Midiendo RPKI

Geoff Huston
João Damas
APNIC

Midiendo RPKI

Filtrado por validación de origen

João Damas
Geoff Huston
APNIC

Seguridad en Routing

¿Cuál es el objetivo de la seguridad en routing?

Seguridad en Routing

¿Cuál es el objetivo de la seguridad en routing?

- ❑Proteger el sistema de routing de todas las formas de accidentes en los operadores?
- ❑Proteger el sistema de routing de algunas las formas de accidentes en los operadores?
- ❑Proteger el sistema de routing de todos los ataques?
- ❑Proteger el sistema de routing de algunos ataques?
- ❑Prevenir el encaminamiento de prefijos *bogus*
- ❑Prevenir el uso de AS *bogus* en el sistema?
- ❑Prevenir la inyección de rutas sintéticas en el sistema de routing?
- ❑Prevenir retiradas (withdrawal) de rutas sin autorización?
- ❑Proteger a los usuarios de redireccionamientos?

Pasito a pasito!

Por ahora un sistema que asegurase que las rutas de BGP son correctas desde el punto de vista de protocolo y de “policy” supera lo que BGP y sus mecanismo de control pueden hacer.

La Validación de Origen de Ruta (Route Origin Validation, ROV) se ha diseñado para evitar que los routers BGP no acepten y/o prefieran rutas que no están autorizadas por el “dueño” del prefijo.

La intención de evitar preferir rutas no autorizadas es evitar que el trafico de los usuarios vaya por esas rutas

Seguridad en Routing

¿Cuál es el objetivo de la seguridad en routing?

- ❑Proteger el sistema de routing de todas las formas de accidents en los operadores?
- ❑Proteger el sistema de routing de algunas las formas de accidents en los operadores?
- ❑Proteger el sistema de routing de todos los ataques?
- ❑Proteger el sistema de routing de algunos ataques?
- ❑Prevenir el en-rutamiento de prefijos bogus
- ❑Prevenir el uso de AS bogus en el sistema?
- ❑Prevenir la inyección de rutas sintéticas en el sistema de routing?
- ❑Prevenir retiradas (withdrawal) de rutas sin autorización?
- ☑Proteger a los usuarios de redireccionamientos?

Nuestro Objetivo

- Medir el impacto del filtrado de rutas inválidas en los usuarios
- Nuestra pregunta es desde el punto de vista de los usuarios
  - **¿Qué proporción de usuarios no pueden llegar a un destino cuando la ruta a ese destino es inválida según ROV?**
- Nuestra idea es medir esto de forma continuada en el tiempo y a largo plazo para observar el despliegue de filtrado RoV en los próximos meses y años

Producción vs consumo

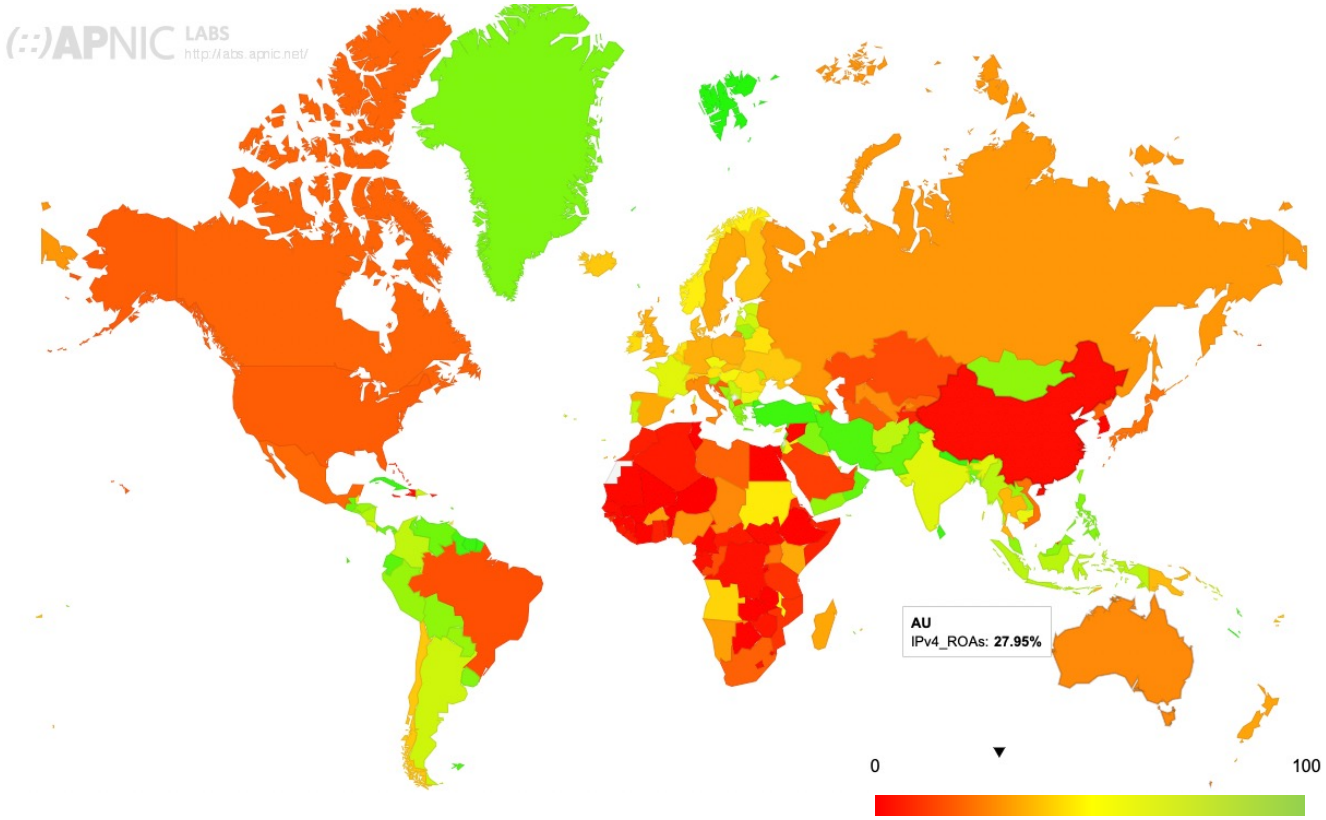
Este sistema tiene dos aspectos distintos:

- Generar ROAs para describir el origen autorizado para los prefijos
- Observar que redes permiten y propagan rutas inválidas.
  - O sea, que redes no están llevando a cabo filtrado BGP que descarte rutas inválidas en los anuncios de BGP

Producción

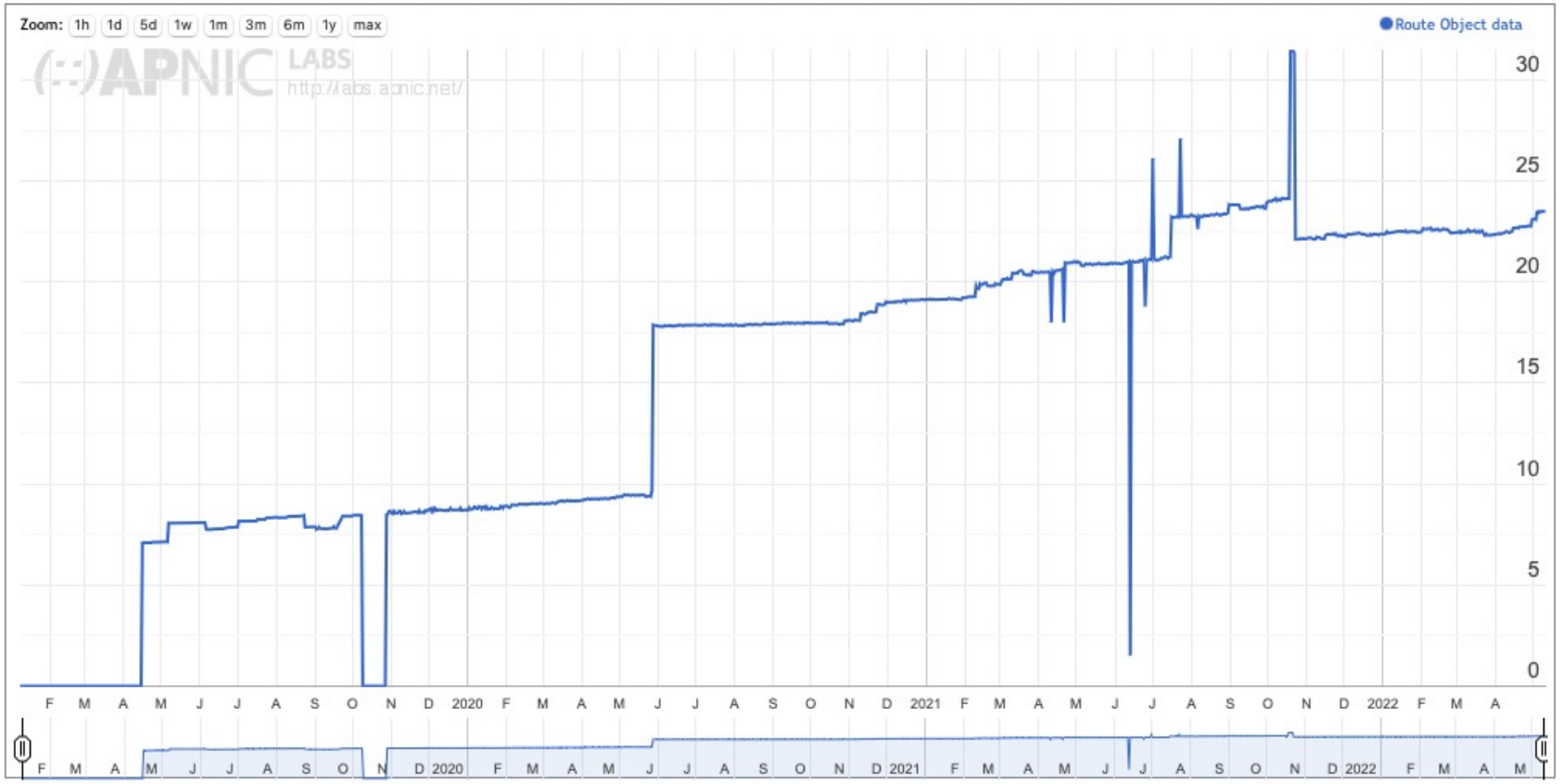
¿Cómo va la cosa país a país?

