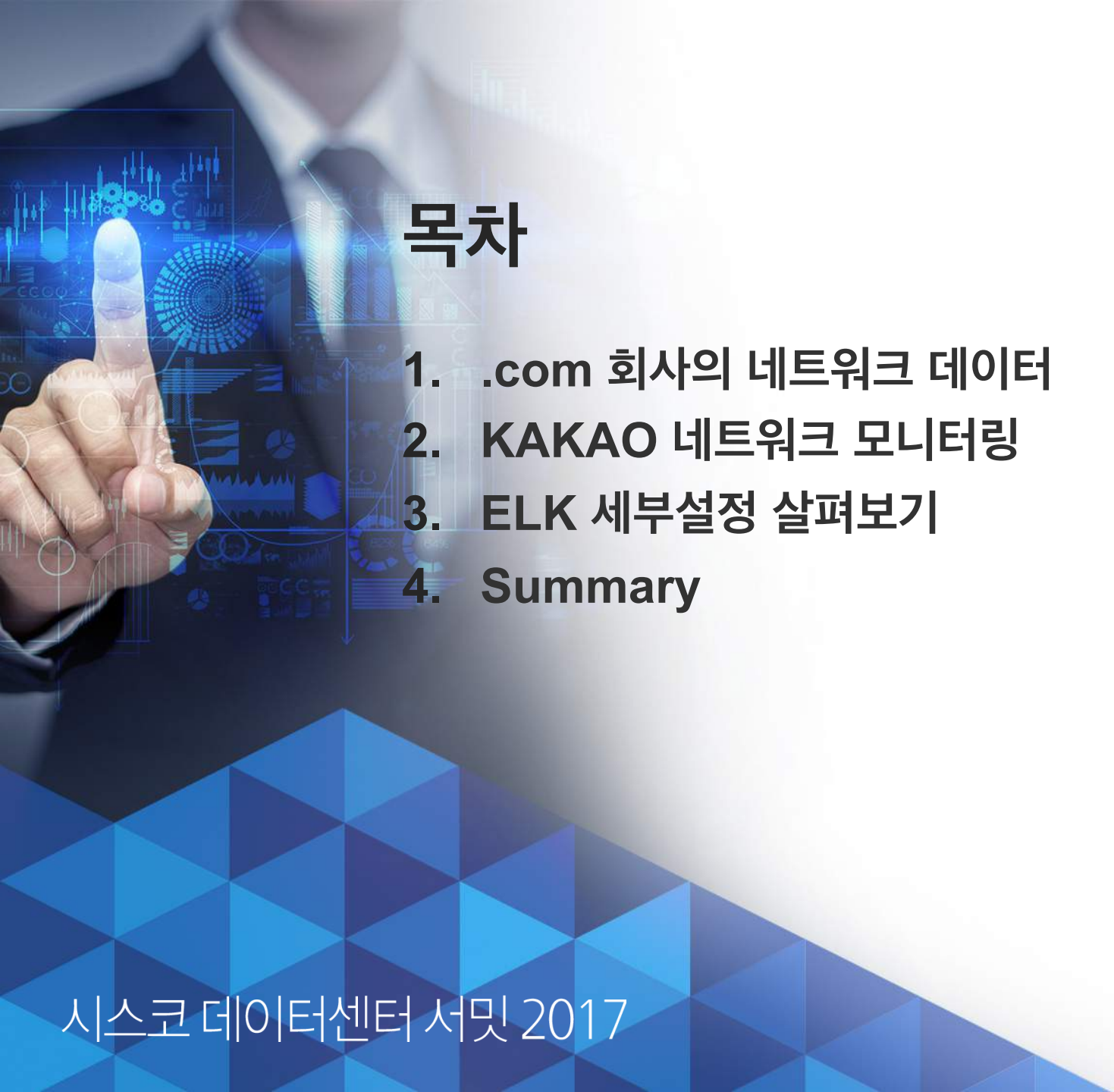
ELK를 활용한 데이터센터 네트워크 모니터링

서상덕 차장, KAKAO



목차

1. .com 회사의 네트워크 데이터
2. KAKAO 네트워크 모니터링
3. ELK 세부설정 살펴보기
4. Summary

.com 회사의 network data

- **사용자 중 NE 가 아닌 사람들이 더 많음**
  - 네트워크 장비 특정포트의 Traffic Statistics 류의 정보는 효용이 적다.
  - 네트워크 정보중 각 조직, 특정 정보를 원하는대로 조직화/식별 가능해야
  - 조직/서비스형태 등은 각각 다름

- **대부분의 상용 NMS는 개별 조직의 요구에 일치되지 않음**
- **Flexible UI를 넘어, API 제공을 요구 (automation / self-service 추세)**

→ 전용의 NMS 를 개발하되, 오픈소스를 최대한 활용하기로.. (custom code 최소화)

.com 회사의 network data

- **SNMP..**
  - 개발자도 다루기 쉽지않음
  - 아직은 REST API 를 지원하지 않는 장비가 많이 남아 있음
  - 오래되어 다른 tool 등과 api 를 통한 연동성이 없음

- **네트워크(팀) 정보는 가시성이 충분하지 않으며 개방되어 있지 않다**
  - NE 아닌 사람이 traceroute 등의 결과를 온전히 해독하기 어려움
  - 손실/병목등의 의심사항을 직접 조사할 수 없고, 단순 문의/응답에 의존

- **네트워크 운영자 조차도 트래픽에 대한 가시성이 충분하지 않다**
  - 서버군 (group) 에 대한 인터넷 트래픽 정보
  - 여러 관점에서의 인터넷/내부 트래픽 통계
  - 각각의 host 에 대한 traffic profile 등

