Amazon Virtual Private Cloud (VPC): VPC Peering, Network Gateways, Endpoints, and AWS PrivateLink

Andru Estes
Principal Author
andru-estes

VPC Peering

VPC Peering

Feature to enable secure and direct communication between VPCs

Traffic remains within the AWS network infrastructure

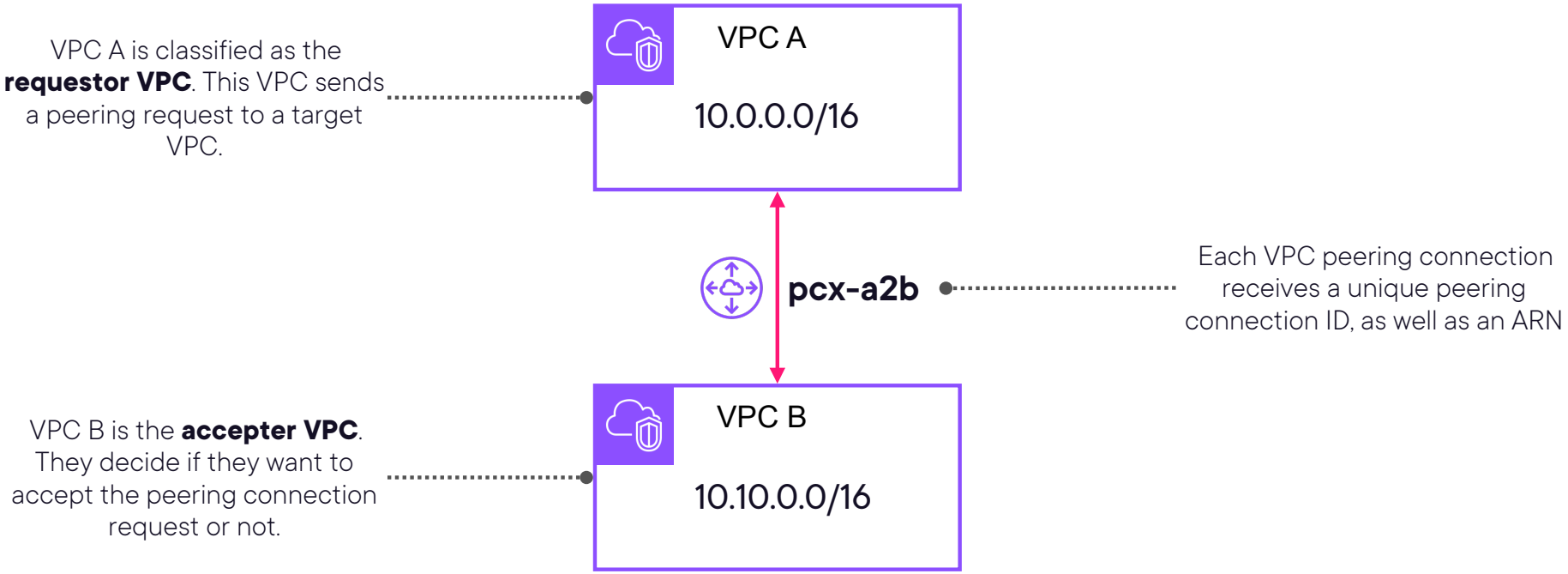
Enables private resources to communicate and interact

Feature ensures there is no single point of failure for a connection

Connect Cross-Account, Same Account, and even Cross-Region

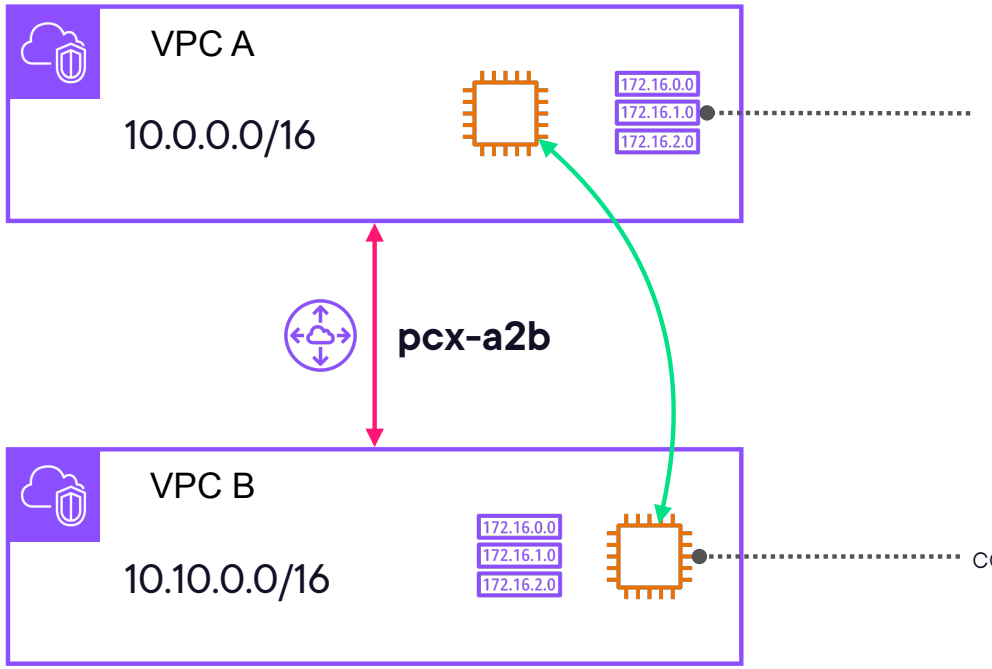
VPC Peering Architecture Diagram

In this example we will assume VPC A is wanting to establish a peering connection with VPC B



VPC Peering Architecture Diagram

In this example we will assume VPC A is wanting to establish a peering connection with VPC B

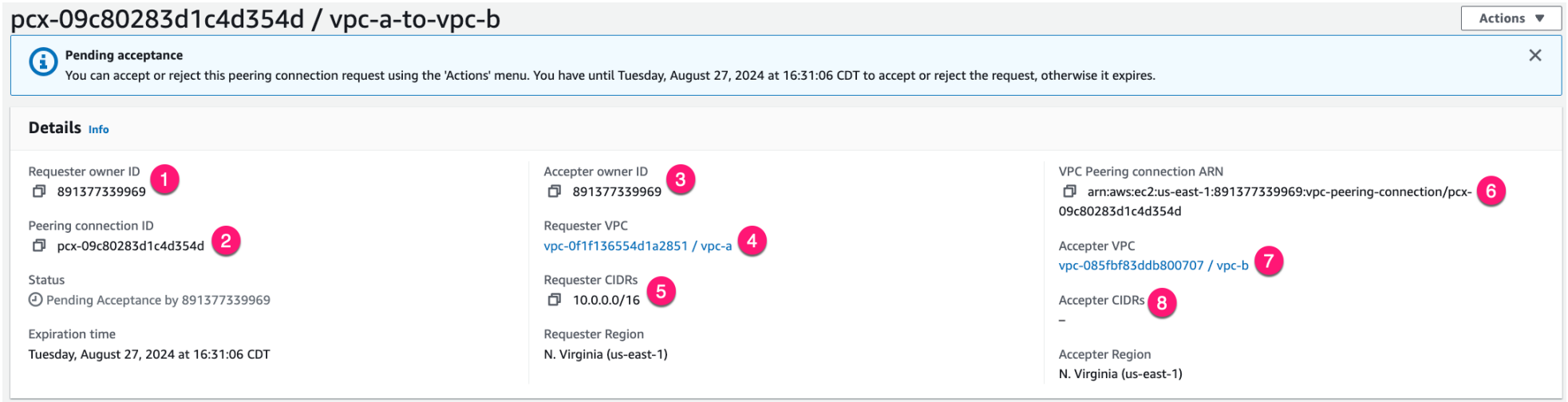


Once VPC peering is in place, you update the VPC route tables to correctly route the traffic between VPCs

