                          Redirect Mechanism for
            the Internet Key Exchange Protocol Version 2 (IKEv2)

## Abstract

   The Internet Key Exchange Protocol version 2 (IKEv2) is a protocol
   for setting up Virtual Private Network (VPN) tunnels from a remote
   location to a gateway so that the VPN client can access services in
   the network behind the gateway.  This document defines an IKEv2
   extension that allows an overloaded VPN gateway or a VPN gateway that
   is being shut down for maintenance to redirect the VPN client to
   attach to another gateway.  The proposed mechanism can also be used
   in Mobile IPv6 to enable the home agent to redirect the mobile node
   to another home agent.

## Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

## Copyright Notice

Table of Contents

1.  Introduction

   IKEv2 [2] is used for setting up IPsec-based [7] 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
   gateway 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 redirect mechanism for IKEv2 that enables a
   VPN gateway to redirect the VPN client to another VPN gateway, for
   example, based on the load condition.  The redirect can be done
   during the IKE_SA_INIT or the IKE_AUTH exchange.  Gateway-initiated

redirect in the middle of a session is also supported.  The redirect
mechanism can also be used in conjunction with anycast addresses.  In
this case, an 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 redirect can also happen because of administrative or optimal-
routing reasons.  This document does not attempt to provide an
exhaustive list of reasons for redirecting a VPN client to another
VPN gateway.

## 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 Initial Exchange with Redirect

This section describes the use of the redirect mechanism during the
IKE_SA_INIT exchange.  Gateway-initiated redirect during an active
session and the use of redirect during IKE_AUTH exchange are
explained in subsequent sections.

The VPN client indicates support for the IKEv2 redirect mechanism and
its willingness to be redirected by including a REDIRECT_SUPPORTED
notification message in the initial IKE_SA_INIT request (see
Section 9.1).  The gateway MUST keep track of those clients that
indicated support for the redirect mechanism and those that didn't.

To redirect an IKEv2 session to another VPN gateway, the VPN gateway
that initially received the IKE_SA_INIT request selects another VPN
gateway (how the selection is made is beyond the scope of this
document) and replies with an IKE_SA_INIT response containing a
REDIRECT notification message (see Section 9.2).  The notification
includes information about the selected VPN gateway and the nonce
data from the Ni payload in the IKE_SA_INIT request.  If the
IKE_SA_INIT request did not indicate support for the redirect
mechanism, the responder MUST NOT send the REDIRECT payload to the
VPN client.  This is applicable to all REDIRECT scenarios described
in this document.

Note that when the IKE_SA_INIT response includes the REDIRECT
notification, the exchange does not result in the creation of an
IKE_SA and the responder Security Parameter Index (SPI) will be zero.

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

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

                            (Initial_IP_R:500 -> IP_I:500)
                      <-- HDR(A,0), N(REDIRECT, New_GW_ID, Ni_data)
```

When the client receives the IKE_SA_INIT response, it MUST verify
that the nonce data matches the value sent in the IKE_SA_INIT
request.  If the values do not match, the client MUST silently
discard the response (and keep waiting for another response).  This
prevents certain denial-of-service (DoS) attacks on the initiator
that could be caused by an attacker injecting IKE_SA_INIT responses
with REDIRECT payloads.

After verifying the nonce data, the client initiates a new
IKE_SA_INIT exchange with the VPN gateway listed in the REDIRECT
payload, provided this is allowed by its Peer Authorization Database
(PAD) entries.  In the IKE_SA_INIT exchange with the new VPN gateway,
the client MUST include the REDIRECTED_FROM payload (see
Section 9.3).  The VPN client includes the IP address of the original
VPN gateway that redirected the client in the REDIRECTED_FROM
notification.  The IKEv2 exchange then proceeds as it would have
proceeded with the original VPN gateway.

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

  (IP_I:500 -> IP_R:500)
  HDR(A,0), SAi1, KEi, Ni,    -->
  N(REDIRECTED_FROM, Initial_IP_R)

                            (IP_R:500 -> IP_I:500)
                      <-- HDR(A,B), SAr1, KEr, Nr,[CERTREQ]

  (IP_I:500 -> IP_R:500)
  HDR(A,B), SK {IDi, [CERT,] [CERTREQ,]
  [IDr,]AUTH, SAi2, TSi, TSr} -->

                            (IP_R:500 -> IP_I:500)
                      <-- HDR(A,B), SK {IDr, [CERT,] AUTH,
                                        SAr2, TSi, TSr}
```

The client MAY get redirected again by the new VPN gateway if the new
VPN gateway also cannot serve the client.  The client does not have
to include the REDIRECT_SUPPORTED payload again in the IKE_SA_INIT
exchange with the new gateway after a redirect.  The presence of the
REDIRECT_FROM payload in the IKE_SA_INIT exchange with the new
gateway indicates to the new gateway that the client supports the
redirect mechanism.

