

REDIMadrid: Situación actual del análisis de ataques DDOS en REDIMadrid

David Rincón

XVI Jornadas de REDIMadrid
21 de octubre de 2021



Dirección General de Investigación
e Innovación Tecnológica
CONSEJERÍA DE EDUCACIÓN,
UNIVERSIDADES, CIENCIA
Y PORTAVOCÍA



Licitación de software para análisis DDoS



- La licitación tenía por objetivo buscar una solución abierta que nos diera visibilidad de los ataques DDoS que se estaban produciendo, también era importante que la mitigación se pudiera realizar con diferentes soluciones del mercado.
- En 2020 Se adjudica el contrato al licitador Axians que presenta una solución del fabricante Genie Networks con el producto GENIE ATM.



Licitación de software para analisis DDoS



- En 2021 se finaliza la configuración a nivel general de la herramienta.
- También en 2021 se ofrece a las instituciones un curso de formación sobre GENIE ATM.
- Actualmente esta totalmente configurada y operativa y se esta trabajando con las instituciones para configurar cada dashboard y las casuísticas de cada una.

Event List

Anomaly	Category: Severity:	Total		Traffic Anomaly		Worm or DDoS	
		Yellow	Red	Yellow	Red	Yellow	Red
Ongoing (In Last 24H) 2020-10-15 11:13:57		1	3	0	0	1	3

Resource Type: ALL
Anomaly Type: Worm or DDoS
Time Period: Time Range
Duration: min(s)
Traffic Amount: bps

Traffic Direction: ALL
Anomaly Status: ALL
Minimum Severity: Yellow
User Checked: All
Victim/Infected IP Prefix:

Top 10 Statistics

Attacked IP by DDoS			IPs Doing Scans or Infection			Types of Anomalies			
	#	%		#	%		#	%	
1	193.147.107.5	2	100.00			1	Host TCP Traffic	2	100.00

2 Anomalies

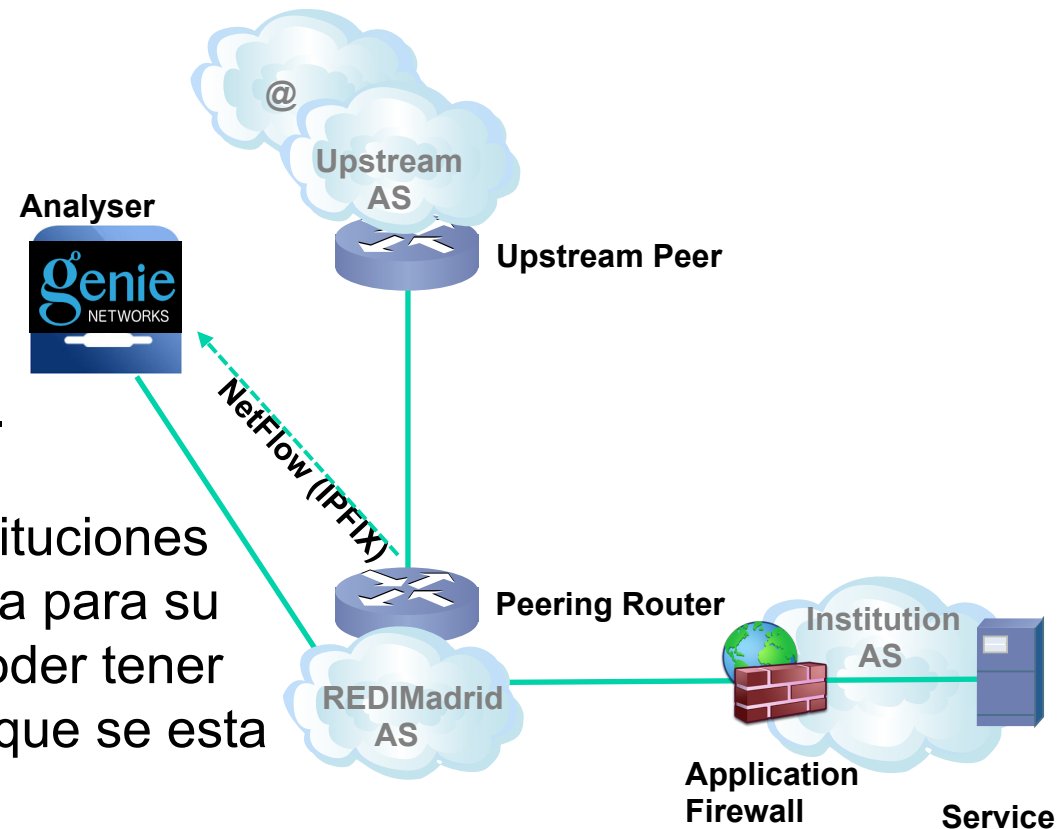
No.	ID	CHK	Traffic	Severity	Status	Start Time	End Time	Duration	Direction	Type	Resource	Victim IP
1	A90549			147.65 Mbps over 95.33 Mbps max 150.24 Mbps	Recovered	10-14 02:34	10-14 03:09	34 mins 27 secs	To Home	DDOS Host TCP Traffic bps	IMDEA SOFTWARE	193.147.107.5
2	A89372			95.71 Mbps over 95.33 Mbps max 109.32 Mbps	Recovered	10-13 14:07	10-13 14:11	4 mins	To Home	DDOS Host TCP Traffic bps	IMDEA SOFTWARE	193.147.107.5



