Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 15, 2009

V. Devarapalli
WiChorus
K. Weniger
Panasonic
P. Eronen
Nokia
July 14, 2008

**Re-direct Mechanism for IKEv2**
**draft-devarapalli-ipsec-ikev2-redirect-02.txt**

Status of this Memo



Abstract

IKEv2 is a popular protocol for setting up VPN tunnels from a remote location to a gateway so that the VPN client can access services in the network behind the gateway. Currently there is no standard mechanism specified that allows an overloaded VPN gateway to re-direct the VPN client to attach to another gateway. This document proposes a re-direct mechanism for IKEv2. The proposed mechanism can also be used for Mobile IPv6 to enable the home agent to re-direct the mobile node to another home agent.

Table of Contents

## 1. Introduction

IKEv2 [2] is widely used for setting up IPsec-based VPNs. The IP address of the VPN gateway can be configured on the VPN client. But this does not scale well, when the number of VPN gateways is large. Dynamic discovery of VPN gateways using DNS is quite widely used too. However, using DNS is not flexible when it comes to assigning a VPN gateway to the VPN client based on the load on the VPN gateways. The VPN client typically tries to connect to the IP address of the VPN gateways that appears first in the DNS response. If the VPN tunnel setup fails, then the VPN client tries to attach to the other VPN gateways returned in the DNS response.

This document proposes a re-direct mechanism for IKEv2 that enables a VPN gateway to re-direct the VPN client to another VPN gateway, for example, based on the load condition. The re-direct is done during the IKE_SA_INIT exchange. The re-direct mechanism can also be used in conjunction with anycast addresses. In this case, anycast address for the cluster of VPN gateways is stored in the DNS instead of a list of unicast IP addresses of the VPN gateways.

The re-direct can also happen because of administrative or optimal routing reasons. This document does not attempt to provide an exhaustive list of reasons for re-directing a VPN client to another VPN gateway.

Mobile IPv6 [3] may use IKEv2 for mutual authentication between the mobile node and the home agent. IKEv2 may also be used for home address configuration and setting up IPsec security associations for protecting Mobile IPv6 signaling messages [4]. The IKEv2 exchange precedes the exchange of Mobile IPv6 signaling messages. Therefore the mechanism described in this document can be also be used by a Mobile IPv6 home agent to re-direct a mobile node to another home agent.

There is a Home Agent Switch mechanism available for re-directing a mobile node to another home agent, described in [5]. The Home Agent Switch mechanism can only be used after the binding cache had been created at the home agent for the mobile node. The disadvantage with this is that quite a bit of state is created on the home agent before the mobile node can be re-directed to another home agent. The mechanism described in this document can be used for re-directing a mobile node before any state is created on the home agent.

## 2. Terminology

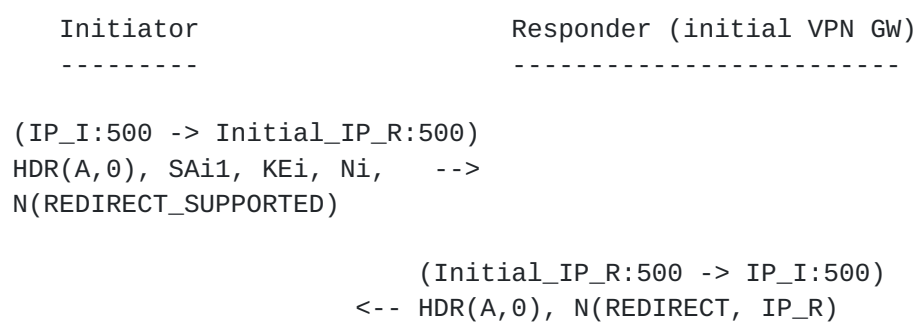
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

