In an Azure App Service, API requests typically flow from a client application to an API Gateway (if used), then to the App Service web app hosting the API, and back to the client with a response. If authentication and authorization are required, they may be handled by the API Gateway or App Service itself before the request reaches the backend application.

Here's a more detailed breakdown:

1. **1. Client Request:**

A client application (web app, mobile app, etc.) initiates an API request by sending an HTTP request to the endpoint URL of the App Service.

1. **2. API Gateway (Optional):**

If an Azure API Management service is configured, the request first goes to the API Gateway. The API Gateway can perform actions like authentication, authorization, request transformation, and rate limiting before forwarding the request to the App Service.

1. **3. App Service:**

The request is then routed to the specific web app within the App Service that hosts the API.

1. **4. Backend Processing:**

The web app's code processes the request, interacts with databases or other services, and generates a response.

1. **5. Response:**

The response is sent back through the API Gateway (if used) and then to the client application.

1. **6. Authentication/Authorization:**

If the API is protected, the client application may need to provide credentials (like an API key or OAuth token) in the request. The API Gateway or App Service verifies these credentials to determine if the client is authorized to access the API.

1. **7. Rate Limiting:**

Azure API Management can also be used to enforce rate limits on API requests, preventing abuse and ensuring fair usage.