

REDIMadrid: Situación actual del análisis de ataques DDOS en REDIMadrid

**David Rincón
Alicia Cardeñosa**

**XVII Jornadas de REDIMadrid
18 de octubre de 2022**



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



Licitación de software para análisis DDoS

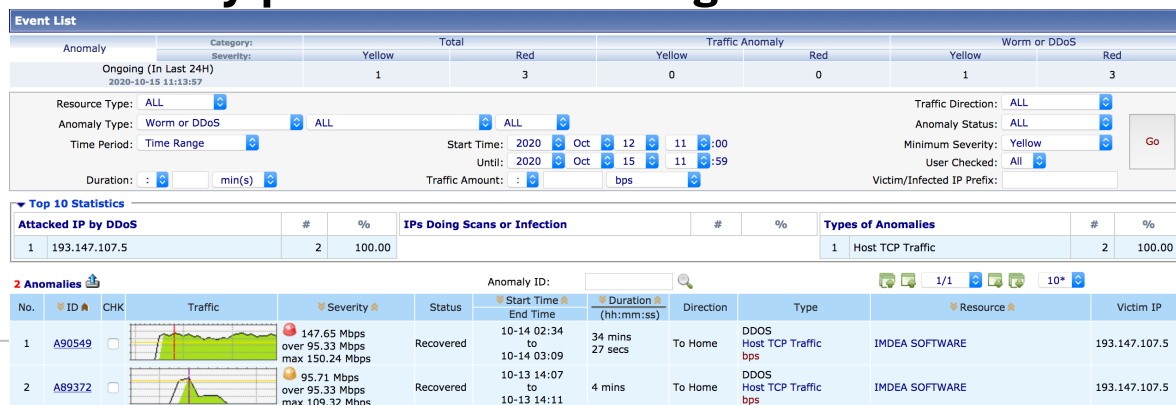
- En 2020 Se adjudica el contrato al licitador Axians que presenta una solución del fabricante Genie Networks con el producto GENIE-ATM (REM-Golem). La licitación tenía por objetivo buscar una solución abierta que nos diera visibilidad de los ataques DDoS se estaban produciendo.



- Entre 2021 y comienzos de 2022 se finaliza la configuración a nivel general de la herramienta. Problemas para afinar la herramienta debido al teletrabajo.





- Actualmente esta totalmente configurada y operativa, las instituciones tienen acceso a la herramienta y pueden hacer un seguimiento de los ataques que reciben.



The screenshot displays the 'Event List' interface with various filters and a table of detected anomalies. The 'Attacked IP by DDoS' table shows 100% of traffic targeting 193.147.107.5. The 'Anomalies' table lists two specific DDoS events, both identified as 'IMDEA SOFTWARE' attacks on 'Host TCP Traffic'.

Event List									
Anomaly	Category	Severity	Total	Red	Yellow	Traffic Anomaly	Red	Yellow	Worm or DDoS
Ongoing (In Last 24H)			1	3	0		0	1	3

