DDOS in academic Networks

Grupos de Trabajo 2014.

CSIC. 4 de Junio 2014

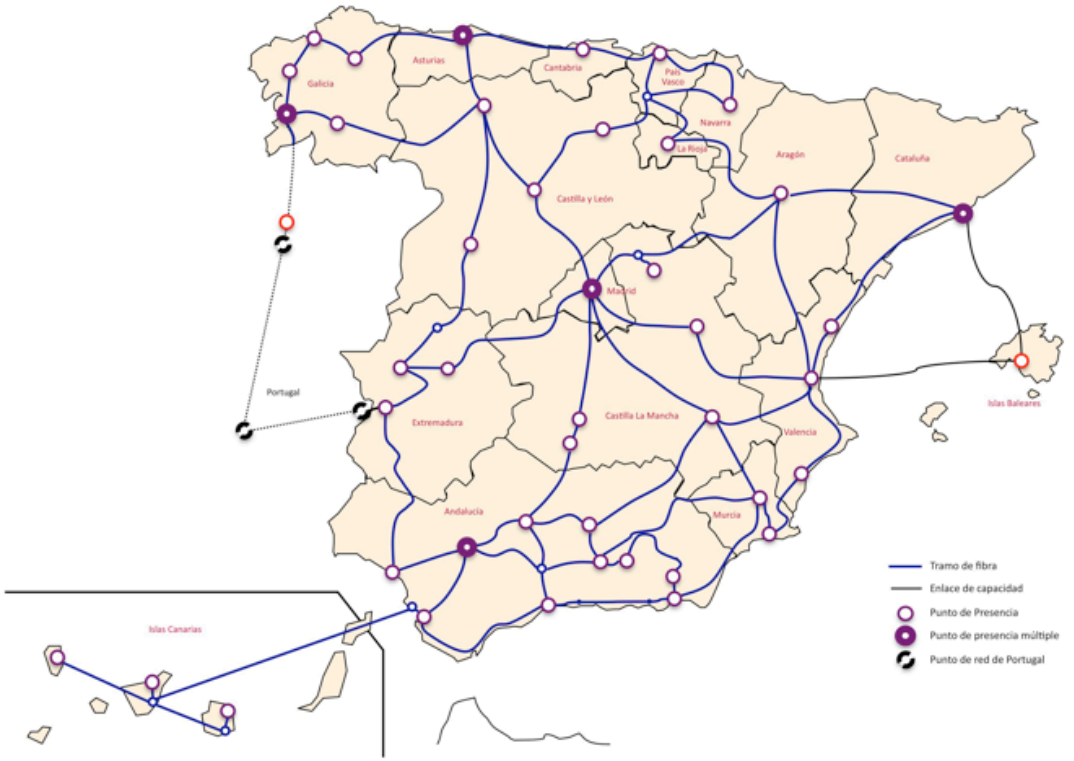
GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

Academic networks ?

- Real Target for DDOS ?
- Lesson learned; DDOS @RedIRIS
- Mitigation Projects

About RedIRIS

- Spanish Academic & research network ….
- Universities, research centers, ….
- Not schools for now
- But also a lot of government organizations



In a far NREN a long time ago …

- We were not critical targets
  - Users were mostly University & research centers
  - Open Networks, public internet & big internet pipe…
  - Used for DDOS but not real target for DDOS
  - Sometimes received a DDOS attacks against non critical servers (IRC wars, etc).
  - Internet was for fun (not a utility)

But now …

- “Internet can’t be down”. Organizations need internet connection.
- DDOS is not only for script kiddies , but still is quite easy to launch DDOS attacks.
  - DDOS as service
- Bandwidth is a shared resource between the research centers .
  - A DDOS affect other links and organizations that share the same link

Prevention

- Be prepared: Basic Risk Analysis
  - What services need to be online ?
  - What is the impact if service XX is not working/offline , etc?
- What can be done to prevent this Risk ?

  Traffic analysis & monitoring.

  Segregation of traffic.

