CLOUDFLARE

Tendencias de los ataques DDoS T1 '2022

Francisco Allegro - Territory Account Manager

La red global de Cloudflare

Más de 270

ciudades en más de 100 países, incluida China continental

10 500

redes conectadas directamente a Cloudflare, incluyendo los ISP, proveedores en la nube y grandes empresas

142 Tbps

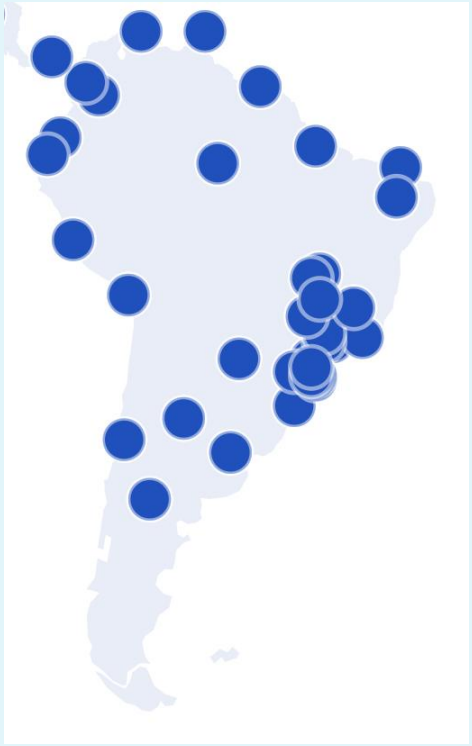
de capacidad y crecimiento del perímetro de la red

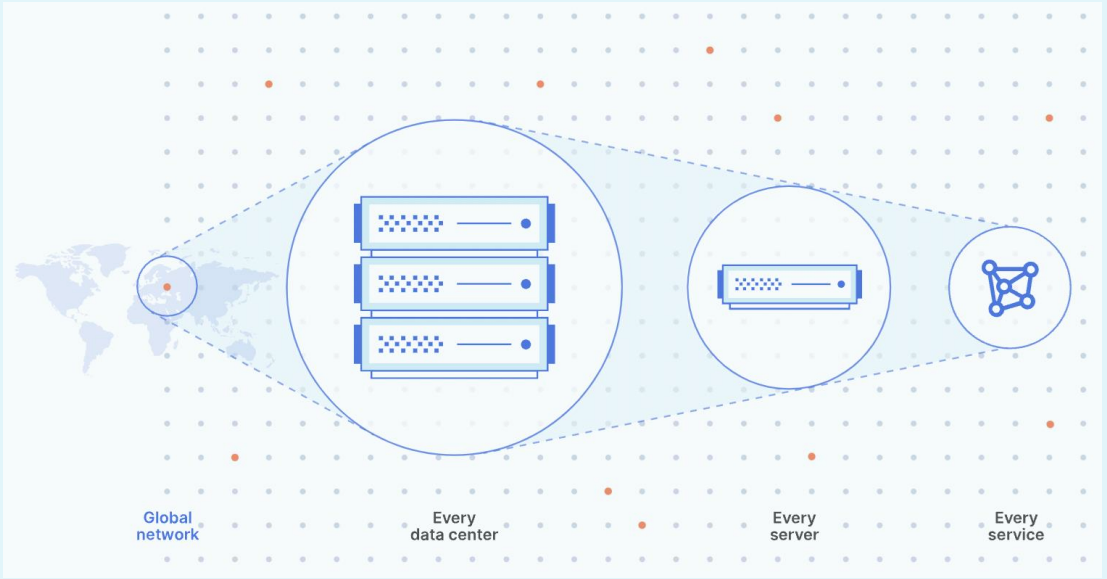
86 000 millones

de amenazas cibernéticas bloqueadas por día en el T3 '21

CLOUDFLARE

● = Ciudad de Cloudflare (datos del mapa al 15 de septiembre de 2021)





