Packet loss and high tcp reassembly with upgrade to 5.x

We experience periods of packet loss at times when using Suricata 5.0.5 that we do not see in a 4.1.8 instance with the same traffic, hardware (on a separate host), and config. We had a previous case open in #3320 where adding the stream-depth with a value of 1mb on the SMB parser improved the situation, but we still experience the issue. The stats.tcp.reassembly_gap_delta value is also often much higher on the 5.0.5 version, especially during these times of high dropped packets. Finally, it may not be related or significant, but I have noticed too that stats.tcp.pkt_on_wrong_thread grows slowly on our 5.0.5 version (currently at 42) but has mostly been at 0 for our 4.1.8 instance.

The current comparison is not being done on our production sensors, so are lab boxes where I can make changes if needed. The 4.1.8 version in this case does not have Rust enabled. I have run the Rust enabled 4.1.8 version side-by-side the 5.0.5 instance and we still have these situations where the 4.1.8 with Rust has no drops but the 5.0.5 version does. However, the 4.1.8 version with Rust does seem to generally have more packet loss.

I will attach stats logs from two separate occasions where significant drops occurred on our 5.0.5 instance but did not occur on the 4.1.8 version. Note that it seems our packet counters may have rolled over because if you follow the deltas we have not had even close to a noticeable percentage of packets dropped on either host long term, save these bursts on the 5.0.5 and every now and then drops on both the 4.1.8 and 5.0.5 instance at the same time. *Note that the data is a few weeks old now as I was pulled away from this issue to work on something else but I can get more current data if needed.

One example of numbers is on 2021-02-01 22:48:16 on our 5.0.5 host we had 20,501,550 dropped packets where our 4.1.8 host had 0. The minute surrounding this time on both sides had several million packets dropped on the 5.0.5 host and none and the 4.1.8 as well. The strange thing is there also appears to be a burst in the number of packets received on the 5.0.5 host and if you subtract the difference, the number of packets between both hosts is closer, though the 5.0.5 one still has much lower numbers packets that are not dropped so it is still quite significant. The stats.tcp.reassembly_gap_delta peaks at 2021-02-01 22:49:56 at 60,844 on the 5.0.5 version but the 4.1.8 instance has 0 at this time and the surrounding period.

Another example is 2021-02-01 08:28:02 there were 9,885,141 drops on 5.0.5 and 4.1.8 had 0. At this same time the tcp reassembly gap was at 3862 on 5.0.5 and under 10 on 4.1.8.

We do have eve logs with the deltas enabled on stats, so if you would prefer those logs let me know. That is what we typically use for comparisons, but to avoid sending over alert data included in our eve logs I am including the stats logs and am hoping you have tools to read these.

I can also provide our config outside of Redmine.

Some additional info that applies to both 4.1.8 and 5.0.5 instances:
- CentOS Linux release 7.9.2009 (Core) / 3.10.0-1160.11.1.el7.x86_64 #1 SMP Fri Dec 18 16:34:56 UTC 2020 x86_64 x86_64 GNU/Linux
- 128GB memory
- (lscpu info) Model name: Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz, CPU: 40
- Pcap capture method (using --pcap command-line option) with workers runmode
- Myricom cards.

ProductCode Driver Version
10G-PCIE2-8C2-2S myri_snf 3.0.23.50919
#2 - 02/05/2022 09:56 PM - Andreas Herz
- Status changed from New to Assigned
- Assignee set to Eric Urban

It should also have improved much with 6.0.4 can you compare this again?

#3 - 02/24/2022 10:04 AM - Victor Julien
- Status changed from Assigned to Feedback

#4 - 02/25/2022 06:40 PM - Eric Urban
I cannot say for certain at this time, but it seems as though there is improvement. We still do have periods of loss that I feel was not something we experienced on 4.x. However, we no longer have any 4.x instances running alongside our 6.x versions so I cannot provide any absolute comparisons and am going off of memory (which may have its flaws :).)

We did upgrade to 6.0.4 earlier this month. I looked back when we were still on 6.0.2 and see 12, 10, and 9 weeks ago when we had significant sustained packet loss. This is based on our Myricomstats. There were a couple of weeks while still on 6.0.2 that did not look overly bad though and even a few weeks that looked better than weeks since we have upgraded to 6.0.4. For sure though while we have been on 6.0.4 we have had nothing close to those amounts of sustained loss at 12, 10, and 9 weeks ago on version 6.0.2. I will keep an eye on it and can try to remember to report back after more weeks pass.

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>suricata_5_0_5-stats_build_info.tar.gz</td>
<td>297 KB</td>
<td>02/12/2021</td>
<td>Eric Urban</td>
</tr>
<tr>
<td>suricata_4_1_8-stats_build_info.tar.gz</td>
<td>252 KB</td>
<td>02/12/2021</td>
<td>Eric Urban</td>
</tr>
</tbody>
</table>