

서버와 네트워크를 가장 잘 알고 있는 회사 (주) 코리아서버호스팅

데이터 기반의 통찰력과 의사결정을 가능토록 합니다. (운영 가시성과 통찰력 확보)

ITEASY insight

네트워크 모니터링 서비스 가이드

목차

1. 개요

1.1. 서비스 컨셉	2
1.2. 서비스 동의	2
1.3. 샘플링 방식으로 트래픽 수집	2

2. 기능 명세

2.1. 보안 이벤트	3
2.2. 보고서	3
2.3. 트래픽 분석	3
2.4. 요약	3
2.5. 문의하기	3
2.6. 고객 의견	3
2.7. 서비스 철회	3

3. 베타 서비스 vs 정식 서비스	4
---------------------------	---

4. 서비스 시작하기

4.1. 서비스 동의하기	5
4.2. 전체 서버 요약	8
4.3. 대시보드 홈페이지 입장	12

5. 대시보드 가이드

5.1. 대시보드 첫 화면	13
5.2. 좌측 메뉴	14
5.3. 상단 메뉴	15
5.4. 전체 서버	16
5.4.1. 전체서버 요약	16
5.4.2. 전체서버 목록	20
5.5. 그룹 생성	21
5.6. 그룹 서버	23
5.6.1. 그룹서버 요약	23
5.6.2. 그룹수정 및 그룹삭제	27
5.6.3. 그룹서버 목록	29
5.7. 개별서버 요약	30
5.8. 트래픽 분석	34
5.8.1. 트래픽 분석 순서	35
5.9. 보안 이벤트	38
5.9.1. 보안 이벤트 설정	39
5.9.2. 보안 이벤트 목록	41
5.9.3. 보안 이벤트 상세	42

5.10. 보고서	45
5.10.1. 보고서 설정	46
5.10.2. 보고서 목록	48
5.10.3. 보고서 상세	49
5.10.4. 주간 보고서(이메일)	54
5.11. 문의하기	56
5.11.1. 문의 목록	56
5.11.2. 문의하기	57
5.11.3. 문의 상세	57
5.12. 고객의견	58
5.12.1. 고객의견 목록	58
5.12.2. 고객의견	59
5.12.3. 고객의견 상세	59
5.13. History	60
5.14. 설정	61
5.14.1. 보안 이벤트 설정	61
5.14.2. 보고서 설정	64
5.14.3. 서비스 철회	67

6. Appendix

6.1. 보안 이벤트(공격탐지)	68
6.2. 보안 이벤트(블랙리스트IP 접근탐지)	69
6.3. 보안 이벤트 대응방법	69
6.3.1. SELF 대응	69
6.3.2. 상담 및 지원	69
6.4. 보안 이벤트 구조적 문제	70

네트워크 모니터링 서비스 가이드

날짜: 2021.04.01

버전: 1.0

설명: 본 문서는 네트워크 모니터링 서비스 가이드 문서입니다.

1. 개요

네트워크 모니터링 서비스의 컨셉, 서비스를 이용하는 첫단추인 서비스 동의, 기반기술에 대한 설명을 드립니다.

1.1. 서비스 컨셉

이용자서버 트래픽을 면밀하게 분석하여 '유해요소'를 탐지합니다. (보안 이벤트)

이용자서버 트래픽을 면밀히 분석하여 유익한 통계정보를 제공해 드립니다. (보고서)

이용자서버 트래픽을 정밀하게 분석할 수 있는 Tool을 제공해 드립니다. (트래픽 분석)

이용자서버가 많아도, 트래픽 통계 정보를 한눈에 파악할 수 있습니다. (전체서버 요약, 그룹서버 요약)

이용자 서버에 설치하는 서비스가 아닙니다.

서비스 동의를 하시면, 당사 별도 장비에서 트래픽을 수집하고 분석합니다.

이용자서버 자원은 서비스하는 곳에서만 온전히 사용하세요.

당사 호스팅 및 코로케이션 이용자에게 무료로 제공되는 서비스입니다.

1.2. 서비스 동의

이용자께서 동의를 해 주셔야 사용이 가능한 서비스입니다.

원하는 서비스가 아니라고 생각되면, 언제든지 서비스 철회가 가능합니다.

이용자께서 동의를 하지 않으셨더라도, 24시간 동안 트래픽 데이터를 수집하고 있습니다.

동의 시점에 서비스를 바로 보여드리기 위함입니다. (너그러운 이해 부탁드립니다.)

동의를 하지 않은 이용자의 트래픽 데이터는 자정을 기준으로 삭제합니다.

1.3. 샘플링 방식으로 트래픽 수집

sflow 기술을 이용한 서비스입니다.

1/4000 비율로 트래픽을 수집하며, 트래픽 용량을 계산할 때 4000의 가중치로 계산합니다. (BMT 결과, 10Mb/s 이상의 트래픽 이용자에서는 90% 이상의 정확도를 확인하였습니다.)

2. 기능 명세

네트워크 모니터링 서비스의 중요기능을 간략하게 설명을 드립니다. (상세 내용은 해당 문서 '대시보드 가이드' 를 참고해 주시기 바랍니다.)

2.1. 보안 이벤트

이용자 서버의 트래픽을 면밀히 분석하여, 네트워크 공격 및 블랙리스트IP 접근을 탐지합니다.
탐지 정보를 이용자에게 제공해 드리며, SELF 대응 방법에 대해서도 기술합니다.

저희 엔지니어팀이 대기중에 있습니다.

조치하시기 어려우시거나, 지원이 필요할 경우 언제든지 문의주십시오. ([온라인 문의](#), 전화 번호 : 1600-8324[서비스운영팀])

2.2. 보고서

주간 보고서에는 다음과 같은 내용이 기술됩니다.

1. 트래픽 추이
2. 일간/시간별 서버 및 클라이언트 트래픽 통계, 국가 접근 통계
3. 일간/시간별 서버 및 공격IP 보안 이벤트 통계

이용자께서는 보고서의 내용으로 서비스 방향 및 정책을 수립할 수 있습니다.

2.3. 트래픽 분석

이용자 서버에서 발생한 트래픽 정보를 상세하게 확인할 수 있습니다. (클라이언트IP, 서비스Port)

2.4. 요약

특정기간동안 ' 전체서버 ' / ' 그룹서버 ' / ' 개별서버 ' 에서 발생한 트래픽 데이터를 분석하고, 분석 내용을 요약하여 제공해드립니다.

2.5. 문의하기

궁금사항, 개선사항, 서비스 불편사항이 있으시다면, 언제든지 [문의](#)하실 수 있습니다. 기술적인 지원이 필요하시다면, 언제든지 문의하실 수 있습니다.

2.6. 고객님의견

서비스에 의견이 있으시다면, 언제든지 의견을 남기실 수 있습니다.

2.7. 서비스 철회

서비스에 만족하지 못하셨다면, 언제든지 서비스 철회가 가능합니다. 서비스 철회 후 다시 서비스를 이용하실 수 있습니다. (서비스 동의 후 재사용)

3. 베타 서비스 vs 정식 서비스

해당 서비스는 오픈베타이며, 정식서비스 오픈일은 미정입니다. (오픈베타를 진행하는 동안 이용자 의견등을 수렴하여 정식서비스에 반영할 예정입니다.)

3.1. 베타 서비스 vs 정식 서비스

항목		베타 서비스	정식 서비스
데이터 보존 기간		30일	1년
이벤트 보존 기간		무제한	
그룹 생성수		5개	10개
보안 이벤트	생성수	5개	10개
	이용자에게 보여주는 방식	웹	웹, 메일
	알림 수단	-	카카오톡 메시지
보고서	생성수	5개	10개
	종류	주간 보고서	주간 보고서 월간 보고서 분기 보고서 반기 보고서 연간 보고서
	이용자에게 보여주는 방식	웹, 메일	
	알림 수단	-	카카오톡 메시지
고객 지원		온라인, 오프라인	
웹사이트 기준 해상도		1440px ~	
지원 브라우저		Chrome, Firefox, Edge(최신 버전 사용을 권고드립니다.)	

4. 서비스 시작하기

네트워크 모니터링 서비스를 시작하는 방법에 대해 설명드립니다.

[[iTEASY 홈페이지](#)]에 로그인 후 서비스 동의를 하시면, 그 즉시 네트워크 모니터링 서비스를 이용할 수 있습니다.

4.1. 서비스 동의하기

1. <https://iteasy.co.kr>에 접속 후 로그인을 합니다.

The screenshot shows the iTEASY website homepage. The header includes the logo "iTEASY It is easy, IT is easy" and a navigation menu with items: 통합컨설팅, 클라우드, 서버·IDC, 보안, 도메인, 메시지, 기업솔루션, 고객센터. There are buttons for "로그인" and "회원가입".

The main banner features the text: "EVENT 세상을 잇는 모든 IT가 다 있지! IT를 쇼핑하라, 일지마켓". Below this, it says: "코리아서버호스팅의 새로운 브랜드, 아이티이지! 서비스 무료쿠폰과 1만 포인트 적립 혜택을 누릴 수 있습니다." There are buttons for "자세히 보기" and "진행중인 이벤트 >".

At the bottom of the banner, there are three items: "실시간 이용후기", "도메인 가격 저렴해서 좋습니다.", and "고객만족도 4.9/5". To the right, it says "랭키닷컴 IDC 분야 6년연속 1위".

Below the banner, the text reads: "Easy Service for e-Business". Underneath, it says: "iTEASY는 E-Business를 위한 Total Infra 서비스를 제공합니다. iTEASY의 모든 서비스들은 모두 연결될 수 있으며, 더해질수록 큰 시너지를 발휘합니다."

2. 상단 메뉴 [서버.IDC] 하단에 [14가지 무료혜택] 을 선택합니다.

The screenshot shows the iTEASY website header with navigation links: 통합컨설팅, 클라우드, **서버.IDC**, 보안, 도메인, 메시지, 기업솔루션, 고객센터. A '로그인' button and a search icon are also visible. Below the header, the '서버.IDC' section is highlighted with a red box. Underneath, a grid of services is shown, with '14가지 무료혜택' (14 Free Benefits) highlighted in red. Other services include 서버호스팅, 코로케이션, 즉시개통 서버, 서버관리대행, 보안서비스, 부가서비스, and 온라인 자동 견적. A banner below the grid features a '실시간 이용후기' (Real-time User Review) section with the text '좋은 회사네요..' and a customer satisfaction score of 4.9/5. The main heading 'Easy Service for e-Business' is centered below the banner.

3. iTEASY INSIGHT 를 선택합니다.

The screenshot shows the iTEASY website with the '서버.IDC' menu highlighted in red. Below the header, a grid of services is displayed, with 'iTEasy INSIGHT' highlighted in red. The services include: 실시간 트래픽 사용량 (Real-time Traffic Usage), 웹로그 분석 (Weblog Analysis), 10G 백업공간 제공 (10G Backup Space Provided), KR도메인 무료 (KR Domain Free), Easy CarePack, and iTEasy INSIGHT. The iTEasy INSIGHT service description is: '고객서버로 접근하는 트래픽을 분석 및 제공하여 효율적인 의사결정을 돕습니다' (Analyze and provide traffic accessed by customer servers to help with efficient decision-making).

4. [모니터링 서비스 이용에 대한 안내] 에 동의하시면, 즉시 네트워크 모니터링 서비스를 이용하실 수 있습니다.



이용자께서 동의를 해 주셔야 사용이 가능한 서비스입니다.

이용자께서 동의를 하지 않으셨더라도, 24시간 동안 트래픽 데이터를 수집하고 있습니다.
동의 시점에 서비스를 바로 보여드리기 위함입니다. (너그러운 이해 부탁드립니다.)
동의를 하지 않은 이용자의 트래픽 데이터는 자정을 기준으로 삭제합니다.

4.2. 전체서버 요약

대시보드 홈페이지에 입장하기 전, 맛보기 페이지입니다.

iTEASY

마이페이지 홈 요금 관리 내 정보 관리 포인트 / 쿠폰

로그아웃 고객센터 ☰

member since 2017.02

견적문의 >

서비스문의 >

작업의뢰 >

원격지원 >

서비스문의 49 건

작업의뢰 225 건

적립 Point 0 포인트

사용 가능 쿠폰 0 장

진행중인 이벤트

INSIGHT

마지막접속일 : 2021년 03월 31일 09:31

공지사항 / 뉴스
쉽고 안전한 IT인프라 토탈 서비스 '아이티이시' OPEN
2020. 11. 23

🏠
서버 / IDC
모니터링
ITEASY INSIGHT

ITEASY INSIGHT

이용자 서버 트래픽을 면밀히 분석하여, '유해요소'와 '유익한 통계정보'를 제공해 드립니다.
 이용자께서는 위 데이터를 기반으로 운영 가시성, 현명하고 효율적인 의사결정, 전체 서비스에 대한 통찰력을 확보할 수 있습니다.

모니터링 서비스로 이동하기

보안 이벤트

서버명	서버IP	이벤트	Date
Full Rack	1234	불특 IP 에서 접속 시도가 많...	21/04/09 15:30
Full Rack	1234	불특 IP 에서 접속 시도가 많...	21/04/09 15:00
IP대역	1234	불특 IP 에서 접속 시도가 많...	21/04/09 15:00
IP대역	58.229	불특 IP 에서 접속 시도가 많...	21/04/09 14:30
Full Rack	1234	불특 IP 에서 접속 시도가 많...	21/04/09 13:30

공지사항

제목	Date
통합 모니터링 공지사항 테스트입니다.	21/04/01 19:58
공지사항 길이 테스트 공지사항 길이 테스트 공지사항 길이 테스트	21/03/17 15:28
통합 모니터링 공지사항 입니다.	21/03/17 14:58
테스트 공지사항1234	21/03/11 15:15
테스트 공지	21/02/26 12:48

트래픽 Top5

인바운드

2021/04/09 00:00 - 2021/04/09 17:00

클라이언트 IP Top5

인바운드

2021/04/09 00:00 - 2021/04/09 17:00

- 9.9% 14.192.89.9(KR)
- 8.9% 121.78.238.222(KR)
- 7.6% 121.78.247.18(KR)
- 6.5% 1.201.146.37(KR)
- 6.4% 121.78.238.224(KR)
- 60.6% 기타

클라이언트 IP	서버IP	용량(비율)
14.192.89.9(KR)	선택 그룹	281.9CB(9.9%)
121.78.238.222(KR)		252.7CB(8.9%)
121.78.247.18(KR)		216.6CB(7.6%)
1.201.146.37(KR)		184.8CB(6.5%)
121.78.238.224(KR)		181.7CB(6.4%)

서버 IP Top5

인바운드

2021/04/09 00:00 - 2021/04/09 17:00

- 15.9% 58.229 (KR)
- 14.3% 58.229 (KR)
- 12.7% 1.234 (KR)
- 11.3% 1.234 (KR)
- 5.6% 1.234 (KR)
- 40.2% 기타

클라이언트 IP	서버IP	용량(비율)
*	58.229 (KR)	451.7CB(15.9%)
	58.229 (KR)	404.1CB(14.3%)
	1.234 (KR)	360.0CB(12.7%)
	1.234 (KR)	321.5CB(11.3%)
	1.234 (KR)	158.6CB(5.6%)

4.2.1. 전체서버 요약의 각 항목 설명

보안 이벤트

금일에 발생한 보안 이벤트입니다.

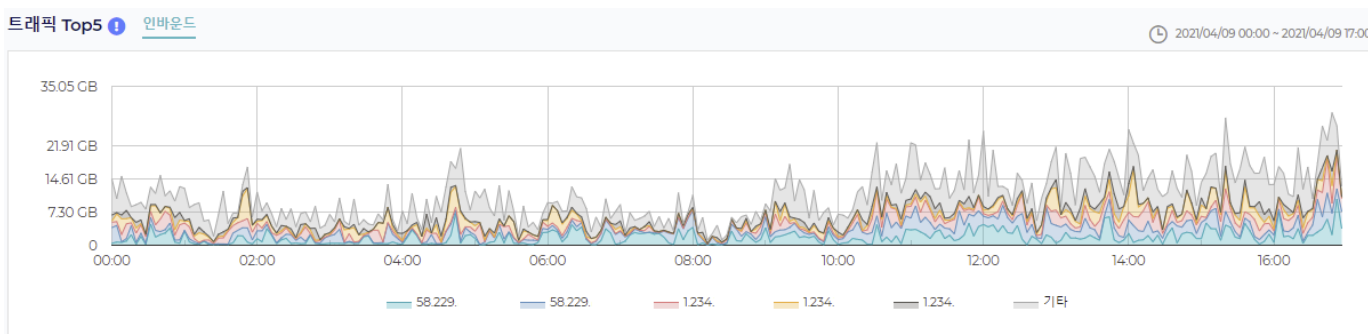
보안 이벤트 ⓘ			
서버명	서버IP	이벤트	Date
Full Rack	1.234.	블랙 IP 에서 접속 시도가 감...	21/04/09 15:30
Full Rack	1.234.	블랙 IP 에서 접속 시도가 감...	21/04/09 15:00
IP대역	1.234.	블랙 IP 에서 접속 시도가 감...	21/04/09 15:00
IP대역	58.229.	블랙 IP 에서 접속 시도가 감...	21/04/09 14:30
Full Rack	1.234.	블랙 IP 에서 접속 시도가 감...	21/04/09 13:30

트래픽 Top5

금일 0시부터 현시간까지의 트래픽 그래프이며, 이용자께서 운영하시는 전체서버중에 트래픽을 가장 많이 사용한 서버 5대의 트래픽 그래프입니다.

인바운드 트래픽만 표시됩니다.

대시보드로 이동하시면 좀 더 상세한 내용을 확인할 수 있습니다.



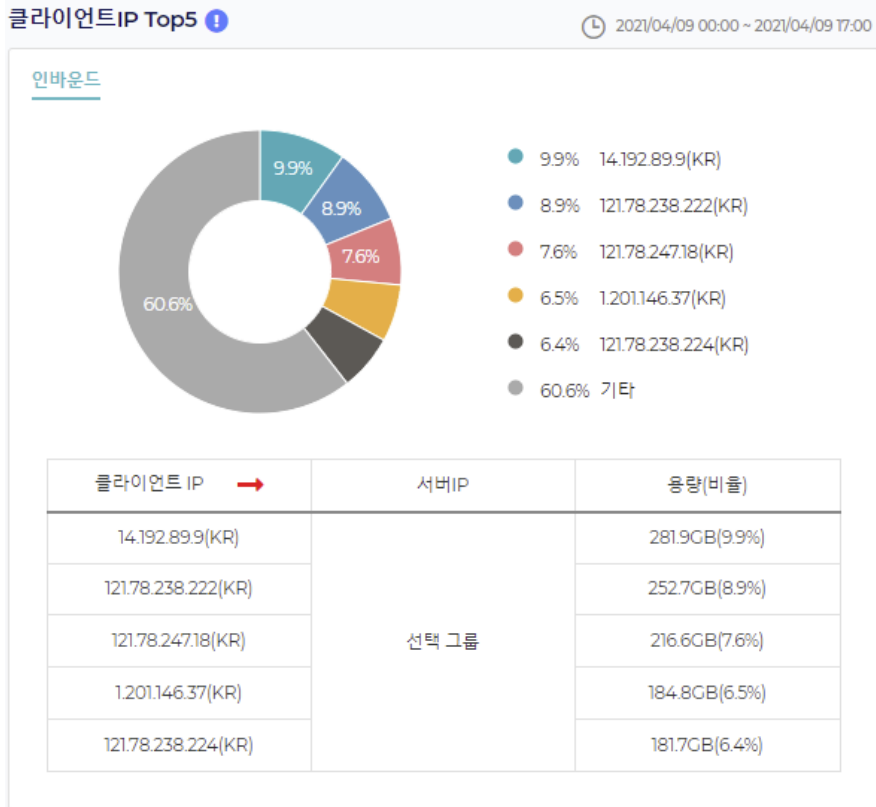
클라이언트IP Top5

금일 0시부터 현시간까지 트래픽 차트이며, 이용자께서 운영하시는 전체서버에 가장 많이 접근한 클라이언트 5개의 IP 입니다.

클라이언트의 트래픽 용량을 확인할 수 있습니다.

인바운드 트래픽만 표시됩니다.

대시보드로 이동하시면 좀 더 상세한 내용을 확인할 수 있습니다.



KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 '-' 으로 표시됩니다.

