Luciano Minuchin – CIO

Sebastian Motta – CSO

NIC ARGENTINA

Security Infrastructure NIC.AR

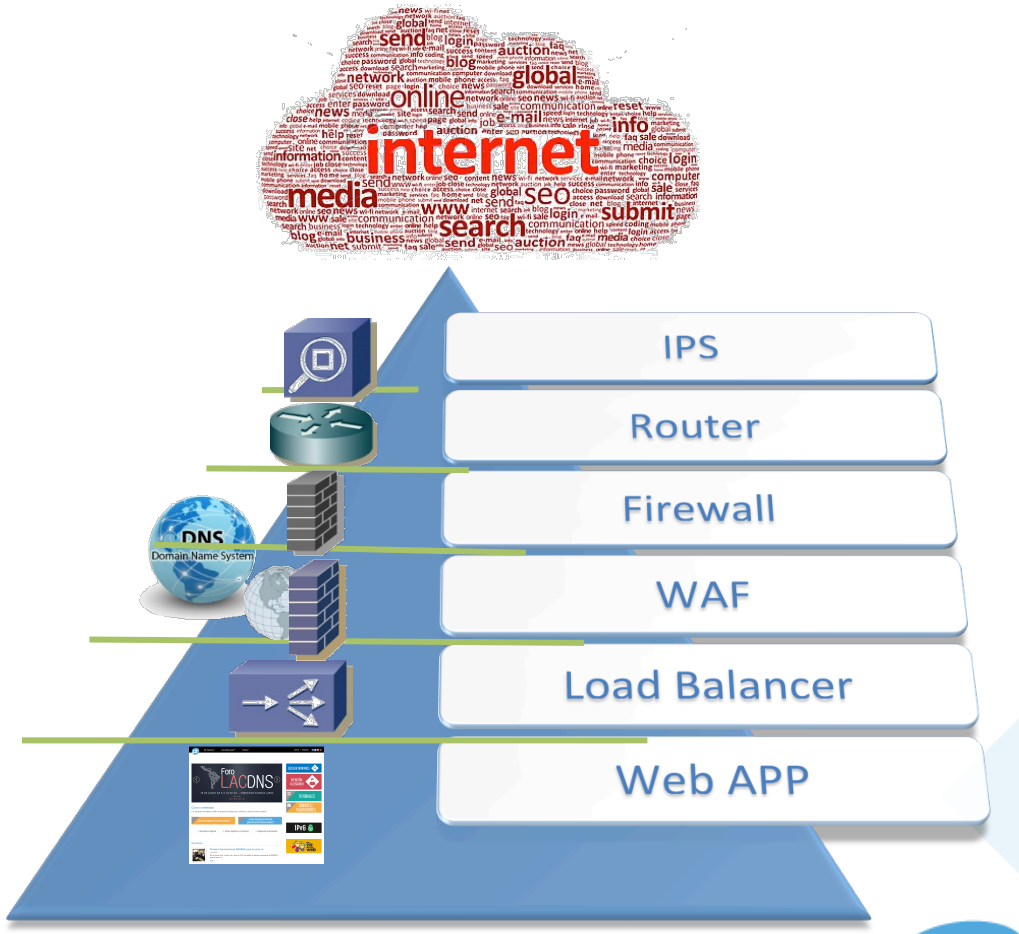
The security structure was increased by installing hardware in different physical layers.

New security policies were defined and applied specific traffic behavior policies.

Firewall rules were applied to limit public access.

Load Balancer system was installed to distribute the traffic load on different servers.

A redundant structure for the entire platform is made. Links to Internet, servers, routers, etc.

