

Routing security for enterprises: secure your supply chain

Is your connectivity provider a threat vector or the first line of defense?

Andrei Robachevsky <arobachevsky@globalcyberalliance.org>



37th Annual FIRST Conference



Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats. Otherwise - they are part of the problem.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can't charge extra for it.

A secure routing system benefits all. But even if you do everything right, your security is still in the hands of other networks.

This is a collective action problem.



A collaborative approach: Mutually Agreed Norms for Routing Security (MANRS)

An undisputed minimum security baseline – the norm.

- Defined through MANRS Actions

Demonstrated commitment by the participants

- Measured by the Observatory and published on <https://www.manrs.org>

Two pillars

An undisputed minimum security baseline – the norm.

- Defined through MANRS Actions

Demonstrated commitment by the participants

- Measured by the Observatory and published on <https://www.manrs.org>



MANRS Actions for Network Operators (2014)

Action 1

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Action 2

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Action 3

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible, up-to-date contact information in common routing databases

Action 4

Routing Information

Facilitate validation of routing announcements on a global scale

Publish your data so others can validate

MANRS Programs



Network
Operators (2014)



Internet Exchange Points (2018)



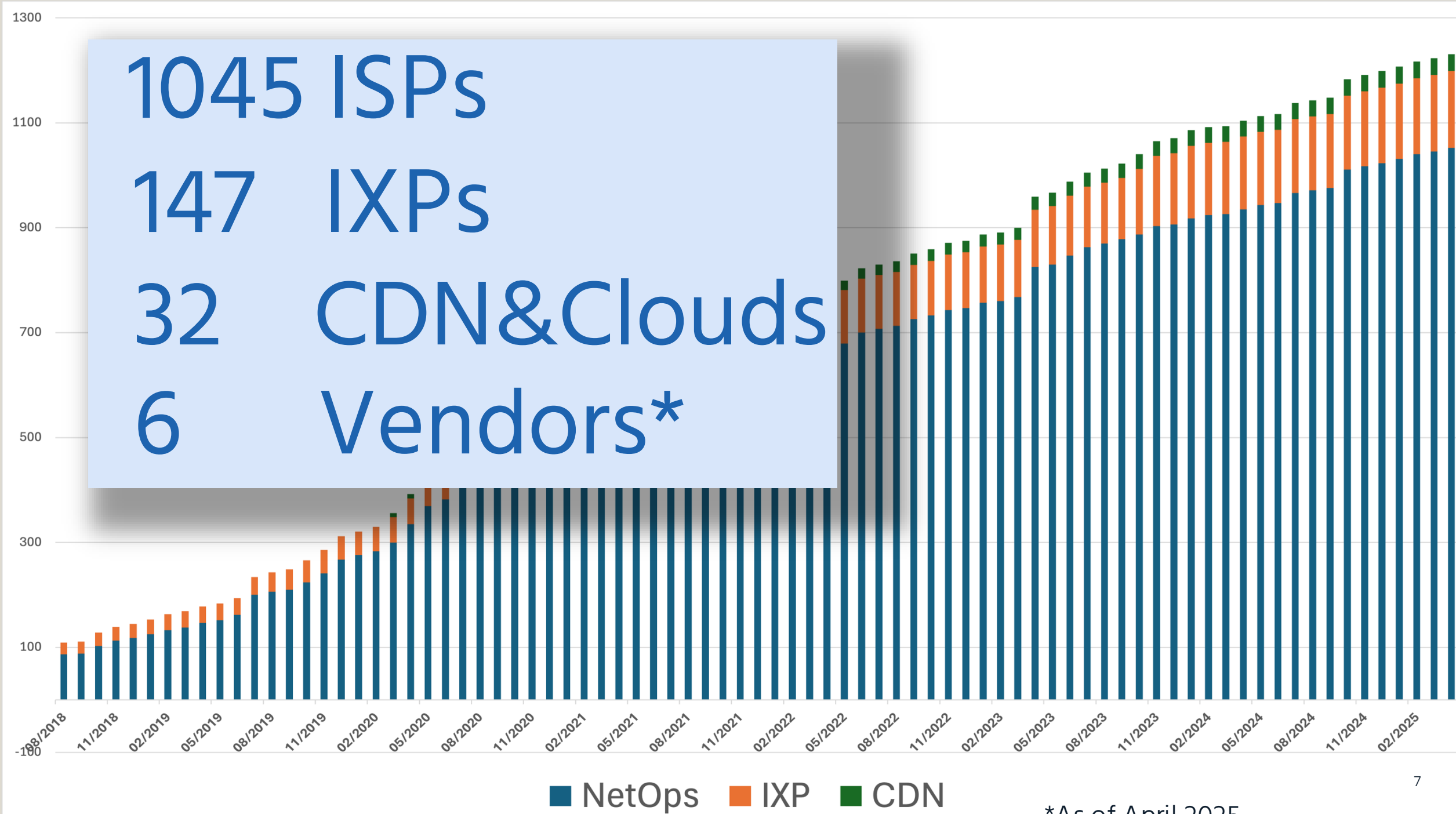
Content Delivery Networks (CDNs)
and Cloud Providers (2020)