https://stats.labs.apnic.net/roas



ROAs en las redes españolas

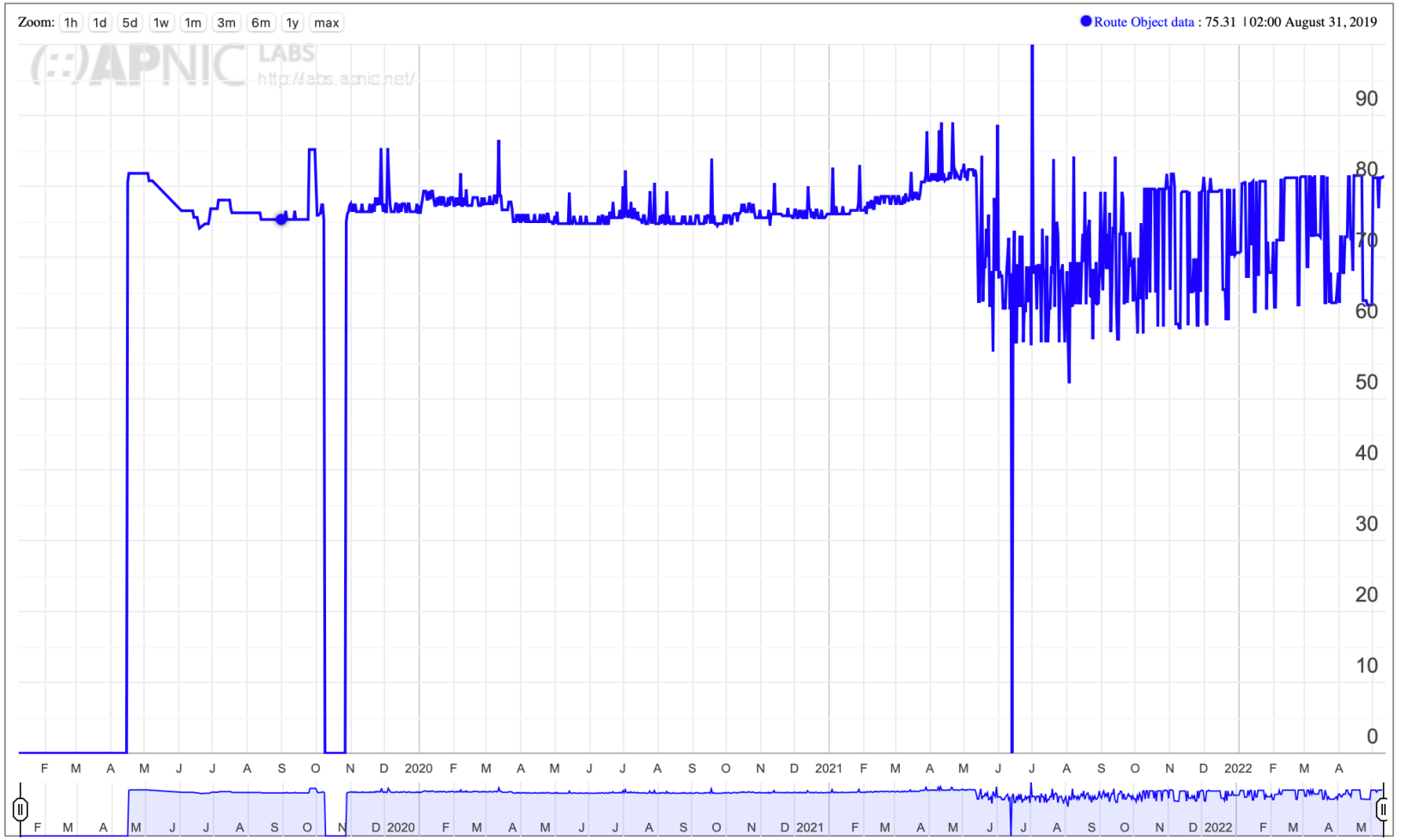
Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv4**, **Percent** (of Total)



ROAs for individual networks

RPKI ROA-Validation of Advertised Routes for AS35699: ADAMOEU-AS Adamo Telecom Iberia S.A., Spain (ES)

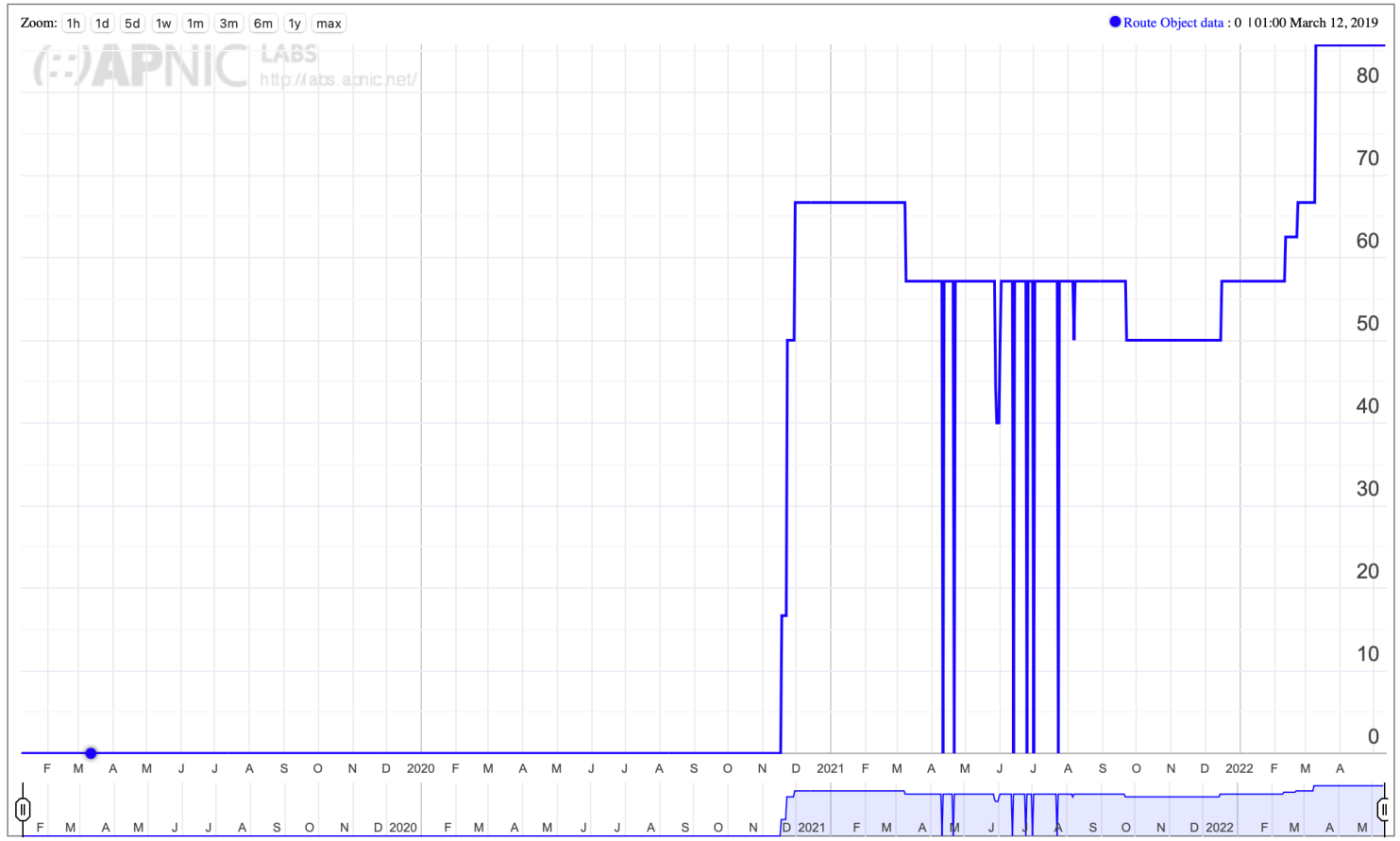
Display: **Route Objects** (Advertised ROA-Validated Route Advertisements), **IPv4**, **Percent** (of Total)



ROAs for individual networks

RPKI ROA-Validation of Advertised Routes for AS3262: SARENET, Spain (ES)

Display: **Route Objects** (Advertised ROA-Validated Route Advertisements), **IPv4**, **Percent** (of Total)



75%

Producción vs consumo

- Esto era la parte de producción: quien está generando ROAs
- La siguiente pregunta es: ¿Quién está usando esos ROAs para decidir qué aceptar y qué no?

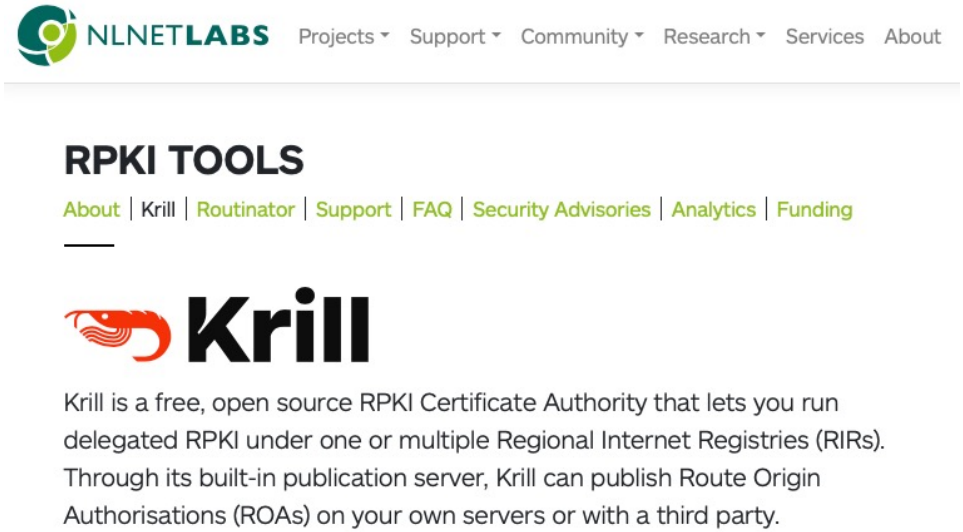
El experimento

Si queremos medir la eficacia del sistema de routing a la hora de bloquear los intentos de llevar a los usuarios por caminos incorrectos, montamos un experimento que:

- Exponga una ruta *bogus* (RPKI RoV-inválido) como única ruta hacia el prefijo
- Llevamos a un gran numero de usuarios por toda la Internet a intentar conectarse a un servidor web alojado en ese prefijo
- Usamos un ‘control’ con una ruta válida a ese mismo destino
- Medimos y comparamos

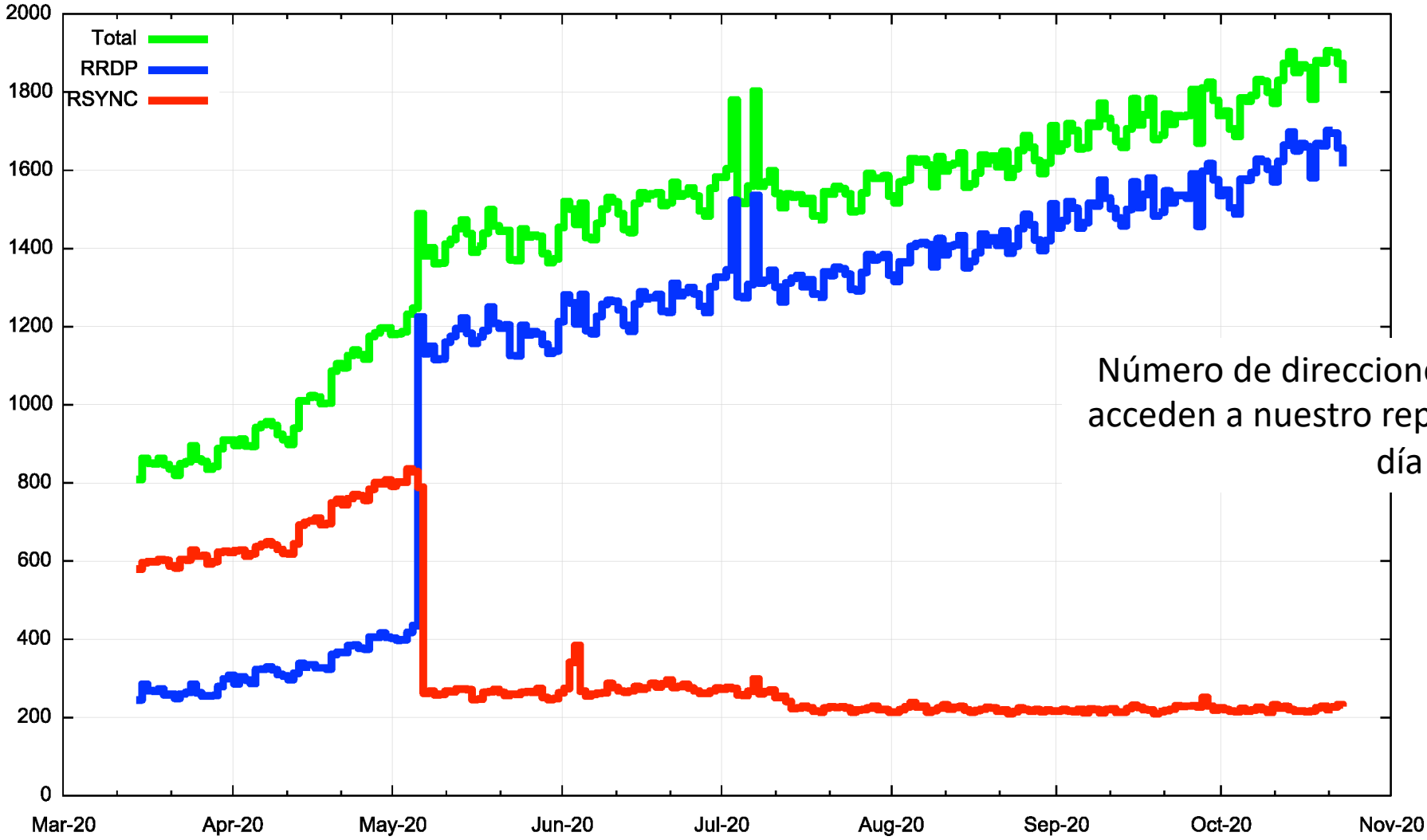
Metodología

- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Usamos Krill para esto
  - It Just Worked! tm



