ESpanix

Identificar y mitigar ataques DDoS
Soluciones y tecnologías (para ISPs)

Amedeo Beck Peccoz

ES.NOG34

Barcelona - 30 de octubre de 2025

Advertencia

Transparencias realizadas con IN*

Posible presencia de:

- errores tipográficos
- sarcasmo
- algo útil

IN: Inteligencia Natural – en extinción, suplantada por la artificial

Hoy hablamos de...

Los ataques
Detección
Mitigación
Topologías
Precios
Configuraciones

Incremento de los ataques

Incremento en el número, extensión e intensidad

- número: +358% 2024/2025 Fuente: CloudFlare
- extensión: N x 10min
- intensidad: N x 10Gbps → N x 100Gbps
- hiper-volumétricos

Ataques hiper-volumétricos

> 1Tbps

> 1Bpps

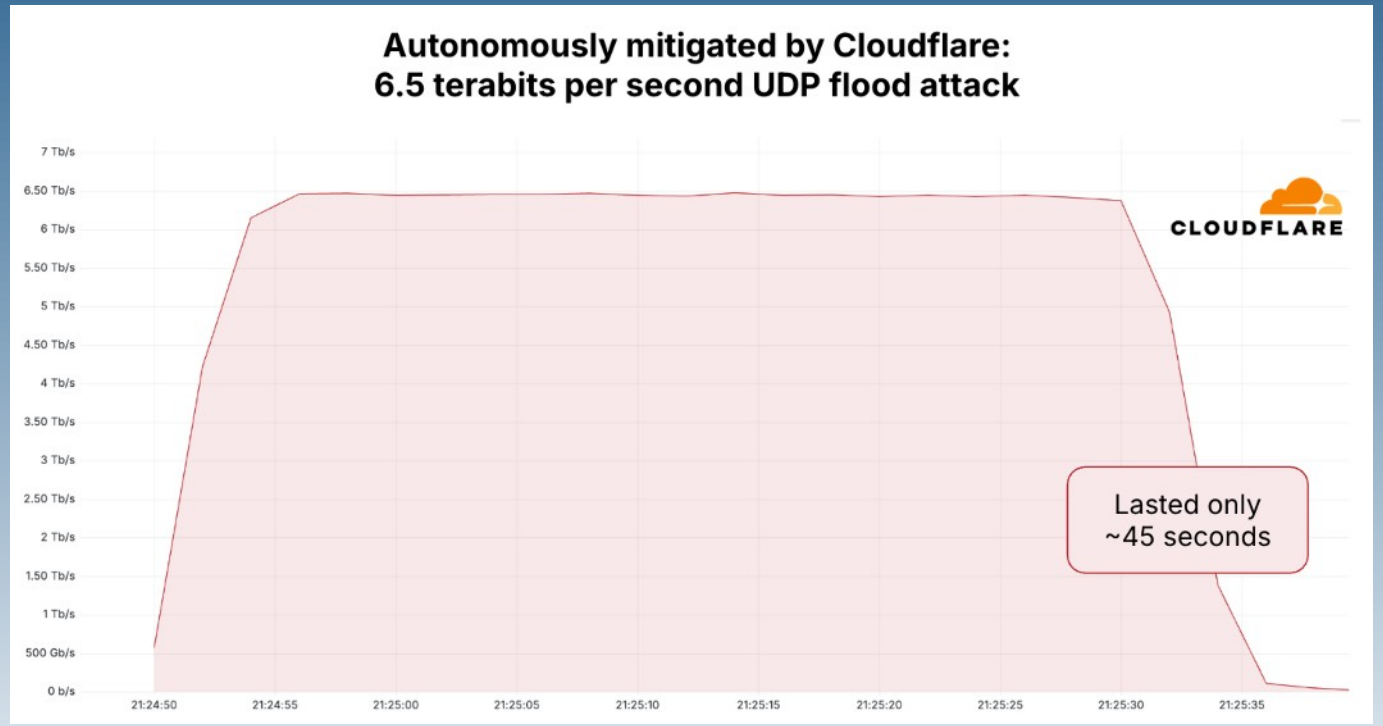
Limitados a pocos segundos (35 - 45)

UDP

Origen IoT (cientos de miles)

