Suricata - Bug #4740
libnet error with reject action on pfSense
10/06/2021 04:29 PM - Orion Poplawski

Status: New
Priority: Normal
Assignee: 
Category: 
Target version: 
Affected Versions: 6.0.3
Effort: 
Difficulty: 
Label: 

Description
Running 6.0.3 on pfSense-plus 21.05.1. When I set a rule action to reject I get the following error in the suricata.log:

6/10/2021 -- 09:50:03 -- <Error> -- [ERRCODE: SC_ERR_LIBNET_WRITE_FAILED(147)] -- libnet_write_raw_ipv4 failed: libnet_write_raw_ipv4(): -1 bytes written (Invalid argument)

History
#1 - 10/06/2021 04:45 PM - Orion Poplawski
libnet version is 1.1.6_5,1

#2 - 10/06/2021 06:24 PM - Bill Meeks
I am the package maintainer for Suricata on pfSense. I can reproduce this error on a pfSense virtual machine running the current version of pfSense (which is based on FreeBSD 12.2-STABLE). However, I am unable to reproduce the error when testing with the exact same Suricata binary and YAML configuration on a plain-vanilla FreeBSD 12.2-STABLE virtual machine.

The fact the same Suricata binary works on one and not the other seems to somewhat vindicate Suricata as being at fault here. The version of the libnet shared library was also exactly the same on the two virtual machines. Investigation is continuing.

#3 - 10/07/2021 07:48 PM - Bill Meeks
Some further research on the pfSense end uncovered what looks like the solution. In my virtual machine testing, I could eliminate the error in pfSense by removing the default IPv6 gateway (when there was in fact no IPv6 address configured on the WAN interface). This testing was being done on the WAN interface.

I will leave it to the original poster to take action on this issue, but so far as I can tell the problem is unique to pfSense (and a particular setting inside pfSense itself). I do not believe Suricata is at fault here. The solution has been shared with the OP and others on the Netgate IDS/IPS forum (for pfSense).