¿Qué estará haciendo mi validador RPKI en este momento? ©

Santiago Aggio

CONICET BB, UTN-FRBB

LACNIC 45
Ciudad de Panamá
Mayo de 2026

Resource Public Key Infrastructure (RPKI)

- Es una Infraestructura en permanente evolución
- Mayor adopción
  - Publicación de ROAs por parte de los miembros
  - Implementación de validadores en los operadores
- Actualización de los protocolos
- Consolidación en los proyectos de desarrollo de código de validadores
- Soporte en routers de fabricantes y por software
- Resulta un tema de Interés en el ámbito científico y académico

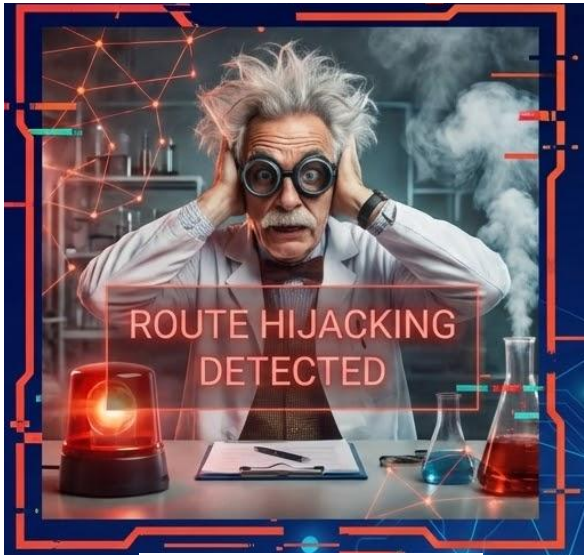
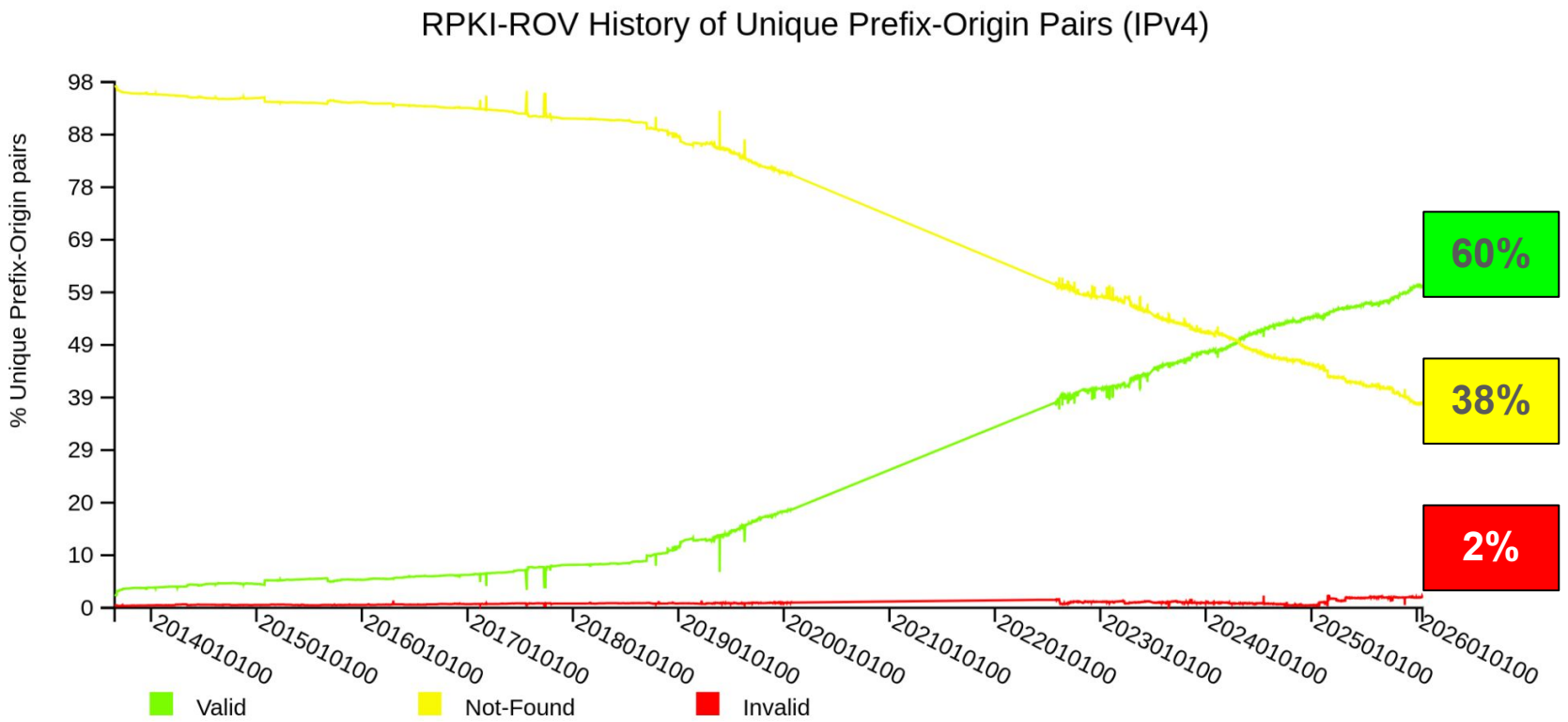
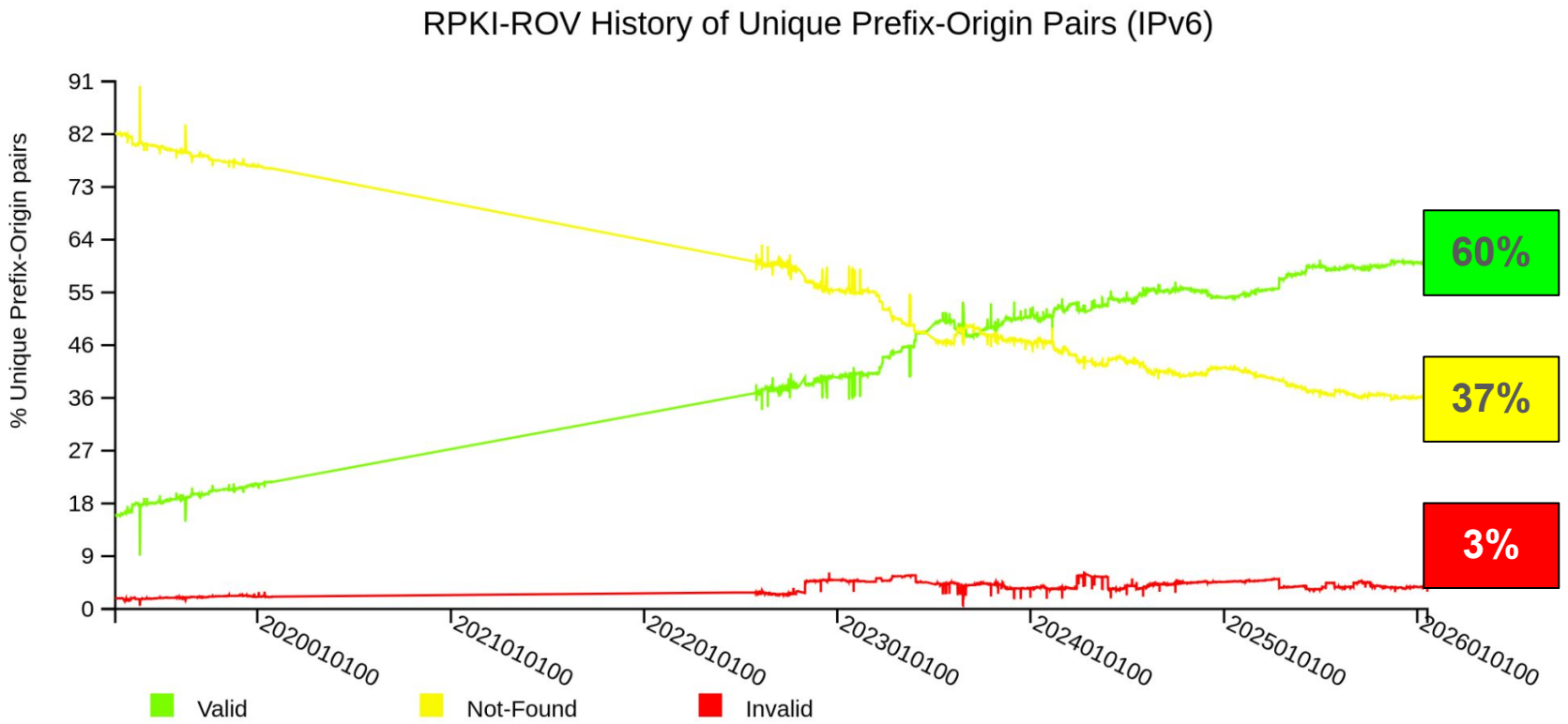


