Networking in AWS

Chetan Agrawal, Solutions Architect
Deven Suri, Account Manager

31-Jul-2020

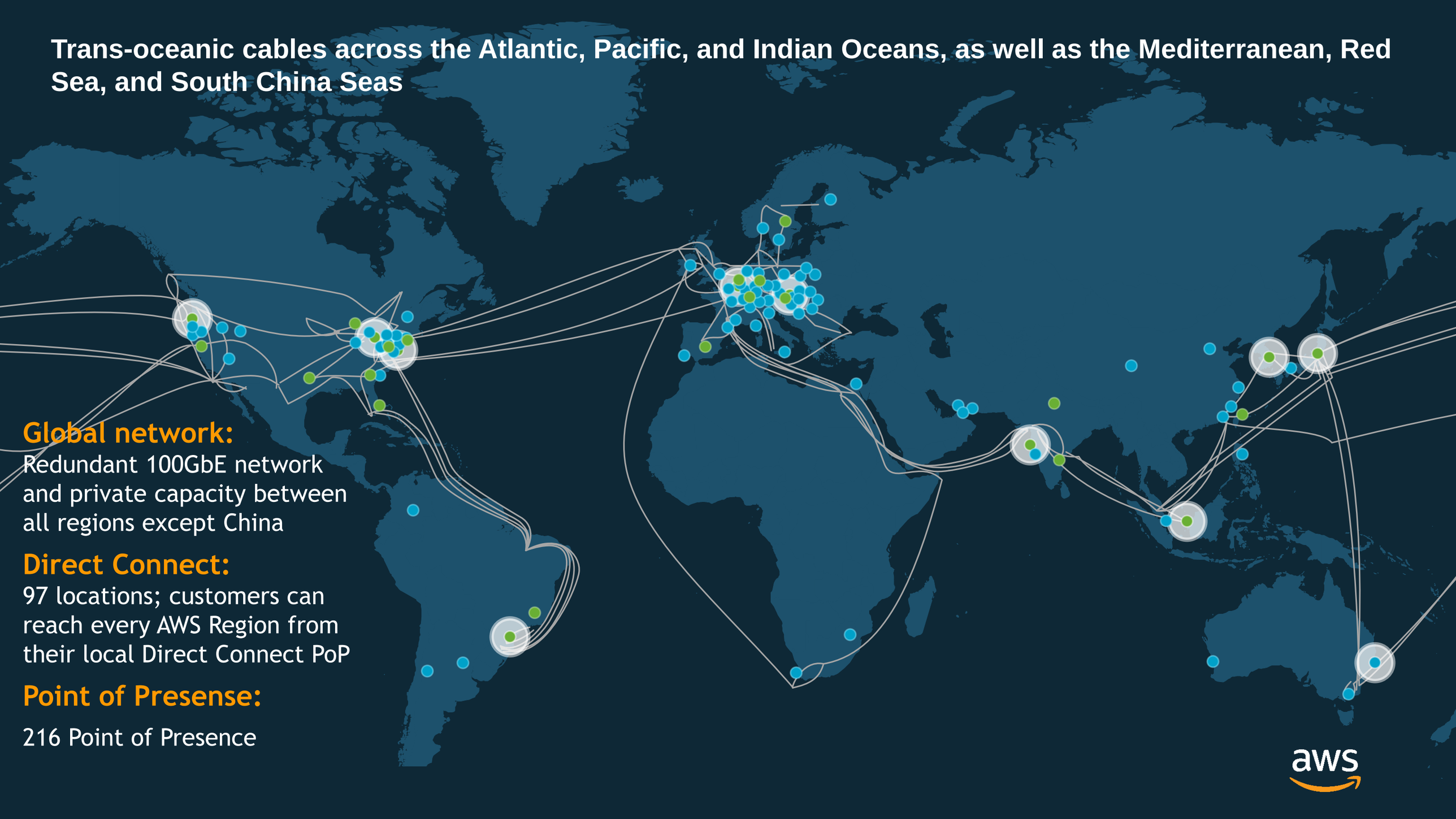
Agenda

- AWS Global Network
- Amazon VPC – Virtual Private Cloud
- VPC Building Blocks
    - VPC, Subnets, Route Tables
    - Demo (Walkthrough)
- VPC Connectivity Options
    - VPC Endpoint (Demo)
    - VPC Peering (Demo)
    - Transit Gateway
- Connect your Data Center to AWS
    - AWS Managed VPN
    - AWS Direct Connect

aws

24 Regions, 77 availability zones, 1 local Region

Trans-oceanic cables across the Atlantic, Pacific, and Indian Oceans, as well as the Mediterranean, Red Sea, and South China Seas



Global network:

Redundant 100GbE network and private capacity between all regions except China

Direct Connect:

97 locations; customers can reach every AWS Region from their local Direct Connect PoP

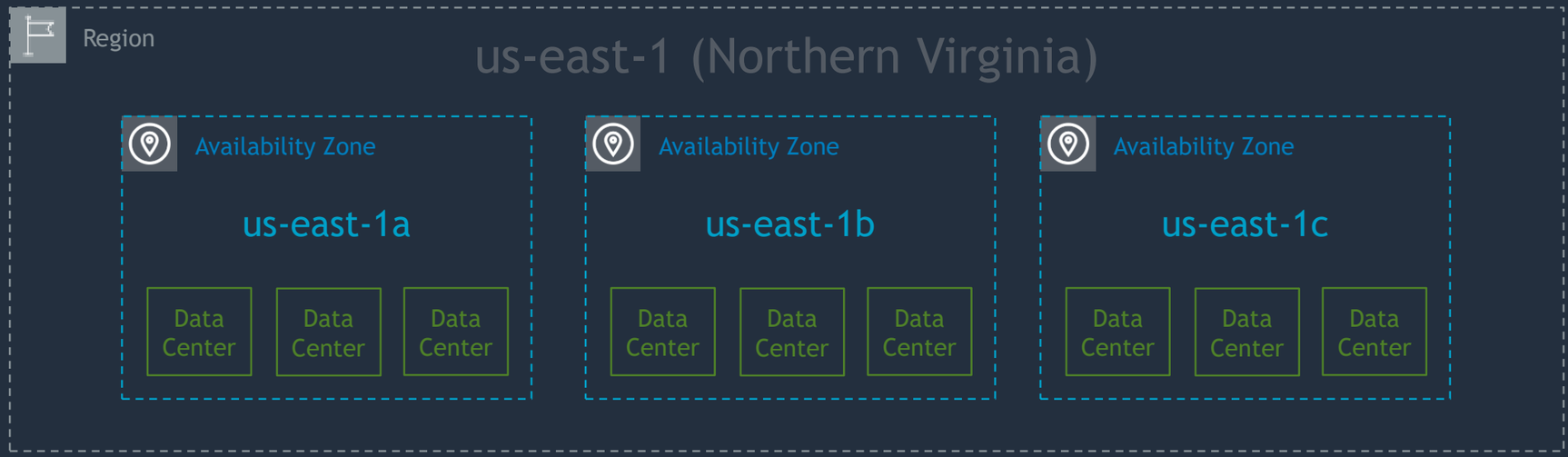
Point of Presense:

216 Point of Presence

aws

Availability Zones

- A region is comprised of multiple Availability Zones (typically 3)
- Fully independent partitions on isolated fault lines, flood plains, and power grids
- Each AZ: redundant power and redundant dedicated network
- Each AZ: typically multiple data centers
- Between AZs: high throughput, low latency (<10ms) network
- Between AZs: physical separation < 100km (60mi)



aws

Amazon VPC

aws

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

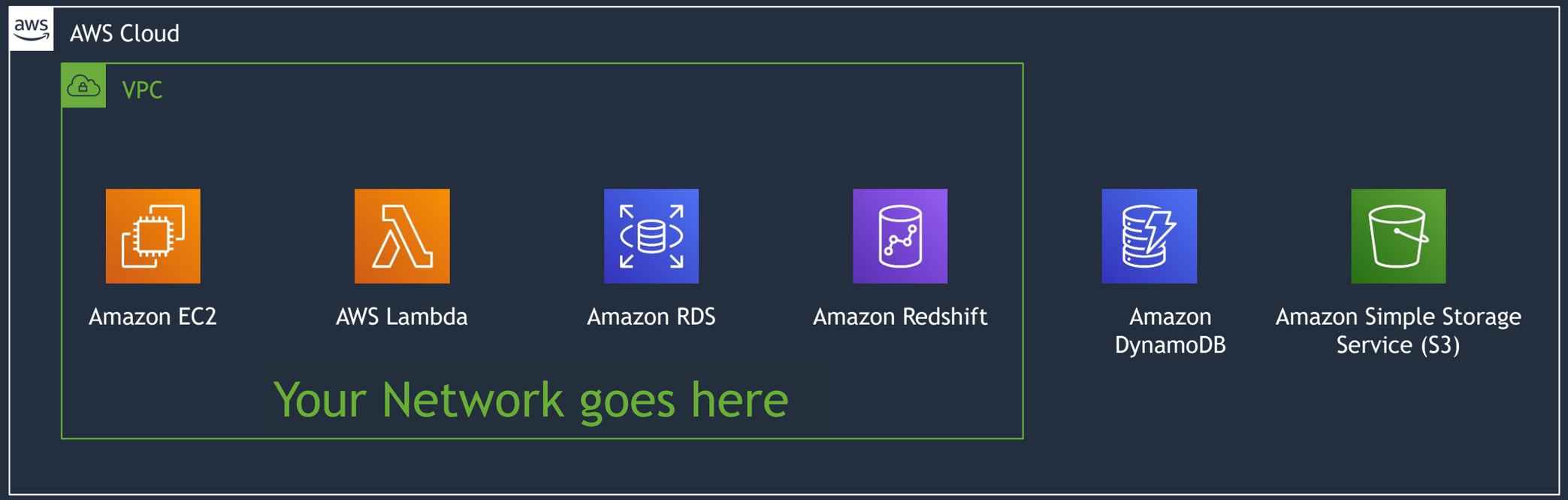
Network Topology

Routing Rules

Security Rules

aws

Amazon Virtual Private Cloud (VPC)



Choosing an IP address range for your VPC

VPC CIDR

Make sure you chose correct CIDR while creating VPC

10.0.0.0/16

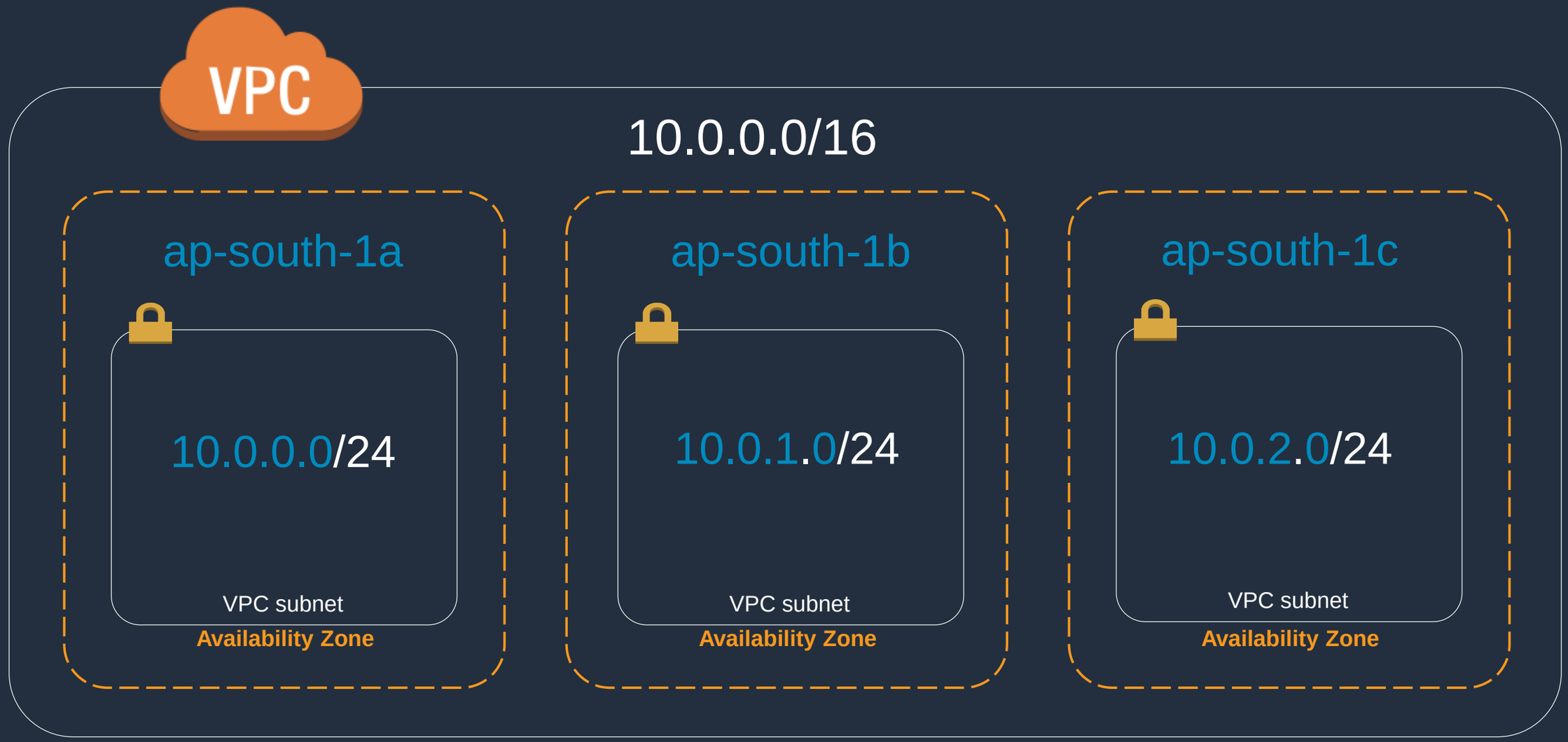
Recommended: RFC1918 range

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Appropriately sized CIDR (example /16 = 65536 IP addresses)

aws

VPC subnets and Availability Zones



aws

VPC subnet recommendations

- Appropriately sized VPCs
  - /16 largest (65,536 addresses)
  - /28 smallest (16 addresses)
- At least /24 subnets (256 addresses)
  - Can be as small as /28 (16 addresses)
  - Note: AWS reserves five IP addresses out of the CIDR (first four and last)
- Use multiple Availability Zones per VPC through multiple subnets

