Suricata - Task #3301

Research: Failover support within the current IPS implementation

11/01/2019 04:28 PM - Andreas Herz

Status: New
Priority: Normal
Assignee: Community Ticket
Category: 
Target version: TBD
Effort: 
Difficulty: 
Label: 

Description
Failover support would make sure that if there are multiple Suricata instances and one of those disappears, the other Suricata IPS instances would 'do the right thing'. What doing the right thing is is an open question. Some of the ideas:

- sync flow table so that flow tracking would stay active
- sync 'drop settings' per flow/host/etc
- sync thresholding
- datasets?

I think one of the first things that needs to be done is analyze how Suricata currently works in an IPS failover case.

Related issues:
Related to Task #3288: Suricon 2019 brainstorm

History
#1 - 11/02/2019 09:51 AM - Victor Julien
- Description updated
- Assignee changed from OISF Dev to Community Ticket

#2 - 11/03/2019 09:49 PM - Jason Ish
Existing fail over solutions may be worth looking into.

CARP is for failover of IP addresses for firewalls. It uses a virtual IP address for the firewall, then when one fails, the spare takes over that IP address. This might be re-useable as is in a IPS setup, especially if routing is used.

But CARP is only for the address redundancy. PF has a tool called "pfsync" (see https://www.openbsd.org/faq/pf/carp.html) that takes care of syncing the firewall state. This is probably a close example to what would be needed between 2 Suricata instances.

I'd also start by the bare minimum, perhaps stuff like datasets could be in a phase 2 on the understanding that failover may not sync all state.

#3 - 11/05/2019 10:51 AM - Victor Julien
- Parent task deleted (#3288)

#4 - 11/05/2019 10:51 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added