ESP Header Compression (EHC)

draft-mglt-ipsecme-diet-esp, draft-mglt-ipsecme-ikev2-diet-esp-extension

Migault Gugemos, Schinazi, Bormann

ESP Header Compression (EHC)

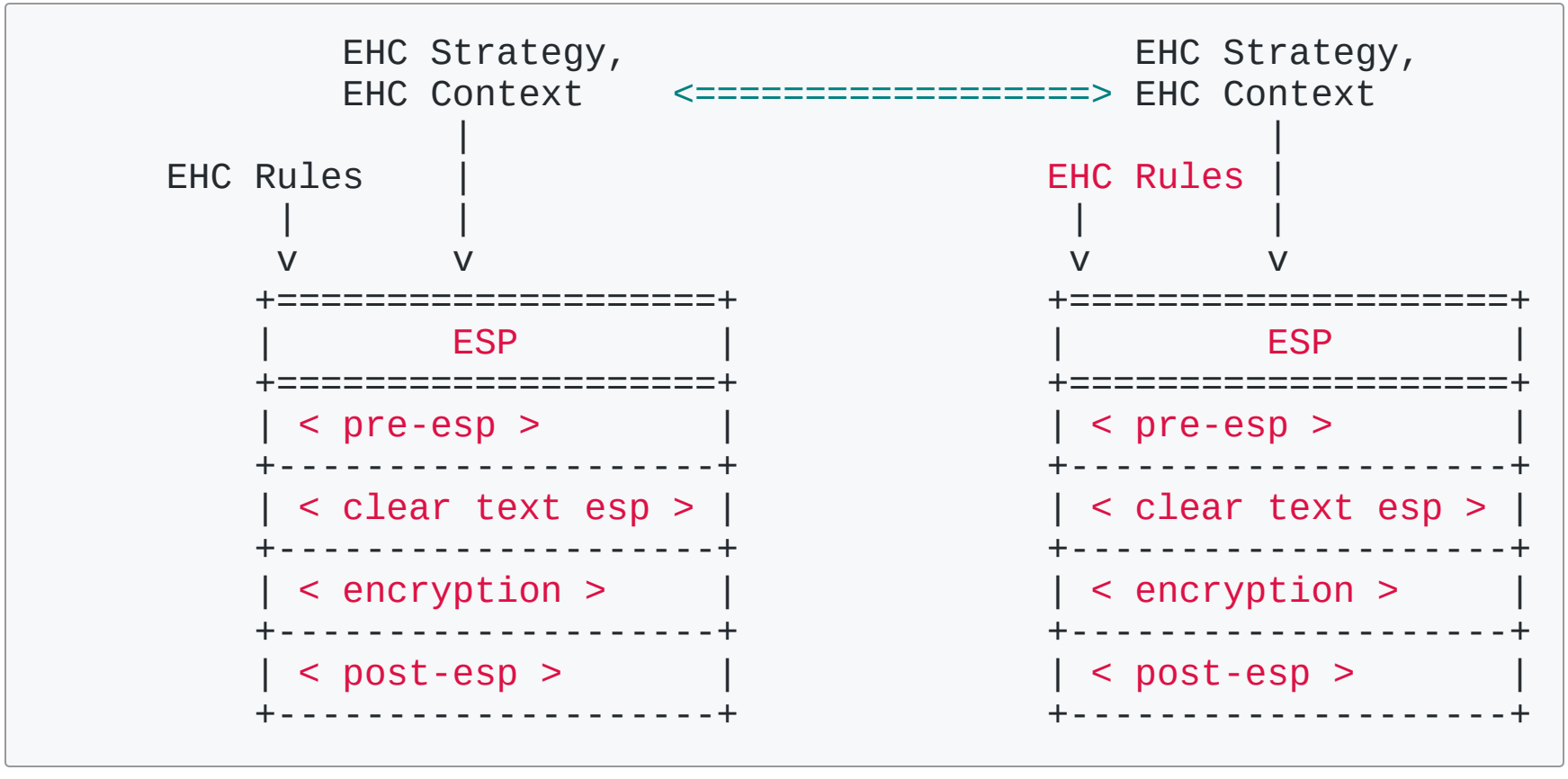
EHC provides a framework to compress ESP protected payloads:

- To increase the life time of battery powered devices
- To enable IPsec interoperability with constrained devices

EHC takes advantage of the SA agreement (configuration) to:

- Prevent repeating fields already defined by the SA
- Agree on ESP and inner packet compression rules
- Prevent any compression signaling within the ESP packet.

EHC - Architecture



EHC - Architecture

EHC Rules (de)compresses fields during ESP processing:

- pre-esp: inner packet (de)compression (before ESP)
- clear-text esp: non encrypted ESP packet (de)compression
- post-esp: encrypted ESP packet (de)compression

EHC Context provides parameters necessary for the EHC Rules

EHC Strategy defines the coordination of EHC Rules

- Derivation of EHC Context parameters (SA or not)
- Choice and order of EHC Rules

EHC - Architecture

EHC takes advantage of an explicit negotiation (IKEv2)

- EHC Strategy
- EHC Context

EHC Context and EHC Strategy :

- Defines EHC Rules that are activated
- Provides the sufficient parameters to (de)compress

EHC does not rely on

- In-band signaling of the compression
- Learning, discovery phases - ROHC

EHC - EHC Rules

```
+---------------+-------+---------+----------------+
|   EHC Rule    | Field | Action  |  Parameters    |
+---------------+-------+---------+----------------+
|               | f1    |    a1   | p1_1, ... p1_n |
|               +-------+---------+----------------+
| EHC_RULE_NAME ~      ...                         ~
|               +-------+---------+----------------+
|               | fm    |    am   | pm_1, ... pm_n |
+---------------+-------+---------+----------------+
```

