

**IntiGate**



*Smart Traffic Management & Protection*

# NP5508 소개서

(QoS 보안 스위치)



# 개요

- ✓ NP5508 은 L7 기반의 QoS(Quality of Service) 보안 스위치로서 네트워크의 서비스 품질을 보장하며 내외부의 네트워크 위협이나 비정상적인 트래픽을 탐지하여 네트워크에 연결된 기기들을 보호 한다.
- ✓ NP5508의 기능들은 자체 개발한 STMP(Smart Traffic Management and Protection) 테크놀로지를 활용하여 보다 세밀하게 네트워크의 품질 제어를 구현 하였으며 네트워크 트래픽을 분석하여 위협을 방지함으로써 보다 효율적이며 안전한 네트워크 환경을 조성하며, NP Manager 클라이언트 프로그램을 통해서 네트워크 현황을 가시화하고 트래픽 및 보안위협에 대한 제어 및 관리를 쉽고 간단하게 수행 한다.
- ✓ 기존 QoS 제품은 5 tuples 정보를 활용한 Flow 기반으로 트래픽의 품질을 제어 하는 반면에 STMP 테크놀로지 기반의 스마트한 QoS 는 DPI(Deep Packet Inspection) 자체기술에 의해서 확보된 어플리케이션 아이디를 활용하여 L7 기반으로 정밀한 트래픽 관리를 수행 하며, 또한 캐리어급의 NAT 기능도 지원 한다.
- ✓ 내부의 서버 계정탈취를 위해서 다양한 수단으로 공격 시도들을 탐지하고 방어하며, 비정상 트래픽의 분석을 통해서 좀비화된 IoT 디바이스 또는 PC 들의 탐지를 통해서 네트워크 자원의 낭비를 없애고 정상적인 네트워크 서비스가 수행 되도록 함으로서 안정적인 망을 유지토록 한다.

## 어플리케이션 미인지

- P2P 트래픽의 대역 잠식
- 실시간 게임 트래픽 미보호
- 양방향 서비스 지연

## 비정상 트래픽 발생

- CCTV/IoT 기기 취약점 상존
- 계정탈취 공격 후 좀비 이식
- 일부 비트코인 채굴 시 발생

## 세부 모니터링 미지원

- 현재 링크 위주 통합관리
- 플로우별 분석 미지원
- 트래픽 검색 미지원

네트워크 품질 저하 지속

심각한 피해 야기

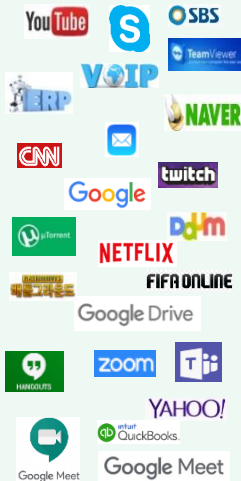
내부 네트워크 관리 안됨

**안정적인 트래픽 관리 및 네트워크 보호 필요**

## Smart Traffic Management & Protection

### 트래픽 정보 실시간 수집/관리

#### Application



국내외 1950+

#### 5tuples + meta data

IP, Port, Protocol,  
IP Group,  
App. Group, Policy,  
Toward, Etc.

#### Data 사용량

실시간 / 평균  
/ 누적

패킷 수 / 바이트 수  
/ 플로우 수

실시간  
전송

### 트래픽 관리 (QoS 보안)



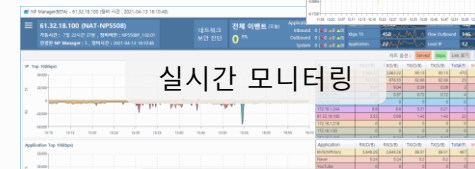
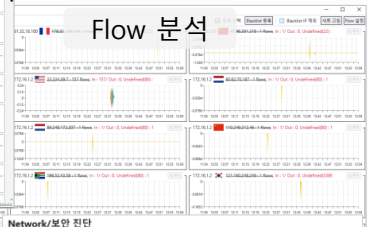
NP5508