ELK

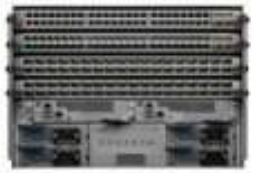
❖ Question:

- 특정 서버그룹의 내부(east-west)트래픽을 제외한 인터넷 트래픽의 양
- 전체트래픽 중 (dest|source) port 80 / 443 Traffic 의 비율
- 특정 transit 회선으로 (들어오는 | 나가는) 트래픽의 Top ASN 과 그 비율
- 각각의 회선별 TCP Flag (SYN | SYN-ACK | FIN | RST..) 비율 및 시간대별 추이
- (인터넷) x.x.x.x/yy 대역에서의 24시간 접근기록, 사용량 및 송수신 경로
- Server port-range 30000-40000 을 사용하는 서버의 목록

→ NMS 보다 검색엔진이 더 적합할 수 있음

ELK

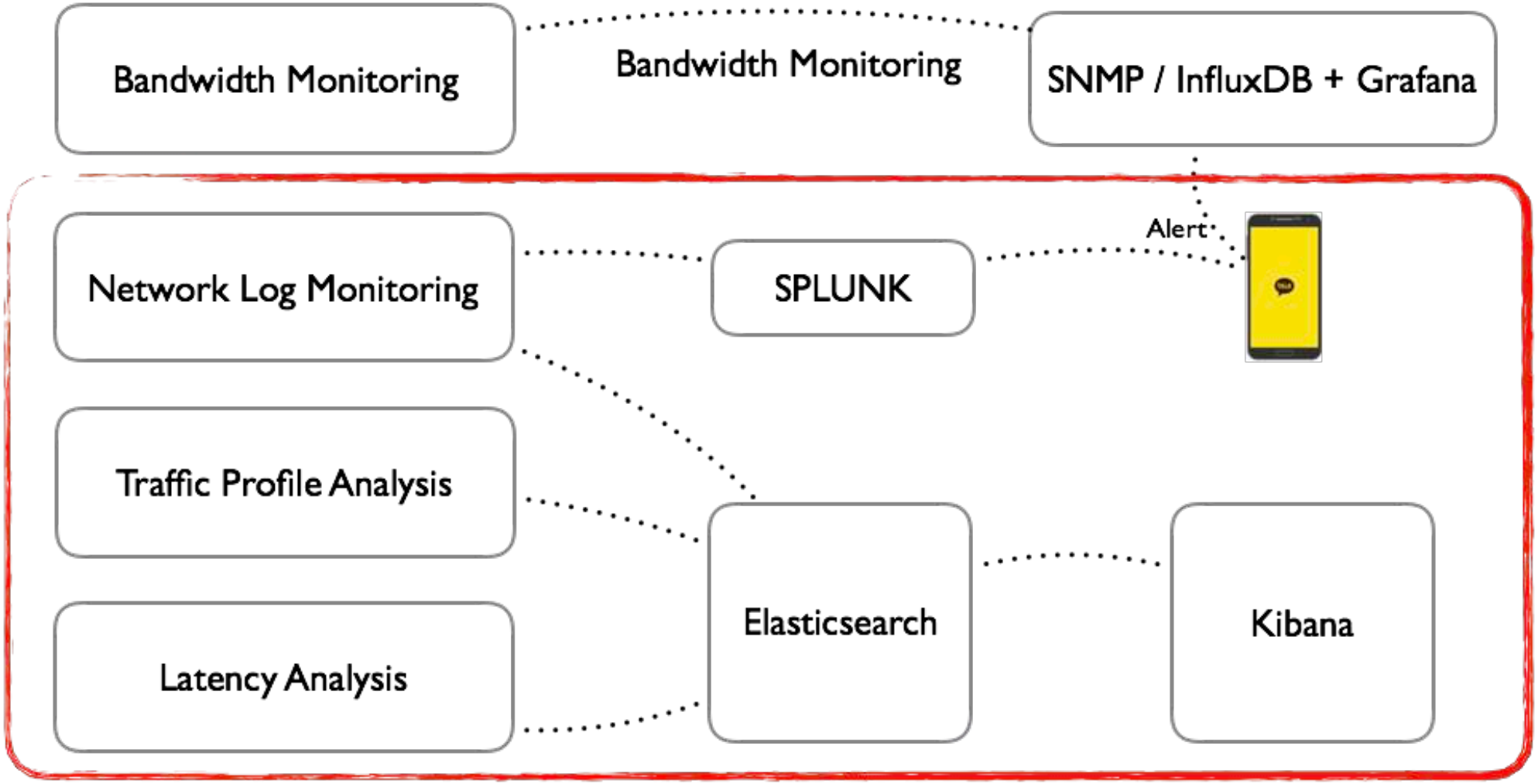
- (net|sflow) Decoder ← (netflow|sflow)



