Strengthening the business case for routing security

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

KLAYswap: $1.9M USD Stolen

BANK INFO SECURITY®

Topics News Training Resources Events Jobs

TRENDING: The Latest From RSAC 2023! • Strategies for CISOs in the Age of Increasing Vulnerabilities •

Blockchain & Cryptocurrency , Cryptocurrency Fraud , Fraud Management & Cybercrime

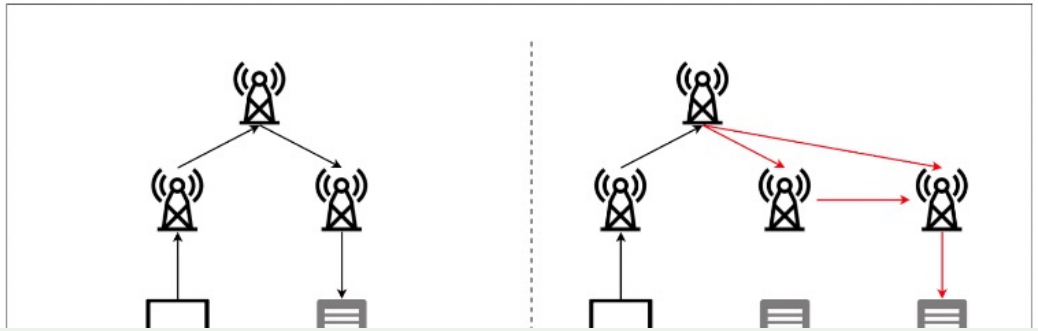
Crypto Exchange KLAYswap Loses $1.9M After BGP Hijack

Hackers Performed Border Gateway Protocol Hack to Conduct Illegal Transactions

Prajeet Nair (@prajeetspeaks) • February 16, 2022

Credit Eligible

Get Permission



What Happened?

Hackers stole ~ USD 1.9M worth of cryptocurrency assets

They didn’t attack KLAYswap directly; they went after a vendor called KakaoTalk, a marketing and tech support service

Attackers used the **Internet routing system** to perform a BGP hijack against KakaoTalk to serve a malicious file and redirect traffic

This attack could have been avoided or mitigated if networks implemented routing security best practices

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)

