ESP Header Compression Profile

`draft-mglt-ipsecme-diet-esp`

Migault, Hatami, Cespedes, Atwood, Liu, Guggemos, Bormann, Schinazi

ESP Header Compression Profile (EHCP) defines a profile to compress communications protected with IPsec/ESP.

Compression / Decompression is based on the Generic Framework for Static Context Header (SCHC) [RFC8724].

- joint work with the SCHC WG

We beleive the draft is ready for WGLC

We are working on adding an appendix section with the output of the implementation with openschc.

Relevant links:

- pyesp integrates specs with openschc
  - Plan to finalize pyesp and the specs by the end of the year.
- IETF 118 SCHC WG is integrating Diet-ESP in openschc
- PoC (contiki - without SCHC) Diet-ESP: IP layer security for IoT Journal of Computer Security, vol. 25, no. 2, pp. 173-203, 2017

ESP Header Compression Profile

`draft-mglt-ipsecme-diet-esp`

Migault, Guggemos, Schinazi, Liu, Preda, Hatami, Cespedes, Atwood

EHC Profile Diet-ESP requires Attributes for Rules Generation (AfRG) to be agreed between the peers

- some of these parameters are agreed via the standard CREATE_CHILD_SA exchange
- others are not

This document defines:

1. an IKEv2 extension for Header Compression Profile to agree on specific AfRG
2. the necessary AfRG for Diet-ESP (a specific EHCP)

```
Initiator                          Responder
-------------------------------------------------------------------
HDR, SA, KEi, Ni -->
                             <-- HDR, SA, KEr, Nr
HDR, SK {IDi, AUTH,
     SA, TSi, TSr,
     N(HCP_SUPPORTED
         Proposal_ID=1, HCP Name="Diet-ESP"
           AfRG_a
           ...
           AfRG_i
         ...
         Proposal_ID=2, HCP Name="Diet-ESP"
           AfRG_a
           ...
           AfRG_j)
                             <-- HDR, SK {IDr, AUTH,
                                      SA, TSi, TSr,
                                      N(HCP_SUPPORTED
                                        Proposal_ID=2, HCP Name="Diet-ESP"
                                          AfRG_a
                                          ...
                                          AfRG_j,
                                          AfRG_k,
                                          ...
                                          AfRG_u)
```

If you want to propose multiple values:

- the different AfRG values may be sent in a Proposal
- we defined a range(AfRG_min, AfRG_max)
- you may omit the AfRG to indicate you accept all values.

Thanks!