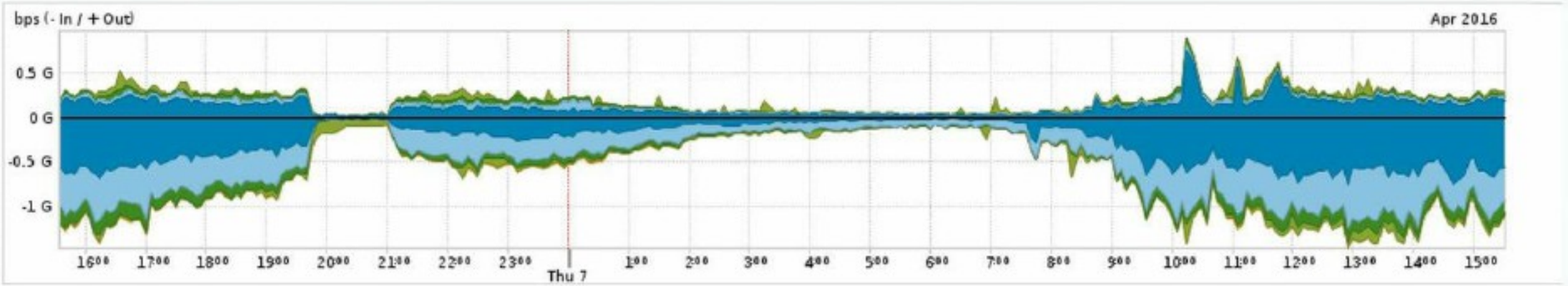
Monitorización de los dispositivos de Red (perimetral)

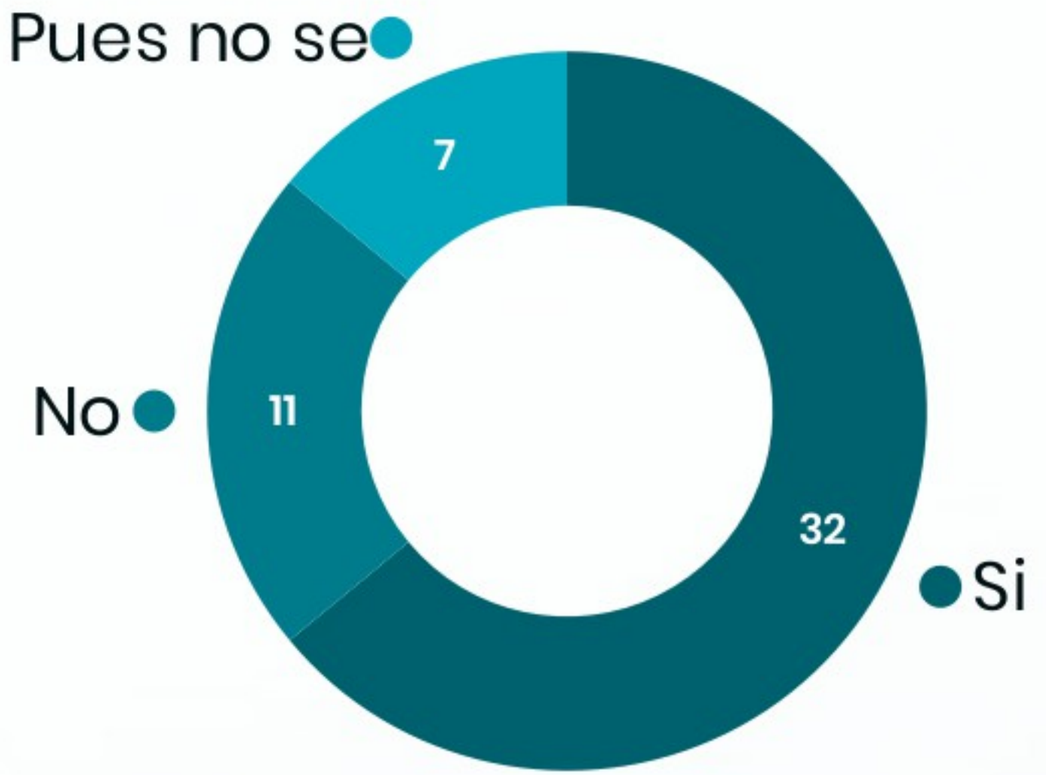
Francisco Monserrat

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
Red IRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

