2024’

Ntopng 패킷 캡처 기반 트래픽분석 시스템 소개 자료

NMS구축 및 유지보수 전문기업
HOSTING GLOBAL
SINCE 2008

ntop

ChatGPT Powered

CONTENTS

Ntopng란?

Ntopng 소개

1. Ntop:

- Ntop은 “Network top"의 약자로, 네트워크 트래픽 모니터링을 위한 오픈 소스 도구입니다.
- 1998년에 Luca Deri에 의해 개발되었습니다.
- 웹 기반 인터페이스를 통해 네트워크 사용량과 성능을 실시간으로 모니터링할 수 있습니다.
- 현재는 Ntopng로 대체되었습니다.

2. Ntopng:

- Ntopng는 "next generation ntop"의 약자로, Ntop의 후속 버전입니다.
- 더 강력하고 현대적인 기능을 제공하며, 고성능 네트워크 트래픽 분석 및 모니터링 도구입니다.
- 실시간 네트워크 트래픽 모니터링, 프로토콜 분석, 패킷 캡처, 플로우 분석 등 다양한 기능을 제공합니다.
- 웹 기반 GUI를 통해 사용자 친화적인 인터페이스를 제공합니다.
- 오픈 소스 및 상용 버전이 모두 제공됩니다.

3. Ntop team:

- Ntop team은 Ntop 및 Ntopng를 포함한 다양한 네트워크 모니터링 및 보안 도구를 개발하는 팀입니다.
- Luca Deri가 이끄는 이 팀은 이탈리아에 본사를 두고 있습니다.
- 오픈 소스 프로젝트와 상용 제품을 동시에 개발하고 있습니다.
- Ntop, Ntopng 외에도 nProbe, n2disk, nBox 등 다양한 네트워크 관련 도구를 개발하고 있습니다.
- 네트워크 모니터링, 트래픽 분석, 보안, 성능 최적화 등의 분야에서 혁신적인 솔루션을 제공하고 있습니다.

Ntop team은 지속적으로 제품을 개선하고 새로운 기능을 추가하며, 네트워크 관리자와 보안 전문가들에게 중요한 도구를 제공하고 있습니다. 그들의 제품은 기업, 교육 기관, 정부 기관 등 다양한 조직에서 널리 사용되고 있습니다.

CHAPTER II

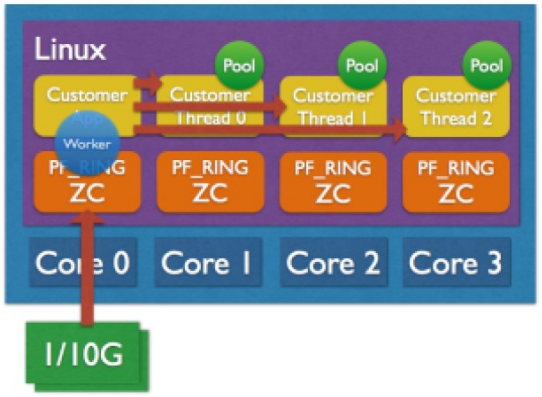
nTopNG 기능

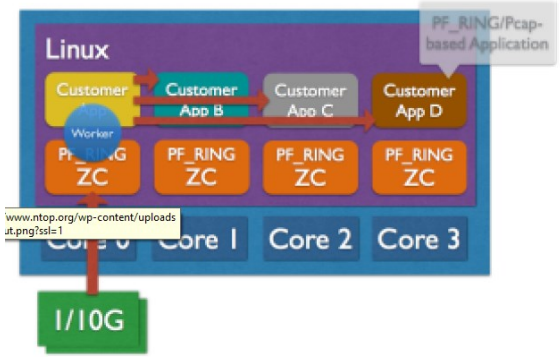
1. 주요기능
2. 트래픽 가시화 구현 기능
3. 실시간 트래픽 분석
4. 그외 유용한 기능
5. 향후 개발 예정 사항 소개

II nTopNG 기능소개

01. 주요기능

» 고성능 패킷 처리를 위한 PF_RING ZC (Zero Copy) 기술 탑재
» 커널을 Bypass 하여 트래픽을 Application 으로 직접 Forwarding 하는 기술
» Linux Based OS Support, Intel 10G, Melanox 40G/100G NIC Support





PF_RING ZC (Zero Copy)

Multi-10 Gbit RX/TX Packet Processing from Hosts and Virtual Machines

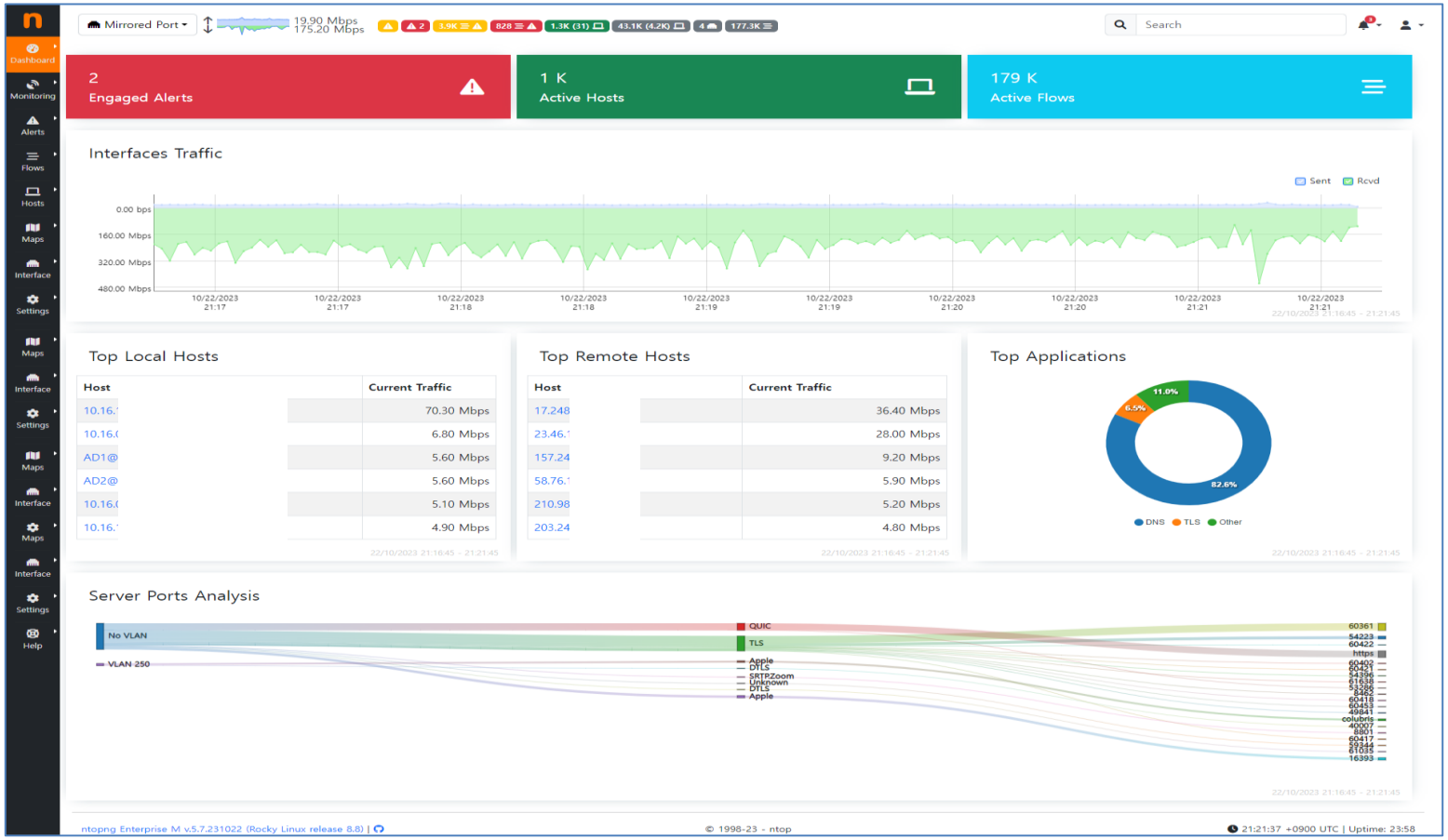
PF_RING™ ZC (Zero Copy) is a flexible packet processing framework that allows you to achieve 1/10 Gbit line rate packet processing (both RX and TX) at any packet size. It implements zero copy operations including patterns for inter-process and inter-VM (KVM) communications. It can be considered as the successor of DNA/LibZero that offers a single and consistent API based on the lessons learnt on the past few years.

It features a clean and flexible API that implement simple building blocks (queue, worker and pool) that can be used from threads, applications and virtual machines. This to implement 10 Gbit line-rate packet processing.

