suricata reload not working after configuring rules in disable.conf

04/09/2020 05:12 AM - Manish Kumar

Status: Closed
Priority: Normal
Assignee:
Category:
Affected Versions:
Label:

Description
Topology
-------- -------- -------- -------- --------
LAN ----- suricata ----- WAN

Description
-----------
suricata reload was not working when we change the configuration files.

steps and observation
---------------------
1. Added emerging-scan.rules in enable.con and started the suricata.
2. Used pytbull to send attacks and i have observed the log(ET SCAN Suspicious inbound to mySQL port 3306) at fast.log.
3. I have removed the emerging-scan.rules and added in disable.conf, then reload the rules.
4. Again started sending attacks using pytbull and able to see the log at fast.log.
5. After going through suricata.yaml, seen flow timeout values and performed same test by waiting for 600s i.e tcp established time.
6. even changing flow timeouts and also defrag to no, observed same issue.
7. we are testing with NFQ.
Don't know why even after disabling the rule, rules are getting hit.

History
#1 - 04/09/2020 03:29 PM - Jason Ish
Can you please provide your enable.conf and disable.conf?
Are you running suricata-update after modifying your enable.conf and disable.conf, then telling Suricata to reload the rules?
Can you verify that Suricata is loading the rules managed by Suricata-Update? By default this would a single rule file at /var/lib/suricata/rules/suricata.rules?

#2 - 04/09/2020 03:42 PM - Victor Julien
- Priority changed from Immediate to Normal

#3 - 04/09/2020 05:17 PM - Manish Kumar
I am sorry, suricata reload is working properly, it was environment issue.

#4 - 04/09/2020 05:17 PM - Manish Kumar
Manish Kumar wrote in #note-3:

I am sorry, suricata reload is working properly, it was environment issue.

Thanks for your time.

#5 - 04/10/2020 08:35 AM - Victor Julien
- Tracker changed from Bug to Support
- Status changed from New to Closed
- Target version deleted (4.1.8)
- Effort deleted (high)