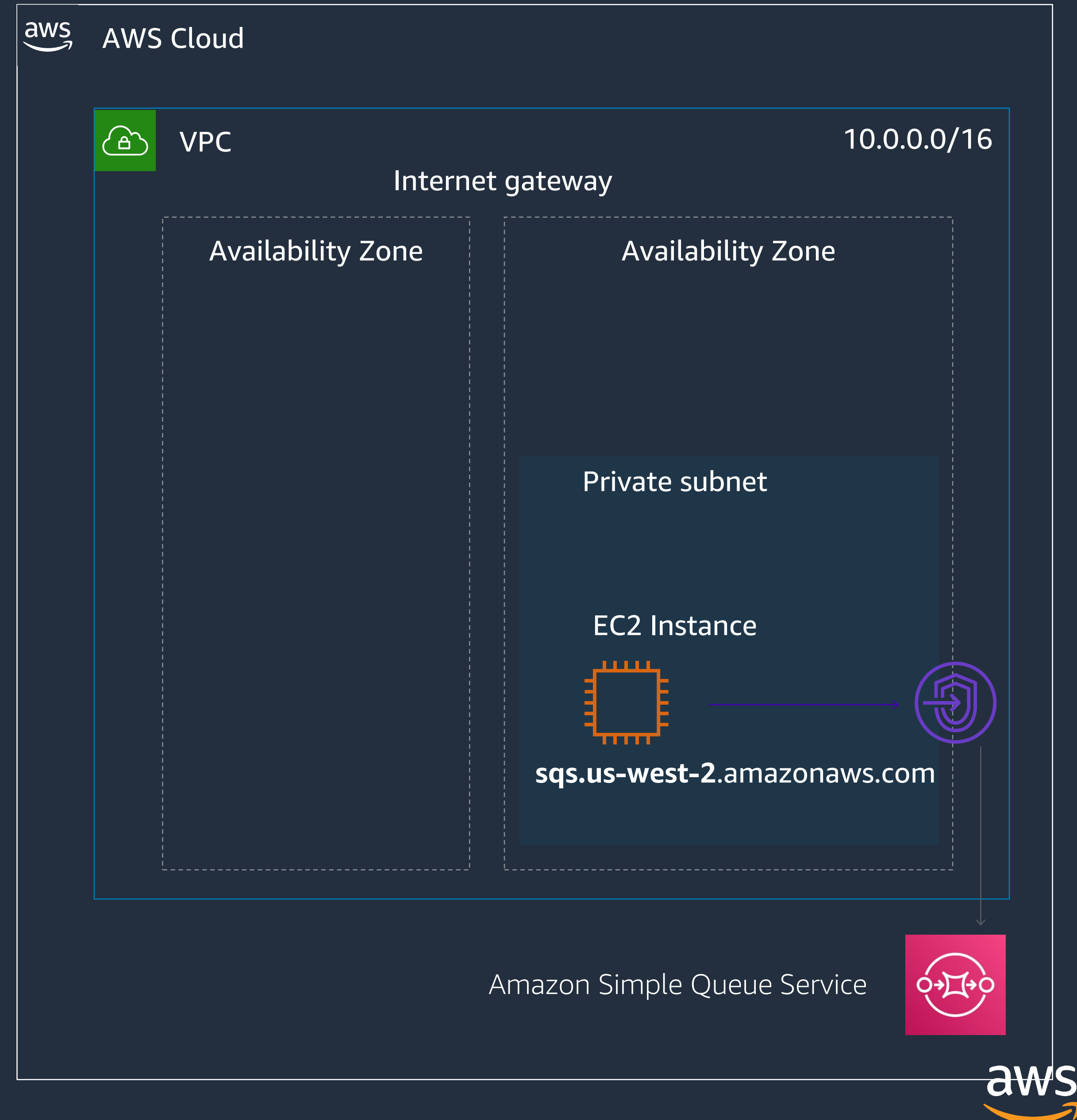


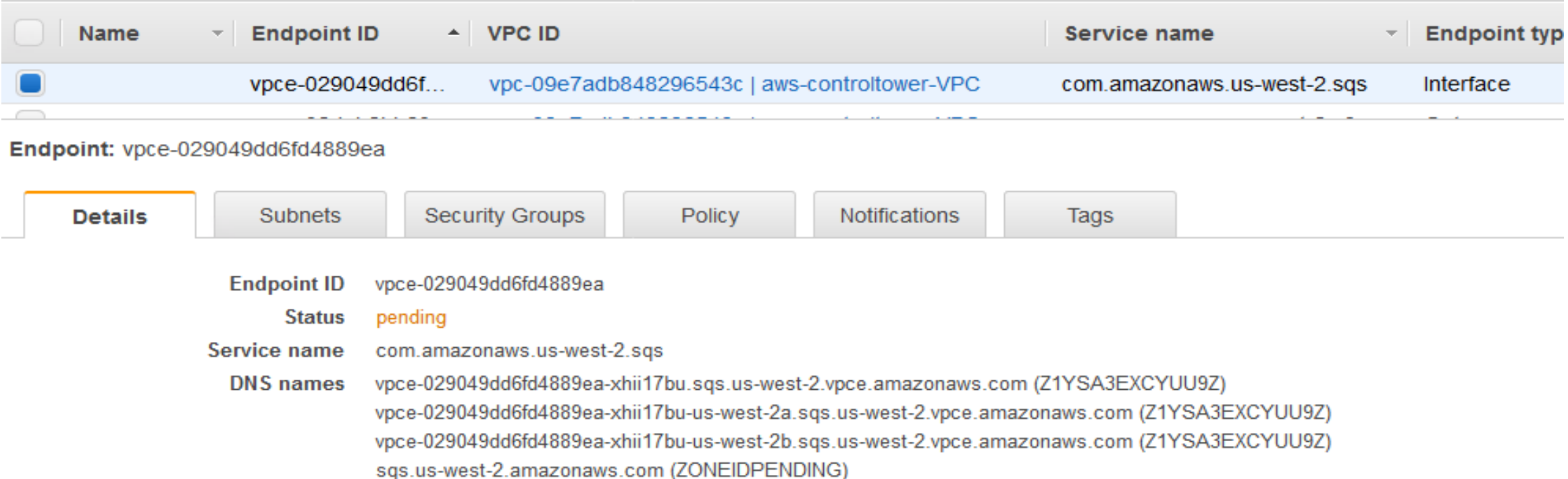
VPC Endpoints

- Privately connect your VPC to supported AWS services
- Traffic traveling between your VPC and the AWS service does not leave the Amazon network.
- VPC Endpoints are horizontally scaled, redundant and highly available
- Two types of VPC endpoints
 - Interface endpoints
 - Gateway endpoints



Interface Endpoints

- Accessed via an elastic network interface (ENI)
- Assigned a private IP address from the address range of your chosen subnet(s)
- Serve as an entry point for traffic destined to a supported service
- AWS creates endpoint-specific DNS hostnames that you can use to communicate with the target AWS service



The screenshot shows the AWS Management Console interface for an Interface Endpoint. At the top, a table lists the endpoint with columns for Name, Endpoint ID, VPC ID, Service name, and Endpoint type. Below this, the 'Details' tab is selected, displaying the following information:

