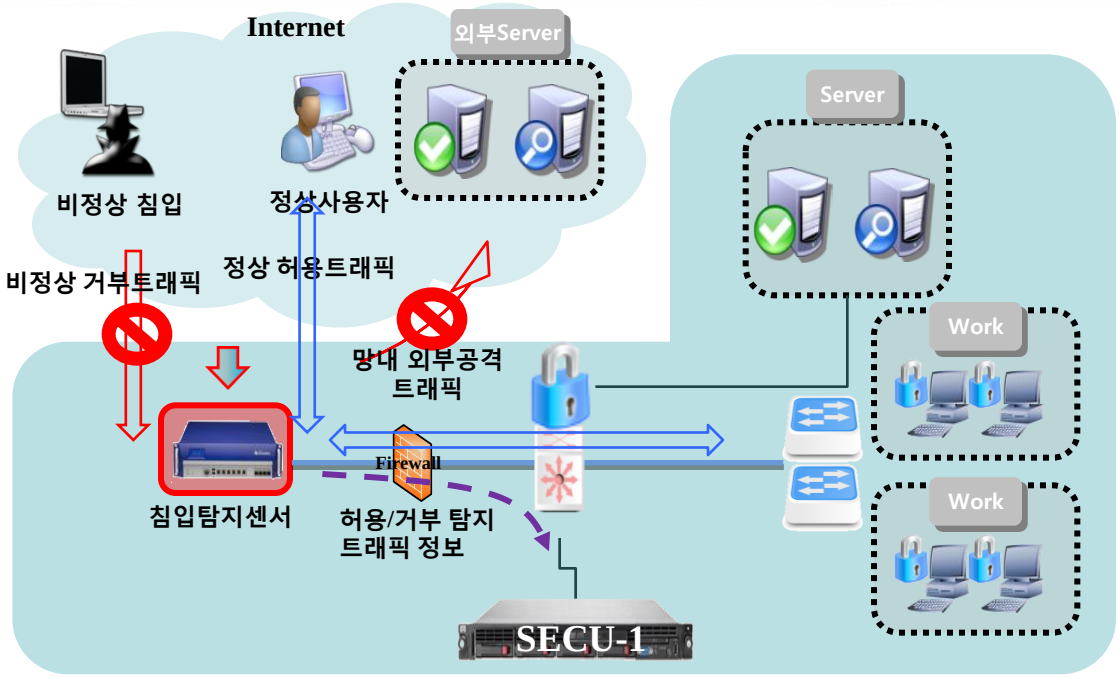
주요기능

- 전체 트래픽 모니터링기능 제공
- 허용 대상자IP/ 대상자Port/ SourceIP /프로토콜/트래픽 모니터링 기능 제공
- 거부 대상자IP/ 대상자Port/ 공격자IP /프로토콜/트래픽 모니터링 기능 제공
- 비정상 이벤트 정보 제공,
  공격 발생시
  Alarm 을 통해 사용자에게 인지
- 관제 옵션 선택 및
  시스템/센서 리소스 모니터링 기능

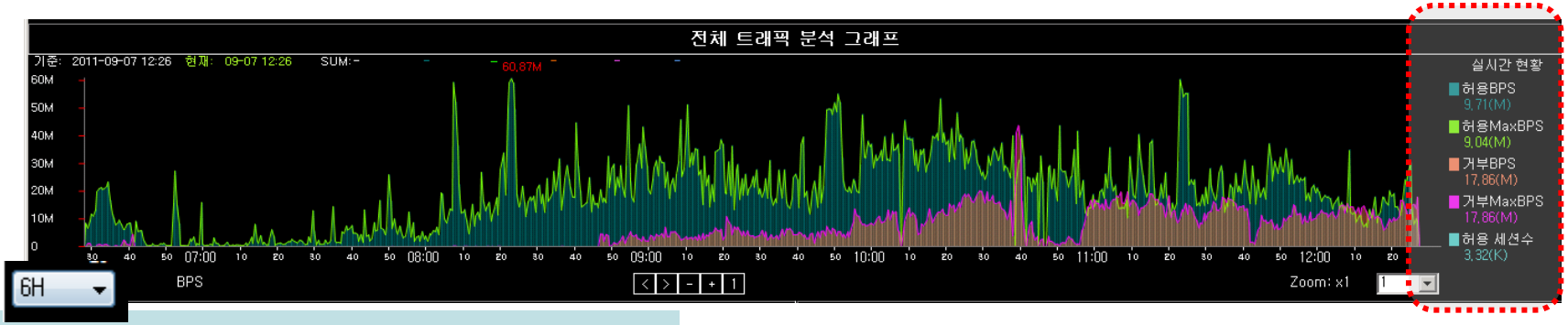
Copyright © by S2INFO All rights reserved.

