23 May 2023

MANRS Update

MANRS Community Meeting #11

Kevin Meynell
MANRS Co-Lead
meynell@isoc.org

Agenda

1) The MANRS Community
2) MANRS Activities in 2023
3) MANRS+
4) Maturing the MANRS documentation and development process
5) MANRS: 2024 and beyond

The MANRS Community

What is the MANRS Community?

MANRS is a collaborative initiative of Internet operators

The MANRS Participants are the Internet operators that meet the requirements of the (currently) 4 MANRS programmes:

- Network Operators – 838 participants (1,038 ASNs) +102 since RIPE 85
- IXPs – 111 participants +6
- CDN/Cloud Providers – 26 participants +4
- Vendors – 6 participants

MANRS Partners are 20 organisations recognised by the MANRS Community as supporting MANRS through promotion, training, resourcing and/or in other ways

MANRS Steering Committee

The Internet Society has developed and supported the MANRS initiative, which has grown quickly and also gained credibility outside of the operator community

MANRS has become bigger than what ISOC staff can support alone

Increasing number of decisions also need to be made :

- Auditing questions as they arise
- How to strengthen the existing MANRS Actions
- Development of ongoing MANRS conformance criteria
- How to handle participants failing to meet the necessary criteria for MANRS conformance
- Development of new programmes
- Revenue

Aim is a self-regulating community – see https://www.manrs.org/about/governance/community-charter/

MANRS Steering Committee Membership

Warrick Mitchell (AARNet) – Chair, until 31 Oct 2024
Andrew Gallo (GWU) – Deputy-Chair, until 31 Oct 2024
Melchior Aelmans (Juniper) - until 31 Oct 2025
Musa Steven Honlue (APNIC) – until 31 Oct 2025
Tony Tauber (Comcast) – until 31 Oct 2025
Flavio Luciani (NAMEX) – until 31 Oct 2024
Nick Hilliard (INEX) – until 31 Oct 2023
Arnold Nipper (DE-CIX) – until 31 Oct 2023
Arturo Sevrin (Google) – until 31 Oct 2023

Joe Hall (ISOC) – ex-officio

Next election will be November 2023 – at least 3 positions

MANRS Auditing Officers

Mat Ford (ISOC)
Kevin Meynell (ISOC)
Andrei Robachevsky (ISOC)
Aftab Siddiqui (ISOC)
Ashlyn Witter (ISOC)

MANRS Activities in 2023

MANRS Observatory Developments

A lot of work to improve the MANRS Observatory:

- MANRS Observatory collates data from third-party data sources BGPStream, GRIP, CIDR Report, RIR databases, PeeringDB, and CAIDA Spoofer
- BGPStream is no longer actively maintained
- Started to use GRIP (Global Routing Intelligence Platform) but this tends to generate false positives so needs improvements to tune and improve accuracy
- Administrative bogons are a significant issue that are being addressed
- More automated processing of MANRS applications to improve response times
- Self-management of MANRS Observatory accounts

