VPC Overview

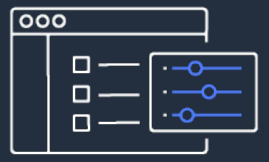
Jinsung Heo

Amazon Virtual Private Cloud

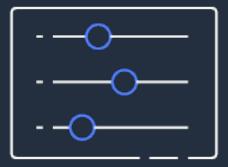
Amazon VPC - Virtual Private Cloud

Provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define

Bring your own network



IP Addresses



Subnets

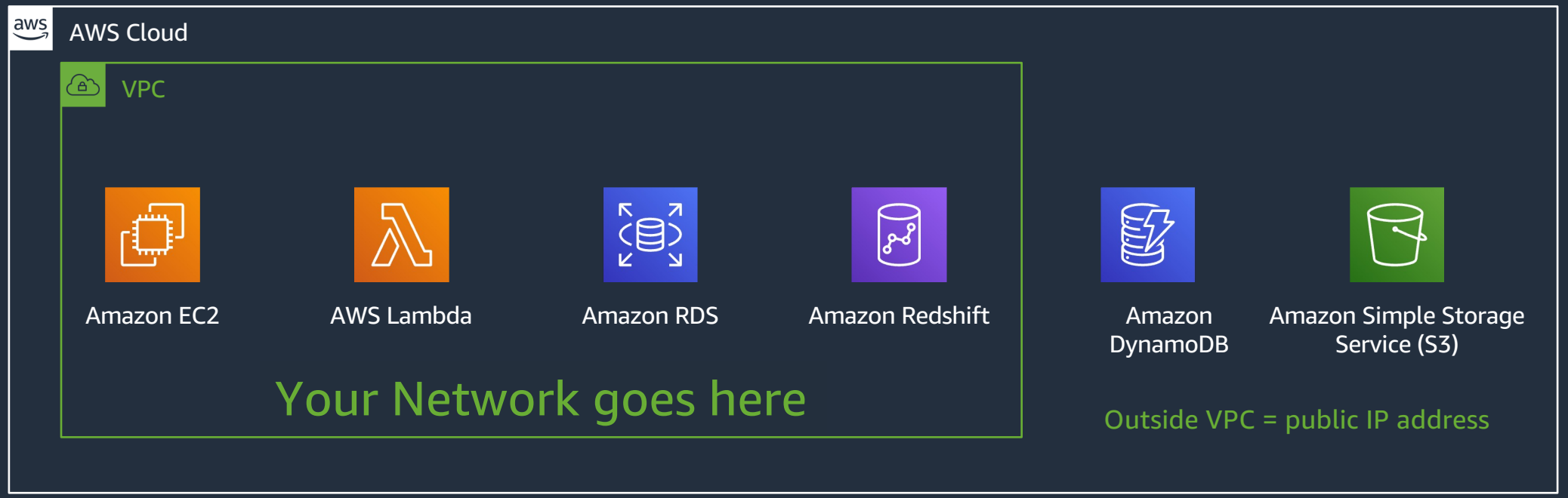
Network Topology

Routing Rules

Security Rules

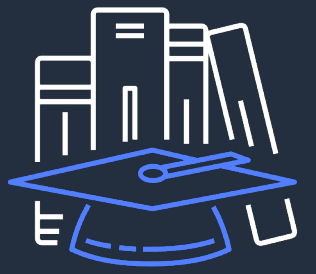
aws

Amazon Virtual Private Cloud (VPC)



CIDR notation review

CIDR range example:



```
172.31.0.0/16
1010 1100 0001 1111 0000 0000 0000 0000
```


aws

Choosing an IP address range for your VPC

VPC

Avoid ranges that overlap with other networks to which you might connect

172.31.0.0/16

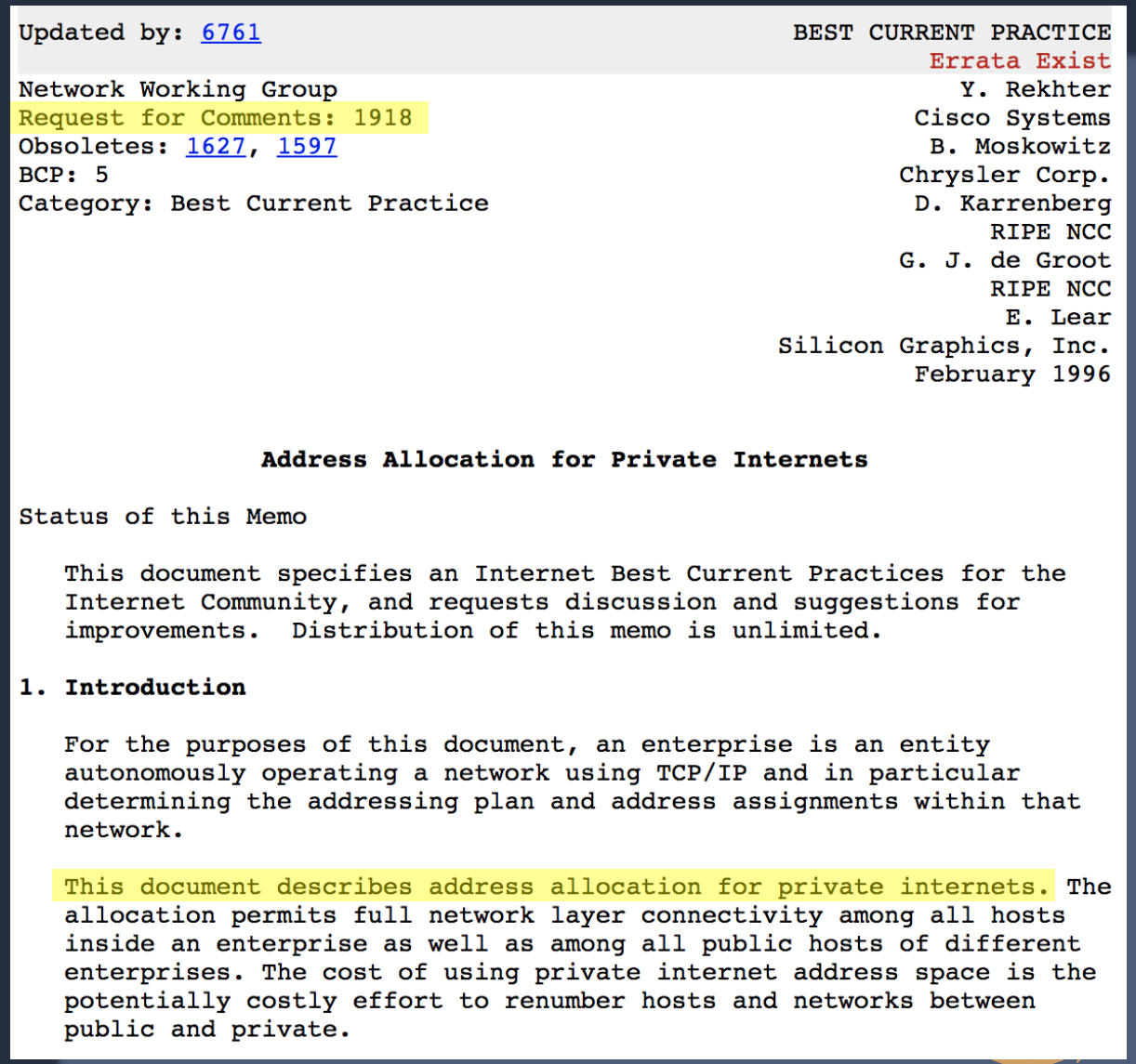
Recommended: RFC1918 range

aws

Private IP address range for your VPC – IPv4

- "CIDR" Range ?
  - Classless Inter-domain Routing
  - No more Class A, B, C
- RFC1918
  - 192.168.0.0 /16
  - 172.16.0.0 /12
  - 10.0.0.0 /8
- Other IP ranges*
- How Big ?

*View here for more details on what IPv4 Ranges can be assigned to a VPC



Updated by: 6761 BEST CURRENT PRACTICE
Errata Exist

Network Working Group Y. Rekhter
Request for Comments: 1918 Cisco Systems
Obsoletes: 1627, 1597 B. Moskowitz
BCP: 5 Chrysler Corp.
Category: Best Current Practice D. Karrenberg
RIPE NCC
G. J. de Groot
RIPE NCC
E. Lear
Silicon Graphics, Inc.
February 1996

Address Allocation for Private Internets

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

1. Introduction

For the purposes of this document, an enterprise is an entity autonomously operating a network using TCP/IP and in particular determining the addressing plan and address assignments within that network.

This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private.

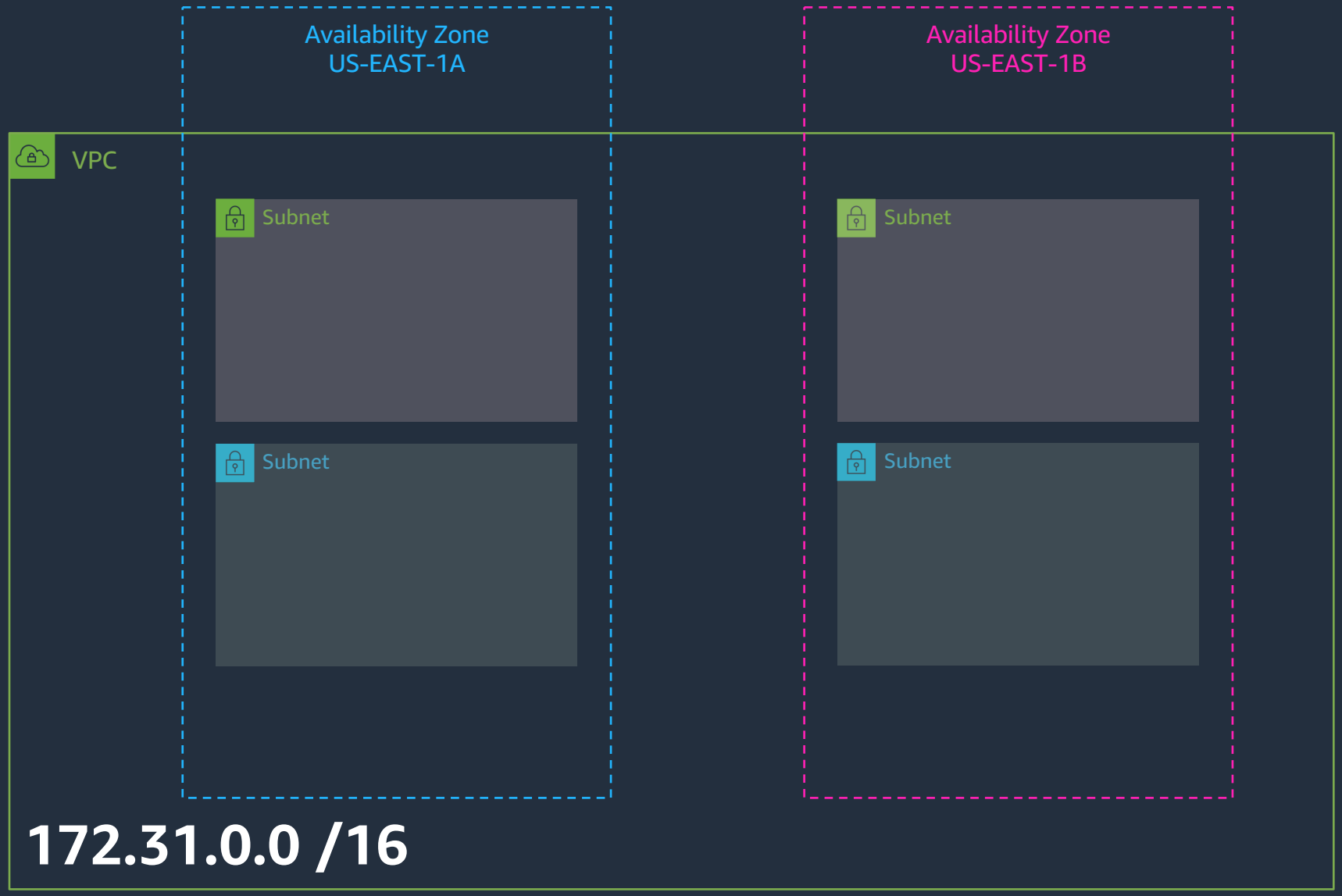
VPC IPv4 address space design considerations

- Bring your own addressing plan
- Plan for future expansion to additional Regions & Availability Zones
- Consider connectivity to corporate networks
- Avoid overlapping IP space
- RFC1918 address exhaustion challenge - Options to use RFC6598 blocks (100.64.0.0/10) and 198.19.0.0/16
- Consider subnet design
    - VPC CIDR cannot be modified once created
    - New CIDRs can be added for expansion
    - Choose VPC CIDR ranges :

/16 = largest address space for VPC
/28 = smallest address space for VPC

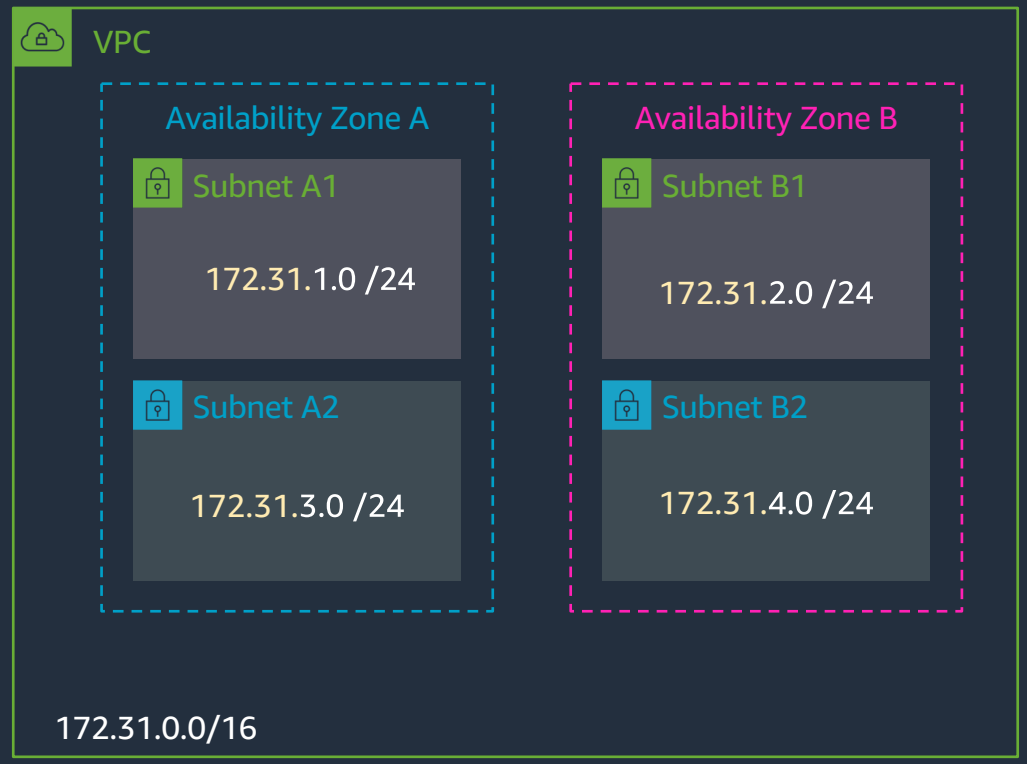
aws

VPC CIDR /16



How to segment my networks inside a VPC?
VPC Subnets

- You can add one or more subnets in each Availability Zone
- AZs provides fault isolations
- Subnets are allocated as a subset of the VPC CIDR range
- Even distribution of IP space across AZs
- Use at least 2 AZs
- How big? How many?



Subnets are AZ specific

aws

VPC and Subnet recommendations

/16 VPC or smaller from private IPv4 address ranges

At least /24 subnets (251 usable addresses)

Use multiple Availability Zones per VPC through multiple subnets

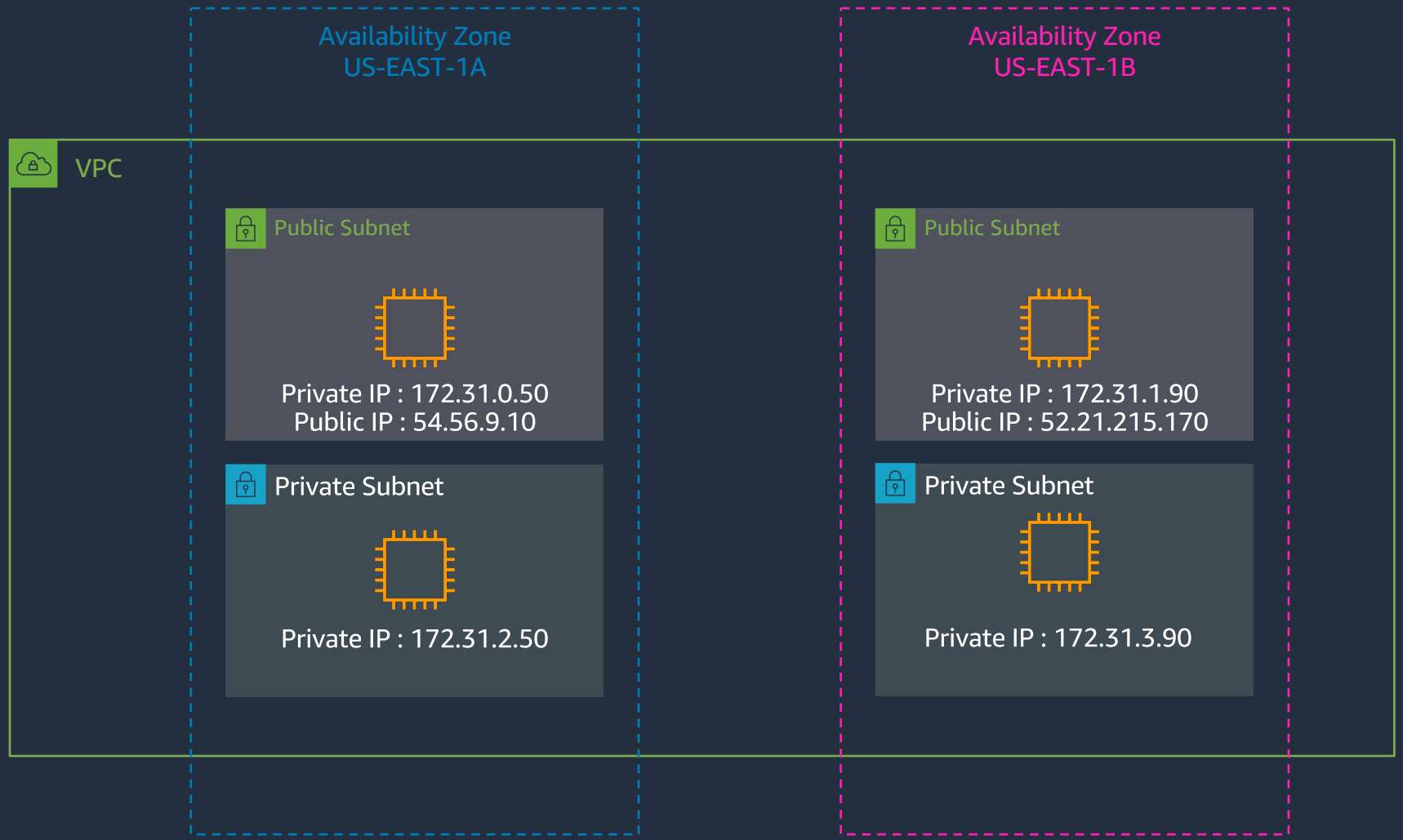
You can expand your VPC by adding additional IP address ranges

aws

Public and Private Subnets

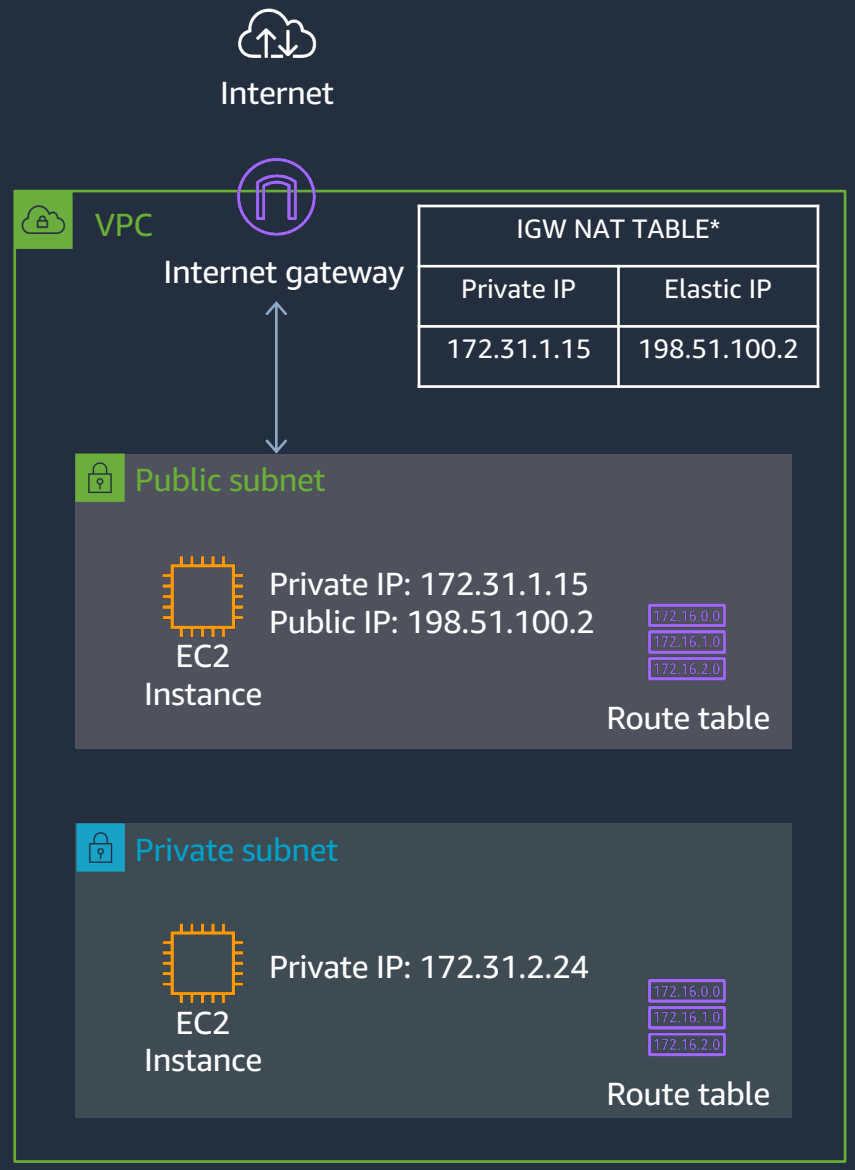
- **Public Subnet**
  - A subnet whose traffic is routed to an Internet Gateway.
  - Allows the use of Elastic IP and Public IP addresses
  - Useful as DMZ infrastructure for web servers & internet ELBs
  - EC2 instances will be assigned Private IP and Public IP that is mapped to the Private through network address translation (NAT).
- **Private Subnet**
  - Subnet that DOES NOT have route to Internet Gateway.
  - Can indirectly route to Internet via NAT instance or NAT gateway.
  - NAT devices reside in a public subnet
  - Useful for application servers and databases
  - EC2 instances will be assigned Private IP in subnet range

Public and Private IP addresses



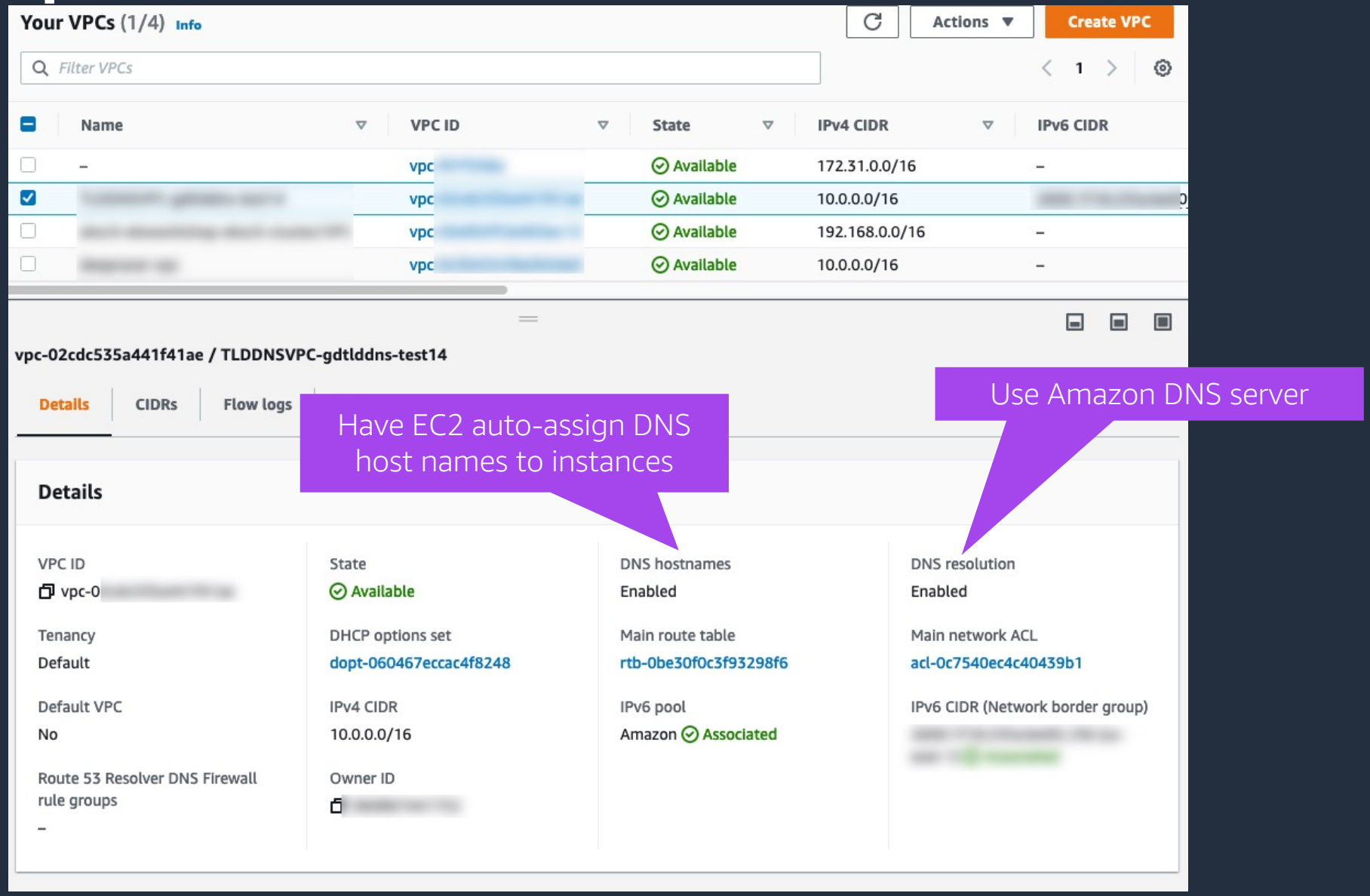
How to connect my VPC to the Internet? Internet Gateway

- Horizontally scaled, redundant, highly available VPC component
- Used to connect your VPC Subnets to the Internet
- Must be attached to the VPC
- Must be referenced on the Route Table
- Performs stateless 1:1 NAT between Public and Private IP Addresses



*AWS Configures this on your behalf

VPC DNS Options



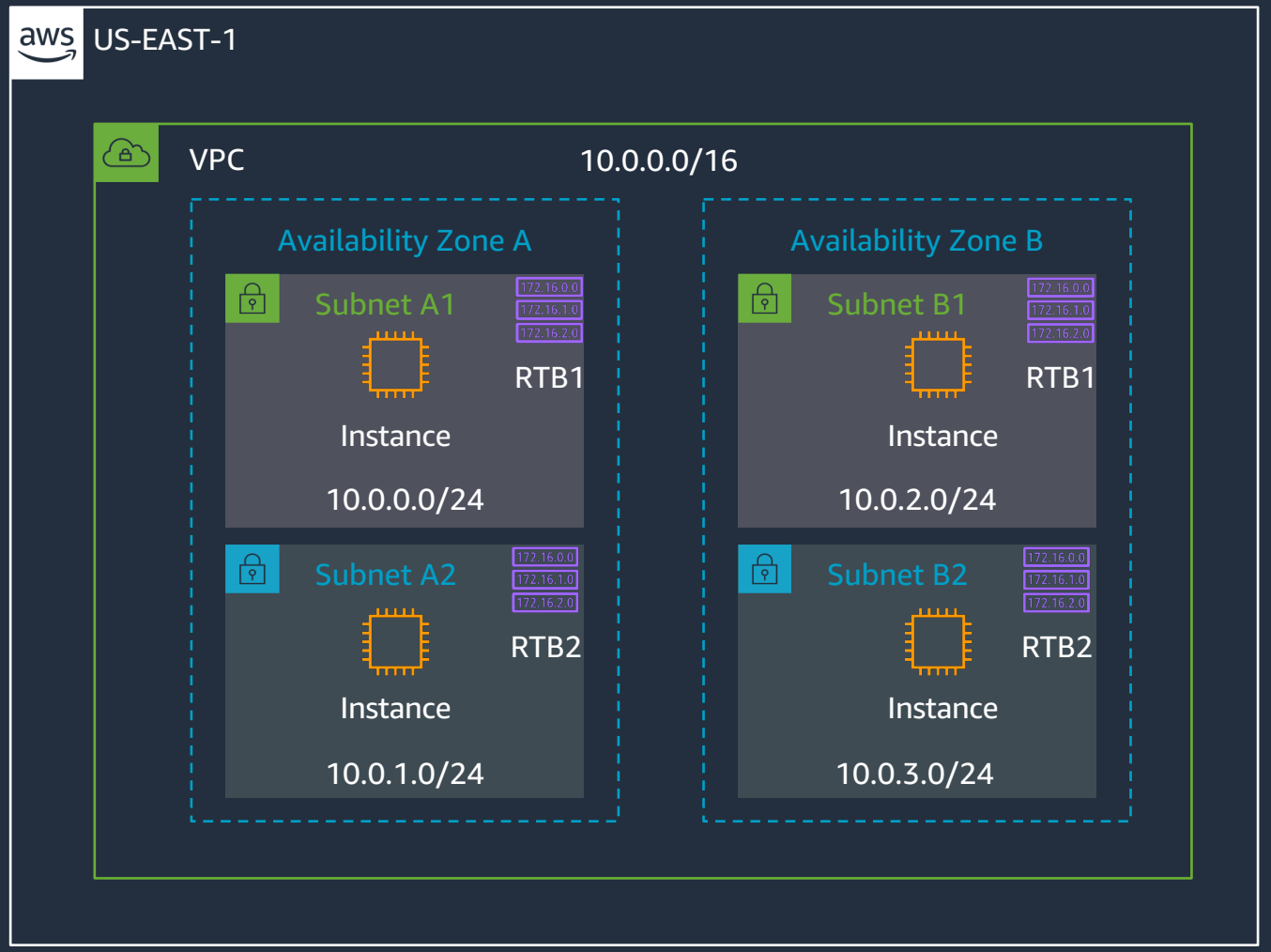
Routing in your VPC

- Route tables contain rules for which packets go where
- Your VPC has a default route table
- But, you can assign different route tables to different subnets

aws

Routing tables

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- You can have 50 routes per route table.



