ipsecme
Internet-Draft
Intended status: Standards Track
Expires: December 27, 2018

D. Migault
Ericsson
T. Guggemos
LMU Munich
D. Schinazi
Apple Inc.

June 25, 2018

Internet Key Exchange version 2 (IKEv2) extension for the ESP Header Compression (EHC) Strategy
draft-mglt-ipsecme-ikev2-diet-esp-extension-01

Abstract

ESP Header Compression (EHC) reduces the ESP overhead by compressing ESP fields. Compression results from a coordination of various EHC Rules designed as EHC Strategies. An EHC Strategy may require to be configured with some configuration parameters.

When a Security Association (SA) is enabling EHC, the two peers need to agree which EHC Strategy is applied as well as its associated configuration parameters.

This document describes an extension of IKEv2 that enables two peers to agree on a specific EHC Strategy as well as its associated configuration parameters.

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 https://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 December 27, 2018.

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. Terminology

This section defines terms and acronyms used in this document.

- EHC Strategy : EHC Strategy is a generic term defined in [I-D.mglt-ipsecme-diet-esp] that defines the way EHC Rules are coordinated.

- Designated EHC Strategy: the specific EHC Strategy agreed between the two peers. [I-D.mglt-ipsecme-diet-esp] defines Diet-ESP as an EHC Strategy and other may be defined in the future. This document only considers Diet-ESP but provides negotiation mechanisms so future EHC Strategies may also be negotiated. New EHC Strategies will require to register the necessary associated EHC Strategy Configuration Parameters. This will typically include a specific designation as well as specific configuration parameters. The parameters are designated as EHC Strategy Configuration Parameter (Parameter)

- EHC Strategy Configuration Parameter (Parameter): describes the configuration parameters associated to a specific EHC Strategy. The Parameters includes the EHC Strategy as well as configuration parameters.

- EHC Strategy Configuration Parameter Attributes (Attribute): designates the necessary attributes associated to each Parameter exchanged in order to agree on the EHC Strategy Configuration Parameter. This document considers two type of attributes: the Range Attribute that indicates a range for a given Parameter, and the Value Attribute that indicates a fixed value associated to a Parameter.

  - Range Attribute: the payload that indicates a supported range of values on an specific EHC Strategy Configuration Parameter. In this document, all Parameters are associated a specific Range Attribute.

  - Value Attribute: the payload that indicates a value of an specific EHC Strategy Configuration Parameter. In this document, all Parameters are associated a specific Value Payload.

3. Introduction

ESP Header Compression (EHC) [I-D.mglt-ipsecme-diet-esp] reduces the ESP overhead by compressing ESP fields. Compression results from a coordination of various EHC Rules performed by the EHC Strategy. The EHC Strategy may require to be configured with some configuration parameters designated as EHC Strategy Configuration Parameter (or simply Parameter).

When a Security Association (SA) is enabling EHC the two peers needs to agree which EHC Strategy strategy is applied as well as its associated configuration parameters.

This document describes an extension of IKEv2 that enables two peers to agree on a specific EHC Strategy as well as its associated Parameters.

4. Protocol Overview

ESP Header Compression requires IKEv2 to negotiate the IPsec mode and the used EHC strategy and its corresponding parameters.

First, the peers need to agree to the IPsec mode used for compression. [I-D.mglt-ipsecme-diet-esp] defines "Compressed Transport Mode" and "Compressed Tunnel Mode". This is done by a new Notify Payload USE_COMPRESSED_MODE. In order to negotiate "Compressed Transport Mode", the initiator sends the USE_COMPRESSED_MODE Notify Payload and USE_TRANSPORT_MODE Notify Payload which is defined in [RFC7296]. In order to negotiate "Compressed Tunnel Mode" the initiator sends the USE_COMPRESSED_MODE Notify Payload. Tunnel mode is the default behaviour defined in [RFC7296], why it does not need any further negotiation. The protocol behaviour of USE_COMPRESSED_MODE is the same as the one of USE_TRANSPORT_MODE, the initiator sends the USE_COMPRESSED_MODE Notify Payload and the responder responds with USE_COMPRESSED_MODE Notfiy Payload.

EHC Strategies are configured on a per-SA basis and need to be agreed between the two peers. An EHC Strategy is agreed when peers have agreed on the EHC Strategy as well as its associated Parameters.

