

# REDCAYLE Estado Actual

Grupos de Trabajo de RedIRIS



RedIRIS

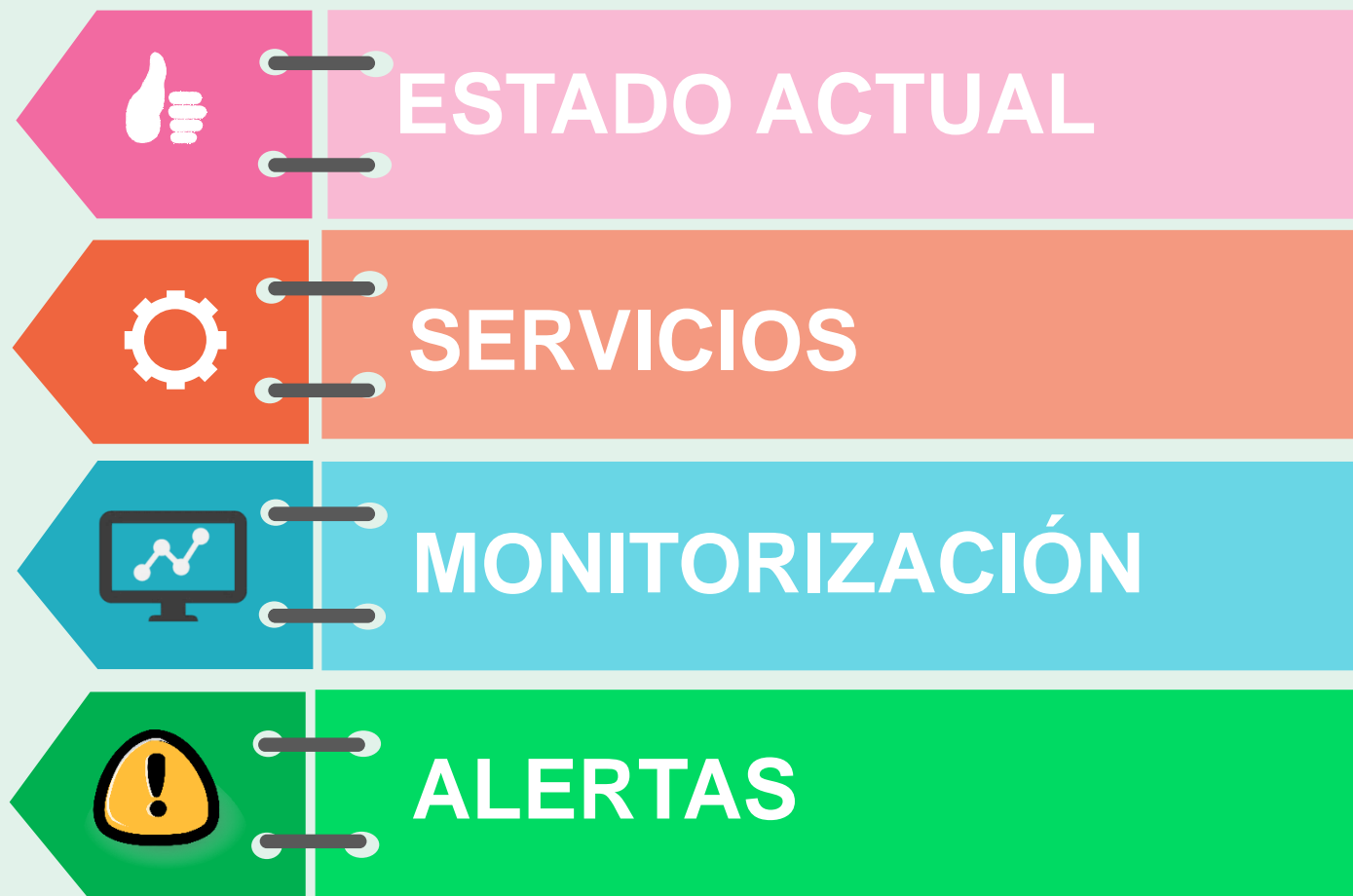
Mariví López López

28 Noviembre 2019

Universidad de Valladolid



# Contenido





# ESTADO ACTUAL

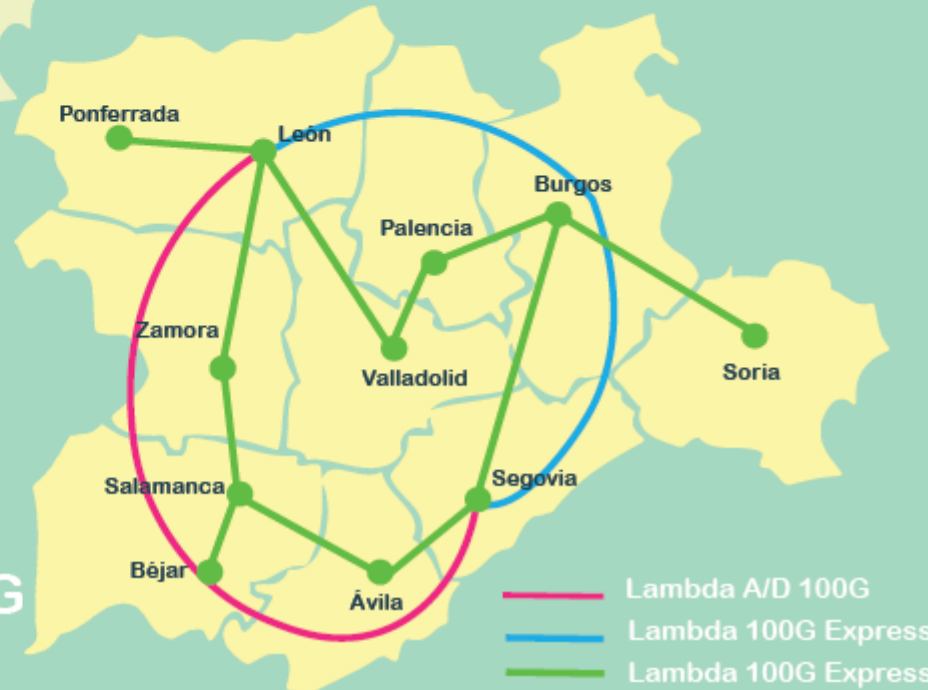
# RED CAYLE

RED DE CIENCIA Y TECNOLOGÍA  
CASTILLA Y LEÓN

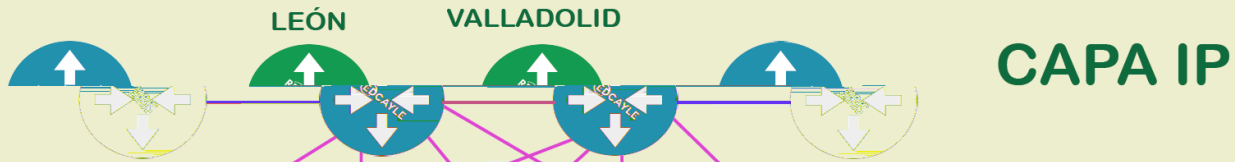


HUELLA DE FIBRA  
DE 1233KM

CAPACIDAD  
ÓPTICA 200G



# ESTADO ACTUAL



CAPA IP



CAPA ÓPTICA



PONFERRADA

BÉJAR

ÁVILA

ZAMORA

SORIA

SEGOVIA

PALENCIA



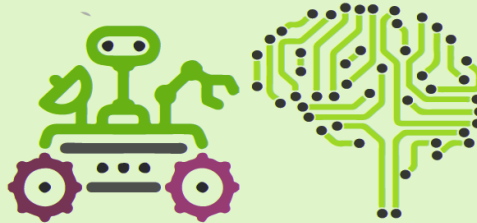
Centros Educativos



Hospitales Universitarios



Infraestructuras Científicas



Centros Tecnológicos  
Parques Científicos

2018 – 2019

ENTIDADES MIGRADAS 20  
AMPLIACION Equipos 120K

Fibra Urbana Hospital Univ. León  
**CEDER → Último centro conectado!!**

2020 en adelante

ENTIDADES adicionales con  
posibilidad de conectar 13

Ampliación de capilaridad urbana









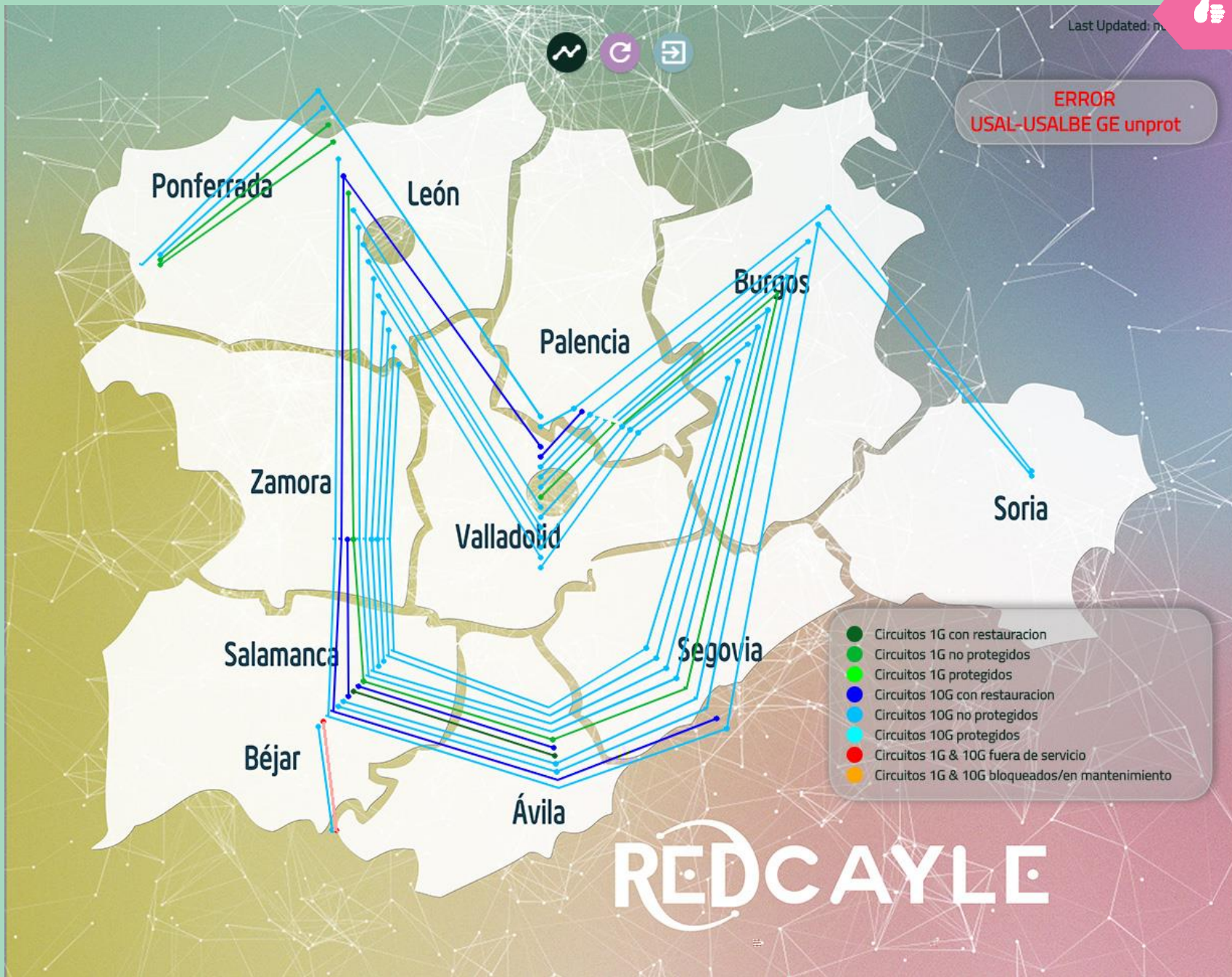


# ESTADO ACTUAL

Last Updated: n



**ERROR**  
USAL-USALBE GE unprot



- Circuitos 1G con restauracion
- Circuitos 1G no protegidos
- Circuitos 1G protegidos
- Circuitos 10G con restauracion
- Circuitos 10G no protegidos
- Circuitos 10G protegidos
- Circuitos 1G & 10G fuera de servicio
- Circuitos 1G & 10G bloqueados/en mantenimiento