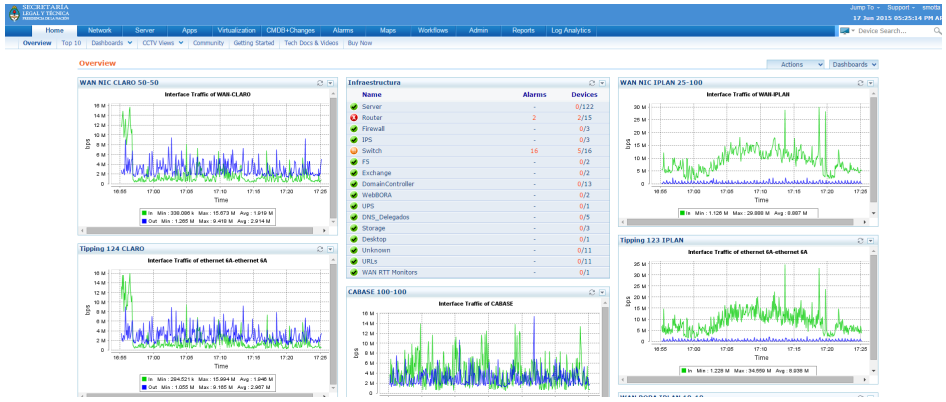


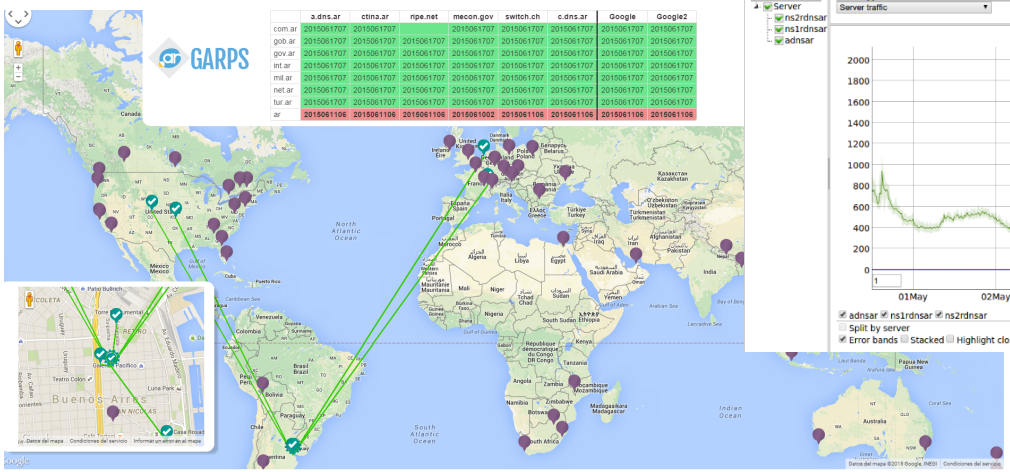
Monitoring and Statistics

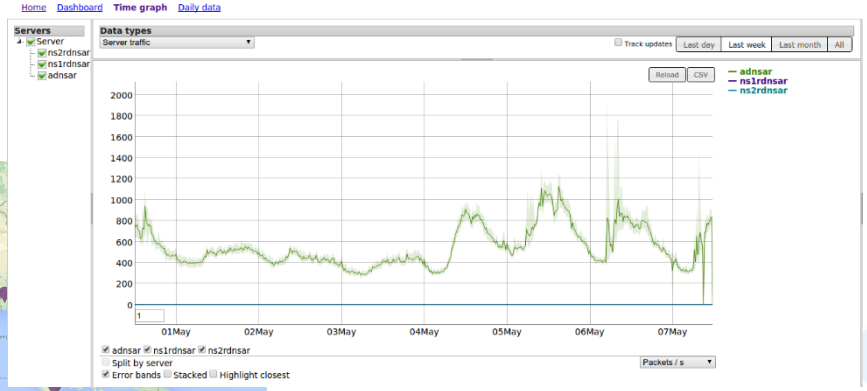
New monitoring traffic by type, to understand the use.

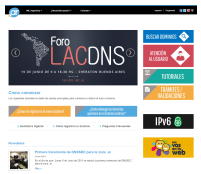
DNS servers new statistics were collected worldwide.

The health of our servers and their replicas monitoring tools were developed.









Attack 04/05/2014 - Details and Learning

Details:

Our first contact with Anonymous and DDoS attacks.

For several hours they maintained an intense UDP packets sent to various ports on the NIC AR WEB servers using hundreds of different IP origins.