II nTopNG 기능소개

01. 주요기능

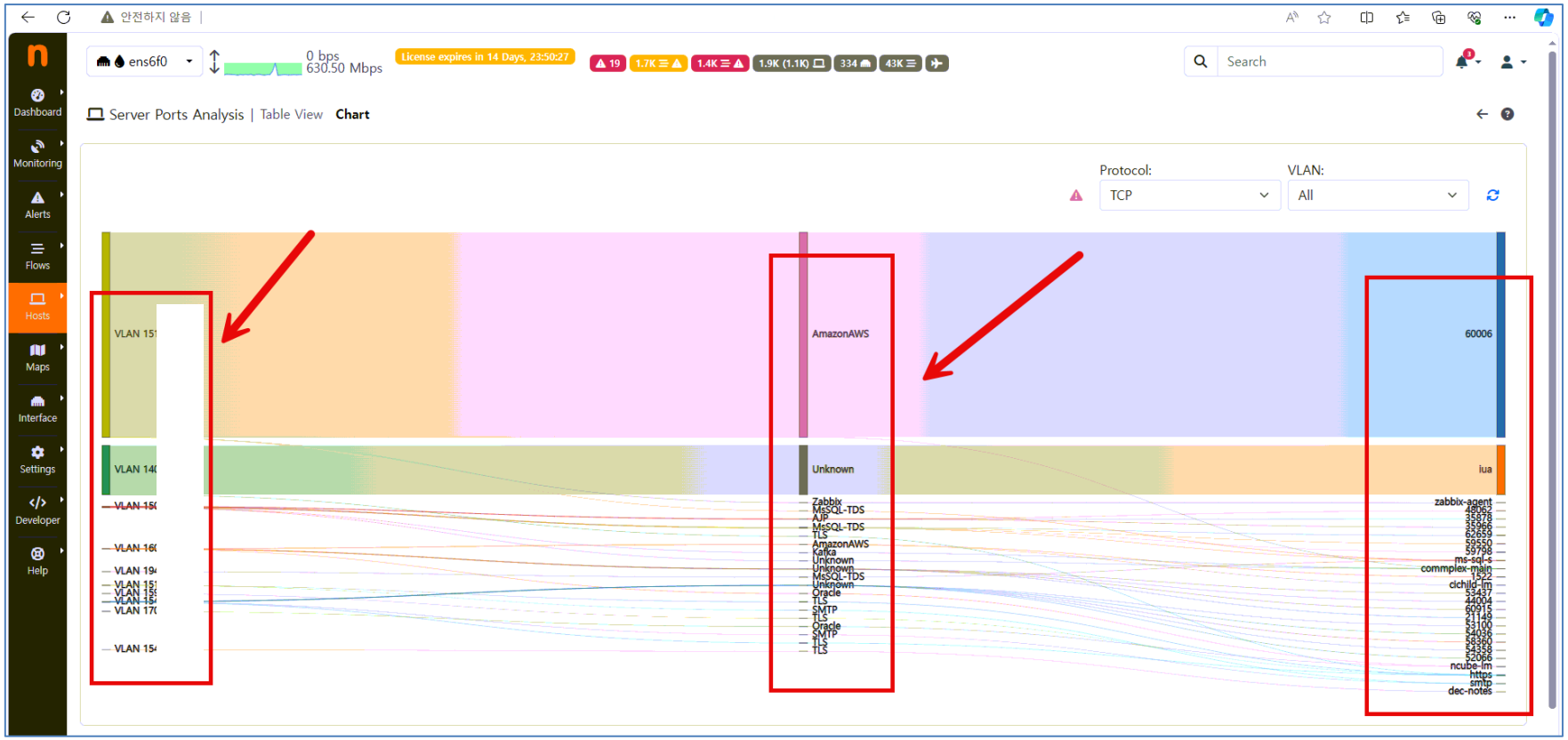
» Realtime Packet Capture 방식 사용
» 발신지 IP, 수신지 IP 대상 포트, L7 어플리케이션 등의 정보를 분석하여 보여줌
» 많이 쓰는 사용자의 IP를 조회하여 어떤 사용자가 사용하고 있는지 확인 가능함
» HTTPS 프로토콜의 헤더 정보 해독 가능



II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

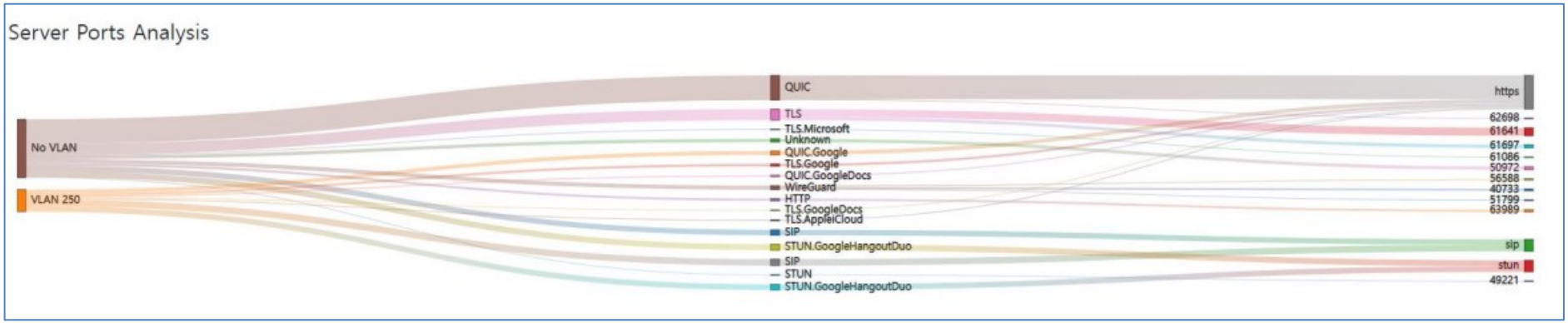
» VLAN 별로 발생되는 트래픽 양 확인 가능
» 어떤 경로를 통해서 트래픽이 이동하는지 확인 가능
» 최종 목적지 정보 확인 가능