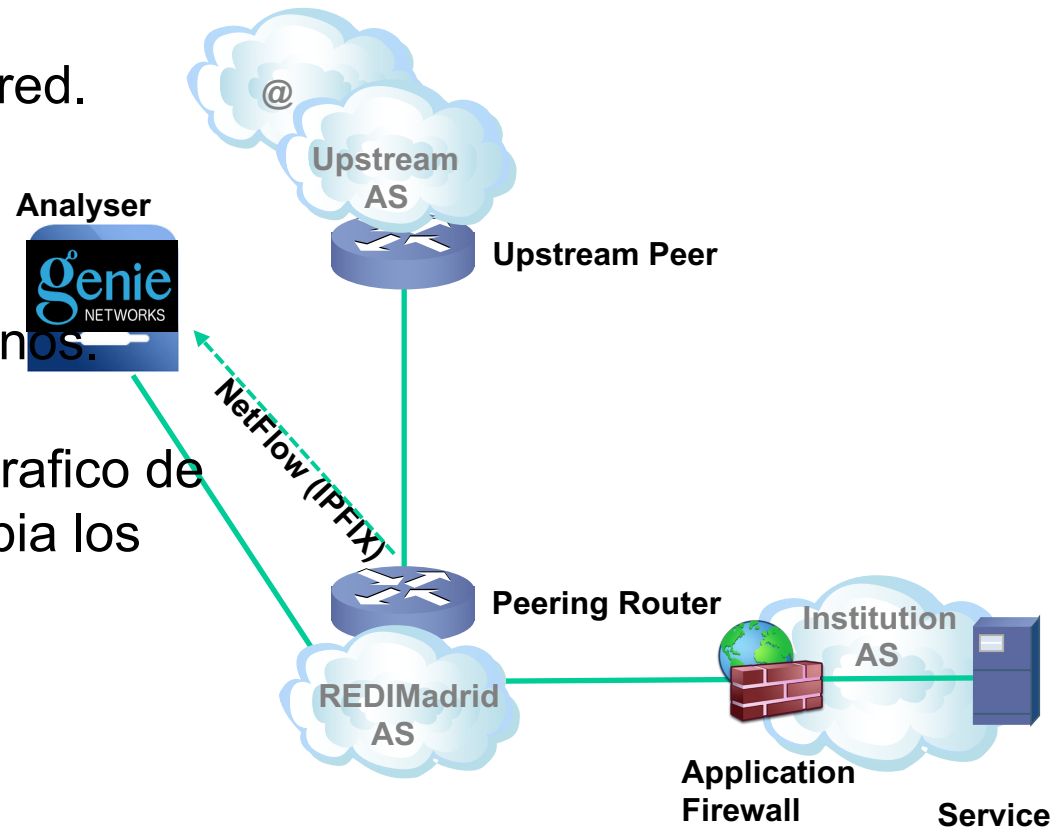
Attacked IP by DDoS				IPs Doing Scans or Infection				Types of Anomalies			
#	%	#	%	#	%	#	%	#	%		
1	100.00	2	100.00	1	100.00	2	100.00	1	100.00		

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	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	IMDEA SOFTWARE	193.147.107.5

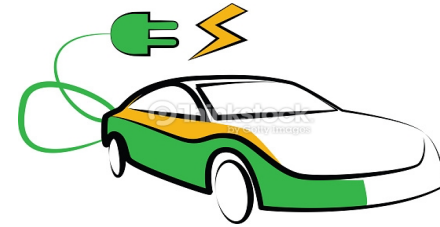
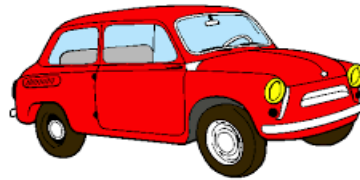
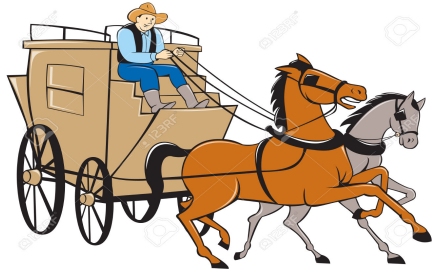


Solución de análisis de DDoS (REM-Golem)

- Genie ATM utiliza Netflow (IPFIX) y los datos recibidos vía SNMP para detectar ataques DDoS.
- No es necesario insertar el analizador físicamente en la red.
- La herramienta es versátil, detecta tanto ataques DDoS como tráfico anómalo y gusanos.
- La herramienta aprende del tráfico de la institución y cada día cambia los umbrales.
- Tiene una API abierta para soluciones de mitigación externas (REMeDDoS).



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 tráfico de la maquina que se compromete.