Imagen generada por Gemini

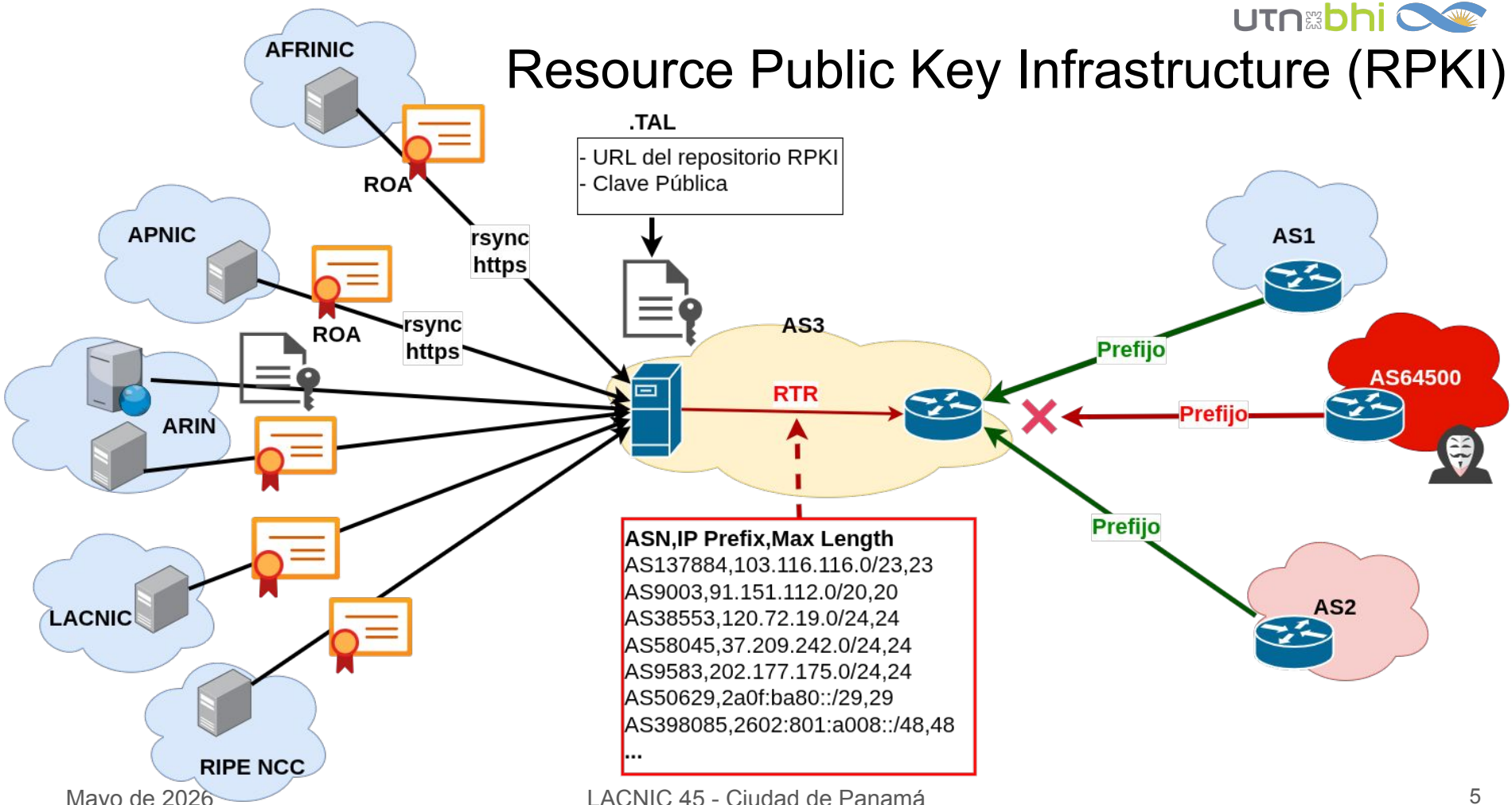


NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All **URL:** https://rpki-monitor.antd.nist.gov/ROV#div4

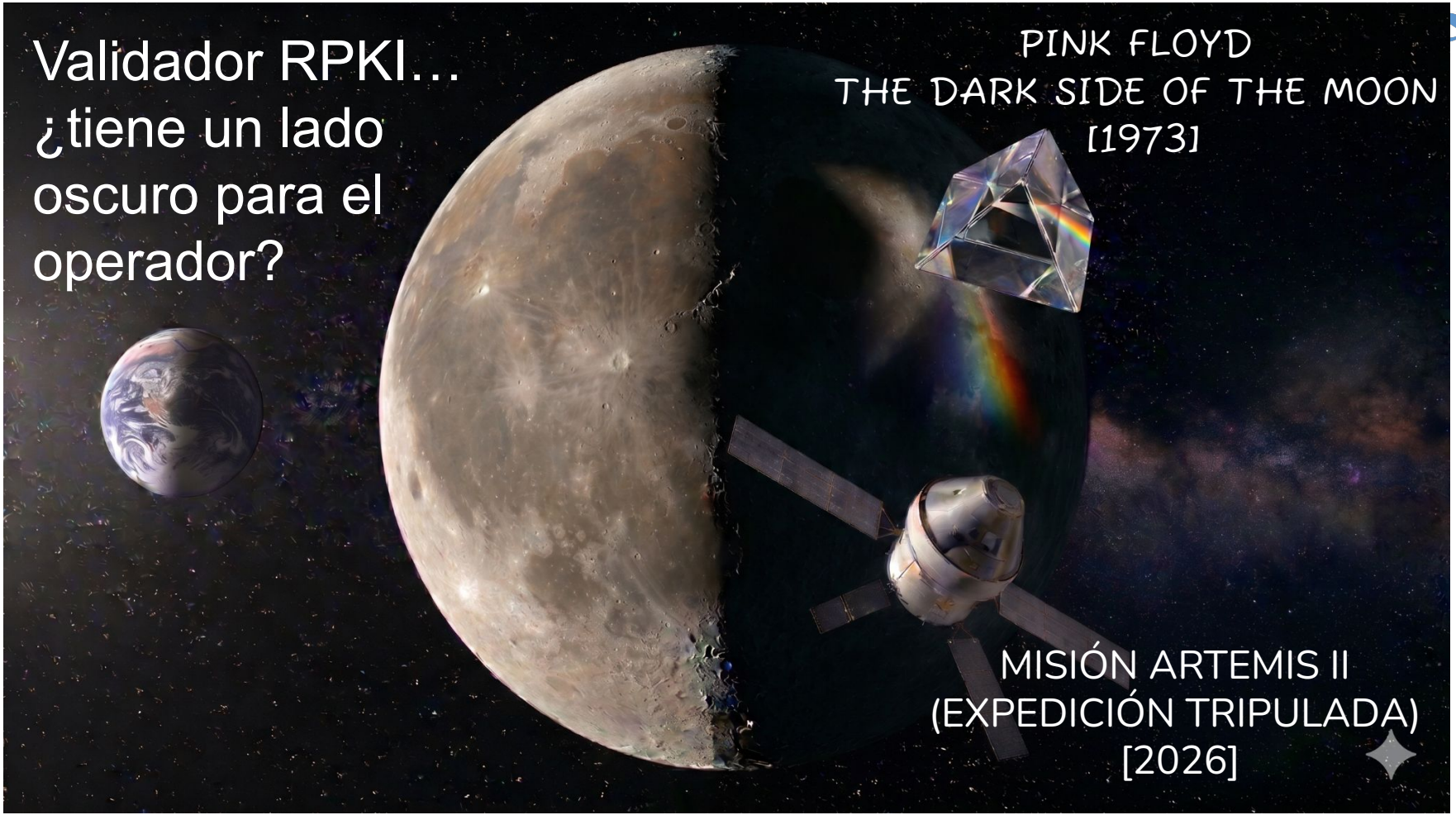


NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv6 **RIR:** All **URL:** https://rpki-monitor.antd.nist.gov/ROV#div2

Resource Public Key Infrastructure (RPKI)

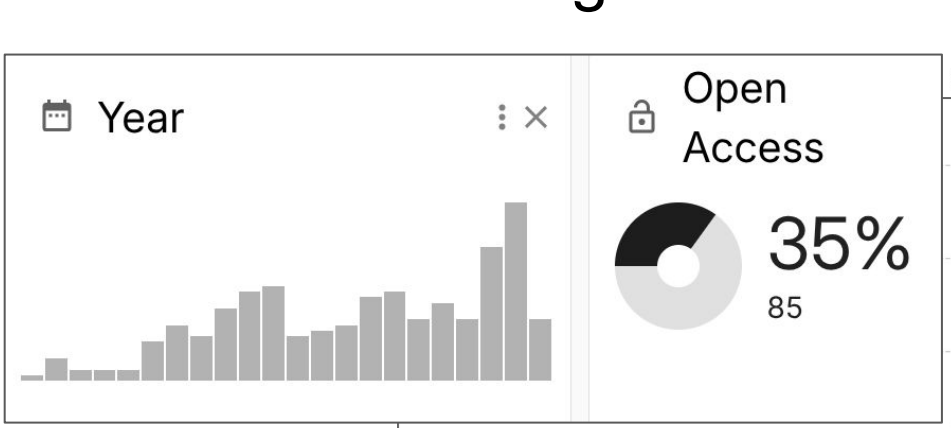


Validador RPKI… ¿tiene un lado oscuro para el operador?




Tasas de despliegue y adopción
Vulnerabilidades
Sincronización con repositorios
Resiliencia
RPKI
Desempeño
Monitoreo
Distribución geográfica
Infraestructura
Mediciones
Imagen generada por OpenAI