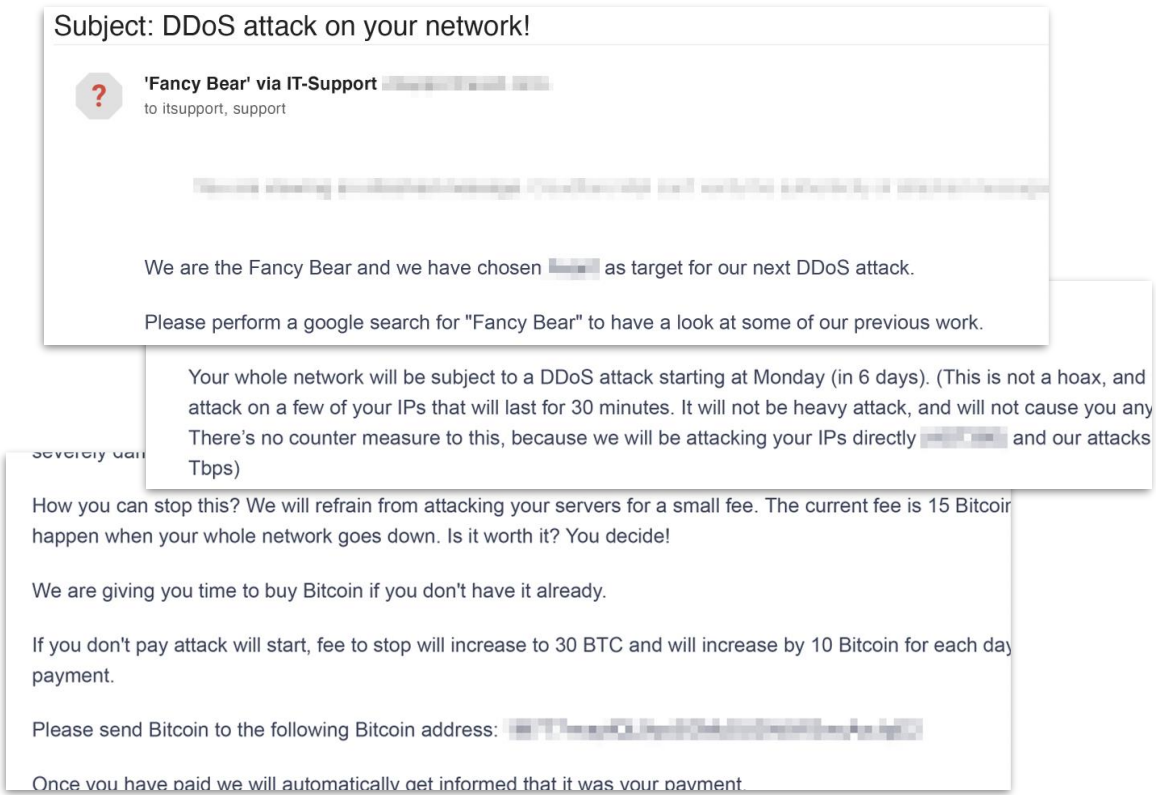
Servicio en 45 Ciudades en Latinoamérica

Ransom DDoS Attacks

CLOUDFLARE

Los ataques de Ransomware y Ransom-DDoS (RDDoS) siguen incrementándose

- Organizaciones de todos los tamaños y zonas geográficas están siendo víctimas
- Grupos que dicen ser: REvil, Fancy Bear, Cozy Bear, Lazarus
- Lanzamiento de un pequeño ataque DDoS como demostración de la capacidad
- Exigir el pago del rescate en bitcoin



Subject: DDoS attack on your network!

'Fancy Bear' via IT-Support [redacted]
to itsupport, support

[redacted]

We are the Fancy Bear and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" to have a look at some of our previous work.

Your whole network will be subject to a DDoS attack starting at Monday (in 6 days). (This is not a hoax, and attack on a few of your IPs that will last for 30 minutes. It will not be heavy attack, and will not cause you any There's no counter measure to this, because we will be attacking your IPs directly [redacted] and our attacks Tbps)

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 15 Bitcoir happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Once you have paid we will automatically get informed that it was your payment

¿Qué hacer si recibe una nota de rescate?

Recomendamos no pagar el rescate

Pagar el rescate solo alienta a los atacantes.

No hay garantía de que no ataquen su red ahora o más tarde.

Notifique a las autoridades locales

También es probable que soliciten una copia de la carta de rescate que recibió.