Target: grandes operadores que los puedan recibir

Se pueden mitigar



Actores

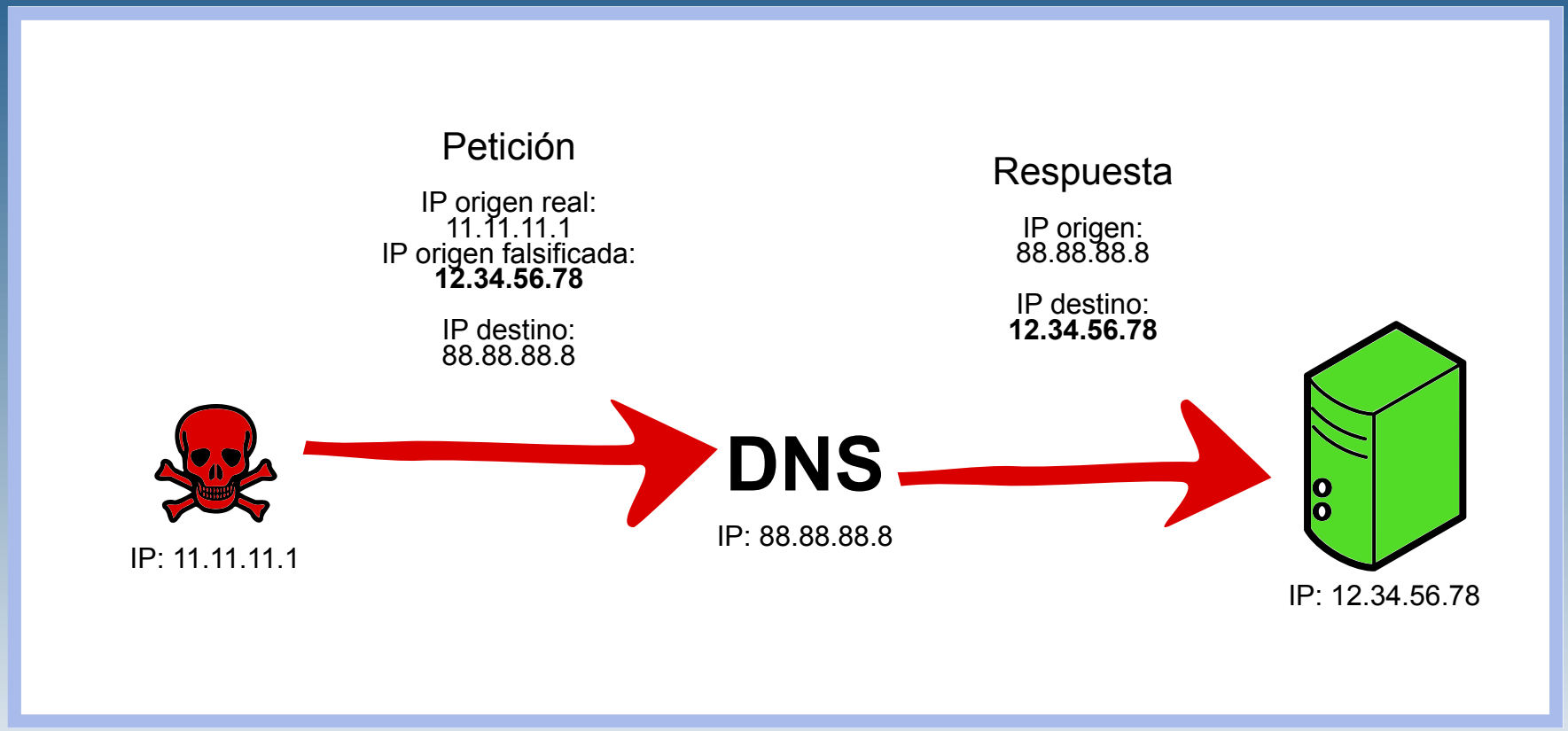
- **No se sabe (la mayoría)**
- Competidor (videojuegos y apuestas)
- Agencia estatal
- Cliente/usuario descontento
- Self-DDoS
- Extorsión
- Ex empleado