RPKI en la investigación

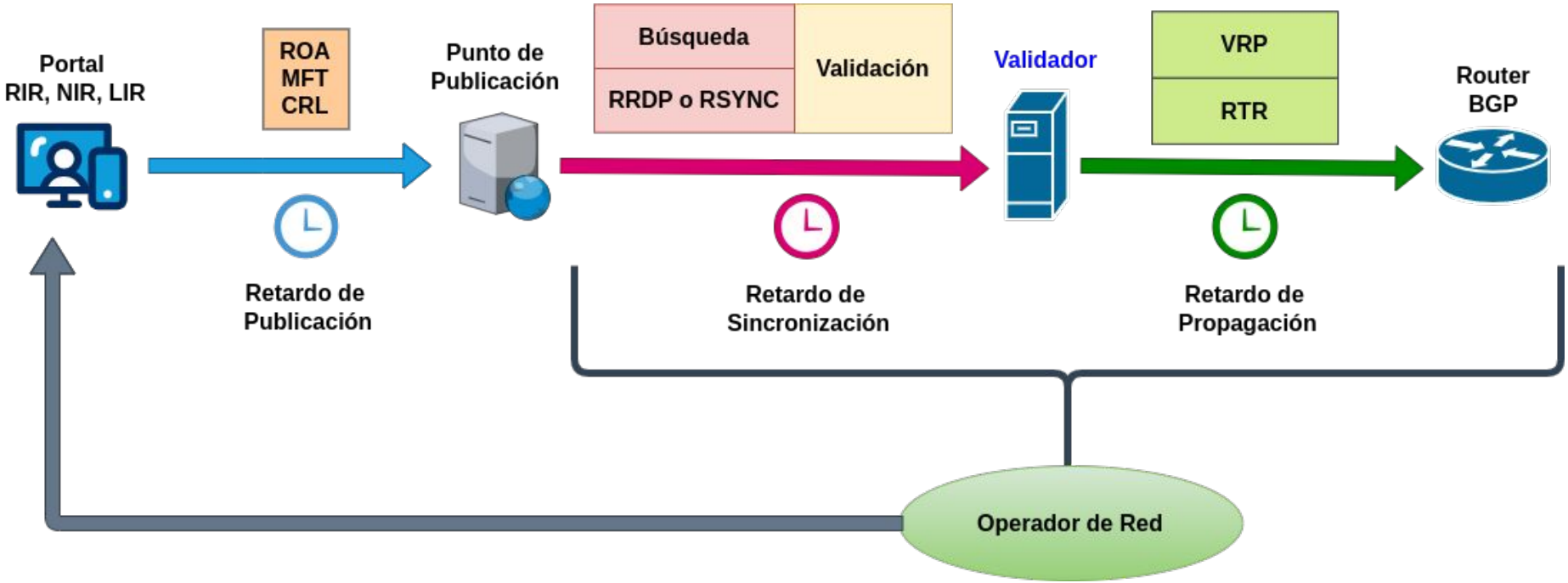


IETF

26 Drafts activos!!!

- RPKI Publication Server Best Current Practices
  - https://datatracker.ietf.org/doc/draft-ietf-sidrops-publication-server-bcp
- RPKI Repository Problem Statement and Analysis
  - https://datatracker.ietf.org/doc/draft-li-sidrops-rpki-repository-problem-statement
- Decentralized RPKI Repository Architecture
  - https://datatracker.ietf.org/doc/draft-li-sidrops-drr-architecture
- The Erik Synchronization Protocol for use with the Resource Public Key Infrastructure (RPKI)
  - https://datatracker.ietf.org/doc/draft-ietf-sidrops-rpki-erik-protocol

Retardos en la Infraestructura RPKI



Referencia: [1][2][3]

Objetivos como operadores de red

Instalar y entender cómo funcionan los Validadores

- Protocolos involucrados
- Tiempos de conexión y refresco
- ¿Qué herramientas nos ofrecen?
- ¿Qué podemos visualizar y medir?



Visualizar el estado e interpretar las métricas que nos ofrece el Validador

Medir el retardo de sincronización desde los puntos de publicación

RPKI Relaying Party Software - Validadores

FORT-Validator (lenguaje C)

https://nicmx.github.io/FORT-validator

Routinator 3000 (Rust)

https://routinator.docs.nlnetlabs.nl/en/stable

rpki-prover (Haskell)

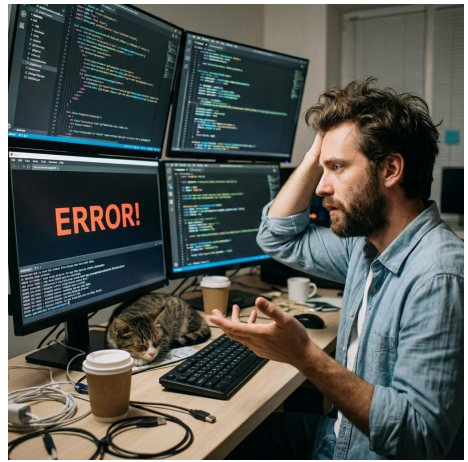
https://github.com/lolepezy/rpki-prover

rpki-client (lenguaje C)

https://rpki-client.org

StayRTR (Go)

https://github.com/bgp/stayrtr



Protocolo de sincronización: RRDP (RFC8182)

Usa HTTPS:

- Permite usar CDNs. y distribuir la carga ante peticiones simultáneas de los operadores

Atomicidad:

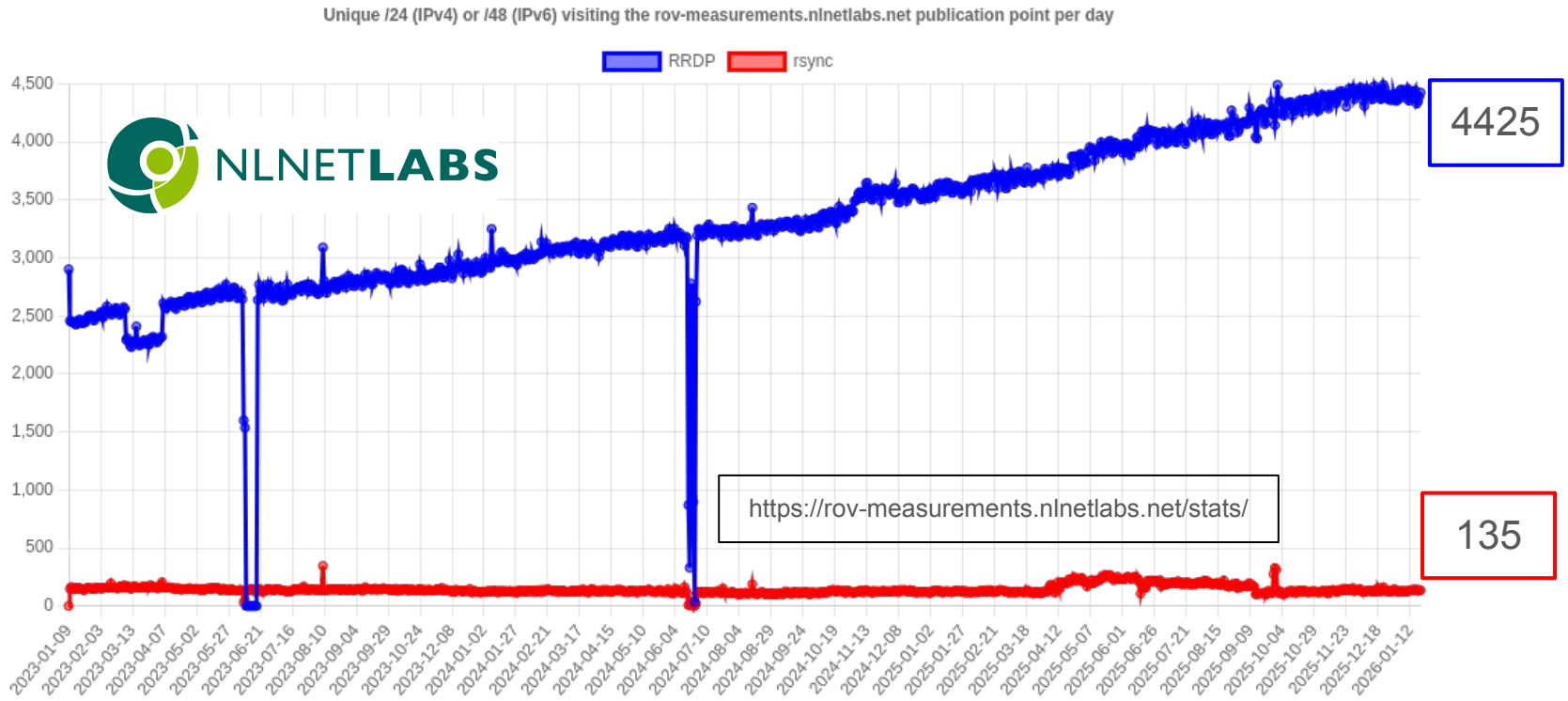
- RRDP trata el repositorio RPKI como un sistema de versiones y se evita bases de datos corruptas o con estados inconsistentes de ROAs
- El servidor le responde con una lista de cambios (Deltas) o, si es necesario, con una copia nueva de todo (Snapshot)

Menor carga en el servidor:

- El servidor solo sirve archivos estáticos (XML sobre HTTPS), no tiene que ejecutar procesos de sincronización por cada cliente

Se prioriza RRDP por defecto, dejando rsync solo como mecanismo de respaldo (fallback)

RRDP vs RSYNC en un Punto de Publicación



¿Qué usamos en la obtención de las métricas?



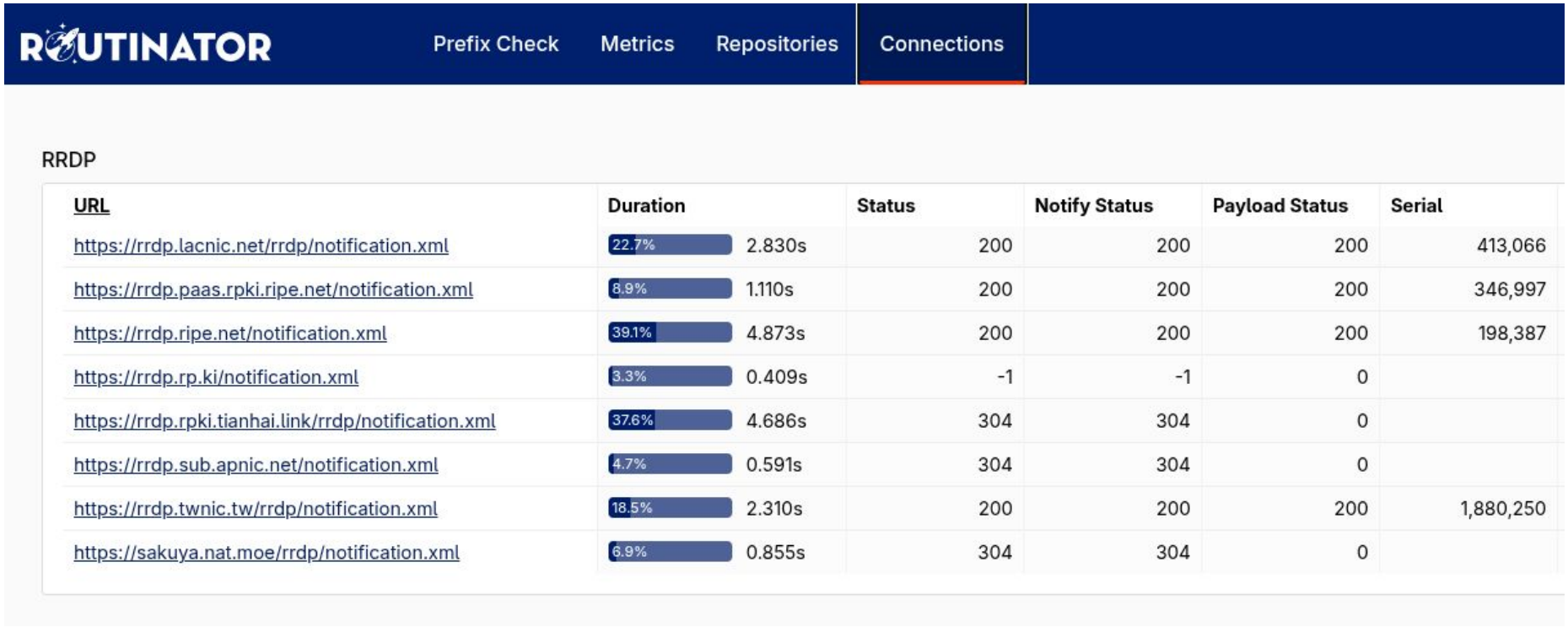
Información disponibles en los validadores