  Knows your internet provider …

Case 1. Real DDOS

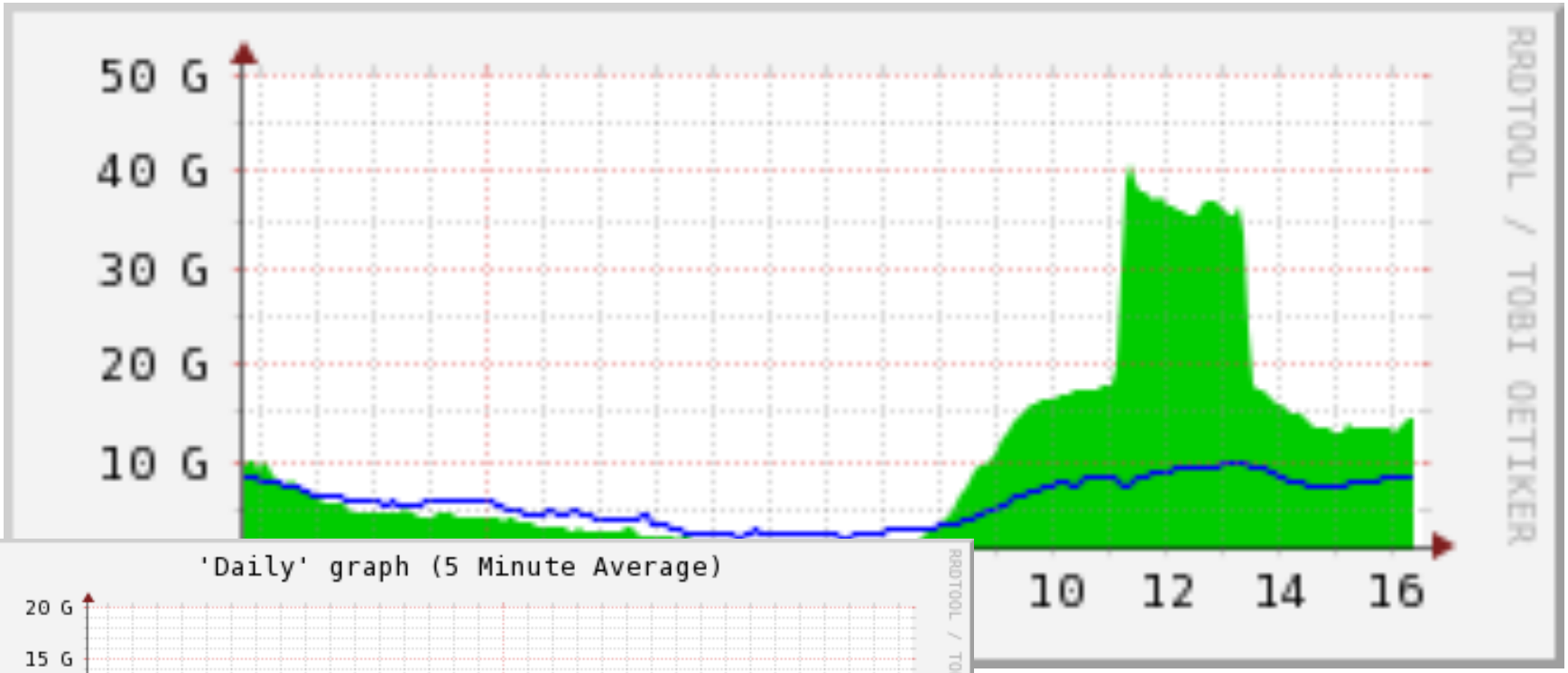
- DDOS announced against one organization
  - Contact with the security contact
  - Warm about the DDOS
  - Do the dailyjob…