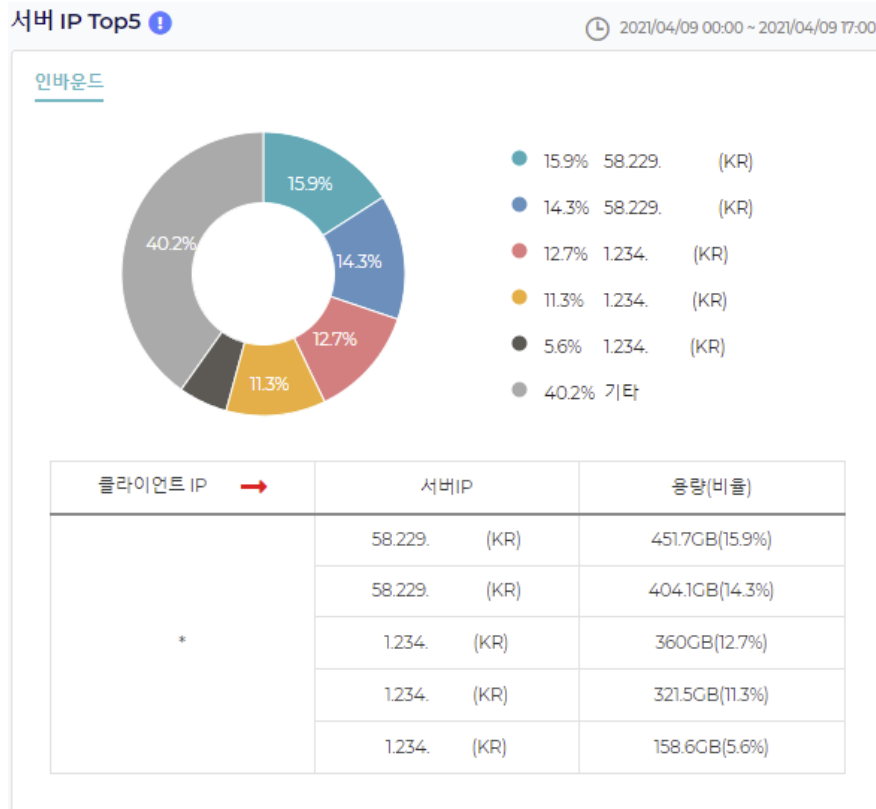
서버IP Top5

금일 0시부터 현재시간까지 트래픽 차트이며, 이용자께서 운영하시는 전체서버중에 트래픽을 가장 많이 사용한 서버 5대입니다.

서버의 트래픽 용량을 확인할 수 있습니다.

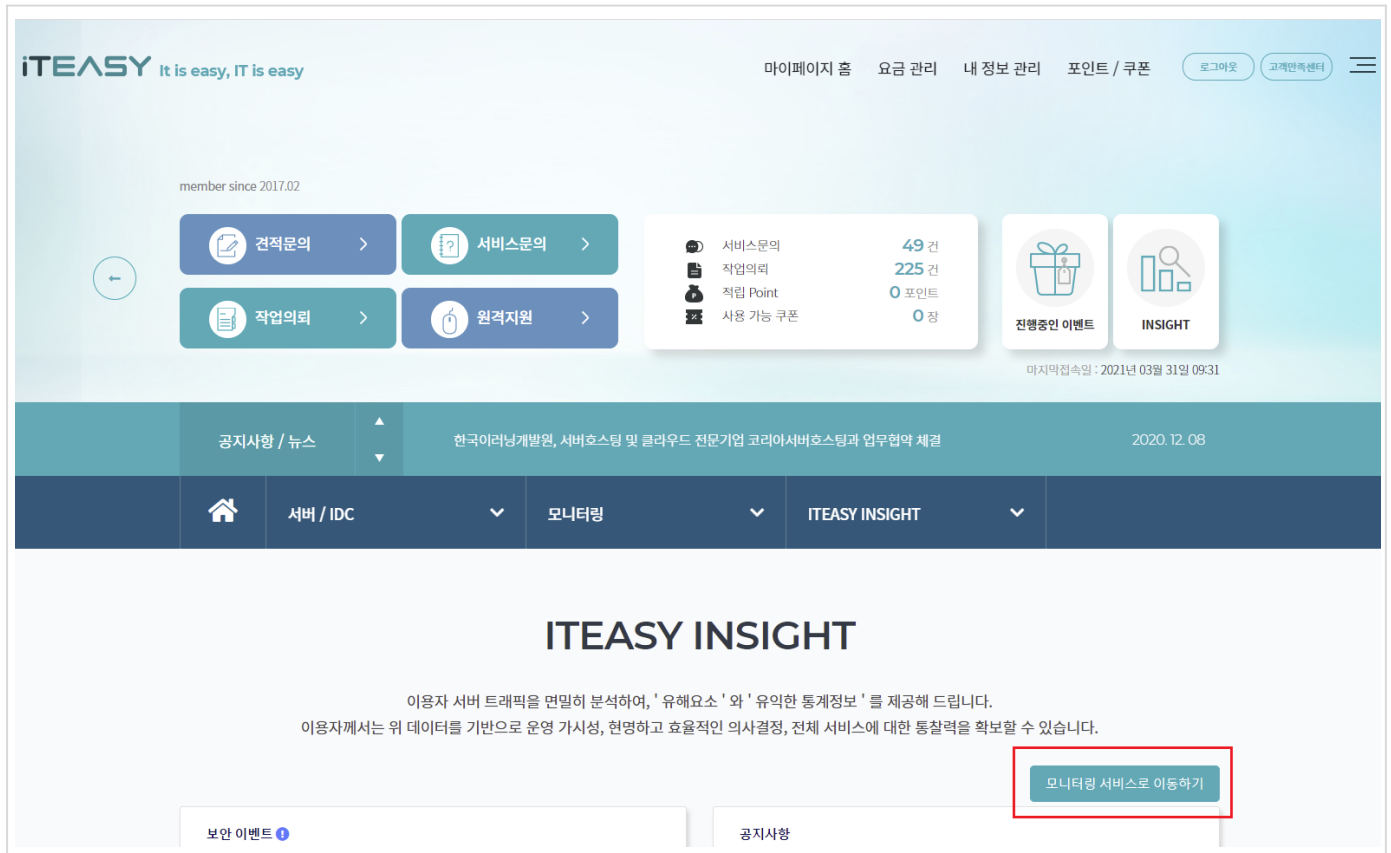
인바운드 트래픽만 표시됩니다.

대시보드로 이동하시면 좀 더 상세한 내용을 확인할 수 있습니다.



4.3. 대시보드 홈페이지 입장

'모니터링 서비스로 이동하기' 버튼을 클릭하면, [대시보드 홈페이지] 로 이동합니다.



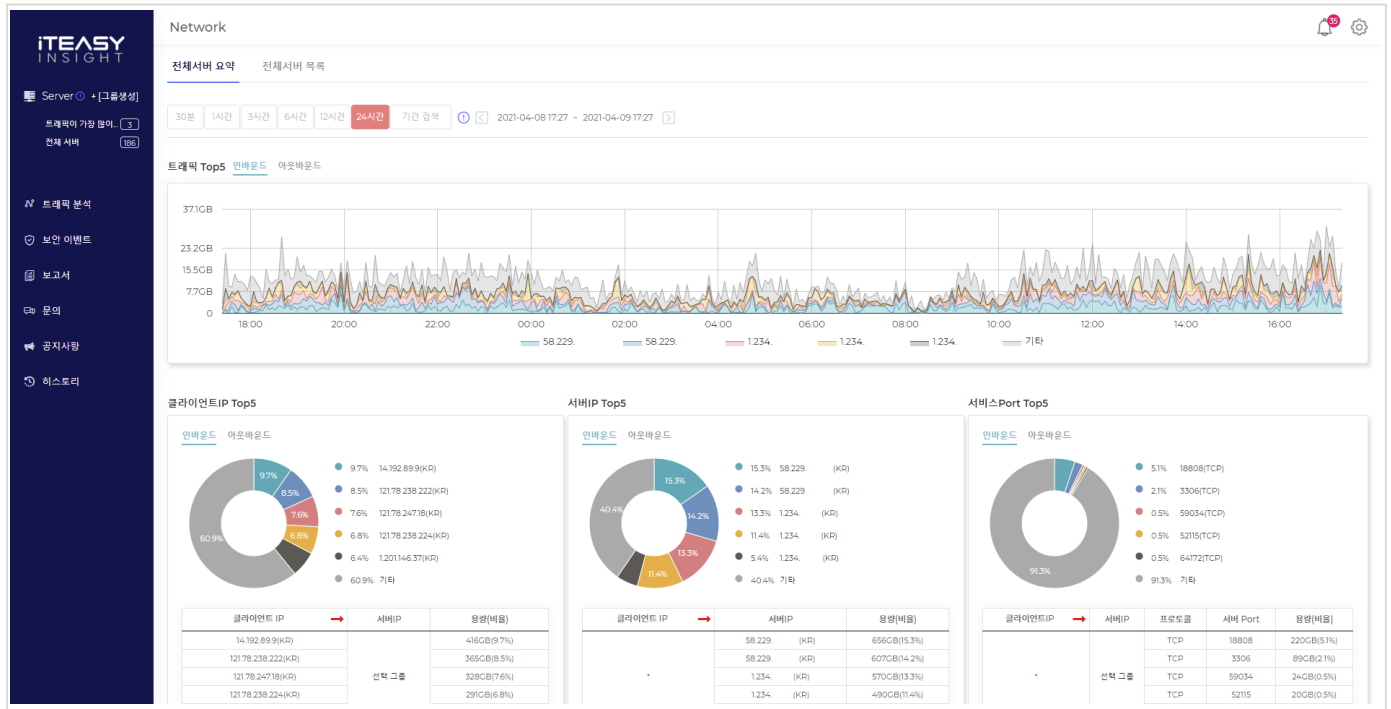
5. 대시보드 가이드

대시보드의 상세한 내용을 설명 드립니다.

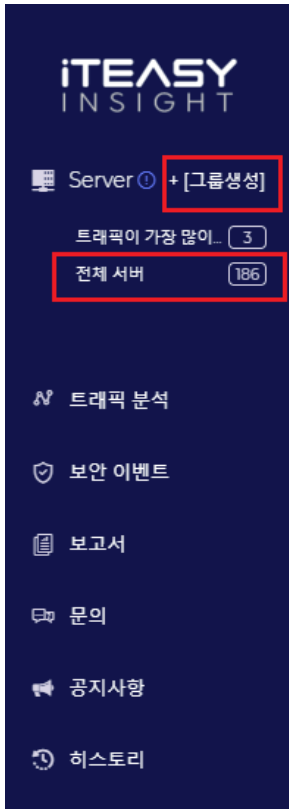
5.1. 대시보드 첫 화면

iTEASY 홈페이지에서 '모니터링 서비스로 이동하기' 버튼 클릭 시, '전체서버 요약' 페이지로 이동합니다.

이미 서비스 동의를 하셨다면, Direct 로 [[대시보드 홈페이지](https://console.iteasy.co.kr)] 에 접근할 수 있습니다. (<https://console.iteasy.co.kr>)



5.2. 좌측 메뉴



5.2.1. 전체 서버

당사에서 호스팅을 받고 있는 서버를 의미합니다.

5.2.2. 그룹 생성

많은 서버를 한번에 관리하기 어려운 부분이 있습니다.

서비스 목적에 맞게 그룹을 생성하고, 그룹별로 모니터링하실 수 있습니다. (해당 문서 하단에서 좀 더 자세하게 설명드리겠습니다.)

다음과 같은 이유로 그룹을 생성합니다.

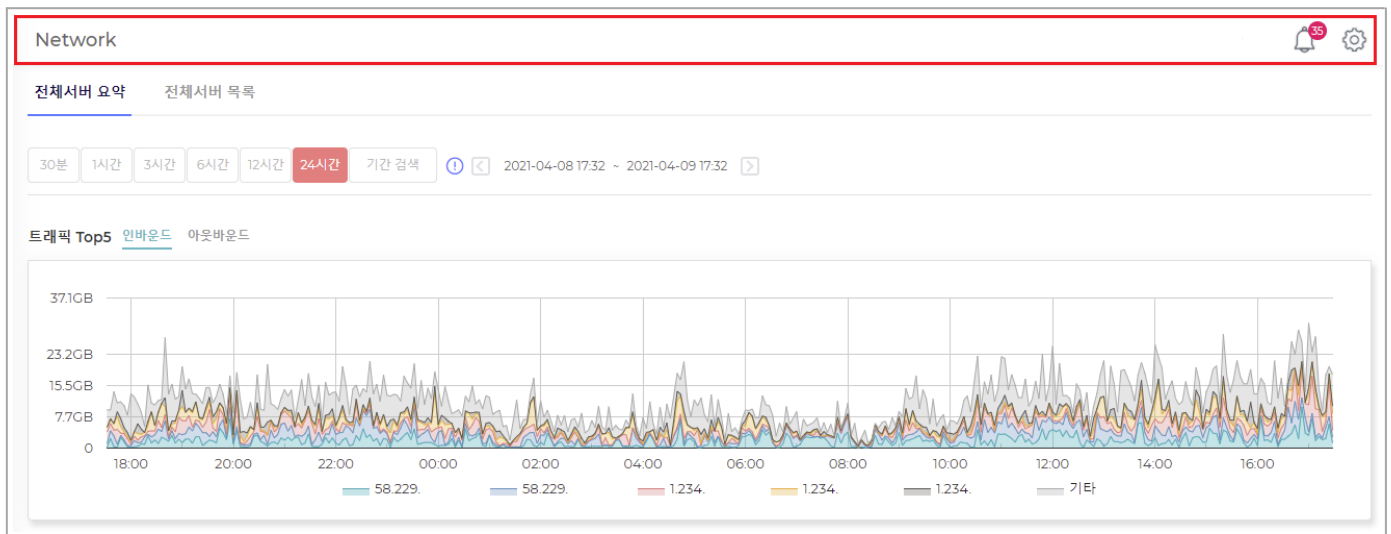


1. 그룹 서버별로 요약을 확인할 수 있습니다.
2. 그룹 서버별로 보안이벤트를 수신할 수 있습니다.
3. 그룹 서버별로 보고서를 수신할 수 있습니다.



트래픽을 기준으로 서버 목록을 생성하고 있어, 트래픽이 적게 나오는 서버는 목록에서 누락될 수 있습니다.
(이럴 경우, [[문의하기](#)] 를 통하여 서버를 추가해 달라고 요청하실 수 있습니다.)

5.3. 상단 메뉴



5.3.1. 종

금일에 발생한 보안 이벤트 목록입니다.

종을 클릭하면, 보안 이벤트 페이지로 이동합니다. (해당 문서 하단에서 좀 더 자세하게 설명드리겠습니다.)

5.3.2. 설정

보안 이벤트, 보고서 설정 페이지입니다.

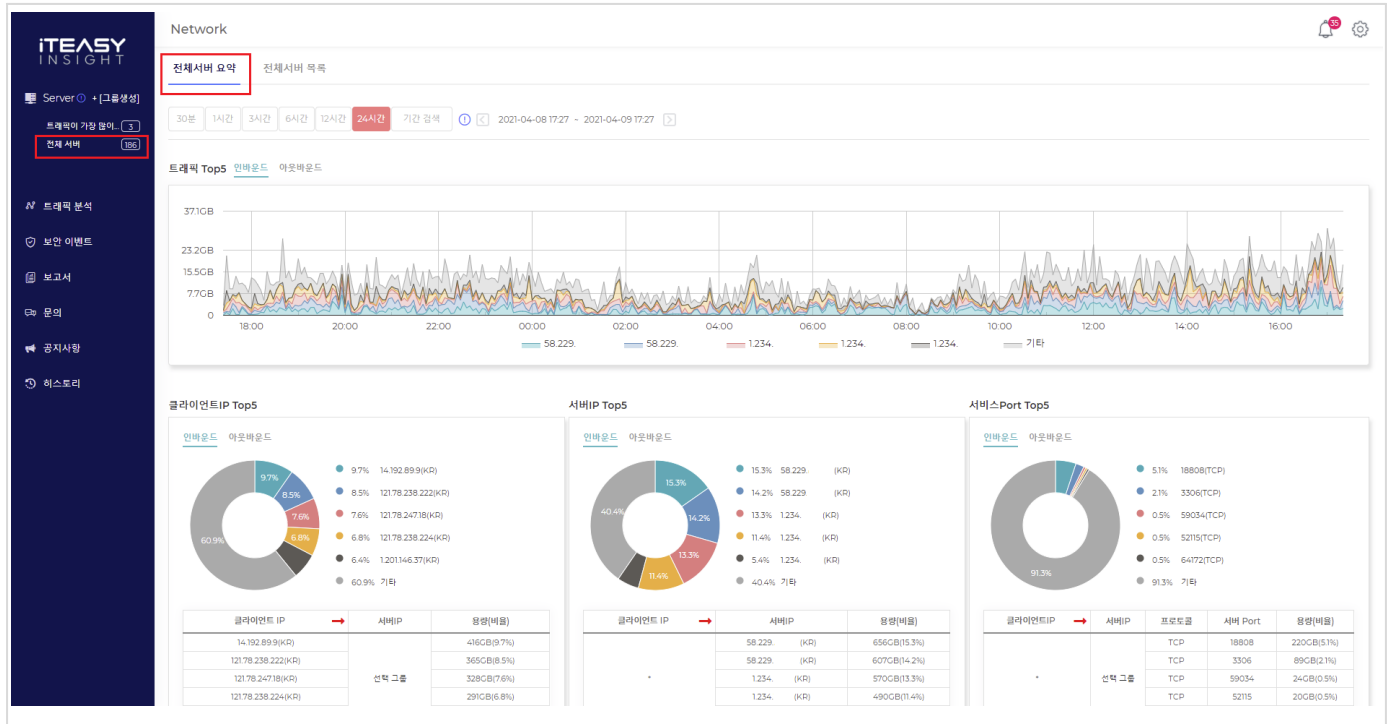
서비스가 마음에 들지 않을 경우, 서비스 철회를 할 수 있는 페이지도 포함되어 있습니다. (해당 문서 하단에서 좀 더 자세하게 설명드리겠습니다.)

5.4. 전체 서버

5.4.1. 전체서버 요약

이용자께서 운영하시는 전체서버의 통계 데이터입니다.

좌측 메뉴 '전체 서버' 를 클릭하시면, 전체서버 요약 페이지로 이동합니다.

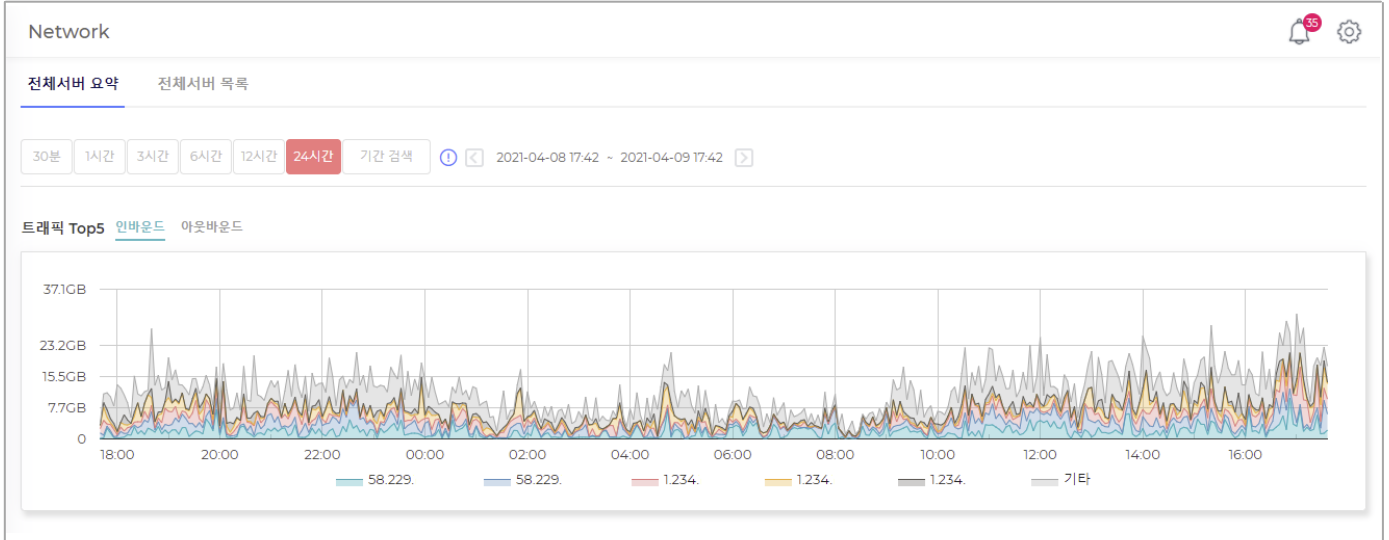


5.4.1.1. 전체서버 요약의 각 항목 설명

트래픽 Top5

최근 24시간 동안 전체서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 전체서버중에 트래픽을 가장 많이 사용한 서버 5대의 트래픽 그래프입니다.

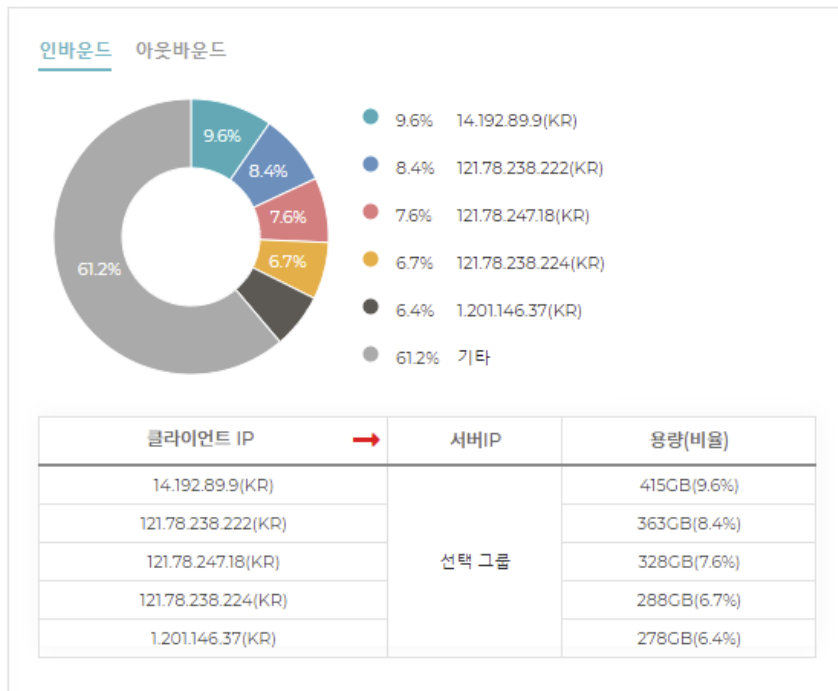


클라이언트IP Top5

최근 24시간 동안 전체서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 전체서버에 가장 많이 접근한 클라이언트 5개의 IP 입니다. 클라이언트의 트래픽 용량도 확인할 수 있습니다.

