Assessing the feasibility of routing security compliance tests

Moritz Müller, Lisa Bruder | RIPE 91 Routing WG

SIDN LABS

About us

Moritz Müller

- 10 years of experience as research engineer at SIDN Labs
- RIPE DNS-WG co-chair

Lisa Bruder

- Research engineer at SIDN Labs since 2024
- Current research focus: BGP security (RPKI, ROA/ROV, BGPsec)

Why compliance tests?

MANRS is working on an elevated tier “MANRS+”

Question: Can we measure routing security controls with a high assurance level?

Starting point: feasibility study in a local testbed

MANRS+ routing security controls

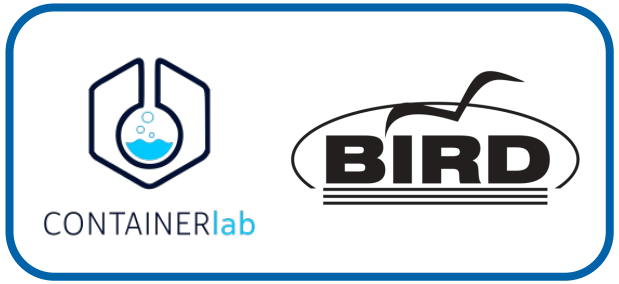
Route Origin Validation

Prefix filtering of customers

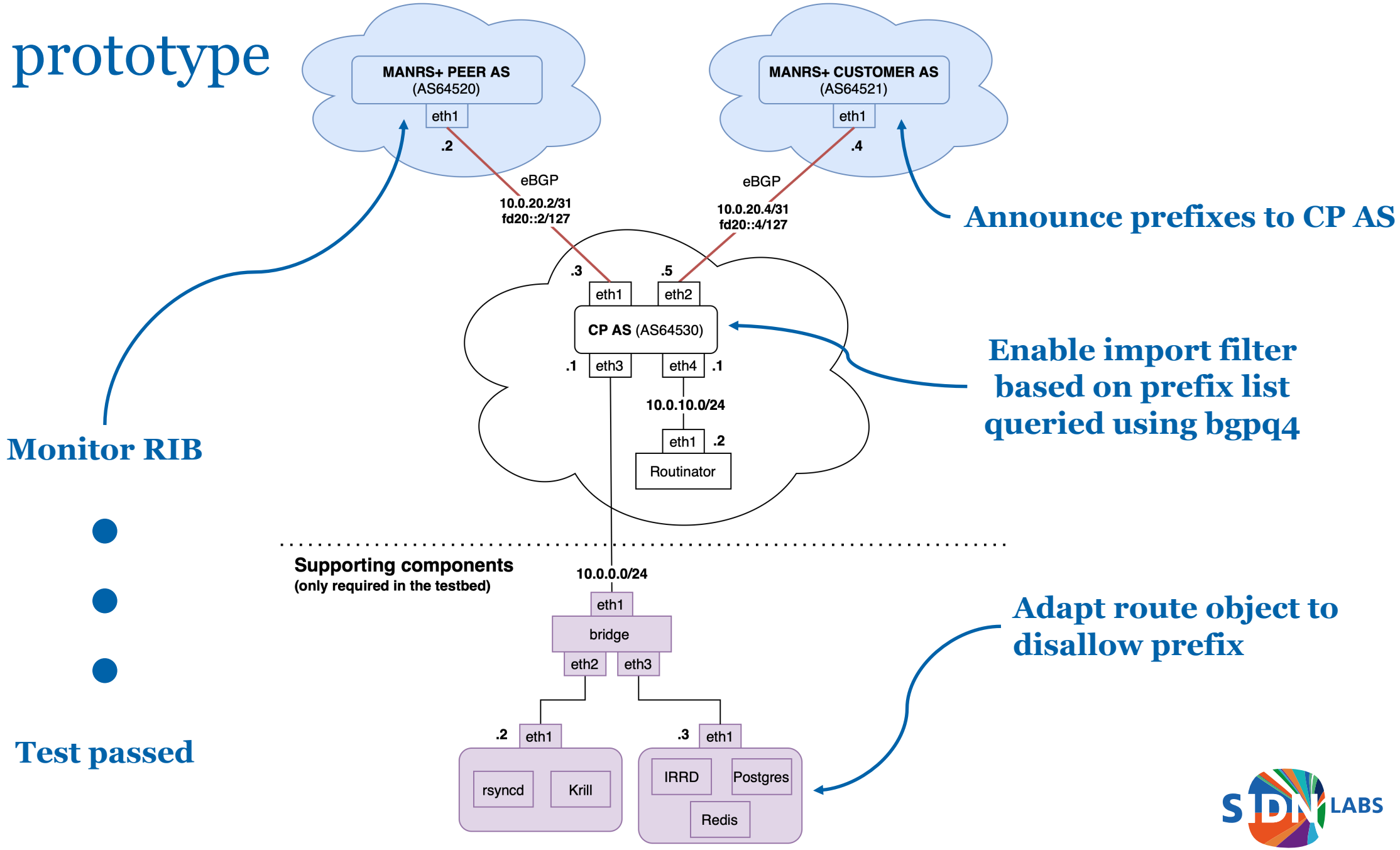
Control a set of customer ASes

Filtering of bogons

The prototype



The prototype



In conclusion: It works …

… in a testbed

Pitfalls when running tests in the wild

RPKI and IRR info does not propagate immediately
-> *take propagation delay into account*