### 세부 트래픽 가시화 및 진화된 관리



#### 대시보드

#### Flow 분석

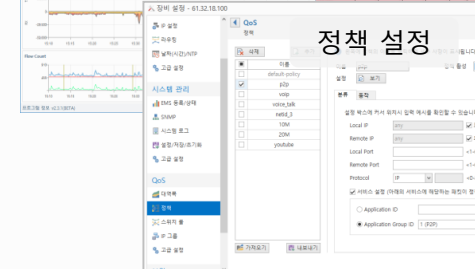


#### 실시간 모니터링

#### 네트워크/보안 진단

- Network/보안 진단
  - 보통 24시간의 데이터를 통해 Network 이상 설정이나 보안 취약점을 감지합니다. 진단을 시작하려면 '진단' 버튼을 클릭하십시오.
- Policy 진단
  - 권장된 설정 이외의 설정이거나 적용되지 않는 결과가 발생할 수 있는 Policy 설정을 진단합니다. 10M Policy/Dynamic-queue Bandwidth 설정에 대한 담당자의 확인이 필요합니다. 20M Policy 설정을 다시 확인해주시기 바랍니다.
- QoS 진단
  - 권장된 설정 이외의 설정이거나 적용되지 않는 결과가 발생할 수 있는 QoS 설정을 진단합니다. QoS 설정이 정상입니다.
- NTP 진단
  - NTP 설정이 정상입니다.
- DNS 설정 및 오류 진단
  - DNS 설정이 모두 정상입니다.
- 보안취약점 진단
  - Remote Desktop/Teletype/SSH의 취약점이 없습니다.
- 내부 감염 PC 진단
  - 내부에서 감염(흔들린) PC를 진단합니다. 감염된 내부의 흔적 PC는 없습니다.
- 외부 Attack 진단 (DDoS 등)
  - 안전합니다.