When the client gets redirected, it MUST use the same Peer
Authorization Database (PAD) and Security Policy Database (SPD)
entries as it would have used with the original gateway.  Receiving a
redirect notification MUST NOT result in the modification of any PAD
or SPD entries.  In practice, this means the new gateway either has
to use the same responder identity (IDr) as the original gateway, or
both should be part of a group of responders that are authorized by
the same PAD entry.  See Section 4.4.3.1 of [7] on using DNS names to
represent a group of peers in a PAD entry.

This document allows the client to be redirected in several protocol
states.  In some of them, the gateway is already authenticated at the
point of redirect; in others, it is not.  We emphasize that the above
rules regarding the identity of the new gateway and the PAD and SPD
entries apply equally to all these scenarios.

4.  Use of Anycast Addresses with the Redirect Mechanism

Using anycast addresses will avoid the necessity of configuring 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 the DNS resolution
of a Fully Qualified Domain Name (FQDN), the VPN client sends the
IKE_SA_INIT request to the anycast address.  The REDIRECT_SUPPORTED
payload is included in the IKE_SA_INIT request sent 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, New_GW_ID, Ni_data)
```

   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 redirect the VPN client to a unicast
   address of one of the VPN gateways.  The VPN gateway that received
   the IKE_SA_INIT request MAY redirect 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 during an Active Session

   The redirect mechanism may also be used by a VPN gateway to redirect
   the client to another VPN gateway in the middle of a session.  To
   redirect a client, the gateway should send an INFORMATIONAL message
   with the REDIRECT Notify payload.  The REDIRECT payload MUST carry
   information about the new VPN gateway.  The gateway MUST NOT include
   any nonce data in the REDIRECT payload, since it is a gateway-
   initiated redirect and is protected by the IKEv2 security
   association.  When the client receives this message, it sends a
   response (usually empty) to the gateway.  The gateway retransmits the
   redirect INFORMATIONAL message as described in [2], until it gets a
   response.  The following illustrates the INFORMATIONAL message
   exchange for gateway-initiated redirect.

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

                              <--  HDR, SK {N(REDIRECT, New_GW_ID)}

   HDR, SK {} -->
```

   The INFORMATIONAL message exchange described above is protected by
   the existing IKEv2 SA between the client and the gateway.

   Once the client sends an acknowledgement to the gateway, it SHOULD
   delete the existing security associations with the old gateway by
   sending an INFORMATIONAL message with a DELETE payload.  The gateway
   MAY also decide to delete the security associations without any

signaling from the client, again by sending an INFORMATIONAL message
with a DELETE payload; however, it should allow sufficient time for
the client to set up the required security associations with the new
security gateway.  This time period should be configurable on the
gateway.

## 6.  Redirect during IKE_AUTH Exchange

If the gateway decides to redirect the client during the IKE_AUTH
exchange, based on the identity presented by the client in the
IKE_AUTH request message, it prevents the creation of a CHILD SA and
sends the REDIRECT payload in the IKE_AUTH response.  The gateway
MUST verify the client's AUTH payload before sending the REDIRECT
payload, and the client MUST verify the gateway's AUTH payload before
acting on the REDIRECT payload.  Since the AUTH payloads were
exchanged and successfully verified, the IKEv2 security association
is valid.  When the client receives the IKE_AUTH response with the
REDIRECT payload, it SHOULD delete the IKEv2 security association
with the gateway by sending an INFORMATIONAL message with a DELETE
payload.

