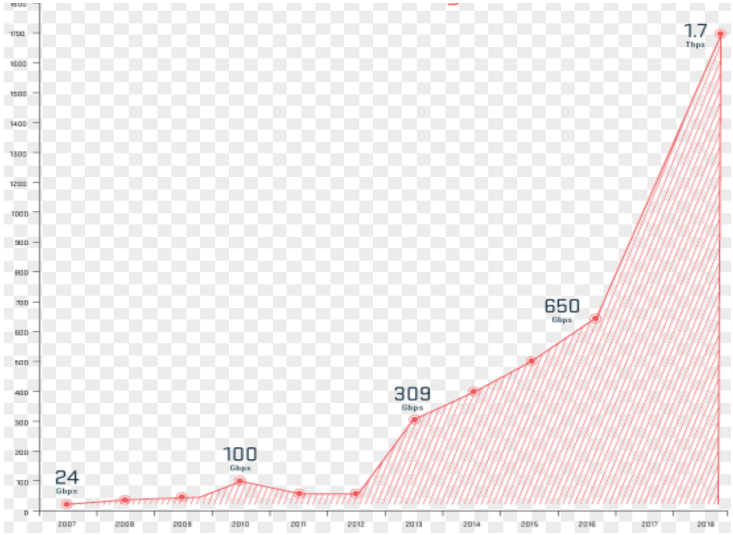
REDIMadrid: Situación actual del análisis de ataques DDOS en REDIMadrid

David Rincón

XV Jornadas de REDIMadrid

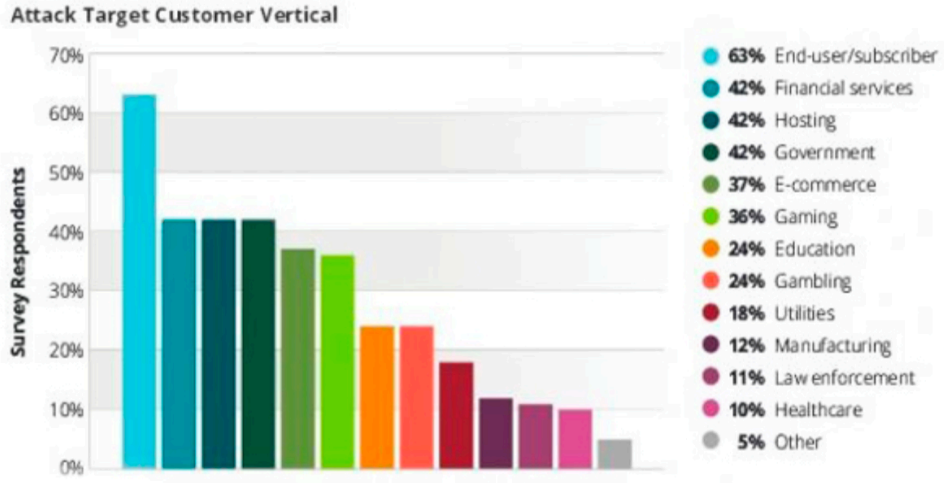
20 de octubre de 2020

Ataques de DDoS



En el 2015, por primera vez en la historia, se registró un ataque DDoS que superó la marca de 500 Gbps, en 2016 se supero la marca de 1Tbps.

¿A quien se ataca? El 24% de los ataques se realizan a las instituciones que se decidan a la educación



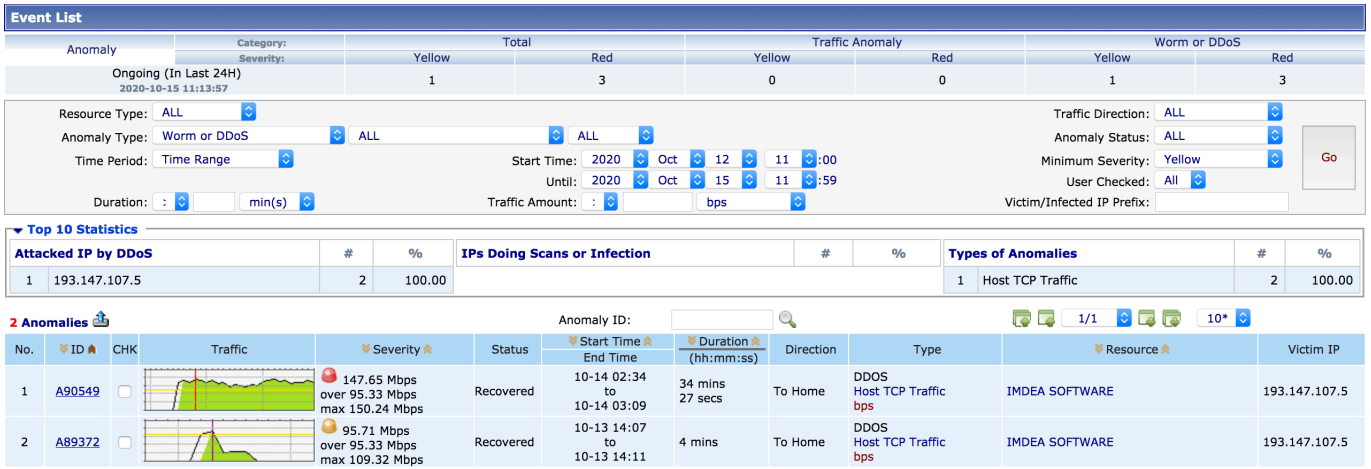
Gráficos obtenidos de la empresa arbor - netscout

Licitación de software para analisis DDoS

- El ultimo trimestre del año 2019 sale a licitación publica el equipamiento para analizar DDoS.