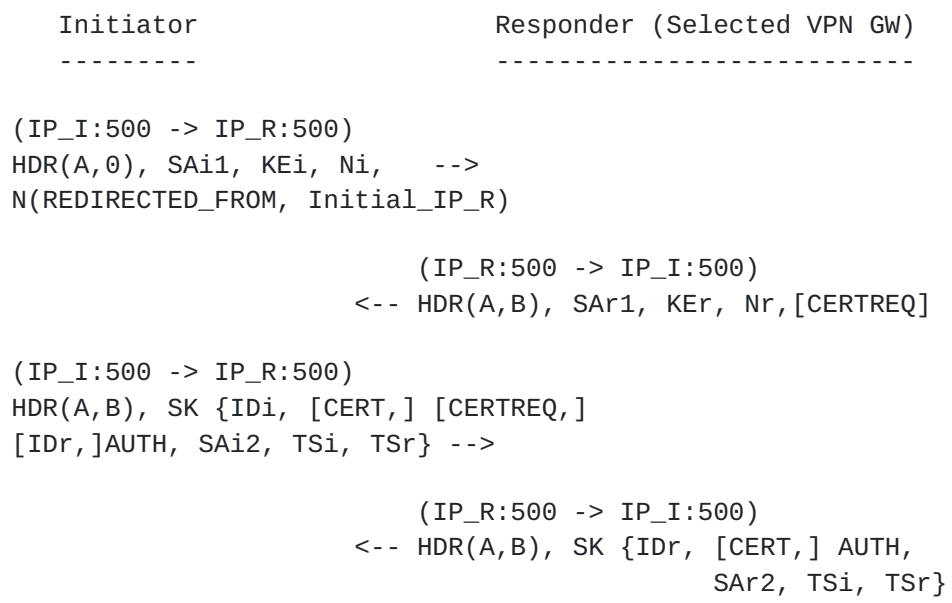
## 3. IKEv2 Exchange with Redirect

To redirect a IKEv2 session to another VPN gateway, the VPN gateway that initially received the IKE_SA_INIT request selects another VPN gateway and responds to the VPN client with a REDIRECT Notification payload. The mechanism by which the initial VPN gateway selects another VPN gateway is out of scope for this document. The IP address of the selected VPN gateway is sent in the REDIRECT payload.

The VPN client indicates support for the IKEv2 redirect mechanism by including a REDIRECT_SUPPORTED notification message in the initial IKE_SA_INIT request. If the IKE_SA_INIT request did not include the REDIRECT_SUPPORTED payload, the responder MUST NOT send the REDIRECT payload to the VPN client.




When the VPN client receives the IKE_SA_INIT response with the REDIRECT payload, it initiates a new IKE_SA_INIT exchange with the VPN gateway listed in the REDIRECT payload. The VPN client includes the IP address of the original VPN gateway that re-directed the client. The IKEv2 exchange then proceeds as normal with the selected VPN gateway.




When this mechanism is used with Mobile IPv6, a mobile node's security associations with its home agent may expire while it still has a valid binding cache entry at the home agent. In this case, the mobile node MUST NOT use the original home agent address as the destination address in the IKE_SA_INIT exchange to setup new security associations. It MUST try to setup security associations with its existing home agent.

## 4. Use of Anycast Addresses with the Re-direct Mechanism

The use of anycast addresses will avoid having to configure a particular VPN gateway's IP address in the DNS. Instead, the anycast address that represents the group of VPN gateways is stored in the DNS. When the VPN client performs a DNS lookup for the VPN gateway, it receives the anycast address of the VPN gateway in the DNS response.

If an anycast address is returned in response to DNS resolution of an FQDN, the IKEv2 transaction between the VPN client and the VPN gateway is slightly modified. The VPN client sends the IKE_SA_INIT request to the anycast address. The IKE_SA_INIT request is routed to one of the VPN gateways that is part of the anycast group. The VPN gateway that receives the IKE_SA_INIT request responds with an IKE_SA_INIT reply from the anycast address.

```
   Initiator                    Responder (any VPN GW)
   ---------                    ----------------------

 (IP_I:500 -> ANYCAST:500)
 HDR(A,0), SAi1, KEi, Ni)   -->
 N(REDIRECT_SUPPORTED)

                             (ANYCAST:500 -> IP_I:500)
                          <-- HDR(A,0), N(REDIRECT, IP_R)
```

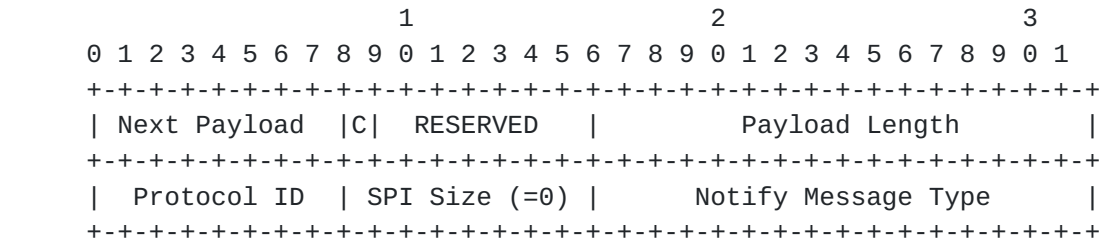
If the destination address on the IKE_SA_INIT request is an anycast address, the VPN gateway that received the IKE_SA_INIT request MUST include the REDIRECT payload to re-direct the VPN client to a unicast address of one of the VPN gateway. The VPN gateway that received the IKE_SA_INIT request MAY re-direct the client to its own unicast address, if it is not overloaded.