Auditing multiple CP ASes
-> *observe announcements at peer AS before path selection*

Test prefixes can propagate unintentionally
-> *Withdraw as soon as possible; document test resources*

Recommended next steps

- Run tests with ASes with public prefixes
- Test more controls in other domains

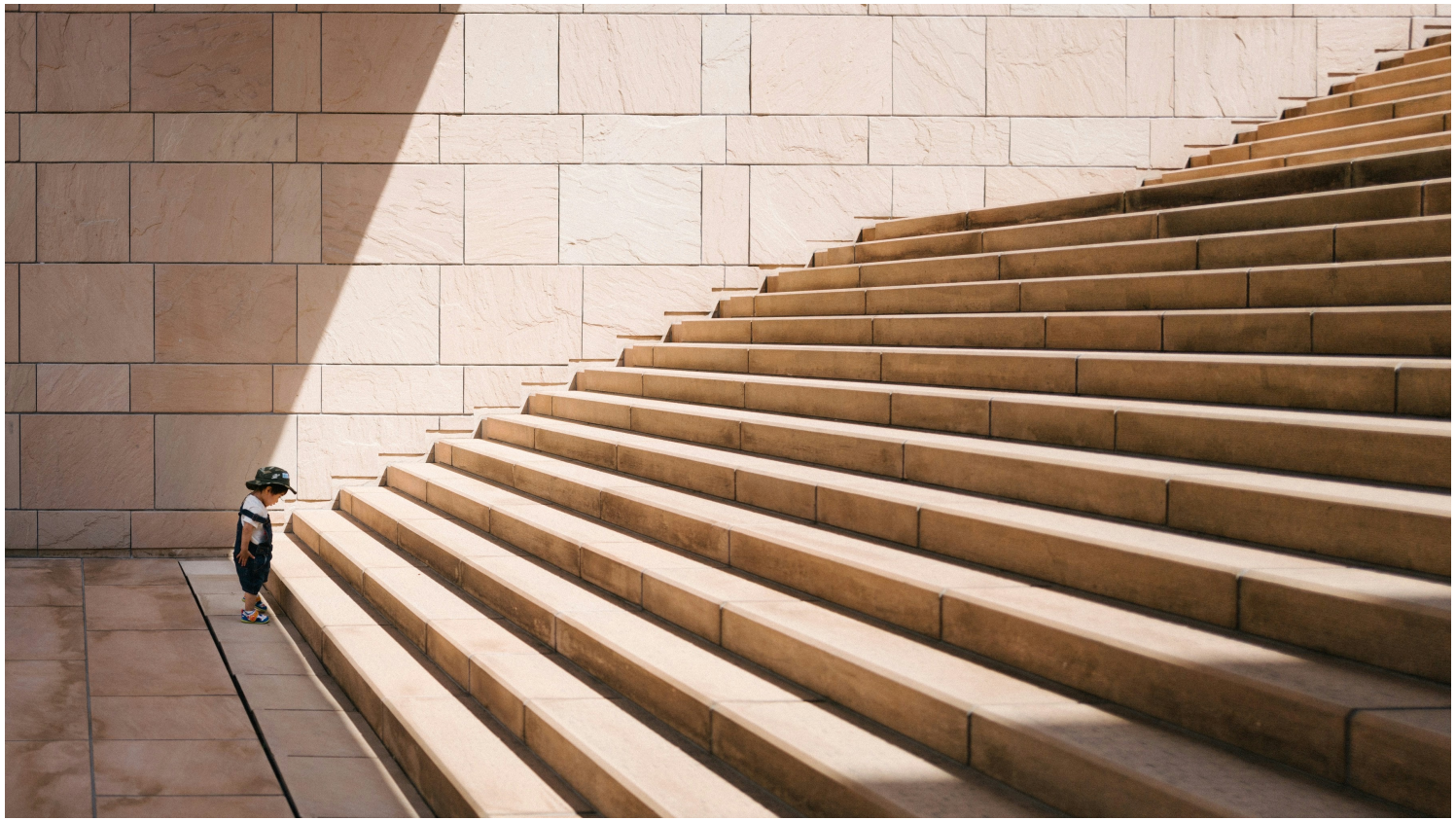


Photo by Jukan Tateisi on Unsplash

Feedback welcome

- What else could hinder deployments in the wild?
- Could this tool be handy for other people?
- Anything else?

Testbed code on GitHub:
https://github.com/SIDN/manrs-prototype

More detailed at the MANRS Community meeting on the 12th of November.

Are there any questions?

Public report (PDF)