

Network Working Group
Internet-Draft
Updates: [4555](#) (if approved)
Intended status: Standards Track
Expires: May 19, 2022

V. Smyslov
ELVIS-PLUS
November 15, 2021

Responder Initiated IP Addresses Update in MOBIKE
draft-smyslov-ipsecme-ikev2-r-mobike-09

Abstract

IKEv2 Mobility and Multihoming Protocol (MOBIKE), defined in [[RFC4555](#)] allows peers to update their IP addresses without re-establishing IKE and IPsec Security Associations (SAs). In the MOBIKE protocol it is the initiator of the IKE SA, who is responsible for selecting new SA addresses and for initiating the IP addresses update procedure. This document presents an extension to the MOBIKE protocol that allows the responder to initiate IP address update. The document updates [[RFC4555](#)].

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 May 19, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

Internet-Draft

R-MOBIKE

November 2021

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology and Notation	3
3.	Protocol Overview	3
4.	Protocol Description	4
4.1.	Capability Advertising	4
4.2.	Responder Initiated IP Address Update	5
5.	Payload Formats	7
5.1.	MOBIKE_SUPPORTED Notification	7
5.2.	SWITCH_TO_IP_ADDRESS Notification	7
6.	Security Considerations	7
7.	IANA Considerations	8
8.	References	8
8.1.	Normative References	8
8.2.	Informative References	8
	Author's Address	8

[1.](#) Introduction

The Internet Key Exchange protocol version 2 (IKEv2), specified in [[RFC7296](#)], is a key part of the IP Security (IPsec) architecture. It allows peers to perform authenticated key exchange, which results in establishing IKE Security Association (IKE SA) and to create a data protection channels called IPsec Security Associations (IPsec SAs). In original IKEv2 the IKE and IPsec SAs are established between the IP addresses used in IKEv2 negotiation. The IKEv2 Mobility and Multihoming Protocol (MOBIKE), specified in [[RFC4555](#)], extends the IKEv2 functionality by allowing peers to dynamically change IP addresses of the established SAs without the need to re-establish these SAs.

The main use case for the MOBIKE protocol is a remote access user that travels and moves from one IP address to another without re-establishing existing SAs with the VPN gateway. However, the MOBIKE also supports more complex scenarios when VPN gateway is multihomed and its addresses may change over time.

In the MOBIKE it is the original initiator of the IKE SA (e.g. the remote access client) who is responsible for detecting the working IP addresses pairs and for deciding which pair to use. In other words, the responder (e.g. the VPN gateway) plays a passive role and could neither initiate the IP address update process nor tell the initiator

which IP address is preferred to use. This limitation makes use of complex scenarios less efficient and decreases the value of MOBIKE protocol.

For example, if the VPN gateway is a load sharing cluster where each node has its own IP address, then the cluster must be able to move SA between nodes depending on their current load. Currently Redirect Mechanism for IKEv2 [[RFC5685](#)] can accomplish this task, however it requires new IKE SA to be established, that is very inefficient. Another possible solution is to use IKE SA Cloning along with the MOBIKE (see [[RFC7791](#)] for scenario description), but the limitation of the MOBIKE protocol makes this problematic. Obviously, the client has insufficient information to choose when and to which of cluster IP addresses to move an SA to and the VPN gateway has no means to provide the client with this information.

This specification extends the MOBIKE protocol by adding ability for the responder to ask the initiator for IP address update and to provide it with the new IP address to use.

[2.](#) Terminology and Notation

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.

In this document the term "initiator" means the party who originally initiated the first IKE SA (in a series of possibly several rekeyed IKE SAs), and "responder" means the other party. This is consistent with a way these terms are used in [[RFC4555](#)]. Note, that in [[RFC7296](#)] the terms "original initiator" and "original responder" mean the party, who initiated (or responded to) the latest IKE SA in a series of possibly several rekeyed IKE SAs.

