6lo
Internet-Draft
Intended status: Standards Track
Expires: August 21, 2015

D. Migault, Ed.
Ericsson

February 17, 2015

Diet-ESP Context IKEv2 Extension
draft-mglt-6lo-diet-esp-context-ikev2-extension-02.txt

Abstract

Diet-ESP has been designed for IoT to limit the IPsec ESP overhead in each IPsec packet. Diet-ESP is based on the standard IPsec ESP, and needs that peers agree on a Diet-ESP Context that defines how standard ESP packets can be compressed before being sent over the wire.

Standard IPsec ESP can be agreed between peers using IKEv2. However, current IKEv2 does not make possible to negotiate a Diet-ESP Context, and thus to negotiate a Diet-ESP communication.

This draft defines an extension for IKEv2 so peers can agree the Diet-ESP Context, and thus negotiate a Diet-ESP association.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 21, 2015.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Requirements notation

This section defines terms and acronyms used in this document.

- Diet-ESP Context: Defines the necessary parameters that are needed in order to set a Diet-ESP session. A Diet-ESP Context is a set of parameters with no particular format.

- Diet-ESP Proposal Payload: Defines the payload that carries the necessary information to derive the Diet-ESP Context. It can be seen as a container for Diet-ESP Context parameters. The Diet-ESP Proposal Payload is associated to a Diet-ESP Context, and Diet-ESP Context may evolve over time. As a result, the Diet-ESP Proposal needs to identify the Diet-ESP Context (using a Diet-ESP Context ID). When one peers wants to propose a set of various values, there may be some more optimal ways to presents these proposals. The Diet-ESP Proposal also identifies the Diet-ESP Context Payload with the Diet-ESP Context Payload Format. The Diet-ESP Context Payload Format defines the Diet-ESP Context Payload.

- Diet-ESP Context Payload: Is associated to a Diet-ESP Context ID and Diet-ESP Context Payload Format. It defines how the remaining bits must be interpreted to derive the parameters associated to a Diet-ESP Context.

3. Introduction

Diet-ESP [I-D.mglt-6lo-diet-esp] [I-D.mglt-6lo-diet-esp-payload-compression] has been designed to reduce the ESP overhead on IP packet sent over the wire.

The principle of Diet-ESP is to use ESP and compress each field. Compression depends on the context and the environment and is defined by the Diet-ESP Context.

IKEv2 [RFC7296] enables negotiation of ESP Security Associations, but does not enable the negotiation of the Diet-ESP Context. Thus preventing establishment of Diet-ESP SA. This document describes an extension of IKEv2 that make possible two peers to agree on a Diet-ESP Context and thus make possible the establishment of a Diet-ESP SA.

4. Protocol Overview

When an initiator wants to negotiate an Security Association (SA) using Diet-ESP, it negotiates a regular SA with a SA Payload, and indicates its willingness to establish a Diet-ESP session. In order to set the Diet-ESP session, a Diet-ESP Context MUST be agreed between the two peers. As a result, the initiator and the responder MUST negotiate and agree on a Diet-ESP Context.

To indicate its preference for a Diet-ESP instead of standard ESP, the initiator adds a DIET_ESP_CONTEXT_PROPOSAL Notify Payload. This Notify Payload carries a Diet-ESP Proposal Payload which can be seen as a container proposing Diet-ESP Contexts Payload. The Diet-ESP Proposal Payload indicates the Diet-ESP Context ID, a Diet-ESP Context Payload Format. These parameters make possible to derive properly the Diet-ESP Context parameters from the Diet-ESP Context Payload.

A Diet-ESP Context Payload is defined for each Diet-ESP Context ID and Diet-ESP Context Payload Format. The Diet-ESP Context ID indicates the Diet-ESP Context it refers to. For example, a Diet-ESP Context ID set to 0 indicates the initiator and responder refers to the Diet-ESP Context defined in this document. The Diet-ESP Context Payload Format corresponds to a convenient ways to present the proposals.