- EHC_RULE_NAME designates the name of the EHC Rule
- Field designates the field to be compressed
- Action: how (de)compression is performed
- Parameters: necessary arguments to perform the action
    - Provided by the EHC Context

EHC - EHC Rules

(De)compression actions are one of the following actions:

Function	Compression	Decompression
send-value	No	No
elided	Not send	Get from EHC Context
lsb(_lsb_size)	Sent LSB	Get from EHC Context
lower	Not send	Get from lower layer
checksum	Not send	Compute checksum.
padding(_align)	Compute padding	Get padding

EHC - EHC Rules

EHC Rules compress:

- The Inner IPv6 Packet fields
- The ESP fields

There is no one-to-one mapping between EHC Rule and fields

- One EHC Rule may compress multiple fields
- One field may be addressed by multiple EHC Rules
    - Selection is performed by the EHC Strategy

EHC - EHC Context

For each field EHC Context provides:

- The value of the field - for example negotiated out-of-band
- An indication
  - Where the value may be derived from
  - How the value may be derived from

In most cases, the value has already been agreed with IKEv2

- part of the SA

EHC Strategy: Diet-ESP

EHC Strategy defines the orchestration of the EHC Rules

- EHC Rules are not agreed individually between the peers
- EHC Strategies are standardized
- EHC Strategies are described with EHC Rules but can be implemented differently

This presentation defines the EHC Strategy named: Diet-ESP

Diet-ESP results results from a compromise between:

- Compression efficiency,
- Ease to configure Diet-ESP (EHC Context)
- Various use cases (IoT, standard VPN)

EHC Strategy: Diet-ESP

- Ease to configure:
  - Selecting "OUTER" EHC Rules
  - Most commonly used parameters.
    - esp_sn_gen is set to "Incremental"
- Use cases vs Compression efficiency:
  - IPv4 compression has been limited in favor of IPv6 (IoT)
- Diet-ESP defines a logic to set the necessary parameters from SA
  - limits the setting of parameters.

EHC Strategy: Diet-ESP

If Diet-ESP is agreed (in SA):

- ESP EHC Rule set is activated
  If ip_version == 4 (in SA):
- IPv4 EHC Rule set is activated
  If ip_version == 6 (in SA):
- IPv6 EHC Rule set is activated
  If l4_proto == UDP (SA):
- UDP EHC Rule set activated
  If l4_proto == TCP (SA):
- TCP EHC Rule set is activated

EHC Strategy: Diet-ESP

Parameters that the two peers needs to agree on are:

- esp_sn_lsb
- esp_spi_lsb
- esp_align
- udplite_coverage
- tcp_lsb
- tcp_options
- tcp_urgent

EHC Strategy: Diet-ESP - Single UDP Session IoT VPN

- esp_sn_lsb: 0
- esp_spi_lsb: 0
- esp_align: 8

Diet-ESP results in a reduction of 61 bytes overhead.

Implicit_IV results in a 8 byte compression (ENCR_AES_CCM_8_IIV)

EHC Strategy: Diet-ESP - Traditional VPN

- esp_sn_lsb: 2
- esp_spi_lsb: 2
- esp_align: 8

Diet-ESP results in a reduction of 32 bytes.

Implicit_IV results in a 8 byte compression (ENCR_AES_CCM_8_IIV)