Fuente: encuesta de CloudFlare

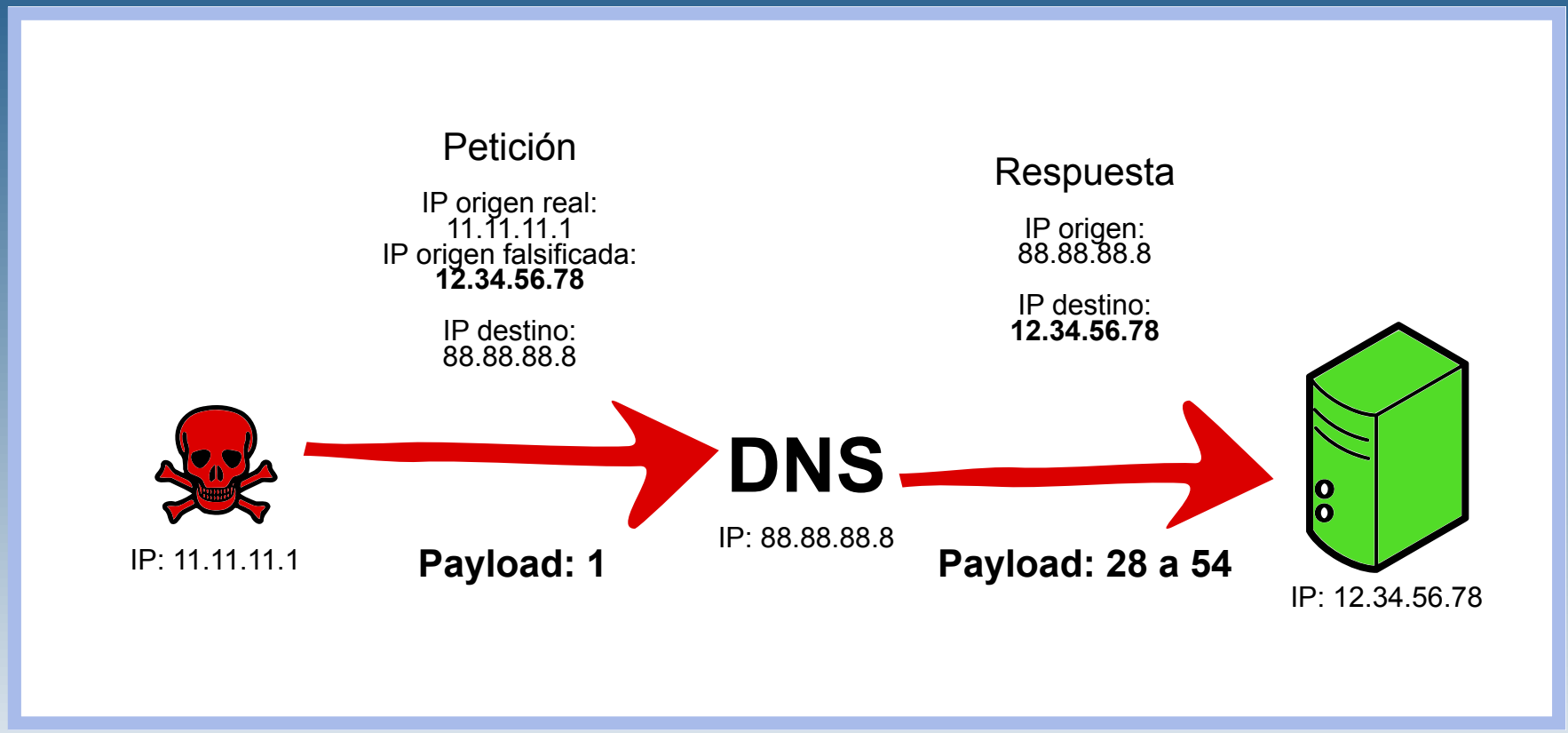
Vectores de ataque

- **SYN Flood**
- **DNS Flood**
- **Mirai (IoT)**
- UDP Flood
- RST Flood
- SSDP Flood
- Amplificación

Falsificación de origen



Amplificación



Ataques de amplificación

- DNS (mDNS) 2-10
- BitTorrent 3,8
- NetBIOS 3,8
- Steam Protocol 5,5
- **SNMPv2 6,3**
- Portmap (RPCbind) 7 a 28
- **DNS 28 a 54**
- SSDP 30,8
- LDAP 46 a 55
- TFTP 60
- Quake Network Protocol 63,9
- RIPv1 131,24
- QOTD 140,3
- CHARGEN 358,8
- **NTP 556,9**
- **Memcached hasta 51.000**