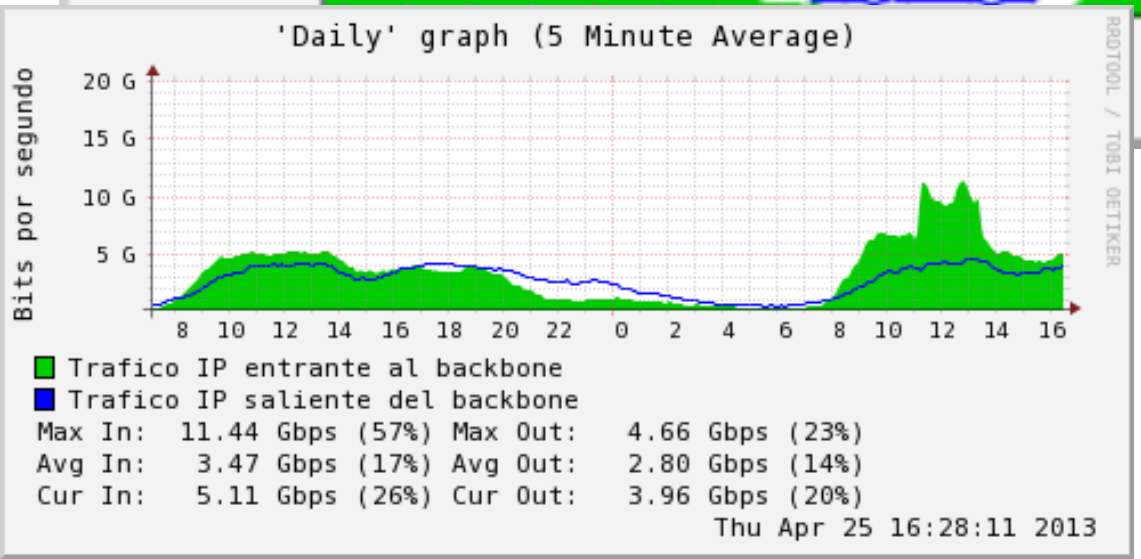
- No real preparation for the DDOS attacks

Case 1. Real DDOS

- Bad timing
  - If something could fail it will fails.
    - RedIRIS NOVA backbone migration
    - Training session day for staff
    - Other people attending meetings & workgroups
  - No Previous feedback from the organization
  - Some time trying to contact the right person inside RedIRIS

