Origin Validation Signaling

draft-ymbk-sidrops-ov-signal-02.txt

2019.03.26

randy@psg.com

Evaluator

- RPKI-enabled Origin Validation device
- With BGP feeds from other devices in the same PoP
- ROV evaluates the BGP announcements
- Signals Invalid announcements back to the devices which sent bad BGP
- So they can then drop Invalids

Why

- Better OV scale-out in a PoP if all devices do not have to do ROV, load RPKI cache
- More consistent ROV evaluation
- Same philosophy as Route Reflectors

Trust Boundary

- Only within a PoP
- This is not outsourcing trust
- Do not share with customers or friends

Devices send BGP, or maybe BMP, to Evaluator

Signaling Alternatives

- In-Band – Evaluator sends the BGP announcement back to the device with some coloring
- A new AFI/SAFI
- Augment the RPKI-Router protocol
- Create a whole new protocol

In-Band

- Send BGP back to originator of Invalid announcement
- Tag with the BGP Prefix Origin Validation State Extended Community per RFC8097
- Or some other way to color the announcement
- And the originator the drops the path

New AFI/SAFI

- Create a new AFI/SAFI
- Return Invalid BGP announcements back to sender marked with new AFI/SAFI
- Could contain high granularity info on why it is Invalid
- And the originator the drops the path
- But this is a lot of implementation

Augment RPKI-Router

- Add one or more PDUs to RFC6810
- Device is sending BGP to Evaluator
- Establish RPKI-Router between Evaluator and device
- Evaluator acts role of cache++
- Signals Invalid paths back to device
- And the device drops the Invalid path

Create a New Protocol

You're kidding, right?

All these have good and bad points

None are perfect or simple

But, as ROV deploys, it would be *really really* useful to have something in this space

The draft chose In-band Marking with the BGP Prefix Origin Validation State Extended Community