Provides crucial fixes to reduce the most important routing threats

Two pillars

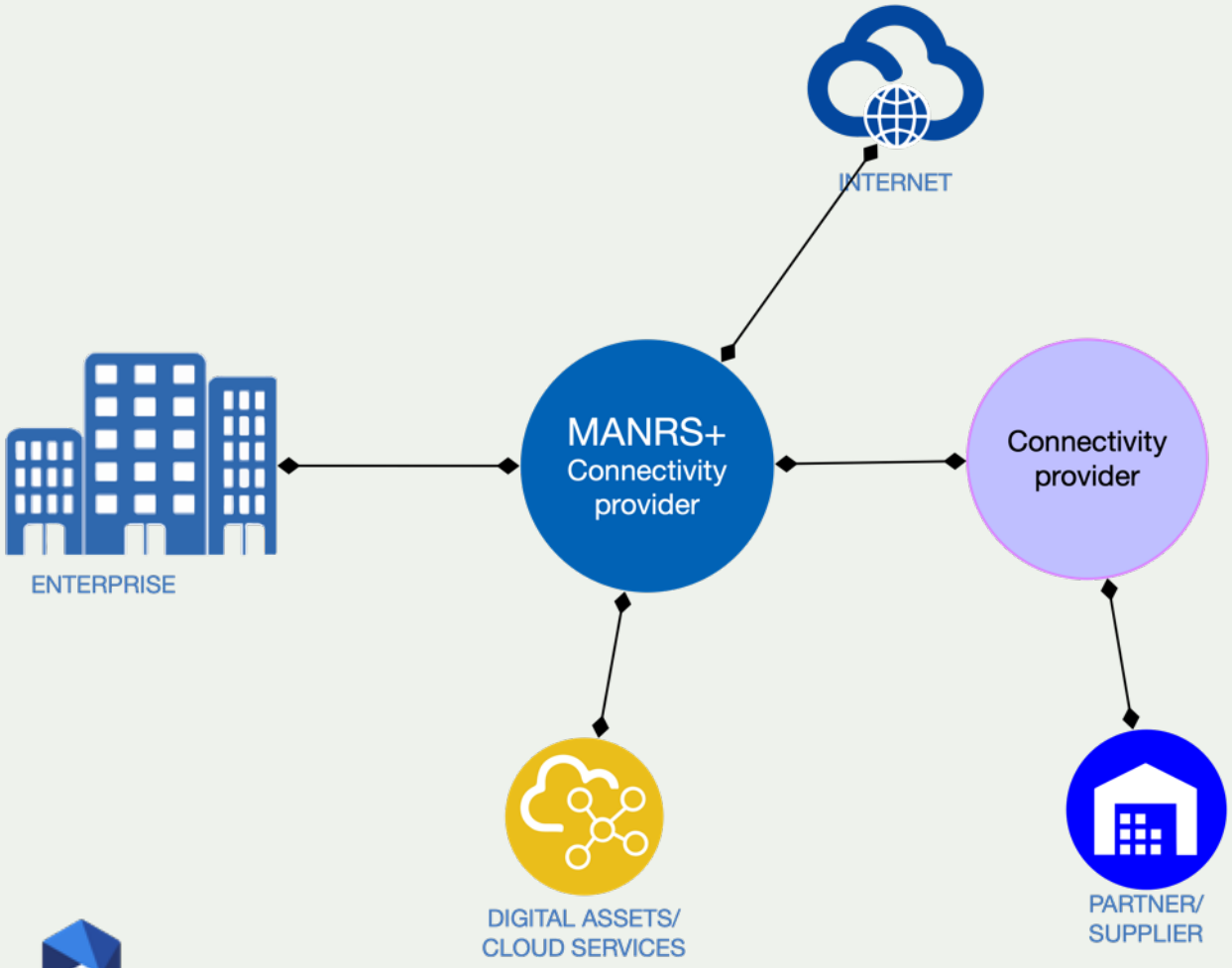
An undisputed minimum security baseline – the norm.