- Se adjudica el contrato al licitador Axians que presenta una solución del fabricante Genie Netwworks con el software GENIE ATM

- Actualmente se esta configurando y poniendo en servicio.



Event List

Anomaly	Category:	Total		Traffic Anomaly		Worm or DDoS	
	Severity:	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 ALL ALL
Time Period: Time Range
Start Time: 2020 Oct 12 11 :00
Until: 2020 Oct 15 11 :59
Duration: : min(s)
Traffic Amount: : bps
Traffic Direction: ALL
Anomaly Status: ALL
Minimum Severity: Yellow
User Checked: All
Victim/Infected IP Prefix:
Go

Top 10 Statistics

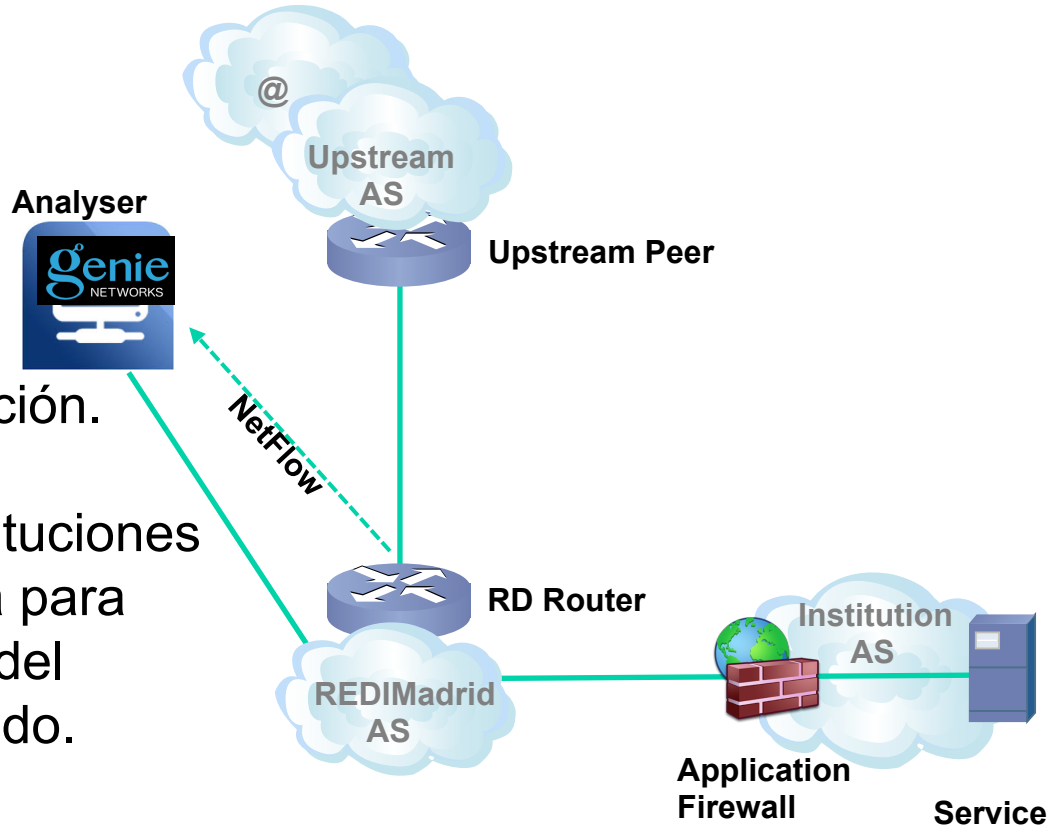
Attacked IP by DDoS	#	%	IPs Doing Scans or Infection	#	%	Types of Anomalies	#	%
1 193.147.107.5	2	100.00				1 Host TCP Traffic	2	100.00

2 Anomalies Anomaly ID: 1/1 10*

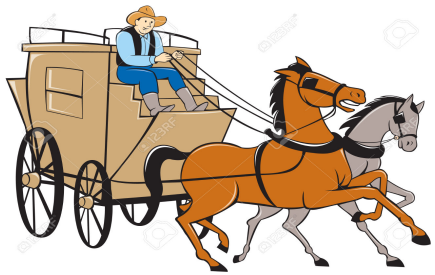
No.	ID	CHK	Traffic	Severity	Status	Start Time / End Time	Duration (hh:mm:ss)	Direction	Type	Resource	Victim IP
1	A90549			147.65 Mbps over 95.33 Mbps max 150.24 Mbps	Recovered	10-14 02:34 to 10-14 03:09	34 mins 27 secs	To Home	DDOS Host TCP Traffic bps	IMDEA SOFTWARE	193.147.107.5
2	A89372			95.71 Mbps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

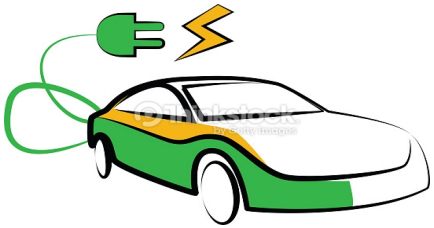
Solución de analisis y mitigación DDoS

- Genie utiliza Netflow 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.
- REDIMadrid ofrece a las instituciones tener acceso a la herramienta para poder tener mas información del ataque que se esta produciendo.



