5. Connect to and consume Azure services and third-party services

└ **5.1 Implement API Management**

└ **5.1.3 Configure access to APIs**

1. What authentication mechanisms are supported by Azure API Management (APIM)?
2. How do you secure APIs using subscription keys?
3. How do you configure OAuth 2.0 authentication with APIM?
4. How to configure a client application to call an APIM-secured API using a bearer token?
5. How do you restrict API access using IP filtering in APIM?
6. What is the role of policies in controlling access to APIs?
7. How can you enforce rate limits and quotas per subscription in APIM?
8. How do you enable CORS in API Management?
9. What is the difference between product-level and API-level access control?
10. How do you use managed identities to call APIs behind APIM securely?

---

1. What authentication mechanisms are supported by Azure API Management (APIM)?

- Subscription key
- OAuth 2.0 / OpenID Connect
- JWT validation
- Client certificates
- Managed identities

---

2. How do you secure APIs using subscription keys?

- Add APIs to a product.
- Require subscription on the product.
- Each caller must pass `Ocp-Apim-Subscription-Key` in header or query.

---

3. How do you configure OAuth 2.0 authentication with APIM?

- Register APIM as a client app in Microsoft Entra ID (or other provider).
- Configure OAuth 2.0 settings in APIM (under security tab).
- Set `validate-jwt` policy in inbound section of the API to enforce token validation.

---

4. What are the steps to configure a client application to call an APIM-secured API using a bearer token?

1. Register the client app in Entra ID.
2. Acquire token using MSAL or ADAL libraries.
3. Call the API with `Authorization: Bearer <token>` header.
4. Ensure APIM has a `validate-jwt` policy matching token settings.

---

5. How do you restrict API access using IP filtering in APIM?

- Use the `check-header` or `check-ip` policy in the inbound policy section.
- Example:

```
<check-header name="X-Forwarded-For" failed-check-httpcode="403" failed-check-error-message="Access denied">
  <value>203.0.113.1</value>
</check-header>
```

6. What is the role of policies in controlling access to APIs?

- Policies define request/response behavior at runtime.
- Used to enforce security (e.g., validate-jwt, check-header), rate limits, IP restrictions, CORS, etc.
- Applied at inbound, backend, outbound, or on error sections.

---

7. How can you enforce rate limits and quotas per subscription in APIM?

- Use built-in rate-limit and quota policies.
- Define policies in product or API scope.
- Example:

```
<rate-limit calls="10" renewal-period="60" />
<quota calls="1000" renewal-period="604800" />
```

---

8. How do you enable CORS in API Management?

- Add the cors policy in the inbound section.
- Example:

```
<cors allow-credentials="true">
  <allowed-origins><origin>*</origin></allowed-origins>
  <allowed-methods><method>GET</method></allowed-methods>
</cors>
```

---

9. What is the difference between product-level and API-level access control?

- Product-level: Controls who can access any API within the product using subscriptions.
- API-level: Policies or restrictions applied to individual APIs regardless of product membership.

---

10. How do you use managed identities to call APIs behind APIM securely?

- Enable system-assigned or user-assigned identity on APIM.
- Grant API backend (e.g., Azure Function) the necessary role (e.g., Function App Contributor).
- Use authentication-managed-identity policy in outbound call:

```
<authentication-managed-identity resource="https://<resource>" />
```