Suricata - Feature #716

configurable packet_stats.csv and packet_stats.log

01/12/2013 10:07 AM - Peter Manev

Status: New
Priority: Normal
Assignee: Community Ticket
Category:
Target version: TBD
Effort:
Difficulty:

Description
Just like we can configure stats.log
Currently if enabled on high traffic - packet_stats.csv can get to 1GB in size in under 10 min.

This(packet_stats.csv/log) is very beneficial in terms that one can actually profile the entire network traffic as well.

History
#1 - 01/14/2013 06:42 AM - Victor Julien
At this point this profiling facility is not meant to be used in live traffic situations. It produces way too much data for that.

#2 - 01/15/2013 03:54 AM - Peter Manev
Maybe we can make use of a socket?

#3 - 10/26/2013 10:21 AM - Victor Julien
- Target version set to TBD

#4 - 01/01/2016 06:16 PM - Andreas Herz
- Assignee set to OISF Dev

#5 - 01/02/2016 03:27 AM - Peter Manev
I am wondering if this can not be made configurable interval wise - like stats.log.

#6 - 11/28/2018 07:01 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous

Not really seeing the use case, but open to considering more ideas.

#7 - 11/28/2018 07:08 AM - Peter Manev
Not seeing it too beneficial with csv output.

#8 - 02/23/2019 10:11 PM - Andreas Herz
- Assignee set to Community Ticket