Having a strong infrastructure of firewall and security equipment the attack failed to penetrate nor violate any critical system, but internet connections reached 100% capacity or causing a drop time out of service.

Resolution:

After several hours trying to mitigate the attack without obtaining positive results, we chose to disconnect all ISPs saving one that implemented a series of Access List in their routers so the connection is not saturated.

Conclusion:

As much as the provision of a strong enough security infrastructure is very complex avoid saturation of service without the help of ISPs on DDoS attacks.
It was determined that the use of the website is much criticism within the country and globally is very important to have as many anycast networks.

Chalenges:

Improve communication with the ISPs.
Log redundancy and expand the local IPX.
Check our Internet publication to restrict public access.

Improving monitoring systems to detect attacks faster.

Extend the Anycast DNS network.

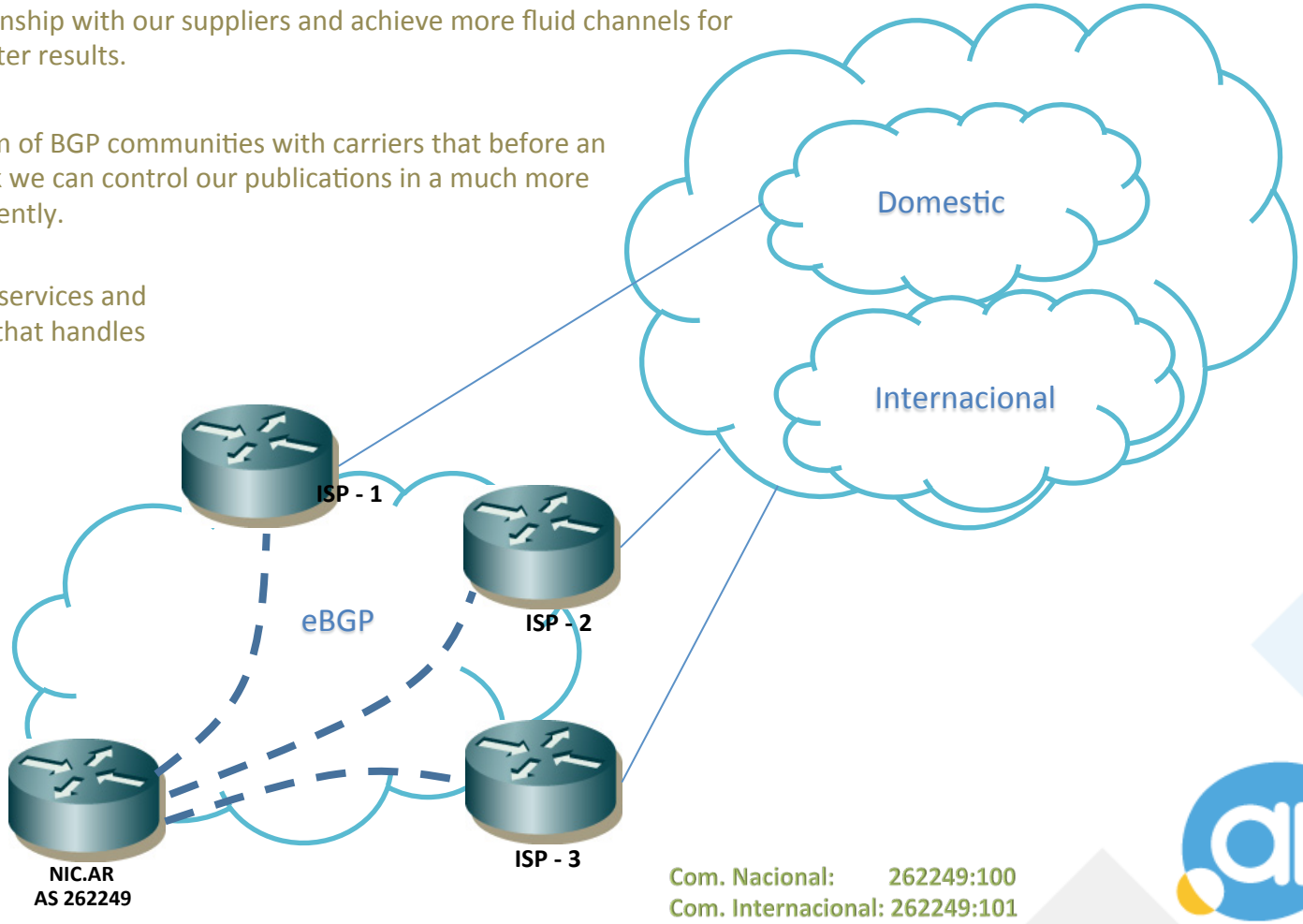
Create a CSIRT in order to combat these attacks as any cybercrime that may arise whether domestic or international.

