PGPCC - Mentor session

Flow and Structure for MS4

Course 2 Week 3

“VPC, R53, WAF”

Agenda

- Total duration 120 mins
- Recap and Case analysis (50)
- VPC at scale (5 mins)
- Local and Wavelength zones (5 mins)
- Q&A from participants (60 mins)

greatlearning

AWS Week 3 – VPC , Route 53, WAF

- Module 14 - VPC
- Module 15 – Hybrid Cloud and Networking
- Module 16 – Walkthrough AWS VPC Console
- Module 17 – Creating and using VPC- Step by Step
- Module 18 – VPC Peering
- Module 19 – VPC Endpoint, Services, Route 53 & VPC endpoint in S3 and Global Accelerator
- Module 20 –WAF Next Generation

Module 14 – N/W Overview & VPC

Overview of concepts :-

- ❑ VPC, **Public, Private** Subnets , **CIDR** blocks
- ❑ **Internet Gateway** (IG), **RT** (Route table), **Bastion Host/Jump Hosts**
- ❑ **NAT G/W**, NAT Instances
- ❑ **VPC Peering**, **VPC endpoints**, **R53**

- **VPC**
- ❑ Subnets Vs AZ
- ❑ What gets created automatically in default VPC ? – Default RT, Default SG, Default NACL, Subnets
- ❑ CIDR Explanation – Example – 10.0.1.0/20
- ❑ Does **AWS reserve** some **IP's** in CIDR ?
- ❑ Did you check in VPC Console on how many default VPC it lists ?
- ❑ **Peering** - What is it ? Transitive Peering – YES or NO

Why you need your own VPC when you have default one for you ? – For security as Default is too liberal

Module 15 – Hybrid Cloud and Networking

- ❑ Public, Private, Hybrid Clouds

- ❑ Hybrid , what it means in terms of N/W elements…let us see..
- ❑ How do you connect ? – **Direct Connect**, **VPN**

- ❑ Now when you have hybrid cloud how do you transfer data ? Any smart options for **large data sets** ?

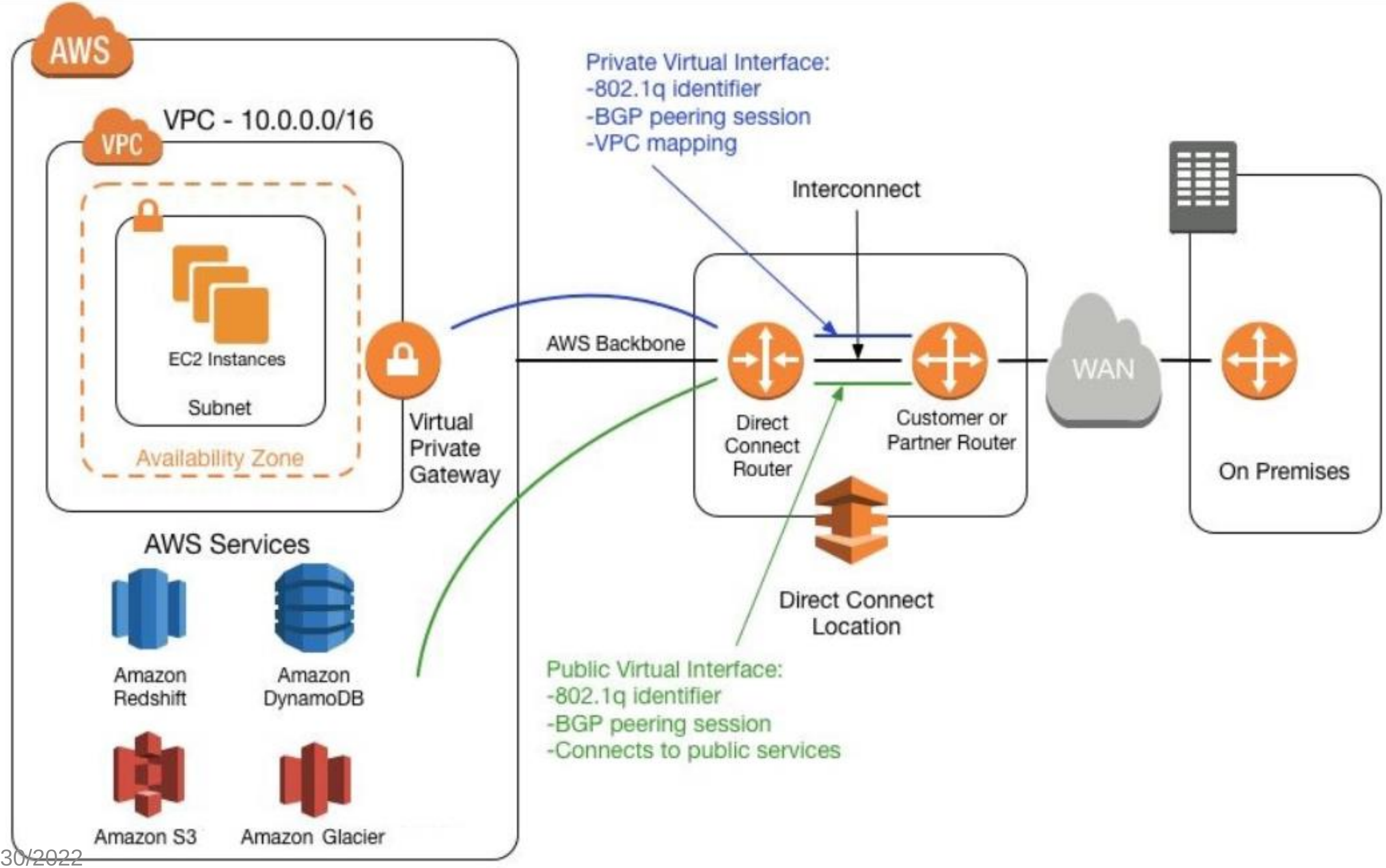
- ✓ Snow family! – **Snowball edge**, **Snowball**, **Snow Mobile**

- ❑ N/W element to think about when you configure N/W – **No CIDR overlap**…please

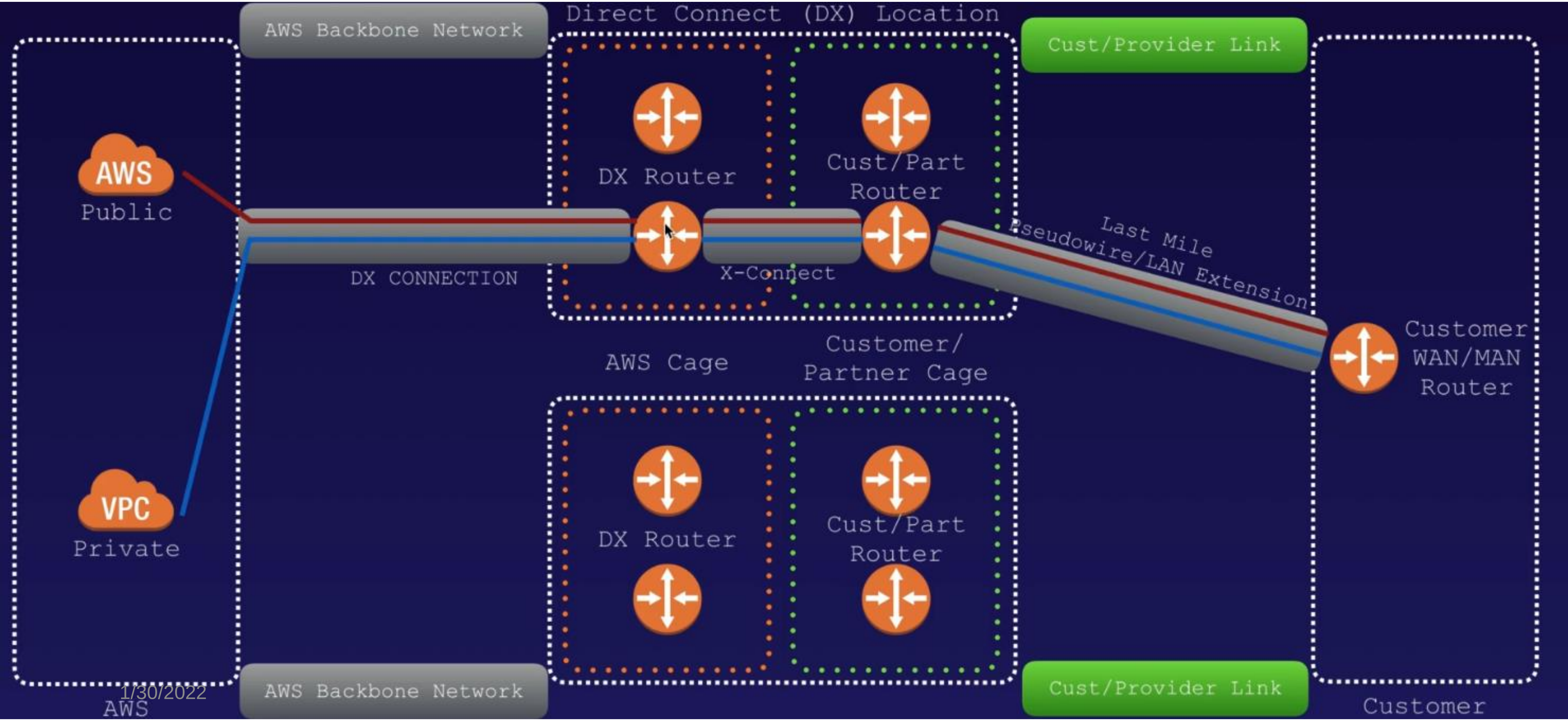
- ❑ What range of CIDR do you have /16 largest and /28 smallest
- ❑ ACL What is that ? – **Stateful Vs Stateless**
- ❑ VPC and subnets has **default limits per region** – but can be extended
- ➢ **Elastic IP** – Why ? – You want to use a fixed public IP (note for long term usage use Elastic IP), it is charged if unused.