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

   (IP_I:500 -> IP_R:500)
   HDR(A,0), SAi1, KEi, Ni,    -->
   N(REDIRECTED_SUPPORTED)

                                  (IP_R:500 -> IP_I:500)
                             <-- HDR(A,B), SAr1, KEr, Nr,[CERTREQ]

   (IP_I:500 -> IP_R:500)
   HDR(A,B), SK {IDi, [CERT,] [CERTREQ,]
   [IDr,]AUTH, SAi2, TSi, TSr} -->

                                  (IP_R:500 -> IP_I:500)
                             <-- HDR(A,B), SK {IDr, [CERT,] AUTH,
                                        N(REDIRECT, New_GW_ID)}
```

In case the IKE_AUTH exchange involves Extensible Authentication
Protocol (EAP) authentication (as described in Section 2.16 of RFC
4306 [2]) or multiple authentication methods (as described in RFC
4739 [6]), the gateway may decide to redirect the client based on the
interaction with the Authentication, Authorization, and Accounting
(AAA) server or the external authentication server.  In this case,
the gateway MUST send the REDIRECT Notify payload in either the first
or the last IKE_AUTH response.  The client and the gateway MUST
verify the AUTH payloads as described above.

When EAP is used, the gateway MAY also redirect the client based on
the unauthenticated identity presented by the client in the first
IKE_AUTH exchange, itself.  Since EAP is used as the authentication
mechanism, the client does not include AUTH payload to authenticate
its identity, but the server MUST still include its own AUTH payload,
and the client MUST verify it.  Note that the IKEv2 SA is not created
in this case and the client does not have to explicitly delete the
IKEv2 SA.

In all of the cases above, the client MUST accept the REDIRECT
notification only in the first IKE_AUTH response or the last IKE_AUTH
response.  It MUST NOT accept the REDIRECT notification in an
intermediate IKE_AUTH response.

7.  Handling Redirect Loops

The client could end up getting redirected multiple times in a
sequence, either because of a wrong configuration or a DoS attack.
The client could even end up in a loop with two or more gateways
redirecting the client to each other.  This could deny service to the
client.  To prevent this, the client SHOULD be configured to not
accept more than a certain number of redirects (MAX_REDIRECTS) within
a short time period (REDIRECT_LOOP_DETECT_PERIOD) for a particular
IKEv2 SA setup.  The default value for the MAX_REDIRECTS
configuration variable is 5.  The default value for the
REDIRECT_LOOP_DETECT_PERIOD configuration variable is 300 seconds.
Client implementations may allow these variables to be configured,
depending on a specific deployment or system configuration.

8.  Using the Redirect Mechanism with Mobile IPv6

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

There is a Home Agent Switch mechanism available for redirecting a
mobile node to another home agent, described in [5].  The Home Agent
Switch mechanism can only be used after the binding cache has 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 redirected to another home agent.  The
mechanism described in this document can be used for redirecting a
mobile node before any state related to the Mobile IPv6 binding is
created on the home agent.

When running IKEv2 between a Mobile IPv6 mobile node (MN) and home
agent (HA), redirecting the IKEv2 exchange to another HA is not
enough; the Mobile IPv6 signaling also needs to be sent to the new HA
address.  The MN MAY treat the information received in the
IKE_SA_INIT response in a similar way as it would treat HA discovery
information received from other unauthenticated (and potentially
untrustworthy) sources (such as DNS lookups not protected with DNS
Security (DNSSEC)).  However, if the MN has authenticated information
about its home agent, it MUST NOT be updated based on the IKE_SA_INIT
response.

If the REDIRECT notification is received during the IKE_AUTH exchange
(after the HA has been authenticated; see Section 6), the MN MAY pass
the new address to Mobile IPv6 and treat it in a similar fashion as
information from the Home Agent Switch message [5].

Gateway-initiated REDIRECT notifications exchanged in INFORMATIONAL
exchanges (see Section 5) MUST NOT result in updating any Mobile IPv6
state.  In such cases, the Home Agent Switch message specified in [5]
is used instead.

## 9.  Redirect Messages

## 9.1.  REDIRECT_SUPPORTED

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

```
                     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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Protocol ID(=0)| SPI Size (=0) |      Notify Message Type      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

The 'Payload Length' field is set to the length in octets of the
entire payload, including the generic payload header.  The 'Notify
Message Type' field is set to indicate the REDIRECT_SUPPORTED payload
(16406).

