Suricata - Bug #2258

rate_filter inconsistency: triggered after "count" detections when by_rule, and after count+1 detections when by_src/by_dst.

11/01/2017 12:45 PM - Ruslan Usmanov

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Ruslan Usmanov</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>4.1beta1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
When I trying to rate_filter by rule, the filter triggered on "count" detections. When I change rate_filter to by src/dst, program allows one more detection before triggering the filter.
In function ThresholdHandlePacketRule() (used on by_rule), event filtered when current_count >= td->count, but in corresponding code in function ThresholdHandlePacketHost() (used on by src/dst), event triggered when current_count > td->count.
This situation leads to inconsistency.

History
#1 - 11/30/2017 07:19 AM - Andreas Herz
- Assignee set to Anonymous
- Target version set to TBD

Are you interested in working on that part of the code?

#2 - 12/08/2017 02:56 PM - Ruslan Usmanov
Yes

#3 - 12/09/2017 03:37 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from Anonymous to Ruslan Usmanov

#4 - 12/12/2017 02:52 PM - Ruslan Usmanov
https://github.com/OISF/suricata/pull/3080

#5 - 07/17/2018 10:18 AM - Victor Julien
- Status changed from Assigned to Closed
- Target version changed from TBD to 4.1beta1

https://github.com/OISF/suricata/pull/3080