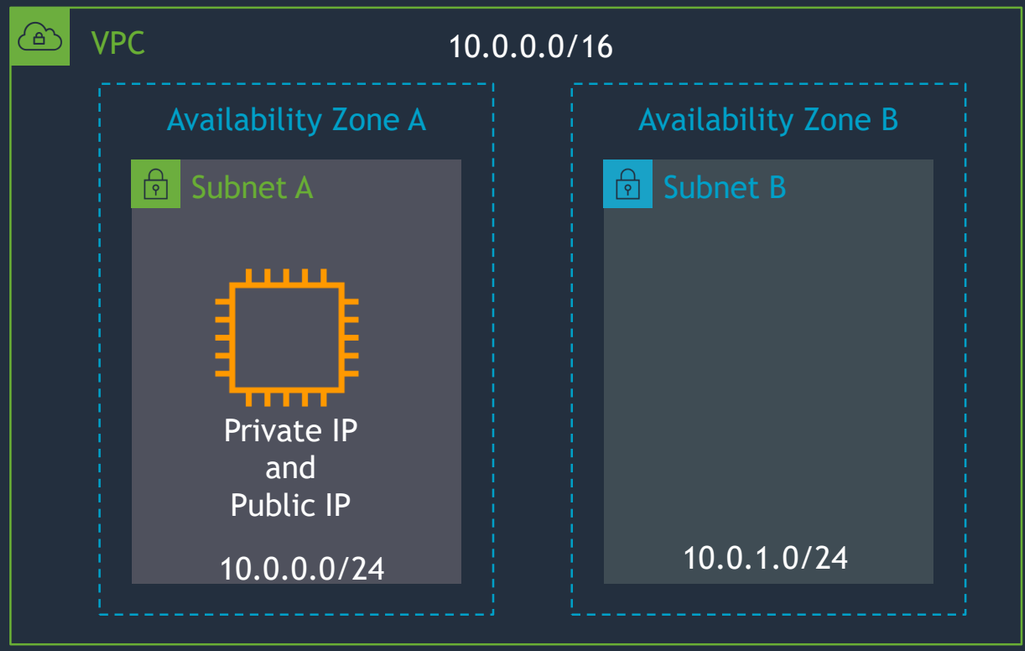
aws

VPC Building Blocks

aws

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
- Example: CIDR = 10.0.0.0/24
- Subnet also has attribute “Auto Assign Public IP” for instances

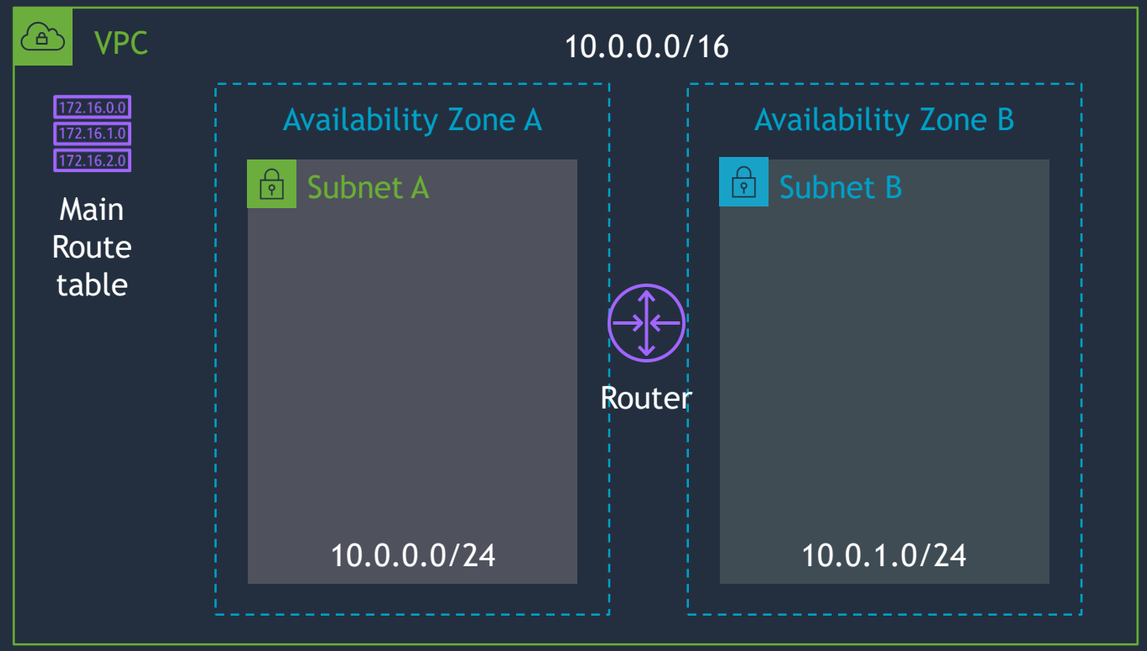


aws

How to route traffic inside a VPC?

Route Table

- Every VPC comes with default Route table called “Main” route table
- All subnets are by default associated with this main Route table.
- Route table has “Local Route” entry which enables communication within VPC

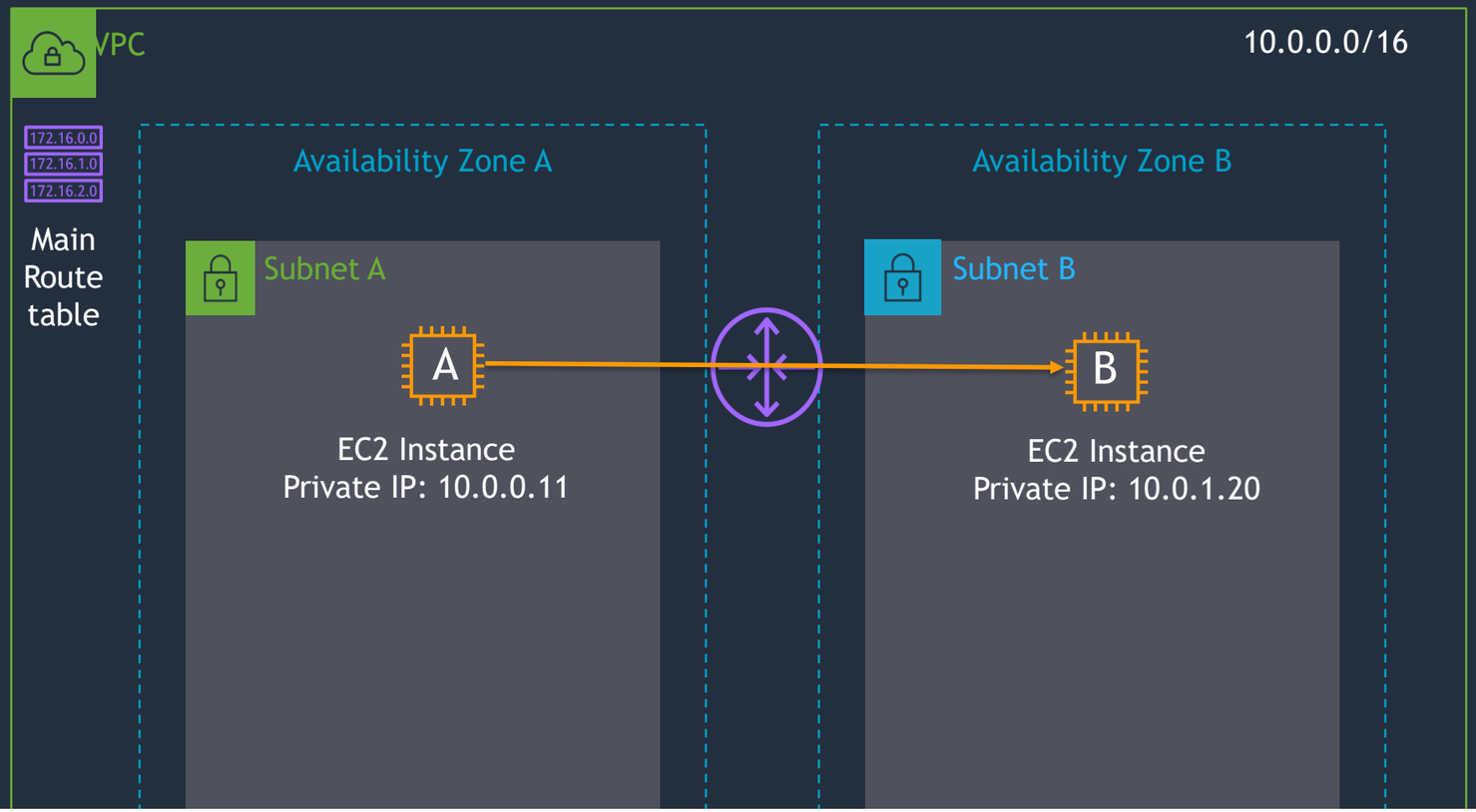


View: All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

aws

Can EC2 instance A talk to instance B?

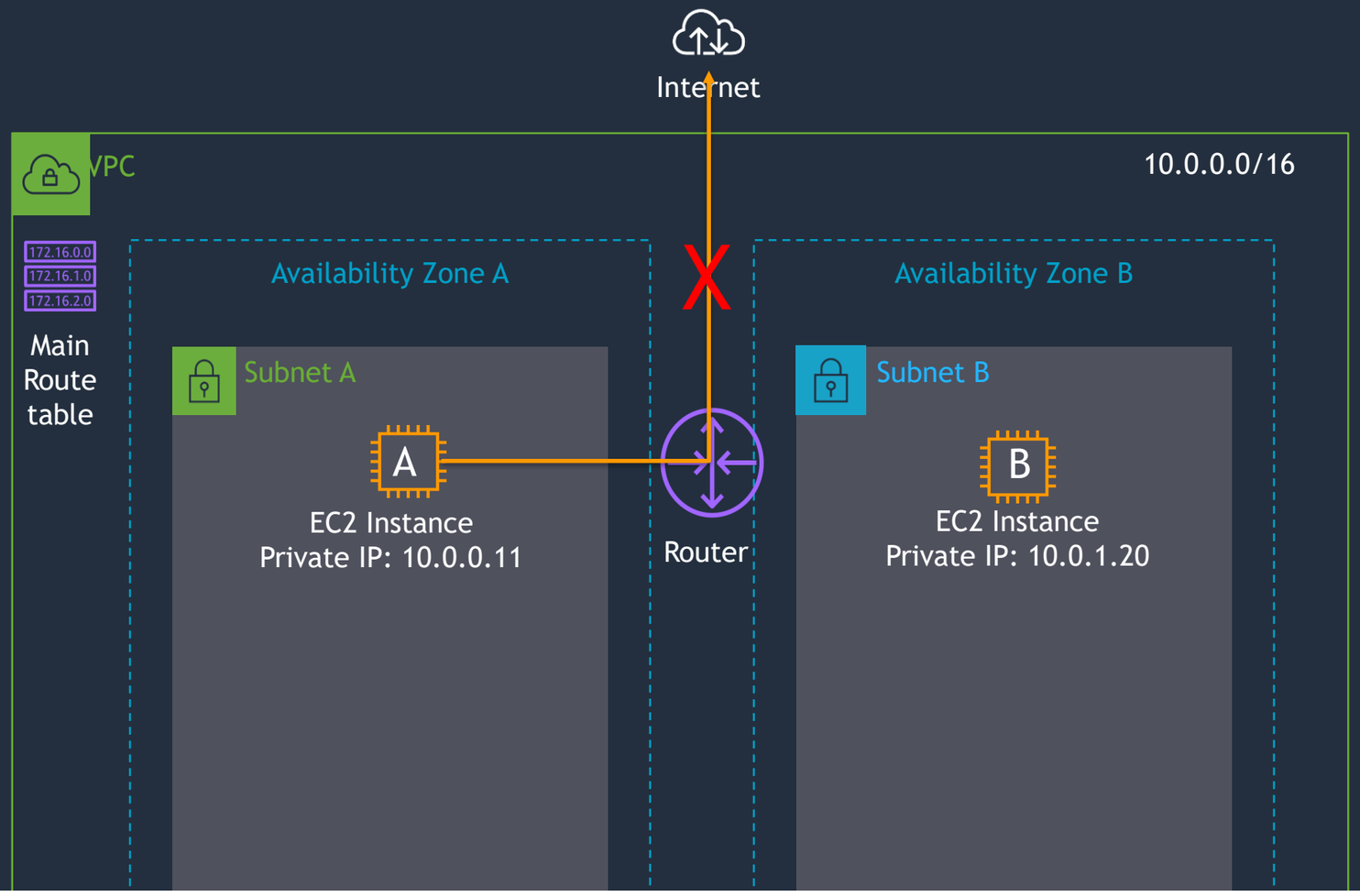


View: All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

aws

Can EC2 instance A talk to internet?



View: All routes

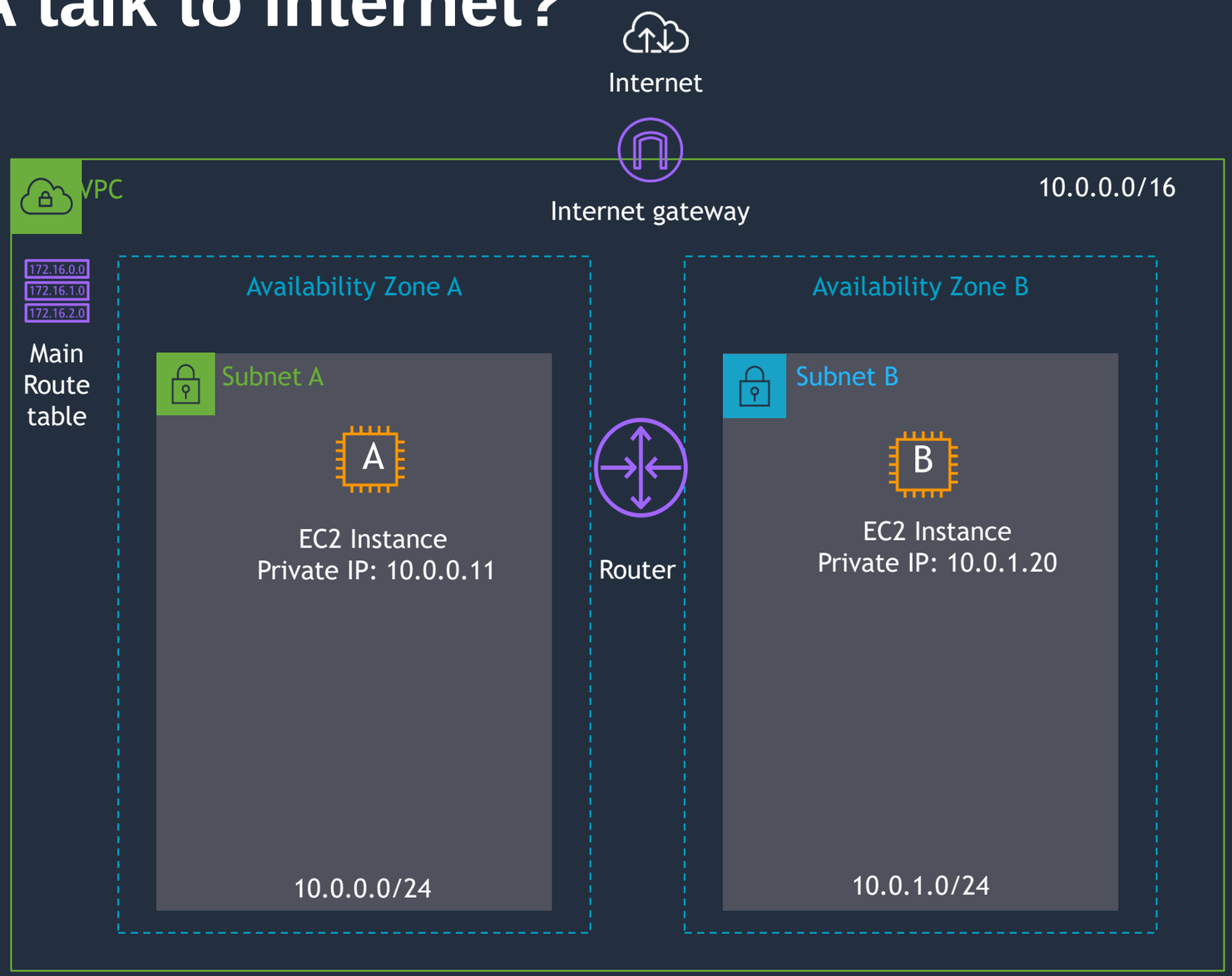
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

aws

How can EC2 instance A talk to internet?

