Suricata - Bug #1925

FreeBSD+netmap can't capture PPPoE

10/18/2016 03:59 PM - Franco Fichtner

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Affected Versions:		**Difficulty:**	
Effort:		**Label:**	

Description

Hi,

Variants of PPPoE do not seem to work: traffic is passed cleanly without being inspected/dropped by the engine. We are not sure if Suricata itself or FreeBSD or both in combination will cause these issues.

Reports seem to indicate that this used to be working in FreeBSD 10.2 with Suricata 3.0, but as we are unable to reproduce in a lab env it's hard to narrow down at the moment.

OPNsense currently uses 3.1.2 and FreeBSD10.3.

What further logging / output can we gather from affected users to see what's happening?

```
igb0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=3ab<RXCSUM,TXCSUM,VLAN_MTU,JUMBO_MTU,VLAN_HWCSUM,TSO4,TSO6>
        ether xx:xx:xx:xx:xx:xx
        inet6 fe80::230:18ff:fec5:8cd1%igb0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
igb0_vlan35: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether xx:xx:xx:xx:xx:xx
        inet6 fe80::230:18ff:fec5:8cd1%igb0_vlan35 prefixlen 64 scopeid 0xa
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
        vlan: 35 parent interface: igb0
pppoe0: flags=289d1<UP,POINTOPOINT,RUNNING,NOARP,PROMISC,SIMPLEX,MULTICAST,PPROMISC> metric 0 mtu
1492
        inet6 fe80::230:18ff:fec5:8cd1%pppoe0 prefixlen 64 scopeid 0xb
        inet6 fe80::230:18ff:fec6:2554%pppoe0 prefixlen 64 scopeid 0xb
        inet xxx.xxx.x.xx --> xxx.xxx.x.x netmask 0xffffffff
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

Original threads:
https://forum.opnsense.org/index.php?topic=3630
https://forum.opnsense.org/index.php?topic=3795

History

#1 - 10/18/2016 04:03 PM - Victor Julien

Any chance we could get a pcap of the traffic?

#2 - 10/23/2016 04:50 PM - Andreas Herz

- Assignee set to Anonymous

- Target version set to TBD

Could you also add the information about how suricata is started/running?
And maybe some log output, check if any packets are received (see stats.log for example).

And did I read the 2nd thread correctly, that it's also an issue without PPPoE?

#3 - 09/06/2017 04:15 PM - Andreas Herz

- Status changed from New to Closed

Closed due to no response

#4 - 10/19/2017 12:57 AM - Victor Julien

- Target version deleted (TBD)