Additional network interface can be used for Management N/W communication and be attached to Instances. Option -> EC2 console -> N/W interface -> Create Interface then Attach

Direct Connect – Let the diagram speak

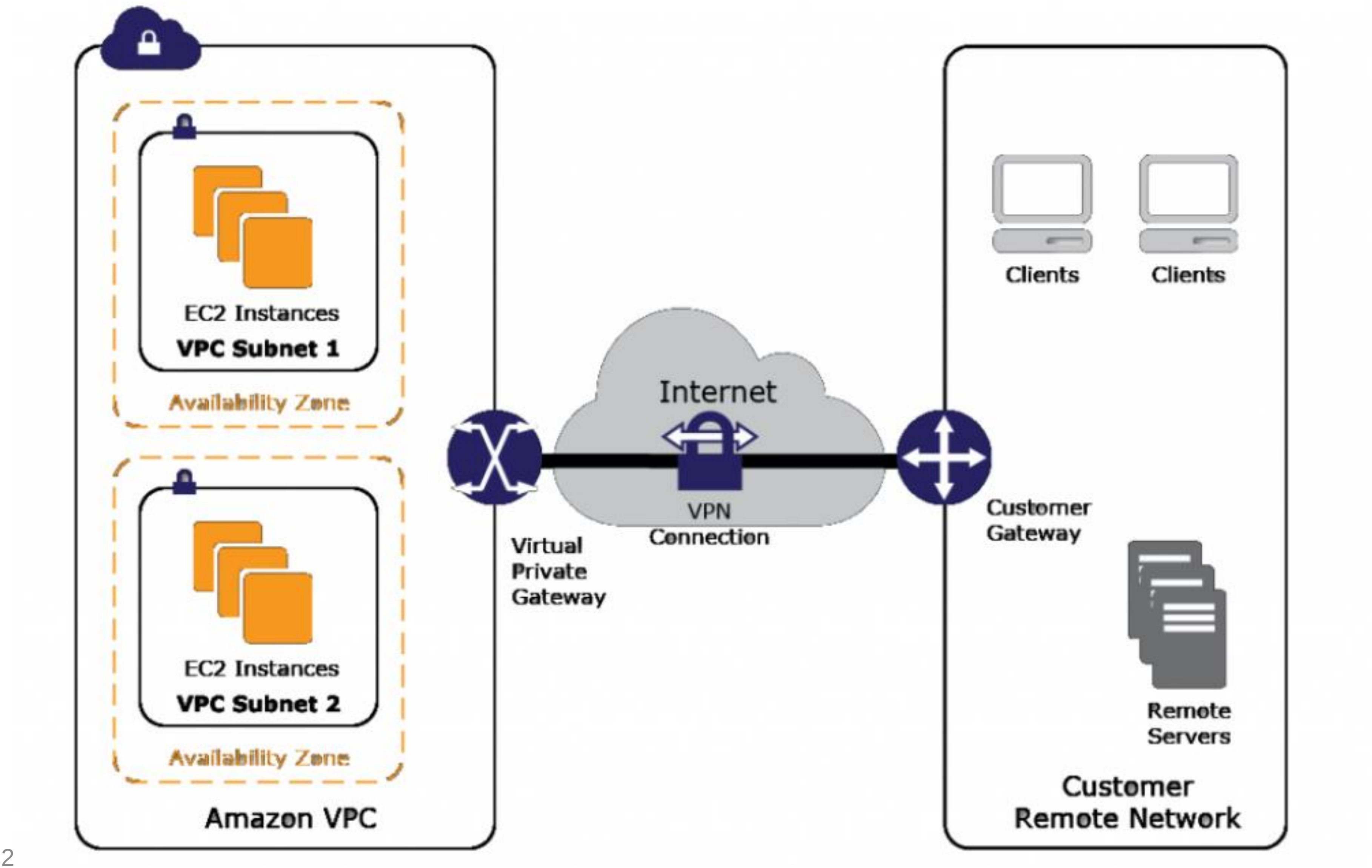


Another one – Direct Connect

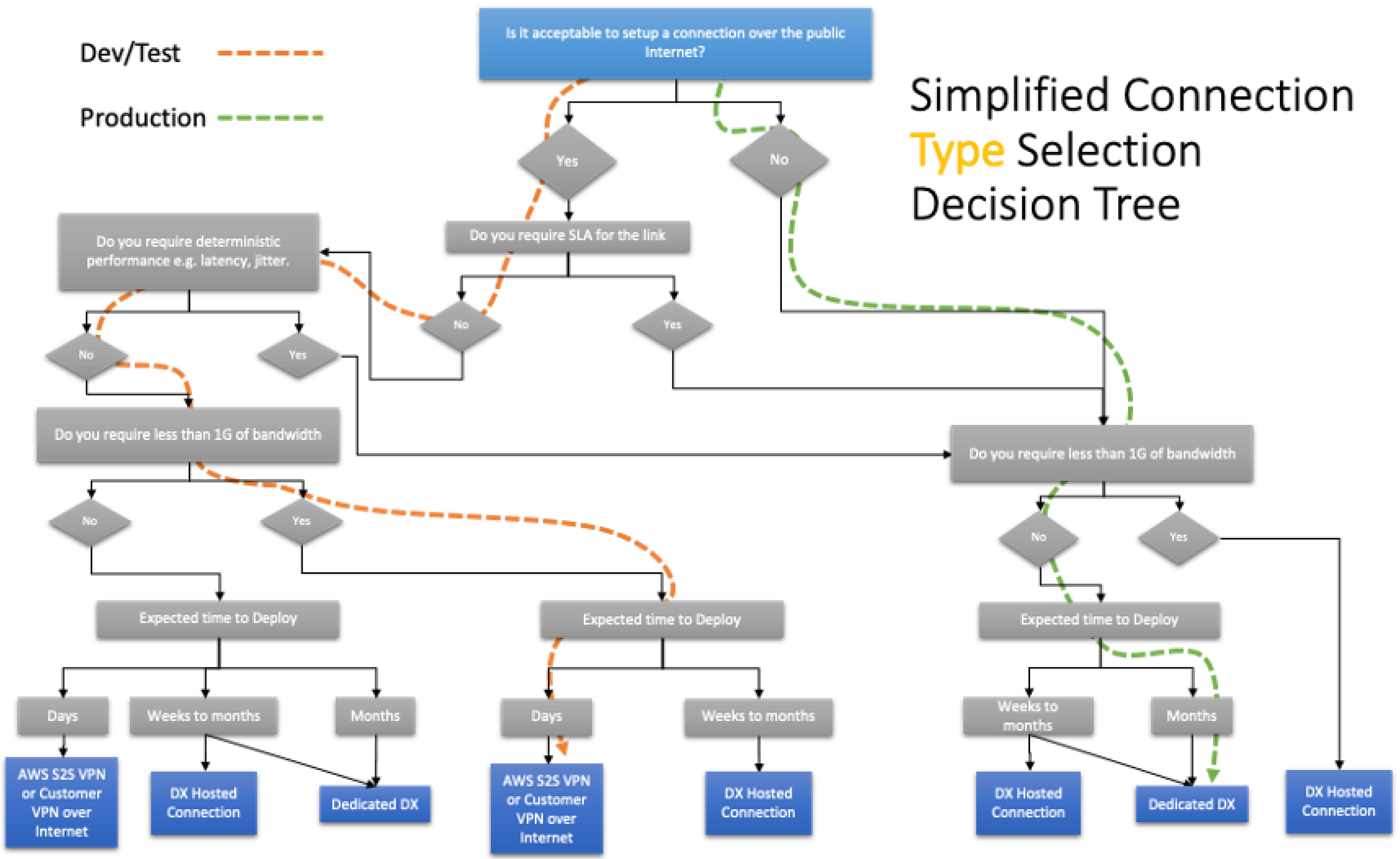


1/30/2022

AWS Managed VPN – Simple diagram



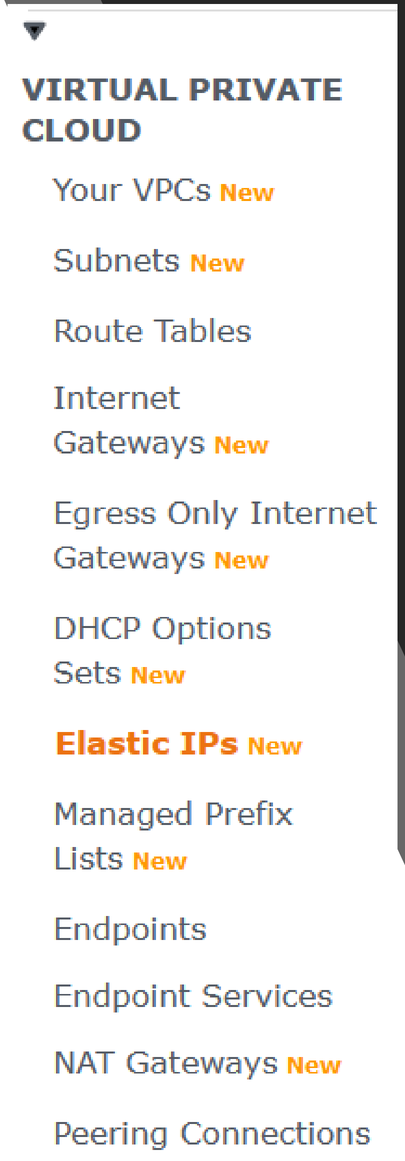
Process: Selecting & Designing Your Hybrid Connectivity Model