Internet Gateway

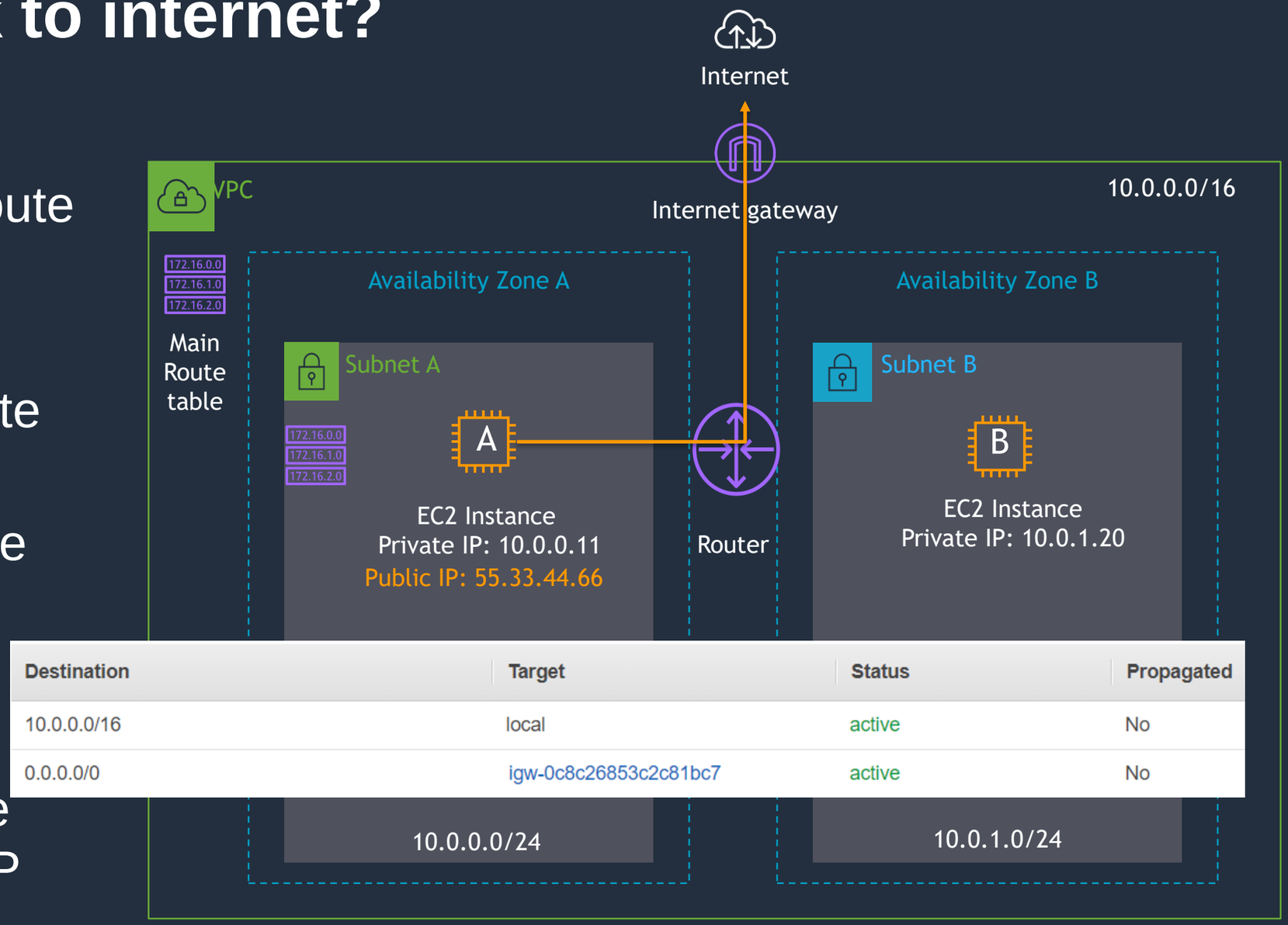
- Horizontally scaled, redundant, highly available VPC component
- Connect your VPC Subnets to the Internet
- Must be referenced on the Route Table
- Performs NAT between Public and Private IP Addresses



aws

Can now EC2 A talk to internet?

- No, unless you modify route table
- 2 options we have
    1. Modify Main Route Table
    2. Create new Route table for subnet
- Can EC2 now talk to internet?
- No, unless EC2 instance also has Public/Elastic IP

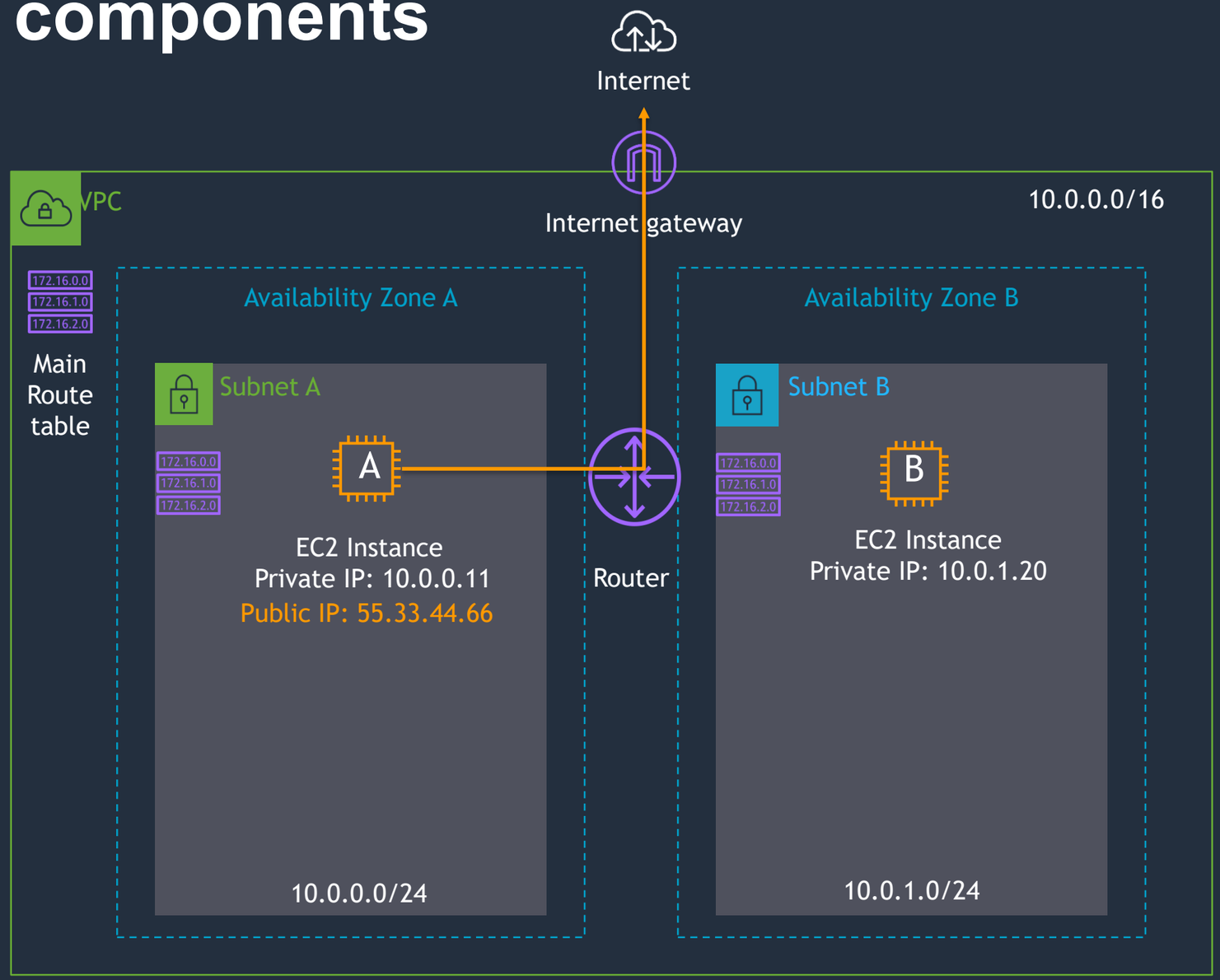


Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0c8c26853c2c81bc7	active	No

aws

Let’s create VPC and all components we discussed

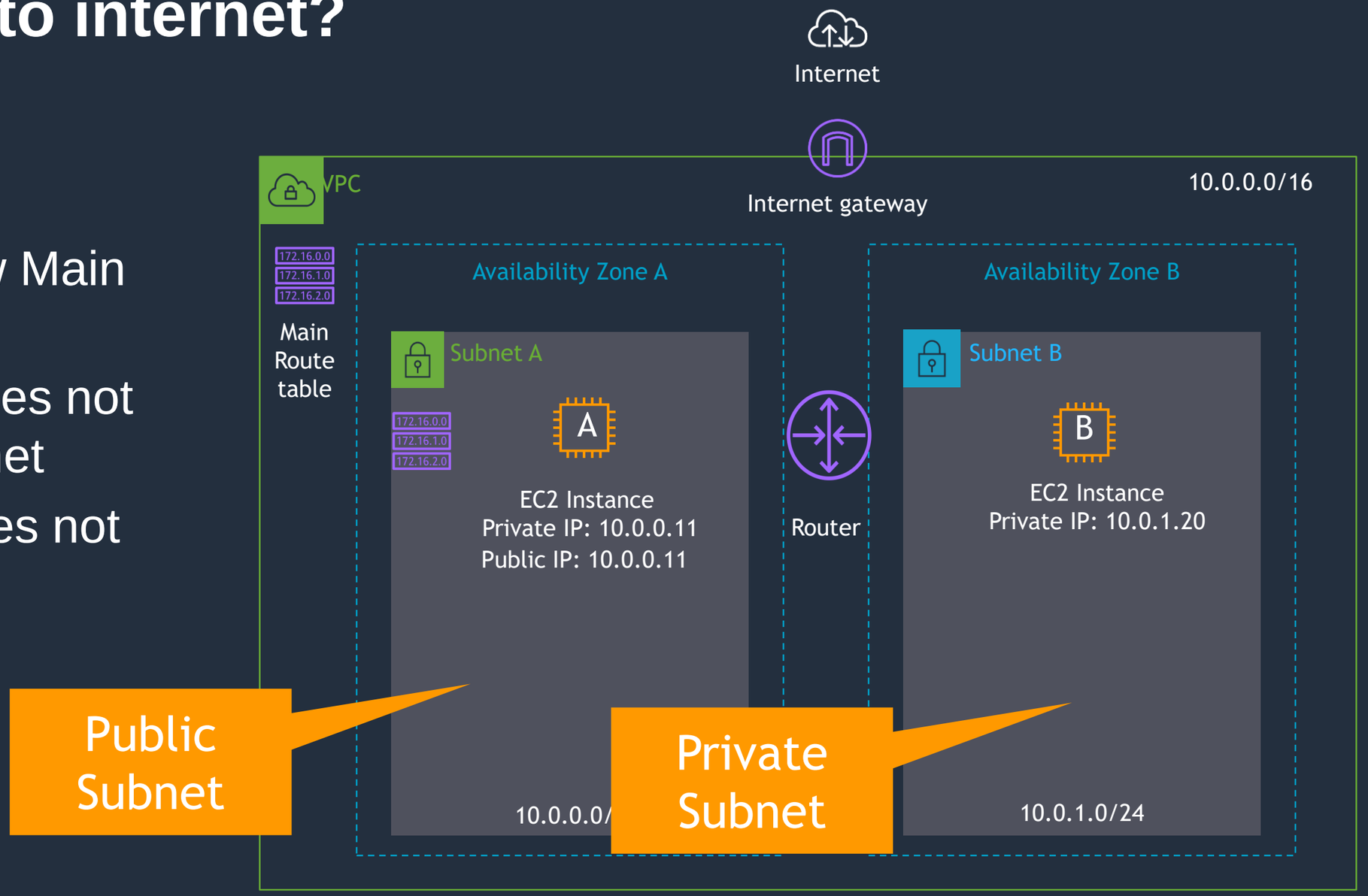
1. Create VPC (10.0.0.0/16)
2. Create Internet Gateway
3. Create Subnet A (10.0.0.0/24)
4. Create Subnet B (10.0.1.0/24)
5. Create Route Table A (Public)
6. Create Route Table B (Private)
7. Launch EC2 instances in both the subnets
8. Connect to EC2-A
9. From there connect to EC2-B



aws

Can EC2 B talk to internet?

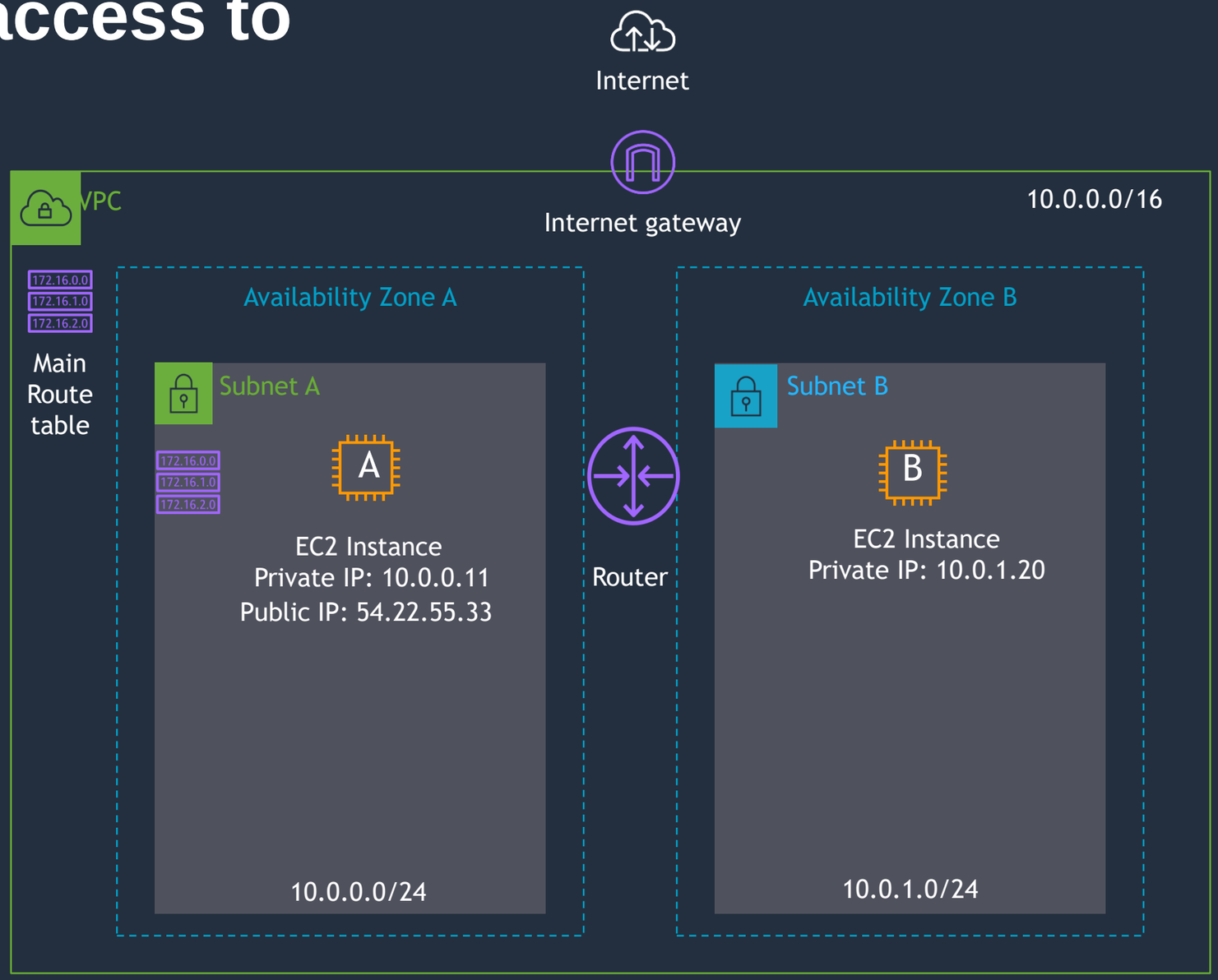
- No, because ..
- Subnet B still follow Main route table
- Main route table does not have route to internet
- EC2 B instance does not have Public IP



How to enable internet access to instance B?