Tipos de mitigación





ACLs

- No Escala.
- Mucha consumición de tiempo para realizar las configuraciones.
- La configuración se debe realizar lo más cerca de la fuente.
- Granular.

2004

RTBH

- Escalable.
- Rápida implementación.
- No es Granular
- Afecta a todo el trafico de la maquina que se compromete.

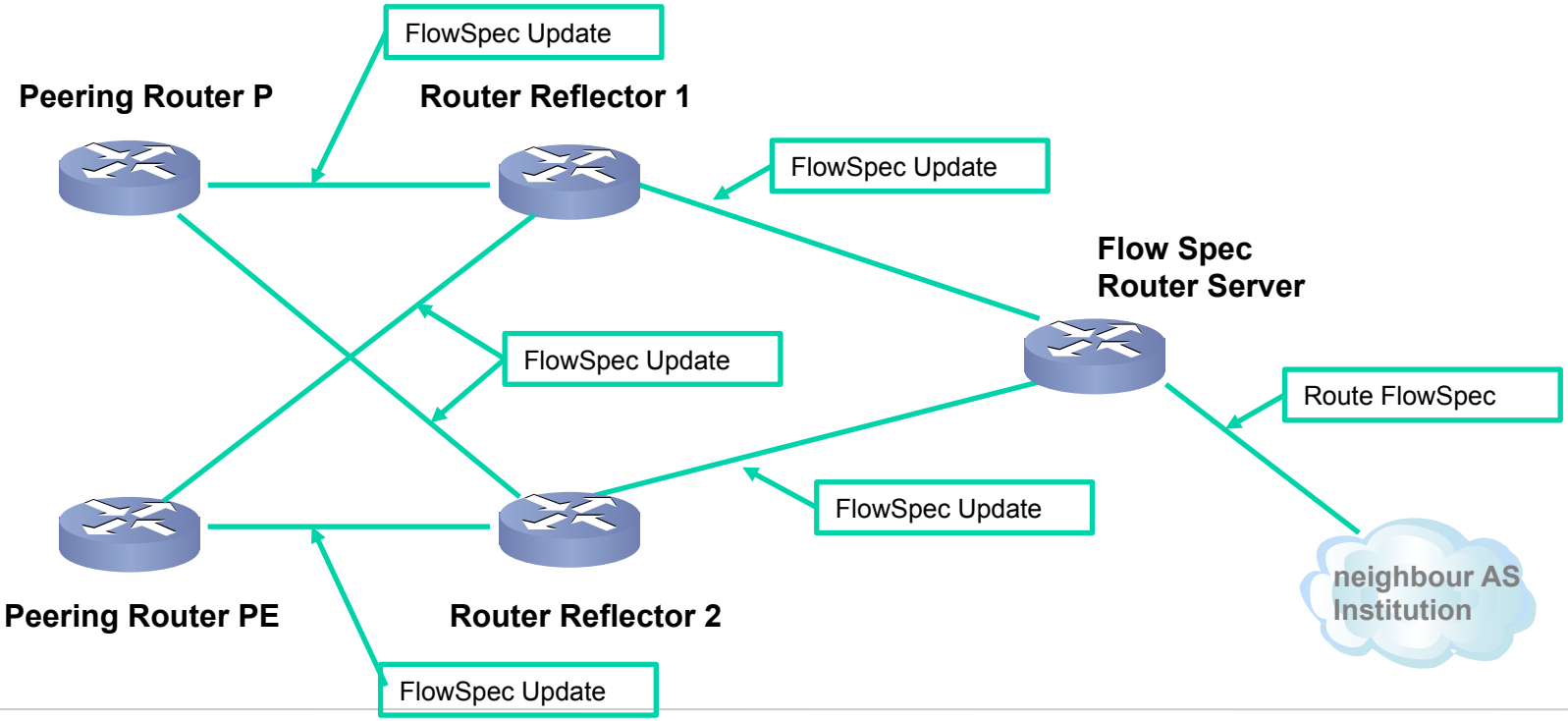
2009

BGP-FS

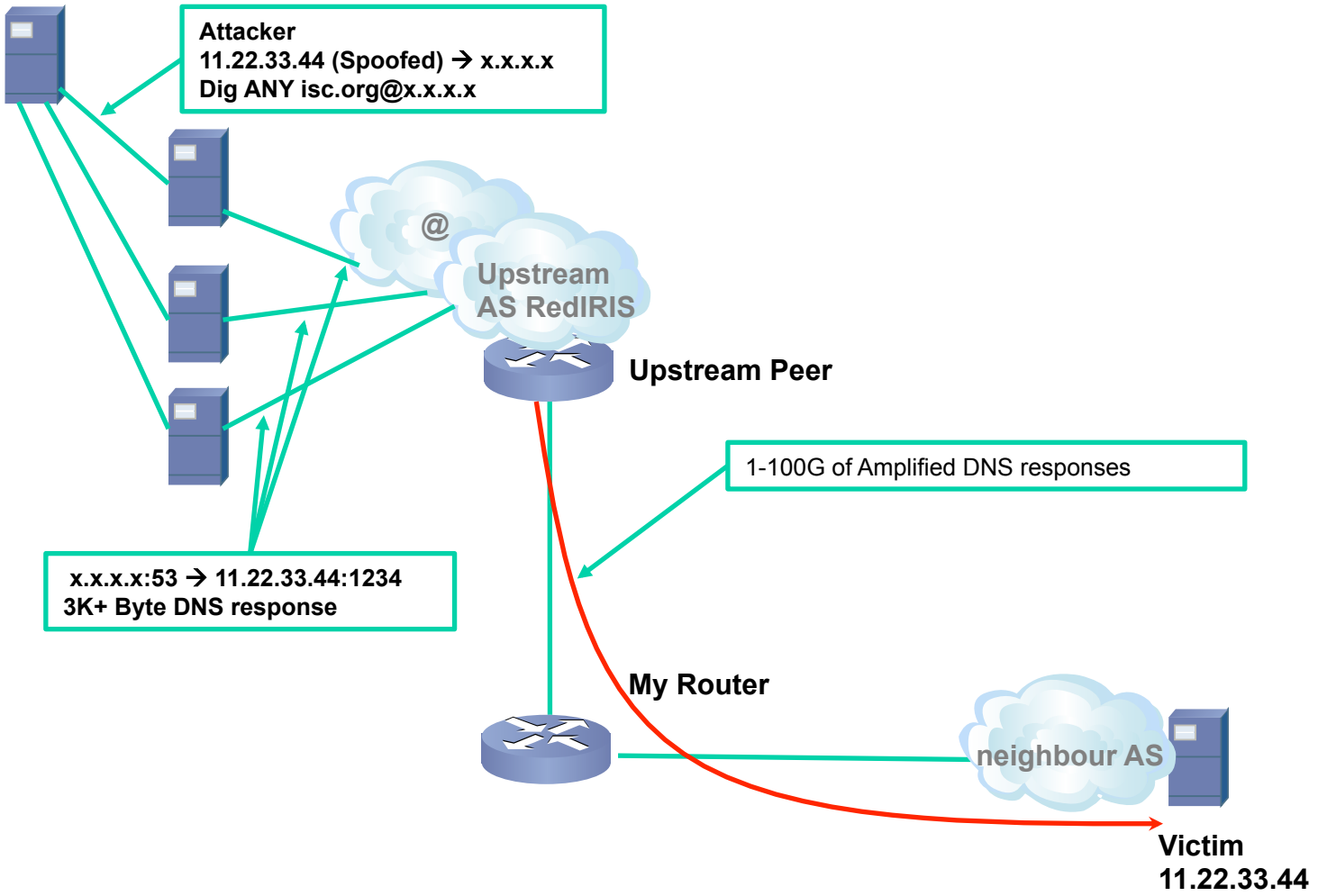
Escalable.
