BGPsec Validation State Signaling

draft-borchert-sidrops-bgpsec-validation-signaling-00

IETF 104 Prague

O. Borchert, D. Montgomery
NIST
Proposal

• We propose to define a new opaque extended BGP community to carry the BGPsec path validation state within an autonomous system (AS).

draft-borchert-sidrops-bgpsec-validation-signaling-00
Validation State via Extended Community

• By signaling the BGPsec validation state of updates to iBGP peers, it may be possible for iBGP peers to reduce path validation workload.

• BGPsec routers could prioritize path validation resources for updates received over eBGP and those received over iBGP that have not yet been validated.

• Re-validating iBGP routes that have already been validated by other iBGP speakers in the AS could be given the lowest priority, or deferred completely.
RFC 8205: “defer validation”

• Section 5 of [RFC8205] (BGPsec Protocol Specification):

"... a BGPsec speaker MAY temporarily defer validation of incoming BGPsec UPDATE messages. The treatment of such BGPsec UPDATE messages, whose validation has been deferred, is a matter of local policy”.

• Note, as a result a BGPsec router may select and propagate in iBGP a route that has not been validated.
RFC 8205
“status of deferred messages is visible”

• Section 5 of [RFC8205] (BGPsec Protocol Specification):
  “...However, an implementation SHOULD ensure that deferment of validation and status of deferred messages is visible to the operator.”

• Omitting the extended community string does not specifically indicate that no validation was performed.
  • Note, the reason why no validation was performed is not relevant, just the fact that no validation was performed!

• The validation state “Unverified” proposed at IETF 103 allows to indicate to the operator that no validation was performed.
  See: draft-borchert-sidrops-bgpsec-validation-unverified-00
Questions

?  

oliver.borchert@nist.gov & dougm@nist.gov