# REDCAYLE



## SERVICIOS Adicionales

### Servidores de HORA



**tic.redcayle.es**

185.179.104.7

Stratum 1 con fuente GPS

**tac.redcayle.es**

185.179.104.12

Stratum 1 con fuente GPS

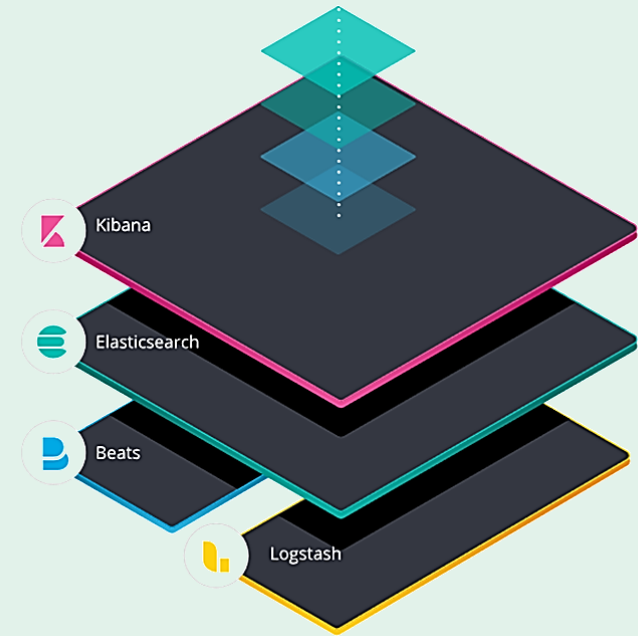
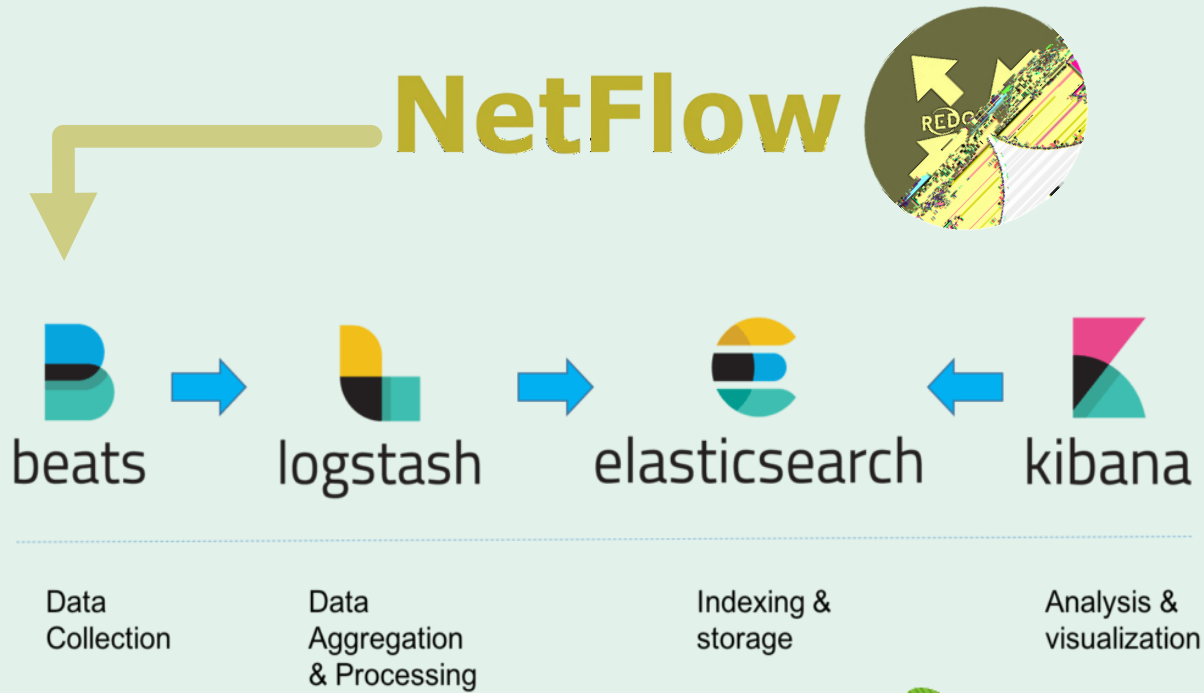


**IPERF** (previa solicitud al NOC)





# MONITORIZACIÓN



**Nagios**<sup>®</sup>

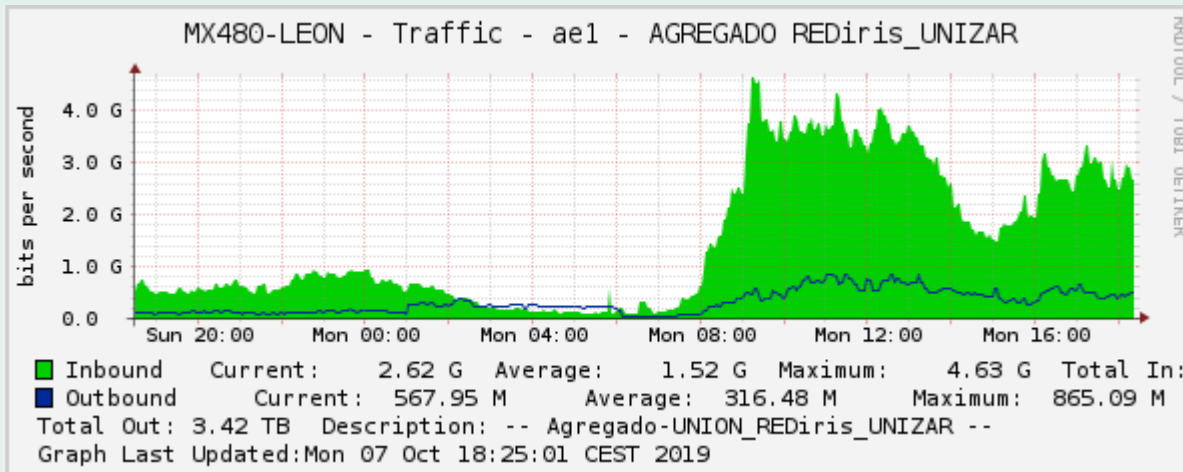


**graylog**

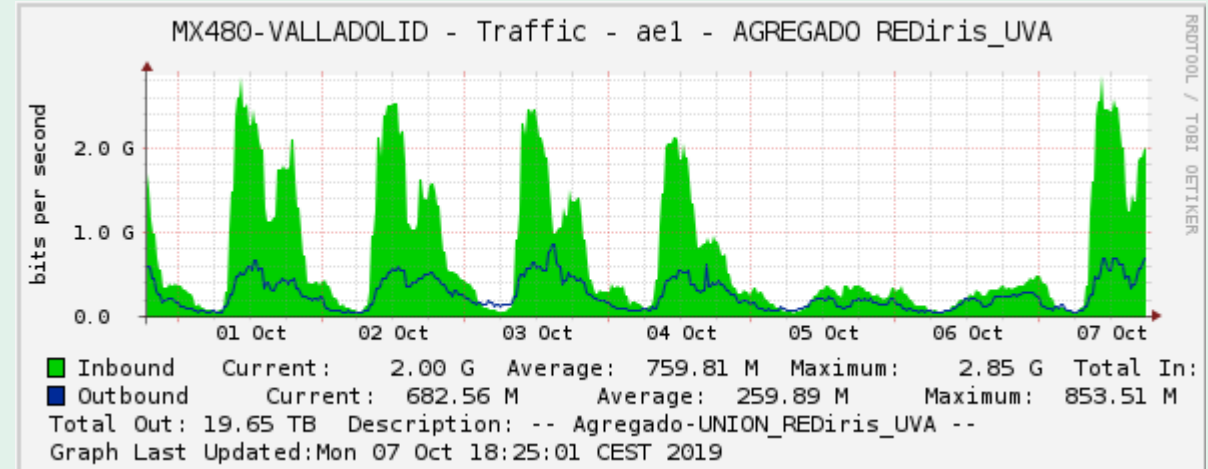
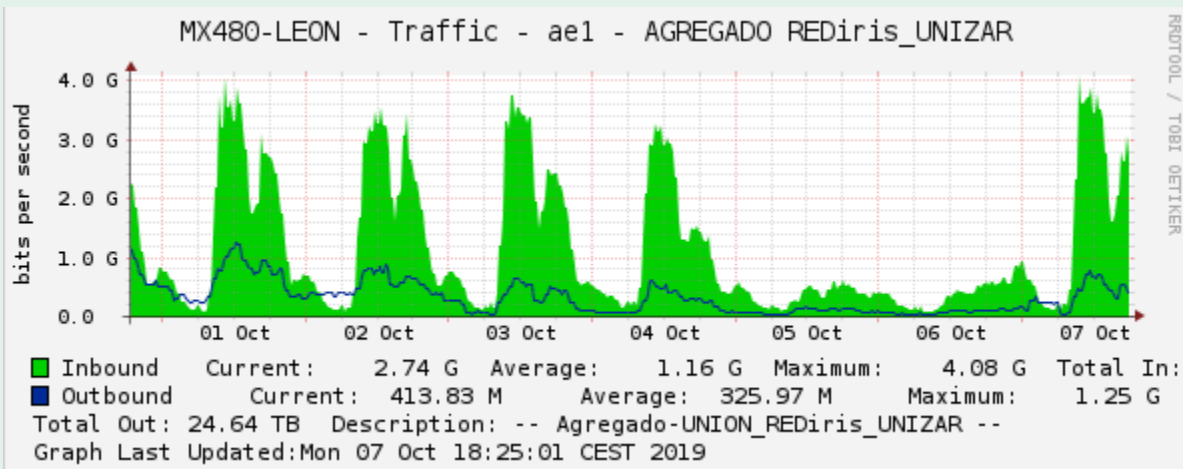
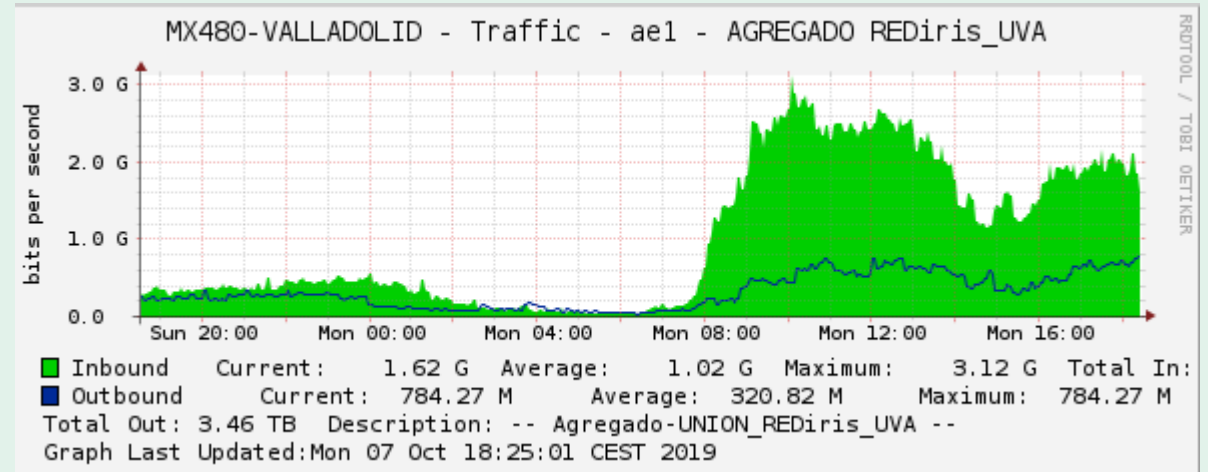