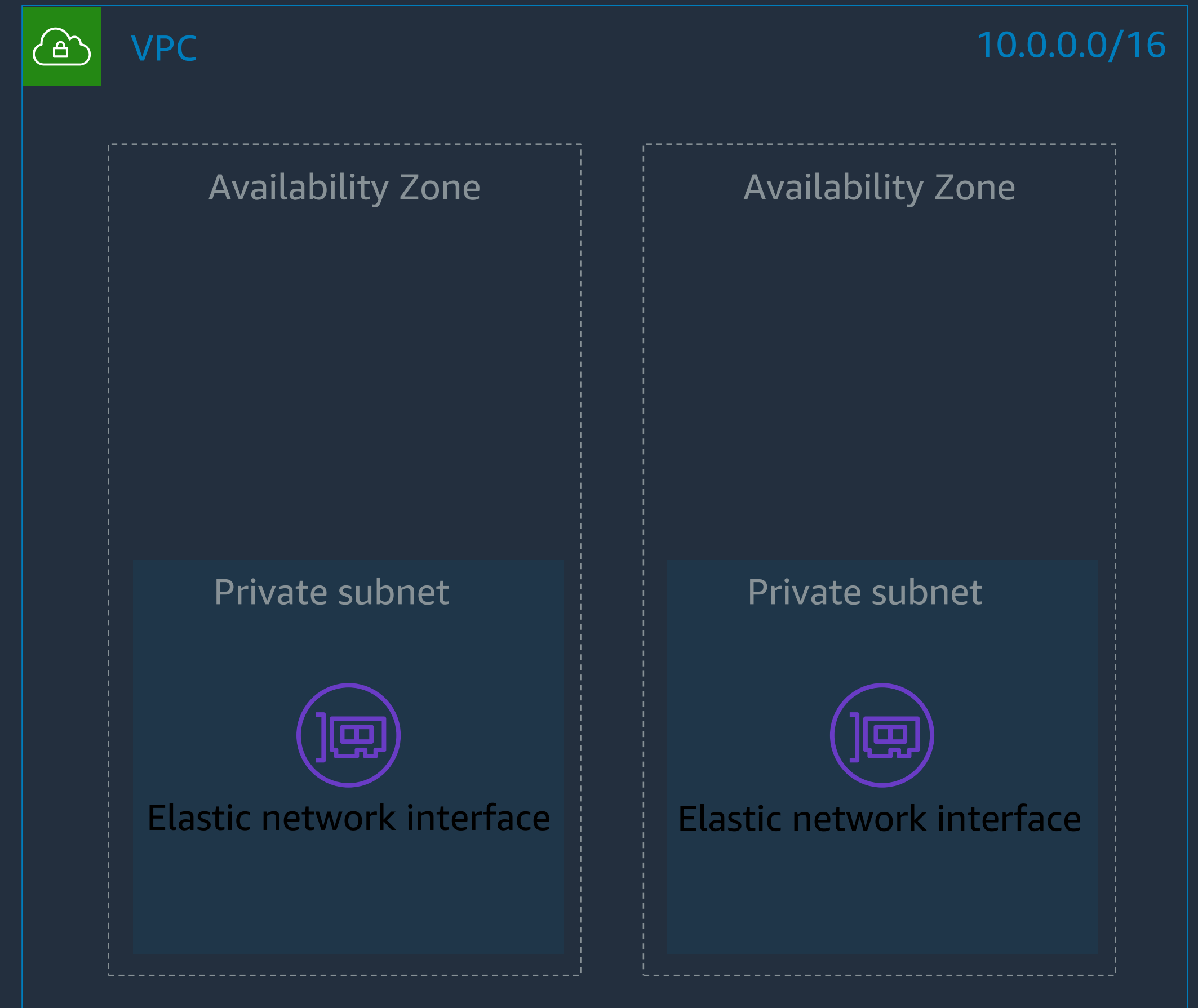
Endpoint ID	vpce-029049dd6fd4889ea
Status	pending
Service name	com.amazonaws.us-west-2.sqs
DNS names	vpce-029049dd6fd4889ea-xhii17bu.sqs.us-west-2.vpce.amazonaws.com (Z1YSA3EXCYUU9Z) vpce-029049dd6fd4889ea-xhii17bu-us-west-2a.sqs.us-west-2.vpce.amazonaws.com (Z1YSA3EXCYUU9Z) vpce-029049dd6fd4889ea-xhii17bu-us-west-2b.sqs.us-west-2.vpce.amazonaws.com (Z1YSA3EXCYUU9Z) sqs.us-west-2.amazonaws.com (ZONEIDPENDING)

For a list of supported services, check here:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Interface Endpoints: High Availability

- Accessed via one or more Elastic Network Interfaces (ENI)
- Each ENI exists in a single subnet in a single availability zone (AZ)
- Provisioned in each availability zone in which you plan to run your application to increase availability.
- Each ENI supports 10 Gbps per AZ by default. Additional capacity may be added automatically based on your usage.

