Suricata - Feature #4241

Protocol support: PostgreSQL (pgsql)

12/28/2020 09:17 PM - Jason Ish

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

Description

Add support for the PostgreSQL protocol. Not only will this add support for PostgreSQL but other databases that use the PostgreSQL wire format like CockroachDB, and I believe there are others.

The protocol is documented here: https://www.postgresql.org/docs/13/protocol.html

Initial basics should include support for:
- connection username and database
- queries

Thought should be given to what could be normalized in terms of detection keywords and logging with other database protocols, such as MySQL.

Subtasks:

Optimization # 4991: pgsql: convert parser to nom7 functions  
Closed

Related issues:

Related to Feature #4566: pgsql: add subprotocol-states  
New
Related to Feature #4986: postgresql: support frames  
In Progress

History

#1 - 12/30/2020 02:59 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Juliana Fajardini Reichow
- Target version set to 7.0rc1

#2 - 05/12/2021 09:40 AM - Juliana Fajardini Reichow
- Status changed from Assigned to In Progress

#3 - 07/27/2021 01:33 PM - Juliana Fajardini Reichow
- Related to Feature #4566: pgsql: add subprotocol-states added

#4 - 08/23/2021 12:58 PM - Juliana Fajardini Reichow
- Priority changed from Normal to High

#5 - 01/17/2022 03:13 PM - Juliana Fajardini Reichow
- Subject changed from Protocol support: PostgreSQL to Protocol support: PostgreSQL (pgsql)
- Status changed from In Progress to In Review

PR under review: https://github.com/OISF/suricata/pull/6799

#6 - 01/18/2022 06:30 PM - Juliana Fajardini Reichow
- Related to Feature #4986: postgresql: support frames added

#7 - 01/20/2022 01:26 PM - Juliana Fajardini Reichow

07/16/2022 1/2
Merged with: https://github.com/OISF/suricata/pull/6822

#8 - 04/25/2022 12:28 PM - Victor Julien
  - Status changed from In Review to Closed