클라이언트IP Top5



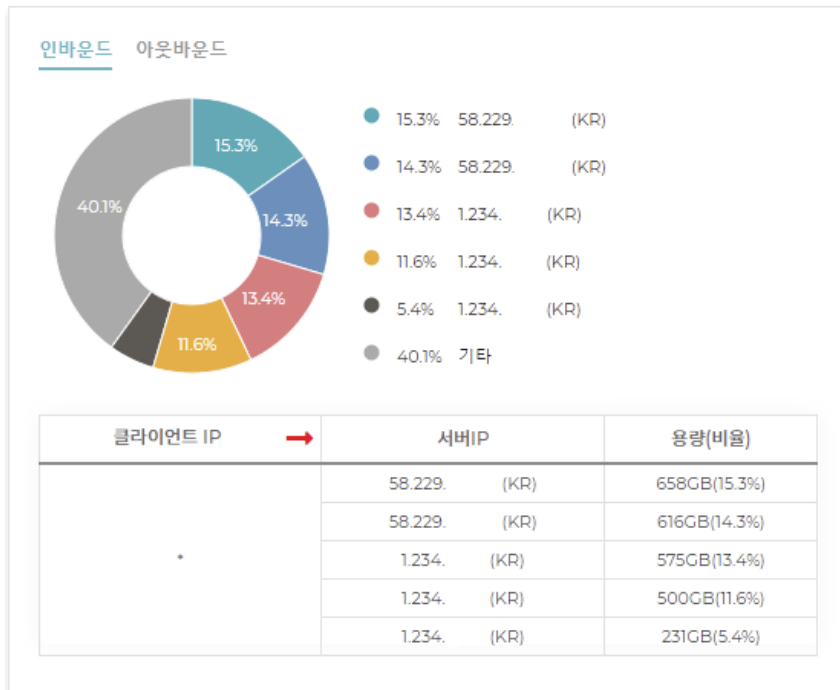
KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 ' - ' 으로 표시됩니다.

서버IP Top5

최근 24시간 동안 전체서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 전체서버중에 트래픽을 가장 많이 사용한 서버 5대입니다. 트래픽 용량도 확인할 수 있습니다.

서버IP Top5

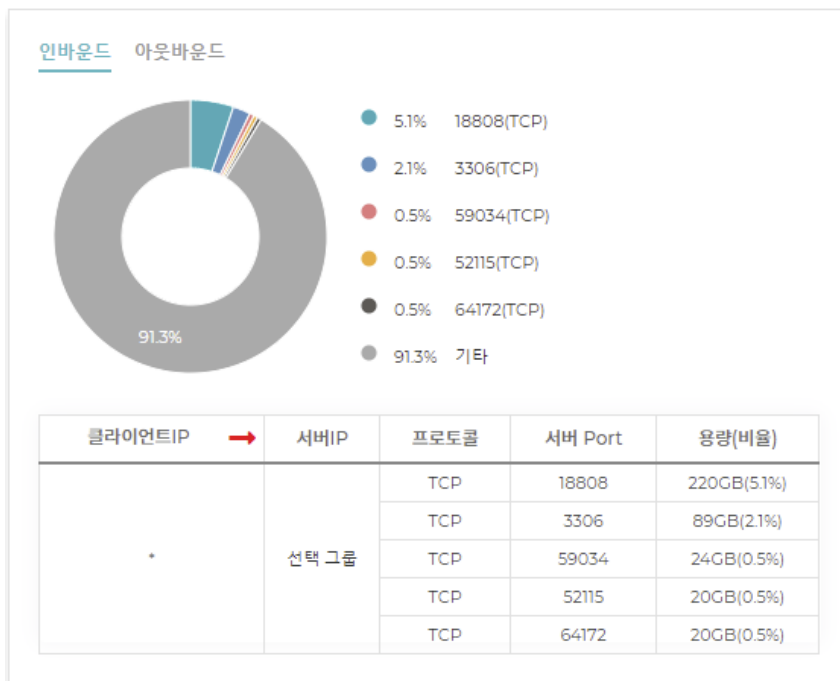


서비스Port Top5

최근 24시간 동안 전체서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

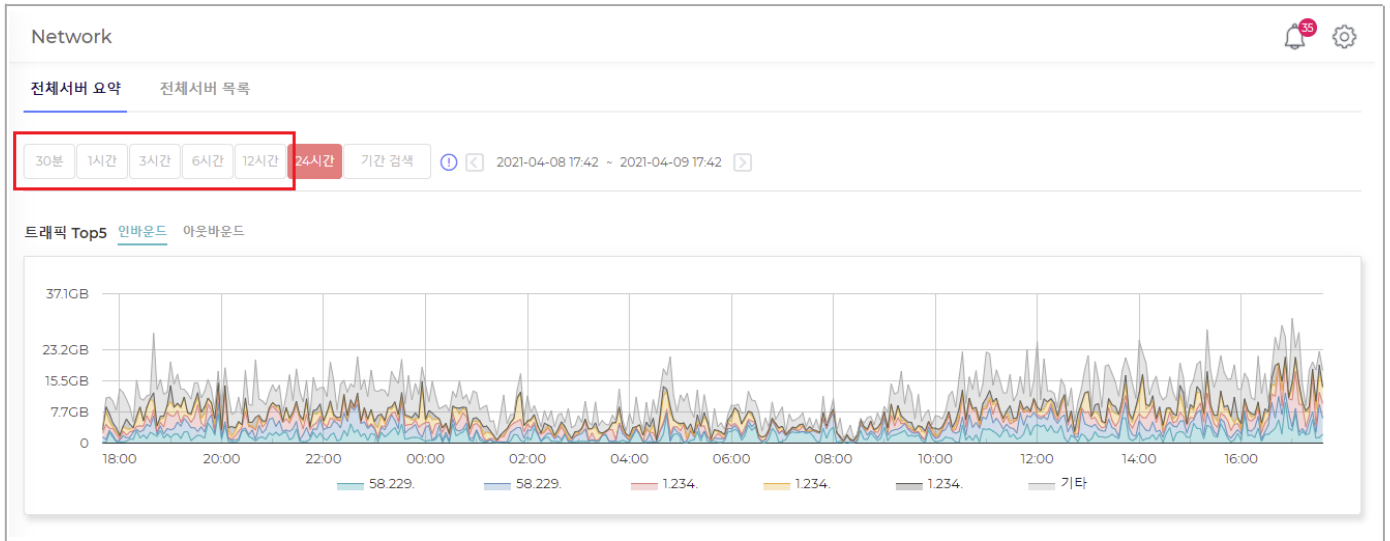
이용자께서 운영하시는 전체서버중에 트래픽을 가장 많이 사용한 서비스 Port 5개 입니다. 프로토콜, 서버Port, 용량을 확인할 수 있습니다.

서비스Port Top5



실시간 검색

실시간 데이터를 검색 할 수 있는 버튼입니다. (24시간까지만 실시간 검색이 가능합니다.)

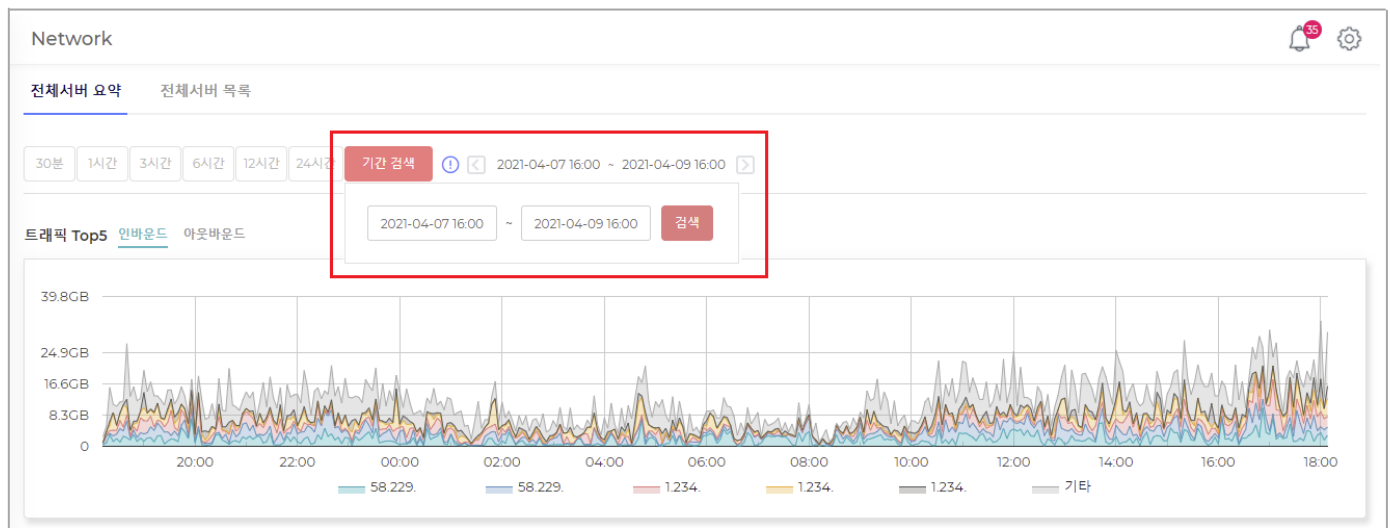


기간 검색

실시간 데이터를 검색 할 수 없지만, 현재시간-2H 까지 검색이 가능하며, 최대 30일 이전의 데이터를 검색할 수 있습니다.

현재시간이 13:00 이라면, 11:00까지 검색 가능합니다. (검색범위 : -30일~현재시간-2H)

최소 검색 단위는 2시간 입니다.



검색 후 < > 버튼을 이용하여, 시간을 이동할 수 있습니다. (해당 기능은 기간 검색에서만 가능합니다.)

5.4.2. 전체서버 목록

이용자께서 운영하시는 전체서버입니다. (코리아서버호스팅에서 호스팅을 받고 있는 서버)

Traffic

금일 0시부터 현재시간까지의 누적 트래픽 용량입니다.

Network 🔔³⁶ ⚙️

전체서버 요약 전체서버 목록

🔍
검색 초기화 정렬 초기화

NO.	↓	서버명	서버IP	운영체제	트래픽(outbound) 📈	트래픽(inbound) 📉	수정
186		SuperServer 5029S-TF	58.229.	linux	2TB	455GB	🔗
185		SuperServer 5029S-TF	58.229.	linux	482MB	124GB	🔗
184		SuperServer 5029S-TF	58.229.	linux	697MB	174GB	🔗
183		SuperServer 5029S-TF	58.229.	linux	3TB	515GB	🔗
182		SuperMicro SS6028R	1.234.	linux	705MB	177GB	🔗
181		SuperMicro SS6028R	1.234.	linux(CentOS6)	19MB	148MB	🔗
180		SuperMicro SS6028R	1.234.	linux	984KB	240KB	🔗
179		SuperMicro SS6028R	1.234.	linux	612MB	159GB	🔗
178		SuperMicro SS6028R	1.234.	linux	721MB	179GB	🔗
177		SuperMicro SS6028R	58.229.	linux	16GB	12GB	🔗
176		SuperMicro SS6028R	1.234.	linux	676MB	163GB	🔗
175		SuperMicro SS6028R	1.234.	linux	7GB	12GB	🔗
174		SuperMicro SS5029S-TF	58.229.	linux	173GB	2GB	🔗
173		SuperMicro SS5029S-TF	1.234.	linux	952KB	240KB	🔗
172		SuperMicro SS5029S-TF	1.234.	linux	293GB	7GB	🔗
171		SuperMicro SS5029S-TF	1.234.	linux	373GB	7GB	🔗
170		SuperMicro SS5029S-TF	58.229.	linux	0	240KB	🔗
169		SuperMicro SS5029S-TF	58.229.	linux(CentOS6)	558GB	8GB	🔗

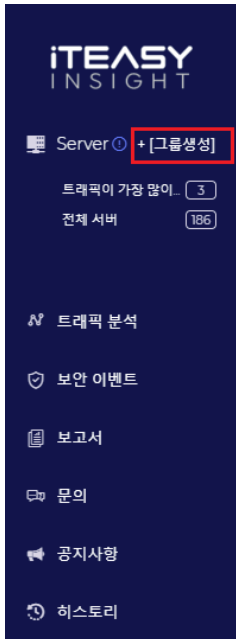


트래픽을 기준으로 서버 목록을 생성하고 있어, 트래픽이 적게 나오는 서버는 목록에서 누락될 수 있습니다.
 (이럴 경우, [문의하기](#)) 를 통하여 서버를 추가해 달라고 요청하실 수 있습니다.)

5.5. 그룹 생성

좌측메뉴의 '그룹생성' 을 클릭하면, 그룹생성 팝업 페이지가 나타납니다.

그룹생성 팝업 페이지에서 그룹을 생성할 수 있습니다.



그룹 만들기 ⓘ

그룹 이름 *

그룹내에 포함될 서버를 선택하세요 *

<input type="checkbox"/> 전체서버	<input type="checkbox"/> IP대역(58.229.)
<input type="checkbox"/> dfsa(58.229.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> Full Rack(58.229.)	<input type="checkbox"/> IP대역(58.229.)
<input type="checkbox"/> IP대역(58.229.)	<input type="checkbox"/> Full Rack(1.234.)
<input type="checkbox"/> aaaaaaaaa...(58.229.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> SuperMicro...(1.234.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> Full Rack(58.229.)	<input type="checkbox"/> IP대역(58.229.)

취소 그룹 생성

최소 1대의 서버를 선택하여야, 그룹을 생성할 수 있습니다. (그룹에 등록 가능한 서버수는 무제한 입니다.)

서버는 여러 그룹에 포함될 수 있습니다.

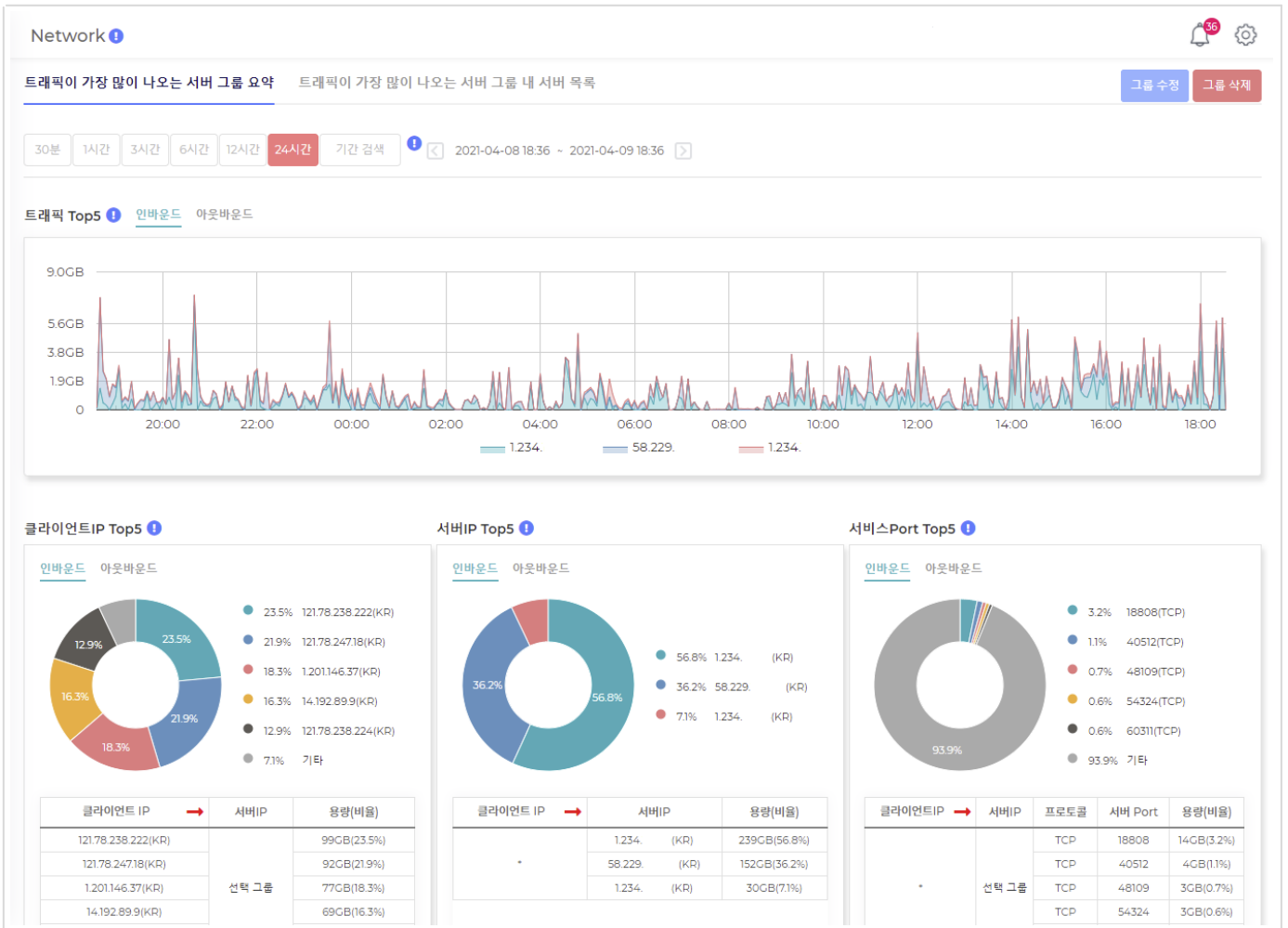
최대 5개의 그룹을 생성할 수 있습니다.

다음과 같은 이유로 그룹을 생성합니다.



1. 그룹 서버별로 요약을 확인할 수 있습니다.
2. 그룹 서버별로 보안이벤트를 수신할 수 있습니다.
3. 그룹 서버별로 보고서를 수신할 수 있습니다.

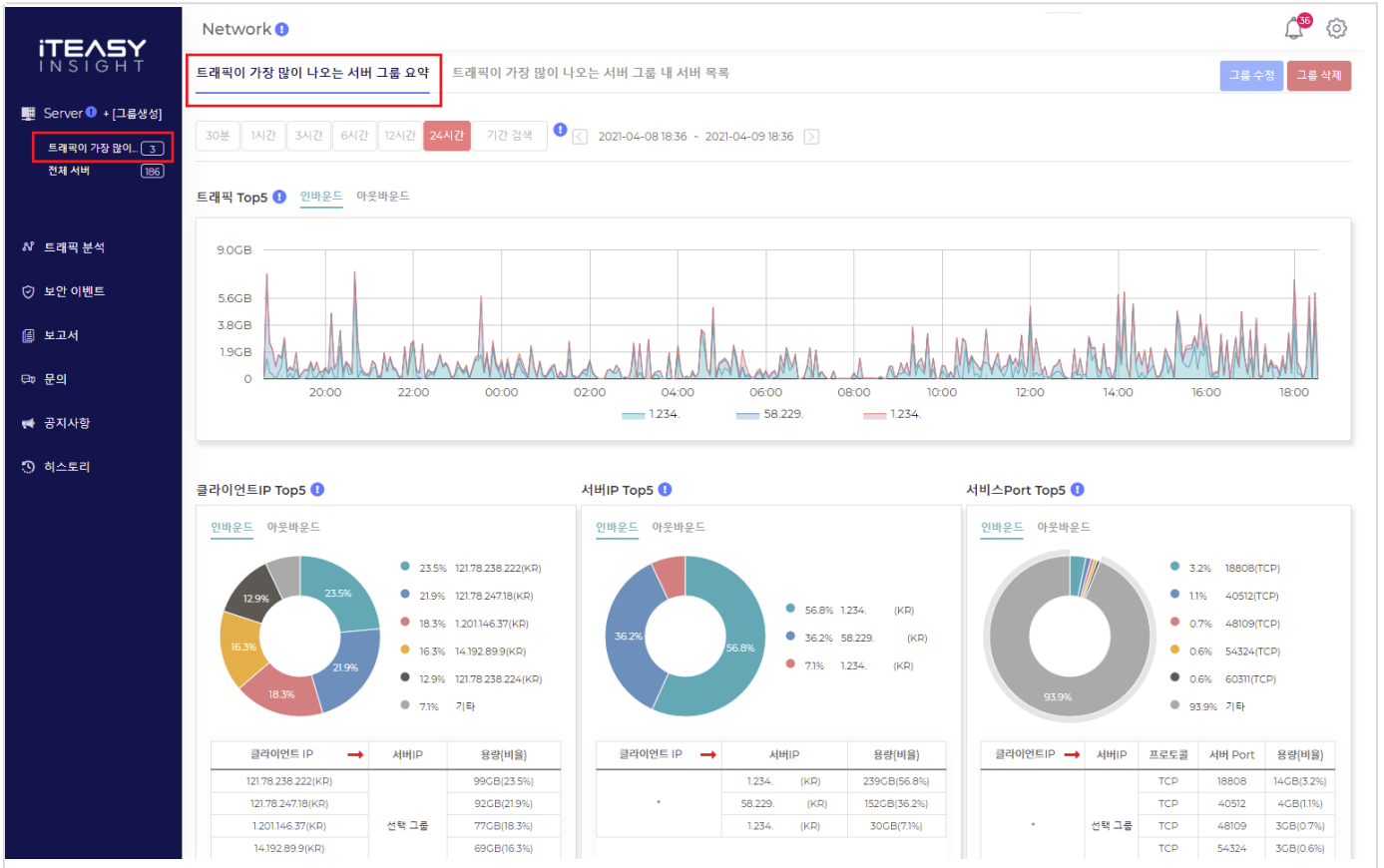
그룹 생성 후 그룹 요약 페이지로 이동합니다.