Rápida implementación.
Granular
El trafico comprometido es configurable, menos agresivo que con RTBH.

Mitigación actual en REDIMadrid

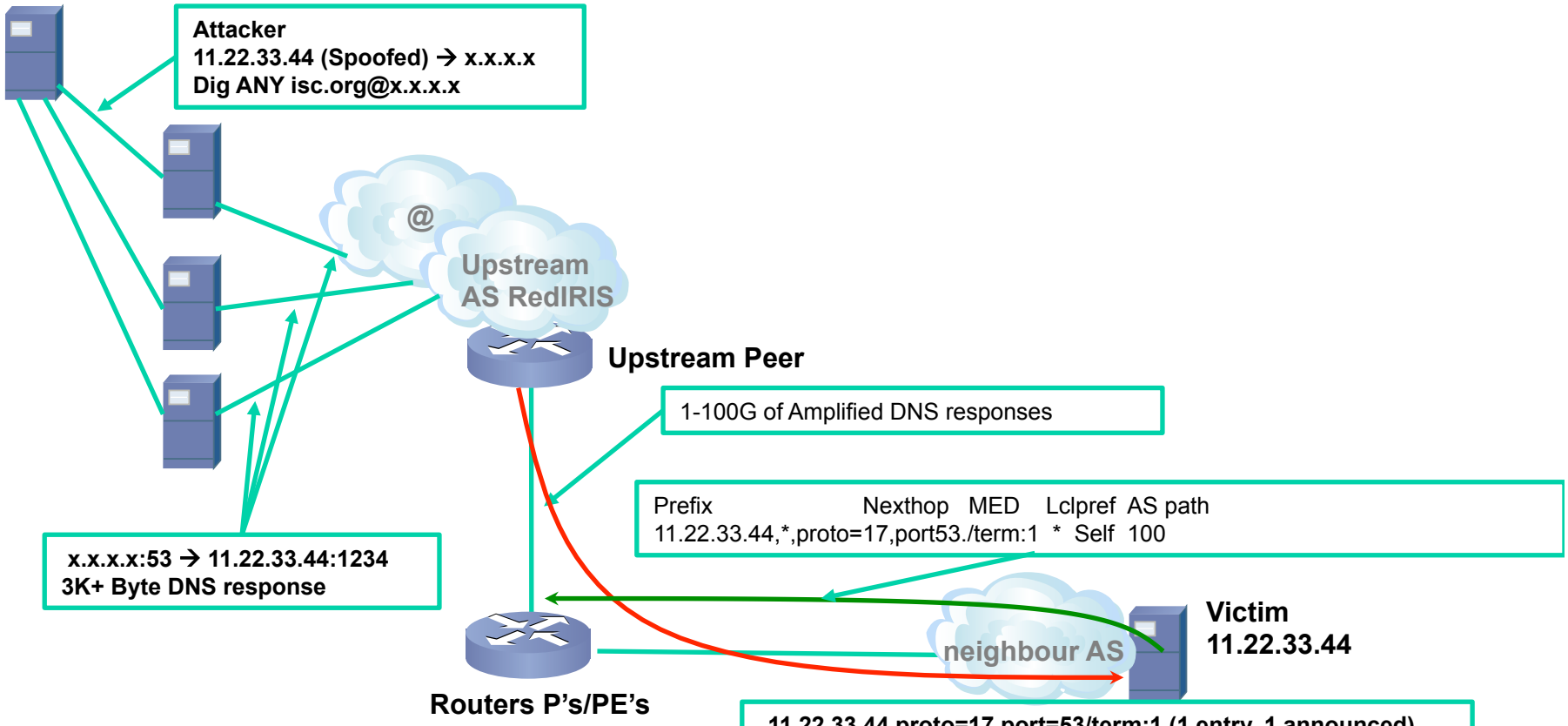
Se configura un router dedicado para agregar todas las rutas de Flow Spec por parte de las instituciones, este router exporta las rutas a los Router Reflector y estos router reflectan todas las rutas a los router P y PE's de REDIMadrid.



