BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90
	)	

COMMENTS OF INTERNET SOCIETY

Joseph Lorenzo Hall
Distinguished Technologist, Strong Internet

Olaf Kolkman
Principal, Internet Technology, Policy, and Advocacy

Megan Kruse
Director, Partner Engagement and Communications

Ryan Polk
Director, Internet Policy

Andrei Robachevsky
Senior Director, Technology Programmes

Aftab Siddiqui
Senior Manager, Internet Technology, Asia-Pacific

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190
703-439-2120

April 11, 2022

I. Summary

The Internet Society (ISOC)[1] appreciates the opportunity to submit comments in response to the Federal Communication Commission's (FCC or the Commission) Notice of Inquiry (NOI), "Secure Internet Routing."

The technical community has made significant progress over the past few decades in securing Internet technologies, e.g., the secure form of the Hypertext Transport Protocol (HTTP), called HTTPS, is now ubiquitous. However, securing the routing layer of the Internet—which involves technologies that manage and exchange network reachability information via the Border Gateway Protocol (BGP)—is a major area where there has been less success, as routing poses particularly frustrating technical and collective action problems.

The best practices, technical standards, implementations, and the "discipline" of routing security is still a relatively nascent and evolving area—e.g., one of the most important current routing security technologies, called Resource Public Key Infrastructure (RPKI), enjoys only around 35% adoption.[2]

Given the evolution and direction of existing and emerging technologies in routing security, mandates are unlikely to be helpful in securing more networks and more likely to "freeze" aspects of an evolving security ecosystem in unhelpful states. Mandates that require certain

[1] Founded by Internet pioneers, the Internet Society is a non-profit organization dedicated to ensuring the open development, evolution, and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that enable universal access. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

[2] As we discuss later in this comment (see Section VI.4.1.1), this 35% is only in the most basic sense of announcing secure routes (via Route Origin Authorizations (ROAs)), and not the added step of validating those ROAs and dropping invalid routes (which involves setting up infrastructure to perform Route Origin Validation (ROV), which validates route announcements from published ROAs and drops any routes that fail validation or are otherwise invalid).

entities to employ specific routing security measures may seem like a natural solution but are more than likely to have negative consequences for overall security and stability of the Internet. For example, as we explain later in this comment (see Section VI.5), mandates or requirements based on technologies like BGPsec would be impractical and cumbersome, and potentially take momentum away from promising new technologies.

While we do not believe that mandates are the appropriate regulatory solution in this space, we do see areas where policymakers and regulators may have a constructive role in promoting routing security:

- *Incentives:* Grant programs or other efforts to reduce the costs to deploy routing security measures could be very useful for resource-constrained entities, given that costs of employing existing and future routing security measures are nontrivial.
- *Procurement:* Preferential procurement of services from network providers, equipment vendors, and other suppliers that support routing security measures would ensure increased availability of those features in the market.
- *Critical Infrastructure:* Certainly, entities that provide or protect critical national functions and infrastructure should be held to a higher level of network security; routing security is an important but neglected area of critical infrastructure protection.

II. Table of Contents

III. Introduction

The Internet Society thanks the FCC for its interest in this important topic. Below we first provide some general considerations and then respond to specific questions from the NOI.

IV. Key Considerations

The security of the routing system, with its decentralized management and distributed nature, is a shared concern of everyone that values a secure and trustworthy Internet. Routing security requires a *think global, act local* approach where stakeholders use the appropriate tools given their roles and responsibilities in the routing ecosystem to improve the integrity of how data flows around the Internet. Routing security is a classic collective action problem in networked security: any one individual network may not see direct benefits from investing in and employing routing security measures as that benefit is distributed across all networks in the system (see Section VI.4.3). Ultimately, the resulting collective action must be global, such that the vulnerabilities of insecure networks are exceptions rather than the norm.

At its core, the routing system is built on trust among networks. Individual networks make independent decisions while also interoperating as one global Internet using the Border Gateway Protocol (BGP). This structure allows flexibility for network operators to develop network architectures and solutions to best fit the needs of their customers and users. The intertwined nature of these networks contributes to the Internet's resilience, scalability, and ease of adoption. With no single point of failure, the routing system is difficult to break on a global level—if a path fails, a network can simply choose to route traffic around the problem. These qualities have made the Internet successful and enabled its continued growth.

These same attributes also contribute to some of the routing system's challenges. Because BGP was developed when the Internet was a mostly academic endeavor with a small community of

people who all knew each other, it has no built-in mechanism to validate that routing announcements are either legitimate or correct. In today's Internet, this can lead to BGP hijacks, BGP leaks, and IP address spoofing, which in turn can lead to DDoS attacks, traffic surveillance, lost revenue, reputational damage, and more.

There are technical solutions available, and many have become part of best current practice. Their deployment and use are not universal, however, either because network operators are unaware of them, or because operators are unwilling or unable to devote resources to implementing them.

We have seen a shift over the last few years, with technical solutions such as RPKI seeing a significant increase in deployment. There are several efforts underway both to stimulate the deployment of these solutions (e.g., the Mutually Agreed Norms for Routing Security initiative, or MANRS that the Internet Society supports) and develop new technologies to further secure the Internet routing system.

There are opportunities to improve adoption of routing security best practices, including creating positive incentives, building it into government procurement requirements, and working with high-risk sectors, such as critical infrastructure entities, to build up more operational expertise and standard operating procedure that can then be applied to sectors with less inherent risk. With that in mind, it is better to 'nudge' the existing market forces, for instance through generating customer demand, lowering barriers, and developing technologies that make routing security easier to implement when developing networks.

In such a large and complex interdependent system, there are no low-hanging fruit or singular approaches that can easily or comprehensively secure Internet routing. Regulation that prescribes specific solutions is unlikely to be effective, likely to be outdated as the industry evolves, and

may bring unintended consequences. Routing security requires individual network operators to implement and adhere to routing security practices with collective responsibility for the resilience and security of Internet infrastructure in mind.

In such a complex, decentralized global system made up of tens of thousands of individual networks, there is no one 'silver bullet' that will make it secure.

V. A Survey of MANRS participants

The Internet Society supports and facilitates the community of MANRS participants. The MANRS community consists of network operators, Internet exchange operators, content delivery network operators, and network equipment vendors that have pledged to support the MANRS program by taking specific actions to increase the state of routing security.

We surveyed the community of MANRS participants to get specific answers to the questions in the NOI. Details about the survey instrument, the responses received, and data obtained by the survey can be found in the Appendix (Section VIII). It is important to remember that the survey is biased towards stakeholders that have made routing security a priority by becoming MANRS participants and that the survey sample was based on self-selection, in that answering the survey was not compulsory but encouraged.

VI. Specific Responses to Questions from the NOI

We have specific responses to several the questions from the NOI. We mark quotes from the NOI as single-spaced text with a vertical bar on the left margin:

> This is an example of how text in this document appears when quoting the FCC NOI.

VI.1 Scope

> 8. *Scope of Inquiry*. we seek comment on the extent to which Internet Service Providers, public Internet Exchange Providers, and providers of interconnected VoIP service have deployed BGP routers in their networks.

The BGP is the most common *external* routing protocol[3] on the Internet. There are a variety of protocols used to route traffic internally within networks.

This question does not distinguish between *external* and *internal* routing in networks. While BGP is universally used for inter-AS routing, routing inside each individual network can be done using different protocols including MPLS[4] and BGP.[5] General statements about the use of BGP internal to networks cannot be made; there is simply no global visibility into the use of routing protocols internal to networks.

VI.1.1 BGP use inside of networks

> […] Do content delivery networks, and providers of cloud services operate BGP routers in their networks as well?

All autonomous systems (or AS)[6] on the Internet use BGP to build a "roadmap" to forward data from the source to the destination. If a network, regardless of its type—e.g., content delivery networks, and providers of cloud services—needs to have control over how its traffic is being routed, it must participate in the Internet routing system as an independent entity—i.e., as an AS—and, therefore, will need to have BGP routers to exchange routing information using BGP.

---

[3] A *routing protocol* is the way in which a network determines the path a data packet is going to take. To route traffic between networks, most networks use the Border Gateway Protocol (BGP).
[4] *See Multiprotocol Label Switching Architecture* (RFC 3031), INTERNET ENGINEERING TASK FORCE (Jan. 2001), *available at* https://datatracker.ietf.org/doc/html/rfc3031.
[5] *See, e.g.*, Abhashkumar, Anubhavnidhi, Kausik Subramanian, Alexey Andreyev, Hyojeong Kim, Nanda Kishore Salem, Jingyi Yang, Petr Lapukhov, Aditya Akella, & Hongyi Zeng, *Running BGP in Data Centers at Scale*, 65-81 (Apr. 2021), *available at* https://www.usenix.org/system/files/nsdi21-abhashkumar.pdf.
[6] An autonomous system is a group of routing prefixes under a common administration and routing policy.

The fact that all networks on the Internet make autonomous decisions about how to organize their routing makes the Internet itself more resilient. In fact, the decentralized management and distributed routing system is what we have identified as a critical property of the Internet.[7]

VI.1.2 Operators of BGP routers

> […] What other types of entities operate BGP routers? We recognize that there are entities that do not operate BGP routers, but that are otherwise well positioned to support the development and implementation of BGP security practices. (examples provided include regional, national, and local Internet registries, ICANN through its affiliate, Internet Assigned Numbers Authority (IANA).

Entities that may operate BGP routers include:

- *Internet Service Providers* is a broad category that may include broadband access providers and transit providers up to tier-1 networks. Most of them define their own routing policy and operate an AS.
- Many *enterprises* (businesses, universities, etc.) also operate their own AS and, therefore, participate in the Internet inter-domain routing using BGP.
- Some *research initiatives*[8] operate *BGP routers* in a passive mode—only collecting BGP announcements and not providing any traffic forwarding services.
- Some *research initiatives* operate *BGP beacons*[9] which are BGP speakers that announce and withdraw a particular prefix at predetermined time intervals that aid research to, for example, better understanding BGP route propagation and convergence.

---

[7] The Internet Society has worked to articulate a set of five "critical properties" of the Internet as part of our work on the Internet Way of Networking. Please see the Internet Impact Assessment Toolkit and associated materials here: https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/.

[8] *See, e.g.*, *University of Oregon Route Views Project*, ROUTE VIEWS, http://www.routeviews.org/routeviews/; *Routing Information Service*, RIPE NETWORK COORDINATION CENTER, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris.

[9] *See RIS Routing Beacons*, RIPE NETWORK COORDINATION CENTER, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-routing-beacons.

In general, the barrier to become a BGP speaker is low. One must connect to another BGP speaker that will forward their view of Internet routes. The ability to connect and become part of the Internet makes for an accessible infrastructure, what we consider another critical property of the Internet.[10] Secure routing practices of the neighbors to which the new network just connected are crucial for the security and integrity of the routing system.

VI.1.3 Role of Entities

> We seek comment on what role these and other entities, including vendors of BGP routers or other networking equipment, have in supporting the development and implementation of BGP security practices.

Routing security and its deployment depends on many stakeholders in the community:

- Vendors, operators, and technical specialists are involved in the design and standardization of the technologies needed.
- Regional Internet Registries (RIR) are responsible, in collaboration with the network operators, to maintain correct and up-to-date information of Internet number resource allocations i.e., a registry of IP and AS allocations.
- Operators of the Internet Routing Registries. That is, entities that accept descriptions of routing information from network operators and publish those records as part of a registry of Internet routing data called an Internet Routing Registry (IRR).
- Operators of RPKI services issue digital certificates and support the creation of related objects, such as ROAs. They also operate RPKI repositories. Network operators need to act to cryptographically sign certain data that other networks (relying parties) can use to route traffic securely.
- Network operators need to implement routing security measures such as filtering routes based on information in routing registries or validated using RPKI.

