VPC Endpoints

Brock Tubre

TECHNICAL INSTRUCTOR

Two Types of VPC Endpoints

Interface Endpoints

- Powered by AWS PrivateLink.
- An elastic network interface with a private IP address.
- Serves as an entry point for traffic.
- Many services are supported.

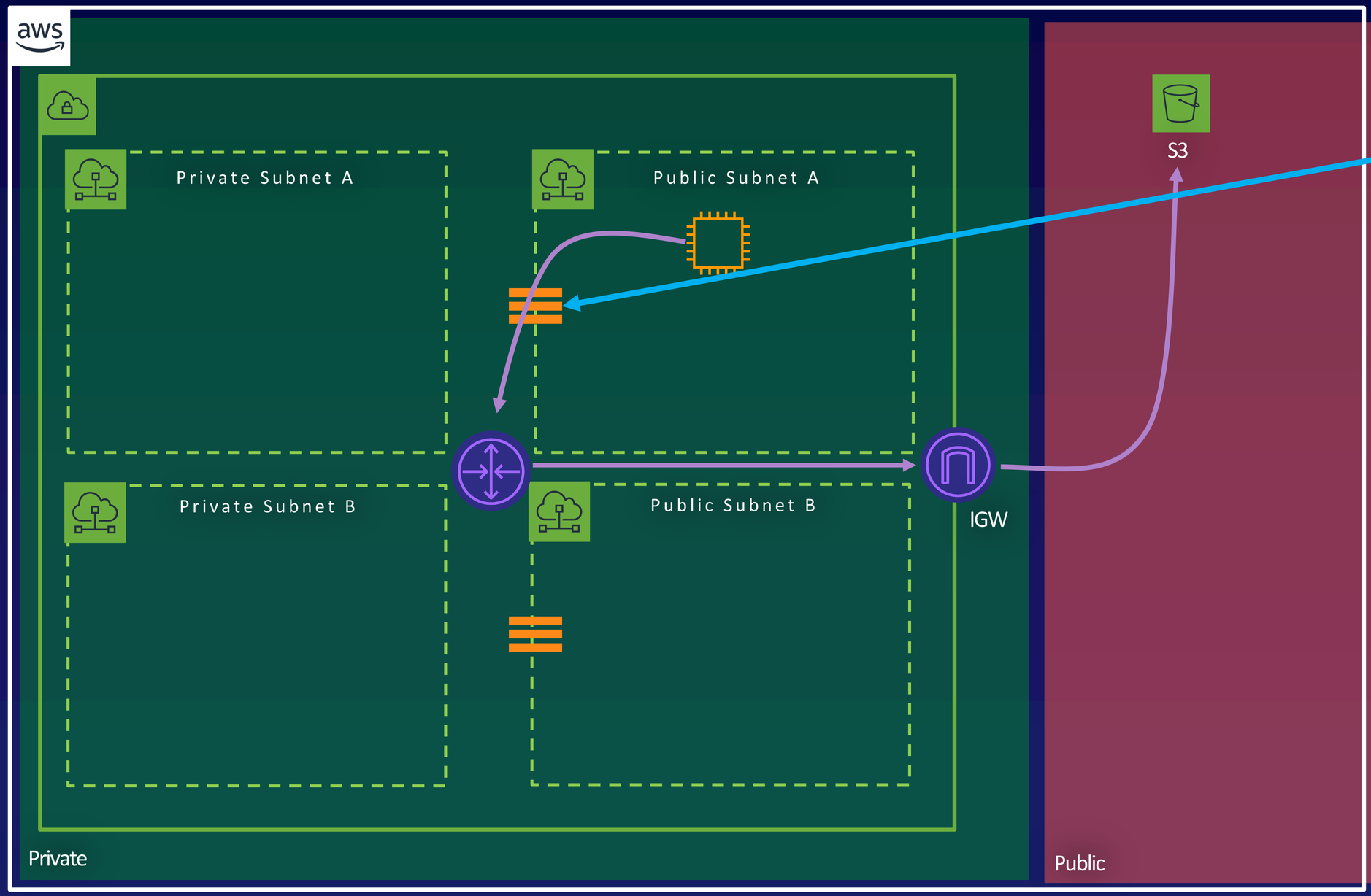
Gateway Endpoints

- Gateway that we can specify as a target in our route table.
- S3 and DynamoDB are supported.

