SecGW Support for EAP-MD5

Feature Description

SecGW uses RADIUS interface between AAA and SecGW for EAP-MD5 authentication of IPSec peer. Radius protocol is used between AAA Server and SecGW. SecGW will act as EAP-pass-through only.

Assumptions and Limitation

- The implementation will be valid only for SecGW RAS mode.

- EAP payload will not be validated only header will be validated.

- The prefix in Idi payload, which decides the EAP-Type to be performed for authentication is out of scope for this feature. As there is no prefix digit assigned to it, it will be decided by mutual agreement between SecGW peer (like FAP) and AAA server.

Configuring SecGW Support for EAP-MD5

Use the following configuration to configure SecGW Support for EAP-MD5.

associate subscriber-map *subscriber-map_name*

```
config
   context context_name
      wsg-service service_name
         associate subscriber-map subscriber_map_name
      end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature SecGW Support for EAP-MD5:

show crypto stats ikev2:

EAP-MD5:

- Current: Failure:

- Attempt: Success:

Existing Show command outputs significant to EAP-MD5 feature:

show wsg-service stats

- Auth failure:

show radius counters all

- Access-Request Sent:

- Access-Challenge Received:

- Access-Accept Received:

- Access-Reject Received: