Routing Security Landscape

Doug Madory (Kentik)

Global Adoption Statistics

Measuring RPKI deployment progress

Two steps needed to identify and reject RPKI-Invalid BGP routes

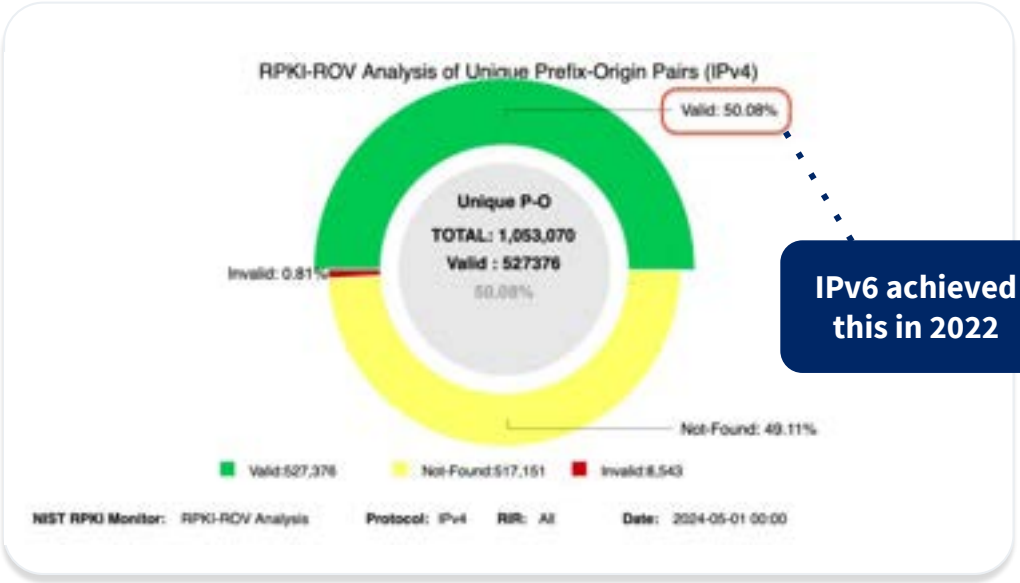
1

Create ROAs to define correct origins for address space

2

ASes reject RPKI-invalid routes that don’t match ROAs

Measuring RPKI deployment progress



IPv6 achieved this in 2022

May 1, 2023: Milestone in adoption:

- >50% of IPv4 routes in global routing table have ROAs (NIST RPKI monitor)

Measuring RPKI deployment progress

But RPKI ROV is ultimately about protecting traffic, so…

Beginning a couple of years ago, I started using Kentik's aggregate NetFlow to gain a deeper understanding of RPKI ROV adoption.

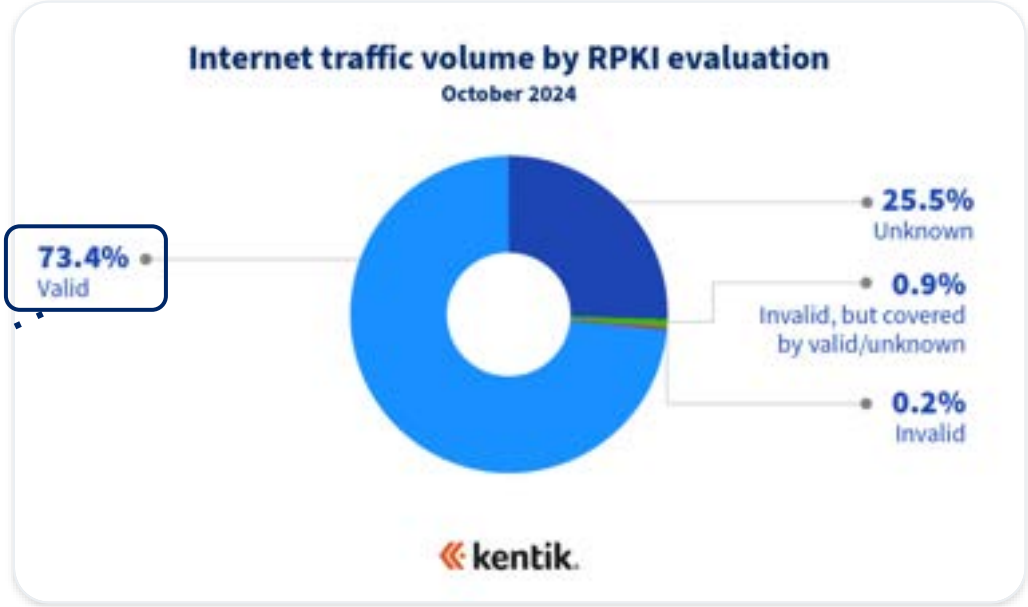
- Kentik has over 450 customers, almost half have opted-in to the use of their data as part of aggregate analysis.
  - Note: analysis is subject to biases of the customer set which includes (NSPs, CDNs and enterprises) and is skewed toward the US.