5.6. 그룹서버

5.6.1. 그룹서버 요약

좌측 메뉴 그룹이름을 클릭하시면, 그룹서버 요약 페이지로 이동합니다.



다음과 같은 이유로 그룹을 생성합니다.



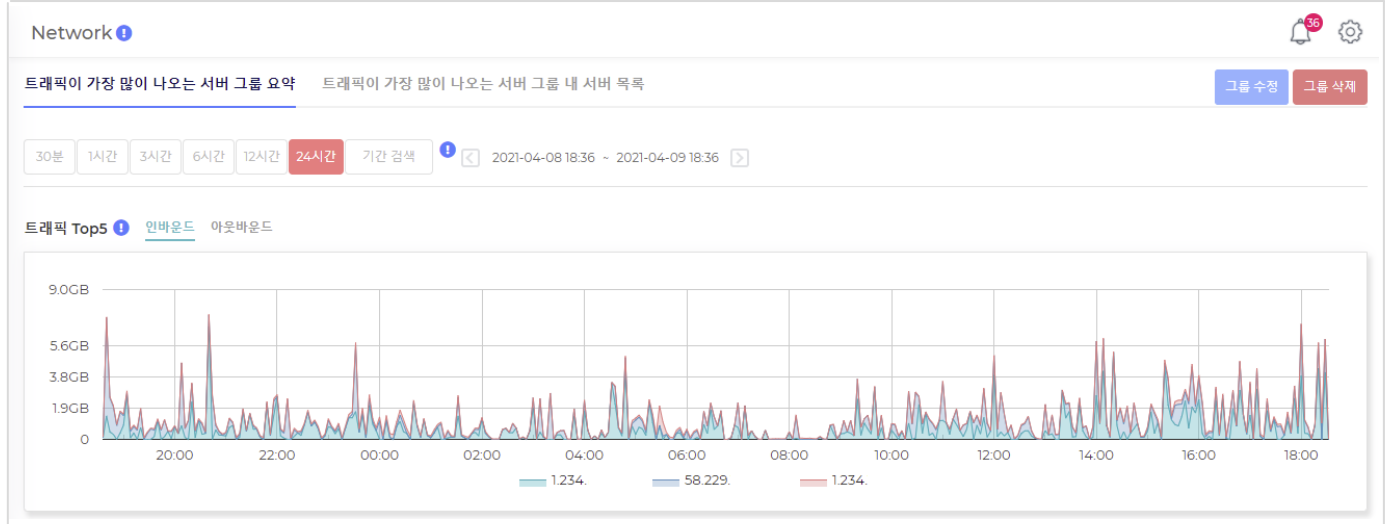
1. 그룹 서버별로 요약을 확인할 수 있습니다.
2. 그룹 서버별로 보안이벤트를 수신할 수 있습니다.
3. 그룹 서버별로 보고서를 수신할 수 있습니다.

5.6.1.1. 그룹서버 요약의 각 항목 설명

트래픽 Top5

최근 24시간 동안 그룹서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 그룹서버중에 트래픽을 가장 많이 사용한 서버 5대의 트래픽 그래프입니다.

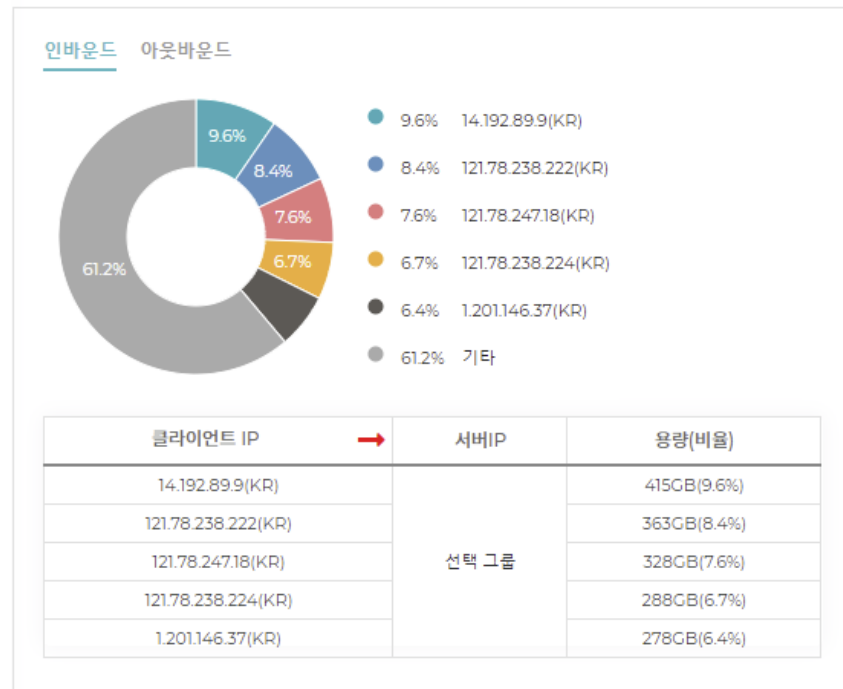


클라이언트IP Top5

최근 24시간 동안 그룹서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 그룹서버에 가장 많이 접근한 클라이언트 5개의 IP 입니다. 클라이언트의 트래픽 용량도 확인할 수 있습니다.

클라이언트IP Top5



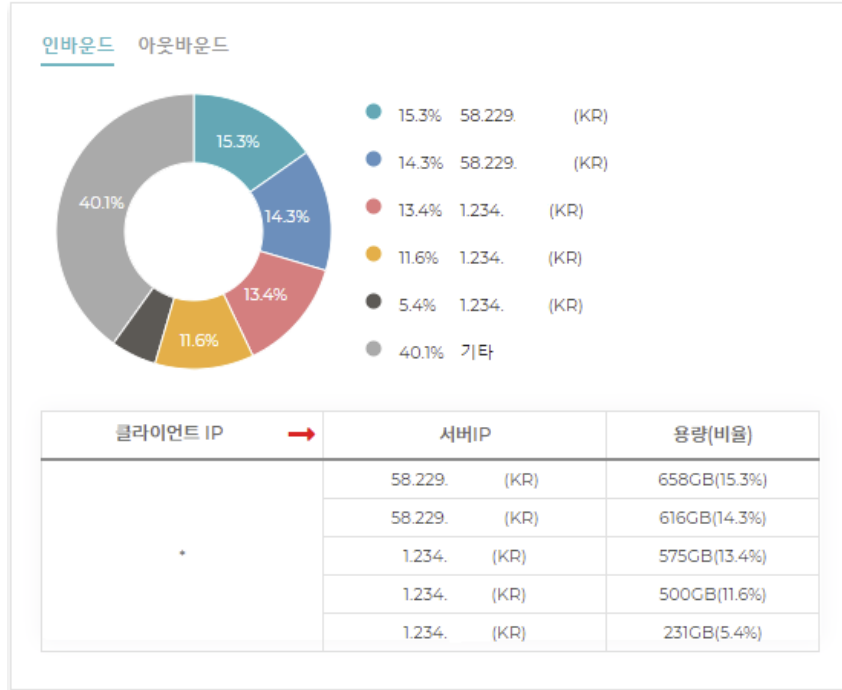
KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 '-' 으로 표시됩니다.

서버IP Top5

최근 24시간 동안 그룹서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 그룹서버중에 트래픽을 가장 많이 사용한 서버 5대입니다. 트래픽 용량도 확인할 수 있습니다.

서버IP Top5

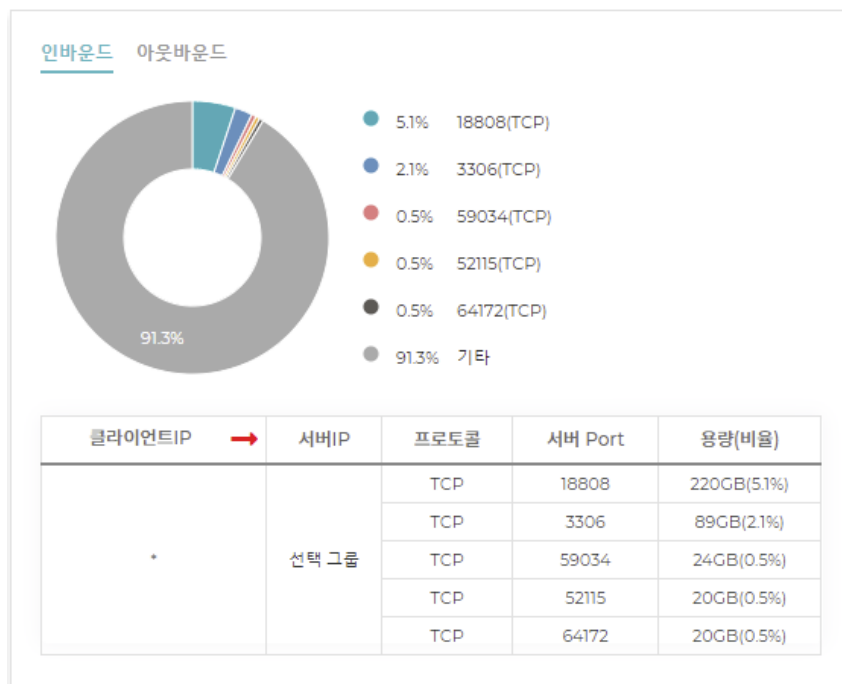


서비스Port Top5

최근 24시간 동안 그룹서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

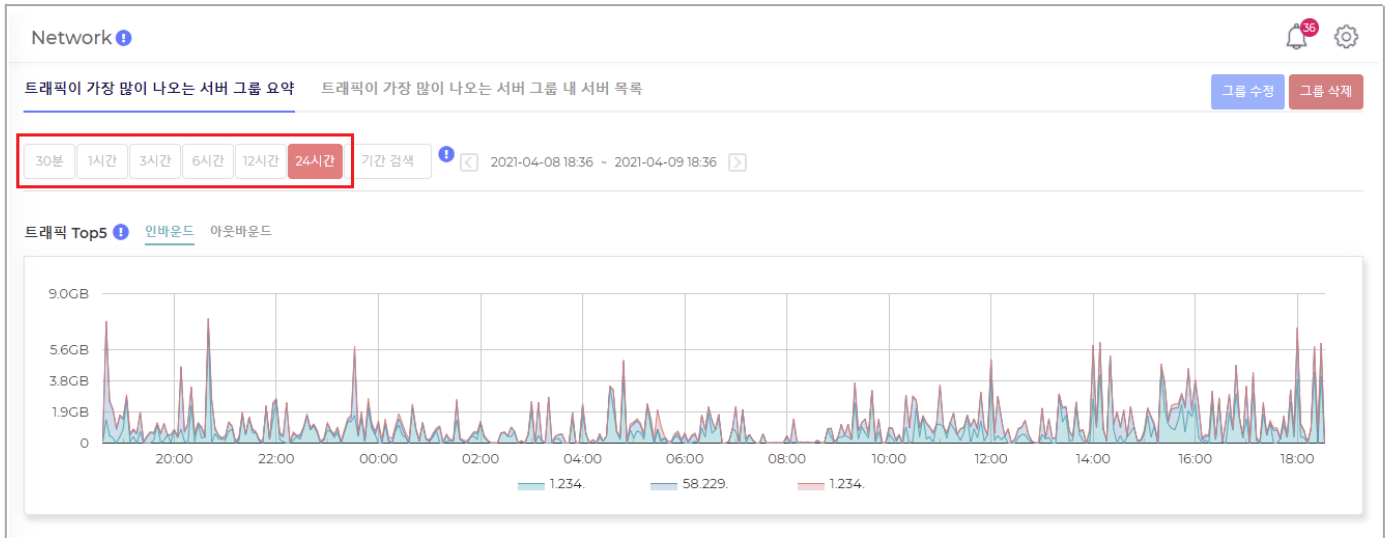
이용자께서 운영하시는 그룹서버중에 트래픽을 가장 많이 사용한 서비스 Port 5개 입니다. 프로토콜, 서버Port, 용량을 확인할 수 있습니다.

서비스Port Top5



실시간 검색

실시간 데이터를 검색 할 수 있는 버튼입니다. (24시간까지만 실시간 검색이 가능합니다.)



기간 검색

실시간 데이터를 검색 할 수 없지만, 현재시간-2H 까지 검색이 가능하며, 최대 30일 이전의 데이터를 검색할 수 있습니다.

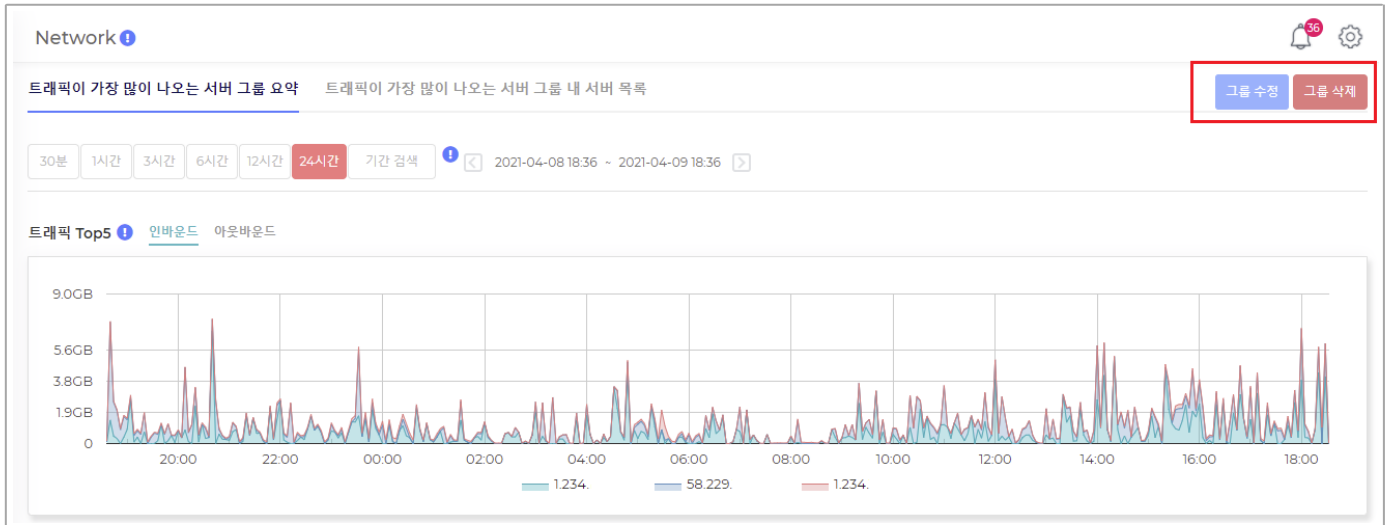
현재시간이 13:00 이라면, 11:00까지 검색 가능합니다. (검색범위 : -30일~현재시간-2H)

최소 검색 단위는 2시간 입니다.



검색 후 < > 버튼을 이용하여, 시간을 이동할 수 있습니다. (해당 기능은 기간 검색에서만 가능합니다.)

5.6.2. 그룹수정 및 그룹삭제



그룹 수정

그룹의 이름과 서버를 수정할 수 있습니다.

그룹 수정하기

그룹 이름 *

그룹내에 포함될 서버를 선택하세요 *

<input type="checkbox"/> 전체서버	
<input type="checkbox"/> dfsa(58.229.)	<input type="checkbox"/> IP대역(58.229.)
<input type="checkbox"/> Full Rack(58.229.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> IP대역(58.229.)	<input type="checkbox"/> IP대역(58.229.)
<input checked="" type="checkbox"/> aaaaaaaaaa...(58.229.)	<input checked="" type="checkbox"/> Full Rack(1.234.)
<input checked="" type="checkbox"/> SuperMicro...(1.234.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> Full Rack(58.229.)	<input type="checkbox"/> IP대역(58.229.)

취소 그룹 수정

그룹 삭제

그룹을 삭제하는 기능입니다.

주의하실 점은 그룹 삭제 시, 해당 그룹과 연계 등록되어 있는 '보안 이벤트 설정', '보고서 설정'도 같이 삭제됩니다.

그룹 삭제하기 ! ×

그룹 이름 *

그룹내에 포함될 서버를 선택하세요 *

<input type="checkbox"/> 전체서버	
<input type="checkbox"/> dfsa(58.229.)	<input type="checkbox"/> IP대역(58.229.)
<input type="checkbox"/> Full Rack(58.229.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> IP대역(58.229.)	<input type="checkbox"/> IP대역(58.229.)
<input checked="" type="checkbox"/> aaaaaaaaaa...(58.229.)	<input checked="" type="checkbox"/> Full Rack(1.234.)
<input checked="" type="checkbox"/> SuperMicro...(1.234.)	<input type="checkbox"/> Full Rack(58.229.)
<input type="checkbox"/> Full Rack(58.229.)	<input type="checkbox"/> IP대역(58.229.)

5.6.3. 그룹서버 목록

이용자께서 운영하시는 그룹서버입니다. (코리아서버호스팅에서 호스팅을 받고 있는 서버)

Traffic

금일 0시부터 현재시간까지의 누적 트래픽 용량입니다.

Network ! 98

트래픽이 가장 많이 나오는 서버 그룹 요약 트래픽이 가장 많이 나오는 서버 그룹 내 서버 목록 그룹 수정 그룹 삭제

서버명, 서버IP, 운영체제 검색 초기화 정렬 초기화

NO.	↓	서버명	서버IP	운영체제	트래픽(outbound) !	트래픽(inbound) !	수정
3		SuperMicro S56028R	1.234.	linux	768MB	191GB	
2		Full Rack	1.234.		1021GB	23GB	
1		aaaaaaaaabbbbbbbcccccccccdd	58.229.		454MB	116GB	

20 ↕ < 1 >



트래픽을 기준으로 서버 목록을 생성하고 있어, 트래픽이 적게 나오는 서버는 목록에서 누락될 수 있습니다.
(이럴 경우, [문의하기](#)) 를 통하여 서버를 추가해 달라고 요청하실 수 있습니다.)

5.7. 개별서버 요약

전체서버 목록 또는 그룹서버 목록에서 '서버명' 또는 '서버IP' 를 클릭하면, 개별서버 요약으로 이동합니다.