EHC Strategy: Diet-ESP - Performance

M3 devices from INRIA's IoT-LAB platform

- IEEE 802.15.4
- Contiki 2.7 OS

Radio Packet are 127 byte long

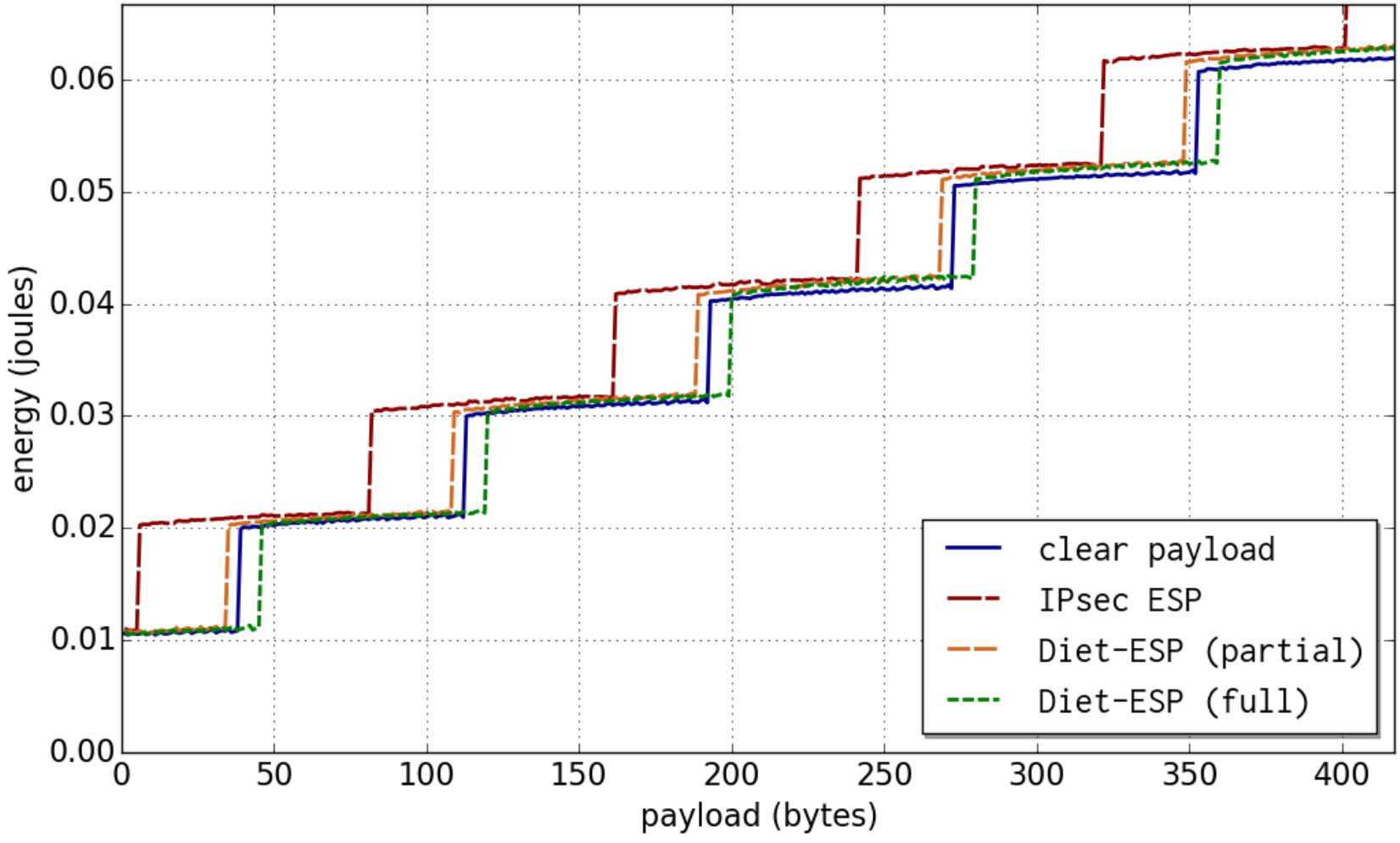
- 80 bytes for the IP packet

Diet-ESP overhead over uncenrcypted is less 2%

Diet-ESP cuts the bill:

- up to 100% for a 10 byte payload
- up to 30 % for a 190 byte payload

EHC Strategy: Diet-ESP - Performance



EHC Strategy: Diet-ESP - IKEv2

Enabling Diet-ESP requires the agreement of:

- The EHC Strategy: ehc_strategy
- The necessary parameters
- esp_sn_lsb
- esp_spi_lsb
- esp_align
- udplite_coverage
- tcp_lsb
- tcp_options
- tcp_urgent

EHC Strategy: Diet-ESP - IKEv2

Agreement is performed using IKEv2

- Exchange of EHC_STRATEGY_SUPPORTED Notify Payload

The Initiator provides:

- Acceptable value range for each parameters
- Default range values limit the size of the payloads
  - Default ehc_strategy is set to Diet-ESP
  - Default range: accept everything

The Responder provides:

- Acceptable chosen value for each parameters
- Default values limit the size of the payloads

EHC Strategy: Diet-ESP - IKEv2

Parameter	Value	Description
ehc_strategy	0*	Diet-ESP
esp_align	0*, 1, 2	8, 16, 32 bit alignment
esp_spi_lsb	0*, 1, 2, 3, 4	0, 8, 16, 24, 32 bit length SPI
esp_sn_lsb	0*, 1, 2, 3, 4	0, 8, 16, 24, 32 bit length SN
tcp_urgent	0, 1*	Urgent pointer field compressed, uncompressed
tcp_options	0, 1*	TCP option field compressed, uncompressed
udplite_coverage	0*	Coverage is UDP Length
	8-65535	Coverage 8 (the UDP-Lite Header)

EHC Strategy: Diet-ESP - IKEv2

```
Initiator                                Responder
 ------------------------------------------------------------------------
 HDR, SA, KEi, Ni -->
                                  <-- HDR, SA, KEr, Nr
 HDR, SK {IDi, AUTH,
      SA, TSi, TSr,
      N(EHC_STRATEGY_SUPPORTED)} -->
                                  <-- HDR, SK {IDr, AUTH,
                                       SA, TSi, TSr,
                                       N(EHC_STRATEGY_SUPPORTED)
```

