Google Cloud

Edge Security

SAML

Security assertion markup language (SAML)

- SAML enables applications to exchange authentication and authorization information in XML format
- SAML terminology
  - Service Provider
    - Validates SAML tokens on API calls
  - Identity Provider
    - Generates SAML tokens used on API calls
- Edge supports both SP and IP roles

Generate SAML assertion policy

Outbound token generation

```
<GenerateSAMLAssertion name="SAML" ignoreContentType="false">
  <CanonicalizationAlgorithm />
  <Issuer ref="reference">Issuer name</Issuer>
  <KeyStore>
    <Name ref="reference">keystorename</Name>
    <Alias ref="reference">alias</Alias>
  </KeyStore>
  <OutputVariable>
    <FlowVariable>assertion.content</FlowVariable>
    <Message name="request">
      <Namespaces>
        <Namespace prefix="test">http://www.example.com/test</
Namespace>
      </Namespaces>
      <XPath>/envelope/header</XPath>
    </Message>
  </OutputVariable>
  <SignatureAlgorithm />
  <Subject ref="reference">Subject name</Subject>
  <Template ignoreUnresolvedVariables="false">
    <!-- A lot of XML goes here, in CDATA, with {} around
         each variable -->
  </Template>
</GenerateSAMLAssertion>
```

Validate SAML assertion policy

Inbound authentication and authorization

```
<ValidateSAMLAssertion name="SAML" ignoreContentType="false">
  <Source name="request">
    <Namespaces>
      <Namespace prefix='soap'>http://schemas.xmlsoap.org/soap/envelope/</Namespace>
      <Namespace prefix='wsse'>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd</Namespace>
      <Namespace prefix='saml'>urn:oasis:names:tc:SAML:2.0:assertion</Namespace>
    </Namespaces>
    <XPath>/soap:Envelope/soap:Header/wsse:Security/saml:Assertion</XPath>
  </Source>
  <TrustStore>TrustStoreName</TrustStore>
  <RemoveAssertion>false</RemoveAssertion>
</ValidateSAMLAssertion>
```

SAML for management server

- Edge Management Server for UI & API supports the following types of authentication
  - Basic Auth and Basic Auth with two-factor authentication
  - OAuth2
- Edge also supports SAML 2.0 as the authentication mechanism.
- You can generate OAuth2 tokens from SAML assertions returned by an identity provider.
- SAML supports a single sign-on (SSO) environment.
- SAML is supported as the authentication mechanism only for the Cloud version of Edge. It is not supported for Edge for the Private Cloud.

THANK YOU