https://www.nlnetlabs.nl/projects/rpki/krill/

Contar los clientes de RPKI



Número de direcciones IP distintas que acceden a nuestro repositorio RPKI cada día

Metodología

- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Revocar y re-emitir ROAs a intervalos regulares para hacer oscilar el sistema entre estados válido e inválido

```
# Flip to "good" at 00:00 on Fri/Mon/Thu
0 0 * * 1,4,5 /home/krill/.cargo/bin/krillc roas update --delta ./delta-in.txt > /tmp/krillc-in.log 2>&1
# Flip to "bad" at 12:00 on sat/Tue/Thu
0 12 * * 2,4,6 /home/krill/.cargo/bin/krillc roas update --delta ./delta-out.txt > /tmp/krillc-out.log 2>&1
```

Estos dos commandos conmutan el estado del ROA entre tener un ASN válido y otro inválido como origen para un prefijo nuestro

Metodología

- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Revocar y re-emitir ROAs a intervalos regulares para hacer oscilar el sistema entre estados válido e inválido
- Publicar la pareja prefijo/AS usando Anycast desde varios puntos de la Internet
  - Usamos 3 ubicaciones: US (LA), DE (FRA), SG
  - Usamos 3 proveedores de tránsito
  - El servidor web en cada sitio sirve solo imágenes de 1x1 pixeles
  - Por ahora solo usamos IPv4

Metodología

- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Revocar y re-emitir ROAs a intervalos regulares para hacer oscilar el sistema entre estados válido e inválido
- Publicar la pareja prefijo/AS usando Anycast desde varios puntos de la Internet
  - Empezamos con 3 ubicaciones: US (LA), DE (FRA), SG
  - Después añadimos un proveedor de Cloud grande y nos expandimos a más de 200 ubicaciones

Metodología

- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Revocar y re-emitir ROAs a intervalos regulares para hacer oscilar el sistema entre estados válido e inválido
- Publicar la pareja prefijo/AS usando Anycast desde varios puntos de la Internet
- Publicar un URL que lleve al destino cubierto por el ROA
  - La componente de DNS usa un nombre de DNS único y usamos HTTPS para evitar/detectar intercepción por proxies, etc

Metodología

- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Revocar y re-emitir ROAs a intervalos regulares para hacer oscilar el sistema entre estados válido e inválido
- Publicar la pareja prefijo/AS usando Anycast desde varios puntos de la Internet
- Publicar un URL que lleve al destino cubierto por el ROA
- Meter un script en un anuncio de adwords
  - El script va a buscar el URL anterior

Metodología

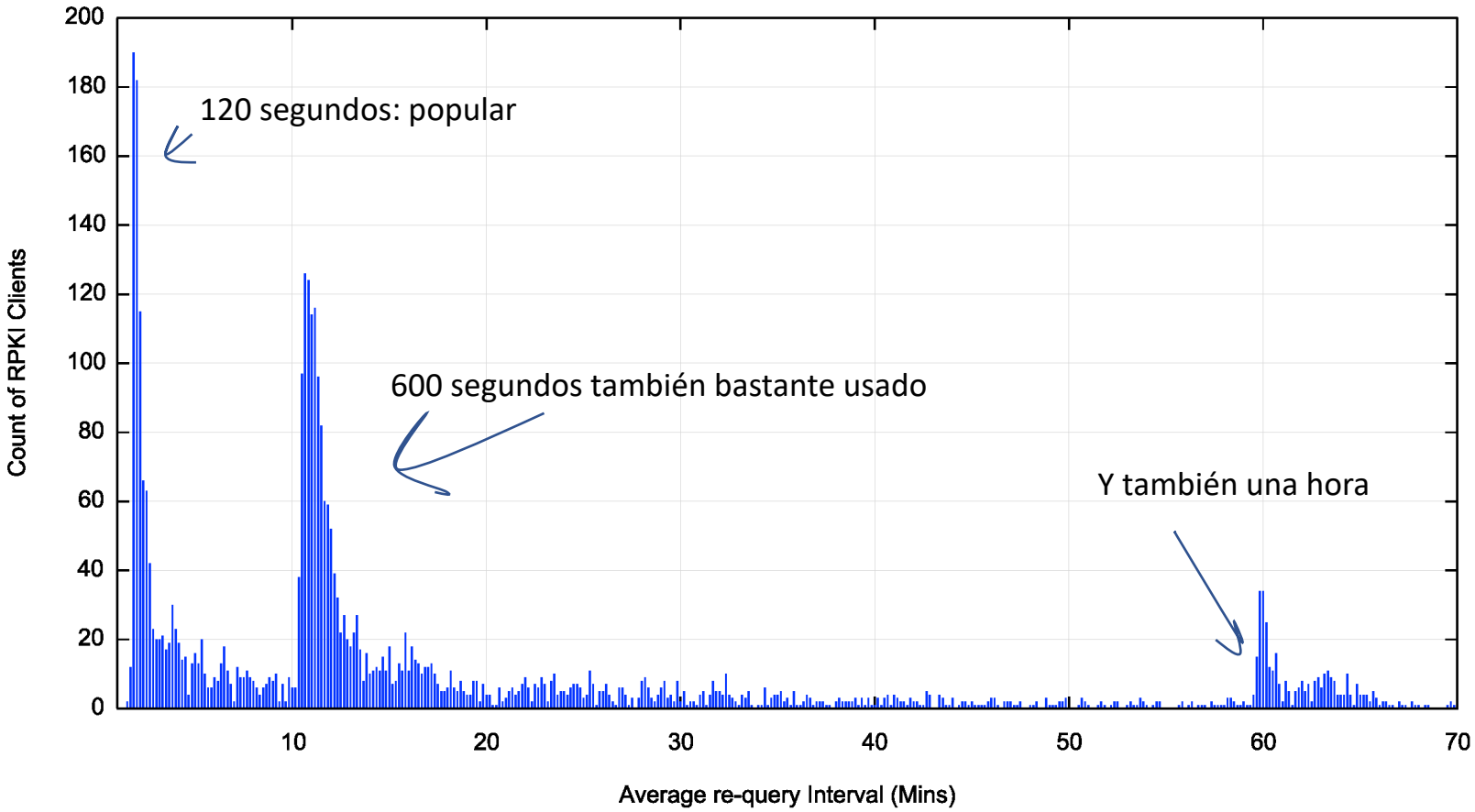
- Configurar un prefijo y un AS en un repositorio delegado de RPKI
- Revocar y re-emitir ROAs a intervalos regulares para hacer oscilar el sistema entre estados válido e inválido
- Publicar la pareja prefijo/AS usando Anycast desde varios puntos de la Internet
- Publicar un URL que lleve al destino cubierto por el ROA
- Meter un script en un anuncio de adwords
- Recopilar y analizar los datos

Alternancia de estados del ROA

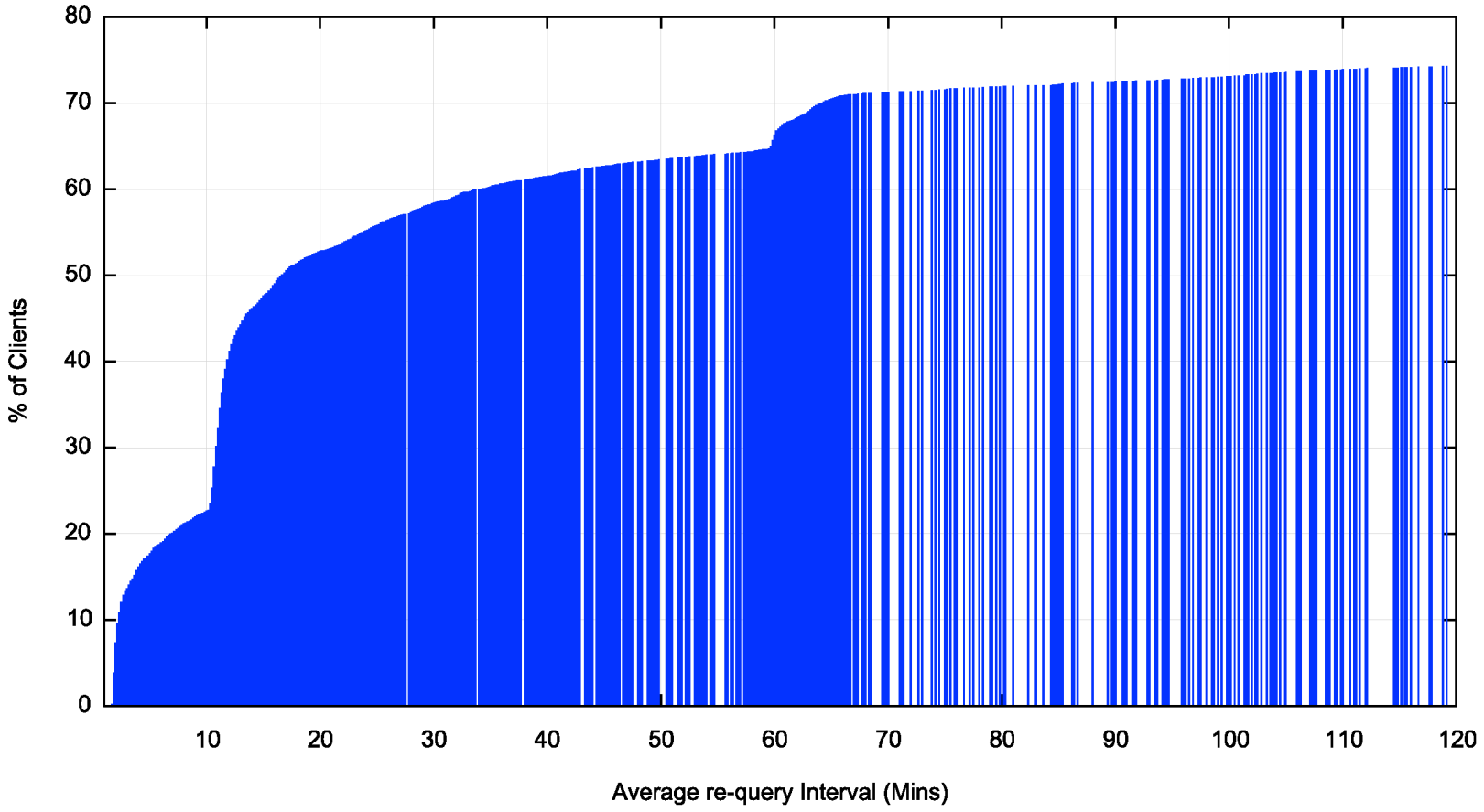
- ¿Cuál seria una buena frecuencia para alternar los estados?
  - Depende de cuanto tarda el sistema de routing en aprender que una ruta que antes era válida ahora es inválida. Lo mismo para la transición inversa.