Network Equipment Vendors (2021)



1045 ISPs
147 IXPs
32 CDN&Clouds
6 Vendors*



*As of April 2025

10 years of community action

Key factors:

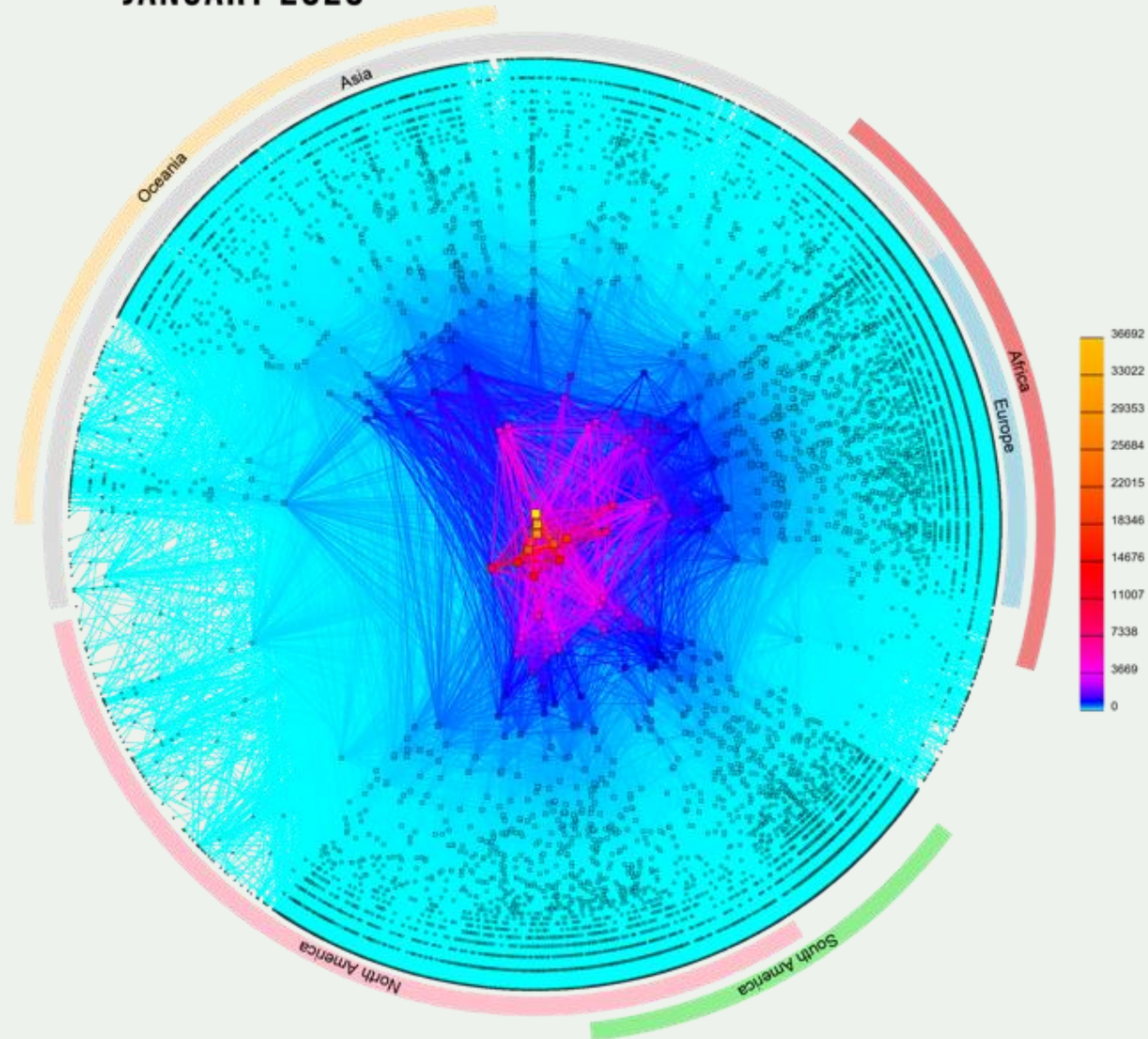
- **Uptake:** with more than 1,200 participants from across the globe
- **Diversity:** from one original program to four
- **Impact:** an industry-driven reference for operators and policy-makers
- **Objectivity:** compliance is effectively tracked through the MANRS Observatory

The Internet Society launched the MANRS project in 2014. After nine years of providing the MANRS secretariat, they partnered with the Global Cyber Alliance to take on that role as of January 2024.

