Re-direct Mechanism for IKEv2

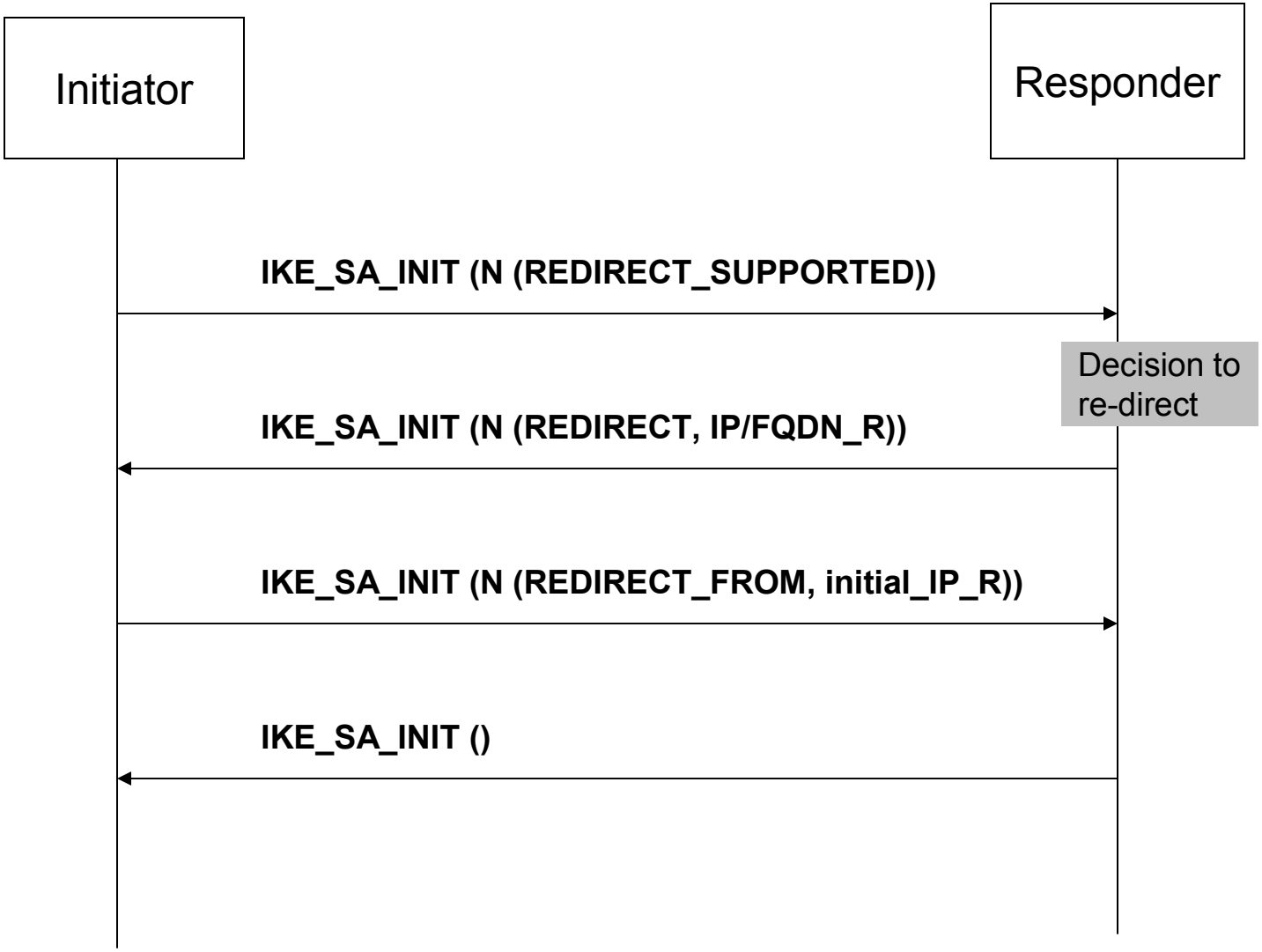
IPSECME, IETF 72

Vijay Devarapalli (vijay@wichorus.com)
Pasi Eronen (pasi.eronen@nokia.com)
Kilian Weniger (kilian.weniger@eu.panasonic.com)

IKEv2 Re-direct Mechanism

- The re-direct mechanism for IKEv2 allows a IKEv2 responder to re-direct the client to another responder
- Mainly useful for client-gateway IKEv2 exchanges
  - IPsec VPNs
  - Mobile IPv6 sessions between mobile nodes and home agents
- Typically based on load condition
  - Other use cases like subscription profile-based also possible

IKEv2 Re-direct Mechanism



Use of Anycast Addresses

- The use of anycast address avoids configuring a particular VPN gateway's IP address in the DNS
  - Anycast address stored in the DNS
- The IKE_SA_INIT request is sent to the anycast address
- The response comes back from the anycast address re-directing the client to a particular VPN gateway
  - Use of any other address as the source address may cause the firewalls to drop the packet
  - If the initial responder is not over-loaded, it re-directs the client to it's own unicast address
- The one disadvantage is that there is always an additional round trip during the IKE_SA_INIT exchange

New Notification Message Types

- Three new Notification Message Types
- REDIRECT_SUPPORTED
- REDIRECT
  - May include the FQDN, IPv4 address or the IPv6 address of the new gateway
- REDIRECTED_FROM

Open Issue – Re-direct during IKE_AUTH exchange

- If re-direct is based on the user's subscription profile, then the re-direct has to happen during the IKE_AUTH exchange
  - The identity is sent in the IDi payload in the IKE_AUTH request message
  - Once the identity is known, the user's subscription profile is looked up
- Supporting this would require sending the REDIRECT message in the IKE_AUTH response
- The client would initiate a fresh IKE_SA_INIT exchange with the new gateway

Open Issue – Gateway initiated re-direct

- Currently the re-direct happens when the client initiates an IKEv2 exchange
- Gateway initiated re-direct allows re-directing the clients to another gateway in the middle of a session
- Requires an Informational Message with the REDIRECT payload from the gateway to the client
- Should this be supported?