Monthly Reports

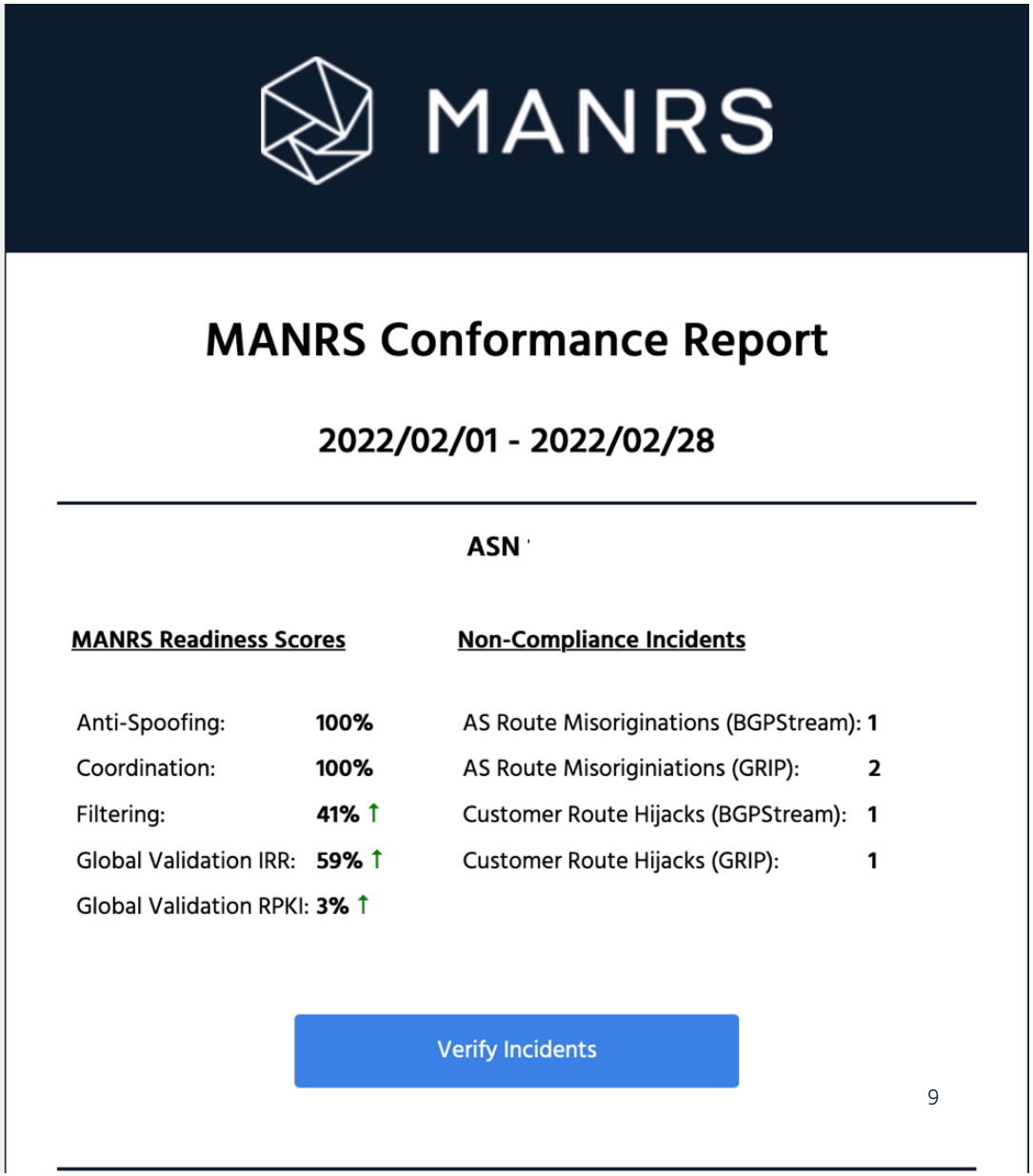
Sent to all MANRS Network Operators

Validate incident data -> tune down false positives

Raise awareness of network conformance status

Use as a regular communication channel (e.g. verify Action 3 contacts)

Can be sent to primary + any secondary contacts



MANRS

MANRS Conformance Report

2022/02/01 - 2022/02/28

ASN

MANRS Readiness Scores		Non-Compliance Incidents	
Anti-Spoofing:	**100%**	AS Route Misoriginations (BGPStream):	**1**
Coordination:	**100%**	AS Route Misoriginiations (GRIP):	**2**
Filtering:	**41%** ↑	Customer Route Hijacks (BGPStream):	**1**
Global Validation IRR:	**59%** ↑	Customer Route Hijacks (GRIP):	**1**
Global Validation RPKI:	**3%** ↑		

Verify Incidents

MANRS Observatory API

MANRS Observatory data now available via REST-based API

Requires Observatory account:

- **MANRS Participants** get access to all MANRS scores + detailed info on own ASN(s)
- **MANRS Partners** get access to selected ASN(s)
- **API-only users** get access to all public data

How to access API:

- Go to your Observatory profile (top-right icon)
- Click button to generate API key
- API documentation

MANRS

Publishing MANRS Readiness Scores

Network operators across the globe have already committed to the MANRS initiative and implemented the Actions defined in the MANRS document.