The MANRS (and routing security) business case

- **Protecting own network** by improving security processes and deploying essential controls
- **Improving security of the global routing system** (overcoming the collective action problem), because
 - routing security is a sum of all contributions
 - this is a way to promote a new baseline
 - a community has gravity to attract others
- **Gaining competitive advantage** by responding to **customer demands?**

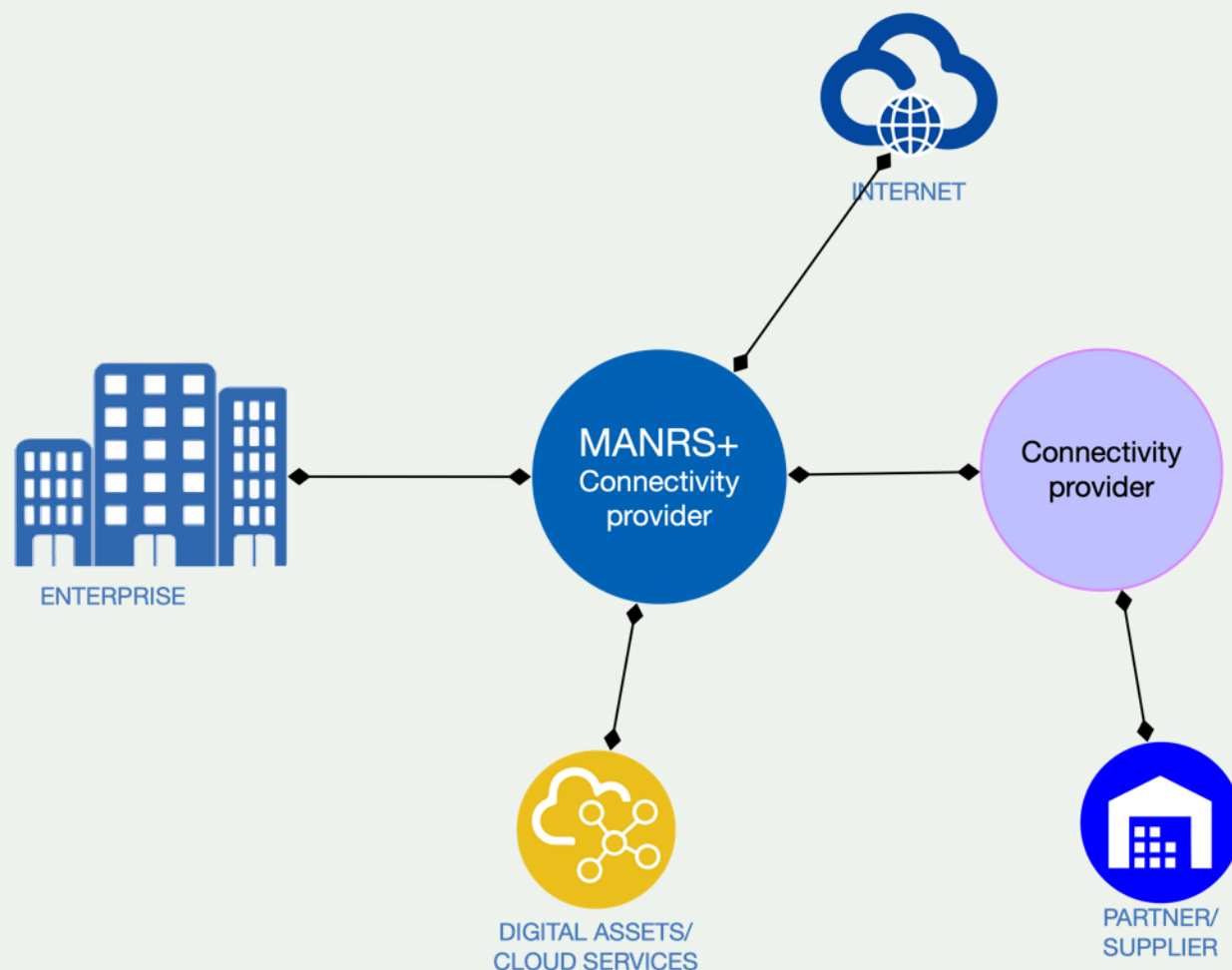
CAIDA'S IPV4 AS CORE GRAPH JANUARY 2020



COPYRIGHT © 2020 UC REGENTS

<https://www.caida.org/>

Traffic security for enterprises – a smaller Internet

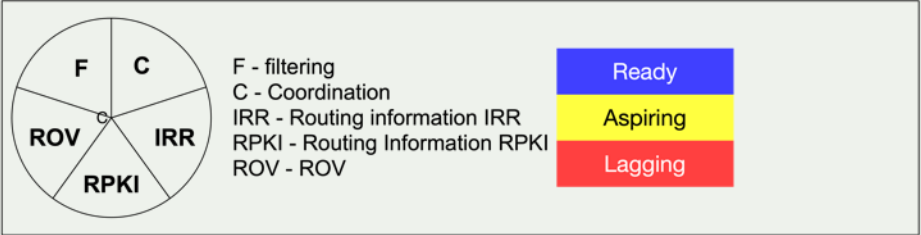
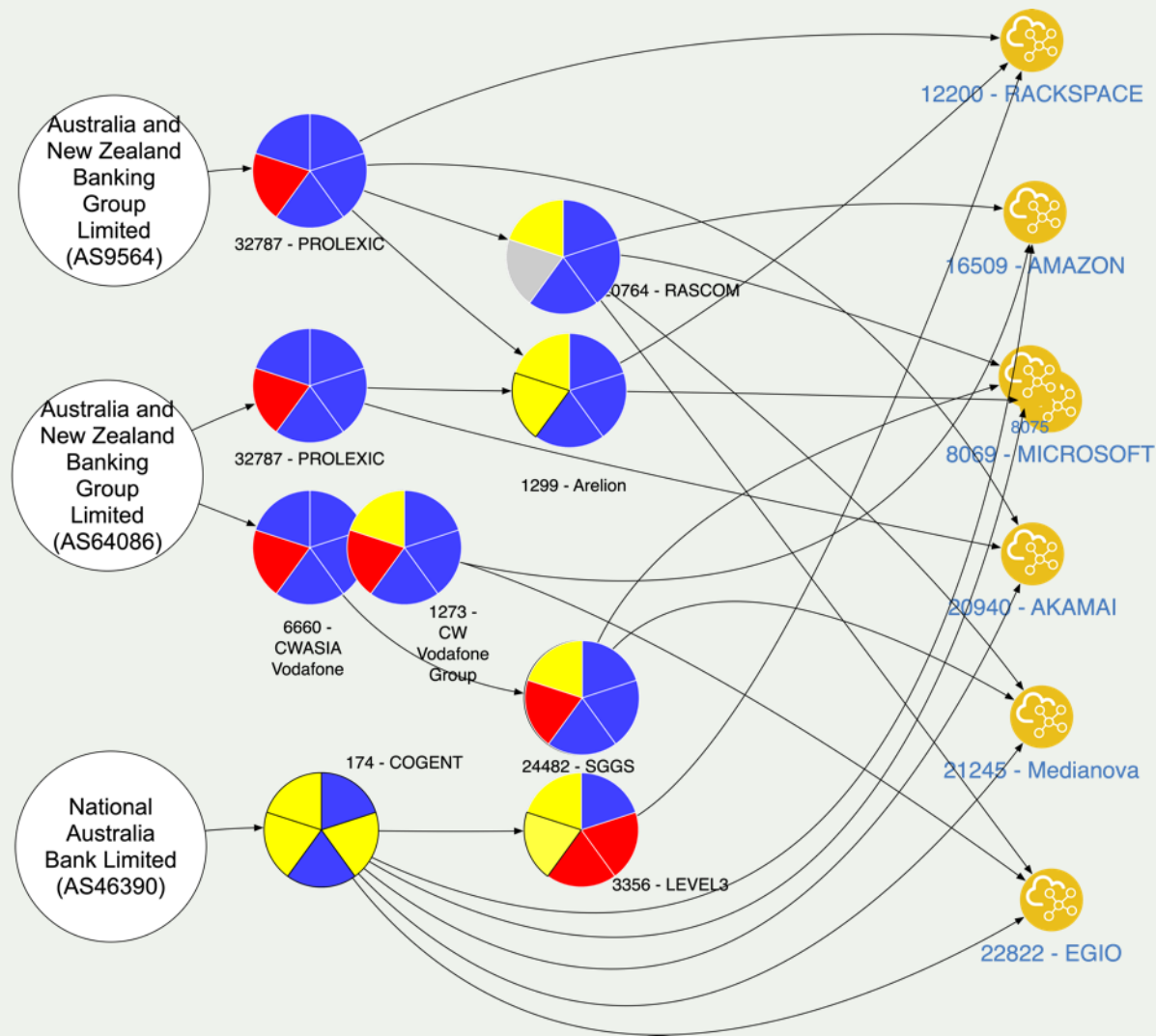


Enterprise's connectivity provider is the first line of defense against routing incidents.