# Monitorización - Cacti

## Router LEON Tráfico Agregado con REDIRIS



## Router VALLADOLID Tráfico Agregado con REDIRIS

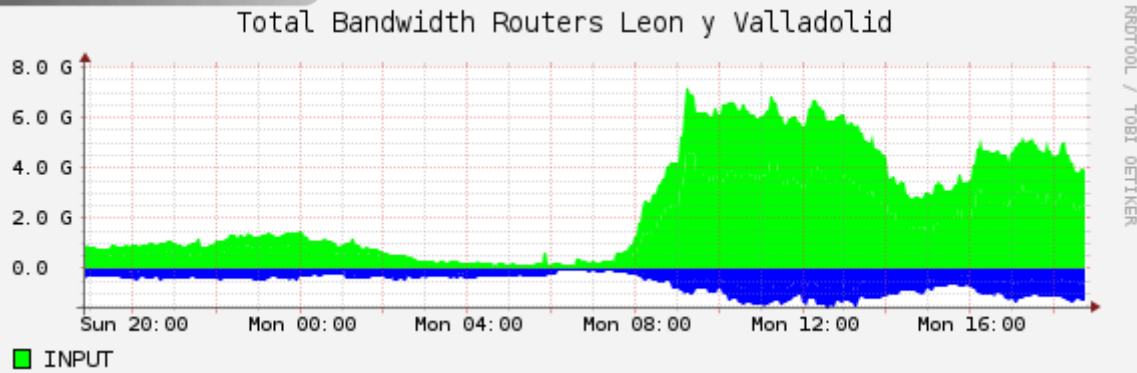




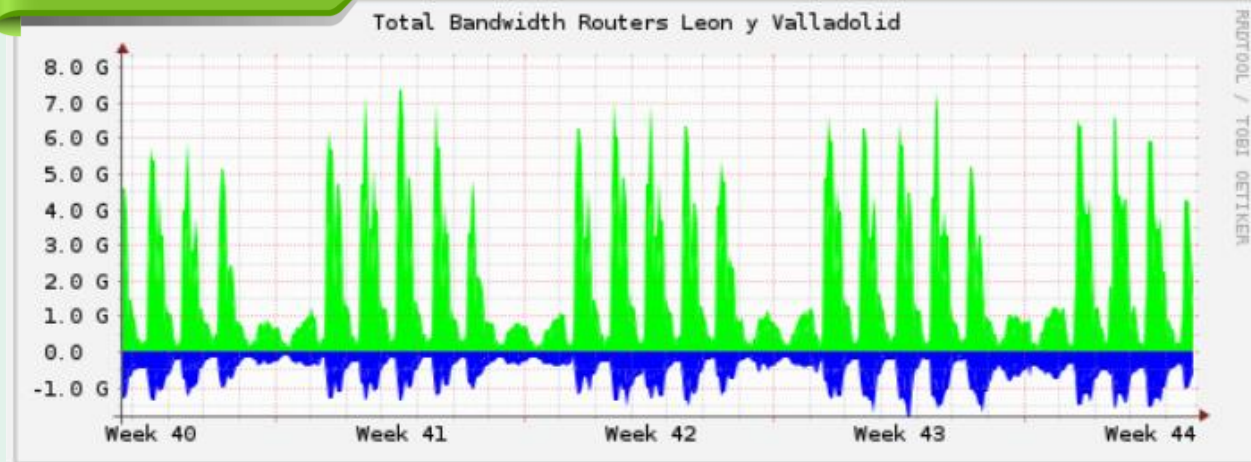
# Monitorización - Cacti

## Día

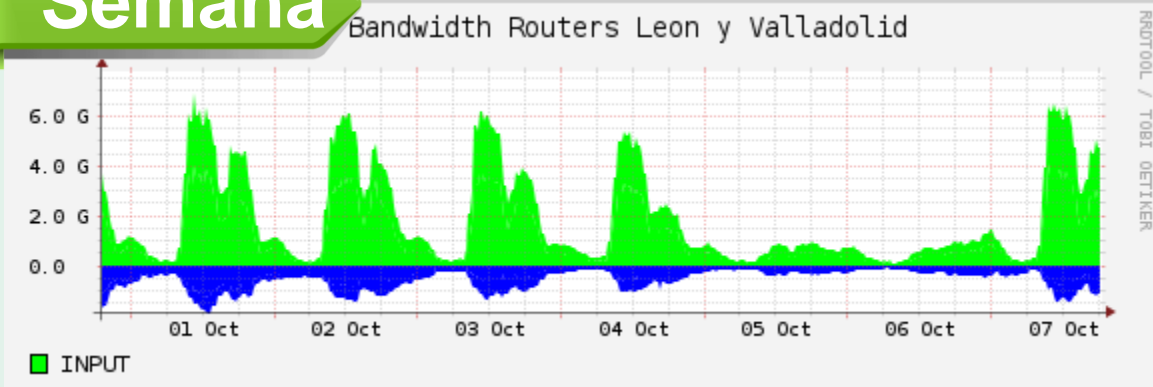
### Tráfico Intercambio IP con REDIRIS



## Mes



## Semana



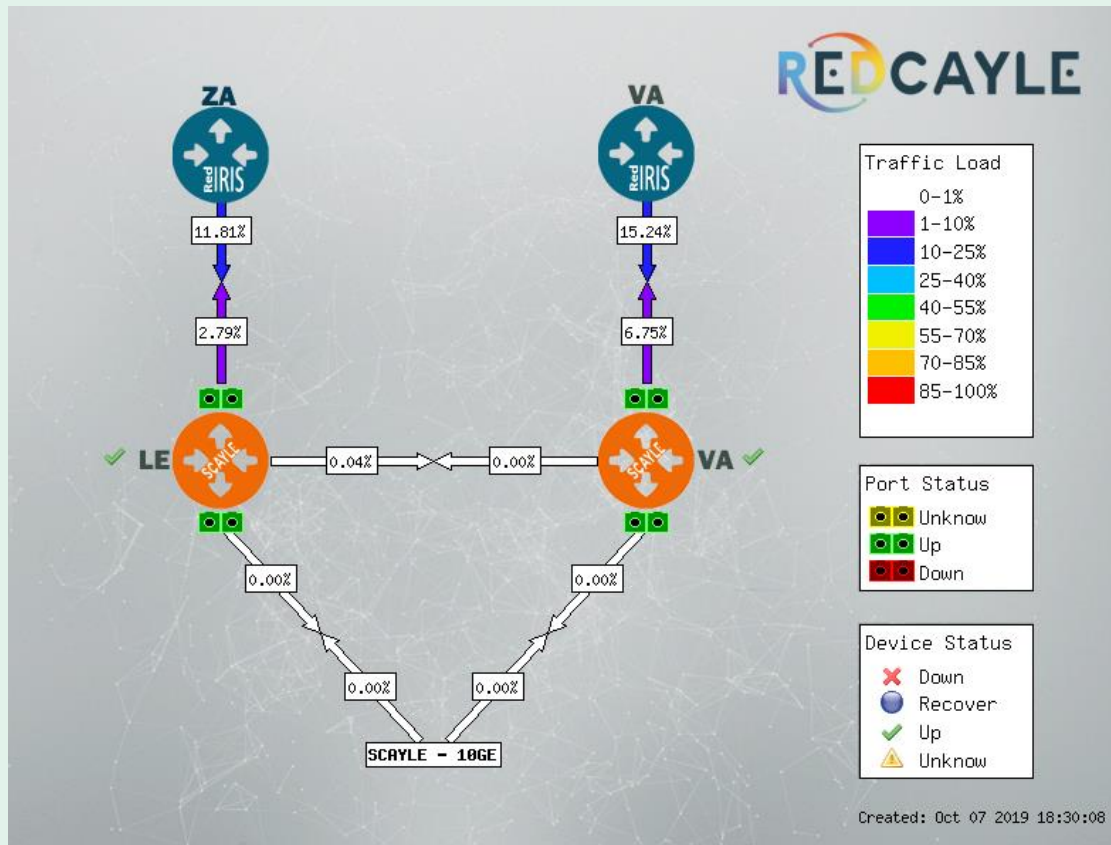
Octubre 677TB

Octubre 205 TB

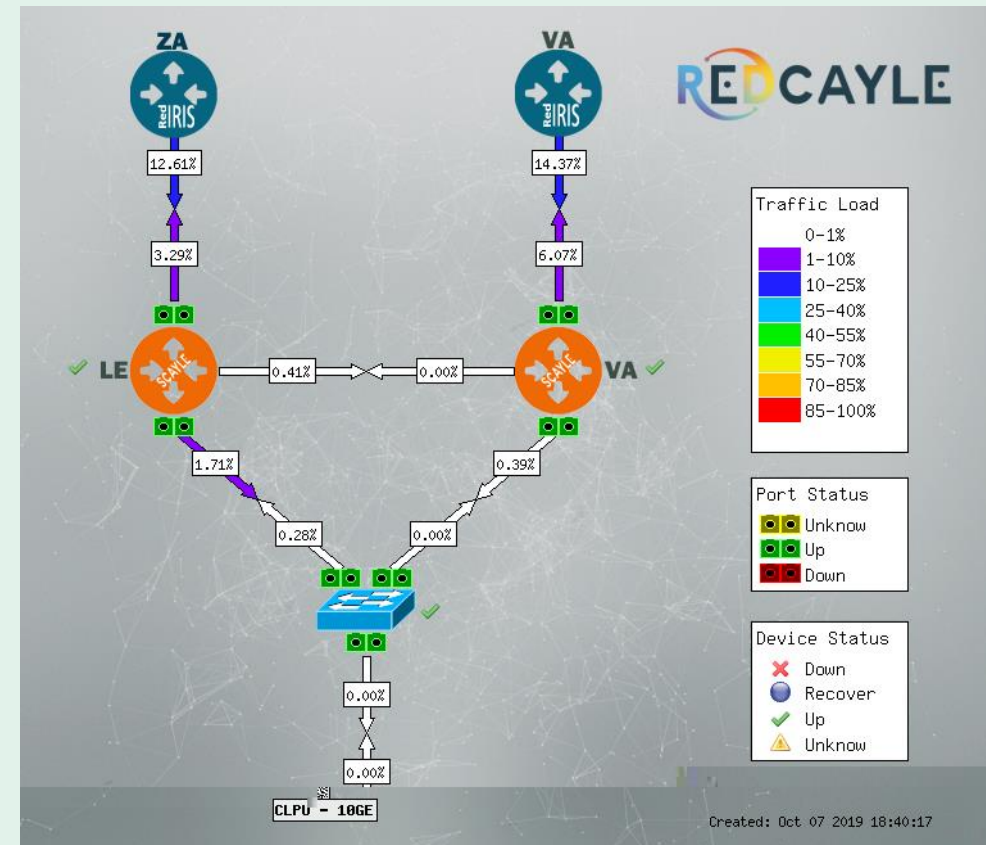


# Monitorización - Weathermap

## TIPO A



## TIPO B

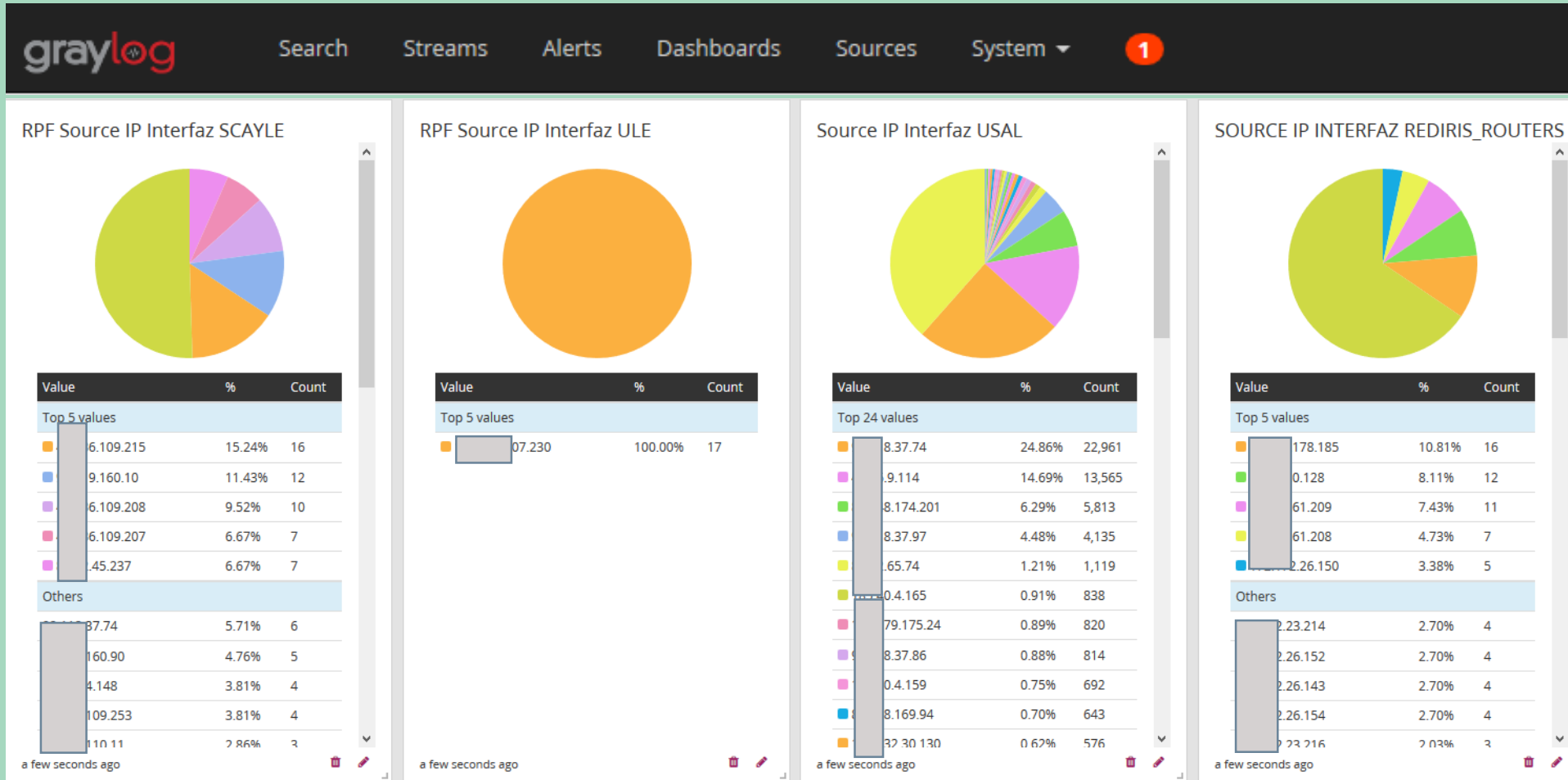






