Suricata - Support #3428
fail-open config no effect
12/30/2019 07:44 AM - John Smith

Status: New
Priority: Normal
Assignee: John Smith
Category: 
Affected Versions: 
Label: 

Description
suricata version is 4.1.4.
run command: `suricata -c suricata.yaml -q 0`
In suricata.yaml, the nfq config:
mode: accept
fail-open: yes
But when I set the nf_queue size is 1, and send packets to test "fail-open" function, there is no effect. Packets were dropped when suricata couldn't keep pace.
I had saw the libnetfilter_queue source code and source_nfq.c. There is no problem in those code.
So I want to know some ways to solve the problem.
Thank you very much!

History
#1 - 12/30/2019 07:59 AM - John Smith
And the Linux kernel is 4.4

#2 - 12/30/2019 08:22 AM - John Smith
libs had been installed:
libnfnetlink-dev is already the newest version (1.0.1-3).
libnfnetlink0 is already the newest version (1.0.1-3).
libnetfilter-queue-dev is already the newest version (1.0.2-2).
libnetfilter-queue1 is already the newest version (1.0.2-2)

#3 - 12/31/2019 01:21 AM - John Smith
The rule in iptables is: `sudo iptables -A FORWARD -j NFQUEUE --queue-bypass`.
So when I use the "fail-open" and set the nf_queue max-leng to 1. Packets will be dropped.
But when I change the rule to: `sudo iptables -A FORWARD -j NFQUEUE`.
The "fail-open" function is ok!

#4 - 01/20/2020 08:23 PM - Andreas Herz
- Assignee changed from Victor Julien to John Smith

What kernel version are you running?