

SCAYLE

Supercomputación Castilla y León

RedCAYLE estado actual y futuro

III Jornada RedCAYLE, 10/11/2022



Contenido



ESTADO ACTUAL

Red Óptica 10G



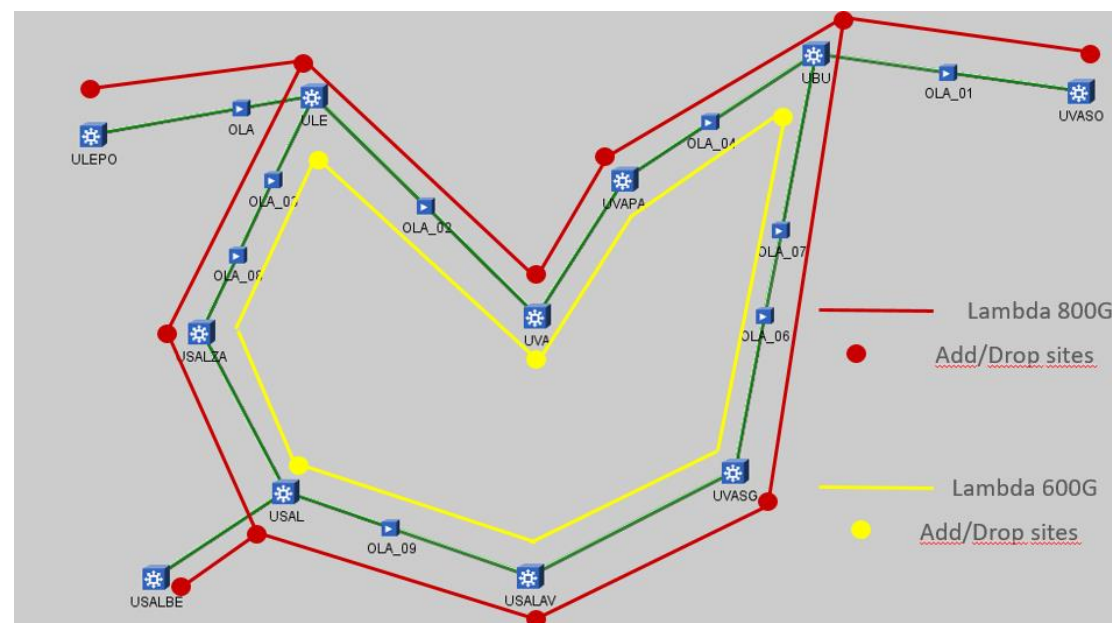
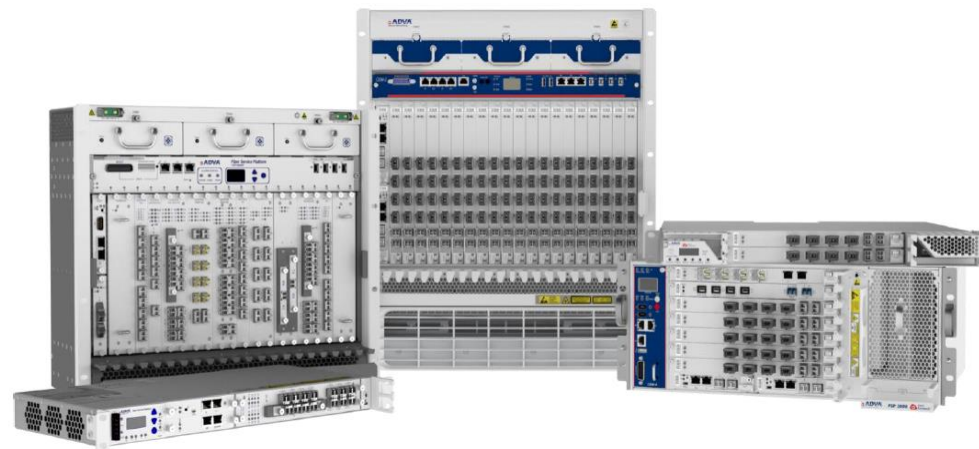


ESTADO ACTUAL

Licitación nueva Red Óptica 100G Pliego publicado 10 Noviembre 2022

Características Generales

- Solución DWDM, al menos, 100G
- Restauración de canales
- Protección completa
- Plano de control distribuido
- Interfaces cliente 1G/10G/100G(QSFP28)
- Provisión automática de nuevos servicios



ESTADO ACTUAL

Licitación nueva Red Óptica 100G

- Sistema de Gestión y monitorización avanzado
- OTDR dispositivo para la supervisión de la fibra óptica
- Proyecto de migración
- Soporte 24x7 con reemplazo 8h
- Garantía 5 años
- Precio Licitación 3.945.000 €

Criterios de Valoración (100 puntos)

Criterio Económico	15 puntos
---------------------------	-----------

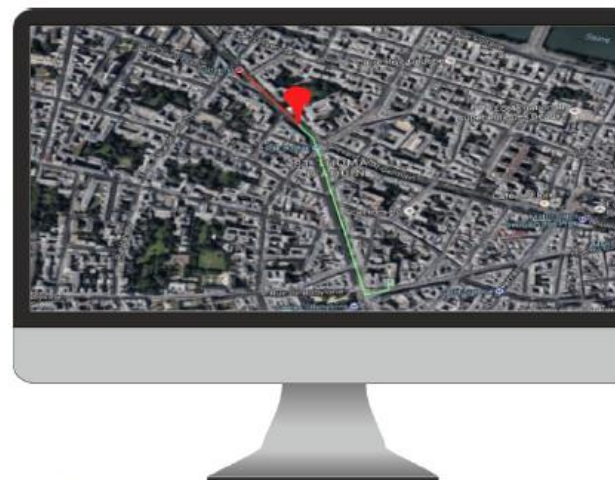
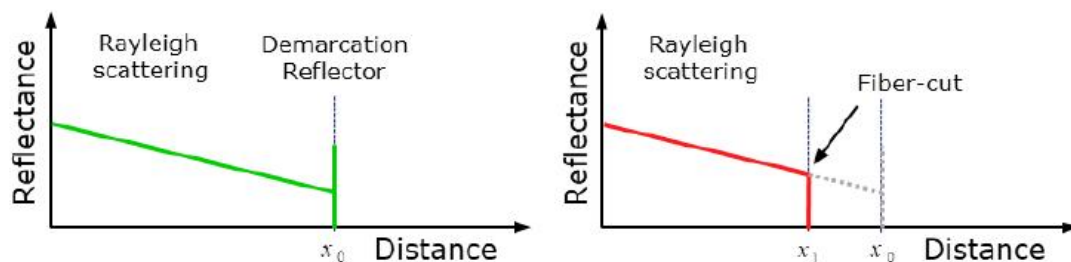
Criterios **Técnicos Cuantificables**

mediante fórmula	55 puntos
mediante juicio de valor	30 puntos



Novedades

Monitorización grafica 24x7 fibra oscura



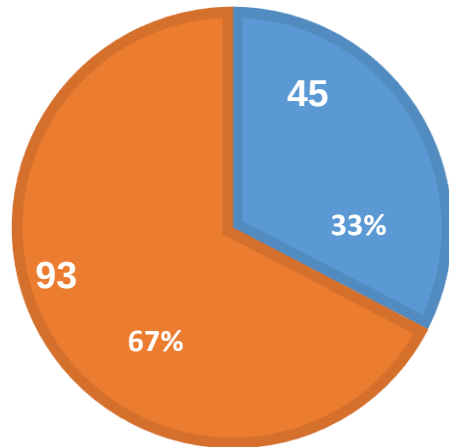
- Monitorización en **24x7** de las FFOO en uso
- Infraestructura de **crítico funcionamiento**
- **Integración** completa mediante SNMP en gestores de **cliente** OpenView, Nagios....
- Soporte de **mapas GIS**
- Envío de eventos SNMP con **identificación de punto KM de fallo**
- Generación de **graficas OTDR sin necesidad de cortar la conectividad**
- Detección de **intrusiones** en el sistema



INCIDENCIAS en RedCAYLE

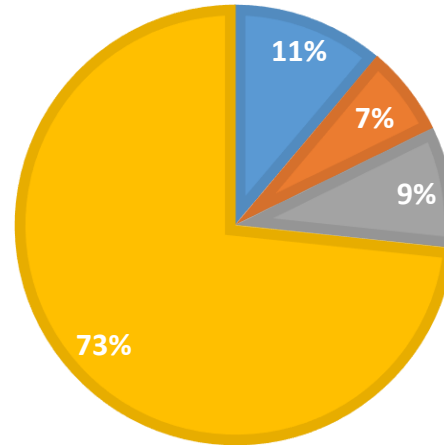


■ Incidencias ■ Solicitudes



INCIDENCIAS

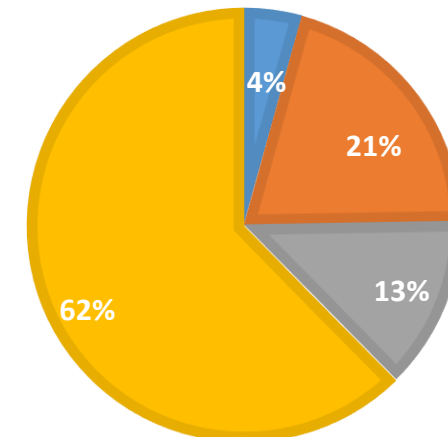
■ Cortes fibra ■ Problema acceso ■ Alarmas equipos ■ Otros



