AWS re:Invent

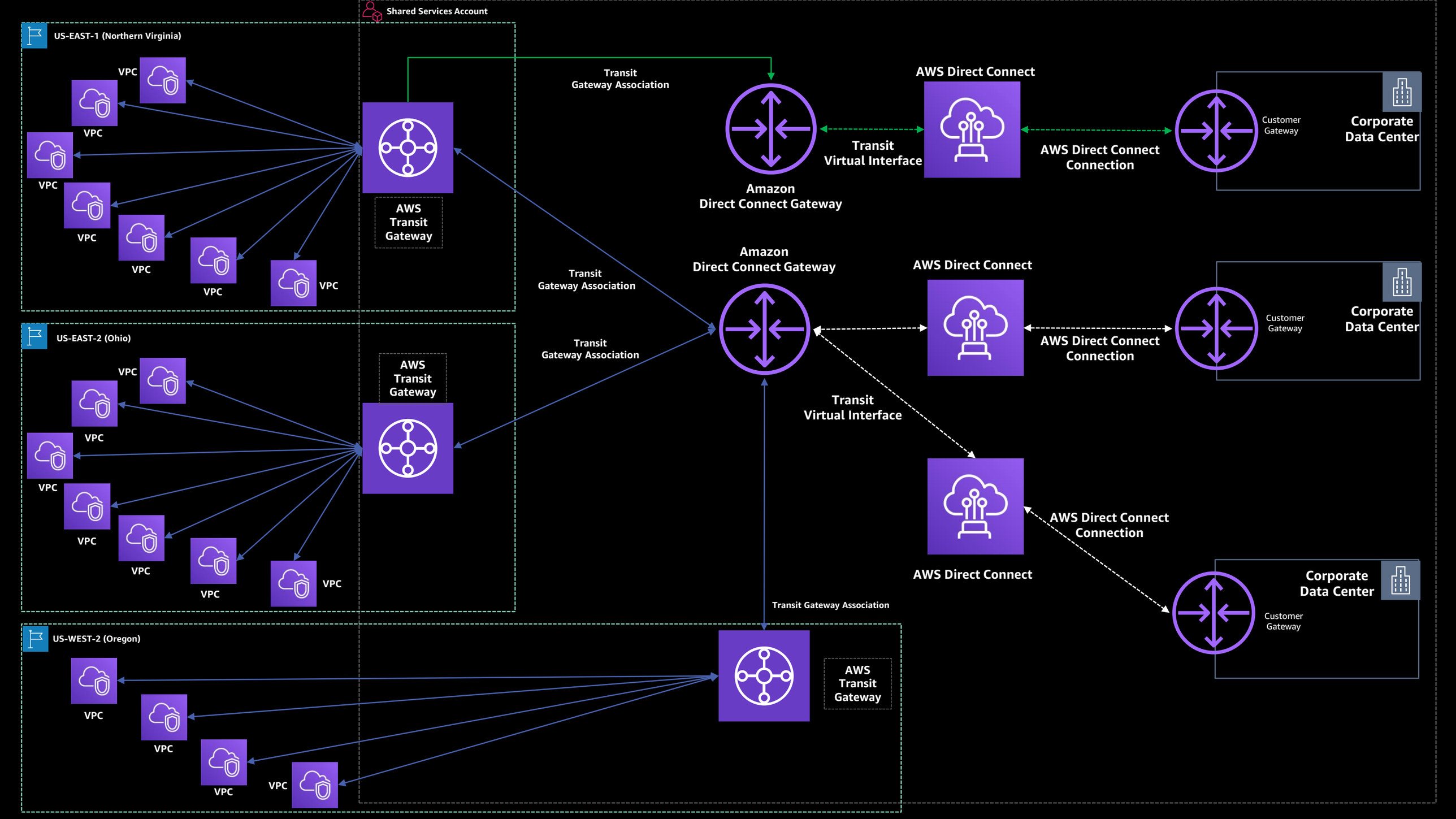
ARC304

From one to many: Evolving Amazon Virtual Private Cloud (VPC) design

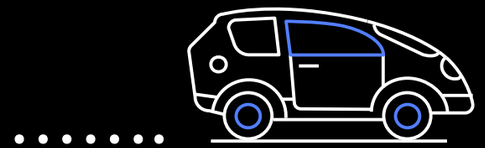
Androski Spicer
Solutions Architect
Amazon Web Services

"The beginning is the most important part of the work. ……**Plato**"

Networking Simplified


Shared Services Account
US-EAST-1 (Northern Virginia)
VPC
VPC
VPC
VPC
VPC
VPC
VPC
AWS
Transit
Gateway
Transit
Gateway Association
Amazon
Direct Connect Gateway
Transit
Virtual Interface
AWS Direct Connect
AWS Direct Connect
Connection
Customer
Gateway
Corporate
Data Center
US-EAST-2 (Ohio)
VPC
VPC
VPC
VPC
VPC
VPC
VPC
AWS
Transit
Gateway
Transit
Gateway Association
Amazon
Direct Connect Gateway
AWS Direct Connect
AWS Direct Connect
Connection
Customer
Gateway
Corporate
Data Center
Transit
Virtual Interface
AWS Direct Connect
AWS Direct Connect
Connection
AWS Direct Connect
Customer
Gateway
Corporate
Data Center
Transit Gateway Association
US-WEST-2 (Oregon)
VPC
VPC
VPC
VPC
AWS
Transit
Gateway

Let’s go on a journey,



Evolution of customers networking needs from PoC to going all in on AWS

ABC Company

IT Team

From one

The VPC as a single unit of networking

Evolving Design Requirements

Through the eyes of a multi-tiered web application migration

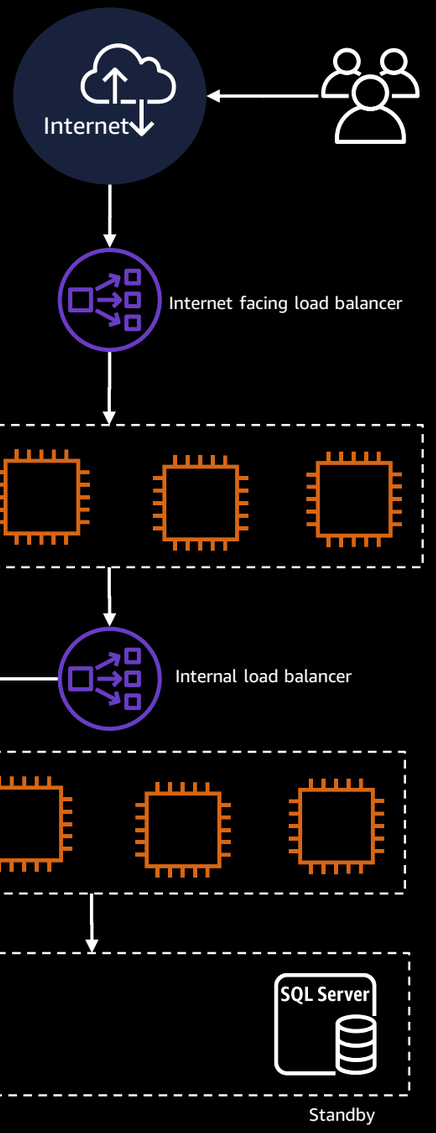
Requirement List 1: IP Space & Internet Access

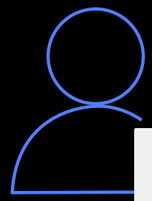
- ✓ One (1) - Internet facing load balancer
- ✓ Four (4) - Apache web servers front end)
- ✓ One (1) - Internal facing load balancer
- ✓ Four (4) - Application servers
- ✓ Multi-AZ Microsoft SQL server configuration

PoC components

- ❑ Private & public IPv4 space
- ❑ Design VPC for high availability
- ❑ Internet access for public and private IP space

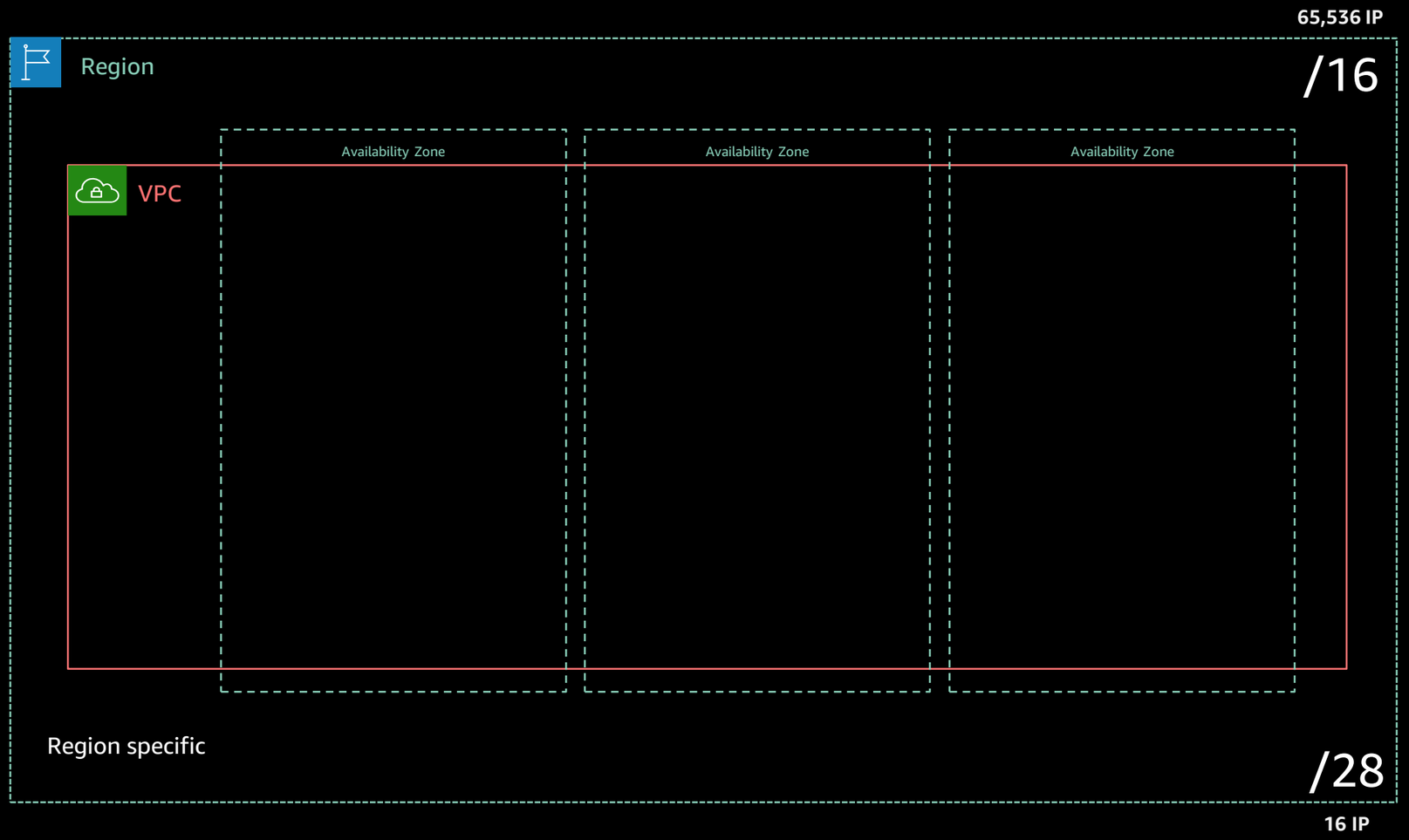
PoC requirements





Let’s take a quick look at the basics!

VPC: What is it ?



IPv6.

Optional

IPv4

Mandatory

Logically isolated segment of the AWS cloud

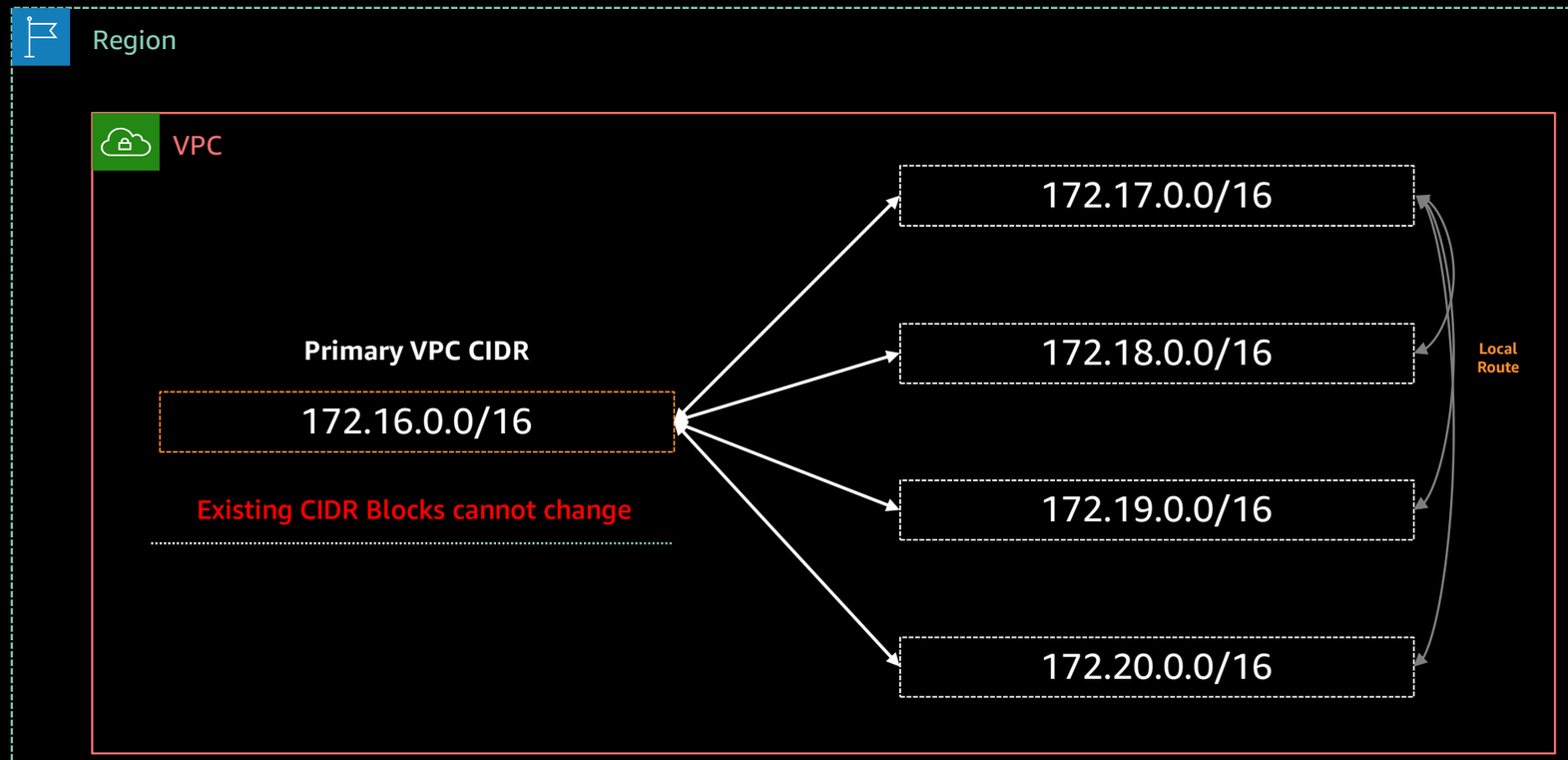
Design VPC for scale

Connectivity to on-premises resources

VPC purpose

*Default VPC limits per region = 5

VPC Resizing



Primary CIDR range dictates which other RFC1918 ranges can be used

For example, if you use 172.16.0.0/12, then your additional CIDRs must be from the RFC1918 range

Secondary CIDR blocks can be removed

Primary CIDR blocks cannot be changed

CIDR block/s cannot overlap

CIDR block must not be the same or larger than the CIDR range of a route in any of the VPC route tables