5. 상세기능 소개

관제- 전체 트래픽 관제



30초 단위 실시간
허용 / 거부 탐지 트래픽 정보
그래프 범례



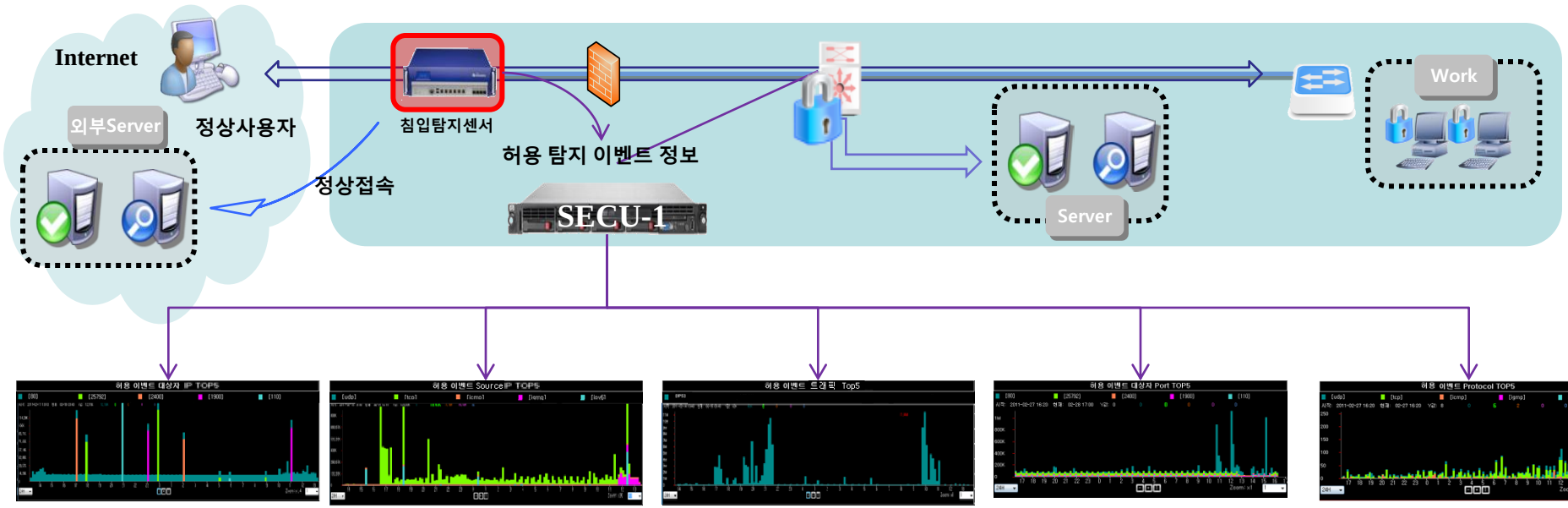
실시간 기준시간 변경 (15m/30m/1h/2h/4h/6h)

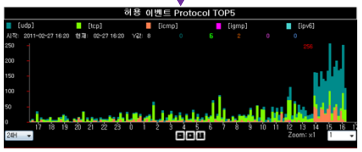
Copyright © by S2INFO All rights reserved.

S2info 에스2정보 (주)

5. 상세기능 소개

관제- 허용 이벤트 관제





허용 대상자 IP

- 허용된 망내/ 망외 대상자IP 정보기준 관제화면

허용 Source IP

- 허용된 망내/ 망외 Source IP 정보기준 관제화면

허용 트래픽

- 허용된 망내 / 망외 트래픽 정보기준 관제 화면

허용 Port

- 허용된 망내/ 망외 Port 정보기준 관제화면

허용 Protocol

- 허용된 망내/ 망외 Protocol 정보기준 관제 화면

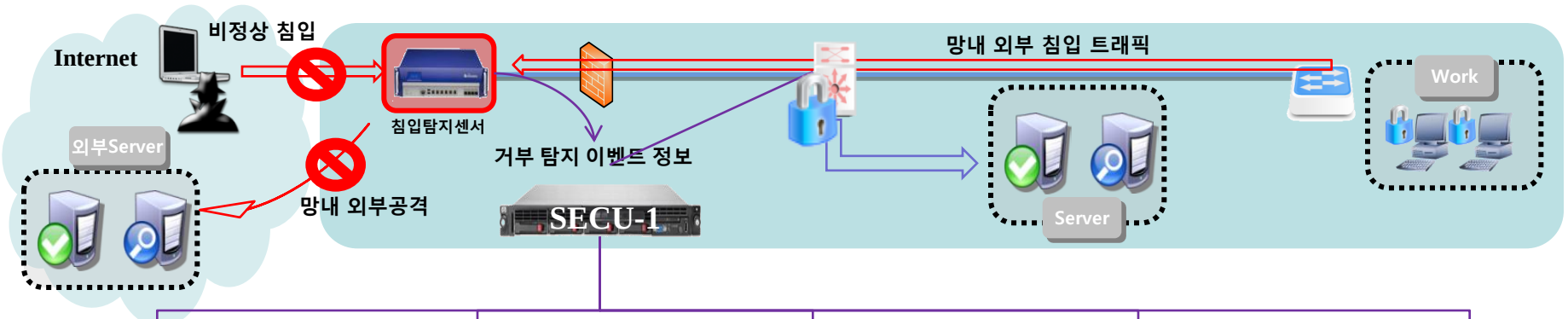
15초 기준 화면이 반복

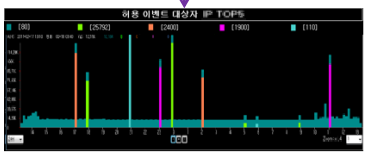
Copyright © by S2INFO All rights reserved.

