Hey Team,
I have a some misunderstanding such Suricata behavior purpose. In IPS mode, which use AF_PACKET Suricata drops some GRE packet.
How I can do, so that Suricata will ignore and bypass GRE traffic in IPS mode?

drop.log:

02/06/2020-11:08:39.354518: IN= OUT= SRC=<src_ip> DST=<dest_ip> LEN=64 TOS=0x00 TTL=253 ID=51883 PROTO=GRE Unknown protocol
02/06/2020-11:08:41.757095: IN= OUT= SRC=<src_ip> DST=<dest_ip> LEN=64 TOS=0x00 TTL=253 ID=57167 PROTO=GRE Unknown protocol
02/06/2020-11:08:42.891276: IN= OUT= SRC=<src_ip> DST=<dest_ip> LEN=64 TOS=0x00 TTL=253 ID=59688 PROTO=GRE Unknown protocol
02/06/2020-11:08:45.069087: IN= OUT= SRC=<src_ip> DST=<dest_ip> LEN=64 TOS=0x00 TTL=253 ID=64274 PROTO=GRE Unknown protocol
02/06/2020-11:08:47.539530: IN= OUT= SRC=<src_ip> DST=<dest_ip> LEN=64 TOS=0x00 TTL=253 ID=3785 PROTO=GRE Unknown protocol

For IPS mode you probably should look at 'pass' rules for that:

Thank you for quick answer. Yes, it's nice solution, but I faced with problem by adding bypass keyword in rule - segfault, like observed here https://redmine.openinfosecfoundation.org/issues/2953.
I have Suricata 5.0.0-dev (rev 69d0d484e), and will try to upgrade to 5.0.1.

For example, rule

alert ip any any <> any any (msg:"pass all service traffic GRE"; sid:1000002;ip_proto 47;noalert;bypass;)

Segfault message:

[1672076.320163] W#02-ens192[23770]: segfault at 40 ip 0000561353bee7c8 sp 0000?f57f50e3560 error 4 in suricata[561353b57000+47f000]

Just as a follow up. The rule above is missing "." after "ip_proto".

Out of curiosity is the result the same with the following rule and latest git:

pass ip any any <> any any (msg:"pass all service traffic GRE"; sid:1000002;ip_proto: 47;noalert;bypass;)