

# Building Virtual Private Cloud (VPC) Networks

---



**Kien Bui**

DevOps & Platform Engineer

# Virtual Private Cloud



AWS manages underlying VPC infrastructure and is responsible for reliability of VPC network components

You still must design your VPC properly to take advantage of its reliability

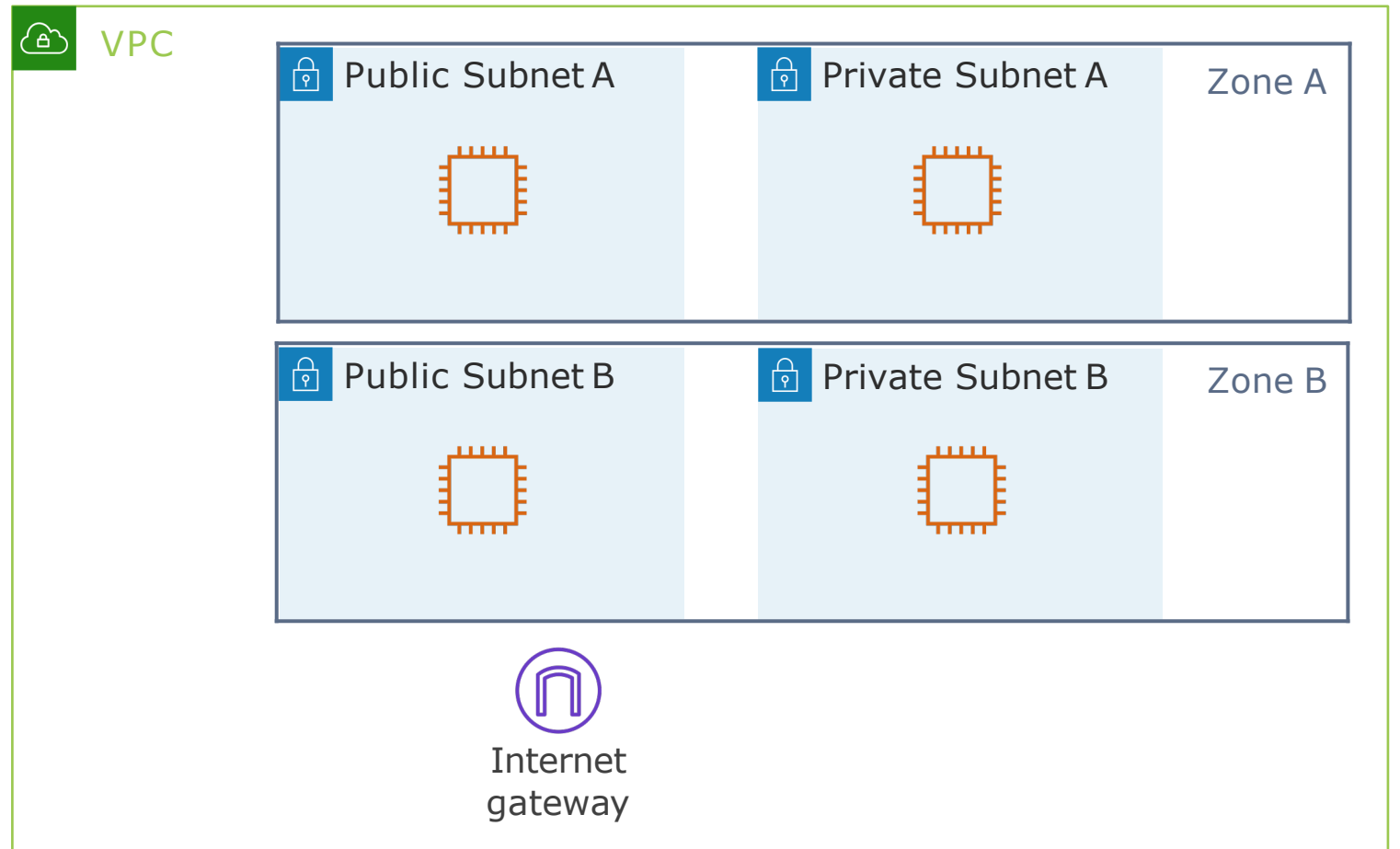
# **VPCs, Subnets, and Instances**

VPC contains one or more subnets

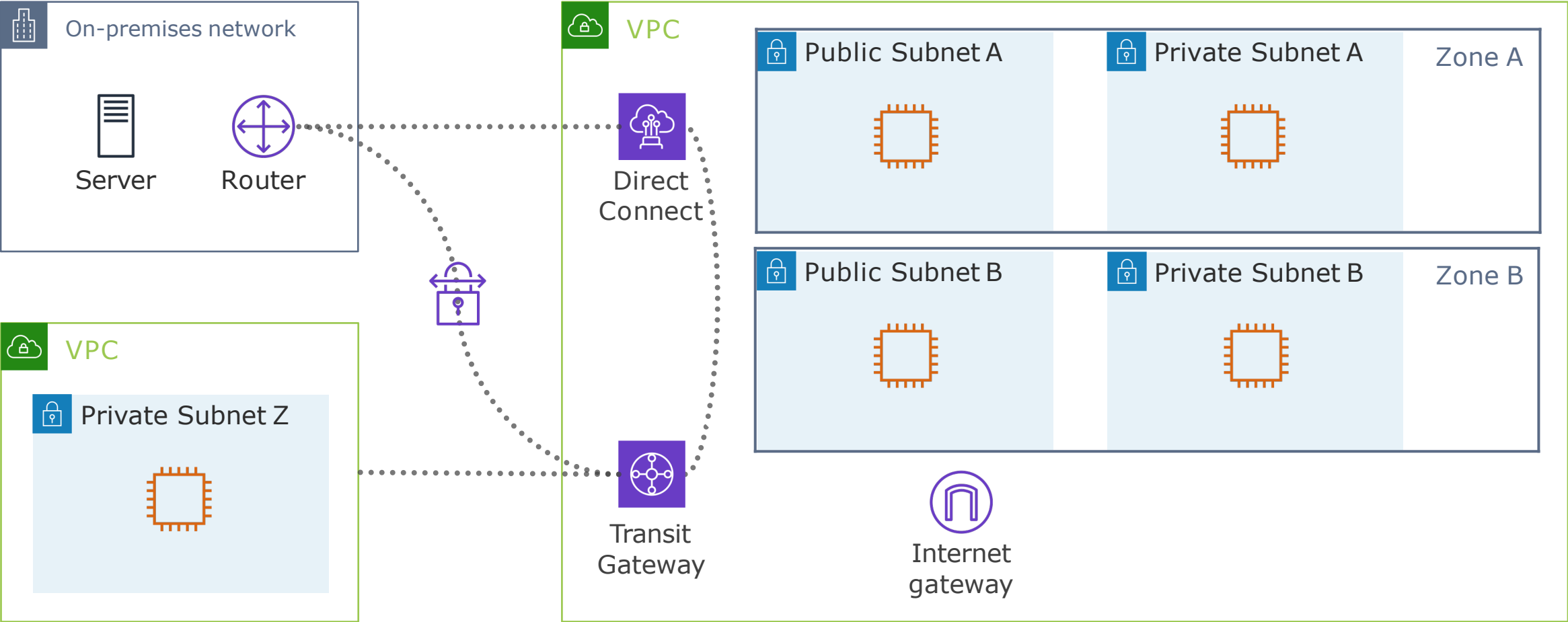
- A subnet exists in an availability zone
- An instance exists in a subnet

You achieve redundancy by having instances in multiple subnets in different zones

# VPC Architecture



# VPC Architecture



# Module Overview



Allocating an elastic IP address

Creating a VPC

Creating public and private subnets

Launching instances into subnets

Direct Connect

Transit gateways

# Allocating an Elastic IP Address

---

# Elastic IP Address (EIP)



You allocate an EIP to your account and keep it as long as you want

EIP allows an instance to retain the same public IP address

EIP is bound to an ENI, which is attached to an instance

You can move an EIP to different ENI



**If an instance has a public IP address, allocating an EIP to the instance will replace the public IP address.**

# Types of Elastic IP Addresses

## Amazon owned

Tied to an AWS region

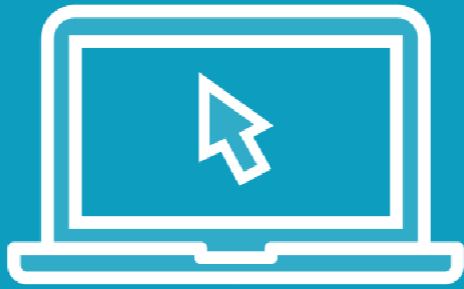
AWS picks the address for you

## Customer owned

Bring your own IP (BYOIP)