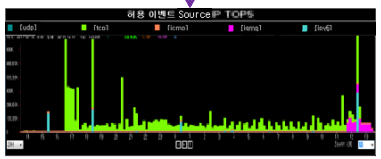
S2info 에스2정보(주)

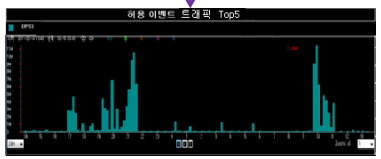
5. 상세기능 소개

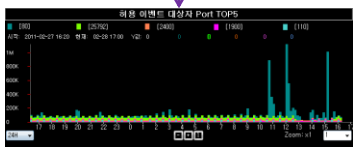
관제- 거부 이벤트 관제

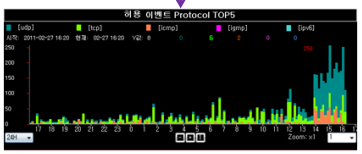












거부 대상자 IP

- 거부된 망내/ 망외 대상자IP 정보기준 관제화면

거부 공격자 IP

- 거부된 망내/ 망외 공격자 IP 정보기준 관제화면

거부 트래픽

- 거부된 망내 / 망외 트래픽 정보기준 관제 화면

거부 Port

- 거부된 망내/ 망외 Port 정보기준 관제화면

거부 Protocol

- 거부된 망내/ 망외 Protocol 정보기준 관제 화면

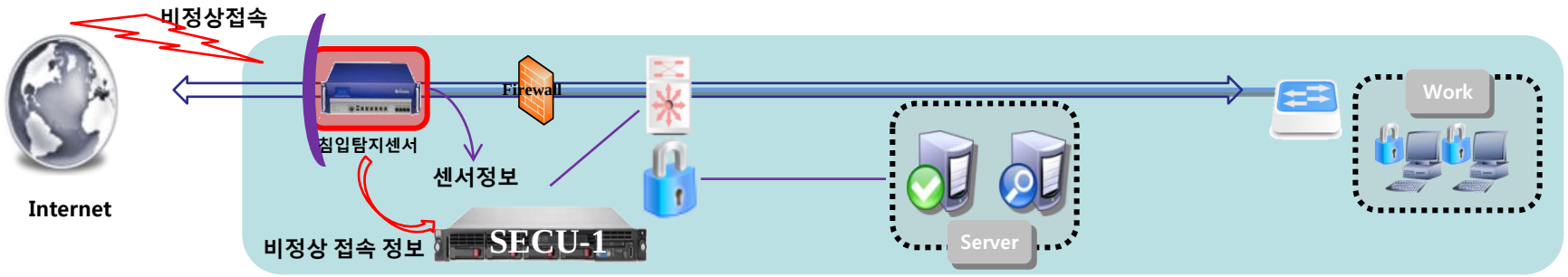
15초 기준 화면이 반복

Copyright © by S2INFO All rights reserved.

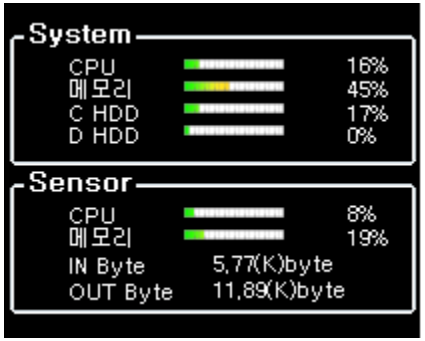
S2info 에스2정보(주)

5. 상세기능 소개

○ 관제_비정상 이벤트 알림 / 리소스 모니터링



초치 정보



최근 비정상 침입 탐지 정보 알람

■외부에서 들어오는 비정상 침입 탐지 거부 정보를 알람으로 제공

조치정보(DETECT/BLOCK/PASS)로 정보제공

시스템/센서 리소스 모니터링

■ SECU-1 서버 (침입탐지센서) CPU/메모리/HDD(in,out 정보)를 1분 단위 실시간으로 제공

Copyright © by S2INFO All rights reserved.

S2Info 에스2정보 (주)

