# Virtual Private Cloud

CHAPTER 3

# Virtual Private Cloud (VPC) Overview

EPISODE 3.01

# Virtual Private Cloud (VPC)


- Not yo mamma's Microsoft VPC
- "Virtually" private
- Personal data center in the cloud
- VPN connections can be made to the VPC

# VPC Provisions

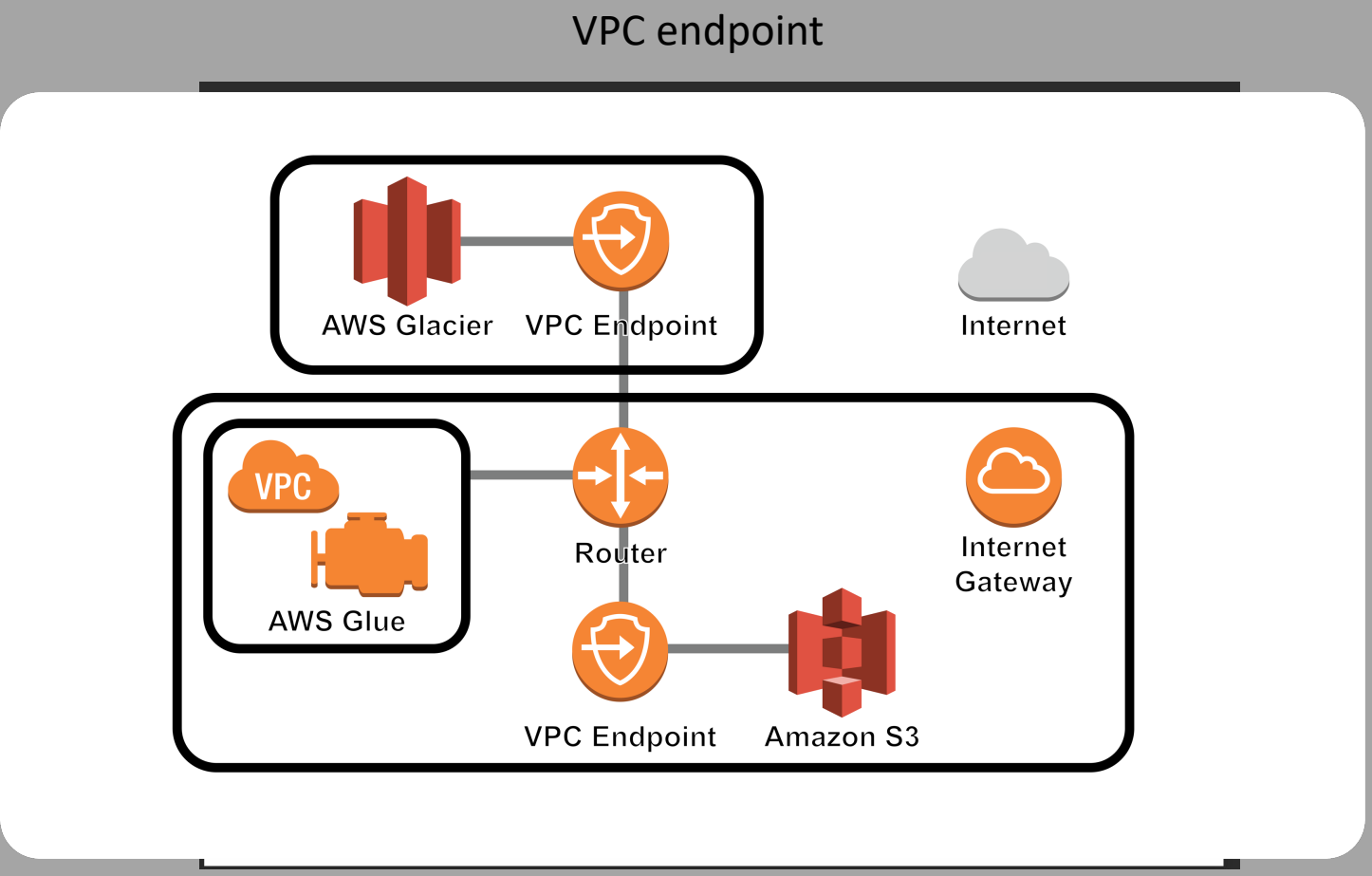
- Applications run in the VPC or on-premises
- Subnets can be created in the VPC
  - Public subnets
  - Private subnets

