I am trying the new track "by_both" option for rule thresholding (https://github.com/OISF/suricata/pull/3056), but this option does not appear to work properly.

To test this option, I had created some test rules as follows:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"CUSTOM: HTTP Port Scan / DoS Abuse"; flow:to_server; flags: S; threshold: type both, track by_both, count 5, seconds 30; sid:4100005; nfq_set_mark:0x10/0x10;)
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"CUSTOM: SSL Port Scan / DoS Abuse"; flow:to_server; flags: S; threshold: type both, track by_both, count 5, seconds 30; sid:4100006; nfq_set_mark:0x10/0x10;)
alert tcp $HOME_NET any -> 50.56.19.116 80 (msg:"CUSTOM: TEST RULE"; flow:to_server; flags: S; sid:4100007;)
```

However, the "DoS Abuse" rule does not appear to be firing even though more than 5 SYNs have been seen by Suricata, as the log shows by me trying some rapid replays:

```
```

However, the "DoS Abuse" rule does not appear to be firing even though more than 5 SYNs have been seen by Suricata, as the log shows by me trying some rapid replays:

```
```

However, if I change the by_both option to by_src, then the rule would match successfully. This suggests to me that somehow the by_both option may not be working properly. This was tested on Suricata 4.0.5.

Thoughts?

History

#1 - 07/25/2018 05:40 AM - Victor Julien
This is a new feature in the 4.1 branch, so it's not part of 4.0.5. Did you not get parsing errors?

#2 - 07/26/2018 07:14 AM - David Lam
No parsing errors - didn't realize it wasn't in 4.0.5 yet - will give 4.1 a try - thanks.

#3 - 07/26/2018 08:23 AM - David Lam
Okay, looks like I am seeing the signature errors if I run suricata in the foreground (instead of the daemon service) - in 4.1rc1, it's still displaying
26/7/2018 -- 01:20:06 - <Notice> - all 8 packet processing threads, 4 management threads initialized, engine started.

26/7/2018 -- 01:20:06 - <Notice> - rule reload starting

26/7/2018 -- 01:20:06 - <Error> - [ERRCODE: SC_ERR_PCRE_MATCH(2)] - pcre_exec parse error, ret -1, string type both, track by_both, count 5, seconds 30

26/7/2018 -- 01:20:06 - <Error> - [ERRCODE: SC_ERR_INVALID_SIGNATURE(39)] - error parsing signature "alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"CUSTOM: HTTP Port Scan / DoS Abuse"; flow:to_server; flags: S; threshold: type both, track by_both, count 5, seconds 30; sid:4100005; nfq_set_mark:0x10/0x10;)", from file /usr/share/suricata/rules/CUSTOM.rules at line 13

26/7/2018 -- 01:20:06 - <Error> - [ERRCODE: SC_ERR_INVALID_SIGNATURE(39)] - error parsing signature "alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"CUSTOM: SSL Port Scan / DoS Abuse"; flow:to_server; flags: S; threshold: type both, track by_both, count 5, seconds 30; sid:4100006; nfq_set_mark:0x10/0x10;)", from file /usr/share/suricata/rules/CUSTOM.rules at line 14

26/7/2018 -- 01:20:11 - <Info> - 31 rule files processed. 16081 rules successfully loaded, 2 rules failed

Is this feature only in the final 4.1 version?

#4 - 07/26/2018 08:39 AM - Victor Julien
- Tracker changed from Bug to Feature
- Subject changed from Threshold Track by_both Not Matching to support 'by_both' in threshold rule keyword
- Assignee deleted (Ruslan Usmanov)
- Target version set to TBD
- Effort set to low
- Difficulty set to medium
- Affected Versions deleted (4.0.5)

I've checked the code and it seems 'by_both' is only implemented in one place: the rate_filter keyword that you can use in the threshold.config. So the above is expected behavior.

I'll change this into a feature ticket so it can be addressed.

#5 - 08/04/2018 09:25 AM - Victor Julien
- Assignee set to Anonymous

#6 - 02/23/2019 10:03 PM - Andreas Herz
- Assignee set to Community Ticket

#7 - 11/03/2019 04:38 PM - Todd Mortimer
- Status changed from New to Assigned
- Assignee changed from Community Ticket to Todd Mortimer

Addressed in #2694

#8 - 05/05/2020 05:41 PM - Todd Mortimer
- Status changed from Assigned to Resolved

#9 - 05/05/2020 05:48 PM - David Lam

Hi Todd - I just got an email saying it was resolved. Which version was this implemented in? Thanks.

#10 - 05/05/2020 06:54 PM - Todd Mortimer

David Lam wrote in #note-9:

Hi Todd - I just got an email saying it was resolved. Which version was this implemented in? Thanks.

It was merged in this PR: https://github.com/OISF/suricata/pull/4760 and tagged with 6.0.

#11 - 05/05/2020 06:58 PM - David Lam
Awesome thanks.

#12 - 05/06/2020 05:55 AM - Victor Julien

- Status changed from Resolved to Closed
- Target version changed from TBD to 6.0.0beta1