VPC ENDPOINTS

Classic Access to S3

A CLOUD GURU

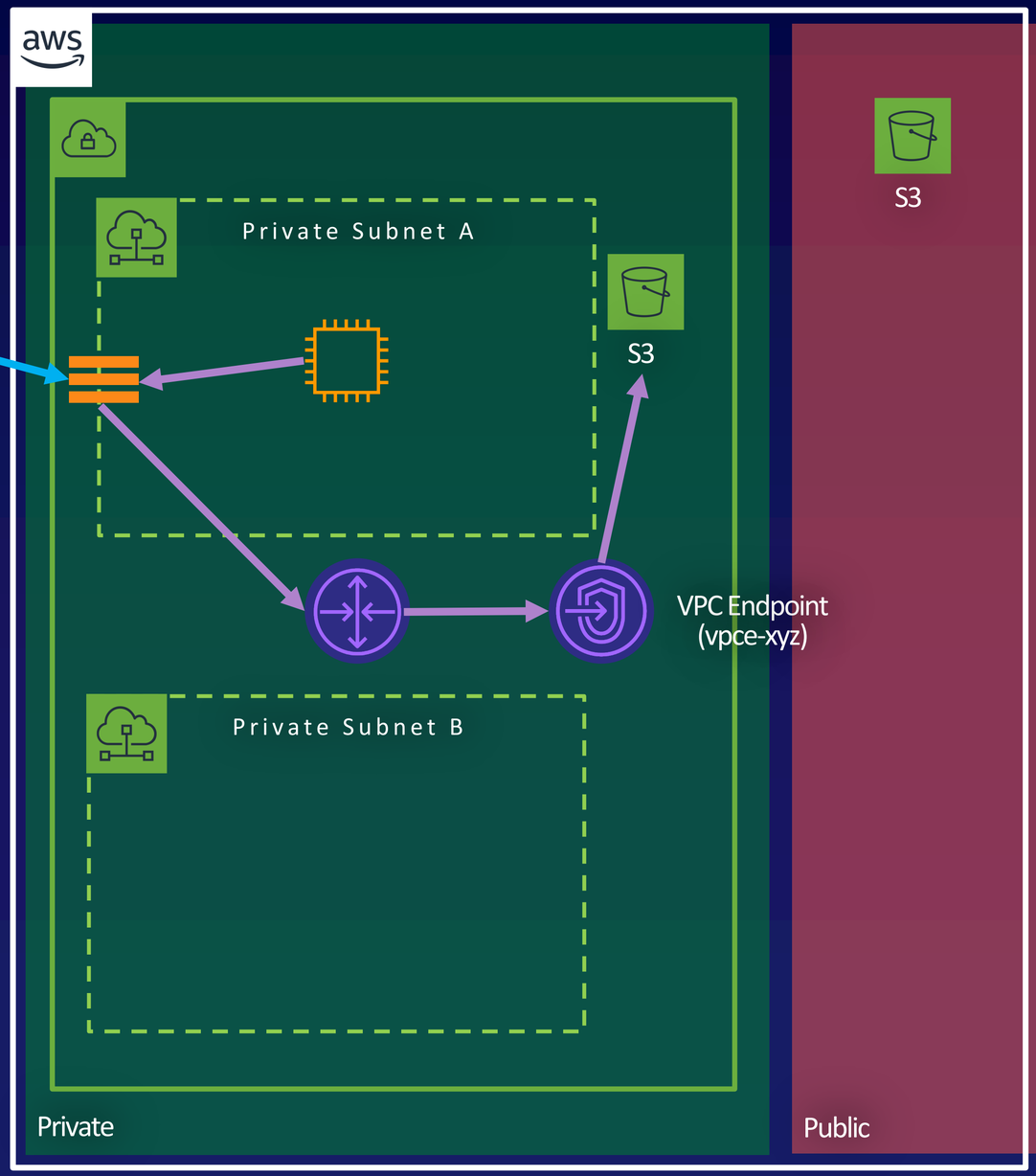


Destination	Target
VPC CIDR	local
0.0.0.0/0	IGW

Simple VPC Endpoint

Destination	Target
VPC CIDR	local
pl-id s3	vpce-xyz

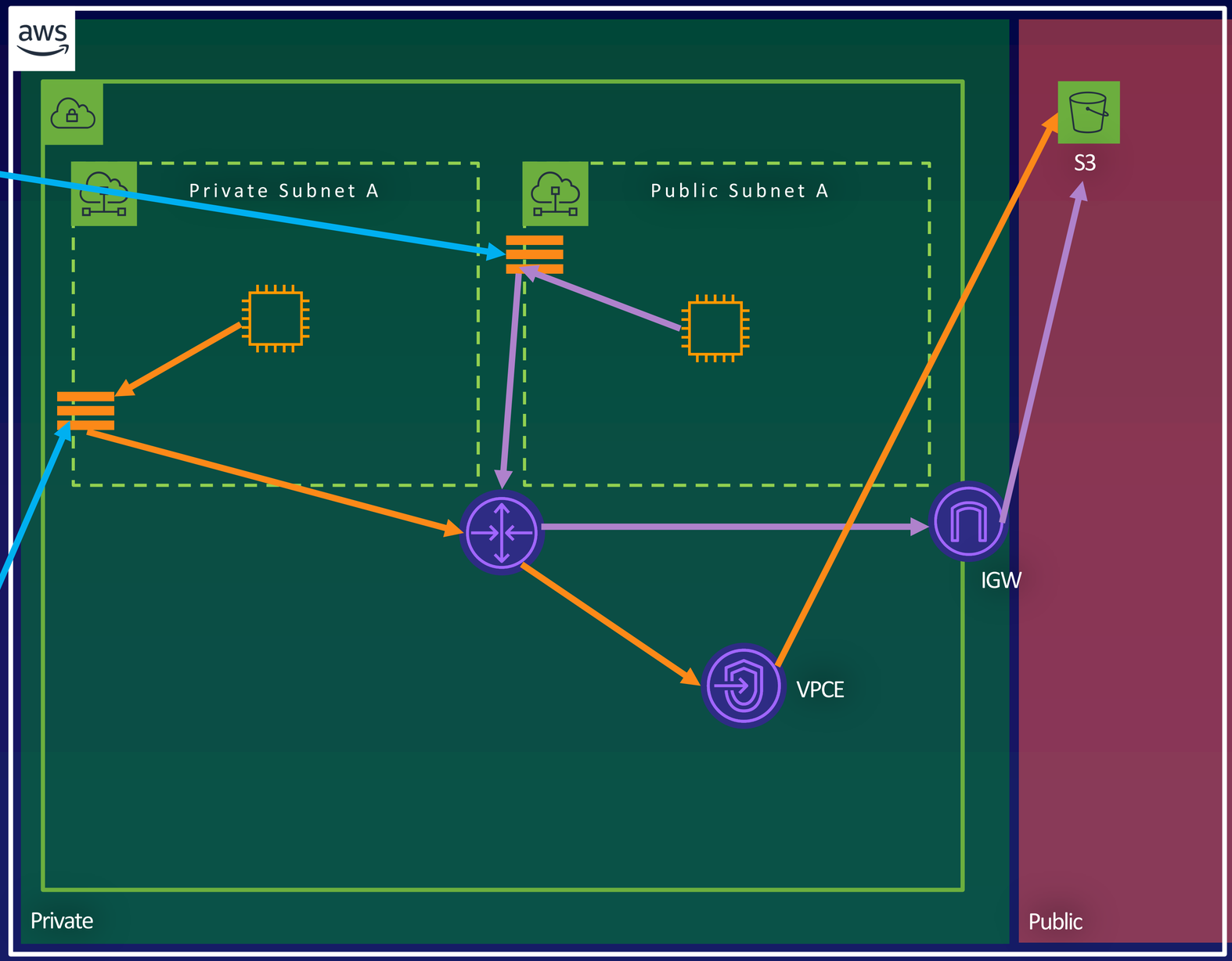
com.amazonaws.region.service



Classic Access and VPC Endpoints

A CLOUD GURU

Destination	Target
VPC CIDR	local
0.0.0.0/0	IGW



Destination	Target
VPC CIDR	local
pl-id s3	VPCE

VPC Endpoints Key Points

1

Endpoints Are A Regional Service

Endpoints are region-scoped services. You cannot create a VPC endpoint for a VPC in a different region than where the service (S3) is located.

2

VPC Boundaries

Endpoints are not extendable across VPC boundaries. They cannot be accessed from outside a VPC or from another VPC.