Dev/Test
Production
Is it acceptable to setup a connection over the public internet?
Yes
No
Do you require SLA for the link
No
Yes
Do you require deterministic performance e.g. latency, jitter.
No
Yes
Do you require less than 1G of bandwidth
No
Yes
Expected time to Deploy
Days
Weeks to months
Months
AWS S2S VPN or Customer VPN over Internet
DX Hosted Connection
Dedicated DX
Expected time to Deploy
Days
Weeks to months
AWS S2S VPN or Customer VPN over Internet
DX Hosted Connection
Do you require less than 1G of bandwidth
No
Yes
Expected time to Deploy
Weeks to months
Months
DX Hosted Connection
Dedicated DX
DX Hosted Connection

Simplified Connection Type Selection Decision Tree

Snow family – Interesting right ?

Learn more about Snowcone »
Learn more about Snowball »
Learn more about Snowmobile »



▼

VIRTUAL PRIVATE CLOUD

- Your VPCs New
- Subnets New
- Route Tables
- Internet Gateways New
- Egress Only Internet Gateways New
- DHCP Options Sets New
- **Elastic IPs** New
- Managed Prefix Lists New
- Endpoints
- Endpoint Services
- NAT Gateways New
- Peering Connections

- Module 16 – Walkthrough AWS VPC Console

Module 17 – Creating and using VPC- Step by Step

- ➢ VPC, Subnets, IG, NAT Instance Vs NAT G/W , RT, EC2 , SG – Order of creation
- ➢ Monitoring – VPC Flow logs – Captured at VPC, subnet and network interface level
- ✓ Final-outcome towards the end of the exercise – Separation of N/W and security
- ✓ Advantages of NAT G/W against NAT Instance – AWS manage Vs you manage, no bottleneck Vs HA and scalable by AWS, Not a bastion Vs can be used as bastion host

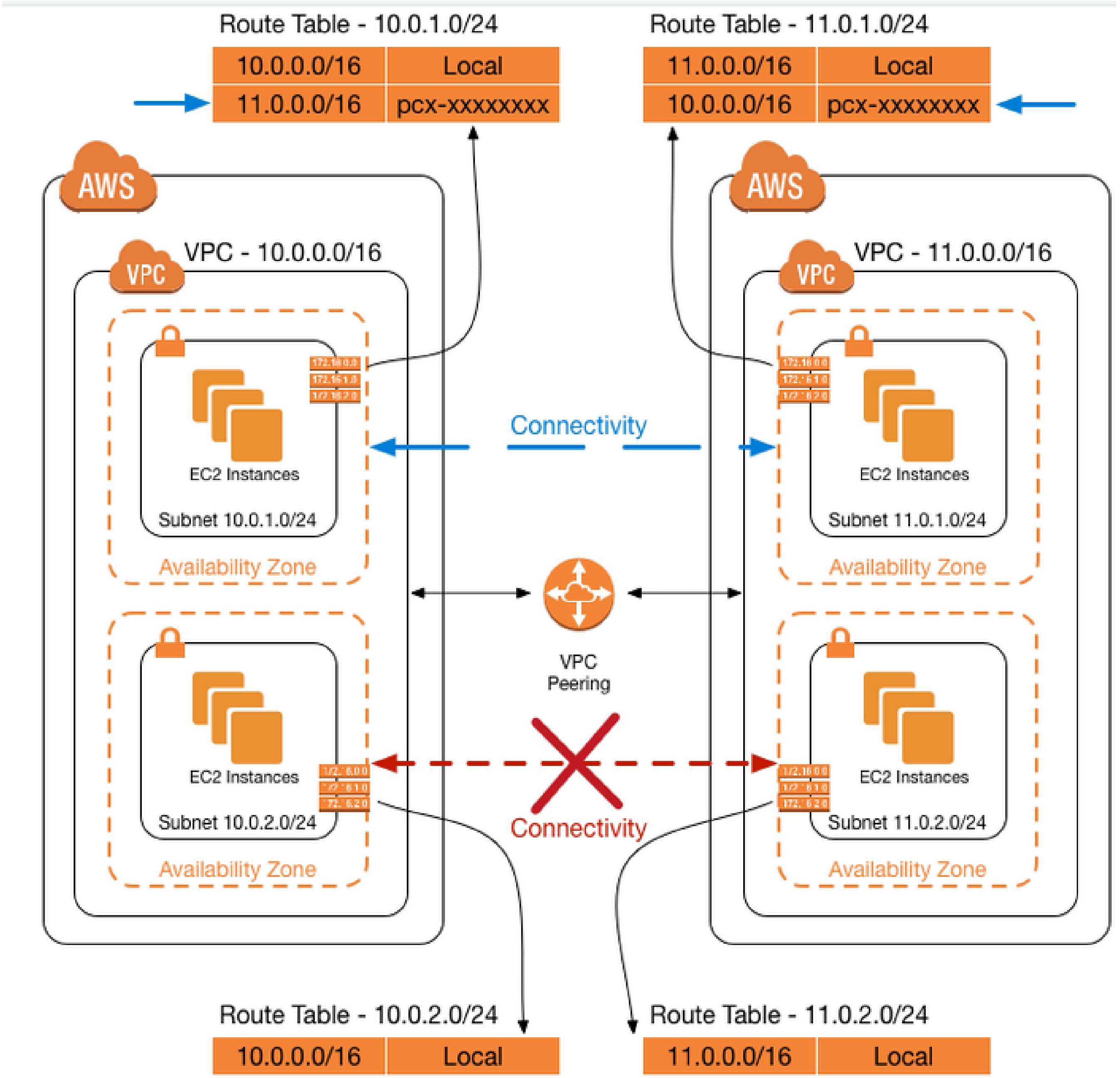
Module 18 – VPC Peering

Know the steps

VPC Peering – there is requestor and acceptor, RT entries.

NO Transitive - Which means

- If A->B and B->C is there , does not make it A-> C automatic



Route Table - 10.0.1.0/24

10.0.0.0/16	Local
11.0.0.0/16	pcx-xxxxxxxx

Route Table - 11.0.1.0/24

11.0.0.0/16	Local
10.0.0.0/16	pcx-xxxxxxxx

Route Table - 10.0.2.0/24

10.0.0.0/16	Local

Route Table - 11.0.2.0/24

11.0.0.0/16	Local

Module 19 – VPC Endpoint, Services, Route 53 & VPC endpoint in S3 and Global Accelerator

- **A VPC endpoint enables** you to ***privately connect*** your VPC to supported ***AWS services*** and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Traffic between your VPC and the other service ***does not leave the Amazon network***.

