Chapter 3
Virtual Private Cloud

Episode 3.01
Virtual Private Cloud (VPC) Overview

Virtual Private Cloud (VPC)

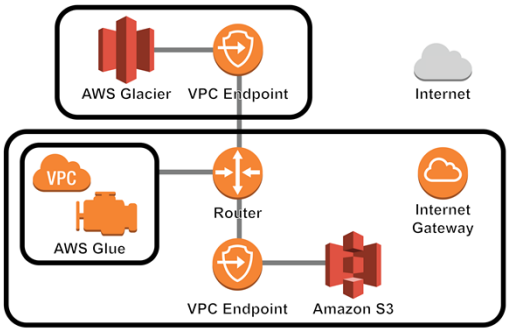
- Not the same as Microsoft's older VPC
- A cloud that is "virtually" private
- Like a data center in the cloud
- VPN connections can be made to the VPC

VPC Provisions

- Applications run in the VPC or on-premises
- Subnets can be created in the VPC
  - Public subnets
  - Private subnets
- Direct Connect provides VPN connections
- Multiple VPCs can be connected

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
Creating a VPC Lab

DEMO

- Creating VPCs
- Creating subnets in a VPC
- Connecting VPCs with Direct Connect

Episode 3.03
Configuring DHCP Options Lab

DEMO

- Creating DHCP option sets

Episode 3.04
Elastic IP Addresses (EIPs)

Elastic IP Addresses (EIPs)

- Public IP addresses from the VPC region
- Permanently allocated to your account until released
- Account is charged until release
- Network interfaces consume EIPs
- EIPs can be moved between instances in the same region

DEMO

- Creating an EIP

Episode 3.05
Elastic Network Interfaces (ENIs)

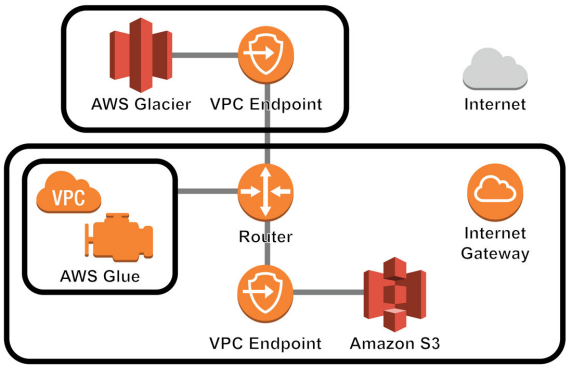
Elastic Network Interfaces (ENIs)

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

DEMO

- Creating an endpoint

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 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

- Owner role of one VPC sends a request to the other VPC
  - IP CIDR blocks in each VPC must not overlap
- Owner of the other VPC accepts the request
- Each VPC needs a route to the other VPC in their route tables
- Security group rules may require updates

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
Creating a VPC Peering Connection Lab

DEMO

- Creating a VPC peer

Episode 3.09
Security Groups

Security Group Overview

- Like a firewall assigned to an instance in a VPC
- Defines allowed traffic flows
  - Ingress
  - Egress
- Applied at the instance level rather than the subnet level
- Supports only allow rules – deny is implicit
- Stateful processing is used

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 at the subnet level
- Stateless processing
- Supports both allow and deny rules
- Rule number defines precedence
  - Lowest numbered rules first
  - First match applies

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)
SAGEFOX

NAT Concepts

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

SAGEFOX

NAT Instances

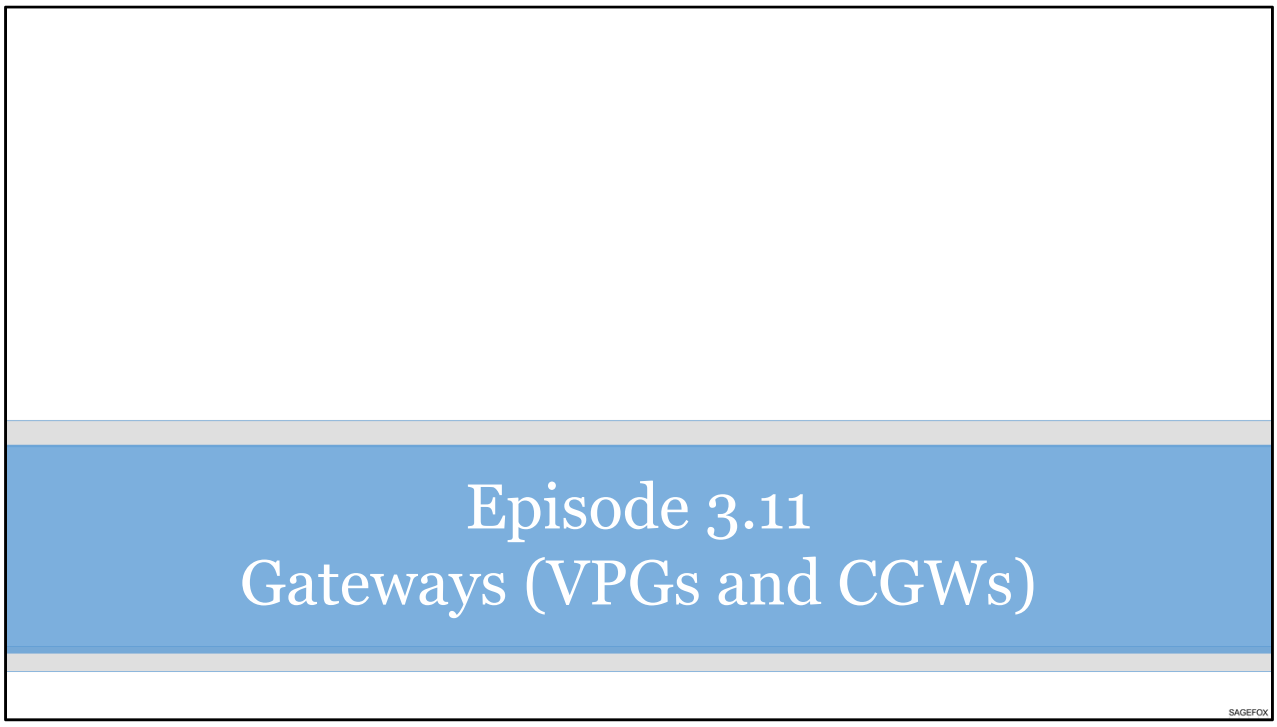
- NAT implemented on a private and public subnet
  - EIP associated with NAT instance
- Instances in the private subnet connect through the NAT instance

SAGEFOX

NAT Gateways

- Work more like traditional NAT servers/appliances

SAGEFOX


Episode 3.11
Gateways (VPGs and CGWs)
SAGEFOX

Virtual Private Gateway (VPG)

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

SAGEFOX

Customer Gateway (CGW)

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

SAGEFOX

Alternative Connections

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

SAGEFOX