3

DNS Resolution Is Required

DNS resolution is needed within a VPC. The internal VPC DNS redirects requests to the VPC endpoint, thus requiring DNS resolution with the VPC.

VPC Endpoints Key Points

4

Default VPC Endpoint Policy

By default the VPC endpoint policy is unrestricted but can be further locked down. VPC endpoint policies do not overwrite resource-specific policies (e.g. S3 bucket policy).

5

Controlling Access

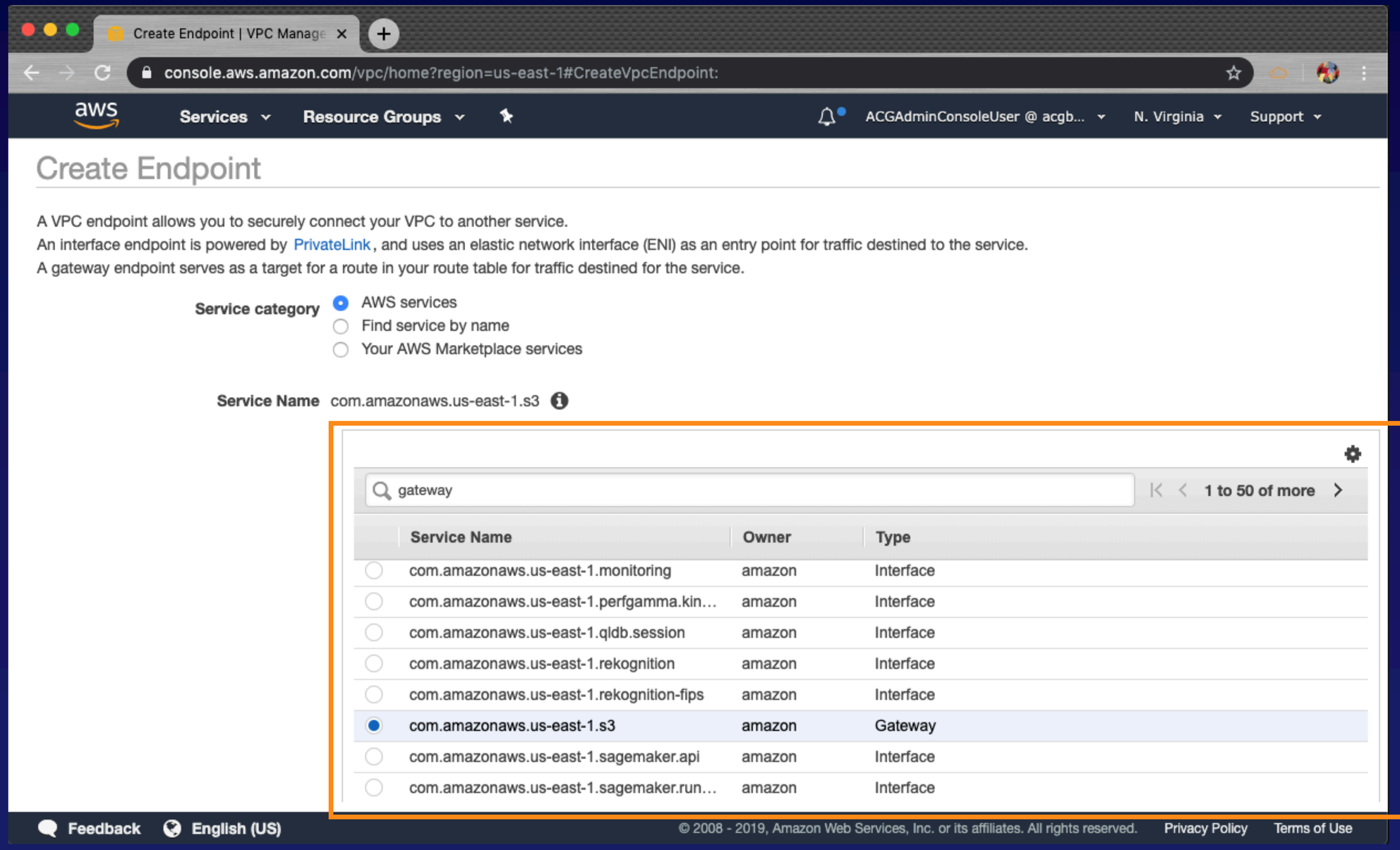
Controlling access to VPC endpoints via NACLs can be problematic. Instead, using SGs is preferred because you can reference logical networking objects (e.g. the VPC endpoint).