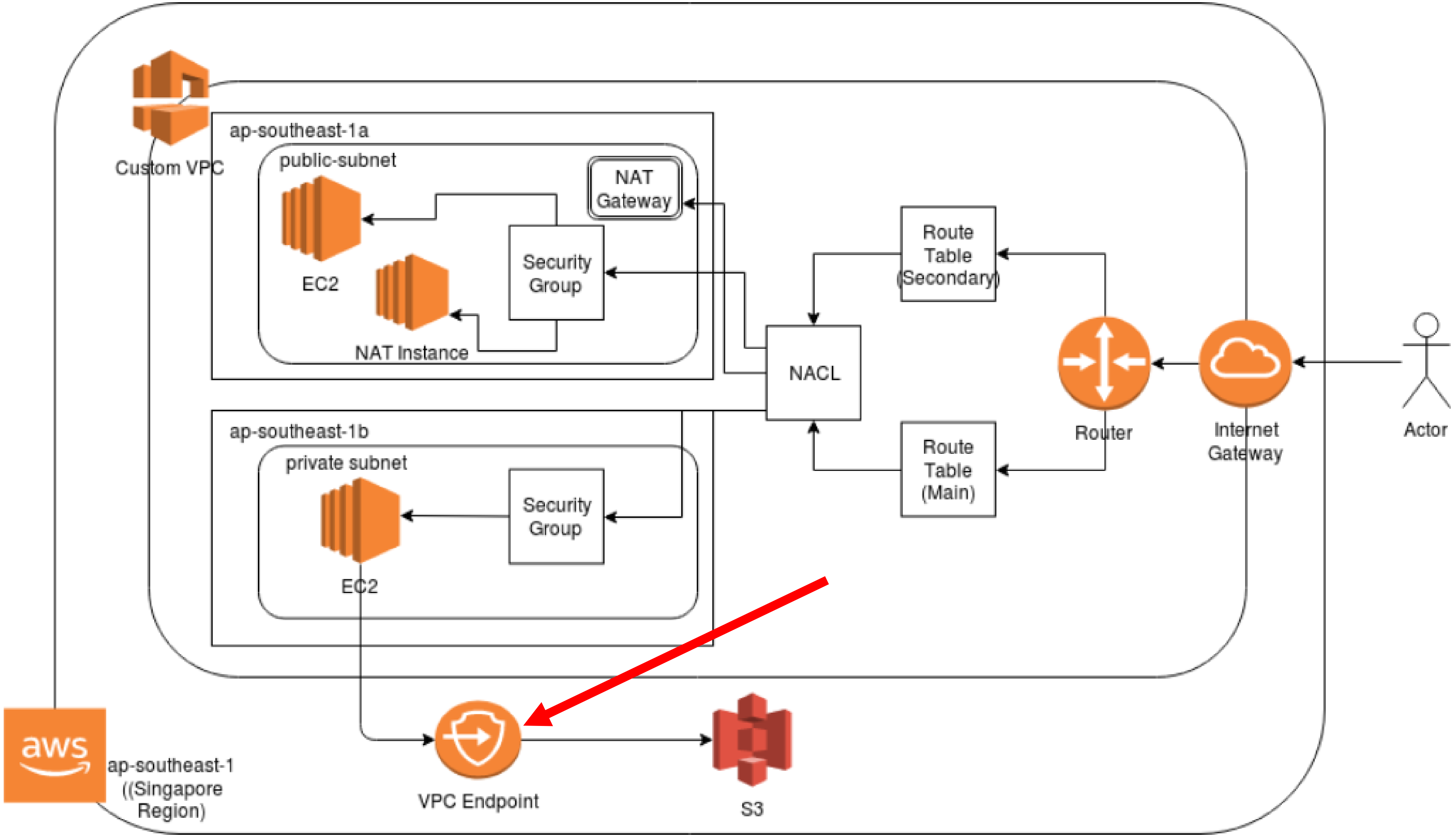
Endpoints are **virtual devices**. They are ***horizontally scaled, redundant, and highly available*** VPC components. There are two types of VPC endpoints: *interface endpoints* and *gateway endpoints*.

- **Interface endpoints** is an ***elastic network interface*** with a ***private IP address*** from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses.

- **Gateway endpoints** is a gateway that you specify as a ***target*** for a route in your ***route table*** for traffic destined to a supported AWS service. The following AWS services are supported:

- Amazon S3
- DynamoDB

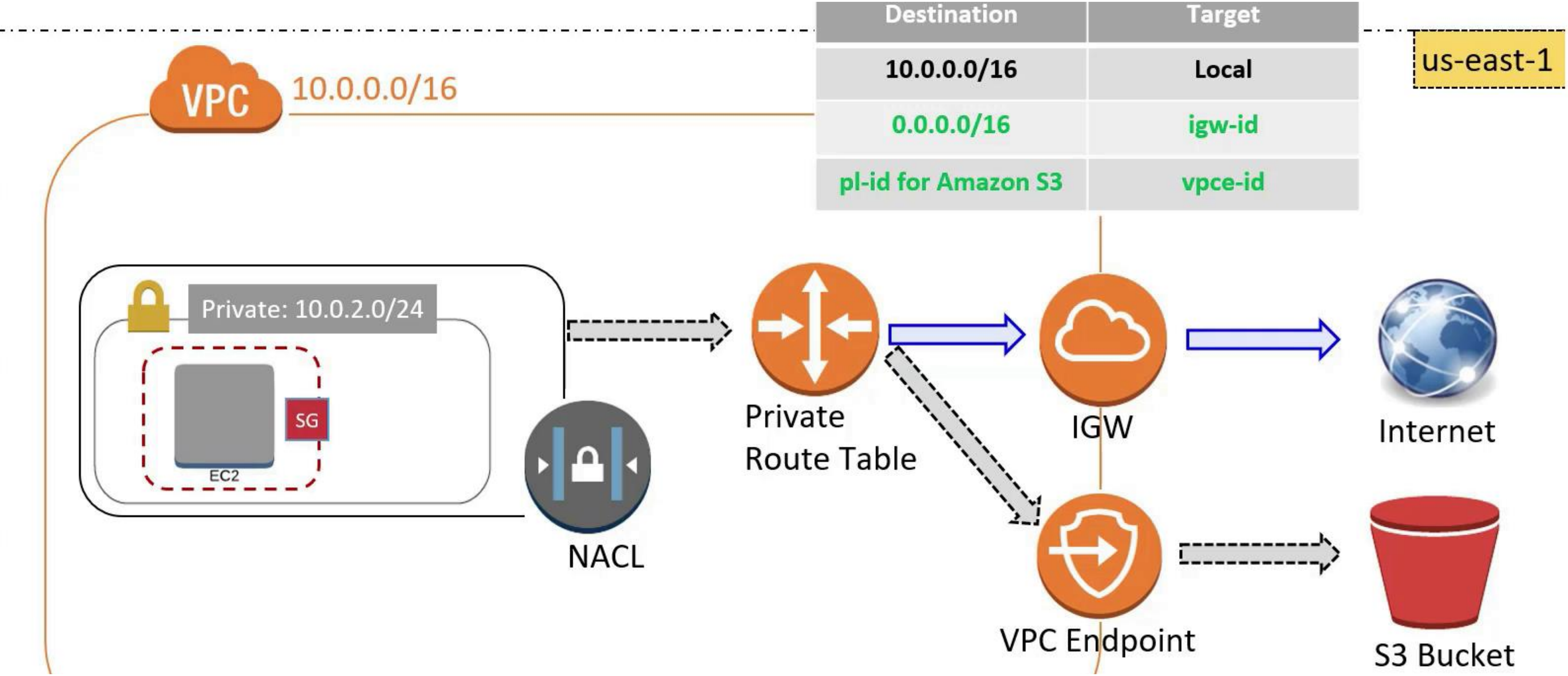
Diagram for VPC Gateway Endpoint - S3



1/30/2022

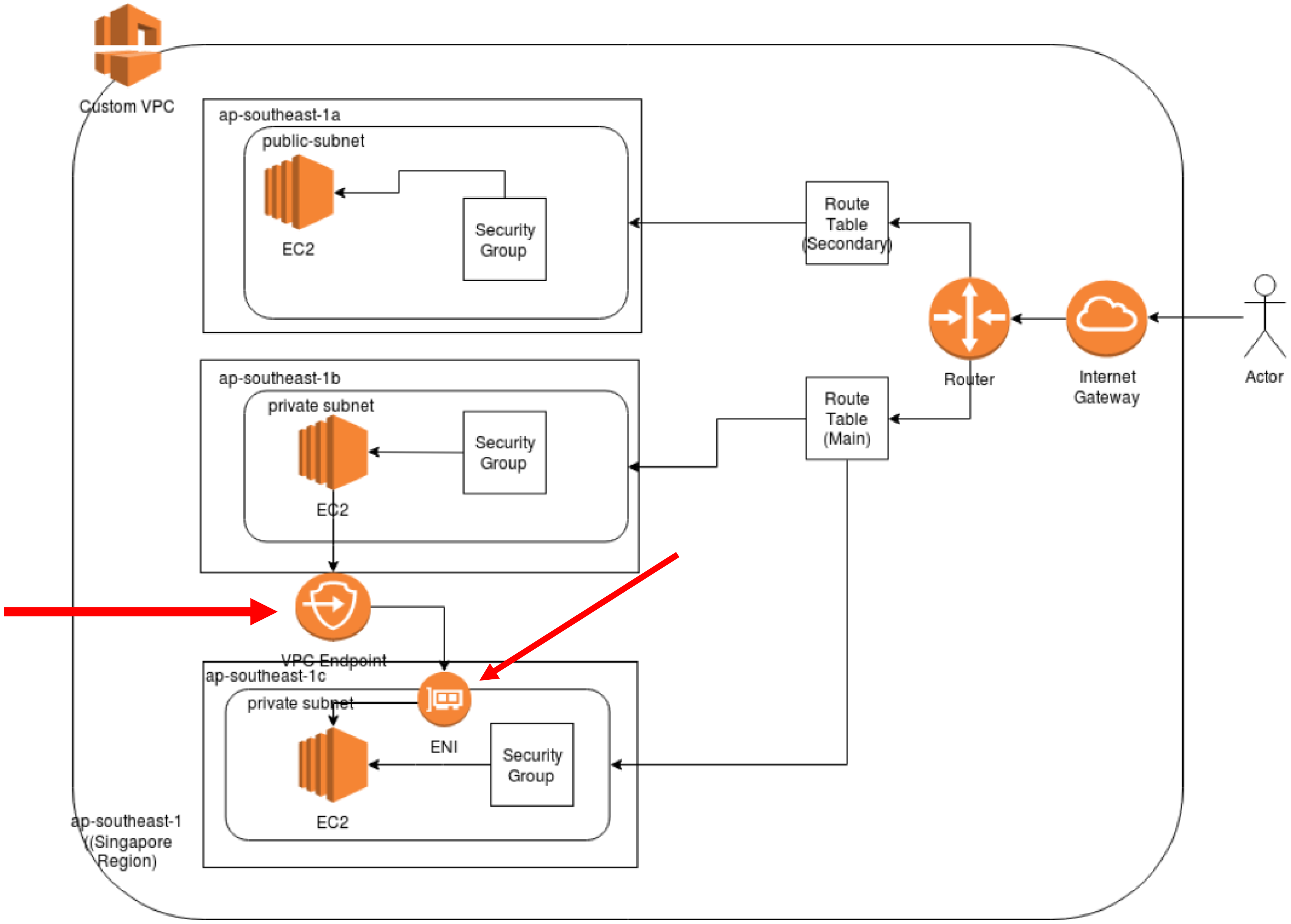
Connecting from an EC2 instance to AWS S3 via AWS VPC Gateway Endpoint