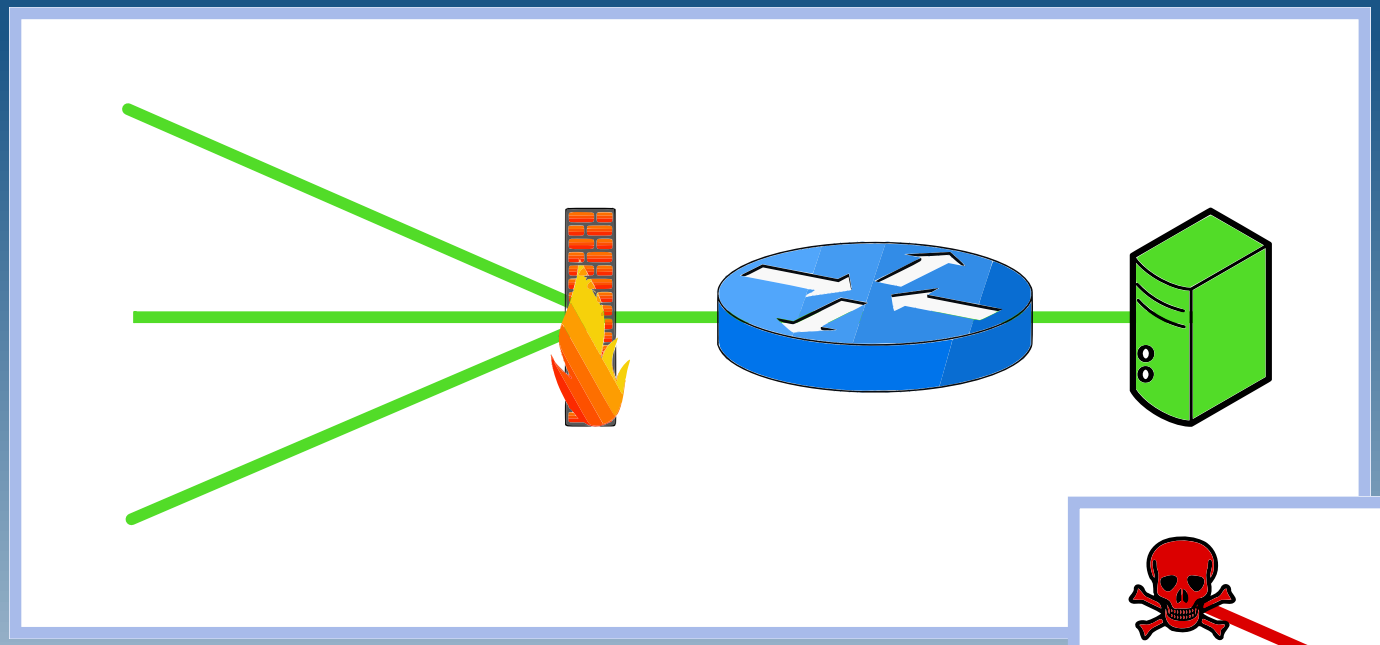
Fuente: Dave Phelan - APNIC

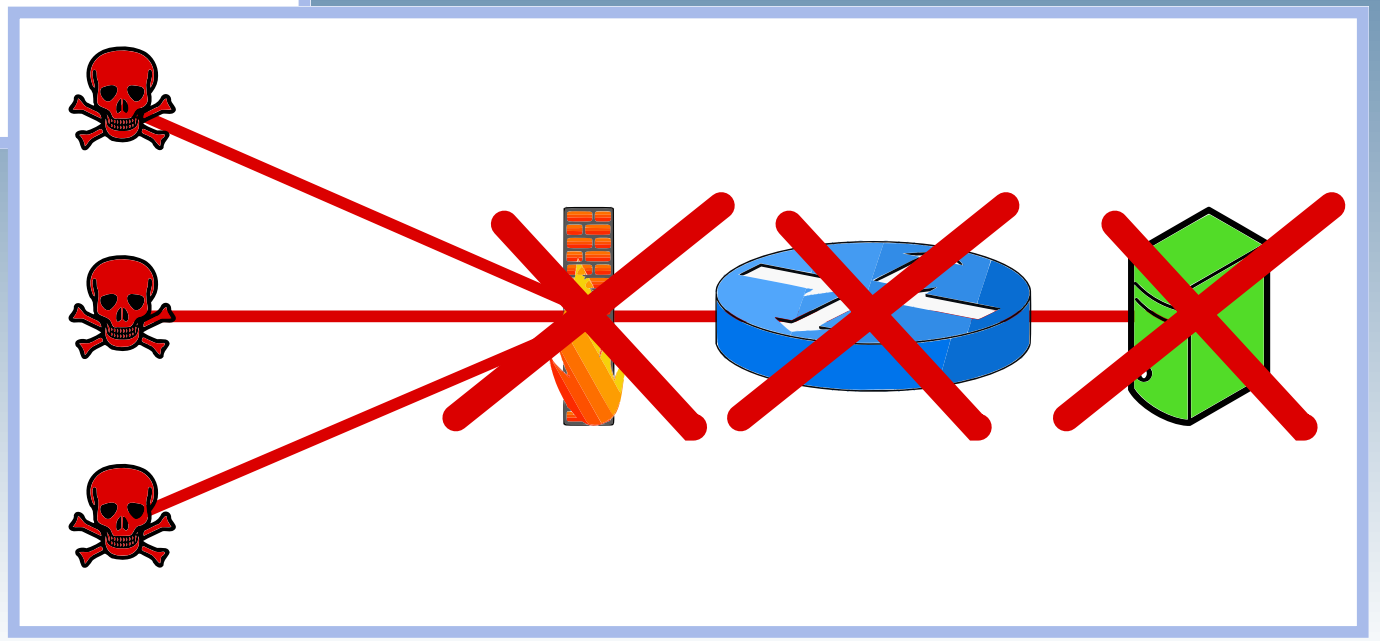
Mirai: la fabrica de Botnets

Usuario	Contraseña	Usuario	Contraseña
666666	666666	root	7ujMko0admin
888888	888888	root	7ujMko0vizxv
admin	(ninguna)	root	888888
admin	1111	root	admin
admin	1111111	root	anko
admin	1234	root	default
admin	12345	root	dreambox

Fuente: https://arxiv.org/pdf/2508.01909
Angela Famera, Ben Hilger, Suman Bhunia, Patrick Heil