Contacte a Cloudflare

Podemos ayudarlo a garantizar que su sitio web y su infraestructura de red estén protegidos contra ataques de cualquier tamaño o tipo.

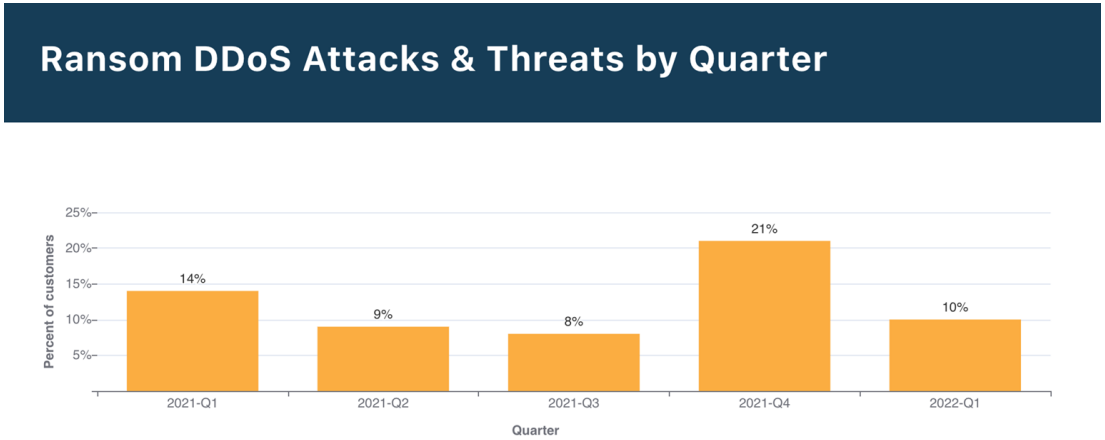
CLOUDFLARE

Tendencias de los ataques DDoS T1 '22

Ataques DDoS a la capa de aplicación (HTTP) Capa 7

Ataques DDoS de rescate (Ramson DDoS)

- En el primer mes de T1, el 17% de los clientes que estaban bajo ataque reportaron que recibieron una notificación de amenaza previa. Febrero bajó a un 6% y Marzo 3%.
- Comparándolo con el T anterior, los ataques decrecieron un 52%

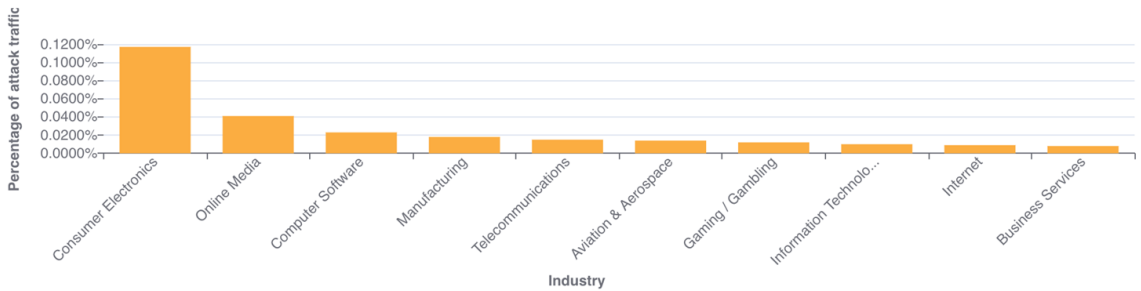


Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Industrias que más sufrieron ataques DDoS

- Consumos Electrónicos fue la Industria más atacada con un crecimiento del 5086% T/T
- Segunda fueron los Medios Online con 2031% de crecimiento T/T y en tercer lugar las compañías de Computer Software con 76% T/T