Search Participants: Internet2 | Show 10 entries | Download CSV

Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation
Internet2	US	11164, 11537, 13436, 55038, 396450, 396955, 396961	✓	✓	✓	✓
Organization Name	**Areas Served**	**ASNs**	**Action 1 Filtering**	**Action 2 Anti-Spoofing**	**Action 3 Coordination**	**Action 4 Global Validation**

MANRS

Deployment Plan, Stage 1

- Publish Actions 2, 3, 4IRR and 4RPKI in first instance:
  - Action 1 data is not accurate enough yet – BGPstream, GRIP, admin bogons
- Participants are **opt-in** by default. They can opt-out by requesting this from the MANRS Secretariat (not through the portal) – contact@manrs.org
- The scores are monthly readiness scores from the past month
- Will be 7-day delay in publishing so MANRS participants can review
- There will be an appeal process based on the mechanism for reporting FPs.
- Deploy beginning **July 2023** with a notice to the MANRS community

MANRS Readiness Scores

Column sorting removed from ASN and Action columns as it doesn't make any sense with mixed or multiple values.

Organization Name ↕	Date Approved ↕	Areas Served ↕	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Completeness		
							IRR	RPKI	
Bornaryn Trading	23rd Mar 2021	AU	12345, 5432	✔	100%	100%	100%	100%	Opted in
Boonta Brand	4th Mar 2022	KH	34552	✔	✔	✔	✔		Opted out
Coronet Ion Works	17th Jun 2020	PR	785674, 234		100%	100%	100%	100%	Opted in
Dynamet Corporation	26th Jan 2022	CR	442245		85%	0%	100%	100%	Opted in
Multycorp	3rd Oct 2021	BR	86745, 4353	✔		✔	✔		Opted out
Outer Rim Supply Co.	6th Dec 2022	DE	8093	✔	No Data	100%	100%	100%	Opted in
Sienar Fleet Technologies	13th Sep 2021	NG	30285	✔	No Data	100%	35%	100%	Opted in
Twin Suns	11th Oct 2021	NP	5628	✔	✔	✔	✔		Opted out
Voorson	14th Apr 2022	ZA	10456			✔	✔		Opted out
Wickstrom	21st Aug 2021	NL	5526, 8765	✔	81%	100%	100%	100%	Opted in
Zikon	29th Nov 2022	CL, US	12003	✔	90%	0%	100%	100%	Opted in
Organization Name ↕	Date Approved ↕	Areas Served ↕	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	IRR	RPKI	
							Action 4 Routing Completeness		

MANRS

Deployment Plan, Stage 2

- Implement filtering of false positives in GRIP data
  - Estimate that >80% of FPs are filtered out
- Publish scores of Action 1 on the MANRS website
  - Implement appeal process allowing participants to flag potential false positives in the reported incidents for auditor's review. Auditors can clear an incident or decline.
  - Participants are given a week to review their scores and underlying data and report inconsistencies.
- Considering averaging scores over extended periods of time (e.g. 3 months)
  - Make it consistent with the MANRS Observatory

Addressing the bogon problem

- An administrative bogon (a MANRS-defined term) is a number resource legitimately assigned to an operator, but which has been marked reserved by a RIR for administrative reasons – typically loss of contact or unpaid bill
- Normally marked bogon for a short period and thereafter reverts to assigned
- RIRs do not publicly distinguish between different types of bogons
- RIRS policies on marking number resources bogon are all different and not published
- Admin bogons constitute 80% of all bogons (and 40% of all route incidents)
- Causing significant problems with measuring route incidents and therefore conformance with routing security best practice

How do we solve the problem?