When the responder receives a DIET_ESP_CONTEXT_PROPOSAL Notify Payload. If the responder also wants to establish a Diet-ESP session, it responds with a DIET_ESP_CONTEXT_PROPOSAL Notify Payload with the chosen Diet-ESP Context. The chosen Diet-ESP Context is sent back using a specific Diet-ESP Proposal Payload. From this point, both peers have agreed with a standard ESP SA and a Diet-ESP Context. IP packets related to this specific SA are sent on the wired using the compressed format defined by the Diet-ESP Context.

If the responder does not accept the values proposed by the initiator for the Diet-ESP Context, the DIET_ESP_CONTEXT_PROPOSAL Notify Payload is ignored and no response is sent back.

If the responder does not agree with the proposals it MUST respond with a UNACCEPTABLE_DIET_ESP_CONTEXT.

If the initiator does not understand the Diet-ESP Proposal Payload received by the responder, the SA MUST be deleted.

5. Diet-ESP Context

The Diet-ESP Context is a set of values defined [I-D.mglt-6lo-diet-esp] and [I-D.mglt-6lo-diet-esp-payload-compression]. The Diet-ESP Context is a structure that defines fields and accepted values. A instance or a set of instance of Diet-ESP Context is exchanged on the wire using specific Diet-ESP Context Payload. The different types of Diet-ESP Context Payload are defined in Table 1.

Table 1 presents the various fields and associated values of the Diet-ESP Context defined in this document.

Fields Definition	Values
ALIGN	0 for 8 bit alignment
	1 for 16 bit alignment
	2 for 32 bit alignment
	3 for 64 bit alignment
SPI_SIZE	0 for 0 byte of SPI
	1 for 1 byte of SPI
	2 for 2 bytes of SPI
	3 for 4 bytes of SPI
SN_SIZE	0 for 0 byte of SN
	1 for 1 byte of SN
	2 for 2 bytes of SN
	3 for 4 bytes of SN
NH	0 indicates Next Header is removed
	1 indicates Next Header is present
PAD	0 indicates Pad Length is removed
	1 indicates Pad Length is present
Diet-ESP_ICV_SIZE	0 for 0 byte of ICV
	1 for 1 byte of ICV
	2 for 2 bytes of ICV
	3 for 4 bytes of ICV
COMPRESS_ESP_PAYLOAD	0 indicates TS are not considered
	1 indicates TS are considered
TRANSPORT_CHECKSUM_LSB	0 for 0 byte of Checksum
	1 for 1 byte of Checksum
	2 for 2 bytes of Checksum
TRANSPORT_SEQUENCE_NUMBER_LSB	0 for 0 byte of TCP Sequence Number
	1 for 1 byte of TCP Sequence Number
	2 for 2 bytes of TCP Sequence Number
	3 for 4 bytes of TCP Sequence Number

Table 1: Diet-ESP Context Definition

6. Protocol details

6.1. Diet-ESP Context Negotiation

Negotiation of Diet-ESP Compression is separate from the negotiation of cryptographic parameters associated with a Child SA. A initiator requesting a Child SA MAY advertise its support for one or more Diet-ESP Context through one Notify payloads of type DIET_ESP_CONTEXT_PROPOSALS. This Notify message may be included only in a message containing an SA payload negotiating a Child SA and indicates a willingness by its sender to use Diet-ESP on this SA. The responder MAY indicate acceptance of a single Diet-ESP Context with a Notify payload of type DIET_ESP_CONTEXT_PROPOSALS. These payloads MUST NOT occur in messages that do not contain SA payloads.

Diet-ESP has been designed to compress ESP only. As a result, when a SA Payload embeds multiple proposals, the negotiated Diet-ESP Context concerns all proposals with an Protocol ID set to ESP, and MUST be ignored for any other Protocol IDs.

If the responder accepts at least one proposal, the responder responds with a DIET_ESP_CONTEXT_PROPOSALS Notify Payload. This notification carries a Diet-ESP Proposal Payload of Diet-ESP Context Payload Format SINGLE_CONTEXT. The format provides a single Diet-ESP Context with each parameter uniquely specified.

If the responder does not support the Diet-ESP extension, it ignores the DIET_ESP_CONTEXT_PROPOSALS Notify Payload. By default, in case, no Diet-ESP Context have been agreed, the SA negotiated is ESP.