Application-Layer DDoS Attacks - Distribution by industry

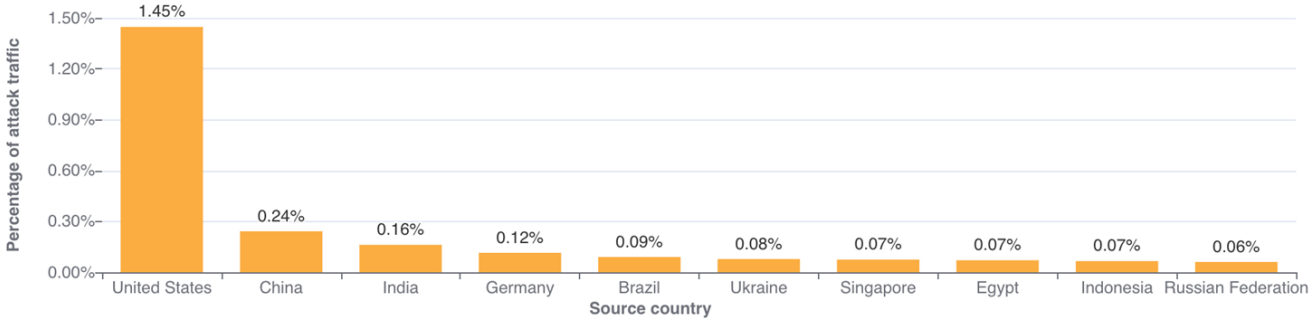


Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Dónde se origina la mayoría de los ataques DDoS

- Después de 4 T seguidos donde China encabeza la lista con el porcentaje más alto de ataques de tráfico, US registró un aumento del 6777% T/T

Application-Layer DDoS Attacks - Distribution by source country

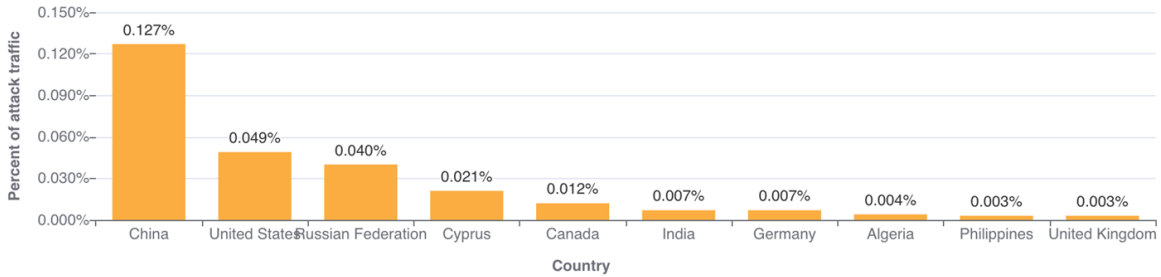


Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Países que más sufrieron ataques DDoS

- Después de 3 trimestres consecutivos donde el target era US, ahora el país más atacado es China. Seguido por US, Rusia, Chipre y Canadá respectivamente.