[10] INTERNET SOCIETY, *supra* note 7.

- Operators of monitor services that scan the routing system and report vulnerabilities to their customers are observers of the routing system.
- The research community has other observers of the routing system, often looking for systemic issues, trends, or anomalies.
- Vendors (including open-source groups) make available implementations on which network operators can rely to perform these functions.

VI.1.3.1 Threats to Internet Routing

> What threats to Internet routing should the Commission consider within the scope of this inquiry in addition to BGP hijacking? For example, to what extent could BGP security measures prevent pervasive monitoring?

We consider BGP hijacking, route leaks, and address spoofing in scope. For clarity we provide definitions.[11]

A *BGP hijack*, or *route hijack*, is when an attacker disguises itself as another network; it announces network prefixes (ranges of IP addresses) belonging to another network as if those prefixes are theirs. If this false information is accepted by neighboring networks and propagated further using BGP, it distorts the "roadmap" of the Internet. As a result, traffic is forwarded to the attacker instead of its legitimate destination.

Similar to a hijack but often without malicious intent is a BGP leak, or route leak. Many organizations connect to more than one network, or upstream provider, to increase reliability or performance, a practice called multihoming (if one path is not available for whatever reason, they can use the second path). A route leak happens when an organization (often accidentally) announces to one upstream provider that it has a route to a destination through the other upstream provider, regardless of whether this is a desirable path. Route leaks can be accidental or

[11] *See* Kevin Meynell, *What are Routing Incidents? (Part 4)*, MANRS (July 16, 2020), https://www.manrs.org/2020/07/what-are-routing-incidents/.

malicious but most often arise from accidental misconfigurations. Full definitions of various types of route leaks can be found in RFC 7908.[12]

While route hijacks are mostly used as a denial-of-service (DoS) attack[13] or for impersonation attacks, route leaks, while unintentional, can create an opportunity for surveillance, reconnaissance activities, and eavesdropping (also called "machine-in-the-middle") attacks.

Address spoofing is the ability of attackers on a network to successfully send IP packets with a falsified source IP address to a destination in a distant network. It is an important step in what are called reflection-amplification distributed-DoS (DDoS) attacks—where an attacker can flood an unsuspecting computer or network by cleverly misaddressing IP packets. The IP packets are sent to services that respond with relatively big responses, such as the DNS, that then reply to the victim hosts that are reachable at the IP address that was falsified, flooding the victim with traffic and potentially taking it offline.

We have seen evidence of routing attacks in the past that seem to have national security or intelligence-gathering purposes behind them.[14] These often involve path-based-attacks and require both origin authentication (RPKI) and IRR-based filtering in tandem to mitigate (at least until practical technologies for protecting paths are developed, such as ASPA, *See* Section VI.3.1).

---

[12] *See Problem Definition and Classification of BGP Route Leaks* (RFC 7908), INTERNET ENGINEERING TASK FORCE (June 2016), *available at* https://datatracker.ietf.org/doc/html/rfc7908.

[13] *Denial-of-service attack*, WIKIPEDIA, https://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=1080877918 (accessed April 8, 2022).

[14] *See* Anne Edmundson, Roya Ensafi, Nick Feamster, & Jennifer Rexford, *A First Look into Transnational Routing Detours*, 567-568 (Aug. 22, 2016).

VI.2 Measuring BGP Security

9. Measuring BGP Security. We seek comment on whether industry has defined metrics for identifying BGP routing security incidents and for quantifying their scope and impact.

VI.2.1 Tools

To what extent are available tools, such as NIST's RPKI Monitor, Automatic and Real-Time detection and Mitigation System (ARTEMIS), BGPstream, BGPMon, Kentik, and Traceroute, able to rapidly and accurately detect BGP hijacks or router misconfigurations?

Some of the tools listed in the question above are complementary and cannot be used alone for incident detection. All the listed tools require that an operator registers the "intent" behind their routing scheme (i.e., how networks they operate should be announced in the routing system) and can compare that with the actual state of the routing system to detect inconsistencies, which may be routing incidents.

These tools are quite accurate at detecting route hijacks, but route leaks may be more difficult to detect as they require information about feasible paths and interconnections between the networks. The accuracy of detection depends on the distribution of the vantage points from which the state of the global routing system is observed. Some of the interconnections and announcements may simply be invisible to these vantage points and, therefore, cannot be detected. There are known cases that some of the attacks exploiting routing vulnerabilities are conducted in a local IXP environment with limited propagation and, therefore, not visible beyond the networks participating in the IXP.[15]

[15] *See, e.g.*, Florian Streibelt, Franziska Lichtblau, Robert Beverly, Anja Feldmann, Cristel Pelsser, Georgios Smaragdakis, & Randy Bush, *BGP Communities: Even more Worms in the Routing Can*, 279–292 (Oct. 31, 2018)https://doi.org/10.1145/3278532.3278557.

There are commercial services that provide routing incident information, but few publicly available tools[16] can detect routing incidents. One challenge of such systems is a relatively high level of false positives due to lack of information about interconnections and their intent.

Our survey indicates that the most prevalent tools to measure routing incidents are:

Table 1: tools used by MANRS participants to measure routing incidents

MANRS Observatory	55	69.62%
Routeviews	32	40.51%
BGPStream.com	19	24.70%
Kentik	10	13.00%
Artemis	10	13.00%
Qrator	8	10.40%
RIPE Tools	7	9.10%
BPGAlerter	5	6.50%
other	5	6.50%
zabbix	2	2.60%

VI.2.2 The Promises of Artificial Intelligence and Machine learning

> To what extent do these tools distinguish malicious routing changes from accidental ones? Do artificial intelligence and machine learning tools promise advancements in this area?

Distinguishing between malicious and accidental routing incidents is inherently difficult. There may be some benefit in applying machine learning (ML) classifiers and artificial intelligence (AI) based tools to the problem, but in the short term we do not think that they will be more efficient than human investigators relying on observable routing data and communications with affected parties. In addition, making such distinctions is often a problem of attribution and

[16] There are many commercial services which provides route incident information but very few such as Cisco BGPStream (because CAIDA has BGPStream as well and Georgia Tech GRIP) are free/publicly available tools.

judging intent of the potentially malicious party, which can involve investigatory data that is not available to such automated systems, i.e., they will always have certain blind spots.

In an operational environment, attribution will most certainly not be the priority. Routing incidents must be dealt with, whatever the cause, so we hope that any AI or ML tools can aid in filtering and rapid response when an incident seems likely, despite the underlying intent or party responsible.

VI.3 Deployment of BGP Security Measures

> Deployment of BGP Security Measures. We seek comment on the security measures that have been developed and deployed by industry to secure BGP.

VI.3.1 On other standards and practices that address BGP vulnerabilities

> In addition to the measures recommended by CSRIC III and VI (RPKI, MANRS, and applicable IETF Best Common Practice standards), BGPsec, and the NIST practice guide, what other standards, specifications, or best practices have been developed to address potential attacks that exploit BGP vulnerabilities?

A method called "peer-lock" allows networks that directly peer with a specific network to specify additional providers that can also pass traffic to that network. This mechanism is not standardized but is used by some network operators. It provides a reasonable mitigation of route leaks.[17]

A downside of the peer-lock is that it requires manual configuration for each transit provider that supports this feature. A more general proposal, based on RPKI and cryptographic validation, is "Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization" or ASPA.[18] The idea in ASPA is to protect and validate parts of the whole AS-PATH, exposing potential route leaks and hijacks. The proposal

---

[17] *See* Job Snijders, *Practical everyday BGP filtering with AS_PATH filters: Peer Locking* NANOG 67 (June 2016), https://archive.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf.

[18] *See Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization,* INTERNET ENGINEERING TASK FORCE, https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/.

expired last month, and progress has been slow to move it forward, but it seems promising, especially in light of the problems we discuss with BGPsec.

VI.4 Deployment of BGP Security Measures

10 Deployment of BGP Security Measures.

To implement basic routing security measures on the Internet, BGP speakers filter incoming (ingress) and outgoing (egress) routing information (routes) based on route policies, which are also bound by business or other organizational relationships. Today, these routing filters can be based on Internet Routing Registry data (maintained by many big operators and Regional Internet Registries) or based on ROA using RPKI.

It can be hard to pinpoint any one flaw with BGPsec that has resulted in such low adoption. We discuss problems with BGPsec further in Section VI.5, but mention here three: the lack of OS support for BGPsec, the associated computational loads required, and research on limits of adoption. BGPsec implementations are not available in any of the production-ready network operating systems. There is some beta-testing of BGPsec in network operating systems available, but the support is little to non-existent, even though BGPsec was standardized in 2017.[19] Additionally, performing the cryptographic validation required for each route and then also for routing updates on an ongoing basis can be computationally prohibitive. (For example, having to reboot a single router managing a large set of connections could take many minutes to hours to complete the initial cryptographic validation of routes, resulting in potentially crippling

[19] *See BGPsec Protocol Specification* (RFC 8205), INTERNET ENGINEERING TASK FORCE (Sept. 2017), https://datatracker.ietf.org/doc/html/rfc8205.

downtime.) Finally, there is academic research from Lychev et al. that indicates BGPsec could never reach the level of adoption needed to adequately deliver on its security guarantees.[20]

VI.4.1 Actual deployments

We seek comment on the security measures that have been developed and deployed by industry to secure BGP.

When it comes to actual deployment of developed technologies, RPKI is most easily measured. We present some data about deployment of RPKI in Section VI.4.1.1 and then route origin validation deployment based on IRR data and RPKI in Sections VI.4.1.1.2 and VI.4.1.1.3 respectively.

VI.4.1.1 Deployment of RPKI

We can measure RPKI deployment. RPKI is foundational technology needed to prove attestations of address use by autonomous networks. As mentioned above, a ROA is a cryptographically signed object that states which AS is authorized to originate a particular IP address prefix or set of prefixes. Essentially, a ROA is an object that proves an entity owns or controls certain IP space and can announce routes to that space. A ROA is composed of an ROA name, an AS number (ASN), a validity date range, and one or more IP addresses (along with a CIDR block designation—a way of denoting a range of IP addresses—and an optional max length).[21]

There are several tools that give an impression about the state of RPKI deployment.

[20] Robert Lychev, Sharon Goldberg, & Michael Schapira, *BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?*, 171-182 (July 10, 2013).
[21] *See*, *e.g.*, *Route Origin Authorization Overview*, AMERICAN REGISTRY FOR INTERNET NUMBERS, https://www.arin.net/resources/manage/rpki/roa_request/.

VI.4.1.1.1 MANRS Route Origin Attestation Statistics

The MANRS community maintains a tool called the ROA Stats tool (ROAST)[22] that demonstrates the state of ROA deployment by showing the number of prefixes that have an associated ROA and their validation status. This tool can be used to get a snapshot of the state of ROAs per country,[23] per AS, and in aggregate.