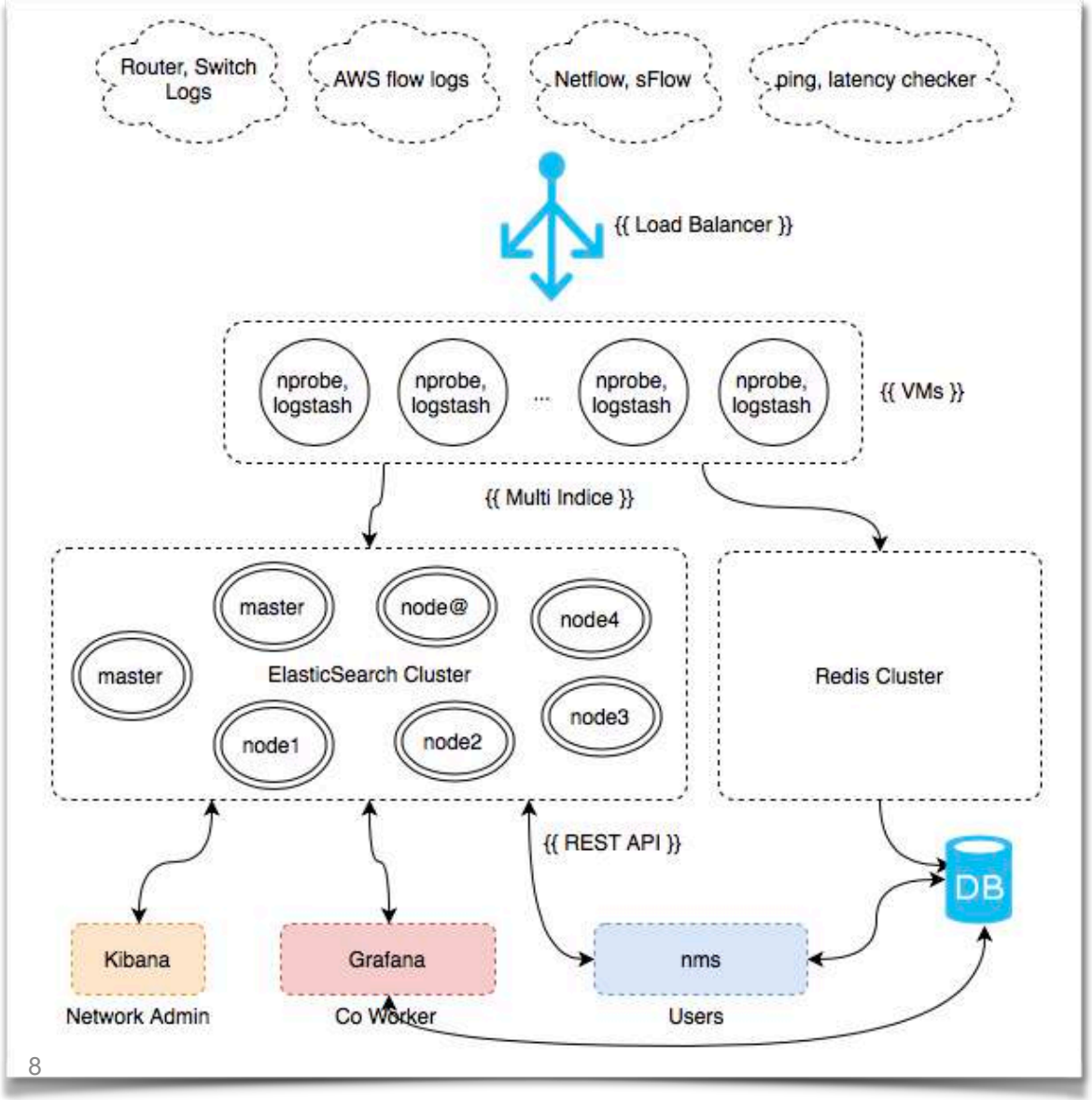
- Logstash : 데이터 수집기 (비정형데이터 -> 정형 데이터셋)
- Elasticsearch —> 검색엔진
- Kibana : User interface

https://www.elastic.co

KAKAO 네트워크 모니터링



KAKAO 네트워크 모니터링



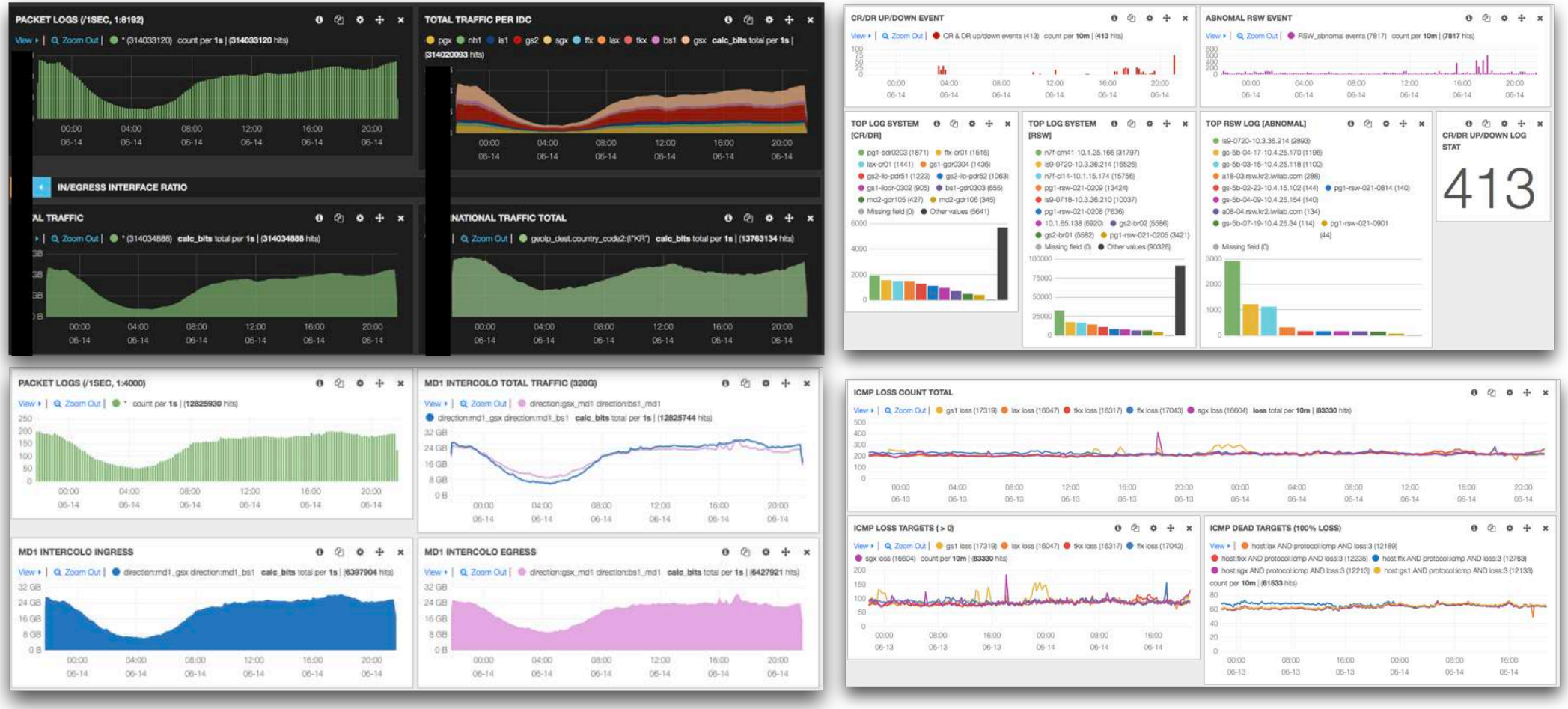
- 네트워크 장비 로그
- AWS flow-log
- Netflow, sFlow
- Ping, latency checker

