rate_filter doesn't honor "timeout" if it is longer than "seconds" parameter

11/01/2017 12:19 PM - Ruslan Usmanov

When rate_filter set with "timeout" longer than "seconds" (which is common configuration, see example in [http://suricata.readthedocs.io/en/latest/configuration/global-thresholds.html](http://suricata.readthedocs.io/en/latest/configuration/global-thresholds.html)), program restarts counting of detections when "seconds" expire after last detection, not when "timeout" expires.

In function ThresholdTimeoutCheck(), tv_timeout not taken into consideration, causing program to ignore this parameter and allowing the entry to expire.

---

Hi Ruslan, did you submit a fix for this ticket as well? I don't see the ticket number referenced in the commits you have in the tree.

Hi Julien, sorry for delay in the answer, I don't think I fixed this issue, created the ticket in order to address it later.

Are you willing to submit a PR for that?