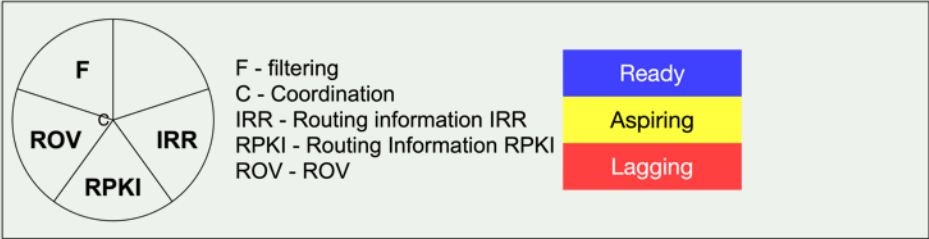
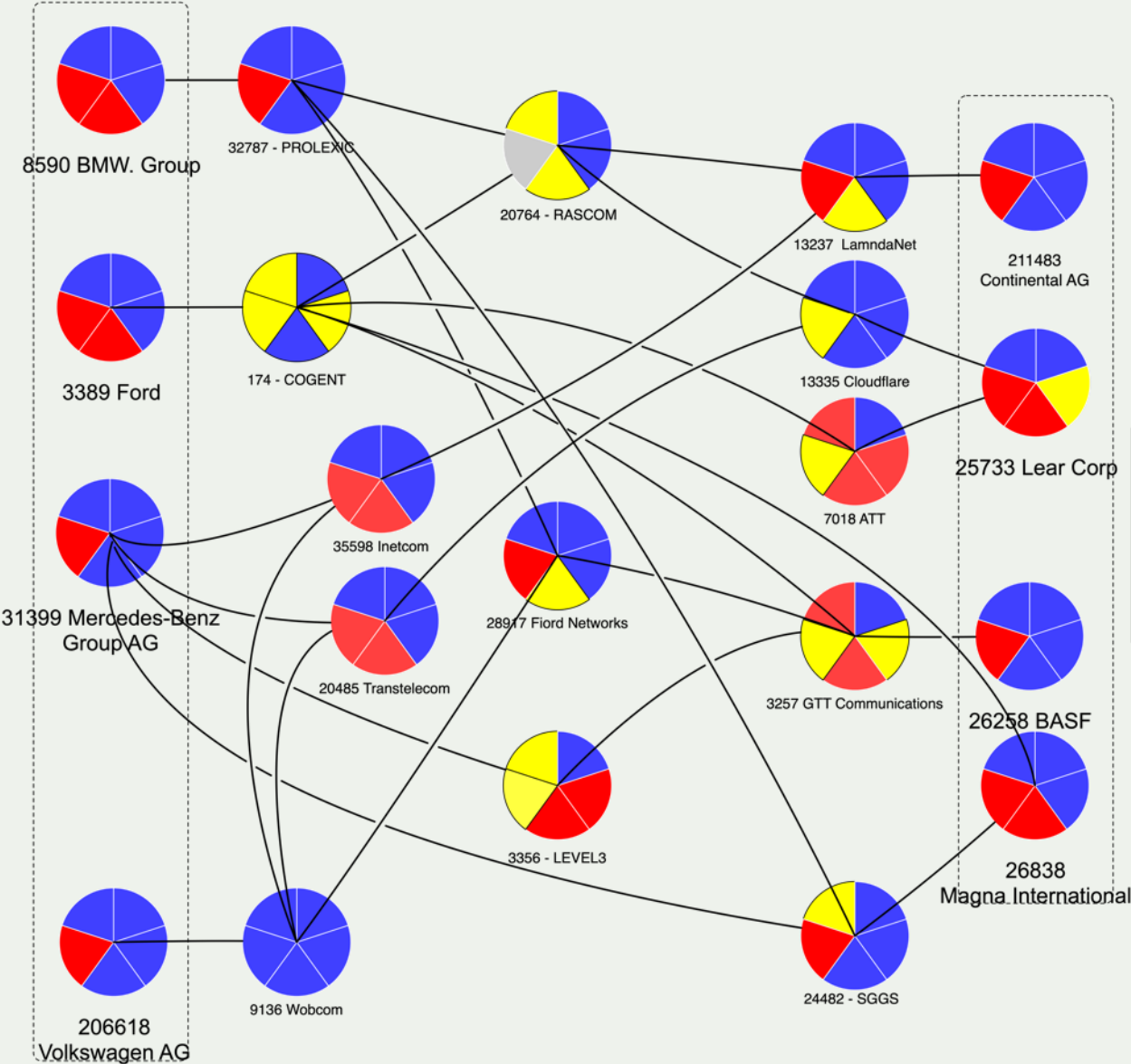
Enterprise can reduce risk by implementing the MANRS actions.

A strong and reliable tie with the connectivity provider(s) can achieve much more – secure the company supply chain.