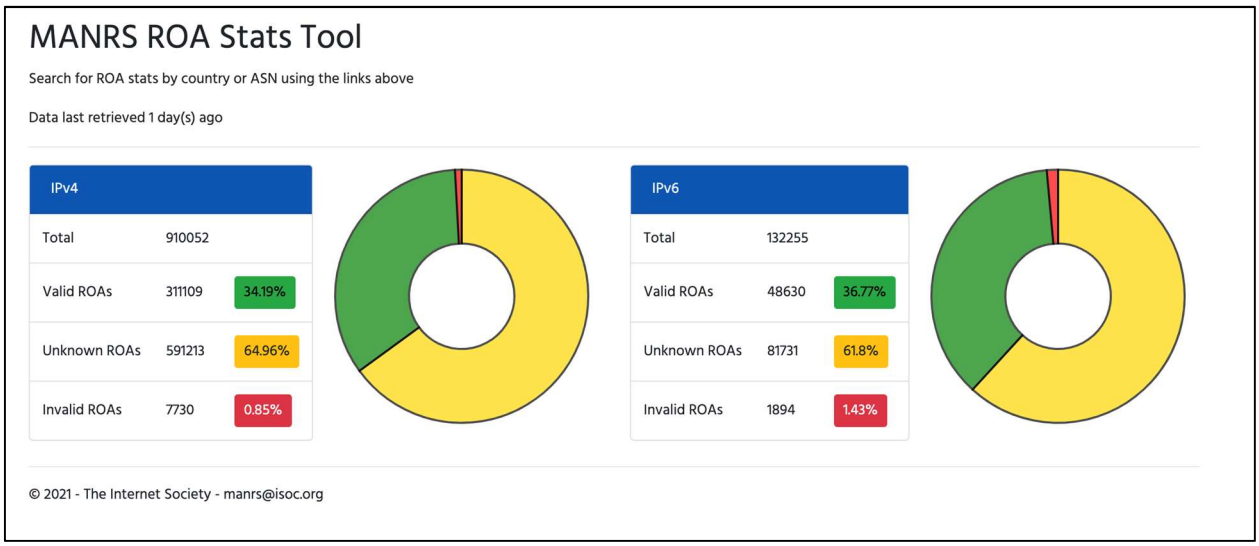


Figure 1: MANRS ROA stats tool aggregate state of prefixes with associated ROAs (captured March 22, 2022, source MANRS)

VI.4.1.1.2 The NIST RPKI Monitor

The NIST RPKI monitor[24] provides a similar perspective on the use of ROAs for route origin validation. Its longitudinal data shows a significant increase of signed and valid route origin validation, from about 10% in 2019 to over 35% in March 2022.

[22] The ROA Stats Tool (ROAST) can be found here: https://roa-stats.manrs.org/.
[23] United States historical data can be found here: https://roa-stats.manrs.org/country/US.
[24] *See NIST RPKI Monitor,* https://rpki-monitor.antd.nist.gov/.

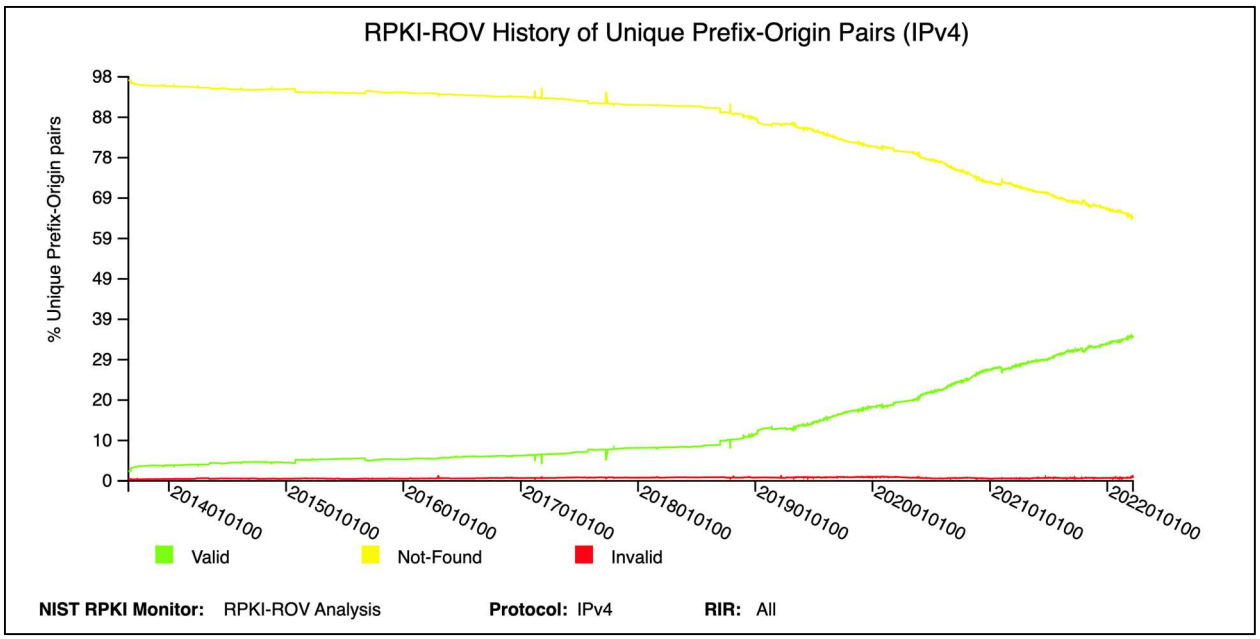


Figure 2: Historical development of RPKI Route Origin Validation in IPv4 (captured March 22, 2022, source NIST)

VI.4.1.1.3 APNIC Routing Origin Validation Measurements

APNIC Labs created a measurement system to calculate the status of ROV across the Internet.[25] They provide a detailed view of where invalid routes were being propagated and show a longitudinal view of how things are changing over time per geographic region. This shows a relatively high level of RPKI validation in the fall of 2020 that has since stabilized around 15-20%.

[25] *See I-Rov Filtering Rate by country (%),* https://stats.labs.apnic.net/rpki.

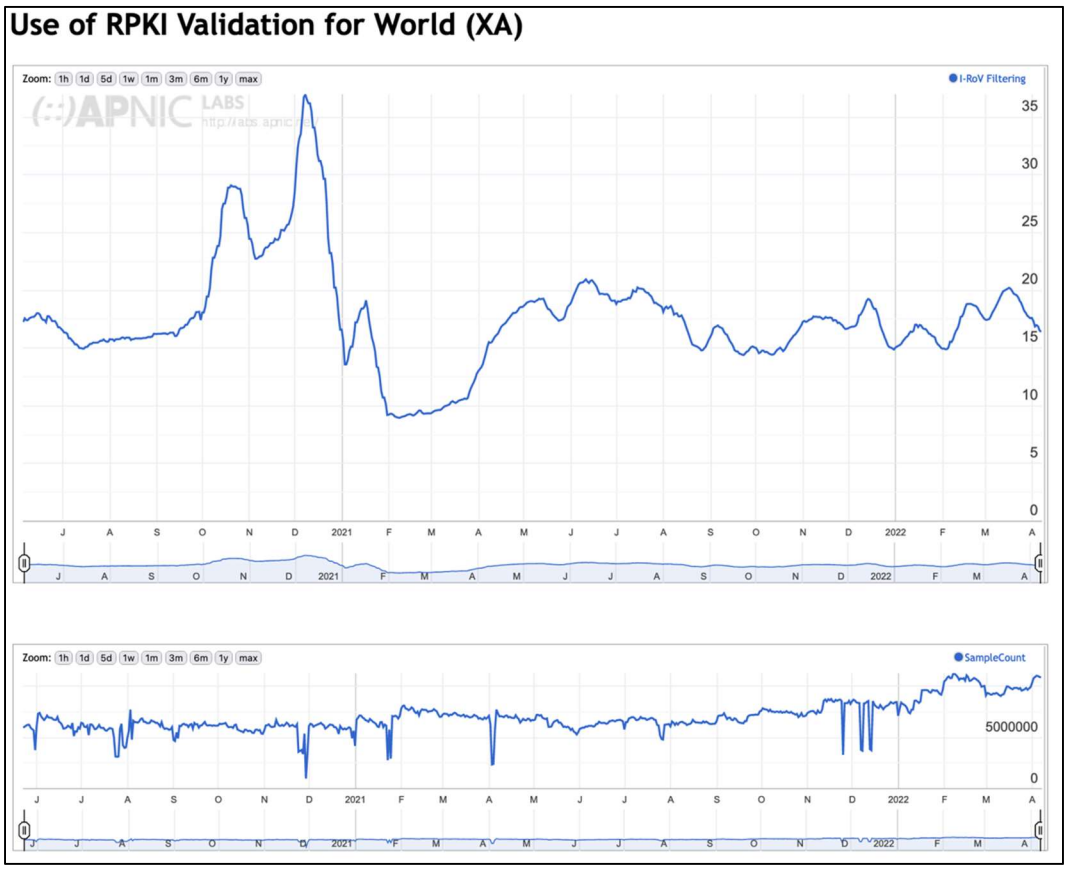


Figure 3: Longitudinal graph of RKPI validation for the World (XA) region from APNIC.

VI.4.1.2 Origin Validation

Route filtering based on RPKI relies on the creation and maintenance of ROAs, which must be in place to do ROV and associated filtering. The growth of ROA publication is a good sign, but it does not correlate to measuring the adoption of ROV. It is safe to assume that more valid ROAs will encourage operators to implement ROV; the other way around is also true.

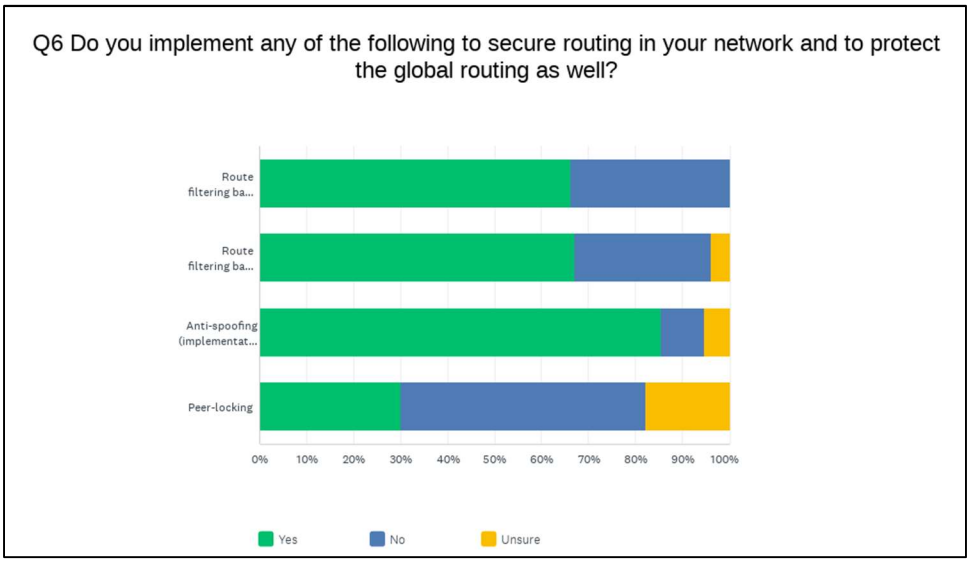
VI.4.2 What BGP Measures and how effective?

> We seek comment on the extent to which network operators have implemented any of the available BGP security measures developed by industry. How effective are these measures in practice? What obstacles have prevented them from doing so?

