Network
Internet-Draft
Intended status: Experimental
Expires: 4 September 2025

A. Antony
secunet
P. Kerpan
Cohesive Networks
P. Wouters
Aiven

3 March 2025

IKEv2 support for specifying a Delete notify reason
draft-pwouters-ipsecme-delete-info-03

Abstract

This document defines the DELETE_REASON Notify Message Status Type Payload for the Internet Key Exchange Protocol Version 2 (IKEv2) to support adding a reason for the deletion of the IKE or Child SA(s).

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 4 September 2025.

Table of Contents

1. Introduction

The IKEv2 [RFC7296] protocol supports sending a Delete Notify message, but this message cannot convey the reason why a particular Child SA or IKE SA is being deleted. It can be useful to know why a certain IPsec IKE SA or Child SA was deleted by the peer. Sometimes, when the peer's operator notices a specific SA is down, they have no idea whether this is permanent or temporary problem, and have no idea how long an outage might last. The DELETE_REASON Notify message can be added to any exchange that contains a Delete (42) payload to give more information about why the deletion is happening. The initial Delete Reason values are specified in Section 4.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Payload Format

All multi-octet fields representing integers are laid out in big endian order (also known as "most significant byte first", or "network byte order").

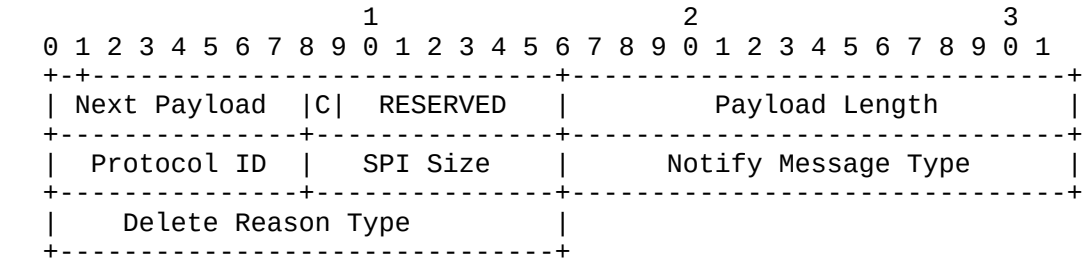
2. Delete Reason Usage

Whenever an IKE peer wishes to relay the reason for why it is deleting an IKE SA or one or more IPsec SAs, it MAY include a DELETE_REASON notify payload. The notify payload contains a single Reason Type.

A DELETE_REASON payload MUST be ignored if the exchange does not contain a Delete payload.

If multiple Delete payloads are present, the DELETE_REASON message applies to all of these. If separate different reasons should be conveyed for different Child SAs or IKE SA, those Delete messages and their accompanied DELETE_REASON messages should be sent in separate Informational Exchange messages.

3. DELETE_REASON Notify Status Message Payload format



* (C)ritical bit - MUST be 0.

* Protocol ID (1 octet) - MUST be 0. MUST be ignored if not 0.

* SPI Size (1 octet) - MUST be 0. MUST be ignored if not 0.

* Notify Status Message Type (2 octets) - set to [TBD1]

* Delete Reason Type (2 octets) - See Section 4

4. Initial Delete Reason Registry Values

The initial list of Delete Reason values and their meanings

4.1. SERVICE_SHUTDOWN

The IPsec (IKE) service is being shutdown. This implies all connections to this peer are being terminated. The service might not be restored. If the service was reached via DNS, it might be useful to refresh the DNS lookup or use another one of the IP addresses returned for the service. If the service was reached via an IKEv2 Redirect [RFC5685], it might be useful to attempt a new connection via the original redirect server again.

4.2. SERVICE_RESTART

The IPsec (IKE) service is being restarted. This implies all connections to this peer are being terminated for a brief moment while the service is restarting. Reconnecting to the service can be attempted, although there might be a brief outage trying to do so. Session Resumption tickets [RFC5723] are unlikly to be usable.

4.3. CONFIGURATION_CHILD_DELETED

The configuration for the specific Child SA parameters has been removed. This implies the peer’s IKE configuration has not been removed. If static tunnels are deployed, this means the endpoint administrators have updated the configuration and any unexpected change should be resolved by the operators. The connection likely will not work and might need to be disabled. If the configuration of the Child SA was dynamic, such as an address pool IP obtained via narrowed traffic selectors, the connection can be retried (either with the current IKE SA, or possibly by tearing down the IKE SA as well and restarting the entire connection from scratch.

4.4. CONFIGURATION_IKE_DELETED

The configuration for the specific IKE SA peer has been removed. This implies the peer will not accept a new connection with the exact same IKE parameters as those that were just in use.

4.5. CONFIGURATION_IKE_UPDATED

The configuration for the specific IKE SA peer has been updated. Depending on the configuration change, this might require an update to the location configuration or not. For example, an updated PreSharedKey would require a configuration update. A change of accepted algorithms might mean that the IKE SA can be established with a different algorithm that the one that was in use on this IKE SA.