You also need to correctly configure NACLs and security groups

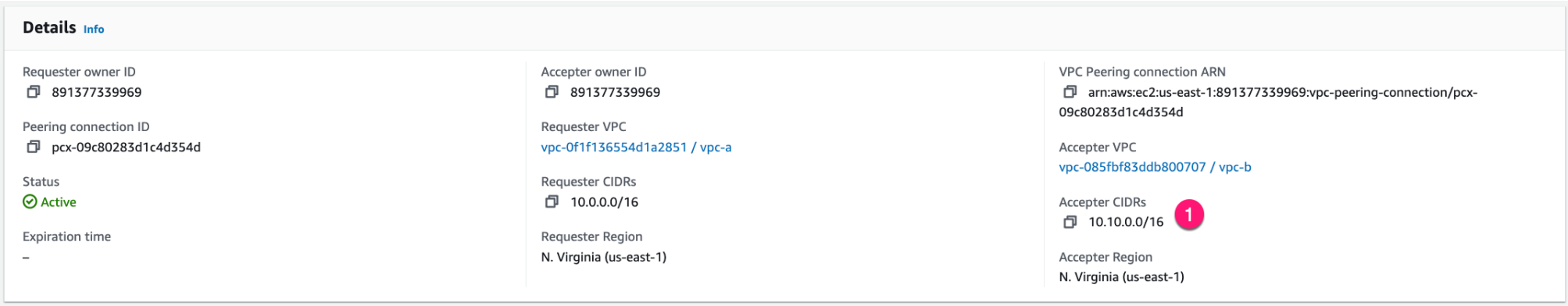
Compute can now start communicating with the peered VPC resources

VPC Peering Requested



1. The requesting VPC AWS account ID
2. The peering connection ID
3. The accepting VPC AWS account ID
4. The requesting VPC ID/name
5. The requesting VPC CIDR
6. The VPC peering connection ARN
7. The accepting VPC ID/name
8. Hidden accepting VPC CIDR

VPC Peering Accepted



1. The accepting VPC CIDR is now visible after the connection was accepted

You can enable a VPC to resolve public IPv4 DNS hostnames to private IPv4 addresses when queried from instances in the peer VPC.

To accomplish this, both VPCs must be enabled for DNS hostnames and DNS resolution.