As mentioned, we have surveyed MANRS participants to better understand the use of various routing security measures, how effective they are perceived to be by MANRS participants, and what kinds of obstacles have prevented participants from putting them in place.[26]

VI.4.2.1 Implementation of Routing Security Measures by MANRS participants

We surveyed MANRS participants about routing security measures they employ:



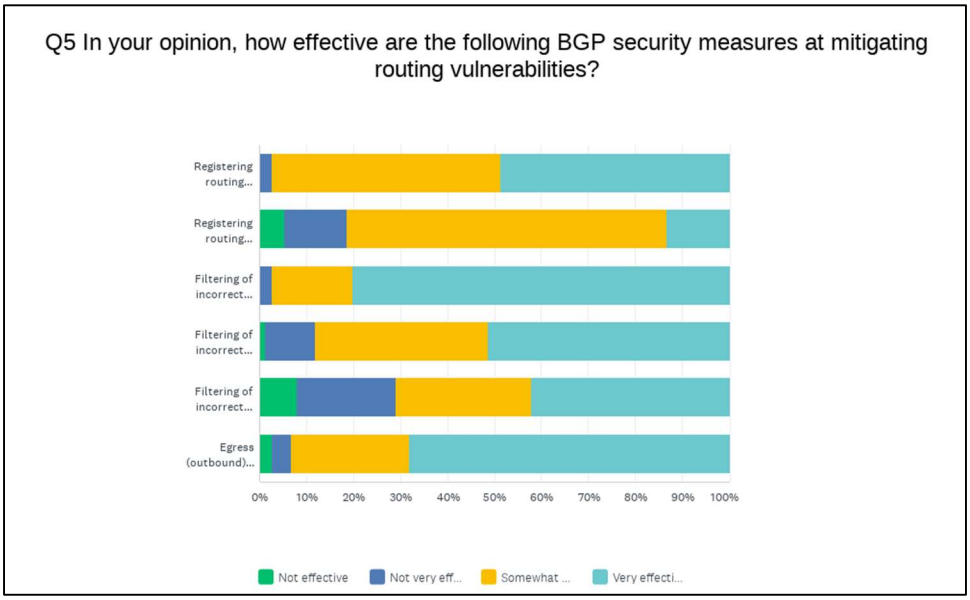
	Yes		No		Unsure		Total
Route filtering based on IRR data	66.22%	49	33.78%	25	0.00%	0	74
Route filtering based on RPKI (Route Origin Validation)	67.11%	51	28.95%	22	3.95%	3	76
Anti-spoofing (implementation of BCP38)	85.53%	65	9.21%	7	5.26%	4	76
Peer-locking	30.14%	22	52.05%	38	17.81%	13	73

This data shows that among responding MANRS participants, anti-spoofing protections are the most popular with both IRR-based and RPKI-based filtering being almost equally popular and peer-locking being the least implemented of routing security measures.

[26] Note: These numbers are not generalizable to the broader ecosystem as this was a survey of MANRS participants—who are already predisposed to acting on routing security—and not a comprehensive survey (with approximately 1/10 of MANRS participants responding to the survey).

VI.4.2.2 Perceived Effectiveness of Routing Security Measures

We surveyed MANRS participants about routing security measure effectiveness:



	Not effective		Not very effective		Somewhat effective		Very effective		Total
Registering routing information in the RPKI (creating ROAs)	0.00%	0	2.63%	2	48.68%	37	48.68%	37	76
Registering routing information in the IRR (creating aut-num, as-set and route objects)	5.33%	4	13.33%	10	68.00%	51	13.33%	10	75
Filtering of incorrect announcements from your customers	0.00%	0	2.63%	2	17.11%	13	80.26%	61	76
Filtering of incorrect announcements from your (lateral) peers	1.32%	1	10.53%	8	36.84%	28	51.32%	39	76
Filtering of incorrect announcements from your transit providers	7.89%	6	21.05%	16	28.95%	22	42.11%	32	76
Egress (outbound) filtering of your own (invalid) announcements	2.67%	2	4.00%	3	25.33%	19	68.00%	51	75

We see here that there are many respondents that consider these routing security measures effective, with each measure achieving 70% effectiveness or higher. We see strong perceptions about the relative effectiveness of IRR-based filtering (13% consider very effective) compared to filtering of incorrect announcements from customer networks (80% consider very effective).

VI.4.2.3 Barriers to Implementing Routing Security Measures

Additionally, we surveyed MANRS participants about perceived barriers to implementing and deploying routing security measures:

What is the main reason for not implementing 'Route filtering based on IRR data'?		
Answer Choices	Responses	
The protection that it offers is not worth the costs to implement	36.36%	8
The associated risks are too low to justify the costs	9.09%	2
The risks associated with it are not fully understood	36.36%	8
Other (please specify)	18.18%	4
	Answered	**22**
	Skipped	**62**

What is the main reason for not implementing 'Route filtering based on RPKI (Route Origin Validation)'?		
Answer Choices	Responses	
The protection that it offers is not worth the costs to implement	25.00%	5
The associated risks are too low to justify the costs	5.00%	1
The risks associated with it are not fully understood	20.00%	4
Other (please specify)	50.00%	10
	Answered	**20**
	Skipped	**64**

What is the main reason for not implementing 'Anti-spoofing (implementation of BCP38)'?		
Answer Choices	Responses	
The protection that it offers is not worth the costs to implement	40.00%	2
The associated risks are too low to justify the costs	0.00%	0
The risks associated with it are not fully understood	40.00%	2
Other (please specify)	20.00%	1
	Answered	**5**
	Skipped	**79**

What is the main reason for not implementing 'Peer-locking'?		
Answer Choices	Responses	
The protection that it offers is not worth the costs to implement	13.33%	4
The associated risks are too low to justify the costs	0.00%	0
The risks associated with it are not fully understood	53.33%	16
Other (please specify)	33.33%	10

	Answered	**30**
	Skipped	**54**

First, we should note that we are asking a community of routing security proponents about barriers to routing security measures that many have already implemented, so the number of respondents answering these questions that focus on non-implementation is low. We see some evidence of risks being poorly understood and concerns with costs. With the last routing security measure, peer locking, general unfamiliarity with the concept—a few of the "Other (please specify)" responses to this question made it clear that several people had not heard of it—and what risks might be involved with deploying it. (Note that we also asked why they implement the protections that they do use; please see the full survey results in the Appendix (Section VIII).)

VI.4.3 Measures of effectiveness

> We seek comment on how to assess, measure, demonstrate, or increase the effectiveness of these security measures. To the extent that network operators have not implemented security measures, we seek comment on why such measures have not been implemented.

The routing system is based on chains of trust; each network relies on not only its own security efforts but those of its neighboring networks (which in turn rely on their neighbors, etc.). Efforts to deploy routing security measures do not necessarily produce proportional protection. On the other hand, the system is open to "free-riding"—if other network operators implement the measures, one may enjoy additional protection even without deploying the mentioned security controls. This is exacerbated by the fact that it is hard to determine if a particular network implements security measures.

Implementation of any security measure has a cost associated with it, whether it is actual resource cost or perceived cost. All security measures face the challenge that each network operator must decide whether or not to deploy them based on its own business objectives.

Further, many router vendors provide a very open default configuration, allowing an operator to start operating the network without any import and export policy or related controls defined; said differently, when a default allows an operator to start a router without employing routing security measures, the router is likely to persist in that insecure state. This issue is addressed by RFC 8212.[27]

VI.5 The BGPsec protocol

> *BGPsec:* We seek comment on whether and to what extent network operators anticipate integrating BGPsec-capable routers into their networks.
>
> The specification for the BGPsec extension to BGP became available in 2017, but it appears that BGPsec has not been widely deployed despite BGP's known vulnerabilities. Why have network operators not taken more aggressive steps to adopt BGPsec? What particular obstacles or concerns about BGPsec have slowed their adoption?

There are various reasons why BGPsec has not seen wide adoption and deployment, but the most important is that BGPsec does not protect against route leaks; it is susceptible to a downgrade attack—if one network on the path does not implement BGPsec the whole path cannot be protected and any party deploying it will suffer a performance hit.[28] The question whether the *Juice is Worth the Squeeze* has been eloquently asked and answered by Lychev et al,[29] who show a variety of flaws with wide BGPsec deployment, including security downgrade attacks, new vulnerabilities and instabilities that would not exist without BGPsec, and in general no real benefit over origin authentication (e.g., RPKI).

In BGPsec, routers must cryptographically sign and verify every BGP message. This creates a significant computational overhead, which could require routers to be upgraded and eventually

---

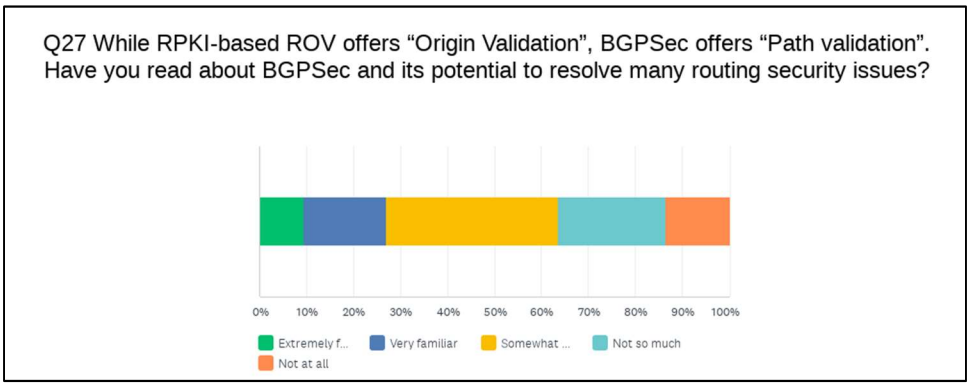
[27] *See Default External BGP (EBGP) Route Propagation Behavior without Policies* (RFC 8212), INTERNET ENGINEERING TASK FORCE (July 2017), https://datatracker.ietf.org/doc/html/rfc8212.

[28] BGPsec does a PKI signature validation for each node in the path, which can be exceptionally large for certain environments that connect lots of networks (e.g., LINX with 1000 networks has a config file a million lines long meaning 7-8 million PKI sig validations on boot. In addition it will need to validate the hundreds of updates per second it receives.

[29] Lychev et al., *supra* note 20.

could slow BGPsec deployment further as operators may have to wait for funding/budget to purchase, test, deploy, and maintain new equipment. Again, any security solution faces the common challenge that each network must decide whether to deploy it based on its own business objectives.

In terms of MANRS participant familiarity with BGPsec, we asked to what extent they had read about BGPsec and its potential to solve routing security issues through "path validation" (as compared to "origin validation" of RPKI). Over 60% of MANRS participants that responded to this question were somewhat, very, or extremely familiar with BGPsec:



For survey respondents that answered this question (Q27) with "somewhat" familiar or higher, we asked a series of three additional questions, asking to what extent they have tested or reviewed BGPsec beta implementations, if they have inquired with their vendors about future BGPsec support, and if they would need to procure new network equipment to deploy BGPsec.

Have you reviewed/tested any beta implementation of BGPSec?		
Answer Choices	Responses	
Yes	14.89%	7
No, there is no beta implementation available from any vendor	6.38%	3
No, I'm not aware of any beta implementation	40.43%	19
No, because it's not in our roadmap to deploy in near future	36.17%	17
No, Other (please specify)	2.13%	1

We see here that a significant number of respondents don't have test (beta) implementations of BGPsec in the routing operating systems they use and a similar number simply don't have plans to examine BGPsec further in the future.

Have you asked your preferred vendor about their roadmap to ship workable code to implement BGPsec?		
Answer Choices	Responses	
Yes	23.40%	11
No	76.60%	36

Obviously, here we see general disinterest from respondents in that three of four respondents said they haven't even asked their vendor about BGPsec. It seems this is not something that these respondents are demanding from the market.

Would you need to replace existing routers and network equipment to support BGPsec?		
Answer Choices	Responses	
Yes	57.45%	27
No	42.55%	20

The answer here indicates a relatively even split from those that responded in terms of need to update their equipment to be able to handle BGPsec. Clearly many would have to have more substantially performant routing equipment to support BGPsec. And for the respondents that don't need to make investments in new equipment, it still appears that there is little interest or demand in BGPsec.

VI.6 MANRS

> 13 To what extent do the network operators that participate in MANRS support both its required and recommended routing security actions, as well as applicable IETF Best Common Practice standards on which those actions are based? To what extent do the network operators that participate in MANRS support both its required and recommended routing security actions,

The intent of MANRS is to create a norm of secure network design and operation as it relates to routing. It defines baseline requirements that can be relatively easily implemented and still protect against major BGP vulnerabilities. All MANRS participants conform to these requirements (called "MANRS actions" for each program). Currently, conformance checks are only performed at the application stage and are not repeated after a participant has joined. The MANRS community recognizes the need for ongoing conformance checks and is working to make more regular conformance checks possible. To raise awareness about networks' MANRS readiness and inform network operators' corrective actions, a special tool was developed and launched—the MANRS Observatory[30] that measures the level of conformance to MANRS Actions, called MANRS Readiness, every month.