- Defined through MANRS Actions

Demonstrated commitment by the participants

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

Traffic security for enterprises – a smaller Internet



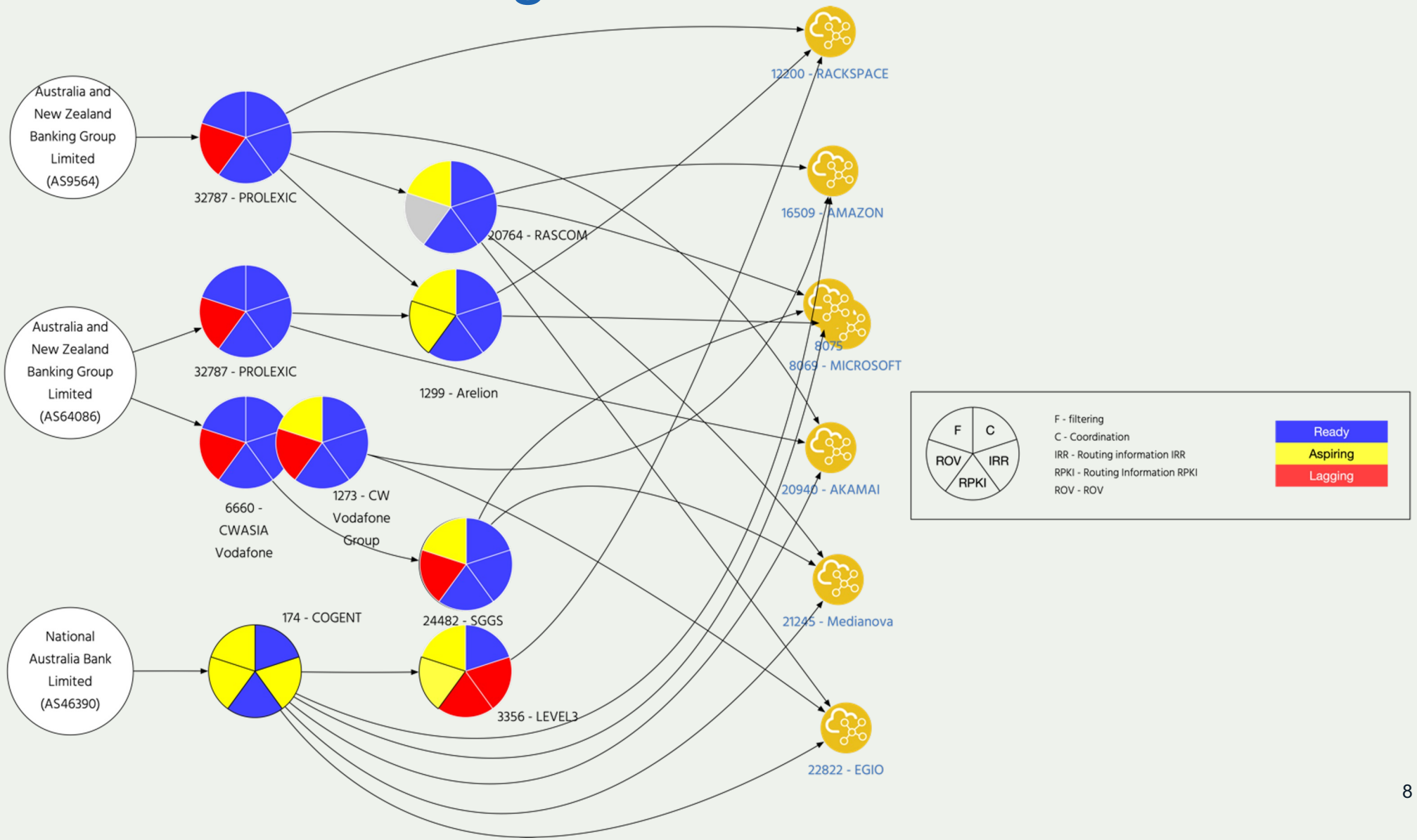
Your connectivity provider is the first line of defense in your supply chain.

You can reduce risk by implementing the MANRS actions.