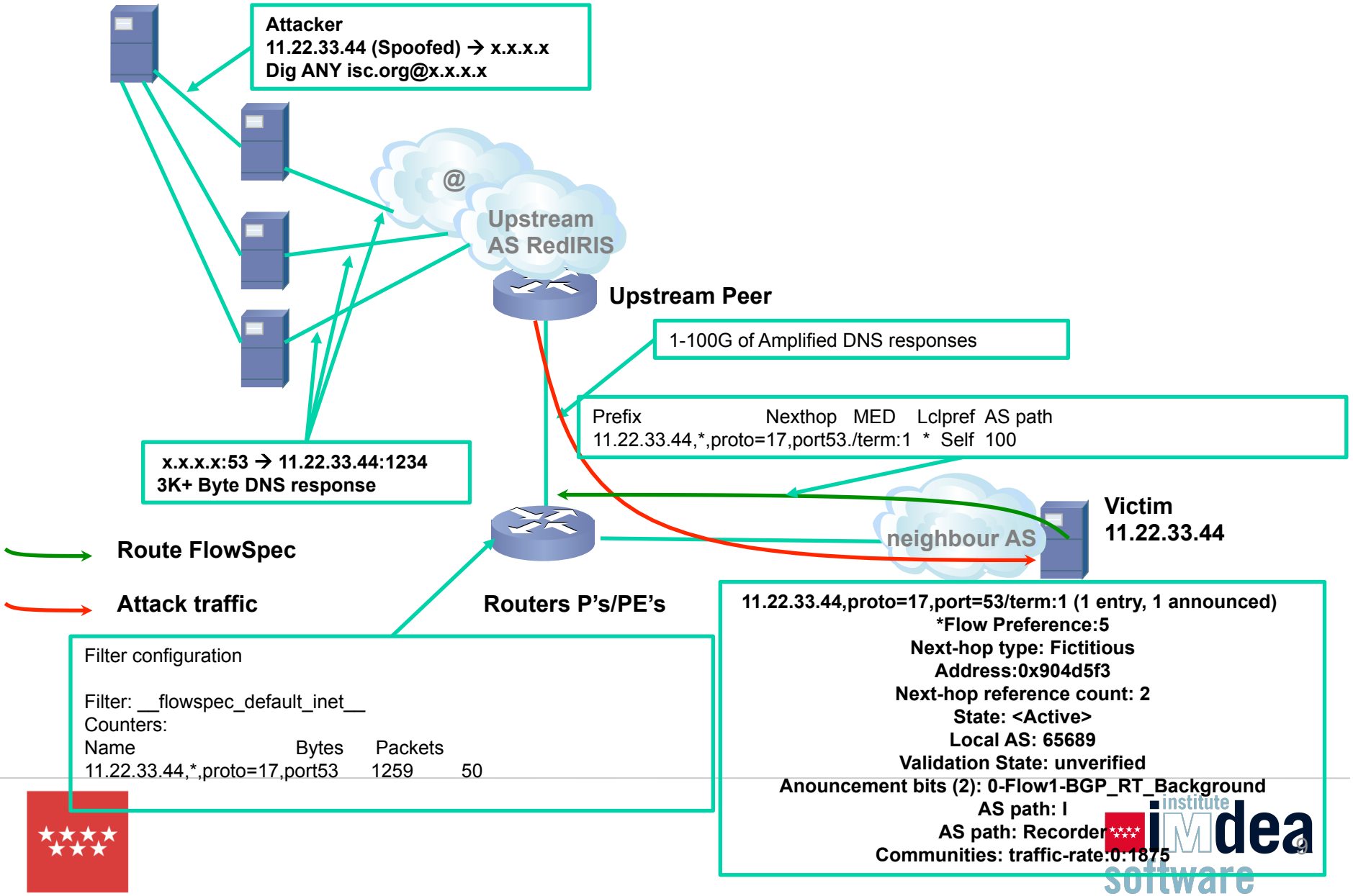
¿Como funciona?



