Assessing the feasibility of routing security compliance tests

Moritz Müller, Lisa Bruder

2nd MANRS Community Meeting 2025

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)

MANRS+ control matrix

MANRS+ Controls Ver. 20250204

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)	Ownership	Comments
Routing Security						
Routing Security	RPKI Route Origin Validation	RS-01	Any announcement received from a BGP neighbor or originated by the CP that is invalidated by an existing RPKI ROA is discarded and not announced to other BGP neigbours.	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] 2. Verify that all RPKI setup is documented, including the validation workflow, which RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported, and how often these updates are published to their routers.[Self-declared][Audited]	Connectivity Provider (CP)	Efficacy of RS-01 depends on the implementation of controls RI-01 and RI-03 by the Enterprise Customers (EC).
Routing Security	Prefix Filtering of Customers	RS-02	In cases where RPKI Route Origin Validation cannot be effectively applied (e.g. no matching ROA is found), announcements received from a direct customer and its customer cone (if exists) are filtered using a whitelist (permit-list) generated from the IRR or by other means. Exception is the cases where unless the number of aggregated prefixes from a customer exceeds 1000 (discuss).	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. In case these cases happen on intrafaces that excluded from the requirement, verify that the number of aggregated prefixes exceeds 1000 (discuss) [Measured][Audited] 2. Check that the "Permit-list" prefix filtering is performed for all customers 3. Verify that the process for configuring new customer connections is documented and includes description of how the customer prefix-lists are generated and applied, how they are validated, and how often these prefix-lists are published to their routers. [Self-declared][Audited]	CP	Efficacy of RS-02 depends on the implementation of controls RI-02 and RI-03 by the Enterprise Customers (EC).
Routing Security	Control a set of customer ASes (that can originate announcements)	RS-03	The CP implements filtering permitting only ASNs for a direct customer and its downstream customers (if exist) to originate announcements. The set of permitted ASNs is obtained from an AS-SET in an IRR or by other means.	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured][Audited] 2. Verify that the Customer AS set is maninatained [Measured][Audited] 3. The process for configuring new customer connections is documented and includes description of how the filter list of ASNs of the customer and its downstream customers (if exist) is build, how it is validated, and how often this filter is published to the routers. [Self-declared][Audited]		
Routing Security	Assistance with RPKI or IRR maintenance for a customer	RS-04	Assist a customer with implementing controls RI-01, RI-02 and RI-03.	1. Examine a documented list of the RPKI and IRR maintenance operations that the provider can perform at customer's request on their behalf.[Self-declared][Audited]	CP	
Routing Security	Prevent route leaks	RS-05	Route leaks are mitigated by using a peerlock technique (describe, or provide a reference)	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine documentation, which includes information about the technical architecture and processes of maintaining the control [Self-declared][Audited]	CP	
Routing Security	Filtering of bogons	RS-06	Bogon announcements are not propagated to BGP neighbours	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] For the purpose of this metric, the bogons are defined as follows: a. Pv4: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml b. IPv6: https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml c. ASN: https://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml 2. Examine documentation, which includes information about the technical architecture and processes of maintaining this control. [Self-declared][Audited]	CP	
Routing Security	BGP session protection	RS-07	Measures are taken to ensure security of the BGP sessions with the neighbours	1. Check that CP's IP ranges do not appear on the Shadowserver reports https://shadowserver.org/what-we-do/network-reporting/accessible-bgp-service-report/ https://shadowserver.org/what-we-do/network-reporting/open-bgp-service-report/ [measured] 2. Examine documentation, which includes information how controls specified by RFC 7454 are implemented [Self-declared][Audited]		
DDoS Attack Mitigation						
DDoS Attack Mitigation	Detection of volumetric DDoS attack traffic	DA-01	Ingress and egress traffic can be monitored for a set of IP addresses and malicious traffic can be detected and reported.	1. Examine documentation describing detection capabilities and its parameters. The documentation should demonstrate: - capabilities for detecting and reporting egress attack traffic at the customer-facing PE [mandatory] - capabilities for detecting ingress attack traffic at the PE from all neightbours [optional] - capabilities for reporting ingress attack traffic at the customer-facing PE [optional] [Self-declared][Audited]	CP	
DDoS Attack Mitigation	Rate limiting of malicious traffic	DA-02	Attack traffic can be rate limited.	1. Examine documentation describing rate limiting capabilities and its parameters. The documentation should describe which points in the network are capable of rate-limiting attack traffic. This should include filtering options available, such as source address, destination address, port, protocol, and interface. [Self-declared][Audited]	CP	