Different routes for different subnets

Public subnet

Destination	Target	Status	Propagated
::/0	igw-047	Active	No
235a:be00::/56	local	Active	No
0.0.0.0/0	igw-047	Active	No
10.0.0.0/16	local	Active	No

To get to the Internet go via the Internet Gateway (IGW)

Private subnet

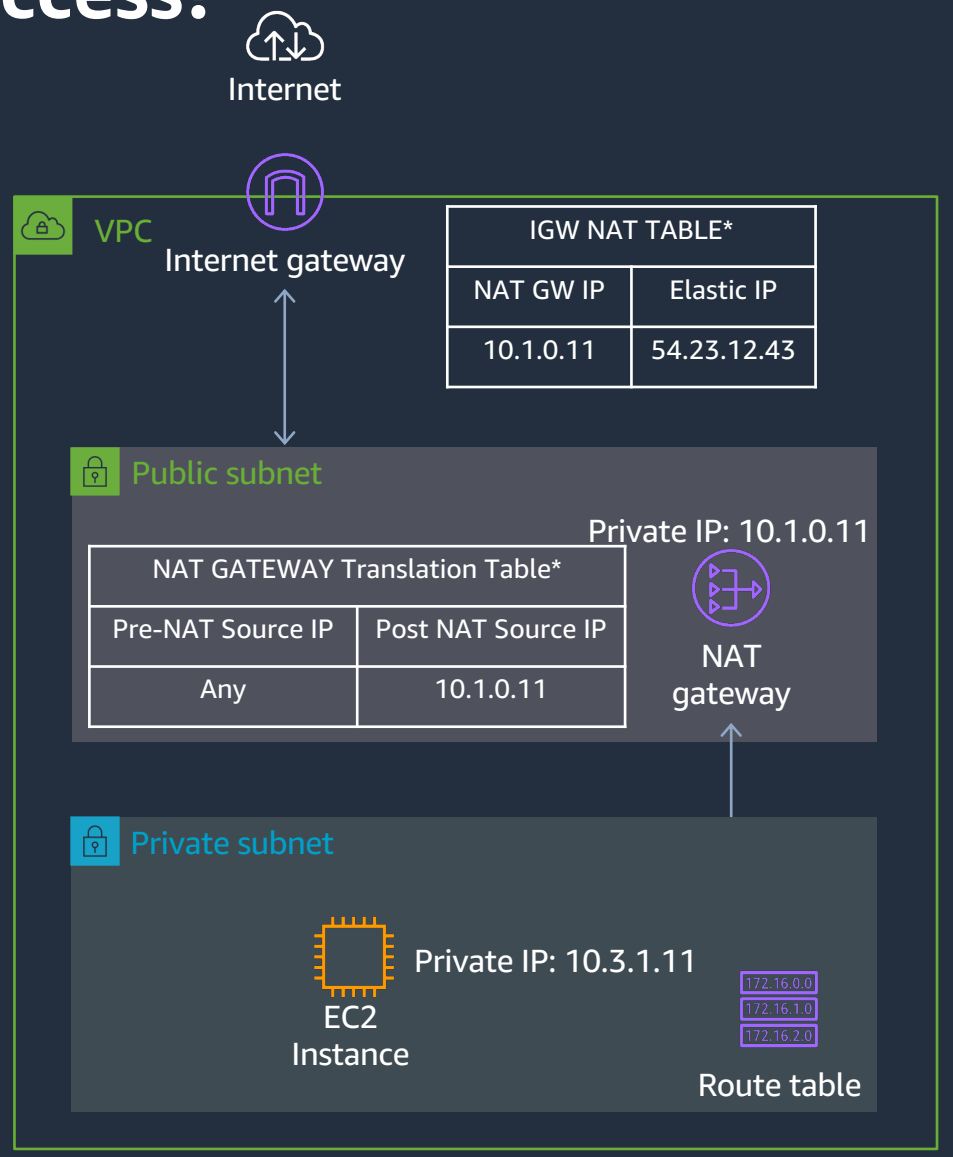
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
235a:be00::/56	local	Active	No

To get to anything in the VPC – stay local. No route anywhere else.

aws

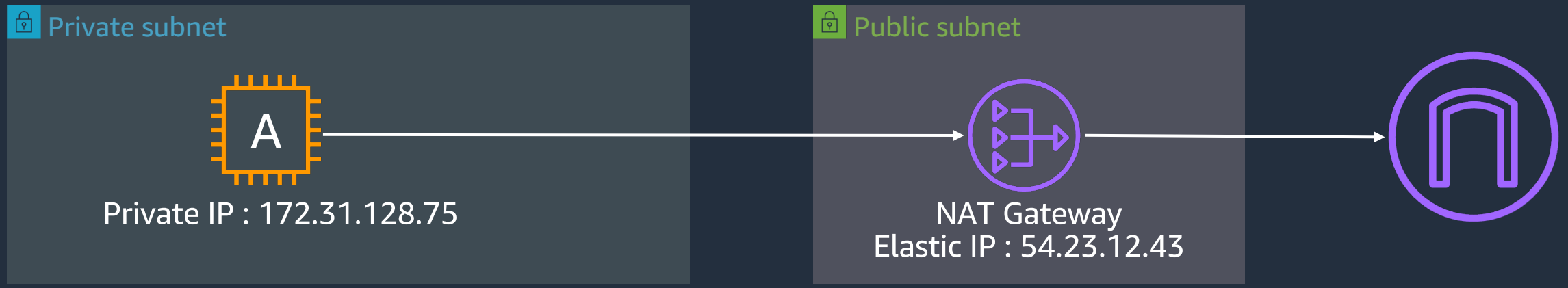
Can I have outbound only Internet access? NAT Gateway

- Enable outbound connection to the internet
- No incoming connection - useful for OS/packages updates, public web services access
- Fully managed by AWS
- Highly available
- Up to 100Gbps bandwidth
- Supports TCP, UDP, and ICMP protocols
- Assign an EIP to each NAT Gateway



*AWS Configures this on your behalf

Network Address Translation (NAT) Gateway



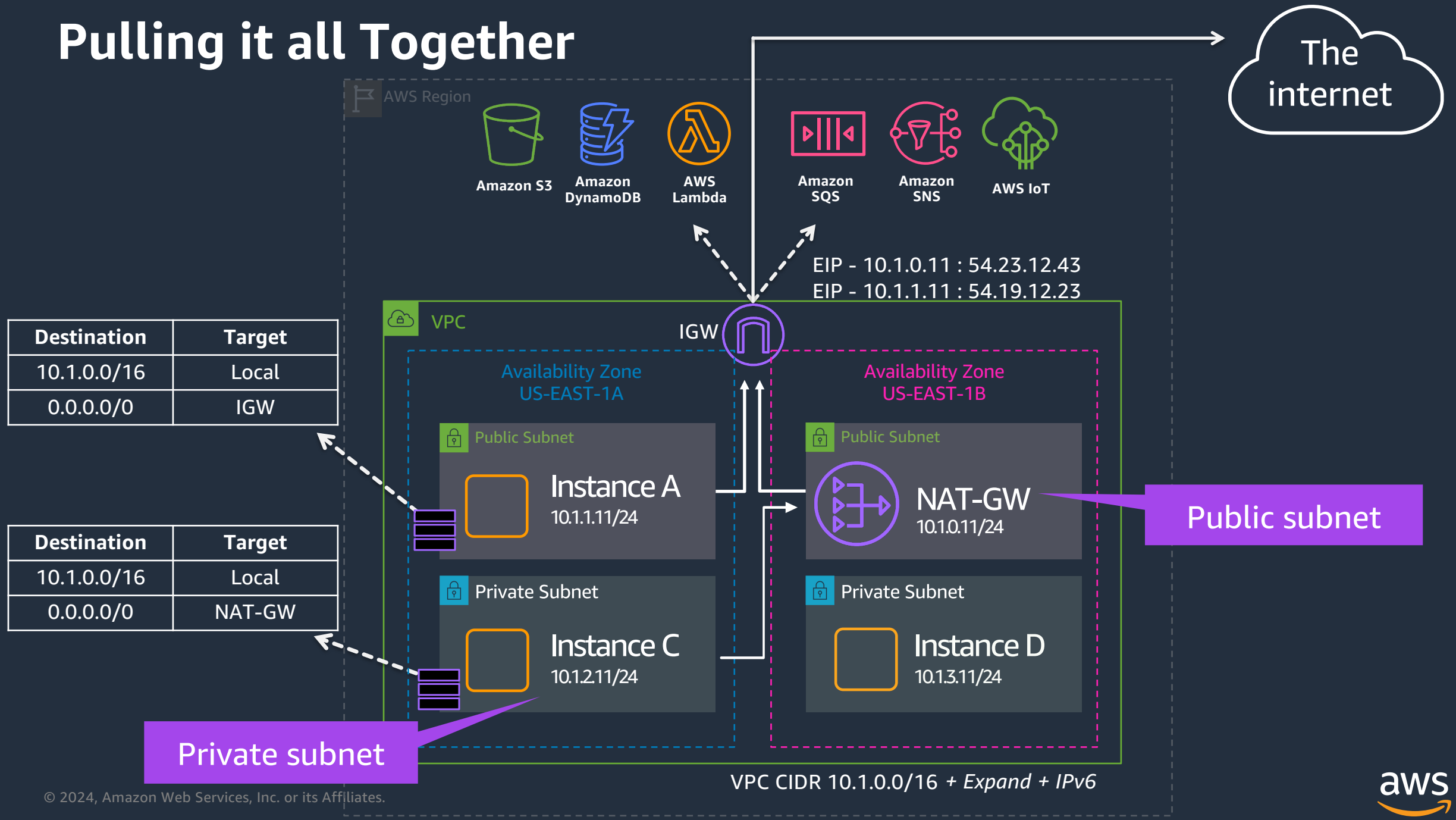
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	nat-09[redacted]	Active	No

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09e[redacted]	Active	No
::/0	igw-09e[redacted]	Active	No

- The Route Table for the Private Subnet says to send all IPv4 Internet Traffic to the NAT Gateway.
- The NAT Gateway translates all traffic it receives such that it appears to come from itself.
- The Route Table for the Public Subnet says to send all Internet Traffic to the Internet Gateway.

aws

Pulling it all Together



Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW

Public subnet

Private subnet

IP Address Management

IP Address Management

- IPAM makes it easier to plan, track, and monitor IPv4 and IPv6 addresses across AWS accounts and AWS Regions

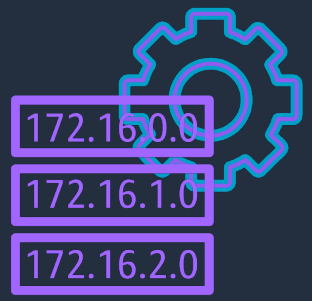
- Use Cases:
  - Automate IP address assignments
  - Monitor across network
  - Retrospective analysis
  - Manage BYOIP

aws

Setting up IPAM

Create IPAM

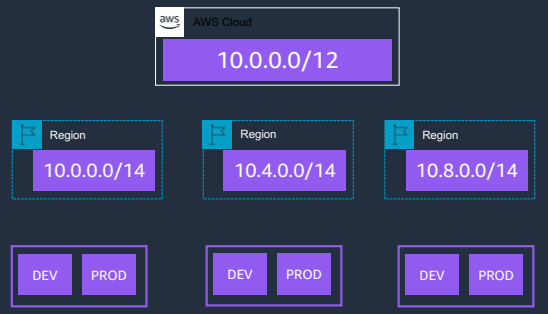
single IPAM to manage IPs across Regions and accounts



IPAM provides you the flexibility to host it in any Region

(typically choose the Region where most of your workloads reside)

Arrange IPs based on routing and security needs



An example for organizing IPs

Set business rules for allocation

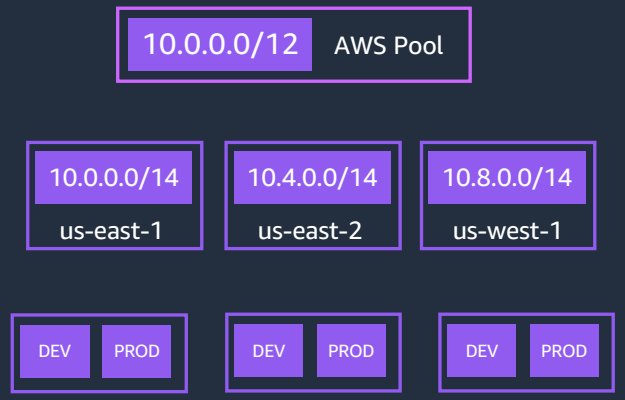
Few examples:

- Which account can use IPs
- Regions where IPs can be used

Examples For Organizing IP Addresses

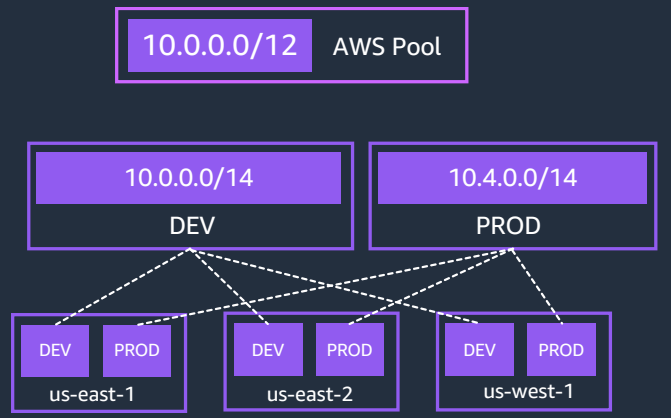
Example1

Pools for easy aggregation per region



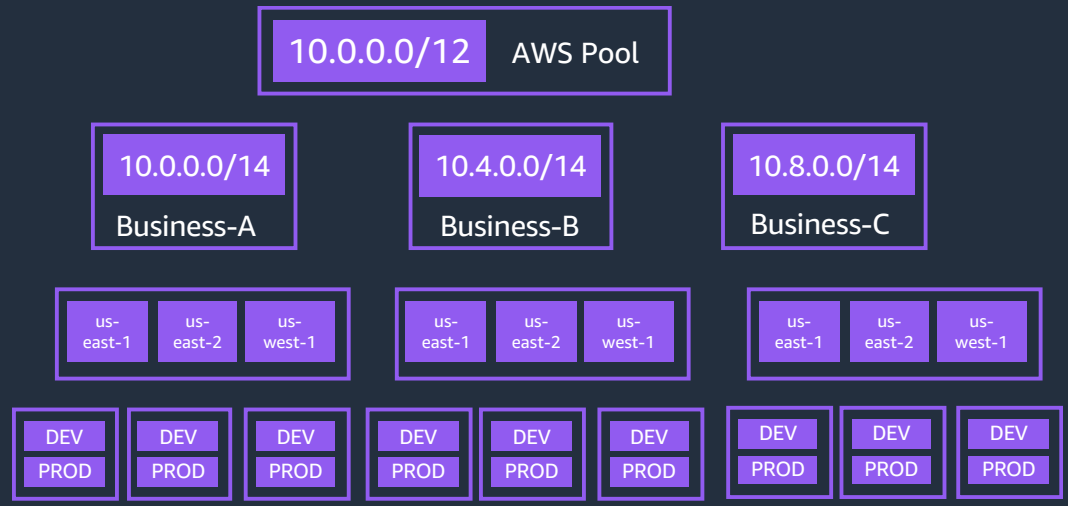
Example2

Pools for easy aggregation per workload type (DEV and PROD)



Example3

Pools for easy aggregation per line of business

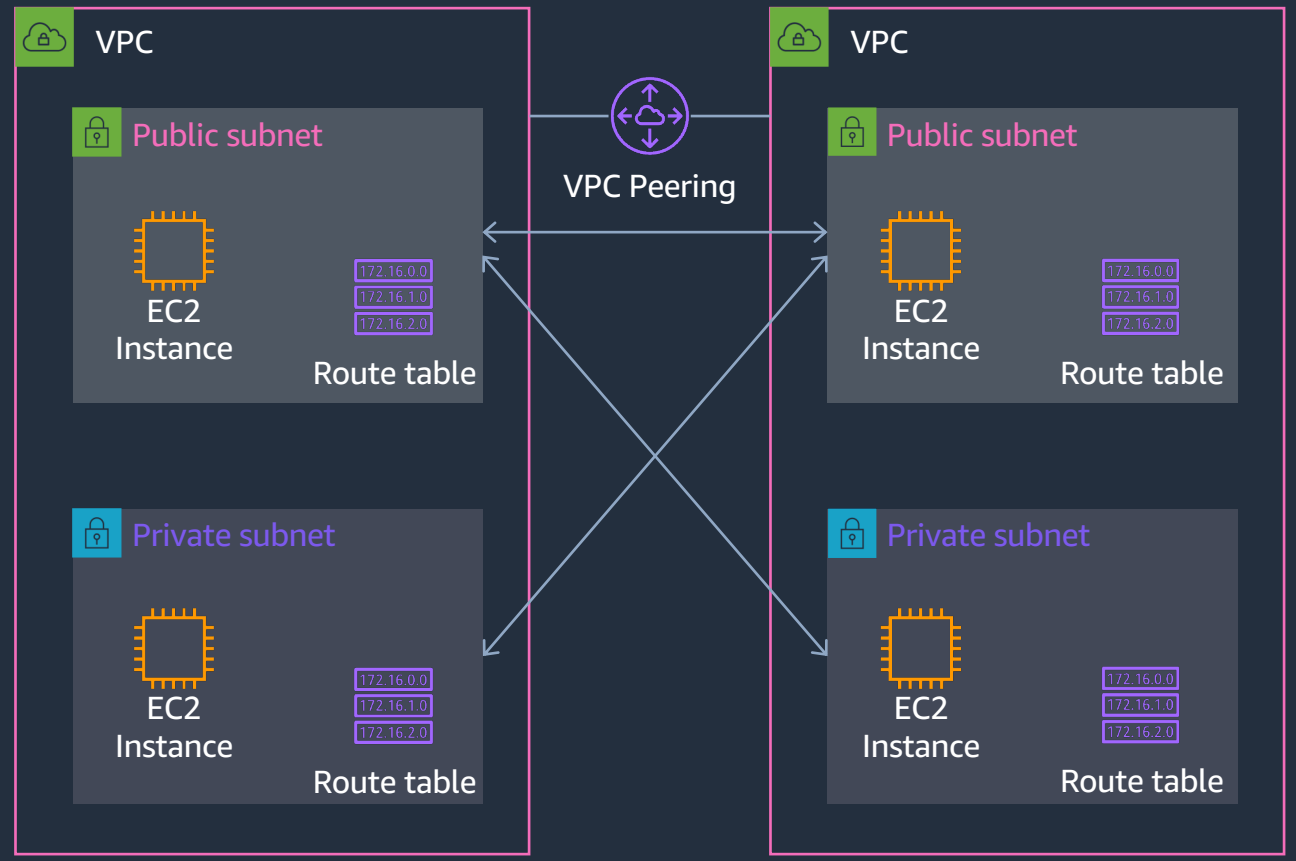


aws

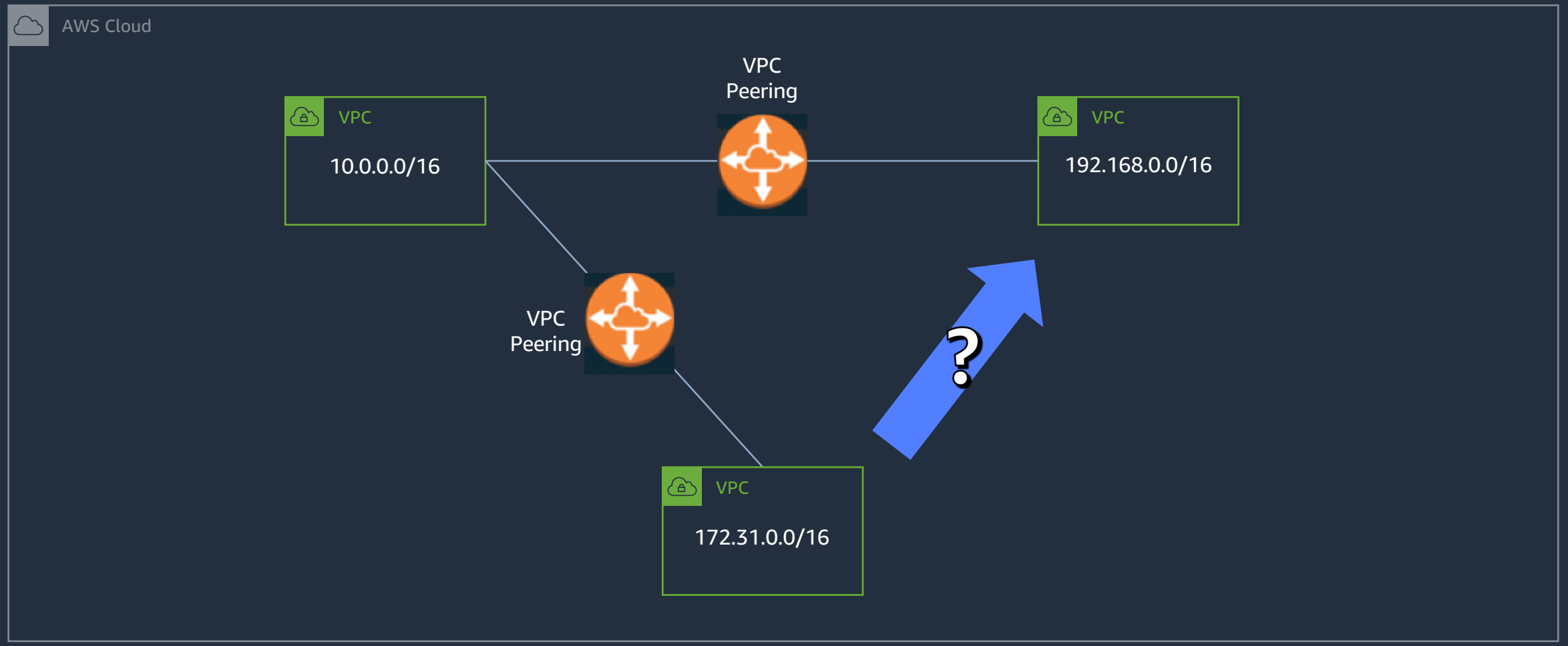
VPC Connectivity Option

Connect multiple VPCs: VPC Peering

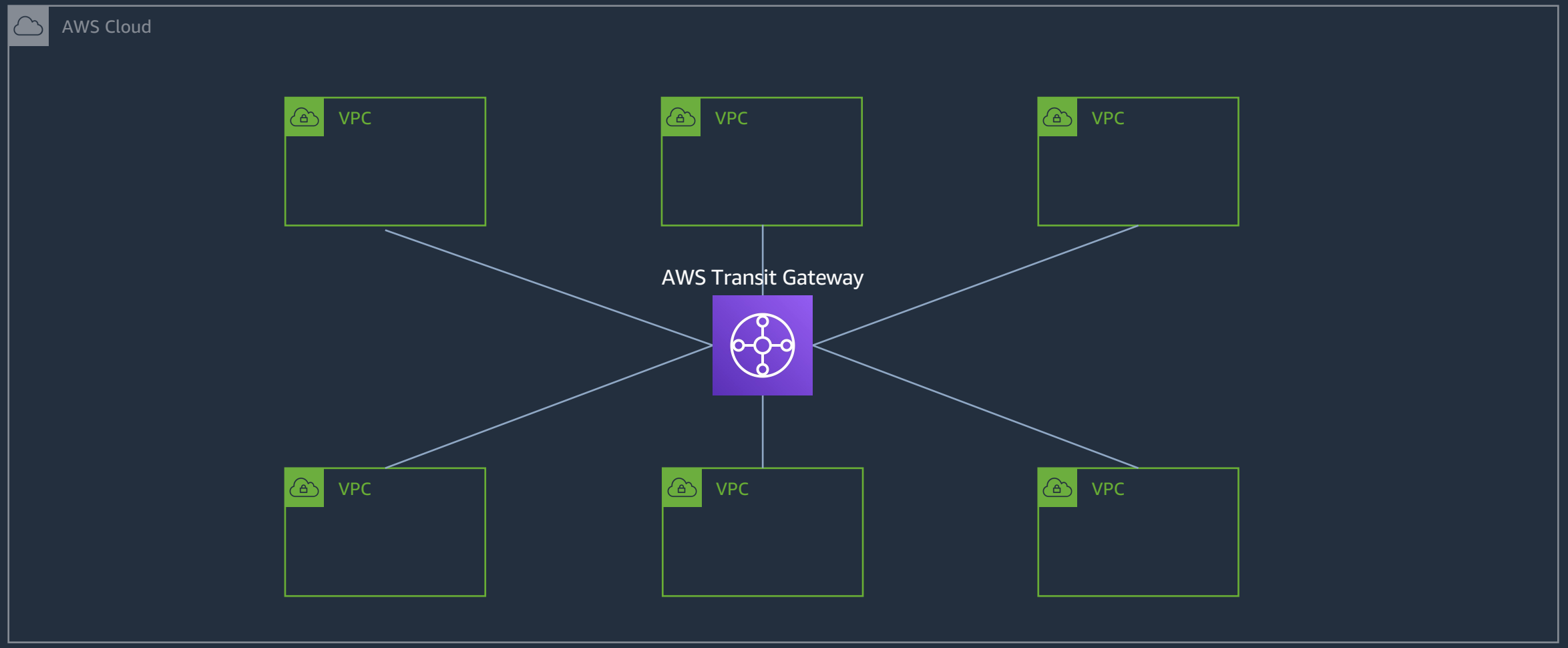
- Scalable and high available
- Supported between AWS accounts
- Supported across AWS Regions
- Bi-directional traffic
- Remote Security groups can be referenced
- Routing policy with Route Tables
  - Not all subnets need to connect to each other
- No overlapping IP addresses
- No transitive routing



