Suricata - Task #3294

Test the maximum size for messages passed to the unix socket
11/01/2019 04:01 PM - Andreas Herz

<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>Jason Ish</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>

**Description**

When logging to unix dgram socket the max message size is 64k. Goal is to test what happens if the messages we generate exceed that and come up with recommendations for how to handle this case.

**Related issues:**

Related to Task #3288: Suricon 2019 brainstorm

**History**

#1 - 11/05/2019 10:52 AM - Victor Julien
- Parent task deleted (#3288)

#2 - 11/05/2019 10:52 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#3 - 11/05/2019 11:14 AM - Victor Julien
- Description updated

#4 - 11/06/2020 03:58 PM - Victor Julien

I think its safer to use the unix_stream option. Syslog output may have the same issue depending on which syslog daemon and network transport is in use. Should be documented.

#5 - 04/22/2021 05:31 PM - Jason Ish

On a modern Linux system I hit failures somewhere between 200000 and 250000 bytes. Interestingly, the failure was inside Suricata, not on the receiver. Too large of a write fails. I was unable to create the condition where the received message may be truncated. This is a good thing I suppose.

I do expect messages to be truncated when done over a UDP socket however, but we don't support that mode.

#6 - 04/22/2021 05:42 PM - Jason Ish

On FreeBSD the message size does appear be 65535 (at least by default). But like in Linux, the error is on Suricata's side where the message fails to send:

```
[100599] 22/4/2021 -- 11:40:00 [CS:logopenfile] -- <Warning> -- [ERRCODE: SC_ERR_SOCKET(200)] - Write error on Unix socket "/tmp/suricata": Message too long; reconnecting...
```

In my opinion we don't have an issue here to worry about. Suricata will clearly fail, and the option is to move to unix_stream, or a file out.

NOTE: I had to modify the code to generate messages this size, but it doesn't mean that a logging situation couldn't be created to get to this size.

#7 - 04/22/2021 06:05 PM - Jason Ish

Even 5000 bytes seems to large for FreeBSD (at least on a default install).

#8 - 04/23/2021 06:01 AM - Victor Julien

The error message should probably indicate that the user should switch to unix_stream? And/or that certain options should be disabled, like payload logging?