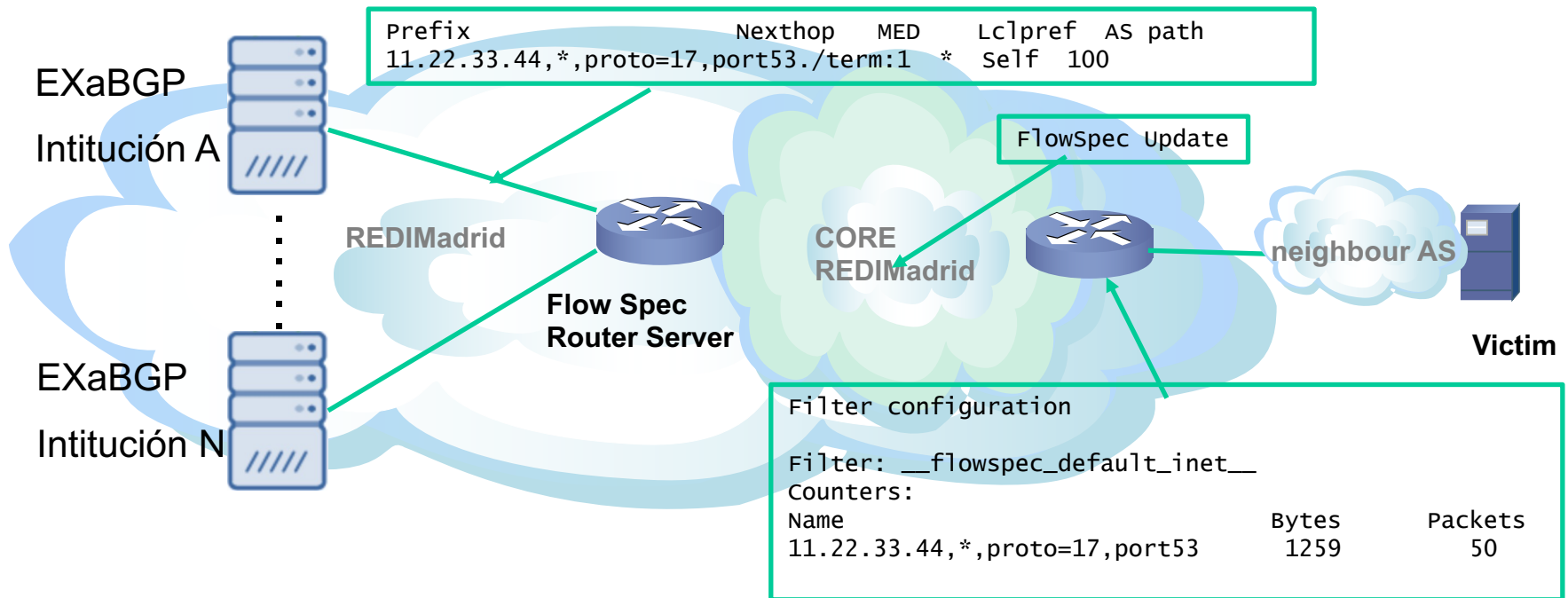
2009

BGP-FS

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

ExaBGP → Antigua solución para mitigar ataques

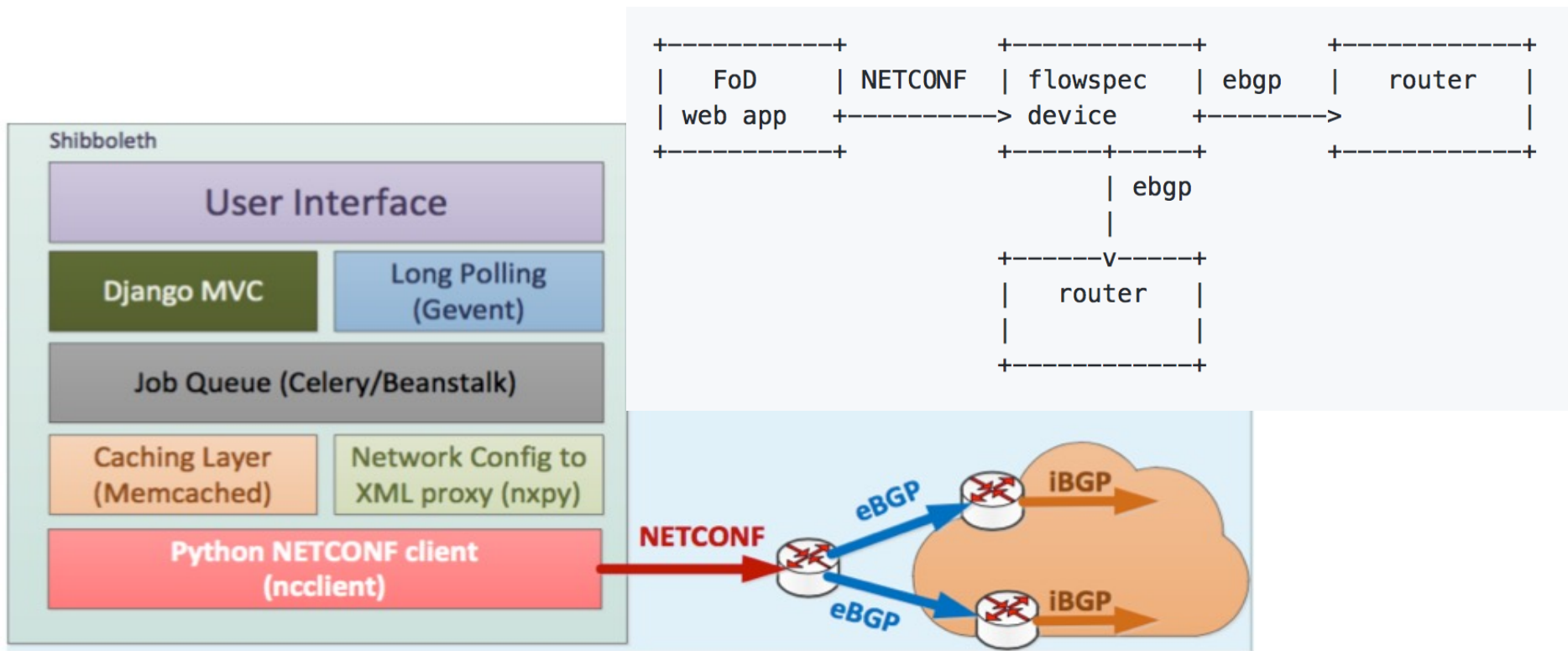
- La antigua solución de REDIMadrid para anunciar rutas BGP-Flow-Spec fue utilizar ExaBGP.
- Se implanto esta solución como algo transitorio hasta que estuviera en servicio la aplicación REMeDDoS.



REMeDDoS nuevo software visual de mitigación de ataques.



REDIMadrid ha desarrollado una herramienta visual para poder realizar mitigación de ataques con bgp-flowspec, la solución se basa en una herramienta liberada por GEANT llamada FOD, esta herramienta ha sido modificada y actualizada.



- REM-GOLEM detecta el ataque y envía esta información a REM-e-DDOS a través de webhook y preguntas por API.
- Se avisa a la institución a través de Slack y/o e-mail, donde recibirá toda la información relevante del ataque, así como su progreso y finalización.



REMeDiDoS APP 14:50

Nuevo ataque DDoS contra el recurso 'punch.software.imdea.org' con id A393097 de tipo ['TCP SYN Flooding']. Consulte nuestra [web](#) donde se podrán ver las reglas propuestas para mitigar el ataque. Para más información sobre el ataque visite el siguiente link: https://193.145.15.26:443/atm_popup_anomaly?anomaly_info=MSwyMDlyMTAsNCxBMzkzMDk3.

El ataque DDoS con id A393097 de tipo ['TCP SYN Flooding'] a la institución punch.software.imdea.org persiste y hemos actualizado los datos del ataque. Consulte nuestra [web](#) donde se podrán ver las reglas propuestas para mitigar el ataque. Para más información sobre el ataque visite el siguiente link: https://193.145.15.26:443/atm_popup_anomaly?anomaly_info=MSwyMDlyMTAsNCxBMzkzMDk3.







