draft-ymbk-sidrops-ov-egress
origin validation for
egress filtering
and some related considerations

Rüdiger Volk
Deutsche Telekom

SIDROPS WG, IETF 104
March 26th 2019, Praha
overview

• what/where/why
• corner cases
• need to add? (my questions)
• your questions/comments
• ramblings beyond the draft...
origin validation filtering – where/why?

• “deploying RPKI” – “OV filtering policies”

• 1st order thinking was/is “protect my AS” from importing bad routes (OV invalid) and consequences

• 2nd order protect at all internal route generation/injection points (not so easy...)

• forgotten: final control of what you announce to the world (are you sure you solved 1st&2nd order perfectly?)

• are you acting responsibly as a network provider?

• embarrass yourself by relying on your neighbors to protect the world from your occasional bad routes?

• detect your bad routes seeing them not propagate via a neighbor or track damage done by the leaked route?
corner cases on egress

• egress policy is the final and robust point of control and origin validation is applicable but has corner cases

• MUST use effective origin AS as of post-policy and can be different from pre-policy RIB view

• confederation

• remove-private-as

• weird policy primitives manipulating AS-path

• weird AS-paths (e.g. mixed private/public ASNs)

• in absence of weirdness predicting effective AS looks easy
my questions — need to add... ?

• explain this does **not change** protocol?
  (standard ./. informational?)
  (**bug to be fixed** ./. feature request?)

• implementation considerations?
  (special primitive “apply drop valid” after policy?)

• operational considerations: **want** to easily access list of dropped invalids! alarms?

• ... reports about implementations being/becoming conformant?!?

• your questions/comments?
more thoughts following -ov-egress beyond/outside of the draft content

- have a clear understanding/definition/documentation which of your routes are meant for the DFZ or NOT
- do NOT do ROAs for routes NOT meant for DFZ!!!
- if you need to leak non-DFZ-routes to a neighbor you need agreement of controlled bypassing of OV filters policies
... another thought

- be prepared to regularly do special case bypassing of OV policy filters for routes not conforming to their intended appearance in the DFZ (e.g. for customers supported on private AS)

- the idea of internally tweaking the RPKI view (LTA and other tricks on the certificate system) probably has very limited applicability – unless you expect routers implementing a split horizon OV for egress and ingress/injection (how many different views?)
looking at AS numbers

- classification (using “delegated-extended”)
  - \(U\) – assigned by RIR to some User
  - \(I\) – IANA specials+pools
  - \(R\) – RIR blocked/pools
  - ? – User might want to block public use

- yesterday’s ROAs reference

<table>
<thead>
<tr>
<th>(\Sigma)</th>
<th>(U)</th>
<th>(I)</th>
<th>(R)</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>7277</td>
<td>7168</td>
<td>42</td>
<td>67</td>
<td>0/?</td>
</tr>
</tbody>
</table>
... and what do about it?

- on RPKI cache server can/should replace I/R/\?ASN in VRPs replace by ASo before feeding routers via rpki-rtr

- (???? find ways for AS-Owners to indicate “?”
i.e. disallowing the AS being used on public Internet!)