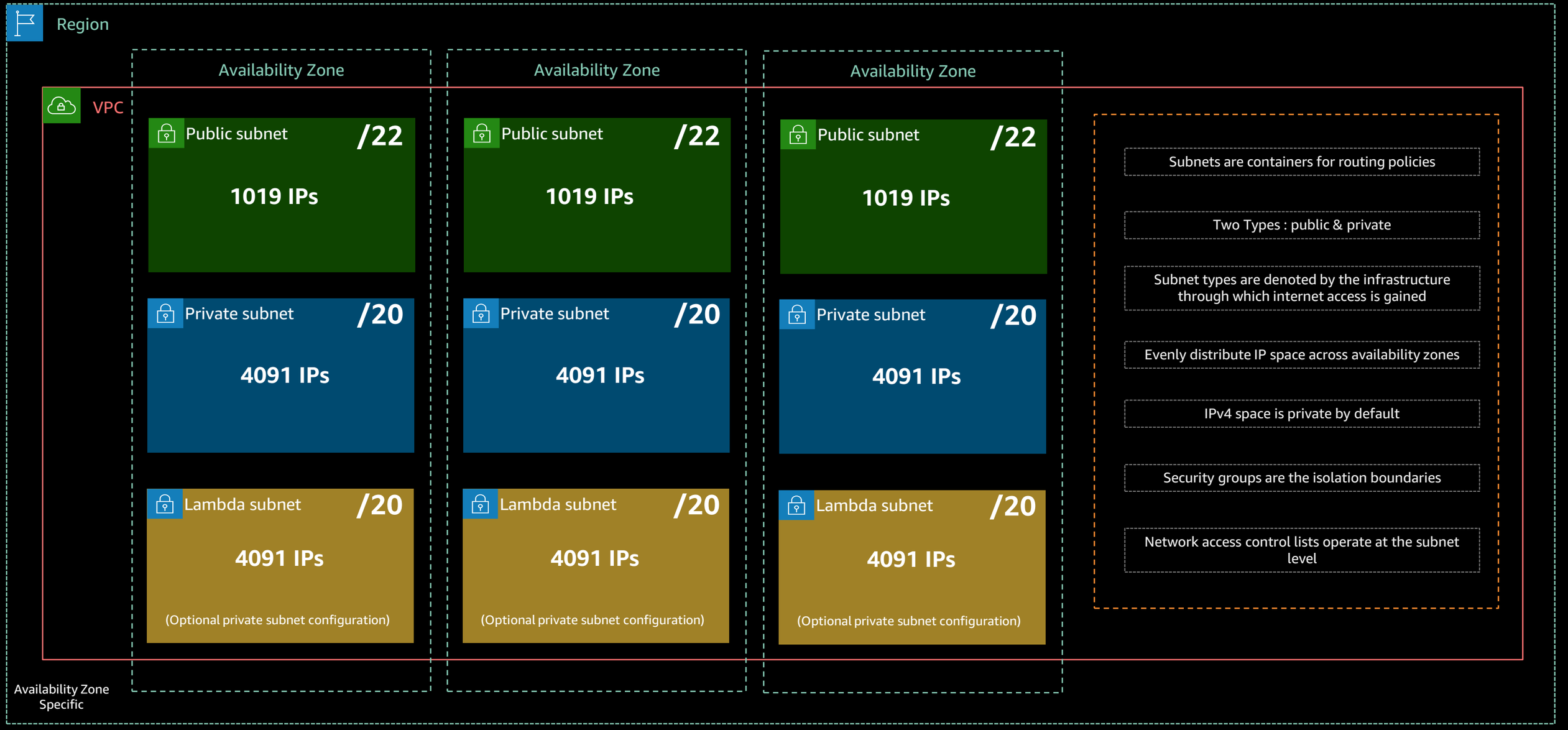
Region Specific

*Soft Limit of = 5 CIDR blocks per VPC

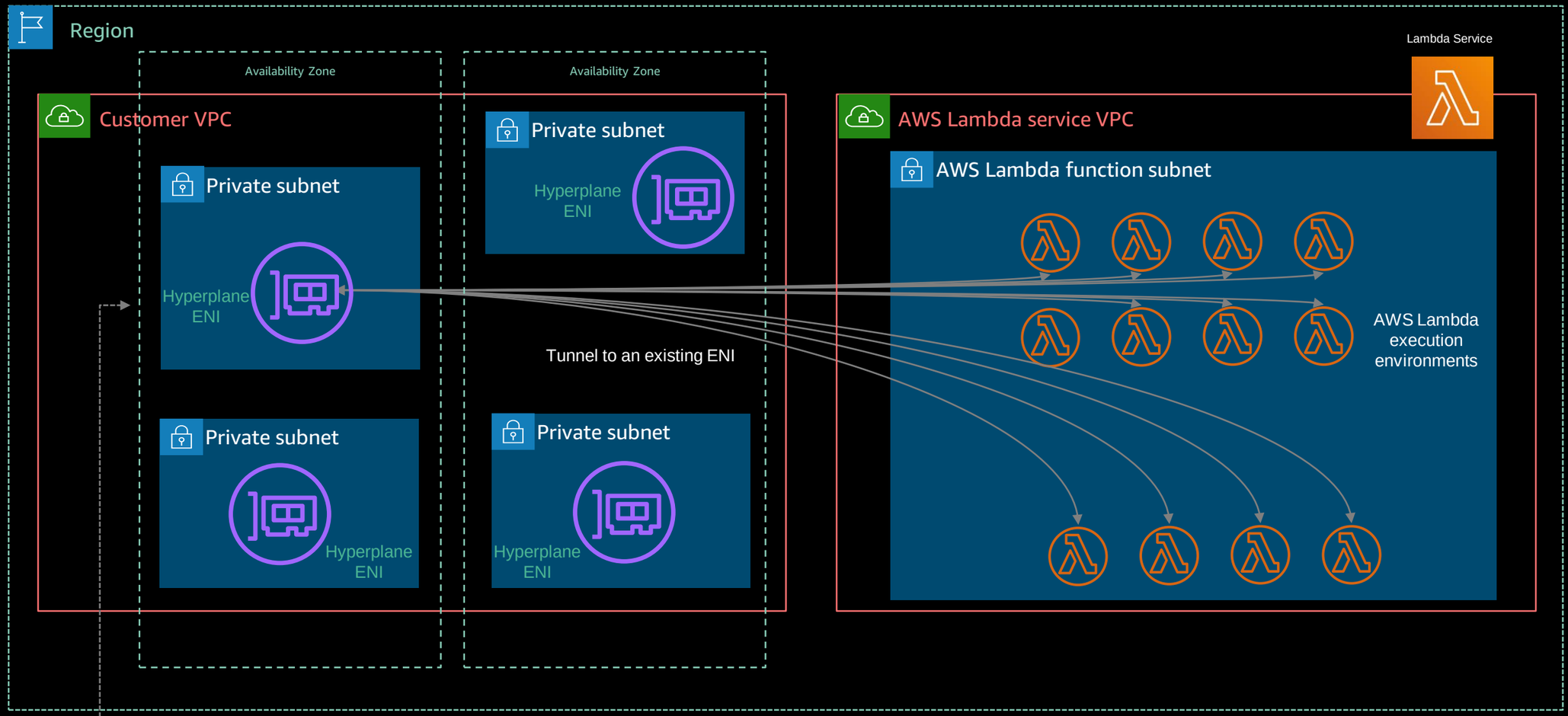
Max Limit of 50 CIDR blocks per VPC

Subnet Design

172.16.0.0/16



VPC Specific Lambda Function



Recommendations

Choose at least two subnets

Think through egress requirements

AWS Lambda functions now access customer VPC via an

AWS Hyperplane managed ENI

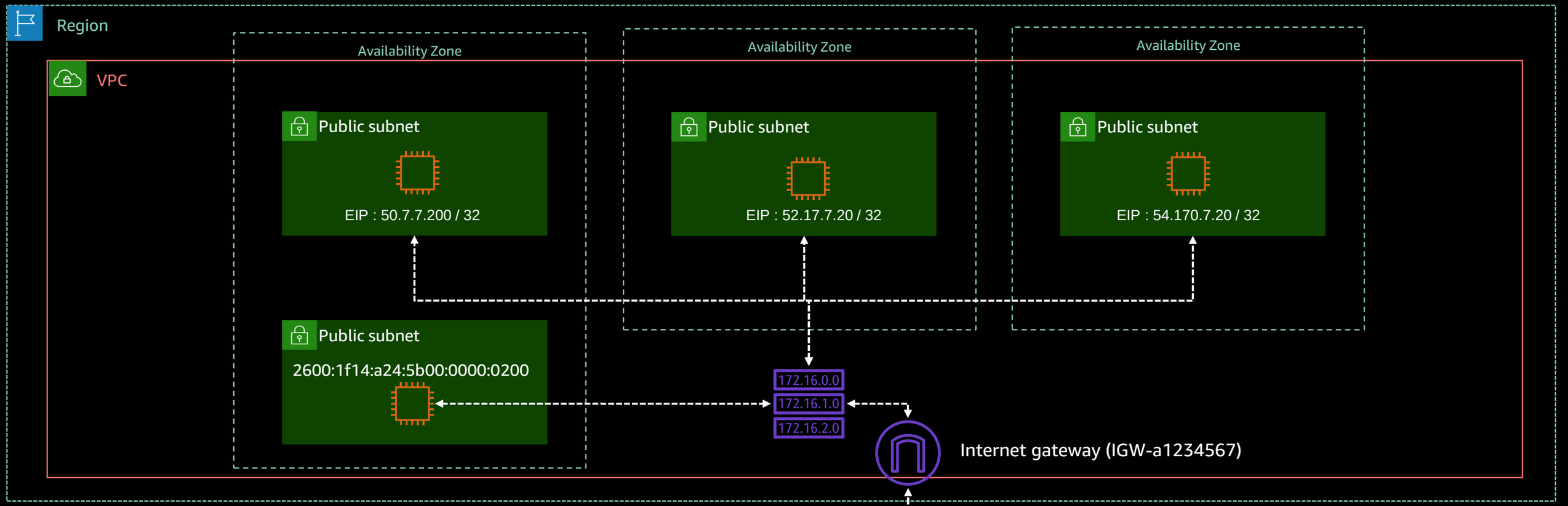
scale to support large numbers of concurrent function executions

The network interface creation happens when your AWS Lambda function is created or its VPC settings are updated

Subnet Design

2600:1f14:a24:5b00::/56

Public Subnet Internet Access

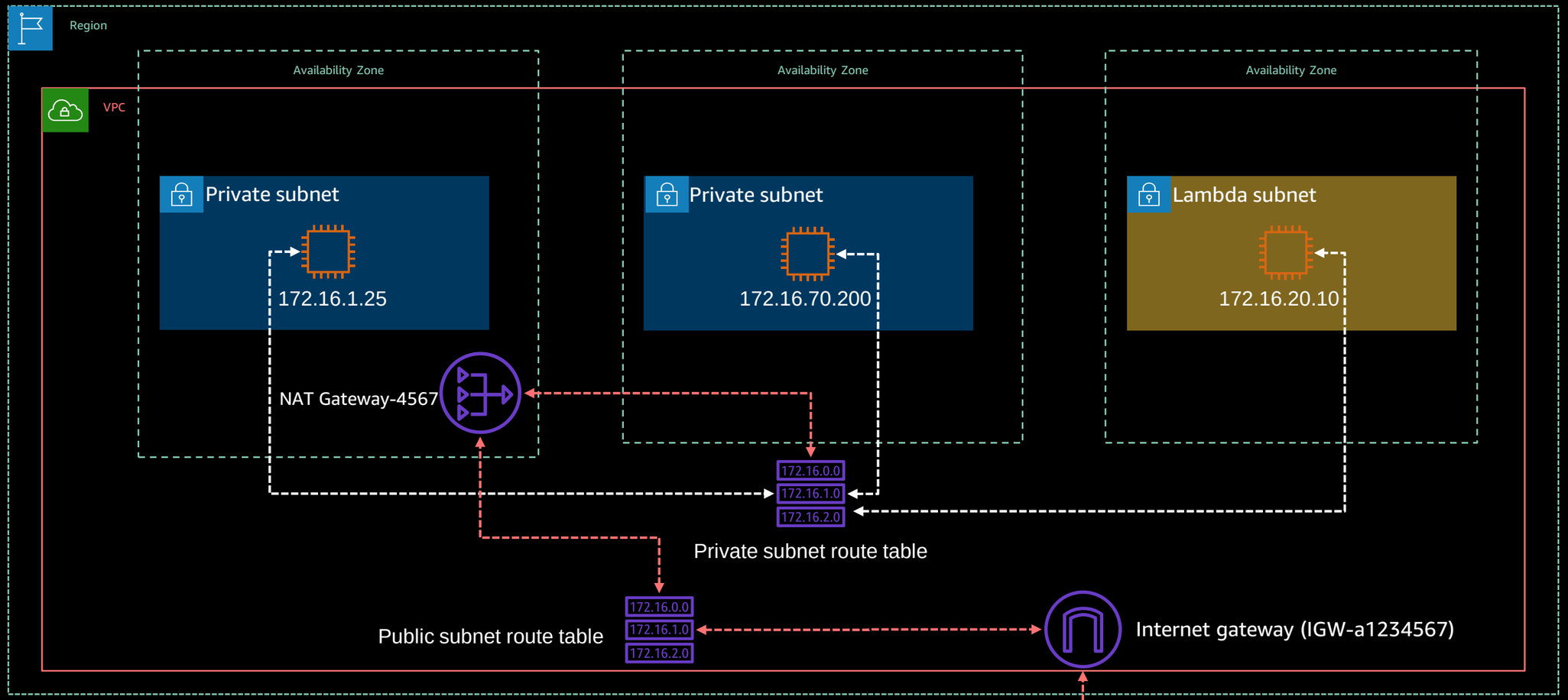


Main Route Table	
Destination	Target
172.16.0.0/16	Local
2600:1f14:a24:5b00::/56	Local
0.0.0.0/0	Igw-a1234567
::/0	Igw-a1234567

Resources with a public IP can only gain access to the internet via the internet gateway

Internet gateway is aware of the public/elastic IP address

Private Subnet Internet Access



Main route table	
Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	Nat-gw-4567

NAT gateway is AWS managed
Highly available in per AZ
Bandwidth burst up to 10Gbps
Routes its request to the IGW
Network access control list

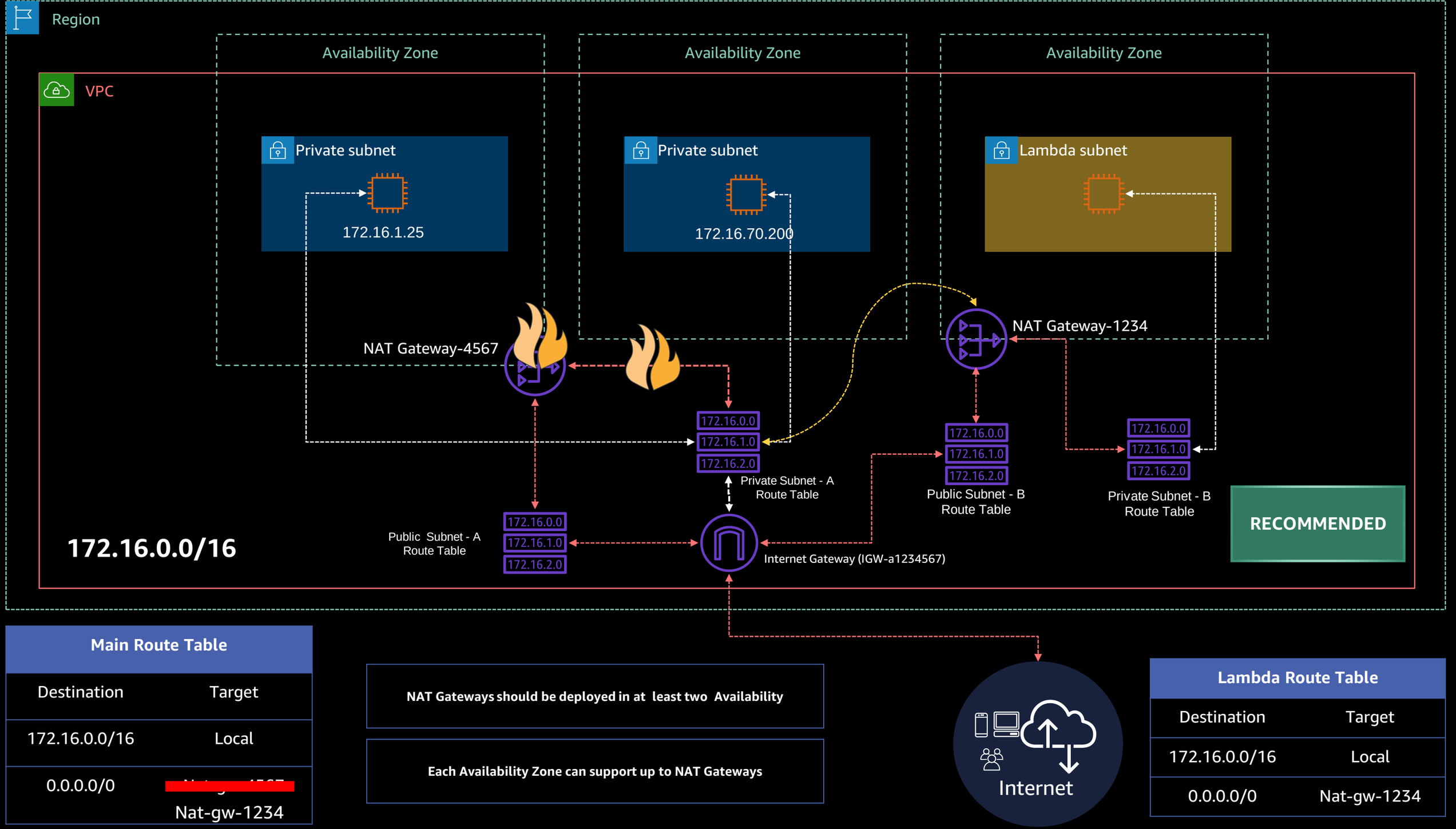
Public Subnet Route table	
Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	IGW-a1234567