1º Paso: ISPs, BGP y Redundancy

Improve the relationship with our suppliers and achieve more fluid channels for communication faster results.

Implement a system of BGP communities with carriers that before an international attack we can control our publications in a much more agile and independently.

Add more Internet services and connect to the IXP that handles domestic traffic

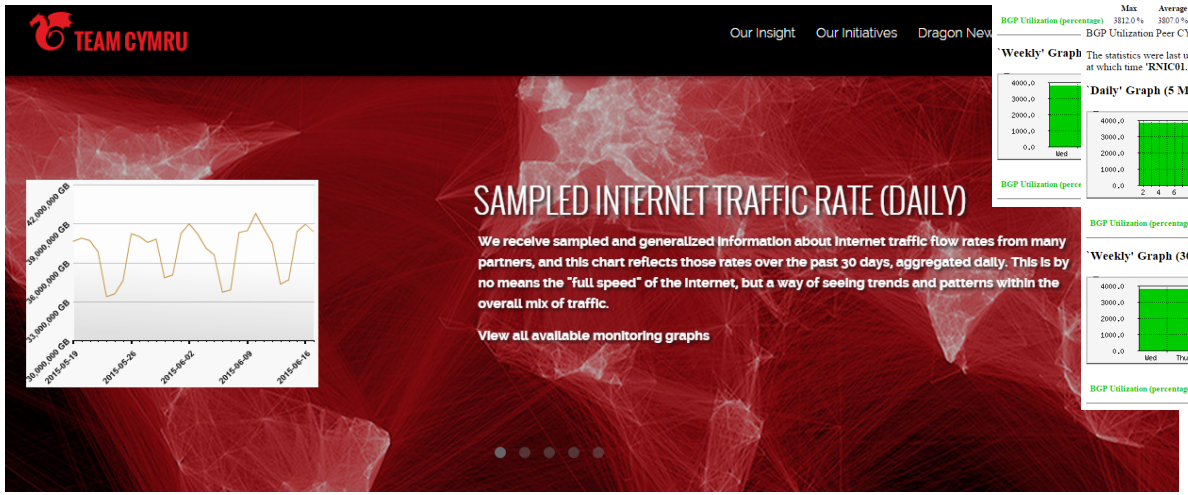


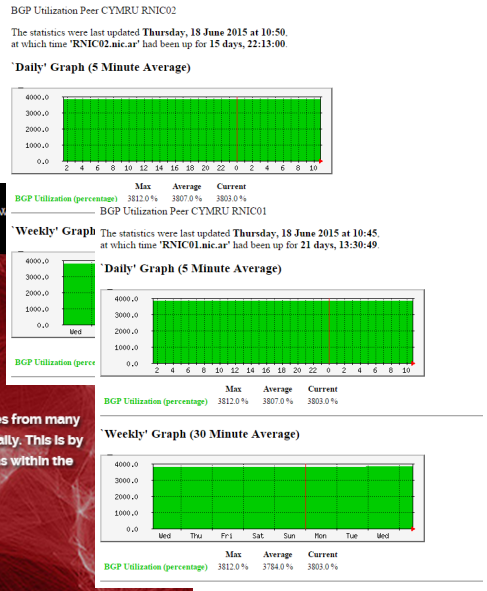
Com. Nacional: 262249:100
Com. Internacional: 262249:101

2º Paso: Conexión con Team CYMRU

Team Cymru provides a free service that lets through a BGP session IPv4 / IPv6 stay informed about bogons networks - Netblocks - etc.

