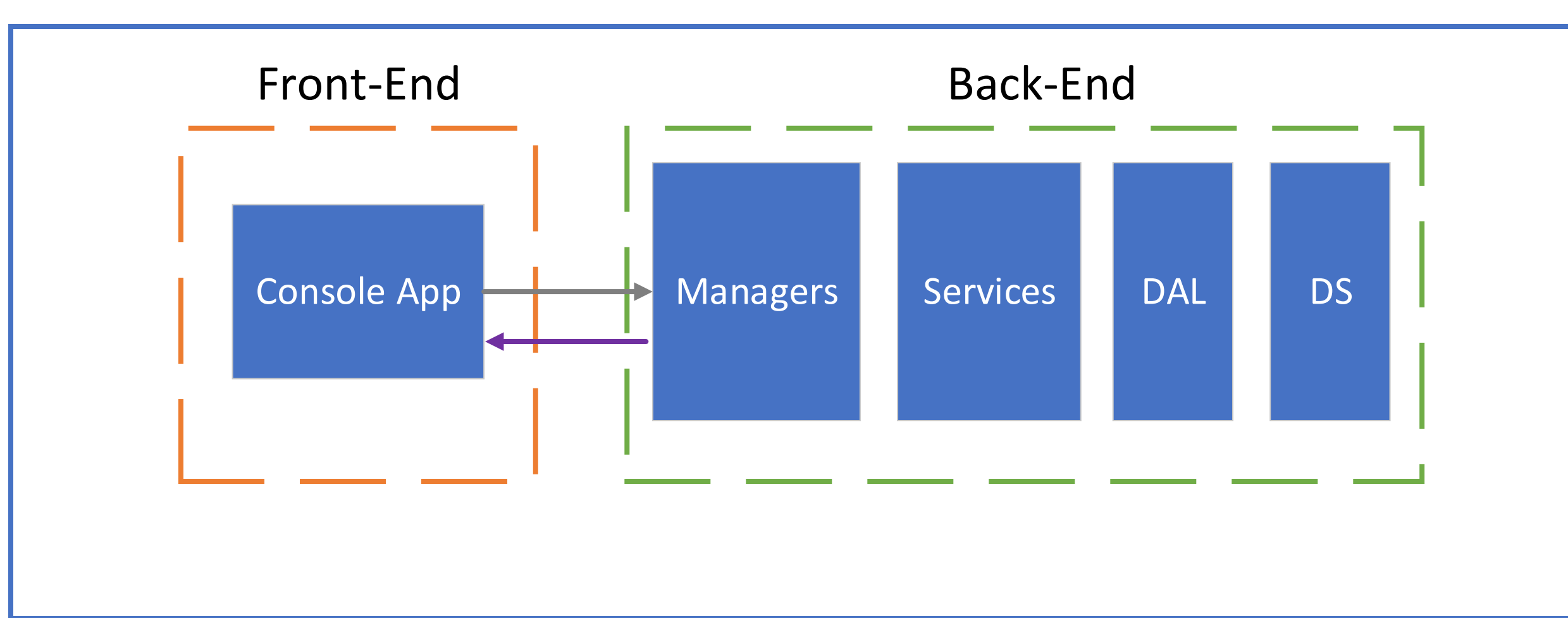