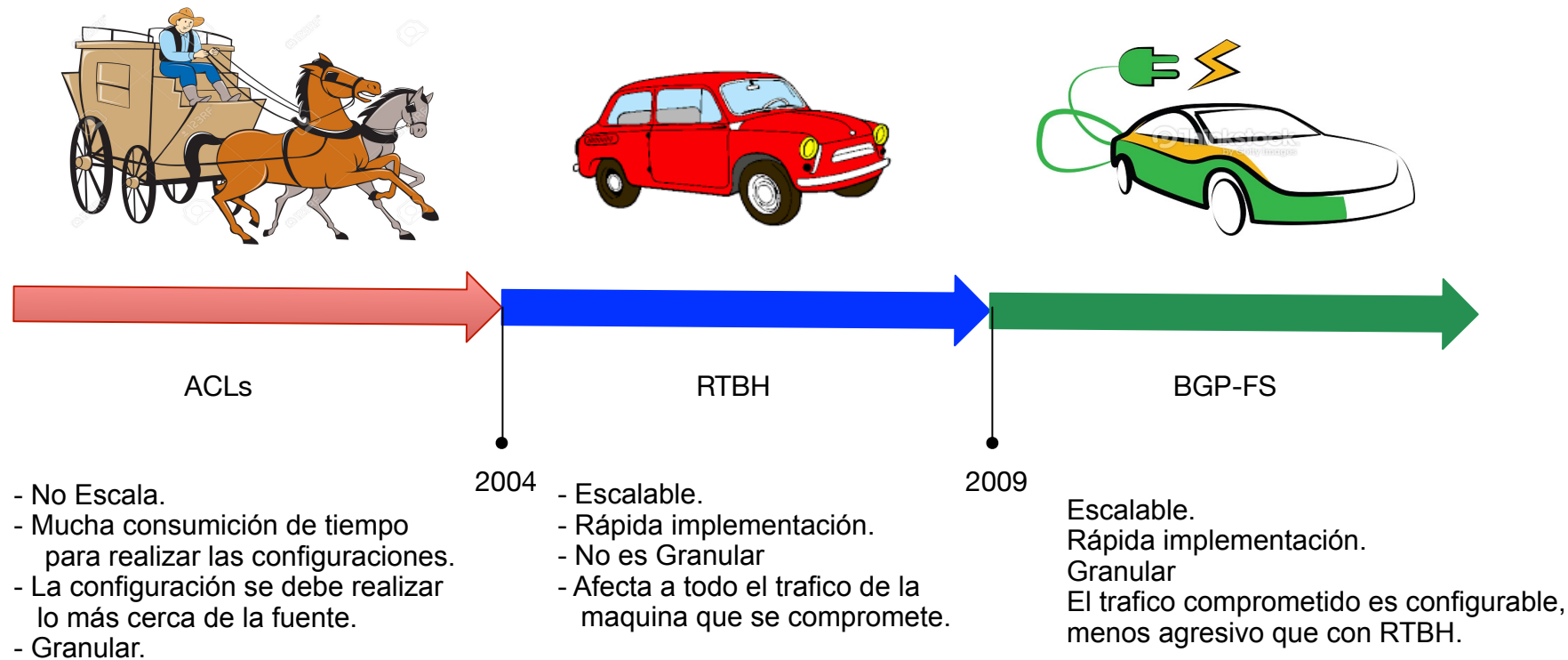
Solución de análisis y mitigación DDoS



- Genie utiliza Netflow (IPFIX) y los datos recibidos vía SNMP para detectar ataques DDoS.
- No es necesario insertar el analizador físicamente en la red.
- Tiene una API abierta para soluciones futuras de mitigación (scrubbing center).
- REDIMadrid ofrece a las instituciones tener acceso a la herramienta para su network y de esta manera poder tener más información del ataque que se está produciendo.