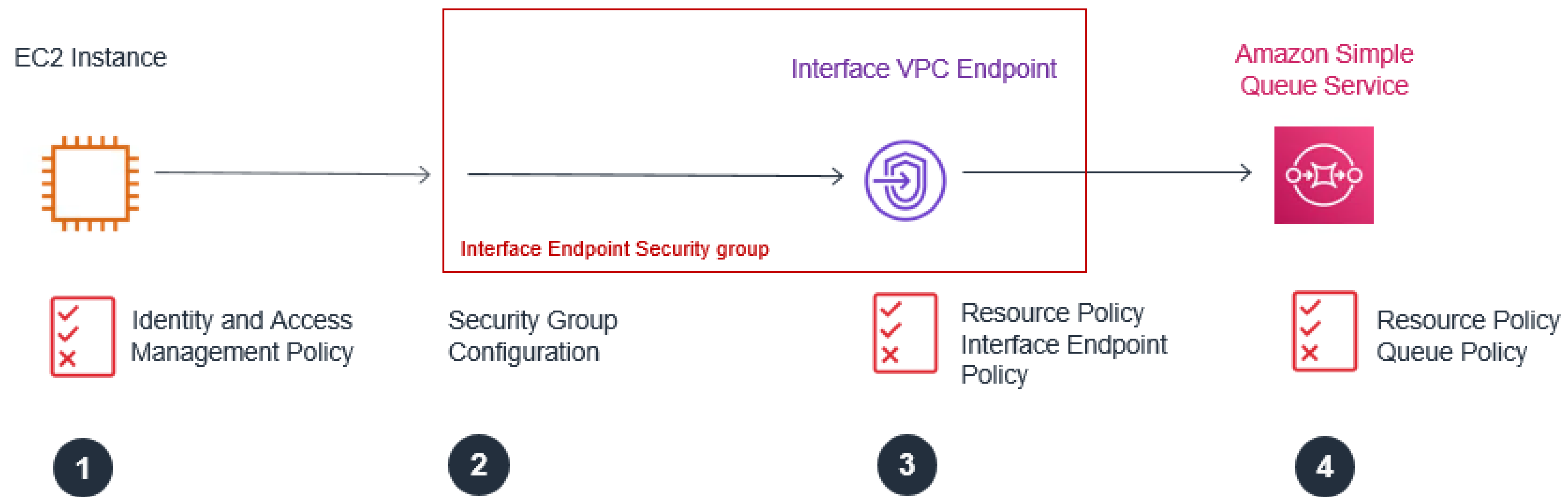


Interface Endpoints: Access via DNS entries

By default, private DNS entries are created for endpoints that reference AWS services

- A **default DNS** name for the target service (e.g. **sqs.us-west-2**.amazonaws.com) that resolves to the private IP addresses of the endpoint network interfaces in your VPC
- An **endpoint-specific regional DNS** hostname that we generate for the interface endpoint. The hostname includes a unique endpoint identifier, service identifier, the Region, and vpce.amazonaws.com in its name (e.g. **vpce-029049dd6fd4889ea-xhii17bu**.sqs.us-west-2.vpce.amazonaws.com)
- An **endpoint-specific zonal DNS** hostname that we generate for each Availability Zone in which the endpoint is available. The hostname includes the Availability Zone in its name (e.g. **vpce-029049dd6fd4889ea-xhii17bu-us-west-2b**.sqs.us-west-2.vpce.amazonaws.com). You might use this option if your architecture isolates Availability Zones for fault containment or to reduce regional data transfer costs.