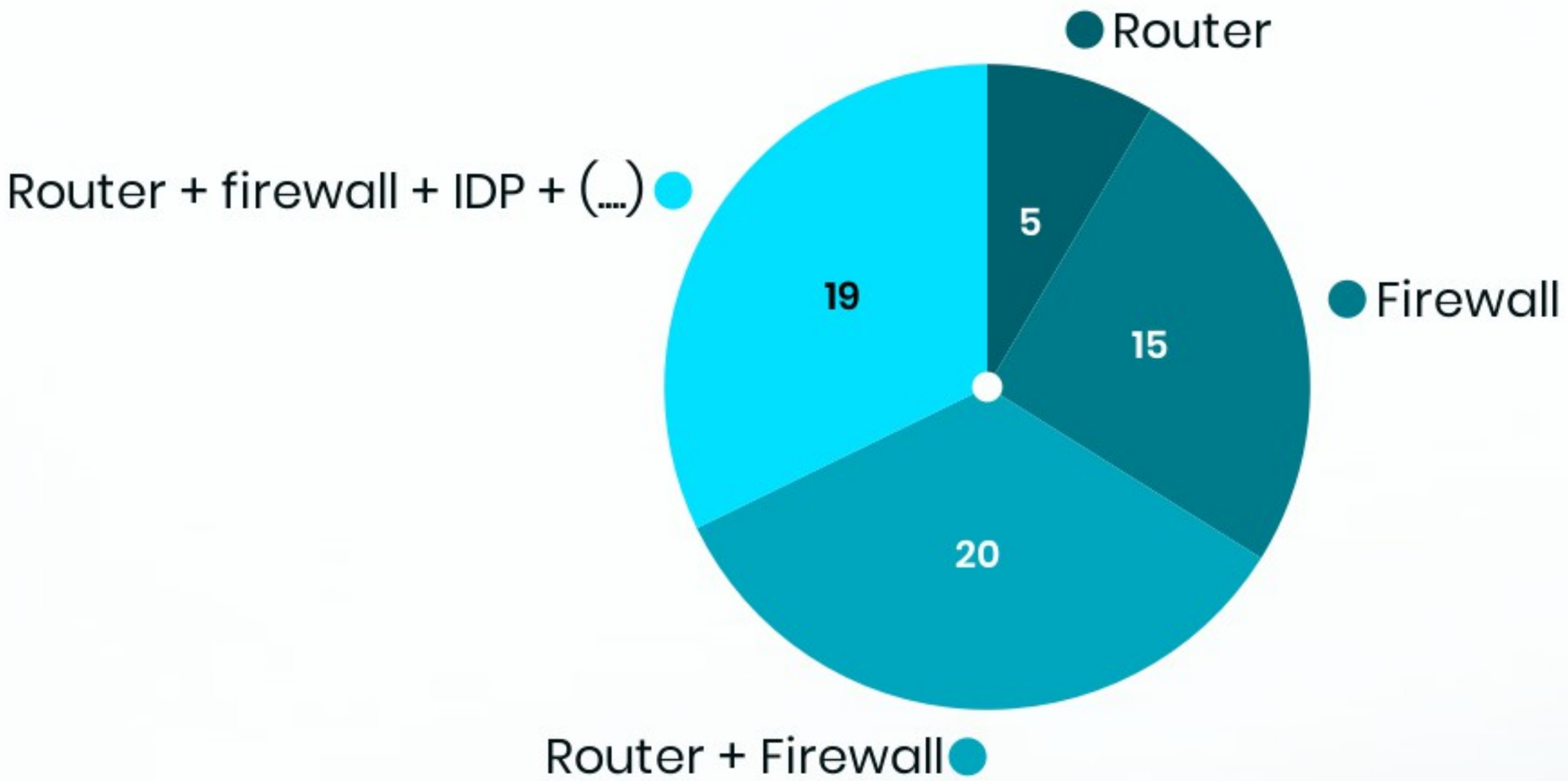
A traffic drop



¿Habeis tenido caidas de este tipo ?



¿Que teneis en vuestro perimetro ?



¿como lo detectais ?

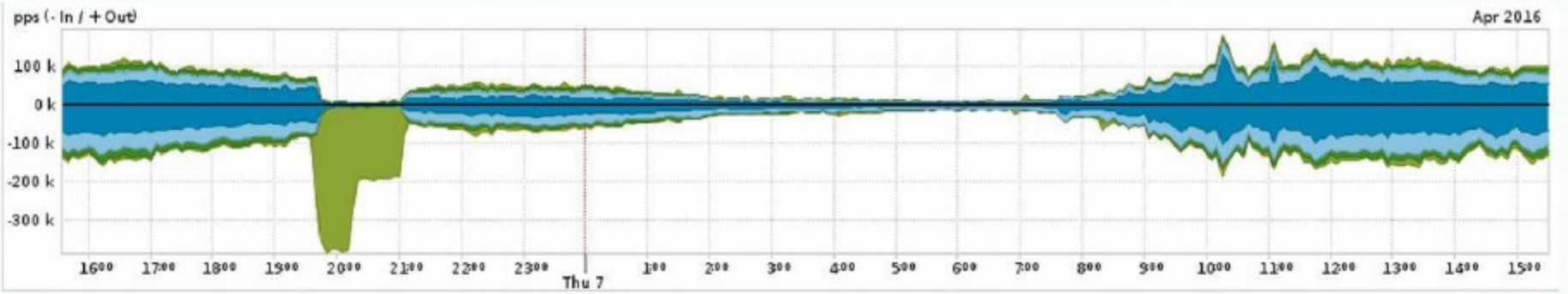
Por los usuarios

Por alarmas del dispositivo

¡¡ Sorpresa !!

