

VPC Endpoints



Brock Tubre

TECHNICAL INSTRUCTOR

Two Types of VPC Endpoints

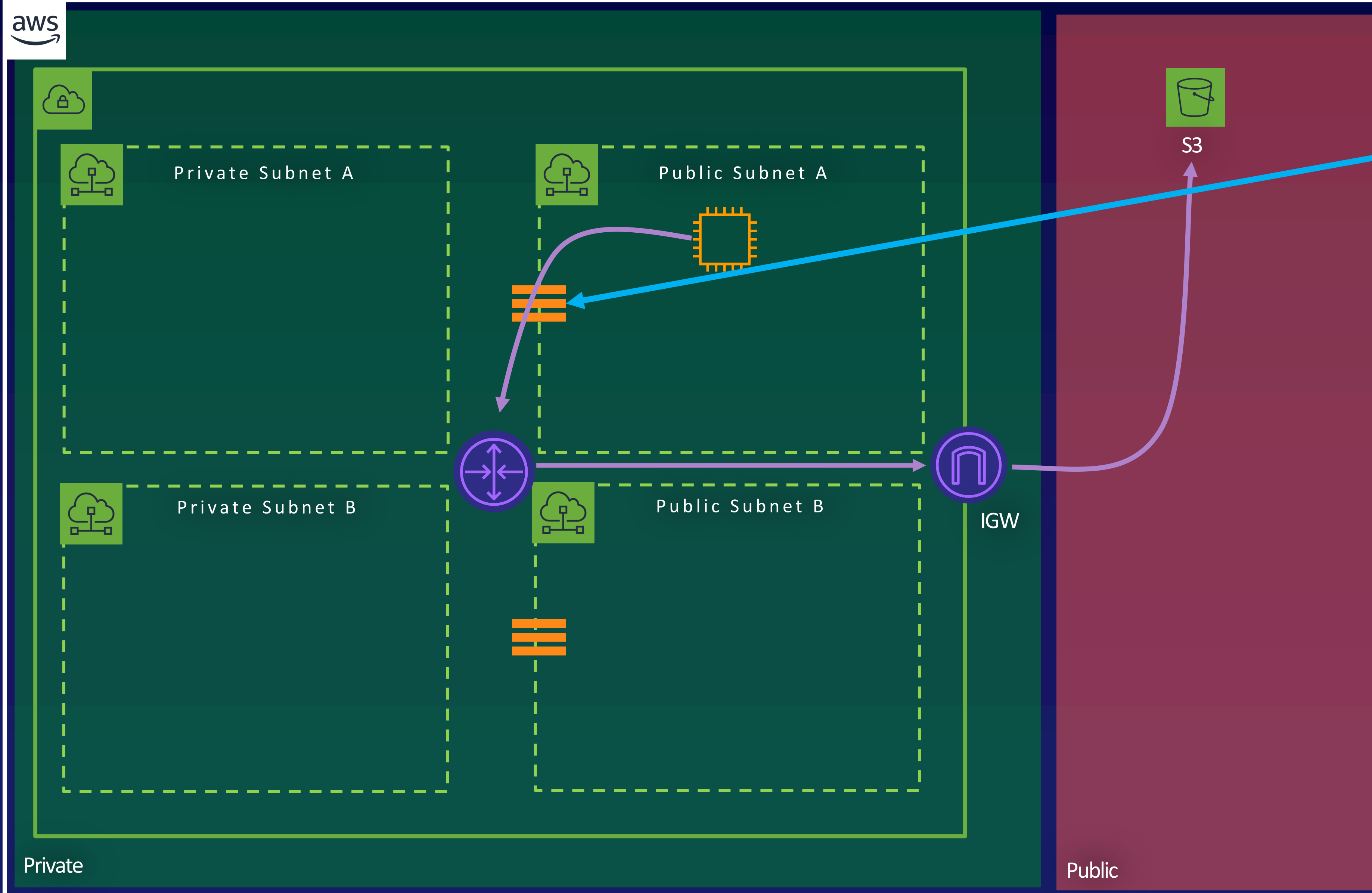
Interface Endpoints

- 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.