■ Otros
Pérdida de conectividad (VRRP, BGP)
Caída circuitos (mantenimiento
equipamiento cliente)
Estado equipos (temperatura, filtros, fallo
eléctrico)

SOLICITUDES

■ Trabajos Tefonica ■ Trabajos preventivos
■ Mejoras hw/sw ■ Resto

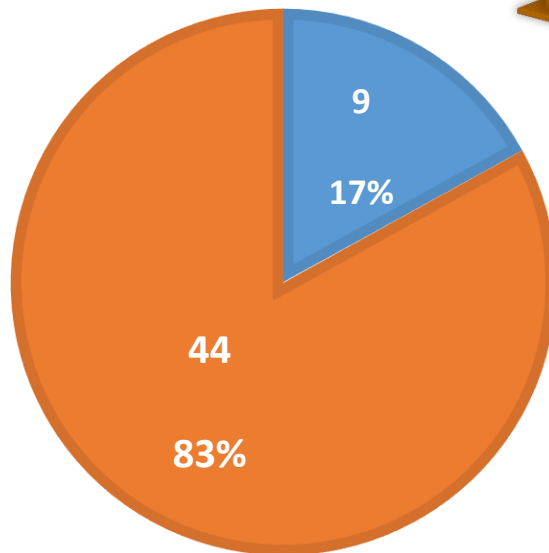


0 Fallos Hardware !!

INCIDENCIAS en RedIRIS

TICKETS REDIRIS

■ Trabajos Programados ■ Otros



INCIDENTES INCIBE-CERT

Centro de respuesta a incidentes de seguridad operado por el Instituto Nacional de Ciberseguridad

- 1 Servidor Exchange vulnerable a ProxyShell
- 2 Servidores NTP expuesto a ataques de denegación de servicio por amplificación



MONITORIZACIÓN

Nagios[®]



kubernetes



ELK Stack



Grafana

graylog



kibana



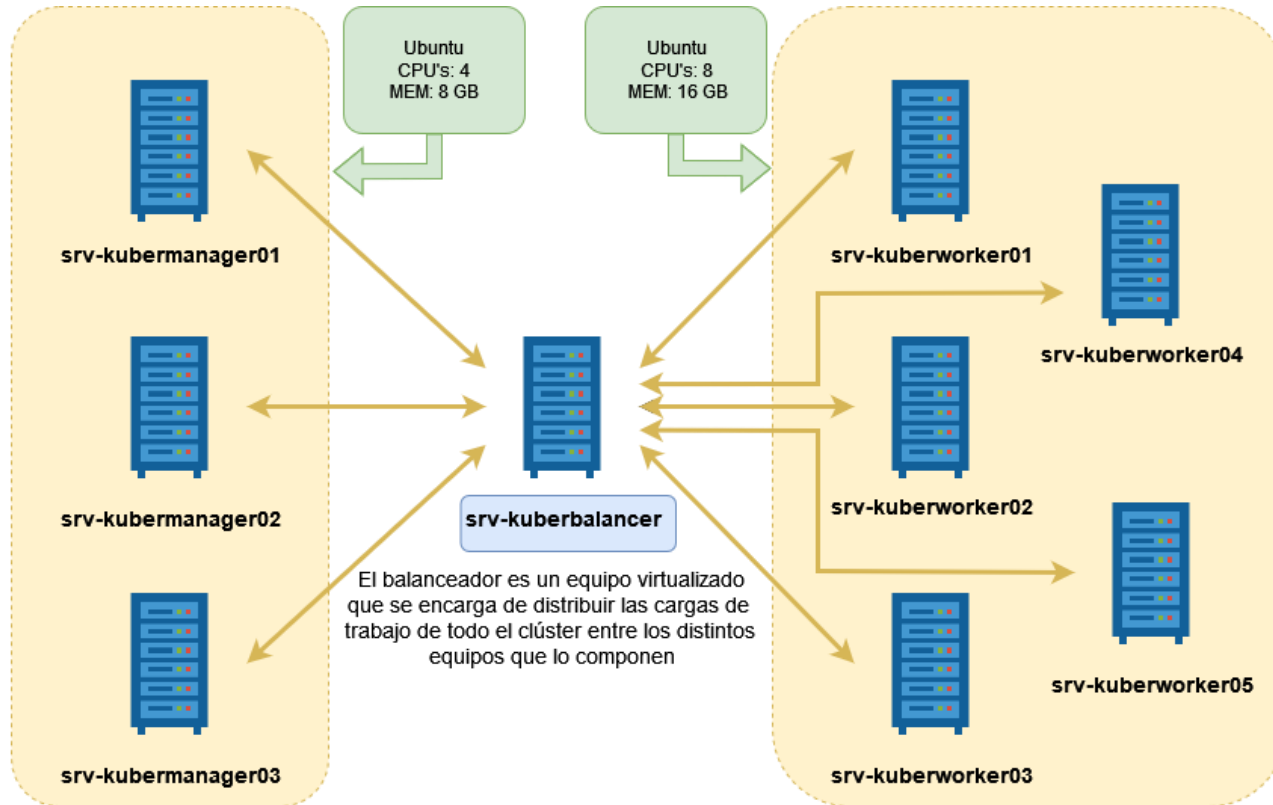
telegraf



influxdb



MONITORIZACIÓN



El grupo de "managers" está compuesto por un total de tres equipos virtualizados, encargados de mantener el control sobre las distintas tareas y aplicaciones que se ejecutan en el clúster

El grupo de "workers" está compuesto por un total de cinco equipos virtualizados, sobre los cuales se ejecutan las distintas tareas y aplicaciones del clúster

Infraestructura Virtual

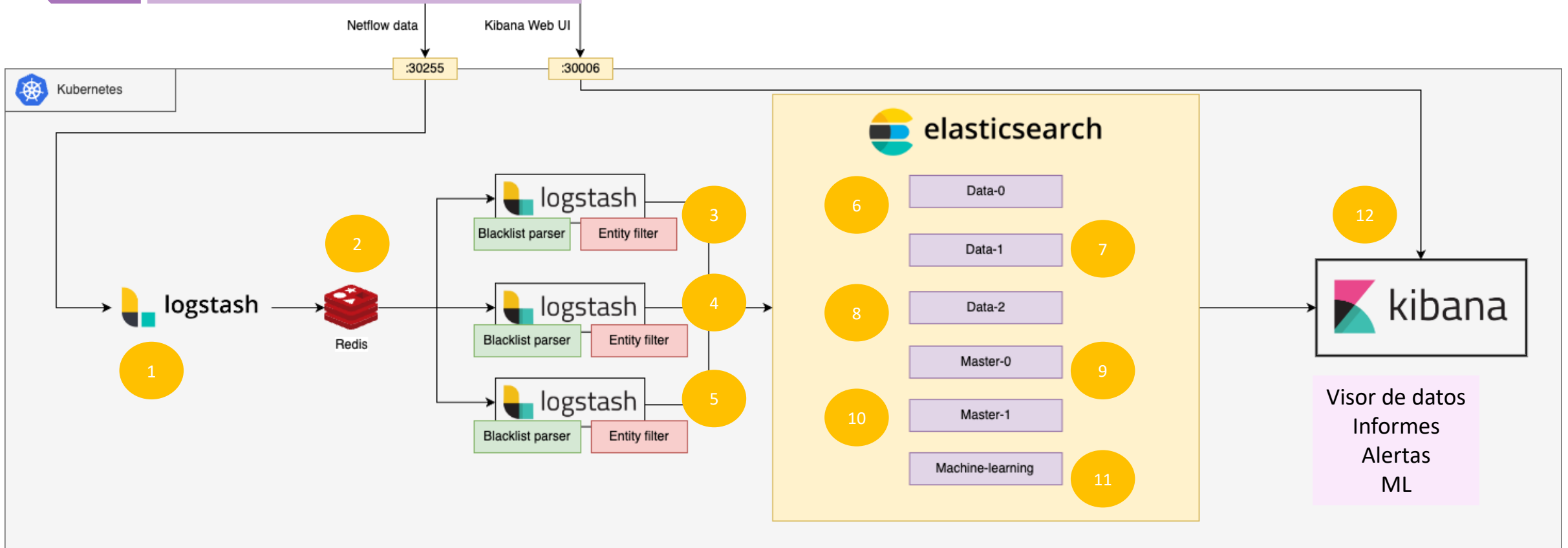


kubernetes

Sistema de código abierto para automatizar el despliegue, el escalado y la gestión de aplicaciones en contenedores

MONITORIZACIÓN

Infraestructura de Contenedores

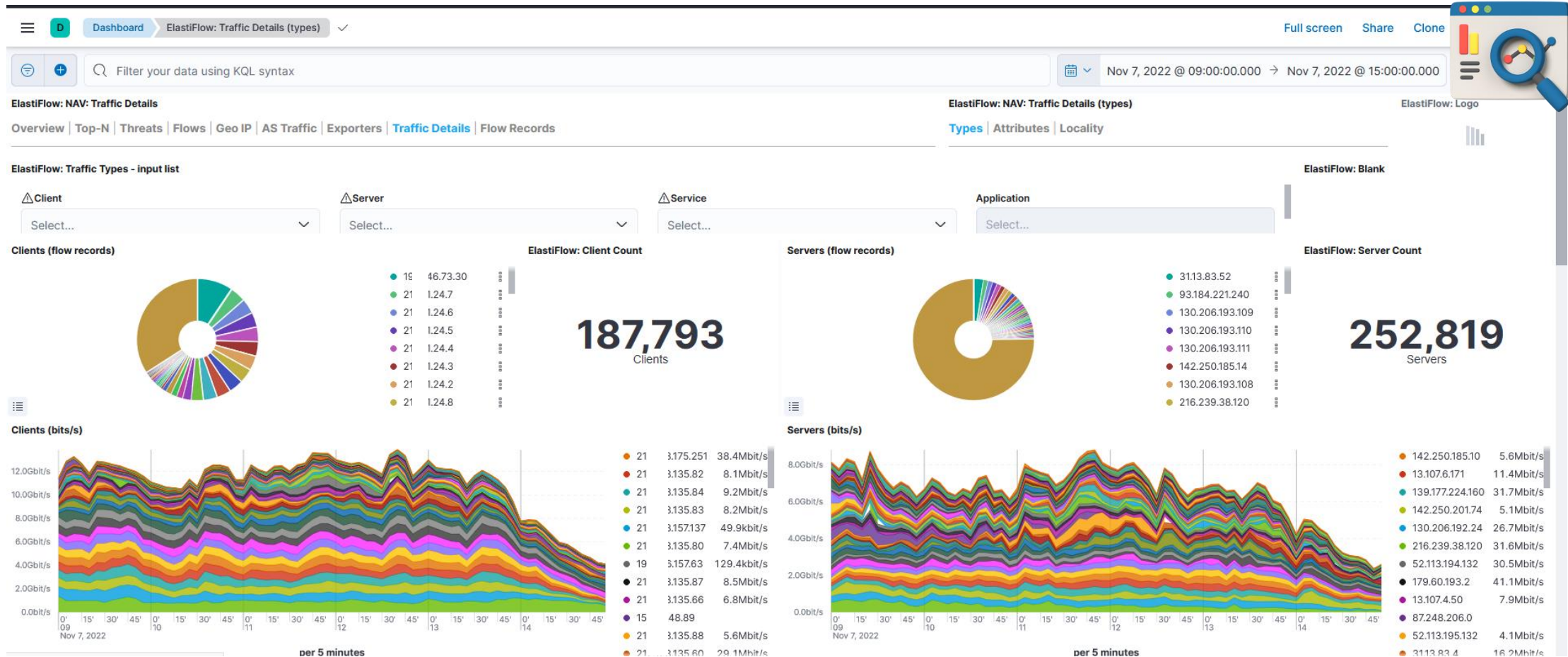


- 1 Recibe el trafico netflow y lo pasa a formato legible
- 2 Es un BD que retiene la información hasta que es requerida
- 3,4 y 5 Recogen la información de 2 y la enriquecen con valores añadidos

- Clúster de elasticsearch compuesto por 3 nodos datos, que son los encargados de almacenar los datos recibidos (6,7 y8), 2 nodos master que Coordinan y dan acceso a los datos (9 y10) y un nodo de machine-learning(11)