- Kentik's NetFlow analytics platform annotates flow records with an RPKI evaluation of route of destination IP upon intake.
  - Built to gauge how much traffic would be lost by rejecting invalids.
  - Can also be used to understand RPKI from a traffic-volume perspective.

Measuring RPKI deployment progress

At NANOG 84 in Austin, TX, I explored ROA creation using Kentik's aggregate NetFlow:

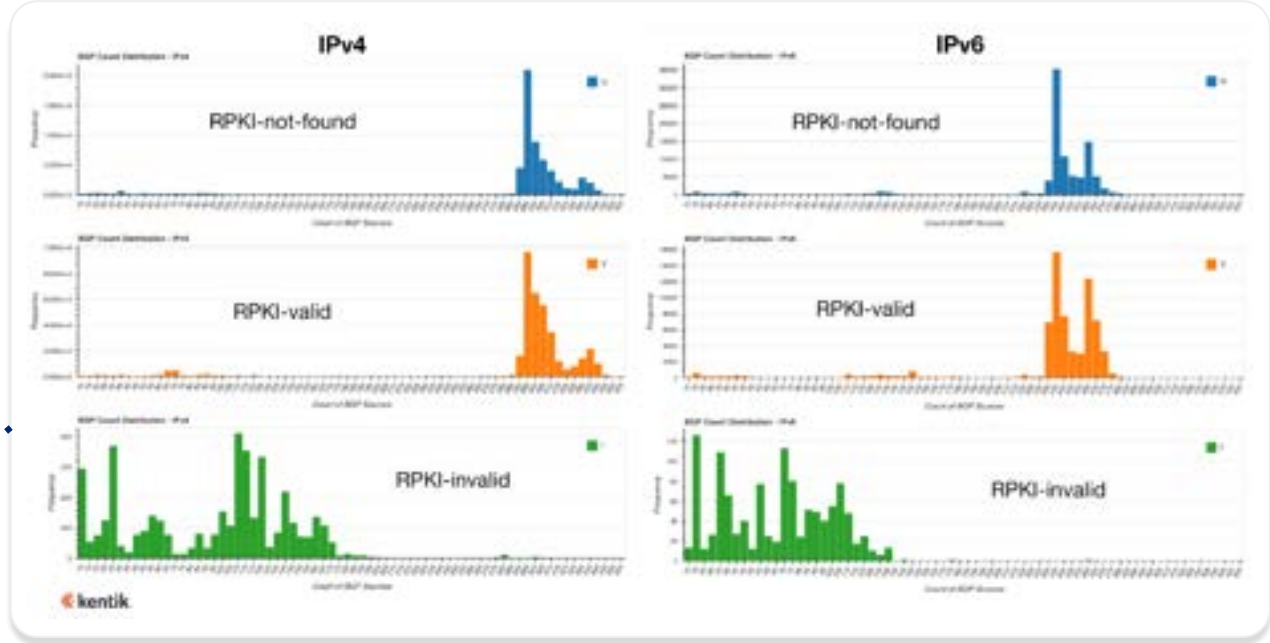
- **Feb 2022**: 1/3 of BGP routes had ROAs, >1/2 of traffic (bps) went to routes with ROAs
- **Oct 2024**: >1/2 of BGP routes have ROAs, <3/4 of traffic (bps) went to routes with ROAs



Propagation Reduction of RPKI-Invalids

- ROAs alone are useless if only a few networks are rejecting invalid routes.
- 2022 analysis showed propagation of RPKI-invalid routes is half or less than other types.