Supply chain: AU banking



Supply chain: Automotive (B2B)



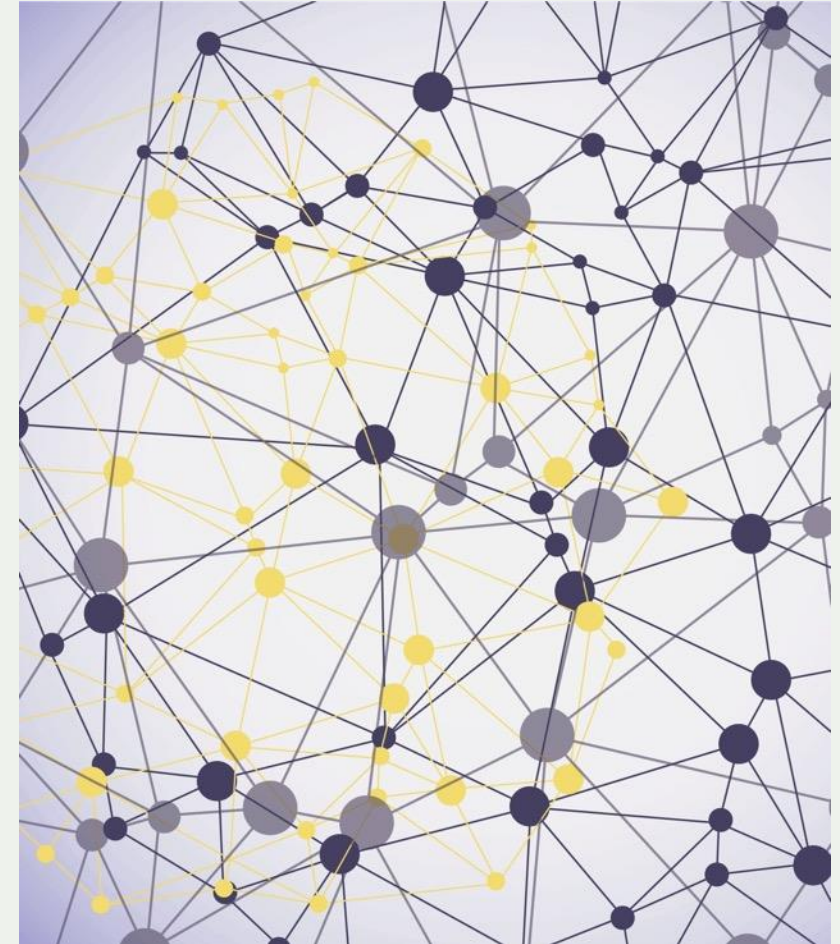
Routing security as part of supply chain security

85% of all ASes are origin-only networks. They fully depend on their connectivity provider for accessing their external digital assets and the Internet.

However, origin-only networks, mostly “enterprises” can contribute to a better routing security by:

1. Enterprises **implementing** routing security best practices in their network infrastructure.
2. Enterprises **demanding** proper routing security controls from their connectivity and cloud providers.

Is your connectivity or cloud provider the first line of defense, or the weakest link?