Next Steps

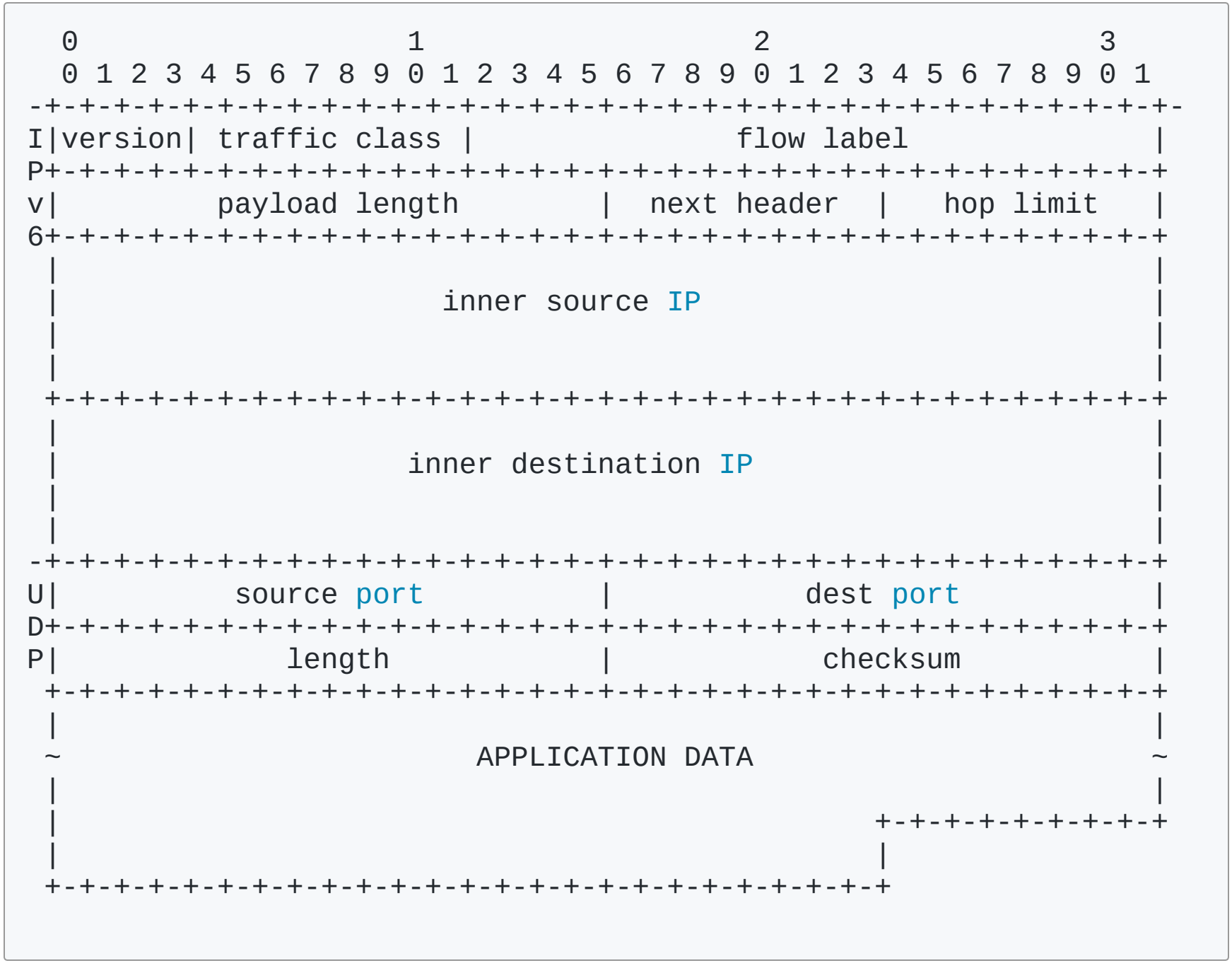
We beleive proposals are quite ready.

We have EHC implementation:

- Contiki 2.7
- Riot (ongoing)
- looking for Linux Kernel

Appendix

EHC - Inner IPv6 Packet Example



EHC - Inner IPv6 Packet

Inner IPv6 packet compression:

- IPv6 compression only occurs with IPsec Tunnel mode
- Occurs in the pre esp phase

Compression of the Inner IPv6 packet is performed in two phases:

- Inner IPv6 header compression
- Inner transport compression

EHC - Inner IPv6 Header - EHC Context

EHC Context provides the following IPv6 header information:

Context Attribute	In SA	Possible Values
ip_version	Yes	"IPv4", "IPv6"
ip6_tcfl_comp	No	"Outer", "Value", "UnComp"
ip6_tc	No	IPv6 Traffic Class
ip6_fl	No	IPv6 Flow Label
ip6_hl_comp	No	"Outer", "Value", "UnComp"
ip6_hl	No	Hop Limit Value
ip6_src	Yes	IPv6 Source Address
ip6_dst	Yes	IPv6 Destination Address

EHC - Inner IPv6 Header - EHC Rules

EHC Rules defines inner IPv6 header (de)compression:

EHC Rule	Field	Action	Parameters
IP6_OUTER	Version	elided	ip_version
	Traffic Class	lower	
	Flow Label	lower	
IP6_VALUE	Version	elided	ip_version
	Traffic Class	elided	ip6_tc
	Flow Label	elided	ip6_fl

EHC - Inner IPv6 Header - EHC Rules

EHC Rule	Field	Action	Parameters
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

EHC - Inner UDP - EHC Context

EHC Context provides the following UDP information:

Context Attribute	In SA	Possible Values
l4_proto	Yes	IPv6/ESP Next Header,IPv4 Protocol
l4_src	Yes	UDP/UDP-Lite/TCP Source Port
l4_dst	Yes	UDP/UDP-Lite/TCP Destination Port