9.2.  REDIRECT

   When the responder wants to redirect the initiator to another VPN
   gateway, the REDIRECT payload is included in either an IKE_SA_INIT
   response from the responder or an INFORMATIONAL message from the
   responder.  The message includes the new responder's IP address or
   DNS name.
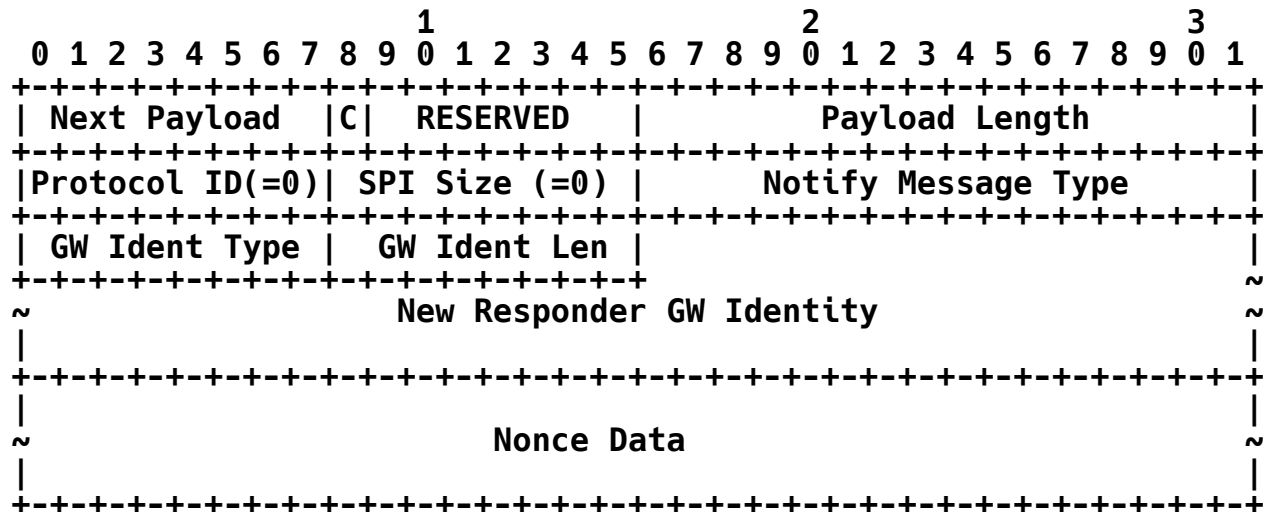
```
                        1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Next Payload  |C|  RESERVED   |          Payload Length       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Protocol ID(=0)| SPI Size (=0) |      Notify Message Type       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | GW Ident Type | GW Ident Len  |                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               ~
   ~                    New Responder GW Identity                 ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ~                         Nonce Data                           ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

   The 'Payload Length' field is set to the length in octets of the
   entire payload, including the generic payload header.  The 'Notify
   Message Type' field is set to indicate the REDIRECT payload (16407).
   The 'GW Identity Type' field indicates the type of information that
   is sent to identify the new VPN gateway.  The following values are
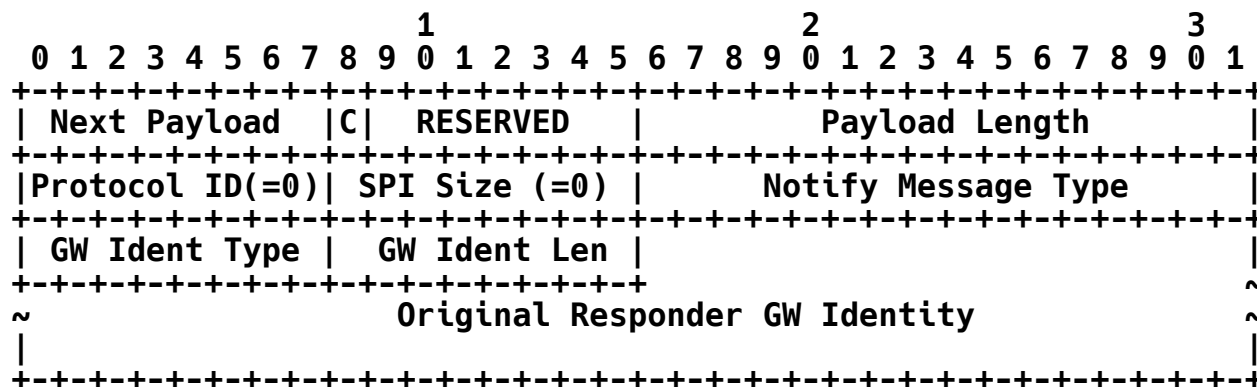   valid in the REDIRECT payload.

      1 - IPv4 address of the new VPN gateway

      2 - IPv6 address of the new VPN gateway

      3 - FQDN of the new VPN gateway

The 'GW Ident Len' field is set to the length of the gateway identity
information.  The identity of the new VPN gateway is carried in the
'New Responder GW Identity' field.  The IPv4 address, the IPv6
address, or the FQDN of the new VPN gateway MUST be encoded as
described in Section 3.5 of [2].

The 'Nonce Data' field carries the nonce data from the Ni payload
sent by the initiator.  The size of the nonce MUST be between 16 and
256 bytes, as described in Section 3.9 of [2].  The 'Nonce Data'
field is present in the REDIRECT payload only when the REDIRECT
payload is sent in the IKE_SA_INIT response message.  It MUST NOT be
included in the REDIRECT payload if sent in an IKE_AUTH response or
in a gateway-initiated redirect message.

## 9.3.  REDIRECTED_FROM

The REDIRECTED_FROM Notify payload 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 redirected the initiator.
The original VPN gateway's IP address is included in the message.  If
the IKE_SA_INIT request was sent to any anycast address (see
Section 4), then the anycast address is included in the message.
This payload also serves the purpose of indicating support for the
redirect mechanism to the new VPN gateway after a redirect.