For example, [I-D.mglt-ipsecme-diet-esp] defines an EHC Strategy

called as Diet-ESP which requires the following Parameters to be set: udplite_coverage, tcp_lsb, tcp_options, tcp_urgent, esp_sn_lsb, esp_spi_lsb, esp_align.

The negotiation of the EHC Strategy as well as its Parameters is performed via the EHC_STRATEGY_SUPPORTED Notify Payload exchange.

When the initiator is willing to negotiate an EHC Strategy for a given SA, it sends a single EHC_STRATEGY_SUPPORTED Notify Payload in its IKE_AUTH and CREATE_CHILD_SA exchange. This Notify Payload indicates the support to negotiate EHC Strategies. In addition, the Notify Payload MAY indicates with a Range Attribute, the supported values for each Parameter, including the Designated EHC Strategy. If the initiator does not have any restriction regarding a specific Parameter, there is no need to provide an Range Value associated to that Parameter.

Currently, the only defined EHC Strategy is Diet-ESP, and the EHC_STRATEGY_SUPPORTED Notify Payload indicates the support for Diet-

ESP unless Diet-ESP is explicitly excluded by the Range Attribute. In the future, when other EHC Strategies will be defined, the support of that new Designated EHC Strategy will need to be explicitly announced with its associated Range Attribute. Other Parameters MAY also have their own associated Range Attribute. Note that if multiple EHC Strategies that share a given Parameter, the Range Attribute is applied for all designated EHC Strategies. In other words, it is not possible to have a given Parameter associated with different values depending on the EHC Strategy.

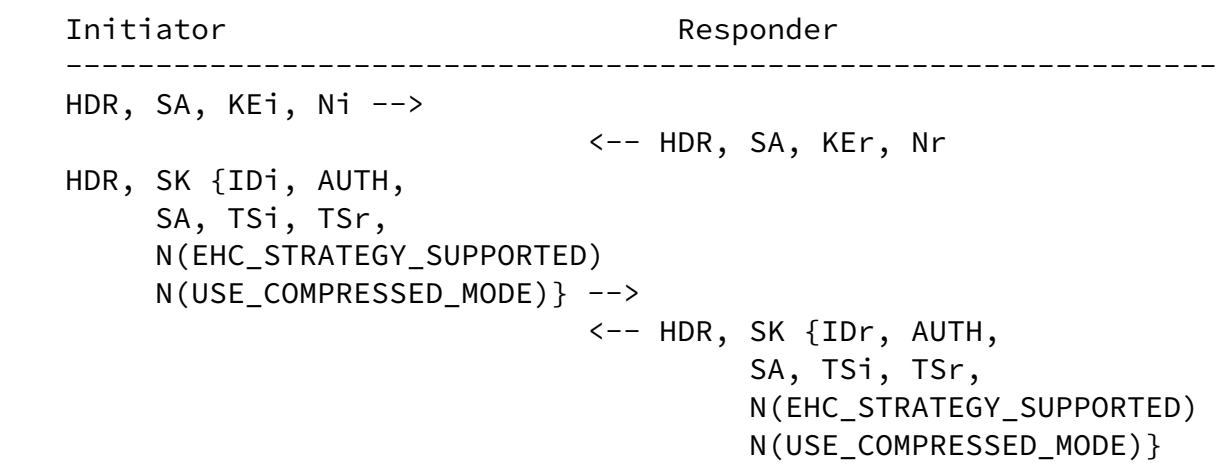
Upon receiving the IKE_AUTH and CREATE_CHILD_SA with a EHC_STRATEGY_SUPPORTED Notify Payload, a receiver that does not support this extension or that is not willing to activate EHC ignores the Notify Payload and the negotiation continues as a standard ESP negotiation. If the responder supports EHC Strategy negotiation and chooses to apply a supported EHC Strategy to the negotiated SA, it reads all Range Attributes and selects a Designated EHC Strategy as well as specific values for each Parameter associated to the Designated EHC Strategy. The responder enables EHC for the negotiated SA and responds with an EHC_STRATEGY_SUPPORTED Notify Payload which indicates the selected Parameters' values using Value Attributes. The responder MAY send a Value Attribute that

corresponds to all selected Parameters. On the other hand, the responder MAY also send only the Value Attribute of Parameters whose value differs from the default value. In fact each EHC Strategy defines default values for each Parameters.

