Suricata - Feature #721
full nfq zero copy mode
01/16/2013 08:13 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>Community Ticket</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty</td>
<td>high</td>
</tr>
</tbody>
</table>

Description
Currently the nfq lib doesn't support zero copy. Each "recv" call will overwrite an internal buffer, so that it's not possible to just keep a reference to this buffer.

In the single/workers runmodes this is not a problem, as all packets are processed before the next recv call.

But in auto/autofp recv, verdict and all other packet handling runs async, so we may have multiple recv calls before a packet is processed and verdicted fully. Therefore, these modes need to work on copies of the data.

Work is being done by the netfilter project to address this, once that is available, we can support zero copy for all runmodes properly.

History
#1 - 12/22/2015 04:56 PM - Andreas Herz
Victor Julien wrote:

Work is being done by the netfilter project to address this, once that is available, we can support zero copy for all runmodes properly.

Do you have more details on that?

#2 - 01/17/2016 06:44 AM - Victor Julien
Sadly, no. Florian, Eric and myself talked about doing a new nfq API but AFAIK nothing was implemented by any of us.

#3 - 11/29/2016 04:28 AM - Victor Julien
- Status changed from Assigned to New
- Assignee changed from Eric Leblond to Anonymous

#4 - 07/13/2018 08:14 PM - Victor Julien
- Effort set to medium
- Difficulty set to high

#5 - 02/23/2019 10:11 PM - Andreas Herz
- Assignee set to Community Ticket