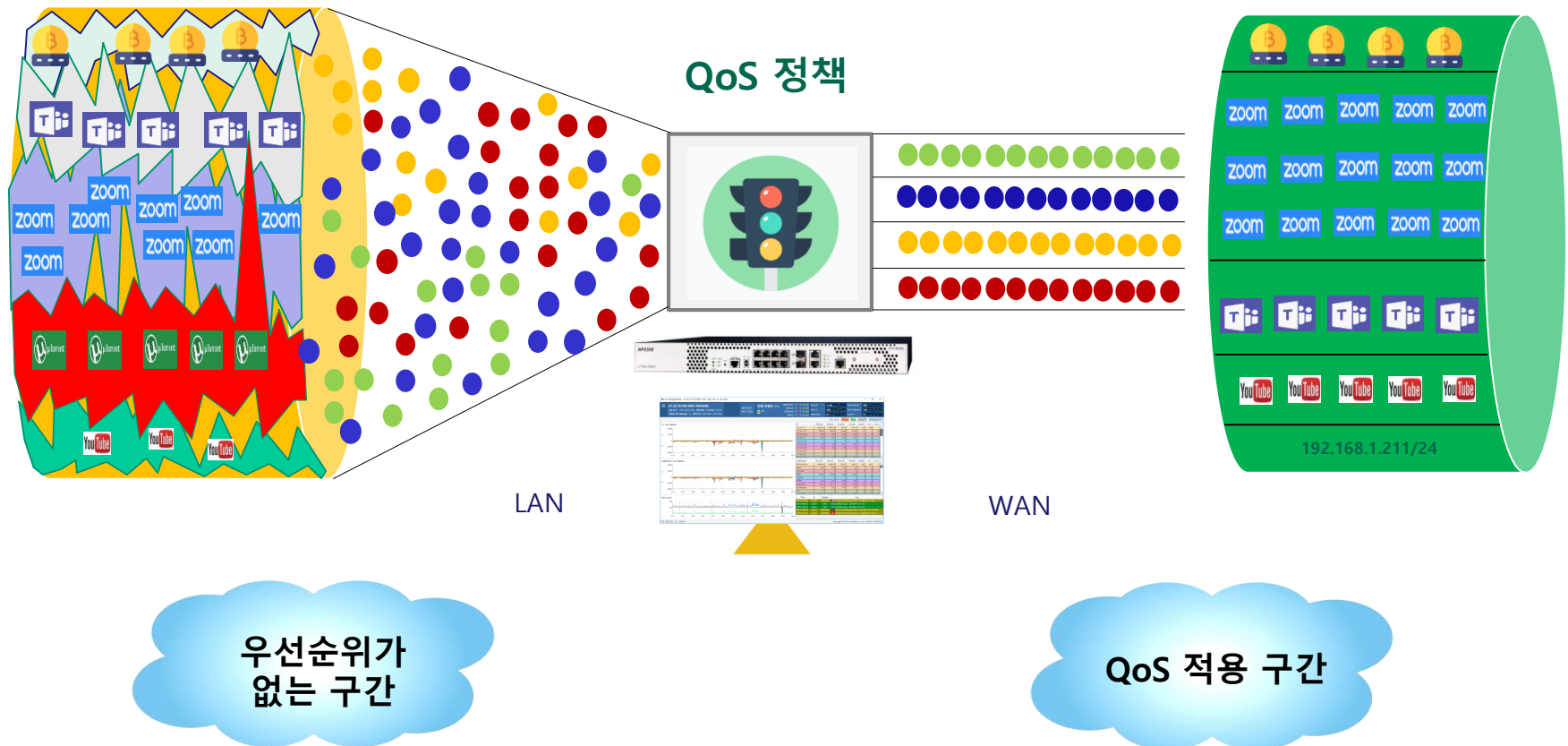
#### 정책 설정



NP Manager

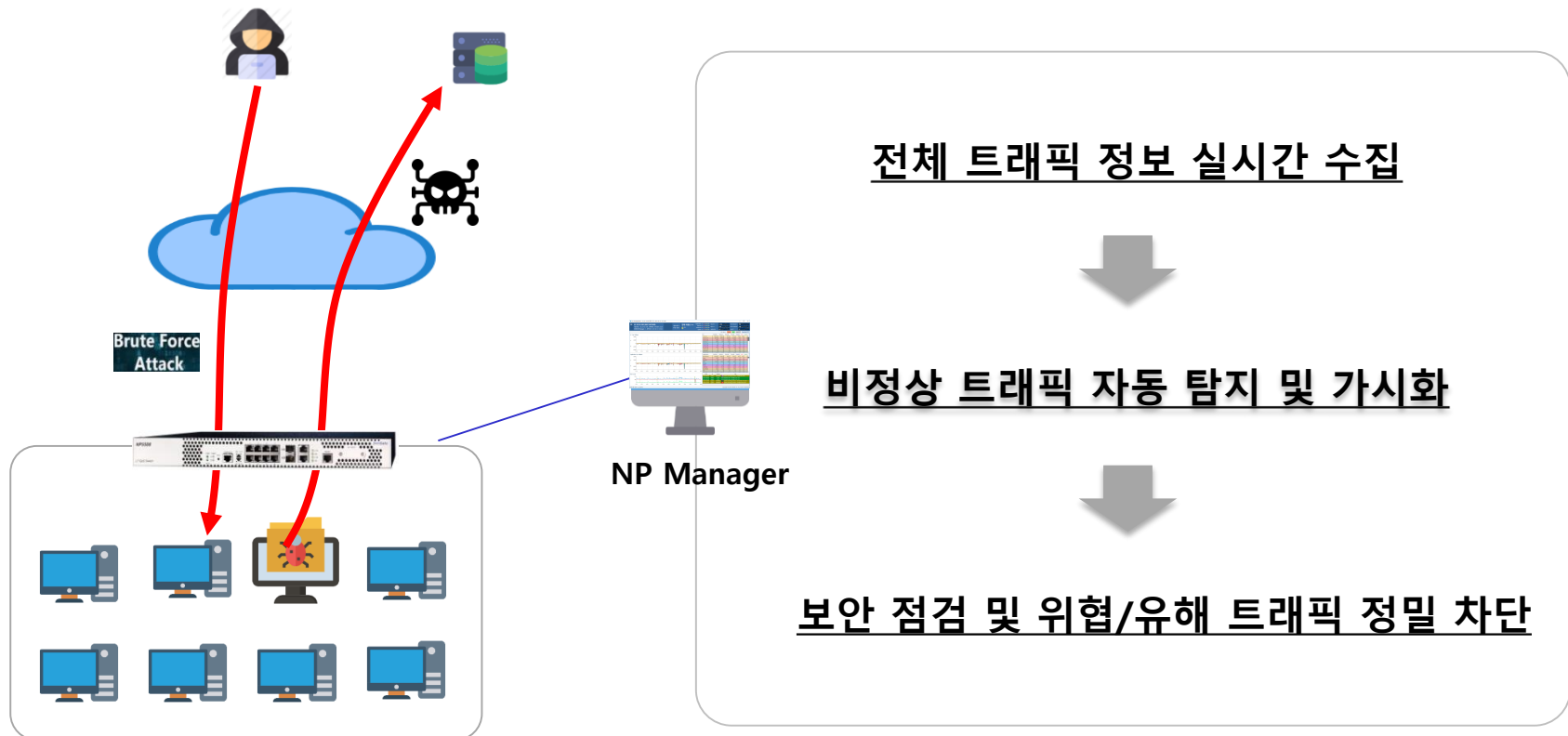
## 트래픽 폭주 상황 속에서도 안정적인 인터넷 서비스 제공

\* 어플리케이션 등 실시간으로 인지된 다양한 트래픽 정보를 활용



## 계정 탈취, 좀비 활동 등 네트워크 공격 및 피해 자동 탐지 및 관리

- \* 연속적으로 수행되는 비정상 로그인 시도 패턴을 자동 탐지하여 계정 탈취 위협으로부터의 보호
- \* 내부 좀비 PC에서 외부로 공격 (또는 외부에서 내부로 공격)하는 트래픽을 탐지 및 관리





