

ESP Header Compression (EHC)

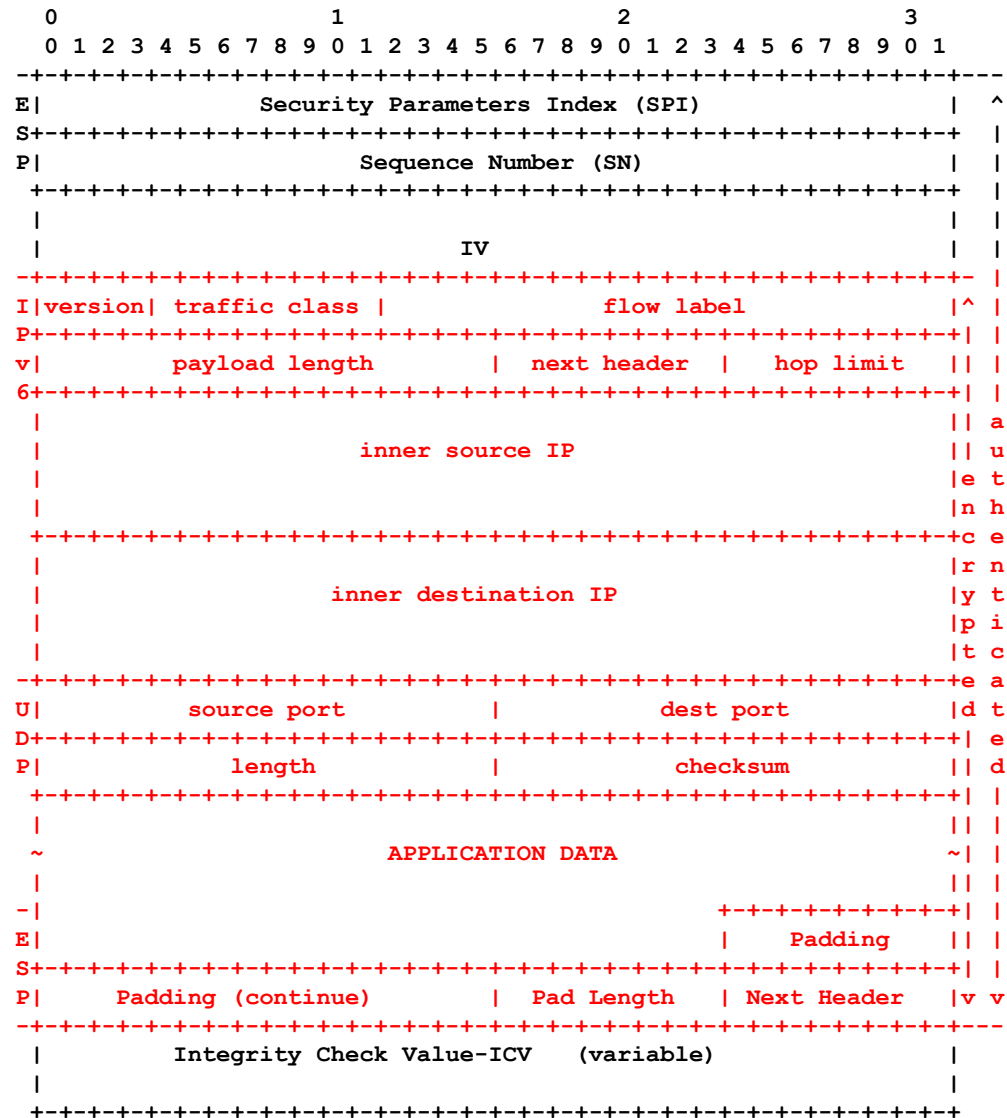
draft-mgmt-ipsecme-diet-esp-07

Tobias Guggemos

lpwan@IETF 104

26.03.2019

Problems when compressing

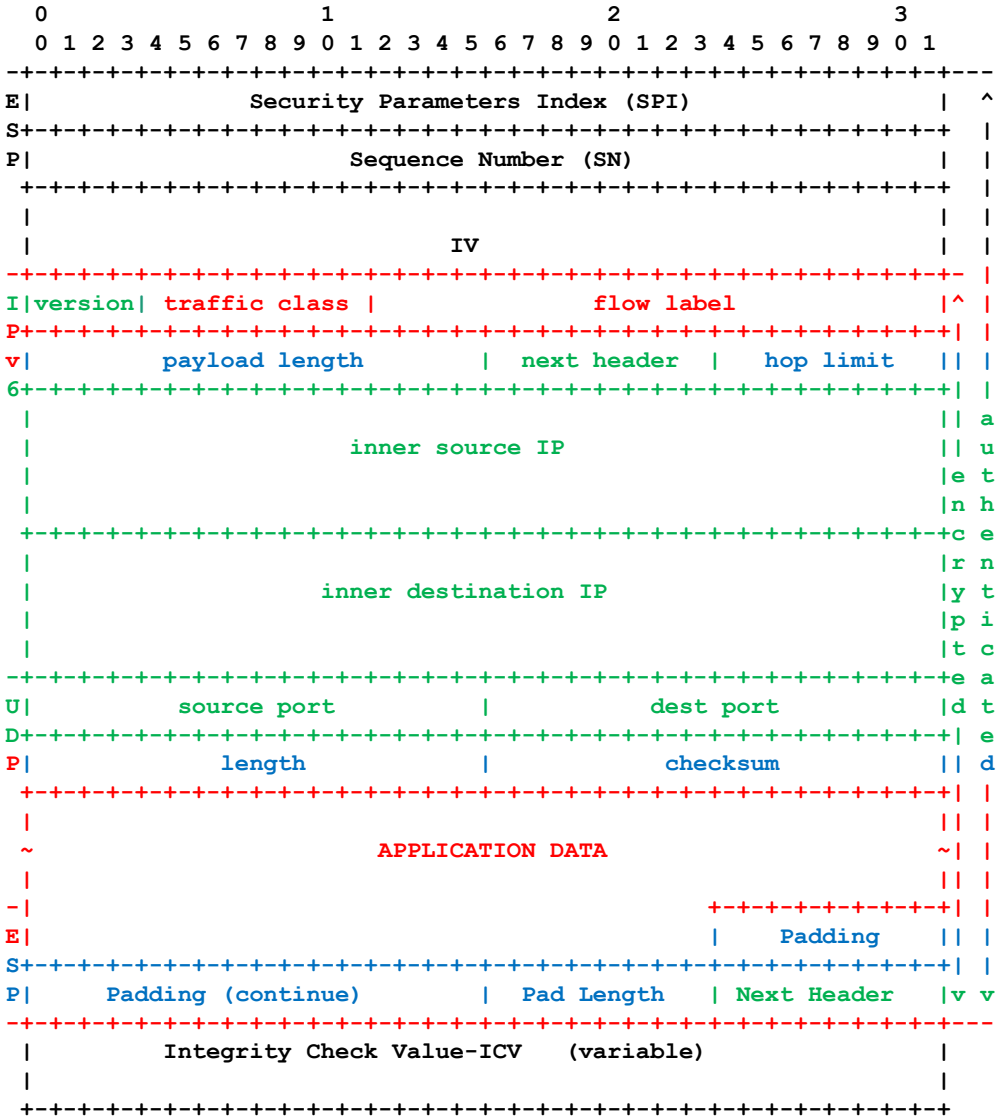


Example of an IP Tunnel

- Compression usually takes place between L2 and L3
- At that time, ESP payload is already encrypted

➔ Only ESP header can be compressed without touching the ESP implementation

ESP Header Compression



Example of an IP Tunnel

- Is already in the IPsec SA
- Can be calculated

ESP Header Compression (EHC)

- 😊 IPsec already has a **static** state (IPsec SAs)
 - 😊 IPsec already has a separate channel to agree on (and update) a state
 - IKEv2, G-IKEv2, (even HIP could be used)
 - Static
 - 😊 The state already holds some context (Traffic Selector)
 - 😊 We have done this before (ROH Cover IPsec RFC5856)
-
- We just need to define how to make use of it!

EHC Actions and Rules

Function	Compression	Decompression	EHC Rule	Field	Action	Parameters
send-value	No	No	IP6_OUTER	Version	elided	ip_version
elided	Not send	Get from EHC Context		Traffic Class	lower	
lsb(_lsb_size)	Sent LSB	Get from EHC Context		Flow Label	lower	
lower	Not send	Get from lower layer	IP6_VALUE	Version	elided	ip_version
checksum	Not send	Compute checksum.		Traffic Class	elided	ip6_tc
padding(_align)	Compute padding	Get padding		Flow Label	elided	ip6_fl
			IP6_LENGTH	Payload Length	lower	
			IP6_NH	Next Header	elided	l4_proto
			IP6_HL_OUTER	Hop Limit	lower	
			IP6_HL_VALUE	Hop Limit	elided	ip6_hl
			IP6_SRC	Source Address	elided	ip6_src
			IP6_DST	Dest. Address	elided	ip6_dst

- ➔ Inspired from ROHC and SCHC
- ➔ Defined for ESP/IPv6/IPv4/TCP/UDP/UDP-Lite
- ➔ EHC Strategy Diet-ESP is designed to optimize context exchange
- ➔ Compressing 44 header fields with 9 context values