Suricata - Feature #1348

OOBE -6- increasing max-pending-packets default value

12/23/2014 05:57 AM - Peter Manev

<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>Peter Manev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>

Label: 

Description
This is part of OOBE tickets line.
Out Of the Box Experience(OOBE) is aimed at providing better defaults values in suricata.yaml

- single: 128
- workers: 4096
- autofp: 32768 (or maybe 2048 * thread cnt)
- cuda: 64k

History

#1 - 01/01/2016 05:51 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to 70

#2 - 02/18/2019 11:07 PM - Andreas Herz
any thoughts what we should use nowadays?

#3 - 02/19/2019 06:11 AM - Victor Julien
- Status changed from New to Feedback
- Assignee changed from OISF Dev to Peter Manev

#4 - 05/28/2019 09:03 PM - Andreas Herz
Could we make it based on some other values so it will be calculated?

#5 - 05/28/2019 09:20 PM - Peter Manev
Think it makes sense to base it on number of threads somehow.

#6 - 09/24/2019 09:27 PM - Andreas Herz
I looked into that but couldn't find a proper way. One idea is to change the value to be per-thread but would brake too much.
Is there a value you think that would be safe to just use as a new default value?

#7 - 09/25/2019 07:31 AM - Victor Julien
The value is currently already per thread.

#8 - 09/25/2019 07:08 PM - Peter Manev
The challenge here is that we also need to be cautious as to for the situations where Suricata is run on very small devices. In those cases we would also want to offer good experience right out if the box.
I have been going back and forth (internally :) ) quite a few times on this. It seems it might be better to offer some sort of quick "perf guide" where a user can just adjust a few basic settings without needing to dive into advanced tuning.

#9 - 09/25/2019 07:39 PM - Andreas Herz
Well if someone is running suricata on a small device like raspi I would expect some knowledge/time to tune it. I would expect the default to match a "normal" system. I would suggest 32k or 64k as that shouldn't really have a huge impact right?
Well it is a good point what is a "normal" system and "normal" traffic? :) I would say going to 4/8 x times the current default should be ok though. Think it would still keep it all under .5G ram

- Target version changed from 70 to TBD