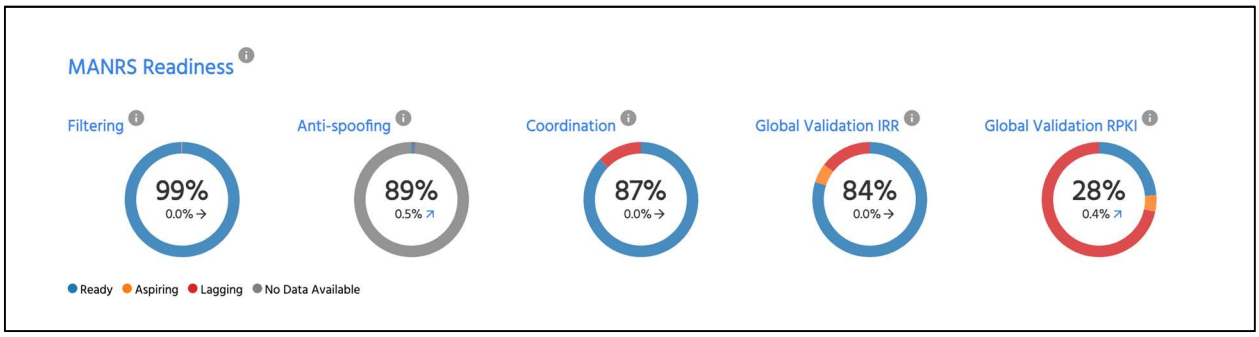


Figure 4: MANRS Readiness scores for selected networks (captured March 22, 2020, source MANRS observatory)

To what extent do network operators participate in MANRS' various programs, including its equipment vendor program, launched in 2021, which aims to enable routing security features on network equipment and provide support and training guidance to use them, or take advantage of the MANRS Observatory.

Each of the four current MANRS programs—Network Operators, Internet Exchange Points (IXPs), Content Delivery Networks (CDN) and Cloud Providers, Equipment Vendors—is specifically designed to maximize impact that category can make on routing security. As of March 22, 2022, 684 network operators, 102 IXPs, 18 CDN and Cloud Providers and 6 Equipment Vendors participate in the programs.

[30] *See State of Routing Security*, MANRS, https://observatory.manrs.org.

According to our survey, nearly 70% of MANRS participants responding actively use the MANRS Observatory (See Section VI.2.1 above).

VI.7 The Commission's Role

> *14. Commission's Role:* We seek comment on steps the Commission, in coordination with other federal agencies, could take to prevent BGP hijacking or otherwise promote secure Internet routing.

We think that the Commission's role in routing security is best focused on providing incentives and working with other agencies to examine the role routing security plays in the cybersecurity of critical infrastructure sectors.

While costs of implementing routing security measures has not been comprehensively studied, we did ask MANRS participants in our survey about relative capital and operational expenses for deploying and maintaining routing security measures (*See* the full survey results in the Appendix, Section VIII). This data is not representative of the larger set of network operators, but it seems to indicate that costs are non-trivial, which indicates that grant, cost-sharing, or tax incentive plans for investment in routing security measures could increase deployment.

We also see a role for the power of the US Government purse in demanding positive evidence of reasonable routing security measures as part of procurement requirements. This would need to be done carefully, as each set of stakeholders in the Internet ecosystem may support routing security in very different ways. (For example, a network operator and an equipment vendor do very different things within the scope of their control to support routing security measures.)

Finally, while we think mandates here could have serious unintended consequences, including potential splintering of the Internet and freezing certain evolving routing security measures before they can fully develop, there may be areas where positive requirements to meet some basic level of routing security maturity could allow "testing the waters" so to speak. Critical infrastructure sectors are a natural place to start given the relative risk of compromise to society,

their increased attention to cybersecurity in recent years, and support structures like Information Sharing and Analysis Centers, that could allow these kinds of requirements to be carefully developed and tailored per stakeholder community.

VI.8 International experiences

> We seek comment on the extent to which other nations' telecommunications regulators and multistakeholder organizations have issued rules, guidance, or otherwise encouraged network operators, network security organizations, and equipment vendors to implement BGP security measures and on any lessons learned from those endeavors.

We are aware that RPKI features on the Dutch government's procurement 'comply or explain' list, which means an entity seeking to have services or goods procured by the Dutch government must either do RPKI or explain why they cannot.[31] In addition, the World Economic Forum has stressed the importance of routing security measures in its work on cybercrime prevention principles for Internet service providers.[32]

VI.9 Equity and Inclusion

> 19 Digital Equity and Inclusion. Finally, the Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related consideration, and benefits (if any) that may be associated with the proposals and issues discussed herein.
>
> Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

The tech sector faces particularly stark diversity issues. These issues manifest differently around the world. We are committed to working through routing security programs that we support, to identify and cultivate opportunities and make the industry more diverse and inclusive.

---

[31] *See* https://www.forumstandaardisatie.nl/open-standaarden/rpki (or through google translate: https://www-forumstandaardisatie-nl.translate.goog/open-standaarden/rpki?_x_tr_sl=nl&_x_tr_tl=en&_x_tr_hl=nl&_x_tr_pto=wapp).

[32] *See* Adrian Wan, *ISPs Should Strongly Consider MANRS to Fight Cybercrime: World Economic Forum Report*, MANRS (Jan. 23, 2020), https://www.manrs.org/2020/01/isps-should-strongly-consider-manrs-to-fight-cybercrime-wef-report/.

VII. Conclusion

Thank you for the opportunity to submit comments and provide some answers to questions in the NOI. We look forward to responding to any additional questions that may arise in the Reply round of this proceeding.

Respectfully submitted,

By: /s/

Joseph Lorenzo Hall
Distinguished Technologist, Strong Internet

Olaf Kolkman
Principal, Internet Technology, Policy, and Advocacy

Megan Kruse
Director, Partner Engagement and Communications

Ryan Polk
Director, Internet Policy

Andrei Robachevsky
Senior Director, Technology Programmes

Aftab Siddiqui
Senior Manager, Internet Technology, Asia-Pacific

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190
703-439-2120

April 11, 2022

VIII. Appendix: Survey Details

VIII.1 The Survey

The survey of MANRS participants to support our response to this NOI was launched on 19 March 2022 on the MANRS members mailing list by sending a SurveyMonkey URI that participants could click on in a web browser and fill out the survey instrument. The survey was closed on 26 March 2022. We received 84 responses with an 88% completion rate (10.3% of the 810 current MANRS participants).

The survey is biased in the sense that it surveyed a community of routing-conscious MANRS participants and that respondents self-selected. In that sense the survey results should be seen as indicative and not as representative.

The survey had some basic branching logic to ask question specifically of respondents that identified that they do or do not employ certain kinds of routing security measures. We include the summary results for each question in the subsequent pages, but some brief description of branching logic and other features warrant specific mention:

- In Q1, which asks about what category of MANRS participant the respondent represents, we had initially left out the option to identify as “Research and/or Educational Network” (also known as “NRENs”) and there were 5 additional responses in “Other (please specify” that mentioned they were an NREN, bringing the total responses for that category to 18 or 21.4%.
- In Q3, there were a few tools mentioned by more than one respondent in “Other (please specify)” that warrant mention: Radar by Qrator, RIPEStat and RIPE tools, and BGPalerter.

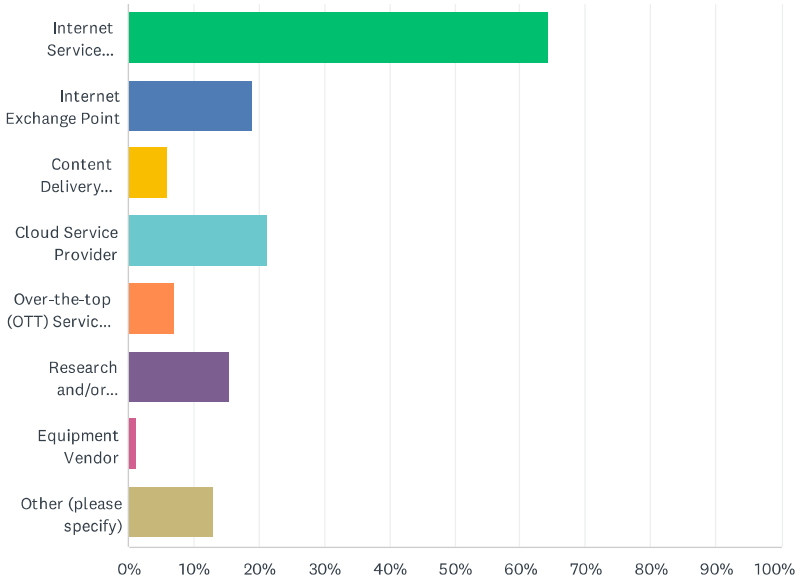
- Q6 represents the first point at which we apply branching logic to expose or hide subsequent questions. For those that answer “yes” to these questions, they are asked three additional questions: “What is the main reason for implementing [X]?” and how they would rate the capital and operational expenditures associated with deploying and maintaining the given routing security measure. For those that answer “no” to any of the elements in Q6, they are asked one follow-up question, “What is the main reason for not implementing [X]?”
- Similarly, in Q23 and Q24, any respondent that answers that less than 75% of resources are covered by these measures, is presented with Q25 and Q26 respectively that asks why this is the case.
- Finally, Q27 asks about awareness of BGPsec and those that answered “somewhat familiar”, “very familiar”, and “extremely familiar” were presented with the final three questions Q28, Q29, and Q30.

VIII.2 Questions and Results

Please see the following pages for summary results from the survey.

Q1 How would you categorize the network you operate or work for (select all that apply)

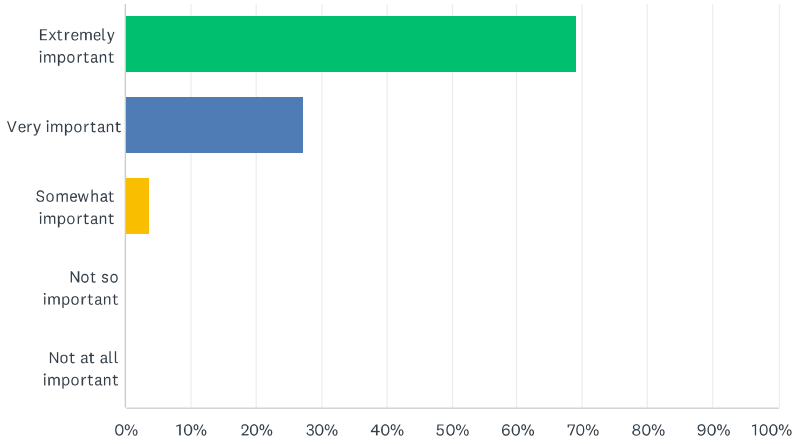
Answered: 84 Skipped: 0



ANSWER CHOICES	RESPONSES	
Internet Service Provider	64.29%	54
Internet Exchange Point	19.05%	16
Content Delivery Network	5.95%	5
Cloud Service Provider	21.43%	18
Over-the-top (OTT) Service Provider (e.g., VOIP)	7.14%	6
Research and/or Educational Network	15.48%	13
Equipment Vendor	1.19%	1
Other (please specify)	13.10%	11
Total Respondents: 84		

Q2 In your opinion, how important is routing security for your network stability, reliability and performance

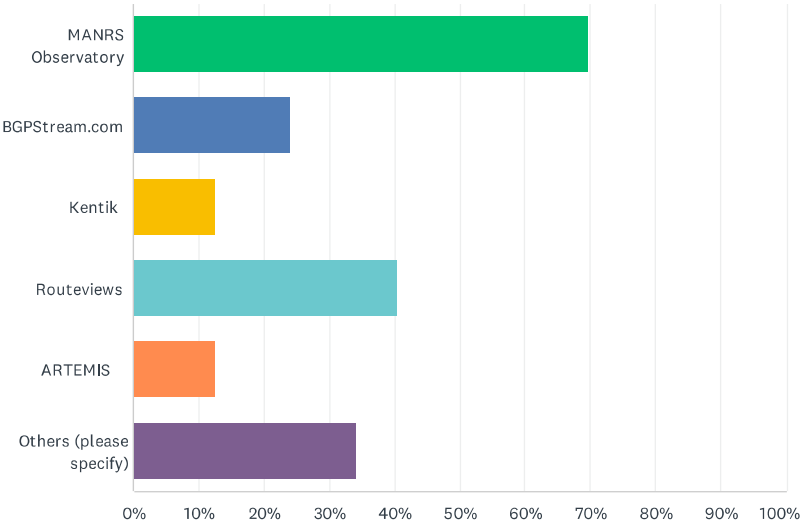
Answered: 84 Skipped: 0



ANSWER CHOICES	RESPONSES	
Extremely important	69.05%	58
Very important	27.38%	23
Somewhat important	3.57%	3
Not so important	0.00%	0
Not at all important	0.00%	0
TOTAL		84

Q3 Do you use any of the following tools to measure/monitor routing incidents?