If the responder understand all proposals but accepts none of the proposed Diet-ESP Context, it MUST indicate the initiator that these values are not acceptable with a UNACCEPTABLE_DIET_ESP_CONTEXT Notify Payload. By default, the SA is then agreed using standard ESP, so if the responder does not want this SA, it MUST Delete the SA.

If the initiator does not understand the responded Diet-ESP Context by the responder, the initiator MUST delete its SA, re-initiates the IKEv2 negotiation using standard ESP.

Figure 1 illustrates the case where the initiator and the responder agree on a Diet-ESP Context. The negotiation occurs during the IKE_AUTH exchange. However, the negotiation can occurs for any Child SA negotiation.

```
   Initiator                          Responder
   -------------------------------------------------------------------
   HDR, SK { IDi, CERT, AUTH,
                  CP(CFG_REQUEST),
                  SAi2, TSi, TSr,
                  N(DIET_ESP_PROPOSALS) }
                              <-- HDR, SK { IDr, CERT, AUTH,
                                  CP(CFG_REPLY), SAr2, TSi, TSr,
                                   N(DIET_ESP_PROPOSALS) }
```

Figure 1

6.2. Error Handling

To indicate that a responder supports the Diet-ESP extension but does not agree with the proposed Diet-ESP Context, the responder sends a UNACCEPTABLE_DIET_ESP_CONTEXT Notify Payload.

7. Payload Description

Figure 2 illustrates the Notify Payload packet format as described in section 3. 10 of [RFC7296]. This format is used for the DIET_ESP_CONTEXT_PROPOSALS notification.

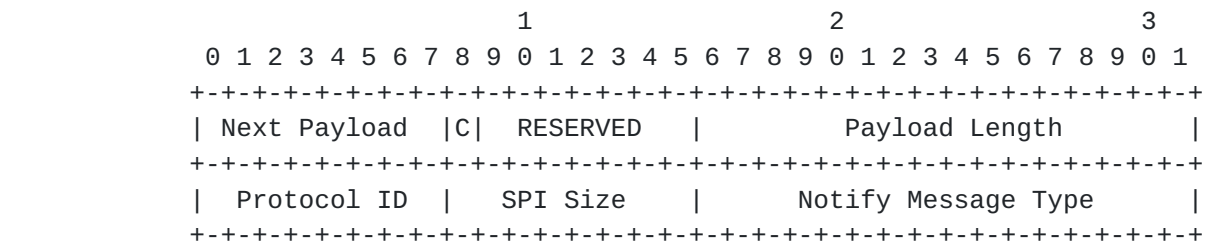

Figure 2: Notify Payload

The fields Next Payload, Critical Bit, RESERVED and Payload Length are defined in [RFC7296]. Specific fields defined in this document are:

- Protocol ID (1 octet): set to zero.

- SPI Size (1 octet): set to zero.

- Notify Message Type (2 octets): Specifies the type of notification message. It is set to <TBA by IANA> for the DIET_ESP_CONTEXT_PROPOSALS and UNACCEPTABLE_DIET_ESP_CONTEXT notification.

7.1. DIET_ESP_CONTEXT_PROPOSALS Notify Payload

The DIET_ESP_CONTEXT_PROPOSALS Notify Payload is used to:

- By the initiator: To announce its support of Diet-ESP as a well as the accepted Diet-ESP Contexts.

- By the responder: To announce its support of Diet-ESP as well as the agreed Diet-ESP Context

To announce the accepted values for each fields of the Diet-ESP Contexts, the initiator sends a DIET_ESP_CONTEXT_PROPOSALS Notify Payload with one or multiple Diet-ESP Proposal Payload.

7.1.1. Diet-ESP Proposal Payload

The Diet-ESP Payload can be seen as a container for a Diet-ESP Context. The format for signaling Diet-ESP Attributes takes a similar format to the Transform Attributes described in Section 3.3.5 of [RFC7296] and is represented in Figure 3

Note that the Diet-ESP Context is provided with all parameters, and the current specification does not make possible to provide each parameter individually. Providing the whole Diet-ESP Context reduces the number of byte of the Attribute Payload over providing each parameter individually.