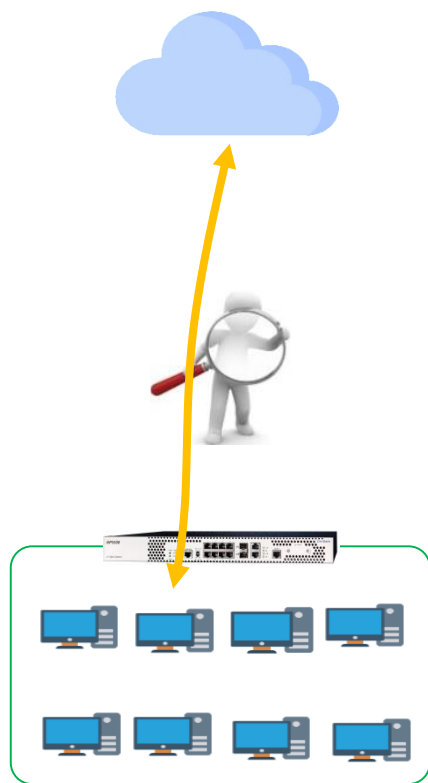
# 특징

# 네트워크 가시성

IntiGate

## 전체 트래픽 현황을 IP, 어플리케이션, 디바이스 별로 가시화

\* 다양한 화면을 통해 전체 및 특정 트래픽의 가시화 및 통계 데이터 표시

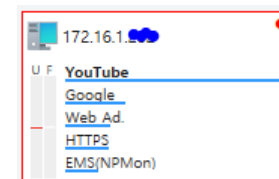


대시보드 (전체 디바이스 정보)

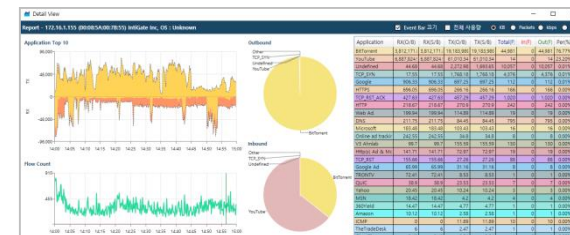


디바이스 종류 별 연결 현황  
(PC, IP 전화기, 서버, CCTV 등)

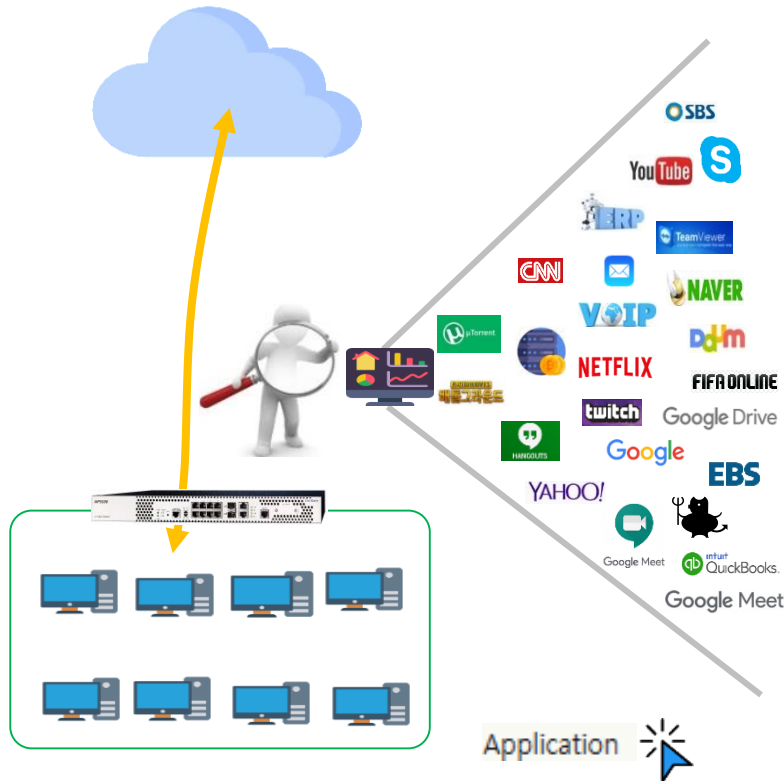
1개 디바이스 정보



디바이스 세부 정보  
(Detail View)



