Suricata - Feature #4986
Feature # 4174 (In Progress): tracking: app-layer frame inspection support
Task # 4871 (New): tracking: implement frames for all parsers

postgresql: support frames
01/18/2022 08:04 AM - Victor Julien

<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>Juliana Fajardini Reichow</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>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

Related issues:
Related to Feature #4241: Protocol support: PostgreSQL (pgsql) Closed

History
#1 - 01/18/2022 06:30 PM - Juliana Fajardini Reichow
   - Related to Feature #4241: Protocol support: PostgreSQL (pgsql) added

#2 - 02/07/2022 03:28 PM - Juliana Fajardini Reichow
   - Status changed from Assigned to In Progress

#3 - 02/08/2022 09:47 AM - Victor Julien
   - Tracker changed from Task to Feature

#4 - 02/14/2022 12:08 PM - Juliana Fajardini Reichow
   A proposal for `pgsql` frame rule keywords:

   Introduction: `postgresql` app-layer protocol "header", when it is present, is basically a char (byte) to identify the message (sometimes its meaning is dependent of further message contents and/or state) and a length field to inform message length. With that in mind, we propose the following frame keywords for `pgsql`:

   From the client:
   - `request`: any message from the client
   - `startup`: specific for when the client tries to connect to the server
   - `query`: specific for query commands
   - `copy_data`: specific for COPY subprotocol*

   From the server:
   - `response`: any message from the server
   - `data_row`: specific for results of SELECT queries
   - `copy_data`: specific for COPY subprotocol*

   Usage: these work with keywords that go with sticky buffer. Example:

   ```
   alert psql $EXTERNAL_NET any -> any any (msg: "pgsql: external select attempt"); frame:pgsql.query; content:"select"); sid:1; rev:1);
   ```

   The `query`, `data_row` and `copy_data` keywords could be used to identify specific contents at risk of data breaches, as an example.

(*) Reference: https://www.postgresql.org/docs/14/protocol-flow.html#PROTOCOL-COPY

07/17/2022