APIM (Application programming interface management) services:

* We should allow the users to communicate with system and to take the response back so for that we are maintaining API management services.
* Creating subnet and providing the network security group to subnet.
* In network security group we must apply our own inbound customised rule.
* We must create public IP and we have assigned the virtual network while creating the APIM.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Services deploying is done through azure Kubernetes services.

* Each service has an external IP.
* Developers will give the service endpoint and we must add in the API services.
* Whenever we test the services, we must get the “200” error code i.e., our services are up and running.
* In APIM we must register a new API called login we need to specify the name, display name, web URL (uniform resource locator) https:// external IP: port number.
* We need to provide operation names

GET, PUT, DEL, POST: service endpoint.

* We must provide headers in test tab and test data will be given by application team.

ERROR codes:

200-399 (API is working fine/service endpoint)

400-499(problem from APIM

401-JWT token issue

403-forbidden

404-data not found)

500-501(internal server issue)

502-503(Application gateway timeout)

APPLICATION GATEWAY:

* With the help of application gateway, we can protect our APIM service endpoint, and it works as a web application fire wall system.