**Suricata - Optimization #5178**

Bug # 4941 (New): alerts: 5.0.8/6.0.4 count noalert sigs towards built-in alert limit

Optimization # 4207 (In Review): Use configurable or more dynamic @ PACKET_ALERT_MAX@

detect/alert: improve packet alert queue handling

03/07/2022 05:51 PM - Juliana Fajardini Reichow

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Juliana Fajardini Reichow</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>TBD</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

With the change from a fixed size to a configurable packet alert queue (max), some issues with how the current queue is handled were exposed.

Improve that, to ensure there are no memory leaks with the dynamic allocation of the packet alerts queue.

--------------

This task will most likely be done as a backports-only candidate, in favour of the approach proposed by #5123 from 7.0.x onwards.

**Related issues:**

- Related to Task #5179: stats/alert: log out to stats alerts that have been discarded from packet queue added
- Related to Task #5180: detect/alert: make sure that signatures with `drop` action are respected, even if the alert is discarded added
- Related to Optimization #5123: alerts: use alert queuing in DetectEngineThreadCtx added

**History**

#1 - 03/07/2022 05:54 PM - Juliana Fajardini Reichow
  - Related to Task #5179: stats/alert: log out to stats alerts that have been discarded from packet queue added

#2 - 03/07/2022 06:00 PM - Juliana Fajardini Reichow
  - Related to Task #5180: detect/alert: make sure that signatures with `drop` action are respected, even if the alert is discarded added

#3 - 03/07/2022 06:11 PM - Juliana Fajardini Reichow
  - Related to Optimization #5123: alerts: use alert queuing in DetectEngineThreadCtx added

#4 - 03/07/2022 06:13 PM - Juliana Fajardini Reichow
  - Description updated
  - Target version changed from 7.0rc1 to TBD

#5 - 03/10/2022 01:46 PM - Juliana Fajardini Reichow
  - Status changed from New to In Progress

#6 - 03/10/2022 04:03 PM - Juliana Fajardini Reichow
  - Status changed from In Progress to In Review

PR for review [https://github.com/OISF/suricata/pull/7133](https://github.com/OISF/suricata/pull/7133)