We need to exclude administrative bogons from routing conformance measurement:

- Makes accurate measurement more difficult
- Reduces routing security assurances (e.g. MANRS Action 1)
- Makes ROV and dropping of invalid routes more problematic (technically and legally)
- Optimal solution = support from RIRs to categorise different types of bogon

Progress…

We need to exclude administrative bogons from routing conformance measurement:

- Bogon issue was raised at BCOP Task Force @ RIPE 85
- Communique detailing issue was sent to NRO
- Discussed at NRO Registration Services Coordination Group on 16 April 2023

MANRS Mentors & Ambassadors Program 2023

formerly known as MANRS Ambassadors & Fellows Program

Aims to extend outreach and involve the wider Internet community in routing security

- **Mentors** are individuals well established in the MANRS Community who provide mentorship, guidance, and feedback to others in the routing security community
- **Ambassadors** are emerging leaders who can enthusiastically bring knowledge and skills about routing security to their communities
- **Tracks:**
  - **Training** – Conduct online tutorials and workshops; help improve existing contents and labs.
  - **Research** – Collect and analyze relevant information on routing incidents; collect feedback from the community.
  - **Policy** – Review documents targeting issues that can be addressed through MANRS actions; help improve existing policy documents for MANRS.

MANRS Mentors & Ambassadors 2023

Training Ambassadors

Sergio Hernández Torres (Ireland)
Sandra Munoz (Mexico)
Anand Raje (India)

Training Mentor

Erika Vega (Colombia)

Policy Ambassadors

Dessalegn Yehuala (Ethopia)
Hernan Moguilevsky (Chile)
Mujtaba Hussain (Pakistan)

Policy Mentor

Harish Chowdhary (India)

Research Ambassadors

Thomas Holterbach (France)
Adefoulou Jediel (Benin)
Nicolas Boettcher (Chile)

Research Mentor

Tijay Chung (USA)

Training

- Capacity building is an important part of MANRS
  - Internet Society moderated courses (https://www.isoc.org/learning/manrs/)
  - Self-paced online tutorials (https://www.manrs.org/resources/training/tutorials/)
  - Hands-on workshops (both directly and via our Mentors and Ambassadors Program)
- Training labs for network engineers and administrators to learn how to configure routing security features
- Implementation Guides provide step-by-step instructions to implement MANRS Actions (see https://www.manrs.org/netops/guide/)
- 26 training workshops (MANRS staff and M&A) in 2022– 2,800 trainees (includes virtual)

Policymaker Engagement

- The global routing system is increasingly being recognized as a critical component of the Internet and routing security is therefore increasingly gaining the attention of policymakers
- MANRS is often referenced by government agencies and has provided input to governmental inquiries (e.g. FCC Notice of Inquiry on Secure Internet Routing)
- Our standpoint is that industry-led best practices are the most appropriate way of improving routing security
- MANRS will continue to monitor and provide input where appropriate to regulatory-related developments as these happen

MANRS+:
Is your connectivity provider a threat vector or a first line of defense?

Focus on enterprises/customers

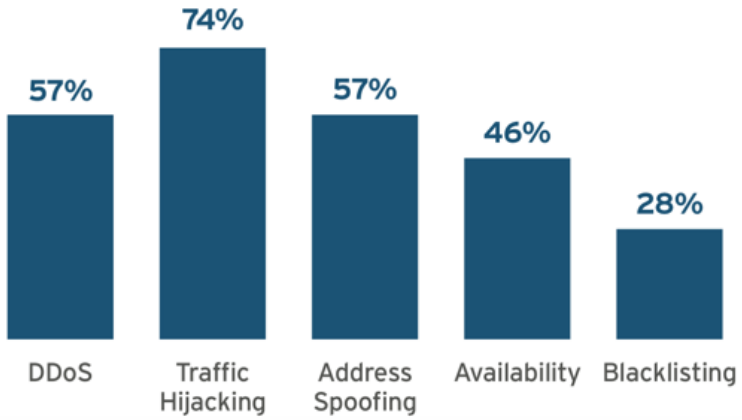
Organization's connectivity provider is the first line of defense. It is part of organization's supply chain security.

In the context of Internet routing a single organization can mitigate some of the risks by a strong security posture (e.g. by implementing the MANRS baseline). A strong and reliable tie with its connectivity provider(s) can achieve much more.

