Encrypt AES-GCM Algorithm

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	IPSec
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *IPSec Reference* • *Command Line Interface Reference*

Revision History

Revision Details	Release
First Introduced	21.28

Feature Description

The P-GW (Packet Data Network Gateway) support IPsec and IKEv2 encryption using IPv4 and IPv6 addressing in LTE/SAE (Long-Term Evolution/System Architecture Evolution) networks.

IPsec and IKEv2 encryption enables network domain security for all IP packet switched networks, providing confidentiality, integrity, authentication, and anti replay protection through secure IPsec tunnels.

In StarOS 21.28.0 and later releases, URL redirection encryption mechanism is enhanced with an aes-gcm-256 encryption option:

The following preferences are supported for the AES-GCM Encryption Algorithm:

- AES Key size (Preferred 256)
- GCM IV length (Preferred 12)
- GCM Tag length (Preferred 16)
- MD (SHA384)

Note The aes-gcm-256 algorithms do not affect the function that supports multiple algorithms with different rulebase that is installed from PCRF at the same time.

Configuring aes-gcm-256 Encryption

The encryption mechanisms list is enhanced by additionally supporting AES-GCM.

```
configure
  active-charging service service_name  charging-action  charging_action_name
    billing action rf
   flow action redirect-url redirect_url encryption  aes-gcm-256  encrypted
 key key
    flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action  lower-ip-precedence

    pco-custom 1 3
    tft packet-filter tft-pmb
  exit
```

NOTES:

- **flow action redirect-url** *redirect_url* **encryption aes-gcm-256 encrypted key** *key* : Performs AES-GCM-256 encryption for redirect URL data.

Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting the AES-GCM Encryption Algorithm feature.

Show Commands and Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show configuration active-charging service all | grep flow

The following example displays the flow action of the redirect URL performed for AES-GCM-256 encryption method.

```
[local]qvpc-si(config)# active-charging service acs
[local]qvpc-si(config-acs)# charging-action sa-redirect-pmb
[local]qvpc-si(config-charging-action)# billing-action rf
[local]qvpc-si(config-charging-action)# flow action redirect-url abc.com encryp
tion
encryption - Enable encryption for dynamic fields of redirect url
[local]qvpc-si(config-charging-action)# flow action redirect-url abc.com encryp
tion
aes-cbc-128 aes-cbc-256 aes-gcm-256 blowfish128 blowfish64
[local]qvpc-si(config-charging-action)# flow action redirect-url abc.com encryp
tion aes-gcm-256 encrypted key 7625e224dc0f0ec91ad28c1ee67b1eb96d1a5459533c5c95
0f44aae1e32f2da3
```