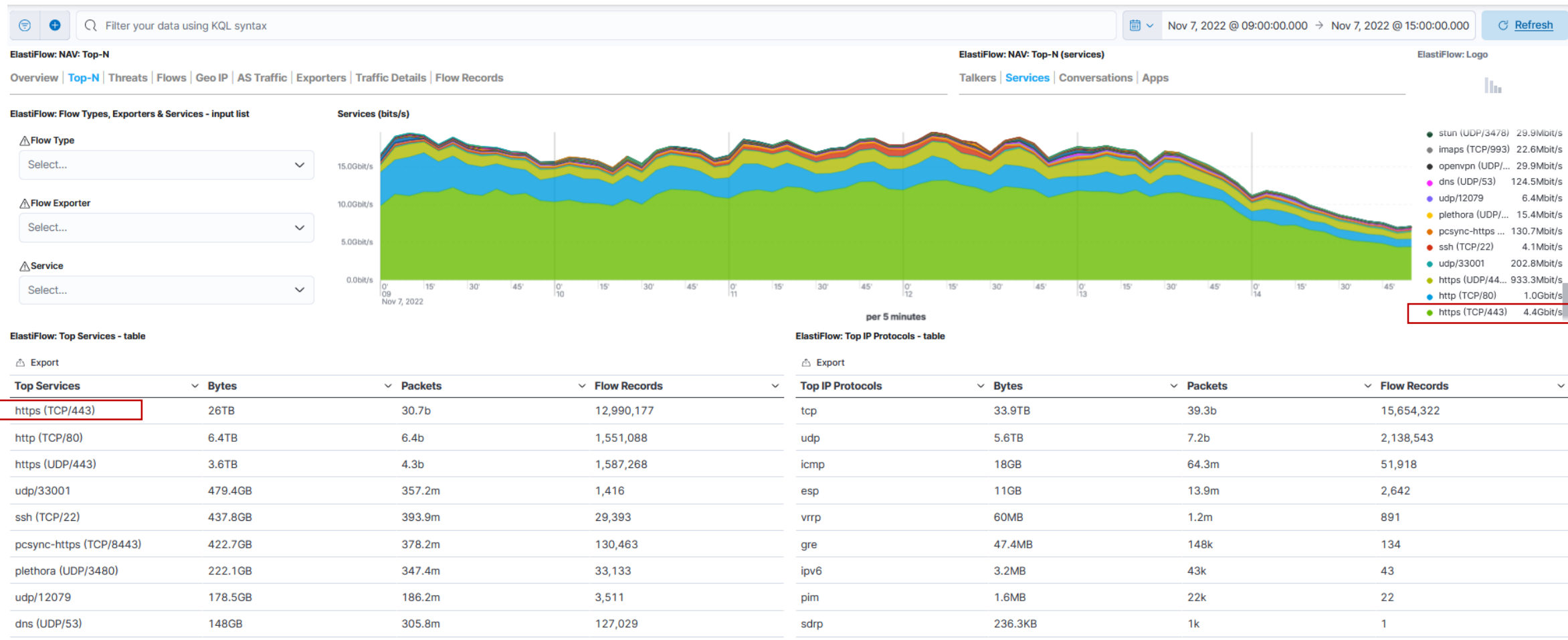
MONITORIZACIÓN

Tráfico



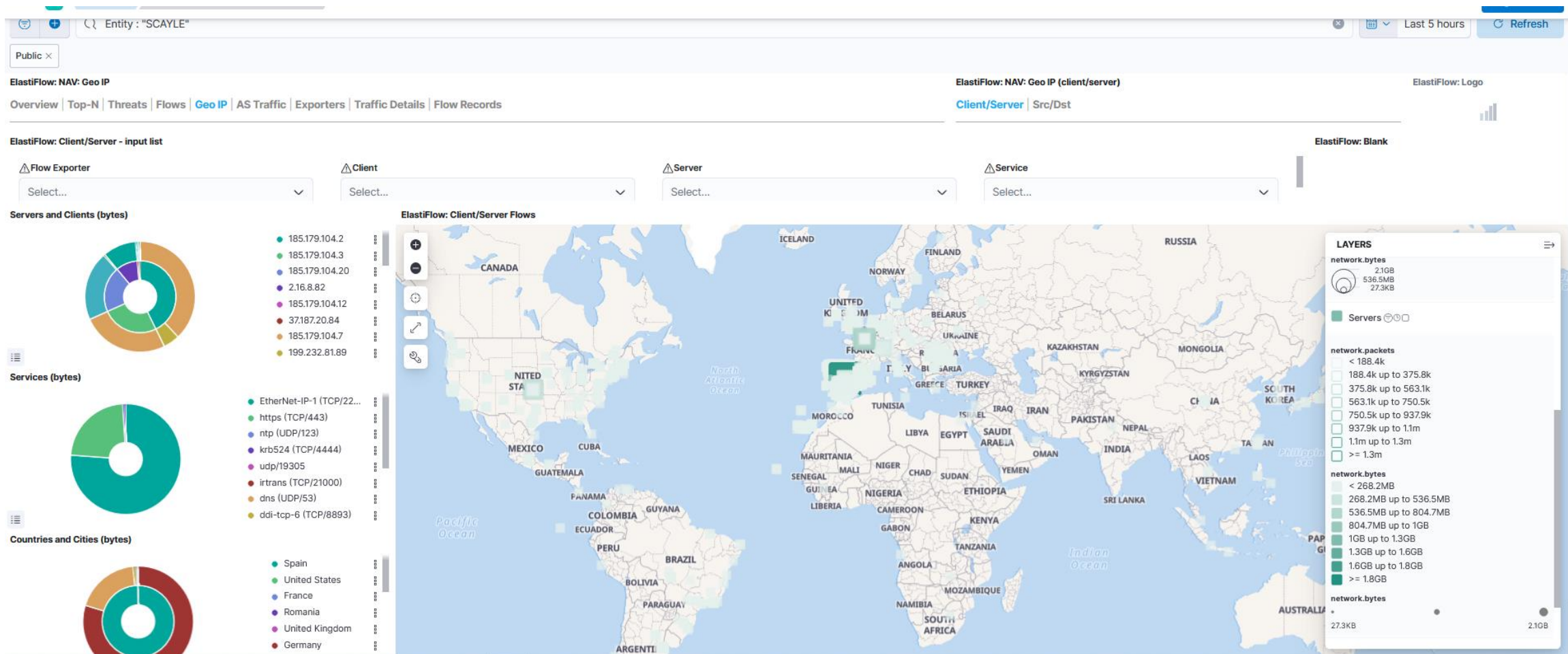
MONITORIZACIÓN

Servicios Top N



MONITORIZACIÓN

Geo IP



MONITORIZACIÓN

Flujos

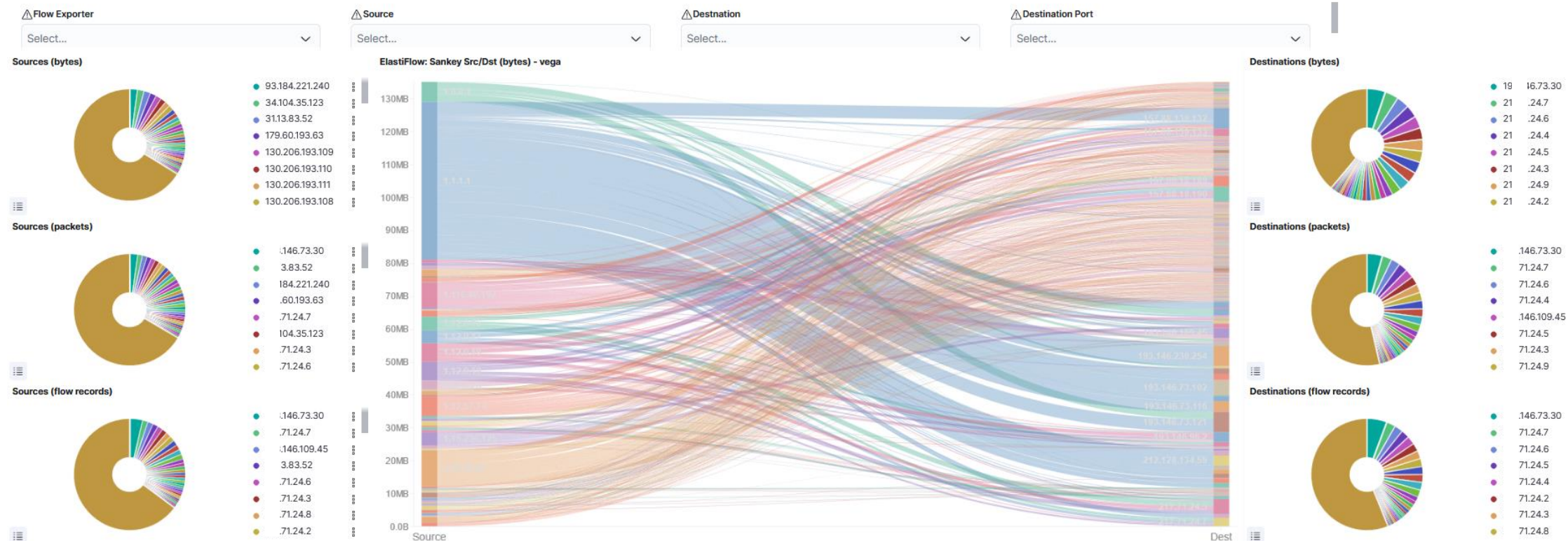


Overview | Top-N | Threats | **Flows** | Geo IP | AS Traffic | Exporters | Traffic Details | Flow Records