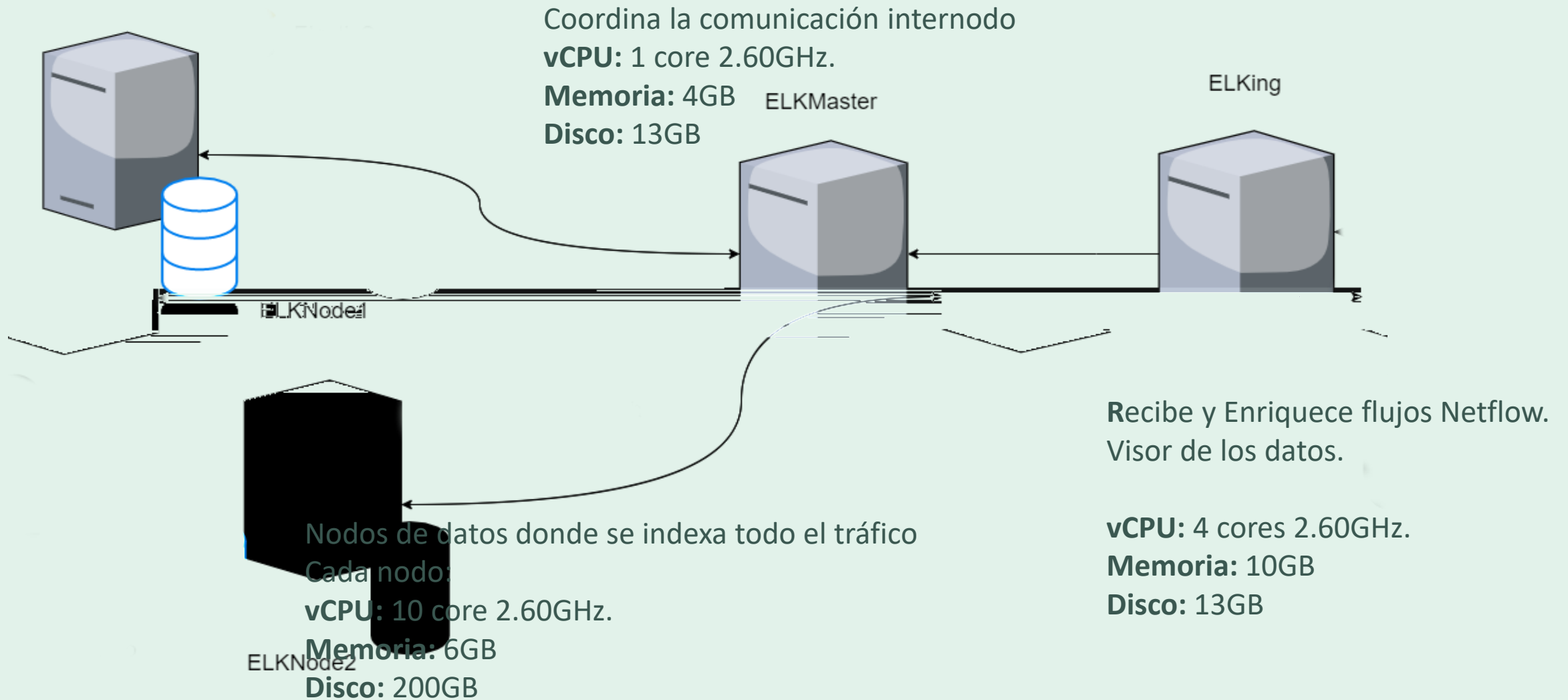
# Monitorización - Graylog

## EJEMPLO: UNICAST Reverse Path Forwarding (MANRS)





# Monitorización - ELK Stack





# Monitorización - ELK Stack

Elastic Sack Cluster SCAYLE

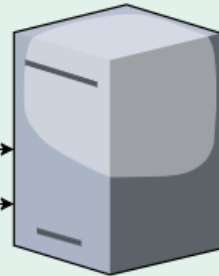


ELKNode1

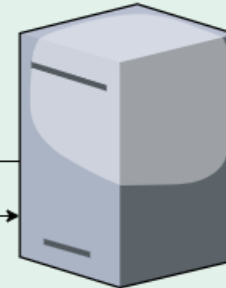


ELKNode2

ELKMaster



ELKing



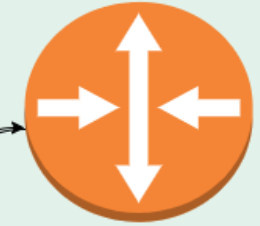
Plugins

**ElastiFlow:** Dashboards y gráficos mejorados para Kibana.

**SearchGuard:** Autenticación/Autorización para Kibana.

Cifrado de comunicaciones entre los nodos.

