Suricata - Feature #352

Switching to message queuing system for output

10/19/2011 11:18 AM - Eric Leblond

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description

Actual threading model consider output modules as standard functions which are run synchronously in the life of a packet inside suricata. But logging functions involve I/O on disk or on the network. They thus can be really time expensive. There is a potential performance issue there because, the building the alert message trigger the locking of resources like flow. It will thus be interesting to switch:

- to asynchronous I/O operation OR
- to a message queueing system where an alert structure build from a copy of information is sent to the output modules.

History

#1 - 10/24/2011 10:56 PM - delta yeh
ZeroMQ maybe a candidate

#2 - 11/07/2011 11:37 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Eric Leblond
- Target version set to 1.3beta2

Message queueing a good idea. Lets implement this for 1.3.
Can you come up with a higher level design?

#3 - 04/10/2012 10:33 AM - Victor Julien
- Target version changed from 1.3beta2 to 1.4

#4 - 08/23/2012 03:11 AM - Victor Julien
- Target version changed from 1.4 to 2.0rc2

Lets discuss this in Amsterdam next month.

#5 - 07/09/2013 07:12 AM - Victor Julien
- Target version changed from 2.0rc2 to TBD

#6 - 10/23/2013 05:18 AM - Victor Julien
- Target version changed from TBD to 3.0RC2

#7 - 11/05/2014 04:50 AM - Victor Julien
- Target version changed from 3.0RC2 to Soon

#8 - 01/29/2016 04:28 AM - Victor Julien
We now support redis. Probably good enough for now?

#9 - 07/26/2017 04:35 AM - James Mistry
I'm interested in this as a way of using Suricata as a pre-filter for traffic/parse results to be passed to external software components - that are very loosely-coupled with Suricata - for more advanced/complex analysis in real-time.

Some things that would make this feature work well for this use case:

- Messages are serialised to a format that supports explicit/formal schemas, ideally that can be evolved in a backwards-compatible way. For example, Apache Avro or Protobufs.
- Output flow/packet parse results with alerts, as well as raw packet/session data, in a way that is cheap to de-serialise (e.g. avoid Base64).
- Control topics associated with messages within the signature.

I'm happy to have this feature assigned to me if that helps.

#10 - 07/17/2018 08:21 AM - Victor Julien
- Status changed from Assigned to New
- Assignee changed from Eric Leblond to Anonymous
- Target version changed from Soon to TBD
- Effort set to medium
- Difficulty set to high

Setting difficulty to high as this could severely impact perf if done wrong.

#11 - 02/23/2019 10:07 PM - Andreas Herz
- Assignee set to Community Ticket

#12 - 11/07/2019 11:06 PM - Jason Ish
I propose we close/reject this issue as it's something we often agree is not to be part of Suricata. Our queue is the disk, or the socket or named pipe (and whatever is at the end of that). And we have other issues to address specific performance issues of the logging output.

#13 - 11/09/2019 09:14 AM - Victor Julien
- Status changed from New to Closed
- Assignee deleted (Community Ticket)
- Target version deleted (TBD)
- Effort deleted (medium)
- Difficulty deleted (high)

Agreed, thanks Jason.