In some cases, the supported values provided by the initiator may not match those of the responder, and so EHC cannot be activated. The responder may want to indicate the supported range provided by the initiator were not acceptable by responding with a EHC_STRATEGY_UNACCEPTABLE_PARAMETER. The initiator MAY carry Range Attributes in order to indicates what it supports.

Upon receiving a EHC_STRATEGY_SUPPORTED Notify Payload back, the initiator reads the Value Attributes and checks the Parameters match the supported range. The initiator may configure the EHC Strategy with the provided parameters or abort the negotiation with a Delete Payload as specified in section 3.11 of [RFC7296].

Upon receiving a EHC_STRATEGY_UNACCEPTABLE_PARAMETER Notify Payload, the initiator may use the regular ESP or delete the SA. When the SA is deleted, the initiator is expected to restart a negotiation providing contraints that respect those of the responder.



Protocol Overview

5. Notify Payload

Figure 1 illustrates the Notify Payload packet format as described in section 3.10 of [RFC7296], used for USE_COMPRESSED_MODE, EHC_STRATEGY_SUPPORTED and EHC_STRATEGY_UNACCEPTABLE_PARAMETER Notify Payloads.

The USE_COMPRESSED_MODE Notify Payload is used during the IKE_AUTH and CREATE_CHILD_SA.

Similarly, EHC_STRATEGY_SUPPORTED and EHC_STRATEGY_UNACCEPTABLE_PARAMETER Notify Payloads are used during the IKE_AUTH and CREATE_CHILD_SA. The sender is expected to send only a single payload. When multiple payloads are received, the receiver MAY consider the first one and MUST ignore the remaining ones.

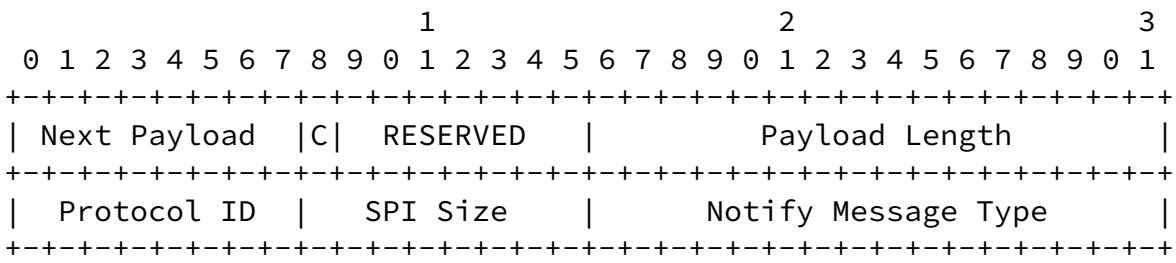


Figure 1: Notify Payload

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:

  <TBA1 by IANA> for the USE_COMPRESSED_MODE

  <TBA2 by IANA> for the EHC_STRATEGY_SUPPORTED

<TBA3 by IANA> for EHC_STRATEGY_UNACCEPTABLE_PARAMETER

5.1. USE_COMPRESSED_MODE Notify Payload

The USE_COMPRESSED_MODE Notify Payload indicates that an SA with either "Compressed Transport Mode" or "Compressed Tunnel Mode" should be set up.

A responder not understanding USE_COMPRESSED_MODE Notify Payload MUST ignore it and any other Notify Payload defined in this document as it may otherwise result in unexpected behaviour during the communication if the negotiated SA is not in correct IPsec Mode.

5.2. EHC_STRATEGY_SUPPORTED Notify Payload

The EHC_STRATEGY_SUPPORTED Notify Payload indicates the supported EHC Strategies.

When sent by the initiator, it MAY contain Range Attributes (see Section 7.1). A responder not understanding a Range Attribute MUST ignore it. This is intended to ease the negotiation of new EHC Strategies with new Parameters. It is its responsibility to understand the Parameters associated to the negotiated EHC Strategy.

When sent by the responder, it MAY contain Value Attributes (see Section 7.2). An initiator not understanding a Value Payload MUST NOT create the SA and SHOULD send a Delete Payload to the responder as described in section 3.11 of [RFC7296].