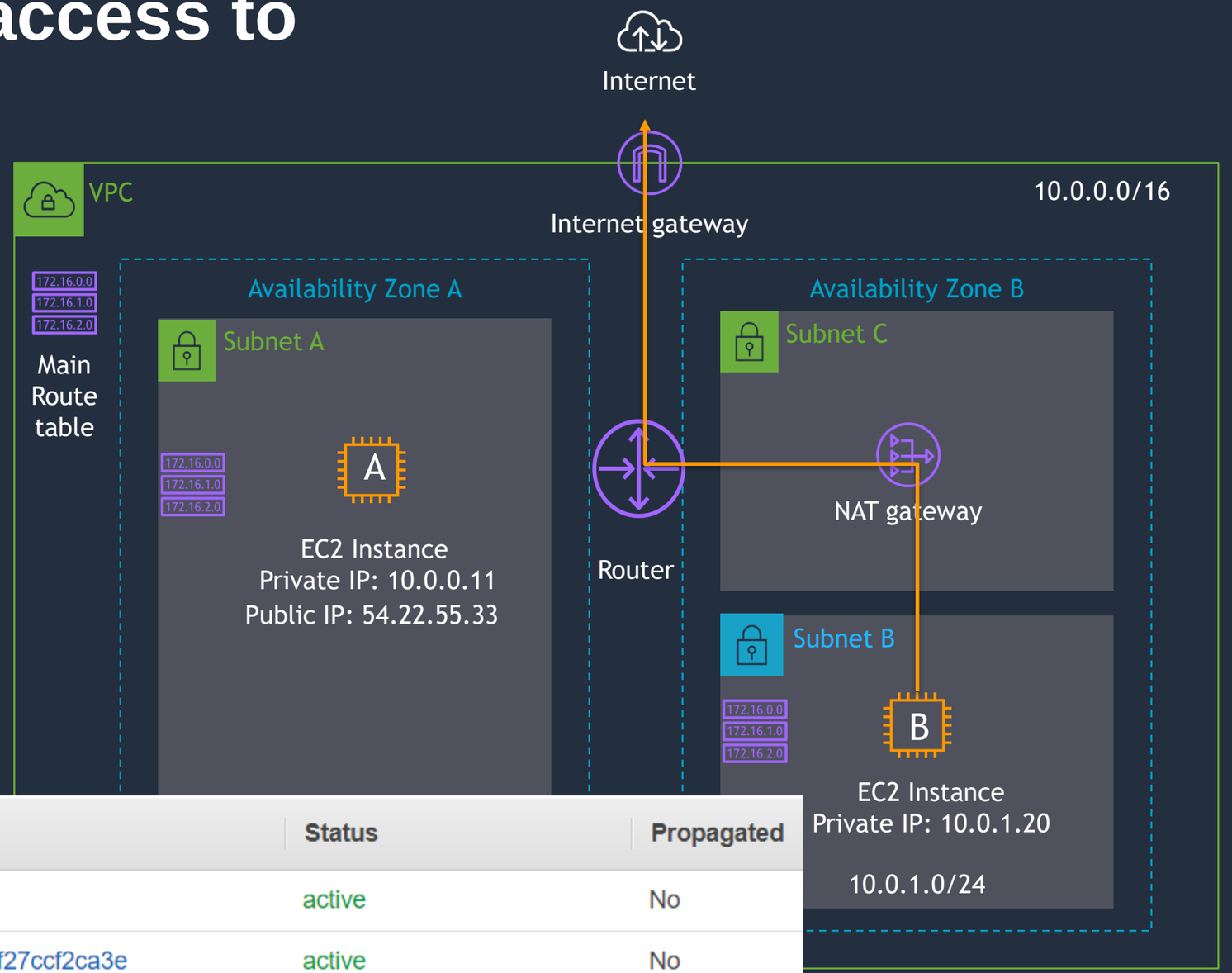
NAT Gateway

- 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 10Gbps bandwidth
- Supports TCP, UDP, and ICMP protocols
- Network ACLs apply to NAT gateway's traffic



How to enable internet access to instance B?

- Modify Subnet B route table to route internet traffic through NAT gateway

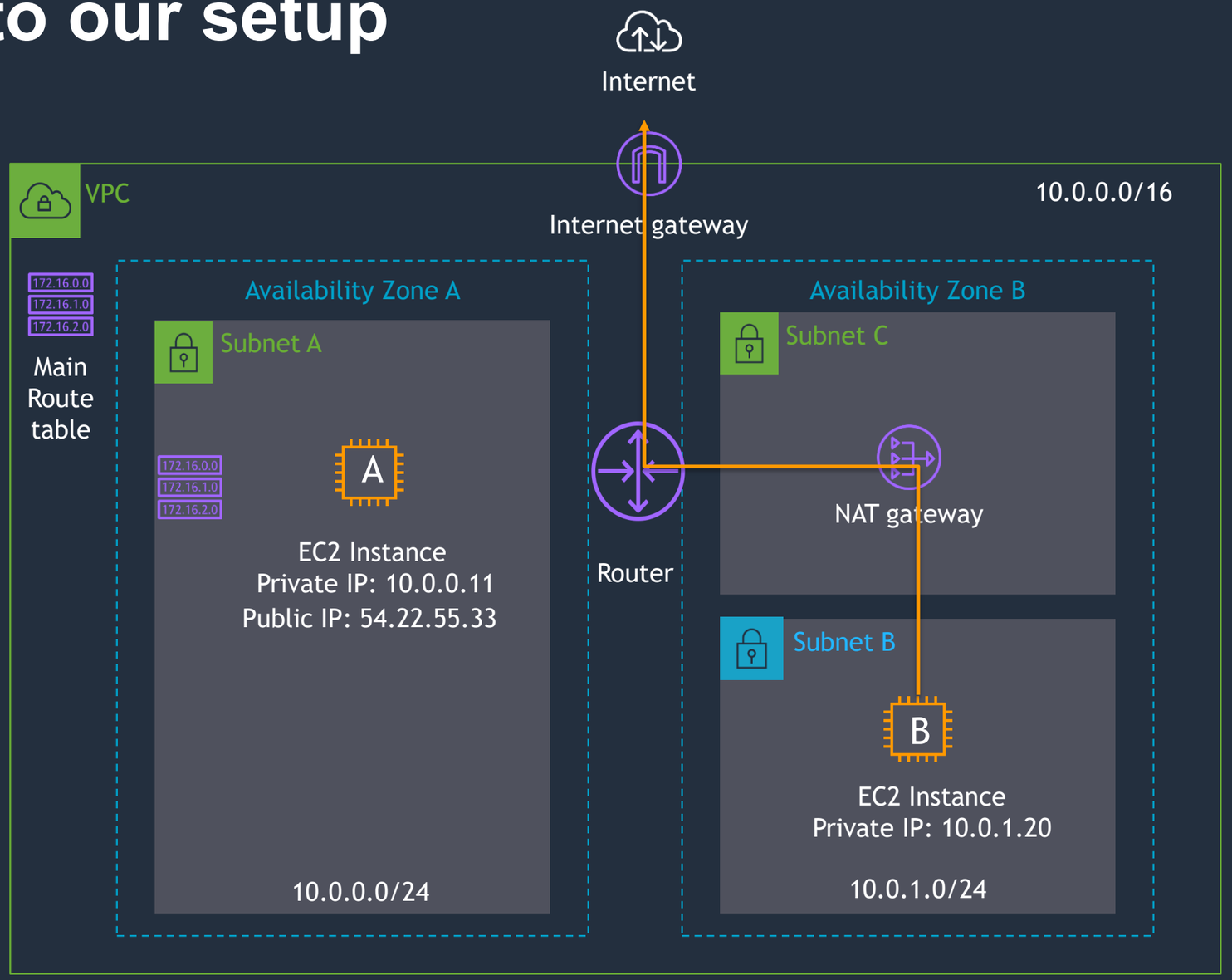


Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-085190f27ccf2ca3e	active	No

aws

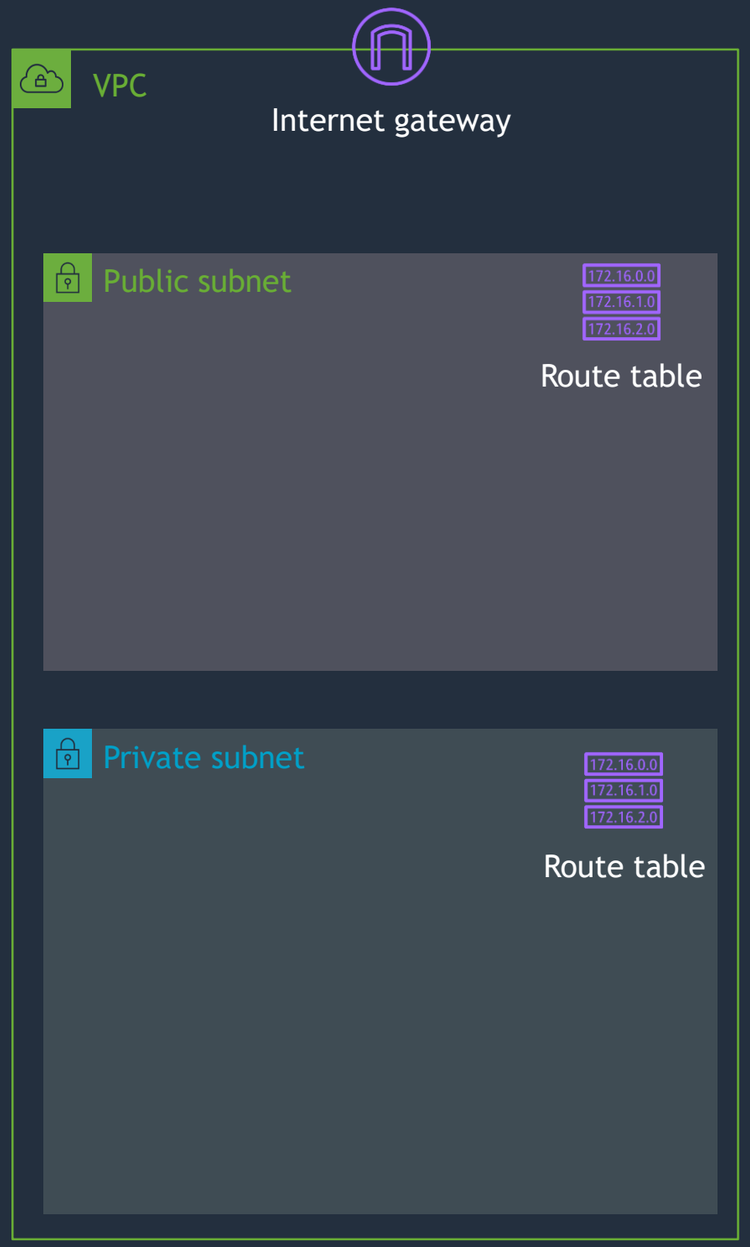
Let’s add NAT gateway to our setup

1. Create NAT Gateway
2. Modify Private Route table of Subnet B and add route for internet via NAT Gateway
3. Try to access internet from EC2-B



VPC routing summary

- Route Tables direct traffic out of the VPC, towards:
  - Internet Gateway
  - Virtual Private Gateway
  - VPC Endpoints
  - Direct Connect
  - VPC Peering
  - AWS Transit Gateway



aws

VPC Security

aws

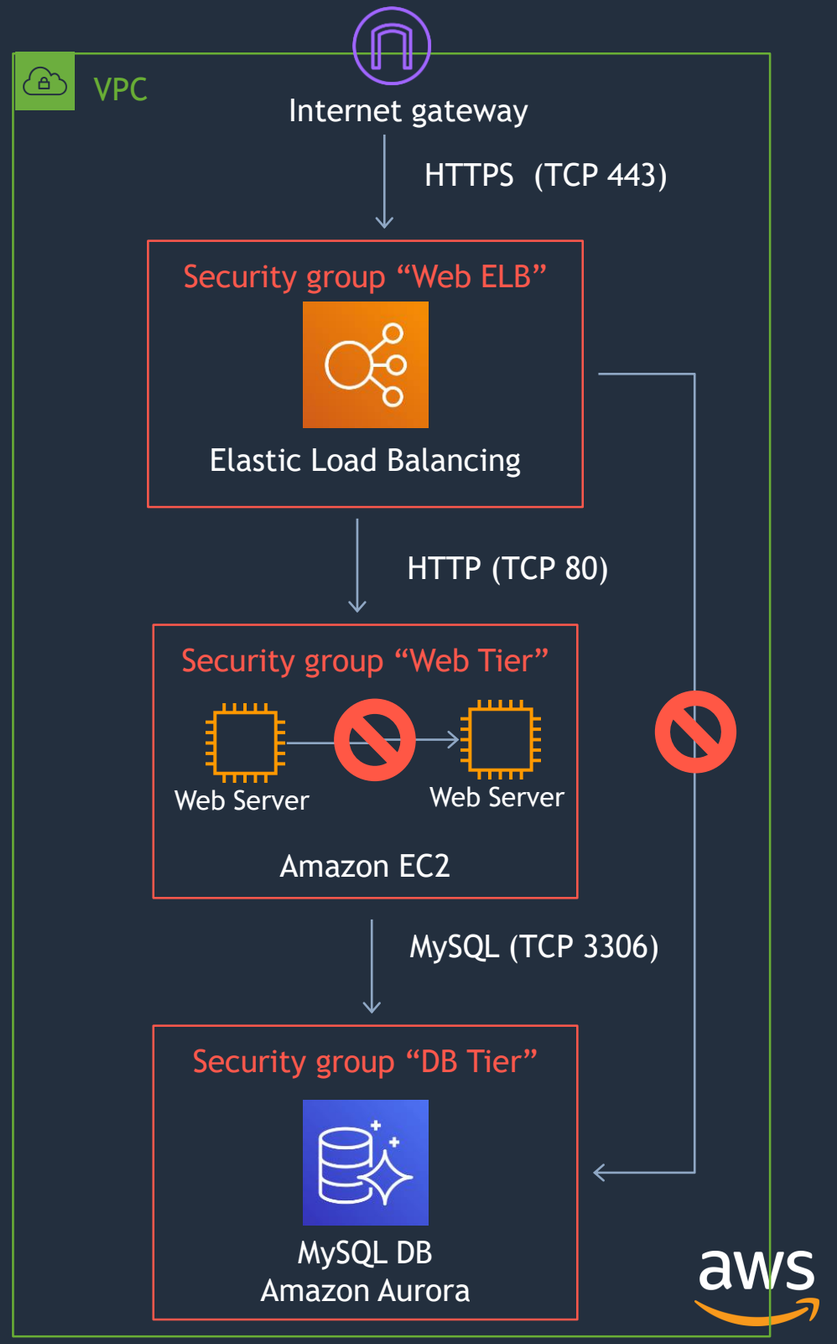
Can I filter traffic reaching my instances?