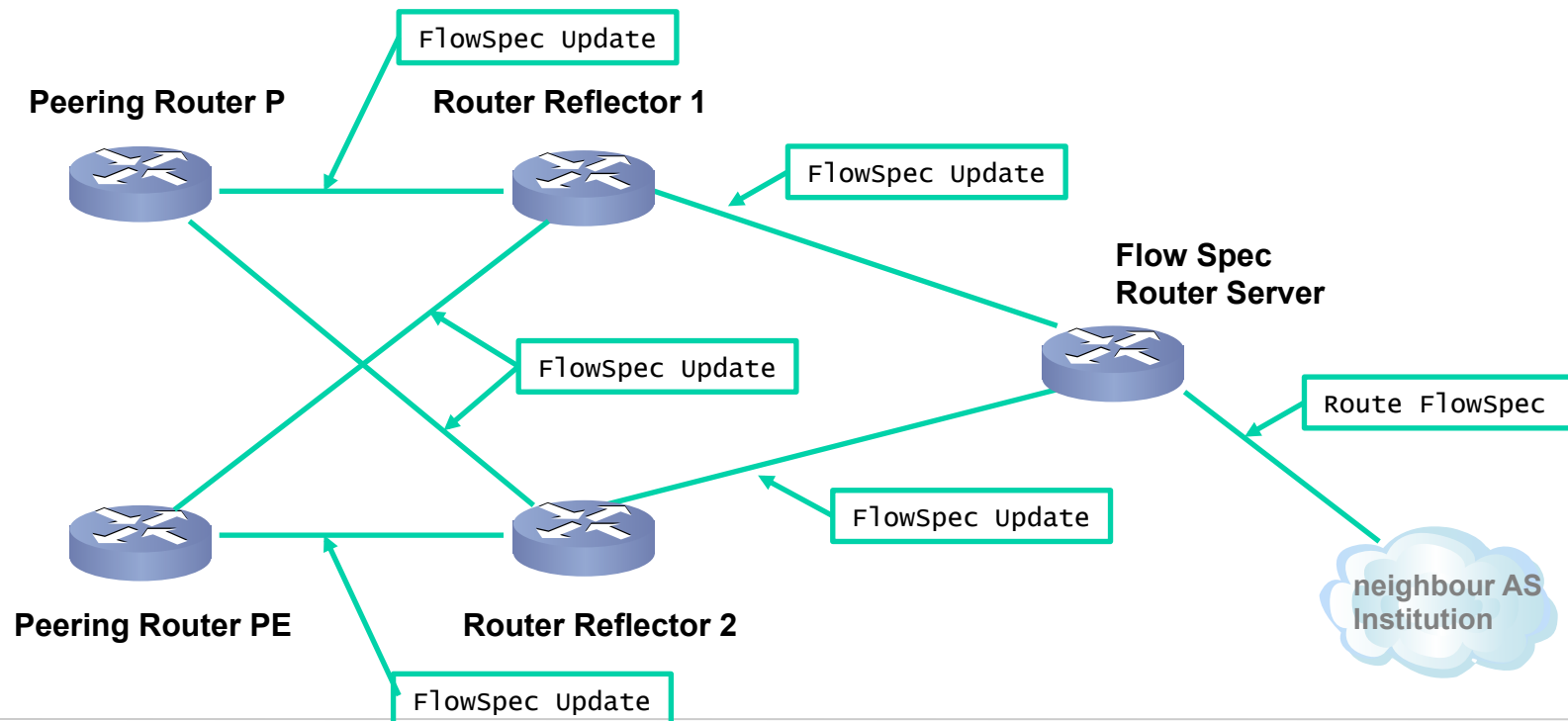
Tipos de mitigación



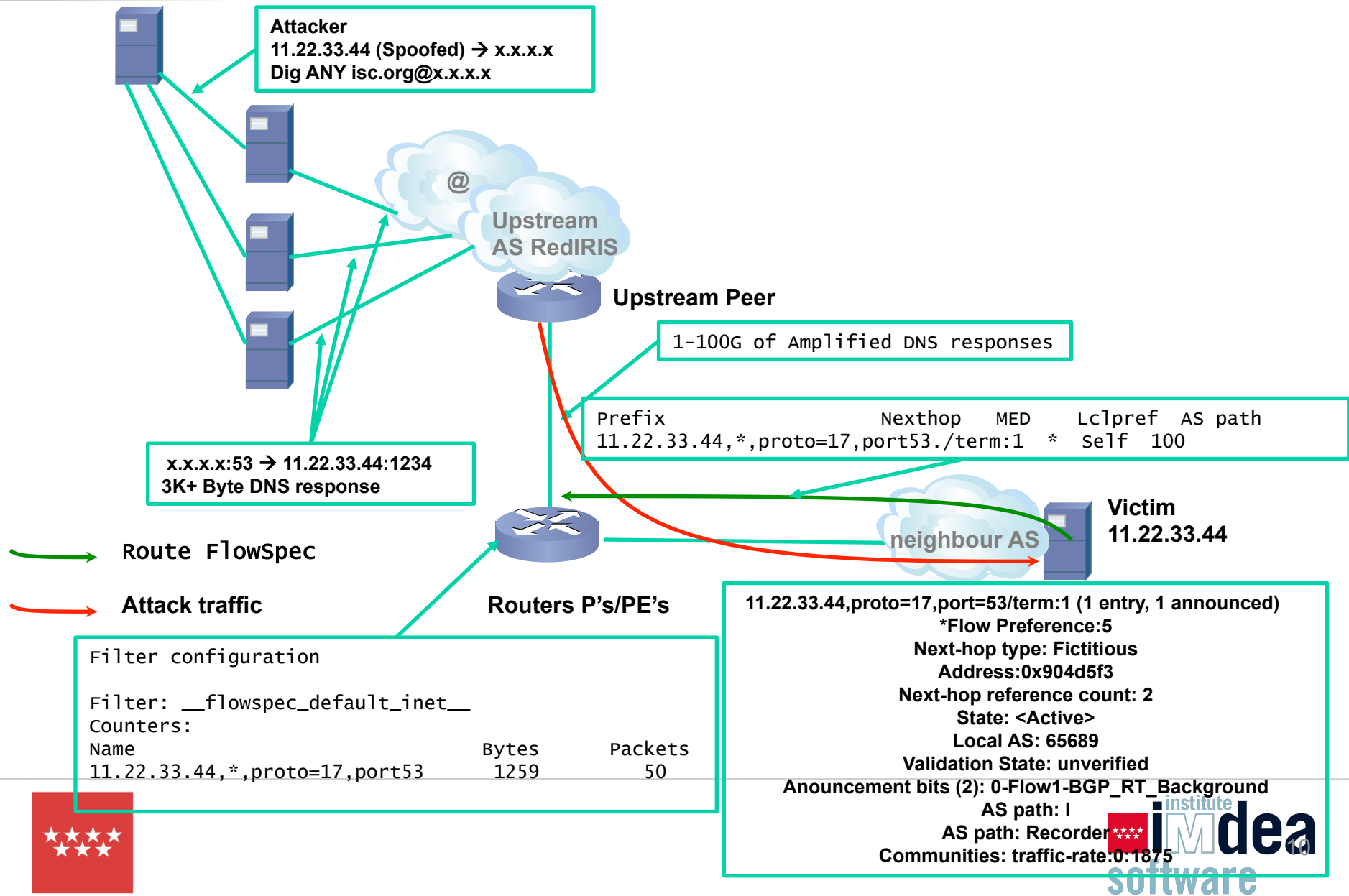
Mitigación actual en REDIMadrid



Se configura un router dedicado para agregar todas las rutas de Flow-Spec por