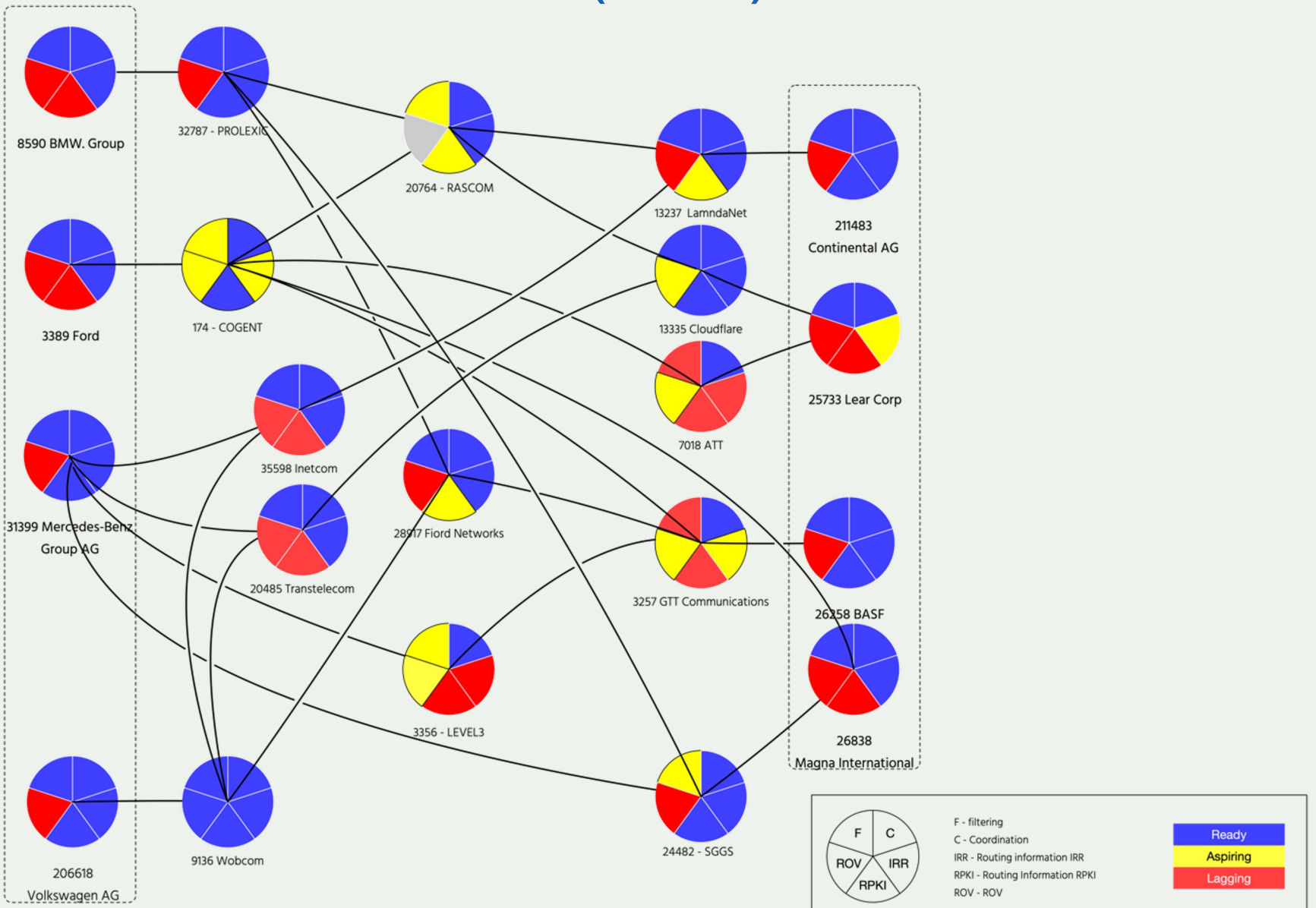
A strong and reliable tie with your connectivity provider(s) can achieve much more.

Is this a business case for routing security?

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 but can also cause a routing incident.

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

1. Enterprises demanding proper routing security controls from their connectivity and cloud providers.

2. Enterprises implementing routing security best practices in your network infrastructure.

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
- 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.
- Extended set of requirements, covering a broader set of risks related to routing and traffic security

What should enterprises require from their connectivity provider? MANRS+ Requirements