Security Groups

- Virtual stateful firewall
- Inbound and Outbound customer defined rules
- Mandatory, all instances have an associated Security Group
- Only supports allow rules

Outbound rules

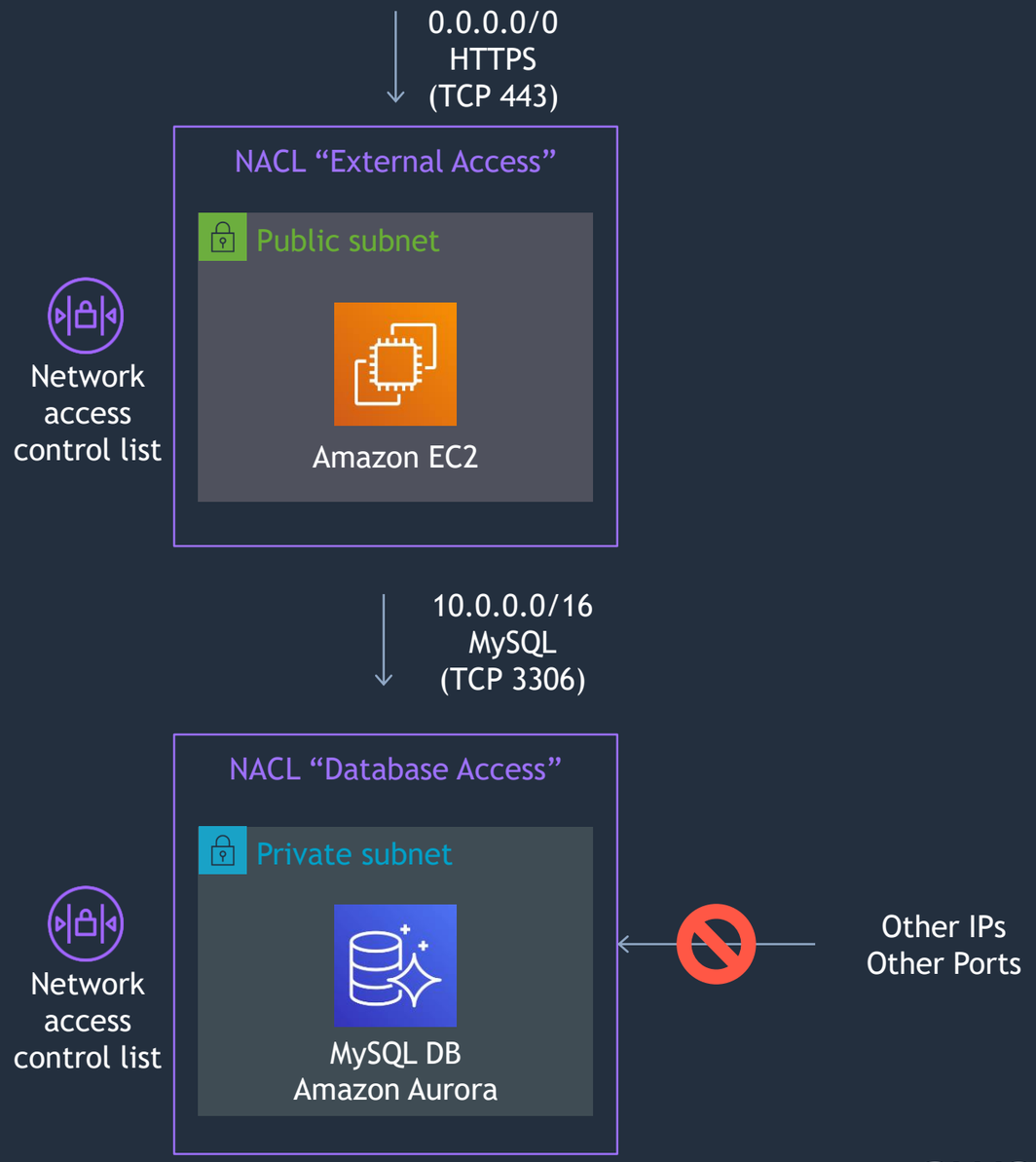
Type	Protocol	Port range	Destination
All traffic	All	All	0.0.0.0/0



Can I filter traffic on a subnet level?

Network Access Control List

- Inbound and Outbound
- Subnet level inspection
- Optional level of security
- By default, allow all traffic
- Stateless
- IP and TCP/UDP port based
- Supports allow and deny rules
- Deny all at the end

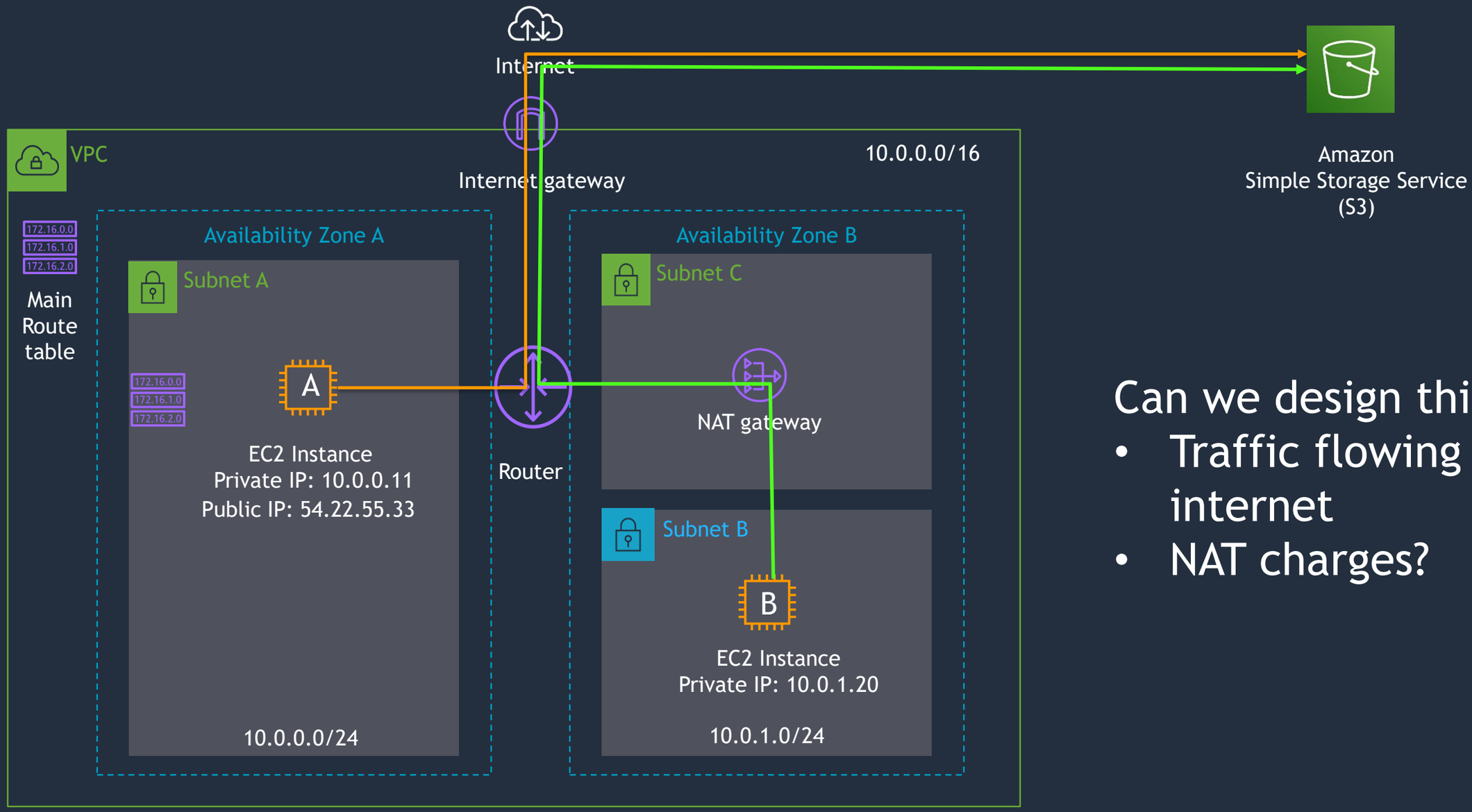


aws

VPC Connectivity Options

aws

How to access AWS services from VPC?

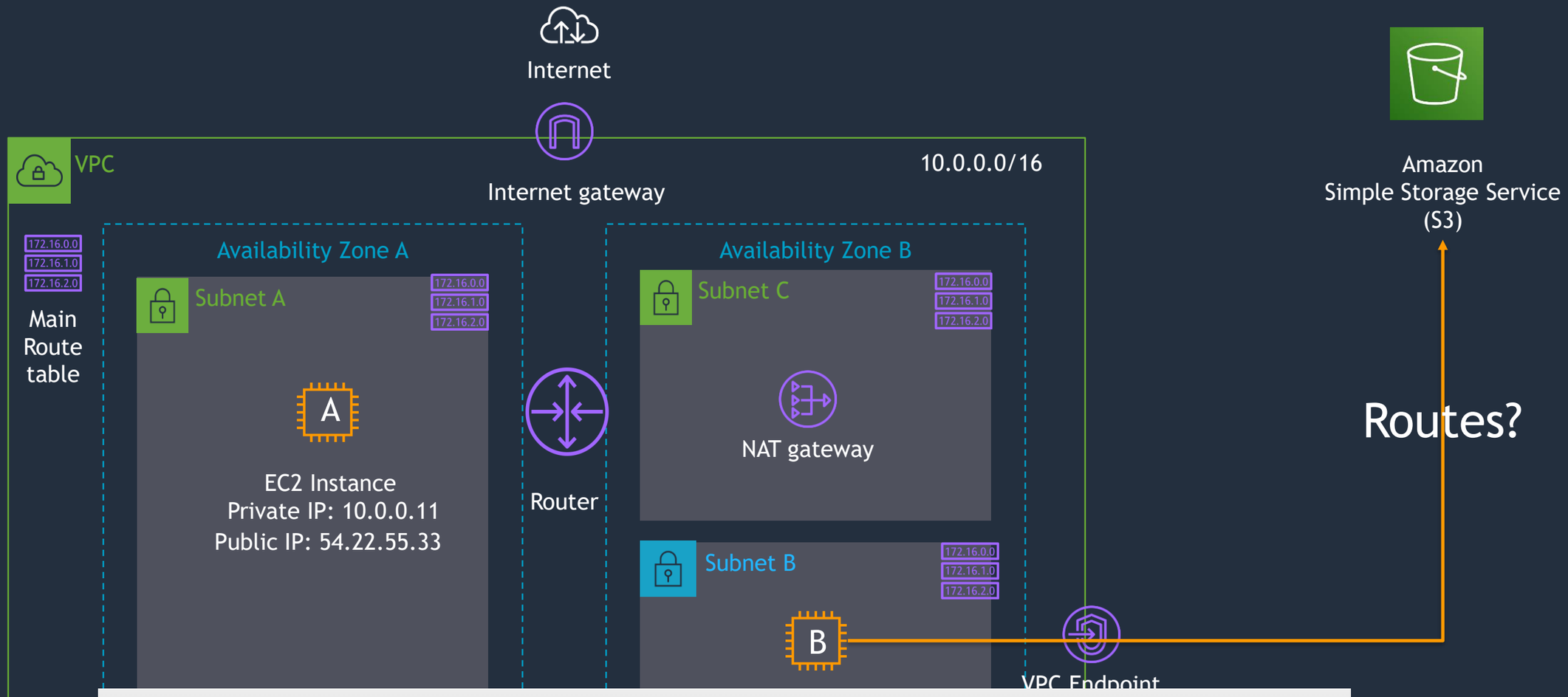


Can we design this better?

- Traffic flowing over internet
- NAT charges?