Stats from Aug 2022:
How has this changed since?



www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/

RPKI-Invalid Propagation Declining

- RIPE NCC and Job Snijders (AS15562) announce RPKI-invalid (and RPKI valid) routes for measurement of RPKI ROV deployment.
- Invalid routes from each of these beacons all experienced an overall decline in propagation while the control routes saw increased propagation.

JANUARY 3, 2024

ROV and the Orange España outage

- Hacker was able to log into company's RIPE NCC portal using the password "ripeadmin" found in a leak of stolen credentials. Oops!
- Hacker altered Orange España's RPKI configuration, rendering many of its BGP routes RPKI-invalid.
- Outage marked the first time RPKI ROV was used as a vector for a denial-of-service.

Outage only possible due to rejections of RPKI-invalids

Regional Adoption Statistics

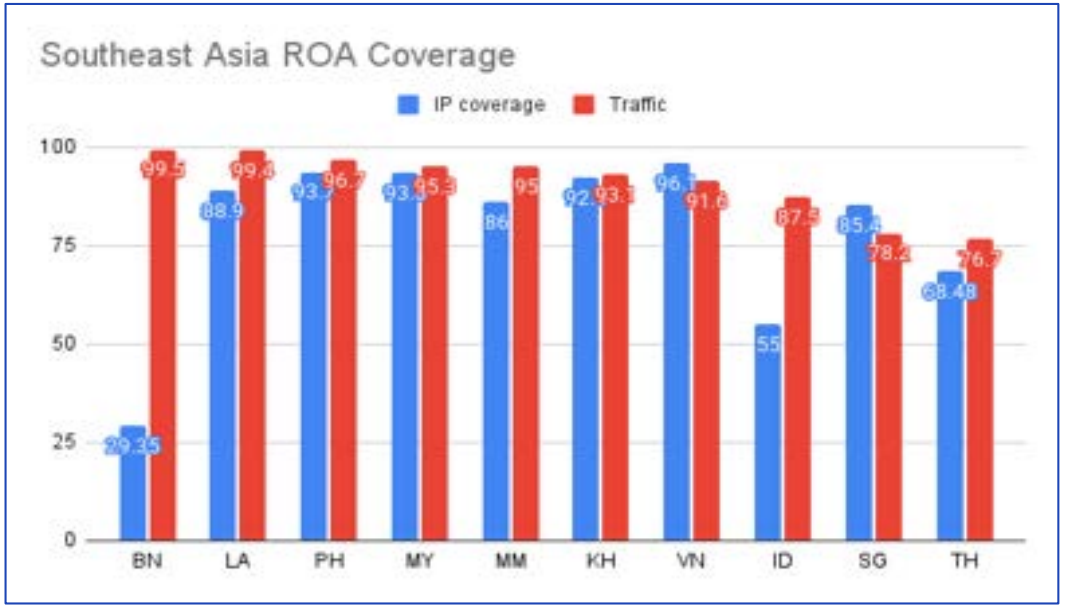
ROA Coverage Statistics

Beginning with Southeast Asia

- We'll use two metrics:
- "IP coverage" from RIPEstat
  - Percentage of IPv4 space covered by ROAs
- "Traffic coverage" from Kentik aggregate NetFlow
  - % of traffic (bits/sec) by RPKI-evaluation

ROA Coverage Statistics (Southeast Asia)

- Overall, ROA coverage is excellent



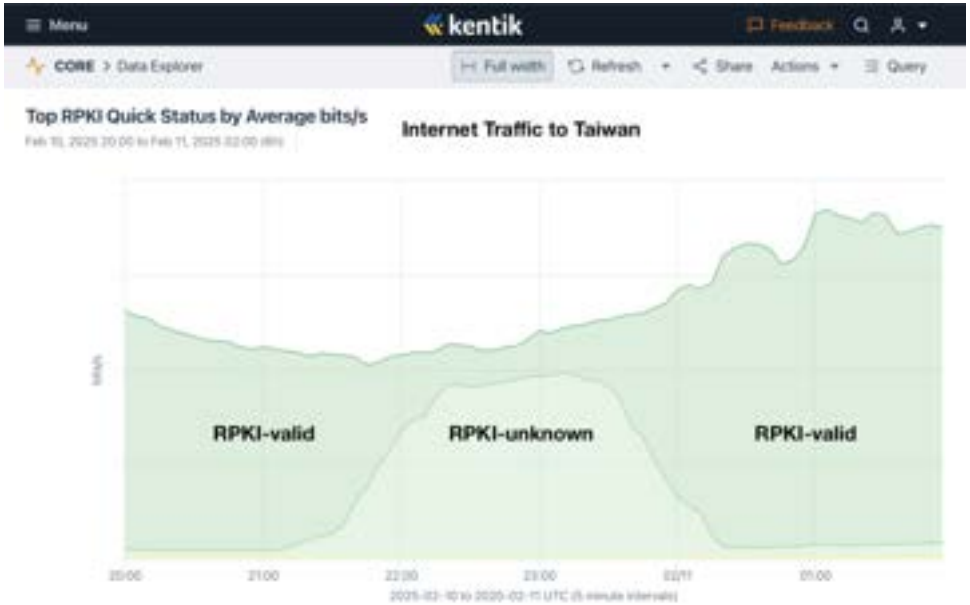
- Note: RIPEstat reports very low IPv4 coverage for Brunei (BN), but we see nearly all traffic to the country heading to AS10094 (UNN) which has ~100% ROA coverage.