Gateway S3 Endpoint



Destination	Target
10.0.0.0/16	Local
0.0.0.0/16	igw-id
pl-id for Amazon S3	vpce-id

VPC Endpoint – Elastic Endpoint



Connecting from an EC2 instance to another EC2 instance via VPC Interface Endpoint

Route 53

- What is R53 and why the name !

- Little history – IANA controls root domains. Domain registrations , ICANN (company to process root level domain registration)

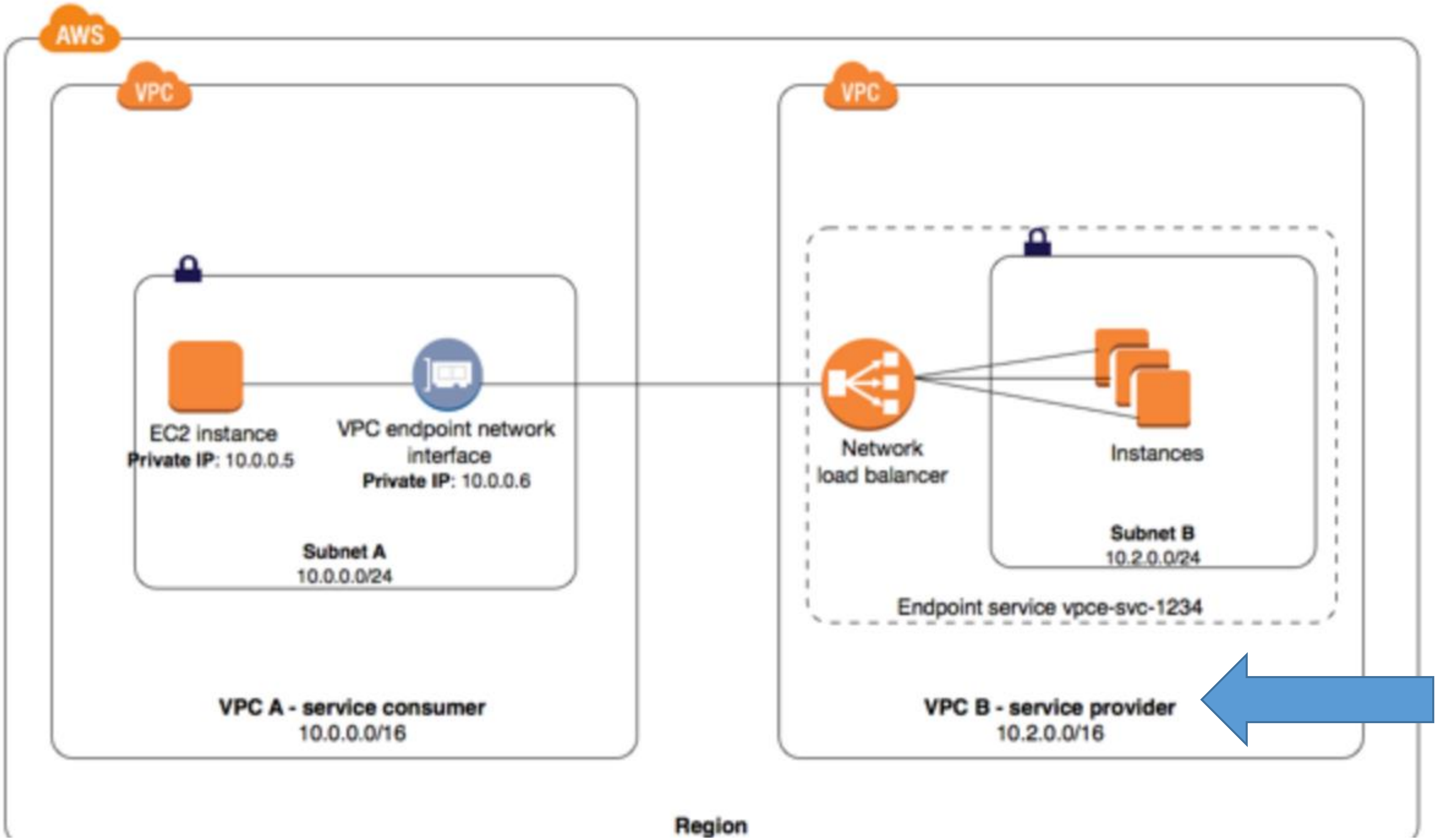
- Important concepts in DNS: SOA Records, NS, A, **CNAME**, MX, PTR , **ALIAS**

- Is R53 just a DNS service ?– Register domains, Routes traffic to resources, Checks health of resources
- **R53 policy**

1. **Simple** – Want to know more – It is **random** selection of records
2. **Weighted** – Distribute into **%** - Remember you can create HC record in record set.
3. **Latency** based – Based on point in time latency (it variable) - Remember latency and Geo-proximity will not be always true !
4. **Failover** – Create **Active/Passive** (here it is via HC again)
5. **Geolocation** – Self explanatory , e.g US users traffic goes to US and EU users goes to EU – Think why would you need it ?
6. **Geo-proximity** – location of user & resource and you define a bias – Quite advanced way….
7. **Multivalue** answer policy – **Simple with HC**

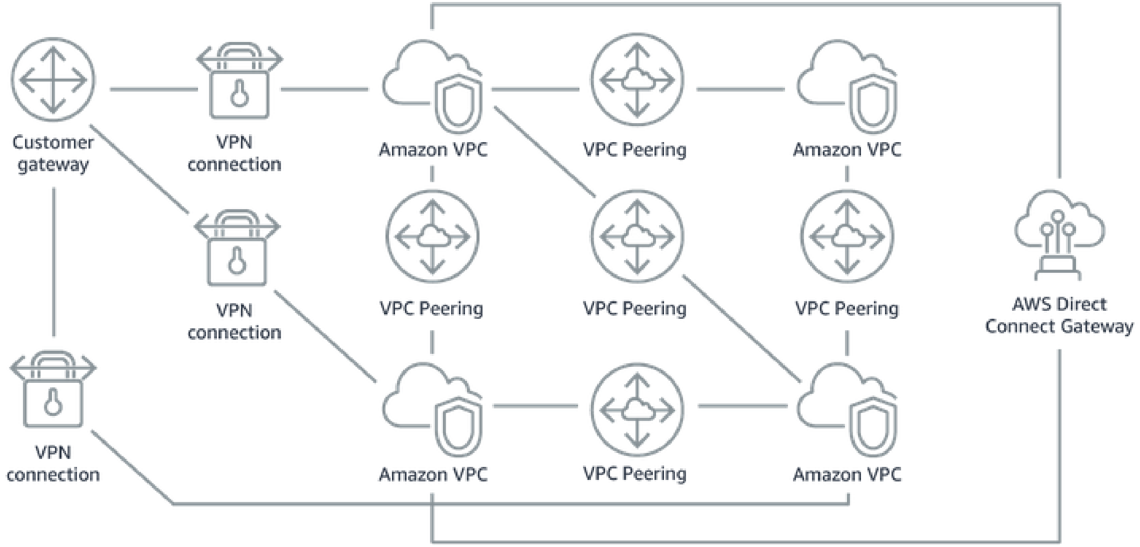
VPC Private Link / VPC Endpoint service

- ✓ Why you need this end point services ?
- ✓ What is required at customer end ? – Network interface