Client/Server | **Src/Dst** | AS

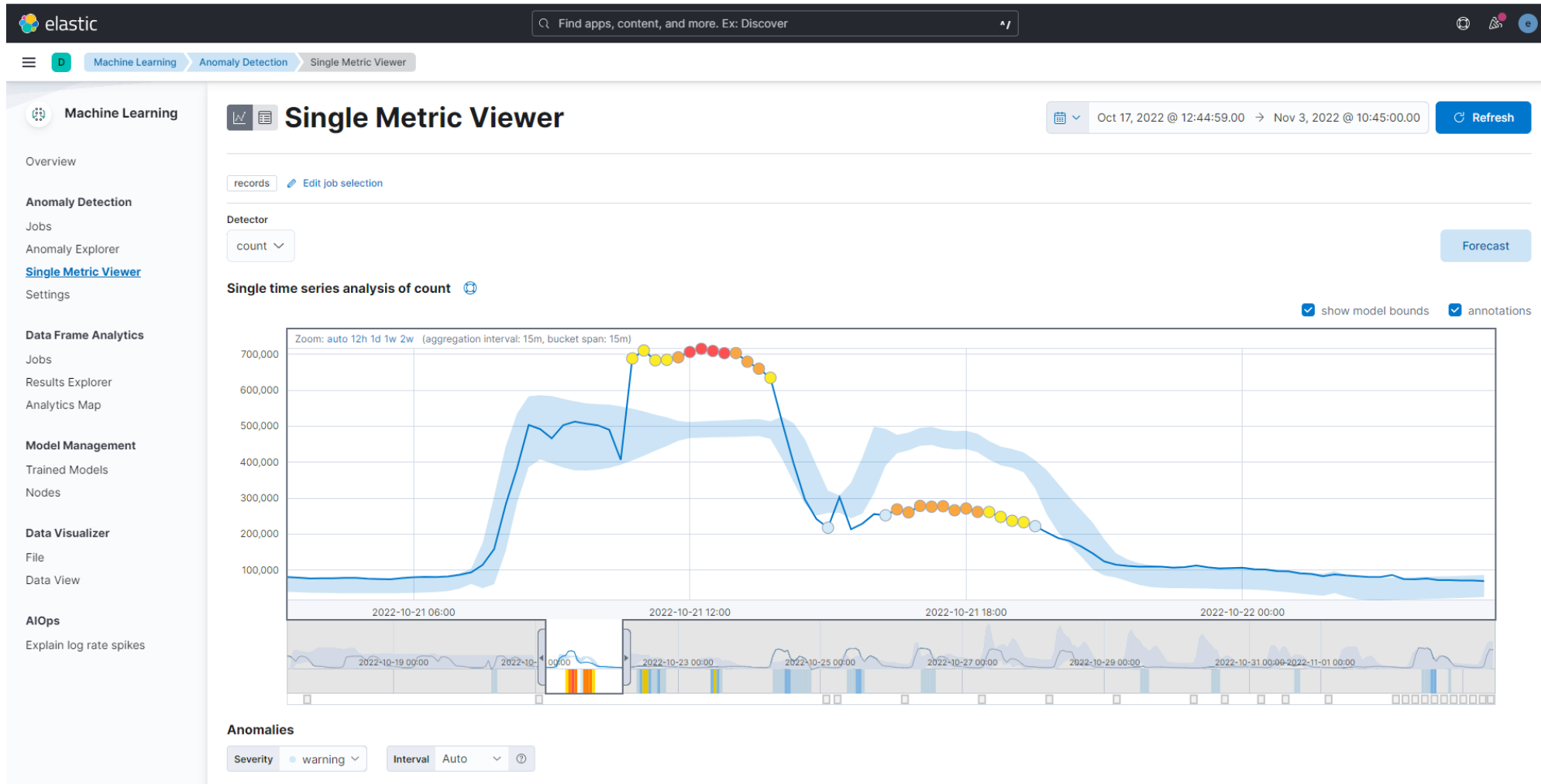
ElasticFlow: Src/Dst - input list

ElasticFlow: Blank



MONITORIZACIÓN

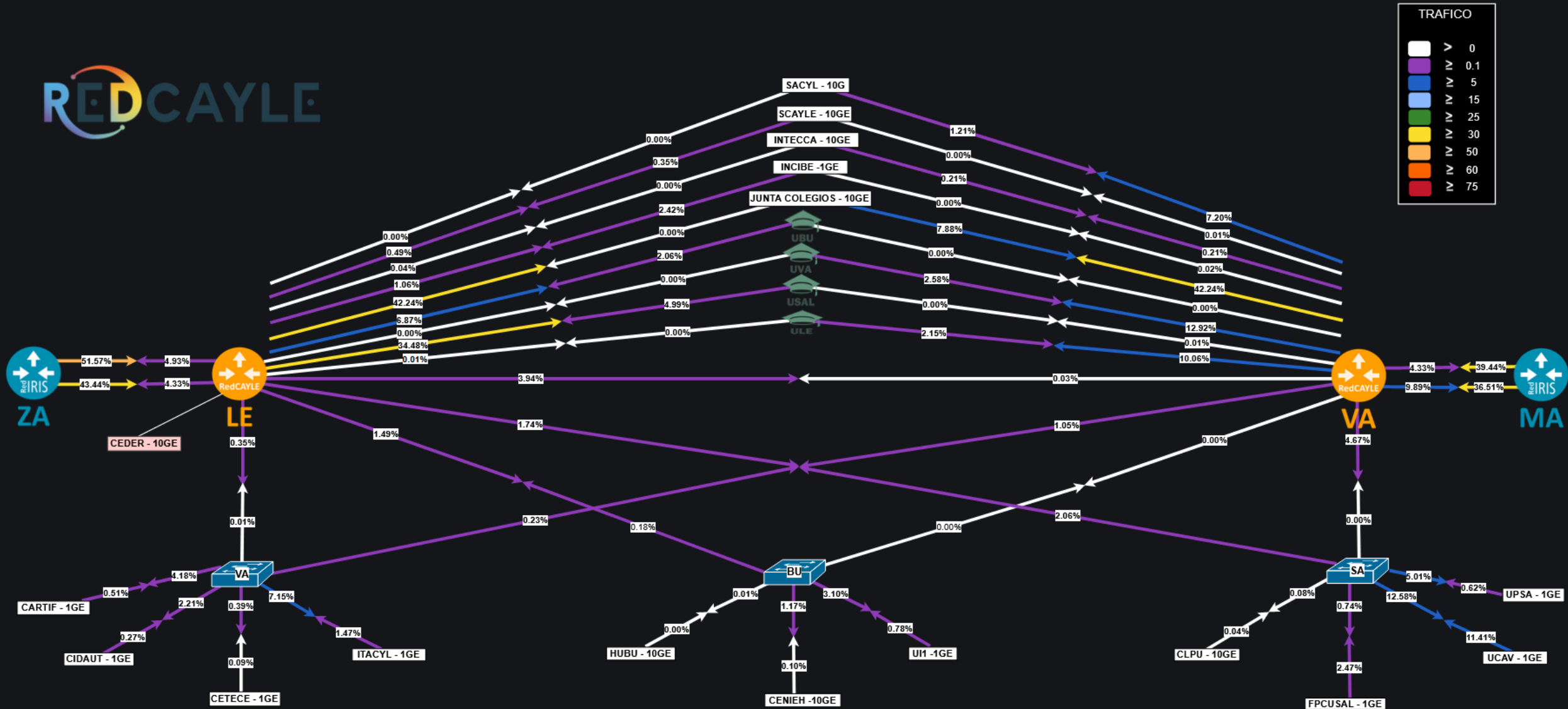
Machine Learning





MONITORIZACIÓN

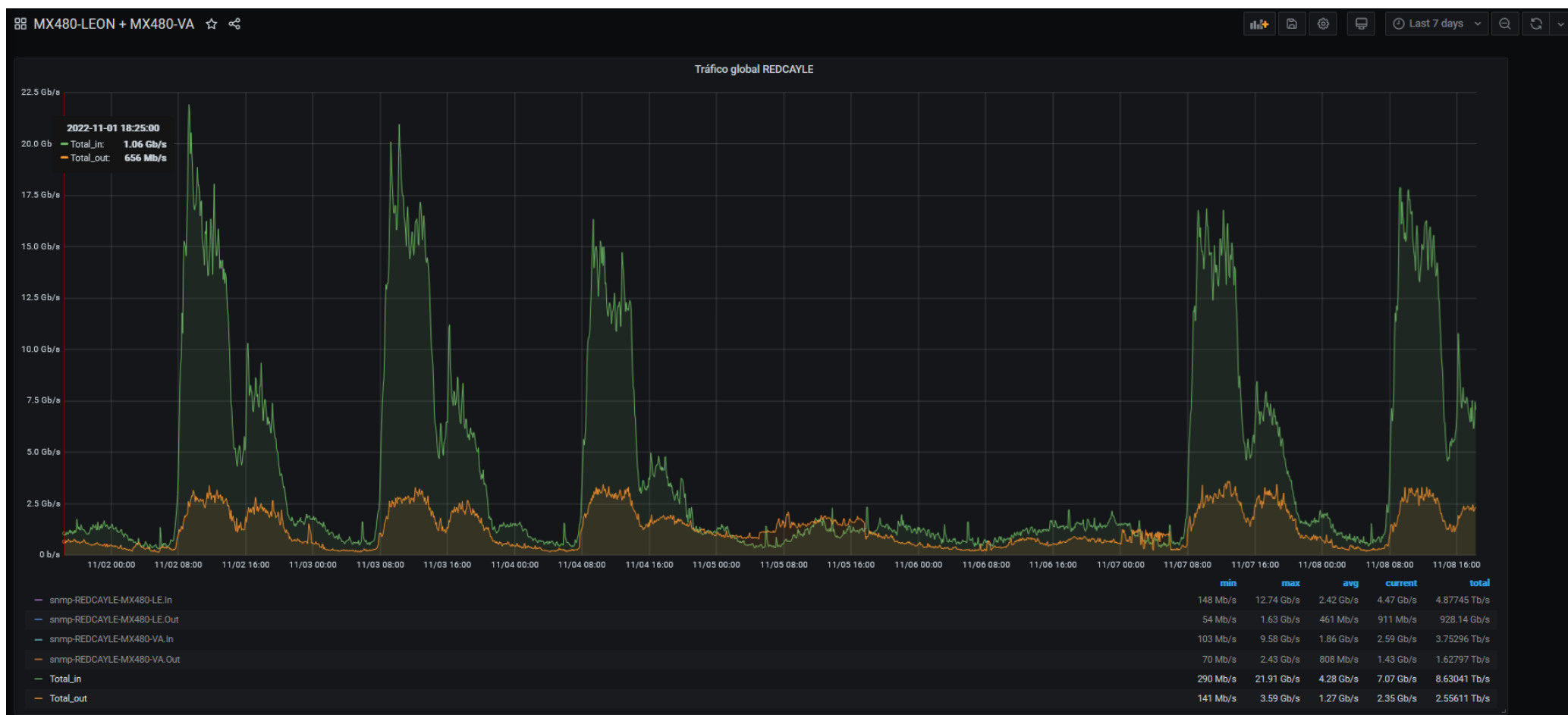
Tráfico IP RedCAYLE





MONITORIZACIÓN

Tráfico Global RedCAYLE



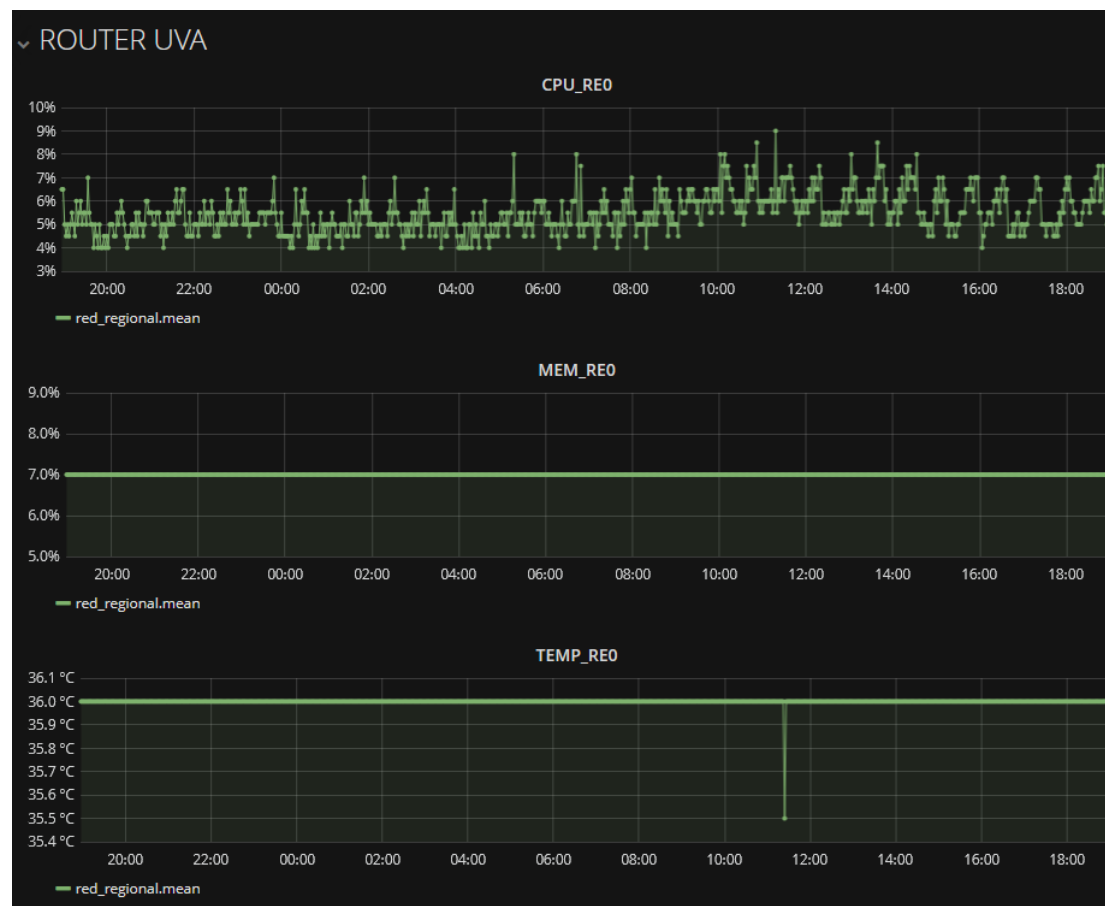


MONITORIZACIÓN

CPU

MEM

TEMPERATURA





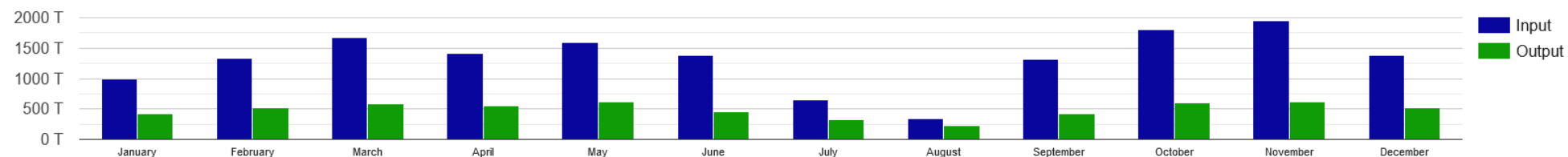
MONITORIZACIÓN

Tráfico Acumulado

	January	February	March	April	May	June	July	August	September	October	November	December	TOTAL
Input	998.28 T	1.33 P	1.68 P	1.42 P	1.60 P	1.39 P	653.38 T	336.34 T	1.32 P	1.80 P	1.95 P	1.38 P	15.86 P
Output	414.77 T	523.11 T	583.30 T	545.85 T	614.42 T	461.63 T	321.29 T	224.48 T	424.76 T	604.58 T	610.79 T	523.40 T	5.85 P

