Suricata - Task #5050

Feature # 4174 (In Progress): tracking: app-layer frame inspection support

rules/frames: settle on rule syntax

02/08/2022 09:49 AM - Victor Julien

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

> Currently frames are accessed through a frames keyword. We could also allow using the frame names directly in rules, like alert sip ... (request_line; content: "REGISTER"; (...). This needs more thought about how it ties in to other rule syntax.

See also [https://github.com/OISF/suricata/pull/6915/commits/ae71c5813fd77d22a5e03b71b1012d670b13b698](https://github.com/OISF/suricata/pull/6915/commits/ae71c5813fd77d22a5e03b71b1012d670b13b698)

### Related issues:
- Related to Task #5181: detect/engine-analyzer: add rule analyzer warnings about rules that could use the frame keyword/semantics/feature added
- Related to Documentation #4705: userguide: add sections about frame support added

### History

#### #1 - 03/07/2022 06:08 PM - Juliana Fajardini Reichow
- Related to Task #5181: detect/engine-analyzer: add rule analyzer warnings about rules that could use the frame keyword/semantics/feature added

#### #2 - 03/07/2022 06:22 PM - Juliana Fajardini Reichow
- Related to Documentation #4705: userguide: add sections about frame support added