Classic Access to S3

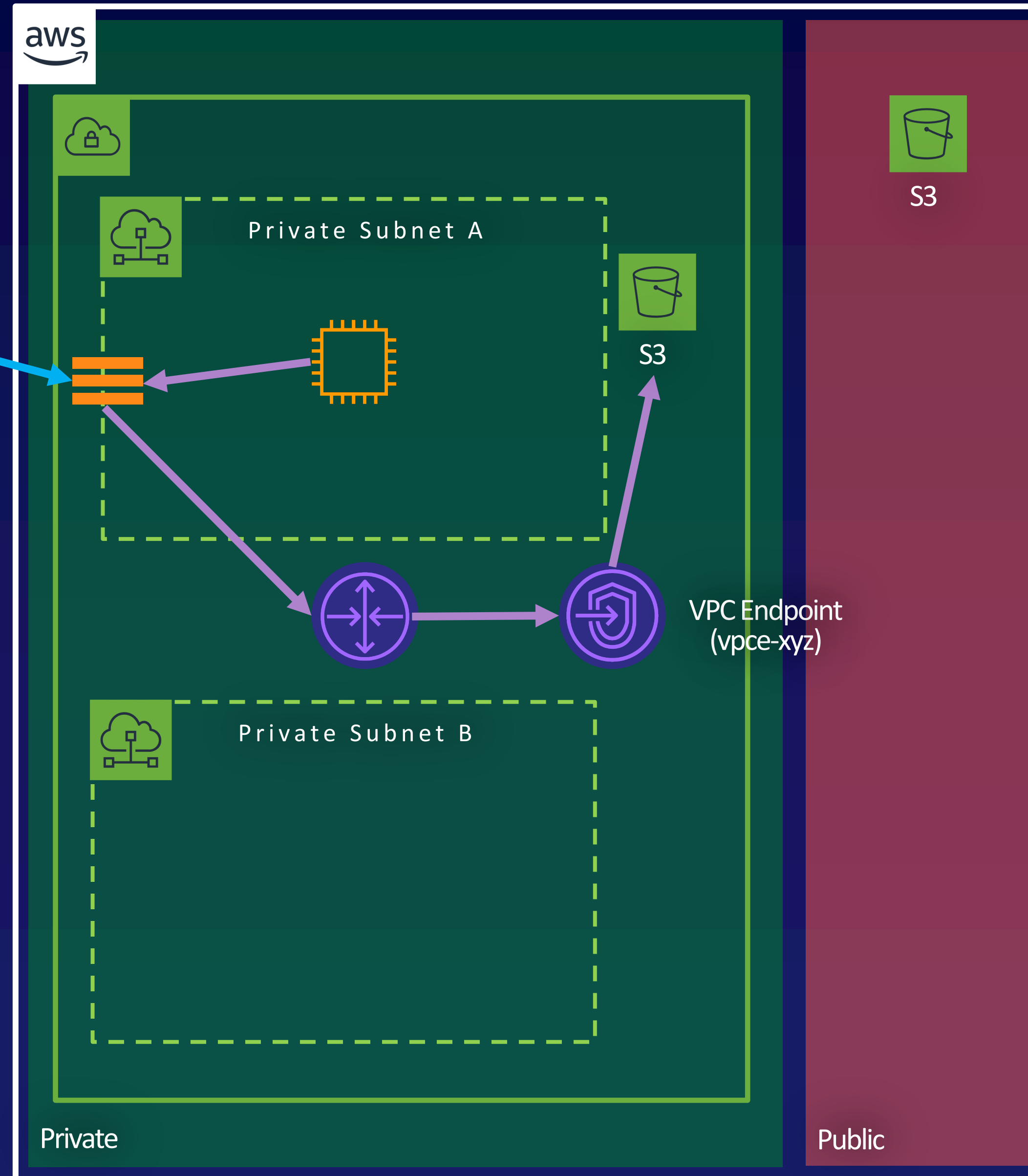


Destination	Target
VPC CIDR	local
0.0.0.0/0	IGW

Simple VPC Endpoint

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