Saturación de los upstreams





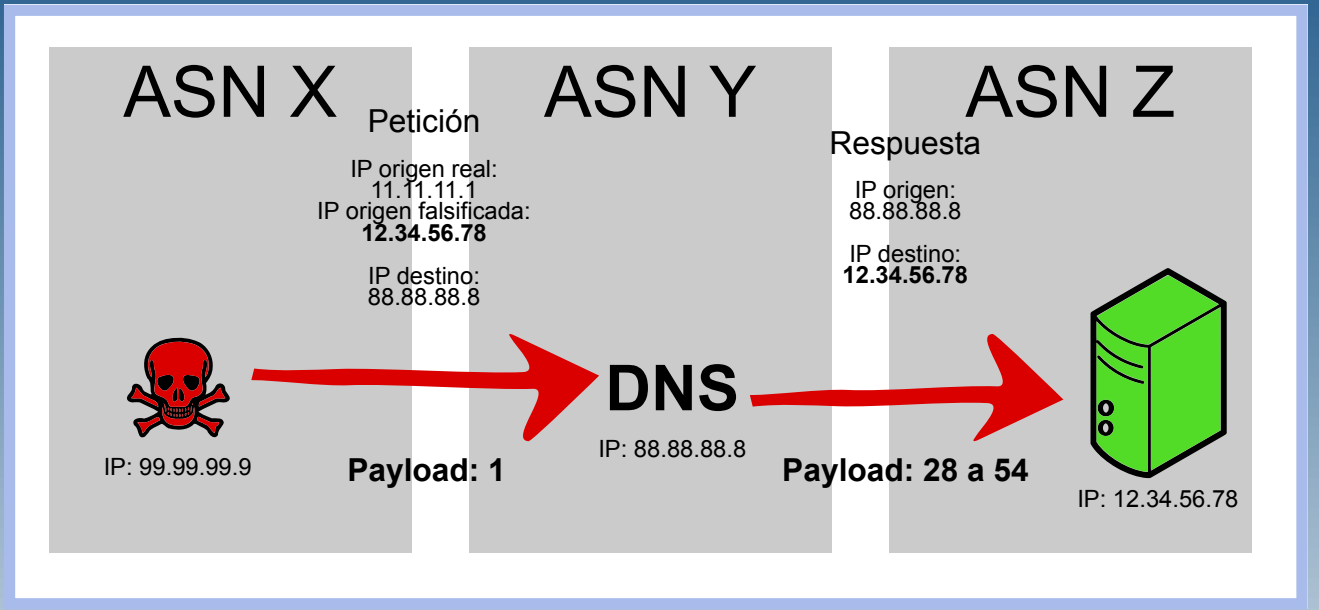
Blackholing

- Blackholing de las IP atacadas
- Permite aliviar la presión en la red
- El ataque tiene éxito
- BGP community 65535:666
- Lo puedes contratar a los upstreams (cuidado con los anuncios más específicos)