# VPC Provisions

- Direct Connect can provide VPN connections
- Multiple VPCs can be interconnected

# VPC Provisions

- VPC endpoints connect to resources



# The Default VPC

- One in each Region
- Amazon recommends not deleting
- Features:
  - Dynamic private IP
  - Dynamic public IP
  - AWS-provisioned DNS names
  - Private DNS names
  - Public DNS names

# Creating a VPC Lab

EPISODE 3.02

# Configuring DHCP Options Lab

EPISODE 3.03

# Elastic IP Addresses (EIPs)

EPISODE 3.04

# EIPs

- Public IP addresses from the VPC Region
- Permanently allocated to your account until released
- Account is charged until release

# EIPs

- Network interfaces consume EIPs
- EIPs can be moved between instances in the same Region

# Elastic Network Interfaces (ENIs)

EPISODE 3.05

# ENIs

- Virtual network interface attached to an instance
- Only available within a VPC
- Associated with a subnet

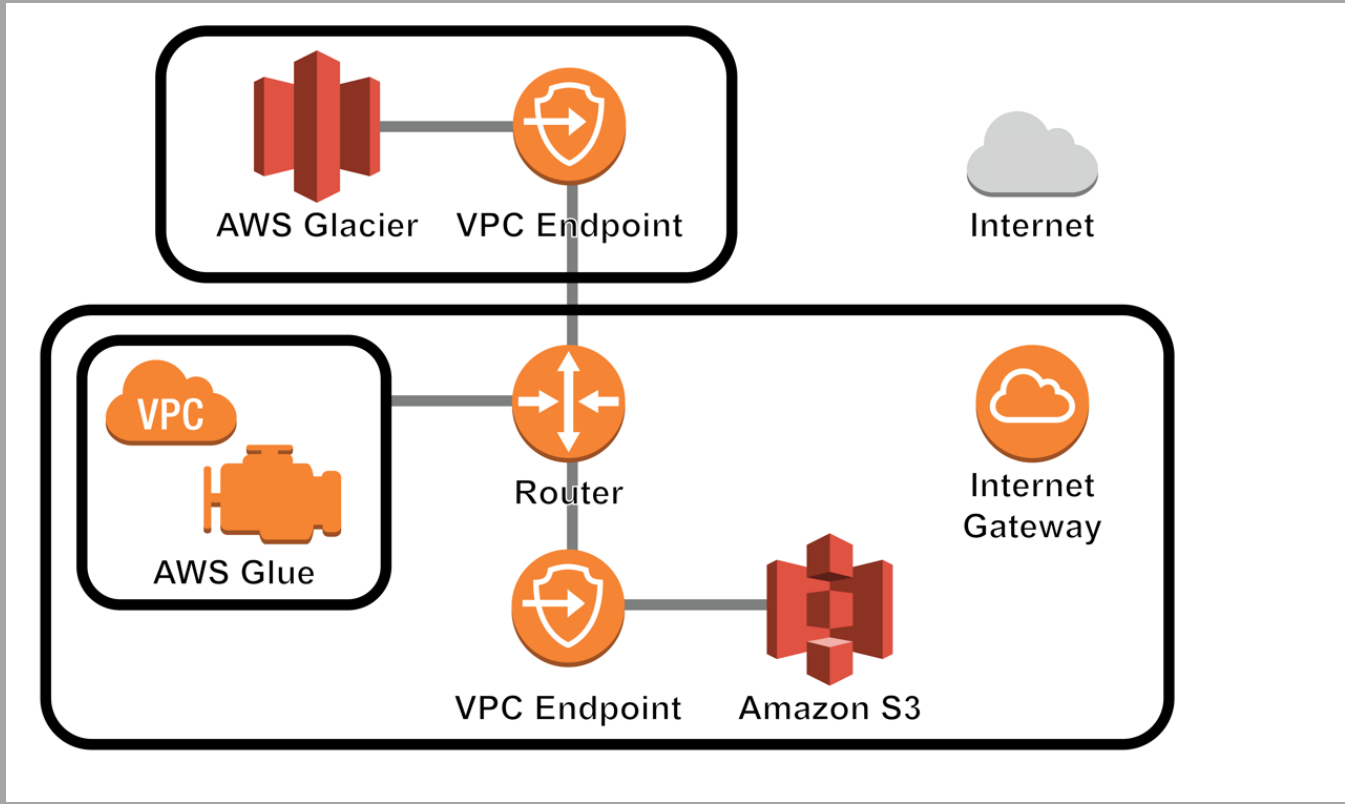
# ENIs

- Allows dual-homing
- One public address and multiple private addresses

# Endpoints

EPISODE 3.06

# Endpoints




- AWS endpoints connect VPCs to AWS services
- Can enforce policies on different endpoints

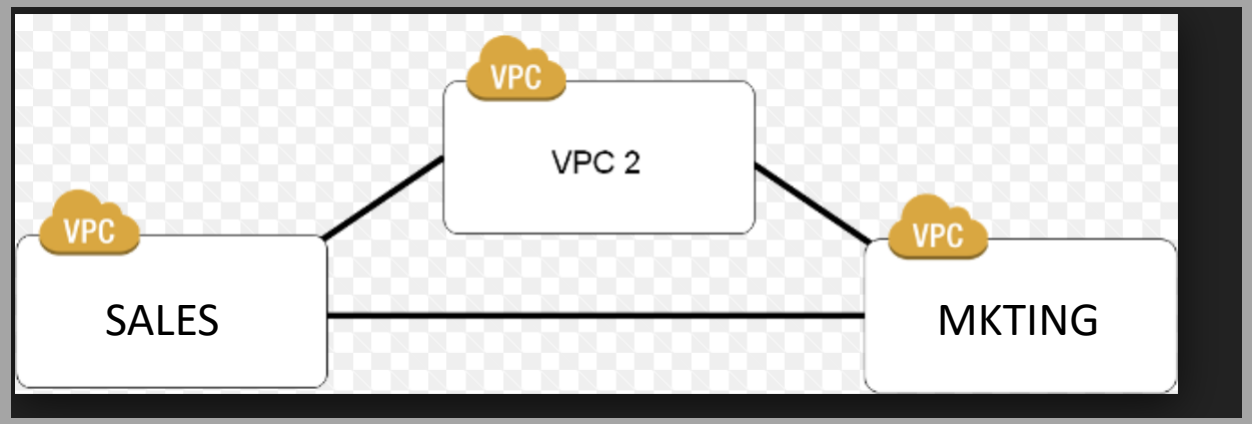
# Creating an Endpoint

- Specify the Amazon VPC
- Specify the service
  - com.amazonaws.<region>.<service>
- Specify the policy
- Specify route tables