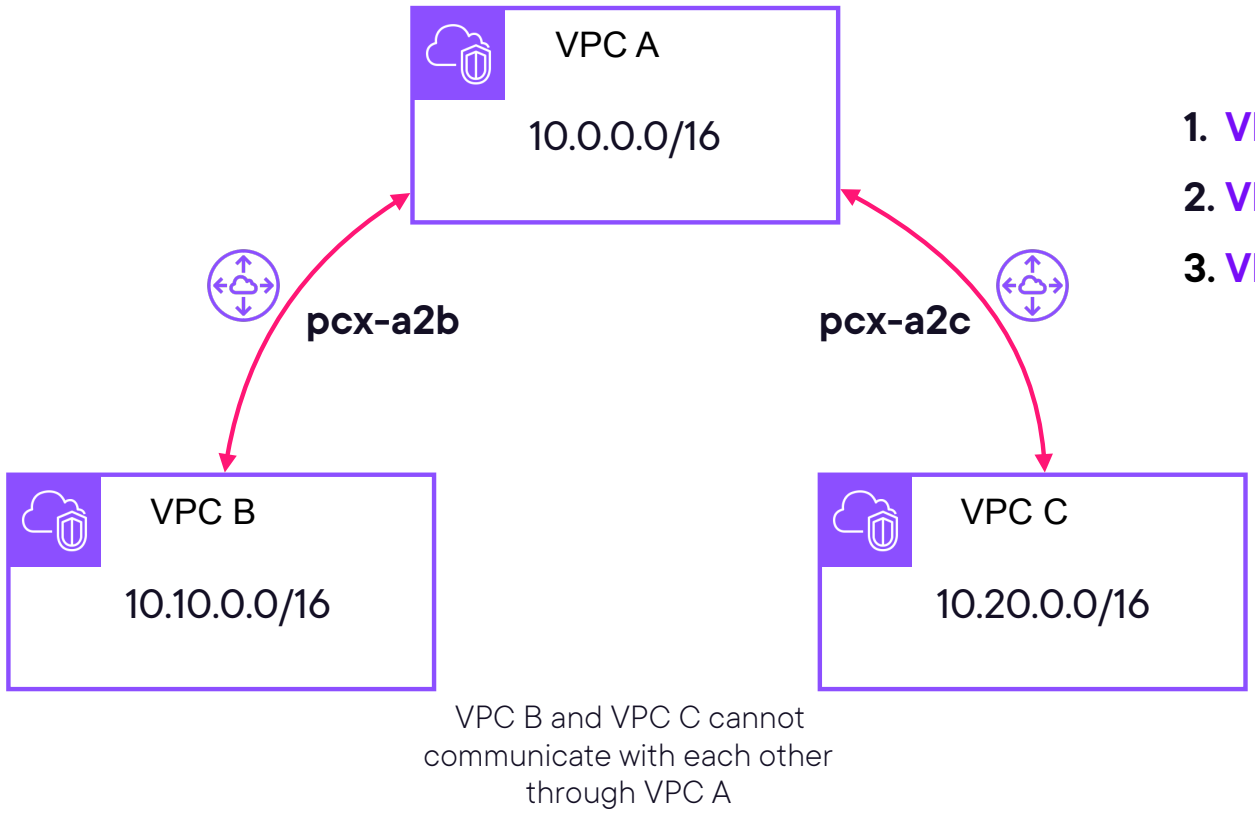
VPC Peering Must Knows

Peered VPCs cannot have any overlapping IP CIDRs

Peering does NOT allow for transitive routing

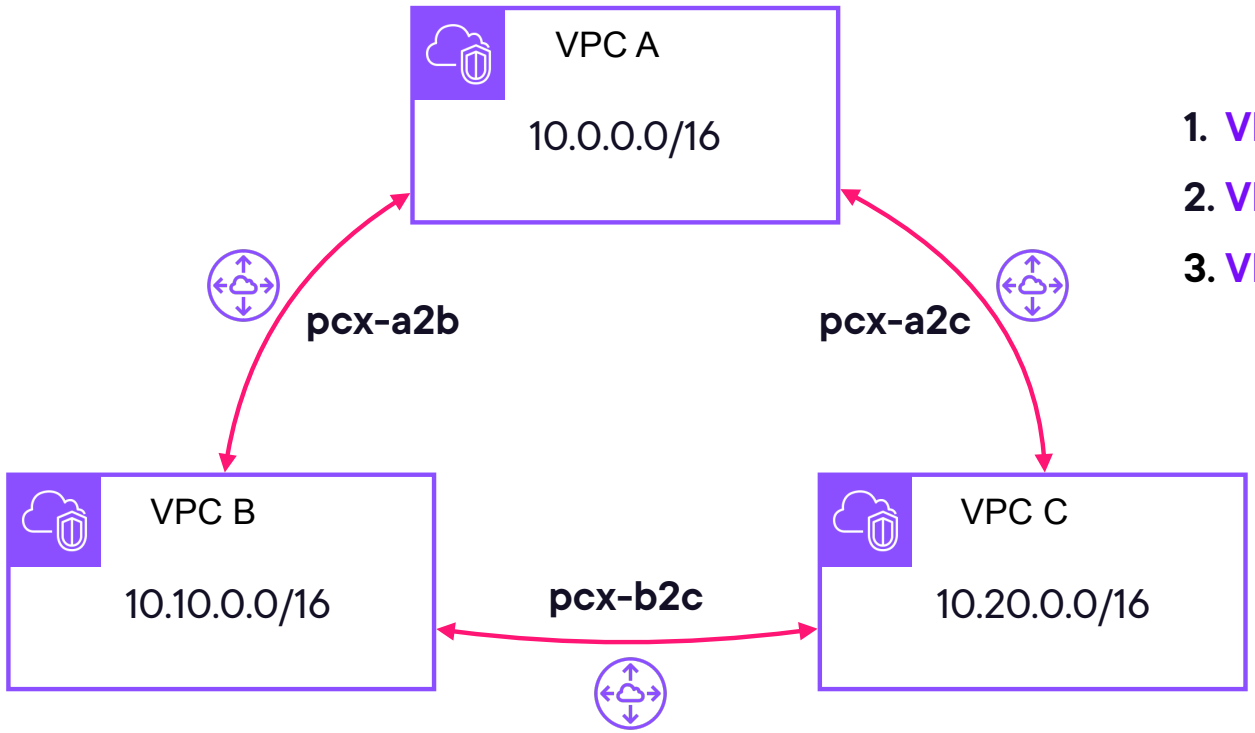
Route tables must be updated to correctly route the traffic destined for a peered VPC

What Does “Not Transitive” Mean?



1. VPC A can talk to VPC B? ✅
2. VPC A can talk to VPC C? ✅
3. VPC B can talk to VPC C? ❌

What Does “Not Transitive” Mean?

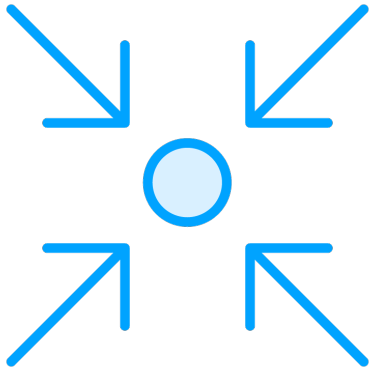


1. VPC A can talk to VPC B? ✅
2. VPC A can talk to VPC C? ✅
3. VPC B can talk to VPC C? ✅

With another peering connection in place, VPC B and VPC C can now talk

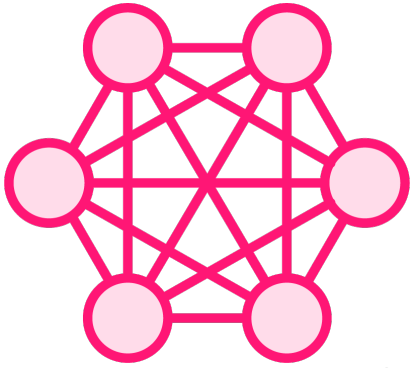
Pro Exam Tip: When VPCs are peered in the same Region, you can reference peered VPC Security IDs as needed (*e.g. Security Group Rules*)

VPC Peering Use Cases



Centralized Shared Services VPC

Multi-Region Internal Application Deployment



Cross-account VPC Integration for Collaboration or Merger/Acquisition

Public NAT Gateways

Network Address Translation (NAT)

...a service that operates on a router or edge platform to connect private networks to public networks like the internet. With NAT, an organization needs one IP address or one limited public IP address to represent an entire group of devices as they connect outside their network

Citation: https://www.cisco.com/c/en/us/products/routers/network-address-translation.html

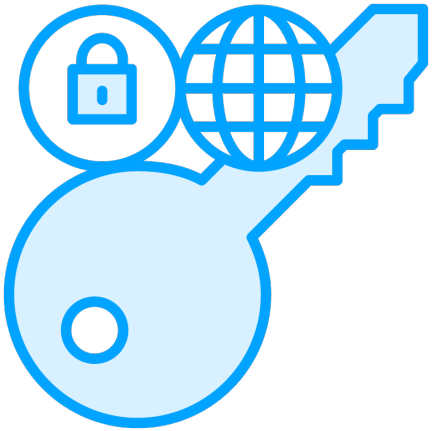
AWS NAT Gateway

A NAT gateway is a Network Address Translation (NAT) service.

You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

Citation: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Why NAT?



Private

Allows resources in private subnets to connect to the internet, peered VPCs, an on-prem networks

Secure

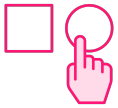
Private resources cannot receive unsolicited connection requests from outside the network

NAT Gateways and NAT Instances

NAT Instance: Outdated, should avoid. Provides network address translation via an EC2 instance that you own and manage! Lots of overhead.

NAT Instances require that you **disable Source/Destination Check**

NAT Gateways: Automatically scale as needed (*5 Gbps to 100 Gbps*). Deployed to a single AZ. Leverage an Elastic IP address.



You will likely choose NAT Gateways over NAT Instances whenever you can.

For true resiliency, you must deploy a NAT Gateway in multiple AZs. In this scenario you need to keep an eye on costs!

You must deploy a NAT device within a public subnet to allow internet access!

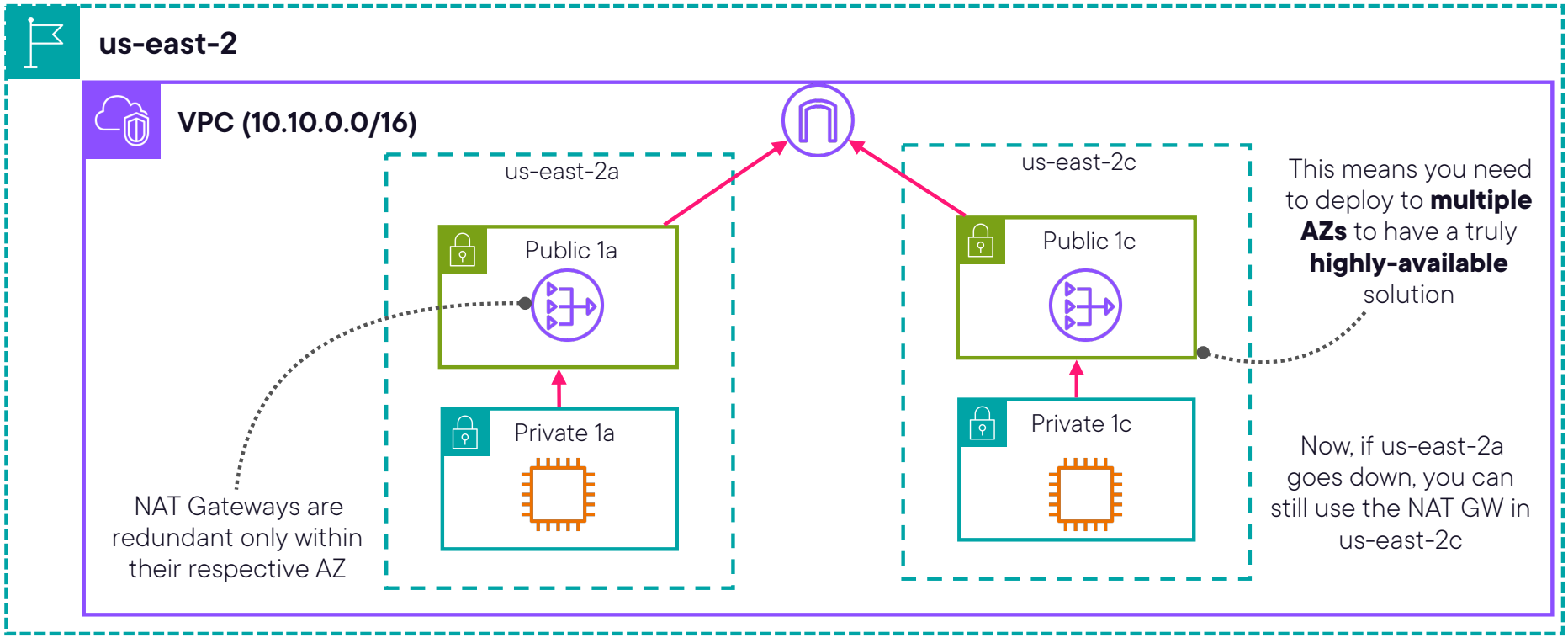
Elastic IP Address (EIP)

...a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is allocated to your AWS account, and is yours until you release it.