What are the requirements for the connectivity provider?

Figure 1: Internet Security Concerns

Source: 451 Research study: MANRS Perception & Action, July, 2017



MANRS+

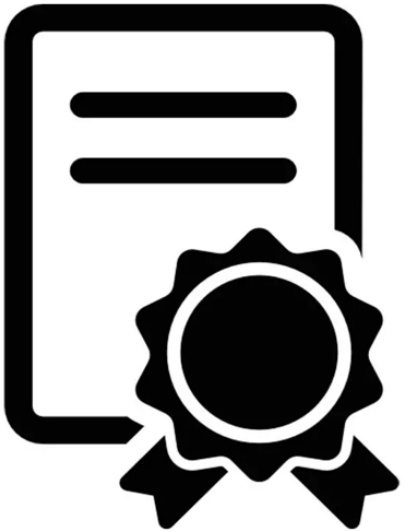
A second, elevated tier of MANRS participation for network operators that comply with more stringent requirements and auditing.

Work with industry partners to increase demand for security from their connectivity providers.

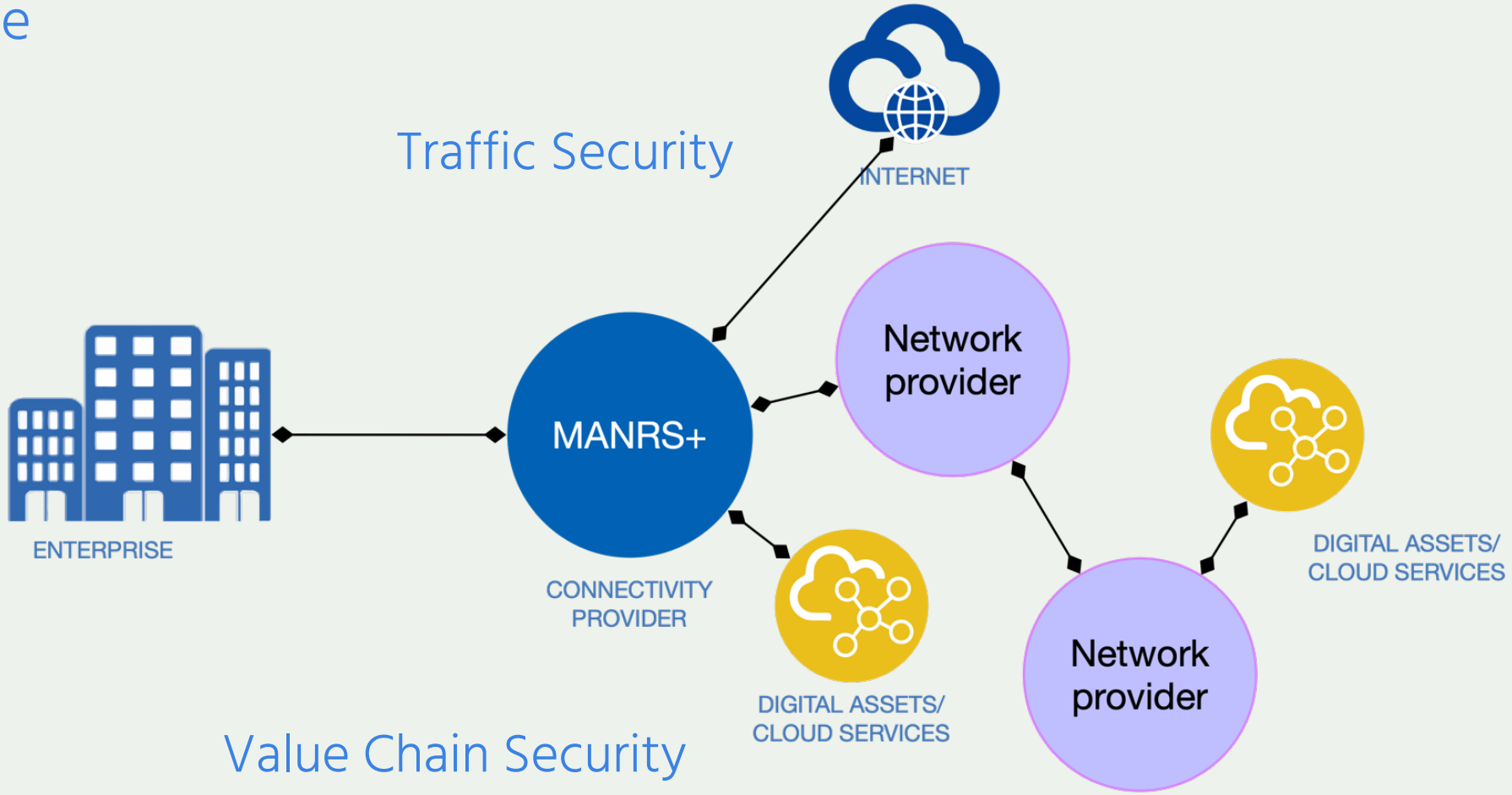
Connectivity Providers and their customers setting the requirements of the future quality mark for traffic security with the goal of eventually incorporating it in procurement policies and recommendations.