[3.](#) Protocol Overview

The MOBIKE protocol is designed in such a way, that it is the IKE SA initiator, who is responsible for performing the actions concerned with the selecting of a working IP addresses pair and for initiating an IP addresses update exchange. Usually the initiator selects an IP addresses pair by periodically probing different pairs and choosing the working one. If several pairs work then the choice between them is arbitrary. The responder cannot influence the process of selecting and cannot ask the client to immediately switch to a particular gateway's address. As a result the process of selection a

new pair takes substantial time and may ends up with a suboptimal path.

Obviously, this limitation comes from the fact that there might be middleboxes on the path like Network Address Translators (NAT) or firewalls, that might disallow IP packets to come from VPN gateway to the client unless the client first contacts the VPN gateway. For example, the client might reside behind a dynamic NAT that creates a mapping when IP packet first comes from the client to the gateway. If the gateway tries to send an IP packet to the client from different IP address, the packet would be dropped since the NAT box has no corresponding mapping.

This specification provides the following solution to the described problem. When the responder decides that its end of existing SA should be switched from its original IP address IP_R1 to a new IP address IP_R2, it initiates an INFORMATIONAL exchange containing a new notification SWITCH_TO_IP_ADDRESS, that contains IP_R2. Once the initiator completes an exchange containing SWITCH_TO_IP_ADDRESS notification, it immediately initiates standard MOBIKE procedure for updating SA addresses by starting the INFORMATIONAL exchange containing UPDATE_SA_ADDRESSES notification.

[4.](#) Protocol Description

[4.1.](#) Capability Advertising

According to [[RFC4555](#)], the peers must exchange MOBIKE_SUPPORTED notifications in the IKE_AUTH exchange before they can use the MOBIKE

protocol. If the initiator supports this specification and is willing to use it, then it MUST include a single octet 0x52 ('R') in the notification data of the MOBIKE_SUPPORTED notification sent to the responder. There is no need for the initiator to know whether the responder supports this specification or not, so the MOBIKE_SUPPORTED notification sent by the responder has an empty notification data.

Note, that [\[RFC4555\]](#) specifies that MOBIKE_SUPPORTED notification must contains no data when sending and the content of the notification data must be ignored while parsing. So, if the responder doesn't support this specification, it will just ignore the content of the MOBIKE_SUPPORTED notification and will use MOBIKE without this extension.

```
(IP_I1:500 -> IP_R1:500) -->
HDR, SAi1, KEi, Ni,
    N(NAT_DETECTION_SOURCE_IP),
    N(NAT_DETECTION_DESTINATION_IP)

<-- (IP_R1:500 -> IP_I1:500)
    HDR, SAr1, KEr, Nr,
        N(NAT_DETECTION_SOURCE_IP),
        N(NAT_DETECTION_DESTINATION_IP)

(IP_I1:4500 -> IP_R1:4500) -->
HDR, SK { IDi, CERT, AUTH,
    SAi2, TSi, TSr,
    N(MOBIKE_SUPPORTED('R')) }

<-- (IP_R1:4500 -> IP_I1:4500)
    HDR, SK { IDr, CERT, AUTH,
        SAr2, TSi, TSr,
        N(MOBIKE_SUPPORTED),
        N(ADDITIONAL_IP4_ADDRESS) }
```

[4.2.](#) Responder Initiated IP Address Update

If the initiator advertised its support for this specification during the initial exchange as described in [Section 4.1](#), then the responder is free to initiate IP Address Update request at any time. If the initiator doesn't indicate its support for this extension, then the responder MUST NOT initiate IP Address Update request. The IP Address Update request MUST NOT be initiated by the initiator, the responder MUST NOT take any action if it receives such a request (apart from sending an empty response message to complete the exchange).

It is up to the responder to decide when to initiate an IP Address Update request and what new address to include into it. Some of the possible reasons are:

- o the responder is multihomed and wishes to switch an SA to a different IP address
- o the responder is a cluster and wishes to move an SA to a different node having its own IP address