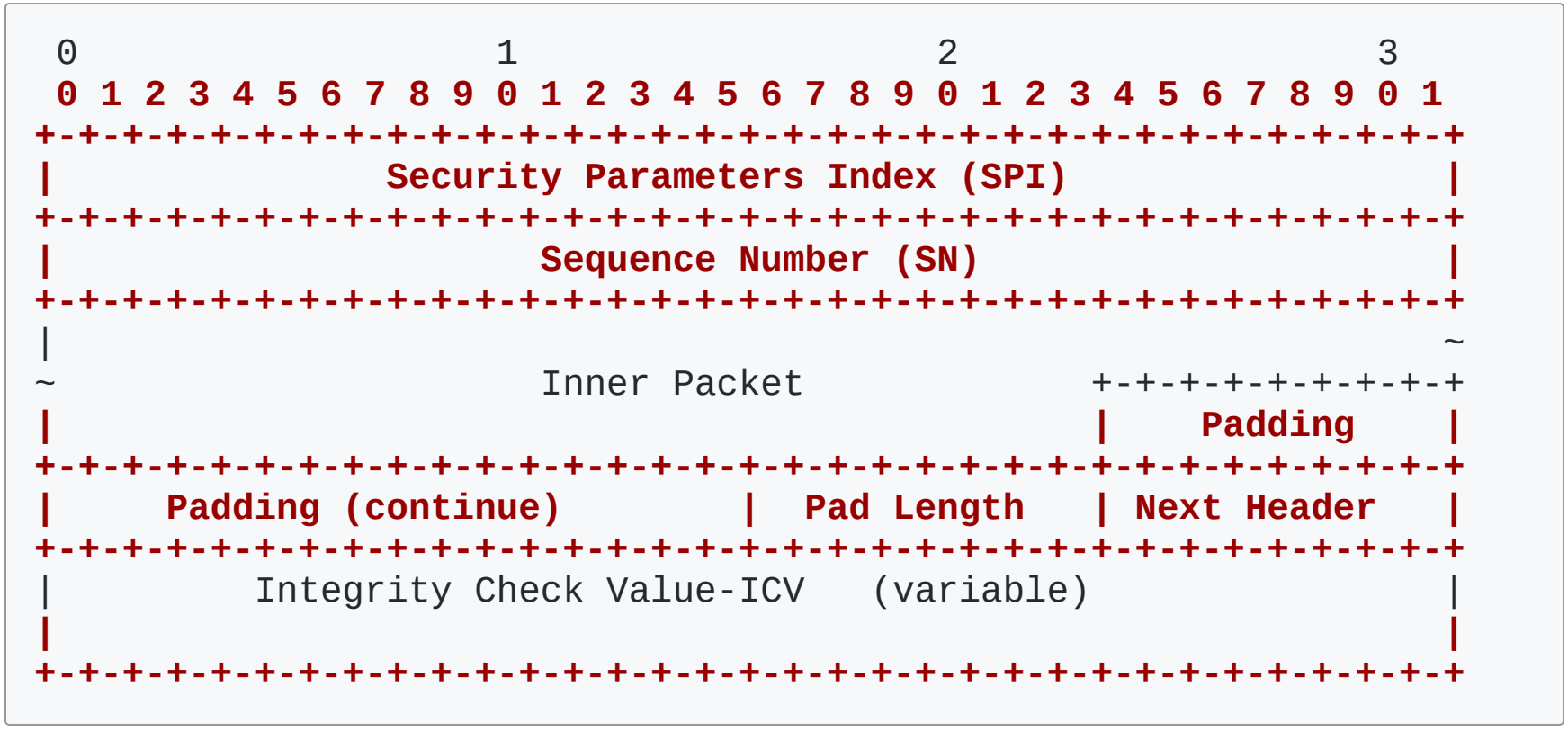
EHC - Inner UDP - EHC Rules

EHC Rules defines inner UDP (de)compression:

EHC Rule	Field	Action	Parameters
UDP_SRC	Source Port	elided	l4_source
UDP_DST	Dest. Port	elided	l4_dest
UDP_LENGTH	Length	lower	
UDP_CHECK	UDP Checksum	checksum	

EHC - ESP

Standard IPv6 VPN ESP packet:



EHC - ESP - EHC Context

EHC Context provides the following ESP information:

Context Attribute	In SA	Possible Values
ipsec_mode	Yes	"Tunnel", "Transport"
outer_version	Yes	"IPv4", "IPv6"
esp_spi	Yes	ESP SPI
esp_spi_lsb	No	0, 1, 2, 3, 4
esp_sn	Yes	ESP Sequence Number
esp_sn_lsb	No	0, 1, 2, 3, 4
esp_sn_gen	No	"Time", "Incremental"
esp_align	No	8, 16, 24, 32
esp_encr	Yes	ESP Encryption Algorithm

EHC - ESP - EHC Rules

EHC Rules defines inner ESP (de)compression:

EHC Rule	Field	Action	Parameters
ESP_SPI	SPI	lsb	esp_spi_lsb, esp_spi
ESP_SN	Seq. Number	lsb	esp_sn_lsb, esp_sn_gen,
			esp_sn
ESP_NH	Next Header	elided	l4_proto, ipsec_mode
ESP_PAD	Pad Length,	padding	esp_align, esp_encr
	Padding		

EHC Strategy: Diet-ESP

ESP:

EHC Rule	Activated if	Parameter	Value
ESP_SPI	Diet-ESP	esp_spi_lsb	Negotiated
		esp_spi	In SA
ESP_SN	Diet-ESP	esp_sn_lsb	Negotiated
		esp_sn_gen	Negotiated
		esp_sn	In SA
ESP_NH	Diet-ESP	ipsec_mode	In SA
		l4_proto	In SA
ESP_PAD	Diet-ESP	esp_align	Negotiated
		esp_encr	In SA

EHC Strategy: Diet-ESP

IPv6:

EHC Rule	Activated if	Parameter	Value
IP6_OUTER	ip_version==6	ip_version	In SA
IP6_LENGTH	ip_version==6	None	
IP6_NH	ip_version==6	l4_proto	In SA
IP6_HL_OUTER	ip_version==6	None	
IP6_SRC	ip_version==6	ip6_src	In SA
IP6_DST	ip_version==6	ip6_dst	In SA

