Suricata - Feature #3002
Flow and Netflow Not Logging ESP Traffic
05/31/2019 03:50 PM - Eric Urban

Status: Closed
Priority: Normal
Assignee: Emmanuel Thompson
Category:
Target version: 7.0rc1
Effort:
Difficulty:
Label: Protocol

Description

Summary
With both flow and netflow enabled in the eve log, I do not see any log entries for ESP traffic (IP protocol 50). If I create a rule to alert on ESP traffic, then there are alerts generated.

Details
I tested this running Suricata version 4.1.4 both with live ESP traffic and also in pcap offline mode. Neither produced any flow or netflow log entries in the eve log. The only protocols I found in flow/netflow after letting it run for some time were TCP, UDP, ICMP, IPv6, IPv6-ICMP, and SCTP. To confirm ESP traffic was being processed in some way by Suricata I added the following rule:

```
alert ip any any -> any any (msg:"IP Proto 50 (ESP)"; ip_proto:50; classtype:non-standard-protocol ; sid:10010002; rev:1;)
```

With the rule enabled there were alerts generated for the ESP traffic as expected.

I found a capture containing ESP traffic from [https://wiki.wireshark.org/SampleCaptures#IPsec_-_ESP_Payload_Decryption_and_Authentication_Checking_Examples](https://wiki.wireshark.org/SampleCaptures#IPsec_-_ESP_Payload_Decryption_and_Authentication_Checking_Examples) to use for testing. I will attach ipsec_esp_capture_1.tgz from that page for convenience and for historical purposes in case the link or content changes.

I enabled debug and found that when running through a pcap only containing ESP traffic that there were messages like "7/5/2019 -- 11:40:09 - <Debug> - packet 1 has flow? no", which I believe is a message from [https://github.com/OISF/suricata/blob/16643befe7bebb9736d44f3a02edf71135a7b84/src/flow-worker.c#L199](https://github.com/OISF/suricata/blob/16643befe7bebb9736d44f3a02edf71135a7b84/src/flow-worker.c#L199). When I used a capture containing additional packets that were logged in flow/netflow I saw output like "packet x has flow? yes". This is possibly a coincidence but when inspecting output-json-flow.c and output-json-netflow.c I see that both rely on data from the flow object, so I am wondering if this is a potential source of the problem?

Steps to reproduce

2. Extract the attached ipsec_esp_capture_1.tgz file and get ipsec_esp_capture1.tgz:/t1/capture.pcap.
3. (Optional) Add the ESP rule from above to confirm that Suricata is reading this traffic as ESP.
4. Run Suricata in pcap offline mode. The command I used was:

```
suricata -vv -c /etc/suricata/suricata.yaml --runmode autofp -k none --pidfile suricata.pid -l logging/ -r esp_capture_filtered.pcap
```

5. Check the log output to note that there are no flow or netflow entries for this traffic.

History

#1 - 05/31/2019 03:52 PM - Eric Urban
Issue was also submitted to mailing list. For reference see [https://lists.openinfosecfoundation.org/pipermail/oisf-users/2019-May/016905.html](https://lists.openinfosecfoundation.org/pipermail/oisf-users/2019-May/016905.html).

#2 - 05/31/2019 08:22 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to Support
Hi Eric, we don't specifically decode ESP currently. It's not hard to add though.

Question: what would be the flow? srcip/dstip/ipproto? Or should the ESP SPI field be mixed in? The latter would make implementation more tricky.

Hello Victor,

Our use case would be satisfied by either implementation. The srcip/dstip/proto/spi combo is preferable in cases where the two same endpoints would have multiple sessions open, so would be nice, but isn't not all that important for why we were looking into this feature in the first place. If that makes implementation more tricky, the SPI addition is maybe best suited as a separate feature enhancement request? I would be happy to file one if this issue turns into a feature request for implementing an ESP decoder.

Is there some where to find what protocols currently do show up in the flow/netflow logs? I assumed that for netflow logging if ESP or other IP protocols weren't being decoded that they would show up with the protocol IP (possibly with number) and be logged with minimal details.

- Tracker changed from Support to Feature
- Target version set to TBD
- Affected Versions deleted (4.1.4)

- Status changed from New to Closed
- Assignee changed from Community Ticket to Emmanuel Thompson
- Target version changed from TBD to 7.0rc1
- Label Protocol added

https://github.com/OISF/suricata/pull/5351 merged in https://github.com/OISF/suricata/pull/5743