These are Regional resources that do not change over time.

Citation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

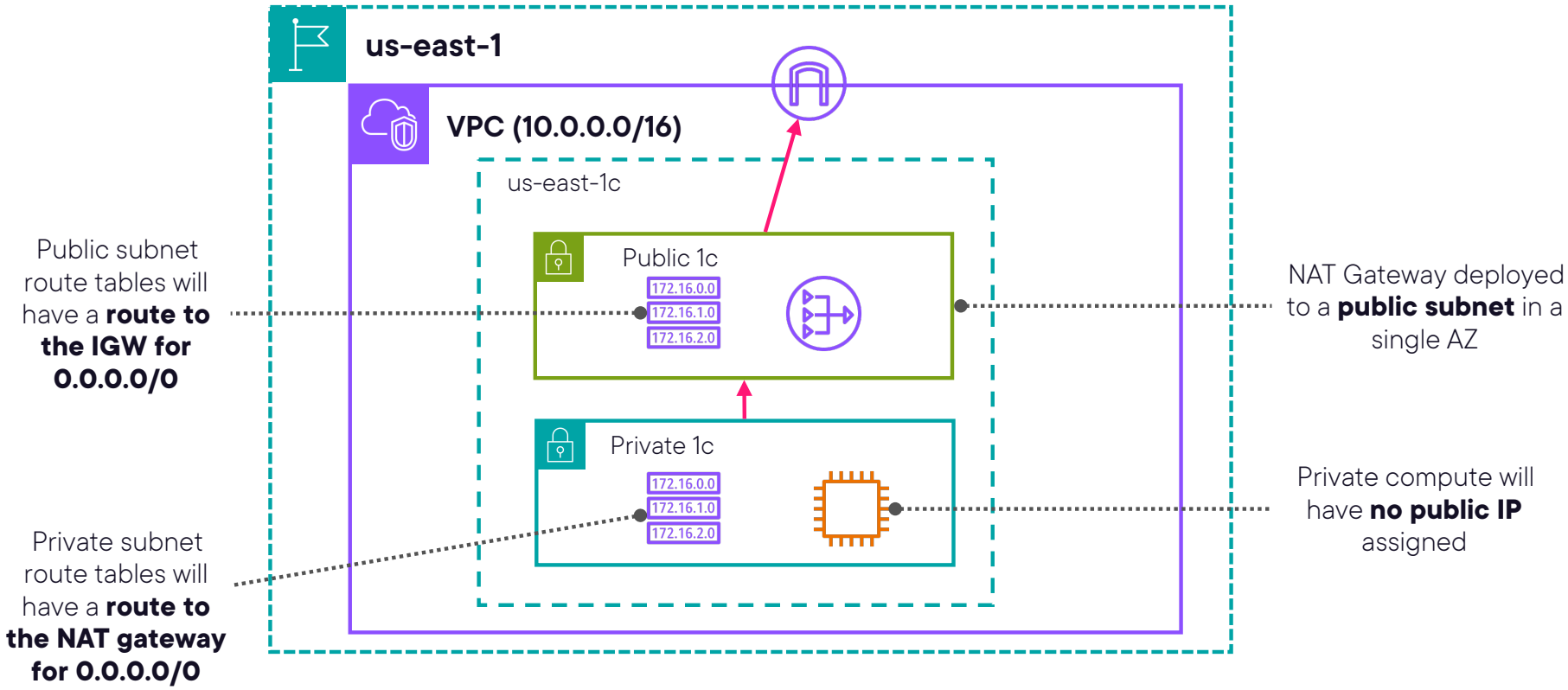
Highly-available NAT Gateway Architecture Diagram



Exam Pro Tip 1: If you need private resources to have secure internet access, then NAT Gateway is likely the best choice!

Exam Pro Tip 2: You do not assign security groups to NAT Gateways.