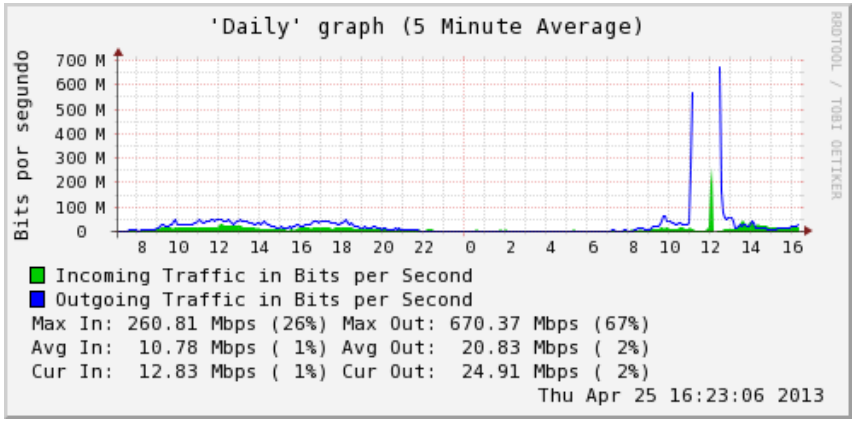
A big bunch of traffic

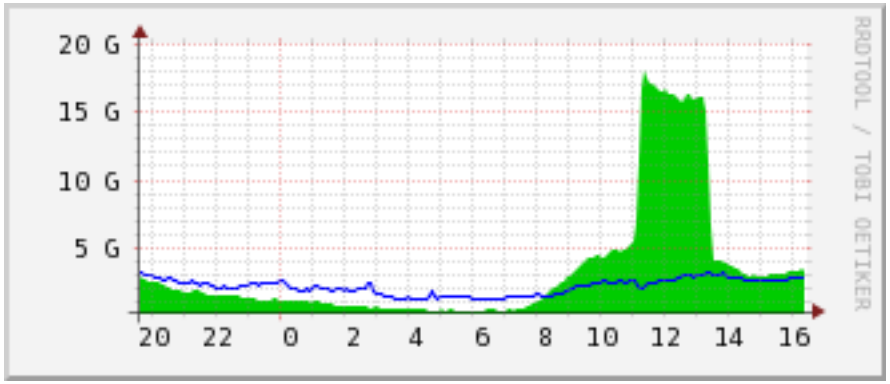




Case 1: Not only a customer DDOS

- This traffic impact also in our backbone infrastructure
- Customer links completely saturated
- Traffic analysis show port 80/UDP traffic against web server.
- 400 sources outside RedIRIS network→ Applied filtering in outside peerings connections.
- Contact international ISP security contacts to block & filters the bots





Case 1. Conclusions

- What we learn..
  - To prepare in advance for the DDOS.
    - Traffic monitoring, what is the “normal” traffic.
    - Prepare (In advance) border filtering rules.
    - Define the contact point.
  - Prepare mitigation &contention strategy.

Case2. best preparation

- Another DDOS, this time the organization contacted with RedIRIS CSIRT.
- Time to prepare in advance, but no “magical device” to mitigate the DDOS.
- Closely work with the customer.

Case2. Working with the organization.

- Explicit separation of traffic, users (generated traffic & outside web connections traffic).
- Internal traffic analysis with client confirmation of allowed traffic .
- Prepare to block foreign traffic to the client if needed.
- Static web pages generated
- Setup a machine in RedIRIS premises with static web content.
- Apply filters in peerings links several days before the DDOS. (block not allowed traffic)

Case2: Setting a external web cache

- If there is too much HTTP traffic , this can be redirected to the external cache using BGP injection.
- The IP is “removed” from the client network and placed in the provider datacenter.
- External web cache will reply with the contents.

Case 2: External server vs extenal cache

- Difficult to configure an external web server:
  - “static” means different things.
  - IIS usually don’t care about lower & upper case.
  - Virtual paths, etc.
  - Hardware configuration for high bandwidth web server .
- Better to move to a “web cache farm”

Case 2. Leason learn.

- Not always a DDOS warning is a DDOS attack.
- Good preparation and filtering in place, work closely with the client.
- “Hosting on demand” is top much time/ resource costly, move to a external web cache.

Case 2: Web cache farm

- Static content on client webserver.
  - Use another IP address for cache client connection
  - Redirect web server IP address to cache farm.
  - Cache farm will assume client IP addresses. , retrieve and cache the static content.
  - Apply security configuration in web cache.
    - Limit query rate
    - Applied security profiles

RedIRIS new network services

- Current lines of work:
  - BGP redirection of traffic.
  - Deploy a derivation network. 3Q-2014
  - DDOS mitigation tools. 4Q-2014
  - Service for projects.
    - Self IP address blocking 3Q-2014
    - On demand temporal cache 3Q-2014 (tested)
    - On demand DDOS mitigation (4Q-2014)

SELF IP blocking

Autobloqueo de direcciones IP de la organización en el bloqueo

Solicitud por parte del PER

- Rango IP
- Router BGP de organización.

SELF IP blocking

Autobloqueo de direcciones IP de la organización en el bloqueo

Establecimiento sesión BGP

- Solamente /32
- Limitado a X anuncios
- Limitado a blackhole

SELF IP blocking

Autobloqueo de direcciones IP de la organización en el bloqueo

Ante un problema la institución realiza el anuncio de la dirección IP.

