Suricata - Feature #3316
Unix socket: support dumping flow table
11/05/2019 11:10 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Description
Idea is to use the unix socket interface dump the flow table. This could be used to analyse the internal state of flows.
The conntrack tool from Linux/Netfilter could be an example.

Related issues:
- Related to Task #3288: Suricon 2019 brainstorm
- Related to Feature #3295: Unix socket: support to receive flow shunting information

History
#1 - 11/05/2019 11:10 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#2 - 11/05/2019 11:11 AM - Victor Julien
- Related to Feature #3295: Unix socket: support to receive flow shunting information added

#3 - 11/05/2019 11:12 AM - Victor Julien
Suggestions about use cases and things like syntax and such are welcome.

#4 - 11/05/2019 11:12 AM - Victor Julien
- Description updated

#5 - 11/05/2019 09:21 PM - Danny Browning
One thing as we were exploring saving flow state is that there is not currently a stable identifier for flows between suricata runs. If we plan to load the dumped flow table, flow hash_id will need to be stable (no seed), or support for community flow id will need to be added to flow as a way to marry dumped state and captured flows.