- La validez/invalidez está dada por lo que publicamos en nuestro repositorio delegado de RPKI
  - Cada transición conlleva una revocación del certificado vigente y la emisión de un nuevo ROA y certificado
- ¿Cuál es el periodo de recarga de certificados en los clientes?
  - Pues al no haber un estándar cada uno hace lo que le parece bien

Intervalos de contacto con el punto de publicación de RPKI

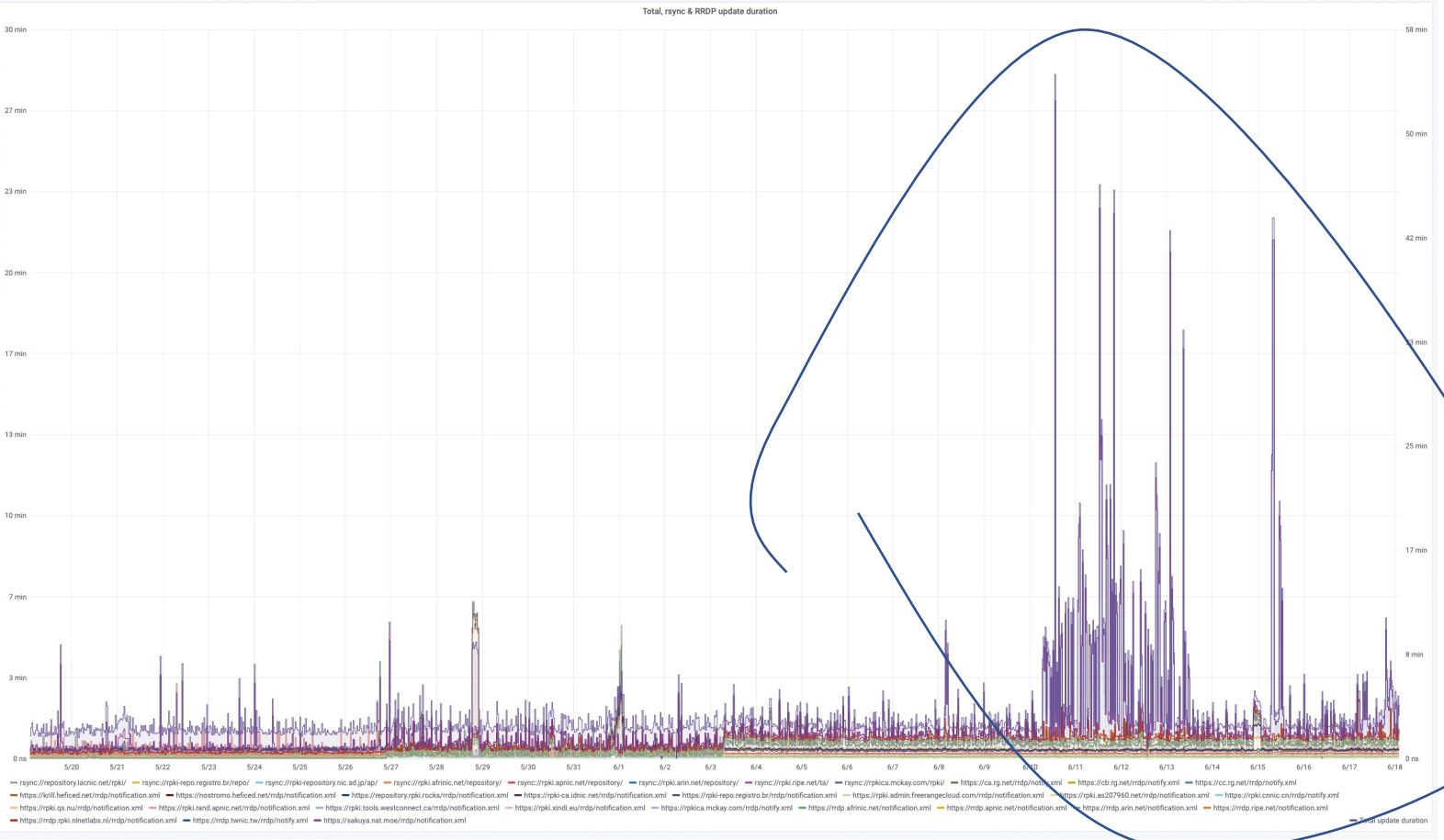


Distribución acumulativa



En las primeras 2 horas un 75% de los clientes han accedido

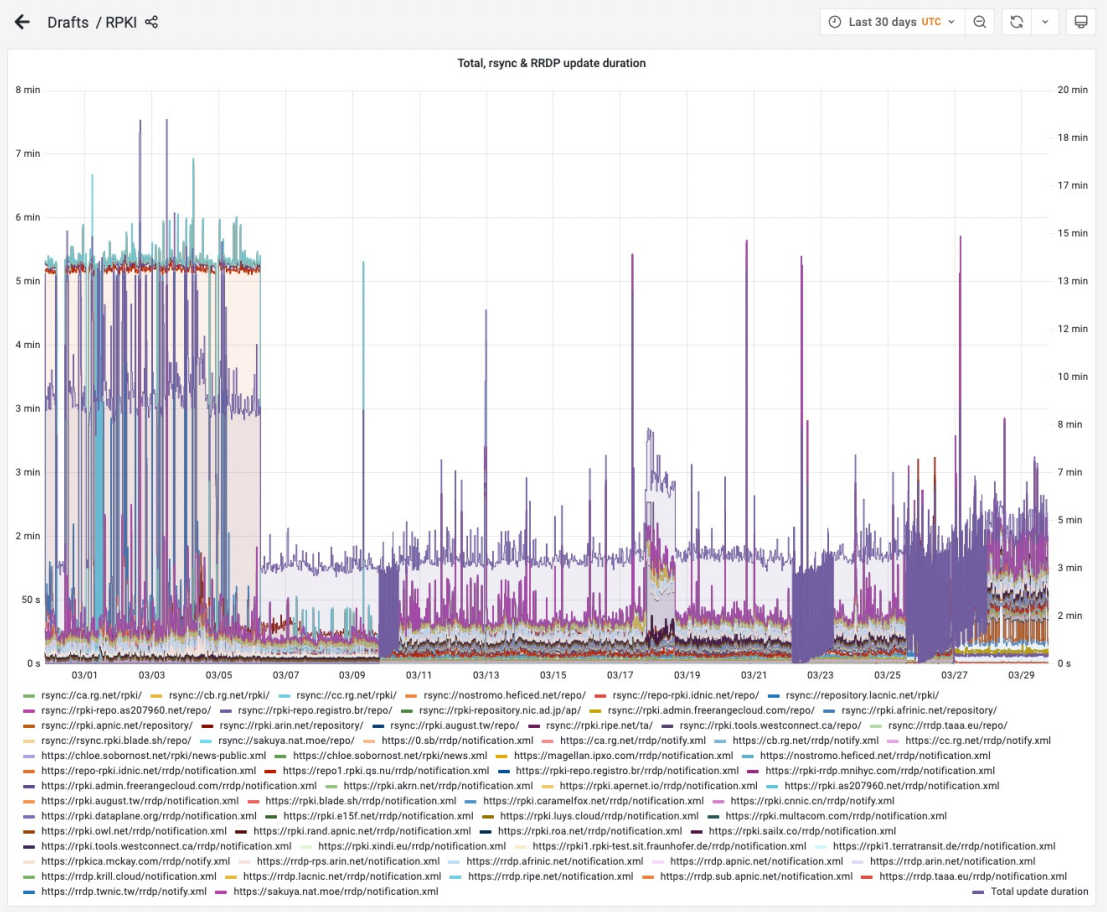
¿Y el resto?



Los clientes pueden llegar a tardar un tiempo bastante grande en contactar a todos los repositorios de todo el Sistema distribuido de RPKI lo cual hace que el sistema sea lento

https://grafana.wikimedia.org/d/UwUa77GZk/rpki?panelId=59&fullscreen&orgId=1&from=now-30d&to=now

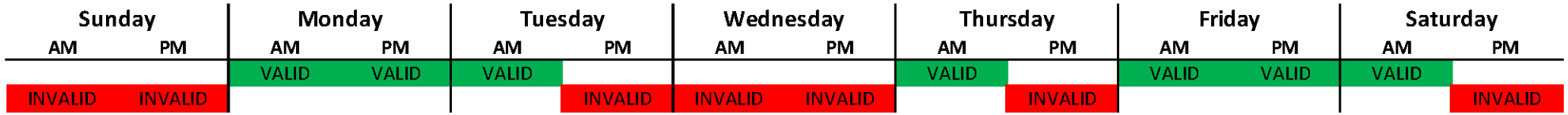
Esto no escala bien



Al ir añadiendo más puntos de publicación todo el Sistema se hace más lento y más errático

https://grafana.wikimedia.org/d/UwUa77GZk/rpki?from=now-30d&orgId=1&to=now&viewPanel=59

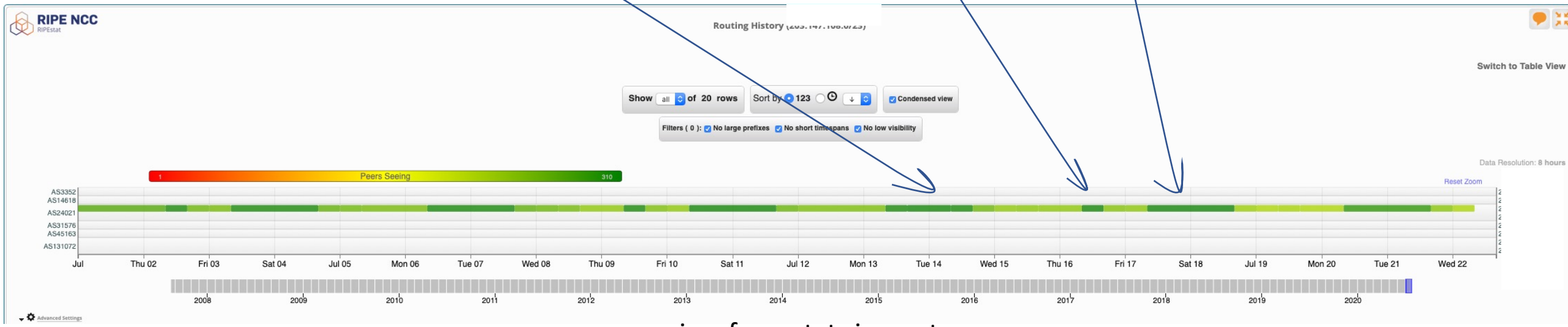
Nuestra elección: 12 y 36 horas



La validez de la ruta oscila con un periodo de 7 días usando intervalos de 12 y 36 horas

