Suricata - Feature #4756

capture: support ips stats for all IPS capture methods

10/14/2021 01:05 PM - Victor Julien

Status: In Progress
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Target version: 7.0rc1

Description
NFQUEUE has

<table>
<thead>
<tr>
<th>Activity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips.accepted</td>
<td>203125723</td>
</tr>
<tr>
<td>ips.blocked</td>
<td>11980</td>
</tr>
<tr>
<td>ips.replaced</td>
<td>1</td>
</tr>
</tbody>
</table>

We need to also support this for AF_PACKET, NETMAP and other IPS implementations.

Related issues:
Related to Feature #4573: add IPS drop total to eve log output New

History
#1 - 10/14/2021 01:05 PM - Victor Julien
- Related to Feature #4573: add IPS drop total to eve log output added

#2 - 10/26/2021 12:40 PM - Jeff Lucovsky
- Status changed from New to In Progress

#3 - 10/28/2021 12:55 PM - Jeff Lucovsky
https://github.com/OISF/suricata/pull/6531