Controlling Filtering Rules Using DOTS Signal Channel
draft-ietf-dots-signal-filter-control

IETF#105 Montreal, July 2019
K. Nishizuka, M. Boucadair, T. Reddy, T. Nagata
Changes Since Prague

- ACLs attributes may be included in a first mitigation request when an attack is detected or in an mitigation with adjusted scope
  - In both cases, a new “mid” must be used
  - Recommendation to first send a mitigation request without ACL attributes, and then a request with the ACL
    - Rationale: avoid delaying the mitigation when an error is encountered due to ACL processing
Changes Since Prague

• Add more details about the behavior of the DOTS agents
  – If the DOTS server does not find the ACL name included in a request, it replies with 4.04 (Not Found)
  – If the ACL is found
    • The activation type is updated
    • The lifetime is updated as if the request was received using data channel
  – If any failure is encountered to enforce the ACL update
    • Return 5.03 with failed ACL update in the diagnostic payload
    • The DOTS client must immediately send a new mitigation request without the failed ACL
Changes Since Prague

• When an attack evolves, acl-activation types may be adjusted by a DOTS client
  – deactivate an ACL, for example
  – a new “mid” is used
• When an attack is stopped, the DOTS client can use the data channel to retrieve the ACLs
  – Examples are added to the draft
• Further clarify that ACL-related actions are done using DOTS data channel when no attack is detected
• Update the security considerations
What’s Next?

• No issue is pending
• The content is stable
  – Request WGLC