El ataque DDoS con id A393097 a la institución punch.software.imdea.org ha terminado. Más información en [REMeDDoS](#) o REM-GOLEM.

- REM-e-DDoS propondrá automáticamente reglas de firewall (que se irán actualizando) en base a la información que reciba desde REM-GOLEM.

Reglas propuestas para mitigar el ataque: [A393097](#)

Las reglas se crean en base a la información que se recibe desde la aplicación REM-GOLEM. Los valores seleccionados son ip origen, protocolo y puerto con mas tráfico así como los valores propio del protocolo como pueden ser tcpflags, icmptype e icmpcode.

← REM-GOLEM events

ID	Creación	Dir Destino	Dir Origen	Más información	Estado	Otros
A393097_Punch_1	14:50, 13 Oct 2022	193.147.107.24	41.105.101.84	Protocolo: tcp Port: 123	PROPOSED	  
A393097_Punch_2	14:54, 13 Oct 2022	193.147.107.24	81.130.177.140	Protocolo: tcp Port: 123	PROPOSED	  



- La información relacionada con los ataques se registrará en REM-e-DDoS durante una semana, aún así los eventos también pueden ser vistos en REM-GOLEM.
- Nos tomamos en serio la seguridad:
 - Protección del espacio de cada institución → solo puedes aplicar reglas de tu espacio de direccionamientos.
 - Revisión diaria de REMeDDoS.
 - Doble factor de autenticación para configurar una regla.

REM-e-DDoS
Aplicación diseñada para la mitigación de ataques, aquí podrá configurar reglas de firewall que le ayude a proteger su red. Está aplicación también recoge información desde REM-Golem para informarle a través de Slack sobre los últimos ataques que haya recibido, proponiendo a su vez distintas reglas que usted podrá personalizar a su gusto. Para más información:

Show 5 entries Search:

Nombre	Creada	Mas información	Estado
pgtest_Punch	10:20, 13 Oct 2022	193.145.15.29/32 0.0.0.0/0 Protocolo: icmp	ACTIVE

Showing 1 to 1 of 1 entries Previous 1 Next

Shortcuts

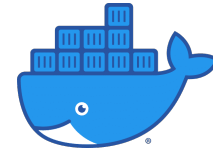
- Añadir Regla
- Reglas
- Reglas propuestas
- Dashboard