--> 다양한 비정형 데이터들을 가공후 저장

- Redis 는 NMS 연동을 위해 사용
  - Data aggregation
  - 검색엔진 부하감소

- Kibana : Networ 운영자용
- Grafana : 다른 인프라팀 및 개발부서 제공용
- NMS : 기타 모든 사내 사용자

KAKAO 네트워크 모니터링



- Internet / East-West Traffic
- Network Syslog
- Global Latency

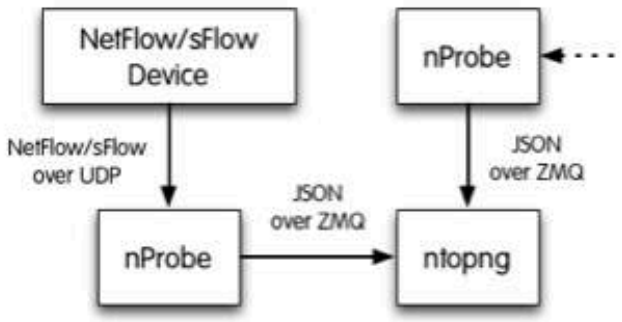
ELK 세부설정 살펴보기
(configuration & sample output)

시스코 데이터센터 서밋 2017

Nprobe – OSS netflow / sflow decoder

http://www.ntop.org

Nprobe – OSS netflow / sflow decoder



As explained in the ntopng README file, nProbe and ntopng must be started as follows:

1. Flow collection/generation (nProbe)
   `nprobe --zmq "tcp://*:5556" -i eth1 -n none` (probe mode)
   `nprobe --zmq "tcp://*:5556" -i none -n none --collector-port 2055` (sFlow/NetFlow collector mode)
2. Data Collector (ntopng)
   `ntopng -i tcp://127.0.0.1:5556`

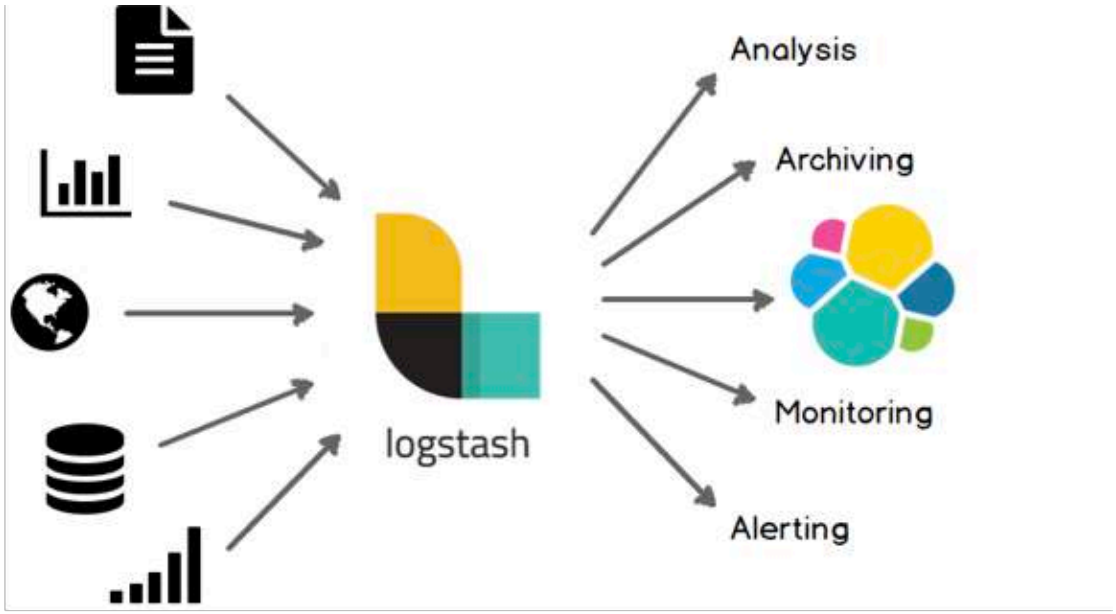
Sample Config

```
nprobe --zmq tcp://*:5556 -i none -n none --collector-port 2055 --tcp 127.0.0.1:5557 --json-labels -M 10000000000 -F 10
-T "%EXPORTER_IPV4_ADDRESS %IPV4_SRC_ADDR %IPV4_DST_ADDR %IPV4_NEXT_HOP %INPUT_SNMP
%OUTPUT_SNMP %IN_PKTS %IN_BYTES %FIRST_SWITCHED %LAST_SWITCHED %L4_SRC_PORT
%L4_DST_PORT %TCP_FLAGS %PROTOCOL %IP_PROTOCOL_VERSION" &
```