parte de las instituciones, este router exporta las rutas a los Router Reflector y estos router reflejan todas las rutas a los router P y PE's de REDIMadrid.



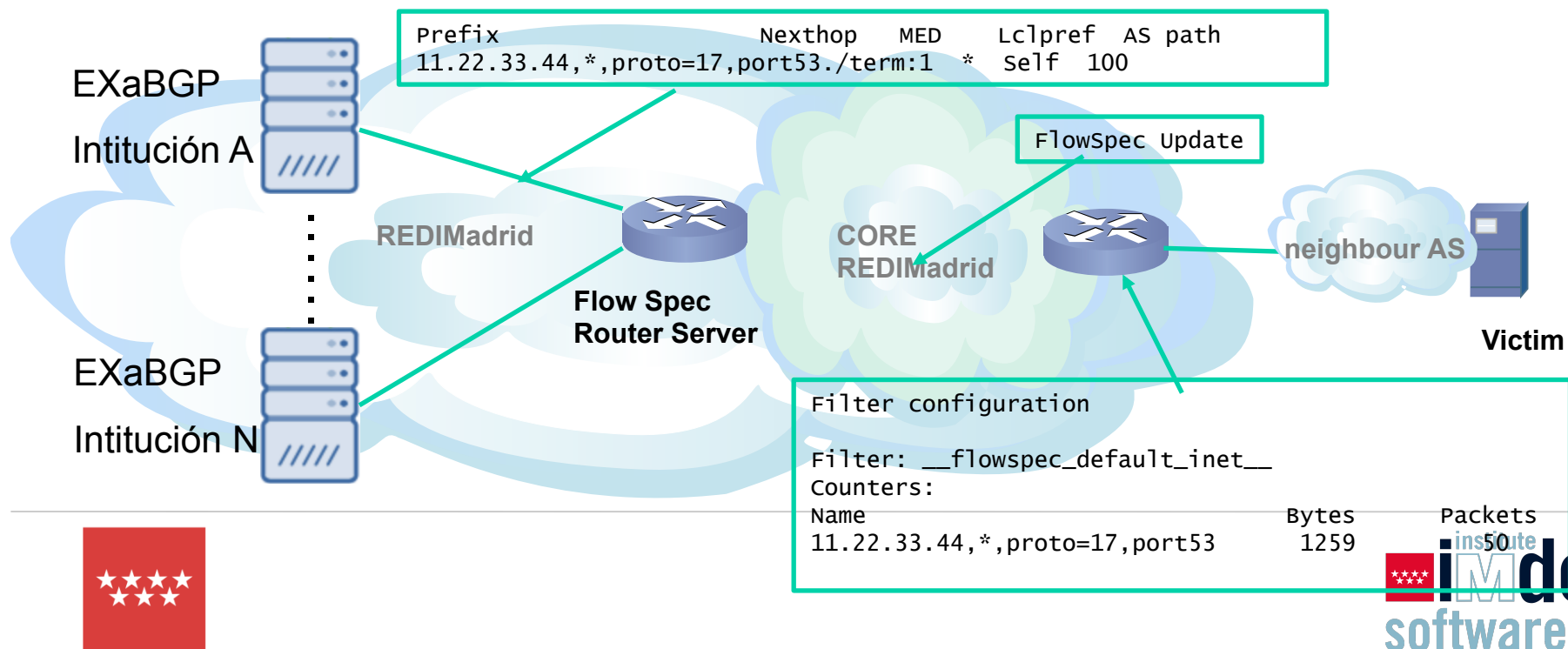
¿Como funciona?



