Virtual Private Cloud (VPC)

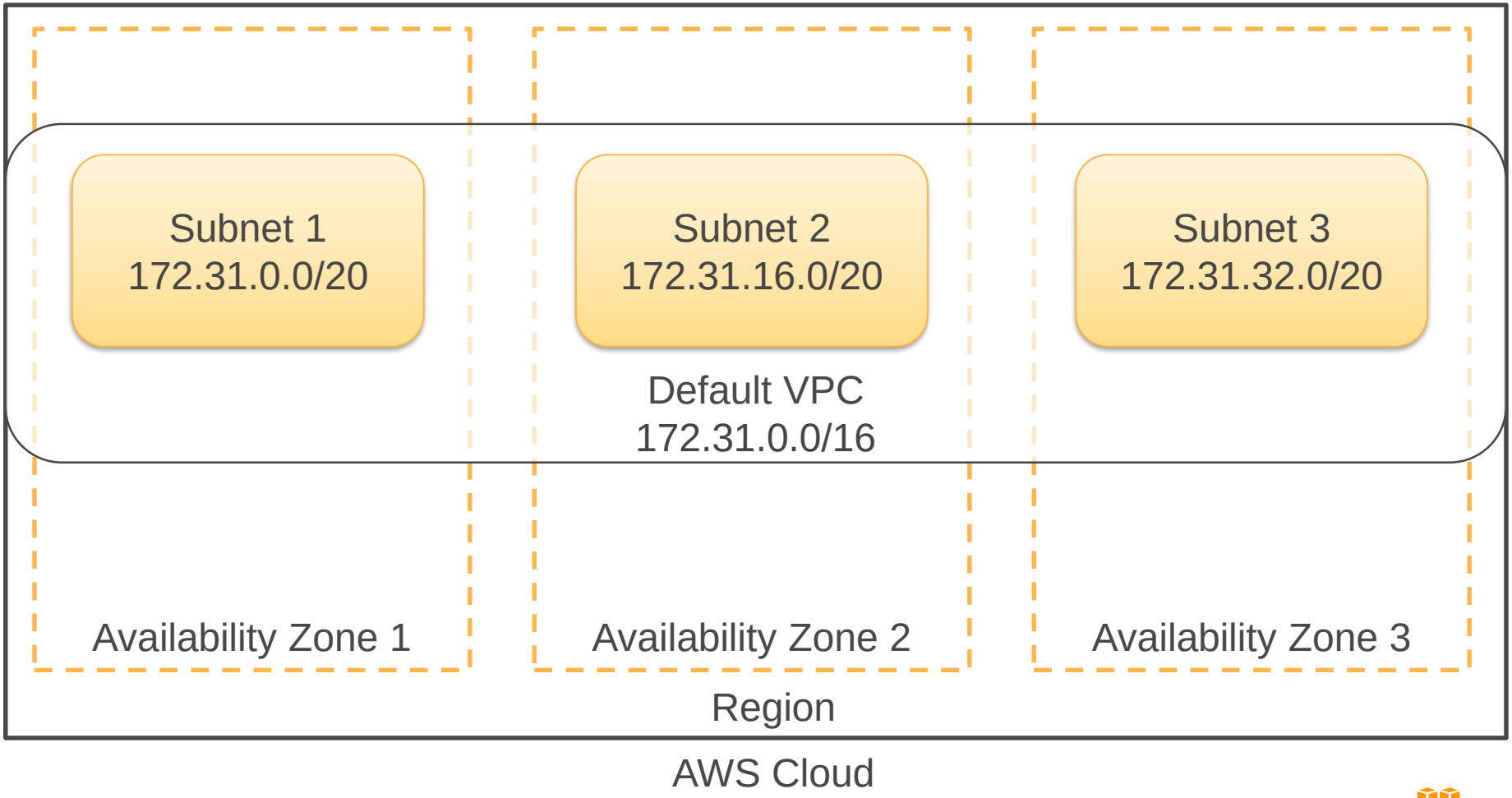
Your own private network in the AWS cloud

