Hey Team,

I am currently running Suricata 4.1.5 inline in AF_Packet mode. I have the engine running in IPS mode, but I am still seeing traffic get through.

I am currently running in AF_Packet mode with details shown below:

```
[root@us4suricata1 ~]# suricata --dump-config | grep af.packet
af-packet = (null)
af-packet.0 = interface
af-packet.0.interface = em2
af-packet.0.threads = auto
af-packet.0.cluster-id = 99
af-packet.0.cluster-type = cluster_flow
af-packet.0.defrag = no
af-packet.0.use-mmap = yes
af-packet.0.mmap-locked = yes
af-packet.0.ring-size = 20000
af-packet.0.copy-mode = ips
af-packet.0.copy-iface = em1
af-packet.1 = interface
af-packet.1.interface = em1
af-packet.1.threads = auto
af-packet.1.cluster-id = 98
af-packet.1.cluster-type = cluster_flow
af-packet.1.defrag = no
af-packet.1.use-mmap = yes
af-packet.1.ring-size = 20000
af-packet.1.copy-mode = ips
af-packet.1.copy-iface = em2
af-packet.2 = interface
af-packet.2.interface = default
```

```
[root@us4suricata1 ~]# suricata --dump-config | grep stream
outputs.7.pcap-log.use-stream-depth = no
app-layer.protocols.modbus.stream-depth = 0
stream = (null)
stream.memcap = 64mb
stream.checksum-validation = yes
stream.inline = yes
stream.reassembly = (null)
stream.reassembly.memcap = 256mb
stream.reassembly.depth = 1mb
```

With the copy-mode set to ips and the stream.inline option set to yes, I would expect Suricata to be dropping alerts marked as "drop". However, the traffic is still passing through. Suricata is recognizing that packets should be dropped, as shown in the drop.log and eve.json alerts (I have attached screenshots). I can re trigger this alert by navigating to check.torproject.org in a web browser on my host machine, and even though Suricata is reporting the alert as "blocked", I can still hit the web server (I opened in a private browser to ensure the website was not cached). I also see an entry hit the drop.log file.

I used the command "suricata -c /etc/suricata/suricata.yaml --af-packet" to start the engine.
I have also attached my suricata.yaml file hoping that can provide any more detail to you guys.

Any help would be greatly appreciated as I have been left scratching my head for the last few days trying to figure out why traffic is not actually being dropped even though Suricata thinks it is.

Thank you for the help in advance and for you guys continuous deployment of this great tool!

Best Regards,
Taylor

History
#1 - 12/06/2019 10:49 PM - Andreas Herz
- Tracker changed from Bug to Support
- Status changed from New to Feedback
- Assignee set to Taylor Walton

Can you try http://testmyids.com/ with the rule 2100498 and convert it to drop?
From a first view I don't see an issue, only that you mmap-locked on one interface.

#2 - 12/06/2019 11:03 PM - Taylor Walton
- File interfaces.PNG added

Hey Andreas,

Thank for reaching out.

So I am wondering if my understanding of AF_Packet and Suricata is wrong.

I have Suricata sitting inline between a firewall and core switch. The core switch serves multiple vlans below it but all internal traffic routes:

internal host -> core switch -> (downstream interface em2) suricata (upstream interface em1) -> firewall -> Internet

And vice versa with traffic coming from the Internet.

I am trying to take advantage of the AF_Packet setting with my interfaces and I have "net.ipv4.ip_forward = 1"

Does traffic from an internal host hit the downstream interface (em2) -> Suricata evaluates the packet against a rule -> if rule is not a drop, copies the packet to the upstream interface (em1) -> passes to firewall and continues route to internet?

Or does the copy-mode in Af_packet work by copying packets over to an interface that serves the same network (almost like a span port) so the downstream interface would receive a packet -> copy to another downstream interface -> and then that interface will forward its received packets to the upstream interface?

When I start the Suricata engine with AF_Packet mode, I see no issues with traffic flowing through and Suricata evaluating it, but traffic Suricata marks as "dropped" still get through, looking like the traffic passes no matter what.

From what I see in the Suricata documentation, no iptables rules are needed when running Suricata so I am wondering if my understanding of AF_packet mode is just wrong.

I really appreciate any insight you guys can provide.

Thanks,
Taylor

#3 - 12/16/2019 04:49 PM - Vincent Li
Taylor Walton wrote:

Hey Andreas,

Thank for reaching out.

So I am wondering if my understanding of AF_Packet and Suricata is wrong.

I have Suricata sitting inline between a firewall and core switch. The core switch serves multiple vlans below it but all internal traffic routes:
internal host -> core switch -> (downstream interface em2) suricata (upstream interface em1) -> firewall -> Internet
And vice versa with traffic coming from the Internet.

I am trying to take advantage of the AF_Packet setting with my interfaces and I have "net.ipv4.ip_forward = 1".

I don't think ip_forward = 1 is needed. From my understanding, af-packet mode is like software bridge setup by suricata, no need to have ip_forward set which is kernel iptable setting.

Does traffic from an internal host hit the downstream interface (em2) -> Suricata evaluates the packet against a rule -> if rule is not a drop, copies the packet to the upstream interface (em1) -> passes to firewall and continues route to internet?

this seems correct

Or does the copy-mode in AF_packet work by copying packets over to an interface that serves the same network (almost like a span port) so the downstream interface would receive a packet -> copy to another downstream interface -> and then that interface will forward its received packets to the upstream interface?

I don't think a downstream interface need to copy packet to another downstream interface.

you can try the note suggested in https://redmine.openinfosecfoundation.org/issues/3377#note-1

#4 - 12/19/2019 09:12 PM - Andreas Herz
Taylor Walton wrote:

Does traffic from an internal host hit the downstream interface (em2) -> Suricata evaluates the packet against a rule -> if rule is not a drop, copies the packet to the upstream interface (em1) -> passes to firewall and continues route to internet?

yes

When I start the Suricata engine with AF_Packet mode, I see no issues with traffic flowing through and Suricata evaluating it, but traffic Suricata marks as "dropped" still get through, looking like the traffic passes no matter what.

Did you try the rule I suggested and convert it to "drop" instead of "alert" and test the command to trigger it?

From what I see in the Suricata documentation, no iptables rules are needed when running Suricata so I am wondering if my understanding of AF_packet mode is just wrong.

In that scenario iptables settings are not relevant.

You can also try to produce a pcap for that and run suricata -r foop.ccap --simulate-ips.

Files

eve_json_blocked.PNG    61.5 KB    12/03/2019    Taylor Walton
drop.log.PNG             13.8 KB    12/03/2019    Taylor Walton
suricata.yaml            72.6 KB    12/03/2019    Taylor Walton
interfaces.PNG           35.2 KB    12/06/2019    Taylor Walton