Cache temporal

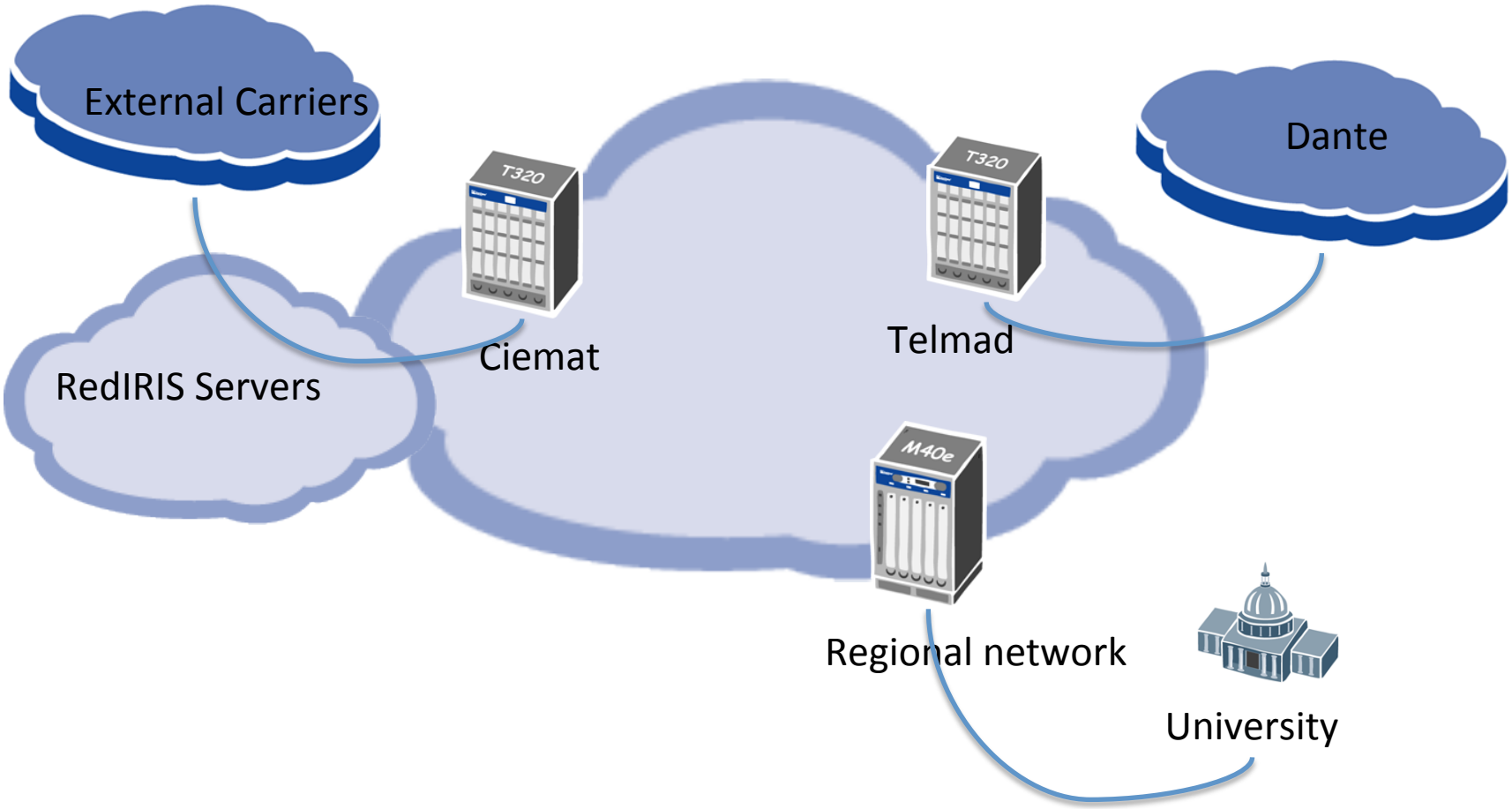
- Cache temporal HTTP
- La dirección IP del servidor WWW es anunciada en el backbone y dirigida a un equipo de cache.
- El equipo cache es configurado con la IP del servidor para responder a las consultas a la página.
- Internamente el servidor cache reencamina la consulta a otra dirección IP de la organización donde estén los datos.