Interface Endpoints: Access



1. IAM Role, Policy
2. Security Group
3. Interface Endpoint Resource Policy
4. Target Service Resource

Gateway Endpoints

Configured and accessed **differently** than an interface endpoint

- Available only for Amazon Simple Storage Service (S3) and Amazon DynamoDB
- A target route is added by AWS in a route table of your choosing. This results in traffic destined being routed via the gateway to reach the supported AWS service
- When you create a gateway endpoint, you specify
 - VPC in which to create the gateway
 - An endpoint policy that allows access to some or all parts of the service (e.g. a list of S3 buckets or DynamoDB tables you want to make accessible via the gateway)
 - One or more route tables entries which will routes service requests via the gateway

Gateway Endpoints: Prefix Lists

AWS will add routes to the route tables you select. The route identifies the AWS service with a *prefix list*.

The prefix list ID uses the form:

pl-xxxxxxx

A prefix list name uses the form:

"com.amazonaws.region.service"

aws

Services

Resource Groups

Admin/ncharris-Isengard @ nc...

N. Virginia

Support

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Create route table

Actions

Filter by tags and attributes or search by keyword

1 to 4 of 4

Name	Route Table ID	Explicit subnet associatio	Main
	rtb-07901f4934ae92b61	-	Yes
Private subnet 1A	rtb-0c4804c600462ad8f	subnet-07372103f000e353c	No
Private subnet 2A	rtb-0c23cfce43d03d95f	subnet-043d7df3749379a16	No

Route Table: rtb-0c4804c600462ad8f

SummaryRoutesSubnet AssociationsRoute PropagationTags

Edit routes

ViewAll routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
pl-63a5400a (com.amazonaws.us-east-1.s3, 54.231.0.0/17, 52.216.0.0/15)	vpce-0f93d5fde027c62e4	active	No
0.0.0.0/0	nat-01163c20b03d6de19	active	No

Gateway Endpoints: Prefix Lists

- The prefix list ID logically represents the range of public IP addresses used by the service
- All instances in subnets associated with the specified route tables automatically use the gateway endpoint to access the service; subnets that are not associated with the specified route tables do not use the gateway endpoint
- This enables you to keep resources in other subnets separate from your gateway endpoint. To view the current public IP address range for a given service, you can use the [describe-prefix-lists](#) command
- You cannot explicitly add, modify, or delete an endpoint route in your route table by using the route table APIs, or by using the Route Tables page in the Amazon VPC console

Gateway Endpoints: Routing

The most specific route will be matched and determine the traffic path

The public CIDR ranges used by S3 are provided by the prefix list

The endpoint route takes precedence for all traffic destined for the service, because the IP address range for the service is more specific than 0.0.0.0/0