5. 상세기능 소개

⊙허용 패킷 분석

Internet

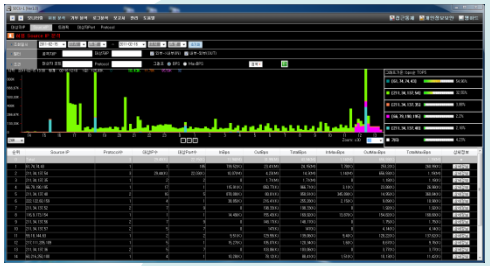
침입탐지센서

센서에서
허용된 트래픽
탐지정보

허용 대상자IP 분석

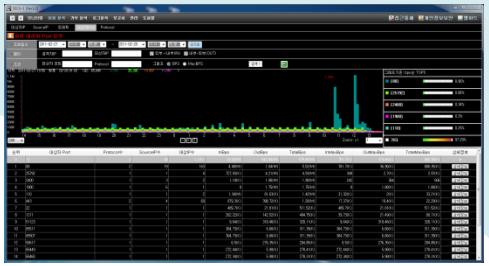
탐지 통계정보

SECU-1



허용 Source IP 분석

허용 프로토콜 분석



허용 대상자 포트 분석

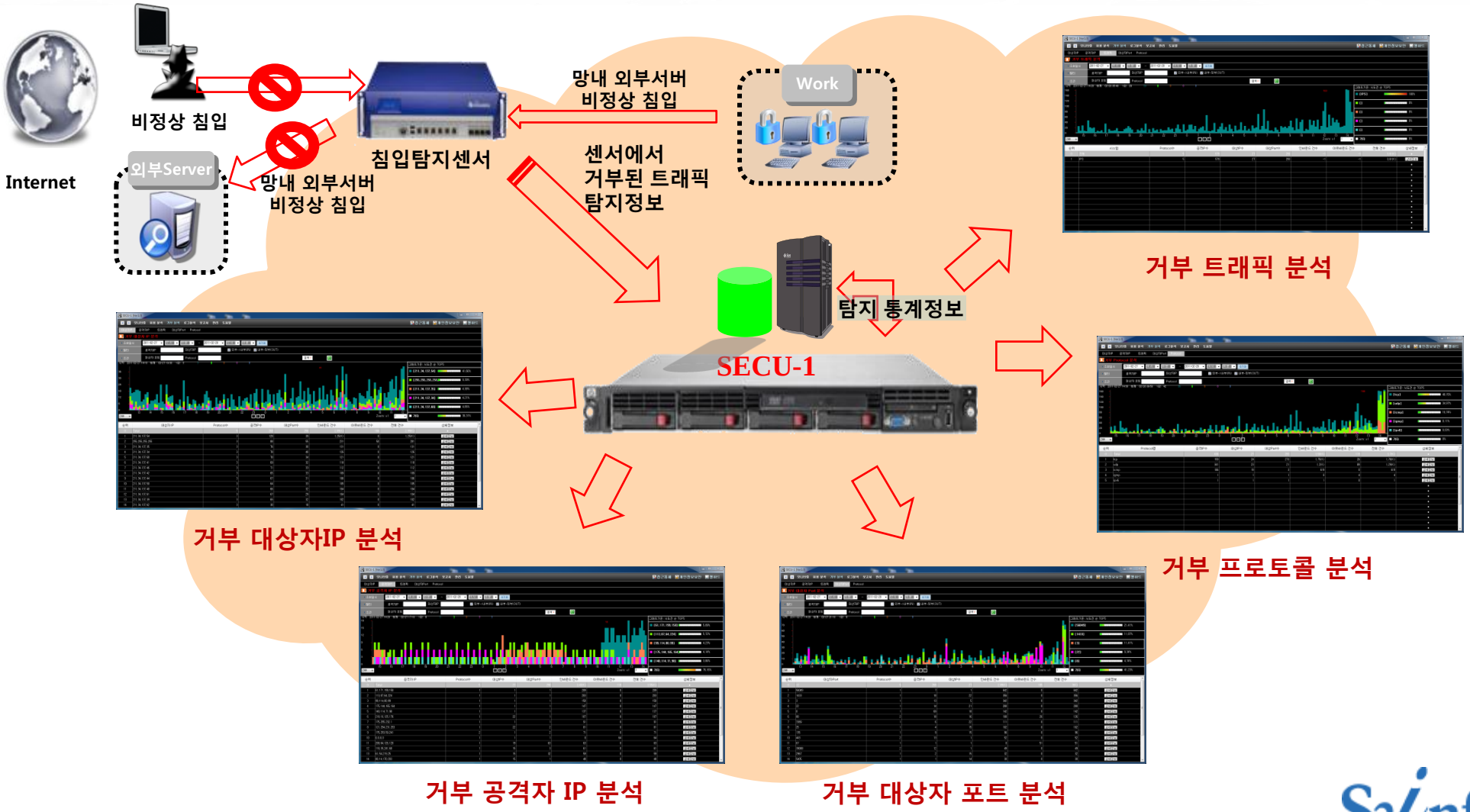
허용 트래픽 분석

Copyright © by S2INFO All rights reserved.

S2info
에스2정보 (주)

5. 상세기능 소개

거부 패킷 분석



Copyright © by S2INFO All rights reserved.

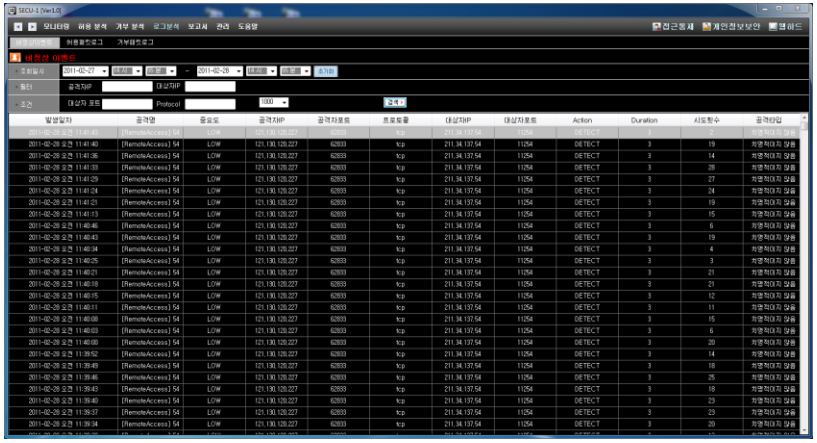
S2info 에스2정보 (주)

5. 상세기능 소개

로그 분석- 비정상 이벤트 로그 분석

발생일자	공격명	중요도	공격자IP	공격자포트	프로토콜
2011-02-28 오전 11:41:43	[RemoteAccess] 54	LOW	121.130.120.227	62833	tcp
2011-02-28 오전 11:41:40	[RemoteAccess] 54	LOW	121.130.120.227	62833	tcp
2011-02-28 오전 11:41:36	[RemoteAccess] 54	LOW	121.130.120.227	62833	tcp
2011-02-28 오전 11:41:33	[RemoteAccess] 54	LOW	121.130.120.227	62833	tcp

대상자IP	대상자포트	Action	Duration	시도횟수	공격타입
211.34.137.54	11254	DETECT	3	2	치명적이지 않음
211.34.137.54	11254	DETECT	3	19	치명적이지 않음
211.34.137.54	11254	DETECT	3	14	치명적이지 않음



- 24시간 기준 조회일시에 대한 침입탐지 센서에서 발생하는 비정상 이벤트 로그 조회하여 언제 어떤 공격자 IP에서 어느 대상자 IP으로 어떤 공격을 몇번 받았으며 그공격됬을때 침입탐지 센서가 어떤 행동을 했는지 알 수 있는 로그내역을 볼 수 있습니다.

Copyright © by S2INFO All rights reserved.

S2info 에스2정보(주)

5. 상세기능 소개

로그 분석- 허용패킷 로그 분석

센서에서
허용된 트래픽
탐지정보

발생일자	중요도	공격자IP	공격자포트	프로토콜	대상자IP
2011-02-28 오후 2:59:52	7	211.34.137.35	3072	udp	239.255.255.250
2011-02-28 오후 2:59:52	7	211.34.137.54	50017	tcp	119.67.182.41
2011-02-28 오후 2:59:52	7	211.34.137.54	50017	tcp	143.248.99.109
2011-02-28 오후 2:59:52	7	211.34.137.54	22574	udp	208.51.0.252

대상자포트	Send Byte	Recv Byte	Duration	Interface
1900	2962	0	20	Internal
4450	198	0	19	Internal
1842	198	0	19	Internal

- 24시간 기준 조회일시에 대한 침입탐지 센서에서 발생하는 허용 패킷 탐지 정보에 관한 로그 조회하여 언제 어떤 Source IP에서 어느 대상자 IP으로 얼마나 많은 트래픽이 발생되었는지 알 수 있는 로그내역을 볼 수 있습니다.

Copyright © by S2INFO All rights reserved.

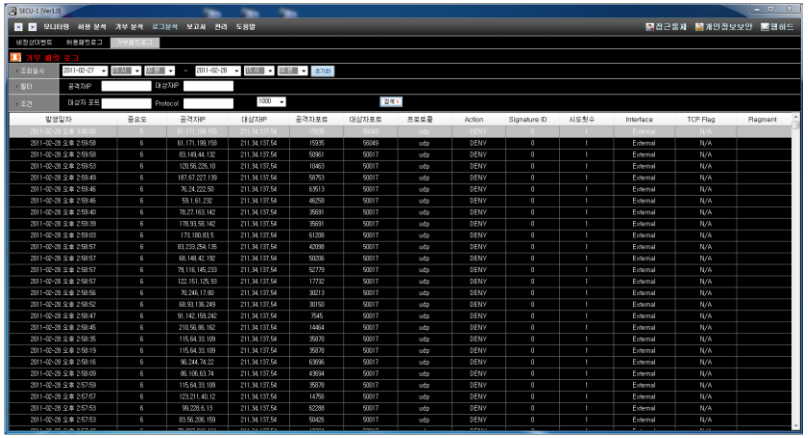
S2info 에스2정보 (주)

5. 상세기능 소개

로그 분석- 거부패킷 로그 분석

발생일자	중요도	공격자IP	대상자IP	공격자포트	대상자포트	프로토콜
2011-02-28 오후 3:00:00	6	61,171,199,158	211,34,137,54	15935	56049	udp
2011-02-28 오후 2:59:58	6	61,171,199,158	211,34,137,54	15935	56049	udp
2011-02-28 오후 2:59:58	6	83,149,44,132	211,34,137,54	50961	50017	udp

Action	Signature ID	시도횟수	Interface	TCP Flag	Flagment
DENY	0	1	External	N/A	
DENY	0	1	External	N/A	
DENY	0	1	External	N/A	



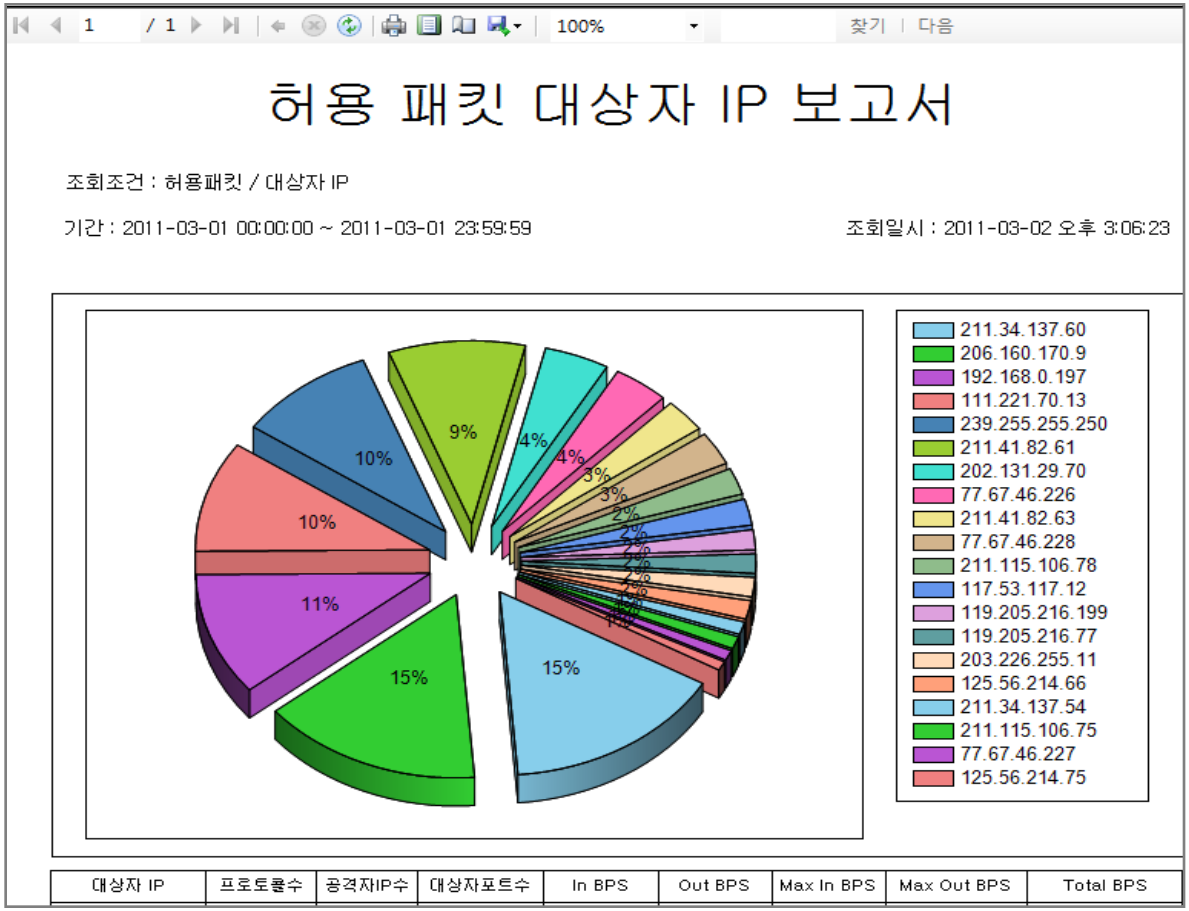
- 24시간 기준 조회일시에 대한 침입탐지 센서에서 발생하는 거부 패킷 탐지 정보에 관한 로그 조회하여 언제 어떤 공격자 IP에서 어느 대상자 IP으로 얼마나 많은 공격시도가 발생되었는지 알 수 있는 로그내역을 볼 수 있습니다.

Copyright © by S2INFO All rights reserved.

S2info 에스2정보 (주)