Connect multiple VPCs: VPC Peering

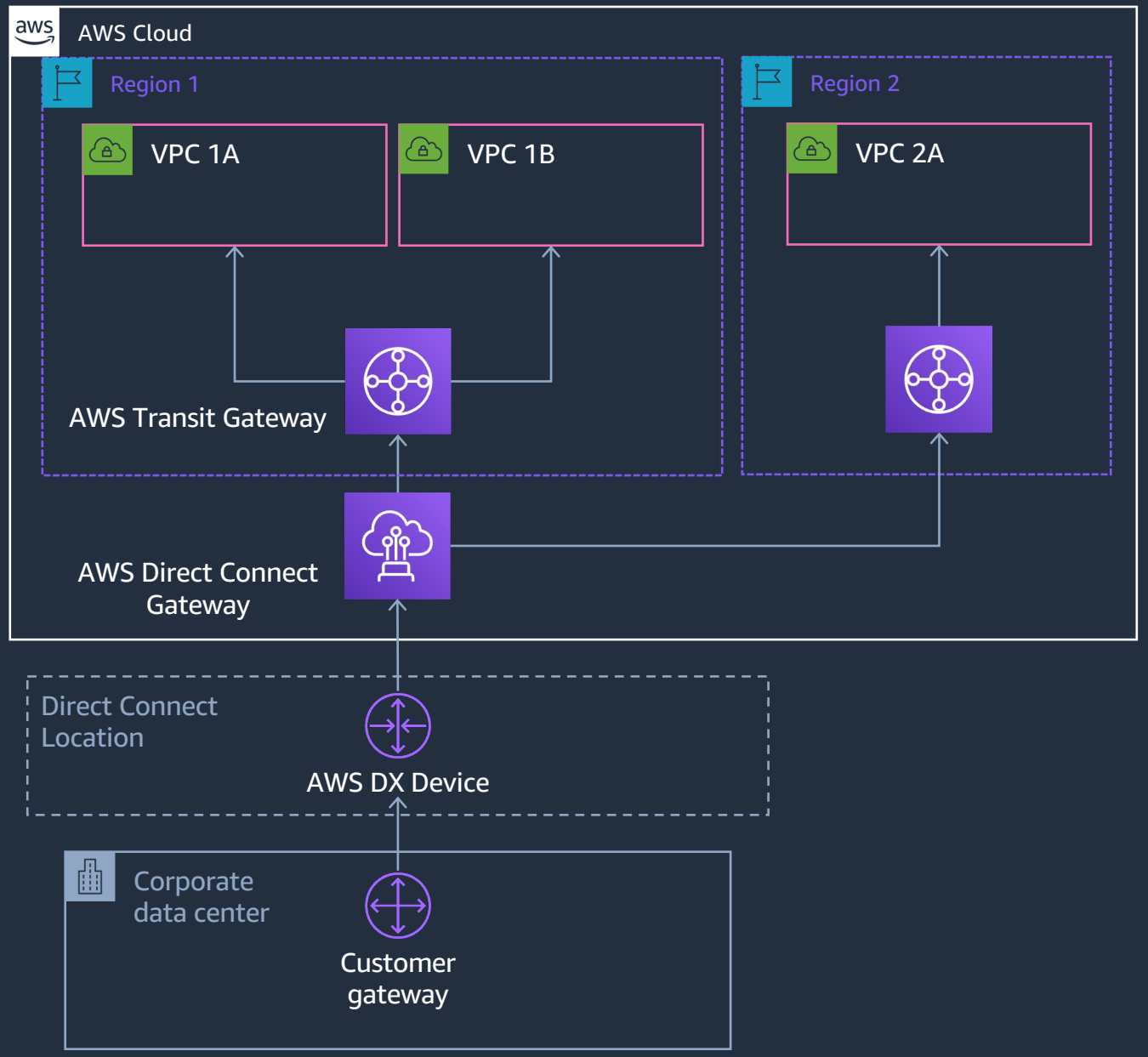


Multiple VPCs access models – AWS Transit Gateway



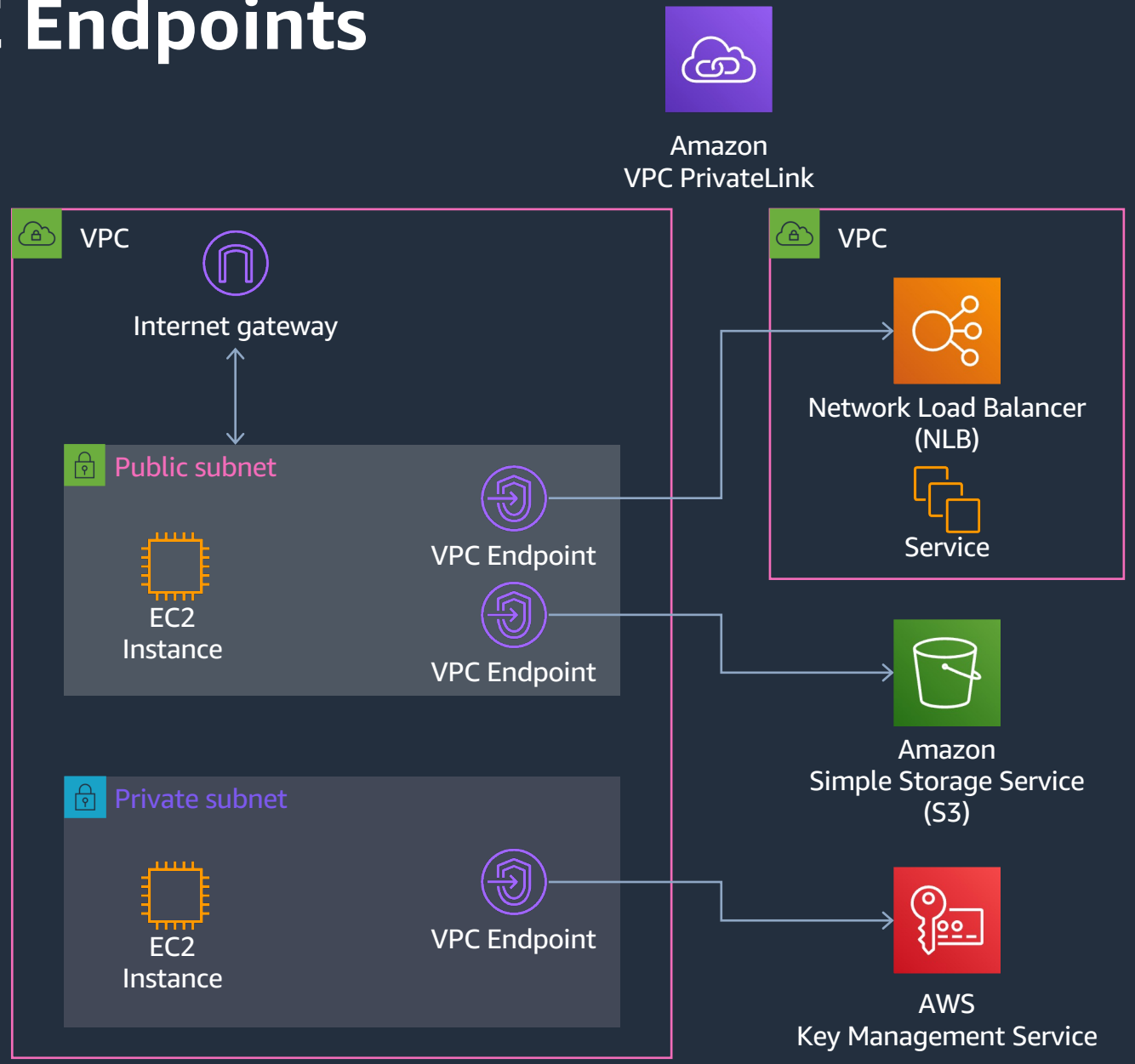
Connect at global scale: DX Gateway + Transit Gateway

- Transit VIF
  - Connects to a AWS Transit Gateway
- Simplify your network architecture and management overhead
- Create a hub-and-spoke model that spans multiple
  - VPCs
  - Regions
  - AWS accounts



Stay on AWS network: VPC Endpoints

- Connect your VPC to:
  - Supported AWS services
  - VPC endpoint services powered by PrivateLink
- Doesn't require public IPs or Internet connectivity
- Horizontally scaled, redundant, and highly available
- Robust access control
- Metrics for traffic visibility

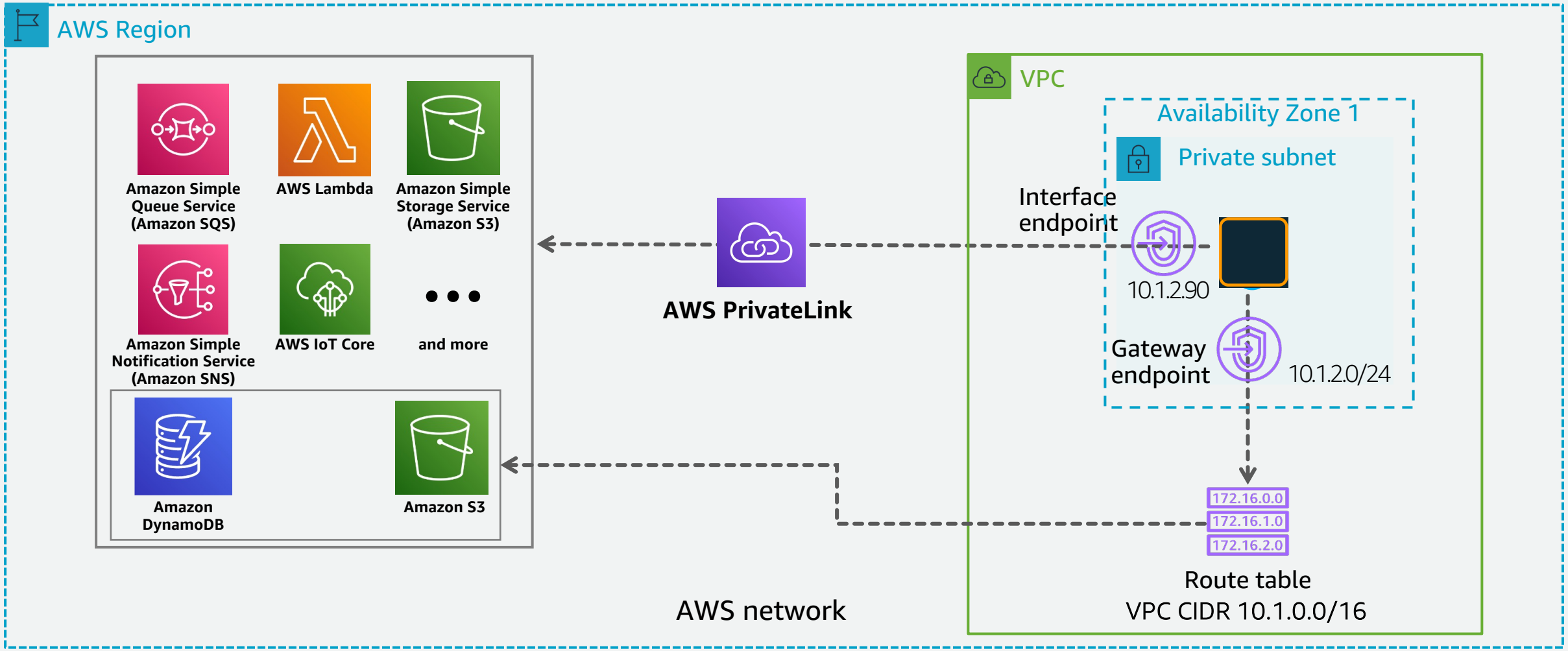


VPC Endpoint

Concepts

- VPC endpoint enables you to privately connect your VPC to supported AWS services.
- Instances in your VPC do not require public IP addresses to communicate with resources in the service.
- Traffic between your VPC and the other service does not leave the Amazon network.
- Two types of VPC Endpoints:
  - *Gateway Endpoints*
  - *Interface Endpoints*

Concepts

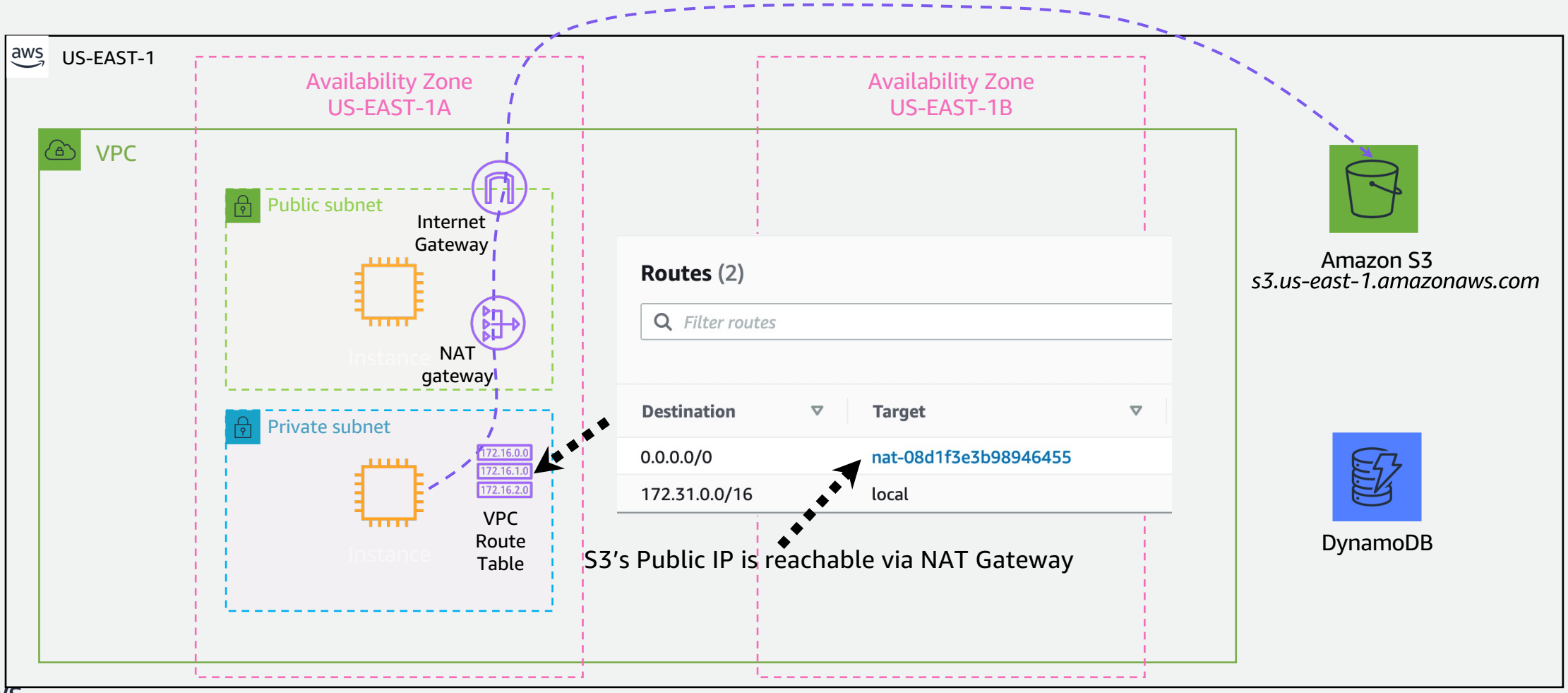


Gateway Endpoint

Gateway Endpoints

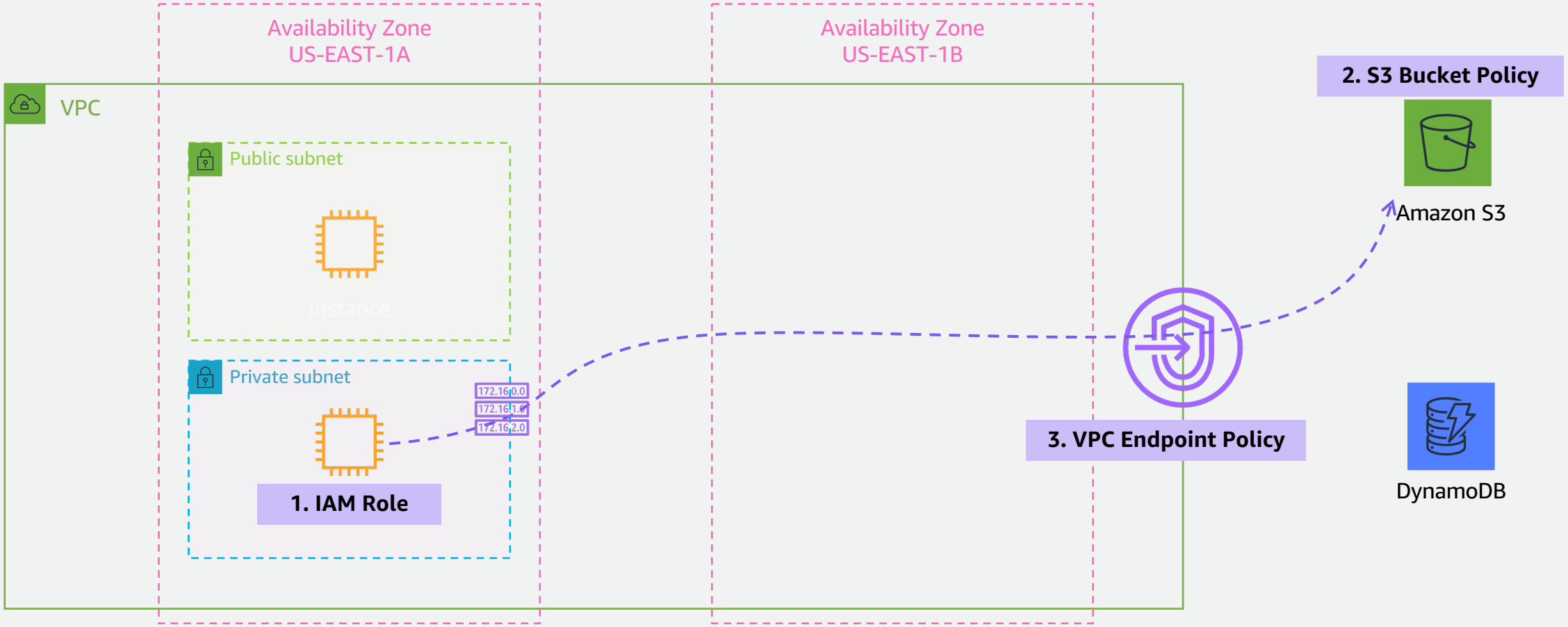
- Target for traffic destined to a supported AWS service
- Requires VPC route table entry with VPC endpoint being the next-hop
- Service prefix list is the destination CIDR
- Supported Services:
  - Amazon S3
  - DynamoDB