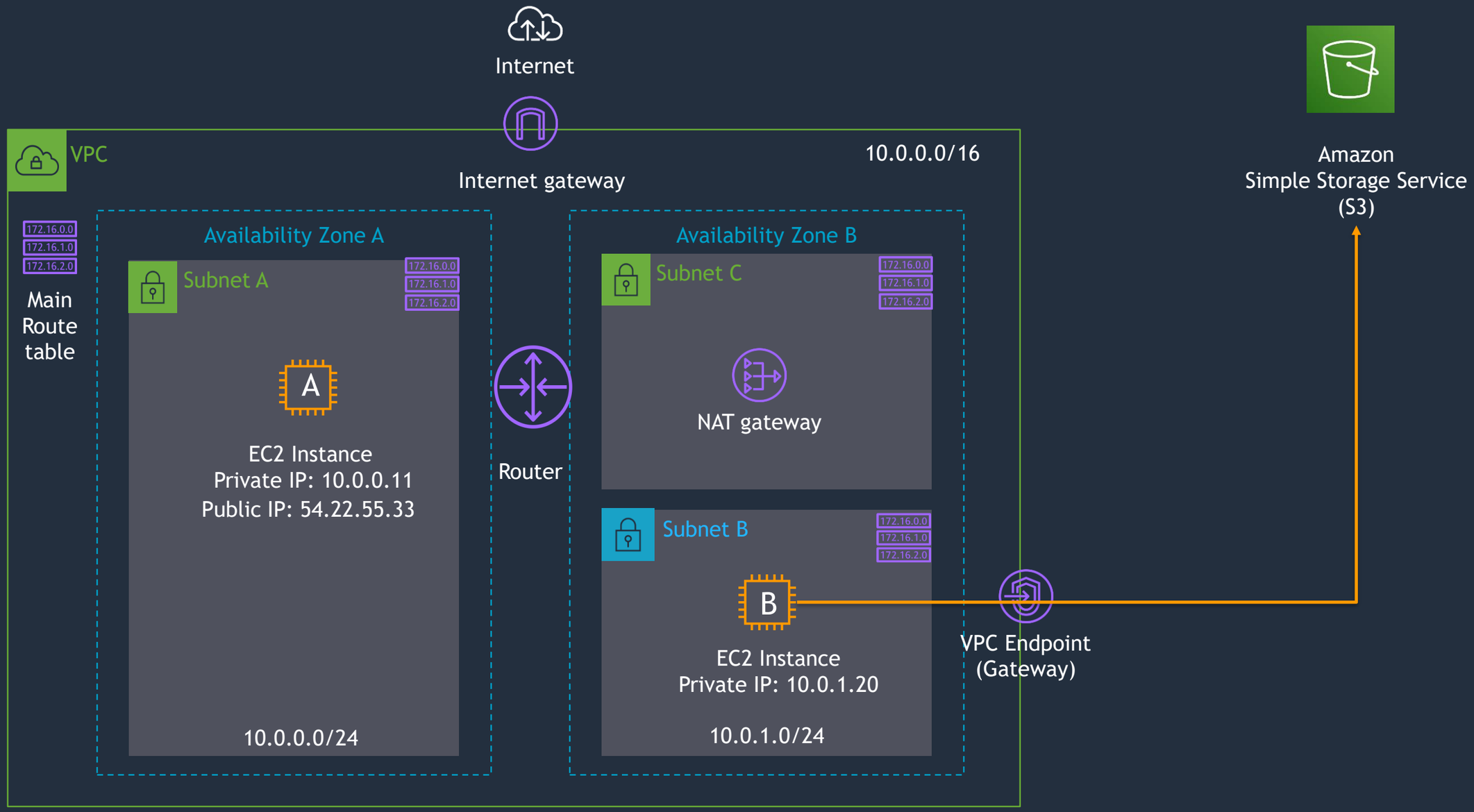
aws

Solution: VPC Gateway Endpoint



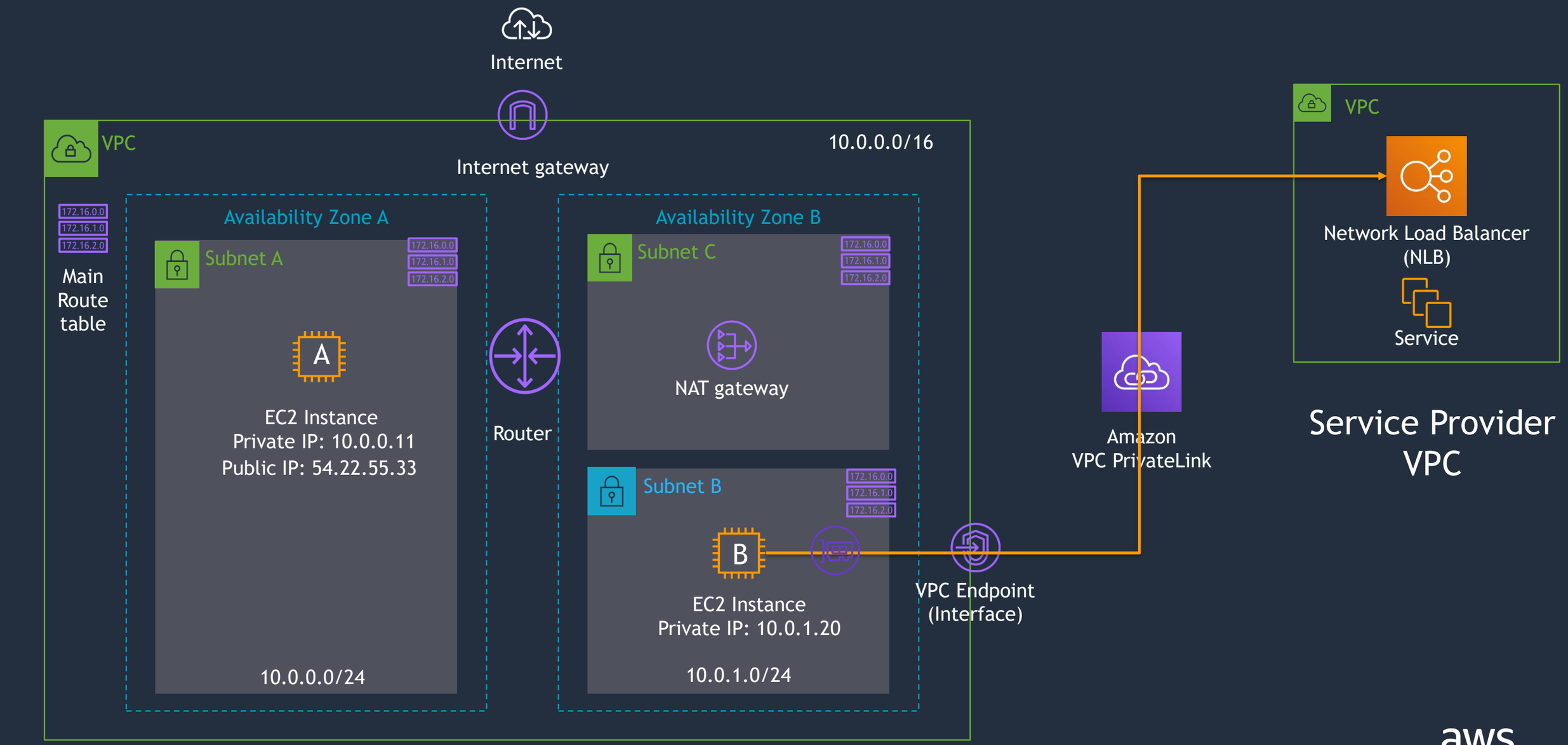
Destination	Target	Status
10.0.0.0/16	local	active
pl-78a54011 (com.amazonaws.ap-south-1.s3, 52.219.62.0/23, 3.5.212.0/23, 3.5.208.0/22, 52.219.64.0/22)	vpce-0e89398e630ab0bcf	active
0.0.0.0/0	nat-085190f27ccf2ca3e	active

Let’s create VPC endpoint and modify routes



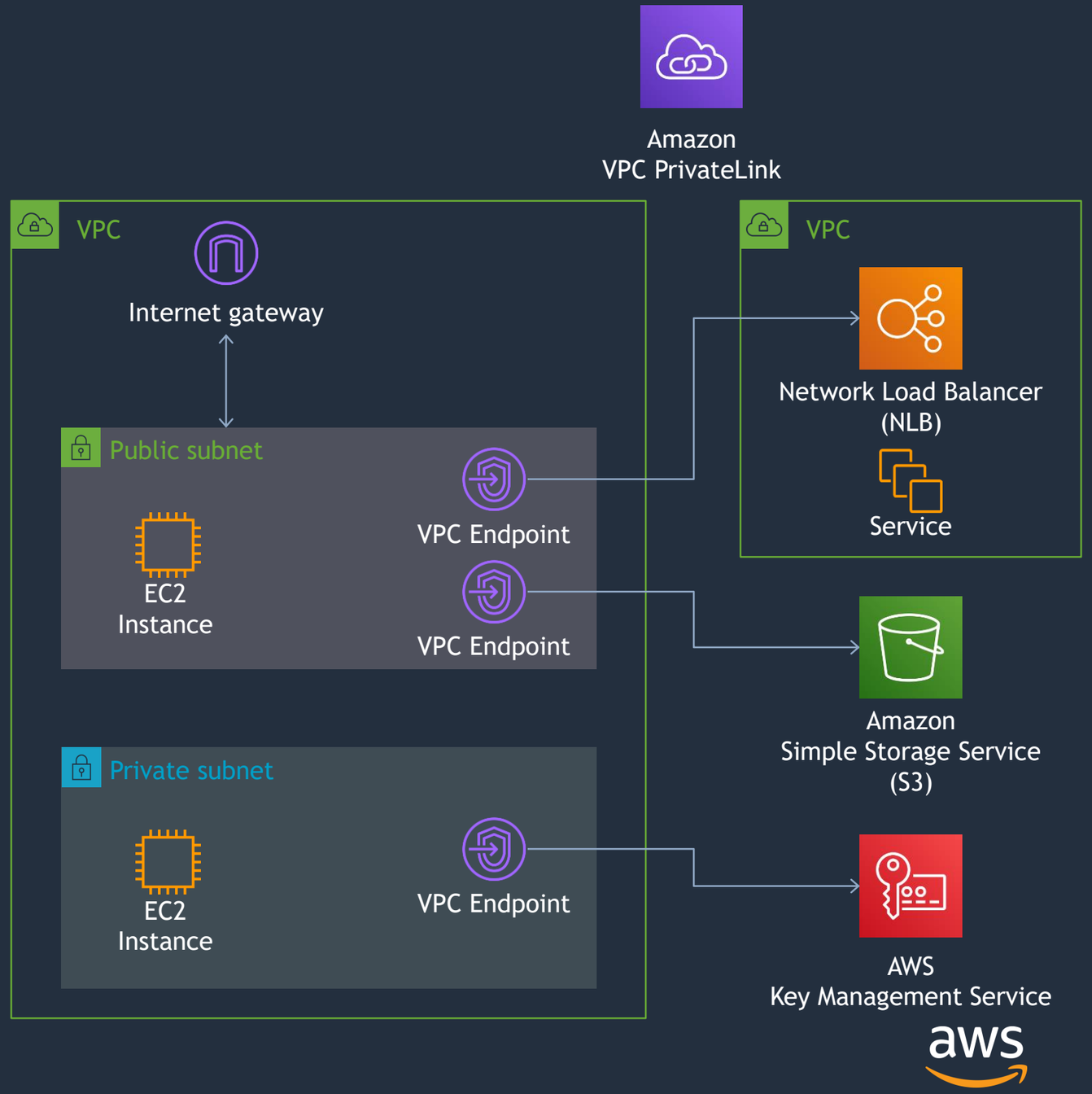
aws

How do you connect to other VPC services?



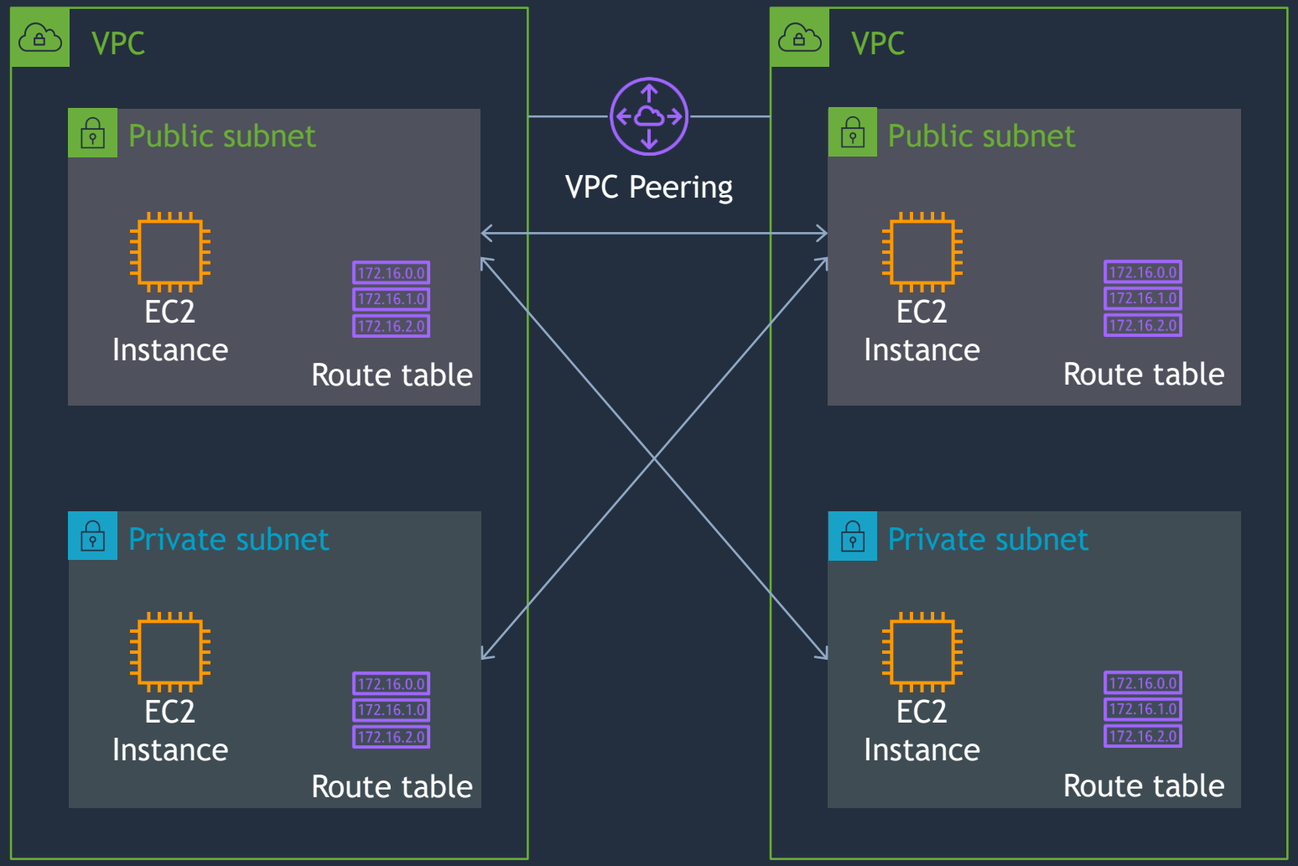
VPC Endpoints summary

- Connect your VPC to:
  - Supported AWS services
  - VPC endpoint services powered by PrivateLink
- Doesn’t require public IPs or Internet connectivity
- Traffic does not leave the AWS network.
- Horizontally scaled, redundant, and highly available
- Robust access control



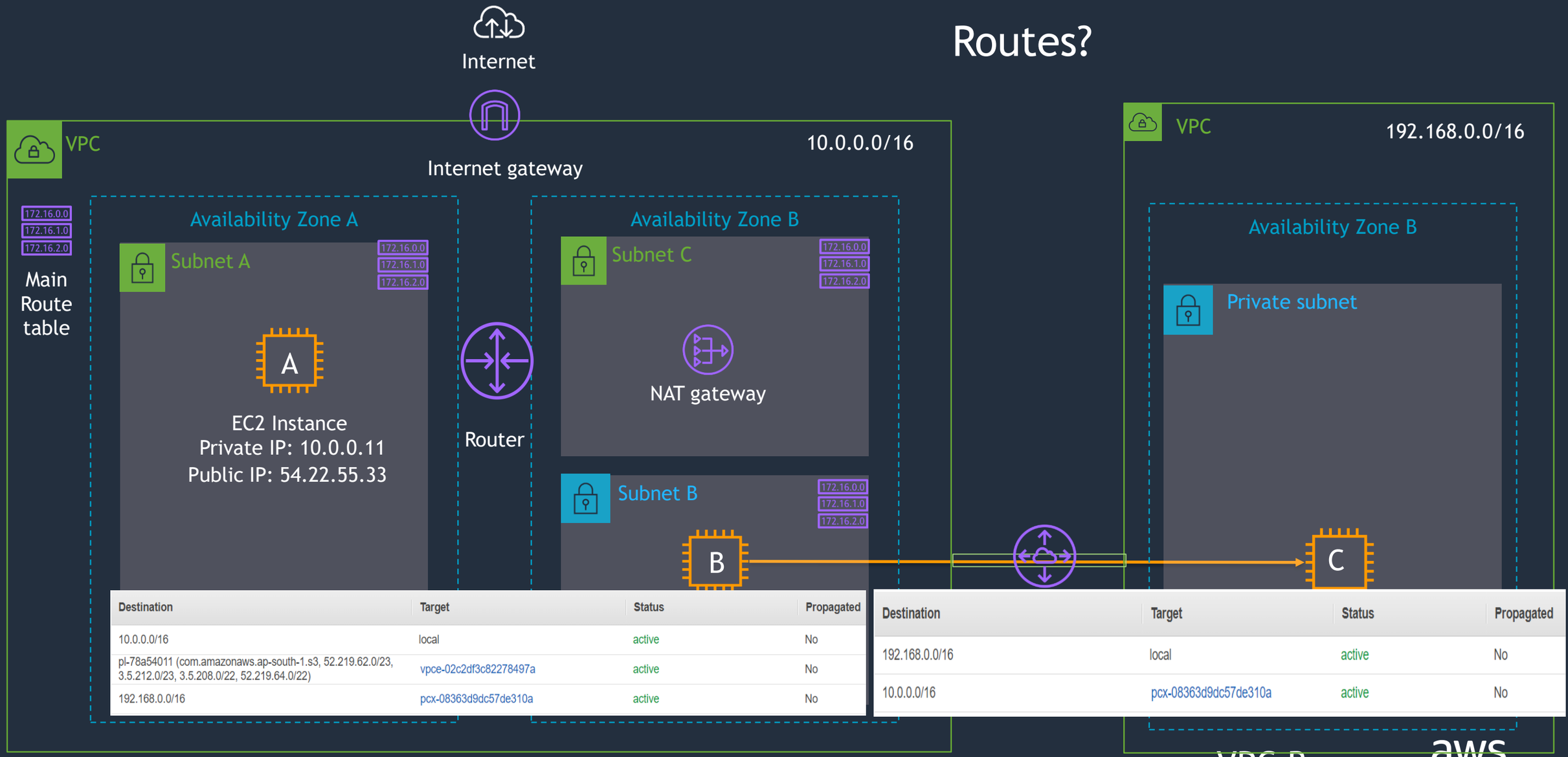
How to connect directly to other VPCs?
VPC Peering