To connect with them allowed us to filter both inbound traffic as corresponding to different types of attacks and botnet.





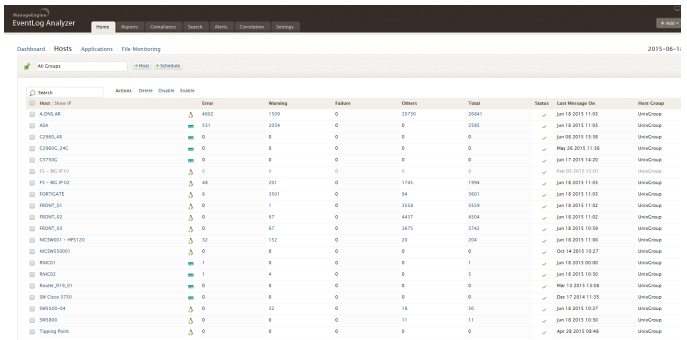
3º Paso: Monitoring– SIEM – Netflow – External Reports

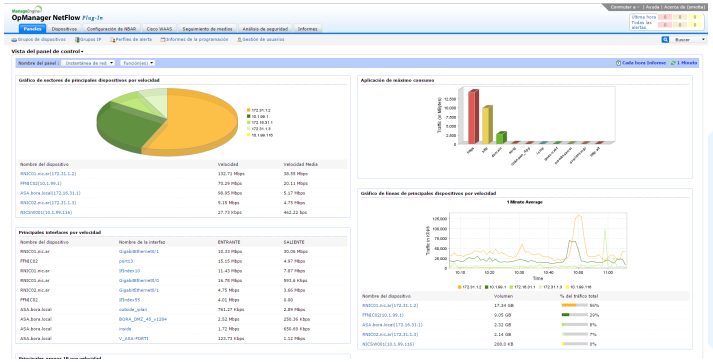
Monitoring systems to detect attacks were improved more quickly.

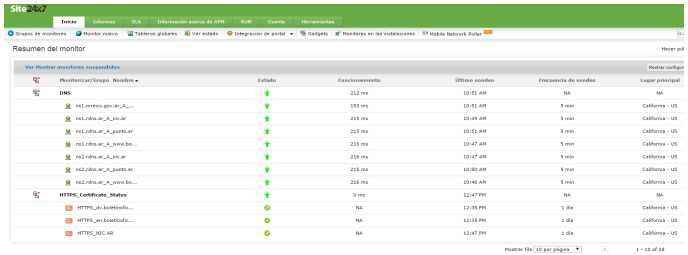
System statistics using NetFlow alerting changes in behavior or the use of unauthorized protocols are installed.

SIEM to visualize any unusual behavior easily and teams see errors more clearly.

External reporting system that allows monitoring the state of the network from different parts of the world and have a system of alerts to external infrastructure.







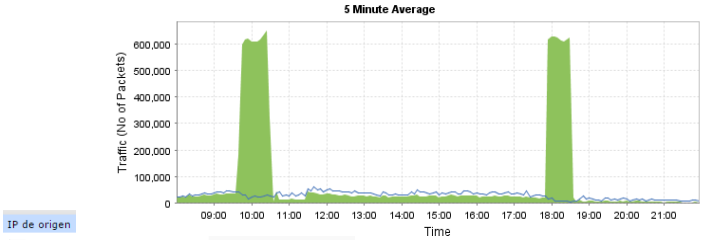
New Attaks

Since the first attack we suffered until now were recurrent attacks on our site and servers from port scanning to DDoS.

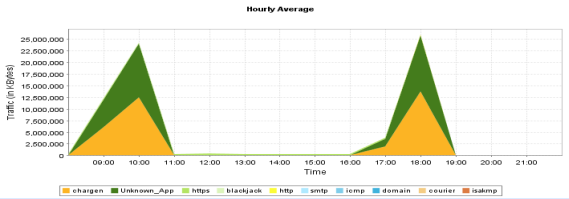
After the changes we have to face these attacks without suffering full service cuts.

Many of the attacks were detected by the alarm system allowing quick actions and complete them on time.

