Suricata - Feature #4566
pgsql: add subprotocol-states

07/27/2021 01:32 PM - Juliana Fajardini Reichow

Status: New
Priority: Normal
Assignee: Juliana Fajardini Reichow
Category: Target version: 7.0rc1
Effort: Label: Protocol

Description
In order to keep adding PostgreSQL support in Suricata, cover sub-protocol states:
- Extended query
- COPY operators
- Replication
- Function call
- Termination

Even though PostgreSQL refers to those as sub-protocols, to Suri, they're more like sub-states, where we'll expect to parse different sets of messages.

These could then be used in some Detect situations as well.

More details about each sub-protocol can be found in the protocol official documentation:
https://www.postgresql.org/docs/13/protocol-flow.html

Subtasks:
Feature # 4854: pgsql: Add COPY subprotocol-state

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

History
#1 - 07/27/2021 01:33 PM - Juliana Fajardini Reichow
- Assignee set to Juliana Fajardini Reichow

#2 - 07/27/2021 01:33 PM - Juliana Fajardini Reichow
- Related to Feature #4241: Protocol support: PostgreSQL (pgsql) added

#3 - 11/25/2021 03:33 PM - Juliana Fajardini Reichow
- Subject changed from Protocol support: PostgreSQL - add subprotocols to Protocol support: PostgreSQL - add subprotocol-states
- Description updated

Updating to better explain what sub-protocols meant, here.

#4 - 11/26/2021 06:51 AM - Victor Julien
- Subject changed from Protocol support: PostgreSQL - add subprotocol-states to pgsql: add subprotocol-states