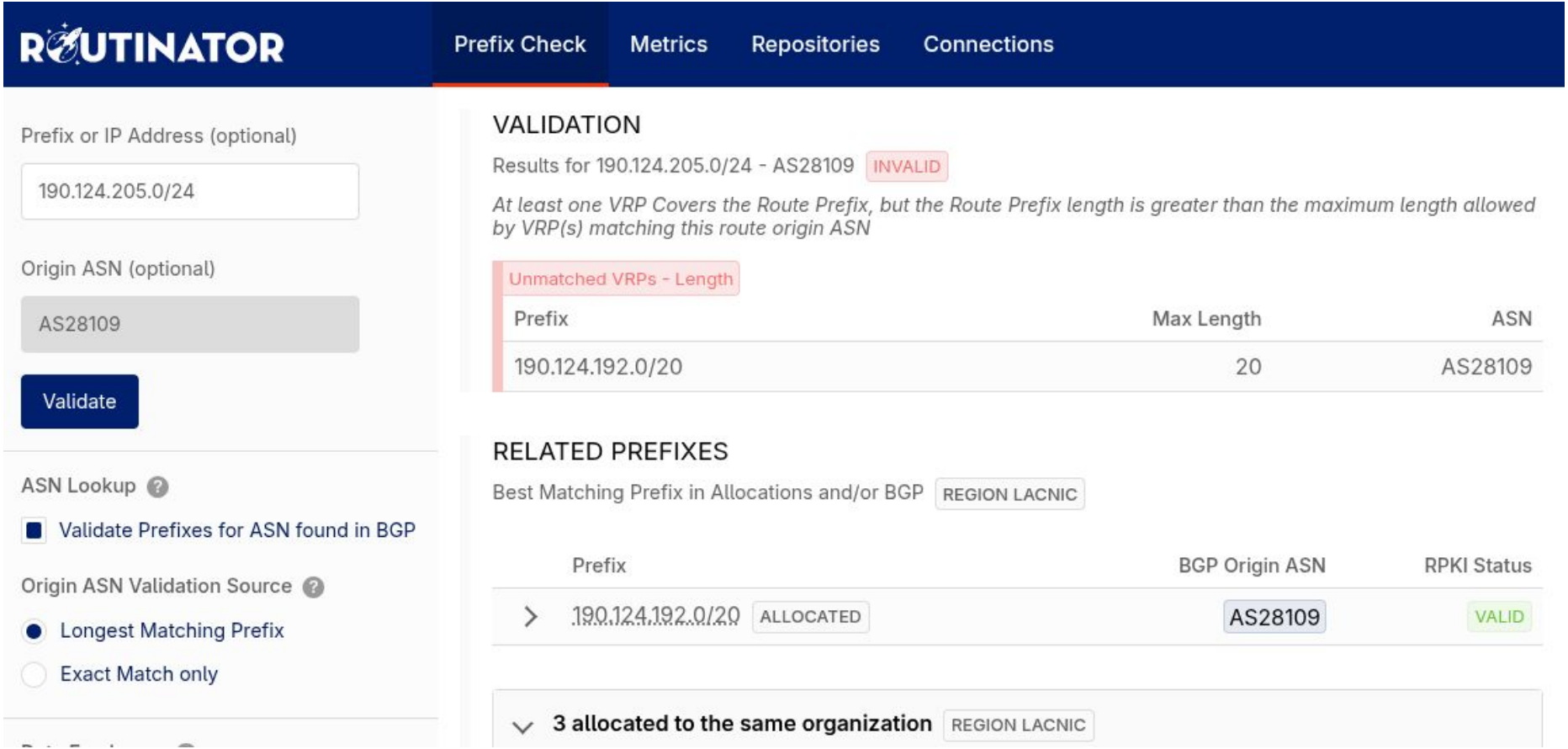
- Exporter Prometheus de Routinator 3000 + Grafana
- Página web con métricas y estadísticas que nos provee rpki-prover y Routinator
- Archivos de notificaciones de Fort

Mediciones de ping y traceroute mediante sondas RIPE Atlas de Argentina

Routinator - VRPs en RIRs




ROUTINATOR
Prefix Check
Metrics
Repositories
Connections
RRDP
URL
Duration
Status
Notify Status
Payload Status
Serial
https://rrdp.lacnic.net/rrdp/notification.xml 22.7% 2.830s 200 200 200 413,066
https://rrdp.paas.rpki.ripe.net/notification.xml 8.9% 1.110s 200 200 200 346,997
https://rrdp.ripe.net/notification.xml 39.1% 4.873s 200 200 200 198,387
https://rrdp.rp.ki/notification.xml 3.3% 0.409s -1 -1 0
https://rrdp.rpki.tianhai.link/rrdp/notification.xml 37.6% 4.686s 304 304 0
https://rrdp.sub.apnic.net/notification.xml 4.7% 0.591s 304 304 0
https://rrdp.twnic.tw/rrdp/notification.xml 18.5% 2.310s 200 200 200 1,880,250
https://sakuya.nat.moe/rrdp/notification.xml 6.9% 0.855s 304 304 0


ROUTINATOR
Prefix Check
Metrics
Repositories
Connections
Prefix or IP Address (optional)
190.124.205.0/24
Origin ASN (optional)
AS28109
Validate
ASN Lookup
Validate Prefixes for ASN found in BGP
Origin ASN Validation Source
Longest Matching Prefix
Exact Match only
VALIDATION
Results for 190.124.205.0/24 - AS28109 INVALID
At least one VRP Covers the Route Prefix, but the Route Prefix length is greater than the maximum length allowed by VRP(s) matching this route origin ASN
Unmatched VRPs - Length
Prefix
Max Length
ASN
190.124.192.0/20
20
AS28109
RELATED PREFIXES
Best Matching Prefix in Allocations and/or BGP REGION LACNIC
Prefix
BGP Origin ASN
RPKI Status
190.124.192.0/20 ALLOCATED
AS28109
VALID
3 allocated to the same organization REGION LACNIC