Pick any address you want

# Demo



Allocate an elastic IPaddress

# Global Accelerator

---

# Global Accelerator



Provides two anycast IPv4 addresses

Not tied to any AWS region

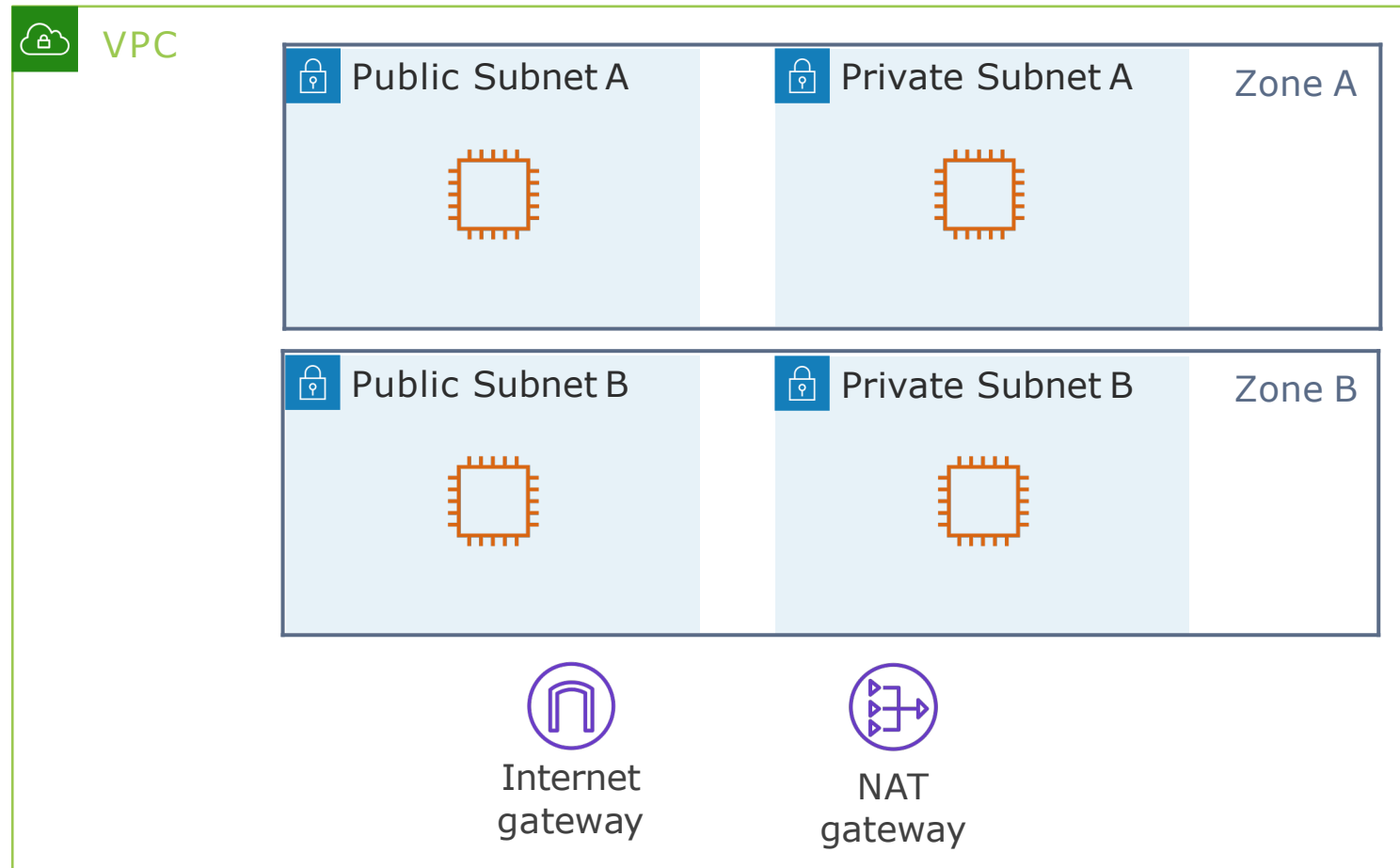
Advertised from points-of-presence (POPs) around the world

Connections to a Global Accelerator address can be forwarded to resources in any AWS region

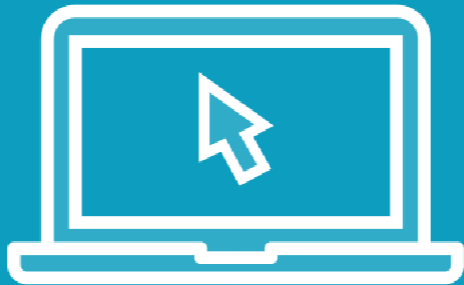
# Creating a VPC

---

# VPC Architecture



# Demo



Use the new VPC wizard to create a new VPC

- Public and private subnet
- NAT gateway



# Public Subnet

Associated with a route table that has a route with an Internet gateway as its target

# Route Tables

Public route table	
Destination	Target
0.0.0.0/0	Internet gateway

Private route table	
Destination	Target
0.0.0.0/0	NAT gateway

# NAT Gateway

Has two interfaces:

- Private subnet
- Public subnet

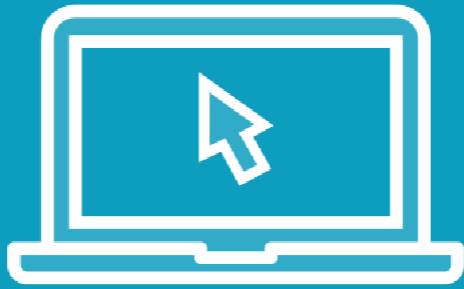
Instance in private subnet sends Internet-bound traffic to NAT gateway

NAT gateway sends traffic to Internet gateway

# Creating Public and Private Subnets

---

# Demo



Create a new public and private subnet in a different zone

# Launching an Instance into a Public Subnet

---

# Demo



Launch instance into public subnet B  
(10.0.11.0/24)

Allocate another elastic IPaddress

Associate it with theinstance

Terminate the instance

# AWS Shield Standard



Free service that detects against distributed denial-of-service (DDoS) attacks

Always on



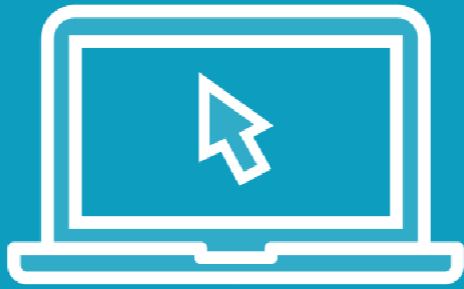
# Launching an Instance into a Private Subnet

---

```
$ aws ec2 run-instances --image-id ami-01d025118d8e760db --subnet-id [private-subnet-id] --instance-type t3.micro
```

## Launching an Instance into a Private Subnet

# Demo



Delete the NAT gateway

Release its elastic IP address

# Direct Connect and Transit Gateway

---

# Connectivity Options



Direct Connect



Virtual private network (VPN)

# **Direct Connect**

Low-latency connection to an AWS region

Bypasses the Internet

Two types:

- Dedicated
- Hosted

# Direct Connect Dedicated Connection

Physical connection that  
terminates at a Direct  
Connect location

1or 10 Gbps

# Direct Connect Hosted Connection

“Last-mile” connection  
provided by a Direct  
Connect partner

50 Mbps to 10 Gbps



# **VPN Connection**

Encrypted IPsec connection over the Internet

Unpredictable latency

Can be implemented in two ways

- Virtual private gateway
- Transit gateway

# Virtual Private Gateway



Enables you to establish a VPN tunnel with only one VPC

Doesn't scale well

# Transit Gateway



Connects VPCs and on-premises networks

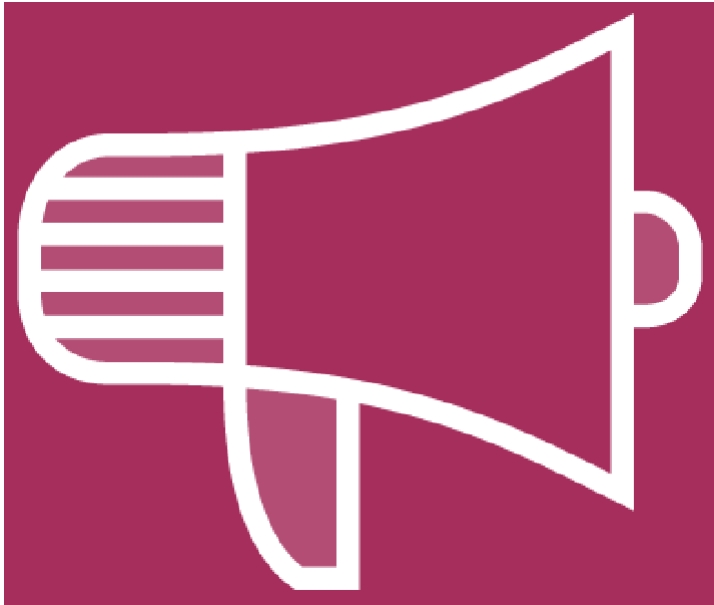
- Terminates multiple VPN connections
- Supports Direct Connect

Connects multiple VPCs together

# Transit Gateway Route Tables


Control how traffic is routed between subnets

Can block (blackhole) traffic



---

Transit gateway supports multicast!

# Connecting VPCs Using a Transit Gateway

---

# Demo



Create a transit gateway

Create two new VPCs

- One subnet each

Attach transit gateway to the subnets

# Summary

y



Allocating and assigning elasticIP addresses

Creating VPCs

Creating public and private subnets

Launching instances into subnets

Transit gateways



# Coming up Next



Automated deployments with  
CloudFormation