# VPC Peering

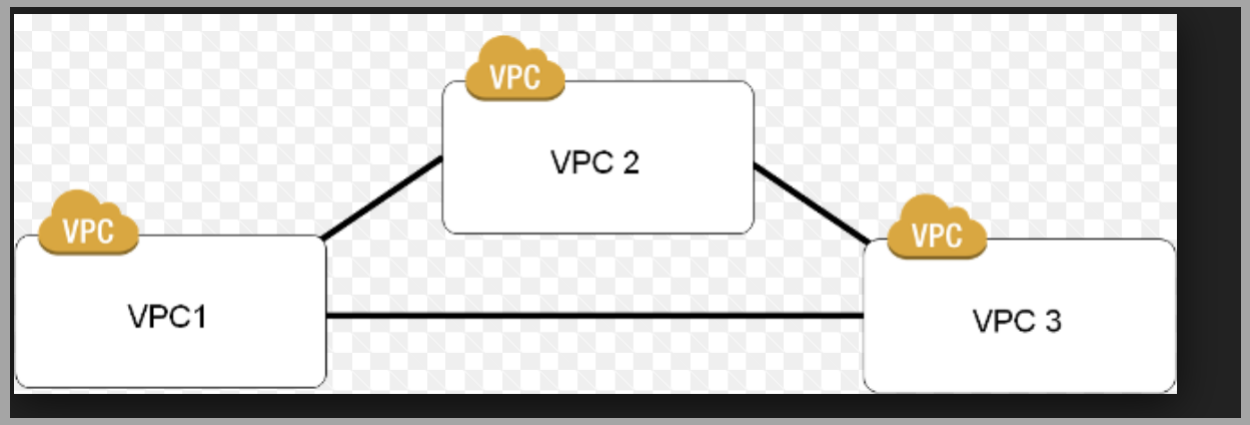
EPISODE 3.07

# VPC Peering




- Connects one VPC to another
- Many possible scenarios
  - Management VPC > Production VPC
  - Development VPC > Production VPC
  - Corporate VPC > Partner VPC

# VPC Peering




- VPC peering is not transitive
  - VPC A peered with VPC B
  - VPC B peered with VPC C
  - VPC A is not able to pass through VPC B to VPC C

# Creating VPC Peers

- Initiating VPC sends a request to the receiving VPC
  - Owner role required
  - IP CIDR blocks in each VPC must not overlap
- Receiving VPC accepts the request
  - Owner role required

# Creating VPC Peers

- Each VPC needs a defined route to the other VPC
  - May require routing table modifications
- Security group rules
  - May require modification for the VPC peers

# Creating a VPC Peering Connection Lab

EPISODE 3.08

# DEMO

- Creating a VPC peer

# Security Groups Overview

EPISODE 3.09

# Security Group Overview

- Acts like a firewall
  - Assigned to an instance in a VPC
  - Applied to instances not to subnets
- Defines allowed traffic flows
  - Ingress (entrance)
  - Egress (exit)

# Security Group Overview

- Supports only allow rules – deny is implicit
- Stateful processing is used

# Network Access Control Lists (NACLs)

- Applied on subnets
- Stateless processing
- Supports both allow and deny rules

# Network Access Control Lists (NACLs)

- Rule number defines precedence
  - Lowest numbered rules first
  - First match applies

# Network Address Translation (NAT)

EPISODE 3.10

# NAT Concepts

- NAT translates between:
  - Private IP addresses
  - Public IP addresses

# NAT Instances

1. NAT implemented on a private and public subnet
   - EIP associated with NAT instance
2. Instances in the private subnet connect through the NAT instance

# NAT Gateways

- Work more like traditional NAT servers/appliances

# DEMO

- Creating a NAT instance
- Creating a NAT gateway

# Gateways (VPGs and CGWs)

EPISODE 3.11

# Virtual Private Gateway (VPG)

- Connects local networks to the VPC
- VPG is the VPN concentrator

# Customer Gateway (CGW)

- Physical device or software application
- Anchor on the customer side
  - Connects to the VPG

# Alternative Connections

- AWS hardware VPN
- AWS Direct Connect
- VPN CloudHub
- Software VPN

# DEMO

- Creating a VPC with VPN access

- EPISODE 3.01
- Virtual Private Cloud (VPC) Overview

# Virtual Private Cloud (VPC)

- Not yo mamma's Microsoft VPC
- "Virtually" private
- Personal data center in the cloud
- VPN connections can be made to the VPC

# VPC Provisions

- Applications run in the VPC or on-premises
- Subnets can be created in the VPC
  - Public subnets
  - Private subnets