Demo: Deploying a NAT Gateway



Transit VPCs

Transit VPCs

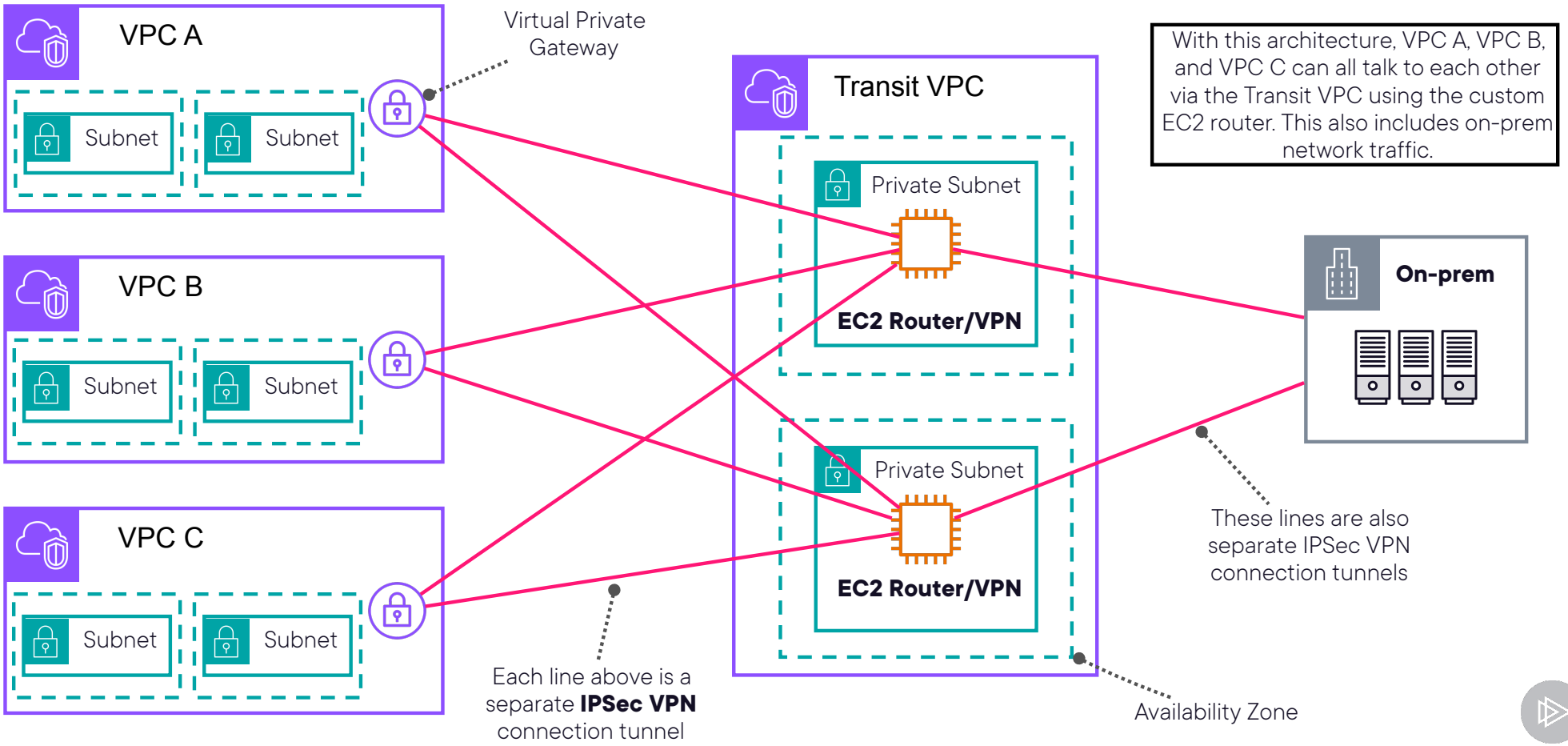
Not Transitive by Default

Remember that peering VPCs does not offer transitive routing by default

VPN

You can achieve a Transit VPC by leveraging a VPN solution

Transit VPC Architecture Diagram



A Virtual Private Gateway (VGW) is simply the VPN concentrator on the Amazon side of a Site-to-Site VPN connection.

You attach a VGW to a VPC that needs access to the VPN connection.

VPC Endpoints and AWS PrivateLink

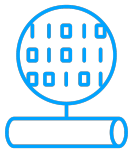
AWS PrivateLink

... a highly available, scalable technology that you can use to privately connect your VPC to services as if they were in your VPC.

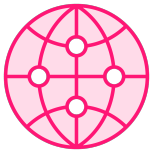
Citation: https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html

Remember that every AWS service is going to leverage the public endpoint by default.

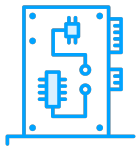
AWS PrivateLink



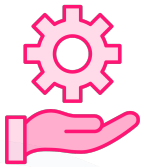
TL;DR: PrivateLink allows your private resources to communicate with services entirely within the AWS private network infrastructure



Allows you to remove need of IGWs, NAT Gateways, VPNs, Direct Connects

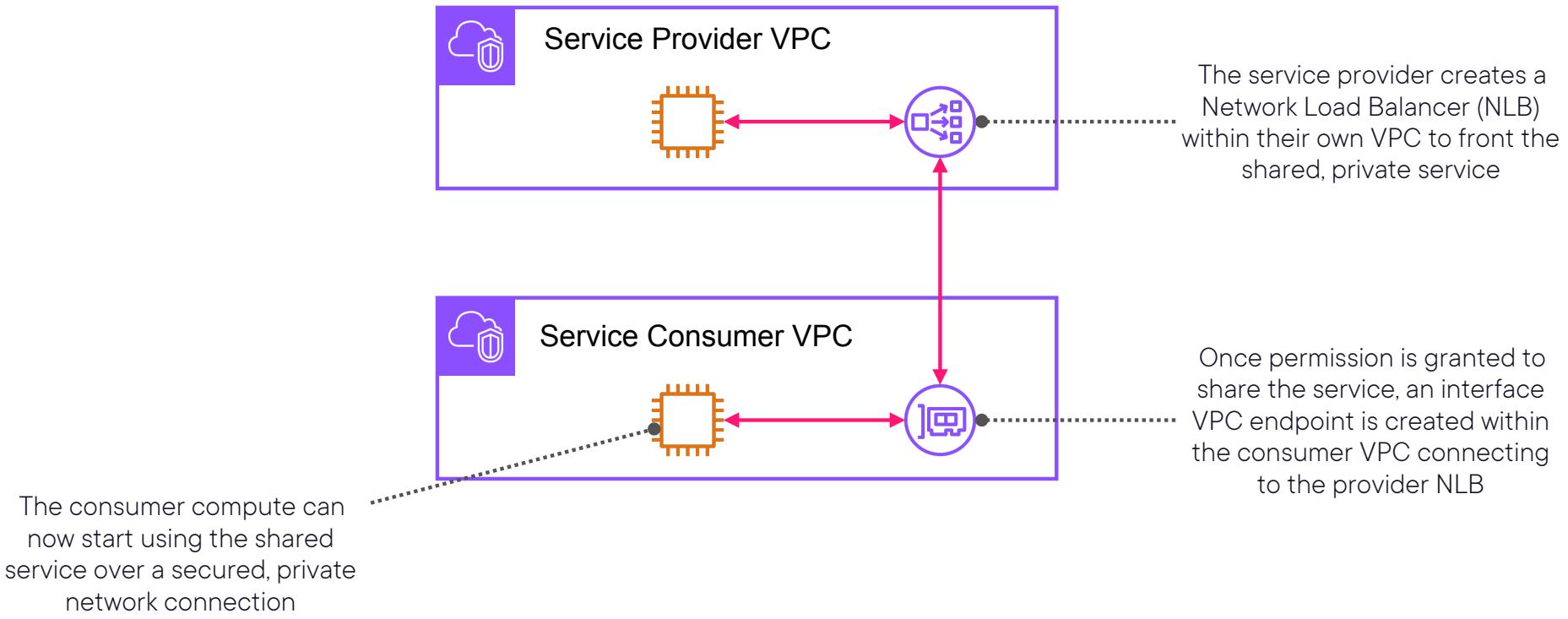


Create endpoints within your VPC to control and secure traffic



Capable of hosting your own private services as well by setting up a service provider and a service consumer

AWS PrivateLink Architecture Diagram



AWS PrivateLink is what powers VPC Interface Endpoints, which will be discussed soon!

Gateway Endpoints

Gateway VPC endpoints provide reliable, secure connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC.