## P2P 서비스와 같은 어플리케이션을 인지하여 제어 수행

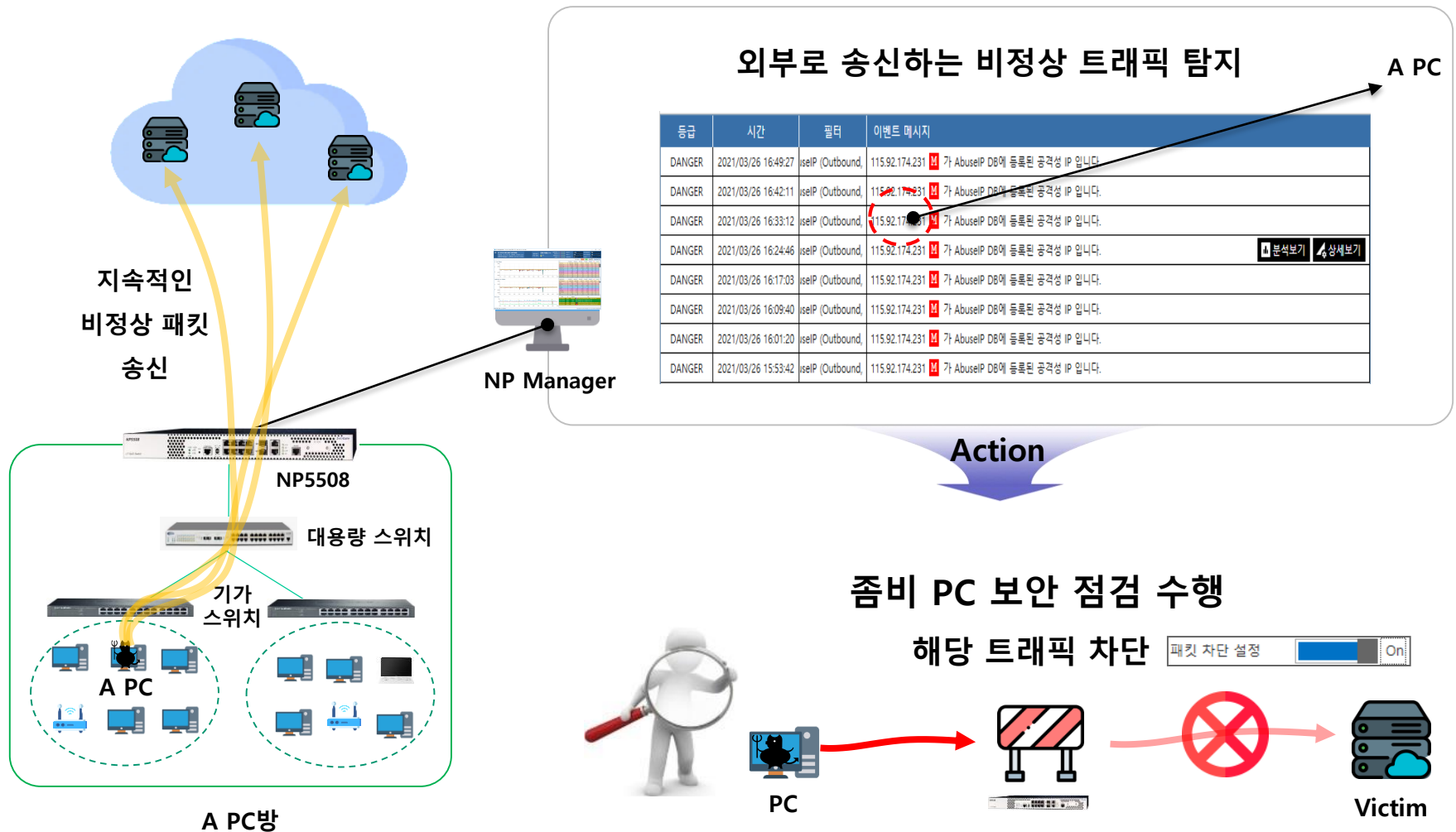


| Application | RX(O/B)   | RX(S/B)   |
|-------------|-----------|-----------|
| BitTorrent  | 18,658.63 | 18,658.63 |
| YouTube     | 1,104.72  | 1,104.72  |
| Microsoft   | 1,006.9   | 1,006.9   |

\* DPI 기술을 활용한 어플리케이션 인지



## 내부 좀비 PC에서 발생하는 비정상 트래픽 탐지 및 방지



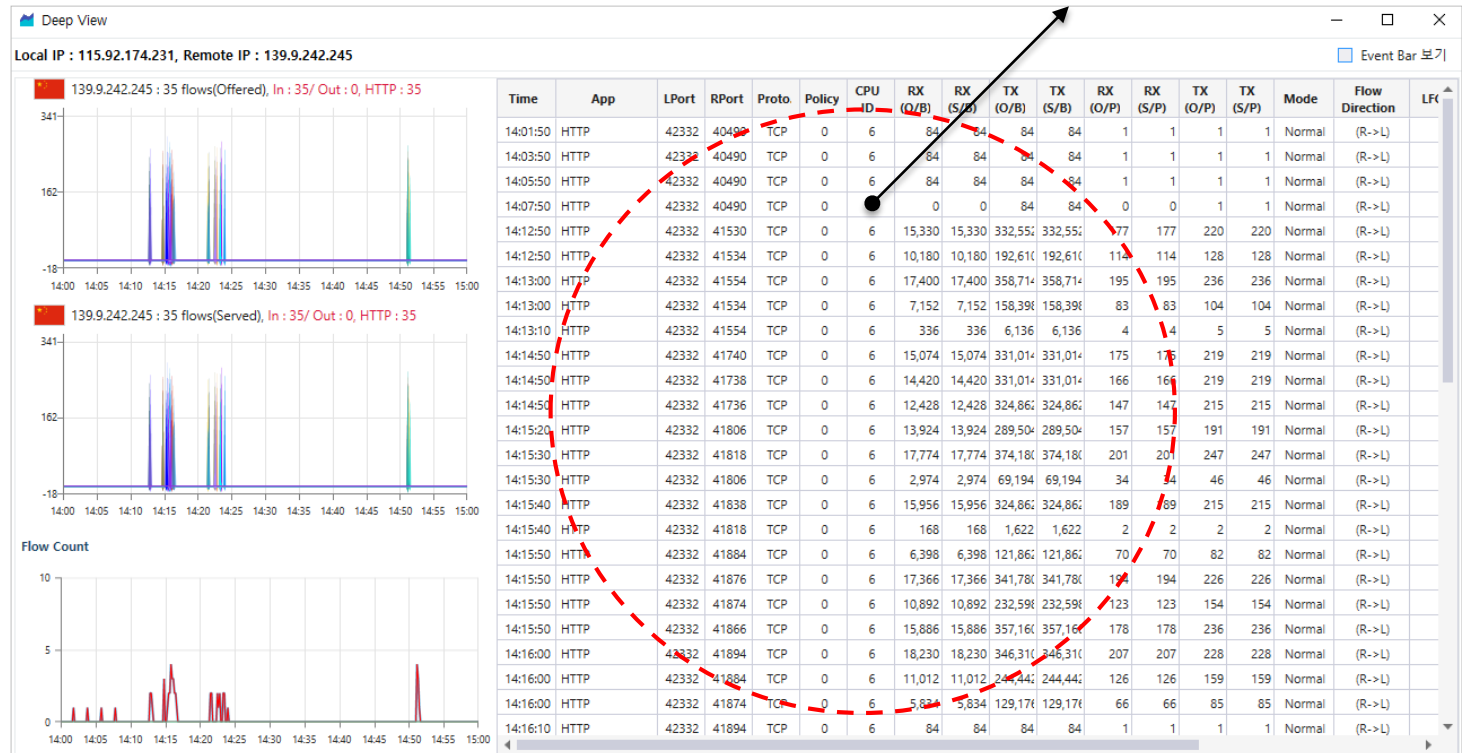
# ※ 좀비 탐지 (예시)