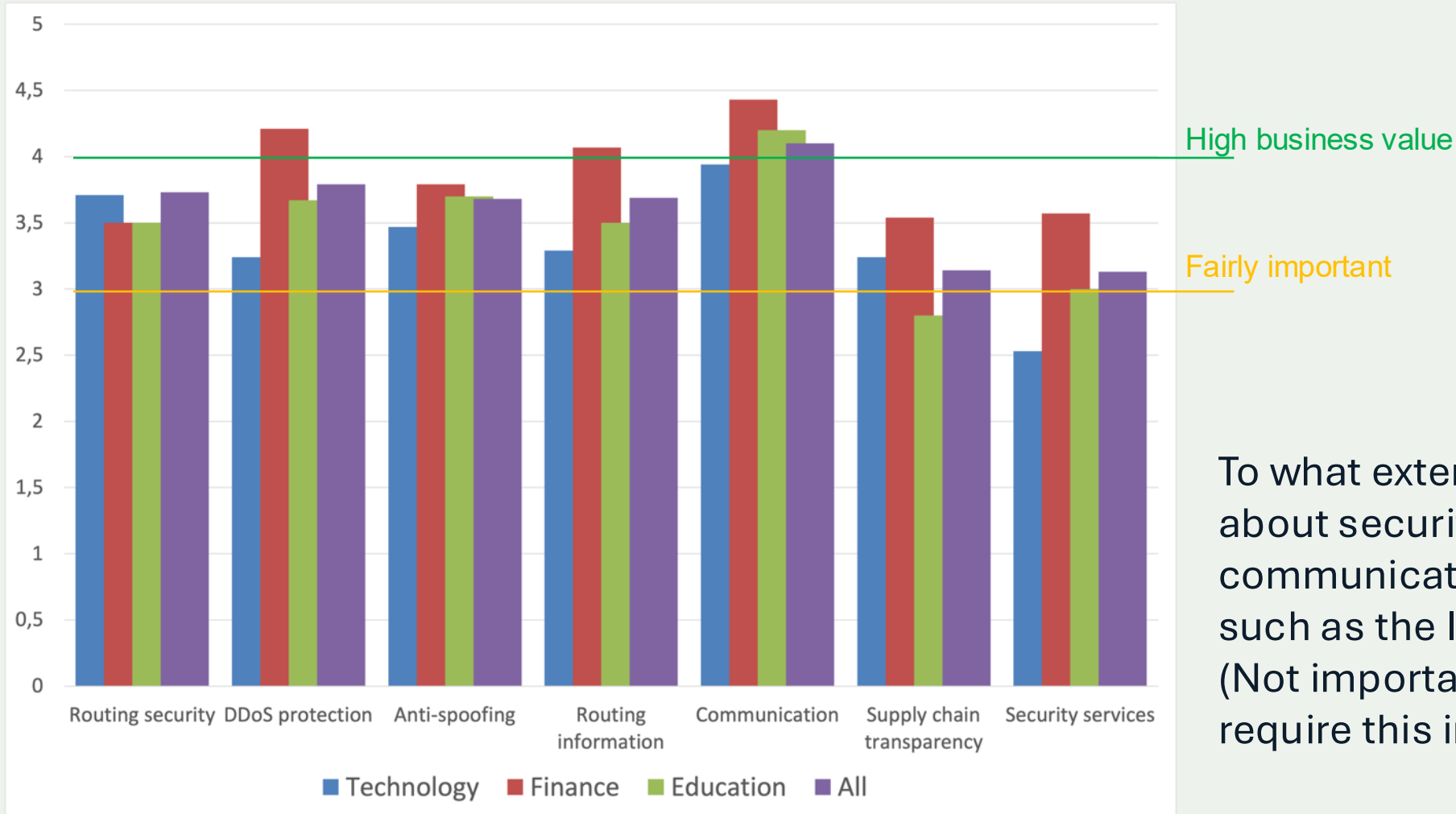


MANRS+

- A framework for routing security, essential part of supply chain security
- Focus on the demands of enterprise customers in various industry sectors
 - *Extended set of requirements, covering a broader set of risks related to routing and traffic security*
- Conditioned to be included in/referenced from common infosec frameworks
 - *Stronger and more detailed requirements enforcing best practices in traffic security*
 - *High level of assurance of conformance. This includes more profound technical audit and process audit.*
 - *Developed in an transparent and inclusive manner – Standard Development Process*



Does traffic security matter to enterprises?



To what extent enterprise care about security of the global communication infrastructure, such as the Internet? Rating from 1 (Not important) to 5 (Essential, we require this in contracts).

Survey on Traffic security controls, <https://www.manrs.org/2023/08/survey-shows-enterprises-value-routing-security-may-underestimate-their-ability-to-influence-vendors/>

What Should Enterprises Require from their Connectivity Provider?



Routing Security
7 Controls



DDoS Attack Mitigation
4 Controls



Anti-spoofing Protection
2 Controls

Maintaining Routing Info.
3 Controls



Global Communication
1 Control




Security Services
3 Controls



Current status

- Work is done by the MANRS+ WG:
 - <https://manrs.org/about/manrs-working-group/>
 - The WG meets monthly on Zoom, ongoing discussions are on the mailinglist
 - Anyone can join this effort → contact@manrs.org
 - The final draft of the Controls Matrix is ready
 - A self-assessment survey

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)
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 neighbours.	1. Check metrics from the measurement system indicating occurrence of incidents via the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine the validation workflow 3. Examine documentation which includes information about RPKI processes including RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported how often these updates are published to their routers. Ensure that the documented procedures reflect best practices for ROV. [Self-declared][Audited]
Routing Security	IRR Filtering of Direct 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 enterprise customer and its customer cone (if exists) are filtered using a whitelist (allow-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 via the control. Ensure that the metrics are within the defined range. In case these cases have on interfaces that excluded from the requirement, verify that the number of aggregated prefixes exceeds 1000 (discuss)[Measured][Audited] 2. Examine the validation workflow that includes a fallback to prefix list filtering in case cannot be performed (ROA not found). 3. Examine documentation of the process for configuring new customer connections, which includes description of how the direct customer cone prefix lists are generated and applied how they are validated, and how often these prefix lists are published to their routers. Must include templates or description of the automation process used to generate and the prefix lists. [Self-declared][Audited]
Routing Security	Control a set of customer ASes (that can originate announcements)	RS-XX	The CP implements filtering permitting only ASNs for a direct customer and its downstream customers (if exists) 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 via the control. Ensure that the metrics are within the defined range. [Measured][Audited] 2. Examine the validation workflow that includes filtering on origin ASN. 3. Examine documentation of the process for configuring new customer connections, which includes description of how the list of ASNs of the customer and its downstream customer (if exists), how it is validated, and how often this filter is published to their routers. This includes templates or description of the automation process used to generate and apply filter. [Self-declared][Audited]