AWS provided options for internet access

NAT instance

NAT gateway

A NAT Gateway can use an AWS provided Elastic IPs
Or Customer owned IPs



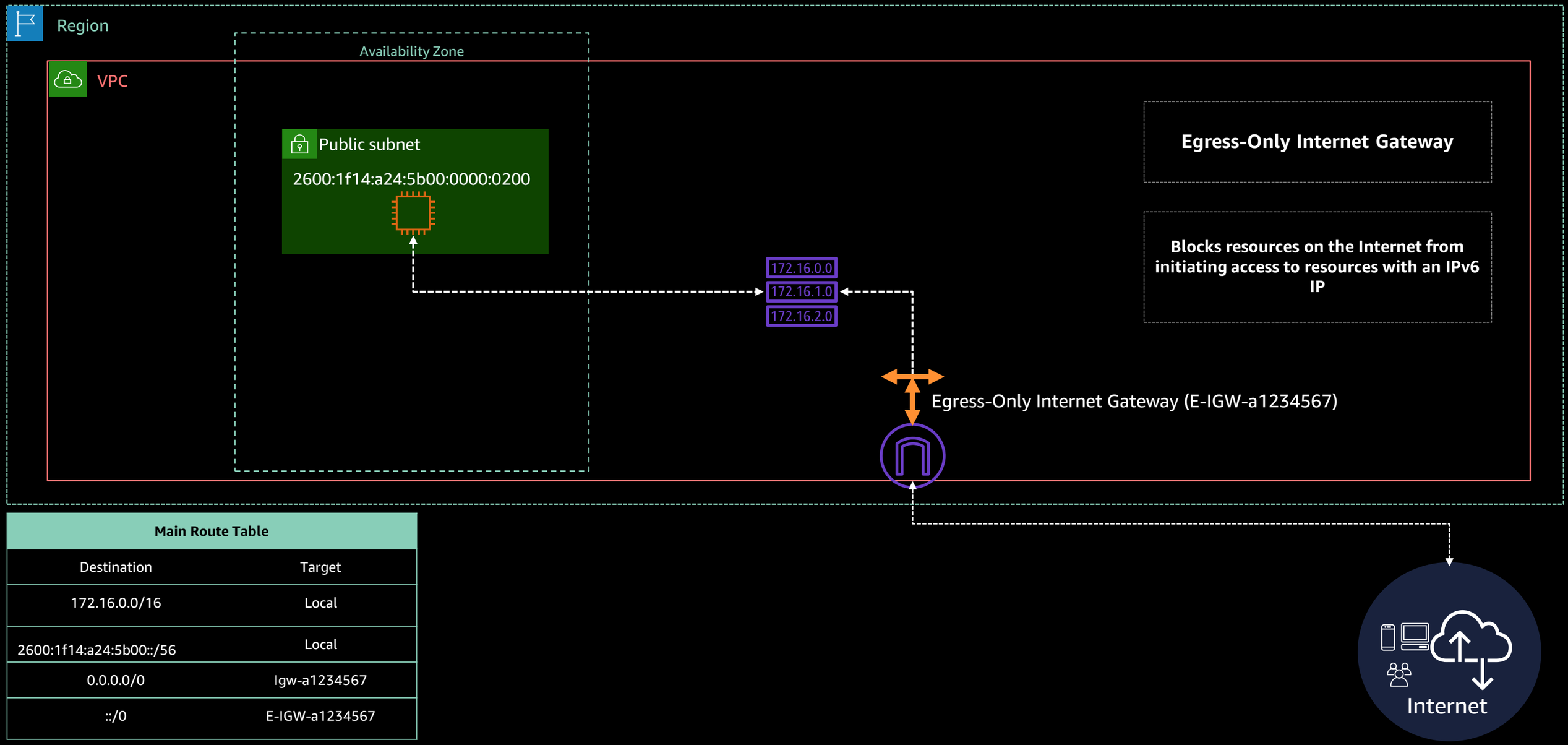
Main Route Table	
Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	Nat-gw-1234

NAT Gateways should be deployed in at least two Availability

Each Availability Zone can support up to NAT Gateways

Lambda Route Table	
Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	Nat-gw-1234

Private Subnet Internet Access for IPv6



Main Route Table	
Destination	Target
172.16.0.0/16	Local
2600:1f14:a24:5b00::/56	Local
0.0.0.0/0	Igw-a1234567
::/0	E-IGW-a1234567

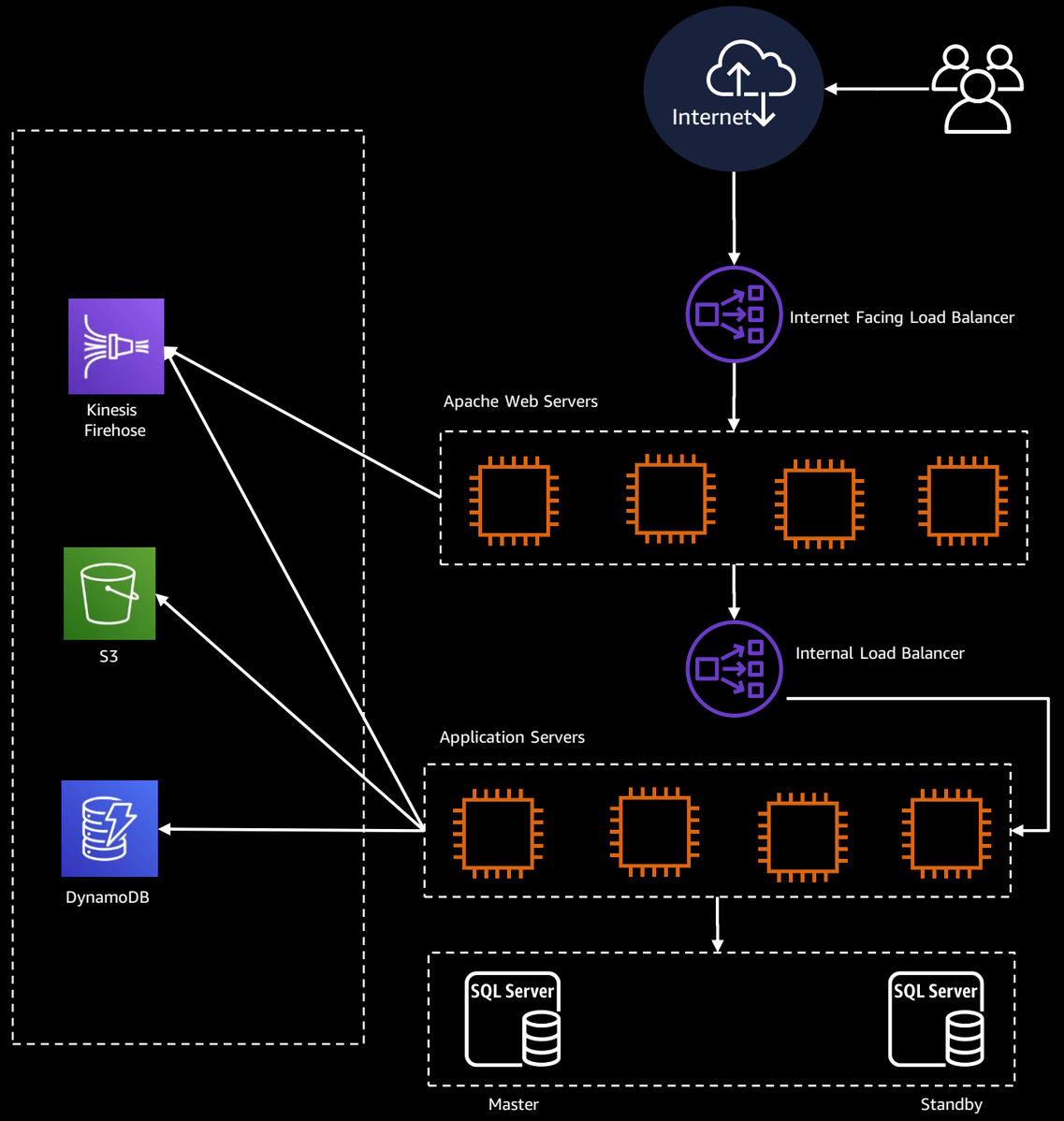
Evolving Design Requirements

Through the eyes of a multi-tiered web application migration

Requirement List 2: Private & Secure Access to AWS Public Services

- ✓ Private & Public IPv4 Space
- ✓ Internet Access for Public and Private IP Space
- ❑ Private Access to Amazon S3 & DynamoDB
- ❑ Push log data to Kinesis Fire Hose

PoC Requirements



> *Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.*

VPC Endpoints

Two Types: Gateway & Interface Endpoint

Gateway Endpoints

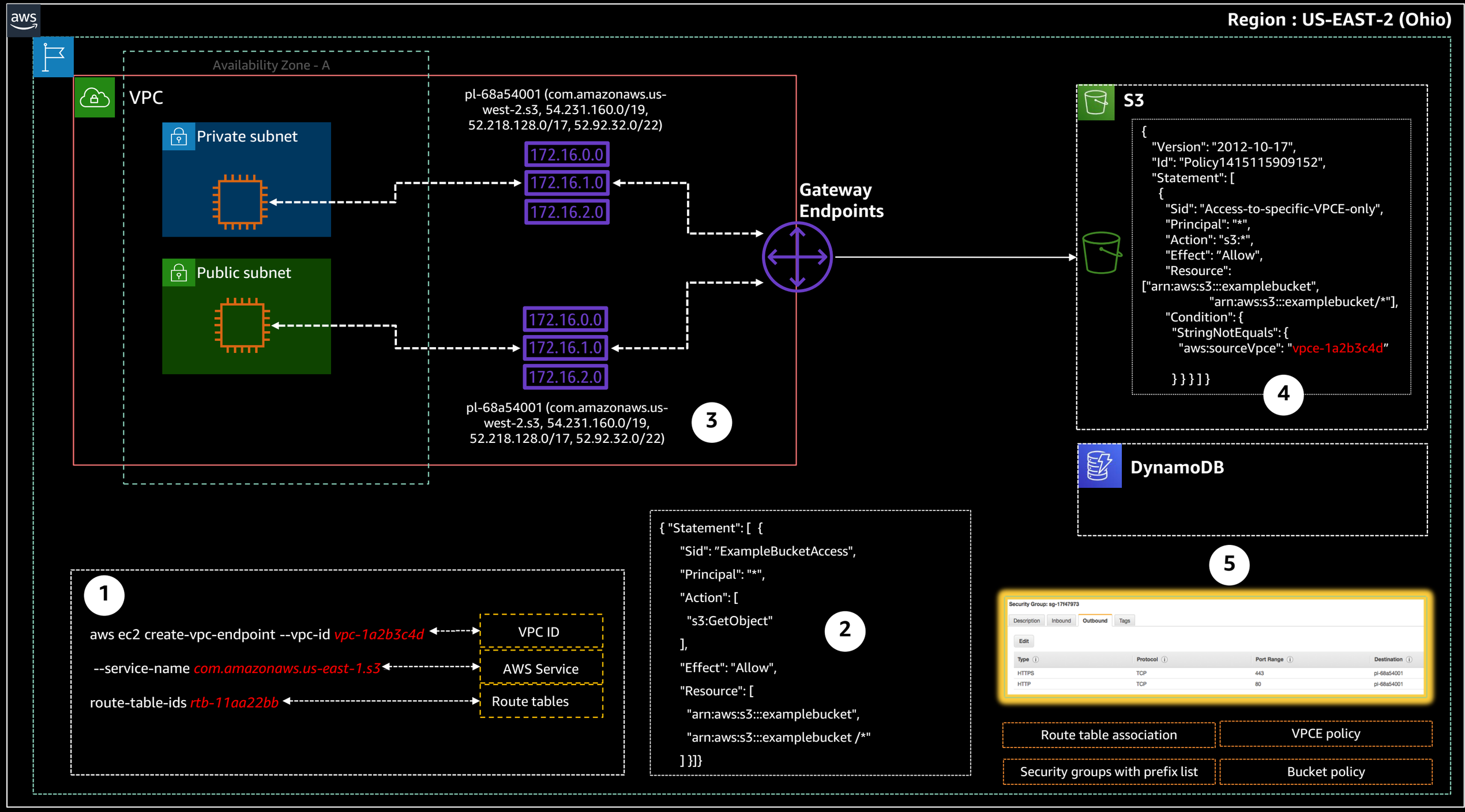
First VPC Endpoint feature to be launched by AWS

Access Two Amazon Services

Amazon S3

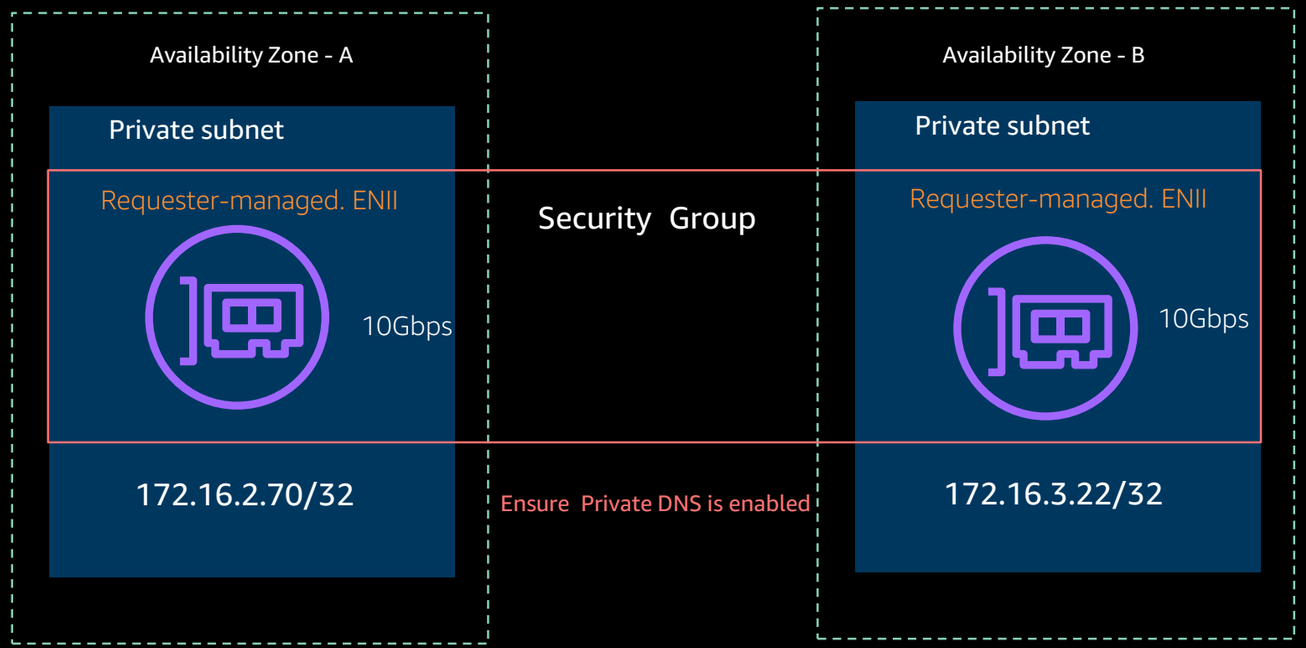
DynamoDB

via an optimized network access path


Region : US-EAST-2 (Ohio)
Availability Zone - A
VPC
Private subnet
Public subnet
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)
172.16.0.0
172.16.1.0
172.16.2.0
Gateway Endpoints
S3
{
"Version": "2012-10-17",
"Id": "Policy1415115909152",
"Statement": [
{
"Sid": "Access-to-specific-VPCE-only",
"Principal": "*",
"Action": "s3:*",
"Effect": "Allow",
"Resource":
["arn:aws:s3:::examplebucket",
"arn:aws:s3:::examplebucket/*"],
"Condition": {
"StringNotEquals": {
"aws:sourceVpce": "vpce-1a2b3c4d"
}}}]}
4
3
DynamoDB
1
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d
--service-name com.amazonaws.us-east-1.s3
route-table-ids rtb-11aa22bb
VPC ID
AWS Service
Route tables
{ "Statement": [{
"Sid": "ExampleBucketAccess",
"Principal": "*",
"Action": [
"s3:GetObject"
],
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::examplebucket",
"arn:aws:s3:::examplebucket /*"
] }]}
2
5
Security Group: sg-17f47973
Description
Inbound
Outbound
Tags
Edit
Type
Protocol
Port Range
Destination
HTTPS
TCP
443
pl-68a54001
HTTP
TCP
80
pl-68a54001
Route table association
VPCE policy
Security groups with prefix list
Bucket policy

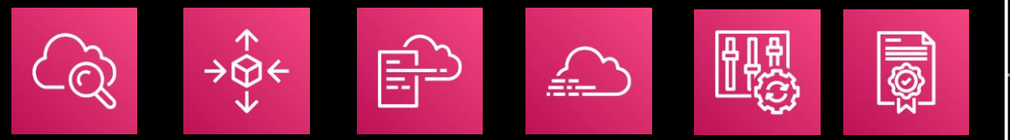
Interface Endpoints

Powered by PrivateLink



DNS
AWS Default DNS Hostname
com.amazonaws.us-*east*-2.kinesis-firehose
Endpoint Specific Regional DNS Hostname
vpce-0fe5b17a0707d6abc-29p5708s.kinesis-firehose.us-east-2.vpce.amazonaws.com
Endpoint Specific Zonal DNS Hostnames
vpce-0fe5b17a0707d6abc-29p5708s-us-east-2a.kinesis-firehose.us-east-2.vpce.amazonaws.com
vpce-0fe5b17a0707d6abc-29p5708s-us-east-2b.kinesis-firehose.us-east-2.vpce.amazonaws.com
vpce-0fe5b17a0707d6abc-29p5708s-us-east-2c.kinesis-firehose.us-east-2.vpce.amazonaws.com

