Suricata - Bug #5380
IPS: ip only rules, but with negated addresses not treated like pure ip-only rules in IPS context (6.0.x backport)
06/02/2022 04:06 PM - Jason Ish

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category:
Target version: 6.0.6
Affected Versions: 6.0.5

Description
Given 2 rules:

pass tcp $HOME_NET any -> $EXTERNAL_NET 80 (sid:1;)
drop ip any any -> any any (msg:"Drop everything else"; sid:2;)

the response packets to the HTTP flow are getting dropped by the drop rule, and not being allowed as expected. However, the return packets are passed as expected with the following rule:

pass tcp $HOME_NET any -> any 80 (sid:1;)

The different here is that $EXTERNAL_NET contains a negation, "!any" which means the rule as not processed as a pure IP only rule. Pure IP only rules have are setup such that the pass is applied to the flow. While this should happen for the IP-only-rule-with-negation, this logic is missing for this case.

Related issues:
Copied from Bug #5361: IPS: ip only rules, but with negated addresses not tre... Closed

History
#1 - 06/02/2022 04:06 PM - Jason Ish
- Copied from Bug #5361: IPS: ip only rules, but with negated addresses not treated like pure ip-only rules in IPS context added

#2 - 06/07/2022 05:57 AM - Victor Julien
- Assignee changed from Jason Ish to Victor Julien

#3 - 06/10/2022 11:37 AM - Victor Julien
https://github.com/OISF/suricata/pull/7495

#4 - 06/10/2022 11:38 AM - Victor Julien
- Status changed from In Progress to Closed