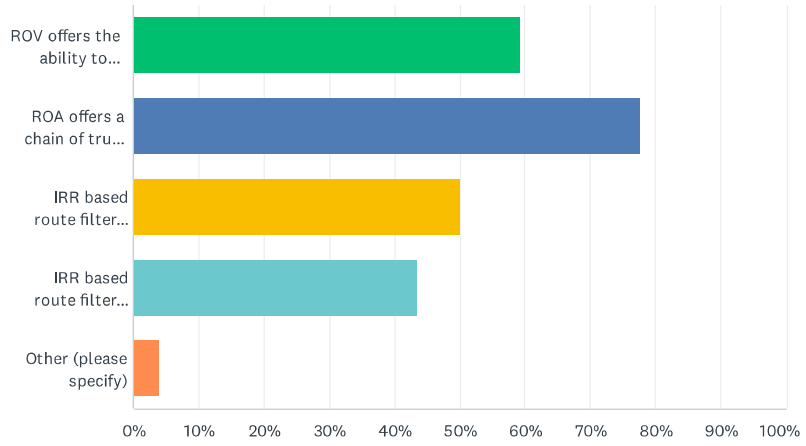
Answered: 79 Skipped: 5



ANSWER CHOICES	RESPONSES	
MANRS Observatory	69.62%	55
BGPStream.com	24.05%	19
Kentik	12.66%	10
Routeviews	40.51%	32
ARTEMIS	12.66%	10
Others (please specify)	34.18%	27
Total Respondents: 79		

Q4 In your opinion, which of the following are the most significant differences between Route Origin Validation (ROV) filtering and IRR (route object) based route filtering?

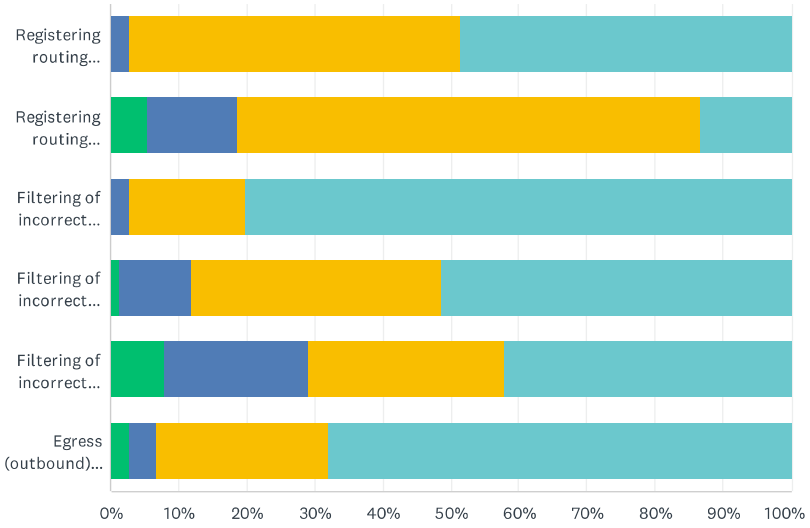
Answered: 76 Skipped: 8



ANSWER CHOICES	RESPONSES	
ROV offers the ability to instantly block route hijack incidents	59.21%	45
ROA offers a chain of trust which is not possible in the IRR database	77.63%	59
IRR based route filtering require certain level of customized automation	50.00%	38
IRR based route filtering is usually implemented on 12/24hrs cycle	43.42%	33
Other (please specify)	3.95%	3
Total Respondents: 76		

Q5 In your opinion, how effective are the following BGP security measures at mitigating routing vulnerabilities?

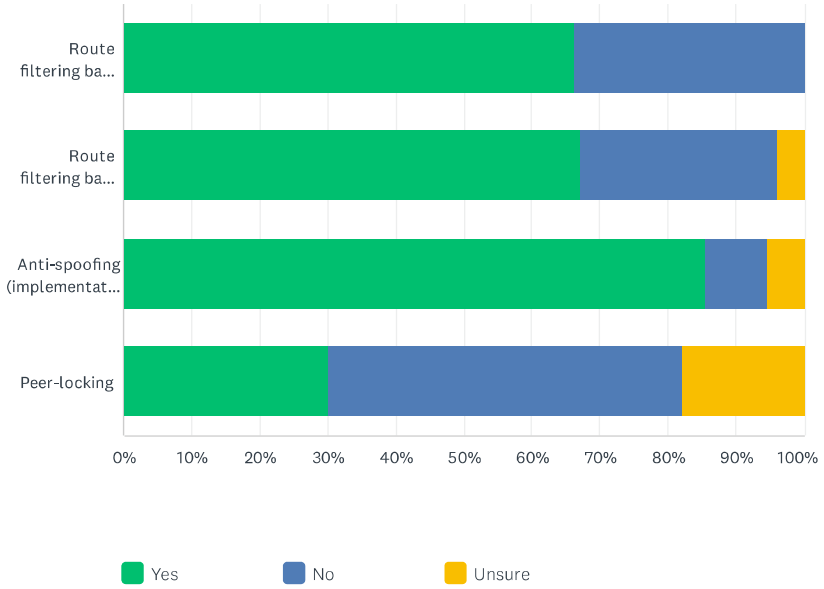
Answered: 76 Skipped: 8



	NOT EFFECTIVE	NOT VERY EFFECTIVE	SOMEWHAT EFFECTIVE	VERY EFFECTIVE	TOTAL	WEIGHTED AVERAGE
Registering routing information in the RPKI (creating ROAs)	0.00% 0	2.63% 2	48.68% 37	48.68% 37	76	3.46
Registering routing information in the IRR (creating aut-num, as-set and route objects)	5.33% 4	13.33% 10	68.00% 51	13.33% 10	75	2.89
Filtering of incorrect announcements from your customers	0.00% 0	2.63% 2	17.11% 13	80.26% 61	76	3.78
Filtering of incorrect announcements from your (lateral) peers	1.32% 1	10.53% 8	36.84% 28	51.32% 39	76	3.38
Filtering of incorrect announcements from your transit providers	7.89% 6	21.05% 16	28.95% 22	42.11% 32	76	3.05
Egress (outbound) filtering of your own (invalid) announcements	2.67% 2	4.00% 3	25.33% 19	68.00% 51	75	3.59

Q6 Do you implement any of the following to secure routing in your network and to protect the global routing as well?

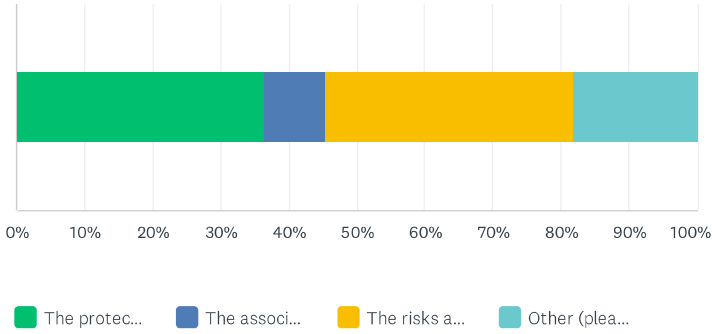
Answered: 76 Skipped: 8



	YES	NO	UNSURE	TOTAL
Route filtering based on IRR data	66.22% 49	33.78% 25	0.00% 0	74
Route filtering based on RPKI (Route Origin Validation)	67.11% 51	28.95% 22	3.95% 3	76
Anti-spoofing (implementation of BCP38)	85.53% 65	9.21% 7	5.26% 4	76
Peer-locking	30.14% 22	52.05% 38	17.81% 13	73

Q7 What is the main reason for not implementing 'Route filtering based on IRR data'?

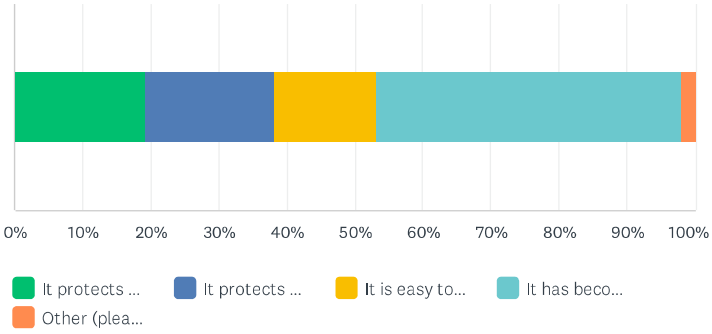
Answered: 22 Skipped: 62



ANSWER CHOICES	RESPONSES	
The protection that it offers is not worth the costs to implement	36.36%	8
The associated risks are too low to justify the costs	9.09%	2
The risks associated with it are not fully understood	36.36%	8
Other (please specify)	18.18%	4
TOTAL		22

Q8 What is the main reason for implementing 'Route filtering based on IRR data'?

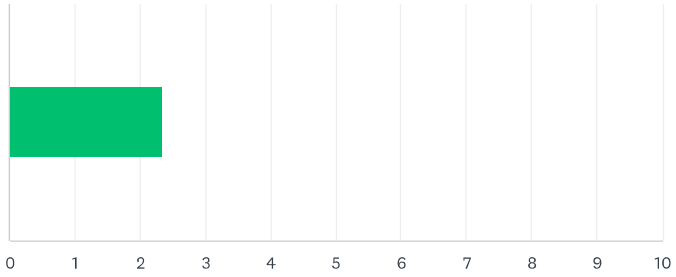
Answered: 47 Skipped: 37



ANSWER CHOICES	RESPONSES	
It protects our network from outages	19.15%	9
It protects our network from PR/reputational damage	19.15%	9
It is easy to implement and has very low implementation cost	14.89%	7
It has become baseline industry standard for routing security	44.68%	21
Other (please specify)	2.13%	1
TOTAL		47

Q9 How would you estimate the capital expenditure (CAPEX) associated to deploy 'Route filtering based on IRR data'?