The rest of the IKEv2 exchange is the same as described in Section 3.

## 5. Redirect Messages

### 5.1. REDIRECT_SUPPORTED

The REDIRECT_SUPPORTED payload is included in the initial IKE_SA_INIT request by the initiator to indicate support for the IKEv2 re-direct mechanism described in this document.

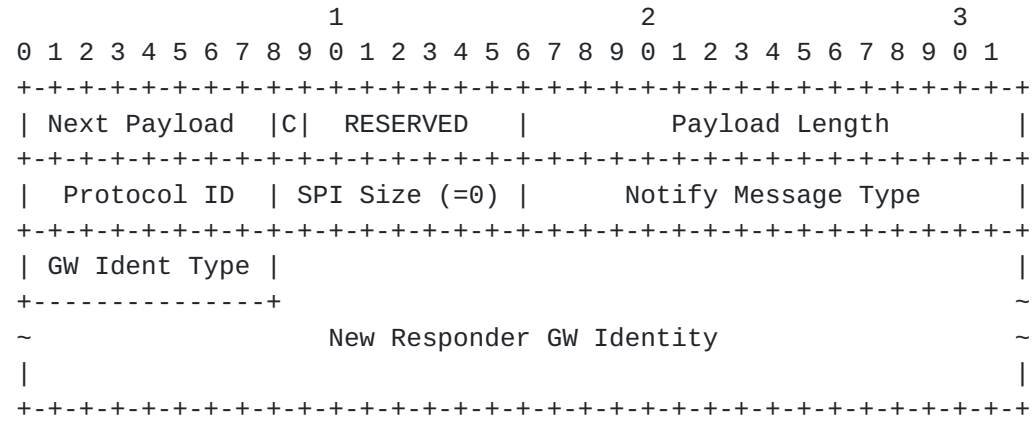



The 'Next Payload', 'Payload Length', 'Protocol ID', 'SPI Size' and the 'Notify Message Type' fields are the same as described in Section 3.10 of RFC 4306 [2]. The 'SPI Size' field MUST be set to 0 to indicate that the SPI is not present in this message.

The 'Payload Length' field MUST be set to '8'. The 'Notify Message Type' field is set to indicate the REDIRECT_SUPPORTED payload <value to be assigned by IANA>.

## 5.2. REDIRECT

The REDIRECT payload is included in an IKE_SA_INIT response from the responder when the responder wants to re-direct the initiator to another VPN gateway. The message includes the new responder's IP address.




The 'Next Payload', 'Payload Length', 'Protocol ID', 'SPI Size' and the 'Notify Message Type' fields are the same as described in Section 3.10 of RFC 4306 [2]. The 'SPI Size' field MUST be set to 0 to indicate that the SPI is not present in this message.

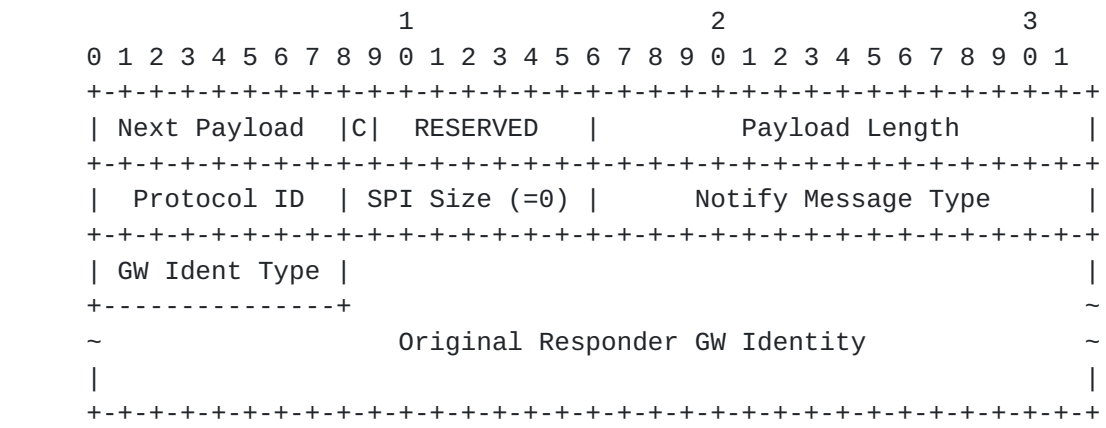
The 'Payload Length' field MUST be set to either '13' or '25' depending on whether an IPv4 or IPv6 address of the new VPN gateway is sent in the message. The 'Notify Message Type' field is set to indicate the REDIRECT payload <value to be assigned by IANA>. The 'GW Identity Type' field indicates the type of information that is sent to identify the new VPN gateway. The following values are reserved by this document.