The responder requests the initiator to update SA address by initiating the INFORMATIONAL exchange containing a new status type notification SWITCH_TO_IP_ADDRESS. Its notification data contains a new IP address the responder requests the initiator to use for the IKE SA and its Child SAs. In the example below the SA was

established using IP_I1 and IP_R1 addresses for the initiator and responder respectively, and the responder wishes to change the address of its end of the SA to IP_R2. So, it initiates the INFORMATIONAL exchange from IP_R1 address containing the SWITCH_TO_IP_ADDRESS notification with IP_R2 address.

```

                                <-- (IP_R1:4500 -> IP_I1:4500)
                                HDR, SK { N(SWITCH_TO_IP_ADDRESS(IP_R2)) }
(IP_I1:4500 -> IP_R1:4500) -->
HDR, SK {}
```

Upon receiving the SWITCH_TO_IP_ADDRESS notification the initiator extracts its content and makes a decision whether the received IP address is appropriate for the SA. If the received IP address is among the addresses previously received from the responder in

ADDITIONAL_IP4_ADDRESS or ADDITIONAL_IP6_ADDRESS notifications, then it is appropriate for the SA. Otherwise local policy must be consulted to decide whether the received IP is appropriate. If the address is considered inappropriate, then the initiator MUST current address. It is RECOMMENDED that the initiator immediately initiates Liveness Check exchange to ensure that the responder is able to operate using its current address.

If the initiator makes a decision that the received address is appropriate the initiator initiates an IP address update procedure according to the MOBIKE specification by sending an INFORMATIONAL exchange request message containing the UPDATE_SA_ADDRESSES notification. See [\[RFC4555\]](#) for details. As a result, the remote IP address of the SA is changed from IP_R1 to IP_R2. Note that only the IP address is changed, the port remains the same.

```
(IP_I1:4500 -> IP_R2:4500) -->
HDR, SK { N(UPDATE_SA_ADDRESSES),
          N(NAT_DETECTION_SOURCE_IP),
          N(NAT_DETECTION_DESTINATION_IP),
          N(COOKIE2) }

<-- (IP_R2:4500 -> IP_I1:4500)
HDR, SK { N(NAT_DETECTION_SOURCE_IP),
          N(NAT_DETECTION_DESTINATION_IP),
          N(COOKIE2) }
```

The responder MUST NOT change IP addresses of the SA until it receives the UPDATE_SA_ADDRESSES notification from the initiator.

[5.](#) Payload Formats

[5.1.](#) MOBIKE_SUPPORTED Notification

The MOBIKE_SUPPORTED Notification is defined in [\[RFC4555\]](#), [Section 4.2.1](#) with the Notify Message Type 16396. This definition requires the notification data to be empty while sending and to be ignored when notification is received.

This document updates the definition from [[RFC4555](#)]. Exchange initiator sets the notification data of the MOBIKE_SUPPORTED Notification to a single octet 0x52 ('R') to indicate that this specification is supported.

5.2. SWITCH_TO_IP_ADDRESS Notification

The Notify Message Type for this notification is <TBA by IANA>. The notification data contains new responder's IP address.

For IPv4, the notification data is 4 octets long and is defined as follows:

```

          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
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
    |                                     New Responder's IPv4 Address                                     |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

For IPv6, the notification data is 16 octets long and is defined as follows:

```

          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
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
    |                                     New Responder's IPv6 Address                                     |
    |                                     |                                     |
    |                                     |                                     |
    |                                     |                                     |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The Protocol ID and SPI Size fields are set to zero.

6. Security Considerations

This specification is an extension of the MOBIKE protocol, so the Security Considerations described in [[RFC4555](#)] are applied.

7. IANA Considerations

This document defines new Notify Message Types in the "IKEv2 Notify Message Types - Status Types" registry:

<TBA> SWITCH_TO_IP_ADDRESS

8. References

8.1. 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>>.
- [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>>.
- [RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", [RFC 4555](#), DOI 10.17487/RFC4555, June 2006, <<https://www.rfc-editor.org/info/rfc4555>>.
- [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>>.

8.2. 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>>.
- [RFC7791] Migault, D., Ed. and V. Smyshlov, "Cloning the IKE Security Association in the Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 7791](#), DOI 10.17487/RFC7791, March 2016, <<https://www.rfc-editor.org/info/rfc7791>>.

Author's Address

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd) 124460
Russian Federation

Phone: +7 495 276 0211
Email: svan@elvis.ru

Smyslov

Expires May 19, 2022

[Page 9]