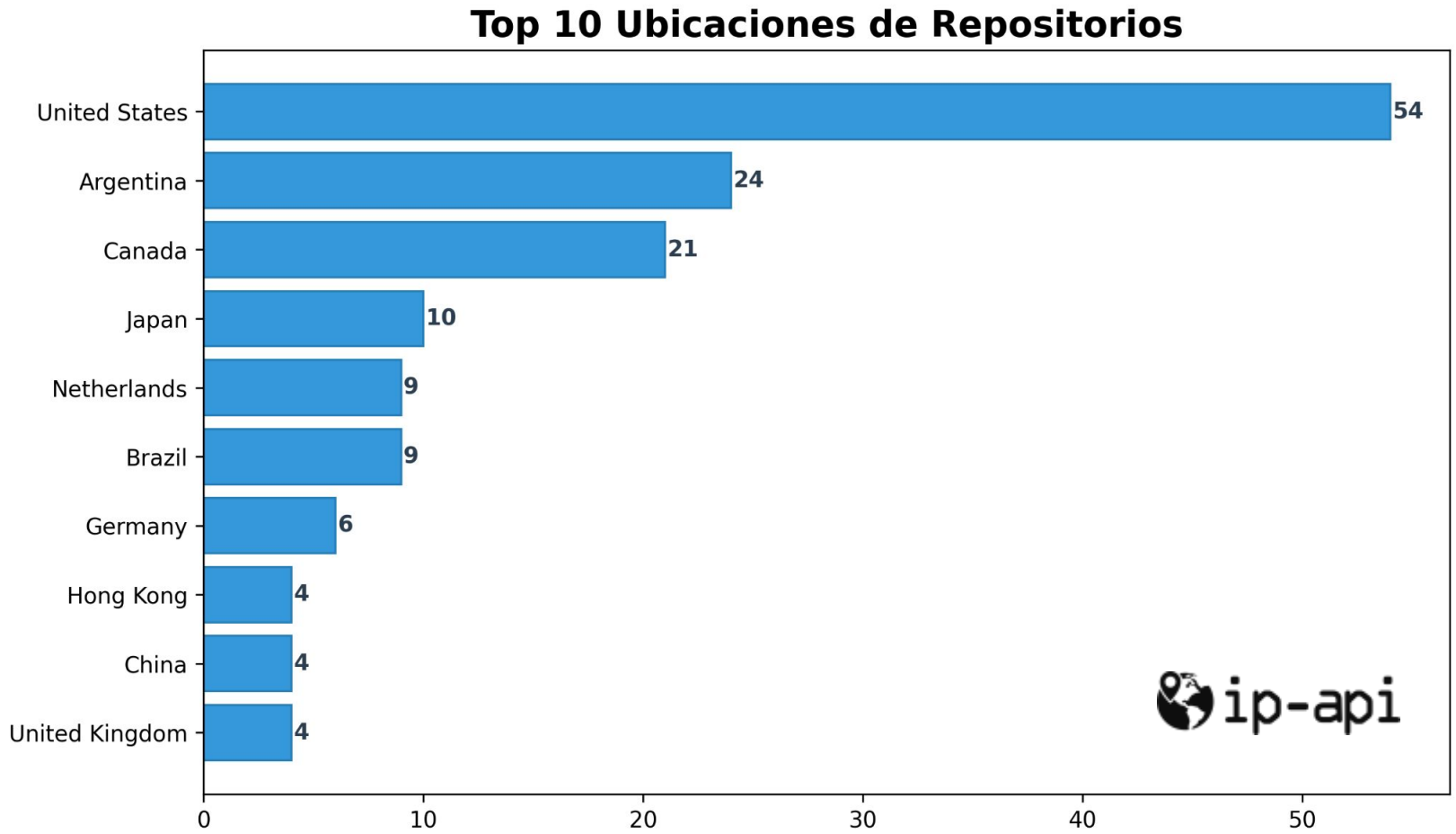
rpki-prover

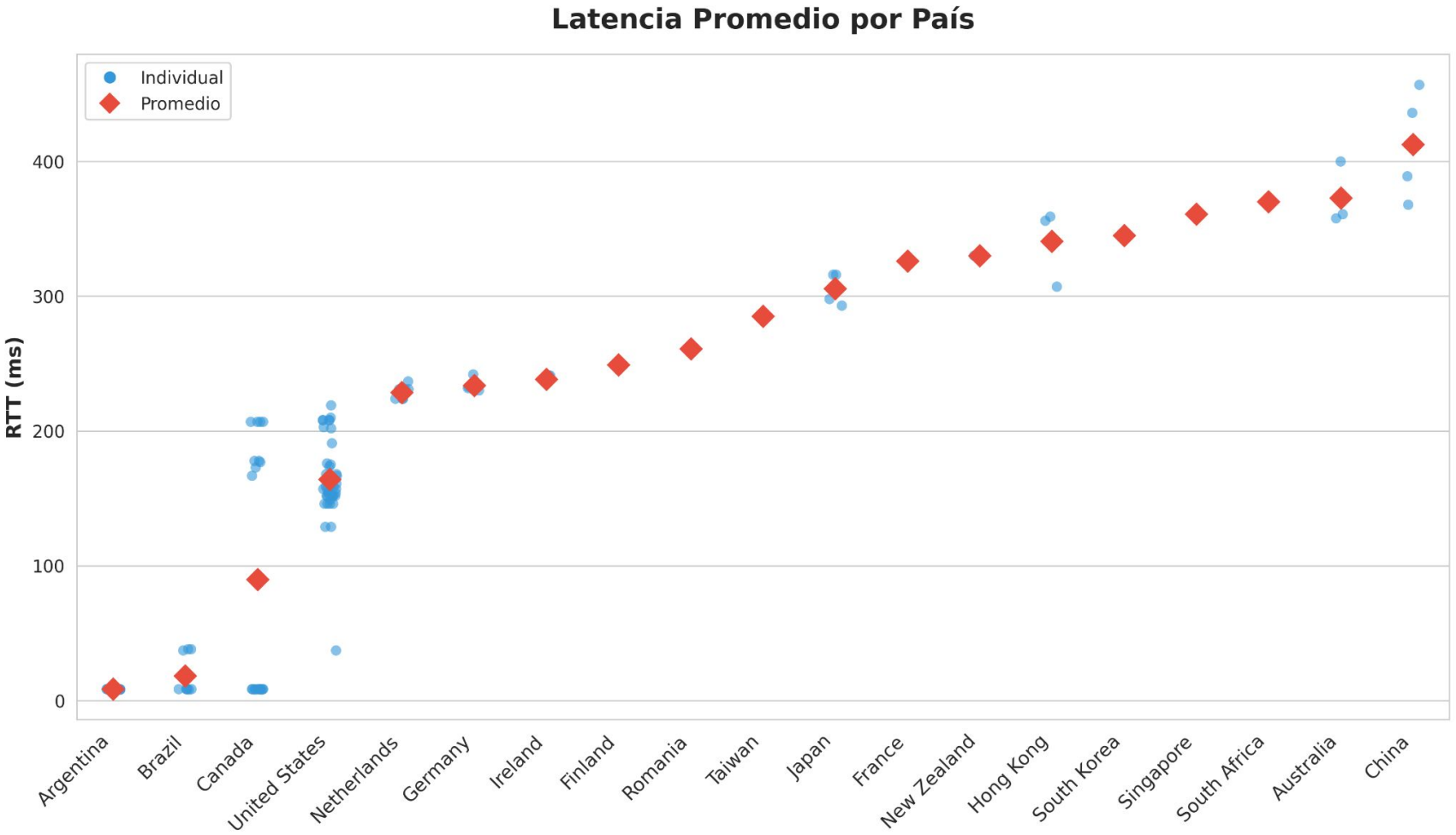
Validation metrics

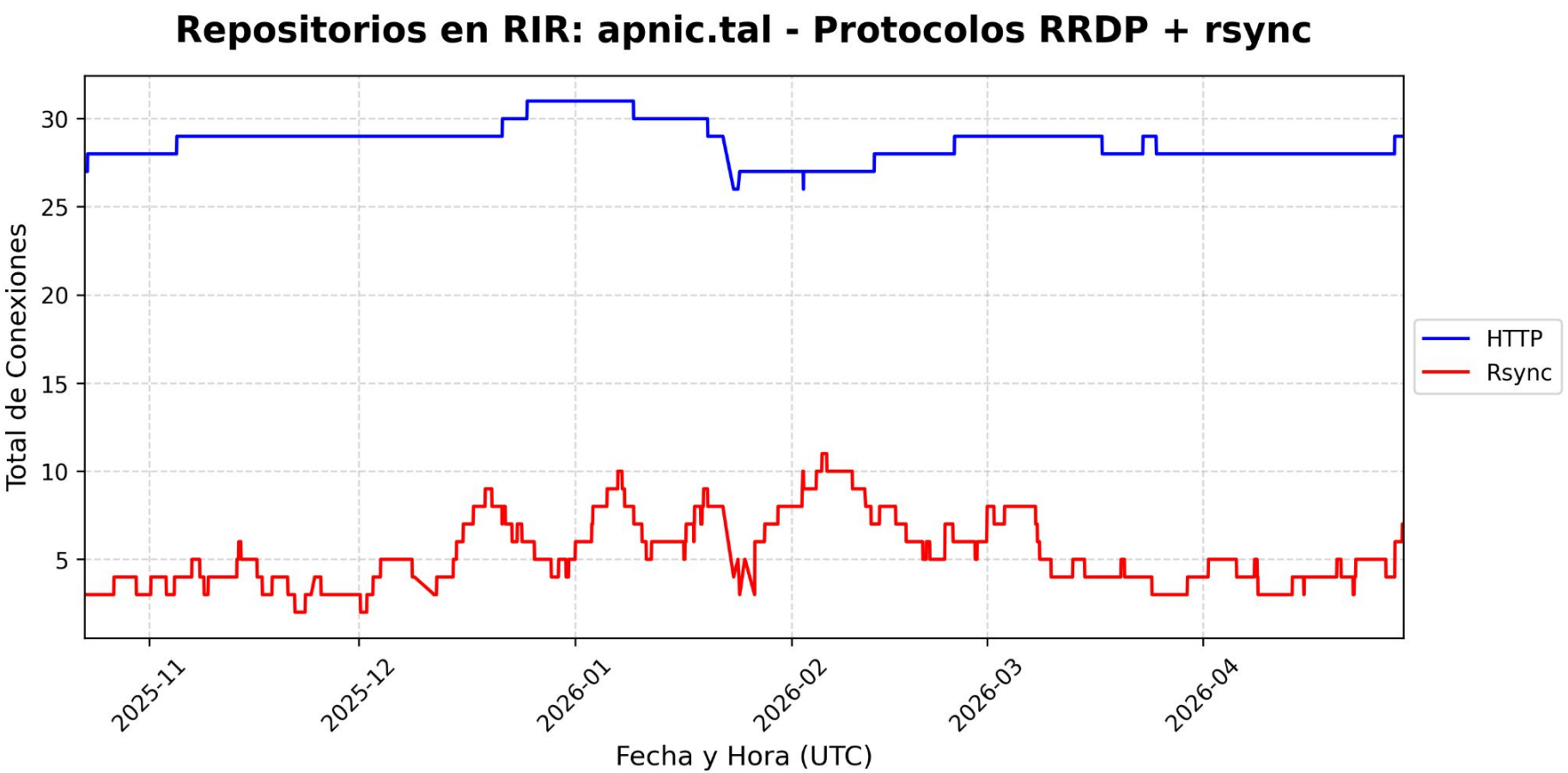
Trust Anchor (5 in total)	Validated at	Validation time	Original VRPs	Unique VRPs	Objects	ROAs	Certificates	Manifests	CRLs	GBRs	ASPAs
afrinic	2026-01-22 04:39:23	11411ms	28443	24925	14750	10946	1268	1268	1268	0	0
apnic	2026-01-22 04:53:34	10757ms	169043	166358	77970	40495	12498	12485	12485	0	7
arin	2026-01-22 04:53:34	14187ms	235289	234109	229181	204469	8234	8218	8218	0	42
lacnic	2026-01-22 04:39:23	27489ms	40513	40513	52241	32990	6419	6390	6390	0	52
ripe	2026-01-22 04:53:34	13189ms	323795	323771	121298	55370	21810	21742	21742	1	631
Total	-	-	797083	789676	495440	344270	50229	50103	50103	1	732

