Support for RFC 5685 Redirect Mechanism for Internet Key Exchange Protocol V2(IKEv2)

This chapter describes support for RFC 5685 Redirect Mechanism for Internet Key Exchange Protocol V2 (IKEv2).

- Feature Description, on page 1
- ePDG Reselection Configuration, on page 2

Feature Description

Overview

ePDG complies with RFC 5685 partially. 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. The SWu interface between UE and ePDG also uses IKEv2 to establish secured tunnel over untrusted Wifi access. RFC 5685 defines an IKEv2 extension that allows an overloaded ePDG or an ePDG that is being shut down for maintenance to redirect the UE to attach to another ePDG.

ePDG supports the following:

- Additional payloads specified in RFC 5685 in the IKEv2 stack.
- Optimized backhaul utilization by redirecting a UE to another ePDG closer to the last-visited (and possibly topologically closest to UE) PGW for the UICC devices. This redirection is implemented based on RFC5685.
- For non-UICC devices the HSS may not have any entry of last visited PGW and the location of the device is identified based on the IPSec tunnel endpoint address. The AAA server can access a database which maps IP address range to the closest PGW identity and with that the same mechanism is used to redirect the UE to the closest PGW.

Limitations

With this release 20.1 compliance to RFC 5685 is limited to get peak hour traffic redirection from one zone to another zone to achieve better overall capacity management.

Scope & Assumptions

Scope

1. ePDG supports validation and parsing of REDIRECT_SUPPORTED and REDIRECTED_FROM payloads in IKE_INIT messages from UE as per RFC 5685.
2. ePDG supports inclusion of REDIRECT payload with IPv4 or IPv6 address in the final IKE_AUTH message to UE.
3. REDIRECT payload in IKE_INIT Response and Information Request message will not be supported.
4. REDIRECT payload in IKE_AUTH message will not support sending ePDG FQDN.
5. In case the AAA server sends multiple APN configurations in DEA message and more than one has a PGW FQDN present in APN configuration, ePDG will just use the one associated with the selected APN. All other PGW identities will be ignored and will not be used for DNS query and filtering of the alternate ePDG node.

Assumptions

1. UE supports IKEv2 redirection as per RFC 5685.
2. DNS servers can be configured with APN FQDN for APNs serviced by ePDG with the service parameter.
3. HSS will always retain the last visited PGW identity (FQDN) and will send it to ePDG via AAA server on Swm interface.
4. The LTE network will perform PGW selection based on topological proximity and if the UE performs LTE attach the last visited PGW identify in HSS closest to the UE location.
5. The ePDG will be configured to do topology based DNS query for PGW nodes during initial attach. This would ensure that WiFi attach also goes to the topologically closest PGW once an ePDG is selected after re-direction.

ePDG Reselection Configuration

Configuring ePDG Reselection Configuration

Syntax

```
configure
    apn-profile
        gateway-selection alternate-epdg strip-labels strip_labels
max-alternate-pgw max_alternate_pgw_attempts
        remove gateway-selection alternate-epdg strip-labels strip_labels
max-alternate-pgw
    end
```

show crypto ikev2 security-association

The following show output is added to **show crypto ikev2 security-association** command as part of this release.

- Redirection Supported
- Redirection From

show apn-profile full all

The following show output is added to **show apn-profile full all** command as part of this release.

- Alternate ePDG Selection
- Num Stripped Labels

show epdg statistics

The following bulk statistics are added under Alternate ePDG Selection Stats section.

- Redirect-enabled UE
- Selection Required
- Selection Aborted
- Selection Initiated
- Selection Succeeded
- Selection Failed