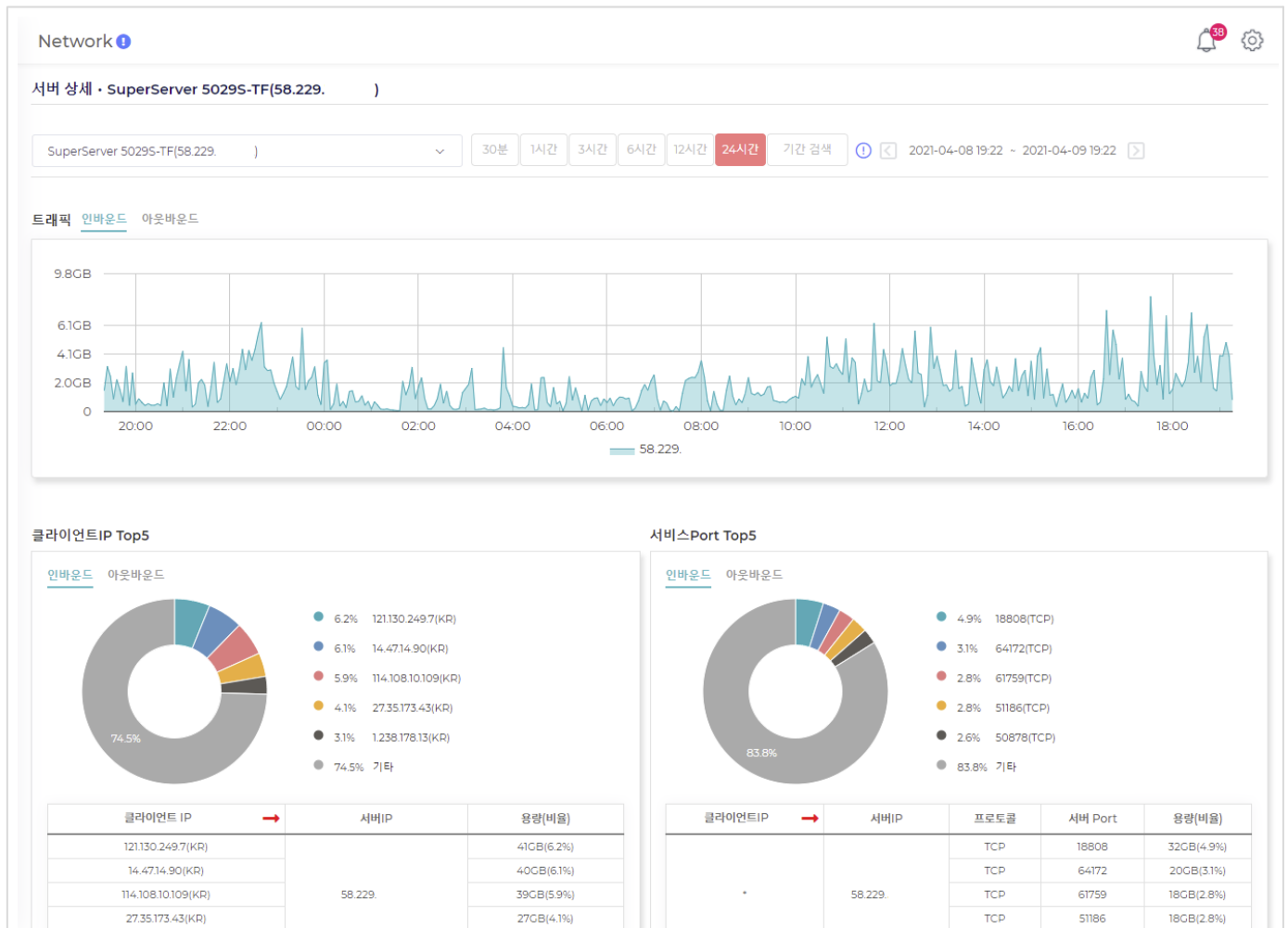
Network 🔔 ⚙️

전체서버 요약 전체서버 목록

서버명, 서버IP, 운영체제 🔍 검색 초기화 정렬 초기화

NO.	↓	서버명	서버IP	운영체제	트래픽(outbound) 🔔	트래픽(inbound) 🔔	수정
186		SuperServer 5029S-TF	58.229.	linux	3TB	506GB	⚙️
185		SuperServer 5029S-TF	58.229.	linux	503MB	130GB	⚙️
184		SuperServer 5029S-TF	58.229.	linux	775MB	192GB	⚙️
183		SuperServer 5029S-TF	58.229.	linux	3TB	578GB	⚙️
182		SuperMicro SS6028R	1.234.	linux	754MB	189GB	⚙️
181		SuperMicro SS6028R	1.234.	linux(CentOS6)	20MB	150MB	⚙️
180		SuperMicro SS6028R	1.234.	linux	984KB	240KB	⚙️

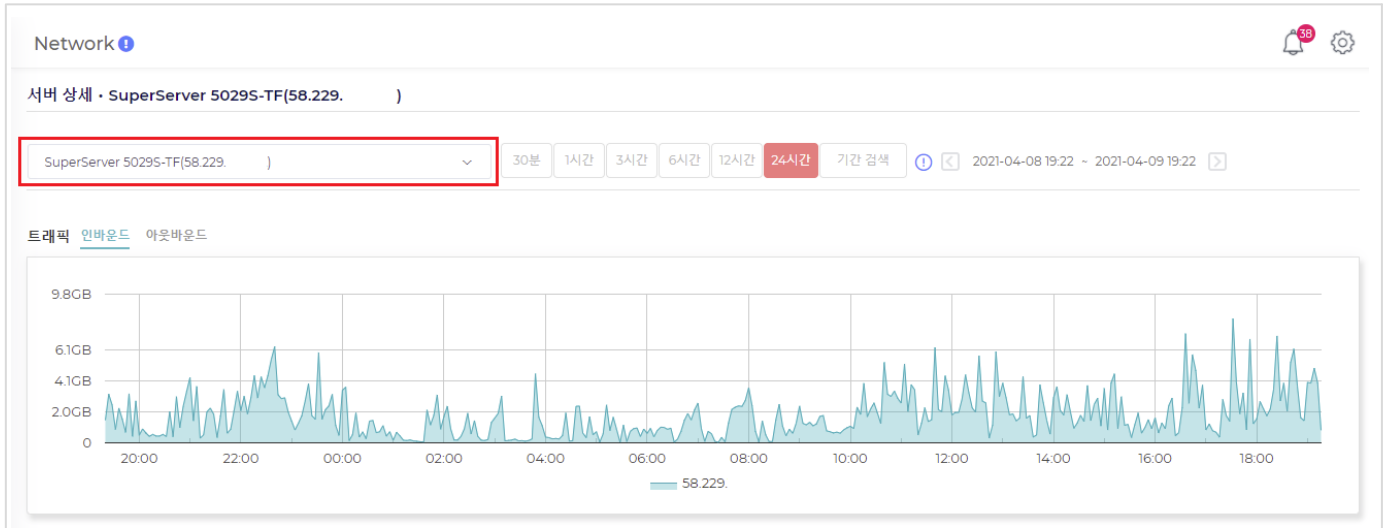
개별서버 요약



5.7.1. 개별서버 요약의 각 항목 설명

개별서버 변경

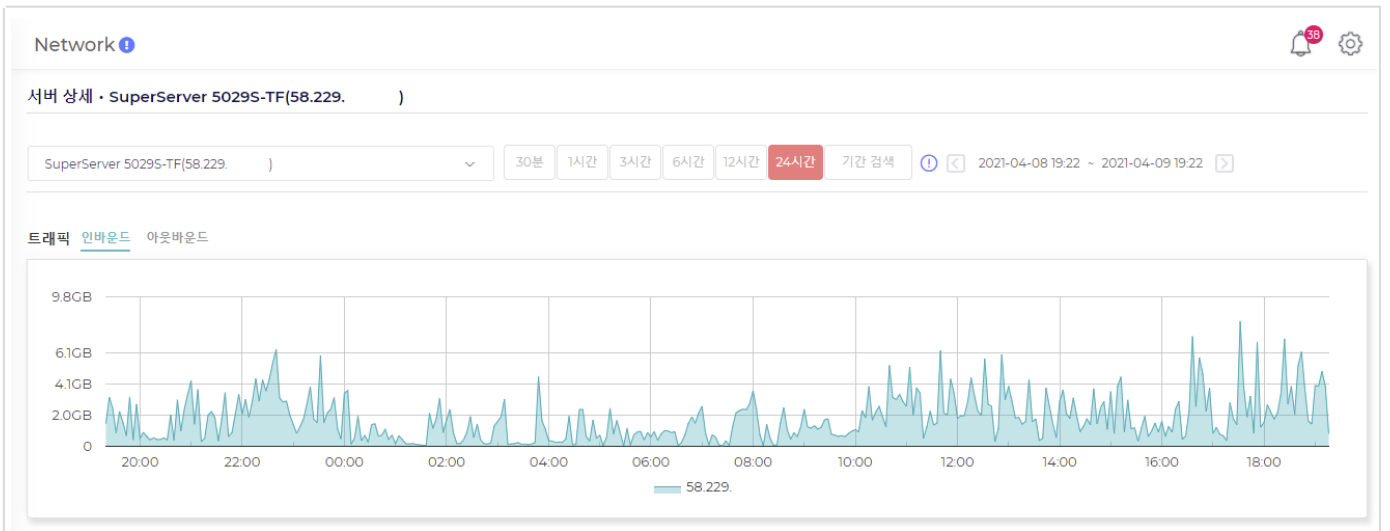
다른 개별서버로 변경할 수 있습니다.



트래픽 Top5

최근 24시간 동안 개별서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 개별서버 트래픽 그래프입니다.

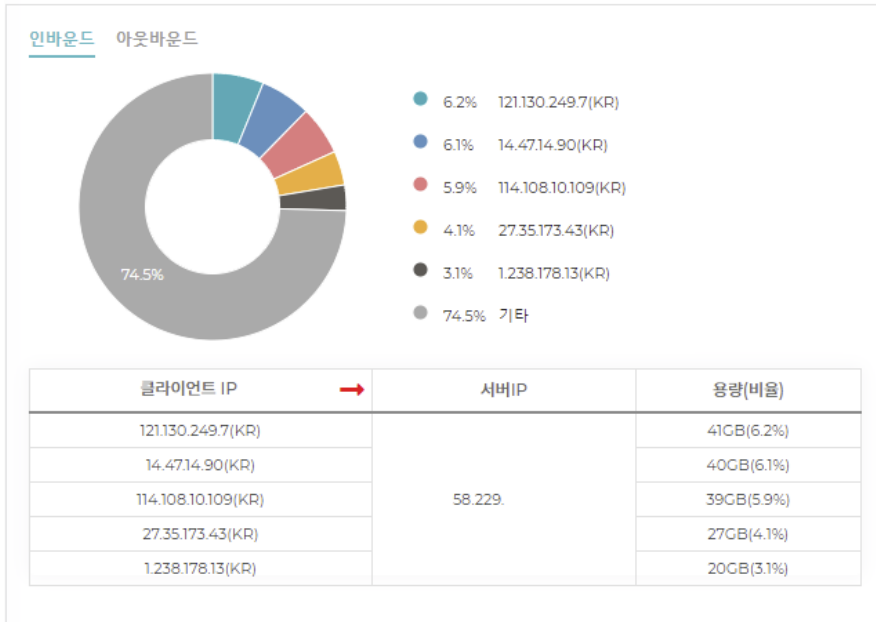


클라이언트IP Top5

최근 24시간 동안 개별서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

이용자께서 운영하시는 개별서버에 가장 많이 접근한 클라이언트 5개의 IP 입니다. 클라이언트의 트래픽 용량도 확인할 수 있습니다.

클라이언트IP Top5



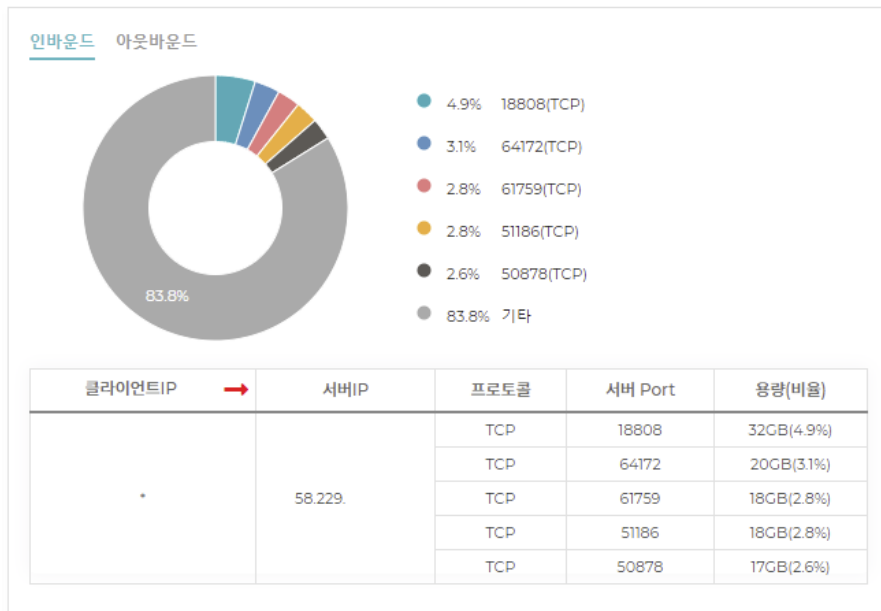
KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 ' - ' 으로 표시됩니다.

서비스Port Top5

최근 24시간 동안 개별서버에 대한 통계 정보입니다. (시간과 기간을 변경하여 검색할 수 있습니다.)

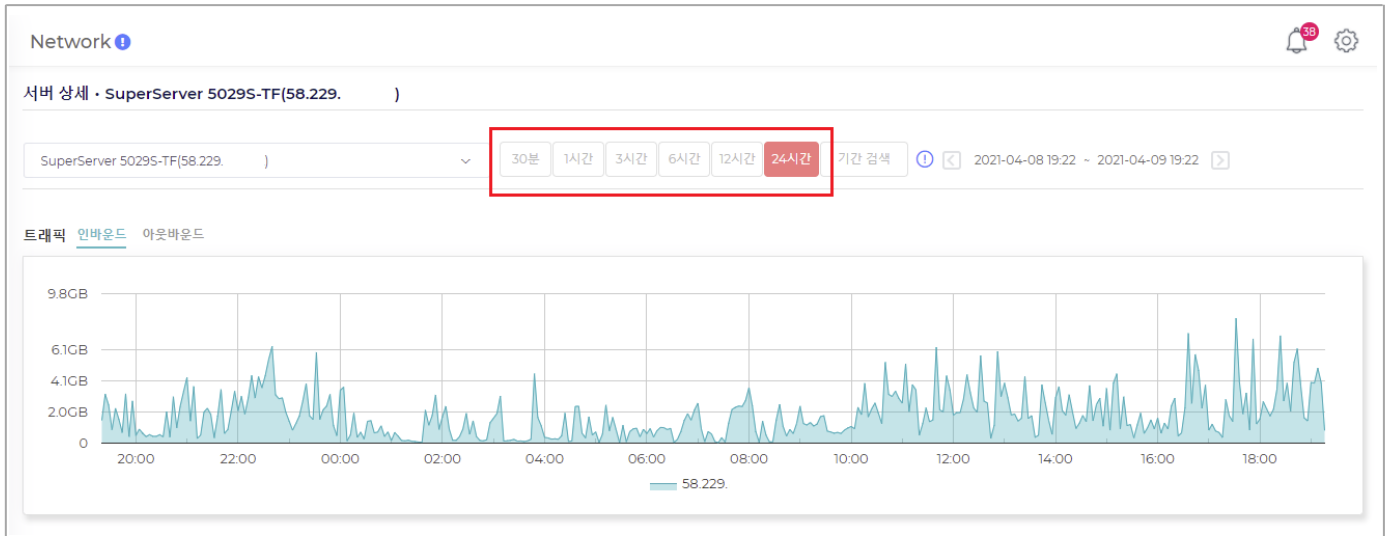
이용자께서 운영하시는 개별 서버에 트래픽을 가장 많이 사용한 서비스 Port 5개 입니다. 프로토콜, 서버Port, 용량을 확인할 수 있습니다.

서비스Port Top5



실시간 검색

실시간 데이터를 검색 할 수 있는 버튼입니다. (24시간까지만 실시간 검색이 가능합니다.)

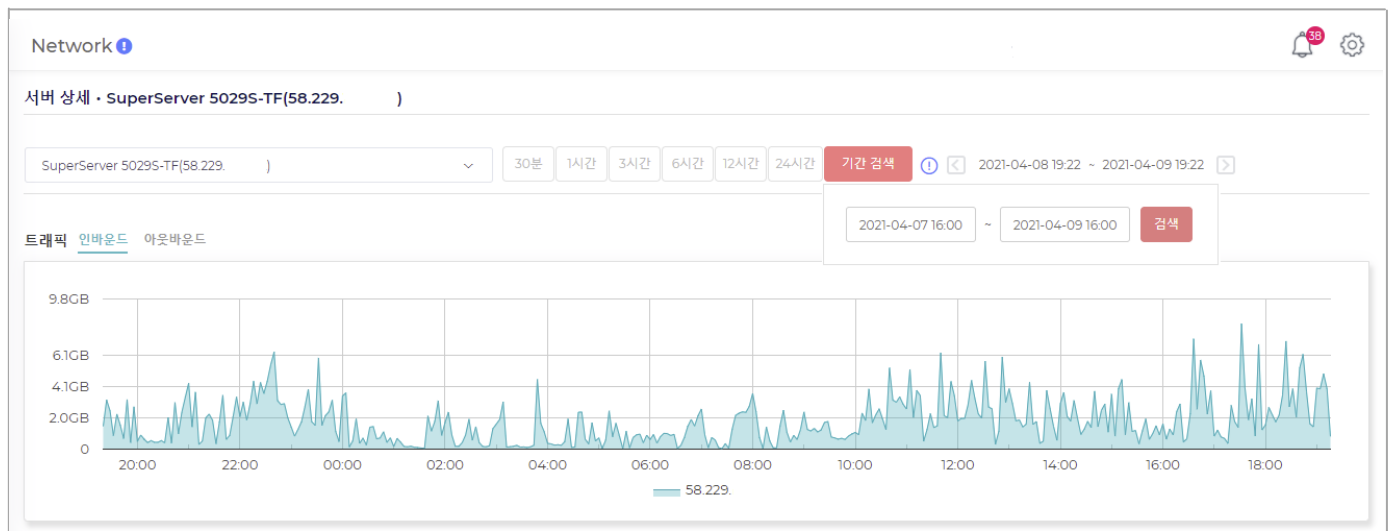


기간 검색

실시간 데이터를 검색 할 수 없지만, 현재시간-2H 까지 검색이 가능하며, 최대 30일 이전의 데이터를 검색할 수 있습니다.

현재시간이 13:00 이라면, 11:00까지 검색 가능합니다. (검색범위 : -30일~현재시간-2H)

최소 검색 단위는 2시간 입니다.



검색 후 < > 버튼을 이용하여, 시간을 이동할 수 있습니다. (해당 기능은 기간 검색에서만 가능합니다.)

5.8. 트래픽 분석

특정 시간 & 특정 서버에 접속한 클라이언트를 상세하게 분석하는 페이지입니다.

1. 접속이 많은 클라이언트IP 와 트래픽 용량을 확인할 수 있습니다.
2. 접속이 많은 서비스Port 와 트래픽 용량을 확인할 수 있습니다.

iTEASY
INSIGHT

Server + [그룹생성]

트래픽이 가장 많이... 3

현재 서버 196

트래픽 분석

보안 이벤트

보고서

문의

공지사항

히스토리

Network

트래픽 분석

트래픽 분석 서버 선택

IP대역(58.229.)
 IP대역(58.229.)
 Full Rack(58.229.)
 Full Rack(58.229.)
 IP대역(58.229.)
 IP대역(58.229.)
 IP대역(58.229.)
 aaaaaaaaaa...(58.229.)
 Full Rack(1.234.)
 SuperMicro...(1.234.)

INBOUND | IP | 30분 | 1시간 | 3시간 | 6시간 | 12시간 | 24시간 | 기간 검색 | 2021-04-08 20:00 ~ 2021-04-09 20:00

트래픽 차트

트래픽 분석 결과

* 상위 100개의 데이터만 표시합니다.

클라이언트IP	서버IP	트래픽 용량	국가	도시	최근 접속일
121.78.238.222	선택 서버	95GB(21.8%)	KR	-	21/04/09 19:53:27
121.78.247.18	선택 서버	88GB(20.1%)	KR	-	21/04/09 19:58:24
14.192.89.9	선택 서버	74GB(17.1%)	KR	-	21/04/09 19:52:00

5.8.1. 트래픽 분석 순서

트래픽 분석 방법에 대해 설명드립니다.

1. 분석할 서버를 선택합니다.



한번에 분석 가능한 서버수는 10대 입니다.

2. 확인하고 싶은 정보를 선택합니다. (INBOUND/OUTBOUND, IP/PORT)

3. 시간을 선택하면, 결과가 출력됩니다.

The screenshot shows the 'Network' dashboard with '트래픽 분석' (Traffic Analysis) selected. Under '트래픽 분석 서버 선택' (Traffic Analysis Server Selection), several server types are listed with checkboxes: Full Rack, IP대역, SuperMicro, and SuperServe. Below this, there are dropdown menus for 'INBOUND' and 'IP', and a time range selector with options: 30분, 1시간, 3시간, 6시간, 12시간, 24시간, and 기간 검색. The selected time range is 2021-04-08 20:00 ~ 2021-04-09 20:00.

4. 결과 출력

특정 시간 & 특정 서버에 접속한 클라이언트를 확인할 수 있습니다.

The screenshot shows the 'Network' dashboard with the traffic analysis results. A '트래픽 차트' (Traffic Chart) is displayed, showing traffic volume over time for various servers. Below the chart, the '트래픽 분석 결과' (Traffic Analysis Results) section shows a table of client IP addresses. The table includes columns for Client IP, Server IP, Traffic Volume, Country, City, and Last Access Time.

클라이언트IP	서버IP	트래픽 용량	국가	도시	최근 접속일
121.78.238.222	선택 서버	95GB(21.8%)	KR	-	21/04/09 19:53:27
121.78.247.18	선택 서버	88GB(20.1%)	KR	-	21/04/09 19:58:24
14.192.89.9	선택 서버	74GB(17.1%)	KP	-	21/04/09 19:52:00

상위 100개의 통계 데이터를 표시합니다.



KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 ' - ' 으로 표시됩니다.

5.8.2. 트래픽 분석의 검색 항목 설명

실시간 검색

실시간 데이터를 검색 할 수 있는 버튼입니다. (24시간까지만 실시간 검색이 가능합니다.)

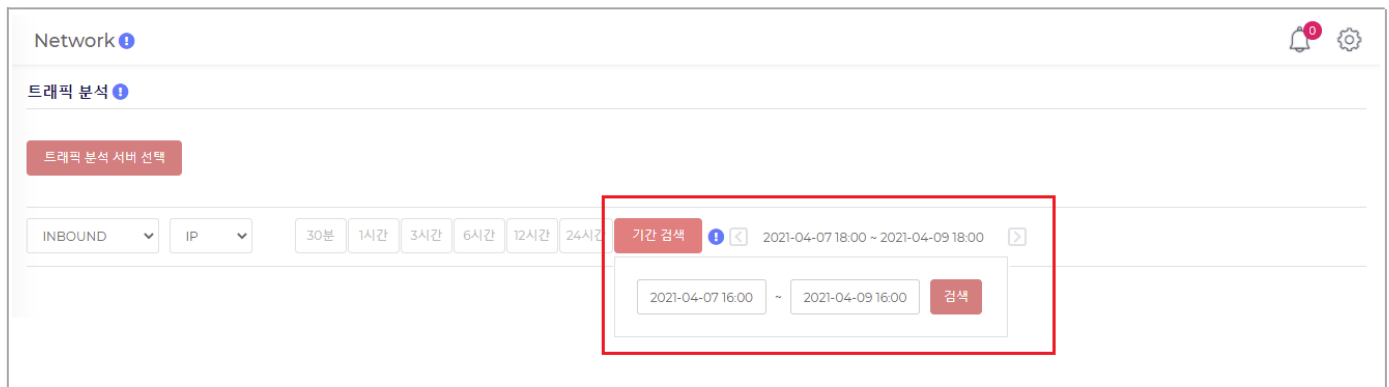


기간 검색

실시간 데이터를 검색 할 수 없지만, 현재시간-2H 까지 검색이 가능하며, 최대 30일 이전의 데이터를 검색할 수 있습니다.

현재시간이 13:00 이라면, 11:00까지 검색 가능합니다. (검색범위 : -30일~현재시간-2H)

최소 검색 단위는 2시간 입니다.



검색 후 < > 버튼을 이용하여, 시간을 이동할 수 있습니다. (해당 기능은 기간 검색에서만 가능합니다.)

5.9. 보안 이벤트

이용자 서버의 트래픽을 면밀히 분석하여, 네트워크 공격 및 블랙리스트IP 접근을 탐지합니다.

이용자께서는 해당 정보를 이용하여 서버의 보안 정책을 수립할 수 있습니다.

NO.	탐지 유형	서버명	서버 IP	공격IP	제목	메모	Date
714	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 20:00
713	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 19:00
712	블랙리스트IP 접근탐지	Full Rack	1.234.	163.172.36.126(FR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 19:00
711	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 18:00
710	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 17:00
709	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 15:30
708	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 5개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 15:00
707	블랙리스트IP 접근탐지	IP대역	1.234.	45.143.200.38(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 15:00
706	블랙리스트IP 접근탐지	IP대역	58.229.	203.133.180.143(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 14:30
705	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 3개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 13:30
704	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 13:00

보안 이벤트 (공격탐지)

공격이 탐지되었을 경우, 탐지정보와 대응방법을 제공해 드립니다.

보안 이벤트 (블랙리스트IP 접근탐지)

블랙리스트IP 접근이 탐지되었을 경우, 탐지정보와 대응방법을 제공해 드립니다.

보안 이벤트는 이용자께서 직접 등록하셔야 합니다.

그룹별로 보안이벤트를 등록할 수 있습니다.

보안이벤트는 최대 5개까지 등록 가능합니다.

보안 이벤트 수신을 원하지 않으시다면, [보안 이벤트 설정] 페이지에서 해당 보안 이벤트를 삭제하시면 됩니다.

보안 이벤트 수신 상태를 '정지' 로 변경하여, 일시적으로 수신하지 않을 수 있습니다.

' 공격탐지 ', ' 블랙리스트IP 접근탐지 ' 중에서 1개만 선택하실 수도 있습니다.



보안 이벤트 탐지에 대한 SELF 대응방법이 해당 문서 Appendix 에 수록되어 있습니다.

저희 엔지니어팀이 대기중에 있습니다. 스스로 조치하시기 어려우시거나, 지원이 필요할 경우 언제든지 문의해 주실 수 있습니다.

([유라인 문의](#), 전화 번호 : 1600-8324[서비스운영팀])

5.9.1. 보안 이벤트 설정

보안이벤트는 이용자께서 직접 등록하셔야 합니다. 그래야 보안 이벤트가 생성됩니다.

NO.	탐지 유형	서버명	서버 IP	공격IP	제목	메모	↓ Date
714	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 20:00
713	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 19:00
712	블랙리스트IP 접근탐지	Full Rack	1.234.	163.172.36.126(FR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 19:00
711	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 18:00
710	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 17:00
709	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 15:30
708	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 5개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 15:00
707	블랙리스트IP 접근탐지	IP대역	1.234.	45.143.200.38(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 15:00
706	블랙리스트IP 접근탐지	IP대역	58.229.	203.133.180.143(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 14:30
705	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 3개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/09 13:30

'보안 이벤트 설정 바로가기' 또는 아이콘을 클릭하여 보안 이벤트 설정 페이지로 이동합니다.

5.9.1.1. 보안 이벤트 설정 목록

No.	탐지 유형	그룹명	상태	수정	삭제
1	공격탐지, 블랙리스트 IP 접근 탐지	전체서버(186)	동작중		

'보안 이벤트 등록하기' 버튼을 클릭하여 보안이벤트를 등록합니다.

5.9.1.2. 보안 이벤트 등록

보안 이벤트 등록하기 ! ×

그룹별로 보안이벤트를 생성합니다.

보안이벤트를 등록할 그룹을 선택하세요 *

전체서버 ▼

보안 이벤트 탐지 유형을 선택하세요. * (모든 탐지유형을 선택하는 것을 권고드립니다.)

공격을 탐지합니다. 블랙리스트IP 접근을 탐지합니다.

취소 등록

그룹별로 보안이벤트를 등록할 수 있습니다. (보안이벤트를 등록하시면, 그룹별로 보안이벤트를 탐지합니다.)

탐지 유형 (공격탐지, 블랙리스트IP 접근탐지) 을 선택할 수 있지만, 가급적 2개 모두 선택하시는 것을 권고 드립니다.

보안 이벤트는 최대 5개까지 등록 가능합니다.

보안이벤트 설정에 대해 하단에서 좀 더 자세하게 설명드리겠습니다.

5.9.2. 보안 이벤트 목록

Network ?

보안 이벤트 ?
보안이벤트 설정 바로가기 ➔

검색 초기화 | 정렬 초기화

NO.	탐지 유형	서버명	서버 IP	공격IP	제목	메모 ?	↓	Date
714	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 20:00
713	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR)	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 19:00
712	블랙리스트IP 접근탐지	Full Rack	1.234.	163.172.36.126(FR)	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 19:00
711	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 18:00
710	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 17:00
709	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 15:30
708	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 5개	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 15:00
707	블랙리스트IP 접근탐지	IP대역	1.234.	45.143.200.38(NL)	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 15:00
706	블랙리스트IP 접근탐지	IP대역	58.229.	203.133.180.143(KR)	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 14:30
705	블랙리스트IP 접근탐지	Full Rack	1.234.	117.111.1.248(KR) 외 3개	블랙리스트IP 접근이 탐지되었습니다.	0		21/04/09 13:30

탐지 유형

공격탐지와 블랙리스트IP 접근탐지 2가지 유형이 있습니다.

공격IP

이용자 서버에 접근 혹은 공격한 IP 이며, 해당 IP 에 국가를 표시합니다. (국가 표시에 '-' 으로 나올 수 있습니다. 아래 툴팁 참고)

제목

제목을 클릭하시면, 보안 이벤트 상세로 이동합니다.

메모

각 보안 이벤트에 대해 메모를 남길 수 있습니다.



KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 '-' 으로 표시됩니다.

5.9.3. 보안 이벤트 상세

공격탐지와 블랙리스트IP 접근탐지 2가지 유형이 있습니다.

공격탐지와 블랙리스트IP 접근탐지의 상세 내용은 조금 다릅니다.

5.9.3.1. 공격탐지 상세

Network ⓘ

 35

보안 이벤트 상세

상세정보

서버명(서버IP)	SuperServer 5029S-TF (58.229.)																				
제목	TCP ACK Flooding 공격이 탐지되었습니다.																				
탐지시간	21/03/24 19:43 ~ 21/03/24 19:44																				
총 공격횟수	1132회																				
공격상세	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">공격IP</th> <th style="width: 20%;">서버Port</th> <th style="width: 20%;">공격횟수</th> <th style="width: 30%;">비고</th> </tr> </thead> <tbody> <tr> <td>49.173.65.126 (-)</td> <td>65214</td> <td>433회</td> <td>-</td> </tr> <tr> <td>49.173.65.126 (-)</td> <td>54993</td> <td>66회</td> <td>-</td> </tr> <tr> <td>222.104.39.59 (-)</td> <td>60174</td> <td>87회</td> <td>-</td> </tr> <tr> <td>118.223.89.6 (-)</td> <td>53151</td> <td>77회</td> <td>-</td> </tr> </tbody> </table>	공격IP	서버Port	공격횟수	비고	49.173.65.126 (-)	65214	433회	-	49.173.65.126 (-)	54993	66회	-	222.104.39.59 (-)	60174	87회	-	118.223.89.6 (-)	53151	77회	-
	공격IP	서버Port	공격횟수	비고																	
	49.173.65.126 (-)	65214	433회	-																	
	49.173.65.126 (-)	54993	66회	-																	
	222.104.39.59 (-)	60174	87회	-																	
118.223.89.6 (-)	53151	77회	-																		

공격설명

공격 설명	공격자가 대용량 ICMP 패킷을 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. 심할 경우 시스템이 Crash 되는 현상이 발생할 수 있습니다.
대응 방법	<ol style="list-style-type: none"> 1. 운영중인 서버에 최신 보안 패치 적용 2. 취약 프로그램 소스 수정 3. 공격IP 차단 (SELF 대응) <ul style="list-style-type: none"> - KSHosting 방화벽으로 공격 차단 (https://ksidc.net 의 [방화벽 관리] 에서 공격IP 를 차단할 수 있습니다.) - Linux 계열 서버라면, iptables 를 이용하여 공격IP 를 차단할 수 있습니다. - Windows 계열 서버라면, Windows 자체에 있는 방화벽을 이용하여 공격IP 를 차단할 수 있습니다. 4. 보안 컨설팅 <ul style="list-style-type: none"> - 취약점 점검 수행 - 모의해킹 수행 (권고) : 전반적인 모의해킹을 실시하여 취약점 제거 및 수정 5. 보안 장비 <ul style="list-style-type: none"> - 취약점에 맞는 보안 장비 도입
유의사항	이용자께서 공격에 대해 조치를 하셨더라도, 보안이벤트가 발생할 수 있습니다. [보안 이벤트 발생 이유]

목록
메모 작성

제목

탐지된 공격 이름입니다. (당사 서비스에서 탐지하는 공격유형은 해당 문서 Appendix 에 수록되어 있습니다.)

공격 상세

공격IP(공격IP 국가), 공격을 당한 서버Port, 공격횟수를 표시합니다. (국가 표시에 '-' 으로 나올 수 있습니다. 아래 톨팁 참고)

공격유형 중 서버Port 를 직접적으로 공격하지 않는 공격은 ' 서버Port ' 항목이 표시되지 않으며,

Ping of Death 공격유형은 기준용량 항목이 추가됩니다. (Ping of Death : ICMP 프로토콜을 기준용량 이상으로 전송하는 공격유형입니다.)

대응 방법

대응 방법에 대해 기술되어 있습니다.

유의사항

보안 이벤트 발생에 대한 구조적 문제점에 대해 기술되어 있습니다. (보안 이벤트의 구조적 문제는 해당 문서 Appendix 에 수록되어 있습니다.)

5.9.3.2. 블랙리스트IP 접근탐지 상세

Network ⓘ 🔔 35 ⚙️

보안 이벤트 상세

상세정보

서버명(서버IP)	Full Rack (1.234.)				
제목	블랙리스트IP 접근이 탐지되었습니다.				
탐지시간	21/03/17 18:00 - 21/03/17 18:30				
총 접근횟수	1회				
접근상세	블랙리스트IP	프로토콜	서버Port	접근횟수	비고
	180.166.228.244 (-)	tcp	7885	1회	-

공격설명

블랙리스트IP 설명	당사는 KISA 로 부터 사이버위협정보를 제공받고 있습니다. ('악성코드 감염IP', '공격시도IP', '악성 이메일IP' ...) 사이버위협정보가 이용자서버에 접근하면, 해당 내용을 이용자에게 알려드립니다.
대응 방법	1. 공격IP 차단 (SELF 대응) - KSHosting 방화벽으로 공격 차단 (https://ksidc.net 의 [방화벽 관리] 에서 블랙리스트IP 를 차단할 수 있습니다.) - Linux 계열 서버라면, iptables 를 이용하여 블랙리스트IP 를 차단할 수 있습니다. - Windows 계열 서버라면, Windows 자체에 있는 방화벽을 이용하여 블랙리스트IP 를 차단할 수 있습니다. 2. 보안 컨설팅 - 취약점 점검 수행 - 모의해킹 수행 (권고) : 전반적인 모의해킹을 실시하여 취약점 제거 및 수정 3. 보안 장비 - 취약점에 맞는 보안 장비 도입
유의사항	이용자께서 블랙리스트IP에 대해 조치를 하셨더라도, 보안이벤트가 발생될 수 있습니다. [보안 이벤트 발생 이유]

목록 메모 작성

대응 방법

대응 방법에 대해 기술되어 있습니다.

유의사항

보안 이벤트 발생에 대한 구조적 문제점에 대해 기술되어 있습니다. (보안 이벤트의 구조적 문제는 해당 문서 Appendix 에 수록되어 있습니다.)

각 보안 이벤트에 대해 메모를 남길 수 있습니다.

메모 작성하기

내용*

취소 작성



공격탐지

14개 공격 유형을 탐지합니다. (공격탐지의 유형은 계속 업데이트 할 예정이며, 상세 내용은 하단 Appendix 에서 설명드리겠습니다.)

블랙리스트IP 접근탐지

당사는 KISA 의 CTAS 회원사이며, KISA 는 CTAS 회원사에게 사이버 위협 정보를 제공합니다. (상세 내용은 하단 Appendix 에서 설명드리겠습니다.)

보안 이벤트는 인바운드 트래픽에 대해서만 탐지합니다.



보안 이벤트 탐지에 대한 SELF 대응방법이 하단 Appendix 에 수록되어 있습니다.

저희 엔지니어팀이 대기중에 있습니다. 스스로 조치하시기 어려우시거나, 지원이 필요할 경우 언제든지 문의해 주실 수 있습니다.
([온라인 문의](#), 전화 번호 : 1600-8324[서비스운영팀])



KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 ' - ' 으로 표시됩니다.

5.10. 보고서

이용자 서버의 트래픽을 면밀히 분석하여 유익한 통계정보를 제공해 드립니다.

이용자께서는 해당 정보를 이용하여 서비스 방향 및 정책을 수립할 수 있습니다.

NO.	그룹	보고서 유형	제목	Date
4	전체서버	주간 보고서	[전체서버] iTEASY 2021년 4월 둘째주 트래픽 보고서	21/04/12 02:00
3	트래픽이 가장 많이	주간 보고서	[트래픽이 가장 많이 나오는 서버] iTEASY 2021년 4월 둘째주 트래픽 보고서	21/04/12 02:00
2	전체서버	주간 보고서	[전체서버] iTEASY 2021년 3월 다섯째주 트래픽 보고서	21/04/05 02:00
1	전체서버	주간 보고서	[전체서버] iTEASY 2021년 3월 셋째주 트래픽 보고서	21/03/22 16:11

주간 보고서에는 다음과 같은 내용이 기술됩니다.

1. 금주와 전주의 트래픽 용량과 트래픽 추이를 확인할 수 있습니다.
2. 트래픽을 많이 사용한 날짜(요일)와 시간을 확인할 수 있습니다.
3. 트래픽을 많이 발생시킨 클라이언트IP와 국가를 확인할 수 있습니다.
4. 트래픽을 많이 사용한 이용자 서버를 확인할 수 있습니다.
5. 보안 이벤트가 많이 발생한 날짜(요일)와 시간을 확인할 수 있습니다.
6. 보안 이벤트를 많이 발생시킨 공격IP를 확인할 수 있습니다.
7. 보안 이벤트가 많이 발생한 이용자 서버를 확인할 수 있습니다.

서비스 이용 동의시에 보고서는 자동 등록됩니다. (전체서버 대상으로 등록)

그룹별로 보고서를 등록할 수 있습니다.

보고서는 최대 5개까지 등록 가능합니다.

보고서를 이메일로 수신 받을 수 있습니다.

보고서 수신을 원하지 않으시다면, [[보고서 설정](#)] 페이지에서 보고서를 삭제하시면 됩니다.

보고서 수신 상태를 '정지'로 변경하여, 일시적으로 수신하지 않을 수 있습니다.

주간 보고서 생성 및 발송 시간

03/15(월) ~ 03/21(일)의 주간 보고서는 03/22(월) 새벽에 생성 및 메일로 전송해 드립니다.

5.10.1. 보고서 설정

서비스 이용 동의시에 보고서는 자동 등록됩니다. (전체서버 대상으로 등록)
 추가로 보고서를 등록할 수 있습니다.

Network 1

보고서 1 보고서 설정 바로가기

제목 검색 초기화 정렬 초기화

NO.	그룹	보고서 유형	제목	Date
4	전체서버	주간 보고서	[전체서버] ITEASY 2021년 4월 둘째주 트래픽 보고서	21/04/12 02:00
3	트래픽이 가장 많이	주간 보고서	[트래픽이 가장 많이 나오는 서버] ITEASY 2021년 4월 둘째주 트래픽 보고서	21/04/12 02:00
2	전체서버	주간 보고서	[전체서버] ITEASY 2021년 3월 다섯째주 트래픽 보고서	21/04/05 02:00
1	전체서버	주간 보고서	[전체서버] ITEASY 2021년 3월 셋째주 트래픽 보고서	21/03/22 16:11

20 < 1 >

'보고서 설정 바로가기' 또는 아이콘을 클릭하여 보고서 설정 페이지로 이동합니다.

5.10.1.1. 보고서 설정 목록

Network 1

보안 이벤트 설정 보고서 설정 서비스 질의 1

No.	그룹명	이름	이메일	상태	수정	삭제
2	트래픽이 가장 많이 나오는 서버(3)			등록중		
1	전체서버(186)			등록중		

보고서 등록하기

5.10.1.2. 보고서 등록

보고서 등록하기 ⓘ

그룹별로 보고서를 생성합니다.

보고서를 등록할 그룹을 선택하세요 *

전체서버

이름

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

이메일

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

취소 등록



그룹별로 보고서를 등록할 수 있습니다. (보고서를 등록하시면, 그룹별로 보고서를 받아보실 수 있습니다.)

보고서는 최대 5개까지 등록 가능합니다.

보고서를 메일로 받아 보시기를 원하신다면, 메일주소를 기입하시면 됩니다.

보고서 설정에 대해 하단에서 좀 더 자세하게 설명드리겠습니다.

5.10.2. 보고서 목록

Network 1 57  

보고서 1 보고서 설정 바로가기

제목 검색 초기화 정렬 초기화

NO.	그룹	보고서 유형	제목	↓ Date
4	전체서버	주간 보고서	[전체서버] iTEASY 2021년 4월 둘째주 트래픽 보고서	21/04/12 02:00
3	트래픽이 가장 많이 나오는 서버	주간 보고서	[트래픽이 가장 많이 나오는 서버] iTEASY 2021년 4월 둘째주 트래픽 보고서	21/04/12 02:00
2	전체서버	주간 보고서	[전체서버] iTEASY 2021년 3월 다섯째주 트래픽 보고서	21/04/05 02:00
1	전체서버	주간 보고서	[전체서버] iTEASY 2021년 3월 셋째주 트래픽 보고서	21/03/22 16:11

20 < 1 >

그룹

해당 그룹에 대한 주간보고서입니다.

보고서 유형

베타 서비스 기간에는 주간 보고서만 제공하며, 정식 서비스에서는 월간 / 분기 / 반기 / 연간 보고서 제공 예정입니다.

제목

제목을 클릭하시면, 주간 보고서 상세로 이동합니다.

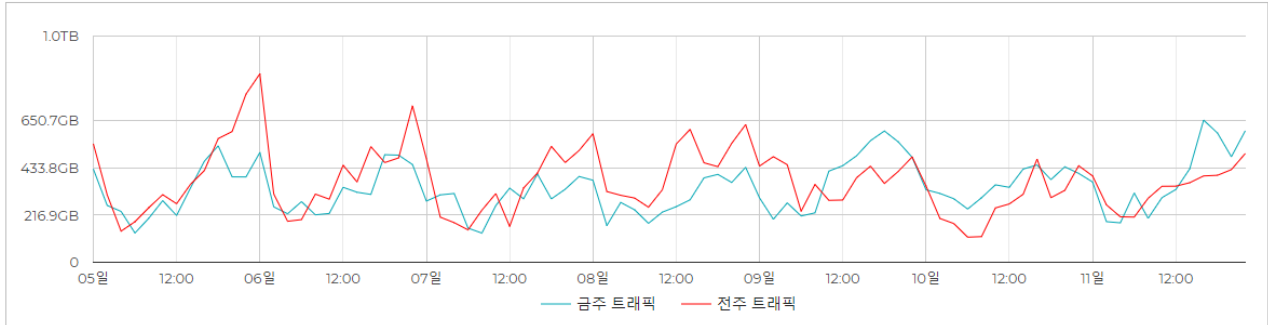
5.10.3. 보고서 상세

[전체서버] iTEASY 2021년 4월 둘째주 트래픽 보고서입니다. (21/04/05 00:00 ~ 21/04/11 23:59)

■ 개요

그룹명	전체 서버	서버수	238대
트래픽 용량 (인바운드)	28TB(전주트래픽 : 31TB)	트래픽 용량 (아웃바운드)	182TB(전주트래픽 : 194TB)
보안 이벤트	53300개(전주 보안이벤트 : 114847개)		

■ 트래픽 인바운드 아웃바운드



5.10.3.1. 개요

보고서 생성 시점에 그룹에 대한 정보입니다.