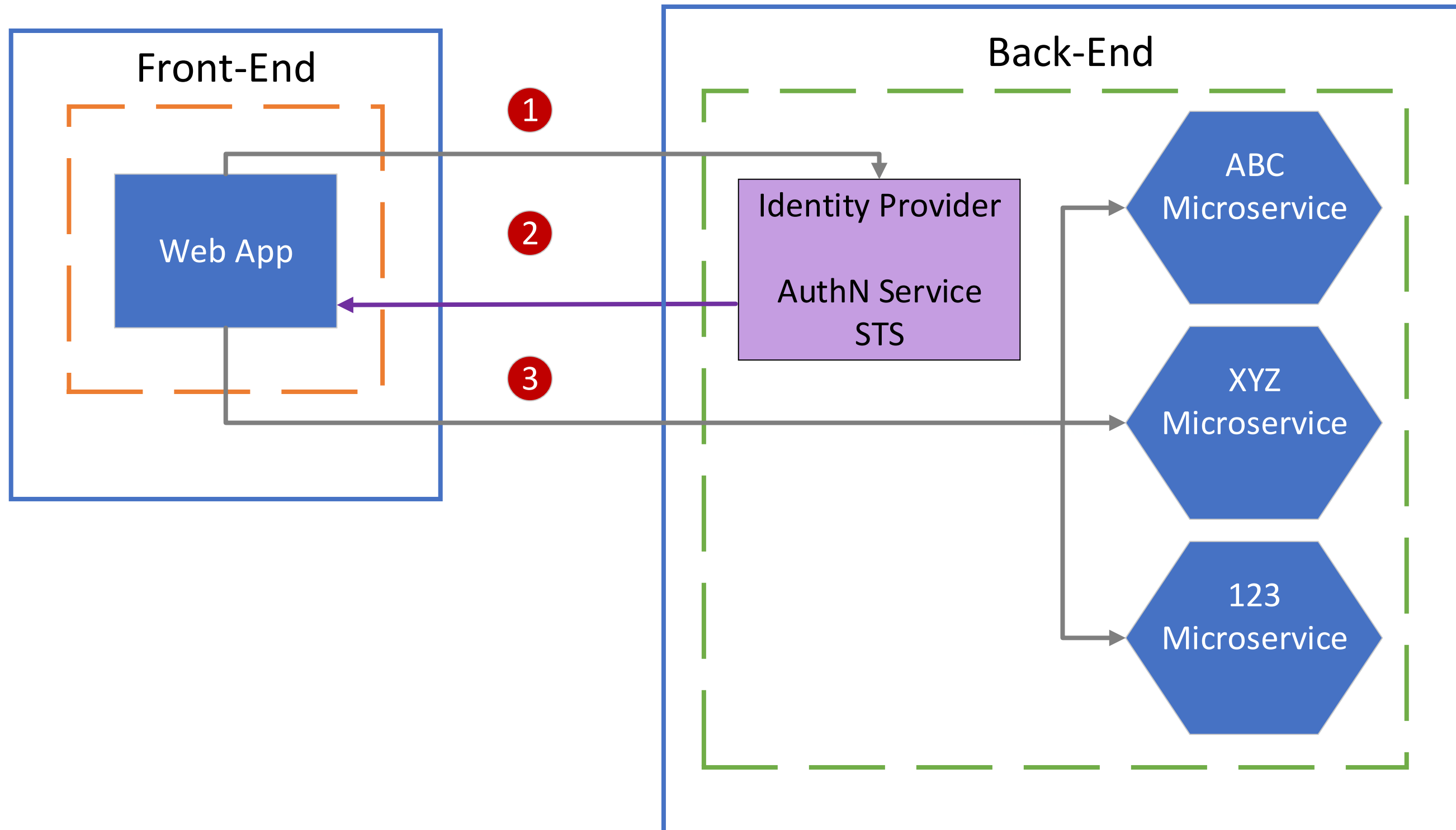