Answered: 44 Skipped: 40



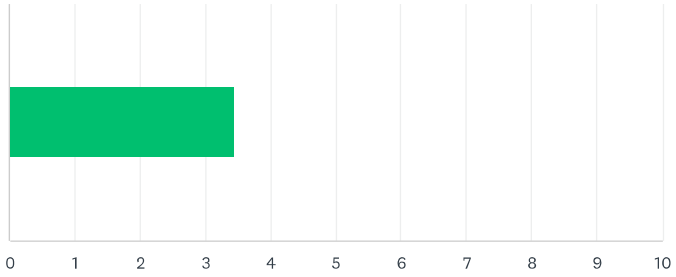
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	2	103	44
Total Respondents: 44			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	8.00	2.00	2.34	2.18

Q10 How would you estimate the operational expenditure (OPEX) associated to maintain 'Route filtering based on IRR data'?

Answered: 44 Skipped: 40



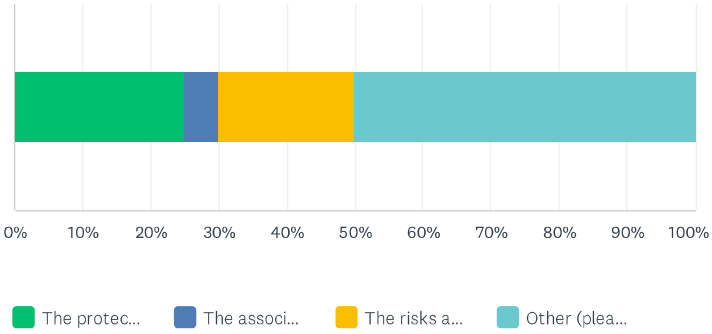
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	3	152	44
Total Respondents: 44			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	8.00	3.00	3.45	2.29

Q11 What is the main reason for not implementing 'Route filtering based on RPKI (Route Origin Validation)'?

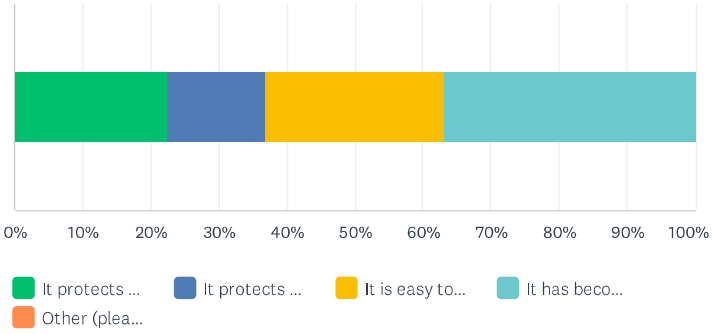
Answered: 20 Skipped: 64



ANSWER CHOICES	RESPONSES	
The protection that it offers is not worth the costs to implement	25.00%	5
The associated risks are too low to justify the costs	5.00%	1
The risks associated with it are not fully understood	20.00%	4
Other (please specify)	50.00%	10
TOTAL		20

Q12 What is the main reason for implementing 'Route filtering based on RPKI (Route Origin Validation)'?

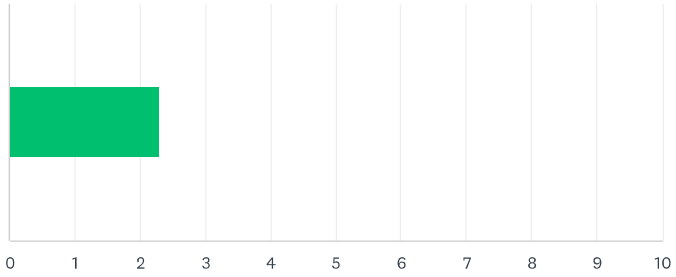
Answered: 49 Skipped: 35



ANSWER CHOICES	RESPONSES	
It protects our network from outages	22.45%	11
It protects our network from PR/reputational damage	14.29%	7
It is easy to implement and has very low implementation cost	26.53%	13
It has become baseline industry standard for routing security	36.73%	18
Other (please specify)	0.00%	0
TOTAL		49

Q13 How would you estimate the capital expenditure (CAPEX) associated to deploy 'Route filtering based on RPKI (Route Origin Validation)'?

Answered: 46 Skipped: 38



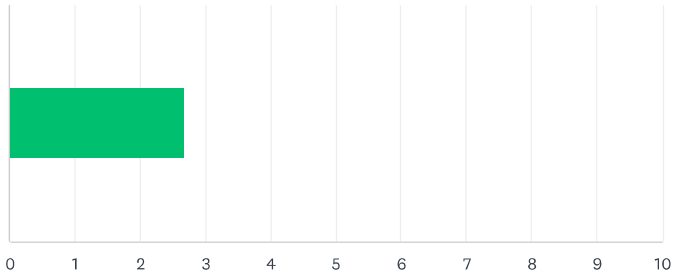
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	2	106	46
Total Respondents: 46			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	8.00	1.00	2.30	2.30

Q14 How would you estimate the operational expenditure (OPEX) associated to maintain 'Route filtering based on RPKI (Route Origin Validation)'?

Answered: 44 Skipped: 40



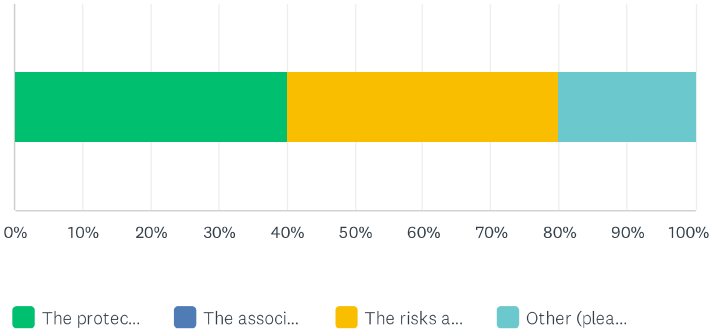
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	3	118	44
Total Respondents: 44			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	7.00	2.00	2.68	2.12

Q15 What is the main reason for not implementing 'Anti-spoofing (implementation of BCP38)'?

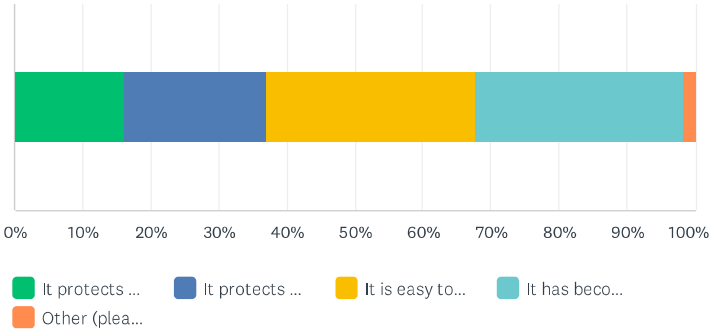
Answered: 5 Skipped: 79



ANSWER CHOICES	RESPONSES	
The protection that it offers is not worth the costs to implement	40.00%	2
The associated risks are too low to justify the costs	0.00%	0
The risks associated with it are not fully understood	40.00%	2
Other (please specify)	20.00%	1
TOTAL		5

Q16 What is the main reason for implementing 'Anti-spoofing (implementation of BCP38)'?

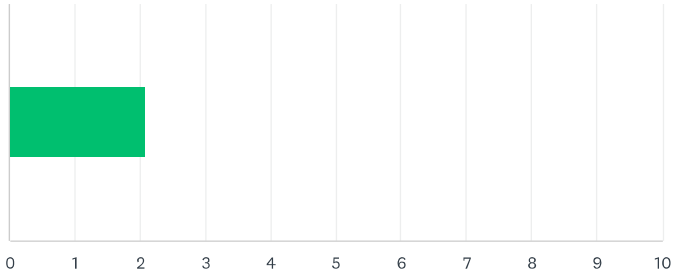
Answered: 62 Skipped: 22



ANSWER CHOICES	RESPONSES	
It protects our network from outages	16.13%	10
It protects our network from PR/reputational damage	20.97%	13
It is easy to implement and has very low implementation cost	30.65%	19
It has become baseline industry standard for routing security	30.65%	19
Other (please specify)	1.61%	1
TOTAL		62

Q17 How would you estimate the capital expenditure (CAPEX) associated to deploy 'Anti-spoofing (implementation of BCP38)'?

Answered: 51 Skipped: 33



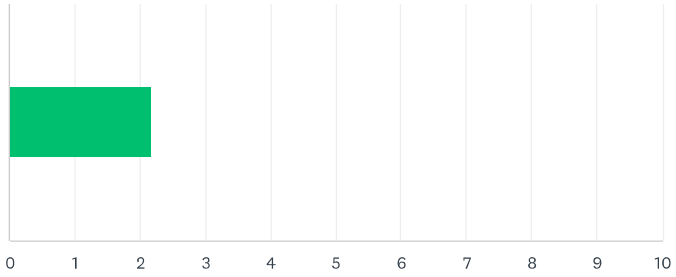
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	2	107	51
Total Respondents: 51			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	10.00	1.00	2.10	2.60

Q18 How would you estimate the operational expenditure (OPEX) associated to maintain 'Anti-spoofing (implementation of BCP38)'?

Answered: 53 Skipped: 31



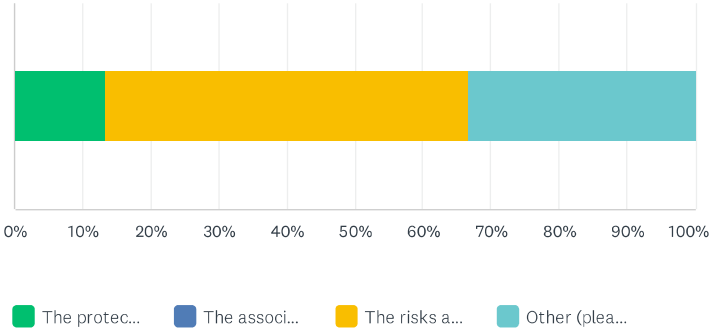
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	2	115	53
Total Respondents: 53			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	9.00	2.00	2.17	1.85

Q19 What is the main reason for not implementing 'Peer-locking'?

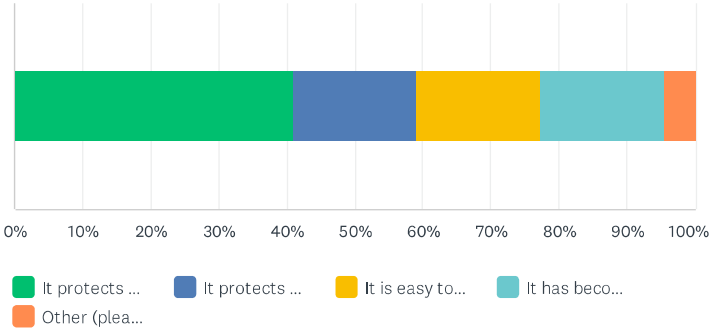
Answered: 30 Skipped: 54



ANSWER CHOICES	RESPONSES	
The protection that it offers is not worth the costs to implement	13.33%	4
The associated risks are too low to justify the costs	0.00%	0
The risks associated with it are not fully understood	53.33%	16
Other (please specify)	33.33%	10
TOTAL		30

Q20 What is the main reason for implementing 'Peer-locking'?

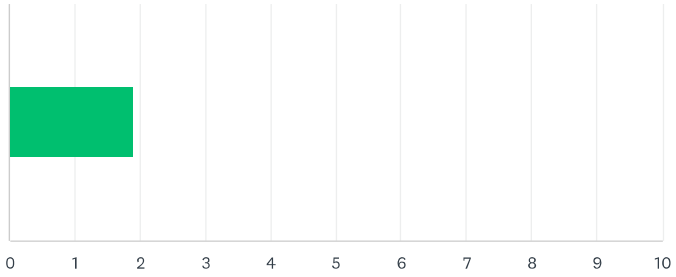
Answered: 22 Skipped: 62



ANSWER CHOICES	RESPONSES	
It protects our network from outages	40.91%	9
It protects our network from PR/reputational damage	18.18%	4
It is easy to implement and has very low implementation cost	18.18%	4
It has become baseline industry standard for routing security	18.18%	4
Other (please specify)	4.55%	1
TOTAL		22

Q21 How would you estimate the capital expenditure (CAPEX) associated to deploy 'Peer-locking'?

