Details

MANRS stands for Mutually Agreed Norms for Routing Security. Internet2 is a MANRS participant, as are several of our member institutions. MANRS outlines four simple but concrete actions that network operators should take.

Filtering

"Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity"

1. "Prevent propagation of incorrect routing information."
   a. Define a clear routing policy, reflected in your IRR information.
   b. Use prefix-lists to filter announcements from your customers.
   c. Use AS-PATH filters to help prevent route leaks.
   d. Verify that your customers own the ASNs and routes they are advertising to you.
2. You can use IRRs and RPKI (recommended) to produce prefix lists.
3. You can use RPKI and validators to tag valid, unknown, and invalid routes. Invalid routes that are signed by Network A but advertised by Network B.

Anti-spoofing

"Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure"

1. Run Spoofer.
2. Use uRPF, IP verify source, and/or access-lists.
3. Follow BCP38/84 and use prefix-filters at your border.
   a. Block all traffic **sourced from your IPs** from entering your border via the internet.
   b. Prevent all traffic that **is not sourced from your IPs** from leaving your network.
   c. Prevent all **RFC1918 addresses** from entering or leaving your network. (Extra points for blocking bogons!)
   d. If you have customer networks, use an IRR or internal documentation to only allow inbound traffic **sourced from that customer's IPs.**
   e. Don't forget IPv6!

Coordination

"Maintain globally accessible up-to-date contact information"

Update your contact information in ARIN, RADb, etc. How long has it been since you checked your phone number? Is one of your contacts retired by now? Has your office moved? Would it be a good thing to put a listserv email address instead of a single person's email? Update your Admin-C, Tech-C, and Zone-C!

Also, remember to update your contact info in PeeringDB!

Global Validation

"Publish your data, so others can validate routing information on a global scale"

MANRS requires the following updated information in the following places.

Object	Source	Description
aut-num	IRR	Policy documentation
route/route6	IRR	NLRI/origin
as-set	IRR	Customer cone
ROA	RPKI	NLRI/origin

https://www.manrs.org/isps/guide/global-validation/

Using an IRR to register your routes is a good thing. As major peers like Google and Hurricane Electric begin to use IRR information to inform their routing policies, this piece becomes more important. We encourage each of our members to work with their regional provider to ensure their information is correctly reflected in an IRR.

However, having your objects registered in an IRR does not mean you have provided irrefutable proof that you own these networks. Only signing your routes by creating ROAs, as part of the RPKI system, can provide irrefutable proof.