DOTS Signal Channel and Data Channel drafts

https://tools.ietf.org/html/draft-ietf-dots-signal-channel-02

Prague, June 2017

Presenter: Nik Teague
DOTS Signal Channel and Data Channel drafts

• Addressed all comments received from the WG for both drafts
• Mitigation request
  – Replaced policy-id with mitigation-id

• Session channel session configuration
  – Replaced policy-id with session-id
• Alias can be created either using DOTS data channel or direct configuration

• DOTS server derives the DOTS client identity using the algorithm discussed in Section 7 of RFC7589 to couple DOTS signal and data channel sessions.
Next updates to draft-ietf-dots-signal-channel-02

• -1 value for lifetime parameter in mitigation request to indicate indefinite mitigation lifetime.

• Add a new parameter in the mitigation request to signal the DOTS server to initiate mitigation only after the DOTS server ceases to receive DOTS client signals.
Next updates for draft-ietf-dots-signal-channel-02

- Mitigation lifetime is negotiated in Mitigation request/response
  - Is there a need to negotiate mitigation lifetime during the DOTS signal channel session configuration?
• Extended the “ietf-access-control-list” ACL YANG data model in https://tools.ietf.org/html/draft-ietf-netmod-acl-model-11 to handle fragments and support rate-limit action.
• YANG module structure

```yaml
module: ietf-dots-access-control-list
    +-- (rate-limit)
      +-- rw rate-limit? decimal64
  augment /ietf-acl:access-lists/ietf-acl:acl/ietf-acl:access-list-entries/ietf-acl:ace:
    +-- rw fragments? empty
```
Filtering fragments to defend against DDoS attacks that use only noninitial fragments.

- For Layer 3 ACL entry with fragment parameter
  - Noninitial fragment matching the ACL entry, action associated with the ACL entry will be enforced.
  - Initial or non-fragment matching the ACL entry, the next ACL entry will be processed.

- For Layer 3 and Layer 4 ACL entry with fragment parameter
  - In the deny action case, instead of denying a non-initial fragment, the next ACL entry is processed.
  - In the permit action case, it is assumed that the Layer 4 information in the non-initial fragment, if available, matches the Layer 4 information in the ACL entry.
Comments and suggestions are welcome for both drafts.