In the case of DDoS through expanding bandwidth, agreements with suppliers and filters communities, achieved withstand denial of service without leaving service.

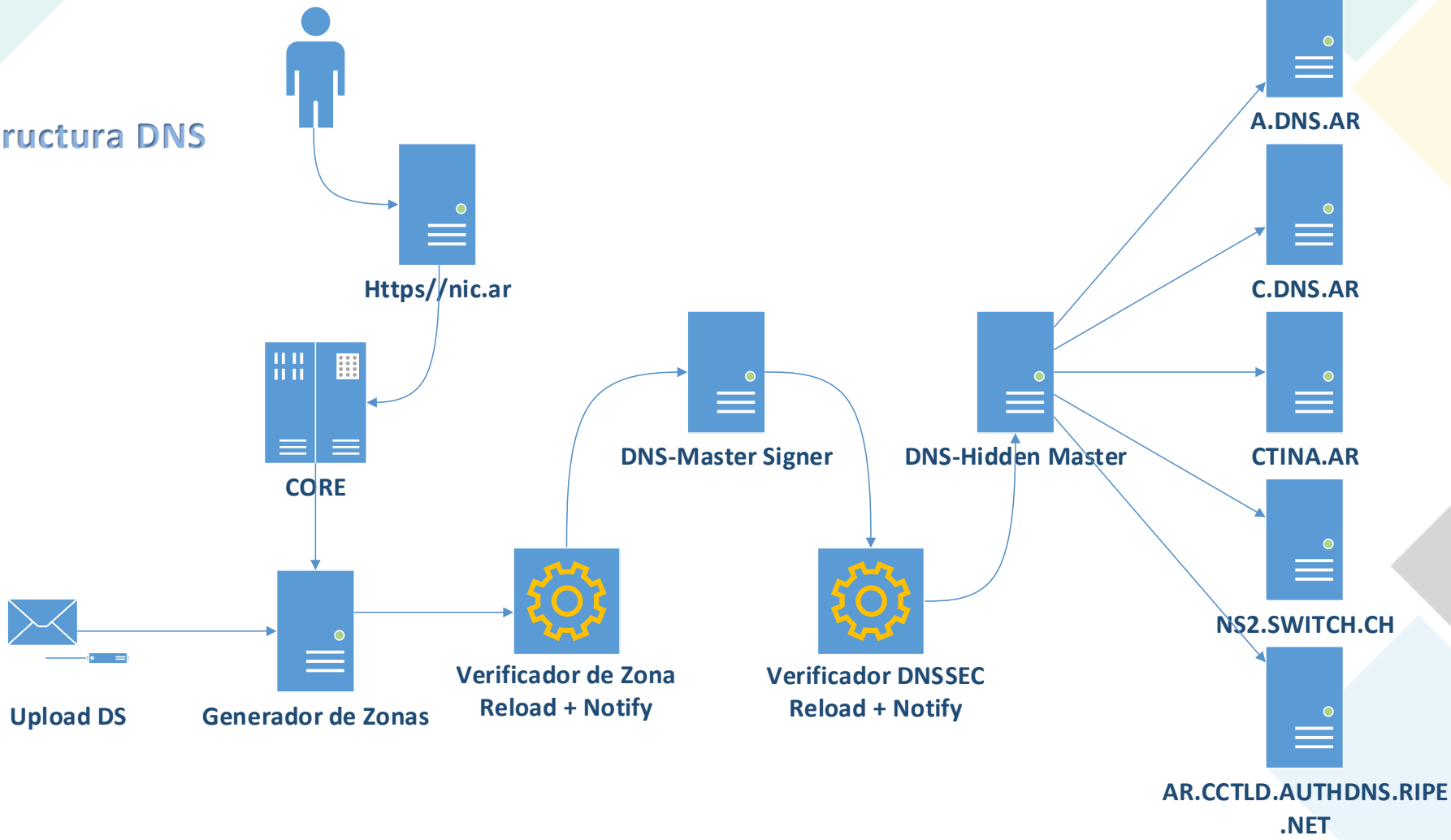


IP de origen	
186.182.30.41	200.108.146.10
89.211.48.42	200.108.146.10
189.194.192.82	200.108.146.10
195.69.221.144	
14.199.192.205	
69.38.33.51	
210.211.124.201	
75.103.235.234	
59.148.180.168	
77.40.48.194	
49.1.248.90	
66.46.124.134	200.108.146.10
210.211.125.78	200.108.146.10
222.57.47.2	200.108.146.10
61.237.242.21	200.108.146.10
173.242.124.40	200.108.146.10
47.23.50.186	200.108.146.10
1.215.163.146	200.108.146.10
119.160.128.92	200.108.146.10
81.177.174.112	200.108.146.10
113.164.17.30	200.108.146.10
201.148.65.197	200.108.146.10



Aplicación	Tráfico(Total: 68.57 GB)	% del tráfico total
chargen	34.21 GB	50%