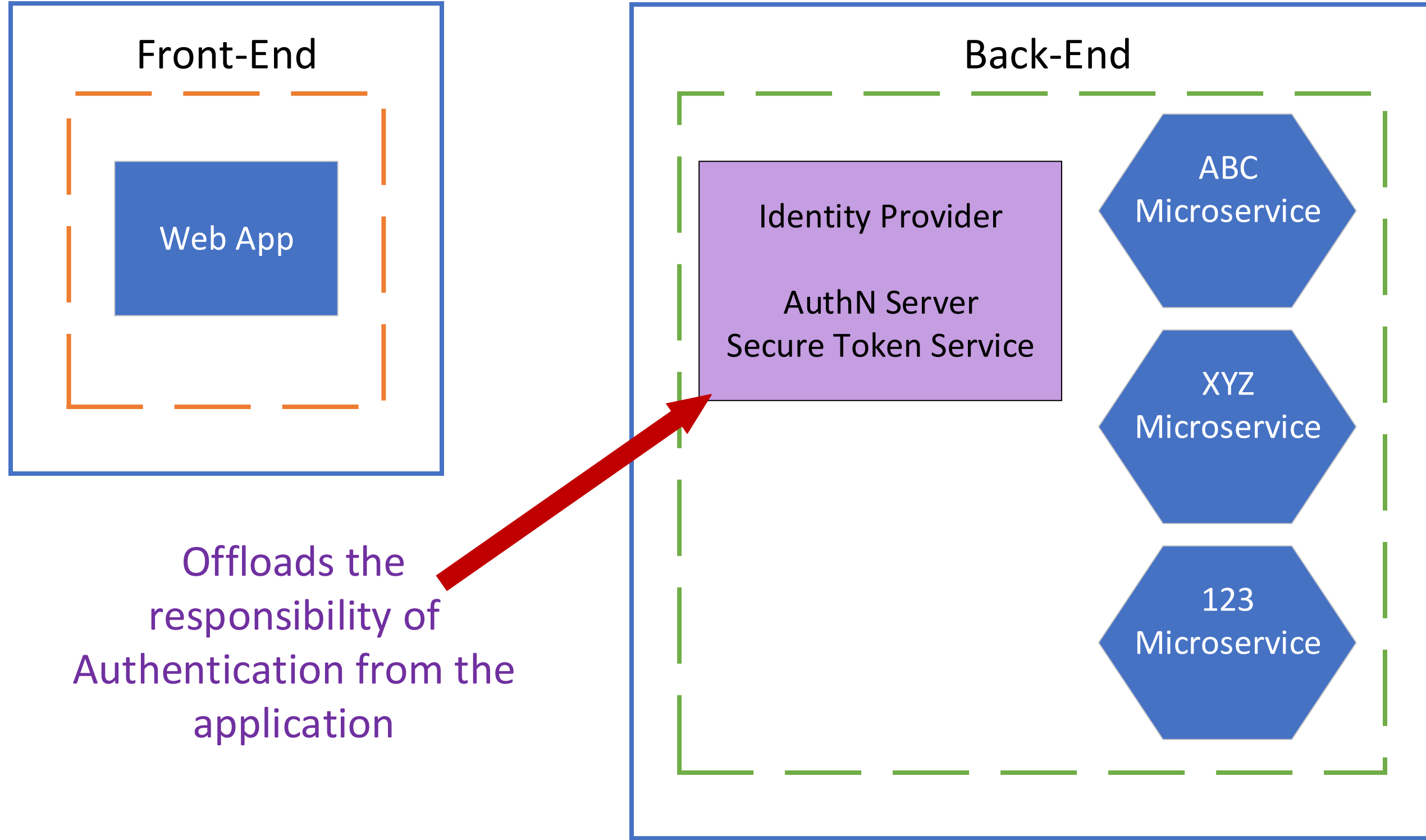