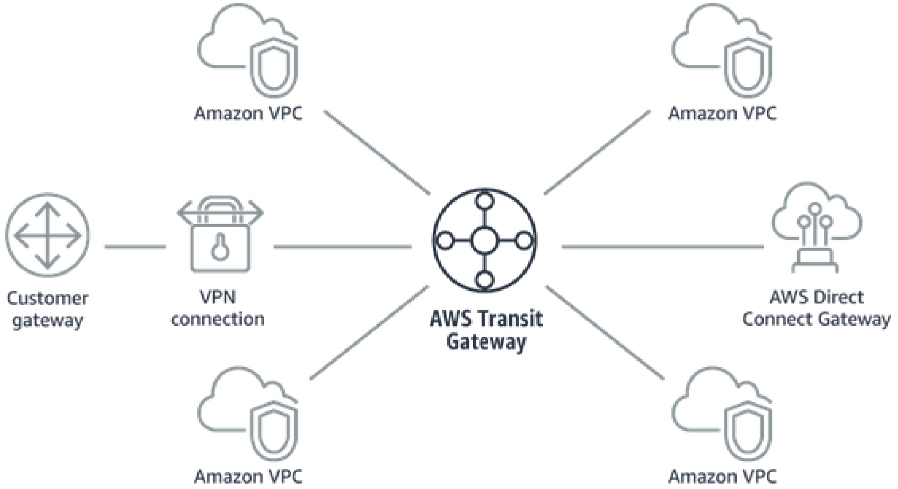
Transit Gateways

Without AWS Transit Gateway



Complexity increases with scale. You must maintain routing tables within each VPC and connect to each onsite location using separate network gateways.

With AWS Transit Gateway

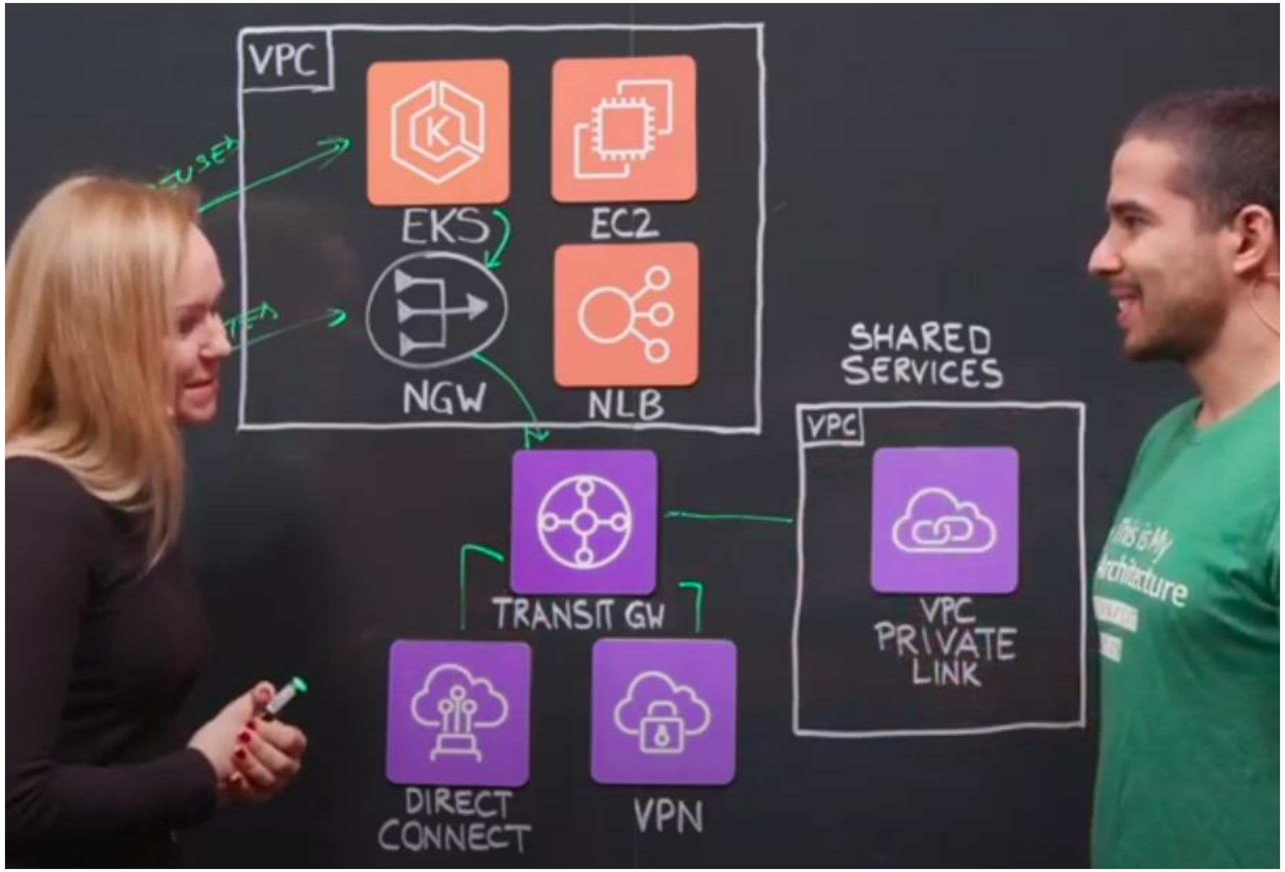


Your network is streamlined and scalable. AWS Transit Gateway routes all traffic to and from each VPC or VPN, and you have one place to manage and monitor it all.

Explanation above

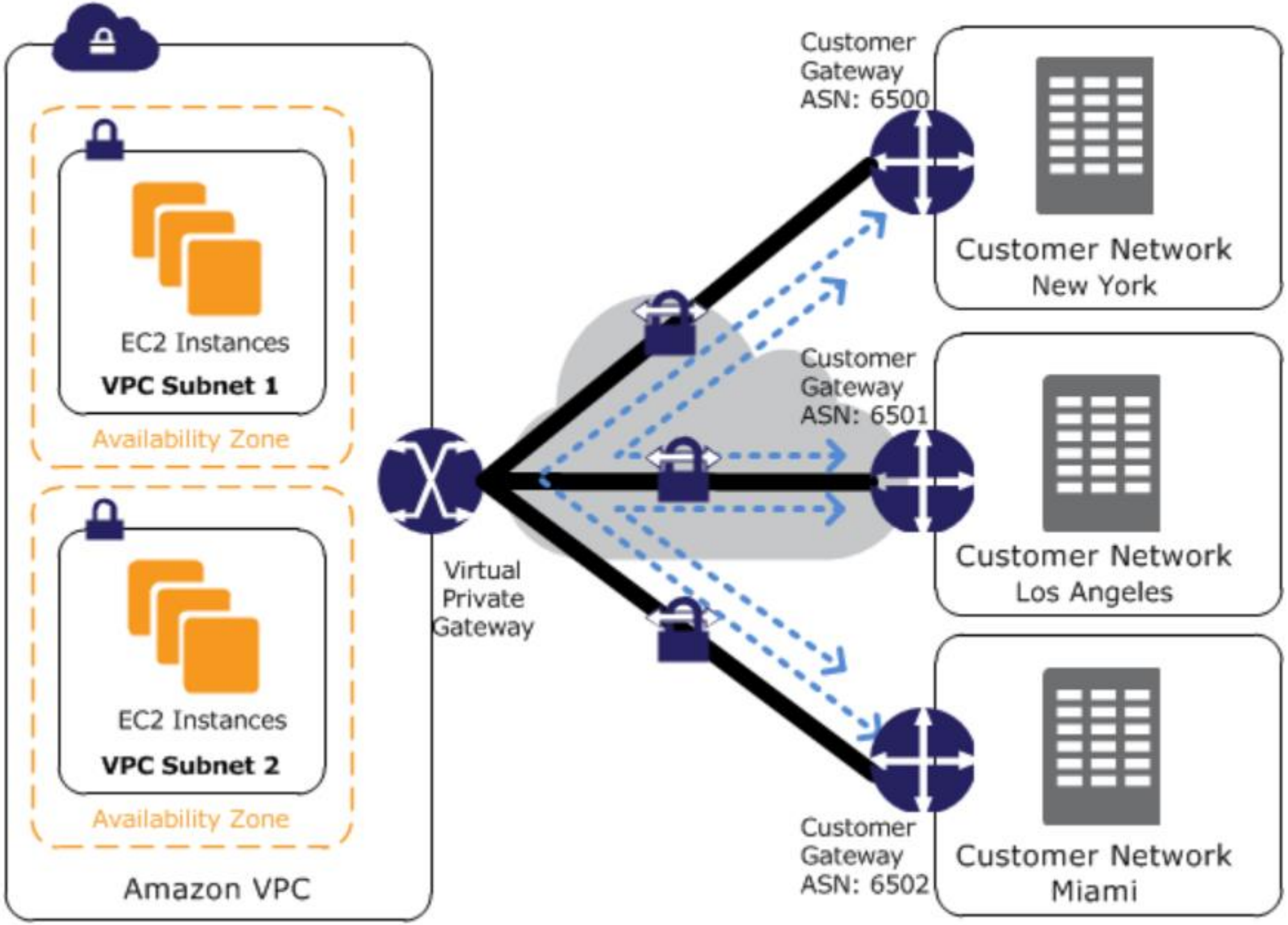
Case - 1000’ of VPCs @Adobe

- 1000’ of AWS accounts and hence 1000’ of VPCs, manage that!
- Issue with setup, lots of confusion, obviously
- IP CIDR allocation strategy [*Reuse CIDR, Routed CIDR*]
- All VPCs are connecting to the “**Transit Gateway**” for information exchange and apps connecting to each other
- 3rd party/ customers exposing services via “VPC Private link” for private data sharing with Adobe



VPN CloudHub

- ✓ What ? Hub and spoke for your multiple VPN
- ✓ Why ? If you have multiple AWS Site-to-Site VPN connections, you can provide ***secure communication between sites***.