MANRS+ control matrix

MANRS+ Controls	Ver. 20250204		
Control Domain	**Control Title**	**Control ID**	**Control Speci**
Routing Security			
Routing Security	RPKI Route Origin Validation	RS-01	Any announcement received from a BGP neighbo invalidated by an existing RPKI ROA is discarded a neigbours.
Routing Security	Prefix Filtering of Customers	RS-02	In cases where RPKI Route Origin Validation cann ROA is found), announcements received from a d exists) are filtered using a whitelist (permit-list) g Exception is the cases where unless the number exceeds 1000 (discuss).
Routing Security	Control a set of customer ASes (that can originate announcements)	RS-03	The CP implements filtering permitting only ASNs customers (if exist) to originate announcements. from an AS-SET in an IRR or by other means.
Routing Security	Assistance with RPKI or IRR maintenance	RS-04	Assist a customer with implementing controls RI-

MANRS+ control matrix

	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)	Ownership	
ted by the CP that is ounced to other BGP	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range [Measured] 2. Verify that all RPKI setup is documented, including the validation workflow, which RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported, and how often these updates are published to their routers.[Self-declared][Audited]	Connectivity Provider (CP)	Efficacy controls
ively applied (e.g. no matching ner and its customer cone (if om the IRR or by other means. d prefixes from a customer	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. In case these cases happen on intrafaces that excluded from the requirement, verify that the number of aggregated prefixes exceeds 1000 (discuss) [Measured][Audited] 2. Check that the "Permit-list" prefix filtering is performed for all customers 3. Verify that the process for configuring new customer connections is documented and includes description of how the customer prefix-lists are generated and applied, how they are validated, and how often these prefix-lists are published to their routers. [Self-declared][Audited]	CP	Efficacy controls
customer and its downstream ermitted ASNs is obtained	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range [Measured] Audited] 2. Verify that the Customer AS set is manintained [Measured][Audited] 3. The process for configuring new customer connections is documented and includes description of how the filter list of ASNs of the customer and its downstream customers (if exist) is build, how it is validated, and how often this filter is published to the routers. [Self-declared][Audited]		
d RI-03.	1. Examine a documented list of the RPKI and IRR maintenance operations that the provider can perform at customer's request on their behalf [Self-declared][Audited]	CP	

MANRS+ control matrix

Question: How can we measure routing security controls?