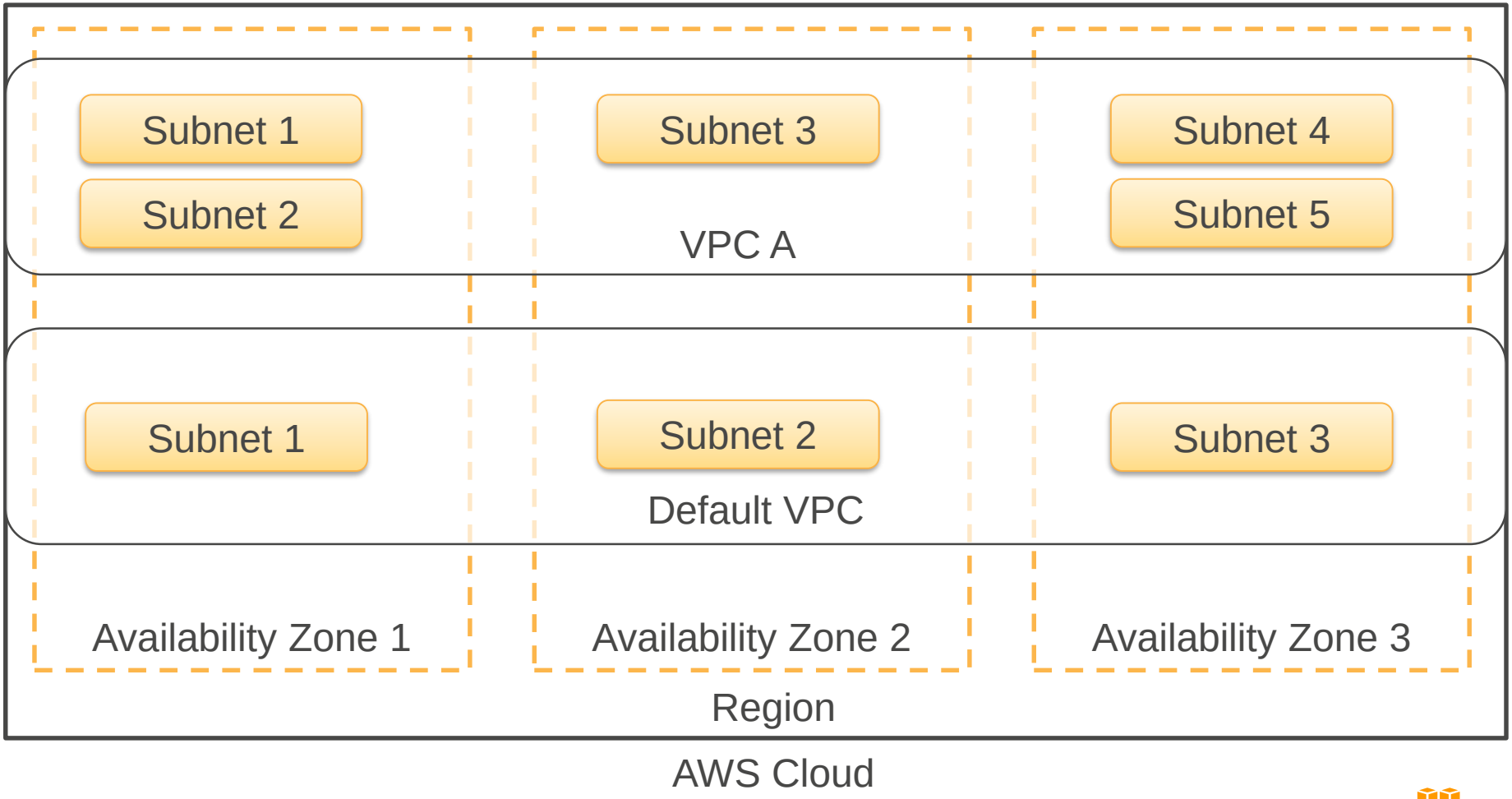
Content Prepared By: Chandra Lingam, Cloud Wave LLC

amazon web services

VPC

- Virtual Network Dedicated to your AWS Account
- Logically isolated from other virtual networks in the AWS Cloud
- Launch resources such as EC2 instances in your VPC
- Select your own IP Address range
- Create Subnets
- Configure route tables, network gateways
- Support for IPv4 and IPv6
- Simple to use