What does + mean?

- 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
- More focus on the demands of relying parties



A use case


Traffic Security
INTERNET
Network provider
MANRS+
ENTERPRISE
CONNECTIVITY PROVIDER
DIGITAL ASSETS/ CLOUD SERVICES
DIGITAL ASSETS/ CLOUD SERVICES
Network provider
Value Chain Security

Requirements

Path Security - Connectivity provider has detection capabilities and can mitigate the risk that traffic will be hijacked or detoured as a result of a mistake or an attack.

DDoS Attack Protection - Connectivity provider has detection and mitigating capabilities reducing the risk of a (volumetric) DoS attack.

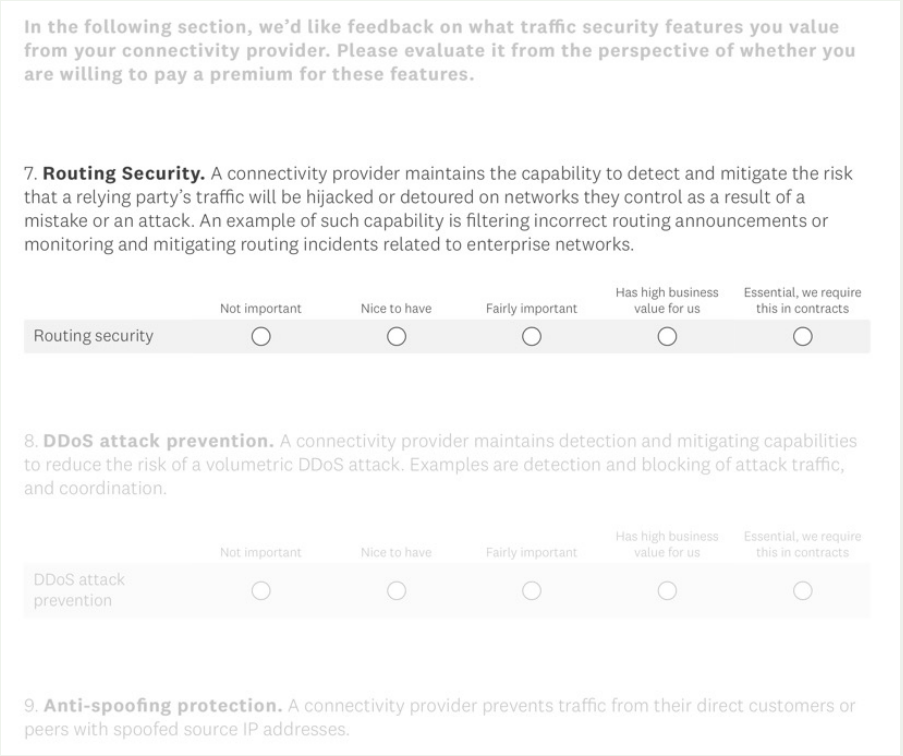
Anti-Spoofing Protection - Connectivity provider detects and prevents traffic from their direct customers or peers with spoofed source IP addresses

Routing Information - Connectivity provider has accessible complete and up-to-date documentation of the intended routing announcements (e.g. RPKI ROAs) and other information on its routing policy (e.g AS-SET) that is necessary for deploying effective security controls by the Network.