```
                      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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Protocol ID(=0)| SPI Size (=0) |      Notify Message Type      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| GW Ident Type | GW Ident Len  |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               ~
~                 Original Responder GW Identity                ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

The 'Payload Length' field is set to the length in octets of the
entire payload, including the generic payload header.  The 'Notify
Message Type' field is set to indicate the REDIRECTED_FROM payload

(16408).  The 'GW Identity Type' field indicates the type of
information that is sent to identify the new VPN gateway.  The
following values are valid in the REDIRECTED_FROM payload.

    1 - IPv4 address of the original VPN gateway

    2 - IPv6 address of the original VPN gateway

The 'GW Ident Len' field is set to the length of the gateway identity
information.  The identity of the original VPN gateway is carried in
the 'Original Responder GW Identity' field.

## 10.  Use of the Redirect Mechanism between IKEv2 Peers

The redirect mechanism described in this document is mainly intended
for use in client-gateway scenarios.  However, the mechanism can also
be used between any two IKEv2 peers.  But this protocol is
asymmetric, meaning that only the original responder can redirect the
original initiator to another server.

## 11.  Security Considerations

An eavesdropper on the path between a 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 the REDIRECTED_FROM payload is intended to discourage a
rogue VPN gateway from redirecting a large number of VPN clients to a
particular VPN gateway.  It does not prevent such a DoS attack.

The redirect mechanism MUST NOT update any state on the client apart
from the VPN gateway information.  When used with Mobile IPv6, care
must be taken to ensure that the home agent information that the
mobile node has configured is not modified wrongly by the redirect
message.

Redirecting based on the unauthenticated identities from the client
might leak out information about the user when an active attacker,
pretending to be a VPN client, can get information on the gateway to
which the real user was redirected.  If redirection is based on some
internal information of the user, it might leak information (that
might not be available otherwise) about the user to the attacker.  To
prevent these kinds of attacks, redirection based on unauthenticated
IDs should be avoided and should be done only after the client has
also authenticated itself.

## 12.  IANA Considerations

This document defines three new IKEv2 Notify Message Types, as
described in Section 9.  The three Notify Message Types have been
assigned the following values:

   16406 - REDIRECT_SUPPORTED

   16407 - REDIRECT

   16408 - REDIRECTED_FROM

This document creates a new namespace called the "Gateway Identity
Type".  This is used to indicate the type of information regarding
the VPN gateway that is carried in the REDIRECT (Section 9.2) and
REDIRECTED_FROM (Section 9.3) Notify payloads.  The following values
have been assigned.

   1 - IPv4 address of the VPN gateway

   2 - IPv6 address of the VPN gateway

   3 - FQDN of the VPN gateway

Value '0' is reserved.  Values 4-240 are unassigned.  New values can
be allocated by Expert Review [8].  Values 241-255 are set aside for
private use.  A specification that extends this registry MUST also
mention which of the new values are valid in which Notify payload.

## 13.  Acknowledgements

The use of anycast addresses with IKEv2 was first proposed by K.
Weniger and F. Dupont in the context of home agent assignment in
Mobile IPv6 / Network Mobility (NEMO) bootstrapping.  It was then
added to an early version of [4] and later removed before the RFC was
published.  The authors of RFC 5026 are acknowledged.

## 14.  References

### 14.1.  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.

### 14.2.  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]   Eronen, P. and J. Korhonen, "Multiple Authentication Exchanges
      in the Internet Key Exchange (IKEv2) Protocol", RFC 4739,
      November 2006.

[7]   Kent, S. and K. Seo, "Security Architecture for the Internet
      Protocol", RFC 4301, December 2005.

[8]   Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA
      Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

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

   EMail: vijay@wichorus.com


   Kilian Weniger
   Unaffiliated

   EMail: kilian.weniger@googlemail.com