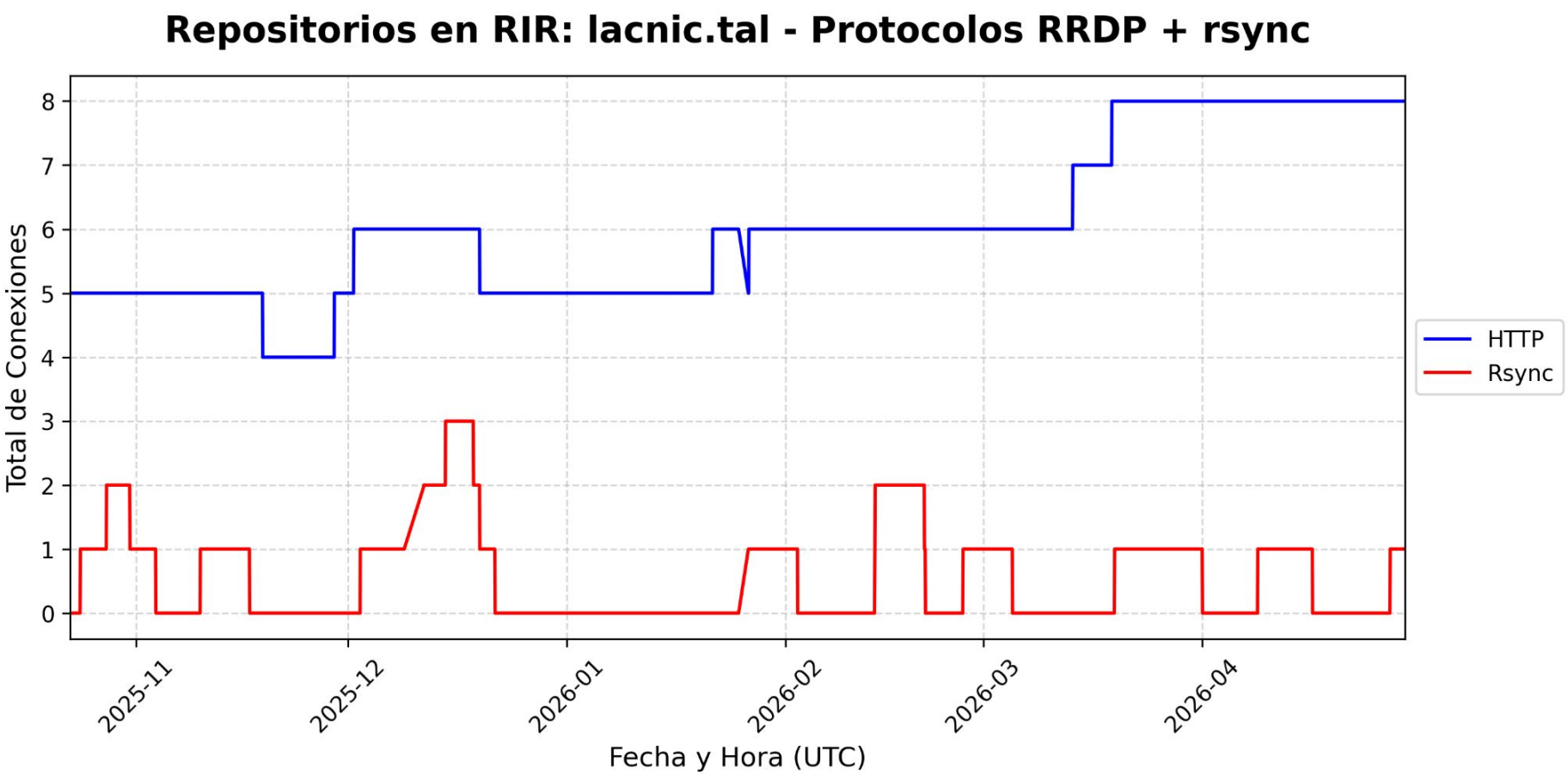
Crudos

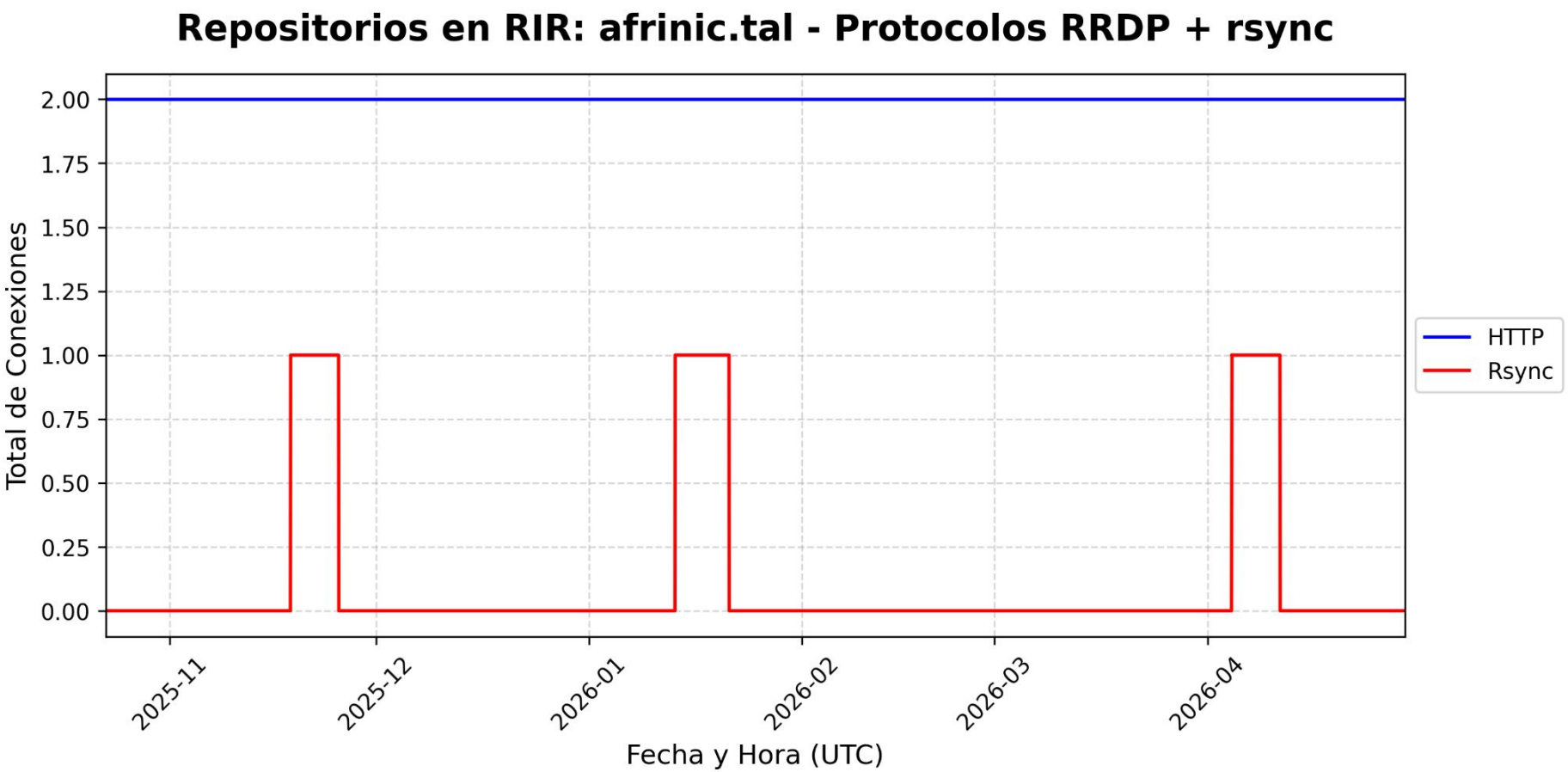
Optimizados

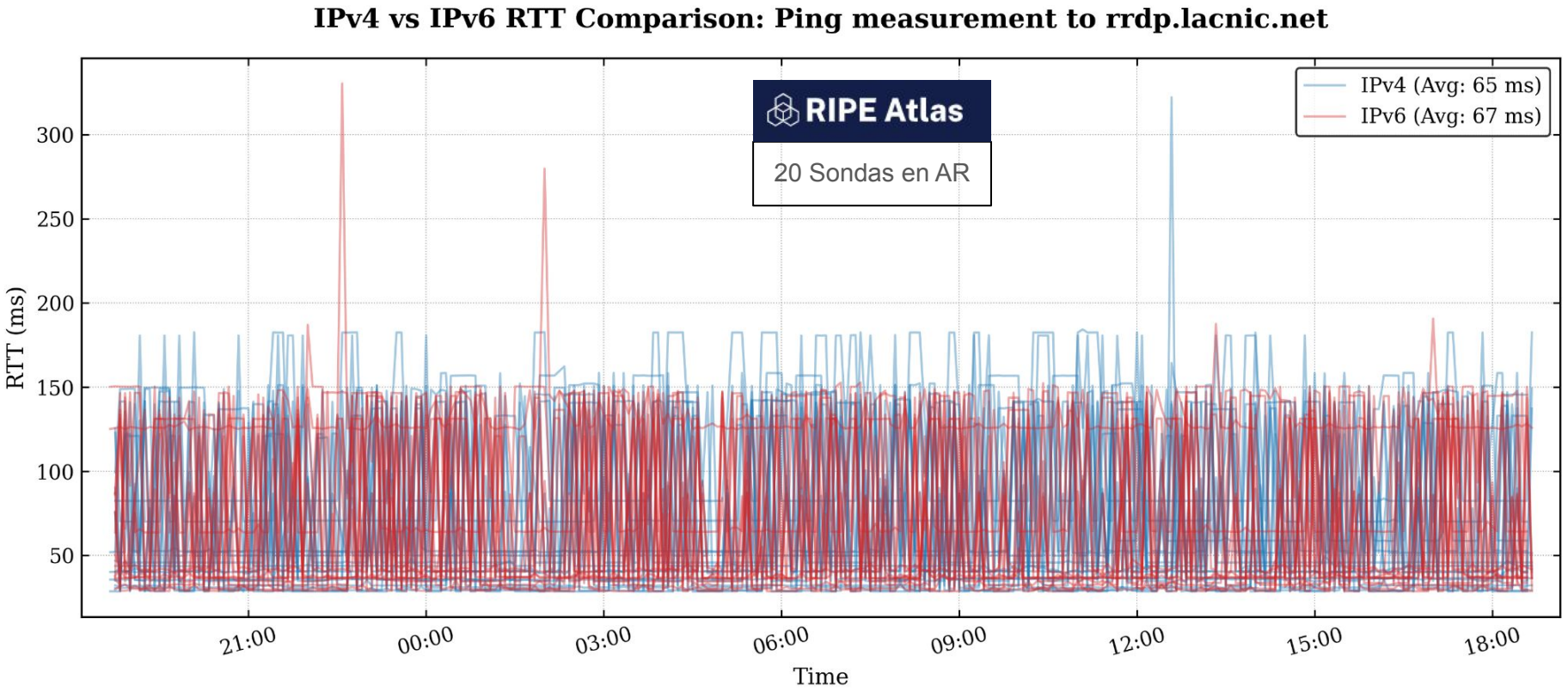

Top 10 Ubicaciones de Repositorios
United States
Argentina
Canada
Japan
Netherlands
Brazil
Germany
Hong Kong
China
United Kingdom
54
24
21
10
9
9
6
4
4
4
0
10
20
30
40
50
ip-api