AWS Public Services



Endpoint services hosted by other AWS accounts

Supported AWS Marketplace partner services

& Many More

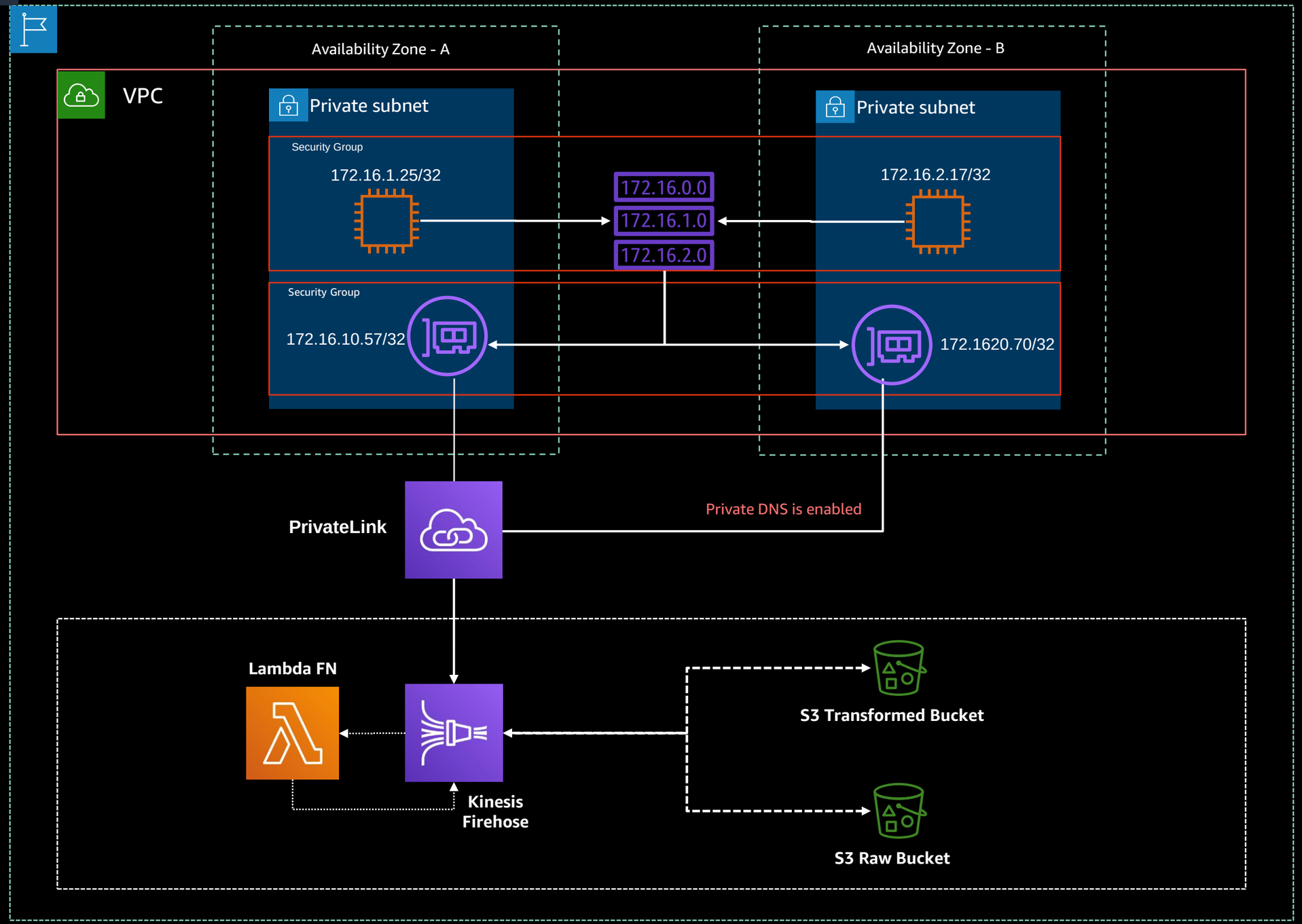
Specify at least 2 subnets when creating endpoints

Tightly configure security groups and Endpoint policies

Supports TCP Only

NACLs should be configured to allow traffic to flow to the **Endpoint ENI**

Region : US-EAST-2 (Ohio)



Interface Endpoints for Firehose

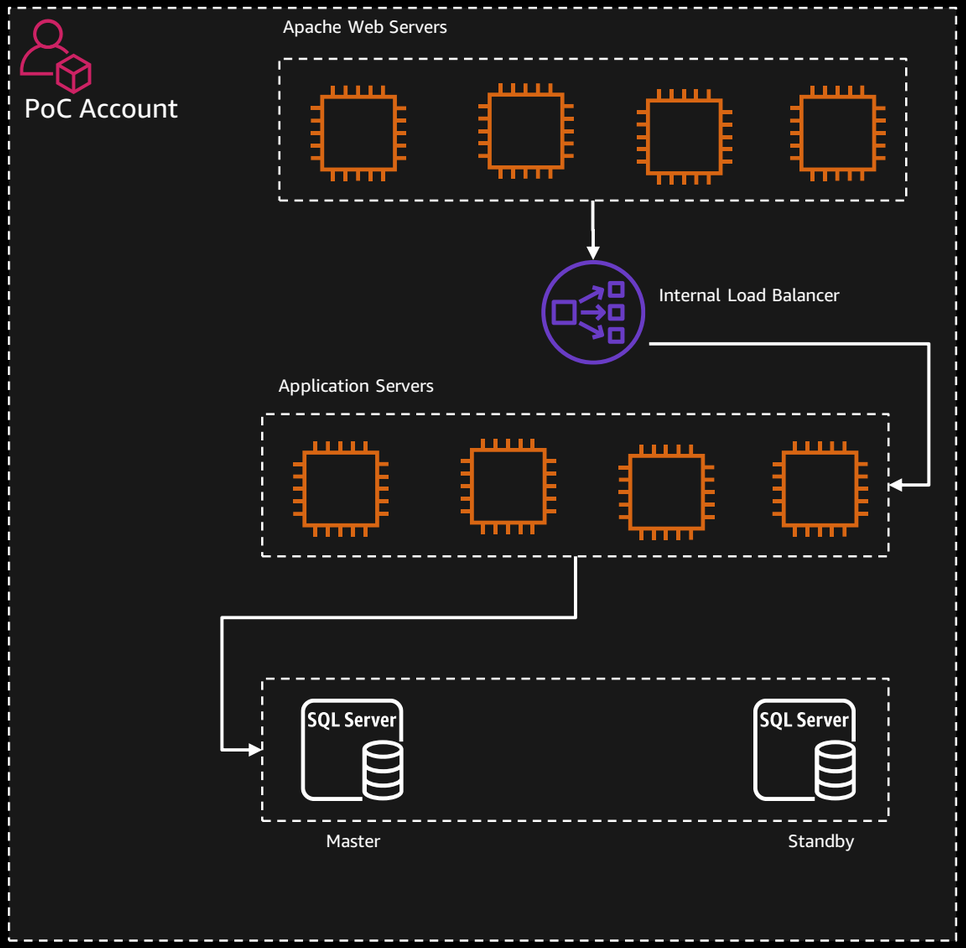
Evolving Design Requirements

Through the eyes of a multi-tiered web application migration

Requirement List 4: Establish WAN Connectivity to on-premises & Hybrid DNS

- ❑ Establish a site to site VPN between Amazon VPC and on-premises data center
- ❑ Allow on-premises resources to resolve VPC specific DNS hostnames

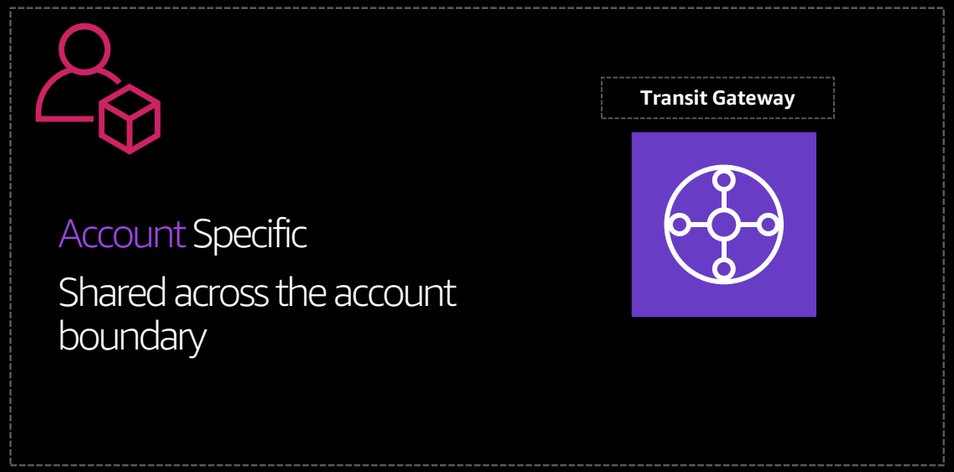
PoC Requirements



WAN Connectivity: Site-2-Site VPN

AWS Provides Two (2) Infrastructure for Site-2-Site VPN

Customer Gateway

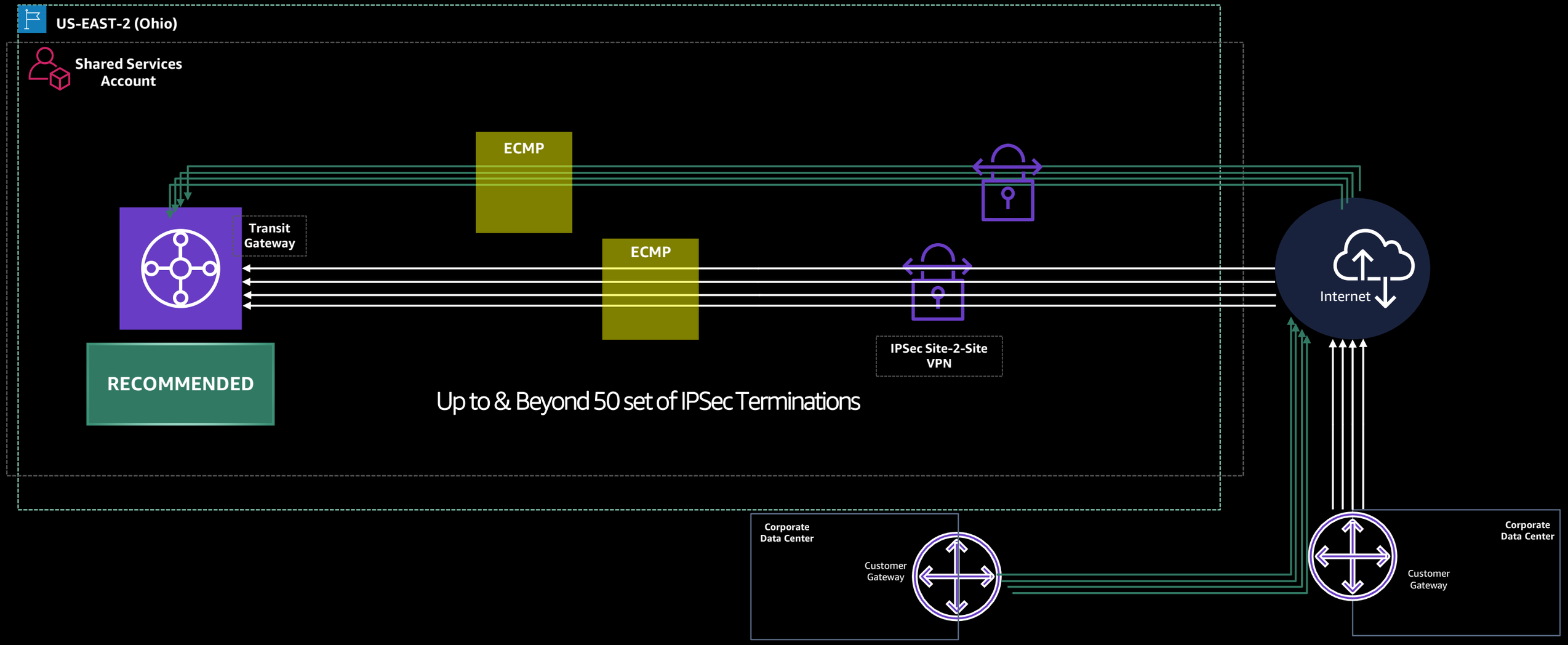


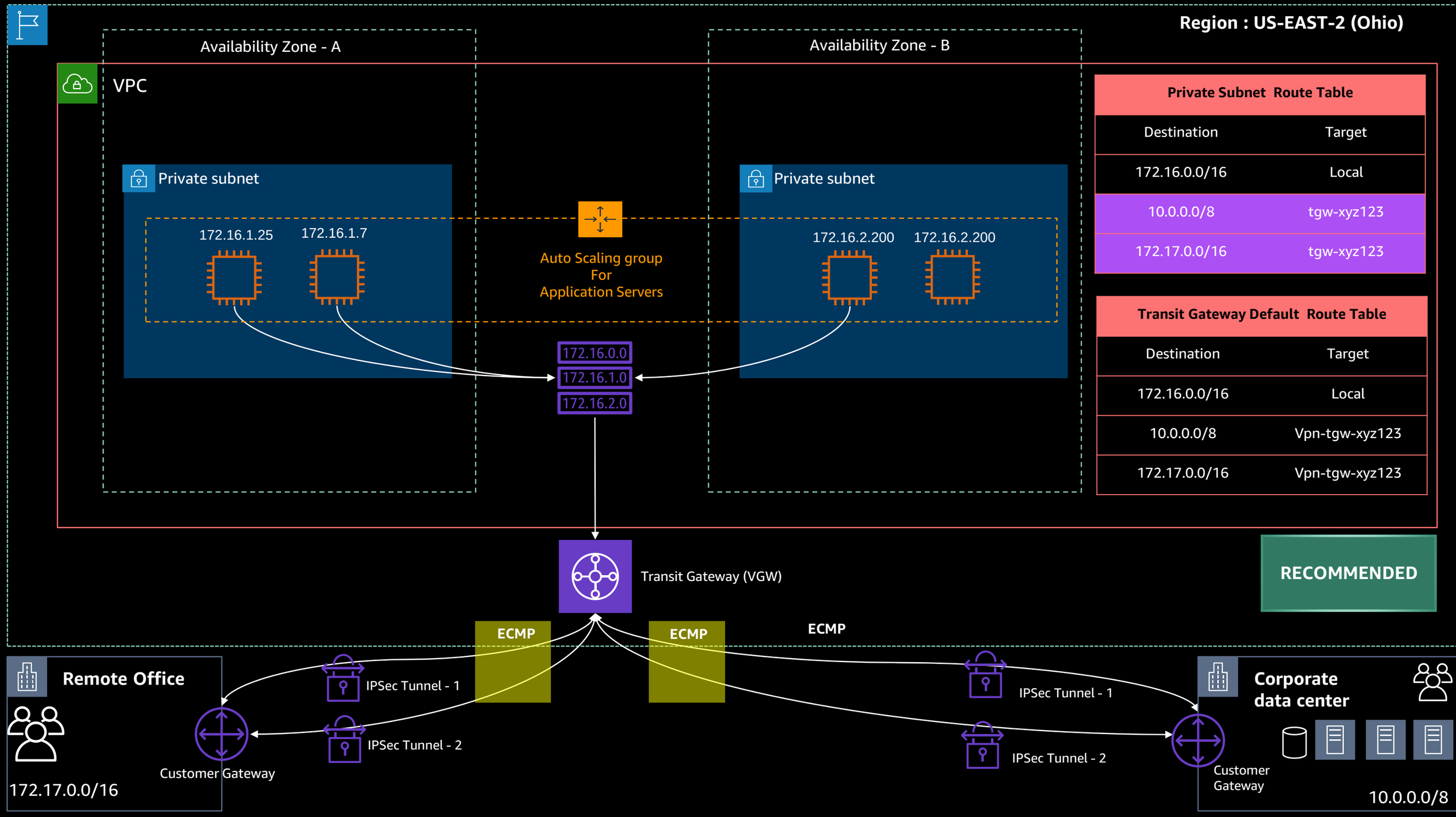
Supported Functionality
Two IPSec Tunnels per connection
Routing Protocols: Static Routes & Border Gateway Protocol (BG)
Bring your own ASN
Secrets
Inside Tunnel IPs

Supports IPSec Termination to multiple remote sites

WAN Connectivity: Site-2-Site VPN

Transit Gateway / WAN Concentrator:




Region : US-EAST-2 (Ohio)
Availability Zone - A
Availability Zone - B
VPC
Private subnet
Private subnet
172.16.1.25
172.16.1.7
172.16.2.200
172.16.2.200
Auto Scaling group
For
Application Servers
172.16.0.0
172.16.1.0
172.16.2.0
Private Subnet Route Table
Destination
Target
172.16.0.0/16
Local
10.0.0.0/8
tgw-xyz123
172.17.0.0/16
tgw-xyz123
Transit Gateway Default Route Table
Destination
Target
172.16.0.0/16
Local
10.0.0.0/8
Vpn-tgw-xyz123
172.17.0.0/16
Vpn-tgw-xyz123
RECOMMENDED
Transit Gateway (VGW)
ECMP
ECMP
ECMP
Remote Office
IPSec Tunnel - 1
IPSec Tunnel - 2
Customer Gateway
172.17.0.0/16
IPSec Tunnel - 1
IPSec Tunnel - 2
Corporate
data center
Customer
Gateway
10.0.0.0/8

Amazon VPC Hostname Resolution

By On-premises Resources

Region

.2

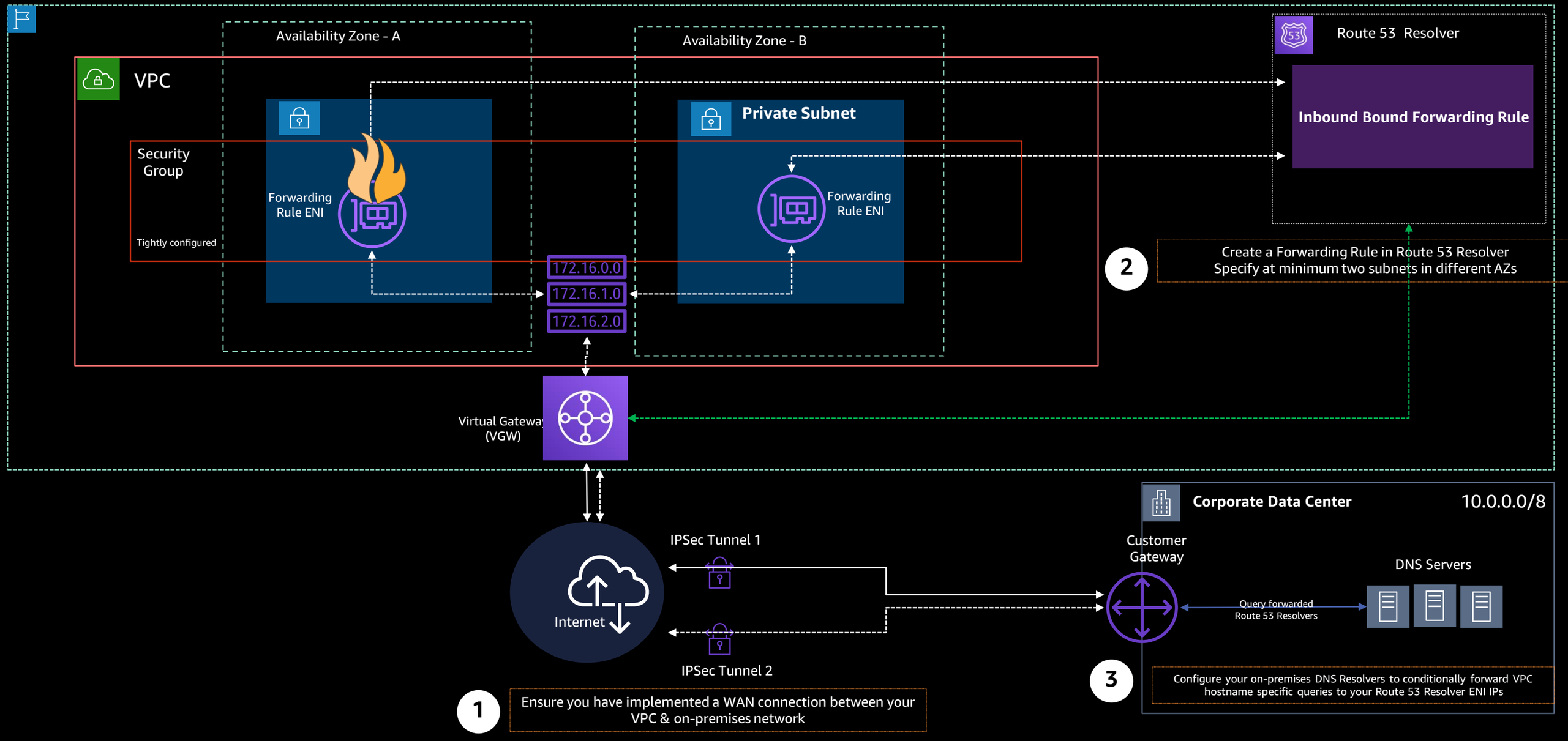
Route 53 Resolver

For

Hybrid Networks

- Recursive lookups against public name servers for all other domain names.
- VPC domain names such as domain names for EC2 instances or ELB load balancers.
- Route 53 Resolver allows you to create Inbound & Outbound Rules
- Allows on-premises resources to resolve VPC Specific DNS hostnames
- Allows VPC resources to resolve on-premises DNS hostnames seamlessly
- Conditionally forward queries from a VPC to resolvers on your

Route 53 Resolver Inbound Rules



Success!
Application Migrated Successfully

Great! 