Gateway Endpoints

Perfect for keeping S3 and DynamoDB traffic from traversing the internet

These do NOT leverage AWS PrivateLink

They are free to use

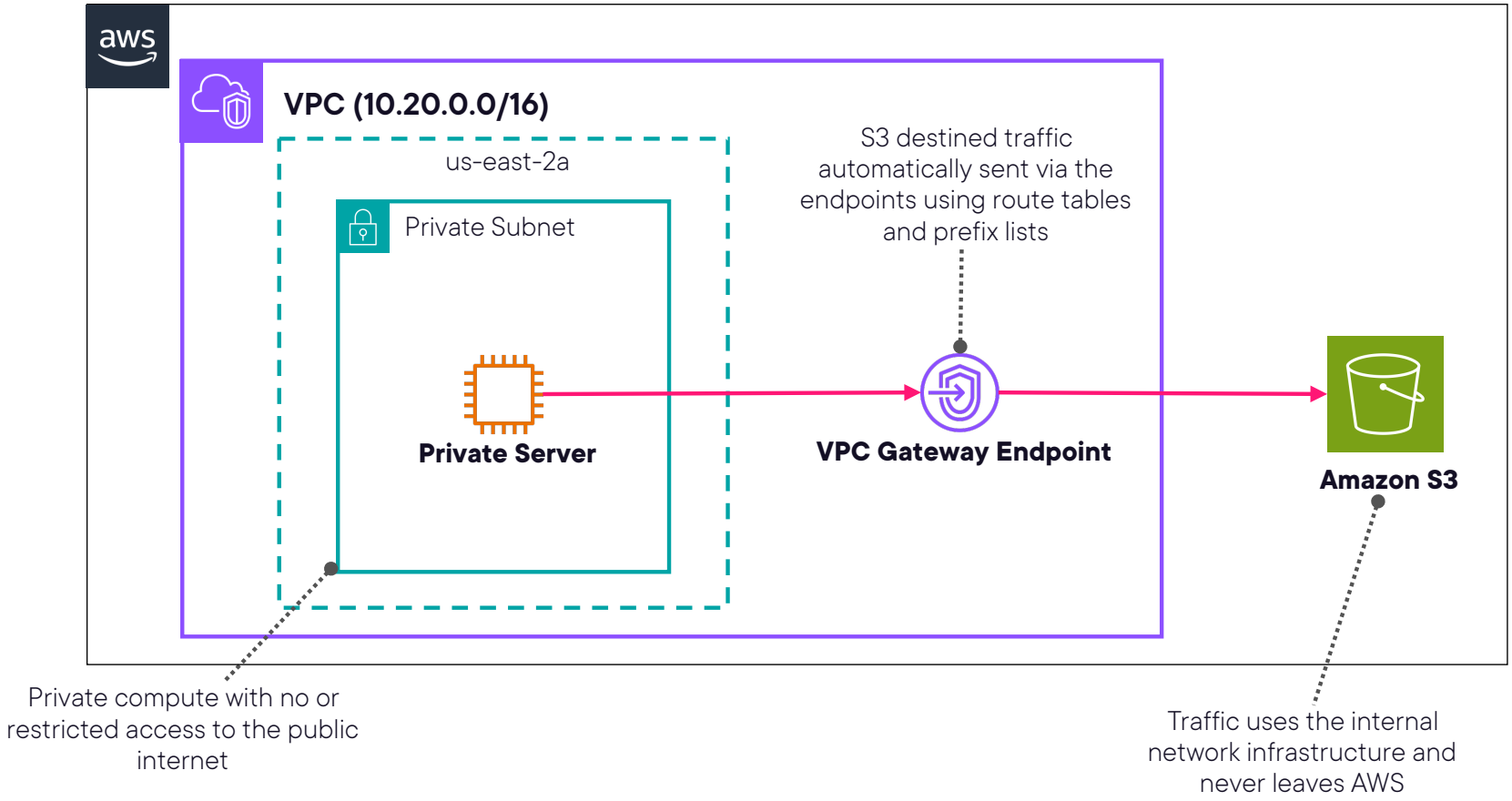
They require updates to route tables to direct traffic correctly

Easy to use and reference via a Managed Prefix List for routes

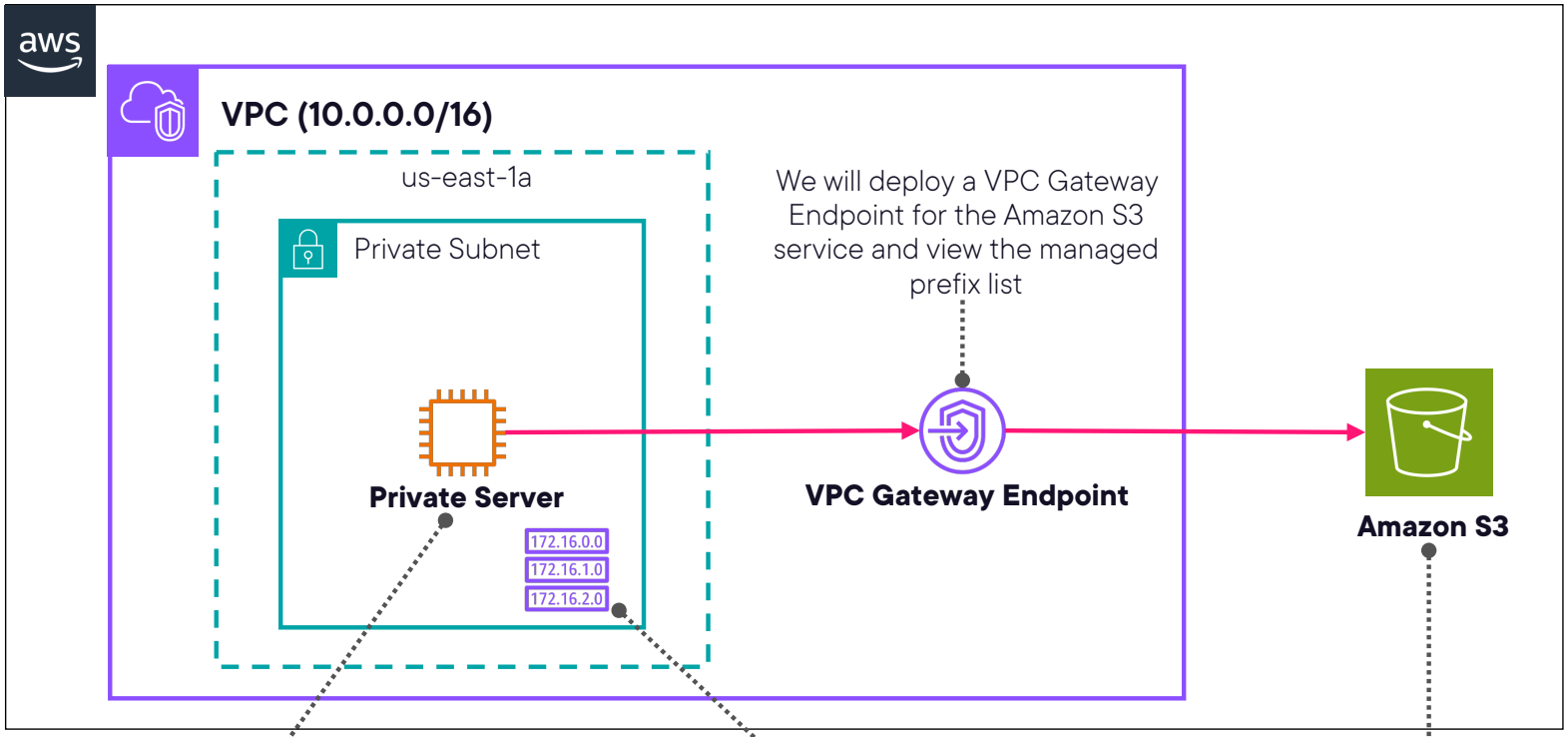
Pro Exam Tip 1: Gateway Endpoints do not require any security group updates!

Pro Exam Tip 2: These currently only support Amazon S3 and Amazon DynamoDB.

Gateway VPC Endpoints Architecture Diagram



Demo: Gateway Endpoints



Interface Endpoints

Interface Endpoints

Deploys an Elastic Network Interface (ENI)* into chosen VPC subnets

Requires management of an attached security group

Supports more services than gateway endpoints, but costs money for each ENI

** An ENI is essentially a virtual network interface for a VPC*

Interface Endpoints - DNS Resolution

Traffic is sent to AWS services via private endpoints, which require use of Regional and zonal DNS names

Regional DNS Name

vpce-078bad00d40f22a11.logs.us-east-1.vpce.amazonaws.com

Interface Endpoints - DNS Resolution

Traffic is sent to AWS services via private endpoints, which require use of Regional and zonal DNS names

Regional DNS Name

vpce-078bad00d40f22a11.logs.us-east-1.vpce.amazonaws.com

The VPC Endpoint ID

Interface Endpoints - DNS Resolution

Traffic is sent to AWS services via private endpoints, which require use of Regional and zonal DNS names

Regional DNS Name

vpce-078bad00d40f22a11.logs.us-east-1.vpce.amazonaws.com

Service ID

Interface Endpoints - DNS Resolution

Traffic is sent to AWS services via private endpoints, which require use of Regional and zonal DNS names

