Suricata - Feature #3464
suricata-verify: Add unix-socket support
02/11/2020 09:12 AM - Shivani Bhardwaj

Status: Assigned
Priority: Low
Assignee: Jason Ish
Category:
Target version: QA
Effort:
Difficulty:

Description
suricata-verify should be able to test unix-socket commands.

History
#1 - 02/11/2020 09:15 AM - Victor Julien
  - Priority changed from Normal to Low

I wonder if we should split this ticket in 2:

1. be able to run the standard tests in unix socket (so instead of running suricata -r ... set up unix socket and run through suricatasc)
2. add special support for adding tests that interact with unix socket to test issues like #3448

#2 - 09/22/2020 05:12 AM - Shivani Bhardwaj
  - Assignee changed from Shivani Bhardwaj to Community Ticket

#3 - 01/29/2021 08:54 AM - Shivani Bhardwaj

Relevant conversation:

Victor Julien
In shell you would start suri to go into the background suricata .... & and then issue the commands, where you capture suri's PID so you can kill it after you're done.

But I think this isn't as nice as an error in the script can easily leave suri running.

Shivani Bhardwaj
I see. We could probably have a blanket try..except..finally block which makes sure that suri is killed (how barbaric!) even if there was an exception. Would it still miss any cases?

Victor Julien
That sounds sane to me. We'd first issue a shutdown over unix socket, and if suri is still running after that do a force kill and fail the test.

#4 - 04/19/2021 03:33 PM - Jason Ish
  - Assignee changed from Community Ticket to Jason Ish