MANRS+ Self-assessment

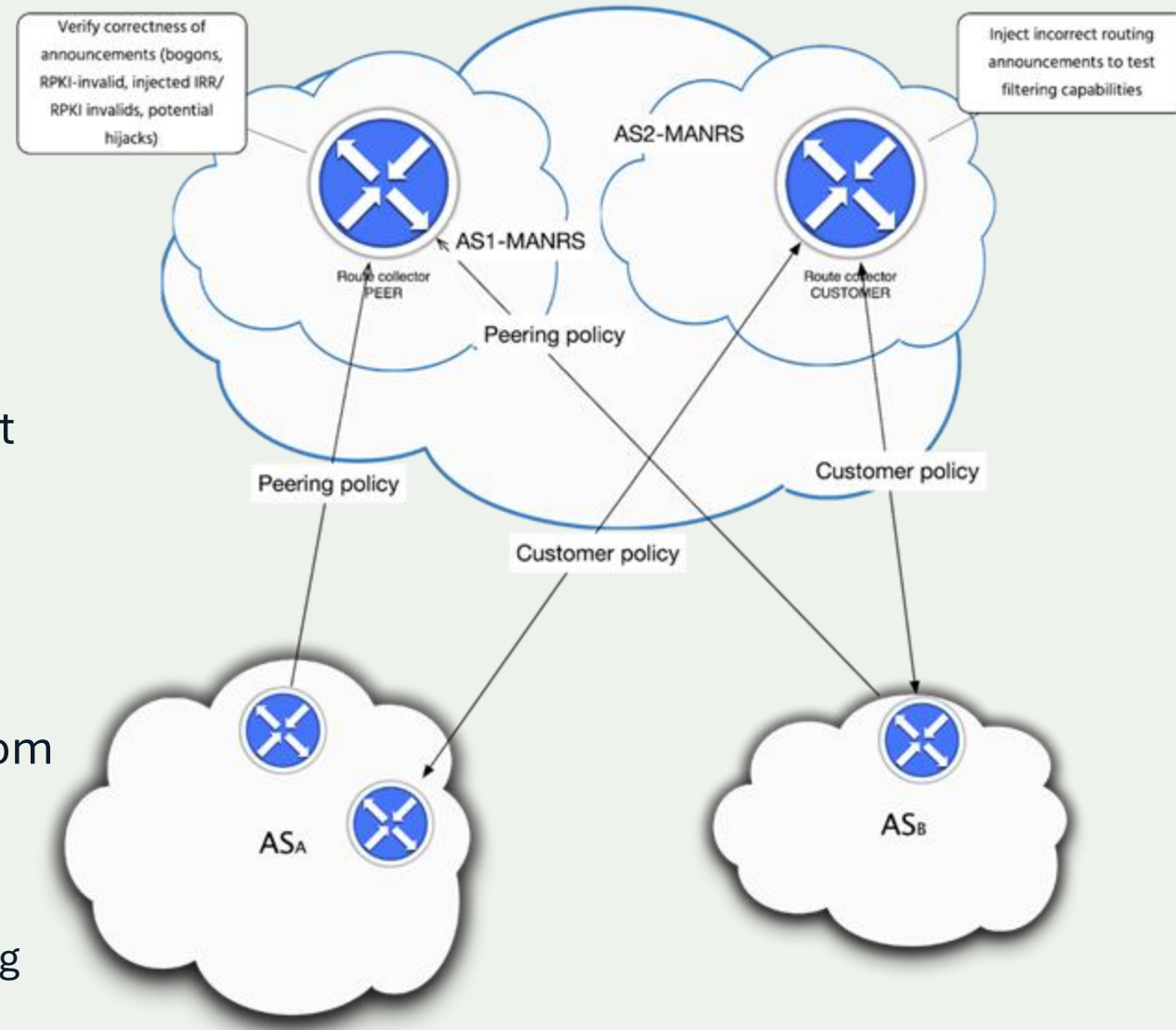
Control Domain: Routing Security

RS-01: RPKI Route Origin Validation
 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 neighbours.

	Not at all	Somewhat/Partially	Completely
RPKI ROV is deployed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Work in progress

- Pilot the extended measurement infrastructure
 - Collaboration with SIDN Labs
- Test-run the audit procedures with a select group of operators
 - Contact us if you are interested → contact@manrs.org
- Raise awareness and generate demand from the customer side
 - Work on inclusion in common infosec frameworks, e.g. M3AAWG Internet Routing Security Profile based on NIST CSF



Thank you.

contact@manrs.org

manrs.org