## 이벤트

| 등급     | 시간                  | 필터              | 이벤트 메시지                                                                                    |
|--------|---------------------|-----------------|--------------------------------------------------------------------------------------------|
| DANGER | 2021/03/26 16:49:27 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |
| DANGER | 2021/03/26 16:42:11 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |
| DANGER | 2021/03/26 16:33:12 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |
| DANGER | 2021/03/26 16:24:46 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다. <span>분석보기</span> <span>상세보기</span> |
| DANGER | 2021/03/26 16:17:03 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |
| DANGER | 2021/03/26 16:09:40 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |
| DANGER | 2021/03/26 16:01:20 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |
| DANGER | 2021/03/26 15:53:42 | IsIP (Outbound, | 115.92.174.231 <b>M</b> 가 AbuselIP DB에 등록된 공격성 IP 입니다.                                     |

Local IP가 Malware 다운로드 IP로 등록된 경우

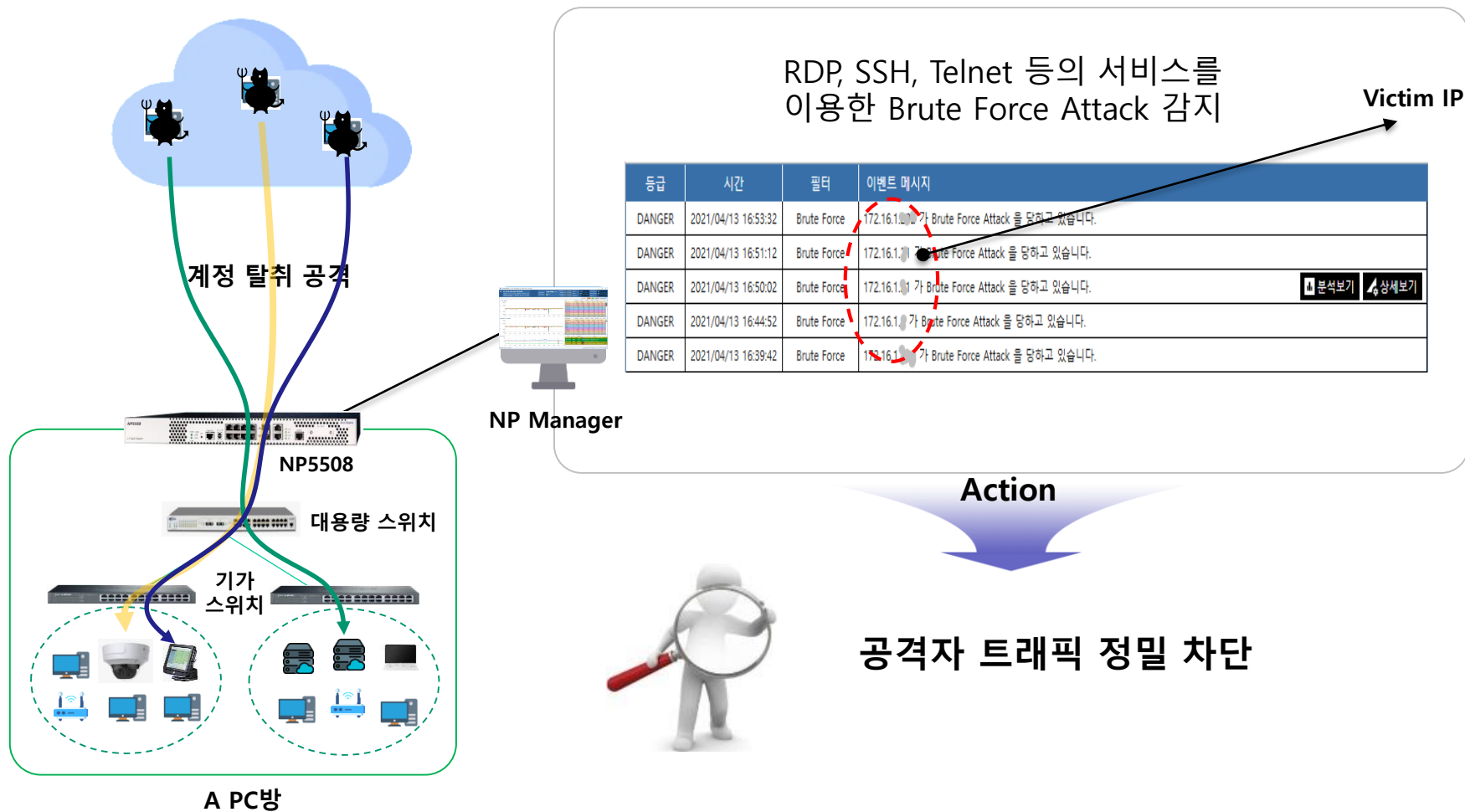
HTTP 및 특정 Port 로 접속한 Malware 다운로드 트래픽 확인