- Scalable and high available
- Inter-account peering
- Same or different 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 transitive routing, requires full-mesh to interconnect multiple VPCs
- No support for overlapping IP addresses



aws

VPC peering

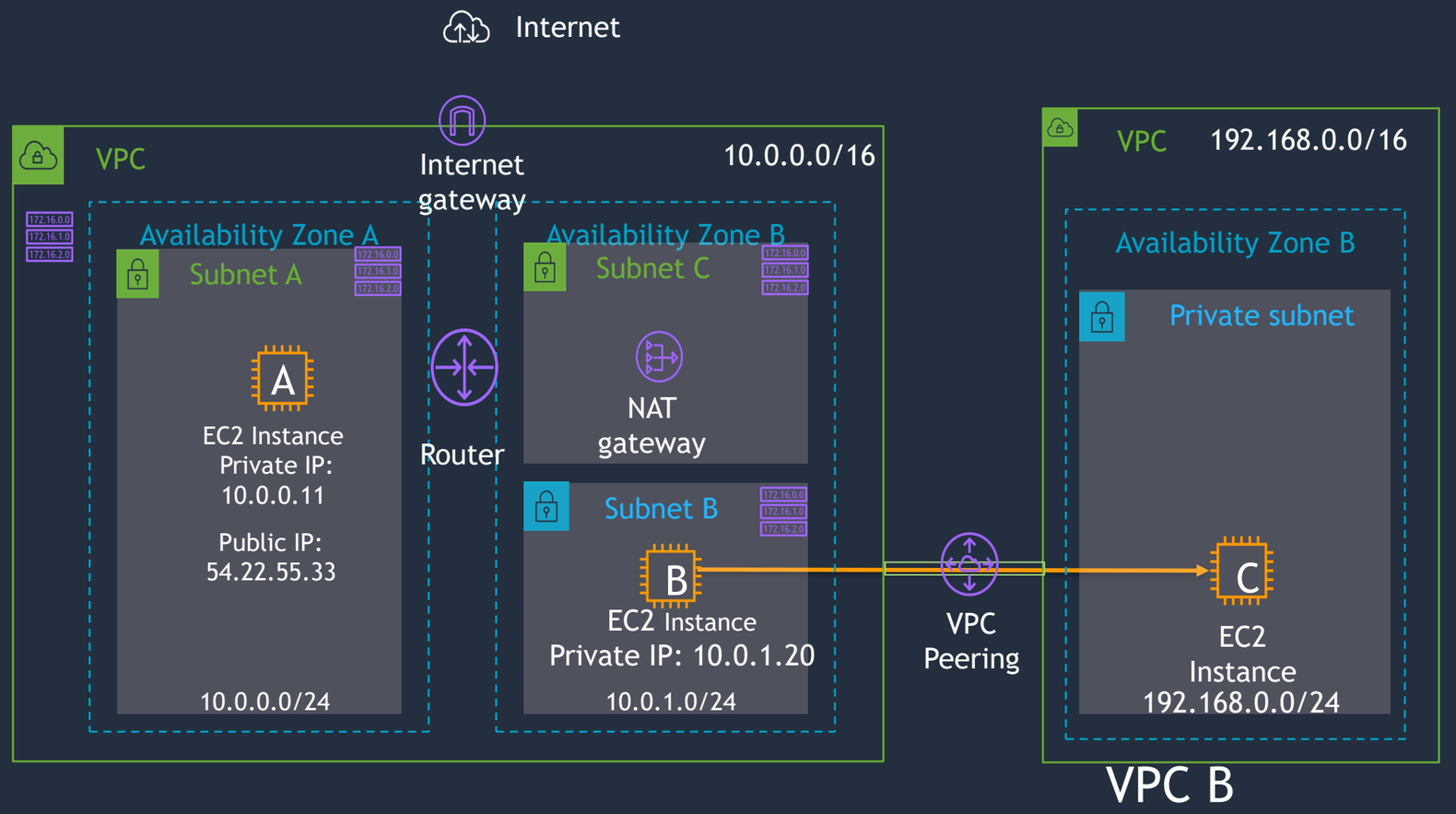


Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
pl-78a54011 (com.amazonaws.ap-south-1.s3, 52.219.62.0/23, 3.5.212.0/23, 3.5.208.0/22, 52.219.64.0/22)	vpce-02c2df3c82278497a	active	No
192.168.0.0/16	pcx-08363d9dc57de310a	active	No

Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
10.0.0.0/16	pcx-08363d9dc57de310a	active	No

Let’s set up VPC peering

1. Create new VPC-B in N.Virginia
2. Create VPC Peering connection request from Mumbai VPC
3. Accept request in N.Virginia VPC
4. Modify Route Tables at both the ends
5. Modify/make sure Security group on EC2-C allows inbound traffic from Mumbai VPC



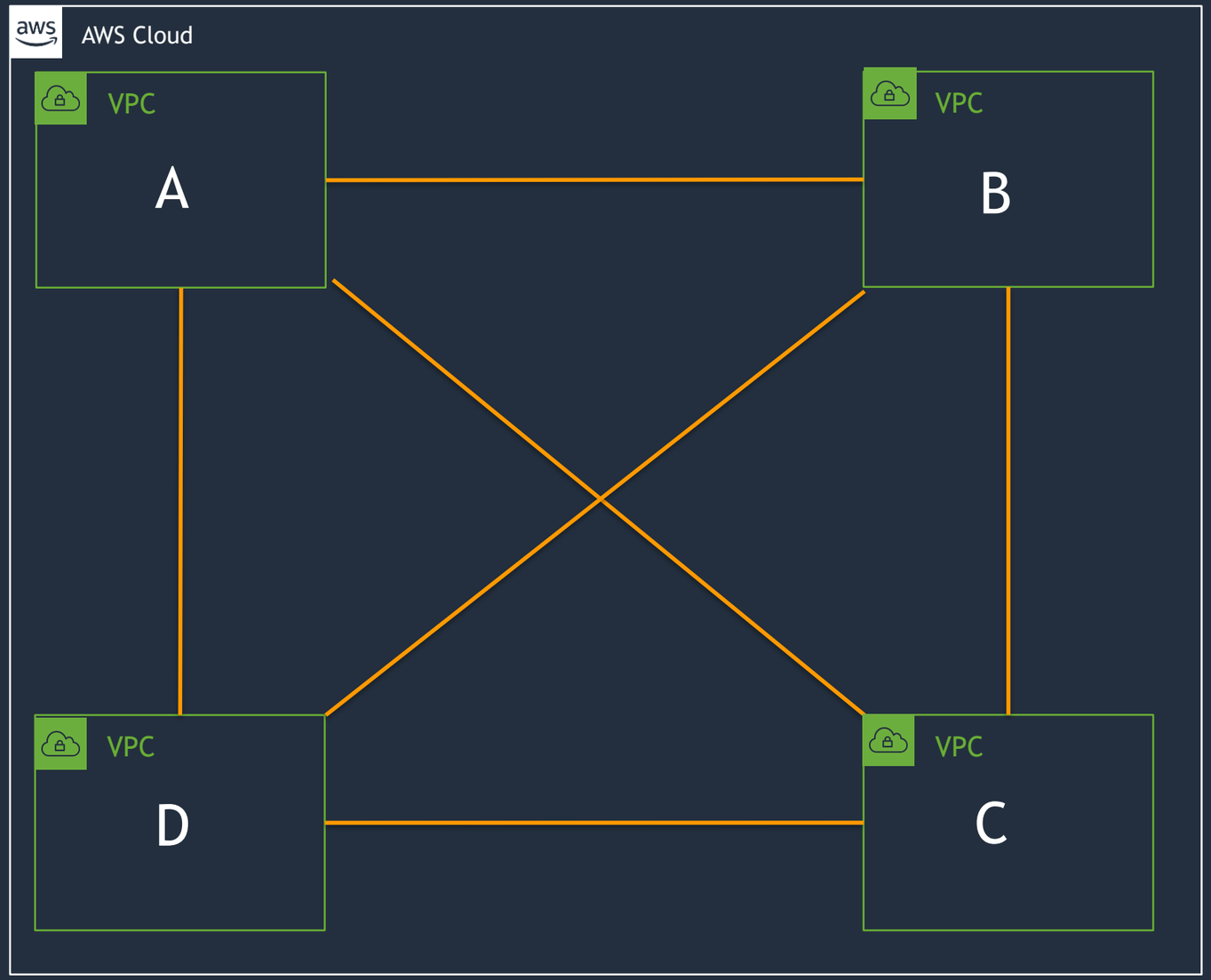
aws

How to connect multiple VPCs together?

What if we use VPC peering?

I want to connect 4 VPCs such that all VPCs are able to communicate with each other?

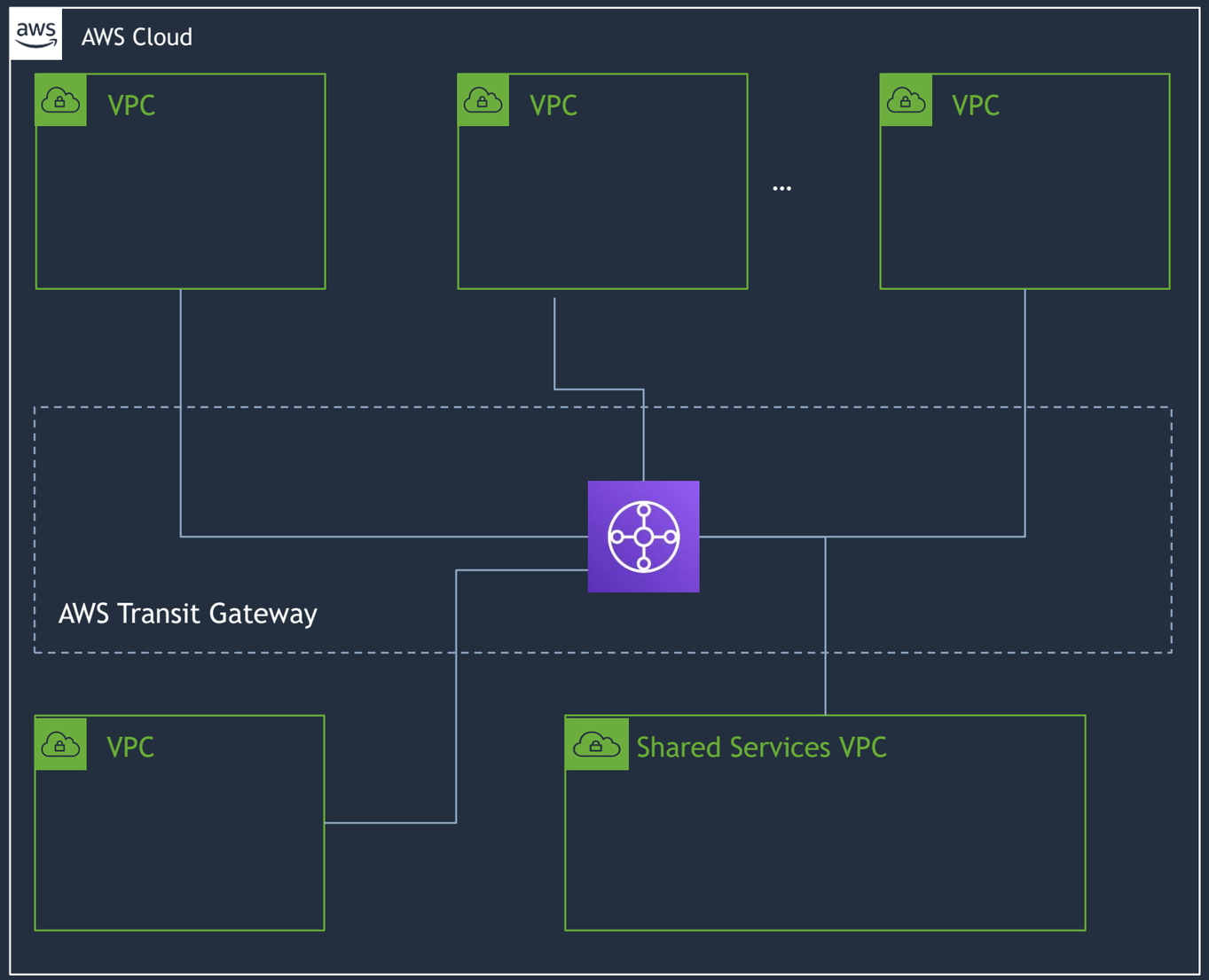
> How many VPC peering connections I will need?



How to connect multiple VPCs together?

AWS Transit Gateway

- Connect thousands of VPC across accounts
- Connect your VPCs and on-premises through a single gateway
- Centralize VPN and AWS Direct Connect connections
- Control segmentations and data flow with Routing Tables
- Hub and Spoke design
- Up to 50 Gbps per VPC connection (burst)

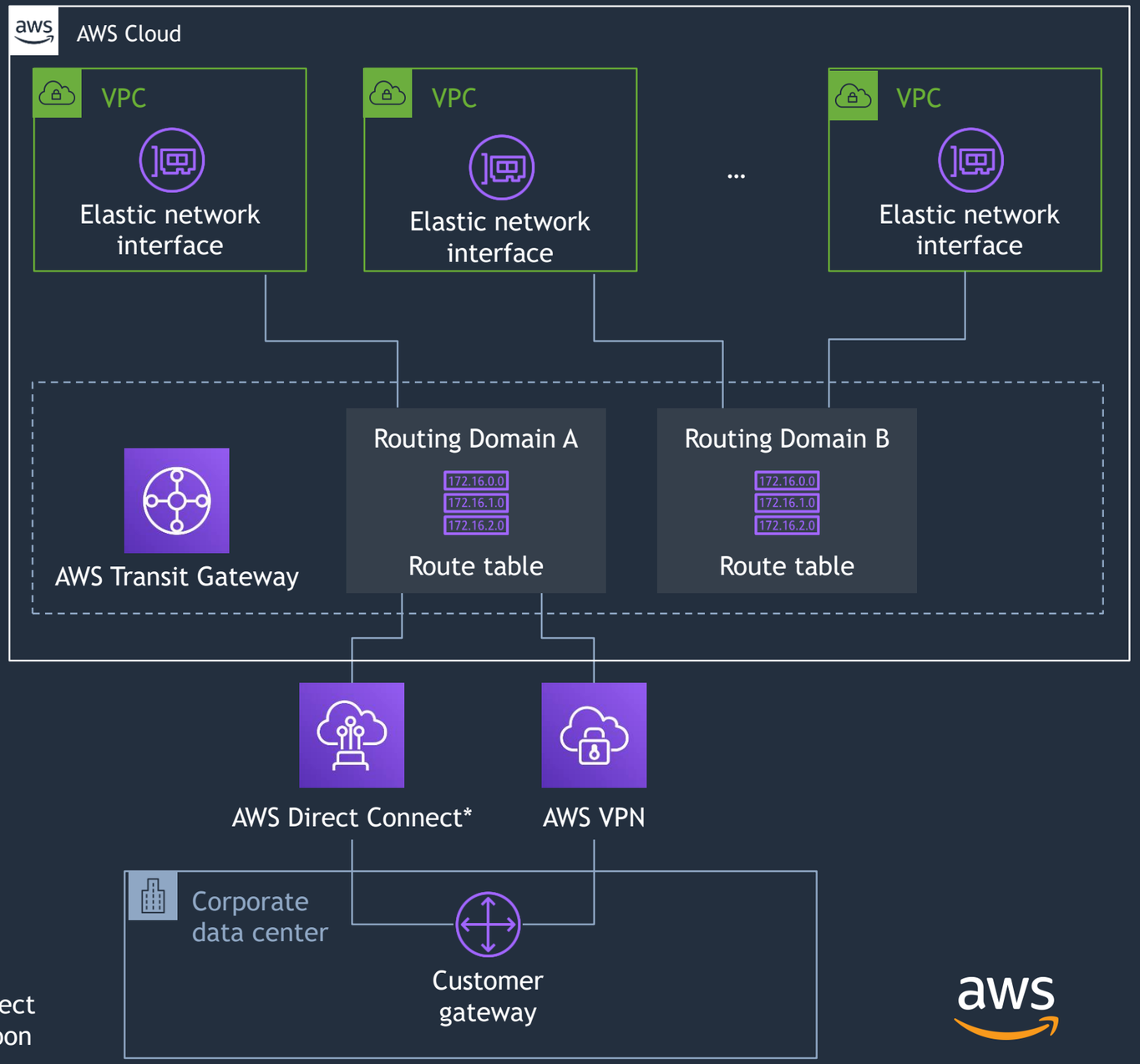


aws

How to connect all my VPC and on-premises network?