Accessing S3 and DynamoDB Without VPC Gateway Endpoint



Accessing S3 via Gateway VPC Endpoints

Access controls



S3 Bucket Policy

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909152",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPCE-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpce": "vpce-1a2b3c4d"
         }
       }
     }
   ]
}
```

VPC Endpoint Policy Example

RESTRICTING ACCESS TO A SPECIFIC BUCKET

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"]
    }
  ]
}
```

Considerations

- A gateway endpoint is **available only** in the **Region where you created it**. Be sure to create your gateway endpoint in the same Region as your S3 buckets.
- Should be enabled both DNS hostnames and DNS resolution for your VPC.
- Endpoint connections cannot be extended out of a VPC.
- Default quota of **20 gateway endpoints per Region**. [Amazon VPC Quota]

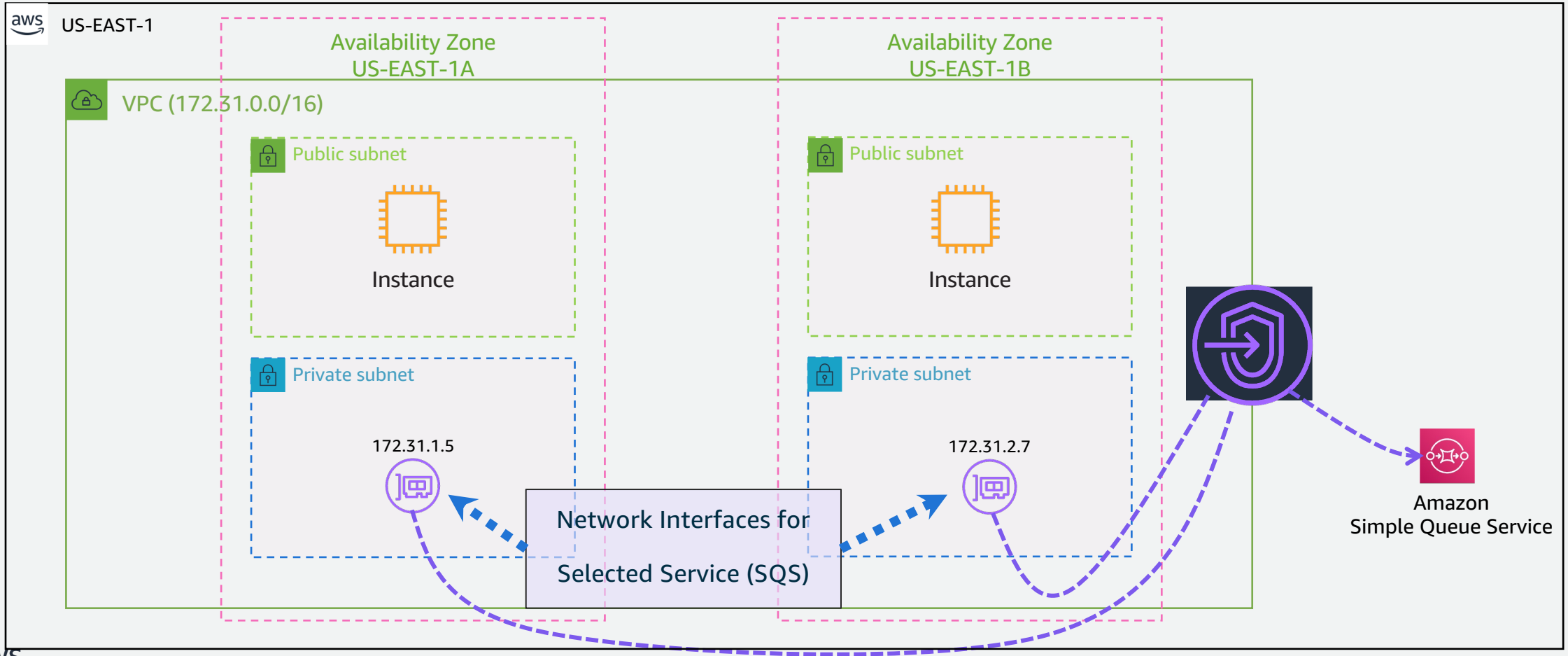
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html#gateway-endpoint-considerations-s3

Interface Endpoint

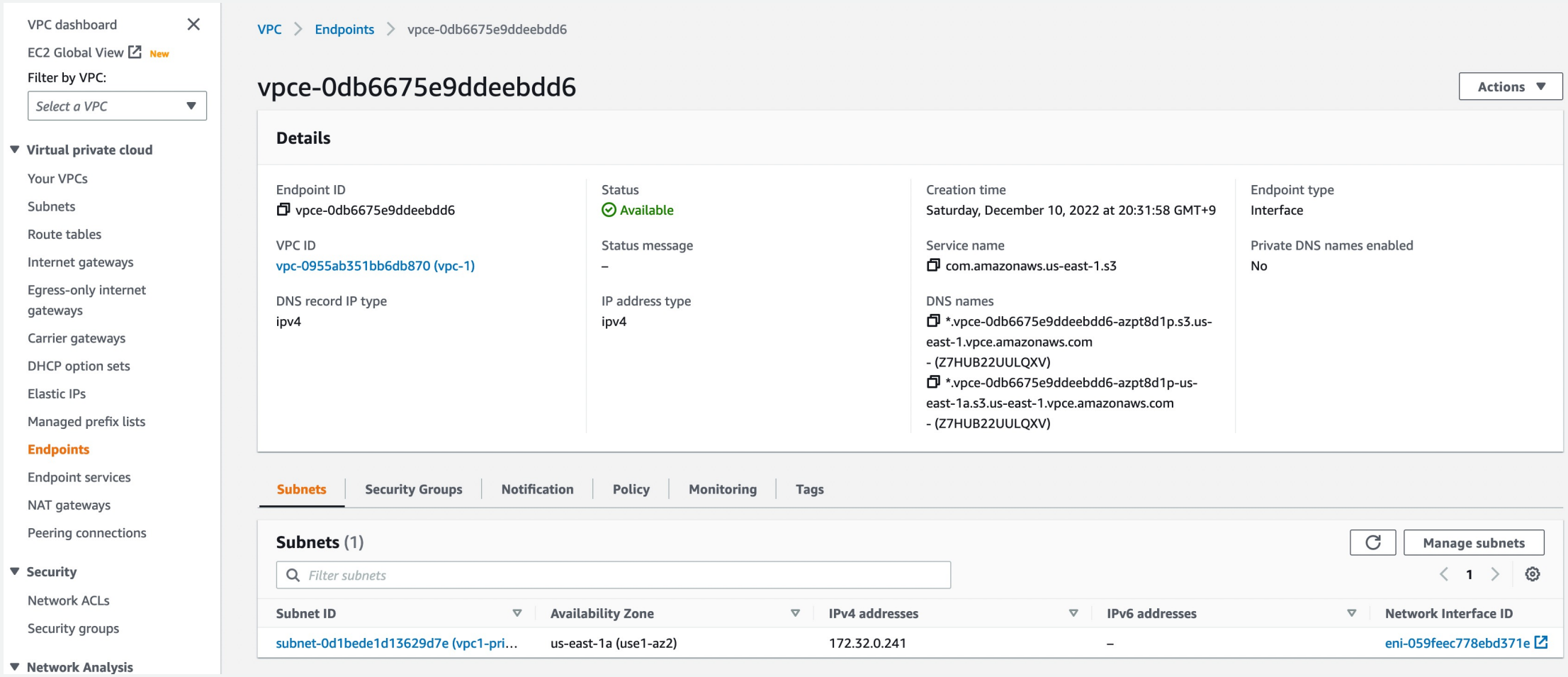
Interface Endpoints

- **Elastic network interface (ENI)** with a private IP address is deployed in your subnet.
- **Multiple services are supported:**
  - S3 (Supports both Gateway & Interface endpoints)
  - Amazon API Gateway
  - Amazon AppStream 2.0
  - AWS App Mesh
  - Amazon Athena
  - etc…

Accessing SQS With Interface Endpoint



Interface Endpoint



Interface Endpoint

```
 ~/ [main] nslookup s3.vpce-0db6675e9ddeebdd6-azpt8d1p.s3.us-east-1.vpce.amazonaws.com
Server:         210.220.163.82
Address:        210.220.163.82#53

Non-authoritative answer:
Name:   s3.vpce-0db6675e9ddeebdd6-azpt8d1p.s3.us-east-1.vpce.amazonaws.com
Address: 172.32.0.241

 ~/ [main]
```

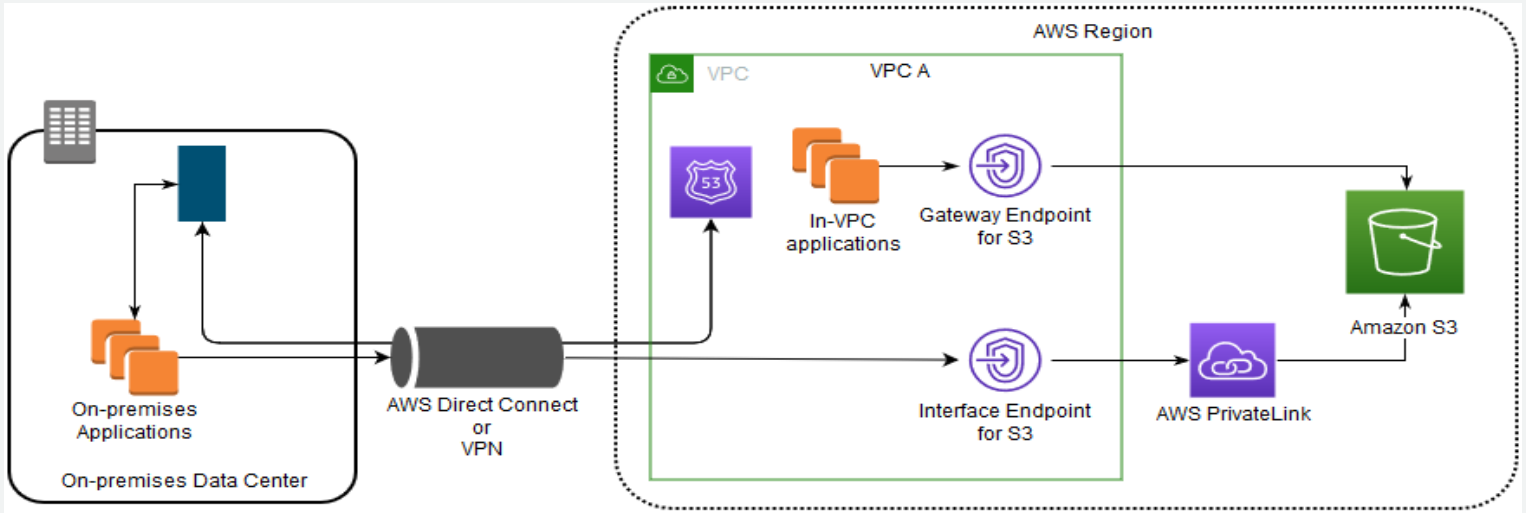
https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html

Considerations

- **Each interface endpoint** can support a bandwidth of **up to 10 Gbps per Availability Zone** and **automatically scales** up to 100 Gbps.
- AWS services accept connection requests automatically. The service can't initiate requests to resources in your VPC through the VPC endpoint. The endpoint only returns responses to traffic that was initiated by resources in your VPC.
- **The security group** for the interface endpoint **must allow communication between the endpoint network interface and the resources in your VPC** that must communicate with the service

  https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

AWS VPC S3 Endpoints – Gateway vs Interface

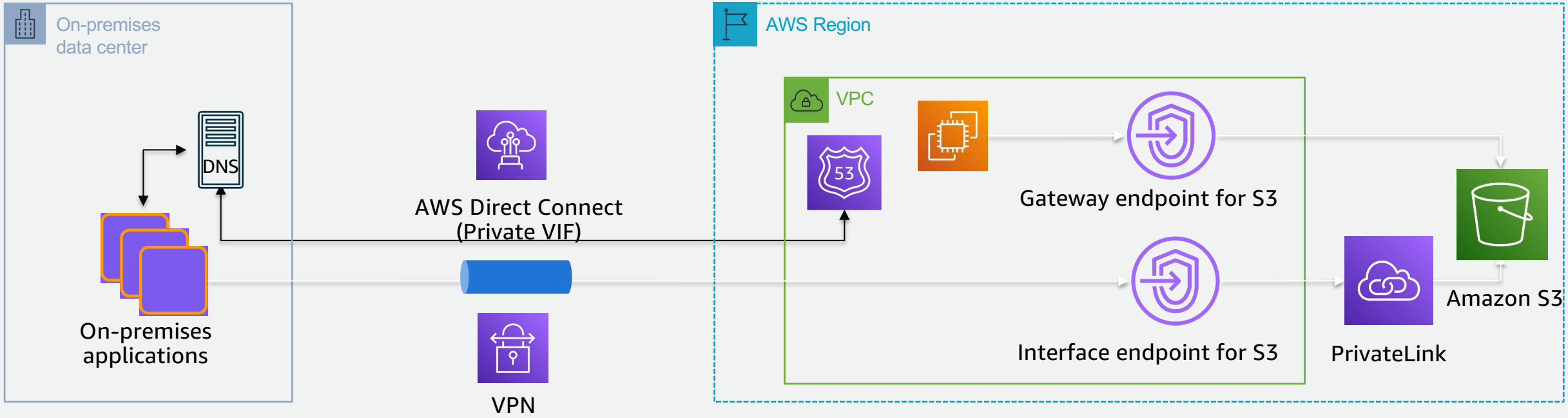


구분	Gateway endpoints	Interface endpoints
보안성	your network traffic remains on the AWS network.	
S3 IP address	Use Amazon S3 public IP addresses	Use private IP addresses from your VPC
접근성	접근불가(on premises , Another Region)	접근가능
Charge	Not billed	Billed

https://docs.aws.amazon.com/vpc/latest/privatelink/integrated-services-vpce-list.html
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/privatelink-interface-endpoints.html

