Multiple ePDG Certificates Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	ASR 5500
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *ePDG Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Changes

ePDG now supports multiple device certificates as described below.

- Crypto template supports additional four device certificates, retaining the existing associated certificate, thus maintaining the backward compatibility

- A new CLI command is introduced to configure CA certificate list in order of their issuance. Maximum four CA-Certificate lists are allowed
- The existing configuration to associate ca-certificates is enhanced to associate sixteen ca-certificates from four, so that certificate chaining can be configured for each device certificate
- In the certificate request from peer, there can be multiple CA-Hash present, and ePDG will send the Certificate (and its intermediate CA Cert) with first match. If there is no match, then the certificate configured under existing configuration will be treated as default certificate and it will be sent
- If the certificate sent is selected from new configuration, then CN name will be extracted from it and sent with ID payload in IKE_AUTH response, otherwise the existing implementation of using the configured value of ID under crypto template is used

Use Cases

Peer does not send Certificate Request Payload:

If peer does not send Certificate Request payload in first IKE-AUTH request, then ePDG will not send any certificate, even if they are associated with crypto template. It is existing behaviour.

Peer sends Certificate Request payload:

- Receiving Certificate Request payload itself enables ePDG to send the device certificate. Sending of intermediate CA for certificate chaining will be decided after matching of CA Hash received with Certificate Request payload.
- Below are two scenarios to be taken care after receiving Certificate Request payload:
  - Hash of only one CA (or Intermediate CA) is received :
    - ePDG will match the received CA-Hash, with the CA-Hash of configured CA-Certificates
    - If a matching CA-Certificate is found, then the Certificate signed by it will be sent in Certificate Payload
    - Also, there is possibility that peer has sent CA-Hash of an intermediate CA-Certificate, and then all the intermediate CA-Certificates will be sent, forming a Certificate Chain
    - The first Certificate Payload will contain ePDG Certificate and rest will be Intermediate CA Certificates. The last Intermediate CA Certificate will the one, which is signed by the Intermediate CA-Hash received from peer
    - Maximum of four Certificate Payload will be supported, first one will be ePDG Certificate and rest three will be Intermediate CA certificates.
  - Hash of multiple CA (or Intermediate CA) are received
    - All the steps mentioned in above case is applicable here also, except that the first match for CA-Hash found from the CA-Hash list received will be used to send ePDG Certificate(with Certificate Chain if applicable)

Important If there is no matching CA certificate or Intermediate CA certificate present under crypto template configuration, then the default certificate associated with “certificate <>” cli will be sent with certificate Payload. No intermediate CA certificate(s) will be sent in this scenario.

Assumptions and Limitations

- If there is no CA-Hash match found, then default ePDG certificate configured with CLI “certificate <>” under crypto template will be sent
- Maximum of five ePDG certificates can be configuration under crypto template. One is existing(default) and four more will be allowed with new CLI
- If ePDG Certificate is selected from the new configuration, then the ID payload of IKE_AUTH response will be filled with CN name extracted from the certificate. Using ID from the crypto template when default ePDG Certificate sent will be retained for backward compatibility
- Only four Certificate Payload is sent in case of Certificate Chaining scenario, so care should be taken to configure at maximum of three Intermediate CA Certificates for an ePDG certificate
- While sending CA-Hash in Certificate Request Payload, only first four CA-Certificate will be used, this is can be configured by CLI which is under Crypto Template
- A maximum of 20 CA certificates can be configured at global level. Currently 16 certificates are supported

Command Changes

ca-certificate-list name

The **ca-certificate-list name** CLI command is introduced to configure multiple ePDG certificates.

```
configure
  ca-certificate-list name ca_cert_list_name ca-cert-name ca_cert_name_1
ca-cert-name ca_cert_name_2 ca-cert-name ca_cert_name_3 ca-cert-name ca_cert_name_4

  no ca-certificate-list name
  end
```

server-certificate

The **server-certificate** CLI command is added in the Crypto Template Configuration Mode to configure multiple ePDG certificates.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
    server-certificate server_certificate_name ca-certificate-list
```

```
ca_cert_list_name [ validate ]
     no server certificate server_certificate_name [ validate ]
     end
```

clear ca-certificate-list statistics

The **clear ca-certificate-list statistics** command has been added to clear certificate list statistics.

clear ca-certificate-list statistics

Performance Indicator Changes

ePDG Schema

Below new statistics are introduced to support Multiple ePDG Certificates in ePDG Schema:

Counter	Description	Trigger
ikev2-ca-cert-chains-sent	Total IKEv2 certification statistics (CA certificate chains sent)	Increments when CA certificate chain is sent in IKE payload
ikev2-server-certs-sent	Total IKEv2 certification statistics (server certificates sent excluding CA certificates)	Increments when non CA certificate is sent in IKE payload

show ca-certificate-list statistics

The following new fields are added to the output of this command to display the Certificate-list Statistics:

CA-Certificate-Lists:

- ca_cert_list_name
- ca_cert_name_1
- ca_cert_name_2
- ca_cert_name_3
- ca_cert_name_4

show crypto statistics

The following new fields are added to the output of this command to display the Crypto Statistics

- Server Certificates Sent
- CA Certificate Chains Sent