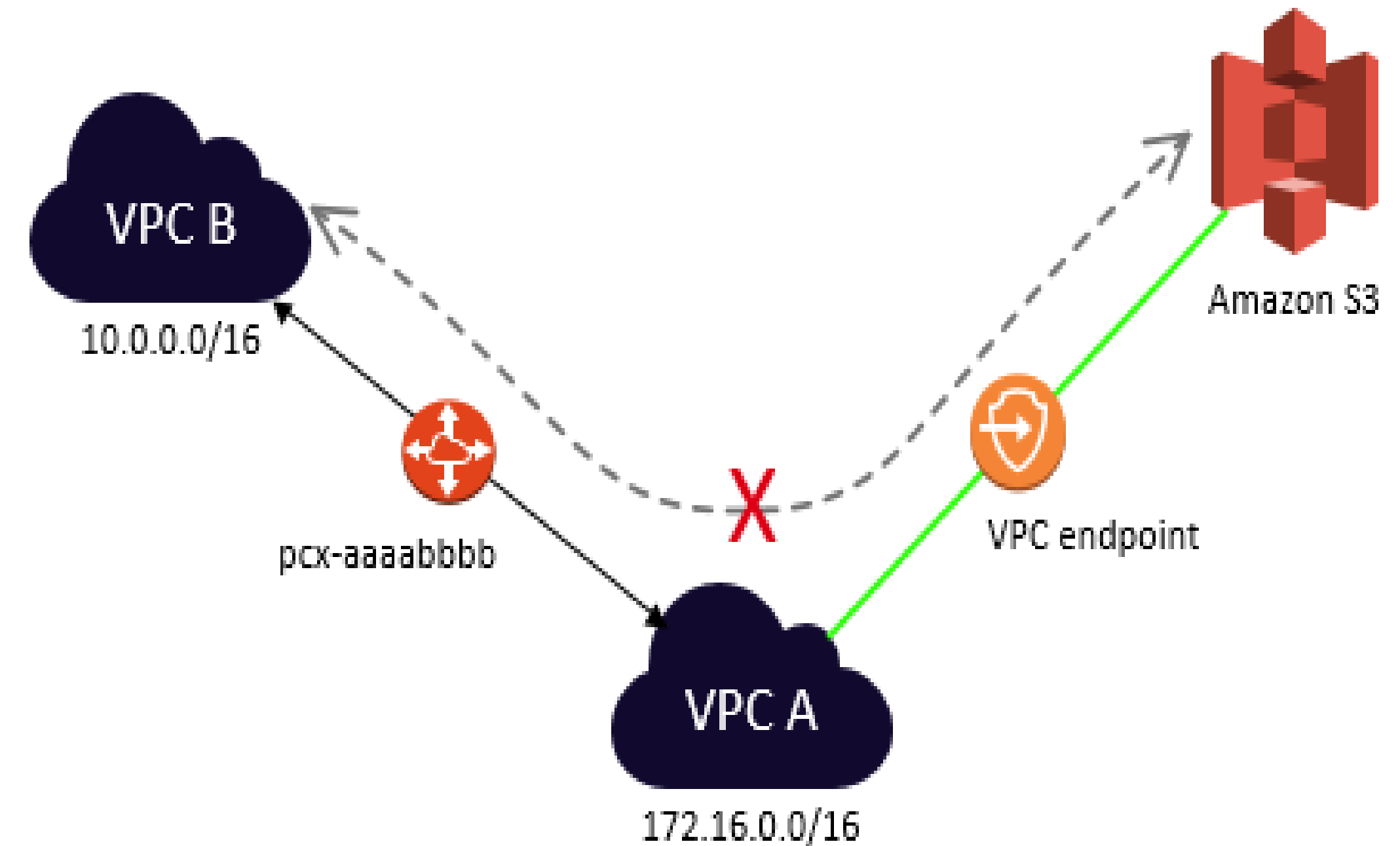
Destination	Target
10.0.0.0/16	local
pl-63a5400a (com.amazonaws.us-east-1.s3, 54.231.0.0/17, 52.216.0.0/15)	vpce-0f93d5fde027c62e4
0.0.0.0/0	nat-01163c20b03d6de19

Gateway Endpoints: Routing

AWS services cannot initiate requests to resources in your VPC through the endpoint.

Gateway endpoints will only service requests that were initiated within the same VPC

An endpoint only returns responses to traffic initiated from resources in your VPC



Resource Policies for VPC Endpoints

- A VPC endpoint policy is a resource policy that you attach to an endpoint (interface or gateway)
- If you do not attach a policy when you create an endpoint, AWS attaches a default policy for you that allows full access to the service
- An endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies). It is a separate policy for controlling access from the endpoint to the specified service
- You cannot attach more than one policy to an endpoint.

Resource Policies for VPC Endpoints: Request Evaluation

When AWS receives a request, AWS completes several steps to determine whether to ALLOW or DENY the request.

- Authentication – AWS first authenticates the principal that makes the request, if necessary
- Processing the Request Context – AWS processes the information gathered in the request to determine which policies apply to the request
- Evaluating Policies Within a Single Account – AWS evaluates all of the policy types, which affect the order in which the policies are evaluated
- Determining Whether a Request Is Allowed or Denied Within an Account – AWS then processes the policies against the request context to determine whether the request is allowed or denied.

IAM policies provide access to AWS services. Endpoint policies allow you to control the use of the endpoints.

Let's go
build

<http://bit.ly/vpc-endpoints-lab>