IKEv2
Configuration Payload Extension
for Private-IPv4 support
for FMC Interworking
draft-so-ipsecme-ikev2-cpext-01

tso@zteusa.com       zu.qiang@ericsson.com
Tricci  So          Zu  Qiang

IETF 83rd  Meeting
Problem Statement (FMC Interworking using Private IPv4)
– FAP Location Identification over NA(P)T for FMC Policy Control

How mobile network’s “policy control function” identifies the location of the FAP in order to apply FMC’s policy?
IKE-CP Extension Solution Overview for FMC with Femto

IKEv2 Message 1
HDR, SAi1, KEi, Ni

IKEv2 Message 2
HDR, SAr1, KEr, Nr, [CERTREQ]

IKEv2 Message 3
HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] CP(CFG_REQUEST),
SAi2, TSi, TSr}

IKEv2 Message 4
HDR, SK {IDr, [CERT,] AUTH, CP(CFG_REPLY),
SAr2, TSi, TSr}

NOTE: NATed Encap IPv4 info includes both NATed source IPv4 address and port#

FAP retrieves the NATed (i.e. “Public”) IPv4 from IKEv2’s Configuration Payload

FAP sends NATed IPv4 Info to Mobile Core Network within IPSEC’s Payload (i.e. inband femto signaling)

During FAP initial attachment to Fixed Network to connect to its Mobile Network, FAP includes “new” CFG Payload in already supported IKEv2 msg which includes CFG_REQUEST & CFG_REPLY