2021

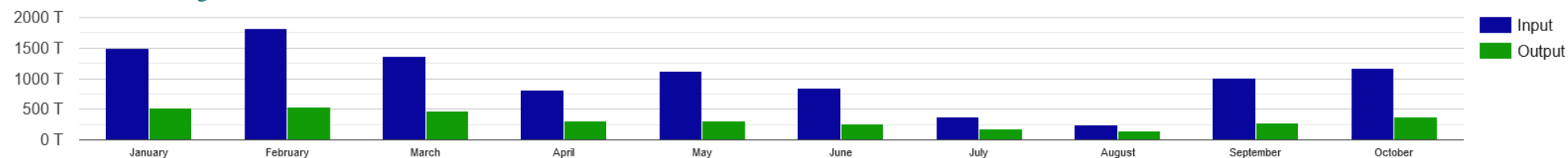
16P / 6P



	January	February	March	April	May	June	July	August	September	October	TOTAL
Input	1.49 P	1.82 P	1.36 P	813.64 T	1.12 P	852.19 T	373.94 T	249.52 T	1.01 P	1.17 P	10.26 P
Output	520.77 T	542.06 T	471.82 T	314.21 T	312.48 T	254.86 T	179.67 T	144.67 T	269.53 T	366.70 T	3.38 P

2022

10P / 3P





MONITORIZACIÓN

Filtros Anti-Spoofing



R_D_Source_IP_Interfaz_USAL



Value	%	Count
Top 5 values		
200.56.1	61.11%	11
248.165.68	16.67%	3
164.214.243	5.56%	1
1.241.202.21	5.56%	1
1.111.174.81	5.56%	1
Others		
89.248.165.86	5.56%	1

a few seconds ago

R_D_PFE_FW_SYSLOG_ETH_IPFW_SCAY...



Value	%	Count
Top 5 values		
164.52.6.130	50.00%	1
89.248.165.68	50.00%	1

R_D_Source_IP_Interfaz_JCYL_COLEGIOS



Value	%	Count
Top 5 values		
8 48.165.68	35.29%	6
8 48.165.86	17.65%	3
1 111.174.112	5.88%	1
1 116.169.61	5.88%	1
1 94.138.80	5.88%	1
Others		
2 8.14.140	5.88%	1
1 61.99.70	5.88%	1
8 46.7.198	5.88%	1
1 126.220.218	5.88%	1
8 48.165.52	5.88%	1

a few seconds ago

Prevención del tráfico con direcciones IP de origen falso
uRPF (Unicast Reverse Path Forwarding)
Aplicado en las interfaces de cliente.

 MONITORIZACIÓN

Control de Logs



ROUTER ESTADO AGREGADOS index set Default index set
ROUTER AGREGADOS
0 messages/second. Must match at least one of the 2 configured stream rules. [Show stream rules](#)

[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)

ROUTER SNMP AUTH index set Default index set
ROUTER SNMP AUTH
0 messages/second. Must match at least one of the 1 configured stream rule. [Show stream rules](#)

[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)

ROUTER VRRP index set Default index set
Detección de cambio en el VRRP
0 messages/second. Must match all of the 1 configured stream rule. [Show stream rules](#)

[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)

STORM CONTROL index set Default index set
Storm control from switches
0 messages/second. Must match all of the 1 configured stream rule. [Show stream rules](#)

[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)

STORM CONTROL (ITACYL) index set Default index set
Storm control exclusively for ITACYL
0 messages/second. Must match all of the 1 configured stream rule. [Show stream rules](#)

[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)

TRAPS INFINERA equipo entró en baterías index set Default index set
traps messages
0 messages/second. Must match all of the 1 configured stream rule. [Show stream rules](#)

[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)

TRAPS INFINERA GENERICO index set Default index set
trap generico
0 messages/second. Must match all of the 5 configured stream rules. [Show stream rules](#)

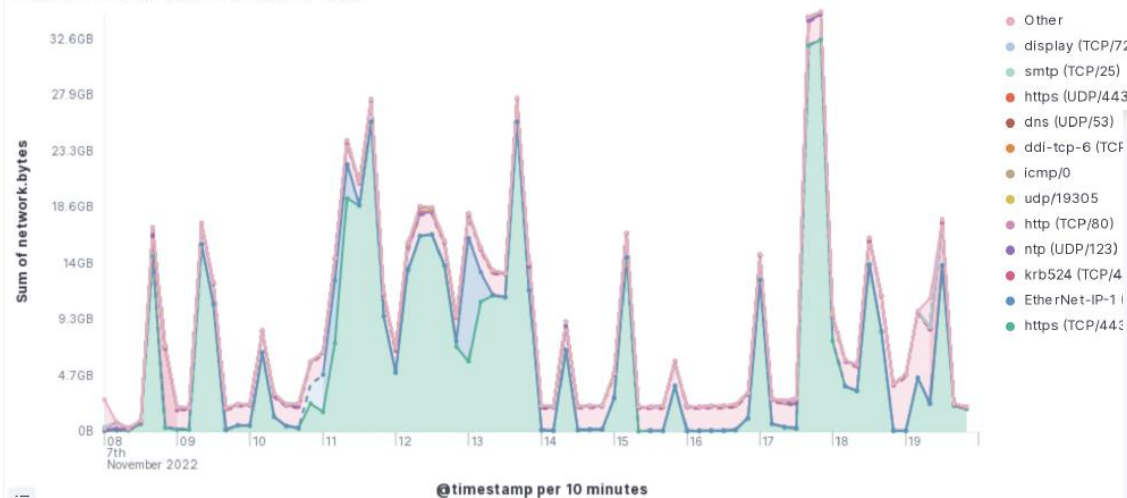
[Manage Rules](#) [Manage Outputs](#) [Manage Alerts](#) [Pause Stream](#) [More Actions](#)



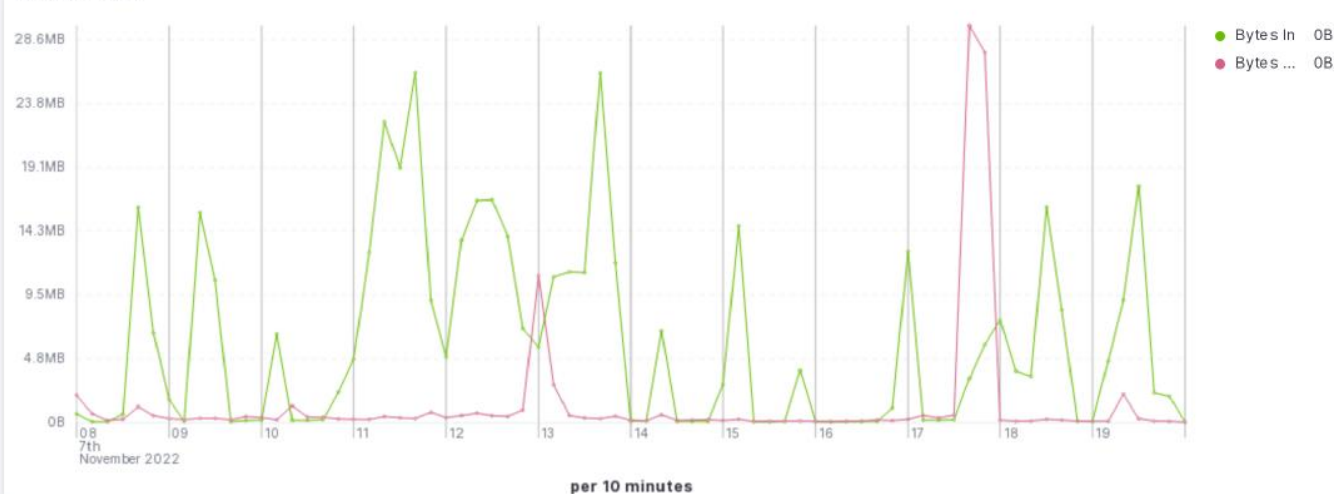
SERVICIOS

Informes por Institución

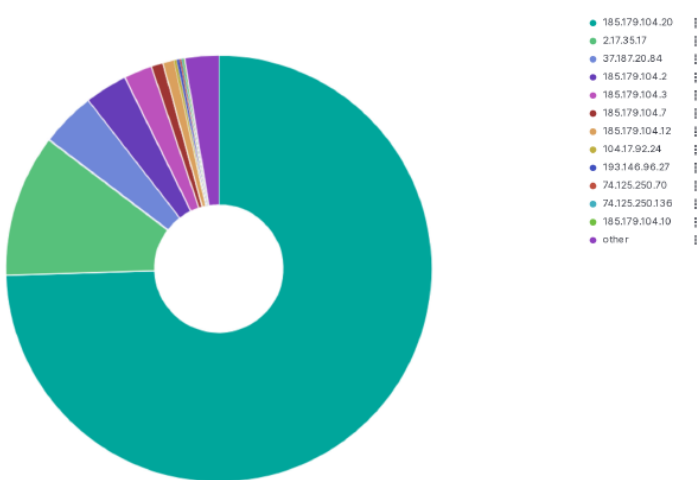
Protocol Summary Stacked Trend Chart - Total