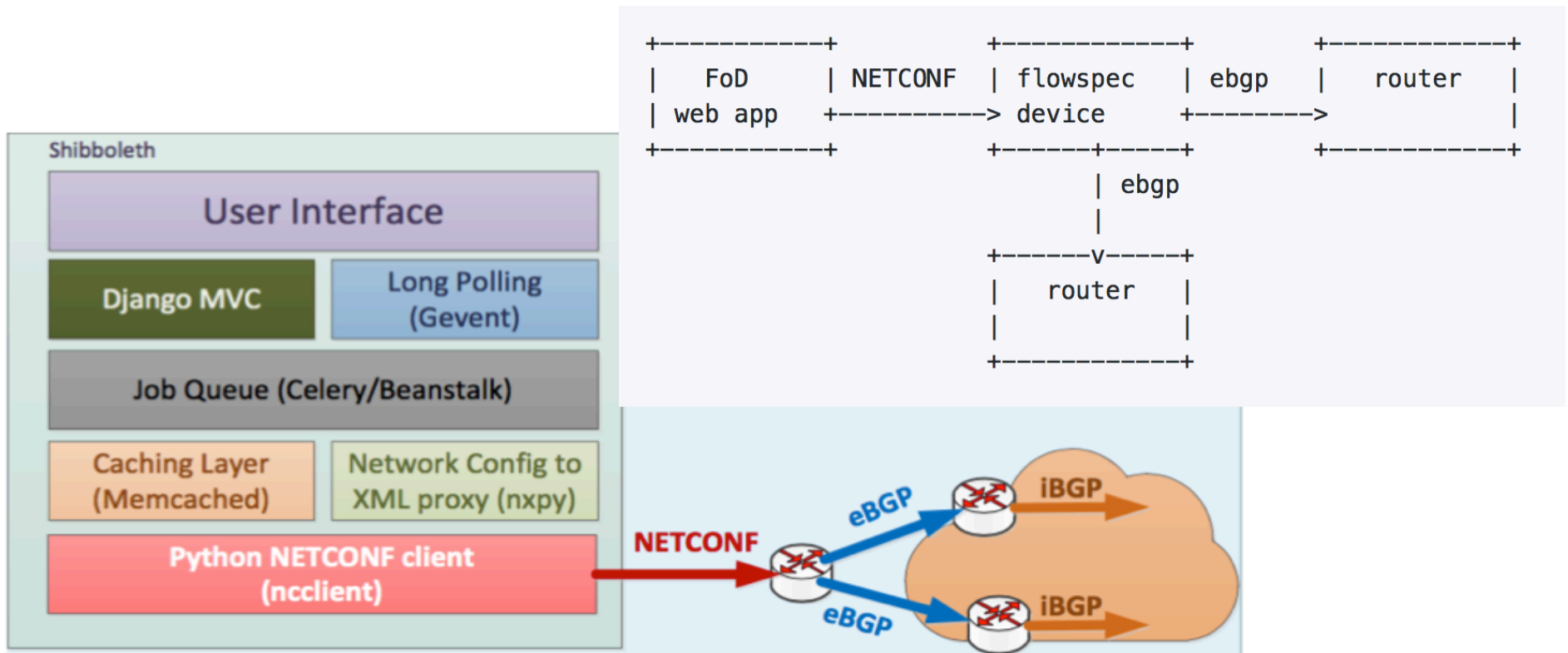
Como configurar BGP-FS para anunciar rutas de mitigación? → ExaBGP



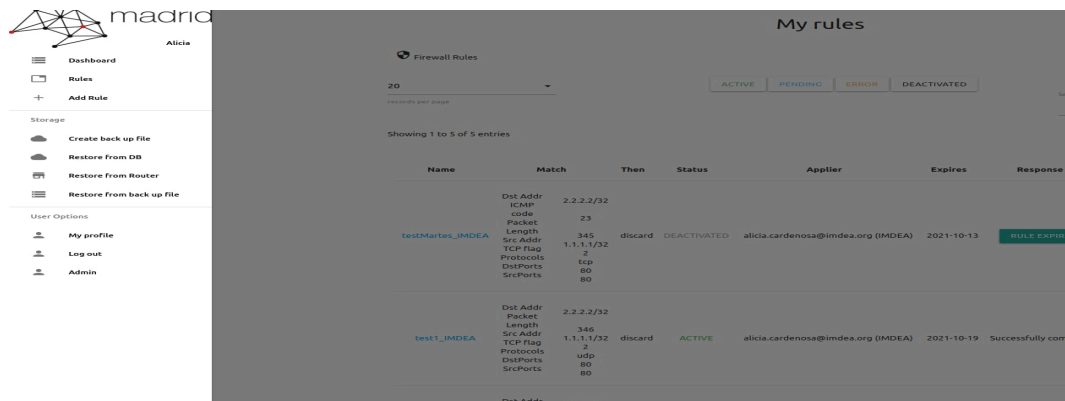
- La solución actual de REDIMadrid para anunciar rutas BGP-Flow-Spec es utilizar ExaBGP.
- Esta es una solución transitoria ya que se debe realizar un trabajo muy manual y poco visual, con lo que puede llevar a errores u olvidos a la hora de realizar las configuraciones.



REDIMadrid esta ultimando una nueva herramienta mas visual que sustituirá a ExaBGP, esta herramienta se basa en una solución de software libre similar al FOD de GEANT.