Routing Security

DDoS Attack Mitigation

Anti-spoofing Protection

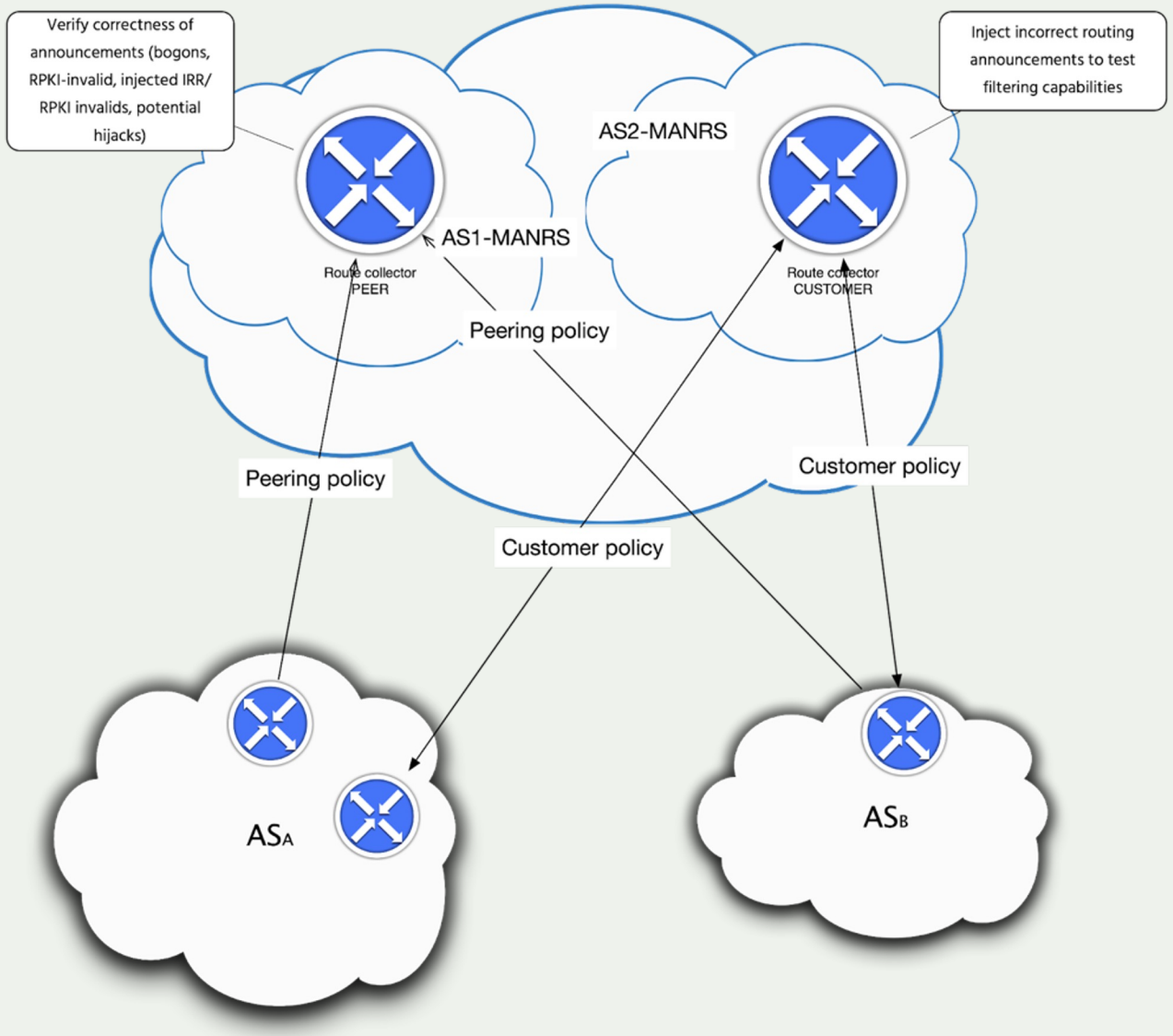
Maintaining Routing Information

Global Communication

Security Services

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 ~~generated internally~~ 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. Examine documentation which includes information about RPKI processes including 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. Ensure that the documented procedures reflect best practices for ROV. [Self-declared][Audited]	Connectivity Provider (CP)	Efficacy of RS-01 depends on the impl controls RI-01 and RI-03 by the Enter Customers (EC).
Routing Security	IRR Filtering of Direct Customers	RS-02	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.	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 of the process for configuring new customer connections, which includes description of how ~~IRR~~ the direct customer cone prefix-lists are generated and applied, how they are validated, ~~including which IRRs and what objects are used,~~ and how often these prefix-lists are published to their routers. This must include templates or description of the automation process used to generate and apply the prefix-lists.[Self-declared][Audited]	CP	Efficacy of RS-02 depends on the impl controls RI-02 and RI-03 by the Enter Customers (EC).
Routing Security	Assistance with RPKI or IRR maintenance for a customer	RS-03	Assist a customer with implementing controls RI-01, RI-02 and RI-03.	1. Examine a 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-04	Route leaks are mitigated by using a peerlock tecnhnique	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-05	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 d. All announcements invalidated by the AS0 TAL (currently APNIC and LACNIC) 2. Examine documentation, which includes information about the technical architecture and processes of maintaining this control. [Self-declared][Audited]	CP	

Enhancing measurements



Current status

End of 2023 – the Concept document and a first draft of the “Control Matrix

For 2024 the WG identified 3 working areas:

- Detailed audit requirements, including descriptions of the audit metrics
- Extended measurement framework
- Measurement infrastructure

The WG meets monthly on Zoom, ongoing discussions are on the mailinglist

Join this effort if you are interested -> contact@manrs.org

Thank you.

contact@manrs.org

manrs.org