6

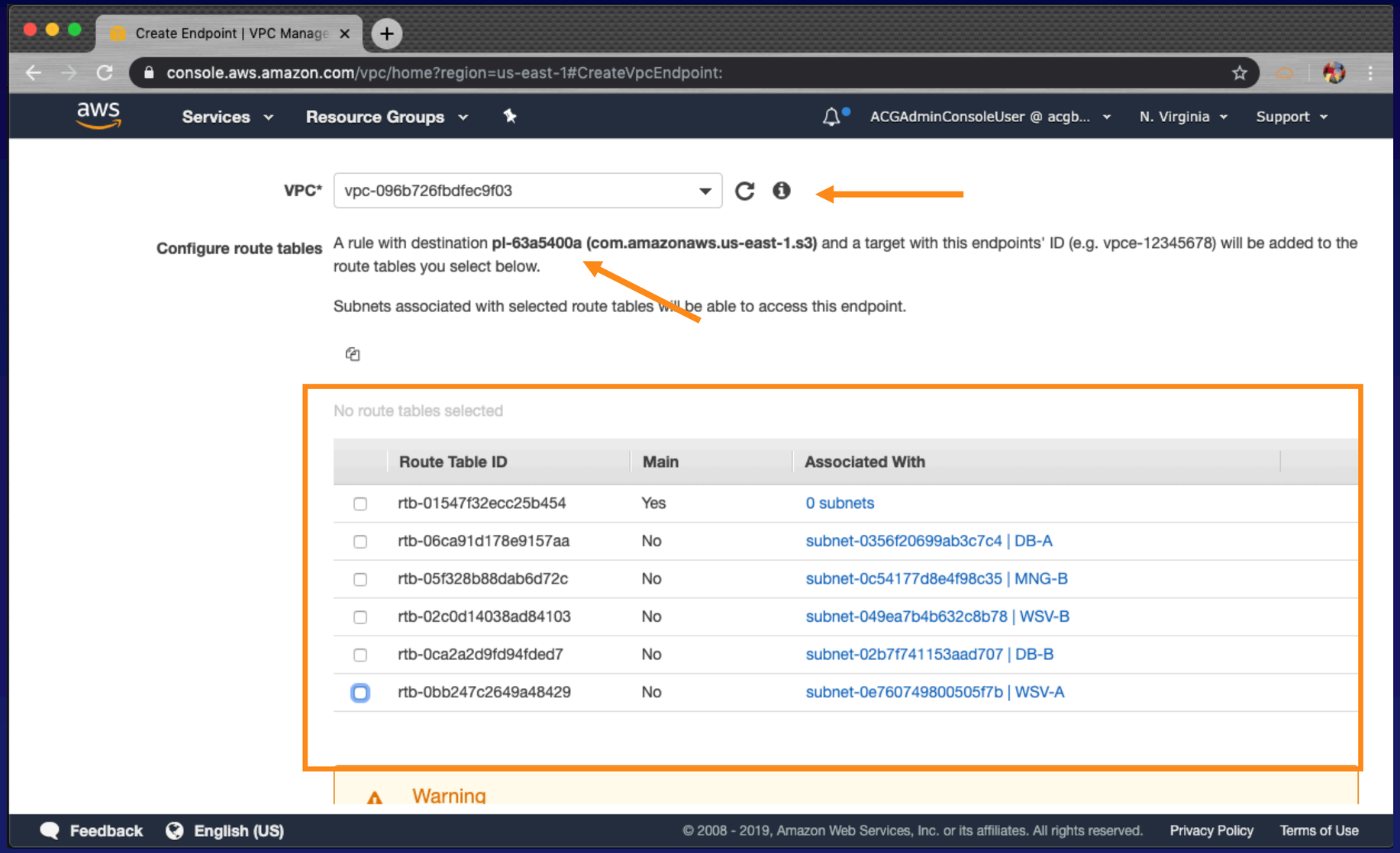
Multiple VPC Endpoints

You can have multiple VPC endpoints within the same VPC – even for the same service. Each endpoint can have its own policy, and each can be applied to different subnets (e.g. the specific subnet route table).

Creating a VPC Endpoint



Creating a VPC Endpoint



Creating a VPC Endpoint