**Cerebro:** Monitorización Cluster Elastic Stack



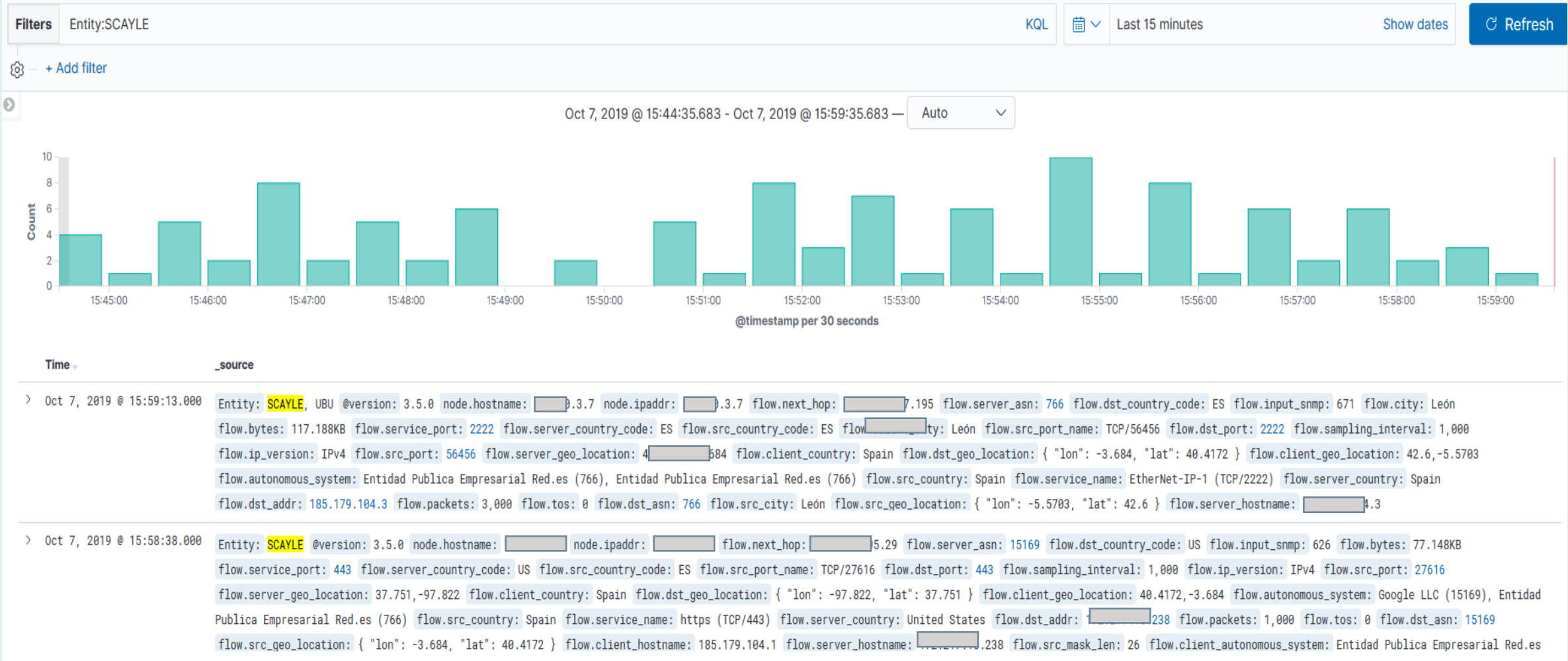
Netflow



Search Guard



# Monitorización - ELK Stack







# Monitorización - ELK Stack

Dashboard / **ElastiFlow: Overview** admin

Filters  Lucene Last 15 minutes Show dates Refresh

+ Add filter

Overview | Top-N | Threats | Flows | Geo IP | AS Traffic | Exporters | Traffic Details | Flow Records

Flow Exporter: Select... Client: Select... Server: Select... Service: Select...

**Servers and Clients (bytes)**

- 31.13.83.52
- 130.206.193.110
- 93.184.221.240
- 130.206.193.109
- 130.206.193.108
- 130.206.193.111
- 216.58.201.170
- 130.206.192.10
- 17.253.37.205
- 130.206.192.23
- 130.206.192.24
- 211.22.51

**Services (bytes)**

- https (TCP/443)
- http (TCP/80)
- https (UDP/443)
- ssh (TCP/22)
- imaps (TCP/993)
- rsync (TCP/873)
- smtp-tls (TCP/587)
- UDP/33484
- TCP/43412
- TCP/51904
- smtp (TCP/25)
- UDP/41151

**TCP Flag - Count**

ACK, SYN, PSH, ECE, FIN, RST, CWR

**Autonomous Systems (bytes)**

- Entidad Publica Em...
- Google LLC (15169)
- Facebook, Inc. (32...
- Apple Inc. (6185)
- Junta de Castilla y ...
- Netflix Streaming S...
- Akamai Technologi...
- MCI Communicatio...
- Level 3 Parent, LLC...
- Akamai Internation...
- Amazon.com, Inc. (...)
- Microsoft Corporat...

**IP Versions and Protocols (bytes)**

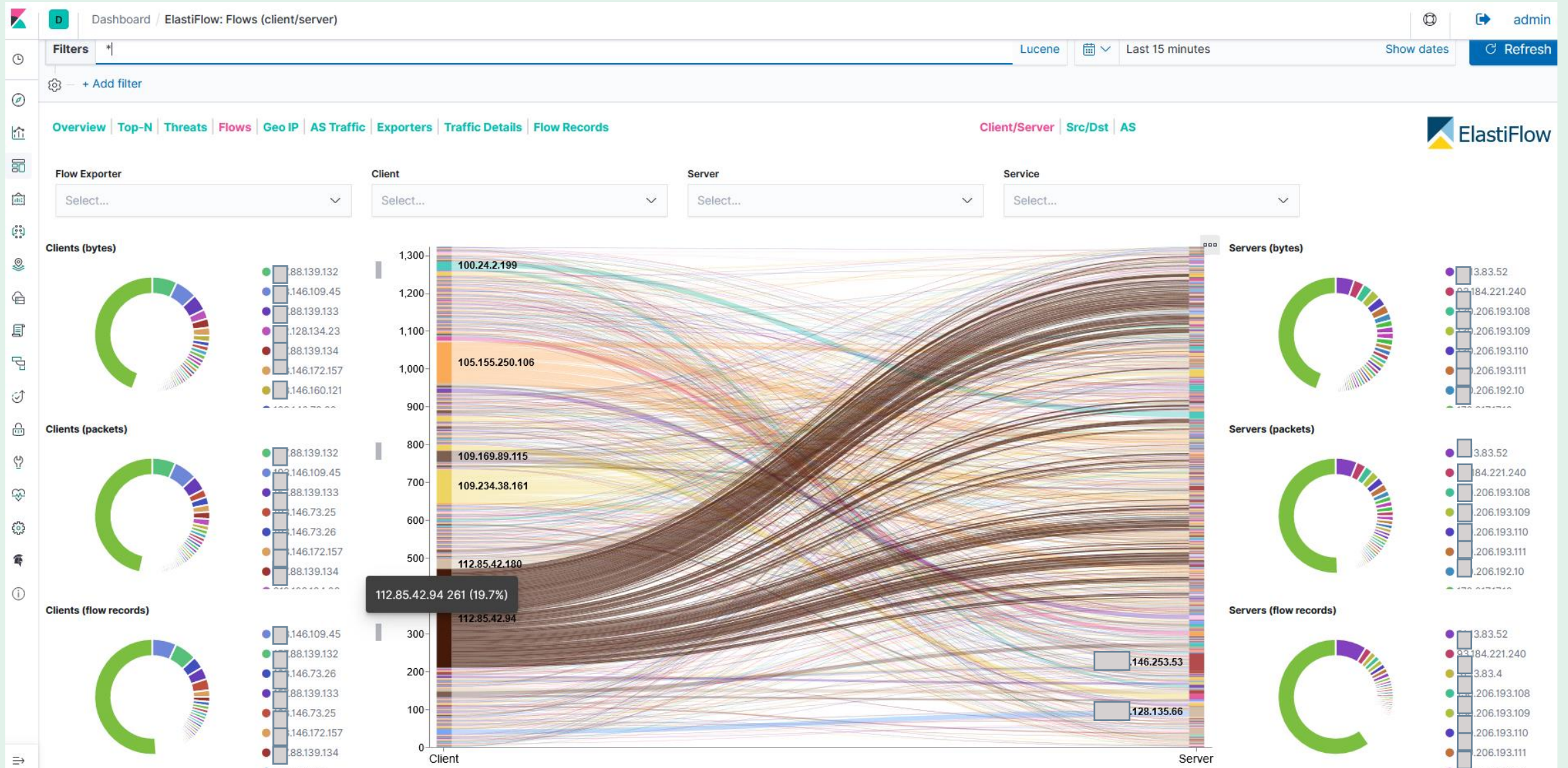
- IPv4
- TCP
- UDP
- ICMP
- ESP
- GRE
- IPv6
- VRRP
- PIM

**Word Cloud**

suspicious, apache, bot, http, bruteforce, dns, smtp, ssh, ftp, spam, asterisk, mailer, voip, named, dovecot, postfix, cms, modsec, owncloud, wordpress, email, pop3, sip, telnet, ddos, auth, nginx, sasl, exim, mailer, spam, ftp, ssh, dns, smtp, voip, named, dovecot, postfix, cms, modsec, owncloud, wordpress, email, pop3, sip, telnet, ddos, auth, nginx, sasl, exim

