Suricata - Feature #2291

traffic-id: ruleset for traffic classification and bypass

11/27/2017 03:10 AM - Victor Julien

Status: Assigned
Priority: Normal
Assignee: Jason Ish
Category: Traffic classification and flow bypass
Target version: TBD
Effort:
Difficulty:

Label:

Description
As discussed at SuriCon Prague, the goal is to start creating a ruleset for traffic classification and flow bypass.
Classification is mostly to add metadata to alerts/flows.
Flow bypass is a performance optimization.
This ticket will likely spin into a separate 'sub project'.

Related issues:
Related to Task #2309: SuriCon 2017 brainstorm

History
#1 - 12/01/2017 05:04 AM - Victor Julien
  - Related to Task #2309: SuriCon 2017 brainstorm added

#2 - 11/16/2018 09:59 PM - Raymond Hansen
  Needs proper description and sufficient examples (specifically bypass examples).

#3 - 08/07/2020 02:15 PM - Victor Julien
  - Target version changed from 70 to TBD