VPC Components

Component	Description
VPC	Isolated virtual network in AWS cloud
Subnet	Isolated segment of your VPC
Internet Gateway	VPC side of connection to internet
NAT Gateway	AWS managed Network Address Translation Service to make outbound internet connection from your private subnet (IPv4)
NAT Instance	Customer managed NAT (IPv4)
Egress-only Internet Gateway	IPv6 outbound internet access

VPC Components

Component	Description
Router	Routes traffic inside VPC
Security Group	Instance level stateful firewall. Supports only Allow rules
Network Access Control List	ACLs are subnet level stateless firewall. Supports Allow and Deny rules

Demo – Create Public VPC

- ***Create a VPC with Public Subnet***
- ***Launch EC2 instance***
- ***Connect to EC2 instance***
- Restrict Access to instance using Security Groups and Network Access Control List

VPC Security

Identity and Access Management (IAM)

Control who can create, manage and use VPCs

Firewalls

Control inbound and outbound traffic

Flow Logs

Capture information about IP traffic going to and from your VPC – Troubleshoot Issues, Monitor Traffic

Security - Firewall

Security Group – Firewall at EC2 instance level

Network Access Control List – Firewall at subnet level

Architecture Diagram

Table: Comparison of Security Group and Network ACL

Security – Flow Logs

Flow Log capture is configurable at VPC, Subnet or a network interface

Specify type of traffic to capture (ACCEPT or REJECT or ALL)

Traffic flow is recorded as *flow log record*

Flow Log Record Structure

Flow Log Record Captures network flow for 5-tuple consisting of :

- Source (*address and port*)
- Destination (*address and port*)
- Protocol

Flow Log Service aggregates data during a capture window (10-15 minutes) before publishing flow log records

Demo – Restrict Access with Firewall

- Create a VPC with Public Subnet
- Launch EC2 instance
- Connect to EC2 instance
- ***Restrict Access to instance using Security Groups and Network Access Control List***

Demo – Enable Ping (IPv4)

- Ping is used for checking if an instance is reachable over network
- EC2 Default Settings do not allow ping traffic
- Add Security Group Rule to allow *ICMP Rule for IPv4 Echo Request*

Demo – Enable IPv6 Support

- VPC uses IPv4; IPv6 is optional
- When enabled, IPv6 CIDR Block is assigned by AWS
- IPv4 and IPv6 traffic flows are treated separately
- Need to configure VPC, Subnet, Route Table, Network ACL, Security Groups to support IPv6
- Ping Command

  Linux: *ping6 <address>*

  Windows: *ping -6 <address>*

VPC Components – Hybrid Architecture

Component	Description
Internet	Suitable for Internet accessible resources
Hardware VPN Connection	Secure connection between your datacenter and VPC (over internet or over direct connect)
Virtual Private Gateway	AWS side of VPN connection
Customer Gateway	Customer side of VPN connection
Direct Connect	Dedicated Private connectivity between customer on-premises network/Offices to AWS

VPC Components – Connecting VPCs

Component	Description
Peering Connection	Connect two VPCs and access resources with private IP address
VPC Endpoint	Access AWS resources like S3, DynamoDB without using NAT or Internet Gateway. Limit access to resources from specific VPCs
Gateway Endpoint	New name for VPC Endpoints
Interface Endpoint	New Capability powered by AWS Private Link. Setup private connections to AWS Supported Services, Services hosted by AWS Partners, Customers and Marketplace partners

VPC Peering Connection

- VPC Peering connection connects two VPCs to make it into one logical network
- Data Transfer between Peered VPCs are on AWS private network and never traverses internet
- Address should not overlap between VPCs
- Instances can communicate using private IP addresses
- VPC Peering across regions supported as of Nov 2017

VPC Peering Connection

- Only one peering connection between two VPCs – It is bi-directional
- Multiple peering connections are supported from one VPC to multiple VPCs
- VPCs can be part of one account or different accounts
- Owner of the peer VPC needs to accept the request