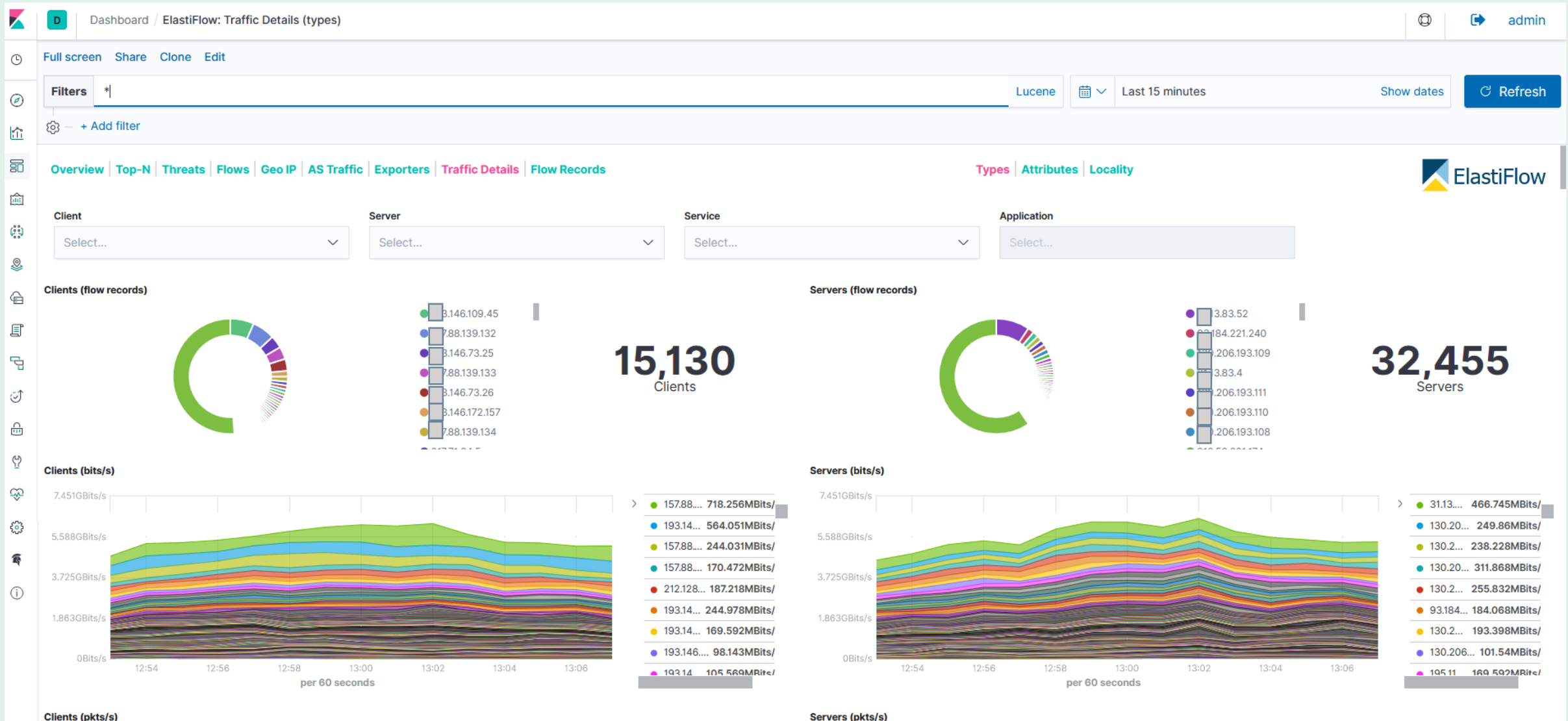


# Monitorización - ELK Stack





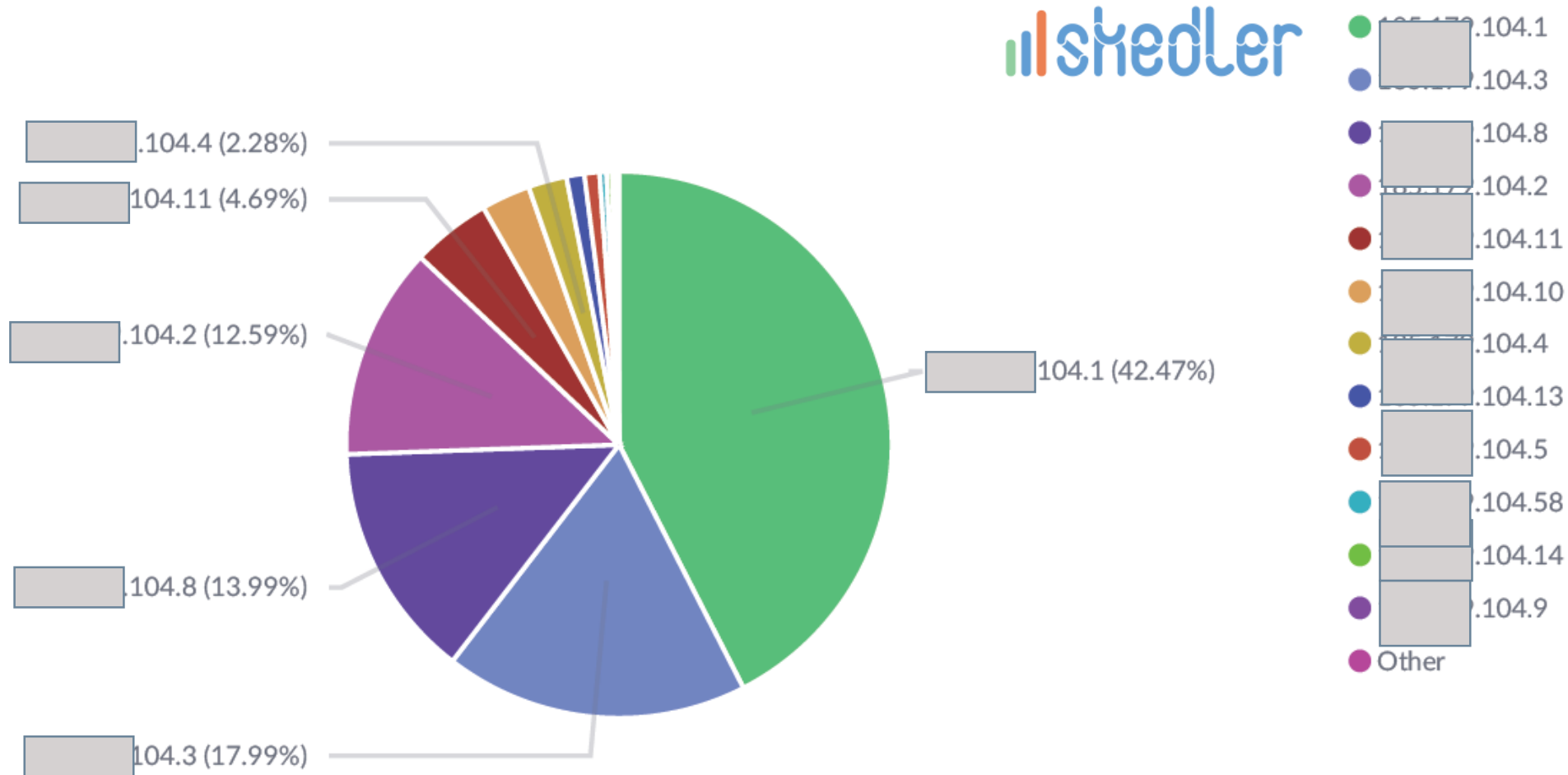
# Monitorización - ELK Stack





# Monitorización - Informes

SCAYLE Top 12 Source IP Addresses

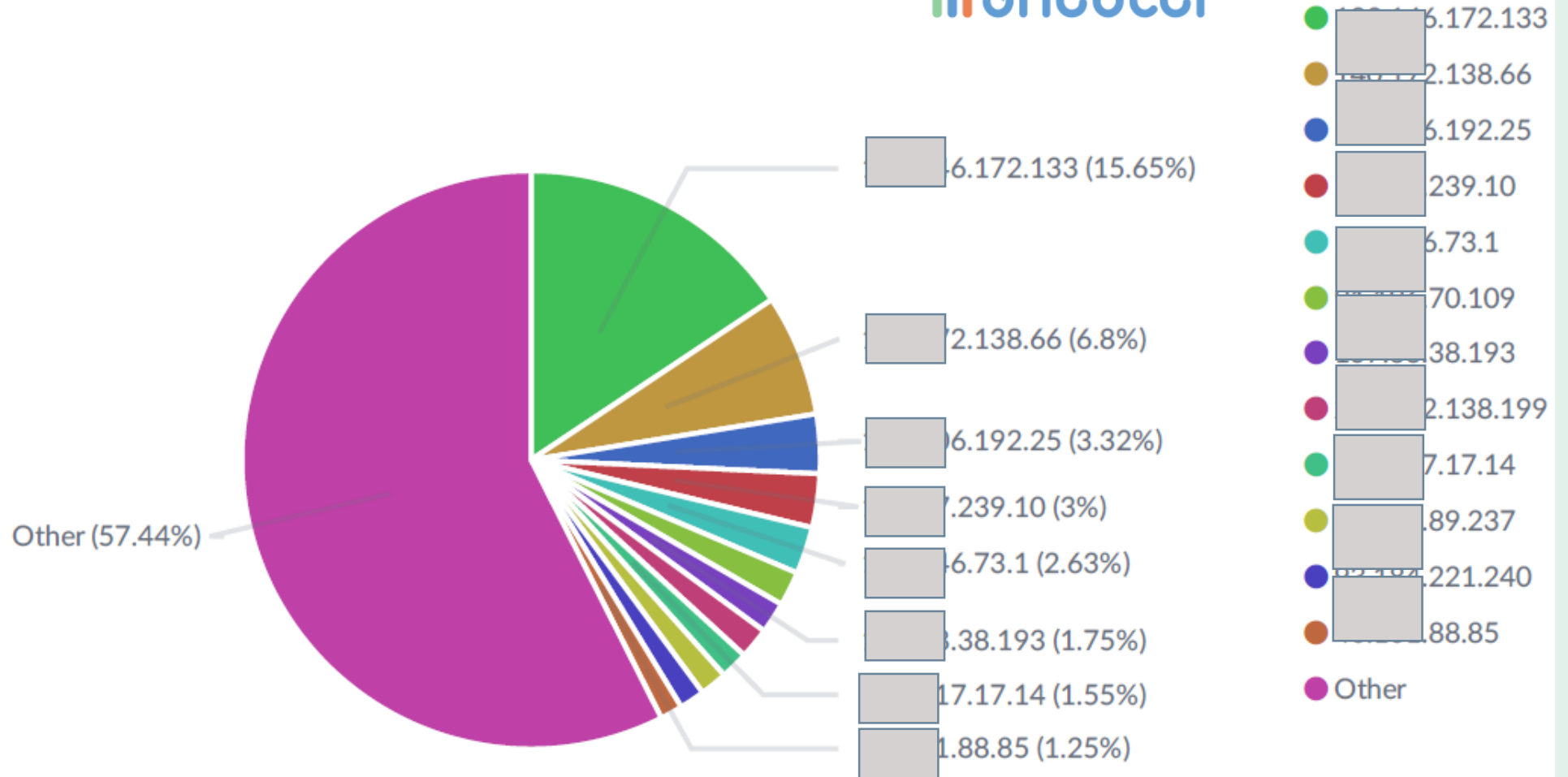






# Monitorización - Informes

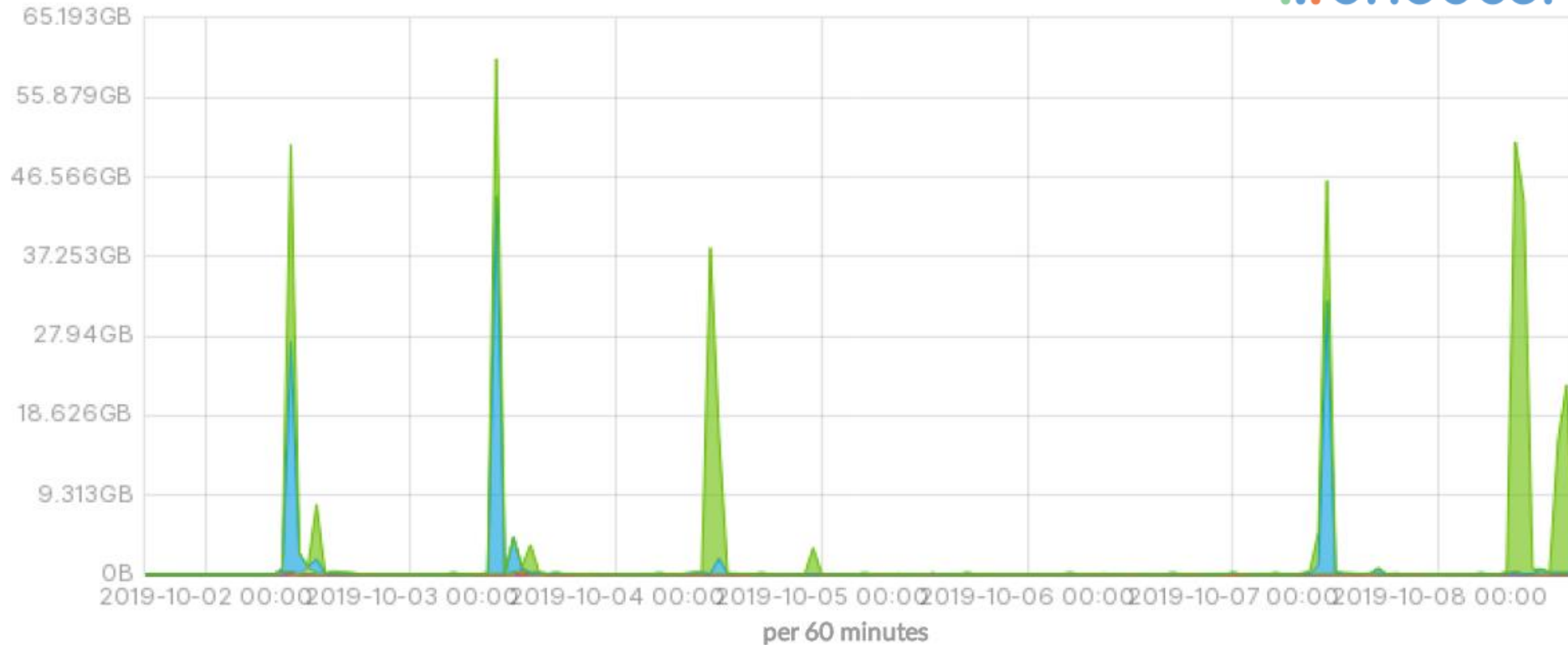
SCAYLE Top 12 Destination IP Addresses





# Monitorización - Informes

SCAYLE Top 12 Source Traffic (Bytes)

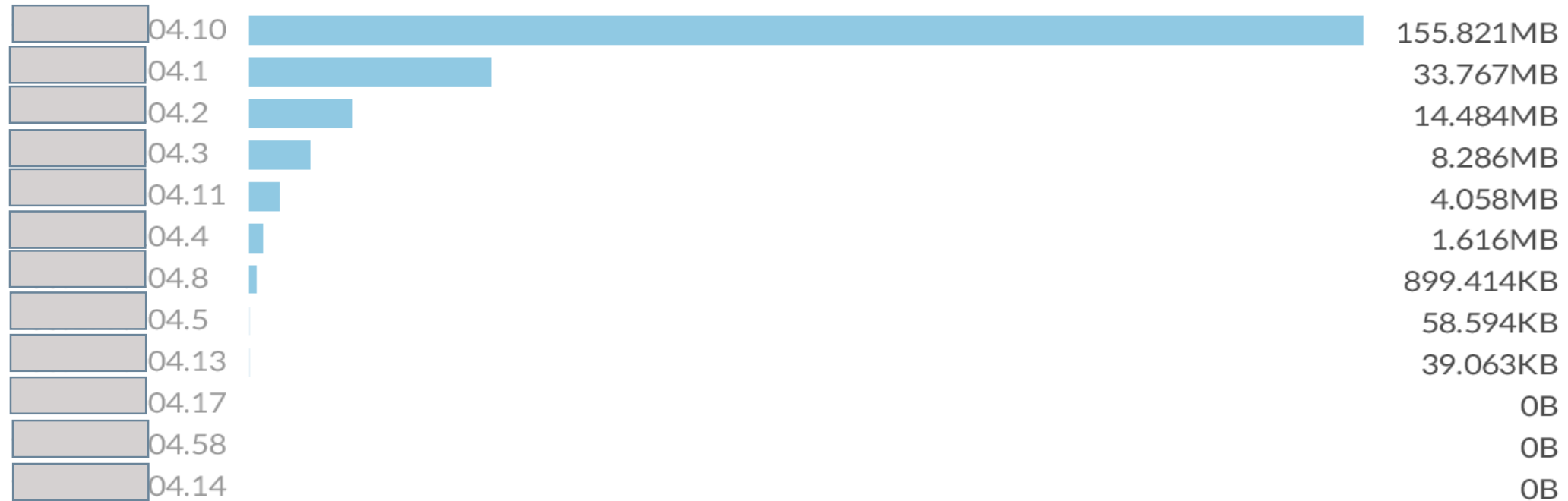


● [redacted] 9.104.2 14.484MB	● [redacted] 9.104.3 8.286MB	● [redacted] 9.104.1 33.767MB	● [redacted] 9.104.10 155.821MB
● [redacted] 9.104.13 39.063KB	● [redacted] 9.104.8 899.414KB	● [redacted] 9.104.11 4.058MB	● [redacted] 9.104.14 0B
● [redacted] 9.104.58 0B	● [redacted] 9.104.4 1.616MB	● [redacted] 9.104.5 58.594KB	● [redacted] 9.104.17 0B



# Monitorización - Informes

SCAYLE Top 12 Descending Source Traffic (Bytes)





# Alertas Proactivas

## WHAT DO USERS WANT?

WHEN ANOMALIES  
HAPPEN



QUICK NOTIFICATIONS

FOR AN IMMEDIATE  
ACTION

shedler

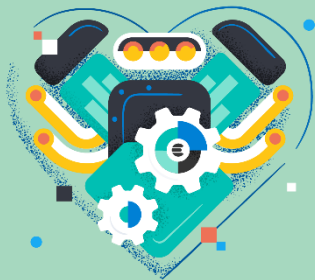
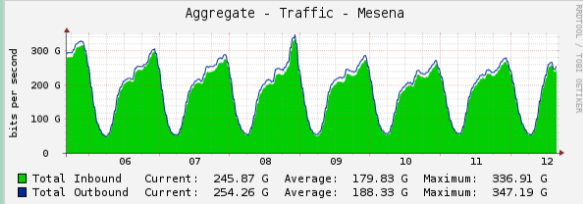
Alertas + Informes


≈10,000\$/año







# Alertas Proactivas




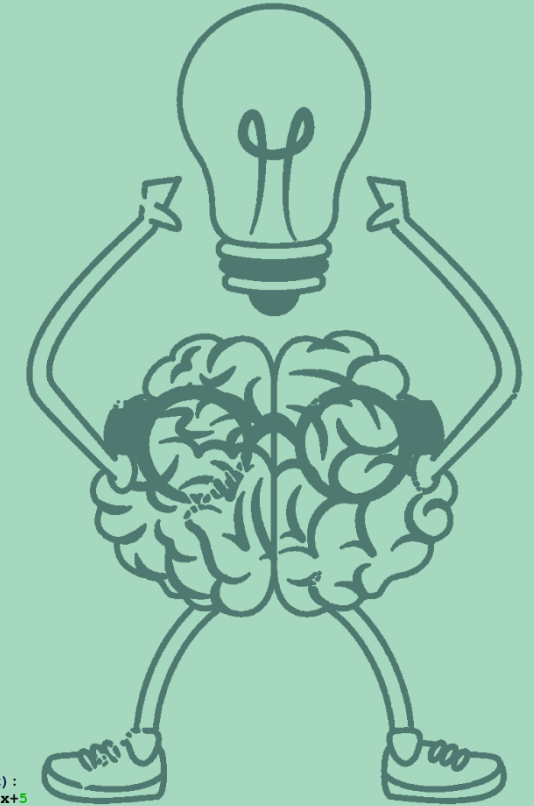
01 

 kibana 02

03 

 elasticsearch 04

05  python



```
def add5(x):
    return x+5

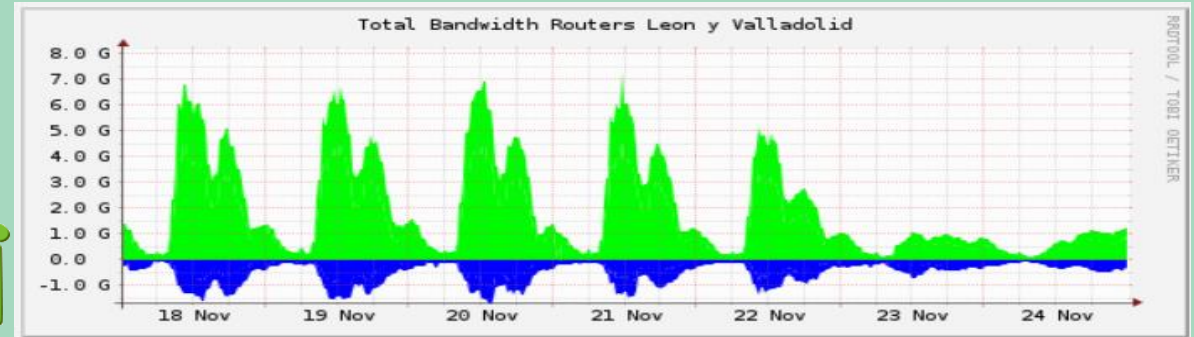