Volume Traffic



Host Summary Pie Chart - From



Host Summary Pie Table - From

Export	
Top Servers	
185.179.104.20	56.5GB
217.35.17	21.6GB
37.187.20.84	16.9GB
185.179.104.2	11.2GB
185.179.104.3	4.7GB
185.179.104.7	4.5GB
185.179.104.12	1.2GB
104.17.92.24	1.2GB
193.146.96.27	694.3MB
74.125.250.70	574.2MB
74.125.250.136	559.7MB
185.179.104.10	13.6GB
other	521.9GB



SERVICIOS

Acceso Monitorización

<https://extranet.scayle.es/>
<https://extranet2.scayle.es/>



Bienvenido al portal de acceso seguro de SCAYLE
Portal SSL-VPN de SCAYLE

Usuario

Introduzca usuario y contraseña.

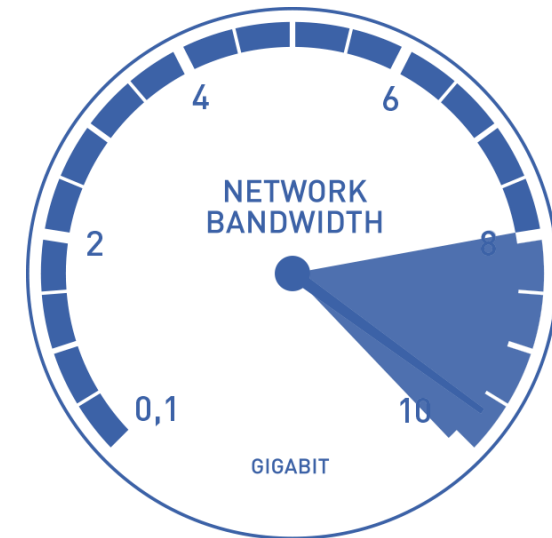
Contraseña

Acceder

IPERF

Mediciones del ancho de banda

Previa solicitud al NOC





Servidores de HORA

tic.redcayle.es

185.179.104.7

Stratum 1 con fuente GPS



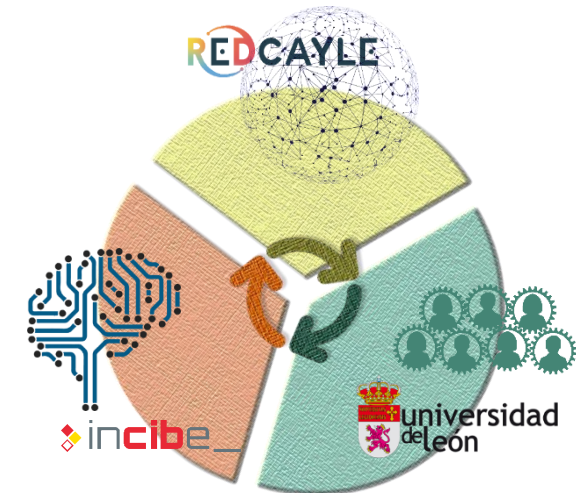
tac.redcayle.es

185.179.104.12

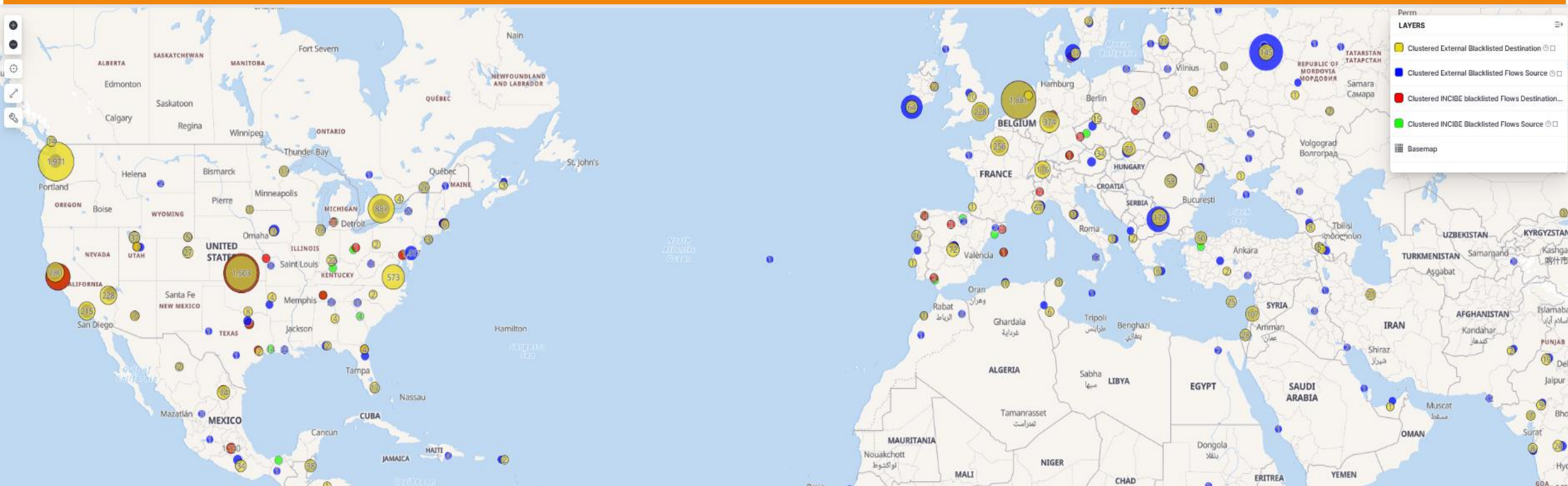
Stratum 1 con fuente GPS

Blacklisted Flows

Nov 8, 2022 @ 08:00:00.000 → Nov 8, 2022 @ 15:00:00.000

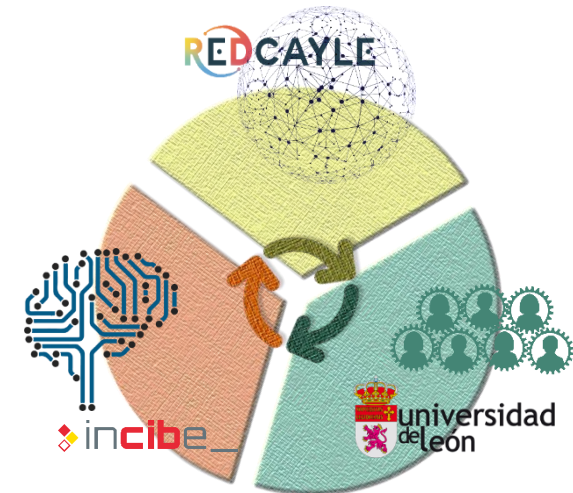


Blacklisted Flows GeoPosition

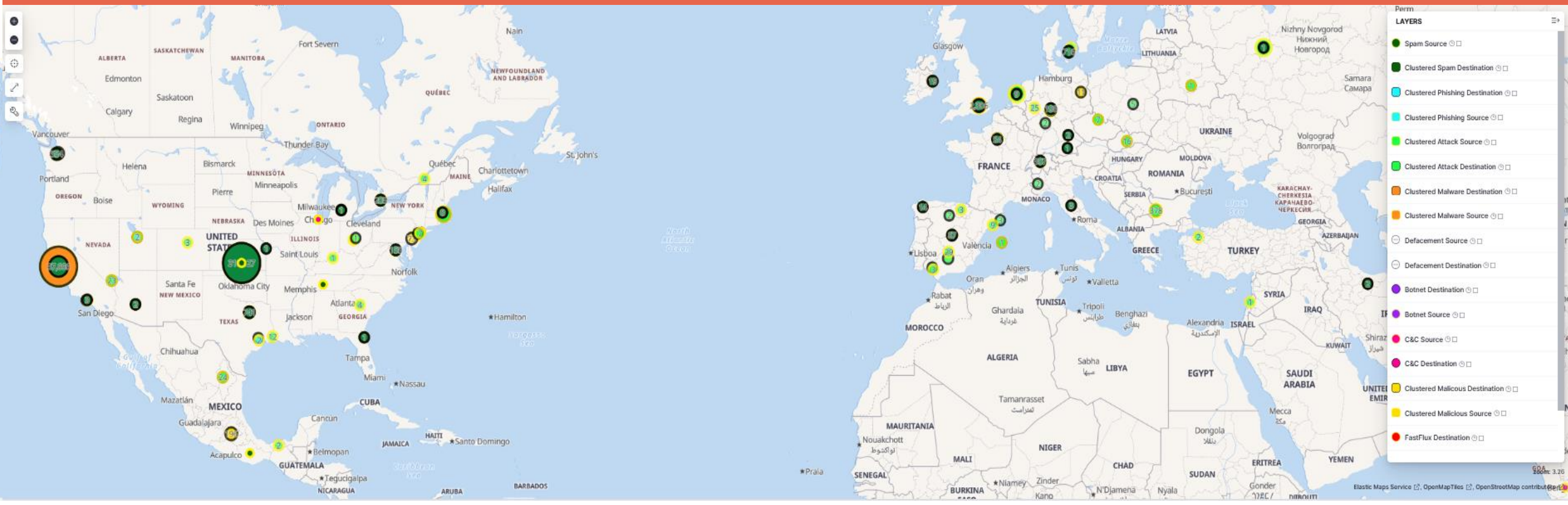


Blacklisted IP por Tipo

Nov 8, 2022 @ 08:00:00.000 → Nov 8, 2022 @ 15:00:00.000

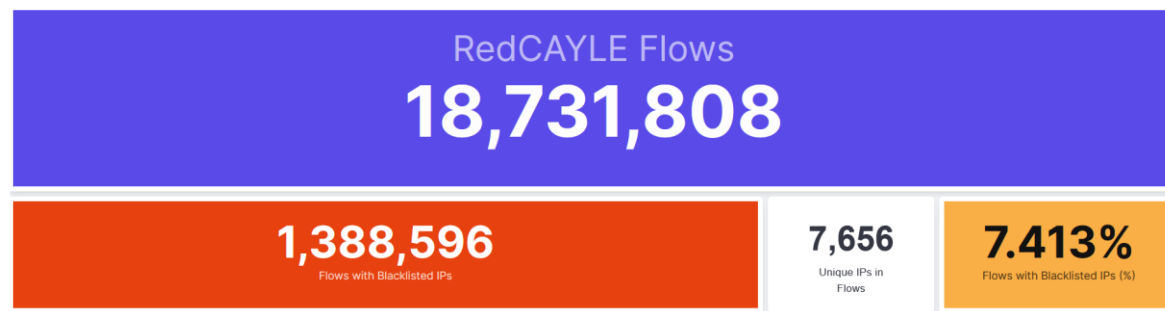


INCIBE Blacklisted Flows GeoPosition by Type



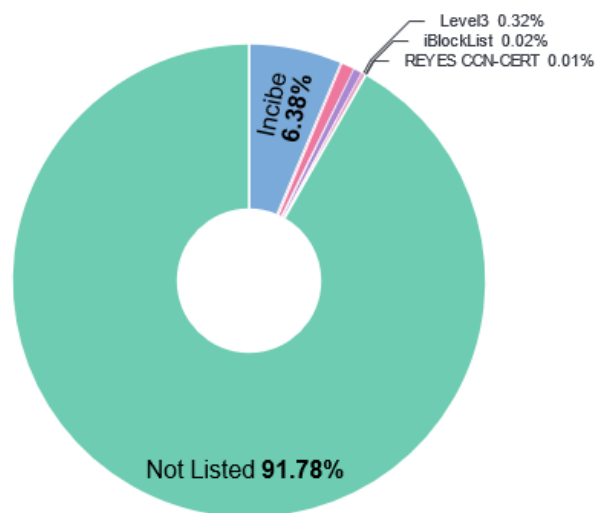
Otros SERVICIOS

Blacklisted Flows