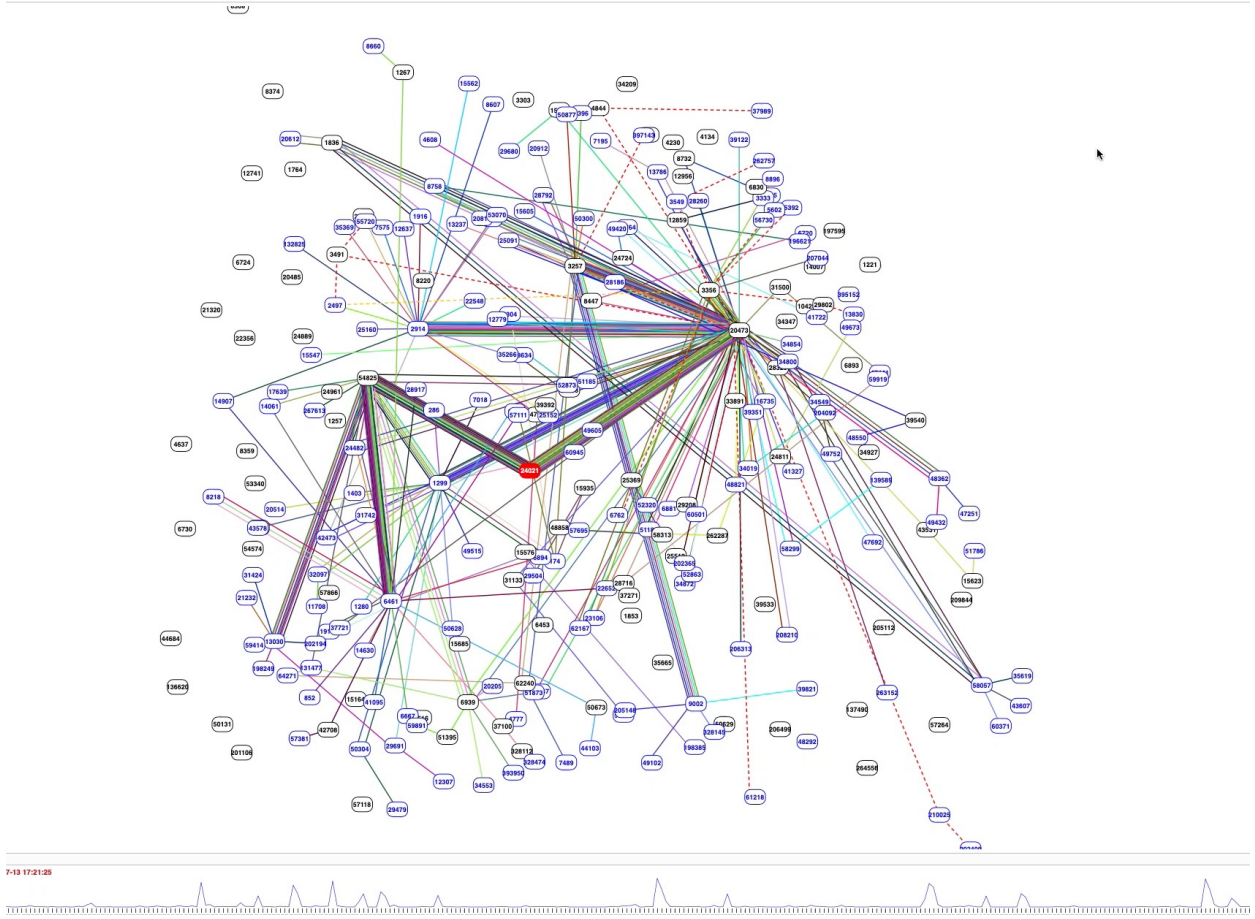
Nuestra elección: 12 y 36 horas

Sunday		Monday		Tuesday		Wednesday		Thursday		Friday		Saturday	
AM	PM	AM	PM	AM	PM	AM	PM	AM	PM	AM	PM	AM	PM
		VALID	VALID	VALID				VALID		VALID	VALID	VALID	
INVALID	INVALID				INVALID	INVALID	INVALID		INVALID				INVALID



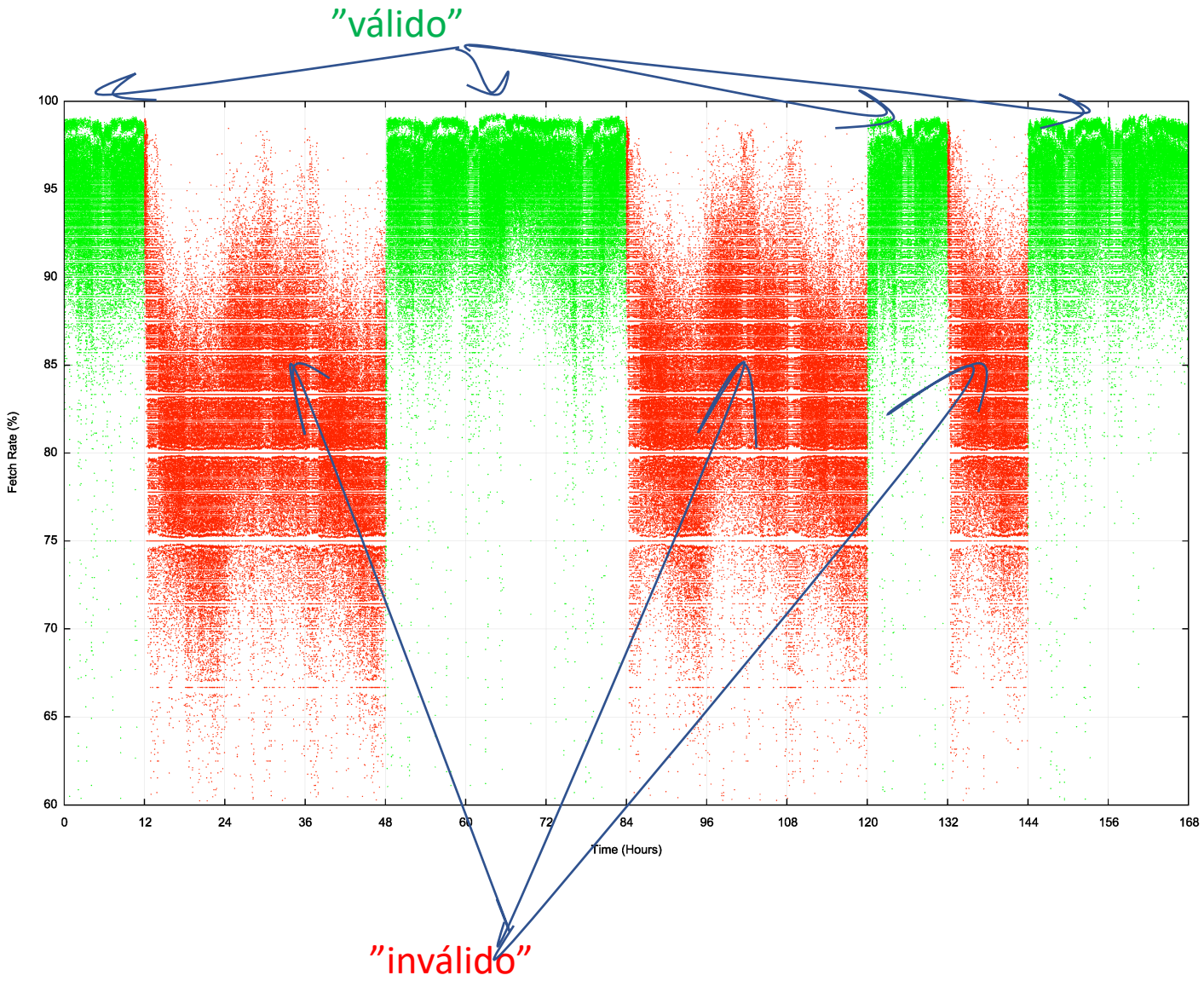
view from stat.ripe.net

Nuestra elección: 12 y 36 horas



Mirando en BGP Play

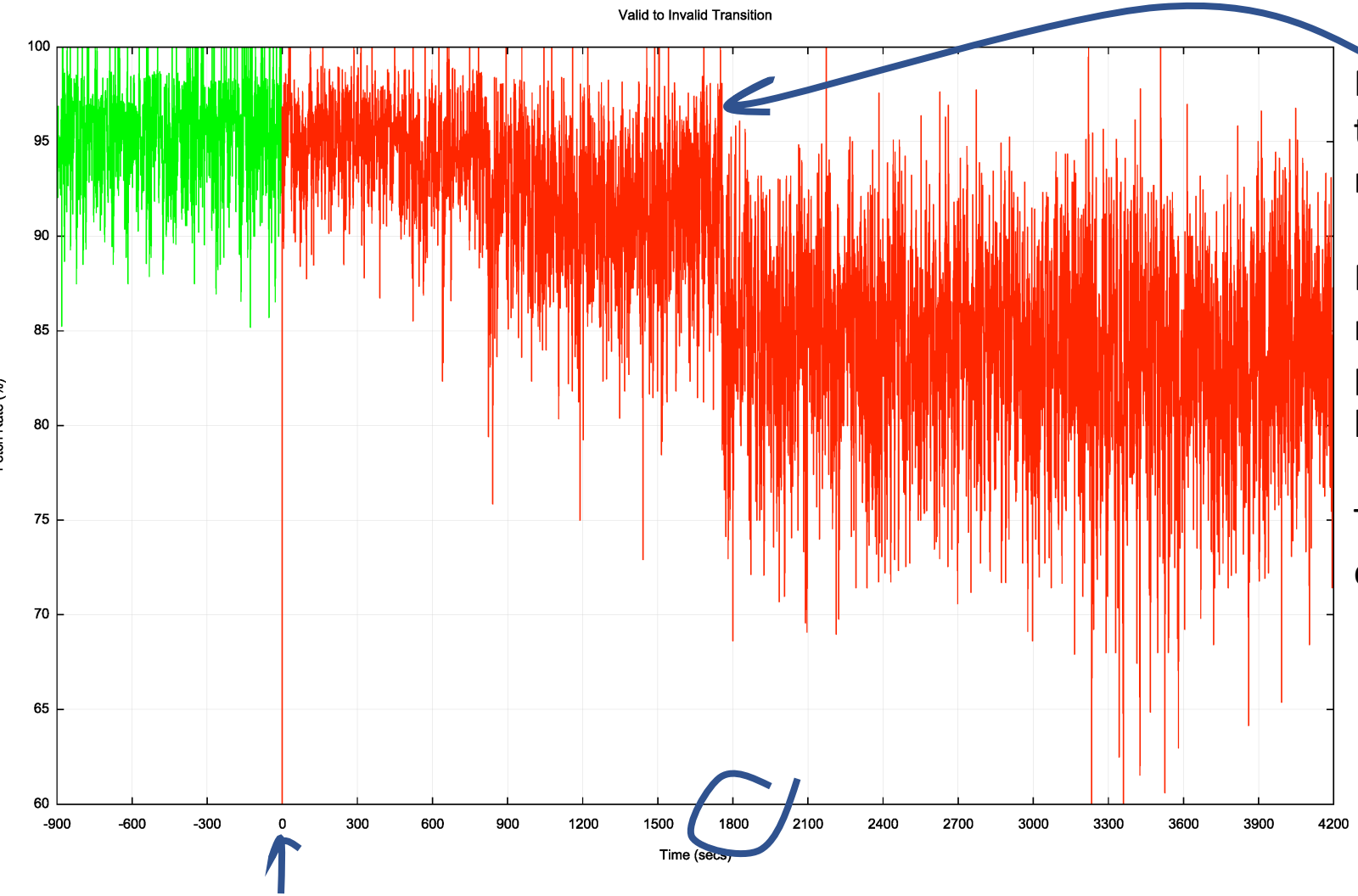
Nuestra elección: 12 y 36 horas



En la gráfica mostramos el numero de HTTP GET por segundo durante cada periodo a lo largo de una semana