Netflow | Sflow 를 Decode 해서 ZMQ 에 적재

- http://www.ntop.org/ntopng/filling-the-pipe-exporting-ntopng-flows-to-logstash/
- http://www.ntop.org/nprobe/why-nprobejsonzmq-instead-of-native-sflownetflow-support-in-ntopng/

Logstash – data parse & transform



http://www.elastic.co

Logstash – default

```
input {
    tcp {
        port => "5557"
        codec => "json"
    }
}

filter {
    grok {}
    mutate {}
    gsub {}
    geoip {}
     …
}

output {
    stdout {}
}
```

configuration

Default output

```
{
    "130" => "2.252.10.10",
    "8" => "110.45.243.149",
    "12" => "112.214.102.118",
    "15" => "0.0.0.0",
    "10" => 18,
    "14" => 321,
    "2" => 8192,
    "1" => 12288000,
    "22" => 1497495476,
    … omitted
    "4" => 6,
    "5" => 0,
    "16" => 3786,
    "17" => 10036,
    "9" => 0,
    "13" => 0,
    "60" => 4,
    "42" => 4080,
    "@version" => "1",
    "@timestamp" => "2017-06-15T02:58:27.142Z",
    "host" => "127.0.0.1",
    "port" => 54256
}
```

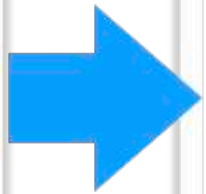
output

Logstash – filter & custom fields

```
filter {
        mutate {
                rename => [
                    "130", "router",
                      "8", "source",
                      "12", "dest",
                      "15", "nexthop",
                      "10", "input_snmp",
                      "14", "output_snmp",
                       … omitted
                      "28", "ipv6_dest",
                      "29", "ipv6_source_mask",
                      "30", "ipv6_dst_mask",
                      "62", "ipv6_nexthop",
                      "60", "ip_version"
                ]

                convert => [
                        "protocol", "string",
                        "other_message", "string"
                ]

                replace => [
                        "host", "gsx"
                         add_field => " …"
                ]
}
```



```
{
        "@version" => "1",
        "@timestamp" => "2017-06-15T03:11:44.626Z",
        "host" => "gsx",
        "port" => 54562,
        "router" => "2.252.10.10",
        "source" => "114.108.157.112",
        "dest" => "175.208.240.245",
        "nexthop" => "0.0.0.0",
        "input_snmp" => 74,
        … omitted
        "s_port" => 80,
        "d_port" => 8986,
        "other_message" => [
        [0] "ACK",
        [1] "TCP"
        ],
        "protocol" => "TCP",
        "src_tos" => 0,
        "source_as" => 3786,
        "dest_as" => 4766,
        "ipv4_src_mask" => 0,
        "ipv4_dst_mask" => 0,
        "total_flows_exp" => 642,
        "ip_version" => 4,
        "calc_bits" => 979763.2
}
```

Logstash – output

```
output {

        stdout {
                codec => rubydebug
        }

        elasticsearch {
                hosts => ["1.1.1.1","2.2.2.2","3.3.3.3","4.4.4.4","5.5.5.5"]
                index => "north-south-traffic-netflow-%{+YYYY.MM.dd}"
                workers => 4
                template_overwrite => "true"
                template => "/opt/logstash/vendor/…omitted./outputs/elasticsearch/dcflow-template.json"
        }

        redis {
                host => "test.redis.com"
                port => 31725
                password => "xxxx"
                data_type => "list"
                key => "flow-gsx-1"
        }

        … many others.
}
```

https://www.elastic.co/guide/en/logstash/current/output-plugins.html

Elastic search

```
search-master1:~$ cat /etc/elasticsearch/elasticsearch.yml
cluster.name: dcflow.test
node.name: "search-master1"
node.master: true
node.data: false
index.number_of_shards: 10
index.number_of_replicas: 1
path.data: /data1/es-data
bootstrap.mlockall: true

#total cluster
discovery.zen.ping.unicast.hosts: [“1.1.1.1”,“1.1.1.2”,“1.1.1.3”,“1.1.1.4”,“1.1.1.5” ,,,,,”x.x.x.x”]

http.cors.enabled: true
index.cache.field.type: soft
indices.fielddata.cache.size:  40%
network.bind_host: 0.0.0.0
```

https://www.elastic.co/guide/en/logstash/current/output-plugins.html

Kibana – flow

PACKET LOG

0 to 100 of 500 available for paging

@timestamp	source	dest	s_port	d_port	other_message	host	geoip_source.asn	geoip_dest.asn	geoip_source.number	geoip_dest.number	tags	nexthop_asn
2017-06-24T14:08:02.267+09:00	203.133.166.61	223.33.165.94	80	55394	ACK,TCP	pgx	Kakao Corp	SK Telecom	AS9764	AS9644	egress	skt
2017-06-24T14:08:02.267+09:00	210.103.249.198	203.184.56.237	30314	18814	0,UDP	sgx	Kakao Corp	CallPlus Services Limit...	AS45991	AS9790	egress	ix
2017-06-24T14:08:02.266+09:00	210.103.249.197	111.125.109.210	28074	18898	0,UDP	sgx	Kakao Corp	Converge ICT Solutions ...	AS45991	AS17639	egress	ix
2017-06-24T14:08:02.266+09:00	203.133.166.61	223.62.222.93	80	53546	ACK,TCP	pgx	Kakao Corp	SK Telecom	AS9764	AS9644	egress	skt
2017-06-24T14:08:02.265+09:00	210.103.249.197	87.200.50.51	29846	16018	0,UDP	sgx	Kakao Corp	Emirates Integrated Tel...	AS45991	AS15802	egress	ix
2017-06-24T14:08:02.264+09:00	210.103.249.196	116.12.89.221	34888	16844	0,UDP	sgx	Kakao Corp	Lanka Communication Ser...	AS45991	AS5087	egress	ix
2017-06-24T14:08:02.264+09:00	210.103.249.197	116.87.217.18	28778	17634	0,UDP	sgx	Kakao Corp	Starhub Internet Pte Lt...	AS45991	AS55430	egress	sggs
2017-06-24T14:08:02.263+09:00	210.103.249.196	171.6.157.172	33074	15404	0,UDP	sgx	Kakao Corp	Triple T Internet/Tripl...	AS45991	AS45758	egress	ix

