Suricata needs a "disable action ordering" option.

Forexample; with the pseudo ruleset as below, If drop action processed first, all packets to userGroup-25 will be dropped. If pass action processed first, drop rule for Others will not be processed. So that, suricata should process rules without reordering.

#Ruleset for userGroup-25
pass tls any any -> $userGroup-25 any (msg:"SSL Cert Denied"; tls.subject:"example.com"; sid:3230002; rev:1;)
pass tls any any -> $userGroup-25 any (msg:"SSL Cert Denied"; tls.subject:"example.net"; sid:3230004; rev:1;)
drop tcp any any -> $userGroup-25 any (msg:"Default Drop For userGroup-25"; sid:3230010; rev:1;)
...

#Rules for other userGroups
...

#Ruleset for Others
drop tls any any -> any any (msg:"SSL Cert Denied"; tls.subject:"example1.com"; sid:3230007; rev:1;)
pass tcp any any -> any any (msg:"Default Pass"; sid:3230011; rev:1;)

History

#1 - 01/05/2016 01:57 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 05/02/2017 04:11 PM - Andreas Herz
What order do you want to achieve? That's something you might want to solve when setting up the rules so that you have proper pass rules.

#3 - 05/02/2017 04:23 PM - Özkan KIRIK
Andreas Herz wrote:

What order do you want to achieve? That's something you might want to solve when setting up the rules so that you have proper pass rules.

The problem occurs when defining a default policy. I think the solution as you explain should be like

drop tls any any -> ![[$userGroup-25, $userGroup-23, $userGroup-24, $userGroup-21, ...] any (msg:"SSL Cert Denied"; tls.subject:"example1.com"; sid:3230007; rev:1;)

If this is ok, we can close this feature request.

#4 - 02/18/2019 10:47 PM - Andreas Herz
- Status changed from New to Closed

Hi, we're closing this issue since there have been no further responses.
If you think this bug is still relevant, try to test it again with the most recent version of suricata and reopen the issue. If you want to improve the bug report please take a look at