Answered: 18 Skipped: 66



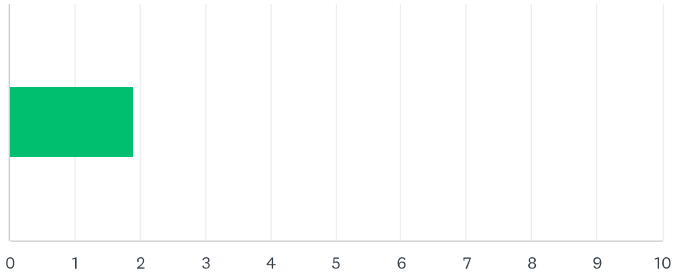
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	2	34	18
Total Respondents: 18			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	7.00	1.50	1.89	1.85

Q22 How would you estimate the operational expenditure (OPEX) associated to maintain 'Peer-locking'?

Answered: 18 Skipped: 66



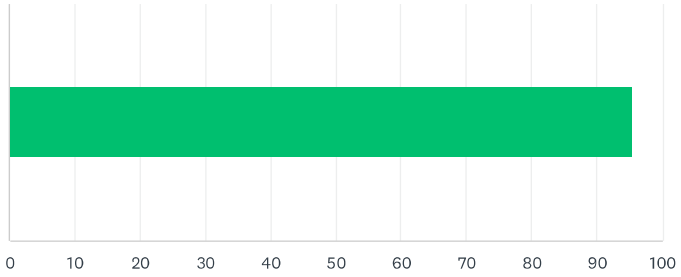
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	2	34	18
Total Respondents: 18			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	6.00	1.50	1.89	1.70

Q23 How much (in percentage) of your network resources (IPv4 and IPv6) are covered by IRR based route objects?

Answered: 74 Skipped: 10



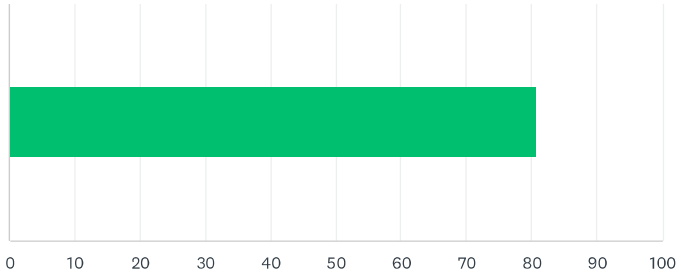
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	96	7,072	74
Total Respondents: 74			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
1.00	100.00	100.00	95.57	15.89

Q24 How much (in percentage) of your network resources (IPv4 and IPv6) are covered by RPKI Route Origin Authorization (ROA)?

Answered: 72 Skipped: 12



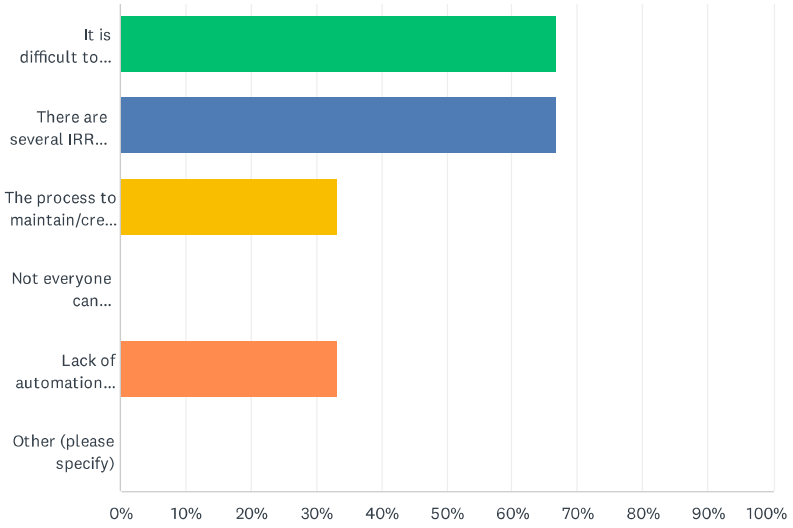
ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	81	5,822	72
Total Respondents: 72			

BASIC STATISTICS

MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
0.00	100.00	100.00	80.86	34.36

Q25 Why is less than 75% of your network resources (IPv4 and IPv6) covered by IRR based route objects?

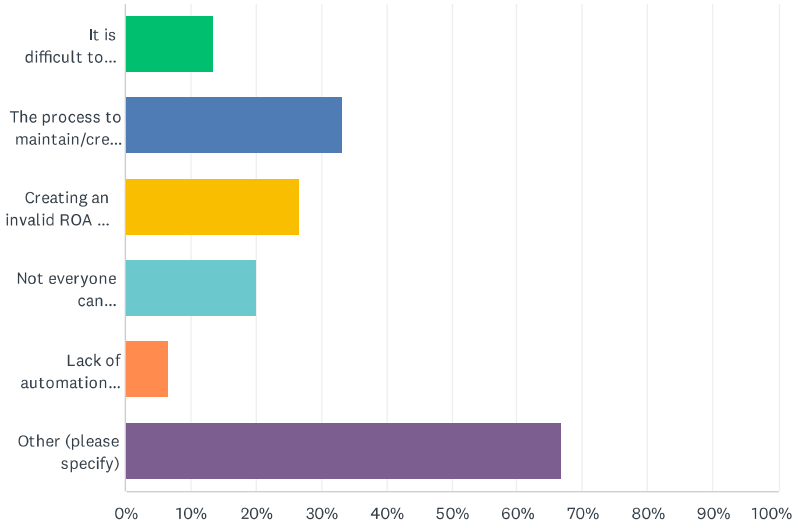
Answered: 3 Skipped: 81



ANSWER CHOICES	RESPONSES	
It is difficult to maintain up to date route objects	66.67%	2
There are several IRR database and many of them filled with incorrect data making accuracy impossible	66.67%	2
The process to maintain/create route objects is somewhat complicated	33.33%	1
Not everyone can maintain/create route object in the organization due to access issue	0.00%	0
Lack of automation provided by RIRs to help the process	33.33%	1
Other (please specify)	0.00%	0
Total Respondents: 3		

Q26 Why is less than 75% of your network resources (IPv4 and IPv6) covered by ROAs?

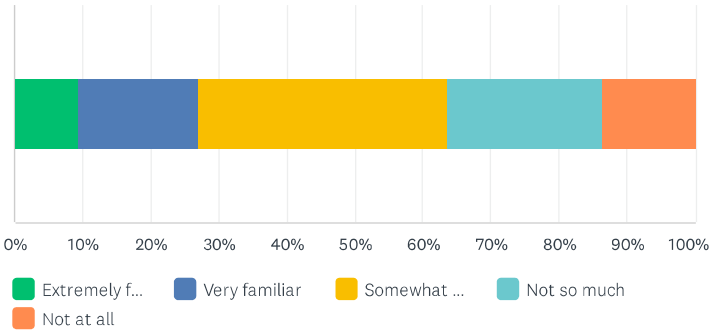
Answered: 15 Skipped: 69



ANSWER CHOICES	RESPONSES	
It is difficult to maintain up to date ROA	13.33%	2
The process to maintain/create ROA is somewhat complicated	33.33%	5
Creating an invalid ROA has very significant consequences (outage) therefore we avoid frequent updates	26.67%	4
Not everyone can maintain/create ROA in the organization due to access control issues	20.00%	3
Lack of automation provided by RIRs to help the process	6.67%	1
Other (please specify)	66.67%	10
Total Respondents: 15		

Q27 While RPKI-based ROV offers “Origin Validation”, BGPSec offers “Path validation”. Have you read about BGPSec and its potential to resolve many routing security issues?

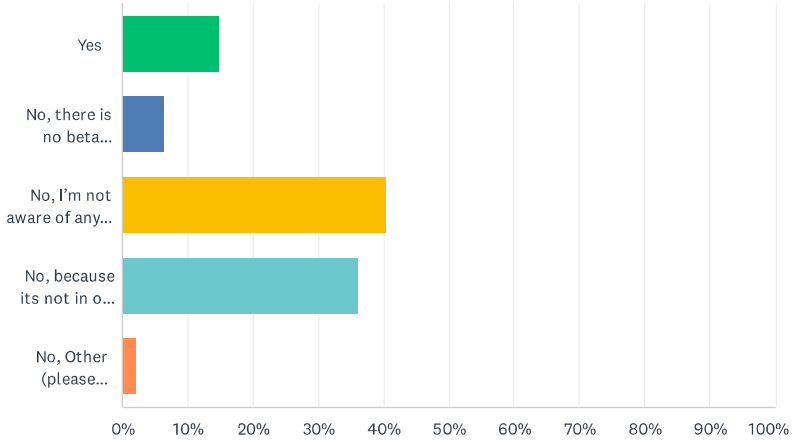
Answered: 74 Skipped: 10



ANSWER CHOICES	RESPONSES	
Extremely familiar	9.46%	7
Very familiar	17.57%	13
Somewhat familiar	36.49%	27
Not so much	22.97%	17
Not at all	13.51%	10
TOTAL		74

Q28 Have you reviewed/tested any beta implementation of BGPSec?

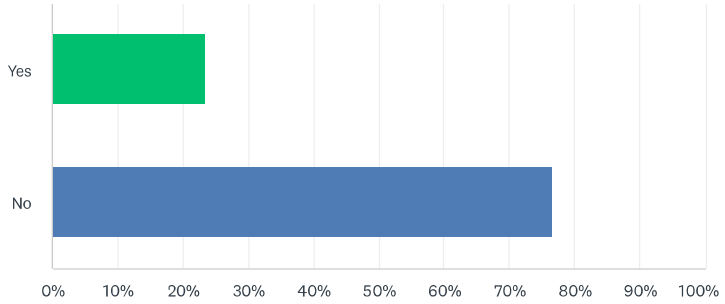
Answered: 47 Skipped: 37



ANSWER CHOICES	RESPONSES	
Yes	14.89%	7
No, there is no beta implementation available from any vendor	6.38%	3
No, I'm not aware of any beta implementation	40.43%	19
No, because its not in our roadmap to deploy in near future	36.17%	17
No, Other (please specify)	2.13%	1
TOTAL		47

Q29 Have you asked your preferred vendor about their roadmap to ship workable code to implement BGPSec?

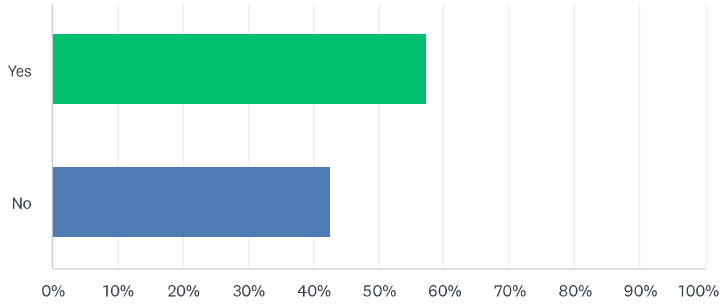
Answered: 47 Skipped: 37



ANSWER CHOICES	RESPONSES	
Yes	23.40%	11
No	76.60%	36
TOTAL		47

Q30 Would you need to replace existing routers and network equipment to support BGPsec?

Answered: 47 Skipped: 37



ANSWER CHOICES	RESPONSES	
Yes	57.45%	27
No	42.55%	20
TOTAL		47