MANRS

Mutually Agreed Norms for Routing Security

MANRS Actions for Network Operators

Version 2.3 – 30 September 2019

1. Introduction

Mutually Agreed Norms for Routing Security (MANRS) is an initiative to greatly improve the security and resilience of the Internet's global routing system. It does this by encouraging those running BGP to implement well-established industry best practices and technological solutions that can address the most common threats.

Throughout the history of the Internet, collaboration among its participants and shared responsibility for its smooth operation have been two of the pillars supporting its tremendous growth and success. This document aims to build on this spirit by defining the actions that should be taken by network operators. By doing so, network operators demonstrate a commitment to improving security, develop a culture of collective responsibility, and build a responsible community.

MANRS has the following objectives:

- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility towards the security and resilience of the Internet's global routing system.
- Demonstrate the ability of the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

2. Scope

MANRS is based around a set of actions that aim to address three main classes of problem:

1) Incorrect routing information
2) Traffic with spoofed source IP addresses
3) Coordination and collaboration between networks

The *Compulsory Actions* define the steps that network operators should be taking at a minimum to better ensure the security and resilience of the Internet's global routing system and must be implemented by network operators to be accepted as a MANRS participant.

The *Recommended Actions* are steps that help address the underlying cause of DDoS attacks, as well as allowing for the cryptographic validation of number resources belonging to other networks.

These actions are based on well-established industry best practices and have been selected on the basis of an assessment of the balance between small, incremental costs to individual network operators and the potential common benefits. However, these actions are not exhaustive and many network operators may already be implementing even stronger measures and controls.

It is also recognised that these actions are not a comprehensive solution to the outlined problems, but each offers steps that if implemented by a large number of network operators, will result in significant improvements in the security and resilience of the Internet's global routing system.

3. Definitions

To articulate the specifics of the Compulsory and Expected Actions, it is necessary to define a number of terms relating to their general usage within the Internet industry.

BGP	Border Gateway Protocol, responsible for exchanging routing and reachability information amongst *Autonomous Systems* on the Internet.
Infrastructure	A network operator's internal network(s) which may or may not be reachable on the Internet.
Autonomous System	Network(s) forming a single administrative domain that are identified by a unique Autonomous System Number (ASN) and present a common and clearly defined routing policy to the Internet.
End User	Endpoint within a network operator's AS where traffic is destined for and/or originates from.
Transit Network	An external network to which traffic originating from a network operator's *Infrastructure* and *Customer Networks* is sent, and from which traffic from the wider Internet is received.
Customer Network	An external network for which a network operator provides transit services. These can be categorised as *Directly Connected Customers* who may, and *Indirectly Connected Customers* who may not, have a business relationship with the network operator.
Peer Network	An external network to which a network operator is directly connected and exchanges traffic on a settlement free basis.
Stub Network	A directly connected external network which itself has no customer network although it may have peer networks.
Single-Homed	An *End User* or *Customer Network* that only has a single connection to the network operator's infrastructure over which traffic can flow.

Multi-Homed	An *End User*, *Customer Network* or other type of network that has two or more connections to the Internet which provides multiple paths over which traffic can flow.
RIR	Regional Internet Registry that manages the allocation and registration of Internet number resources within a region of the world.
NIR	National Internet Registry that manages the allocation and registration of Internet number resources for some countries of the world.

4. Compulsory Actions

Action 1: Prevent propagation of incorrect routing information

Network operator must implement a system whereby they only announce to adjacent networks the AS numbers and IP prefixes they or their customers are legitimately authorised to originate.

Network operator must check whether the announcements of their customers are correct; specifically, that each customer legitimately holds the AS numbers and IP address space they announce.

Discussion:

It is most important to secure inbound routing advertisements, especially from Customer Networks, through the use of explicit prefix-level filters or equivalent mechanisms. AS-path filters might also be used to require that Customer Networks are explicit about which Autonomous Systems (ASes) are downstream of that customer. Alternately, AS-path filters that block announcements by Customer Networks of ASes with which the provider is peering can prevent some types of routing 'leaks'. Filtering customer BGP announcements by AS-path filters alone is insufficient to prevent catastrophic routing problems at a systemic level.