¿Como funciona?

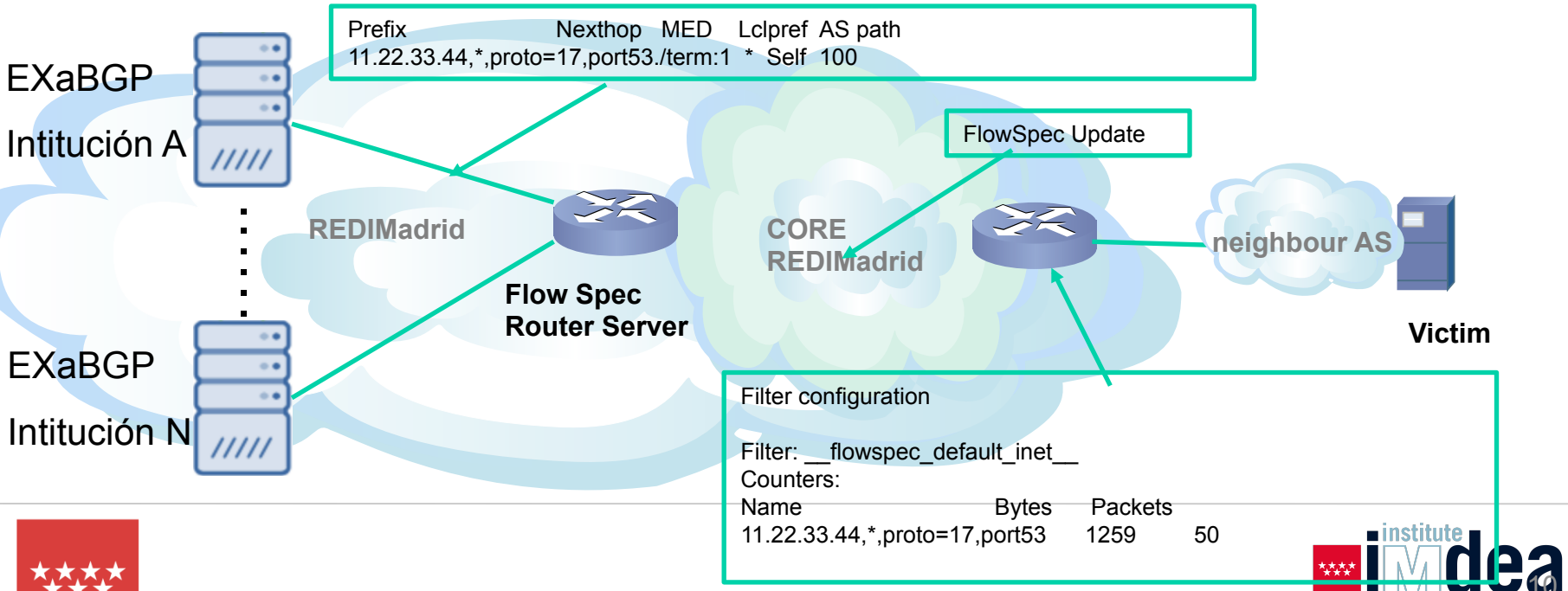


¿Como funciona?



Como configurar BGP-FS para anunciar rutas de mitigación?

- REDIMadrid ofrece una maquina virtual por cada institución interesada para poder importar a la red rutas del trafico infectado.
- Esta solución se basa en ExaBgp
- Se decide dar la solución desde REDIMadrid para que si la institución se compromete no haya problemas en tener acceso al "mitigrador", además de facilitar esta labor a las instituciones.



Como configurar BGP-FS para anunciar rutas de mitigación?

- ExaBGP es sencillo de usar y se basa en linux.
- Agradecimiento a la UC3M y en especial a Rafael Calzadas por las pruebas realizas para certificar la solución.
- La institución solo puede anunciar rutas de su rango de direccionamiento, cualquier anuncio de rutas de otro rango que no sea el suyo no será aceptado.

Consulta de los routers BGP vecinos:

```
[root@accdiba exabgp]# exabgpcli show neighbors summary
Peer            AS        up/down state       |     #sent     #recvd
[redacted]      [redacted]  2 days, 20:39:04 established          2          0
```

