

Route Filtering at the Edge

AS15169

GORE 23

Arturo Servin



Background

- Pretty much self explanatory why routing security matters, but if you ask me to say ...
- Sending/receiving route hijacks, leaks, mitms, etc hurts

The problems



So in 2019

AS15169 will start to apply stricter filters to BGP announcements on all peering sessions

Route Data Sources

IRR, RPKI, <internal TE>

- IRR data for what peers think they will be sending
- RPKI data where available to validate IRR data
- Internal TE sources to limit further if required

The Plan

1. Notify peers (howdy!) that this is going to start happening
2. Collect data regularly (daily?)
3. Parse and place into internal data service
4. Create per-ASN filter content
5. Apply changes to network device(s)
6. Mark today, drop tomorrow

Notification

- <https://isp.google.com>
- Plans to enhance portal feature to display current data set for your ASN
- Implement ability to request 'update my filter because I updated my data' by peer(s)
- Feedback once this is working will be important!

How would we collect data?

- IRR data is relatively easy to find:
 - `ftp://ftp.radb.net/`
 - But there are others too ...
- Decide on which IRR databases to collect and parse
 - We will use RADB, RIPE, APNIC, AFRINIC, ARIN, CenturyLink and NTT
- If you need another one please let us know

Parse IRR data

- IRR data is generally formatted
 - Follow the AS -> Maintainer -> AS-SET trees...
 - 'Everyone' keeps theirs updated, right?
 - (these aren't really IRR problems as such)
- What tooling exists for this today?
 - Irrtoolset - no
 - Bgpq3 - not usable (internal problems)
 - Run a local IRRd... doesn't actually solve the problem of making the data available to the other tooling used
 - ISOC/MANRS is coordinating some data:
 - [github.com/manrs-tools/...](https://github.com/manrs-tools/)

Create per ASN filter

Vendor Neutral Formatting

- OpenConfig(OC) sounds right
- This is a request from the internal(google) service owners
- Output for configuration generation system in OC form
- Probably OC is fine
- Internal tooling already knows OC
- Policy application is a simple prefix-list and associated matching policies (v4/v6)

Applying and updating the filters

Apply Changes as Required

- When changes arrive, apply them in the normal fashion
- Follow existing device configuration processes
- New processes are bad/hard/problems

When

Goal is to start marking routes based on filter inclusion / exclusion by May 2019.

Reject/Drop by September 2019

FAQ

- I do not have any IRR object. Would AS15169 accept my prefixes?
 - No. If you do not have any IRR object AS15169 won't accept any routing data from the BGP session(s) with your ASN.
- I modified some IRR objects. How long would take Google to process it?
 - We automatically process new data every day, so allow a period of 24hrs for our systems to update. If you encounter any problem or you have an emergency please contact the NOC.
- Where can I find more information and updates?
 - <https://peering.google.com> for general information
 - <https://isp.google.com> for specific information about your network

What else are we working on?

- Preventing ourselves from being the leaker (making progress!)
- Signing ROAs and studying data
- Implementing this into our peering policy
- MANRS

How do I peer with AS15169?

- Check your PeeringDB record is up to date
- Check your IRR objects
- Make the request using a company valid email address
- Check our peering locations at <https://www.peeringdb.com/asn/15169>
- And then, only then go to <https://peering.google.com/iwantpeering>

Thanks!

arturoservin@gmail.com