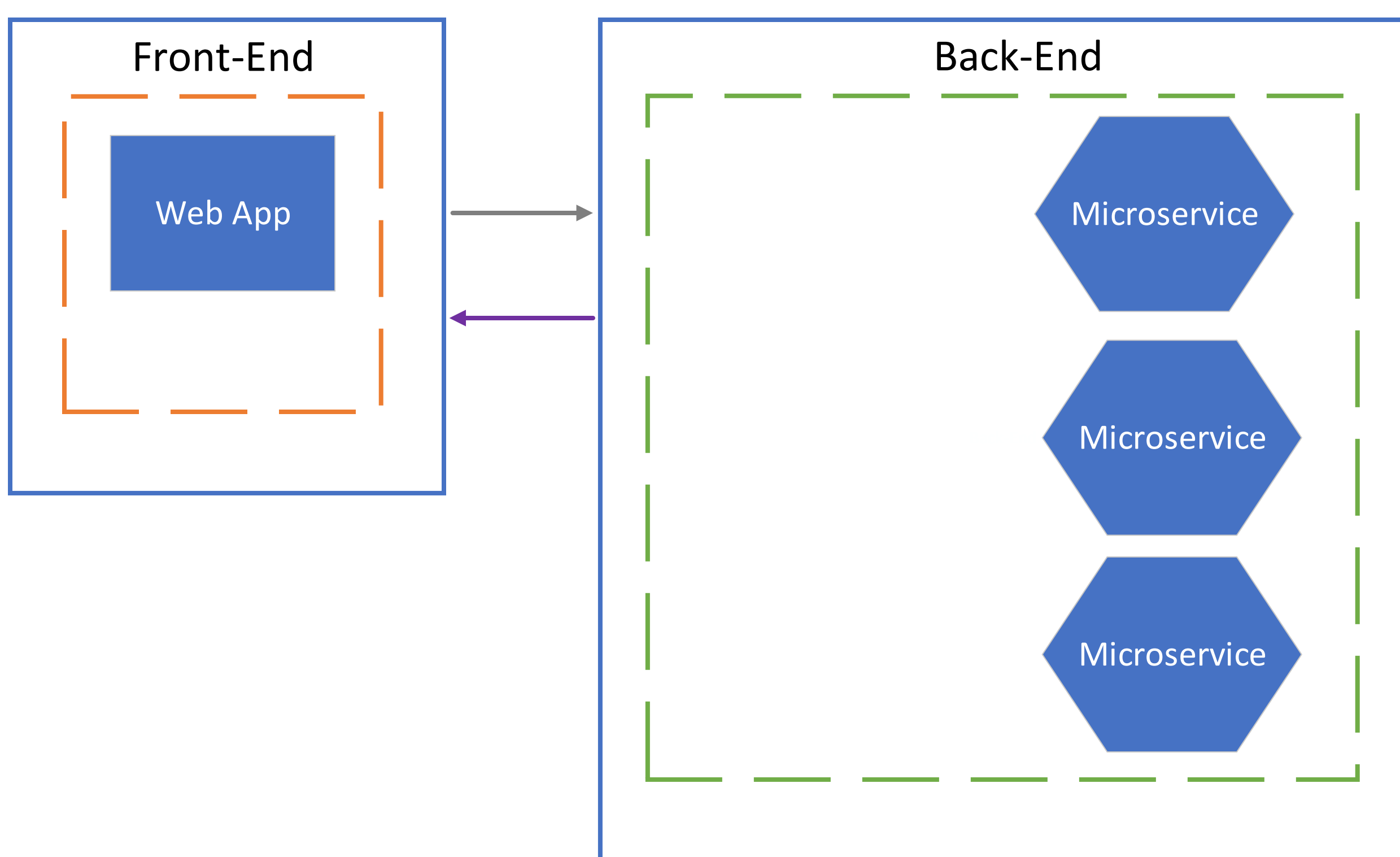