References:

- Recommended Internet Service Provider Security Services and Procedures, Section Network Infrastructure - http://www.rfc-editor.org/bcp/bcp46.txt
- BGP operations and security - http://tools.ietf.org/html/draft-ietf-ops
- Border Gateway Protocol Security, NIST: Special Publication SP800K54 - http://csrc.nist.gov/publications/nistpubs/800K54/SP800K54.pdf
- Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure - http://tools.ietf.org/html/rfc3871
- Using RPSL in Practice - http://tools.ietf.org/html/rfc2650
- Using the RIPE Database as an Internet Routing Registry - https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry

- BGP Security Best Practices, FCC CSRIC III WG4 Final Report - http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Action 3: Facilitate global operational communication and coordination

Network operator must ensure that up-to-date contact information is entered and maintained in the appropriate RIR (or NIR) database and/or in PeeringDB. It is strongly recommended that contact information is made publicly available, but at a minimum must be available to other network operators registered with PeeringDB.

Discussion:

Network operators should register and maintain NOC contact information for each AS and netblock(s) that they are responsible for. This must include an email address to which operational queries may be sent and expected to reply within 48 hours, and a telephone number and dedicated abuse email address (e.g. abuse-c) should also be provided. Networks are encouraged to document their routing policies in an IRR, and additional information (e.g. Looking Glass URL) in the appropriate field of their PeeringDB record is welcome.

References:

- Using RPSL in Practice - http://tools.ietf.org/html/rfc2650
- PeeringDB - https://www.peeringdb.com
- RADB - http://www.radb.net

Action 4: Facilitate routing information on a global scale - IRR

Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry, RADB or an RADB-mirrored IRR. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.

A network operator may alternatively implement *Action 4: Facilitate routing information on a global scale - RPKI* (defined below) in lieu of a publicly documented routing policy.

Discussion:

To facilitate validation of routing information by other networks on a global scale, information about routing policy, including ASNs and IP prefixes that are intended to be advertised to external parties, is necessary. Routing policy can be publicly documented using RPSL in one of the Internet Routing Registries (IRRs) mirrored by RADB (e.g. AfriNIC, APNIC, ARIN, RIPE).

Network operators must register and maintain one (at minimum) or more “as-set” IRR objects containing a list of ASNs intended to be advertised to external parties that can be used by automatic tools to generate prefix filters. Network operators must also maintain their information in the IRR to ensure that is it up-to-date.

References:

- Using RPSL in Practice - http://tools.ietf.org/html/rfc2650
- Using the RIPE Database as an Internet Routing Registry - https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry

5. Recommended Actions

Action 2: Prevent traffic with spoofed source IP addresses - Filtering

A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.

A network operator must test whether their network is able to send packets with forged source IP addresses using the CAIDA Spoofer Software. This is to alert the network operator as to whether their network might be used to originate Distributed Denial-of-Service (DDos) attacks, whilst generating publicly accessible information allowing that network to be checked by others.

Discussion:

Common approaches to this problem involve software features such as SAV (Source-Address Validation) on cable modem networks or strict uRPF (unicast Reverse-Path Forwarding) validation on router networks. These methods can reduce the administrative overhead in cases where routing and topology are less relatively dynamic. Another approach could be to use inbound prefix filter information to create a packet filter, that would allow only packets with source IP addresses for which the network could legitimately advertise reachability.

References:

CAIDA Spoofer Project - https://spoofer.caida.org

Network Ingress Filtering: Defeating Denial-of-Service Attacks which employ IP Source Address Spoofing - http://tools.ietf.org/html/bcp38

Ingress Filtering for Multi-homed Networks- http://tools.ietf.org/html/bcp84

Securing the Edge - http://www.icann.org/committees/security/sac004.txt

RIPE Anti-Spoofing Task Force HOWTO - http://www.ripe.net/ripe/docs/ripe-431

BGP Security Best Practices, FCC CSRIC III WG4FinalReport - http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Action 4: Facilitate routing information on a global scale - RPKI

A network operator should create a valid Route Origination Authorization (ROA) for each IP prefix or set of prefixes it is legitimately authorised and intends to originate.

Discussion:

The most secure method of facilitating validation on a global scale is through the RPKI system which allows their routing announcements to be cryptographically verified. Network operators can obtain RPKI certificates for their own IP prefixes from the RIRs that allocated them, and then generate, publish, and maintain Route of Origin Authorizations (ROAs) corresponding to the IP prefixes they announce. Network operators must also encourage their Customer Network operators to do so as well.