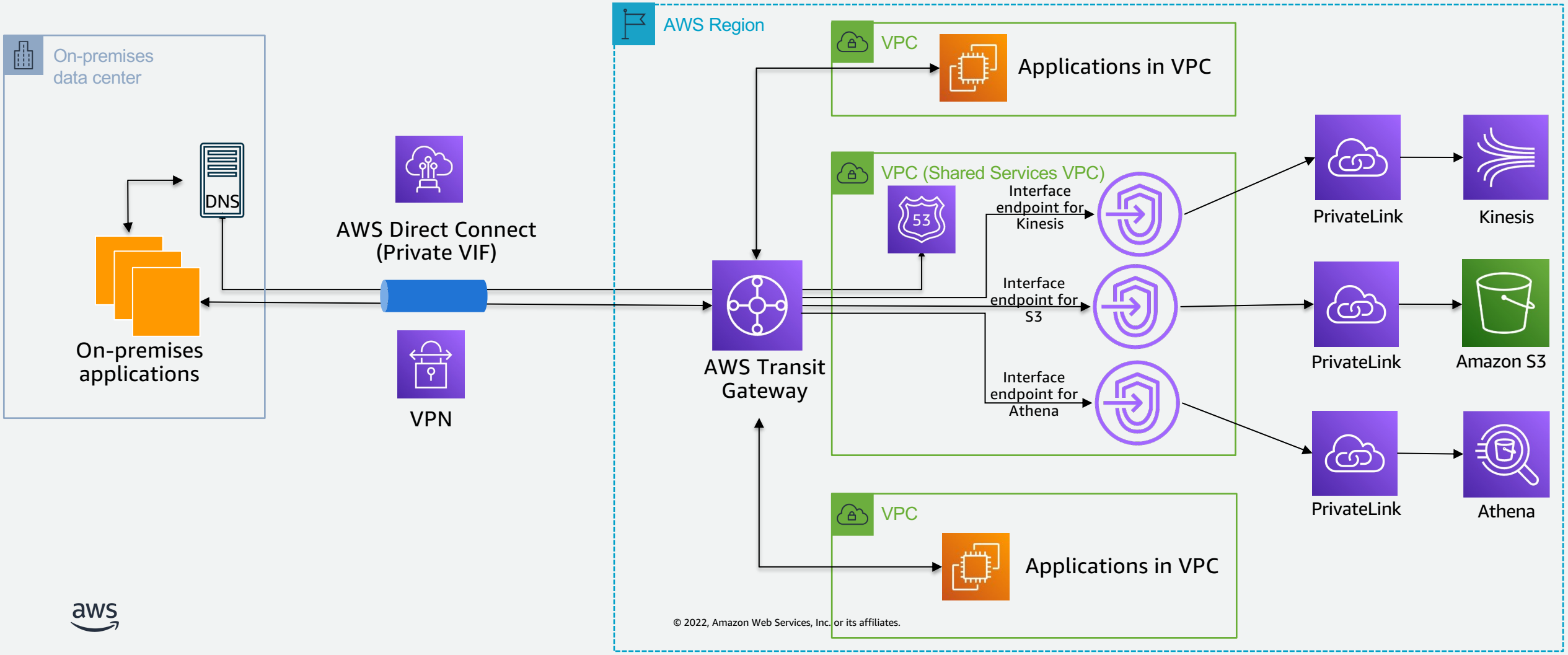
Use Case

S3 Access in a Hybrid Environment

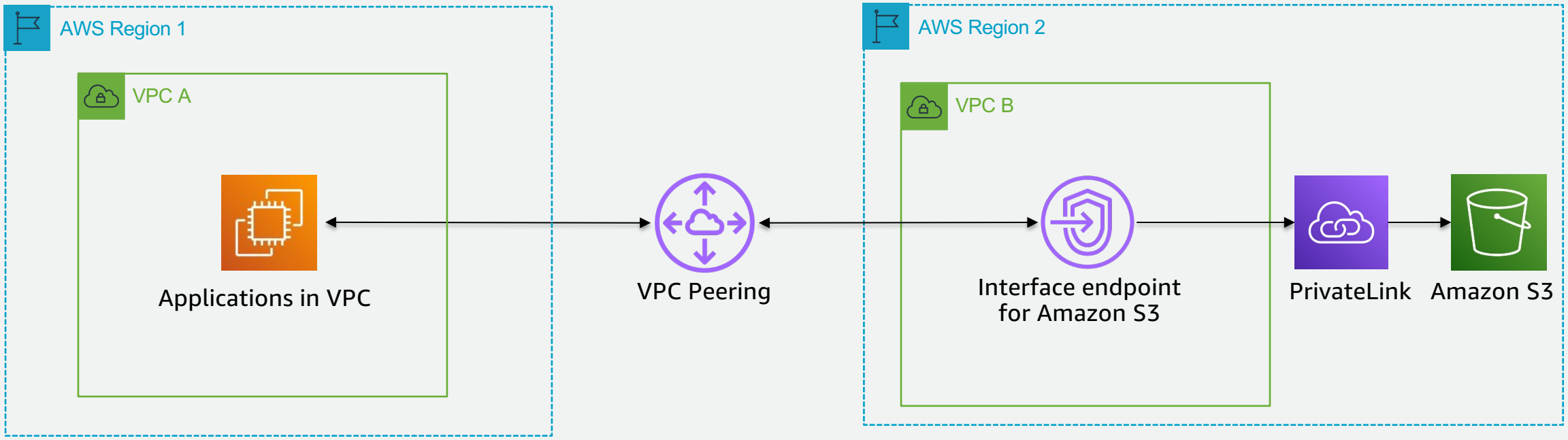


On-premises applications access S3 through the interface endpoint, apps in the VPC access S3 through the gateway endpoint

Centralized Access with a Shared Services VPC



S3 Access from Apps in a Different Region



Access S3 from apps in a different AWS region using interface endpoints for S3

Further Reading

- Choosing Your VPC Endpoint Strategy for Amazon S3 - Blog

실습

설정

- ✓ Private Subnet 에 EC2 Instance (Amazon Linux) 생성
  - ✓ No public IP assigned
  - ✓ No key pair
- ✓ Role 생성 후 EC2 연결 (SSM / S3)
- ✓ VPC Endpoint 설정
  - ✓ ssm / ssmmessage / ec2messages
- ✓ VPC Endpoint Policy **(Option)**
  - ✓ 여러 S3 bucket 중 생성한 VPC Endpoint 에서는 특정 S3 Bucket 만 접근할 수 있도록 적용

참고. 인터넷 접근 없는 Private 환경의 EC2 원격 접속 설정 방법

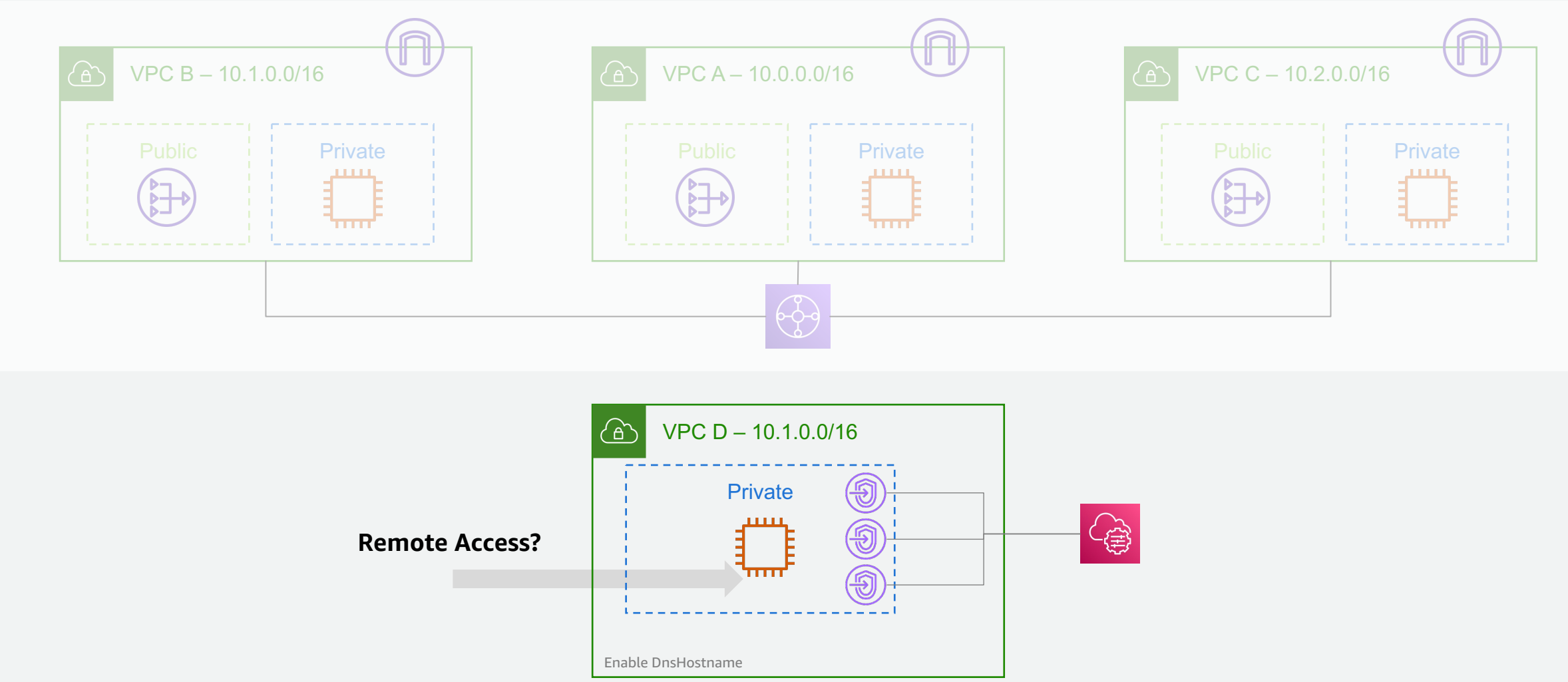
- ✓ VPC Endpoint 생성
  - ✓ com.amazonaaws.[region].**ssm / ec2messages / ssmmessages**
  - ✓ endpoint 가 사용할 Security Group 은 inbound HTTPS (port 443) 허용하도록 설정 (Source : VPC CIDR)
- ✓ 인스턴스 내 SSM Agent 설치
- ✓ Systems Manager 사용을 위한 Role 생성 (AmazonSSMManagedInstanceCore)
- ✓ EC2 에 생성한 Role 연결 (EC2 에 설정된 Security Group 는 inbound traffic 설정 필요 없음)

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-systems-manager-vpc-endpoints/?nc1=h_ls

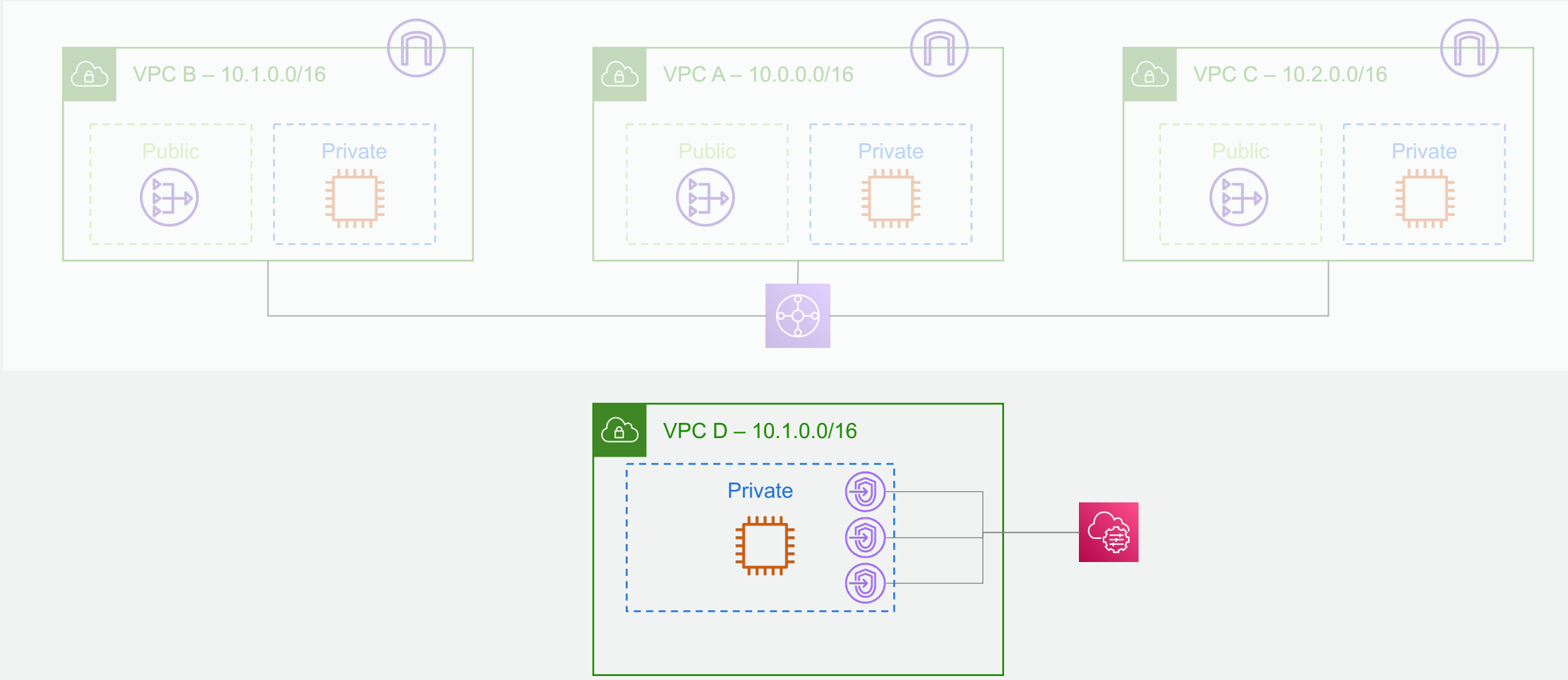
검증

- ✓ Laptop 에서 Systems manager (SSM) 을 활용하여 EC2 접속
- ✓ EC2 에서 정상적으로 S3 bucket 생성 또는 조회 확인
- ✓ VPC Policy 가 예상한 대로 정상 동작 하는지 확인