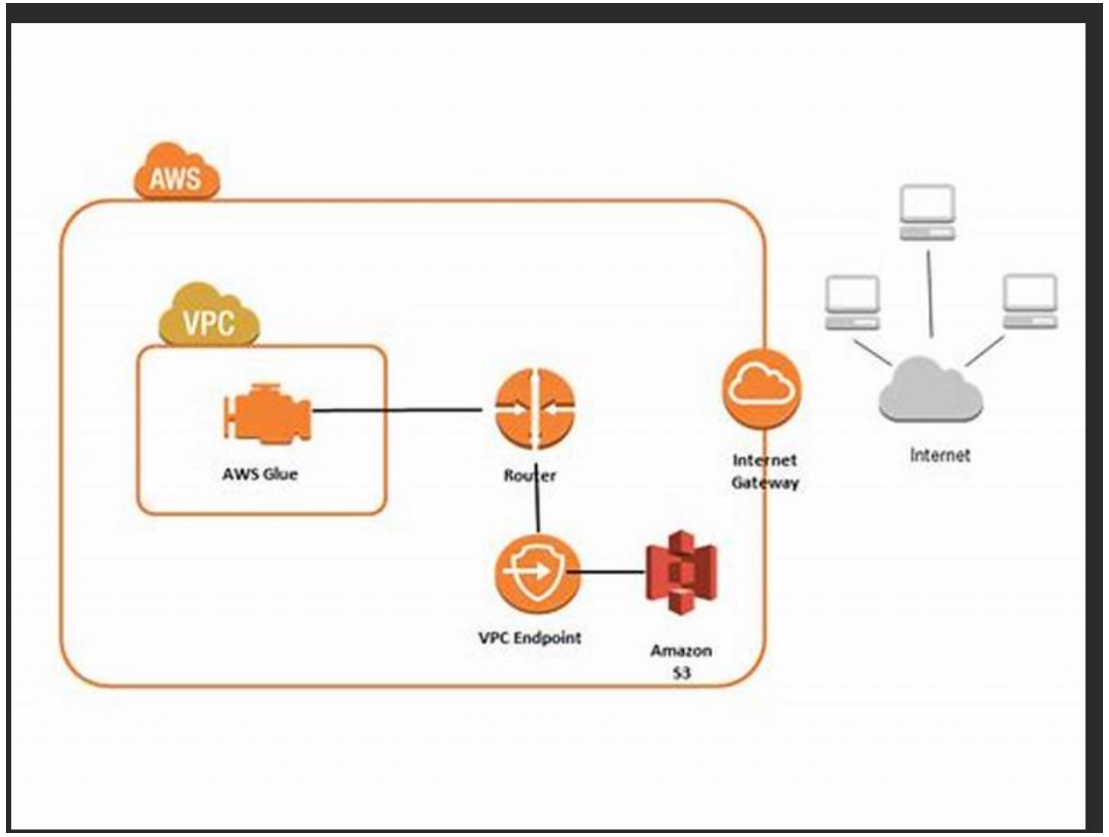
# VPC Provisions

- Direct Connect can provide VPN connections
- Multiple VPCs can be interconnected

VPC endpoint

# VPC Provisions

- VPC endpoints connect to resources



# The Default VPC

- One in each Region
- Amazon recommends not deleting
- Features:
  - Dynamic private IP
  - Dynamic public IP
  - AWS-provisioned DNS names
  - Private DNS names
  - Public DNS names

- EPISODE 3.02
- VPC Lab

- EPISODE 3.03
- DHCP Lab

- EPISODE 3.04
  - Elastic IP (EIP) Addresses

# EIPs

- Public IP addresses from the VPC region
- Permanently allocated to your account until released
- Account is charged until release

# EIPs

- Network interfaces consume EIPs
- EIPs can be moved between instances in the same region

- EPISODE 3.05
- Elastic Network Interfaces (ENI)

# ENIs

- Virtual network interface attached to an instance
- Only available within a VPC
- Associated with a subnet