Module 20– WAF and WAF Next Generation

- ✓ What is WAF – Layer 7 Firewall. – Allow, Block or Count
- ✓ What does next Gen offer ? – Prime ones -AWS managed rules, WebACL Based on computing needs, rule nesting.
- ✓ What are the AWS resources it can associate it (at this moment!) – CloudFront, API G/W, ALB, AWS App Sync

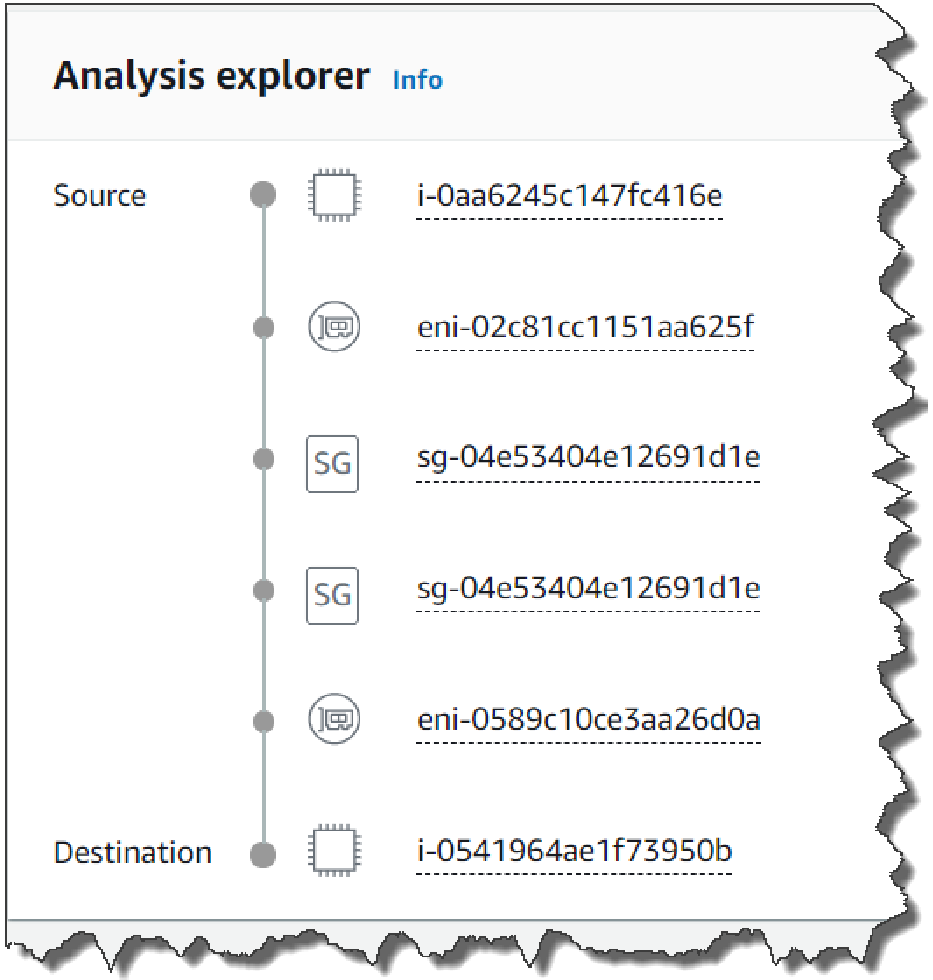
Lab – Important to know the Inspect , Matching condition and Text transformation criteria

Do read the capacity Unit – As on date of this lecture – 1500CU/WebACL
Pricing – per ACL per month, per rule per month, per million requests processed

AWS Shield - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS

What’s new?

- VPC **Reachability Analyzer**
- Ensuring Your Network Configuration is as Intended
- You have full control over your virtual network environment, including choosing your own IP address range, creating subnets, and configuring route tables and network gateways.
- You can also easily customize the network configuration of your VPC.
- Security-sensitive backend systems such as databases and application servers can be placed on private subnets that do not have internet access.
- You can use multiple layers of security, such as security groups and network access control list (ACL), to control access to entities of each subnet by protocol, IP address, and port number.



Analysis explorer Info

Source i-0aa6245c147fc416e

eni-02c81cc1151aa625f

SG sg-04e53404e12691d1e

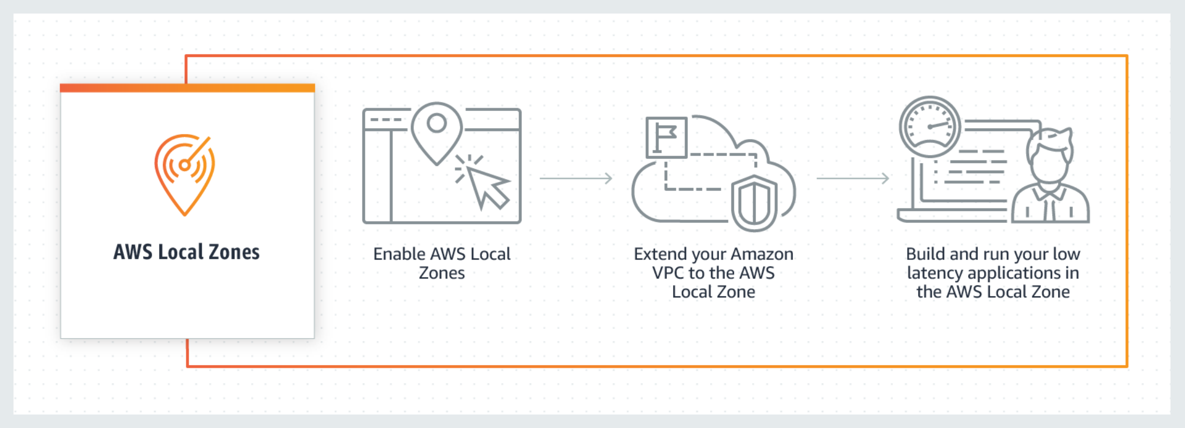
SG sg-04e53404e12691d1e

eni-0589c10ce3aa26d0a

Destination i-0541964ae1f73950b

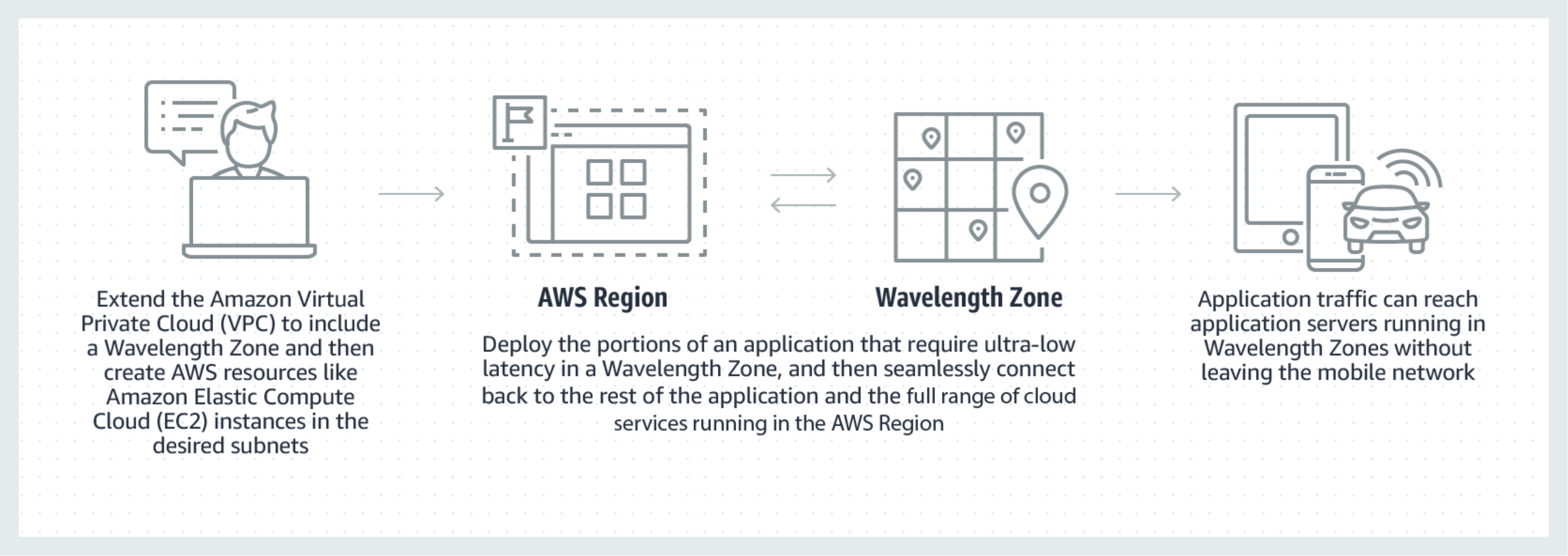
Local zones

- AWS Local Zones are a type of AWS infrastructure deployment that **places AWS** compute, storage, database, and other select services **close to large population, industry, and IT centers**.
- You can easily run applications that need single-digit millisecond latency closer to end-users in a specific geography.
- Ideal for use cases such as media & entertainment content creation, real-time gaming, live video streaming, and machine learning inference.
- They are an **extension of an AWS Region** where you can run your latency-sensitive applications using AWS services
- Note :Available only in Los Angles, preview in Boston, Houston, Miami at this time