5.10.3.2. 트래픽

7일 동안 사용한 트래픽 용량이며, 전주트래픽과 금주트래픽을 비교할 수 있습니다.

5.10.3.3. 트래픽 분석

7일 동안 수집된 트래픽 정보를 분석한 결과이며, 트래픽 분석 하부에 10개의 분석 항목으로 나뉘어 집니다.

트래픽 분석		
■ 일간 트래픽 Top3		
인바운드	2021/04/09(금)	4.7T(2.2%)
	2021/04/11(일)	4.6T(2.2%)
	2021/04/10(토)	4.2T(2%)
아웃바운드	2021/04/11(일)	28.7T(13.7%)
	2021/04/10(토)	27.6T(13.1%)
	2021/04/05(월)	26.6T(12.7%)
■ 시간 트래픽 Top3		
인바운드	2021/04/11(일) 23:00 ~ 00:00	372G(1.3%)
	2021/04/11(일) 16:00 ~ 17:00	347.4G(1.2%)
	2021/04/09(금) 18:00 ~ 19:00	320.8G(1.1%)
	2021/04/11(일) 19:00 ~ 20:00	318.6G(1.1%)
	2021/04/11(일) 17:00 ~ 18:00	306.8G(1.1%)
아웃바운드	2021/04/09(금) 21:00 ~ 22:00	1.7T(1%)
	2021/04/10(토) 23:00 ~ 00:00	1.7T(0.9%)
	2021/04/05(월) 00:00 ~ 01:00	1.6T(0.9%)
	2021/04/11(일) 21:00 ~ 22:00	1.6T(0.9%)
	2021/04/08(목) 22:00 ~ 23:00	1.6T(0.9%)
■ 서버 Top5(주간)		
인바운드	58.229.	4.1T(14.4%)
	58.229.	4T(14.2%)
	1.234.	3.8T(13.5%)
	1.234.	3.8T(13.3%)
	1.234.	1.5T(5.3%)
아웃바운드	58.229.	28.1T(15.5%)
	58.229.	27.6T(15.2%)
	1.234.	24T(13.2%)
	1.234.	22.4T(12.3%)
	1.234.	11.3T(6.2%)
■ 클라이언트 Top5(주간)		
인바운드	14.192.89.9	2.6T(9.3%)
	121.78.238.222	2.1T(7.5%)
	121.78.247.18	2T(7.2%)
	121.78.238.224	1.9T(6.7%)
	1.201.146.37	1.8T(6.4%)

1> 일간 트래픽 Top3

7일 중에 트래픽을 가장 많이 사용한 날짜(요일) Top3 입니다.

2> 시간 트래픽 Top5

7일 중에 트래픽을 가장 많이 사용한 시간 Top5 입니다.

3> 서버 Top5

7일 동안 트래픽을 가장 많이 사용한 서버 Top5 입니다.

4> 클라이언트 Top5

7일 동안 트래픽을 가장 많이 발생시킨 클라이언트IP Top5 입니다.

■ 서비스 Port Top5(주간)				■ 접속국가 Top5(주간)		
인바운드	18808	TCP	1.6T(5.8%)	인바운드	KR	27.6T(98%)
	3306	TCP	629.1G(2.2%)		US	401.8G(1.4%)
	59434	TCP	77.8G(0.3%)		RO	30.5G(0.1%)
	53319	TCP	74.4G(0.3%)		BR	21.5G(0.1%)
	80	TCP	71.1G(0.2%)		CN	19.9G(0.1%)
아웃바운드	18808	TCP	125T(68.7%)	아웃바운드	KR	178.9T(98.3%)
	8082	TCP	2T(1.1%)		US	1.2T(0.7%)
	80	TCP	1.7T(0.9%)		CN	462.4G(0.2%)
	3306	TCP	829.1G(0.4%)		VN	299.3G(0.2%)
	50763	TCP	76.9G(0%)		JP	166.1G(0.1%)
■ 일간 보안이벤트 Top5			■ 시간 보안이벤트 Top5			
인바운드	2021/04/11(월)	36619(36576,43)	인바운드	2021/04/11(월) 13:00 ~ 14:00	12830(12828,2)	
	2021/04/06(화)	7026(6568,458)		2021/04/11(월) 19:00 ~ 20:00	11988(11987,1)	
	2021/04/08(목)	4429(4300,129)		2021/04/11(월) 00:00 ~ 01:00	2466(2466,0)	
		2021/04/08(목) 00:00 ~ 01:00		2381(2354,27)		
				2021/04/11(월) 16:00 ~ 17:00	2328(2327,1)	
■ 서버 보안이벤트 Top5			■ 공격IP Top5			
인바운드	1.234.	19662(19655,7)	인바운드	183.100.180.178	8498(8498,0)	
	1.234.	14654(14460,194)		112.148.108.230	3863(3863,0)	
	58.229.	8963(7452,1511)		49.173.65.126	3360(3360,0)	
	58.229.	3989(3931,58)		59.14.74.56	2086(0,2086)	
	1.234.	3388(3388,0)		58.226.19.179	1558(1558,0)	

5> 서비스 Port Top5

7일 동안 트래픽을 가장 많이 사용한 서비스Port Top5 입니다.

6> 접속국가 Top5

7일 동안 트래픽을 가장 많이 발생시킨 국가 Top5 입니다.

7> 일간 보안 이벤트 Top3

7일 중에 보안 이벤트가 가장 많이 발생한 날짜(요일) Top3 입니다.

8> 시간 보안 이벤트 Top5

7일 중에 보안 이벤트가 가장 많이 발생한 시간 Top5 입니다.

9> 서버 보안 이벤트 Top5

7일 동안 보안 이벤트가 가장 많이 발생한 서버 Top5 입니다.

10> 공격IP Top5

7일 동안 보안 이벤트를 가장 많이 발생시킨 공격IP Top5 입니다.



KR, JP 등의 국가 표시가 없는 경우가 있습니다. IP 에 대한 국가 데이터베이스가 없기 때문이며, 이럴 경우에 ' - ' 으로 표시됩니다.

5.10.3.4. 데이터

7일 동안 수집된 트래픽 정보를 날짜와 시간단위로 구분한 결과이며, 데이터 하부에 4개의 데이터 항목으로 나뉘어 집니다.

데이터

■ 일간별 트래픽

인바운드

2021/04/05(월)	30.4T(14.5%)
2021/04/06(화)	29.4T(14%)
2021/04/07(수)	29.1T(13.9%)
2021/04/08(목)	27.3T(13%)
2021/04/09(금)	28.9T(13.7%)
2021/04/10(토)	31.8T(15.1%)
2021/04/11(일)	33.2T(15.8%)

아웃바운드

2021/04/05(월)	30.4T(14.5%)
2021/04/06(화)	29.4T(14%)
2021/04/07(수)	29.1T(13.9%)
2021/04/08(목)	27.3T(13%)
2021/04/09(금)	28.9T(13.7%)
2021/04/10(토)	31.8T(15.1%)
2021/04/11(일)	33.2T(15.8%)

■ 시간별 트래픽

인바운드

날짜(요일)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2021/04/05(월)	223.9G	205.4G	107.9G	153.8G	135.8G	98.4G	70.3G	64.5G	98.8G	104G	158.6G	125.2G	112.6G	102.8G	147.4G	194.7G	233.7G	231.7G	278.7G	257.2G	202.4G	190.7G	165.3G	227.5G
2021/04/06(화)	268.5G	237G	177.9G	77.3G	125.5G	97.9G	130.1G	149.1G	110.2G	108.3G	116.2G	108.5G	177.3G	167.8G	137.7G	184.8G	175.2G	137.2G	281.5G	213.7G	211.1G	282G	246.9G	202.9G
2021/04/07(수)	124.5G	157.2G	151.9G	158.3G	233.5G	83.2G	85.8G	71.4G	30.4G	103.9G	112.8G	148.3G	151.6G	189.6G	169.9G	122.3G	229.9G	176.3G	163G	128.7G	147.9G	188.3G	145.9G	249G
2021/04/08(목)	206.3G	171.3G	128.2G	40.7G	151G	124.5G	94.3G	147.4G	72.4G	106.8G	116.4G	114.4G	103.5G	152.6G	154.7G	132.9G	194.7G	193.8G	193.5G	211.1G	173.2G	194G	220.8G	216.3G
2021/04/09(금)	170.6G	126.1G	101.8G	96.1G	155.6G	117.8G	122G	91.1G	73.7G	153.9G	183.6G	236G	204G	240.5G	230.3G	260.1G	266G	293.8G	320.8G	283.6G	283.3G	270.9G	271G	212.4G
2021/04/10(토)	180.1G	153.6G	151.5G	165.5G	144.9G	147.7G	99G	146.2G	129.3G	167.8G	190.5G	166G	170G	174.9G	198.6G	230.6G	264.4G	183.6G	152G	228.4G	203.1G	236.4G	210G	199G
2021/04/11(일)	206.5G	163.2G	91.9G	95.2G	98.4G	83G	173.3G	145.3G	100.9G	101.3G	155G	142.6G	143.1G	192.1G	248.9G	181.3G	347.4G	306.8G	276.4G	318.6G	199G	286.6G	233.2G	372G

아웃바운드

날짜(요일)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2021/04/05(월)	1.6T	1.3T	1.1T	922.7G	777G	878.3G	729G	849.4G	804.7G	938.3G	1T	1.1T	900.2G	1T	1.1T	1.2T	1.1T	1.1T	1.3T	1.4T	1.5T	1.4T	1.5T	
2021/04/06(화)	1.5T	1.2T	934.3G	773.8G	765.1G	713.9G	690.9G	621.8G	709.6G	959.9G	969.1G	987.4G	987.4G	938.7G	1T	1.1T	1.1T	1T	1.1T	1.3T	1.4T	1.6T	1.6T	1.5T
2021/04/07(수)	1.4T	1.1T	903.2G	833.2G	755.8G	709.1G	767.1G	688.1G	245.7G	954.7G	1.1T	1.3T	1.3T	1.1T	1.1T	1.1T	1.2T	1.1T	1.2T	1.4T	1.6T	1.5T	1.5T	
2021/04/08(목)	1.4T	1.2T	759.8G	655.7G	640G	581.5G	657.9G	622.5G	725G	903.5G	1T	899.3G	891.3G	1008.1G	958.8G	914G	980.9G	1012.5G	1.1T	1.2T	1.3T	1.5T	1.6T	1.6T
2021/04/09(금)	1.2T	891.5G	785.1G	666.9G	523.2G	530.1G	486.9G	608.3G	602.5G	831.7G	1T	1012.8G	1012.5G	1008.3G	1.1T	1.3T	1.1T	1.2T	1.2T	1.4T	1.4T	1.7T	1.5T	1.3T
2021/04/10(토)	1.3T	1.2T	842.8G	729.4G	692.3G	659.1G	730.6G	835.9G	981.4G	1.1T	1.3T	1.3T	1.3T	1.3T	1.2T	1.1T	1.1T	1.1T	1.3T	1.4T	1.5T	1.5T	1.5T	1.7T
2021/04/11(일)	1.5T	1.2T	955G	739.3G	596.8G	600G	729.9G	954.7G	1.1T	1.1T	1.3T	1.1T	1.2T	1.2T	1.4T	1.5T	1.5T	1.4T	1.3T	1.4T	1.4T	1.6T	1.5T	1.5T

1> 일간별 트래픽

일간별 누적 트래픽입니다.

2> 시간별 트래픽

시간별 누적 트래픽이며, 빨간색으로 표시된 데이터는 트래픽을 많이 사용한 시간이며, 파란색으로 표시된 데이터는 트래픽을 적게 사용한 시간을 의미합니다.

빨간색 5개, 파란색 5개를 표시합니다.

■ 일간별 보안이벤트

2021/04/05(월)	1852(305,1547)
2021/04/06(화)	7026(6568,458)
2021/04/07(수)	3129(1442,1687)
2021/04/08(목)	4429(4300,129)
2021/04/09(금)	122(1,121)
2021/04/10(토)	123(3,120)
2021/04/11(일)	36619(36576,43)

■ 시간별 보안이벤트

날짜(요일)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2021/04/05(월)	3 (0,3)	0 (0,0)	1 (0,1)	307 (305,2)	4 (0,4)	2 (0,2)	1 (0,1)	3 (0,3)	96 (0,96)	255 (0,255)	1 (0,1)	5 (0,5)	2 (0,2)	2 (0,2)	0 (0,0)	1 (0,1)	0 (0,0)	1 (0,1)	775 (0,775)	383 (0,383)	0 (0,0)	7 (0,7)	2 (0,2)	1 (0,1)
2021/04/06(화)	1898 (1883,15)	1596 (1589,7)	1465 (1464,1)	2 (0,2)	8 (0,8)	2 (0,2)	2 (0,2)	3 (0,3)	1 (0,1)	51 (0,51)	78 (0,78)	4 (0,4)	192 (0,192)	1 (0,1)	2 (0,2)	3 (0,3)	78 (0,78)	5 (0,5)	0 (0,0)	1 (0,1)	0 (0,0)	1 (0,1)	1632 (1632,0)	1 (0,1)
2021/04/07(수)	45 (0,45)	15 (0,15)	8 (0,8)	2 (0,2)	0 (0,0)	4 (0,4)	4 (0,4)	3 (0,3)	0 (0,0)	0 (0,0)	0 (0,0)	0 (0,0)	0 (0,0)	0 (0,0)	0 (0,0)	78 (0,78)	100 (0,100)	663 (0,663)	312 (0,312)	168 (0,168)	97 (0,97)	71 (0,71)	1533 (1442,91)	26 (0,26)
2021/04/08(목)	2381 (2354,27)	13 (0,13)	1 (0,1)	1 (0,1)	1 (0,1)	2 (0,2)	1 (0,1)	1 (0,1)	0 (0,0)	1946 (1946,0)	2 (0,2)	4 (0,4)	61 (0,61)	1 (0,1)	0 (0,0)	2 (0,2)	0 (0,0)	4 (0,4)	2 (0,2)	2 (0,2)	1 (0,1)	1 (0,1)	2 (0,2)	0 (0,0)
2021/04/09(금)	3 (0,3)	1 (0,1)	3 (0,3)	15 (0,15)	3 (0,3)	2 (1,1)	3 (0,3)	0 (0,0)	0 (0,0)	13 (0,13)	0 (0,0)	31 (0,31)	12 (0,12)	7 (0,7)	17 (0,17)	2 (0,2)	1 (0,1)	2 (0,2)	4 (0,4)	1 (0,1)	0 (0,0)	1 (0,1)	1 (0,1)	0 (0,0)
2021/04/10(토)	1 (0,1)	2 (0,2)	2 (1,1)	1 (0,1)	0 (0,0)	0 (0,0)	1 (0,1)	4 (0,4)	1 (0,1)	4 (1,3)	5 (0,5)	0 (0,0)	0 (0,0)	2 (0,2)	5 (0,5)	6 (0,6)	2 (0,2)	2 (1,1)	14 (0,14)	65 (0,65)	1 (0,1)	0 (0,0)	3 (0,3)	2 (0,2)
2021/04/11(일)	2466 (2466,0)	7 (0,7)	2 (0,2)	1 (0,1)	6 (0,6)	1 (0,1)	0 (0,0)	1 (0,1)	1 (0,1)	4 (0,4)	3 (0,3)	0 (0,0)	1 (0,1)	12830 (12828,2)	1583 (1580,3)	1 (0,1)	2328 (2327,1)	1630 (1626,4)	0 (0,0)	11988 (11987,1)	1 (0,1)	2307 (2307,0)	3 (1,2)	1455 (1454,1)

3> 일간별 보안이벤트

일간별 보안이벤트입니다.

4> 시간별 보안이벤트

시간별 보안 이벤트이며, 빨간색으로 표시된 데이터는 보안이벤트가 많이 사용한 시간을 의미합니다.

빨간색 5개를 표시하지만, 동일한 수가 많다면, 5개 미만으로 혹은 5개 이상으로 표시될 수 있습니다.

5.10.4. 주간 보고서 (이메일)

보고서 설정에 메일주소를 입력하셨다면, 보고서 간략 내용을 메일로 수신 받으실 수 있습니다.

[전체서버] iTEASY 2021년 4월 둘째주 트래픽 보고서 입니다. (21/04/05 00:00 ~ 21/04/11 23:59)

본 메일은 발신전용으로 회신 할수 없습니다.

■ 개요

그룹명	그룹명	그룹명	238대
트래픽 용량 (인바운드)	28TB(전주트래픽 : 31TB)	트래픽 용량 (인바운드)	182TB(전주트래픽 : 194TB)
보안 이벤트	53300개(전주 보안이벤트 :11484개)		

■ 요약

트래픽

인바운드 통계이며, 보다 상세한 내용은 [홈페이지] 에서 확인 하실수 있습니다.

일간 트래픽	7일 중에 트래픽을 가장 많이 사용한 날짜는 2021/04/09(금) 이며, 트래픽 용량은 4.7T(2.2%) 입니다.
시간 트래픽	7일 중에 트래픽을 가장 많이 사용한 시간대는 2021/04/11(일) 23:00 ~ 00:00 이며, 트래픽 용량은 372G(1.3%) 입니다.
서버 트래픽	7일 동안 트래픽을 가장 많이 사용한 서버는 58.229. 이며, 트래픽 용량은 4.1T(14.4%) 입니다.
클라이언트 트래픽	7일 동안 트래픽을 가장 발생시킨 클라이언트는 14.192.89.9 이며, 트래픽 용량은 2.6T(9.3%) 입니다.
서비스Port 트래픽	7일 동안 트래픽을 가장 많이 사용한 서비스Port는 18808 이며, 트래픽 용량은 TCP 입니다.
접속국가 트래픽	7일 동안 트래픽을 가장 많이 발생시킨 국가는 KR 이며, 트래픽 용량은 27.6T(98%) 입니다.

보안이벤트

일간 보안이벤트	7일 중에 보안이벤트가 가장 많이 발생한 날짜는 2021/04/11(일) 이며, 보안이벤트수는 36619(36576,43)입니다.
시간 보안이벤트	7일 중에 보안이벤트가 가장 많이 발생한 시간대는 2021/04/11(일) 13:00 ~ 14:00 이며, 보안이벤트수는 12830(12828,2)입니다.
서버 보안이벤트	7일 동안 보안이벤트가 가장 많이 발생한 서버는 1.234. 이며, 보안이벤트수는 19662(19655,7)입니다.
공격IP	7일 동안 보안이벤트가 가장 많이 발생시킨 공격IP는 183.100.180.178 이며, 보안이벤트수는 8498(8498,0)입니다.

- 상세한 보고서 내용은 [홈페이지] 에서 확인할 수 있습니다.
- 보고서 메일을 수신하지 않기를 원하신다면, [보고서설정] 에서 설정하시기 바랍니다.
- 궁금사항, 개선사항, 서비스 불편사항이 있으시면, [온라인문의] 를 통해 문의하실 수 있습니다.

본 메일은 발신전용으로 회신할 수 없습니다. 문의사항은 홈페이지를 이용해주세요기 바랍니다.
COPYRIGHT. ITEASY.CO.KR ALL RIGHTS RESERVED.

5.10.4.1. 개요

보고서 생성 시점에 그룹에 대한 정보입니다.

5.10.4.2. 요약

7일 동안 수집된 트래픽 정보를 분석한 결과입니다.

트래픽 분석 하부에 10개의 분석 항목으로 나뉘어지며, 각 분석 항목에서 가장 많이 발생한 내용을 기술합니다.

보다 상세한 내용은 홈페이지를 통해 확인하실 수 있습니다.

1> 일간 트래픽

7일 중에 트래픽을 가장 많이 사용한 날짜(요일) Top1 입니다.

2> 시간 트래픽

7일 중에 트래픽을 가장 많이 사용한 시간 Top1 입니다.

3> 서버 트래픽

7일 동안 트래픽을 가장 많이 사용한 서버 Top1 입니다.

4> 클라이언트 트래픽

7일 동안 트래픽을 가장 많이 발생시킨 클라이언트IP Top1 입니다.

5> 서비스 Port 트래픽

7일 동안 트래픽을 가장 많이 사용한 서비스Port Top1 입니다.

6> 접속국가 트래픽

7일 동안 트래픽을 가장 많이 발생시킨 국가 Top1 입니다.

7> 일간 보안 이벤트

7일 중에 보안 이벤트가 가장 많이 발생한 날짜(요일) Top1 입니다.