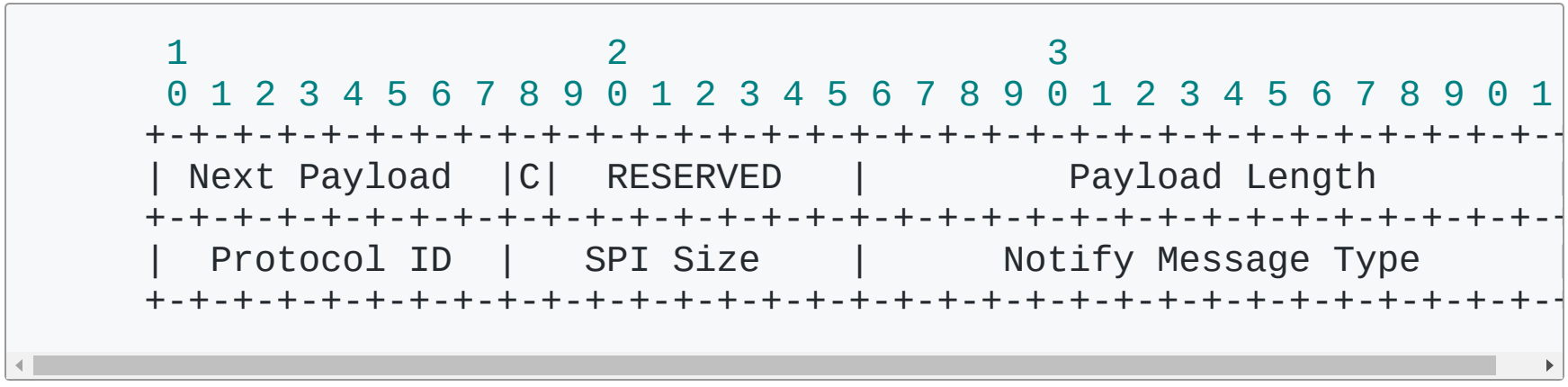
EHC Strategy: Diet-ESP

UDP

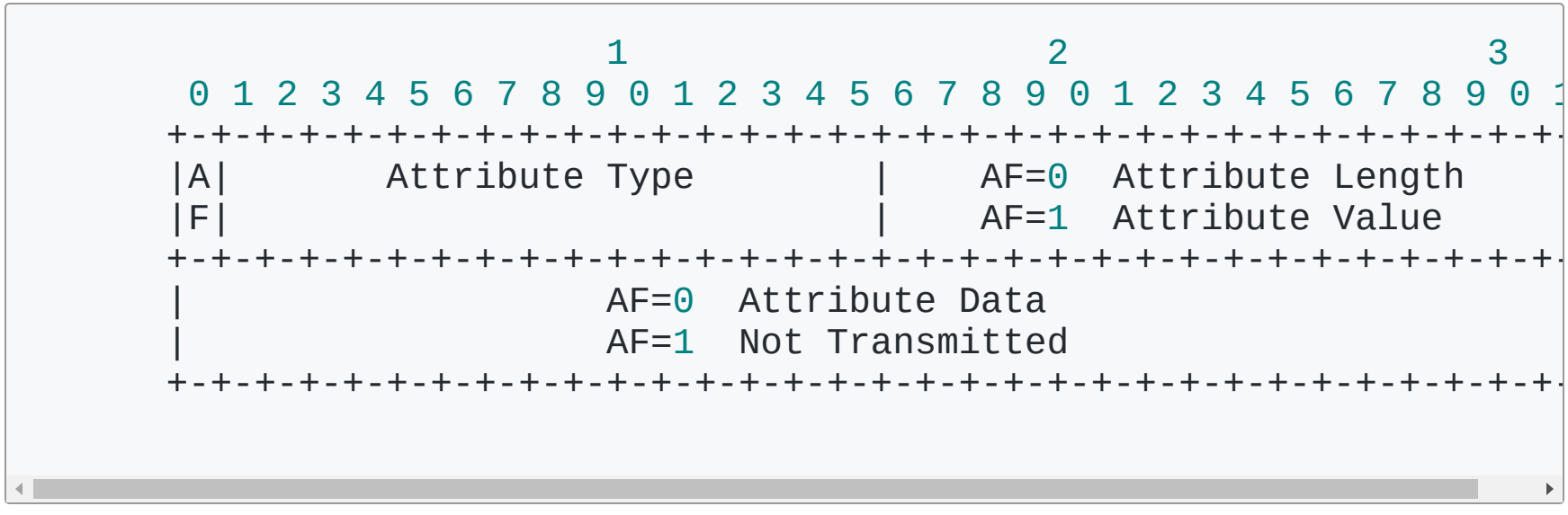
EHC Rule	Activated if	Parameter	Value
UDP_SRC	l4_proto==17	l4_source	In SA
UDP_DST	l4_proto==17	l4_dest	In SA
UDP_LENGTH	l4_proto==17	None	
UDP_CHECK	l4_proto==17	None	