Now, let’s do this for all of our Applications

To Many

Simplifying Multi-VPC Architectures via Centralization

AWS re:Invent

aws

Evolving Design Requirements

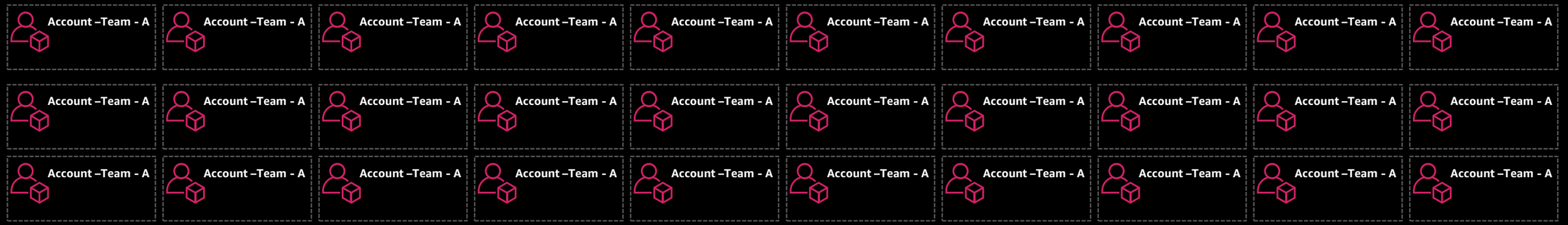
Multi-VPC, Multi-Region Environment

1. Thirty (30) Application Teams, each requiring an individual accounts for DEV, Test , & Production
2. Resources for DEV can be hosted in a shared IP space that is managed by another account
3. Each account requires access to
    a. **VPCs of the same account type whether they are in the same Region or not**
    b. **Internet for resources in private subnets**
    c. **AWS Public Services**
    d. **On-premises data centers**

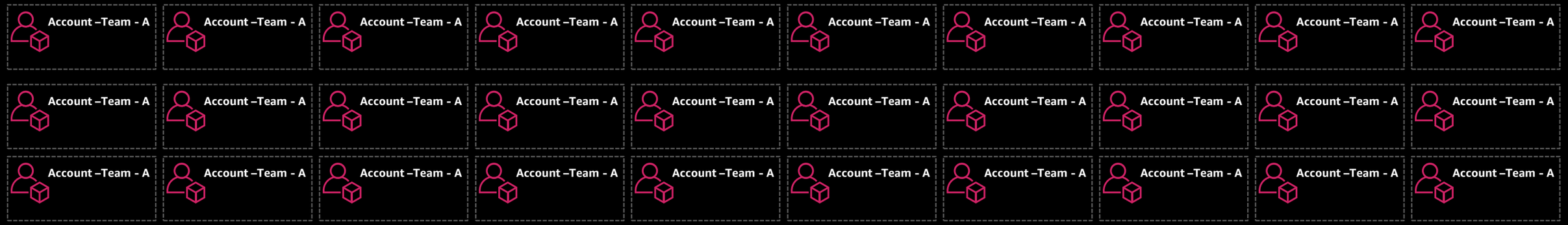
Technical Requirements

Requirement: 1

Prod



TEST

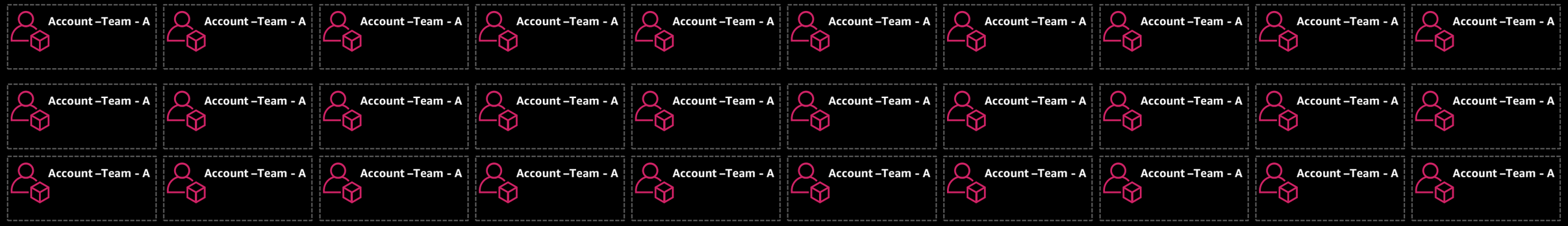


90 ACCOUNTS

On-premises Access
Internet Access
DNS

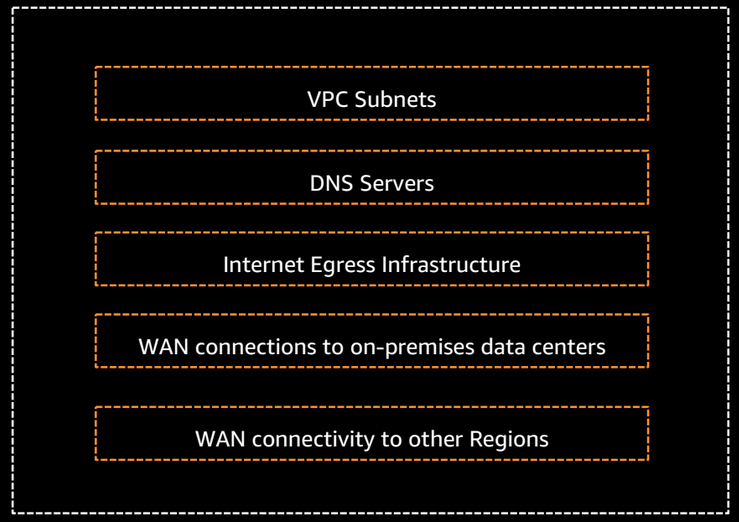
How can I satisfy these requirements and simplify implementation & management

DEV



1

Centrally Distribute Network Services that are essential successful operation of network on AWS



2

Amazon Resource Access Manager

3

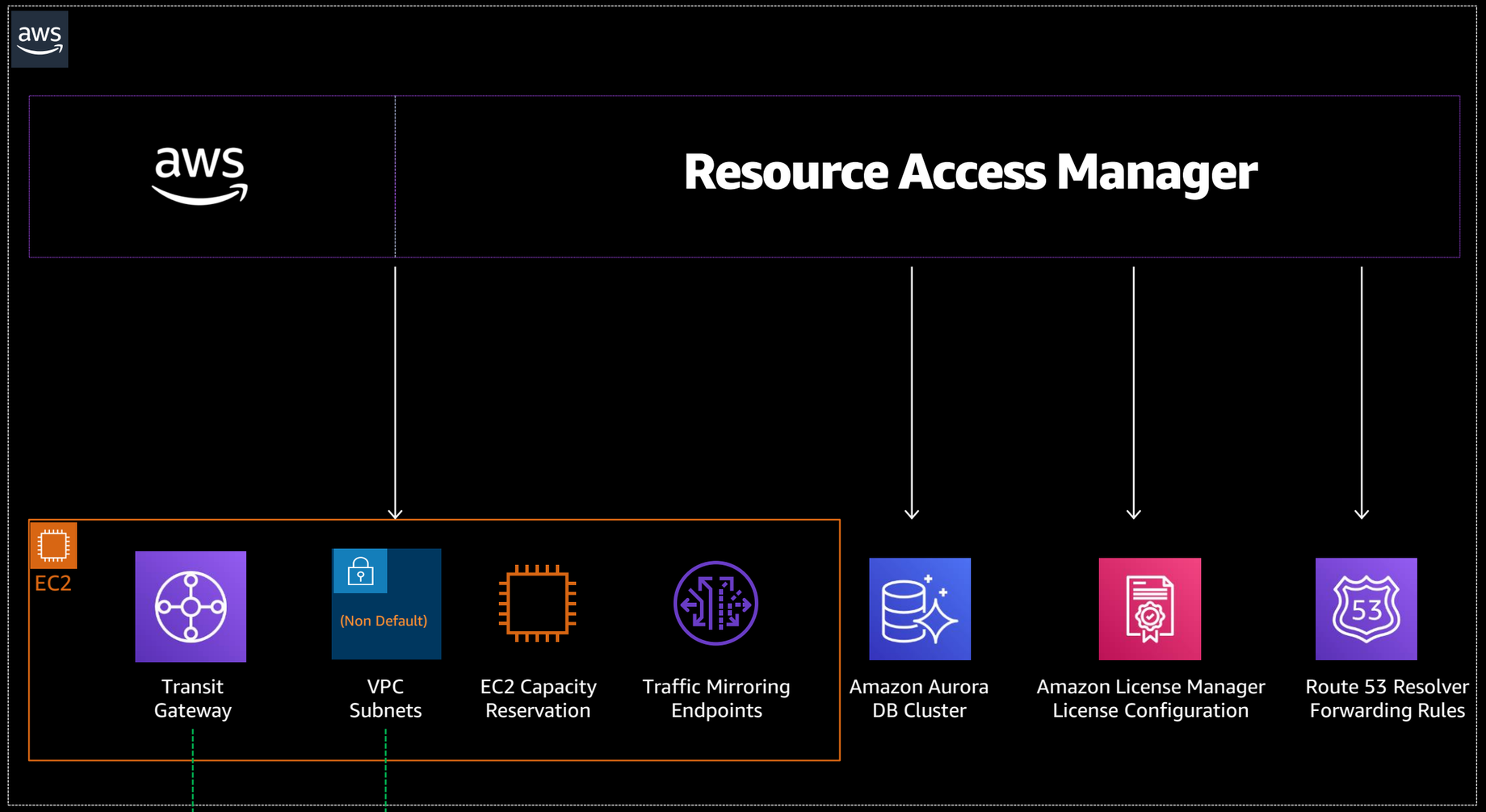
Amazon Transit Gateway

>

Amazon Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any

- An Account
- Organizational Unit
- An Entire AWS Organization



2

Transit Gateway

1. A Transit Gateway will be created in the Shared Services Account
2. Then shard to each account via AWS RAM
3. Routing & WAN connectivity will be established & distributed

1

VPC Sharing

Sharing Private & Public Subnets from the Shared Services Account with each DEV account.

Eliminating the need to create a VPC per DEV Account & Each of their connectivity infrastructure

Amazon VPC Sharing

Centrally distributing VPC resources across the account boundary

Requirement 2: Shared IP Space for DEV

AWS re:Invent

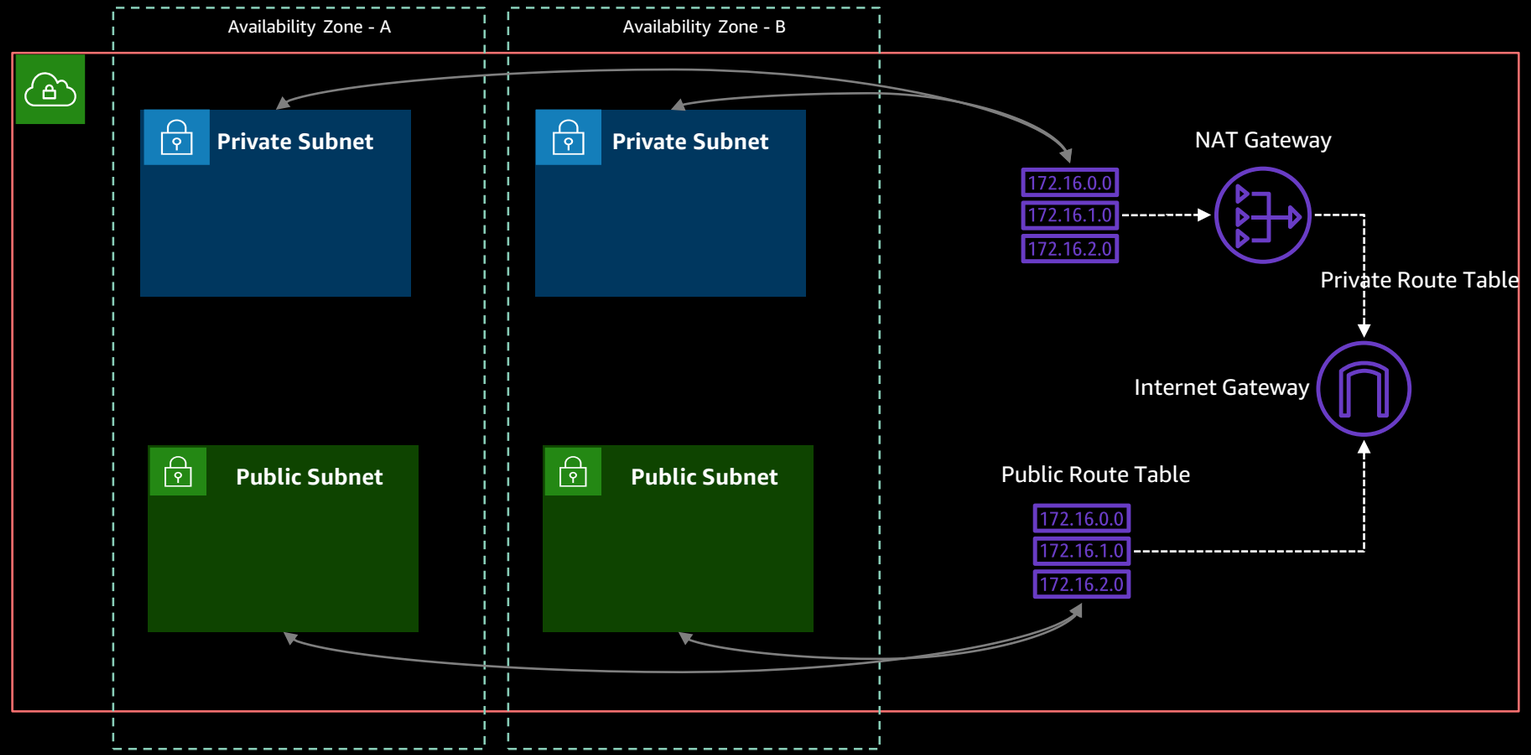
aws

Amazon VPC Sharing

Shared Services Account

Allows multiple AWS accounts that belong to the same AWS Organization to create their application resources into a shared, centrally-managed non-default Amazon VPC

VPC Owner
Responsible for creating & managing VPCs and all VPC-level resources
Cannot modify/delete participant resources including security groups created by participants
Create flow log subscriptions at the VPC, subnet, or ENI level



Participating Account
View, create, modify, and delete their application resources in the subnets shared with them
Cannot view, modify, or delete resources that belong to other participants / VPC owner