Regional DNS Name

vpce-078bad00d40f22a11.logs.us-east-1.vpce.amazonaws.com

Region Code

Interface Endpoints - DNS Resolution

Traffic is sent to AWS services via private endpoints, which require use of Regional and zonal DNS names

Regional DNS Name

vpce-078bad00d40f22a11.logs.us-east-1.vpce.amazonaws.com

VPC Endpoint

Interface Endpoints - DNS Resolution

Traffic is sent to AWS services via private endpoints, which require use of Regional and zonal DNS names

Zonal DNS Name

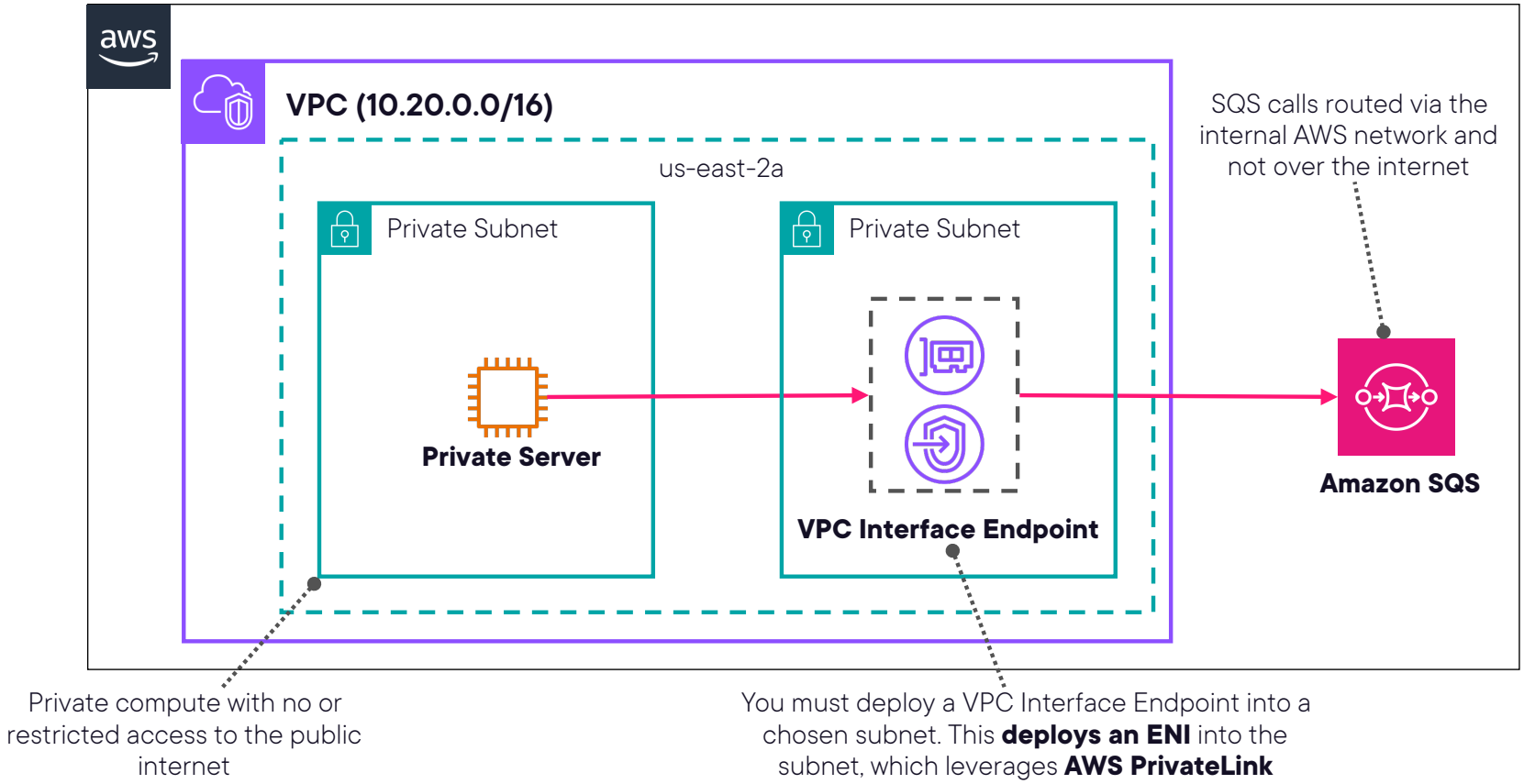
vpce-078bad00d40f22a11-us-east-1b.logs.us-east-1.vpce.amazonaws.com

Availability Zone Name

Private DNS

Enabling this feature in your VPC enables you to make requests to a service using the public endpoint DNS name, all while leveraging private connectivity via the interface VPC endpoint.

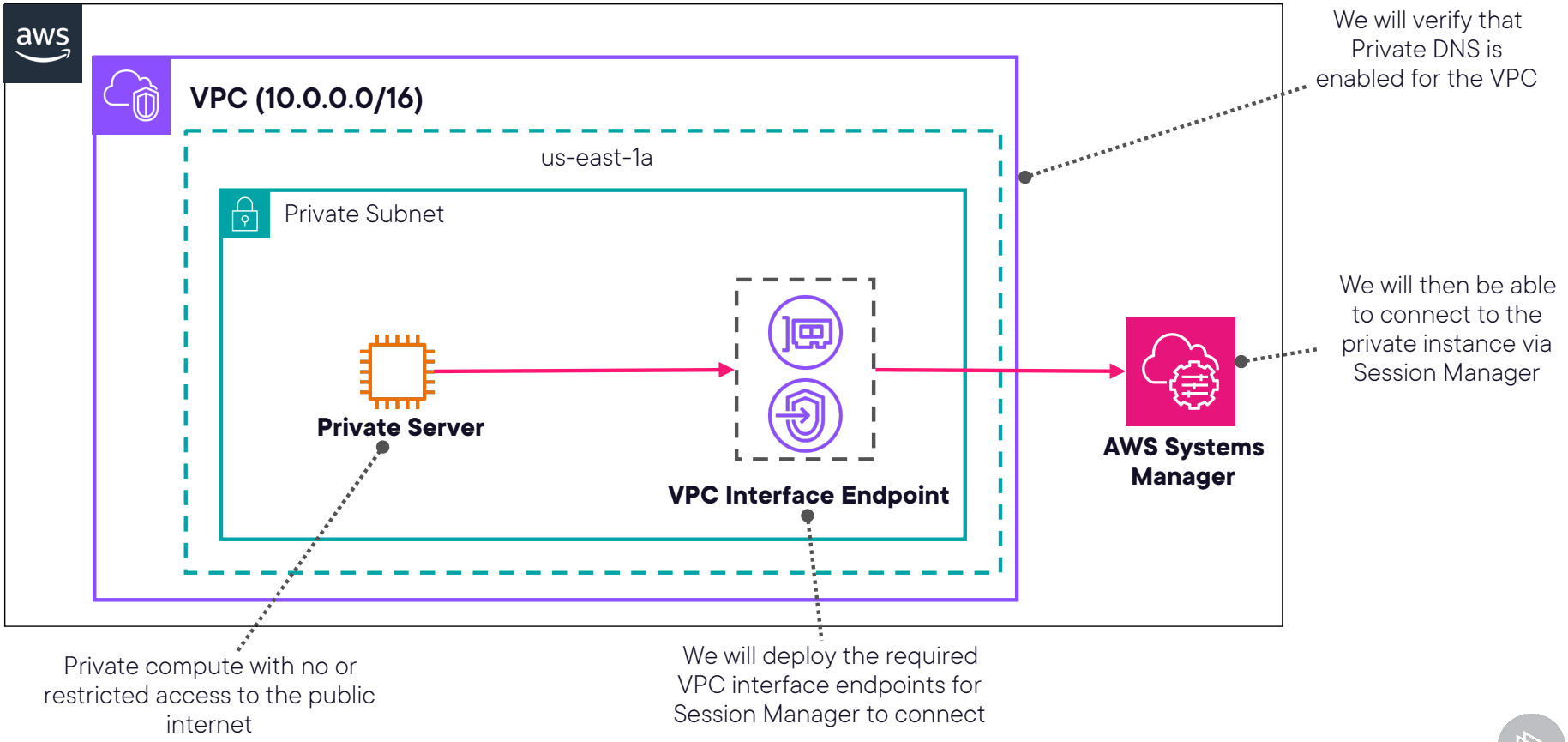
Interface VPC Endpoints Architecture Diagram



Amazon S3 can leverage both types of endpoints!