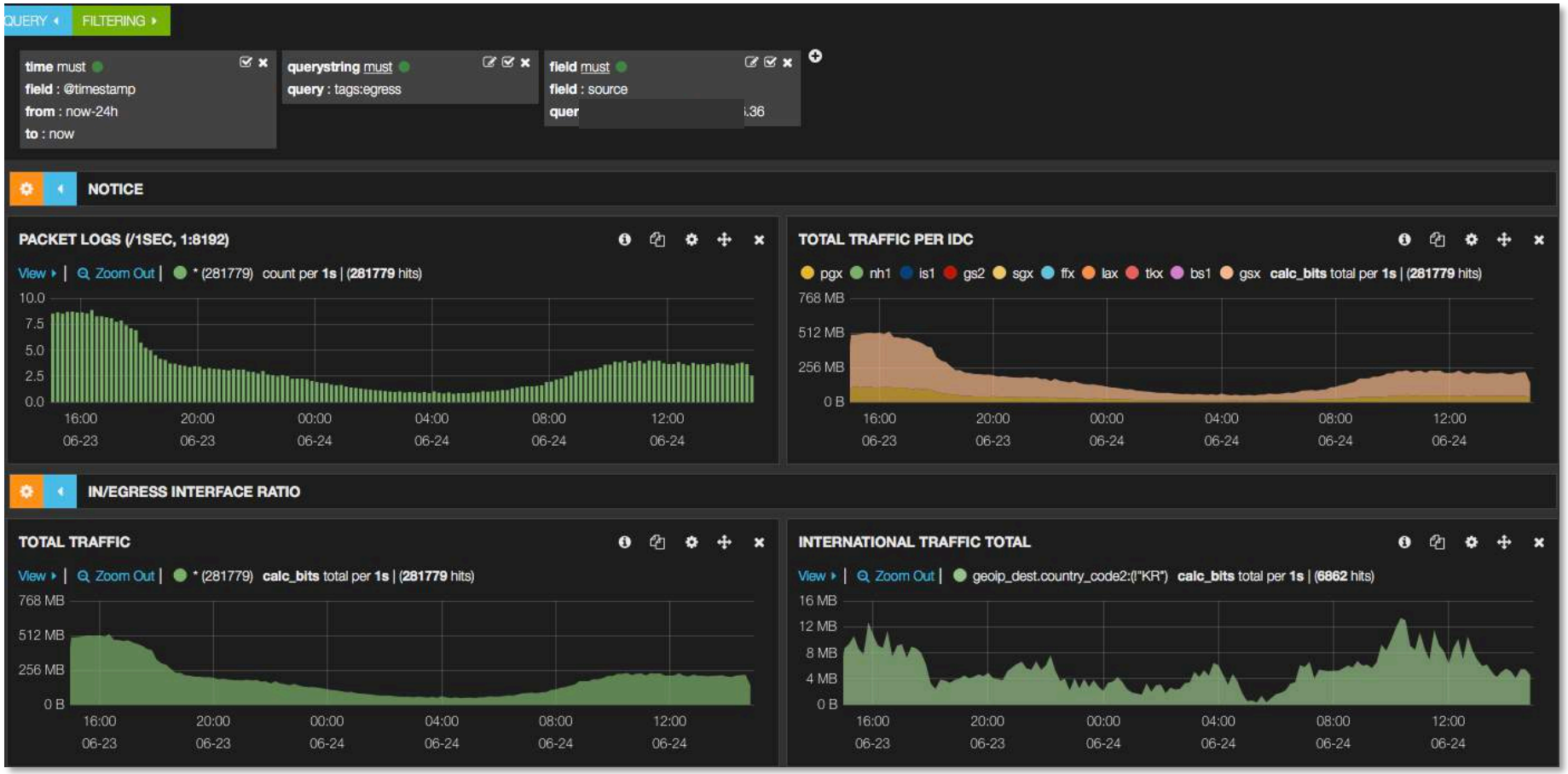
1 packet → 1 line (document)

Kibana - flow

Field	Action	Value
@timestamp		2017-06-24T05:21:10.425Z
@version		1
_id		AVzYi_fPlw_UrWd0zX6s
_index		dcflow-2017.06.24
_type		logs
calc_bits		90368000
calc_bits_10m		150613
calc_bits_1m		1506133
calc_bits_5m		301226
d_port		54078
dest		223.62.169.110
first_switched		1498281599
geoip_dest.asn		SK Telecom
geoip_dest.country_code2		KR
geoip_dest.country_name		Korea, Republic of
geoip_dest.ip		223.62.169.110
geoip_dest.number		AS9644
geoip_source.asn		Kakao Corp
geoip_source.country_code2		KR
geoip_source.country_name		Korea, Republic of
geoip_source.ip		211.231.104.249
geoip_source.number		AS38099

- Custom fields
  - ingress, egress,
  - Nexthop_asn, Input_asn
- Netflow fields
- Geoip fields

Kibana – flow (bandwidth)

