Suricata - Support #2972
How can I get the mac at the NFQ mode
05/08/2019 06:58 AM - John Smith

Status: Closed
Priority: Normal
Assignee: 
Category: 
Affected Versions: 4.0.5

Description
When I start suricata as NFQ mode, as suricata -c /etc/suricata/suricata.yaml -q 0 -q 1. I can't get the mac address from the package, because if a package is from NFQ, there is no mac bytes when I use wireshark to get the package.

History
#1 - 05/08/2019 08:46 AM - Alexander Gozman
John Smith wrote:

When I start suricata as NFQ mode, as suricata -c /etc/suricata/suricata.yaml -q 0 -q 1. I can't get the mac address from the package, because if a package is from NFQ, there is no mac bytes when I use wireshark to get the package.

At best (AFAIK), NFQ can provide source MAC address but never a destination one (because it's unknown at the moment of capture).

#2 - 05/08/2019 03:08 PM - Victor Julien
- Target version deleted (4.1.4)

#3 - 05/08/2019 03:08 PM - Victor Julien
- Assignee deleted (Victor Julien)

#4 - 05/23/2019 09:24 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to Support

#5 - 05/24/2019 04:54 AM - Victor Julien
- Status changed from New to Closed
- Assignee deleted (Community Ticket)
- Target version deleted (Support)
- Difficulty deleted (high)