Authorization based on Certificate fields

This feature enables to authorize peer while IKEv2 tunnel establishment in case of SecGW product while using Certificate based authentication method.

Feature Description

Authorization of peer will be based on match of CN field in peer's certificate with list of configured allowed entries.

Assumptions and Limitations

- CN part will be such a way that it matches fully with one of the configured value.
- All peers are provided with the same Certificate or some set of known certificates. Hence CN will be same (or set of CN's) and will be limited in exclusive numbers. One such configuration can match all peers using said certificate.
- This feature is not applicable for non-certificate authentication method.
- Only 64 entries can be configured under one cert-policy and one cert-policy can be attached to one crypto template used for SecGW service.

Configuring Authorization based on Certificate fields

Use the following configuration to configure Authorization based on Certificate fields.

certificate policy

```
config
   context context_name
        [ no ]  certificate policy   ert-policy_name
          end
```

id

```
config
   context context_name
        [ no ]  id  id
         id  id_value  match-criteria { common-name value comm-name_val  |
domain-name value dom_name_value }
          end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature to support Authorization based on Certificate fields:

show crypto ikev2-ikesa certificate policy

Crypto Cert Policy Name cert_test

- ID 1 Match-Type common-name Match-Value wsg0@cisco.com
- ID 2 Match-Type common-name Match-Value wsg1@cisco.com
- ID 3 Match-Type common-name Match-Value wsg2@cisco.com

Crypto Cert Policy Name cert_test1

- ID 2 Match-Type common-name Match-Value wsg1@cisco.com

Crypto Cert Policy Name test

- ID 1 Match-Type common-name Match-Value wsg_test@cisco.com

show config

ikev2-ikesa certificate policy cert_test1

- id 2 match-criteria common-name value wsg1@cisco.com

ikev2-ikesa certificate policy cert_test

- id 1 match-criteria common-name value wsg0@cisco.com
- id 2 match-criteria common-name value wsg1@cisco.com
- id 2 match-criteria common-name value wsg1@cisco.com

crypto template template-name ikev2-dynamic

- ikev2-ikesa cert-policy cert_test

Bulkstats

Below fields are added for Certificate Authentication Statistics:

- Authorisation policy failure