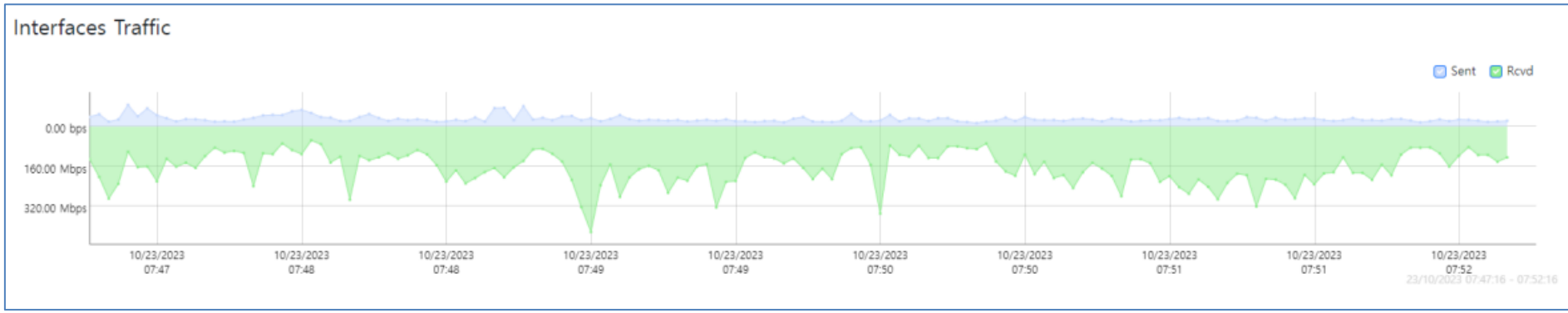


II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

» 실시간으로 트래픽을 분석하여 접속 상황을 도식화하여 표시하는 기능 구현
» 실시간 트래픽 사용량을 그래프로 표시하는 기능 구현

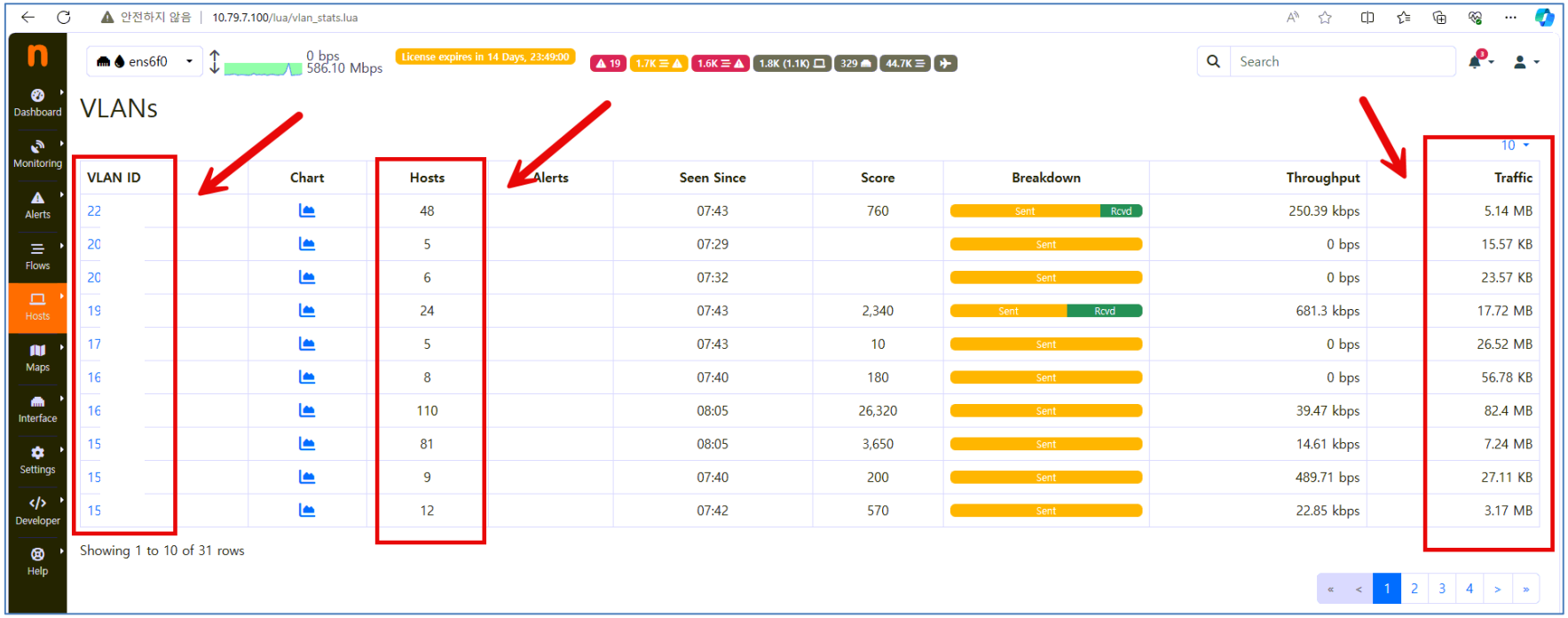




II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

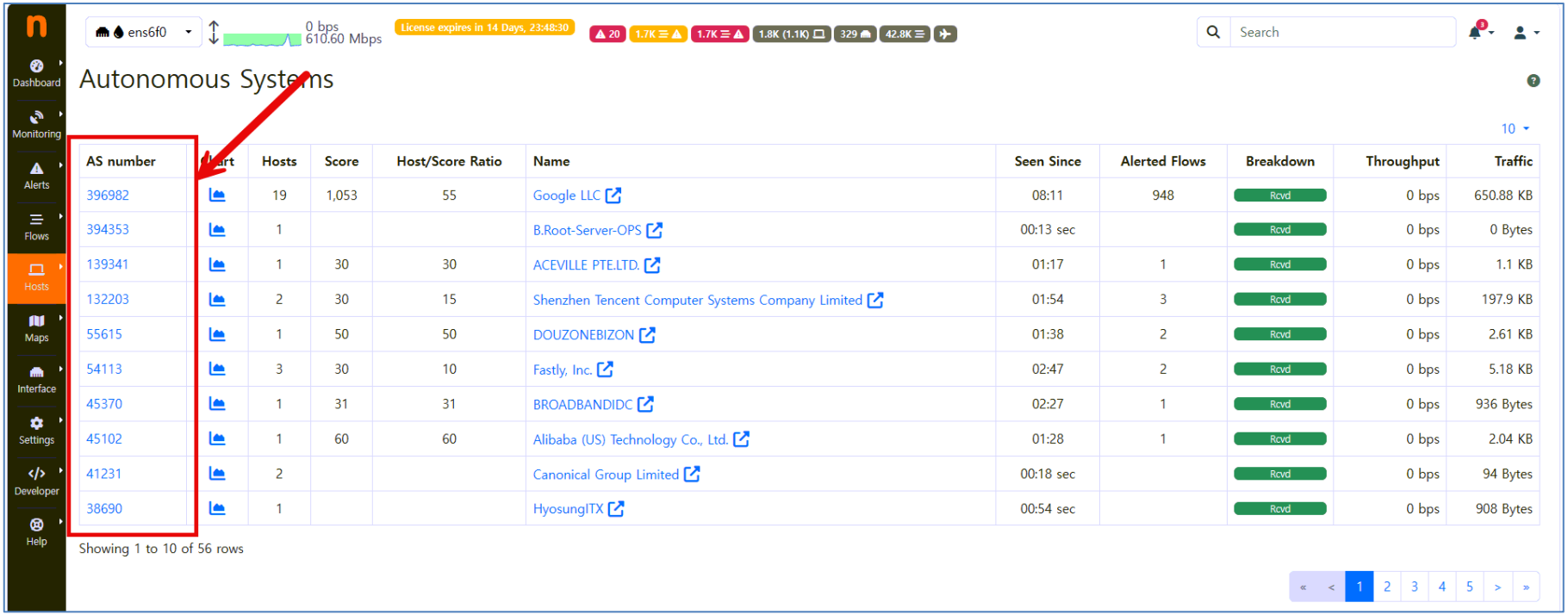
» VLAN 별 통신하는 호스트 수량 파악 가능
» VLAN 별 통신하는 트래픽 정보 파악 가능



II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

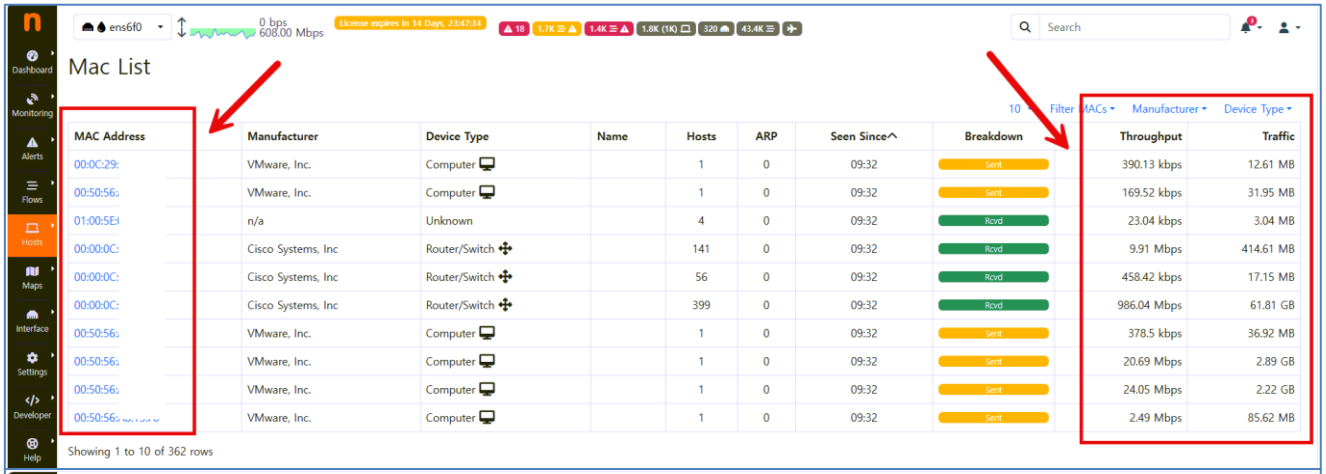
» Autonomous Number 별로 호스트 정보 정보 파악 가능
» Autonomous Number 별로 트래픽 정보 파악 가능

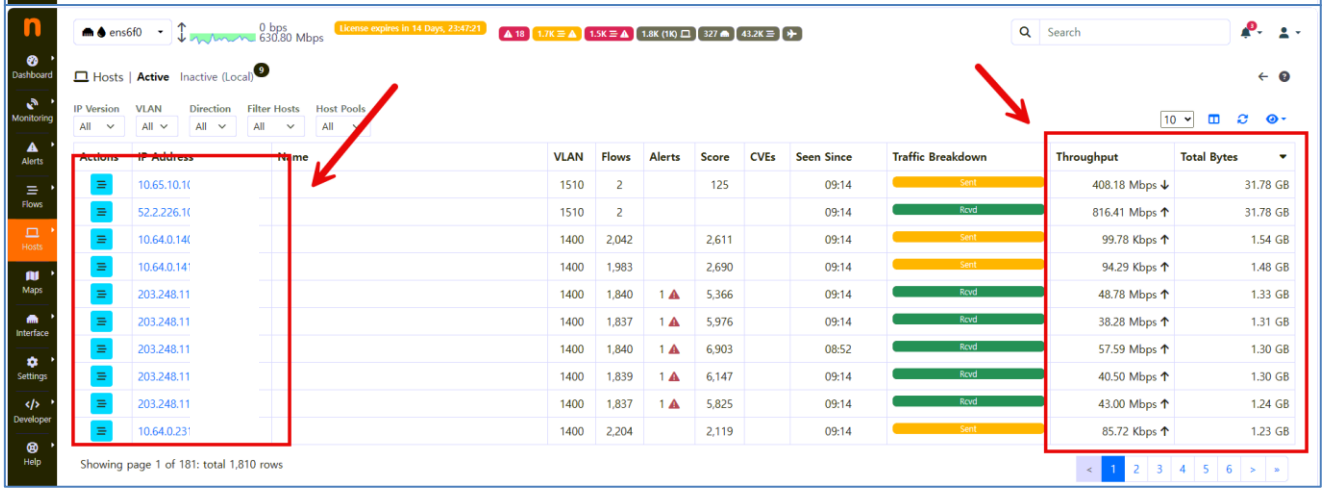


II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

» MAC Address 별 통신하는 트래픽 속도와 트래픽 양 파악 가능
» Hosts 별 통신하는 트래픽 속도와 트래픽 양 파악 가능





II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

» 사용자가 임의로 네트워크 대역으로 등록할수 있는 기능 제공
» 생성한 네트워크 대역에 해당하는 호스트 정보 확인 가능
» 생성한 네트워크 대역에 해당하는 트래픽 정보 확인 가능

