draft-boutros-nvo3-ipsec-over-geneve-00

Sami Boutros
Dan Wing
Calvin Qian
[VMware]

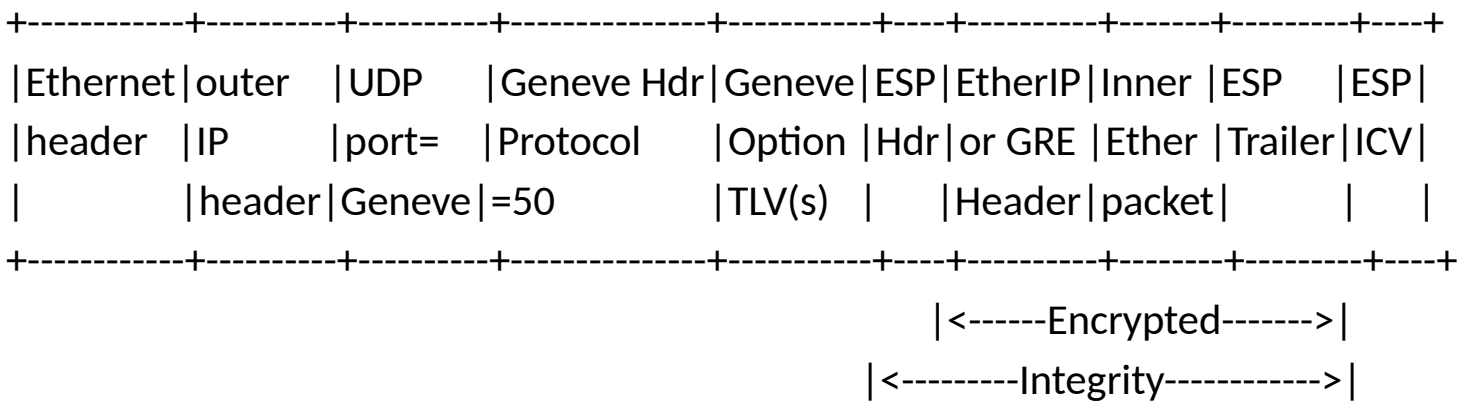
IETF 99, July 2017
Prague

What is this about?

Specifies how Generic Network Virtualization Encapsulation (Geneve) can be used to carry:

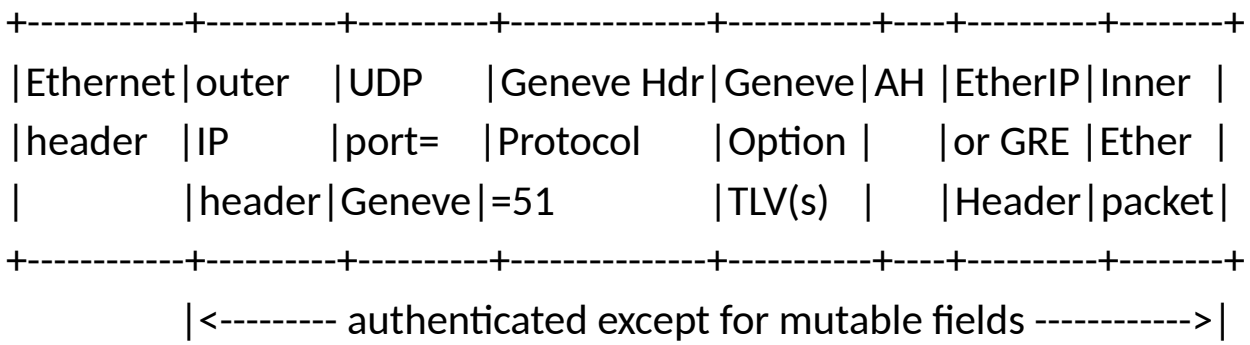
- IP Encapsulating Security Payload (ESP)
- IP Authentication Header (AH)

Encapsulation Security Payload (ESP) over Geneve tunnel



The ESP Next Header field will be set to inner payload protocol which can be either EtherIP (97) or to the Generic Routing Encapsulation (GRE) (47). The GRE protocol type will be set to the Ethernet protocol type.

IP Authentication header (AH) over Geneve tunnel



The AH Next Header field will be set to inner payload protocol which can be either EtherIP (97) or to the Generic Routing Encapsulation (GRE) (47). The GRE protocol type will be set to the Ethernet protocol type.

It is to be noted that some of the option TLV(s) in the Geneve header SHOULD be treated as mutable fields and not included in the AH authentication.

Control Plane Considerations

Network Virtualization Endpoint (NVE) to express the next protocol that can be carried by Geneve to its peers using control plane.

In this document the next protocol signaled in control plane by NVE(s) can be ESP or AH.

Once 2 NVE(s) agree to carry ESP or AH as next protocol, Security Association and Key Management Protocol defined in [RFC2408] can be used to negotiate, establish, modify and delete Security Associations. As well, mechanisms to perform key exchange defined in [RFC2409] can be used.

Next steps

- Seeking comments?

Thank you