Application-Layer DDoS Attacks - Distribution by target country

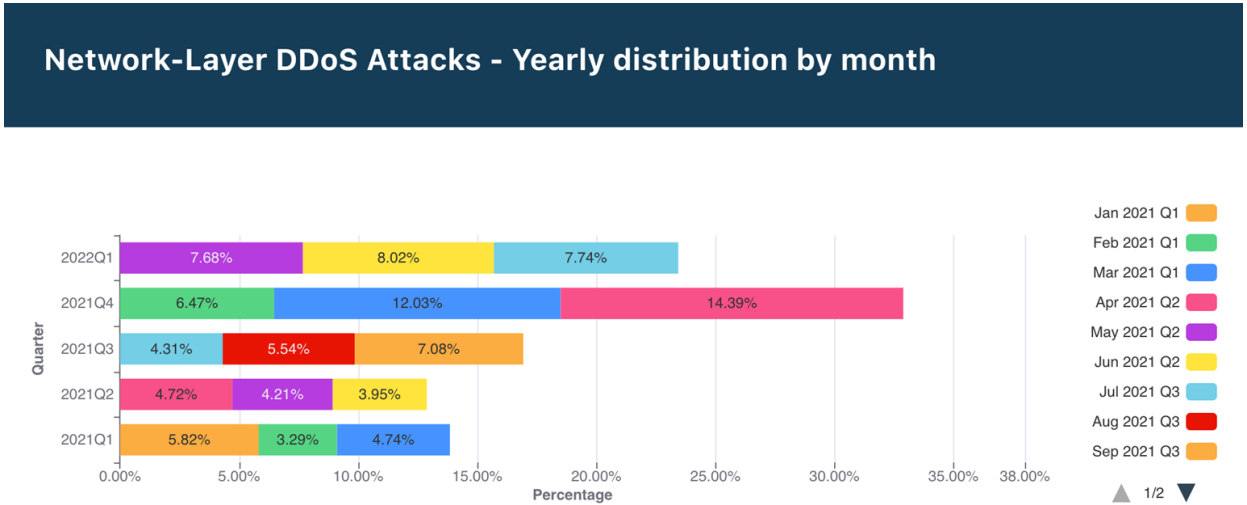


Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Ataques DDoS a la capa de red (capas 3/4)

Network Layer -Ataques DDoS por mes

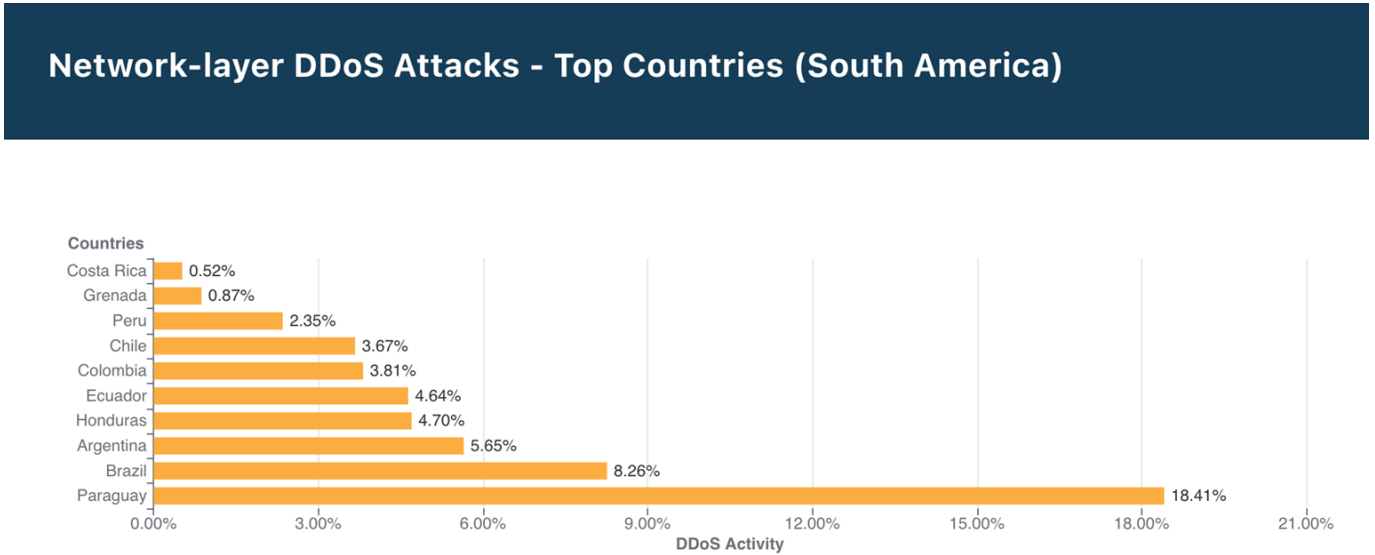
- El T1 '22 Decreció 58% comparado al trimestre anterior pero anualmente los ataques crecieron un 71%



Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

¿Qué pasa en Latinoamérica?