8> 시간 보안 이벤트

7일 중에 보안 이벤트가 가장 많이 발생한 시간 Top1 입니다.

9> 서버 보안 이벤트

7일 동안 보안 이벤트가 가장 많이 발생한 서버 Top1 입니다.

10> 공격IP

7일 동안 보안 이벤트를 가장 많이 발생시킨 공격IP Top1 입니다.

5.11. 문의하기

궁금사항, 개선사항, 서비스 불편사항이 있으시다면, 언제든지 문의하실 수 있습니다.

기술적인 지원이 필요하시다면, 언제든지 문의하실 수 있습니다.

휴대전화번호를 남겨주시면, 답변 완료 문자를 보내드립니다.

Network **1**

1:1 문의하기 고객의견

문의를 남겨주시면, 신속히 답변드리도록 하겠습니다. (접수시간: 평일 09:00 ~ 18:00 / 급한 문의는 언제나 1600-8324 [서비스운영팀] 연락주세요.)

제목, 내용, 답변 검색 초기화 정렬 초기화

NO.	상태	제목	Date
데이터가 없습니다			

20 < >

문의하기

5.11.1. 문의 목록

Network **1**

1:1 문의하기 고객의견

문의를 남겨주시면, 신속히 답변드리도록 하겠습니다. (접수시간: 평일 09:00 ~ 18:00 / 급한 문의는 언제나 1600-8324 [서비스운영팀] 연락주세요.)

제목, 내용, 답변 검색 초기화 정렬 초기화

NO.	상태	제목	Date
데이터가 없습니다			


20 < >

문의하기

제목

제목을 클릭하시면, 문의 상세로 이동합니다.

5.11.2. 문의하기

Network 1 0 

1:1 문의하기 **고객의견**

문의사항을 남겨주시면 신속, 정확, 친절하게 처리해드리겠습니다. (문의 : 평일 - 09:00-17:00)

이름	<input type="text"/>
이메일	<input type="text"/>
휴대전화	숫자만 입력해주세요
제목 *	<input type="text"/>
내용 *	<div style="border: 1px solid #ccc; height: 150px;"></div>
첨부파일	<input type="button" value="첨부파일"/>

휴대전화번호를 남겨주시면, 답변 완료 문자를 보내드립니다.

5.11.3. 문의 상세

문의에 대한 답변을 확인할 수 있습니다.

5.12. 고객의견

서비스에 의견이 있으시다면, 언제든지 의견을 남기실 수 있습니다.

휴대전화번호를 남겨주시면, 답변 완료 문자를 보내드립니다.

Network 1

1:1 문의하기 **고객의견**

제대로 동작하지 않는 페이지가 있나요? 서비스 이용에 불편한 점이 있으신가요? 개선할 점이 있나요? 고객님의께서 주시는 의견, 적극적으로, 신속하게 반영토록 하겠습니다. (접수시간 : 평일 09:00 ~ 18:00)

제목, 내용, 답변

NO.	상태	제목	Date
데이터가 없습니다			

20 < >

고객의견

5.12.1. 고객의견 목록

Network 1

1:1 문의하기 **고객의견**

제대로 동작하지 않는 페이지가 있나요? 서비스 이용에 불편한 점이 있으신가요? 개선할 점이 있나요? 고객님의께서 주시는 의견, 적극적으로, 신속하게 반영토록 하겠습니다. (접수시간 : 평일 09:00 ~ 18:00)

제목, 내용, 답변

NO.	상태	제목	Date
데이터가 없습니다			


20 < >

고객의견

제목

제목을 클릭하시면, 의견 상세로 이동합니다.

5.12.2. 고객의견

Network 

1:1 문의하기 **고객의견**

제대로 동작하지 않는 페이지가 있나요? 서비스 이용에 불편한 점이 있으신가요? 개선할 점이 있나요? 고객님의께서 주시는 의견 적극적이고, 신속하게 반영하겠습니다.

이름	<input type="text"/>
이메일	<input type="text"/>
휴대전화	숫자만 입력해주세요
제목 *	<input type="text"/>
내용 *	<div style="border: 1px solid #ccc; height: 150px;"></div>
첨부파일	<input type="button" value="첨부파일"/>

휴대전화번호를 남겨주시면, 답변 완료 문자를 보내드립니다.

5.12.3. 고객의견 상세

의견에 대한 답변을 확인할 수 있습니다.

5.13. History

이용자 액션을 간략하게 기술합니다.

The screenshot displays the 'History' section of the iTEASY INSIGHT interface. The left sidebar contains a menu with the following items: Server + [그룹생성], 전체 서버, 트래픽 분석, 보안 이벤트, 보고서, 문의, 공지사항, and History (highlighted with a red box). The main content area shows a table with the following data:

NO.	내용	Date
1	서비스 이용에 동의하셨습니다.	2021-04-12 15:53:07

Additional UI elements include a search bar with the text '내용', a pagination control showing '20' items per page and '1' page, and a notification bell icon in the top right corner.

5.14. 설정

5.14.1. 보안 이벤트 설정

이용자 서버의 트래픽을 면밀히 분석하여, 네트워크 공격 및 블랙리스트IP 접근을 탐지합니다.
 이용자께서는 해당 정보를 이용하여 서버의 보안 정책을 수립할 수 있습니다.

보안 이벤트는 이용자께서 직접 등록하셔야 합니다.

그룹별로 보안 이벤트를 등록할 수 있습니다.
 보안 이벤트는 최대 5개까지 등록 가능합니다.

보안 이벤트 수신을 원하지 않으시다면, [[보안 이벤트 설정](#)] 페이지에서 보안 이벤트를 삭제하시면 됩니다.

보안 이벤트 수신 상태를 '정지' 로 변경하여, 일시적으로 수신하지 않을 수 있습니다.
 '공격탐지', '블랙리스트IP 접근탐지' 중에서 1개만 선택하실 수도 있습니다.

5.14.1.1. 보안 이벤트 설정 목록

No.	탐지유형	그룹명	상태	수정	삭제
1	공격탐지, 블랙리스트 IP 접근 탐지	전체서버(186)	동작중		

5.14.1.2. 보안 이벤트 등록

보안 이벤트 등록하기 !

그룹별로 보안이벤트를 생성합니다.

보안이벤트를 등록할 그룹을 선택하세요 *

전체서버

보안 이벤트 탐지 유형을 선택하세요. * (모든 탐지유형을 선택하는 것을 권고드립니다.)

공격을 탐지합니다. 블랙리스트IP 접근을 탐지합니다.

취소 등록

그룹별로 보안이벤트를 등록할 수 있습니다. (보안이벤트를 등록하시면, 그룹별로 보안이벤트를 탐지합니다.)

탐지 유형 (공격탐지, 블랙리스트IP 접근탐지) 을 선택할 수 있지만, 가급적 2개 모두 선택하시는 것을 권고 드립니다.

보안 이벤트는 최대 5개까지 등록 가능합니다.

5.14.1.3. 보안 이벤트 수정

보안 이벤트 수정하기 !

그룹별로 보안이벤트를 생성합니다.

보안이벤트를 등록할 그룹을 선택하세요 *

전체서버

보안 이벤트 탐지 유형을 선택하세요. * (모든 탐지유형을 선택하는 것을 권고드립니다.)

공격을 탐지합니다. 블랙리스트IP 접근을 탐지합니다.

상태 !

동작

취소 수정

탐지 유형과 상태를 변경할 수 있습니다. (정지 : 보안 이벤트가 탐지되어도, 보안 이벤트를 생성하지 않습니다.)

5.14.1.4. 보안 이벤트 삭제

보안 이벤트 삭제하기 ! ×

그룹별로 보안이벤트를 생성합니다.

보안이벤트를 등록할 그룹을 선택하세요 *

전체서버 ▼

보안 이벤트 탐지 유형을 선택하세요. * (모든 탐지유형을 선택하는 것을 권고드립니다.)

공격을 탐지합니다. 블랙리스트IP 접근을 탐지합니다.

상태 !

동작 ▼

취소 삭제

보안 이벤트를 수신하기 원치 않으시면, 등록된 보안 이벤트를 삭제하시면 됩니다.



보안 이벤트를 메일로 수신하실 수 없습니다. (현재 웹에만 보실 수 있으시며, 정식 서비스에서는 메일 발송 예정입니다.)

5.14.2. 보고서 설정

이용자 서버의 트래픽을 면밀히 분석하여 유익한 통계정보를 제공해 드립니다.

이용자께서는 해당 정보를 이용하여 서비스 방향 및 정책을 수립할 수 있습니다.

서비스 이용 동의시에 보고서는 자동 등록됩니다. (전체서버 대상으로 등록)

그룹별로 보고서를 등록할 수 있습니다.

보고서는 최대 5개까지 등록 가능합니다.

보고서를 이메일로 수신 받을 수 있습니다.

보고서 수신을 원하지 않으시다면, [[보고서 설정](#)] 페이지에서 보고서를 삭제하시면 됩니다.

보고서 수신 상태를 '정지' 로 변경하여, 일시적으로 수신하지 않을 수 있습니다.

주간 보고서 생성 및 발송 시간

03/15(월) ~ 03/21(일) 의 주간 보고서는 03/22(월) 새벽에 생성 및 메일로 전송해 드립니다.

5.14.2.1. 보고서 설정 목록

No.	그룹명	이름	이메일	상태	수정	삭제
2	트래픽이 가장 많이 나오는 서버(3)			동작중		
1	전체서버(186)			동작중		

보고서 등록하기

5.14.2.2. 보고서 등록

보고서 등록하기 ⓘ

그룹별로 보고서를 생성합니다.

보고서를 등록할 그룹을 선택하세요 *

전체서버

이름

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

이메일

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

취소 등록

그룹별로 보고서를 등록할 수 있습니다. (보고서를 등록하시면, 그룹별로 보고서를 받아보실 수 있습니다.)

보고서는 최대 5개까지 등록 가능합니다.

보고서를 메일로 받아 보시기를 원하신다면, 메일주소를 기입하시면 됩니다.

5.14.2.3. 보고서 수정

보고서 수정하기 ⓘ

그룹별로 보고서를 생성합니다.

보고서를 등록할 그룹을 선택하세요 *

트래픽이 가장 많이 나오는 서버

이름

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

이메일

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

상태 ⓘ

동작

취소 수정

이름, 이메일, 상태를 변경할 수 있습니다. (정지 : 보고서가 생성되지 않습니다.)

5.14.2.4. 보고서 삭제

보고서 삭제하기 ! ×

그룹별로 보고서를 생성합니다.

보고서를 등록할 그룹을 선택하세요 *

트래픽이 가장 많이 나오는 서버 ▼

이름

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

이메일

보고서를 메일로 수신하기 원하신다면, 이름과 메일주소를 입력해주세요.

상태 !

동작 ▼

취소 삭제

보고서를 수신하기 원치 않으시면, 등록된 보고서를 삭제하시면 됩니다.



베타 서비스 기간에는 주간 보고서만 제공하며, 정식 서비스에서는 월간 / 분기 / 반기 / 연간 보고서 제공 예정입니다.

5.14.3. 서비스 철회

서비스에 만족하지 못하셨다면, 언제든지 서비스 철회가 가능합니다.

서비스 철회 시, 해당 서비스에 등록하신 모든 정보와 수집 데이터는 삭제되며, 삭제 후에는 복구가 불가능합니다.

서비스 철회 후 다시 서비스를 이용하실 수 있습니다. (서비스 동의 후 재사용)

5.14.3.1. 서비스 철회

Network ⓘ

보안 이벤트 설정 | 보고서 설정 | **서비스 철회 ⓘ**

※ 서비스 철회 시, 이용자께서 등록하는 정보와 수집 데이터는 모두 삭제되며, 복구가 되지 않습니다.

개선사항

개선사항과 의견을 남겨주셔서 감사합니다.

서비스 철회하기

6. Appendix

6.1. 보안 이벤트 (공격 탐지)

14개 공격 유형을 탐지합니다. (공격유형은 계속 업데이트 할 예정입니다.)

No	공격 유형	공격 설명
1	TCP SYN Flooding	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x02' 설정)
2	UDP Flooding	DoS 공격의 한 방법으로 대량의 UDP 패킷을 이용하여 대상 호스트의 네트워크 자원을 소모시키게 하는 공격 기법입니다.
3	ICMP Flooding	공격자가 ICMP 패킷을 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다.
4	TCP ACK Flooding	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x10' 설정)
5	TCP RST Flooding	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다.(패킷 조작 : TCP Header 내 Flags 를 '0x04' 설정)
6	TCP PSH Flooding	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x08' 설정)
7	TCP URG Flooding	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x20' 설정)
8	TCP SYN-FIN Attack	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x03' 설정) ※ SYN+FIN 조합으로 이루어진 정상적인 패킷은 없습니다.
9	TCP Xmas Attack	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 FIN[0x01], RST[0x04], PSH[0x08], URG[0x20] 설정)
10	Land Attack	공격자가 임의로 자신의 IP 와 Port 를 대상서버의 IP 와 Port 와 동일하게 패킷을 조작하고 전송함으로써, 서버의 실행속도가 느려지거나, 마비하게 하는 공격입니다.
11	Ping of Death	공격자가 대용량 ICMP 패킷을 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. 심할 경우 시스템이 Crash 되는 현상이 발생할 수 있습니다.
12	TCP Null Scan	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x00' 설정)
13	TCP FIN Scan	Dos 공격의 한 방법으로 서버가 정상적인 서비스를 하지 못하게 하는 공격 기법입니다. 클라이언트가 패킷을 조작하여 서버로 대량으로 전송하면, 서버는 이를 처리하기 위해 많은 자원을 소모하게 되고, 그로 인해 정상적인 서비스를 하지 못하게 됩니다. (패킷 조작 : TCP Header 내 Flags 를 '0x01' 설정)
14	TCP Port Scan	TCP PortScan 을 통하여 서버에 정상적으로 열려있는 서비스 Port 를 탐지 할 수 있습니다. 공정적인 면에서는 자신의 서비스 Port 를 점검하거나, 서비스 Port 의 취약점을 확인하기 위해서 사용할 수 있습니다. 부정적인 면에서는 해커가 해킹을 시도하기 전, 이용자 서버에 열려 있는 Port 를 확인하거나, 취약점을 파악하기 위한 정보 수집 차원에서 활용할 수 있습니다.

6.2. 보안 이벤트 (블랙리스트IP 접근탐지)

당사는 KISA의 CTAS 회원사이며, KISA는 CTAS 회원사에게 아래와 같은 사이버 위협 정보를 제공합니다.

'악성코드 감염IP', '공격시도IP', '악성 이메일IP', 기타 ('유포지IP', '피싱IP', '파밍IP', '스미싱IP', '정보유출지IP', '어뷰징IP') 이와 같은 사이버 위협 정보를 이용하여, 트래픽을 분석하고 보안에 문제가 있다고 판단될 경우 보안 이벤트를 생성합니다.

최근 30일 동안의 블랙리스트IP 로만 탐지하며, 그 개수는 2만개 정도가 됩니다. (블랙리스트IP는 실시간으로 업데이트됩니다.)

6.3. 보안 이벤트 대응 방법

6.3.1. SELF 대응

KSHosting 방화벽으로 공격 차단

<https://ksidc.net> 의 [방화벽 관리] 에서 공격IP 를 차단할 수 있습니다.

Linux 서버 자체 방화벽으로 공격 차단

Linux 계열 서버라면, iptables 를 이용하여 공격IP 를 차단할 수 있습니다.

Windows 서버 자체 방화벽으로 공격 차단

Windows 계열 서버라면, Windows 자체에 있는 방화벽을 이용하여 공격IP 를 차단할 수 있습니다.

6.3.2. 상담 및 지원

당사는 보안관제 및 보안 솔루션에 대해 별도 서비스를 운영하고 있습니다. ([Eyeon Security](#))

보안 컨설팅

보안 컨설팅을 통하여, [취약점 점검] 및 [모의 해킹] 을 점검 받아 보시기 바랍니다.

보안 솔루션

서버 취약점을 보완할 수 있는 보안 솔루션을 상담 받아보시기 바랍니다.

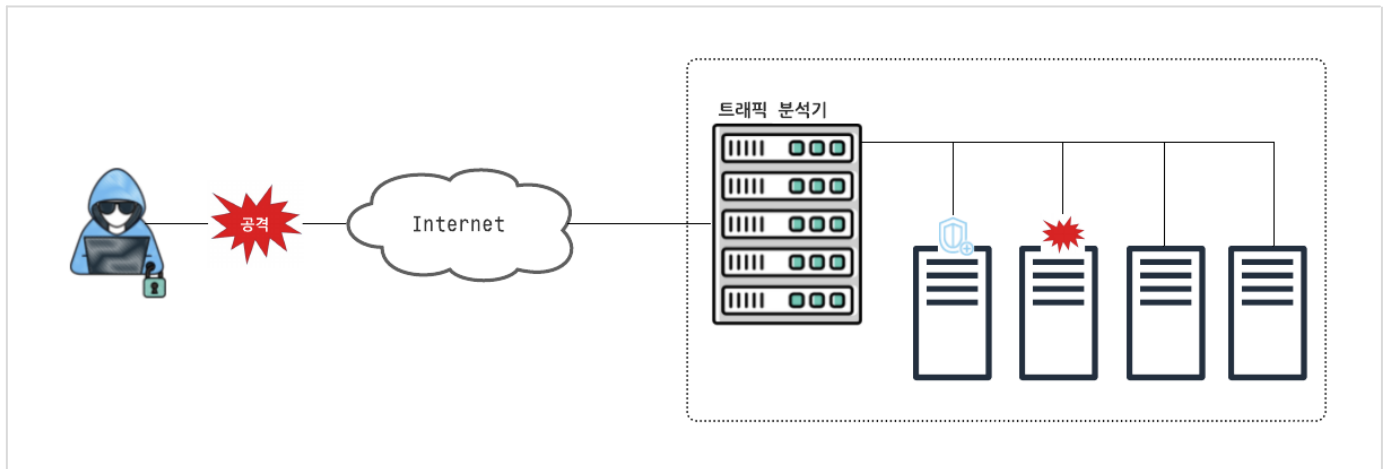


저희 엔지니어팀이 대기중에 있습니다. 스스로 조치하시기 어려우시거나, 지원이 필요할 경우 언제든지 문의해 주실 수 있습니다.
([온라인 문의](#), 전화 번호 : 1600-8324[서비스운영팀])

6.4. 보안 이벤트 구조적 문제

트래픽은 분석장비를 거쳐 이용자서버로 이동하기 때문에

이용자서버에 보안조치를 하셨더라도, 그것을 알지 못하는 분석장비는 보안이벤트를 발생시킬 수 밖에 없습니다.



이용자께서 보안조치를 하셨다면, 분명 이용자서버에서는 공격이 차단되며, 보안조치를 인지한 공격자는 무의미한 공격을 멈추게 됩니다.

해당 시점에 보안이벤트 발생이 멈추게 됩니다.

이용자께서 신속히 보안조치를 하셔야 보안이벤트 발생이 빠른 시간내에 멈출 뿐만 아니라, 이용자서버도 안전하게 지키실 수 있습니다.

NO.	탐지 유형	서버명	서버 IP	공격IP	제목	메모	Date
852	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 16:00
851	블랙리스트IP 접근탐지	SuperMicro S56028R	1.234.	200.73.132.213(AR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 15:00
850	블랙리스트IP 접근탐지	SuperMicro S56028R	1.234.	45.143.200.38(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 14:00
849	블랙리스트IP 접근탐지	IP대역	114.203.	146.88.240.4(US) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 14:00
848	블랙리스트IP 접근탐지	SuperMicro S56028R	1.234.	51.75.141.128(FR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 12:30
847	블랙리스트IP 접근탐지	Full Rack	58.229.	119.2.66.30(ID)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 12:30
846	블랙리스트IP 접근탐지	IP대역	1.234.	146.88.240.4(US)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 12:30
845	블랙리스트IP 접근탐지	SuperMicro S56028R	1.234.	65.151.169.17(US) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 12:00
844	블랙리스트IP 접근탐지	Full Rack	1.234.	211.36.141.67(KR) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 11:30
843	블랙리스트IP 접근탐지	IP대역	58.229.	20.63.72.228(US)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 11:30
842	블랙리스트IP 접근탐지	Full Rack	1.234.	211.36.141.67(KR) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 11:00
841	블랙리스트IP 접근탐지	SuperMicro S55029S-TF	1.234.	211.36.141.67(KR) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 11:00
840	블랙리스트IP 접근탐지	SuperServer 5029S-TF	58.229.	211.36.141.67(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 11:00
839	블랙리스트IP 접근탐지	IP대역	58.229.	45.133.1.42(NL) 외 2개	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 10:00
838	블랙리스트IP 접근탐지	SuperServer 5029S-TF	58.229.	223.62.216.175(KR)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 09:30
837	블랙리스트IP 접근탐지	SuperMicro S56028R	1.234.	138.121.170.141(CL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 09:30
836	블랙리스트IP 접근탐지	Full Rack	58.229.	116.228.233.91(CN)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 09:30
835	블랙리스트IP 접근탐지	IP대역	58.229.	45.148.10.190(NL)	블랙리스트IP 접근이 탐지되었습니다.	0	21/04/12 09:30

[[보안이벤트 페이지](#)] 에서 공격이 줄어드는 것을 확인하실 수 있습니다.