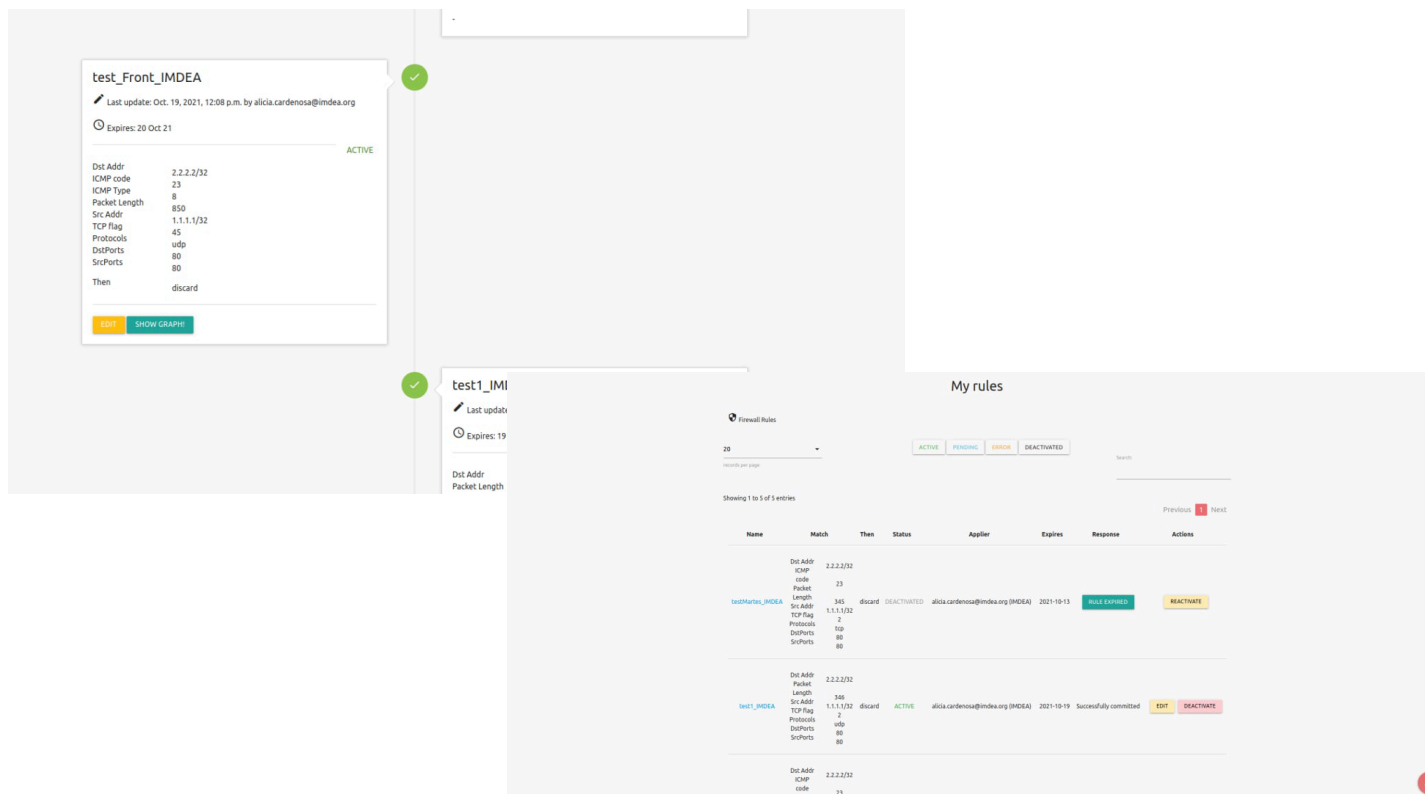
- La herramienta se ha rediseñado totalmente para adaptarla a las necesidades actuales.



- La seguridad de la herramienta es muy importante, por tanto tendrá implementados los mejores sistemas de seguridad.
- También estamos implementando sistemas de back-up de reglas configuradas y redundancia en los anuncios de flow-spec.



- La primera versión tendrá la posibilidad de ver los hits de cada regla de flow-spec aplicada.