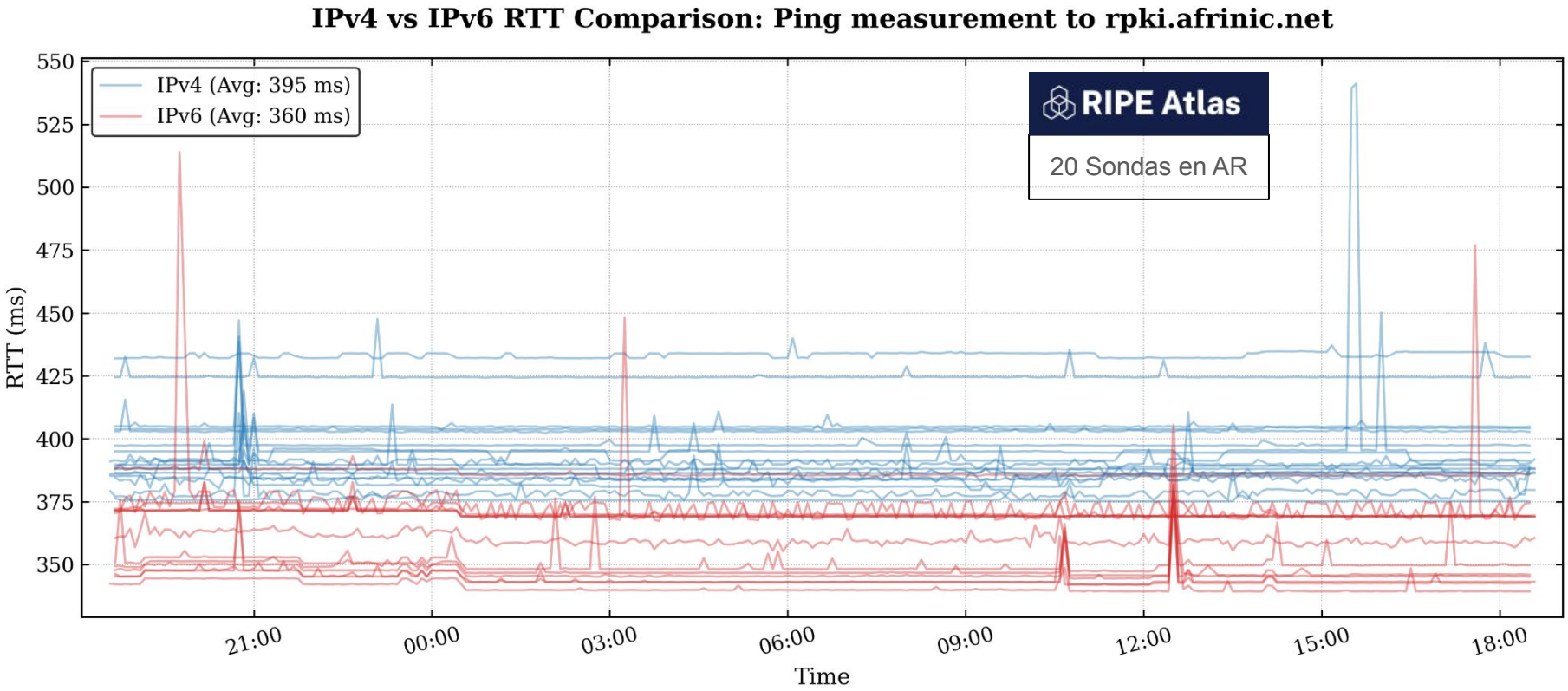

Latencia Promedio por País
Individual
Promedio
RTT (ms)
0
100
200
300
400
Argentina
Brazil
Canada
United States
Netherlands
Germany
Ireland
Finland
Romania
Taiwan
Japan
France
New Zealand
Hong Kong
South Korea
Singapore
South Africa
Australia
China

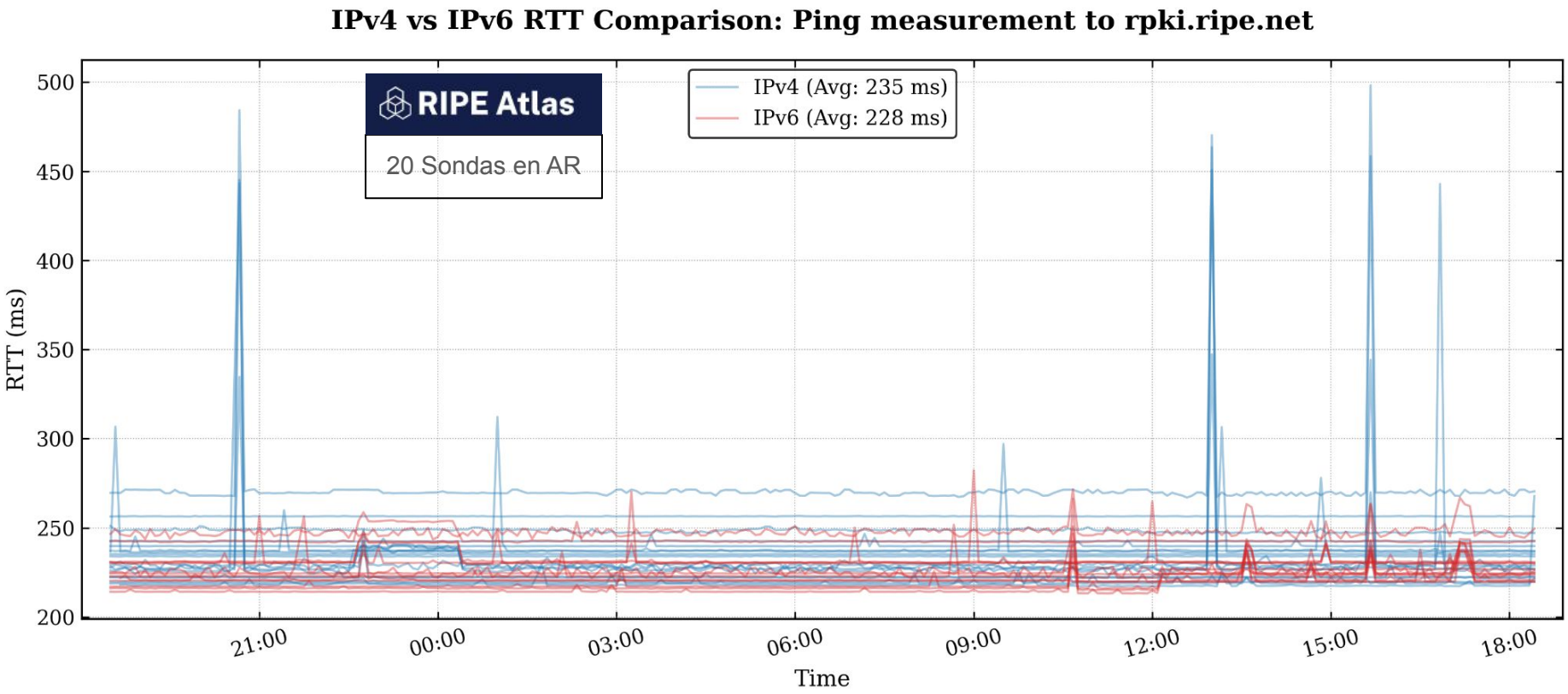

Repositorios en RIR: apnic.tal - Protocolos RRDP + rsync
Total de Conexiones
30
25
20
15
10
5
2025-11
2025-12
2026-01
2026-02
2026-03
2026-04
Fecha y Hora (UTC)
HTTP
Rsync


Repositorios en RIR: lacnic.tal - Protocolos RRDP + rsync
Total de Conexiones
0
1
2
3
4
5
6
7
8
2025-11
2025-12
2026-01
2026-02
2026-03
2026-04
Fecha y Hora (UTC)
HTTP
Rsync


Repositorios en RIR: afrinic.tal - Protocolos RRDP + rsync
Total de Conexiones
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
2025-11
2025-12
2026-01
2026-02
2026-03
2026-04
Fecha y Hora (UTC)
HTTP
Rsync

