Suricata - Feature #2410
Create a reset counter and track maximum number of parallel flows

01/12/2018 05:53 AM - Maurizio Abba

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

Description
This feature introduces a new kind of counter that gets reset every time it's dumped. This feature is controlled by a flag, STATS_FLAGS_RESETTING, enabling the reset of the counter after running StatsOutput (or its equivalent StatsOutputCounterSocket).

History
#1 - 01/15/2018 05:48 AM - Maurizio Abba
UPDATE: after a first PR (https://github.com/OISF/suricata/pull/3146) I will modify the feature to provide both the new counter type and a counter that use this new feature (reset after every dump).
This counter will report the maximum number of parallel flows Suricata is tracking. This counter is updated every time a flow is created/destroyed.

#2 - 01/15/2018 05:48 AM - Maurizio Abba
- Subject changed from Create a counter that gets reset after every dump to Create a reset counter and track maximum number of parallel flows

#3 - 01/20/2018 06:16 PM - Andreas Herz
- Target version set to TBD

#4 - 09/27/2019 07:58 AM - Victor Julien
- Status changed from Assigned to New
- Assignee changed from Maurizio Abba to Community Ticket

The reset counter concept can perhaps also be considered implemented by the 'delta' logging?