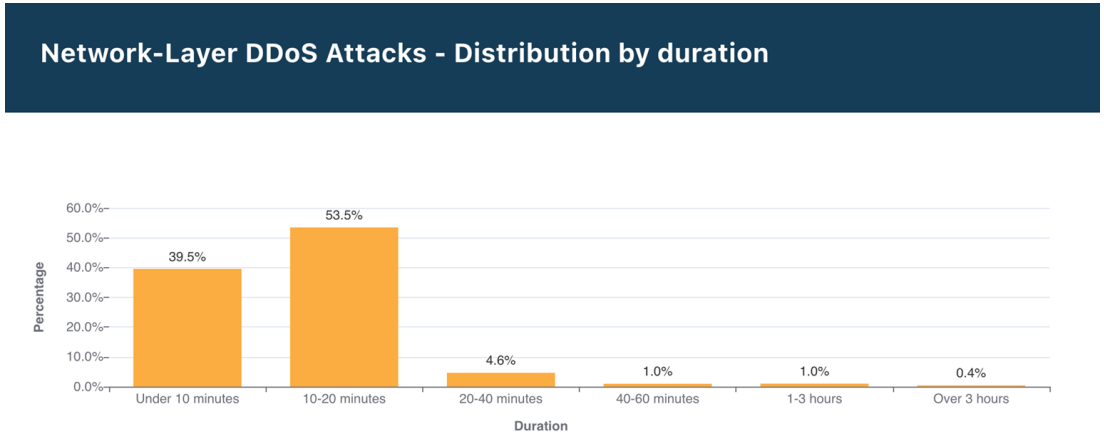
- De todo el tráfico en Argentina el 5,65% es originado por ataques de capa 3 y 4. SYN flood sigue siendo el vector de ataque más utilizado.



Source: https://radar.cloudflare.com/notebooks/undefined

Ataques por velocidad de bits

- Mientras que los ataques por encima de 1 Tbps son cada vez más frecuentes, la mayoría de los ataques aún son pequeños con picos por debajo de los 500 Mbps (94,7 %).
- El tiempo del ataque es menos de 1 hora, por eso recomendamos tener siempre una herramienta automática y activa para redireccionar paquetes, bytes o request a nuestra red de Cloudflare Global



Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Protección DDoS de Cloudflare

Protección frente a DDoS, en cada capa del Modelo OSI

7	Capa de aplicación
6	Capa de presentación
5	Capa de sesión
4	Capa de transporte
3	Capa de red
2	Capa de enlace de datos
1	Capa física

Cloudflare WAF y CDN
Proxy inverso de capa 7

Cloudflare Spectrum
Proxy inverso de capa 4

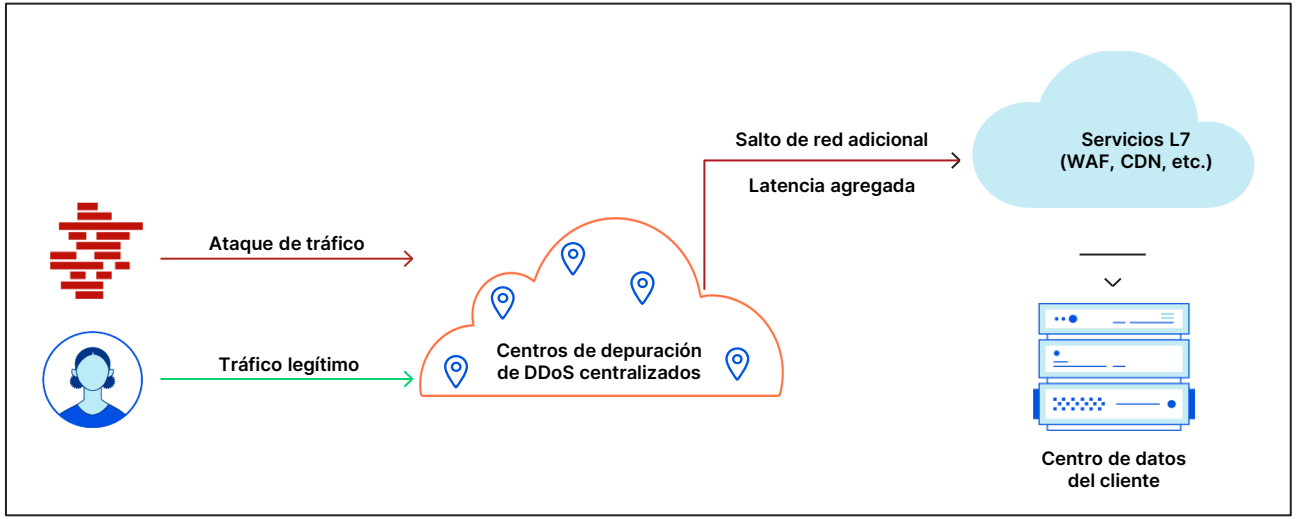
Magic Transit de Cloudflare
Enrutamiento de capa 3