def dotwrite(ast):
    nodename = getNodename()
    label=symbol.sym_name.get(int(ast[0]),ast[0])
    print ' %s [label="%s" % (nodename, label),
    if isinstance(ast[1], str):
        if ast[1].strip():
            print '=' % ast[1]
        else:
            print ''
    else:
        print ''
    children = []
    for n, child in enumerate(ast[1:]):
        children.append(dotwrite(child))
    print ' %s -> {' % nodename,
    for name in children:
        print '%s' % name,
```



# Alertas Proactivas

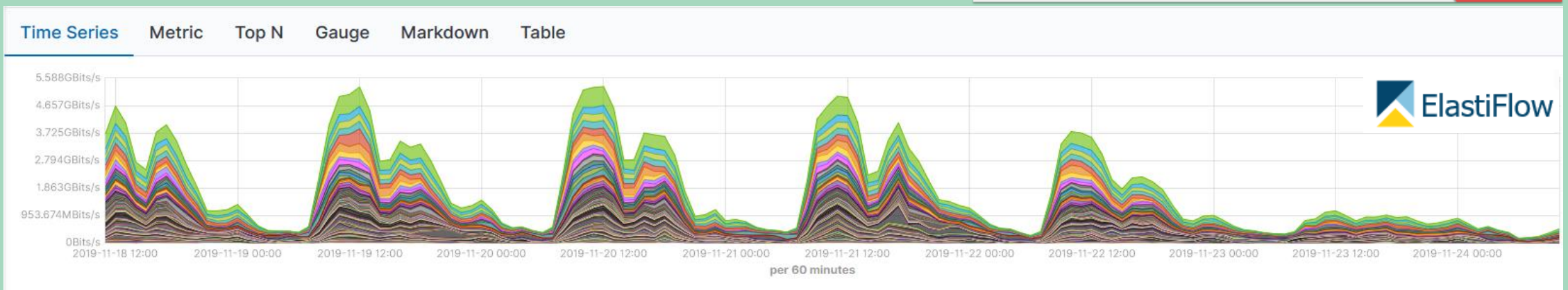
01

TENDENCIAS TRÁFICO



TENDENCIAS TRÁFICO

02





# Alertas Proactivas

03

## NetFlow

```
geoasn.asn: 766 dst_geoasn.as_org: Entidad Publica Empresarial Red.es host: 10.200.4.254 bytes: 52 @timestamp: January 23rd 2019, 08:00:58.000 name_protocol: TCP @version: 1 src_geoip.country_code3: CN src_geoip.latitude: 28.55 src_geoip.region_name: Jiangxi src_geoip.location.lon: 115.933 src_geoip.location.lat: 28.55 src_geoip.timezone: Asia/Shanghai src_geoip.country_code2: CN src_geoip.longitude: 115.933 src_geoip.ip: 182.97.210.0 src_geoip.country_name: China src_geoip.continent_code: AS src_geoip.region_code: 36 src_geoip.city_name: Nanchang src_port_name: 54793 netflow.src_mask: 12 netflow.protocol: 6 netflow.ipv4_next_hop: 185.179.107.212 netflow.src_as: 4,134 netflow.sampling_algorithm: 0
```

