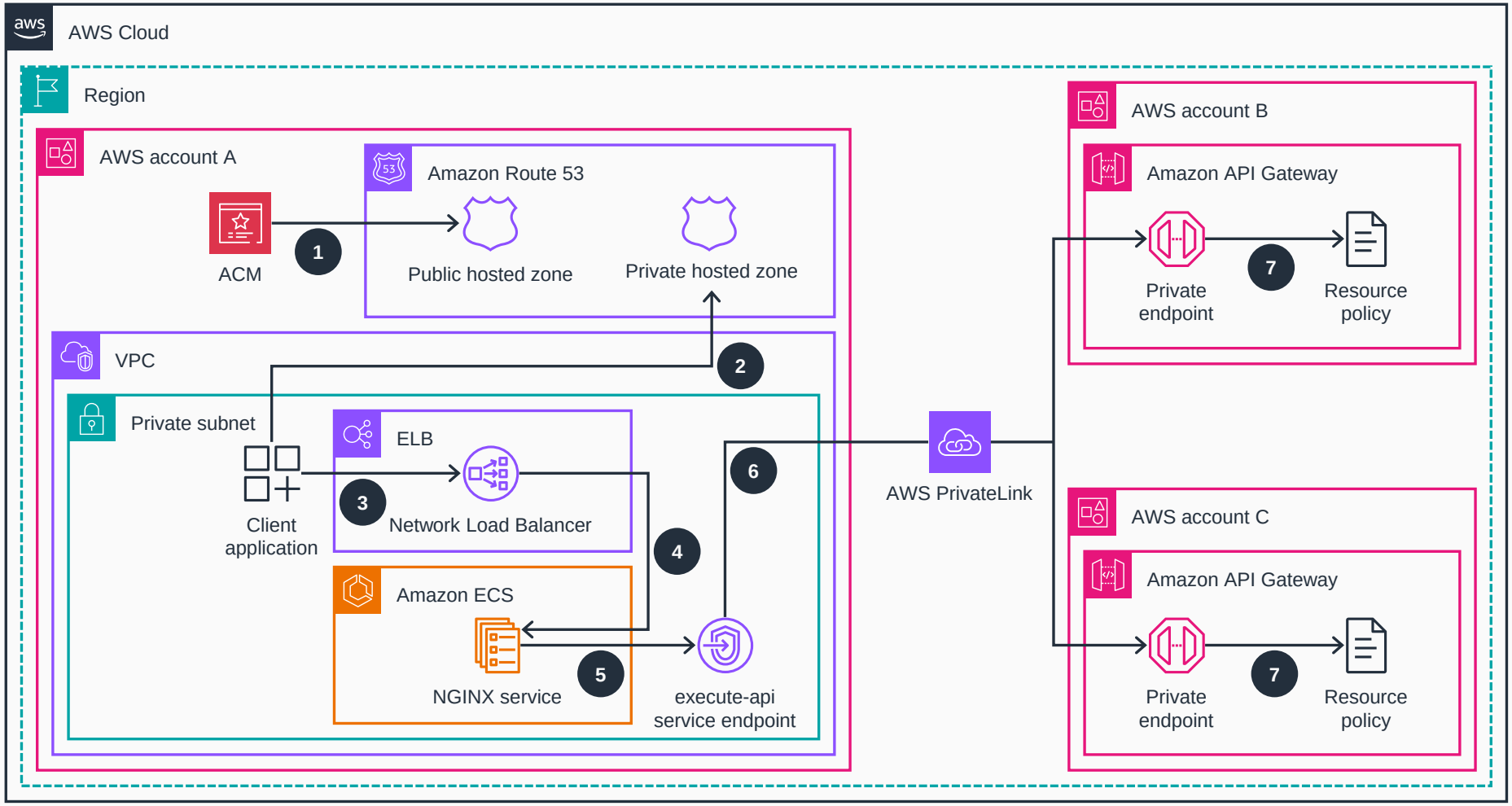
Guidance for Custom Domain Names on Amazon API Gateway Private Endpoints

This architecture diagram shows how to use Elastic Load Balancing (ELB), AWS PrivateLink, and a reverse proxy running on AWS Fargate to facilitate access to private APIs using custom domain names on AWS.



1. **AWS Certificate Manager (ACM)** issues a wildcard certificate for the custom domain (*.example.com) using DNS validation against the **Amazon Route 53** public hosted zone for the “example.com” domain.
2. The client application queries the **Route 53** private hosted zone associated with your environment in **Amazon Virtual Private Cloud (Amazon VPC)** and receives a Canonical Name Record referencing the Network Load Balancer in **Elastic Load Balancing (ELB)**.
3. The client application sends a RESTful API call to the Network Load Balancer.
4. The Network Load Balancer forwards the request to the NGINX service running on **AWS Fargate** in **Amazon Elastic Container Service (Amazon ECS)**.
5. The NGINX service maps the Host header in the RESTful API call to the appropriate **Amazon API Gateway** private endpoint and forwards the request to the execute-api service endpoint in the same **Amazon VPC**.
6. The request is forwarded to the appropriate **API Gateway** private endpoint using **AWS PrivateLink**.
7. **API Gateway** validates the RESTful call source’s VPC endpoint, path, stage, and method against the resource policy and implements the request if allowed.

Reviewed for technical accuracy June 5, 2024

AWS Reference Architecture