Protección DDoS de Cloudflare

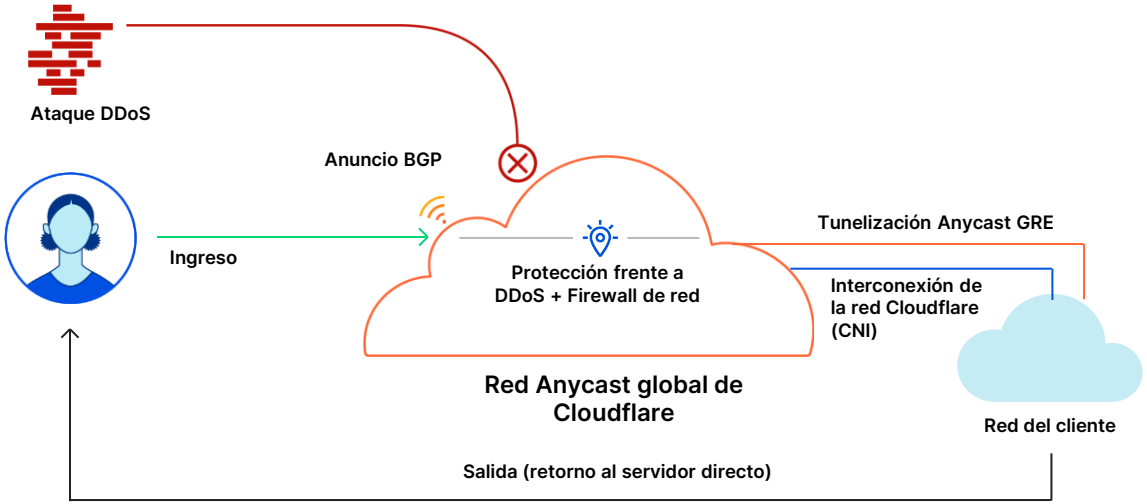
CLOUDFLARE

No todos los proveedores de nube se construyen de la misma manera

- Los "centros de depuración" centralizados y exclusivos son **puntos de congestión para el tráfico de la red**
- El tráfico se reenvía **a centros de datos alternativos** para servicios L7 adicionales (como inspección WAF, CDN, etc.)
- Esto provoca una **latencia inaceptable**



Bloquea ataques DDoS. De cualquier tamaño, cualquier protocolo y sin importar su origen



Conectar

Con los anuncios de ruta BGP, Cloudflare absorbe el tráfico de la red del cliente

Proteger y procesar

Todo el tráfico se inspecciona de manera automática e inmediata para detectar ataques

Acelerar

El tráfico limpio se redirige a la red del cliente a través de la tunelización Anycast GRE o de las conexiones directas

La diferencia del DDoS de Cloudflare

Arquitectura moderna y distribuida

- Capacidad de red de 1—-0 Tbps
- Menos de 3 s de TTM a nivel global, 0 s de TTM para reglas estáticas
- Sin centros de depuración, mitiga los ataques DDoS más cerca a la fuente

Información para detectar amenazas a escala

- Información sobre amenazas aprovechada de millones de propiedades de Internet en Cloudflare
- Modelos de aprendizaje automático impulsan la creación de nuevas reglas que se implementan en segundos a nivel global
- Como un sistema inmunológico para Internet

Fácil de usar y rentable

- Incorporación e implementación en minutos y horas, no en días y semanas
- Creación de reglas con autoservicio y fácil implementación, sin necesidad de contratar servicios profesionales
- Protección frente a DDoS ilimitada y gratuita

CLOUDFLARE

Gracias!

Fallegro@cloudflare.com

https://radar.cloudflare.com/ -> Sitio sobre estadísticas

https://radar.cloudflare.com/notebooks/ddos-2022-Q1 -> Reporte completo

https://blog.cloudflare.com/26m-rps-ddos/ > Blog

https://www.cloudflare.com/magic-transit/ -> Magic Transit Landing Page

https://www.cloudflare.com/es-es/under-attack-hotline/ -> Linea de emergencia

https://www.cloudflare.com/es-es/ransom-ddos/ -> Ransom DDoS , que hacer