Re-direct Mechanism for IKEv2

IPSECME, IETF 73
Vijay Devarapalli (vijay@wichorus.com)
Kilian Weniger (kilian.weniger@eu.panasonic.com)
IKEv2 Re-direct Mechanism

- Allows an IKEv2 responder to re-direct the client to another responder
  - During the IKE_SA_INIT exchange
  - Gateway-initiated re-direct at any time

- Mainly useful for client-gateway IKEv2 exchanges
  - IPsec VPNs
  - Mobile IPv6 – Home Agent re-directing a mobile node
  - Proxy Mobile IPv6 – LMA re-directing a MAG
IKEv2 Re-direct Mechanism

Client

GW1

GW2

IKE_SA_INIT (N (REDIRECT_SUPPORTED))

Decision to re-direct

IKE_SA_INIT (N (REDIRECT, IP/FQDN_GW2))

IKE_SA_INIT (N (REDIRECT_FROM, initial_IP_GW))

IKE_SA_INIT ()
Gateway Initiated Re-direct

- The re-direct message is re-transmitted if no ack is received
- Protected by the IKEv2 SA
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

- IKEv2 SA with the original gateway needs to be deleted