ROA Coverage Statistics (Greater Asia)

- Too many countries to list, but here are some highlights
- Numerous APRICOT countries have high ROA coverage! (bps)
  - **> 90%: MV, BD, MN, TW, LK, MO**
  - **> 70%: TL, IN, HK, JP, NZ, AU, PG**
- Notable countries with low coverage (<5%)
  - **China (2.5%), North Korea (0%) — trust issues?**
  - **South Korea (6%)**
    - RPKI-valid traffic is mostly foreign cloud providers.
    - KRNIC controls issuance of ROAs — can we improve this process?

ROA Coverage Statistics (Greater Asia)

- TW has one of the highest levels of ROA coverage in the world!
  - 98.5% IP, 98.2% traffic
- Recently suffered a multi-hour outage which expired all of its ROAs.
- No disruption of traffic.
- During outage, only TW RPKI-valid routes were from foreign cloud providers.



RPKI Database Growth

A Year of RPKI Database Growth

- Year-over-year analysis of the RPKI database using RPKIviews.org snapshots
  - Based on the the ARIN, AFRINIC, APNIC, LACNIC, and RIPE NCC Trust Anchors.

	2023-12-31	2024-12-31	
Total cache size (KiB):	1,546,728	2,021,784	(+31%)
Total number of files (objects):	309,802	415,384	(+34%)
Wall time validation run (seconds):	163	228	(+40%)
Publication servers (FQDNs):	63	53	(-16%)
Certification authorities:	40,511	44,935	(+11%)
Route origin authorizations:	188,345	280,692	(+49%)
Uniq VRPs:	497,341	639,909	(+29%)
Average ROAIPAddresses per ROA:	2.7	2.3	(-15%)
IPv4 addresses covered:	2,502,293,068	2,726,513,768	(+ 9%)
Uniq IPv4 addresses covered:	1,502,281,680	1,658,281,248	(+10%)
IPv6 addresses covered:	17,263 * 10^30	17,392 * 10^30	(+ 1%)
Uniq IPv6 addresses covered:	15,128 * 10^30	15,139 * 10^30	(+ 0%)
Uniq origin ASNs in ROAs:	40,656	47,282	(+16%)
Uniq ASPA Customer ASIDs:	56	87	(+55%)

- Credit: Job Snijders' RPKI's 2024 Year in Review

A Year of RPKI Database Growth

- Year-over-year analysis of the RPKI database using RPKIviews.org snapshots
  - Based on the the ARIN, AFRINIC, APNIC, LACNIC, and RIPE NCC Trust Anchors.

	2023-12-31	2024-12-31	
Total cache size (KiB):	1,546,728	2,021,784	(+31%)
Total number of files (objects):	309,802	415,384	(+34%)
Wall time validation			
Publication servers			
Certification authorities:	40,511	44,935	(+11%)
Route origin authorizations:	188,345	280,692	(+49%)
Uniq VRPs:	497,341	639,909	(+29%)
Average ROAIPAddresses per ROA:			
IPv4 addresses covered:	2,50		
Uniq IPv4 addresses covered:	1,502,281,680	1,658,281,248	(+10%)
IPv6 addresses covered:	17,263 * 10^30	17,392 * 10^30	(+ 1%)
Uniq IPv6 addresses covered:	15,128 * 10^30	15,139 * 10^30	(+ 0%)
Uniq origin ASNs in ROAs:	40,656	47,282	(+16%)
Uniq ASPA Customer ASIDs:	56	87	(+55%)

The size of the database growth by 31% in 2024.