AWS Transit Gateway

- Centralize VPN and AWS Direct Connect
- Thousands of VPC across accounts
- Spread traffic over many VPN Connections
- Network interfaces in Subnets
- Control segmentations and sharing with routing

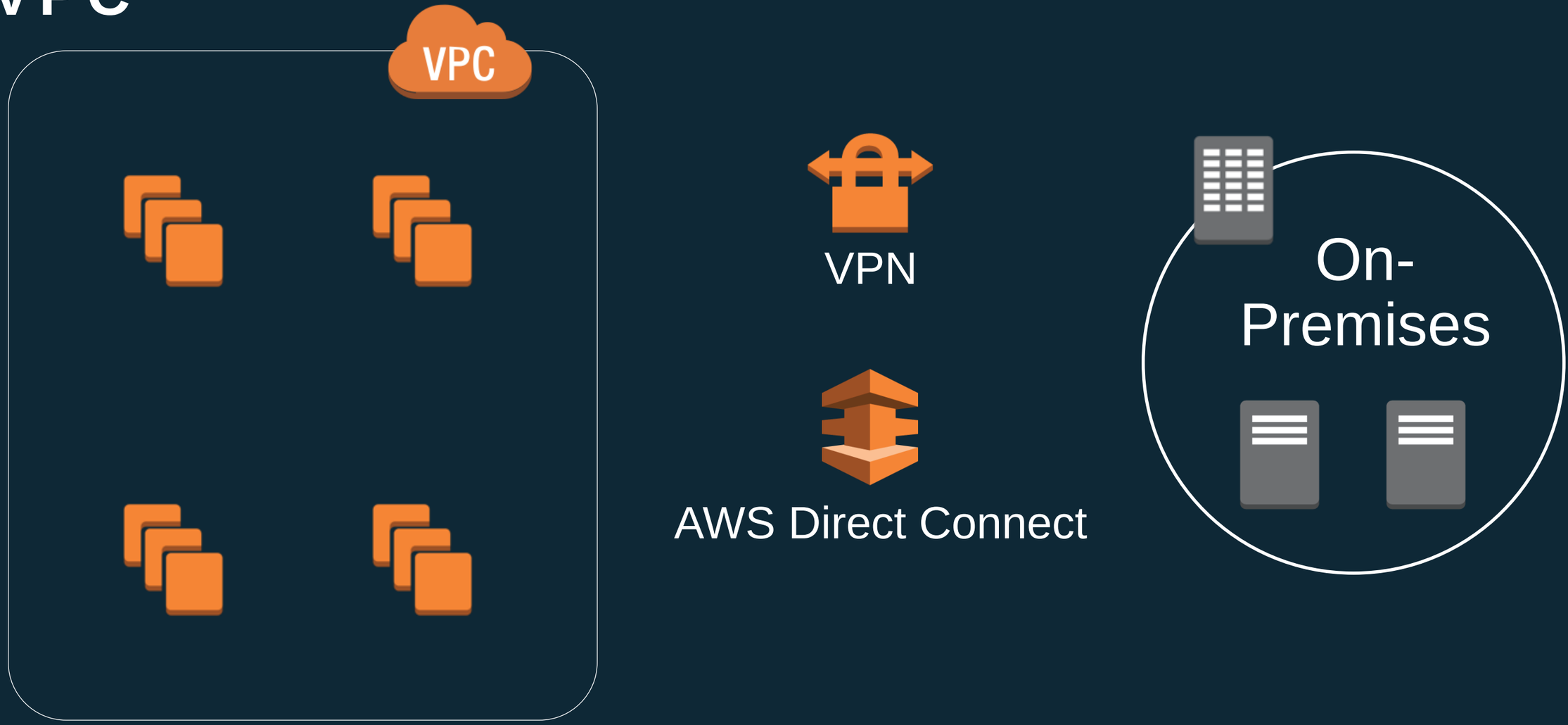


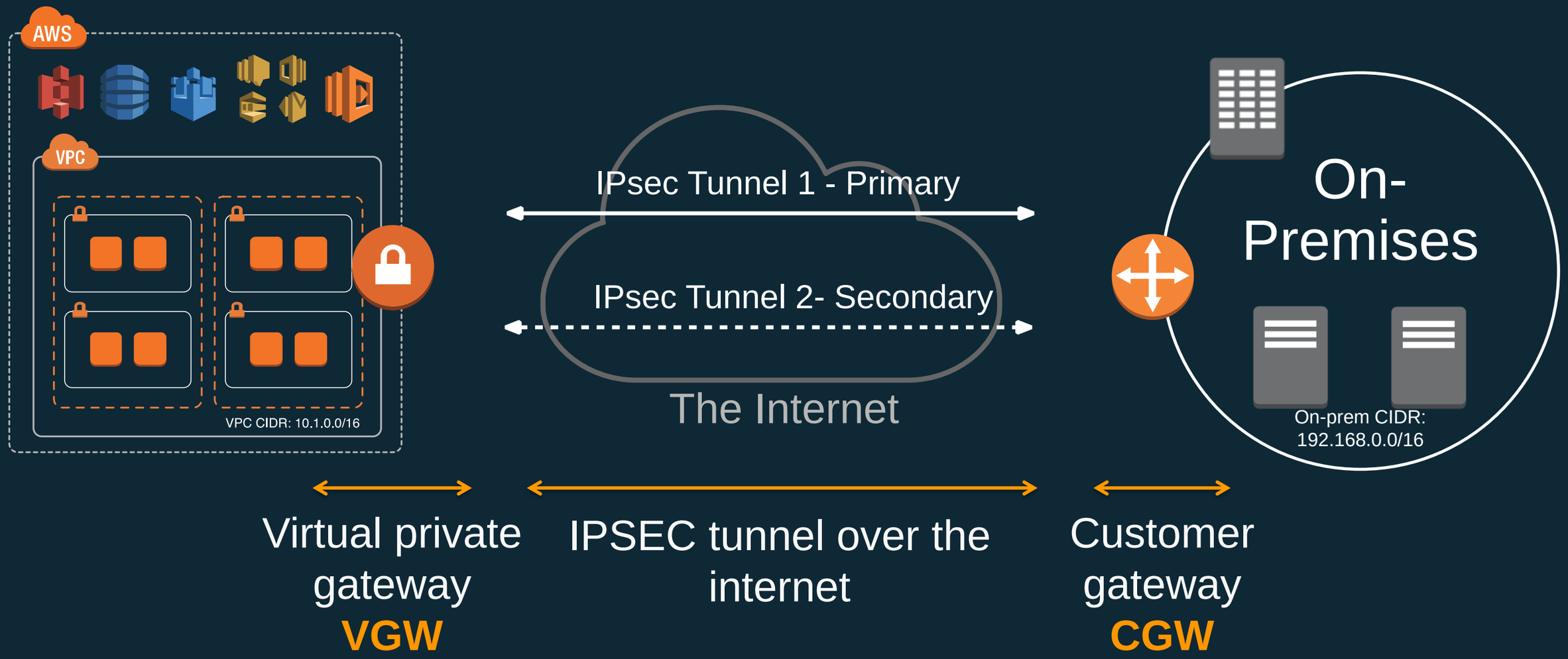
* AWS Direct Connect support coming soon

Connect Your Data Center to AWS

aws

Extend an on-premises network into your VPC



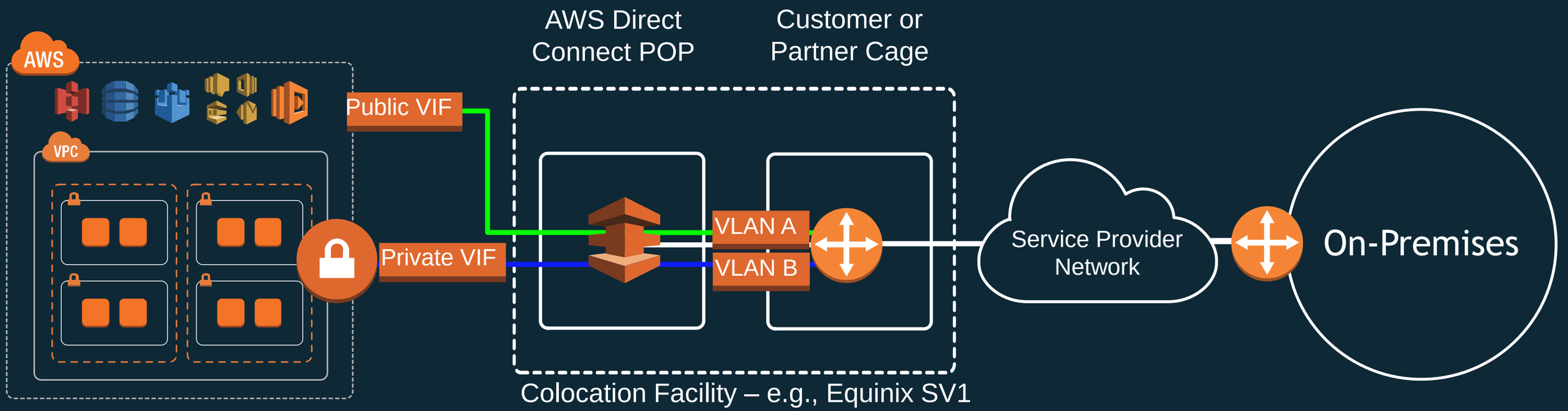


AWS Managed VPN

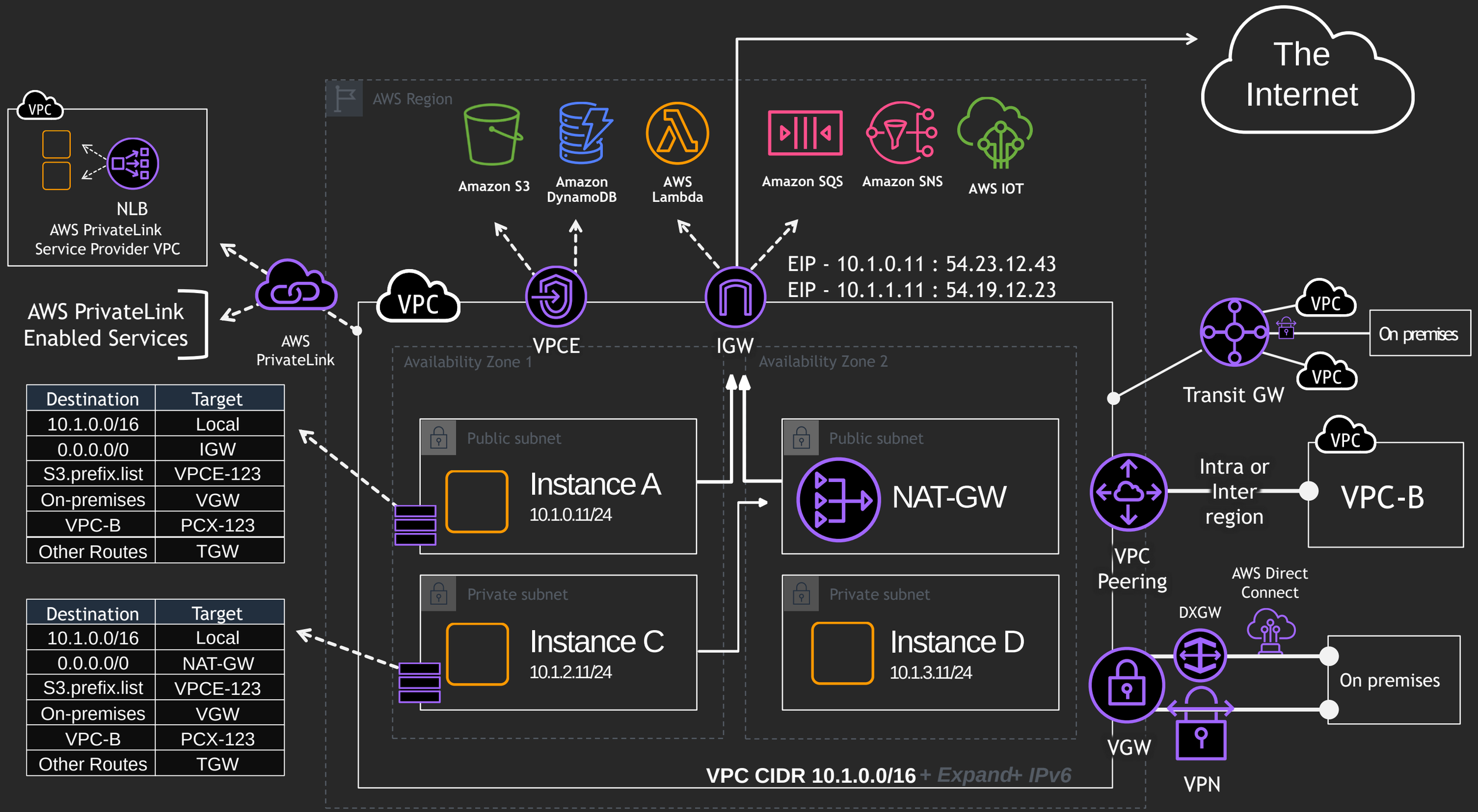
- Fully managed and highly available VPN termination endpoints at AWS end
- 1 connection, 2 VPN tunnels per VPC
- IPSec site-to-site tunnel with AES-256, SHA-2, and latest DH groups
- Support for NAT-T
- Pay $0.05 per hour per VPN connection
- Static or dynamic (BGP)

aws

AWS Direct Connect - what's that?



Wrapping up into single slide



Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other Routes	TGW

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other Routes	TGW

Thank you

Chetan Agrawal (agrcheta@amazon.com)

aws