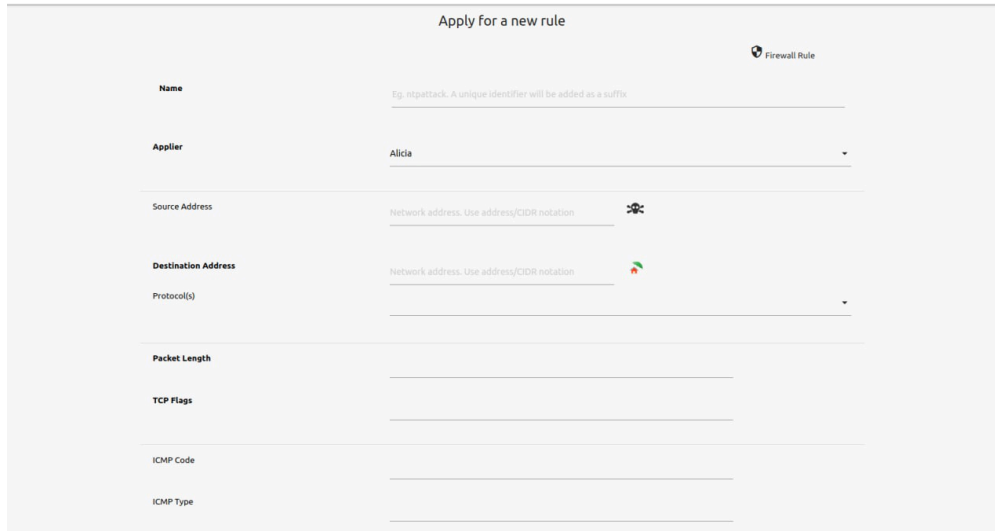
The screenshot displays the REDIFoD interface. On the left, a rule configuration window for 'test_Front_IMDEA' is shown, with fields for Dst Addr (2.2.2.2/32), ICMP code (23), ICMP Type (8), Packet Length (850), Src Addr (1.1.1.1/32), TCP flag (45), Protocols (udp), DstPorts (80), and SrcPorts (80). The rule is set to 'discard' and is currently 'ACTIVE'. Below this, another rule configuration window for 'test1_IMI' is partially visible.

On the right, a 'My rules' table lists the configured rules:

Name	Match	Then	Status	Applic	Expires	Response	Actions
test_Front_IMDEA	Dst Addr: 2.2.2.2/32 ICMP code: 23 Packet Length: 850 Src Addr: 1.1.1.1/32 TCP Flag: 45 Protocols: udp DstPorts: 80 SrcPorts: 80	discard	DEACTIVATED	alicia.cardenosa@imdea.org (IMDEA)	2021-10-19	FILE EXPIRED	REACTIVATE
test1_IMI	Dst Addr: 2.2.2.2/32 Packet Length: 850 Src Addr: 1.1.1.1/32 TCP Flag: 45 Protocols: udp DstPorts: 80 SrcPorts: 80	discard	ACTIVE	alicia.cardenosa@imdea.org (IMDEA)	2021-10-19	Successfully committed	EDIT DEACTIVATE
	Dst Addr: 2.2.2.2/32 ICMP code: 23						



- La planificación inicial es que este operativa en el primer trimestre de 2022.



Apply for a new rule

Firewall Rule

Name Eg. ntpattack. A unique identifier will be added as a suffix

Applier **Alicia**

Source Address Network address. Use address/CIDR notation

Destination Address Network address. Use address/CIDR notation

Protocol(s)

Packet Length

TCP Flags

ICMP Code

ICMP Type

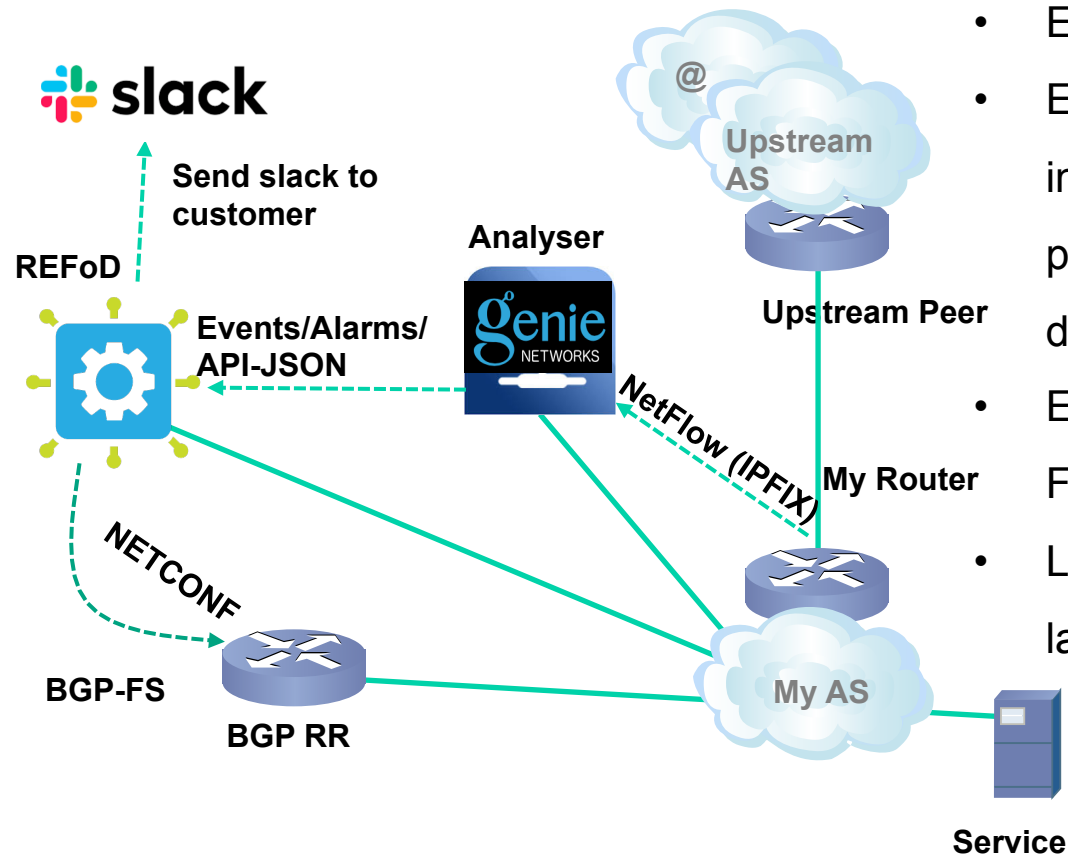
- Será una primera versión, después se sacaran nuevas versiones con las propuestas que cada institución nos esta transmitiendo.
- La herramienta se ha dockerizado y estará disponible para cualquier institución que quiera implementarla.



