

## pfSense - Bug #5257

### tcpdump is not working with zerocopy enabled (net.bpf.zerocopy\_enable=1)

10/05/2015 03:09 PM - Jim Pingle

<b>Status:</b>	Resolved	<b>Start date:</b>	10/05/2015
<b>Priority:</b>	High	<b>Due date:</b>	
<b>Assignee:</b>	Luiz Souza	<b>% Done:</b>	100%
<b>Category:</b>	Operating System	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	2.3	<b>Affected Architecture:</b>	All
<b>Affected Version:</b>	2.3		

#### Description

tcpdump is failing when zerocopy is enabled (net.bpf.zerocopy\_enable=1) which is the default.

Sample failure message:

```
: tcpdump -i em0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 65535 bytes
tcpdump: pcap_loop: BIOCROTZBUF: Capabilities insufficient
```

I had seen this a few weeks back but only on a vtnet interface. At the time, gnn found the bug in FreeBSD, but the fix does not seem to have made its way into pfSense 2.3 yet.

I've tried with multiple types of NICs (vmx, vtnet, em --real and virtualized, and re) -- same behavior on all. All on current snapshots.

#### History

##### #1 - 10/05/2015 08:22 PM - Chris Buechler

- Status changed from New to Confirmed
- Priority changed from Normal to High

seems to affect all interface types, physical hardware, VMs, virtual interfaces (PPPoE, GRE, gif)

##### #2 - 10/12/2015 09:51 AM - Luiz Souza

- Assignee set to Luiz Souza

##### #3 - 10/13/2015 10:24 PM - Luiz Souza

The recent fixes I did in bpf (that fixed the zerocopy buffers in bpf) caused this issue (now that tcpdump is really trying to use the zero copy buffers).

There is a disallowed ioctl in capsicum.

I'll submit the fix to upstream.

##### #4 - 10/14/2015 10:14 AM - Luiz Souza

Fix submitted to upstream: <https://github.com/the-tcpdump-group/tcpdump/pull/486>

##### #5 - 10/19/2015 04:30 PM - Luiz Souza

I am disabling the zero copy buffers in pfSense until all the raised issues are fixed in FreeBSD.

**#6 - 11/11/2015 02:41 PM - Luiz Souza**

- *Status changed from Confirmed to Feedback*

- *% Done changed from 0 to 100*

Workaround committed to 2.3.

Awaiting the next tcpdump release (and the hostapd fix) to enable the zero copy buffers again.

**#7 - 11/18/2015 05:19 PM - Chris Buechler**

- *Status changed from Feedback to Resolved*

fixed