EHC Strategy: Diet-ESP - IKEv2

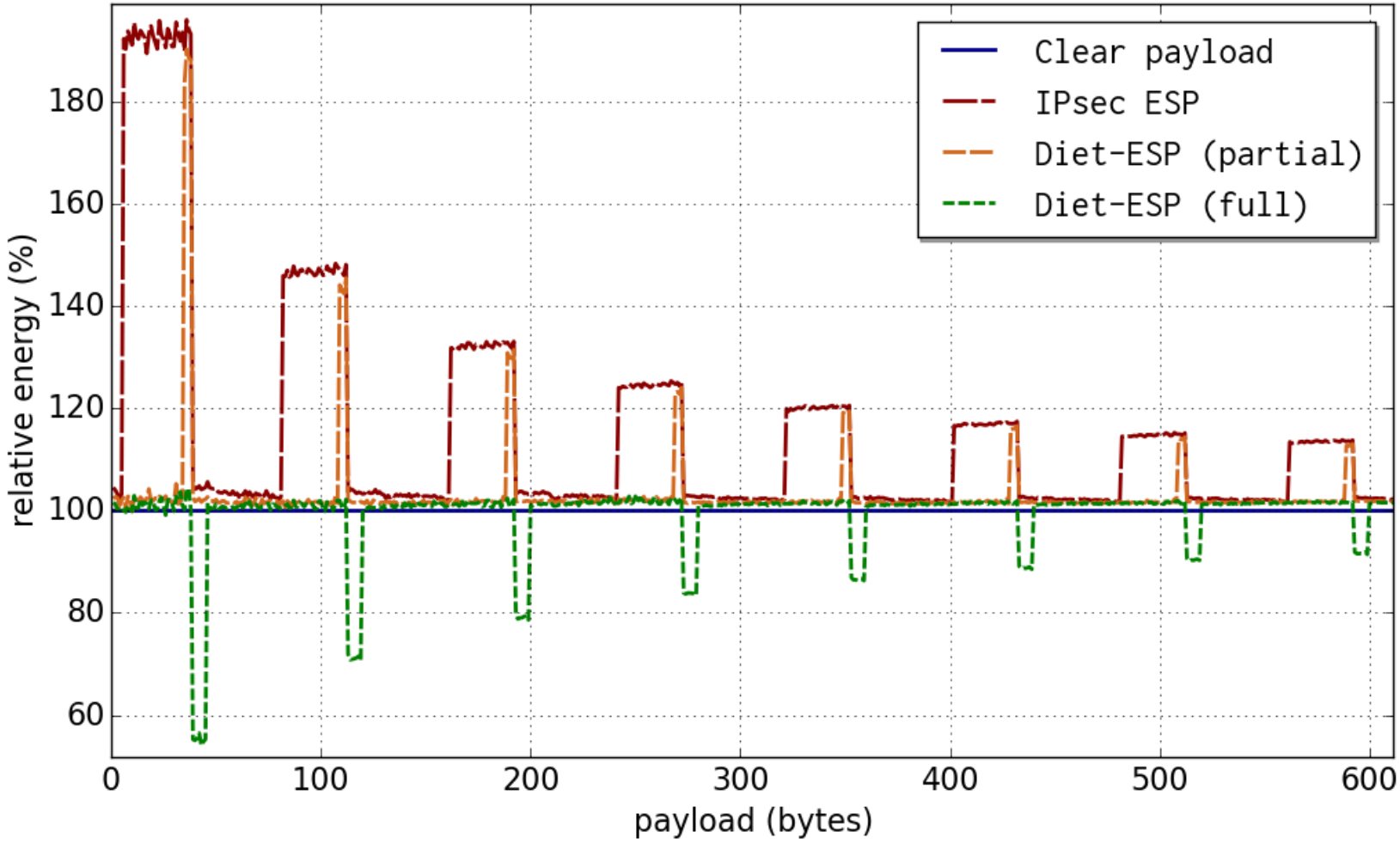
EHC_STRATEGY_SUPPORTED Notify Payload



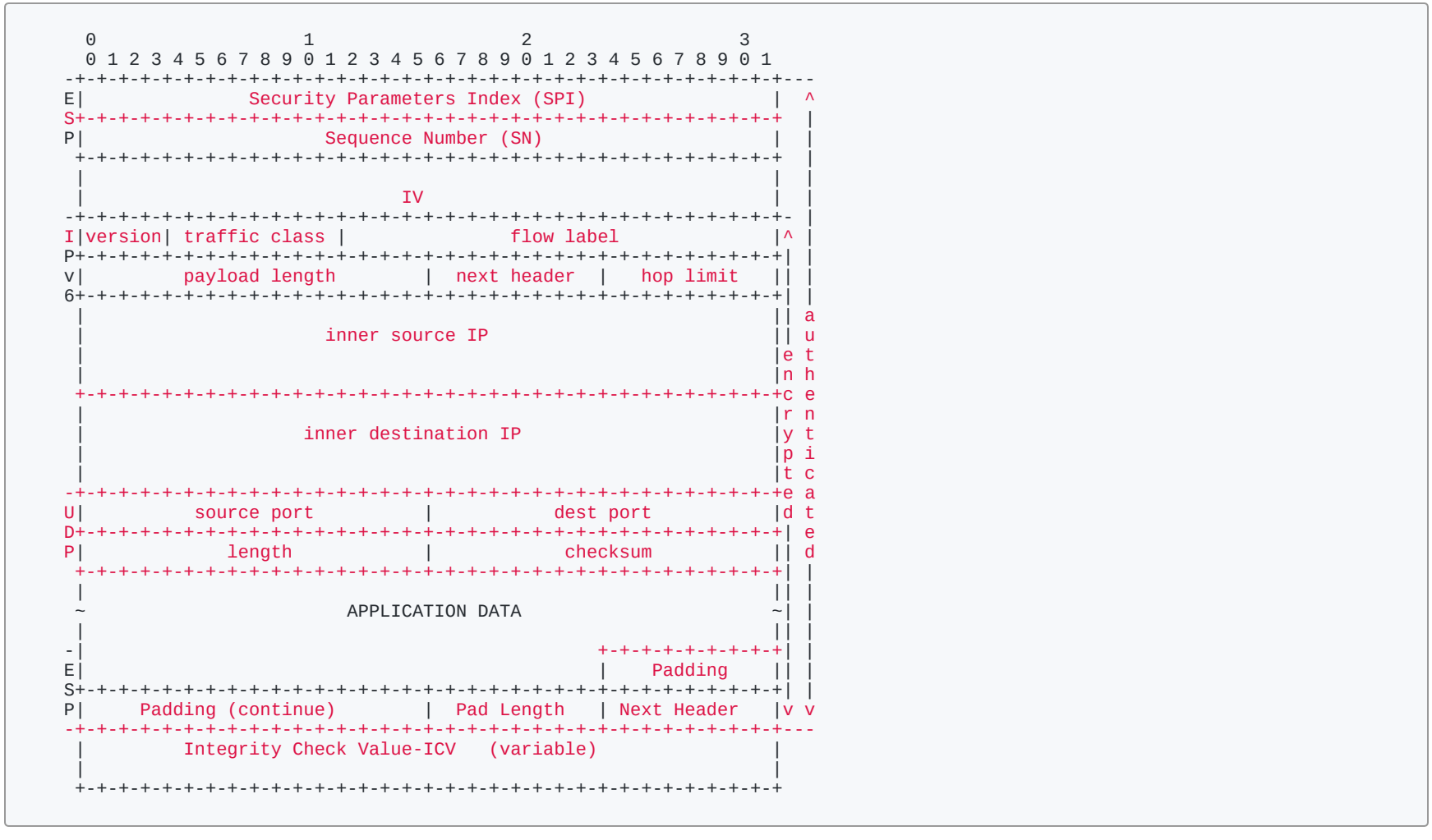
EHC Strategy Configuration Parameter Attributes



