According to https://redmine.openinfosecfoundation.org/issues/2093 if tcp session has a gap then suricata either hoping that next segment can fill the gap or attempting to resync and carry on.

Let's suppose that traffic for suricata comes from some mirror port, which sometimes can produce packet loss(because of poor network quality, high load on a switch or something similar that suricata cannot control). In this scenario tcp gap can occur and there is no way to fill it. Let's say we have modbus protocol or any other without gap parser support. After gap suricata will wait for lost segment until session will be closed, which could take a long time, and there is no way to inspect packet at app-layer during this time.

Is there any setting/workaround for this in suricata? Could I somehow reset tcp session after gap or something like this?

Related issues:
- Related to Task #3553: Tracking: enable GAP recovery for all TCP app-layer protocols added
- Related to Task #3554: modbus: support GAP recovery added

History

#1 - 03/25/2020 12:44 PM - Victor Julien
We're adding support for recovering after a gap to the various protocols. It's a tricky job to scan the traffic after a gap for the start of a new record. This has not yet been done for modbus.

#2 - 03/27/2020 08:45 PM - Victor Julien
- Related to Task #3553: Tracking: enable GAP recovery for all TCP app-layer protocols added

#3 - 03/27/2020 08:45 PM - Victor Julien
- Related to Task #3554: modbus: support GAP recovery added

#4 - 03/27/2020 08:46 PM - Victor Julien
- Status changed from New to Closed

Closing this. We're tracking the actual work in the related tickets #3553 and #3554