Networks

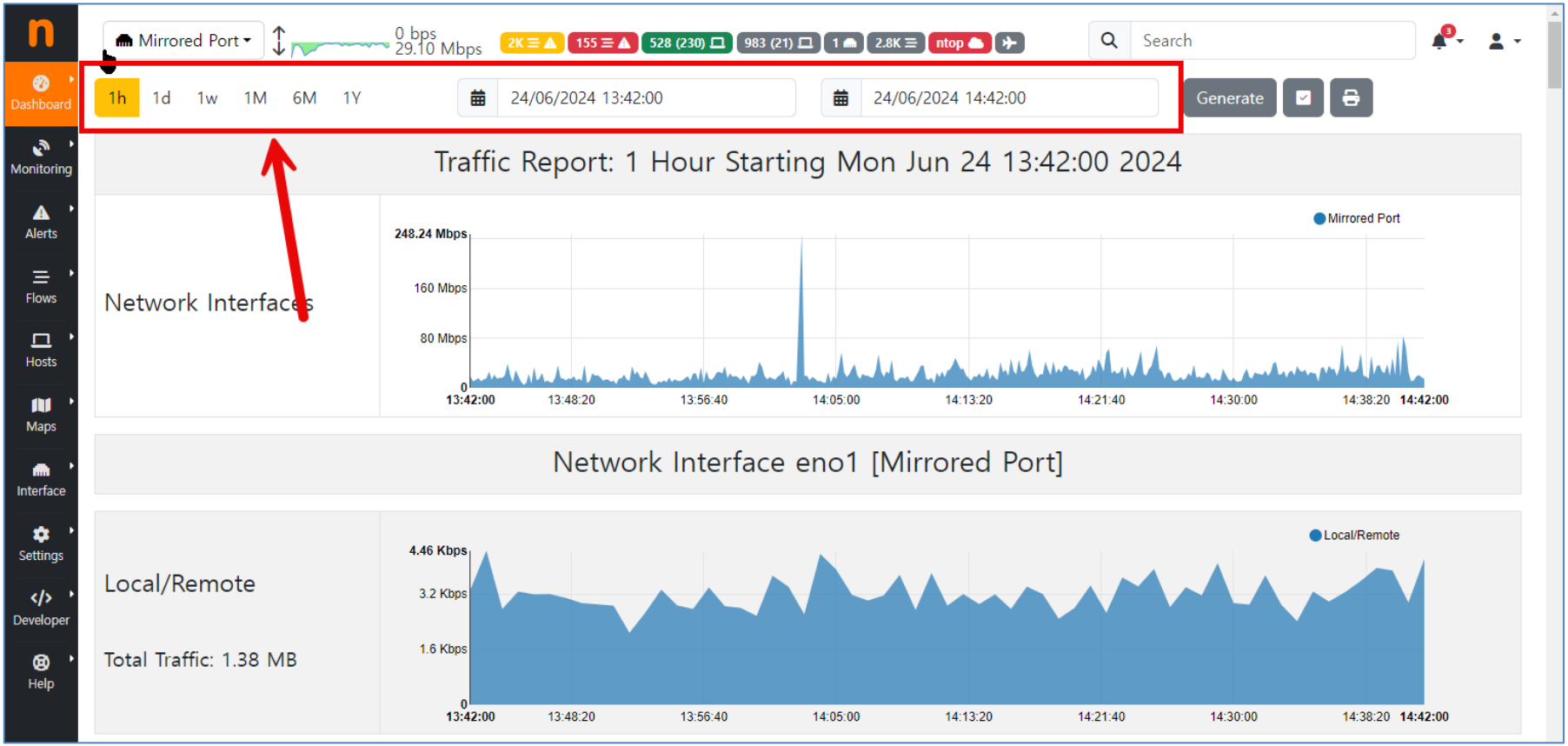
Networks Score

Network Name	Chart	Hosts	Score	Host/Score Ratio	Alerted Flows	Breakdown	Throughput	Traffic
6.0.0/16]		64	13,833	216	161,379	Rcvd	6.01 Mbps	26.36 GB
.0.0/16]		149	14,440	96	202,064	Rcvd	20.18 Mbps	17.77 GB
0.8.2.0/24]		46	6,853	148	76,516	Rcvd	63.35 kbps	17.21 GB
24]		14	2,560	182	80,441	Rcvd	544.66 kbps	13.75 GB
.0/24]		79	30,238	382	131,224	Rcvd	4.11 Mbps	13.19 GB
/24]		15	16,244	1,082	106,819	Rcvd	8.58 Mbps	9.45 GB
0.10.2.0/24]		64	1,633	25	70,301	Rcvd	15.53 kbps	6.27 GB
.0.0/16]		9	2,128	236	31,539	Rcvd	486.64 kbps	3.48 GB
0.8.1.0/24]		65	3,257	50	72,966	Rcvd	90.78 kbps	2.86 GB
0.0/16]		8	942	117	6,032	Rcvd	3.38 Mbps	639.36 MB

II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

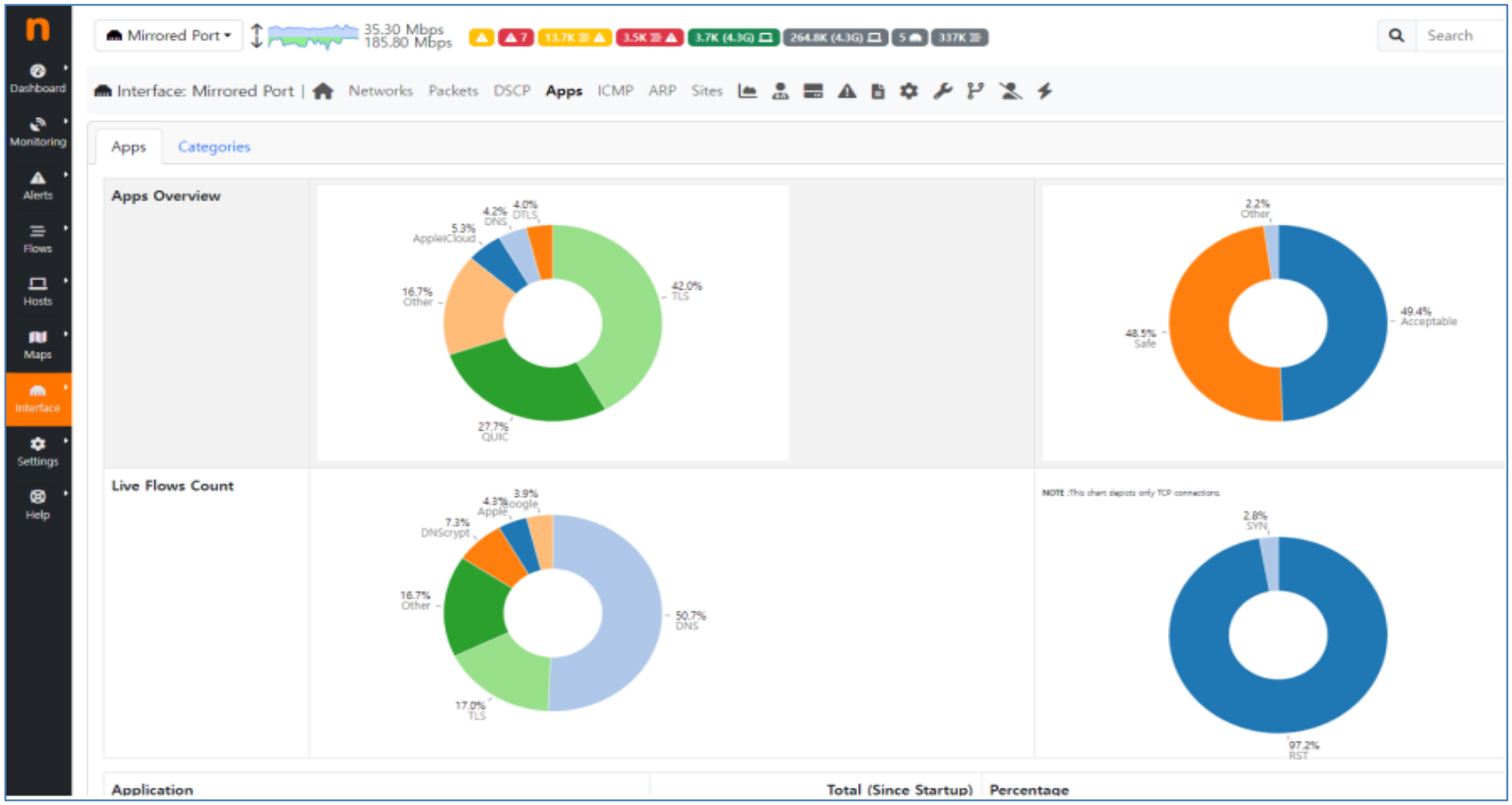
» 1시간, 1일, 1주일, 1달, 6개월, 1년 의 기간을 정해서 정보 확인 가능
» 사용자 임의의 기간을 정해서 정보 확인 가능
» 트래픽 정보와, 네트워크 대역 정보, 사용하는 어플리케이션 정보 확인 가능



II nTopNG 기능소개

03. 어플리케이션별 트래픽 분석 구현

» 어떤 종류의 트래픽을 많이 쓰는지 자체 포트번호 매핑 기능을 통하여 보여줌
» 등록되지 않은 포트명은 수동으로 추가 가능



II nTopNG 기능소개

03. 어플리케이션별 트래픽 분석 구현

» 실시간으로 흐르는 트래픽 정보를 DPI(Deep Packet Inspection) 기술로 분류 가능
» SSL, TLS, QUIC 등 암호화된 패킷 정보의 헤더를 분석하여 Youtube, Facebook, Google등 분류 가능

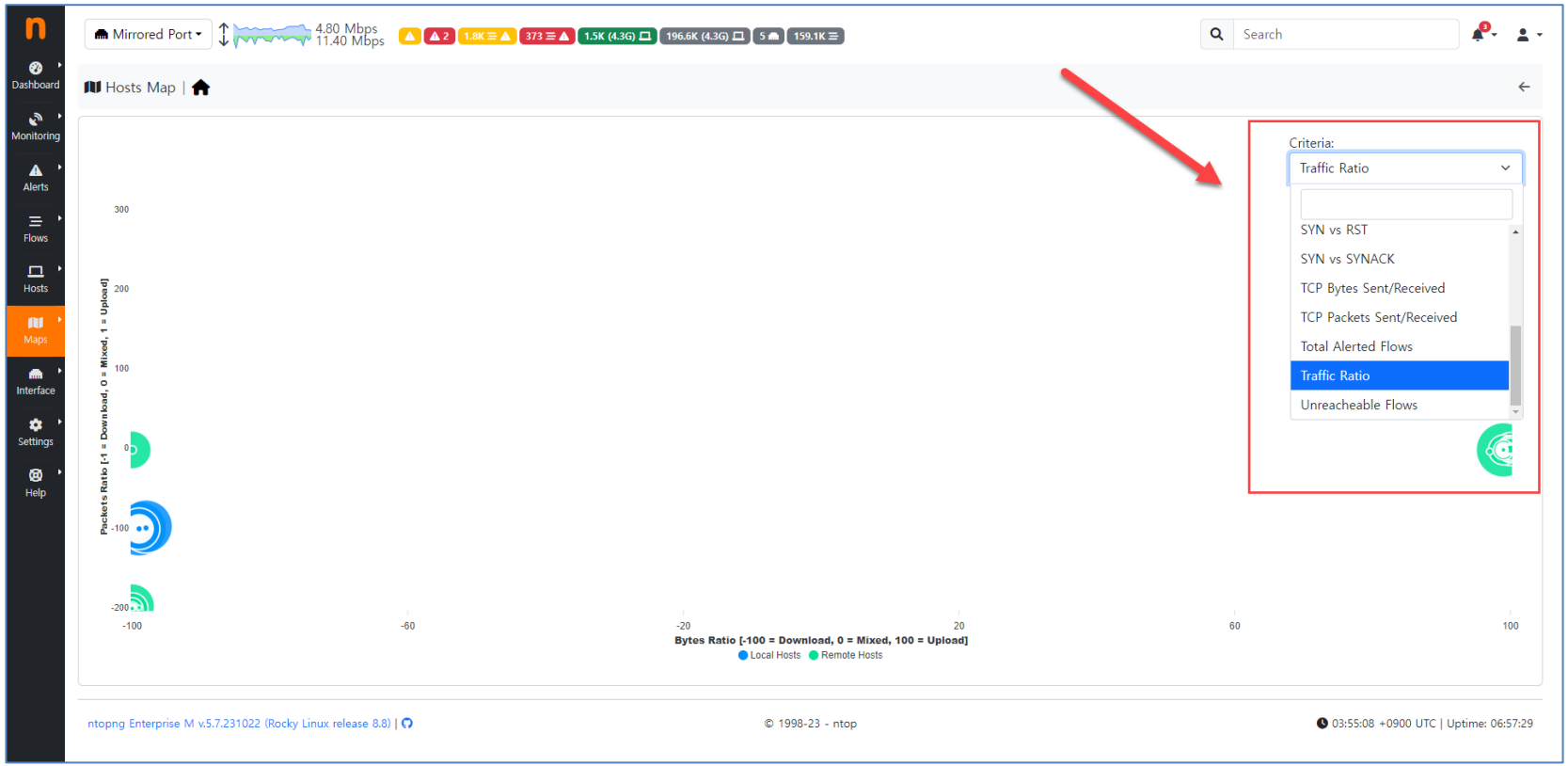
Application	Total (Since Startup)	Percentage
ADS_Analytic_Track	12.46 MB	0.0 %
AVAST	1.22 KB	0.0 %
Alibaba	3.89 MB	0.0 %
Amazon	1.29 MB	0.0 %
AmazonAWS	22.71 MB	0.0 %
Apple	714.88 MB	0.6 %
ApplePush	902.96 KB	0.0 %

Category	Apps	Total (Since Startup)	Percentage
Malware		657.43 KB	0.0 %
Streaming	1kxun, AppleiTunes, AppleTVPlus, Dailymotion, Dazn and 11 more	126.13 KB	0.0 %
Web	AccuWeather, AJP, Alibaba, Amazon, Apple and 28 more	99.37 GB	84.7 %
Game	Activision, AmongUs, Armagetron, CoD_Mobile, CryNetwork and 32 more	328.11 KB	0.0 %
Video	AdobeConnect, BFCP, IFLIX, NetFlix, Pluralsight and 3 more	2.04 MB	0.0 %
Cloud	AliCloud, AmazonAWS, AmazonVideo, ApplePush, Azure and 14 more	209.93 MB	0.2 %