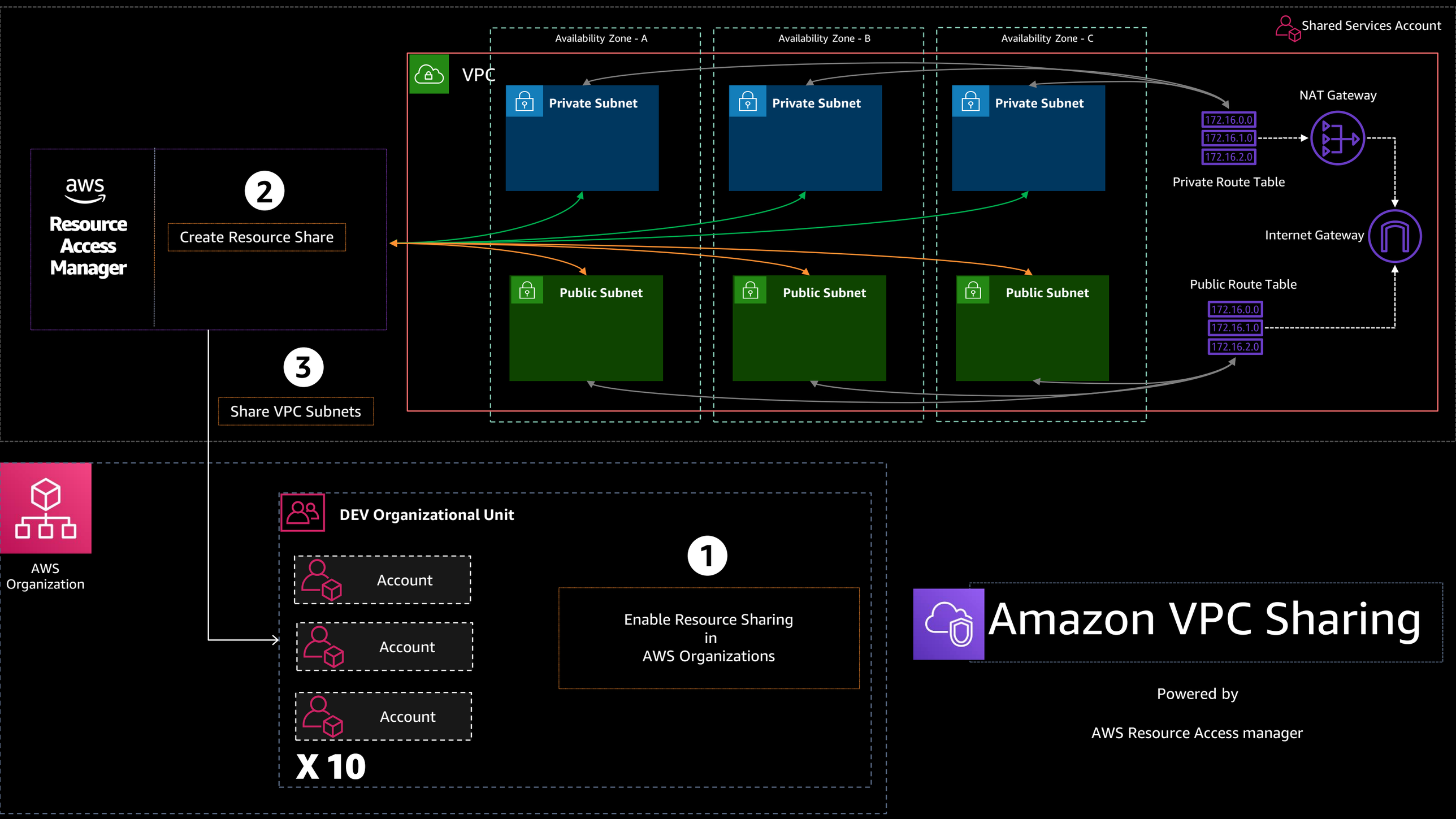
Packet Segmentation

Subnetting

Route Tables

Security Groups

NACLs


Shared Services Account
Availability Zone - A
Availability Zone - B
Availability Zone - C
VPC
Private Subnet
Private Subnet
Private Subnet
NAT Gateway
172.16.0.0
172.16.1.0
172.16.2.0
Private Route Table
Internet Gateway
Public Subnet
Public Subnet
Public Subnet
Public Route Table
172.16.0.0
172.16.1.0
172.16.2.0
aws
Resource Access Manager
2
Create Resource Share
3
Share VPC Subnets
AWS Organization
DEV Organizational Unit
Account
Account
Account
X 10
1
Enable Resource Sharing in AWS Organizations
Amazon VPC Sharing
Powered by
AWS Resource Access manager

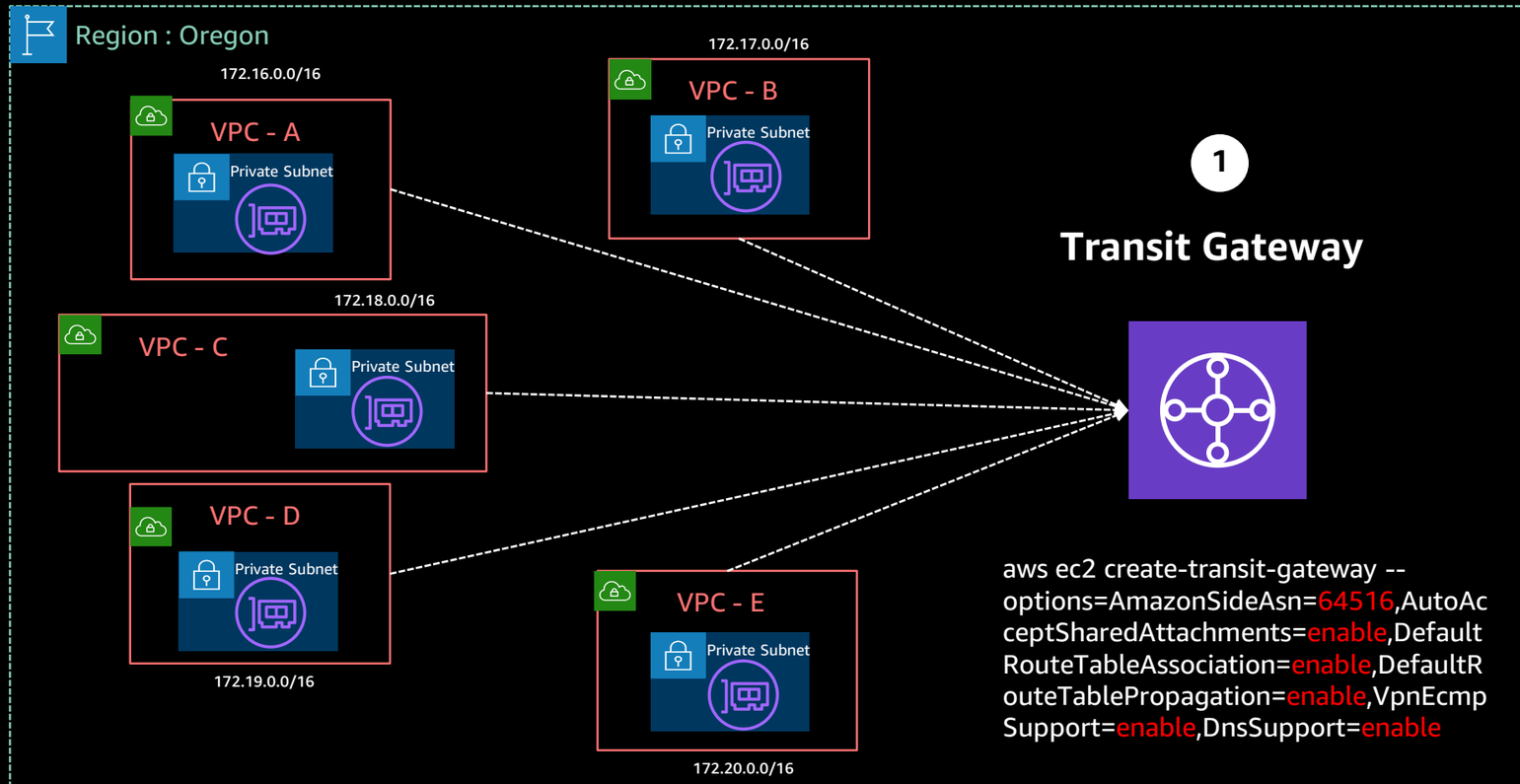
Amazon Transit Gateway

Inter-VPC Routing

Requirement 3a: Route traffic between VPCs of the same account type

AWS re:Invent

aws



1

Transit Gateway

aws ec2 create-transit-gateway --options=AmazonSideAsn=64516,AutoAcceptSharedAttachments=enable,DefaultRouteTableAssociation=enable,DefaultRouteTablePropagation=enable,VpnEcmpSupport=enable,DnsSupport=enable

Transit Gateway

Regional router that is VPC Agnostic
Supports attachment of VPCs, VPN, Direct Connect Gateway
Allows you to connect up to 5,000 VPCs
Supports Egress to external networks via IPSec and Direct Connect
Layer 3 Routing Segmentation (VRF Like Functionality like Route leaking)
Supports up to 10,000 Routes
Supports ECMP, BGP Routing Protocol (DX & VPN), Static Routing (VPN only)

Up on Creation

- ❑ Elastic Network Interface (ENI) Added to each subnet specified during or after creation
  - ❑ Enables all subnet in that Availability Zone to reach the Transit Gateway

Recommendation : Specify at minimum two subnets across different Availability Zones

- ❑ Resources that reside in Availability Zones where there is no transit gateway attachment will not be able to reach the transit gateway.

2

create-resource-share --name "Network Ops resource share"

--principals [‘acct-1’, ‘account-2’, ‘account-3’] //same OU

--resource-arns ["arn:aws:ec2:us-east-1:12345678901:tgw/tgw-rtb-abc3232

"]

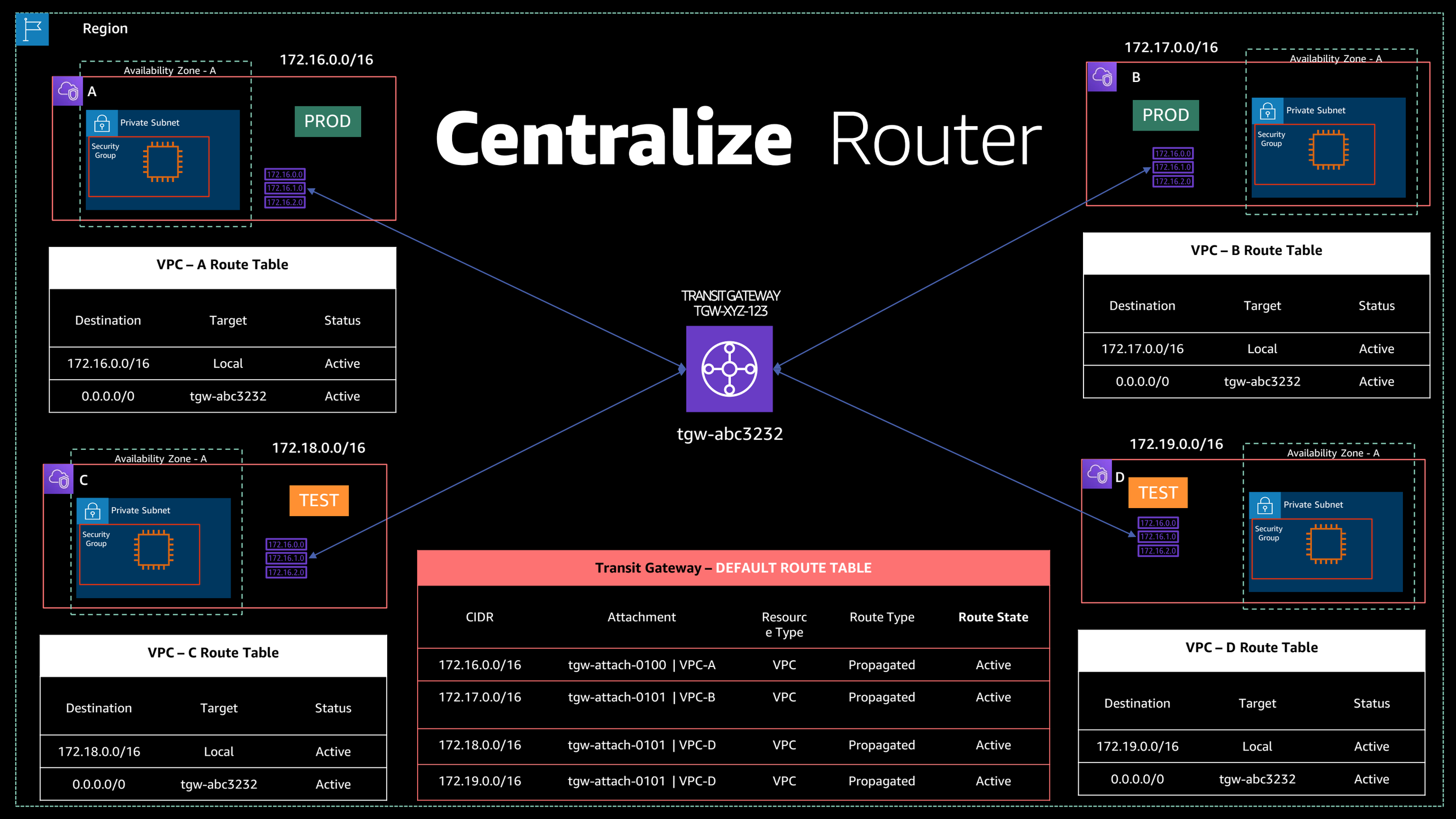
3

aws ec2 create-transit-gateway-vpc-attachment

--transit-gateway-id tgw-14324bbc412a43243

--vpc-id vpc-2321314314

--subnet-ids subnet-12312312,subnet-41343432



VPC – A Route Table

Destination	Target	Status
172.16.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

VPC – B Route Table

Destination	Target	Status
172.17.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

VPC – C Route Table

Destination	Target	Status
172.18.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

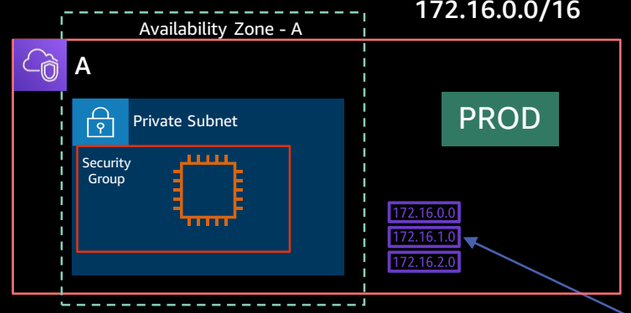
VPC – D Route Table

Destination	Target	Status
172.19.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

Transit Gateway – DEFAULT ROUTE TABLE

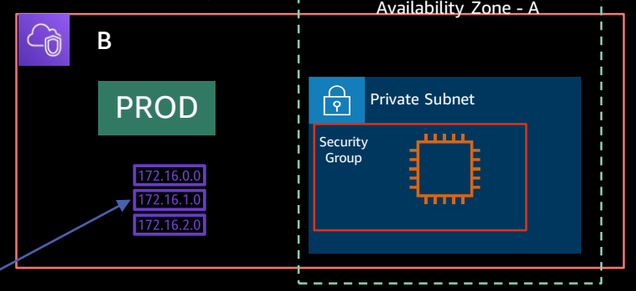
CIDR	Attachment	Resource Type	Route Type	**Route State**
172.16.0.0/16	tgw-attach-0100 | VPC-A	VPC	Propagated	Active
172.17.0.0/16	tgw-attach-0101 | VPC-B	VPC	Propagated	Active
172.18.0.0/16	tgw-attach-0101 | VPC-D	VPC	Propagated	Active
172.19.0.0/16	tgw-attach-0101 | VPC-D	VPC	Propagated	Active

Route Isolation



Transit Gateway - PROD Route Table

CIDR	Attachment	Resource Type	Route Type	**Route State**
172.16.0.0/16	tgw-attach-0100 | VPC-A	VPC	Propagated	Active
172.17.0.0/16	tgw-attach-0101 | VPC-B	VPC	Propagated	Active



VPC – A Route Table

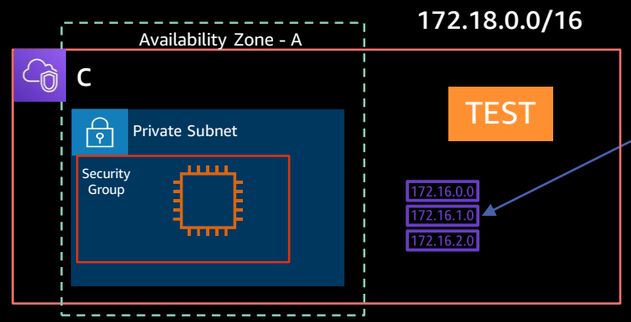
Destination	Target	Status
172.16.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

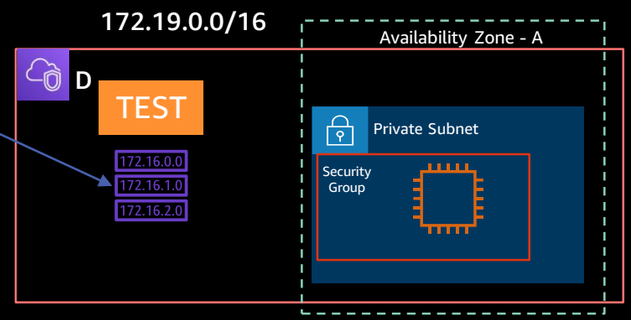
TRANSIT GATEWAY
TGW-XYZ-123

tgw-abc3232

VPC – B Route Table

Destination	Target	Status
172.17.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active





VPC – C Route Table

Destination	Target	Status
172.18.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

Transit Gateway - TEST Route Table

CIDR	Attachment	Resource Type	Route Type	**Route State**
172.18.0.0/16	tgw-attach-0100 | VPC-C	VPC	Propagated	Active
172.19.0.0/16	tgw-attach-0101 | VPC-D	VPC	Propagated	Active

VPC – D Route Table

Destination	Target	Status
172.19.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