Unknown_App	31.12 GB	45%

Estructura DNS

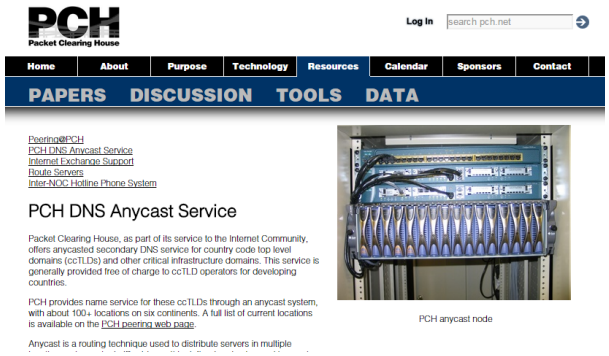


Anycast

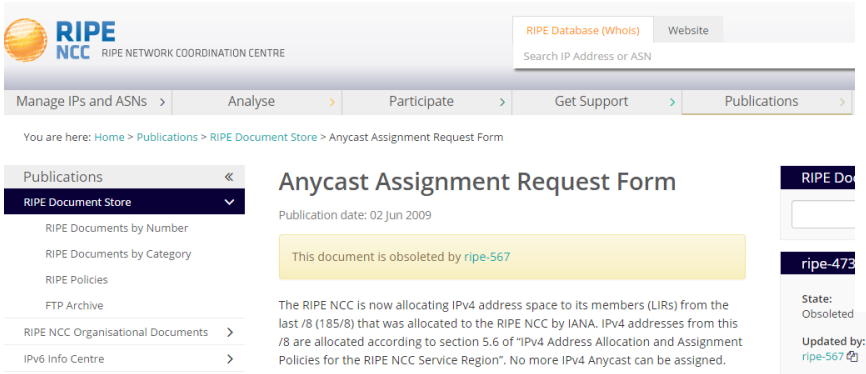
Another very important to ensure service stability contribution was participation in Anycast networks.

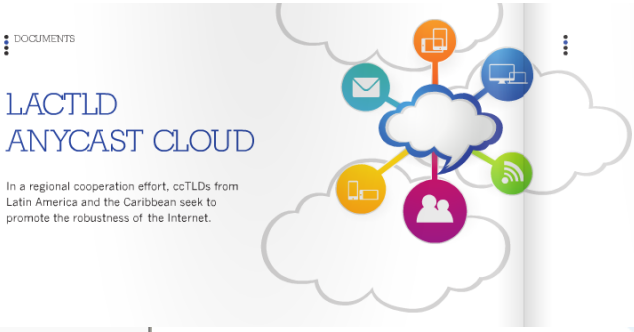
Our first steps were incorporating us to the RIPE network and PCH

We are currently working with LACTLD in the new "anycast" network, also a new "anycast" national network traffic.



PCH anycast node





Nuevos Desafíos

- Continue to improve monitoring systems and automating tools.
- Expand our networks Anycast.
- Keep learning new techniques and technologies.
- Expanding the work of our CSIRT

Luciano Minuchin – minuchinl@nic.gob.ar

Sebastian Motta– mottas@nic.gob.ar

MUCHAS GRACIAS

ICANN | 53
Buenos Aires
21-25 JUNE 2015