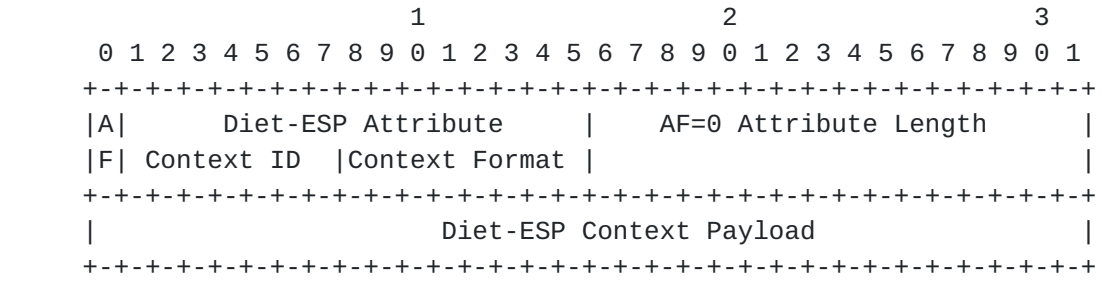

Figure 3: Diet-ESP Payload

- AF=0 (1 bit) : Specified the attribute format is of Type/Length/ Value.

- Diet-ESP Context ID (7 bits) : The ID of the Diet-ESP Context.

  - 0: The Diet-ESP Context defined in this document.

  - 1 - 127: Unassigned

- Diet-ESP Context Format (4 bits) : indicates the Diet-ESP Context Payload Format. The following values are considered:

  - 0 FULL_SUPPORT: The initiator indicates it has no restrictions on the fields values of the Diet-ESP Context and supports all defined values.

  - 1 SINGLE_CONTEXT: Defines a single Diet-ESP Context. It can be used by the initiator if only a single value is accepted for each field of the Diet-ESP Context. It is used by the responder to indicate the agreed Diet-ESP Context.

  - 2 MINIMAL_CONTEXT: The initiator indicates for each field of the Diet-ESP Context the minimal accepted values.

  - 3 MAXIMAL_CONTEXT: The initiator indicates for each field of the Diet-ESP Context the maximal accepted values.

  - 4 RANGE_CONTEXT: The initiator indicates for each field of the Diet-ESP Context a range of accepted values.

  - 5 - 255: Unassigned

7.1.1.1. FULL_SUPPORT Diet-ESP Context Payload Format

The Diet-ESP Context Payload of format FULL_SUPPORT is an empty payload.

7.1.1.2. SINGLE_CONTEXT Diet-ESP Context Payload Format

The Diet-ESP Context Payload that corresponds to the SINGLE_CONTEXT Format assigns a specific value for each field. This format may be used by the initiator to indicate a very specific proposal, or by the responder to indicate its choice of values for the agreed Diet-ESP Context. The Format of the Payload is defined by Table 2. The fields value are described in Table 1

Bit	Fields Definition
0 - 1	ALIGN: (2 bits)
2 - 3	SPI_SIZE: (2 bits)
4 - 5	SN_SIZE: (2 bits)
6	NH: (1 bit)
7	PAD: (1 bit)
8 - 9	Diet-ESP_ICV_SIZE: (2 bits)
10	COMPRESS_ESP_PAYLOAD: (1 bit)
11 - 12	TRANSPORT_CHECKSUM_LSB: (2 bits)
13 - 14	TRANSPORT_SEQUENCE_NUMBER_LSB: (2 bits)
15	Unassigned

Table 2: MINIMAL_CONTEXT Diet-ESP Context Format

7.1.1.3. MINIMAL_CONTEXT Diet-ESP Context Payload Format

The Diet-ESP Context Payload of format MINIMAL_CONTEXT defines for all fields a minimal value. The Format of the Payload is defined by Table 2. The fields value are described in Table 1

7.1.1.4. MAXIMAL_CONTEXT Diet-ESP Context Payload Format

The Diet-ESP Context Payload of format MAXIMAL_CONTEXT defines for all fields a maximal value. The Format of the Payload is defined by Table 2. The fields value are described in Table 1