Demo – Peering Connection (same region)

Setup peering connection between default VPC and PublicDemo VPC

Configure routes on both VPCs to allow traffic on peering connection

EC2 Instances ping using private IP over peering connection

Demo – Peering Across Regions

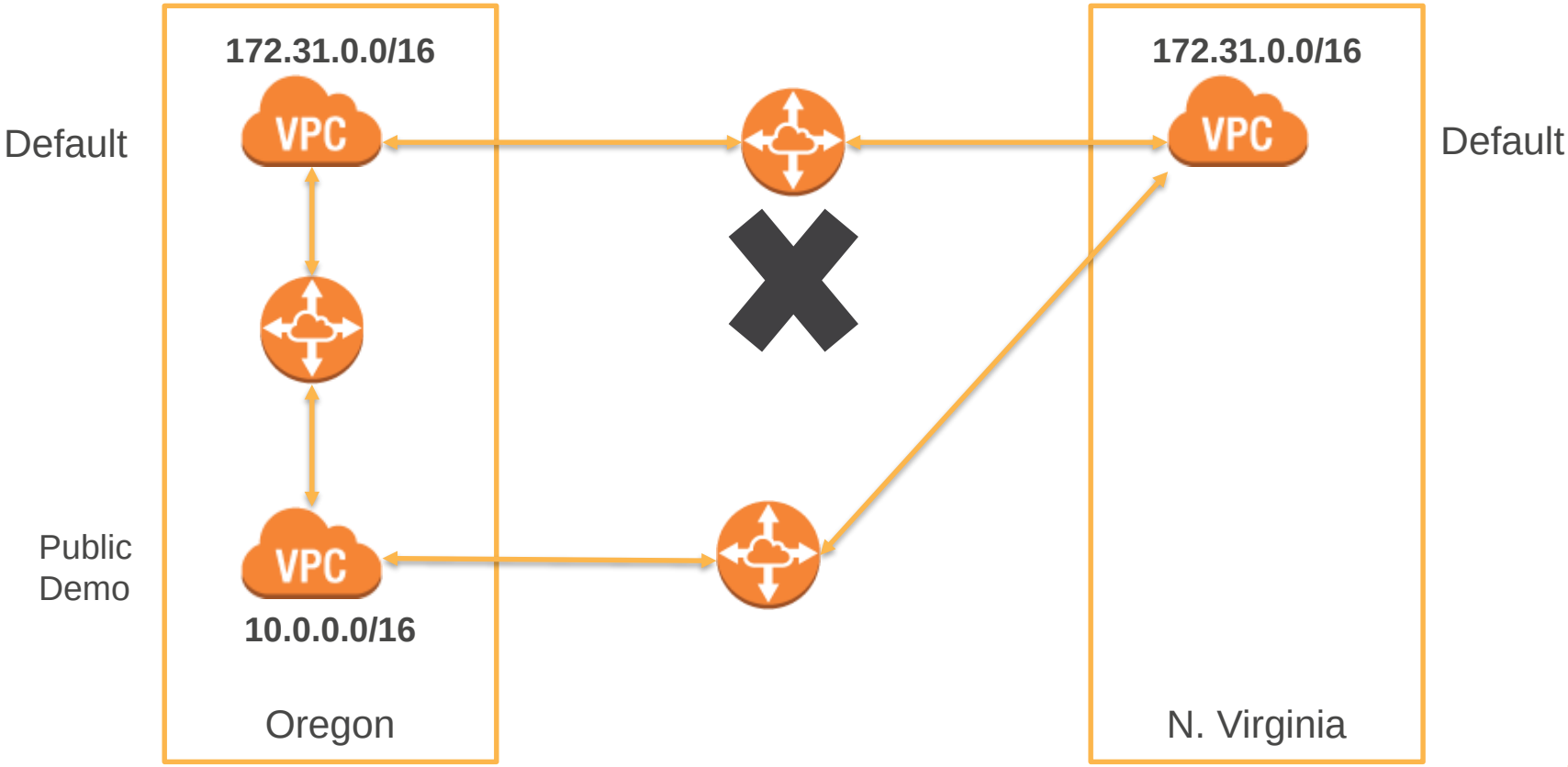
Create a peering connection between VPCs in Oregon and N. Virginia Regions