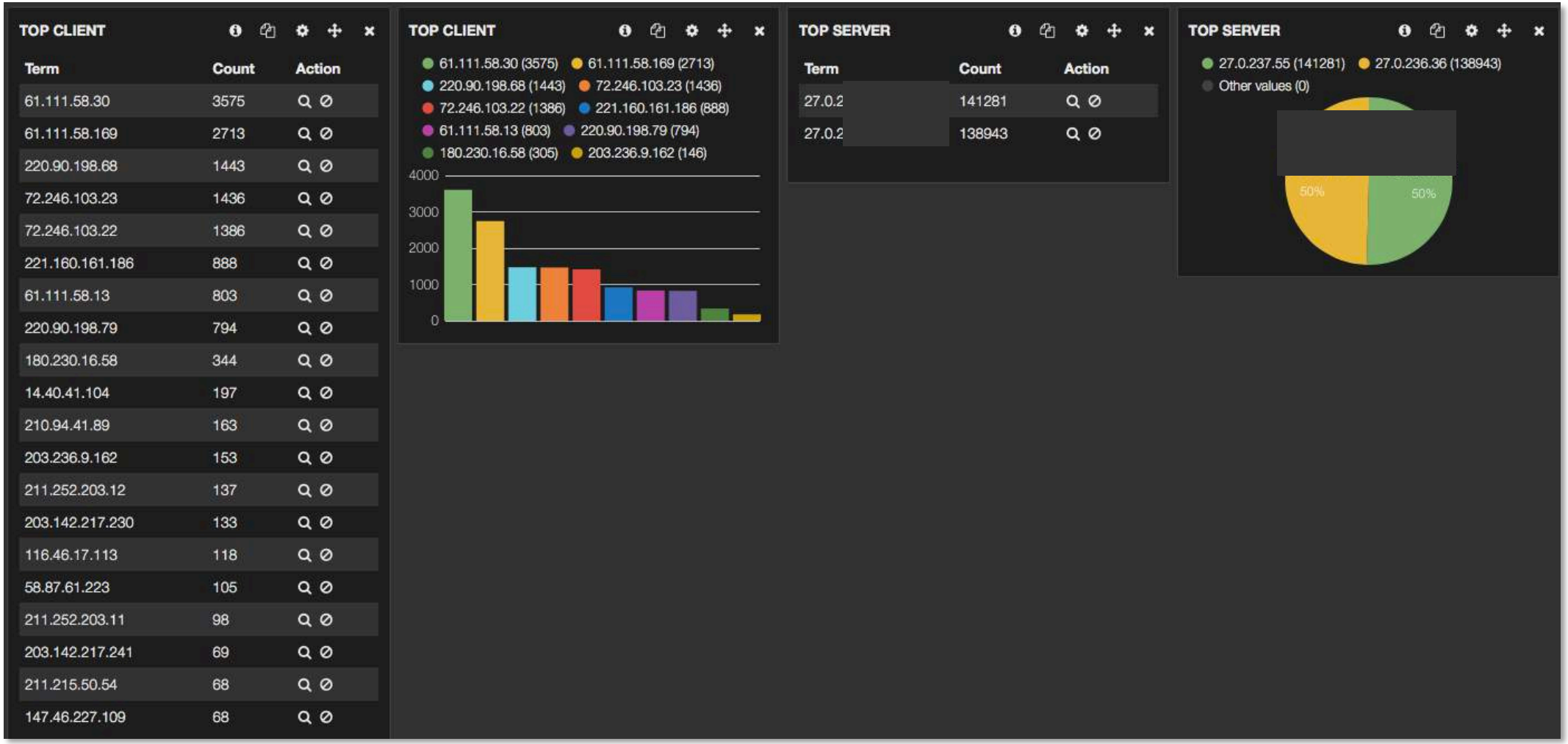


- Query: *
- Filter: source:x.x.x.x OR source:y.y.y.y

Kibana – flow (packet flag)

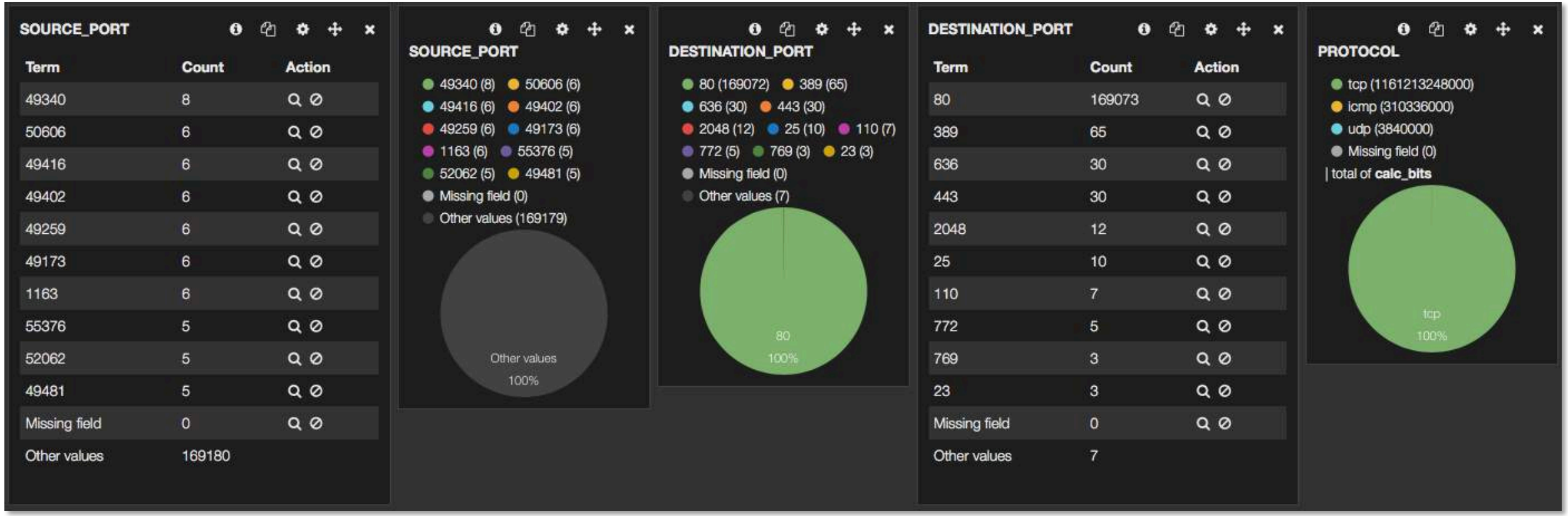
- Packet 분석이 필요한 업무 90% 이상 감소
- QoS 변화를 추정가능
- **효과적인 DDoS 등의 모니터링**