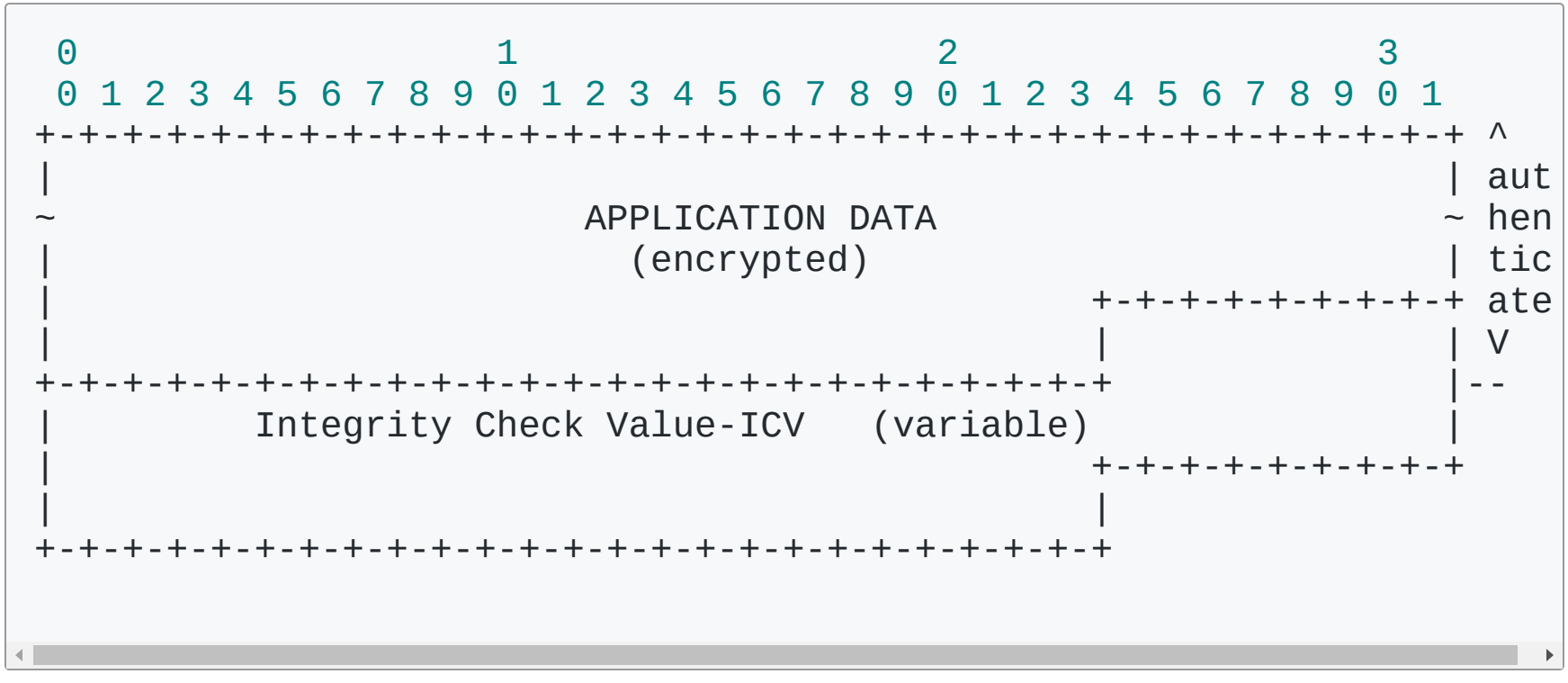
EHC Strategy: Diet-ESP - Performance



EHC Strategy: Diet-ESP - Single UDP Session IoT VPN



EHC Strategy: Diet-ESP - Single UDP Session IoT VPN



EHC Strategy: Diet-ESP - Traditional VPN

Standard ESP VPN Packet Description

EHC Strategy: Diet-ESP - Traditional VPN

Diet-ESP VPN Packet Description

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+---
|             SPI               |             SN                |  ^
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--|
|  Next Header  |                                               |^ |
+-+-+-+-+-+-+-+-+                                               || |
|                                                               || |
|                    inner destination IP                       || |
|                                                               || |a
|               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+| |u
|               |          source port          |  dest. port   ~|e|t
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+|n|h
~  (continue)   |            TCP Sequence Number (SN)           ~|c|e
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+|r|n
~  (continue)   |    ACK Sequence Number (SN)                   ~|y|t
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+|p|i
~  (continue)   |Off. | Rserv |      Flags      | Window Size   ~|t|c
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+|e|a
~  (continue)   |             Checksum          |   Urgent      ~|d|t
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+| |e
~ Pointer       |                                               || |d
+-+-+-+-+-+-+-+-+                                               || |
~                        APPLICATION DATA                       ~| |
|                                                               || |
|                                                               |v v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+---
|         Integrity Check Value-ICV   (variable)                |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```