Configure Route Tables

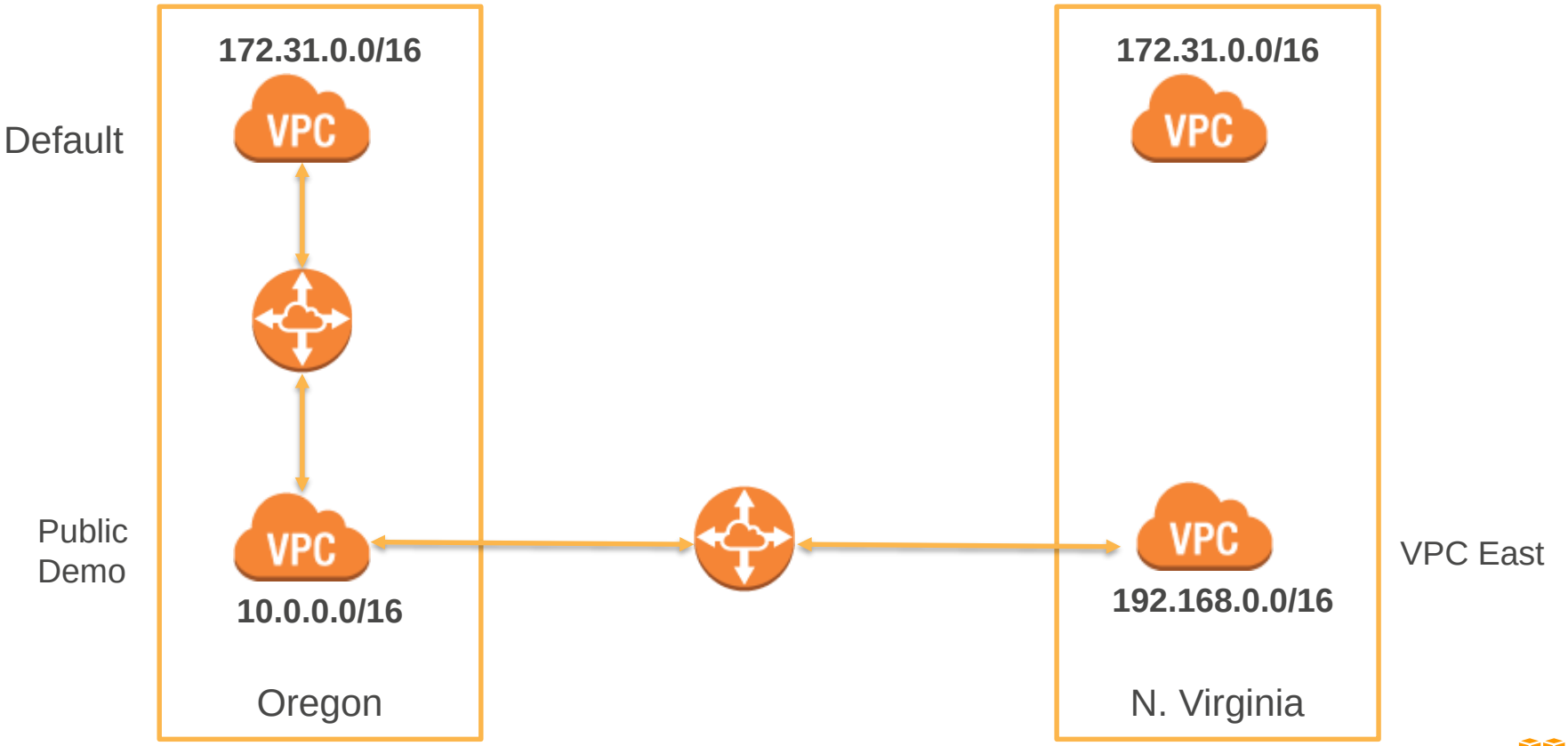
Observe Latency – Same Region and Cross Region