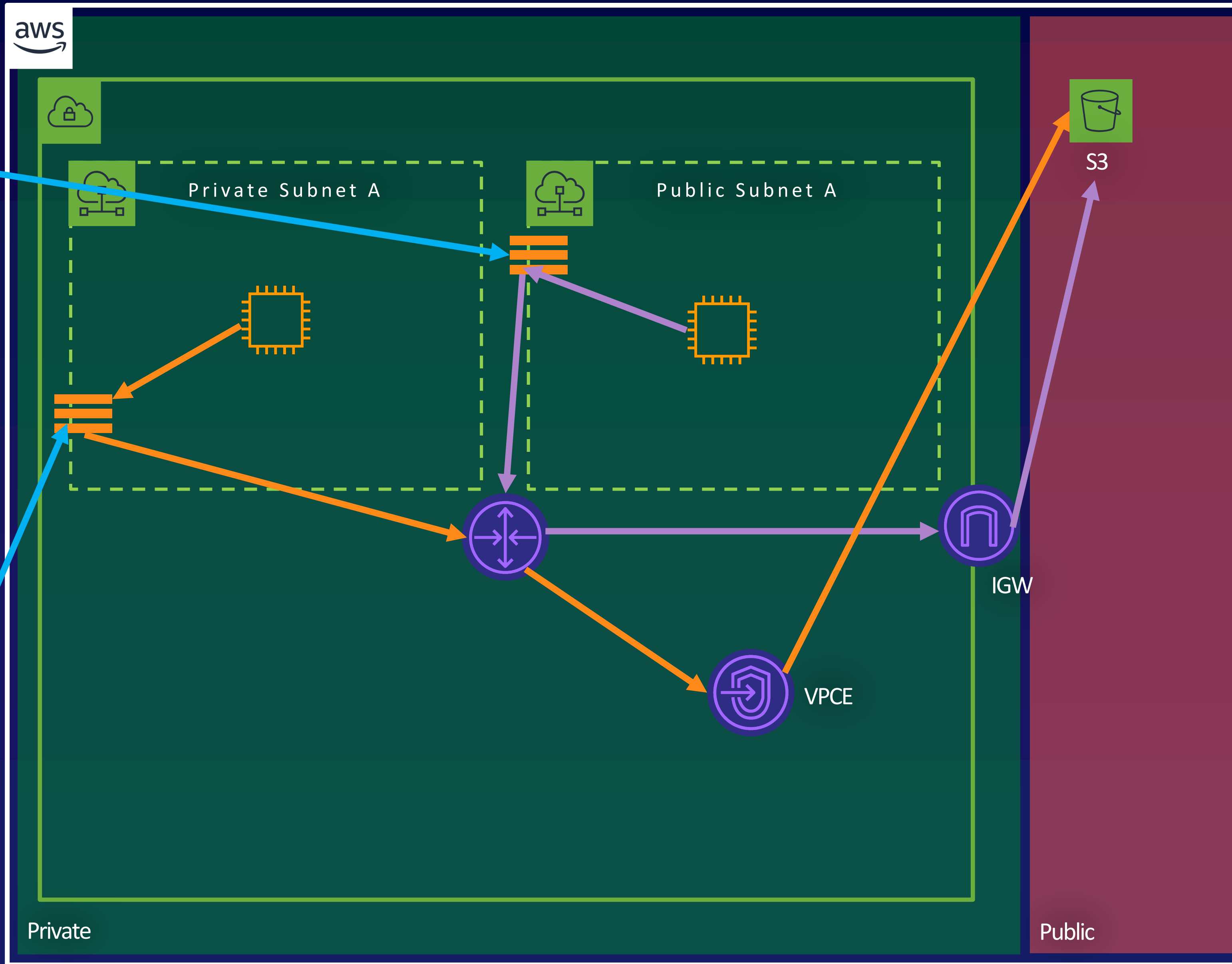
com.amazonaws.region.service



Classic Access and VPC Endpoints

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.