The number of ROAs is up 49%!

- Credit: Job Snijders' RPKI's 2024 Year in Review

A Year of RPKI Database Growth

- Year-over-year analysis of the RPKI database using RPKIviews.org snapshots
  - Based on the the ARIN, AFRINIC, APNIC, LACNIC, and RIPE NCC Trust Anchors.

	2023-12-31	2024-12-31	
Total cache size (KiB):	1,546,728	2,021,784	(+31%)
Total number of files (objects):	309,802	415,384	(+34%)
Wall time validation run (seconds):	**163**	**228**	**(+40%)**
Publication servers (FQDNs):	**63**	**53**	**(-16%)**
Certification authorities:	40,511	44,935	(+11%)
Uniq IPv4 addresses covered:	1,502,281,680	1,658,281,248	(+10%)
IPv6 addresses covered:	17,263 * 10^30	17,392 * 10^30	(+ 1%)
Uniq IPv6 addresses covered:	15,128 * 10^30	15,139 * 10^30	(+ 0%)
Uniq origin ASNs in ROAs:	40,656	47,282	(+16%)
Uniq ASPA Customer ASIDs:	56	87	(+55%)

The time it takes to load and cryptographically validate grew 40%. Not yet a concern, but something to keep an eye on.

The fewer publication points, the better. Every validator on the planet MUST contact every publication server.

- Credit: Job Snijders' RPKI's 2024 Year in Review

A Year of RPKI Database Growth

- Year-over-year analysis of the RPKI database using RPKIviews.org snapshots
  - Based on the the ARIN, AFRINIC, APNIC, LACNIC, and RIPE NCC Trust Anchors.

	2023-12-31	2024-12-31	
Total cache size (KiB):	1,546,728	2,021,784	(+31%)
Total number of files:			
Wall time validation run (seconds):	165	228	(+40%)
Publication servers (FQDNs):	63		
Certification authorities:	40,511		
Route origin authorizations:			
Uniq VRPs:			
Average ROAIPAddresses per ROA:	2.7	2.3	(-15%)
IPv4 addresses covered:	2,502,293,068	2,726,513,768	(+ 9%)
Uniq IPv4 addresses covered:	1,502,281,680	1,658,281,248	(+10%)
IPv6 addresses covered:	17,263 * 10^30	17,392 * 10^30	(+ 1%)
Uniq IPv6 addresses covered:	15,128 * 10^30	15,139 * 10^30	(+ 0%)
Uniq origin ASNs in ROAs:	40,656	47,282	(+16%)
Uniq ASPA Customer ASIDs:	56	87	(+55%)

10% more unique IPv4 addresses covered.

No change for IPv6.

16% more ASNs in these ROAs.

- Credit: Job Snijders' RPKI's 2024 Year in Review

Measuring Success

Measuring Success is Challenging

- Did you know?: Routing leaks are still occurring with some regularity!

Improvements in route hygiene are containing these leaks.

Measuring Success is Challenging

- In September, Brazil ordered X (Twitter) to be blocked.
- Some ISPs used BGP to hijack/blockhole X.
  - …and leaked the hijacks (like Myanmar in 2021 and Russia in 2022)
- But the only hijacked X routes that appeared in public data were those without ROAs.
  - Likely explanation: RPKI-invalids were rejected.
  - No disruption of X outside of Brazil.
  - RPKI-ROV did its job and no one knew.

Conclusion

- The system is working as designed!
- Progress due to the dedicated efforts of hundreds of engineers at dozens of companies.
  - 1/2 of BGP routes have ROAs, >2/3 of traffic (bps) went to routes with ROAs
  - Propagation of RPKI-invalids continues to decline, Zayo now rejecting invalids
- RPKI ROV doesn’t solve all the issues surrounding Internet routing security.
  - Only an opening salvo towards addressing the various “determined adversary” scenarios best characterized by the recent attacks against cryptocurrency services.
- Need to build off the progress made by RPKI ROV to address more difficult scenarios.

Thank you!

Doug Madory
dmadory@kentik.com

@DougMadory
in/DougMadory