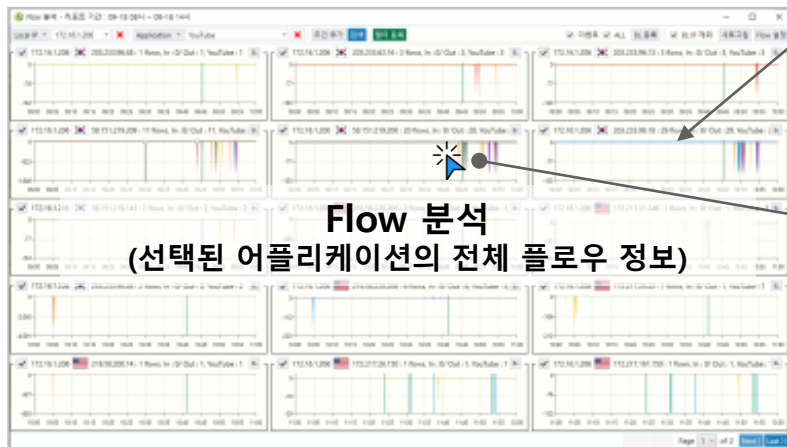
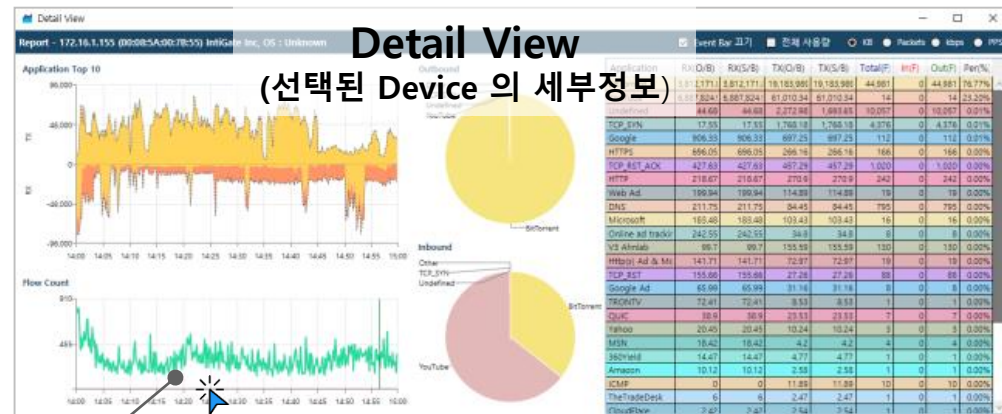
플로우 기반  
트래픽 사용 정보  
(Deep View)

## 계정 탈취를 위한 Brute Force Attack 을 감지 하고 방지

\* CCTV, IoT 기기 등의 보안 취약성을 이용하여 계정 탈취 공격 후 바이러스 이식

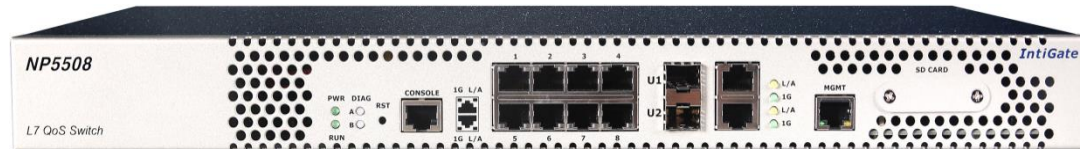


## 전체 트래픽 가시화 및 간편한 정책 관리 수행 (NP Manager)



NP5508 은 플로우 기반으로 전체 트래픽 정보를 실시간으로 수집하고 제어하는 QoS 보안 스위치로, STMP 테크놀로지를 적용하여 호스트에서 발생하는 어플리케이션 등 트래픽 정보를 상세히 관리 및 가시화 하고 QoS 및 보안 서비스 정책에 따라 관리를 수행 한다.