1 - IPv4 address of the new VPN gateway
2 - IPv6 address of the new VPN gateway
3 - FQDN of the new VPN gateway

All other values for this field are reserved and MUST NOT be used. The identity of the new VPN gateway is carried in the 'New Responder GW Identity' field.

## 5.3. REDIRECTED_FROM

The REDIRECTED_FROM message type is included in the IKE_SA_INIT request from the initiator to the new VPN gateway to indicate the IP address of the original VPN gateway that re-directed the initiator. The original VPN gateway's IP address is included in the message.




The 'Next Payload', 'Payload Length', 'Protocol ID', 'SPI Size' and the 'Notify Message Type' fields are the same as described in Section 3.10 of RFC 4306 [2]. The 'SPI Size' field MUST be set to 0 to indicate that the SPI is not present in this message.

The 'Payload Length' field MUST be set to either '13' or '25' depending on whether an IPv4 or IPv6 address of the original VPN gateway is sent in the message. The 'Notify Message Type' field is set to indicate the REDIRECTED_FROM payload <value to be assigned by IANA>. The 'GW Identity Type' field indicates the type of information that is sent to identify the new VPN gateway. The following values are reserved by this document.

1 - IPv4 address of the original VPN gateway
2 - IPv6 address of the original VPN gateway

All other values for this field are reserved and MUST NOT be used. The identity of the original VPN gateway is carried in the 'Original Responder GW Identity' field.

## 6. Security Considerations

An eavesdropper on the path between VPN client and server may send a redirect to the client upon receiving an IKE_SA_INIT message from this client. This is no problem regarding DoS attacks for the VPN connection, since an on-path-attacker can as well drop the IKE_SA_INIT requests to prevent VPN access for the client. But an eavesdropper on the path between VPN client and server can redirect a large number of clients to a victim, which is then flooded with IKE_SA_INIT requests. Flooding only happens if many clients initiate IKEv2 exchange at almost the same time, which is considered a rare event. However, this may happen if a Home Agent/VPN server is shutdown for maintenance and all clients need to re-establish VPN connections with another Home Agent/VPN server or if the on-path

attacker forces all IPsec security associations to expire by dropping all received IKEv2 messages.

The use of REDIRECTED_FROM payload is intended to discourage a rogue VPN gateway from re-directing a large number of VPN clients to a particular VPN gateway. It does not prevent such a DoS attack.

## 7. IANA Considerations

This document defines three new IKEv2 Notification Message types as described in Section 5. The three Notify Message Types must be assigned values between 16396 and 40959.

- REDIRECT_SUPPORTED
- REDIRECT
- REDIRECTED_FROM

## 8. Acknowledgements

The use of anycast address with IKEv2 was first described in [6]. It was then added to an early draft version of RFC 5026 and later removed before the RFC was published. Therefore the authors of [6] and RFC 5026 are acknowledged.

Thanks to Tero Kivinen for suggesting the use of REDIRECTED_FROM payload. The authors would also like to thank Yaron Sheffer and Arnaud Ebalard for their reviews and comments.

## 9. References

### 9.1. Normative References

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

[2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

### 9.2. Informative References

[3] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[4] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[5] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.

[6] Weniger, K. and F. Dupont, "IKEv2-based Home Agent Assignment in Mobile IPv6/NEMO Bootstrapping", draft-dupont-ikev2-haassign-02 (work in progress), January 2007.

## Authors' Addresses

Vijay Devarapalli
WiChorus
3590 North First St
San Jose, CA 95134
USA

Email: vijay@wichorus.com

Killian Weniger
Panasonic R&D Center Germany
Monzastr. 4c
Langen 63225
Germany

Email: kilian.weniger@eu.panasonic.com

Pasi Eronen
Nokia
P.O. Box 407
FIN-0045 Nokia Group
Finland

Email: pasi.eronen@nokia.com

## Full Copyright Statement



## Intellectual Property