4.6. ADMINISTRATIVELY_DOWN

The configuration for the IKE SA or Child SA has been disabled and the running connection has been torn down. This implies that reconnection is prevented until an administrative issue is resolved. This could be related to temporary network topology changes (e.g. subnet is no longer being offered) or billing related (e.g. user needs to pay a bill)

4.7. IDLE_TIMEOUT

The instance of the IKE SA or Child SA has been disabled due to inactivity. This implies reconnecting again is possible.

4.8. INITIAL_CONTACT_REPLACED

A new IKE SA with this peer was established that signaled INITIAL_CONTACT, meaning the peer claimed all older instances of this IKE SA and all its Child SAs are no longer alive and should be terminated.

4.9. REPLACED_SA

This IKE SA or Child SA was replaced by a newer one and is therefor terminated. This could be the losing SA in a simultanious rekey event, the peer has re-authenticaed and established a new IKE SA and child SAs and this SA is no longer used, or the peer established fresh IKE SA or fresh Child SAs and the older ones are being deleted. For example when a peer does not allow or support identical Child SAs under different IKE SAs.

4.10. LIFETIME_EXCEEDED

The IKE SA or Child SA reached its local lifetime counter (bytes or seconds or packets) and was not rekeyed in time.

5. Operational Considerations

The reason for supporting Deletion Reasons is for peer systems and their administrators to get a better idea of what is going on. Often in the field, people attempt to debug a failed connection only to find out much later that the configuration was simply removed from the peer. Administrators would now be able to find a reason for the connection being brought down by the peer.

While most reasons might be useful primarily to interactive operations that are (re)configuring and testing their configurations, some automated actions could be taken. For example, a connection that received ADMINISTRATIVELY_DOWN, could place a connection in "standby mode" and prevent further attempts for IKE SA or Child SA connections. Such behaviour SHOULD NOT be done without sending a high priority alert on the device. It might even make sense to keep a limited retry alive (for example hourly) in case the peer send such a message by mistake. This would allow a recovery - even if slowly.

6. Security Considerations

As Delete Reasons are authenticated by the peer, these can be trusted and acted upon in the determinations on what to do in response to the deletion of the IKE or Child SA. This only allows improved fine tuning of a system, but does not change the security aspect in any way beyond the above mentioned Operational Considerations.

7. IANA Considerations

This document adds one new IKEv2 Notify Message Status Type value and one new IKEv2 registry.

7.1. Delete Reason Notify

The following Notify Message Status is added:

Value	IKEv2 Notify Message Status Type	Reference
[TBD1]	DELETE_REASON	[this document]

Figure 1

7.2. Delete Reason Registry

This document requests IANA create the IKEv2 Notify Message Delete Reason Registry under the Internet Key Exchange Version 2 (IKEv2) Parameters Registry with the following fields and initial values:

Type	Reason Name	Reference
0	RESERVED	[this document]
1	SERVICE_SHUTDOWN	[this document]
2	SERVICE_RESTART	[this document]
3	CONFIGURATION_CHILD_DELETED	[this document]
4	CONFIGURATION_IKE_DELETED	[this document]
5	CONFIGURATION_IKE_UPDATED	[this document]
6	ADMINISTRATIVELY_DOWN	[this document]
7	IDLE_TIMEOUT	[this document]
9	INITIAL_CONTACT_REPLACED	[this document]
10	REPLACED_SA	[this document]
11	LIFETIME_EXCEEDED	[this document]
12-255	Unassigned	
256 - 65279	Unassigned	
65280 - 65535	Private Use Values	

Figure 2

The registry values 0-255 are assigned using the RFC Required registration policy.

The registry values 256-65279 are assigned using the First Come First Servce registration policy.

The registry values 65280-65535 are reserved for Private Use and Experimental Use

7.3. Designated Expert Advise

The Designated Expert (DE) for this new registry should verify that the entry makes sense within the IKEv2 protocol context and is distinct from existing entries in the registry.

8. Implementation Status

[Note to RFC Editor: Please remove this section and the reference to [RFC6982] before publication.]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was

supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

Authors are requested to add a note to the RFC Editor at the top of this section, advising the Editor to remove the entire section before publication, as well as the reference to [RFC7942].

8.1. Libreswan

Organization: The Libreswan Project

Name: https://libreswan.org/

Code: https://github.com/libreswan/libreswan

Description: An initial IKE implementation using the Private Use value 40960 for the Notify payload

Level of maturity: Beta

Coverage: Implements the draft’s example reasons

Licensing: GPLv2

Implementation experience: TBD

Contact: Libreswan Development: swan-dev@libreswan.org

9. References

9.1. Normative References

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[RFC5685] Devarapalli, V. and K. Weniger, "Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5685, DOI 10.17487/RFC5685, November 2009, <https://www.rfc-editor.org/info/rfc5685>.

[RFC5723] Sheffer, Y. and H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption", RFC 5723, DOI 10.17487/RFC5723, January 2010, <https://www.rfc-editor.org/info/rfc5723>.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, DOI 10.17487/RFC6982, July 2013, <https://www.rfc-editor.org/info/rfc6982>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

Authors' Addresses

Antony Antony
secunet Security Networks AG
Email: antony.antony@secunet.com

Patrick Kerpan
Cohesive Networks
Email: pjkerpan@cohesive.net

Paul Wouters
Aiven
Email: paul.wouters@aiven.io