MANRS

Mutually Agreed Norms for Routing Security

Call for Comments:
MANRS for CDN and Cloud Providers – A Draft Action Set

Background

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society that provides crucial fixes to reduce the most common routing threats. Originally designed for network operators, the initiative has already been adapted once to address the unique needs and concerns of IXPs. This resulted in the development of a so-called MANRS IXP Programme.

Two sets of requirements for MANRS, developed by the community in collaborative fashion, already exist:

1. Network Operators/ISPs
2. IXPs

How were Action Sets for ISPs and IXPs developed?

In early 2014, a small group of network operators began working on a way to gather the wider operator community to improve the security and resilience of the global routing system. This eventually became an initiative we called the ***Routing Resilience Manifesto***, and it produced a set of initial recommendations that we published as a draft document in July 2014 for community review and comment.

Once the community review and feedback period closed on 31 August 2014, we consolidated all the comments, updated the draft into the final version of the "**Mutually Agreed Norms for Routing Security (MANRS)" document**, and officially launched the MANRS site with an initial list of supporters. See the homepage for more information on the current status of the Manifesto and the ever-growing list of proponents.

A similar process was applied when developing the Action Set for IXPs. The idea was first presented at the EURO-IX 28th forum in 2016 and a task force was formed to develop draft requirements. Their work was presented in the course of 2017 to the IXP community at the major peering forums in all regions. Consensus was reached in early 208 and in April 2018 a **MANRS IXP Programme** was launched.

A next phase of this work, presented in this document, focuses on CDN and Cloud providers and aims at making MANRS more accessible and impactful to these categories of operators.

This draft was developed by a Task Force. Members of the Task Force are:

- Alejandro Becerra Gonzalez (Telefonica)
- Andrei Robachevsky (Internet Society, Editor)
- Arturo Servin (Google)
- Carlos Asensio (Nexica)
- Chris Morrow (Google)
- Christian Kaufmann (Akamai)
- Daniel Ponticello (Redder)
- Gary Ratterree (Microsoft)
- Ibrahim Seremet (Verisign)
- Jerome Fleury (Cloudflare)
- JJ Crawford (Facebook)
- Kay Rechthien (Akamai)
- Kevin Blumberg (TORIX)
- Marcus Grando (Azion)
- Martin J. Levy (Cloudflare)
- Marty Strong (Facebook)
- Rob Spiger (Microsoft)
- Rogério Mariano (Azion)
- Ronan Mullally (Akamai)
- Ray Sliteris (Facebook)
- Steve Peters (Facebook)
- Tale Lawrence (Oracle)
- Tony Tauber (Comcast)
- Yong Kim (Verisign)

The requirements outlined in this document address the CDN or Cloud network (or networks) itself and its peers.

By a peer in this document we mean a BGP neighbor network with a peer-peer policy: only own network and its customer cone is announced, no global transit is provided.

This document is a draft Action Set for CDN and Cloud networks.

Please send your comments to: manrs-cdn-cloud@elists.isoc.org.

Action Set (Draft)

Action 1. Prevent propagation of incorrect routing information (Mandatory)

Ensure correctness of own announcements. Ensure correctness of announcements of their peers (non-transit) by implementing explicit (whitelist) filtering with prefix granularity.

Description:

Cloud providers and content providers do have own internal networks, such as corporate networks, or other sub-networks for R&D and other purposes. With regard to those networks good filtering practice should still apply to help prevent propagation of incorrect routing information due to human error or failures in automation.

CDNs and Cloud providers have many peering (networks that do not provide transit for the CDN/Cloud) relationships. Implementing ingress filtering for all non-transit peers and their customers not only will make a significant positive impact on routing security but will also send a clear signal that incorrect routing announcements are not acceptable. Whenever feasible, checks should be made that the announcements are originated from legitimate holders.

Conformance checks:

1. This requirement is part of the peering policy of the CDN/Cloud provider and is publicly available (e.g. on their website or peering portal).

Action 2. Prevent traffic with illegitimate source IP addresses (Mandatory)

Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network (egress filters).

Description:

There is a difference between CDN and Cloud network with regards to this Action. There is additional challenge for Cloud providers, since they have to monitor and control what a virtual machine can do on the network. This Action requires controls that prevent traffic with illegitimate source IP addresses leaving the Autonomous System of the CDN or Cloud provider.

Conformance checks:

1. A cloud provider periodically runs a Spoofer (https://www.caida.org/projects/spoofer/) test from a VPS (typical setup) confirming that controls are in place. A CDN can run the test from their own infrastructure segment.

Action 3. Facilitate global operational communication and coordination (Mandatory)

Maintain globally accessible up-to-date contact information in PeeringDB and relevant RIR databases.

Description:

The operator should register and maintain contact information in PeeringDB and appropriate RIRs' whois databases. This contact information should include the operator's current point of contact information for the NOC of the AS.

Conformance checks:

1. Check that phone or e-mail address (other than abuse-c) for provider's AS'es is present in at least one RIR database

2. Check that PeeringDB contains Contact information for provider's AS'es

Action 4. Facilitate validation of routing information on a global scale (Mandatory)

Publicly document ASNs and prefixes that are intended to be advertised to external parties. Two main types of repositories are IRRs and RPKI. The requirement is to publish this information in at least one type of the repository (there may be more than one appropriate IRR), a recommendation is to maintain in both.

Description:

CDN and Cloud provider also indirectly contribute to the facilitation of validation on global scale by implementing Action 1. It effectively results in motivating third parties to maintain their routing information. This will have a significant impact on the quality and completeness of such data.

Conformance checks:

1. Check that the announcements originated by the provider's AS'es are registered in at least one IRR and/or RPKI systems.

Action 5. Encourage MANRS adoption (Mandatory)

Actively encourage MANRS adoption among the peers.

Description:

There is benefit in encouraging the implementation of good practices on routing security from the peers. Even if Action 1 is implemented by a CDN/Cloud provider, an incorrect announcement from a peer can still find its way in the routing table, e.g. through a transit arrangement. Implementation of the MANRS Actions by a peer ensures this won't happen. Additionally, a reference to a clearly defined specific baseline as MANRS can align such requests and amplify them. This is essential for scaling up the adoption of MANRS. This is a path for transforming MANRS in true norms with the global effect.

Conformance checks:

1. A publicly available policy, a peering form or an e-mail template with a recommendation to implement MANRS.

Action 6. Provide monitoring and debugging tools to the peering partners (Optional)

Provide a mechanism to inform peering partners if their announcements did not meet the requirements of the peering policy of the CDN and Cloud provider.

Description:

To facilitate debugging of potential routing problems and provide feedback to peers on the effects of policy controls applied by a CDN and Cloud provider, the provider offers a tool, accessible publicly, or at least to the peering partners.

Conformance checks:

1. Description of the tool
2. Availability of the tool publicly or to the peers