Suricata - Feature #4174

tracking: app-layer frame inspection support


<table>
<thead>
<tr>
<th>Status:</th>
<th>In Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Effort to make it possible to avoid raw tcp data inspection. Many rules looking for application records make assumptions about pdu's aligning with packets.

Rules should be able to do something like alert ftp ... (frame:ftp.command; content:"USER"; ...).

Frames should be defined by the app-layer parsers.

**Subtasks:**

- Task # 4871: tracking: implement frames for all parsers
- Feature # 4872: nfs: add stream app-layer frame support
- Feature # 4904: dcerpc: add stream app-layer records support
- Feature # 4905: smtp: add stream app-layer frame support
- Feature # 4906: ftp: add stream app-layer frame support
- Feature # 4984: dns: add frames support
- Feature # 4985: quic: support frames
- Feature # 4986: postgresql: support frames
- Feature # 5036: sip: add frames support
- Feature # 4976: frames: implement/complete profiling support
- Optimization # 4977: frames: gap handling in inspection
- Feature # 4979: frames: implement dynamic logic to disable frames of a type
- Feature # 4980: docrames: document frame rule keyword
- Feature # 4981: frames: add general <app_proto>.stream frames
- Feature # 4983: frames: support UDP
- Optimization # 4987: frames: unify handling of getting frame data, flags
- Feature # 4988: frames: logging improvements
- Feature # 4982: frames: selective frame logging
- Feature # 4989: eve/alert: make frame logging configurable
- Feature # 4990: eve/frames: make payload logging configurable
- Feature # 5051: output/frames: allow tx logging to reference frames
- Feature # 5049: detect/frames: allow mixing with txs
- Task # 5050: rules/frames: settle on rule syntax

**Related issues:**

- Related to Task #4097: Suricon 2020 brainstorm
- Related to Documentation #4697: devguide: document app-layer frame support
- Related to Task #4772: tracking: parity between fields logged and fields avai...
- Related to Documentation #4697: devguide: document app-layer frame support added

#3 - 10/11/2021 02:09 PM - Victor Julien
- Status changed from Assigned to In Progress

#4 - 12/15/2021 09:17 AM - Victor Julien
- Related to Task #4871: tracking: implement frames for all parsers added

#5 - 12/15/2021 09:18 AM - Victor Julien
- Subject changed from tracking: app_record / pdu inspection support to tracking: app-layer frame inspection support
- Description updated

#6 - 04/25/2022 12:20 PM - Victor Julien
- Related to Task #4772: tracking: parity between fields logged and fields available for detection added