A posteriori

Non volumetric attacks



FW Limit

- El numero de sesiones establecidas (que suele ser muy alto)
- El numero de sesiones de detección (IDs/IDP) que pueden tener / establecer por segundo
- El número total de sesiones que se pueden establecer por segundo.

Soluciónes:

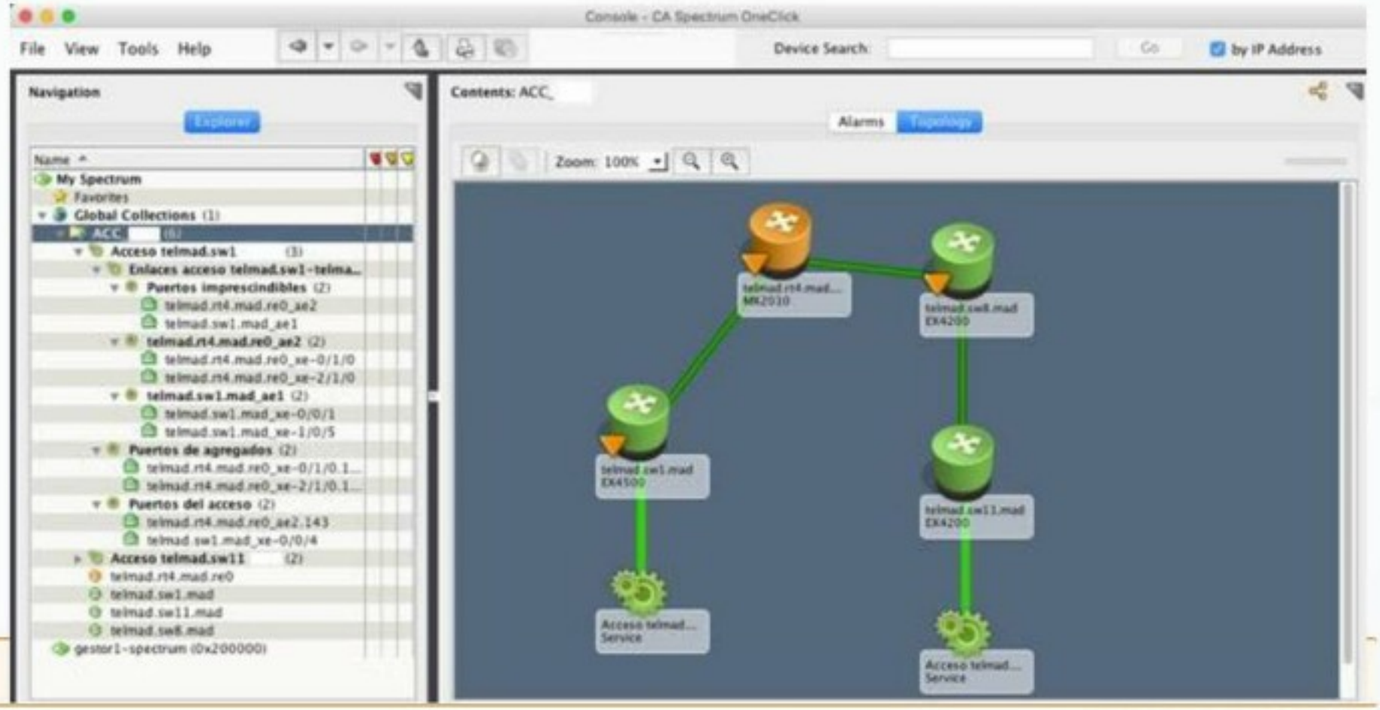
- Dispositivos de protección para el FW
- Reglas de mitigación y descarte de trafico
- Limitaciones de trafico por zonas geográficas , protocolos, etc.

Problemas:

- Valores “umbral” dependientes de cada instalación
- Información dependiente del vendedor .

¿Que monitorizar ?

- Contadores clasicos:
  - Paquetes por segundo.
  - Bytes por segundo.
- O más elaborados :tamaño medio del paquete
- No en el dispositivo.
  - Netflow
  - Router



¿Qué falta ?


bgp
concienciación
comunidad
central mon rediris
firewall as a service
personal
gatitos
yippy
pasta
coordinación
necesitamos un paco
dos o tres pacos
sonda
dinero
apco

Page 10 - gt2018-mediciones.pptx

Red IRIS

THANK YOU VERY MUCH!

GOBIERNO DE ESPAÑA | MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES | MINISTERIO DE ECONOMÍA Y EMPRESA

red.es

RedIRIS