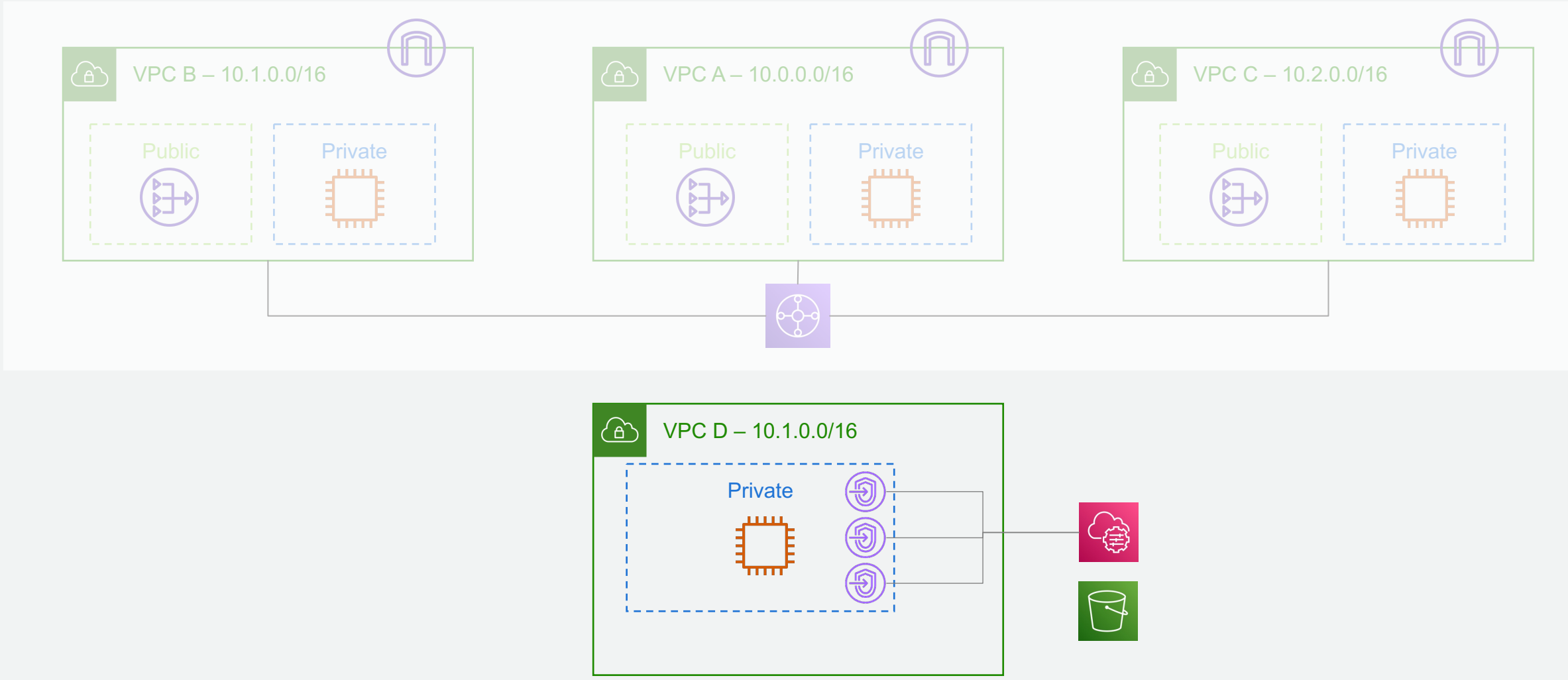
Step 1. Creating VPC without Internet-Access



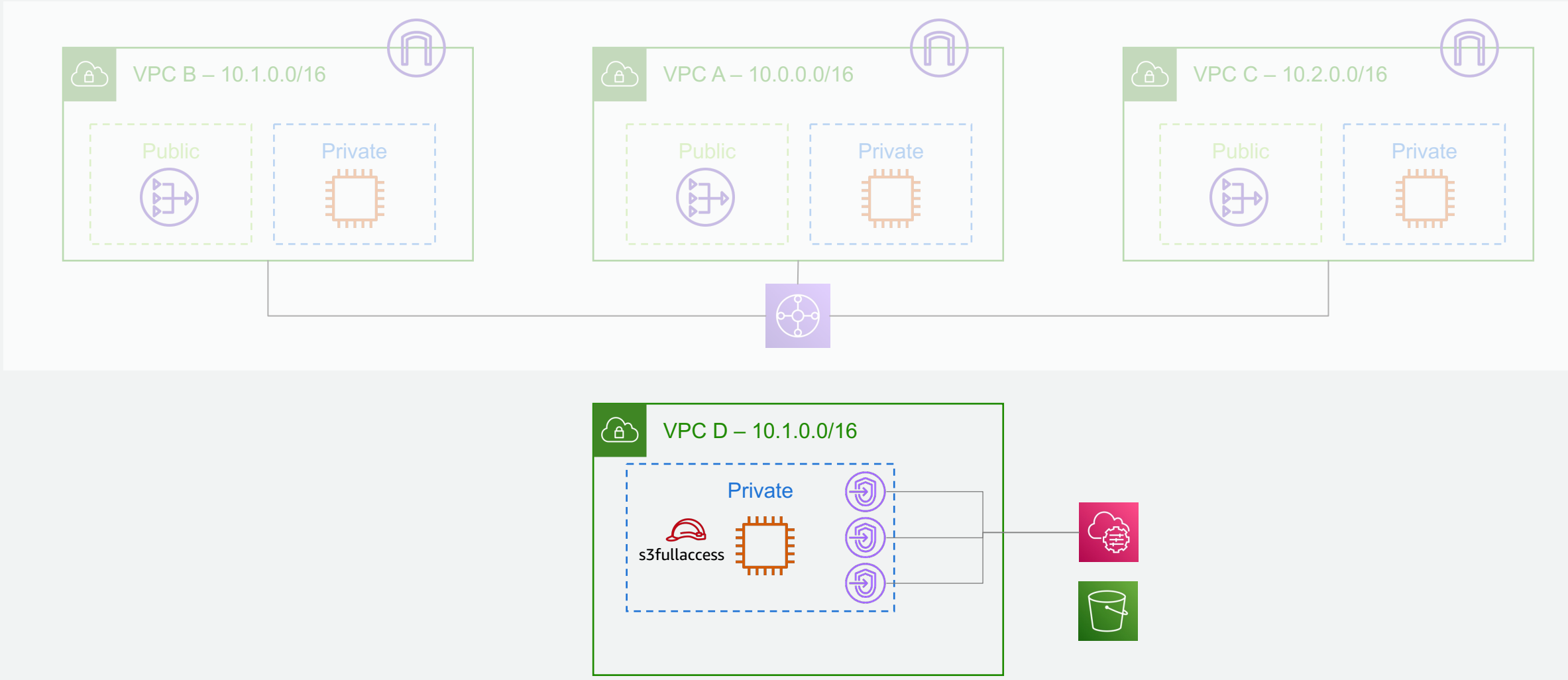
Step 2. Create VPC Endpoints



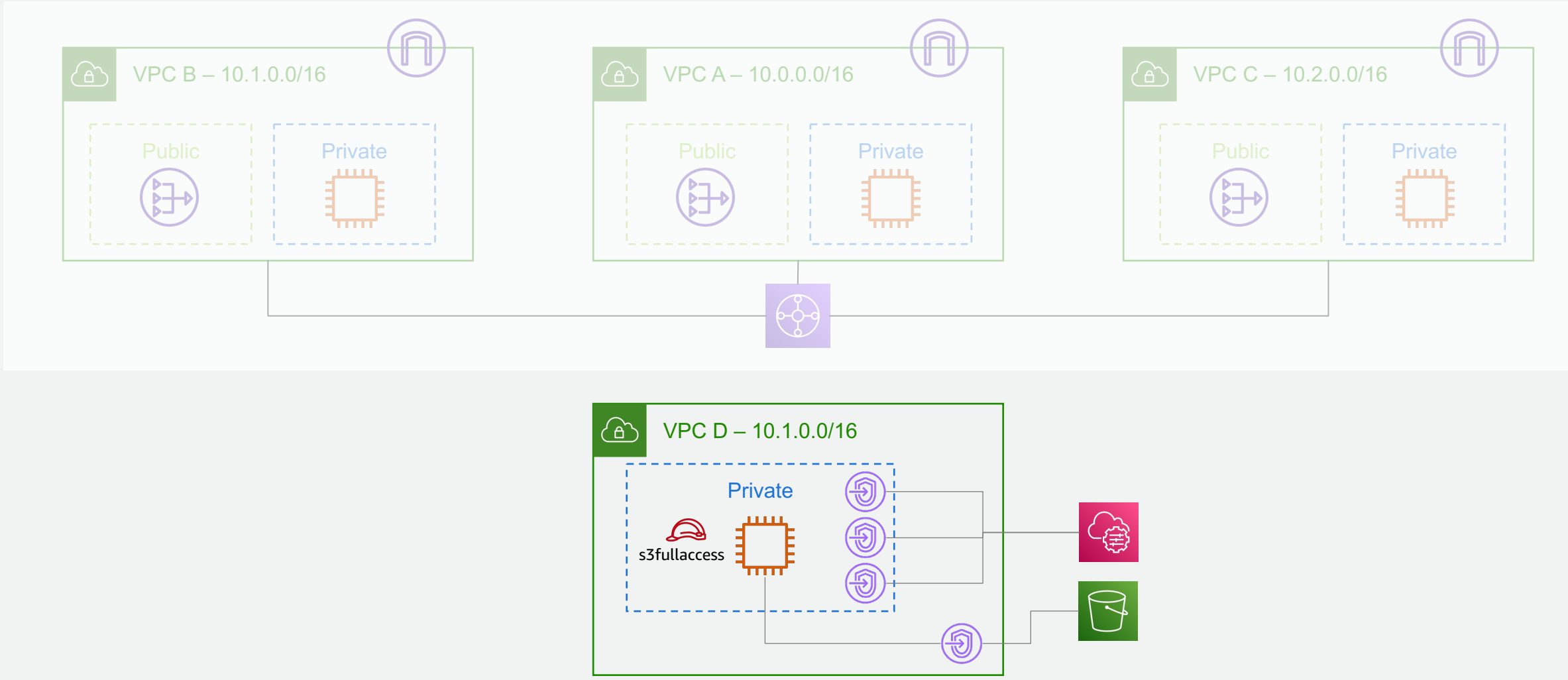
Step 3. Create S3 Bucket



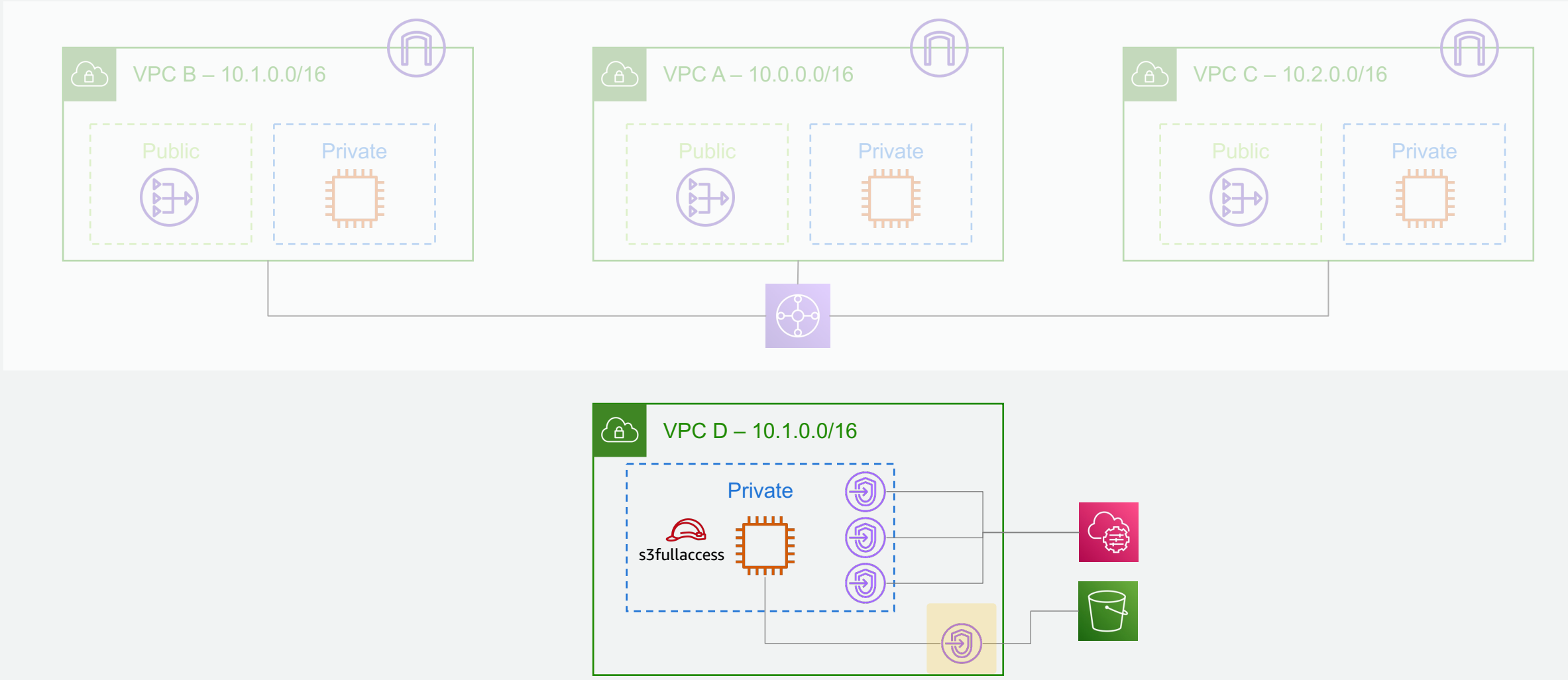
Step 4. Configure IAM Role to access S3



Step 5. Configure VPC Endpoint for S3



Step 6. Configure VPC Endpoint Policy



참고. VPC Endpoint Policy Example

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"]
    }
  ]
}
```

Thank you!