5. 상세기능 소개

통계 보고서



주요기능

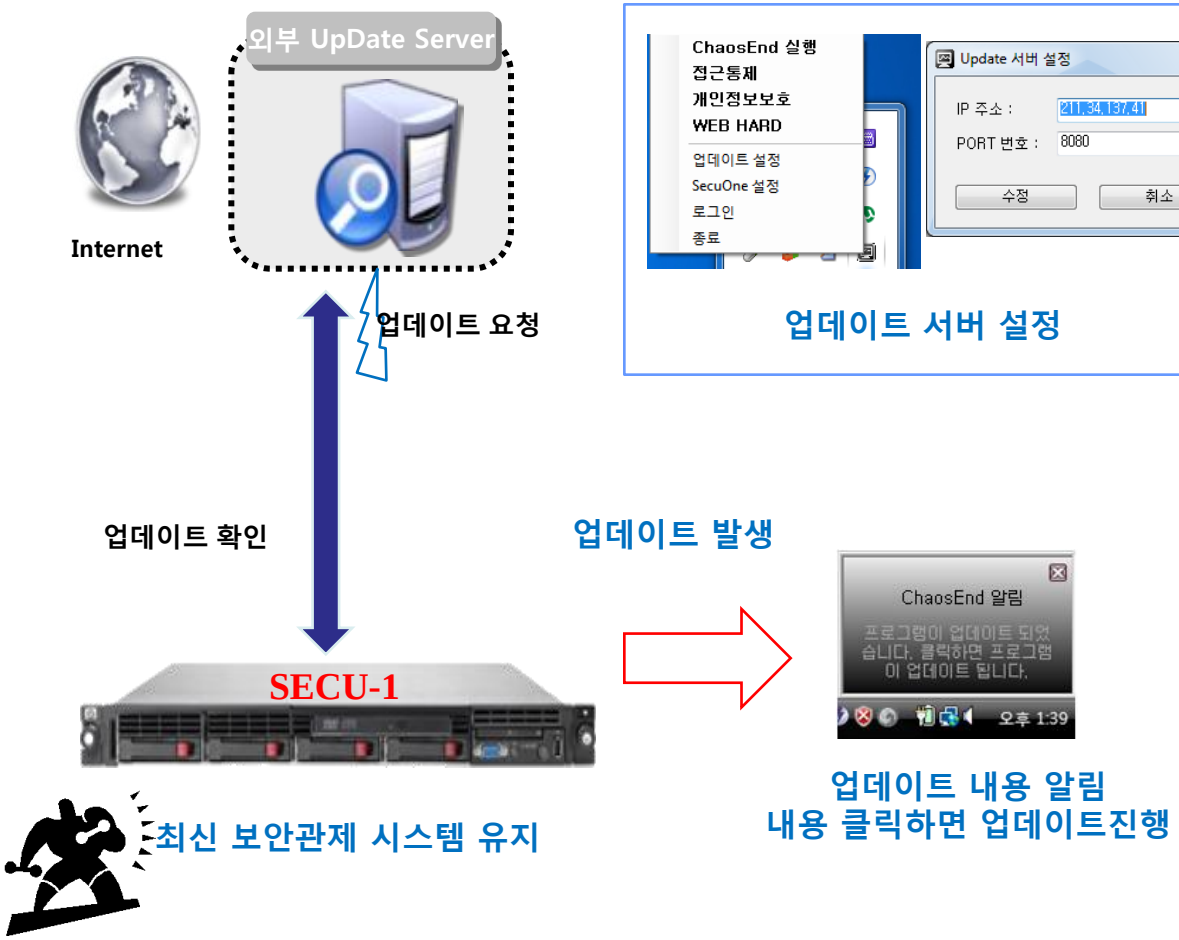
- ■월/주/일별 이벤트 통계 보고서
- ■ 대상자 IP / 공격자 IP / 트래픽 / 대상자 Port / 프로토콜 별 Top20 그래프 및 리스트 통계보고서 제공

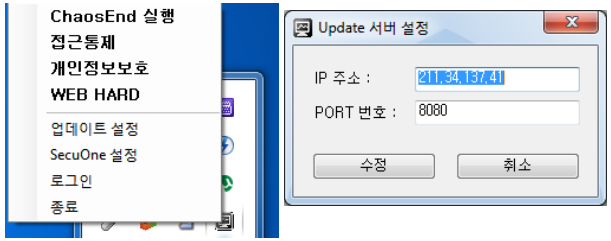
Copyright © by S2INFO All rights reserved.

S2Info 에스2정보(주)