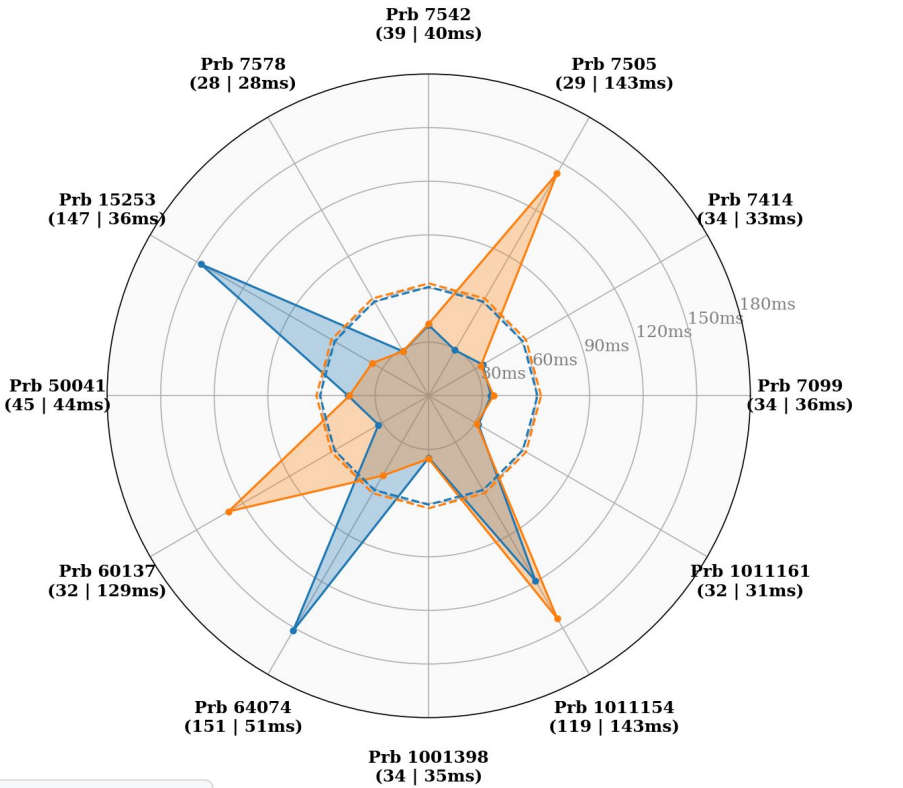

IPv4 vs IPv6 RTT Comparison: Ping measurement to rrdp.lacnic.net
RIPE Atlas
20 Sondas en AR
IPv4 (Avg: 65 ms)
IPv6 (Avg: 67 ms)
RTT (ms)
300
250
200
150
100
50
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
Time


IPv4 vs IPv6 RTT Comparison: Ping measurement to rpki.afrinic.net
IPv4 (Avg: 395 ms)
IPv6 (Avg: 360 ms)
RIPE Atlas
20 Sondas en AR
RTT (ms)
550
525
500
475
450
425
400
375
350
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
Time


IPv4 vs IPv6 RTT Comparison: Ping measurement to rpki.ripe.net
RIPE Atlas
20 Sondas en AR
IPv4 (Avg: 235 ms)
IPv6 (Avg: 228 ms)
RTT (ms)
500
450
400
350
300
250
200
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
Time

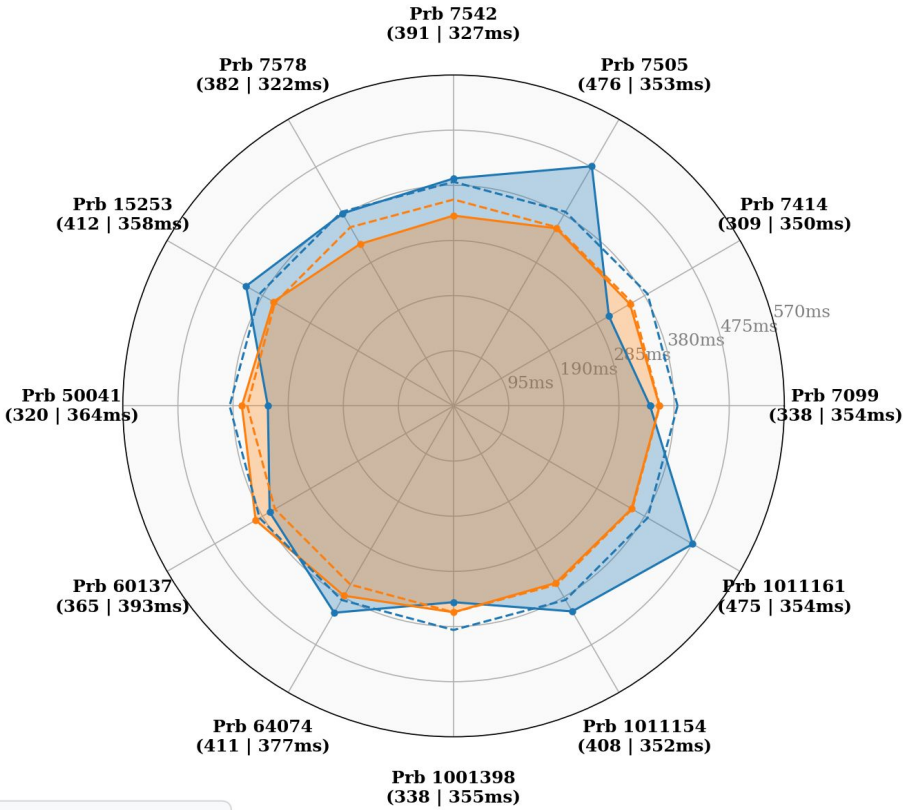
RIPE Atlas

20 Sondas en AR



RIPE Atlas

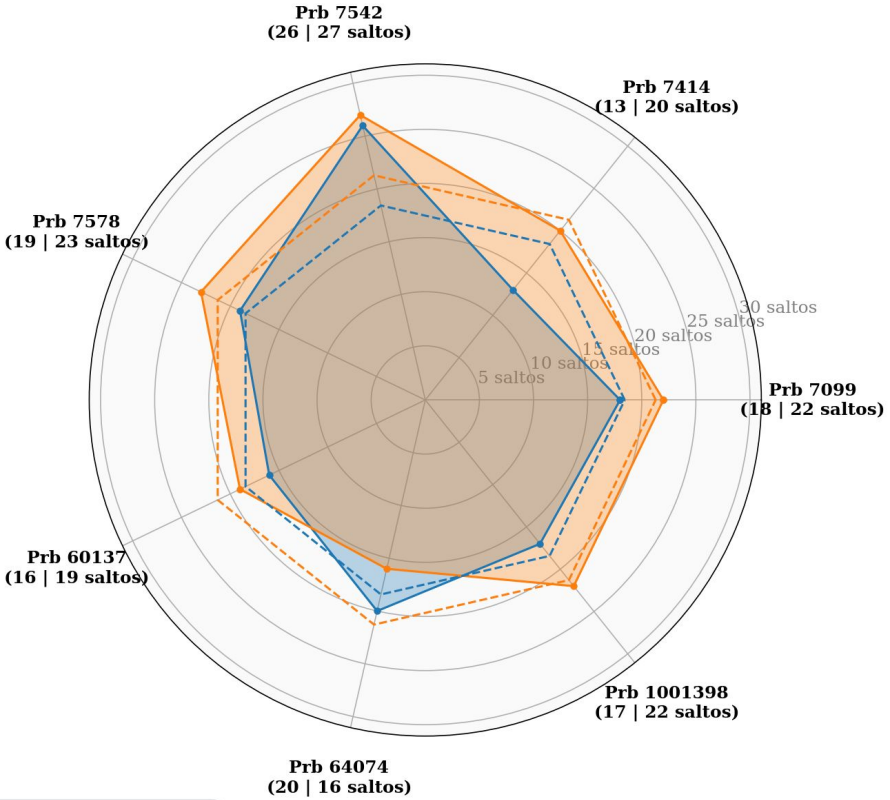
20 Sondas en AR



Comparative Hop Count Radar
M1: Traceroute measurement to rpki.apnic.net

RIPE Atlas

20 Sondas en AR



Conclusiones

- RPKI está en permanente evolución
- Obtener distintas métricas nos permite conocer mejor el comportamiento del validador y entender cómo funciona en la infraestructura global de RPKI
- La latencia asociada a la ubicación geográfica del proveedor influye en los tiempos de sincronización
- La eficiencia de RRDP por sobre RSYNC ha disminuido la cantidad de información a transferir en los ciclos de validación
- Todo aporte desde cualquier ámbito ayuda a mejorar los diferentes aspectos de RPKI. No olvidemos que somos una comunidad!!!

Recomendaciones

- Considerar las capacidades de la MV donde correrá mi validador (Memoria, tmpFS, CPU…..GPU a futuro?)
- Instalar más de un software validador a modo de respaldo y redundancia
- Utilizar diferentes direcciones IPv4 e IPv6 en cada validador hacia los repositorios (Evitar probables filtros DDoS)
- RPKi depende del DNS: usar resolvers con resolución en paralelo
- Monitorear las dos caras del Validador: puntos de publicación (RRDP / rsync) y routers (RTR)
- Proxy RTRTR puede ser una buena alternativa para grandes y medianos operadores

Referencias

- “¿Qué estará haciendo ‘X’ en este momento?” ©. CQC,

  https://es.wikipedia.org/wiki/Caiga_quien_caiga_(Argentina)

- Prometheus colector. https://prometheus.io/
- Grafana. https://grafana.com/grafana
- RIPE Atlas. https://atlas.ripe.net
- Proyecto Fort https://fortproject.net/



Referencias

- N. Rodday et al., "The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects," in IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 2353-2373, April 2024.
- Fontugne, R., Phokeer, A., Pelsser, C., Vermeulen, K., & Bush, R. (2023). RPKI Time-of-Flight: Tracking Delays in the Management, Control, and Data Planes. In Passive and Active Measurement: 24th International Conference, PAM 2023 (pp. 429–457). Springer.
- Sediqi, Khwaja Zubair, Romain Fontugne, Amreesh Phokeer, Massimiliano Stucchi, Massimo Candela and Anja Feldmann. “RPKI Syncing: Delay in Relying Party Synchronization.” 2025 9th Network Traffic Measurement and Analysis Conference (TMA) (2025): 1-11.

¿Preguntas?

¡¡Gracias Totales!!

slaggio@criba.edu.ar