Se pueden observar fácilmente los distintos estados

Transición – Válido a Inválido



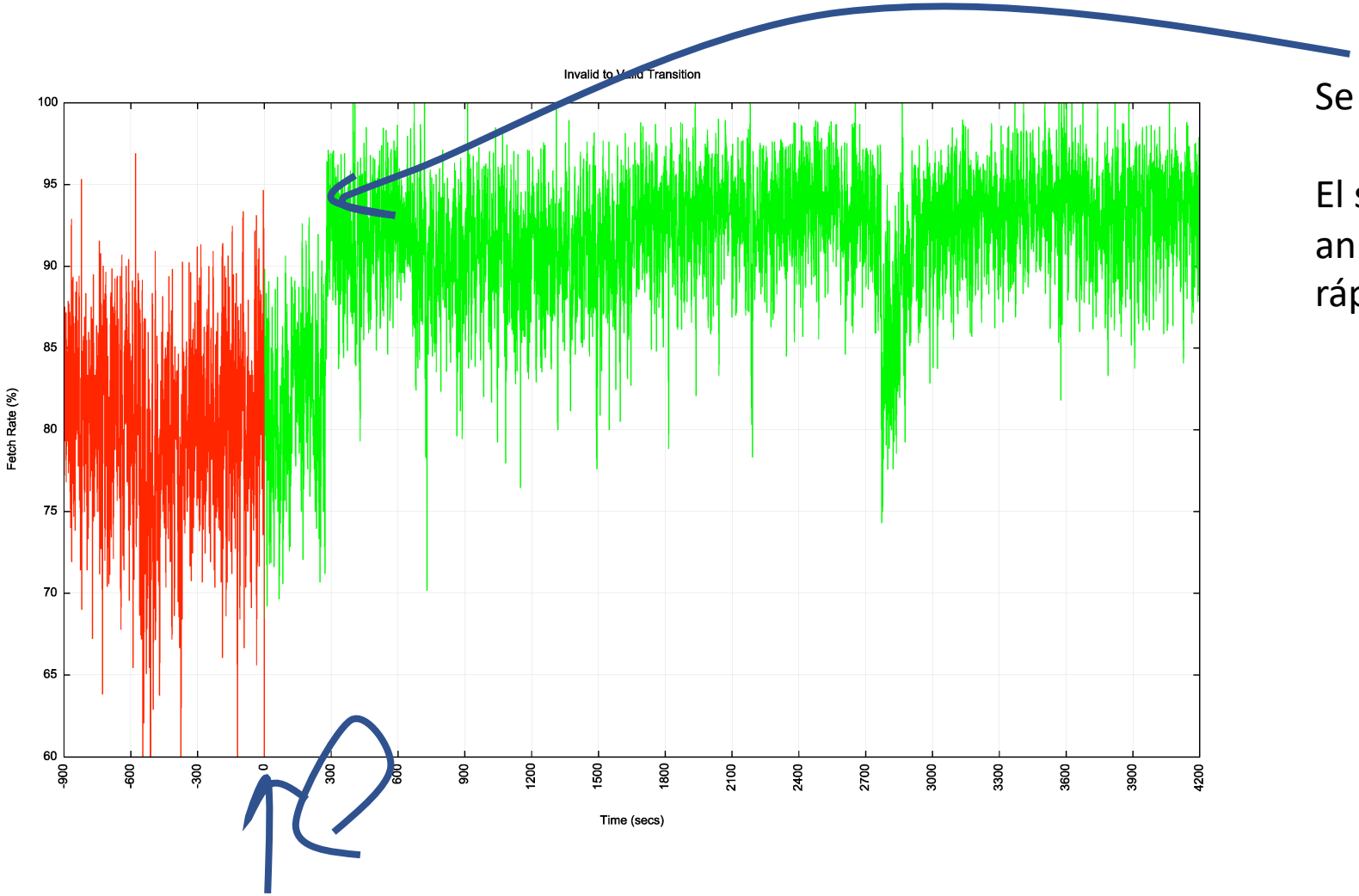
Time of ROA change at the RPKI repository

Pasan hasta 30 minutos para poder ver la transición de válido a inválido en estas medidas

Pensamos que es una combinación de retrasos en volver a preguntar al punto de publicación de RPKI y retrasos en actualizar los filtros que se pasan a los routers.

También dependemos del ultimo proveedor en retirar un filtro

Transición – Inválido a válido



Momento de transición

Se tardan unos 5 minutos en ver la transición

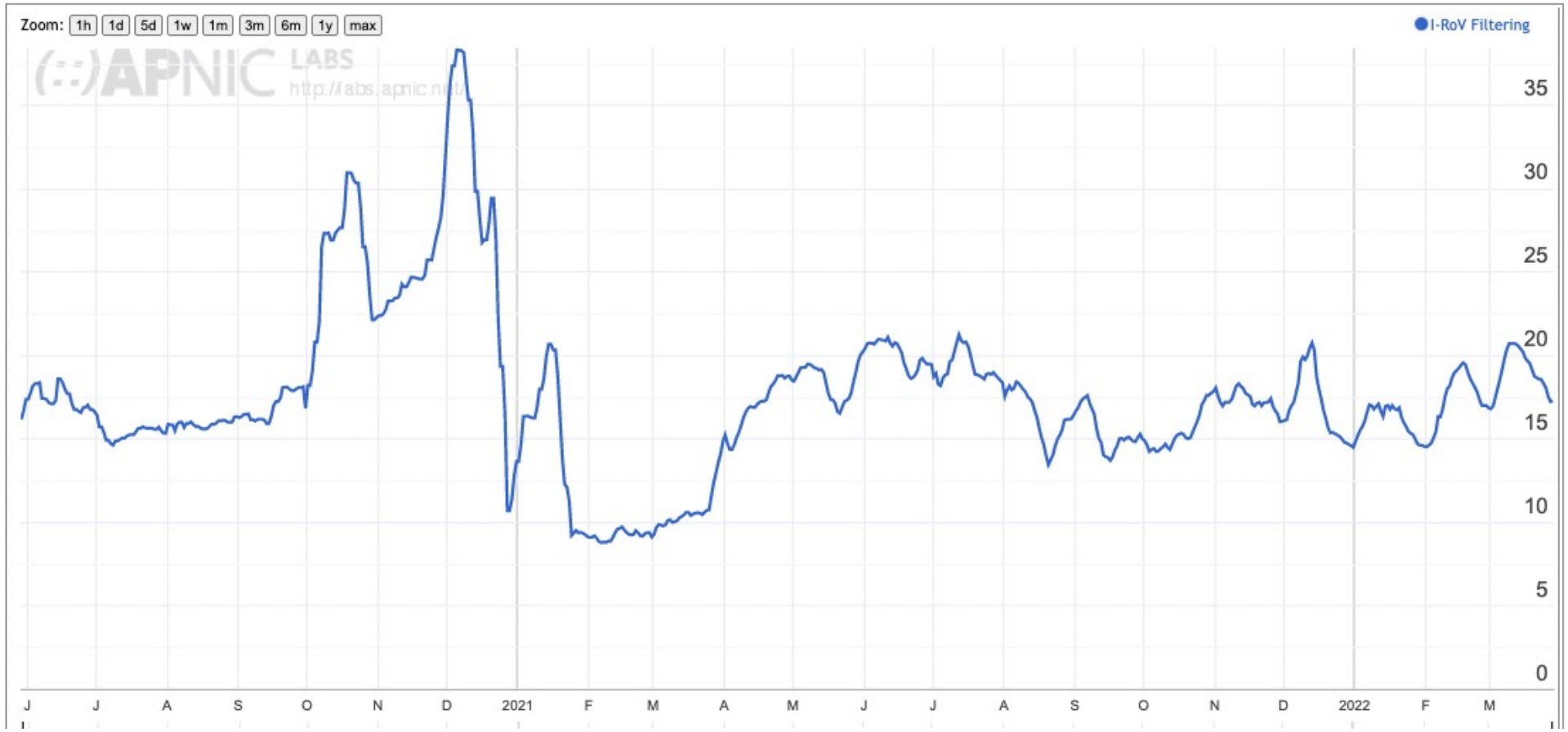
El sistema depende del primer tránsito que anuncia así que reacciona como el más rápido

Software de recolección RPKI

- Se ven relojes de 2, 10 y 60 minutos
- 2 minutos parece un poco excesivo ya que la respuesta del sistema depende en realidad de los clientes más lentos
- Por otro lado 60 minutos parece demasiado

Puede que 10 minutos sea un equilibrio razonable (?)

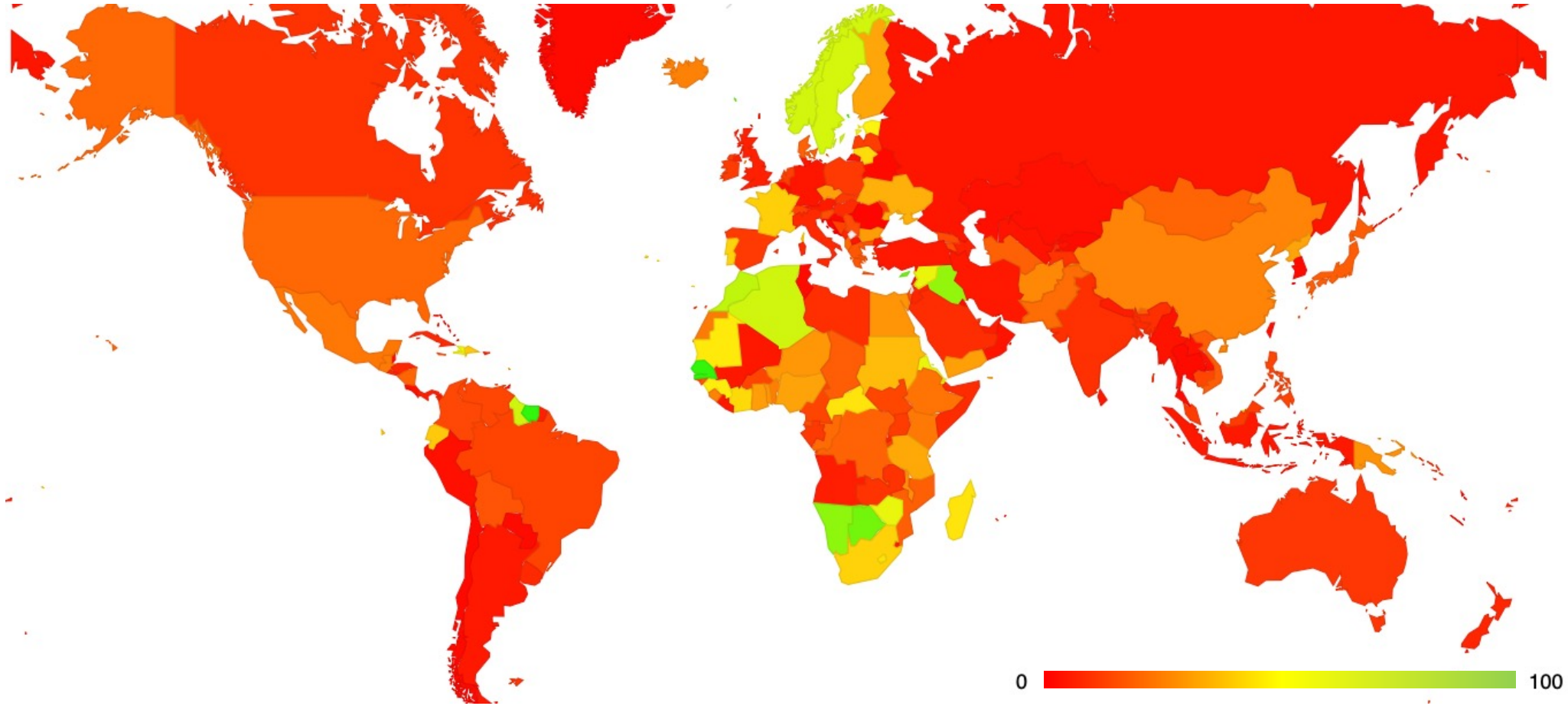
Impacto en los usuarios del filtrado RPKI



