Suricata - Feature #4854

Feature # 4566 (New):  pgsql: add subprotocol-states

pgsql: Add COPY subprotocol-state

11/25/2021 11:06 AM - Juliana Fajardini Reichow

| Status:   | New               |
| Priority: | Normal            |
| Assignee: | Juliana Fajardini Reichow |
| Category: |                  |
| Target version: | 7.0rc1            |
| Effort:   |                  |
| Difficulty: |                |

Label:  

Description

When the postgresql backend sends or receives the following commands:
- "COPY FROM STDIN"
- "COPY TO STDOUT"
It enters the COPY subprotocol-state, which comprises a different set of messages.

Currently, if Suri has the pgsql app-layer enabled and sees one of those messages, it doesn't know what to do and stops parsing pgsql messages from that flow altogether, afterwards.

PostgreSQL documentation: [https://www.postgresql.org/docs/14/protocol-flow.html#PROTOCOL-COPY](https://www.postgresql.org/docs/14/protocol-flow.html#PROTOCOL-COPY)

History

#1 - 11/25/2021 04:03 PM - Juliana Fajardini Reichow
- Subject changed from PGSQL app-layer-parser: Add COPY subprotocol to PGSQL app-layer-parser: Add COPY subprotocol-state
- Description updated

Updating this to better word that these are postgresql subprotocols, which are somewhat interpreted as sub-states, by Suri.

#2 - 11/26/2021 06:50 AM - Victor Julien
- Subject changed from PGSQL app-layer-parser: Add COPY subprotocol-state to pgsql: Add COPY subprotocol-state