AWS Local Zones
Enable AWS Local Zones
Extend your Amazon VPC to the AWS Local Zone
Build and run your low latency applications in the AWS Local Zone

Wavelength zones

- AWS Wavelength is an AWS Infrastructure offering optimized for mobile edge computing applications.
- Wavelength Zones are AWS infrastructure deployments that **embed AWS** compute and storage services **within** communications service providers' **(CSP)** datacenters at the edge of the 5G network, so application traffic from 5G devices can reach application servers running in Wavelength Zones without leaving the telecommunications network.
- This avoids the latency that would result from application traffic having to traverse multiple hops across the Internet to reach their destination, enabling customers to take full advantage of the latency and bandwidth benefits offered by modern 5G networks.
- AWS Wavelength Zones are available in ten cities across the U.S. with Verizon, in Tokyo and Osaka, Japan with KDDI, and in Daejeon, South Korea with SKT.



Extend the Amazon Virtual Private Cloud (VPC) to include a Wavelength Zone and then create AWS resources like Amazon Elastic Compute Cloud (EC2) instances in the desired subnets

AWS Region

Wavelength Zone

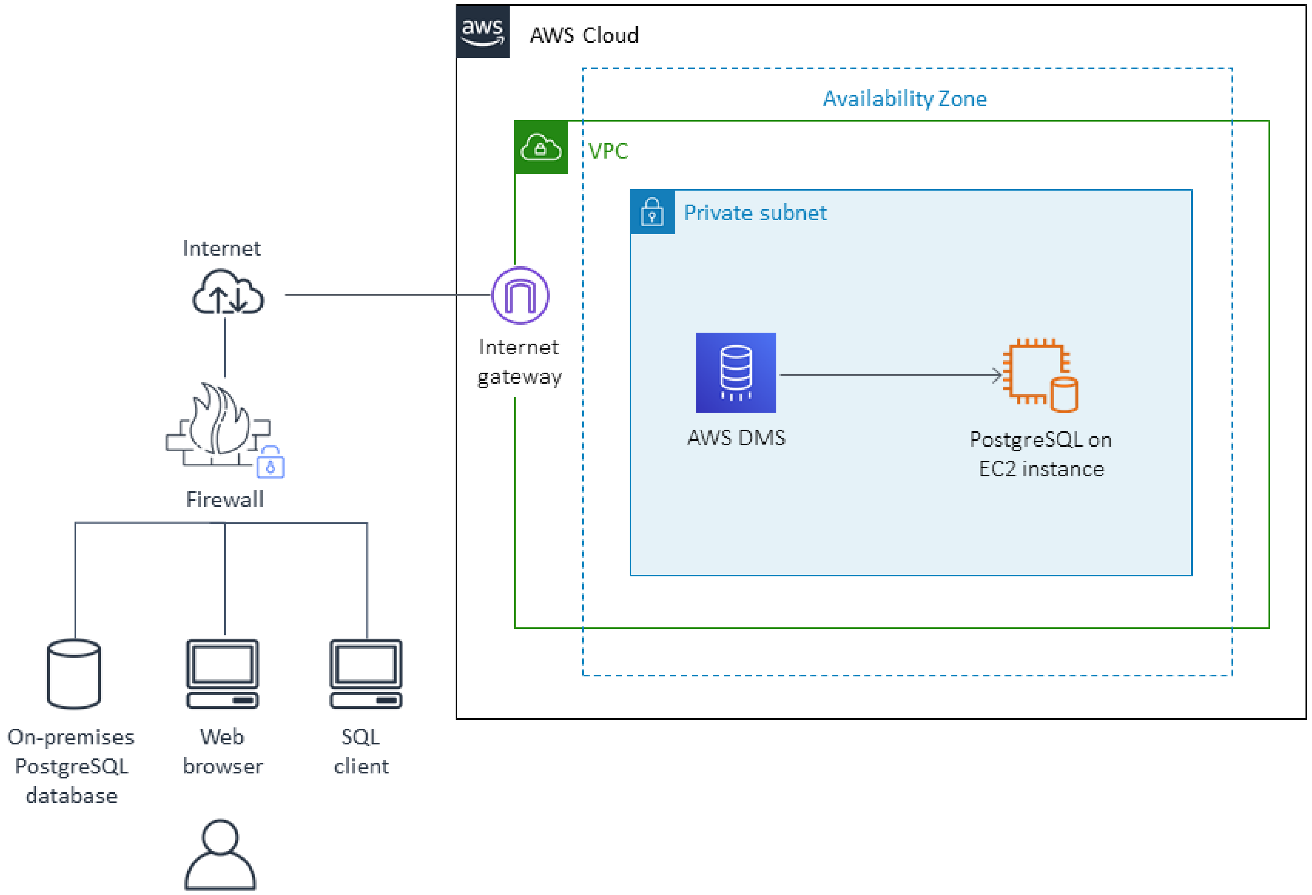
Deploy the portions of an application that require ultra-low latency in a Wavelength Zone, and then seamlessly connect back to the rest of the application and the full range of cloud services running in the AWS Region

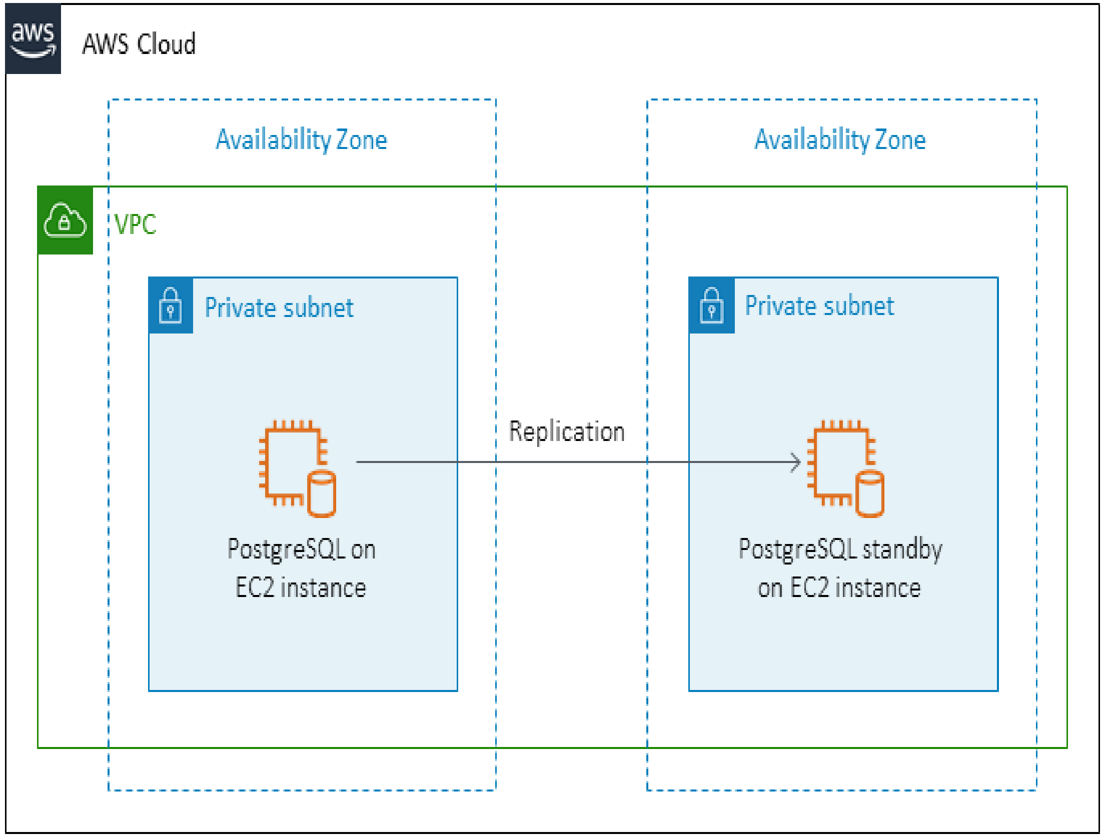
Application traffic can reach application servers running in Wavelength Zones without leaving the mobile network

Q&A

greatlearning

Case: Application & Database migration





Thank you

Happy Learning!