No está nada mal haber alcanzado un 20% para un sistema tan reciente

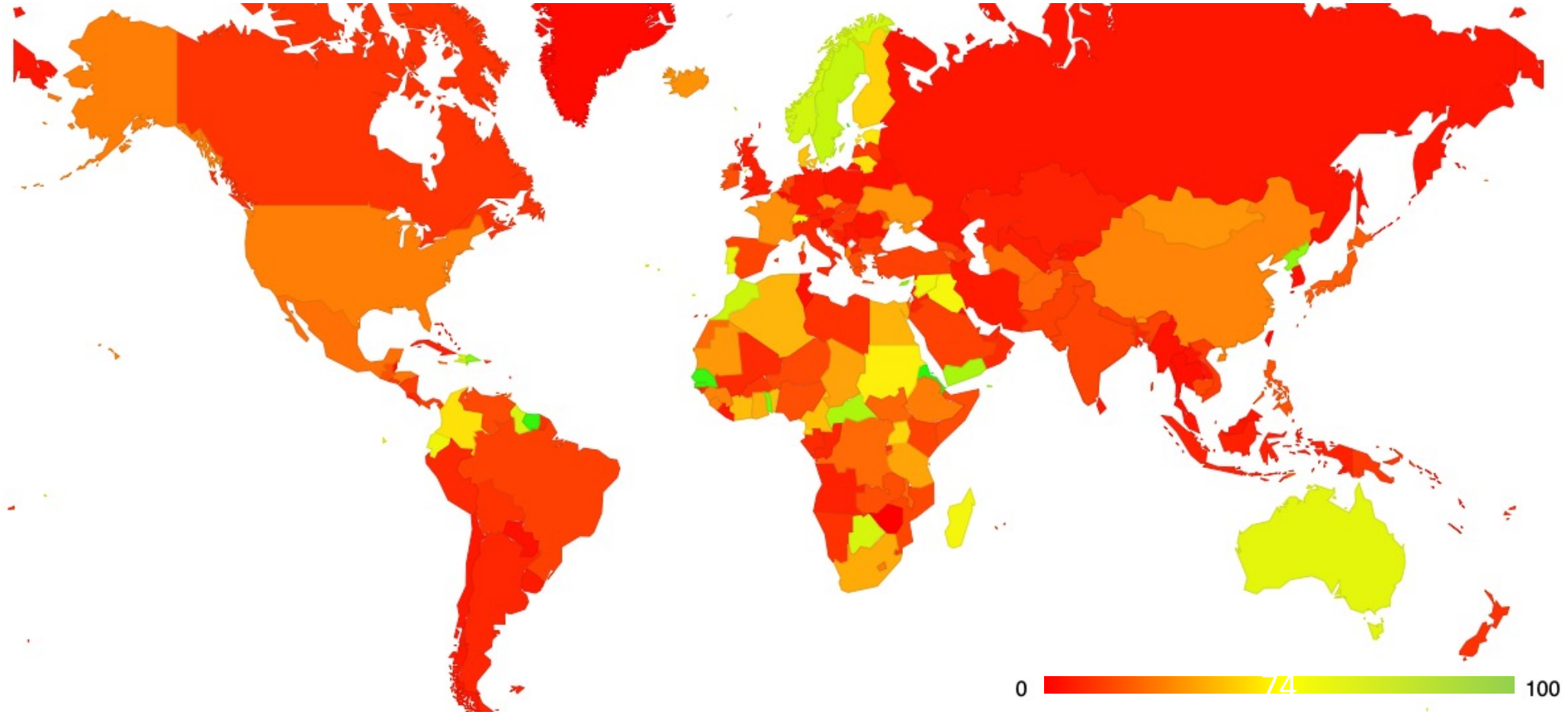
Aunque es verdad que se ven pocos cambios durante el tiempo que hemos estado midiendo

Resultados: Impacto en los usuarios del filtrado RPKI – Jul 2020



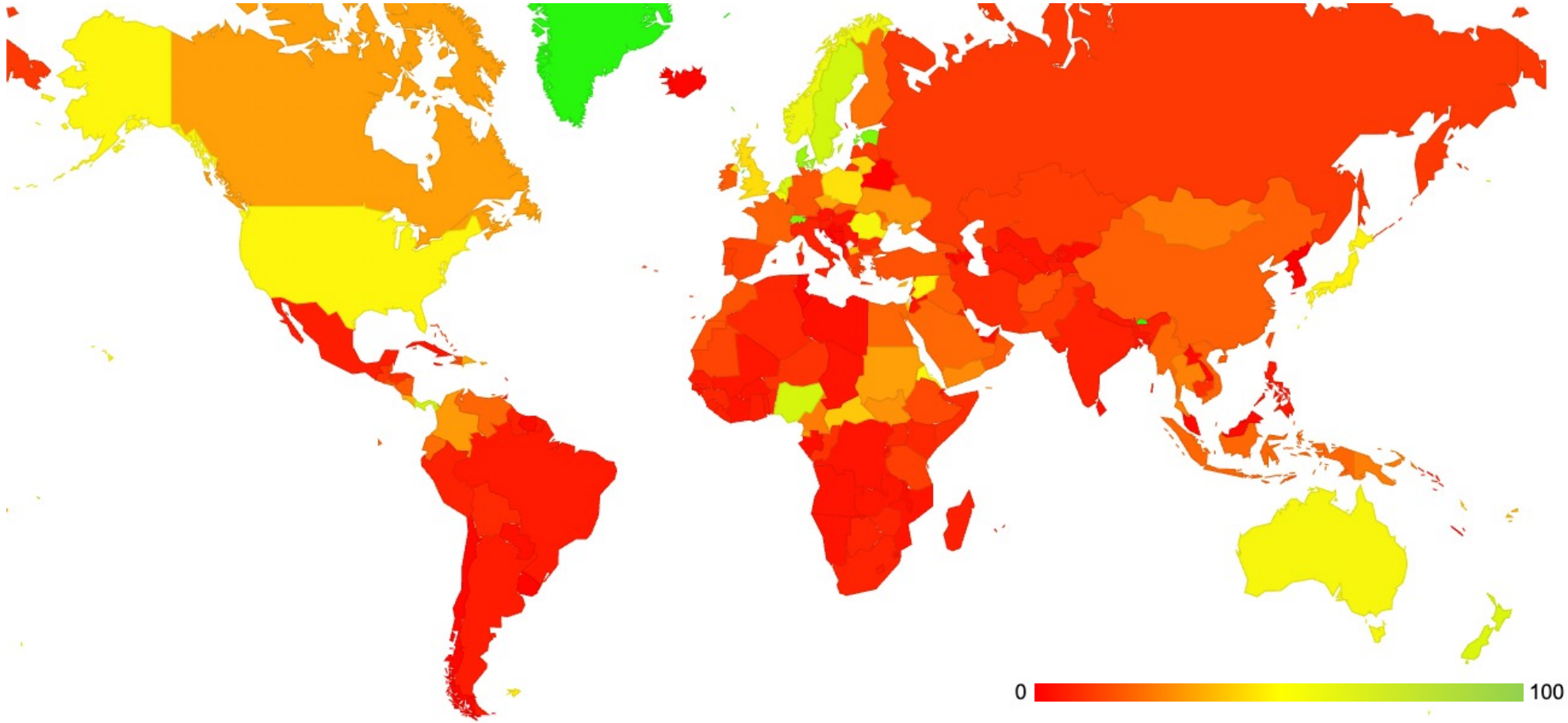
https://stats.labs.apnic.net/rpki

Resultados: Impacto en los usuarios del filtrado RPKI – Oct 2020



https://stats.labs.apnic.net/rpki

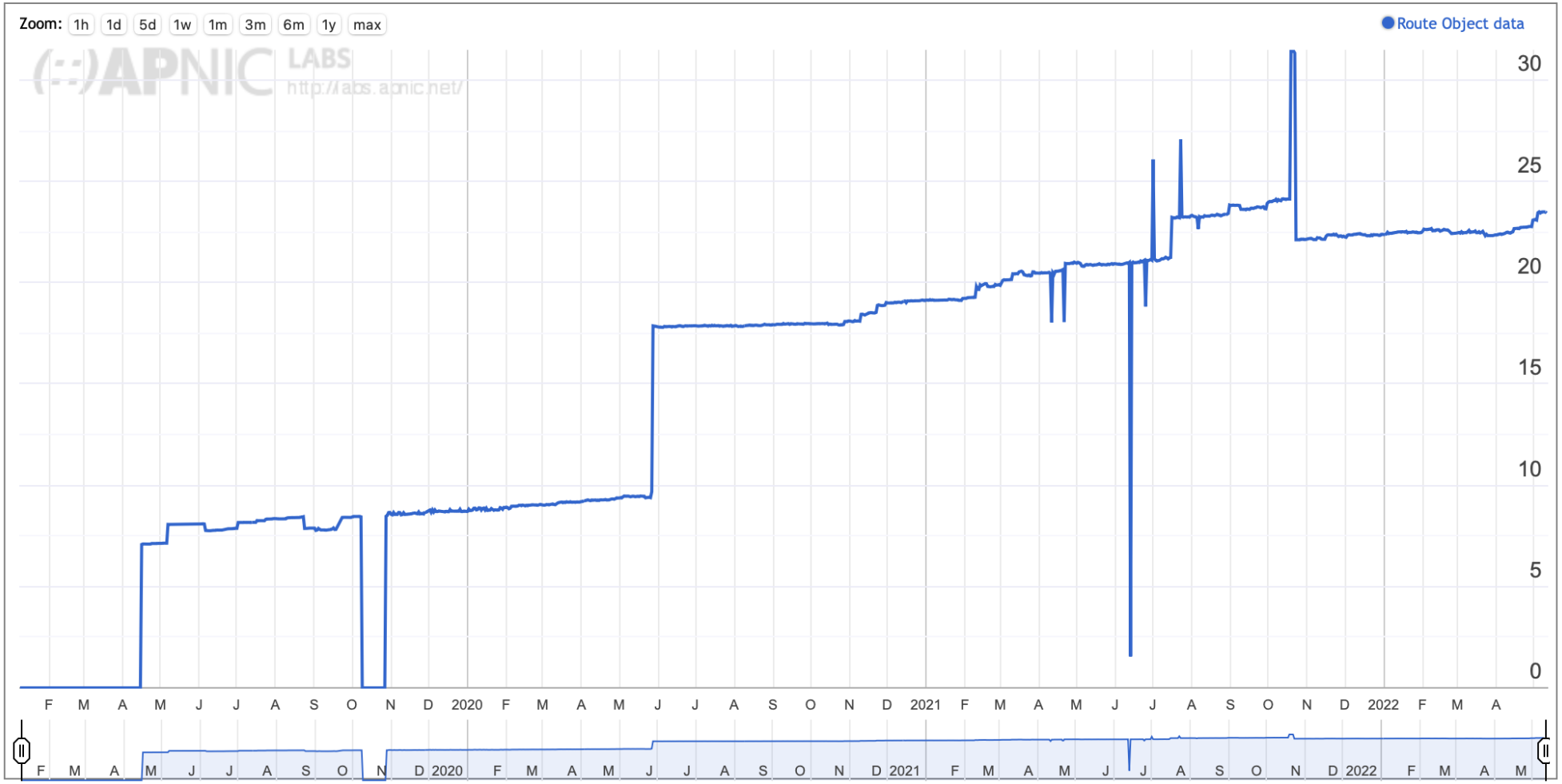
Resultados: Impacto en los usuarios del filtrado RPKI – Mar 2022