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

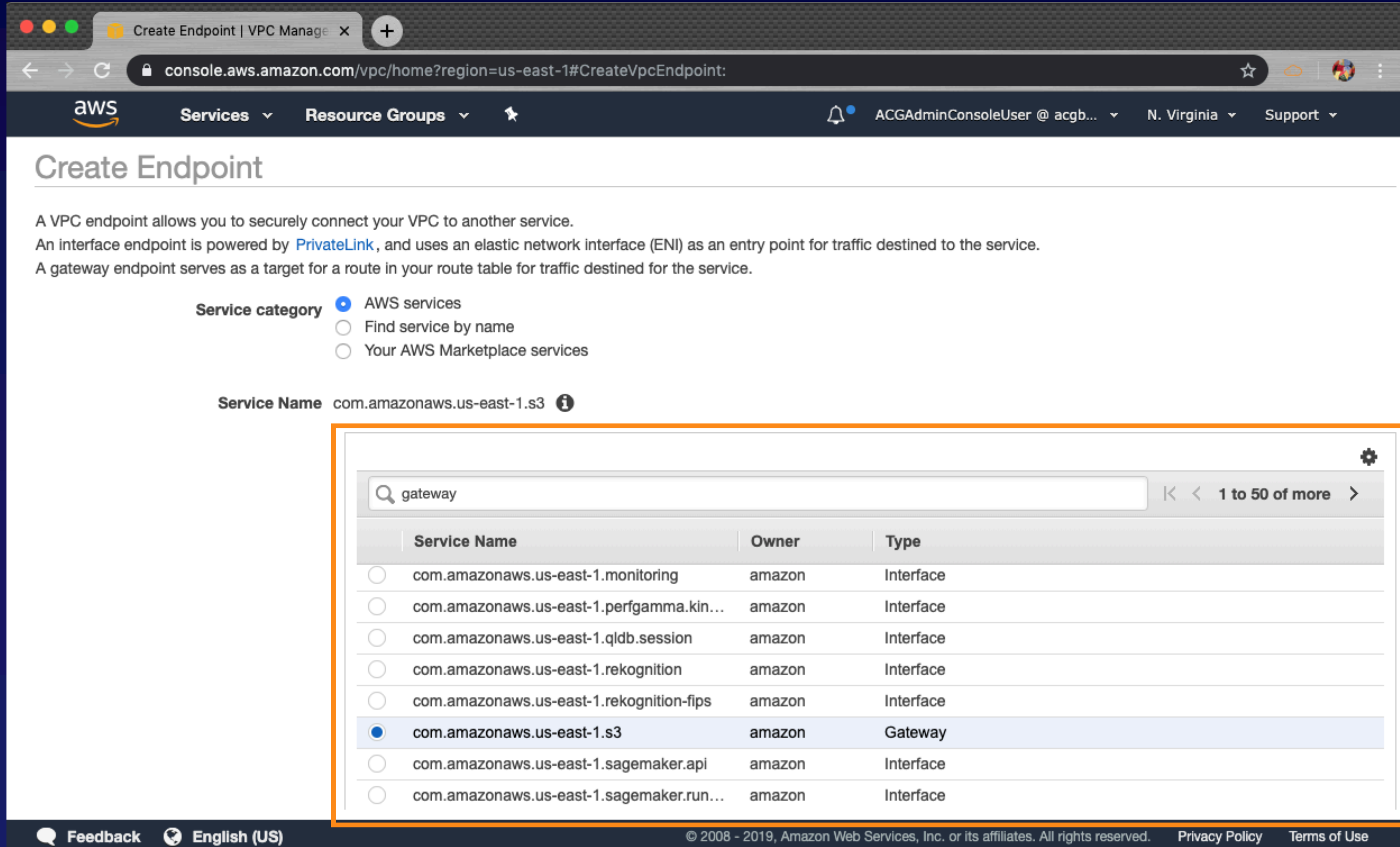
Controlling Access

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).



Create Endpoint | VPC Manage x

console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:

aws Services Resource Groups ACGAdminConsoleUser @ acgb... N. Virginia Support

Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by [PrivateLink](#), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service category AWS services
 Find service by name
 Your AWS Marketplace services

Service Name com.amazonaws.us-east-1.s3 ⓘ

gateway

Service Name	Owner	Type
<input type="radio"/> com.amazonaws.us-east-1.monitoring	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.perfgamma.kin...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.qldb.session	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.rekognition	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.rekognition-fips	amazon	Interface
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-1.sagemaker.api	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.sagemaker.run...	amazon	Interface

