Suricata - Feature #1300
profiling: per flow recording of profiling data
10/10/2014 10:46 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>low</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

**Description**

Flows track number of packets, so adding a total ticks count would allow calculating an average.

We could then output (in the flow log):
- absolute and relative cost of a flow

Also, a simple keyword could perhaps match on this. Then we'd alert on overly expensive flows (and even drop/pass them?).

Both should greatly help debugging performance issues.

**History**

#1 - 10/12/2014 03:35 AM - Peter Manev
Great idea I think.

#2 - 01/01/2016 06:00 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#3 - 09/18/2018 07:14 AM - Victor Julien
- Effort set to low
- Difficulty set to medium

I think this would be quite easy now. Just capture the ticks within the lock of the FlowWorker and store that in the Flow in a new field.