5.3. EHC_STRATEGY_UNACCEPTABLE_PARAMETER Notify Payload

The EHC_STRATEGY_UNACCEPTABLE_PARAMETER Notify Payload indicates the responder supports of EHC Strategy negotiation but was not able to configure it due to the constraints provided by the initiator. The responder MAY insert Range Attributes (see Section 7.1) to inform the initiator of its supported ranges.

The responder has configured the SA without enabling the EHC. Upon receiving the Notify Payload, the initiator MAY accept the SA without

EHC. It MAY also Delete the SA as described in section 3.11 of

[RFC7296] and renegotiate the SA, considering the responder's supported ranges.

6. EHC Strategy Configuration Parameters

This document only considers Diet-ESP, which requires the following Parameters to be agreed by the two peers: esp_align, esp_spi_lsb, esp_spi_sn, tcp_urgent, tcp_options, tcp_lsb, udplite_coverage. In addition, in order to enable future EHC Strategies, the following parameter has been introduce to designate the agreed EHC Strategy: ehc_strategy. Figure 2 lists these Parameters with description and associated values.

In addition, each of these parameter is associated to a default value. The default value is considered unless other values are specified by the responder. The associated default value is specified in Figure 2.

Parameter	Value	Description	Default
ehc_strategy	0	Diet-ESP	*
	1-127	Unassigned	
	128-255	Private Used	
esp_align	0	8 bit alignment	*
	1	16 bit alignment	
	2	32 bit alignment	
	3-255	Unassigned	
esp_spi_lsb	0	0 bit length SPI	*
	1	8 bit length SPI	
	2	16 bit length SPI	
	3	24 bit length SPI	
	4	24 bit length SPI	
	5-255	Unassigned	
esp_spi_sn	0	0 bit length SPI	*
	1	8 bit length SN	
	2	16 bit length SN	
	3	24 bit length SN	
	4	24 bit length SN	
	5-255	Unassigned	
tcp_urgent	0	Urgent pointer field compressed	
	1	Urgent pointer field uncompressed	*
	2-255	Unassigned	
tcp_options	0	TCP option field compressed	
	1	TCP option field uncompressed	*
	2-255	Unassigned	
tcp_lsb	0	0 bit length SN	
	1	8 bit length SN	
	2	16 bit length SN	
	3	24 bit length SN	
	4	24 bit length SN	
	5-255	Unassigned	
udplite_coverage	0	Coverage is UDP Length	
	8-65535	Coverage 8 (the UDP-Lite Header)	
	1-7	Unassigned	

Figure 2: Parameter Values

7. EHC Strategy Configuration Parameter Attributes

For each of these Parameters, the initiator or responder may indicate acceptable values of these Parameters. Such constraints are expressed with the Range Attributes. Each Parameters has its corresponding payload which carries the minimum and maximum acceptable values associated to the parameters (see Section 7.1).

Similarly, for each of these Parameters, the responder needs to be able to provide the selected value associated to the Parameter. Each of these Parameters' value can be expressed by via the Value Attribute. Each parameter has a corresponding payload which carries the associated value (see Section 7.2).

The Range Attribute and Value Attribute use the format of the Transform Attribute of section 3.3.5 of [RFC7296] represented in Figure 3. The fields are described in [RFC7296].

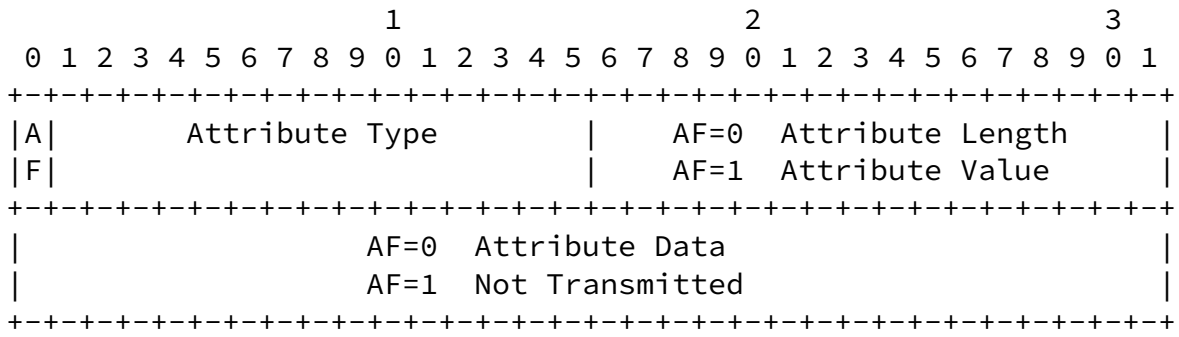


Figure 3: Parameter Attributes

The document considers only the TLV format so AF = 0 with the Parameter Types defined in Figure 4 and acceptable and default Parameter's Values are defined in Figure 2.