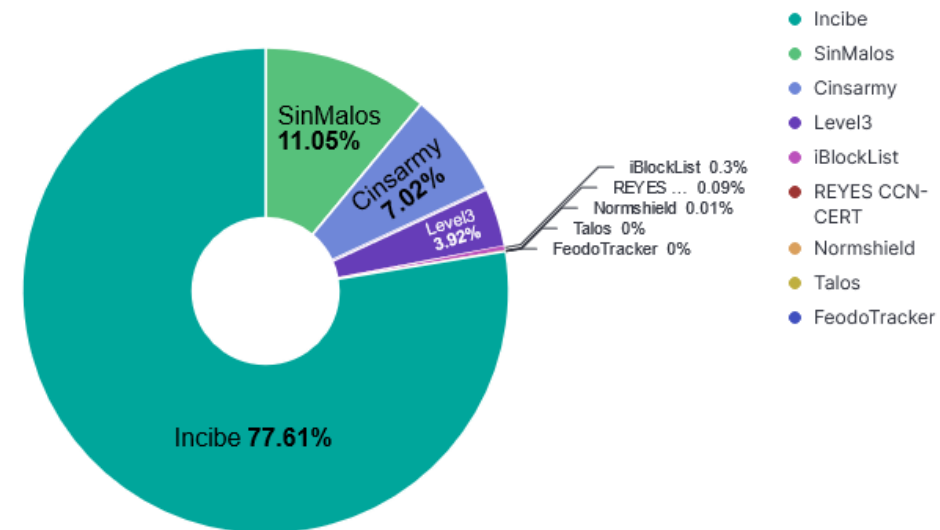


Detailed percentage of Blacklists

Percentage of Flows appearance in Blacklists



- Not Listed
- Incibe
- SinMalos
- Cinsarmy
- Level3
- iBlockList
- REYES CCN-CERT
- Normshield
- Talos
- FeodoTracker



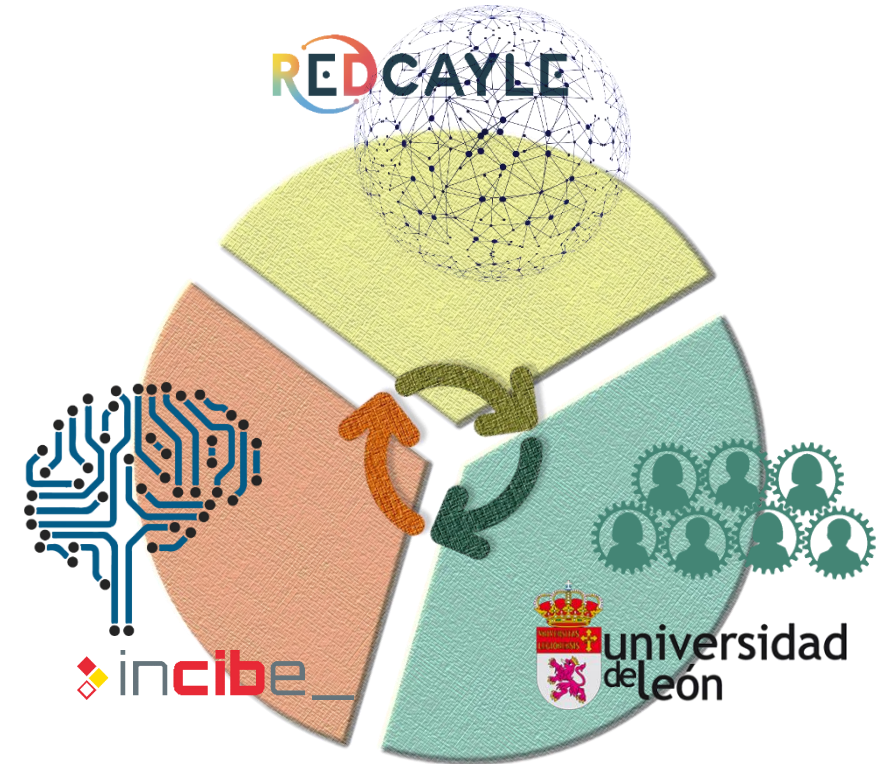
Otros SERVICIOS

¿Qué es FuzzItAll?



- Plataforma para facilitar el proceso de realizar **fuzzing** sobre un proyecto de código fuente, utilizando para ello las capacidades de un sistema HPC
 - El fuzzing es una técnica para descubrir fallos en un software
 - Funciona de manera automatizada o semiautomatizada mediante la introducción de datos inválidos, aleatorios o inesperados a la entrada de dicho software
- Actualmente está en fase de pruebas

<http://fuzzing.scayle.es>



El **fuzzing** consiste en enviar datos aleatorios, inválidos y no esperados de entrada de una aplicación buscando alguna vulnerabilidad en ella.

MEJORAS

- **Migración Red 100G**
- **Nuevo Sistema de Monitorización**
- **Servicio Blacklisted IP**
- **Incorporación de nuevas Entidades**
 - **Academias Militares**
 - **Sistema Videovigilancia Incendios**

Muchas gracias

marivi.lopez@scayle.es

España | digital ²⁰₂₆



universidad
de león

NOS
IMPULSA



Junta de
Castilla y León



FONDO EUROPEO DE
DESARROLLO
REGIONAL



UNIÓN EUROPEA



Unión Europea
Fondo Europeo
de Desarrollo Regional
"Una manera de hacer Europa"