Kibana – flow (top talker)



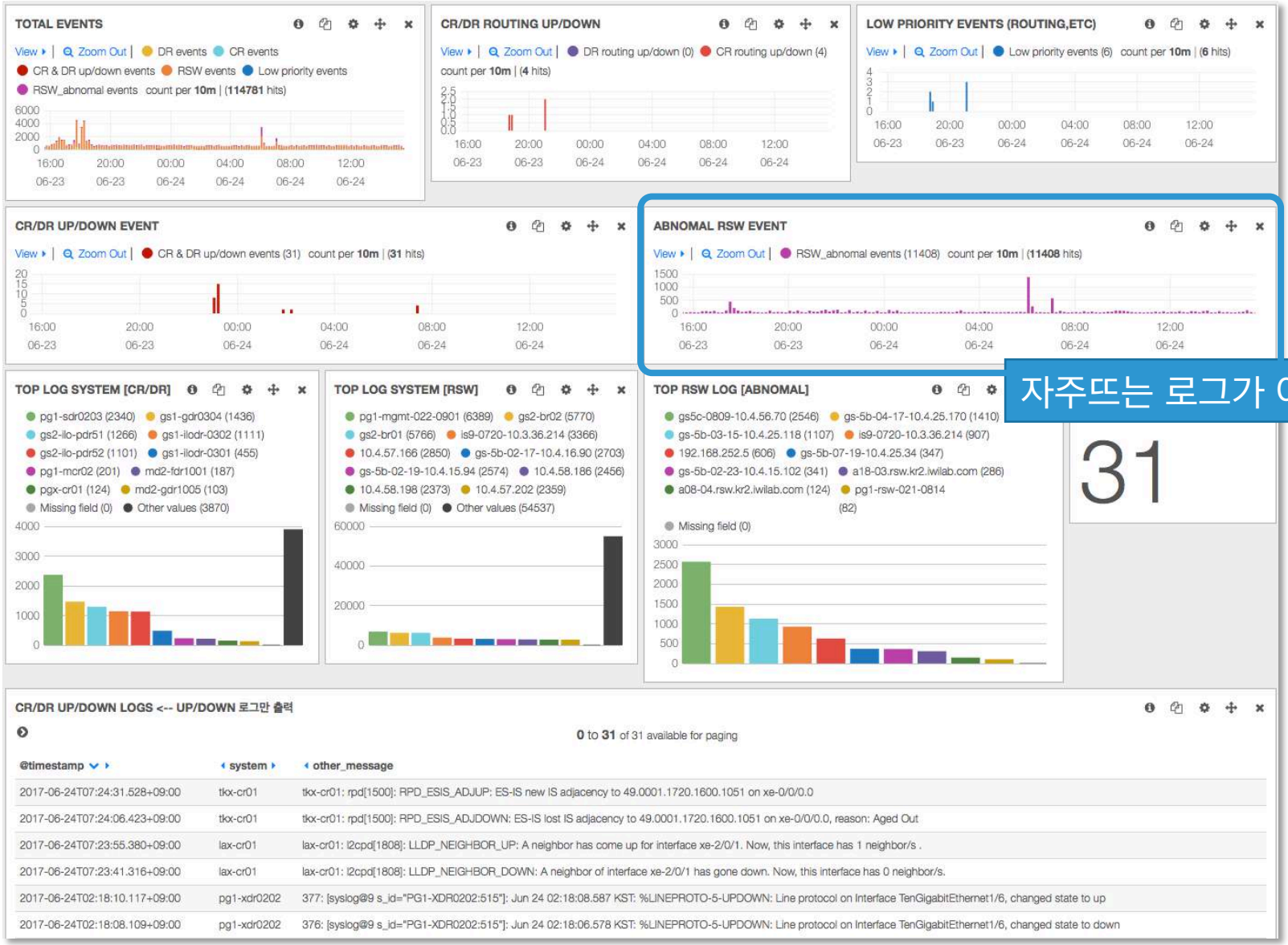
- Query: *
- Filter: (x.x.x.xOR y.y.y.y) AND (tags:ingress)

Kibana – flow (top port)



- Query: *
- Filter: x.x.x.x OR y.y.y.y

Kibana – network log analysis



자주뜨는 로그가 아닌 다른 특이한 로그만

31

Kibana – global latency analysis

개별 Pop / Transit line 품질차이를 분석

Summary

- ✓ **ELK 는?**
  - Netflow, sFlow 분석에 좋은 대안이 될 수 있음
  - Log, Latency, LLDP 등 각종 비정형 데이터에 적용가능
  - 상용 NMS 보다 더 자유로운 질의가 가능
  - 저장된 모든 data 는 REST API 를 통해 다른 프로그램과 연동
  - 수많은 관련 개발작업 감소

- ✓ **각종 비정형네트워크 데이터들을 손쉽게 통합**
- ✓ **네트워크 운용에 폭넓은 시너지를 제공**
- ✓ **최근에는 다양한 네트워크 OSS, 벤더들이 관련한 언급을 시작**

THANK YOU

시스코 데이터센터 서밋 2017