II nTopNG 기능소개

02. 분석된 트래픽 가시화 구현

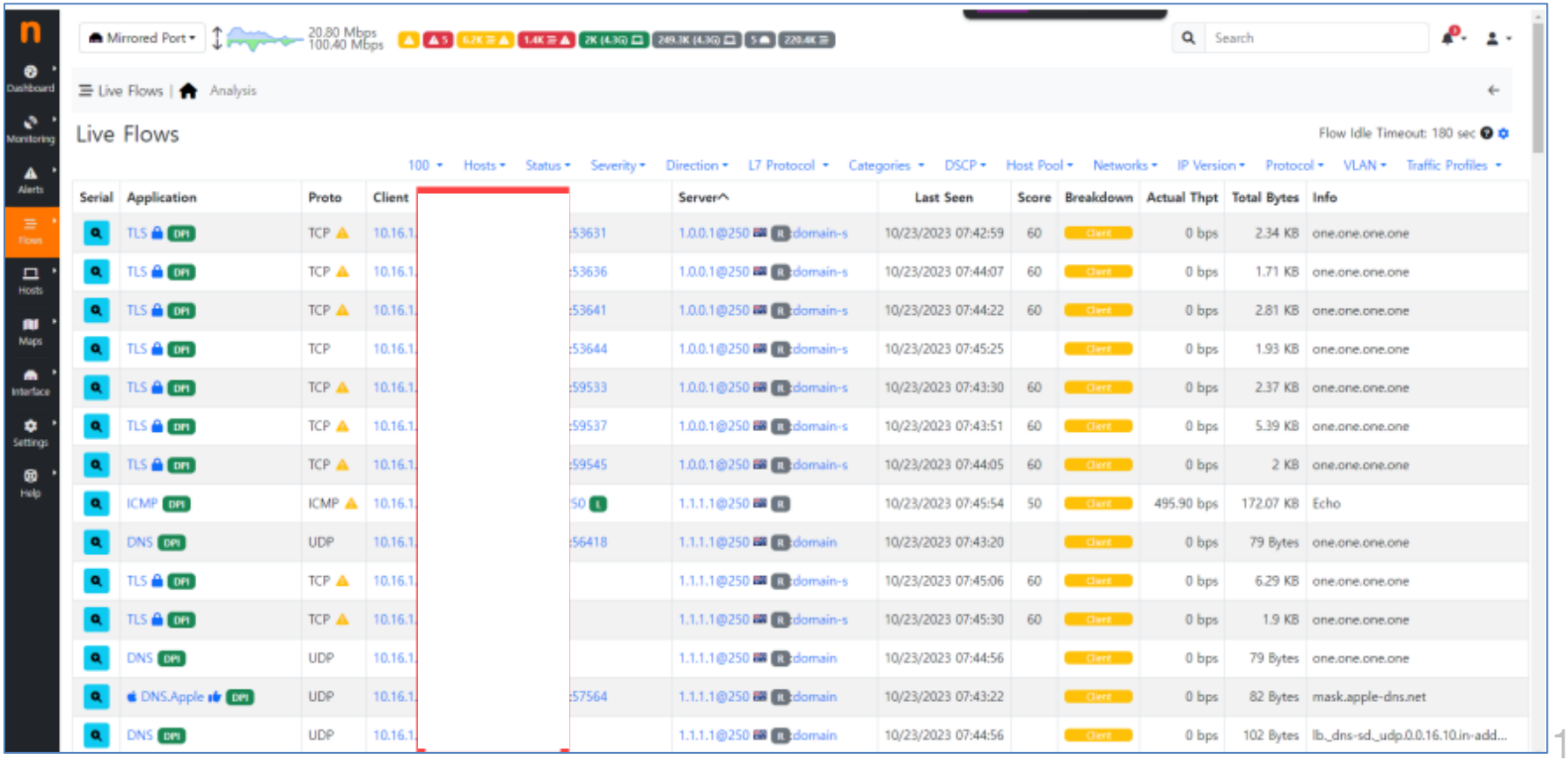
» Category 종류에 따라 호스트 정보를 가시화 하여 표시해 줌



II nTopNG 기능소개

03. 실시간 트래픽 분석

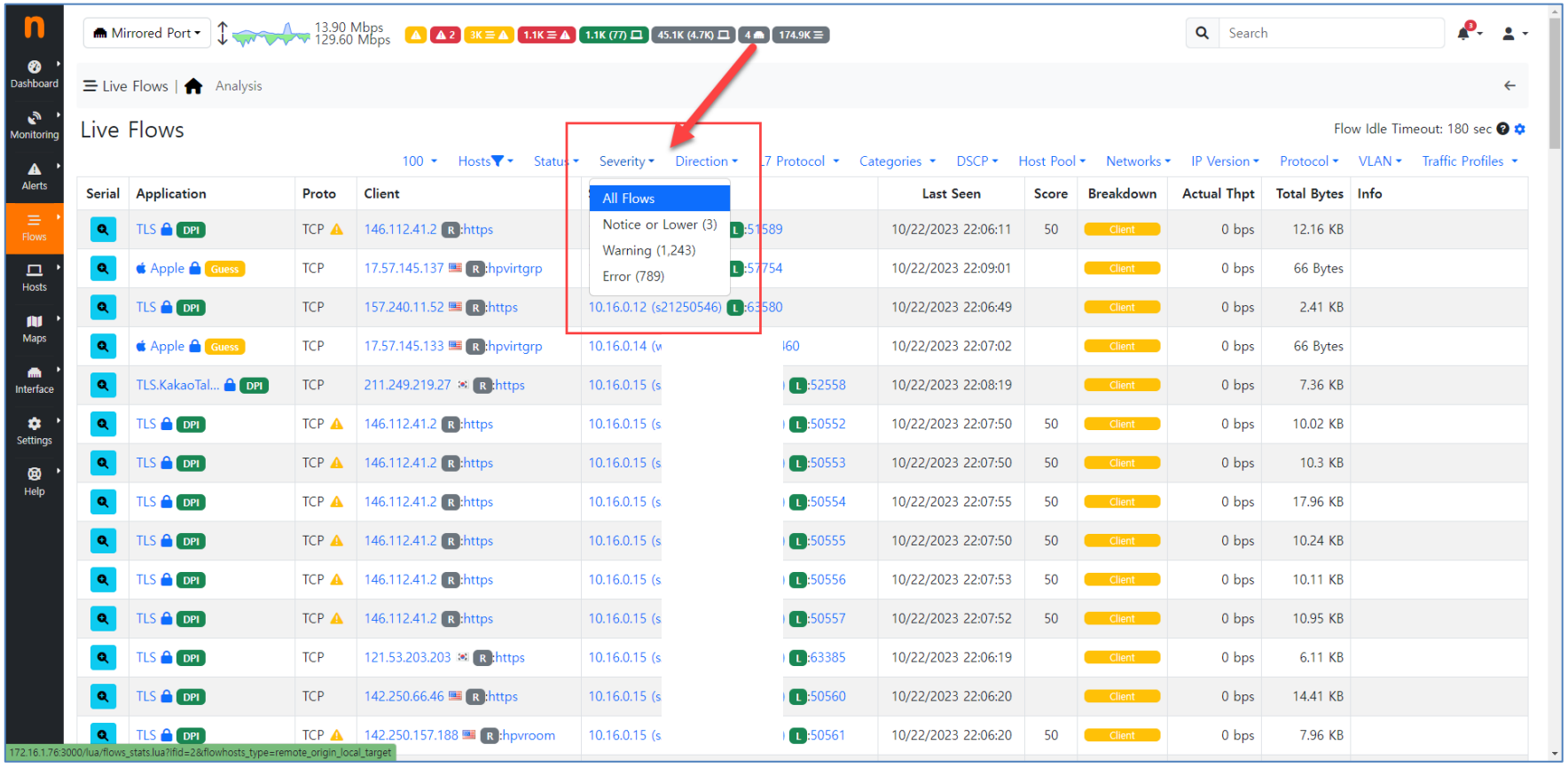
» Realtime Traffic Analysis 기능 지원 (반영시간 3 ~ 5초 정도)
» 조건 필터링을 통하여 원하는 내용 출력
» API 기능 지원으로 외부 시스템과 데이터 연동하여 화면에 표시하는 기능 구현



II nTopNG 기능소개

03. 실시간 트래픽 분석

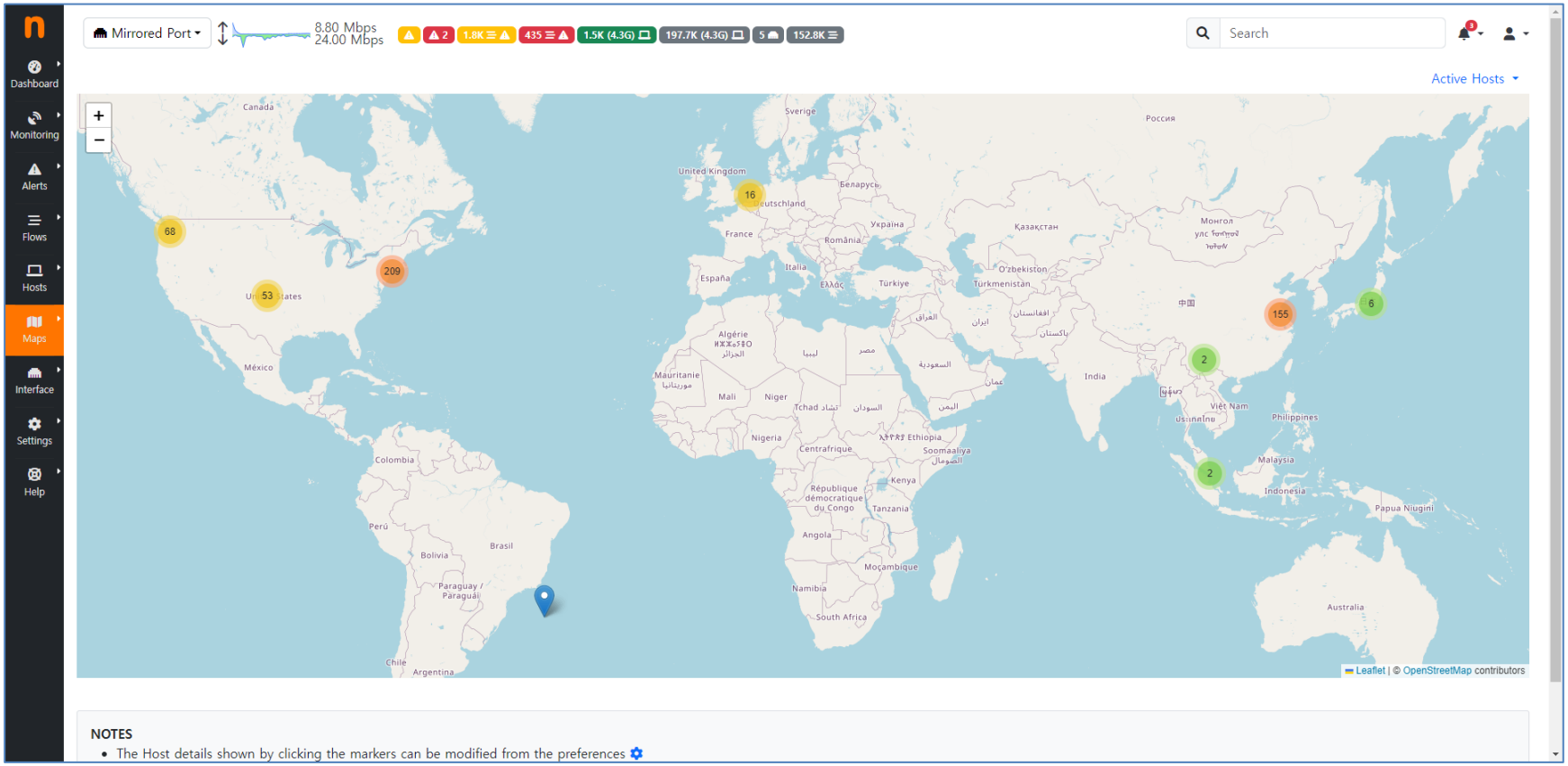
» 트래픽 상태별 필터링 기능
» 트래픽 상태 심각도 별 필터링 기능
» 카테고리별 필터링 기능
» 네트워크 대역별 필터링 등 가능