References:

- Origin Validation Operation based on the Resource Public Key Infrastructure (RPKI) - http://www.rfc-editor.org/bcp/bcp185.txt

6. Conformance Requirements

A network operator must generally fulfill the minimum requirements outlined in this section in order to be accepted as MANRS conformant and therefore eligible to be a MANRS participant. It is recognised however, that there can be legitimate reasons as to why some requirements cannot be met 100%, and exceptions may be granted where an adequate explanation is provided.

A network operator may become a MANRS participant if at least 50% of ASNs are MANRS conformant.

Action 1: Prevent propagation of incorrect routing information

Joining requirements:

A network operator must provide a detailed description of the following:

- If prefix filters are used, what are the mechanisms for generating them? If not, what kind of controls are used?
- How frequently are these filters are updated?
- What is the mechanism for checking that a customer legitimately holds the ASN and IP blocks they intend to announce?
- An ASN must be visible and announcing IP prefixes to the Internet's global routing system for a minimum of 3 months.
- An ASN must not have, in the previous 3 months, announced an AS number and/or IP prefix they or their customers are not legitimately authorised to originate.

Ongoing requirements:

A network operator must continue to maintain controls that prevent the announcement of AS numbers and/or IP prefixes they or their customers are not legitimately authorised to originate.

Action 2: Prevent traffic with spoofed source IP addresses

Joining requirements:

A network operator must run the CAIDA Spoofer Software on at least two network segments using public IP addresses, and the results must appear in the CAIDA Spoofer Database.

Ongoing requirements:

It is proposed that it becomes a requirement that a network operator should run anti-spoofer checks on an ongoing basis, preferably in an automated manner. This might take the form of a wider suite of conformance-checking software.

Action 3: Facilitate global operational communication and coordination

Joining requirements:

The contact information of a network operator will be checked for completeness upon application to become a MANRS participant, and a confirmation e-mail will be sent to the designated contact as listed in the application or as subsequently updated in the MANRS Observatory. The network operator must reply to this communication within 14 days in a manner that confirms the contact details are correct and demonstrates that communications are being actively read and responded to.

Ongoing requirements:

It is proposed that contact details will be checked for completeness and confirmation e-mails sent to the designated contact every three months thereafter.

Action 4: Facilitate routing information on a global scale

Joining requirements:

A network operator must have either have a publicly documented routing policy that includes all AS numbers and IP prefixes they advertise to other networks OR they have created valid Route Origination Authorizations (ROAs) for all IP prefixes or sets of prefixes they are legitimately authorised to originate.

Ongoing requirements:

A network operator must ensure they continue to publicly document all AS numbers and IP prefixes they intend to advertise to other networks OR they must create valid Route

Origination Authorization (ROAs) for all IP prefixes or sets of prefixes they are legitimately authorised to originate.

7. Failure to maintain minimum standards

It is important that network operators are not only conformant with the MANRS principles upon joining but also continue to demonstrate conformance on an ongoing basis. The value of MANRS towards improving the security and resilience of the Internet's global routing system is dependent upon its participants continuing to implement the Compulsory Actions at a minimum.

It is fully recognised that mistakes and false positives can occur, and that MANRS participants should be given every opportunity to provide explanations and undertake any necessary remedial actions if issues are identified. Nevertheless, there does need to be a process to handle situations whereby network operators fail to address routing security incidents, fail to respond to communications in a timely manner, or demonstrate persistent non-conformance with the MANRS Actions.

It is proposed to further describe the criteria for non-conformance on a per-action basis, timelines for taking corrective measures, and outcomes for persistent non-conformance.

8. MANRS Observatory

The MANRS Observatory (https://observatory.manrs.org/) collates data from publicly available data sources in order to track routing incidents and provide an overview of the state of global routing security. This data can also be displayed by region and country/economy, whilst MANRS participants may access data about their own network(s).

MANRS Observatory data is used to determine the level of MANRS readiness of network operators. For each of the Actions, a composite metric defines three states of conformance: Lagging (non-compliant), Aspiring (minor improvements are needed), and Ready.

The measurement framework and the thresholds are documented at https://observatory.manrs.org/#/about(Measurement Framework).

Acknowledgements

Andrei Robachevsky, Kevin Meynell, David Belson, Jean-Michel Combes, Rich Compton