Centralized NAT

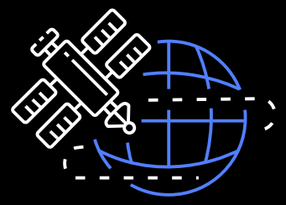
via Transit Gateway & NAT Gateway

Requirement 3b: Internet Access for VPCs

AWS re:Invent

aws

Centralized NAT : How To Guide

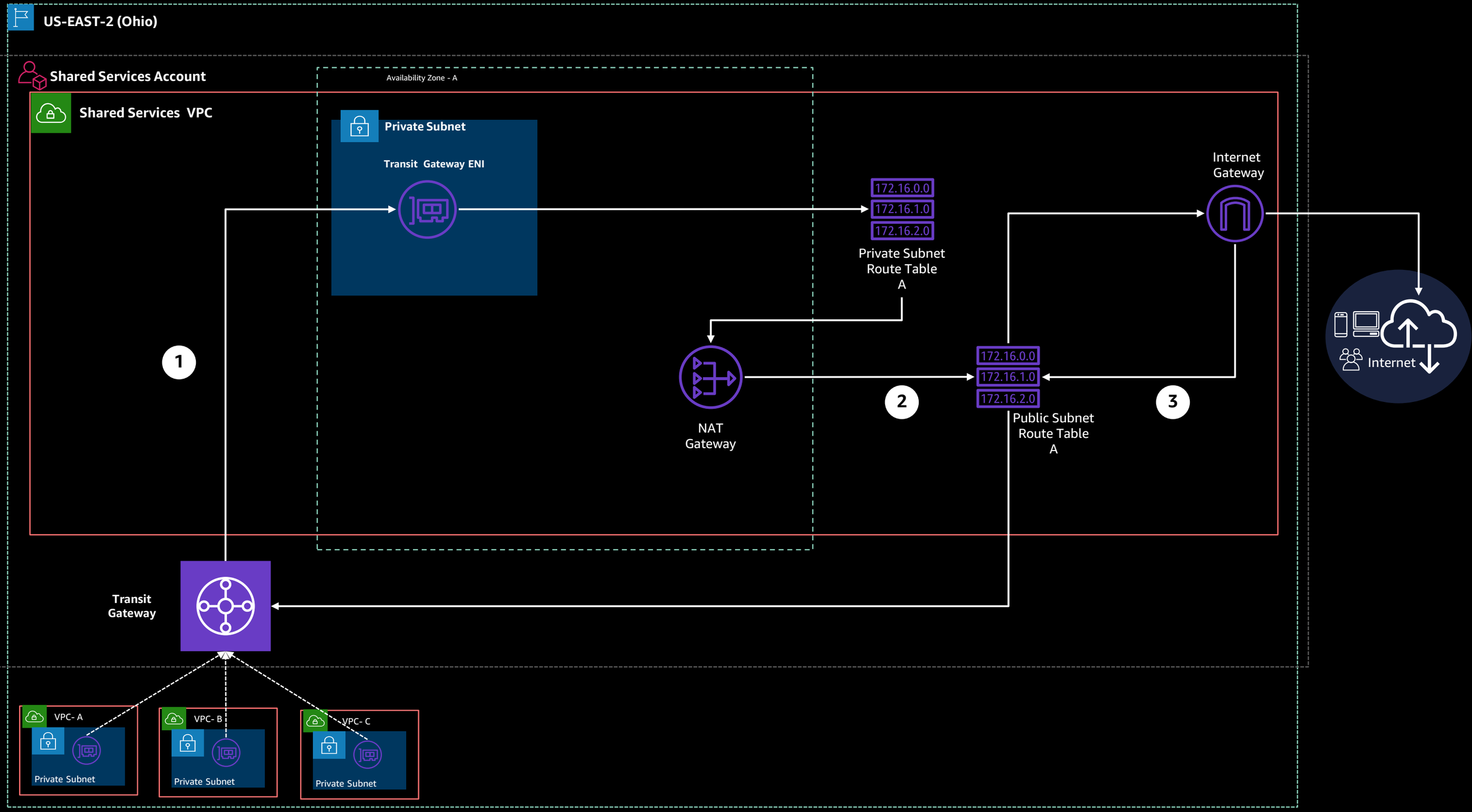


Create Two NAT Gateways in Public Subnets

Add a Default Route to VPC Route Table(s)

Configure Summarized Routes on Public Subnet Route Tables

Configure Default Route on Transit Gateway Route Table(s) that points to the Shared Services VPC as next hop


US-EAST-2 (Ohio)
Shared Services Account
Availability Zone - A
Shared Services VPC
Private Subnet
Transit Gateway ENI
172.16.0.0
172.16.1.0
172.16.2.0
Private Subnet Route Table A
Internet Gateway
1
NAT Gateway
2
172.16.0.0
172.16.1.0
172.16.2.0
Public Subnet Route Table A
3
Internet
Transit Gateway
VPC- A
Private Subnet
VPC- B
Private Subnet
VPC- C
Private Subnet

Centralized NAT Route Config

Transit Gateway Default Route Table

CIDR	Attachment	Resource Type	Route Type	**Route State**
172.16.0.0/16	tgw-attach-0100 | VPC-A	VPC	Propagated	Active
172.17.0.0/16	tgw-attach-0101 | VPC-B	VPC	Propagated	Active
172.18.0.0/16	tgw-attach-0102 | VPC-C	VPC	Propagated	Active
172.19.0.0/16	tgw-attach-0103 | VPC-D	VPC	Propagated	Active
172.20.0.0/16	tgw-attach-0104 | Egress-VPC	VPC	Propagated	Active
0.0.0.0/0	tgw-attach-0104 | Egress-VPC	VPC	Static	Active

Shared Services VPC – Public Subnet Route Table

Destination	Target	Status
172.20.0.0/16	Local	Active
0.0.0.0/0	igw-abc123	Active
172.17.0.0/16	tgw-abc3232	Active
172.18.0.0/16	tgw-abc3232	Active
172.19.0.0/16	tgw-abc3232	Active
172.16.0.0/16	tgw-abc3232	Active

Shared Services VPC – Private Subnet Route Table

Destination	Target	Status
172.20.0.0/16	Local	Active
0.0.0.0/0	nat-gw-xyz-123	Active

VPC – A Route Table

Destination	Target	Status
172.16.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

VPC – B Route Table

Destination	Target	Status
172.17.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

VPC – C Route Table

Destination	Target	Status
172.18.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

VPC – D Route Table

Destination	Target	Status
172.19.0.0/16	Local	Active
0.0.0.0/0	tgw-abc3232	Active

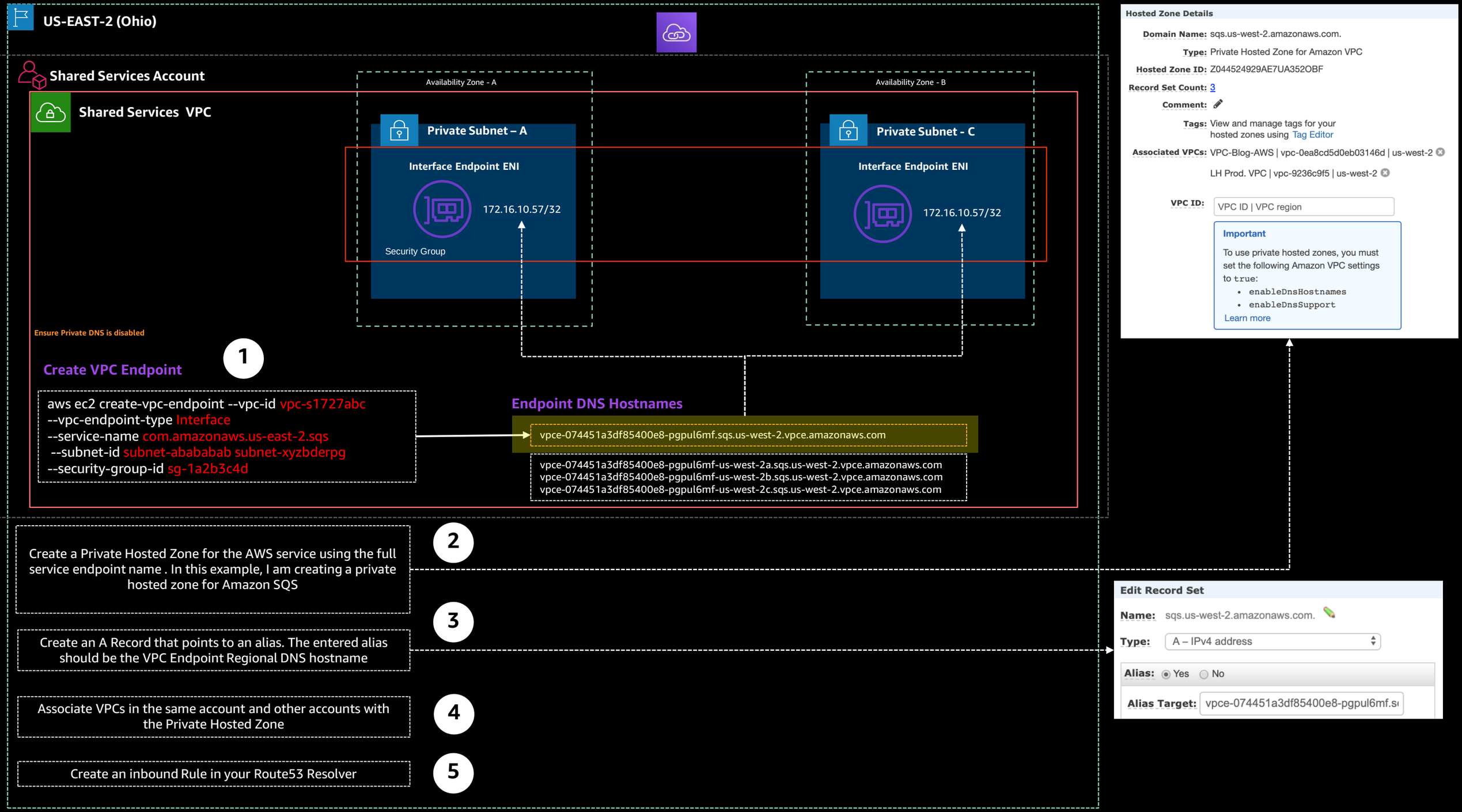
PrivateLink Interface Endpoint

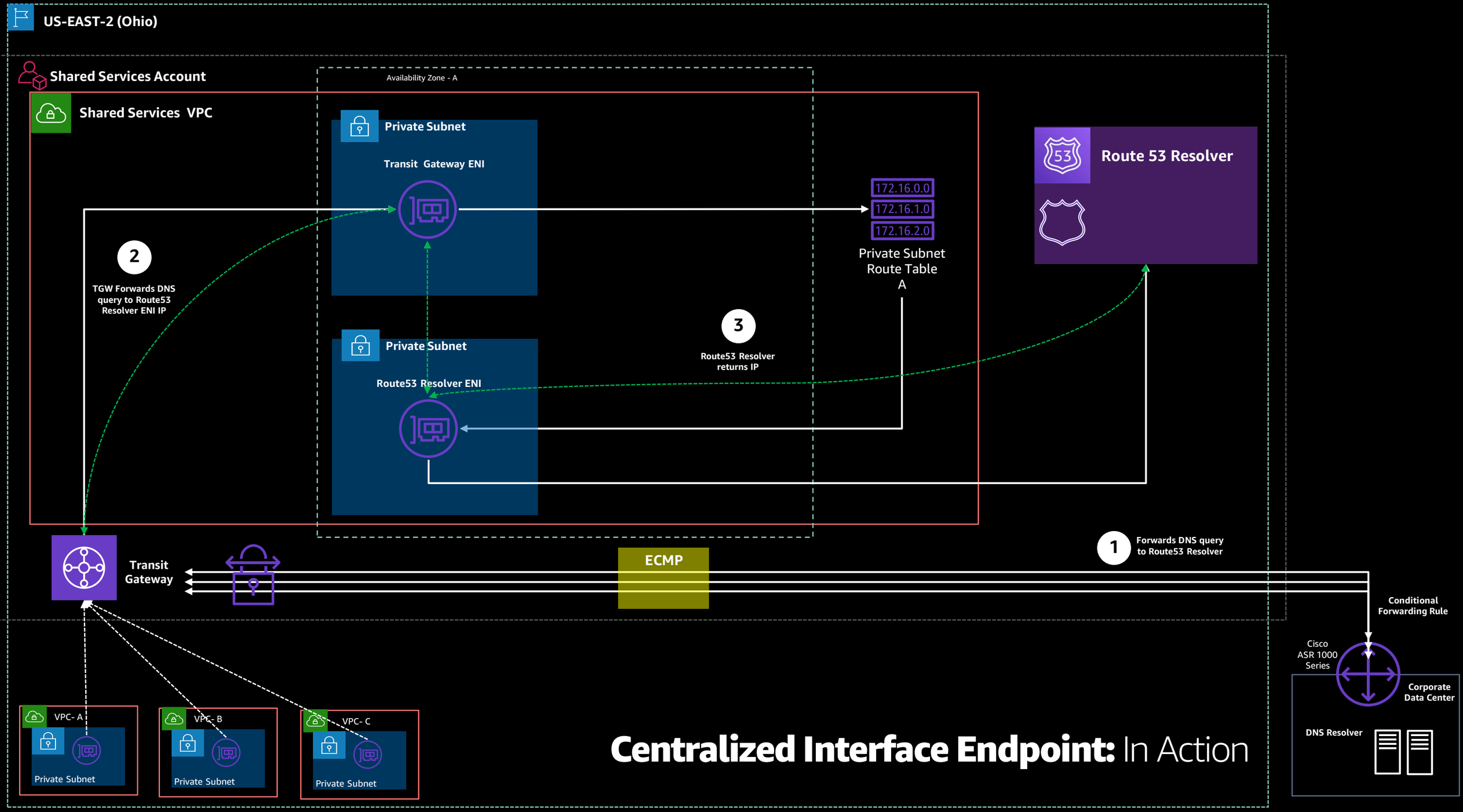
Centralization via Transit Gateway & Route 53

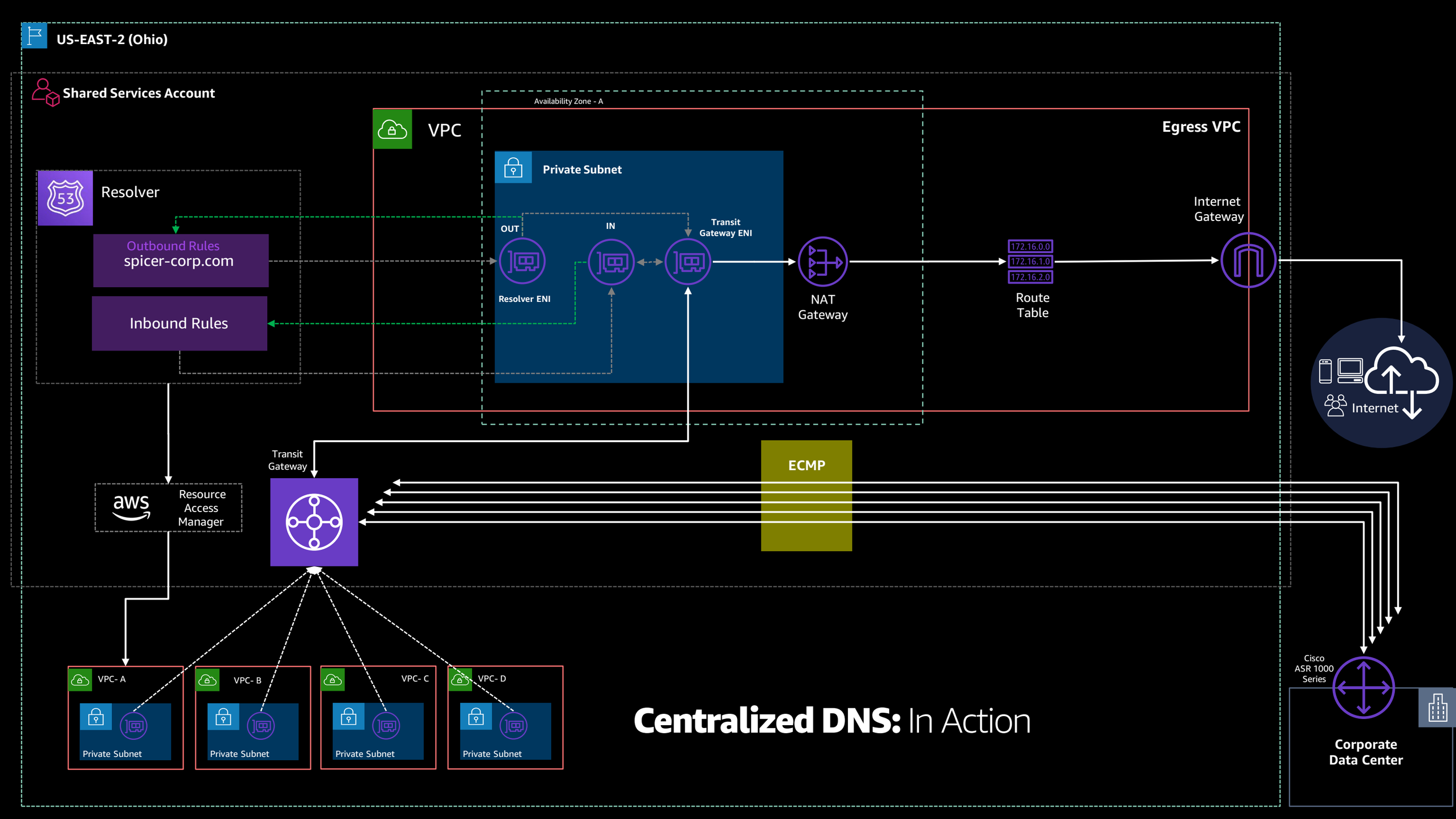
Requirement 3c: Access to AWS Public Services