II nTopNG 기능소개

03. 실시간 트래픽 분석

» AS number 별로 통신상태와 트래픽 양 확인 가능
» VLAN 별로 통신상태와 트래픽 양 확인 가능
» 국가별 통신상태와 트래픽 양 확인 가능
» IP주소 DB에 관련하여 통신하고 있는 IP의 대략적인 위치(참고용도) 확인 가능



II nTopNG 기능소개

04. 그외 유용한 기능

» 주기적으로 Active Ping 을 보내서 장비 상태와 응답속도 측정 및 확인
» Node Port로 접근 여부 확인 기능 탑재

Mirrored Port | 26.30 Mbps 82.70 Mbps | Search

Dashboard | Monitoring | Alerts | Flows | Hosts | Maps | Interface | Settings | Help

Active Monitoring

Show 10 entries | Measurement | Alert Status | + | Search:

URL	Last IP	Measurement	Chart	Threshold	Last 24 Hours	Last Measurement	Measurement	Mean RTT / Jitter	Actions
10.30.0.	10.30.	Continuous ICMP		99 %		00:07	100 %	0.6 / 0.2 ms	
10.15.0.	10.15	Continuous ICMP		99 %		00:07	100 %	0.4 / 0.1 ms	
10.10.25	10.10.2	Continuous ICMP		99 %		00:07	100 %	0.4 / 0.1 ms	
10.10.25	10.10.2	Continuous ICMP		99 %		00:07	100 %	0.4 / 0.1 ms	

Showing 1 to 4 of 4 entries

« < 1 > »

Manage Configurations

NOTES:

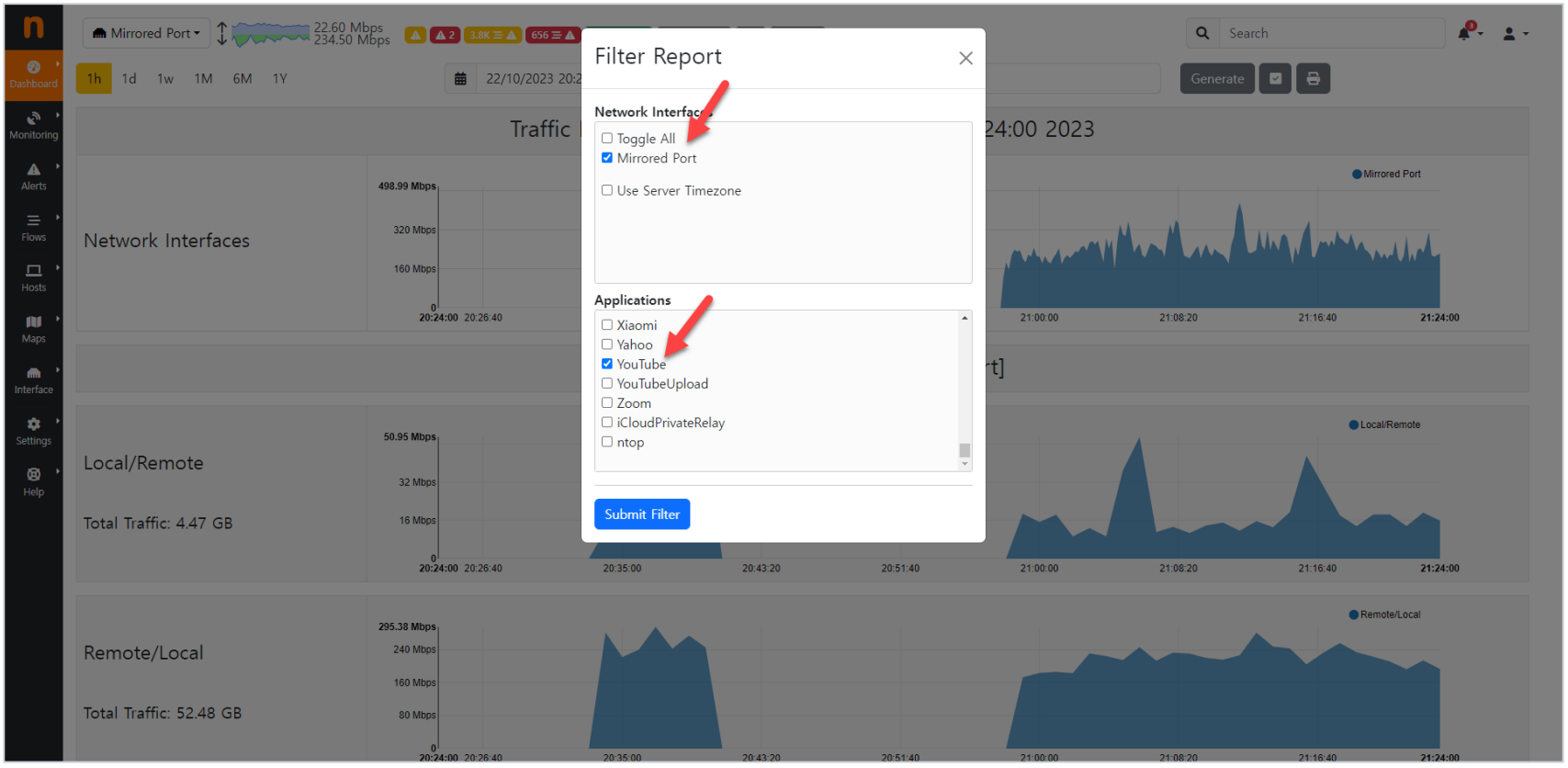
- ntopng generates traffic towards the configured hosts in order to perform measurements.
- An alert is triggered when the calculated measurement exceeds the threshold set.
- The dashed element identifies the current measurement hour.
- The availability percentage shows the percentage of time that the measurement has been within the configured threshold in the last day.

ntopng Enterprise M v.5.7.231022 (Rocky Linux release 8.8) | © 1998-23 - ntop | 21:51:03 +0900 UTC | Uptime: 53:24

II nTopNG 기능소개

04. 그외 유용한 기능

» 보려고하는 인터페이스, 어플리케이션 별 확인 가능
» 예시) 유튜브 등



II nTopNG 기능소개

04. 그외 유용한 기능

» nBPF 필터를 사용하여 원하는 트래픽을 추출하는 방법 소개
» 좌측 메뉴 SETTINGS -〉 TRAFFIC PROFILE에서 사용
» 필터 적용된 데이터는 DB에 저장되며 쿼리문 사용하여 데이터 추출 가능

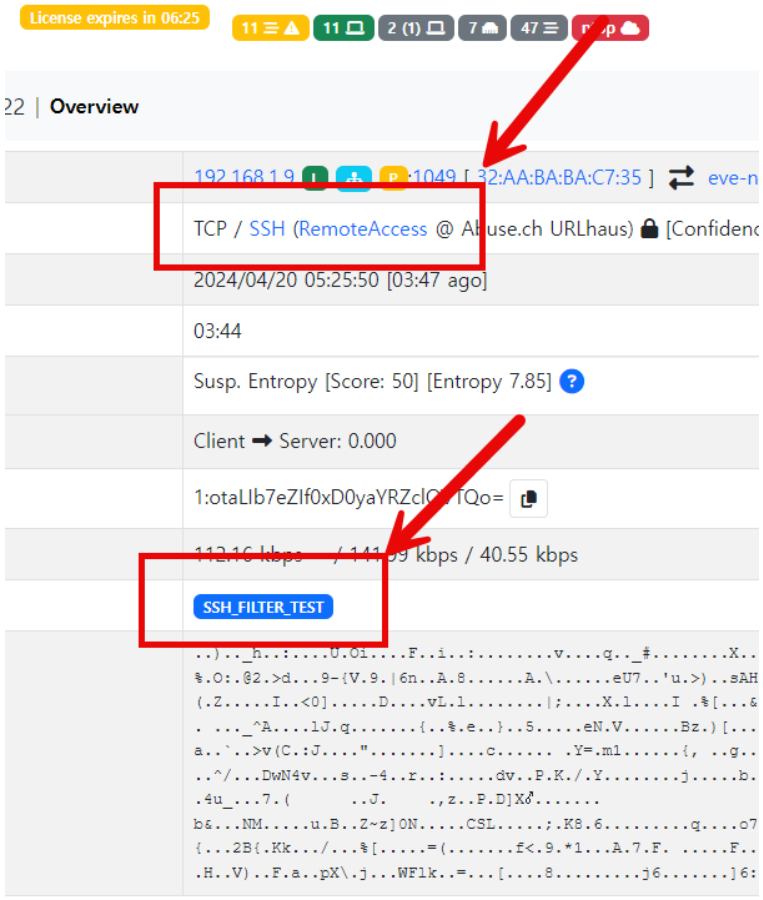
Profile Name	Traffic Filter (nBPF Format)
SSH_FILTER_TEST	ether host 00:0C:29:DF:EB:56 and host 32:AA:BA:BA:C7:35 and l7proto SSH
TCP_FILTER_TEST	ether host 00:0C:29:DF:EB:56 and host 32:AA:BA:BA:C7:35 and port (80 or 443)

```
> select * from "profile:traffic" where "ifid"='3' and "profile"='SSH_FILTER_TEST'
name: profile:traffic
time                bytes   ifid profile
----                -----   ---- -------
1713590760000000000 44138   3    SSH_FILTER_TEST
1713590820000000000 356770  3    SSH_FILTER_TEST
1713590880000000000 659996  3    SSH_FILTER_TEST
1713590940000000000 959302  3    SSH_FILTER_TEST
1713591000000000000 1263336 3    SSH_FILTER_TEST
1713591060000000000 1566142 3    SSH_FILTER_TEST
1713591120000000000 1871120 3    SSH_FILTER_TEST
1713591180000000000 2174520 3    SSH_FILTER_TEST
1713591240000000000 2476464 3    SSH_FILTER_TEST
1713591300000000000 2787450 3    SSH_FILTER_TEST
1713591420000000000 299938  3    SSH_FILTER_TEST
1713591480000000000 612736  3    SSH_FILTER_TEST
1713591540000000000 953898  3    SSH_FILTER_TEST
1713591600000000000 1256322 3    SSH_FILTER_TEST
1713591660000000000 1582394 3    SSH_FILTER_TEST
```