Siguientes pasos → REDIFoD conectada con Genie



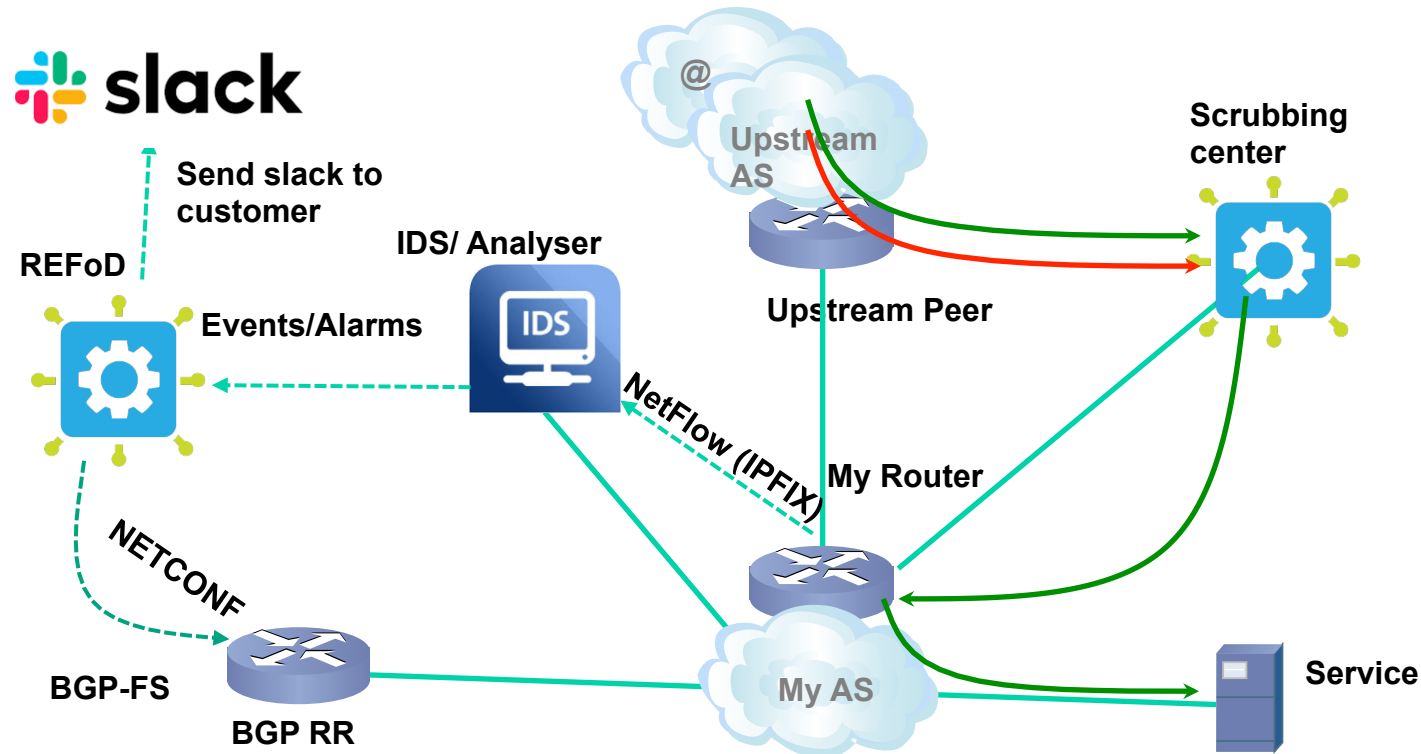
Como funciona la solución:



- El Genie detecta un DDoS
- Envía el evento al REFoD.
- El REFoD envía un slack al cliente indicando que hay un ataque y que puede aplicar una regla predefinida de BGP-FS para mitigar.
- El cliente confirma la regla de BGP-FS.
- La regla de BGP-FS se envía a toda la red por netconf y se mitiga el ataque.



¿Quizás el Futuro? → Scrubbing center



→ Legitimate traffic
→ Attack traffic

¿Quizás el futuro venga por la Instalación de scrubbing center para la limpieza de trafico no legitimo?



REDIMadrid: Situación actual del análisis de ataques DDOS en REDIMadrid

PREGUNTAS

XVI Jornadas de REDIMadrid

21 de octubre de 2021



Comunidad
de Madrid

Dirección General de Investigación
e Innovación Tecnológica
CONSEJERÍA DE EDUCACIÓN,
UNIVERSIDADES, CIENCIA
Y PORTAVOCÍA

