Considerations for Adjustments of ESP Trailer

draft-pan-ipsecme-esp-trailer-adjustment

Wei Pan
Chenyuan Fang

IETF 118

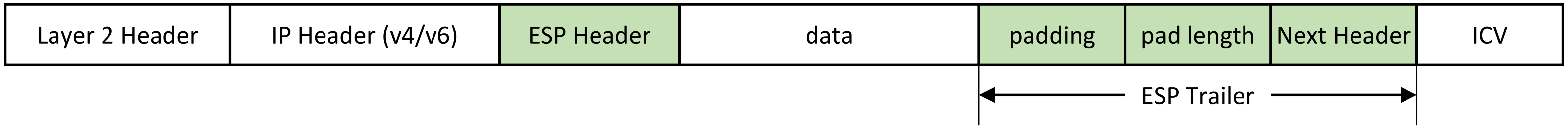
November 2023

Motivation

- To improve IPsec performance:
  - efficient algorithms, such as AES-GCM
  - cryptographic hardware acceleration
  - …
- Still not enough for high traffic bandwidth scenarios:
  - E.g., the **traffic between data centers can be Tbps or even higher**
- What can be considered?
  - MACsec [IEEE 802.1AE] can reach the line rate
    - The magic is that it’s totally implemented by hardware (not only the encryption/decryption operations)
  - **So, implementing the whole IPsec by hardware too**

Problem Statement

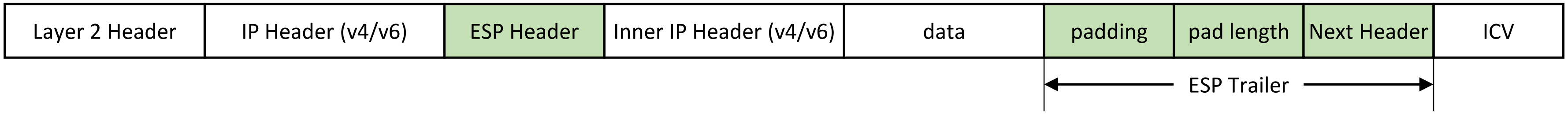
- Current ESP packet format
  - Transport mode



Layer 2 Header	IP Header (v4/v6)	ESP Header	data	padding	pad length	Next Header	ICV

ESP Trailer

  - Tunnel mode



Layer 2 Header	IP Header (v4/v6)	ESP Header	Inner IP Header (v4/v6)	data	padding	pad length	Next Header	ICV

ESP Trailer

- `Next Header` field decides how to reset the “next header” related fields in the L2 or IP header. But, it’s at the end of the packet...
- The chip must cache the packet before getting the Next Header field
  - **DECRYPT THEN TRANSMIT** cannot be achieved
  - **More chip area** is needed to implement caching
    - **More chip area means more energy consumption, which is not eco-friendly**

Possible Solution 1

- Super high IPsec performance is only needed at scenarios like data centers, and these scenarios usually use ESP tunnel mode.

- A solution for ESP tunnel mode: **Judge the type of inner IP header according to its first byte**
  - In ESP tunnel mode, it's an IP packet encapsulated after ESP header.
  - The first byte of IPv4 header or IPv6 header indicates the IP version, 4 for IPv4 and 6 for IPv6.

Advantage	· Easy to implement
Disadvantage	· Only ESP tunnel mode can be supported · Dummy Packet function cannot be supported

Possible Solution 2

- A solution for both mode: **Move the ESP trailer immediately after ESP Header**

- **Advantage** · Both ESP transport and tunnel modes are supported

- **Disadvantage** · Significant changes to ESP protocol

Further Considerations

- What’s the reason of putting ESP trailer at the end of the packet?
- Is this problem worth solving?
  - What solution is more reasonable?
  - Any other solution?