Información

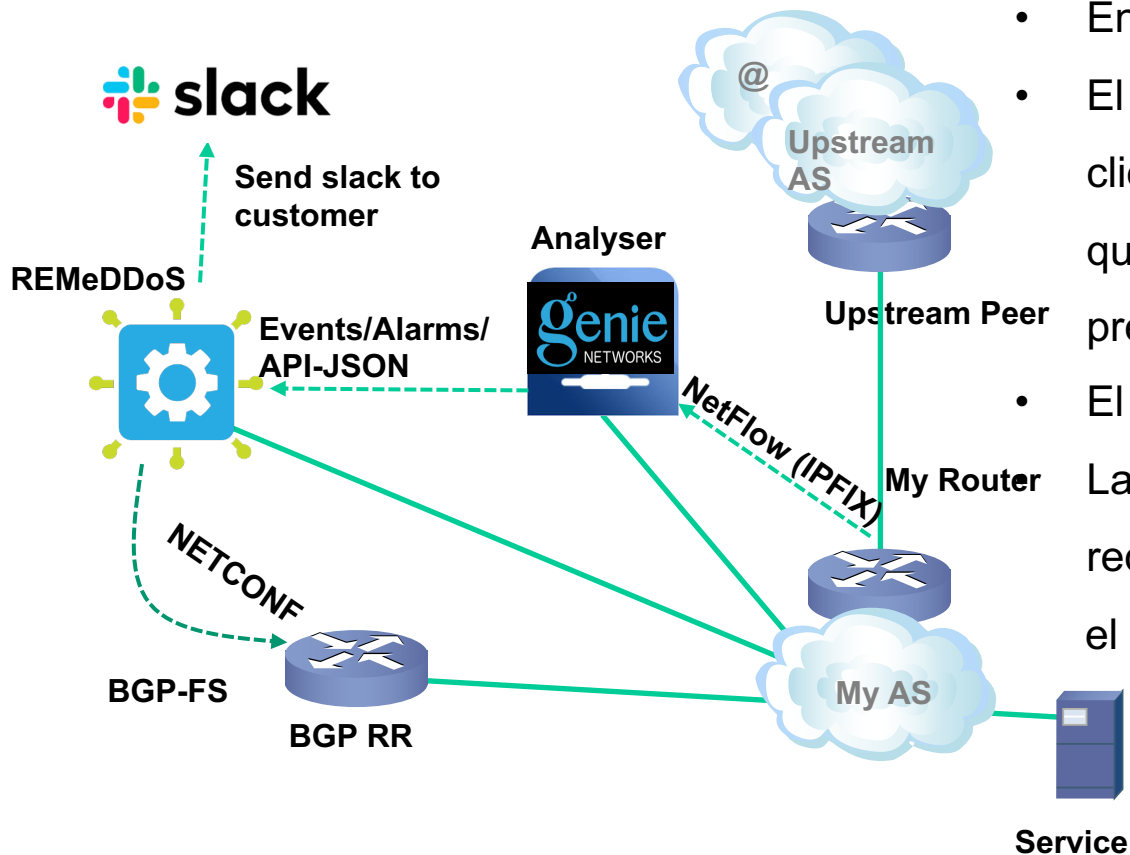
Status: ACTIVE Cuando el estado de una regla es 'ACTIVE' significa que ha sido guardada en su base de datos y configurada en el router.	Status: DEACTIVATED Cuando el estado de una regla es 'DEACTIVATED' significa que ha sido desactivada porque ha expirado.	Status: OUTOFSYNC Cuando el estado de una regla es 'OUTOFSYNC' significa que ha habido algún tipo de problema y la regla solo ha sido configurada en uno de los routers.	Status: PROPOSED Cuando el estado de una regla es 'PROPOSED' significa que ha sido propuesta por REM-e-DDoS, está guardada en la base de datos y está a la espera de ser aplicada al router.	Status: INACTIVE Cuando el estado de una regla es 'INACTIVE' significa que ha sido desactivada por el usuario.	Status: ERROR Cuando el estado de una regla es 'ERROR' significa que ha habido un error a la hora de configurar o eliminar una regla del router, en ese caso por favor contacte con los administradores de la aplicación.
---	--	--	--	--	---



- Cambios de software y versiones mas importes usadas:
 - Django 3.2
 - Python 3.8
 - Docker
- Redundancia de configuración de equipos:
Configuración de reglas en dos router.
- Autenticación con LDAP.
- Integración con REM-GOLEM, Zabbix, Slack.
- Back-up diarios para resincronizar la base de datos con los router y viciversa.
- Control diario de las reglas configuradas entre router y BBD.



Como funciona la solución:



- REM-Golem detecta un DDoS.
- Envía el evento al REMeDDoS.
- El REMeDDoS 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.

REDIMadrid: Situación actual del análisis de ataques DDOS en REDIMadrid

Video demostración



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



Buscamos instituciones interesadas en probar la herramienta



Fechas de implementación:

- **01/11/22** → Comienzo de las pruebas de la herramienta con las instituciones interesadas.
- **31/12/22** → Finalización de pruebas, análisis de las mejoras/cambios propuestos y puesta en servicio si aplica.

¿Nos ayudas a probar la herramienta y proponer mejoras? O simplemente, decirnos que lo que hemos estado haciendo nos os sirve y tenemos que plantearlo todo de nuevo....

Ponte en contacto con nosotros y comenzamos las pruebas.



REDIMadrid: Situación actual del análisis de ataques DDOS en REDIMadrid

PREGUNTAS

XVII Jornadas de REDIMadrid

18 de octubre de 2022



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