https://stats.labs.apnic.net/rpki

España

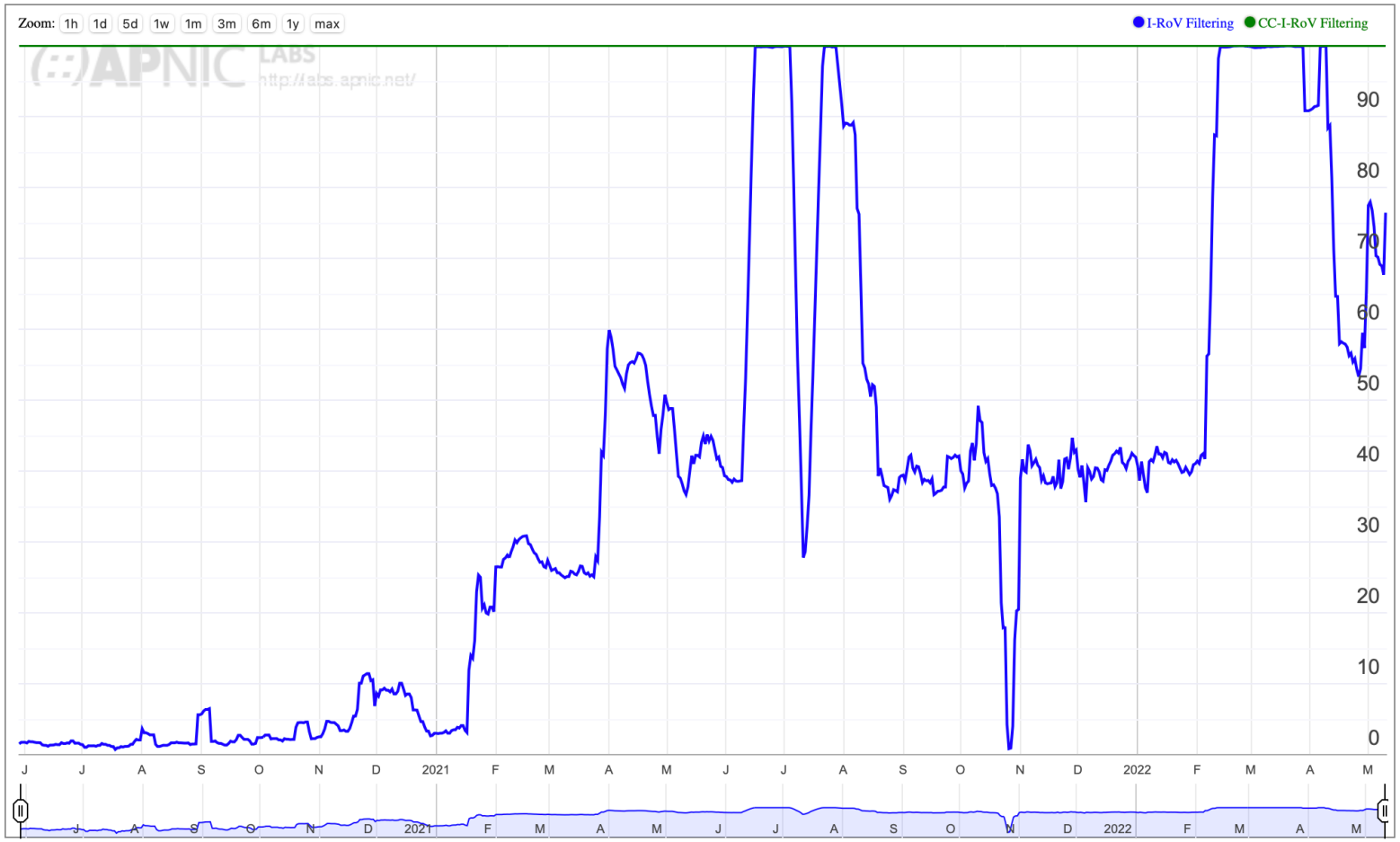
Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv4**, **Percent** (of Total)



% usuarios en ES

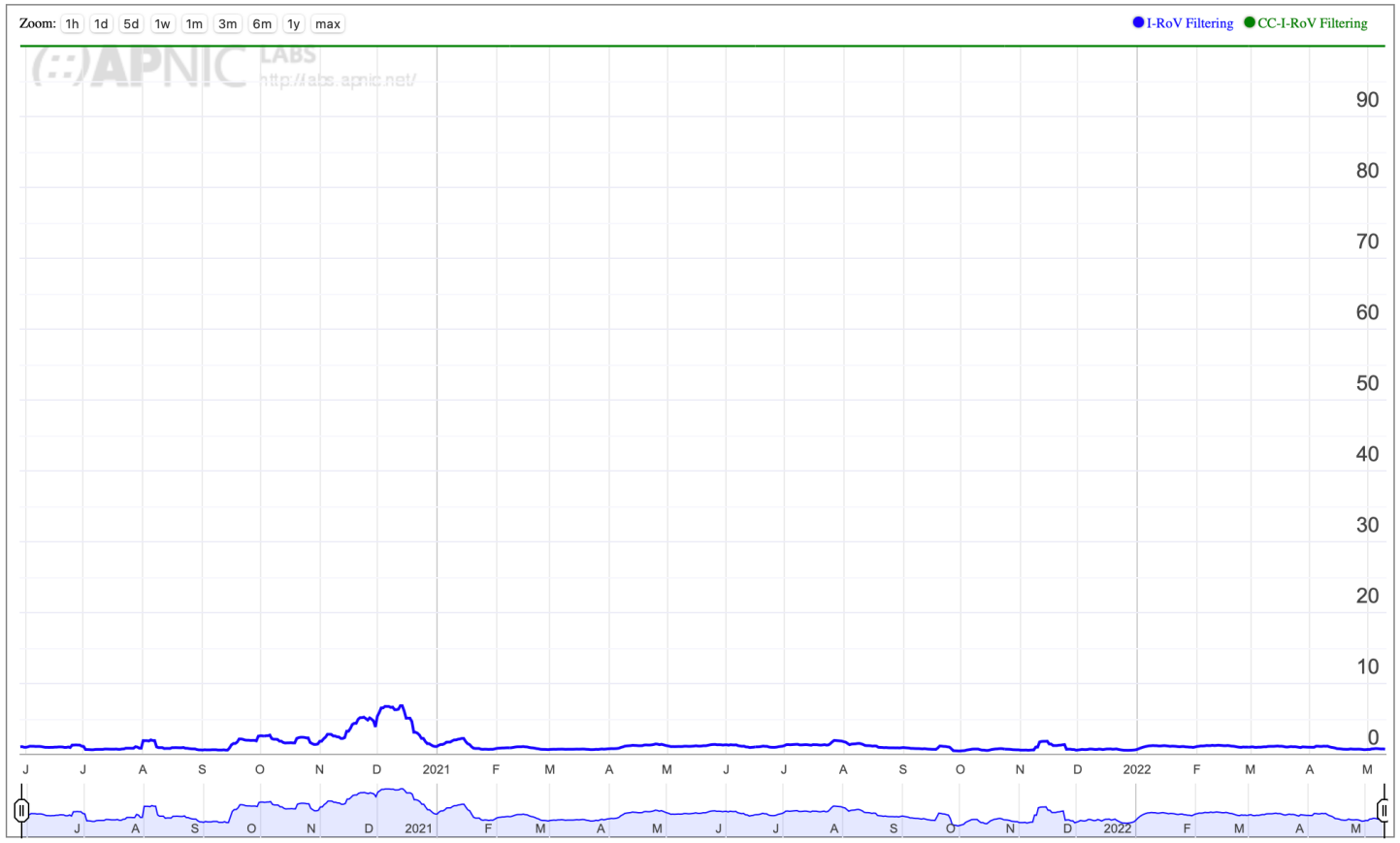
Filtrado por ROV

RPKI I-ROV Per-Country filtering for AS57269: DIGISPAINTELECOM, Spain (ES)



Filtrado por ROV

RPKI I-ROV Per-Country filtering for AS3352: TELEFONICA_DE_ESPANA, Spain (ES)



Proveedores locales

ASN	AS Name	I-RoV Filtering	Samples
AS3262	SARENET	100.00%	73
AS199652	TELITEC	99.01%	101
AS35699	ADAMOEU-AS Adamo Telecom Iberia S.A.	97.71%	741
AS50926	AXARNET-AS	87.80%	82
AS200521	SEAP-AGE	84.48%	58
AS204811	ZINNIA	83.52%	182
AS202147	VOZPLUS	82.73%	110
AS57269	DIGISPAINTELECOM	76.43%	6,127
AS50129	TVHORADADA	72.69%	260
AS197722	TELECABLEANDALUCIA-AS	68.52%	54
AS12338	EUSKALTEL	58.02%	2,792

¿Tiene que participar todo el mundo?

Aquí hay dos factores en juego:

- Hay redes que filtran

y

- Redes que no filtran pero que tienen proveedores de tránsito que filtran

En ambos casos están cubiertos los objetivos de la validación RPKI ya que los usuarios de esas redes no están expuestos a rutas inválidas

Siguientes pasos

Esto es una primera medida y creemos que se puede mejorar:

- Se puede intentar hacer traceroute selectivos desde los servidores anycast para identificar las redes que están filtrando?
  - Ahora mismo vemos lo que ve el usuario pero no podemos determinar cual de las redes individuales está haciendo el filtrado
- Podríamos hace más análisis en los route collectors para identificar los patrones de anuncios cuando cambia el estado de nuestro ROA?

Preguntas sobre las que pensar

Stub vs Tránsito

- ¿Es necesario que cada AS tenga su proprio sistema de validación de ROV RPKI y filtre las rutas inválidas?
- Si no es así, ¿cuál es el menor conjunto de redes filtradoras que podría dar un nivel equivalente de filtrado para toda la Internet?
- ¿Cuál seria el beneficio marginal de que los AS stub hicieran filtrado por ROV?

Preguntas sobre las que pensar (2)

Ingress vs Egress

- ¿Debería un AS filtrar (RoV) solo sus propios anuncios?
- ¿Deberían todos los AS filtrar sus proprios anuncios?
- ¿Qué se pretende? Proteger a otros que no filtren o protegerse a uno mismo de los errores de otros?
- ¿Qué pasa en un escenario de adopción parcial?

Preguntas sobre las que pensar (3)

¿Cuándo y cómo se protegerá el AS Path?

- ASPA drafts en el IETF?

- ¿Qué beneficios aporta la protección del origen sin protección del AS Path?

Gracias!