7.1.1.5. RANGE_CONTEXT Diet-ESP Context Payload Format

The Diet-ESP Context Payload of format RANGE_CONTEXT defines for all fields a minimum and a maximum value. The only field that is where only the minimal value is provided is the ALIGN field. The Format of the Payload is defined by Table 3. The fields value are described in Table 1

Bit	Fields Definition
0 - 1	ALIGN: (Minimal accepted value)
2 - 3	SPI_SIZE: (Minimal accepted value)
4 - 5	SN_SIZE: (Minimal accepted value)
6	NH: (Minimal accepted value)
7	PAD: (Minimal accepted value)
8 - 9	Diet-ESP_ICV_SIZE: (Minimal accepted value)
10	COMPRESS_ESP_PAYLOAD: (Minimal accepted value)
11 - 12	TRANSPORT_CHECKSUM_LSB: (Minimal accepted value)
13 - 14	TRANSPORT_SEQUENCE_NUMBER_LSB: (Minimal accepted value)
15 - 16	SPI_SIZE: (Maximal accepted value)
17 - 18	SN_SIZE: (Maximal accepted value)
19	NH: (Maximal accepted value)
20	PAD: (Maximal accepted value)
21 - 22	Diet-ESP_ICV_SIZE: (Maximal accepted value)
23	COMPRESS_ESP_PAYLOAD: (Maximal accepted value)
24 - 25	TRANSPORT_CHECKSUM_LSB: (Minimal accepted value)
26 - 27	TRANSPORT_SEQUENCE_NUMBER_LSB: (Minimal accepted value)
28 - 31	Unassigned

Table 3: RANGE_CONTEXT Diet-ESP Context Format

7.2. UNACCEPTABLE_DIET_ESP_CONTEXT Notify Payload

This Notify Payload my return a Diet-ESP Proposal Payload accepted by the responder.

8. Acknowledgment

The current work on Diet-ESP results from exchange and cooperation between Orange, Ludwig-Maximilians-Universitaet Munich, Universite Pierre et Marie Curie. We thank Daniel Palomares and Carsten Bormann for their useful remarks, comments and guidances on the design. We thank Sylvain Killian for implementing an open source Diet-ESP on Contiki and testing it on the FIT IoT-LAB [fit-iot-lab] funded by the French Ministry of Higher Education and Research. We thank the IoT-Lab Team and the INRIA for maintaining the FIT IoT-LAB platform and for providing feed backs in an efficient way.

9. IANA Considerations

IANA is requested to allocate two values in the IKEv2 Notify Message Types - Status Types registry:

IKEv2 Notify Message Types - Status Types	
DIET_ESP_CONTEXT_PROPOSALS	- TBA
UNACCEPTABLE_DIET_ESP_CONTEXT	- TBA

Diet-ESP Attribute Types (Diet-ESP ID = 0)	
FULL_SUPPORT	- 256
SINGLE_CONTEXT	- 257
MINIMAL_CONTEXT	- 258
MAXIMAL_CONTEXT	- 259
RANGE_CONTEXT	- 260

10. Security Considerations

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, October 2014.

11.2. Informational References

[I-D.mglt-6lo-diet-esp] Migault, D. and T. Guggemos, "Diet-ESP: a flexible and compressed format for IPsec/ESP", draft-mglt-6lo-diet-esp-00 (work in progress), January 2015.

[I-D.mglt-6lo-diet-esp-payload-compression] Migault, D. and T. Guggemos, "Diet-IPsec: ESP Payload Compression of IPv6 / UDP / TCP / UDP-Lite", draft-mglt-6lo-diet-esp-payload-compression-00 (work in progress), January 2015.

[fit-iot-lab] "Future Internet of Things (FIT) IoT-LAB", <https://www.iot-lab.info>.

Appendix A. Document Change Log

01 -

- Changing affiliation

01 -

- Adding Change log section
- Adding Acknowledgment section
- Updating references 6lo
- Updating notation coherent with draft-mglt-6lo-diet-esp-payload-compression
-

00-First version published

Author's Address

Daniel Migault (editor)
Ericsson
8400 boulevard Decarie
Montreal, QC H4P 2N2
Canada

Email: mglt.ietf@gmail.com