Contrastar la falsificación de origen

IETF BCP 38

- Estática: RFC 2827 (p. ej. ACL marcianos)
- Estática multihomed: RFC 3704
- Dinámica (completa): RFC 8704



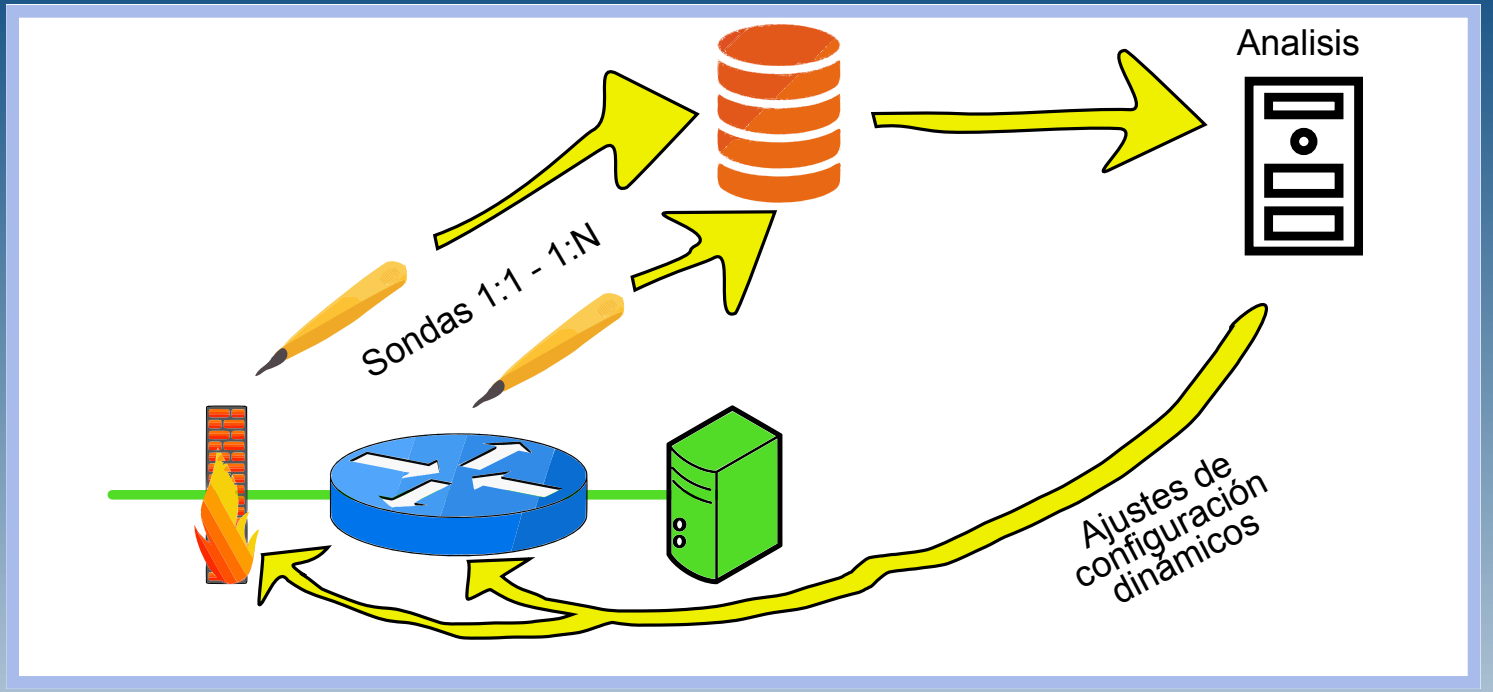
Configuraciones que **reducen** el problema