II nTopNG 기능소개

04. 그외 유용한 기능

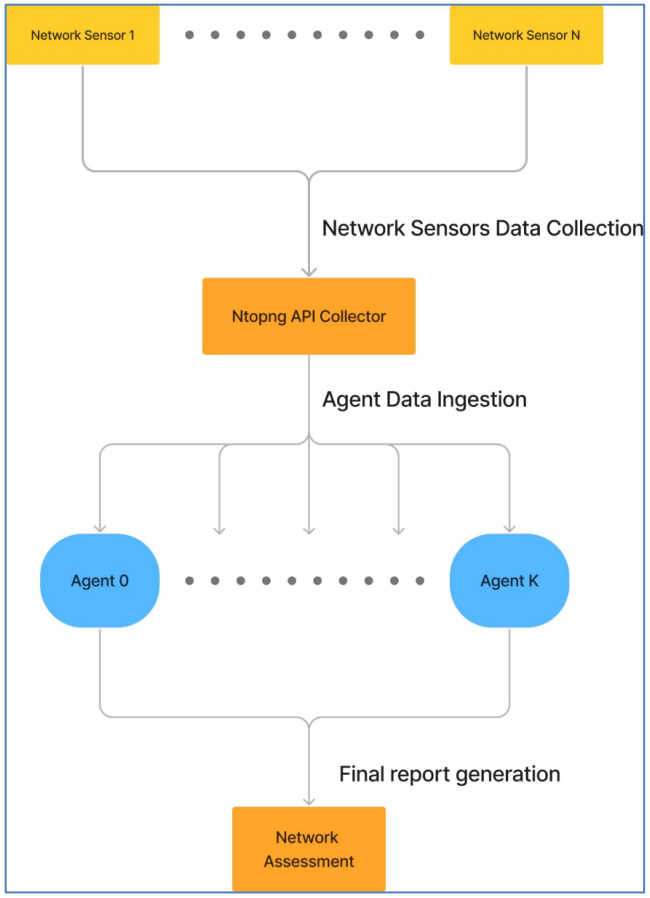
» nBPF 필터를 사용하여 원하는 트래픽을 추출하는 방법 소개
» 좌측 메뉴 SETTINGS -〉 TRAFFIC PROFILE에서 사용
» 필터 적용된 데이터는 DB에 저장되며 쿼리문 사용하여 데이터 추출 가능

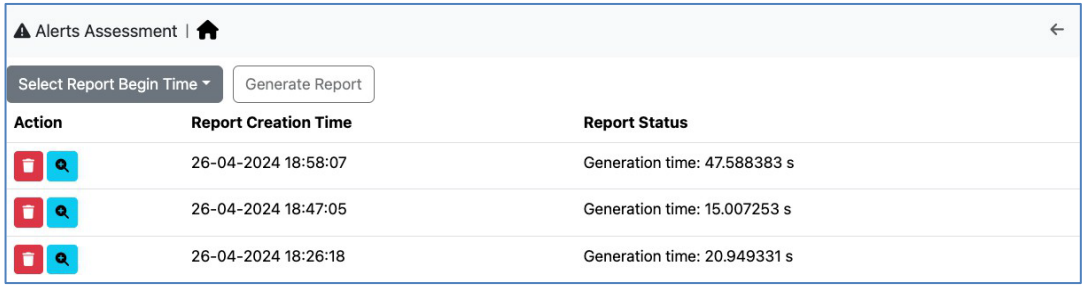


II nTopNG 기능소개

05. 향후 LLMs를 이용한 트래픽 분석

» OpenAI, Llama, Groq, Mistral, Mixtral 다양한 LLMs 분석접근방법으로 네트워크 취약점 분석
» 현재 Gabriel Deri 개발자에 의해서 개발중이며 향후 메뉴에 추가 예정
» 트래픽에서 발생한 주의깊은 공격, 취약점에 대한 보고서 제공 예정





II nTopNG 기능소개

05. 향후 LLMs를 이용한 트래픽 분석

» 엄청난 양의 로그 데이터를 사람이 일일히 읽지 않고 기계가 읽어서 문제점을 찾아줄수 있슴
» 다양한 학습 방법 (Fine Tuning) 기법에 의해서 분석 능력은 더 스마트 할수 있슴
» 악성파일 공격, DNS Attack 공격등 다양한 취약점 분석에 활용할수 있슴

Tier 3 Cybersecurity Analyst Report

Common Risk Grouping:

The provided IP addresses have been grouped based on common risk factors, indicating potential security threats to the network.

Group 1: Malware Distribution

- **Source IP Address: 185.5.211.33**
  - **Alert Content:** Transfer of file Portable Executable (PE32/PE32+) found
  - **Explanation:** The presence of PE32/PE32+ files indicates potential malware or exploitation risk. It poses a worst-case scenario where the files could be malware, potentially installing ransomware, keyloggers, or Trojans, compromising system security.
  - **Solution:** Block IP address, purge malwares, and remove suspicious files if accessible.
- **Source IP Address: 68.197.216.158**
  - **Alert Content:** Transfer of file Portable Executable (PE32/PE32+) found
  - **Explanation:** The repeated transfers (3 times) from this source IP address suggest suspicious behavior. The PE32/PE32+ files could be malware, posing a potential security threat to the network.
  - **Solution:** Block IP address, purge malwares, and remove suspicious files if accessible.

Group 2: Untrusted Host File Transfers

- **Source IP Address: 2.40.60.244**
  - **Alert Content:** Transfer of file www.extrasoftware.it/extraupdates/READMETERTEST/checkscript_rma.exe
  - **Explanation:** The file transfer from an untrusted host poses a potential vulnerability. The worst-case scenario involves ransomware infection, data encryption, and exfiltration of sensitive data to unauthorized parties.
  - **Solution:** Block IP address, purge malwares, and remove suspicious files if accessible.
- **Source IP Address: 93.145.252.50**
  - **Alert Content:** Transfer of file www.extrasoftware.it/extraupdates/READMETERTEST/checkscript_rma.exe
  - **Explanation:** The file transfer of an executable file (.exe) poses a potential security risk. In the worst-case scenario, it could lead to ransomware infection, compromising system security.
  - **Solution:** Block IP address, purge malwares, and remove suspicious files if accessible.

Recommendations:

1. Block the identified IP addresses to prevent further malicious activity.
2. Purge any malware or suspicious files from the affected systems.
3. Implement additional security measures to prevent future attacks.
4. Conduct a thorough investigation to determine the source and scope of the attacks.

Conclusion:

The provided IP addresses pose significant security risks to the network. It is crucial to take immediate action to mitigate these threats and prevent further attacks. DNS alerts are not present

CHAPTER III

데모 시연

데모 시연

제안사는 네트웍 관리시스템 전문회사로써 우수한 인력과 유사사업의
수행경험을 바탕으로 본 실시간 트래픽 분석시스템 구축사업을

FINISH

성공적으로 완수할 것임을 약속 드립니다.

1. Global No.1 제품의 검증된 시스템 도입을 통한 운영 안정성 확보
2. 고성능 장비 구축으로 서비스 속도 향상 및 서비스 확장성 확보
3. 유사 사업의 수행 경험을 통해 확보된 수행역량 활용