AWS re:Invent

aws


US-EAST-2 (Ohio)
Shared Services Account
Shared Services VPC
Availability Zone - A
Availability Zone - B
Private Subnet – A
Private Subnet - C
Interface Endpoint ENI
172.16.10.57/32
Interface Endpoint ENI
172.16.10.57/32
Security Group
Ensure Private DNS is disabled
Create VPC Endpoint
1
aws ec2 create-vpc-endpoint --vpc-id vpc-s1727abc
--vpc-endpoint-type Interface
--service-name com.amazonaws.us-east-2.sqs
--subnet-id subnet-abababab subnet-xyzbderpg
--security-group-id sg-1a2b3c4d
Endpoint DNS Hostnames
vpce-074451a3df85400e8-pgpul6mf.sqs.us-west-2.vpce.amazonaws.com
vpce-074451a3df85400e8-pgpul6mf-us-west-2a.sqs.us-west-2.vpce.amazonaws.com
vpce-074451a3df85400e8-pgpul6mf-us-west-2b.sqs.us-west-2.vpce.amazonaws.com
vpce-074451a3df85400e8-pgpul6mf-us-west-2c.sqs.us-west-2.vpce.amazonaws.com
Hosted Zone Details
Domain Name: sqs.us-west-2.amazonaws.com.
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: Z044524929AE7UA352OBF
Record Set Count: 3
Comment:
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPCs: VPC-Blog-AWS | vpc-0ea8cd5d0eb03146d | us-west-2
LH Prod. VPC | vpc-9236c9f5 | us-west-2
VPC ID:
VPC ID | VPC region
Important
To use private hosted zones, you must set the following Amazon VPC settings to true:
enableDnsHostnames
enableDnsSupport
Learn more
2
Create a Private Hosted Zone for the AWS service using the full service endpoint name . In this example, I am creating a private hosted zone for Amazon SQS
3
Create an A Record that points to an alias. The entered alias should be the VPC Endpoint Regional DNS hostname
4
Associate VPCs in the same account and other accounts with the Private Hosted Zone
5
Create an inbound Rule in your Route53 Resolver
Edit Record Set
Name: sqs.us-west-2.amazonaws.com.
Type: A – IPv4 address
Alias: Yes No
Alias Target: vpce-074451a3df85400e8-pgpul6mf.s


US-EAST-2 (Ohio)
Shared Services Account
Availability Zone - A
Shared Services VPC
Private Subnet
Transit Gateway ENI
172.16.0.0
172.16.1.0
172.16.2.0
Private Subnet Route Table A
Route 53 Resolver
2
TGW Forwards DNS query to Route53 Resolver ENI IP
3
Route53 Resolver returns IP
Private Subnet
Route53 Resolver ENI
Transit Gateway
ECMP
1
Forwards DNS query to Route53 Resolver
Conditional Forwarding Rule
Cisco ASR 1000 Series
Corporate Data Center
DNS Resolver
VPC- A
Private Subnet
VPC- B
Private Subnet
VPC- C
Private Subnet
Centralized Interface Endpoint: In Action


US-EAST-2 (Ohio)
Shared Services Account
Availability Zone - A
VPC
Egress VPC
Private Subnet
Resolver
Outbound Rules
spicer-corp.com
Inbound Rules
OUT
IN
Transit Gateway ENI
Resolver ENI
NAT Gateway
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Internet Gateway
Internet
Transit Gateway
ECMP
aws
Resource Access Manager
VPC- A
VPC- B
VPC- C
VPC- D
Private Subnet
Private Subnet
Private Subnet
Private Subnet
Cisco ASR 1000 Series
Corporate Data Center
Centralized DNS: In Action

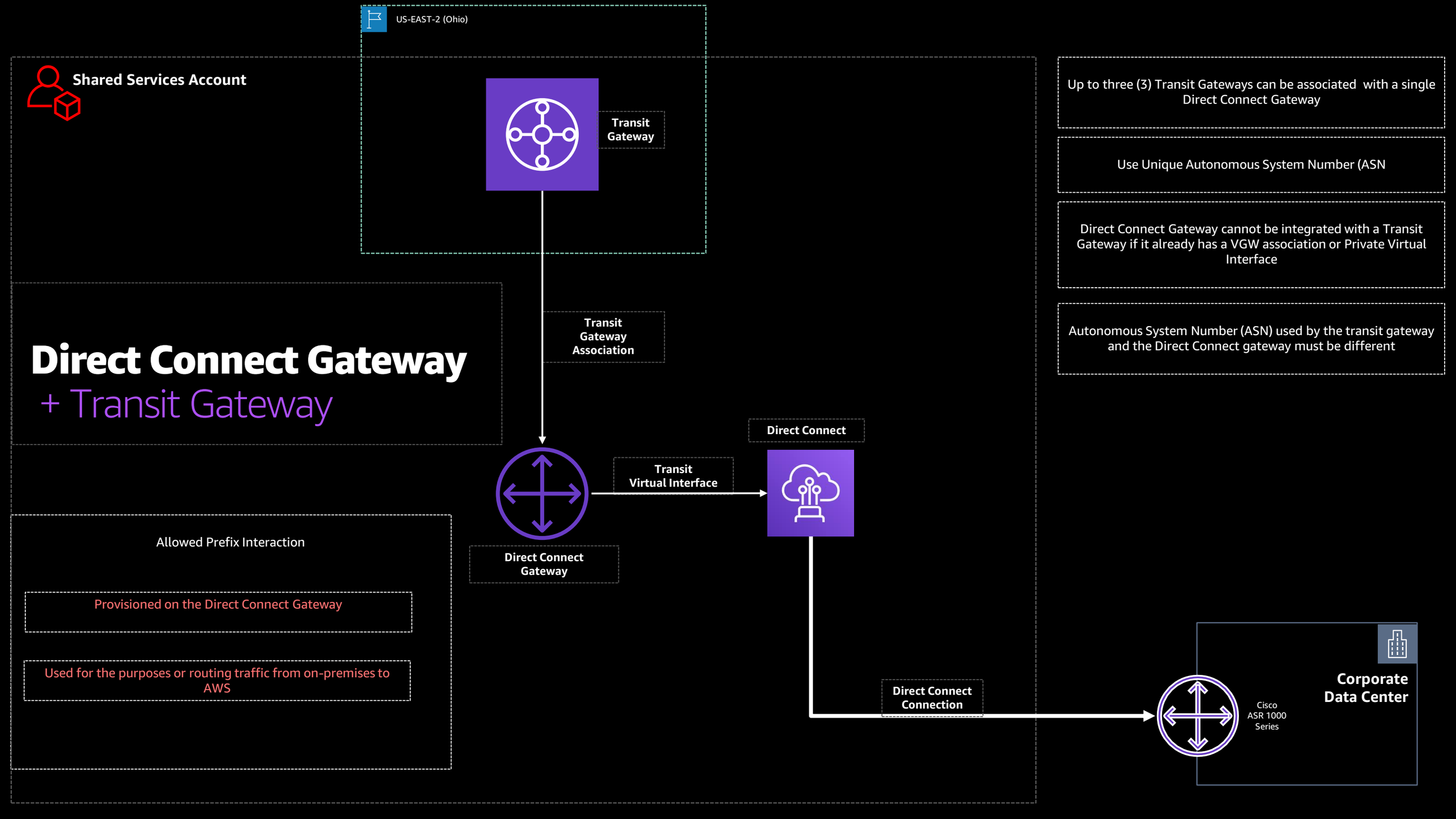
Multi-Region Transit Architectures

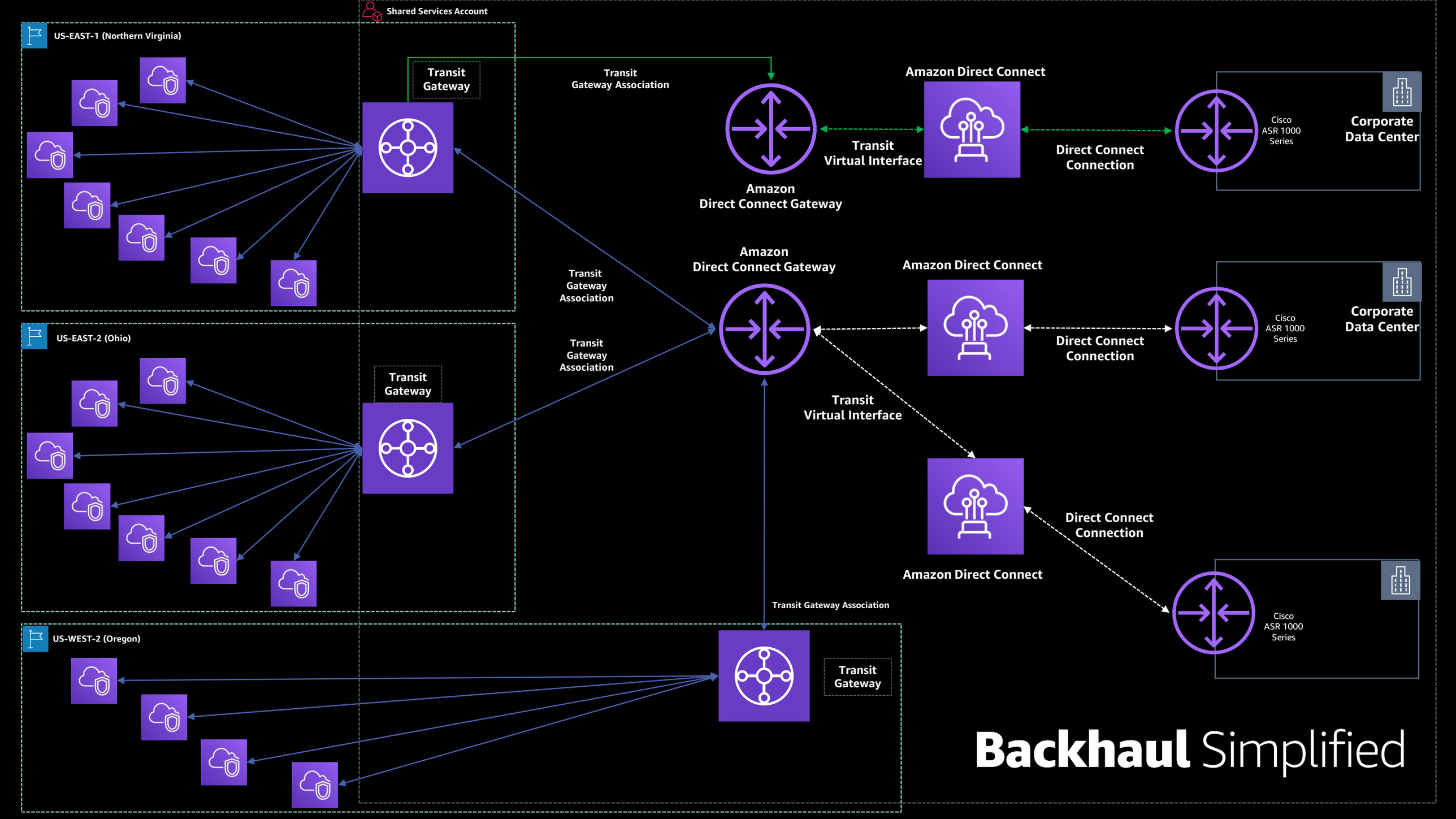
via Transit Gateway & Direct Connect Gateway

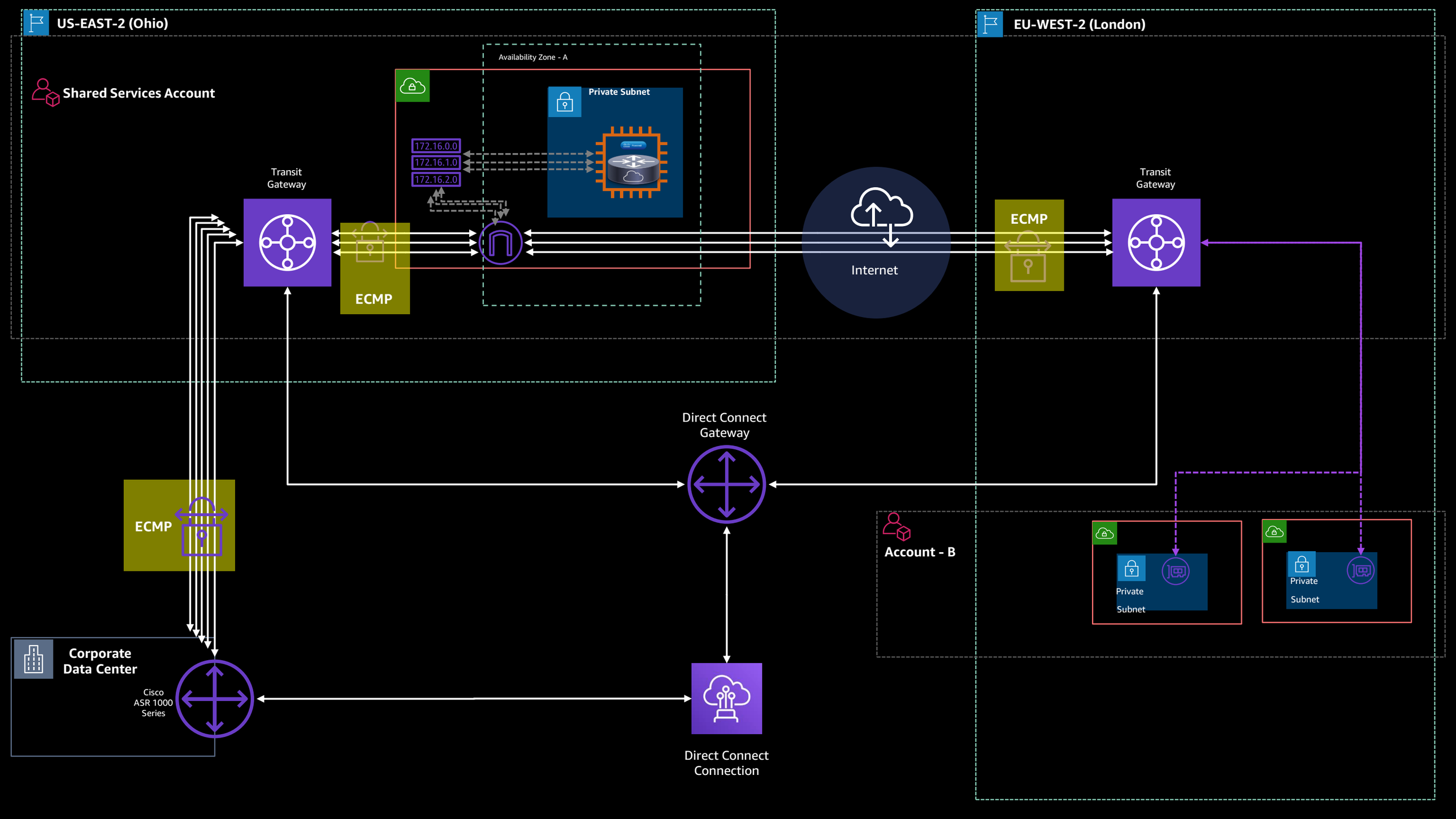
Requirement 3d: Accessing resources on premises from any AWS Region

AWS re:Invent

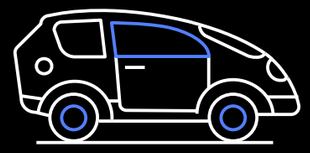
aws


US-EAST-2 (Ohio)
Shared Services Account
Transit Gateway
Transit Gateway Association
Direct Connect Gateway + Transit Gateway
Direct Connect
Transit Virtual Interface
Direct Connect Gateway
Allowed Prefix Interaction
Provisioned on the Direct Connect Gateway
Used for the purposes or routing traffic from on-premises to AWS
Direct Connect Connection
Cisco ASR 1000 Series
Corporate Data Center
Up to three (3) Transit Gateways can be associated with a single Direct Connect Gateway
Use Unique Autonomous System Number (ASN
Direct Connect Gateway cannot be integrated with a Transit Gateway if it already has a VGW association or Private Virtual Interface
Autonomous System Number (ASN) used by the transit gateway and the Direct Connect gateway must be different


Shared Services Account
US-EAST-1 (Northern Virginia)
Transit Gateway
Transit Gateway Association
Amazon Direct Connect
Amazon Direct Connect Gateway
Transit Virtual Interface
Direct Connect Connection
Cisco ASR 1000 Series
Corporate Data Center
US-EAST-2 (Ohio)
Transit Gateway
Transit Gateway Association
Amazon Direct Connect Gateway
Amazon Direct Connect
Direct Connect Connection
Cisco ASR 1000 Series
Corporate Data Center
Transit Virtual Interface
Amazon Direct Connect
Direct Connect Connection
Cisco ASR 1000 Series
Transit Gateway Association
US-WEST-2 (Oregon)
Transit Gateway
Backhaul Simplified

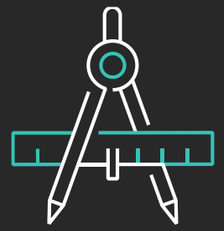

US-EAST-2 (Ohio)
EU-WEST-2 (London)
Shared Services Account
Availability Zone - A
Private Subnet
172.16.0.0
172.16.1.0
172.16.2.0
Transit Gateway
ECMP
Internet
ECMP
Transit Gateway
Direct Connect Gateway
ECMP
Account - B
Private Subnet
Private Subnet
Corporate Data Center
Cisco ASR 1000 Series
Direct Connect Connection

In conclusion .....



Learn to architect with AWS Training and Certification

Resources created by the experts at AWS to propel your organization and career forward



Free foundational to advanced digital courses cover AWS services and teach architecting best practices

Classroom offerings, including Architecting on AWS, feature AWS expert instructors and hands-on labs

Validate expertise with the **AWS Certified Solutions Architect - Associate** or **AWS Certification Solutions Architect - Professional** exams

Visit aws.amazon.com/training/path-architecting/

aws training and certification

Thank you!

Androski Spicer

androsks@amazon.com

Please complete the session survey in the mobile app.