The idea here is that in some cases it might be possible to pass the shunting info to another part of the network where the decision could be made to not send packets to Suricata for that flow. This would be very efficient from Suricata's point of view.

The request at suricon 2019 was a way to push these events to unix socket somehow.

Maybe the easiest way would be to create a new output for it, than could then log to file, redis, unix socket, etc. Perhaps even a eve event_type? Eve is multi-instance so it would be possible to have an dedicated eve to just push this new record type to unix socket, while having a separate eve for normal operations.

Related issues:
Related to Task #3288: Suricon 2019 brainstorm
Related to Feature #3316: Unix socket: support dumping flow table

History
#1 - 11/05/2019 10:52 AM - Victor Julien
- Parent task deleted (#3288)

#2 - 11/05/2019 10:52 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#3 - 11/05/2019 11:11 AM - Victor Julien
- Related to Feature #3316: Unix socket: support dumping flow table added

#4 - 11/09/2019 01:09 PM - Victor Julien
- Subject changed from Unix socket support to receive flow shunting information to Unix socket: support to receive flow shunting information
- Description updated