- Solución cuando se preeve un aumento significativo de trafico HTTP , por demanda o DDOS

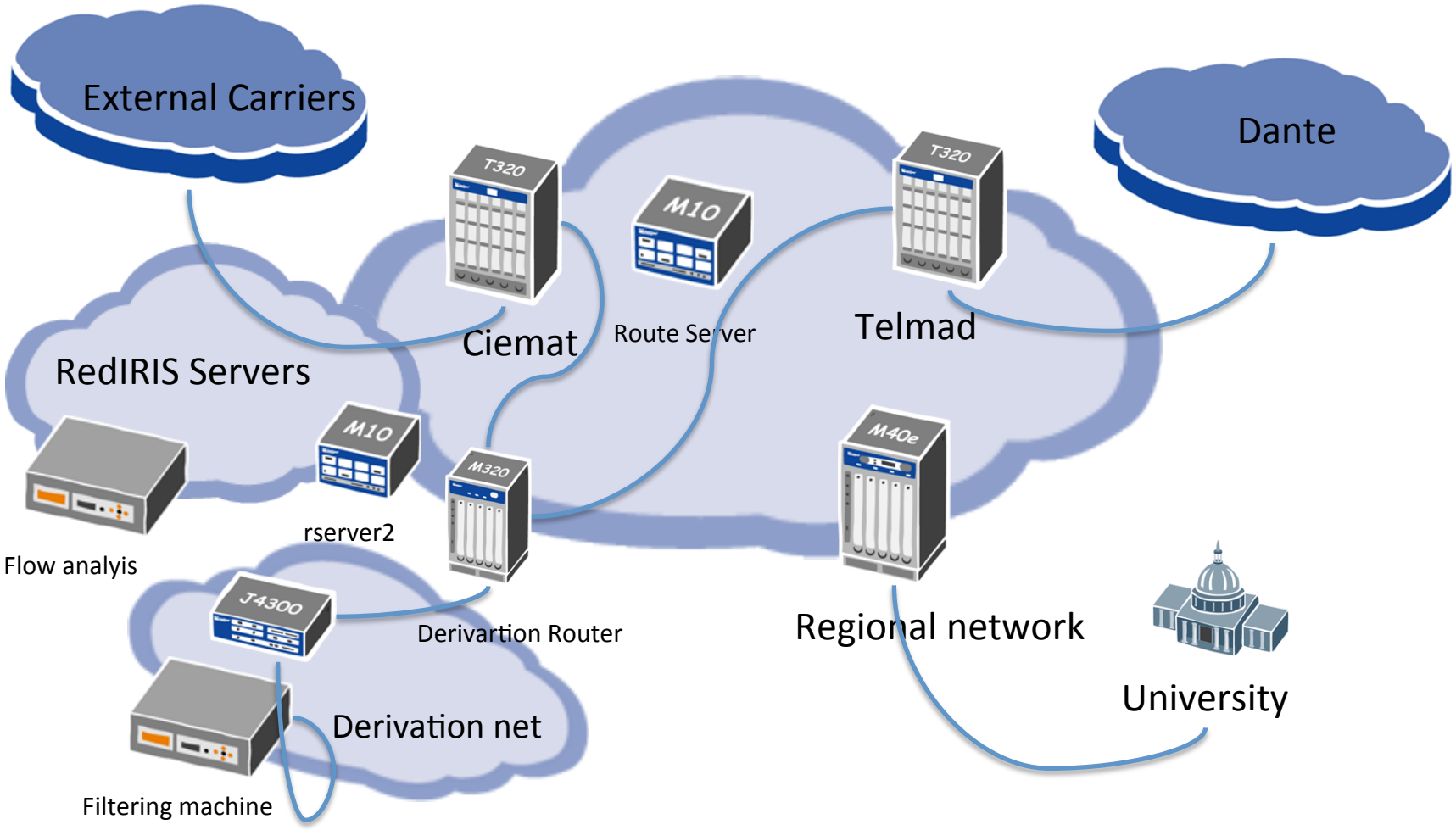
Mitigación DDOS

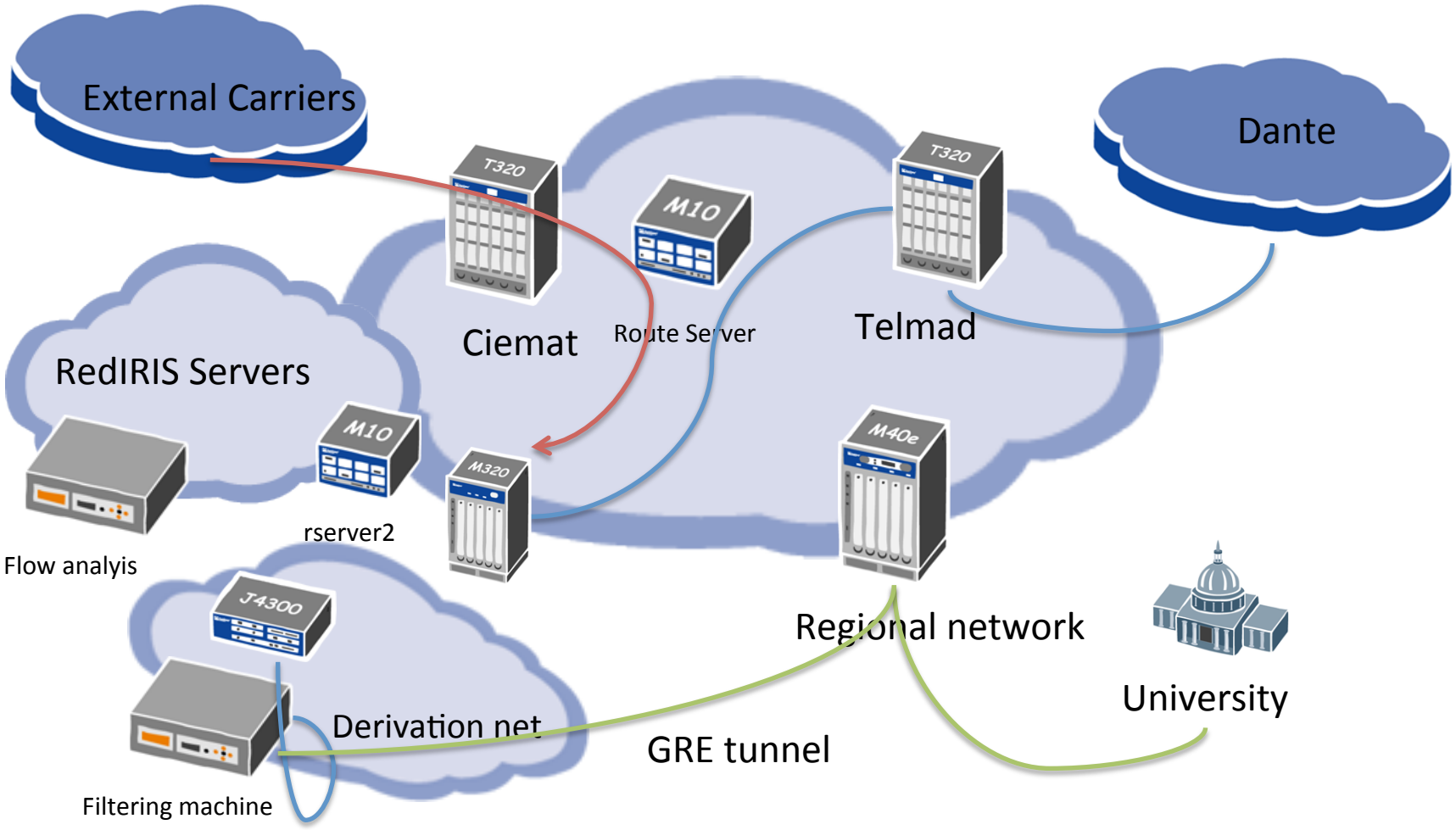
- Equipos de limpieza de trafico ante DDOS
- Objetivo: mitigar los problemas que un DDOS puede causar al backbone de RedIRIS
- Requiere planificación previa , documentación de trafico y configuraciones en las instituciones.

Network: current



Derivation network in place




External Carriers
Dante
T320
M10
T320
Ciemat
Route Server
Telmad
RedIRIS Servers
M10
M320
M40e
rserver2
Flow analyis
J4300
Regional network
University
Derivation net
GRE tunnel
Filtering machine

¡Muchas gracias!

Más de 25 años al servicio de la investigación