Attribute Type	Value	Associated Parameter
EHC Designated Strategy Range	0	ehc_strategy
ESP Alignment Range	1	esp_align
ESP LSB SPI Range	2	esp_spi_lsb
ESP LSB SN Range	3	esp_spi_sn
TCP Urgent Range	4	tcp_urgent
TCP Options Range	5	tcp_options
TCP LSB Range	6	tcp_lsb
UDP-Lite Coverage Range	7	udplite_coverage
Unassigned	8-63	
EHC Designated Strategy Value	64	ehc_strategy
ESP Alignment Value	65	esp_align
ESP LSB SPI Value	66	esp_spi_lsb
ESP LSB SN Value	67	esp_spi_sn
TCP Urgent Value	68	tcp_urgent
TCP Options Value	69	tcp_options
TCP LSB Value	70	tcp_lsb
UDP-Lite Coverage Value	71	udplite_coverage
Unassigned	72-99	
Private Use	100-127	

Figure 4: Attribute Type

7.1. Range Attribute

The Parameter's value of ehc_strategy, esp_align, esp_spi_lsb, esp_sn_lsb, tcp_urgent, tcp_options, tcp_lsb and udplite_coverage is coded on 1 byte, so the Attribute Data of the Range Attribute is 2 byte long and the Attribute Length is set to 4. The first byte indicates the minimal acceptable value, while the second byte indicates the maximal value.

Similarly, udplight_coverage is coded on 2 bytes, so the Attribute Data of the Range Attribute is 4 byte long, and Attribute Length is set to 6.

7.2. Value Attribute

The Parameters ehc_strategy, esp_align, esp_spi_lsb, esp_sn_lsb, tcp_urgent, tcp_options and tcp_lsb the Attribute Data is codes on 1 byte, and Attribute Length is set to 3.

Similarly, udplight_coverage is coded on 2 bytes, so the Attribute Data of the Value Attribute is 2 byte long and the Attribute Length is set to 4.

8. IANA Considerations

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

IKEv2 Notify Message Types - Status Types	
USE_COMPRESSED_MODE	TBA1
EHC_STRATEGY_SUPPORTED	TBA2
EHC_STRATEGY_UNACCEPTABLE_PARAMETER	TBA3

Attribute Type	Value	
EHC Designated Strategy Range	0	
ESP Alignment Range	1	
ESP LSB SPI Range	2	
ESP LSB SN Range	3	
TCP Urgent Range	4	
TCP Options Range	5	
TCP LSB Range	6	
UDP-Lite Coverage Range	7	
Unassigned		8-42
Private Use		43-63
EHC Designated Strategy Value		64
ESP Alignment Value		65

ESP LSB SPI Value	66
ESP LSB SN Value	67
TCP Urgent Value	68
TCP Options Value	69
TCP LSB Value	70
UDP-Lite Coverage Value	71
Unassigned	72-116
Private Use	117-127

Attribute Type

9. Security Considerations

10. Normative References

[I-D.mglt-ipsecme-diet-esp]
Migault, D., Guggemos, T., Bormann, C., and D. Schinazi, "ESP Header Compression and Diet-ESP", draft-mglt-ipsecme-diet-esp-06 (work in progress), May 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

Authors' Addresses

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint-Laurent, QC H4S
Canada

Email: daniel.migault@ericsson.com

Tobias Guggemos
LMU Munich
Oettingenstr. 67
80538 Munich
Germany

Email: guggemos@nm.ifi.lmu.de
URI: www.nm.ifi.lmu.de/~guggemos

David Schinazi
Apple Inc.
One Apple Park Way
Cupertino, California 95014
USA

Email: dschinazi@apple.com