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

VPC*

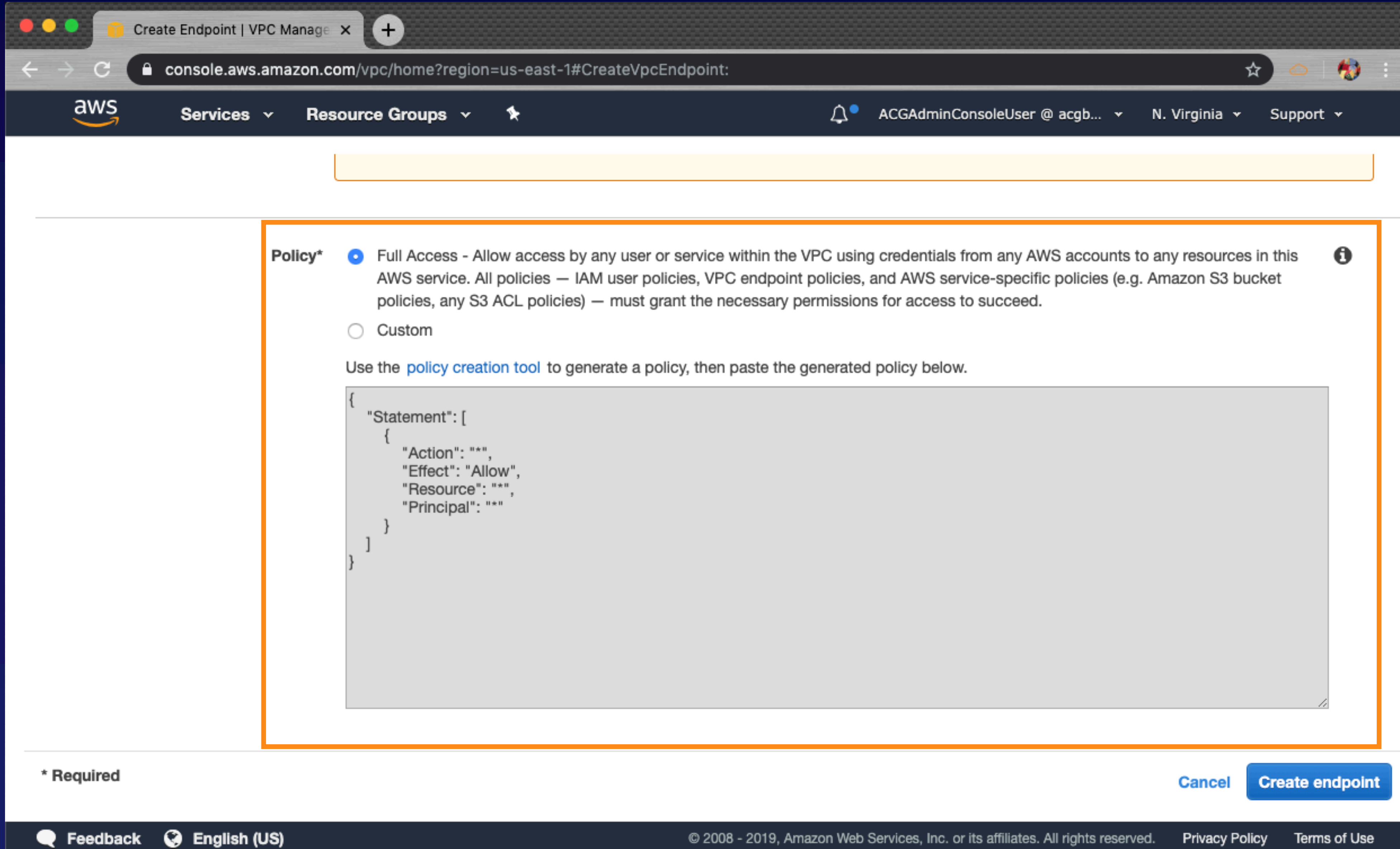
Configure route tables A rule with destination **pl-63a5400a (com.amazonaws.us-east-1.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

No route tables selected

	Route Table ID	Main	Associated With
<input type="checkbox"/>	rtb-01547f32ecc25b454	Yes	0 subnets
<input type="checkbox"/>	rtb-06ca91d178e9157aa	No	subnet-0356f20699ab3c7c4 DB-A
<input type="checkbox"/>	rtb-05f328b88dab6d72c	No	subnet-0c54177d8e4f98c35 MNG-B
<input type="checkbox"/>	rtb-02c0d14038ad84103	No	subnet-049ea7b4b632c8b78 WSV-B
<input type="checkbox"/>	rtb-0ca2a2d9fd94ded7	No	subnet-02b7f741153aad707 DB-B
<input checked="" type="checkbox"/>	rtb-0bb247c2649a48429	No	subnet-0e760749800505f7b WSV-A

Warning



console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:

aws Services Resource Groups ACGAdminConsoleUser @ acgb... N. Virginia Support

Policy*

Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed. ⓘ

Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

* Required

Cancel Create endpoint

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use