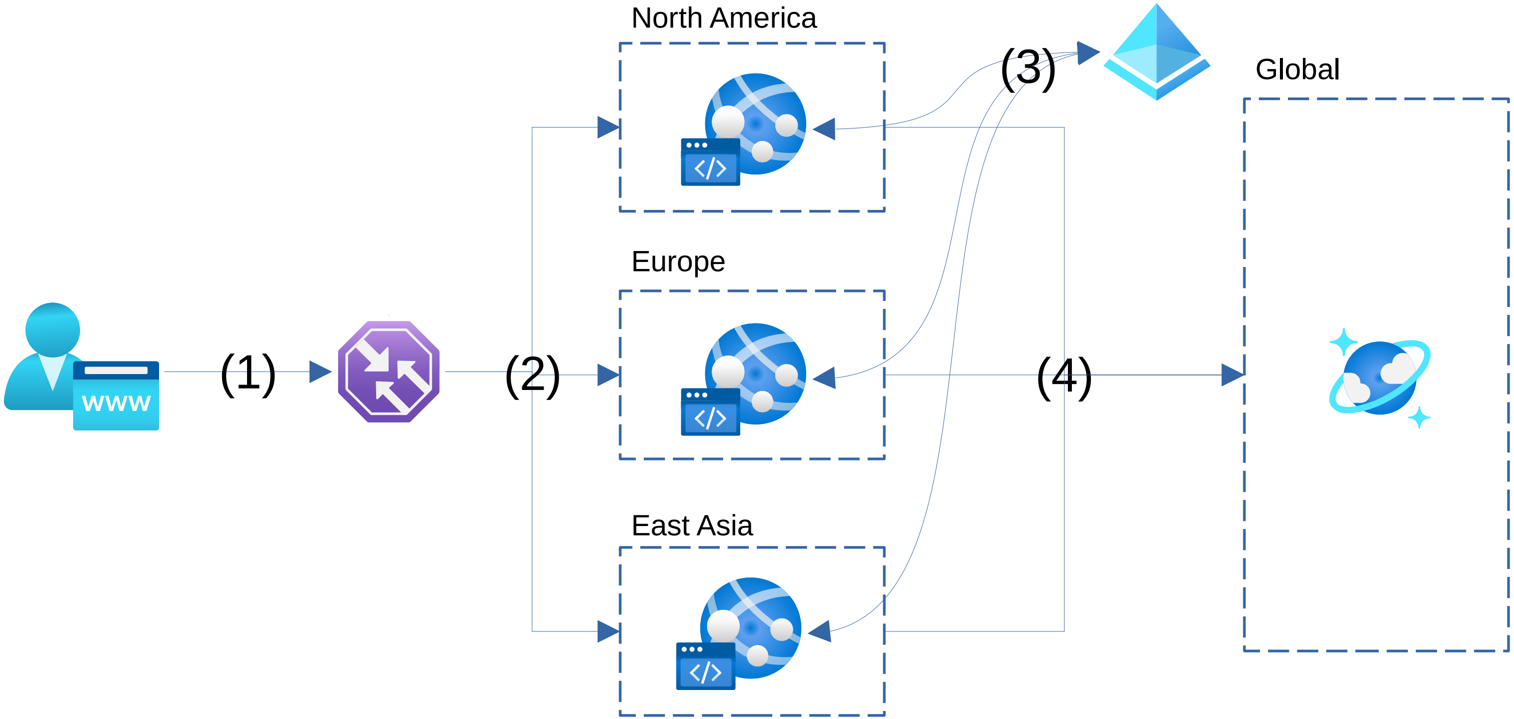
Architecture



FANGOUS DAMIEN – Stellium Exam | Solution Architecture

Scenario

The user connects to the app (1), he is redirected to the instance with the lowest latency through the Azure Traffic Manager (2).

The front-end allows him to connect with his credentials on the AAD authentication page which returns users information and set headers (3) for subsequent calls.

The back-end calls Cosmos DB with managed identity (4) to store or retrieve data.

Azure Traffic Manager

Role

- Receives users requests and redirect to app instance based on lowest latency

Configuration

- Direct to endpoint based on latency response (how-to here)
- Every region has to be added as endpoint in the service

App Service (1/2)

Role

- Host the application
- Back-end serves the front end as SPA

Configuration

- Enable built in authentication (how-to here)
- Authorization is managed inside the application based on the authenticated user
- The app is deployed on multiple region based on client's agencies locations

App Service (2/2)

Configuration

- Allows unauthenticated requests to
  - Allow users to sign in directly into the application
  - Allow apps to call the back-end with AAD delivered token using managed identities
- Disable all built-in authentication except AAD (how-to here)

Cosmos DB

Role

- Store the application data across regions

Configuration

- Enable multi-region write (how-to here)

Considerations

Applications (including the front-end) are authenticated with the back-end with a AAD delivered token. This approach is overkill regarding the front-end since it’s served by the back-end but is more coherent when we consider that the back-end can be called by other applications.