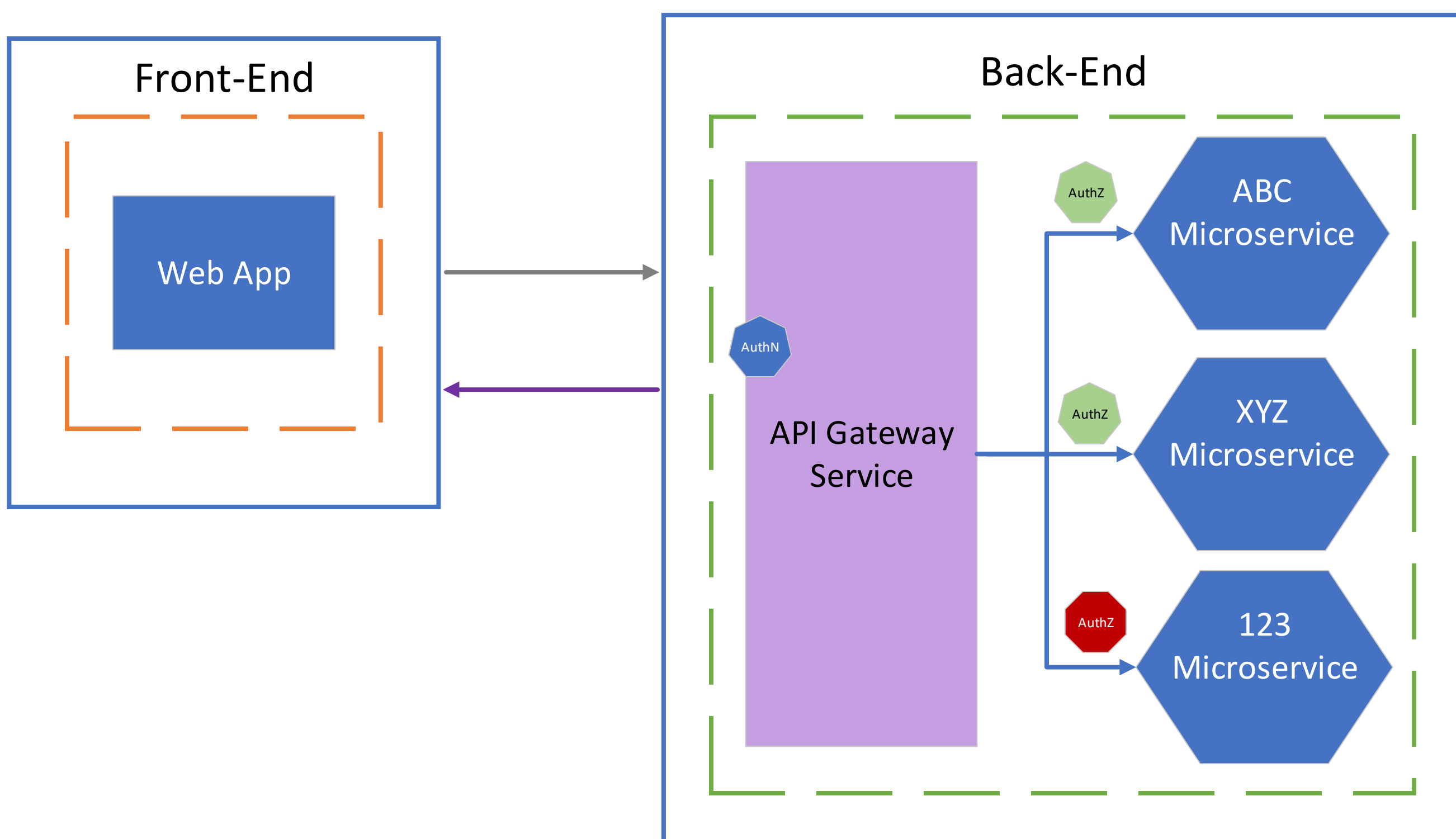
Centralized System



Distributed System



Cloud Provider



Security Tokens

- ID Token
- Access Token
- Refresh Token
- Revoke Token

JSON Web Tokens (JWT)



Check <https://jwt.io> to verify signature

ID Token (JWT)

- Proof of Authentication
- Required Claims
 - * iss (issuer)
 - * sub (subject)
 - * aud (audience[s])
 - * exp (expiration)
 - * iat (issued at)
- Recommended Claims
 - * auth_time
 - * nonce
- Optional Claims
 - * azp (authorized party)
 - * at_hash (access token hash)

Validation Steps

1. Validate JWT Signature
2. Validate aud claim
3. Validate Nonce

ID Token Sample:

```
iss: "https://idp.myapp.com"
sub: "f5f45-54f54f-f54ff"
aud: "as5d46f6a5sd4"
auth_time: 1675282445
exp: 1675286044
iat: 1675282445
```

email: "john.doe@example.com"

Access Token (JWT)

- Use for Authorization
- Required Claims
 - * iss (issuer)
 - * sub (subject)
 - * aud (audience[s])
 - * exp (expiration)
 - * iat (issued at)
 - * azp (authorized party)
 - * scope

Validation Steps

1. Validate JWT Signature
2. Validate token aud claim
3. Validate scope claim

Access Token Sample:

```
iss: "https://idp.myapp.com"
sub: "f5f45-54f54f-f54ff"
aud: "as5d46f6a5sd4"
auth_time: 1675282445
exp: 1675286044
iat: 1675282446
```

client_id: 65f0oq5io2l32a7nanjpj0lsl
username: john.doe@example.com

scope: "read:all write:profile"

scope: "admin"

Standard Claims
https://openid.net/specs/openid-connect-core-1_0.html#StandardClaims