Check for Transitive Peering

Demo – Cross Region Setup Options



Demo – Cross Region Setup Options



amazon web services

Billing

- Pricing
- VPC – No additional charge for creating or using VPC
- VPN – $0.05 per VPN Connection Hour
- NAT Gateway
  - $0.045 per hour
  - $0.045 per GB data processed
- NAT Instance – Pricing varies based on Instance Type and applicable EC2 data transfer charges
  - $0.1 per GB to internet
  - $0.01 per GB for intra-region
  - $0.02 per GB for inter-region

Route Tables

- Most specific route that matches the traffic determine how traffic is routed
- VPC has a main route table that is implicitly applied to all subnets
- You can apply custom route table to a subnet
- You can make your custom table as main route table
- CIDR blocks are used to specify routes. IPv4 and IPv6 CIDR are treated separately

VPC Connectivity

- Connect to Internet from public subnets
- Connect to Internet from private subnets with Network Address Translation
- Connect to corporate datacenter using Virtual Private Network (VPN)
- Connect VPCs together using Peering
- Connect to S3 with private IP address using VPC endpoint
- Combine connectivity methods

History - Before VPC

- *EC2-Classic*. Original Release of EC2 supported a single, flat network that was shared with all customers
- Older AWS Accounts still support EC2-Classic
- VPC Benefits
    - Assign Static Private IP Addresses to your instance
    - Multiple IP Addresses per instance
    - Define network interface, attach one or more network interface to your instance
    - Security Groups and ACLs for ingress and egress filtering
    - Single Tenant Hardware Support

VPC Wizard

- VPC with a Single Public subnet
- VPC with Public and Private subnets
- VPC with Public and Private subnets and Hardware VPN Access
- VPC with Private subnet and Hardware VPN Access

VPC Configuration Examples

Default VPC

Non-default VPC with private only access

Non-default VPC with Elastic IP + Internet Gateway

Internet Access from public subnet - Inbound and Outbound

1. Attach Internet Gateway to your VPC
2. EC2 instances need to have either a public IP Address or Elastic IP address
3. Update Route
4. Connect to Internet or other AWS Services
5. Receive requests from Internet (Example: webserver)

VPC Configuration Examples

Non-default VPC Private subnet + NAT Gateway

Non-default VPC Private subnet + NAT Instance

Internet Access from Private subnet – Outbound Only

1. Attach Internet Gateway to your VPC
2. Attach Network Address Translation to your VPC Public subnet - NAT Gateway or NAT Instance
3. Attach Elastic IP to NAT
4. Update Route to send outbound internet traffic from Private subnet to NAT
5. Connect to Internet or other AWS Services

VPC Configuration Examples

VPC to Corporate/Home Network

VPN CloudHub

Extend your corporate datacenter to AWS Cloud

1. Attach Virtual Private Gateway to your VPC
2. Attach Customer Gateway to your datacenter
3. Establish IPSec VPN connection (encrypted channel)
4. Update Route to send traffic to Virtual Private Gateway
5. Connect to your datacenter systems from VPC and vice versa

VPC Configuration Examples

IPv6 Routing

IPv6 Internet Access from public subnet - Inbound and Outbound

1. IPv6 routes are separate from IPv4 routes
2. Attach Internet Gateway to your VPC
3. Add IPv6 CIDR to your VPC
4. Update route to send IPv6 traffic to Internet gateway
5. Update ACL, Security Group for IPv6
6. Launch instances in VPC
7. Connect to Internet or other AWS services

VPC Configuration Examples

IPv6 Traffic + Egress only Internet Gateways

Internet Access from Private subnet for IPv6 Traffic – Outbound Only

1. Attach Egress-only Internet Gateway to your VPC
2. Update Route to send IPv6 outbound internet traffic to egress only internet gateway
3. Connect to Internet or other AWS Services

VPC and AWS Services

List: VPC with other AWS Services

Deploy resources from other AWS services into your VPC

VPC Limits

Table: VPC Limits for your account

IPv4 and IPv6

Table: Comparison between IPv4 and IPv6