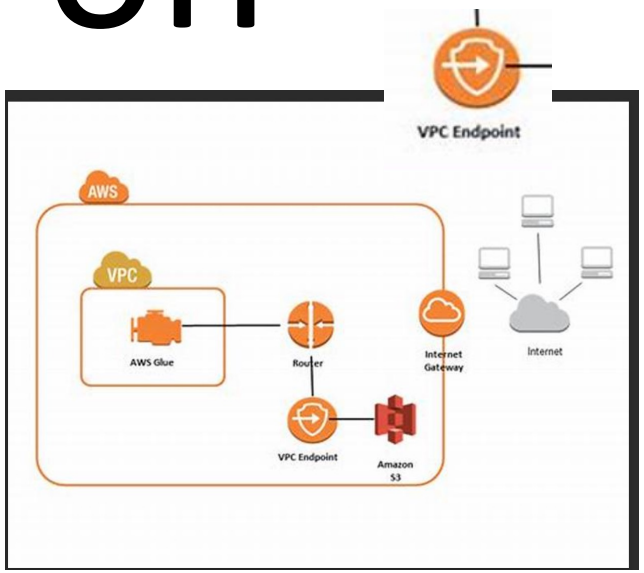
# ENIs

- Allows dual-homing
- One public address and multiple private addresses

- EPISODE 3.06
- Endpoints

# Endpoints

- AWS endpoints connect VPCs to AWS services
- Can enforce policies on different endpoints



# Creating an Endpoint

- Specify the Amazon VPC
- Specify the service
  - com.amazonaws.<region>.<service>
- Specify the policy
- Specify route tables

- EPISODE 3.07
- VPC Peering

# VPC Peering

- Connects one VPC to another
- Many possible scenarios
  - Management VPC > Production VPC
  - Development VPC > Production VPC
  - Corporate VPC > Partner VPC

# VPC Peering

- VPC peering is not transitive
  - VPC A peered with VPC B
  - VPC B peered with VPC C
  - VPC A is not able to pass through VPC B to VPC C

# Creating VPC Peers

- Initiating VPC sends a request to the receiving VPC
  - Owner role required
  - IP CIDR blocks in each VPC must not overlap
- Receiving VPC accepts the request
  - Owner role required

# Creating VPC Peers

- Each VPC needs a defined route to the other VPC
  - May require routing table modifications
- Security group rules
  - May require modification for the VPC peers

- EPISODE 3.08
- VPC Peering Lab

# DEMO

- Creating a VPC peer

- EPISODE 3.09
- Security Groups

# Security Group Overview

- Acts like a firewall
  - Assigned to an *instance* in a VPC
  - Applied on instances not on subnets
- Defines allowed traffic flows
  - Ingress
  - Egress

# Security Group Overview

- Supports only allow rules – deny is implicit
- Stateful processing is used

# Network Access Control Lists (NACLs)

- Applied on subnets
- Stateless processing
- Supports both allow and deny rules

# Network Access Control Lists (NACLs)

- Rule number defines precedence
  - Lowest numbered rules first
  - First match applies

- EPISODE 3.10
- Network Address Translation (NAT)

# NAT Concepts

- NAT translates between:
  - Private IP addresses
  - Public IP addresses

# NAT Instances

1. NAT implemented on a private and public subnet
   - EIP associated with NAT instance
2. Instances in the private subnet connect through the NAT instance

# NAT Gateways

- NAT Gateways work more like traditional NAT servers/appliances

# DEMO

- Creating a NAT instance
- Creating a NAT gateway

- EPISODE 3.11
- Gateways (VPGs and CGWs)

# Virtual Private Gateway (VPG)

- Connects local networks to the VPC
- VPG is the VPN concentrator

# Customer Gateway (CGW)

- Physical device or software application
- Anchor on the customer side
  - Connects to the VPG

# Customer Gateway (CGW)

- Anchors the customer's side of the VPN
- Physical device or software application

# Alternative Connections

- AWS hardware VPN
- AWS Direct Connect
- VPN CloudHub
- Software VPN

# DEMO

- Creating a VPC with VPN access