Choosing the right endpoint type will likely come down to a very specific requirement within the exam scenarios.

Demo: Interface Endpoints



Module Summary and Exam Tips

NAT Gateway Review

Redundant within the deployed AZ

Scales automatically up to 100 Gbps

No infrastructure to manage

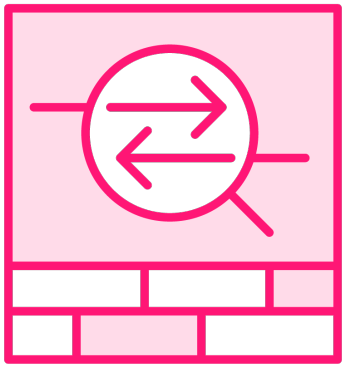
Allow private resources to reach the internet securely

Deploy them into multiple AZs for true high-availability

Remember that NAT Gateways need to be in a public subnet to allow internet access!

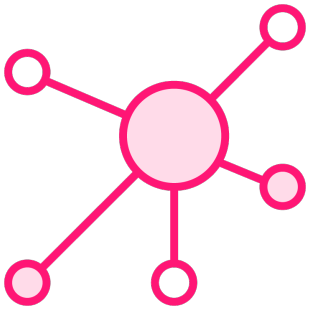
VPC Peering

Securely connect VPCs via a direct network route



Peer across Regions, and across account

No transitive routing



Compute behaves as if they're on the same network

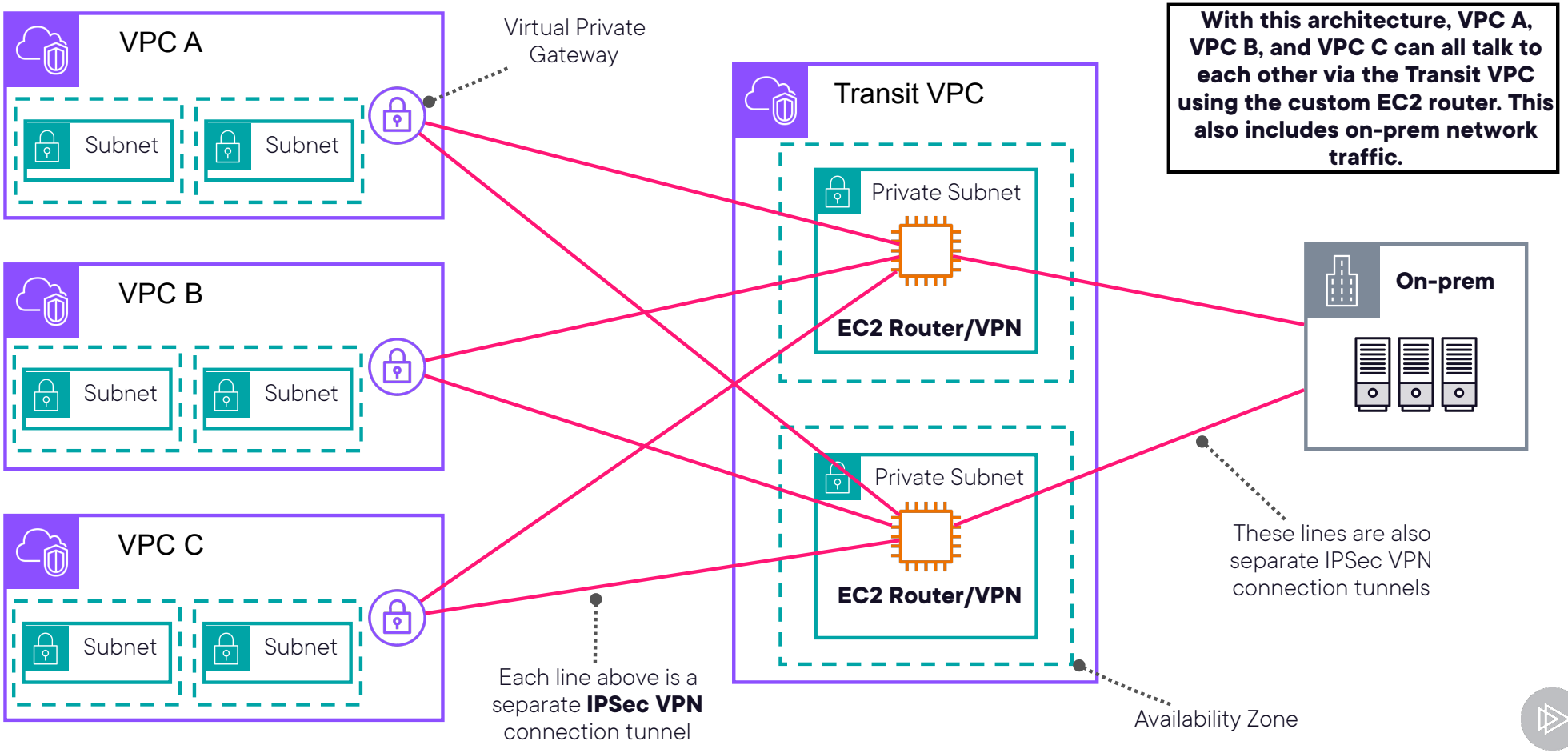
VPCs cannot be peered if they have any overlapping CIDR blocks!

Two Parts to VPC Peering

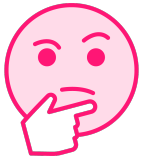
Requestor VPC requests a VPC peering connection

Accepter VPC can accept or deny the VPC peering connection

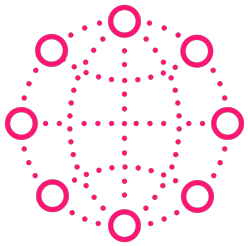
Transit VPC Architecture Diagram



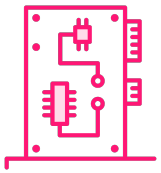
AWS PrivateLink Review



If you see a question asking about peering VPCs to tens, hundreds, or thousands of customer VPCs to access a service, think AWS PrivateLink



Doesn't require VPC peering; no route tables, NAT gateways, internet gateways, etc.



Requires a Network Load Balancer on the service provider VPC side and a shared ENI on the consumer VPC side

VPC Endpoints

Perfect for when you want to connect AWS services without leaving the Amazon internal network

2 types of endpoints:

- Interface (*Cost money*)
- Gateway (*Free*)

Gateway endpoint supported services:

- Amazon S3
- Amazon DynamoDB

Remember that Amazon S3 can leverage both types of endpoints!