Bloqueo de tráfico FlowSpec

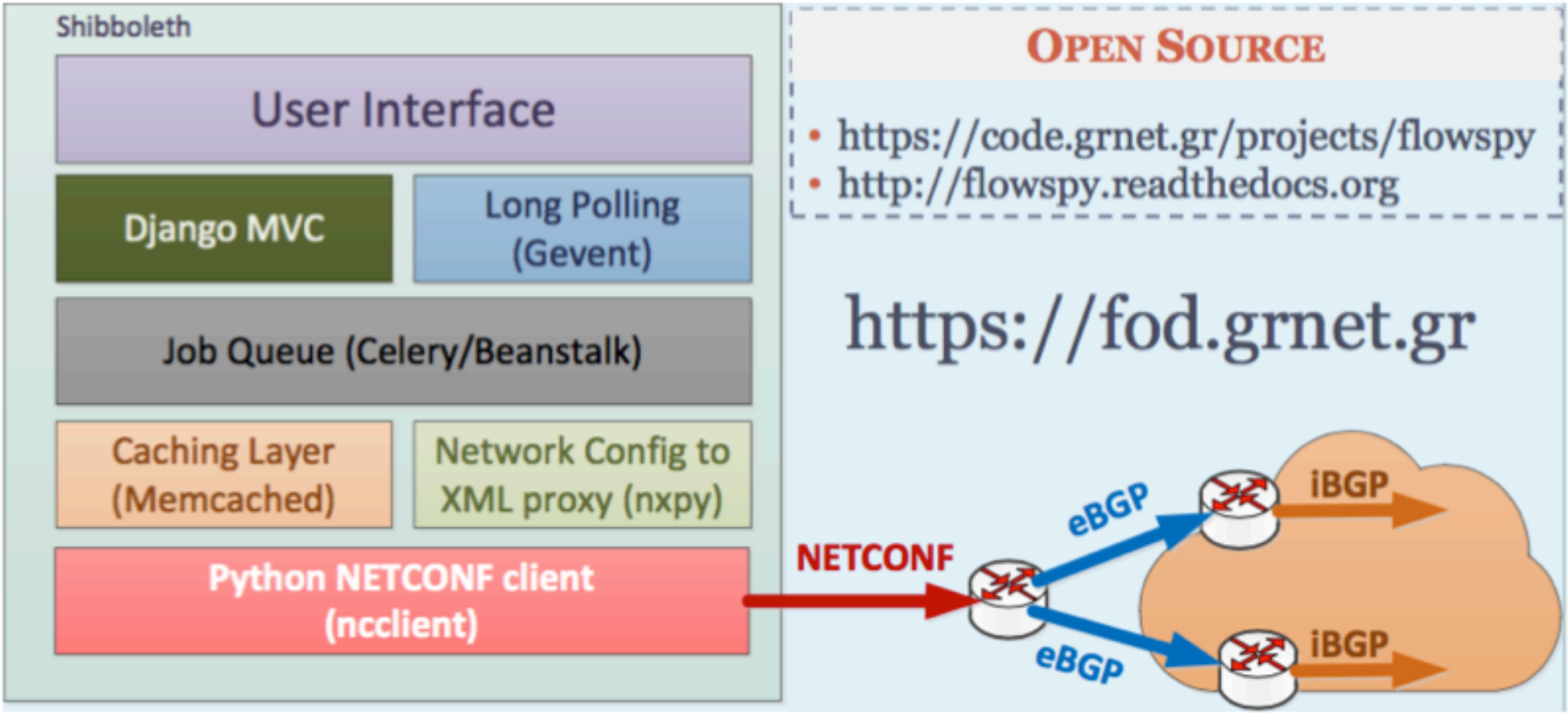
En este caso se puede bloquear el tráfico con las capacidades de una Access-List de un router, es decir, haciendo uso de los campos de la cabecera TCP/IP.

Por ejemplo para bloquear el tráfico Telnet (23/tcp) con destino a la red [redacted].

```
[root@accdiba exabgp]# bin/exabgpcli show adj-rib out
[root@accdiba exabgp]# bin/exabgpcli announce flow 'route { match { destination
163.117.0.0/16; destination-port 23; protocol tcp;} then { discard; } } }'
[root@accdiba exabgp]# bin/exabgpcli show adj-rib out
neighbor [redacted] ipv4 flow flow destination-ipv4 [redacted] protocol =tcp
destination-port =23
```