Starting point: feasibility study in a local testbed

MANRS+ routing security controls

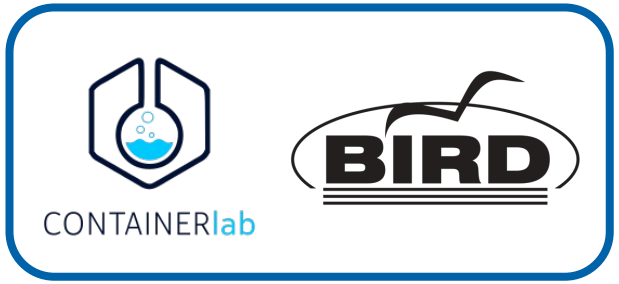
Route Origin Validation

Prefix filtering of customers

Control a set of customer ASes

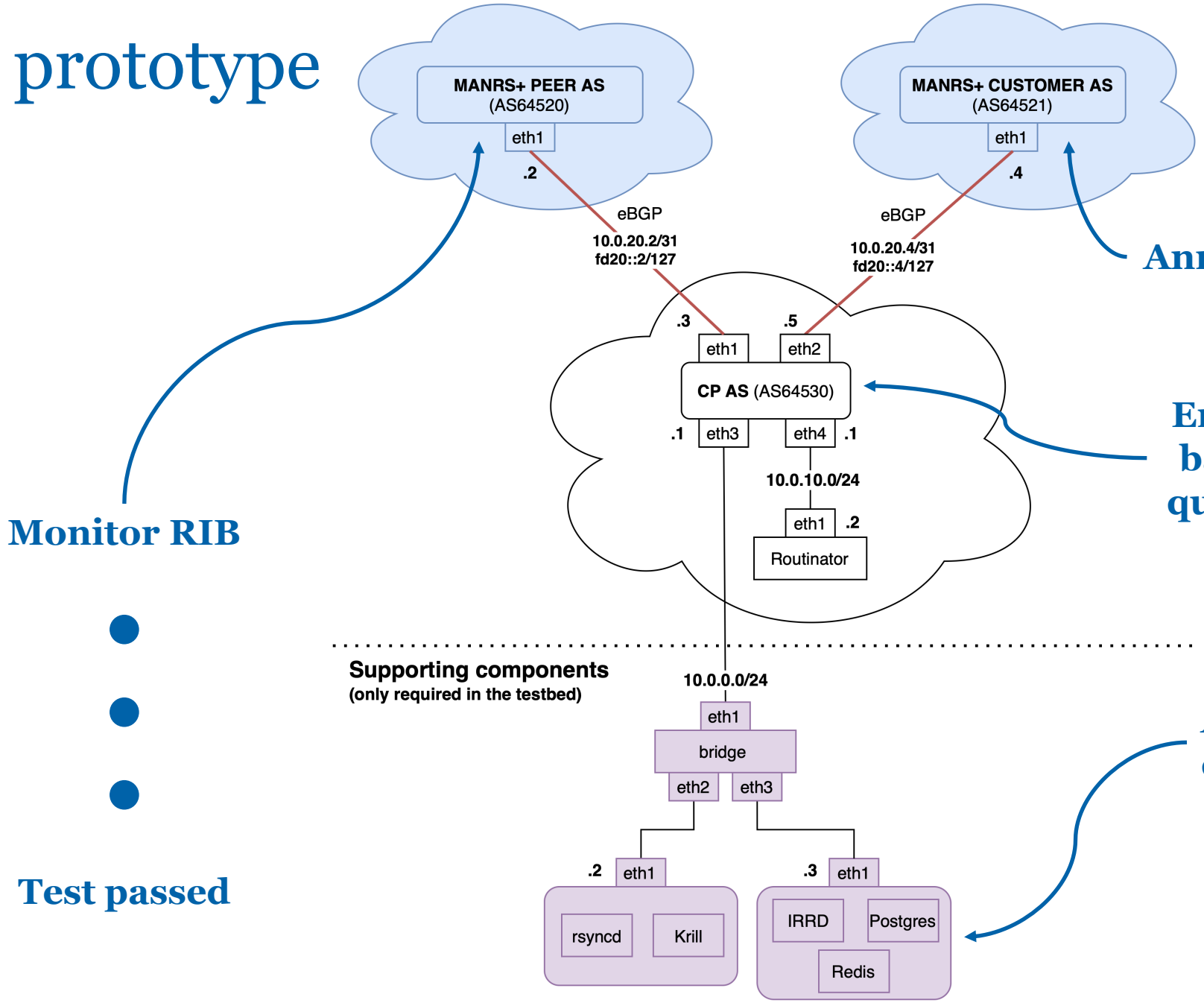
Filtering of bogons

The prototype



SDN LABS

The prototype



Monitor RIB

Announce prefixes to CP AS

Enable import filter based on prefix list queried using bgpq4

Adapt route object to disallow prefix

Test passed

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*

Feedback so far and recommended next steps

- RIPE 91 feedback:
  - Location of test ASes crucial

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

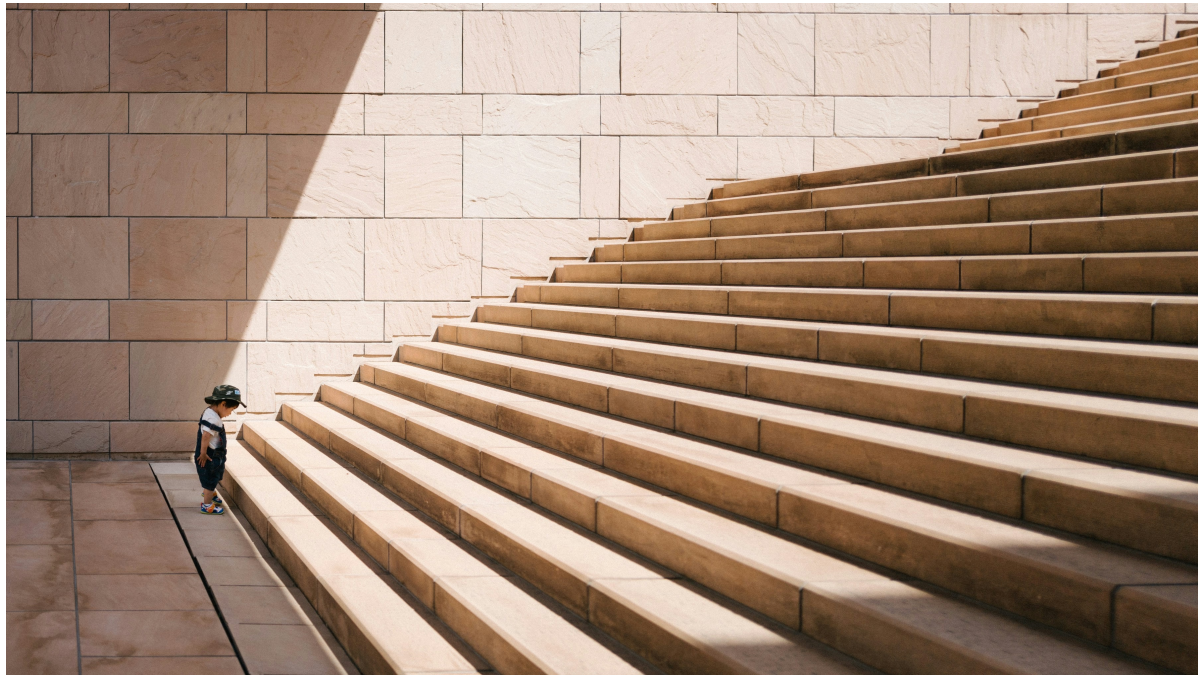


Photo by Jukan Tateisi on Unsplash

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

Are there any questions?

Public report (PDF)