Por lo menos no eres parte del ataque

Algunos operadores prefieren no aplicar BCP 38 para mover más tráfico

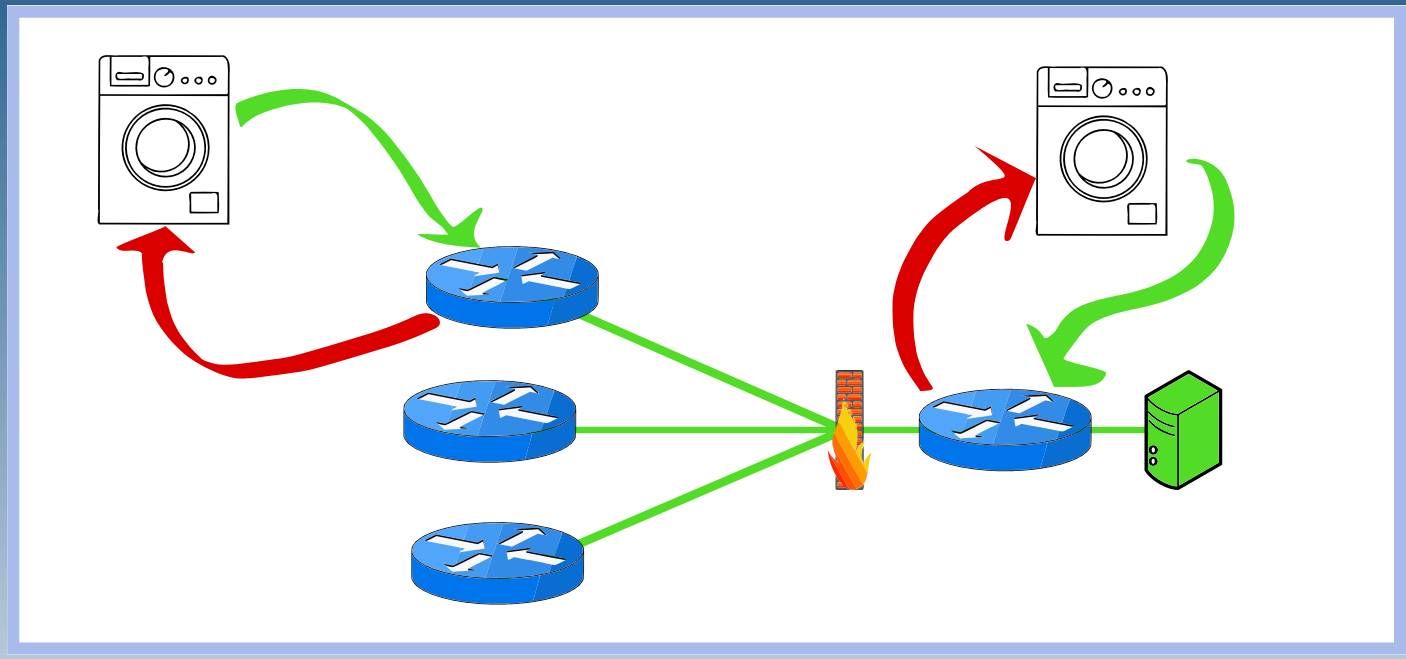
Detección y mitigación (sin lavadora)

- On prem
- Contratado a un tercero o hecho en casa
- Puede ser un upstream
- L3 – BGP flowspec
- L4 – 5 ACLs dinámicas (Netconf)



Detección y mitigación (con lavadora)

- Servicio cloud vs on prem
- Soberanía del dato
- Latencia
- L3-L7
- IA
- Bloquea **sólo** el ataque



Precios

- Por tiempo o eventos / por ancho de banda
- Responsabilidad del cliente / responsabilidad del proveedor
- Recurrente (licencia)

¡Gracias!

Amedeo Beck Peccoz

amedeo@espanix.net