### Agregación 1

```
"aggs": {
  "2": {
    "terms": {
      "field": "netflow.ipv4_dst_addr.keyword",
      "size": 5,
      "order": {
        "1": "desc"
      }
    }
  },
  "aggs": {
    "1": {
      "sum": {
        "field": "netflow.in_bytes"
      }
    }
  }
},
```

### Agregación 2

```
},
"3": {
  "terms": {
    "field": "src_port_name.keyword",
    "size": 5,
    "order": {
      "1": "desc"
    }
  },
  "aggs": {
    "1": {
      "sum": {
        "field": "netflow.in_bytes"
      }
    }
  }
},
```



elasticsearch

04



# Alertas Proactivas

05



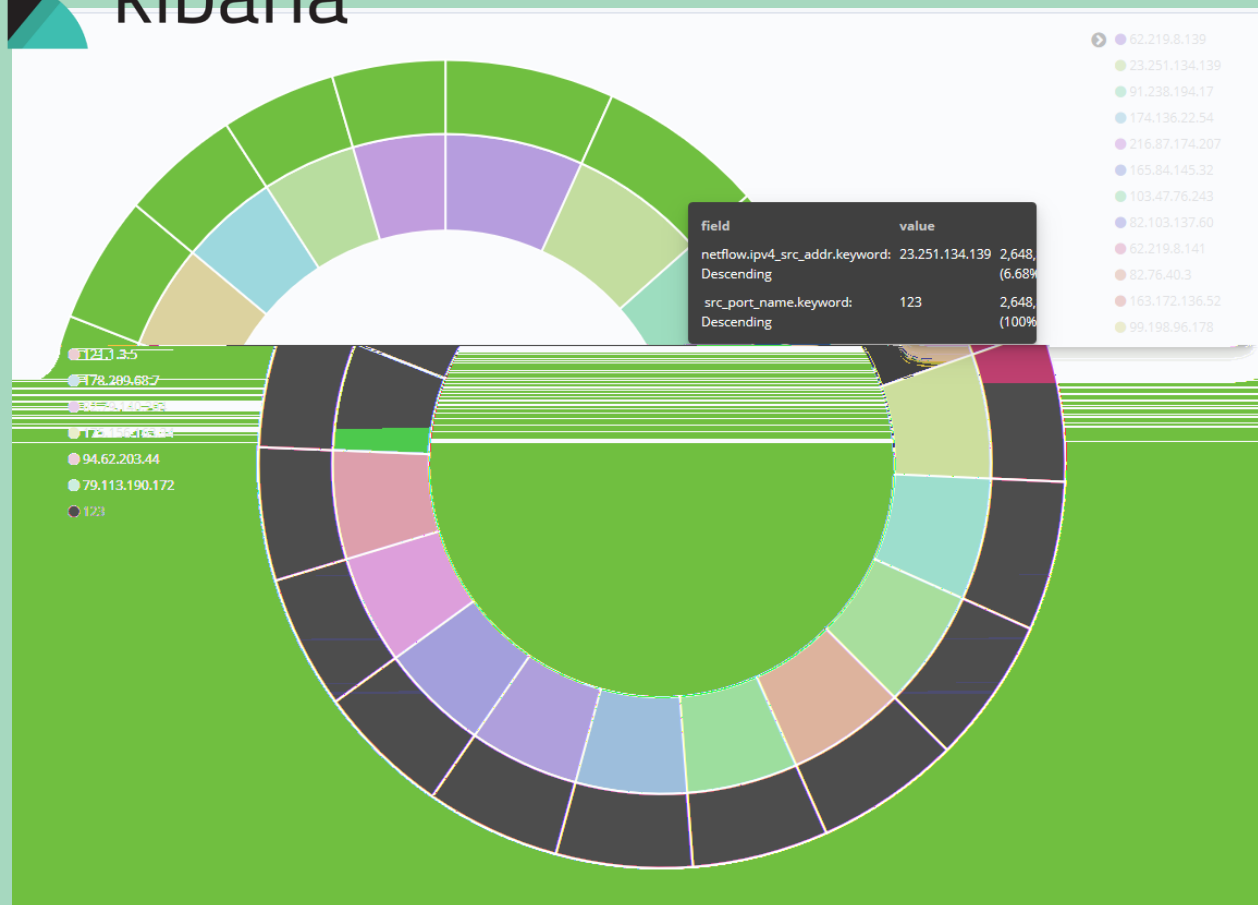
```
1 GLOBAL VARS:
2
3 LAST_TOP_IP, LAST_STATE=0, TIME_WINDOW=5m, ALERT_LEVEL=0
4
5 MATRIZ TENDENCIA TRAFICO SEMANAL
6
7 1. Para TIME_WINDOW
8   Obtener los documentos indexados en elasticsearch
9   Calcular los bytes/s --> (Gbps)
10  Obtener top 5 de host de destinos y puertos y seleccionar ACTUAL_TOP_IP que genera mas del 50% de los Gbps
11
12
13 2.Comparar los Gbps obtenidos con la tendencia de tráfico en esa hora (MATRIZ_TENDENCIA)
14   Si los Gbps superan UMBRAL{
15     ALERT_LEVEL = 1
16     Si LAST_STATE = 1 {      <--- si se ha mantenido durante el TIME_WINDOW anterior
17       ALERT_LEVEL = 2
18       Si ACTUAL_TOP_IP = LAST_TOP_IP{      <--- si ACTUAL_TOP_IP se mantiene
19         ALERT_LEVEL = 3
20       }
21     }
22
23     LAST_STATE=1      <--- en el estado actual se ha superado umbral
24     LAST_TOP_IP = ACTUAL_TOP_IP <--- registramos la ip con más actividad
25   }
26   Si no {
27     LAST_STATE = 0      <--- No se registraron anomalías
28     LAST_TOP_IP = None
29   }
30
31 3. Si ALERT_LEVEL != 0 {
32   Enviar mensaje correo ALERT_LEVEL
33   <--- ALERT_LEVEL 1 : Cuando ha habido anomalía aislada
34   <--- ALERT_LEVEL 2 : Cuando ha habido anomalía mantenida desde el ultimo TIME_WINDOW
35   <--- ALERT_LEVEL 3 : Cuando ha habido anomalía mantenida desde el ultimo TIME_WINDOW y ACTUAL_TOP_IP = LAST_TOP_IP
36
37 }
38
```



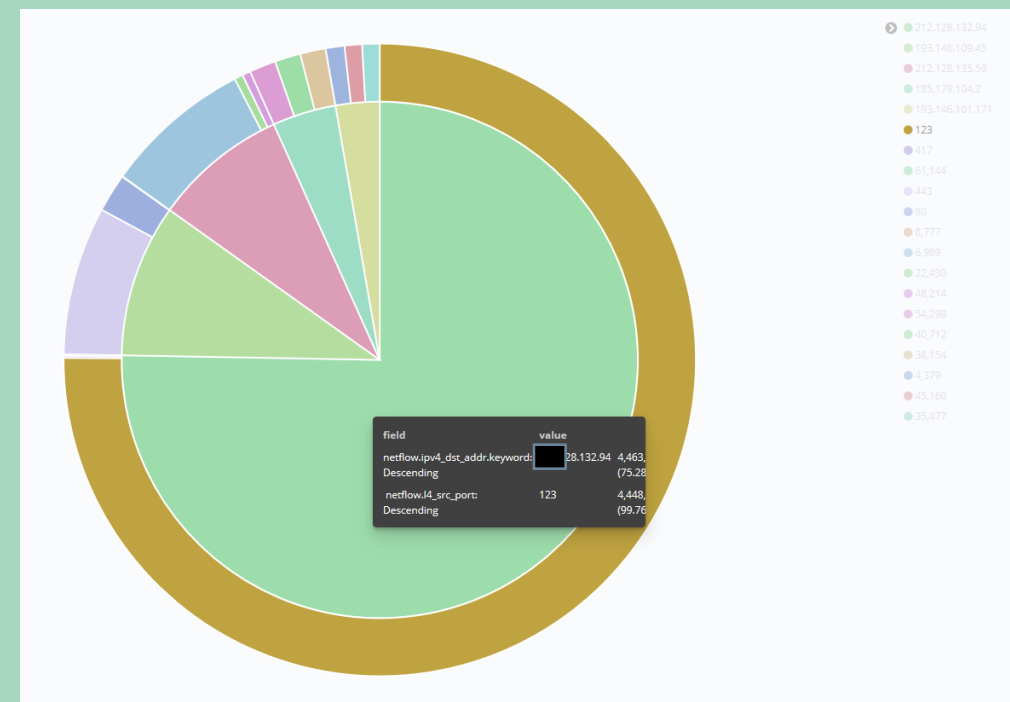


# Alertas Proactivas

kibana



## DDOS amplificación NTP





# Alertas Proactivas

05



```
root@srv-elk:/home/elk/python_script# python3 script.py
LAST_STATE: 1
LAST_TOPIP: ['128.132.94', '146.109.45', '43.79.232', '128.135.105', '.128.161.136']
[+] Connection: <Elasticsearch([{'host': 'localhost', 'port': 9200}])>
[+] Total flow bytes (in GBps) NO TREATMENT: 514192551.0
[+] Total flow bytes (in GBps): 411.3540408
[+] Total Gbps: 1.371180136
[+][+] TOP_DST_PORTS: 19003
[+][+] TOP_SRC_PORTS: 123
[+] Top 1 destiny IP by bytes: 128.132.94 with 0.509165897 Gbps
[+] Top 2 destiny IP by bytes: 146.109.45 with 0.000594787 Gbps
[+] Top 3 destiny IP by bytes: 128.135.59 with 0.000364584 Gbps
[+] Top 4 destiny IP by bytes: 128.161.136 with 0.000258483 Gbps
[+] Top 5 destiny IP by bytes: 128.134.24 with 0.000174179 Gbps
[+] local ips ['.128.132.94', '.146.109.45', '.128.135.59', '.128.161.136', '128.134.24']
ALERT LEVEL 1
ALERT LEVEL 2
ALERT LEVEL 3
```

# Gracias !!



SCAYLE



**Europa impulsa  
nuestro crecimiento**

FONDO  
EUROPEO DE  
DESARROLLO  
REGIONAL  
(FEDER)



universidad  
de león