5. 상세기능 소개

원격패치





업데이트 서버 설정

주요기능

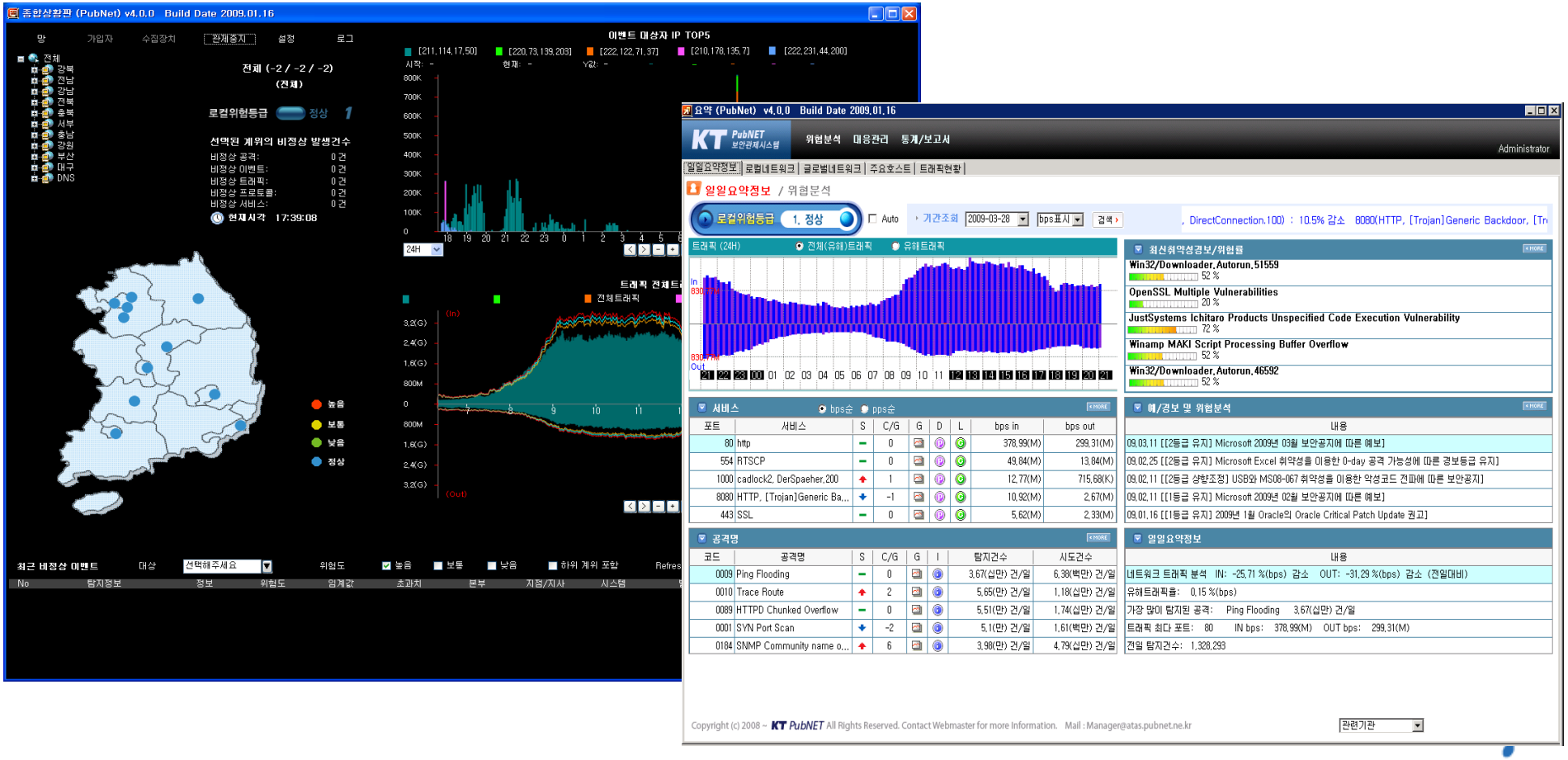
- 업데이트 서버 설정 기능
- 업데이트 발생시 프로그램을 통한 최신 보안관제 소프트웨어 패치 기능

Copyright © by S2INFO All rights reserved.

S2Info 에스2정보 (주)

6. 구축사례

국가정보통신망 보안관제시스템
PubNET 보안관제시스템



Copyright © by S2INFO All rights reserved.

7. 제품스펙

CHAOSEND SPEC				
구분	**패키지구성요소**	**Function**	**Q'ty**	**비고**
H/W	H/W & S/W	- CPU : 2GHz * 1 - Memory : 1GB * 4 - HDD : 300GB * 2 - OS : Windows 2008 Ent - DB : MS-SQL Server 2008 R2 Std.	1 EA	기본 H/W 스펙 기본 사양보다 상위 기종 변경 시 별도 협의
S/W	CHAOSEND	- 침입 탐지 실시간 모니터링 - 비정상 트래픽 탐지 및 알람기능	1식	Ver 1.0
탐지센서	IPS	- SECUI NXG	1 식	기본 : NXG 100F 망 대역폭에 따른 NXG 장비 변경 시 별도 협의 타사 IPS 장비 연동 시 별도 협의

※ 제품 공급 가격 : ₩50,000,000
(기본스펙 H/W 및 S/W, IPS 포함, 부가세 별도)

Copyright © by S2INFO All rights reserved.

S2info
에스2정보 (주)

7. 제품스펙

구분	기능	비고
모니터링 기능	전체 트래픽에 대한 허용/거부 트래픽 통계 그래프 기능 제공	
	허용/거부 이벤트에 대한 TOP N 모니터링 기능	
	대상자 IP 등 이벤트 별 그래프 모니터링 기능	
	수집서버, 센서에 대한 CPU,메모리 사용량 등의 성능정보 표시 기능 제공	
	Sound, 팝업창 등을 이용한 사용자 인지 기능	
	동일경보 필터링 및 경보 등급별 표시 기능	
허용 분석 기능	대상자 IP, Source IP, 트래픽, 대상자 Port, Protocol 등 유형별 허용 로그 분석을 위한 조건 설정 및 조회 기능	
	이벤트 항목별 기간 및 bps/pps 조건 검색 기능	
	특정 이벤트 조건별 (출발지, 목적지, 포트, 프로토콜 등) 조회 기능	
거분 분석 기능	대상자 IP, 공격자 IP, 트래픽, 대상자 Port, Protocol 등 유형별 거부 로그 분석을 위한 조건 설정 및 조회 기능	
	특정 이벤트 조건별 (출발지, 목적지, 포트, 프로토콜 등) 조회 기능	
로그 분석 기능	비정상 이벤트 로그 및 허용/거부 로그에 대한 분석 기능	
보고서 기능	대상자 IP, 공격자 IP 등 유형별 통계 분석 보고서 기능	
업그레이드 기능	업그레이드시 프로그램을 통한 원격 패치기능 제공	
로그 수집 기능	Syslog 등을 통한 실시간 로그 수집	

Copyright © by S2INFO All rights reserved.

S2info 에스2정보(주)