## - 형상 및 제원



| 구 분    | 내 용                               |
|--------|-----------------------------------|
| LAN 포트 | 8 x 10/100/1,000Mbps TX           |
| WAN 포트 | 2 x 1Gbps FX/TX Combo             |
| Size   | 240mm (W) * 250mm (D) * 43 mm (H) |

| 구 분    | NP5508                                                                                                                                                                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 네트워크   | <ul style="list-style-type: none"> <li>- IPv4 / IPv6</li> <li>- Static Routing (L3)</li> <li>- NAT (N:1, N:M)</li> <li>- DHCP Server/Client</li> <li>- STP, Port Mirroring, IGMP Snooping, VLAN</li> </ul>                                                                      |
| QoS    | <ul style="list-style-type: none"> <li>- 트래픽 분류 : 5tuples, Application, IP Group, Application Group</li> <li>- 트래픽 관리 : Flow 또는 Application 기반</li> <li>- 다양한 정책 설정 및 제어(drop, VL, Q모드, 대역폭)</li> <li>- 시그니처 기반의 P2P 서비스 감지 및 제어</li> <li>- 자체 어플리케이션 DB 및 주기적인 업데이트</li> </ul> |
| 보안     | <ul style="list-style-type: none"> <li>- DDoS 공격 탐지 및 방어 (Portscan, TCP syn/ICMP/UDP flooding)</li> <li>- 계정 탐지 공격 방어 (Brute force attack)</li> <li>- 링크 단위 TCP syn, ICMP, Port# 기준의 PPS 트래픽량 제어</li> <li>- CPU 향 비정상 트래픽 제어</li> </ul>                                         |
| 시스템 관리 | <ul style="list-style-type: none"> <li>- GUI 기반의 Configuration</li> <li>- SNMP, syslog / telnet, SSH</li> <li>- 원격 OS, configuration, 시그니처 DB 업그레이드</li> <li>- Dying gasp / Auto recovery / Die reason</li> <li>- 임계치 설정 (CPU, memory, temp., fan) 및 알람</li> </ul>              |

| 구 분                                                | NP Manager                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 대시보드<br>/<br>리포팅<br>/<br>네트워크<br>보안 진단<br>/<br>NDR | <ul style="list-style-type: none"> <li>- 대시보드/리포팅</li> <li>- 플로우 기반의 다양한 트래픽 정보 수집 및 저장 (5tuples, Application, Policy, 트래픽양)</li> <li>- 특정 시간대 트래픽 정보 요약 및 상세 보기</li> <li>- 네트워크/보안 진단 서비스</li> <li>- 설정된 Policy, QoS, NTP, DNS 정보 진단</li> <li>- 보안취약점, 내부 감염PC, 외부 attack 진단</li> <li>- NDR</li> <li>- 네트워크 위협 트래픽을 카테고리 별로 이벤트 발생</li> <li>- 카테고리 : Inbound, Outbound, Application, System</li> </ul> |
| 블랙리스트                                              | <ul style="list-style-type: none"> <li>- 블랙리스트</li> <li>- IP, 플로우 방향, 프로토콜, 포트 별 블랙리스트 관리</li> <li>- 관리 화면을 통한 전체 공격자 IP / 예외 IP 관리</li> </ul>                                                                                                                                                                                                                                                          |
| 실시간 모니터링                                           | <ul style="list-style-type: none"> <li>- IP/Application/Policy 별 Top 10 그래프</li> <li>- IP/Application/Policy 별 entry 정보 (RX/TX, Offered/Served, Kbps/PPS, Flow 트래픽량)</li> <li>- 전체 Flow Count (Total, Inbound, Outbound)</li> <li>- 알람 정보 테이블</li> </ul>                                                                                                                                                |
| 장비 설정                                              | <ul style="list-style-type: none"> <li>- 시스템, 네트워크, QoS, 보안 관련 설정</li> </ul>                                                                                                                                                                                                                                                                                                                            |

\* NP Manager 설치 환경 (권장) : Win10 Pro, 8G RAM, 512G SSD



## (주)인티게이트

#804~805, Mega Center, SKntechnopark, 124, Sagimakgol-ro, Jungwon-gu, Seongnam-si, Gyeonggi-do, Korea

TEL : +82-31-776-2430 FAX : +82-31-776-2432 URL : [www.intigate.com](http://www.intigate.com) E-mail : [marketing@intigate.com](mailto:marketing@intigate.com)