A Survey: An enterprise perspective

Evaluate the value proposition of security requirements for the “MANRS+ relying parties” – organizations interested in choosing a connectivity provider with a strong security posture

A typical use case: Is your connectivity provider a threat vector or a first line of defense?



In the following section, we’d like feedback on what traffic security features you value from your connectivity provider. Please evaluate it from the perspective of whether you are willing to pay a premium for these features.

7. **Routing Security.** A connectivity provider maintains the capability to detect and mitigate the risk that a relying party’s traffic will be hijacked or detoured on networks they control as a result of a mistake or an attack. An example of such capability is filtering incorrect routing announcements or monitoring and mitigating routing incidents related to enterprise networks.

	Not important	Nice to have	Fairly important	Has high business value for us	Essential, we require this in contracts
Routing security	○	○	○	○	○

8. **DDoS attack prevention.** A connectivity provider maintains detection and mitigating capabilities to reduce the risk of a volumetric DDoS attack. Examples are detection and blocking of attack traffic, and coordination.

	Not important	Nice to have	Fairly important	Has high business value for us	Essential, we require this in contracts
DDoS attack prevention	○	○	○	○	○

9. **Anti-spoofing protection.** A connectivity provider prevents traffic from their direct customers or peers with spoofed source IP addresses.

Maturing the MANRS documentation and development process

From a BCOP to a recognised standard?

- Documentation policy:
  - Versioning and Archiving Policy
- MANRS Standard Development Process/Policy
  - Org Governance
  - Standard development process and approval
  - Appeal process
- Patent policy

MANRS: 2024 and beyond

MANRS Activities

Essential Services

Application Auditing

Ongoing Conformance Checking

MANRS Observatory hosting and maintenance

Steering Committee support

Desirable Activities

MANRS Observatory development

MANRS Programme development

Training & Knowledge Transfer

Promotion & Outreach

Value-Add Activities

Ambassadors & Fellows Programme

Development of different maturity levels, including quality mark?

Funding and Sustainability

- ISOC has funded MANRS initiative for past 8 years, but now needs your support to continue to grow and strengthen the routing security community
- If you are a MANRS participant such as a network operator, IXP, CDN/Cloud Provider or Vendor, please become an **ISOC Organizational Member** to help us continue to secure the global Internet for everyone
  - Self-selecting tiers: Copper (USD 3.5k), Bronze (USD 10k), Silver (USD 25k), Gold (USD 50k), Platinum (USD 100k)
- We are also looking for industry sponsors interested in supporting the **MANRS Observatory**, **Mentors and Ambassadors Program**, **Training Program**, and community events including the **Routing Security Summit**

Planned Activities

- Engaging government policymakers who are increasingly looking to regulate the global routing system
- Improving the business case for MANRS by implementing the MANRS Actions as industry standards under a recognized standards body
- Developing a certification program and quality mark with enhanced assurances to aid business decisions such as procurement
- MANRS Mentors & Ambassadors program to extend our advocacy, technical capacity building and consultancy, and providing input to policymakers
- Developing economic case for MANRS by analysing costs of routing incidents

Routing Security Summit (formerly RPKI Week)

17-21 Jul 2023 – 1-2 hour online sessions per day

Proposed programme:

- **ROV:** ROV 101 (tutorial), How to deploy ROV (training), ROV case studies, ROV research, Why ROV needs policy backing
- **Routing Security for Governments/Financial Service/Healthcare etc:** MANRS+ etc..
- **Routing Security for Cybersecurity Communities:** CSIRTS, CISOs, etc..
- **Policy:** Threats and opportunities for policy and decision makers
- **Other ideas?**

Join the MANRS Community

Visit https://www.manrs.org

- Fill out the sign-up form with as much detail as possible
- We will create MANRS Observatory account for your network

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the MANRS Actions

MANRS