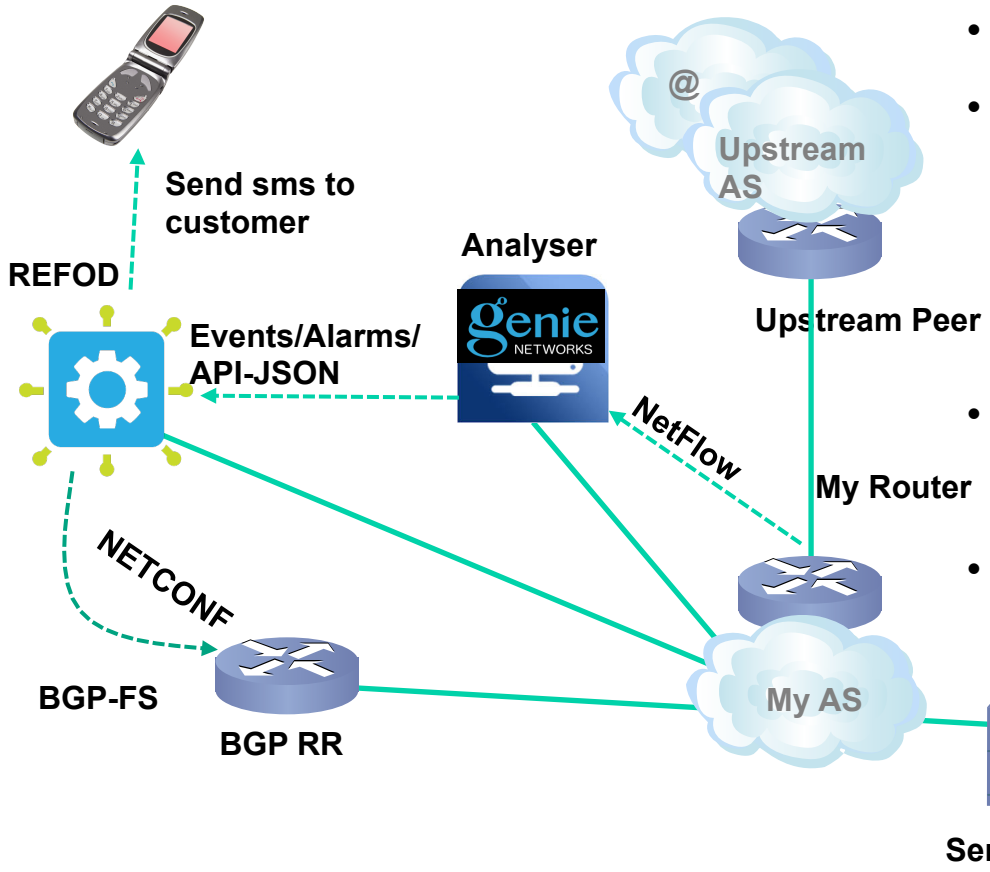
Siguientes pasos

REDIMadrid esta trabajando en una solución similar al FOD de GEANT, pero todavía no esta disponible.



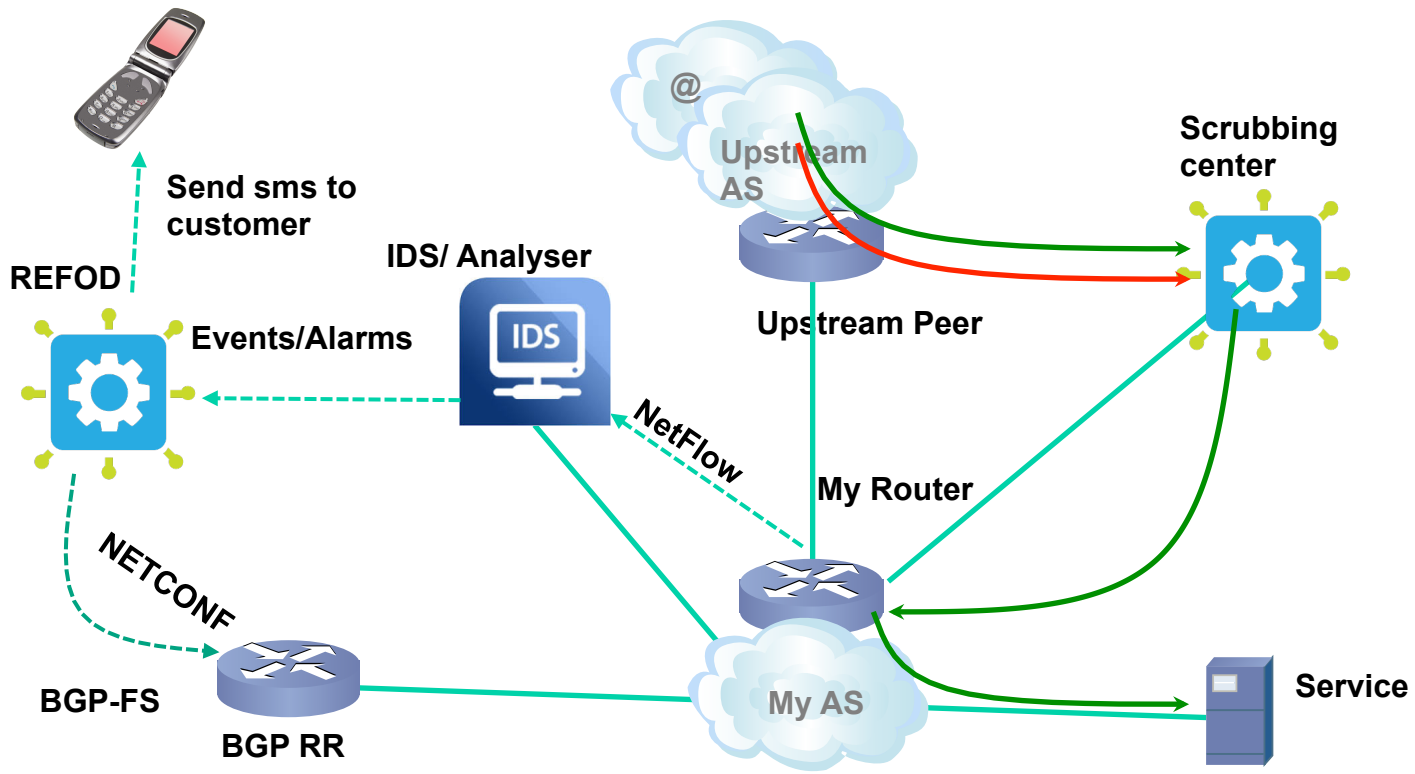
Siguientes pasos

Como funciona la solución:



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

¿Quizás el Futuro?



¿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

XV Jornadas de REDIMadrid

20 de octubre de 2020